Yealink W60P DECT IP Phone Administrator Guide

Version 81.30

Feb. 2018

Copyright

Trademarks

Warranty

(1) **Warranty**

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

(2) **Disclaimer**

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

(3) **Limitation of Liability**

Yealink and/or its respective suppliers are not responsible for the suitability of the information contained in this document for any reason. The information is provided "as is", and Yealink does not provide any warranty and is subject to change without notice. All risks other than risks caused by use of the information are borne by the recipient. In no event, even if Yealink has been suggested the occurrence of damages that are direct, consequential, incidental, special, punitive or whatsoever (Including but not limited to loss of business profit, business interruption or loss of business information), shall not be liable for these damages.

End User License Agreement

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

Patent Information

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

Customer Feedback

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

Technical Support

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

GNU GPL INFORMATION

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

The original GPL license, source code of components licensed under GPL and used in Yealink products can be downloaded from Yealink web site:
http://www.yealink.com/GPLOpenSource.aspx?BaseInfoCateId=293&NewsCateId=293&CateId=293.

Introduction

About This Guide

Yealink administrator guide is intended for administrators who need to properly configure, customize, manage, and troubleshoot the DECT IP phone system rather than end-users. This guide will help you understand the Voice over Internet Protocol (VoIP) network and Session Initiation Protocol (SIP) components, and provides descriptions of all available phone features.

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

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

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

The information detailed in this guide is applicable to firmware version 81 or higher. The firmware format is like x.x.x.x.rom. The second x from left must be greater than or equal to 81 (e.g., the firmware version of: 77.81.0.10.rom).

Chapters in This Guide

This administrator guide includes the following chapters:

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

- Chapter 7, "Configuring Security Features" describes how to configure the security features on DECT IP phones.
- Chapter 8, "Troubleshooting" describes how to troubleshoot DECT IP phones and provides some common troubleshooting solutions.
- Chapter 9, "Appendix" provides the glossary, time zones, trusted certificates, auto provisioning flowchart, reference information about DECT IP phones compliant with RFC 3261, SIP call flows and some other function lists (e.g., Time Zones).

Related Documentations

This guide covers W60P DECT IP phones. The following related documents are available:

- Quick Start Guides, which describe how to assemble DECT IP phones and configure the most basic features available on DECT IP phones.
- User Guides, which describe how to configure and use the basic and advanced features available on DECT IP phones via handset user interface.
- Auto Provisioning Guide, which describes how to provision DECT IP phones using the boot file and configuration files.

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

  Note that Yealink administrator guide contains most of parameters. If you want to find out more parameters which are not listed in this guide, please refer to *Description of Configuration Parameters in CFG Files* guide.
- y000000000000.boot template boot file.
- y000000000077.cfg and <MAC>.cfg template configuration files.
- Deployment Guide for BroadSoft UC-One Environment, which describes how to configure BroadSoft features on the BroadWorks web portal and DECT IP phones.
- DECT IP phone Features Integrated with BroadSoft UC-One User Guide, which describes how to configure and use DECT IP phone features integrated with BroadSoft UC-One on Yealink DECT IP phones.

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

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

Conventions Used in Yealink Documentations

Yealink documentations contain a few typographic conventions and writing conventions.

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

Convention	Description
Bold	Highlights the web/handset user interface items such as menus, menu selections, soft keys, or directory names when they are involved in a procedure or user action (e.g., Click on **Settings**->**Upgrade**.). Also used to emphasize text (e.g., **Important!**).
Italics	Used to show the format of examples (e.g., *http(s)://[IPv6 address]*), or to show the title of a section in the reference documentations available on the Yealink Technical Support Website (e.g., *Triggering the DECT IP phone to Perform the Auto Provisioning*).
Blue Text	Used for cross references to other sections within this documentation (e.g., refer to Call Waiting on page 214), for hyperlinks to non-Yealink websites (e.g., RFC 3315) or for hyperlinks to Yealink Technical Support website.
Blue Text in Italics	Used for hyperlinks to Yealink resources outside of this documentation such as the Yealink documentations (e.g., *Yealink DECT IP Phones Description of Configuration Parameters in CFG Files_V81.xlsx*).

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

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

Reading the Configuration Parameter Tables

The feature descriptions discussed in this guide include two tables. One is a summary table of provisioning methods that you can use to configure the features. The other is a table of details of the configuration parameters that you configure to make the features work.

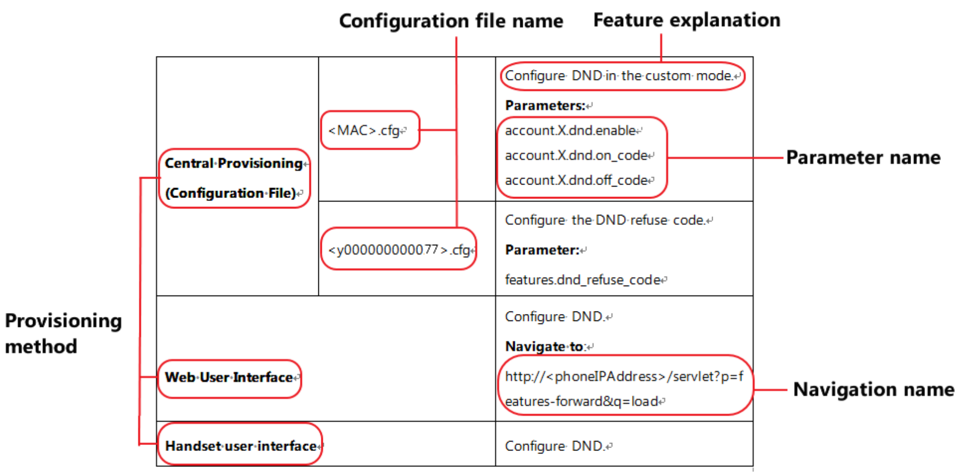
This brief section describes the conventions used in the summary table and configuration parameter table. In order to read the tables and successfully perform configuration changes, an understanding of these conventions is necessary.

Summary Table Format

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

The central provisioning method requires you to configure parameters located in CFG format configuration files that Yealink provides. For more information on configuration files, refer to Configuration Files on page 86. As shown below, the table specifies the configuration file name and the corresponding parameters. That is, the <MAC>.cfg file contains the *account.X*.dnd.enable, *account.X.dnd.on_code* and *account.X.dnd.off_code* parameters, and the y000000000077.cfg file contains the *feature.dnd_refuse_code* parameter.

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



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

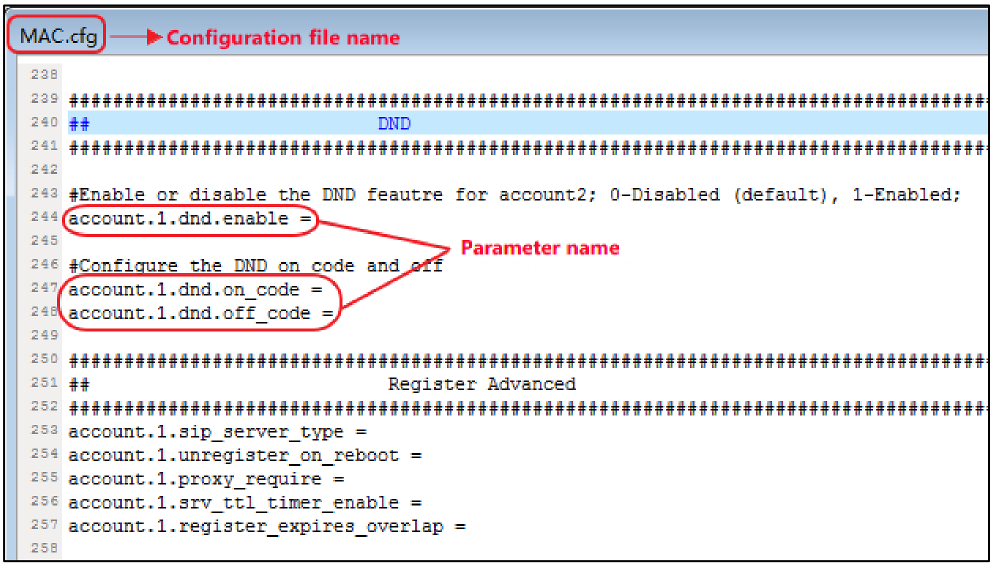
Method 1: Central Provisioning

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

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

For example, if you want to enable the DND feature for account 1, you need to locate the account.1.dnd.enable in the MAC.cfg file and then configure it as required (e.g., *account.1*.dnd.enable = 1).

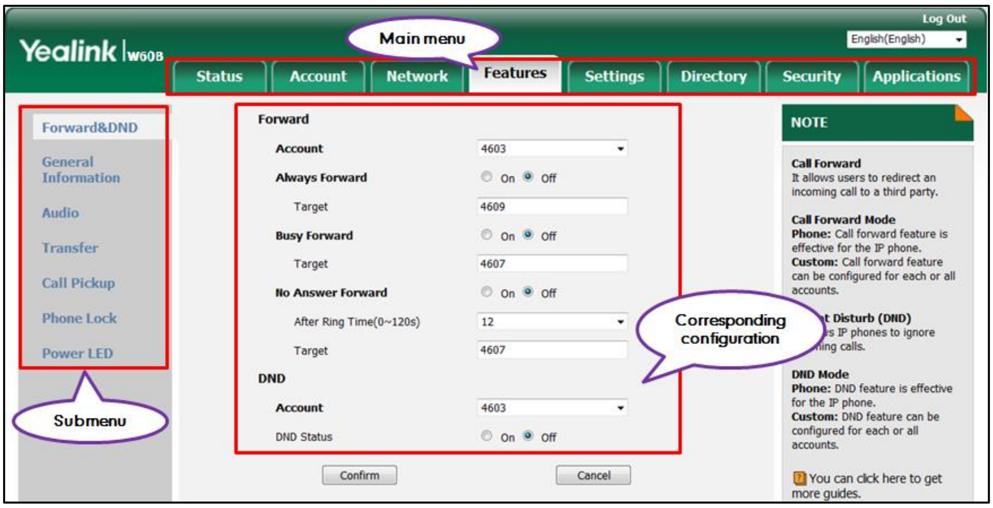
The following shows a segment of MAC.cfg file:



Method 2: Web User Interface

As described in the chapter Summary Table Format, you can directly navigate to the specified webpage to configure the feature. You can also first log into the web user interface, the default user name and password for the administrator are both “admin” (case-sensitive). Yealink DECT IP phones support both HTTP and HTTPS protocols for accessing the web user interface. For more information, refer to Web User Interface on page 83.

The following web user interface takes **Features**->**Forward&DND** as an example:



Method 3: Handset User Interface

An administrator or a user can configure and use DECT IP phones via handset user interface. Not all features are available on handset user interface. You can only access some features when the handset disconnects with the base station.

Recommended References

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

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

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

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

Understanding VoIP Principle and SIP Components

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

VoIP Principle

VoIP

VoIP (Voice over Internet Protocol) is a technology using the Internet Protocol instead of traditional Public Switch Telephone Network (PSTN) technology for voice communications.

It is a family of technologies, methodologies, communication protocols, and transmission techniques for the delivery of voice communications and multimedia sessions over IP networks. The H.323 and Session Initiation Protocol (SIP) are two popular VoIP protocols that are found in widespread implementation.

H.323

H.323 is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network. The H.323 standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences.

It is widely implemented by voice and video conference equipment manufacturers, is used within various Internet real-time applications such as GnuGK and NetMeeting and is widely deployed by service providers and enterprises for both voice and video services over IP networks.

SIP

SIP (Session Initiation Protocol) is the Internet Engineering Task Force's (IETF's) standard for multimedia conferencing over IP. It is an ASCII-based, application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints. Like other VoIP protocols, SIP is designed to address functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control attributes of an end-to-end call.

SIP provides capabilities to:

- Determine the location of the target endpoint -- SIP supports address resolution, name mapping, and call redirection.
- Determine media capabilities of the target endpoint -- Via Session Description Protocol (SDP), SIP determines the "lowest level" of common services between endpoints. Conferences are established using only media capabilities that can be supported by all endpoints.
- Determine the availability of the target endpoint -- A call cannot be completed because the target endpoint is unavailable, SIP determines whether the called party is already on the DECT IP phone or does not answer in the allotted number of rings. It then returns a message indicating why the target endpoint is unavailable.
- Establish a session between the origin and target endpoint -- The call can be completed,

SIP establishes a session between endpoints. SIP also supports mid-call changes, such as the addition of another endpoint to the conference or the change of a media characteristic or codec.

- Handle the transfer and termination of calls -- SIP supports the transfer of calls from one endpoint to another. During a call transfer, SIP simply establishes a session between the transferee and a new endpoint (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions between all parties.

SIP Components

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

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

User Agent Client (UAC)

The UAC is an application that initiates up to six feasible SIP requests to the UAS. The six requests issued by the UAC are: INVITE, ACK, OPTIONS, BYE, CANCEL and REGISTER. When the SIP session is being initiated by the UAC SIP component, the UAC determines the information essential for the request, which is the protocol, the port and the IP address of the UAS to which the request is being sent. This information can be dynamic and will make it challenging to put through a firewall. For this reason, it may be recommended to open the specific application type on the firewall. The UAC is also capable of using the information in the request URI to establish the course of the SIP request to its destination, as the request URI always specifies the host which is essential. The port and protocol are not always specified by the request URI. Thus if the request does not specify a port or protocol, a default port or protocol is contacted. It may be preferential to use this method when not using an application layer firewall. Application layer firewalls like to know what applications are flowing through which ports and it is possible to use content types of other applications other than the one you are trying to let through what has been denied.

User Agent Server (UAS)

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

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

Summary of Changes

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

Changes for Release 81, Guide Version 81.30

The following section is new for this version:

- Number of Active Handsets on page 151

Major updates have occurred to the following sections:

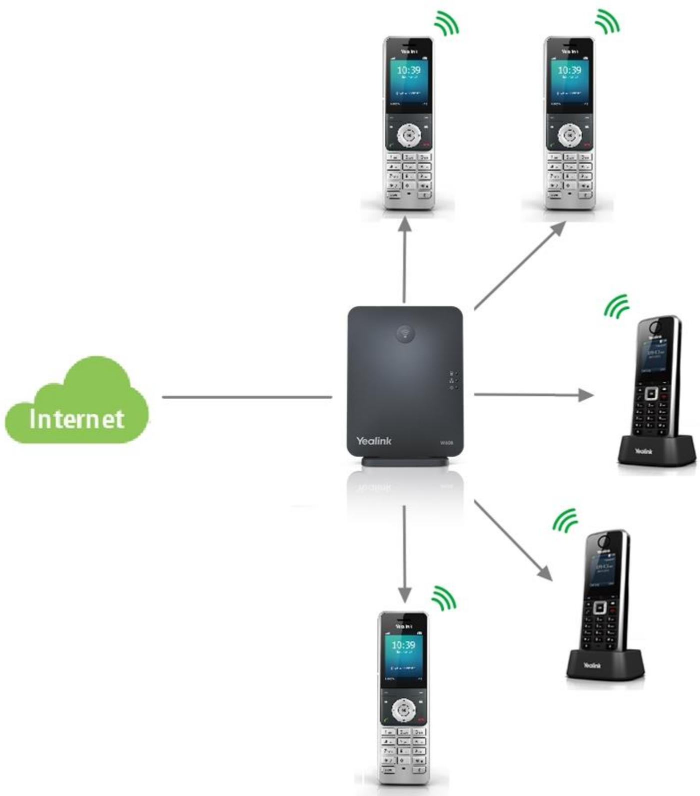
- Registering the Handset on page 8
- Number of Simultaneous Outgoing Calls on page 152
- Number Assignment on page 156
- Dial Plan on page 186
- Transport Layer Security (TLS) on page 403

Table of Contents

Product Overview

Yealink DECT IP phone is a SIP Cordless Phone System designed for small business, which consists of base station and cordless handset. Yealink DECT IP phone supports the following features:

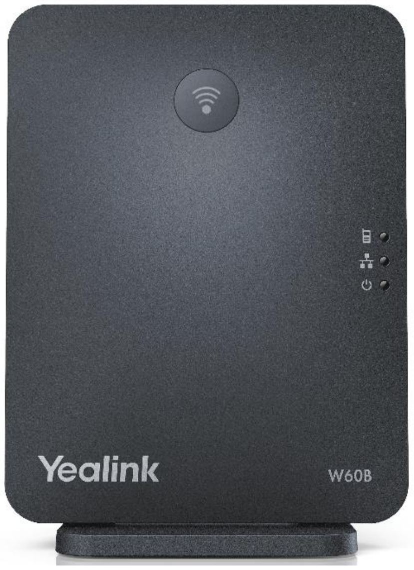
- Up to 8 handsets for one base depending on your needs.
- Up to 4 different bases to register per handset.
- Up to 8 simultaneous calls per base station.
- Up to 2 simultaneous calls per handset.
- Increase range with up to 6 repeaters (RT10) or 5 repeaters (RT20/RT20U).
- Energy-saving ECO features.



This chapter contains the following information about DECT IP phones:

- Base Station
- Handset Models
- Battery Information

Base Station



Physical Features:

3 LEDs on Base: 1*power, 1*network, 1* registration

1*RJ45 10/100Mbps Ethernet port

1 dedicated hard key (Paging key)

8 VoIP accounts

Indoor range: 20m~50m (The ideal distance is 50m)

Outdoor range: 300m (In ideal conditions)

Power adapter: DC 5V/600mA output

Power over Ethernet (IEEE 802.3af)

Handset Models

W56H

2.4'' 240x320 pixels color display

10 numerical keys, 6 function keys, 5 navigation keys, 2 softkeys, # key, * key

1 earphone jack (3.5 mm)

14 key backlight

Energy-saving ECO mode/ECO Mode+

Power adapter: DC 5V/600mA output

W52H

1.8'' 128x160 pixels color display

10 numerical keys, 6 function keys, 5 navigation keys, 2 softkeys, # key, * key

1 earphone jack (2.5 mm)

18 keys backlight

Energy-saving ECO mode/ECO Mode+

Power adapter: DC 5V/600mA output

Battery Information

For W56H

Applicable Standards: GB/T 18287−2013/GB 31241-2014

Voltage: 3.7V

Capacity: 1460mAh

Maximum charging voltage: 4.2V

Charge Temperature: 0~45℃

Charging time: approximately 3.5~4 hours (from fully discharged to full capacity).

Standby time: up to 400 hours when the backlight is disabled.

Talk time: up to 30 hours active talk time (with full charged battery).

For W52H

Technology: Nickel Metal Hydride (NiMH)

Size: AAA

Voltage: 1.2V

Capacity: 800mAh

Charging time: approximately 6 hours (fully discharged to full capacity).

Standby time: up to 100 hours when the backlight is disabled.

Talk time: up to 10 hours active talk time (with full charged batteries).

Note Due to their construction, they will undergo some wear and tear. The lifetime of battery also depends on correct maintenance. Charging and discharging are the most important factors.

Getting Started

This chapter describes where Yealink DECT IP phones fit in your network and provides basic installation instructions.

This chapter provides the following sections:

- What DECT IP Phones Need to Meet
- Connecting the DECT IP Phones
- Initialization Process Overview
- Verifying Startup

What DECT IP Phones Need to Meet

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

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

Connecting the DECT IP Phones

Connecting the Base Station

You have two options for power and network connection of the base station. Your system administrator will advise you which one to use.

- AC power (Optional)
- Power over Ethernet (PoE)

Note

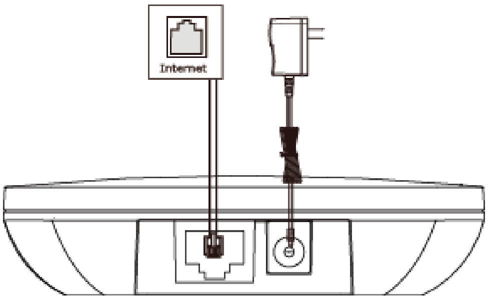
Please pay attention to the radio coverage of the base station. It is up to 300m in unobstructed outdoor areas and up to 50m inside buildings.

Set up the base station and the charger cradle at a central location on a flat, non-slip surface in your house or apartment.

AC Power (Optional)

To connect the AC power:

1. Connect the DC plug on the power adapter to the DC5V port on the base stationand connect the other end of the power adapter into an electrical power outlet.
2. Connect the supplied Ethernet cable between the Internet port on the base station and the Internet port in your network or the switch/hub device port.



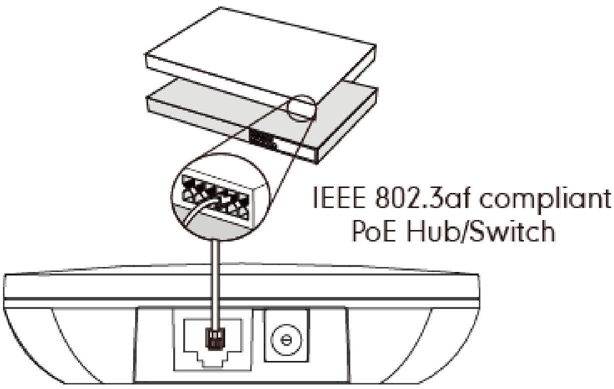
Note The base station should be used with original power adapter (5V/600mA) only. The use of the third-party power adapter may cause the damage to the phone.

Power over Ethernet

Using a regular Ethernet cable, the base station can be powered from a PoE-compliant (IEEE 802.3af) switch or hub.

To connect the PoE:

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



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

Important! Do not remove the power and network to the base station while it is updating firmware and configurations.

Setting up the Handset

To insert battery into the handset:

1. Open the battery cover.
2. Insert the battery and press it down.
3. Close the battery cover.

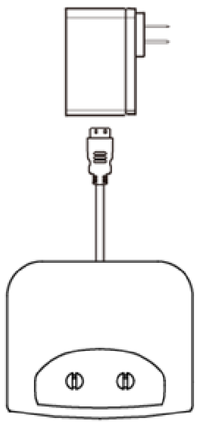
Note

> Do not short-circuit the battery, as short-circuiting the terminals may damage the battery or the handset.
>
> Do not use a damaged battery, as this may cause an explosion.
>
> Before replacing the battery, please turn off the handset to prevent memory loss.

Setting up the Charger Cradle

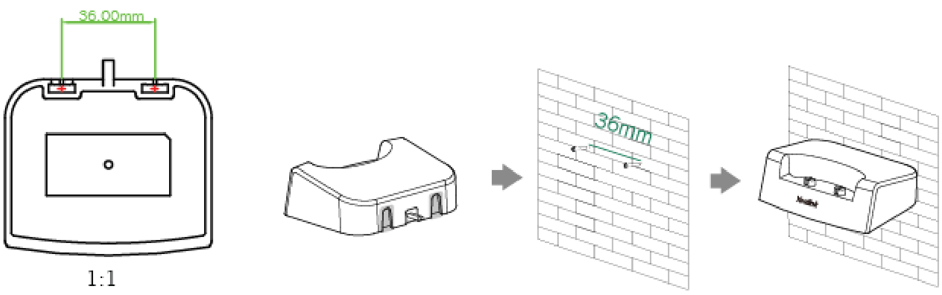
For W56H

1. Connect the USB plug on the charger cradle to the DC5V port on the power adapter.
2. Connect the power adapter into an electrical power outlet.



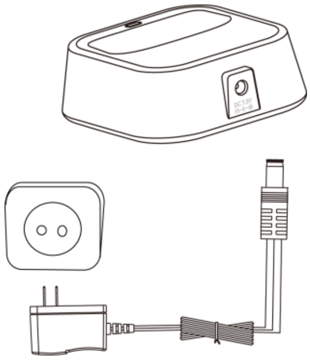
You can also mount the charger cradle on the wall, as shown below:

1. Drive the screws into the wall using the wall template as shown below.
2. Mount the charge cradle securely on the screws.



For W52H

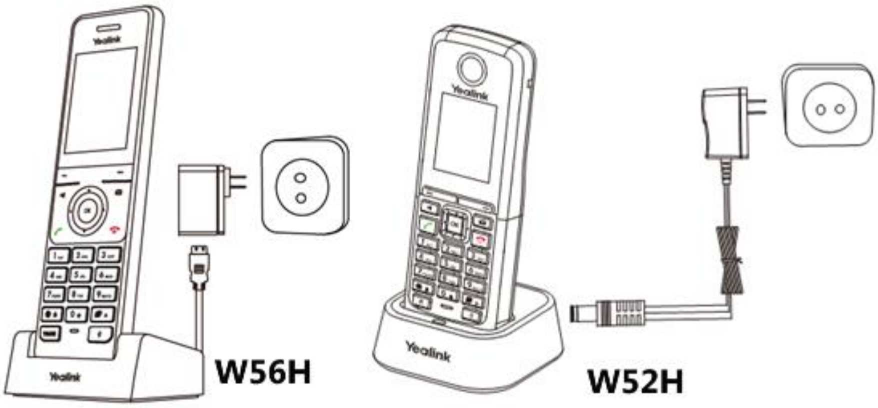
1. Connect the DC plug on the power adapter to the DC5V port on the charger cradle.
2. Connect the other end of the power adapter into an electrical power outlet.



Charging the Handset

To charge the handset:

1. After setting up the handset and charger cradle, place the handset in the charger cradle.



Note The handset should be used with Yealink original power adapter (5V/600mA) only. The use of third-party power adapter may cause the damage to the phone.

Registering the Handset

You can register up to 8 handsets to one base station. Each handset can be registered to 4 different base stations.

To register a new handset manually:

When the handset LCD screen prompts "Press base page 2s then press Reg.", long press  on the base station till the registration LED flashes.

Easy Registration:

1. Press the **Reg** soft key on the handset to register quickly.

Normal Registration:

1. Press the **OK** soft key on the handset, and then select **Register Handset**.
2. Select the desired base and then press the **OK** soft key. The handset begins searching the base.
3. Press the **OK** soft key after searching a base successfully.
4. Enter the base PIN (default: 0000), and then press the **Done** soft key to complete registration.

After the success of registration, the handset LCD screen prompts "Handset Subscribed" and "Base NO. (The last 4 characters of connected Base's MAC address)".

After initializing data successfully, an icon with internal handset number and handset name appears on the LCD screen.

To register to multiple base stations:

1. Press the **OK** key to enter the main menu.
2. Select **Settings**->**Registration**->**Register Handset**.
3. Repeat steps 2-4 mentioned in normal registration to register multiple base stations.

You can also enable the registration mode of the base station via web user interface at the path **Status**->**Handset&VoIP**->**Register New Handsets**.

Note

If the handset LCD screen prompts "Searching for Base", please check if your base station is powered on.

Initialization Process Overview

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

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

During the initialization process, the following events take place:

Loading the ROM file

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

Configuring the VLAN

If the DECT IP phone is connected to a switch, the switch notifies the DECT IP phone of the VLAN information defined on the switch (if using LLDP or CDP). The DECT IP phone can then proceed with the DHCP request for its network settings (if using DHCP). For more information on VLAN, refer to VLAN on page 32.

Querying the DHCP (Dynamic Host Configuration Protocol) Server

The DECT IP phone is capable of querying a DHCP server. DHCP is enabled on the DECT IP phone by default. The following network parameters can be obtained from the DHCP server during initialization:

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

You need to configure network parameters of the DECT IP phone manually if any of them is not supplied by the DHCP server. For more information on configuring network parameters manually, refer to Configuring Network Parameters Manually on page 24.

Contacting the provisioning server

If the DECT IP phone is configured to obtain configurations from the provisioning server, it will connect to the provisioning server, download the boot file(s) and configuration file(s) during startup. The DECT IP phone will be able to resolve and update configurations written in the configuration file(s). If the DECT IP phone does not obtain configurations from the provisioning server, the DECT IP phone will use configurations stored in the flash memory. For more information, refer to Setting Up Your Phones with a Provisioning Server on page 74.

Updating firmware

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

You can manually upgrade firmware if the DECT IP phone does not download firmware from the provisioning server. For more information, refer to Upgrading Firmware on page 94.

Downloading the resource files

In addition to configuration file(s), the DECT IP phone may require resource files before it can deliver service. These resource files are optional, but if some particular features are being deployed, these files are required.

The followings show examples of resource files:

- Language packs

- Ring tones
- Contact files

For more information on resource files, refer to Resource Files on page 87.

Verifying Startup

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

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

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

You can view the system status on your handset. Available information of the system status includes:

- **Base station status** (IPv4 status or IPv6 status, firmware version, MAC address and device certificate status, RFPI and network information)
  - IPv4 uses a 32-bit address.
  - IPv6 is an updated version of the current Internet Protocol to meet the increased demands for unique IP addresses, using a 128-bit address.
- **Handset status** (handset model, hardware version, firmware version, IPUI code, SN code and area)
- **Line status**

Note SN code is not availbale on W52H handset.

Setting Up Your System

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

This chapter provides the following sections:

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

Setting Up Your Phone Network

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

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

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

- DHCP
- DHCP Option
- Configuring Network Parameters Manually
- Web Server Type
- VLAN
- IPv6 Support
- VPN
- Network Address Translation (NAT)
- Quality of Service (QoS)
- 802.1X Authentication

DHCP

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to dynamically allocate network parameters to network hosts. The automatic allocation of network parameters to hosts eases the administrative burden of maintaining an IP network. DECT IP phones comply with the DHCP specifications documented in RFC 2131. If using DHCP, DECT IP phones connected to the network become operational without having to be manually assigned IP addresses and additional network parameters.

Procedure

DHCP can be configured using the following methods.

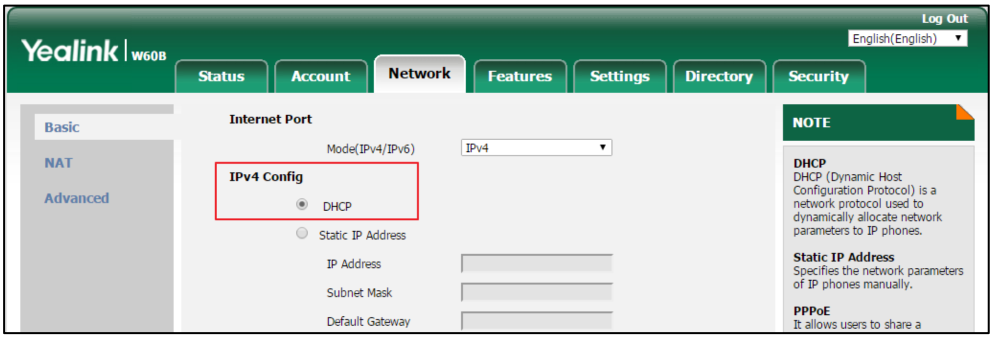
Central Provisioning (Configuration File)	<MAC>.cfg	Configure DHCP on the DECT IP phone. **Parameter:** static.network.internet_port.type
Web User Interface		Configure DHCP on the DECT IP phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=network&q=load
Handset User Interface		Configure DHCP on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

Details of Configuration Parameter:

Parameter	Permitted Values	Default
static.network.internet_port.type	**0 or 2**	**0**
Description: Configures the Internet port type for IPv4. **0**-DHCP **2**-Static IP Address **Note**: It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type		

To configure DHCP via web user interface:

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



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

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

To configure DHCP via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**System Settings**->**Network** (default PIN: 0000) ->**Basic**.
3. Press ▼ to select **IPv4**, and then press the **OK** soft key.
4. Press ◀ or ▶ to select **DHCP** from the **IP Address Type** field.
5. Press the **Save** soft key to accept the change.

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

Static DNS

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

Procedure

Static DNS can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the static DNS feature. **Parameter:** static.network.static_dns_enable
	<MAC>.cfg	Configure static DNS address. **Parameters:** static.network.primary_dns static.network.secondary_dns
Web User Interface		Configure the static DNS feature. Configure static DNS address.

	Navigate to: http://<phoneIPAddress>/servlet?p=network&q=load
Handset User Interface	Configure the static DNS feature. Configure static DNS address.

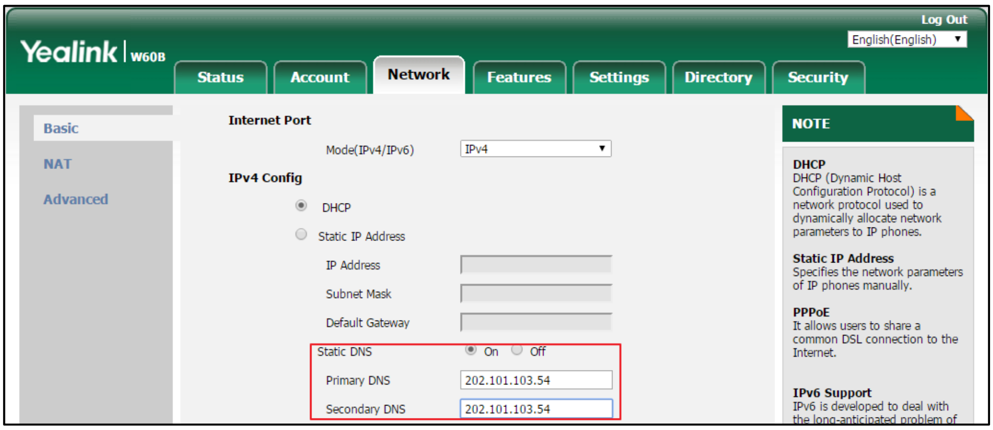
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.static_dns_enable	**0 or 1**	**0**
Description: Triggers the static DNS feature to on or off. **0**-Off **1**-On If it is set to 0 (Off), the DECT IP phone will use the IPv4 DNS obtained from DHCP. If it is set to 1 (On), the DECT IP phone will use manually configured static IPv4 DNS. **Note**: It works only if the value of the parameter "static.network.internet_port.type" is set to 0 (DHCP). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static DNS **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type: DHCP->DNS Type: Manual		
static.network.primary_dns	**IPv4 Address**	**Blank**
Description: Configures the primary IPv4 DNS server. **Example:** static.network.primary_dns = 202.101.103.55 **Note**: It works only if the value of the parameter "static.network.static_dns_enable" is set to 1 (On). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->Primary DNS **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic >IPv4->IP Address		

Parameters	Permitted Values	Default
Type: DHCP->DNS Type: Manual->Primary DNS		
static.network.secondary_dns	**IPv4 Address**	**Blank**
Description: Configures the secondary IPv4 DNS server. **Example:** static.network.secondary_dns = 202.101.103.54 **Note**: It works only if the value of the parameter "static.network.static_dns_enable" is set to 1 (On). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->Secondary DNS **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type: DHCP->DNS Type: Manual->Secondary DNS		

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

1. Click on **Network**->**Basic**.
2. In the **IPv4 Config** block, mark the **DHCP** radio box.
3. In the **Static DNS** block, mark the **On** radio box.
4. Enter the desired values in the **Primary DNS** and **Secondary DNS** fields.



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

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

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

1. Press **OK** to enter the main menu.

2. Select **Settings**->**System Settings**->**Network** (default PIN: 0000) ->**Basic**.
3. Press ▼ to select **IPv4**, and then press the **OK** soft key.
4. Press ◀ or ▶ to select **Manual** from the **DNS Type** field when **DHCP** is selected from the **IP Address Type** field.
5. Enter the valid value in the **Primary DNS** and **Secondary DNS** field respectively.
6. Press the **Save** soft key to accept the change.

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

DHCP Option

DHCP provides a framework for passing information to TCP/IP network devices. Network and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options.

DHCP can be initiated by simply connecting the DECT IP phone with the network. DECT IP phones broadcast DISCOVER messages to request the network information carried in DHCP options, and the DHCP server responds with specific values in corresponding options.

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

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

Parameter	DHCP Option	Description
TFTP Server Name	66	Identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.

For more information on DHCP options, refer to RFC 2131 or RFC 2132.

If you do not have the ability to configure the DHCP options for discovering the provisioning server on the DHCP server, an alternate method of automatically discovering the provisioning server address is required. Connecting to the secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server address is one possibility. For more information, refer to RFC 3925. If a single alternate DHCP server responds, this is functionally equivalent to the scenario where the primary DHCP server responds with a valid provisioning server address. If no DHCP servers respond, the INFORM query process will retry and eventually time out.

DHCP Option 66 and Option 43

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

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

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

Procedure

DHCP Ative can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure DHCP active. **Parameter:** static.auto_provision.dhcp_option.enable
		Configure the custom DHCP option. **Parameter:** static.auto_provision.dhcp_option.list_user_options
Web User Interface		Configure DHCP Active. Configure the custom DHCP option. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-autop&q=load

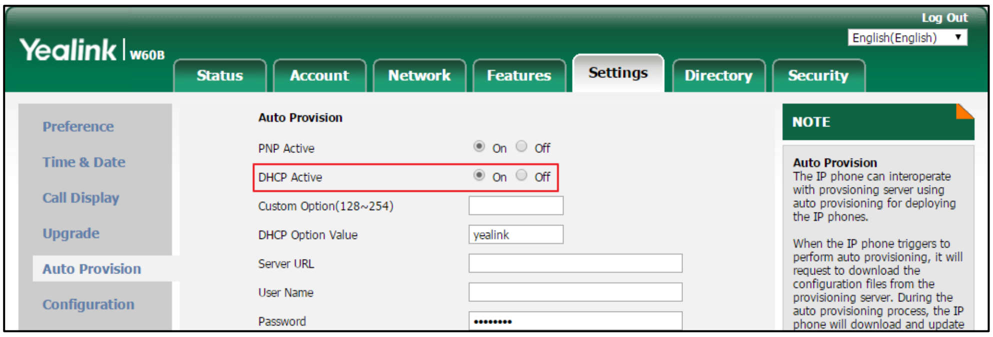
Details of Configuration Parameter:

<table>
<tr><th>Parameter</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>static.auto_provision.dhcp_option.enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Triggers the DHCP active feature to on or off.
0-Off
1-On, the IP phone will obtain the provisioning server address by detecting DHCP options.
If it is set to 1 (On), the DECT IP phone will obtain the provisioning server address by detecting DHCP options.
Web User Interface:
Settings->Auto Provision->DHCP Active
Handset User Interface:
None</td></tr>
<tr><td>static.auto_provision.dhcp_option.list_user_options</td><td>Integer from 128 to 254</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the custom DHCP option for requesting provisioning server address.
Multiple options are separated by commas.
Note: It works only if the value of the parameter “static.auto_provision.dhcp_option.enable” is set to 1 (On).
Web User Interface:
Settings->Auto Provision->Custom Option(128-254)
Phone User Interface:
None</td></tr>
</table>

To configure the DHCP active feature via web user interface:

1. Click on **Settings**->**Auto Provision**.

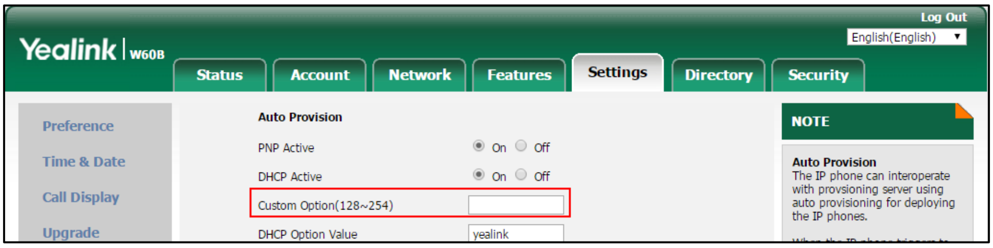
2. Mark the **On** radio box in the **DHCP Active** field.



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

To configure the custom DHCP option via web user interface:

1. Click on **Settings**->**Auto Provision**.
2. Enter the desired value in the **Custom Option(128~254)** field.



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

DHCP Option 42 and Option 2

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

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

To update time with the offset time offered by the DHCP server, make sure the DHCP Time feature is enabled at the web path **Settings**->**Time & Date**->**DHCP Time**. For more information on how to configure DHCP time feature, refer to NTP Time Server on page 165.

DHCP Option 12 Hostname on the DECT IP Phone

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

Procedure

DHCP option 12 hostname can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the DHCP option 12 hostname. **Parameter:**

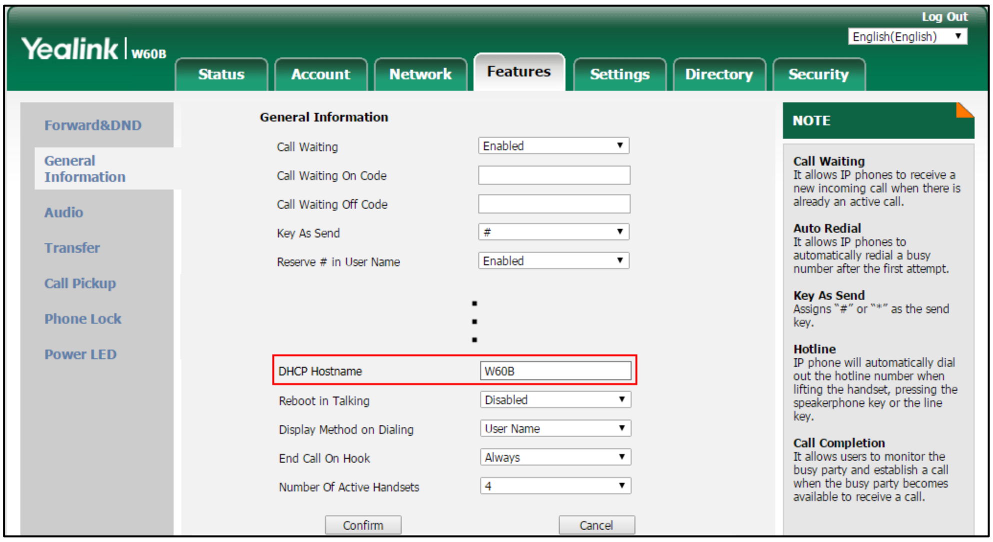
		static.network.dhcp_host_name
Web User Interface		Configure the DHCP option 12 hostname. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
static.network.dhcp_host_name	**String within 99 characters**	**W60B**
Description: Configures the DHCP option 12 hostname on the DECT IP phone. **Note**: If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Features->General Information->DHCP Hostname **Handset User Interface:** None		

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

1. Click on **Feature**->**General Information**.
2. Enter the desired host name in the **DHCP Hostname** field.



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

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

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

Configuring Network Parameters Manually

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

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

Procedure

Network parameters can be configured manually using the following methods.

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

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.internet_port.type	**0 or 2**	**0**

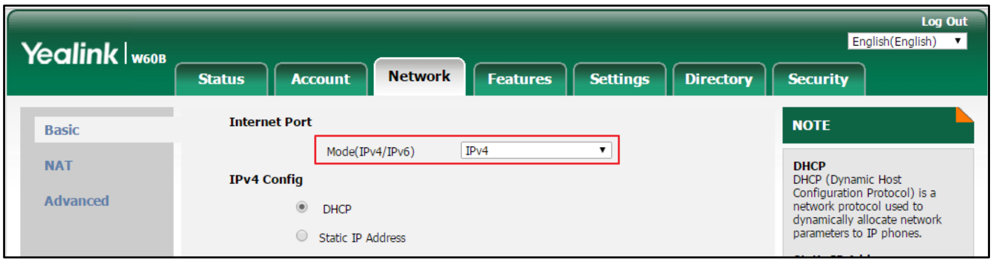
<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Configures the Internet port type for IPv4.
0-DHCP
2-Static IP Address
Note: It works only if the value of the parameter “static.network.ip_address_mode” is set to 0 (IPv4) or 2 (IPv4 & IPv6). If you change this parameter, the DECT IP phone will reboot to make the change take effect.
Web User Interface:
Network->Basic->IPv4 Config
Handset User Interface:
OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type</td></tr>
<tr><td>static.network.ip_address_mode</td><td>0, 1 or 2</td><td>0</td></tr>
<tr><td colspan="3">Description:
Configures the IP address mode.
0-IPv4
1-IPv6
2-IPv4 & IPv6
Note: If you change this parameter, the DECT IP phone will reboot to make the change take effect.
Web User Interface:
Network->Basic->Internet Port->Mode(IPv4/IPv6)
Handset User Interface:
OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IP Mode</td></tr>
<tr><td>static.network.internet_port.ip</td><td>IPv4 Address</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the IPv4 address.
Example:
static.network.internet_port.ip = 192.168.1.20
Note: It works only if the value of the parameter “static.network.ip_address_mode” is set to 0 (IPv4) or 2 (IPv4 & IPv6), and “static.network.internet_port.type” is set to 2 (Static IP Address). If you change this parameter, the DECT IP phone will reboot to make the change take effect.
Web User Interface:</td></tr>
</table>

Parameters	Permitted Values	Default
Network->Basic->IPv4 Config->Static IP Address->IP Address **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type: Static->IP Address		
static.network.internet_port.mask	**Subnet Mask**	**Blank**
Description: Configures the IPv4 subnet mask. **Example:** static.network.internet_port.mask = 255.255.255.0 **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP Address). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->Subnet Mask **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type: Static->Subnet Mask		
static.network.internet_port.gateway	**IPv4 Address**	**Blank**
Description: Configures the IPv4 default gateway. **Example:** static.network.internet_port.gateway = 192.168.1.254 **Note**: It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP Address). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->Default Gateway **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type: Static->Default Gateway		
static.network.primary_dns	**IPv4 Address**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the primary IPv4 DNS server. **Example:** static.network.primary_dns = 202.101.103.55 **Note**: It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP Address). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->Primary DNS **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type: Static->Primary DNS		
static.network.secondary_dns	**IPv4 Address**	**Blank**
Description: Configures the secondary IPv4 DNS server. **Example:** static.network.secondary_dns = 202.101.103.54 **Note**: It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP Address). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->Secondary DNS **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type: Static->Secondary DNS		

To configure the IP address mode via web user interface:

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



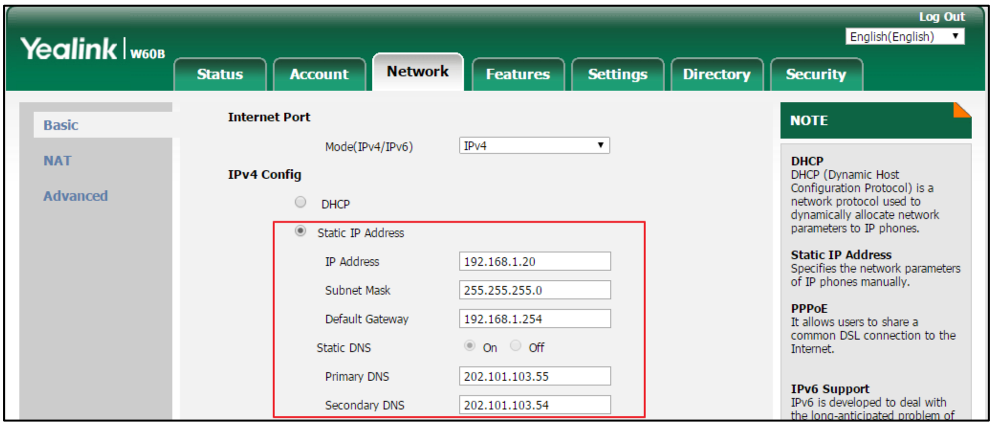
3. Click **Confirm** to accept the change.

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

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

To configure a static IPv4 address via web user interface:

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



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

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

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

To configure the IP address mode via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**System Settings**->**Network** (default PIN: 0000) ->**Basic**.
3. Press ◀ or ▶ to select **IPv4**, **IPv6** or **IPv4&IPv6** from the **IP Mode** field.
4. Press the **Save** soft key to accept the change.

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

To configure a static IPv4 address via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**System Settings**->**Network** (default PIN: 0000) ->**Basic**.

3. Press ▼ to select **IPv4**, and then press the **OK** soft key.
4. Press ◀ or ▶ to select **Static** from the **IP Address Type** field.
5. Enter the valid value in the **IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS** and **Secondary DNS** field respectively.
6. Press the **Save** soft key to accept the change.

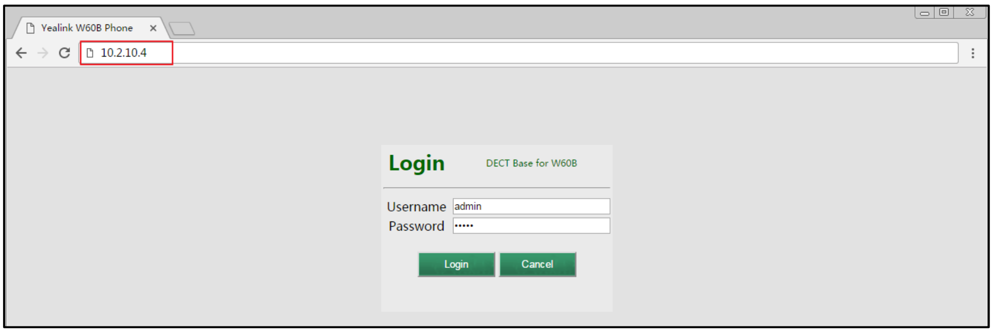
   The DECT IP phone reboots automatically to make settings effective after a period of time.

Web Server Type

Users can configure the user or administrator features of the phone via web user interface. Web server type determines access protocol of the DECT IP phone's web user interface. DECT IP phones support both HTTP and HTTPS protocols for accessing the web user interface. This can be disabled when it is not needed or when it poses a security threat. For more information on accessing the web user interface, refer to Web User Interface on page 83.

HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. HTTPS is a web protocol that encrypts and decrypts user page requests as well as pages returned by the web server. Both HTTP and HTTPS port numbers are configurable.

Access web user interface of the DECT IP phone using the HTTP/HTTPS protocol as the following shown (take HTTP protocol for example):



Procedure

Web server type can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the web access type, HTTP port and HTTPS port. **Parameters:** static.wui.http_enable static.network.port.http static.wui.https_enable static.network.port.https
Web User Interface		Configure the web access type, HTTP port and HTTPS port.

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

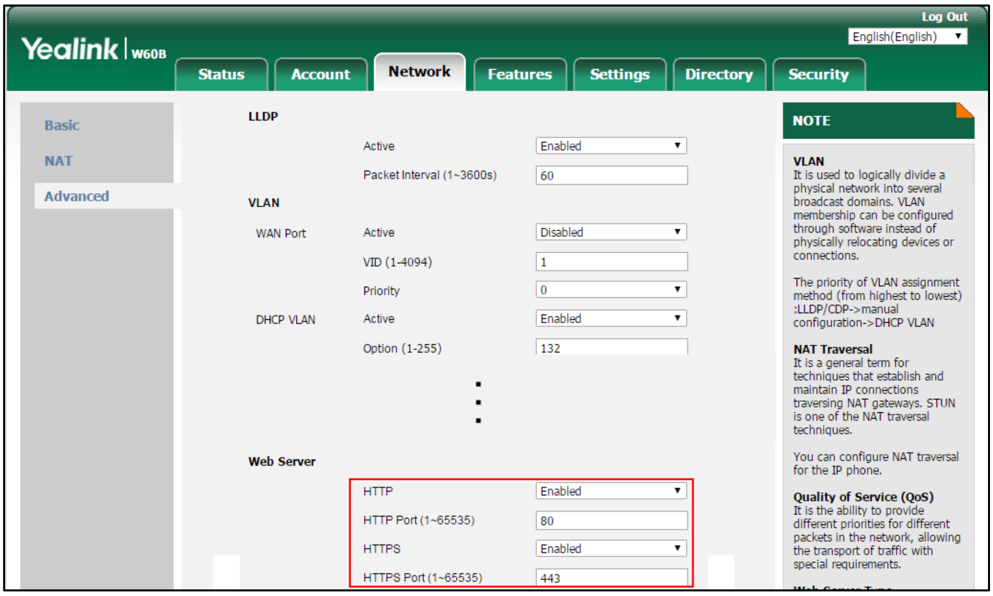
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.wui.http_enable	**0 or 1**	**1**
Description: Enables or disables the user to access web user interface of the DECT IP phone using the HTTP protocol. **0**-Disabled **1**-Enabled **Note**: If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Web Server->HTTP **Handset User Interface:** None		
static.network.port.http	**Integer from 1 to 65535**	**80**
Description: Configures the HTTP port for the user to access web user interface of the DECT IP phone using the HTTP protocol. **Note**: Please take care when choosing an alternate port. If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Web Server->HTTP Port(1~65535) **Handset User Interface:** None		
static.wui.https_enable	**0 or 1**	**1**
Description: Enables or disables the user to access web user interface of the DECT IP phone using the HTTPS protocol. **0**-Disabled **1**-Enabled		

Parameters	Permitted Values	Default
Note: If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Web Server->HTTPS **Handset User Interface:** None		
static.network.port.https	**Integer from 1 to 65535**	**443**
Description: Configures the HTTPS port for the user to access web user interface of the DECT IP phone using the HTTPS protocol. **Note**: Please take care when choosing an alternate port. If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Web Server->HTTPS Port(1~65535) **Handset User Interface:** None		

To configure web server type via web user interface:

1. Click on **Network**->**Advanced**.
2. Select the desired value from the pull-down list of **HTTP**.
3. Enter the desired HTTP port number in the **HTTP Port(1~65535)** field.
4. Select the desired value from the pull-down list of **HTTPS**.
5. Enter the desired HTTPS port number in the **HTTPS Port(1~65535)** field.



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

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

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

VLAN

VLAN (Virtual Local Area Network) is used to logically divide a physical network into several broadcast domains. VLAN membership can be configured through software instead of physically relocating devices or connections. Grouping devices with a common set of requirements regardless of their physical location can greatly simplify network design. VLANs can address issues such as scalability, security and network management.

The purpose of VLAN configurations on the DECT IP phone is to insert tag with VLAN information to the packets generated by the DECT IP phone. When VLAN is properly configured for Internet port on the DECT IP phone, the DECT IP phone will tag all packets from these ports with the VLAN ID. The switch receives and forwards the tagged packets to the corresponding VLAN according to the VLAN ID in the tag as described in IEEE Std 802.3.

In addition to manual configuration, the DECT IP phone also supports automatic discovery of VLAN via LLDP, CDP or DHCP. The assignment takes effect in this order: assignment via LLDP/CDP, manual configuration, then assignment via DHCP.

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

Procedure

VLAN assignment method can be configured using the configuration files.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the VLAN assignment method. **Parameter:**

		static.network.vlan.vlan_change.enable

Details of Configuration Parameter:

Parameter	Permitted Values	Default
static.network.vlan.vlan_change.enable	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to obtain VLAN ID using lower priority of VLAN assignment method or disable VLAN feature when the DECT IP phone cannot obtain VLAN ID using the current VLAN assignment method. **0**-Disabled **1**-Enabled The priority of each method is: LLDP/CDP>Manual>DHCP VLAN. If it is set to 1 (Enabled), the DECT IP phone will attempt to use the lower priority of VLAN assignment method when failing to obtain the VLAN ID using higher priority of VLAN assignment method. If all the methods are attempted, the phone will disable VLAN feature. **Note:** If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** None **Handset User Interface:** None		

LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows DECT IP phones to receive and/or transmit device-related information from/to directly connected devices on the network that are also using the protocol, and store the information about other devices.

When LLDP feature is enabled on DECT IP phones, the DECT IP phones periodically advertise their own information to the directly connected LLDP-enabled switch. The DECT IP phones can also receive LLDP packets from the connected switch. When the application type is "voice", DECT IP phones decide whether to update the VLAN configurations obtained from the LLDP packets. When the VLAN configurations on the DECT IP phones are different from the ones sent by the switch, the DECT IP phones perform an update and reboot. This allows the DECT IP phones to be plugged into any switch, obtain their VLAN IDs, and then start communications with the call control.

Procedure

LLDP can be configured using the following methods.

Central Provisioning **(Configuration File)**	y000000000077.cfg	Configure LLDP feature. **Parameters:** static.network.lldp.enable static.network.lldp.packet_interval
Web User Interface		Configure LLDP feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load
Handset User Interface		Configure LLDP feature.

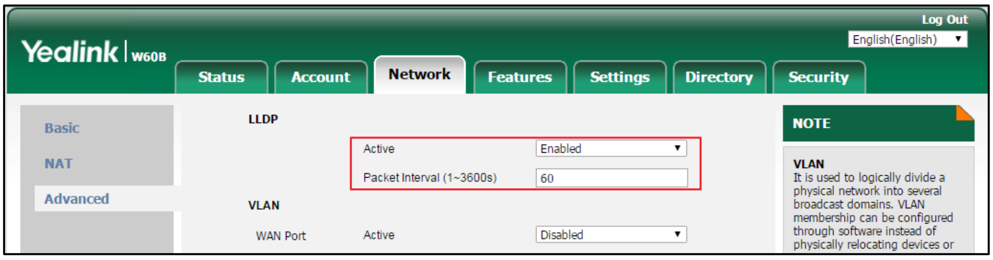
Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>static.network.lldp.enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables the LLDP (Linker Layer Discovery Protocol) feature on the DECT IP phone.
0-Disabled
1-Enabled
If it is set to 1 (Enabled), the DECT IP phone will attempt to determine its VLAN ID through LLDP.
Note: If you change this parameter, the DECT IP phone will reboot to make the change take effect.
Web User Interface:
Network->Advanced->LLDP->Active
Handset User Interface:
None</td></tr>
<tr><td>static.network.lldp.packet_interval</td><td>Integer from 1 to 3600</td><td>60</td></tr>
<tr><td colspan="3">Description:
Configures the interval (in seconds) for the DECT IP phone to send the LLDP (Linker Layer Discovery Protocol) request.
Note: It works only if the value of the parameter “static.network.lldp.enable” is set to 1 (Enabled). If you change this parameter, the DECT IP phone will reboot to make the change take effect.
Web User Interface:
Network->Advanced->LLDP->Packet Interval (1~3600s)
Handset User Interface:
None</td></tr>
</table>

To configure LLDP feature via web user interface:

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

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



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

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

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

Manual Configuration for VLAN in the Network

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

Procedure

VLAN can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure VLAN for the Internet port manually. **Parameters:** static.network.vlan.internet_port_enable static.network.vlan.internet_port_vid static.network.vlan.internet_port_priority
Web User Interface		Configure VLAN for the Internet port manually. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load
Handset User Interface		Configure VLAN for the Internet port manually.

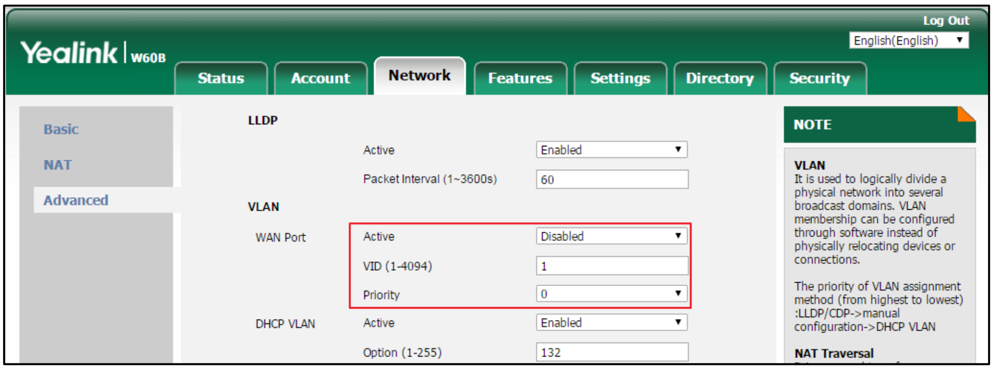
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.vlan.internet_port_enable	**0 or 1**	**0**

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Enables or disables VLAN for the Internet port.
0-Disabled
1-Enabled
Note: If you change this parameter, the DECT IP phone will reboot to make the change take effect.
Web User Interface:
Network->Advanced->VLAN->WAN Port->Active
Handset User Interface:
OK->Settings->System Settings->Network (default PIN: 0000) ->VLAN->VLAN Parameter->Status</td></tr>
<tr><td>static.network.vlan.internet_port_vid</td><td>Integer from 1 to 4094</td><td>1</td></tr>
<tr><td colspan="3">Description:
Configures VLAN ID for the Internet port.
Note: If you change this parameter, the DECT IP phone will reboot to make the change take effect.
Web User Interface:
Network->Advanced->VLAN->WAN Port->VID (1-4094)
Handset User Interface:
OK->Settings->System Settings->Network (default PIN: 0000) ->VLAN->VLAN Parameter->Status: Enabled->VID</td></tr>
<tr><td>static.network.vlan.internet_port_priority</td><td>Integer from 0 to 7</td><td>0</td></tr>
<tr><td colspan="3">Description:
Configures VLAN priority for the Internet port.
7 is the highest priority, 0 is the lowest priority.
Note: If you change this parameter, the DECT IP phone will reboot to make the change take effect.
Web User Interface:
Network->Advanced->VLAN->WAN Port->Priority
Handset User Interface:
OK->Settings->System Settings->Network (default PIN: 0000) ->VLAN->VLAN Parameter->Status: Enabled->Priority</td></tr>
</table>

To configure VLAN for Internet port via web user interface:

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



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

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

To configure VLAN for Internet port via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**System Settings**->**Network** (default PIN: 0000) ->**VLAN**->**VLAN** Parameter.
3. Press ◀ or ▶ to select **Enabled** from the **Status** field.
4. Enter the valid value in the **VID** and **Priority** field respectively.
5. Press the **Save** soft key to accept the change.

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

DHCP VLAN

DECT IP phones support VLAN discovery via DHCP. When the VLAN Discovery method is set to DHCP, the DECT IP phone will examine DHCP option for a valid VLAN ID. The predefined option 132 is used to supply the VLAN ID by default. You can customize the DHCP option used to request the VLAN ID.

Procedure

DHCP VLAN can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure DHCP VLAN discovery feature. **Parameters:** static.network.vlan.dhcp_enable

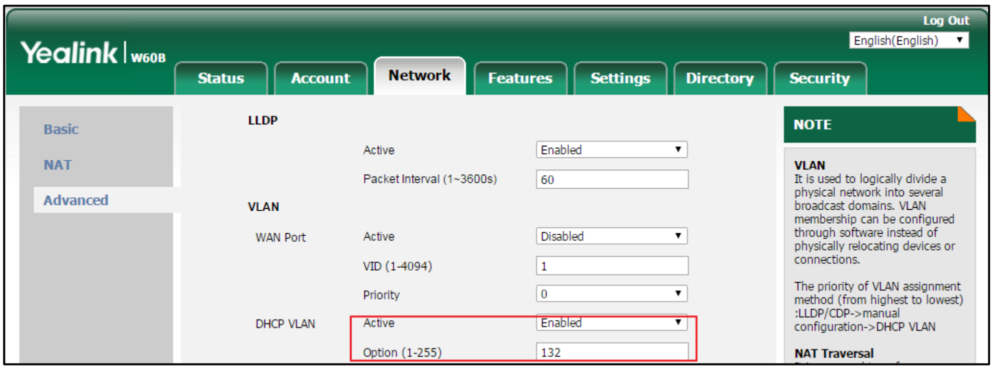
		static.network.vlan.dhcp_option
Web User Interface		Configure DHCP VLAN discovery feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load
Handset User Interface		Configure DHCP VLAN discovery feature.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.vlan.dhcp_enable	**0 or 1**	**1**
Description: Enables or disables DHCP VLAN discovery feature on the DECT IP phone. **0**-Disabled **1**-Enabled **Note:** If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN->DHCP VLAN->Active **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->VLAN->VLAN DHCP->Status		
static.network.vlan.dhcp_option	**Integer from 1 to 255**	**132**
Description: Configures the DHCP option from which the DECT IP phone will obtain the VLAN settings. You can configure at most five DHCP options and separate them by commas. **Note:** If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN->DHCP VLAN->Option (1-255) **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->VLAN->VLAN DHCP->Status: Enabled->Options		

To configure DHCP VLAN discovery via web user interface:

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



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

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

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

To configure DHCP VLAN discovery via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**System Settings**->**Network** (default PIN: 0000) ->**VLAN**->**VLAN DHCP**.
3. Press ◀ or ▶ to select **Enabled** from the **Status** field.
4. Enter the valid value in the **Options** field.
5. Press the **Save** soft key to accept the change.

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

IPv6 Support

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

IPv6 is developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. Yealink DECT IP phone supports IPv4 addressing mode, IPv6 addressing mode, as well as an IPv4&IPv6 dual stack addressing mode. IPv4 uses a 32-bit address, consisting of four groups of three decimal digits separated by dots; for example, 192.168.1.100. IPv6 uses a 128-bit address, consisting of eight groups of four hexadecimal digits separated by colons; for example, 2026:1234:1:1:215:65ff:fe1f:caa.

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

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

IPv6 Address Assignment Method

Supported IPv6 address assignment methods:

- **Manual Assignment:** An IPv6 address and other configuration parameters (e.g., DNS server) for the DECT IP phone can be statically configured by an administrator.
- **Stateless Address Autoconfiguration (SLAAC)/ICMPv6:** SLAAC is one of the most convenient methods to assign IP addresses to IPv6 nodes. SLAAC requires no manual configuration of the DECT IP phone, minimal (if any) configuration of routers, and no additional servers. To use IPv6 SLAAC, the DECT IP phone must be connected to a network with at least one IPv6 router connected. This router is configured by the network administrator and sends out Router Advertisement announcements onto the link. These announcements can allow the on-link connected DECT IP phone to configure itself with IPv6 address, as specified in RFC 4862.

How the DECT IP phone obtains the IPv6 address and network settings?

The following table lists where the DECT IP phone obtains the IPv6 address and other network settings:

SLAAC (ICMPv6)	How the DECT IP phone obtains the IPv6 address and network settings?
Disabled	You have to manually configure the static IPv6 address and other network settings.
Enabled	The DECT IP phone can obtain the IPv6 address via SLAAC, but the other network settings must be configured manually.

Procedure

IPv6 can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the IPv6 address assignment method. **Parameters**: static.network.ip_address_mode static.network.ipv6_internet_port.type static.network.ipv6_internet_port.ip static.network.ipv6_prefix static.network.ipv6_internet_port.gateway

		Configure the IPv6 static DNS address. **Parameters**: static.network.ipv6_primary_dns static.network.ipv6_secondary_dns
	<MAC>.cfg	Configure the IPv6 static DNS. **Parameter:** static.network.ipv6_static_dns_enable
Web User Interface		Configure the IPv6 address assignment method. Configure the IPv6 static DNS address. Configure the IPv6 static DNS. **Navigate to**: http://<phoneIPAddress>/servlet?p=network&q=load
Handset User Interface		Configure the IPv6 address assignment method. Configure the IPv6 static DNS address. Configure the IPv6 static DNS.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.ip_address_mode	**0, 1 or 2**	**0**
Description: Configures the IP address mode. **0**-IPv4 **1**-IPv6 **2**-IPv4 & IPv6 **Note:** If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->Internet Port->Mode (IPv4/IPv6) **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IP Mode		
static.network.ipv6_internet_port.type	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Configures the Internet port type for IPv6. **0**-DHCP **1**-Static IP Address **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type		
static.network.ipv6_static_dns_enable	**0 or 1**	**0**
Description: Triggers the static IPv6 DNS feature to on or off. **0-**Off **1-**On If it is set to 0 (Off), the DECT IP phone will use the IPv6 DNS obtained from DHCP. If it is set to 1 (On), the DECT IP phone will use manually configured static IPv6 DNS. **Note:** It works only if the value of the parameter "static.network.ipv6_internet_port.type" is set to 0 (DHCP). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->IPv6 Static DNS **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type: DHCP->DNS Type: Manual		
static.network.ipv6_internet_port.ip	**IPv6 address**	**Blank**
Description: Configures the IPv6 address. **Example:** static.network.ipv6_internet_port.ip = 2026:1234:1:1:215:65ff:fe1f:caa		

Parameters	Permitted Values	Default
Note: It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP Address). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->Static IP Address->IP Address **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type: Static->IP Address		
static.network.ipv6_prefix	**Integer from 0 to 128**	**64**
Description: Configures the IPv6 prefix. **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP Address). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->Static IP Address->IPv6 Prefix(0~128) **Handset User Interface:** OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type: Static->IPv6 Prefix		
static.network.ipv6_internet_port.gateway	**IPv6 address**	**Blank**
Description: Configures the IPv6 default gateway. **Example:** static.network.ipv6_internet_port.gateway = 3036:1:1:c3c7:c11c:5447:23a6:255 **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP Address). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->Static IP Address->Default Gateway **Handset User Interface:**		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type: Static->Default Gateway</td></tr>
<tr><td>static.network.ipv6_primary_dns</td><td>IPv6 address</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the primary IPv6 DNS server.
Example:
static.network.ipv6_primary_dns = 3036:1:1:c3c7: c11c:5447:23a6:256
Note: It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure the value of the parameter "static.network.ipv6_static_dns_enable" is set to 1 (On). If you change this parameter, the DECT IP phone will reboot to make the change take effect.
Web User Interface:
Network->Basic->IPv6 Config->Static IP Address->Primary DNS
Handset User Interface:
OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type: Static->Primary DNS</td></tr>
<tr><td>static.network.ipv6_secondary_dns</td><td>IPv6 address</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the secondary IPv6 DNS server.
Example:
static.network.ipv6_secondary_dns = 2026:1234:1:1:c3c7:c11c:5447:23a6
Note: It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure the value of the parameter "static.network.ipv6_static_dns_enable" is set to 1 (On). If you change this parameter, the DECT IP phone will reboot to make the change take effect.
Web User Interface:
Network->Basic->IPv6 Config->Static IP Address->Secondary DNS
Handset User Interface:
OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type: Static->Secondary DNS</td></tr>
</table>

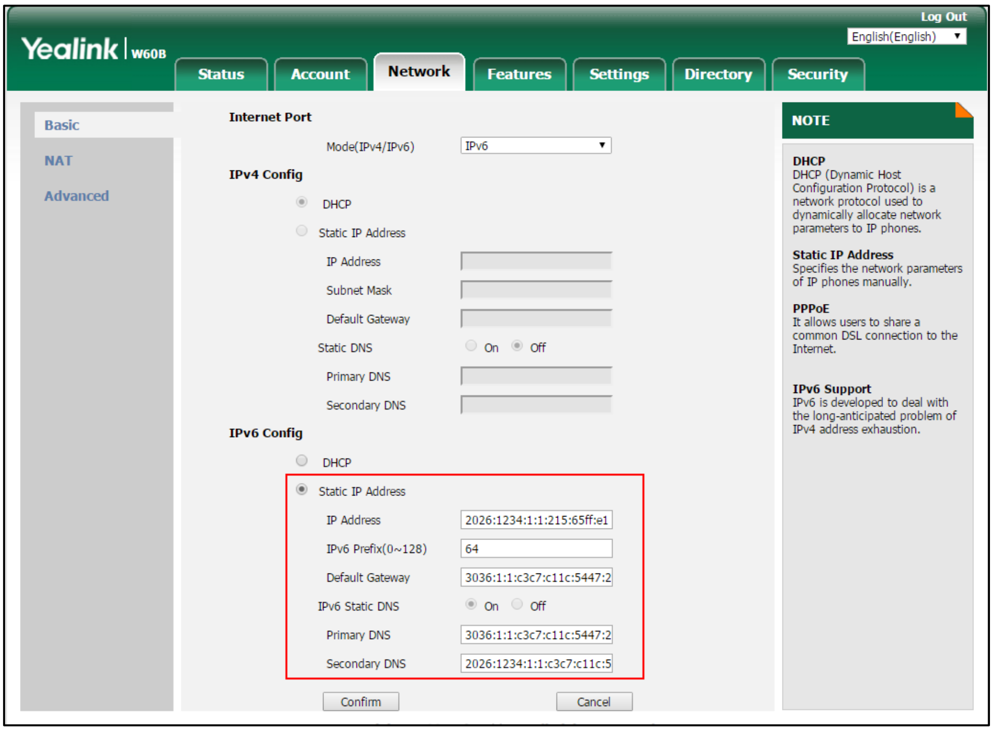
To configure IPv6 address assignment method via web user interface:

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

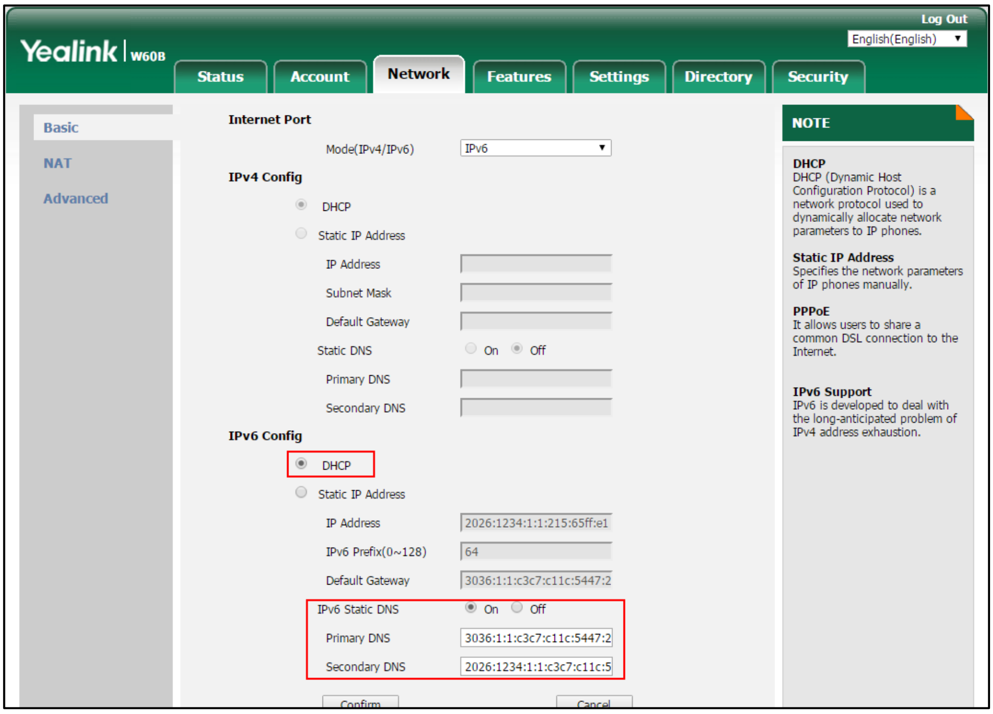
Mode(IPv4/IPv6).

3. In the **IPv6 Config** block, mark the **DHCP** or the **Static IP Address** radio box.

   - If you mark the **Static IP Address** radio box, configure the IPv6 address and other configuration parameters in the corresponding fields.



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



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

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

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

To configure IPv6 address assignment method via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**System Settings**->**Network**.
3. Enter the system PIN (default: 0000), press the **Done** soft key.
4. Press ◀ or ▶ to select **IPv6** or **IPv4&IPv6** from the **IP Mode** field.
5. Press ▼ to select **IPv6**, and then press the **OK** soft key.
6. Press ◀ or ▶ to select **Static** from the **IP Address Type** field.
7. Enter the valid value in the **IP Address**, **IPv6 Prefix**, **Default Gateway**, **Primary DNS** and **Secondary DNS** field respectively.
8. Press the **Save** soft key to accept the change.

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

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

1. Press **OK** to enter the main menu.
2. Select **Settings**->**System Settings**->**Network**.
3. Enter the system PIN (default: 0000), press the **Done** soft key.
4. Press ▼ to select **IPv6**, and then press the **OK** soft key.
5. Press ◀ or ▶ to select **Manual** from the **DNS Type** field.
6. Enter the valid value in the **Primary DNS** and **Secondary DNS** field respectively.
7. Press the **Save** soft key to accept the change.

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

VPN

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

VPN Technology

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

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

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

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

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

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

Procedure

VPN can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure VPN feature and upload a TAR file to the DECT IP phone. **Parameters:** static.network.vpn_enable static.openvpn.url
Web User Interface		Configure VPN feature and upload a TAR file to the DECT IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load
Handset User Interface		Configure VPN feature.

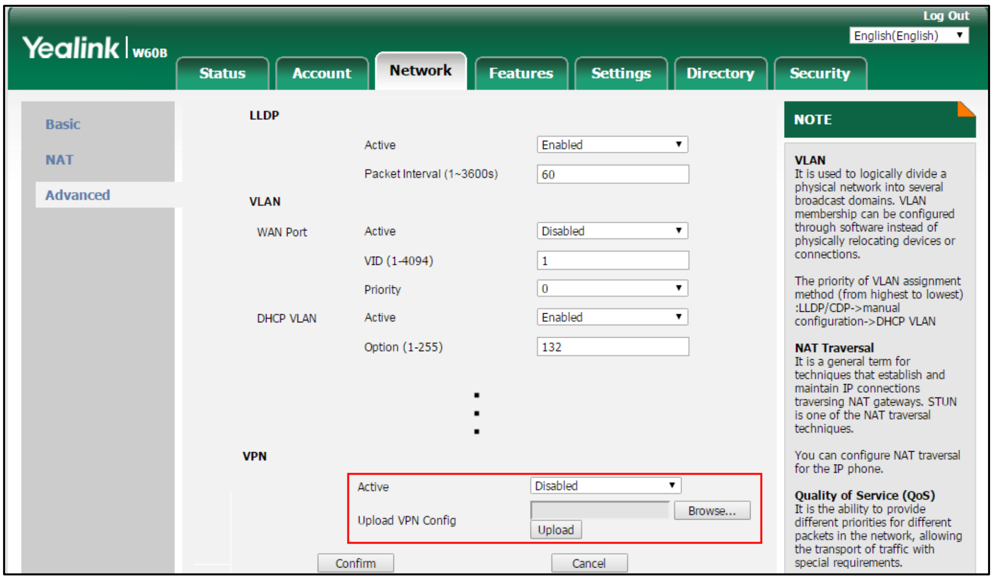
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.vpn_enable	**0 or 1**	**0**
Description: Enables or disables OpenVPN feature on the DECT IP phone.		

Parameters	Permitted Values	Default
0-Disabled **1**-Enabled **Note:** If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VPN->Active **Handset User Interface:** None		
static.openvpn.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the *.tar file for OpenVPN. **Example:** static.openvpn.url = http://192.168.10.25/OpenVPN.tar **Web User Interface:** Network->Advanced->VPN->Upload VPN Config **Handset User Interface:** None		

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

1. Click on **Network**->**Advanced**.
2. Click **Browse** to locate the TAR file from the local system.
3. Click **Upload** to upload the TAR file.



The web user interface prompts the message "Import config…".

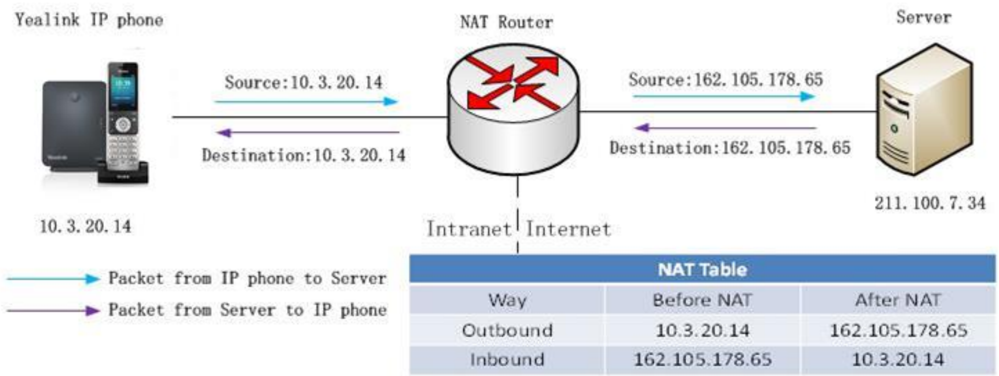
4. In the **VPN** block, select the desired value from the pull-down list of **Active**.
5. Click **Confirm** to accept the change.

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

Network Address Translation (NAT)

Network Address Translation (NAT) is one of the technologies for solving the network problem – the shortage of IP addresses. Many countries provide only one public IP address for the whole company. They configure NAT to advertise the IP address for the entire network to the outside world. This can reduce the need for a large number of public IP addresses.

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



NAT Types

Symmetrical NAT

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

Full Cone NAT

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

Address Restricted Cone NAT

Restricted cone NAT works in a similar way like full cone NAT. Apublic host (hAddr:any) can send packets to iAddr: port1through eAddr: port2 only if iAddr: port1 has previously sent a packet to hAddr: any. "Any" means the port number which doesn't matter.

Port Restricted Cone NAT

Port restricted cone NAT works in a similar way like full cone NAT. A public host (hAddr:hPort) can send packets to iAddr: port1through eAddr: port2 only if iAddr: port1 has previously sent a packet to hAddr: hPort.

NAT Traversal

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

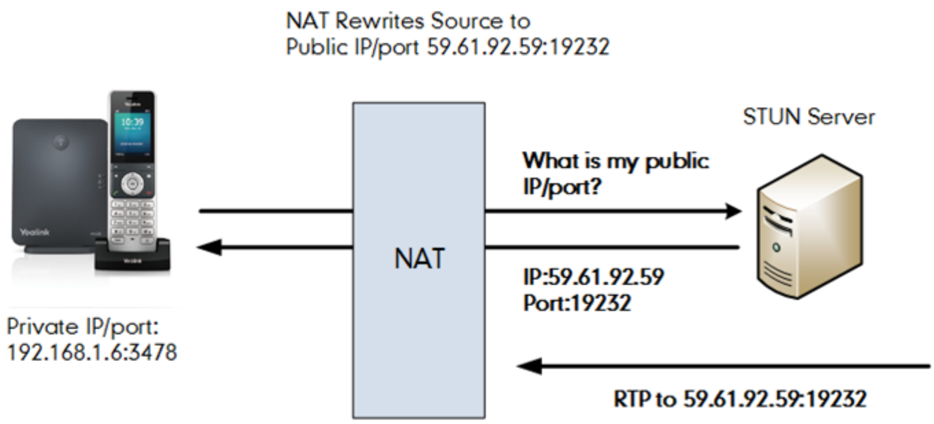
AT traversal is a general term for techniques that establish and maintain IP connections traversing NAT gateways, typically required for client-to-client networking applications, especially for VoIP deployments. Yealink IP phones support three NAT traversal techniques: manual NAT, STUN and ICE. If manual NAT and STUN are all enabled, the IP phone will use the manually configured external IP address for NAT traversal. The TURN protocol is used as part of the ICE approach to NAT traversal.

Manual NAT (Static NAT)

Manual NAT helps IP connections traverse NAT gateways without the third-party network server (STUN/TURN server). If manual NAT feature is enabled, the configured public IP address and port can be carried in the SIP requests or RTP packets, in which the other party obtains the phone’s public address. It is useful to reduce the cost of the company’s network deployment.

STUN (Simple Traversal of UDP over NATs)

STUN is a network protocol, used in NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications. The STUN protocol allows entities behind a NAT to first discover the presence of a NAT and the type of NAT (for more information on the NAT types, refer to NAT Types on page 50) and to obtain the mapped (public) IP address and port number that the NAT has allocated for the UDP connections to remote parties. The protocol requires assistance from a third-party network server (STUN server) usually located on public Internet. The IP phone can be configured to act as a STUN client, to send exploratory STUN messages to the STUN server. The STUN server uses those messages to determine the public IP address and port used, and then informs the client.



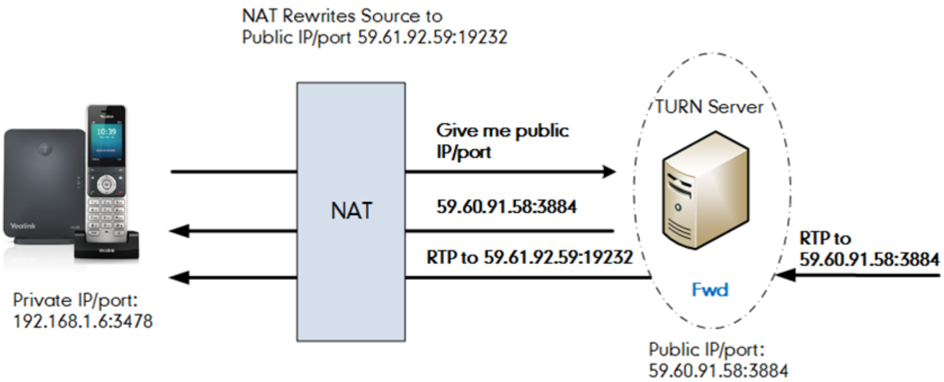
Capture packets after you enable the STUN feature, you can find that the IP phone sends Binding Request to the STUN server, and then mapped IP address and port is placed in the Binding Response: Binding Success Response MAPPED-ADDRESS: 59.61.92.59:19232.

No.	Time	Source	Destination	Protocol	Length	Info
444	18.587848	192.168.1.6	218.107.220.74	STUN	62	Binding Request
447	18.711349	218.107.220.74	192.168.1.6	STUN	98	Binding Success Response MAPPED-ADDRESS: 59.61.92.59:19232

STUN will not work if the NAT device is symmetric. This may be a drawback in many situations as most enterprise-class firewalls are symmetric.

TURN (Traversal Using Relays around NAT)

TURN is a network protocol described in RFC 5766, whicth allows a host located behind a NAT (called the TURN client) to communicate and exchange packets with other hosts (peers, called the TURN server) using a relay. In these situations, the host uses the services of an intermediate node to act as a communication relay. It governs the reception of data over a Transmission Control Protocol (TCP) or a UDP connection. This solves the problems of clients behind symmetric NATs which cannot rely on STUN to solve the NAT traversal issue. This method is appropriate in some situations, but it scales poorly since the media must go through the TURN server.



If you configure both STUN and TURN on the phone, it discovers what type of NAT device is between the phone and the public network. If the NAT device is full cone, address restricted cone, or port restricted cone, the phone will use STUN. If the NAT device is symmetric, the phone will use TURN. TURN is compatible with all types of NAT devices but can be costly since all traffic goes through a media relay (which can be slow, can exchange more messages, and requires the TURN server to allocate bandwidth for calls).

Although TURN will almost always provide connectivity to a client, it comes at high cost to the provider of the TURN server. Therefore other mechanisms (such as STUN or direct connectivity) will be preferred when possible.

ICE (Interactive Communications Establishment)

ICE, described in RFC 5245, is a technique for Network Address Translator (NAT) traversal for UDP-based media streams established by the offer/answer model, not intended for NAT traversal for SIP. It is an extension to the offer/answer model, and works by including a multiplicity of IP addresses and ports in SDP offers and answers, which are then tested for connectivity by peer-to-peer connectivity checks.

ICE makes use of the STUN protocol and its extension, TURN. In an ICE environment, two IP phones communicating at different locations are able to communicate via the SIP protocol by exchanging Session Description Protocol (SDP) messages. At the beginning of the ICE process, the phones are ignorant of their own topologies. In particular, they might or might not be behind a NAT. ICE allows IP phones to discover enough information about their topologies to find the optimal path(s) by which they can communicate.

ICE optimizes the media path. For an example, when two IP phones in the same network are calling each other via a long media path through other external networks, with ICE enabled, the short media path in the same network would be chosen, which will probably have better quality than the long one.

ICE is a complex solution to the problem of NAT traversal. Due to its complexity there is very limited client support for ICE today.

SIP Ports for NAT Traversal

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

- Local SIP Port
- TLS SIP Port

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

Procedure

NAT traversal can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure STUN feature and STUN server on a phone basis. **Parameters:** sip.nat_stun.enable sip.nat_stun.server sip.nat_stun.port
		Configure manual NAT feature on a phone basis. **Parameters:** network.static_nat.enable network.static_nat.addr
		Configure ICE feature. **Parameter:** ice.enable
		Configure TURN feature and TURN server. **Parameters:** sip.nat_turn.enable

		sip.nat_turn.server sip.nat_turn.port sip.nat_turn.username sip.nat_turn.password
		Configure local SIP port and TLS SIP port. **Parameters:** sip.listen_port sip.tls_listen_port
	<MAC>.cfg	Configure NAT traversal on a per-line basis. **Parameter:** account.X.nat.nat_traversal
Web User Interface		Configure manual NAT feature on a phone basis. Configure ICE feature. Configure TURN feature and TURN server. Configure STUN feature and STUN server on a phone basis. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-nat&q=load
		Configure local SIP port and TLS SIP port. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-sip&q=load
		Configure NAT traversal on a per-line basis. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0
Phone User Interface		Configure STUN feature and STUN server on a phone basis. Configure NAT traversal on a per-line basis.

Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>sip.nat_stun.enable</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables the STUN (Simple Traversal of UDP over NATs) feature on the IP phone.
0-Disabled
1-Enabled
Note: If you change this parameter, the IP phone will reboot to make the change take effect.
Web User Interface:
Network->NAT->STUN->Active
Phone User Interface:
None</td></tr>
<tr><td>sip.nat_stun.server</td><td>IP address or domain name</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the IP address or the domain name of the STUN (Simple Traversal of UDP over NATs) server.
Example:
sip.nat_stun.server = 218.107.220.201
Note: It works only if the value of the parameter "sip.nat_stun.enable" is set to 1 (Enabled). If you change this parameter, the IP phone will reboot to make the change take effect.
Web User Interface:
Network->NAT->STUN->STUN Server
Phone User Interface:
None</td></tr>
<tr><td>sip.nat_stun.port</td><td>Integer from 1024 to 65000</td><td>3478</td></tr>
</table>

Parameters	Permitted Values	Default
Description: Configures the port of the STUN (Simple Traversal of UDP over NATs) server. **Example:** sip.nat_stun.port = 3478 **Note:** It works only if the value of the parameter "sip.nat_stun.enable" is set to 1 (Enabled). If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->NAT->STUN->STUN Port (1024~65000) **Phone User Interface:** None		
account.X.nat.nat_traversal (X ranges from 1 to 8)	**0, 1 or 2**	**0**
Description: Enables or disables the NAT traversal for account X. **0**-Disabled **1**-STUN **2**-Manual NAT **Note**: If it is set to 1 (STUN), it works only if the value of the parameter "sip.nat_stun.enable" is set to 1 (Enabled); if it is set to 2 (Manual NAT), it works only if the value of the parameter "network.static_nat.enable" is set to 1 (Enabled). **Web User Interface:** Account->Register->NAT **Phone User Interface:** None		
network.static_nat.enable	**0 or 1**	**0**
Description: Enables or disables the manual NAT feature on the IP phone. **0**-Disabled **1**-Enabled **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->NAT->Nat Manual->Active		

Parameters	Permitted Values	Default
Phone User Interface: None		
network.static_nat.addr	**IP address**	**Blank**
Description: Configures the IP address to be advertised in SIP signaling. It should match the external IP address used by the NAT device. **Example**: network.static_nat.addr = 10.3.5.33 **Note**: It works only if the value of the parameter "network.static_nat.enable" is set to 1 (Enabled). If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->NAT->Nat Manual->IP Address **Phone User Interface:** None		
ice.enable	**0 or 1**	**0**
Description: Enables or disables the ICE (Interactive Connectivity Establishment) feature on the IP phone. **0**-Disabled **1**-Enabled **Note:** To use ICE feature, you have to configure the STUN and/or TURN server address in advance. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->NAT->ICE->Active **Phone User Interface:** None		
sip.nat_turn.enable	**0 or 1**	**0**
Description: Enables or disables the TURN (Traversal Using Relays around NAT) feature on the IP phone. **0**-Disabled		

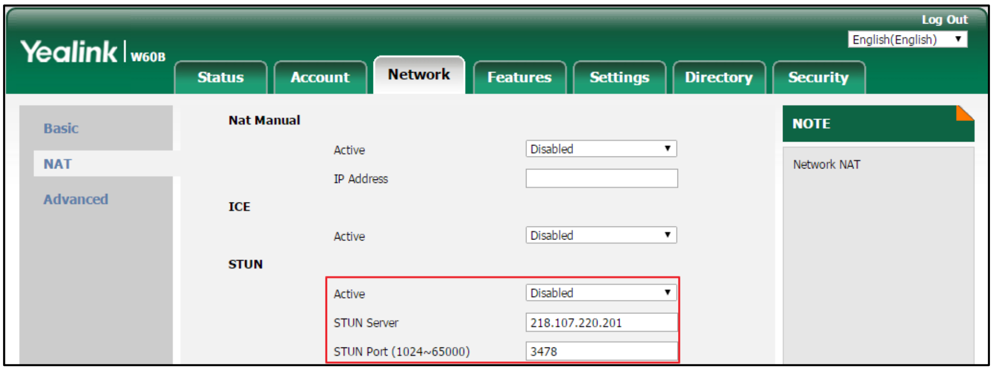
Parameters	Permitted Values	Default
1-Enabled **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->NAT->TURN->Active **Phone User Interface:** None		
sip.nat_turn.server	**IP address or domain name**	**Blank**
Description: Configures the IP address or the domain name of the TURN (Traversal Using Relays around NAT) server. **Example:** sip.nat_turn.server = 218.107.220.202 **Note:** It works only if the value of the parameter "sip.nat_turn.enable" is set to 1 (Enabled). If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->NAT->TURN->TURN Server **Phone User Interface:** None		
sip.nat_turn.port	**Integer from 1 to 65535**	**3478**
Description: Configures the port of the TURN (Traversal Using Relays around NAT) server. **Example:** sip.nat_turn.port = 3478 **Note:** It works only if the value of the parameter "sip.nat_turn.enable" is set to 1 (Enabled). If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->NAT->TURN->TURN Port (1~65535) **Phone User Interface:** None		
sip.nat_turn.username	**String**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the user name to authenticate to TURN (Traversal Using Relays around NAT) server. **Example**: sip.nat_turn.username = admin **Note:** It works only if the value of the parameter "sip.nat_turn.enable" is set to 1 (Enabled). If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->NAT->TURN->User Name **Phone User Interface:** None		
sip.nat_turn.password	**String**	**Blank**
Description: Configures the password to authenticate to the TURN (Traversal Using Relays around NAT) server. **Example**: sip.nat_turn.password = yealink1105 **Note:** It works only if the value of the parameter "sip.nat_turn.enable" is set to 1 (Enabled). If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->NAT->TURN->Password **Phone User Interface:** None		
sip.listen_port	**Integer from 1024 to 65535**	**5060**
Description: Configures the local SIP port. **Web User Interface:** Settings->SIP->Local SIP Port **Phone User Interface:** None		
sip.tls_listen_port	**Integer from 1024 to 65535**	**5061**

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

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

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

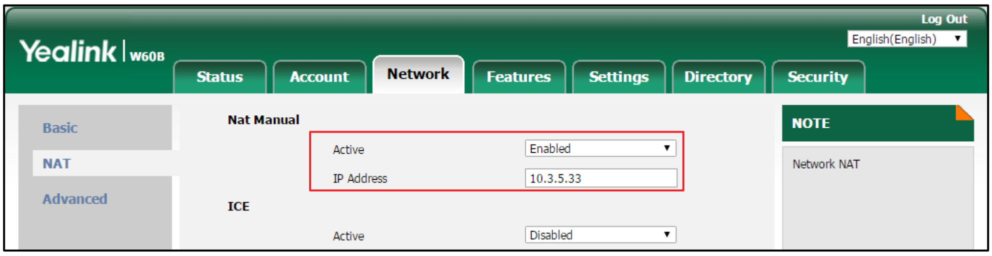


5. Click **Confirm** to accept the change.

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

To configure manual NAT via web user interface:

1. Click on **Network**->**NAT**.
2. In the **Nat Manual** block, select the desired value from the pull-down list of **Active**.
3. Enter the external IP address in the **IP Address** field.



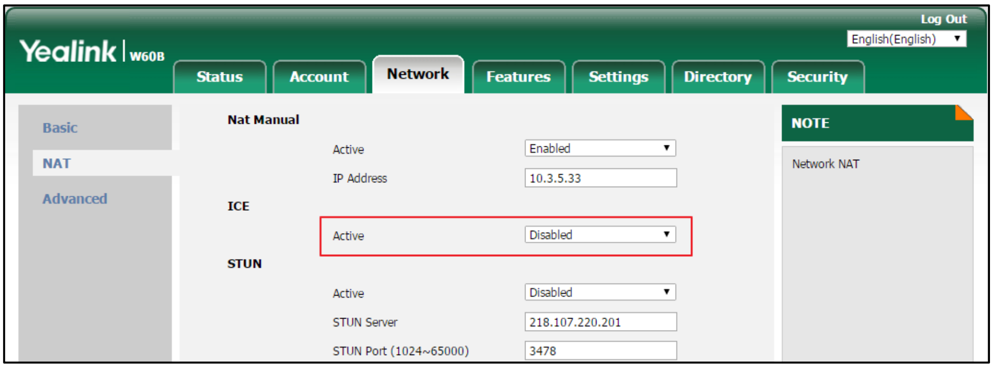
4. Click **Confirm** to accept the change.

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

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

To configure ICE feature via web user interface:

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

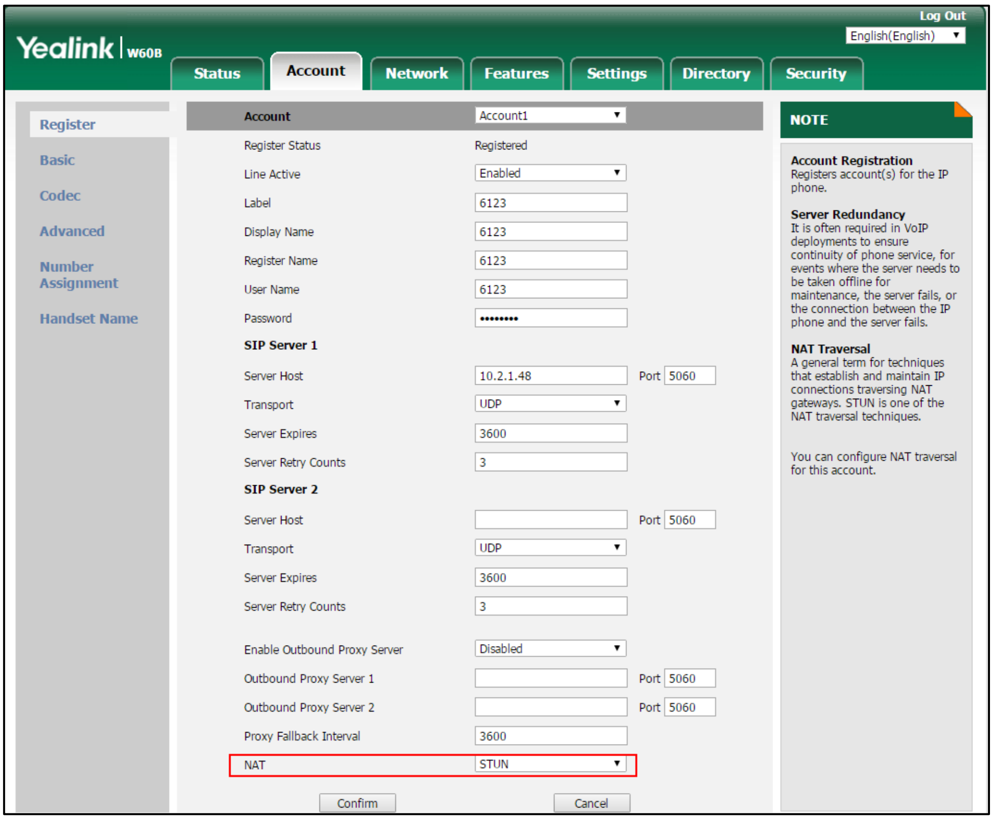


3. Click **Confirm** to accept the change.

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

To configure NAT traversal and STUN for account via web user interface:

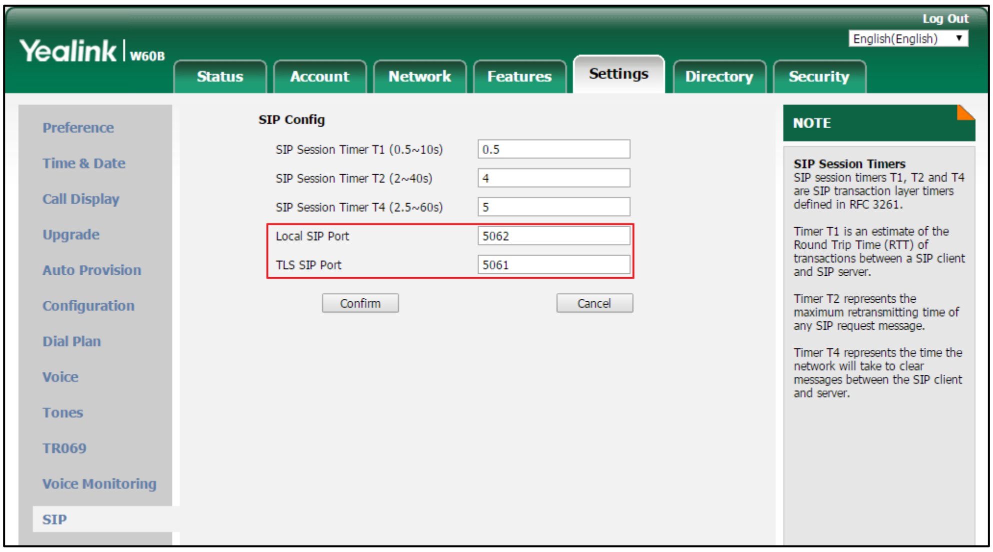
1. Click on **Account**->**Register**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **STUN**/**Manual NAT** from the pull-down list of **NAT**.



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

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

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



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

Keep Alive

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

Procedure

Keep alive feature can be configured using the following methods.

Configuration File	<MAC>.cfg	Configure the type of keep-alive packets on a per-line basis. **Parameters:** account.X.nat.udp_update_enable
		Configure the keep-alive interval on a per-line basis. **Parameters:** account.X.nat.udp_update_time
Local	Web User Interface	Configure the type of keep-alive packets on a per-line basis. Configure the keep-alive interval on a per-line basis. **Navigate to**:

		http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

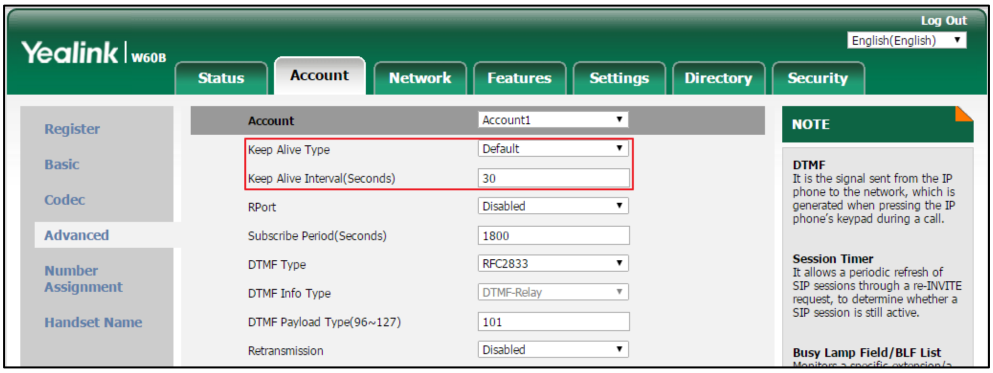
Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.nat.udp_update_enable (X ranges from 1 to 8)	**0, 1, 2 or 3**	**1**
Description: Configures the type of keep-alive packets sent by the DECT IP phone to the NAT device to keep the communication port open so that NAT can continue to function for account X. **0**-Disabled **1**-Default (the DECT IP phone sends UDP packets to the server) **2**-Options (the DECT IP phone sends SIP OPTIONS packets to the server) **3**-Notify (the DECT IP phone sends SIP NOTIFY packets to the server) **Web User Interface:** Account->Advanced->Keep Alive Type **Handset User Interface:** None		
account.X.nat.udp_update_time (X ranges from 1 to 8)	**Integer from 15 to 2147483647**	**30**
Description: Configures the keep-alive interval (in seconds) for account X. **Example:** account.1.nat.udp_update_time = 60 **Note**: It works only if the value of the parameter "account.X.nat.udp_update_enable" is set to 1, 2 or 3. **Web User Interface:** Account->Advanced->Keep Alive Interval(Seconds) **Handset User Interface:** None		

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

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

4. Enter the keep-alive interval in the **Keep Alive Interval(Seconds)** field.



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

Rport

The Session Initiation Protocol (SIP) operates over UDP and TCP. When used with UDP, responses to requests are returned to the source address the request came from, and returned to the port written into the topmost "Via" header of the request message. However, this behavior is not desirable when the client is behind a Network Address Translation (NAT) or firewall. So a new parameter "rport" for the "Via" header field is required.

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

Rport feature depends on support from a SIP server.

Procedure

Rport feature can be configured using the following methods.

Configuration File	<MAC>.cfg	Configure NAT Rport feature for account. **Parameters:** account.X.nat.rport
Local	Web User Interface	Configure NAT Rport feature for account. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

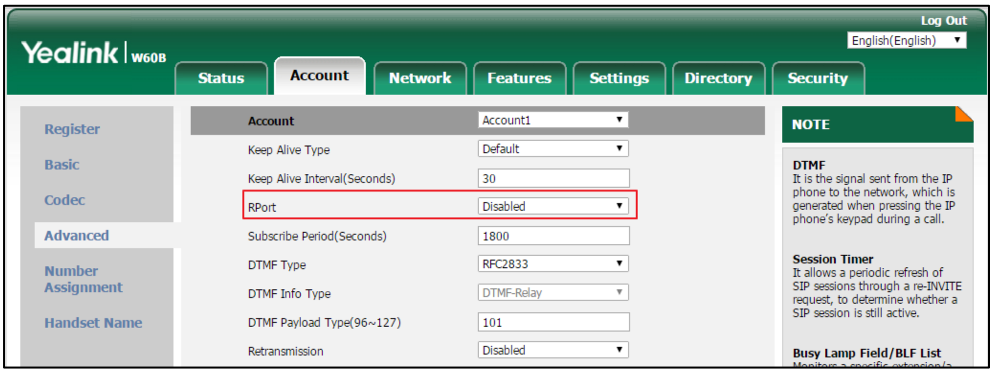
Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.nat.rport (X ranges from 1 to 8)	**0, 1 or 2**	**0**

Parameters	Permitted Values	Default
Description: Enables or disables NAT RPort feature for account X. **0**-Disabled **1**-Enabled **2**-Enable Direct Process **Web User Interface:** Account->Advanced->RPort **Handset User Interface:** None		

To configure Rport feature via web user interface:

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



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

Quality of Service (QoS)

Quality of Service (QoS) is the ability to provide different priorities for different packets in the network, allowing the transport of traffic with special requirements. QoS guarantees are important for applications that require fixed bit rate and are delay sensitive when the network capacity is insufficient. There are four major QoS factors to be considered when configuring a modern QoS implementation: bandwidth, delay, jitter and loss.

QoS provides better network service through the following features:

- Supporting dedicated bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion

- Shaping network traffic
- Setting traffic priorities across the network

The Best-Effort service is the default QoS model in IP networks. It provides no guarantees for data delivering, which means delay, jitter, packet loss and bandwidth allocation are unpredictable. Differentiated Services (DiffServ or DS) is the most widely used QoS model. It provides a simple and scalable mechanism for classifying and managing network traffic and providing QoS on modern IP networks. Differentiated Services Code Point (DSCP) is used to define DiffServ classes and stored in the first six bits of the ToS (Type of Service) field. Each router on the network can provide QoS simply based on the DiffServ class. The DSCP value ranges from 0 to 63 with each DSCP specifying a particular per-hop behavior (PHB) applicable to a packet. A PHB refers to the packet scheduling, queuing, policing, or shaping behavior of a node on any given packet.

Four standard PHBs available to construct a DiffServ-enabled network and achieve QoS:

- **Class Selector PHB** -- backwards compatible with IP precedence. Class Selector code points are of the form "xxx000". The first three bits are the IP precedence bits. These class selector PHBs retain almost the same forwarding behavior as nodes that implement IP precedence-based classification and forwarding.
- **Expedited Forwarding PHB** -- the key ingredient in DiffServ model for providing a low-loss, low-latency, low-jitter and assured bandwidth service.
- **Assured Forwarding PHB** -- defines a method by which BAs (Bandwidth Allocations) can be given different forwarding assurances.
- **Default PHB** -- specifies that a packet marked with a DSCP value of "000000" gets the traditional best effort service from a DS-compliant node.

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

Voice QoS

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

SIP QoS

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

DSCPs for voice and SIP packets can be specified respectively.

Note

For voice and SIP packets, the IP phone obtains DSCP info from the network policy if LLDP feature is enabled, which takes precedence over manual settings. For more information on LLDP, refer to LLDP on page 33.

Procedure

QoS can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the DSCPs for voice packets and SIP packets. **Parameters:** static.network.qos.audiotos static.network.qos.signaltos
Web User Interface		Configure the DSCPs for voice packets and SIP packets. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load

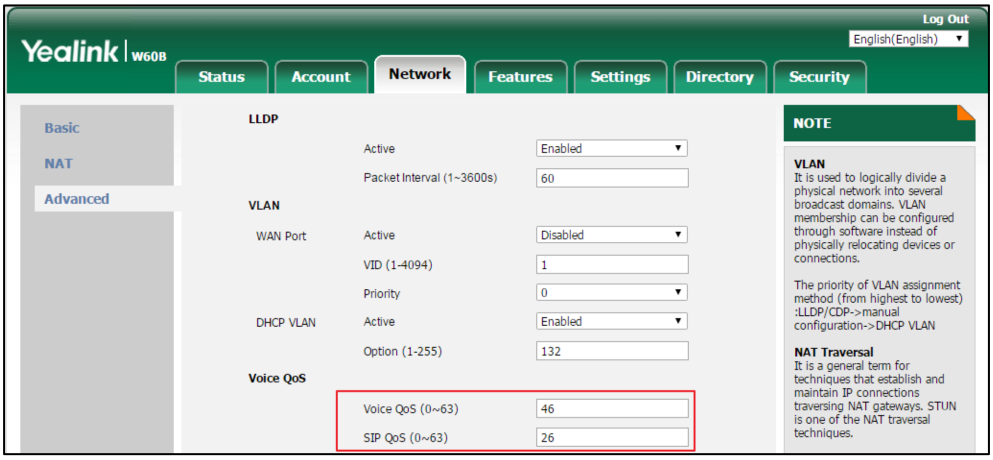
Details of Configuration Parameters:

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

Parameters	Permitted Values	Default
Handset User Interface: None		

To configure DSCPs for voice packets and SIP packets via web user interface:

1. Click on **Network**->**Advanced**.
2. Enter the desired value in the **Voice QoS (0~63)** field.
3. Enter the desired value in the **SIP QoS (0~63)** field.



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

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

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

802.1X Authentication

IEEE 802.1X authentication is an IEEE standard for Port-based Network Access Control (PNAC), part of the IEEE 802.1 group of networking protocols. It offers an authentication mechanism for devices to connect/link to a LAN or WLAN.

The 802.1X authentication involves three parties: a supplicant, an authenticator and an authentication server. The supplicant is the DECT IP phone that wishes to attach to the LAN or WLAN. With 802.1X port-based authentication, the DECT IP phone provides credentials, such as user name and password, for the authenticator, and then the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the DECT IP phone is allowed to access resources located on the protected side of the network.

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

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

- EAP-TTLS/EAP-MSCHAPv2 (requires CA certificates)
- EAP-PEAP/GTC (requires CA certificates)
- EAP-TTLS/EAP-GTC (requires CA certificates)
- EAP-FAST (supports EAP In-Band provisioning, requires CA certificates if the provisioning mode is Authenticated Provisioning)

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

Procedure

802.1X authentication can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the 802.1X authentication. **Parameters:** static.network.802_1x.mode static.network.802_1x.eap_fast_provision_mode static.network.802_1x.anonymous_identity static.network.802_1x.identity static.network.802_1x.md5_password static.network.802_1x.root_cert_url static.network.802_1x.client_cert_url
Web User Interface		Configure the 802.1X authentication. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.802_1x.mode	**0, 1, 2, 3, 4, 5, 6 or 7**	**0**
Description: Configures the 802.1x authentication method. **0**-EAP-None **1**-EAP-MD5 **2**-EAP-TLS **3**-EAP-PEAP/MSCHAPv2 **4**-EAP-TTLS/EAP-MSCHAPv2 **5**-EAP-PEAP/GTC		

Parameters	Permitted Values	Default
6-EAP-TTLS/EAP-GTC **7**-EAP-FAST If it is set to 0 (EAP-None), 802.1x authentication is not required. **Note:** If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->802.1x->802.1x Mode **Handset User Interface:** None		
static.network.802_1x.eap_fast_provision_mode	**0 or 1**	**0**
Description: Configures the EAP In-Band provisioning method for EAP-FAST. **0**-Unauthenticated Provisioning **1**-Authenticated Provisioning If it is set to 0 (Unauthenticated Provisioning), EAP In-Band provisioning is enabled by server unauthenticated PAC (Protected Access Credential) provisioning using anonymous Diffie-Hellman key exchange. If it is set to 1 (Authenticated Provisioning), EAP In-Band provisioning is enabled by server authenticated PAC provisioning using certificate based server authentication. **Note:** It works only if the value of the parameter "static.network.802_1x.mode" is set to 7 (EAP-FAST). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->802.1x->Provisioning Mode **Handset User Interface:** None		
static.network.802_1x.anonymous_identity	**String within 512 characters**	**Blank**
Description: Configures the anonymous identity (user name) for 802.1X authentication. It is used for constructing a secure tunnel for 802.1X authentication. **Example:** static.network.802_1x.anonymous_identity = anonymous **Note:** It works only if the value of the parameter "static.network.802_1x.mode" is set to 2,		

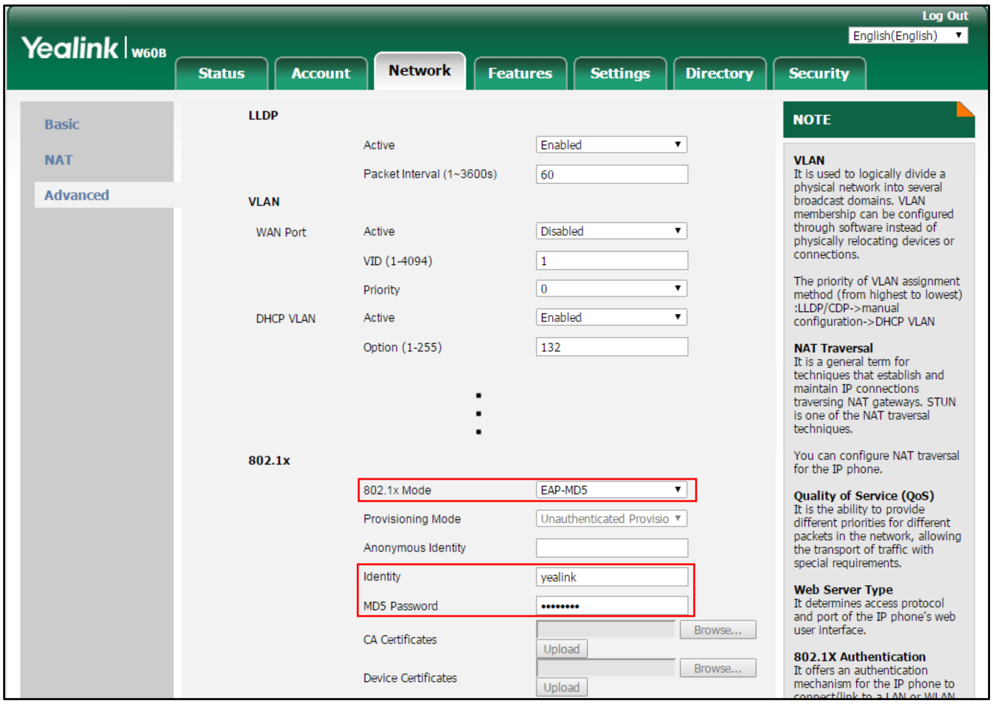
Parameters	Permitted Values	Default
3, 4, 5, 6 or 7. If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->802.1x->Anonymous Identity **Handset User Interface:** None		
static.network.802_1x.identity	**String within 32 characters**	**Blank**
Description: Configures the identity (or user name) for 802.1x authentication. **Example:** static.network.802_1x.identity = yealink **Note:** It works only if the value of the parameter "static.network.802_1x.mode" is set to 1, 2, 3, 4, 5, 6 or 7. If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->802.1x->Identity **Handset User Interface:** None		
static.network.802_1x.md5_password	**String within 32 characters**	**Blank**
Description: Configures the password for 802.1x authentication. **Example:** static.network.802_1x.md5_password = admin123 **Note:** It works only if the value of the parameter "static.network.802_1x.mode" is set to 1, 3, 4, 5, 6 or 7. If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->802.1x->MD5 Password **Handset User Interface:** None		
static.network.802_1x.root_cert_url	**URL within 511 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the access URL of the CA certificate. **Example:** static.network.802_1x.root_cert_url = http://192.168.1.10/ca.pem **Note:** It works only if the value of the parameter "static.network.802_1x.mode" is set to 2, 3, 4, 5, 6 or 7. If the authentication method is EAP-FAST, you also need to set the value of the parameter "static.network.802_1x.eap_fast_provision_mode" to 1 (Authenticated Provisioning). The format of the CA certificate must be *.pem, *.crt, *.cer or *.der. **Web User Interface:** Network->Advanced->802.1x->CA Certificates **Handset User Interface:** None		
static.network.802_1x.client_cert_url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the device certificate. **Example:** static.network.802_1x.client_cert_url = http://192.168.1.10/client.pem **Note:** It works only if the value of the parameter "static.network.802_1x.mode" is set to 2 (EAP-TLS). The format of the device certificate must be *.pem. **Web User Interface:** Network->Advanced->802.1x->Device Certificates **Handset User Interface:** None		

To configure the 802.1X authentication via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **802.1x** block, select the desired protocol from the pull-down list of **802.1x Mode**.
    a) If you select **EAP-MD5**:
        1) Enter the user name for authentication in the **Identity** field.

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



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

1) (Optional.) Enter the anonymous user name for authentication in the **Anonymous Identity** field.

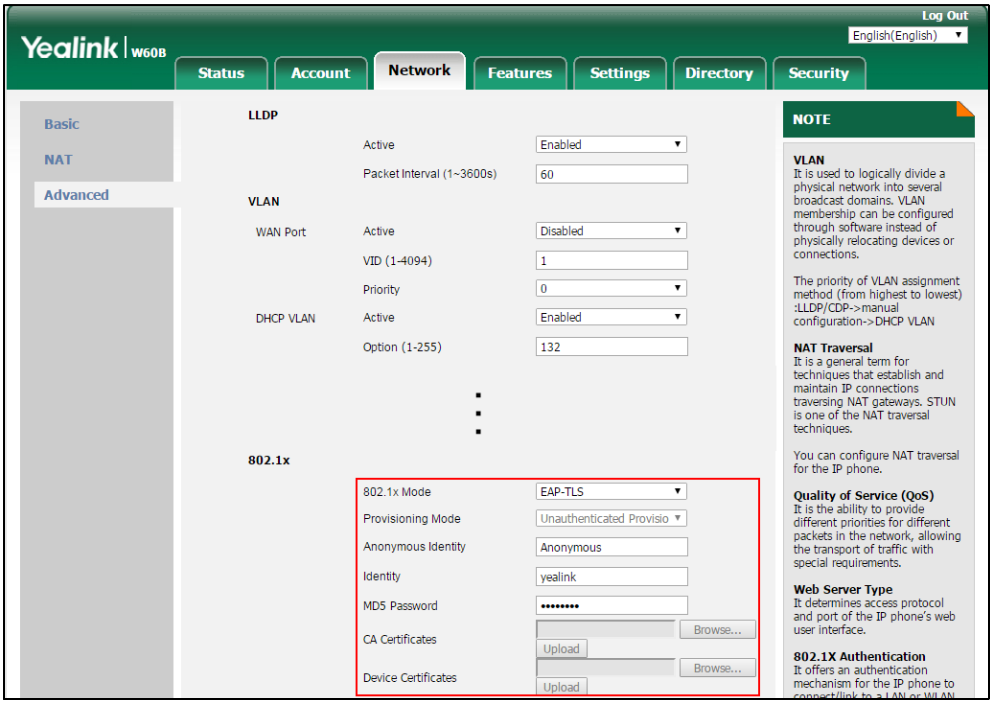
2) Enter the user name for authentication in the **Identity** field.

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

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

5) In the **Device Certificates** field, click **Browse** to select the desired client (*.pem or *.cer) certificate from your local system.

6) Click **Upload** to upload the certificates.



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

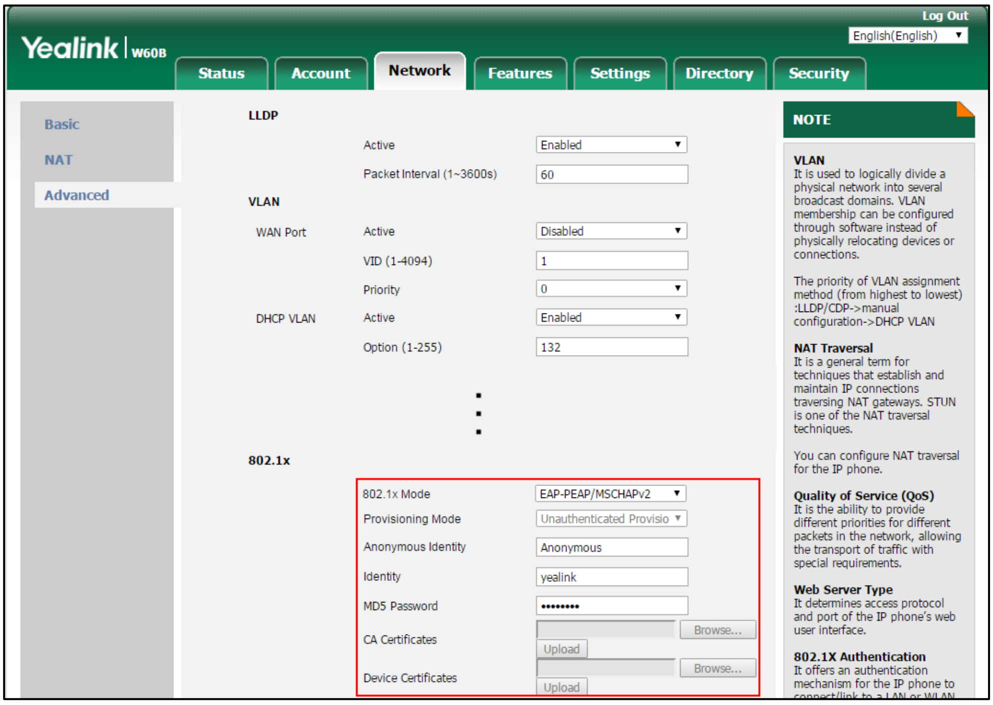
1) (Optional.) Enter the anonymous user name for authentication in the **Anonymous Identity** field.

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

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

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

5) Click **Upload** to upload the certificate.



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

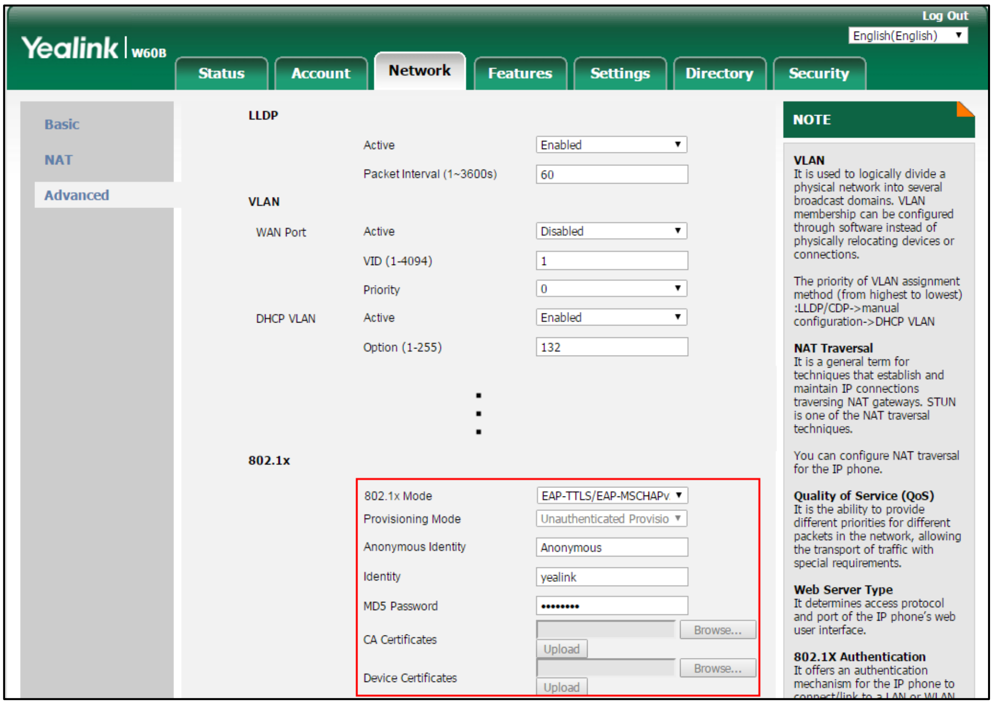
1) (Optional.) Enter the anonymous user name for authentication in the **Anonymous Identity** field.

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

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

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

5) Click **Upload** to upload the certificate.



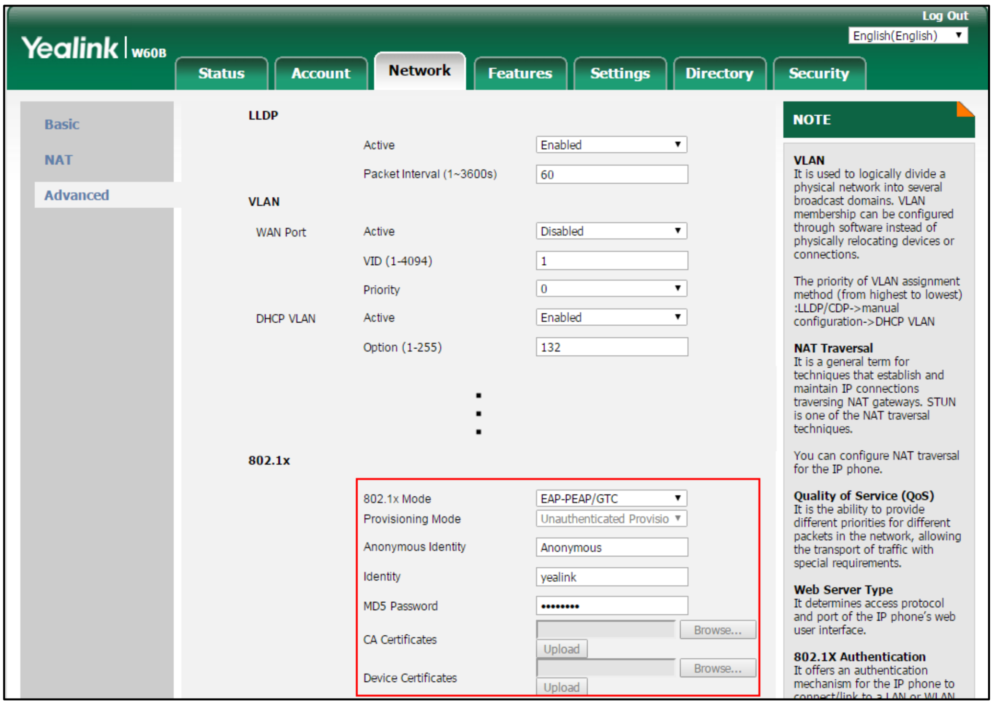
e) If you select **EAP-PEAP/GTC**:

1) (Optional.) Enter the anonymous user name for authentication in the **Anonymous Identity** field.

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

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

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



5) Click **Upload** to upload the certificate.

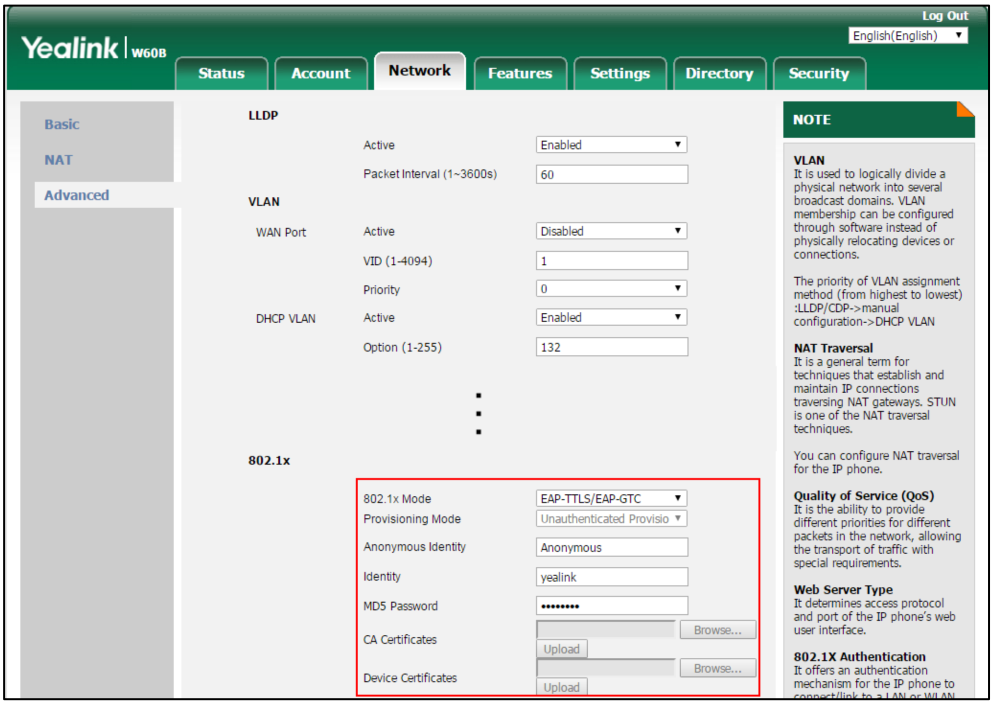
f) If you select **EAP-TTLS/EAP-GTC**:

1) (Optional.) Enter the anonymous user name for authentication in the **Anonymous Identity** field.

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

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

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



5) Click **Upload** to upload the certificate.

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

1) (Optional.) Enter the anonymous user name for authentication in the **Anonymous Identity** field.

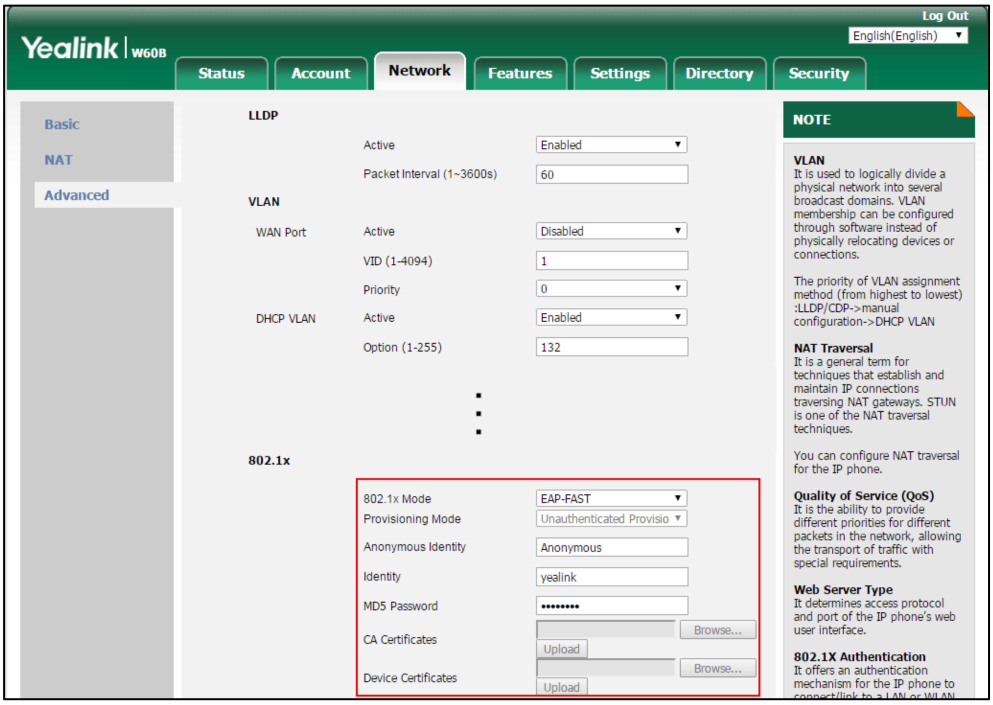
2) Enter the user name for authentication in the **Identity** field.

3) Select the desired value from the pull-down list of **Provisioning Mode**.

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

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

The CA certificate needs to be uploaded only when **Authenticated Provisioning** mode is selected from the **Provisioning Mode** field.



6) Click **Upload** to upload the certificate.

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

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

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

Setting Up Your Phones with a Provisioning Server

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

This chapter consists of the following sections:

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

Provisioning Points to Consider

- If you are provisioning a mass of DECT IP phones, we recommend you to use central provisioning method as your primary configuration method. For more information on central provisioning, refer to Central Provisioning on page 82.

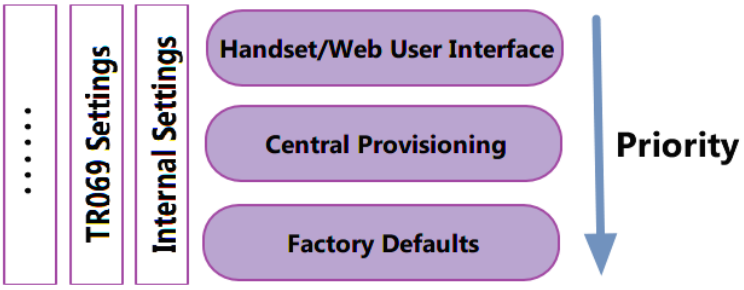
- A provisioning server maximizes the flexibility you have when installing, configuring, upgrading, and managing the DECT IP phones, and enables you to store boot, configuration, log, and contact files on the server. You can set up a provisioning server on the local area network (LAN) or anywhere on the Internet. For more information, refer to Setting Up a Provisioning Server on page 91.
- If the DECT IP phone cannot obtain the address of a provisioning server during startup, and has not been configured with settings from any other source, the DECT IP phone will use configurations stored in the flash memory. If the phone that cannot obtain the address of a provisioning server has previously been configured with settings it will use those previous settings.

Provisioning Methods

DECT IP phones can be configured automatically through configuration files stored on a central provisioning server, manually via web user interface or handset user interface, or by a combination of the automatic and manual methods. If a central provisioning server is not available, you can configure most features using manual method.

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

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



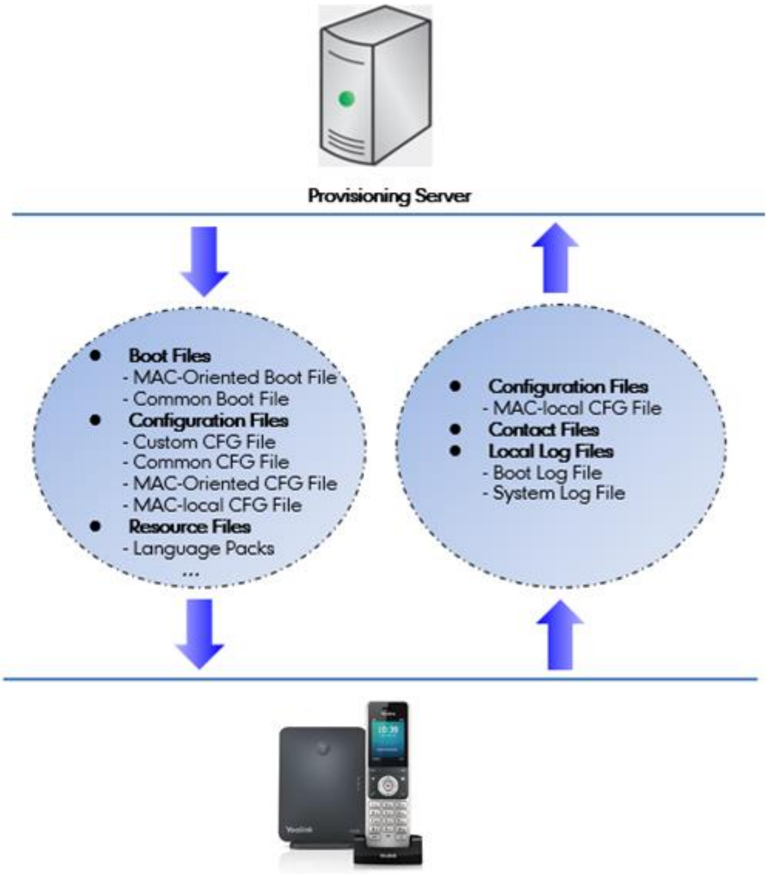
Note

The priority mechanism takes effect only if the value of the parameter "static.auto_provision.custom.protect" is set to 1. For more information on this parameter, refer to Configuration Parameters on page 106.

Static settings have no priority. For example, settings associated with auto provisioning/network/syslog, TR069 settings and internal settings (e.g., the temporary configurations to be used for program running). For more information, refer to Appendix E: Static Settings on page 474.

Central Provisioning

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



Using the boot files and configuration files to provision the phones and to modify features and configurations is called the central provisioning method. You can use a text-based editing application to edit boot files and configuration files, and then store boot files and configuration files to a provisioning server. DECT IP phones can be centrally provisioned from a provisioning server. For more information on the provisioning server, refer to Setting Up a Provisioning Server on page 91. For more information on boot files, refer to Boot Files on page 84. For more information on configuration files, refer to Configuration Files on page 86.

DECT IP phones can obtain the provisioning server address during startup. Then DECT IP phones download boot files and configuration files from the provisioning server, resolve and update the configurations written in configuration files. This entire process is called auto provisioning. For more information on auto provisioning, refer to *Yealink SIP IP Phones Auto Provisioning Guide_V81*. In addition to the boot files and configuration files, the DECT IP phones also download resource files during auto provisioning. For more information on resource files, refer to Resource Files on page 87.

Yealink DECT IP phones support keeping user personalized configuration settings using the MAC-local CFG file. For more information on this file, refer to MAC-local CFG File on page 86.

The DECT IP phones can be configured to upload log files (log files provide a history of phone events) and contact files to the provisioning server. You can configure a separate directory for each of these files to help organize: a log file directory. For more information, refer to Viewing Log Files on page 425.

Manual Provisioning

When you manually configure a phone via web user interface or handset user interface, the changes associated with non-static settings 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 on page 86. This file is stored on the phone, but a copy can be also uploaded to the provisioning server or a specific URL (if configured).

There are two ways to manually provision DECT IP phones:

- Web User Interface
- Handset User Interface

Web User Interface

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

An administrator or a user can configure DECT IP phones via web user interface; but accessing the web user interface requires password. The default user name and password for the administrator are both “admin” (case-sensitive). The default user name and password for the user are both “user” (case-sensitive). For more information on configuring passwords, refer to User and Administrator Passwords on page 397.

This method enables you to perform configuration changes on a per-phone basis. Note that the features can be configured via web user interface are limited. So, you can use the web user interface method as the sole configuration method or in conjunction with central provisioning method and handset user interface method.

DECT IP phones support both HTTP and HTTPS protocols for accessing the web user interface. For more information, refer to Web Server Type on page 29.

Handset User Interface

You can configure DECT IP phones via handset user interface on a per-phone basis. As with the web user interface, handset user interface makes configurations available to users and administrators.

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

Boot Files, Configuration Files and Resource Files

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

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

- Boot Files
- Configuration Files
- Resource Files
- Obtaining Boot Files/Configuration Files/Resource Files

Boot Files

Yealink DECT IP phones running firmware version 81 or later support a new boot file in which you can customize the download sequence of configuration files. It is efficiently for you to provision your DECT IP phones in different deployment scenarios, especially when you want to apply a set of features or settings to a group of phones.

Note You can select whether to use the boot file or not for auto provisioning according to your deployment scenario. If you do not use the boot file, proceed to Configuration Files on page 86. That is, you can also use the old mechanism for auto provisioning.

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

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

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

The following figure shows an example of common boot file:

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

```
include:config "http://10.2.5.206/configure/account.cfg"
overwrite_mode = 1
```

Learn the following:

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

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

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

Note

Overwrite mode only affects the non-static settings configured using configuration files.

If you do not use the boot file for auto provisioning, overwrite mode is disabled by default and you are not allowed to enable it.

For more information on how to customize boot file, refer to *Yealink SIP IP Phones Auto Provisioning Guide_V81*.

Common Boot File

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

MAC-Oriented Boot File

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

The MAC-Oriented boot file is named after the MAC address of the IP phone. MAC address, a unique 12-digit serial number assigned to each phone, can be obtained from the bar code on the back of the IP phone. For example, if the MAC address of an IP phone is 00156574B150, the name of the MAC-Oriented boot file is 00156574b150.boot (case-sensitive).

Configuration Files

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

Yealink configuration files consist of:

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

Common CFG File

Common CFG file, fixed named y000000000077.cfg, contains parameters that affect the basic operation of the DECT IP phone, such as language and volume. It will be effectual for all DECT IP phones.

MAC-Oriented CFG File

MAC-Oriented CFG file, named <MAC>.cfg, contains parameters unique to a particular phone, such as account registration. It will only be effectual for a specific DECT IP phone.

The MAC-Oriented CFG file is named after the MAC address of the DECT IP phone. MAC address, a unique 12-digit serial number assigned to each phone, can be obtained from the bar code on the back of the base. For example, if the MAC address of an DECT IP phone is 00156574B150, the name of the MAC-Oriented CFG file is 00156574b150.cfg (case-sensitive).

MAC-local CFG File

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

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

Note After the provisioning priority mechanism is enabled (configured by the parameter "static.auto_provision.custom.protect"), all older changes made via web/phone user interface will not be saved in the <MAC>-local.cfg file. But the older settings still take effect on the phone. For more information on this parameter, refer to Configuration Parameters on page 106.

Keeping User Personalized Settings

The MAC-local CFG file is stored locally on the DECT IP phone and can also be uploaded to the provisioning server/a specific URL (if configured, refer to Configuration Parameters). This file enables users to keep their personalized configuration settings, even though the DECT IP phone reboots or upgrades. For more information on how to keep user personalized settings, refer to Keeping User Personalized Settings after Auto Provisioning on page 106.

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

- To clear the MAC-local CFG file, reset the DECT IP phone to factory configuration settings by selecting **Reset local settings** via handset user interface (navigate to **OK**->**Settings**->**System Settings** ->**Base Reset** (default password: 0000) ->**Reset Config**).
- To clear the MAC-local CFG file, reset the DECT IP phone to factory configuration settings by navigating to the **Upgrade** menu via web user interface and clicking **Reset local setting**.

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

Most configurations made by users via handset user interface and web user interface can be saved to the <MAC>-local.cfg file, but some static settings will never be saved to the <MAC>-local.cfg file. For more information, refer to Appendix E: Static Settings on page 474.

You need to reset the phone configurations not saved in the <MAC>-local.cfg file separately. For more information, refer to Resetting Issues on page 453.

By default, the 00156574b150-local.cfg file will be stored on the DECT IP phone. The DECT IP phone can be configured to upload this file to the provisioning server each time the file updates. For more information, refer to the parameter “static.auto_provision.custom.sync” described in the section Configuration Parameters on page 106.

Custom CFG File

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

For more information on how to create a new CFG file, refer to *Yealink SIP IP Phones Auto Provisioning Guide_V81*.

Resource Files

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

If you want to specify the desired phone to use the resource file, the access URL of resource file should be specified in the MAC-Oriented CFG file. During provisioning, the DECT IP phones will request the resource files in addition to the configuration files. For more information on the access URL of resource file, refer to the corresponding section in this guide.

The followings show examples of resource files:

- Language packs
- Ring tones
- Local contact file

For more information on resource files, refer to Obtaining Boot Files/Configuration Files/Resource Files on page 89.

If you want to delete resource files from a phone at a later date - for example, if you are giving the phone to a new user - you can reset the DECT IP phone to factory configuration settings. For more information, refer to Resetting Issues on page 453.

Obtaining Boot Files/Configuration Files/Resource Files

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

The names of the Yealink-supplied template files are:

Template File		File Name	Description
Boot File		y000000000000.boot	Allows you to customize the download sequence of the configuration files during auto provisioning. For more information, refer to Boot Files on page 84.
Configuration Files	Common CFG File	Common.cfg	Allow you to deploy and maintain a mass of Yealink DECT IP phones. For more information, refer to Common CFG File and MAC-Oriented CFG File on page 86.
	MAC-Oriented CFG File	MAC.cfg	
	Custom CFG Files	For example, sip.cfg account.cfg	Allow you to apply a set of features or settings to a group of Yealink DECT IP phones. For more information, refer to Custom CFG File on page 87.
Resource Files	AutoDST Template	AutoDST.xml	Allows you to add or modify time zone and DST settings for your area. For more information, refer to Customizing an AutoDST Template File on page 180.

Template File		File Name	Description
	Language Packs	For example, 000.GUI.English.lang 1.English_note.xml 1.English.js	Allow you to customize the translation of the existing language on the phone/web user interface. For more information, refer to Loading Language Packs on page 133.
	Replace Rule Template	dialplan.xml	Allows you to customize multiple replace rules for DECT IP phone dial plan. For more information, refer to Customizing Replace Rule Template File on page 189.
	Dial Now Template	dialnow.xml	Allows you to customize multiple dial now rules for DECT IP phone dial plan. For more information, refer to Customizing Dial Now Template File on page 194.
	Local Contact File	ContactData.xml	Allows you to add or modify multiple contacts at a time for your DECT IP phone. For more information, refer to Customizing a Directory Template File on page 209.
	Blacklist File	blacklist.xml	Allows you to add or modify multiple black contacts at a time for your DECT IP phone.
	Super Search Template	super_search.xml	Allows you to customize the search source list for your DECT IP phone. For more information, refer to Customizing a Super Search Template File on page 210.
	Remote Phone Book Template	Department.xml Menu.xml	Allows you to add or modify multiple remote contacts for your DECT IP phone. For more information, refer to Customizing Remote Phone Book Template File on page 292.

To download template files:

1. Go to Yealink Document Download page and select the desired phone model.
2. Download and extract the combined files to your local system.
3. Open the folder you extracted and identify the template file you will edit according to the table introduced above.

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

<table>
<tr><th>Server
Platform</th><th>HTTP/HTTPS</th><th>TFTP/FTP</th></tr>
<tr><td>Windows</td><td>Support: ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } (including space)<br><b>Not Support:</b> | < > : " / \ * ? # % & = +</td><td><b>Support:</b> ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } % & = + (including space)
Not Support: | < > : " / \ * ? #</td></tr>
<tr><td>Linux</td><td>Support: ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } | < > : " (including space)<br><b>Not Support:</b> / \ * ? # % & = +</td><td><b>Support:</b> ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } | < > : " % & = + (including space)
Not Support: / \ * ? #</td></tr>
</table>

Setting Up a Provisioning Server

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

This chapter consists of the following sections:

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

Why Using a Provisioning Server?

You can use a provisioning server to configure your DECT IP 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.

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

For more information on auto provisioning, refer to *Yealink SIP IP Phones Auto Provisioning Guide_V81*.

The DECT IP phones can be configured to periodically upload the log files to the provisioning server or specific server, which can help an administrator more easily find the system problem and fix it. For more information on log files, refer to Viewing Log Files on page 425.

Supported Provisioning Protocols

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

Note

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

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

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

Configuring a Provisioning Server

The provisioning server can be set up on the local LAN or anywhere on the Internet. Use the following procedure as a recommendation if this is your first provisioning server setup. For more information on how to set up a provisioning server, refer to *Yealink SIP IP Phones Auto Provisioning Guide_V81*.

To set up the provisioning server:

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

For more information on how to deploy DECT IP phones using boot files and configuration files, refer to Deploying Phones from the Provisioning Server on page 93.

Note

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

Deploying Phones from the Provisioning Server

During auto provisioning, DECT IP phones download the boot file first, and then download the configuration files referenced in the boot file in sequence. The parameters in the new downloaded configuration files will override the duplicate parameters in files downloaded earlier. For more information on boot files and configuration files, refer to Boot Files on page 84 and Configuration Files on page 86.

The boot files can only be used by the DECT IP phones running firmware version 81 or later. The configuration files, supplied with each firmware release, must be used with that release. Otherwise, configurations may not take effect, and the DECT IP phone will behave without exception. Before you configure parameters in the configuration files, Yealink recommends that you create new configuration files containing only those parameters that require changes.

To deploy DECT IP phones from the provisioning server:

1. Create per-phone boot files by performing the following steps:
   a) Obtain a list of phone MAC addresses (the bar code label on the back of the W60B base station or on the outside of the box).
   b) Create per-phone <MAC>.boot files by using the template boot file.
   c) Specify the configuration files paths in the file as desired.
2. Edit the common boot file by performing the following step:
   a) Specify the configuration files paths in the file as desired.
3. Create per-phone configuration files by performing the following steps:
   a) Create per-phone <MAC>.cfg files by using the MAC-Oriented CFG file from the distribution as templates.
   b) Edit the parameters in the file as desired.
4. Create new common configuration files by performing the following steps:
   a) Create y000000000077.cfg files by using the Common CFG file from the distribution as templates.
   b) Edit the parameters in the file as desired.
5. Copy boot files and configuration files to the home directory of the provisioning server.
6. Reboot DECT IP phones to trigger the auto provisioning process.

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

For protecting against unauthorized access, you can encrypt configuration files. For more information on encrypting configuration files, refer to Encrypting and Decrypting Files on page 416.

Note

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

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

- **PnP**: PnP feature allows DECT IP phones to discover the provisioning server address by broadcasting the PnP SUBSCRIBE message during startup.
- **DHCP**: DHCP option can be used to provide the address or URL of the provisioning server to DECT IP phones. When the DECT IP phone requests an IP address using the DHCP protocol, the resulting response may contain option 66 or the custom option (if configured) that contains the provisioning server address.
- **Static**: You can manually configure the server address via handset user interface or web user interface.

For more information on the above methods, refer to *Yealink SIP IP Phones Auto Provisioning Guide_V81*.

Upgrading Firmware

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

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

Note

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

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

Upgrading Firmware from the Provisioning Server

DECT IP phones support using FTP, TFTP, HTTP and HTTPS protocols to download configuration files and firmware from the provisioning server, and then upgrade firmware automatically. You can upgrade firmware for different handset models at the same time.

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

- Check for configuration files and then download firmware during startup.

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

Method of checking for configuration files is configurable.

Procedure

Configuration changes can be performed using the following methods.

<table>
<tr><td rowspan="4">Central Provisioning
(Configuration File)</td><td rowspan="4">y000000000077.cfg</td><td>Configure the way for the DECT IP phone to check for configuration files.
Parameters:
static.auto_provision.power_on
static.auto_provision.repeat.enable
static.auto_provision.repeat.minutes
static.auto_provision.weekly.enable
static.auto_provision.weekly_upgrade_interval
static.auto_provision.inactivity_time_expire
static.auto_provision.weekly.begin_time
static.auto_provision.weekly.end_time
static.auto_provision.weekly.dayofweek
static.auto_provision.flexible.enable
static.auto_provision.flexible.interval
static.auto_provision.flexible.begin_time
static.auto_provision.flexible.end_time</td></tr>
<tr><td>Specify the access URL of firmware for base station.
Parameter:
static.firmware.url</td></tr>
<tr><td>Specify the access URL of firmware for handset.
Parameters:
over_the_air.url
over_the_air.url.w52h
over_the_air.url.w56h</td></tr>
<tr><td>Configure the OTA upgrading feature for handset.
Parameters:
over_the_air.base_trigger
over_the_air.handset_tip</td></tr>
</table>

		over_the_air.handset_trigger
Web User Interface		Configure the way for the DECT IP phone to check for configuration files. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-autop&q=load
		Upgrade firmware. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-upgrade&q=load

Details of Configuration Parameters:

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

Parameters	Permitted Values	Default
Web User Interface: Settings->Auto Provision->Repeatedly **Handset User Interface:** None		
static.auto_provision.repeat.minutes	**Integer from 1 to 43200**	**1440**
Description: Configures the interval (in minutes) for the DECT IP phone to perform an auto provisioning process repeatedly. **Note**: It works only if the value of the parameter "static.auto_provision.repeat.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Interval(Minutes) **Handset User Interface:** None		
static.auto_provision.weekly.enable	**0 or 1**	**0**
Description: Triggers the weekly feature to on or off. **0**-Off **1**-On If it is set to 1 (On), the DECT IP phone will perform an auto provisioning process weekly. **Web User Interface:** Settings->Auto Provision->Weekly **Handset User Interface:** None		
static.auto_provision.weekly_upgrade_interval	**Integer from 0 to 12**	**0**
Description: Configures the period for the DECT IP phone to perform an auto provisioning. If it is set to 0, the DECT IP phone will perform an auto provisioning process during the specified time period (configured by the parameters "static.auto_provision.weekly.begin_time" and "static.auto_provision.weekly.end_time") of the day(s) (configured by the parameter static.auto_provision.weekly.dayofweek) every week.		

Parameters	Permitted Values	Default
If it is set to to other values (e.g., 2), the DECT IP phone will perform an auto provisioning process during the specified time period (configured by the parameters "static.auto_provision.weekly.begin_time" and "static.auto_provision.weekly.end_time") at a random day of the specified day(s) (configured by the parameter static.auto_provision.weekly.dayofweek) every 2 weeks. **Note**: It works only if the value of the parameter "static.auto_provision.weekly.enable" is set to 1 (On). Week here means from Sunday to Saturday, for example, today is Thursday (Dec. 22), the first week starts from Sunday (Dec. 25) to this Saturday (Dec. 31). **Web User Interface:** Settings->Auto Provision->Weekly Upgrade Interval(0~12week) **Handset User Interface:** None		
static.auto_provision.inactivity_time_expire	**Integer from 0 to 120**	**0**
Description: Configures the delay time (in minutes) to perform an auto provisioning process when the DECT IP phone is inactive at regular week. If it is set to 0, the IP phone will perform an auto provisioning process at random during the time period (configured by the parametera "static.auto_provision.weekly.begin_time" and "static.auto_provision.weekly.end_time"). If it is set to other values (e.g., 60), the IP phone will perform an auto provisioning process only when the IP phone has been inactivated for 60 minutes (1 hour) during the time period (configured by the parameters "static.auto_provision.weekly.begin_time" and "static.auto_provision.weekly.end_time"). **Note**: The auto provisioning may be performed during normal working hours when the IP phone has been inactivated for the designated time between the starting time and ending time. It works only if the value of the parameter "static.auto_provision.weekly.enable" is set to 1 (On). Week here means from Sunday to Saturday, for example, today is Thursday (Dec. 22), the first week starts from Sunday (Dec. 25) to this Saturday (Dec. 31). **Web User Interface:** Settings->Auto Provision->Inactivity Time Expire(0~120min) **Handset User Interface:** None		
static.auto_provision.weekly.begin_time	**Time from 00:00 to 23:59**	**00:00**
Description: Configures the starting time of the day for the DECT IP phone to perform an auto		

Parameters	Permitted Values	Default
provisioning process weekly. **Note**: It works only if the value of the parameter "static.auto_provision.weekly.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Time **Handset User Interface:** None		
static.auto_provision.weekly.end_time	**Time from 00:00 to 23:59**	**00:00**
Description: Configures the ending time of the day for the DECT IP phone to perform an auto provisioning process weekly. **Note**: It works only if the value of the parameter "static.auto_provision.weekly.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Time **Handset User Interface:** None		
static.auto_provision.weekly.dayofweek	**0, 1, 2, 3, 4, 5, 6 or a combination of these digits**	**0123456**
Description: Configures the days of the week for the DECT IP phone to perform an auto provisioning process weekly. If you configure two or more days, the DECT IP phone only performs the auto provisioning at a random day. **0**-Sunday **1**-Monday **2**-Tuesday **3**-Wednesday **4**-Thursday **5**-Friday **6**-Saturday **Example**: static.auto_provision.weekly.dayofweek = 01		

Parameters	Permitted Values	Default
It means the DECT IP phone will perform an auto provisioning process by randomly selecting a day from Sunday and Monday weekly. **Note**: It works only if the value of the parameter "static.auto_provision.weekly.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Day of Week **Handset User Interface:** None		
static.auto_provision.flexible.enable	**0 or 1**	**0**
Description: Triggers the flexible feature to on or off. **0**-Off **1**-On If it is set to 1 (On), the DECT IP phone will perform an auto provisioning process at random between a starting time configured by the parameter "static.auto_provision.flexible.begin_time" and an ending time configured by the parameter "static.auto_provision.flexible.end_time" on a random day within the period configured by the parameter "static.auto_provision.flexible.interval". **Note**: The day within the period is decided based upon the phone's MAC address and does not change with a reboot whereas the time within the start and end is calculated again with every reboot. **Web User Interface:** Settings->Auto Provision->Flexible Auto Provision **Handset User Interface:** None		
static.auto_provision.flexible.interval	**Integer from 1 to 1000**	**1**
Description: Configures the interval (in days) for the DECT IP phone to perform an auto provisioning process. The auto provisioning occurs on a random day within this period based on the phone's MAC address. **Example**: static.auto_provision.flexible.interval = 30 The DECT IP phone will perform an auto provisioning process on a random day (e.g., 18) based on the phone's MAC address.		

Parameters	Permitted Values	Default
Note: It works only if the value of the parameter "static.auto_provision.flexible.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Flexible Interval Days **Handset User Interface:** None		
static.auto_provision.flexible.begin_time	**Time from 00:00 to 23:59**	**02:00**
Description: Configures the starting time of the day for the DECT IP phone to perform an auto provisioning process at random. **Note**: It works only if the value of the parameter "static.auto_provision.flexible.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Flexible Time **Handset User Interface:** None		
static.auto_provision.flexible.end_time	**Time from 00:00 to 23:59**	**Blank**
Description: Configures the ending time of the day for the DECT IP phone to perform an auto provisioning process at random. If it is left blank or set to a specific value equal to starting time configured by the parameter "static.auto_provision.weekly.begin_time", the DECT IP phone will perform an auto provisioning process at the starting time. If it is set to a specific value greater than starting time configured by the parameter "static.auto_provision.weekly.begin_time", the DECT IP phone will perform an auto provisioning process at random between the starting time and ending time. It it is set to a specific value less than starting time configured by the parameter "static.auto_provision.weekly.begin_time", the DECT IP phone will perform an auto provisioning process at random between the starting time on that day and ending time in the next day. **Note**: It works only if the value of the parameter "static.auto_provision.flexible.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Flexible Time		

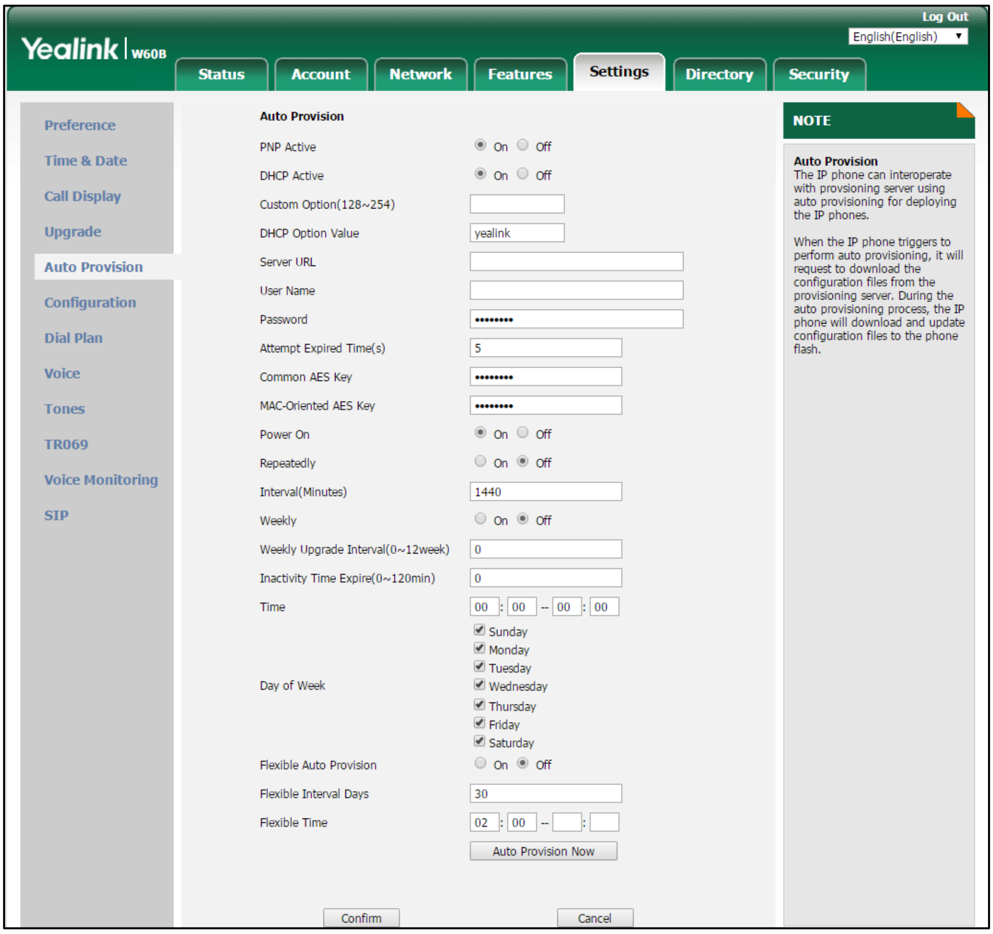
Parameters	Permitted Values	Default
Handset User Interface: None		
static.firmware.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the base firmware file. **Example:** static.firmware.url = http://192.168.1.20/77.81.0.10.rom **Note:** If you change this parameter, the W60B base station will reboot to make the change take effect. **Web User Interface:** Settings->Upgrade->Select and Upgrade Firmware **Handset User Interface:** None		
over_the_air.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the handset (W52H or W56H) firmware file. **Example:** over_the_air.url = http://192.168.1.20/61.81.30.rom **Note:** The priority of parameter "over_the_air.url" is lower than "over_the_air.url.w52h" and "over_the_air.url.w56h". If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Upgrade->Select and Upgrade Handset Firmware **Handset User Interface:** None		
over_the_air.url.w52h	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the W52H handset firmware file. **Example:** over_the_air.url.w52h = http://192.168.1.20/26.81.0.1.rom **Note:** The priority of parameter "over_the_air.url.w52h" is higher than "over_the_air.url". If you change this parameter, the DECT IP phone will reboot to make the change take effect.		

Parameters	Permitted Values	Default
Web User Interface: None **Handset User Interface:** None		
over_the_air.url.w56h	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the W56H handset firmware file. **Example:** over_the_air.url.w56h = http://192.168.1.20/61.81.0.30.rom **Note:** The priority of parameter "over_the_air.url.w56h" is higher than "over_the_air.url". If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** None **Handset User Interface:** None		
over_the_air.handset_tip	**0 or 1**	**1**
Description: Enables or disables to pop up a tip when upgrading the handset firmware from the provisioning server. **0-**Disabled **1-**Enabled If it is set to 1 (Enabled), the handset will pop up the message "Handset has a new firmware, update now?". **Note:** It works only if the value of the parameters "over_the_air.base_trigger" and "over_the_air.handset_trigger" are set to 0 (Disabled). **Web User Interface:** None **Handset User Interface:** None		
over_the_air.base_trigger	**0 or 1**	**1**
Description: Enables or disables to upgrade the handset firmware compulsively when the base detects a new handset firmware from the provisioning sever.		

Parameters	Permitted Values	Default
0-Disabled **1**-Enabled If it is set to 0 (Disabled) and the value of the parameter "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 the value of the parameter "over_the_air.handset_tip" is set to 0, you may go to **Settings**->**Upgrade Firmware** on handset to trigger the upgrading manually. If it is set to 1 (Enabled), it will upgrade the handset firmware compulsively without a pop-up tip on the handset. **Web User Interface:** None **Handset User Interface:** None		
over_the_air.handset_trigger	**0 or 1**	**1**
Description: Enables or disables to upgrade the handset firmware compulsively when the handset is registered to a base or turned on successfully. It is only applicable when the current handset firmware is different with the one on provisioning server. **0-**Disabled **1-**Enabled If it is set to 0 (Disabled) and the value of the parameter "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 the value of the parameter "over_the_air.handset_tip" is set to 0, you may go to **Settings**->**Upgrade Firmware** on handset to trigger the upgrading manually. If it is set to 1 (Enabled), it will upgrade the handset firmware compulsively without a pop-up tip on the handset. **Web User Interface:** None **Handset User Interface:** None		

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

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



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

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

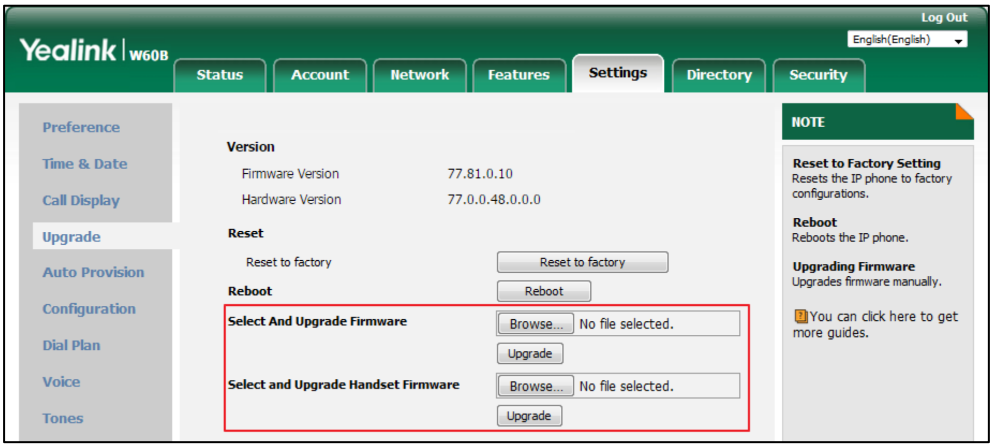
Upgrading Firmware via Web User Interface

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

To upgrade firmware manually via web user interface:

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

3. Click **Upgrade**.



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

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

Keeping User Personalized Settings after Auto Provisioning

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

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

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

Configuration Parameters

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

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

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

Parameters	Permitted Values	Default
Description: Configures the URL for uploading/downloading the <MAC>-local.cfg file. If it is left blank, the DECT IP phone will try to upload/download the <MAC>-local.cfg file to/from the root directory of provisioning server. **Note**: It works only if the value of the parameter "static.auto_provision.custom.sync" is set to 1 (Enabled). **Web User Interface:** None **Handset User Interface:** None		
static.auto_provision.custom.upload_method	**0 or 1**	**0**
Description: Configures the way the DECT IP phone uploads the <MAC>-local.cfg file to the provisioning server (for HTTP/HTTPS server only). **0**-PUT **1**-POST **Note**: It works only if the value of the parameter "static.auto_provision.custom.sync" is set to 1 (Enabled). **Web User Interface:** None **Handset User Interface:** None		
auto_provision.handset_configured.enable	**0 or 1**	**1**
Description: Enables or disables the handsets to keep user personalized settings after auto provisioning. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the base station will not deliver handset configurations via auto provisioning to the handset. The handset settings can be only changed via handset user interface. If it is set to 1 (Enabled), the base station will deliver the handset configurations via auto provisioning to the handset. Handset reboot or registration will also trigger the base station to deliver the stored handset settings to the handset. If the parameter		

Parameters	Permitted Values	Default
"static.auto_provision.custom.protect" is also set to 0 (Disabled), the personalized handset settings will be overridden, and other handset settings will be changed. If the parameter "static.auto_provision.custom.protect" is set to 1 (Enabled), the personalized handset settings will not be overridden, but other handset settings will be changed. **Web User Interface:** None **Handset User Interface:** None		

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

Scenario A Keep user personalized configuration settings

Keep user personalized configuration settings of the Base

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

For more information on the flowchart of keep user personalized configuration settings, refer to Appendix D: Auto Provisioning Flowchart (Keep User Personalized Configuration Settings) on page 473.

Note The parameters described in this scenario have been changed for the phones running firmware version 81 or later. For more information, refer to *Yealink DECT IP Phone Administrator Guide _V80*.

Scenario Conditions:

- W60B base station current firmware version: 77.81.0.1. This firmware supports keeping personalized settings and generating a <MAC>-local.cfg file.
- W60B base station target firmware version: 77.81.0.10. This firmware supports keeping personalized settings and generating a <MAC>-local.cfg file.
- W60B base station MAC: 001565770984
- Provisioning server URL: tftp://192.168.1.211
- Place the target firmware to the root directory of the provisioning server.

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

Do one of the following operations:

Scenario Operations I:

1. Edit the following parameters in the y000000000077.cfg file you want the DECT IP phone to download:

auto_provision.custom.protect = 1
auto_provision.custom.sync = 1
firmware.url = tftp://192.168.1.211/77.81.0.10.rom

2. Trigger the DECT IP phone to perform the auto provisioning process. For more information on how to trigger auto provisioning process, refer to *Triggering the DECT IP phone to Perform the Auto Provisioning* section in *Yealink SIP IP Phones Auto Provisioning Guide_V81*.

   During auto provisioning, the DECT IP phone first downloads the y000000000077.cfg file, and then downloads firmware from the root directory of the provisioning server.

   The DECT IP phone reboots to complete firmware upgrade, and then starts auto provisioning process again which is triggered by phone reboot (the power on mode is enabled by default). It downloads the y000000000077.cfg, 001565770984.cfg and the 001565770984-local.cfg file in sequence from the provisioning server, and then updates configurations in these downloaded configuration files orderly to the DECT IP phone system. The DECT IP phone starts up successfully, and the personalized settings in the 001565770984-local.cfg file are kept after auto provisioning.

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

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

Scenario Operations II:

1. Edit the following parameters in the y000000000077.cfg file you want the DECT IP phone to download:

   auto_provision.custom.protect = 1

   auto_provision.custom.sync = 0

   firmware.url = tftp://192.168.1.211/77.81.0.10.rom

2. Trigger the DECT IP phone to perform the auto provisioning process. For more information on how to trigger auto provisioning process, refer to *Triggering the DECT IP phone to Perform the Auto Provisioning* section in *Yealink SIP IP Phones Auto Provisioning Guide_V81*.

During auto provisioning, the DECT IP phone first downloads the y000000000077.cfg file, and then downloads firmware from the root directory of the provisioning server.

The DECT IP phone reboots to complete firmware upgrade, and then starts auto provisioning process again which is triggered by phone reboot (the power on mode is enabled by default). It downloads the y000000000077.cfg and 001565770984.cfg files in sequence, and then updates configurations in the downloaded configuration files orderly to the DECT IP phone system. As the value of the parameter "auto_provision.custom.protect" is set to 1, configurations in the 001565770984-local.cfg file saved on the DECT IP phone are also updated. The DECT IP phone starts up successfully, and personalized settings are kept after auto provisioning.

When a user customizes feature configurations via web/handset user interface, the DECT IP phone will save the personalized settings to the 001565770984-local.cfg file on the DECT IP phone only.

Note

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

If a configuration item is both in the <MAC>-local.cfg file on the IP phone and Common CFG file/MAC-Oriented CFG file downloaded from auto provisioning server, setting of the

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

Keep user personalized configuration settings of the Handset

The handset settings can be configured via handset user interface or auto provisioning. The personalized handset settings stand for the handset settings configured via handset user interface. The administrator wishes to change some handset settings via auto provisioning, but protect personalized handset settings after auto provisioning.

Scenario Conditions:

- The current firmware version of the W60B base station and W56H handset are 77.81.0.10 and 61.81.0.30 respectively. This firmware version supports protecting personalized handset settings after auto provisioning.
- Provisioning server URL: tftp://192.168.1.211.

To configure the handset settings via auto provisioning, you need to configure the value of the parameter "auto_provision.handset_configured.enable" to 1. To protect personalized handset settings after auto provisioning, you need to configure the value of the parameter "auto_provision.custom.protect" to 1.

Do the following operations:

1. Add/Edit the following parameters in the y000000000077.cfg file or 001565770984.cfg file

you want the DECT IP phone to download:

static.auto_provision.custom.protect = 1

auto_provision.handset_configured.enable = 1

2. Trigger the DECT IP phone to perform the auto provisioning process. For more information on how to trigger auto provisioning process, refer to *Yealink SIP IP Phones Auto Provisioning Guide_V81*.

During auto provisioning, the DECT IP phone will download the configuration files and update configurations in the configuration files. As the value of the parameter "auto_provision.handset_configured.enable" is set to 1, handset settings will be changed via auto provisioning. As the value of the parameter "static.auto_provision.custom.protect" is set to 1, the personalized handset settings will be remained after auto provisioning.

If value of the parameter "static.auto_provision.custom.protect" is set to be 0, and the value of the parameter "auto_provision.handset_configured.enable" is set to 1, the personalized handset settings will be overridden after auto provisioning. If the value of the parameter "auto_provision.handset_configured.enable" is set to 0, the handset settings cannot be changed via auto provisioning no matter what the value of the parameter "static.auto_provision.custom.protect" is.

Scenario B Clear user personalized configuration settings

Clear user personalized configuration settings of the Base

When the W60B base station is given to a new user but many personalized configurations settings of last user are saved on the phone; or when the end user encounters some problems because of the wrong configurations, the administrator or user may wish to clear user personalized configuration settings via phone/web user interface.

Scenario Conditions:

- W60B base station MAC: 001565770984
- The current firmware of the base station: 77.81.0.10 or later
- Provisioning server URL: tftp://192.168.1.211
- static.auto_provision.custom.protect = 1

Note

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

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

To reset the base station via handset user interface:

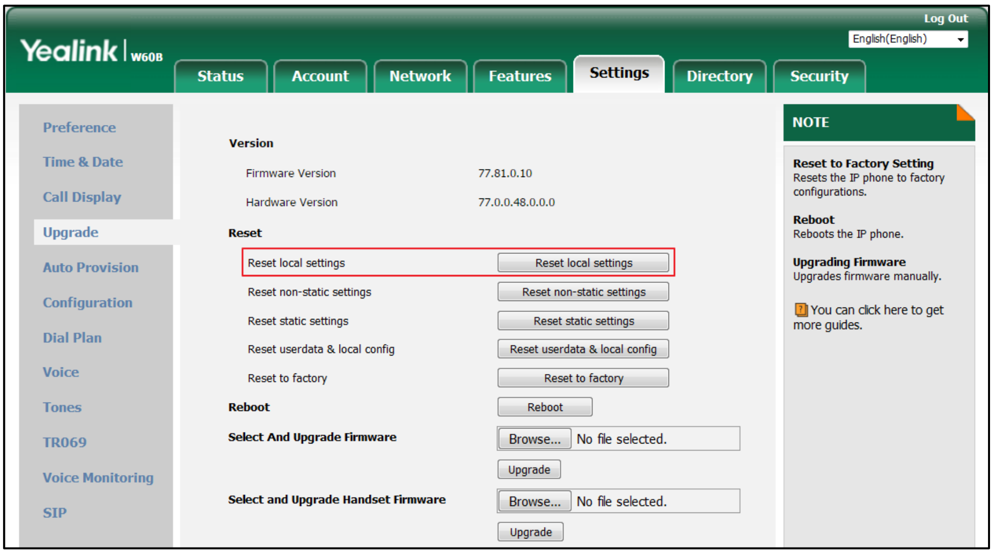
1. Press **OK** to enter the main menu.

2. Select **Settings**->**System Settings**.
3. Select **Base Reset**, and then press the **OK** soft key.
4. Enter the base PIN (default: 0000), and then press the **OK** soft key.
5. Select **Reset local**, and then press the **OK** soft key.

   The LCD screen prompts “Reset base local configuration now?”
6. Press the **Yes** soft key.

To clear personalized configuration settings via web user interface:

1. Click on **Settings**->**Upgrade**.
2. Click Reset local settings.



The web user interface prompts “Clear local.cfg settings?”.

3. Click **OK**.

Configurations in the 001565770984-local.cfg file saved on the phone will be cleared. If the DECT IP phone is triggered to perform auto provisioning after resetting local configuration, it will download the configuration files from the provisioning server and update the configurations to the phone system. As there is no configuration in the 001565770984-local.cfg file, configurations in the y000000000077.cfg/001565770984.cfg file will take effect. If there are no configuration files on the provisioning server, the DECT IP phone will be reset to factory defaults.

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

Clear user personalized configuration settings of the Handset

The administrator or user wishes to clear personalized settings of the specified handset.

Scenario Conditions:

- The handset 1 was registered to the base station.

Note You can only clear the personalized settings of the handset via handset user interface.

Scenario Operations:

To clear personalized settings of the handset:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**System Settings**.
3. Select **Handset Reset**, and then press the **OK** soft key.

   The LCD screen prompts "Reset handset to default?".
4. Press the **Yes** soft key.

Note If the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled), the handset settings (configured via auto provisioning) stored on the base station will be delivered to the handset after handset reset. If the value of this parameter is set to 0 (Disabled), the handset settings will not be delivered to the handset after handset reset.

Scenario C Keep user personalized settings after factory reset

The W60B base station requires factory reset when it has a breakdown, but the user wishes to keep personalized settings of the phone after factory reset.

Scenario Conditions:

- W60B base station MAC: 001565770984
- Provisioning server URL: tftp://192.168.1.211
- static.auto_provision.custom.sync = 1

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

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

To reset the phone to factory via handset user interface:

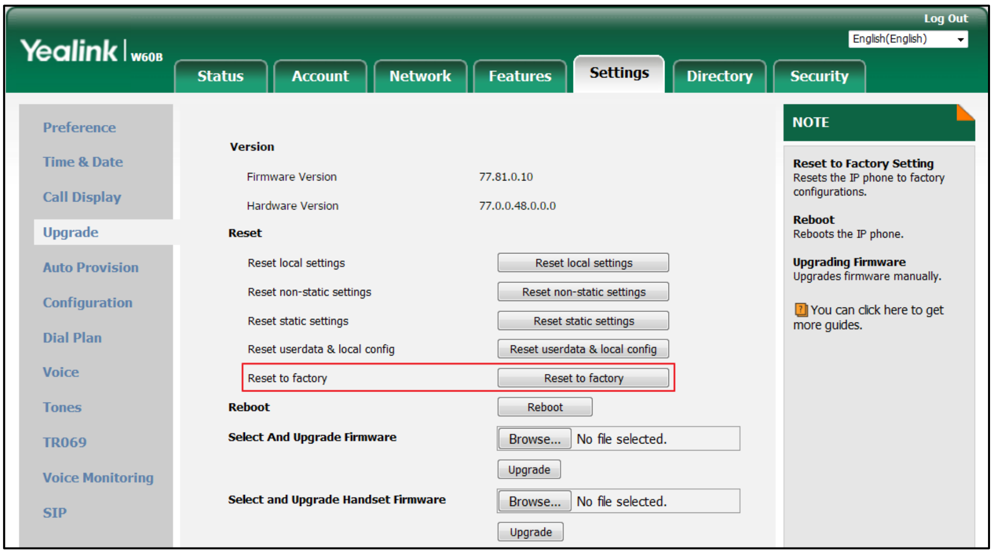
1. Press **OK** to enter the main menu.
2. Select **Settings**->**System Settings**.
3. Select **Base Reset**, and then press the **OK** soft key.
4. Enter the system PIN (default: 0000), and then press the **Done** soft key.
5. Select **Reset to factory**, and then press the **OK** soft key.

The LCD screen prompts "Reset base to factory configuration now?".

6. Press the **Yes** soft key.

To reset the phone to factory via web user interface:

1. Click on **Settings**->**Upgrade**.
2. Click **Reset to factory** to reset the phone.



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

3. Click **OK**.

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

To retrieve personalized settings of the phone after factory reset:

1. Set the values of the parameters "static.auto_provision.custom.sync" and "static.auto_provision.custom.protect" to be 1 in the configuration file (y000000000077.cfg or 001565770984.cfg).
2. Trigger the phone to perform the auto provisioning process.

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

Scenario D Import or export the local configuration file

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

Scenario Conditions:

- W60B base station MAC: 001565770984
- The current firmware of the base station: 77.81.0.10 or later
- Provisioning server URL: tftp://192.168.1.211

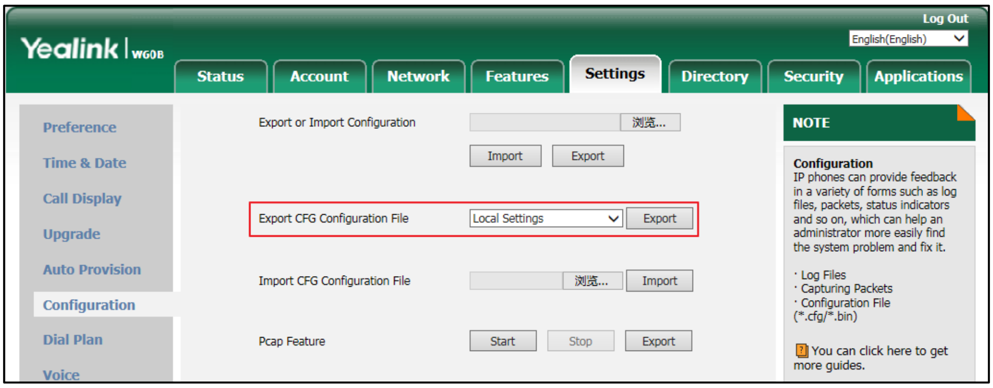
Note

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

Scenario Operations:

To export local configuration file via web user interface:

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

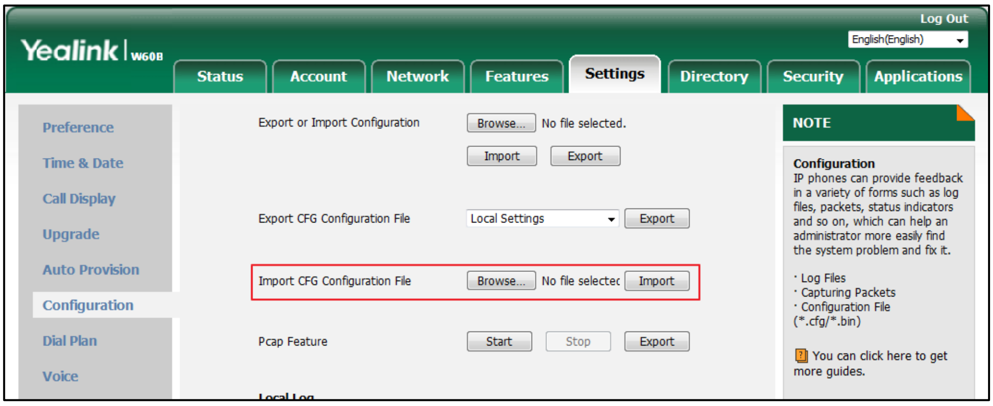


The administrator or user can edit the 001565770984-local.cfg file after exporting.

