# Yealink

# VP59/SIP-T58A/CP960 IP Phones Administrator Guide

# Copyright

**Copyright © 2019 YEALINK(XIAMEN) NETWORK TECHNOLOGY**

# Trademarks

# End User License Agreement

# Patent Information

# 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.

# Before You Begin

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 running firmware version 83:

- VP59 flagship smart video phones.
- T58A smart business phones.
- CP960 IP conference phones.
- Expansion modules: EXP50.

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/phone user interface items such as menus, menu selections, soft keys, or directory names when they are involved in a procedure or user action (for example, click **Settings**->**Upgrade**.).<br><br>Also used to emphasize text (for example, **Important!**). |
| *Italics* | Used to emphasize text, to show the example values or inputs (format of examples: *http(s)://[IPv6 address]*). |
| 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**->**Basic Settings** indicates that you need to select **Basic Settings** from the **Settings** menu. |

# Table of Contents

# Getting Started

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

**Topics**

## 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.

## Yealink IP Phones in a Network

Most Yealink phones are connected physically through a Category 5E (CAT5E) cable to a 10/100/1000Mbps Ethernet LAN, and send and receive all data using the same packet-based technology. Some phones support the wireless network.

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

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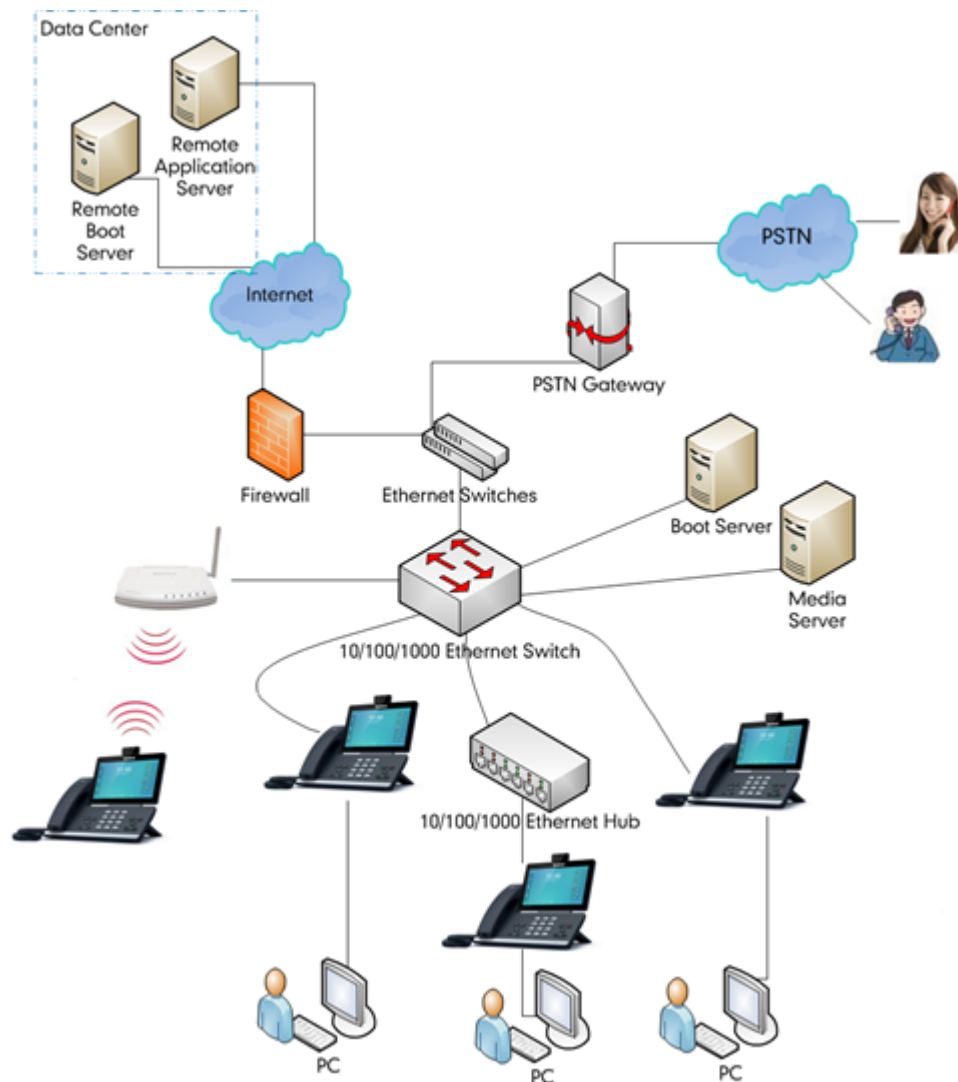
# Initialization Process Overview

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

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 IP phone begins the initialization process, it cycles through the following steps:

1. The power LED indicator/mute LED indicator glows red.
2. The message "Welcome Initializing... please wait" appears on the phone screen when the IP phone starts up.
3. The main phone screen displays the following:
   - Time and date
   - Android keys (for VP59/T58A)
   - Pre-installed applications (for CP960)
4. Tap **Settings**->**Status** to check the IP phone status, the phone screen displays the valid IP address, MAC address, firmware version, and so on.

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

# Phone Network

You can make custom network configurations.

## Topics

## IPv4 and IPv6 Network Settings

You can configure the phones to operate in IPv4, IPv6, or dual stack (IPv4/IPv6) mode.

After establishing network connectivity, the phones obtain the IPv4 or IPv6 network settings from a Dynamic Host Configuration Protocol (DHCPv4 or DHCPv6) server. We recommend using DHCP where 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 DHCPv6 specifications documented in RFC 3315. |

## Topics

### 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<br>**1**-IPv6<br>**2**-IPv4 & IPv6 | |
| Default | 0 | |

| Web UI | Network->Basic->Internet Port->Mode (IPv4/IPv6) |
|---|---|
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->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.<br><br>**Note**: It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). | |
| Permitted Values | **0**-DHCP<br><br>**1**-PPPoE (not applicable to VP59 phones)<br><br>**2**-Static IP | |
| Default | 0 | |
| Web UI | Network->Basic->IPv4 Config->Configuration Type | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->Type | |
| Parameter | static.network.internet_port.ip[1] | <y0000000000xx>.cfg |
| Description | It configures the IPv4 address.<br><br>**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). | |
| Permitted Values | IPv4 Address | |
| Default | Blank | |
| Web UI | Network->Basic->IPv4 Config->Configuration Type (Static IP)->IP Address | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->Type (Static IP) ->IP Address | |
| Parameter | static.network.internet_port.mask[1] | <y0000000000xx>.cfg |
| Description | It configures the IPv4 subnet mask.<br><br>**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). | |
| Permitted Values | Subnet Mask | |
| Default | Blank | |
| Web UI | Network->Basic->IPv4 Config->Configuration Type (Static IP)->Subnet Mask | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->Type (Static IP) ->Subnet Mask | |
| Parameter | static.network.internet_port.gateway[1] | <y0000000000xx>.cfg |
| Description | It configures the IPv4 default gateway.<br><br>**Note**: It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "stat- | |

| | ic.network.internet_port.type" is set to 2 (Static IP). | |
|---|---|---|
| **Permitted Values** | IPv4 Address | |
| **Default** | Blank | |
| **Web UI** | Network->Basic->IPv4 Config->Configuration Type (Static IP)->Default Gateway | |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->Type (Static IP) ->Gateway | |
| **Parameter** | static.network.static_dns_enable[1] | <y0000000000xx>.cfg |
| **Description** | It triggers the static DNS feature to on or off.<br><br>**Note**: It works only if "static.network.internet_port.type" is set to 0 (DHCP). | |
| **Permitted Values** | **0**-Off, the phone will use the IPv4 DNS obtained from DHCP.<br><br>**1**-On, the phone will use manually configured static IPv4 DNS. | |
| **Default** | 0 | |
| **Web UI** | Network->Basic->IPv4 Config->Static DNS | |
| **Phone UI** | Settings->Advanced Settings (default password: admin)->Network->WAN Port->IPv4->Type (DHCP) ->Static DNS | |
| **Parameter** | static.network.primary_dns[1] | <y0000000000xx>.cfg |
| **Description** | It configures the primary IPv4 DNS server.<br><br>**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->Configuration Type (Static IP)/Configuration Type (DHCP)->Primary DNS | |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->Static DNS (Enabled) ->Primary DNS | |
| **Parameter** | static.network.secondary_dns[1] | <y0000000000xx>.cfg |
| **Description** | It configures the secondary IPv4 DNS server.<br><br>**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->Configuration Type (Static IP)/Configuration Type (DHCP)->Secondary DNS | |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->Static DNS (Enabled) ->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), DHCPv6 or by manually entering an IP address. Ensure that your network environment supports IPv6. Contact your ISP for more information.

When you enable both SLAAC and DHCPv6 on the phone, the server can specify the IP phone to obtain the IPv6 address and other network settings either from SLAAC or from DHCPv6, if the SLAAC server is not working, the phone will try to obtain the IPv6 address and other network settings via DHCPv6.

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. <br><br> **Note**: It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). | |
| Permitted Values | **0**-DHCP <br><br> **1**-Static IP | |
| Default | 0 | |
| Web UI | Network->Basic->IPv6 Config->Configuration Type | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->Type | |
| Parameter | static.network.ipv6_internet_port.ip[1] | <y0000000000xx>.cfg |
| Description | It configures the IPv6 address. <br><br> **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). | |
| Permitted Values | IPv6 Address | |
| Default | Blank | |
| Web UI | Network->Basic->IPv6 Config->Configuration Type (Static IP)->IP Address | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->Type (Static IP) ->IP Address | |
| Parameter | static.network.ipv6_prefix[1] | <y0000000000xx>.cfg |
| Description | It configures the IPv6 prefix. <br><br> **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). | |
| Permitted Values | Integer from 0 to 128 | |
| Default | 64 | |
| Web UI | Network->Basic->IPv6 Config->Configuration Type (Static IP)->IPv6 Prefix(0~128) | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->Type (Static IP) ->IPv6 IP Prefix | |
| Parameter | static.network.ipv6_internet_port.gateway[1] | <y0000000000xx>.cfg |
| Description | It configures the IPv6 default gateway. <br><br> **Note**: It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "stat- | |

| | |
|---|---|
| | ic.network.ipv6_internet_port.type" is set to 1 (Static IP). |
| **Permitted Values** | IPv6 Address |
| **Default** | Blank |
| **Web UI** | Network->Basic->IPv6 Config->Configuration Type (Static IP)->Default Gateway |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->Type (Static IP) ->Gateway |

| **Parameter** | static.network.ipv6_static_dns_enable[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It triggers the static IPv6 DNS feature to on or off.<br><br>**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.<br><br>**1**-On, the phone will use manually configured static IPv6 DNS. | |
| **Default** | 0 | |
| **Web UI** | Network->Basic->IPv6 Config->Static IPv6 DNS | |
| **Phone UI** | Settings->Advanced Setting (default: admin) ->Network->WAN Port->IPv6->Type (DHCP) ->Static DNS | |

| **Parameter** | static.network.ipv6_primary_dns[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the primary IPv6 DNS server.<br><br>**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 IPv6 DNS->Primary DNS | |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->Type (Static IP) ->Primary DNS<br><br>Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->Type (DHCP) ->Static DNS (Enabled) ->Primary DNS | |

| **Parameter** | static.network.ipv6_secondary_dns[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the secondary IPv6 DNS server.<br><br>**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 IPv6 DNS->Secondary DNS | |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->Type (Static IP) ->Secondary DNS<br><br>Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv6->Type (DHCP) ->Static DNS (Enabled) ->Secondary DNS | |

| Parameter | static.network.ipv6_icmp_v6.enable[1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to obtain IPv6 network settings via SLAAC (Stateless Address Auto-configuration).<br><br>**Note**: It works only if "static.network.ipv6_internet_port.type" is set to 0 (DHCP). | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Web UI | Network->Advanced->ICMPv6 Status->Active | |

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

# DHCP Option for IPv4

The 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

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. |

| Parameters | DHCP Option | Description |
|---|---|---|
| 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 automatically detects the DHCP option for obtaining the provisioning server address. The priority is as follows: custom option>option 66 (identify the TFTP server)>option 43.

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

| Note |
|---|
| If you fail to configure the DHCP options for discovering the provisioning server on the DHCP server, enable the phone to automatically discover the provisioning server address. 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. |

### 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.

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 | For VP59: VP59. | |

| | For T58A: SIP-T58. |
|---|---|
| | For CP960: SIP-CP960. |
| **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. Servers can use option 43 to return the vendor-specific information to the client.

You can set the DHCP option 60 type.

## Topic

## 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.<br>**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->DHCP Option Value | |

# PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) is a network protocol used by Internet Service Providers (ISPs) to provide Digital Subscriber Line (DSL) high-speed Internet services. PPPoE allows an office or building-full of users to share a common DSL connection to the Internet.

PPPoE connection is supported by the IP phone Internet port. Contact your ISP for the PPPoE user name and password.

It is not applicable to VP59 phones.

## Topic

## PPPoE Configuration

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

| Parameter | static.network.pppoe.user[1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the user name for PPPoE connection.<br><br>**Note**: It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 1 (PPPoE). It is not applicable to VP59 phones. | |
| Permitted Values | String within 32 characters | |
| Default | Blank | |
| Web UI | Network->Basic->IPv4 Config->Configuration Type (PPPoE)->PPPoE->User | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->Type (PPPoE) ->PPPoE User | |
| Parameter | static.network.pppoe.password[1] | <y0000000000xx>.cfg |
| Description | It configures the password for PPPoE connection.<br><br>**Note**: It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 1 (PPPoE). It is not applicable to VP59 phones. | |
| Permitted Values | String within 99 characters | |
| Default | Blank | |
| Web UI | Network->Basic->IPv4 Config->Configuration Type (PPPoE)->PPPoE->Password | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->WAN Port->IPv4->Type (PPPoE) ->PPPoE Password | |

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

# VLAN

The purpose of VLAN configurations on the phone is to insert a tag with VLAN information to the packets generated by the phone. When VLAN is properly configured for the ports (Internet port and PC port) on the 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 advertise its identity and capabilities on the local network.

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 and obtain their VLAN IDs.

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<br>**1**-Enabled, the phone attempts to determine its VLAN ID through LLDP. | |
| **Default** | 1 | |
| **Web UI** | Network->Advanced->LLDP->Active | |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->LLDP->LLDP Status | |
| **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.<br>**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) | |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->LLDP->Packet Interval | |

[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 local network.

When CDP feature is enabled on the phones, the phones periodically advertise their own information to the directly connected CDP-enabled switch. The phones can also receive LLDP packets from the connected switch and obtain their VLAN IDs.

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<br>**1**-Enabled, the phone attempts to determine its VLAN ID through CDP. | |
| **Default** | 1 | |

| Web UI | Network->Advanced->CDP->Active |
|---|---|
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->CDP->CDP Status |
| 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) |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->CDP->Packet Interval |

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

## Manual VLAN Configuration

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

For CP960 phones, you can only configure VLAN for the Internet port manually, because they only have Internet port.

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 | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->VLAN->WAN Port->VLAN 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) | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->VLAN->WAN Port->VID Number | |
| 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 | Integer from 0 to 7 | |

| Values | |
|---|---|
| **Default** | 0 |
| **Web UI** | Network->Advanced->VLAN->WAN Port->Priority |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->VLAN->WAN Port->Priority |
| **Parameter** | static.network.vlan.pc_port_enable[1] | <y0000000000xx>.cfg |
| **Description** | It enables or disables the VLAN for the PC port.<br><br>**Note**: It works only if "static.network.pc_port.enable" is set to 1 (Auto Negotiation). It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |
| **Web UI** | Network->Advanced->VLAN->PC Port->Active |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->VLAN->PC Port->VLAN Status |
| **Parameter** | static.network.vlan.pc_port_vid[1] | <y0000000000xx>.cfg |
| **Description** | It configures the VLAN ID for the PC port.<br><br>**Note**: It works only if "static.network.pc_port.enable" is set to 1 (Auto Negotiation) and "static.network.vlan.pc_port_enable" is set to 1 (Enabled). It is not applicable to CP960 phones. |
| **Permitted Values** | Integer from 1 to 4094 |
| **Default** | 1 |
| **Web UI** | Network->Advanced->VLAN->PC Port->VID (1-4094) |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->VLAN->PC Port->VID Number |
| **Parameter** | static.network.vlan.pc_port_priority[1] | <y0000000000xx>.cfg |
| **Description** | It configures the VLAN priority for the PC port.<br><br>7 is the highest priority, 0 is the lowest priority.<br><br>**Note**: It works only if "static.network.pc_port.enable" is set to 1 (Auto Negotiation) and "static.network.vlan.pc_port_enable" is set to 1 (Enabled). It is not applicable to CP960 phones. |
| **Permitted Values** | Integer from 0 to 7 |
| **Default** | 0 |
| **Web UI** | Network->Advanced->VLAN->PC Port->Priority |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->VLAN->PC Port->Priority |

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

## DHCP VLAN

When the VLAN discovery method is set to DHCP, the phone examines DHCP option for a valid VLAN ID. 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<br>**1**-Enabled | |
| Default | 1 | |
| Web UI | Network->Advanced->VLAN->DHCP VLAN->Active | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->VLAN->DHCP VLAN->DHCP VLAN | |
| Parameter | static.network.vlan.dhcp_option[1] | <y0000000000xx>.cfg |
| Description | It configures the DHCP option from which the phone will obtain the VLAN settings.<br><br>Multiple DHCP options (at most five) are separated by commas. | |
| Permitted Values | Integer from 1 to 255 | |
| Default | 132 | |
| Web UI | Network->Advanced->VLAN->DHCP VLAN->Option (1-255) | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->VLAN->DHCP VLAN->Option | |

[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 | 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.<br><br>The priority of each method is: LLDP/CDP>Manual>DHCP VLAN. | |
| Permitted Values | **0**-Disabled<br><br>**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. | |
| Default | 0 | |

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

## Wi-Fi

Wi-Fi feature enables you to connect the phones to the organization's wireless network.

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

| Note |
|---|
| For VP59/T58A phones, you have to disable the Wi-Fi feature if you want to use the wired network. |

**Topic**

# Wi-Fi Configuration

The following table lists the parameters you can use to configure Wi-Fi.

| Parameter | static.wifi.function.enable[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the Wi-Fi feature. | |
| **Permitted Values** | **0**-Disabled <br> **1**-Enabled | |
| **Default** | 1 | |
| **Parameter** | static.wifi.enable | <y0000000000xx>.cfg |
| **Description** | It activates or deactivates the Wi-Fi mode. <br><br> **Note**: It works only if "static.wifi.function.enable" is set to 1 (Enabled). | |
| **Permitted Values** | **0**-Disabled <br> **1**-Enabled | |
| **Default** | 0 | |
| **Phone UI** | Settings->Basic Settings->Wi-Fi->Wi-Fi | |
| **Parameter** | static.wifi.X.label[2] | <y0000000000xx>.cfg |
| **Description** | It configures the profile name of a specific wireless network. <br><br> **Note**: It works only if "static.wifi.enable" is set to 1 (Enabled). | |
| **Permitted Values** | String within 32 characters | |
| **Default** | Blank | |
| **Parameter** | static.wifi.X.ssid[2] | <y0000000000xx>.cfg |
| **Description** | It configures the SSID of a specific wireless network. <br><br> SSID is a unique identifier for accessing wireless access points. <br><br> **Note**: It works only if "static.wifi.enable" is set to 1 (Enabled). | |
| **Permitted Values** | String within 32 characters | |
| **Default** | Blank | |
| **Parameter** | static.wifi.X.priority[2] | <y0000000000xx>.cfg |
| **Description** | It configures the priority for a specific wireless network. <br><br> 5 is the highest priority, 1 is the lowest priority. <br><br> **Note**: It works only if "static.wifi.enable" is set to 1 (Enabled). | |
| **Permitted Values** | Integer from 1 to 5 | |
| **Default** | 1 | |
| **Parameter** | static.wifi.X.security_mode[2] | <y0000000000xx>.cfg |
| **Description** | It configures the security mode of a specific wireless network. | |

| | | |
|---|---|---|
| **Note**: It works only if "static.wifi.enable" is set to 1 (Enabled). | | |
| **Permitted Values** | NONE, WEP, WPA/WPA2 PSK, 802.1x EAP | |
| **Default** | NONE | |
| **Parameter** | static.wifi.X.cipher_type[2] | <y0000000000xx>.cfg |
| **Description** | It configures the encryption type of a specific wireless network. If "static.wifi.X.security_mode" is set to **NONE**, the permitted value of this parameter is **NONE**. If "static.wifi.X.security_mode" is set to **802.1x EAP**, the permitted values of this parameter are **PEAP**, **TLS**, **TTLS** or **PWD**. **Note**: It works only if "static.wifi.enable" is set to 1 (Enabled). | |
| **Permitted Values** | NONE, PEAP, TLS, TTLS, PWD | |
| **Default** | NONE | |
| **Parameter** | static.wifi.X.password[2] | <y0000000000xx>.cfg |
| **Description** | It configures the password of a specific wireless network. **Note**: It works only if "static.wifi.enable" is set to 1 (Enabled). | |
| **Permitted Values** | String within 64 characters | |
| **Default** | Blank | |
| **Parameter** | static.wifi.X.eap_type[2] | <y0000000000xx>.cfg |
| **Description** | It configures the EAP authentication mode of a specific wireless network. **Note**: It works only if "static.wifi.enable" is set to 1 (Enabled). | |
| **Permitted Values** | TTLS, PEAP or TLS | |
| **Default** | Blank | |
| **Parameter** | static.wifi.X.eap_user_name[2] | <y0000000000xx>.cfg |
| **Description** | It configures the EAP authentication username of a specific wireless network. **Note**: It works only if "static.wifi.enable" is set to 1 (Enabled). | |
| **Permitted Values** | String within 32 characters | |
| **Default** | Blank | |
| **Parameter** | static.wifi.X.eap_password[2] | <y0000000000xx>.cfg |
| **Description** | It configures the EAP authentication password of a specific wireless network. **Note**: It works only if "static.wifi.enable" is set to 1 (Enabled). | |
| **Permitted Values** | String within 64 characters | |
| **Default** | Blank | |
| **Parameter** | static.network.ethernet_as_wifi.enable[1] | <y0000000000xx>.cfg |

| | |
|---|---|
| **Description** | It enables or disables the network type value returned from interface "ConnectivityManager.getActiveNetworkInfo()" to be changed from Ethernet to WIFI.<br><br>**Note**: Some applications may have restrictions on network type, causing some functions to be unavailable. Then you can enable this feature to help solve the problem. It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled, the returned network type value is the current actual network type.<br><br>**1**-Enabled |
| **Default** | 0 |

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

[2]X is Wi-Fi ID. X=1-5.

# Real-Time Transport Protocol (RTP) Ports

Since the phone supports conferencing and multiple RTP streams, it can use several ports concurrently. You can specify the phone's RTP port range.

The UDP port used for RTP streams is traditionally an even-numbered port. If the port 11780 is used to send and receive RTP for the first voice session, additional 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.

It is only applicable to CP960 phones.

## 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.<br><br>**Note**: It is only applicable to CP960 phones. | |
| **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.<br><br>**Note**: It is only applicable to CP960 phones. | |
| **Permitted Values** | Integer from 1024 to 65535 | |
| **Default** | 12780 | |
| **Web UI** | Network->Advanced->Local RTP Port->Max RTP Port (1024~65535) | |

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

# Network Address Translation (NAT)

NAT enables phones with private unregistered addresses to communicate with devices with globally unique registered addresses.

## Topics

## NAT Traversal Configuration

The phones can traverse NAT gateways to establish and maintain connections with external devices.

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**: It works only if "static.sip.nat_stun.enable" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled **1**-STUN | |
| Default | 0 | |
| Web UI | Account->Register->NAT | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Accounts->AccountX->NAT Status | |
| 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->Advanced->NAT->Active | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->NAT->NAT Status | |
| 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->Advanced->NAT->STUN Server | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->NAT->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->Advanced->NAT->STUN Port (1024~65535) |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->NAT->STUN Port |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

[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. | |
| 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. For VP59/T58A, X=1-16, for CP960, X=1.

## Rport Configuration

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. For more information, refer to RFC 3581.

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<br><br>**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.<br><br>**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. For VP59/T58A, X=1-16, for CP960, X=1.

## 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.<br><br>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.<br><br>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 | |

## Reserved Ports

By default, the phone communicates through UDP ports in the 50000 - 50249 range for video and voice control. The phone uses only a small number of these ports during a call. The exact number depends on the number of participants in the call, the protocol used, and the number of ports required for the type of call: video or voice.

It is not applicable to CP960 phones.

### Topics

Guidelines for Determining the Range of Port Numbers
Reserved Ports Configuration

# Guidelines for Determining the Range of Port Numbers

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

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

| Call Type | Number of Required Ports for T58 | Number of Required Ports for VP59 |
|---|---|---|
| Video | 4 UDP ports | 8 UDP ports (4 UDP ports when not using content sharing) |
| Voice | 2 UDP ports | 2 UDP ports |
| Each additional video participant requires 4 UDP ports. | | |
| Each additional audio participant requires 2 UDP ports. | | |

Use the following information as a guide when determining the range of port numbers.

| Phone | Maximum Connections | Required Ports for a SIP Call | |
|---|---|---|---|
| VP59/T58A | Three-way video call and two audio-only calls | 16 UDP | 50000-50015 |

## Related Topic

Reserved Ports Configuration

# Reserved Ports Configuration

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

| Parameter | static.sip.min_udp_port[1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the minimum UDP port.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | Integer from 1024 to 65535 | |
| Default | 50000 | |
| Web UI | Network->Advanced->Reserve Port->UDP Port Scope (1024~65535) | |
| Parameter | static.sip.max_udp_port[1] | <y0000000000xx>.cfg |
| Description | It configures the maximum UDP port.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | Integer from 1024 to 65535 | |
| Default | 50249 | |
| Web UI | Network->Advanced->Reserve Port->UDP Port Scope (1024~65535) | |
| Parameter | static.sip.min_tcp_port[1] | <y0000000000xx>.cfg |
| Description | It configures the minimum TCP port. | |

| | |
|---|---|
| | **Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | Integer from 1024 to 65535 |
| **Default** | 50000 |
| **Web UI** | Network->Advanced->Reserve Port->TCP Port Scope (1024~65535) |
| **Parameter** | static.sip.max_tcp_port[1]        <y0000000000xx>.cfg |
| **Description** | It configures the maximum TCP port.<br>**Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | Integer from 1024 to 65535 |
| **Default** | 50249 |
| **Web UI** | Network->Advanced->Reserve Port->TCP Port Scope (1024~65535) |

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

# Internet Port and PC Port

Yealink phones support two Ethernet ports: Internet port and PC port. You can enable or disable the PC port on the phones. The CP960 phones have Internet port only.

### Topics

Supported Transmission Methods
Internet Port and PC Port Configuration

## Supported Transmission Methods

Three optional methods of transmission configuration for IP phone Internet port and PC port (the CP960 phones have Internet port only):

- Auto-negotiate
- Half-duplex (transmit in 10Mbps or 100Mbps)
- Full-duplex (transmit in 10Mbps, 100Mbps or 1000Mbps)

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

## Internet Port and PC Port Configuration

The following table lists the parameters you can use to configure Internet port and PC port.

| | |
|---|---|
| **Parameter** | static.network.pc_port.enable[1]        <y0000000000xx>.cfg |
| **Description** | It enables or disables the PC port.<br>**Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled<br>**1**-Auto Negotiation |
| **Default** | 1 |
| **Web UI** | Network->PC Port->PC Port Active |
| **Parameter** | static.network.internet_port.speed_duplex[1]        <y0000000000xx>.cfg |

| | |
|---|---|
| **Description** | It configures the network speed over Ethernet of the Internet port.<br><br>**Note**: You can set the transmission speed to 1000Mbps/Auto Negotiation to transmit in 1000Mbps if the phone is connected to the switch supports Gigabit Ethernet. We recommend that you do not change this parameter. |
| **Permitted Values** | **0**-Auto Negotiation<br><br>**1**-Full Duplex 10Mbps<br><br>**2**-Full Duplex 100Mbps<br><br>**3**-Half Duplex 10Mbps<br><br>**4**-Half Duplex 100Mbps<br><br>**5**-Full Duplex 1000Mbps |
| **Default** | 0 |
| **Web UI** | Network->Advanced->Port Link->WAN Port Link |

| **Parameter** | static.network.pc_port.speed_duplex[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the network speed over Ethernet of the PC port.<br><br>**Note**: It works only if "static.network.pc_port.enable" is set to 1 (Auto Negotiation). You can set the transmission speed to 1000Mbps/ Auto Negotiation to transmit in 1000Mbps if the phone is connected to the switch supports Gigabit Ethernet. We recommend that you do not change this parameter. It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Auto Negotiation<br><br>**1**-Full Duplex 10Mbps<br><br>**2**-Full Duplex 100Mbps<br><br>**3**-Half Duplex 10Mbps<br><br>**4**-Half Duplex 100Mbps<br><br>**5**-Full Duplex 1000Mbps | |
| **Default** | 0 | |
| **Web UI** | Network->Advanced->Port Link->PC Port Link | |

| **Parameter** | static.network.vlan.pc_port_mode[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures how the phone processes packets for the PC port when VLAN is enabled on the PC port.<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-The phone forwards the packets sent from the PC port to the Internet port directly.<br><br>**1**-If there are no VLAN tags in the packets sent from the PC port to the Internet port, the phone tags the packets and then forward them; else, the phone forwards the packets directly. | |
| **Default** | 1 | |

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

# 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<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Network->Advanced->VPN->Active | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->VPN->VPN Active | |
| Parameter | static.openvpn.url | <y0000000000xx>.cfg |
| Description | It configures the access URL of the *.tar file for OpenVPN.<br><br>**Example**:<br><br>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.

## Video QoS

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

## SIP QoS

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

DSCPs for voice and SIP packets can be specified respectively.

## Wi-Fi QoS

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

**Note**

For voice and SIP packets, the 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, Video and SIP QoS Configuration

# Voice, Video and SIP QoS Configuration

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

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

| Parameter | static.network.qos.videotos[1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the DSCP (Differentiated Services Code Point) for video packets. The default DSCP value for H264 packets is 34 (Assured Forwarding). **Note**: It is not applicable to CP960 phones. | |
| Permitted Values | Integer from 0 to 63 | |
| Default | 34 | |
| Web UI | Network->Advanced->QoS->Video QoS (0~63) | |
| Parameter | static.network.qos.signaltos[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->QoS->SIP QoS (0~63) | |
| Parameter | static.wifi.802_11e.enable[1] | <y0000000000xx>.cfg |
| Description | It enables or disables the WMM (Wi-Fi MultiMedia) feature. **Note**: WMM is an 802.11 quality of service (QoS) implementation based on a subnet of the draft 802.11e standard supplement. | |
| Permitted Values | **0**-Disabled **1**-Enabled | |
| Default | 1 | |

[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<br><br>**1**-EAP-MD5<br><br>**2**-EAP-TLS<br><br>**3**-EAP-MSCHAPv2<br><br>**4**-EAP-TTLS/EAP-MSCHAPv2<br><br>**5**-EAP-PEAP/GTC<br><br>**6**-EAP-TTLS/EAP-GTC<br><br>**7**-EAP-FAST | |
| **Default** | 0 | |
| **Web UI** | Network->Advanced->802.1x->802.1x Mode | |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->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.<br><br>**Note**: It works only if "static.network.802_1x.mode" is set to 7 (EAP-FAST). | |
| **Permitted Values** | **0**-Unauthenticated Provisioning, EAP In-Band provisioning is enabled by server unauthenticated PAC (Protected Access Credential) provisioning using the anonymous Diffie-Hellman key exchange.<br><br>**1**-Authenticated Provisioning, EAP In-Band provisioning is enabled by server authenticated PAC provisioning using certificate based server authentication. | |
| **Default** | 0 | |
| **Web UI** | Network->Advanced->802.1x->Provisioning Mode | |
| **Parameter** | static.network.802_1x.anonymous_identity[1] | <y0000000000xx>.cfg |
| **Description** | It configures the anonymous identity (user name) for 802.1X authentication.<br><br>It is used for constructing a secure tunnel for 802.1X authentication.<br><br>**Note**: It works only if "static.network.802_1x.mode" is set to 2, 3, 4, 5, 6 or 7. | |
| **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 |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->802.1x->Identity |
| **Parameter** | static.network.802_1x.md5_password[1] | <y0000000000xx>.cfg |
| **Description** | It configures the password for 802.1x authentication. <br><br> **Note**: It is required for all methods except EAP-TLS. |
| **Permitted Values** | String within 32 characters |
| **Default** | Blank |
| **Web UI** | Network->Advanced->802.1x->MD5 Password |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->802.1x->MD5 Password |
| **Parameter** | static.network.802_1x.root_cert_url | <y0000000000xx>.cfg |
| **Description** | It configures the access URL of the CA certificate. <br><br> The format of the certificate must be *.pem, *.crt, *.cer or *.der. <br><br> **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). |
| **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. <br><br> The format of the certificate must be *.pem. <br><br> **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 |
| **Parameter** | static.network.802_1x.proxy_eap_logoff.enable[1] | <y0000000000xx>.cfg |
| **Description** | It enables or disables the 802.1x-logoff feature for the PC port. <br><br> **Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled <br><br> **1**-Enabled, the 802.1x logoff message is sent to the authenticator when the PC is disconnected. |
| **Default** | 0 |

[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.<br><br>File types supported by the phones are:<br><br>• Firmware Image<br>• Configuration File |
| Upload | This method is used to cause the CPE to upload a specified file to the designated location.<br><br>File types supported by the phones are:<br><br>• Configuration File<br>• 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<br>**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.<br>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.<br>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.<br>**Note**: The phones also support obtaining the URL of the ACS by detecting DHCP option 43. | |
| **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_pass- | <y0000000000xx>.cfg |

| | word | |
|---|---|---|
| **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<br>**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.<br>**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

You can provision multiple phones with the same settings for large-scale deployments.

For more information, refer to Yealink SIP IP Phones Auto Provisioning Guide.

## Topics

## 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

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 specific phone models
- 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

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 IP phone. |

## Boot File Attributes

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

| Attributes | Description |
| --- | --- |
| #!version:1.0.0.1 | It must be placed in the first line. Do not edit and delete. |
| include:config <xxx.cfg><br><br>include:config "xxx.cfg" | Each "include" statement can specify a location of a configuration file. The configuration file format must be *.cfg.<br><br>The locations in the angle brackets or double quotation marks support two forms:<br><br>• Relative path (relative to the boot file):<br>For example, sip.cfg, HTTP Directory/sip.cfg<br>• Absolute path (or URL):<br>For example, http://10.2.5.258/HTTP Directory/sip.cfg<br><br>The location must point to a specific CFG file. |
| [$MODEL] | The [$MODEL] can be added to specify settings for specific phone models. $MODEL represents the phone model name.<br><br>The valid phone model names are: VP59, T58 and CP960.<br><br>Multiple phone models are separated by commas. For example, [T58, CP960]. |
| 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.<br><br>**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.<br><br>**0**-(Disabled) - If the value of a parameter in configuration files is left blank, deleted or commented out, the pre-configured value is kept.<br><br>**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. |

| Attributes | Description |
|---|---|
| specific_model.excluded_mode | Enable or disable the exclude mode. The exclude mode applies to the configuration files specified in the boot file.<br><br>**0**-Disabled (Append Mode), the phone downloads its own model-specific configuration files, and downloads other model-unspecified configuration files.<br><br>**1**-Enabled (Exclude Mode), the phone attempts to download its own model-specific configuration files; if there are no own model-specific configuration files found on the server, it downloads model-unspecified configuration files.<br><br>**Note**: Exclude mode can only be used in boot files. If a boot file is used but "specific_model.excluded_mode" is not configured, the exclude mode is disabled 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. To specify configuration files for specific phone models, add specific phone models in front of include:config <> or include:config "". Multiple phone model names are separated by commas.

    [T58,VP59]include:config <configure/sip.cfg>

    [CP960]include:config "http://10.2.5.206/configure/account.cfg"

    ## file sip.cfg only applies to VP59 and T58A phones, file account.cfg only applies to CP960 phones

5. Specify the overwrite mode and exclude mode.

    For example:

    overwrite_mode = 1

    specific_model.excluded_mode = 1

6. 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

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 |
|:---:|:---:|
| VP59 | y000000000091.cfg |
| T58A | y000000000058.cfg |
| CP960 | y000000000073.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 phone user interface (for example, changes for time and date formats, ring tones, and DSS keys).

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:

   *local_time.time_format = 1*

   *account.1.dnd.enable = 1*

   *account.2.dnd.enable = 1*

   *features.dnd.enable = 0*

3. To specify parameters for specific phone models, add specific phone models in the front of the corresponding parameters. Multiple phone model names are separated by commas.

   For example:

   *[CP960]features.dnd.enable = 1*

   *[T58]features.dnd.enable = 0*

   ## These parameters only apply to their own specific phone models.

4. 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<br><br>(for example, account.1.dnd.enable = 1) | Specify the parameters and values to apply specific settings to the phones.<br><br>• Separate each configuration parameter and value with an equal sign<br>• Set only one configuration parameter per line<br>• Put the configuration parameter and value on the same line, and do not break the line |
| [$MODEL] | The [$MODEL] can be added in front of the configuration parameter to specify the value for specific phone models. $MODEL represents the phone model.<br><br>The valid phone model names are: VP59, T58 and CP960.<br><br>Multiple phone models are separated by commas. For example, [T58, CP960].<br><br>**Note**: The phone updates model-specific configurations and those model-unspecified configurations. |

> **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,<br>000.GUI.English.lang<br>1.English_note.xml<br>1.English.js | Customize the translation of the existing language on the phone/web user interface. | Language for Phone Display Customization<br>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 |
| Softkey Layout Template (not applicable to CP960 phones) | CallFailed.xml<br>CallIn.xml<br>Connecting.xml<br>Dialing.xml<br>RingBack.xml<br>Talking.xml | Customize soft key layout for different call states. | Softkey Layout File Customization |
| Directory Template | favorite_setting.xml | Customize the directory list. | Directory List 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 |

| Template File | File Name | Description | Reference in Section |
|---|---|---|---|
| Remote Phone Book Template | Department.xml<br><br>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:
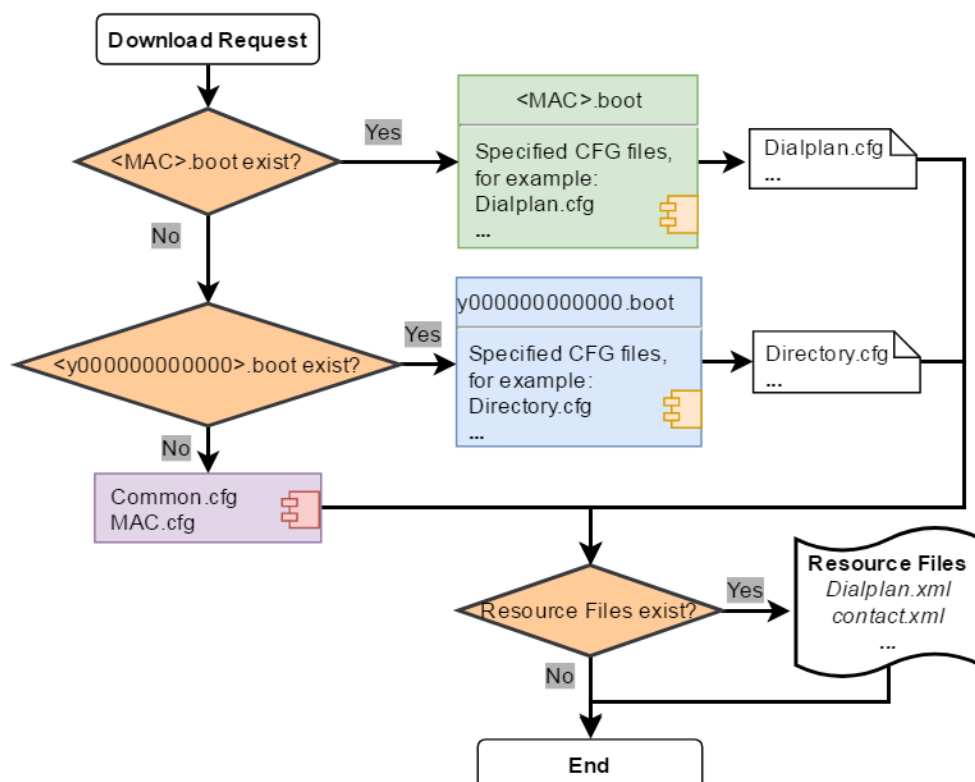


The parameters in the newly downloaded configuration files will override the same parameters in files downloaded earlier.

## Provisioning Methods

Yealink provides two ways to provision your phones:

- Manual Provisioning: provisioning via the local phone 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 phone 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 phone user interface method. We recommend using centralized provisioning as your primary provisioning method when provisioning multiple phones.

### Topics

Provisioning Methods Priority
Web User Interface

# 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):
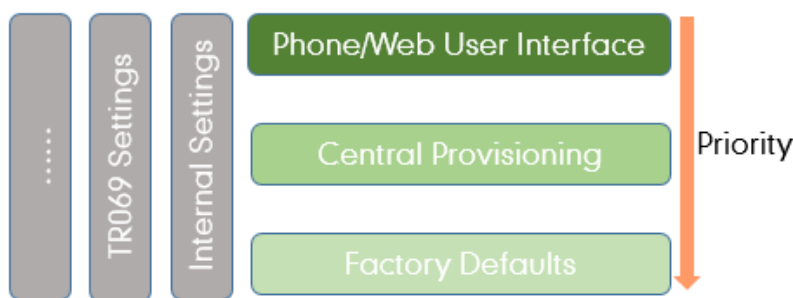


| Note |
| --- |
| The provisioning priority mechanism takes effect only if "static.auto_provision.custom.protect" is set to 1. For more information on this parameter, refer to Keeping User's Personalized Settings Configuration.<br><br>Static parameters have no priority. They take effect no matter what method (web user interface or phone user interface or configuration files) you are using for provisioning.<br><br>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 phone 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

### Procedure

1. Find the phone IP address. Navigate to **Settings**->**Status**->**General**.
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.

| 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.<br><br>**Note**: It works only if "static.wui.https_enable" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br><br>**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.<br><br>Multiple domain names are separated by semicolons.<br><br>**Example**:<br><br>wui.secure_domain_list = test.abc.com<br><br>You are only allowed to use test.abc.com or IP address to access the web user interface of the phone.<br><br>**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<br><br>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<br>**1**-Enabled | |
| Default | 1 | |
| Web UI | Network->Advanced->Web Server->HTTP | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->Web Server->HTTPS Status | |
| 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) | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->Web Server->HTTP Port | |
| 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<br>**1**-Enabled | |
| Default | 1 | |
| Web UI | Network->Advanced->Web Server->HTTPS | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Network->Web Server->HTTPS Status | |
| 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) | |

| | |
|---|---|
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->Web Server->HTTPS Port |

[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**:
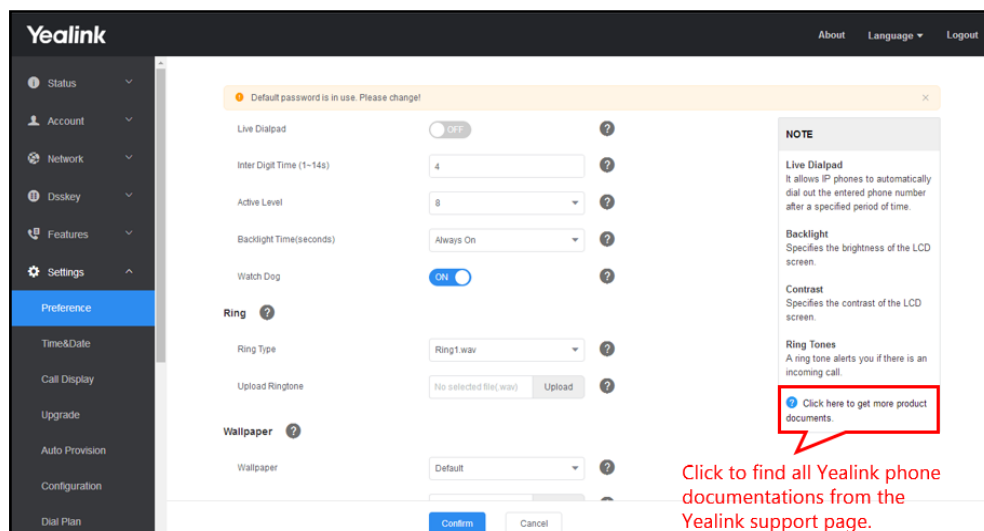


### Phone User Interface

Phone user interface makes configurations available to users and administrators; but the **Advanced Settings** option is only available to administrators and requires an administrator password (default: admin).

You can configure the phones via Phone user interface on a per-phone basis.

| Note |
|---|
| When you manually configure a phone via phone 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. |

### Related Topic

User and Administrator Identification

### 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:

Provisioning Server

SIP IP Phone
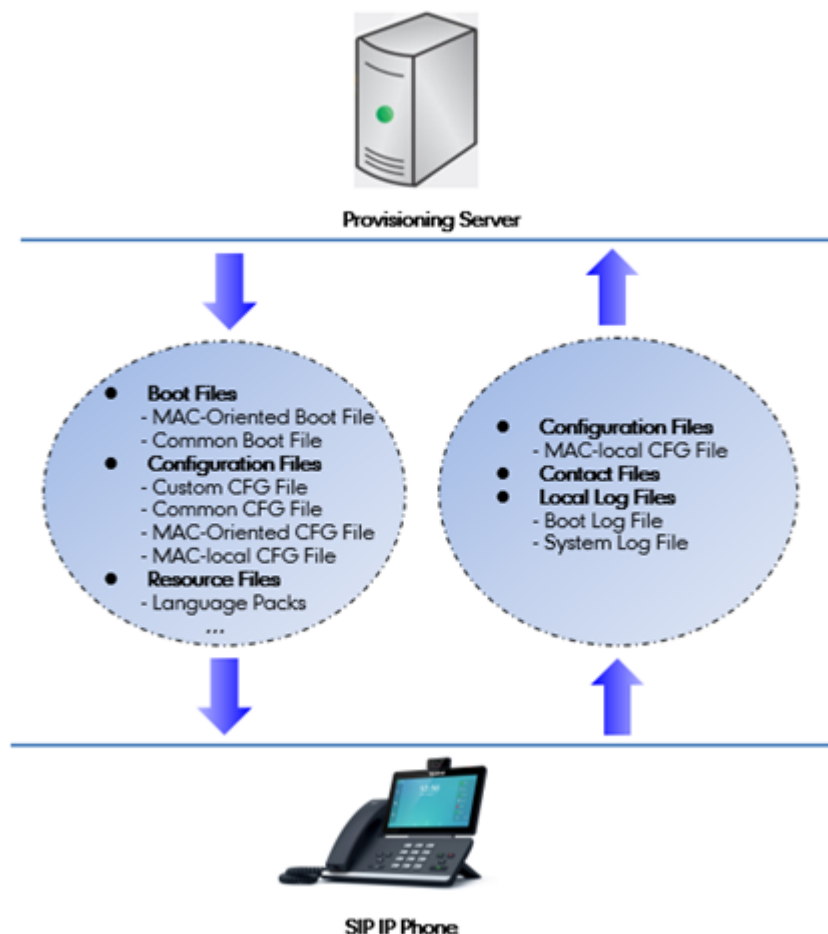
Yealink phones can obtain the provisioning server address during startup. Then the phones first download boot files and configuration files from the provisioning server, and then resolve and update the configurations written in configuration files. This entire process is called auto provisioning. For 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.<br><br>**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** | features.action_uri_force_autop | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the phone to end the call for triggering auto provisioning immediately when receiving an HTTP or HTTPS GET request with the variable value set to AutoP during a call. **Note**: It works only if "features.action_uri.enable" is set to 1 (Enabled). | |
| **Permitted Values** | **0**-Disabled, the phone triggers auto provisioning after the call. **1**-Enabled | |
| **Default** | 0 | |

| **Parameter** | static.auto_provision.power_on | <y0000000000xx>.cfg |
|---|---|---|

| | |
|---|---|
| **Description** | It triggers the power on feature to on or off. |
| **Permitted Values** | **0**-Off<br>**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<br>**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.<br>**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<br>**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.<br>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.<br>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.<br>**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. <br><br>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". <br><br>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. <br><br>**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). | |
| 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 | It configures the days of the week for the phone to perform auto provisioning weekly. <br><br>**Example**: <br><br>static.auto_provision.weekly.dayofweek = 01 <br><br>If "static.auto_provision.weekly_upgrade_interval" is set to 0, it means the phone performs auto provisioning every Sunday and Monday. <br><br>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. <br><br>**Note**: It works only if "static.auto_provision.weekly.enable" is set to 1 (On). | |
| Permitted Values | 0,1,2,3,4,5,6 or a combination of these digits <br><br>**0**-Sunday <br><br>**1**-Monday <br><br>**2**-Tuesday <br><br>**3**-Wednesday <br><br>**4**-Thursday <br><br>**5**-Friday <br><br>**6**-Saturday | |
| Default | 0123456 | |
| Web UI | Settings->Auto Provision->Day of Week | |
| Parameter | static.auto_provision.weekly.begin_time <br><br>static.auto_provision.weekly.end_time | <y0000000000xx>.cfg |
| Description | It configures the starting/ending time of the day for the phone to perform auto provisioning weekly. <br><br>**Note**: It works only if "static.auto_provision.weekly.enable" is set to 1 (On). | |

| | |
|---|---|
| **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** | It triggers the flexible feature to on or off.<br><br>**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. |
| **Permitted Values** | **0**-Off<br><br>**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.<br><br>The auto provisioning occurs on a random day within this period based on the phone's MAC address.<br><br>The phone performs auto provisioning on a random day (for example, 18) based on the phone's MAC address.<br><br>**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.<br><br>**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.<br><br>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.<br><br>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_pro-vision.weekly.begin_time", the phone performs auto provisioning at random between the starting time on that day and ending time in the next day.<br><br>**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 |

| **Parameter** | static.auto_provision.prompt.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the phone to prompt you for the configuration update and the result (if any configuration changes) during auto provisioning.<br><br>**Note**: If the phone performs auto provisioning when receiving a SIP NOTIFY message which contains the header "Event: check-sync", the phone will display the prompt message no matter whether the configuration is updated. | |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled | |
| **Default** | 0 | |

| **Parameter** | static.auto_provision.connect.keep_alive | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the long connection for downloading files via auto provisioning. | |
| **Permitted Values** | **0**-Disabled, the phone uses the short connection for downloading files via auto provisioning<br>**1**-Enabled | |
| **Default** | 0 | |

| **Parameter** | custom.auto_provision.save_rps_info.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the phone to save the entered user name and password when performing RPS (Redirection and provisioning server) update for auto provisioning. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 1 | |

| **Parameter** | static.auto_provision.authentication.expired_time | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the timeout (in seconds) after which the authentication pop-up box for auto provisioning disappears. | |
| **Permitted Values** | **0**-The authentication pop-up box does not disappear from the phone screen automatically.<br><br>**Integer from 10 to 86400** -The authentication pop-up box automatically disappears from the phone screen after the designated time. | |
| **Default** | 7200 | |

[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** | It configures the activation code to trigger auto provisioning.<br><br>The activation code can be numeric characters, special characters # * or a combination of them.<br><br>**Example**:<br><br>static.autoprovision.1.code = 123<br><br>static.autoprovision.2.code = **<br><br>static.autoprovision.3.code = *123 | |
| **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 | |

[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

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

The following table lists the parameter 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.<br>**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<br><br>**2**-HTTPS<br><br>**3**-FTP<br><br>**Other values**-TFTP | |
| Default | TFTP | |

[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:

- **Zero Touch**: Zero Touch feature guides you to configure network settings and the provisioning server address via phone user interface after startup.
- **PnP**: PnP feature allows 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 phone user interface or web user interface.

## Topics

### Zero Touch Provision Configuration

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

| Parameter | static.zero_touch.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the zero touch for the phone to configure the network parameters and provisioning server address via phone user interface during startup. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Web UI** | Settings->Auto Provision->Zero Active | |
| **Parameter** | static.zero_touch.wait_time | <y0000000000xx>.cfg |
| **Description** | It configures the duration time (in seconds) for the phone to display Zero Touch screen during startup. | |
| **Permitted Values** | Integer from 1 to 100 | |
| **Default** | 5 | |
| **Web UI** | Settings->Auto Provision->Wait Time(1~100s) | |
| **Parameter** | static.zero_touch.network_fail_wait_times | <y0000000000xx>.cfg |
| **Description** | It configures the reconnection times when zero touch module fails to obtain network parameters. | |
| **Permitted Values** | Integer from 1 to 2147483646 | |
| **Default** | 8 | |
| **Parameter** | static.zero_touch.network_fail_delay_times | <y0000000000xx>.cfg |
| **Description** | It configures the duration time (in milliseconds) of every reconnection when zero touch module fails to obtain network parameters. | |
| **Permitted Values** | Integer from 1000 to 2147483646 | |
| **Default** | 1000 | |

| Parameter | static.features.hide_zero_touch_url.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to hide the provisioning URL item on the Zero Touch screen. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |

## 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<br><br>**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<br><br>**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 custom DHCP option for requesting provisioning server address.<br><br>Multiple options are separated by commas.<br><br>**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->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.<br><br>**Note**: The configured characters must be in accordance with the actual directory name of the provisioning server. | |
| Permitted | String within 32 characters | |

| Values | |
|---|---|
| **Default** | For VP59 phones: VP59.<br><br>For T58A phones: T58.<br><br>For CP960 phones: CP960. |

## 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.<br>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, wallpaper or DSS keys) 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

## 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.<br><br>**Note**: The provisioning priority mechanism (phone/web user interface >central provisioning >factory defaults) takes effect only if the value of this parameter is set to 1 (Enabled). If "overwrite_mode" is set to 1 in the boot file, the value of this parameter will be set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, <MAC>-local.cfg file generates and personalized non-static settings configured via the web or phone 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.<br><br>**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 | **0**-Disabled | |

| Values | **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.<br><br>If it is left blank, the phone will try to upload/download the \<MAC\>-local.cfg file to/from the pro-visioning server.<br><br>**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<br>**1**-POST | |
| Default | 0 | |

## 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.
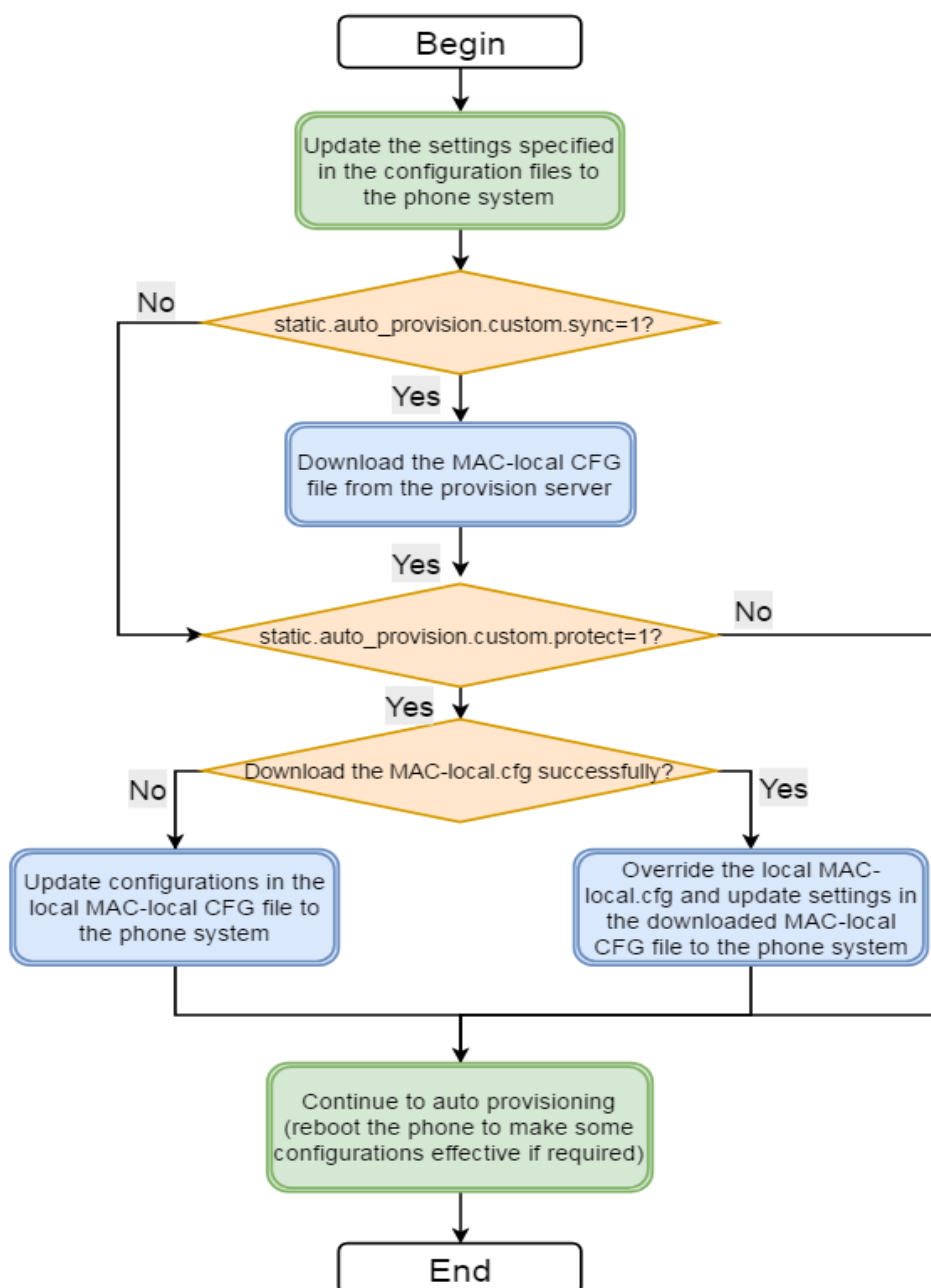
## Example: Keeping User's Personalized Settings

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 phone user interface at the path: **Settings**->**Advanced Settings** (default password: admin) ->**Reset config**->**Reset local settings**.
- Via web user interface at the path: **Settings**->**Upgrade**->**Reset Local Settings**.

| Note |
| --- |
| The **Reset local settings** option on the web/phone 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. |

# Example: Deploying Phones from the Provisioning Server

After setting up your provisioning server(s), you can deploy your phone devices. The following example shows you how to use the boot and configuration files to deploy phones from the provisioning server.

## Procedure

1. Create per-phone boot file and common boot file.

    For example, 001565b09d886.boot and y000000000000.boot.

2. Create per-phone configuration files or common configuration files, and edit the feature parameters in the file you want to apply to the phones. For example,

| Custom configuration file: | local_time.time_format = 1 |
| --- | --- |
| CustomSettings.cfg | lang.gui = Chinese_S |

| | |
|---|---|
| | [CP960]features.dnd.enable = 1 |
| | [T58]features.dnd.enable = 0 |
| Custom configuration file:<br><br>Linekey.cfg | linekey.2.type=13 |
| | linekey.2.line=1 |
| | linekey.2.value = 4603 |
| | linekey.2.label=Bill |
| MAC-Oriented configuration files:<br><br>001565b09d886.cfg | account.1.enable = 1 |
| | account.1.label = Bill |
| | account.1.display_name = 1023 |
| | account.1.auth_name = 1023 |
| | account.1.user_name = 1023 |
| | account.1.password = 1023 |
| | account.1.sip_server.1.address = 10.2.1.199 |
| | account.1.sip_server.1.port = 5060 |

**3.** Place the configuration files to the home directory of the provisioning server. For example, D:\TFTP Provision.

**4.** Specify the configuration files paths in the boot file as desired. For example,

| | |
|---|---|
| y000000000000.boot | include:config<tftp:/10.2.5.193/CustomSettings.cfg><br><br>[T58,VP59]include:config "tftp:/10.2.5.193/Linekey.cfg" |
| 001565b09d886.boot | include:config<tftp:/10.2.5.193/Linekey.cfg><br><br>include:config<tftp:/10.2.5.193/001565b09d886.cfg> |

**5.** Place the boot files to the home directory of the provisioning server. For example, D:\TFTP Provision.

**6.** Reboot the phones to trigger auto provisioning.

For the phone with MAC 001565b09d886, it will download the 001565b09d886.boot file, and then download Linekey.cfg and 001565b09d886.cfg files referenced in the 001565b09d886.boot file in sequence from the provisioning server.

For the phones except for MAC-specific phone, they will request to download the y000000000000.boot file, and then request to download the referenced files. The phone-specific configuration file Linekey.cfg only applies to T58A and VP59 phones. The only difference is that T58A and VP59 phones will download both the two files, since the exclude mode is disabled by default. The other phones will only download the CustomSettings.cfg file.

For the parameter settings in the CustomSettings.cfg file, the phone-specific parameters will only take effect on the specific phone models.

# Security Features

This chapter provides information about configuring the security features for the phone.

## Topics

## 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 the configurations on the web user interface and phone user interface. Yealink phones support the 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

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 for the user to access the phone's web user interface. | |
| Permitted Values | String within 32 characters | |
| Default | user | |
| Parameter | static.security.user_name.admin | <y0000000000xx>.cfg |
| Description | It configures the user name for the administrator to access the phone's web user interface. | |
| Permitted Values | String within 32 characters | |
| Default | admin | |

| Parameter | static.security.user_name.var | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the user name for the var to access the phone's web user interface.<br><br>**Note**: It works only if "static.security.var_enable" is set to 1 (Enabled). | |
| Permitted Values | String within 32 characters | |
| Default | var | |

| Parameter | static.security.user_password | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the password.<br><br>The phone uses "user" as the default user password, "var" as the default var password and "admin" as the default administrator password.<br><br>The valid value format is <username>:<new password>.<br><br>**Example**:<br><br>static.security.user_password = user:123 means setting the password of user to 123.<br><br>static.security.user_password = admin:456 means setting the password of administrator to 456.<br><br>static.security.user_password = var:789 means setting the password of var to 789.<br><br>**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. | |
| Permitted Values | String within 32 characters | |
| Default | Blank | |
| Web UI | Security->Password | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Set Password<br><br>**Note**: You cannot change the user password via phone user interface. | |

## 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 | **0**-Disabled<br>**1**-Enabled | |
| 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 | It configures the default access level to access the phone user interface.<br><br>**Note**: It works only if "static.security.var_enable" is set to 1 (Enabled). | |
| Permitted Values | **0**-user<br><br>**1**-var<br><br>**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 the phone will 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

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) | |

# Phone Lock

You can lock the IP phone to prevent it from unauthorized use. Once the IP phone is locked, anyone must enter the password to unlock it.

You can lock the phone in two ways:

- Long press the pound key when the IP phone is idle (not applicable to CP960 phones)
- Tap the phone lock key (if configured) when the IP phone is idle.

You can set a waiting time after which the phone is locked automatically. If the waiting time is set to 0, the phone will not be automatically locked. You need to lock the phone manually.

| Note |
|---|
| The Volume key, HEADSET key and Speakerphone key are always available even when you lock the phone. |

## Topics

## Operation Behaviors on Lock Phone

For VP59/T58A, all keys and screen are locked except the HEADSET key, Volume key, digit keys, # key, * key and Speakerphone key.

For CP960, when the phone is locked, mute touch keys and touch screen (except 📞 ) are locked. You are only allowed to dial emergency numbers, reject incoming calls, answer incoming calls and end the call.

## Phone Lock Configuration

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

| Parameter | phone_setting.phone_lock.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone lock feature. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Features->Phone Lock->Phone Lock Enable | |
| Phone UI | Settings->Advanced Settings (default password: admin)->Phone Lock->Lock Enable | |
| Parameter | phone_setting.phone_lock.unlock_pin | <y0000000000xx>.cfg |
| Description | It configures the password for unlocking the phone. | |
| Permitted Values | Characters within 15 digits | |
| Default | 123 | |
| Web UI | Features->Phone Lock->Phone Unlock PIN (0~15 Digit) | |
| Phone UI | Settings->Basic Settings->Change PIN | |
| Parameter | phone_setting.phone_lock.lock_time_out | <y0000000000xx>.cfg |
| Description | It configures the idle time (in seconds) before the phone is automatically locked.<br><br>The default value is 0 (the phone is locked only by long pressing the pound key or pressing the phone lock DSS key).<br><br>**Note**: It works only if "phone_setting.phone_lock.enable" is set to 1 (Enabled). | |
| Permitted Values | Integer from 0 to 3600 | |
| Default | 0 | |
| Web UI | Features->Phone Lock->Auto Lock (0~3600s) | |
| Phone UI | Settings->Advanced Settings (default password: admin) ->Phone Lock->Auto Lock | |
| Parameter | phone_setting.emergency.number | <y0000000000xx>.cfg |
| Description | It configures emergency numbers.<br><br>Multiple emergency numbers are separated by commas.<br><br>If "phone_setting.phone_lock.enable" is set to 1 (Enabled), you are only allowed to dial the configured | |

| | |
|---|---|
| | emergency numbers. |
| **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 trans-mission, allowing the phones to communicate with other remote parties and connect to the HTTPS URL for pro-visioning in a way that is designed to prevent the data from being eavesdropped and tampered.