To import local configuration file via web user interface:

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

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



3. Click **Import**.

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

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

Configuring the Handset

Power Indicator LED for W56H Handset

Handset power indicator LED indicates power status and phone status. It is only applicable to W56H handset.

There are four configuration options for handset power indicator LED.

Common Power Light On

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

Ringing Power Light Flash

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

Voice/Text Mail Power Light Flash

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

MissCall Power Light Flash

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

Procedure

Power indicator LED can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the handset power indicator LED. **Parameters:** phone_setting.common_power_led_enable phone_setting.ring_power_led_flash_enable phone_setting.mail_power_led_flash_enable phone_setting.missed_call_power_led_flash.enable
Web User Interface		Configure the handset power indicator LED.

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

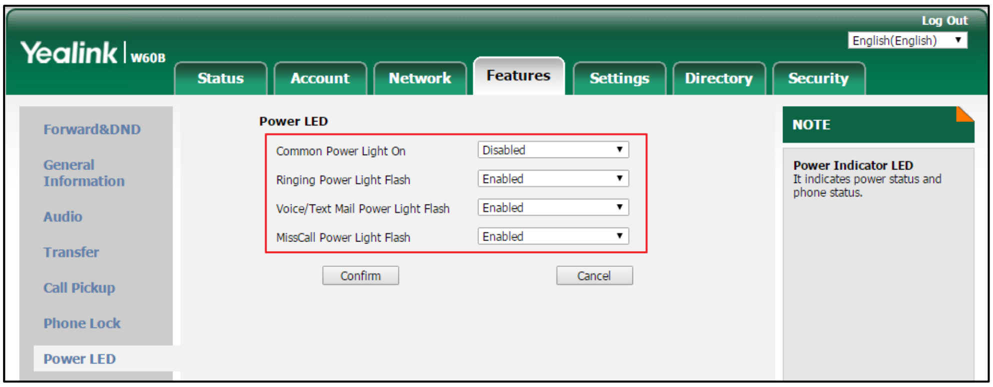
Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.common_power_led_enable	**0 or 1**	**0**
Description: Enables or disables the handset power indicator LED to be turned on when the handset is idle. **0**-Disabled (handset power indicator LED is off) **1**-Enabled (handset power indicator LED is solid red) **Note:** It is not applicable to W52H handset. **Web User Interface:** Features->Power LED->Common Power Light On **Handset User Interface:** None		
phone_setting.ring_power_led_flash_enable	**0 or 1**	**1**
Description: Enables or disables the handset power indicator LED to flash when the handset receives an incoming call. **0**-Disabled (handset power indicator LED does not flash) **1**-Enabled (handset power indicator LED fast flashes (300ms) red) **Note:** It is not applicable to W52H handset. **Web User Interface:** Features->Power LED->Ringing Power Light Flash **Handset User Interface:** None		
phone_setting.mail_power_led_flash_enable	**0 or 1**	**1**
Description: Enables or disables the handset power indicator LED to flash when the handset receives a voice mail. **0**-Disabled (handset power indicator LED does not flash) **1**-Enabled (handset power indicator LED slow flashes (1000ms) red)		

Parameters	Permitted Values	Default
Note: It is not applicable to W52H handset. **Web User Interface:** Features->Power LED->Voice/Text Mail Power Light Flash **Handset User Interface:** None		
phone_setting.missed_call_power_led_flash.enable	**0 or 1**	**1**
Description: Enables or disables the handset power indicator LED to flash when the handset misses a call. **0**-Disabled (handset power indicator LED does not flash) **1**-Enabled (handset power indicator LED slow flashes (1000ms) red) **Note:** It is not applicable to W52H handset. **Web User Interface:** Features->Power LED->MissCall Power Light Flash **Handset User Interface:** None		

To configure the power Indicator LED via web user interface:

1. Click on **Features**->**Power LED**.
2. Select the desired value from the pull-down list of **Common Power Light On**.
3. Select the desired value from the pull-down list of **Ringing Power Light Flash.**
4. Select the desired value from the pull-down list of **Voice/Text Mail Power Light Flash**.
5. Select the desired value from the pull-down list of **MissCall Power Light Flash**.



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

Keypad Light

You can enable the keypad light to make the keypad light up when any key is pressed. This helps you distinguish keys from each other in a dark environment. It is only applicable to W56H handset.

Procedure

The keypad's light of handset can be configured using the following methods.

Configuration File	y000000000077.cfg	Configure the keypad light. **Parameter:** custom.handset.keypad_light.enable
Handset User Interface		Configure the keypad light.

Details of Configuration Parameter:

Parameter	Permitted Values	Default
custom.handset.keypad_light.enable	**0 or 1**	**1**
Description: 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. **0**-Disabled **1**-Enabled **Note:** It will take effect on all handsets that are registered on the same base station. It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled). It is not applicable to W52H handset. **Web User Interface:** None **Handset User Interface:** OK->Settings->Display->Keypad LED		

To configure keypad light via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Display**->**Keypad LED**.
3. Press the **Change** soft key to check or uncheck the **Keypad LED** checkbox.

Notification Light for W52H Handset

Notification light is used to indicate voice mails and missed calls. When the handset receives a voice mail or misses a call, the message key LED will flash red. You can configure the notification light to indicate the voice mails or missed calls respectively. It is only applicable to W52H handset.

Voice Mail Light Flash

Voice Mail Light Flash allows the message key LED to flash when the registered handset receives a voice mail.

Miss Call Light Flash

Miss Call Light flash allows the message key LED to flash when the registered handset misses a call.

Procedure

The notification light of handset can be configured using the following methods.

Configuration File	y000000000077.cfg	Configure the light when receiving a voice mail on the handset. **Parameter:** custom.handset.voice_mail_notify_light.enable
		Configure the light when missing a call on the handset. **Parameter:** custom.handset.missed_call_notify_light.enable
Handset User Interface		Configure the notification light on handset.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
custom.handset.voice_mail_notify_light.enable	**0 or 1**	**1**
Description: Enables or disables the message key LED to flash when the handset receives a voice mail. **0**-Disabled **1**-Enabled		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Note: It will take effect on all handsets that are registered on the same base station. It works only if the value of the parameter “auto_provision.handset_configured.enable” is set to 1 (Enabled).
Note: It is not applicable to W56H handset.
Web User Interface:
None
handset User Interface:
OK->Settings->Display->Notification LED->Voice Mail</td></tr>
<tr><td>custom.handset.missed_call_notify_light.enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables the message key LED to flash red when the handset misses a call.
0-Disabled
1-Enabled
Note: It will take effect on all handsets that are registered on the same base station. It works only if the value of the parameter “auto_provision.handset_configured.enable” is set to 1 (Enabled).
Note: It is not applicable to W56H handset.
Web User Interface:
None
handset User Interface:
OK->Settings->Display->Notification LED->Missed Call</td></tr>
</table>

To configure notification light via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Display**->**Notification LED**.
3. Press ◀ or ▶ to select the desired value from the **Voice Mail** field.
4. Press ◀ or ▶ to select the desired value from the **Missed Call** field.
5. Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

Advisory Tone

Advisory tones are acoustic signals of your handset, which inform you of different actions and states. The following advisory tones can be configured independently of each other:

- **Keypad Tone**: plays when a user presses any key of the keypad.

- **Confirmation**: plays when a user saves settings or places the handset in the charger cradle.
- **Low Battery**: plays when the capacity of the batteries is low and the handset requires charging.

Procedure

Advisory tone can be configured using the following methods.

Configuration File	y000000000077.cfg	Configure keypad's tone on the handset. **Parameter:** custom.handset.keypad_tone.enable
		Configure confirmation's tone on the handset. **Parameter:** custom.handset.confirmation_tone.enable
		Configure low battery tone on the handset. **Parameter:** custom.handset.low_battery_tone.enable
Handset User Interface		Configure keypad's tone on the handset. Configure confirmation's tone on the handset. Configure low battery tone on the handset.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
custom.handset.keypad_tone.enable	**0 or 1**	**1**
Description: Enables or disables the handset to play a tone when any key is pressed. **0**-Disabled **1**-Enabled		

Parameters	Permitted Values	Default
Note: It will take effect on all handsets that are registered on the same base station. It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled) and the silent mode is off. **Web User Interface:** None **Handset User Interface:** OK->Settings->Audio->Advisory Tones->Keypad Tone		
custom.handset.confirmation_tone.enable	**0 or 1**	**1**
Description: Enables or disables the handset to play a tone when a user saves settings or places the handset in the charger cradle. **0**-Disabled **1**-Enabled **Note:** It will take effect on all handsets that are registered on the same base station. It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled) and the silent mode is off. **Web User Interface:** None **Handset User Interface:** OK->Settings->Audio->Advisory Tones->Confirmation		
custom.handset.low_battery_tone.enable	**0 or 1**	**1**
Description: Enables or disables the handset to play a tone when the capacity of battery is low. **0**-Disabled **1**-Enabled **Note:** It will take effect on all handsets that are registered on the same base station. It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled) and the silent mode is off. **Web User Interface:** None **Handset User Interface:** OK->Settings->Audio->Advisory Tones->Low Battery		

To configure advisory tone via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Audio**->**Advisory Tones**.
3. Press ◀ or ▶ to select the desired value from the **Keypad Tone** field.
4. Press ◀ or ▶ to select the desired value from the **Confirmation** field.
5. Press ◀ or ▶ to select the desired value from the **Low Battery** field.
6. Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

Backlight

Handset backlight status in the charging state or out of the charging state can be configured independently of each other. If enabled, the backlight is always on. Otherwise, the backlight is turned off after the handset is idle for a period of time. But the backlight is automatically turned on when an incoming call arrives, a key is pressed or the status of handset changes. You can disable the backlight to save power.

Procedure

Backlight can be configured using the following methods.

Configuration File	y000000000077.cfg	Configure the backlight of the handset LCD screen. **Parameters:** custom.handset.backlight_in_charger.enable custom.handset.backlight_out_of_charger.enable
Handset User Interface		Configure the backlight of the handset LCD screen.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
custom.handset.backlight_in_charger.enable	**0 or 1**	**1**
Description: Enables or disables the handset to always turn on the backlight when it is in the charging state. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the backlight will be turned off after the handset is idle for a period of time when it is in the charging state.		

Note: It will take effect on all handsets that are registered on the same base station. It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled). **Web User Interface:** None **Handset User Interface:** OK->Settings->Display->Display Backlight->In Charger		
custom.handset.backlight_out_of_charger.enable	**0 or 1**	**0**
Description: Enables or disables the handset to always turn on the backlight when it is not in the charging state. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the backlight will be turned off after the handset is idle for a period of time when it is not in the charging state. **Note**: It will take effect on all handsets that are registered on the same base station. It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled). **Web User Interface:** None **Handset User Interface:** OK->Settings->Display->Display Backlight->Out Of Charger		

To configure the backlight via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Display**->**Display Backlight**.
3. Press ◀ or ▶ to select the desired value from the **In Charger** field.
4. Press ◀ or ▶ to select the desired value from the **Out Of Charger** field.
5. Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

Wallpaper for W56H Handset

Wallpaper is an image used as the background of the handset idle screen. Users can select an image from handset's built-in background. It is only applicable to W56H handset.

Procedure

Wallpaper can be configured using the following methods.

Configuratio	y000000000077.cfg	Configure the wallpaper displayed on

n File		the handset LCD screen. **Parameter:** custom.handset.wallpaper
Handset User Interface		Configure the wallpaper displayed on the handset LCD screen.

Details of Configuration Parameters:

Parameter	Permitted Values	Default
custom.handset.wallpaper	**Integer from 1 to 8**	**1**
Description: Configures the wallpaper displayed on the handset LCD screen. **1**-Wallpaper1 **2**-Wallpaper2 **3**-Wallpaper3 **4**-Wallpaper4 **5**-Wallpaper5 **Note**: It will take effect on all handsets that are registered on the same base station. It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled). It is not applicable to W52H handset. **Web User Interface:** None **Handset User Interface:** OK->Settings->Display->Wallpaper		

To change the wallpaper via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Display**->**Wallpaper**.
3. Press ◀ or ▶ to select the desired image.
4. Press the **Save** soft key to accept the change.

   The handset displays the corresponding wallpaper on the idle screen.

Screen Saver

The screen saver of the handset is designed to protect your LCD screen by filling it with an analog clock. You can enable the screen saver to protect the LCD screen if you do not use your handset for a long time. When the screen saver is enabled, an analog clock will be activated and appear on the LCD screen if the handset is idle for approximately 10 seconds.

Procedure

Screen saver can be configured using the following methods.

Configuration File	y000000000077.cfg	Configure the screensaver of the handset LCD screen. **Parameter:** custom.handset.screen_saver.enable
Handset User Interface		Configure the screen saver of the handset LCD screen.

Details of Configuration Parameters:

Parameter	Permitted Values	Default
custom.handset.screen_saver.enable	**0 or 1**	**1**
Description: Enables or disables screen saver feature. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), an analog clock will be activated and appear on the LCD screen if no user activity is sensed for approximately 10 seconds. **Note:** It will take effect on all handsets that are registered on the same base station. It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled). **Web User Interface:** None **Handset User Interface:** OK->Settings->Display->Screen Saver		

To configure screen saver via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Display**->**Screen Saver**.
3. Press the **Change** soft key to check or uncheck the **Screen Saver** checkbox.

Color Scheme for W52H Handset

You can change the background of your handset by changing the color theme. There are 2 color themes available. It is only applicable to W52H handset.

Procedure

Color scheme can be configured using the following methods.

Configuration File	y000000000077.cfg	Configure the screen scheme of the LCD screen. **Parameter:** custom.handset.color_scheme
Handset User Interface		Configure the screen scheme of the LCD screen.

Details of Configuration Parameters:

Parameter	Permitted Values	Default
custom.handset.color_scheme	**0 or 1**	**1**
Description: Configures the color scheme of the handset. **0**-Color scheme 1 **1**-Color scheme 2 **Note:** It will take effect on all handsets that are registered on the same base station. It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled). It is not applicable to W56H handset. **Web User Interface:** None **Handset User Interface:** OK->Settings->Display->Color Schemes		

To change color scheme via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Display**->**Color Schemes**.
3. Press ▲ or ▼ to highlight the desired color scheme and preview its effect.
4. Press the **Select** soft key to mark the radio box of the highlighted color theme.

   The color theme of the handset is changed accordingly.

Handset Name

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

Procedure

Handset name can be configured using the following methods.

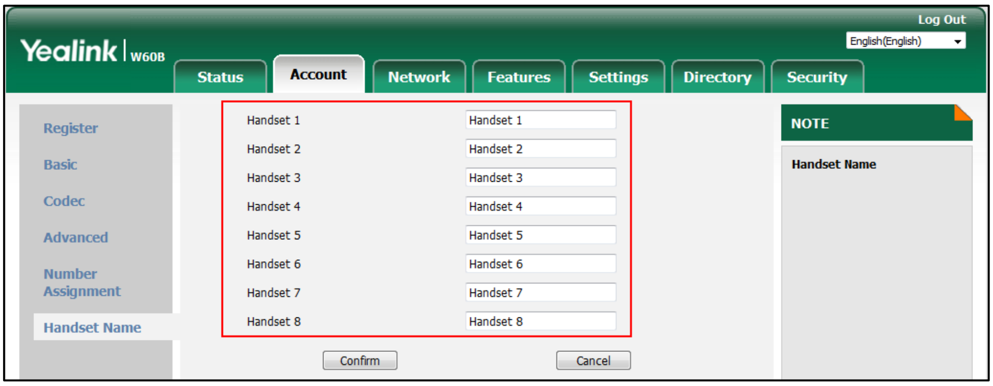
<table>
<tr><td>Configuration File</td><td>y000000000077.cfg</td><td>Configure the handset name.
Parameter:
handset.X.name</td></tr>
<tr><td colspan="2">Web User Interface</td><td>Configure the handset name.
Navigate to:
http://<phoneIPAddress>/servlet?p=account-handsetname&q=load</td></tr>
<tr><td colspan="2">Handset User Interface</td><td>Configure the handset name.</td></tr>
</table>

Details of Configuration Parameters:

<table>
<tr><th>Parameter</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>handset.X.name
(X ranges from 1 to 8)</td><td>String within 24 characters</td><td>Refer to the following content</td></tr>
<tr><td colspan="3">Description:
Configures the name of handset X.
It will be displayed on the handset LCD screen.
Default:
The handset name for handset 1 is Handset 1.
The handset name for handset 2 is Handset 2.
The handset name for handset 3 is Handset 3.
The handset name for handset 4 is Handset 4.
The handset name for handset 5 is Handset 5.
The handset name for handset 6 is Handset 6.
The handset name for handset 7 is Handset 7.
The handset name for handset 8 is Handset 8.
Note: If it is set to blank, it will display the corresponding default handset name.
Web User Interface:
Account->Handset Name->Handset X (X ranges from 1 to 8)
Handset User Interface:
OK->Settings->Handset Name</td></tr>
</table>

To rename the handset via web user interface:

1. Click on **Account**->**Handset Name**.
2. Edit the current name in the **Handset X** (X ranges from 1 to 8) field.



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

To rename the handset via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Handset Name**.
3. Edit the current name in the **Rename** field.

   You can press to enter special characters and then press to switch among input modes.
4. Press the **Save** soft key to accept the change or to cancel.

Language

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

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

Handset	Web User Interface
English	English
French	French
German	German
Italian	Italian
Polish	Polish
Portuguese	Portuguese
Spanish	Spanish
Turkish	Turkish

Handset	Web User Interface
Czech (only for W52H) Swedish Hebrew (only for W52H) Russian	Russian

Loading Language Packs

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

You can ask the distributor or Yealink FAE for language packs. You can also obtain the language packs online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the language packs, refer to Obtaining Boot Files/Configuration Files/Resource Files on page 89.

Note

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

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

Customizing a Language for Web User Interface

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

Available Language	Associated Language Pack	Associated Note Language Pack
English	1.English.js	1.English_note.xml
French	2.French.js	4.French_note.xml
German	3.German.js	5.German_note.xml
Italian	4.Italian.js	6.Italian_note.xml
Polish	5.Polish.js	7.Polish_note.xml
Portuguese	6.Portuguese.js	8.Portuguese_note.xml
Spanish	7.Spanish.js	9.Spanish_note.xml
Turkish	8.Turkish.js	10.Turkish_note.xml

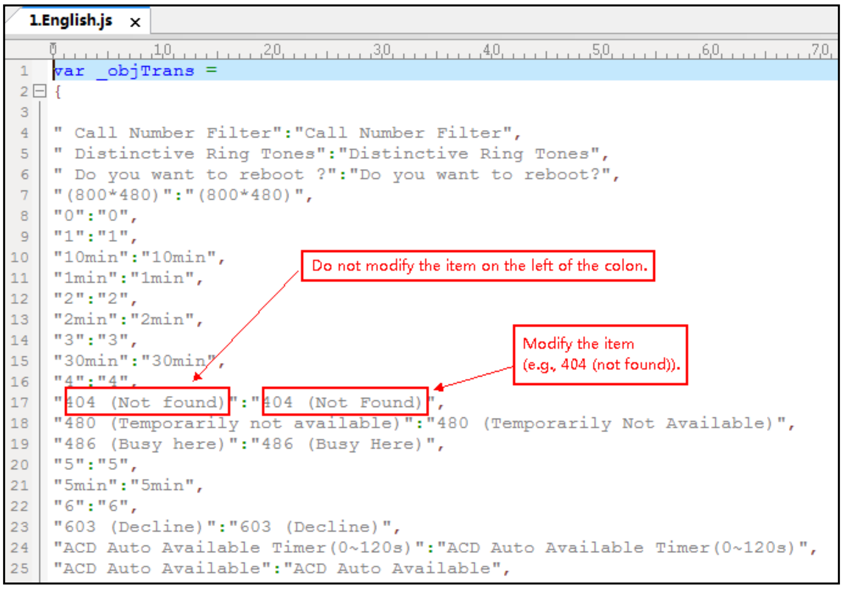
Available Language	Associated Language Pack	Associated Note Language Pack
Russian	9.Russian.js	11.Russian_note.xml

When adding a new language pack for the web user interface, the language pack must be formatted as "Y.name.js" (Y starts from 10, "name" is replaced with the language name). If the language name is the same as the existing one, the existing language file will be overridden by the new uploaded one. We recommend that the name of the new language file should not be the same as the existing languages.

To customize a language file:

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

   The following shows a portion of the language pack "1.English.js" for the web user interface:

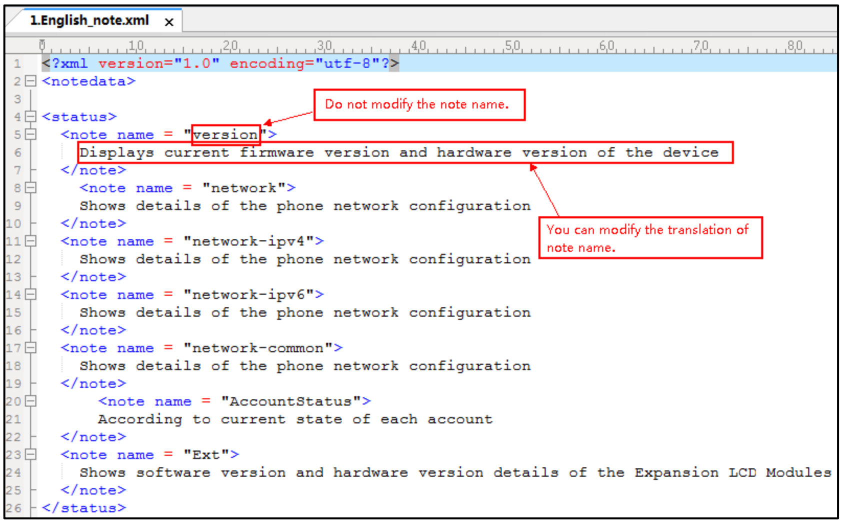


3. Save the language file and place it to the provisioning server (e.g., 192.168.10.25).
4. Specify the access URL of the web user interface language pack in the configuration files.

To customize a note language file:

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

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




```
<?xml version="1.0" encoding="utf-8"?>
<notedata>

<status>
  <note name = "version">
    Displays current firmware version and hardware version of the device
  </note>
    <note name = "network">
    Shows details of the phone network configuration
  </note>
  <note name = "network-ipv4">
    Shows details of the phone network configuration
  </note>
  <note name = "network-ipv6">
    Shows details of the phone network configuration
  </note>
  <note name = "network-common">
    Shows details of the phone network configuration
  </note>
      <note name = "AccountStatus">
      According to current state of each account
  </note>
  <note name = "Ext">
    Shows software version and hardware version details of the Expansion LCD Modules
  </note>
</status>
```

3. Save the language file and place it to the provisioning server (e.g., 192.168.10.25).

4. Specify the access URL of the note language pack of the web user interface.

If you want to add a new language (e.g., Wuilan) to DECT IP phones, prepare the language file named as “12.Wuilan.js” and “12.Wuilan_note.xml” for downloading. After update, you will find a new language selection “Wuilan” in the pull-down list of language, and new note information is displayed in the icon when the new language is selected.

Procedure

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

Configuration File	y000000000077.cfg	Specify the access URL of the custom language pack for web user interface. **Parameter:** wui_lang.url
		Delete custom language packs of the web user interface. **Parameter:** wui_lang.delete
		Specify the access URL of the custom note language pack for web user interface. **Parameter:** wui_lang_note.url

Details of the Configuration Parameter:

Parameters	Permitted Values	Default
wui_lang.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom language pack for the web user interface. **Example:** wui_lang.url = http://192.168.10.25/1.English.js During the auto provisioning process, the DECT IP phone connects to the HTTP provisioning server "192.168.10.25", and downloads the language pack "1.English.js". The English language translation will be changed accordingly if you have modified the language template file. If you want to download multiple language packs to the web user interface simultaneously, you can configure as following: wui_lang.url = http://192.168.10.25/1.English.js wui_lang.url = http://192.168.10.25/9.Russian.js **Web User Interface:** None **Handset User Interface:** None		
wui_lang.delete	**http://localhost/all or http://localhost/*Y.name.js***	**Blank**
Description: Delete the specified or all custom web language packs of the web user interface. **Example:** Delete all custom language packs of the web user interface: wui_lang.delete = http://localhost/all Delete a custom language pack of the web user interface (e.g., 9.Russian.js): wui_lang.delete = http://localhost/9.Russian.js **Web User Interface:** None **Handset User Interface:** None		
wui_lang_note.url	**URL within 511 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the access URL of the custom note language pack for web user interface. **Example:** wui_lang_note.url = http://192.168.10.25/1.English_note.xml During the auto provisioning process, the DECT IP phone connects to the HTTP provisioning server "192.168.10.25", and downloads the note language pack "1.English_note.xml". The English language translation will be changed accordingly if you have modified the language template file. If you want to download multiple language packs to the phone simultaneously, you can configure as following: wui_lang.url = http://192.168.10.25/1.English_note.xml wui_lang.url = http://192.168.10.25/11.Russian_note.xml **Web User Interface:** None **Handset User Interface:** None		

Specifying the Language to Use

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

Procedure

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

Configuration File	y000000000077.cfg	Specify the languages for the web user interface. **Parameter:** lang.wui
		Specify the language for the handset user interface. **Parameter:** custom.handset.language

Web User Interface	Specify the language for the web user interface.
Handset User Interface	Specify the language for the handset user interface.

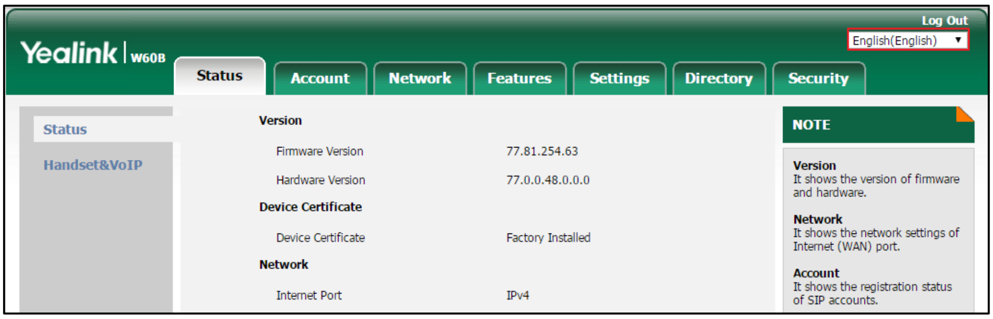
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.lang.wui	**Refer to the following content**	**English**
Description: Configures the language used on the web user interface. **Permitted Values:** English, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian or the custom language name. **Example:** static.lang.wui = English If you want to use the custom language (e.g., Wuilan) for the DECT IP phone, configure the parameter "lang.wui = Wuilan". **Note:** If the language of your browser is not supported by the DECT IP phone, the web user interface will use English by default. **Web User Interface:** Settings->Preference->Language **Handset User Interface:** None		
custom.handset.language	**Refer to the following content**	**0**
Description: Configures the language of the handset. **For W56H handset:** **0**-English **1**-French **2**-German **3**-Italian **4**-Polish **5**-Portuguese **6**-Spanish **7**-Turkish		

Parameters	Permitted Values	Default
8-Swedish **9**-Russian **For W52H handset:** **0**-English **1**-French **2**-German **3**-Italian **4**-Polish **5**-Portuguese **6**-Spanish **7**-Turkish **8**-Czech **9**-Swedish **10**-Hebrew **11**-Russian **Note:** It will take effect on all handsets that are registered on the same base station. It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled). **Web User Interface:** None **Handset User Interface:** OK->Settings->Language		

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

1. Select the desired language from the pull-down list of **Language**.



Text displayed on the web will change to the selected language.

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

1. Press **OK** to enter the main menu.

2. Select **Settings**->**Language**.
3. Press ▲ or ▼ to highlight the desired language and then press the **Select** soft key.

   The LCD screen prompts "Change phone language to xxx?" (xxx is the language you selected).
4. Press the **Yes** soft key to accept the change.

   Text displayed on the handset will change to the selected language.

Configuring Basic Features

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

- Register Power Light Flash
- Account Registration
- Number of Active Handsets
- Number of Simultaneous Outgoing Calls
- Call Display
- Number Assignment
- Display Method on Dialing
- Time and Date
- Input Method
- Key As Send
- Dial Plan
- Emergency Dialplan
- Off Hook Hot Line Dialing
- Local Directory
- Search Source List In Dialing
- Save Call Log
- Call Waiting
- Auto Answer
- Allow IP Call
- Accept SIP Trust Server Only
- Anonymous Call
- Anonymous Call Rejection
- Do Not Disturb (DND)
- Busy Tone Delay
- Return Code When Refuse
- Early Media
- 180 Ring Workaround
- Use Outbound Proxy in Dialog
- SIP Session Timer

- Session Timer
- Call Hold
- Call Forward
- Call Transfer
- Network Conference
- Feature Key Synchronization
- Recent Call In Dialing
- Call Number Filter
- Call Park
- Calling Line Identification Presentation (CLIP)
- Connected Line Identification Presentation (COLP)
- Intercom
- Call Timeout
- Ringing Timeout
- Send user=phone
- SIP Send MAC
- SIP Send Line
- Reserve # in User Name
- Unregister When Reboot
- 100 Reliable Retransmission
- Reboot in Talking
- Quick Login
- End Call on Hook

Register Power Light Flash

Register Power Light Flash allows the base power indicator LED to flash when registering an account successfully.

Procedure

The register power light flash can be configured using the following method.

Configuration File	y000000000077.cfg	Configure the register power light flash. **Parameter:** features.registered_power_led_flash.enable

Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.registered_power_led_flash.enable	**0 or 1**	**0**
Description: Enables or disables the base power indicator LED to flash when registering an account successfully. **0**-Disabled (base power indicator LED does not flash) **1**-Enabled (base power indicator LED slow flashes (1000ms) green) **Web User Interface:** None **Handset User Interface:** None		

Account Registration

Registering a SIP account makes it easier for the DECT IP phones to receive an incoming call or dial an outgoing call. Yealink DECT IP phones support registering 8 accounts on a DECT phone; each account requires an extension or phone number.

The DECT IP phones support SIP server redundancy for account registration. For more information, refer to Server Redundancy on page 327.

Procedure

Account registration can be configured using the following methods.

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

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.enable (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Enables or disables the account X. **0**-Disabled **1**-Enabled **Web User Interface:** Account->Register->Line Active **Handset User Interface:** None		
account.X.label (X ranges from 1 to 8)	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label to be displayed on the LCD screen for account X. **Web User Interface:** Account->Register->Label **Handset User Interface:** None		
account.X.display_name (X ranges from 1 to 8)	**String within 99 characters**	**Blank**
Description: Configures the display name to be displayed on the called party's LCD screen for account X. **Web User Interface:** Account->Register->Display Name **Handset User Interface:** None		
account.X.auth_name (X ranges from 1 to 8)	**String within 99 characters**	**Blank**
Description: Configures the user name for register authentication for account X. **Note**: The user name for register authentication is provided by ITSP. It is always matched		

Parameters	Permitted Values	Default
with a password (configured by the parameter "account.X.password") used for register authentication, if required by the server. **Web User Interface:** Account->Register->Register Name **Handset User Interface:** None		
account.X.user_name (X ranges from 1 to 8)	**String within 99 characters**	**Blank**
Description: Configures the register user name for account X. **Note**: The register user name is provided by ITSP. It is used to identify the account. **Web User Interface:** Account->Register->User Name **Handset User Interface:** None		
account.X.password (X ranges from 1 to 8)	**String within 99 characters**	**Blank**
Description: Configures the password for register authentication for account X. **Note**: The password for register authentication is provided by ITSP. **Web User Interface:** Account->Register->Password **Handset User Interface:** None		
account.X.sip_server.Y.address (X ranges from 1 to 8, Y ranges from 1 to 2)	**String within 256 characters**	**Blank**
Description: Configures the IP address or domain name of the SIP server Y that accepts registrations for account X. **Example:** account.1.sip_server.1.address = 10.2.1.48 **Web User Interface:** Account->Register->SIP Server Y->Server Host		

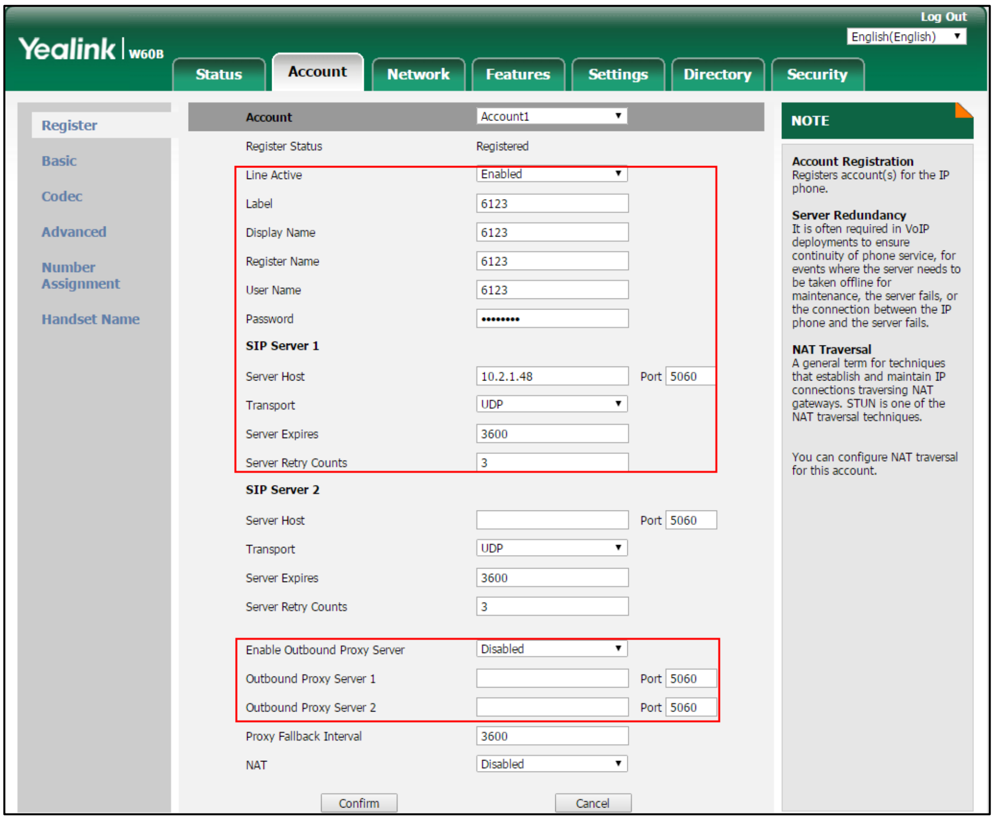
Parameters	Permitted Values	Default
Handset User Interface: None		
account.X.sip_server.Y.port (X ranges from 1 to 8, Y ranges from 1 to 2)	**Integer from 0 to 65535**	**5060**
Description: Configures the port of the SIP server Y that specifies registrations for account X. **Example:** account.1.sip_server.1.port = 5060 **Note**: If the value of this parameter is set to 0, the port used depends on the value specified by the parameter "account.X.sip_server.Y.transport_type". **Web User Interface:** Account->Register->SIP Server Y->Port **Handset User Interface:** OK->Settings->Telephony->Server (default PIN: 0000) ->Server Y (Account X) ->Port		
account.X.outbound_proxy_enable (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to send requests to the outbound proxy server for account X. **0**-Disabled **1**-Enabled **Web User Interface:** Account->Register->Enable Outbound Proxy Server **Handset User Interface:** OK->Settings->Telephony->Server (default PIN: 0000) ->Outbound Proxy (Account X) ->Outbound Proxy Server		
account.X.outbound_proxy.Y.address (X ranges from 1 to 8, Y ranges from 1 to 2)	**IP address or domain name**	**Blank**
Description: Configures the IP address or domain name of the outbound proxy server Y for account X. **Example:** account.1.outbound_proxy.1.address = 10.1.8.11 **Note:** It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled).		

Parameters	Permitted Values	Default
Web User Interface: Account->Register->Outbound Proxy Server Y **Handset User Interface:** None		
account.X.outbound_proxy.Y.port (X ranges from 1 to 8, Y ranges from 1 to 2)	**Integer from 0 to 65535**	**5060**
Description: Configures the port of the outbound proxy server Y for account X. **Example:** account.1.outbound_proxy.1.port = 5060 **Note:** It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled). **Web User Interface:** Account->Register->Outbound Proxy Server Y->Port **Handset User Interface:** OK->Settings->Telephony->Server (default PIN: 0000) ->Outbound Proxy (Account X) ->Port (only applicable to port 1)		
account.X.reg_fail_retry_interval (X ranges from 1 to 8)	**Integer from 0 to 1800**	**30**
Description: Configures the interval (in seconds) for the DECT IP phone to retry to re-register account X when registration fails. **Example:** account.1.reg_fail_retry_interval = 30 **Note**: It works only if the values of the parameters "account.X.reg_failed_retry_min_time" and "account.X.reg_failed_retry_max_time" are set to 0. **Web User Interface:** Account->Advanced->SIP Registration Retry Timer(0~1800s) **Handset User Interface:** None		

To register an account via web user interface:

1. Click **Account**->**Register**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **Enabled** from the pull-down list of **Line Active**.

4. Enter the desired value in **Label**, **Display Name**, **Register Name**, **User Name**, **Password** and **SIP Server1/2** field respectively.
5. If you use outbound proxy servers, do the following:
   1) Select **Enabled** from the pull-down list of **Enable Outbound Proxy Server**.
   2) Enter the desired IP address or domain name in the **Outbound Proxy Server 1/2** field and the desired port of the outbound proxy server 1/2 in the **Port** field respectively.

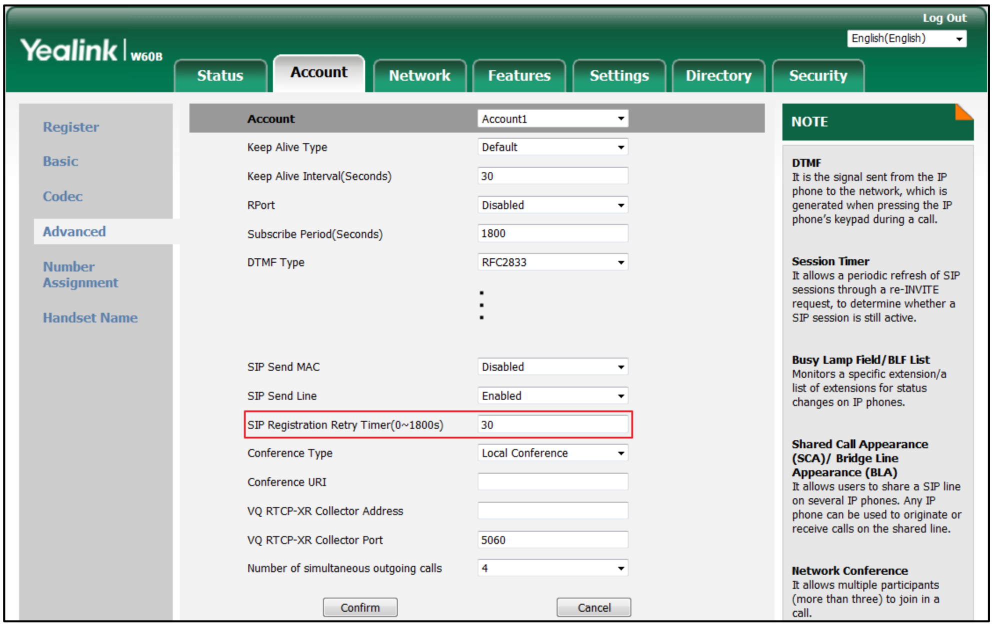


6. Click **Confirm** to accept the change.

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

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

3. Enter the desired interval in the **SIP Registration Retry Timer(0~1800s)** field.



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

Number of Active Handsets

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

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

Number of Active Handsets	Number of Simultaneous Active Calls
4	4
8	8

Note The W60B base station can handle a maximum of 6 simultaneous active calls when using opus codec.

Procedure

Number of active handsets can be configured using the following methods.

Configuration File	<y000000000077>.cfg	Configure max number of active handsets. **Parameter:** base.active_handset.number
Web User Interface		Configure max number of active

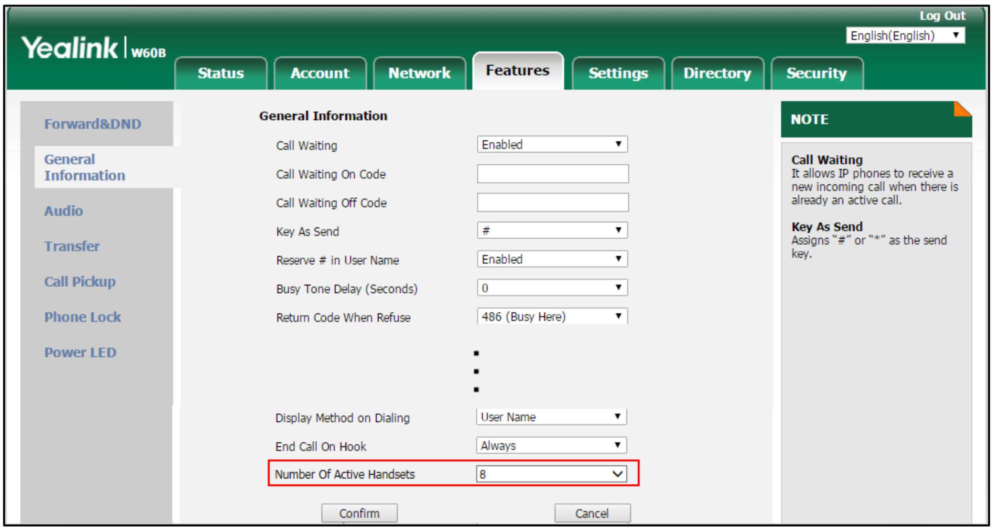
	handsets. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
base.active_handset.number	**4 or 8**	**4**
Description: Configures the max number of active handsets. **Note:** If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Features->General Information->Number Of Active Handset **Handset User Interface:** None		

To configure number of active handsers via web user interface:

1. Click on Features->General Information.
2. Select the desired value from the pull-down list of **Number Of Active Handsets**.



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

Number of Simultaneous Outgoing Calls

Number of simultaneous outgoing calls allows you to configure the max number of simultaneous outgoing calls for a specific account on a base. The number of active handsets affects this feature.

Procedure

Number of simultaneous outgoing calls can be configured using the following methods.

Configuration File	<MAC>.cfg	Configure max number of simultaneous outgoing calls. **Parameter:** account.X.simultaneous_outgoing.num
Web User Interface		Configure max number of simultaneous outgoing calls. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

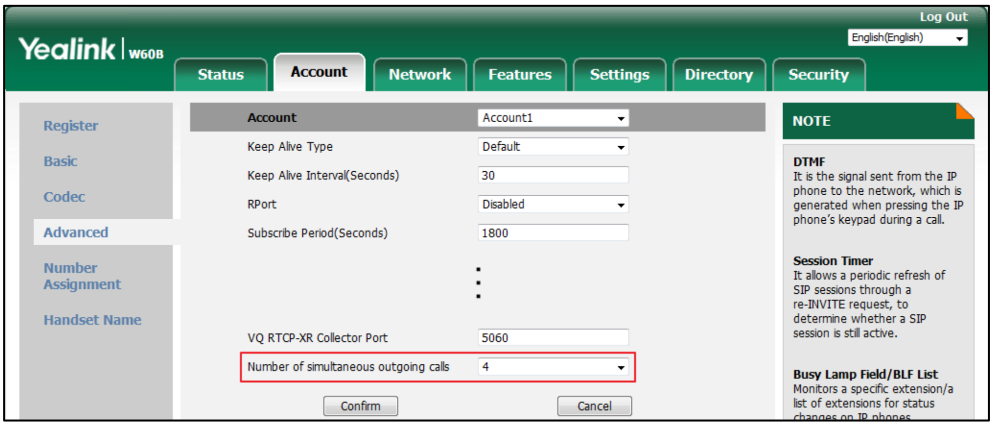
Details of Configuration Parameter:

Parameter	Permitted Values	Default
account.X.simultaneous_outgoing.num (X ranges from 1 to 8)	**1, 2, 3, 4, 5, 6, 7 or 8**	**8**
Description: Configures the max number of simultaneous outgoing calls for account X on a base station. **Note:** You should set the value of this parameter lower than or equal to the value of the parameter "base.active_handset.number". **Web User Interface:** Account->Advanced->Number of simultaneous outgoing calls **Handset User Interface:** None		

To configure number of simultaneous outgoing calls via web user interface:

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

2. Select the desired value from the pull-down list of **Number of simultaneous outgoing calls**.



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

Call Display

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

You can customize the call information to be displayed on the handsets as required. DECT IP phones support five call information display methods: Number+Name, Name, Name+Number, Number or Full Contact Info (display name<sip:xxx@domain.com>). The methods: Number+Name, Name and Number are not applicable to W52H handset.

Procedure

Call Display can be configured using the following methods.

Configuration File	y000000000077.cfg	Configure display called party information feature. **Parameter:** phone_setting.called_party_info_display.enable
		Specify the call information display method. **Parameter:** phone_setting.call_info_display_method
Web User Interface		Configure display called party information feature. Specify the call information display method.

	Navigate to: http://<phoneIPAddress>/servlet?p=settings-calldisplay&q=load

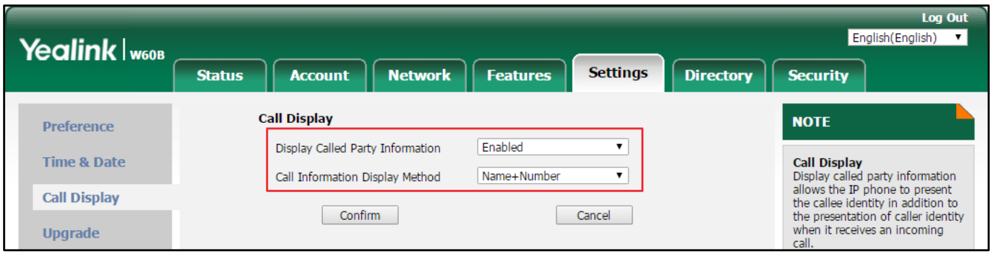
Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.called_party_info_display.enable	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to display the called account information when receiving an incoming call. **0**-Disabled **1**-Enabled **Note:** It is not applicable to W52H handset. **Web User Interface:** Settings->Call Display->Display Called Party Information **Handset User Interface:** None		
phone_setting.call_info_display_method	**0, 1, 2, 3 or 4**	**0**
Description: Specifies the call information display method when the handset receives an incoming call, dials an outgoing call or is during an active call. **0**-Name+Number **1**-Number+Name (not applicable to W52H handset) **2**-Name (not applicable to W52H handset) **3**-Number (not applicable to W52H handset) **4**-Full Contact Info (display name<sip:xxx@domain.com>) **Web User Interface:** Settings->Call Display->Call Information Display Method **Handset User Interface:** None		

To configure call display features via web user interface:

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

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



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

Number Assignment

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

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

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

Procedure

Number Assignment can be configured using the following methods.

Configuration File	y000000000077.cfg	Configure the incoming lines of the handset. **Parameter:** handset.X.incoming_lines
		Configure the outgoing lines of the handset. **Parameter:** handset.X.dial_out_lines
		Configure the default outgoing line of the handset. **Parameter:** handset.X.dial_out_default_line
Web User Interface		Configure the incoming lines of the handset. Configure the outgoing lines of the handset. Configure the default outgoing

	line of the handset. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-assignment&q=load
Handset User Interface	Configure the incoming lines of the handset. Configure the outgoing lines of the handset. Configure the default outgoing line of the handset.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
handset.X.incoming_lines (X ranges from 1 to 8)	**Integer from 1 to 8**	**Refer to the following content**
Description: Configures the lines to receive incoming calls for handset X. Multiple line IDs are separated by commas. **1**-Line 1 **2**-Line 2 **3**-Line 3 **4**-Line 4 **5**-Line 5 **6**-Line 6 **7**-Line 7 **8**-Line 8 **Default value:** The incoming line for handset 1 is line 1. The incoming line for handset 2 is line 2. The incoming line for handset 3 is line 3. The incoming line for handset 4 is line 4. The incoming line for handset 5 is line 5. The incoming line for handset 6 is line 6. The incoming line for handset 7 is line 7. The incoming line for handset 8 is line 8. **Web User Interface:**		

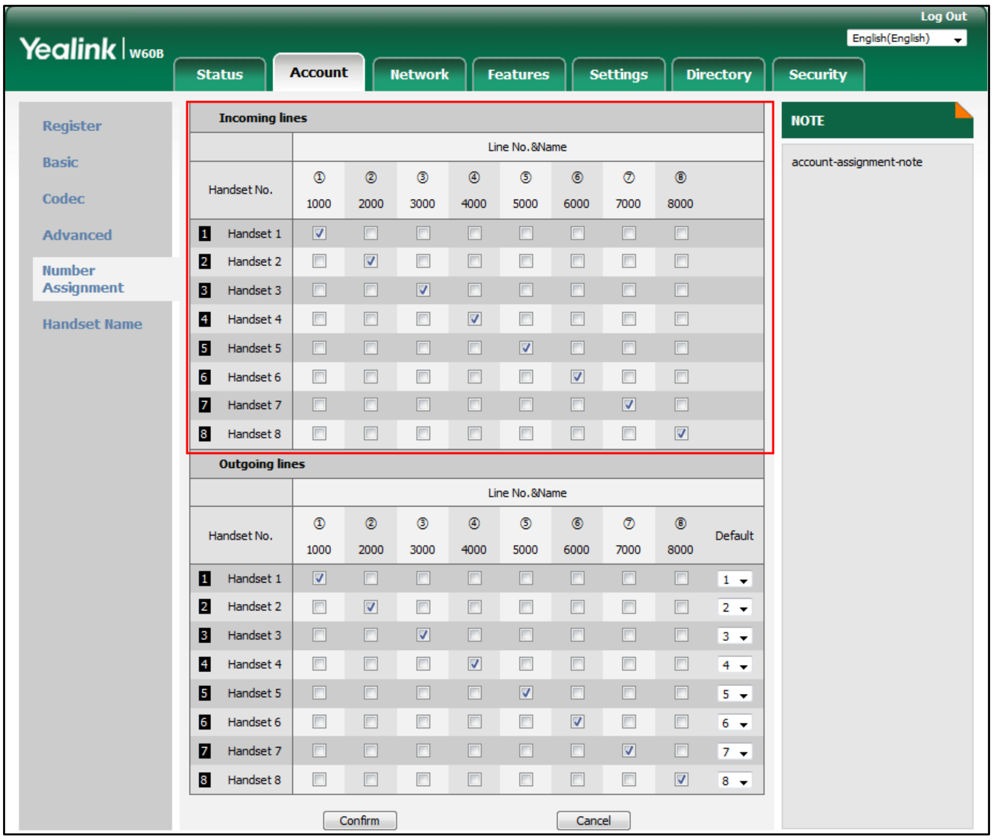
Parameters	Permitted Values	Default
Account->Number Assignment->Incoming lines **Handset User Interface:** OK->Settings->Telephony->Incoming Lines (Default PIN:0000) ->HandsetX		
handset.X.dial_out_lines (X ranges from 1 to 8)	**Integer from 1 to 8**	**Refer to the following content**
Description: Configures the lines to place outgoing calls for handset X. Multiple line IDs are separated by commas. **1**-Line 1 **2**-Line 2 **3**-Line 3 **4**-Line 4 **5**-Line 5 **6**-Line 6 **7**-Line 7 **8**-Line 8 **Default value:** The outgoing line for handset 1 is line 1. The outgoing line for handset 2 is line 2. The outgoing line for handset 3 is line 3. The outgoing line for handset 4 is line 4. The outgoing line for handset 5 is line 5. The incoming line for handset 6 is line 6. The incoming line for handset 7 is line 7. The incoming line for handset 8 is line 8. **Web User Interface:** Account->Number Assignment->Outgoing lines **Handset User Interface:** None		
handset.X.dial_out_default_line (X ranges from 1 to 8)	**Integer from 1 to 8**	**Refer to the following content**
Description: Configures the default line to place outgoing calls for handset X. **Default value:**		

Parameters	Permitted Values	Default
The default outgoing line for handset 1 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. The default outgoing line for handset 6 is 6. The default outgoing line for handset 7 is 7. The default outgoing line for handset 8 is 8. **Note:** It works only if the line you want to select to be default outgoing line should be configured as outgoing line for handset X in advance. **Web User Interface:** Account->Number Assignment->Outgoing lines->Default **Handset User Interface:** OK->Settings->Telephony->Default Line		

To assign the incoming line of the handset via web user interface:

1. Click on **Account**->**Number Assignment**.

2. To assign incoming lines, to check the desired account from **Line No.&Name** field to the corresponding handset in the **Handset No.** field.



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

To assign the incoming line to handsets via handset user interface:

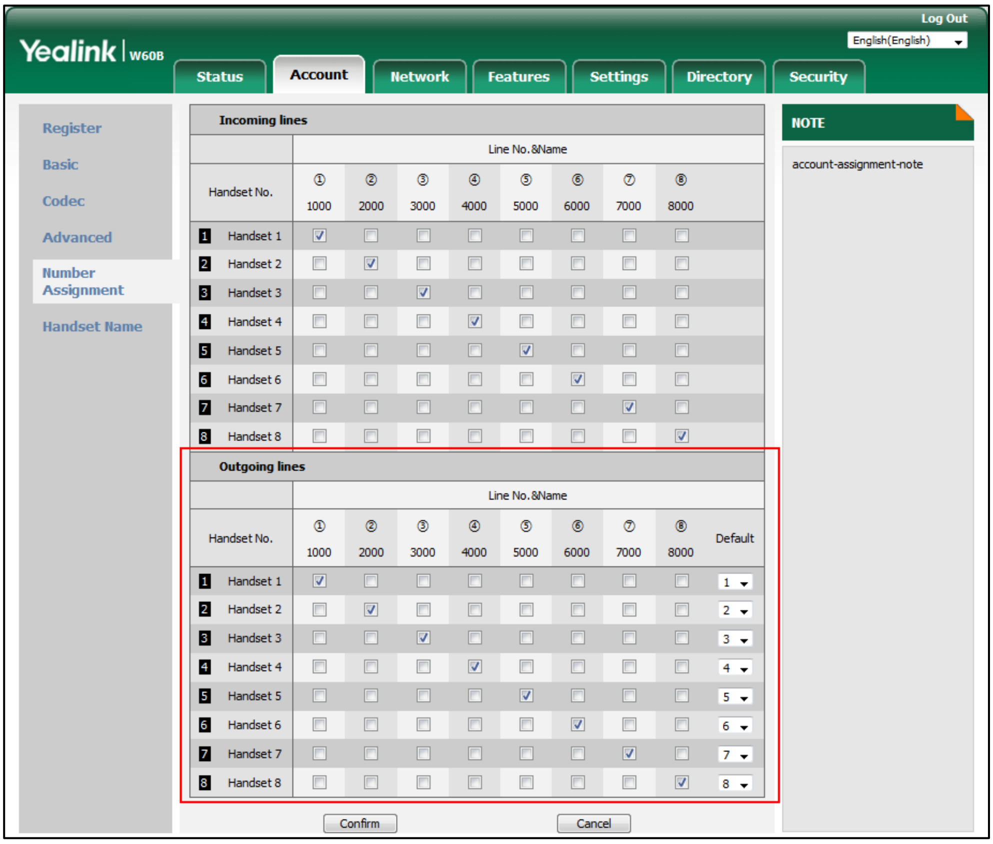
1. Press **OK** to enter the main menu.
2. Select **Settings**->**Telephony**->**Incoming Lines**.
3. Enter the system PIN (default: 0000), and then press the **Done** soft key.

   The LCD screen displays all handsets registered to the base station. The handset itself is highlighted and followed by a left arrow.
4. Press ▲ or ▼ to highlight the desired handset, and then press the **OK** soft key.
5. Press ◀ or ▶ to select **Accept** from the desired line fields.
6. Press the **Save** soft key to accept the change.
7. Press the **Back** soft key to return to the previous screen.
8. Repeat steps 5-8 to assign incoming lines for other handsets.

   If a line is assigned to multiple handsets as an incoming line, an incoming call to this line will cause these handsets to ring simultaneously, but the incoming call can be only answered by one of them.

To assign the outgoing line of the handset via web user interface:

1. Click on **Account**->**Number Assignment**.
2. To assign outgoing lines, to check the desired account from **Line No.&Name** field to the corresponding handset in the **Handset No.** field.
3. Select the desired default outgoing line number from the pull-down list of corresponding **Default**.



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

To change the default outgoing line of the handset via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Telephony**->**Default Line**.

   The LCD screen displays all outgoing lines currently assigned to the handset. The default outgoing line is highlighted and followed by a left arrow.
3. Press ▲ or ▼ to highlight the desired line, and then press the **OK** soft key.

   The default outgoing line is changed successfully.

Display Method on Dialing

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

You can customize the account information to be displayed on the handsets as required. DECT IP phones support three account information display methods: Label, Display Name or User Name. You can also hide the account information display.

Procedure

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

Central Provisioning (Configuration File)	y000000000077.cfg	Configure display method on dialing. **Parameter:** features.caller_name_type_on_dialing
Web User Interface		Configure display method on dialing. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

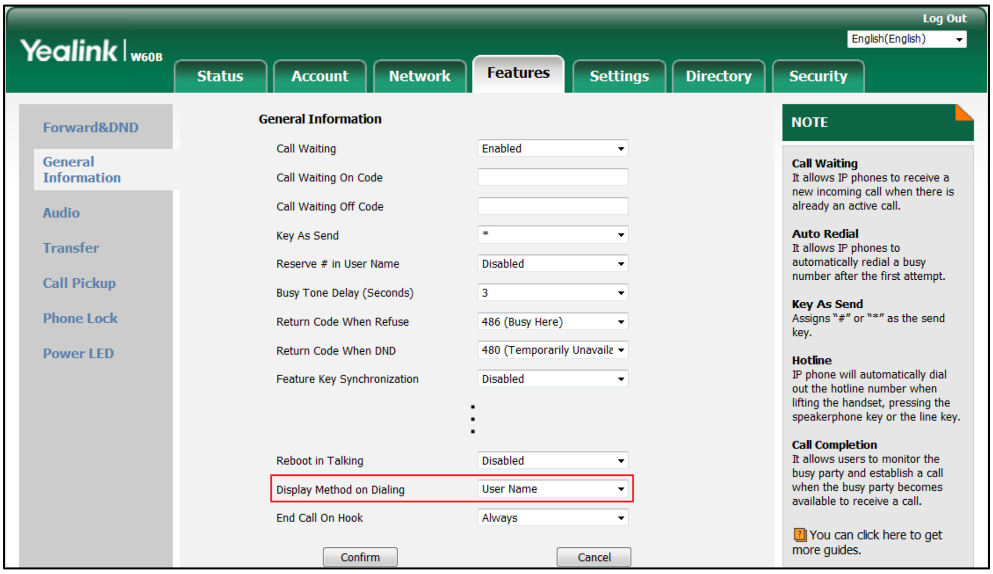
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.caller_name_type_on_dialing	**1, 2 or 3**	**3**
Description: Configures the account information displayed on the top center of the LCD screen when the DECT IP phone is on the pre-dialing or dialing screen. **1**-Label **2**-Display Name **3**-User Name **Note**: It works only if the value of the parameter "account.X.hide_local_number.enable" is set to 0 (Disabled). **Web User Interface:** Features->General Information->Display Method on Dialing **Handset User Interface:** None		
account.X.hide_local_number.enable (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Enables or disables the handset to hide the account information on the pre-dialing, dialing or ringing screen. **1**-Disabled		

Parameters	Permitted Values	Default
1-Enabled If it is set to 1 (Enabled), the LCD screen will display Line X (X ranges from 1 to 8 for the corresponding account) instead of account information. **Web User Interface:** None **Handset User Interface:** None		

To configure display method on dialing via web user interface:

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



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

Time and Date

DECT IP phones maintain a local clock. The time and date can be displayed in several formats on the idle screen of handset. You can select one of the default time/date formats or customize the date format.

There are 2 available time formats: “12 Hour” or “24 Hour”. For example, for the time format “12 Hour”, the time will be displayed in 12-hour format with AM or PM specified. For the time format “24 Hour”, the time will be displayed in 24-hour format (e.g., 9:00 PM displays as 21:00).

The time formats available:

Time Format	Example
12 Hour	09:39 PM
24 Hour	21:39

There are 7 available date formats by default. For example, for the date format "WWW DD MMM", "WWW" represents the abbreviation of the weekday, "DD" represents the two-digit day, and "MMM" represents the first three letters of the month.

The date formats available:

Date Format	**Example** (2016-09-02)
WWW MMM DD	Fri. Sep 02
DD-MMM-YY	02-Sep-16
YYYY-MM-DD	2016-09-02
DD/MM/YYYY	02/09/2016
MM/DD/YY	09/02/16
DD MMM YYYY	02 Sep 2016
WWW DD MMM	Fri. 02 Sep

Yealink DECT IP phones also support customizing date format. For example, YYYY-MMM-DDD-WWW, and W,MD, etc. For more information, refer to Time and Date Settings on page 170.

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

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

Option	Configuration Methods
	Web User Interface Handset User Interface
Date Format (custom)	Configuration Files
Daylight Saving Time	Configuration Files Web User Interface

NTP Time Server

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

The DECT IP phones synchronize the time and date automatically from the NTP time server by default. The NTP time server address can be offered by the DHCP server or configured manually. NTP by DHCP Priority feature can configure the priority for the DECT IP phone to use the NTP time server address offered by the DHCP server or configured manually.

Time Zone

A time zone is a region on Earth that has a uniform standard time. It is convenient for areas in close commercial or other communication to keep the same time. When configuring the DECT IP phone to obtain the time and date from the NTP time server, you must set the time zone.

Procedure

NTP time server and time zone can be configured using the following methods.

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

	Configure the NTP server, time zone. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-datetime&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
local_time.manual_ntp_srv_prior	**0 or 1**	**0**
Description: Configures the priority for the DECT IP phone to use the NTP server address offered by the DHCP server. **0**-High (use the NTP server address offered by the DHCP server preferentially) **1**-Low (use the NTP server address configured manually preferentially) **Web User Interface:** Settings->Time & Date->NTP by DHCP Priority **Handset User Interface:** None		
local_time.dhcp_time	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to update time with the offset time offered by the DHCP server. **0**-Disabled **1**-Enabled **Note**: It is only available to offset from Greenwich Mean Time (GMT). **Web User Interface:** Settings->Time & Date->DHCP Time **Handset User Interface:** None		
local_time.ntp_server1	**IP address or domain name**	**cn.pool.ntp.org**
Description: Configures the IP address or the domain name of the NTP server 1. The DECT IP phone will obtain the current time and date from the NTP server 1. **Example:**		

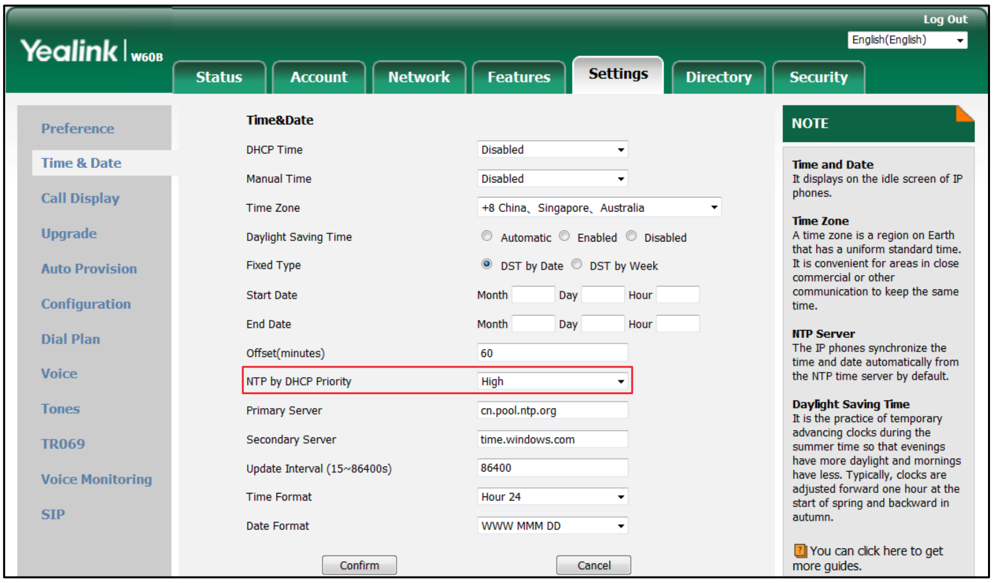
Parameters	Permitted Values	Default
local_time.ntp_server1 = 192.168.0.5 **Web User Interface:** Settings->Time & Date->Primary Server **Handset User Interface:** None		
local_time.ntp_server2	**IP address or domain name**	**pool.ntp.org**
Description: Configures the IP address or the domain name of the NTP server 2. If the NTP server 1 is not configured (configured by the parameter "local_time.ntp_server1") or cannot be accessed, the DECT IP phone will request the time and date from the NTP server 2. **Example:** local_time.ntp_server2 = 192.168.0.6 **Web User Interface:** Settings->Time & Date->Secondary Server **Handset User Interface:** None		
local_time.interval	**Integer from 15 to 86400**	**1000**
Description: Configures the interval (in seconds) to update time and date from the NTP server. **Example:** local_time.interval = 1000 **Web User Interface:** Settings->Time & Date->Update Interval (15~86400s) **Handset User Interface:** None		
local_time.time_zone	**-11 to +14**	**+8**

Parameters	Permitted Values	Default
Description: Configures the time zone. For more available time zones, refer to Appendix B: Time Zones on page 469. **Example:** local_time.time_zone = +8 **Web User Interface:** Settings->Time & Date->Time Zone **Handset User Interface:** None		
local_time.time_zone_name	**String within 32 characters**	**China(Beijing)**
Description: Configures the time zone name. The available time zone names depend on the time zone configured by the parameter "local_time.time_zone". For more information on the available time zone names for each time zone, refer to Appendix B: Time Zones on page 469. **Example:** local_time.time_zone_name = China(Beijing) **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 2 (Automatic) and the parameter "local_time.time_zone" should be configured in advance. **Web User Interface:** Settings->Time & Date->Location **Handset User Interface:** None		

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

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

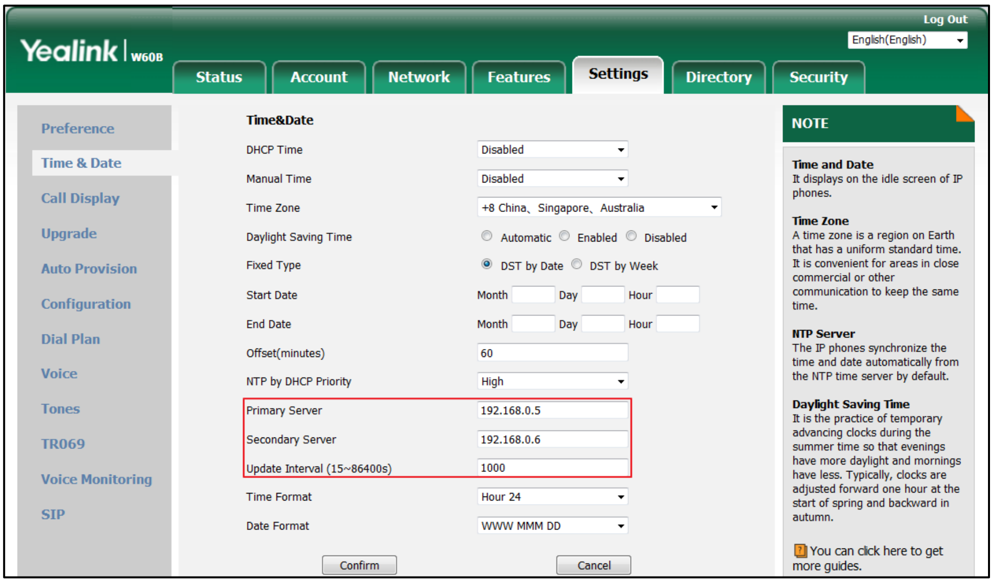
2. Select the desired value from the pull-down list of **NTP by DHCP Priority**.



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

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

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



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

Time and Date Settings

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

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

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

Procedure

Time and date can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the time and date manually. **Parameter:** local_time.manual_time_enable
		Configure the time and date formats. **Parameters:** custom.handset.time_format

		custom.handset.date_format
		Customize the date format. **Parameter:** lcl.datetime.date.format
Web User Interface		Configure the time and date manually. Configure the time and date formats. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-datetime&q=load
Handset User Interface		Configure the time and date manually. Configure the time and date formats.

Details of Configuration Parameters:

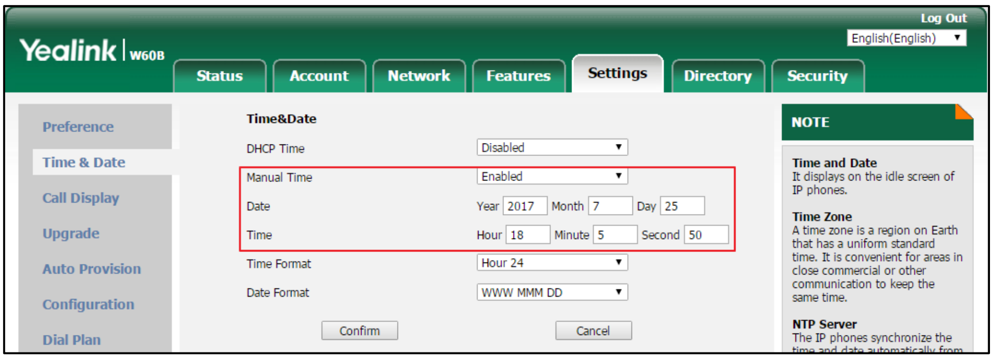
Parameters	Permitted Values	Default
local_time.manual_time_enable	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to obtain time and date from manual settings. **0**-Disabled (obtain time and date from NTP server) **1**-Enabled (obtain time and date from manual settings) **Web User Interface:** Settings->Time & Date->Manual Time **Handset User Interface:** None		
custom.handset.time_format	**0 or 1**	**1**
Description: Configures the time format for all registered handsets. **0**-Hour 12 **1**-Hour 24 If it is set to 0 (Hour 12), the time will be displayed in 12-hour format with AM or PM specified.		

Parameters	Permitted Values	Default
If it is set to 1 (Hour 24), the time will be displayed in 24-hour format (e.g., 2:00 PM displays as 14:00). **Note:** It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Time & Date->Time Format **Handset User Interface:** OK->Settings->Display->Time Format		
custom.handset.date_format	**0, 1, 2, 3, 4, 5 or 6**	**0**
Description: Configures the date format for all registered handsets. **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 **Note**: "WWW" represents the abbreviation of the week, "DD" represents a two-digit day, "MMM" represents the first three letters of the month, "YYYY" represents a four-digit year, and "YY" represents a two-digit year. The value configured by the parameter "lcl.datetime.date.format" takes precedence over that configured by this parameter. It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Time & Date->Date Format **Handset User Interface:** OK->Settings->Display->Date Format		
lcl.datetime.date.format	**String**	**Blank**
Description: Configures the format of date string. **Y** = year, **M** = month, **D** = day, **W** = day of week **Value formats are:** ● Any combination of W, M, D and the separator (e.g., space, dash, slash).		

Parameters	Permitted Values	Default
Example: lcl.datetime.date.format = W,MD The handset will display the date in "W,MD" format (e.g., Wed,0420). ● Any combination of Y, M, D, W and the separator (e.g., space, dash, slash). **Example:** lcl.datetime.date.format = YYYY-MMM-DDD-WWW The handset will display the date in "YYYY-MMM-DDD-WWW" format (e.g., 2016-Apr-20-Wednesday). **Note**: "Y"/"YY" represents a two-digit year, more than two "Y" letters (e.g., YYYY) represent a four-digit year, "M"/"MM" represents a two-digit month, "MMM" represents the abbreviation of the month, three or more than three "M" letters (e.g., MMM) represent the long format of the month, one or more than one "D" (e.g., DDD) represents a two-digit day, "W"/"WW" represents the abbreviation of the day of week, three or more three "W" letters (e.g., WWW) represent the long format of the day of week. It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled). **Web User Interface:** None **Handset User Interface:** None		

To configure the time and date manually for all registered handsets via web user interface:

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



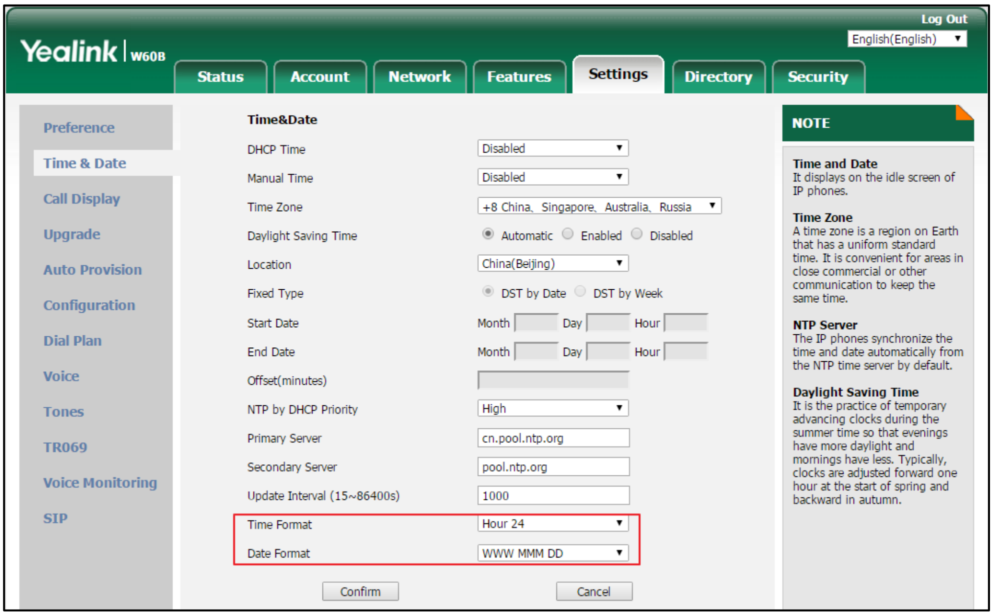
4. Click **Confirm** to accept the change.

To configure the time and date formats for all registered handsets via web user interface:

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

2. Select the desired value from the pull-down list of **Time Format**.

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



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

To configure time and date manually via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Date & Time**.
3. Edit the current value in the **Date** and **Time** field respectively.
4. Press the **Save** soft key to accept the change.

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

To configure the time format via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Display**->**Time Format**.
3. Press ▲ or ▼ to highlight the desired time format.
4. Press the **Change** soft key.

   The radio box of the highlighted time format is marked.

The time format displayed on the LCD screen will be changed accordingly.

To configure the date format via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Display**->**Date Format**.
3. Press ▲ or ▼ to highlight the desired date format.
4. Press the **Change** soft key.

   The radio box of the selected date format is marked.

The date format displayed on the LCD screen will be changed accordingly.

Note Before you configure date and time manually via handset user interface, you should enable the **Manual Time** via web user interface first, or it would not take effect.

Daylight Saving Time (DST)

Daylight Saving Time (DST) is the practice of temporary advancing clocks during the summer time so that evenings have more daylight and mornings have less. Typically, clocks are adjusted forward one hour at the start of spring and backward in autumn. Many countries have used the DST at various times, details vary by location. By default, the DST is set to Automatic, so it can be adjusted automatically from the current time zone configuration. You can configure DST for the desired area as required.

Procedure

Daylight saving time can be configured using the following methods.

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

Details of Configuration Parameters:

Parameters	Permitted Values	Default
local_time.summer_time	**0, 1 or 2**	**2**
Description: Configures Daylight Saving Time (DST) feature. **0**-Disabled **1**-Enabled **2**-Automatic		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Note: If there is no available time zone name for the configured time zone, you can set the value of the parameter “local_time.summer_time” to be 1 (Enabled), and configure the DST time manually.
Web User Interface:
Settings->Time & Date->Daylight Saving Time
Handset User Interface:
None</td></tr>
<tr><td>local_time.dst_time_type</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Configures the Daylight Saving Time (DST) time type.
0-DST by Date
1-DST by Week
Note: It works only if the value of the parameter “local_time.summer_time” is set to 1 (Enabled).
Web User Interface:
Settings->Time & Date->Fixed Type
Handset User Interface:
None</td></tr>
<tr><td>local_time.start_time</td><td>Time</td><td>1/1/0</td></tr>
<tr><td colspan="3">Description:
Configures the starting time of the Daylight Saving Time (DST).
Value formats are:
● Month/Day/Hour (for DST by Date)
● Month/Week of Month/Day of Week/Hour of Day (for DST by Week)
If “local_time.dst_time_type” is set to 0 (DST by Date), use the mapping:
Month: 1=January, 2=February,..., 12=December
Day: 1=the first day in a month,..., 31= the last day in a month
Hour: 0=0am, 1=1am,..., 23=11pm
Example:
local_time.start_time = 1/1/2
If “local_time.dst_time_type” is set to 1 (DST by Week), use the mapping:
Month: 1=January, 2=February,..., 12=December
Week of Month: 1=the first week in a month,..., 5=the last week in a month</td></tr>
</table>

Parameters	Permitted Values	Default
Day of Week: 1=Monday, 2=Tuesday,..., 7=Sunday **Hour of Day**: 0=0am, 1=1am,..., 23=11pm **Example**: local_time.start_time = 1/1/7/0 **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings->Time & Date->Start Date **Handset User Interface:** None		
local_time.end_time	**Time**	**12/31/23**
Description: Configures the ending time of the Daylight Saving Time (DST). **Value formats are:** ● Month/Day/Hour (for DST by Date) ● Month/Week of Month/Day of Week/Hour of Day (for DST by Week) If "local_time.dst_time_type" is set to 0 (DST by Date), use the mapping: **Month**: 1=January, 2=February,..., 12=December **Day**: 1=the first day in a month,..., 31= the last day in a month **Hour**: 0=0am, 1=1am,..., 23=11pm **Example**: local_time.start_time = 12/12/22 If "local_time.dst_time_type" is set to 1 (DST by Week), use the mapping: **Month**: 1=January, 2=February,..., 12=December **Week of Month**: 1=the first week in a month,..., 5=the last week in a month **Day of Week**: 1=Monday, 2=Tuesday,..., 7=Sunday **Hour of Day**: 0=0am, 1=1am,..., 23=11pm **Example**: local_time.start_time = 4/3/2/3 **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings->Time & Date->End Date **Handset User Interface:**		

Parameters	Permitted Values	Default
None		
local_time.offset_time	**Integer from -300 to 300**	**Blank**
Description: Configures the offset time (in minutes) of Daylight Saving Time (DST). **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings->Time & Date->Offset(minutes) **Handset User Interface:** None		

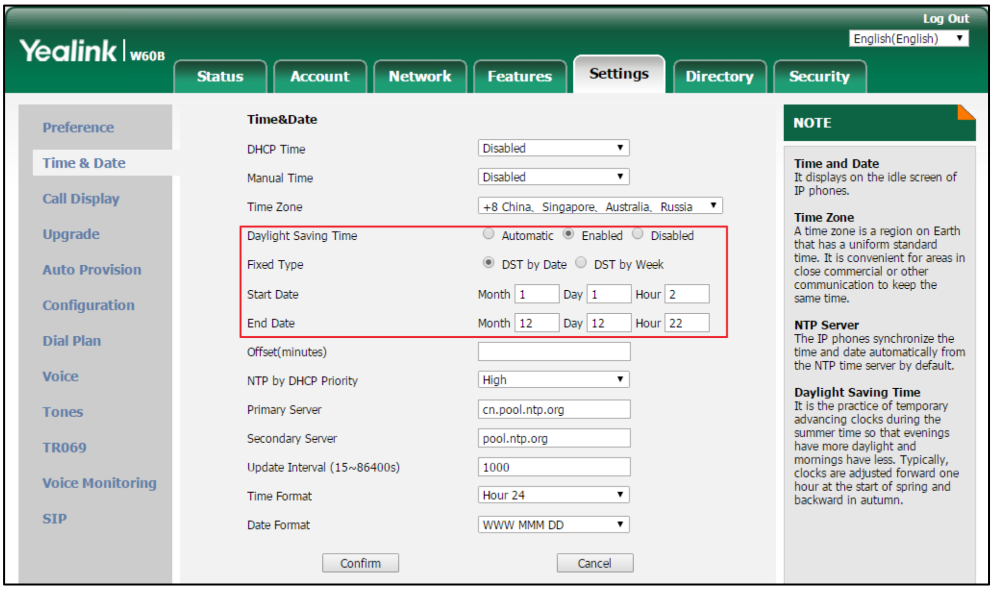
To configure the DST via web user interface:

1. Click on **Settings**->**Time & Date**.
2. Select **Disabled** from the pull-down list of **Manual Time**.
3. Select the desired time zone from the pull-down list of **Time Zone**.
4. Enter the domain name or IP address in the **Primary Server** and **Secondary Server** field respectively.
5. Enter the desired time interval in the **Update Interal (15~86400s)** field.
6. Mark the **Enabled** radio box in the **Daylight Saving Time** field.

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

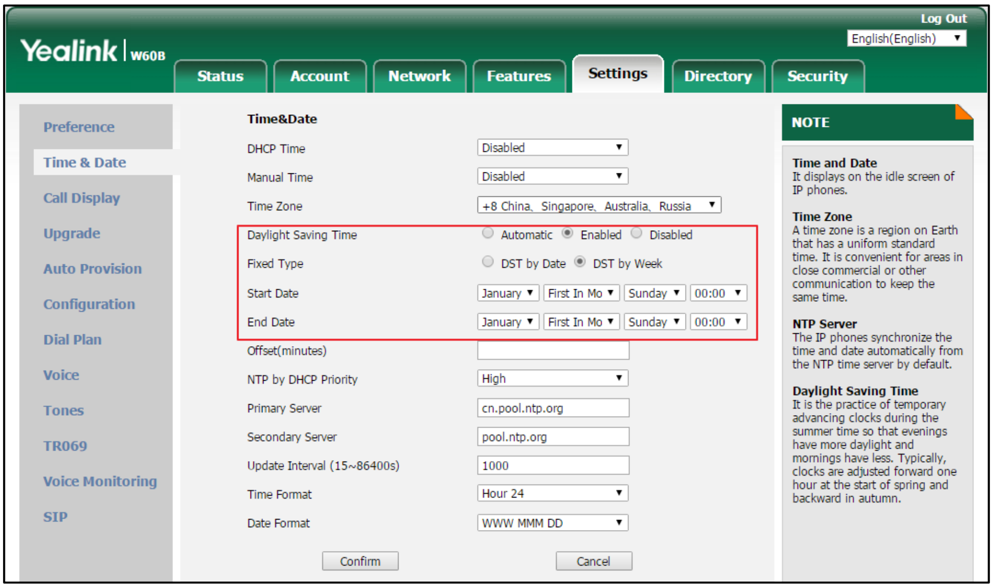
     Enter the starting time in the **Start Date** field.

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



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

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



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

Customizing an AutoDST Template File

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

Before customizing, you need to obtain the AutoDST file. You can ask the distributor or Yealink FAE for DST template. You can also obtain the DST template online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the template file, refer to Obtaining Boot Files/Configuration Files/Resource Files on page 89.

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

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

Element	Type	Values	Description
		keep their daylight saving time the same)	
iType	optional	0/1 **0**: DST by Date **1**: DST by Week	DST time type (This item is needed if you want to configure DST.)
szStart	optional	**Month/Day/Hour** (for **iType=0**) Month: 1~12 Day: 1~31 Hour: 0 (midnight)~23 **Month/Week of Month/Day of Week/Hour of Day** (for **iType=1**) Month: 1~12 Week of Month: 1~5 (the last week) Day of Week: 1~7 Hour of Day: 0 (midnight)~23	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

When customizing an AutoDST file, learn the following:

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

Customizing an AutoDST file:

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

   Example 1:

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

AutoDST.xml*

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

Modify it:
iType="1" szStart="10/1/7/2" szEnd="4/1/7/3" szOffset="60"

Add DST

Example 2:

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

AutoDST.xml

```
<DST szTime="+4:30"  szZone="Afghanistan(Kabul)"/>
<DST szTime="+5"    szZone="Kazakhstan(Aqtobe)"/>
<DST szTime="+5"    szZone="Kyrgyzstan(Bishkek)" />
<DST szTime="+5"    szZone="Pakistan(Islamabad)" iType="0" szStart="4/15/0"     szEnd="11/1/0"
<DST szTime="+5"    szZone="Russia(Chelyabinsk)"  />
<DST szTime="+5:30"   szZone="India(Calcutta)"/>
<DST szTime="+5:45"  szZone="Nepal(Katmandu)"/>
<DST szTime="+6"  szZone="Paradise" iType="1" szStart="3/5/7/2" szEnd="10/5/7/3" szOffset="30"/>
<DST szTime="+6"    szZone="Kazakhstan(Astana,Almaty)"/>
<DST szTime="+6"    szZone="Russia(Novosibirsk,Omsk)" />
<DST szTime="+6:30"  szZone="Myanmar(Naypyitaw)" />
<DST szTime="+7"    szZone="Russia(Krasnoyarsk)"  />
<DST szTime="+7"    szZone="Thailand(Bangkok)"/>
<DST szTime="+8"    szZone="China(Beijing)"/>
<DST szTime="+8"    szZone="Singapore(Singapore)" />
<DST szTime="+8"    szZone="Australia(Perth)" iType="1" szStart="10/1/7/2"    szEnd="3/5/7/3"
<DST szTime="+8"    szZone="Russia(Irkutsk, Ulan-Ude)"/>
<DST szTime="+8:45"  szZone="Eucla"/>
<DST szTime="+9"    szZone="Korea(Seoul)"/>
<DST szTime="+9"    szZone="Japan(Tokyo)"/>
<DST szTime="+9"    szZone="Russia(Yakutsk, Chita)"/>
<DST szTime="+9:30"  szZone="Australia(Adelaide)" iType="1" szStart="10/1/7/2"    szEnd="4/1/7/3
<DST szTime="+9:30"  szZone="Australia(Darwin)" />
<DST szTime="+10"   szZone="Australia(Sydney,Melbourne,Canberra)" iType="1" szStart="10/1/7/2"
<DST szTime="+10"   szZone="Australia(Brisbane)"/>
```

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

Procedure

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

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

Details of Configuration Parameter:

Parameter	Permitted Values	Default
auto_dst.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the AutoDST file (AutoDST.xml). **Example:** auto_dst.url = tftp://192.168.1.100/AutoDST.xml During the auto provisioning process, the DECT IP phone connects to the provisioning server "192.168.1.100", and downloads the AutoDST file "AutoDST.xml". After update, you will find a new time zone "Paradise" and updated DST of "Pakistan (Islamabad)" and "India (Calcutta)" via web user interface: **Settings**->**Time & Date**->**Time Zone**. **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 2 (Automatic). **Web User Interface:** None **Handset User Interface:** None		

Input Method

Specifying the Default Input Method

You can also specify the default input method for the DECT IP phone when searching for contacts.

Procedure

Specify the default input methods using the configuration file.

Configuration File	y000000000077.cfg	Specify the default input method when searching for contacts. **Parameter:** directory.search_default_input_meth od

Details of Configuration Parameter:

<table>
<tr><th>Parameter</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>directory.search_default_input_method</td><td>Integer from 1 to 12</td><td>1</td></tr>
<tr><td colspan="3">Description:
Configures the default input method when the user searches for contacts in the Local Directory, LDAP, Remote Phone Book or Blacklist.
1-Abc
2-123
3-ABC
4-abc
5-ΑΒΓ
6-AÄÅ
7-aäå
8-SŚŠ
9-sśš
10-абв
11-АБВ
12-אבג
Example:
directory.search_default_input_method = 1
Note: It works only when the corresponding input method is enabled via handset user interface at the path: OK->Settings->Display->Input Method.
Web User Interface:
None
Handset User Interface:
None</td></tr>
</table>

To configure the input method via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Display**->**Input Method**.

   The LCD screen displays all available input methods.
3. Press ▲ or ▼ to highlight the desired input method.
4. Press the **Change** soft key to check or uncheck the checkbox.

Key As Send

Key as send allows assigning the pound key ("#") or asterisk key ("*") as the send key.

Procedure

Key as send can be configured using the following methods.

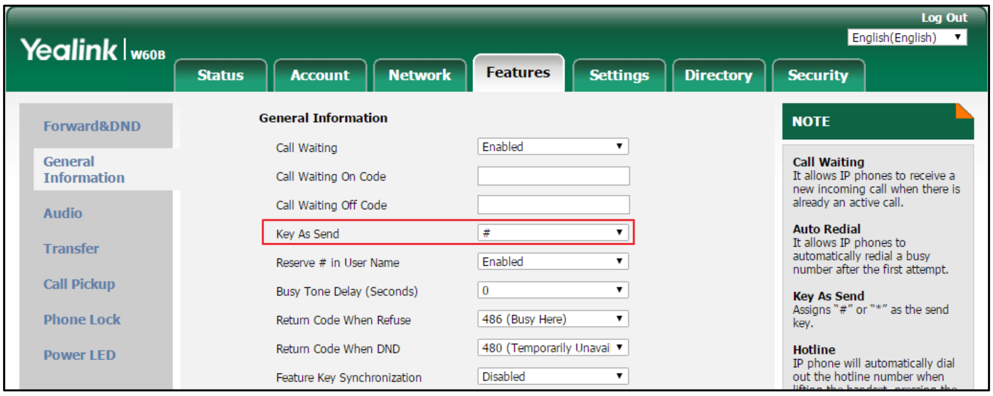
Central Provisioning (Configuration File)	y000000000077.cfg	Configure a send key. **Parameter:** features.key_as_send
Web User Interface		Configure a send key. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.key_as_send	**0, 1 or 2**	**1**
Description: Configures the "#" or "*" key as the send key. **0**-Disabled **1**-# key **2**-* key If it is set to 0 (Disabled), neither "#" nor "*" can be used as the send key. If it is set to 1 (# key), the pound key is used as the send key. If it is set to 2 (* key), the asterisk key is used as the send key. **Web User Interface:** Features->General Information->Key As Send **Handset User Interface:** None		

To configure a send key via web user interface:

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



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

Dial Plan

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

Regular expression can be used to define DECT IP phone dial plan. Dial plan is a string of characters that governs the way for DECT IP phones to process the inputs received from the DECT IP phone's keypads.