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 186 built-in trusted certificates. You can upload 10 custom certificates at most. The format of the trusted certificate files must be *.pem,*.cer,*.crt and *.der and the maximum file size is 5MB.
- **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. Resetting the IP phone to factory defaults will delete trusted and server certificates settings by default. However, this feature is configurable by the parameter "phone_setting.reserve_certs_config.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
- Starfield Root Certificate Authority - G2
- TC TrustCenter Class 2 CA II
- TC TrustCenter Class 3 CA II
- TC TrustCenter Class 4 CA II
- TC TrustCenter Universal CA I
- TC TrustCenter Universal CA III
- Thawte Universal CA Root
- VeriSign Class 3 Secure Server CA - G2
- VeriSign Class 3 Secure Server CA – G3
- Thawte SSL CA
- StartCom Certification Authority
- StartCom Certification Authority G2
- Starfield Services Root Certificate Authority - G2
- RapidSSL CA
- Go Daddy Root Certificate Authority - G2
- Cybertrust Global Root
- COMODOSSLCA
- COMODO RSA Domain Validation Secure Server CA
- COMODO RSA Certification Authority
- AmazonRootCA4
- AmazonRootCA3
- AmazonRootCA2
- AmazonRootCA1
- Yealink Root CA
- Yealink Equipment Issuing CA
- (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
- AAA Certificate Services
- AC Raíz Certicámara S.A.
- ACCVRAIZ1
- ACEDICOM Root
- Actalis Authentication Root CA
- AddTrust Class 1 CA Root
- AddTrust Public CA Root
- AddTrust Qualified CA Root

- AffirmTrust Commercial
- AffirmTrust Networking
- AffirmTrust Premium
- AffirmTrust Premium ECC
- America Online Root Certification Authority 1
- America Online Root Certification Authority 2
- ApplicationCA
- Atos TrustedRoot 2011
- A-Trust-nQual-03
- Autoridad de Certificacion Firmaprofesional CIF A62634068
- Buypass Class 2 CA 1
- Buypass Class 2 Root CA
- Buypass Class 3 CA 1
- Buypass Class 3 Root CA
- CA Disig
- CA Disig Root R1
- CA Disig Root R2
- Certigna
- Certinomis - Autorité Racine
- certSIGN ROOT CA
- Certum CA
- Certum Trusted Network CA
- Chambers of Commerce Root
- Chambers of Commerce Root - 2008
- China Internet Network Information Center EV Certificates Root
- CNNIC ROOT
- COMODO Certification Authority
- COMODO ECC Certification Authority
- ComSign Secured CA
- DST ACES CA X6
- D-TRUST Root Class 3 CA 2 2009
- D-TRUST Root Class 3 CA 2 EV 2009
- EBG Elektronik Sertifika Hizmet Sağlayıcısı
- EC-ACC
- EE Certification Centre Root CA
- e-Guven Kok Elektronik Sertifika Hizmet Saglayicisi
- Entrust Root Certification Authority - EC1
- Entrust.net Secure Server Certification Authority
- ePKI Root Certification Authority
- E-Tugra Certification Authority
- FNMT Clase 2 CA
- Global Chambersign Root
- Global Chambersign Root – 2008

- GlobalSign Root CA - R3
- Government Root Certification Authority
- GTE CyberTrust Global Root
- Hellenic Academic and Research Institutions RootCA 2011
- Hongkong Post Root CA 1
- IGC/A
- Izenpe.com
- Juur-SK
- KISA RootCA 1
- KISA RootCA 3
- Microsec e-Szigno Root CA
- Microsec e-Szigno Root CA 2009
- NetLock Arany (Class Gold) Főtanúsítvány
- NetLock Expressz (Class C) Tanusitvanykiado
- NetLock Kozjegyzoi (Class A) Tanusitvanykiado
- NetLock Uzleti (Class B) Tanusitvanykiado
- Network Solutions Certificate Authority
- OISTE WISeKey Global Root GA CA
- QuoVadis Root CA 2
- QuoVadis Root CA 3
- QuoVadis Root Certification Authority
- Root CA Generalitat Valenciana
- RSA Security 2048 V3
- Secure Certificate Services
- Secure Global CA
- SecureSign RootCA11
- SecureTrust CA
- Security Communication EV RootCA1
- Security Communication RootCA1
- Security Communication RootCA2
- Sonera Class2 CA
- Staat der Nederlanden Root CA
- Staat der Nederlanden Root CA - G2
- Starfield Class 2 Certification Authority
- Swisscom Root CA 1
- Swisscom Root CA 2
- Swisscom Root EV CA 2
- SwissSign Gold CA - G2
- SwissSign Silver CA - G2
- TDC Internet Root CA
- TeliaSonera Root CA v1
- Trusted Certificate Services
- Trustis FPS Root CA

- T-TeleSec GlobalRoot Class 3
- TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3
- TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. (c) Aralık 2007
- TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. (c) Kasım 2005
- TWCA Global Root CA
- TWCA Root Certification Authority
- UTN - DATACorp SGC
- UTN-USERFirst-Hardware
- ValiCert Class 1 Policy Validation Authority
- ValiCert Class 2 Policy Validation Authority
- ValiCert Class 3 Policy Validation Authority
- Visa eCommerce Root
- Wells Fargo Root Certificate Authority
- WellsSecure Public Root Certificate Authority
- XRamp Global Certification Authority

**Note**

Yealink endeavors to maintain a built-in list of most common used CA Certificates. Due to memory constraints, we cannot ensure a complete set of certificates. If you are using a certificate from a commercial Certificate Authority not in the list above, you can send a request to your local distributor. At this point, you can upload your particular CA certificate into your phone.

## 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<br><br>**1**-TCP<br><br>**2**-TLS<br><br>**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 | |
| 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<br><br>**3**-SSL V23 (automatic negotiation with the server. The phone starts with TLS1.2 for negotiation.)<br><br>**4**-TLS 1.1<br><br>**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<br><br>**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<br><br>**1**-Custom Certificates<br><br>**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<br>**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<br><br>**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.<br><br>**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** | http://localhost/all | |

| Values | |
|---|---|
| **Default** | Blank |
| **Parameter** | static.server_certificates.url         \<y0000000000xx\>.cfg |
| **Description** | It configures the access URL of the certificate the phone sends for authentication.<br><br>**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<br>**1**-Enabled |
| **Default** | 0 |
| **Parameter** | phone_setting.reserve_certs_config.enable[3]         \<y0000000000xx\>.cfg |
| **Description** | It enables or disables the phone to reserve the trusted and server certificates settings after the phone reset to factory defaults. |
| **Permitted Values** | **0**-Disabled, "static.security.trust_certificates", "static.security.ca_cert", "static.security.cn_validation" and "static.security.dev_cert" will be reset.<br><br>**1**-Enabled, "static.security.trust_certificates", "static.security.ca_cert", "static.security.cn_validation", "static.security.dev_cert" and "phone_setting.reserve_certs_config.enable" will not be reset. |
| **Default** | 0 |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

[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.

# 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:NzFlNTUwZDk2OGVlOTc3YzNkYTkwZWVkMTM1YWFj

a=crypto:2 AES_CM_128_HMAC_SHA1_32 >inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWFm

a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDliMWIzZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0

a=rtpmap:0 PCMU/8000

a=rtpmap:8 PCMA/8000

a=rtpmap:18 G729/8000

a=fmtp:18 annexb=no

a=rtpmap:9 G722/8000

a=fmtp:101 0-15

a=rtpmap:101 telephone-event/8000

a=ptime:20

a=sendrecv
```

The callee receives the INVITE message with the RTP encryption algorithm, and then answers the call by responding with a 200 OK message which carries the negotiated RTP encryption algorithm.

Example of the RTP encryption algorithm carried in the SDP of the 200 OK message:

```
m=audio 11780 RTP/SAVP 0 101

a=rtpmap:0 PCMU/8000

a=rtpmap:101 telephone-event/8000

a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NGY4OGViMDYzZjQzYTNiOTNkOWRiYzRlMjM0Yzcz