Yealink DECT IP phones support the following dial plan features:

- Replace Rule
- Dial Now
- Area Code
- Block Out

You can configure these dial plan features via web user interface or using configuration files. You can select to add a replace rule/dial now rule one by one or using the replace rule/dial now template file to add multiple replace rules at a time.

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

.	The dot "." can be used as a placeholder or multiple placeholders for any string. Example: "12." would match "12**3**", "12**34**", "12**345**", "12**abc**", etc.
x	The "x" can be used as a placeholder for any character. Example:

	“12x” would match “12**1**”, “12**2**”, “12**3**”, “12**a**”, etc.
-	The dash “-” can be used to match a range of characters within the brackets. Example: “[5-7]” would match the number “**5**”, “**6**” or “**7**”.
,	The comma “,” can be used as a separator within the bracket. Example: “[2,5,8]” would match the number “**2**”, “**5**” or “**8**”.
[]	The square bracket "[]" can be used as a placeholder for a single character which matches any of a set of characters. Example: "91[5-7]1234"would match “91**5**1234”, “91**6**1234”, “91**7**1234”.
()	The parenthesis "( )" can be used to group together patterns, for instance, to logically combine two or more patterns. Example: "([1-9])([2-7])3" would match “**92**3”, “**15**3”, “**67**3”, etc.
$	The “$” followed by the sequence number of a parenthesis means the characters placed in the parenthesis. The sequence number stands for the corresponding parenthesis. Example: A replace rule configuration, Prefix: "001(xxx)45(xx)", Replace: "9001$145$2". When you dial out "0012354599" on your phone, the DECT IP phone will replace the number with "9001**235**45**99**". “$1” means 3 digits in the first parenthesis, that is, “235”. “$2” means 2 digits in the second parenthesis, that is, “99”.

Replace Rule

Replace rule is an alternative string that replaces the numbers entered by the user. DECT IP phones support up to 100 replace rules, which can be created either one by one or in batch using a replace rule template. For more information on how to customize a replace rule template, refer to Customizing Replace Rule Template File on page 189.

Procedure

Replace rule can be created using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Create the replace rule for the DECT IP phone. **Parameters:** dialplan.replace.prefix.X dialplan.replace.replace.X dialplan.replace.line_id.X
Web User Interface		Create the replace rule for the

	DECT IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-dialplan&q=load

Details of Configuration Parameters:

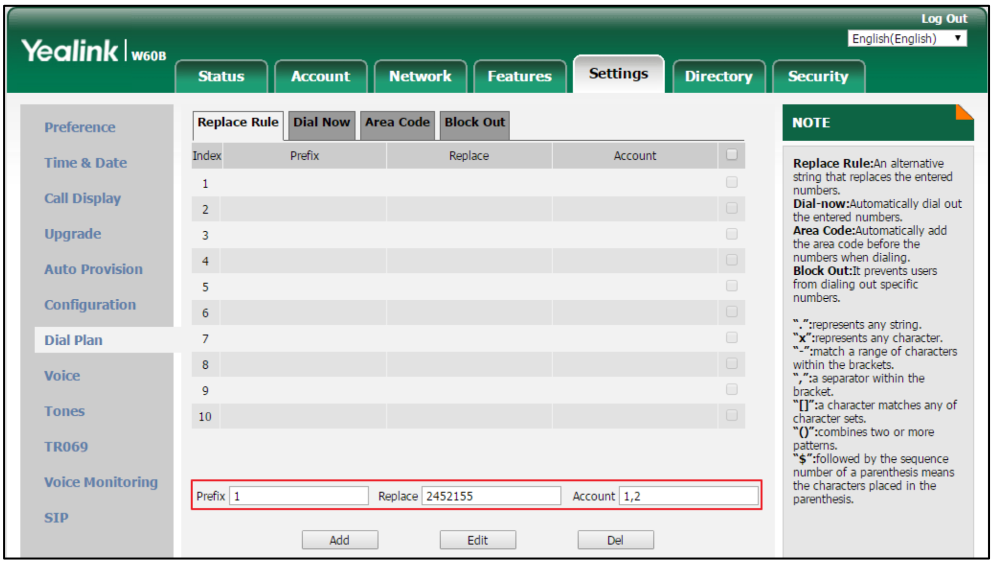
Parameters	Permitted Values	Default
dialplan.replace.prefix.X (X ranges from 1 to 100)	**String within 32 characters**	**Blank**
Description: Configures the entered number to be replaced. **Example:** dialplan.replace.prefix.1 = 1 **Web User Interface:** Settings->Dial Plan->Replace Rule->Prefix **Handset User Interface:** None		
dialplan.replace.replace.X (X ranges from 1 to 100)	**String within 32 characters**	**Blank**
Description: Configures the alternate number to replace the entered number. **Example:** dialplan.replace.prefix.1 =1 and dialplan.replace.replace.1 = 254245 When you enter the number "1" and then press the send key, the number "254245" will replace the entered number "1". **Web User Interface:** Settings->Dial Plan->Replace Rule->Replace **Handset User Interface:** None		
dialplan.replace.line_id.X (X ranges from 1 to 100)	**Integer from 0 to 8**	**Blank (for all lines)**
Description: Configures the desired line to apply the replace rule. The digit 0 stands for all lines. If it is left blank, the replace rule will apply to all lines on the DECT IP phone. **Example:**		

Parameters	Permitted Values	Default
dialplan.replace.line_id.1 = 1,2 **Web User Interface:** Settings->Dial Plan->Replace Rule->Account **Handset User Interface:** None		

To create a replace rule via web user interface:

1. Click on **Settings**->**Dial Plan**->**Replace Rule**.
2. Enter the string in the **Prefix** field.
3. Enter the string in the **Replace** field.
4. Enter the desired line ID in the **Account** field or leave it blank.

   If you leave this field blank or enter 0, the replace rule will apply to all accounts on the DECT IP phone.



5. Click **Add** to add the replace rule.

Customizing Replace Rule Template File

The replace rule template helps with the creation of multiple replace rules.

You can ask the distributor or Yealink FAE for replace rule template. You can also obtain the replace rule template online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the replace rule template, refer to Obtaining Boot Files/Configuration Files/Resource Files on page 89.

When editing a replace rule template file, learn the following:

- <DialRule> indicates the start of the template file and </DialRule> indicates the end of the template file.

- When specifying the desired line(s) to apply the replace rule, the valid values are 0 and line ID (0~8). Multiple line IDs are separated by commas.
- At most 100 replace rules can be added to the DECT IP phone.

The expression syntax in the replace rule template is the same as that introduced in the section Dial Plan on page 186.

To customize a replace rule template:

1. Open the template file using an ASCII editor.

2. Create replace rules between <DialRule> and </DialRule>.

For example:

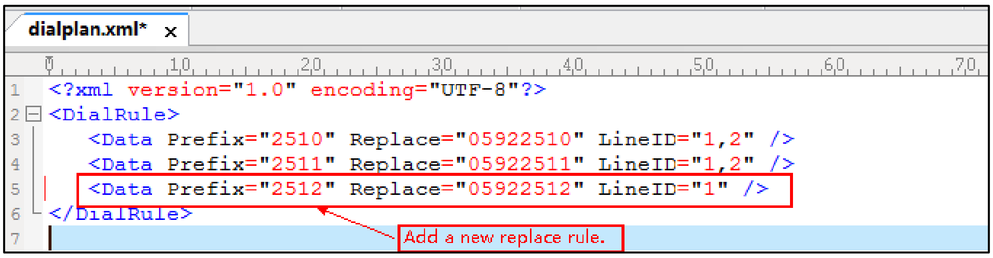
<Data Prefix="2512" Replace="05922512" LineID="1" />

Where:

Prefix="" specifies the numbers to be replaced.

Replace="" specifies the alternate string instead of what the user enters.

LineID="" specifies the desired line(s) for this rule. When you leave it blank or enter 0, this replace rule will apply to all lines.



If you want to change the replace rule, specify the values within double quotes.

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

4. Specify the access URL of the replace rule template in the configuration files.

Procedure

Specify the access URL of the replace rule template using the configuration files.

Central Provisioning (Configuration File)	y000000000077.cfg	Specify the access URL of the replace rule template. **Parameter:** dialplan_replace_rule.url

Details of Configuration Parameter:

Parameter	Permitted Values	Default
dialplan_replace_rule.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the replace rule template file. **Example:** dialplan_replace_rule.url = http://192.168.10.25/dialplan.xml During the auto provisioning process, the DECT IP phone connects to the provisioning server "192.168.10.25", and downloads the replace rule file "dialplan.xml". **Web User Interface:** None **Handset User Interface:** None		

Dial Now

Dial now is a string used to match numbers entered by the user. When entered numbers match the predefined dial now rule, the DECT IP phone will automatically dial out the numbers without pressing the send key. DECT IP phones support up to 20 dial now rules, which can be created either one by one or in batch using a dial now rule template. For more information on how to customize a dial now template, refer to Customizing Dial Now Template File on page 194. It is not applicable to W52H handset.

Time Out for Dial Now Rule

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

Procedure

Dial now rule can be created using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Create the dial now rule for the DECT IP phone. **Parameters:** dialplan.dialnow.rule.X dialplan.dialnow.line_id.X
		Configure the delay time for the dial now rule.

		Parameter: phone_setting.dialnow_delay
Web User Interface		Create the dial now rule for the DECT IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-dialnow&q=load
		Configure the delay time for the dial now rule. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameters:

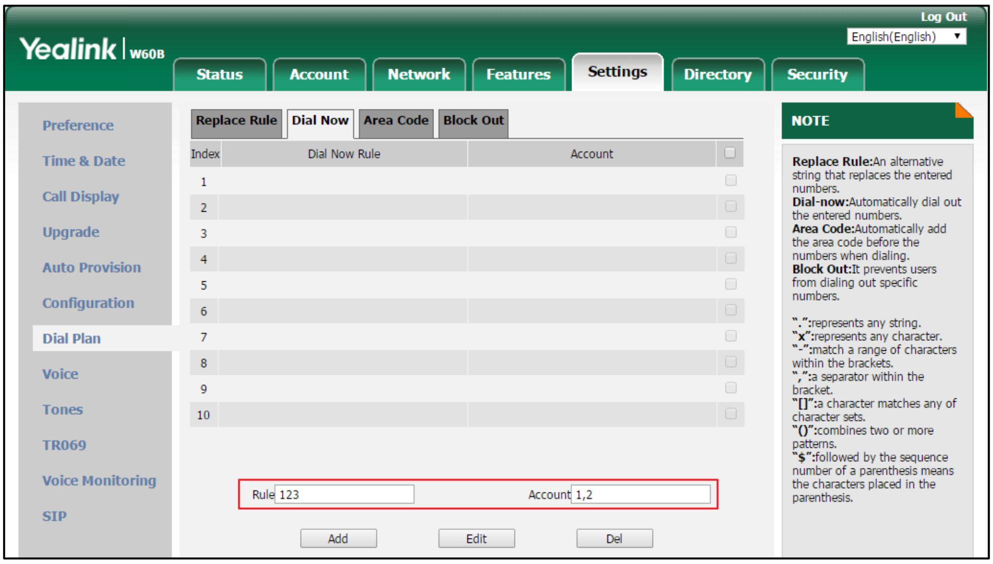
Parameters	Permitted Values	Default
dialplan.dialnow.rule.X (X ranges from 1 to 20)	**String within 24 characters**	**Blank**
Description: Configures the dial now rule (the string used to match the numbers entered by the user). When entered numbers match the predefined dial now rule, the DECT IP phone will automatically dial out the numbers without pressing the send key. **Example:** dialplan.dialnow.rule.1 = 123 **Note:** It is not applicable to W52H Handset. **Web User Interface:** Settings->Dial Plan->Dial Now->Rule **Handset User Interface:** None		
dialplan.dialnow.line_id.X (X ranges from 1 to 20)	**Integer from 0 to 8**	**Blank (for all lines)**
Description: Configures the desired line to apply the dial now rule. The digit 0 stands for all lines. If it is left blank, the dial now rule will apply to all lines on the DECT IP phone. **Example:** dialplan.dialnow.line_id.1 = 1,2		

Parameters	Permitted Values	Default
Note: Multiple line IDs are separated by commas. It is not applicable to W52H handset. **Web User Interface:** Settings->Dial Plan->Dial Now->Account **Handset User Interface:** None		
phone_setting.dialnow_delay	**Integer from 0 to 14**	**1**
Description: Configures the delay time (in seconds) for the dial now rule. When entered numbers match the predefined dial now rule, the DECT IP phone will automatically dial out the entered number after the designated delay time. If it is set to 0, the DECT IP phone will automatically dial out the entered number immediately. **Note**: It is not applicable to W52H handset. **Web User Interface:** Features->General Information->Time Out for Dial Now Rule **Handset User Interface:** None		

To create a dial now rule via web user interface:

1. Click on **Settings**->**Dial Plan**->**Dial Now**.
2. Enter the desired value in the **Rule** field.
3. Enter the desired line ID in the **Account** field or leave it blank.

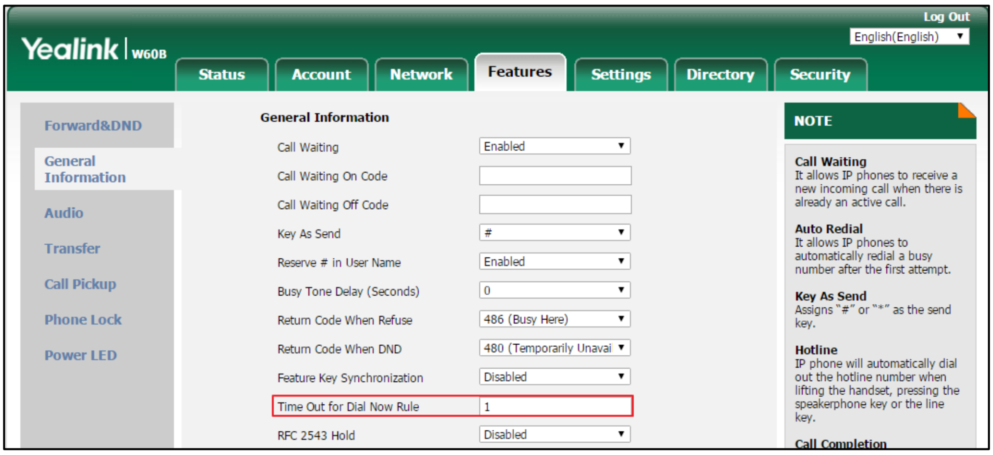
If you leave this field blank or enter 0, the dial now rule will apply to all accounts on the DECT IP phone.



4. Click **Add** to add the dial now rule.

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

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



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

Customizing Dial Now Template File

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

You can ask the distributor or Yealink FAE for dial now template. You can also obtain the dial now template online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the dial now template, refer to Obtaining Boot Files/Configuration Files/Resource Files on page 89.

When editing a dial now template, learn the following:

- <DialNow> indicates the start of a template and </DialNow> indicates the end of a template.
- When specifying the desired line(s) for the dial now rule, the valid values are 0 and line ID (0~8). Multiple line IDs are separated by commas.
- At most 100 rules can be added to the DECT IP phone.

The expression syntax in the dial now rule template is the same as that introduced in the section Dial Plan on page 186.

To customize a dial now template:

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

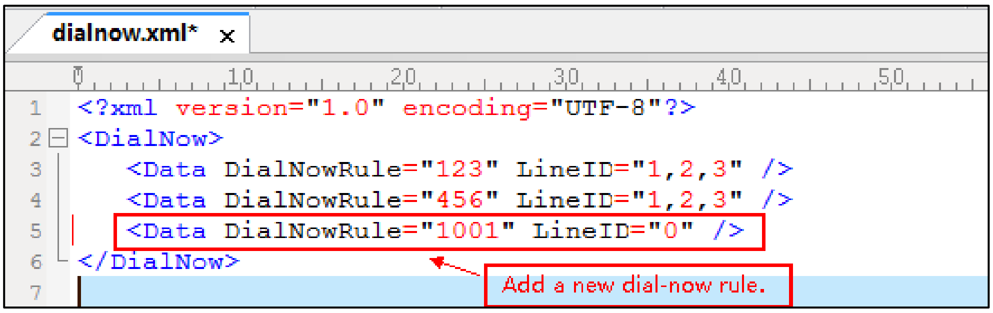
   For example:

   <Data DialNowRule="1001" LineID="0" />

   Where:

   DialNowRule="" specifies the dial now rule.

   LineID="" specifies the desired line(s) for this rule. When you leave it blank or enter 0, this dial now rule will apply to all lines.



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

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

Procedure

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

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the access URL of the dial now template. **Parameter:** dialplan_dialnow.url

Details of Configuration Parameter:

Parameter	Permitted Values	Default
dialplan_dialnow.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the dial now rule template file. **Example:** dialplan_dialnow.url = http://192.168.10.25/dialnow.xml During the auto provisioning process, the DECT IP phone connects to the provisioning server "192.168.10.25", and downloads the dial now rule file "dialnow.xml". **Note**: It is not applicable to W52H handset. **Web User Interface:** None **Handset User Interface:** None		

Area Code

Area codes are also known as Numbering Plan Areas (NPAs). They usually indicate geographical areas in one country. When entered numbers match the predefined area code rule, the DECT IP phone will automatically add the area code before the numbers when dialing out them. DECT IP phones only support one area code rule.

Procedure

Area code rule can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Create the area code rule and specify the maximum and minimum lengths of entered numbers. **Parameters:** dialplan.area_code.code dialplan.area_code.min_len dialplan.area_code.max_len dialplan.area_code.line_id
Web User Interface		Create the area code rule and specify the maximum and minimum lengths of entered

	numbers. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-areacode&q=load

Details of Configuration Parameters:

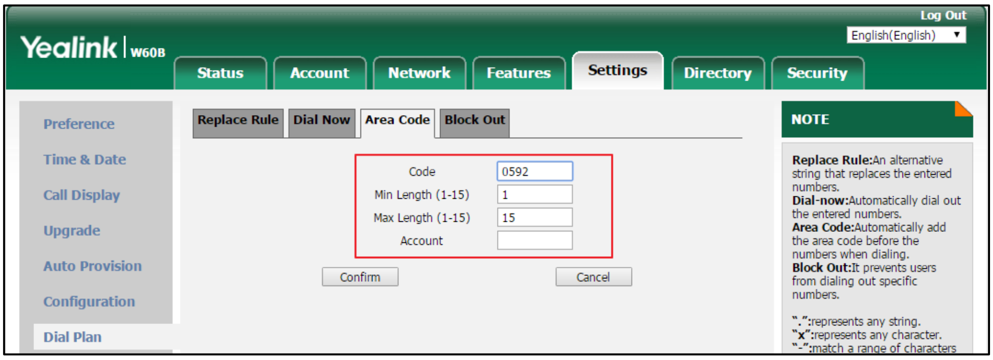
Parameters	Permitted Values	Default
dialplan.area_code.code	**String within 16 characters**	**Blank**
Description: Configures the area code to be added before the entered numbers when dialing out. **Example:** dialplan.area_code.code = 0592 **Note**: The length of the entered number must be between the minimum length configured by the parameter "dialplan.area_code.min_len" and the maximum length configured by the parameter "dialplan.area_code.max_len". **Web User Interface:** Settings->Dial Plan->Area Code->Code **Handset User Interface:** None		
dialplan.area_code.min_len	**Integer from 1 to 15**	**1**
Description: Configures the minimum length of the entered numbers. **Web User Interface:** Settings->Dial Plan->Area Code->Min Length (1-15) **Handset User Interface:** None		
dialplan.area_code.max_len	**Integer from 1 to 15**	**15**
Description: Configures the maximum length of the entered numbers. **Note**: The value must be larger than the minimum length. **Web User Interface:** Settings->Dial Plan->Area Code->Max Length (1-15) **Handset User Interface:**		

Parameters	Permitted Values	Default
None		
dialplan.area_code.line_id	**Integer from 0 to 8**	**Blank (for all lines)**
Description: Configures the desired line to apply the area code rule. The digit 0 stands for all lines. If it is left blank, the area code rule will apply to all lines on the DECT IP phone. **Example:** dialplan.area_code.line_id = 1 **Note:** Multiple line IDs are separated by commas. **Web User Interface:** Settings->Dial Plan->Area Code->Account **Handset User Interface:** None		

To configure an area code rule via web user interface:

1. Click on **Settings**->**Dial Plan**->**Area Code**.
2. Enter the desired values in the **Code**, **Min Length (1-15)** and **Max Length (1-15)** fields.
3. Enter the desired line ID in the **Account** field or leave it blank.

   If you leave this field blank or enter 0, the area code rule will apply to all accounts on the DECT IP phone.



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

Block Out

Block out rule prevents users from dialing out specific numbers. When entered numbers match the predefined block out rule, the LCD screen prompts "Forbidden Number". DECT IP phones support up to 10 block out rules.

Procedure

Block out rule can be created using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Create the block out rule for the DECT IP phone. **Parameters:** dialplan.block_out.number.X dialplan.block_out.line_id.X
Web User Interface		Create the block out rule for the DECT IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-blackout&q=load

Details of Configuration Parameters:

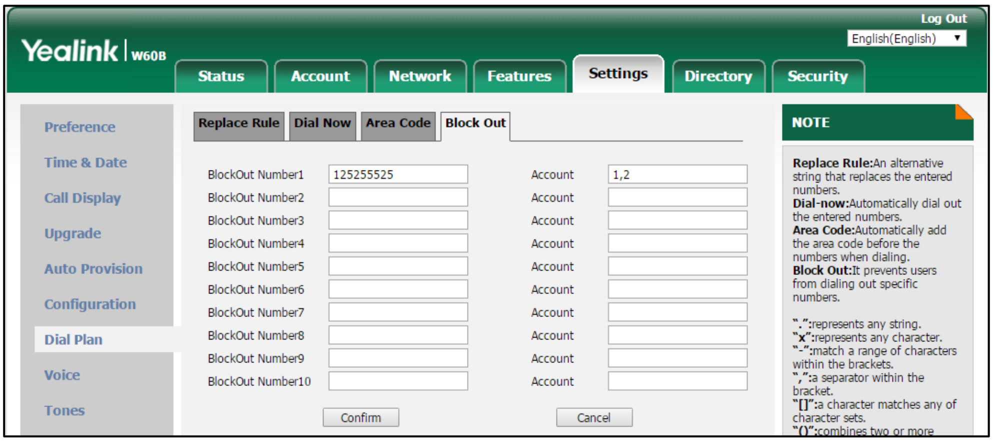
Parameters	Permitted Values	Default
dialplan.block_out.number.X (X ranges from 1 to 10)	**String within 32 characters**	**Blank**
Description: Configures the block out numbers. **Example:** dialplan.block_out.number.1 = 4321 When you dial the number “4321” on your phone, the dialing will fail and the LCD screen will prompt "Forbidden Number". **Web User Interface:** Settings->Dial Plan->Block Out->BlockOut NumberX **Handset User Interface:** None		
dialplan.block_out.line_id.X (X ranges from 1 to 10)	**Integer from 0 to 8**	**Blank (for all lines)**
Description: Configures the desired line to apply the block out rule. The digit 0 stands for all lines. If it is left blank, the block out rule will apply to all lines on the DECT IP phone. **Example:** dialplan.block_out.line_id.1 = 1,2,3 **Web User Interface:**		

Parameters	Permitted Values	Default
Settings->Dial Plan->Block Out->Account **Handset User Interface:** None		

To create a block out rule via web user interface:

1. Click on **Settings**->**Dial Plan**->**Block Out**.
2. Enter the desired value in the **BlockOut NumberX** field.
3. Enter the desired line ID in the **Account** field or leave it blank.

   If you leave this field blank or enter 0, the block out rule will apply to all accounts on the DECT IP phone.



4. Click **Confirm** to add the block out rule.

Emergency Dialplan

Yealink DECT IP phones support dialing emergency telephone numbers when the phone is locked. Due to the fact that the DECT IP phone must have a registered account or a configured SIP server, it may not meet the need of dialing emergency telephone number at any time.

Emergency dialplan allows users to dial the emergency telephone number (emergency services number) at any time when the DECT IP phone is powered on and has been connected to the network. It is available even if your phone keypad is locked or no SIP account is registered.

Note Contact your local phone service provider for available emergency numbers in your area.

Emergency Dial Plan

Users can configure the emergency dial plan on the phone (e.g., emergency number, emergency routing). The phone determines if this is an emergency number by checking the emergency dial plan configured on the phone. When placing an emergency call, the call is directed to the configured emergency server. Multiple emergency servers may need to be configured for emergency routing, avoiding that emergency calls couldn't get through because of the server failure. If the phone is not locked, it checks against the regular dial plan (refer to Dial Plan). If the phone is locked, it checks against the emergency dial plan.

Emergency Location Identification Number (ELIN)

The DECT IP phones support Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED). LLDP-MED allows the phone to use the location information, Emergency Location Identification Number (ELIN), sent by the switch, as a caller ID for making emergency calls. The outbound identity used in the P-Asserted-Identity (PAI) header of the SIP INVITE request is taken from the network using an LLDP-MED Emergency Location Identifier Number (ELIN). The administrator can customize the outbound identity. The custom outbound identity will be used if the phone fails to get the LLDP-MED ELIN value.

The following is an example of the PAI header:

P-asserted-identity: <sip: **1234567890**@abc.com > (where 1234567890 is the custom outbound identity.)

P-Access-Network-Info (PANI)

When placing an emergency call, the MAC address of the phone/connected switch should be added in the P-Access-Network-Info (PANI) header of the INVITE message. It helps the aid agency to immediately identify the caller's location, improving rescue efficiency.

The following is an example of the PANI header:

P-Access-Network-Info: IEEE-802.3; eth-location="**00:15:65:74:b1:6e**" (where 00156574B16E is the phone's MAC address.)

Procedure

Emergency dialplan can be configured using the configuration file.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the emergency dialplan. **Parameters:** dialplan.emergency.asserted_id_source dialplan.emergency.custom_asserted_id dialplan.emergency.server.X.address dialplan.emergency.server.X.port dialplan.emergency.server.X.transport_type dialplan.emergency.X.value dialplan.emergency.X.server_priority

Details of Configuration Parameters:

Parameters	Permitted Values	Default
dialplan.emergency.asserted_id_source	**ELIN or CUSTOM**	**ELIN**
Description: Configures the precedence of source of emergency outbound identities when placing an emergency call. If it is set to ELIN, the outbound identity used in the P-Asserted-Identity (PAI) header of the SIP INVITE request is taken from the network using an LLDP-MED Emergency Location Identifier Number (ELIN). The custom outbound identity configured by "dialplan.emergency.custom_asserted_id" will be used if the phone fails to get the LLDP-MED ELIN value. If it is set to CUSTOM, the custom outbound identity configured by "dialplan.emergency.custom_asserted_id" will be used; if the value of the parameter "dialplan.emergency.custom_asserted_id" is left blank, the LLDP-MED ELIN value will be used. **Note**: If the obtained LLDP-MED ELIN value is blank and no custom outbound identity, the PAI header will not be included in the SIP INVITE request. **Web User Interface:** None **Handset User Interface:** None		
dialplan.emergency.custom_asserted_id	**10-25 digits, SIP URI, or TEL URI**	**Blank**
Description: Configures the custom outbound identity when placing an emergency call. If using a TEL URI, for example, tel:+16045558000. The full URI is included in the P-Asserted-Identity (PAI) header (e.g., <tel:+16045558000>). If using a SIP URI, for example, sip:1234567890123@abc.com. The full URI is included in the P-Asserted-Identity (PAI) header and the address will be replaced by the emergency server (e.g., <sip:1234567890123@emergency.com>). If using a 10-25 digit number, for example, 1234567890. The SIP URI constructed from the number and SIP server (e.g., abc.com) is included in the P-Asserted-Identity (PAI) header (e.g., <sip:1234567890@abc.com>). **Web User Interface:** None **Handset User Interface:**		

Parameters	Permitted Values	Default
None		
dialplan.emergency.server.X.address (X ranges from 1 to 3)	**IP address or domain name**	**Blank**
Description: Configures the IP address or domain name of the emergency server X to be used for routing calls. **Note**: If the account is registered successfully or failed (the account information has been configured), the emergency calls will be dialed using the following priority: SIP server>emergency server; if the account is not registered, the emergency server will be used. **Web User Interface:** None **Handset User Interface:** None		
dialplan.emergency.server.X.port (X ranges from 1 to 3)	**Integer from 1 to 65535**	**5060**
Description: Configures the port of emergency server X to be used for routing calls. **Web User Interface:** None **Handset User Interface:** None		
dialplan.emergency.server.X.transport_type (X ranges from 1 to 3)	**0, 1, 2 or 3**	**0**
Description: Configures the transport method the DECT IP phone uses to communicate with the emergency server X. **0**-UDP **1**-TCP **2**-TLS **3**-DNS-NAPTR **Web User Interface:** None **Handset User Interface:**		

Parameters	Permitted Values	Default
None		
dialplan.emergency.X.value (X ranges from 1 to 255)	**number or SIP URI**	**Refer to the following content**
Description: Configures the emergency number to use on your DECT IP phone so a caller can contact emergency services in the local area when required. **Default**: When X = 1, the default value is 911; When X = 2-255, the default value is Blank. **Web User Interface:** None **Handset User Interface:** None		
dialplan.emergency.X.server_priority (X ranges from 1 to 255)	**a combination of digits 1, 2 and 3**	**1, 2, 3**
Description: Configures the priority for the emergency servers to be used. The digits are separated by commas. The servers to be used in the order listed (left to right). The DECT IP phone tries to send the INVITE request to the emergency server with higher priority. If the emergency server with higher priority does not respond correctly to the INVITE, then the phone tries to make the call using the emergency server with lower priority, and so forth. The DECT IP phone tries to send the INVITE request to each emergency server for three times. **Example**: dialplan.emergency.1.server_priority = 2, 1, 3 It means the DECT IP phone sends the INVITE request to the emergency server 2 first. If the emergency server 2 does not respond correctly to the INVITE, then tries to make the call using the emergency server 1. If the emergency server 1 does not respond correctly to the INVITE, then tries to make the call using the emergency server 3. The DECT IP phone tries to send the INVITE request to each emergency server for three times. **Note**: If the IP address of the emergency server with higher priority has not been configured, the emergency server with lower priority will be used. If the account is registered successfully or failed (the account information has been configured), the		

Parameters	Permitted Values	Default
emergency calls will be dialed using the following priority: SIP server>emergency server; if the account is not registered, the emergency server will be used. **Web User Interface:** None **Handset User Interface:** None		

Off Hook Hot Line Dialing

For security reasons, DECT IP phones support off hook hot line dialing feature, which allows the phone to first dial out the pre-configured number when the user dials out a call using the account with this feature enabled. The SIP server may then prompt the user to enter an activation code for call service. Only if the user enters a valid activation code, the DECT IP phone will use this account to dial out a call successfully.

Off hook hot line dialing feature is configurable on a per-line basis and depends on support from a SIP server.

Note

> Off hook hot line dialing feature limits the call-out permission of this account and disables the hotline feature.
>
> The server actions may vary from different servers.
>
> It is also applicable to the IP call and intercom call.

Procedure

Off hook hot line dialing can be configured using the configuration file.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure off hook hot line dialing feature. **Parameter:** account.X.auto_dial_enable
		Specify the number that the phone first dials out. **Parameter:** account.X.auto_dial_num

Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>account.X.auto_dial_enable
(X ranges from 1 to 8)</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables the DECT IP phone to first dial out a pre-configured number when a user dials out a call using account X.
0-Disabled
1-Enabled
If it is set to 1 (Enabled), the phone will first dial out the pre-configured number (configured by the parameter "account.X.auto_dial_num") when a user dials out a call using account X.
Note: The server may prompt the user to enter an activation code to use this account for call service. This feature requires support from the SIP server.
Web User Interface:
None
Handset User Interface:
None</td></tr>
<tr><td>account.X.auto_dial_num
(X ranges from 1 to 8)</td><td>String within 32 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the number that the DECT IP phone first dials out when a user dials out a call using account X.
Note: It works only if the value of the parameter "account.X.auto_dial_enable" is set to 1 (Enabled).
Web User Interface:
None
Handset User Interface:
None</td></tr>
</table>

Local Directory

You can store the frequently used contacts in the handset's local directory, where names and numbers can be freely added, deleted and edited. You can store up to 100 contacts per handset, each with a name, a mobile number and an office number. Yealink DECT IP phones support both *.xml and *.csv format contact files.

Procedure

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

Configuration File	y000000000077.cfg	Specify the access URL of the directory template file. **Parameter:** handset.X.contact_list.url
Local	Web User Interface	Configure the Directory. **Navigate to**: http://<phoneIPAddress>/servlet?p=contactsbasic&q=load

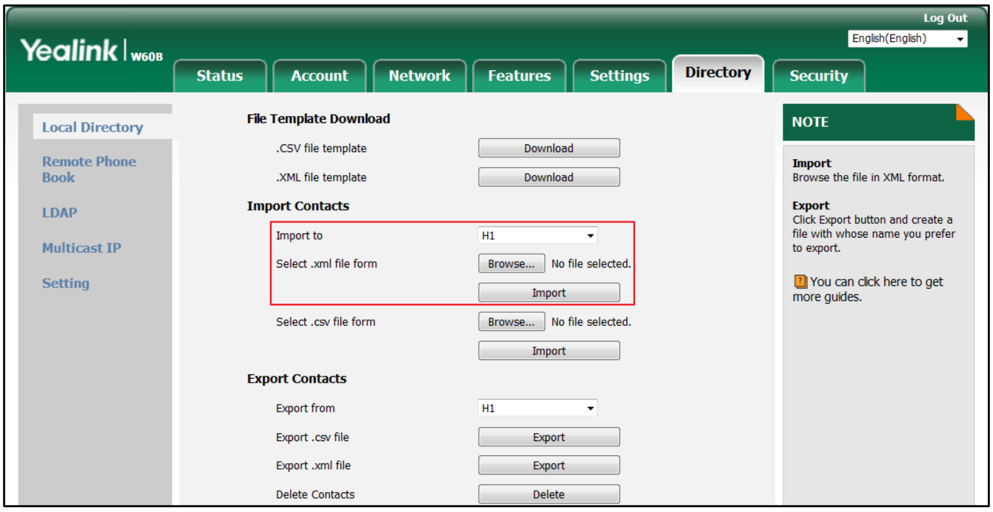
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
handset.X.contact_list.url (X ranges from 1 to 8)	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the contact file of handset X. The format of the file must be *.xml. **Example:** handset.1.contact_list.url= http://192.168.1.20/favorite_setting.xml During the auto provisioning process, the IP DCET phone connects to the provisioning server "192.168.1.20", and downloads the directory file "favorite_setting.xml". **Web User Interface:** Directory->Local Directory->Import Contacts **Handset User Interface:** None		

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

1. Click on **Directory**->**Local Directory**.
2. Select the desired handset from the pull-down list of **Import to**.

3. Click **Browse** to locate a contact list file (the file format must be *.xml) from your local system.



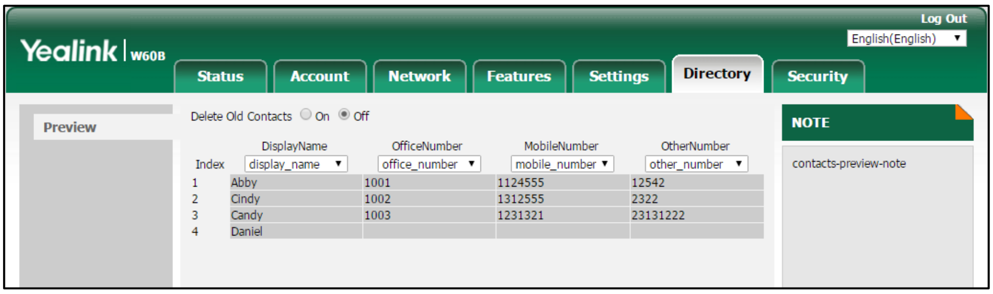
4. Click **Import** to import the contact list.
5. Click **OK** to complete importing the contact list.

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

1. Click on **Directory**->**Local Directory**.
2. Select the desired handset from the pull-down list of **Import to**.
3. Click **Browse** to locate a contact list file (the file format must be *.csv) from your local system.
4. Click **Import** to import the contact list.
5. (Optional.) Mark the **On** radio box in the **Delete Old Contacts** field.

   It will delete all existing contacts while importing the contact list.
6. Select the contact information you want to import into the local directory from the pull-down list of **Index**.

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



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

To export a contact list via web user interface:

1. Click on **Directory**->**Local Directory**.
2. In **Export Contacts** block, click **Export** from **Export.xml file** (or **Export.csv file**) field.

3. Click **Save** to save the contact list to your local system.

To delete contacts via web user interface:

1. Click on **Directory**->**Local Directory**.
2. In **Export Contacts** block, click **Delete** from the **Delete Contacts** field.

Customizing a Directory Template File

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. For more information on obtaining the directory template, refer to Obtaining Boot Files/Configuration Files/Resource Files on page 89.

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

Element	Values	Description
root_contact	no	Contact list's root element.
contact	no	Contact's root element.
display_name	String	An element of contact. Contact name. **Note**: This value cannot be blank or duplicated.
office_number	String	Office number of the contact.
mobile_number	String	Mobile number of the contact.
other_number	String	Other number of the contact.

Customizing a directory template:

1. Open the template file using an ASCII editor.
2. For each directory list that you want to configure, edit the corresponding string in the file. For example, configure the local directory list, edit the values within double quotes in the following strings:

   <contact display_name="" office_number="" mobile_number="" other_number=“”/>

```
<?xml version="1.0" encoding="utf-8"?>
<root_contact>
    <contact display_name="" office_number="" mobile_number="" other_number="" />

</root_contact>
```

3. Save the change and place this file to the provisioning server (e.g., 192.168.1.20).
4. Specify the access URL of the custom directory template file in the configuration files (e.g., handset.1.contact_list.url = http://192.168.1.20/favorite_setting.xml).

Search Source List In Dialing

Search source list in dialing allows the DECT IP phone to automatically search entries from the search source list based on the entered string, and display results on the pre-dialing/dialing screen. The user can select the desired entry to dial out quickly.

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

It is not applicable to W52H handset.

Customizing a Super Search Template File

You can ask the distributor or Yealink FAE for super search template. You can also obtain the super search template online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the super search template, refer to Obtaining Boot Files/Configuration Files/Resource Files on page 89.

The following table lists meaning of each variable in the super search template file:

Element	Attribute	Description
root_super_search	No	File root element
Item	No	Super search list's root element
id_name	local_directory_search calllog_search remote_directory_search ldap_search BroadSoft_directory_search	The directory list (For example, "local_directory_search" for the local directory list). **Note**: Do not edit this field.
display_name	Local Contacts History Remote Phonebook LDAP Network Directories	The display name of the directory list. **Note**: We recommend you do not edit this field. Network Directories list is hidden for DECT IP phones in neutral firmware, which are designed for the BroadWorks environment.
priority	1, 2, 3, 4 and 5. 1 is the highest priority, 5 is the lowest.	The priority of the search results.
enable	0/1, **0**: Disabled	Enable or disable the DECT IP phone to search the desired

Element	Attribute	Description
	1: Enabled	directory list.

Customizing a super search template:

1. Open the template file using an ASCII editor.
2. For each directory list that you want to configure, edit the corresponding string in the file. For example, configure the local directory list, edit the values within double quotes in the following strings:

   <item id_name="local_directory_search" display_name="Local Contacts" priority="1" enable="1"/>

```
<root_super_search>
  <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="1" />
  <item id_name="remote_directory_search" display_name="Remote Phonebook" priority="3" enable="0" />
  <item id_name="ldap_search" display_name="LDAP" priority="4" enable="0" />
  <item id_name="BroadSoft_directory_search" display_name="Network Directories" priority="5" enable="0" />
</root_super_search>
```

3. Save the change and place this file to the provisioning server (e.g., 192.168.1.20).
4. Specify the access URL of the custom super search template file in the configuration files (e.g., super_search.url = http://192.168.1.20/super_search.xml).

Procedure

Search source list in dialing can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Specify the access URL of the super search template file. **Parameter:** super_search.url
Web User Interface		Configure the search source list in dialing. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-favorite&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
super_search.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the super search template file. **Example**:		

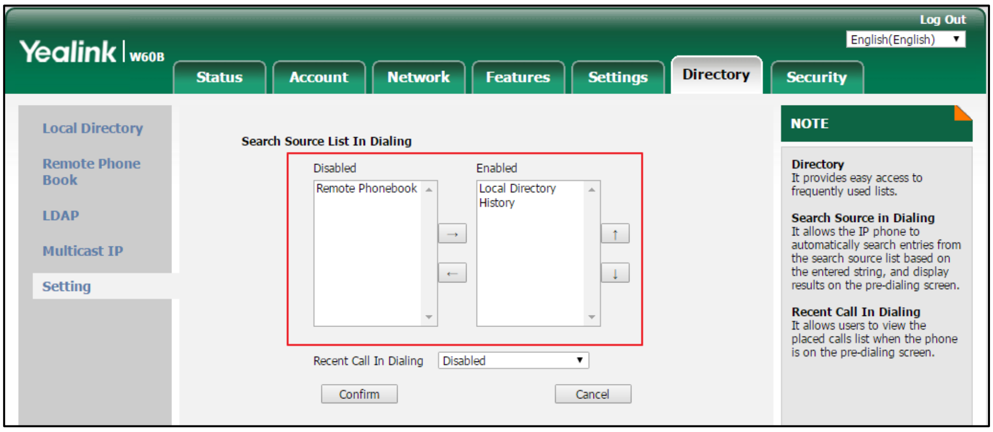
Parameter	Permitted Values	Default
super_search.url = http://192.168.1.20/super_search.xml During the auto provisioning process, the DECT IP phone connects to the provisioning server "192.168.1.20", and downloads the super search template file "super_search.xml". **Note:** It is not applicable to W52H handset. **Web User Interface:** Directory->Setting->Search Source List In Dialing **Handset User Interface:** None		

To configure search source list in dialing via web user interface:

1. Click on **Directory**->**Setting**.
2. In the **Search Source List In Dialing** block, select the desired list from the **Disabled** column and then click →.

   The selected list appears in the **Enabled** column.
3. Repeat the step 2 to add more lists to the **Enabled** column.
4. To remove a list from the **Enabled** column, select the desired list and then click ←.
5. To adjust the display order of search results, select the desired list and then click ↑ or ↓.

   The LCD screen displays the search results in the adjusted order.



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

Save Call Log

DECT IP phones record and maintain phone events to a call log, also known as a call list. The call log contains call information such as remote party identification, time and date of the call, and call duration. It can be used to redial previous outgoing calls, return incoming calls, and save contact information from call log lists to the contact directory.

The DECT IP phones maintain a local call log. Call log consists of four lists: All Calls, Missed Calls, Placed Calls and Received Calls. Each call log list supports up to 100 entries. To store call information, you must enable save call log feature in advance.

Procedure

Call log can be configured using the following methods.

<table>
<tr><td rowspan="2">Central Provisioning
(Configuration File)</td><td rowspan="2">y000000000077.cfg</td><td>Configure call log feature.
Parameter:
features.save_call_history</td></tr>
<tr><td>Configure call log display method.
Parameter:
features.cumulative_display_call_lo
g.enable</td></tr>
<tr><td colspan="2">Web User Interface</td><td>Configure call log feature.
Navigate to:
http://<phoneIPAddress>/servlet?
p=features-general&q=load</td></tr>
<tr><td colspan="2">Handset User Interface</td><td>Configure call log feature.</td></tr>
</table>

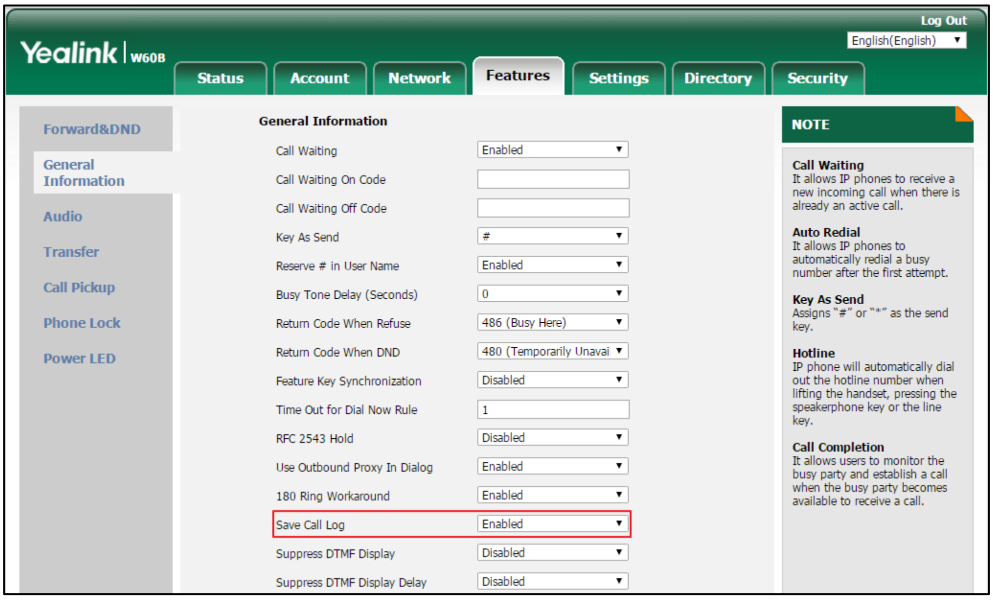
Details of the Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>features.save_call_history</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables the DECT IP phone to save the call log.
0-Disabled
1-Enabled
If it is set to 0 (Disabled), the DECT IP phone cannot log the missed calls, placed calls and received calls in the call log lists.
Web User Interface:
Features->General Information->Save Call Log
Handset User Interface:
None</td></tr>
<tr><td>features.cumulative_display_call_log.enable</td><td>0 or 1</td><td>1</td></tr>
</table>

Parameters	Permitted Values	Default
Description: Enables or disables the DECT IP phone to display the same call log of a day cumulatively. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the same call log will display in a list respectively. If it is set to 1 (Enabled), the same call log of a day will display cumulatively. **Web User Interface:** None **Handset User Interface:** None		

To configure call log feature via web user interface:

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



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

Call Waiting

Call waiting allows DECT IP phones to receive a new incoming call when there is already an active call. The new incoming call is presented to the user visually on the LCD screen.

Call waiting tone allows the DECT IP phone to play a short tone, to remind the user audibly of a new incoming call during conversation. Call waiting tone works only if call waiting is enabled. You can customize call waiting tone or select specialized tone sets (vary from country to country) for your DECT IP phone. For more information, refer to Tones on page 361.

The call waiting on code and call waiting off code configured on DECT IP phones are used to activate/deactivate the server-side call waiting feature. They may vary on different servers.

Procedure

Call waiting and call waiting tone can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure call waiting and call waiting tone. **Parameters:** call_waiting.enable call_waiting.tone call_waiting.on_code call_waiting.off_code
Web User Interface		Configure call waiting. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
		Configure call waiting tone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-audio&q=load
Handset User Interface		Configure call waiting and call waiting tone.

Details of Configuration Parameters:

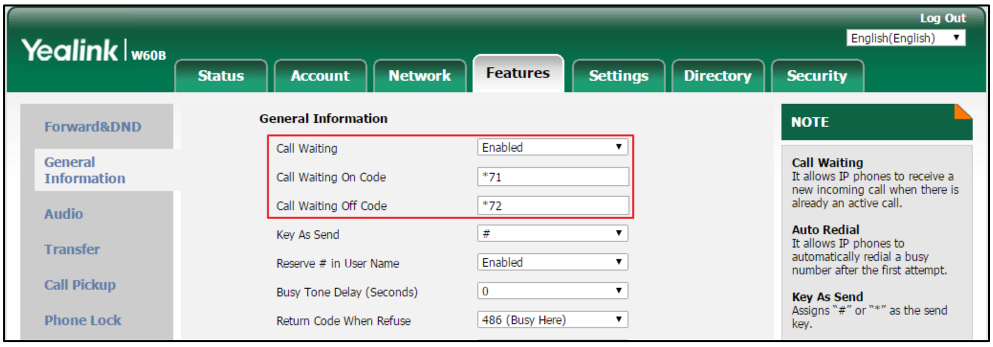
Parameters	Permitted Values	Default
call_waiting.enable	**0 or 1**	**1**
Description: Enables or disables call waiting feature. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), a new incoming call is automatically rejected by the DECT IP phone with a busy signal (configured by the parameter "features.normal_refuse_code") while during a call. If it is set to 1 (Enabled), the LCD screen will present a new incoming call while during a call. In both cases, users can put an active call on hold to make outgoing calls. **Web User Interface:** Features->General Information->Call Waiting **Handset User Interface:**		

Parameters	Permitted Values	Default
OK->Call Features->Call Waiting->Status		
call_waiting.tone	**0 or 1**	**1**
Description: Enables or disables the DECT IP phone to play the call waiting tone when the DECT IP phone receives an incoming call during a call. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the DECT IP phone will perform an audible indicator when receiving a new incoming call during a call. **Note**: It works only if the value of the parameter "call_waiting.enable" is set to 1 (Enabled). **Web User Interface:** Features->Audio->Call Waiting Tone **Handset User Interface:** OK->Call Features->Call Waiting->Tone		
call_waiting.on_code	**String within 32 characters**	**Blank**
Description: Configures the call waiting on code to activate the server-side call waiting feature. The DECT IP phone will send the call waiting on code to the server when you activate call waiting feature on the DECT IP phone. **Example:** call_waiting.on_code = *71 **Web User Interface:** Features->General Information->Call Waiting On Code **Handset User Interface:** None		
call_waiting.off_code	**String within 32 characters**	**Blank**
Description: Configures the call waiting off code to deactivate the server-side call waiting feature. The DECT IP phone will send the call waiting off code to the server when you deactivate call waiting feature on the DECT IP phone. **Example:** call_waiting.off_code = *72		

Parameters	Permitted Values	Default
Web User Interface: Features->General Information->Call Waiting Off Code **Handset User Interface:** None		

To configure call waiting via web user interface:

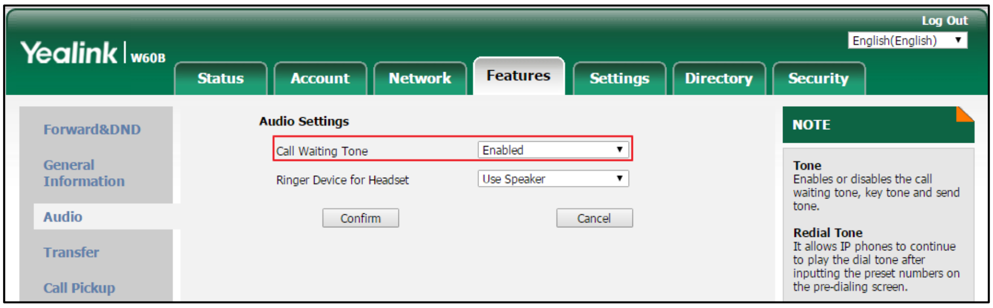
1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Call Waiting**.
3. (Optional.) Enter the call waiting on code in the **Call Waiting On Code** field.
4. (Optional.) Enter the call waiting off code in the **Call Waiting Off Code** field.



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

To configure call waiting tone via web user interface:

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



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

To configure call waiting feature via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Call Features**->**Call Waiting**.
3. Press ◀ or ▶ to select the desired value from the **Status** field.

4. Press ◀ or ▶ to select the desired value from the **Tone** field.
5. Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

Auto Answer

Auto answer allows DECT IP phones to automatically answer an incoming call by picking up the handset from the charger cradle without having to press the off-hook key. DECT IP phones will not automatically answer the incoming call during a call even if auto answer is enabled. The auto answer feature works only if the handset is placed in the charger cradle.

Procedure

Auto answer can be configured using the following methods.

Configuration File	y000000000077.cfg	Configure auto answer. **Parameter:** custom.handset.auto_answer.enable
Handset User Interface		Configure auto answer.

Details of Configuration Parameter:

Parameter	Permitted Values	Default
custom.handset.auto_answer.enable	**0 or 1**	**1**
Description: Enables or disables a user to answer incoming calls by lifting the handset from the charger cradle without having to press the off-hook key. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the DECT IP phone can automatically answer an incoming call. **Note:** It works if the handset is placed in the charger cradle and the parameter “auto_provision.handset_configured.enable” is set to 1 (Enabled). **Web User Interface:** None **Handset User Interface:** OK->Settings->Telephony->Auto Answer		

To configure auto answer via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Telephony**->**Auto Answer**.
3. Press the **Change** soft key to check or uncheck the **Auto Answer** checkbox.

Allow IP Call

Allow IP Call feature allows DECT IP phones to receive or place an IP address call. You can neither receive nor place an IP address call if allow IP call feature is disabled.

Procedure

Allow IP call can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure allow IP call. **Parameter:** features.direct_ip_call_enable
Web User Interface		Configure allow IP call. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

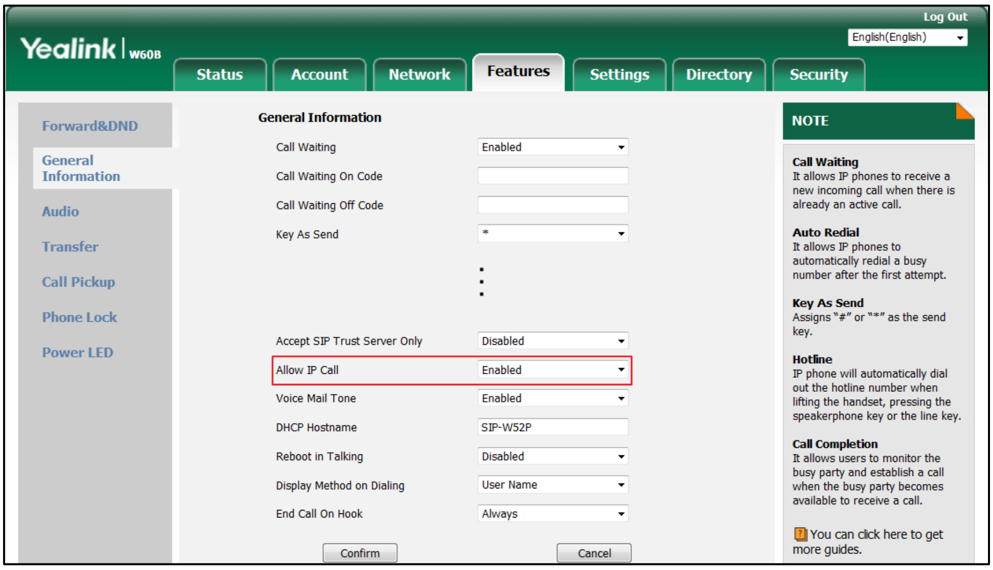
Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.direct_ip_call_enable	**0 or 1**	**1**
Description: Enables or disables allow IP address call. **0**-Disabled **1**-Enabled **Note**: If you want to receive an IP address call, make sure the value of the parameter "sip.trust_ctrl" is set to 0 (Disabled). **Web User Interface:** Features->General Information->Allow IP Call **Handset User Interface:** None		

To configure allow IP call feature via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **Allow IP Call**.



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

Accept SIP Trust Server Only

Accept SIP trust server only enables the DECT IP phones to only accept the SIP message from your SIP server and outbound proxy server. It can prevent the phone receiving ghost calls from random numbers like 100, 1000, etc. To stop this from happening, you also need to disable allow IP call feature. For more information on allow IP call, refer to Allow IP Call on page 220.

Procedure

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

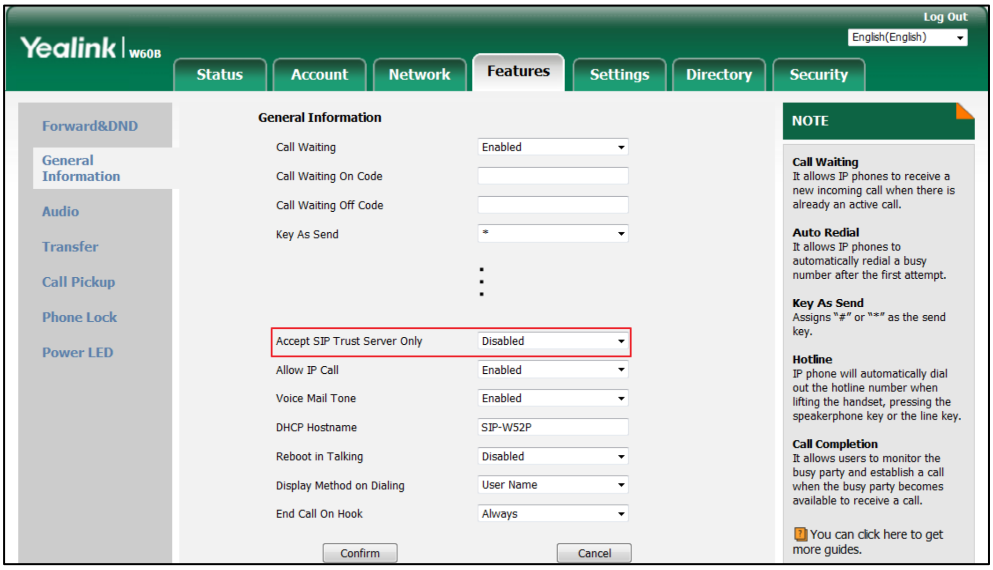
Central Provisioning (Configuration File)	y000000000077.cfg	Configure accept SIP trust server only. **Parameter:** sip.trust_ctrl
Web User Interface		Configure accept SIP trust server only. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
sip.trust_ctrl	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to only accept the SIP message from the SIP server and outbound proxy server. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Accept SIP Trust Server Only **Handset User Interface:** None		

To configure accept SIP trust server only feature via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Accept SIP Trust Server Only**.



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

Anonymous Call

Anonymous call allows the caller to conceal the identity information displayed on the callee's screen. The callee's phone LCD screen prompts an incoming call from anonymity. Anonymous call is configurable on a per-line basis.

Example of anonymous SIP header:

```
Via: SIP/2.0/UDP 10.3.20.14:5060;branch=z9hG4bK3074920774
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=131654239
To: <sip:1006@10.2.1.48:5060>
Call-ID: 0_288363101@10.3.20.14
CSeq: 1 INVITE
Contact: <sip:1009@10.3.20.14:5060>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH,
UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink W60B 77.81.0.10
Allow-Events: talk,hold,conference,refer,check-sync
P-Preferred-Identity: <sip:1009@10.2.1.48>
Privacy: id
Content-Length: 302
```

The anonymous call on code and anonymous call off code configured on DECT IP phones are used to activate/deactivate the server-side anonymous call feature. They may vary on different servers. Send Anonymous Code feature allows DECT IP phones to send anonymous on/off code to the server.

Procedure

Anonymous call can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure anonymous call. **Parameters:** features.provision_anonymous_call_on_gui.enable account.X.anonymous_call account.X.send_anonymous_code account.X.anonymous_call_oncode account.X.anonymous_call_offcode
Web User Interface		Configure anonymous call. **Navigate to**: http://<phoneIPAddress>/servlet?p=acc

	ount-basic&q=load&acc=0
Handset User Interface	Configure anonymous call.

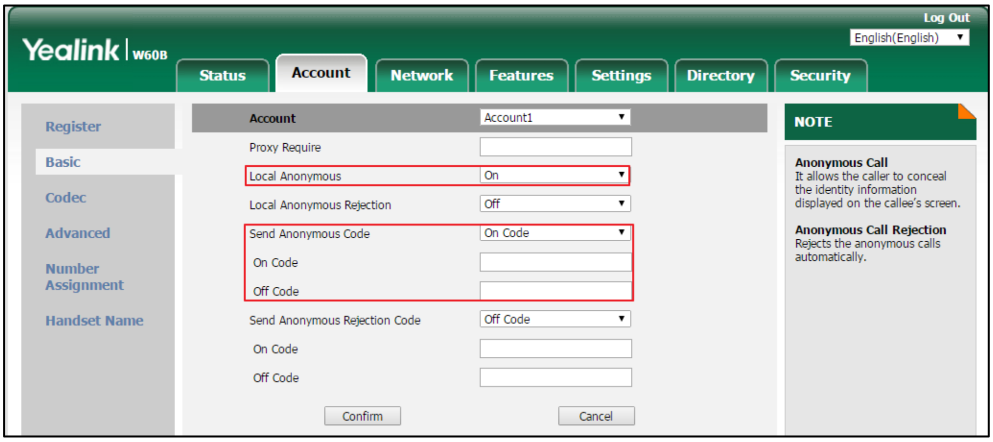
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.provision_anonymous_call_on_gui.enable	**0 or 1**	**1**
Description: Enables or disables to display the anonymous call setting on the handset. **0-**Disabled **1-**Enabled **Web User Interface:** None **Handset User Interface:** None		
account.X.anonymous_call (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Triggers the anonymous call feature to on or off for account X. **0**-Off **1**-On If it is set to 1 (On), the DECT IP phone will block its identity from showing up to the callee when placing a call. The callee's phone LCD screen presents anonymous instead of the caller's identity. **Web User Interface:** Account->Basic->Local Anonymous **Handset User Interface:** OK->Call Features->Anonymous Call->Line X->Status (only display when the parameter "features.provision_anonymous_call_on_gui.enable" is set to 1 (Enabled))		
account.X.send_anonymous_code (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Configures the DECT IP phone to send anonymous on/off code to activate/deactivate the server-side anonymous call feature for account X. **0**-Off Code **1**-On Code		

Parameters	Permitted Values	Default
If it is set to 0 (Off Code), the DECT IP phone will send anonymous off code to the server when you activate/deactivate the anonymous call feature. If it is set to 1 (On Code), the DECT IP phone will send anonymous on code to the server when you activate/deactivate the anonymous call feature. **Web User Interface:** Account->Basic->Send Anonymous Code **Handset User Interface:** None		
account.X.anonymous_call_oncode (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the anonymous call on code to activate the server-side anonymous call feature for account X. **Example:** account.1.anonymous_call_oncode = *72 **Note:** It works only if the value of the parameter "account.X.send_anonymous_code" is set to 1 (On Code). **Web User Interface:** Account->Basic->Send Anonymous Code->On Code **Handset User Interface:** None		
account.X.anonymous_call_offcode (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the anonymous call off code to deactivate the server-side anonymous call feature for account X. **Example:** account.1.anonymous_call_offcode = *73 **Note:** It works only if the value of the parameter "account.X.send_anonymous_code" is set to 0 (Off Code). **Web User Interface:** Account->Basic->Send Anonymous Code->Off Code **Handset User Interface:** None		

To configure anonymous call via web user interface:

1. Click on **Account**->**Basic**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Local Anonymous**.
4. Select the desired value from the pull-down list of **Send Anonymous Code**.
5. (Optional.) Enter the anonymous call on code in the **On Code** field.
6. (Optional.) Enter the anonymous call off code in the **Off Code** field.



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

To configure anonymous call feature for a specific line via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Call Features**->**Anonymous Call**.

   The LCD screen displays the outgoing lines currently assigned to the handset. The default outgoing line is highlighted and followed by a left arrow.
3. Press ▲ or ▼ to highlight the desired line, and then press the **OK** soft key.
4. Press ◀ or ▶ to select the desired value from the **Status** field.
5. Press the **OK** soft key to accept the change.

Anonymous Call Rejection

Anonymous call rejection allows DECT IP phones to automatically reject incoming calls from callers whose identity has been deliberately concealed. The anonymous caller's phone LCD screen presents "Anonymity Disallowed". Anonymous call rejection is configurable on a per-line basis.

The anonymous call rejection on code and anonymous call rejection off code configured on DECT IP phones are used to activate/deactivate the server-side anonymous call rejection feature. They may vary on different servers. Send Anonymous Rejection Code feature allows DECT IP phones to send anonymous call rejection on/off code to the server.

Procedure

Anonymous call rejection can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure anonymous call rejection. **Parameters:** account.X.reject_anonymous_call account.X.send_anonymous_rejection_code account.X.anonymous_reject_oncode account.X.anonymous_reject_offcode
Web User Interface		Configure anonymous call rejection. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0
Handset User Interface		Configure anonymous call rejection.

Details of Configuration Parameters:

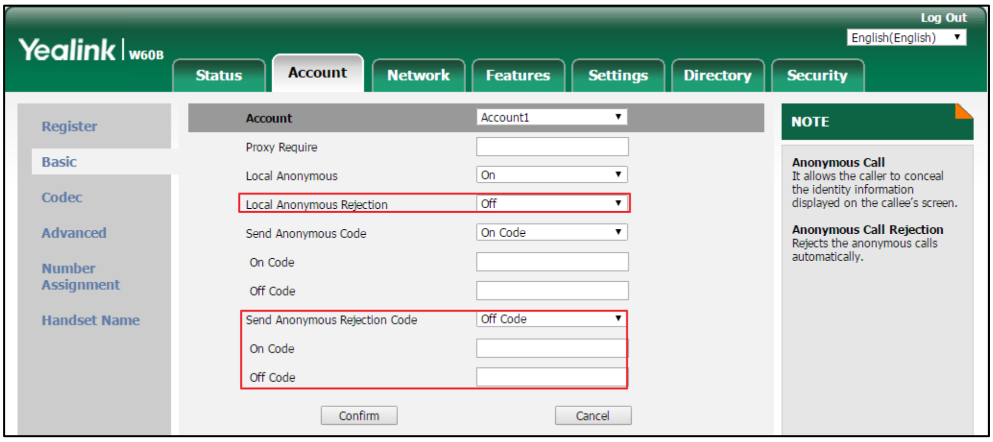
Parameters	Permitted Values	Default
account.X.reject_anonymous_call (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Triggers the anonymous call rejection feature to on or off for account X. **0**-Off **1**-On If it is set to 1 (On), the DECT IP phone will automatically reject incoming calls from users enabled anonymous call feature. The anonymous user's phone LCD screen presents "Forbidden". **Web User Interface:** Account->Basic->Local Anonymous Rejection **Handset User Interface:** OK->Call Features->Anon.Call Rejection->Line X->Status		
account.X.send_anonymous_rejection_code (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Configures the DECT IP phone to send anonymous rejection on/off code to activate/deactivate the server-side anonymous call rejection feature for account X.		

Parameters	Permitted Values	Default
0-Off Code **1**-On Code If it is set to 0 (Off Code), the DECT IP phone will send anonymous rejection off code to the server when you deactivate the anonymous call rejection feature. If it is set to 1 (On Code), the DECT IP phone will send anonymous rejection on code to the server when you activate the anonymous call rejection feature. **Web User Interface:** Account->Basic->Send Anonymous Rejection Code **Handset User Interface:** None		
account.X.anonymous_reject_oncode (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the anonymous call rejection on code to activate the server-side anonymous call rejection feature for account X. **Example:** account.1.anonymous_reject_oncode = *74 **Note:** It works only if the value of the parameter "account.X.send_anonymous_rejection_code" is set to 1 (On Code). **Web User Interface:** Account->Basic->Send Anonymous Rejection Code->On Code **Handset User Interface:** None		
account.X.anonymous_reject_offcode (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the anonymous call rejection off code to deactivate the server-side anonymous call rejection feature for account X. **Example:** account.1.anonymous_reject_offcode = *75 **Note:** It works only if the value of the parameter "account.X.send_anonymous_rejection_code" is set to 0 (Off Code). **Web User Interface:** Account->Basic->Send Anonymous Rejection Code->Off Code **Handset User Interface:**		

Parameters	Permitted Values	Default
None		

To configure anonymous call rejection via web user interface:

1. Click on **Account**->**Basic**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Local Anonymous Rejection**.
4. Select the desired value from the pull-down list of **Send Anonymous Rejection code**.
5. (Optional.) Enter the send anonymous rejection on code in the **On Code** field.
6. (Optional.) Enter the send anonymous rejection off code in the **Off Code** field.



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

To configure anonymous call rejection feature for a specific line via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Anon.Call Rejection**.

   The LCD screen displays the incoming lines currently assigned to the handset.
3. Press ▲ or ▼ to highlight the desired line, and then press the **OK** soft key.
4. Press ◀ or ▶ to select the desired value from the **Status** field.
5. Press the **OK** soft key to accept the change.

Do Not Disturb (DND)

DND allows DECT IP phones to ignore incoming calls. DND feature can be configured on a phone or a per-line basis depending on the DND mode.

The DND on code and DND off code configured on DECT IP phones are used to activate/deactivate the server-side DND feature. They may vary on different servers.

Procedure

DND can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure DND feature. **Parameters:** account.X.dnd.enable account.X.dnd.on_code account.X.dnd.off_code
	y000000000077.cfg	Configure the DND refuse code. **Parameter:** features.dnd_refuse_code
Web User Interface		Configure DND feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-forward&q=load
Handset User Interface		Configure DND feature.

Details of Configuration Parameters:

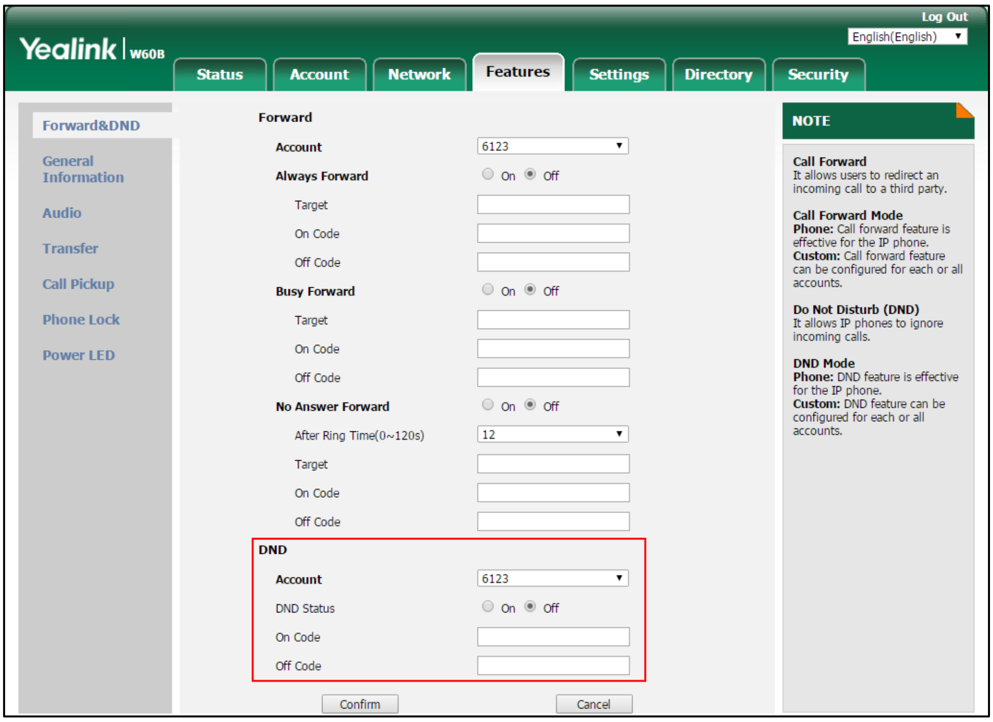
Parameters	Permitted Values	Default
account.X.dnd.enable (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Triggers DND feature to on or off for account X. **0**-Off **1**-On If it is set to 1 (On), the DECT IP phone will reject incoming calls on account X. **Web User Interface:** Features->Forward&DND->DND->DND Status **Handset User Interface:** OK->Call Features->Do Not Disturb->LineX->Status		
account.X.dnd.on_code (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the DND on code to activate the server-side DND feature for account X. The DECT IP phone will send the DND on code to the server when you activate DND feature for account X on the DECT IP phone.		

Parameters	Permitted Values	Default
Example: account.1.dnd.on_code = *73 **Web User Interface:** Features->Forward&DND->DND->On Code **Handset User Interface:** None		
account.X.dnd.off_code (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the DND off code to deactivate the server-side DND feature for account X. The DECT IP phone will send the DND off code to the server when you deactivate DND feature for account X on the DECT IP phone. **Example:** account.1.dnd.off_code = *74 **Web User Interface:** Features->Forward&DND->DND->Off Code **Handset User Interface:** None		
features.dnd_refuse_code	**404, 480, 486 or 603**	**480**
Description: Configures a return code and reason of SIP response messages when rejecting an incoming call by DND. A specific reason is displayed on the caller's phone LCD screen. **404**-Not Found **480**-Temporarily Unavailable **486**-Busy Here **603**-Decline If it is set to 486 (Busy here), the caller's phone LCD screen will display the reason "Busy here" when the callee enables DND feature. **Web User Interface:** Features->General Information->Return Code When DND **Handset User Interface:** None		

To configure DND for a specific line via web user interface:

1. Click on **Features**->**Forward&DND**->**DND**.

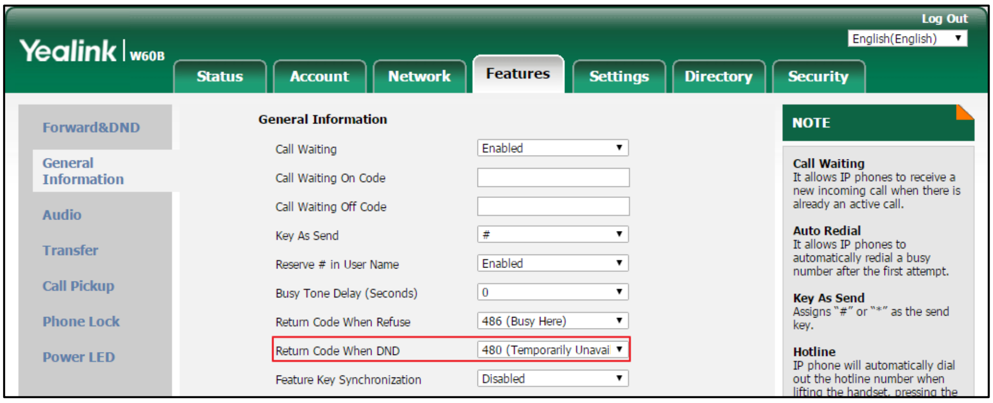
2. Select the desired line from the pull-down list of **Account** field.
3. Mark the desired radio box in the **DND Status** field.
4. Enter the DND on code and off code in the **DND On Code** and **DND Off Code** field respectively.



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

To configure return code when DND via web user interface:

1. Click on **Features**->**General Information.**
2. Select the desired value from the pull-down list of **Return Code When DND**.



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

To activate DND mode for a specific line via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Call Features**->**Do Not Disturb**.

The LCD screen displays the incoming lines currently assigned to the handset.

3. Press ▲ or ▼ to highlight the desired line, and then press the **OK** soft key.
4. Press ◀ or ▶ to select **Enabled** from the **Status** field.
5. Press the **OK** soft key to accept the change.

Busy Tone Delay

Busy tone is audible to the other party, indicating that the call connection has been broken when one party releases a call. Busy tone delay can define a period of time during which the busy tone is audible.

Procedure

Busy tone delay can be configured using the following methods.

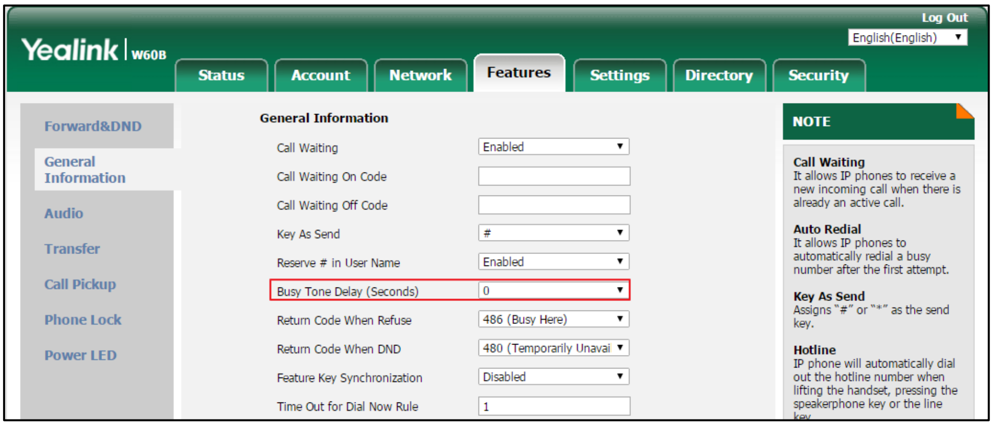
Central Provisioning (Configuration File)	y000000000077.cfg	Configure busy tone delay. **Parameter:** features.busy_tone_delay
Web User Interface		Configure busy tone delay. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.busy_tone_delay	**0, 3 or 5**	**0**
Description: Configures the duration time (in seconds) for the busy tone. When one party releases the call, a busy tone is audible to the other party indicating that the call connection breaks. **0**-0s **3**-3s **5**-5s If it is set to 3 (3s), a busy tone is audible for 3 seconds on the DECT IP phone. **Web User Interface:** Features->General Information->Busy Tone Delay (Seconds) **Handset User Interface:** None		

To configure busy tone delay via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Busy Tone Delay (Seconds)**.



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

Return Code When Refuse

Return code when refuse defines the return code and reason of the SIP response message for the refused call. The caller's phone 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)

Procedure

Return code for refused call can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Specify the return code and the reason of the SIP response message when refusing a call. **Parameter:** features.normal_refuse_code
Web User Interface		Specify the return code and the reason of the SIP response message when refusing a call. **Navigate to**: http://<phoneIPAddress>/servlet?

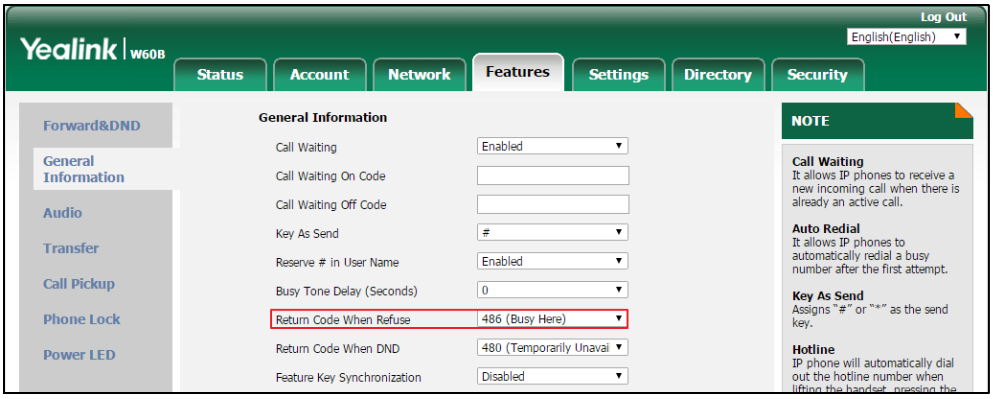
	p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.normal_refuse_code	**404, 480, 486 or 603**	**486**
Description: Configures a return code and reason of SIP response messages when the DECT IP phone rejects an incoming call. A specific reason is displayed on the caller's handset LCD screen. **404**-Not Found **480**-Temporarily Unavailable **486**-Busy Here **603**-Decline If it is set to 486 (Busy Here), the caller's phone LCD screen will display the message "Busy Here" when the callee rejects the incoming call. **Web User Interface:** Features->General Information->Return Code When Refuse **Handset User Interface:** None		

To specify the return code and the reason when refusing a call via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Return Code When Refuse**.



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

Early Media

Early media refers to media (e.g., audio and video) played to the caller before a SIP call is actually established. Current implementation supports early media through the 183 message. When the caller receives a 183 message with SDP before the call is established, a media channel is established. This channel is used to provide the early media stream for the caller.

180 Ring Workaround

180 ring workaround defines whether to deal with the 180 message received after the 183 message. When the caller receives a 183 message, it suppresses any local ringback tone and begins to play the media received. 180 ring workaround allows DECT IP phones to resume and play the local ringback tone upon a subsequent 180 message received.

Procedure

180 ring workaround can be configured using the following methods.

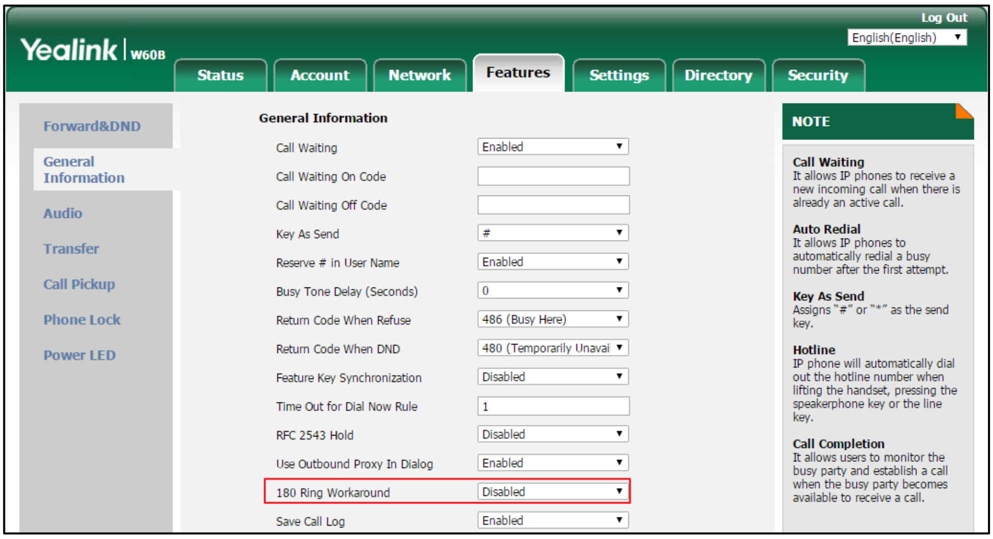
Central Provisioning (Configuration File)	y000000000077.cfg	Configure 180 ring workaround. **Parameter:** phone_setting.is_deal180
Web User Interface		Configure 180 ring workaround. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.is_deal180	**0 or 1**	**1**
Description: Enables or disables the DECT IP phone to deal with the 180 SIP message received after the 183 SIP message. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the DECT IP phone will resume and play the local ringback tone upon a subsequent 180 message received. **Web User Interface:** Features->General Information->180 Ring Workaround **Handset User Interface:** None		

To configure 180 ring workaround via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **180 Ring Workaround**.



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

Use Outbound Proxy in Dialog

An outbound proxy server can receive all initiating request messages and route them to the designated destination. If the DECT IP phone is configured to use an outbound proxy server within a dialog, all SIP request messages from the DECT IP phone will be sent to the outbound proxy server forcibly.

Note

To use this feature, make sure the outbound server has been correctly configured on the IP phone. For more information on how to configure outbound server, refer to Account Registration on page 144.

Procedure

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

Central Provisioning (Configuration File)	y000000000077.cfg	Specify whether to use outbound proxy in a dialog. **Parameter:** sip.use_out_bound_in_dialog
Web User Interface		Specify whether to use outbound proxy in a dialog. **Navigate to:** http://<phoneIPAddress>/servlet?

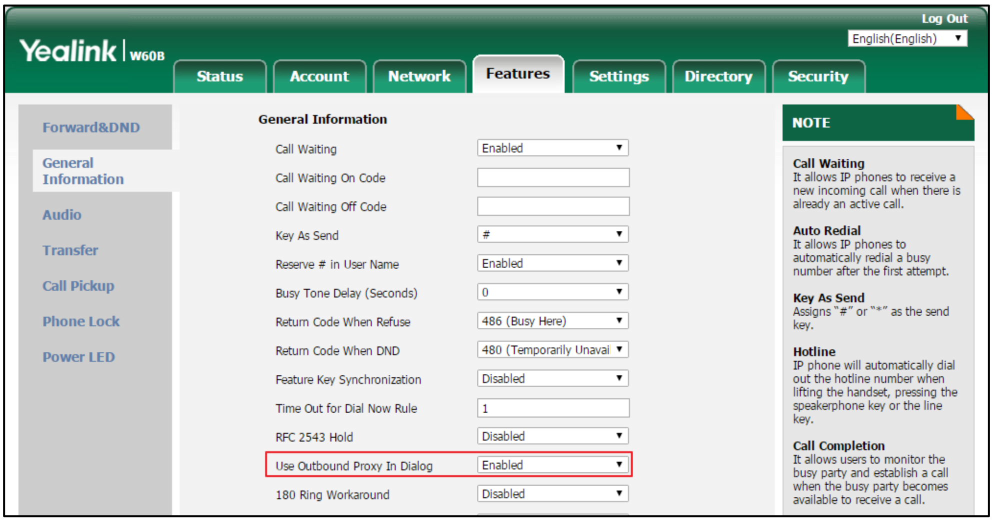
	p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sip.use_out_bound_in_dialog	**0 or 1**	**1**
Description: Enables or disables the DECT IP phone to send all SIP requests to the outbound proxy server forcibly in a dialog. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), only the new SIP request messages from the DECT IP phone will be sent to the outbound proxy server in a dialog. If it is set to 1 (Enabled), all the SIP request messages from the DECT IP phone will be forced to send to the outbound proxy server in a dialog. **Note**: It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled) and the outbound server address has been correctly configured on the phone. **Web User Interface:** Features->General Information->Use Outbound Proxy In Dialog **Handset User Interface:** None		

To configure use outbound proxy in dialog via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Use Outbound Proxy In Dialog**.



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

SIP Session Timer

SIP session timers T1, T2 and T4 are SIP transaction layer timers defined in RFC 3261. These session timers are configurable on DECT IP phones.

Timer T1

Timer T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server.

Timer T2

Timer T2 represents the maximum retransmitting time of any SIP request message. The re-transmitting and doubling of T1 will continue until the retransmitting time reaches the T2 value.

Example:

The user registers a SIP account for the DECT 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 DECT IP phone and SIP server. The re-transmitting and doubling of Timer T1 (0.5) will continue until the retransmitting time reaches the Timer T2 (4). The total registration request retry time will be less than 64 times of T1 (64 * 0.5 = 32). The re-transmitting interval in sequence is: 0.5s, 1s, 2s, 4s, 4s, 4s, 4s, 4s, 4s and 4s.

Timer T4

Timer T4 represents the time the network will take to clear messages between the SIP client and server.

Procedure

SIP session timer can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure SIP session timer. **Parameters:** sip.timer_t1 sip.timer_t2 sip.timer_t4
Web User Interface		Configure SIP session timer. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-sip&q=load

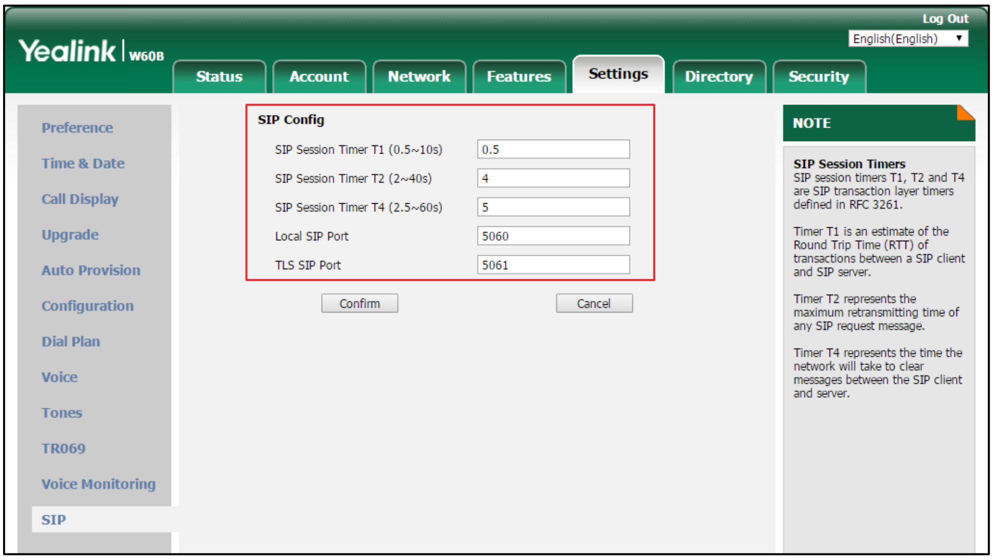
Details of Configuration Parameters:

Parameters	Permitted Values	Default
sip.timer_t1	**Float from 0.5 to10**	**0.5**
Description: Configures the SIP session timer T1 (in seconds). T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server. **Web User Interface:** Settings->SIP->SIP Session Timer T1 (0.5~10s) **Handset User Interface:** None		
sip.timer_t2	**Float from 2 to 40**	**4**
Description: Configures the SIP session timer T2 (in seconds). Timer T2 represents the maximum retransmitting time of any SIP request message. **Web User Interface:** Settings->SIP->SIP Session Timer T2 (2~40s) **Handset User Interface:** None		
sip.timer_t4	**Float from 2.5 to 60**	**5**
Description: Configures the SIP session timer of T4 (in seconds). T4 represents the maximum duration a message will remain in the network. **Web User Interface:** Settings->SIP->SIP Session Timer T4 (2.5~60s) **Handset User Interface:** None		

To configure session timer via web user interface:

1. Click on **Settings**->**SIP**.
2. Enter the desired value in the **SIP Session Timer T1 (0.5~10s)** field.
3. Enter the desired value in the **SIP Session Timer T2 (2~40s)** field.

4. Enter the desired value in the **SIP Session Timer T4 (2.5~60s)** field.



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

Session Timer

Session timer allows a periodic refresh of SIP sessions through a re-INVITE request, to determine whether a SIP session is still active. Session timer is specified in RFC 4028. The DECT IP phones support two refresher modes: UAC and UAS. The UAC mode means refreshing the session from the client, while the UAS mode means refreshing the session from the server. The session expiration and session refresher are negotiated via the Session-Expires header in the INVITE message. The negotiated refresher will send a re-INVITE/UPDATE request at or before the negotiated session expiration.