a=sendrecv

a=ptime:20

a=fmtp:101 0-15
```

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/video encryption service. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Optional, the phone will negotiate with the other phone what type of encryption to use for the session.<br><br>**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. For VP59/T58A, X=1-16, for CP960, X=1.

# 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

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, y000000000058_Security.enc for y000000000058.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.

## 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 | **0**-Disabled, the phone will download the configuration files (for example, sip.cfg, account.cfg, <MAC>-local.cfg) and <MAC>-contact.xml file from the server during auto provisioning no matter whether the files are encrypted or not. And then resolve these files and update settings onto the phone system. **1**-Enabled, the phone will only download the encrypted configuration files (for example, sip.cfg, account.cfg, <MAC>-local.cfg) or <MAC>-contact.xml file from the server during auto provisioning, and then resolve these files and update settings onto the phone system. | |
| 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 | **0**-Disabled, the phone will decrypt the encrypted configuration files using plaintext AES keys configured on the phone. **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). | |
| Default | 0 | |
| Parameter | static.auto_provision.aes_key_16.com | <y0000000000xx>.cfg |
| Description | It configures the plaintext AES key for encrypting/decrypting the Common CFG/Custom CFG file. The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ _ { } ~. | |

| | |
|---|---|
| | **Example**:<br><br>static.auto_provision.aes_key_16.com = 0123456789abcdef<br><br>**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". |
| **Permitted Values** | 16 characters |
| **Default** | Blank |
| **Web UI** | Settings->Auto Provision->Common AES Key |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Set AES Key->Common AES |
| **Parameter** | static.auto_provision.aes_key_16.mac        <y0000000000xx>.cfg |
| **Description** | It configures the plaintext AES key for encrypting/decrypting the MAC-Oriented files (<MAC>.cfg, <MAC>-local.cfg and <MAC>-contact.xml).<br><br>The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ _ { } ~.<br><br>**Example**:<br><br>static.auto_provision.aes_key_16.mac = 0123456789abmins<br><br>**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". |
| **Permitted Values** | 16 characters |
| **Default** | Blank |
| **Web UI** | Settings->Auto Provision->MAC-Oriented AES Key |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Set AES Key->MAC-Oriented AES |
| **Parameter** | static.autoprovision.X.com_aes[1][2]        <y0000000000xx>.cfg |
| **Description** | It configures the plaintext AES key for decrypting the Common CFG file.<br>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.<br>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".<br><br>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).
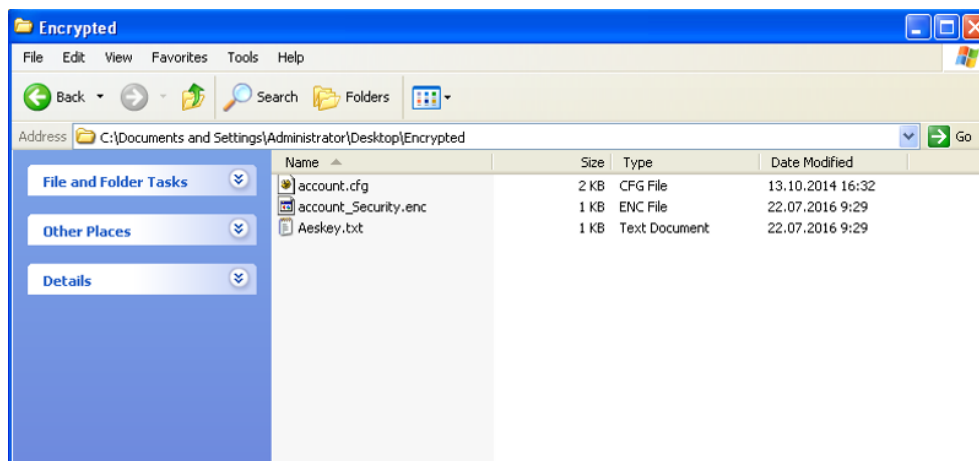


# Incoming Network Signaling Validation

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.<br><br>**Example**:<br><br>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.<br><br>**Example**:<br><br>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.<br><br>If it is left blank, all events will be validated. | |
| Permitted Values | A valid string | |
| Default | Blank | |

# USB Port Lock

You can lock the USB port on Yealink phones.

The following features are not available when you disable the USB port:

- USB camera for video calls on VP59/T58A - no near-site video
- USB recording
- USB flash drive
- USB headset
- USB charging devices on CP960
- Using Handsets with VP59/T58A Phones

**Topic**

# USB Port Lock Configuration

The following table lists the parameters you can use to configure USB port lock.

| Parameter | static.usb.power.enable[1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the USB port.<br><br>**Note**: For T58A phones, this parameter only applies to the rear USB port; for VP59 phones, this parameter only applies to the side USB port. So if you want to disable all USB ports for the VP59/T58A phones, you need to set "static.usb.power.enable" and "static.camera.function.enable" to 0 (Disabled). | |
| Permitted Values | **0**-Disabled, the phone does not provide power to the USB port and not detect USB devices attached to the USB port.<br>**1**-Enabled | |
| Default | 1 | |
| Parameter | static.usbdisk.function.enable[1] | <y0000000000xx>.cfg |
| Description | It enables or disables the USB flash drive feature.<br><br>**Note**: It works only if "static.usb.power.enable" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled, the phone cannot detect the USB flash drive attached to the USB port. Users cannot tap **USB** item in the control center to access the **File Manager**.<br>**1**-Enabled | |
| Default | 1 | |

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

# 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 |
| --- | --- | --- |
| VP59 | 91.x.x.x.rom | 91.183.0.1.rom |
| T58A | 58.x.x.x.rom | 58.83.0.15.rom |
| CP960 | 73.x.x.x.rom | 73.83.0.25.rom |

## 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->Upgrade Firmware | |

# 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.<br><br>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** | **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. <br><br> **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. |
| **Default** | 1 |
| **Web UI** | Settings->Configuration->Enable Local Log |

| **Parameter** | static.local_log.level | <y0000000000xx>.cfg |
|---|---|---|

| | |
|---|---|
| **Description** | It configures the lowest level of local log information to be rendered to the <MAC>-sys.log file. <br><br> 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. |
| **Permitted Values** | **0**-system is unusable <br><br> **1**-action must be taken immediately <br><br> **2**-critical condition <br><br> **3**-error conditions <br><br> **4**-warning conditions <br><br> **5**-normal but significant condition <br><br> **6**-informational |
| **Default** | 3 |
| **Web UI** | Settings->Configuration->Local Log Level |

| **Parameter** | static.local_log.max_file_size | <y0000000000xx>.cfg |
|---|---|---|

| | |
|---|---|
| **Description** | 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. <br><br> When this size is about to be exceeded, <br><br> (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. <br><br> (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. <br><br> Example: <br><br> static.local_log.max_file_size = 1024 |
| **Permitted Values** | Integer from 2048 to 20480 |
| **Default** | 20480 |
| **Web UI** | Settings->Configuration->Max Log File Size (2048-20480KB) |

| Parameter | static.auto_provision.local_log.backup.enable | \<y0000000000xx\>.cfg |
|---|---|---|

| Description | 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. <br><br> **Note**: The upload path is configured by the parameter "static.auto_provision.local_log.backup.path". |
|---|---|

| Permitted Values | **0**-Disabled <br><br> **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: <br><br> - Auto provisioning is triggered; <br><br> - The size of the local log files reaches the maximum configured by the parameter "static.local_log.max_file_size"; <br><br> - 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 | 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. <br><br> **Note**: It works only if "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled). |
|---|---|

| Permitted Values | Integer from 30 to 86400 |
|---|---|

| Default | 30 |
|---|---|

| Parameter | static.auto_provision.local_log.backup.path | \<y0000000000xx\>.cfg |
|---|---|---|

| Description | It configures the upload path of the local log files (\<MAC\>-boot.log and \<MAC\>-sys.log). <br><br> If you leave it blank, the phone will upload the local log files to the provisioning server. <br><br> 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. <br><br> 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. <br><br> **Example**: <br><br> static.auto_provision.local_log.backup.path = tftp://10.3.6.133/upload/ <br><br> **Note**: It works only if "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled). |
|---|---|

| Permitted Values | URL within 1024 characters |
|---|---|

| Default | Blank |
|---|---|

| Parameter | static.auto_provision.local_log.backup.append | \<y0000000000xx\>.cfg |
|---|---|---|

| Description | 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. |
|---|---|

| Permitted Values | **0**-Overwrite <br><br> **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. <br> **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. | |
| **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. | |
| **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 ipvp[887]: ANY <0+emerg > 807.194.980:ipvp log :type=1,time=1,E=3,W=4,N=5,I=6,D=7
4  May 26 00:00:07 ipvp[887]: ANY <0+emerg > 807.196.179:Version  :1.0.0.8 for release
5  May 26 00:00:07 ipvp[887]: ANY <0+emerg > 807.197.104:Built-at :Feb 29 2016,14:11:35
6  May 26 00:00:07 ipvp[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]
L0 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
L1 Jun  1 07:28:17 sys [1111]: ANY <0+emerg > LSYS=3
L2 Jun  1 11:34:57 sua [835]: SUB <3+error > [000] BLF Can't find js by sid(0)
L3 Jun  1 11:34:57 sua [835]: SUB <3+error > [000] BLF Can't find js by sid(0)
L4 [ web ]
L5 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<br>**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. |
| **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. |
| **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<br><br>**1**-TCP<br><br>**2**-TLS |
| **Default** | 0 |
| **Web UI** | Settings->Configuration->Syslog->Syslog Transport Type |

| **Parameter** | static.syslog.level | <y0000000000xx>.cfg |
|---|---|---|

| | |
|---|---|
| **Description** | It configures the lowest level of syslog information that displays in the syslog.<br><br>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. |
| **Permitted Values** | **0**-Emergency: system is unusable<br><br>**1**-Alert: action must be taken immediately<br><br>**2**-Critical: critical conditions<br><br>**3**-Critical: error conditions<br><br>**4**-Warning: warning conditions<br><br>**5**-Warning: normal but significant condition<br><br>**6**-Informational: informational messages |

| Default | 3 |
|---|---|
| **Web UI** | Settings->Configuration->Syslog->Syslog Level |
| **Parameter** | static.syslog.facility | &lt;y0000000000xx&gt;.cfg |
| **Description** | It configures the facility that generates the log messages.<br><br>**Note**: For more information, refer to RFC 3164. | |
| **Permitted Values** | **0**-Kernel Messages<br><br>**1**-User-level Messages<br><br>**2**-Mail System<br><br>**3**-System Daemons<br><br>**4**-Security/Authorization Messages (Note 1)<br><br>**5**-Messages are generated internally by syslog<br><br>**6**-Line Printer Subsystem<br><br>**7**-Network News Subsystem<br><br>**8**-UUCP Subsystem<br><br>**9**-Clock Daemon (note 2)<br><br>**10**-Security/Authorization Messages (Note 1)<br><br>**11**-FTP Daemon<br><br>**12**-NTP Subsystem<br><br>**13**-Log Audit (note 1)<br><br>**14**-Log Alert (note 1)<br><br>**15**-Clock Daemon (Note 2)<br><br>**16**-Local Use 0 (Local0)<br><br>**17**-Local Use 1 (Local1)<br><br>**18**-Local Use 2 (Local2)<br><br>**19**-Local Use 3 (Local3)<br><br>**20**-Local Use 4 (Local4)<br><br>**21**-Local Use 5 (Local5)<br><br>**22**-Local Use 6 (Local6)<br><br>**23**-Local Use 7 (Local7)<br><br>**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. | |
| **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<br>**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: ZWQ3MWM5ZDgwZDMyMmZjY2JkN2YyMzQ1NTJiNWI5Nzg.
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 recv: (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

## Reset to Factory Configuration

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

| Parameter | features.reset_by_long_press_enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to reset to factory by long pressing REDIAL key.<br><br>**Note**: For CP960, It enables or disables the phone to reset to factory by long tapping the left Mute key. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Parameter | features.factory_pwd_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to prompt for the administrator password when you long press the REDIAL key or tap the left Mute key to perform factory reset on the idle screen. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |

## 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 Configuration** 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<br><br>**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.<br><br>**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 Configuration | |

## 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 **Delete** in the **Delete Factory Configuration** field.
   The web user interface prompts you whether to delete the 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.

## Topics

# Capturing the Packets via Web User Interface

For Yealink phones, you can export the packets file to the local system and analyze it.

Yealink phones support the following two modes for capturing the packets:

- **Normal**: Export the packets file after stopping capturing.
- **Enhanced**: Export the packets file while capturing.

## Topics

## Capturing the Packets in Enhanced Way

### Procedure

1. From the web user interface, navigate to **Settings**->**Configuration**.
2. Select **Enhanced** from the pull-down list of **Pcap Type**.
3. Click **Start** in the **Pcap Feature** field to start capturing signal traffic.
4. Reproduce the issue to get stack traces.
5. Click **Stop** in the **Pcap Feature** field to stop capturing.
6. Select a location for saving the packets file on your local system while capturing.
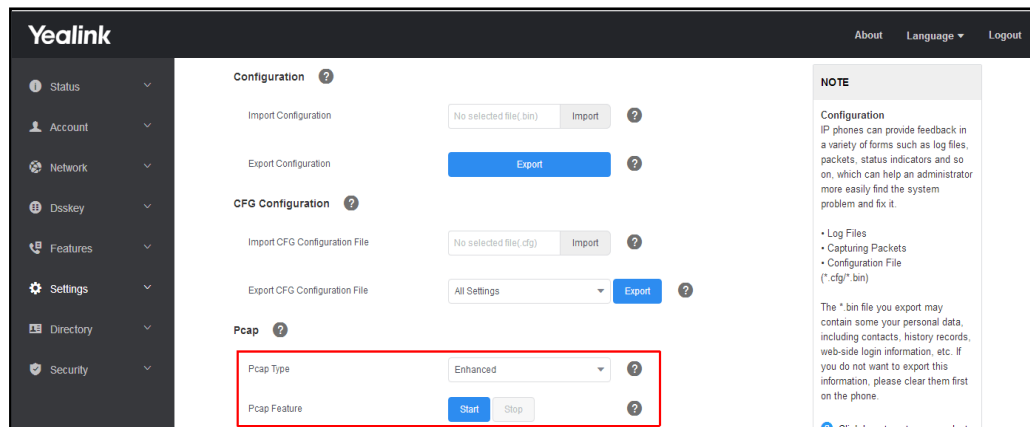


| Note |
|------|
| The steps may differ for different web browsers. |

## Capturing the Packets in Normal Way

### Procedure

1. From the web user interface, navigate to **Settings**->**Configuration**.
2. Select **Normal** from the pull-down list of **Pcap Type**.
3. Click **Start** in the **Pcap Feature** field to start capturing signal traffic.
4. Reproduce the issue to get stack traces.

5. Click **Stop** in the **Pcap Feature** field to stop capturing.

6. Click **Export** to open the file download window, and then save the file to your local system.

## Ethernet Software Capturing Configuration

You can choose to capture the packets using the Ethernet software in two ways:

- Receiving data packets from the hub: Connect the Internet port of the IP phone and the PC to the same hub, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic.

- Receiving data packets from PC port: Connect the Internet port of the IP phone to the Internet and the PC port of the IP phone to a PC. Before capturing the signal traffic, make sure the phone can span data packets received from the Internet port to the PC port. It is not applicable to CP960 phones.

### Topic

Span to PC Port Configuration

### Span to PC Port Configuration

The following table lists the parameter you can use to configure span to PC port.

| Parameter | static.network.span_to_pc_port[1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to span data packets received from the WAN port to the PC port. **Note**: It works only if "static.network.pc_port.enable" is set to 1 (Auto Negotiation). It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled **1**-Enabled, all data packets from Internet port can be received by PC port. | |
| Default | 0 | |
| Web UI | Network->Advanced->Span to PC->Span to PC Port | |

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

# 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

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 CFG Configuration File** 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

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 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 **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

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.<br><br>**Note**: The file format of the custom configuration file must be *.bin. | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |
| Web UI | Settings->Configuration->Configuration->Import Configuration | |

[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:

- General information (IPv4 address or IPv6 address, phone MAC address, Machine ID, Wi-Fi MAC address, firmware version and warning).
- Network status (IPv4 status or IPv6 status, IP mode, phone MAC address, and Wi-Fi MAC address).
- Phone status (product name, hardware version, firmware version, product ID(Firmware ID), phone MAC address, Wi-Fi MAC address, Bluetooth MAC address, Android version and device certificate status).
- Account status (registration status of SIP accounts).
- Storage status (only applicable to VP59/T58A).
- Dongle status (mode, hardware version, APP version, rom version, RFPI, area; only applicable when DECT USB dongle DD10K is connected to the VP59/T58A).

## Topic

Viewing the Phone Status

## Viewing the Phone Status

You can view phone status via phone user interface by navigating to **Settings**->**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

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

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".<br>**1**-The phone will reboot.<br>**2**-The phone will ignore the SIP NOTIFY message. | |
| Default | 1 | |

## Rebooting the IP Phone via Phone User Interface

You can reboot your IP phone via phone user interface.

### Procedure

1. Tap **Settings**->**Advanced Settings** (default password: admin)->**Reboot**.
2. Tap **Reboot** 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

## 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.
- Ensure that the Wi-Fi feature is disabled.

If your phone connects to the wireless network:

- If the network is secure, ensure the entered password is correct.
- Ensure your gateway/router enables the wireless network feature.

## Solving the IP conflict problem

Do one of the following:

- Reset another available IP address for the IP phone.
- Check network configuration via phone user interface at the path **Settings**->**Advanced Settings** (default password: admin) ->**Network**->**WAN Port**->**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.

# Display Issues

## The phone screen is blank

Do one of the following:

- Ensure that the IP phone is properly plugged into a functional AC outlet.
- Ensure that the IP phone is plugged into a socket controlled by a switch that is on.
- If the IP phone is plugged into a power strip, try plugging it directly into a wall outlet.
- If your phone is PoE powered, ensure that you are using a PoE-compliant switch or hub.

## The phone displays "No Service"

The touch screen prompts "No Service" message when there is no available SIP account on the IP phone.

Do one of the following:

- Ensure that an account is actively registered on the phone at the path **Settings**->**Status**->**Accounts**.
- Ensure that the SIP account parameters have been configured correctly.

# 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 (handset, 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

# Camera and Video Issues

## The video quality is bad

- Ensure that the display device is with the suitable resolution.
- Check whether the packet has been lost.
- Ensure that camera settings are configured correctly, such as brightness and white balance.
- Avoid high-intensity indoor light or direct sunlight on the camera.

## You cannot preview local video when the phone is idle

If the camera is properly connected to the IP phone but there are no images on the screen when you launch **Camera** or swipe down from the top of the screen and then tap **Video**, you may need to replace the camera.

## There is some dazzle light on the images when previewing the local video

If the camera lens is oily or soiled, there may be some dazzle light on the images. Please try to clean it up.

# Wi-Fi and Bluetooth Issues

## The wireless signal strength is low

Ensure the IP phone and your gateway/ router are within the working range and there is no obvious interference (walls, doors, and so on.) between them.

## The phone cannot connect to Bluetooth devices all the time

Try to delete the registration information of the Bluetooth device on both IP phone and Bluetooth device, and then pair and connect it again. Contact Yealink field application engineer and your Bluetooth device manufacturer for more information.

## The Bluetooth headset affects IP phone's voice quality

You may not experience the best voice quality if you use a Bluetooth headset while the 2.4 GHz band is enabled or while you are in an environment with many other Bluetooth devices. This possible loss in voice quality is due to inherent limitations with Bluetooth technology.

## You cannot connect the IP phone to the 2.4G/5G wireless network

If you successfully connect the IP phone to the 2.4G/5G wireless network, but the video images is not smooth. Or, you cannot connect the IP phone to the 2.4G/5G wireless network.

- Check if there are too many wireless devices connecting to the same 2.4G/5G wireless network.
- Verify whether the distance between IP phone and the wireless router is too far.

# 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

Tap **Settings**->**Status** when the IP phone is idle to check the firmware version. For example: 58.83.0.15.
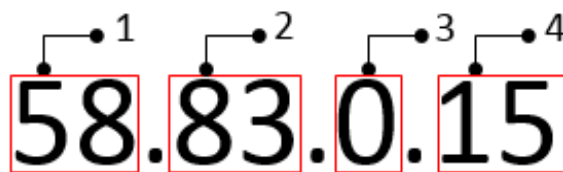


| | Item | Description |
|---|---|---|
| 1 | 58 | Firmware ID.<br><br>The firmware ID for each IP phone model is:<br><br>- 91: VP59 |

| | Item | Description |
|---|---|---|
| | | • 58: T58A<br>• 73: CP960 |
| 2 | 83 | Major version.<br><br>**Note**: The larger it is, the newer the major version is. |
| 3 | 0 | A fixed number. |
| 4 | 15 | Minor version.<br><br>**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.
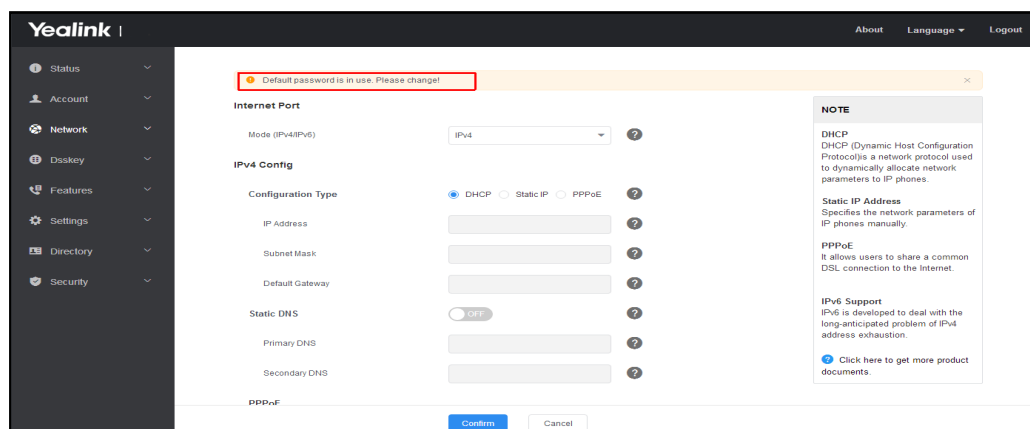


# Power and Startup Issues

## Both PoE cable and power adapter is connected to the phone

The phones use the PoE preferentially.

## 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:

- Reboot your IP phone.
- Replace the power adapter.

## The Phone screen is black

If the power LED indicator is on, the keypad is usable but the phone screen is black, please reboot your IP phone.

# 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 touch 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.



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.

# Using Handsets with VP59/T58A Phones

You can turn Yealink VP59/T58A phone to the corded-cordless phone. The corded-cordless phone consists of a VP59/T58A phone, a DECT USB dongle DD10K and at least a handset. The supported handsets include W52H, W56H, W53H and DD phone. The VP59/T58A phone acts as a base station and Handset 1. Users can register up to other four handsets to one phone. It allows users to manage calls when they are away from their desk.

To use this feature, you should insert a DD10K into the rear/side USB port on the phone in advance.

Note that you can still use the phone features as usual on the corded-cordless phone.

| Note |
| --- |
| To use this feature, you should set "static.usb.power.enable" to 1 (Enabled). |

## Topics

Handset Backlight
Handset Keypad Light
Handset Wallpaper
Handset Screen Saver
Handset Name
Number Assignment
End Call on Hook
Advisory Tones
Base PIN
DECT Intercom
Shared Directory
Master-Slave Mode
Repeater Settings Parameters
Handset Settings Parameters
Handset Firmware Upgrade Configuration

# Handset Backlight

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

For W53H/W56H, 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.

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 charged. **Note:** It will take effect on all handsets that are registered on the same phone. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled). | |
| 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 charged. **Note:** It will take effect on all handsets that are registered on the same phone. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled). | |
| 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 Keypad Light

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

It is only applicable to W56H/W53H handsets.

## 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 to the same phone. 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 Wallpaper

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

It is only applicable to W56H/W53H handsets.

## 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.<br>**Note:** It will take effect on all handsets that are registered on the same phone. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled). | |
| Permitted Values | **1**-Wallpaper1<br><br>**2**-Wallpaper2<br><br>**3**-Wallpaper3<br><br>**4**-Wallpaper4<br><br>**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 phones.

## 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.<br>**Note:** It will take effect on all handsets that are registered on the same phone. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br><br>**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 phone. 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.<br>**Note:** If it is set to blank, it will display the corresponding default handset name. | |
| **Permitted Values** | String within 24 characters | |
| **Default** | For VP59, the handset name for handset 1 is VP59 Phone; for T58A, the handset name for handset 1 is T58 Phone.<br><br>The handset name for handset 2 is Handset 2.<br><br>The handset name for handset 3 is Handset 3.<br><br>The handset name for handset 4 is Handset 4.<br><br>The handset name for handset 5 is Handset 5. | |
| **Web UI** | Status->Handset->Handset Name->Handset X[1] | |
| **Handset UI** | OK->Settings->Handset Name | |
| **Phone UI** | DECT Settings->Handsets->Handset X[1] | |

[1]X is the handset ID. X=2-5.

# Number Assignment

After the handset is registered to the phone, you can assign one or more outgoing lines or incoming lines for the handset. For VP59, the phone acts as the Handset 1 (VP59 Phone); For T58A, the phone acts as the Handset 1 (T58 Phone).

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 via the assigned incoming line(s). You can assign incoming lines to all handsets that are registered to the same phone.

## Topic

## 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 | **1**-Line 1<br><br>**2**-Line 2<br><br>**3**-Line 3<br><br>**4**-Line 4<br><br>**5**-Line 5<br><br>Multiple line IDs are separated by commas. | |
| Default | The incoming line for VP59 Phone/T58 Phone is line 1-line5;<br><br>The incoming line for handset 2 is line 2.<br><br>The incoming line for handset 3 is line 3.<br><br>The incoming line for handset 4 is line 4.<br><br>The incoming line for handset 5 is line 5. | |
| Web UI | Account->Number Assignment->Incoming lines | |
| Handset UI | W53H/W56H:<br><br>OK->Settings->Telephony->Incoming Lines (Default PIN:0000) ->HandsetX[1]<br><br>DD Phone:<br><br>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.<br>Multiple line IDs are separated by commas. | |
| Permitted Values | **1**-Line 1<br><br>**2**-Line 2<br><br>**3**-Line 3<br><br>**4**-Line 4<br><br>**5**-Line 5 | |
| Default | The outgoing line for VP59 Phone/T58 Phone is line 1-line5;<br><br>The outgoing line for handset 2 is line 2.<br><br>The outgoing line for handset 3 is line 3.<br><br>The outgoing line for handset 4 is line 4.<br><br>The outgoing line for handset 5 is line 5. | |

| Web UI | Account->Number Assignment->Outgoing lines | |
|---|---|---|
| Parameter | handset.X.dial_out_default_line[1] | <y0000000000xx>.cfg |
| Description | It configures the default line to place outgoing calls for a specific handset. | |
| Permitted Values | Integer from 1 to 5 | |
| Default | The default outgoing line for VP59 Phone/T58 Phone is 1; The default outgoing line for handset 2 is 2. The default outgoing line for handset 3 is 3. The default outgoing line for handset 4 is 4. The default outgoing line for handset 5 is 5. | |
| Web UI | Account->Number Assignment->Outgoing lines->Default | |
| Handset UI | W53H/W56H: OK->Settings->Telephony->Default Line | |

[1]X is the handset ID. X=1-5.

# 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 DD 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 | |

# Advisory Tones

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

It is not applicable to DD phones.

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

- **Keypad Tone**: plays when you press any key of the keypad.
- **Confirmation**: plays when you save settings or place the handset in the charger cradle.

- **Low Battery**: plays when battery capacity is low and the handset requires being charged.

## Topic

# 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. <br><br> **Note:** It will take effect on all handsets that are registered on the same phone. 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. | |
| Permitted Values | **0**-Disabled <br><br> **1**-Enabled | |
| Default | 1 | |
| Handset UI | 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. <br><br> **Note:** It will take effect on all handsets that are registered on the same phone. 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. | |
| Permitted Values | **0**-Disabled <br><br> **1**-Enabled | |
| Default | 1 | |
| Handset UI | 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. <br><br> **Note**: It will take effect on all handsets that are registered on the same phone. 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. | |
| Permitted Values | **0**-Disabled <br><br> **1**-Enabled | |
| Default | 1 | |
| Handset UI | OK->Settings->Audio->Advisory Tones->Low Battery | |

# Base PIN

To avoid unauthorized registration 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

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** | <u>W53H/W56H:</u><br><br>OK->Settings->System Settings->Change Base PIN<br><br><u>DD Phone:</u><br><br>Menu->Settings->Advanced Settings (default password: 0000) ->Change Password | |
| **Phone UI** | Dect Settings->Change Base 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.<br><br>**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.<br><br>**Note**: It works only if "base.double_pin_code.enable" is set to 1 (Enabled). | |
| **Permitted Values** | Integer from 0000 to 9999 | |
| **Default** | 0000 | |

# DECT Intercom

Intercom is a useful feature in an office environment to quickly connect with the operator or the secretary. Users can make internal intercom calls and external intercom calls on the handset. Internal intercom calls are made among handsets registered to the same phone.

The handset can automatically answer an incoming external intercom call and play warning tone.

**Topic**

# DECT Intercom Configuration

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

| Parameter | custom.handset.auto_intercom | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the auto intercom feature on the handset. | |
| **Permitted Values** | **-1**-Do not modify the configuration.<br><br>**0**-Off, auto intercom feature is disabled. Users need to answer incoming internal intercom calls manually.<br><br>**1**-On(Beep Off), the phone/handset answers an incoming internal intercom call automatically without a warning tone.<br><br>**2**-On(Beep On), the phone/handset answers an incoming internal intercom call automatically and plays a warning tone. It works when the silence mode is off. | |
| **Default** | -1 | |
| **Phone UI** | Dect Settings->Auto Intercom->Auto Intercom | |
| **Handset UI** | OK->Settings->Telephony->Auto Intercom | |
| **Parameter** | features.intercom.headset_prior.enable | <y0000000000xx>.cfg |
| **Description** | It configures the channel mode when an incoming intercom call is automatically answered.<br><br>**Note**: It works only if "custom.handset.auto_intercom" is set to 1 or 2. For the phone, the headset mode should be activated for use; for the handset registered to the phone, the headset should be connected in advance. | |
| **Permitted Values** | **0**-Speaker Mode<br><br>**1**-Headset Mode | |
| **Default** | 1 | |

# Shared Directory

Users can manage and call the contacts in the Shared Directory on the phone and all the registered handsets.

The shared directory can store up to 1000 contacts.

It is not applicable to DD phones.

## Topics

## 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 phone and registered 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 Values** | URL within 511 characters | | |
| **Default** | Blank | | |
| **Web UI** | Directory->Dect 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

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. **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. |
| | line | Do not modify this attribute and value. |
| | ring | Do not modify this attribute and value. |
| | default_photo | Do not modify this attribute and value. |
| | selected_photo | Do not modify this attribute and value. |
| | group_id_name | Do not modify this attribute and value. |

## 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="" line="-1" ring="Auto" default_photo="Default:default_contact_image.png" selected_photo="0" group_id_name="All Contacts"/> 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.

# Master-Slave Mode

Yealink phone can be bound with a slave handset. After binding, the phone acts as the master handset. The slave handset can share the line and contacts with the master handset. The call can be shifted between the master handset and slave handset.

It is not applicable to DD phones.

| Important |
| --- |
| Master-slave mode is available only when one handset is registered to the phone. |

The following is an example of receiving an incoming call:
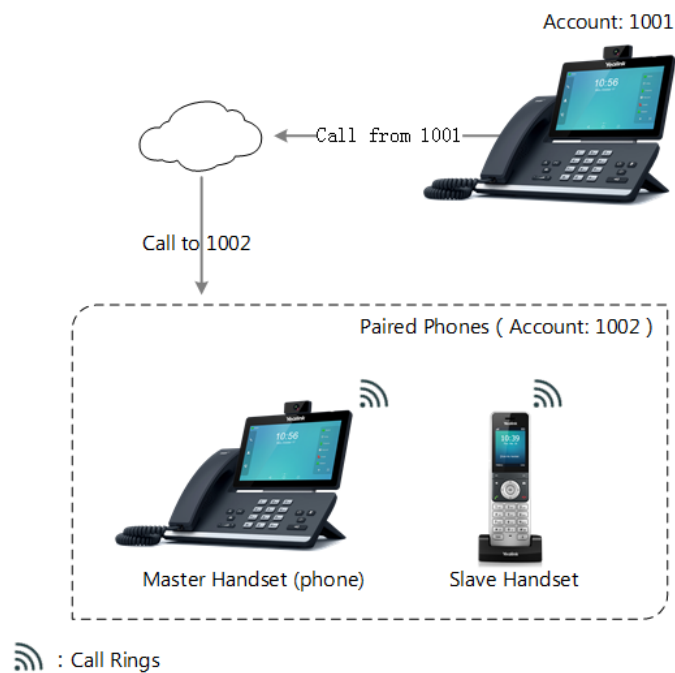


When a call is made from 1001 to 1002, both the master handset and slave handset ring. Users can answer the call either on the master handset or slave handset.

When using master-slave mode, note the following:

- The incoming and outgoing lines originally assigned to the slave handset are disabled.
- Calls made from the slave handset are handled as calls made from the master handset (in the above example, 1002). (The caller information for such calls will be that of extension 1002.)
- You can configure a mode for whether to continue the conversation on the slaver handset when the phone goes off hook, or to send a busy signal to one of the paired phones while the device is not in a call but tries to initiate a call (prohibited on that device).

**Topics**

## Master-Slave Mode Configuration

The following table lists the parameters you can use to configure master-slave mode.

| Parameter | features.ms.X.slave_handset_number[1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It specifies which handset is the slave handset for the master handset. | |
| Permitted Values | **0**-None, the master-slave mode is disabled. <br><br>**2**-Handset 2 <br><br>**3**-Handset 3 <br><br>**4**-Handset 4 <br><br>**5**-Handset 5 | |
| Default | 0 | |
| Web UI | Status->Handset->Master and Slave->Slave Handset Number | |
| Phone UI | Dect Settings->Select Slave->Select handset | |
| Parameter | features.ms.X.mode[1] | <y0000000000xx>.cfg |
| Description | It configures the master-slave mode for a master handset. <br><br>**Note**: It works only if "features.ms.X.slave_handset_number" is configured correctly. | |
| Permitted Values | **0**-Busy, users cannot switch the active call between the phone and slave handset. Regardless of the master handset or the slave handset, the device which is during the call can initiate a new call. If users not in a call try to initiate a call on the phone/handset, the phone/handset will prompt "Path Busy". <br><br>**1**-Take over call, when the slave handset is during the call, users can retrieve the call after off-hook on the master handset. When the master handset is during the call, users can push the call to the slave handset. | |
| Default | 1 | |
| Web UI | Status->Handset->Master and Slave->Mode | |
| Phone UI | Dect Settings->Select Slave->Select mode | |

[1]X is the master handset ID. X is equal to 1.

## Example: Configuring the Master-Slave Mode Feature

You can configure the master-slave mode only when one handset is registered to the phone.

The following table lists the supported phones and handsets:

| Phone | Handset |
|---|---|
| T58A<br>VP59 | W52H |
| | W53H |
| | W56H |
| | DD Phone (W41P) |

As an example, two W56H handsets along with two T58 phones are in use.



For Group 1:

features.ms.1.slave_handset_number = 2

features.ms.1.mode = 0

After provisioning, Handset 2 is the slave handset for T58 Phone. Users cannot switch the active call between the phone and slave handset. Only the device which is during the call can initiate a new call. If users not in a call try to initiate a call on the phone/handset, the phone/handset screen will prompt "Path Busy".

For Group 2:

features.ms.1.slave_handset_number = 4

features.ms.1.mode = 1

After provisioning, Handset 4 is the slave handset for T58 Phone. When the slave handset is during the call, users can retrieve the call after off-hook on the master handset. When the master handset is during the call, users can push the call to the slave handset.

# Repeater Settings Parameters

| Parameter | static.base.repeater_mode.enable[1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the repeater mode to extend the radio coverage of the phone.<br><br>**Note**: It is not applicable to DD phones. | |

| Permitted Values | **0**-Disabled |
| --- | --- |
| | **1**-RT10, RT20 or RT20U |
| | **2**-RT30 |
| **Default** | 0 |
| **Phone UI** | Dect Settings->Repeater Mode->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** | OK->Settings->System Settings->Eco Mode | |
| **Parameter** | custom.handset.missed_call_notify_light.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the message key LED to flash red when the handset misses a call. | |
| | **Note:** It will take effect on all W52H handsets that are registered on the same phone. 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->Notification Light->Missed Call | |
| **Parameter** | custom.handset.voice_mail_notify_light.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the message key LED to flash when the handset receives a voice mail. | |
| | **Note:** It will take effect on all W52H handsets that are registered on the same phone. 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->Notification Light->Voice Mail | |
| **Parameter** | custom.handset.language | <y0000000000xx>.cfg |
| **Description** | It configures the language used on the DECT handset user interface. | |
| | **Note:** It will take effect on all handsets that are registered on the same phone. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled). It is not applicable to DD phones. | |
| **Permitted** | **For W56H/W53H handset:** | |

| | |
|---|---|
| **Values** | **0**-English<br><br>**1**-French<br><br>**2**-German<br><br>**3**-Italian<br><br>**4**-Polish<br><br>**5**-Portuguese<br><br>**6**-Spanish<br><br>**7**-Turkish<br><br>**8**-Swedish<br><br>**9**-Russian<br><br>**For W52H handset**:<br><br>**0**-English<br><br>**1**-French<br><br>**2**-German<br><br>**3**-Italian<br><br>**4**-Polish<br><br>**5**-Portuguese<br><br>**6**-Spanish<br><br>**7**-Turkish<br><br>**8**-Czech<br><br>**9**-Swedish<br><br>**10**-Hebrew<br><br>**11**-Russian |
| **Default** | 0 |
| **Handset UI** | OK->Settings->Language |

| **Parameter** | custom.handset.auto_answer.enable | <y0000000000xx>.cfg |
|---|---|---|

| | |
|---|---|
| **Description** | It enables or disables a user to answer incoming calls by lifting the handset from the charger cradle without pressing the off-hook key.<br><br>**Note**: It works if the handset is placed in the charger cradle and the parameter "static.auto_pro-vision.handset_configured.enable" is set to 1 (Enabled). It is not applicable to DD phones. |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled |
| **Default** | 1 |
| **Handset UI** | OK->Settings->Telephony->Auto Answer |

| 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). It is not applicable to DD phones. | |
| 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 | OK->Settings->Display->Time Format | |
| Parameter | custom.handset.date_format | <y0000000000xx>.cfg |
| Description | It configures the date format for all registered handsets. Note: It is not applicable to DD phones. | |
| Permitted Values | **0**-WWW MMM DD **1**-DD-MMM-YY **2**-YYYY-MM-DD **3**-DD/MM/YYYY **4**-MM/DD/YY **5**-DD MMM YYYY **6**-WWW DD MMM Use the following mapping: "WWW" represents the abbreviation of the week; "DD" represents a two-digit day; "MMM" represents the first three letters of the month; "YYYY" represents a four-digit year, and "YY" represents a two-digit year. | |
| Default | 0 | |
| Web UI | Settings->Time&Date->Date Format | |
| Handset UI | OK->Settings->Display->Date Format | |
| 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 | |
| Parameter | static.auto_provision.handset_configured.enable | <y0000000000xx>.cfg |
| Description | It enables or disables the handsets to keep user personalized settings after auto provisioning. | |

| | |
|---|---|
| | **Note**: It is only applicable to the custom handset related configurations. It is not applicable to DD phones. |
| **Permitted Values** | **0**-Disabled, the phone will not deliver custom handset configurations via auto provisioning/handset reboot to the handset. The custom handset settings can be only changed via handset user interface.<br><br>**1**-Enabled, the phone will deliver the custom handset configurations via auto provisioning to the handset. Handset reboot or registration will also trigger the phone to deliver the stored handset settings to the handset. 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 handset reboot or registration.<br><br>**Note**: It works only if "static.auto_provision.handset_configured.enable" is set to 0 (Disabled). It is not applicable to DD phones. It is only applicable to the custom handset related configurations. | |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled | |
| **Default** | 1 | |

| Parameter | handset.X.contact_list.url[2] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the access URL of the contact file (*.xml) for a specific handset.<br><br>**Example**:<br><br>handset.2.contact_list.url= http://192.168.10.25/contact.xml | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Directory->Dect Directory->Import Contacts->Import to (Handset X)->Select .xml file form | |

[1]X is the handset ID. X=1 to 5.

[2]X is the handset ID. X=2 to 5.

## Custom Handset Related Configurations

This section shows you the custom handset related configurations.

| Parameter | Related Topic |
|---|---|
| custom.handset.date_format | Handset Settings Parameters |
| custom.handset.time_format | |
| custom.handset.eco_mode.enable | Handset Settings Parameters |
| custom.handset.auto_answer.enable | Auto Answer Configuration |
| custom.handset.missed_call_notify_light.enable | Handset Settings Parameters |
| custom.handset.voice_mail_notify_light.enable | Handset Settings Parameters |

| custom.handset.low_battery_tone.enable | |
|---|---|
| custom.handset.confirmation_tone.enable | Advisory Tones Configuration |
| 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 | DECT Intercom Configuration |
| custom.handset.language | Handset Settings Parameters |

## Handset Firmware Upgrade Configuration

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

| Parameter | over_the_air.url | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the access URL of the handset firmware file.<br>**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.w52h". | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |
| Web UI | Settings->Upgrade->Select and update handset firmware. | |
| Parameter | over_the_air.url.w56h | <y0000000000xx>.cfg |
| Description | It configures the access URL of the W56H handset firmware file.<br>**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.handset_tip | <y0000000000xx>.cfg |
| Description | It enables or disables to pop up a tip when upgrading the handset firmware from the provisioning server.<br>**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<br>**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 phone or turned on successfully.<br>It is only applicable when the current handset firmware is different with the one on provisioning server. | |

| | |
|---|---|
| | **Note**: It is not applicable to DD phones. |
| **Permitted Values** | **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 of firmware upgrade. If "over_the_air.handset_tip" is set to 0, you may go to **Settings**->**Upgrade Firmware** on handset to trigger the upgrading manually.<br><br>**1**-Enabled, it will upgrade the handset firmware compulsively without a pop-up tip on the handset. |
| **Default** | 1 |
| **Parameter** | over_the_air.base_trigger                      \<y0000000000xx>.cfg |
| **Description** | It enables or disables to upgrade the handset firmware compulsively when the phone detects a new handset firmware from the provisioning sever. |
| **Permitted Values** | **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** on handset to trigger the upgrading manually.<br><br>**1**-Enabled, it will upgrade the handset firmware compulsively without a pop-up tip on the handset. |
| **Default** | 1 |
| **Parameter** | over_the_air.url.w52h                        \<y0000000000xx>.cfg |
| **Description** | It configures the access URL of the W52H handset firmware file.<br><br>**Note:** The priority of parameter "over_the_air.url.w52h" 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.<br><br>**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 |

# Using CP960 Star Connection Feature

You can deploy up to four CP960 conference phones in a star layout in a large meeting room, one as the master phone and others as the slave phones. The master phone keeps all features, while the slave phones only sync some key features of the master phone, such as DND and call mute. After connecting, the slave phones are mainly used to work as speakers or microphones.

This feature allows users to control the calls either on the master phone or on the slave phones; it also helps all participants to hear each other clearly even though they are distance away in the meeting room.

The following shows an example for setting up a star connection group:



## Topics

# Guidelines for Configuring Star Connection Feature

The following instructions you need to know when configuring star connection feature for CP960:

- Ensure all the phones are deployed in the same subnet.

- Ensure all the phones are running the same firmware versions.

- You can only deploy the CP960 phones in a star layout in the wired network.

- If the master phone is not in the broadcast status, the slave phones will not reconnect automatically after reboot.

- The slave phones are unable to sync some custom features of master phone, for example, wallpaper or contact avatar.

- You cannot access the web user interface of the slave phones.

- If you upgrade firmware via web user interface for the master phone, only the master phone will be upgraded. After upgrading, the slave phones are disconnected from the master phone because of the different firmware version.
- If you upgrade firmware via auto provisioning, both the master phone and slave phones will be upgraded.

**Related Topic**

# CP960 Star Connection Feature Configuration

The following table lists the parameters you can use to configure CP960 star connection feature.

| Parameter | features.cp_star_connection.master.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It specifies whether or not the phone to be a master phone. | |
| Permitted Values | **0**-Not a master phone<br><br>**1**-master phone, the phone automatically generates a four-digit PIN number and sends broadcast. Users do not need to manually create a star connection group on the phone. | |
| Default | 0 | |
| Phone UI | Settings->Advanced Settings (default password: admin)->CP Star Connection->Create Group | |
| Parameter | features.cp_star_connection.slave.X.mac[1] | <y0000000000xx>.cfg |
| Description | It specifies the MAC address of a slave phone on the master phone.<br><br>After configured, the phone with this MAC address is authorized to connect with the master phone.<br><br>**Example**:<br><br>features.cp_star_connection.slave.1.mac = 805EC0092F4B<br><br>Note that the MAC address is case insensitive, and the following format of the MAC address is invalid: 80:5E:C0:09:2F:4B.<br><br>**Note**: It works only if "features.cp_star_connection.master.enable" is set to 1 (Enabled). | |
| Permitted Values | MAC Address | |
| Default | Blank | |
| Parameter | features.cp_star_connection.master.mac[2] | <y0000000000xx>.cfg |
| Description | It specifies the MAC address of master phone on the slave phones.<br><br>After configured, the phones can join the star connection group created by the master phone with this MAC address.<br><br>**Example**:<br><br>features.cp_star_connection.master.mac=805EC0092F33<br><br>Note that the MAC address is case insensitive, and the following format of the MAC address is invalid: 80:5E:C0:09:2F:4B.<br><br>**Note**: It works only if "features.cp_star_connection.master.enable" is set to 0 (Disabled), and the phone is authorized by the master phone to connect with it. | |
| Permitted | MAC Address | |

| Values | |
|---|---|
| Default | Blank |

[1]X is the slave phone ID. X = 1-3.

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

## Related Topic

Example: Configuring CP960 Star Connection Feature

# Example: Configuring CP960 Star Connection Feature

**Scenario Conditions**

- The MAC address of phone A is 805EC0092F33.
- The MAC address of phone B is 805EC0092F4B.
- The MAC address of phone C is 805EC009223B.
- The MAC address of phone D is 805EC0033E2B.
- All the phones are in the same subnet, and are running the same firmware versions.

You want phone A to act as a master phone, and phone B, phone C and phone D act as the slave phones.

The following example shows configuration for the phones:

**Example**

######For Phone A (master phone)######

features.cp_star_connection.master.enable=1

features.cp_star_connection.slave.1.mac=805EC0092F4B

features.cp_star_connection.slave.2.mac=805EC009223B

features.cp_star_connection.slave.3.mac=805EC0033E2B

######For Phones B、C、D (slave phones)######

features.cp_star_connection.master.enable=0

features.cp_star_connection.master.mac=805EC0092F33

After reboot, phone A, B, C, D are in a star connection group.

# Audio Features

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

## Topics

## Alert Tone

You can configure the following audio alert for the phone:

- Redial tone: allow the phones to continue to play the dial tone after inputting the preset numbers on the dialing screen.
- 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.
- Send tone: allow the IP phone to play a key tone when you tap the send key. It works only if the key tone is enabled.
- Dial tone: allow the IP phone to play a specific dial tone for a specified time.
- Key tone: allow the IP phone to play a key tone when you press or tap any key.

### Topic

## Alert Tone Configuration

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

| Parameter | features.redial_tone | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures that after you enter a specific number on the dialing screen, the phone will replay the dial tone.<br><br>**Note**: It is not applicable to CP960 phones.<br><br>**Example**:<br><br>features.redial_tone = 123<br><br>The phone will continue to play the dial tone after entering "123" on the dialing screen. | |

| Permitted Values | Integer within 6 digits | |
|---|---|---|
| **Default** | Blank | |
| **Web UI** | Features->Audio->Redial Tone | |
| **Parameter** | account.X.dial_tone[1] | <MAC>.cfg |
| **Description** | It configures the dial tone for the phone.<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Default (depend on the country tone by "voice.tone.country")<br><br>**1**-440/250,0/250<br><br>**2**-1000/250,0/250 | |
| **Default** | 0 | |
| **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.<br><br>**Note**: It works only if "account.X.display_mwi.enable" is set to 1 (Enabled). | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 1 | |
| **Web UI** | Features->General Information->Voice Mail Tone | |
| **Parameter** | features.send_key_tone | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to play a key tone when a user presses a send key.<br><br>**Note**: It works only if "features.key_tone" is set to 1 (Enabled). | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 1 | |
| **Web UI** | Features->Audio->Send Tone | |
| **Parameter** | features.key_tone | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to play a key tone when a user presses any key on your phone keypad. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 1 | |
| **Web UI** | Features->Audio->Key Tone | |
| **Phone UI** | Settings->Basic Settings->Sound->Key Tone->Key Tone | |

# Ring Tones

Ring tones are used to play for incoming calls. You can select a built-in ring tone or a custom ring tone for the phone system or specific line registration. To set the custom ring tones, you need to upload the custom ring tones to the IP phone in advance.

You can also specify a period of time after which the phone will stop ringing if the call is not answered.

## Topics

## Custom Ringtone Limit

The ring tone format must meet the following:

| Phone Model | Format | Single File Size |
|---|---|---|
| VP59/T58A/CP960 | .wav | <=8MB |

| Note |
|---|
| The ring tone file must be in PCMU/PCMA audio format, mono channel, 8K sample rate and 16-bit resolution. |

## Ringtone Configuration

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

| Parameter | phone_setting.ring_type | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures a ring tone for the phone. | |
| Permitted Values | Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (for example, Customring.wav) | |
| Default | Ring1.wav | |
| Web UI | Settings->Preference->Upload Ringtone->System Ring | |
| Phone UI | Settings->Basic Settings->Sound->Ring Tones->Common | |
| Parameter | account.X.ringtone.ring_type[1] | <MAC>.cfg |
| Description | It configures a ring tone.<br>**Example**:<br>account.1.ringtone.ring_type = Ring3.wav<br>It means configuring Ring3.wav for account1.<br>account.1.ringtone.ring_type = Common<br>It means account1 will use the ring tone selected for the phone configured by the parameter "phone_setting.ring_type". | |
| Permitted Values | Common, Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (for example, Customring.wav) | |
| Default | Common | |
| Web UI | Account->Basic->Ring Type | |
| Phone UI | Settings->Basic Settings->Sound->Ring Tones->Account X | |

| Parameter | ringtone.url | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the access URL of the custom ring tone file. | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |
| Web UI | Settings->Preference->Upload Ringtone->Custom Ring | |
| Parameter | ringtone.delete | <y0000000000xx>.cfg |
| Description | It deletes all custom ring tone files. | |
| Permitted Values | http://localhost/all | |
| Default | Blank | |
| 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 1 to 3600 | |
| Default | 120 | |
| Parameter | phone_setting.ring_for_tranfailed | <y0000000000xx>.cfg |
| Description | It configures the ring tone when the phone fails to transfer a call and display "Transfer failed" on the screen. | |
| Permitted Values | Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav or Splash.wav | |
| Default | Ring1.wav | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# Distinctive Ring Tones

The feature of distinctive ring tones allows certain incoming calls to trigger the phones to play distinctive ring tones. The IP phone inspects the INVITE request for an "Alert-Info" header when receiving an incoming call. If the INVITE request contains an "Alert-Info" header, the phone strips out the URL or keyword parameter and maps it to the appropriate ring tone.

| Note |
|---|
| If the caller already exists in the local directory, the ring tone assigned to the caller should be preferentially played. |

### Topics

Supported Alert-Info Headers Format
Distinctive Ring Tones Configuration

# Supported Alert-Info Headers Format

Yealink phones support Alert-Info headers in four formats: Bellcore-drN, ringtone-N (or MyMelodyN), <URL> and info-o=info text;x-line-id=0.

| Note |
| --- |
| If the Alert-Info header contains multiple types of keywords, the phone will process the keywords in the following order: AutoAnswer>URL>info text/Bellcore-drN/ringtone-N (ringtone-RingN)>MyMelodyN (MyMelodyRingN). |

## Topics

Alert-Info: Bellcore-drN
Alert-Info: ringtone-N/Alert-Info: ringtone-RingN.wav (or Alert-Info: MyMelodyN/Alert-Info: MyMelodyRingN.wav)
Alert-Info: <URL>
Alert-Info: info=info text;x-line-id=0

## Alert-Info: Bellcore-drN

When the Alter-Info header contains the keyword "Bellcore-drN", the phone will play the desired ring tone.

The following table identifies the corresponding ring tone:

| Value of N | Ring Tone<br>(features.alert_info_tone = 1) | Ring Tone<br>(features.alert_info_tone = 0) |
| --- | --- | --- |
| 1 | Bellcore-dr1 | Ring1.wav |
| 2 | Bellcore-dr2 | Ring2.wav |
| 3 | Bellcore-dr3 | Ring3.wav |
| 4 | Bellcore-dr4 | Ring4.wav |
| 5 | Bellcore-dr5 | Ring5.wav |
| 6 | Ring6.wav | |
| 7 | Ring7.wav | |
| 8 | Ring8.wav | |
| 9 | Silent.wav | |
| 10 | Splash.wav | |
| N<1 or N>10 | Ring1.wav | |

**Examples**:

| |
| --- |
| Alert-Info: http://127.0.0.1/Bellcore-dr1 |
| Alert-Info: test/Bellcore-dr1 |
| Alert-Info: Bellcore-dr1 |
| Alert-Info: Bellcore-dr1;x-line-id=1 |
| Alert-Info: <http://10.1.0.31>;info=Bellcore-dr1 |

The following table identifies the different Bellcore ring tone patterns and cadences (These ring tones are designed for the BroadWorks server).

| Bellcore Tone | Pattern ID | Pattern | Cadence | Minimum Duration (ms) | Nominal Duration (ms) | Maximum Duration (ms) |
|---|---|---|---|---|---|---|
| Bellcore-dr1(standard) | 1 | Ringing | • 2s On | 1800 | 2000 | 2200 |
| | | Silent | • 4s Off | 3600 | 4000 | 4400 |
| Bellcore-dr2 | 2 | Ringing | Long | 630 | 800 | 1025 |
| | | Silent | | 315 | 400 | 525 |
| | | Ringing | Long | 630 | 800 | 1025 |
| | | Silent | | 3475 | 4000 | 4400 |
| Bellcore-dr3 | 3 | Ringing | Short | 315 | 400 | 525 |
| | | Silent | | 145 | 200 | 525 |
| | | Ringing | Short | 315 | 400 | 525 |
| | | Silent | | 145 | 200 | 525 |
| | | Ringing | Long | 630 | 800 | 1025 |
| | | Silent | | 2975 | 4000 | 4400 |
| Bellcore-dr4 | 4 | Ringing | Short | 200 | 300 | 525 |
| | | Silent | | 145 | 200 | 525 |
| | | Ringing | Long | 800 | 1000 | 1100 |
| | | Silent | | 145 | 200 | 525 |
| | | Ringing | Short | 200 | 300 | 525 |
| | | Silent | | 2975 | 4000 | 4400 |
| Bellcore-dr5 | 5 | Ringing | | 450 | 500 | 550 |

**Note**

If the user is waiting for a call, "Bellcore-dr5" is a ring splash tone that reminds the user that the DND or Always Call Forward feature is enabled on the server side.

## Alert-Info: ringtone-N/Alert-Info: ringtone-RingN.wav (or Alert-Info: MyMelodyN/Alert-Info: MyMelodyRingN.wav)

When the Alter-Info header contains the keyword "ringtone-N/ringtone-RingN" or "MyMolodyN/MyMelodyRingN", the phone will play the corresponding local ring tone (RingN.wav), or play the first local ring tone (Ring1.wav) in about 10 seconds if "N" is greater than 10 or less than 1.

**Examples**:

Alert-Info: ringtone-2

Alert-Info: ringtone-Ring2.wav

Alert-Info: ringtone-2;x-line-id=1

Alert-Info: <http://10.1.0.31>;info=ringtone-2

Alert-Info: <http://127.0.0.1/ringtone-2>

Alert-Info: MyMelody2

Alert-Info: MyMelodyRing2.wav

Alert-Info: MyMelody2;x-line-id=1

Alert-Info: <http://10.1.0.31>;x-line-id=0;info=MyMelody2

The following table identifies the corresponding local ring tone:

| Value of N | Ring Tone |
|---|---|
| 1 | Ring1.wav |
| 2 | Ring2.wav |
| 3 | Ring3.wav |
| 4 | Ring4.wav |
| 5 | Ring5.wav |
| 6 | Ring6.wav |
| 7 | Ring7.wav |
| 8 | Ring8.wav |
| 9 | Silent.wav |
| 10 | Splash.wav |
| N<1 or N>10 | Ring1.wav |

## Alert-Info: <URL>

When the Alert-Info header contains a remote URL, the phone will try to download the WAV ring tone file from the URL and then play the remote ring tone if "account.X.alert_info_url_enable" is set to 1 (or the item called "Distinctive Ring Tones" on the web user interface is Enabled), or play the preconfigured local ring tone in about 10 seconds if "account.X.alert_info_url_enable" is set to 0 or if the IP phone fails to download the remote ring tone.

**Example**:

Alert-Info: http://192.168.0.12:8080/Custom.wav

## Alert-Info: info=info text;x-line-id=0

When the Alert-Info header contains an info text, the phone will map the text with the Internal Ringer Text preconfigured (or "distinctive_ring_tones.alert_info.X.text" is configured) on the IP phone, and then play the ring tone associated with the Internal Ringer Text (the ring tone can be configured by the parameter "distinctive_ring_tones.alert_info.X.ringer"). If no internal ringer text maps, the phone will play the preconfigured local ring tone in about 10 seconds.

**Example**:

Alert-Info: info=family;x-line-id=0

| | |
|---|---|
| Alert-Info: <http://10.1.0.31>;info=family | |
| Alert-Info: <http://10.1.0.31>;info=family;x-line-id=0 | |

**Auto Answer**

If the INVITE request contains the following type of strings, the phone will answer incoming calls automatically without playing the ring tone:

- Alert-Info: Auto Answer
- Alert-Info: info = alert-autoanswer
- Alert-Info: answer-after = 0 (or Alert-Info: Answer-After = 0)
- Alert-Info: Intercom

If the auto answer tone feature is enabled, the phone plays a warning tone to alert you before answering the incoming call.

## Related Topic

Auto Answer

## Distinctive Ring Tones Configuration

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

| Parameter | account.X.alert_info_url_enable[1] | <MAC>.cfg |
|---|---|---|
| Description | It enables or disables the phone to download the ring tone from the URL contained in the Alert-Info header. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Web UI | Account->Advanced->Distinctive Ring Tones | |
| Parameter | features.alert_info_tone | <y0000000000xx>.cfg |
| Description | It enables and disables the phone to map the keywords in the Alert-Info header to the specified Bellcore ring tones. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Parameter | distinctive_ring_tones.alert_info.X.text[2] | <y0000000000xx>.cfg |
| Description | It configures the internal ringer text to map the keywords contained in the Alert-Info header. | |
| Permitted Values | String within 32 characters | |
| Default | Blank | |
| Web UI | Settings->Ring->Internal Ringer X[2]->Text | |
| Parameter | distinctive_ring_tones.alert_info.X.ringer[2] | <y0000000000xx>.cfg |
| Description | It configures the desired ring tone for each internal ringer text. | |
| Permitted | - Integer from 1 to 10 (the digit stands for the appropriate ring tone) or ring tone name: | |

| Values | 1 or **Ring1.wav**<br>2 or **Ring2.wav**<br>3 or **Ring3.wav**<br>4 or **Ring4.wav**<br>5 or **Ring5.wav**<br>6 or **Ring6.wav**<br>7 or **Ring7.wav**<br>8 or **Ring8.wav**<br>9 or **Silent.wav**<br>10 or **Splash.wav**<br><ul><li>Custom ring tone name (for example, Customring.wav)</li></ul> |
|---|---|
| Default | 1 |
| Web UI | Settings->Ring->Internal Ringer X[2]->File |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

[2]X is the ring tone ID. X=1-10.

# Ringer Device

You can use either or both the speaker and the headset as the 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.

If the ringer device is set to Headset or Headset&Speaker, the headset (either a wired headset, Bluetooth headset or USB headset) should be connected to the IP phone and the headset mode also should be activated in advance. You can press the HEADSET key to activate the headset mode.

You can press the HEADSET key to activate the headset mode. For more information, refer to the Yealink phone-specific user guide.

It is not applicable to CP960 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 phone.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Use Speaker<br><br>**1**-Use Headset<br><br>**2**-Use Headset & Speaker | |
| Default | 0 | |
| Web UI | Features->Audio->Ringer Device for Headset | |

# Audio Volume

You can configure the sending volume and ringer volume for the phone.

**Topics**

## Sending Volume Configuration

You can configure the sending volume of currently engaged audio devices (handset, speakerphone or headset) when the phone is in use.

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

| Parameter | voice.handfree_send[1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the sending volume of the speaker.<br><br>**Note**: We recommend that you modify this parameter cautiously. An unsuitable value may render the voice quality bad. | |
| Permitted Values | Integer from -50 to 50 | |
| Default | 0 | |
| Web UI | Features->Audio->Handfree Send Volume (-50~50) | |
| Parameter | voice.handfree.autoreset_spk_vol | <y0000000000xx>.cfg |
| Description | It configures the speaker's volume level during a call. | |
| Permitted Values | **0**-The speakerphone volume at the end of a call persists between calls.<br><br>**1 to 15**-The speakerphone volume does not persist between calls, and resets to this specified level each new call. | |
| Default | 0 | |
| Parameter | voice.handset_send[1] | <y0000000000xx>.cfg |
| Description | It configures the sending volume of the handset.<br><br>**Note**: We recommend that you modify this parameter cautiously. An unsuitable value may render the voice quality bad. It is not applicable to CP960 phones. | |
| Permitted Values | Integer from -50 to 50 | |
| Default | 0 | |
| Web UI | Features->Audio->Handset Send Volume (-50~50) | |
| Parameter | voice.handset.autoreset_spk_vol | <y0000000000xx>.cfg |
| Description | It configures the handset's volume level during a call.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-The handset volume at the end of a call persists between calls.<br><br>**1 to 15**-The handset volume does not persist between calls, and resets to this specified level each new call. | |

| | |
|---|---|
| **Default** | 0 |
| **Parameter** | voice.headset_send[1]                    `<y0000000000xx>`.cfg |
| **Description** | It configures the sending volume of the headset.<br><br>**Note**: We recommend that you modify this parameter cautiously. An unsuitable value may render the voice quality bad. It is not applicable to CP960 phones. |
| **Permitted Values** | Integer from -50 to 50 |
| **Default** | 0 |
| **Web UI** | Features->Audio->Headset Send Volume (-50~50) |
| **Parameter** | voice.headset.autoreset_spk_vol          `<y0000000000xx>`.cfg |
| **Description** | It configures the headset's volume level during a call.<br><br>**Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-The headset volume at the end of a call persists between calls.<br><br>**1 to 15**-The headset volume does not persist between calls, and resets to this specified level each new call. |
| **Default** | 0 |
| **Parameter** | voice.side_tone[1]                       `<y0000000000xx>`.cfg |
| **Description** | It configures the volume of the side tone. |
| **Permitted Values** | Integer from -100 to 0 |
| **Default** | -25 |
| **Parameter** | voice.bluetooth_headset_send[1]        `<y0000000000xx>`.cfg |
| **Description** | It configures the sending volume of the Bluetooth headset.<br><br>**Note**: We recommend that you modify this parameter cautiously. An unsuitable value may render the voice quality bad. It is not applicable to CP960 phones. |
| **Permitted Values** | Integer from -50 to 50 |
| **Default** | 0 |

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

# 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 (not applicable to CP960 phones) |
| Secondary Dial | When adding a comma "," to the digit map (For more information on digit map, refer to Dial Plan Defined by Digit Map (New Dial Plan Mechanism)) |
| Ring Back | Ring-back tone |
| Busy | When the callee is busy |
| Congestion | When the network is congested |
| Call Waiting | Call waiting tone (For more information on call waiting, refer to Call Waiting) |
| Dial Recall | When receiving a call back |

| Condition | Description |
|---|---|
| Info | When receiving a special message |
| Stutter | When receiving a voice mail (For more information on voice mail tone, refer to Alert Tone) |
| Auto Answer | When automatically answering a call (For more information on auto answer, refer to Auto Answer) |

## 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 | It customizes the dial tone.<br><br>tone list = element[,element] [,element]…<br><br>Where<br><br>**element** = [!]Freq1[+Freq2][+Freq3][+Freq4] /Duration<br><br>**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.<br><br>**Duration**: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms.<br><br>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).<br><br>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).<br><br>**Note**: It works only if "voice.tone.country" is set to Custom. It is not applicable to CP960 phones. | |
| Permitted Values | String | |
| Default | Blank | |
| Web UI | Settings->Tones->Dial | |
| Parameter | features.partition_tone[1] | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to play the different dial tones when there is no active account.<br><br>**Note**: It works only if "voice.tone.dial" is configured. It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled. If there is an active account, the phone will play the default dial tone. If there is no active account, the phone will play the dial tone configured by "voice.tone.dial". | |

| Default | 0 | |
|---|---|---|
| **Parameter** | voice.tone.secondary_dial | <y0000000000xx>.cfg |
| **Description** | It customizes the secondary dial tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note**: It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0. | |
| **Permitted Values** | String | |
| **Default** | 350+440/3000 | |
| **Web UI** | Settings->Tones->Secondary Dial | |
| **Parameter** | voice.tone.ring | <y0000000000xx>.cfg |
| **Description** | It customizes the ringback tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note**: It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0. | |
| **Permitted Values** | String | |
| **Default** | Blank | |
| **Web UI** | Settings->Tones->Ring Back | |
| **Parameter** | voice.tone.busy | <y0000000000xx>.cfg |
| **Description** | It customizes the tone when the callee is busy. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note**: It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0. | |
| **Permitted Values** | String | |
| **Default** | Blank | |
| **Web UI** | Settings->Tones->Busy | |
| **Parameter** | voice.tone.congestion | <y0000000000xx>.cfg |
| **Description** | It customizes the tone when the network is congested. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note**: It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0. | |
| **Permitted Values** | String | |

| Default | Blank | |
|---|---|---|
| Web UI | Settings->Tones->Congestion | |
| Parameter | voice.tone.callwaiting | <y0000000000xx>.cfg |
| Description | It customizes the call waiting tone.<br><br>The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".<br><br>**Note**: It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0. | |
| Permitted Values | String | |
| Default | Blank | |
| Web UI | Settings->Tones->Call Waiting | |
| Parameter | voice.tone.dialrecall | <y0000000000xx>.cfg |
| Description | It customizes the call back tone.<br><br>The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".<br><br>**Note**: It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0. | |
| Permitted Values | String | |
| Default | Blank | |
| Web UI | Settings->Tones->Dial Recall | |
| Parameter | voice.tone.info | <y0000000000xx>.cfg |
| Description | It customizes the info tone. The phone will play the info tone with the special information, for example, the number you are calling is not in service.<br><br>The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".<br><br>**Note**: It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0. | |
| Permitted Values | String | |
| Default | Blank | |
| Web UI | Settings->Tones->Info | |
| Parameter | voice.tone.stutter | <y0000000000xx>.cfg |
| Description | It customizes the tone when the IP phone receives a voice mail.<br><br>The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".<br><br>**Note**: It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0. | |

| | |
|---|---|
| **Permitted Values** | String |
| **Default** | Blank |
| **Web UI** | Settings->Tones->Stutter |
| **Parameter** | voice.tone.autoanswer<br><y0000000000xx>.cfg |
| **Description** | It customizes the warning tone for the auto answer.<br><br>The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".<br><br>**Note**: It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0. |
| **Permitted Values** | String |
| **Default** | Blank |
| **Web UI** | Settings->Tones->Auto Answer |

# 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 |
|---|---|---|---|---|---|
| G.722.1c | G.722.1c | RFC 5577 | 48 Kbps | 32 Ksps | 20ms |
| G.722.1c | | RFC 5577 | 32 Kbps | 32 Ksps | 20ms |
| G.722.1c | | RFC 5577 | 24 Kbps | 32 Ksps | 20ms |
| G.722.1 | G.722.1 | RFC 5577 | 24 Kbps | 16 Ksps | 20ms |
| G722 | G.722 | RFC 3551 | 64 Kbps | 16 Ksps | 20ms |

| Codec | Algorithm | Reference | Bit Rate | Sample Rate | Packetization Time |
|-------|-----------|-----------|----------|-------------|-------------------|
| 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 |
| G723_53/ G723_63 | G.723.1 | RFC 3551 | 5.3 Kbps<br>6.3 Kbps | 8 Ksps | 30ms |
| iLBC | iLBC | RFC 3952 | 15.2 Kbps<br>13.33 Kbps | 8 Kps | 20ms<br>30ms |
| opus | opus | RFC 6716 | 8-12 Kbps<br>16-20 Kbps<br>28-40 Kbps<br>48-64 Kbps<br>64-128 Kbps | 8 Ksps<br>12 Ksps<br>16 Ksps<br>24 Ksps<br>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 |
|-------------|------------------------|----------------------|
| VP59/T58A/CP960 | G.722.1c (48kb/s), G.722.1c (32kb/s), G.722.1c (24kb/s), G.722.1 (24kb/s), G722, PCMU, PCMA, G729, G726-40, G726-32, G726-24, G726-16, iLBC, G723_53, G723_63, Opus | G.722.1c (48kb/s), G.722.1c (32kb/s), G.722.1c (24kb/s), G.722.1 (24kb/s), G722, PCMU, PCMA, G729 |

## 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.<br><br>The name (payload_type) of the audio codec:<br><br>**g722_1c_48kpbs**-G.722.1c (48kb/s)<br><br>**g722_1c_32kpbs**-G.722.1c (32kb/s)<br><br>**g722_1c_24kpbs**-G.722.1c (24kb/s)<br><br>**g722_1_24kpbs**-G.722.1 (24kb/s)<br><br>**g722**-G722<br><br>**pcmu**-PCMU<br><br>**pcma**-PCMA<br><br>**g729**-G729<br><br>**g726_16**-G726-16<br><br>**g726_24**-G726-24<br><br>**g726_32**-G726-32<br><br>**g726_40**-G726-40<br><br>**g723_53**-G723_53<br><br>**g723_63**-G723_63<br><br>**opus**-Opus<br><br>**ilbc**-iLBC<br><br>**Example**:<br><br>account.1.codec.g722.enable = 1<br><br>**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<br>**1**-Enabled | |
| Default | **Default**:<br><br>When the audio codec is G.722.1c (48kb/s), the default value is 1;<br><br>When the audio codec is G.722.1c (32kb/s), the default value is 1;<br><br>When the audio codec is G.722.1c (24kb/s), the default value is 1;<br><br>When the audio codec is G.722.1 (48kb/s), the default value is 1;<br><br>When the audio codec is G722, the default value is 1;<br><br>When the audio codec is PCMU, the default value is 1; | |

| | |
|---|---|
| | When the audio codec is PCMA, the default value is 1; |
| | When the audio codec is G729, the default value is 1; |
| | When the audio codec is G726-16, the default value is 0; |
| | 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 G723_53, the default value is 0; |
| | When the audio codec is G723_63, 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 |
| **Parameter** | account.X.codec.<payload_type>.priority[1] <span style="float:right">\<MAC\>.cfg</span> |
| **Description** | It configures the priority of the enabled audio codec. The name of the audio codec: **g722_1c_48kpbs**-G.722.1c (48kb/s) **g722_1c_32kpbs**-G.722.1c (32kb/s) **g722_1c_24kpbs**-G.722.1c (24kb/s) **g722_1_24kpbs**-G.722.1 (24kb/s) **g722**-G722 **pcmu**-PCMU **pcma**-PCMA **g729**-G729 **g726_16**-G726-16 **g726_24**-G726-24 **g726_32**-G726-32 **g726_40**-G726-40 **g723_53**-G723_53 **g723_63**-G723_63 **opus**-Opus **ilbc**-iLBC **Example**: account.1.codec.g722.priority = 1 **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. |
| **Permitted Values** | Integer from 0 to 16 |
| **Default** | **Default**: <br><br> When the audio codec is G722.1c (48kb/s), the default value is 1; <br><br> When the audio codec is G722.1c (32kb/s), the default value is 2; <br><br> When the audio codec is G722.1c (24kb/s), the default value is 3; <br><br> When the audio codec is G722.1 (24kb/s), the default value is 4; <br><br> When the audio codec is G722, the default value is 5; <br><br> When the audio codec is PCMU, the default value is 6; <br><br> When the audio codec is PCMA, the default value is 7; <br><br> When the audio codec is G729, the default value is 8; <br><br> When the audio codec is G726_16, the default value is 0; <br><br> When the audio codec is G726_24, the default value is 0; <br><br> When the audio codec is G726_32, the default value is 0; <br><br> When the audio codec is G726_40, the default value is 0; <br><br> When the audio codec is G723_53, the default value is 0; <br><br> When the audio codec is G723_63, the default value is 0; <br><br> When the audio codec is Opus, the default value is 0; <br><br> When the audio codec is iLBC, the default value is 0; |
| **Web UI** | Account->Codec->Audio Codec |

| **Parameter** | account.X.codec.opus.para[1] | <MAC>.cfg |
|---|---|---|
| **Description** | It configures the sample rate of the Opus audio codec. | |
| **Permitted Values** | **opus-fb**-Opus-FB (48KHz) <br><br> **opus-swb**-Opus-SWB (24KHz) <br><br> **opus-wb**-Opus-WB (16KHz) <br><br> **opus-mb**-Opus-MB (12KHz) <br><br> **opus-nb**-Opus-NB (8KHz) | |
| **Default** | opus-fb | |
| **Web UI** | Account->Codec->Opus Sample Rate | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# Packetization Time (PTime)

PTime is a measurement of the duration (in milliseconds) that how long the audio data in each RTP packet is sent to the destination, and defines how much the 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) |
|---|---|---|
| G.722.1c(48kb/s) | 20ms | 60ms |
| G.722.1c(32kb/s) | 20ms | 60ms |
| G.722.1c(24kb/s) | 20ms | 60ms |
| G.722.1(24kb/s) | 20ms | 60ms |
| G722 | 10ms | 40ms |
| PCMA | 10ms | 40ms |
| PCMU | 10ms | 40ms |
| G729 | 10ms | 80ms |
| G726-16 | 10ms | 30ms |
| G726-24 | 10ms | 30ms |
| G726-32 | 10ms | 30ms |
| G726-40 | 10ms | 30ms |
| G723_53/ G723_63 | 30ms | 60ms |
| iLBC | 20ms | 30ms |
| opus | 10ms | 20ms |

## 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<br><br>**10**-10<br><br>**20**-20<br><br>**30**-30<br><br>**40**-40<br><br>**50**-50<br><br>**60**-60 | |
| Default | 20 | |
| Web UI | Account->Advanced->PTime(ms) | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# 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.

### 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<br><br>**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 | |

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

# Headset Prior

Headset prior allows users to use headset preferentially if a headset is physically connected to the IP phone. This feature is especially useful for permanent or full-time headset users.

It is not applicable to CP960 phones.

| Note |
| --- |
| It is not applicable to the Bluetooth headset and USB headset. |

## Topic

## Headset Prior Configuration

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

| Parameter | features.headset_prior | <y0000000000xx>.cfg |
| --- | --- | --- |
| Description | It enables or disables to preferentially use the headset mode for all incoming and outgoing calls.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled, the headset mode will be deactivated after the call, if you switch the headset mode to speakerphone/handset mode.<br><br>**1**-Enabled, the headset mode will not be deactivated after the call, even if you switch the headset mode to speakerphone/handset mode. | |
| Default | 0 | |
| Web UI | Features->General Information->Headset Prior | |

# Dual Headset

Dual headset allows you to use two headsets on one IP phone. To use this feature, you need to physically connect two headsets to the headset and handset jacks respectively. Once the IP phone connects to a call, the headset connected to the headset jack has full-duplex capability, with the headset connected to the handset jack is only used for listening.

| Note |
| --- |
| Dual headset is not applicable to the Bluetooth headset and USB headset. It is not applicable to CP960 phones. |

## Topic

## Dual Headset Configuration

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

| Parameter | features.headset_training | <y0000000000xx>.cfg |
| --- | --- | --- |
| Description | It enables or disables the dual headset feature.<br><br>**Note**: It works only if "features.headset_mode.enable" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, users can use two headsets on one phone. When the IP phone joins a call, the headset connected to the headset jack has full-duplex capability, with the headset connected to the handset jack is only used for listening. | |
| Default | 0 | |

| | |
|---|---|
| **Web UI** | Features->General Information->Dual Headset |

# Acoustic Clarity Technology

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

## Topics

Acoustic Echo Cancellation (AEC)
Noise Suppression
Background Noise Suppression (BNS)
Automatic Gain Control (AGC)
Voice Activity Detection (VAD)
Comfort Noise Generation (CNG)
Jitter Buffer
Smart Noise Block
Acoustic Shield

## Acoustic Echo Cancellation (AEC)

Yealink phones employ advanced AEC for hands-free operation. You can configure the AEC feature to remove the echo of the local loudspeaker from the local microphone without removing the near-end speech.

AEC is not normally required for calls via the handset. In some cases, where echo is experienced by the remote party, AEC may be used to reduce/avoid echo when you use the handset.

| **Note** |
|---|
| Utilizing acoustic echo cancellation will introduce a small increase of delay into an audio path which might cause a lower voice quality. |

## Topic

AEC Configuration

### AEC Configuration

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

| **Parameter** | voice.echo_cancellation | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the AEC (Acoustic Echo Canceller) feature. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 1 | |
| **Web UI** | Settings->Voice->Echo Cancellation->ECHO | |

## Noise Suppression

The impact noise in the room is picked-up, including paper rustling, coffee mugs, coughing, typing, and silverware striking plates. These noises, when transmitted to remote participants, can be very distracting.

You can enable the Noise Suppression feature to suppress these noises.

## Topic

### Noise Suppression Configuration

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

| Parameter | voice.tns.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the Noise Suppression feature. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Web UI | Settings->Voice->Noise Proof->Noise Suppression | |

## 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

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<br>**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

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<br>**1**-Enabled | |
| **Default** | 1 | |
| **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

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<br><br>**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.<br><br>**Note**: It works only if "voice.jib.adaptive" is set to 1 (Adaptive). The value of this parameter should be less than or equal to that of "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.<br><br>**Note**: It works only if "voice.jib.adaptive" is set to 1 (Adaptive). The value of this parameter should be | |

| | |
|---|---|
| | greater than or equal to that of "voice.jib.normal". |
| **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 or equal to that of "voice.jib.min" and less than or equal to that of "voice.jib.max". |
| **Permitted Values** | Integer from 0 to 400 |
| **Default** | 120 |
| **Web UI** | Settings->Voice->JITTER BUFFER->Normal |
| **Parameter** | voice.jib.wifi.adaptive | <y0000000000xx>.cfg |
| **Description** | It configures the type of jitter buffer in the wireless network. |
| **Permitted Values** | **0**-Fixed <br> **1**-Adaptive |
| **Default** | 1 |
| **Parameter** | voice.jib.wifi.min | <y0000000000xx>.cfg |
| **Description** | It configures the minimum delay time (in milliseconds) of jitter buffer in the wireless network. **Note**: It works only if "voice.jib.wifi.adaptive" is set to 1 (Adaptive). The value of this parameter should be less than or equal to that of "voice.jib.wifi.normal". |
| **Permitted Values** | Integer from 0 to 500 |
| **Default** | 60 |
| **Parameter** | voice.jib.wifi.max | <y0000000000xx>.cfg |
| **Description** | It configures the maximum delay time (in milliseconds) of jitter buffer in the wireless network. **Note**: It works only if "voice.jib.wifi.adaptive" is set to 1 (Adaptive). The value of this parameter should be greater than or equal to that of "voice.jib.wifi.normal". |
| **Permitted Values** | Integer from 0 to 500 |
| **Default** | 500 |
| **Parameter** | voice.jib.wifi.normal | <y0000000000xx>.cfg |
| **Description** | It configures the normal delay time (in milliseconds) of jitter buffer in the wireless network. **Note**: It works only if "voice.jib.wifi.adaptive" is set to 0 (Fixed). The value of this parameter should be greater than or equal to that of "voice.jib.wifi.min" and less than or equal to that of "voice.jib.wifi.min". |
| **Permitted Values** | Integer from 0 to 500 |

| Default | 240 |
|---------|-----|

## Smart Noise Block

You can use the Smart Noise Block feature to block out the noises when there is no speech in a call.

### Topic

Smart Noise Block Configuration

### Smart Noise Block Configuration

The following table lists the parameter you can use to configure smart noise block.

| Parameter | voice.ans_nb.enable | \<y0000000000xx\>.cfg |
|-----------|---------------------|------------------------|
| Description | It enables or disables the Smart Noise Block feature.<br><br>**Note**: It works only if "voice.tns.enable" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Settings->Voice->Noise Proof->Smart Noise Block | |

## Acoustic Shield

The acoustic shield feature is designed for background noise suppression when you are using the phone handset or a connected headset.

It is particularly used in the open office environment, such as call center, where background noise can impact far-end audio quality.

It is not applicable to CP960 phones.

### Topic

Acoustic Shield Configuration

### Acoustic Shield Configuration

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

| Parameter | features.acoustic_shield.mode | \<y0000000000xx\>.cfg |
|-----------|-------------------------------|------------------------|
| Description | It enables or disables the acoustic shield feature during the call.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, you need to manually enable acoustic shield by tapping the **Acoustic Shield** soft key during the call.<br><br>**2**-Auto, acoustic shield is automatically enabled when the call is set up. You can tap the **Acoustic Shield** soft key during the call to disable it. | |
| Default | 0 | |
| Web UI | Settings->Voice->Acoustic Shield->Acoustic Shield Mode | |

| Parameter | features.acoustic_shield.level | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the noise suppression level for handsets and headsets.<br><br>The higher value represents the better noise suppression effect.<br><br>If it is set to 3, the phone automatically shields the noise out of 20 centimeters (7.9 inch) when you are using the phone handset or a headset.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | Integer from 1 to 3 | |
| Default | 2 | |

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

**DTMF Keypad Frequencies:**

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

| 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

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.<br><br>**1**-RFC2833, DTMF digits are transmitted by RTP Events compliant to RFC 2833.<br><br>**2**-SIP INFO, DTMF digits are transmitted by the SIP INFO messages.<br><br>**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.<br><br>**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.<br><br>**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<br><br>**2**-DTMF<br><br>**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 300 | |
| 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. For VP59/T58A, X=1-16, for CP960, X=1.

[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<br>**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 | |

## Transfer via DTMF

Call transfer is implemented via DTMF on some servers. The IP phone sends specified DTMF digits to the server for transferring calls to third parties.

### Topic

Transfer via DTMF Configuration

### Transfer via DTMF Configuration

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

| Parameter | features.dtmf.replace_tran | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to send designated DTMF sequences for transfer function when tapping the**Transfer** soft key or TRAN/TRANSFER key. | |
| Permitted Values | **0**-Disabled **1**-Enabled | |
| Default | 0 | |
| Web UI | Features->General Information->DTMF Replace Tran | |
| Parameter | features.dtmf.transfer | <y0000000000xx>.cfg |
| Description | It configures the DTMF sequences to be transmitted to perform call transfer. Valid values are: 0-9, *, # and A-D. **Note**: It works only if "features.dtmf.replace_tran" is set to 1 (Enabled). | |
| Permitted Values | String within 32 characters | |
| Default | Blank | |
| Web UI | Features->General Information->Tran Send DTMF | |

## Local DTMF Tone

Local DTMF tone allows the phones to play a local DTMF tone during an active call. If this feature is enabled, you can hear the DTMF tone when pressing the IP phone's keypad during a call.

### Topic

## Local DTMF Tone Configuration

The following table lists the parameter you can use to configure the local DTMF tone.

| Parameter | features.play_local_dtmf_tone_enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to play a local DTMF tone. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled, you can hear the DTMF tone when pressing the phone's keypad during a call. | |
| Default | 1 | |
| Web UI | Features->General Information->Play Local DTMF Tone | |

# 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<br>**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<br>**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<br>**1**-Enabled | |
| **Default** | 0 | |
| **Web UI** | Settings->Voice Monitoring->VQ RTCP-XR Session Report | |
| **Parameter** | phone_setting.vq_rtcpxr.interval_report.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to send an interval quality report to the central report collector peri- | |

| | |
|---|---|
| | odically throughout a call. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |
| **Web UI** | Settings->Voice Monitoring->VQ RTCP-XR Interval Report |
| **Parameter** | phone_setting.vq_rtcpxr_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.<br><br>**Note**: It works only if "phone_setting.vq_rtcpxr.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_rtcpxr_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.<br><br>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.<br><br>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_rtcpxr_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.<br><br>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.<br><br>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** | 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. |

| | 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.<br><br>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. |
|---|---|
| **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** | 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.<br><br>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.<br><br>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. |
| **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 or phone user interface. You can also specify the options of the RTP status to be displayed on the phone user interface. Options of the RTP status displayed on the web user interface cannot be specified.

| **Note** |
|---|
| You can configure the softkey layout feature to display the **RTP Status** soft key during the conference. Then you can press the **RTP Status** soft key to check the voice quality data with different parties. For more information, refer to Softkey Layout. |

## 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** | **0**-Disabled<br>**1**-Enabled |

| Values | |
|---|---|
| **Default** | 0 |
| **Web UI** | Settings->Voice Monitoring->Display Report Options on Web |
| **Parameter** | phone_setting.vq_rtcpxr.states_show_on_gui.enable `<y0000000000xx>.cfg` |
| **Description** | It enables or disables the voice quality data of the last call or current call to be displayed on the phone screen. You can view the voice quality data of the last call on the phone at the path **Settings**->**Status**->**RTP Status**. You can view the voice quality data of the current call by tapping the **RTP Status** soft key during a call. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |
| **Web UI** | Settings->Voice Monitoring->Display Report Options on Phone |
| **Parameter** | phone_setting.vq_rtcpxr_display_start_time.enable `<y0000000000xx>.cfg` |
| **Description** | It enables or disables the phone to display Start Time on the phone screen.<br>**Note**: It works only if "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 1 |
| **Web UI** | Settings->Voice Monitoring->Report Options on Phone->Start Time |
| **Parameter** | phone_setting.vq_rtcpxr_display_stop_time.enable `<y0000000000xx>.cfg` |
| **Description** | It enables or disables the phone to display Current Time or Stop Time on the phone screen.<br>**Note**: It works only if "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 1 |
| **Web UI** | Settings->Voice Monitoring->Report Options on Phone->Current Time |
| **Parameter** | phone_setting.vq_rtcpxr_display_local_call_id.enable `<y0000000000xx>.cfg` |
| **Description** | It enables or disables the phone to display Local User on the phone screen.<br>**Note**: It works only if "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 1 |
| **Web UI** | Settings->Voice Monitoring->Report Options on Phone->Local User |
| **Parameter** | phone_setting.vq_rtcpxr_display_remote_call_id.enable `<y0000000000xx>.cfg` |
| **Description** | It enables or disables the phone to display Remote User on the phone screen<br>**Note**: It works only if "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). |
| **Permitted** | **0**-Disabled |

| | |
|---|---|
| **Values** | **1**-Enabled |
| **Default** | 1 |
| **Web UI** | Settings->Voice Monitoring->Report Options on Phone->Remote User |
| **Parameter** | phone_setting.vq_rtcpxr_display_local_codec.enable  <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to display Local Codec on the phone screen<br><br>**Note**: It works only if "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 1 |
| **Web UI** | Settings->Voice Monitoring->Report Options on Phone->Local Codec |
| **Parameter** | phone_setting.vq_rtcpxr_display_remote_codec.enable  <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to display Remote Codec on the phone screen<br><br>**Note**: It works only if "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 1 |
| **Web UI** | Settings->Voice Monitoring->Report Options on Phone->Remote Codec |
| **Parameter** | phone_setting.vq_rtcpxr_display_jitter.enable  <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to display Jitter on the phone screen.<br><br>**Note**: It works only if "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 1 |
| **Web UI** | Settings->Voice Monitoring->Report Options on Phone->Jitter |
| **Parameter** | phone_setting.vq_rtcpxr_display_jitter_buffer_max.enable  <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to display Jitter Buffer Max on the phone screen.<br><br>**Note**: It works only if "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 1 |
| **Web UI** | Settings->Voice Monitoring->Report Options on Phone->Jitter Buffer Max |
| **Parameter** | phone_setting.vq_rtcpxr_display_packets_lost.enable  <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to display Packets lost on the phone screen.<br><br>**Note**: It works only if "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |

| | |
|---|---|
| **Default** | 1 |
| **Web UI** | Settings->Voice Monitoring->Report Options on Phone->Packets lost |
| **Parameter** | phone_setting.vq_rtcpxr_display_symm_oneway_delay.enable     <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to display SymmOneWayDelay on the phone screen.<br>**Note**: It works only if "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |
| **Web UI** | Settings->Voice Monitoring->Report Options on Phone->SymmOneWayDelay |
| **Parameter** | phone_setting.vq_rtcpxr_display_round_trip_delay.enable     <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to display RoundTripDelay on the phone screen.<br>**Note**: It works only if "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |
| **Web UI** | Settings->Voice Monitoring->Report Options on Phone->RoundTripDelay |
| **Parameter** | phone_setting.vq_rtcpxr_display_moslq.enable     <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to display MOS-LQ on the phone screen.<br>**Note**: It works only if "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 1 |
| **Web UI** | Settings->Voice Monitoring->Report Options on Phone->MOS-LQ |
| **Parameter** | phone_setting.vq_rtcpxr_display_moscq.enable     <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to display MOS-CQ on the phone screen.<br>**Note**: It works only if "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled |
| **Default** | 1 |
| **Web UI** | Settings->Voice Monitoring->Report Options on Phone->MOS-CQ |

## 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_rtcpxr.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_rtcpxr.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_rtcpxr.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. For VP59/T58A, X=1-16, for CP960, X=1.

# Silent Mode

You can use silent mode feature to block the incoming call/message from producing ring tone/notification tone from phone's speaker. It is helpful for users not to be disturbed by the tone.

Yealink phones support the following three methods to enable the silent mode feature:

- Turn on the silent mode via phone user interface at the path: **Settings**->**Basic Settings**->**Sound**.
- Swipe down from the top of the screen to enter the control center, tap **Silent**.
- Press the Volume key to adjust the ringer volume to the minimum.

By default, the users can enable or disable the silent mode. You can disable the users to configure it.

## Topic

Silent Mode Configuration

## Silent Mode Configuration

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

| Parameter | phone_setting.permit_silent_mode.enable | \<y0000000000xx\>.cfg |
|---|---|---|
| Description | It enables or disables the user to have the permission to use the silent mode feature. | |
| Permitted Values | **0**-Disabled, the Silent Mode item will disappear from the phone user interface at the path: **Settings**->**Basic Settings**->**Sound**. Users can neither enable the silent mode feature from the control center or via phone user interface, nor adjust the ringer volume to minimum.<br>**1**-Enabled | |
| Default | 1 | |

# Phone Customization

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

**Topics**

## Language

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

**Topics**

### 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 phone user interface and the web user interface.

| Phone User Interface | | Web User Interface | | |
|---|---|---|---|---|
| Language | Language Pack | Language | Language Pack | Note Language Pack |
| English | 000.GUI.English.lang | English | 1.English.js | 1.English_note.xml |
| Chinese Simplified | 001.GUI.Chinese_S.lang | Chinese Simplified | 2.Chinese_S.js | 2.Chinese_S_note.xml |
| Chinese Traditional | 002.GUI.Chinese_T.lang | Chinese Traditional | 3.Chinese_T.js | 3.Chinese_T_note.xml |
| French | 004.GUI.French.lang | French | 4.French.js | 4.French_note.xml |
| German | 005.GUI.German.lang | German | 5.German.js | 5.German_note.xml |
| Italian | 006.GUI.Italian.lang | Italian | 6.Italian.js | 6.Italian_note.xml |
| Polish | 007.GUI.Polish.lang | Polish | 7.Polish.js | 7.Polish_note.xml |
| Portuguese | 008.GUI.Portuguese.lang | Portuguese | 8.Portuguese.js | 8.Portuguese_note.xml |
| Spanish | 010.GUI.Spanish.lang | Spanish | 9.Spanish.js | 9.Spanish_note.xml |
| Turkish | 012.GUI.Turkish.lang | Turkish | 10.Turkish.js | 10.Turkish_note.xml |
| Russian | 013.GUI.Russian.lang | Russian | 11.Russian.js | 11.Russian_note.xml |

## Language Display Configuration

The default language displayed on the phone 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 user interface and web user interface respectively.

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

| Parameter | lang.gui | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the language used on the phone user interface. | |
| Permitted Values | English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian or the custom language name. | |
| Default | English | |
| Phone UI | Settings->Basic Settings->Language & Input->Language | |
| Parameter | lang.wui | <y0000000000xx>.cfg |
| Description | It configures the language used on the web user interface. | |
| Permitted Values | English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian or the custom language name. | |
| Default | English | |
| Web UI | On the top-right corner of the web user interface | |

## Language for Phone Display Customization

You can customize the translation of the existing language on the phone user interface. Languages available for selection depend on language packs currently loaded to the IP phone. You can also add new languages (not included in the

available language list) available for phone display by loading language packs to the IP phone.

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

## Topics

### Customizing a Language Pack for Phone Display

When you add a new language pack for the phone user interface, the language pack must be formatted as "X.GUI.-name.lang" (X starts from 014, "name" is replaced with the language name). If the language name is the same as the existing one, the existing language pack will be overridden by the newly uploaded one. We recommend that the filename 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 file (for example, 000.GUI.English.lang).

Modify the characters within the double quotation marks on the right of the equal sign. Do not modify the item on the left of the equal sign.

The following shows a portion of the language pack "000.GUI.English.lang" for the phone user interface:



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

### Custom Language for Phone Display Configuration

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

| Parameter | gui_lang.url | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the access URL of the custom LCD language pack for the phone user interface.<br><br>**Note**: You can also download multiple language packs to the phone simultaneously. | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |
| Parameter | gui_lang.delete | <y0000000000xx>.cfg |
| Description | It deletes the specified or all custom LCD language packs of the phone user interface. | |
| Permitted Values | For example: http://localhost/all or http://localhost/X.GUI.name.lang<br><br>X starts from 014, "name" is replaced with the language name. | |
| Default | Blank | |

## Example: Setting a Custom Language for Phone Display

The following example shows the configuration for uploading custom language files "015.GUI.English_15.lang" and "016.GUI.English_16.lang", and then specify "015.GUI.English_15.lang" to display on the phone user interface. These language files are customized and placed on the provisioning server "192.168.10.25".

**Example**

*gui_lang.url= http://192.168.10.25/015.GUI.English_15.lang*

*gui_lang.url= http://192.168.10.25/016.GUI.English_16.lang*

*lang.gui=English_15*

After provisioning, text displayed on the phone user interface will change to the custom language you defined in "015.GUI.English_15.lang". You can also find a new language selection"English_15" and "English_16" on the IP phone user interface: **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 also customize the translation of the note language pack. The note information is displayed in the icon 🔵 of the web user interface.

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
Customizing a Language Pack for Note Display
Custom Language for Web and Note 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. |
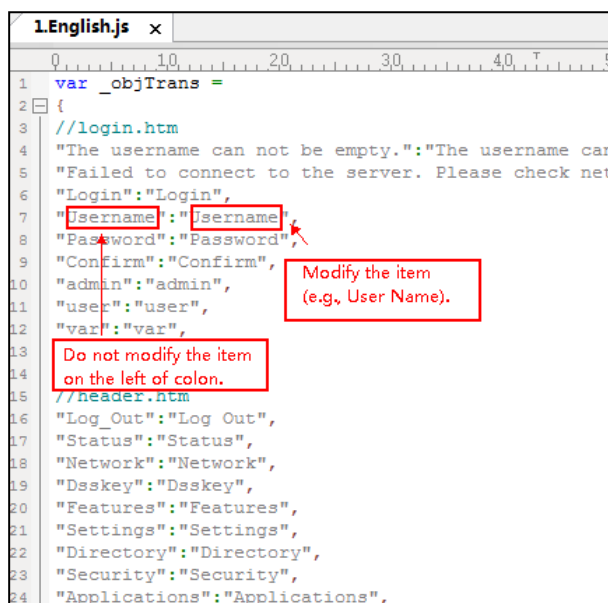
## Procedure

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:



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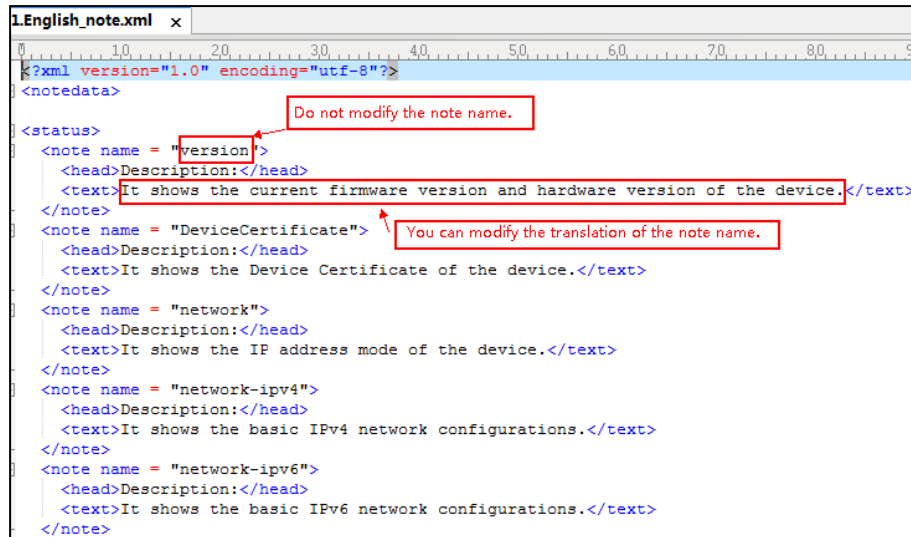
Save the note language pack and place it to the provisioning server.

## Custom Language for Web and Note Display Configuration

If you want to add a new language (for example, Wuilan) to phones, prepare the language file named as "12.Wuilan.js" and "12.Wuilan_note.xml" for downloading. After the update, you will find a new language selection "Wuilan" at the top-right corner of the web user interface, and new note information is displayed in the icon when the new language is selected.

The following table lists the parameters you can use to configure a custom language for web and note 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_note.url | <y0000000000xx>.cfg |
| Description | It configures the access URL of the custom note language pack for web user interface. | |
| Permitted Values | URL within 511 characters  For example: http://localhost/X.name_note.xml  X starts from 12, "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 | |

196

# Wallpaper

Wallpaper is a picture used as the background of the phone. The phone comes with a default picture. You can change it to a built-in picture or custom wallpaper from personal pictures.

The wallpaper is applicable to the VP59/T58A/CP960 phones and expansion module EXP50 (connected to the T58A phones).

**Topics**

## Wallpaper Configuration

You can change the wallpaper to any built-in picture or custom picture.

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

For VP59/T58A phones, you can also set a custom picture stored in local or USB flash drive (if connected) as the wallpaper.

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

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

| Parameter | phone_setting.backgrounds | <y0000000000xx>.cfg |
| --- | --- | --- |
| Description | It configures the wallpaper displayed on the phone Idle screen. | |
| Permitted Values | Default.jpg, 01.jpg, 02.jpg, 03.jpg, 04.jpg, 05.jpg, 06.jpg, 07.jpg, 08.jpg, 09.jpg or 10.jpg or uploaded custom wallpaper name (for example, wallpaper.jpg) | |
| Default | Default.jpg | |
| Web UI | Settings->Preference->Upload Wallpaper->System Wallpaper | |
| Phone UI | Settings->Basic Settings->Display->Wallpaper | |
| Parameter | expansion_module.backgrounds | <y0000000000xx>.cfg |
| Description | It configures the wallpaper displayed on the expansion module. **Note**: It is only applicable to EXP50 expansion modules connected to the T58A phones. | |
| Permitted Values | Default-exp50.jpg, 01-exp50.jpg, 02-exp50.jpg, 03-exp50.jpg, 04-exp50.jpg, 05-exp50.jpg, 06-exp50.jpg, 07-exp50.jpg, 08-exp50.jpg, 09-exp50.jpg or 10-exp50.jpg or custom | |
| Default | Default-exp50.jpg | |
| Web UI | Settings->Preference->Upload Wallpaper->System Expansion Wallpaper | |
| Phone UI | Settings->Basic Settings->Display->EXP Background | |

# Wallpaper Customization

You can configure a custom picture, such as company logo, and then upload the custom picture to the IP phone that users can choose from when changing the wallpaper for the phone idle screen, expansion module.

## Topics

## Custom Wallpaper Picture Limit

Either the smaller or the larger picture will be scaled proportionally to fit the screen. The wallpaper picture format must meet the following:

| Format | Resolution | Single File Size |
|---|---|---|
| *.jpg | <=2.0 megapixels | <=5MB |

## Custom Wallpaper Configuration

The following table lists the parameter you can use to upload a custom picture.

| Parameter | wallpaper_upload.url | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the access URL of the custom wallpaper picture. | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |
| Web UI | Settings->Preference->Upload Wallpaper->Custom Wallpaper | |

## Deleting a Custom Picture

You can delete the uploaded custom pictures for a specific IP phone via web user interface at the path: **Settings**->**Preference**->**Wallpaper**, select the desired custom picture and click Delete. You can also delete the custom pictures via phone user interface at the path: **Settings**->**Basic Settings**->**Display**->**Wallpaper**. You can only delete the custom pictures.

## Example: Setting a Custom Picture as Wallpaper

The following example shows the configuration for uploading custom picture named "wallpaper.jpg" and set it as idle screen wallpaper. The custom picture is placed on the provisioning server "192.168.10.25".

**Example**

wallpaper_upload.url = http://192.168.10.25/wallpaper.jpg

phone_setting.backgrounds = wallpaper.jpg

After provisioning, the phone idle screen wallpaper changes to custom picture "wallpaper.jpg".

# Screen Saver

The screen saver will automatically start when the IP phone is idle for the preset waiting time. You can stop the screen saver at any time by pressing any key or touching the screen. When your phone is idle again for a preset waiting time,

the screen saver starts again.

For T58A phones, if you connect a color-screen expansion module EXP50 to the phone, the screen saver will start or stop on the phone and EXP50 synchronously.

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

**Topic**

Screensaver Configuration

## Screensaver Configuration

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

| Parameter | screensaver.wait_time | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the time (in seconds) to wait in the idle state before the screen saver starts. | |
| Permitted Values | **15**-15s<br><br>**30**-30s<br><br>**60**-1min<br><br>**120**-2min<br><br>**300**-5min<br><br>**600**-10min<br><br>**1800**-30min | |
| Default | 600 | |
| Phone UI | Settings->Basic Settings->Display->Screen Saver->Screensaver Waiting Time | |
| Parameter | screensaver.type | <y0000000000xx>.cfg |
| Description | It configures the type of screen saver to display. | |
| Permitted Values | **0**-Clock<br><br>**1**-Colours<br><br>**2**-Photo Frame<br><br>**3**-Photo Table | |
| Default | 1 | |
| Phone UI | Settings->Basic Settings->Display->Screen Saver->Clock/Colours/Phone Frame/Photo Table | |
| Parameter | features.blf_active_backlight.enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to turn on the backlight or stop the screen saver when the BLF/BLF list status changes. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |

# Backlight

You can change the backlight brightness of the phone screen during phone activity and inactivity. The backlight brightness automatically changes when the phone is idle for a specified time.

You can change the screen backlight brightness and time in the following settings:

**Active Level**: The brightness level of the LCD screen when the phone is active. Digits (1-10) represent different brightness levels. 10 is the brightest level.

**Inactive Level**: The brightness of the LCD screen when the phone is inactive. You can select a low brightness or turn off the backlight.

**Backlight Time**: The delay time to change the brightness of the LCD screen when the phone is inactive. Backlight time includes the following settings you can choose from:

- **Always On**: Backlight is on permanently.
- **15s**, **30s**, **1min**, **2min**, **5min**, **10min** or **30min**: Backlight is changed when the phone is inactive after the designated time (in seconds).

### Topics

Supported Backlight Options
Backlight and Time Configuration

## Supported Backlight Options

The following table lists available configuration options to configure the backlight of phone models/expansion modules:

| Phone Model (and the connected expansion module) | Configuration Options |
|---|---|
| T58A(EXP50)<br>VP59<br>CP960 | Inactive Level<br><br>Active Level (Backlight Active Level)<br><br>Backlight Time |

## Backlight and Time Configuration

The following table lists the parameters you can use to configure screen backlight and time.

| Parameter | phone_setting.active_backlight_level | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the intensity of the LCD screen when the phone is active.<br>**Note**: If the expansion module is connected, the backlight on the expansion module automatically changes to match this setting. | |
| Permitted Values | Integer from 1 to 10 | |
| Default | 8 | |
| Web UI | Settings->Preference->Active Level | |
| Phone UI | Settings->Basic Settings->Display->Backlight->Backlight Active Level | |

| Parameter | phone_setting.backlight_time | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the delay time (in seconds) to change the intensity of the LCD screen when the phone is inactive. | |
| Permitted Values | **0**-Always On<br><br>**15**-15s<br><br>**30**-30s<br><br>**60**-1min<br><br>**120**-2min<br><br>**300**-5min<br><br>**600**-10min<br><br>**1800**-30min | |
| Default | 0 | |
| Web UI | Settings->Preference->Backlight Time(seconds) | |
| Phone UI | Settings->Basic Settings->Display->Backlight->Backlight Time | |

# Page Tips

Page tips feature allows the breathing light or page icon to indicate different key status on the non-current page. It is mainly used when multi-page line keys are configured.

Page tips feature is available on Yealink VP59/T58A/CP960 phones and the expansion module EXP50 only when connected to T58A phones.

## Topics

Phone Page Tips
Expansion Module Page Tips

## Phone Page Tips

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

For VP59/T58A phones, if page tips feature is enabled, the breathing light will appear at the top/bottom of the DSS key field when the status of a particular feature (e.g., BLF) assigned to the line key on the non-current page changes.

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

## Topics
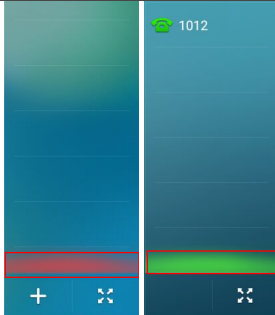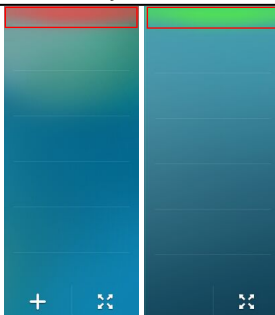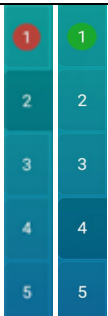
Phone Page Tips Indicator
Phone Page Tips Configuration

### Phone Page Tips Indicator

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

| Line Key Type | Color Type |
|:---:|:---:|
| Call Park | Red |
| Intercom | Red |
| Line | Green |
| BLF | Red |

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

| Phone Models | Breathing Light | Description |
|:---:|:---:|:---|
| VP59/T58A | <br>(Drag up to view the desired feature key)<br><br><br>(Drag down to view the desired feature key) | • There is a call parked to the line on the non-current page.<br><br>• The intercom target extension receives an incoming intercom call on the non-current page.<br><br>• The line receives an incoming call on the non-current page.<br><br>• The call of the line is placed on hold on the non-current page.<br><br>• The BLF monitored user receives an incoming call on the non-current page. |
| CP960 | <br>(Tap corresponding page icon to | |

| Phone Models | Breathing Light | Description |
|---|---|---|
| | view the desired feature key) | |

## Phone Page Tips Configuration

The following table lists the parameter you can use to configure phone page tips.

| Parameter | phone_setting.page_tip | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the breathing light and page icon to indicate different status of line keys on the non-current page. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Dsskey->Line Key->Enable Page Tips | |

# Expansion Module Page Tips

On expansion module EXP50, the page tips feature allows the page switch key LED to indicate that BLF monitored user receives an incoming call on the non-current page.

It is not applicable to VP59/CP960 phones.

## Topics

## Expansion Module Page Tips Indicator

The following table lists the status of page switch key LED displayed on the expansion module:

| Models | LED Status | Icons | Description |
|---|---|---|---|
| EXP50 | Flashing red | / | The BLF monitored user receives an incoming call on the non-current pages. |

## Expansion Module Page Tips Configuration

The following table lists the parameters you can use to configure expansion module page tips.

| Parameter | expansion_module.page_tip.blf_call_in.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the page switch key LED on the expansion module to indicate when BLF monitored user receives an incoming call on the non-current pages.<br><br>**Note**: It is only applicable to EXP50 expansion modules connected to the T58A phones. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Parameter | expansion_module.page_tip.blf_call_in.led | <y0000000000xx>.cfg |
| Description | It configures the page switch key LED status on the expansion module when BLF monitored user receives an incoming call on the non-current pages. | |

| | This value uses the same macro action string syntax as an Enhanced DSS key.<br><br>If it is left blank, the default value takes effect.<br><br>**Example**:<br><br>expansion_module.page_tip.blf_call_in.led = $LEDr300o300$<br><br>It means an infinite loop for page switch key LED status: glow red for 300ms and then be in the off state for 300ms.<br><br>**Note**: It works only if "expansion_module.page_tip.blf_call_in.enable" is set to 1 (Enabled). It is only applicable to EXP50 expansion modules connected to the T58A phones. |
|---|---|
| **Permitted Values** | String |
| **Default** | $LEDr300o300$ |

# 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 | +1 | Namibia(Windhoek) |
| -11 | Samoa | +2 | Estonia(Tallinn) |
| -11 | Midway Island | +2 | Finland(Helsinki) |
| -10 | United States-Hawaii-Aleutian | +2 | Gaza Strip(Gaza) |
| -10 | United States-Alaska-Aleutian | +2 | Greece(Athens) |
| -9:30 | French Polynesia | +2 | Harare |
| -9 | United States-Alaska Time | +2 | Israel(Tel Aviv) |
| -8 | Canada(Vancouver,Whitehorse) | +2 | Jordan(Amman) |
| -8 | Mexico(Tijuana,Mexicali) | +2 | Latvia(Riga) |

| Time Zone | Time Zone Name | Time Zone | Time Zone Name |
|---|---|---|---|
| -8 | United States-Pacific Time | +2 | Lebanon(Beirut) |
| -8 | Baja California | +2 | Moldova(Kishinev) |
| -7 | Canada(Edmonton,Calgary) | +2 | Pretoria |
| -7 | Mexico(Mazatlan,Chihuahua) | +2 | Romania(Bucharest) |
| -7 | United States-Mountain Time | +2 | Russia(Kaliningrad) |
| -7 | United States-MST no DST | +2 | Syria(Damascus) |
| -7 | Chihuahua,la Paz | +2 | Turkey(Ankara) |
| -7 | Arizona | +2 | Ukraine(Kyiv, Odessa) |
| -6 | Guatemala | +2 | Bulgaria(Sofia) |
| -6 | El Salvador | +2 | Cairo |
| -6 | Honduras | +2 | E Europe |
| -6 | Nicaragua | +2 | Istanbul |
| -6 | Costa Rica | +2 | Jerusalem |
| -6 | Belize | +2 | Lithuania(Vinius) |
| -6 | Canada-Manitoba(Winnipeg) | +2 | Tripol |
| -6 | Chile(Easter Islands) | +3 | East Africa Time |
| -6 | Guadalajara | +3 | Iraq(Baghdad) |
| -6 | Monterrey | +3 | Russia(Moscow) |
| -6 | Mexico(Mexico City,Acapulco) | +3 | Kuwait,Rlyadh |
| -6 | United States-Central Time | +3 | Minsk |
| -6 | Saskatchewan | +3 | Nairobi |
| -5 | Peru | +3 | St.Petersburg |
| -5 | Bahamas(Nassau) | +3 | Volgograd(RTZ 2) |
| -5 | Canada(Montreal,Ottawa,Quebec) | +3:30 | Iran(Teheran) |
| -5 | Cuba(Havana) | +4 | Armenia(Yerevan) |
| -5 | United States-Eastern Time | +4 | Azerbaijan(Baku) |
| -5 | Bogota.Lima | +4 | Georgia(Tbilisi) |
| -5 | Indiana(East) | +4 | Kazakhstan(Aktau) |
| -5 | Quito | +4 | Russia(Samara) |
| -4:30 | Venezuela(Caracas) | +4 | Abu Dhabi,Muscat |
| -4 | Canada(Halifax,Saint John) | +4 | Izhevsk,Samara(RTZ 3) |

| Time Zone | Time Zone Name | Time Zone | Time Zone Name |
|---|---|---|---|
| -4 | Atlantic Time (Canada) | +4 | Port Louis |
| -4 | Chile(Santiago) | +4:30 | Afghanistan(Kabul) |
| -4 | Paraguay(Asuncion) | +5 | Kazakhstan(Aqtobe) |
| -4 | United Kingdom-Bermuda(Bermuda) | +5 | Kyrgyzstan(Bishkek) |
| -4 | United Kingdom(Falkland Islands) | +5 | Pakistan(Islamabad) |
| -4 | Trinidad&Tobago | +5 | Russia(Chelyabinsk) |
| -4 | Manaus,Cuiaba | +5 | Ekaterinburg(RTZ 4) |
| -4 | Georgetown | +5 | Karachi |
| -4 | San Juan | +5 | Tashkent |
| -3:30 | Canada-New Foundland(St.Johns) | +5:30 | India(Calcutta) |
| -3 | Argentina(Buenos Aires) | +5:30 | Kolkata,New Delhi |
| -3 | Brazil(no DST) | +5:30 | Mumbai,Chennai |
| -3 | Brazil(DST) | +5:30 | Sri Jayawardenepura |
| -3 | Greenland(Nuuk) | +5:45 | Nepal(Katmandu) |
| -3 | Cayenne, Fortaieza | +6 | Kazakhstan(Astana, Almaty) |
| -3 | Brasilia | +6 | Russia(Novosibirsk,Omsk) |
| -3 | Montevideo | +6 | Bangladesh(Dhaka) |
| -3 | Salvador | +6:30 | Myanmar(Naypyitaw) |
| -2:30 | Newfoundland and Labrador | +6:30 | Yangon(Rangoon) |
| -2 | Brazil(no DST) | +7 | Russia(Krasnoyarsk) |
| -2 | Mid-Atlantic | +7 | Thailand(Bangkok) |
| -1 | Portugal(Azores) | +7 | Jakarta |
| -1 | Cape Verde Islands | +7 | Vletnam(Hanoi) |
| 0 | Denmark-Faroe Islands(Torshavn) | +8 | China(Beijing) |
| 0 | Ireland(Dublin) | +8 | Singapore(Singapore) |
| 0 | GMT | +8 | Australia(Perth) |
| 0 | Portugal(Lisboa,Porto,Funchal) | +8 | Russia(Irkutsk, Ulan-Ude) |
| 0 | Spain-Canary Islands(Las Palmas) | +8 | Hong Kong,Urumqi |
| 0 | United Kingdom(London) | +8 | Kuala Lumpur |
| 0 | Greenland | +8 | Taipei |

| Time Zone | Time Zone Name | Time Zone | Time Zone Name |
|---|---|---|---|
| 0 | Morocco | +8 | Ulaanbaatar |
| 0 | Edinburgh | +8:45 | Eucla |
| 0 | Casablanca | +9 | Korea(Seoul) |
| 0 | Lisbon | +9 | Japan(Tokyo) |
| 0 | Monrovia | +9 | Russia(Yakutsk,Chita) |
| 0 | Reykjavik | +9:30 | Australia(Adelaide) |
| 0 | Western Europe Time | +9:30 | Australia(Darwin) |
| +1 | Albania(Tirane) | +10 | Australia(Sydney,Melbourne,Canberra) |
| +1 | Austria(Vienna) | +10 | Australia(Brisbane) |
| +1 | Belgium(Brussels) | +10 | Australia(Hobart) |
| +1 | Caicos | +10 | Russia(Vladivostok) |
| +1 | Croatia(Zagreb) | +10 | Magadan(RTZ 9) |
| +1 | Czech Republic(Prague) | +10 | Solomon Islands |
| +1 | Denmark(Kopenhagen) | +10 | Guam,Port Moresby |
| +1 | France(Paris) | +10:30 | Australia(Lord Howe Islands) |
| +1 | Germany(Berlin) | +11 | New Caledonia(Noumea) |
| +1 | Hungary(Budapest) | +11 | Russia(Srednekolymsk Time) |
| +1 | Italy(Rome) | +11 | Chokurdakh(RTZ 10) |
| +1 | Spain(Madrid) | +11:30 | Norfolk Island |
| +1 | Belgrade | +12 | New Zealand(Wellington,Auckland) |
| +1 | Bratislava | +12 | Russia(Kamchatka Time) |
| +1 | Chad | +12 | Anadyr |
| +1 | Copenhagen | +12 | Fiji Islands |
| +1 | Ljublijana | +12 | Marshall Islands |
| +1 | Poland(Warsaw) | +12 | Petropavlovsk-Kamchatsky(RTZ 11) |
| +1 | Sweden(Stockholm) | +12:45 | New Zealand(Chatham Islands) |
| +1 | Switzeriland(Bern) | +13 | Tonga(Nukualofa) |
| +1 | West Central Africa | +13 | Nuku'alofa |
| +1 | Luxembourg(Luxembourg) | +13:30 | Chatham Islands |
| +1 | Macedonia(Skopje) | +14 | Kiribati |
| +1 | Netherlands(Amsterdam) | | |

# 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

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)<br>**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.<br>**Note**: It is only available to offset from Greenwich Mean Time GMT 0. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Web UI** | Settings->Time&Date->DHCP Time | |
| **Phone UI** | Settings->Basic Settings->Time&Date->DHCP Time->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 | |
| **Phone UI** | Settings->Basic Settings->Time&Date->General->Type (SNTP Settings) ->NTP Server1 | |
| **Parameter** | local_time.ntp_server2 | \<y0000000000xx>.cfg |
| **Description** | It configures the IP address or the domain name of the secondary NTP server.<br>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 | |
|---|---|---|
| **Phone UI** | Settings->Settings->Time&Date->General->Type (SNTP Settings) ->NTP Server2 | |
| **Parameter** | local_time.interval | &lt;y0000000000xx&gt;.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 | &lt;y0000000000xx&gt;.cfg |
| **Description** | It configures the time zone. | |
| **Permitted Values** | -12 to +14<br><br>For available time zones, refer to Time Zone. | |
| **Default** | +8 | |
| **Web UI** | Settings->Time&Date->Time Zone | |
| **Phone UI** | Settings->Basic Settings->Time&Date->General->Type (SNTP Settings) ->Time Zone | |
| **Parameter** | local_time.time_zone_name | &lt;y0000000000xx&gt;.cfg |
| **Description** | It configures the time zone name.<br><br>**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<br><br>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 | |
| **Phone UI** | Settings->Basic Settings->Time&Date->General->Type (SNTP Settings) ->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<br><br>**0**: DST by Date<br><br>**1**: DST by Week | DST time type<br><br>(This item is needed if you want to configure DST.) |
| szStart | optional | Month/Day/Hour (for iType=0)<br><br>Month: 1~12<br><br>Day: 1~31<br><br>Hour: 0 (midnight)~23<br><br>Month/Week of Month/Day of Week/Hour of Day (for iType=1)<br><br>Month: 1~12<br><br>Week of Month: 1~5 (the last week)<br><br>Day of Week: 1~7<br><br>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://sup-port.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"/>

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)".



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<br><br>**1**-Enabled<br><br>**2**-Automatic | |
| Default | 2 | |
| Web UI | Settings->Time&Date->Daylight Saving Time | |
| Phone UI | Settings->Basic Settings->Time&Date->General->Type (SNTP Settings) ->Daylight Saving | |
| Parameter | local_time.dst_time_type | <y0000000000xx>.cfg |
| Description | It configures the Daylight Saving Time (DST) type.<br><br>**Note**: It works only if "local_time.summer_time" is set to 1 (Enabled). | |
| Permitted Values | **0**-DST by Date<br><br>**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).<br><br>**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:<br><br>**Month**: 1=January, 2=February,..., 12=December | |

211

| | |
|---|---|
| | **Day**: 1=the first day in a month,..., 31= the last day in a month |
| | **Hour**: 0=0am, 1=1am,..., 23=11pm |
| | Month/Week of Month/Day of Week/Hour of Day-DST by Week, use the following mapping: |
| | **Month**: 1=January, 2=February,..., 12=December |
| | **Week of Month**: 1=the first week in a month,..., 5=the last week in a month |
| | **Day of Week**: 1=Monday, 2=Tuesday,..., 7=Sunday |
| | **Hour of Day**: 0=0am, 1=1am,..., 23=11pm |
| **Default** | 1/1/0 |
| **Web UI** | Settings->Time&Date->Start Date |
| **Parameter** | local_time.end_time      <y0000000000xx>.cfg |
| **Description** | It configures the end time of the Daylight Saving Time (DST).<br>**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:<br>**Month**: 1=January, 2=February,..., 12=December<br>**Day**: 1=the first day in a month,..., 31= the last day in a month<br>**Hour**: 0=0am, 1=1am,..., 23=11pm<br>Month/Week of Month/Day of Week/Hour of Day-DST by Week, use the following mapping:<br>**Month**: 1=January, 2=February,..., 12=December<br>**Week of Month**: 1=the first week in a month,..., 5=the last week in a month<br>**Day of Week**: 1=Monday, 2=Tuesday,..., 7=Sunday<br>**Hour of Day**: 0=0am, 1=1am,..., 23=11pm |
| **Default** | 12/31/23 |
| **Web UI** | Settings->Time&Date->End Date |
| **Parameter** | local_time.offset_time      <y0000000000xx>.cfg |
| **Description** | It configures the offset time (in minutes) of Daylight Saving Time (DST).<br>**Note**: It works only if "local_time.summer_time" is set to 1 (Enabled). |
| **Permitted Values** | Integer from -300 to 300 |
| **Default** | Blank |
| **Web UI** | Settings->Time&Date->Offset(minutes) |
| **Parameter** | auto_dst.url      <y0000000000xx>.cfg |
| **Description** | It configures the access URL of the DST file (AutoDST.xml).<br>**Note**: It works only if "local_time.summer_time" is set to 2 (Automatic). |
| **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.<br>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 | local_time.time_format | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the time format. | |
| Permitted Values | 0-Hour 12, the time will be displayed in 12-hour format with AM or PM specified.<br>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 | |
| Phone UI | Settings->Basic Settings->Time&Date->Time & Date Format->Time Format | |
| Parameter | local_time.date_format | <y0000000000xx>.cfg |
| Description | It configures the date format. | |
| Permitted Values | 0-WWW MMM DD<br>1-DD-MMM-YY<br>2-YYYY-MM-DD<br>3-DD/MM/YYYY<br>4-MM/DD/YY<br>5-DD MMM YYYY<br>6-WWW DD MMM<br>Use the following mapping:<br>"WWW" represents the abbreviation of the week; | |

| | |
|---|---|
| | "DD" represents a two-digit day; |
| | "MMM" represents the first three letters of the month; |
| | "YYYY" represents a four-digit year, and "YY" represents a two-digit year. |
| **Default** | 0 |
| **Web UI** | Settings->Time&Date->Date Format |
| **Phone UI** | Settings->Basic Settings->Time&Date->Time & Date Format->Date Format |

## Date Customization Rule

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

| Format | Description |
|---|---|
| Y/YY | It represents a two-digit year.<br><br>For example, 16, 17, 18... |
| Y is used more than twice (for example, YYY, YYYY) | It represents a four-digit year.<br><br>For example, 2016, 2017, 2018... |
| M/MM | It represents a two-digit month.<br><br>For example, 01, 02,..., 12 |
| MMM | It represents the abbreviation of the month.<br><br>For example, Jan, Feb,..., Dec |
| M is used more than three times (for example, MMMM) | It represents the long format of the month.<br><br>For example, January, February,..., December |
| D is used once or more than once (for example, DD) | It represents a two-digit day.<br><br>For example, 01, 02,..., 31 |
| W/WW | It represents the abbreviation of the day of week.<br><br>For example, Mon, Tue,..., Sun |
| W is used more than twice (for example, WWW, WWWW) | It represents the long format of the day of week.<br><br>For example, Monday, Tuesday,..., Sunday |

## Call Display

By default, the phones present the contact information (including avatar and identity) when receiving an incoming call, dialing an outgoing call or engaging in a call.
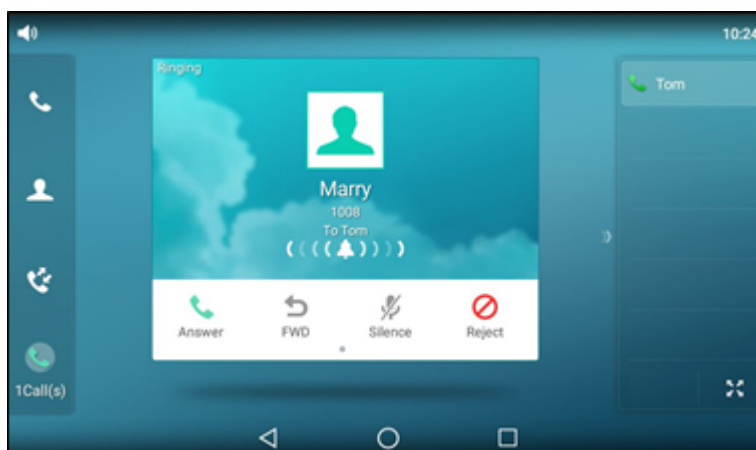
You can configure what contact information presents and how to display the contact information. If the contact exists in the phone directory, the phone displays the saved contact name and number. If not, it will use Calling Line Identification Presentation (CLIP) or Connected Line Identification Presentation (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 | account.X.picture_info_enable[1] | <MAC>.cfg |
|---|---|---|
| Description | It enables or disables the phone to download the picture from the URL contained in the Call-Info or Caller-Image header of INVITE message. | |
| Permitted Values | 0-Disabled<br>1-Enabled | |
| Default | 0 | |
| 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.<br>**Note**: The information display method is configured by the parameter "phone_setting.call_info_display_method". | |
| Permitted Values | 0-Disabled<br>1-Enabled | |
| Default | 0 | |
| 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<br>1-Number+Name<br>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<br>**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<br>**1**-Enabled |
| **Default** | 0 |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

[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.
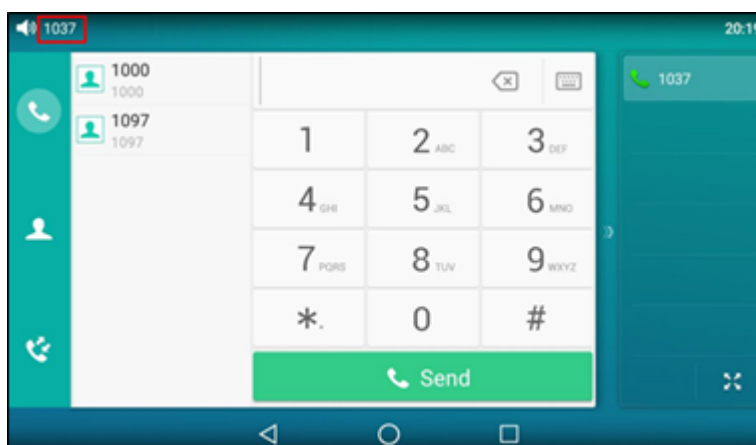


Yealink phones support three display methods: Label, Display Name and User Name. You can customize the account information to be displayed on the IP phone as required.

## 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.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **1**-Label, configured by the parameter "account.X.label".<br><br>**2**-Display Name, configured by the parameter "account.X.display_name".<br><br>**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.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled, neither "#" nor "*" can be used as the send key.<br><br>**1**-# key<br><br>**2**-* key | |
| Default | 1 | |
| Web UI | Features->General Information->Key As Send | |
| Phone UI | Settings->Features->Key As Send->Key As Send | |
| Parameter | features.send_pound_key | <y0000000000xx>.cfg |
| Description | It configures the behavior when the user presses the # key twice on the dialing screen.<br><br>**Note**: It works only if "features.key_as_send" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| Permitted Values | **0**-The phone will dial out "#".<br><br>**1**-The phone will not dial out "#". After the user presses the # key again, the phone will dial out "##". | |
| Default | 0 | |
| Web UI | Features->General Information->Send Pound Key | |

# Softkey Layout

Softkey layout is used to customize the soft keys at the bottom of the phone screen for best meet users' requirements. In addition to specifying which soft keys to display, you can determine their display order. The configurations for softkey layout are based on call states.

It is not applicable to CP960 phones.

The following shows the soft keys displaying on the phone in the CallIn state:
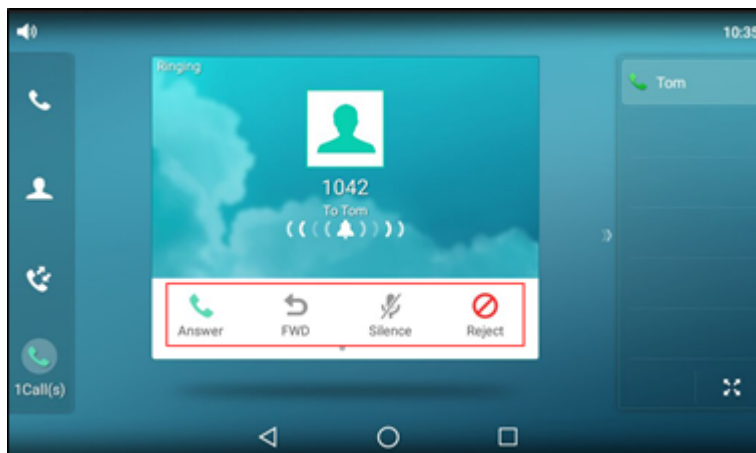


> **Note**
>
> You can configure the EDK soft keys in different call states. Configuring the EDK soft keys may affect the softkey layout in different call states. For more information on EDK soft keys, refer to EDK Soft Keys Configuration.

## Topics

Supported Call States and Soft Keys
Softkey Layout File Customization
Softkey Layout Configuration
Example: Setting the Soft Keys Layout in Talking State

## Supported Call States and Soft Keys

The following table lists soft keys available for phones in different call states.

| Call States | Enabled Soft Keys | Disabled Soft Keys |
|---|---|---|
| CallFailed (Call Fail) | NewCall | Switch<br>End Call |
| CallIn (Incoming Call) | Answer<br><br>Forward<br><br>Silence<br><br>Reject | Empty<br><br>Switch<br><br>Decline<br><br>Video<br><br>Audio |

| Call States | | Enabled Soft Keys | Disabled Soft Keys |
|---|---|---|---|
| Connecting | Connecting | End Call | Switch |
| | SemiAttendTrans (Transfer Connecting) | Transfer<br>End Call | Switch |
| RingBack | RingBack (Ring Back) | Cancel | Switch |
| | SemiAttendTransBack (Transfer Ring Back) | Transfer<br>Cancel | Switch |
| Talking | Talk (On Talk/Talking) | Transfer<br><br>Hold<br><br>Conference<br><br>End Call | Mute<br><br>SWAP<br><br>NewCall<br><br>Switch<br><br>PriHold<br><br>Park<br><br>GPark<br><br>RTP Status<br><br>Record<br><br>Security<br><br>Add Video<br><br>Audio Only |
| | Hold | Transfer<br><br>Resume<br><br>NewCall<br><br>End Call | Switch<br><br>Record<br><br>Security |
| | Held | Hold<br><br>End Call | Switch<br><br>NewCall<br><br>Record<br><br>Security |
| | Conferenced | Split<br><br>Hold<br><br>Conference<br><br>End Call | Switch<br><br>Mute<br><br>RTP Status<br><br>Record<br><br>Security |

## Softkey Layout File Customization

You can also configure the softkey layout using the softkey layout templates for different call states.

You can ask the distributor or Yealink FAE for softkey layout template. You can also obtain the softkey layout template online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage.

## Topics

## Softkey Layout File Elements and Attributes

The following table lists the elements and attributes you need to understand in the softkey layout file. We recommend you do not edit these elements and attributes.

| Elements & Attributes | Description |
|---|---|
| <Disable> | Specify the disabled soft key list. |
| </Disable> | The phone screen will not display the disabled soft keys. |
| <Enable> | Specify the enabled soft key list. |
| </Enable> | The phone screen will display the enabled soft keys. |
| <Default> | Specify the default soft key list. |
| </Default> | The phone screen displays these soft keys by default. |
| <Key Type=" "/> | Specify the soft key type. |

## Customizing Softkey Layout File

1. Open the template file.
2. For each soft key that you want to enable, move the string from the disabled soft key list to enabled soft key list in the file or replace the Empty in the enabled soft key list. The **More** soft key appears when more than 4 soft keys are enabled.

   The following shows a portion of the softkey layout file "CallFailed.xml":
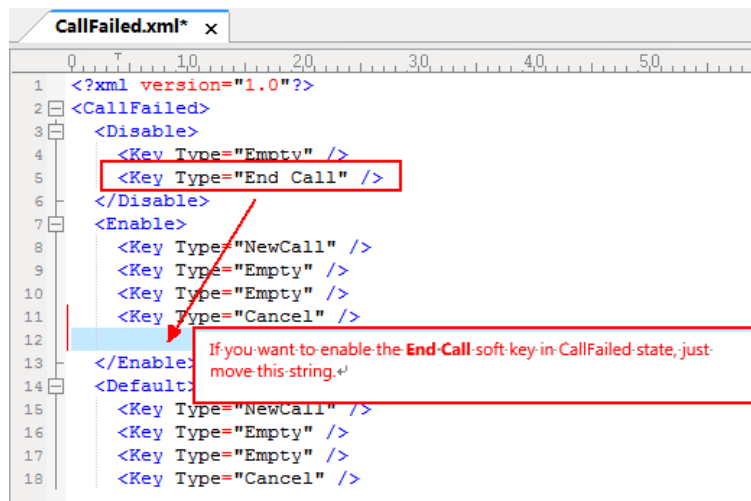


3. For each soft key that you want to disable, just move the string from the enabled soft key list to disabled soft key list.

   The following shows a portion of the softkey layout file "CallFailed.xml":
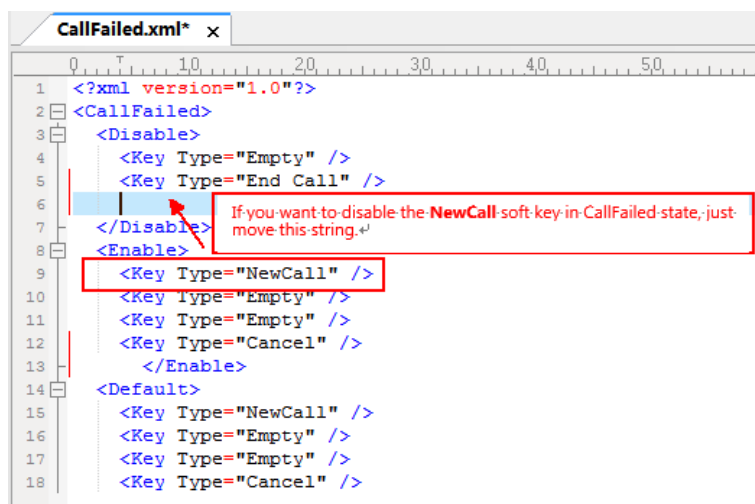
**4.** Save the change and place this file to the provisioning server.

## Softkey Layout Configuration

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

| Parameter | phone_setting.custom_softkey_enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the custom soft keys layout feature.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Settings->Softkey Layout->Custom SoftKey | |
| Parameter | custom_softkey_call_failed.url | <y0000000000xx>.cfg |
| Description | It configures the access URL of the custom softkey layout file in the CallFailed state.<br>**Note**: It works only if "phone_setting.custom_softkey_enable" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |
| Parameter | custom_softkey_call_in.url | <y0000000000xx>.cfg |
| Description | It configures the access URL of the custom softkey layout file in the CallIn state.<br>**Note**: It works only if "phone_setting.custom_softkey_enable" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |
| Parameter | custom_softkey_connecting.url | <y0000000000xx>.cfg |
| Description | It configures the access URL of the custom softkey layout file in the Connecting state. | |

| | |
|---|---|
| | **Note**: It works only if "phone_setting.custom_softkey_enable" is set to 1 (Enabled). It is not applicable to CP960 phones. |
| **Permitted Values** | URL within 511 characters |
| **Default** | Blank |

| **Parameter** | custom_softkey_ring_back.url | <y0000000000xx>.cfg |
|---|---|---|

| | |
|---|---|
| **Description** | It configures the access URL of the custom softkey layout file in the RingBack state. **Note**: It works only if "phone_setting.custom_softkey_enable" is set to 1 (Enabled). It is not applicable to CP960 phones. |
| **Permitted Values** | URL within 511 characters |
| **Default** | Blank |

| **Parameter** | custom_softkey_talking.url | <y0000000000xx>.cfg |
|---|---|---|

| | |
|---|---|
| **Description** | It configures the access URL of the custom softkey layout file in the Talking state. **Note**: It works only if "phone_setting.custom_softkey_enable" is set to 1 (Enabled). It is not applicable to CP960 phones. |
| **Permitted Values** | URL within 511 characters |
| **Default** | Blank |

## Example: Setting the Soft Keys Layout in Talking State

The following example shows the configuration for setting the soft key layout in the talking state. It is not applicable to CP960 phones.

Customize a softkey layout file "Talking.xml" and place this file to the provisioning server "http://192.168.10.25".

**Example**

*phone_setting.custom_softkey_enable = 1*

*custom_softkey_talking.url = http://192.168.10.25/Talking.xml*

After provisioning, you can use the enabled soft keys during a call.

## Notification Popups

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

The following shows an example of missing a call:

Pop-up message box
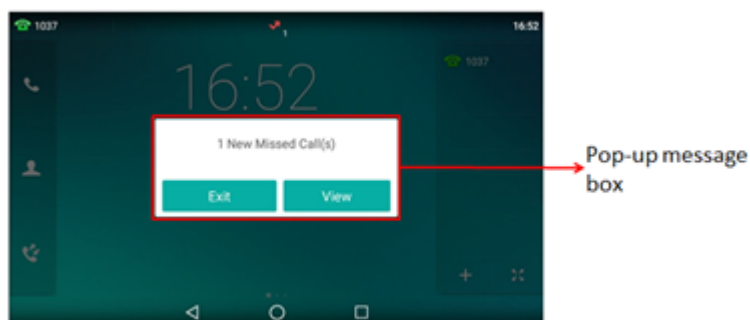
## Topic

## Notification Popups Configuration

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

| Parameter | features.voice_mail_popup.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to pop up the message when it receives a new voice mail.<br><br>If the message disappears, it will not pop up again unless the phone receives a new voice mail or the user re-registers the account that has unread voice mail(s).<br><br>**Note**: It works only if "account.X.display_mwi.enable" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Web UI | Features->Notification Popups->Display Voice Mail Popup | |

| Parameter | features.missed_call_popup.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to pop up the message when it misses a call.<br><br>**Note**: It works only if "account.X.missed_calllog" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Web UI | Features->Notification Popups->Display Missed Call Popup | |

| Parameter | features.forward_call_popup.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to pop up the message when it forwards an incoming call to another party. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Web UI | Features->Notification Popups->Display Forward Call Popup | |

# Power/Mute LED Indicator

Power LED indicator indicates power status and phone status of VP59/T58A. The mute LED indicator indicates phone status for CP960.

You can configure the power LED indicator behavior for VP59/T58A in the following scenarios:

- The IP phone receives an incoming call
- The IP phone receives a voice mail
- A call is muted
- A call is placed on hold or is held
- The IP phone is busy
- The IP phone misses a call

When a call is placed on hold or held, you can configure the mute LED indicator behavior for CP960.

## Topic

Power/Mute LED Indicator Configuration

## Power/Mute LED Indicator Configuration

The following table lists the parameters you can use to configure power/mute LED indicator.

| Parameter | phone_setting.common_power_led_enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the power LED indicator to be turned on.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled (power LED indicator is off)<br><br>**1**-Enabled (power LED indicator glows 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 power LED indicator to flash when the phone receives an incoming call.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled (power LED indicator does not flash)<br><br>**1**-Enabled (power LED indicator fast flashes (0.3s) red) | |
| Default | 1 | |
| Web UI | Features->Power LED->Ringing Power Light Flash | |
| Parameter | phone_setting.mail_power_led_flash_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the power LED indicator to flash when the phone receives a voice mail.<br><br>**Note**: It works only if "account.X.display_mwi.enable" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled (power LED indicator does not flash)<br><br>**1**-Enabled (power LED indicator slowly flashes (1s) red) | |
| Default | 1 | |

| Web UI | Features->Power LED->Voice/Text Mail Power Light Flash | |
|---|---|---|
| **Parameter** | phone_setting.mute_power_led_flash_enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the power LED indicator to flash when a call is muted.<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled (power LED indicator does not flash)<br><br>**1**-Enabled (power LED indicator fast flashes (0.3s) red) | |
| **Default** | 0 | |
| **Web UI** | Features->Power LED->Mute Power Light Flash | |
| **Parameter** | phone_setting.hold_and_held_power_led_flash_enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the power LED indicator (for VP59/T58A)/mute LED indicator (for CP960) to flash when a call is placed on hold or is held.<br><br>**Note**: For CP960, it works only if the phone is not in the mute state. | |
| **Permitted Values** | **0**-Disabled (power LED indicator/mute LED indicator does not flash)<br><br>**1**-Enabled ( power LED indicator/mute LED indicator fast flashes (0.5s) red) | |
| **Default** | 0 | |
| **Web UI** | Features->Power LED->Hold/Held Power Light Flash (not for CP960) | |
| **Parameter** | phone_setting.talk_and_dial_power_led_enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the power LED indicator to be turned on when the phone is busy.<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled (power LED indicator is off)<br><br>**1**-Enabled (power LED indicator glows red) | |
| **Default** | 0 | |
| **Web UI** | Features->Power LED->Talk/Dial Power Light On | |
| **Parameter** | phone_setting.missed_call_power_led_flash.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the power LED indicator to flash when the phone misses a call.<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled (power LED indicator does not flash)<br><br>**1**-Enabled (power LED indicator slowly flashes (1s) red) | |
| **Default** | 1 | |
| **Web UI** | Features->Power LED->MissCall Power Light Flash | |

# Bluetooth

You can pair and connect the Bluetooth-enable mobile phone with your phone, and make and receive mobile calls on the IP phone. After connecting the Bluetooth-enabled mobile phone, you can choose to synchronize the mobile contacts to the IP phone. It is only applicable to VP59/T58A phones.

For CP960 phones, you can also use your IP phone as a Bluetooth speaker for your mobile phone and set up a conference among the calls on your IP phone, the PC and connected mobile phone.

For VP59/T58A phones, you can also connect the other Bluetooth devices (for example, Bluetooth headset) with your phone. And you can transfer files via Bluetooth, sharing images/videos with other Bluetooth devices.

## Topic

## Bluetooth Configuration

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

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. <br> **1**-Enabled | |
| **Default** | 1 | |
| **Parameter** | features.bluetooth_enable | <y0000000000xx>.cfg |
| **Description** | It triggers the Bluetooth mode to on or off. <br> **Note**: It works only if "static.bluetooth.function.enable" is set to 1 (Enabled). | |
| **Permitted Values** | **0**-Off <br> **1**-On | |
| **Default** | 0 | |
| **Web UI** | Features->Bluetooth->Bluetooth Active | |
| **Phone UI** | Settings->Basic Settings->Bluetooth->Bluetooth | |
| **Parameter** | features.bluetooth_adapter_name | <y0000000000xx>.cfg |
| **Description** | It configures the Bluetooth device name. <br> **Note**: It works only if "features.bluetooth_enable" is set to 1 (On). | |
| **Permitted Values** | String within 64 characters | |
| **Default** | For VP59 phones: VP59. <br> For T58A phones: Yealink-T58. <br> For CP960 phones: Yealink-CP960. | |
| **Phone UI** | Settings->Basic Settings->Bluetooth->Bluetooth (On) ->Edit My Device Information->Device Name | |
| **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. | |

| | |
|---|---|
| | **Note**: It is only applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled, the prompt will not appear during the call. After the call, users can tap the request notification message from the notification center, and then select to accept or reject the connection request. |
| **Default** | 0 |
| **Parameter** | bluetooth.a2dp_sink[1] | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to act as the connected Bluetooth-enabled mobile phone player.<br><br>**Note**: It is only applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled, the Media audio item is hidden on the connected Bluetooth-enabled mobile phone.<br><br>**1**-Enabled, you need to enable the Media audio feature manually after the Bluetooth-enabled mobile phone is paired and connected. Enable the Media audio feature via phone user interface at the path:<br><br>**Bluetooth**->**Bluetooth (On)**-> ⁚ ->**Media audio**.<br><br>**2**-Enabled, the phone automatically acts as the Bluetooth-enabled mobile phone player after you pair and connect the Bluetooth-enabled mobile phone to the phone successfully. |
| **Default** | 1 |

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

# Handset/Headset/Speakerphone Mode

The VP59/T58A phones support three ways to place/answer a call: using the handset, using the headset or using the speakerphone.

It is not applicable to CP960 phones.

## Topic

Handset/Headset/Speakerphone Mode Configuration

## Handset/Headset/Speakerphone Mode Configuration

The following table lists the parameters you can use to configure handset/headset/speakerphone mode.

| | | |
|---|---|---|
| **Parameter** | features.group_listen_in_talking_enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to enter into the group listening mode by pressing the Speakerphone key when you first answer the call using the handset.<br><br>**Note**: The audio is sent only through the handset. So you are able to speak and listen through the handset, but you can only listen through the speaker. It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 1 | |
| **Parameter** | phone_setting.headsetkey_mode | <y0000000000xx>.cfg |
| **Description** | It configures headset mode during a call.<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted** | **0**-Always use (pressing the Speakerphone key and picking up the handset are not effective when the | |

| Values | headset mode is activated) |
| --- | --- |
| | **1**-Use as normal |
| **Default** | 1 |

# DSS Keys

There are four kinds of DSS keys: Line Keys, Programmable Keys, Ext Keys and Shortcut Keys. You can assign various functions to DSS keys. This section explains how to set these keys.

Ext key is only applicable to expansion modules connected to T58A phones. Shortcut Keys is only applicable to CP960 phones.

## Topics

Supported DSS Keys
Supported Dsskey Types
Shortcut Key/Programmable Key Icons Limit
Line Keys
Programmable Keys
Shortcut Keys
Ext Keys
Shortcut Key/Programmable Key Icons Customization

## Supported DSS Keys

The following table lists the number of DSS keys you can configure for each phone model:

| Phone Model | Line Keys | Programmable Keys | Ext Keys | Shortcut Keys |
| --- | --- | --- | --- | --- |
| CP960 | 30 | 3 | / | 6 |
| T58A | 27 | 7 | 60 | / |
| VP59 | 27 | 8 | / | / |

## Supported Dsskey Types

The supported Dsskey function types vary by line keys, programmable keys, ext keys and shortcut keys.

| ID | DSS Key Types | ID | DSS Key Types | ID | DSS Key Types |
| --- | --- | --- | --- | --- | --- |
| 0 | N/A | 22 | XML Group | 51 | Switch Account Up (Programmable key) |
| 1 | Conference (Line key/Ext key) | 23 | Group Pickup | 52 | Switch Account Down (Programmable key) |
| 2 | Forward | 24 | Paging(Multicast Paging) (Line key/Ext key) | 56 | Retrieve Park (Line key/Ext key) |
| 3 | Transfer (Line key/Ext key) | 25 | Record (Line key/Ext key) | 61 | Directory |
| 4 | Hold (Line key/Ext key) | 27 | XML Browser | 66 | Paging List |
| 5 | DND | 28 | History (Programmable key) | 72 | Missed Call |

| ID | DSS Key Types | ID | DSS Key Types | ID | DSS Key Types |
|---|---|---|---|---|---|
| 7 | ReCall | 29 | Directory (Programmable key) | 73 | Custom Key (only appear when "features.enhanced_dss_keys.enable = 1") |
| 9 | Pickup(Pick up/ Direct Pickup) | 30 | Menu (Programmable key) | 77 | Mobile Line (only applicable when the Bluetooth-enabled mobile phone is connected) |
| 10 | Call Park (Line key/Ext key) | 33 | Status (Programmable key) | 85 | Favorite (Local Favorite) |
| 11 | DTMF (Line key/Ext key) | 34 | Hot Desking | 304 | Open Door |
| 12 | Voice Mail (Line key/Ext key) | 35 | URL Record (Line key/Ext key) | 305 | Video Monitoring |
| 13 | Speed Dial(SpeedDial) | 38 | LDAP(only appear when "ldap.enable=1") | 306 | Custom |
| 14 | Intercom | 39 | BLF List | 308 | Dial (Programmable key/Shortcut key) |
| 15 | Line (Line key/Ext key) | 40 | Prefix | 309 | Bluetooth (Programmable key/Shortcut key) |
| 16 | BLF (Line key/Ext key) | 41 | Zero Touch | 310 | Dect Intercom (Line key) |
| 17 | URL (Line key/Ext key) | 42 | ACD (Line key/Ext key) | | |
| 18 | Group Listening (Line key/Ext key) | 45 | Local Group | | |
| 20 | Private Hold | 50 | Phone Lock (Line key/Ext key) | | |

## Shortcut Key/Programmable Key Icons Limit

The shortcut key/programmable key icon format must meet the following:

| Phone Model | Format | Resolution |
|---|---|---|
| VP59/T58A/CP960 | .png | <=130*130 pixels |

**Note**

We recommend you use a mixture of letters and characters for the icon names.

## Line Keys

Line keys provide one-touch feature (for example, one-touch park). This allows you to quickly access features and to view the monitored status when the line keys are assigned with particular features (for example, BLF).

## Topics

Line Keys Configuration

Example: Set a Park/Retrieve Key for FAC Call Park Mode
Example: Set a Park/Retrieve Key for Transfer Call Park Mode
Example: Setting a Line Key as Directed Pickup key
Example: Setting a Line Key as Group Pickup key
Example: Setting a Line Key as BLF List key
Example: Setting a Line Key as Private Hold key
Example: Setting a Line Key as Multicast Paging key
Example: Setting a Line Key as Open Door Key
Example: Setting a Line Key as Video Monitoring Key

## Line Keys Configuration

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

| Parameter | linekey.X.type[1] | | <y0000000000xx>.cfg |
|---|---|---|---|
| **Description** | It configures the key feature. | | |
| **Permitted Values** | **0**-N/A<br>**1**-Conference (not applicable to CP960 phones)<br>**2**-Forward<br>**3**-Transfer  (not applicable to CP960 phones)<br>**4**-Hold<br>**5**-DND<br>**7**-Recall<br>**9**-Pickup(pick up/Direct Pickup)<br>**10**-Call Park<br>**11**-DTMF<br>**12**-Voice Mail<br>**13**-SpeedDial(Speed Dial)<br>**14**-Intercom | **15**-Line<br>**16**-BLF<br>**17**-URL<br>**18**-Group Listening<br>**20**-Private Hold<br>**22**-XML Group<br>**23**-Group Pickup<br>**24**-Paging(Multicast Paging)<br>**25**-Record<br>**27**-XML Browser<br>**34**-Hot Desking<br>**35**-URL Record | **38**-LDAP (only appear when "ldap.enable=1")<br>**39**-BLF List<br>**40**-Prefix<br>**41**-Zero Touch<br>**42**-ACD (not applicable to CP960 phones)<br>**45**-Local Group<br>**50**-Phone Lock<br>**56**-Retrieve Park<br>**61**-Directory<br>**66**-Paging List<br>**72**-Missed Call (not applicable to CP960 phones)<br>**73**-Custom Key (only available when "features.enhanced_dss_keys.enable=1") (not applicable to CP960 phones)<br>**77**-Mobile Account<br>**304**-Open Door (not applicable to CP960 phones)<br>**305**-Video Monitoring  (not applicable to CP960 phones)<br>**306**-Custom<br>**310**-Dect Intercom (not applicable to CP960 phones) |
| **Default** | 15 | | VP59/T58A: X= 1-16 |

| | | CP960: Line key 1 |
|---|---|---|
| | 0 | other line keys |
| **Web UI** | Dsskey->Line Key->Line KeyX->Type | |
| **Phone UI** | Menu->Features->DSS Keys->Line Key X->Type | |
| **Parameter** | linekey.X.line[1] | <y0000000000xx>.cfg |
| **Description** | It configures the desired line to apply the line key feature. **Note**: You do not need to configure this parameter when "linekey.X.type" is set to 1, 2, 3, 4, 5, 6, 7, 9, 11, 17, 18, 20, 22, 24, 25, 27, 34, 35, 38, 39, 40, 41, 42, 45, 50, 61, 66 , 73, 77, 84 or 85". | |
| **Permitted Values** | VP59/T58A: 1-16 (if linekey.X.type = 310, 1-4 stand for Handset 2-Handset 5) CP960: 1 | |
| **Default** | 1 | |
| **Web UI** | Dsskey->Line Key->Line KeyX->Line | |
| **Phone UI** | Settings->Features->Dsskey->Line Key X->Account ID | |
| **Parameter** | linekey.X.value[1] | <y0000000000xx>.cfg |
| **Description** | It configures the value for some line key features. For example, when you assign the Speed Dial to the line key, this parameter is used to specify the contact number you want to dial out. For open door feature: It configures the open door URL of 2N IP intercom. The valid URL format is: http(s) ://<IP address of the IP intercom>/api/switch/ctrl?switch=<switch identifier, typically 1 to 4>&action=trigger or http(s)://username:password@<IP address of the IP intercom>/api/switch/ctrl?switch=<switch identifier, typically 1 to 4>&action=trigger. For video monitoring feature: It configures the video access URL of IP intercom camera. The valid URL format is: http(s)://<IP address of the IP intercom>/mjpg/video.mjpg or http(s)://username:password@<IP address of the IP intercom>/mjpg/video.mjpg. **Note**: You do not need to configure this parameter when "linekey.X.type" is set to 4, 5, 7, 8, 18, 20, 22, 25, 34, 38, 39, 41, 42, 45, 50, 61 or 66. | |
| **Permitted Values** | String within 99 characters | |
| **Default** | Blank | |
| **Web UI** | Dsskey->Line Key->Line KeyX->Value | |
| **Phone UI** | Settings->Features->Dsskey->Line Key X->Value | |
| **Parameter** | linekey.X.label[1] | <y0000000000xx>.cfg |
| **Description** | It configures the label displayed on the phone screen. This is an optional configuration. | |

| Permitted Values | String within 99 characters | |
|---|---|---|
| **Default** | Blank | |
| **Web UI** | Dsskey->Line Key->Line KeyX->Label | |
| **Phone UI** | Settings->Features->Dsskey->Line Key X->Label | |
| **Parameter** | linekey.X.extension[1] | <y0000000000xx>.cfg |
| **Description** | For multicast paging: It configures the channel of the multicast paging group. For BLF/BLF list/intercom feature: It configures the pickup code. For speed dial feature: It configures the key sequence you want to send via DTMF. For open door/video monitoring feature: It configures the number or IP address of the IP intercom that this key will apply to. **Note**: It is only applicable when "linekey.X.type" is set to 13, 14, 16, 24 or 39. | |
| **Permitted Values** | For multicast paging: 0 to 31 For BLF/BLF list/intercom/open door/video monitoring feature: String within 256 characters For speed dial feature: String | |
| **Default** | Blank | |
| **Web UI** | Dsskey->Line Key->Line KeyX->Extension | |
| **Phone UI** | Settings->Features->Dsskey->Line Key X->Extension | |
| **Parameter** | linekey.X.xml_phonebook[1] | <y0000000000xx>.cfg |
| **Description** | It specifies a specific group/phone book when multiple groups/phone books are configured on the phone. For example, both Remote Phone Book 1 "Sell" and Remote Phone Book 2 "Market" are configured on the phone, you can configure "linekey.X.xml_phonebook = 0" to specify the Remote Phone Book 1 "Sell" for the specific line key. The user can press this line key to access the Remote Phone Book 1 "Sell". **Note**: It is only applicable when "linekey.X.type" is set to 22 or 45. | |
| **Permitted Values** | Integer from 0 to 48 | |
| **Default** | 0 | |
| **Web UI** | Dsskey->Line Key->Line KeyX->Line | |

| Parameter | features.flash_url_dsskey_led.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the LED indicator of the URL DSS key.<br><br>The LED indicator behavior depends on the response message from the server when you press the URL DSS key on the phone.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled | |
| Default | 1 | |

[1]X is the line key ID. X=1-27.

## Example: Set a Park/Retrieve Key for FAC Call Park Mode

| Scenario Conditions | Related Topic |
|---|---|
| features.call_park.park_code = *68 | |
| features.call_park.park_retrieve_code = *88 | Call Park and Retrieve |
| features.call_park.park_mode = 1 | |

**Example**

######Set a Park key######

linekey.1.type = 10

linekey.1.value =4603

linekey.1.label =Bill

######Set a Retrieve key####

linekey.3.type = 56

linekey.3.line =1

linekey.3.value =4603

linekey.3.label =Retrieve Bill

After provisioning, you can easily tap the Park key (line key 1) to park a call to a specific extension (4603) during a call, and tap the Retrieve key (line key 3) to retrieve the parked call from the specific extension (4603) when the phone is idle.

If the "linekey.1.value" is set to blank, the park key will perform as the **Park** soft key.

| Note |
|---|
| In FAC call park mode, the Park/Retrieve key invokes the call park code/park retrieve code by default. Therefore, the phone dials out *684603 to park a call, and dials out *884603 to retrieve a call. If these codes are not set, you can assign code and extension to "linekey.X.value", for example, "*684603". |

## Example: Set a Park/Retrieve Key for Transfer Call Park Mode

| Scenario Conditions | Related Topic |
|---|---|

| | |
|---|---|
| features.call_park.park_mode = 2 | Call Park and Retrieve |
| features.call_park.line_restriction.enable = 1 | |

**Example**

######Set a Park key######

linekey.1.type = 10

linekey.1.value =*01

linekey.1.line = 1

linekey.1.label =Bill

######Set a Retrieve key####

linekey.3.type = 56

linekey.3.line = 1

linekey.3.value =*11

linekey.3.label =Retrieve Bill

After provisioning, you can easily tap the Park key (line key 1) to park a call to the specific shared parking lot (*01) during a call, and tap the Retrieve key (line key 3) to retrieve the parked call from the shared parking lot (*01) using the retrieve code (*11). You can only perform call park feature on the specific line (line 1).

If the "features.call_park.line_restriction.enable" is set to 0 (Disabled), the phone will park/retrieve the call to the server on the current line in use.

| Note |
|---|
| In Transfer call park mode, if you press the Park key when the phone is idle, the Park key will invoke the call park code. Therefore, you can use a Park key to park and retrieve a call. In this case, you need to assign the park retrieve code (*11) to "features.call_park.park_code". When you tap the Park key again on idle screen, the phone will dial out "*11*01" to retrieve the parked call. |

## Example: Setting a Line Key as Directed Pickup key

| Scenario Conditions | Related Topic |
|---|---|
| account.1.direct_pickup_code = *97<br><br>or<br><br>features.pickup.direct_pickup_code = *97 | Directed Call Pickup |

**Example**

linekey.1.type = 9

linekey.1.line =1

linekey.1.value= 4603

linekey.1.label=Bill

After provisioning, you can easily tap the DPickup key (line key 1) to pick up an incoming call to a specific phone (4603).

**Note**

The DPickup invokes the directed pickup code by default. Therefore, the phone dials out *974603 to pick up a call. If the directed code is not set, you can assign code and extension to "linekey.X.value", for example, "*974603".

## Example: Setting a Line Key as Group Pickup key

The following example shows the configuration for a group pickup key.

**Example**

linekey.1.type = 23

linekey.1.line =1

linekey.1.value =*98

linekey.1.label =Sell

After provisioning, you can easily tap the GPickup key (line key 1) to pick up an incoming call to any phone within a predefined group of phones.

**Note**

If the "linekey.X.value" is not assigned with a group pickup code, the Park key will invoke the group pickup code set by "features.pickup.group_pickup_code" or "account.X.group_pickup_code".

## Example: Setting a Line Key as BLF List key

The following example shows the configuration for a BLF List key.

| Scenario Conditions | Related Topic |
|---|---|
| phone_setting.auto_blf_list_enable = 0 | BLF List Configuration |

**Example**

linekey.1.type = 39

linekey.1.line =1

After provisioning, a BLF List key displays on line key 1. You can easily use this key to monitor a remote line. The monitored line depends on a pre-configured SIP server.

## Example: Setting a Line Key as Private Hold key

The following example shows the configuration for a Private Hold key.

**Example**

linekey.1.type = 20

linekey.1.label =Private Hold

After provisioning, you can tap the line key 1 to hold calls without notifying other phones registered with the shared line, the shared line displays active to others shared line. It is only applicable to Shared Line Appearance.

## Example: Setting a Line Key as Multicast Paging key

The following example shows the configuration for a Multicast Paging key.

**Example**

linekey.1.type = 24

linekey.1.value = 224.5.6.20:10008

linekey.1.label = Sales

linekey.1.extension = 2

After provisioning, you can tap the line key 1 to send announcements quickly to the Sales group.

### Example: Setting a Line Key as Open Door Key

The following example shows the configuration for an open door key.

**Example**

linekey.1.type = 304

linekey.1.value = http://192.168.1.1/api/switch/ctrl?switch=1&action=trigger

linekey.1.label = Door Phone1

linekey.1.extension = 1048

After provision, you can tap the line key 1 to open the door at any time.

### Example: Setting a Line Key as Video Monitoring Key

The following example shows the configuration for an open door key.

**Example**

linekey.1.type = 305

linekey.1.value = http://192.168.1.1/mjpg/video.mjpg

linekey.1.label = Door Phone2

linekey.1.extension = 1048

After provision, you can tap the line key 1 to check the camera video at any time.

## Programmable Keys

You can customize programmable keys on the phone to enable users to access frequently used functions, or, if your phone does not have a particular hard key, you can create a soft key. For example, if the phone does not have a Do Not Disturb hard key, you can create a Do Not Disturb soft key.

The programmable key takes effect only when the IP phone is idle.

The following shows the custom soft keys displayed on the phone:

For CP960:

For VP59/T58A:
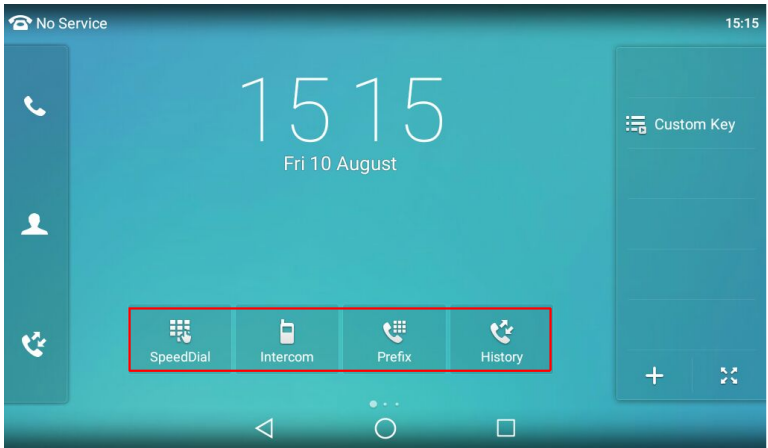


## Topics

## Supported Programmable Keys

The following tables list programmable keys for each phone model.

| Programmable Key IDs | VP59 | T58A | CP960 |
|---|---|---|---|
| 1 | SoftKey1 | SoftKey1 | SoftKey1 |
| 2 | SoftKey2 | SoftKey2 | SoftKey2 |
| 3 | SoftKey3 | SoftKey3 | SoftKey3 |

| Programmable Key IDs | VP59 | T58A | CP960 |
|:---:|:---:|:---:|:---:|
| 4 | SoftKey4 | SoftKey4 | / |
| 12 | HOLD | HOLD | / |
| 13 | MUTE | MUTE | / |
| 14 | TRAN | TRAN | / |
| 17 | Redial | / | / |

## Programmable Keys Configuration

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

| Parameter | programablekey.X.type[1] | | <y0000000000xx>.cfg |
|---|---|---|---|
| **Description** | It configures key feature for a specific programmable key. | | |
| **Permitted Values** | 0-N/A<br><br>2-Forward<br><br>5-DND<br><br>7-Recall<br><br>9-Pickup<br><br>13-Speed Dial<br><br>14-Intercom<br><br>22-XML Group<br><br>23-Group PickUp<br><br>24-Multicast Paging (Paging) | 27-XML Browser<br><br>28-History<br><br>29-Directory<br><br>30-Menu<br><br>33-Status<br><br>34-Hot Desking<br><br>38-LDAP (only appear when "ldap.enable = 1"<br><br>40-Prefix<br><br>41-Zero Touch | 43-Local Directory (Local Phonebook)<br><br>45-Local Group<br><br>47-XML Directory (XML Phonebook)<br><br>50-Phone Lock<br><br>51-Switch Account Up<br><br>52-Switch Account Down<br><br>61-Directory<br><br>66-Paging List<br><br>73-Custom Key (only appear when "features.enhanced_dss_keys.enable = 1")<br><br>308-Dial<br><br>309-Bluetooth |
| | **Note**: The CP960 phones only support the following types: N/A (0), XML Browser (27), Dial (308), Directory (29) and Bluetooth (309). The VP59/T58A phones do not support the following types: Dial (308) and Bluetooth (309). | | |
| **Default** | **For CP960**:<br><br>X=1, default: 308 - Dial<br><br>X=2, default: 29 - Directory<br><br>X=3, default: 309 – Bluetooth | | **For VP59/T58A**:<br><br>X=1, default: 0 - NA<br><br>X=2, default: 0 - NA<br><br>X=3, default: 0 – NA<br><br>X=4, default: 0 - NA<br><br>X=12, default: 0 - NA<br><br>X=13, default: 0 – NA<br><br>X=14, default: 2- Forward<br><br>X=17, default: 0 – NA (only for VP59) |

| Web UI | Dsskey->Programmable Key->Type | |
|---|---|---|
| **Parameter** | programablekey.X.history_type[1] | <y0000000000xx>.cfg |
| **Description** | It configures the history type of programmable key. | |
| **Permitted Values** | **0**-Local History<br>**1**-Network CallLog (only appear when "bw.enable=1" and "bw.xsi.call_log.enable=1") | |
| **Default** | 0 | |
| **Web UI** | Dsskey->Programmable Key->Line | |
| **Parameter** | programablekey.X.line[1] | <y0000000000xx>.cfg |
| **Description** | It configures the desired line to apply the programmable key feature.<br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | 1-Line 1<br>2-Line 2<br>...<br>16-Line 16 | |
| **Default** | 1 | |
| **Web UI** | Dsskey>Programmable Key->Line | |
| **Parameter** | programablekey.X.value[1] | <y0000000000xx>.cfg |
| **Description** | It configures the value for some programmable key features.<br>**Note**: You need to configure this parameter when "programablekey.X.type" is set to 2, 9, 13, 14, 23, 24, 27, 40 or 73. | |
| **Permitted Values** | String within 99 characters | |
| **Default** | Blank | |
| **Web UI** | Dsskey->Programmable Key->Value | |
| **Parameter** | programablekey.X.label[1]<br>(X=1-4) | <y0000000000xx>.cfg |
| **Description** | It configures the label displayed on the phone screen for a specific programmable key.<br>This is an optional configuration. | |
| **Permitted Values** | String within 99 characters | |
| **Default** | Blank | |
| **Web UI** | Dsskey->Programmable Key->Label | |
| **Parameter** | programablekey.X.extension[1] | <y0000000000xx>.cfg |
| **Description** | For multicast paging:<br>It configures the channel of the multicast paging group.<br>For intercom feature: | |

| | It configures the pickup code. |
|---|---|
| | For speed dial feature: |
| | It configures the key sequence you want to send via DTMF. |
| | **Note**: It is only applicable when "programablekey.X.type" is set to 13, 14 or 24. It is only applicable to VP59/T58A phones. |
| **Permitted Values** | For multicast paging: |
| | 0 to 31 |
| | For intercom feature: |
| | String within 256 characters |
| | For speed dial feature: |
| | String |
| **Default** | 0 |
| **Web UI** | Dsskey->Programmable Key->Extension |

| **Parameter** | programablekey.X.xml_phonebook[1] | | <y0000000000xx>.cfg |
|---|---|---|---|
| **Description** | It specifies a specific group/phone book when multiple groups/phone books are configured on the IP phone. | | |
| | For, example, both Remote Phone Book 1 "Sell" and Remote Phone Book 2 "Market" are configured on the phone, you can configure "programablekey.X.xml_phonebook = 0" to specify the Remote Phone Book 1 "Sell" for the specific programmable key. The user can tap this line key to access the Remote Phone Book 1 "Sell". | | |
| | **Note**: It is only applicable when "programablekey.X.type" is set to 22 or 45. It is not applicable to CP960 phones. | | |
| **Permitted Values** | Integer from 0 to 48 | | |
| **Default** | 0 | | |
| **Web UI** | Dsskey->Programmable Key->Line | | |

[1]X is the programmable key ID. For VP59: X = 1-4, 12-14, 17; For T58A: X = 1-4, 12-14; for CP960: X = 1-3.

## Related Topic

Shortcut Key/Programmable Key Icons Customization Configuration

## Shortcut Keys

You can add up to six-specific shortcut keys on a new idle screen. Users can use these functions from the phone screen directly, for example, XML Browser.
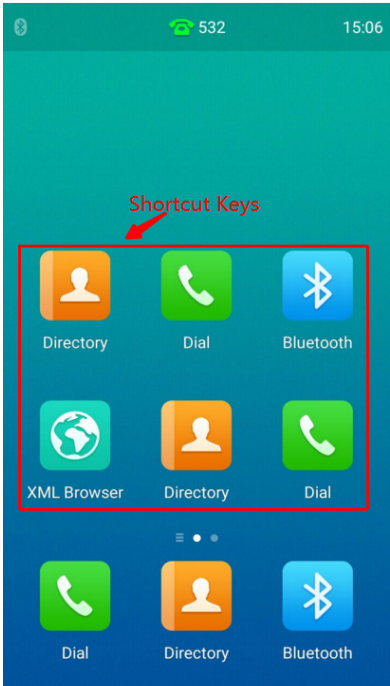
It is only applicable to CP960 phones.

## Topic

Shortcut Keys Configuration

## Shortcut Keys Configuration

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

| Parameter | shortcutkey.X.type[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures key feature for a specific shortcut key. | |
| **Permitted Values** | **0**-N/A<br><br>**27**-XML Browser<br><br>**29**-Directory<br><br>**308**-Dial<br><br>**309**-Bluetooth | |
| **Default** | 0 | |
| **Web UI** | Dsskey->Shortcut Key->Type | |
| **Parameter** | shortcutkey.X.label[1] | <y0000000000xx>.cfg |
| **Description** | It configures the label displayed on the LCD screen for a specific shortcut key.<br><br>This is an optional configuration. | |
| **Permitted Values** | String within 99 characters | |
| **Default** | Blank | |

| Web UI | Dsskey->Shortcut Key->Label | |
|---|---|---|
| **Parameter** | shortcutkey.X.value[1] | <y0000000000xx>.cfg |
| **Description** | It configures the value for some shortcut key features.<br><br>**Note**: You need to configure this parameter when "shortcutkey.X.type" is set to 27 (XML Browser). | |
| **Permitted Values** | String within 99 characters | |
| **Default** | Blank | |
| **Web UI** | Dsskey->Shortcut Key->Value | |

[1]X is the shortcut key ID. X = 1-6.

## Related Topic

Shortcut Key/Programmable Key Icons Customization Configuration

## Ext Keys

The ext keys take effect only if the expansion module is connected to the IP phone.

It is only applicable to T58A phones.

## Topic

Ext Keys Configuration

## Ext Keys Configuration

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

| **Parameter** | expansion_module.X.key.Y.type[1] | | <y0000000000xx>.cfg |
|---|---|---|---|
| **Description** | It configures the feature for a specific ext key.<br><br>**Note**: It is only applicable to T58A phones. | | |
| **Permitted Values** | **0**-N/A<br><br>**1**-Conference<br><br>**2**-Forward<br><br>**3**-Transfer<br><br>**4**-Hold<br><br>**5**-DND<br><br>**7**-Recall<br><br>**8**-SMS<br><br>**9**-Direct Pickup<br><br>**10**-Call Park<br><br>**11**-DTMF<br><br>**12**-Voice Mail<br><br>**13**-Speed Dial | **15**-Line<br><br>**16**-BLF<br><br>**17**-URL<br><br>**18**-Group Listening<br><br>**20**-Private Hold<br><br>**22**-XML Group<br><br>**23**-Group Pickup<br><br>**24**-Multicast Paging (Paging)<br><br>**25**-Record<br><br>**27**-XML Browser<br><br>**34**-Hot Desking<br><br>**35**-URL Record | **38**-LDAP (only appears when "ldap.enable=1")<br><br>**39**-BLF List<br><br>**40**-Prefix<br><br>**41**-Zero Touch<br><br>**42**-ACD<br><br>**45**-Local Group<br><br>**50**-Phone Lock<br><br>**56**-Retrieve Park<br><br>**61**-Directory<br><br>**66**-Paging List<br><br>**73**-Custom Key (only available when "features.enhanced_dss_keys.enable=1")<br><br>**77**-Mobile Account |

| | | | | 304-Open Door |
|---|---|---|---|---|
| | 14-Intercom | | | 305-Video Monitoring |
| | | | | |
| **Default** | Y = 1-60, default: 0 – NA | | | |
| **Web UI** | Dsskey->Ext Key->Type | | | |
| **Parameter** | expansion_module.X.key.Y.line[1] | | | \<y0000000000xx\>.cfg |
| **Description** | It configures the desired line to apply the ext key feature. **Note**: It is only applicable to T58A phones. | | | |
| **Permitted Values** | 1-16 | | | |
| **Default** | 1 | | | |
| **Web UI** | Dsskey->Ext Key->Line | | | |
| **Parameter** | expansion_module.X.key.Y.value[1] | | | \<y0000000000xx\>.cfg |
| **Description** | It configures the value for some ext key features. For open door feature: It configures the open door URL of 2N IP intercom. The valid URL format is: http(s) ://<IP address of the IP intercom>/api/switch/ctrl?switch=<switch identifier, typically 1 to 4>&action=trigger or http(s)://username:password@<IP address of the IP intercom>/api/switch/ctrl?switch=<switch identifier, typically 1 to 4>&action=trigger. For video monitoring feature: It configures the video access URL of IP intercom camera. The valid URL format is: http(s)://<IP address of the IP intercom>/mjpg/video.mjpg or http(s)://username:password@<IP address of the IP intercom>/mjpg/video.mjpg. **Note**: You do not need to configure this parameter when "expansion_module.X.key.Y.type" is set to 4, 5, 7, 8, 18, 20, 22, 25, 34, 37, 38, 39, 41, 42, 45, 50, 61 or 66. It is only applicable to T58A phones. | | | |
| **Permitted Values** | String within 99 characters | | | |
| **Default** | Blank | | | |
| **Web UI** | Dsskey->Ext Key->Value | | | |
| **Parameter** | expansion_module.X.key.Y.label[1] | | | \<y0000000000xx\>.cfg |
| **Description** | It configures the label displayed on the LCD screen for a specific programmable key. This is an optional configuration. **Note**: It is only applicable to T58A phones. | | | |
| **Permitted Values** | String within 99 characters | | | |
| **Default** | Blank | | | |

| Web UI | Dsskey->Ext Key->Label | |
|---|---|---|
| **Parameter** | expansion_module.X.key.Y.extension[1] | <y0000000000xx>.cfg |
| **Description** | For multicast paging:<br><br>It configures the channel of multicast paging group.<br><br>For BLF/BLF list/intercom feature:<br><br>It configures the pickup code.<br><br>For speed dial feature:<br><br>It configures the key sequence you want to send via DTMF.<br><br>For open door/video monitoring feature:<br><br>It configures the number or IP address of the IP intercom that this key will apply to.<br><br>**Note**: It is only applicable when "expansion_module.X.key.Y.type" is set to 14, 16, 24 or 39. It is only applicable to T58A phones. | |
| **Permitted Values** | For multicast paging:<br><br>0 to 31<br><br>For BLF/BLF list/intercom/open door/video monitoring feature:<br><br>String within 256 characters<br><br>For speed dial feature:<br><br>String | |
| **Default** | 0 | |
| Web UI | Dsskey->Ext Key->Extension | |
| **Parameter** | expansion_module.X.key.Y.xml_phonebook[1] | <y0000000000xx>.cfg |
| **Description** | It specifies a specific group/phone book when multiple groups/phone books are configured on the phone.<br><br>For, example, both Remote Phone Book 1 "Sell" and Remote Phone Book 2 "Market" are configured on the phone, you can configure "programablekey.X.xml_phonebook = 0" to specify the Remote Phone Book 1 "Sell" for the specific ext key. The user can press this line key to access the Remote Phone Book 1 "Sell".<br><br>**Note**: It is only applicable when "expansion_module.X.key.Y.type" is set to 22 or 45. It is only applicable to T58A phones. | |
| **Permitted Values** | Integer from 0 to 48 | |
| **Default** | 0 | |
| Web UI | Dsskey->Ext Key->Ext KeyX->Line | |

[1]X is the expansion module ID, Y is the EXT key ID.  For T58A, X=1-3, Y=1-60.

## Shortcut Key/Programmable Key Icons Customization

You can customize the personalized icons for shortcut keys or programmable keys.

Shortcut keys are only applicable to CP960 phones.

## Topics

## Shortcut Key/Programmable Key Icons Customization Configuration

The following table lists the parameters you can use to configure the shortcut key/programmable key icons.

| Parameter | dsskey.icon.url | \<y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the access URL of a TAR icon file for shortcut key/programmable key. The format of the icon must be *.png. The icon file should be compressed into a TAR file in advance and then place it to the provisioning server. **Example**: dsskey.icon.url = tftp://192.168.10.25/icon_directory.tar **Note**: We recommend you use a mixture of letters and characters for the icon and TAR file names. Shortcuts key are only applicable to CP960 phones. | |
| Permitted Values | String | |
| Default | Blank | |
| Parameter | shortcutkey.X.icon[1] | \<y0000000000xx>.cfg |
| Description | It configures the icon for a specific shortcut key. **Note**: It is only applicable to CP960 phones. After configuration, the icon will not change even if "shortcutkey.X.type" is set to another value. | |
| Permitted Values | 0 (default icon) or uploaded custom icon name (for example, icon_directory.png) | |
| Default | Blank | |
| Parameter | programablekey.X.icon[2] | \<y0000000000xx>.cfg |
| Description | It configures the icon for a specific programmable key. **Note**: It works only if "programablekey.X.type" is not set to 0 (N/A). | |
| Permitted Values | 0 (default icon) or uploaded custom icon name (for example, icon_settings.png) | |
| Default | 0 | |
| Parameter | dsskey.icon.delete | \<y0000000000xx>.cfg |
| Description | It deletes the specified or all custom shortcut key/programmable key icons. **Example**: Delete all custom shortcut/programmable key icons: dsskey.icon.delete = http://localhost/all Delete a specified shortcut/programmable key icon (for example, icon_directory.png): | |

| | dsskey.icon.delete = http://localhost/icon_directory.png |
|---|---|
| **Permitted Values** | http://localhost/all or http://localhost/name.png |
| **Default** | Blank |

[1]X is the shortcut key ID. X = 1-6.

[2]X is the programmable key ID. For VP59: X = 1-4, 12-14, 17; For T58A: X = 1-4, 12-14; for CP960: X = 1-3.

## Related Topics

Shortcut Key/Programmable Key Icons Limit
Preparing the Tar Formatted File

## Example: Customizing an Icon for a Specific Shortcut Key

The following example shows the configuration for customizing an icon for the second shortcut key. The shortcut key is only applicable to CP960 phones.

Prepare the custom key icon "icon_directory.png", compress it into a tar file "icon_custom.tar", and then place the tar file to the provisioning server "http://192.168.10.25".

**Example**

dsskey.icon.url = http://192.168.10.25/icon_custom.tar

shortcutkey.2.type = 29

shortcutkey.2.icon = icon_directory.png

After auto provisioning, the Directory shortcut key is added to a new idle screen, the key icon is customized as well.
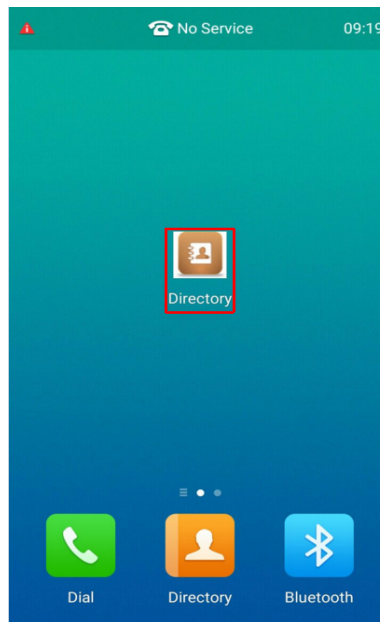


## Related Topics

Shortcut Keys Configuration
Shortcut Key/Programmable Key Icons Customization Configuration
Preparing the Tar Formatted File

## Example: Customizing an Icon for a Specific Programmable Key

The following example shows the configuration for customizing an icon for the second programmable key.

**For CP960**:

Prepare the custom key icon "icon_directory.png", compress it into a tar file "icon_custom.tar", and then place the tar file to the provisioning server "http://192.168.10.25".

**Example**:

*dsskey.icon.url = http://192.168.10.25/icon_custom.tar*

*programablekey.2.icon = icon_directory.png*

After auto provisioning, the second programmable key icon is customized.
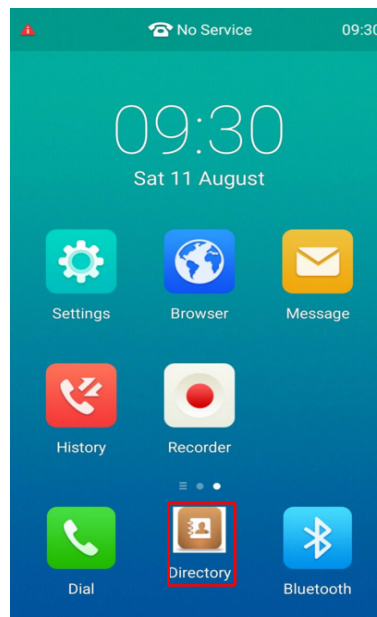


**For VP59/T58A**:

Prepare the custom key icon "icon_settings.png", compress it into a tar file "icon_menu.tar", and then place the tar file to the provisioning server "http://192.168.10.25".

**Example**:

*dsskey.icon.url = http://192.168.10.25/icon_menu.tar*

*programablekey.2.type = 30*

*programablekey.2.icon = icon_settings.png*

After auto provisioning, the second programmable key is assigned the feature to access the menu, and the key icon is customized.
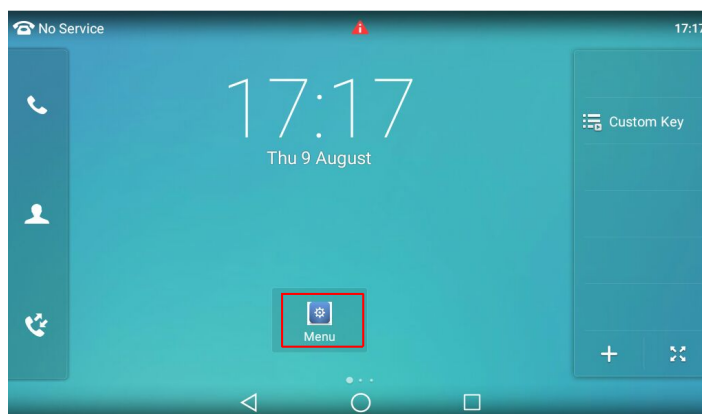
## Related Topics

Programmable Keys Configuration
Shortcut Key/Programmable Key Icons Customization Configuration
Preparing the Tar Formatted File

# Enhanced DSS Keys

Enhanced DSS Keys (EDK) enables users to customize the functions of phone's DSS keys.

With EDK, You can do the following:

- Assign frequently-used function to DSS keys
- Create menu shortcuts for frequently-used phone settings as need.

Application scenarios involve the following:

- Adding new DSS keys to simplify the operation of common telephony tasks that may need more than one key press with the default configuration.
- Removing certain default DSS keys for the functions that may be redundant or never used.

The rules for configuring EDK for DSS keys are different. Before using EDK, you are advised to become familiar with the macro language.

It is not applicable to CP960 phones.

For more information on Enhanced DSS Keys, refer to Using Enhanced DSS Keys on Yealink IP Phones.

## Topics

Guidelines for Configuring Enhanced DSS Keys
Macro Action Strings
EDK Configuration
EDK List Configuration
EDK User Input Prompt Configuration
EDK Soft Keys Configuration
Example: Configuring EDK List for a Line Key

# Guidelines for Configuring Enhanced DSS Keys

The following guidelines will help you to configure EDK efficiently:

- Activation of EDK functions requires valid macro construction.
- Character "$" delimits the parts of the macro string (except the digits only) and it must exist in pairs. For more information, refer to Macro Action Strings.
- Macros can be invoked in the format "!<macro name>", where <macro name> is defined by the parameter "edk.edk-list.X.mname".
- If there are two or more same macros, the soft key or DSS key will invoke the macro with the smallest value of X defined by the parameter "edk.edklist.X.mname".

## Macro Action Strings

Before using EDK, you must be familiar with macro language shown in this section.

The following table shows the basic macro action string syntax when creating EDK macros:

| Macro Action | Description |
|---|---|
| **Digits** | The digits to be sent. You can use only *, #, +, 0-9. The appearance of this parameter depends on the action string.<br><br>**Example:** *981135. |
| **$C<command>$** | This is the command. It can appear anywhere in the action string. Supported commands (or shortcuts) include:<br><br>• hang up (hu)<br>• hold (h)<br>• waitconnect (wc)<br>• pause <number of seconds> (p <num sec>) where the maximum value is 10<br><br>**Example**: 4411$Cwc$$Cp10$ defines dialing 4411>>waitconnect>>connected and lasts 10 seconds. |
| **$T<type>$** | The embedded action type. Multiple actions can be defined. Supported action types include:<br><br>• invite<br>• dtmf<br>• refer<br>• intercom<br><br>**Example**: *338$Tdtmf$ defines sending the *338 by the type of dtmf.<br><br>**Note**: We recommend that you always define this field. If not, the supplied digits are dialed using INVITE. |
| **$M<macro>$** | The embedded macro. The <macro> string must begin with a letter. If the macro name is not defined, the execution of the action string will be ignored.<br><br>**Example**: $MAA$ means invoking the EDK macro AA. |
| **$S<softkey ID>$** | The functionality of performing this action is the same as that of pressing the desired soft key.<br><br>Each soft key has a unique identifier on the IP phone, you can configure this parameter according to the system-defined softkey ID. If the softkey ID is not defined on the phone or there is no matched soft key on the current screen, the execution of the action string will be ignored. The softkey ID is case-insensitive.<br><br>**Example**: $Sanswer$ means pressing the **Answer** soft key. |

| Macro Action | Description |
|---|---|
| | Yealink phones support customizing soft keys. When invoking a custom soft key, the prefix "#" must be added.<br><br>**Example**: If the custom softkey label is IVR1, the custom softkey ID is custom_macro, then $S#custom_macro$ means pressing the **IVR1** soft key.<br><br>**Note**: To view the softkey ID, you can set "features.enhanced_dss_keys.enable" and "edk.id_mode.enable" to 1 (Enabled) and then long press the Volume Up key when the phone is idle. |
| **$K\<key name>$** | The functionality of performing this action is the same as that of pressing the desired hard key.<br><br>Supported key names include:<br><br>• LineKeyX (for VP59/T58A, X=1-27).<br>• SoftKeyX (X ranges from 1 to 4)<br>• VolDown<br>• VolUp<br>• DialPadX (X ranges from 0 to 9)<br>• DialPadPound<br>• DialPadStar<br>• Headset<br>• Mute<br>• Message<br>• Hold<br>• Redial<br>• Transfer<br>• Speaker<br>• ExtX@Y (X stands for the serial number of expansion module key, Y stands for the serial number of expansion module; For T58A: X ranges from 1 to 60, Y ranges from 1 to 3; @Y can be omitted if there is only one expansion module connected to the phone.)<br>• Menu (You can enter menu by executing this command at any interface except the non-executable situations. For example, entering menu is blocked during an active call.)<br>• Home (You can return back to the Home screen by executing this command on any screen)<br><br>**Example**: $KDialPadPound$ means pressing the pound key.<br><br>**Note**: If a key (for example, Redial key) is not found but the function is available, the phone will perform the corresponding action. If a key is not found and the function is unavailable, the execution of the action string will be ignored. |
| **$I\<menu item ID>$** | The action is to position and enter the desired menu item.<br><br>Each menu item has a unique identifier on the IP phone, you can configure this parameter according to the system-defined menu item ID. If the menu item ID is not defined on the phone or there is no matched menu item on the current screen, the execution of the action string will be ignored. The menu item ID is case-insensitive. |

| Macro Action | Description |
|---|---|
| | **Example**: $Istatus_list& means entering the Status menu.<br><br>**Note**: To view the menu item ID, you can set "edk.id_mode.enable" to 1 (Enabled) and then long press the Volume Up key when the phone is idle. |
| **$P<label>&T<title>&C<characters number allowed>&N&M$** | The user input prompt string.<br><br>"label" means the specified label for the user input prompt.<br><br>"title" means the specified title for the user input prompt.<br><br>"characters number allowed" defines the maximum number of input characters.<br><br>If &N is included, the input mode is numeric&symbolic. If &N is not included, the onscreen keyboard is displayed, you can manually change input mode.<br><br>If &M is included, the inputs are masked by the dot characters "•".<br><br>**Example**: **$PPassword&C3&N&M$** means prompting a **Password** pop-up box, the maximum number of input characters is 3, the input type is Number, and the input is masked by the dot characters "•". |
| **$P<EDK user input prompt X>N<characters number allowed>$** | The user input prompt string.<br><br>"EDK user input prompt X" means which EDK user input prompt is invoked. It indicates the X defined by "edk.edkprompt.X.enable".<br><br>"characters number allowed" defines the maximum number of input characters. You need to press the **Enter** soft key to complete data entry.<br><br>**Example**: $P2N5$ means invoking the EDK user input prompt 2 and inputting 5 characters at most.<br><br>**Note**: For more information on EDK user input prompt, refer to EDK User Input Prompt Configuration. |
| **$L<label>$** | This is the label for the entire operation. The value can be any string including the null string (in this case, no label displays).<br><br>This label is used if no label is configured for a custom key DSS key or soft key, otherwise this one is ignored. Make this the first entry in the action string.<br><br>**Example**: $LEDK2$1234$Tinvite$ defines calling out the number 1234 and using the label "EDK2" for a Custom Key DSS key or soft key. |

## EDK Configuration

To configure EDK list, EDK user input prompt, EDK soft keys and custom DSS keys, you have to enable EDK feature. By default, the EDK feature is disabled.

Yealink phones can display the menu item ID by long pressing the Volume Up key. It is especially useful for those users who need to view the menu item ID when configuring EDK macros.

It is not applicable to CP960 phones.

The following graphic shows an example for displaying the menu item ID after accessing a submenu of T58A phones:

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

| Parameter | features.enhanced_dss_keys.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the Enhanced DSS Keys (EDK) feature.<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Parameter** | edk.id_mode.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables to view the menu item ID by long pressing the Volume Up key for three seconds on any screen.<br><br>**Note**: The menu item ID is displayed on the status bar of the phone. Long pressing the Volume Up key again for three seconds to exit. It works only if "features.enhanced_dss_keys.enable" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |

## EDK List Configuration

Using the Enhanced DSS Keys (EDK) List parameters to define a macro is useful when defining more than one soft key or DSS key.

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

| Parameter | edk.edklist.X.enable[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables Enhanced DSS Keys (EDK) macro X.<br><br>**Note**: It works only if "features.enhanced_dss_keys.enable" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |

| Default | 0 | |
|---|---|---|
| **Parameter** | edk.edklist.X.mname[1] | <y0000000000xx>.cfg |
| **Description** | It configures the unique identifier used by the soft key or DSS key configuration to reference the enhanced DSS keys entry for macro X.<br><br>It cannot start with a digit. This parameter must have a value, it cannot be left blank.<br><br>**Example**:<br><br>edk.edklist.2.mname = macro2<br><br>**Note**: If there are two or more same macros, the soft key or DSS key will invoke the macro with the smallest value of X. It works only if "features.enhanced_dss_keys.enable" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | String | |
| **Default** | Blank | |
| **Parameter** | edk.edklist.X.action[1] | <y0000000000xx>.cfg |
| **Description** | It configures the action string that contains a macro definition of the action that the softkey or DSS key performs.<br><br>This parameter must have a value, it cannot be left blank.<br><br>**Example**:<br><br>edk.edklist.2.action = 1013$Tinvite$<br><br>**Note**: It works only if "features.enhanced_dss_keys.enable" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | String | |
| **Default** | Blank | |

[1]X is the macro ID. X=1-255.

## EDK User Input Prompt Configuration

The EDK user input prompt parameters must be used if interactivity with the user is implemented as part of any macro.

The following table lists the parameters you can use to configure EDK user input prompt.

| **Parameter** | edk.edkprompt.X.enable[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables user input prompt X.<br><br>**Note**: If a macro attempts to use an EDK user input prompt that is disabled, the macro execution fails. It works only if "features.enhanced_dss_keys.enable" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Parameter** | edk.edkprompt.X.label[1] | <y0000000000xx>.cfg |

| Description | It configures the text string used as a label of the user input prompt X. | |
|---|---|---|
| | If it is left blank, Default is displayed. | |
| | **Example**: | |
| | edk.edkprompt.1.label = Enter Password | |
| | **Note**: It works only if "features.enhanced_dss_keys.enable" and "edk.edkprompt.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | String | |
| **Default** | Default | |
| **Parameter** | edk.edkprompt.X.type[1] | <y0000000000xx>.cfg |
| Description | It configures the type of characters entered by the user for user input prompt X. | |
| | If it is set to numeric, the default input method is 123, and you can switch among abc/ABC/2aB input methods. | |
| | If it is set to text, the default input method is abc, and you can switch among ABC/2aB/123 input methods. | |
| | **Note**: It works only if "features.enhanced_dss_keys.enable" and "edk.edkprompt.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | text or numeric | |
| **Default** | text | |
| **Parameter** | edk.edkprompt.X.userfeedback[1] | <y0000000000xx>.cfg |
| Description | It configures the user input feedback method for user input prompt X. | |
| | **Note**: It works only if "features.enhanced_dss_keys.enable" and "edk.edkprompt.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | **visible**-the entered text is visible. | |
| | **masked**-the entered text is displayed as dot characters "•". It can be used to mask password fields. | |
| **Default** | visible | |
| **Parameter** | edk.edkprompt.X.title[1] | <y0000000000xx>.cfg |
| Description | It configures the text string used as a title for the user input prompt X. The title appears at the top of the user input prompt screen. | |
| | If it is left blank, EDK Prompt is displayed. | |
| | **Note**: It works only if "features.enhanced_dss_keys.enable" and "edk.edkprompt.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | String | |
| **Default** | EDK Prompt | |

[1]X is the prompt ID. X=1-10.

# EDK Soft Keys Configuration

You can customize the soft keys as need. This feature is typically used to access frequently-used functions or to create menu shortcuts to frequently-used phone settings.

Custom soft keys can be added in the following phone states:

- **Idle** - There are no active calls on the phone.
- **Alerting (or ringing)** – There is an incoming call on the phone.
- **Connecting** – There is an outgoing call on the phone. Moreover, the call is connecting.
- **Transfer connecting** – There is a call being transferred to another phone. Moreover, the call is connecting.
- **Talk** – There is an active call on the phone.
- **Call failed** – The outgoing call encounters a failure.
- **Ring back** - There is an outgoing call on the phone. Moreover, the phone is in the ringback state.
- **Transfer ring back** - There is a call being transferred to another phone. Moreover, the phone is in the ringback state.
- **Hold** – The call is placed on hold on the phone.
- **Held** – The call is held.
- **Conference** – The phone sets up a conference call.

| Note |
| --- |
| Configuring the custom soft keys may affect the softkey layout in different call states. For more information on softkey layout, refer to Softkey Layout. |

The following table lists the parameters you can use to configure EDK soft keys.

| Parameter | softkey.X.enable[1] | <y0000000000xx>.cfg |
| --- | --- | --- |
| Description | It enables or disables the custom soft key X.<br>**Note**: It works only if "features.enhanced_dss_keys.enable" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Parameter | softkey.X.label[1] | <y0000000000xx>.cfg |
| Description | It configures the text displayed on the soft key label.<br>**Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |
| Permitted Values | String | |
| Default | Blank | |
| Parameter | softkey.X.position[1] | <y0000000000xx>.cfg |
| Description | It configures the location on the phone screen for soft key X.<br>**Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |
| Permitted Values | Integer from 0 to 10<br>If it is set to 0, the soft key X is located in the first available position from the left. | |

| Default | 0 | |
|---|---|---|
| **Parameter** | softkey.X.action[1] | <y0000000000xx>.cfg |
| **Description** | It configures the action or function for custom soft key X. | |
| | This value uses the same macro action string syntax as an Enhanced DSS key. | |
| | You can also invoke the EDK macro that was already defined. The macro name follows the character "!". | |
| | **Example**: | |
| | softkey.1.action = !macro1 | |
| | In this example, macro1 stands for the macro name configured by the parameter "edk.edklist.X.mname". | |
| | **Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | String | |
| **Default** | Blank | |
| **Parameter** | softkey.X.use.idle[1] | <y0000000000xx>.cfg |
| **Description** | It enables or disables the custom soft key X to be displayed in the idle state. | |
| | **Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Parameter** | softkey.X.use.incoming_call[1] | <y0000000000xx>.cfg |
| **Description** | It enables or disables the custom soft key X to be displayed in the alerting (ringing) state. | |
| | **Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Parameter** | softkey.X.use.connecting[1] | <y0000000000xx>.cfg |
| **Description** | It enables or disables the custom soft key X to be displayed in the connecting state. | |
| | **Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Parameter** | softkey.X.use.transfer_connecting[1] | <y0000000000xx>.cfg |
| **Description** | It enables or disables the custom soft key X to be displayed in the transfer connecting state. | |
| | **Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted** | **0**-Disabled | |

| | |
|---|---|
| **Values** | **1**-Enabled |
| **Default** | 0 |

| **Parameter** | softkey.X.use.on_talk[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the custom soft key X to be displayed in the talking state. **Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |

| | |
|---|---|
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |

| **Parameter** | softkey.X.use.call_failed[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the custom soft key X to be displayed in the call failed state. **Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |

| | |
|---|---|
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |

| **Parameter** | softkey.X.use.ring_back[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the custom soft key X to be displayed in the ring back state. **Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |

| | |
|---|---|
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |

| **Parameter** | softkey.X.use.transfer_ring_back[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the custom soft key X to be displayed in the transfer ring back state. **Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |

| | |
|---|---|
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |

| **Parameter** | softkey.X.use.hold[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the custom soft key X to be displayed in the hold state. **Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |

| | |
|---|---|
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |

| **Parameter** | softkey.X.use.held[1] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the custom soft key X to be displayed in the held state. | |

| | |
|---|---|
| | **Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |
| **Parameter** | softkey.X.use.conferenced[1]   <y0000000000xx>.cfg |
| **Description** | It enables or disables the custom soft key X to be displayed in the conference state.<br><br>**Note**: It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |

[1]X is the soft key ID. X=1-10.

# Power Saving

The power-saving feature turns off the backlight and screen (also applicable to EXP50 expansion module connected to the T58A phones) to conserve energy. The IP phone and EXP50 (if connected) enter power-saving mode after the phone has been idle for a certain period of time. And the IP phone and EXP50 (if connected) will exit power-saving mode if a phone/EXP50 event occurs - for example, the phone receives an incoming call or a new message, or you tap a key on the phone/EXP50.

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

## Topic

Power Saving Configuration

## Power Saving Configuration

You can enable or disable power saving, and set the different idle timeout for office hours and off hours.

- **Office Hour**: specify the start time and end time of the day's office hour. You can change the office hours to avoid affecting your work.
- **Idle Timeout**: specify the period of time before the IP phone enters the power-saving mode.

You can specify the following three types of idle timeout:

- **Office Hours Idle TimeOut**: specify the idle timeout for office hours.
- **Off Hours Idle TimeOut**: specify the idle timeout for non-office hours.
- **User Input Extension Idle TimeOut**: specify the idle timeout that applies after you use the IP phone (for example, press a key on the phone or pick up/hang up the handset).

By default, the Office Hours Idle Timeout is much longer than the Off Hours Idle TimeOut. If you use the IP phone, the idle timeout that applies (User Input Extension Idle Timeout or Office Hours/Off Hours Idle TimeOut) is the timeout with the highest value.

If the phone has an incoming call or new message, the User Input Extension Idle TimeOut is ignored.

**Note**

For VP59/T58A phones, if you disable the power saving feature, the phone will automatically enter power-saving mode to protect the screen when the phone is inactive for 72 hours. Image persistence may be caused on LCD if power saving is disabled

**Tip**

You can choose to set a higher User Input Extension Idle TimeOut than the Office Hours Idle TimeOut and Off Hours Idle TimeOut so that the phone does not enter the power-saving mode too often after you use the phone.

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

| Parameter | features.power_saving.intelligent_mode | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the power saving intelligent mode. | |
| Permitted Values | **0**-Disabled, the phone stays in power-saving mode even if the office hour arrives the next day.<br><br>**1**-Enabled, the phone automatically identifies the office hour and exits power-saving mode once the office hour arrives the next day. | |
| Default | 1 | |
| Parameter | features.power_saving.enable | <y0000000000xx>.cfg |
| Description | It enables or disables the power saving feature.<br><br>**Note**: For CP960 phones, the power saving feature is enabled by default. It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled, the phone automatically enters the power-saving mode to protect the screen when the phone is inactive for 72 hours. That is, the color screen phones will turn off the backlight and screen, and the black-and-white screen phones will only turn off the backlight. Image persistence may be caused on LCD.<br>**1**-Enabled | |
| Default | 1 | |
| Web UI | Settings->Power Saving->Power Saving | |
| Parameter | features.power_saving.office_hour.idle_timeout | <y0000000000xx>.cfg |
| Description | It configures the time (in minutes) to wait in the idle state before the phone enters power-saving mode during the office hours. | |
| Permitted Values | Integer from 1 to 240 | |
| Default | 120 | |
| Web UI | Settings->Power Saving->Office Hour Idle TimeOut | |
| Parameter | features.power_saving.off_hour.idle_timeout | <y0000000000xx>.cfg |
| Description | It configures the time (in minutes) to wait in the idle state before phone enters power-saving mode during the non-office hours. | |
| Permitted Values | Integer from 1 to 10 | |
| Default | 10 | |
| Web UI | Settings->Power Saving->Off Hour Idle TimeOut | |

| Parameter | features.power_saving.user_input_ext.idle_timeout | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the minimum time (in minutes) to wait in the idle state - after using the phone - before the phone enters the power-saving mode. | |
| Permitted Values | Integer from 1 to 30 | |
| Default | 10 | |
| Web UI | Settings->Power Saving->User Input Extension Idle TimeOut | |
| Parameter | features.power_saving.office_hour.monday<br><br>features.power_saving.office_hour.tuesday<br><br>features.power_saving.office_hour.wednesday<br><br>features.power_saving.office_hour.thursday<br><br>features.power_saving.office_hour.friday<br><br>features.power_saving.office_hour.saturday<br><br>features.power_saving.office_hour.sunday | <y0000000000xx>.cfg |
| Description | It configures the start time and end time of the day's office hour.<br><br>Start time and end time are separated by a comma.<br><br>Start time and end time are separated by a comma.<br><br>**Example**:<br><br>features.power_saving.office_hour.monday = 7,19 | |
| Permitted Values | Integer from 0 to 23, Integer from 0 to 23 | |
| Default | 7,19 - for Monday, Tuesday, Wednesday, Thursday, Friday.<br><br>7,7 - for Saturday, Sunday. | |
| Web UI | Settings->Power Saving->Monday/Tuesday/Wednesday/Thursday/Friday/Saturday/Sunday | |
| Parameter | features.power_saving.power_led_flash.on_time | <y0000000000xx>.cfg |
| Description | It configures the period of time (in milliseconds) when the power LED indicator is on in the power-saving mode.<br><br>If it is set to 0 and "features.power_saving.power_led_flash.off_time" is not set to 0, the power LED indicator will be off when the phone enters the power-saving mode.<br><br>**Note**: It is only applicable to VP59/T58A phones. | |
| Permitted Values | 0, Integer from 100 to 10000 | |
| Default | 500 | |
| Parameter | features.power_saving.power_led_flash.off_time | <y0000000000xx>.cfg |
| Description | It configures the period of time (in milliseconds) when the power LED indicator is off in the power-saving mode.<br><br>If it is set to 0, the power LED indicator will be on when the phone enters the power-saving mode.<br><br>**Note**: It is only applicable to VP59/T58A phones. | |

| Permitted Values | 0, Integer from 100 to 10000 |
|---|---|
| Default | 3000 |

# 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 following shows search results displayed on T58A phones:
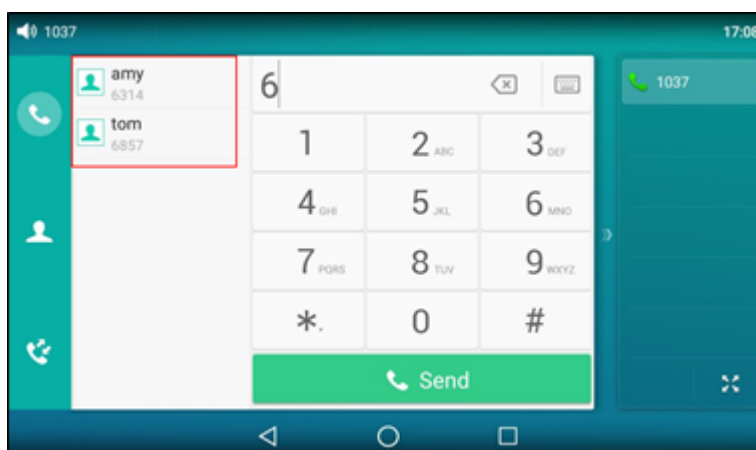


The search source list can be Local Directory, History, Remote Phone Book and LDAP. The search source list can be configured using a supplied super search template file (super_search.xml).

## 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<br><br>calllog_search<br><br>remote_directory_search<br><br>ldap_search | The directory list (For example, "local_directory_search" for the local directory list).<br><br>**Note**: Do not edit this field. |

| Attributes | Valid Values | Description |
|---|---|---|
| | BroadSoft_directory_search<br><br>BroadSoft_UC_search (not applicable to CP960 phones)<br><br>google_directory_search (not applicable to VP59/CP960 phones) | |
| display_name | Local Contacts<br><br>History<br><br>Remote Phonebook<br><br>LDAP<br><br>Network Directories<br><br>BroadSoft Buddies (not applicable to CP960 phones)<br><br>Google Contacts (not applicable to VP59/CP960 phones) | The display name of the directory list.<br><br>**Note**: We recommend you do not edit this field. |
| priority | 1 to 5 (for CP960 phones)<br><br>1 to 7 (for T58A phones)<br><br>1 to 6 (for VP59 phones)<br><br>**For CP960:**<br><br>1 is the highest priority, 5 is the lowest.<br><br>**For T58A:**<br><br>1 is the highest priority, 7 is the lowest.<br><br>**For VP59:**<br><br>1 is the highest priority, 6 is the lowest. | The priority of the search results. |
| enable | 0/1<br><br>**0**: Disabled<br><br>**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.
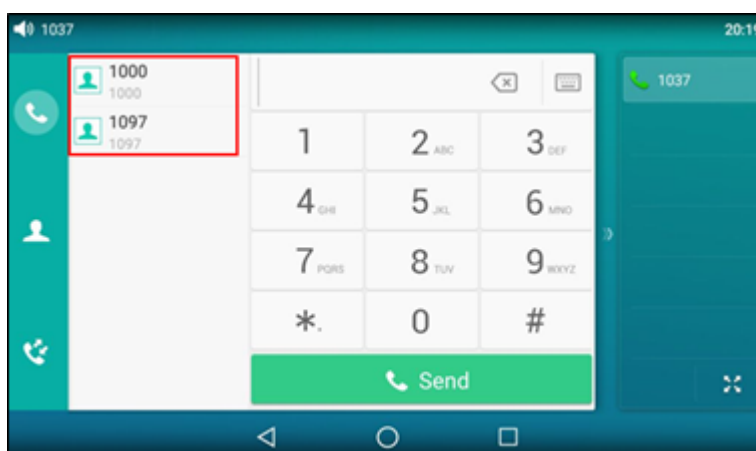
## Search Source List Configuration

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 | |

# Recent Call Display in Dialing

Recent call display allows you to view the placed calls list when the phone is on the dialing screen (lifts the handset, presses the Speakerphone key or taps the desired line key). You can select to place a call from the placed calls list.

The following shows the recent calls displayed on T58A phones:



## 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<br>**1**-Enabled, users can view the placed calls list when the phone is on the dialing screen. | |
| Default | 1 | |
| Web UI | Directory->Setting->Recent Call In Dialing | |

# Door Phone

The IP phone is compatible with the 2N and Baudisch IP intercoms. And you can pair up to 99 IP intercoms on the IP phone.

When a visitor rings your doorbell, the phone will ring also. You can answer the incoming call, and then tap ☐ to open the door.
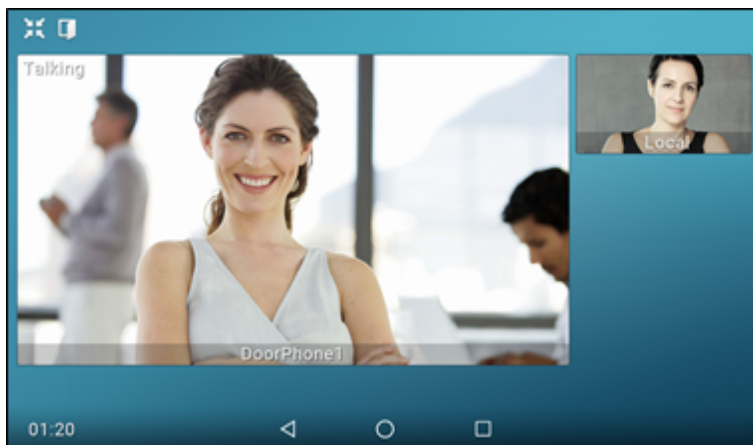


The phones also support the following:

- Preview: get a preview of who's there when receiving a visitor's incoming call.
- One-button Open: open the door at any time.
- Monitoring: check the camera video at any time.

For more information, refer to Using Door Phone Feature on Yealink Smart Media Phones.

In addition to the IP phone, IP intercom should be configured. For more information on how to configure the IP intercom, refer to the documentation from the manufacturer.

Door phone feature is not applicable to CP960 phones.

## Topic

Door Phone Parameters

## Door Phone Parameters

The following table lists the parameters you can use to configure door phone feature.

| Parameter | features.doorphone.amount | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures that how many IP intercoms are supported by the phone.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | Integer from 0 to 99 | |
| Default | 99 | |
| Web UI | Features->Door Phone->Door Phone List | |
| Parameter | features.doorphone.X.device_model[1] | <y0000000000xx>.cfg |
| Description | It configures the device type of the IP intercom.<br><br>**0**-Custom<br><br>**1**-2N<br><br>**3**-Baudisch | |

| | |
|---|---|
| | **Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | 0, 1 or 3 |
| **Default** | 0 |
| **Web UI** | Features->Door Phone->Device Type |
| **Parameter** | features.doorphone.X.display_name[1]     `<y0000000000xx>.cfg` |
| **Description** | It configures the display name of the IP intercom to be displayed on the phone's screen. **Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | String within 99 characters |
| **Default** | Blank |
| **Web UI** | Features->Door Phone->Display Name |
| **Parameter** | features.doorphone.X.phone_number[1]     `<y0000000000xx>.cfg` |
| **Description** | It configures the phone number or IP address of the IP intercom. **Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | String within 32 characters |
| **Default** | Blank |
| **Web UI** | Features->Door Phone->Phone Number |
| **Parameter** | features.doorphone.X.unlock_pin[1]     `<y0000000000xx>.cfg` |
| **Description** | It configures the unlock PIN of the IP intercom. **Example**: features.doorphone.1.unlock_pin=8888* When tapping the **Open Door** soft key after answering the call, the phone will send the DTMF sequence "8888*" to the IP intercom. And if the DTMF sequence matches the code configured on IP intercom, the door will be opened. **Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | String within 99 characters |
| **Default** | Blank |
| **Web UI** | Features->Door Phone->Unlock PIN |
| **Parameter** | features.doorphone.X.full_screen[1]     `<y0000000000xx>.cfg` |
| **Description** | It enables or disables the phone to enter full-screen display automatically after answering the visitor's call. **Note**: It is not applicable to CP960 phones. It works only if "video.enable" is not set to 0 (Disabled). |
| **Permitted Values** | **0**-Disabled **1**-Enabled |
| **Default** | 0 |
| **Web UI** | Features->Door Phone->Full Screen in Call |
| **Parameter** | features.doorphone.X.send_audio[1]     `<y0000000000xx>.cfg` |

| Description | It enables or disables the phone to transmit your audio during a visitor's call. **Note**: It is not applicable to CP960 phones. |
|---|---|
| **Permitted Values** | **0**-Disabled **1**-Enabled |
| **Default** | 1 |
| **Web UI** | Features->Door Phone->Send Audio in Call |
| **Parameter** | features.doorphone.X.send_video[1] <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to transmit your video during a visitor's call. **Note**: It works only if "video.enable" is not set to 0 (Disabled), "static.camera.function.enable" is set to 1 (Enabled), and "features.doorphone.X.device_model" is not set to 3 (Baudisch). It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled **1**-Enabled |
| **Default** | 1 |
| **Web UI** | Features->Door Phone->Send Video in Call |
| **Parameter** | features.doorphone.X.video.stream.httpurl[1] <y0000000000xx>.cfg |
| **Description** | It configures the video access URL of IP intercom camera. The valid URL format is: http(s)://<IP address of the IP intercom>/mjpg/video.mjpg or http(s)://user-name:password@<IP address of the IP intercom>/mjpg/video.mjpg. **Example**: features.doorphone.1.video.stream.httpurl= http://192.168.1.1/mjpg/video.mjpg **Note**: You need to configure this parameter if "features.doorphone.X.device_model" is set to 3 (Baudisch). If you use the first URL format and the IP intercom needs HTTP API authentication, you should configure the authentication account (configured by the parameters "features.doorphone.X.httpapi.username" and "features.doorphone.X.httpapi.password"). It is not applicable to CP960 phones. |
| **Permitted Values** | URL within 511 characters |
| **Default** | Blank |
| **Web UI** | Features->Door Phone->IP Cam |
| **Parameter** | features.doorphone.X.videopreview.enable[1] <y0000000000xx>.cfg |
| **Description** | It enables or disables the video preview when receiving a visitor's incoming call. **Note**: It works only if "account.X.auto_answer" is set to 0 (Disabled) and "video.enable" is not set to 0 (Disabled). It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled **1**-Enabled, when "features.doorphone.X.autopreview.enable" is set to 0 (Disabled), users can tap **Preview** to check the visitor's video when receiving a visitor's incoming call. And the phone will stop playing the ringtone. |
| **Default** | 0 |

| Web UI | Features->Door Phone->Video Preview | |
|---|---|---|
| **Parameter** | features.doorphone.X.autopreview.enable[1] | \<y0000000000xx\>.cfg |
| **Description** | It enables or disables the phone to preview the visitor's video automatically when receiving a visitor's incoming call.<br><br>**Note**: It works only if "features.doorphone.X.videopreview.enable" is set to 1 (Enabled), "account.X.auto_answer" is set to 0 (Disabled) and "video.enable" is not set to 0 (Disabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled, the phone will display the visitor's video automatically when receiving a visitor's incoming call. And the phone keeps playing the ringtone. | |
| **Default** | 0 | |
| **Web UI** | Features->Door Phone->Auto Preview | |
| **Parameter** | features.doorphone.X.httpapi.username[1] | \<y0000000000xx\>.cfg |
| **Description** | It configures the user name for HTTP API authentication.<br><br>**Note**: It is required only when the IP intercom needs the HTTP API authentication. It is not applicable to CP960 phones. | |
| **Permitted Values** | String within 99 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Door Phone->User Name | |
| **Parameter** | features.doorphone.X.httpapi.password[1] | \<y0000000000xx\>.cfg |
| **Description** | It configures the password of HTTP API authentication.<br><br>**Note**: It is required only when the IP intercom needs the HTTP API authentication. It is not applicable to CP960 phones. | |
| **Permitted Values** | String within 99 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Door Phone->Password | |

[1]X ranges from 1 to 99.

# Android Keys Display

Android keys are displayed on the bottom of the touch screen. You can hide the Android keys.
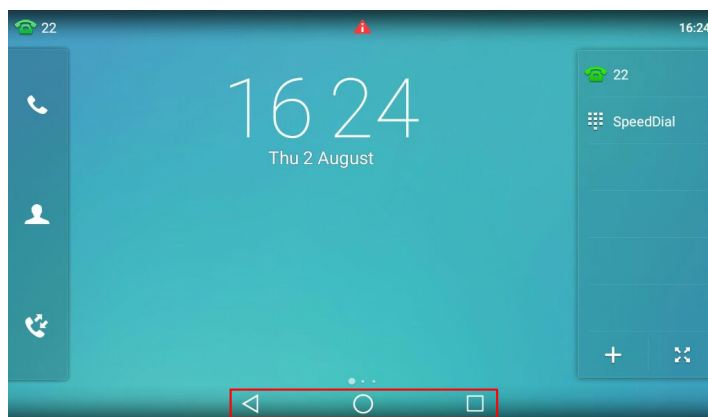
It is only applicable to VP59/T58A phones.

## Topic

## Android Keys Display Configuration

The following table lists the parameter you can use to configure whether to display the Android keys or not.

| Parameter | features.system_funtion_bar.hide[1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables to hide the Android keys from the phone screen.<br>**Note**: It is only applicable to VP59/T58A 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.

## Status Bar and Control/Notification Center Display

The status bar is used to display the phone's default account, some feature status icons and time. The control center or notification center allows users to access common features or view important notifications quickly.

You can disable the phone to display the status bar and control/notification center.

It is only applicable to VP59/T58A phones.

## Topic

## Status Bar and Control/Notification Center Display Configuration

The following table lists the parameter you can use to configure the status bar and control/notification center display.

| Parameter | features.status_bar.hide[1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables to hide the status bar and the control/notification center for the phone.<br>**Note**: It is only applicable to VP59/T58A phones. | |
| Permitted | **0**-Disabled | |

| Values | **1**-Enabled |
|---|---|
| Default | 0 |

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

# Warnings Display

Yealink phones support displaying a warning icon in the status bar, and warning information in the **Status** screen (**General** screen for CP960) when the default password is used. It is used to remind users to change the default password as soon as possible.

## 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<br>**1**-Enabled | |
| Default | 1 | |

# Browser Home Page

When launching the **Browser** on the phone, the default home page is the Yealink website. You can set the web page that you visit the most frequently as the home page.

## Topic

Browser Home Page Configuration

## Browser Home Page Configuration

The following table lists the parameter you can use to configure the browser home page.

| Parameter | phone_setting.browser.url | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the URL of the browser home page. | |
| Permitted Values | String | |
| Default | https://www.yealink.com | |

# Account Settings

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

## Topics

# Account Registration

Registering an account makes it easier for the phones to receive an incoming call or dial an outgoing call. Yealink phones support registering multiple accounts on a phone (CP960 phones only support registering one SIP account); each account requires an extension or phone number.

## Topics

## Supported Accounts

The number of the registered accounts must meet the following:

| Phone Model | Accounts |
|---|---|
| VP59/T58A | <=16 |
| CP960 | 1 |

## 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.<br>**1**-Enabled | |
| **Default** | 0 | |
| **Web UI** | Account->Register->Line Active | |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Accounts->Activation | |
| **Parameter** | account.X.label[1] | <MAC>.cfg |
| **Description** | It configures the label to be displayed on the phone screen. | |
| **Permitted** | String within 99 characters | |

| Values | |
|---|---|
| **Default** | Blank |
| **Web UI** | Account->Register->Label |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Accounts->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 |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Accounts->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 |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Accounts->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 |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->802.1x->802.1x Mode |
| **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 |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Accounts->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** | String within 256 characters |

| | |
|---|---|
| **Values** | |
| **Default** | Blank |
| **Web UI** | Account->Register->SIP Server Y->Server Host |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Network->802.1x->802.1x Mode |
| **Parameter** | account.X.sip_server.Y.port[1][2]      <MAC>.cfg |
| **Description** | It configures the port of SIP server Y.<br>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 |
| **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<br>**1**-Enabled |
| **Default** | 0 |
| **Web UI** | Account->Register->Enable Outbound Proxy Server |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Accounts->Outbound Status |
| **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.<br>**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 |
| **Phone UI** | Settings->Advanced Settings (default password: admin) ->Accounts->Outbound ProxyY |
| **Parameter** | account.X.outbound_proxy.Y.port[1][2]      <MAC>.cfg |
| **Description** | It configures the port of the outbound proxy server Y.<br>**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 |
| **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) |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

[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** | **0**-Disabled<br>**1**-Enabled | |
| **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** | **0**-Disabled<br>**1**-Enabled | |
| **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.<br>For VP59/T58A: 0~15 stand for line1~line16;<br>For CP960: 0 stands for line1. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Web UI** | Account->Advanced->SIP Send Line | |
| **Parameter** | account.X.contact_take_line_param[1] | <MAC>.cfg |
| **Description** | It enables or disables the phone to carry the line parameter in the Contact header of the Register message. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **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<br>**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<br>**2**-BroadSoft (It works only if "bw.enable" is set to 1 (Enabled)) | |
| **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<br>**1**-Enabled | |
| **Default** | 0 | |
| **Web UI** | Account->Advanced->Subscribe Register | |
| **Parameter** | account.X.register_expires_overlap[1] | <MAC>.cfg |
| Description | It configures the renewal time (in seconds) away from the registration lease.<br><br>**Note**: The re-register time negotiated with the server may be different. The phone will attempt to re-register at the beginning of the overlap period. For example, if expires="120" (configured by the parameter "account.X.sip_server.Y.expires") and overlap="30", the phone will re-register after 90 seconds (120−30). | |
| **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 | |

| Parameter | account.X.instance_id.enable | <MAC>.cfg |
|---|---|---|
| Description | It enables or disables the phone to add *+sip.instance* attribute to the Contact header of the REGISTER message. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled | |
| Default | 0 | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

[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.<br><br>**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.<br><br>**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.
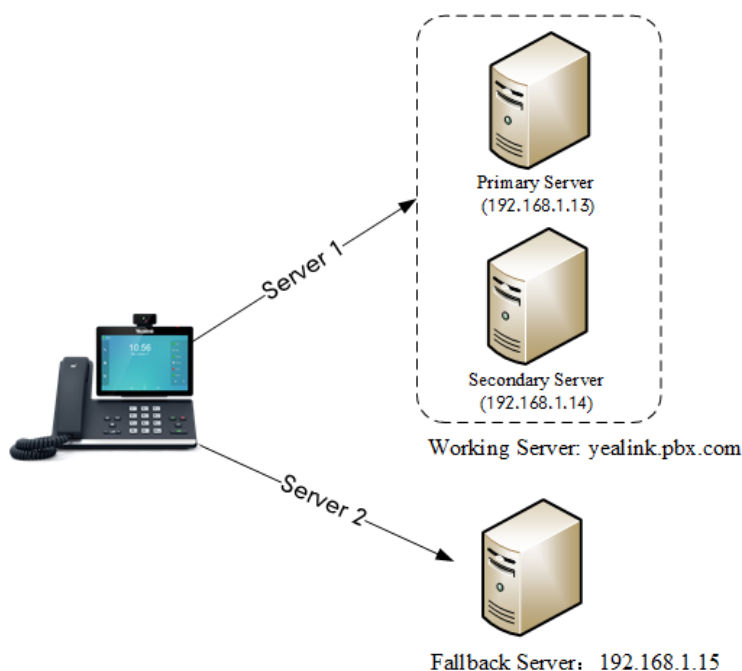


- **Working Server**: Server 1 is configured with the domain name of the working server. For example: yealink.pbx.com. DNS mechanism is used such that the working server is resolved to multiple servers with different IP addresses for failover purpose. The working server is deployed in redundant pairs, 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

# 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.<br><br>**Note**: It is not applicable to outbound proxy servers. | |
| Permitted Values | **0**-Concurrent registration<br><br>**1**-Successive registration | |

| | |
|---|---|
| **Default** | 0 |
| **Parameter** | account.X.fallback.timeout[1] <br> <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. <br><br> **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] <br> <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. <br><br> **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 |
| **Phone UI** | Settings->Advanced Setting (default password: admin) ->Accounts->AccountX->Proxy Fallback Interval |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

## 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] <br> <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. <br><br> **1**-Enabled, the phone will register to the secondary server first, and then send the requests to it. |
| **Default** | 0 |
| **Parameter** | account.X.sip_server.Y.expires[1][2] <br> <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] <br> <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.failback_mode[1][2] <td><MAC>.cfg</td> |
| **Description** | It configures the mode for the phone to retry the primary server in failover. <br><br>**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. <br><br>**1**-DNSTTL: the phone will send requests to the last registered server first. If the time defined by DNSTTL on the registered server expires, the phone will retry to send requests to the primary server. <br><br>**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. <br><br>**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. |
| **Default** | 0 |
| **Parameter** | account.X.sip_server.Y.failback_timeout[1][2] <td><MAC>.cfg</td> |
| **Description** | 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. <br><br>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. <br><br>If you set the parameter between 1 and 59, the timeout will be 60 seconds. <br><br>**Note**: It works only if "account.X.sip_server.Y.failback_mode" is set to 3 (duration). |
| **Permitted Values** | 0, Integer from 60 to 65535 |
| **Default** | 3600 |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

[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<br><br>**1**-TCP<br><br>**2**-TLS<br><br>**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 | |
| 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<br><br>**1**-SRV query using UDP, TCP and TLS. | |
| 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 | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

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

## 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

# 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.<br><br>**1**-Use DNS cache, but do not record the additional records.<br><br>**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<br><br>**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.<br><br>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 **SIP+D2S**: SIP over SCTP **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.<br><br>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<br>**1**-Enabled | |
| **Default** | 1 | |
| **Parameter** | static.network.dns.last_cache_expired | <y0000000000xx>.cfg |
| **Description** | It configures the validity period of the expired DNS cache.<br><br>**Note**: It works only if "static.network.dns.last_cache_expired.enable" is set to 1 (Enabled). | |
| **Permitted Values** | Integer from 0 to 65535<br><br>**0**-the expired DNS cache can only be used once. After using, the phone will perform a DNS query again.<br><br>**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<br>**1**-Enabled | |
| **Default** | 0 | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

[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.

# Logon Wizard

Logon wizard allows the phones to provide the logon wizard during the first startup. It works only if there is no registered account on the IP phone.

## Topic

Logon Wizard Configuration

## Logon Wizard Configuration

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

| **Parameter** | phone_setting.logon_wizard | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the phone to provide the logon wizard after startup when there is no registered account. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Web UI** | Features->General Information->Logon Wizard | |

| Parameter | hotdesking.startup_register_name_enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to provide input field of register name on the logon wizard after startup when there is no registered account.<br><br>**Note**: It works only if "phone_setting.logon_wizard" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Parameter | hotdesking.startup_username_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to provide input field of user name on the logon wizard after startup when there is no registered account.<br><br>**Note**: It works only if "phone_setting.logon_wizard" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Parameter | hotdesking.startup_password_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to provide input field of password on the logon wizard after startup when there is no registered account.<br><br>**Note**: It works only if "phone_setting.logon_wizard" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Parameter | hotdesking.startup_sip_server_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to provide input field of SIP server on the logon wizard after startup when there is no registered account.<br><br>**Note**: It works only if "phone_setting.logon_wizard" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Parameter | hotdesking.startup_outbound_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to provide input field of the outbound server on the logon wizard after startup when there is no registered account.<br><br>**Note**: It works only if "phone_setting.logon_wizard" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Parameter | phone_setting.logon_wizard_forever_wait | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to remain at the hot desking logon wizard even though timeout. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |

| Default | 0 |
|---|---|

# Multiple Line Keys per Account

You can assign multiple line keys to associate with a specific account. The line keys are automatically assigned with Line type from the first unused one (unused one means the line key is configured as N/A or the associated account is not registered). All calls on this account will be distributed evenly among these line keys. It is useful for managing a high volume of calls to an account.

## Topics

Multiple Line Keys per Account Configuration
Default Account

## Multiple Line Keys per Account Configuration

The following table lists the parameters you can use to configure multiple line keys per account.

| Parameter | features.auto_linekeys.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables to assign multiple line keys to associate with a specific account.<br><br>**Note**: The number of the line keys is determined by "account.X.number_of_linekey". | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Features->General Information->Auto Linekeys | |
| Parameter | account.X.number_of_linekey[1] | <MAC>.cfg |
| Description | It configures the number of line keys to be assigned with a specific account from the first unused one.<br><br>If a line key is in used, the phone will skip to the next unused DSS key. | |
| Permitted Values | Integer from 1 to 999<br><br>The number of the line keys varies by phone models, for the supported line keys, refer to Supported DSS Keys. | |
| Default | 1 | |
| Web UI | Account->Advanced->Number of Line Key | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

## Default Account

If there are multiple accounts registered on the phone, the phone will use the default account to dial out by default.

You can tap the label of the default account on the top-left of the idle screen, and then tap the desired account to be the new default account. This is only applicable to VP59/T58A phones.

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

| Parameter | static.features.default_account | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the default account.<br><br>**1**-Account 1 | |

| | |
|---|---|
| | **2**-Account 2<br><br>**3**-Account 3<br><br>...<br><br>**16**-Account 16<br><br>For VP59/T58A, accounts 1-16.<br><br>**Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | Integer from 1 to 16 |
| **Default** | 1 |

| **Parameter** | features.linekey_call_with_default_account | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the phone to switch the default account when pressing the line key to dial.<br><br>For example, the account on line 2 is not the default account, if this feature is enabled, when tapping the line key 2 to dial, the default account will switch to the account on line 2.<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |

# Directory

The Yealink IP phone provides several types of phone directories.

## Topics

# Local Directory

Yealink phones maintain a local directory that you can use to store contacts. The local directory can store up to 1000 contacts and 48 groups.

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

## Preparing the Tar Formatted File

This section provides you on how to package the tar file using 7-Zip.

> **Note**
>
> You can package the tar formatted file using the tool 7-Zip or GnuWin32. You can download 7-Zip online: http://www.7-zip.org/ and GnuWin32 online: http://gnuwin32.sourceforge.net/packages/gtar.htm.
> The procedure may be different if you package the tar formatted file using other software that is not listed above.

### Procedure

1. Download and install 7-Zip on the local system.
2. Create a folder (for example, photo) on the local system (for example, C:\Program Files) and place the file that will be compressed (for example, cutom1.jpg, cutom2.png) to this folder.
3. Start the 7-Zip file manager application (7zFM.exe).
4. Locate the photo folder from the local system (C:\Program Files\photo\).
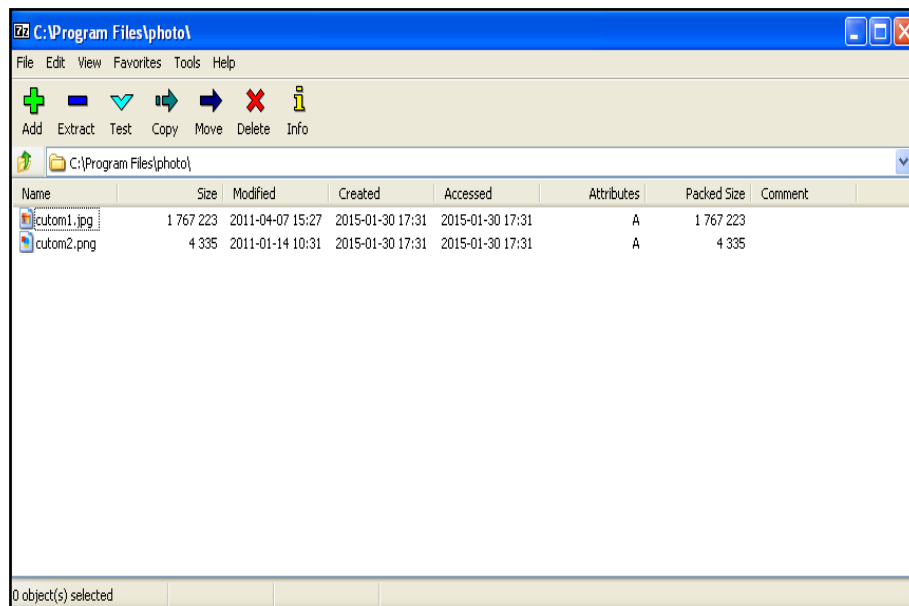
**5.** Select the desired photos that will be compressed.

**6.** Click the **Add** button.

**7.** Select **tar** from the pull-down list of **Archive format**.
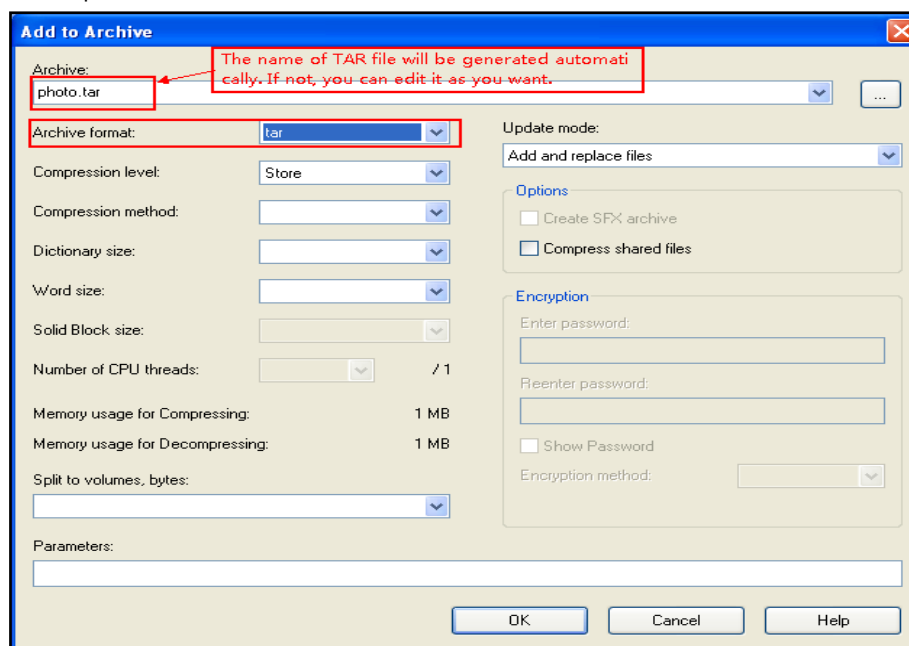


**8.** Click the **OK** button.

A photo.tar file is generated in the directory C:\Program Files\photo.

## 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 |
|---|---|---|
| group | display_name | Specify the group name.<br><br>For example: All Contacts or Blacklist |
| | ring | Specify a ringtone for the group.<br><br>System ring tone:<br><br>Auto<br><br>Silent.wav<br><br>Splash.wav<br><br>RingN.wav (integer N ranges from 1 to 8)<br><br>Custom ring tone:<br><br>Name.wav (the custom ring tone should be uploaded in advance) |
| Contact | display_name | Specify the contact name.<br><br>For example: Jim<br><br>**Note**: The contact name cannot be blank or duplicated. |
| | office_number | Specify the office number or macro EDK Macro Strings |
| | mobile_number | Specify the mobile number or macro EDK Macro Strings |
| | other_number | Specify the other number or macro EDK Macro Strings |
| | line | Specify a registered line for this contact for calling.<br><br>Valid Values: -1~15;<br><br>-1 stands for Auto (the first registered line);<br><br>0~15 stand for line1~line16.<br><br>**Note**: It is not applicable to CP960 phones. |
| | ring | Specify a ringtone for this contact.<br><br>System ring tone:<br><br>Auto<br><br>Silent.wav<br><br>Splash.wav<br><br>RingN.wav (integer N ranges from 1 to 8)<br><br>Custom ring tone:<br><br>XX.wav (for example, Music.wav, the custom ring tone should be uploaded in advance) |
| | group_id_name | Specify which group the contact adds to. |

| Elements | Attributes | Description |
|---|---|---|
| | | Built-in group:<br><br>All Contacts, Blacklist<br><br>Custom group:<br><br>XXX (for example, Friend) |
| | default_photo | Built-in avatar:<br><br>Resource: avatar name and icon name<br><br>Custom avatar:<br><br>Config: custom avatar name and icon name |

## 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 group, add <group display_name="" ring=""/> to the file. Each starts on a new line.
3. To add a contact, add <contact display_name="" office_number="" mobile_number="" other_number="" line="" ring="" group_id_name="" default_photo="" auto_divert = ""/> to the file. Each starts on a new line.
4. Specify the values within double quotes.

    For example:

    <group display_name="Friend" ring="Splash.wav"/>

    <contact display_name="Lily"office_number="1020" mobile_number="1021" other_number="1112" line="1" ring="Ring1.wav" group_id_name="Friend" default_photo="Lily_photo.jpg" auto_divert = "2022"/>

    <contact display_name="Tom" office_number="2020" mobile_number="2021" other_number="2112" line="2" ring="Ring1.wav" group_id_name="Friend" default_photo=" Resource:icon_family_b.png" auto_divert = "2023" />

5. 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, or upload the contact resource, such as contact avatar.

The following table lists the parameters you can use to upload the local contact files and resource.

| Parameter | local_contact.data.url | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the access URL of the local contact file (*.xml).<br><br>**Example**:<br><br>local_contact.data.url = http://192.168.10.25/contact.xml<br><br>**Note**: If "static.auto_provision.local_contact.backup.enable" is set to 1 (Enabled), the contacts in the contact file "contact.xml" downloaded from the provisioning server do not take effect. | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |

| Web UI | Directory->Local Directory->Import Local Directory File | |
|---|---|---|
| **Parameter** | local_contact.photo.url | <y0000000000xx>.cfg |
| **Description** | It configures the access URL of a contact avatar file. The format of the contact avatar must be *.png, *.jpg, *.bmp, *.jpeg. The contact avatar file should be uploaded to the provisioning server in advance. **Example**: local_contact.photo.url = tftp://192.168.10.25/Photo.jpg | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Parameter** | local_contact.image.url | <y0000000000xx>.cfg |
| **Description** | It configures the access URL of a TAR contact avatar file. The format of the contact avatar must be *.png, *.jpg, *.bmp, *.jpeg. The contact avatar file should be compressed as a TAR file in advance and then place it to the provisioning server. **Example**: local_contact.image.url = tftp://192.168.10.25/photo.tar | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Parameter** | local_contact.data_photo_tar.url | <y0000000000xx>.cfg |
| **Description** | It configures the access URL of the compressed TAR file consisting of the avatars TAR file and contact XML file. All avatars needed for contacts should be compressed as a TAR file in advance. **Example**: local_contact.data_photo_tar.url = tftp://192.168.10.25/Contact.tar | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Parameter** | local_contact.icon.url | <y0000000000xx>.cfg |
| **Description** | It configures the access URL of a TAR contact icon file. The format of the contact icon must be *.png, *.jpg, *.bmp. The contact icon file should be compressed as a TAR file in advance and then place it to the provisioning server. **Example**: local_contact.icon.url = tftp://192.168.10.25/photo2.tar | |
| **Permitted** | URL within 511 characters | |

| Values | |
|---|---|
| Default | Blank |

## Example: Adding Contacts Using a Contact File

The following example shows the configuration for customizing a local contact file.

Customize the contact file "contact.xml" and place the contact file "contact.xml" and custom contact source (avatars or icons) to the provisioning server "http://192.168.10.25".

**Example**

*local_contact.photo.url = http://192.168.10.25/Lily_photo.jpg*

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

During auto provisioning, the phone connects to the provisioning server "192.168.10.25", and downloads the local contact file "contact.xml" and an avatar "Lily_photo.jpg". You can view the contacts on their phone, and specify the avatar "Lily_photo.jpg" for a contact.

## Local Contacts Backup

Yealink phones support storing all local contacts to a contact file named <MAC>-contact.xml. You can back up this file to the server, avoiding data loss. Once the contacts update, the phone will automatically upload this file to the provisioning server or a specific server. If a contact file exists on the server, this file will be overridden. The phone will request to download the <MAC>-contact.xml file according to its MAC address from the server during auto provisioning.

The contact file is named after the MAC address of the IP phone. For example, if the MAC address of an IP phone is 00156574B150, the name of the contact file is 00156574B150-contact.xml (uppercase).

| 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 phone. |

The following table lists the parameters you can use to back up the local contacts.

| Parameter | static.auto_provision.local_contact.backup.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to upload the <MAC>-contact.xml file to the server each time the contacts update and download the <MAC>-contact.xml file from the server during auto provisioning.<br><br>**Note**: It does not affect the downloading of the contact avatar/icon files. | |
| Permitted Values | **0**-Disabled, the phone will not upload the contact file "<MAC>-contact.xml" to the server, so the IP phone downloads the contacts in the "contact.xml" from the access URL configured by the parameter "local_contact.data.url" or "local_contact.data_photo_tar.url" during auto provisioning.<br><br>**1**-Enabled, the phone uploads the contact file "<MAC>-contact.xml" to the specific path configured by the parameter "static.auto_provision.local_contact.backup.path" each time the contacts update; and downloads the contacts in the "<MAC>-contact.xml" according to its MAC address from the specific path during auto provisioning. | |
| Default | 0 | |
| Parameter | static.auto_provision.local_contact.backup.path | <y0000000000xx>.cfg |
| Description | It configures a path or URL for the phone to upload/download the <MAC>-contact.xml file. | |

| | |
|---|---|
| | If it is left blank, the phone connects to the provisioning server URL, and uploads/downloads the contact file "<MAC>-contact.xml". <br><br> **Example**: <br><br> static.auto_provision.local_contact.backup.path = http://192.168.1.20/contact <br><br> Once the contacts update, the phone will upload the contact file to the specified path "http://192.168.1.20/contact". <br><br> During auto provisioning, the phone downloads the contact file "<MAC>-contact.xml" from the specified path "http://192.168.1.20/contact". <br><br> **Note**: It works only if "static.auto_provision.local_contact.backup.enable" is set to 1 (Enabled). |
| **Permitted Values** | String |
| **Default** | Blank |
| **Parameter** | static.auto_provision.custom.upload_method     <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 <br> **1**-POST |
| **Default** | 0 |

# Google Contacts

Yealink IP phone supports Google contacts feature. After enabling Google contacts on the phone, users can get Google contacts from their Google accounts.

To use this feature, you need to install the GMS core package, and then the user should add Google accounts on the phone. Please ask the distributor or Yealink FAE for the specific version of GMS core package.

It is only applicable to T58A phones.

## Topic

## Google Contacts Configuration

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

| **Parameter** | pm.gms_install_url     <y0000000000xx>.cfg |
|---|---|
| **Description** | It configures the URL of the GMS core package. <br><br> The GMS core package should be a specific version: open_gapps-arm-5.1-pico-20170709.zip. Please ask the distributor or Yealink FAE for the specific version of GMS core package. <br><br> **Example**: <br><br> pm.gms_install_url = http://192.168.10.25/open_gapps-arm-5.1-pico-20170713.zip <br><br> **Note**: It is only applicable to T58A phones. |

| Permitted Values | String | |
|---|---|---|
| **Default** | Blank | |
| **Parameter** | pm.gms_uninstall | <y0000000000xx>.cfg |
| **Description** | It uninstalls the GMS service.<br><br>**Note**: It is only applicable to T58A phones. | |
| **Permitted Values** | Software package name or APK file name or Application name | |
| **Default** | Blank | |
| **Parameter** | google_contact_server.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the Google contacts.<br><br>**Note**: It works only if GMS core package is installed (configured by "pm.gms_install_url") successfully and Google account is added on the phone. It is only applicable to T58A phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Web UI** | Directory->Google Contacts->Google Contacts | |
| **Phone UI** | Settings->Basic Settings->Google Contacts->Google Contacts | |

## GMS Services List

You can disable some GMS services on the phone.

The following lists all the GMS services you can disable on the phone:

| APK Filename/Software Package Name | Description |
|---|---|
| com.google.android.onetimeinitializer | One-time initialization on first startup. |
| com.google.android.configupdater | Allows updating the unexecutable system components in the wireless network. |
| com.google.android.setupwizard | Out-of-the-box user experience. |
| com.google.android.partnersetup | The initialization service for partner dedicated equipment. |
| com.google.android.feedback | Allows users to send error reports and give feedback about *GoogleLoginService* to Google. |
| com.google.android.syncadapters.calendar | Syncs calendar data to the user's Google account. |
| com.google.android.backuptransport | Backs up data to the user's Google account. |
| com.android.vending | Playstore |

| Note |
|---|
| Disabling GMS services listed above will not affect the use of Google contacts. It can reduce CPU consumption and have a positive performance impact for the phone. |

**Related Topic**

## Example: Configuring the Google Contacts Feature

This section shows an example for you about how to configure Google contacts feature for users.

**Procedure**

1. Ask the distributor or Yealink FAE for the GMS core package (open_gapps-arm-5.1-pico-20170709.zip).
2. Place the GMS core package on the provisioning server "192.168.10.25".
3. Install the GMS core on the phone.

   **Example**

   *pm.gms_install_url = http://192.168.10.25/open_gapps-arm-5.1-pico-20170709.zip*

   After provisioning, there are two applications (**Google Settings** and **Play Store**) added on the second idle screen after phone reboot.
4. Disable some GMS services on the phone.

   **Example**

   ####Multiple GMS servicess are separated by slashs.####

   *app.unavailable = com.google.android.onetimeinitializer/com.google.android.configupdater*
5. Add a Google account via phone user interface: **Settings**->**APP Accounts**->**Add account**->**Google**.
6. Enable Google Contacts feature on the phone.

   *google_contact_server.enable = 1*

   After provisioning, the **Google Contacts** directory appears on the phone. Users can add, edit, delete or search for a Google contact on the phone.

**Related Topics**

## 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

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

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

## 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<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Directory->LDAP->Enable LDAP | |
| Parameter | ldap.name_filter | <y0000000000xx>.cfg |
| Description | It configures the search criteria for LDAP contact names look up.<br><br>The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the name entered by the user.<br><br>**Example**:<br><br>ldap.name_filter = (\|(cn=%)(sn=%))<br><br>When the cn or sn of the LDAP contact matches the entered name, the record will be displayed on the phone screen.<br><br>ldap.name_filter = (&(cn=*)(sn=%))<br><br>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.<br><br>ldap.name_filter = (!(cn=%))<br><br>When the cn of the LDAP contact does not match the entered name, the records will be displayed on the phone screen. | |
| Permitted | String within 99 characters | |

| Values | |
|---|---|
| **Default** | Blank |
| **Web UI** | Directory->LDAP->LDAP Name Filter |
| **Parameter** | ldap.number_filter | <y0000000000xx>.cfg |
| **Description** | It configures the search criteria for LDAP contact numbers look up.<br><br>The "*" symbol in the filter stands for any number. The "%" symbol in the filter stands for the number entered by the user.<br><br>**Example**:<br><br>ldap.number_filter = (\|(telephoneNumber=%)(mobile=%)(ipPhone=%))<br><br>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.<br><br>ldap.number_filter = (&(telephoneNumber=*)(mobile=%))<br><br>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. |
| **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** | **0**-LDAP—The unencrypted connection between the LDAP server and the IP phone (port 389 is used by default).<br><br>**1**-LDAP TLS Start—The TLS/SSL connection between the LDAP server and the IP phone (port 389 is used by default).<br><br>**2**-LDAPs—The TLS/SSL connection between the LDAP server and the IP phone (port 636 is used by default). |
| **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** | Integer from 1 to 65535 |

| | |
|---|---|
| **Values** | |
| **Default** | 389 |
| **Web UI** | Directory->LDAP->Port |

| **Parameter** | ldap.base | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | 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. **Example**: ldap.base = dc=yealink,dc=cn | |
| **Permitted Values** | String within 99 characters | |
| **Default** | Blank | |
| **Web UI** | Directory->LDAP->Base | |

| **Parameter** | ldap.user | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the user name used to log into the LDAP server. 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. **Example**: ldap.user = cn=manager,dc=yealink,dc=cn | |
| **Permitted Values** | String within 99 characters | |
| **Default** | Blank | |
| **Web UI** | Directory->LDAP->User Name | |

| **Parameter** | ldap.password | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the password to log into the LDAP server. 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. | |
| **Permitted Values** | String within 99 characters | |
| **Default** | Blank | |
| **Web UI** | Directory->LDAP->Password | |

| **Parameter** | ldap.max_hits | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | 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. | |
| **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 search results. You can configure multiple name attributes separated by spaces.<br><br>**Example**:<br><br>ldap.name_attr = cn sn<br><br>This requires the "cn" and "sn" attributes set for each contact record on the LDAP server. | |
| **Permitted Values** | String within 99 characters | |
| **Default** | Blank | |
| **Web UI** | Directory->LDAP->LDAP Name Attributes | |
| **Parameter** | ldap.numb_attr | <y0000000000xx>.cfg |
| **Description** | 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.<br><br>**Example**:<br><br>ldap.numb_attr = mobile ipPhone<br><br>This requires the "mobile" and "ipPhone" attributes set for each contact record on the LDAP server. | |
| **Permitted Values** | String within 99 characters | |
| **Default** | Blank | |
| **Web UI** | Directory->LDAP->LDAP Number Attributes | |
| **Parameter** | ldap.display_name | <y0000000000xx>.cfg |
| **Description** | It configures the display name of the contact record displayed on the phone screen.<br><br>The value must start with "%" symbol.<br><br>**Example**:<br><br>ldap.display_name = %cn<br><br>The cn of the contact record is displayed on the phone screen. | |
| **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<br>**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<br>**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<br>**1**-Enabled |
| **Default** | 0 |
| **Web UI** | Directory->LDAP->LDAP Sorting Results |
| **Parameter** | ldap.incoming_call_special_search.enable | <y0000000000xx>.cfg |
| **Description** | 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.<br><br>**Example**:<br><br>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.<br><br>**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. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |
| **Parameter** | ldap.customize_label | <y0000000000xx>.cfg |
| **Description** | It configures the display name of the LDAP phone book.<br><br>If it is left blank, LDAP is displayed.<br><br>**Note**: It works only if "ldap.enable" is set to 1 (Enabled). |

| 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.

> **Note**
>
> We recommend you to download less than 5000 remote contacts from the remote server.

## 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 | `<DirectoryEntry>`<br><br>    `<Name>Contact Name</Name>`<br>    `<Telephone>Contact Number</Telephone>`<br>`<DirectoryEntry>` | Add a contact in a department/group:<br><br>Specify the contact name between `<Name>` and `</Name>`;<br><br>Specify the contact number |

| Template | Element | Valid Values |
|----------|---------|--------------|
| | | between <Telephone> and </Telephone> |
| Menu.xml | <MenuItem><br><br>    <Name>Department</Name><br><br>    <URL>Department URI</URL><br><br></MenuItem> | Add a contact department/group file:<br><br>Specify the department/group name between <Name> and </Name>;<br><br>Specify the department/group access URL between <URL> and</URL> |
| | <SoftKeyItem><br><br>    <Name>#</Name><br><br>    <URL>http://10.2.9.1:99/Department.xml</URL><br><br></SoftKeyItem> | Specify a department/group file for a key:<br><br>Specify *key, # key or digit key between <Name> and </Name>;<br><br>Specify the department/group access URL between <URL> and</URL> |

## 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 60M. | |
| **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** | 0, Integer from 3600 to 1296000 | |

| Values | |
|---|---|
| **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<br>**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 👤 ->**Remote Phone Book** (**Directory**-> Local Directory ⌄ ->**Remote Phone Book**) to access the corporate directory straight from their phones.

## Directory List for Directory Icon

Users can access frequently used directory lists by tapping the directory icon 👥 when the IP phone is idle. The lists include Local Directory, Remote Phone Book and Blacklist by default.

It is only applicable to CP960 phones.

You can add the desired lists to directory list using a directory list file (favorite_setting.xml).

### Topics

Directory List File Customization
Directory List Configuration
Example: Configuring a Directory List

## Directory List File Customization

You can ask the distributor or Yealink FAE for directory template. You can also obtain the directory template online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage.

### Topics

Directory List File Attributes

Customizing Directory List File

## Directory List File Attributes

The following table lists the attributes you can use to add contact lists to the directory list file. We recommend you do not edit these attributes.

| Attributes | Valid Values | Description |
|---|---|---|
| id_name | localdirectory<br><br>networkcalllog<br><br>remotedirectory<br><br>ldap<br><br>broadsoftdirectory<br><br>uc_buddies (not applicable to CP960 phones)<br><br>mobilecontant (not applicable to CP960 phones)<br><br>blacklist<br><br>googledirectory (not applicable to VP59/CP960 phones) | The existing directory list (For example, "localdirectory" for the local directory list).<br><br>**Note**: Do not edit this field. |
| display_ name | Local Directory<br><br>Network CallLog<br><br>Remote Phone Book<br><br>LDAP<br><br>Network Directories<br><br>Buddies (not applicable to CP960 phones)<br><br>Mobile Contacts (not applicable to CP960 phones)<br><br>Blacklist<br><br>Google Contact  (not applicable to VP59/CP960 phones) | The display name of the directory list.<br><br>**Note**: We recommend you do not edit this field. Network Directories is hidden for phones in GA firmware, GA firmware which is designed for the BroadWorks environment. |
| priority | 1 to 6 (for CP960)<br><br>1 to 9 (for T58A)<br><br>1 to 8 (for VP59)<br><br>**For CP960**:<br><br>1 is the highest priority, 6 is the lowest.<br><br>**For T58A**:<br><br>1 is the highest priority, 9 is the lowest.<br><br>**For VP59**:<br><br>1 is the highest priority, 8 is the lowest. | The display priority of the directory list. |
| enable | 0/1<br><br>**0**: Disabled<br><br>**1**: Enabled | Whether to display this list when you press Directory (Dir) on the phone. |

## Customizing Directory List File

1. Open the directory list XML file.
2. To configure each directory list, edit the values within double quotes in the corresponding field.

   For example, enable the local directory, disable the history and specify a priority.

   <item id_name="localdirectory" display_name="Local Directory" priority="1" enable="1" dev="common"/>

   <item id_name="history" display_name="History" priority="2" enable="0" dev="common"/>
3. Save the change and place this file to the provisioning server.

## Directory List Configuration

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

| Parameter | static.directory_setting.url | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the access URL of the custom directory file (favorite_setting.xml). <br> **Note**: It is only applicable to CP960 phones. | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Directory->Settings->Directory | |

## Example: Configuring a Directory List

The following example shows the configuration for the directory list.

Customize the directory list file, and then place this file to the provisioning server "http://192.168.10.25".

**Example**

*static.directory_setting.url = http://192.168.10.25/favorite_setting.xml*

After provisioning, you can tap the directory icon ( 👤 for VP59/T58A, 👤 for CP960) to access the desired contact

list quickly.

# Directory Search Settings

You can configure how the phones search contacts and whether to highlight the matched keywords for contact searching.

## Topic

Directory Search Settings Configuration

## Directory Search Settings Configuration

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

| Parameter | phone_setting.search.highlight_keywords.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the phone to highlight the matched characters in the search results. | |
| **Permitted Values** | **0**-Disabled <br> **1**-Enabled | |
| **Default** | 0 | |

# 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 Forwarded Calls. Each call log list supports up to 100 entries.

**Topics**

Call Log Display
Call Log Configuration
Call Logs Backup

# 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. |
| Line | Shows which line is used. |
| Duration | Shows the duration of the call. |
| Relation | Shows what happened to the call.<br><br>The valid display contents are:<br><br>• **Reject**: Reject an incoming call.<br>• **Forward to X**: Forward an incoming call to X. For example, **Forward to 1048** means you forward an incoming call to 1048.<br>• **Busy**: The outgoing call is rejected.<br>• **Transfer to X**: Transfer a call to X. For example, **Transfer to 1048** means you transfer a call to 1048.<br>• **X**: Answer a transferred/forwarded call from remote party X; your call is transferred/forwarded to X. For example, **1048** means you answer a transferred/forwarded call from remote party 1048.<br><br>It is configurable by "features.calllog_detailed_information". |

**Related Topic**

Call Log Configuration

# Call Log Configuration

The following table lists the parameters 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** | **0**-Disabled, the phone cannot log the placed calls, received calls, missed calls and the forwarded calls in | | |

| Values | the call lists. <br> **1**-Enabled | |
|---|---|---|
| **Default** | 1 | |
| **Web UI** | Features->General Information->Save Call Log | |
| **Phone UI** | Settings->Features->History Record->History Record | |
| **Parameter** | account.X.missed_calllog[1] | <MAC>.cfg |
| **Description** | It enables or disables the phone to record missed calls. <br><br> **Note:** It works only if "features.save_call_history" is set to 1 (Enabled). | |
| **Permitted Values** | **0**-Disabled <br> **1**-Enabled | |
| **Default** | 1 | |
| **Web UI** | Account->Basic->Missed Call Log | |
| **Parameter** | features.call_log_show_num | <y0000000000xx>.cfg |
| **Description** | It configures the display type of the other party's information in the call log lists. <br><br> **Note**: It works only if "features.save_call_history" is set to 1 (Enabled). | |
| **Permitted Values** | **0**-Name, the name is displayed preferentially; if there is no name, the number is displayed <br><br> **1**-Number <br><br> **2**-Name & Number, the name and number are displayed; if there is no name, the number is displayed | |
| **Default** | 0 | |
| **Web UI** | Features->General Information->Call List Show Number | |
| **Parameter** | features.calllog_detailed_information | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to indicate what happened to the call in the call log lists. <br><br> It is applicable to the following scenarios: <br><br> • Reject an incoming call <br> • Forward an incoming call <br> • The outgoing call is rejected <br> • Transfer a call <br> • Answer a transferred/forwarded call from the remote party; your call is transferred/forwarded to another party. <br><br> **Note**: It works only if "features.save_call_history" is set to 1 (Enabled). | |
| **Permitted Values** | **0**-Disabled <br><br> **1**-Enabled, you can get the detailed call-disposition information at the **History Details** screen of call log item. | |
| **Default** | 1 | |
| **Parameter** | features.save_init_num_to_history.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to log the transfer party's phone number in the call history list. | |
| **Permitted Values** | **0**-Disabled, the phone will log the transfer-to party's phone number in the call history list. <br> **1**-Enabled | |

| Default | 1 | |
|---|---|---|
| **Parameter** | features.local_calllog.received.replace_rule | <y0000000000xx>.cfg |
| **Description** | It configures the string of the digit map to be applied to the caller ID for incoming calls before it is recorded to call history list.<br><br>**Example**:<br><br>features.local_calllog.received.replace_rule = <00:+>x.\|<5:1>xx<br><br>When the caller's phone number is 001234567, then +1234567 is recorded in the call history list because "001234567" matches the "<00:+>x." in the digit map;<br><br>When the caller's phone number is 532, then 132 is recorded in the call history list because "532" matches the "<5:1>xx" in the digit map. | |
| **Permitted Values** | String | |
| **Default** | Blank | |

## Related Topic

<span style="color:blue">Basic Regular Expression Syntax for Digit Map</span>

# Call Logs Backup

Yealink phones support storing all call logs to a call log file named <MAC>-calllog.xml. You can back up this file to the server, avoiding data loss. Once the call logs update, the phone will automatically upload this file to the provisioning server or a specific server. If a call log file exists on the server, it will be overridden. The phone will request to download the <MAC>-calllog.xml file according to its MAC address from the server during auto provisioning.

The call log file is named after the MAC address of the IP phone. For example, if the MAC address of an IP phone is 00156574B150, the name of the call log file is 00156574B150-calllog.xml (uppercase).

| **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 IP phone. |

The following table lists the parameters you can use to back up the call log.

| **Parameter** | static.auto_provision.local_calllog.backup.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the phone to upload the <MAC>-calllog.xml file to the server each time the call logs update and download the <MAC>-calllog.xml file from the server during auto provisioning. | |
| **Permitted Values** | **0**-Disabled, the phone does not upload/download the call log file "<MAC>-calllog.xml" to the server.<br><br>**1**-Enabled, the phone uploads the call log file "<MAC>-calllog.xml" to the specific path configured by the parameter "static.auto_provision.local_calllog.backup.path" each time the call logs update; and downloads the call logs in the "<MAC>-calllog.xml" according to its MAC address from the specific path during auto provisioning. | |
| **Default** | 0 | |
| **Parameter** | static.auto_provision.local_calllog.backup.path | <y0000000000xx>.cfg |
| **Description** | It configures a path or URL for the phone to upload/download the <MAC>-calllog.xml file.<br><br>If it is left blank, the phone connects to the provisioning server URL, and uploads/downloads the contact | |

| | file "<MAC>-calllog.xml". |
|---|---|
| | **Example**: |
| | static.auto_provision.local_calllog.backup.path = http://192.168.1.20/calllog |
| | Once the call logs update, the phone will upload the call log file to the specified path "http://192.168.1.20/calllog". |
| | During auto provisioning, the phone downloads the call log file "<MAC>-calllog.xml" from the specified path "http://192.168.1.20/calllog". |
| | **Note**: It works only if "static.auto_provision.local_calllog.backup.enable" is set to 1 (Enabled). |
| **Permitted Values** | String |
| **Default** | Blank |
| **Parameter** | static.auto_provision.local_calllog.write_delay.ter-minated | <y0000000000xx>.cfg |
| **Description** | It configures the delay time (in seconds) for the phone to upload the <MAC>-calllog.xml file each time the call logs update. |
| | **Note**: It works only if "static.auto_provision.local_calllog.backup.enable" is set to 1 (Enabled) |
| **Permitted Values** | Integer from 10 to 600 |
| **Default** | 60 |
| **Parameter** | static.auto_provision.custom.upload_method | <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<br>**1**-POST |
| **Default** | 0 |

# Call Features

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

### Topics

## Dial Plan Defined by Four Patterns (Old Dial Plan Mechanism)

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 100 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.

| Note |
|------|
| If you enable a new dial plan mechanism, old dial plan will be ignored. For more information on the new dial plan, refer to Dial Plan Defined by Digit Map (New Dial Plan Mechanism). |

### Topics

## Basic Regular Expression Syntax for Four Patterns

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

| Regular expression | Description |
|---|---|
| . | The dot "." can be used as a placeholder or multiple placeholders for any string. Example: <br><br> "12." would match "123", "1234", "12345", "12abc", and so on. |
| x | The "x" can be used as a placeholder for any character. Example: <br><br> "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: <br><br> "[5-7]" would match the number "5", "6" or "7". |
| , | The comma "," can be used as a separator within the bracket. Example: <br><br> "[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: <br><br> "91[5-7]1234"would match "91**5**1234", "91**6**1234", "91**7**1234". |
| () | The parenthesis "( )" can be used to group together patterns, for instance, to logically combine two or more patterns. Example: <br><br> "([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: <br><br> 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**235**4**599**". "$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

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. |
| Replace | Specify the alternate string instead of what the user enters. |
| LineID | Specify a registered line to apply the replace rule. Valid Values: 0~16 (VP59/T58A); 0, 1 (CP960) 0 stands for all lines; 1~16 stand for line1~line16 (VP59/T58A) 1 stand for line1 (CP960) 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 100 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

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.<br><br>Valid Values:<br><br>0~16 (VP59/T58A)<br><br>0, 1 (CP960)<br><br>0 stands for all lines;<br><br>1~16 stand for line1~line16 (VP59/T58A)<br><br>1 stand for line1 (CP960)<br><br>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.<br>**Note**: It works only if "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). | |
| **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.<br><br>The entered number is configured by "dialplan.replace.prefix.X".<br><br>**Note**: It works only if "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). | |
| **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.<br><br>Multiple line IDs are separated by commas.<br><br>**Note**: It works only if "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). | |
| **Permitted Values** | 0 to 16 (for VP59/T58A)<br><br>0, 1 (for CP960) | |
| **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.<br><br>For customizing replace rule template file, refer to Replace Rule File Customization.<br><br>**Note**: It works only if "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). | |
| **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** | It configures the dial now rule (the string used to match the numbers entered by the user).<br><br>When entered numbers match the predefined dial now rule, the phone will automatically dial out the numbers without pressing the send key.<br><br>**Example**:<br><br>dialplan.dialnow.rule.1 = 123<br><br>**Note**: It works only if "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). | |
| **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** | It configures the desired line to apply the dial now rule. | |

| | The digit 0 stands for all lines. If it is left blank, the dial-now rule will apply to all lines on the phone. |
|---|---|
| | **Note**: Multiple line IDs are separated by commas. It works only if "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). |
| **Permitted Values** | 0 to 16 (for VP59/T58A)<br><br>0, 1 (for CP960) |
| **Default** | Blank |
| **Web UI** | Settings->Dial Plan->Dial Now->Account |
| **Parameter** | phone_setting.dialnow_delay | <y0000000000xx>.cfg |
| **Description** | It configures the delay time (in seconds) for the dial now rule.<br><br>When entered numbers match the predefined dial now rule, the phone will automatically dial out the entered number after the designated delay time.<br><br>If it is set to 0, the phone will automatically dial out the entered number immediately.<br><br>**Note**: It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). |
| **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** | It configures the access URL of the dial now template file.<br><br>For customizing dial now template file, refer to Dial Now File Customization.<br><br>**Note**: It works only if "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). |
| **Permitted Values** | String within 511 characters |
| **Default** | Blank |

[1]X is from 1 to 100.

## 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.<br><br>**Note**: The length of the entered number must be between the minimum length configured by the parameter "dialplan.area_code.min_len" and the maximum length configured by the parameter "dialplan.area_code.max_len". It works only if "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). | |
| **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.<br><br>**Note**: It works only if "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). | |
| **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.<br><br>**Note**: The value must be larger than the minimum length. It works only if "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). | |
| **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.<br><br>**Note**: Multiple line IDs are separated by commas. It works only if "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). | |
| **Permitted Values** | 0 to 16 (for VP59/T58A)<br><br>0, 1 (for CP960) | |
| **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.<br><br>**Example**:<br><br>dialplan.block_out.number.1 = 4321<br><br>When you dial the number "4321" on your phone, the dialing will fail and the phone screen will prompt "Forbidden Number".<br><br>**Note**: It works only if "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). | |

| 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.<br><br>**Note**: Multiple line IDs are separated by commas. It works only if "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). | |
| Permitted Values | 0 to 16 (for VP59/T58A)<br>0, 1 (for CP960) | |
| 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.

# Dial Plan Defined by Digit Map (New Dial Plan Mechanism)

Digit maps, described in RFC 3435, are defined by a single string or a list of strings. If a number entered matches any string of a digit map, the call is automatically placed. If a number entered matches no string - an impossible match - you can specify the phone's behavior. You can specify the digit map timeout, the period of time before the entered number is dialed out.

## Topics

Basic Regular Expression Syntax for Digit Map
Digit Map for All Lines Configuration
Digit Map for a Specific Line Configuration

## Basic Regular Expression Syntax for Digit Map

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

| T | The timer letter "T" indicates a timer expiry. If "T" is used alone (for example, 123T), the default timeout value of 3 will be used. If "T" is not used alone (for example, 123<Tx>, x can be a digit from 0 to 99), a complete match occurs when waiting x seconds after inputting 123. |
|---|---|
| x | The "x" can be used as a placeholder for any digit from 0 to 9. |

| | |
|---|---|
| | Example: |
| | "12x" would match "121", "122", "123", and so on. |
| [] | The square bracket "[]" can be used as a placeholder for a single character which matches any of a set of characters. Example: |
| | "91[5-7]1234" would match "91**5**1234", "91**6**1234", "91**7**1234". |
| - | The dash "-" can be used to match a range of digits within the brackets. |
| | Example: |
| | "[35-7]" would match the number "3", "5", "6" or "7". |
| | **Note**: The digits must be concrete, for example, [3-x] is invalid. |
| · | The dot "." can be used as a placeholder or multiple placeholders, including zero, of occurrences of the preceding construct. |
| | Examples: |
| | "123.T" would match "123", "1233", "12333", "123333", and so on. |
| | "x.T" would match an arbitrary number. |
| | "[x*#+].T" would match an arbitrary character. |
| | **Note**: If the string ends with a dot (for example, 123.), a match will occur immediately after inputting the characters before the dot (e., 123) since the dot allows for zero occurrences of the preceding construct. Therefore, we recommend you to add a letter "T" after the dot (for example, 123.T) for inputting more characters. |
| R | The letter "R" indicates that certain matched strings are replaced. Using an RRR syntax, you can replace the digits between the first two Rs with the digits between the last two Rs. Example: |
| | "R12R234R" would replace **12** with **234**. |
| <:> | The letter ":" in the angle bracket indicates that certain matched strings are replaced. Using the <:> syntax, you can replace the digits before the colon with the digits after the colon. |
| | Example: |
| | "<12:234>" would replace **12** with **234**. It is the same with R12R234R. |
| ! | The exclamation mark "!" can be used to prevent users from dialing out specific numbers. It can only be put last in each string of the digit map. |
| | Example: |
| | "235x!" would match "2351", "2352", "2353", and so on. The number starting with 235 will be blocked to dial out. |
| , | The comma "," can be used as a separator to generate secondary dial tone. |
| | Example: |
| | "<9,:55>xx", after entering digit "9", secondary dial tone plays and you can complete the remaining two-digit number. |
| | **Note**: The secondary dial tone can be customized. For more information, refer to Tones. |

## Digit Map for All Lines Configuration

The following table lists the parameters you can use to configure digit map for all lines.

| Parameter | dialplan.digitmap.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the digit map feature. | |

| | |
|---|---|
| | **Note**: The value configured by the parameter "account.X.dialplan.digitmap.enable" takes precedence over that configured by this parameter. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |

| **Parameter** | dialplan.digitmap.string | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the digit map pattern used for the dial plan.<br><br>**Example**:<br><br>dialplan.digitmap.string = <[2-9]x:86>3.T\|0x.!\|1xxx<br><br>**Note**: The string must be compatible with the digit map feature of MGCP described in 2.1.5 of RFC 3435. It works only if "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.string" takes precedence over that configured by this parameter. | |
| **Permitted Values** | String within 2048 characters | |
| **Default** | [2-9]11 \| 0T \| 011xxx.T \| [0-1][2-9]xx xxxxxxx \| [2-9]xx xxxxxxx \| [2-9]xxxT \| **x.T \| +x.T\| 00x.T | |

| **Parameter** | dialplan.digitmap.interdigit_long_timer | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the time (in seconds) for the phone to wait before dialing an entered number if it matches part of any string of the digit map.<br><br>If it is set to 0, the phone will not dial the entered number if only a partial match exists.<br><br>The value of this parameter should be greater than that configured by the parameter "dialplan.digitmap.interdigit_short_timer".<br><br>For example:<br><br>dialplan.digitmap.string = 1xxT\|xxxxx<T1><br><br>dialplan.digitmap.interdigit_long_timer = 10<br><br>dialplan.digitmap.interdigit_short_timer = 5<br><br>When you enter 1, it matches part of two-digit maps, the phone tries to wait 10 seconds and then dials out 1 if no numbers entered;<br><br>When you enter 15, it also matches part of two-digit maps, the phone tries to wait 10 seconds and then dials out 15 if no numbers entered;<br><br>When you enter 153, it also matches part of two-digit maps, the phone tries to wait 10 seconds. But after waiting for 5 seconds, it completely matches the first digit map and then immediately dials out 153.<br><br>**Note**: It works only if "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.interdigit_long_timer" takes precedence over that configured by this parameter. | |
| **Permitted Values** | Integer from 0 to 255 | |
| **Default** | 10 | |

| **Parameter** | dialplan.digitmap.interdigit_short_timer | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the timeout interval (in seconds) for any string of digit map. | |

| | |
|---|---|
| | The phone will wait this many seconds before matching the entered digits to the dial plan and placing the call.<br><br>**Note**: It works only if "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.interdigit_short_timer" takes precedence over that configured by this parameter. |
| **Permitted Values** | **Single configuration** (configure a specific value for the timer letter "T" for all strings with "T" of the digit map)<br><br>**Example**:<br><br>dialplan.digitmap.interdigit_short_timer = 5<br><br>If "dialplan.digitmap.string" is set to <[2-9]x:86>3.T\|0T, the phone will wait 5 seconds before matching the entered digits to this dial plan and placing the call.<br><br>**Distribution configuration** (configure a string of positive integers separated by "\|" for each string of the digit map in the corresponding position)<br><br>If there are more digit maps than timeout values, the last timeout is applied to the extra digit map. If there are more timeout values than digit maps, the extra timeout values are ignored.<br><br>**Example**:<br><br>dialplan.digitmap.interdigit_short_timer = 4\|5\|3\|6\|2\|1<br><br>If "dialplan.digitmap.string" is set to <[2-9]x:86>3.T\|2T\|1xxT\|0x.!\|[2-9]11T, 4 is applied to the "<[2-9]x:86>3.T" digit map, 5 is applied to "2T" digit map, 3 is applied to "1xxT" digit map, 6 is applied to "0x.!" digit map, 2 is applied to the "[2-9]11T" digit map, the last digit 1 is ignored. |
| **Default** | 3 |
| **Parameter** | dialplan.digitmap.no_match_action      <y0000000000xx>.cfg |
| **Description** | It configures the behavior when an impossible digit map match occurs.<br><br>**Note**: It works only if "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.no_match_action" takes precedence over that configured by this parameter. |