Procedure

Session timer can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure session timer. **Parameters:** account.X.session_timer.enable account.X.session_timer.expires account.X.session_timer.refresher
Web User Interface		Configure session timer. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

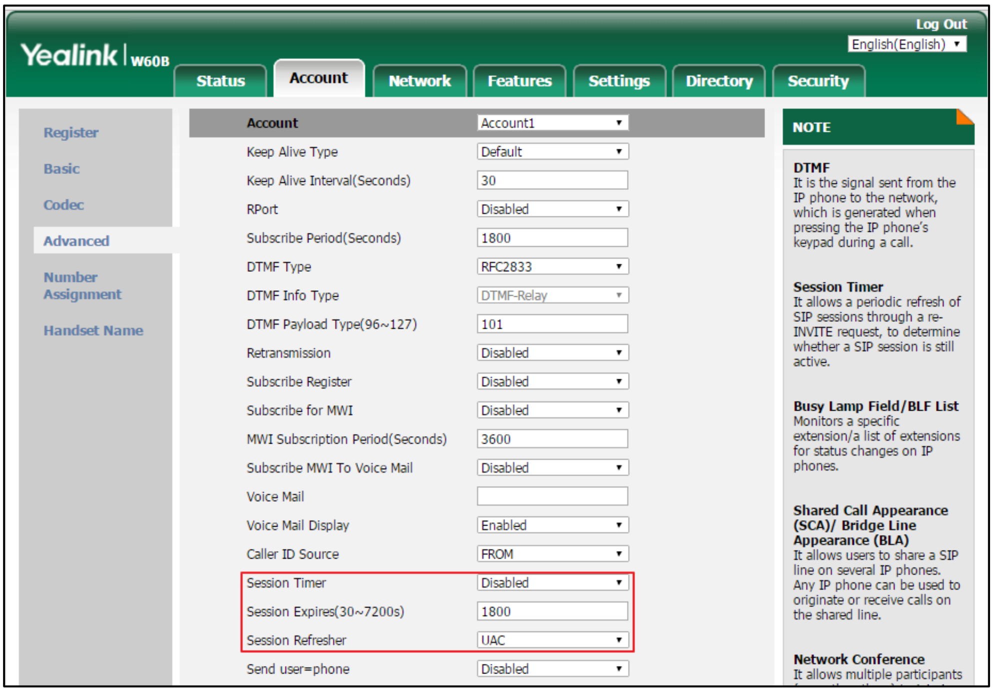
Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.session_timer.enable (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Enables or disables the session timer for account X. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), DECT IP phone will send periodic UPDATE requests to refresh the session during a call. **Web User Interface:** Account->Advanced->Session Timer **Handset User Interface:** None		
account.X.session_timer.expires (X ranges from 1 to 8)	**Integer from 30 to 7200**	**1800**
Description: Configures the interval (in seconds) for refreshing the SIP session during a call for account X. For example, an UPDATE will be sent after 50% of its value has elapsed. If it is set to 1800 (1800s), the DECT IP phone will refresh the session during a call before 900 seconds. **Example:** account.1.session_timer.expires = 1800 **Note**: It works only if the value of the parameter "account.X.session_timer.enable" is set to 1 (Enabled). **Web User Interface:** Account->Advanced->Session Expires(30~7200s) **Handset User Interface:** None		
account.X.session_timer.refresher (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Configures the function of the endpoint who initiates the SIP request for account X. **0**-UAC		

Parameters	Permitted Values	Default
1-UAS **Note**: It works only if the value of the parameter "account.X.session_timer.enable" is set to 1 (Enabled). **Web User Interface:** Account->Advanced->Session Refresher **Handset User Interface:** None		

To configure session timer via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Session Timer**.
4. Enter the desired time interval in the **Session Expires(30~7200s)** field.
5. Select the desired refresher from the pull-down list of **Session Refresher**.



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

Call Hold

Call hold provides a service of placing an active call on hold. The purpose of call hold is to pause activity on the existing call so that you can use the phone for another task (e.g., to place or receive another call).

When a call is placed on hold, the DECT IP phones send an INVITE request with HOLD SDP to request remote parties to stop sending media and to inform them that they are being held. DECT IP phones support two call hold methods, one is RFC 3264, which sets the "a" (media attribute) in the SDP to sendonly, recvonly or inactive (e.g., a=sendonly). The other is RFC 2543, which sets the "c" (connection addresses for the media streams) in the SDP to zero (e.g., c=0.0.0.0).

Procedure

Call hold can be configured using the following methods.

Configuration File	y000000000077.cfg	Specify whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used. **Parameter:** sip.rfc2543_hold
Web User Interface		Specify whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used. **Navigate to**: http://<phoneIPAddress>/servlet?p=phone-features&q=load

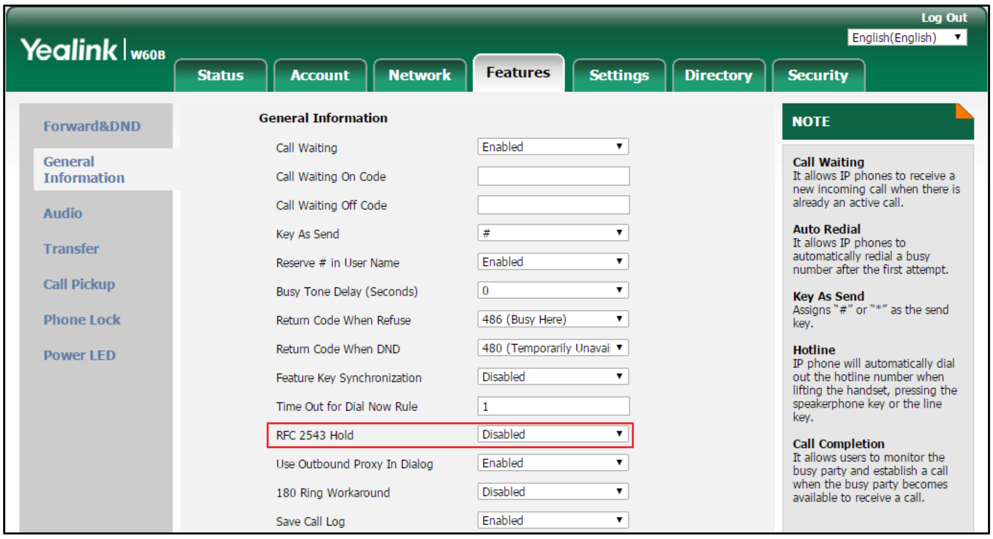
Details of Configuration Parameters:

Parameters	Permitted Values	Default
sip.rfc2543_hold	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to use RFC 2543 (c=0.0.0.0) outgoing hold signaling. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), SDP media direction attributes (such as a=sendonly) per RFC 3264 is used when placing a call on hold. If it is set to 1 (Enabled), SDP media connection address c=0.0.0.0 per RFC 2543 is used when placing a call on hold. **Web User Interface:** Features->General Information->RFC 2543 Hold **Handset User Interface:** None		

To configure call hold method via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **RFC 2543 Hold**.



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

Call Forward

Call forward allows users to redirect an incoming call to a third party. The DECT IP phones redirect an incoming INVITE message by responding with a 302 Moved Temporarily message, which contains a Contact header with a new URI that should be tried. Three types of call forward:

- **Always Forward**--Forward the incoming call immediately.
- **Busy Forward**--Forward the incoming call when the DECT IP phone or the specified account is busy.
- **No Answer Forward**--Forward the incoming call after a period of ring time.

Call forward can be configured on a phone or a per-line basis depending on the call forward mode.

The call forward on code and call forward off code configured on DECT IP phones are used to activate/deactivate the server-side call forward feature. They may vary on different servers.

Procedure

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

Configuration File	<MAC>.cfg	Configure call forward feature. **Parameters:** account.X.always_fwd.enable account.X.always_fwd.target account.X.always_fwd.on_code account.X.always_fwd.off_code account.X.busy_fwd.enable account.X.busy_fwd.target account.X.busy_fwd.on_code account.X.busy_fwd.off_code account.X.timeout_fwd.enable account.X.timeout_fwd.target account.X.timeout_fwd.timeout account.X.timeout_fwd.on_code account.X.timeout_fwd.off_code
		Configure diversion/history-info feature. **Parameter:** features.fwd_diversion_enable
Local	Web User Interface	Configure call forward feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
		Configure diversion/history-info feature. Configure forward international. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Handset User Interface	Configure call forward feature.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.always_fwd.enable (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Triggers always forward feature to on or off for account X. **0**-Off **1**-On If it is set to 1 (On), incoming calls to the account X are forwarded to the destination number immediately. **Web User Interface:** Features->Forward&DND->Forward->Always Forward->On/Off **Handset User Interface:** OK->Call Features->Call Forward->LineX->Always(Disabled/Enabled) ->Status		
account.X.always_fwd.target (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the destination number of the always forward for account X. **Example:** account.1.always_fwd.target = 1003 **Web User Interface:** Features->Forward&DND->Forward->Always Forward->Target **Handset User Interface:** OK->Call Features->Call Forward->LineX->Always(Enabled) ->Target		
account.X.always_fwd.on_code (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the always forward on code to activate the server-side always forward feature for account X. The DECT IP phone will send the always forward on code and the pre-configured destination number to the server when you activate always forward feature for account X on the DECT IP phone. **Example:** account.1.always_fwd.on_code = *72 **Web User Interface:** Features->Forward&DND->Forward->Always Forward->On Code		

Parameters	Permitted Values	Default
Handset User Interface: None		
account.X.always_fwd.off_code (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the always forward off code to deactivate the server-side always forward feature for account X. The DECT IP phone will send the always forward off code to the server when you deactivate always forward feature for account X on the DECT IP phone. **Example:** account.1.always_fwd.off_code= *73 **Web User Interface:** Features->Forward&DND->Forward->Always Forward->Off Code **Handset User Interface:** None		
account.X.busy_fwd.enable (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Triggers busy forward feature to on or off for account X. **0**-Off **1**-On If it is set to 1 (On), incoming calls to the account X are forwarded to the destination number when the callee is busy. **Web User Interface:** Features->Forward&DND->Forward->Busy Forward->On/Off **Handset User Interface:** OK->Call Features->Call Forward->LineX->Busy(Disabled/Enabled) ->Status		
account.X.busy_fwd.target (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the destination number of the busy forward for account X. **Example:** account.1.busy_fwd.target = 3602 **Web User Interface:** Features->Forward&DND->Forward->Busy Forward->Target		

Parameters	Permitted Values	Default
Handset User Interface: OK->Call Features->Call Forward->LineX->Busy(Enabled) ->Target		
account.X.busy_fwd.on_code (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the busy forward on code to activate the server-side busy forward feature for account X. The DECT IP phone will send the busy forward on code and the pre-configured destination number to the server when you activate busy forward feature for account X on the DECT IP phone. **Example:** account.1.busy_fwd.on_code = *74 **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward->On Code **Handset User Interface:** None		
account.X.busy_fwd.off_code (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the busy forward off code to deactivate the server-side busy forward feature for account X. The DECT IP phone will send the busy forward off code to the server when you deactivate busy forward feature for account X on the DECT IP phone. **Example:** account.1.busy_fwd.off_code = *75 **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward->Off Code **Handset User Interface:** None		
account.X.timeout_fwd.enable (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Triggers no answer forward feature to on or off for account X. **0**-Off **1**-On If it is set to 1 (On), incoming calls to the account X are forwarded to the destination number after a period of ring time.		

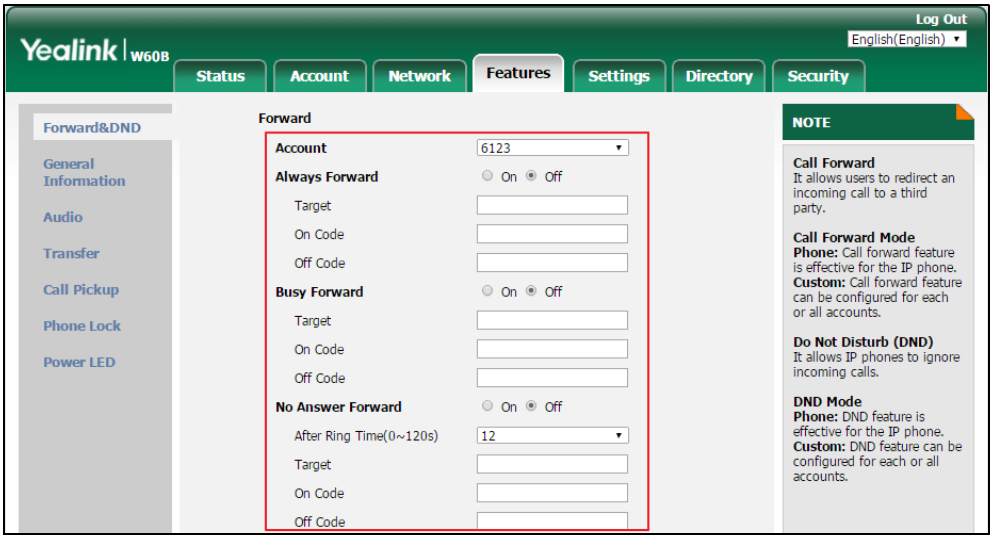
Parameters	Permitted Values	Default
Web User Interface: Features->Forward&DND->Forward->No Answer Forward->On/Off **Handset User Interface:** OK->Call Features->Call Forward->LineX->No Answer(Disabled/Enabled) ->Status		
account.X.timeout_fwd.target (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the destination number of the no answer forward for account X. **Example:** account.1.timeout_fwd.target = 3603 **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward->Target **Handset User Interface:** OK->Call Features->Call Forward->LineX->No Answer(Enabled) ->Target		
account.X.timeout_fwd.timeout (X ranges from 1 to 8)	**Integer from 0 to 20**	**2**
Description: Configures ring times (N) to wait before forwarding incoming calls for account X. Incoming calls will be forwarded when not answered after N*6 seconds. **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward->After RingTime(0~120s) **Handset User Interface:** OK->Call Features->Call Forward->LineX->No Answer(Enabled) ->After Ring Time		
account.X.timeout_fwd.on_code (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the no answer forward on code to activate the server-side no answer forward feature for account X. The DECT IP phone will send the no answer forward on code and the pre-configured destination number to the server when you activate no answer forward feature for account X on the DECT IP phone. **Example:** account.1.timeout_fwd.on_code = *76 **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward->On Code		

Parameters	Permitted Values	Default
Handset User Interface: None		
account.X.timeout_fwd.off_code (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the no answer forward off code to deactivate the server-side no answer forward feature for account X. The DECT IP phone will send the no answer forward off code to the server when you deactivate no answer forward feature for account X on the DECT IP phone. **Example:** account.1.timeout_fwd.off_code = *77 **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward->Off Code **Handset User Interface:** None		
features.fwd_diversion_enable	**0 or 1**	**1**
Description: Enables or disables the DECT IP phone to present the diversion information when an incoming call is forwarded to your DECT IP phone. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Diversion/History-Info **Handset User Interface:** None		

To configure call forward via web user interface:

1. Click on **Features**->**Forward&DND**.
2. In the **Forward** block, mark the desired radio box in the **Mode** field.
   1) Mark the desired radio box in the **Always**/**Busy**/**No Answer Forward** field.
   2) Enter the destination number you want to forward in the **Target** field.
   3) (Optional.) Enter the on code and off code in the **On Code** and **Off Code** fields.

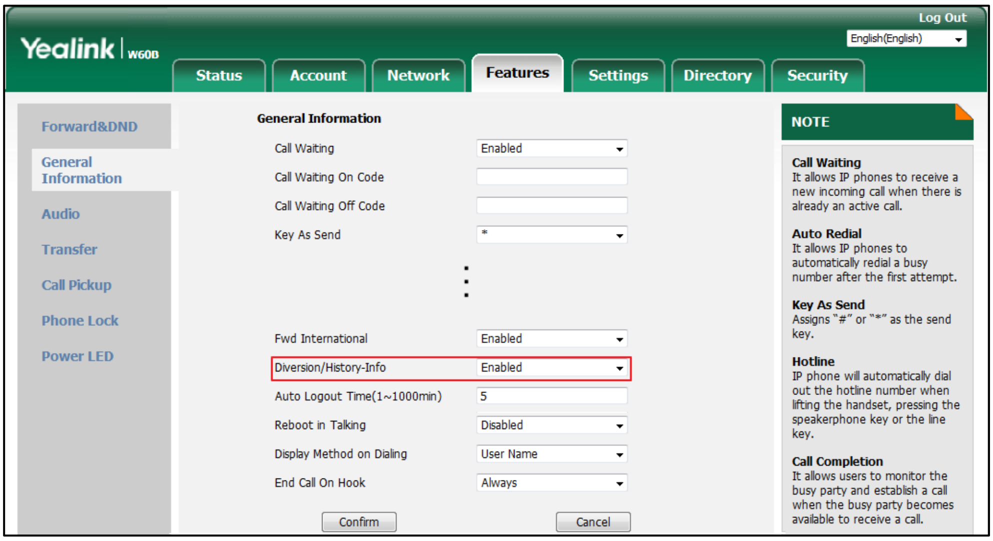
4) Select the ring time to wait before forwarding from the pull-down list of **After Ring Time(0~120s)** (only for the no answer forward).



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

To configure Diversion/History-Info feature via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Diversion/History-Info**.

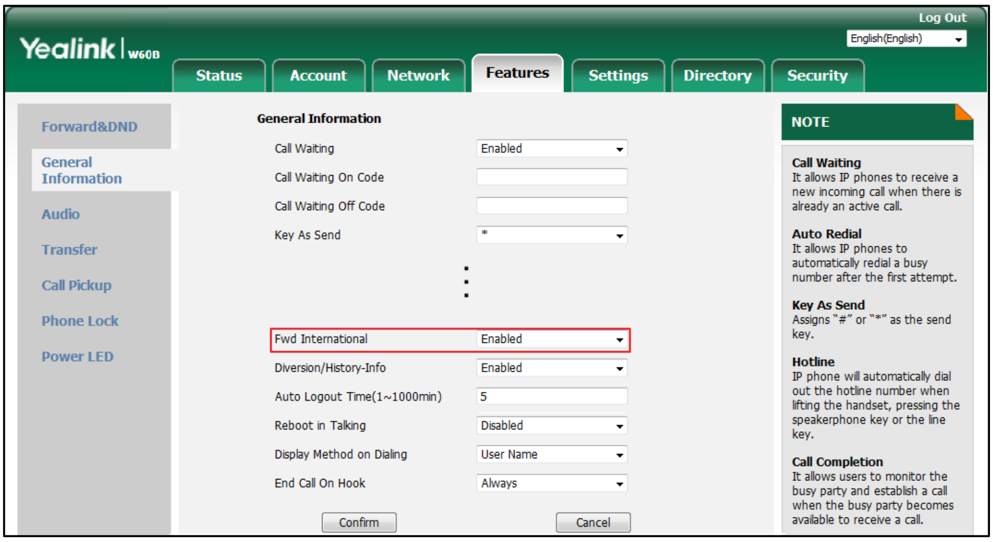


3. Click **Confirm** to accept the change.

To configure forward international via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **Fwd International**.



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

To enable call forward feature for a specific line via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Call Features**->**Call Forward**.

   The LCD screen displays the incoming lines currently assigned to the handset.
3. Press ▲ or ▼ to highlight the desired line, and then press the **OK** soft key.
4. Press ▲ or ▼ to highlight the desired forwarding type, and then press the **OK** soft key.
5. Press ◀ or ▶ to select **Enabled** from the **Status** field.
6. Enter the destination number you want to forward incoming calls to in the **Target** field.
7. Press ◀ or ▶ to select the desired ring time to wait before forwarding from the **After Ring Time** field (only available for No Answer Forward).
8. Press the **Save** soft key to accept the change.

Call Transfer

Call transfer enables DECT IP phones to transfer an existing call to a third party. For example, if party A is in an active call with party B, party A can transfer this call to party C (the third party). Then, party B will begin a new call with party C and party A will disconnect.

DECT IP phones support call transfer using the REFER method specified in RFC 3515 and offer three types of transfer:

- **Blind Transfer** -- Transfer a call directly to another party without consulting. Blind transfer is implemented by a simple REFER method without Replaces in the Refer-To header.
- **Semi-attended Transfer** -- Transfer a call after hearing the ringback tone. Semi-attended transfer is implemented by a REFER method with Replaces in the Refer-To header.
- **Attended Transfer** -- Transfer a call with prior consulting. Attended transfer is

implemented by a REFER method with Replaces in the Refer-To header.

Normally, call transfer is completed by pressing the transfer key. Blind transfer on hook and attended transfer on hook features allow the DECT IP phone to complete the transfer through on-hook.

When a user performs a semi-attended transfer, semi-attended transfer feature determines whether to display the prompt "**n New Missed Call(s)**" ("n" indicates the number of the missed calls) on the destination party's phone LCD screen.

Procedure

Call transfer can be configured using the following methods.

<table>
<tr><td rowspan="2">Central Provisioning (Configuration File)</td><td rowspan="2">y000000000077.cfg</td><td>Specify whether to complete the transfer through on-hook.
Parameters:
transfer.blind_tran_on_hook_enable
transfer.on_hook_trans_enable</td></tr>
<tr><td>Configure semi-attended transfer feature.
Parameter:
transfer.semi_attend_tran_enable</td></tr>
<tr><td colspan="2">Web User Interface</td><td>Specify whether to complete the transfer through on-hook.
Configure semi-attended transfer feature.
Navigate to:
http://<phoneIPAddress>/servlet?p=features-transfer&q=load</td></tr>
</table>

Details of Configuration Parameters:

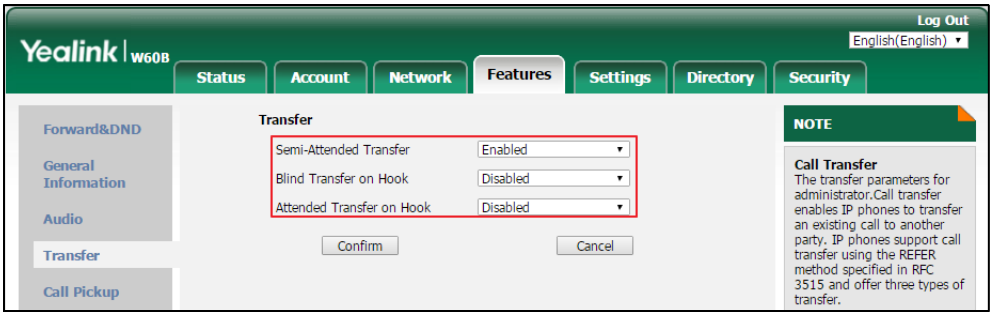
<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>transfer.blind_tran_on_hook_enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables the phone to complete the blind transfer through on-hook besides pressing the TRAN/R key on the handset.
0-Disabled
1-Enabled
Note: Blind transfer means transfer a call directly to another party without consulting.</td></tr>
</table>

Parameters	Permitted Values	Default
Web User Interface: Features->Transfer->Blind Transfer On Hook **Handset User Interface:** None		
transfer.on_hook_trans_enable	**0 or 1**	**1**
Description: Enables or disables the phone to complete the attended transfer through on-hook besides pressing the **TRAN/R** key on the handset. **0**-Disabled **1**-Enabled **Note**: Semi-attended transfer means transfer a call after hearing the ringback tone; Attended transfer means transfer a call with prior consulting. **Web User Interface:** Features->Transfer->Attended Transfer On Hook **Handset User Interface:** None		
transfer.semi_attend_tran_enable	**0 or 1**	**1**
Description: Enables or disables the transfer-to party's phone not to prompt a missed call on the LCD screen before displaying the caller ID when completing a semi-attended transfer. **0**-Disabled **1**-Enabled **Note**: Semi-attended transfer means transfer a call after hearing the ringback tone. **Web User Interface:** Features->Transfer->Semi-Attended Transfer **Handset User Interface:** None		

To configure call transfer via web user interface:

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

2. Select the desired values from the pull-down lists of **Semi-Attended Transfer**, **Blind Transfer on Hook** and **Attended Transfer on Hook**.



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

Network Conference

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

Procedure

Network conference can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure network conference. **Parameters:** account.X.conf_type account.X.conf_uri
Web User Interface		Configure network conference. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

Details of Configuration Parameters:

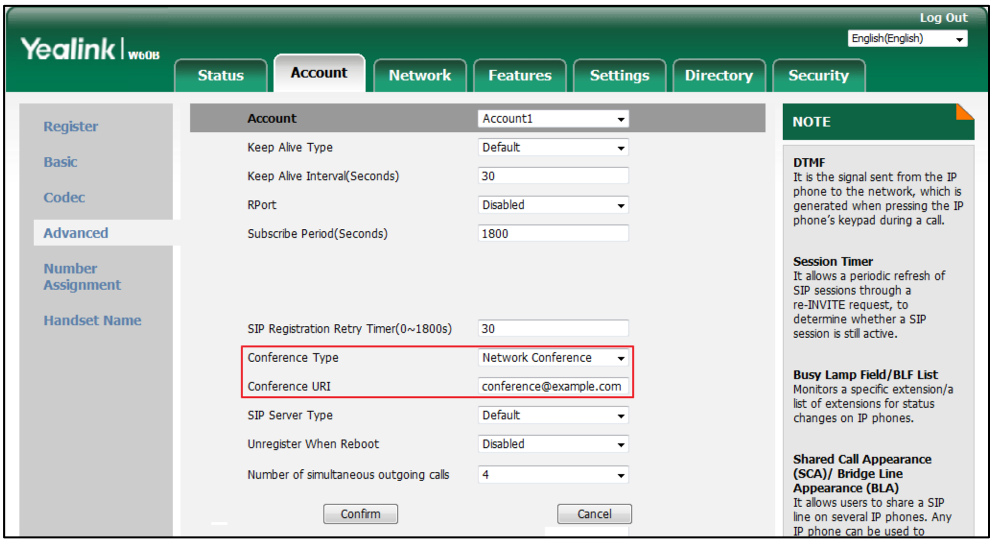
Parameters	Permitted Values	Default
account.X.conf_type (X ranges from 1 to 8)	**0 or 2**	**0**

Parameters	Permitted Values	Default
Description: Configures the network conference type for account X. **0**-Local Conference **2**-Network Conference If it is set to 0 (Local Conference), conferences are set up on the DECT IP phone locally. If it is set to 2 (Network Conference), conferences are set up by the server. **Web User Interface:** Account->Advanced->Conference Type **Handset User Interface:** None		
account.X.conf_uri (X ranges from 1 to 8)	**SIP URI within 511 characters**	**Blank**
Description: Configures the network conference URI for account X. **Example:** account.1.conf_uri = conference@example.com **Note**: It works only if the value of the parameter "account.X.conf_type" is set to 2 (Network Conference). **Web User Interface:** Account->Advanced->Conference URI **Handset User Interface:** None		

To configure the network conference via web user interface:

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

4. Enter the conference URI in the **Conference URI** field.



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

Feature Key Synchronization

Feature key synchronization provides the capability to synchronize the status of the following features between the DECT IP phone and the server:

- Do Not Disturb (DND)
- Call Forwarding Always (CFA)
- Call Forwarding Busy (CFB)
- Call Forwarding No Answer (CFNA)

If feature key synchronization is enabled, a user changes the status of one of these features on the server, and then the server notifies the phone of synchronizing the status. Conversely, if the user changes the feature status on the phone, the DECT IP phone notifies the server of synchronizing the status.

Procedure

Feature key synchronization can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure feature key synchronization. **Parameter:** bw.feature_key_sync
Web User Interface		Configure feature key synchronization. **Navigate to**: http://<phoneIPAddress>/servlet?

	p=features-general&q=load

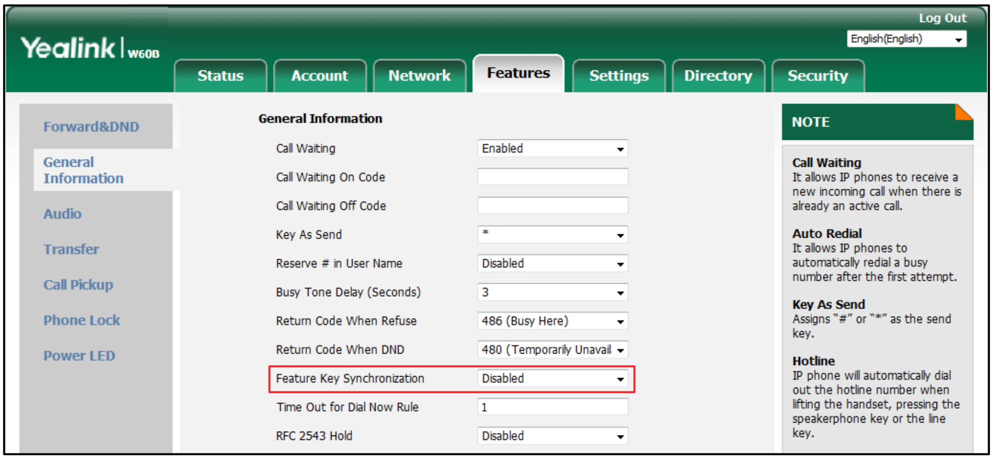
Details of Configuration Parameter:

Parameter	Permitted Values	Default
bw.feature_key_sync	**0 or 1**	**0**
Description: Enables or disables feature key synchronization. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Feature Key Synchronization **Handset User Interface:** None		

To configure feature key synchronization via web user interface:

1. Click on **Features**->**General Information**.

2. Select **Enabled** from the pull-down list of **Feature Key Synchronization**.



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

Recent Call In Dialing

Recent call in dialing feature allows users to view the placed calls list when the phone is on the dialing screen (presses the Speakerphone key). Users can select to place a call from the placed calls list. For some phones, you may need to press up/down navigation key to browse all the placed call number. It is not applicable to W52H handset.

Procedure

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

Central Provisioning (Configuration File)	y000000000077.cfg	Configure recent call in dialing feature. **Parameter:** super_search.recent_call
Web User Interface		Configure recent call in dialing feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-favorite&q=load

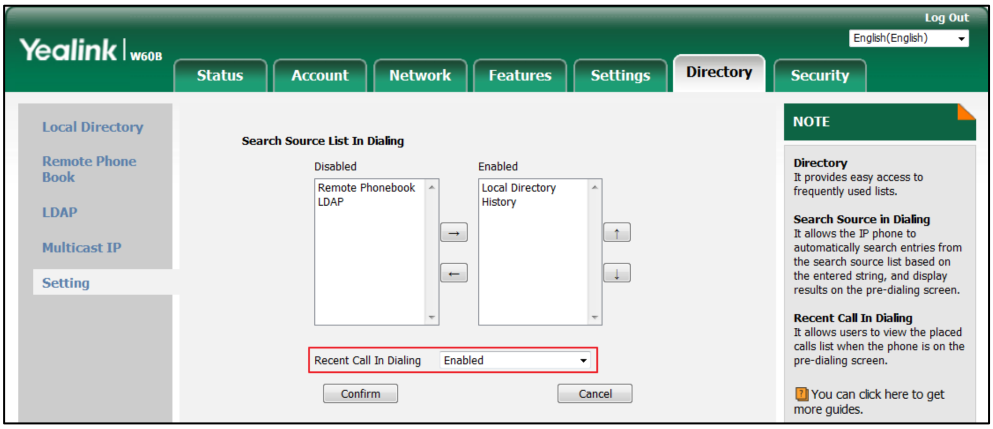
Details of Configuration Parameter:

Parameter	Permitted Values	Default
super_search.recent_call	**0 or 1**	**0**
Description: Enables or disables recent call in dialing feature. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), you can see the placed calls list when the DECT IP phone is on the dialing screen. **Note:** It is not applicable to W52H handset. **Web User Interface:** Directory->Setting->Recent Call In Dialing **Handset User Interface:** None		

To configure recent call in dialing via web user interface:

1. Click on **Directory**->**Setting**.

2. Select the desired value from the pull-down list of **Recent Call In Dialing**.



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

Call Number Filter

When you choose a contact from a directory to dial out, the contact number may contain the SPACE or other special characters. You need to filter the special characters before you dial out. Call number filter feature allows DECT IP phone to automatically filter designated characters when dialing.

Procedure

Call number filter can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the characters the DECT IP phone filters when dialing. **Parameter:** features.call_num_filter
Web User Interface		Configure the characters the DECT IP phone filters when dialing. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

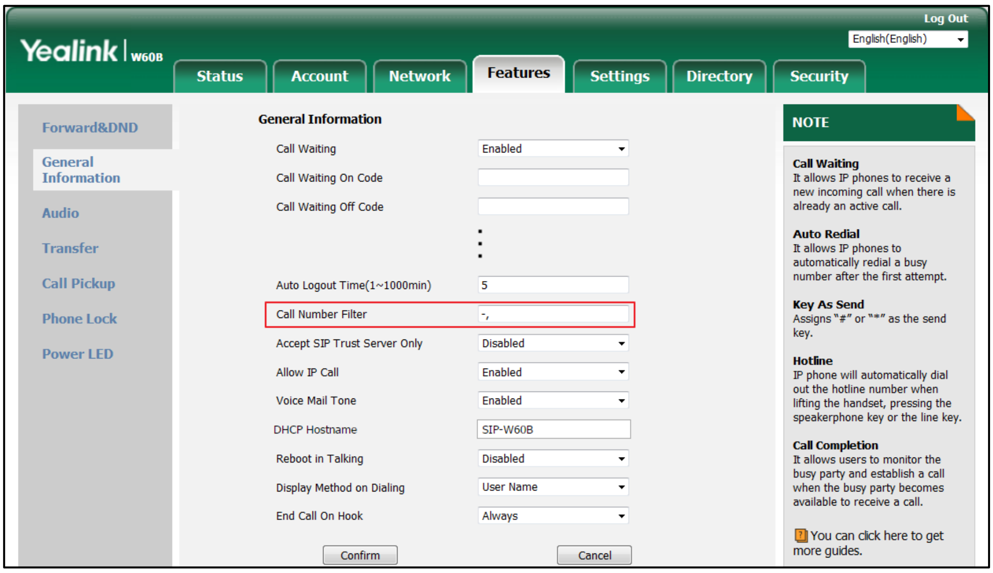
Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.call_num_filter	**String within 99 characters**	**,**
Description:		

Parameter	Permitted Values	Default
Configures the characters the DECT IP phone filters when dialing. If the dialed number contains configured characters, the DECT IP phone will automatically filter these characters when dialing. **Example:** features.call_num_filter = ,- If you choose a contact number 0233-622221 to dial out, the DECT IP phone will filter the character -, and then dial out 0233622221. **Note**: If it is left blank, the DECT IP phone will not automatically filter any characters when dialing. If you want to filter just a space, you have to set the value to " ," (a space first followed by a comma). **Web User Interface:** Features->General Information->Call Number Filter **Handset User Interface:** None		

To configure the characters the DECT IP phone will filter via web user interface:

1. Click on **Feature**->**General Information**.
2. Enter the desired characters in the **Call Number Filter** field.



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

Call Park

Call park allows users to park a call on a special extension and then retrieve it from another phone (for example, a phone in another office or conference room). This feature depends on support from a SIP server. It is not applicable to W52H handset.

Call park feature supports the following two modes:

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

Procedure

Call park can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure call park feature. **Parameters:** features.call_park.park_mode features.call_park.enable features.call_park.park_code features.call_park.park_retrieve_code
Web User Interface		Configure call park feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-callpickup&q=load

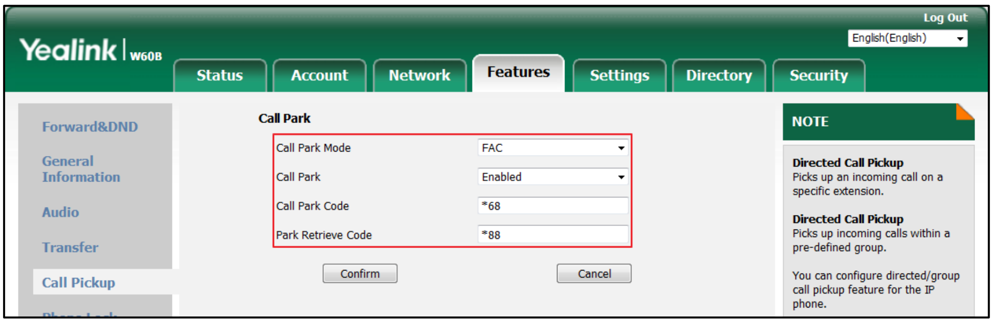
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.call_park.park_mode	**1 or 2**	**2**
Description: Configures the call park mode. **1-**FAC **2**-Transfer **Note:** It is not applicable to W52H handset. **Web User Interface:** Features->Call Pickup->Call Park Mode **Handset User Interface:** None		

Parameters	Permitted Values	Default
features.call_park.enable	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to display the **Park** Option during a call. **0**-Disabled **1**-Enabled **Note:** It is not applicable to W52H handset. **Web User Interface:** Features->Call Pickup->Call Park **Handset User Interface:** None		
features.call_park.park_code	**String within 32 characters**	**Blank**
Description: Configures the call park code for the **Park** option. **Example:** features.call_park.park_code = *68 **Note:** It is not applicable to W52H handset. **Web User Interface:** Features->Call Pickup->Call Park Code **Handset User Interface:** None		
features.call_park.park_retrieve_code	**String within 32 characters**	**Blank**
Description: Configures the park retrieve code. **Example:** features.call_park.park_retrieve_code = *88 **Note:** It is not applicable to W52H handset. **Web User Interface:** Features->Call Pickup->Park Retrieve Code **Handset User Interface:-** None		

To configure call park feature via web user interface:

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



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

Calling Line Identification Presentation (CLIP)

Calling Line Identification Presentation (CLIP) allows DECT IP phones to display the caller identity, derived from a SIP header contained in the INVITE message when receiving an incoming call. DECT IP phones support deriving caller identity from three types of SIP header: From, P-Asserted-Identity (PAI) and Remote-Party-ID (RPID). Identity presentation is based on the identity in the relevant SIP header.

Note If the caller already exists in the local directory, the local contact name assigned to the caller should be preferentially displayed and stored in the call log.

The following sessions show the enhancements of calling line identification presentation according to the calling line identification source configured on the DECT IP phones.

Caller ID source = FROM

1) The DECT IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the calling line identification information will be hidden and the DECT IP phone LCD screen presents anonymous.
2) If there is not any Privacy: id header in the INVITE request, the DECT IP phone checks and presents the caller identification from the P-Preferred-Identity header.
3) If there is not P-Preferred-Identity header in the INVITE request, the DECT IP phone presents the caller identification derived from the FROM header.

Caller ID source = PAI

1) The DECT IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the DECT IP phone

LCD screen presents anonymous.

2) If there is not any Privacy: id header in the INVITE request, the DECT IP phone checks and presents the caller identification from the P-Preferred-Identity header.

3) If there is not P-Preferred-Identity header in the INVITE request, the DECT IP phone checks and presents the caller identification from the P-Asserted-Identity header.

Caller ID source = PAI-FROM

1) The DECT IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the DECT IP phone LCD screen presents anonymous.

2) If there is not any Privacy: id header in the INVITE request, the DECT IP phone checks and presents the caller identification from the P-Preferred-Identity header.

3) If there is not P-Preferred-Identity header in the INVITE request, the DECT IP phone checks and presents the caller identification from the P-Asserted-Identity header.

4) If there is not P-Asserted-Identity header in the INVITE request, the DECT IP phone presents the caller identification derived from the FROM header.

Caller ID source = RPID-FROM

1) The DECT IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the DECT IP phone LCD screen presents anonymous.

2) If there is not any Privacy: id header in the INVITE request, the DECT IP phone checks and presents the caller identification from the P-Preferred-Identity header.

3) If there is not P-Preferred-Identity header in the INVITE request, the DECT IP phone checks and presents the caller identification from the Remote-Party-ID header.

4) If there is not Remote-Party-ID header in the INVITE request, the DECT IP phone presents the caller identification derived from the FROM header.

Caller ID source = PAI-RPID-FROM

1) The DECT IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the DECT IP phone LCD screen presents anonymous.

2) If there is not any Privacy: id header in the INVITE request, the DECT IP phone checks and presents the caller identification from the P-Preferred-Identity header.

3) If there is not P-Preferred-Identity header in the INVITE request, the DECT IP phone checks and presents the caller identification from the P-Asserted-Identity header.

4) If there is not P-Asserted-Identity header in the INVITE request, the DECT IP phone checks and presents the caller identification from the Remote-Party-ID header.

5) If there is not Remote-Party-ID header in the INVITE request, the DECT IP phone presents the caller identification derived from the FROM header.

Caller ID source = RPID-PAI-FROM

1) The DECT IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the

INVITE request, the caller identification information will be hidden and the DECT IP phone LCD screen presents anonymous.

2) If there is not any Privacy: id header in the INVITE request, the DECT IP phone checks and presents the caller identification from the P-Preferred-Identity header.

3) If there is not P-Preferred-Identity header in the INVITE request, the DECT IP phone checks and presents the caller identification from the Remote-Party-ID header.

4) If there is not Remote-Party-ID header in the INVITE request, the DECT IP phone checks and presents the caller identification from the P-Asserted-Identity header.

5) If there is not P-Asserted-Identity in the INVITE request, the DECT IP phone presents the caller identification derived from the FROM header.

For more information on calling line identification presentation, refer to *Calling and Connected Line Identification Presentation on Yealink DECT IP phones*.

Procedure

CLIP can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the presentation of the caller identity. **Parameter:** account.X.cid_source
		Specify whether to process Privacy header field. **Parameter:** account.X.cid_source_privacy
		Specify whether to process the P-Preferred-Identity (PPI) header for caller identity presentation. **Parameter:** account.X.cid_source_ppi
Web User Interface		Configure the presentation of the caller identity. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

Details of the Configuration Parameters:

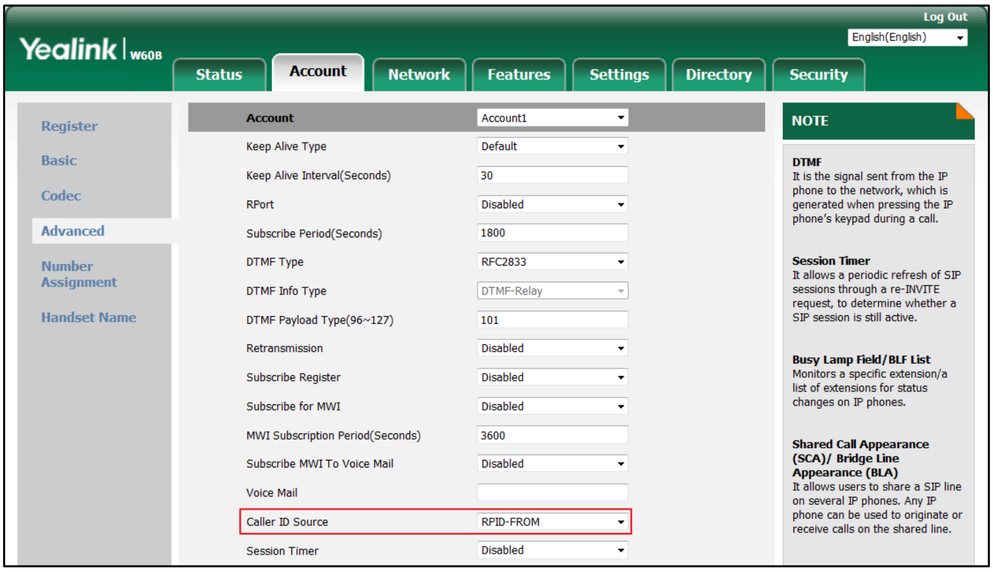
Parameters	Permitted Values	Default
account.X.cid_source	**0, 1, 2, 3, 4**	**0**

Parameters	Permitted Values	Default
(X ranges from 1 to 8)	**or 5**	
Description: Configures the presentation of the caller identity when receiving an incoming call for account X. **0**-FROM **1**-PAI **2**-PAI-FROM **3**-RPID-PAI-FROM **4**-PAI-RPID-FROM **5**-RPID-FROM **Web User Interface:** Account->Advanced->Caller ID Source **Handset User Interface:** None		
account.X.cid_source_privacy (X ranges from 1 to 8)	**0 or 1**	**1**
Description: Enables or disables the DECT IP phone to process Privacy header field in the SIP message for account X. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the DECT IP phone doesn't process Privacy header. If it is set to 1 (Enabled), the caller identification information will be hidden and the DECT IP phone LCD screen presents anonymous if there is a Privacy: id in the INVITE request. **Web User Interface:** None **Handset User Interface:** None		
account.X.cid_source_ppi (X ranges from 1 to 8)	**0 or 1**	**1**
Description: Enables or disables the DECT IP phone to process the P-Preferred-Identity (PPI) header for caller identity presentation when receiving an incoming call for account X.		

Parameters	Permitted Values	Default
0-Disabled **1**-Enabled If it is set to 0 (Disabled), the DECT IP phone doesn't process P-Preferred-Identity (PPI) header. If it is set to 1 (Enabled), the DECT IP phone presents the caller identification from the P-Preferred-Identity (PPI) header. **Web User Interface:** None **Handset User Interface:** None		

To configure the presentation of the caller identity via web user interface:

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



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

Connected Line Identification Presentation (COLP)

Connected Line Identification Presentation (COLP) allows DECT IP phones to display the identity of the connected party specified for outgoing calls. DECT IP phones can display the Dialed Digits, or the identity in a SIP header (Remote-Party-ID or P-Asserted-Identity) received, or the identity in the From header carried in the UPDATE message sent by the callee as described in RFC 4916. Connected line identification presentation is also known as Called line identification presentation. In some cases, the remote party will be different from the called line identification presentation due to call diversion.

Note If the callee already exists in the local directory, the local contact name assigned to the callee should be preferentially displayed.

The following sessions show the enhancements of connected line identification according to the connected line identification source configured on the DECT IP phones.

Connected Line Identification source = PAI-RPID

1) The DECT IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the 18X or 200OK response, the connected line identification information will be hidden and the DECT IP phone LCD screen presents anonymous.

2) If there is not any Privacy: id header in the 18X or 200OK response, the DECT IP phone checks and presents the connected line identification from the P-Asserted-Identity header.

3) If there is not P-Asserted-Identity header in the I8X or 200OK response, the DECT IP phone presents the connected line identification from the Remote-Party-ID header. If no, the DECT IP phone presents the connected line identification according to the dialed digits.

Connected Line Identification source = Dialed digits

Yealink DECT IP phones present the connected line identification according to the dialed digits.

Connected Line Identification source = RFC4916

Yealink DECT IP phones support to present the connected line identification from UPDATE message following the RFC 4916.

1) The DECT IP phone receives an UPDATE message during a call, the connected line identification on the LCD screen should be refreshed according the FROM SIP carried in the UPDATE message.

For more information on connected line identification presentation, refer to *Calling and Connected Line Identification Presentation on Yealink IP phones*.

Procedure

COLP can be configured only using the configuration files.

<table>
<tr><td rowspan="2">Central Provisioning (Configuration File)</td><td rowspan="2"><MAC>.cfg</td><td>Configure the presentation of the callee's identity.
Parameter:
account.X.cp_source</td></tr>
<tr><td>Specify whether to process Privacy header field.
Parameter:
account.X.cid_source_privacy</td></tr>
</table>

Details of the Configuration Parameter:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>account.X.cp_source</td><td>0, 1 or 2</td><td>0</td></tr>
<tr><td colspan="3">Description:
Configures the presentation of the callee's identity for account X.
0-PAI-RPID
1-Dialed Digits
2-RFC 4916
When the RFC 4916 is enabled on the DECT IP phone, the caller sends the SIP request message which contains the from-change tag in the Supported header. The caller then receives an UPDATE message from the callee, and displays the identity in the "From" header.
Web User Interface:
None
Handset User Interface:
None</td></tr>
<tr><td>account.X.cid_source_privacy</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables the DECT IP phone to process Privacy header field in the SIP message for account X.
0-Disabled
1-Enabled
If it is set to 0 (Disabled), the DECT IP phone doesn't process Privacy header.</td></tr>
</table>

Parameters	Permitted Values	Default
If it is set to 1 (Enabled), the caller identification information will be hidden and the DECT IP phone LCD screen presents anonymous if there is a Privacy: id in the INVITE request. **Web User Interface:** None **Handset User Interface:** None		

Intercom

Intercom is a useful feature in an office environment to quickly connect with the operator or the secretary. You can make internal intercom calls and external intercom calls on the phone. Internal intercom calls are made between handsets registered to the same base station. External intercom calls can be made by dialing the feature access code followed by the number. External intercom calls depend on support from a SIP server.

The handset can automatically answer an incoming external intercom call and play warning tone only when there is only one handset subscribed and no call in progress on the handset.

To automatically answer an incoming internal intercom call, you need to enable auto intercom feature on the handset. The following configuration types of auto intercom feature are available for selection:

- **On (Beep On)**: Auto intercom feature is on. The handset will answer an incoming internal intercom call automatically and play a warning tone.
- **On (Beep Off)**: Auto intercom feature is on. The handset will answer an incoming internal intercom call automatically without a warning tone.
- **Off**: Auto intercom feature is off. You need to answer an incoming internal intercom call manually.

Procedure

Intercom can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure incoming intercom call feature. **Parameters:** features.intercom.headset_prior.enable custom.handset.auto_intercom
Handset User Interface		Configure incoming intercom call feature for specified handset.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.intercom.headset_prior.enable	**0 or 1**	**1**
Description: Configures the channel mode when an incoming intercom call is answered through the handset. The headset should be connected in advance. **0**-Speaker Mode **1**-Headset Mode **Web User Interface:** None **Handset User Interface:** None		
custom.handset.auto_intercom	**0, 1 or 2**	**0**
Description: Configures whether the DECT IP phone automatically answers an incoming internal intercom call and plays a warning tone. **0**-Off **1**-On(Beep Off) **2**-On(Beep On) If it is set to 0, users need to answer incoming internal intercom calls manually. If it is set to 1, the handset will answer an incoming internal intercom call automatically without a warning tone. If it is set to 2, the handset will answer an incoming internal intercom call automatically and play a warning tone. It works when the silence mode is off. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled). **Web User Interface:** None **Handset User Interface:** OK->Settings->Telephony->Auto Intercom		

To configure auto intercom via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Telephony**->**Auto Intercom**.

   The LCD screen displays three configuration types.

3. Press ▲ or ▼ to highlight the desired configuration type.
4. Press the **Change** soft key.

   The radio box of the selected configuration type is marked.

Call Timeout

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

Procedure

Call timeout can only be configured using the configuration files.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the duration time in the ringback state. **Parameter:** phone_setting.ringback_timeout

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.ringback_timeout	**Integer from 0 to 3600**	**180**
Description: Configures the duration time (in seconds) in the ringback state. If it is set to 180, the phone will cancel the dialing if the call is not answered within 180 seconds. **Web User Interface:** None **Handset User Interface:** None		

Ringing Timeout

Ringing timeout defines a specific period of time within which the DECT IP phone will stop ringing if the call is not answered.

Procedure

Ringing timeout can only be configured using the configuration files.

Central Provisioning	y000000000077.cfg	Configure the duration time in the

(Configuration File)		ringing state. **Parameter:** phone_setting.ringing_timeout

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.ringing_timeout	**Integer from 0 to 3600**	**180**
Description: Configures the duration time (in seconds) in the ringing state. If it is set to 180, the phone will stop ringing if the call is not answered within 180 seconds. **Web User Interface:** None **Handset User Interface:** None		

Send user=phone

When placing a call, the DECT IP phone will send an INVITE request to the proxy server. Send user=phone feature allows adding user=phone to the SIP header of the INVITE message.

Example of a SIP INVITE message:

```
INVITE sip:101@10.3.5.199:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.3.20.6:5060;branch=z9hG4bK2475812834
From: "1010" <sip:1010@10.3.5.199:5060>;tag=3747068208
To: <sip:101@10.3.5.199:5060;user=phone>
Call-ID: 0_4008470062@10.3.20.6
CSeq: 1 INVITE
Contact: <sip:1010@10.3.20.6:5060>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH,
UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink W60B 77.81.0.10
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length: 300
```

Procedure

Send user=phone can be configured using the following methods.

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

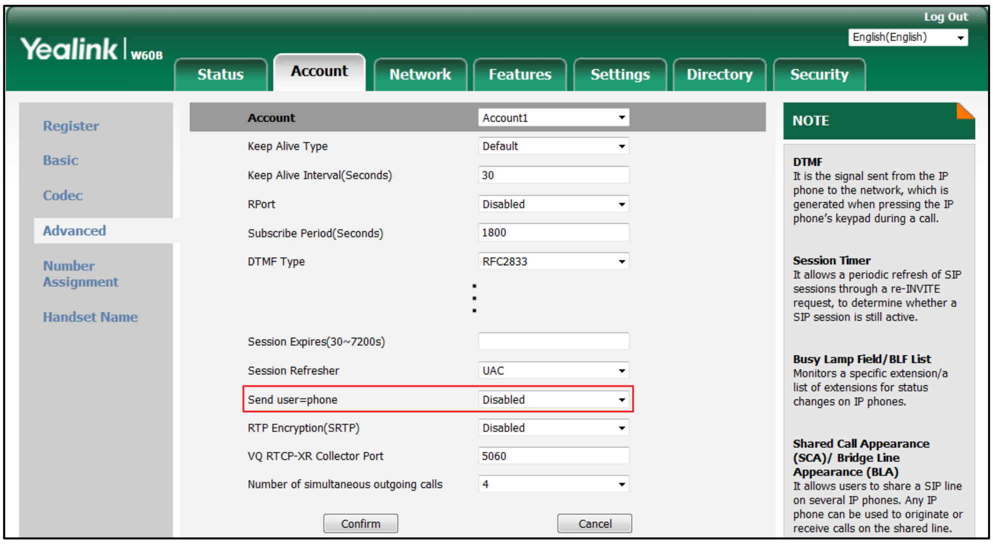
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.enable_user_equal_phone (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to add "user=phone" to the SIP header of the INVITE message for account X. **0**-Disabled **1**-Enabled **Web User Interface:** Account->Advanced->Send user=phone **Handset User Interface:** None		

To configure send user=phone feature via web user interface:

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

3. Select the desired value from the pull-down list of **Send user=phone**.



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

SIP Send MAC

The DECT IP phone can send the MAC address in the REGISTER message. SIP send MAC allow adding “Mac:<PhoneMACAddress>” (e.g., Mac: 00:15:65:5F:9D:7E) to the SIP header of the REGISTER message.

Example of a SIP REGISTER message:

```
REGISTER sip:10.3.5.199:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.14:5060;branch=z9hG4bK3593117201
From: "11" <sip:11@10.3.5.199:5060>;tag=2788360609
To: "11" <sip:11@10.3.5.199:5060>
Call-ID: 1_1863786852@10.3.20.14
CSeq: 2 REGISTER
Contact: <sip:11@10.3.20.14:5060;line=cc75882e976e208>
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH,
UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink W60B 77.81.0.10
Expires: 0
Allow-Events: talk,hold,conference,refer,check-sync
Mac: 00:15:65:5F:9D:7E
Content-Length: 0
```

Procedure

SIP send MAC can be configured using the following methods.

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

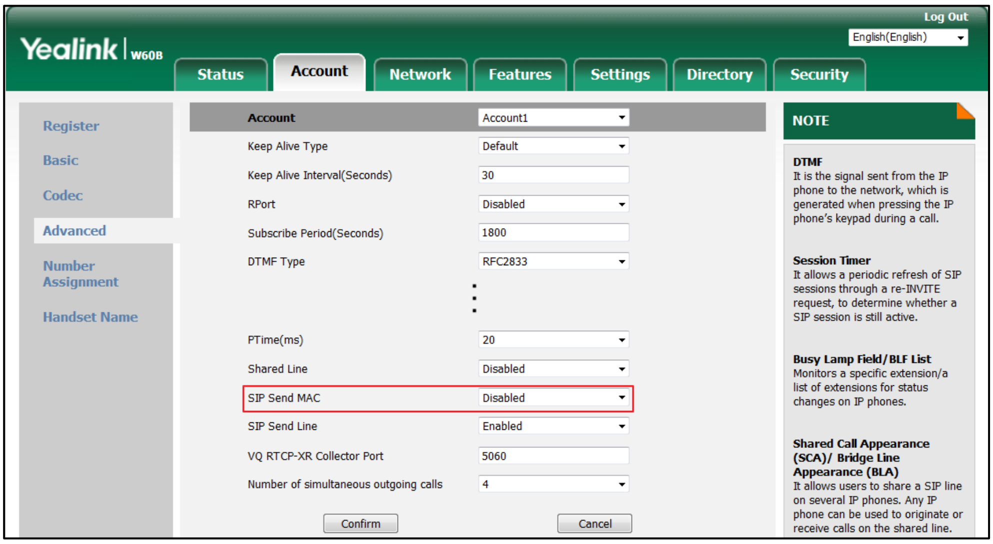
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.register_mac (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to add MAC address to the SIP header of the REGISTER message for account X. **0**-Disabled **1**-Enabled **Web User Interface:** Account->Advanced->SIP Send MAC **Handset User Interface:** None		

To configure SIP send MAC feature via web user interface:

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

3. Select the desired value from the pull-down list of **SIP Send MAC**.



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

SIP Send Line

The DECT IP phone can send the line number in the REGISTER message. SIP send line allow adding “Line:<linenumber>“(e.g., Line: 1) to the SIP header of the REGISTER message. The line number is from 1 to 8.

Example of a SIP REGISTER message:

```
REGISTER sip:10.3.5.199:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.14:5060;branch=z9hG4bK3990593443
From: "11" <sip:11@10.3.5.199:5060>;tag=255071842
To: "11" <sip:11@10.3.5.199:5060>
Call-ID: 1_2369214377@10.3.20.14
CSeq: 2 REGISTER
Contact: <sip:11@10.3.20.14:5060;line=1da6aa8d7254654>
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH,
UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink W60B 77.81.0.10
Expires: 0
Allow-Events: talk,hold,conference,refer,check-sync
Line: 1
Content-Length: 0
```

Procedure

SIP send line can be configured using the following methods.

Central Provisioning	<MAC>.cfg	Configure SIP send line on a per-line

(Configuration File)		basis. **Parameter:** account.X.register_line
Web User Interface		Configure SIP send line on a per-line basis. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

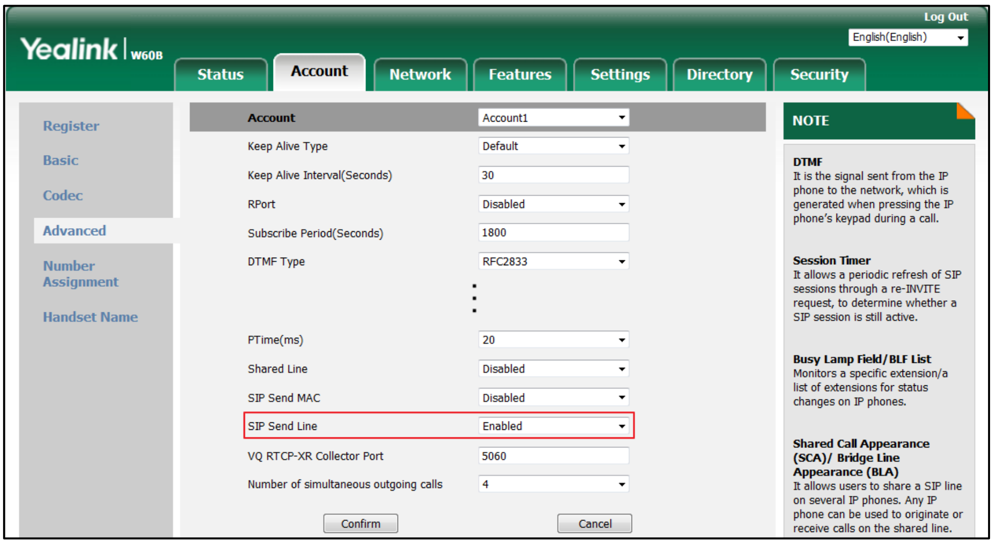
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.register_line (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to add line number to the SIP header of the REGISTER message for account X. **0**-Disabled **1**-Enabled **Web User Interface:** Account->Advanced->SIP Send Line **Handset User Interface:** None		

To configure SIP send Line feature via web user interface:

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

3. Select the desired value from the pull-down list of **SIP Send Line**.



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

Reserve # in User Name

Reserve # in User Name feature allows DECT IP phones to reserve "#" in user name. When Reserve # in User Name feature is disabled, "#" will be converted into "%23". For example, the user registers an account (user name: 1010#) on the phone, the phone will send 1010%23 instead of 1010# in the REGISTER message or INVITE message to SIP server.

Example of a SIP REGISTER message:

```
INVITE sip:2@10.3.5.199:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.6:5060;branch=z9hG4bK1867789050
From: "1010" <sip:1010%23@10.3.5.199:5060>;tag=1945988802
To: <sip:2@10.3.5.199:5060>
Call-ID: 0_2336101648@10.3.20.6
CSeq: 1 INVITE
Contact: <sip:1010%23@10.3.20.6:5060>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH,
UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink W60B 77.81.0.10
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length:    300
```

Procedure

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

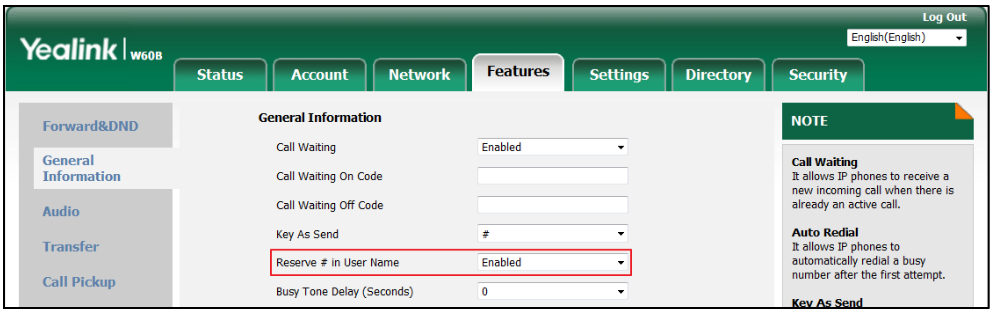
Central Provisioning (Configuration File)	y000000000077.cfg	Configure reserve # in user name. **Parameter:** sip.use_23_as_pound
Web User Interface		Configure reserve # in user name. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sip.use_23_as_pound	**0 or 1**	**1**
Description: Enables or disables the DECT IP phone to reserve the pound sign (#) in the user name. **0**-Disabled (convert the pound sign into "%23") **1**-Enabled **Web User Interface:** Features->General Information->Reserve # in User Name **Handset User Interface:** None		

To configure reserve # in user name feature via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Reserve # in User Name**.



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

Unregister When Reboot

Unregister when reboot feature allows DECT IP phones to unregister first before re-registering the account when finishing a reboot.

Procedure

Unregister when reboot can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure unregister when reboot. **Parameter:** account.X.unregister_on_reboot
Web User Interface		Configure unregister when reboot. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

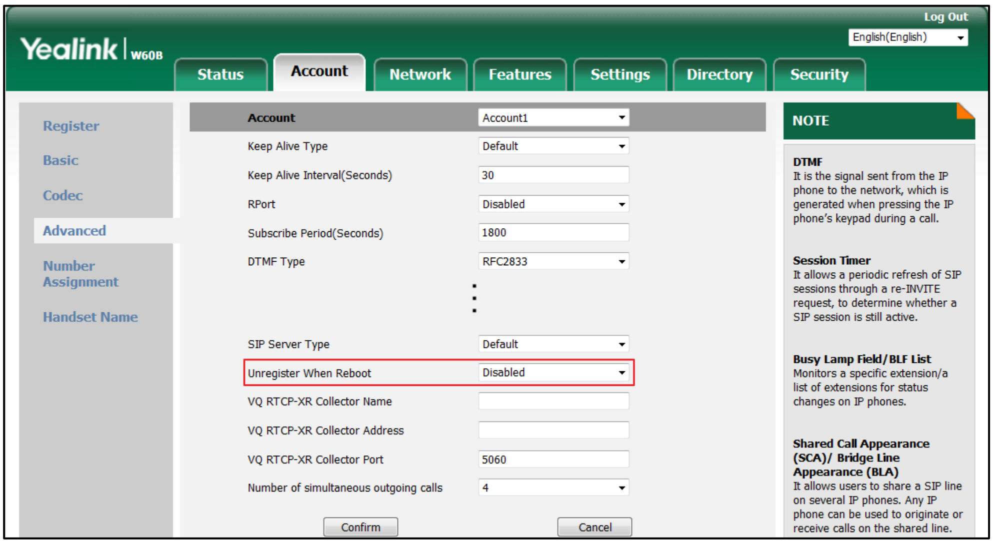
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.unregister_on_reboot (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to unregister first before re-registering account X when finishing a reboot. **0**-Disabled **1**-Enabled **Web User Interface:** Account->Advanced->Unregister When Reboot **Handset User Interface:** None		

To configure unregister when reboot via web user interface:

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

3. Select the desired value from the pull-down list of **Unregister When Reboot**.



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

100 Reliable Retransmission

As described in RFC 3262, 100rel tag is for reliability of provisional responses. When present in a Supported header, it indicates that the DECT IP phone can send or receive reliable provisional responses. When present in a Require header in a reliable provisional response, it indicates that the response is to be sent reliably.

Example of a SIP INVITE message:

```
INVITE sip:1024@pbx.yealink.com:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.6.197:5060;branch=z9hG4bK1708689023
From: "1025" <sip:1025@pbx.yealink.com:5060>;tag=1622206783
To: <sip:1024@pbx.yealink.com:5060>
Call-ID: 0_537569052@10.3.6.197
CSeq: 2 INVITE
Contact: <sip:1025@10.3.6.197:5060>
Authorization: Digest username="1025", realm="pbx.yealink.com",
nonce="BroadWorksXi5stub71Ts2nb05BW", uri="sip:1024@pbx.yealink.com:5060",
response="f7e9d35c55af45b3f89beae95e913171", algorithm=MD5, cnonce="0a4f113b", qop=auth,
nc=00000001
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH,
UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink W60B 77.81.0.10
Supported: 100rel
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length:     302
```

Procedure

100 Reliable Retransmission can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the 100 reliable retransmission. **Parameter:** account.X.100rel_enable
Web User Interface		Configure the 100 reliable retransmission. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

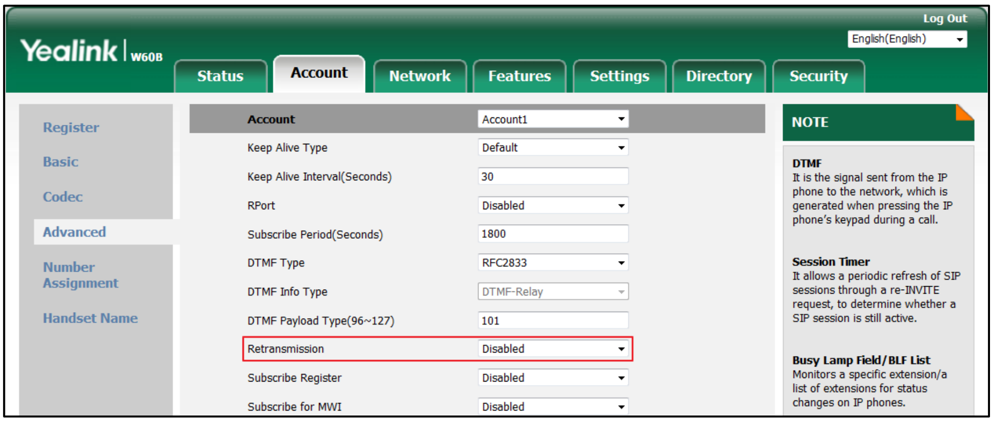
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.100rel_enable (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Enables or disables the 100 reliable retransmission feature for account X. **0**-Disabled **1**-Enabled **Web User Interface:** Account->Advanced->Retransmission **Handset User Interface:** None		

To configure 100 reliable retransmission via web user interface:

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

3. Select the desired value from the pull-down list of **Retransmission**.



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

Reboot in Talking

Reboot in talking feature allows base station to reboot during an active call when it receives a packet.

Procedure

Reboot in talking can be configured using the following methods.

Configuration File	y000000000077.cfg	Configure reboot in talking. **Parameter:** features.reboot_in_talk_enable
Web User Interface		Configure reboot in talking. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameter:

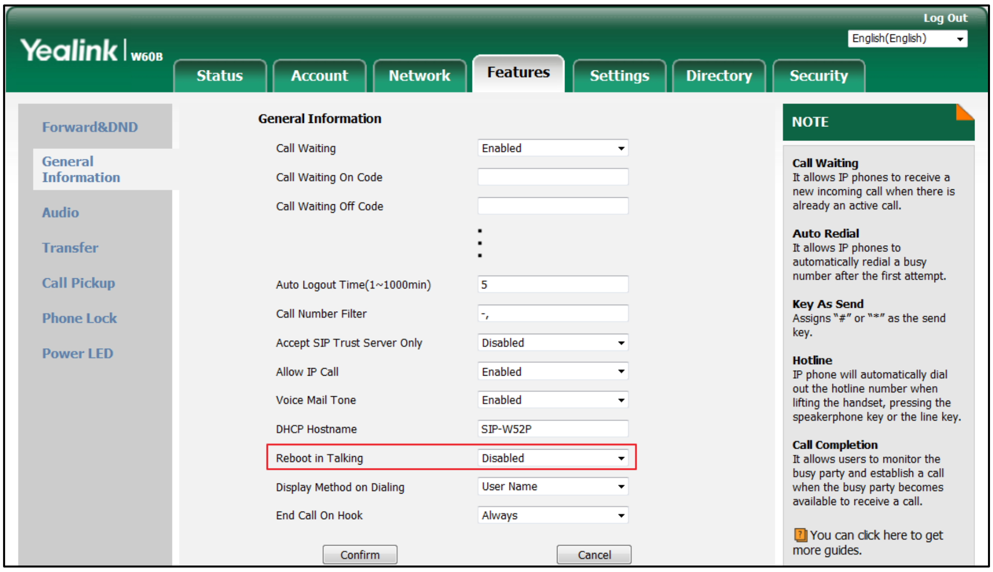
Parameter	Permitted Values	Default
features.reboot_in_talk_enable	**0 or 1**	**0**
Description: Enables or disables the base station to reboot during a call when it receives a packet. **0**-Disabled **1**-Enabled **Web User Interface:**		

Parameter	Permitted Values	Default
Features->General Information->Reboot in Talking **Handset User Interface:** None		

To configure reboot in talking via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **Reboot in Talking**.



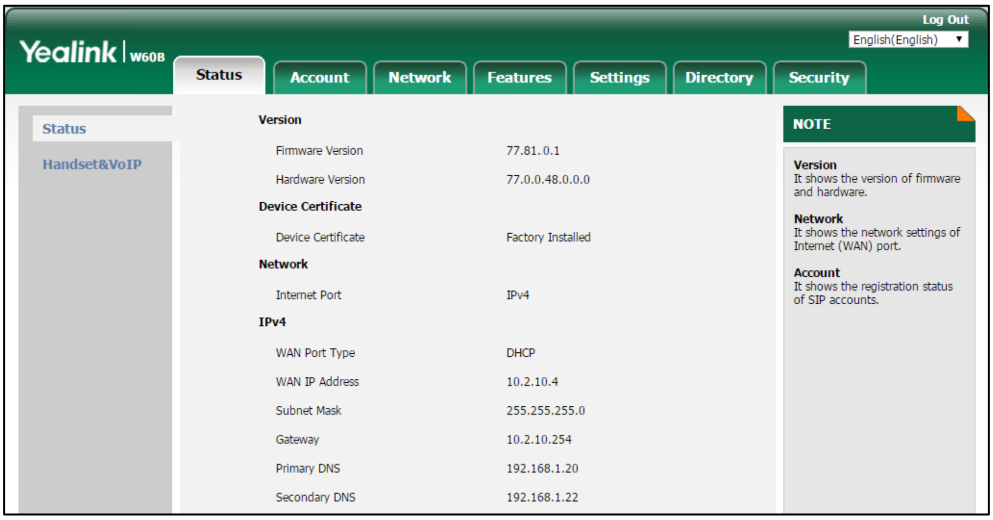
3. Click **Confirm** to accept the change.

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

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

Quick Login

Quick login feature allows users to fast access to web user interface using the request URI "https://username:password@phoneIPAddress" (e.g., https://admin:admin@192.168.0.10). You will navigate to the **Status** web page after accessing the web user interface. It is helpful for users to quickly log into the web user interface without entering the username and password in the login page.



Note

The use of the quick login feature may be restricted by the web explorer (e.g., Internet Explorer). You can use Google or other web explorers.

For security purposes, we recommend you to use this feature in a secure network environment.

Procedure

Quick login can be configured using the configuration file.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure quick login. **Parameter**: wui.quick_login

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
wui.quick_login	**0 or 1**	**0**
Description: Enables or disables the quick login feature. **0**-Disabled		

Parameter	Permitted Values	Default
1-Enabled If it is set to 1 (Enabled), you can quickly log into the web user interface using a request URI (e.g., https://admin:admin@192.168.0.10). **Note**: It works only if the value of the parameter "static.wui.https_enable" is set to 1 (Enabled). **Web User Interface:** None **Handset User Interface:** None		

End Call on Hook

End call on hook feature allows ending a call when placing the handset into the charger cradle.

Procedure

End call on hook can be configured using the configuration files.

Configuration File	y000000000077.cfg	Configure end call on hook. **Parameter:** phone_setting.end_call_on_hook.enable
Local	Web User Interface	Configure end call on hook. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

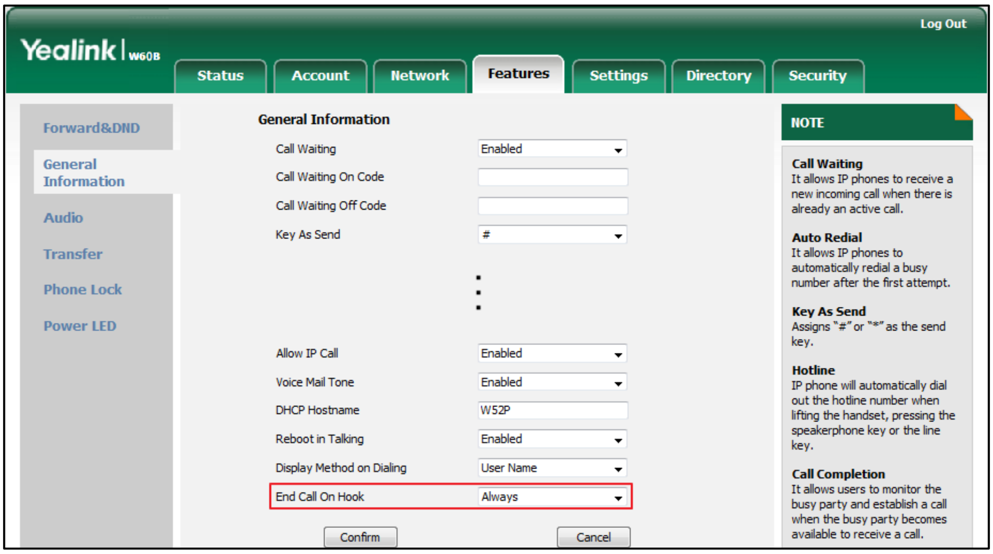
Details of Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.end_call_on_hook.enable	**0 or 1**	**1**
Description: Enables or disables to end a call when placing the handset into the charger cradle. **0**-Never **1**-Always **Web User Interface:** Features->General Information->End Call On Hook **Handset User Interface:**		

Parameter	Permitted Values	Default
None		

To configure end call on hook via web user interface:

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



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

Configuring Advanced Features

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

- Remote Phone Book
- Lightweight Directory Access Protocol (LDAP)
- Shared Call Appearance (SCA)
- Message Waiting Indicator (MWI)
- Multicast Paging
- Server Redundancy
- Static DNS Cache
- Real-Time Transport Protocol (RTP) Ports
- TR-069 Device Management

Remote Phone Book

Remote phone book is a centrally maintained phone book, stored on the remote server. Users only need the access URL of the remote phone book. The DECT 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 handset user interface. DECT IP phones support up to 5 remote phone books. Remote phone book is customizable.

Customizing Remote Phone Book Template File

You can customize the remote phone book for DECT IP phones as required. You can also add multiple remote contacts at a time and/or share remote contacts between DECT IP phones using the supplied template files (Menu.xml and Department.xml). The Menu.xml file defines departments of a remote phone book. The Department.xml file defines contact lists for a department, which is nested in Menu.xml file. After setup, place the files (Menu.xml and Department.xml) to the provisioning server, and specify the access URL of the file (Menu.xml) in the configuration files.

You can ask the distributor or Yealink FAE for remote XML phone book template. You can also obtain the remote XML phone book template online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the remote phone book template, refer to Obtaining Boot Files/Configuration Files/Resource Files on page 89.

When creating a Department.xml file, learn the following:

- <YealinkIPPhoneDirectory> indicates the start of a department file and </YealinkIPPhoneDirectory> indicates the end of a department file.
- Create contact lists for a department between <DirectoryEntry> and </DirectoryEntry>.

To customize a Datacontact.xml file:

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

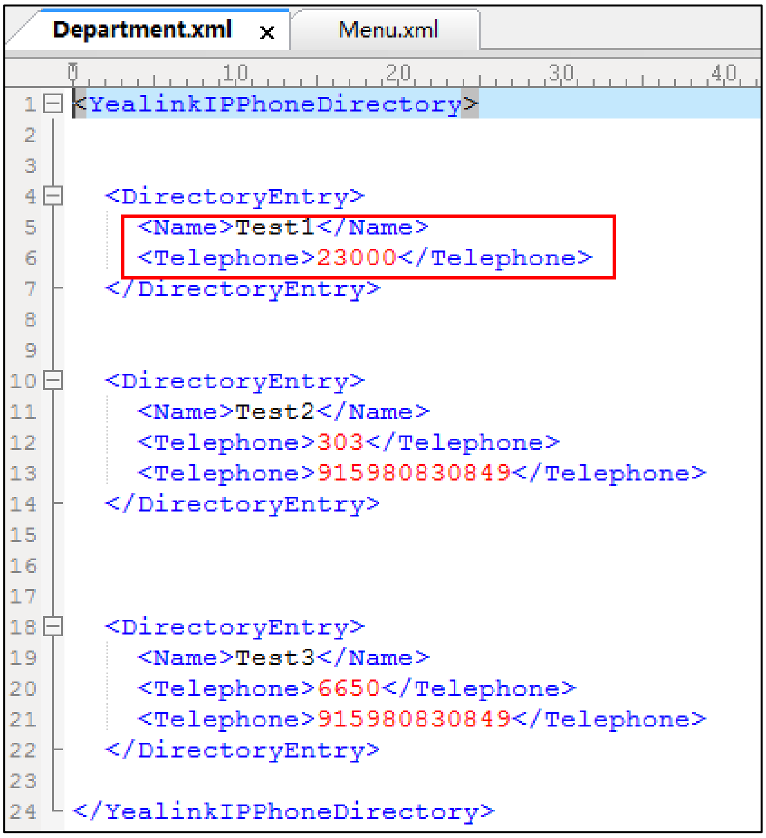
   <Name>*Test1*</Name>

   <Telephone>*23000*</Telephone>

   Where:

   Specify the contact name between <Name> and </Name>.

   Specify the contact number between <Telephone> and </Telephone>.



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

When creating a Menu.xml file, learn the following:

- <YealinkIPPhoneMenu> indicates the start of a remote phone book file and </YealinkIPPhoneMenu> indicates the end of a remote phone book file.
- Create the title of a remote phone book between <Title> and </Title>.
- <MenuItem>indicates the start of specifying a department file and </MenuItem> indicates the end of specifying a department file.

- <SoftKeyItem> indicates the start of specifying an XML file and </SoftKeyItem> indicates the end of specifying an XML file for the digit keys, # key or * key. In the remote phone book contacts screen, pressing the configured digit keys/# key/* key can access the subdirectory. If not configured, the LCD screen displays "URL is empty" when pressing the desired digit keys, # key or * key.

To customize a Menu.xml file:

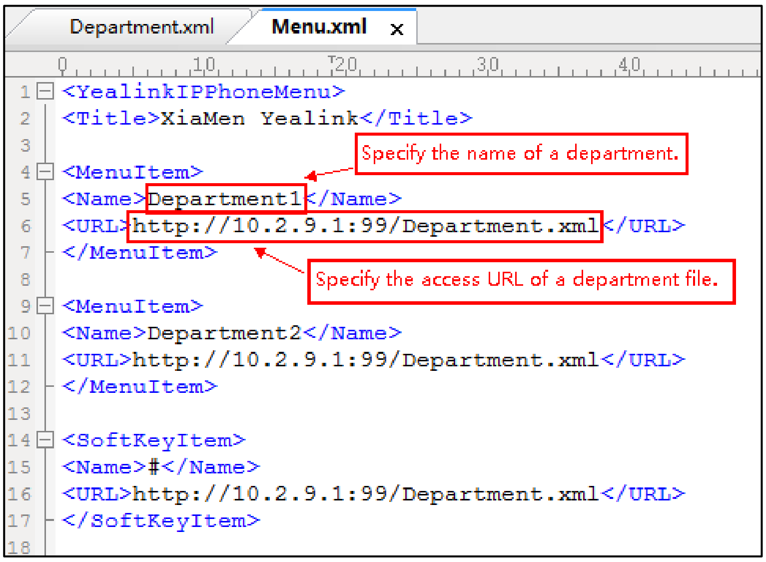
1. Open the template file using an ASCII editor.
2. For each department that you want to add, add the following strings to the file. Each starts on a separate line:

   <MenuItem>

   <Name>*Department1*</Name>

   <URL>http://10.2.9.1:99/Department.xml </URL>

   </MenuItem>



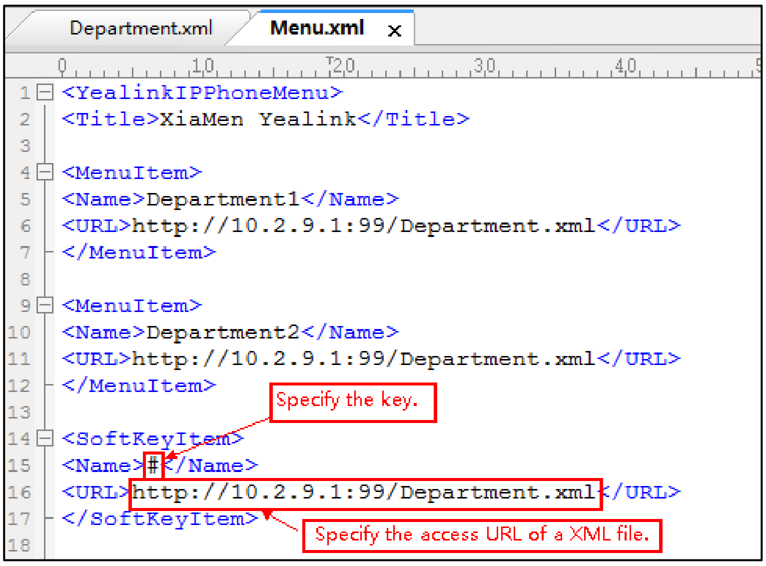
3. For each XML file that you want to add, add the following strings to the file. Each starts on a separate line:

<SoftKeyItem>

<Name>#</Name>

<URL>http://10.2.9.1:99/Department.xml</URL>

</SoftKeyItem>



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

5. Specify the access URL of the remote phone book (remote_phonebook.data.1.url = http://192.168.1.20/Menu.xml).

During the auto provisioning process, the DECT IP phone connects to the provisioning server "192.168.1.20", and downloads the remote phone book file "Menu.xml".

Note Yealink supplies a phonebook generation tool to generate a remote XML phone book. For more information, refer to *Yealink Phonebook Generation Tool User Guide*.

Incoming/Outgoing Call Lookup allows DECT IP phones to search the entry names from the remote phone book for incoming/outgoing calls. Update Time Interval specifies how often DECT IP phones refresh the local cache of the remote phone book.

Procedure

Remote phone book can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Specify the access URL and the display name of the remote phone book. **Parameters:** remote_phonebook.data.X.url remote_phonebook.data.X.name remote_phonebook.display_name

		Specify whether to query the entry name from the remote phone book for outgoing/incoming calls. **Parameter:** features.remote_phonebook.enable
		Specify how often the DECT IP phone refreshes the local cache of the remote phone book. **Parameter:** features.remote_phonebook.flash_time
Web User Interface		Specify the access URL and the display name of the remote phone book. Specify whether to query the entry name from the remote phone book for outgoing/incoming calls. Specify how often the DECT IP phone refreshes the local cache of the remote phone book. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-remote&q=load

Details of Configuration Parameters:

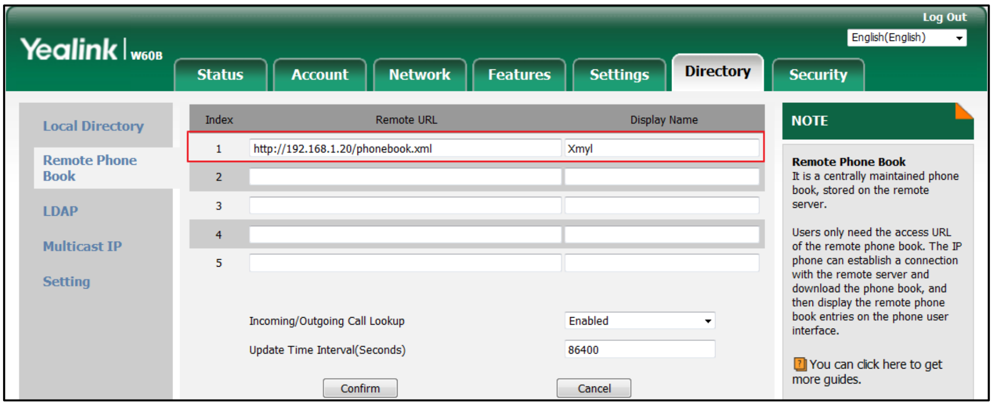
Parameters	Permitted Values	Default
remote_phonebook.data.X.url (X ranges from 1 to 8)	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the remote phone book. **Example:** remote_phonebook.data.1.url = http://192.168.1.20/phonebook.xml **Web User Interface:** Directory->Remote Phone Book->Remote URL **Handset User Interface:** None		
remote_phonebook.data.X.name (X ranges from 1 to 8)	**String within 99 characters**	**Blank**

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Description:
Configures the display name of the remote phone book item.
Example:
remote_phonebook.data.1.name = Xmyl
“Xmyl” will be displayed on the LCD screen at the handset path OK->Directory->Remote Phone Book. The name of Remote Phone Book can be configured by the parameter “remote_phonebook.display_name”.
Web User Interface:
Directory->Remote Phone Book->Display Name
Handset User Interface:
None</td></tr>
<tr><td>remote_phonebook.display_name</td><td>String within 99 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the display name of the remote phone book.
Example:
remote_phonebook.display_name = Friends
“Friends” will be displayed on the LCD screen at the phone path OK->Directory.
If it is left blank, Remote Phone Book will be the display name.
Web User Interface:
None
Handset User Interface:
None</td></tr>
<tr><td>features.remote_phonebook.enable</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables the DECT IP phone to perform a remote phone book search for an incoming or outgoing call and display the matched results on the LCD screen.
0-Disabled
1-Enabled
Web User Interface:
Directory->Remote Phone Book->Incoming/Outgoing Call Lookup
Handset User Interface:
None</td></tr>
</table>

Parameters	Permitted Values	Default
features.remote_phonebook.flash_time	**0, Integer from 3600 to 1296000**	**21600**
Description: Configures how often to refresh the local cache of the remote phone book. If it is set to 3600, the DECT IP phone will refresh the local cache of the remote phone book every 3600 seconds (1 minute). If it is set to 0, the DECT IP phone will refresh the local cache of the remote phone book aperiodically. **Web User Interface:** Directory->Remote Phone Book->Update Time Interval(Seconds) **Handset User Interface:** None		

To specify access URL of the remote phone book via web user interface:

1. Click on **Directory**->**Remote Phone Book**.
2. Enter the access URL in the **Remote URL** field.
3. Enter the name in the **Display Name** field.

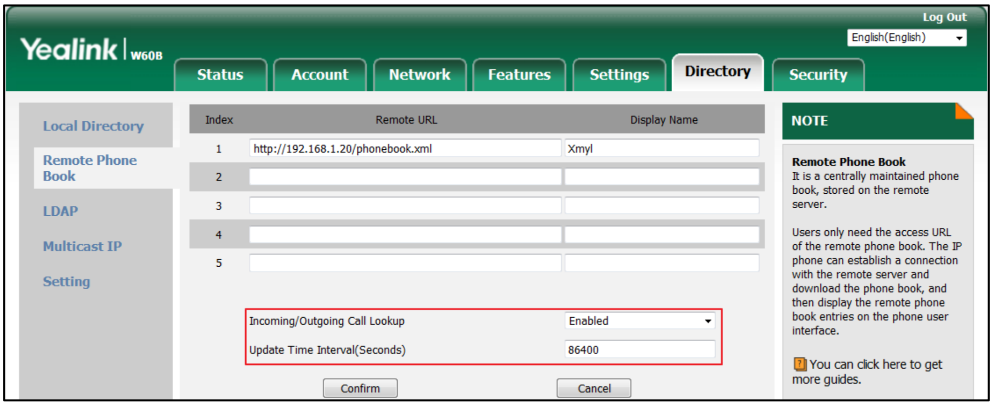


4. Click **Confirm** to accept the change.

To configure incoming/outgoing call lookup and update time interval via web user interface:

1. Click on **Directory**->**Remote Phone Book**.
2. Select the desired value from the pull-down list of **Incoming/Outgoing Call Lookup**.

3. Enter the desired time in the **Update Time Interval(Seconds)** field.



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

Lightweight Directory Access Protocol (LDAP)

LDAP is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. DECT IP phones can be configured to interface with a corporate directory server that supports LDAP version 2 or 3. The following LDAP servers are supported:

- Microsoft Active Directory
- Sun ONE Directory Server
- Open LDAP Directory Server
- Microsoft Active Directory Application Mode (ADAM)

The biggest plus for LDAP is that users can access the central LDAP directory of the corporation using DECT IP phones. Therefore they do not have to maintain the directory locally. Users can search and dial out from the LDAP directory, and save LDAP entries to the local directory. LDAP entries displayed on the DECT IP phone are read only, which cannot be added, edited or deleted by users. When an LDAP server is properly configured, the DECT IP phone can look up entries from the LDAP server in a wide variety of ways. The LDAP server indexes all the data in its entries, and “filters” can be used to select the desired entry or group, and return the desired information.

Configurations on the DECT IP phone limit the amount of the displayed entries when querying from the LDAP server, and decide how attributes are displayed and sorted.

You can set a DSS key to be an LDAP key, and then press the LDAP key to enter the LDAP search screen when the DECT IP phone is idle.

LDAP Attributes

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

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

For more information on LDAP, refer to *LDAP Directory on Yealink IP phones*.

Procedure

LDAP can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure LDAP. **Parameters:** ldap.enable ldap.name_filter ldap.number_filter ldap.tls_mode ldap.host ldap.port ldap.base ldap.user ldap.password ldap.max_hits ldap.name_attr ldap.numb_attr ldap.display_name ldap.version ldap.call_in_lookup

		ldap.call_out_lookup ldap.ldap_sort ldap.incoming_call_special_search.enable
Web User Interface		Configure LDAP. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-LDAP&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
ldap.enable	**0 or 1**	**0**
Description: Enables or disables LDAP feature on the DECT IP phone. **0**-Disabled **1**-Enabled **Web User Interface:** Directory->LDAP->Enable LDAP **Handset User Interface:** None		
ldap.name_filter	**String within 99 characters**	**Blank**
Description: Configures the search criteria for LDAP contact names look up. The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the name prefix entered by the user. **Example:** ldap.name_filter = (|(cn=%)(sn=%)) When the cn or sn of the LDAP contact starts with the entered prefix, the record will be displayed on the LCD screen. ldap.name_filter = (&(cn=*)(sn=%)) When the cn of the LDAP contact is set and the sn of the LDAP contact start with the entered prefix, the records will be displayed on the phone LCD screen. ldap.name_filter = (!(cn=%)) When the cn of the LDAP contact does not start with the entered prefix, the records will be		

Parameters	Permitted Values	Default
displayed on the phone LCD screen. **Web User Interface:** Directory->LDAP->LDAP Name Filter **Handset User Interface:** None		
ldap.number_filter	**String within 99 characters**	**Blank**
Description: Configures the search criteria for LDAP contact numbers look up. The "*" symbol in the filter stands for any number. The "%" symbol in the filter stands for the number prefix entered by the user. **Example:** ldap.number_filter = (|(telephoneNumber=%)(mobile=%)(ipPhone=%)) When the number prefix of the telephoneNumber, mobile or ipPhone of the contact record matches the search criteria, the record will be displayed on the LCD screen. ldap.number_filter = (&(telephoneNumber=*)(mobile=%)) When the telephoneNumber of the LDAP contact is set and the mobile of the LDAP contact starts with the entered prefix, the record will be displayed on the phone LCD screen. **Web User Interface:** Directory->LDAP->LDAP Number Filter **Handset User Interface:** None		
ldap.tls_mode	**0, 1 or 2**	**0**
Description: Configures the connection mode between the LDAP server and the DECT IP phone. **0**-LDAP−Unencrypted connection between LDAP server and the DECT IP phone (port 389 is used by default). **1**-LDAP TLS Start−TLS/SSL connection between LDAP server and the DECT IP phone (port 389 is used by default). **2**-LDAPs−TLS/SSL connection between LDAP server and the DECT IP phone (port 636 is used by default). **Web User Interface:** Directory->LDAP->LDAP TLS Mode **Handset User Interface:**		

Parameters	Permitted Values	Default
None		
ldap.host	**IP address or domain name**	**Blank**
Description: Configures the IP address or domain name of the LDAP server. **Example:** ldap.host = 10.2.1.55 **Web User Interface:** Directory->LDAP->Server Address **Handset User Interface:** None		
ldap.port	**Integer from 1 to 65535**	**389**
Description: Configures the port of the LDAP server. **Example:** ldap.port = 389 **Web User Interface:** Directory->LDAP->Port **Handset User Interface:** None		
ldap.base	**String within 99 characters**	**Blank**
Description: Configures the LDAP search base which corresponds to the location of the LDAP phone book from which the LDAP search request begins. The search base narrows the search scope and decreases directory search time. **Example:** ldap.base = dc=yealink,dc=cn **Web User Interface:** Directory->LDAP->Base **Handset User Interface:** None		

Parameters	Permitted Values	Default
ldap.user	**String within 99 characters**	**Blank**
Description: Configures the user name used to login the LDAP server. This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the user name to login the LDAP server. **Example:** ldap.user = cn=manager,dc=yealink,dc=cn **Web User Interface:** Directory->LDAP->Username **Handset User Interface:** None		
ldap.password	**String within 99 characters**	**Blank**
Description: Configures the password used to login the LDAP server. This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the password to login the LDAP server. **Example:** ldap.password = secret **Web User Interface:** Directory->LDAP->Password **Handset User Interface:** None		
ldap.max_hits	**Integer from 1 to 32000**	**50**
Description: Configures the maximum number of search results to be returned by the LDAP server. If it is set to blank, the LDAP server will return all searched results. **Example:** ldap.max_hits = 50 **Note**: A very large value of this parameter will slow down the LDAP search speed, therefore it should be configured according to the available bandwidth. **Web User Interface:**		

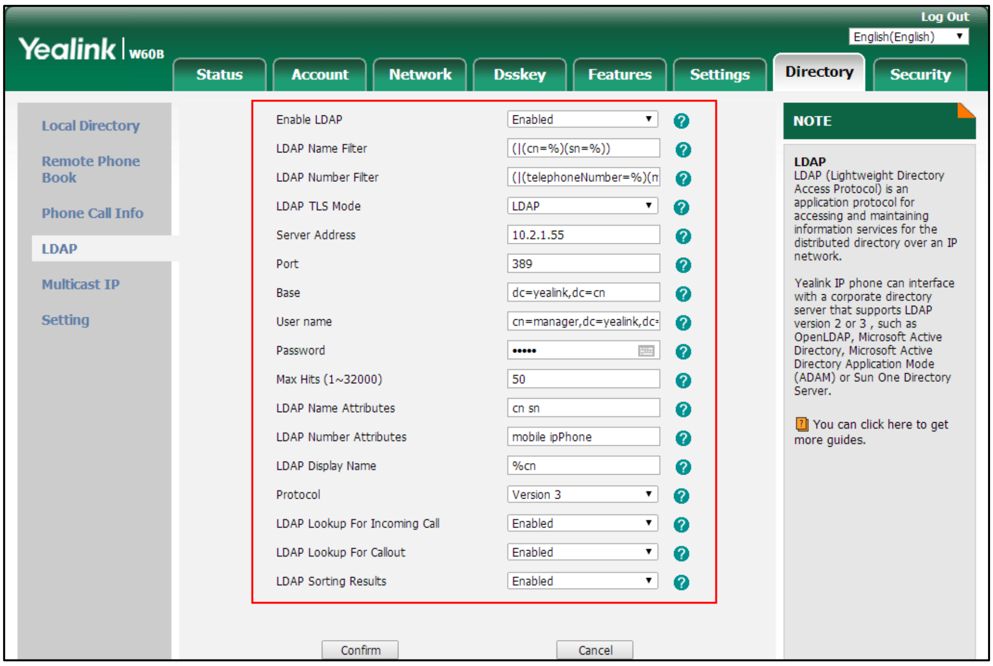
Parameters	Permitted Values	Default
Directory->LDAP->Max Hits (1~32000) **Handset User Interface:** None		
ldap.name_attr	**String within 99 characters**	**Blank**
Description: Configures the name attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple name attributes separated by spaces. **Example:** ldap.name_attr = cn sn This requires the "cn" and "sn" attributes set for each contact record on the LDAP server. **Web User Interface:** Directory->LDAP->LDAP Name Attributes **Handset User Interface:** None		
ldap.numb_attr	**String within 99 characters**	**Blank**
Description: Configures the number attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple number attributes separated by spaces. **Example:** ldap.numb_attr = mobile ipPhone This requires the "mobile" and "ipPhone" attributes set for each contact record on the LDAP server. **Web User Interface:** Directory->LDAP->LDAP Number Attributes **Handset User Interface:** None		
ldap.display_name	**String within 99 characters**	**Blank**
Description: Configures the display name of the contact record displayed on the LCD screen. The value		

Parameters	Permitted Values	Default
must start with "%" symbol. **Example:** ldap.display_name = %cn The cn of the contact record is displayed on the LCD screen. **Web User Interface:** Directory->LDAP->LDAP Display Name **Handset User Interface:** None		
ldap.version	**2 or 3**	**3**
Description: Configures the LDAP protocol version supported by the DECT IP phone. Make sure the protocol value corresponds with the version assigned on the LDAP server. **Web User Interface:** Directory->LDAP->Protocol **Handset User Interface:** None		
ldap.call_in_lookup	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to perform an LDAP search when receiving an incoming call. **0**-Disabled **1**-Enabled **Web User Interface:** Directory->LDAP->LDAP Lookup For Incoming Call **Handset User Interface:** None		
ldap.call_out_lookup	**0 or 1**	**1**
Description: Enables or disables the DECT IP phone to perform an LDAP search when placing a call. **0**-Disabled **1**-Enabled		

Parameters	Permitted Values	Default
Web User Interface: Directory->LDAP->LDAP Lookup For Callout **Handset User Interface:** None		
ldap.ldap_sort	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to sort the search results in alphabetical order or numerical order. **0**-Disabled **1**-Enabled **Web User Interface:** Directory->LDAP->LDAP Sorting Results **Handset User Interface:** None		
ldap.incoming_call_special_search.enable	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to search the telephone numbers starting with "+" symbol and "00" from the LDAP server if the incoming phone number starts with"+" or "00". When completing the LDAP search, the all search results will be displayed on the LCD screen. **0**-Disabled **1**-Enabled For example, If the phone receives an incoming call from the phone number 0044123456789, it will search 0044123456789 from the LDAP sever first, if no result found, it will search +44123456789 from the server again. The phone will display all the search results. **Note:** It works only if the value of the parameter "ldap.call_in_lookup" is set to 1 (Enabled). You may need to set the value of the parameter "ldap.name_filter" to be (|(cn=%)(sn=%)(telephoneNumber=%)(mobile=%)) for searching the telephone numbers starting with "+" symbol. **Web User Interface:** None **Handset User Interface:** None		

To configure LDAP via web user interface:

1. Click on **Directory**->**LDAP**.
2. Enter the values in the corresponding fields.
3. Select the desired values from the corresponding pull-down lists.



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

Shared Call Appearance (SCA)

SCA allows users to share an extension which can be registered on two or more DECT IP phones at the same time. For more information on how to register accounts, refer to Account Registration on page 144.

Any DECT IP phone can be used to originate or receive calls on the shared line. An incoming call can be presented to multiple phones simultaneously. The incoming call can be answered on any DECT IP phone but not all. A call that is active on one DECT IP phone will be presented visually to other DECT IP phones that share the call appearance.

DECT IP phones support SCA using a SUBSCRIBE/NOTIFY mechanism as specified in RFC 3265. The events used are:

- "call-info" for call appearance state notification
- "line-seize" for the DECT IP phone to ask to seize the line

SCA supports the DECT IP phones barging in an active call. In addition, SCA has the call pull capability. Call pull feature allows users to retrieve an existing call from another shared phone that is in active or public hold status.

If the call is placed on public hold, the held call is available for any shared party to retrieve. If the call is placed on private hold, the held call is only available for the hold party to retrieve.

You need to configure either the private hold soft key or a private hold key before you place the call on private hold.

Procedure

SCA can be configured using the following methods.

<table>
<tr><td rowspan="2">Central Provisioning (Configuration File)</td><td rowspan="2"><MAC>.cfg</td><td>Configure the registration line type.
Parameter:
account.X.shared_line</td></tr>
<tr><td>Configure the barge in soft key.
Parameter:
features.display_sca_barge_in.enable</td></tr>
<tr><td colspan="2">Web User Interface</td><td>Configure the registration line type.
Configure the call pull feature access code.
Navigate to:
http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0</td></tr>
</table>

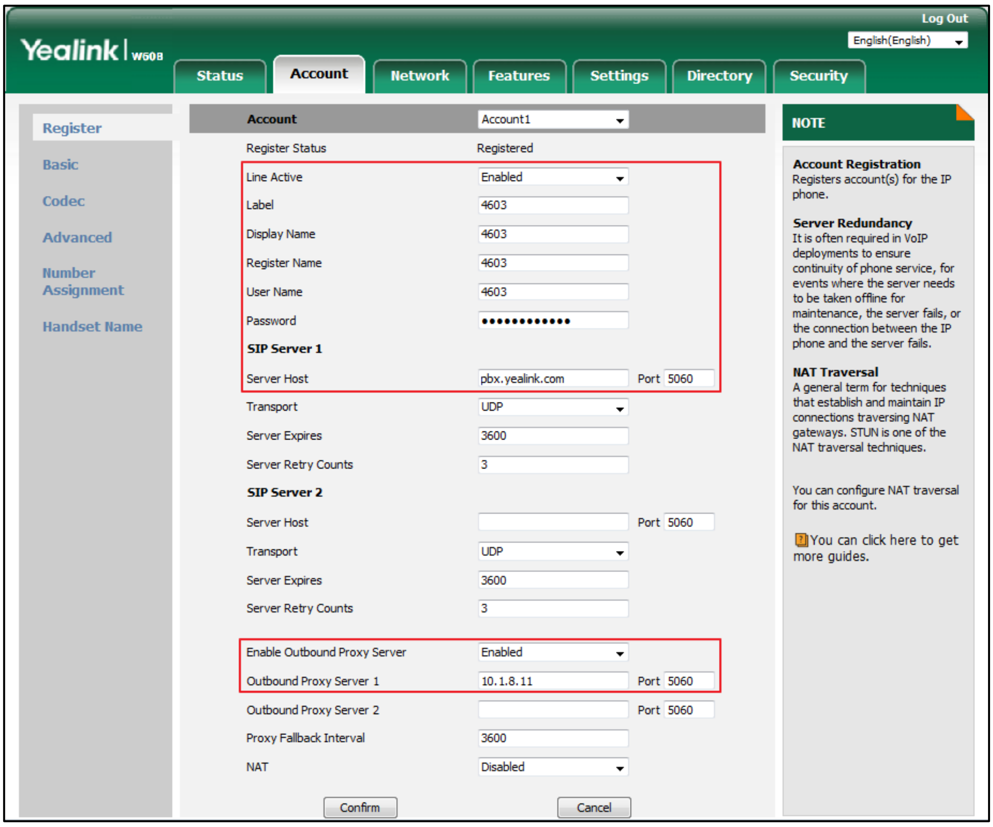
Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>account.X.shared_line
(X ranges from 1 to 8)</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables shared call appearance feature.
0-Disabled
1-Shared Call Appearance
If it is set to 0 (Disabled), the shared line feature is disabled.
Web User Interface:
Account->Advanced->Shared Line
Handset User Interface:
None</td></tr>
<tr><td>features.display_sca_barge_in.enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables to display the barge in option during an SCA call.
0-Disabled</td></tr>
</table>

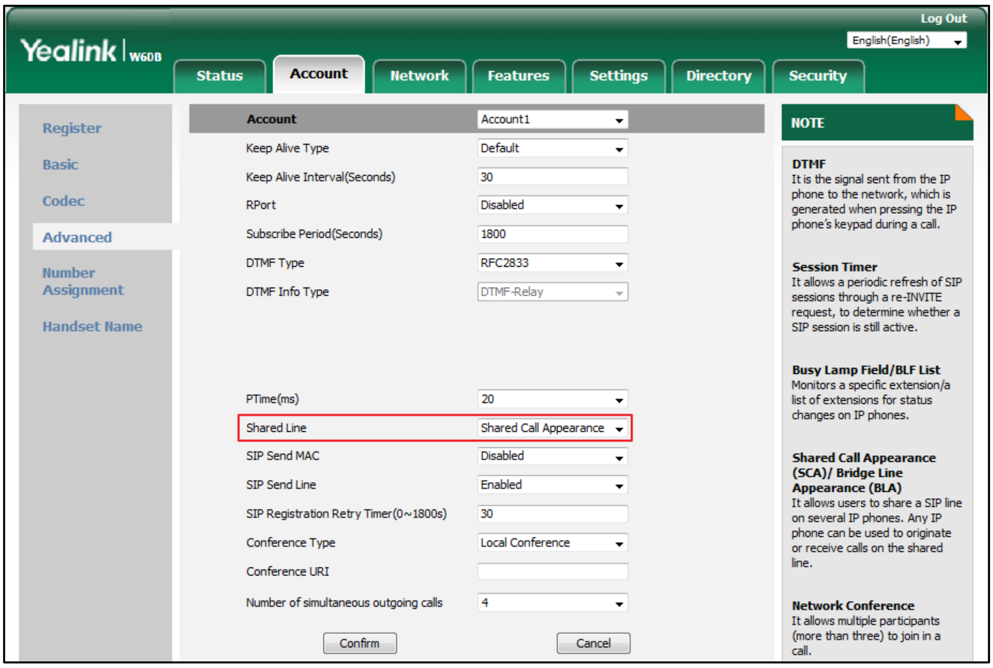
Parameters	Permitted Values	Default
1-Enabled **Web User Interface:** None **Handset User Interface:** None		

To configure the shared line settings on the primary phone via web user interface:

1. Register the primary account (e.g., 4603).



2. Click on **Advanced**, select **Shared Call Appearance** from the pull-down list of **Shared Line**.

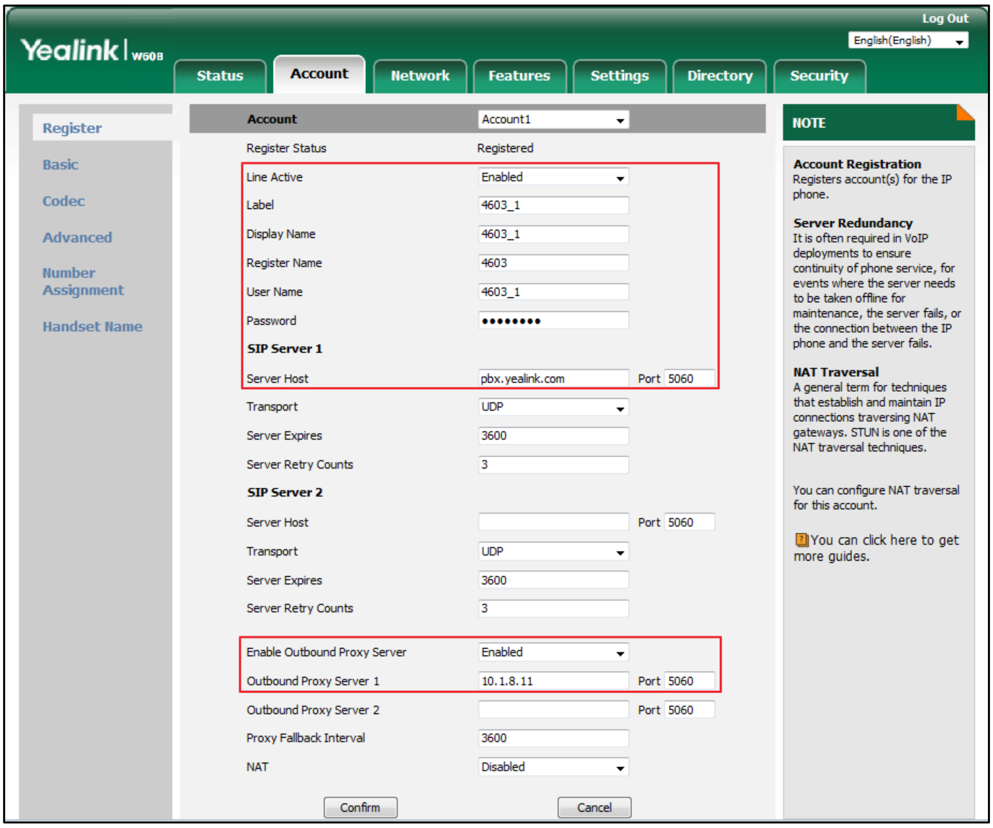


3. Click **Confirm** to accept the change.

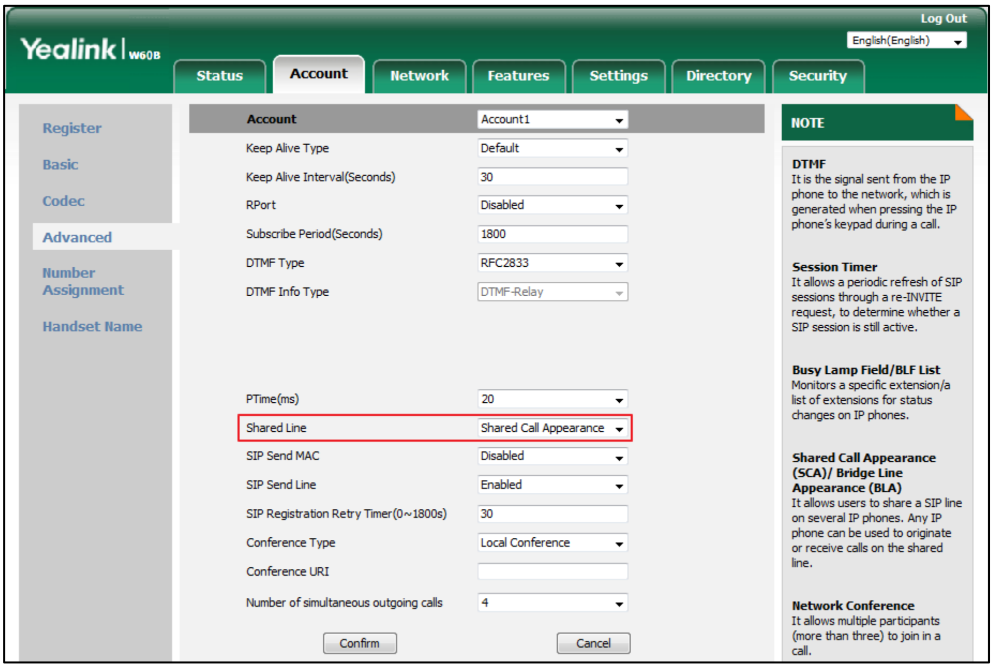
To configure the shared line settings on alternate phone via web user interface:

1. Register the alternate account (e.g., 4603_1).

   (Enter the primary account 4609 in the **Register Name** field.)



2. Click on **Advanced**, select **Shared Call Appearance** from the pull-down list of **Shared Line**.



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

Message Waiting Indicator (MWI)

Message Waiting Indicator (MWI) informs users of the number of messages waiting in their mailbox without calling the mailbox. DECT IP phones support both audio and visual MWI when receiving new voice messages. MWI will be indicated in four ways: a warning tone, an indicator message (including a voice mail icon) on the LCD screen, the power indicator LED slow flashes red (only applicable to W56H handset) or the MESSAGE key LED lights up (only applicable to W52H handset). For more information on power indicator LED, refer to Power Indicator LED on page 118.

DECT IP phones support both solicited and unsolicited MWI.

Unsolicited MWI

Unsolicited MWI is a server related feature. The DECT IP phone sends a SUBSCRIBE message to the server for message-summary updates. The server sends a message-summary NOTIFY within the subscription dialog each time the MWI status changes.

Solicited MWI

For solicited MWI, you must enable MWI subscription feature on DECT IP phones. DECT IP phones support subscribing the MWI messages to the account or the voice mail number.

Procedure

Configuration changes can be performed using the following methods.

<table>
<tr><td rowspan="3">Central Provisioning (Configuration File)</td><td rowspan="3"><MAC>.cfg</td><td>Configure subscribe for MWI.
Parameters:
account.X.subscribe_mwi
account.X.subscribe_mwi_expires</td></tr>
<tr><td>Configure subscribe MWI to voice mail.
Parameter:
account.X.subscribe_mwi_to_vm</td></tr>
<tr><td>Configure the voice mail number on a per-line basis.
Parameter:
voice_mail.number.X</td></tr>
<tr><td colspan="2">Web User Interface</td><td>Configure subscribe for MWI.
Configure subscribe MWI to voice mail.
Configure the voice mail number on a per-line basis.
Navigate to:
http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0</td></tr>
<tr><td colspan="2">Handset User Interface</td><td>Configure the voice mail number on a per-line basis.</td></tr>
</table>

Details of Configuration Parameters:

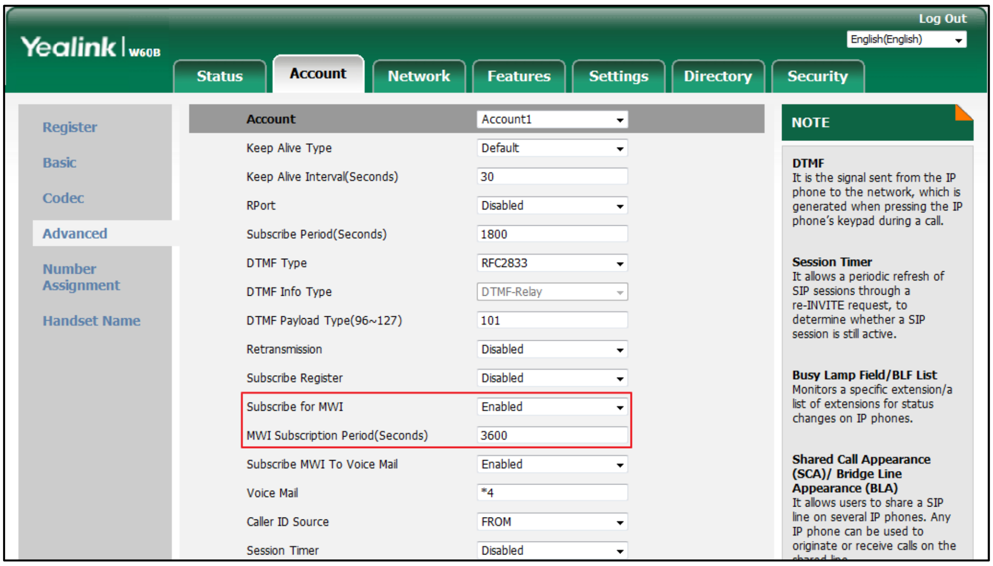
Parameters	Permitted Values	Default
account.X.subscribe_mwi (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to subscribe the message waiting indicator for account X. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the DECT IP phone will send a SUBSCRIBE message to the server for message-summary updates. If it is set to 0 (Disabled), the server automatically sends a message-summary NOTIFY in a		

Parameters	Permitted Values	Default
new dialog each time the MWI status changes. (This requires server support) **Web User Interface:** Account->Advanced->Subscribe for MWI **Handset User Interface:** None		
account.X.subscribe_mwi_expires (X ranges from 1 to 8)	**Integer from 0 to 84600**	**3600**
Description: Configures MWI subscribe expiry time (in seconds) for account X. The DECT IP phone is able to successfully refresh the SUBSCRIBE for message-summary events before expiration of the subscription dialog. **Note**: It works only if the value of the parameter "account.X.subscribe_mwi" is set to 1 (Enabled). **Web User Interface:** Account->Advanced->MWI Subscription Period (Seconds) **Handset User Interface:** None		
account.X.subscribe_mwi_to_vm (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to subscribe the message waiting indicator to the voice mail number for account X. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the DECT IP phone will subscribe the message waiting indicator to the account X. **Note**: It works only if the value of the parameter "account.X.subscribe_mwi" is set to 1 (Enabled) and "voice_mail.number.X" is configured. **Web User Interface:** Account->Advanced->Subscribe MWI To Voice Mail **Handset User Interface:** None		
voice_mail.number.X (X ranges from 1 to 8)	**String within 99 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the voice mail number for account X. **Example:** voice_mail.number.1 = 1234 **Web User Interface:** Account->Advanced->Voice Mail **Handset User Interface:** OK->Voice Mail->Set Voice Mail->LineX->Number		

To configure subscribe for MWI via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Subscribe for MWI**.
4. Enter the period time in the **MWI Subscription Period(Seconds)** field.

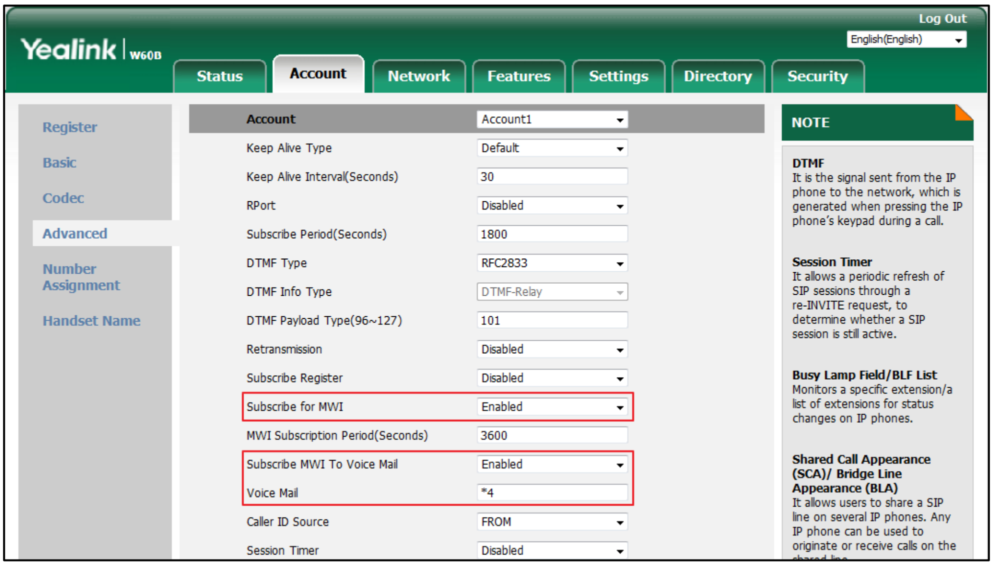


5. Click **Confirm** to accept the change.

To configure subscribe MWI to voice mail via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **Enabled** from the pull-down list of **Subscribe for MWI**.
4. Select the desired value from the pull-down list of **Subscribe MWI To Voice Mail**.

5. Enter the desired voice number in the **Voice Mail** field.



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

Multicast Paging

Multicast paging allows DECT IP phones to send/receive Real-time Transport Protocol (RTP) streams to/from the pre-configured multicast address(es) on the desired channel without involving SIP signaling. Up to 31 listening multicast addresses can be specified on the DECT IP phone.

The following describes 31 paging channels:

- **0**: You can broadcast audio to channel 0. Note that the Yealink IP phones running old firmware version (old paging mechanism) can be regarded as listening to channel 0. It is the default channel.
- **1 to 25**: You can broadcast audio to a specific channel. We recommend that you specify these channels when broadcasting with polycom IP phones which have 25 channels you can listening to.
- **26 to 30**: You can broadcast audio to a specific channel. We recommend that you specify these channels when broadcasting with Yealink IP phones running new firmware version (new paging mechanism).

The DECT IP phones will automatically ignore all incoming multicast paging calls on the different channel.

Sending RTP Stream

Users can send an RTP stream without involving SIP signaling by pressing a configured multicast paging key or a paging list key. A multicast address (IP: Port) and a channel (0 to 30) should be assigned to the multicast paging key, which is defined to transmit RTP stream to a group of designated DECT IP phones on the desired channel.

When the DECT IP phone sends the RTP stream to a pre-configured multicast address belongs to a desired channel, each DECT IP phone preconfigured to listen to the multicast address on the same channel can receive the RTP stream. When the originator stops sending the RTP stream, the subscribers stop receiving it.

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Specify a multicast codec for the DECT IP phone to send the RTP stream. **Parameter:** multicast.codec
		Configure the multicast IP address and port number for a paging list key. **Parameter:** multicast.paging_address.X.ip_address
		Configure the multicast paging group name for a paging list key. **Parameter:** multicast.paging_address.X.label
		Configure the channel of the multicast paging group for a paging list key. **Parameter:** multicast.paging_address.X.channel
Web User Interface		Specify a multicast codec for the DECT IP phone to send the RTP stream. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameters:

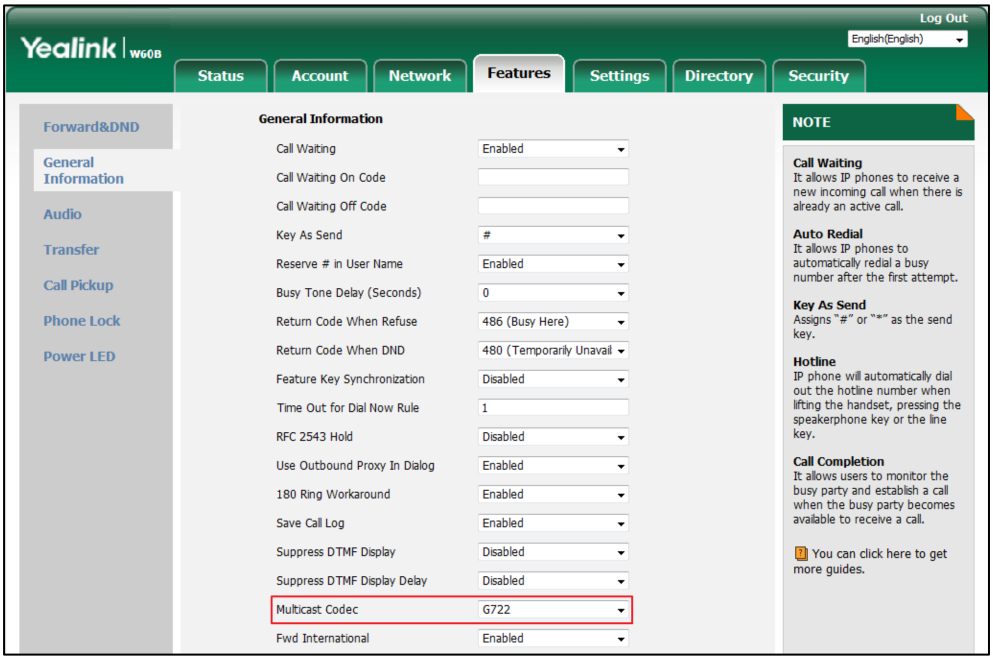
Parameters	Permitted Values	Default
multicast.codec	**PCMU, PCMA, G729, G722**	**G722**
Description: Configures the codec of multicast paging.		

Parameters	Permitted Values	Default
Example: multicast.codec = G722 **Web User Interface:** Features->General Information->Multicast Codec **Handset User Interface:** None		
multicast.paging_address.X.ip_address (X ranges from 1 to 31)	**String**	**Blank**
Description: Configures the IP address and port number of the multicast paging group in the paging list. It will be displayed on the LCD screen when placing the multicast paging call. **Example:** multicast.paging_address.1.ip_address = 224.5.6.20:10008 multicast.paging_address.2.ip_address = 224.1.6.25:1001 **Note**: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255. **Web User Interface:** Directory->Multicast IP->Paging List->Paging Address **Handset User Interface:** None		
multicast.paging_address.X.label (X ranges from 1 to 31)	**String**	**Blank**
Description: Configures the name of the multicast paging group to be displayed in the paging list. It will be displayed on the LCD screen when placing the multicast paging calls. **Example:** multicast.paging_address.1.label = Product multicast.paging_address.2.label = Sales **Web User Interface:** Directory->Multicast IP->Paging List->Label **Handset User Interface:** None		

Parameters	Permitted Values	Default
multicast.paging_address.X.channel (X ranges from 1 to 31)	**Integer from 0 to 30**	**0**
Description: Configures the channel of the multicast paging group in the paging list. If it is set to 0, all the Yealink DECT IP phones running firmware version 80 or prior or Yealink DECT IP phones listens to channel 0 or third-party available devices (e.g., Cisco DECT IP phones) in the paging group can receive the RTP stream. If it is set to 1 to 25, the Polycom or Yealink DECT IP phones preconfigured to listen to the channel can receive the RTP stream. It it is set to 26 to 30, the Yealink DECT IP phones preconfigured to listen to the channel can receive the RTP stream. **Example:** multicast.paging_address.1.channel = 3 multicast.paging_address.2.channel = 5 **Web User Interface:** Directory->Multicast IP->Paging List->Channel **Handset User Interface:** None		

To configure a codec for multicast paging via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired codec from the pull-down list of **Multicast Codec**.

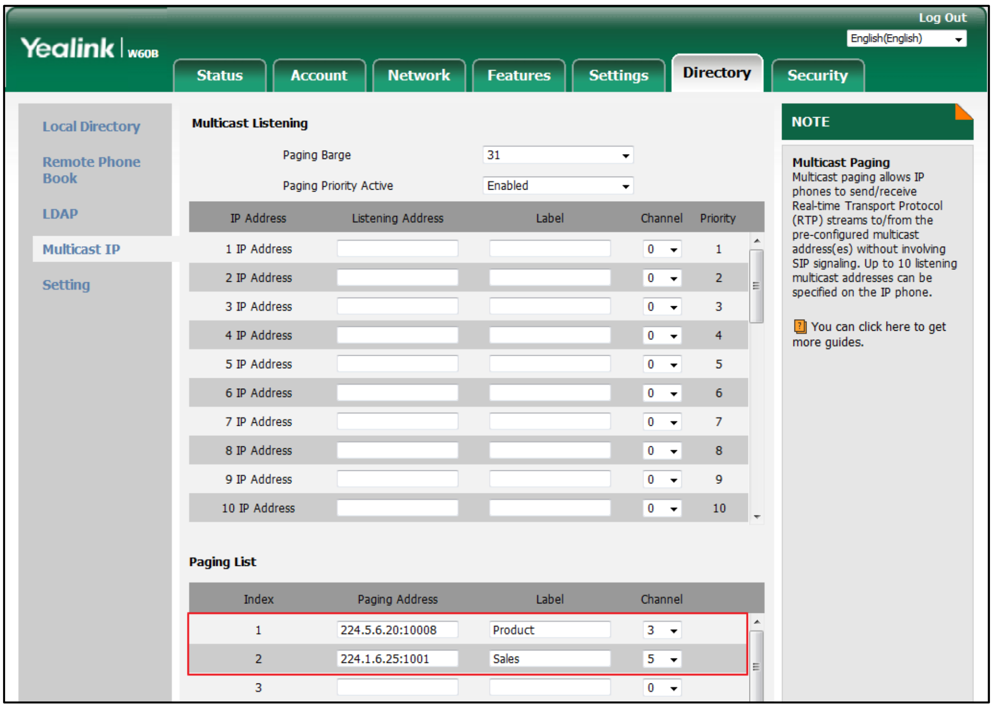


3. Click **Confirm** to accept the change.

To configure two sending multicast addresses via web user interface:

1. Click on **Directory**->**Multicast IP**.
2. Enter the sending multicast address and port number in the **Paging Address** field.
3. Enter the label in the **Label** field.

   The label will appear on the LCD screen when sending the RTP multicast.
4. Select the desired channel from the pull-down list **Channel**.



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

Receiving RTP Stream

IP phones can receive an RTP stream from the pre-configured multicast address(es) on the desired channel without involving SIP signaling, and can handle the incoming multicast paging calls differently depending on the configurations of Paging Barge and Paging Priority Active.

Paging Barge

Paging Barge feature defines the lowest priority of the multicast paging call that can be received when there is a voice call (a normal phone call rather than a multicast paging call) in progress. If it is disabled, all incoming multicast paging calls will be automatically ignored. If it is set to a specify priority value, the incoming multicast paging calls with higher or equal priority are automatically answered and the ones with lower priority are ignored.

Ignore DND

Ignore DND feature defines the lowest priority of the multicast paging call that can be received when DND is activated in phone mode. If it is disabled, all incoming multicast paging calls will be automatically ignored when DND is activated in phone mode. If it is set to a specify priority value, the incoming multicast paging calls with higher or equal priority are automatically answered and the ones with lower priority are ignored. The phone will automatically answer all incoming multicast paging calls when DND is activated in custom mode.

Paging Priority Active

Paging Priority Active feature decides how the IP phone handles the incoming multicast paging calls when there is already a multicast paging call in progress. If it is disabled, the IP phone will automatically ignore all incoming multicast paging calls. If it is enabled, an incoming multicast paging call with higher priority or equal is automatically answered, and the one with lower priority is ignored.

Procedure

Configuration changes can be performed using the following methods.

<table>
<tr><td rowspan="2">Central Provisioning (Configuration File)</td><td rowspan="2">y000000000077.cfg</td><td>Configure the listening multicast address.
Parameters:
multicast.listen_address.X.ip_address
multicast.listen_address.X.label
multicast.listen_address.X.channel
multicast.listen_address.X.volume
multicast.receive.use_speaker</td></tr>
<tr><td>Configure Paging Barge and Paging Priority Active features.
Parameters:
multicast.receive_priority.enable
multicast.receive_priority.priority</td></tr>
<tr><td colspan="2">Web User Interface</td><td>Configure the listening multicast address.
Configure Paging Barge and Paging Priority Active features.
Navigate to:
http://<phoneIPAddress>/servlet?p=contacts-multicastIP&q=load</td></tr>
</table>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
multicast.listen_address.X.ip_address (X ranges from 1 to 31)	**IP address: port**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the multicast address and port number that the DECT IP phone listens to. **Example:** multicast.listen_address.1.ip_address = 224.5.6.20:10008 **Note**: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255. **Web User Interface:** Directory->Multicast IP->Multicast Listening->Listening Address **Handset User Interface:** None		
multicast.listen_address.X.label (X ranges from 1 to 31)	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label to be displayed on the LCD screen when receiving the multicast paging calls. **Example:** multicast.listen_address.1.label = Paging1 **Web User Interface:** Directory->Multicast IP->Multicast Listening->Label **Handset User Interface:** None		
multicast.listen_address.X.channel (X ranges from 1 to 31)	**Integer from 0 to 30**	**0**
Description: Configures the channel that the DECT IP phone listens to. If it is set to 0, the DECT IP phone can receive an RTP stream of the pre-configured multicast address from the DECT IP phones running firmware version 80 or prior, from the DECT IP phones listen to the channel 0, or from the available third-party devices (e.g., Cisco DECT IP phones). If it is set to 1 to 25, the DECT IP phone can receive an RTP stream of the pre-configured multicast address on the channel 1 to 25 respectively from Yealink or Polycom DECT IP phones. It it is set to 26 to 30, the DECT IP phone can receive the RTP stream of the pre-configured multicast address on the channel 26 to 30 respectively from Yealink DECT IP phones. **Example:**		

Parameters	Permitted Values	Default
multicast.listen_address.1.channel = 2 **Web User Interface:** Directory->Multicast IP->Multicast Listening->Channel **Handset User Interface:** None		
multicast.listen_address.X.volume (X ranges from 1 to 31)	**Integer from 0 to 15**	**0**
Description: Configures the volume of the speaker when receiving the multicast paging calls. If it is set to 0, the current volume of the speaker takes effect. The volume of the speaker can be adjusted manually in advance when the phone is during a call. You can also adjust the volume of the speaker during the paging call. If it is set to 1 to 15, the configured volume takes effect and the current volume of the speaker will be ignored. You are not allowed to adjust the volume of the speaker during the paging call. **Example:** multicast.listen_address.1.volume = 1 **Web User Interface:** None **Handset User Interface:** None		
multicast.receive.use_speaker	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to always use the speaker as the audio device when receiving the multicast paging calls. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the engaged audio device will be used when receiving the multicast paging calls. **Note**: If there is an active call on the phone, the call will not be interrupted by the incoming multicast paging calls even if the value of this parameter is set to 1. But there is a warning tone from the speaker. **Web User Interface:** None **Handset User Interface:**		

Parameters	Permitted Values	Default
None		
multicast.receive_priority.enable	**0 or 1**	**1**
Description: Enables or disables the DECT IP phone to handle the incoming multicast paging calls when there is an active multicast paging call on the DECT IP phone. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the DECT IP phone will ignore the incoming multicast paging calls when there is an active multicast paging call on the DECT IP phone. If it is set to 1 (Enabled), the DECT IP phone will receive the incoming multicast paging call with a higher or equal priority and ignore that with a lower priority. **Web User Interface:** Directory->Multicast IP->Paging Priority Active **Handset User Interface:** None		
multicast.receive_priority.priority	**Integer from 0 to 31**	**31**
Description: Configures the priority of the voice call (a normal phone call rather than a multicast paging call) in progress. 1 is the highest priority, 31 is the lowest priority. **0**-Disabled **1**-1 **2**-2 **3**-3 **4**-4 **5**-5 **6**-6 **7**-7 **8**-8 **9**-9 **10**-10 **11**-11 **12**-12		

Parameters	Permitted Values	Default
13-13 **14**-14 **15**-15 **16**-16 **17**-17 **18**-18 **19**-19 **20**-20 **21**-21 **22**-22 **23**-23 **24**-24 **25**-25 **26**-26 **27**-27 **28**-28 **29**-29 **30**-30 **31**-31 If it is set to 0 (Disabled), all incoming multicast paging calls will be automatically ignored when a voice call is in progress. If it is not set to 0 (Disabled), the DECT IP phone will receive the incoming multicast paging call with a higher or same priority than this value and ignore that with a lower priority than this value when a voice call is in progress. **Web User Interface:** Directory->Multicast IP->Paging Barge **Handset User Interface:** None		

To configure multicast listening addresses via web user interface:

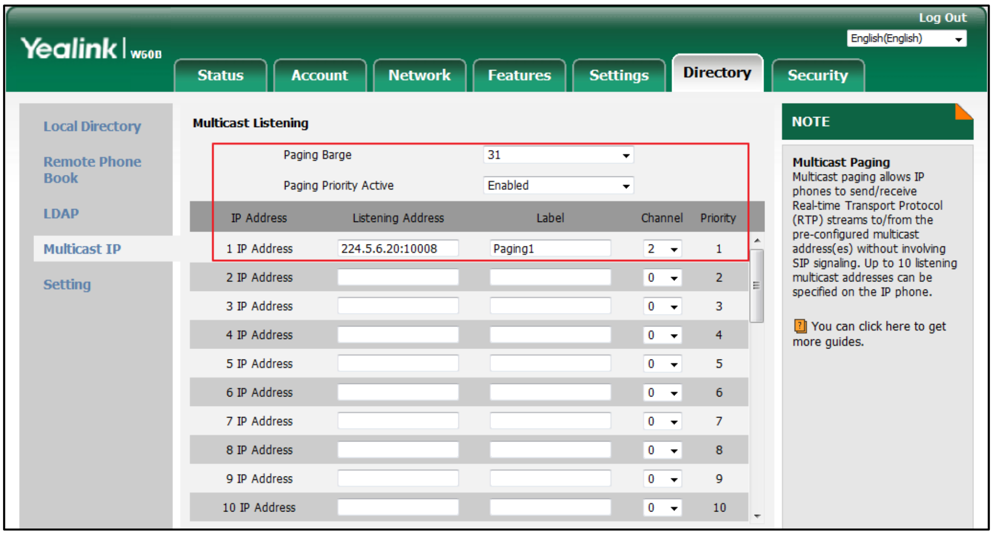
1. Click on **Directory**->**Multicast IP**.
2. Select the desired value from the pull-down list of **Paging Barge**.
3. Select the desired value from the pull-down list of **Paging Priority Active**.
4. Enter the multicast IP address(es) and port number (e.g., 224.5.6.20:10008) which the phone listens to for incoming RTP multicast in the **Listening Address** field.

   1 is the highest priority and 31 is the lowest priority.

5. Enter the label in the **Label** field.

   Label will appear on the LCD screen when receiving the multicast RTP stream.

6. Select the desired channel from the pull-down list of **Channel**.



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

Server Redundancy

Server redundancy is often required in VoIP deployments to ensure continuity of phone service, for events where the server needs to be taken offline for maintenance, the server fails, or the connection between the DECT IP phone and the server fails.

Two types of redundancy are possible. In some cases, a combination of the two may be deployed:

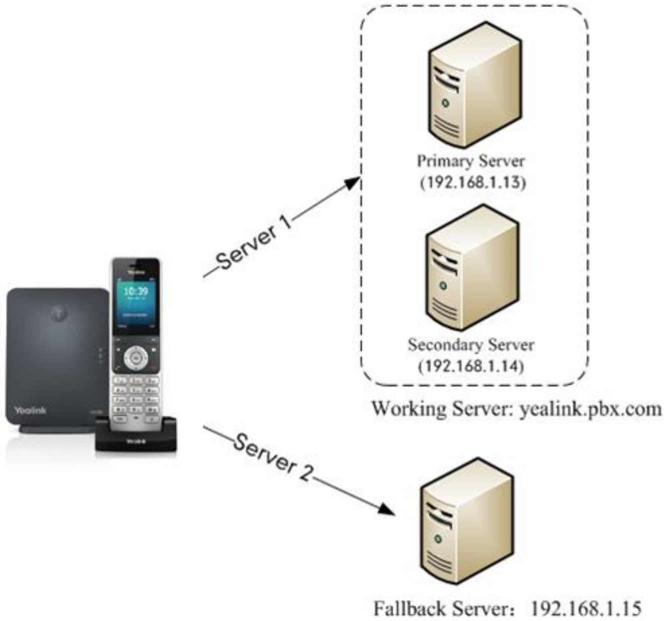
- **Failover:** In this mode, the full phone system functionality is preserved by having a second equivalent capability call server take over from the one that has gone down/off-line. This mode of operation should be done using the DNS mechanism from the primary to the secondary server. Therefore, if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

Note

For concurrent registration mode, it has certain limitation when using some advanced features, and for successive registration mode, the phone service may have a brief interrupt while the server fails. So we recommend you to use the failover mode for server redundancy because this mode can ensure the continuity of the phone service and you can use all the call features while the server fails.

Phone Configuration for Redundancy Implementation

To assist in explaining the redundancy behavior, an illustrative example of how an DECT IP phone may be configured is shown as below. In the example, server redundancy for fallback and failover purposes is deployed. Two separate servers (a working server and a fallback server) are configured for per line registration.



Working Server: Server 1 is configured with the domain name of the working server. For example: yealink.pbx.com. DNS mechanism is used such that the working server is resolved to multiple servers with different IP addresses for failover purpose. The working server is deployed in redundant pairs, designated as primary and secondary servers. The primary server (e.g., 192.168.1.13) has the highest priority server in a cluster of servers resolved by the DNS server. The secondary server (e.g., 192.168.1.14) backs up a primary server when the primary server fails and offers the same functionality as the primary server.

Fallback Server: Server 2 is configured with the IP address of the fallback server. For example, 192.168.1.15. A fallback server offers less functionality than the working server.

Outgoing Call When the Working Server Connection Fails

When a user initiates a call, the DECT IP phone will go through the following steps to connect the call:

1. Sends the INVITE request to the primary server.
2. If the primary server does not respond correctly to the INVITE (that is, the primary server responds to the INVITE with 503 message or the request for responding with 100 Trying message times out (64*T1 seconds, defined in RFC 3261)), then tries to make the call using the secondary server.
3. If the secondary server is also unavailable, the DECT IP phone will try the fallback server until it either succeeds in making a call or exhausts all servers at which point the call will fail.

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

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

Phone Registration

Registration method of the failover mode:

The DECT IP phone must always register to the primary server first except in failover conditions. If this is unsuccessful, the phone will re-register as many times as configured until the registration is successful. When the primary server registration is unavailable, the secondary server will serve as the working server. As soon as the primary server registration succeeds, it returns to being the working server.

Registration methods of the fallback mode include (not applicable to outbound proxy servers):

- **Concurrent registration (default)**: The DECT IP phone registers to SIP server 1 and SIP server 2 (working server and fallback server) at the same time. Note that although the DECT IP phone registers to two SIP servers, only one server works at the same time. In a failure situation, a fallback server can take over the basic calling capability, but without some advanced features (for example, shared lines and MWI) offered by the working server.
- **Successive registration**: The DECT IP phone only registers to one server at a time. The DECT IP phone first registers to the working server. In a failure situation, the DECT IP phone registers to the fallback server, and the fallback server can take over all calling capabilities.

For more information on server redundancy, refer to *Server Redundancy on Yealink IP phones.*

Procedure

Server redundancy can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the SIP server redundancy. **Parameters:** account.X.sip_server.Y.address account.X.sip_server.Y.port account.X.sip_server.Y.expires account.X.sip_server.Y.retry_counts

		Configure the outbound proxy server redundancy. **Parameters:** account.X.outbound_proxy_enable account.X.outbound_proxy.Y.address account.X.outbound_proxy.Y.port
		Fallback Mode **Parameters:** account.X.fallback.redundancy_type account.X.fallback.timeout account.X.outbound_proxy_fallback_interval
		Failover Mode **Parameters:** account.X.sip_server.Y.register_on_enable account.X.sip_server.Y.only_signal_with_registered account.X.sip_server.Y.invite_retry_counts account.X.sip_server.Y.failback_mode account.X.sip_server.Y.failback_timeout account.X.sip_server.Y.failback_subscribe.enable
Web User Interface		Configure the server redundancy on the DECT IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.sip_server.Y.address (X ranges from 1 to 8, Y ranges from 1 to 2)	**String within 256 characters**	**Blank**
Description: Configures the IP address or domain name of the SIP server Y that accepts registrations for account X. **Example:** account.1.sip_server.1.address = yealink.pbx.com **Web User Interface:** Account->Register->SIP Server Y->Server Host		

Parameters	Permitted Values	Default
Handset User Interface: None		
account.X.sip_server.Y.port (X ranges from 1 to 8, Y ranges from 1 to 2)	**Integer from 0 to 65535**	**5060**
Description: Configures the port of the SIP server Y that specifies registrations for account X. **Example:** account.1.sip_server.1.port = 5060 **Note**: If the value of this parameter is set to 0, the port used depends on the value specified by the parameter "account.X.sip_server.Y.transport_type". **Web User Interface:** Account->Register->SIP Server Y->Port **Handset User Interface:** OK->Settings->Telephony->Server (default PIN: 0000) ->Server Y (Account X) ->Port		
account.X.sip_server.Y.expires (X ranges from 1 to 8, Y ranges from 1 to 2)	**Integer from 30 to 2147483647**	**3600**
Description: Configures the registration expiration time (in seconds) of the SIP server Y for account X. **Example:** account.1.sip_server.1.expires = 3600 **Web User Interface:** Account->Register->SIP Server Y->Server Expires **Handset User Interface:** None		
account.X.sip_server.Y.retry_counts (X ranges from 1 to 8, Y ranges from 1 to 2)	**Integer from 0 to 20**	**3**
Description: Configures the retry times for the DECT IP phone to resend requests when the SIP server Y is unavailable or there is no response from the SIP server Y for account X. **Example:** account.1.sip_server.1.retry_counts= 3 The DECT IP phone moves to the next available server after three failed attempts. **Web User Interface:**		

Parameters	Permitted Values	Default
Account->Register->SIP Server Y->Server Retry Counts **Handset User Interface:** None		
account.X.sip_server.Y.register_on_enable (X ranges from 1 to 8, Y ranges from 1 to 2)	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to register to the secondary server before sending requests to it for account X when encountering a failover. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the DECT IP phone won't attempt to register to the secondary server, since the phone assumes that the primary and secondary servers share registration information. So the DECT IP phone will directly send the requests to the secondary server. If it is set to 1 (Enabled), the DECT IP phone will register to the secondary server first, and then send the requests to it. **Note:** It works only if the value of the parameter "account.X.sip_server.Y.failback_mode" is set to 3 (duration). **Web User Interface:** None **Handset User Interface:** None		
account.X.sip_server.Y.only_signal_with_registered (X ranges from 1 to 8, Y ranges from 1 to 2)	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to only send requests to the registered server for account X when encountering a failover. **0**-Disabled **1**-Enabled **Note**: It works only if the value of the parameter "account.X.sip_server.Y.register_on_enable" is set to 1 (Enabled) and the value of the parameter "account.X.sip_server.Y.failback_mode" is set to 1, 2 or 3. **Web User Interface:** None **Handset User Interface:**		

Parameters	Permitted Values	Default
None		
account.X.sip_server.Y.invite_retry_counts (X ranges from 1 to 8, Y ranges from 1 to 2)	**Integer from 1 to 10**	**3**
Description: Configures the number of retries attempted before sending requests to the next available server for account X when encountering a failover. **Web User Interface:** None **Handset User Interface:** None		
account.X.outbound_proxy_enable (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to send requests to the outbound proxy server for account X. **0**-Disabled **1**-Enabled **Web User Interface:** Account->Register->Enable Outbound Proxy Server **Handset User Interface:** OK->Settings->Telephony->Server (default PIN: 0000) ->Outbound Proxy (Account X) ->Outbound Proxy Server		
account.X.outbound_proxy.Y.address (X ranges from 1 to 8, Y ranges from 1 to 2)	**IP address or domain name**	**Blank**
Description: Configures the IP address or domain name of the outbound proxy server Y for account X. **Note:** It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled). **Web User Interface:** Account->Register->Outbound Proxy Server Y **Handset User Interface:** None		

Parameters	Permitted Values	Default
account.X.outbound_proxy.Y.port (X ranges from 1 to 8, Y ranges from 1 to 2)	**Integer from 0 to 65535**	**5060**
Description: Configures the port of the outbound proxy server Y for account X. **Note:** It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled). **Web User Interface:** Account->Register->Outbound Proxy Server Y->Port **Handset User Interface:** OK->Settings->Telephony->Server (default PIN: 0000) ->Outbound Proxy (Account X) ->Port (only applicable to port 1)		
account.X.fallback.redundancy_type (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Configures the registration mode for the DECT IP phone in fallback mode. **0**-Concurrent Registration **1**-Successive Registration **Note:** It is not applicable to outbound proxy servers. **Web User Interface:** None **Handset User Interface:** None		
account.X.fallback.timeout (X ranges from 1 to 8)	**Integer from 10 to 2147483647**	**120**
Description: Configures the time interval (in seconds) for the DECT IP phone to detect whether the working server is available by sending the registration request for account X after the fallback server takes over call control. **Note**: It works only if the value of the parameter "account.X.fallback.redundancy_type" is set to 1 (Successive Registration). It is not applicable to outbound proxy servers. **Web User Interface:** None **Handset User Interface:**		

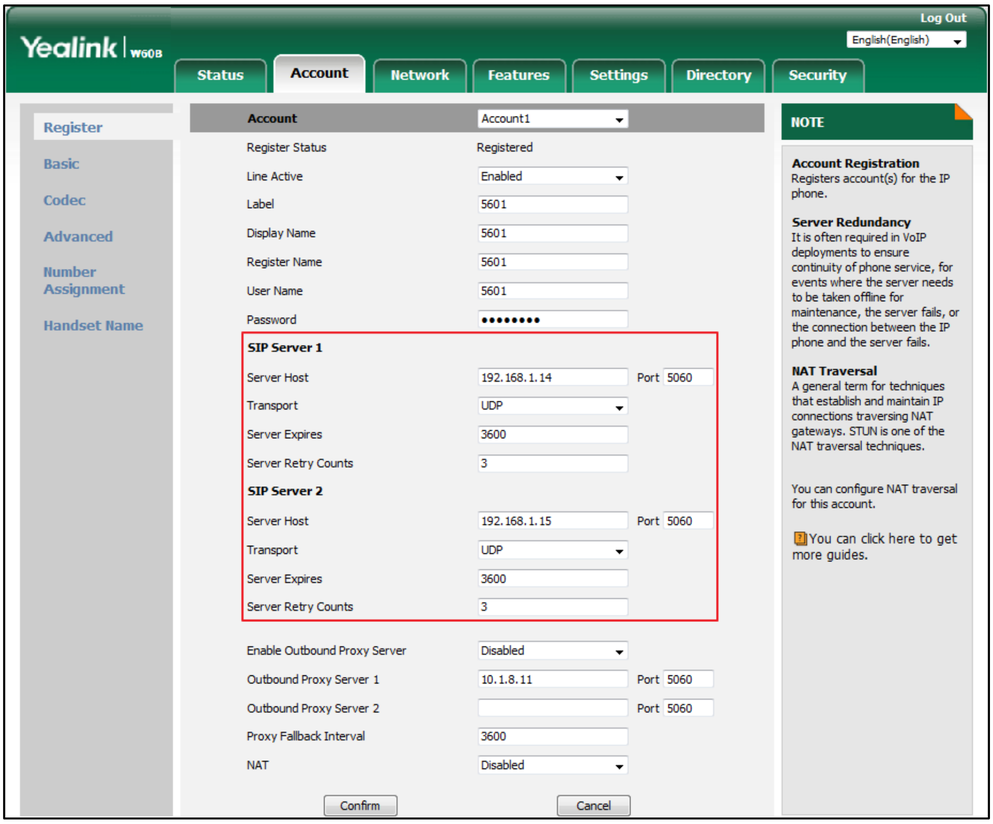
Parameters	Permitted Values	Default
None		
account.X.outbound_proxy_fallback_interval (X ranges from 1 to 8)	**Integer from 0 to 65535**	**3600**
Description: Configures the time interval (in seconds) for the DECT IP phone to detect whether the working outbound proxy server is available by sending the registration request after the fallback server takes over call control. **Example:** account.1.outbound_proxy_fallback_interval = 3600 **Note:** It is only applicable to outbound proxy servers. **Web User Interface:** Account->Register->Proxy Fallback Interval **Handset User Interface:** None		
account.X.sip_server.Y.failback_mode (X ranges from 1 to 8, Y ranges from 1 to 2)	**0, 1, 2 or 3**	**0**
Description: Configures the failback mode for the DECT IP phone to retry the primary server in failover for account X. **0**-newRequests: all requests are sent to the primary server first, regardless of the last server that was used. If the primary server does not respond correctly, the DECT IP phone will try to send requests to the secondary server. **1**-DNSTTL: the DECT IP phone will send requests to the last registered server first. If the TTL for the DNS A records on the registered server expires, the phone will retry to send requests to the primary server. **2**-Registration: the DECT IP phone will send requests to the last registered server first. If the registration expires, the phone will retry to send requests to the primary server. **3**-duration: the DECT IP phone will send requests to the last registered server first. If the time defined by the parameter "account.X.sip_server.Y.failback_timeout" expires, the phone will retry to send requests to the primary server. **Note**: DNSTTL, Registration and duration mode can only be processed when the DECT IP phone is idle (that is, no incoming/outbound calls, no active calls or meetings, etc.). **Web User Interface:** None **Handset User Interface:**		

Parameters	Permitted Values	Default
None		
account.X.sip_server.Y.failback_timeout (X ranges from 1 to 8, Y ranges from 1 to 2)	**0, Integer from 60 to 65535**	**3600**
Description: 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 for account X. If you set the parameter to 0, the DECT IP phone will not send requests to the primary server until a failover event occurs with the current working server. If you set the parameter from 1 to 89, the timeout will be 60 seconds. **Note:** It works only if the value of the parameter "account.X.sip_server.Y.failback_mode" is set to 3 (duration). **Web User Interface:** None **Handset User Interface:** None		
account.X.sip_server.Y.failback_subscribe.enable (X ranges from 1 to 8, Y ranges from 1 to 2)	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to retry to re-subscribe after registering to the secondary server with different IP address for account X when encountering a failover. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the DECT IP phone will immediately re-subscribe to the secondary server, for ensuring the normal use of the features associated with subscription (e.g., SCA). **Note**: It works only if the value of the parameter "account.X.sip_server.Y.failback_mode" is set to 1, 2 or 3. **Web User Interface:** None **Handset User Interface:** None		

To configure server redundancy for fallback purpose via web user interface:

1. Click on **Account**->**Register**.
2. Select the desired account from the pull-down list of **Account**.
3. Configure registration parameters of the selected account in the corresponding fields.

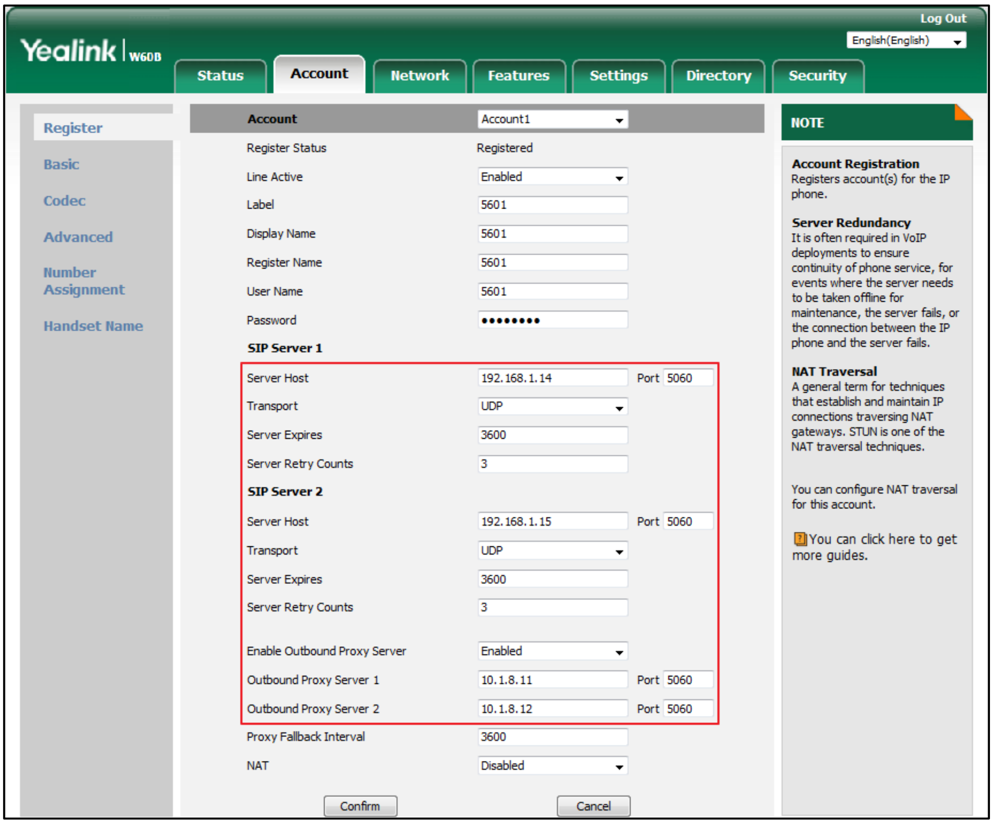
4. Configure parameters of SIP server 1 and SIP server 2 in the corresponding fields.



5. If you use outbound proxy servers, do the following:

   1) Select **Enabled** from the pull-down list of **Enable Outbound Proxy Server**.

2) Configure parameters of outbound proxy server 1 and outbound proxy server 2 in the corresponding fields.



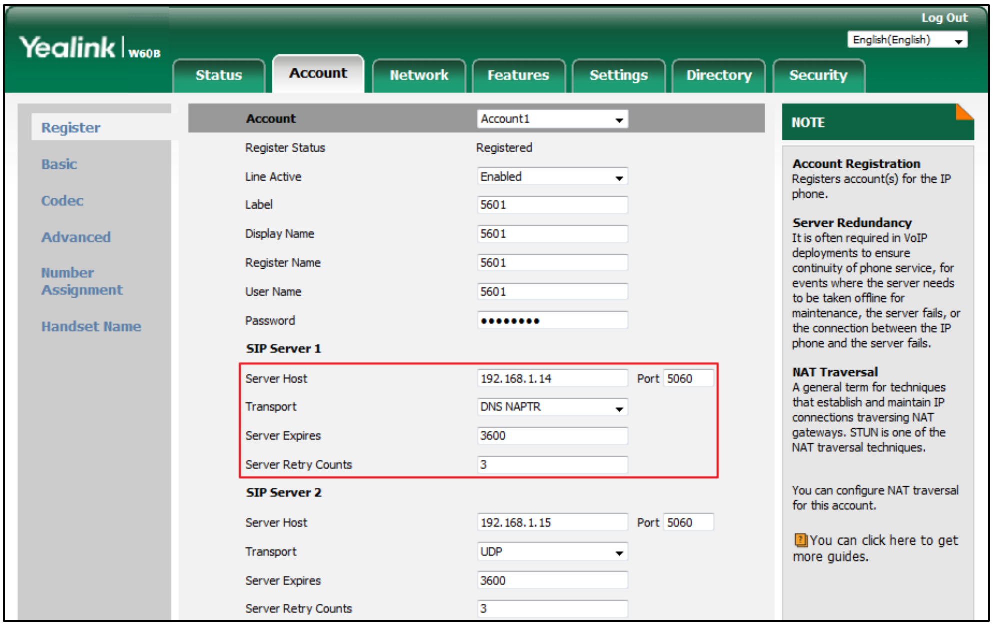
6. Click **Confirm** to accept the change.

To configure server redundancy for failover purpose via web user interface:

1. Click on **Account**->**Register**.
2. Select the desired account from the pull-down list of **Account**.
3. Configure registration parameters of the selected account in the corresponding fields.
4. Configure parameters of the SIP server 1 or SIP server 2 in the corresponding fields.

   You must set the port of SIP server to 0 for NAPTR, SRV and A queries.

5. Select **DNS-NAPTR** from the pull-down list of **Transport**.

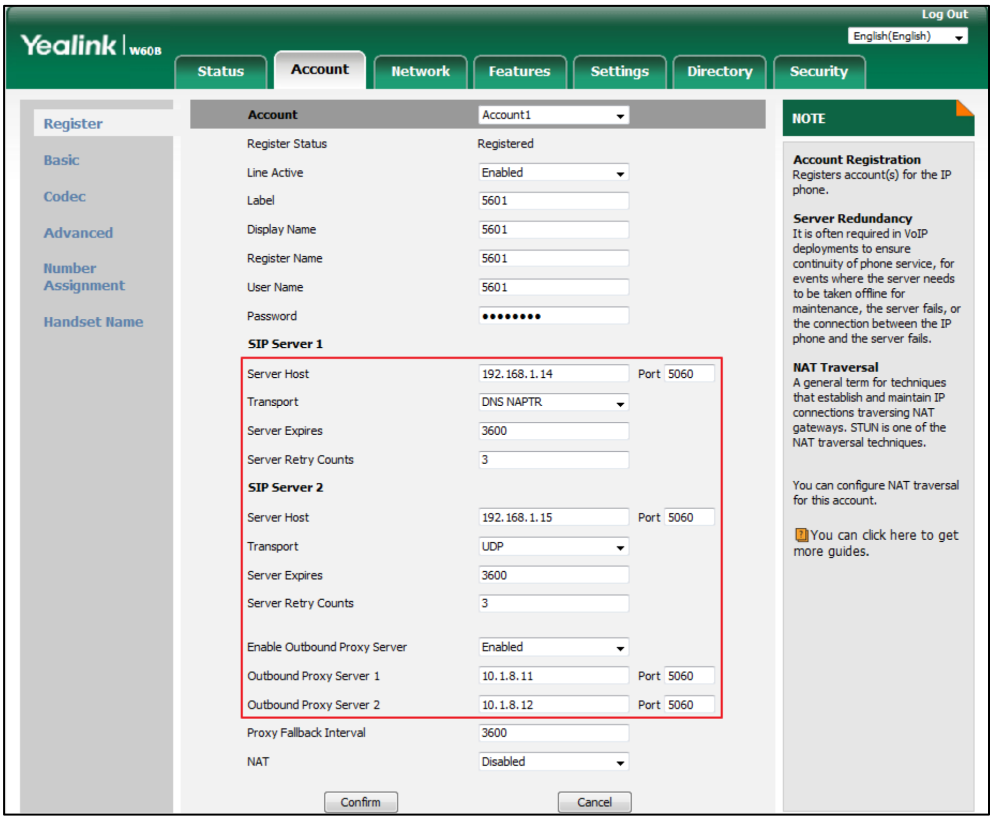


6. If you use outbound proxy servers, do the following:

   1) Select **Enabled** from the pull-down list of **Enable Outbound Proxy Server**.

   2) Configure parameters of outbound proxy server 1/2 in the corresponding fields.

      You must set the port of outbound proxy server to 0 for NAPTR, SRV and A queries.



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

Server Domain Name Resolution

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

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

The following details the procedures of DNS query for the DECT IP phone to resolve the domain name (e.g., yealink.pbx.com) of working server into the IP address, port and transport protocol.

NAPTR (Naming Authority Pointer)

First, the DECT IP phone sends NAPTR query to get the NAPTR pointer and transport protocol. Example of NAPTR records:

	order	pref	flags	service	regexp	replacement
IN NAPTR	90	50	"s"	"SIP+D2T"	""	_sip._tcp.yealink.pbx.com
IN NAPTR	100	50	"s"	"SIP+D2U"	""	_sip._udp.yealink.pbx.com

Parameters are explained in the following table:

Parameter	Description
order	Specify preferential treatment for the specific record. The order is from lowest to highest, lower order is more preferred.
pref	Specify the preference for processing multiple NAPTR records with the same order value. Lower value is more preferred.
Flags	The flag "s" means to perform an SRV lookup.
service	Specify the transport protocols: SIP+D2U: SIP over UDP SIP+D2T: SIP over TCP SIP+D2S: SIP over SCTP SIPS+D2T: SIPS over TCP
regexp	Always empty for SIP services.
replacement	Specify a domain name for the next query.

The DECT IP phone picks the first record because its order of 90 is lower than 100. The pref parameter is unimportant as there is no other record with order 90. The flag "s" indicates performing the SRV query next. TCP will be used, targeted to a host determined by an SRV query of "_sip._tcp.yealink.pbx.com". If the flag of the NAPTR record returned is empty, the DECT IP phone will perform NAPTR query again according to the previous NAPTR query result.

SRV (Service Location Record)

The DECT IP phone performs an SRV query on the record returned from the NAPTR for the host name and the port number. Example of SRV records:

	Priority	Weight	Port	Target
IN SRV	0	1	5060	server1.yealink.pbx.com
IN SRV	0	2	5060	server2.yealink.pbx.com

Parameters are explained in the following table:

Parameter	Description
Priority	Specify preferential treatment for the specific host entry. Lower priority is more preferred.
Weight	When priorities are equal, weight is used to differentiate the preference. The preference is from highest to lowest. Keep the same to load balance.
Port	Identify the port number to be used.
Target	Identify the actual host for an A query.

SRV query returns two records. The two SRV records point to different hosts and have the same priority 0. The weight of the second record is higher than the first one, so the second record will be picked first. The two records also contain a port "5060", the DECT IP phone uses this port. If the Target is not a numeric IP address, the DECT IP phone performs an A query. So in this case, the DECT IP phone uses "server1.yealink.pbx.com" and "server2.yealink.pbx.com" for the A query.

A (Host IP Address)

The DECT IP phone performs an A query for the IP address of each target host name. Example of A records:

Server1.yealink.pbx.com IN A 192.168.1.13

Server2.yealink.pbx.com IN A 192.168.1.14

The DECT IP phone picks the IP address "192.168.1.14" first.

Procedure

SIP Server Domain Name Resolution can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the transport method on the DECT IP phone.

		Parameters: account.X.sip_server.Y.transport_type account.X.naptr_build
Web User Interface		Configure the transport type on the DECT IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-register&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.sip_server.Y.transport_type (X ranges from 1 to 8, Y ranges from 1 to 2)	**0, 1, 2 or 3**	**0**
Description: Configures the transport method the DECT IP phone uses to communicate with the SIP server for account X. **0**-UDP **1**-TCP **2**-TLS **3**-DNS-NAPTR If the value of this parameter is set to 3 (DNS-NAPTR), the value of the parameter “account.X.sip_server.Y.address” is set to a host name and the value of the parameter “account.X.sip_server.Y.port” is set to 0, the DECT IP phone will perform the DNS NAPTR and SRV queries for the transport protocol, ports and servers. If the value of this parameter is set to 3 (DNS-NAPTR), the value of the parameter “account.X.sip_server.Y.address” is set to an IP address and the value of the parameter “account.X.sip_server.Y.port” is set to an explicit port (except 0), then UDP is used. **Web User Interface:** Account->Register->SIP Server Y->Transport **Handset User Interface:** None		
account.X.naptr_build (X ranges from 1 to 8)	**0 or 1**	**0**
Description: Configures the way of SRV query for the DECT IP phone to be performed when no result is returned from NAPTR query for account X.		

Parameters	Permitted Values	Default
0-SRV query using UDP only **1**-SRV query using UDP, TCP and TLS **Web User Interface:** None **Handset User Interface:** None		

Static DNS Cache

Failover redundancy can only be utilized when the configured domain name of the server is resolved to multiple IP addresses. If the DECT 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 DECT IP phone. The DECT IP phone will attempt to resolve the domain name of the SIP server with static DNS cache.

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

- The DECT IP phone performs a DNS query to resolve the domain name from the DNS server.
- If the DNS query returns no results for the domain name, or the returned record cannot be contacted, the values in the static DNS cache (if configured) are used when their configured time intervals are not elapsed.
- If the configured time interval is elapsed, the DECT IP phone will attempt to perform a DNS query again.
- If the DNS query returns a result, the DECT IP phone will use the returned record from the DNS server and ignore the statically configured cache values.

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

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

Support for negative caching of DNS queries as described in RFC 2308 is also provided to allow faster failover when prior DNS queries have returned no results from the DNS server.

DECT IP phones can be configured to use static DNS cache preferentially. Static DNS cache is configurable on a per-line basis.

Procedure

Static DNS cache can be configured only using the configuration files.

<table>
<tr><td rowspan="3">Central Provisioning
(Configuration File)</td><td>y000000000077.cfg</td><td>Configure NAPTR/SRV/A records.
Parameters:
dns_cache_naptr.X.name
dns_cache_naptr.X.flags
dns_cache_naptr.X.order
dns_cache_naptr.X.preference
dns_cache_naptr.X.replace
dns_cache_naptr.X.service
dns_cache_naptr.X.ttl
dns_cache_srv.X.name
dns_cache_srv.X.port
dns_cache_srv.X.priority
dns_cache_srv.X.target
dns_cache_srv.X.weight
dns_cache_srv.X.ttl
dns_cache_a.X.name
dns_cache_a.X.ip
dns_cache_a.X.ttl</td></tr>
<tr><td rowspan="2"><MAC>.cfg</td><td>Configure the DECT IP phone whether to cache the additional DNS records.
Parameter:
account.X.dns_cache_type</td></tr>
<tr><td>Configure the DECT IP phone whether to use static DNS cache preferentially.
Parameter:
account.X.static_cache_pri</td></tr>
</table>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
dns_cache_naptr.X.name (X ranges from 1 to 12)	**Domain name**	**Blank**
Description: Configures the domain name to which NAPTR record X refers.		

Parameters	Permitted Values	Default
Example: dns_cache_naptr.1.name = yealink.pbx.com **Web User Interface:** None **Handset User Interface:** None		
dns_cache_naptr.X.flags (X ranges from 1 to 12)	**S, A, U or P**	**Blank**
Description: Configures the flag of NAPTR record X. (Always "S" for SIP, which means to do an SRV lookup on whatever is in the replacement field). **S**-Do an SRV lookup next **A**-Do an A lookup next **U**-No need to do a DNS query next **P**-Service custom by the user **Example:** dns_cache_naptr.1.flags = S **Note**: For more details of the permitted flags, refer to RFC 2915. **Web User Interface:** None **Handset User Interface:** None		
dns_cache_naptr.X.order (X ranges from 1 to 12)	**Integer from 0 to 65535**	**0**
Description: Configures the order of NAPTR record X. NAPTR record with lower order is more preferred. For example, NAPTR record with the order 90 has the higher priority than that with the order 100 because 90 is lower than 100. **Example:** dns_cache_naptr.1.order = 90 **Web User Interface:** None **Handset User Interface:**		

Parameters	Permitted Values	Default
None		
dns_cache_naptr.X.preference (X ranges from 1 to 12)	**Integer from 0 to 65535**	**0**
Description: Configures the preference of NAPTR record X. NAPTR record with lower value is more preferred when the multiple NAPTR records have the same order value. **Example:** dns_cache_naptr.1.preference = 50 **Web User Interface:** None **Handset User Interface:** None		
dns_cache_naptr.X.replace (X ranges from 1 to 12)	**Domain name with SRV prefix**	**Blank**
Description: Configures a domain name to be used for the next SRV query in NAPTR record X. **Example:** dns_cache_naptr.1.replace = _sip._tcp.yealink.pbx.com **Web User Interface:** None **Handset User Interface:** None		
dns_cache_naptr.X.service (X ranges from 1 to 12)	**String within 32 characters**	**Blank**
Description: Configures the transport protocol available for the server in NAPTR record X. **SIP+D2U**: SIP over UDP **SIP+D2T**: SIP over TCP **SIP+D2S**: SIP over SCTP **SIPS+D2T**: SIPS over TCP **Example:** dns_cache_naptr.1.service = SIP+D2T		

Parameters	Permitted Values	Default
Note: For more information, refer to RFC 2915. **Web User Interface:** None **Handset User Interface:** None		
dns_cache_naptr.X.ttl (X ranges from 1 to 12)	**Integer from 30 to 2147483647**	**300**
Description: Configures the time interval (in seconds) that NAPTR record X may be cached before the record should be consulted again. **Example:** dns_cache_naptr.1.ttl = 3600 **Web User Interface:** None **Handset User Interface:** None		
dns_cache_srv.X.name (X ranges from 1 to 12)	**Domain name with SRV prefix**	**Blank**
Description: Configures the domain name in SRV record X. **Example:** dns_cache_srv.1.name = _sip._tcp.yealink.pbx.com **Web User Interface:** None **Handset User Interface:** None		
dns_cache_srv.X.port (X ranges from 1 to 12)	**Integer from 0 to 65535**	**0**
Description: Configures the port to be used in SRV record X. **Example:** dns_cache_srv.1.port = 5060		

Parameters	Permitted Values	Default
Note: For more information, refer to RFC 2782. **Web User Interface:** None **Handset User Interface:** None		
dns_cache_srv.X.priority (X ranges from 1 to 12)	**Integer from 0 to 65535**	**0**
Description: Configures the priority for the target host in SRV record X. Lower priority is more preferred. For example, SRV record with the priority value 0 is more preferred than that with the priority value 1 because 0 is lower than 1. **Note**: For more information, refer to RFC 2782. **Web User Interface:** None **Handset User Interface:** None		
dns_cache_srv.X.target (X ranges from 1 to 12)	**Domain name**	**Blank**
Description: Configures the domain name of the target host for an A query in SRV record X. **Example:** dns_cache_srv.1.target = server1.yealink.pbx.com **Note**: For more information, refer to RFC 2782. **Web User Interface:** None **Handset User Interface:** None		
dns_cache_srv.X.weight (X ranges from 1 to 12)	**Integer from 0 to 65535**	**0**
Description: Configures the weight of the target host in SRV record X. When priorities are equal, weight is used to differentiate the preference. Higher weight value is more preferred.		

Parameters	Permitted Values	Default
Example: dns_cache_srv.1.weight = 1 **Note**: For more information, refer to RFC 2782. **Web User Interface:** None **Handset User Interface:** None		
dns_cache_srv.X.ttl (X ranges from 1 to 12)	**Integer from 30 to 2147483647**	**300**
Description: Configures the time interval (in seconds) that SRV record X may be cached before the record should be consulted again. **Example:** dns_cache_srv.1.ttl = 3600 **Web User Interface:** None **Handset User Interface:** None		
dns_cache_a.X.name (X ranges from 1 to 12)	**Domain name**	**Blank**
Description: Configures the domain name in A record X. **Example:** dns_cache_a.1.name = yealink.pbx.com **Web User Interface:** None **Handset User Interface:** None		
dns_cache_a.X.ip (X ranges from 1 to 12)	**IP address**	**Blank**
Description: Configures the IP address that the domain name in A record X maps to. **Example:**		

Parameters	Permitted Values	Default
dns_cache_a.1.ip = 192.168.1.13 **Web User Interface:** None **Handset User Interface:** None		
dns_cache_a.X.ttl (X ranges from 1 to 12)	**Integer from 30 to 2147483647**	**300**
Description: Configures the time interval (in seconds) that A record X may be cached before the record should be consulted again. **Example:** dns_cache_a.1.ttl = 3600 **Web User Interface:** None **Handset User Interface:** None		
account.X.dns_cache_type (X ranges from 1 to 8)	**0, 1 or 2**	**1**
Description: Configures whether the DECT IP phone uses the DNS cache for domain name resolution of the server and caches the additional DNS records for account X. **0**-Perform real-time DNS query rather than using DNS cache. **1**-Use DNS cache, but do not cache the additional DNS records. **2**-Use DNS cache and cache the additional DNS records. **Example:** account.1.dns_cache_type = 1 **Web User Interface:** None **Handset User Interface:** None		
account.X.static_cache_pri (X ranges from 1 to 8)	**0 or 1**	**0**
Description:		

Parameters	Permitted Values	Default
Configures whether preferentially to use the static DNS cache for domain name resolution of the server for account X. **0**-Use domain name resolution from the DNS server preferentially **1**-Use static DNS cache preferentially **Example:** account.1.static_cache_pri = 1 **Web User Interface:** None **Handset User Interface:** None		

Real-Time Transport Protocol (RTP) Ports

The Real-time Transport Protocol (RTP) is a network protocol for delivering audio over IP networks. The phone is compatible with RFC 1889 - RTP: A Transport Protocol for Real-Time Applications - and the updated RFC 3550. It treats all RTP streams as bi-directional from a control perspective and expects that both RTP end points will negotiate the respective destination IP addresses and ports.

You can specify the DECT IP phone's RTP port range. Since the DECT IP phone supports conferencing and multiple RTP streams, it can use several ports concurrently. The UDP port used for RTP streams is traditionally an even-numbered port. For example, the default RTP min port on the DECT IP phones is 11780. The first voice session sends RTP on port 11780. Additional calls would then use ports 11782, 11784, 11786, etc. up to the max port.

Procedure

RTP ports can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure RTP ports. **Parameters:** static.network.port.max_rtpport static.network.port.min_rtpport
Web User Interface		Configure RTP ports. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load

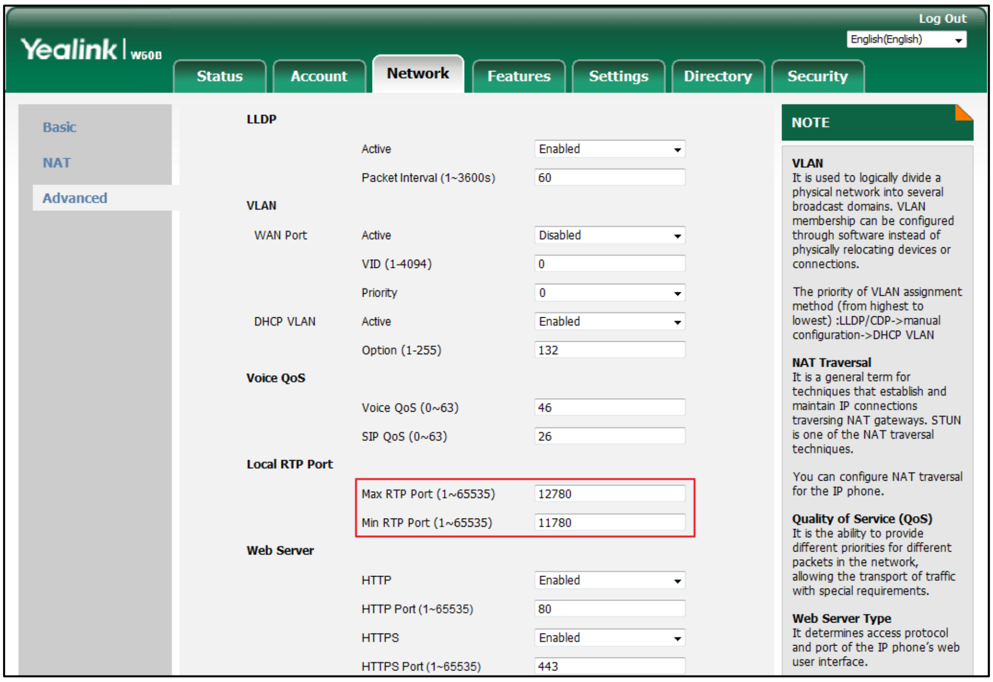
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.port.min_rtpport	**Integer from 1 to 65535**	**11780**
Description: Configures the minimum local RTP port. **Note**: If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Local RTP Port->Min RTP Port(1~65535) **Handset User Interface:** None		
static.network.port.max_rtpport	**Integer from 1 to 65535**	**12780**
Description: Configures the maximum local RTP port. **Note**: The value of the maximum local RTP port cannot be less than that of the minimum local RTP port (configured by the parameter "static.network.port.min_rtpport"). If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Local RTP Port->Max RTP Port(1~65535) **Handset User Interface:** None		

To configure the minimum and maximum RTP port via web user interface:

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

2. In the **Local RTP Port** block, enter the max and min RTP port in the **Max RTP Port(1~65535)** and **Min RTP Port(1~65535)** field respectively.



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

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

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

TR-069 Device Management

TR-069 is a technical specification defined by the Broadband Forum, which defines a mechanism that encompasses secure auto-configuration of a CPE (Customer-Premises Equipment), and incorporates other CPE management functions into a common framework. TR-069 uses common transport mechanisms (HTTP and HTTPS) for communication between CPE and ACS (Auto Configuration Servers). The HTTP(S) messages contain XML-RPC methods defined in the standard for configuration and management of the CPE.

TR-069 is intended to support a variety of functionalities to manage a collection of CPEs, including the following primary capabilities:

- Auto-configuration and dynamic service provisioning
- Software or firmware image management
- Status and performance monitoring
- Diagnostics

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

RPC Method	Description
GetRPCMethods	This method is used to discover the set of methods supported by the CPE.
SetParameterValues	This method is used to modify the value of one or more CPE parameters.
GetParameterValues	This method is used to obtain the value of one or more CPE parameters.
GetParameterNames	This method is used to discover the parameters accessible on a particular CPE.
GetParameterAttributes	This method is used to read the attributes associated with one or more CPE parameters.
SetParameterAttributes	This method is used to modify attributes associated with one or more CPE parameters.
Reboot	This method causes the CPE to reboot.
Download	This method is used to cause the CPE to download a specified file from the designated location. File types supported by DECT IP phones are: ● Firmware Image ● Configuration File
Upload	This method is used to cause the CPE to upload a specified file to the designated location. File types supported by DECT IP phones are: ● Configuration File ● Log File
ScheduleInform	This method is used to request the CPE to schedule a one-time Inform method call (separate from its periodic Inform method calls) sometime in the future.
FactoryReset	This method resets the CPE to its factory default state.
TransferComplete	This method informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.
AddObject	This method is used to add a new instance of an object defined on the CPE.
DeleteObject	This method is used to remove a particular instance of an object.

For more information on TR-069, refer to *Yealink TR-069 Technote*.