| **Permitted Values** | **0**-prevent users from entering a number and immediately dial out the entered numbers<br><br>**1**-the dialing will fail and the phone screen will prompt "Forbidden Number"<br><br>**2**-allow users to accumulate digits and dispatch call manually with the send key or automatically dial out the entered number after a certain period of time configured by the parameter "dialplan.digitmap.interdigit_long_timer" |
| **Default** | 0 |
| **Parameter** | dialplan.digitmap.active.on_hook_dialing      <y0000000000xx>.cfg |
| **Description** | It enables or disables the entered numbers to match the predefined string of the digit map in real time. It is only applicable to the on-hook dialing.<br><br>**Note**: It works only if "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.active.on_hook_dialing" takes precedence over that configured by this parameter. It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |

| Default | 0 |
| --- | --- |
| **Parameter** | dialplan.digitmap.apply_to.on_hook_dial <y0000000000xx>.cfg |
| **Description** | It enables or disables the entered number to match the predefined string of the digit map after pressing a send key when dialing on-hook or pressing the DSS key (for example, speed dial, BLF or prefix key). **Note**: It works only if "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.on_hook_dial" takes precedence over that configured by this parameter. On-hook dialing is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| Default | 1 |
| **Parameter** | dialplan.digitmap.apply_to.directory_dial <y0000000000xx>.cfg |
| **Description** | It enables or disables the digit map to be applied to the numbers dialed from the directory. **Note**: It works only if "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.directory_dial" takes precedence over that configured by this parameter. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| Default | 1 |
| **Parameter** | dialplan.digitmap.apply_to.history_dial <y0000000000xx>.cfg |
| **Description** | It enables or disables the digit map to be applied to the numbers (received calls or missed calls) dialed from call history list. **Note**: It works only if "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.history_dial" takes precedence over that configured by this parameter. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| Default | 0 |
| **Parameter** | dialplan.digitmap.apply_to.forward <y0000000000xx>.cfg |
| **Description** | It enables or disables the digit map to be applied to the numbers that you want to forward to when performing call forward. **Note**: It works only if "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.forward" takes precedence over that configured by this parameter. |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled, the incoming calls will be forwarded to the desired destination number according to the string of the digit map. |
| Default | 1 |
| **Parameter** | dialplan.digitmap.apply_to.press_send <y0000000000xx>.cfg |
| **Description** | It enables or disables the entered number to match the predefined string of the digit map after tapping a send key. It is only applicable to the off-hook dialing. |

| | The off-hook dialing includes: pick up the handset, press the Speakerphone key or tap the line key when the phone is idle. |
| --- | --- |
| | **Note**: It works only if "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.press_send" takes precedence over that configured by this parameter. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 1 |
| **Parameter** | dialplan.digitmap.apply_to.prefix_key | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to apply the predefined string of the digit map after tapping a Prefix key.<br>**Note:** It works only if "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 1 |

## Digit Map for a Specific Line Configuration

The following table lists the parameters you can use to configure digit map for a specific line.

| **Parameter** | account.X.dialplan.digitmap.enable[1] | <MAC>.cfg |
| --- | --- | --- |
| **Description** | It enables or disables the digit map feature for a specific account.<br>**Note**: The value configured by the parameter "account.X.dialplan.digitmap.enable" takes precedence over that configured by the parameter "dialplan.digitmap.enable". |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |
| **Parameter** | account.X.dialplan.digitmap.string[1] | <MAC>.cfg |
| **Description** | It configures the digit map pattern used for the dial plan.<br>**Example**:<br>account.1.dialplan.digitmap.string = <[2-9]x:86>3.T\|0x.!\|1xxx<br>**Note**: The string must be compatible with the digit map feature of MGCP described in 2.1.5 of RFC 3435. It works only if "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.string" takes precedence over that configured by the parameter "dialplan.digitmap.string". |
| **Permitted Values** | String within 2048 characters |
| **Default** | Blank |
| **Parameter** | account.X.dialplan.digitmap.interdigit_long_timer[1] | <MAC>.cfg |
| **Description** | It configures the time (in seconds) to wait before dialing an entered number if it matches part of any string of the digit map for the account X.<br>If it is set to 0, the phone will not dial the entered number if it only a partial match exists. |

| | The value of this parameter should be greater than that configured by the parameter "account.X.dialplan.digitmap.interdigit_short_timer". |
|---|---|
| | For example: |
| | account.1.dialplan.digitmap.string = 1xxT\|xxxxx<T1> |
| | account.1.dialplan.digitmap.interdigit_long_timer = 10 |
| | account.1.dialplan.digitmap.interdigit_short_timer = 5 |
| | When you enter 1, it matches part of two-digit maps, the phone tries to wait 10 seconds and then dials out 1 if no numbers entered; |
| | When you enter 15, it also matches part of two-digit maps, the phone tries to wait 10 seconds and then dials out 15 if no numbers entered; |
| | When you enter 153, it also matches part of two-digit maps, the phone tries to wait 10 seconds. But after waiting for 5 seconds, it completely matches the first digit map and then immediately dials out 153. |
| | **Note**: It works only if "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.interdigit_long_timer" takes precedence over that configured by the parameter "dialplan.digitmap.interdigit_long_timer". |
| **Permitted Values** | Integer from 0 to 255 |
| **Default** | Blank |
| **Parameter** | account.X.dialplan.digitmap.interdigit_short_timer[1] <MAC>.cfg |
| **Description** | It configures the timeout interval (in seconds) for any string of digit map. |
| | The phone will wait this many seconds before matching the entered digits to the dial plan and placing the call. |
| | **Note**: It works only if "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.interdigit_short_timer" takes precedence over that configured by the parameter "dialplan.digitmap.interdigit_short_timer". |
| **Permitted Values** | **Single configuration** (configure a specific value for the timer letter "T" for all strings with "T" of the digit map) |
| | **Example**: |
| | account.1.dialplan.digitmap.interdigit_short_timer = 5 |
| | If "dialplan.digitmap.string" is set to <[2-9]x:86>3.T\|0T, the phone will wait 5 seconds before matching the entered digits to this dial plan and placing the call. |
| | **Distribution configuration** (configure a string of positive integers separated by "\|" for each string of the digit map in the corresponding position) |
| | If there are more digit maps than timeout values, the last timeout is applied to the extra digit map. If there are more timeout values than digit maps, the extra timeout values are ignored. |
| | **Example**: |
| | account.1.dialplan.digitmap.interdigit_short_timer = 4\|5\|3\|6\|2\|1 |
| | If "dialplan.digitmap.string" is set to <[2-9]x:86>3.T\|2T\|1xxT\|0x.!\|[2-9]11T, 4 is applied to the "<[2-9]x:86>3.T" digit map, 5 is applied to "2T" digit map, 3 is applied to "1xxT" digit map, 6 is applied to "0x.!" digit map, 2 is applied to the "[2-9]11T" digit map, the last digit 1 is ignored. |

| Default | 3 |
|---|---|
| **Parameter** | account.X.dialplan.digitmap.no_match_action[1] | <MAC>.cfg |
| **Description** | It configures the behavior when an impossible digit map match occurs.<br><br>**Note**: It works only if "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.no_match_action" takes precedence over that configured by the parameter "dialplan.digitmap.no_match_action". |
| **Permitted Values** | **0**-prevent users from entering a number and immediately dial out the entered numbers<br><br>**1**-the dialing will fail and the phone screen will prompt "Forbidden Number"<br><br>**2**-allow users to accumulate digits and dispatch call manually with the send key or automatically dial out the entered number after a certain period of time configured by the parameter "dial-plan.digitmap.interdigit_long_timer" |
| **Default** | Blank |
| **Parameter** | account.X.dialplan.digitmap.active.on_hook_dialing [1] | <MAC>.cfg |
| **Description** | It enables or disables the entered numbers to match the predefined string of the digit map in real time on the pre-dialing screen.<br><br>To enter the pre-dialing screen, directly enter numbers when the phone is idle.<br><br>**Note**: It works only if "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.active.on_hook_dialing" takes precedence over that configured by the parameter "dialplan.digitmap.active.on_hook_dialing". It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | Blank |
| **Parameter** | account.X.dialplan.digitmap.apply_to.on_hook_dial [1] | <MAC>.cfg |
| **Description** | It enables or disables the entered number to match the predefined string of the digit map after pressing a send key on the pre-dialing screen or pressing the DSS key (for example, speed dial, BLF or prefix DSS key).<br><br>To enter the pre-dialing screen, directly enter numbers when the phone is idle.<br><br>**Note**: It works only if "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.on_hook_dial" takes precedence over that configured by the parameter "dialplan.digitmap.apply_to.on_hook_dial". |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | Blank |
| **Parameter** | account.X.dialplan.digitmap.apply_to.directory_dial [1] | <MAC>.cfg |
| **Description** | It enables or disables the digit map to be applied to the numbers dialed from the directory.<br><br>**Note**: It works only if "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.directory_dial" takes precedence over that configured by the parameter "dialplan.digitmap.apply_to.directory_dial". |
| **Permitted** | **0**-Disabled |

| Values | **1**-Enabled |
|---|---|
| **Default** | Blank |
| **Parameter** | account.X.dialplan.digitmap.apply_to.history_dial[1]   <MAC>.cfg |
| **Description** | It enables or disables the digit map to be applied to the numbers (received calls or missed calls) dialed from call log lists.<br><br>**Note**: It works only if "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.history_dial" takes precedence over that configured by this parameter. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | Blank |
| **Parameter** | account.X.dialplan.digitmap.apply_to.forward[1]   <MAC>.cfg |
| **Description** | It enables or disables the digit map to be applied to the numbers that you want to forward to when performing call forward.<br><br>**Note**: It works only if "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.forward" takes precedence over that configured by the parameter "dialplan.digitmap.apply_to.forward". |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled, the incoming calls will be forwarded to the desired destination number according to the string of the digit map. |
| **Default** | Blank |
| **Parameter** | account.X.dialplan.digitmap.apply_to.press_send[1]   <MAC>.cfg |
| **Description** | It enables or disables the entered number to match the predefined string of the digit map after tapping a send key.<br><br>The off-hook dialing includes: pick up the handset, press the Speakerphone key or tap the line key when the phone is idle.<br><br>**Note**: It works only if "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.press_send" takes precedence over that configured by the parameter "dialplan.digitmap.apply_to.press_send". |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | Blank |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# Emergency Dialplan and Enhanced 911

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 and enhanced 911.

## 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.

## Enhanced 911

E911 (Enhanced 911) is a location technology that enables the called party to identify the geographical location of the calling party. For example, if a caller makes an emergency call to E911, the feature extracts the caller's information for the police department to immediately identify the caller's location.

## Topic

## Emergency Dialplan and Enhanced 911 Configuration

The following table lists the parameters you can use to configure emergency dialplan and Enhanced 911.

| Parameter | dialplan.emergency.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the Emergency dialplan feature. | |
| Permitted Values | **0**-Disabled<br>**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.<br><br>**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.<br><br>**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.<br><br>**GENBAND**-If it is set to **GENBAND**, GENBAND E911 feature is enabled, the location ID will be added to the INVITE and REGISTER SIP messages. | |
| Default | ELIN | |
| Parameter | dialplan.emergency.custom_asserted_id | <y0000000000xx>.cfg |
| Description | It configures the custom outbound identity when placing an emergency call.<br><br>**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>).<br><br>**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.<br><br>**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.<br><br>**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.<br><br>**Note**: It works only if "dialplan.emergency.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-UDP<br><br>**1**-TCP<br><br>**2**-TLS<br><br>**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.<br><br>**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;<br><br>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. |
| **Permitted Values** | a combination of digits 1, 2 and 3 |
| **Default** | 1, 2, 3 |
| **Parameter** | account.X.reg_with_pani_header.enable[3]      <MAC>.cfg |
| **Description** | It enables or disables the phone to carry the PANI header in the REGISTER request message. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |
| **Parameter** | account.X.invite_with_pani_header.enable[3]      <MAC>.cfg |
| **Description** | It enables or disables the phone to carry the PANI header in the INVITE request message.<br><br>The PANI header format is:<br><br>P-Access-Network-Info:IEEE-802.3; eth-location=<MAC Address Of The Phone>; local-time-zone="0800" |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |

[1] X is from 1 to 3.

[2] X is from 1 to 255.

[3]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# Hotline

Hotline, sometimes referred to as hot dialing, is a point-to-point communication link in which a call is automatically directed to the preset hotline number. If you lift the handset, press the Speakerphone key or the line key, and do nothing for a specified time interval, the phone will automatically dial out the hotline number. Yealink phones only support one hotline number.

| **Note** |
|---|
| If you do not specify a line, the phone uses the first available line to dial out the hotline number by default.<br>This feature works only if the Off Hook Hot Line Dialing feature is disabled. For more information, refer to Off Hook Hot Line Dialing. |

## Topic

Hotline Configuration

## Hotline Configuration

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

| Parameter | features.hotline_number | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the hotline number that the phone automatically dials out when you lift the handset, press the Speakerphone key or tap the line key. <br><br> Leaving it blank disables hotline feature. <br><br> **Note**: Handset and Speakerphone key are not applicable to CP960 phones. | |
| Permitted Values | String within 32 characters | |
| Default | Blank | |
| Web UI | Features->General Information->Hotline Number | |
| Phone UI | Settings->Features->Hot Line->Number | |
| Parameter | features.hotline_delay | <y0000000000xx>.cfg |
| Description | It configures the waiting time (in seconds) for the phone to automatically dial out the preset hotline number. <br><br> If it is set to 0 (0s), the phone will immediately dial out the preset hotline number when you lift the handset, press the Speakerphone key or tap the line key. <br><br> If it is set to a value greater than 0, the phone will wait the designated seconds before dialing out the preset hotline number when you lift the handset, press the Speakerphone key or tap the line key. <br><br> **Note**: Handset and Speakerphone key are not applicable to CP960 phones. | |
| Permitted Values | Integer from 0 to 10 | |
| Default | 4 | |
| Web UI | Features->General Information->Hotline Delay(0~10s) | |
| Phone UI | Settings->Features->Hot Line->Hotline Delay | |

## Off Hook Hot Line Dialing

For security reasons, the phones support off hook hot line dialing feature, which allows the phone to dial out the pre-configured number when you lift the handset, press the Speakerphone key or tap desired line key. 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 the 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

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 dial out a pre-configured number when a user lifts the handset, presses the Speakerphone key or taps the desired line key.<br><br>**Note**: Handset and Speakerphone key are not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, the phone will dial out the pre-configured number (configured by "account.X.auto_dial_num"). | |
| Default | 0 | |
| Parameter | account.X.auto_dial_num[1] | <MAC>.cfg |
| Description | It configures the number that the phone dials out when a user lifts the handset, presses the Speakerphone key or taps the desired line key.<br><br>**Note**: It works only if "account.X.auto_dial_enable" is set to 1 (Enabled).<br><br>**Note**: Handset and Speakerphone key are not applicable to CP960 phones. | |
| Permitted Values | String within 1024 characters | |
| Default | Blank | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

## Live Dialpad

Live Dialpad allows the phones to automatically dial out the entered phone number without tapping the send key after a designated period of time.

**Topic**

## Live Dialpad Configuration

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

| Parameter | phone_setting.predial_autodial | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the live dialpad feature. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, the phone will automatically dial out the entered phone number on the pre-dialing screen without tapping a send key. | |
| Default | 0 | |
| Web UI | Settings->Preference->Live Dialpad | |

| Parameter | phone_setting.inter_digit_time | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the delay time (in seconds) for the phone to automatically dial out the entered phone number without tapping a send key.<br><br>**Note**: It works only if "phone_setting.predial_autodial" is set to 1 (Enabled) and "dialplan.digitmap.enable" is set to 0 (Disabled). | |
| Permitted Values | Integer from 1 to 14 | |
| Default | 4 | |
| Web UI | Settings->Preference->Inter Digit Time (1~14s) | |

# Auto Redial

You can set the phone automatically redial the last dialed number when the callee is temporarily unavailable. Both the number of attempts and waiting time between redials are configurable.

## Topic

Auto Redial Configuration

## Auto Redial Configuration

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

| Parameter | auto_redial.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to automatically redial the last dialed number when the callee is temporarily unavailable. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Features->General Information->Auto Redial | |
| Phone UI | Settings->Features->Auto Redial->Auto Redial | |
| Parameter | auto_redial.interval | <y0000000000xx>.cfg |
| Description | It configures the interval (in seconds) for the phone to wait between redials.<br><br>The phone redials the last dialed number at regular intervals till the callee answers the call. | |
| Permitted Values | Integer from 1 to 300 | |
| Default | 10 | |
| Web UI | Features->General Information->Auto Redial Interval (1~300s) | |
| Phone UI | Settings->Features->Auto Redial->Redial Interval | |
| Parameter | auto_redial.times | <y0000000000xx>.cfg |
| Description | It configures the auto redial times when the callee is temporarily unavailable.<br><br>The phone tries to redial the callee as many times as configured till the callee answers the call. | |
| Permitted | Integer from 1 to 300 | |

| | |
|---|---|
| **Values** | |
| **Default** | 10 |
| **Web UI** | Features->General Information->Auto Redial Times (1~300) |
| **Phone UI** | Settings->Features->Auto Redial->Redial Times |
| **Parameter** | features.redial_via_local_sip_server.enable | <y0000000000xx>.cfg |
| **Description** | It configures the phone to redial via local SIP server or remote SIP server. |
| **Permitted Values** | **0**-Remote SIP Server |
| | **1**-Local SIP Server |
| **Default** | 1 |

# Recall Configuration

Recall, also known as last call return, allows you to dial the last received call. Recall is implemented on the phones using a Recall key.

The following shows configuration for a Recall key.

| Line Key Configuration | Programmable Key Configuration |
|---|---|
| linekey.X.type = 7<br><br>linekey.X.label =Recall | programablekey.X.type = 7 |

After provisioning, a Recall key is available on the phone. When you tap the Recall key, the phone places a call to the phone number that last called you.

## Related Topics

Line Keys Configuration
Programmable Keys Configuration

# Speed Dial

Speed dial allows you to speed up dialing the contacts on the phone's idle screen using dedicated DSS keys.

## Topic

Speed Dial Key Configuration

# Speed Dial Key Configuration

You can configure line key or programmable key as Speed Dial key (not applicable to CP960 phones).

| Line Key Configuration | Programmable Key Configuration |
|---|---|
| linekey.X.type = 13<br><br>linekey.X.line = 1<br><br>linekey.X.value = 4603<br><br>linekey.X.label = Bill | programablekey.X.type = 13<br><br>programablekey.X.line = 1<br><br>programablekey.X.value = 4603 |

After provisioning, a Speed Dial key for Bill (4603) is available on the phone, and you can tap the Speed Dial key to call Bill (4603) quickly.

You can configure multiple Speed Dial keys for different contacts which are used frequently or hard to remember.

### Related Topics

Line Keys Configuration
Programmable Keys Configuration

# Password Dial

Password dial feature allows the callee number to be partly displayed on the IP phone when placing a call. The hidden digits are displayed as asterisks on the phone screen. The number in placed call list is also partly displayed on the IP phone. This feature is especially useful for users who often place important and confidential calls.

### Topic

Password Dial Configuration

## Password Dial Configuration

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

| Parameter | features.password_dial.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to partly display the callee number when placing a call. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Features->General Information->PswDial | |
| Parameter | features.password_dial.prefix | <y0000000000xx>.cfg |
| Description | It configures the prefix that the number starts with this prefix will be partly displayed.<br><br>**Example**:<br><br>features.password_dial.prefix = 12<br><br>**Note**: It works only if "features.password_dial.enable" is set to 1 (Enabled). | |
| Permitted Values | String within 32 characters | |
| Default | Blank | |
| Web UI | Features->General Information->PswPrefix | |
| Parameter | features.password_dial.length | <y0000000000xx>.cfg |
| Description | It configures how many digits to be displayed as asterisks.<br><br>**Example**:<br><br>features.password_dial.length = 3<br><br>If you set the prefix to 12 and the length to 3, when you want to dial the number 123456, the entered number is displayed as 12***6 on the phone screen. | |

| | **Note**: It works only if "features.password_dial.enable" is set to 1 (Enabled). |
|---|---|
| **Permitted Values** | Integer from 0 to 32 |
| **Default** | Blank |
| **Web UI** | Features->General Information->PswLength |

# 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 touch 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 | |
|---|---|---|
| Phone UI | Settings->Features->Anonymous->Line X->Local Anonymous | |
| 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. <br><br> **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 | |
| Phone UI | Settings->Features->Anonymous->Line X->Send Anony Code | |
| Parameter | account.X.anonymous_call_oncode[1] | <MAC>.cfg |
| Description | It configures the anonymous call on code. <br><br> 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 | |
| Phone UI | Settings->Features->Anonymous->Line X->On Code | |
| Parameter | account.X.anonymous_call_offcode[1] | <MAC>.cfg |
| Description | It configures the anonymous call off code. <br><br> 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 | |
| Phone UI | Settings->Features->Anonymous->Line X->Off Code | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# 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.<br><br>If the dialed number contains configured characters, the phone will automatically filter these characters when dialing.<br><br>**Example**:<br><br>features.call_num_filter = -<br><br>If you dial 3-61, the phone will filter the character - and then dial out 361.<br><br>**Note**: If it is left blank, the phone will not automatically filter any characters when dialing. | |
| Permitted Values | String within 99 characters | |
| 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.<br><br>**Note**: If you want to receive an IP address call, make sure "sip.trust_ctrl" is set to 0 (Disabled). | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Web UI | Features->General Information->Allow IP Call | |

# Off Hook Answering

You can set whether to answer an incoming call by picking up the handset, pressing the Speakerphone key or pressing the HEADSET key directly.

It is not applicable to CP960 phones.

## Topic

Off Hook Answering Configuration

## Off Hook Answering Configuration

The following table lists the parameter you can use to configure off hook answering.

| Parameter | features.off_hook_answer.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to answer an incoming call by picking up the handset, pressing the Speakerphone key or pressing the HEADSET key directly.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled, the user needs to press the corresponding line key, the **Answer** soft key or the OK key to answer an incoming call after picking up the handset, pressing the Speakerphone key or pressing the HEADSET key.<br>**1**-Enabled | |
| Default | 1 | |

# Auto Answer

Yealink phones support answering a SIP call or an IP address call automatically. Auto answer is configurable on a per-line basis, while IP address call is not.

### Topic

Auto Answer Configuration

## Auto Answer Configuration

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

| Parameter | account.X.auto_answer[1] | <MAC>.cfg |
|---|---|---|
| Description | It enables or disables auto answer a SIP call.<br><br>**Note**: The phone cannot automatically answer the incoming call during a call or while dialing even if auto answer is enabled. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, the phone can automatically answer an incoming call. | |
| Default | 0 | |
| Web UI | Account->Basic->Auto Answer | |
| Phone UI | Settings->Features->Auto Answer->Account X | |
| Parameter | account.X.auto_answer_mute_enable<br><br>(X is equal to 1) | <MAC>.cfg |
| Description | It enables or disables the auto answer mute feature.<br><br>**Note**: It is only applicable to CP960 phones. It works only if the values of parameters "account.X.auto_answer" and "features.allow_mute" are set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, the phone will mute the microphone when an incoming call is automatically answered, and then the other party cannot hear you. | |
| Default | 0 | |

| Web UI | Account->Basic->Auto Answer Mute | |
|---|---|---|
| Phone UI | Settings->Features->Auto Answer->Account 1-> Auto Answer (On) ->Auto Answer Mute | |
| Parameter | features.ip_call.auto_answer.enable | <y0000000000xx>.cfg |
| Description | It enables or disables the auto answer feature for IP call.<br><br>**Note**: It works only if "features.direct_ip_call_enable" is set to 1 (Enabled). The phone cannot automatically answer the incoming IP call when the IP phone is in a call or dialing even if IP call auto answer is enabled. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, the phone can automatically answer the IP call. | |
| Default | 0 | |
| Web UI | Features->General Information->IP Direct Auto Answer | |
| Parameter | features.auto_answer_delay | <y0000000000xx>.cfg |
| Description | It configures the delay time (in seconds) before the phone automatically answers an incoming call.<br><br>**Note**: For the call coming from a SIP account, it works only if "account.X.auto_answer" is set to 1 (Enabled). | |
| Permitted Values | Integer from 1 to 4 | |
| Default | 1 | |
| Web UI | Features->General Information->Auto Answer Delay | |
| Parameter | features.auto_answer_tone.enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to play a warning tone when an incoming call is automatically answered.<br><br>**Note**: For the call coming from a SIP account, it works only if "account.X.auto_answer" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Web UI | Features->General Information->Enable Auto Answer Tone | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# 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 "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

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<br><br>**1**-On, the phone will automatically reject incoming calls from users enabled anonymous call feature. The anonymous user's phone screen presents "Anonymity Disallowed". | |
| Default | 0 | |
| Web UI | Account->Basic->Local Anonymous Rejection | |
| Phone UI | Settings->Features->Anonymous->Line X->Anonymous Rejection | |
| Parameter | features.anonymous_response_code | <y0000000000xx>.cfg |
| Description | It configures the code the phone responds with to the server when it receives an anonymous call.<br><br>**Note**: It works only if "account.X.reject_anonymous_call" is set to 1 (On). | |
| Permitted Values | Integer from 0 to 65535 | |
| Default | 433 | |
| Parameter | account.X.anonymous_reject_oncode[1] | <MAC>.cfg |
| Description | It configures the anonymous call rejection on code.<br><br>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 | |
| Phone UI | Settings->Features->Anonymous->Line X->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 Values | **0**-Off Code, the phone will send anonymous rejection off code to the server when you deactivate the anonymous call rejection feature.<br><br>**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 | |

| Phone UI | Settings->Features->Anonymous->Line X->Send Rejection Code | |
|---|---|---|
| Parameter | account.X.anonymous_reject_offcode[1] | <MAC>.cfg |
| Description | It configures the anonymous call rejection off code.<br><br>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 | |
| Phone UI | Settings->Features->Anonymous->Line X->Off Code | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# 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.<br><br>1-Enabled, the phone screen will present a new incoming call during a call. | |
| Default | 1 | |
| Web UI | Features->General Information->Call Waiting | |
| Phone UI | Settings->Features->Call Waiting->Call Waiting | |
| 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.<br><br>Note: It works only if "call_waiting.enable" is set to 1 (Enabled). | |

| **Permitted Values** | **0**-Disabled <br> **1**-Enabled | |
|---|---|---|
| **Default** | 1 | |
| **Web UI** | Features->Audio->Call Waiting Tone | |
| **Phone UI** | Settings->Features->Call Waiting->Play Tone | |
| **Parameter** | call_waiting.on_code | <y0000000000xx>.cfg |
| **Description** | It configures the call waiting on code. <br><br> 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 | |
| **Phone UI** | Settings->Features->Call Waiting->On Code | |
| **Parameter** | call_waiting.off_code | <y0000000000xx>.cfg |
| **Description** | It configures the call waiting off code. <br><br> 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 | |
| **Phone UI** | Settings->Features->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.

Usually, you can activate DND when the phone is idle. The phone stays in the DND state until you deactivate DND manually.

### Topics

DND Settings Configuration
DND Feature Configuration
DND Synchronization for Server-side Configuration

## DND Settings Configuration

You can change the following DND settings:

- Choose a DND mode. You can configure DND for all lines or specific lines.
- Enable or disable DND emergency feature and specify DND authorized numbers. These numbers will not be DND when the DND feature is enabled. The incoming call will not be logged in the Missed Calls list.

- 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_mode | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the DND mode for the IP phone.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Phone, DND feature is effective for the phone system.<br><br>**1**-Custom, you can configure DND feature for each or all accounts. | |
| Default | 0 | |
| Web UI | Features->Forward&DND->DND->Mode | |
| Parameter | features.dnd.emergency_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to receive incoming calls from authorized numbers when DND feature is enabled.<br><br>**Note**: The authorized numbers are configured by the parameter "features.dnd.emergency_authorized_number". | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Features->Forward&DND->DND->DND Emergency | |
| Parameter | features.dnd.emergency_authorized_number | <y0000000000xx>.cfg |
| Description | It configures the authorized numbers the phone can receive incoming calls from even if DND feature is activated.<br><br>Multiple numbers are separated by commas.<br><br>**Example**:<br><br>features.dnd.emergency_authorized_number = 123,124<br><br>**Note**: It works only if "features.dnd.emergency_enable" is set to 1 (Enabled). | |
| Permitted Values | String within 511 characters | |
| Default | Blank | |
| Web UI | Features->Forward&DND->DND->DND Authorized Numbers | |
| 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. | |
| Permitted Values | **404**-Not Found<br><br>**480**-Temporarily Unavailable<br><br>**486**-Busy Here, the caller's phone screen will display the reason "Busy Here" when the callee enables DND feature.<br><br>**603**-Decline | |

| Default | 480 | |
|---|---|---|
| Web UI | Features->General Information->Return Code When DND | |
| Parameter | features.exit_dnd_mode_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to display **Exit DND mode.** after DND is activated.<br><br>**Note**: It works only if "features.dnd.enable" is set to 1 (On). It is only applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled, users can tap **Exit DND mode.** from the idle screen to deactivate DND. | |
| Default | 1 | |

## DND Feature Configuration

After you choose a DND mode, you can configure DND feature for all lines or a specific line. It depends on the DND mode (except CP960):

- **Phone** (default): DND feature is effective for all lines.
- **Custom:** DND feature can be configured for a specific line or multiple lines.

| Note |
|---|
| DND mode is set by the parameter "features.dnd_mode". |

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

### Topics

DND in Phone Mode Configuration
DND in Custom Mode Configuration

## DND in Phone Mode Configuration

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

| Parameter | features.dnd.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It triggers the DND feature to on or off.<br><br>**Note**: It works only if "features.dnd_mode" is set to 0 (Phone) (except CP960 phones). | |
| Permitted Values | **0**-Off<br><br>**1**-On, the phone will reject incoming calls on all accounts. | |
| Default | 0 | |
| Web UI | Features->Forward&DND->DND->DND Status | |
| Phone UI | Settings->Features->DND->DND Status | |
| Parameter | features.dnd.on_code | <y0000000000xx>.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.<br><br>**Note**: It works only if "features.dnd_mode" is set to 0 (Phone) (except CP960 phones). | |
| Permitted Values | String within 32 characters | |

| Default | Blank | |
|---|---|---|
| **Web UI** | Features->Forward&DND->DND->On Code | |
| **Phone UI** | Settings->Features->DND->On Code | |
| **Parameter** | features.dnd.off_code | <y0000000000xx>.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.<br><br>**Note**: It works only if "features.dnd_mode" is set to 0 (Phone) (except CP960 phones). | |
| **Permitted Values** | String within 32 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Forward&DND->DND->Off Code | |
| **Phone UI** | Settings->Features->DND->Off Code | |

## DND in Custom Mode Configuration

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

| **Parameter** | account.X.dnd.enable[1] | <MAC>.cfg |
|---|---|---|
| **Description** | It triggers the DND feature to on or off.<br><br>**Note**: It works only if "features.dnd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Off<br><br>**1**-On, the phone will reject incoming calls on account X. | |
| **Default** | 0 | |
| **Web UI** | Features->Forward& DND->DND->AccountX->DND Status | |
| **Phone UI** | Settings->Features->DND->AccountX->DND Status | |
| **Parameter** | account.X.dnd.on_code[1] | <MAC>.cfg |
| **Description** | It configures the DND on code to activate the server-side DND feature.<br><br>The phone will send the DND on code to the server when you activate DND feature on the phone.<br><br>**Note**: It works only if "features.dnd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. | |
| **Permitted Values** | String within 32 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Forward& DND->DND->AccountX->On Code | |
| **Phone UI** | Settings->Features->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.<br><br>The phone will send the DND off code to the server when you deactivate DND feature on the phone.<br><br>**Note**: It works only if "features.dnd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. | |

| Permitted Values | String within 32 characters |
|---|---|
| Default | Blank |
| Web UI | Features->Forward& DND->DND->AccountX->Off Code |
| Phone UI | Settings->Features->DND->AccountX->Off Code |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

## DND Synchronization for Server-side Configuration

DND synchronization feature provides the capability to synchronize the status of the DND features between the IP phone and the server.

If the DND is activated in phone mode, the DND status changing locally will be synchronized to all registered accounts on the server; but if the DND status of a specific account is changed on the server, the DND status locally will be changed.

The following table lists the parameters you can use to configure DND synchronization for server-side.

| Parameter | features.feature_key_sync.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables to synchronize the feature status between the IP phone and the server. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, the phone sends a SUBSCRIBE message with event "as-feature-event". | |
| Default | 0 | |
| Parameter | features.dnd.feature_key_sync.enable | <y0000000000xx>.cfg |
| Description | It enables or disables the DND feature synchronization.<br><br>**Note**: It works only if "features.feature_key_sync.enable" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, server-based DND is enabled. Server and local phone DND are synchronized. | |
| Default | 1 | |
| Parameter | features.dnd.feature_key_sync.local_pro-cessing.enable | <y0000000000xx>.cfg |
| Description | It enables or disables the local DND when DND feature synchronization is enabled.<br><br>**Note**: It works only if "features.feature_key_sync.enable" and "features.dnd.feature_key_sync.enable" are set to 1 (Enabled). The value configured by the parameter "account.X.features.dnd.feature_key_syn-c.local_processing.enable" takes precedence over that configured by this parameter. | |
| Permitted Values | **0**-Disabled, DND is performed on the server side only.<br><br>**1**-Enabled, DND is performed on both server side and locally. | |
| Default | 0 | |
| Parameter | account.X.features.dnd.feature_key_sync.local_pro-cessing.enable[1] | <MAC>.cfg |
| Description | It enables or disables the local DND when DND feature synchronization is enabled.<br><br>**Note**: It works only if "features.feature_key_sync.enable" and "features.dnd.feature_key_sync.enable" are set to 1 (Enabled). | |

| Permitted Values | **0**-Disabled, DND is performed on the server side only. |
| --- | --- |
| | **1**-Enabled, DND is performed on both server side and locally. |
| Default | Blank |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# 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).

When you place an active call on hold or the call is held by remote parry, a call hold tone or held tone alerts you after a specific period of time that a call is still on hold or is still held by the remote party. You can configure the call hold tone and held tone.

If supported by the server, you can also configure a music-on-hold URI.

## Topics

Call Hold Configuration
Music on Hold (MoH) 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). It is not applicable to CP960 phones. | |
| 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 | |
| Parameter | features.play_hold_tone.enable | <y0000000000xx>.cfg |

| Description | It enables or disables the phone to play the call hold tone when you place a call on hold. | |
|---|---|---|
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 1 | |
| **Web UI** | Features->General Information->Play Hold Tone | |
| **Parameter** | features.play_hold_tone.delay | <y0000000000xx>.cfg |
| **Description** | It configures the time (in seconds) to wait for the phone to play the initial call hold tone.<br><br>If it is set to 30 (30s), the phone will wait 30 seconds to play the initial call hold tone after you place a call on hold.<br><br>**Note**: It works only if "features.play_hold_tone.enable" is set to 1 (Enabled). | |
| **Permitted Values** | Integer from 3 to 3600 | |
| **Default** | 30 | |
| **Web UI** | Features->General Information->Play Hold Tone Delay | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# Music on Hold (MoH) Configuration

When a call is placed on hold, the phone will send an INVITE message to the specified MoH server account according to the SIP URI. The MoH server account automatically responds to the INVITE message and immediately plays audio from some source located anywhere (LAN, Internet) to the held party. For more information, refer to draft RFC draft-worley-service-example.

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

| **Parameter** | account.X.music_server_uri[1] | <MAC>.cfg |
|---|---|---|
| **Description** | It configures the address of the Music On Hold server.<br><br>Examples for valid values: <10.1.3.165>, 10.1.3.165, sip:moh@sip.com, <sip:moh@sip.com>, <yealink.com> or yealink.com.<br><br>**Note**: The DNS query in this parameter only supports A query. | |
| **Permitted Values** | SIP URI within 256 characters | |
| **Default** | Blank | |
| **Web UI** | Account->Advanced->Music Server URI | |
| **Parameter** | account.X.music_on_hold_type[1] | <MAC>.cfg |
| **Description** | It configures the way to process Music On Hold when placing an active call on hold. | |
| **Permitted Values** | **0**-Calling the Music On Hold server before holding the call<br><br>**1**-Calling the Music On Hold server after holding the call | |
| **Default** | 0 | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# Call Mute

You can mute the microphone of the active audio device (handset, headset or speakerphone) on Yealink phones during an active call or when the phone is on the pre-dialing/dialing/calling/ringing screen. The call is automatically muted when setting up successfully. Muting before a call is answered prevents the other party from hearing local discussion.

You can activate the mute feature by pressing the MUTE key. Normally, the mute feature is automatically deactivated when the active call ends. You can use keep mute feature to keep the mute state persisting across the calls.

## Topics

Microphone Mute Configuration
Keep Mute
Mute Alert Tone

## Microphone Mute Configuration

The following table lists the parameter you can use to configure microphone mute feature.

| Parameter | features.allow_mute | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the allow mute feature for the IP phone. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, you are allowed to mute an active call, or activate the mute feature on the pre-dialing/dialing/calling/ringing screen. | |
| Default | 1 | |
| Web UI | Features->General Information->Allow Mute | |
| Parameter | features.dect_mic.mute.mode | <y0000000000xx>.cfg |
| Description | It configures the mute mode for the phone and the registered Wireless Expansion Mic/connected Wired Expansion Mic. | |
| Permitted Values | **0**-Synchronous mode, the mute/unmute states on the expansion microphone and on the phone are synchronous. When the phone is in a call, you can mute the call on the phone or on the expansion microphone.<br><br>**1**-Standalone mode, the mute/unmute states on the expansion microphone and on the phone are mutually independent. When the phone is in a call, you can mute the phone and the expansion microphone together by tapping **All mute** on the phone, mute the phone only by tapping **Mute** on the phone, or mute the expansion microphone only by tapping the mute button on the expansion microphone.<br><br>**Note**: It is only applicable to CP960 phones. It is not available when using CP960 star connection feature. | |
| Default | 0 | |
| Phone UI | Settings->Wireless Microphone->Synchronous mode/Standalone mode | |

## Keep Mute

Keep mute, also known as persistent mute, allows you to keep the mute state persisting across calls.

In a call center or meet room, if incoming calls are answered automatically, the callers may hear the local discussion. Therefore, you can mute the phone in an idle state to prevent the unintended situation. The mute state persists across calls until you unmute the microphone manually or until the phone restarts.

You can activate the mute feature by pressing the MUTE key in idle/pre-dialing/dialing/ringing/calling/talking state.

## Topic

Keep Mute Configuration

### Keep Mute Configuration

The following table lists the parameter you can use to enable or disable keep mute.

| Parameter | features.keep_mute.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the keep mute feature.<br><br>**Note**: It works only if "features.allow_mute" is set to 1 (Enabled). | |
| Permitted Values | **0**-The mute feature is automatically deactivated when the active call ends.<br><br>**1**-The mute state is kept until you change the mute state manually or the phone restarts. | |
| Default | 0 (for VP59/T58A)<br><br>1 (for CP960) | |

## Mute Alert Tone

You can configure the phone to play an audible tone if the mute status of the phone is changed. This allows you to know if your phone is in the mute or un-mute state. In addition, you can set a periodic reminder which plays the audible tone periodically when the phone is in the mute state. The time interval must not be less than 3 seconds.

It is only applicable to CP960 phones.

## Topic

Mute Alert Tone Configuration

### Mute Alert Tone Configuration

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

| Parameter | features.play_mute_tone.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to play an audible tone when the mute status is changed. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled<br><br>**Note**: It is only applicable to CP960 phones. | |
| Default | 0 | |
| Parameter | features.play_mute_tone.interval | <y0000000000xx>.cfg |
| Description | It configures time interval (in seconds) for playing an audible tone when the phone is in the mute state during the call.<br><br>**Note**: It is only applicable to CP960 phones. | |
| Permitted Values | Integer from 3 to 3600 | |
| Default | 5 | |

# Call Forward

You can forward calls from any line on your phone to a contact. There are two ways of forwarding your calls:

- 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.

  You can set the phone not to forward a call coming from authorized numbers.

- Manually forward an incoming call to a number.

## Topics

## Call Forward Settings Configuration

You can change the following call forward settings:

- Allow or disallow users to forward an incoming call to an international telephone number (the prefix is 00).

- Enable or disable forward emergency feature and specify forward authorized numbers. These numbers will not be forwarded when the call forward feature is enabled. The incoming call will not be logged in the Forwarded Calls list.

- 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_mode | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the call forward mode.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Phone, call forward feature is effective on a phone basis.<br><br>**1**-Custom, you can configure call forward feature on a per-line basis. | |
| Default | 0 | |
| Web UI | Features->Forward&DND->Forward->Mode | |
| Parameter | features.forward.emergency.enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to receive the call from authorized numbers when the call forward feature is activated. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, the call from authorized numbers will not be forwarded when the call forward feature is activated. | |
| Default | 0 | |
| Web UI | Features->Forward&DND->Forward->Forward Emergency | |
| Parameter | features.forward.emergency.authorized_number | <y0000000000xx>.cfg |
| Description | It configures the authorized numbers.<br><br>The call from the authorized numbers cannot be forwarded even if the call forward feature is activated.<br><br>Multiple numbers are separated by commas. | |

| | |
|---|---|
| | **Note**: It works only if "features.forward.emergency.enable" is set to 1 (Enabled). |
| **Permitted Values** | String within 511 characters |
| **Default** | Blank |
| **Web UI** | Features->Forward&DND->Forward->Forward Authorized Numbers |
| **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<br>**1**-Enabled |
| **Default** | 1 |
| **Web UI** | Features->General Information->Fwd International |
| **Phone UI** | Settings->Advanced Setting (default password: admin)->FWD International->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<br><br>**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

After you choose a call forward mode, you can configure call forward feature for all lines or specific lines. It depends on the call forward mode (CP960 except):

- **Phone** (default): Call forward feature is effective for all lines.
- **Custom**: Call forward feature can be configured for a specific line or multiple lines.

| **Note** |
|---|
| Forward mode is set by the parameter "features.fwd_mode". |

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

| **Tip** |
|---|
| You can set a DSS key as a Forward key, and specify a contact you want to forward the incoming calls to for this key. For more information, refer to DSS Keys. |

### Topics

## Call Forward in Phone Mode Configuration

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

| Parameter | forward.always.enable | | | <y0000000000xx>.cfg |
|---|---|---|---|---|
| Description | It triggers the always forward feature to on or off on a phone basis.<br><br>**Note**: It works only if "features.fwd_mode" is set to 0 (Phone)(except CP960 phones) | | | |
| Permitted Values | **0**-Off<br><br>**1**-On, incoming calls are forwarded to the destination number (configured by the parameter "forward.always.target") immediately. | | | |
| Default | 0 | | | |
| Web UI | Features->Forward&DND->Forward->Always Forward->On/Off | | | |
| Phone UI | Settings->Features->Call Forward->Always Forward->Always Forward | | | |
| Parameter | forward.always.target | | | <y0000000000xx>.cfg |
| Description | It configures the destination number of the always forward on a phone basis.<br><br>**Note**: It works only if "features.fwd_mode" is set to 0 (Phone)(except CP960 phones). | | | |
| Permitted Values | String within 32 characters | | | |
| Default | Blank | | | |
| Web UI | Features->Forward&DND->Forward->Always Forward->Target | | | |
| Phone UI | Settings->Features->Call Forward->Always Forward->Forward To | | | |
| Parameter | forward.always.on_code | | | <y0000000000xx>.cfg |
| Description | It configures the always forward on code to activate the server-side always forward feature.<br><br>The phone will send the always forward on code and the pre-configured destination number (configured by the parameter "forward.always.target") to the server when you activate always forward feature on a phone basis.<br><br>**Note**: It works only if "features.fwd_mode" is set to 0 (Phone)(except CP960 phones). | | | |
| Permitted Values | String within 32 characters | | | |
| Default | Blank | | | |
| Web UI | Features->Forward&DND->Forward->Always Forward->On Code | | | |
| Phone UI | Settings->Features->Call Forward->Always Forward->On Code | | | |
| Parameter | forward.always.off_code | | | <y0000000000xx>.cfg |
| Description | It configures the always forward off code to deactivate the server-side always forward feature.<br><br>The phone will send the always forward off code to the server when you deactivate always forward feature on a phone basis.<br><br>**Note**: It works only if "features.fwd_mode" is set to 0 (Phone)(except CP960 phones). | | | |
| Permitted Values | String within 32 characters | | | |
| Default | Blank | | | |
| Web UI | Features->Forward&DND->Forward->Always Forward->Off Code | | | |

| Phone UI | Settings->Features->Call Forward->Always Forward->Off Code | |
|---|---|---|
| **Parameter** | forward.busy.enable | \<y0000000000xx>.cfg |
| **Description** | It triggers the busy forward feature to on or off on a phone basis. <br><br> **Note**: It works only if "features.fwd_mode" is set to 0 (Phone)(except CP960 phones). | |
| **Permitted Values** | **0**-Off <br><br> **1**-On, incoming calls are forwarded to the destination number (configured by the parameter "forward.busy.target") when the callee is busy. | |
| **Default** | 0 | |
| **Web UI** | Features->Forward&DND->Forward->Busy Forward->On/Off | |
| **Phone UI** | Settings->Features->Call Forward->Busy Forward->Busy Forward | |
| **Parameter** | forward.busy.target | \<y0000000000xx>.cfg |
| **Description** | It configures the destination number of the busy forward on a phone basis. <br><br> **Note**: It works only if "features.fwd_mode" is set to 0 (Phone)(except CP960 phones). | |
| **Permitted Values** | String within 32 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Forward&DND->Forward->Busy Forward->Target | |
| **Phone UI** | Settings->Features->Call Forward-> Busy Forward->Forward To | |
| **Parameter** | forward.busy.on_code | \<y0000000000xx>.cfg |
| **Description** | It configures the busy forward on code to activate the server-side busy forward feature. <br><br> The phone will send the busy forward on code and the pre-configured destination number (configured by the parameter "forward.busy.target") to the server when you activate the busy forward feature on a phone basis. <br><br> **Note**: It works only if "features.fwd_mode" is set to 0 (Phone)(except CP960 phones). | |
| **Permitted Values** | String within 32 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Forward&DND->Forward->Busy Forward->On Code | |
| **Phone UI** | Settings->Features->Call Forward->Busy Forward->On Code | |
| **Parameter** | forward.busy.off_code | \<y0000000000xx>.cfg |
| **Description** | It configures the busy forward off code to deactivate the server-side busy forward feature. <br><br> The phone will send the busy forward off code to the server when you deactivate the busy forward feature on a phone basis. <br><br> **Note**: It works only if "features.fwd_mode" is set to 0 (Phone)(except CP960 phones). | |
| **Permitted Values** | String within 32 characters | |
| **Default** | Blank | |

| Web UI | Features->Forward&DND->Forward->Busy Forward->Off Code | |
|---|---|---|
| Phone UI | Settings->Features->Call Forward->Busy Forward->Off Code | |
| Parameter | forward.no_answer.enable | <y0000000000xx>.cfg |
| Description | It triggers the no answer forward feature to on or off on a phone basis.<br><br>**Note**: It works only if "features.fwd_mode" is set to 0 (Phone)(except CP960 phones). DND activated on the IP phone deactivates the local No Answer Forward settings. | |
| Permitted Values | **0**-Off<br><br>**1**-On, incoming calls are forwarded to the destination number (configured by the parameter "forward.no_answer.target") after a period of ring time. | |
| Default | 0 | |
| Web UI | Features->Forward&DND->Forward->No Answer Forward->On/Off | |
| Phone UI | Settings->Features->Call Forward->No Answer Forward->No Answer Forward | |
| Parameter | forward.no_answer.target | <y0000000000xx>.cfg |
| Description | It configures the destination number of the no answer forward on a phone basis.<br><br>**Note**: It works only if "features.fwd_mode" is set to 0 (Phone)(except CP960 phones). | |
| Permitted Values | String within 32 characters | |
| Default | Blank | |
| Web UI | Features->Forward&DND->Forward->No Answer Forward->Target | |
| Phone UI | Settings->Features->Call Forward->No Answer Forward->Forward To | |
| Parameter | forward.no_answer.timeout | <y0000000000xx>.cfg |
| Description | It configures ring times (N) to wait before forwarding incoming calls.<br><br>The incoming calls will be forwarded when not answered after N*M (M is configurable by "phone_setting.ring_duration") seconds.<br><br>**Note**: It works only if "features.fwd_mode" is set to 0 (Phone) (except CP960 phones). | |
| Permitted Values | Integer from 0 to 20 (determined by "features.forward.no_answer.show_ring_times") | |
| Default | 2 | |
| Web UI | Features->Forward&DND->Forward->No Answer Forward->After Ring Time (0~120s) | |
| Phone UI | Settings->Features->Call Forward->No Answer Forward->After Ring Time | |
| Parameter | features.forward.no_answer.show_ring_times | <y0000000000xx>.cfg |
| Description | It configures the permitted values of the ring times (N) to wait before forwarding incoming calls.<br><br>**Example**:<br><br>features.forward.no_answer.show_ring_times = 0,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19<br><br>**Note**: It works only if "forward.no_answer.enable" or "account.X.timeout_fwd.enable" is set to 1 (Enabled). | |
| Permitted | String within 512 characters | |

| | |
|---|---|
| **Values** | |
| **Default** | 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20 (1 is not applicable to BroadSoft users) |
| **Parameter** | phone_setting.ring_duration             \<y0000000000xx>.cfg |
| **Description** | It configures the interval (in seconds) of the ring for the no answer forward feature. <br><br>**Note**: It works only if "forward.no_answer.enable" or "account.X.timeout_fwd.enable" is set to 1 (Enabled). |
| **Permitted Values** | Integer greater than or equal to 0 |
| **Default** | 6 |
| **Parameter** | forward.no_answer.on_code             \<y0000000000xx>.cfg |
| **Description** | It configures the no answer forward on code to activate the server-side no answer forward feature. <br><br>The phone will send the no answer forward on code and the pre-configured destination number (configured by the parameter "forward.no_answer.target") to the server when you activate the no answer forward feature on a phone basis. |
| **Permitted Values** | String within 32 characters |
| **Default** | Blank |
| **Web UI** | Features->Forward&DND->Forward->No Answer Forward->On Code |
| **Phone UI** | Settings->Features->Call Forward->No Answer Forward->On Code |
| **Parameter** | forward.no_answer.off_code             \<y0000000000xx>.cfg |
| **Description** | It configures the no answer forward off code to deactivate the server-side no answer forward feature. <br><br>The phone will send the no answer forward off code to the server when you deactivate the no answer forward feature on a phone basis. <br><br>**Note**: It works only if "features.fwd_mode" is set to 0 (Phone)(except CP960 phones). |
| **Permitted Values** | String within 32 characters |
| **Default** | Blank |
| **Web UI** | Features->Forward&DND->Forward->No Answer Forward->Off Code |
| **Phone UI** | Settings->Features->Call Forward->No Answer Forward->Off Code |

## Call Forward in Custom Mode Configuration

The following table lists the parameters you can use to configure call forward in Custom mode. It is not applicable to CP960 phones.

| | |
|---|---|
| **Parameter** | account.X.always_fwd.enable[1]             \<MAC>.cfg |
| **Description** | It triggers always forward feature to on or off. <br><br>**Note:** It works only if "features.fwd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Off <br><br>**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 |
| **Phone UI** | Settings->Features->Call Forward->AccountX->Always Forward->Always Forward |
| **Parameter** | account.X.always_fwd.target[1] <MAC>.cfg |
| **Description** | It configures the destination number of the always forward.<br><br>**Note:** It works only if "features.fwd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. |
| **Permitted Values** | String within 32 characters |
| **Default** | Blank |
| **Web UI** | Features->Forward&DND->Forward->AccountX->Always Forward->Target |
| **Phone UI** | Settings->Features->Call Forward->AccountX->Always Forward->Forward To |
| **Parameter** | account.X.always_fwd.on_code[1] <MAC>.cfg |
| **Description** | It configures the always forward on code to activate the server-side always forward feature.<br><br>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.<br><br>**Note:** It works only if "features.fwd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. |
| **Permitted Values** | String within 32 characters |
| **Default** | Blank |
| **Web UI** | Features->Forward&DND->Forward->AccountX->Always Forward->On Code |
| **Phone UI** | Settings->Features->Call Forward->AccountX->Always Forward->On Code |
| **Parameter** | account.X.always_fwd.off_code[1] <MAC>.cfg |
| **Description** | It configures the always forward off code to deactivate the server-side always forward feature.<br><br>The phone will send the always forward off code to the server when you deactivate always forward feature on the phone.<br><br>**Note:** It works only if "features.fwd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. |
| **Permitted Values** | String within 32 characters |
| **Default** | Blank |
| **Web UI** | Features->Forward&DND->Forward->AccountX->Always Forward->Off Code |
| **Phone UI** | Settings->Features->Call 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.<br><br>**Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Off<br><br>**1**-On, incoming calls to the account X are forwarded to the destination number (configured by the para- |

| | |
|---|---|
| | meter "account.X.busy_fwd.target") when the callee is busy. |
| **Default** | 0 |
| **Web UI** | Features->Forward&DND->Forward->AccountX->Busy Forward->On/Off |
| **Phone UI** | Settings->Features->Call Forward->AccountX->Busy Forward->Busy Forward |
| **Parameter** | account.X.busy_fwd.target[1]            \<MAC>.cfg |
| **Description** | It configures the destination number of the busy forward. <br><br>**Note:** It works only if "features.fwd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. |
| **Permitted Values** | String within 32 characters |
| **Default** | Blank |
| **Web UI** | Features->Forward&DND->Forward->AccountX->Busy Forward->Target |
| **Phone UI** | Settings->Features->Call Forward->AccountX->Busy Forward->Forward To |
| **Parameter** | account.X.busy_fwd.on_code[1]            \<MAC>.cfg |
| **Description** | It configures the busy forward on code to activate the server-side busy forward feature. <br><br>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. <br><br>**Note:** It works only if "features.fwd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. |
| **Permitted Values** | String within 32 characters |
| **Default** | Blank |
| **Web UI** | Features->Forward&DND->Forward->AccountX->Busy Forward->On Code |
| **Phone UI** | Settings->Features->Call Forward->AccountX->Busy Forward->On Code |
| **Parameter** | account.X.busy_fwd.off_code[1]            \<MAC>.cfg |
| **Description** | It configures the busy forward off code to deactivate the server-side busy forward feature. <br><br>The phone will send the busy forward off code to the server when you deactivate the busy forward feature on the phone. <br><br>**Note:** It works only if "features.fwd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. |
| **Permitted Values** | String within 32 characters |
| **Default** | Blank |
| **Web UI** | Features->Forward&DND->Forward->AccountX->Busy Forward->Off Code |
| **Phone UI** | Settings->Features->Call 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. <br><br>**Note:** It works only if "features.fwd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. |
| **Permitted** | **0**-Off |

| Values | **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 | |
| **Phone UI** | Settings->Features->Call Forward->AccountX->No Answer Forward->No Answer Forward | |
| **Parameter** | account.X.timeout_fwd.target[1] | <MAC>.cfg |
| **Description** | It configures the destination number of the no answer forward.<br>**Note:** It works only if "features.fwd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. | |
| **Permitted Values** | String within 32 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Forward&DND->Forward->AccountX->No Answer Forward->Target | |
| **Phone UI** | Settings->Features->Call Forward->AccountX->No Answer Forward->Forward To | |
| **Parameter** | account.X.timeout_fwd.timeout[1] | <MAC>.cfg |
| **Description** | It configures ring times (N) to wait before forwarding incoming calls.<br>The incoming calls will be forwarded when not answered after N*M (M is configurable by "phone_setting.ring_duration") seconds.<br>**Note:** It works only if "features.fwd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. | |
| **Permitted Values** | Integer from 0 to 20 (determined by "features.forward.no_answer.show_ring_times") | |
| **Default** | 2 | |
| **Web UI** | Features->Forward&DND->Forward->AccountX->No Answer Forward->After Ring Time(0~120s) | |
| **Phone UI** | Settings->Features->Call Forward->AccountX->No Answer Forward->After Ring Time | |
| **Parameter** | account.X.timeout_fwd.on_code[1] | <MAC>.cfg |
| **Description** | It configures the no answer forward on code to activate the server-side no answer forward feature.<br>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.<br>**Note:** It works only if "features.fwd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. | |
| **Permitted Values** | String within 32 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Forward&DND->Forward->AccountX->No Answer Forward->On Code | |
| **Phone UI** | Settings->Features->Call Forward->AccountX->No Answer Forward->On Code | |
| **Parameter** | account.X.timeout_fwd.off_code[1] | <MAC>.cfg |
| **Description** | It configures the no answer forward off code to deactivate the server-side no answer forward feature.<br>The phone will send the no answer forward off code to the server when you deactivate no answer forward feature on the phone. | |

| | |
|---|---|
| | **Note:** It works only if "features.fwd_mode" is set to 1 (Custom). It is not applicable to CP960 phones. |
| **Permitted Values** | String within 32 characters |
| **Default** | Blank |
| **Web UI** | Features->Forward&DND->Forward->AccountX->No Answer Forward->Off Code |
| **Phone UI** | Settings->Features->Call Forward->AccountX->No Answer Forward->Off Code |

[1]X is the account ID. For VP59/T58A, X=1-16.

# Call Forward Synchronization for Server-side Configuration

Call forward synchronization feature provides the capability to synchronize the status of the call forward features between the IP phone and the server.

If the call forward is activated in phone mode, the forward status changing locally will be synchronized to all registered accounts on the server; but if the forward status of the specific account is changed on the server, the forward status locally will be changed.

The following table lists the parameters you can use to configure call forward synchronization for server-side.

| | | |
|---|---|---|
| **Parameter** | features.feature_key_sync.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables to synchronize the feature status between the IP phone and the server. | |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled, the phone send a SUBSCRIBE message with event "as-feature-event" to the server. | |
| **Default** | 0 | |
| **Parameter** | features.forward.feature_key_sync.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the forward feature synchronization.<br><br>**Note**: It works only if "features.feature_key_sync.enable" is set to 1 (Enabled). | |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled, server-based call forward is enabled. Server and local phone call forward are synchronized. | |
| **Default** | 1 | |
| **Parameter** | features.forward.feature_key_sync.local_processing.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the local forward when call forward feature synchronization is enabled.<br><br>**Note**: It works only if "features.feature_key_sync.enable" and "features.forward.feature_key_sync.enable" are set to 1 (Enabled). The value configured by the parameter "account.X.features.forward.feature_key_sync.local_processing.enable" takes precedence over that configured by this parameter. | |
| **Permitted Values** | **0**-Disabled, call forward is performed on the server side only.<br><br>**1**-Enabled, call forward is performed on both server side and locally. | |
| **Default** | 0 | |
| **Parameter** | account.X.features.forward.feature_key_sync.local_processing.enable[1] | <MAC>.cfg |
| **Description** | It enables or disables the local forward when call forward feature synchronization is enabled. | |

| | **Note**: It works only if "features.feature_key_sync.enable" and "features.forward.feature_key_sync.enable" are set to 1 (Enabled). |
|---|---|
| **Permitted Values** | **0**-Disabled, call forward is performed on the server side only. **1**-Enabled, call forward is performed on both server side and locally. |
| **Default** | Blank |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# 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.

## Topics

## 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 taps the **Transfer** key after hearing the ringback tone, the phone will blind transfer the call. **1**-Enabled, when the user taps the **Transfer** 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.multi_call_trans_enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the users to transfer the current call to another existing call when there are multiple calls. | |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled, when the users tap the **Trans**/**Transfer** soft key or press TRAN/TRANSFER key, they can choose to transfer the current call to a new call or another existing call. | |
| Default | 1 | |
| **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 tapping the key.<br><br>**Note**: Blind transfer means transferring a call directly to another party without consulting. It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**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 tapping the key.<br><br>**Note**: Semi-attended transfer means transferring a call after hearing the ringback tone; Attended transfer means transferring a call with prior consulting. It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| **Web UI** | Features->Transfer->Attended Transfer On Hook | |
| **Parameter** | account.X.end_call_when_transferred.enable[1] | <MAC>.cfg |
| **Description** | It enables or disables the call between the transferred party and transfer party to be directly released when call transfer is completed. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

## Transfer Mode for Dsskey Configuration

The following table lists the parameter you can use to configure transfer mode for Dsskey.

| **Parameter** | transfer.dsskey_deal_type | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the transfer mode for DSS key. When the user presses the DSS Key during a call, the DSS Key behavior depends on the transfer mode.<br><br>**Note**: This feature is only applicable to the Speed Dial key, BLF/BLF List key or Transfer key with an | |

| | assigned value. | |
|---|---|---|
| **Permitted Values** | **0**-New Call<br><br>**1**-Attended Transfer<br><br>**2**-Blind Transfer | |
| **Default** | 2 | |
| **Web UI** | Features->Transfer->Transfer Mode via Dsskey | |

# Conference

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

## Topics

## 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<br><br>**2**-Network Conference | |
| **Default** | 0 | |
| **Web UI** | Account->Advanced->Conference Type | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

## Local Conference Configuration

The local conference requires a host phone to process the audio of all parties. Yealink phones support up to 5 parties (including yourself) in a local conference call.

For a local three-way conference, if the conference initiator leaves the conference, all parties are disconnected and the conference call ends. You can enable Transfer on Conference Hang Up feature, and allows the other two parties to remain connected when the conference initiator drops the conference call.

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

| **Parameter** | features.local_conf.combine_with_one_press.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the phone to set up a three-way conference directly after the second party answers the call.<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled, the user needs to tap the **Conference** soft key again to set up a conference after the second party answers the call. | |

| | |
|---|---|
| | **1**-Enabled. The second party joins a conference with the first party after answering the call, both phones play a warning tone. |
| **Default** | 0 |
| **Parameter** | transfer.tran_others_after_conf_enable       <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to transfer the local conference call to the other two parties after the conference initiator drops the local conference call.<br><br>**Note**: It works only if "account.X.conf_type" is set to 0 (Local Conference). |
| **Permitted Values** | **0**-Disabled, all parties are disconnected when the conference initiator drops the conference call.<br><br>**1**-Enabled, the other two parties remain connected when the conference initiator drops the conference call. |
| **Default** | 0 |
| **Web UI** | Features->Transfer->Transfer on Conference Hang up |

## 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.<br><br>**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. For VP59/T58A, X=1-16, for CP960, X=1.

## Call Recording

Yealink phones support recording calls (audio-only calls or video calls) or conferences during a call. By default, the recorded files are saved in the internal SD card. You can also save the recorded files in the connected USB flash drive.

For VP59/T58A phones, If you connect the USB flash drive to the IP phone, the recorded files will be saved according to the priority: USB flash drive >Internal SD card. For CP960 phones, if you connect the USB flash drive to the IP phone, you can choose to save the recorded files to the Internal SD card or USB flash drive.

| |
|---|
| **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**

# Call Recording Configuration

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

| Parameter | features.usb_call_recording.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the call recording feature for the phone. | |
| Permitted Values | **0**-Disabled<br>**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.

| Tip |
|---|
| You can set a DSS key as Multicast Paging key or Paging list key on the phone, which allows you to send announcements to the phones with the pre-configured multicast address(es) on the specific channel(s). For more information, refer to DSS Keys. |

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.<br>**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 | |
| **Phone UI** | Settings->Features->Paging List->Option->Edit->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.<br><br>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 | |
| **Phone UI** | Settings->Features->Paging List->Option->Edit->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** | **0**-all the Yealink phones running old firmware version or Yealink phones listen to channel 0 or third-party available devices in the paging group can receive the RTP stream.<br><br>**1 to 25**-the Polycom or Yealink phones preconfigured to listen to the channel can receive the RTP stream.<br><br>**26 to 30**-the Yealink phones preconfigured to listen to the channel can receive the RTP stream. | |
| **Default** | 0 | |
| **Web UI** | Directory->Multicast IP->Paging List->Paging Address->Channel | |
| **Phone UI** | Settings->Features->Paging List->Option->Edit->Channel | |

[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.<br>**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 phone listens to. | |
| Permitted Values | **0**-the phone can receive an RTP stream of the pre-configured multicast address from the phones running old firmware version, from the phones listen to the channel 0, or from the available third-party devices. **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. **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. | |
| 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.

## DND for Ignoring Paging Call

If you do not want to miss some urgent paging calls when DND is activated. You can use the Ignore DND feature to define the lowest priority of paging group from which the phone can receive an urgent paging call when DND is activ-

ated. 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 the incoming paging calls will be ignored when DND is activated in phone mode.

## Topic

## 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 | **0**-Disabled, the phone will ignore the incoming multicast paging calls when there is an active multicast paging call on the phone.<br><br>**1**-Enabled, the phone will receive the incoming multicast paging call with a higher priority and ignore the one with a lower priority. | |
| Default | 1 | |
| Web UI | Directory->Multicast IP->Paging Priority Active | |
| Parameter | multicast.receive_priority.priority | <y0000000000xx>.cfg |
| Description | It configures the priority of the voice call (a normal phone call rather than a multicast paging call) in progress.<br><br>1 is the highest priority, 31 is the lowest priority. | |
| Permitted Values | **0**-Disabled, all incoming multicast paging calls will be automatically ignored when a voice call is in progress.<br><br>**1**-1<br><br>**2**-2<br><br>**3**-3<br><br>...<br><br>**31**-31<br><br>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. | |
| Default | 31 | |

| Web UI | Directory->Multicast IP->Paging Barge | |
|---|---|---|
| Parameter | multicast.receive.ignore_dnd.priority | <y0000000000xx>.cfg |
| Description | It configures the lowest priority of the multicast paging call that can be received when DND is activated in phone mode.<br><br>1 is the highest priority, 31 is the lowest priority. | |
| Permitted Values | **0**-Disabled, all incoming multicast paging calls will be automatically ignored when DND is activated in phone mode.<br><br>**1**-1<br><br>**2**-2<br><br>**3**-3<br><br>...<br><br>**31**-31<br><br>If it is not set to 0 (Disabled), the phone will receive the incoming multicast paging call with a higher or same priority than this value and ignore that with a lower priority than this value when DND is activated in phone mode. | |
| Default | 0 | |
| Web UI | Directory->Multicast IP->Ignore DND | |
| 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.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled, the engaged audio device will be used when receiving the multicast paging calls.<br>**1**-Enabled | |
| Default | 0 | |

[1]X ranges from 1 to 31.

# Video Features

The VP59/T58A phones support transmission and reception of high quality video images. To transmit video on T58A phones, you need to connect a USB camera CAM50 to the phone in advance.

The video is compatible with RFC 3984 - RTP Payload Format for H.264 Video, RFC 7741 - on RTP Payload Format for VP8 Video.

# Video Settings

The VP59/T58A phones support using USB camera for point-to-point video calls. Users can place and answer video calls. You can configure camera flicker to optimize video calling. Indoor lights powered by a 50Hz or 60Hz power source can produce a flicker. You can adjust the camera flicker frequency according to the power source.

During video calls, near-site and far-site video images are displayed on the touch screen. You can change the default video layout.

### Topic

Video Settings Configuration

## Video Settings Configuration

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

| Parameter | static.camera.function.enable [1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the USB camera feature.<br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled, the top USB port is disabled, and the near-site video image will not be transmitted in outgoing and incoming calls.<br>**1**-Enabled | |
| Default | 1 | |
| Parameter | camera.status_bar_icon.enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to display an icon in the status bar when the camera is not detected.<br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Parameter | video.enable | <y0000000000xx>.cfg |
| Description | It configures the video call feature for the IP phone.<br>**Note**: It is not applicable to CP960 phones. If you want to transmit the near-site video image during the video call, you need to set "static.camera.function.enable" to 1 (Enabled). | |
| Permitted Values | **0**-Disabled, users are only allowed to establish an audio-only call.<br>**1**-Video first, users can establish a video call with the other party that is video-enabled.<br>**2**-Optional, users can choose to establish an audio-only or video call; and switch between the audio-only call and the video call. | |

| Default | 1 | |
|---|---|---|
| **Web UI** | Settings->Video->Video Active | |
| **Parameter** | camera.flicker | <y0000000000xx>.cfg |
| **Description** | It configures camera flicker frequency (Hz).<br><br>**Note**: Indoor lights powered by a 50Hz or 60Hz power source can produce a flicker. You can adjust the camera flicker frequency according to the power source. It is not applicable to CP960 phones. | |
| **Permitted Values** | **50**-50Hz<br><br>**60**-60Hz | |
| Default | 50 | |
| **Parameter** | features.default_layout | <y0000000000xx>.cfg |
| **Description** | It configures the default call layout after a single-way call is set up.<br><br>**Note**: It is not applicable to CP960 phones. It works only if "video.enable" is set to 1 (Video first) or 2 (Optional). There is no near-site video image on the VP59/T58A phones if USB camera is not connected. | |
| **Permitted Values** | **1**-Focus Big: One video image displays in a large size, the other video image along the right side of the screen displays in small size.<br><br>**2**-Focus Full screen: One video image displays in full size, the other video images are hidden.<br><br>**3**-Equal: All video images display in the same size. (only for T58A phones) | |
| Default | 1 | |
| **Web UI** | Features->General Information->Default Layout | |
| **Parameter** | features.full_screen_in_call_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to enter the full screen automatically when a video call is set up. | |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled<br><br>Note: It is not applicable to CP960 phones. It woks only if "video.enable" is set to 1 (Video first) or 2 (Optional). | |
| Default | 1 | |
| **Web UI** | Features->General Information->Full Screen In Call | |
| **Parameter** | features.video_call_bandwidth | <y0000000000xx>.cfg |
| **Description** | It specifies the transmission bandwidth for a video call.<br><br>**Note**: It is not applicable to CP960 phones. It woks only if "video.enable" is set to 1 (Video first) or 2 (Optional). We recommend you to reduce transmission bandwidth when network environment is relatively poor. | |
| **Permitted Values** | **0**-Auto, the default transmission bandwidth is 768kb/s. The network environment may affect the performance of the phone.<br><br>**256**-256kb/s<br><br>**384**-384kb/s<br><br>**512**-512kb/s | |

| | | |
|---|---|---|
| | **640**-640kb/s | |
| | **768**-768kb/s | |
| | **1024**-1024kb/s | |
| | **1280**-1280kb/s | |
| | **1500**-1500kb/s | |
| | **2000**-2000kb/s | |
| **Default** | 0 | |
| **Web UI** | Settings->Video->Video Call Rate | |
| **Parameter** | sip.h264.peer_resolution.default | <y0000000000xx>.cfg |
| **Description** | It configures the default video resolution if other party doesn't specify the resolution in H264 packet. **Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-CIF  **1**-4CIF  **2**-720P  **3**-1080P | |
| **Default** | 2 | |

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

# Video Codecs

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

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

## RTPmap

Codecs and priorities of these codecs are configurable on a per-line basis. The attribute "rtpmap" is used to define a mapping from RTP payload codes to a codec, clock rate and other encoding parameters.

The following table lists the video codecs supported by VP59/T58A phone model:

| Name | MIME Type | Bit Rate | Frame Rate | Frame Size |
|---|---|---|---|---|
| H.264 BP | H264/90000 | 90 kbps to 2048 kbps | 5 fps to 30 fps | Tx: CIF, 360P, W448P, 720P  Rx: Conventional Size Below 720P |
| H.264 HP | H264/90000 | | | |
| VP8 | VP8/90000 | 128kbps to 2048 kbps | | |
| H.263 | H263 | 90 kbps to 2048 kbps | | Tx: CIF, 4CIF  RX: QCIF, CIF, 4CIF |

## Topic

# Video Codecs Configuration

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

| Parameter | account.X.video.<payload_type>.enable<br><br>(where <payload_type> should be replaced by the name of video codec) | <MAC>.cfg |
|---|---|---|
| Description | It enables or disables the specified video codec for account X.<br><br>The name of audio codec:<br><br>**h264**-H264<br><br>**h264hp**-H264HP<br><br>**vp8**-VP8<br><br>**h263**-H263 (only for VP59 phones)<br><br>**Example**:<br><br>account.1.video.h264.enable = 1<br><br>**Note**: The name of video codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect. It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled | |
| Default | 1 | |
| Web UI | Account->Codec->Video Codec | |
| Parameter | account.X.video.<payload_type>.priority<br><br>(where <payload_type> should be replaced by the name of video codec) | <MAC>.cfg |
| Description | It configures the priority of the enabled video codec for account X.<br><br>The name of audio codec:<br><br>**h264**-H264<br><br>**h264hp**-H264HP<br><br>**vp8**-VP8<br><br>**h263**-H263 (only for VP59 phones)<br><br>**Example**:<br><br>account.1.video.h264.priority = 2<br><br>**Note**: The name of video codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect. It is not applicable to CP960 phones. | |

| Permitted Values | **0**-Disabled |
| --- | --- |
| | **1**-Enabled |
| **Default** | 1 |
| **Web UI** | Account->Codec->Video Codec |

# Advanced Features

The advanced features require server support. Consult your server partner to find out if these features are supported.

## Topics

## Call Pickup

You can use call pickup to answer someone else's incoming call on your phone.

The Yealink phones support Directed Call Pickup and Group Call Pickup:

- **Directed Call Pickup**: allows you to pick up incoming calls to a specific phone.
- **Group Call Pickup**: allows you to pick up incoming calls to any phone within a predefined group of phones.

## Topics

## Directed Call Pickup

Directed call pickup is used for picking up an incoming call on a specific extension. You can answer a call that rings on a specific phone. If there are multiple incoming calls on the phone at the same time, you can only pick up the first incoming call.

You can choose to implement directed call pickup using a directed call pick code or using SIP signaling.

### Topic

### Directed Call Pickup Configuration

You can enable directed call pickup, the LCD screen will display a **DPickup** soft key when picking up the handset, pressing the Speakerphone key or pressing the line key (You may need to press the **More** soft key to see the **DPickup** soft key).

You can configure a directed call pickup code and pick up the incoming call using the **DPickup** soft key.

| **Tip** | |
|---|---|
| You can set a DSS key as a Directed Pickup key, and specify a contact you want to pick up a call from for this key. For more information, refer to DSS Keys. | |

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

| Parameter | features.pickup.direct_pickup_enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the user to use **DPickup** soft key when performing directed call pickup feature. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, the phone will display the **DPickup** soft key on the Dialing screen. | |
| Default | 0 | |
| Web UI | Features->Pick up & Park->Directed Call Pickup | |
| Parameter | features.pickup.direct_pickup_code | <y0000000000xx>.cfg |
| Description | It configures the directed call pickup code on a phone basis.<br><br>**Note**: The code configured by "account.X.direct_pickup_code" takes precedence over that configured by this parameter. | |
| Permitted Values | String within 32 characters | |
| Default | Blank | |
| Web UI | Features->Pick up & Park->Directed Call Pickup Code | |
| Parameter | account.X.direct_pickup_code[1] | <MAC>.cfg |
| Description | It configures the directed call pickup code.<br><br>**Note**: The code configured by this parameter takes precedence over that configured by "features.pickup.direct_pickup_code". | |
| Permitted Values | String within 32 characters | |
| Default | Blank | |
| Web UI | Account->Advanced->Directed Call Pickup Code | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

## Group Call Pickup

Group call pickup is used for picking up incoming calls within a predefined group. When any phone within a predefined group of phones receives an incoming call, you can pick up that call easily on the phone.

If you enable group call pickup, the phone screen will display a **GPickup** soft key when picking up the handset, tapping the Speakerphone key or tapping the line key. As shown below:
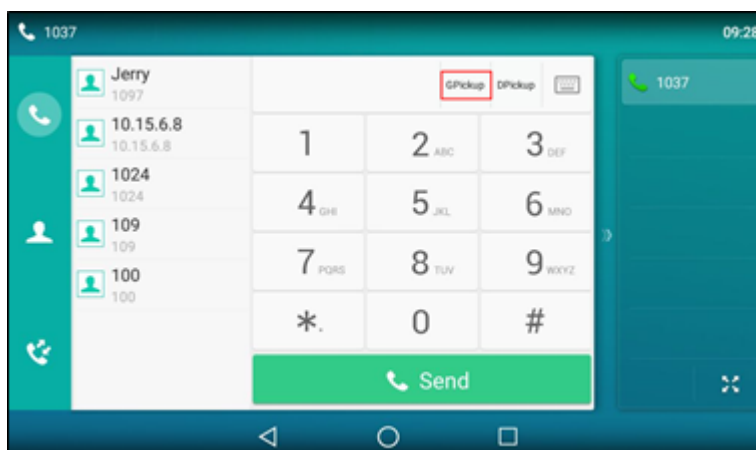
You can pick up the group incoming call using the **GPickup** soft key.

## Topic

## Group Call Pickup Configuration

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

| | | |
|---|---|---|
| **Parameter** | features.pickup.group_pickup_enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the user to use **GPickup** soft key when performing group call pickup feature. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled, the phone will display the **GPickup** soft key on the Dialing screen. | |
| **Default** | 0 | |
| **Web UI** | Features->Pick up & Park->Group Call Pickup | |
| **Parameter** | features.pickup.group_pickup_code | <y0000000000xx>.cfg |
| **Description** | It configures the group call pickup code on a phone basis.<br>**Note**: The code configured by "account.X.group_pickup_code" takes precedence over that configured by this parameter. | |
| **Permitted Values** | String within 32 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Pick up & Park->Group Call Pickup Code | |
| **Parameter** | account.X.group_pickup_code[1] | <MAC>.cfg |
| **Description** | It configures the group pickup code.<br>**Note**: The code configured by this parameter takes precedence over that configured by "features.pickup.group_pickup_code". | |

| Permitted Values | String within 32 characters |
|---|---|
| Default | Blank |
| Web UI | Account->Advanced->Group Call Pickup Code |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# Dialog Info Call Pickup

While some SIP servers implement directed call pickup using a directed call pickup code, others also support implement this feature through SIP signals.

| Note |
|---|
| In this way, you do not need to configure the directed call pickup code. |

If you enable the phone to implement directed call pickup through SIP signals, the phone picks up an incoming call via a SIP INVITE message with a Replaces header. The value of Replaces is derived from a NOTIFY message with dialog-info event. This feature applies only to directed call pick-up attempts initiated against monitored BLF resources. It means you can pick up an incoming call by tapping a BLF/BLF List key.

Example of the dialog-info carried in NOTIFY message:

```
<?xml version="1.0"?>

<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="6" state="partial" entity-y="sip:1011@10.2.1.48:5060">

<dialog id="65603" call-id="0_1756536024@10.10.20.34" local-tag="3408640225" remote-tag="3779921438" direction="recipient">

<state>early</state>

<local>

<identity>sip:1011@10.2.1.48:5060</identity>

<target uri="sip:1011@10.2.1.48:5060"/>

</local>

<remote>

<identity>sip:1058@10.2.1.48:5060</identity>

<target uri="sip:1058@10.2.1.48:5060"/>

</remote>

</dialog>

</dialog-info>
```

Example of the Replaces carried in INVITE message:

```
Via: SIP/2.0/UDP 10.10.20.18:5060;branch=z9hG4bK2026058891

From: "1010" <sip:1010@10.2.1.48:5060>;tag=826048502

To: <sip:1058@10.2.1.48:5060>
```

---

Call-ID: 0_572446084@10.10.20.18

CSeq: 1 INVITE

Contact: <sip:1010@10.10.20.18:5060>

Content-Type: application/sdp

Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH, UPDATE, MESSAGE

Max-Forwards: 70

User-Agent: Yealink T58 58.83.0.15


**Replaces: 0_1756536024@10.10.20.34;to-tag=3779921438;from-tag=3408640225**

Allow-Events: talk,hold,conference,refer,check-sync

Supported: replaces

Content-Length:   304

---

## Related Topics

Dialog Info Call Pickup Configuration
Busy Lamp Field

## Dialog Info Call Pickup Configuration

The following table lists the parameter you can use to configure dialog Info call pickup.

| Parameter | account.X.dialoginfo_callpickup[1] | <MAC>.cfg |
|---|---|---|
| Description | It enables or disables the phone implements directed call pickup through SIP signals for a specific account. **Note**: In this way, you do not need to configure the directed call pickup code. | |
| Permitted Values | **0**-Disabled **1**-Enabled, the phone picks up a call according to the Replaces header in INVITE message. | |
| Default | 0 | |
| Web UI | Account->Advanced->Dialog Info Call Pickup | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

## Call Completion

When you place a call and the callee is temporarily unavailable to answer the call, call completion allows your phone to monitor the busy party and establish a call after the busy party becomes available to receive a call.

Two factors commonly prevent a call from connecting successfully:

- Callee does not answer
- Callee actively rejects the incoming call before answering

Yealink phones support call completion using the SUBSCRIBE/NOTIFY method, which is specified in draft-poetzl-sip-ping-call-completion-00, to subscribe to the busy party and receive notifications of their status changes.

The caller subscribes for update notifications of the dialog event from the busy party. Example of a SUBSCRIBE message:

---

SUBSCRIBE sip:1000@10.10.20.34:5060 SIP/2.0

Via: SIP/2.0/UDP 10.10.20.32:5060;branch=z9hG4bK2880274891

From: "10111" <sip:10111@10.2.1.48:5060>;tag=8643512

To: <sip:1000@10.2.1.48:5060>;tag=4025601441

Call-ID: 4_2103527761@10.10.20.32

CSeq: 2 SUBSCRIBE

Contact: <sip:10111@10.10.20.32:5060>

Accept: application/dialog-info+xml

Max-Forwards: 70

User-Agent: Yealink T58 58.83.0.15

Expires: 60


Event: dialog

Content-Length: 0

---

Example of a NOTIFY message (The subscription (SUBSCRIBE message) of the dialog event "Call Completion" is confirmed by the busy party):

---

NOTIFY sip:10111@10.10.20.32:5060 SIP/2.0

Via: SIP/2.0/UDP 10.10.20.31:5060;branch=z9hG4bK1830418099

From: <sip:1000@10.2.1.48:5060>;tag=1032948194

To: "10111" <sip:10111@10.2.1.48:5060>;tag=722495580

Call-ID: 0_160090766@10.10.20.32

CSeq: 2 NOTIFY

Contact: <sip:1000@10.10.20.31:5060>

Content-Type: application/dialog-info+xml

Max-Forwards: 70

User-Agent: Yealink T58 58.83.0.15

Subscription-State: active;expires=60

Event: dialog

Content-Length:   584


<?xml version="1.0"?>

<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="1" state="full" entity="sip:1000@10.2.1.48:5060">

---

```
<dialog id="65626" call-id="0_3138198645@10.10.20.31" local-tag="2331766736" remote-tag="1786911541" dir-
ection="initiator">

<state>confirmed</state>

<local>

<identity>sip:1000@10.2.1.48:5060</identity>

<target uri="sip:1000@10.2.1.48:5060"/>

</local>

<remote>

<identity>sip:1@10.2.1.48:5060</identity>

<target uri="sip:1@10.2.1.48:5060"/>

</remote>

</dialog>

<dialog id="65622">

<state>terminated</state>

</dialog>

</dialog-info>
```

Example of a NOTIFY message (The busy party has finished the call and is available again. A new notification update from the busy party is received by the caller):

```
NOTIFY sip:10111@10.10.20.32:5060 SIP/2.0

Via: SIP/2.0/UDP 10.10.20.31:5060;branch=z9hG4bK3431394016

From: <sip:1000@10.2.1.48:5060>;tag=1558968605

To: "10111" <sip:10111@10.2.1.48:5060>;tag=140677866

Call-ID: 0_2584152566@10.10.20.32

CSeq: 5 NOTIFY

Contact: <sip:1000@10.10.20.31:5060>

Content-Type: application/dialog-info+xml

Max-Forwards: 70

User-Agent: Yealink T58 58.83.0.15

Subscription-State: active;expires=48

Event: dialog

Content-Length:   217


<?xml version="1.0"?>
```

```
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="4" state="partial" entity-
y="sip:1000@10.2.1.48:5060">

<dialog id="65644">


<state>terminated</state>

</dialog>

</dialog-info>
```

## Topics

## Call Completion Configuration

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

| Parameter | features.call_completion_enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the call completion feature. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Web UI** | Features->General Information->Call Completion | |
| **Phone UI** | Settings->Features->Call Completion->Call Completion | |

## Example: Using Call Completion

The following example shows the configuration for call completion.

**Example**

*features.call_completion_enable = 1*

After provisioning, when you place a call and the callee is temporarily unavailable to answer the call, the phone screen will prompt whether to wait for the callee party. You can activate the call completion feature. After the called party becomes idle, the phone screen will prompt whether to dial the number.

## 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 VP59/T58A phones support the 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.

## Topics

## 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->Pick up & Park->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->Pick up & Park->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->Pick up & Park->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->Pick up & Park->Park Retrieve Code | |
| **Parameter** | sip.call_park_without_blf[1] | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to close the BLF monitoring feature for call park DSS key. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |

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

## Example: Setting Call Park and Retrieve in FAC Mode

The following example shows the configuration for FAC call park mode.

**Example**

*features.call_park.park_mode = 1*

*features.call_park.enable = 1*

*features.call_park.park_code = *68*

*features.call_park.park_retrieve_code = *88*

After provisioning, the call park mode is set to FAC. A **Park** soft key will display on the phone during an active call, and a **Retrieve** soft key will display on the Dialing screen. You can tap the **Park** soft key to park a call, or tap the **Retrieve** soft key to retrieve a parked call.

| Tip |
| --- |
| You can set a line key as a Park key or a Retrieve key, specify an extension you want to park a call to for Park key and specify a parked extension you want to retrieve a parked call from for Retrieve key. For more information, refer to Line Keys. |

## Example: Setting Call Park and Retrieve in Transfer Mode

The following example shows the configuration for Transfer call park mode.

**Example**

*features.call_park.park_mode = 2*

*features.call_park.enable = 1*

*features.call_park.park_code = *01*

*features.call_park.park_retrieve_code = *11*

After provisioning, the call park mode is set to Transfer. A **Park** soft key will display on the phone during an active call and a **Retrieve** soft key will display on the Dialing screen. You can tap the **Park** soft key to park a call to the shared parking lot "*01", or tap the **Retrieve** soft key to retrieve the parked call from the shared parking lot "*01" using the retrieve code "*11".

| Tip |
| --- |
| You can set a line key as a Park key or a Retrieve key, specify a shared parking lot you want to park a call to for Park key and specify a retrieve lot you want to retrieve a parked call from for Retrieve key. For more information, refer to Line Keys. |

# Automatic Call Distribution (ACD)

ACD enables the use of phones in a call-center role by automatically distributing incoming calls to available users or agents. You can enable users to use their phone in a call center agent/a supervisor role on a supported call server.

The users can sign in and sign out of the ACD state as call center agent using soft keys. The server distributes calls to the agent when the agent state is available, and stops distributing calls when the agent changes state to unavailable. The IP phone remains in the unavailable status until the agent manually changes the IP phone status. You can configure how long the IP phone remains unavailable state and changes to available automatically on a supported call server.

It is not applicable to CP960 phones.

**Topics**

## ACD Key Configuration

You can configure a line key as ACD key to log into the ACD system. The ACD key on the IP phone indicates the ACD state.

The following shows configuration for an ACD key.

*linekey.X.type = 42*

*linekey.X.label = ACD*

After provisioning, an ACD key is available on the phone, and you can tap the ACD key to log into the ACD system.

**Related Topic**

Line Keys Configuration

## ACD Configuration

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

| Parameter | account.X.acd.enable[1] | | <MAC>.cfg |
|---|---|---|---|
| Description | It enables or disables the ACD feature. | | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | | |
| Default | 0 | | |
| Parameter | account.X.acd.available[1] | | <MAC>.cfg |
| Description | It enables or disables the phone to display the **Available**/**Avail** or **Unavailable**/**Unavail** soft key after the phone logs into the ACD system.<br>**Note**: It works only if "account.X.acd.enable" is set to 1 (Enabled). | | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | | |
| Default | 0 | | |
| Parameter | account.X.subscribe_acd_expires[1] | | <MAC>.cfg |
| Description | It configures the period (in seconds) of ACD subscription.<br>**Note**: It works only if "account.X.acd.enable" is set to 1 (Enabled). | | |
| Permitted Values | Integer from 120 to 3600 | | |
| Default | 3600 | | |
| Web UI | Account->Advanced->ACD Subscribe Period(120~3600s) | | |
| Parameter | acd.enable | | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to automatically change the status of the ACD agent to available after the designated time. | | |

|  |  |  |
|---|---|---|
|  | **Note**: It works only if "account.X.acd.enable" is set to 1 (Enabled). |  |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |  |
| **Default** | 0 |  |
| **Web UI** | Features->ACD->ACD->ACD Available Auto |  |
| **Parameter** | account.X.acd.unavailable_reason_enable[1] | <MAC>.cfg |
| **Description** | It enables or disables the unavailable/away reason code feature.<br>**Note**: It works only if "account.X.acd.available" is set to 1 (Enabled). |  |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled, the unavailable/away reason of agent state will be displayed on the phone screen (for example, on lunch, in the bathroom, taking a coffee break or a personal break). |  |
| **Default** | 0 |  |
| **Parameter** | acd.auto_available_timer | <y0000000000xx>.cfg |
| **Description** | It configures the interval (in seconds) for the status of the ACD agent to be automatically changed to available.<br>**Note**: It works only if "account.X.acd.enable" and "acd.auto_available" are set to 1 (Enabled). |  |
| **Permitted Values** | Integer from 0 to 120 |  |
| **Default** | 60 |  |
| **Web UI** | Features->ACD->ACD->ACD Auto Available Time (0~120s) |  |

[1]X is the account ID. For VP59/T58A, X=1-16.

## Example: Setting ACD

The following example shows the configuration for ACD. It is not applicable to CP960 phones.

**Example**

######Set an ACD for account 1#######

*account.1.acd.enable = 1*

*account.1.acd.available = 1*

*account.1.subscribe_acd_expires = 3000*

*acd.enable = 1*

*acd.auto_available_timer = 60*

*features.homescreen_softkey.acd.enable = 1*

######Set an ACD key#############

*linekey.1.type=42*

*linekey.1.label=ACD*

After provisioning, you can tap the **Login** soft key or ACD key to log into the ACD system. After logging into the ACD system, **Available**/**Unavailable** soft key appears on the phone screen. You can tap **Available**/**Unavailable**soft key to change ACD state. The ACD key on the IP phone indicates the ACD state.

# Busy Lamp Field

The Busy Lamp Field (BLF) feature enables the IP phone to monitor specific remote lines for state changes on the phone.

Yealink phones support two methods of BLF configuration:

- Configure a line key as BLF key to monitor a specific remote line
- Configure BLF List to monitor a list of specific remote lines

The BLF feature enables the following functions to the users:

- Monitor the status of line on their phone
- Display caller ID information
- Answer incoming calls to the monitored line (called directed call pickup)
- Park and retrieve calls to the monitored line
- Initiate an outgoing intercom call to the monitored line
- Barging In an Active Call by BLF List Key

### Topics

# BLF Key Configuration

You can configure a BLF key for a specific line.

The following shows the configuration of a BLF key for Bill.

*linekey.X.type=16*

*linekey.X.line=1*

*linekey.X.value=1001*

*linekey.X.label=Bill*

### Related Topic

# BLF List Configuration

You can configure a BLF List for monitor phone. It enables the monitor phone to subscribe to a list of lines, and receive status notifications of the monitored lines.

**Note**

The IP phone subscribes to a BLF list that is set up on the server. You must access the server and set up a list of monitored lines.

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

| Parameter | account.X.blf.blf_list_uri[1] | <MAC>.cfg |
|---|---|---|
| Description | It configures the BLF List URI to monitor a list of users for account X.<br><br>**Example**:<br><br>account.1.blf.blf_list_uri = 4609@pbx.test.com | |
| Permitted Values | SIP URI within 256 characters | |
| Default | Blank | |
| Web UI | Account->Advanced->BLF List URI | |
| Parameter | account.X.blf_list_code[1] | <MAC>.cfg |
| Description | It configures the feature access code that initiates a directed call pickup for account X. | |
| Permitted Values | String within 32 characters | |
| Default | Blank | |
| Web UI | Account->Advanced->BLF List Pickup Code | |
| Parameter | account.X.blf_list_barge_in_code[1] | <MAC>.cfg |
| Description | It configures the feature access code of directed call pickup with barge-in for account X. | |
| Permitted Values | String within 32 characters | |
| Default | Blank | |
| Web UI | Account->Advanced->BLF List Barge in Code | |
| Parameter | account.X.blf_list_retrieve_call_parked_code[1] | <MAC>.cfg |
| Description | It configures the feature access code that initiates retrieval of a parked call on the monitored user. | |
| Permitted Values | String within 32 characters | |
| Default | Blank | |
| Web UI | Account->Advanced->BLF List Retrieve Call Parked Code | |
| Parameter | phone_setting.auto_blf_list_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to automatically configure the BLF list DSS keys in order. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Parameter | phone_setting.blf_list_sequence_type | <y0000000000xx>.cfg |
| Description | It configures the order of BLF list DSS keys assigned automatically.<br><br>**Note**: It works only if "phone_setting.auto_blf_list_enable" is set to 1 (Enabled). It is only applicable to | |

| | |
|---|---|
| | T58A phones.To assign Ext Key, make sure the expansion module has been connected to the phone in advance. |
| **Permitted Values** | **0**-linekey->exp1 key->expN key<br><br>**1**-exp1 key ->expN key ->linekey<br><br>**2**-linekey page1->page1 from exp1 key to expN key ->page2 from exp1 key to expN key ->...->linekey from page2 to page3<br><br>**3**-page1 from exp1 key to expN key ->page2 from exp1 key to expN key ->...->linekey<br><br>**Note**: N is the number of your connected expansion modules. |
| **Default** | 0 |

| **Parameter** | features.blf_list_version[2] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the phone to include the Version header in the BLF list NOTIFY message sent by the server. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

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

## State Indicator of Remote Line

The state indicator of the monitored line on BLF/BLF List key varies by phone models.

The following table shows the icons indicator associated with the line you are monitoring.

| Icons | Description |
|---|---|
| | The monitored line is idle. |
| (Flashing) | The monitored line is ringing. |
| (Flashing) | The monitored line is dialing. |
| | The monitored line is busy or in a call. |
| | The monitored line places a call on hold. |
| | A call is parked to the monitored line. |
| | The monitored line fails to register or does not exist. |

## BLF/BLF List Subscription

Yealink phones support BLF using a SUBSCRIBE/NOTIFY mechanism as specified in RFC 3265.

**BLF Subscription**

When you configure the IP phone to monitor a specific line, the phone sends a SUBSCRIBE request with Request-URI containing the monitor line URI to the server, and then receives a NOTIFY request. The NOTIFY message contains an XML body with the status of the specific monitored line.

The following example shows a NOTIFY message for a BLF line "012":

```
<?xml version="1.0"?>

<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="1" state="full" entity="sip:012@10.20.10.42:5060">

<dialog id="0000"><state>terminated</state></dialog>

</dialog-info>
```

## BLF List Subscription

When you configure the IP phone to monitor a list of specific remote lines, the phone sends a SUBSCRIBE request with Request-URI containing the BLF List URI, and then receives a NOTIFY request. The NOTIFY message contains XML body with the status of each monitor line.

The following example shows a NOTIFY message for a BLF List, the BLF List contains 4605 and 4607:

```
<?xml version="1.0" <?xml version="1.0"?>

<list xmlns="urn:ietf:params:xml:ns:rlmi" xmlns="urn:ietf:params:xml:ns:rlmi" version="0" fullState="true">