Procedure

TR-069 can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure TR-069 feature. **Parameters:** static.managementserver.enable static.managementserver.username static.managementserver.password static.managementserver.url static.managementserver.connection_request_username static.managementserver.connection_request_password static.managementserver.periodic_inform_enable static.managementserver.periodic_inform_interval
Web User Interface		Configure TR-069 feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-tr069&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.managementserver.enable	**0 or 1**	**0**
Description: Enables or disables the TR-069 feature. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->TR069->Enable TR069 **Handset User Interface:** None		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>static.managementserver.username</td><td>String within 128 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the user name for the DECT IP phone to authenticate with the ACS (Auto Configuration Servers).
Leave it blank if no authentication is required.
Example:
static.managementserver.username = tr69
Web User Interface:
Settings->TR069->ACS Username
Handset User Interface:
None</td></tr>
<tr><td>static.managementserver.password</td><td>String within 64 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the password for the DECT IP phone to authenticate with the ACS (Auto Configuration Servers).
Leave it blank if no authentication is required.
Example:
static.managementserver.password = tr69
Web User Interface:
Settings->TR069->ACS Password
Handset User Interface:
None</td></tr>
<tr><td>static.managementserver.url</td><td>URL within 511 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the access URL of the ACS (Auto Configuration Servers).
Example:
static.managementserver.url = http://officetelprov.orangero.net:8080/ftacs-digest/ACS</td></tr>
</table>

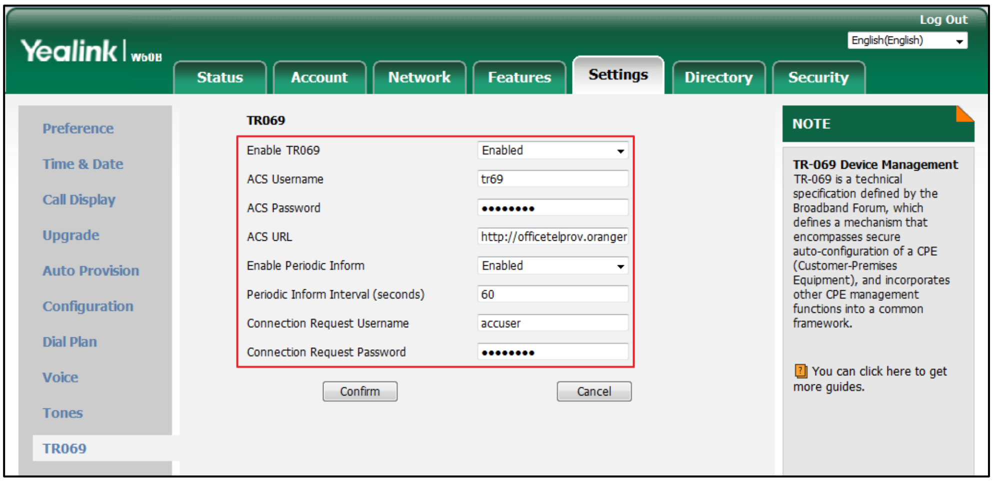
Parameters	Permitted Values	Default
Web User Interface: Settings->TR069->ACS URL **Handset User Interface:** None		
static.managementserver.connection_request_username	**String within 128 characters**	**Blank**
Description: Configures the user name for the DECT IP phone to authenticate the incoming connection requests of the ACS (Auto Configuration Servers). **Example:** static.managementserver.connection_request_username = accuser **Web User Interface:** Settings->TR069->Connection Request Username **Handset User Interface:** None		
static.managementserver.connection_request_password	**String within 64 characters**	**Blank**
Description: Configures the password for the DECT IP phone to authenticate the incoming connection requests of the ACS (Auto Configuration Servers). **Example:** static.managementserver.connection_request_password = acspwd **Web User Interface:** Settings->TR069->Connection Request Password **Handset User Interface:** None		
static.managementserver.periodic_inform_enable	**0 or 1**	**1**
Description: Enables or disables the DECT IP phone to periodically report its configuration information to the ACS (Auto Configuration Servers). **0**-Disabled		

Parameters	Permitted Values	Default
1-Enabled **Web User Interface:** Settings->TR069->Enable Periodic Inform **Handset User Interface:** None		
static.managementserver.periodic_inform_interval	**Integer from 5 to 4294967295**	**60**
Description: Configures the interval (in seconds) for the DECT IP phone to report its configuration to the ACS (Auto Configuration Servers). **Note**: It works only if the value of the parameter "static.managementserver.periodic_inform_enable" is set to 1 (Enabled). **Web User Interface:** Settings->TR069->Periodic Inform Interval (seconds) **Handset User Interface:** None		

To configure TR-069 via web user interface:

1. Click on **Settings**->**TR069**.
2. Select **Enabled** from the pull-down list of **Enable TR069**.
3. Enter the user name and password authenticated by the ACS in the **ACS Username** and **ACS Password** fields.
4. Enter the URL of the ACS in the **ACS URL** field.
5. Select the desired value from the pull-down list of **Enable Periodic Inform**.
6. Enter the desired time in the **Periodic Inform Interval (seconds)** field.

7. Enter the user name and password authenticated by the DECT IP phone in the **Connection Request Username** and **Connection Request Password** fields.



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

Configuring Audio Features

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

- Tones
- Voice Mail Tone
- Ringer Device for Headset
- Audio Codecs
- Acoustic Clarity Technology
- DTMF
- Voice Quality Monitoring (VQM)

Tones

When receiving a message, the DECT IP phone will play a warning tone. You can customize tones or select specialized tone sets (vary from country to country) to indicate different conditions of the DECT IP phone. The default tones used on DECT IP phones are the US tone sets. Available tone sets for DECT IP phones:

- Australia
- Austria
- Brazil
- Belgium
- China
- Czech
- Denmark
- Finland
- France
- Germany
- Great Britain
- Greece
- Hungary
- Lithuania
- India
- Italy

- Japan
- Mexico
- New Zealand
- Netherlands
- Norway
- Portugal
- Spain
- Switzerland
- Sweden
- Russia
- United States
- Chile
- Czech ETSI

Configured tones can be heard on DECT IP phones for the following conditions.

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

Procedure

Tones can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the tones for the DECT IP phone. **Parameters:** voice.tone.country voice.tone.dial voice.tone.ring voice.tone.busy voice.tone.callwaiting
Web User Interface		Configure the tones for the DECT IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?

	p=settings-tones&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
voice.tone.country	**Refer to the following content**	**Custom**
Description: Configures the country tone for the DECT IP phone. **Permitted Values:** Custom, Australia, Austria, Brazil, Belgium, Chile, China, Czech, Czech ETSI, Denmark, Finland, France, Germany, Great Britain, Greece, Hungary, Lithuania, India, Italy, Japan, Mexico, New Zealand, Netherlands, Norway, Portugal, Spain, Switzerland, Sweden, Russia, United States. **Example:** voice.tone.country = Custom **Web User Interface:** Settings->Tones->Select Country **Handset User Interface:** None		
voice.tone.dial	**String**	**Blank**
Description: Customizes the dial tone. tonelist = element[,element] [,element]… **element** = [!]Freq1[+Freq2][+Freq3][+Freq4] /Duration **Freq**: the frequency of the tone (ranges from 200 to 4000Hz). If it is set to 0Hz, it means the tone is not played. **Duration**: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms. You can configure at most eight different tones for one condition, and separate them by commas. (e.g., 250/200,0/1000,200+300/500,200+500+800+1500/1000). If you want the DECT IP phone to play tones once, add an exclamation mark “!” before tones (e.g., !250/200,0/1000,200+300/500,200+500+800+1500/1000). **Note**: It works only if the value of the parameter “voice.tone.country” is set to Custom. If you want to disable this warning tone, set it to 0. **Web User Interface:** Settings->Tones->Dial **Handset User Interface:**		

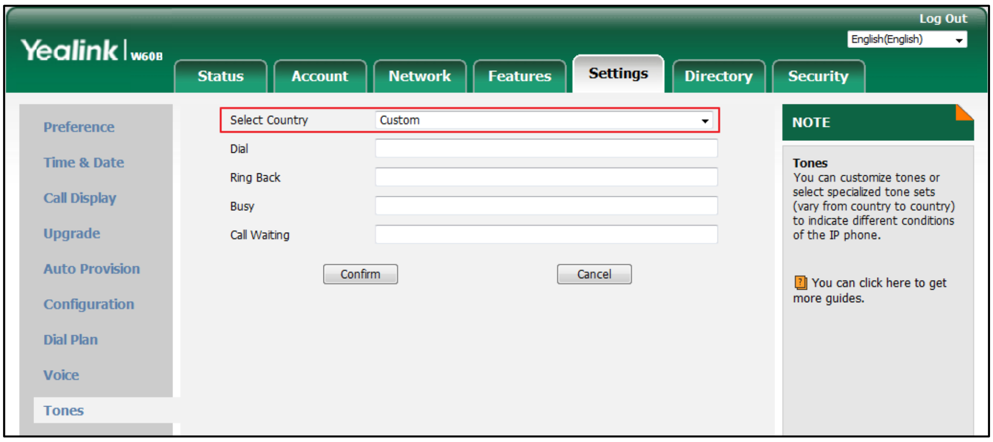
Parameters	Permitted Values	Default
None		
voice.tone.ring	**String**	**Blank**
Description: Customizes the ringback tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note**: It works only if the value of the parameter "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0. **Web User Interface:** Settings->Tones->Ring Back **Handset User Interface:** None		
voice.tone.busy	**String**	**Blank**
Description: Customizes the tone when the callee is busy. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note**: It works only if the value of the parameter "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0. **Web User Interface:** Settings->Tones->Busy **Handset User Interface:** None		
voice.tone.callwaiting	**String**	**Blank**
Description: Customizes the call waiting tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note**: It works only if the value of the parameter "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0. **Web User Interface:**		

Parameters	Permitted Values	Default
Settings->Tones->Call Waiting **Handset User Interface:** None		

To configure tones via web user interface:

1. Click on **Settings**->**Tones**.
2. Select the desired value from the pull-down list of **Select Country**.

   If you select **Custom**, you can customize a tone for each condition of the DECT IP phone.



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

Voice Mail Tone

Voice mail tone feature allows the DECT 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 DECT IP phone. For more information, refer to Tones on page 361.

Procedure

Voice mail tone can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure whether to play a warning tone when the DECT IP phone receives a new voice mail. **Parameter:** features.voice_mail_tone_enable
Web User Interface		Configure whether to play a warning tone when the DECT IP phone receives a new voice mail.

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

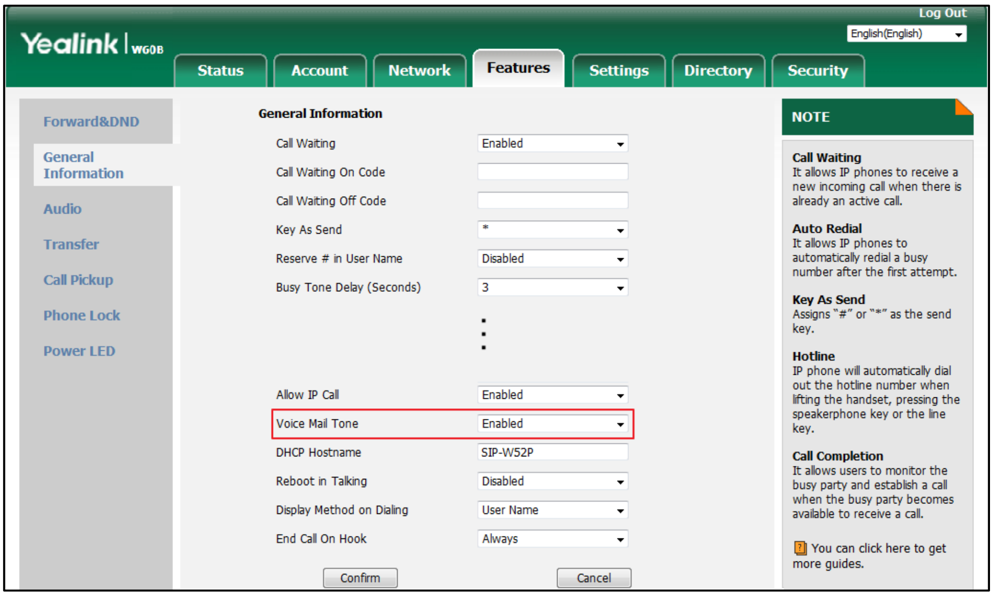
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.voice_mail_tone_enable	**0 or 1**	**1**
Description: Enables or disables the DECT IP phone to play a warning tone when it receives a new voice mail. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Voice Mail Tone **Handset User Interface:** None		

To configure voice mail tone via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **Voice Mail Tone**.



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

Ringer Device for Headset

The DECT IP phones support speaker and headset ringer devices. The feature of Ringer Device for Headset allows users to configure which ringer device to be used when receiving an incoming call. For example, if the ringer device is set to Headset, ring tone will be played through the connected headset. If the headset is not connected, ring tone will be palyed through speaker.

Procedure

Ringer device for headset can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the ringer device for the DECT IP phone. **Parameter:** features.ringer_device.is_use_headset
Web User Interface		Configure the ringer device for the DECT IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-audio&q=load

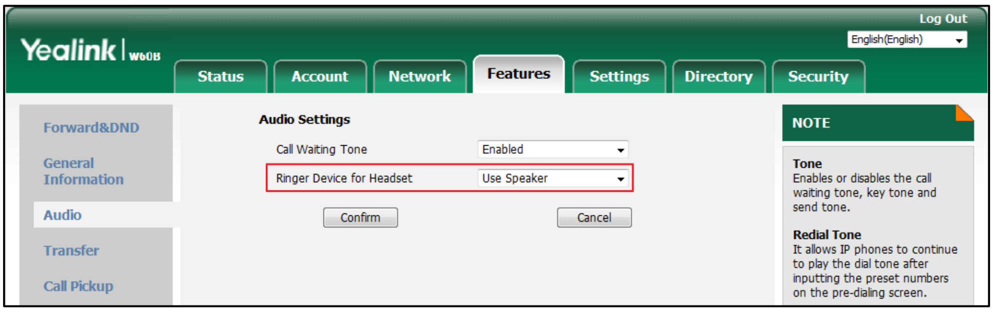
Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.ringer_device.is_use_headset	**0, 1 or 2**	**0**
Description: Configures the ringer device for the DECT IP phone. **0**-Use Speaker **1**-Use Headset **Web User Interface:** Features->Audio->Ringer Device for Headset **Handset User Interface:** None		

To configure ringer device for headset via web user interface:

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

2. Select the desired value from the pull-down list of **Ringer Device for Headset**.



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

Audio Codecs

CODEC is an abbreviation of COmpress-DECompress, capable of coding or decoding a digital data stream or signal by implementing an algorithm. The object of the algorithm is to represent the high-fidelity audio signal with minimum number of bits while retaining the quality. This can effectively reduce the frame size and the bandwidth required for audio transmission.

The audio codec that the phone uses to establish a call should be supported by the SIP server. When placing a call, the DECT IP phone will offer the enabled audio codec list to the server and then use the audio codec negotiated with the called party according to the priority.

Supported Audio Codecs

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

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

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
			20 Kbps	16 Ksps	

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

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.

Audio Codec Configuration

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the codecs to use on a per-line basis. **Parameter:** account.X.codec.<payload_type>.enable
		Configure the priority for the enabled codec. **Parameters:** account.X.codec.<payload_type>.priority
Web User Interface		Configure the codecs to use on a per-line basis. Configure the priority for the enabled codec. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-codec&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.codec.<payload_type>.enable (X ranges from 1 to 8) (where <payload_type> should be replaced by the name of audio codec)	**0 or 1**	**Refer to the following content**
Description: Enables or disables the specified audio codec for account X. **0**-Disabled **1**-Enabled **The name of audio codec**: **g722**-G722 **pcmu**-PCMU **pcma**-PCMA **g729**-G729 **g726_16**-G726-16 **g726_24**-G726-24 **g726_32**-G726-32 **g726_40**-G726-40 **ilbc**-iLBC **opus**-opus **Default:** When audio codec is G722, the default value is 1; When audio codec is PCMU, the default value is 1; When audio codec is PCMA, the default value is 1; When audio codec is G729, the default value is 1; When audio codec is G726-16, the default value is 0; When audio codec is G726-24, the default value is 0; When audio codec is G726-32, the default value is 0; When audio codec is G726-40, the default value is 0; When audio codec is iLBC, the default value is 0; When audio codec is opus, the default value is 0; **Example:** account.1.codec.g722.enable = 1 **Note**: The name of audio codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect. **Web User Interface:** Account->Codec->Audio Codec **Handset User Interface:** None		
account.X.codec.<payload_type>.priority (X ranges from 1 to 8)	**Integer from 0 to 8**	**Refer to the following content**

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>(where <payload_type> should be replaced by the name of audio codec)</td><td></td><td></td></tr>
<tr><td colspan="3">Description:
Configures the priority of the enabled audio codec for account X.
The name of audio codec:
g722-G722 pcmu-PCMU pcma-PCMA g729-G729 g726_16-G726-16 g726_24-G726-24 g726_32-G726-32 g726_40-G726-40
ilbc-iLBC opus-opus
Default:
When audio codec is G722, the default value is 1;
When audio codec is PCMU, the default value is 2;
When audio codec is PCMA, the default value is 3;
When audio codec is G729, the default value is 4;
When audio codec is G726_16, the default value is 0;
When audio codec is G726_24, the default value is 0;
When audio codec is G726_32, the default value is 0;
When audio codec is G726_40, the default value is 0;
When audio codec is iLBC, the default value is 0;
When audio codec is opus, the default value is 0;
Example:
account.1.codec.g722.priority = 1
Note: The priority of 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 audio codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect.
Web User Interface:
Account->Codec->Audio Codec
Handset User Interface:
None</td></tr>
</table>

To configure the codecs to use and adjust the priority of the enabled codecs via web user interface:

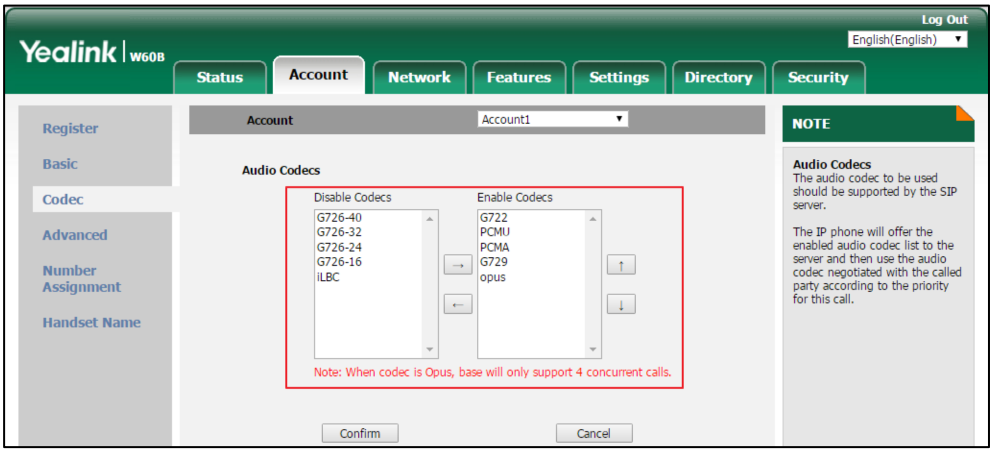
1. Click on **Account**->**Codec**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired codec from the **Disable Codecs** column and then click →.

   The selected codec appears in the **Enable Codecs** column.

4. Repeat the step 4 to add more codecs to the **Enable Codecs** column.

5. To remove the codec from the **Enable Codecs** column, select the desired codec and then click ← .

6. To adjust the priority of codecs, select the desired codec and then click ↑ or ↓ .



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

Packetization Time (PTime)

Ptime is a measurement of the duration (in milliseconds) of the audio data in each RTP packet sent to the destination, and defines how much network bandwidth is used for the RTP stream transfer. Before establishing a conversation, codec and ptime are negotiated through SIP signaling. The valid values of ptime range from 10 to 60, in increments of 10 milliseconds. The default ptime is 20ms. You can also disable the ptime negotiation.

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

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

Codec	Packetization Time (Minimun)	Packetization Time (Maximun)
opus	10ms	20ms

Procedure

PTime can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the ptime. **Parameter:** account.X.ptime
Web User Interface		Configure the ptime. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

Details of Configuration Parameter:

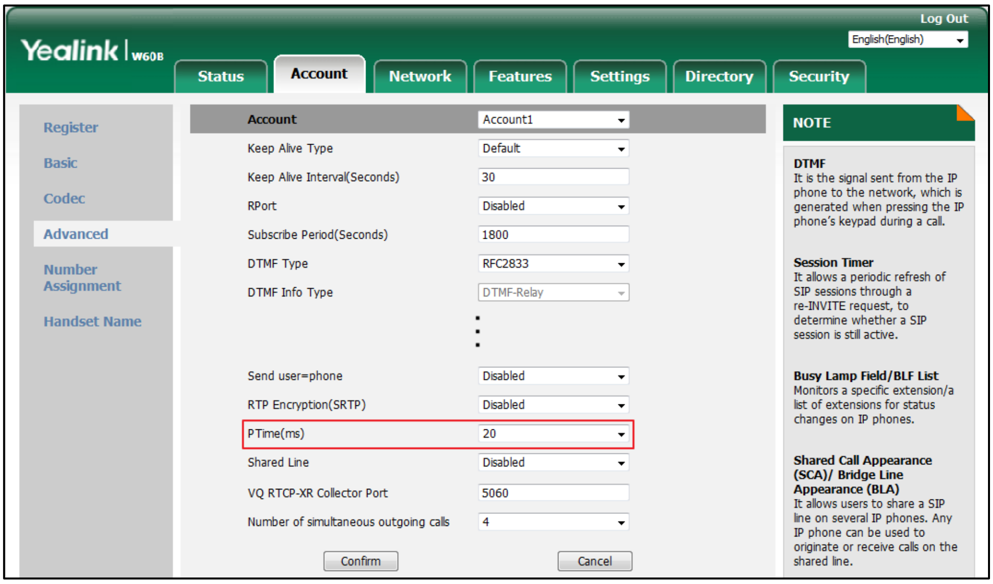
Parameter	Permitted Values	Default
account.X.ptime (X ranges from 1 to 8)	**0, 10, 20, 30, 40, 50 or 60**	**20**
Description: Configures the ptime (in milliseconds) for the codec for account X. **0**-Disabled **10**-10 **20**-20 **30**-30 **40**-40 **50**-50 **60**-60 **Example:** account.1.ptime = 20 **Web User Interface:** Account->Advanced->PTime(ms) **Handset User Interface:** None		

To configure the ptime for the account via web user interface:

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

2. Select the desired account from the pull-down list of **Account**.

3. Select the desired value from the pull-down list of **PTime(ms)**.



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

Acoustic Clarity Technology

Background Noise Suppression (BNS)

Background noise suppression (BNS) is designed primarily for hands-free operation and reduces background noise to enhance communication in noisy environments.

Automatic Gain Control (AGC)

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

Voice Activity Detection (VAD)

Voice Activity Detection (VAD) is used in speech processing to detect the presence or absence of human speech. When detecting period of "silence", VAD replaces that silence efficiently with special packets that indicate silence is occurring. It can facilitate speech processing, and deactivate some processes during non-speech section of an audio session. VAD can avoid unnecessary coding or transmission of silence packets in VoIP applications, saving on computation and network bandwidth.

Procedure

VAD can be configured using the following methods.

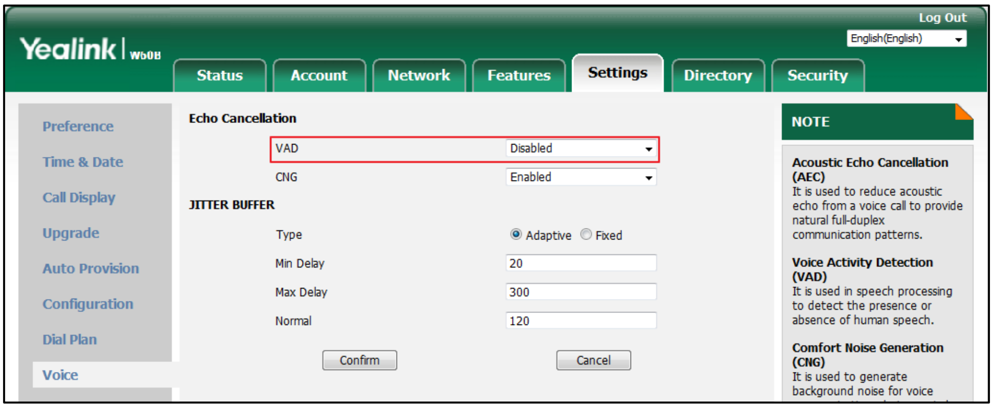
Central Provisioning (Configuration File)	y000000000077.cfg	Configure VAD. **Parameter:** voice.vad
Web User Interface		Configure VAD. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.vad	**0 or 1**	**0**
Description: Enables or disables the VAD (Voice Activity Detection) feature on the DECT IP phone. **0**-Disabled **1**-Enabled **Web User Interface**: Settings->Voice->Echo Cancellation->VAD **Handset User Interface:** None		

To configure VAD via web user interface:

1. Click on **Settings**->**Voice**.
2. Select the desired value from the pull-down list of **VAD**.



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

Comfort Noise Generation (CNG)

Comfort Noise Generation (CNG) is used to generate background noise for voice communications during periods of silence in a conversation. It is a part of the silence suppression or VAD handling for VoIP technology. CNG, in conjunction with VAD algorithms, quickly responds when periods of silence occur and inserts artificial noise until voice activity resumes. The insertion of artificial noise gives the illusion of a constant transmission stream, so that background sound is consistent throughout the call and the listener does not think the line has released. The purpose of VAD and CNG is to maintain an acceptable perceived QoS while simultaneously keeping transmission costs and bandwidth usage as low as possible.

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

For example, A is talking with B.

A: VAD=1, CNG=1

B: VAD=0, CNG=1

If A mutes the call, since VAD=1, A will send CN packets to B. When receiving CN packets, B will generate comfortable noise.

If B mutes the call, since VAD=0, B will not send CN packets to A. So even if CNG=1 (B), A will not hear comfortable noise.

Procedure

CNG can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure CNG. **Parameter:** voice.cng
Web User Interface		Configure CNG. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

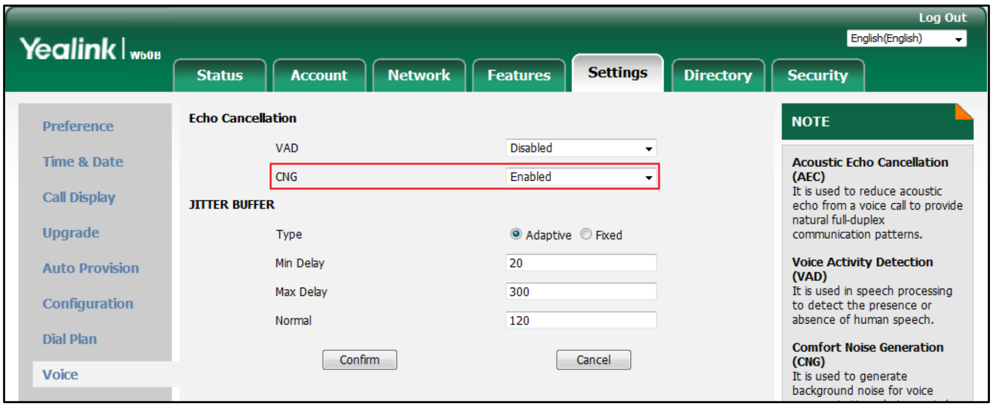
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.cng	**0 or 1**	**1**
Description: Enables or disables the CNG (Comfortable Noise Generation) feature on the DECT IP		

Parameter	Permitted Values	Default
phone. **0**-Disabled **1**-Enabled **Web User Interface**: Settings->Voice->Echo Cancellation->CNG **Handset User Interface:** None		

To configure CNG via web user interface:

1. Click on **Settings**->**Voice**.
2. Select the desired value from the pull-down list of **CNG**.



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

Jitter Buffer

Jitter buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in even intervals. Jitter is a term indicating variations in packet arrival time, which can occur because of network congestion, timing drift or route changes. The jitter buffer, located at the receiving end of the voice connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very little sound distortion. DECT IP phones support two types of jitter buffers: fixed and adaptive. A fixed jitter buffer adds the fixed delay to voice packets. You can configure the delay time for the static jitter buffer on DECT IP phones. An adaptive jitter buffer is capable of adapting the changes in the network's delay. The range of the delay time for the dynamic jitter buffer added to packets can be also configured on DECT IP phones.

Procedure

Jitter buffer can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the mode of jitter buffer and the delay time for jitter buffer in the network. **Parameters:** voice.jib.adaptive voice.jib.min voice.jib.max voice.jib.normal
Web User Interface		Configure the mode of jitter buffer and the delay time for jitter buffer in the network. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
voice.jib.adaptive	**0 or 1**	**1**
Description: Configures the type of jitter buffer in the network. **0**-Fixed **1**-Adaptive **Web User Interface:** Settings->Voice->JITTER BUFFER->Type **Handset User Interface:** None		
voice.jib.min	**Integer from 0 to 400**	**60**
Description: Configures the minimum delay time (in milliseconds) of jitter buffer in the network. **Note**: It works only if the value of the parameter "voice.jib.adaptive" is set to 1 (Adaptive). **Web User Interface:** Settings->Voice->JITTER BUFFER->Min Delay		

Parameters	Permitted Values	Default
Handset User Interface: None		
voice.jib.max	**Integer from 0 to 400**	**240**
Description: Configures the maximum delay time (in milliseconds) of jitter buffer in the network. **Note**: It works only if the value of the parameter "voice.jib.adaptive" is set to 1 (Adaptive). **Web User Interface:** Settings->Voice->JITTER BUFFER->Max Delay **Handset User Interface:** None		
voice.jib.normal	**Integer from 0 to 400**	**120**
Description: Configures the normal delay time (in milliseconds) of jitter buffer in the network. **Note**: It works only if the value of the parameter "voice.jib.adaptive" is set to 0 (Fixed). **Web User Interface:** Settings->Voice->JITTER BUFFER->Normal **Handset User Interface:** None		

To configure Jitter Buffer in the network via web user interface:

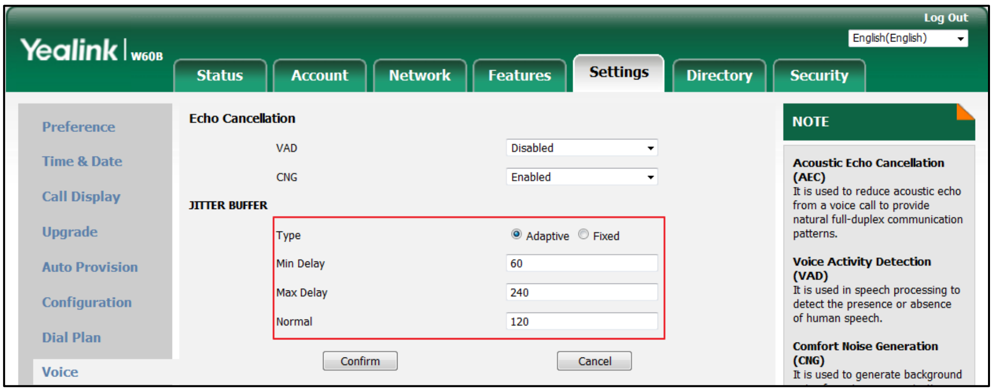
1. Click on **Settings**->**Voice**.
2. Mark the desired radio box in the **Type** field.
3. Enter the minimum delay time for adaptive jitter buffer in the **Min Delay** field.

   The valid value ranges from 20 to 300.
4. Enter the maximum delay time for adaptive jitter buffer in the **Max Delay** field.

   The valid value ranges from 20 to 300.

5. Enter the fixed delay time for fixed jitter buffer in the **Normal** field.

   The valid value ranges from 20 to 300.



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

DTMF

DTMF (Dual Tone Multi-frequency), better known as touch-tone, is used for telecommunication signaling over analog telephone lines in the voice-frequency band. DTMF is the signal sent from the DECT IP phone to the network, which is generated when pressing the DECT IP phone's keypad during a call. Each key pressed on the DECT IP phone generates one sinusoidal tone of two frequencies. One is generated from a high frequency group and the other from a low frequency group.

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

DTMF Keypad Frequencies:

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

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

Methods of Transmitting DTMF Digit

Three methods of transmitting DTMF digits on SIP calls:

- **RFC 2833** -- DTMF digits are transmitted by RTP Events compliant to RFC 2833.
- **INBAND** -- DTMF digits are transmitted in the voice band.
- **SIP INFO** -- DTMF digits are transmitted by SIP INFO messages.

The method of transmitting DTMF digits is configurable on a per-line basis.

RFC 2833

DTMF digits are transmitted using the RTP Event packets that are sent along with the voice path. These packets use RFC 2833 format and must have a payload type that matches what the other end is listening for. The default payload type for RTP Event packets is 101 and the payload type is configurable. The DECT IP phones use the configured value to negotiate with the other end during call establishment.

The RTP Event packet contains 4 bytes. The 4 bytes are distributed over several fields denoted as Event, End bit, R-bit, Volume and Duration. If the End bit is set to 1, the packet contains the end of the DTMF event. You can configure the sending times of the end RTP Event packet.

INBAND

DTMF digits are transmitted within the audio of the DECT IP phone conversation. It uses the same codec as your voice and is audible to conversation partners.

SIP INFO

DTMF digits are transmitted by the SIP INFO messages when the voice stream is established after a successful SIP 200 OK-ACK message sequence. The SIP INFO message is sent along the signaling path of the call. The SIP INFO message can transmit DTMF digits in three ways: DTMF, DTMF-Relay and Telephone-Event.

Procedure

Configuration changes can be performed using the following methods.

<table>
<tr><td rowspan="2">Central Provisioning
(Configuration File)</td><td><MAC>.cfg</td><td>Configure the method of transmitting DTMF digit and the payload type.
Parameters:
account.X.dtmf.type
account.X.dtmf.dtmf_payload
account.X.dtmf.info_type</td></tr>
<tr><td>y000000000077.cfg</td><td>Specify how long the phone should play each DTMF tone for.</td></tr>
</table>

		Parameter: features.dtmf.duration
		Configure the frequency level of DTMF digits. **Parameter**: features.dtmf.volume
Web User Interface		Configure the method of transmitting DTMF digits and the payload type. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0
		Configure the number of times for the DECT IP phone to send the end RTP Event packet. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.dtmf.type (X ranges from 1 to 8)	**0, 1, 2 or 3**	**1**
Description: Configures the DTMF type for account X. **0**-INBAND **1**-RFC 2833 **2**-SIP INFO **3**-RFC2833 + SIP INFO If it is set to 0 (INBAND), DTMF digits are transmitted in the voice band. If it is set to 1 (RFC 2833), DTMF digits are transmitted by RTP Events compliant to RFC 2833. If it is set to 2 (SIP INFO), DTMF digits are transmitted by the SIP INFO messages. If it is set to 3 (RFC2833 + SIP INFO), DTMF digits are transmitted by RTP Events compliant to RFC 2833 and the SIP INFO messages. **Web User Interface:** Account->Advanced->DTMF Type **Handset User Interface:**		

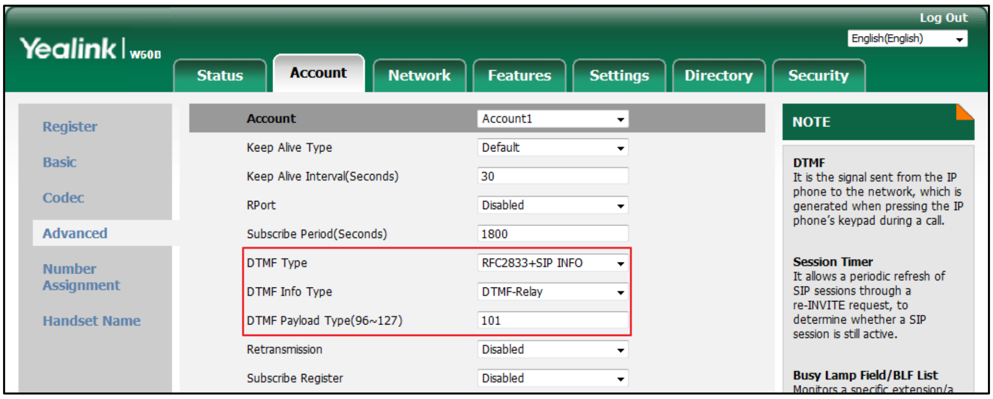
Parameters	Permitted Values	Default
None		
account.X.dtmf.dtmf_payload (X ranges from 1 to 8)	**Integer from 96 to 127**	**101**
Description: Configures the value of DTMF payload for account X. **Note:** It works only if the value of parameter “account.X.dtmf.type” is set to 1 (RFC2833) or 3 (RFC2833 + SIP INFO). **Web User Interface:** Account->Advanced->DTMF Payload Type(96~127) **Handset User Interface:** None		
account.X.dtmf.info_type (X ranges from 1 to 8)	**1, 2 or 3**	**1**
Description: Configures the DTMF info type. **1**-DTMF-Relay **2**-DTMF **3**-Telephone-Event **Note:** It works only if the value of parameter “account.X.dtmf.type” is set to 2 (SIP INFO) or 3 (RFC2833 + SIP INFO). **Web User Interface:** Account->Advanced->DTMF Info Type **Handset User Interface:** None		
features.dtmf.duration	**Integer from 0 to 300**	**100**
Description: 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. If you change this parameter, the DECT IP phone will reboot to make the change take effect.		

Parameters	Permitted Values	Default
Web User Interface: None **Handset User Interface:** None		
features.dtmf.volume	**Integer from -33 to 0**	**-10**
Description: Configures the frequency level of DTMF digits (in db). **Web User Interface:** None **Handset User Interface:** None		

To configure the method of transmitting DTMF digits via web user interface:

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

   If **SIP INFO** or **RFC2833 + SIP INFO** is selected, select the desired value from the pull-down list of **DTMF Info Type**.
4. Enter the desired value in the **DTMF Payload Type(96~127)** field.



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

Suppress DTMF Display

Suppress DTMF display allows DECT IP phones to suppress the display of DTMF digits during an active call. DTMF digits are displayed as "*" on the LCD screen. Suppress DTMF display delay defines whether to display the DTMF digits for a short period of time before displaying as "*".

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure suppress DTMF display and suppress DTMF display delay. **Parameters:** features.dtmf.hide features.dtmf.hide_delay
Web User Interface		Configure suppress DTMF display and suppress DTMF display delay. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

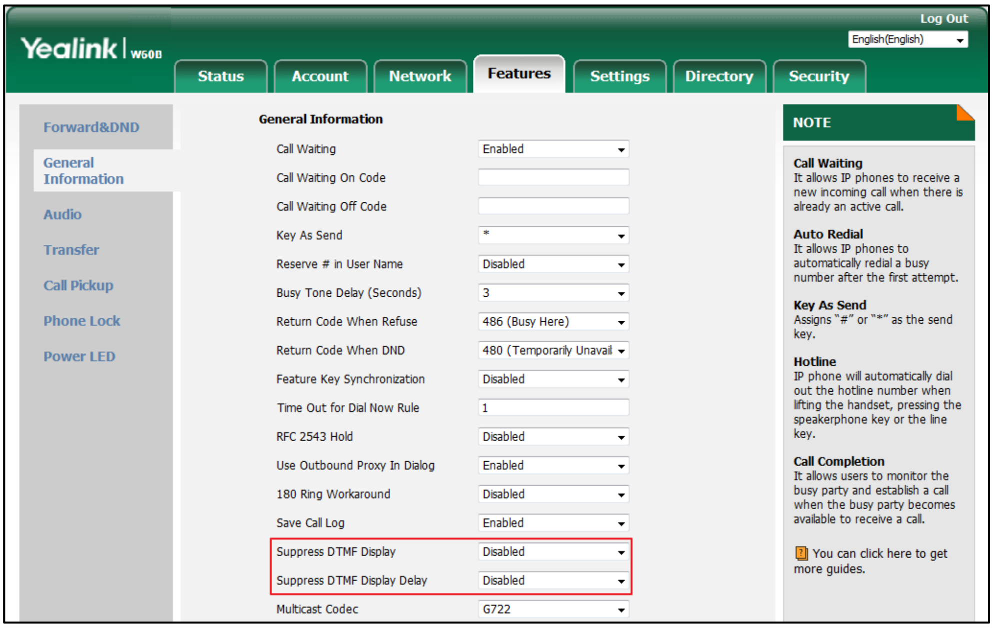
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.dtmf.hide	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to suppress the display of DTMF digits during an active call. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the DTMF digits are displayed as asterisks. **Web User Interface:** Features->General Information->Suppress DTMF Display **Handset User Interface:** None		
features.dtmf.hide_delay	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to display the DTMF digits for a short period before displaying asterisks during an active call. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "features.dtmf.hide" is set to 1 (Enabled). **Web User Interface:**		

Parameters	Permitted Values	Default
Features->General Information->Suppress DTMF Display Delay **Handset User Interface:** None		

To configure suppress DTMF display and suppress DTMF display delay via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Suppress DTMF Display**.
3. Select the desired value from the pull-down list of **Suppress DTMF Display Delay**.



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

Voice Quality Monitoring (VQM)

Voice quality monitoring feature allows the DECT IP phones to generate various quality metrics for listening quality and conversational quality. These metrics can be sent between the phones in RTCP-XR packets. These metrics can also be sent in SIP PUBLISH messages to a central voice quality report collector. Two mechanisms for voice quality monitoring are supported by Yealink DECT IP phones:

- RTCP-XR
- VQ-RTCPXR

RTCP-XR

The RTCP-XR mechanism, complaint with RFC 3611-RTP Control Extended Reports (RTCP XR), provides the metrics contained in RTCP-XR packets for monitoring the quality of calls. These metrics include network packet loss, delay metrics, analog metrics and voice quality metrics.

Procedure

RTCP-XR can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure RTCP-XR. **Parameter:** voice.rtcp_xr.enable
Web User Interface		Configure RTCP-XR. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-voicemonitoring&q=load

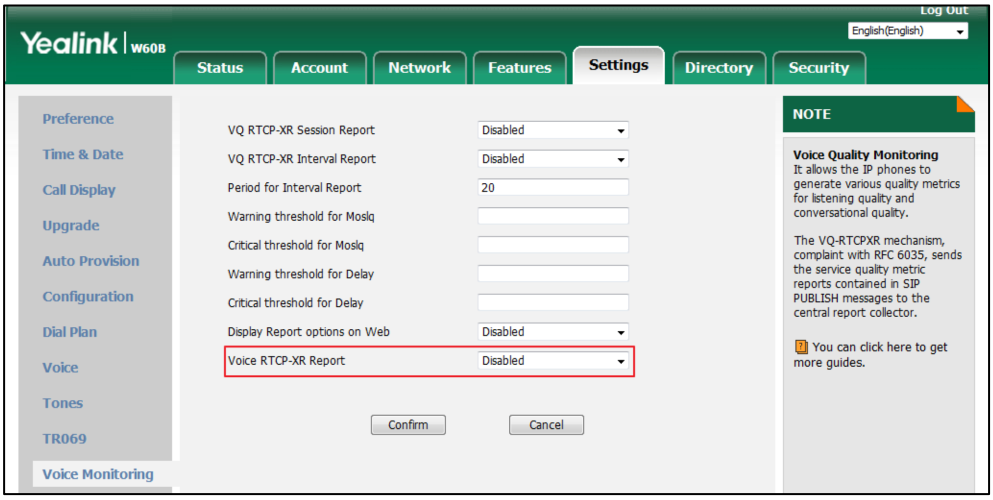
Details of Configuration Parameters:

Parameters	Permitted Values	Default
voice.rtcp_xr.enable	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to send RTCP-XR packets. **0**-Disabled **1**-Enabled **Note:** If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Voice Monitoring->Voice RTCP-XR Report **Handset User Interface:** None		

To configure RTCP-XR feature via web user interface:

1. Click on **Settings**->**Voice Monitoring**.

2. Select the desired value from the pull-down list of **Voice RTCP-XR Report**.



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

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

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

VQ-RTCPXR

The VQ-RTCPXR mechanism, complaint with RFC 6035, sends the service quality metric reports contained in SIP PUBLISH messages to the central report collector. Three types of quality reports can be enabled:

- **Session**: Generated at the end of a call.
- **Interval**: Generated during a call at a configurable period.
- **Alert**: Generated when the call quality degrades below a configurable threshold.

A wide range of performance metrics are generated in the following three ways:

- Based on current values, such as jitter, jitter buffer max and round trip delay.
- Covers the time period from the beginning of the call until the report is sent, such as network packet loss.
- Computed using other metrics as input, such as listening Mean Opinion Score (MOS-LQ) and conversational Mean Opinion Score (MOS-CQ).

To operate with central report collector, DECT IP phones must be configured to forward their voice quality reports to the specified report collector. You can specify the report collector on a per-line basis.

Users can check the voice quality data of the last call via web user interface or handset user interface. Users can also specify the options of the RTP status to be displayed on the handset user interface. Options of the RTP status to be displayed on the web user interface cannot be specified.

Procedure

VQ-RTCPXR can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the generation of session packets. **Parameter:** phone_setting.vq_rtcpxr.session_report.enable
		Configure the generation of interval packets. **Parameters:** phone_setting.vq_rtcpxr.interval_report.enable phone_setting.vq_rtcpxr_interval_period
		Configure the generation of alert packets. **Parameters:** phone_setting.vq_rtcpxr_moslq_threshold_warning phone_setting.vq_rtcpxr_moslq_threshold_critical phone_setting.vq_rtcpxr_delay_threshold_warning phone_setting.vq_rtcpxr_delay_threshold_critical
		Configure the phone to display RTP status showing the voice quality report of the last call on the web user interface. **Parameter:** phone_setting.vq_rtcpxr.states_show_on_web.enable
	<MAC>.cfg	Configure the central report collector. **Parameters:** account.X.vq_rtcpxr.collector_name account.X.vq_rtcpxr.collector_server_host account.X.vq_rtcpxr.collector_server_port
Web User Interface		Configure VQ-RTCPXR. Configure the phone to display RTP status showing the voice quality report of the last call on the web user interface. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-voicemonitoring&q=load
		Configure the central report collector. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.vq_rtcpxr.session_report.enable	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to send a session quality report to the central report collector at the end of each call. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Voice Monitoring->VQ RTCP-XR Session Report **Handset User Interface:** None		
phone_setting.vq_rtcpxr.interval_report.enable	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to send an interval quality report to the central report collector periodically throughout a call. **0**-Disabled **1**-Enabled **Note**: To avoid overload, the interval quality reports only generate when the call is abnormal. **Web User Interface:** Settings->Voice Monitoring->VQ RTCP-XR Interval Report **Handset User Interface:** None		
phone_setting.vq_rtcpxr_interval_period	**Integer from 5 to 20**	**20**
Description: Configures the interval (in seconds) for the DECT IP phone to send an interval quality report to the central report collector periodically throughout a call. **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.interval_report.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Period for Interval Report		

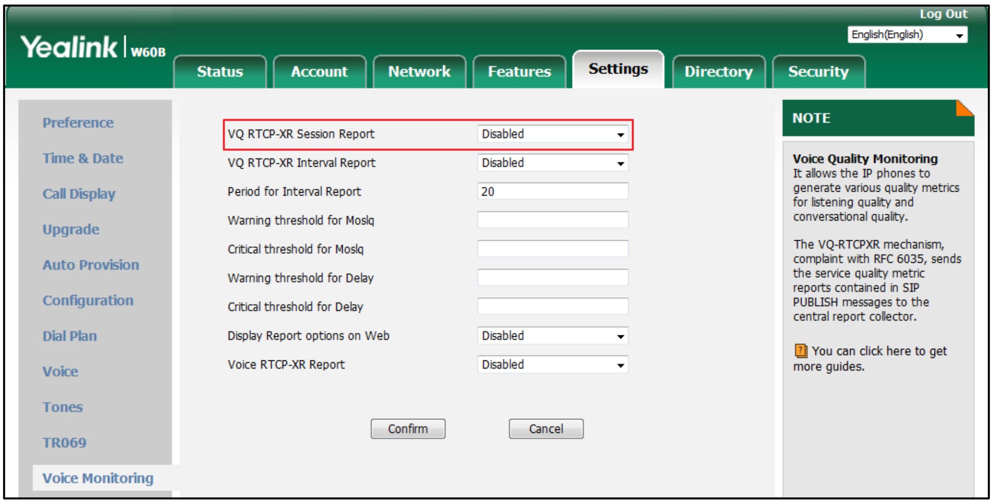
Parameters	Permitted Values	Default
Handset User Interface: None		
phone_setting.vq_rtcpxr_moslq_threshold_warning	**15 to 40**	**Blank**
Description: Configures the threshold value of listening MOS score (MOS-LQ) multiplied by 10. The threshold value of MOS-LQ causes the phone to send a warning alert quality report to the central report collector. For example, a configured value of 35 corresponds to the MOS score 3.5. When the MOS-LQ value computed by the phone is less than or equal to 3.5, the phone will send a warning alert quality report to the central report collector. When the MOS-LQ value computed by the phone is greater than 3.5, the phone will not send a warning alert quality report to the central report collector. If it is set to blank, warning alerts are not generated due to MOS-LQ. **Web User Interface:** Settings->Voice Monitoring->Warning threshold for Moslq **Handset User Interface:** None		
phone_setting.vq_rtcpxr_moslq_threshold_critical	**15 to 40**	**Blank**
Description: Configures the threshold value of listening MOS score (MOS-LQ) multiplied by 10. The threshold value of MOS-LQ causes the phone to send a critical alert quality report to the central report collector. For example, a configured value of 28 corresponds to the MOS score 2.8. When the MOS-LQ value computed by the phone is less than or equal to 2.8, the phone will send a critical alert quality report to the central report collector. When the MOS-LQ value computed by the phone is greater than 2.8, the phone will not send a critical alert quality report to the central report collector. If it is set to blank, critical alerts are not generated due to MOS-LQ. **Web User Interface:** Settings->Voice Monitoring->Critical threshold for Moslq **Handset User Interface:** None		
phone_setting.vq_rtcpxr_delay_threshold_warning	**10 to 2000**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the threshold value of one way delay (in milliseconds) that causes the phone to send a warning alert quality report to the central report collector. For example, If it is set to 500, when the value of one way delay computed by the phone is greater than or equal to 500, the phone will send a warning alert quality report to the central report collector; when the value of one way delay computed by the phone is less than 500, the phone will not send a warning alert quality report to the central report collector. If it is set to blank, warning alerts are not generated due to one way delay. One-way delay includes both network delay and end system delay. **Web User Interface:** Settings->Voice Monitoring->Warning threshold for Delay **Handset User Interface:** None		
phone_setting.vq_rtcpxr_delay_threshold_critical	**10 to 2000**	**Blank**
Description: Configures the threshold value of one way delay (in milliseconds) that causes phone to send a critical alert quality report to the central report collector. For example, If it is set to 500, when the value of one way delay computed by the phone is greater than or equal to 500, the phone will send a critical alert quality report to the central report collector; when the value of one way delay computed by the phone is less than 500, the phone will not send a critical alert quality report to the central report collector. If it is set to blank, critical alerts are not generated due to one way delay. One-way delay includes both network delay and end system delay. **Web User Interface:** Settings->Voice Monitoring->Critical threshold for Delay **Handset User Interface:** None		
phone_setting.vq_rtcpxr.states_show_on_web.enable	**0 or 1**	**0**
Description: Enables or disables the voice quality data of the last call to be displayed on web interface at path **Status**->**RTP Status**. **0**-Disabled **1**-Enabled		

Parameters	Permitted Values	Default
Web User Interface: Settings->Voice Monitoring->Display Report options on Web **Handset User Interface:** None		
account.X.vq_rtcpxr.collector_name (X ranges from 1 to 8)	**String within 32 characters**	**Blank**
Description: Configures the host name of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X. **Web User Interface:** Account->Advanced->VQ RTCP-XR Collector Name **Handset User Interface:** None		
account.X.vq_rtcpxr.collector_server_host (X ranges from 1 to 8)	**IPv4 Address**	**Blank**
Description: Configures the IP address of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X. **Web User Interface:** Account->Advanced->VQ RTCP-XR Collector Address **Handset User Interface:** None		
account.X.vq_rtcpxr.collector_server_port	**Integer from 1 to 65535**	**5060**
Description: Configures the port of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X. **Web User Interface:** Account->Advanced->VQ RTCP-XR Collector Port **Handset User Interface:** None		

To configure session report for VQ-RTCPXR via web user interface:

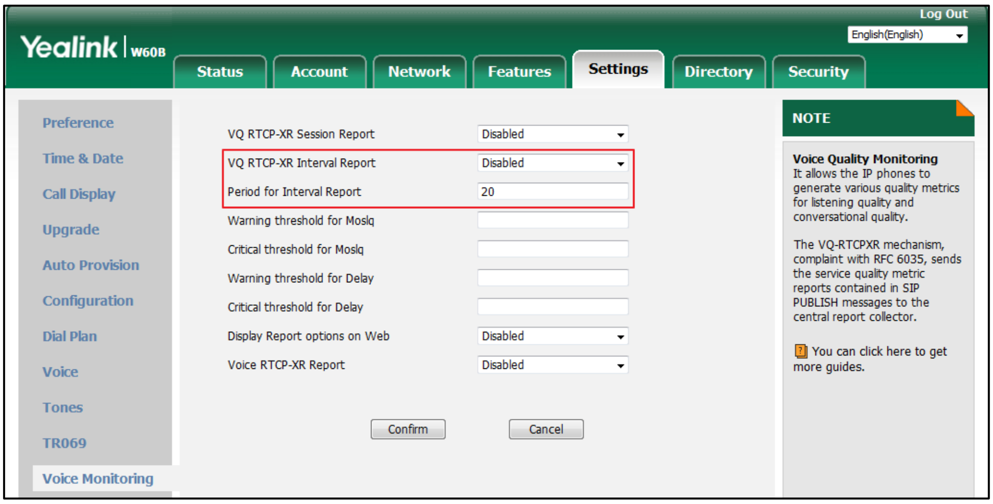
1. Click on **Settings**->**Voice Monitoring**.
2. Select the desired value from the pull-down list of **VQ RTCP-XR Session Report**.



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

To configure interval report for VQ-RTCPXR via web user interface:

1. Click on **Settings**->**Voice Monitoring**.
2. Select the desired value from the pull-down list of **VQ RTCP-XR Interval Report**.
3. Enter the desired value in the **Period for Interval Report** field.

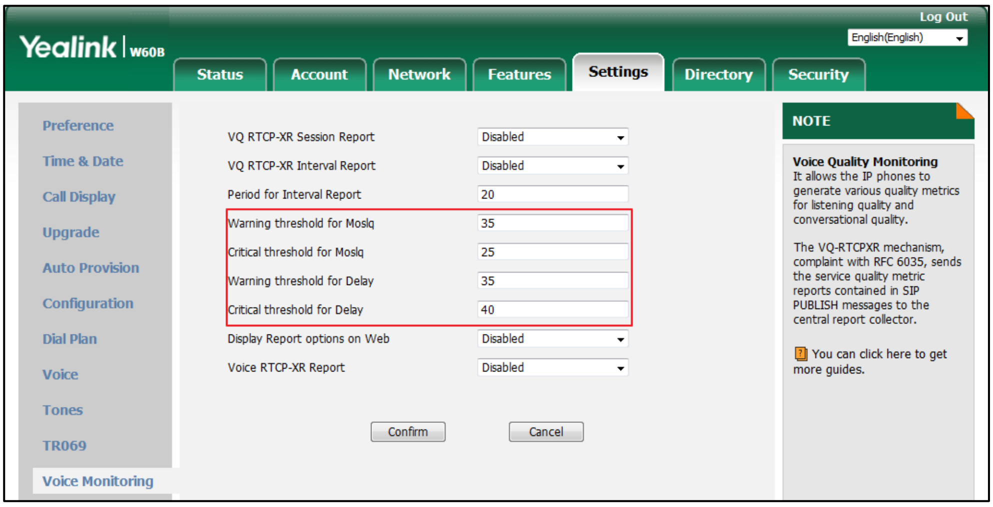


4. Click **Confirm** to accept the change.

To configure alert report for VQ-RTCPXR via web user interface:

1. Click on **Settings**->**Voice Monitoring**.
2. Enter the desired value in the **Warning threshold for Moslq** field.
3. Enter the desired value in the **Critical threshold for Moslq** field.
4. Enter the desired value in the **Warning threshold for Delay** field.

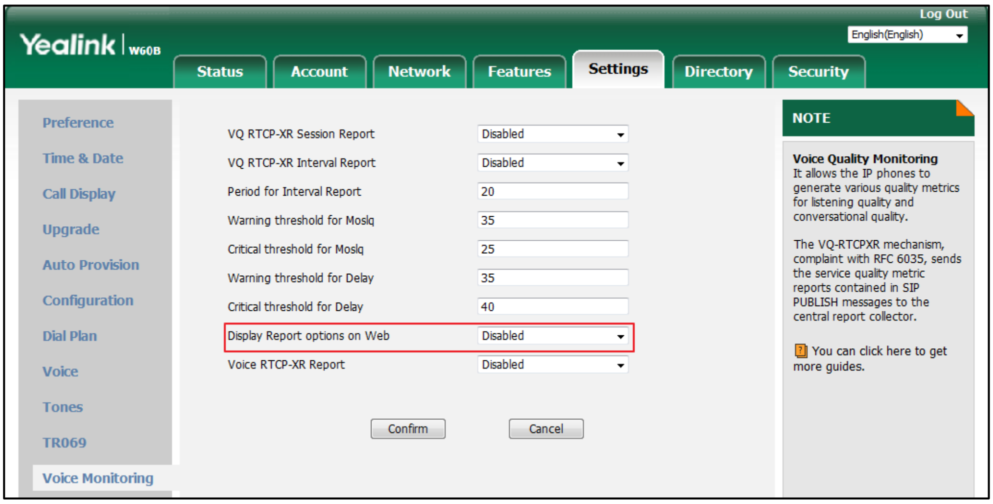
5. Enter the desired value in the **Critical threshold for Delay** field.



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

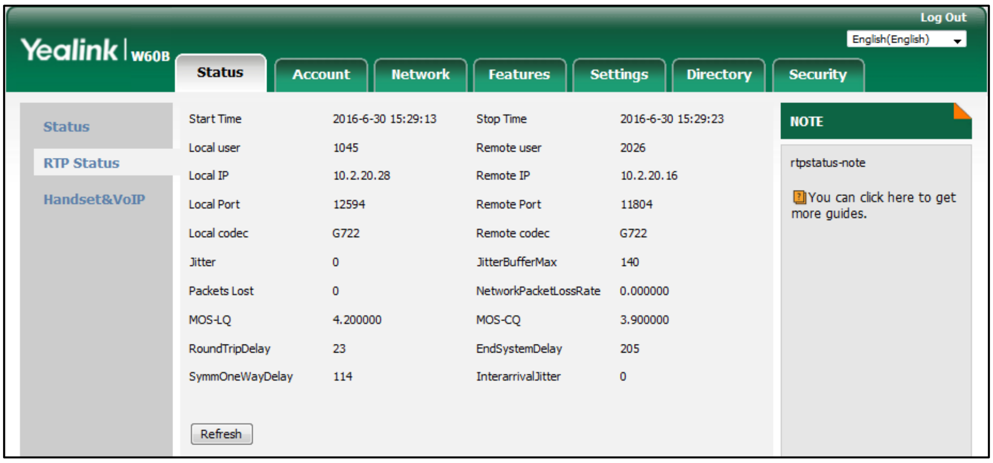
To configure RTP status displayed on the web page via web user interface:

1. Click on **Settings**->**Voice Monitoring**.
2. Select the desired value from the pull-down list of **Display Report options on Web**.



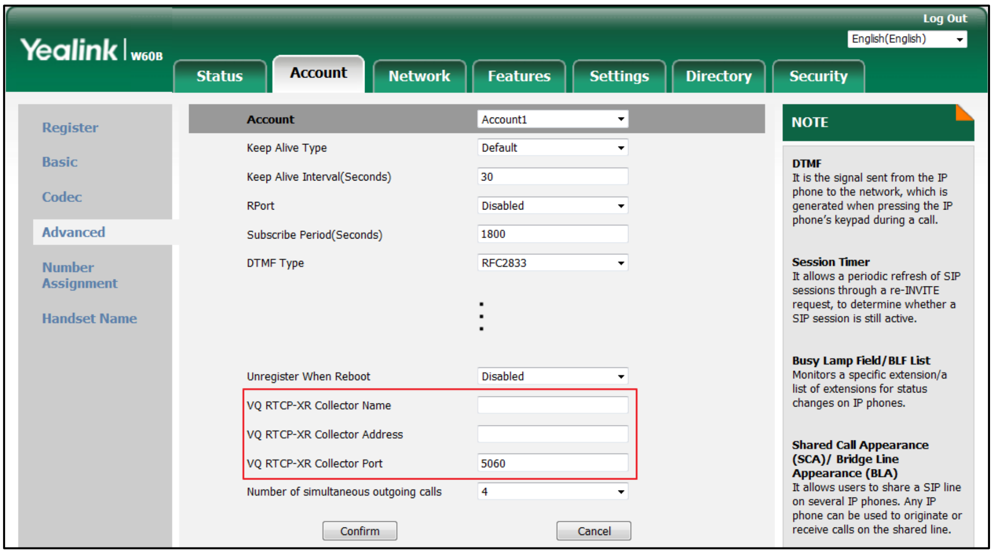
3. Click **Confirm** to accept the change.

The RTP status will appear on the web user interface at the path: **Status**->**RTP Status**.



To configure the central report collector via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Enter the host name of the central report collector in the **VQ RTCP-XR Collector Name** field.
4. Enter the IP address of the central report collector in the **VQ RTCP-XR Collector Address** field.
5. Enter the port of the central report collector in the **VQ RTCP-XR Collector Port** field.



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

Configuring Security Features

This chapter provides information for making configuration changes for the following security-related features:

- User and Administrator Passwords
- Auto Logout Time
- Base
- Transport Layer Security (TLS)
- Secure Real-Time Transport Protocol (SRTP)
- Encrypting and Decrypting Files

User and Administrator Passwords

Some menu options are protected by two privilege levels, user and administrator, each with its own password. When logging into the web user interface, you need to enter the user name and password to access various menu options. The default user password is “user” and the default administrator password is “admin”.

For security reasons, the user or administrator should change the default user or administrator password as soon as possible. A user or an administrator can change the user password. The administrator password can only be changed by an administrator.

Procedure

User or administrator password can be changed using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Change the user or administrator password of the DECT IP phone. **Parameter:** static.security.user_password
Web User Interface		Change the user or administrator password of the DECT IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=security&q=load

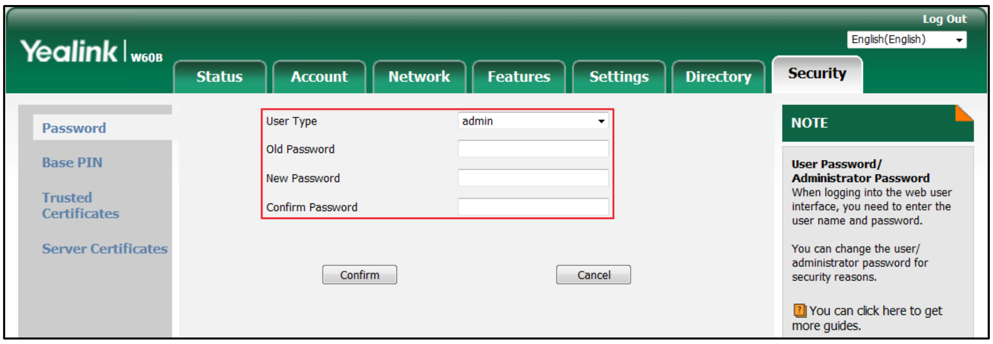
Details of the Configuration Parameter:

<table>
<tr><th>Parameter</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>static.security.user_password</td><td>String within 32 characters</td><td>user</td></tr>
<tr><td colspan="3">Description:
Configures the password of the user or administrator for phone's web user interface access.
The DECT IP phone uses "user" as the default user password and "admin" as the default administrator password.
The valid value format is username: new password.
Example:
static.security.user_password = user:123 means setting the password of user (current user name is "user") to password 123.
static.security.user_password = admin:456 means setting the password of administrator (current user name is "admin") to password 456.
Note: DECT IP phones support ASCII characters 32-126(0x20-0x7E) in passwords.
Web User Interface:
Security->Password
Handset User Interface:
None</td></tr>
</table>

To change the user or administrator password via web user interface:

1. Click on **Security**->**Password**.
2. Select the desired value (**user** or **admin**) from the pull-down list of **User Type**.
3. Enter new password in the **New Password** and **Confirm Password** fields.

   Valid characters are ASCII characters 32-126(0x20-0x7E) except 58(3A).



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

Note If logging into the web user interface of the phone with the user credential, you need to enter the old user password in the **Old Password** field.

Auto Logout Time

Auto logout time defines a specific period of time during which the DECT IP phones will automatically log out if you have not performed any actions via web user interface. Once logging out, you must re-enter username and password for web access authentication.

Procedure

Auto logout time can be configured using the following methods.

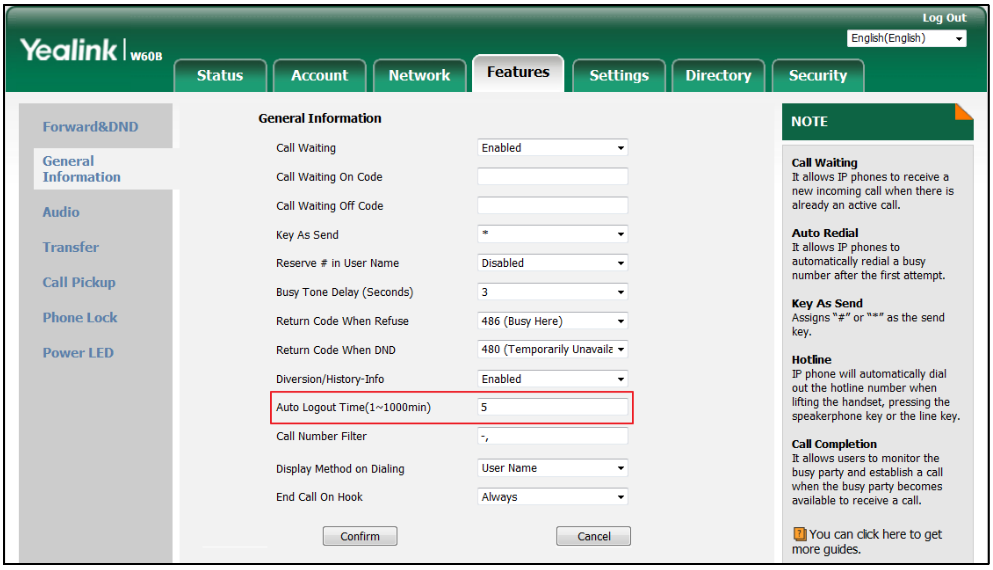
Central Provisioning (Configuration File)	y000000000077.cfg	Configure auto logout time. **Parameter**: features.relog_offtime
Web User Interface		Configure auto logout time. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.relog_offtime	**Integer from 1 to 1000**	**5**
Description: Configures the timeout interval (in minutes) for web access authentication. **Example**: features.relog_offtime = 5 If you log into the web user interface and leave it for 5 minutes, it will automatically log out. **Web User Interface:** Features->General Information->Auto Logout Time(1~1000min) **Handset User Interface:** None		

To configure the auto logout time via web user interface:

1. Click on **Features**->**General Information**.
2. Enter the desired auto logout time in **Auto Logout Time(1~1000min)** field.



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

Base PIN

Base PIN is used to lock the DECT IP phone to prevent it from unauthorized use. For menu options, a user must enter the base PIN to unlock it.

Procedure

Base PIN can be configured using the following methods.

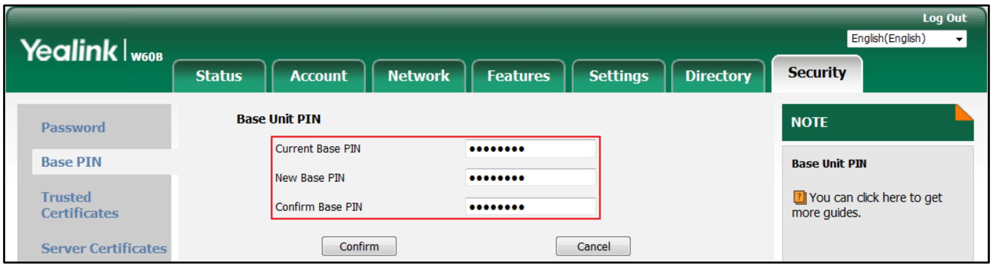
Configuration File	y000000000077.cfg	Change the base PIN. **Parameter:** base.pin_code
Web User Interface		Change the base PIN. **Navigate to**: http://<phoneIPAddress>/servlet?p=security-base-pin&q=load
Handset User Interface		Change the base PIN.

Details of Configuration Parameter:

Parameter	Permitted Values	Default
base.pin_code	**Integer from 0000 to 9999**	**0000**
Description: Configures the system PIN of the base station. **Web User Interface:** Security->Base PIN->Base Unit PIN **Handset User Interface:** OK->Settings->System Settings->Change Base PIN		

To configure base PIN via web user interface:

1. Click on **Security**->**Base PIN**.
2. Enter the current base PIN in the **Current Base PIN** field.
3. Enter new base PIN in the **New Base PIN** and **Confirm Base PIN** fields.



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

To configure base PIN via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**System Settings**->**Change Base PIN**.
3. Enter the system PIN (default: 0000), and then press the **Done** soft key.
4. Enter the new PIN in the **Enter New PIN** and **Re-enter New PIN** field respectively.
5. Press the **Save** soft key to accept the change.

Emergency Number

Public telephone networks in countries around the world have a single emergency telephone number (emergency services number), that allows a caller to contact local emergency services for assistance when necessary.

You can specify the emergency numbers for contacting the emergency services in an emergency situation. The emergency telephone number may differ from country to country. It is typically a three-digit number so that it can be easily remembered and dialed quickly. You can dial these numbers when the phone is locked.

Procedure

Emergency number can be configured using the following methods.

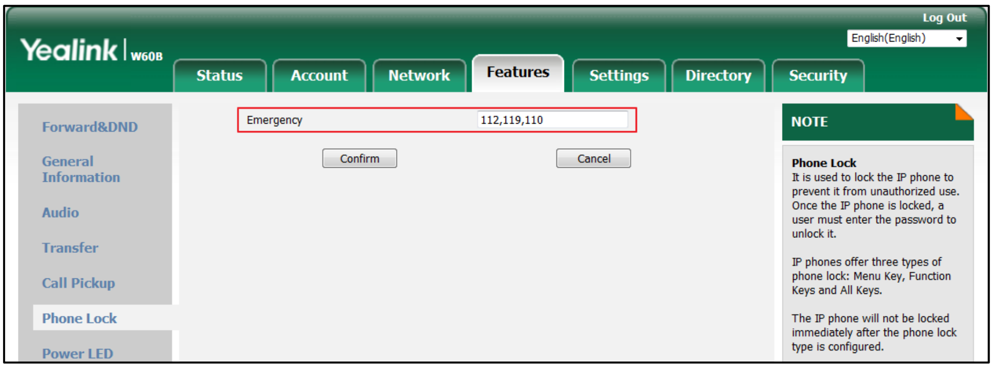
Configuration File	y000000000077.cfg	Configure emergency numbers. **Parameter:** phone_setting.emergency.number
Web User Interface		Configure emergency numbers. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-phonelock&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.emergency.number	**String within 99 characters**	**112, 911, 110**
Description: Configures emergency numbers. Multiple emergency numbers are separated by commas. **Web User Interface:** Features->Phone Lock->Emergency **Handset User Interface:** None		

To configure emergency numbers via web user interface:

1. Click on **Features**->**Phone Lock**.
2. Enter the emergency number in the **Emergency** field.



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

Transport Layer Security (TLS)

TLS is a commonly-used protocol for providing communications privacy and managing the security of message transmission, allowing DECT IP phones to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent eavesdropping and tampering.

TLS protocol is composed of two layers: TLS Record Protocol and TLS Handshake Protocol. The TLS Record Protocol completes the actual data transmission and ensures the integrity and privacy of the data. The TLS Handshake Protocol allows the server and client to authenticate each other and negotiate an encryption algorithm and cryptographic keys before data is exchanged.

The TLS protocol uses asymmetric encryption for authentication of key exchange, symmetric encryption for confidentiality, and message authentication codes for integrity.

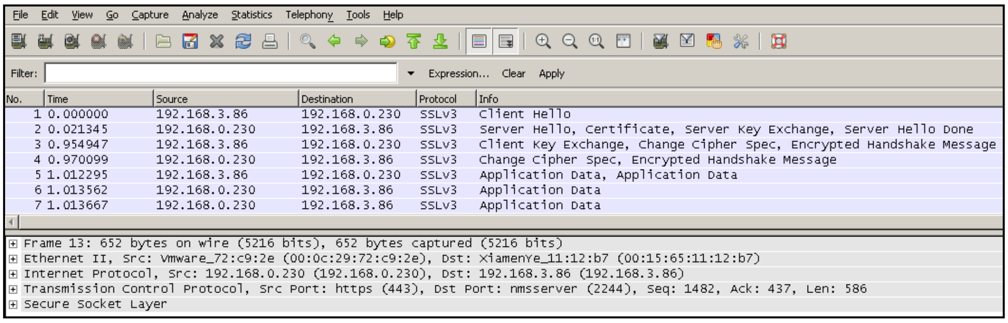
- **Symmetric encryption**: For symmetric encryption, the encryption key and the corresponding decryption key can be told by each other. In most cases, the encryption key is the same as the decryption key.
- **Asymmetric encryption**: For asymmetric encryption, each user has a pair of cryptographic keys – a public encryption key and a private decryption key. The information encrypted by the public key can only be decrypted by the corresponding private key and vice versa. Usually, the receiver keeps its private key. The public key is known by the sender, so the sender sends the information encrypted by the known public key, and then the receiver uses the private key to decrypt it.

DECT IP phones support TLS version 1.0, 1.1 and 1.2. 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. DECT IP phones support the following cipher suites:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- AES256-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA

- RC4-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- EXP1024-DHE-DSS-RC4-SHA
- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC4-MD5

The following figure illustrates the TLS messages exchanged between the DECT IP phone and TLS server to establish an encrypted communication channel:



Step1: DECT IP phone sends "Client Hello" message proposing SSL options.

Step2: Server responds with "Server Hello" message selecting the SSL options, sends its public key information in "Server Key Exchange" message and concludes its part of the negotiation with "Server Hello Done" message.

Step3: DECT IP phone sends session key information (encrypted by server's public key) in the "Client Key Exchange" message.

Step4: Server sends "Change Cipher Spec" message to activate the negotiated options for all future messages it will send.

DECT IP phones can encrypt SIP with TLS, which is called SIPS. When TLS is enabled for an account, the SIP message of this account will be encrypted, and a lock icon appears on the LCD screen after the successful TLS negotiation.

Certificates

The DECT IP phone can serve as a TLS client or a TLS server. The TLS requires the following security certificates to perform the TLS handshake:

- **Trusted Certificate**: When the DECT IP phone requests a TLS connection with a server, the DECT IP phone should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The DECT IP phone has 76 built-in trusted certificates. You can upload 10 custom certificates at most. The format of the trusted certificate files must be *.pem,*.cer,*.crt and *.der and the maximum file size is 5MB. For more information on 76 trusted certificates, refer to Appendix C: Trusted Certificates on page 470.
- **Server Certificate**: When clients request a TLS connection with the DECT IP phone, the DECT IP phone sends the server certificate to the clients for authentication. The DECT 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 DECT 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 DECT IP phone (based on the MAC address) and issued by the Yealink Certificate Authority (CA).
    - **A generic server certificate**: It issued by the Yealink Certificate Authority (CA). Only if no unique certificate exists, the DECT IP phone may send a generic certificate for authentication.

The DECT 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 DECT IP phone accepts: default certificates, custom certificates or all certificates.

Common Name Validation feature enables the DECT IP phone to mandatorily validate the common name of the certificate sent by the connecting server. And Security verification rules are compliant with RFC 2818.

Note

In TLS feature, we use the terms trusted and server certificate. These are also known as CA and device certificates.

Resetting the IP phone to factory defaults will delete custom certificates by default. But this feature is configurable by the parameter "static.phone_setting.reserve_certs_enable" using the configuration files.

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure TLS on a per-line basis. **Parameter:** account.X.sip_server.Y.transport_type
	y000000000077.cfg	Configure the TLS version. **Parameter:** static.security.default_ssl_method
		Configure trusted certificates feature. **Parameters:** static.security.trust_certificates static.security.ca_cert static.security.cn_validation
		Configure server certificates feature. **Parameter:** static.security.dev_cert
		Upload the trusted certificates. **Parameter:** static.trusted_certificates.url
		Delete all uploaded trusted certificates. **Parameter:** static.trusted_certificates.delete
		Upload the server certificates. **Parameter:** static.server_certificates.url
		Delete all uploaded server certificates. **Parameter:** static.server_certificates.delete
		Configure the custom certificates. **Parameter:** static.phone_setting.reserve_certs_enable
Web User Interface		Configure TLS on a per-line basis. **Navigate to:** http://<phoneIPAddress>/servlet?p=accou

	nt-register&q=load&acc=0
	Configure trusted certificates feature. Upload the trusted certificates. **Navigate to**: http://<phoneIPAddress>/servlet?p=truste d-cert&q=load
	Configure server certificates feature. Upload the server certificates. **Navigate to**: http://<phoneIPAddress>/servlet?p=server -cert&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.sip_server.Y.transport_type (X ranges from 1 to 8, Y ranges from 1 to 2)	**0, 1, 2 or 3**	**0**
Description: Configures the transport method the DECT IP phone uses to communicate with the SIP server for account X. **0**-UDP **1**-TCP **2**-TLS **3**-DNS-NAPTR **Web User Interface:** Account->Register->SIP Server Y->Transport **Handset User Interface:** None		
static.security.default_ssl_method	**0, 3, 4 or 5**	**3**
Description: Configures the TLS version the DECT IP phone uses to authenticate with the server. **0**-TLS 1.0 only **3**-SSL V23 (automatic negotiation with server. The phone starts with TLS1.2 for negotiation. **4**-TLS 1.1 only		

Parameters	Permitted Values	Default
5-TLS 1.2 only **Web User Interface:** None **Phone User Interface:** None		
static.security.trust_certificates	**0 or 1**	**1**
Description: Enables or disables the DECT IP phone to only trust the server certificates in the Trusted Certificates list. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the DECT IP phone will trust the server no matter whether the certificate sent by the server is valid or not. If it is set to 1 (Enabled), the DECT IP phone will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, the DECT IP phone will trust the server. **Note:** If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Security->Trusted Certificates->Only Accept Trusted Certificates **Handset User Interface:** None		
static.security.ca_cert	**0, 1 or 2**	**2**
Description: Configures the type of certificates in the Trusted Certificates list for the DECT IP phone to authenticate for TLS connection. **0**-Default Certificates **1**-Custom Certificates **2**-All Certificates **Note:** If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Security->Trusted Certificates->CA Certificates		

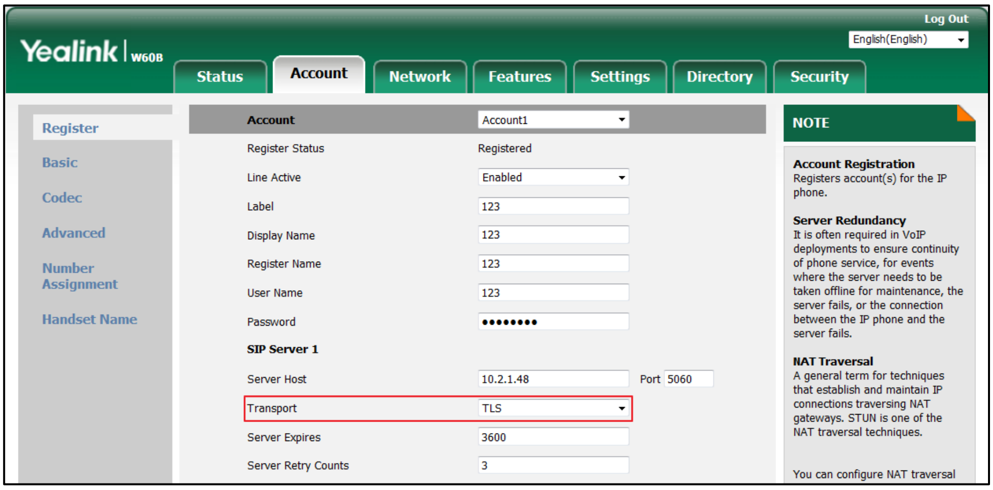
Parameters	Permitted Values	Default
Handset User Interface: None		
static.security.cn_validation	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server. **0**-Disabled **1**-Enabled **Note:** If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Security->Trusted Certificates->Common Name Validation **Handset User Interface:** None		
static.security.dev_cert	**0 or 1**	**0**
Description: Configures the type of the device certificates for the DECT IP phone to send for TLS authentication. **0**-Default Certificates **1**-Custom Certificates **Note:** If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Security->Server Certificates->Device Certificates **Handset User Interface:** None		
static.trusted_certificates.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom trusted certificate used to authenticate the connecting server. **Example:**		

Parameters	Permitted Values	Default
static.trusted_certificates.url = http://192.168.1.20/tc.crt **Note**: The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format. **Web User Interface:** Security->Trusted Certificates->Load trusted certificates file **Handset User Interface:** None		
static.trusted_certificates.delete	**http://localhost/all**	**Blank**
Description: Deletes all uploaded trusted certificates. **Example:** static.trusted_certificates.delete = http://localhost/all **Web User Interface:** None **Handset User Interface:** None		
static.server_certificates.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the server certificate the DECT IP phone sends for authentication. **Example**: static.server_certificates.url = http://192.168.1.20/ca.pem **Note**: The certificate you want to upload must be in *.pem or *.cer format. **Web User Interface:** Security->Server Certificates->Load server cer file **Handset User Interface:** None		
static.server_certificates.delete	**http://localhost/all**	**Blank**
Description: Deletes all uploaded server certificates. **Example:**		

Parameters	Permitted Values	Default
static.server_certificates.delete = http://localhost/all **Web User Interface:** None **Handset User Interface:** None		
static.phone_setting.reserve_certs_enable	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to reserve custom certificates after it is reset to factory defaults. **0**-Disabled **1**-Enabled **Web User Interface:** None **Handset User Interface:** None		

To configure TLS on a per-line basis via web user interface:

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

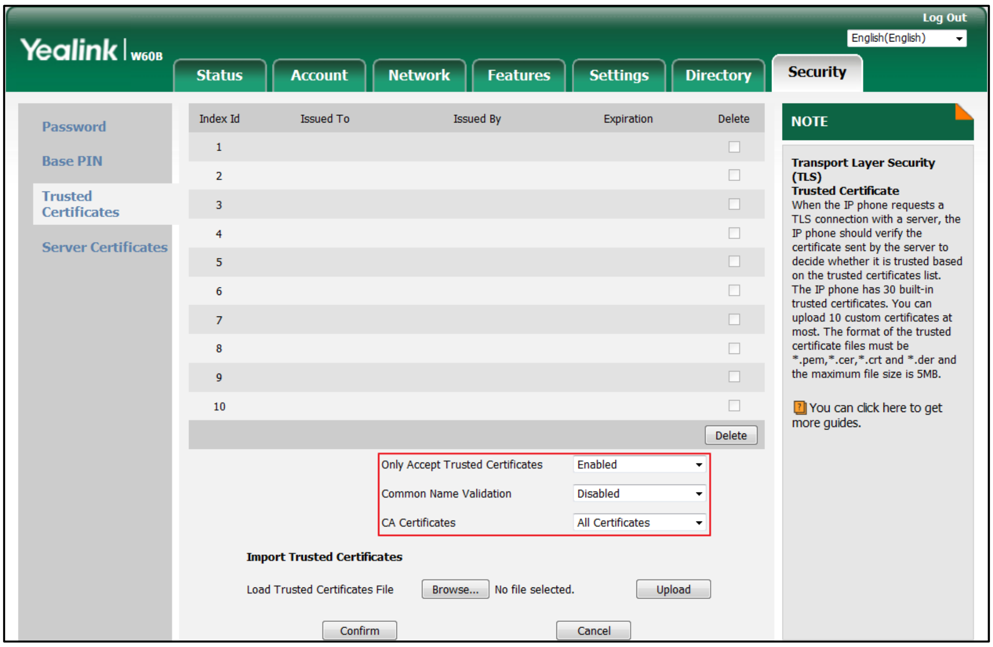


4. Click **Confirm** to accept the change.

To configure the trusted certificates via web user interface:

1. Click on **Security**->**Trusted Certificates**.

2. Select the desired values from the pull-down lists of **Only Accept Trusted Certificates**, **Common Name Validation** and **CA Certificates**.



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

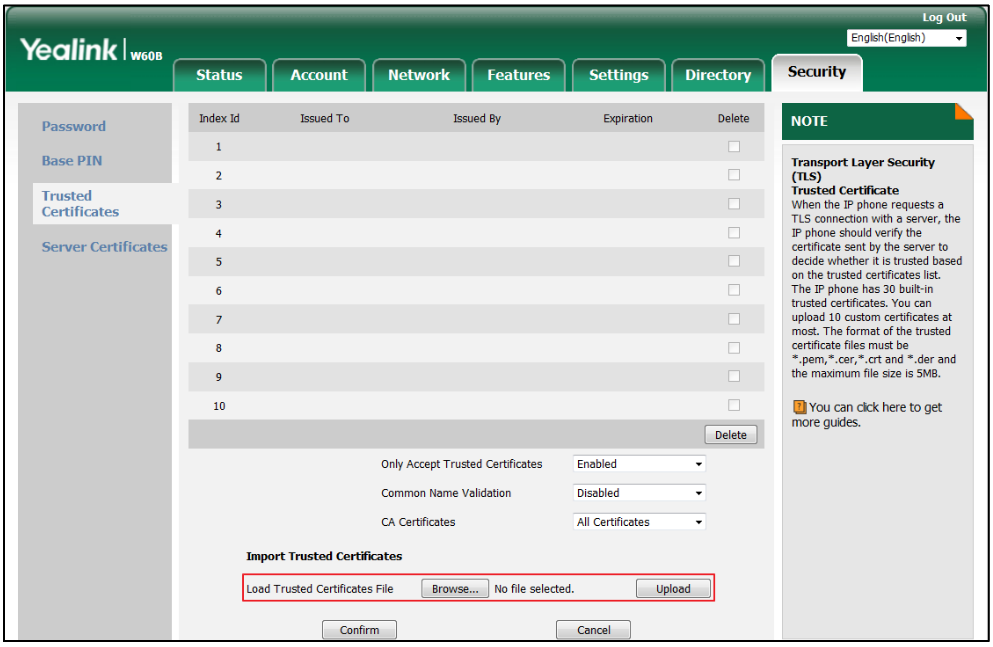
   A dialog box pops up to prompt that the settings will take effect after a reboot.

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

To upload a trusted certificate via web user interface:

1. Click on **Security**->**Trusted Certificates**.

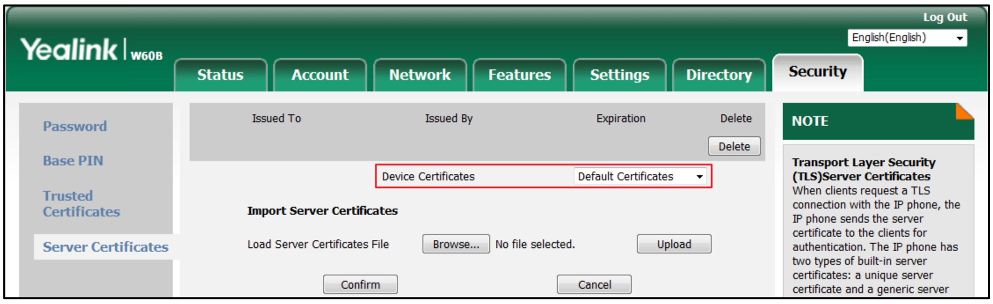
2. Click **Browse** to select the certificate (*.pem, *.crt, *.cer or *.der) from your local system.



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

To configure the server certificates via web user interface:

1. Click on **Security**->**Server Certificates**.
2. Select the desired value from the pull-down list of **Device Certificates**.

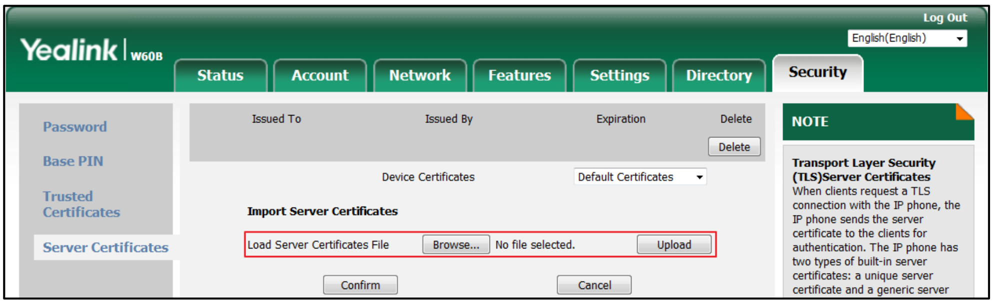


3. Click **Confirm** to accept the change.

To upload a server certificate via web user interface:

1. Click on **Security**->**Server Certificates**.

2. Click **Browse** to select the certificate (*.pem and *.cer) from your local system.



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

Secure Real-Time Transport Protocol (SRTP)

Secure Real-Time Transport Protocol (SRTP) encrypts the RTP during VoDECT IP phone calls to avoid interception and eavesdropping. The parties participating in the call must enable SRTP feature simultaneously. When this feature is enabled on both phones, the type of encryption to utilize for the session is negotiated between the DECT IP phones. This negotiation process is compliant with RFC 4568.

When a user places a call on the enabled SRTP phone, the DECT IP phone sends an INVITE message with the RTP encryption algorithm to the destination phone. As described in RFC 3711, RTP streams may be encrypted using an AES (Advanced Encryption Standard) algorithm.

Example of the RTP encryption algorithm carried in the SDP of the INVITE message:

```
m=audio 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
```

SRTP is configurable on a per-line basis. When SRTP is enabled on both DECT IP phones, RTP streams will be encrypted, and a lock icon appears on the LCD screen of each DECT IP phone after successful negotiation.

Note If you enable SRTP, then you should also enable TLS. This ensures the security of SRTP encryption. For more information on TLS, refer to Transport Layer Security (TLS) on page 403.

Procedure

SRTP can be configured using the following methods.

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

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.srtp_encryption (X ranges from 1 to 8)	**0, 1 or 2**	**0**
Description: Configures whether to use voice encryption service for account X. **0**-Disabled **1**-Optional **2**-Compulsory		

<table>
<tr><th>Parameter</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">If it is set to 0 (Disabled), the DECT IP phone will not use voice encryption service.

If it is set to 1 (Optional), the DECT IP phone will negotiate with the other DECT IP phone what type of encryption to utilize for the session.

If it is set to 2 (Compulsory), the DECT IP phone is forced to use SRTP during a call.

Web User Interface:

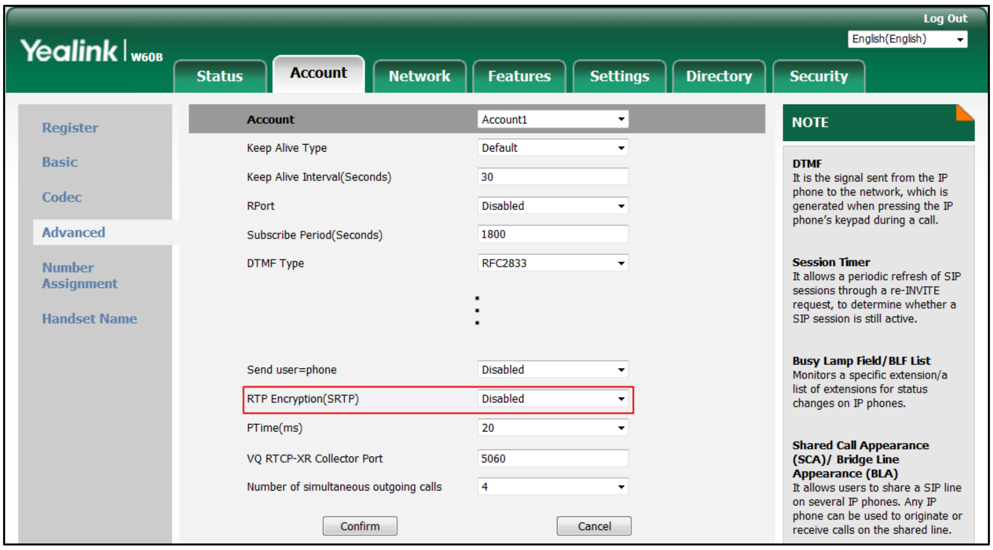
Account->Advanced->RTP Encryption(SRTP)

Handset User Interface:

None</td></tr>
</table>

To configure SRTP feature via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **RTP Encryption(SRTP)**.