<resource uri="sip:4605@pbx.yealink.com">

<name>4605 Yealink</name>

<instance id="JQZxud2qeo" state="active" cid="8y35ri@broadworks"/>

</resource>

<resource uri="sip:4605@pbx.yealink.com">

<name>4607 Yealink</name>

<instance id="pXHQ97tPyQ" state="active" cid="tYzwJM@broadworks"/>

</resource>

</list>
```

## Topic

BLF/BLF List Subscription Configuration

## BLF/BLF List Subscription Configuration

The following table lists the parameters you can use to configure BLF/BLF List subscription.

| 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** | account.X.blf.subscribe_event[1] | <MAC>.cfg |
| **Description** | It configures the event of the BLF subscription. | |
| **Permitted Values** | **0**-dialog<br>**1**-presence | |
| **Default** | 0 | |
| **Parameter** | account.X.out_dialog_blf_enable[1] | <MAC>.cfg |
| **Description** | It enables or disables the phone to handle NOTIFY messages out of the BLF dialog. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Web UI** | Account->Advanced->Out Dialog BLF | |
| **Parameter** | account.X.blf.match_host.enable[1] | <MAC>.cfg |
| **Description** | It enables or disables host match feature for BLF/BLF list feature. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled, the phone can only recognize the NOTIFY message whose host field is the same as the one in the SUBSCRIBE message. | |
| **Default** | 0 | |
| **Parameter** | sip.terminate_notify_sub_delay_time | <y0000000000xx>.cfg |
| **Description** | It configures the interval (in seconds) for the phone to re-subscribe when it receives the NOTIFY message with the subscription state of Terminated.<br><br>If it is set to 0, the phone will re-subscribe immediately. | |
| **Permitted Values** | Integer greater than 0 | |
| **Default** | 0 | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

## Visual and Audio Alert for Monitor Lines

Visual and Audio Alert feature allows the phone to display the caller ID and play an audio alert when a BLF line receives an incoming call.

## Topics

Visual and Audio Alert BLF Lines Configuration

## Visual and Audio Alert BLF Lines Configuration

The following table lists the parameters you can use to configure a visual and audio alert for BLF lines.

| Parameter | features.pickup.blf_visual_enable | <y0000000000xx>.cfg |
|---|---|---|

| Description | It enables or disables the phone to display a visual alert when the monitored user receives an incoming call. | |
|---|---|---|
| Permitted Values | 0-Disabled<br>1-Enabled | |
| Default | 0 | |
| Web UI | Features->Pickup & Park->Visual Alert for BLF Pickup | |
| Parameter | features.pickup.blf_audio_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to play an audio alert when the monitored user receives an incoming call. | |
| Permitted Values | 0-Disabled<br>1-Enabled | |
| Default | 0 | |
| Web UI | Features->Pickup & Park->Audio Alert for BLF Pickup | |
| Parameter | features.blf_pickup_only_send_code | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to only dial out feature access code of directed pick up when performing BLF/BLF list pickup. | |
| Permitted Values | 0-Disabled, the phone dials out feature access code of directed pick up plus monitored number when performing BLF/BLF list pickup.<br>1-Enabled | |
| Default | 0 | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# LED Mode for BLF/BLF List Key

BLF LED Mode provides five kinds of definition for the BLF/BLF List key LED status. BLF LED mode is only applicable to the expansion module EXP50 connected to T58A phones.

## Topics

## Supported BLF LED Modes

The following table lists the LED statuses of the BLF/BLF list key when BLF LED Mode is set to 0, 1, 2, 3 or 4 respectively. The default value of BLF LED mode is 0.

**Expansion Module Key LED** (configured as a BLF key or a BLF List key and BLF LED Mode is set to 0)

| LED Status | Description |
|---|---|
| Solid green | The monitored user is idle. |
| Fast-flashing red (200ms) | The monitored user receives an incoming call. |
| Solid red | The monitored user is dialing.<br>The monitored user is talking.<br>The monitored user's conversation is placed on hold (This LED status requires server sup- |

| LED Status | Description |
|---|---|
| | port). |
| Slow-flashing red (1s) | The call is parked against the monitored user's phone number. |
| Off | The monitored user does not exist. |

**Expansion Module Key LED** (configured as a BLF key or a BLF List key and BLF LED Mode is set to 1)

| LED Status | Description |
|---|---|
| Fast-flashing red (200ms) | The monitored user receives an incoming call. |
| Solid red | The monitored user is dialing.<br><br>The monitored user is talking.<br><br>The monitored user's conversation is placed on hold (This LED status requires server support). |
| Slow-flashing red (1s) | The call is parked against the monitored user's phone number. |
| Off | The monitored user is idle.<br>The monitored user does not exist. |

**Expansion Module Key LED** (configured as a BLF key or a BLF List key and BLF LED Mode is set to 2)

| LED Status | Description |
|---|---|
| Fast-flashing red (200ms) | The monitored user receives an incoming call. |
| Solid red | The monitored user is dialing.<br><br>The monitored user is talking.<br><br>The monitored user's conversation is placed on hold (This LED status requires server support). |
| Slow-flashing red (1s) | The call is parked against the monitored user's phone number. |
| Off | The monitored user is idle.<br>The monitored user does not exist. |

**Expansion Module Key LED** (configured as a BLF key or a BLF List key and BLF LED Mode is set to 3)

| LED Status | Description |
|---|---|
| Fast-flashing green (200ms) | The monitored user receives an incoming calls |
| Solid red | The monitored user is dialing.<br><br>The monitored user is talking.<br><br>The monitored user's conversation is placed on hold (This LED status requires server support). |
| Slow-flashing red (1s) | The call is parked against the monitored user's phone number. |
| Off | The monitored user is idle. |

| LED Status | Description |
|---|---|
| | The monitored user does not exist. |

**Expansion Module Key LED** (configured as a BLF key or a BLF List key and BLF LED Mode is set to 4. This mode is specifically designed for the Genband server.)

| LED Status | Description |
|---|---|
| Solid green | The monitored user is talking. |
| Slow-flashing green (1s) | The monitored user does not exist. |
| Off | The monitored user is idle. |

### BLF LED Mode Configuration

The following table lists the parameters you can use to configure BLF LED Mode.

| Parameter | features.blf_led_mode | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures BLF LED mode.<br><br>**Note**: It is only applicable to the expansion module EXP50 connected to T58A phones. | |
| **Permitted Values** | 0,1,2,3,4 (4 is specifically designed for the Genband server) | |
| **Default** | 0 | |
| **Web UI** | Features->General Information->BLF LED Mode | |

# 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
- Barge in an active call
- Pull a shared call

## Topic

## State Indicator of Shared Line

The shared line is indicated by different line key icon.

The following table shows the icons indicator associated with the shared line:

| Icon | Description |
|---|---|
| | |

| | |
|---|---|
| | The shared line is idle. |
| (Monitoring SCA Phone) | The shared line is seized. |
| (Flashing) | The shared line receives an incoming call. |
| (Flashing) | The shared line is dialing. |
| | The shared line is busy or is in a call. |
| | The call on the shared line is placed on public hold. |
| (Local SCA Phone)<br><br>(Monitoring SCA Phone) | The call on the shared line is placed on private hold. |
| | The call on the shared line is barged in by the other shared line user. |
| | In a multi-party call, place the call on hold at local. |

# 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.

You have the option to provide users the ability to do the following:

- Configure a private hold soft key or Private Hold key and provide users the ability to hold a call privately.
- Configure a call pull code, which allows users to retrieve an existing call from another shared phone that is in an active or public hold status.

## Topic

## 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<br><br>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).<br><br>**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** | account.X.shared_line_callpull_code[1] | <MAC>.cfg |
|---|---|---|

| | |
|---|---|
| **Description** | It configures the call pull feature access code to retrieve an existing call from another shared phone that is in an active or public hold status.<br><br>**Note**: It works only if "account.X.shared_line" is set to 1 (Shared Call Appearance). |
| **Permitted Values** | String within 99 characters |
| **Default** | Blank |
| **Web UI** | Account->Advanced->Call Pull Feature Access Code |

| **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. |
| **Permitted Values** | **0**-Disabled, user register name to barge in, the phone sends INVITE request with the register name when barging in a call<br>**1**-Enabled, the phone sends INVITE request with the user name when barging in a call |
| **Default** | 0 |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# Intercom

Intercom is a useful feature in an office environment to quickly connect with the operator or the secretary. You can press the intercom key to place a call to a contact that is answered automatically on the contact's phone as long as the contact is not in an active call. In addition, the intercom key can be used for monitoring the status changes of a specific line on the phone.

### Topics

Intercom Key Configuration
State Monitor for Intercom Contact
Outgoing Intercom Configuration
Incoming Intercom Configuration

## Intercom Key Configuration

You can configure an Intercom key to provide users the ability to initiate intercom calls directly to the specified contact.

The following shows configuration for an Intercom key.

| Line Key Configuration | Programmable Key Configuration |
|---|---|
| linekey.X.type = 14 | programablekey.X.type = 14 |
| linekey.X.line = 1 | programablekey.X.line = 1 |

| | |
|---|---|
| linekey.X.value = 4603<br><br>linekey.X.label = Bill | programablekey.X.value = 4603 |

After provisioning, an Intercom key for Bill (4603) is available on the phone. You can tap the Intercom key to place an intercom call to Bill (4603).

If you want to use the Intercom key to pick up a call, you need to enable the Intercom key to monitor state changes, and configure the pickup code for the Intercom key, for example, set "linekey.X.extension = *97" or "pro-gramablekey.X.extension = *97". When the monitored user Bill (4603) receives an incoming call, you can tap the Intercom key to pick up the call to Bill (4603) directly.

| **Note** |
|---|
| You cannot use a programmable key to monitor an intercom contact for state changes, but tap it to pick up a call. |

### Related Topics

## State Monitor for Intercom Contact

You can make the phone to monitor a specific intercom user for state changes (busy or idle). When the monitored user receives an incoming call, the supervisor can tap the intercom key to pick up the call directly. The phones support this feature using a SUBSCRIBE/NOTIFY mechanism as specified in RFC 3265.

| **Note** |
|---|
| If you want to use the Intercom key to pick up a call, you need to configure the pickup code for the Intercom key, for example, "linekey.X.extension = *97". |

### Topics

### State Indicator of Intercom Contact

The following table shows the icon indicator associated with the Intercom key:

| Icons | Description |
|---|---|
| | The monitored user is idle. |
| | The monitored user receives an incoming call. |
| | The monitored user is dialing.<br><br>The monitored user is talking. |
| | The monitored user does not exist. |

### State Monitor for Intercom Contact Configuration

The following table lists the parameters you can use to configure state monitor for intercom contact.

| Parameter | features.intercom.led.enable | <y0000000000xx>.cfg |
|---|---|---|

| Description | It enables or disables the phone to display different intercom key icons when the status of monitored user changes.<br><br>**Note**: It works only if "features.intercom.subscribe.enable" is set to 1 (Enabled). |
|---|---|
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |
| **Parameter** | features.intercom.subscribe.enable | `<y0000000000xx>.cfg` |
| **Description** | It enables or disables intercom subscription for the phones. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |

## Outgoing Intercom Configuration

Yealink phones support two methods for initialing intercom calls.

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

| **Parameter** | account.X.call_info[1] | `<MAC>.cfg` |
|---|---|---|
| **Description** | It configures the value of the Call-Info header for intercom feature.<br><br>The value format likes: <sip:XXX (X can be any value)>; answer-after=0.<br><br>**Note:** If both Call-Info header and Alert-Info header (defined by the parameter "account.X.alert_info") are configured, the Call-Info header has a higher priority than the Alert-Info header. | |
| **Permitted Values** | String within 256 characters | |
| **Default** | Blank | |
| **Parameter** | sip.intercom_sub.enable | `<y0000000000xx>.cfg` |
| **Description** | It enables or disables intercom subscription. | |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled | |
| **Default** | 0 | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

## Incoming Intercom Configuration

The IP phone can process incoming calls differently depending on settings.

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

| **Parameter** | features.intercom.allow | `<y0000000000xx>.cfg` |
|---|---|---|
| **Description** | It enables or disables the phone to answer an incoming intercom call. | |
| **Permitted Values** | **0**-Disabled, the phone will handle an incoming intercom call like a normal incoming call.<br><br>**1**-Enabled, the phone will automatically answer an incoming intercom call. | |

| Default | 1 | |
|---|---|---|
| **Web UI** | Features->Intercom->Intercom Allow | |
| **Phone UI** | Settings->Features->Intercom->Intercom Allow | |
| **Parameter** | features.intercom.mute | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to mute the microphone when answering an intercom call.<br><br>**Note**: It works only if "features.intercom.allow" and "features.allow_mute" are set to 1 (Enabled). | |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled, the microphone is muted for intercom calls, and then the other party cannot hear you. | |
| **Default** | 0 | |
| **Web UI** | Features->Intercom->Intercom Mute | |
| **Phone UI** | Settings->Features->Intercom->Intercom Mute | |
| **Parameter** | features.intercom.tone | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to play a warning tone when answering an intercom call.<br><br>**Note**: It works only if "features.intercom.allow" is set to 1 (Enabled). | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 1 | |
| **Web UI** | Features->Intercom->Intercom Tone | |
| **Phone UI** | Settings->Features->Intercom->Intercom Tone | |
| **Parameter** | features.intercom.barge | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to answer an incoming intercom call while there is already an active call on the IP phone.<br><br>**Note**: It works only if "features.intercom.allow" and "call_waiting.enable" are set to 1 (Enabled) and "phone_setting.call_appearance.calls_per_linekey" is greater than 1. | |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled, the phone will automatically answer the intercom call and place the active call on hold. | |
| **Default** | 0 | |
| **Web UI** | Features->Intercom->Intercom Barge | |
| **Phone UI** | Settings->Features->Intercom->Intercom Barge | |
| **Parameter** | features.intercom.barge_in_dialing.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the intercom call to answer an incoming intercom call while dialing.<br><br>**Note**: It works only if "features.intercom.barge" is set to 0 (Disabled). | |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled | |
| **Default** | 0 | |

| Parameter | features.intercom.headset_prior.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the channel mode to use when receiving an incoming intercom call.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Speaker Mode<br><br>**1**-Headset Mode, it works only if you connect the headset to the IP phone and the headset mode is activated for use. | |
| Default | 1 | |
| Parameter | account.X.alert_info[1] | <MAC>.cfg |
| Description | It configures the value of the Alert-Info header for intercom feature.<br><br>The value format likes: <sip:XXX (X can be any value)>; answer-after=0.<br><br>**Note**: If both Call-Info header (defined by the parameter "account.X.call_info") and Alert-Info header are configured, the Call-Info header has a higher priority than the Alert-Info header. | |
| Permitted Values | String within 256 characters | |
| Default | Blank | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# CSTA Control

User Agent Computer Supported Telecommunications Applications (uaCSTA) is explained in detail in Using CSTA for SIP Phone User Agents (uaCSTA) and Services for Computer Supported Telecommunications Applications Phase III.

The uaCSTA feature on the phone may be used for remote control of the phone from computer applications such as PC softphone. You can use the application to control the phone to perform basic call operations. For example, place a call, answer a call, end a call and transfer a call to another party.

### Topic

CSTA Control Configuration

## CSTA Control Configuration

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

| Parameter | features.csta_control.enable[1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the CSTA feature. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Features->Remote Control->CSTA Control | |

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

# Action URL

Action URL allows the phones to interact with web server applications by sending an HTTP or HTTPS GET request.

You can specify a URL that triggers a GET request when a specified event occurs. Action URL can only be triggered by the predefined events (for example, Open DND). The valid URL format is: *http(s)://IP address of the server/help.xml?*.

An HTTP or HTTPS GET request may contain a variable name and a variable value, separated by "=". Each variable value starts with $ in the query part of the URL. The valid URL format is: *http(s)://IP address of server/help.xml?variable name-e=$variable value*. The variable name can be customized by users, while the variable value is predefined. For example, a URL "http://192.168.1.10/help.xml?mac=$mac" is specified for the event Mute, $mac will be dynamically replaced with the MAC address of the IP phone when the IP phone mutes a call.

## Topics

Predefined Events List
Variable Values List
Action URL Configuration

## Predefined Events List

The following table lists the predefined events for action URL.

| Event | Description |
|---|---|
| Setup Completed | When the IP phone completes startup. |
| Registered | When the IP phone successfully registers an account. |
| Unregistered | When the IP phone logs out of the registered account. |
| Register Failed | When the IP phone fails to register an account. |
| Off Hook | When the IP phone is off hook. |
| On Hook | When the IP phone is on hook. |
| Incoming Call | When the IP phone receives an incoming call. |
| Outgoing Call | When the IP phone places a call. |
| Established | When the IP phone establishes a call. |
| Terminated | When the IP phone terminates a call. |
| Open DND | When the IP phone enables the DND mode. |
| Close DND | When the IP phone disables the DND mode. |
| Open Always Forward | When the IP phone enables the always forward. |
| Close Always Forward | When the IP phone disables the always forward. |
| Open Busy Forward | When the IP phone enables the busy forward. |
| Close Busy Forward | When the IP phone disables the busy forward. |
| Open NoAnswer Forward | When the IP phone enables the no answer forward. |
| Close NoAnswer Forward | When the IP phone disables the no answer forward. |
| Transfer Call | When the IP phone transfers a call. |
| Blind Transfer | When the IP phone performs the blind transfer. |

| Event | Description |
|---|---|
| Attended Transfer | When the IP phone performs the semi-attended/attended transfer. |
| Hold | When the IP phone places a call on hold. |
| UnHold | When the IP phone resumes a held call. |
| Held | When a call of the IP phone is held. |
| UnHeld | When a held call is resumed. |
| Mute | When the IP phone mutes a call. |
| UnMute | When the IP phone un-mutes a call. |
| Missed Call | When the IP phone misses a call. |
| IP Changed | When the IP address of the IP phone changes. |
| Idle To Busy | When the state of the IP phone changes from idle to busy. |
| Busy To Idle | When the state of phone changes from busy to idle. |
| Reject Incoming Call | When the IP phone rejects an incoming call. |
| Answer New-In Call | When the IP phone answers a new call. |
| Transfer Failed | When the IP phone fails to transfer a call. |
| Transfer Finished | When the IP phone completes transferring a call. |
| Forward Incoming Call | When the IP phone forwards an incoming call. |
| Autop Finish | When the IP phone completes auto provisioning via power on. |
| Open Call Waiting | When the IP phone enables the call waiting. |
| Close Call Waiting | When the IP phone disables the call waiting. |
| Headset | When the IP phone presses the HEADSET key. |
| Handfree | When the IP phone presses the Speakerphone key. |
| Cancel Call Out | When the phone cancels an outgoing call in the ring-back state. |
| Remote Busy | When an outgoing call is rejected. |
| Call Remote Canceled | When the remote party cancels the outgoing call in the ringing state. |

## Variable Values List

The following table lists predefined variable values.

| Variable Value | Description |
|---|---|
| $mac | The MAC address of the IP phone. |
| $ip | The IP address of the IP phone. |

| Variable Value | Description |
|---|---|
| $model | The IP phone model. |
| $firmware | The firmware version of the IP phone. |
| $active_url | The SIP URI of the current account when the IP phone places a call, receives an incoming call or establishes a call. |
| $active_user | The user part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call. |
| $active_host | The host part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call. |
| $local | The SIP URI of the caller when the IP phone places a call. <br><br> The SIP URI of the callee when the IP phone receives an incoming call. |
| $remote | The SIP URI of the callee when the IP phone places a call. <br><br> The SIP URI of the caller when the IP phone receives an incoming call. |
| $display_local | The display name of the caller when the IP phone places a call. <br><br> The display name of the callee when the IP phone receives an incoming call. |
| $display_ remote | The display name of the callee when the IP phone places a call. <br><br> The display name of the caller when the IP phone receives an incoming call. |
| $call_id | The call-id of the active call. |
| $callerID | The display name of the caller when the IP phone receives an incoming call. |
| $calledNumber | The phone number of the callee when the IP phone places a call. |

## Action URL Configuration

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

| Parameter | action_url.setup_completed | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the action URL the phone sends after startup. <br><br> Example: <br><br> action_url.setup_completed = http://192.168.0.20/help.xml?IP=$ip | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |
| Web UI | Features->Action URL->Setup Completed | |
| Parameter | action_url.registered | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends after an account is registered. <br><br> Example: <br><br> action_url.registered = http://192.168.0.20/help.xml?IP=$ip | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |

| Web UI | Features->Action URL->Registered | |
|---|---|---|
| **Parameter** | action_url.unregistered | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends after an account is unregistered. **Example**: action_url.unregistered = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Unregistered | |
| **Parameter** | action_url.register_failed | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends after a register failed. **Example**: action_url.register_failed = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Register Failed | |
| **Parameter** | action_url.off_hook | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when off hook. **Example**: action_url.off_hook = http://192.168.0.20/help.xml?IP=$ip **Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Off Hook | |
| **Parameter** | action_url.on_hook | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when on hook. **Example**: action_url.on_hook = http://192.168.0.20/help.xml?IP=$ip **Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->On Hook | |
| **Parameter** | action_url.incoming_call | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when receiving an incoming call. | |

| | **Example**: |  |
|---|---|---|
| | action_url.incoming_call = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Incoming Call | |
| **Parameter** | action_url.outgoing_call | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when placing a call.<br>**Example**:<br>action_url.outgoing_call = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Outgoing Call | |
| **Parameter** | action_url.call_established | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when establishing a call.<br>**Example**:<br>action_url.call_established = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Established | |
| **Parameter** | action_url.dnd_on | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when DND feature is activated.<br>**Example**:<br>action_url.dnd_on = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Open DND | |
| **Parameter** | action_url.dnd_off | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when DND feature is deactivated.<br>**Example**:<br>action_url.dnd_off = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |

| Web UI | Features->Action URL->Close DND | |
|---|---|---|
| **Parameter** | action_url.always_fwd_on | \<y0000000000xx\>.cfg |
| **Description** | It configures the action URL the phone sends when the always forward feature is activated.<br>**Example**:<br>action_url.always_fwd_on = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Always Forward On | |
| **Parameter** | action_url.always_fwd_off | \<y0000000000xx\>.cfg |
| **Description** | It configures the action URL the phone sends when the always forward feature is deactivated.<br>**Example**:<br>action_url.always_fwd_off = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Always Forward Off | |
| **Parameter** | action_url.busy_fwd_on | \<y0000000000xx\>.cfg |
| **Description** | It configures the action URL the phone sends when the busy forward feature is activated.<br>**Example**:<br>action_url.busy_fwd_on = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Busy Forward On | |
| **Parameter** | action_url.busy_fwd_off | \<y0000000000xx\>.cfg |
| **Description** | It configures the action URL the phone sends when the busy forward feature is deactivated.<br>**Example**:<br>action_url.busy_fwd_off = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Busy Forward Off | |
| **Parameter** | action_url.no_answer_fwd_on | \<y0000000000xx\>.cfg |
| **Description** | It configures the action URL the phone sends when the no answer forward feature is activated.<br>**Example**:<br>action_url.no_answer_fwd_on = http://192.168.0.20/help.xml?IP=$ip | |

| Permitted Values | URL within 511 characters | |
|---|---|---|
| **Default** | Blank | |
| **Web UI** | Features->Action URL->No Answer Forward On | |
| **Parameter** | action_url.no_answer_fwd_off | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when the no answer forward feature is deactivated.<br><br>**Example**:<br><br>action_url.no_answer_fwd_off = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->No Answer Forward Off | |
| **Parameter** | action_url.transfer_call | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when performing a transfer.<br><br>**Example**:<br><br>action_url.transfer_call = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Transfer Call | |
| **Parameter** | action_url.blind_transfer_call | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when performing a blind transfer.<br><br>**Example**:<br><br>action_url.blind_transfer_call = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Blind Transfer | |
| **Parameter** | action_url.attended_transfer_call | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when performing an attended/semi-attended transfer.<br><br>**Example**:<br><br>action_url.attended_transfer_call = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Attended Transfer | |

| Parameter | action_url.hold | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the action URL the phone sends when placing a call on hold.<br><br>**Example**:<br><br>action_url.hold = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Hold | |
| Parameter | action_url.unhold | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends when resuming a hold call.<br><br>**Example**:<br><br>action_url.unhold = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->UnHold | |
| Parameter | action_url.held | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends when a call is held.<br><br>**Example**:<br><br>action_url.held = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| Parameter | action_url.unheld | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends when a held call is resumed.<br><br>**Example**:<br><br>action_url.unheld = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| Parameter | action_url.mute | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends when muting a call.<br><br>**Example**:<br><br>action_url.mute = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |

| Web UI | Features->Action URL->Mute | |
|---|---|---|
| **Parameter** | action_url.unmute | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when un-muting a call.<br><br>**Example**:<br><br>action_url.unmute = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->UnMute | |
| **Parameter** | action_url.missed_call | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when missing a call.<br><br>**Example**:<br><br>action_url.missed_call = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Missed Call | |
| **Parameter** | action_url.call_terminated | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when terminating a call.<br><br>**Example**:<br><br>action_url.call_terminated = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Terminated | |
| **Parameter** | action_url.busy_to_idle | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when changing the state of the IP phone from busy to idle.<br><br>**Example**:<br><br>action_url.busy_to_idle = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Busy to Idle | |
| **Parameter** | action_url.idle_to_busy | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when changing the state of the phone from idle to busy.<br><br>**Example**:<br><br>action_url.idle_to_busy = http://192.168.0.20/help.xml?IP=$ip | |

| Permitted Values | URL within 511 characters | |
|---|---|---|
| Default | Blank | |
| Web UI | Features->Action URL->Idle to Busy | |
| Parameter | action_url.ip_change | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends when changing the IP address of the phone.<br><br>Example:<br><br>action_url.ip_change = http://192.168.0.20/help.xml?IP=$ip | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |
| Web UI | Features->Action URL->IP Changed | |
| Parameter | action_url.forward_incoming_call | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends when forwarding an incoming call.<br><br>Example:<br><br>action_url.forward_incoming_call = http://192.168.0.20/help.xml?IP=$ip | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |
| Web UI | Features->Action URL->Forward Incoming Call | |
| Parameter | action_url.reject_incoming_call | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends when rejecting an incoming call.<br><br>Example:<br><br>action_url.reject_incoming_call = http://192.168.0.20/help.xml?IP=$ip | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |
| Web UI | Features->Action URL->Reject Incoming Call | |
| Parameter | action_url.answer_new_incoming_call | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends when answering a new incoming call.<br><br>Example:<br><br>action_url.answer_new_incoming_call = http://192.168.0.20/help.xml?IP=$ip | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |
| Web UI | Features->Action URL->Answer New Incoming Call | |

| Parameter | action_url.transfer_finished | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the action URL the phone sends when completing a call transfer.<br><br>**Example**:<br><br>action_url.transfer_finished = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Transfer Finished | |
| **Parameter** | action_url.transfer_failed | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends when failing to transfer a call.<br><br>**Example**:<br><br>action_url.transfer_failed = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Transfer Failed | |
| **Parameter** | action_url.setup_autop_finish | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends when completing auto provisioning via power on.<br><br>**Example**:<br><br>action_url.setup_autop_finish = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Autop Finish | |
| **Parameter** | action_url.call_waiting_on | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends when call waiting feature is enabled.<br><br>**Example**:<br><br>action_url.call_waiting_on = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted Values** | URL within 511 characters | |
| **Default** | Blank | |
| **Web UI** | Features->Action URL->Call Waiting On | |
| **Parameter** | action_url.call_waiting_off | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends when call waiting feature is disabled.<br><br>**Example**:<br><br>action_url.call_waiting_off = http://192.168.0.20/help.xml?IP=$ip | |
| **Permitted** | URL within 511 characters | |

| Values | |
|---|---|
| **Default** | Blank |
| **Web UI** | Features->Action URL->Call Waiting Off |
| **Parameter** | action_url.headset | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when pressing the HEADSET key.<br><br>**Example**:<br><br>action_url.headset = http://192.168.0.20/help.xml?IP=$ip<br><br>**Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | URL within 511 characters |
| **Default** | Blank |
| **Web UI** | Features->Action URL->Headset |
| **Parameter** | action_url.handfree | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when pressing the Speakerphone key.<br><br>**Example**:<br><br>action_url.handfree = http://192.168.0.20/help.xml?IP=$ip<br><br>**Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | URL within 511 characters |
| **Default** | Blank |
| **Web UI** | Features->Action URL->Handsfree |
| **Parameter** | action_url.cancel_callout | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when canceling the outgoing call in the ring-back state.<br><br>**Example**:<br><br>action_url.cancel_callout= http://192.168.0.20/help.xml?IP=$ip |
| **Permitted Values** | URL within 511 characters |
| **Default** | Blank |
| **Web UI** | Features->Action URL->Cancel Call Out |
| **Parameter** | action_url.remote_busy | <y0000000000xx>.cfg |
| **Description** | It configures the action URL the phone sends when the outgoing call is rejected.<br><br>**Example**:<br><br>action_url.remote_busy = http://192.168.0.20/help.xml?IP=$ip |
| **Permitted Values** | URL within 511 characters |
| **Default** | Blank |

| Web UI | Features->Action URL->Remote Busy | |
|---|---|---|
| Parameter | action_url.call_remote_canceled | <y0000000000xx>.cfg |
| Description | It configures the action URL the phone sends when the remote party cancels the outgoing call in the ringing state.<br><br>**Example**:<br><br>action_url.call_remote_canceled= http://192.168.0.20/help.xml?IP=$ip | |
| Permitted Values | URL within 511 characters | |
| Default | Blank | |
| Web UI | Features->Action URL->Call Remote Canceled | |

# Action URI

Yealink phones can perform the specified action by receiving and handling an HTTP or HTTPS GET request or accept a SIP NOTIFY message with the "Event: ACTION-URI" header from a SIP proxy server.

## Topics

Supported HTTP/HTTPS GET Request
Supported SIP Notify Message
Variable Values List
Action URI Configuration
Example: Capturing the Current Screen of the Phone
Example: Placing a Call via Web User Interface

## Supported HTTP/HTTPS GET Request

Opposite to action URL, action URI allows the phones to interact with web server application by receiving and handling an HTTP or HTTPS GET request. When receiving a GET request, the phone will perform the specified action and respond with a 200 OK message.

A GET request may contain a variable named as "key" and a variable value, which are separated by "=". The valid URI format is: http(s)://<phoneIPAddress>/servlet?key=variable value. For example: http://10.3.20.10/servlet?key=OK.

**Note**

Yealink phones are compatible with other two old valid URI formats: http(s)://<phoneIPAddress>/cgi-bin/ConfigManApp.com?key=variable value and http(s)://<phoneIPAddress>/cgi-bin/cgiServer.exx?key=variable value.

For security reasons, the phones do not handle HTTP/HTTPS GET requests by default. You need to specify the trusted IP address for action URI. When the IP phone receives a GET request from the trusted IP address for the first time, the phone screen prompts the message "Allow remote control?". Tap the **OK** soft key on the phone to allow remote control. You can specify one or more trusted IP addresses on the IP phone, or configure the IP phone to receive and handle the URI from any IP address.

## Supported SIP Notify Message

In addition, Yealink phones can perform the specified action immediately by accepting a SIP NOTIFY message with the "Event: ACTION-URI" header from a SIP proxy server. The message body of the SIP NOTIFY message may contain a variable named as "key" and a variable value, which are separated by "=".

This method is especially useful for users who always work in the small office/home office where a secure firewall may prevent the HTTP or HTTPS GET request from the external network.

| Note |
| --- |
| If you want to only accept the SIP NOTIFY message from your SIP server and outbound proxy server, you have to enable the Accept SIP Trust Server Only feature. For more information, refer to Accept SIP Trust Server Only. |

If you use SIP NOTIFY message method, you do not need to specify the trusted IP address for action URI. However, you should enable the IP phone to receive the action URI requests. When the IP phone receives a SIP NOTIFY message with the "Event: ACTION-URI" header from a SIP proxy server for the first time, the LCD screen also prompts the message "Allow remote control?". Tap the **OK** soft key on the phone to allow remote control.

Example of a SIP Notify with the variable value (OK):

---

Message Header

NOTIFY sip:3583@10.2.40.10:5062 SIP/2.0

Via: SIP/2.0/UDP 10.2.40.27:5063;branch=z9hG4bK4163876675

From: <sip:3586@10.2.1.48>;tag=2900480538

To: "3583" <sip:3583@10.2.1.48>;tag=490600926

Call-ID: 2923387519@10.2.40.10

CSeq: 4 NOTIFY

Contact: <sip:3586@10.2.40.27:5063>

Max-Forwards: 70


User-Agent: Yealink T58 58.83.0.15

Event: ACTION-URI

Content-Type: message/sipfrag

**Content-Length: 6**

Message Body


**key=OK**

---

## Variable Values List

Yealink phones also support a combination of the variable values in the URI, but the order of the variable value is determined by the operation of the phone. The valid URI format is: http(s)://<phoneIPAddress>/servlet?key=variable value[;variable value]. Variable values are separated by a semicolon from each other.

The following shows an example of answering an incoming call then mute the call immediately:

http://10.3.20.10/servlet?key=ASW;MUTE.

| Note |
| --- |
| The variable value is not applicable to all events. For example, the variable value "MUTE" is only applicable when the IP phone is during a call. |
| When authentication is required, you can use the following URI format: http(s)://user- |

name:password@<phoneIPAddress>/servlet?key=variable value or http(s)://<phoneIPAddress>/servlet?key=variable value&&@username:password.

The following table lists predefined variable values:

| Variable Value | Phone Action |
| --- | --- |
| OK | Tap **Settings**->**Status**. |
| SPEAKER | Press the Speakerphone key. (not applicable to CP960 phones) |
| F_TRANSFER | Transfer a call to another party. |
| VOLUME_UP | Increase the volume. |
| VOLUME_DOWN | Decrease the volume. |
| MUTE | Mute a call. |
| F_HOLD/HOLD | Place an active call on hold. |
| F_CONFERENCE | Tap the **Conference** soft key (not applicable to CP960 phones). |
| Cancel/CANCEL/X | Cancel actions, reject incoming calls or end a call. |
| 0-9/*/POUND | Press the keypad (0-9, * or #) (not applicable to CP960 phones). |
| L1-LX | Tap the line keys (X=27). |
| MSG | Press the MESSAGE key. (not applicable to CP960 phones) |
| HEADSET | Press the HEADSET key. (not applicable to CP960 phones) |
| RD | Redial the last dialed number (not applicable to CP960 phones). |
| Reboot | Reboot the phone. |
| AutoP | Perform auto provisioning. |
| DNDOn | Activate the DND feature. |
| DNDOff | Deactivate the DND feature. |
| number=xxx&outgoing_uri=y | Place a call to xxx from SIP URI y.<br>**Example**: http://10.3.20.10/servlet?key=number=1234&outgoing_uri=1006@10.2.1.48 (1234 means the number you dial out; 1006@10.2.1.48 means the SIP URL you dial from.) |
| OFFHOOK | Pick up the handset. (not applicable to CP960 phones) |
| ONHOOK | Hang up the handset (not applicable to CP960 phones). |
| ANSWER/ASW/Asw | Answer a call. |

| Variable Value | Phone Action |
|---|---|
| Reset | Reset a phone. |
| ATrans=xxx | Perform a semi-attended/attended transfer to xxx. |
| BTrans=xxx | Perform a blind transfer to xxx. |
| phonecfg=get[&accounts=x][&dnd=x][&fw=x] | Get firmware version, registration, DND or forward configuration information.<br><br>The valid value of "x" is 0 or 1, 0 means you do not need to get configuration information. 1 means you want to get con-figuration information.<br><br>**Note**: The valid URI is: http(s)://<-phoneIPAddress>/servlet?phonecfg=get[&accounts=x][&dnd=x][&fw=x]<br><br>**Example**:<br><br>http://10.3.20.10/servlet?phonecfg=get[&accounts=1][&dnd=0][&fw=1] |
| CallWaitingOn | Activate the call waiting feature. |
| CallWaitingOff | Deactivate the call waiting feature. |
| AlwaysFwdOn/BusyFwdOn/NoAnswFwdOn=xxx=n | Activate an always/busy/no answer forward feature to xxx for the IP phone ("xxx" means the destination number)<br><br>The valid value of "n" means the duration time (seconds) before forwarding incoming calls (n is the times of 6, for example, 24). It is only applicable to no answer forward feature.<br><br>**Note**: For Yealink phones, it works only if call forward mode is Phone, the always/busy/no answer forward feature will apply to all the accounts on the phone.<br><br>**Example**:<br><br>http://10.10.20.10/servlet?key=NoAnswFwdOn=1001=24 |
| AlwaysFwdOff/BusyFwdOff/NoAnswFwdOff | Deactivate the always/busy/no answer forward feature for the IP phone.<br><br>**Note**: For Yealink phones, it works only if call forward mode is Phone, the always/busy/no answer forward feature will apply to all the accounts on the phone.<br><br>**Example**:<br><br>http://10.10.20.10/servlet?key=NoAnswFwdOff |
| CALLEND/CallEnd | End a call. |
| ASW/CANCEL/HOLD/UNHOLD:xxx | Answer/end/hold/unhold a call (xxx refers to the call-id of the active call).<br><br>**Example**: |

| Variable Value | Phone Action |
|---|---|
| | http://10.10.20.10/servlet?key=ASW:33093<br><br>**Note**: To get the call-id of the active call, configure the action URL: http(s)://<phoneIPAddress>/help.xml?CallId=$call_id. For more information, refer to Action URL. |

## Action URI Configuration

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

| Parameter | features.action_uri.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to receive the action URI requests. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Parameter | features.show_action_uri_option | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to pop up the Allow Remote Control prompt when receiving action URI requests.<br><br>**Note**: It works only if "features.action_uri.enable" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Parameter | features.action_uri_limit_ip | <y0000000000xx>.cfg |
| Description | It configures server address from which the phone receives the action URI requests.<br><br>Multiple addresses are separated by commas. (for example, 10.1.4.3,10.1.4.23); Support asterisk wildcard, each asterisk represents a field of the IP address (10.10.*.* represents 10.10.0.0 to 10.10.255.255).<br><br>**Note**: It works only if "features.action_uri.enable" is set to 1 (Enabled). | |
| Permitted Values | IP address<br><br>Blank-the phone will reject any HTTP GET request.<br><br>any-the phone will accept and handle HTTP GET requests from any IP address. | |
| Default | Blank | |
| Web UI | Features->Remote Control->Action URI Allow IP List | |

## Example: Capturing the Current Screen of the Phone

You can capture the screen display of the IP phone using the action URI. The phones can handle an HTTP or HTTPS GET request. The URI format is http(s)://<phoneIPAddress>/screencapture. The captured picture is saved as a BMP or JPEG file.

You can also use the URI "http(s)://<phoneIPAddress>/screencapture/download" to capture the screen display first, and then download the image (which is saved as a JPG file and named with the phone model and the capture time) to the local system.

**Note**

Yealink phones also support capturing the screen display using the old URI "http://<-phoneIPAddress>/servlet?command=screenshot".

Before capturing the phone's current screen, ensure that the IP address of the computer is included in the trusted IP address for Action URI on the phone. When you capture the screen display, the phone may prompt you to enter the user name and password of the administrator if the web browser does not remember the user name and password for web user interface login.

## Procedure

1. Enter request URI (for example, http://10.2.20.252/screencapture) in the browser's address bar and press the Enter key on the keyboard.
2. Do one of the following:
   - If it is the first time you capture the phone's current screen using the computer, the browser will display "Remote control forbidden", and the phone screen will prompt the message "Allow remote control?".

     Tap **OK** on the phone to allow remote control. The phone will return to the previous screen.

     Refresh the web page.

     The browser will display an image of the phone's current screen. You can save the image to your local system.
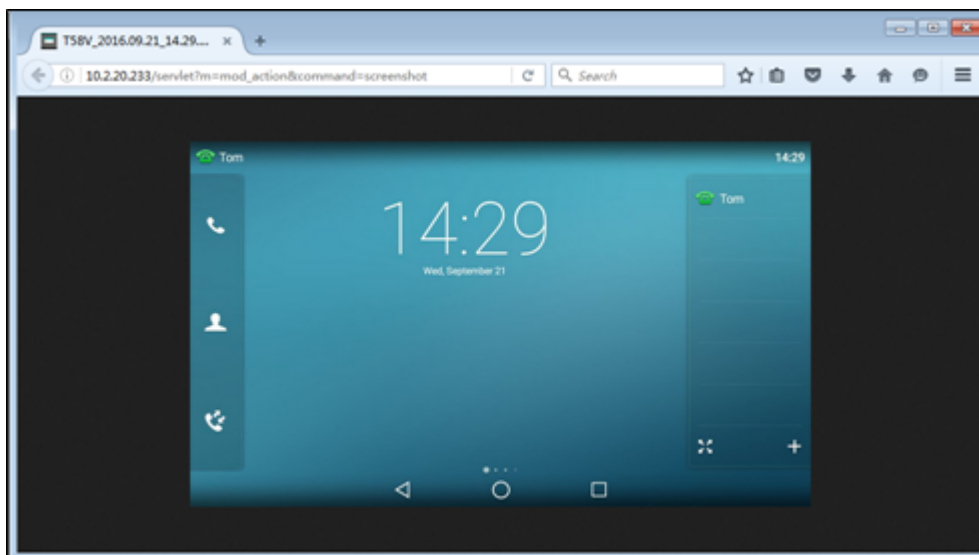


   - Else, the browser will display an image of the phone's current screen directly. You can save the image to your local system.

**Note**

Frequent capture may affect the phone performance. Yealink recommends you to capture the phone screen display within a minimum interval of 4 seconds.

## Example: Placing a Call via Web User Interface

## Procedure

1. Navigate to **Directory**->**Phone Call Info**.
2. Select the desired account from the pull-down list of **Outgoing Identity**.
3. Enter the callee's number in the **Dial Number** field.

**4.** Click **Dial** to dial out the number.

The web user interface prompts "Call Success" and the phone will automatically dial out the number.

You can click **Hang Up** to end the call.

If it is the first time you place a call via web user interface, the LCD screen will prompt the message "Allow remote control?". Tap **OK** on the phone to allow remote control and then the phone will automatically dial out the number.

| Note |
|------|
| You can also place an IP direct call via web user interface. The IP phone supports either IPv4 or IPv6 address.. |

# 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 Values | **0**-Disabled, the server automatically sends a message-summary NOTIFY in a new dialog each time the MWI status changes. (This requires server support).<br><br>**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).<br><br>**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.mwi_parse_terminated[1] <MAC>.cfg |
| **Description** | It enables or disables the phone to parse the Terminated attribute in the received MWI NOTIFY message. |
| **Permitted Values** | **0**-Disabled <br> **1**-Enabled |
| **Default** | 0 |
| **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. <br> **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. <br> **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 |
| **Phone UI** | Message->Set Voice Mail->AccountX No. |
| **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 <br> **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 <br> **1**-Enabled |

| Default | 0 |
|---|---|

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# XML Browser

XML browser simply means that the phone screen display can be managed by external applications. The XML browser feature allows users to develop and deploy custom services which meet user's functional requirements on the server. Users can customize practical applications, such as weather report, stock information, Google search, news service, and so on.

To use the XML browser feature, you must configure an XML browser key in advance.

For more information on XML browser, refer to Yealink IP Phones XML Browser Developer's Guide.

**Topic**

XML Browser Configuration

## XML Browser Configuration

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

| Parameter | push_xml.server | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the address of the push XML server. | |
| Permitted Values | **Blank**-The phone will reject HTTP POST messages from any server.<br><br>**any**-The phone will accept HTTP POST messages from any server.<br><br>**IP address** or **domain name**-Multiple addresses are separated by commas. (for example, 10.1.4.3,10.1.4.23); Support asterisk wildcard, each asterisk represents a field of the IP address (10.10.*.* represents 10.10.0.0 to 10.10.255.255). | |
| Default | Blank | |
| Web UI | Features->Remote Control->Push XML Server IP Address | |
| Parameter | push_xml.block_in_calling | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to block XML applications during a call. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Features->Remote Control->Block XML in Calling | |
| 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<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Features->Remote Control->SIP Notify | |

| Parameter | features.xml_browser.loading_tip.delay | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the time (in milliseconds) to wait for the phone to display the loading tip. If the phone doesn't finish loading an XML page within the specified time, the tip, "Loading, please wait" appears on the LCD screen. If it is set to 0, the loading tip feature is disabled. **Note**: It is not applicable to ImageScreen Object and ImageMenu Object. | |
| Permitted Values | Integer from 0 to 50000 | |
| Default | 100 | |
| Parameter | features.upload_server | <y0000000000xx>.cfg |
| Description | It configures the server address which the DssKey.cfg file is uploaded to when the phone receives an XML command (Command:UploadSystemInfo). | |
| Permitted Values | URL within 1024 characters | |
| Default | Blank | |

# Hot Desking

A primary motivation for hot desking is cost reduction. Hot desking is regularly used in places where not all employees are in the office at the same time, or not in the office for a long time, which means actual personal offices would often be vacant, consuming valuable space and resources.

Hot desking allows the user to clear pre-registration configurations of all accounts on the phone.

To use this feature, you need to assign a Hot Desking key. You can also specify which registration configurations are available for the users.

## Topics

Hot Desking Key Configuration
Hot Desking Configuration

## Hot Desking Key Configuration

The following shows configuration for a Hot Desking key.

| Line Key Configuration | Programmable Key Configuration |
|---|---|
| linekey.X.type = 34 linekey.X.label = Hot Desking | programablekey.X.type = 34 |

After provisioning, a Hot Desking key is available on the phone. You can tap the Hot Desking key to clear pre-registration configurations of all accounts and register their own account on line 1.

## Related Topic

Line Keys Configuration
Programmable Keys Configuration

# Hot Desking Configuration

You can specify available configurations for registration when using hot desking.

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

| Parameter | hotdesking.dsskey_register_name_enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the phone to provide input field of register name on the hot desking login wizard when tapping the Hot Desking DSS key. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Parameter | hotdesking.dsskey_username_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to provide input field of user name on the hot desking login wizard when tapping the Hot Desking DSS key. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Parameter | hotdesking.dsskey_password_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to provide input field of password on the hot desking login wizard when tapping the Hot Desking DSS key. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 1 | |
| Parameter | hotdesking.dsskey_sip_server_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to provide input field of SIP server on the hot desking login wizard when tapping the Hot Desking DSS key. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Parameter | hotdesking.dsskey_outbound_enable | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to provide input field of the outbound server on the hot desking login wizard when tapping the Hot Desking DSS key. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |

# General Features

This section shows you how to configure general features on Yealink phones.

## Topics

# 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 | |

Administrator's Guide for VP59/SIP-T58A/CP960 IP Phones

| | **1**-PAI |
|---|---|
| | **2**-PAI-FROM |
| | **3**-PRID-PAI-FROM |
| | **4**-PAI-RPID-FROM |
| | **5**-RPID-FROM |
| | **6**-PREFERENCE, the phone uses the custom priority order for the sources of caller identity (configured by the parameter "sip.cid_source.preference"). |
| **Default** | 0 |
| **Web UI** | Account->Advanced->Caller ID Source |
| **Parameter** | account.X.cid_source_privacy[1] <MAC>.cfg |
| **Description** | It enables or disables the phone to process the Privacy header field in the SIP message. **Note**: The priority order: PPI>Privacy>PRID/PAI/From. |
| **Permitted Values** | **0**-Disabled, the phone does not process Privacy header. **1**-Enabled, the phone screen presents anonymity instead if there is a Privacy: id in the INVITE request. |
| **Default** | 1 |
| **Parameter** | account.X.cid_source_ppi[1] <MAC>.cfg |
| **Description** | It enables or disables the phone to process the P-Preferred-Identity (PPI) header in the request message for caller identity presentation. |
| **Permitted Values** | **0**-Disabled, the phone does not process the PPI header. **1**-Enabled, the phone presents the caller identity from the PPI header. |
| **Default** | 0 |
| **Parameter** | sip.cid_source.preference <y0000000000xx>.cfg |
| **Description** | It configures the priority order for the sources of caller identity information. **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). |
| **Permitted Values** | String |
| **Default** | P-Preferred-Identity, P-Asserted-Identity, Remote-Party-ID, From |
| **Parameter** | account.X.cp_source[1] <MAC>.cfg |
| **Description** | It configures the identity of the callee according to the response message. |
| **Permitted Values** | **0**-PAI-RPID **1**-Dialed Digits **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. **3**-Contact |

| Default | 0 | |
|---|---|---|
| **Parameter** | account.X.callerid_in_support_header.enable | <MAC>.cfg |
| **Description** | It enables or disables the callerid attribute to be carried in the Supported header of the INVITE message. | |
| **Permitted Values** | **0**-Disabled <br> **1**-Enabled | |
| **Default** | 0 | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# 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 <br><br> **480**-Temporarily Unavailable <br><br> **486**-Busy Here <br><br> **603**-Decline | |
| **Default** | 486 | |
| **Web UI** | Features->General Information->Return Code When Refuse | |

# Hide Feature Access Codes

Hide Feature Access Codes feature enables the IP phone to display the feature name instead of the dialed feature access code automatically. For example, the dialed call park code will be replaced by the identifier "Call Park" when you park an active call.

The hide feature access codes feature is applicable to the following features:

- Voice Mail
- Pick up

- Group Pick up
- Barge In
- Retrieve
- Call Park
- Call Pull

**Topic**

Hide Feature Access Codes Configuration

## Hide Feature Access Codes Configuration

The following table lists the parameters you can use to configure the hide feature access codes.

| Parameter | features.hide_feature_access_codes.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the phone to display the feature name instead of the feature access code when dialing and talking.<br><br>The following feature access codes will be replaced when this feature is enabled:<br><br>- Voice Mail<br>- Pick up<br>- Group Pick up<br>- Barge In<br>- Retrieve<br>- Call Park<br>- Group Park<br>- Call Pull | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Web UI** | Features->General Information->Hide Feature Access Codes | |

## 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 from receiving the ghost calls whose phone number may be 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<br><br>**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 presented in a Supported header, it indicates that the phone can send or receive reliable provisional responses. When presented 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 T58 58.83.0.15

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<br>**1**-Enabled | |

| Default | 0 |
|---|---|
| Web UI | Account->Advanced->Retransmission |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# 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, 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 Values** | Float from 2.5 to 60 | |
| **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 T58 58.83.0.15 |
| Session-Expires: 90;refresher=uac |
| Supported: timer |
| Content-Length: 0 |

## Topic

## 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** | **0**-Disabled | |

| Values | **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 | It configures the interval (in seconds) for refreshing the SIP session during a call.<br><br>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.<br><br>**Note**: It works only if "account.X.session_timer.enable" is set to 1 (Enabled). | |
| 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 | It configures who refresh the SIP session during a call.<br><br>**Note**: It works only if "account.X.session_timer.enable" is set to 1 (Enabled). | |
| Permitted Values | **0**-UAC<br>**1**-UAS | |
| Default | 0 | |
| Web UI | Account->Advanced->Session Refresher | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

# 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 | **0**-Disabled<br>**1**-Enabled | |
| 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  T58 58.83.0.15 |
| Allow-Events: talk,hold,conference,refer,check-sync |
| Content-Length:   300 |

**Topic**

## 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")<br>**1**-Enabled | |
| **Default** | 1 | |
| **Web UI** | Features->General Information->Reserve # in User Name | |

# Busy Tone Delay

The busy tone is an audible signal to indicate that the call is released by the other party. You can define the amount of time that the busy tone lasts.

**Topic**

## 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 (in seconds) that the busy tone lasts when the call is released by the remote party. | |
| Permitted Values | **0**-the phone will not play a busy tone.<br><br>**3**-3s, a busy tone lasts for 3 seconds on the phone.<br><br>**5**-5s, a busy tone lasts 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

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<br>1-Enabled | |
| Default | 0 | |

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

## Broadsoft UC

| Parameter | bw.xmpp.enable[1] | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables the UC feature.<br>**Note**: It works only if "bw.enable" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| Permitted Values | 0-Disabled<br>1-Enabled | |
| Default | 0 | |
| Parameter | features.uc_username | <y0000000000xx>.cfg |
| Description | It configures the user name for UC authentication.<br>**Note**: It works only if "bw.xmpp.enable" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| Permitted Values | String within 99 characters | |
| Default | Blank | |
| Web UI | Applications->Broadsoft XMPP->XMPP Account->XMPP UserName | |
| Parameter | features.uc_password | <y0000000000xx>.cfg |
| Description | It configures the password for UC authentication. | |

| | Note: It works only if "bw.xmpp.enable" is set to 1 (Enabled). It is only applicable to VP59/T58A phones. |
|---|---|
| **Permitted Values** | String within 32 characters |
| **Default** | Blank |
| **Web UI** | Applications->Broadsoft XMPP->XMPP Account->XMPP Password |

| **Parameter** | bw.xmpp.presence_icon.mode | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables to display presence icon in a new style.<br>**Note**: It is only applicable to VP59/T58A phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |

| **Parameter** | bw.xmpp.change_presence.force_manual.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables to synchronize the presence status to BroadWorks server when you change your presence status manually on the IP phone.<br>**Note**: It is only applicable to VP59/T58A phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 1 | |

| **Parameter** | bw.xmpp.change_presence.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the phone to change the user's current presence state locally.<br>**Note**: It works only if "bw.xmpp.enable" is set to 1 (Enabled). It is only applicable to VP59/T58A phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |

| **Parameter** | phone_setting.dsskey_directory_auto.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the Auto Favorite feature.<br>**Note**: It works only if "bw.xmpp.enable" is set to 1 (Enabled). It is only applicable to VP59/T58A phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled, the phone will download information of favorites from the cloud server and automatically configure UC Favorite keys from the first unused line key (the line key type is configured as N/A or Line). If a line key is used, the phone will skip to the next unused line key. | |
| **Default** | 1 | |
| **Web UI** | Features->General Information->Enable Auto Favorite | |

| **Parameter** | features.uc_dir.match_tail_number | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the minimum matched digits of the tail numbers of BroadCloud Buddy. When entered number matches the tail numbers of a buddy in the buddy directory, the phone will automatically display the matched results on the phone screen when placing a call.<br>If it is set to 0, the entered number must exactly match the number of BroadCloud Buddy.<br>If it is set to other values (for example, 4), the entered number less than 4 digits would not match with the | |

| | BroadCloud contact. |
|---|---|
| | **Example**: |
| | If there is a BroadCloud Buddy name "Sunmy" with phone number "785656" and the parameter "features.uc_dir.match_tail_number" is set to "4", "5656", "85656" or "785656" would match "Sunmy (785656)". "656", "56" or "6" would not match "Sunmy (785656)". |
| | **Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | Integer greater than or equal to 0 |
| **Default** | 4 |
| **Parameter** | search_in_dialing.bw_uc_buddies.enable      \<y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to automatically search entries from the BroadSoft Buddies directory, and display results on the pre-dialing/dialing screen.<br>**Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |
| **Parameter** | search_in_dialing.bw_uc_buddies.priority      \<y0000000000xx>.cfg |
| **Description** | It configures the search priority of the BroadSoft Buddies directory.<br>**Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | Integer greater than or equal to 0 |
| **Default** | 6 |
| **Parameter** | directory_setting.bw_uc_buddies.enable      \<y0000000000xx>.cfg |
| **Description** | It enables or disables the users to access the BroadSoft Buddies directory by tapping the directory icon ( 👤 for VP59/T58A, 👤 for CP960).<br>**Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |
| **Parameter** | directory_setting.bw_uc_buddies.priority      \<y0000000000xx>.cfg |
| **Description** | It configures the display priority of the BroadSoft Buddies directory.<br>**Note**: It is not applicable to CP960 phones. |
| **Permitted Values** | Integer greater than or equal to 0 |
| **Default** | 12 |

[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** | **0**-Disabled | |

| Values | 1-Enabled |
|---|---|
| | If it is set to 0 (Disabled), the following features are unavailable on the phone: |
| | 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 |
| | Centralized Call Recording |
| | Executive and Assistant |
| | BroadWorks Mobility |
| | Group Night Forwarding |
| | 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. For VP59/T58A, X=1-16, for CP960, X=1.

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

## Broadsoft ACD

| **Parameter** | account.X.acd.initial_state[1] | <MAC>.cfg |
|---|---|---|
| **Description** | It configures the initial agent state. | |
| | **Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | **1**-Available | |
| | **2**-Unavailable | |

| Default | 1 | |
|---|---|---|
| Parameter | account.X.reason_code.Y[1][2] | <MAC>.cfg |
| Description | It configures the unavailable code which must match one of the codes configured on BroadWorks platform.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | Integer from 1 to 2147483647 | |
| Default | Blank | |
| Parameter | account.X.reason_code_name.Y[1][2] | <MAC>.cfg |
| Description | It configures the unavailable reason which must match one of the reasons configured on BroadWorks platform.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | String within 99 characters | |
| Default | Blank | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

[2]Y is the code ID. Y=1-100.

## Broadsoft Centralized Call Recording

| Parameter | account.X.call_recording.enable[1] | <MAC>.cfg |
|---|---|---|
| Description | It enables or disables the centralized call recording feature. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Parameter | bw.call_recording.mode | <y0000000000xx>.cfg |
| Description | It configures the centralized call recording mode. | |
| Permitted Values | **0**-XSI<br><br>**1**-SIP | |
| Default | 1 | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

## Broadsoft Security Classification

| Parameter | account.X.security_classification.enable[1] | <MAC>.cfg |
|---|---|---|
| Description | It enables or disables security classification feature. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

## Broadsoft Hoteling

| Parameter | account.X.hoteling.enable[1] | <MAC>.cfg |
|---|---|---|
| Description | It enables or disables the hoteling feature. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, users can use any available host (shared) phone by logging in with user credentials. After logging in, users have access to their own guest profile on the host phone. | |
| Default | 0 | |
| Parameter | account.X.hoteling.user_id[1] | <MAC>.cfg |
| Description | It configures the user ID used to log into the guest profile. | |
| Permitted Values | String within 99 characters | |
| Default | Blank | |
| Parameter | account.X.hoteling.password[1] | <MAC>.cfg |
| Description | It configures the password used to log into the guest profile.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | String within 99 characters | |
| Default | Blank | |
| Parameter | account.X.hoteling.expires[1] | <MAC>.cfg |
| Description | It configures the hoteling subscription expiration time (in seconds). | |
| Permitted Values | Integer from 30 to 2147483647 | |
| Default | 3600 | |
| Parameter | account.X.hoteling.auto_login_enable[1] | <MAC>.cfg |
| Description | It enables or disables the phone to save login credentials automatically when logging into the guest profile. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |

[1]X is the account ID. For VP59/T58A, X=1-16.

## Broadsoft Flexible Seating

| Parameter | account.X.flexible_seating.enable[1] | <MAC>.cfg |
|---|---|---|
| Description | It enables or disables the flexible seating feature.<br><br>**Note**: For host, it works only if "account.X.hoteling.enable" and "account.X.acd.enable" are set to 0 (Disabled). | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |

| Default | 0 | |
|---|---|---|
| **Parameter** | account.X.hoteling.mode[1] | <MAC>.cfg |
| **Description** | It configures the hoteling mode. | |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Hoteling<br><br>**2**-Flexible Seating Host<br><br>**3**-Flexible Seating Guest | |
| **Default** | 0 | |
| **Parameter** | account.X.hoteling.pin[1] | <MAC>.cfg |
| **Description** | It configures the flexible seating PIN. | |
| **Permitted Values** | String | |
| **Default** | Blank | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

### Related Topic

Securely Storing the LDAP Credentials

## Broadsoft Call Decline

| **Parameter** | account.X.features.call_decline.enable[1] | <MAC>.cfg |
|---|---|---|
| **Description** | It enables or disables call decline feature.<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | Blank | |
| **Parameter** | features.call_decline.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables call decline feature for the IP phone.<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |

[1]X is the account ID. For VP59/T58A, X=1-16.

## Broadsoft Network Directory

| **Parameter** | bw.xsi.directory.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the network directory feature for the phone.<br><br>**Note**: It works only if "bw.xsi.enable" is set to 1 (Enabled). | |

| | |
|---|---|
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled |
| **Default** | 0 |

| **Parameter** | bw_phonebook.group_enable | <y0000000000xx>.cfg |
|---|---|---|

| | |
|---|---|
| **Description** | It enables or disables the phone to display the group directory.<br>**0**-Disabled<br>**1**-Enabled<br>**Note**: It works only if "bw.xsi.directory.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**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.<br>**Note**: It works only if "bw.xsi.directory.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**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.<br>**Note**: It works only if "bw.xsi.directory.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**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.<br>**Note**: It works only if "bw.xsi.directory.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**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.<br>**Note**: It works only if "bw.xsi.directory.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**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.<br>**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.<br>**Note**: It works only if "bw.xsi.directory.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**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.<br>**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.<br>**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.<br>**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.<br>**Note**: It works only if "bw.xsi.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br>**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.delete.enable      \<y0000000000xx>.cfg |
| **Description** | It enables or disables the user to delete the call log entry from BroadSoft Call Log list on the phone.<br>**Note**: It works only if "bw.xsi.call_log.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled<br><br>**1**-Enabled, if you delete the BroadSoft call log entry on the phone, the call log entry will be also deleted on the BroadWorks server |
| **Default** | 0 |
| **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.<br>**Note**: It works only if "bw.xsi.call_log.enable" is set to 1 (Enabled). It is not applicable to CP960 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<br><br>**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.<br>**Note**: It works only if "bw.xsi.directory.enable" and "bw.xsi.directory.update.enable" are set to 1 (Enabled). |
| **Permitted Values** | Integer from 60 to 34560 |
| **Default** | 60 |
| **Parameter** | bw.xsi.directory.update.enable      \<y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to automatically download all contacts in the BroadSoft Directory from the server.<br>**Note**: It works only if "bw.xsi.directory.enable" is set to 1 (Enabled). |
| **Permitted Values** | **0**-Disabled, the phone downloads partial contacts from the server (the maximum of contacts available for viewing at one time is determined by the server), and you can manually download the remaining contacts as needed. |

| | | |
|---|---|---|
| | **1**-Enabled | |
| **Default** | 1 | |
| **Parameter** | bw_phonebook.group_common_displayname | <y0000000000xx>.cfg |
| **Description** | It configures the display name on the phone screen for the group common directory.<br><br>**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** | bw.calllog_and_dir | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to directly enter the Network Calls screen when tapping    (for VP59/T58A)/**History** (for CP960) on the idle screen.<br><br>**Note**: It works only if "bw.xsi.call_log.enable" is set to 1 (Enabled). | |
| **Permitted Values** | **0**-Disabled, the phone will enter Local Calls screen when tapping    (for VP59/T58A)/**History** (for CP960).<br>**1**-Enabled | |
| **Default** | 0 | |
| **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<br>**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 | |
| **Parameter** | directory_setting.bw_directory.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the users to access the BroadSoft directory by tapping the directory icon (   for VP59/T58A,   for CP960). | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Parameter** | directory_setting.bw_directory.priority | <y0000000000xx>.cfg |
| **Description** | It configures the display priority of the BroadSoft directory. | |
| **Permitted** | Integer greater than or equal to 0 | |

| | |
|---|---|
| **Values** | |
| **Default** | 6 |

## Broadsoft Visual Voice Mail

| | | |
|---|---|---|
| **Parameter** | bw.voice_mail.visual.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the visual voice mail feature for the phone.<br>**Note**: It works only if "bw.xsi.enable" is set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Parameter** | bw.voice_mail.visual.display_videomail.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to display the video mails in the voice mail list.<br>**Note**: It works only if "bw.xsi.enable" and "bw.voice_mail.visual.enable" are set to 1 (Enabled). It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Parameter** | voice_mail.message_key.mode | <y0000000000xx>.cfg |
| **Description** | It configures the phone behavior when pressing the MESSAGE key when the phone is idle.<br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | **0**-enter the Set Voice Mail Code screen if the voice mail access code has not been configured; dial out the voice mail access code if the voice mail access code has been configured.<br>**1**-enter the View Voice Mail screen | |
| **Default** | 0 | |

## Broadsoft SCA

| | | |
|---|---|---|
| **Parameter** | account.X.share_line.barge_in.enable[1] | <MAC>.cfg |
| **Description** | It enables or disables the users to interrupt/barge into an active call on the shared line. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 1 | |
| **Parameter** | account.X.shared_line_one_touch_bargein.enable[1] | <MAC>.cfg |
| **Description** | It enables or disables the phone to barge in the call between remote shared line party and the third party bytapping the line key. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **Parameter** | account.X.shared_line_one_touch_retrieve.enable[1] | <MAC>.cfg |

| Description | It enables or disables the phone to retrieve the public held call on remote shared line party phone by tapping the line key. |
|---|---|
| Permitted Values | **0**-Disabled<br>**1**-Enabled |
| Default | 1 |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

## Broadsoft Call Park

| Parameter | features.call_park.park_mode | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the call park mode. | |
| Permitted Values | **0**-XSI<br><br>**1**-FAC, park a call through dialing the call park code. | |
| Default | 0 | |
| Web UI | Features->Pick up & Park->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<br><br>**1**-Enabled, users can select **GPark** during a call to park a call to the first available user in the call park group, and select **Retrieve** in the dialing screen to retrieve the parked call. | |
| Default | 0 | |
| Web UI | Features->Pickup & Park->Group Call Park | |
| Parameter | features.call_park.park_ring | <y0000000000xx>.cfg |
| Description | It enables or disables the phone to play a warning tone when a call is parked against its line.<br>**Note**: It works only if "features.call_park.park_visual_notify_enable" is set to 1 (Enabled). | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Features->Pickup & Park->Audio Alert for Parked Call | |
| Parameter | features.call_park.park_visual_notify_enable | <y0000000000xx>.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<br>**1**-Enabled | |
| Default | 0 | |
| Web UI | Features->Pickup & Park->Visual Alert for Parked Call | |
| Parameter | features.call_park.group_park_code | <y0000000000xx>.cfg |
| Description | It configures the group call park code.<br>**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->Pickup & Park->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<br>**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. For VP59/T58A, X=1-16, for CP960, X=1.

## Broadsoft Emergency Call

| Parameter | bw.emergency_calling.enable | <y0000000000xx>.cfg |
|---|---|---|
| Description | It enables or disables BroadWorks Emergency Calling feature. | |
| Permitted Values | **0**-Disabled<br>**1**-Enabled, the phone supports network hold and operator ring-back for emergency calls. | |
| Default | 0 | |

## BroadSoft Call Waiting Sync

| Parameter | call_waiting.mode | <y0000000000xx>.cfg |
|---|---|---|
| Description | It configures the call waiting mode.<br>**Note**: If it is set to 1 (XSI), it works only if "bw.xsi.enable" is set to 1 (Enabled). | |
| Permitted Values | **0**-Local<br>**1**-XSI, the status of the call waiting feature between the IP phone and the BroadWorks server can be synchronized. | |
| 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.compact_header_enable[1] | <MAC>.cfg |
|---|---|---|

| Description | It enables or disables the phone to support compact SIP header. | |
|---|---|---|
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 0 | |
| **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.call_id_mode[1] | <MAC>.cfg |
| **Description** | It configures the constitution of call ID. | |
| **Permitted Values** | **0**-Use random digits<br><br>**1**-Use the combination of the digits and letters<br><br>**2**-Use random digits plus MAC address | |
| **Default** | 0 | |
| **Parameter** | features.call_invite_format | <y0000000000xx>.cfg |
| **Description** | It configures the format of callee field in the INVITE message. | |
| **Permitted Values** | **0**-sip:XXX<br><br>**1**-tel:Number, you need to set "account.X.outbound_proxy_enable" to 1. | |
| **Default** | 0 | |
| **Parameter** | sip.escape_characters.enable | <y0000000000xx>.cfg |
| **Description** | It enables or disables the phone to convert ASCII characters. | |
| **Permitted Values** | **0**-Disabled<br>**1**-Enabled | |
| **Default** | 1 | |
| **Case Scenario** | Target characters: **%5F** (escape character **%** plus the ASCII characters **5F**)<br><br>1. If you want to convert the ASCII characters, set the following:<br><br>sip.escape_characters.enable = 1<br><br>sip.reserve_characters = %NULL%<br><br>Result: The target characters **%5F** are converted to _.<br><br>2. If you do not want to convert the ASCII characters, set the following:<br><br>sip.escape_characters.enable = 0<br><br>sip.reserve_characters = %<br><br>Result: The target characters **%5F** remain the same. | |
| **Parameter** | sip.reserve_characters | <y0000000000xx>.cfg |
| **Description** | It specifies the characters that the phone does not recognize as the escape one. | |

| | |
|---|---|
| | Multiple characters are not separated. |
| **Permitted Values** | String |
| **Default** | Blank |
| **Related Parameter** | sip.escape_characters.enable |

| Parameter | sip.tcp_port_random_mode[2] | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the listening port mode. | |
| **Permitted Values** | **0**-random source port (non 506x), fixed ports (506x) carried in the Contact, Via header. **1**-random source port (non 506x) and other ports (non 506x) carried in the Contact, Via header. | |
| **Default** | 1 | |

| Parameter | sip.listen_mode | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the listening mode. | |
| **Permitted Values** | **0**-according to the transport protocol **1**-listening TCP and UDP **2**-listening TCP and UDP, and subscribe for BLF List containing transport=TCP in the Contact header. | |
| **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.call_fail_use_reason.enable | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It enables or disables the phone screen to display the reason carried in the **Reason** header of SIP response when the phone fails to dial out. | |
| **Permitted Values** | **0**-Disabled **1**-Enabled | |
| **Default** | 0 | |

[1]X is the account ID. For VP59/T58A, X=1-16, for CP960, X=1.

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

## Call Settings Parameters

| Parameter | phone_setting.show_code403 | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the display message on the phone screen when receiving a 403 message. If it is left blank, the phone will display the value sent from the server when receiving the 403 message. | |
| **Permitted** | String within 99 characters | |

| Values | |
|---|---|
| **Default** | Blank |

# APP Settings Configuration

| Parameter | app.install_url | <y0000000000xx>.cfg |
|---|---|---|
| **Description** | It configures the access URL of application.<br><br>**Example**:<br><br>app.install_url = http://192.168.1.10/com.google.android.music_48181.apk<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | String | |
| **Default** | Blank | |
| **Parameter** | app.uninstall | <y0000000000xx>.cfg |
| **Description** | It uninstalls the application.<br><br>**Example**:<br><br>To uninstall the application, do one of the following:<br><br>app.uninstall = com.google.android.music_48181.apk<br><br>app.uninstall = Google Play Music<br><br>app.uninstall = com.google.android.music<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | Software package name or APK file name or Application name | |
| **Default** | Blank | |
| **Parameter** | app.autorun | <y0000000000xx>.cfg |
| **Description** | It specifies the application to automatically run after the phone starts up.<br><br>Multiple applications are separated by slashs.<br><br>**Note**: It is not applicable to CP960 phones. | |
| **Permitted Values** | Software package name or APK file name or Application name | |
| **Default** | Blank | |
| **Parameter** | app.unavailable | <y0000000000xx>.cfg |
| **Description** | It configures the IP phone to hide or disable the preloaded applications or GMS services.<br><br>Multiple applications/services are separated by slashs.<br><br>**Example**:<br><br>app.unavailable = com.google.android.onetimeinitializer/com.google.android.configupdater | |
| **Permitted Values** | Software package name or APK file name or Application name | |

| Default | Blank | |
|---|---|---|
| Parameter | features.hide_world_clock.enable | <y0000000000xx>.cfg |
| Description | It enables or disables to hide the world clock.<br><br>**Note**: It is not applicable to CP960 phones. | |
| Permitted Values | **0**-Disabled<br><br>**1**-Enabled, the world clock icon disappears from the digital clock widget. Users can not add the clock of other cities on the phone. | |
| Default | 0 | |

## Related Topic

GMS Services List

# 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.

# Reading Icons

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

| VP59/T58A | CP960 | Description |
|---|---|---|
|  |  | Network is unavailable |
|  |  | Private line registers successfully |
|  |  | Registration failed |
| (Flashing) | (Flashing) | Registering |
|  | / | Hands-free (speakerphone) mode |
|  | / | Handset mode |
|  | / | Headset mode |
|  |  | Voice Mail |
|  |  | Auto Answer |

| VP59/T58A | CP960 | Description |
|:---:|:---:|:---|
| ⊖ | ⊖ | Do Not Disturb |
| ↩ | ↩ | Call Forward |
| (II) | / | Call Hold (video) |
| (II) | / | Call Hold (audio-only) |
| 🎙 | / | Call Mute |
| 🎙 | 🎙 | Keep Mute |
| 🔓 | / | Call is encrypted (video) |
| 🔓 | / | Call is encrypted (audio-only) |
| 🔇 | 🔇 | Silent mode |
| 📷 | / | Camera is not detected |
| 🔒 | 🔒 | Phone Lock |
| 📞 | 📞 | Received Calls |
| 📞 | 📞 | Placed Calls |
| 📞 | 📞 | Missed Calls |
| 📞 | 📞 | Forwarded Calls |
| 🗑 | 🗑 | Recording box is full |
| 🚫 | 🚫 | A call cannot be recorded |
| ⏺ | ⏺ | Recording starts successfully |
| 🚫 | 🚫 | Recording cannot be started |
| 🚫 | 🚫 | Recording cannot be stopped |
| V | V | VPN is enabled |

| VP59/T58A | CP960 | Description |
|---|---|---|
| (Bluetooth icon grey) | (Bluetooth icon grey) | Bluetooth mode is on |
| (Bluetooth icon green) | / | Bluetooth headset is both paired and connected |
| (mobile icon) | (mobile icon green) | Bluetooth-enabled mobile phone is both paired and connected |
| (Wi-Fi icon) | (Wi-Fi icon) | Wi-Fi mode is on |
| (contact icon) | (contact icon) | The default local caller photo and local contact icon |
| (contact icon with bluetooth) | (contact icon with bluetooth) | The default mobile caller photo and mobile contacts icon |
| (DSS key icon) | / | DSS Key |
| (phone icon green) | (phone icon green) | Line key type is Line (line is seized) |
| (keypad icon) | (keypad icon) | Line key type is Speed Dial |
| (mobile icon green) | (mobile icon green) | Line key type is Mobile Account (Bluetooth-enabled mobile phone is connected successfully) |
| (mobile icon grey) | (mobile icon grey with x) | Line key type is Mobile Account (Bluetooth-enabled mobile phone connection failed) |
| (mobile icon green) (Flashing) | (mobile icon green) (Flashing) | Line key type is Mobile Account (Bluetooth-enabled mobile phone is connecting) |
| (contact green) | (contact green) | Line key type is BLF/BLF List (BLF/BLF list idle state) |
| (contact red) | (contact red) | Line key type is BLF/BLF List (BLF/BLF list ringing state) |
| (contact red) | (contact red) | Line key type is BLF/BLF List (BLF hold state) |
| (contact red arrow) | (contact red arrow) | Line key type is BLF/BLF List (BLF/BLF list callout state) |
| (contact grey) | (contact grey) | Line key type is BLF/BLF List (BLF/BLF list failed state) |
| (contact red signal) | (contact red signal) | Line key type is BLF/BLF List (BLF list call park state) |
| (voicemail icon) | (voicemail icon) | Line key type is Voice Mail |
| (pickup icon) | (pickup icon) | Line key type is Direct Pickup |

| VP59/T58A | CP960 | Description |
|---|---|---|
| | | Line key type is Group Pickup |
| | | Line key type is Call Park (park successfully/call park idle state) |
| | | Line key type is Call Park (call park ringing state) |
| | | Park failed |
| | | Line key type is Intercom (intercom idle state) |
| | | Line key type is Intercom (intercom ringing state) |
| Callout | Callout | Line key type is Intercom (intercom callout state) |
| Talking | Talking | Line key type is Intercom (intercom talking state) |
| | | Line key type is Intercom (intercom failed state) |
| | | Line key type is DTMF/Prefix |
| | | Line key type is Local Group/XML Group/LDAP |
| | | Line key type is XML Browser |
| | / | Line key type is Conference |
| | | Line key type is Forward |
| | / | Line key type is Transfer |
| | / | Line key type is Hold |
| | | Line key type is DND |
| | | Line key type is Recall |

| VP59/T58A | CP960 | Description |
|---|---|---|
| | | Line key type is Record/URL Record |
| | | Line key type is Record/URL Record (recording starts successfully) |
| | | Line key type is Multicast Paging/Group Listening (Group Listening is not applicable CP960 phones) |
| | | Line key type is Hot Desking |
| | | Line key type is Zero Touch |
| | | Line key type is URL |
| | / | Line key type is DECT Intercom |
| | / | The ACD state is available |
| | / | The ACD state is unavailable |
| | / | The ACD state is wrap up |
| | / | Log out of the ACD system |
| | | The shared line/bridged line is idle |
| (Flashing) | (Flashing) | The shared line receives ring-back tone |
| (Flashing) | (Flashing) | The shared line receives an incoming call |
| | | The shared line is in conversation |
| | | The shared line conversation is placed on public hold |
| | | USB flash drive is detected |

| VP59/T58A | CP960 | Description |
|---|---|---|
| HD | HD | High Definition Voice |
| | / | Screenshot captured |
| | / | Downloading file |
| | / | Uploading file |
| | / | Upcoming alarm |
| | / | Unread email |
| / | | The slave phone is disconnected with the master phone. |
| / | | The star connection group is set up, but there are no slave phones in the star connection group. |
| / | n | The number of the slave phones connected successfully is less than the maximum number of slave phones in a star connection group. "n" indicates the number of connected slave phones. |
| / | n | All the slave phones in the star connection group are connected successfully. "n" indicates the number of connected slave phones. |
| | | Phone Warning |
| | / | Sharing Content |