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

Encrypting and Decrypting Files

Yealink DECT IP phones support downloading encrypted files from the server and encrypting files before/when uploading them to the server. You can encrypt the following files:

- **Configuration files**: MAC-Oriented CFG file (<MAC>.cfg), Common CFG file (y000000000077.cfg), MAC-local CFG file (<MAC>-local.cfg) or other custom CFG files (e.g., sip.cfg, account.cfg)

To encrypt/decrypt files, you may have to configure an AES key.

Configuration Parameters

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure whether to only download and resolve the encrypted files. **Parameter:** static.auto_provision.update_file_mode
		Configure the decryption method. **Parameter:** static.auto_provision.aes_key_in_file
		Configure AES keys. **Parameters:** static.auto_provision.aes_key_16.com static.auto_provision.aes_key_16.mac
		Specify if the MAC-local CFG file is encrypted when it is uploaded from the phone to the server. **Parameter:** static.auto_provision.encryption.config
Web User Interface		Configure AES keys. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-autop&q=load
Handset User Interface		Configure AES keys.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.auto_provision.update_file_mode	**0 or 1**	**0**
Description: Enables or disables the IP phone only to download the encrypted files. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the DECT IP phone will download the configuration files (e.g.,		

Parameters	Permitted Values	Default
sip.cfg, account.cfg, <MAC>-local.cfg) 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 DECT IP phone system. If it is set to 1 (Enabled), the IP phone will only download the encrypted configuration files (e.g., sip.cfg, account.cfg, <MAC>-local.cfg) from the server during auto provisioning, and then resolve these files and update settings onto the IP phone system. **Web User Interface:** None **Handset User Interface:** None		
static.auto_provision.aes_key_in_file	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to decrypt configuration files using the encrypted AES keys. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the DECT IP phone will decrypt the encrypted configuration files using plaintext AES keys configured on the DECT IP phone. If it is set to 1 (Enabled), the DECT IP phone will download <xx_Security>.enc files (e.g., <sip_Security>.enc, <account_Security>.enc) during auto provisioning, and then decrypts these files into the plaintext keys (e.g., key2, key3) respectively using the phone built-in key (e.g., key1). The DECT IP phone then decrypts the encrypted configuration files using corresponding key (e.g., key2, key3). **Web User Interface:** None **Handset User Interface:** None		
static.auto_provision.aes_key_16.com	**16 characters**	**Blank**
Description: Configures the plaintext AES key for encrypting/decrypting the Common CFG/Custom CFG file. The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: **# $ % * + , - . : = ? @ [ ] ^ _ { } ~**. **Example:**		

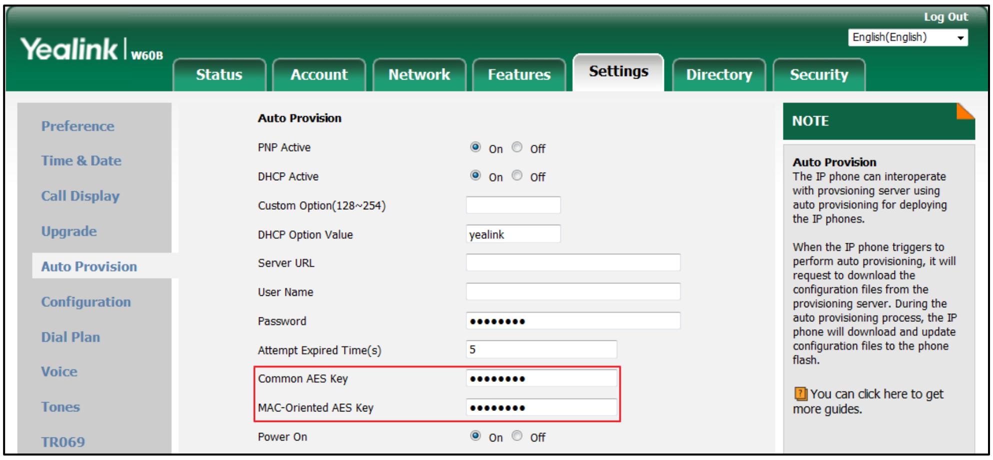
Parameters	Permitted Values	Default
static.auto_provision.aes_key_16.com = 0123456789abcdef **Note**: For decrypting, it works only if the value of the parameter "static.auto_provision.aes_key_in_file" is set to 0 (Disabled). If the downloaded MAC-Oriented file is encrypted and the parameter "static.auto_provision.aes_key_16.mac" is left blank, the DECT IP phone will try to encrypt/decrypt the MAC-Oriented file using the AES key configured by the parameter "static.auto_provision.aes_key_16.com". **Web User Interface:** Settings->Auto Provision->Common AES Key **Handset User Interface:** None		
static.auto_provision.aes_key_16.mac	**16 characters**	**Blank**
Description: Configures the plaintext AES key for encrypting/decrypting the MAC-Oriented files (<MAC>.cfg, <MAC>-local.cfg). The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: **# $ % * + , - . : = ? @ [ ] ^ _ { } ~**. **Example:** static.auto_provision.aes_key_16.mac = 0123456789abmins **Note**: For decrypting, it works only if the value of the parameter "static.auto_provision.aes_key_in_file" is set to 0 (Disabled). If the downloaded MAC-Oriented file is encrypted and the parameter "static.auto_provision.aes_key_16.mac" is left blank, the DECT IP phone will try to encrypt/decrypt the MAC-Oriented file using the AES key configured by the parameter "static.auto_provision.aes_key_16.com". **Web User Interface:** Settings->Auto Provision->MAC-Oriented AES Key **Handset User Interface:** None		
static.auto_provision.encryption.config	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to encrypt <MAC>-local.cfg file using the plaintext AES key. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the MAC-local CFG file is uploaded unencrypted and replaces the		

Parameters	Permitted Values	Default
one (encrypted or unencrypted) stored on the server if you have configured to back up the MAC-local CFG file to the server by the parameter "static.auto_provision.custom.sync". If it is set to 1 (Enabled), the MAC-local CFG file is uploaded encrypted and replaces the one (encrypted or unencrypted) stored on the server if you have configured to back up the MAC-local CFG file to the server by the parameter "static.auto_provision.custom.sync". The plaintext AES key is configured by the parameter "static.auto_provision.aes_key_16.mac". **Web User Interface:** None **Handset User Interface:** None		

To configure AES keys via web user interface:

1. Click on **Settings**->**Auto Provision**.
2. Enter the values in the **Common AES Key** and **MAC-Oriented AES Key** fields.

   AES keys must be 16 characters and the supported characters contain: 0-9, A-Z, a-z and the following special characters are also supported: **# $ % * + , - . : = ? @ [ ] ^ _ { } ~**.



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

Encrypting and Decrypting Configuration Files

Encrypted configuration files can be downloaded from the provisioning server to protect against unauthorized access and tampering of sensitive information (e.g., login passwords, registration information).

Yealink supplies a configuration encryption tool for encrypting configuration files. The encryption tool encrypts plaintext configuration files (e.g., account.cfg, y000000000077.cfg, <MAC>.cfg) (one by one or in batch) using 16-character symmetric keys (the same or different keys for configuration files) and generates encrypted configuration files with the same file name as before.

Note You can also configure the <MAC>-local.cfg files to be automatically encrypted using 16-character symmetric keys when uploading to the server (by setting the value of the parameter "static.auto_provision.encryption.config" to 1).

This tool also encrypts the plaintext 16-character symmetric keys using a fixed key, which is the same as the one built in the DECT IP phone, and generates new files named as <xx_Security>.enc (xx indicates the name of the configuration file, for example, y000000000077_Security.enc for y000000000077.cfg file, account_Security.enc for account.cfg). This tool generates another new file named as Aeskey.txt to store the plaintext 16-character symmetric keys for each configuration file.

For a Microsoft Windows platform, you can use a Yealink-supplied encryption tool "Config_Encrypt_Tool.exe" to encrypt the configuration files respectively.

Note Yealink also supplies a configuration encryption tool (yealinkencrypt) for Linux platform if required. For more information, refer to *Yealink Configuration Encryption Tool User Guide*.

For security reasons, administrator should upload encrypted configuration files, <xx_Security>.enc files to the root directory of the provisioning server. During auto provisioning, the DECT IP phone requests to download the boot file first and then download the referenced configuration files. For more information on boot file, refer to Boot Files on page 84. For example, the DECT IP phone downloads account.cfg file and it is encrypted. The DECT IP phone will request to download <account_Security>.enc file (if enabled) and decrypt it into the the plaintext key (e.g., key2) using the built-in key (e.g., key1). Then the DECT IP phone decrypts account.cfg file using key2. After decryption, the DECT IP phone resolves configuration files and updates configuration settings onto the DECT IP phone system.

The way the DECT IP phone processes other configuration files is the same to that of the account.cfg file.

Procedure to Encrypt Configuration Files

To encrypt the account.cfg file:

1. Double click "Config_Encrypt_Tool.exe" to start the application tool.

   The screenshot of the main page is shown as below:

   When you start the application tool, a file folder named "Encrypted" is created automatically in the directory where the application tool is located.

2. Click **Browse** to locate configuration file(s) (e.g., 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.

3. (Optional.) Click **Browse** to locate the target directory from your local system in the **Target Directory** field.

   The tool uses the file folder "Encrypted" as the target directory by default.

4. (Optional.) Mark the desired radio box in the **AES Model** field.

   If you mark the **Manual** radio box, you can enter an AES key in the **AES KEY** field or click **Re-Generate** to generate an AES key in the **AES KEY** field. The configuration file(s) will be encrypted using the AES key in the **AES KEY** field.

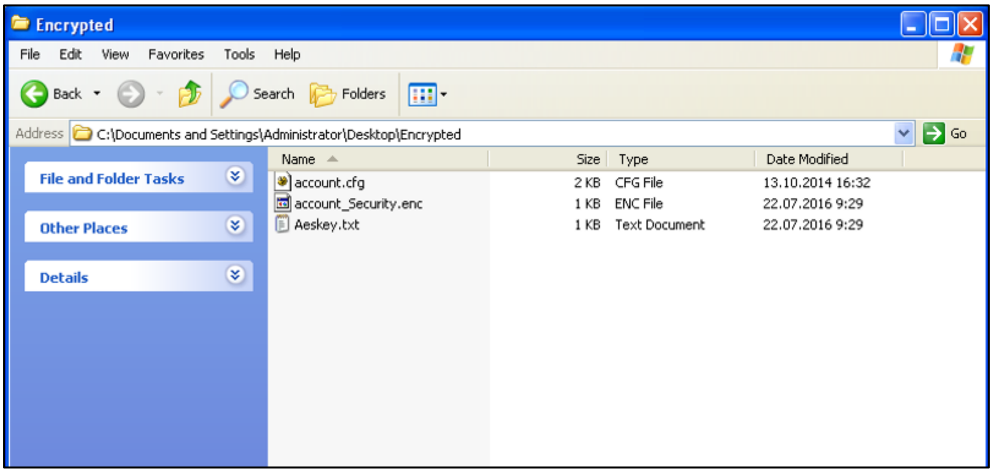
   If you mark the **Auto Generate** radio box, the configuration file(s) will be encrypted using random AES key. The AES keys of configuration files are different.

Note AES keys must be 16 characters and the supported characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: **# $ % * + , - . : = ? @ [ ] ^ _ { } ~**.

5. Click **Encrypt** to encrypt the configuration file(s).

6. Click **OK**.

   The target directory will be automatically opened. You can find the encrypted CFG file(s), encrypted key file(s) and an Aeskey.txt file storing plaintext AES key(s).



Troubleshooting

This chapter provides an administrator with general information for troubleshooting some common problems that he (or she) may encounter while using DECT IP phones.

Troubleshooting Methods

DECT IP phones can provide feedback in a variety of forms such as log files, packets, status indicators and so on, which can help an administrator more easily find the system problem and fix it.

The following are helpful for better understanding and resolving the working status of the DECT IP phone.

- Viewing Log Files
- Capturing Packets
- Enabling Watch Dog Feature
- Analyzing Configuration File
- Exporting All the Diagnostic Files

Viewing Log Files

If your DECT IP phone encounters some problems, commonly the local log files or syslog files are needed.

You can configure the phone to log events locally. There are two types of local log files: <MAC>-boot.log (e.g., 0015659188f2-boot.log) and <MAC>-sys.log (e.g., 0015659188f2-sys.log). These two local log files can be exported via web user interface separately. You can configure the DECT IP phone to periodically upload the local log files to the provisioning server (only support an FTP/TFTP as the provisioning server) or the specific server (if configured), avoiding the local log loss. You can specify the severity level of the log to be reported to the <MAC>-sys.log file. The default local log level is 3.

You can also configure the DECT IP phone to send syslog messages to a syslog server in real time. You can specify the severity level of the syslog to be sent to a syslog server. The default system log level is 3.

Local Logging

Procedure

Local logging can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure local logging feature. **Parameter:** static.local_log.enable
		Configure the severity level of the logs to be reported to the <MAC>-sys.log file. **Parameter:** static.local_log.level
		Configure the maximum size of the log files to be stored on the phone. **Parameter:** static.local_log.max_file_size
		Configure the maximum size of the local log files to be stored on the server. **Parameter:** static.auto_provision.local_log.backup.append.max_file_size
		Configure the DECT IP phone to upload local log files to the server. **Parameter:** static.auto_provision.local_log.backup.enable
		Configure the period of the local log files uploads to the server. **Parameter:** static.auto_provision.local_log.backup.upload_period
		Configure the behavior when local log files on the server reach the maximum size. **Parameter:** static.auto_provision.local_log.backup.append.limit_mode
		Configure whether the local log files on the server are overwritten or appended.

		Parameter: static.auto_provision.local_log.backup.append
		Configure the waiting time before the phone uploads the <MAC>-boot.log file to the server after bootup. **Parameter:** static.auto_provision.local_log.backup.bootlog.upload_wait_time
		Configure the upload path of the local log files. **Parameter:** static.auto_provision.local_log.backup.path
Web User Interface		Configure local logging feature. Configure the severity level of the logs to be reported to the <MAC>-sys.log file. Configure the maximum size of the log files to be stored on the phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-config&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.local_log.enable	**0 or 1**	**1**
Description: Enables or disables the DECT IP phone to record log to the log files locally. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the DECT IP 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. If it is set to 1 (Enabled), the DECT IP 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. **Note**: We recommend you not to disable this feature.		

Parameters	Permitted Values	Default
Web User Interface: Settings->Configuration->Local Log->Enable Local Log **Handset User Interface:** None		
static.local_log.level	**Integer from 0 to 6**	**3**
Description: Configures the lowest level of local log information to be reported to the <MAC>-sys.log file. When you choose a log level, you are including all events of an equal or higher severity level and excluding events of a lower severity level. The logging level you choose determines the lowest severity of events to log. **0**-system is unusable **1**-action must be taken immediately **2**-critical condition **3**-error conditions **4**-warning conditions **5**-normal but significant condition **6**-informational **Web User Interface:** Settings->Configuration->Local Log->Local Log Level **Handset User Interface:** None		
static.local_log.max_file_size	**Integer from 1024 to 2048**	**1024**
Description: Configures the maximum size (in KB) of the log files (<MAC>-boot.log and <MAC>-sys.log) to be stored on the DECT IP phone. When this size is about to be exceeded, (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 DECT IP phone will clear all the local log files on the phone once successfully backing up. (2) If the value of the parameter "static.auto_provision.local_log.backup.enable" is set to 0 (Disabled), the DECT IP phone will erase half of the logs from the oldest log information on the phone.		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Defa ult</th></tr>
<tr><td colspan="3">Example:
static.local_log.max_file_size = 1024
Web User Interface:
Settings->Configuration->Local Log->Max Log File Size (1024-2048KB)
Handset User Interface:
None</td></tr>
<tr><td>static.auto_provision.local_log.backup.enable</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables the DECT IP phone to upload the local log files (<MAC>-boot.log and <MAC>-sys.log) to the provisioning server or a specific server.
0-Disabled
1-Enabled
If it is set to 1 (Enabled), the DECT IP 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:
- Auto provisioning is triggered;
- The size of the local log files reaches maximum configured by the parameter “static.local_log.max_file_size”;
- It’s time to upload local log files according to the upload period configured by the parameter ”static.auto_provision.local_log.backup.upload_period”.
Note: The upload path is configured by the parameter “static.auto_provision.local_log.backup.path”.
Web User Interface:
None
Handset User Interface:
None</td></tr>
<tr><td>static.auto_provision.local_log.backup.upload_period</td><td>Integer from 30 to 86400</td><td>30</td></tr>
<tr><td colspan="3">Description:
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.
Example:
static.auto_provision.local_log.backup.upload_period = 60
Note: It works only if the value of the parameter “static.auto_provision.local_log.backup.enable” is set to 1 (Enabled).</td></tr>
</table>

Parameters	Permitted Values	Default
Web User Interface: None **Handset User Interface:** None		
static.auto_provision.local_log.backup.path	**URL within 1024 characters**	**Blank**
Description: Configures the upload path of the local log files (<MAC>-boot.log and <MAC>-sys.log). If you leave it blank, the DECT IP phone will upload the local log files to the provisioning server. If you configure a relative URL (e.g., /upload), the DECT IP phone will upload the local log files by extracting the root directory from the access URL of the provisioning server. If you configure an absolute URL with protocol (e.g., tftp), the DECT IP phone will upload the local log files using the desired protocol. If no protocol, the DECT IP phone will use the same protocol with auto provisioning for uploading files. **Example:** static.auto_provision.local_log.backup.path = tftp://10.3.6.133/upload/ **Note**: It works only if the value of the parameter “static.auto_provision.local_log.backup.enable” is set to 1 (Enabled). **Web User Interface:** None **Handset User Interface:** None		
static.auto_provision.local_log.backup.append	**0 or 1**	**0**
Description: Configures whether the local log files (<MAC>-boot.log and <MAC>-sys.log) on the provisioning server or a specific server are overwritten or appended. **0-**Overwrite **1-**Append (not applicable to TFTP Server) **Web User Interface:** None **Handset User Interface:** None		

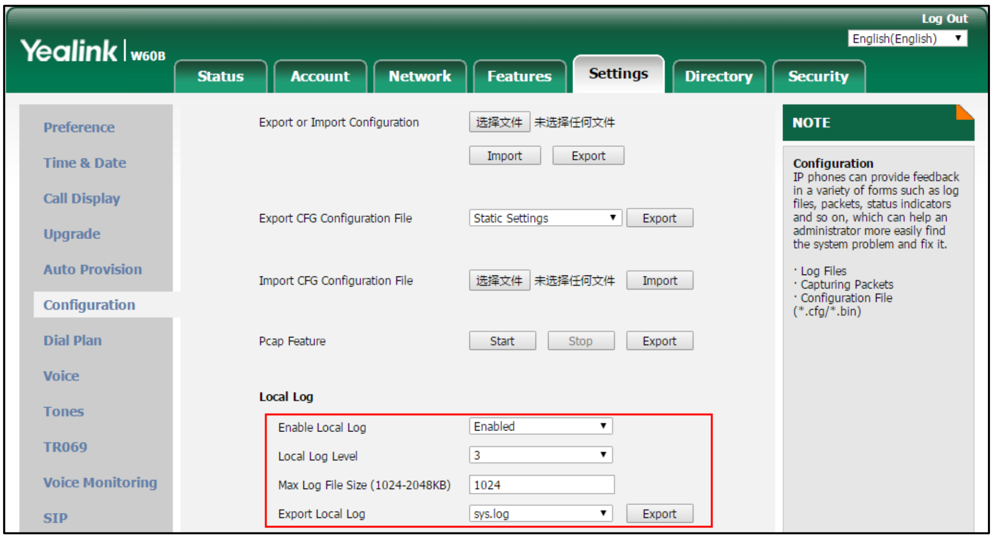
<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>static.auto_provision.local_log.backup.append.limit_mode</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Configures the behavior when local log files (<MAC>-boot.log and <MAC>-sys.log) on the provisioning server or a specific server reach the maximum size.
0-Append Delete
1-Append Stop
If it is set to 1 (Append Delete), the DECT IP phone will delete the old log and start over.
If it is set to 2 (Append Stop), the DECT IP phone will stop uploading log.
Web User Interface:
None
Handset User Interface:
None</td></tr>
<tr><td>static.auto_provision.local_log.backup.append.max_file_size</td><td>Integer from 200 to 65535</td><td>1024</td></tr>
<tr><td colspan="3">Description:
Configures the maximum size (in KB) of the local log files (<MAC>-boot.log and <MAC>-sys.log) to be stored on the provisioning server or a specific server.
Example:
static.auto_provision.local_log.backup.append.max_file_size = 1025
Web User Interface:
None
Handset User Interface:
None</td></tr>
<tr><td>static.auto_provision.local_log.backup.bootlog.upload_wait_time</td><td>Integer from 1 to 86400</td><td>120</td></tr>
<tr><td colspan="3">Description:
Configures the waiting time (in seconds) before the phone uploads the <MAC>-boot.log file to the provisioning server or a specific server after startup.
Example:
static.auto_provision.local_log.backup.bootlog.upload_wait_time = 121
Web User Interface:
None</td></tr>
</table>

Parameters	Permitted Values	Default
Handset User Interface: None		

To export the system log to a local PC via web user interface:

1. Click on **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 (1024-2048KB)** field.
5. Select **sys.log** from the pull-down list of **Export Local Log**.
6. Click **Confirm** to accept the change.



7. Reproduce the issue.
8. Click **Export** to open the file download window, and then save the file to your local system.

To export the boot log to a local PC via web user interface:

1. Click on **Settings**->**Configuration**.
2. Select **Enabled** from the pull-down list of **Enable Local Log**.
3. Select **boot.log** from the pull-down list of **Export Local Log**.
4. Click **Confirm** to accept the change.
5. Click **Export** to open the file download window, and then save the file to your local system.

To view the log files on your local system:

The <MAC>-boot.log file can only log the last reboot events.

The following figure shows a portion of a <MAC>-boot.log (e.g., 00156574b150-boot.log):

```
Jan  1 00:00:24 syslogd started: BusyBox v1.10.3
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
Jan  1 00:00:25 sys [655]: ANY <0+emerg > ANY =3
Jan  1 00:00:25 sys [655]: ANY <0+emerg > Version  :7.2.0.10 for release
Jan  1 00:00:25 sys [655]: ANY <0+emerg > Built-at :Apr 20 2016,11:32:02
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
May 26 00:00:02 Log [706]: ANY <0+emerg > ETLL=3
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
May 26 00:00:02 auto[706]: ANY <0+emerg > ANY =3
May 26 00:00:02 auto[706]: ANY <0+emerg > Version  :6.1.0.8 for release
May 26 00:00:02 auto[706]: ANY <0+emerg > Built-at :May 25 2016,10:26:42
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
May 26 00:00:02 sys [706]: ANY <0+emerg > LSYS=3
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
May 26 00:00:02 ATP [706]: ANY <0+emerg > ANY =3
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
May 26 00:00:05 sys [835]: ANY <0+emerg > LSYS=3
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
May 26 00:00:05 sua [835]: ANY <0+emerg > ANY =5
May 26 00:00:05 sua [835]: ANY <0+emerg > ANY =3
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
May 26 00:00:06 Log [884]: ANY <0+emerg > ANY =5
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
May 26 00:00:07 ipvp[887]: ANY <0+emerg > 807.196.179:Version  :1.0.0.8 for release
May 26 00:00:07 ipvp[887]: ANY <0+emerg > 807.197.104:Built-at :Feb 29 2016,14:11:35
May 26 00:00:07 ipvp[887]: ANY <0+emerg > 807.198.138:ANY =4
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
May 26 00:00:07 sys [887]: ANY <0+emerg > LSYS=3
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 <MAC>-boot.log file is forced to report the logs with all severity levels.

The following figure shows a portion of a <MAC>-sys.log (e.g., 00156574b150-sys.log):

```
May 31 09:02:05 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
May 31 09:02:37 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
May 31 09:03:16 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
May 31 09:03:27 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
May 31 09:03:41 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
May 31 09:03:47 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
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
May 31 19:28:18 sys [1076]: ANY <0+emerg > LSYS=3
Jun  1 02:33:52 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
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
Jun  1 07:28:17 sys [1111]: ANY <0+emerg > LSYS=3
Jun  1 11:34:57 sua [835]: SUB <3+error > [000] BLF Can't find js by sid(0)
Jun  1 11:34:57 sua [835]: SUB <3+error > [000] BLF Can't find js by sid(0)
[ web ]
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.

You can verify whether you got the correct log through the following key fields:

- <0+emerg>
- <1+alert>
- <2+crit>
- <3+error>
- <4+warnin>
- <5+notice>

- <6+info>

Syslog

Procedure

Syslog can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure syslog feature. **Parameter:** static.syslog.enable
		Configure syslog server. **Parameters:** static.syslog.server static.syslog.server_port
		Configure the transport protocol that the DECT IP phone uses to export log to the syslog server. **Parameter:** static.syslog.transport_type
		Configure the lowest severity level of the logs to be displayed in the syslog. **Parameter:** static.syslog.level
		Configure the facility that generates the log messages. **Parameter:** static.syslog.facility
		Configure the DECT IP phone to prepend the MAC address to the log messages exported to the syslog server. **Parameter:** static.syslog.prepend_mac_address.enable
Web User Interface		Configure syslog feature. Configure syslog server. Configure the transport protocol that the DECT IP phone uses to export log to the syslog server. Configure the lowest severity level of the

	logs to be displayed in the syslog. Configure the facility that generates the log messages. Configure the DECT IP phone to prepend the MAC address to the log messages exported to the syslog server. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-config&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.syslog.enable	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to upload log messages to the syslog server in real time. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Configuration->Syslog->Enable Syslog **Handset User Interface:** None		
static.syslog.server	**IP address or domain name**	**Blank**
Description: Configures the IP address or domain name of the syslog server. **Example:** static.syslog.server = 192.168.1.100 **Web User Interface:** Settings->Configuration->Syslog Server **Handset User Interface:** None		
static.syslog.server_port	**Integer from 1 to 65535**	**514**

Parameters	Permitted Values	Default
Description: Configures the port of the syslog server. **Example:** static.syslog.port = 515 **Web User Interface:** Settings->Configuration->Syslog->Syslog Server->Port **Handset User Interface:** None		
static.syslog.transport_type	**0, 1 or 2**	**0**
Description: Configures the transport protocol that the DECT IP phone uses when exporting log messages to the syslog server. **0**-UDP **1**-TCP **2**-TLS **Web User Interface:** Settings->Configuration->Syslog->Syslog Transport Type **Handset User Interface:** None		
static.syslog.level	**Integer from 0 to 6**	**3**
Description: Configures the lowest level of syslog information that displays in the syslog. When you choose a log level, you are including all events of an equal or higher severity level and excluding events of a lower severity level. The logging level you choose determines the lowest severity of events to log. **0**-Emergency: system is unusable **1**-Alert: action must be taken immediately **2**-Critical: critical conditions **3**-Critical: error conditions **4**-Warning: warning conditions **5**-Warning: normal but significant condition		

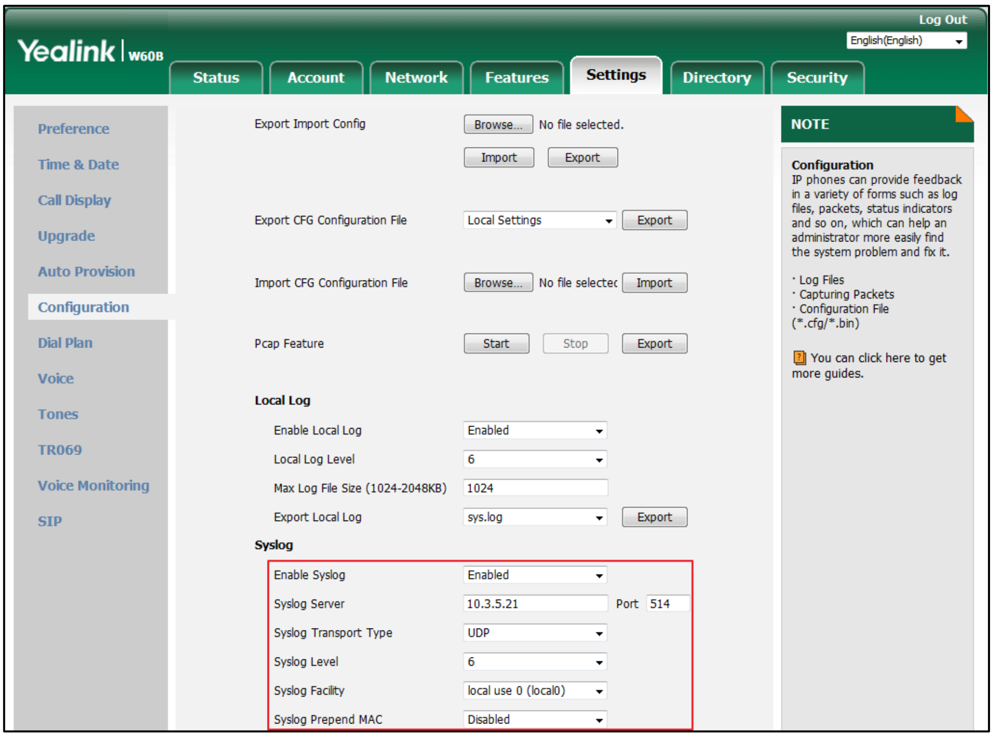
Parameters	Permitted Values	Default
6-Informational: informational messages **Web User Interface:** Settings->Configuration->Syslog->Syslog Level **Handset User Interface:** None		
static.syslog.facility	**Integer from 0 or 23**	**16**
Description: Configures the facility that generates the log messages. **0**-kernel messages **1**-user-level messages **2**-mail system **3**-system daemons **4**-security/authorization messages (note 1) **5**-messages generated internally by syslogd **6**-line printer subsystem **7**-network news subsystem **8**-UUCP subsystem **9**-clock daemon (note 2) **10**-security/authorization messages (note 1) **11**-FTP daemon **12**-NTP subsystem **13**-log audit (note 1) **14**-log alert (note 1) **15**-clock daemon (note 2) **16**-local use 0 (local0) **17**-local use 1 (local1) **18**-local use 2 (local2) **19**-local use 3 (local3) **20**-local use 4 (local4) **21**-local use 5 (local5) **22**-local use 6 (local6) **23**-local use 7 (local7)		

Parameters	Permitted Values	Default
Note: For more information, refer to RFC 3164. **Web User Interface:** Settings->Configuration->Syslog->Syslog Facility **Handset User Interface:** None		
static.syslog.prepend_mac_address.enable	**0 or 1**	**0**
Description: Enables or disables the DECT IP phone to prepend the MAC address to the log messages exported to the syslog server. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Configuration->Syslog->Syslog Prepend MA **Handset User Interface:** None		

To configure the phone to export the system log to a syslog server via web user interface:

1. Click on **Settings**->**Configuration**.
2. Select the desired value from the pull-down list of **Enable Syslog Feature**.
3. Enter the syslog server address in the **Syslog Server** field.
4. Enter the syslog server port in the **Port** field.
5. Select the desired transport type from the pull-down list of **Syslog Transport Type**.
6. Select the desired log level from the pull-down list of **Syslog Level**.
7. Select the desired facility from the pull-down list of **Syslog Facility**.

8. Select the desired value from the pull-down list of **Syslog Prepend MAC**.

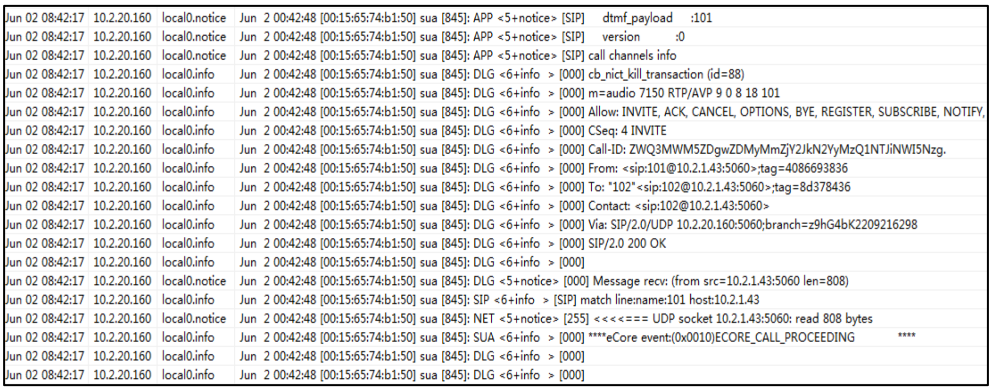


9. Click **Confirm** to accept the change.

To view 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]

Capturing Packets

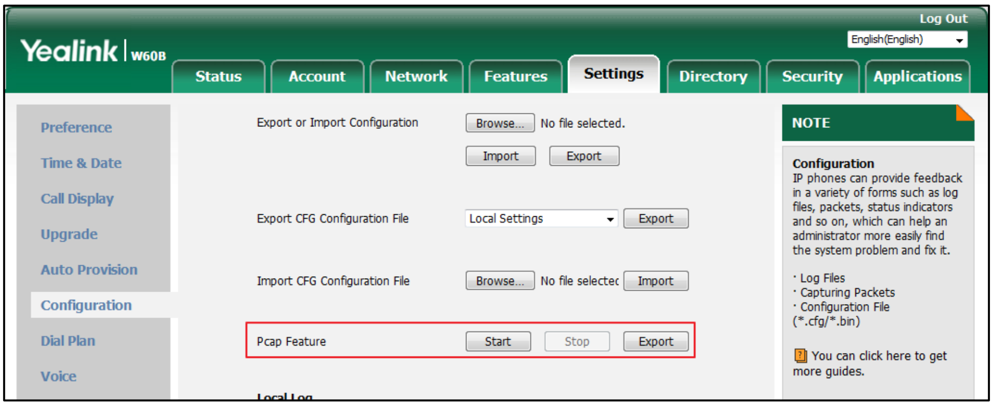
You can capture packet in two ways: capturing the packets via web user interface or using the Ethernet software. You can analyze the packet captured for troubleshooting purpose.

Capturing the Packets via Web User Interface

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

To capture packets via web user interface:

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



2. Click **Start** in the **Pcap Feature** field to start capturing signal traffic.
3. Reproduce the issue to get stack traces.
4. Click **Stop** in the **Pcap Feature** field to stop capturing.
5. Click **Export** to open the file download window, and then save the file to your local system.

Capturing the Packets Using the Ethernet Software

Receiving data packets from the HUB

Connect the Internet port of the DECT IP phone and the PC to the same HUB, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic.

Enabling Watch Dog Feature

The DECT IP phone provides a troubleshooting feature called "Watch Dog", which helps you monitor the DECT IP phone status and provides the ability to get stack traces from the last time the DECT IP phone failed. If Watch Dog feature is enabled, the DECT IP phone will automatically reboot when it detects a fatal failure. This feature can be configured using the configuration files or via web user interface.

Procedure

Watch Dog can be configured using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure Watch Dog feature. **Parameter:** static.watch_dog.enable

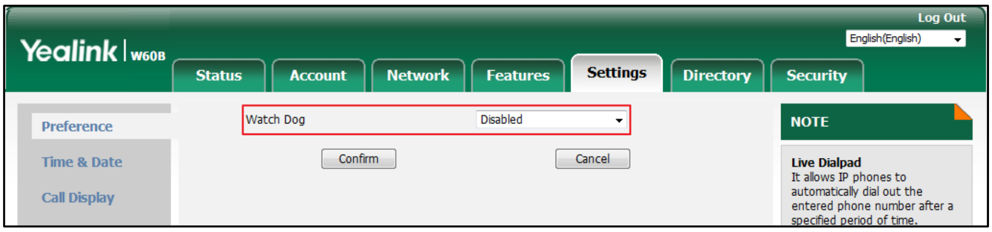
Web User Interface	Configure Watch Dog feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-preference&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
static.watch_dog.enable	**0 or 1**	**1**
Description: Enables or disables the Watch Dog feature. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the DECT IP phone will reboot automatically when the system is broken down. **Web User Interface:** Settings->Preference->Watch Dog **Handset User Interface:** None		

To configure watch dog feature via web user interface:

1. Click on **Settings**->**Preference**.
2. Select the desired value from the pull-down list of **Watch Dog**.



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

Analyzing Configuration Files

Wrong configurations may have an impact on your phone use. You can export configuration file(s) to check the current configuration of the DECT IP phone and troubleshoot if necessary. You can also import configuration files for a quick and easy configuration.

Six types of configuration files can be exported to your local system:

- config.bin

- <MAC>-all.cfg
- <MAC>-local.cfg
- <MAC>-static.cfg
- <MAC>-non-static.cfg
- <MAC>-config.cfg

We recommend you to edit the exported CFG file instead of the BIN file to change the phone's current settings if your phone is running firmware version 73 or later. For more information on configuration files, refer to Configuration Files on page 86.

BIN Configuration Files

The config.bin file is an encrypted file. For more information on config.bin file, contact your Yealink reseller.

Procedure

Configuration changes can be performed using the following methods.

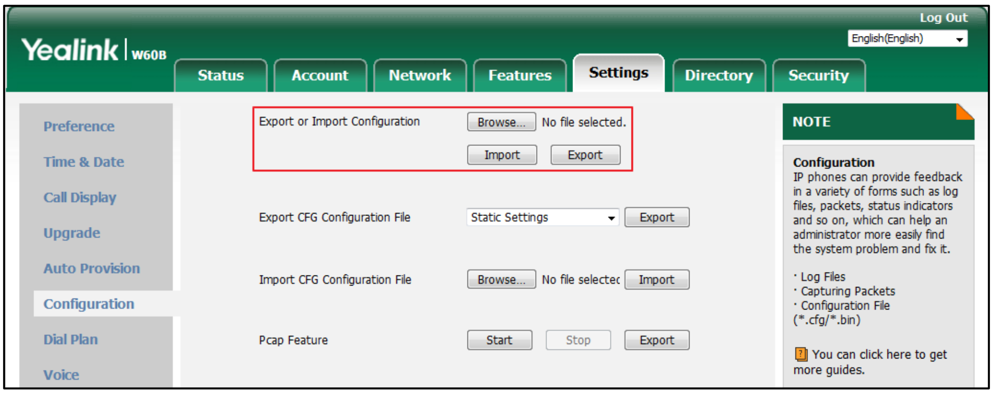
Central Provisioning (Configuration File)	y000000000077.cfg	Specify the access URL for the custom configuration files. **Parameter:** static.configuration.url
Web User Interface		Export or import the custom configuration files. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-config&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
static.configuration.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL for the custom configuration files. **Note**: The file format of custom configuration file must be *.bin. If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Configuration->Export or Import Configuration **Handset User Interface:** None		

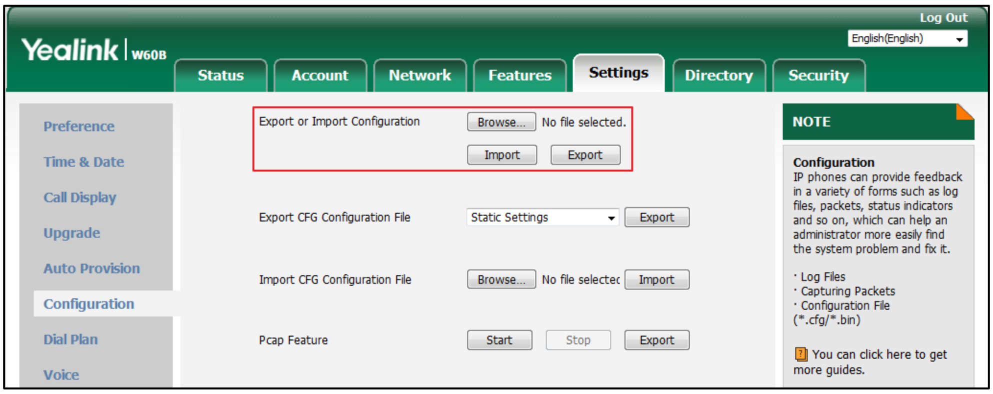
To export BIN configuration files via web user interface:

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



To import a BIN configuration file via web user interface:

1. Click on **Settings**->**Configuration**.
2. In the **Export or Import Configuration** block, click **Browse** to locate a BIN configuration file from your local system.
3. Click **Import** to import the configuration file.



CFG Configuration Files

Five CFG configuration files can be exported:

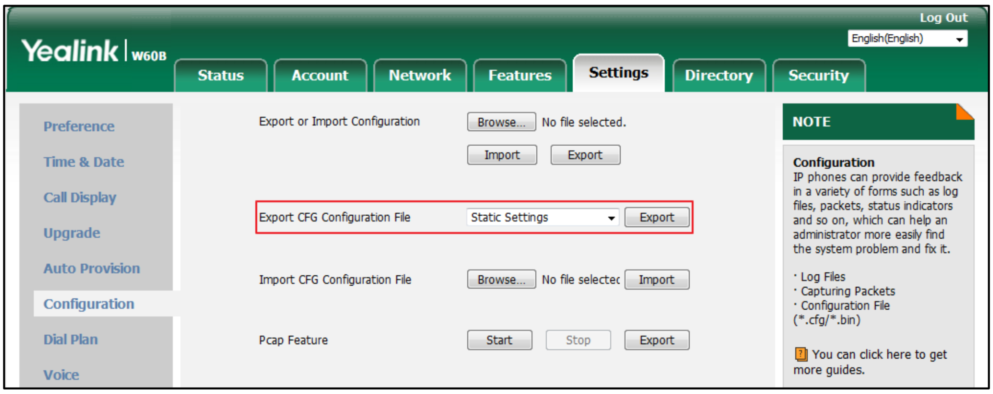
- **<MAC>-local.cfg**: It contains changes associated with non-static settings made via handset user interface and web user interface. It can be exported only if the value of the parameter "static.auto_provision.custom.protect" is set to 1.
- **<MAC>-all.cfg**: It contains all changes made via handset user interface, web user interface and using configuration files.
- **<MAC>-static.cfg**: It contains all changes associated with static settings (e.g., network settings) made via handset user interface, web user interface and using configuration files.
- **<MAC>-non-static.cfg**: It contains all changes associated with non-static settings made

via handset user interface, web user interface and using configuration files.

- **<MAC>-config.cfg**: It contains changes made using configuration files. It can be exported only if the value of the parameter “static.auto_provision.custom.protect” is set to 1.

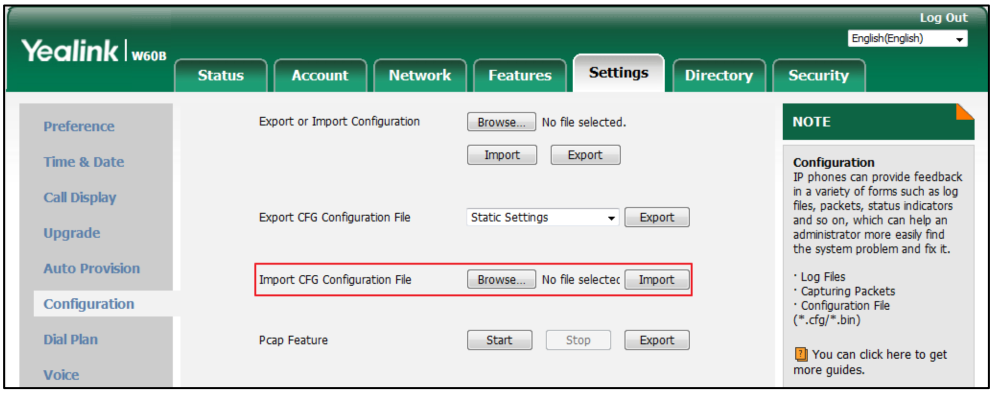
To export CFG configuration files via web user interface:

1. Click on **Settings**->**Configuration**.
2. Select the desired CFG configuration file from the pull-down list of **Export CFG Configuration File**.
3. Click **Export** to open file download window, and then save the file to your local system.



To import CFG configuration files via web user interface:

1. Click on **Settings**->**Configuration**.
2. In the **Import CFG Configuration File** block, click **Browse** to locate a CFG configuration file from your local system.



3. Click **Import** to import the configuration file.

Exporting All the Diagnostic Files

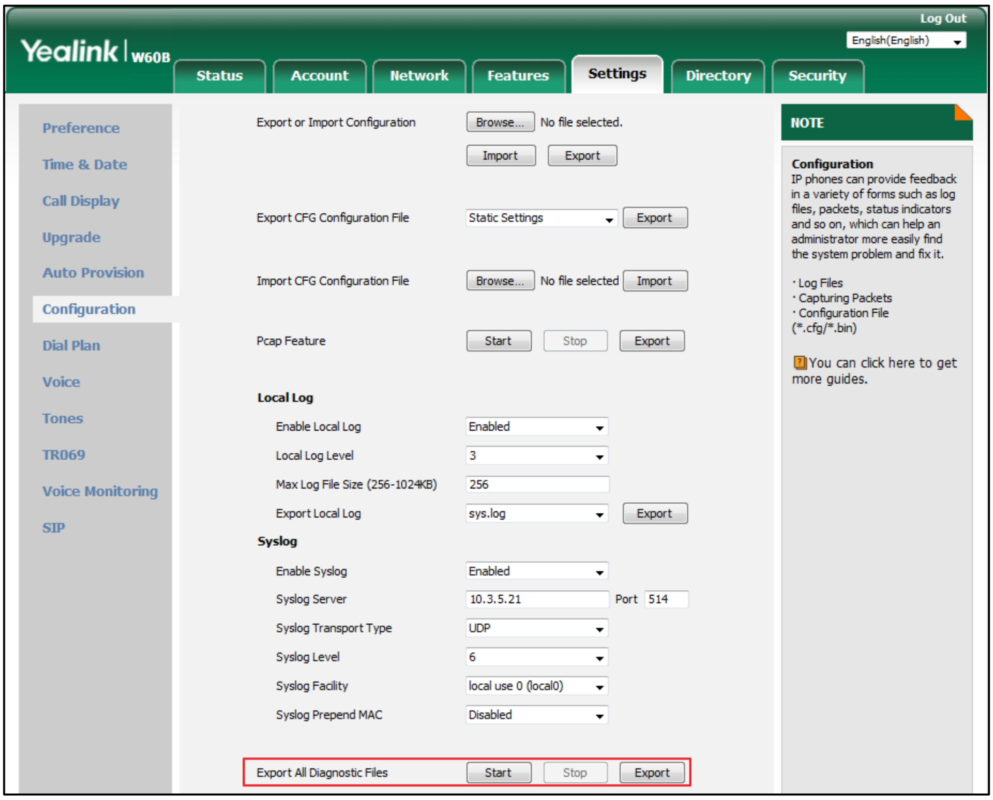
Yealink DECT IP phones support three types of diagnostic files (including Pcap trace, log files (boot.log and sys.log) and BIN configuration files) to help analyze your problem. You can export these files at a time and troubleshoot if necessary. The file format of exported diagnostic file is *.tar.

To export all diagnostic files via web user interface:

1. Click on **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 file download window, and then save the diagnostic file to your local system.



A diagnostic file named **allconfig.tar** is successfully exported to your local system.

Note

If the issue cannot be reproduced, just directly click **Export** to export all diagnostic files.

To view the diagnostic file on your local system:

1. Extract the combined diagnostic files to your local system.
2. Open the folder you extracted to and identify the files you will view.

You can select to export the Pcap trace, log files (boot.log and sys.log) and BIN configuration files respectively.

For more information, refer to Capturing Packets on page 439, Viewing Log Files on page 425 and BIN Configuration Files on page 442.

Troubleshooting Solutions

This section describes solutions to common issues that may occur while using the DECT IP phone. Upon encountering a scenario not listed in this section, contact your Yealink reseller for further support.

IP Address Issues

Why doesn't the DECT IP phone get an IP address?

Do one of the following:

- Ensure that the Ethernet cable is plugged into the Internet port on the base and the Ethernet cable is not loose.
- Ensure that the Ethernet cable is not damaged.
- Ensure that the IP address and related network parameters are set correctly.
- Ensure that your network switch or hub is operational.

How to solve the IP conflict problem?

Do one of the following:

- Reset another available IP address for the DECT IP phone.
- Check network configuration via handset user interface at the path **OK**->**Settings**->**System Settings**->**Network** (default PIN: 0000) ->**Basic**->**IPv4** (or **IPv6**). If the Static IP is selected, select DHCP instead.

Is there a specific format in configuring IPv6 on Yealink DECT IP phones?

Scenario 1:

If the DECT IP phone obtains the IPv6 address, the format of the URL to access the web user interface is "*[IPv6 address]" or "http(s)://[IPv6 address]*". For example, if the IPv6 address of your phone is "fe80::204:13ff:fe30:10e", you can enter the URL (e.g., "[fe80::204:13ff:fe30:10e]" or "http(s)://[fe80::204:13ff:fe30:10e])" in the address bar of a web browser on your PC to access the web user interface.

Scenario 2:

Yealink DECT IP phones support using FTP, TFTP, HTTP and HTTPS protocols to download configuration files or resource files. You can use one of these protocols for provisioning.

When provisioning your DECT IP phone obtaining an IPv6 address, the provisioning server should support IPv6 and the format of the access URL of the provisioning server can be "*tftp://[IPv6 address or domain name]*". For example, if the provisioning server address is "2001:250:1801::1", the access URL of the provisioning server can be "tftp://[2001:250:1801::1]/". For more information on provisioning, refer to *Yealink SIP IP Phones Auto Provisioning Guide_V81*.

Base Issue

Why doesn't the power indicator on the base station light up?

Plug the supplied power adapter to the base station, if the power indicator doesn't light up, it should be a hardware problem. Please contact your vendor or local distributor and send the problem description for help. If you cannot get a support from them, please send a mail which includes problem description, test result, your country and phone's SN to Support@yealink.com.

Why doesn't the network indicator on the base station slowly flash?

It means that the base station cannot get an IP address. Try connecting the base station to another switch port, if the network indicator still slowly flashes, please try a reset.

How to reboot the Base Station remotely?

The base station support remote reboot by a SIP NOTIFY message with "Event: check-sync" header. Whether the DECT IP phone reboots or not depends on the value of the parameter "sip.notify_reboot_enable". If the value is set to 1, or the value is set to 0 and the header of the SIP NOTIFY message contains an additional string "reboot=true", the base station will reboot immediately.

The NOTIFY message is formed as shown:

```
NOTIFY sip:<user>@<dsthost> SIP/2.0

To: sip:<user>@<dsthost>

From: sip:sipsak@<srchost>

CSeq: 10 NOTIFY

Call-ID: 1234@<srchost>

Event: check-sync;reboot=true
```

Procedure

Changes can only be configured using the configuration file.

Configuration File	y000000000077.cfg	Configure the DECT IP phone behavior when receiving a SIP NOTIFY message which contains

		the header "Event: check-sync". **Parameter:** sip.notify_reboot_enable

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sip.notify_reboot_enable	**0, 1 or 2**	**1**
Description: Configure the DECT IP phone behavior when receiving a SIP NOTIFY message which contains the header "Event: check-sync". **0**-The base station will reboot only if the SIP NOTIFY message contains an additional string "reboot=true". **1**-The base station will be forced to reboot. **2**-The base station will ignore the SIP NOTIFY message. **Web User Interface:** None **Handset User Interface:** None		

Register Issue

Why cannot the handset be registered to the base station?

If the network works normally, you can check the compatibility between base station and handset. There are 2 sets of base stations, complied with the FCC and CE standard respectively. You can check it from the back of the base station. There are also 2 sets of handsets, American and Europe area respectively.

The American area handset is compatible with FCC standard base station.

The Europe area handset is compatible with CE standard base station.

Display Issue

Why does the handset prompt the message "Not Subscribed"?

Check the registration status of your handset. If your handset is not registered to the base station, register it manually.

Why does the handset prompt the message “Not in Range” or “Out Of Range”?

- Ensure that the base station is properly plugged into a functional AC outlet.
- Ensure that the handset is not too far from the base station.

Why does the handset prompt the message “Network unavailable”?

- Ensure that the Ethernet cable is plugged into the Internet port on the base station and the Ethernet cable is not loose.
- Ensure that the switch or hub in your network is operational.

Why does the Handset display “No Service”?

The LCD screen prompts “No Service” message when there is no available SIP account on the DECT IP phone.

Do one of the following:

- Ensure that an account is actively registered on the handset at the path **OK**->**Status**->**Line Status**.
- Ensure that the SIP account parameters have been configured correctly.

Upgrade Issue

Why doesn’t the DECT IP phone upgrade firmware successfully?

Do one of the following:

- Ensure that the target firmware version is not the same as the current one.
- Ensure that the target firmware is applicable to the DECT IP phone model.
- Ensure that the current or the target firmware is not protected.
- Ensure that the power is on and the network is available in the process of upgrading.
- Ensure that the web browser is not closed or refreshed when upgrading firmware via web user interface.
- For handset, ensure the handset battery should not less than 40% and is connected to the base station.

Time and Date Issue

Why doesn’t the handset display time and date correctly?

Check if the DECT 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.

Audio Issue

How to increase or decrease the volume?

Press ◀ or ▶ on the handset to increase or decrease the ringer volume when the handset is idle, or to adjust the volume of engaged audio device (earpiece, speakerphone or earphone) when there is an active call in progress.

Why do I get poor sound quality during a call?

If you have poor sound quality/acoustics like intermittent voice, low volume, echo or other noises, the possible reasons could be:

- Users are seated too far out of recommended microphone range and sound faint, or are seated too close to sensitive microphones and cause echo.
- Intermittent voice is mainly caused by packet loss, due to network congestion, and jitter, due to message recombination of transmission or receiving equipment (e.g., timeout handling, retransmission mechanism, buffer under run).
- Noisy equipment, such as a computer or a fan, may cause voice interference. Turn off any noisy equipment.
- Line issues can also cause this problem; disconnect the old line and redial the call to ensure another line may provide better connection.
- The handset is too far from the base station, please move closer and try again.

Why does the DECT IP phone play the local ringback tone instead of media when placing a long distance number without plus 0?

Ensure that the 180 ring workaround feature is disabled. For more information, refer to 180 Ring Workaround on page 236.

Why is there no sound when the other party picks up the call?

If the caller and receiver cannot hear anything - there is no sound at all when the other party picks up the call, the possible reason could be: the phone cannot send the real-time transport protocol (RTP) streams, in which audio data is transmitted, to the connected call.

Try to disable the 180 ring workaround feature. For more information, refer to 180 Ring Workaround on page 236.

Phone Book Issues

What is the difference between a remote phone book and a local phone book?

A remote phonebook is placed on a server, while a local phonebook is placed on the DECT IP phone flash. A remote phonebook can be used by everyone that can access the server, while a local phonebook can only be used by a specific phone. A remote phonebook is always used as a central phonebook for a company; each employee can load it to obtain the real-time data from the same server.

Provisioning Issues

What is auto provisioning?

Auto provisioning refers to the update of DECT IP phones, including update on configuration parameters, local phonebook, firmware and so on. You can use auto provisioning on a single phone, but it makes more sense in mass deployment.

What is PnP?

Plug and Play (PnP) is a method for DECT IP phones to acquire the provisioning server address. With PnP enabled, the DECT IP phone broadcasts the PnP SUBSCRIBE message to obtain a provisioning server address during startup. Any SIP server recognizing the message will respond with the preconfigured provisioning server address, so the DECT IP phone will be able to download the CFG files from the provisioning server. PnP depends on support from a SIP server.

Why doesn’t the DECT IP phone update the configuration?

Do one of the following:

- Ensure that the configuration is set correctly.
- Reboot the base station. Some configurations require a reboot to take effect.
- Ensure that the configuration is applicable to the DECT IP phone model.
- The configuration may depend on support from a server.

Password Issues

How to restore the administrator password?

Factory reset can restore the original password. All custom settings will be overwritten after reset.

System Log Issue

Why can't I export the system log to a provisioning server (FTP/TFTP server)?

Do one of the following:

- Ensure that the FTP/TFTP server is downloaded and installed on your local system.
- Ensure that you have configured the FTP/TFTP server address correctly via web user interface on your DECT IP phone.
- Reboot the base station. The configurations require a reboot to take effect.

Why can't I export the system log to a syslog server?

Do one of the following:

- Ensure that the syslog server supports saving the syslog files exported from DECT IP phone.
- Ensure that you have configured the syslog server address correctly via web user interface on your DECT IP phone.
- Reboot the base station. The configurations require a reboot to take effect.

Hardware Issue

Why is the sending/receiving volume of the headset or handset too low?

Ensure that the headset or handset is not damaged. If the headset or handset is usable, it may be the codec problem on the mainboard.

Why is there no response when pressing the keys on the keypad?

Do one of the following:

- Ensure that the keypad cables is properly connected and not damaged.
- Check if the keypad surface is clean.

Resetting Issues

Generally, some common issues may occur while using the DECT IP phone. You can reset your phone to factory configurations after you have tried all troubleshooting suggestions but do not solve the problem. Resetting the phone to factory configurations clears the flash parameters, removes log files, user data, and cached data, and resets the administrator password to admin. All custom settings will be overwritten after resetting.

Five ways to reset the phone:

- **Reset local settings**: All configurations saved in the <MAC>-local.cfg file on the DECT IP phone will be reset. Changes associated with non-static settings made via web user interface and handset user interface are saved in the <MAC>-local.cfg file.
- **Reset non-static settings**: All non-static settings on the phone will be reset. After resetting the non-static settings, the DECT IP phone will perform the auto provisioning process immediately.
- **Reset static settings**: All static settings on the phone will be reset.
- **Reset userdata & local config**: All the local cache data (e.g., userdata, history, directory) will be cleared. And all configurations saved in the <MAC>-local.cfg configuration file on the DECT IP phone will be reset.
- **Reset to factory**: All configurations on the phone will be reset.

You can reset the DECT IP phone to default factory configurations. The default factory configurations are the settings that reside on the DECT IP phone after it has left the factory. You can also reset the DECT 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.

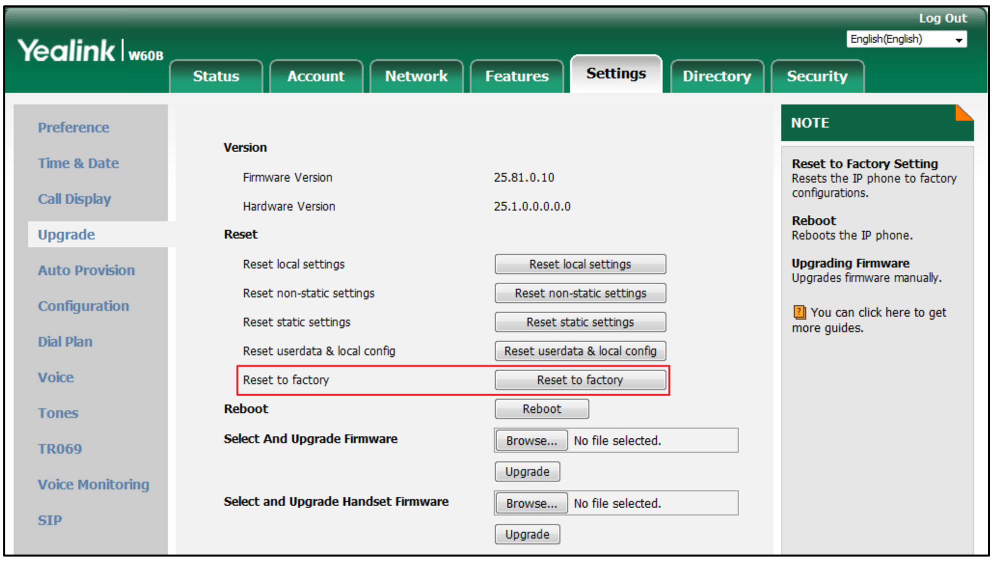
Note

The **Reset local settings/Reset non-static settings/Reset static settings/Reset userdata & local config** option on the web user interface appears only if the value of the parameter "static.auto_provision.custom.protect" is set to 1.

How to reset the DECT IP phone to default factory configurations?

To reset the DECT IP phone via web user interface:

1. Click on **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 DECT IP phone will be reset to factory sucessfully after startup.

Note Reset of your phone may take a few minutes. Do not power off until the phone starts up successfully.

How to reset the DECT IP phone to custom factory configurations?

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the Custom Factory Configuration feature. **Parameter:** static.features.custom_factory_config.enable
		Configure the access URL of the custom factory configuration files. **Parameter:** static.custom_factory_configuration.url
Web User Interface		Configure the access URL of the custom factory configuration files. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-config&q=load

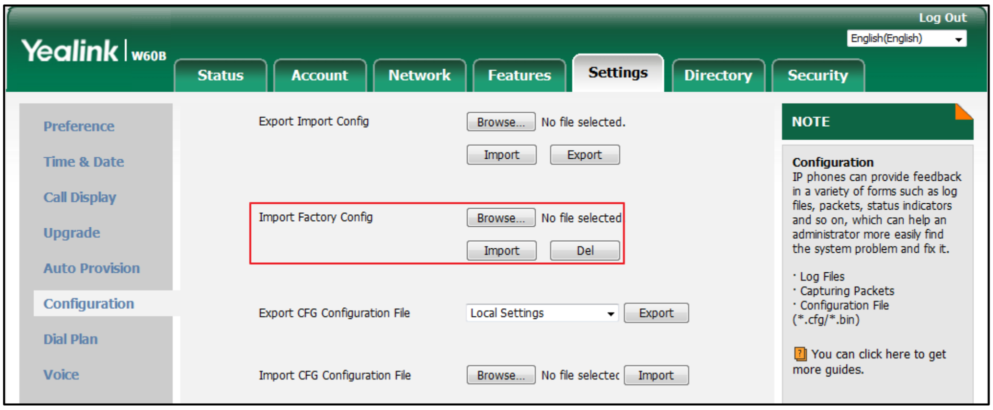
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.features.custom_factory_config.enable	**0 or 1**	**0**
Description: Enables or disables the Custom Factory Configuration feature. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), **Import Factory Config** item will be displayed on the DECT IP phone's web user interface at the path **Settings**->**Configuration**. You can import a custom factory configuration file or delete the user-defined factory configuration via web user interface. **Web User Interface:**		

Parameters	Permitted Values	Default
None **Handset User Interface:** None		
static.custom_factory_configuration.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom factory configuration files. **Note**: It works only if the value of the parameter "static.features.custom_factory_config.enable" is set to 1 (Enabled) and the file format of custom factory configuration file must be *.bin. If you change this parameter, the DECT IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Configuration->Import Factory Config **Handset User Interface:** None		

To import the custom factory configuration files via web user interface:

1. Click on **Settings**->**Configuration**.
2. Click **Browse** to locate the custom factory configuration file from your local system.



3. Click **Import**.

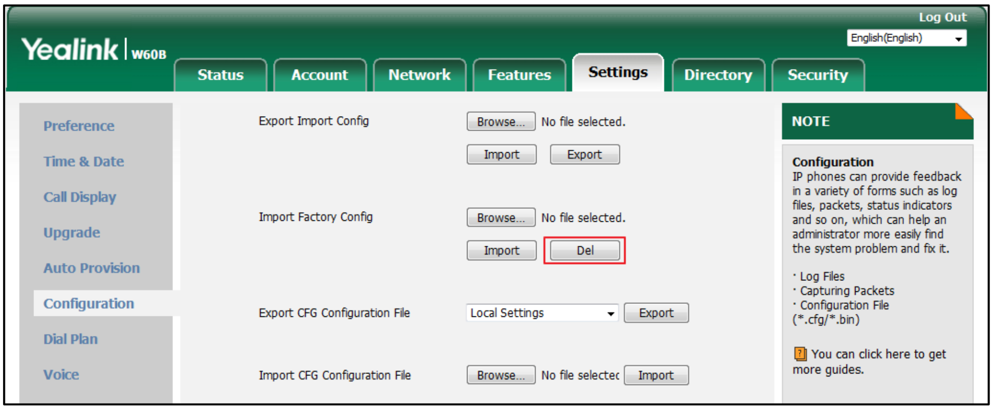
When the custom factory configuration file is imported successfully, you can reset the DECT IP phone to custom factory configurations. For more information on how to reset to factory configuration via web user interface, refer to How to reset the DECT IP phone to default factory configurations? on page 455.

You can delete the user-defined factory configurations via web user interface.

To delete the custom factory configuration files via web user interface:

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

2. Click **Del** in the **Import Factory Configuration** field.



The web user interface prompts the message "Are you sure delete user-defined factory configuration?".

3. Click **OK** to delete the custom factory configuration files.

   The imported custom factory file will be deleted. The DECT IP phone will be reset to default factory configurations after resetting.

Rebooting Issues

How to reboot the DECT IP phone remotely?

DECT IP phones support remote reboot by a SIP NOTIFY message with "Event: check-sync" header. Whether the DECT IP phone reboots or not depends on the value of the parameter "sip.notify_reboot_enable". If the value is set to 1, or the value is set to 0 and the header of the SIP NOTIFY message contains an additional string "reboot=true", the DECT IP phone will reboot immediately.

The NOTIFY message is formed as shown:

```
NOTIFY sip:<user>@<dsthost> SIP/2.0

To: sip:<user>@<dsthost>

From: sip:sipsak@<srchost>

CSeq: 10 NOTIFY

Call-ID: 1234@<srchost>

Event: check-sync;reboot=true
```

Procedure

Changes can only be configured using the configuration files.

Central Provisioning (Configuration File)	y000000000077.cfg	Configure the DECT IP phone behavior when receiving a SIP NOTIFY message which contains

		the header "Event: check-sync". **Parameter:** sip.notify_reboot_enable

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sip.notify_reboot_enable	**0, 1 or 2**	**1**
Description: Configure the DECT IP phone behavior when receiving a SIP NOTIFY message which contains the header "Event: check-sync". **0**-The DECT IP phone will reboot only if the SIP NOTIFY message contains an additional string "reboot=true". **1**-The DECT IP phone will be forced to reboot. **2**-The DECT IP phone will ignore the SIP NOTIFY message. **Web User Interface:** None **Handset User Interface:** None		

How to reboot the DECT IP phone via web/handset user interface?

You can reboot your DECT IP phone via web/handset user interface.

To reboot the phone via handset user interface:

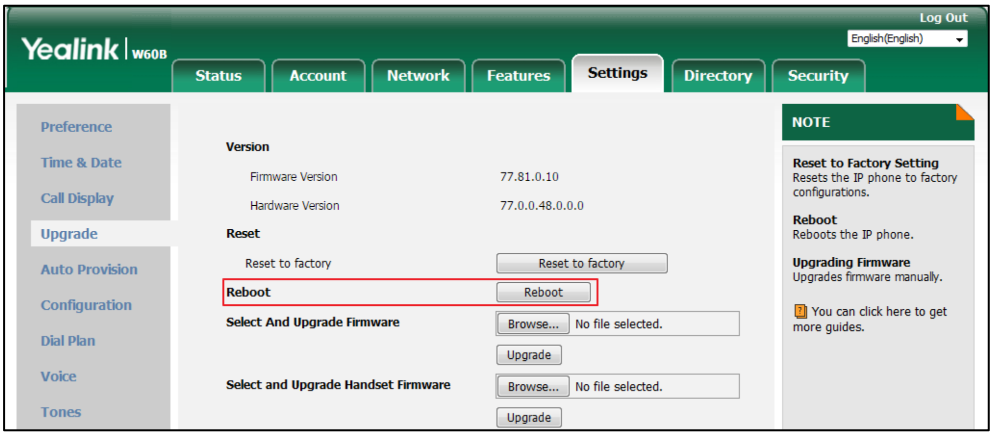
1. Press **OK**->**Settings**->**System Settings**->**Base Restart** (default PIN: 0000).
2. Press the **OK** soft key to reboot the base.

   The phone begins rebooting. Any reboot of the phone may take a few minutes.

To reboot the phone via web user interface:

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

2. Click **Reboot** to reboot the DECT IP phone.



The phone begins rebooting. Any reboot of the phone may take a few minutes.

Protocols and Ports Issues

What communication protocols and ports do Yealink DECT IP phones support?

Source Device	Source IP	Source Port	Destination Device	Destination IP	Destination Port (Listening port)	Protocol	Description of destination port
DECT IP phones	IP address of DECT IP phones	2~65535	DECT IP phone or voice gateway	IP address of DECT IP phone or voice gateway	Determined by destination device.	UDP	RTP protocol port, it is used to send or receive audio stream.
		1024~65535	SIP Server	IP address of SIP server	Determined by destination device.	UDP/TCP	SIP protocol port, it is used for signaling interaction with SIP server.
		1024~65535	TR-069 Server	IP address of TR-069 server	Determined by destination device.	TCP	TR-069 protocol port, it is used to communicate with TR-069server.
		1024~65535	File server	IP address of file server	Determined by destination device.	TCP	HTTP protocol port, it is used to download file.
		1024~65535	Remote phone book server	IP address of remote phone book server	Determined by destination device.	TCP	HTTP protocol port, it is used to access the remote phone book.
		1024~65535	AA	IP address of AA	Determined by destination device.	TCP	HTTP protocol port, it is used for AA communication.
		68	DHCP Server	IP address of DHCP server	67	UDP	DHCP protocol port, it is used to obtain IP address from DHCP server.

Source Device	Source IP	Source Port	Destination Device	Destination IP	Destination Port (Listening port)	Protocol	Description of destination port
		1024~65535	LDAP Server	IP address of LDAP server	Determined by destination device.	TCP	LDAP protocol port, it is used to obtain the contact information from LDAP server.
		1024~65535	NTP Server	IP address of NTP server	123	UDP	NTP protocol port, it is used to synchronize time from NTP time server.
		1024~65535	Syslog Server	IP address of syslog server	514	UDP	Syslog protocol port, it is used for DECT IP phones to upload syslog information to syslog server.
		1024~65535	PNP Server	IP address of PNP server (Default value: 224.0.1.75)	5059	UDP/TCP	Protocol port, it is used to obtain the URL of updating file from PNP server.
			Multipaging	Multipaging	65000 65001		
PC	IP address of PC				1~65535	TCP	HTTP port (default value: 80)
					1~65535	TCP	HTTP port (default value: 443)
SIP Server	IP address of SIP Server				1024~65534	UDP/TCP	SIP protocol port, it is used for signaling interaction with SIP server.
DECT IP phone of voice	IP address of DECT IP phone or	Determined by the destination	DECT IP phones	IP address of DECT IP phones	2~65535	UDP	RTP protocol port, it is used by destination device to send or receive audio stream.

Source Device	Source IP	Source Port	Destination Device	Destination IP	Destination Port (Listening port)	Protocol	Description of destination port
gateway	voice gateway	device.					
TR-069 Server	IP address of TR-069 Server				1024~65535	TCP	TR-069 protocol port, it is used to communicate with TR-069server.

Other Issues

How to recognize the area of handset?

To recognize the area of handset via handset user interface:

1. Press **OK** to enter the main menu.
2. Select **Settings**->**Handset**.

   The LCD screen displays status information of handset status, you can press ▲ or to scroll ▼ through to the **Area** field.

What is the difference among user name, register name and display name?

Both user name and register name are defined by the server. User name identifies the account, while register name matched with a password is for authentication purposes. Display name is the caller ID that will be displayed on the callee's phone LCD screen. Server configurations may override the local ones.

What do "on code" and "off code" mean?

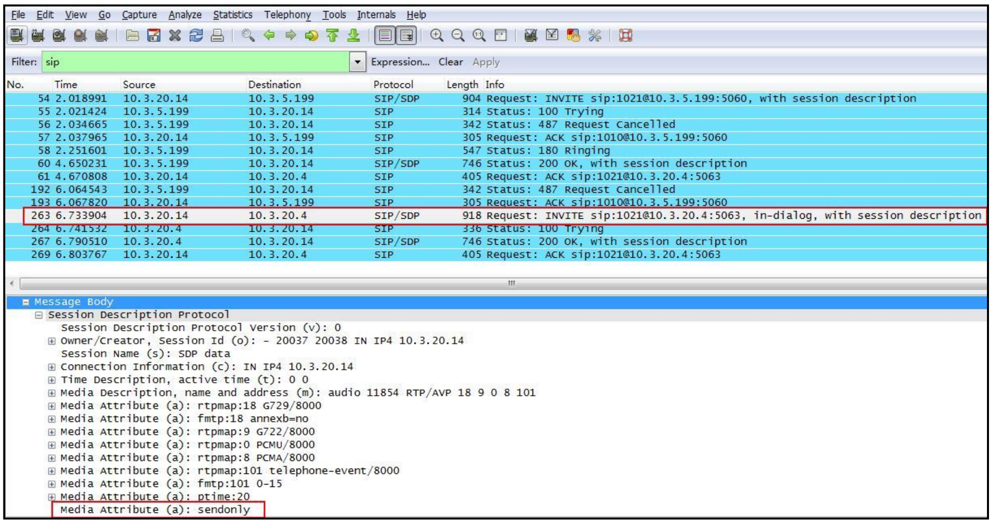
They are codes that the DECT IP phone sends to the server when a certain action takes place. On code is used to activate a feature on the server side, while off code is used to deactivate a feature on the server side.

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 DECT IP phone, the DECT IP phone sends *78201 to the server, and then the server will enable Always Forward feature on the server side, hence being able to get the right status of the extension.

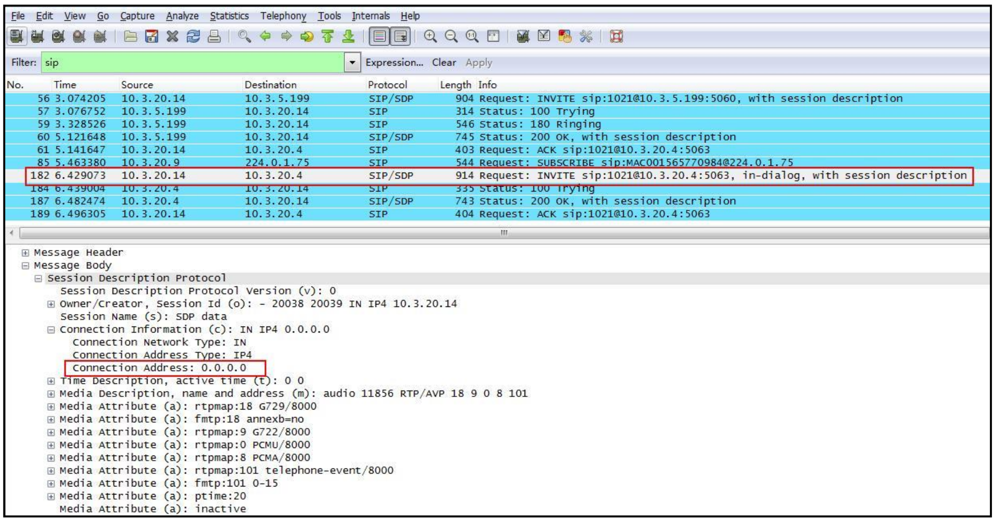
For anonymous call/anonymous call rejection feature, the phone will send either the on code or off code to the server according to the value of Send Anonymous Code/Send Rejection Code. For more information, refer to Anonymous Call on page 223 and Anonymous Call Rejection on page 226.

What is the difference between enabling and disabling the RFC 2543 Hold feature?

Capturing packets after you enable the RFC 2543 Hold feature. SDP media direction attributes (such as a=sendonly) per RFC 2543 is used in the INVITE message when placing a call on hold.



Capturing packets after you disable the RFC 2543 Hold feature. SDP media connection address c=0.0.0.0 per RFC 3264 is used in the INVITE message when placing a call on hold.



For more information on RFC 2543 hold feature, refer to Call Hold on page 243. For more information on capturing packets, refer to Capturing Packets on page 439.

Appendix

Appendix A: Glossary

802.1x--an IEEE Standard for port-based Network Access Control (PNAC). It is a part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

ACS (Auto Configuration server)**--**responsible for auto-configuration of the Central Processing Element (CPE).

Cryptographic Key--a piece of variable data that is fed as input into a cryptographic algorithm to perform operations such as encryption and decryption, or signing and verification.

DHCP (Dynamic Host Configuration Protocol)**--**built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.

DHCP Option--can be configured for specific values and enabled for assignment and distribution to DHCP clients based on server, scope, class or client-specific levels.

DNS (Domain Name System)**--**a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network.

EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5)**--**only provides authentication of the EAP peer to the EAP server but not mutual authentication.

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) **–**provides for mutual authentication, integrity-protected cipher suite negotiation between two endpoints.

PEAP-MSCHAPv2 (Protected Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol version 2) **–**provides for mutual authentication, but does not require a client certificate on the DECT IP phone.

FAC (Feature Access Code)**--**special patterns of characters that are dialed from a phone keypad to invoke particular features.

HTTP (Hypertext Transfer Protocol)**--**used to request and transmit data on the World Wide Web.

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)**--**a widely-used communications protocol for secure communication over a network.

IEEE (Institute of Electrical and Electronics Engineers)**--**a non-profit professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence.

LAN (Local Area Network)**--**used to interconnects network devices in a limited area such as a home, school, computer laboratory, or office building.

MIB (Management Information Base)**--**a virtual database used for managing the entities in a communications network.

OID (Object Identifier)**--**assigned to an individual object within a MIB.

PnP (Plug and Play)**--**a term used to describe the characteristic of a computer bus, or device specification, which facilitates the discovery of a hardware component in a system, without the need for physical device configuration, or user intervention in resolving resource conflicts.

ROM (Read-only Memory)**--**a class of storage medium used in computers and other electronic devices.

RTP (Real-time Transport Protocol)**--**provides end-to-end service for real-time data.

TCP (Transmission Control Protocol)**--**a transport layer protocol used by applications that require guaranteed delivery.

UDP (User Datagram Protocol)--a protocol offers non-guaranteed datagram delivery.

URI (Uniform Resource Identifier)**--**a compact sequence of characters that identifies an abstract or physical resource.

URL (Uniform Resource Locator)--specifies the address of an Internet resource.

VLAN (Virtual LAN)**--** a group of hosts with a common set of requirements, which communicate as if they were attached to the same broadcast domain, regardless of their physical location.

VoIP (Voice over Internet Protocol)**--**a family of technologies used for the delivery of voice communications and multimedia sessions over IP networks.

WLAN (Wireless Local Area Network)**--**a type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes.

XML-RPC (Remote Procedure Call Protocol)**--**which uses XML to encode its calls and HTTP as a transport mechanism.

Appendix B: Time Zones

Time Zone	Time Zone Name
-11	Samoa
-10	United States-Hawaii-Aleutian, United States-Alaska-Aleutian
-9:30	French Polynesia
-9	United States-Alaska Time
-8	Canada(Vancouver,Whitehorse), Mexico(Tijuana,Mexicali), United States-Pacific Time
-7	Canada(Edmonton,Calgary), Mexico(Mazatlan,Chihuahua), United States-MST no DST, United States-Mountain Time
-6	Canada-Manitoba(Winnipeg), Chile(Easter Islands), Mexico(Mexico City,Acapulco), United States-Central Time
-5	Bahamas(Nassau), Canada(Montreal,Ottawa,Quebec), Cuba(Havana), United States-Eastern Time
-4:30	Venezuela(Caracas)
-4	Canada(Halifax,Saint John), Chile(Santiago), Paraguay(Asuncion), United Kingdom-Bermuda(Bermuda), United Kingdom(Falkland Islands), Trinidad&Tobago
-3:30	Canada-New Foundland(St.Johns)
-3	Argentina(Buenos Aires), Brazil(DST), Brazil(no DST), Denmark-Greenland(Nuuk)
-2:30	Newfoundland and Labrador
-2	Brazil(no DST)
-1	Portugal(Azores)
0	Denmark-Faroe Islands(Torshavn), GMT, Greenland, Ireland(Dublin), Morocco, Portugal(Lisboa,Porto,Funchal), Spain-Canary Islands(Las Palmas), United Kingdom(London)
+1	Albania(Tirane), Austria(Vienna), Belgium(Brussels), Caicos, Chad, Croatia(Zagreb), Czech Republic(Prague), Denmark(Kopenhagen), France(Paris), Germany(Berlin), Hungary(Budapest), Italy(Rome), Luxembourg(Luxembourg), Macedonia(Skopje), Namibia(Windhoek), Netherlands(Amsterdam), Spain(Madrid)
+2	Estonia(Tallinn), Finland(Helsinki), Gaza Strip(Gaza), Greece(Athens), Israel(Tel Aviv), Jordan(Amman), Latvia(Riga), Lebanon(Beirut), Moldova(Kishinev), Romania(Bucharest), Russia(Kaliningrad), Syria(Damascus), Turkey(Ankara), Ukraine(Kyiv, Odessa)
+3	East Africa Time, Iraq(Baghdad), Russia(Moscow)
+3:30	Iran(Teheran)
+4	Armenia(Yerevan), Azerbaijan(Baku), Georgia(Tbilisi), Kazakhstan(Aktau), Russia(Samara)
+4:30	Afghanistan(Kabul)

Time Zone	Time Zone Name
+5	Kazakhstan(Aqtobe), Kyrgyzstan(Bishkek), Pakistan(Islamabad), Russia(Chelyabinsk)
+5:30	India(Calcutta)
+5:45	Nepal(Katmandu)
+6	Kazakhstan(Astana, Almaty), Russia(Novosibirsk,Omsk)
+6:30	Myanmar(Naypyitaw)
+7	Russia(Krasnoyarsk), Thailand(Bangkok)
+8	Australia(Perth), China(Beijing), Russia(Irkutsk, Ulan-Ude), Singapore(Singapore)
+8:45	Eucla
+9	Japan(Tokyo), Korea(Seoul), Russia(Yakutsk,Chita)
+9:30	Australia(Adelaide), Australia(Darwin)
+10	Australia(Brisbane), Australia(Hobart), Australia(Sydney,Melboume,Canberra), Russia(Vladivostok)
+10:30	Australia(Lord Howe Islands)
+11	New Caledonia(Noumea), Russia(Srednekolymsk Time)
+11:30	Norfolk Island
+12	New Zealand(Wellington,Auckland), Russia(Kamchatka Time)
+12:45	New Zealand(Chatham Islands)
+13	Tonga(Nukualofa)
+13:30	Chatham Islands
+14	Kiribati

Appendix C: Trusted Certificates

Yealink DECT IP phones trust the following CAs by default:

- DigiCert High Assurance EV Root CA
- Deutsche Telekom Root CA 2
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure Global eBusiness CA-1
- GeoTrust Global CA
- GeoTrust Global CA2
- GeoTrust Primary Certification Authority
- GeoTrust Primary Certification Authority G2
- GeoTrust Universal CA
- GeoTrust Universal CA2
- Thawte Personal Freemail CA

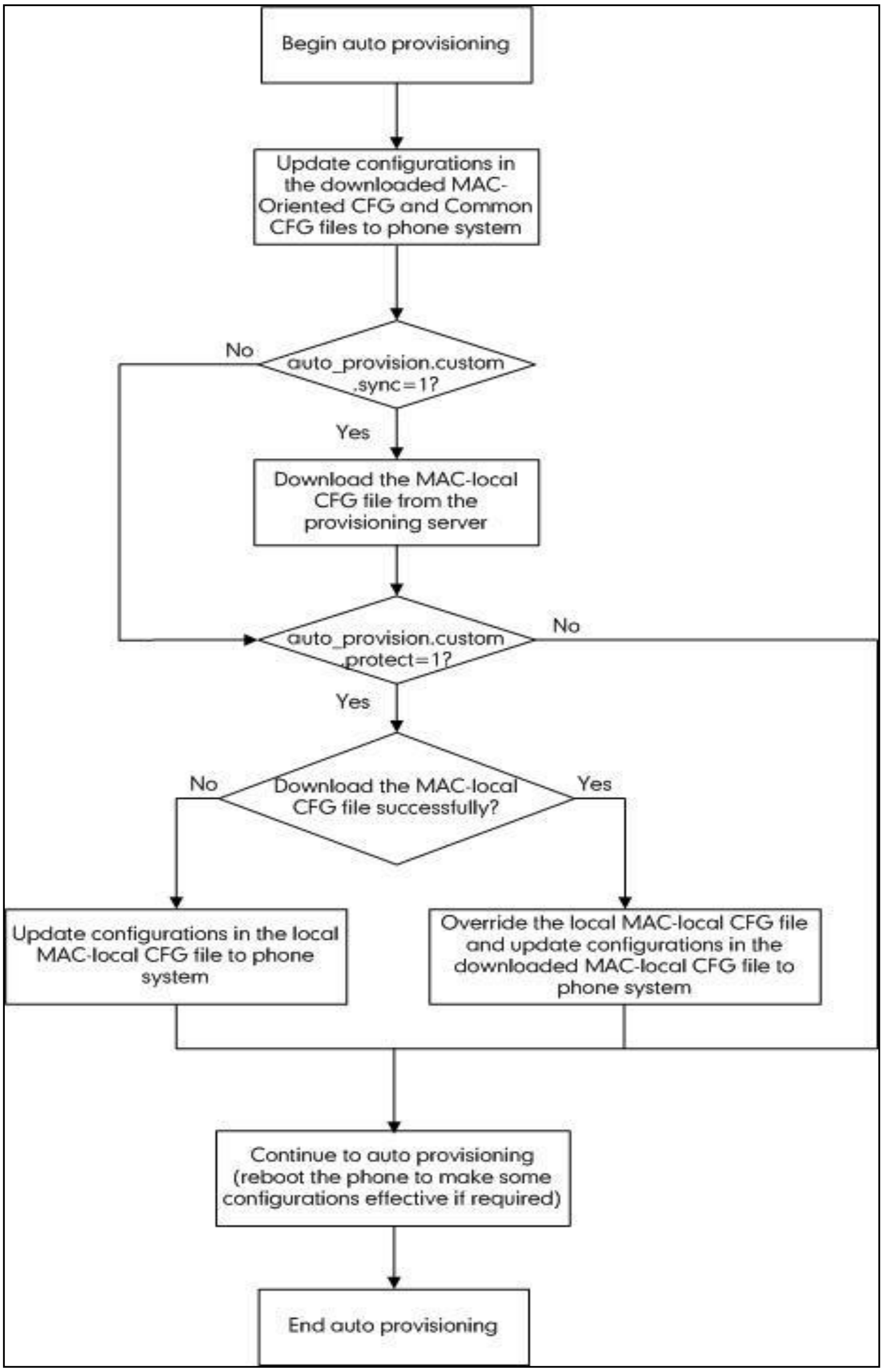
- Thawte Premium Server CA
- Thawte Primary Root CA
- Thawte Primary Root CA - G2
- Thawte Primary Root CA - G3
- Thawte Server CA
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Universal Root Certification Authority
- ISRG Root X1 (Let's Encrypt Authority X1 and Let's Encrypt Authority X2 certificates are signed by the root certificate ISRG Root X1.)
- Baltimore CyberTrust Root
- DST Root CA X3
- Verizon Public SureServer CA G14-SHA2
- AddTrust External CA Root
- Go Daddy Class 2 Certification Authority
- Class 2 Primary CA
- Cybertrust Public SureServer SV CA
- DigiCert Assured ID Root G2
- DigiCert Assured ID Root G3
- DigiCert Assured ID Root CA
- DigiCert Global Root G2
- DigiCert Global Root G3
- DigiCert Global Root CA
- DigiCert Trusted Root G4
- Entrust Root Certification Authority

- Entrust Root Certification Authority - G2
- Entrust.net Certification Authority (2048)
- GeoTrust Primary Certification Authority - G3
- GlobalSign Root CA
- GlobalSign Root CA - R2
- Starfield Root Certificate Authority - G2
- TC TrustCenter Class 2 CA II
- TC TrustCenter Class 3 CA II
- TC TrustCenter Class 4 CA II
- TC TrustCenter Universal CA I
- TC TrustCenter Universal CA III
- Thawte Universal CA Root
- VeriSign Class 3 Secure Server CA - G2
- VeriSign Class 3 Secure Server CA – G3
- Thawte SSL CA
- StartCom Certification Authority
- StartCom Certification Authority G2
- Starfield Services Root Certificate Authority - G2
- RapidSSL CA
- Go Daddy Root Certificate Authority - G2
- Cybertrust Global Root
- COMODOSSLCA
- COMODO RSA Domain Validation Secure Server CA
- COMODO RSA Certification Authority
- AmazonRootCA4
- AmazonRootCA3
- AmazonRootCA2
- AmazonRootCA1
- Yealink Root CA
- Yealink Equipment Issuing CA

Note Yealink endeavors to maintain a built-in list of most common used CA Certificates. Due to memory constraints, we cannot ensure a complete set of certificates. If you are using a certificate from a commercial Certificate Authority not in the list above, you can send a request to your local distributor. At this point, you can upload your particular CA certificate into your phone. For more information on uploading custom CA certificate, refer to Transport Layer Security (TLS) on page 403.

Appendix D: Auto Provisioning Flowchart (Keep User Personalized Configuration Settings)

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



Appendix E: Static Settings

You may need to know the differences between the parameters started with "static." and other common parameters:

- All static settings have no priority. They take effect no matter what method (web user interface or handset user interface or configuration files) you are using for provisioning.
- All static settings are never be saved to <MAC>-local.cfg file.
- All static settings are not affected by the overwrite mode. That is, the actual values will not be changed even if you delete the parameters associated with static settings, or you clear the values of the parameters associated with static settings in the configuration files.

The following table lists all static settings:

Function	Parameter
Network	static.network.attempt_expired_time
	static.network.dhcp_host_name
	static.network.static_dns_enable
	static.network.ipv6_static_dns_enable
	static.network.dns.ttl_enable
	static.network.dhcp.server_mac1
	static.network.dhcp.server_mac2
	static.network.mtu_value
	static.network.dhcp.option60type
	static.network.vlan.internet_port_enable
	static.network.vlan.internet_port_vid
	static.network.vlan.internet_port_priority
	static.network.vlan.dhcp_enable
	static.network.vlan.dhcp_option
	static.network.vlan.vlan_change.enable
	static.network.port.http
	static.network.port.https
	static.network.qos.audiotos
	static.network.qos.signaltos
	static.network.802_1x.mode
	static.network.802_1x.anonymous_identity

Function	Parameter
	static.network.802_1x.eap_fast_provision_mode
	static.network.802_1x.identity
	static.network.802_1x.md5_password
	static.network.802_1x.root_cert_url
	static.network.802_1x.client_cert_url
	static.network.vpn_enable
	static.openvpn.url
	static.network.lldp.enable
	static.network.lldp.packet_interval
	static.network.port.max_rtpport
	static.network.port.min_rtpport
	static.network.ip_address_mode
	static.network.ipv6_prefix
	static.network.ipv6_internet_port.type
	static.network.ipv6_internet_port.ip
	static.network.ipv6_internet_port.gateway
	static.network.ipv6_primary_dns
	static.network.ipv6_secondary_dns
	static.network.internet_port.type
	static.network.internet_port.ip
	static.network.internet_port.mask
	static.network.internet_port.gateway
	static.network.primary_dns
	static.network.secondary_dns
Security	static.security.trust_certificates
	static.security.user_name.user
	static.security.user_name.admin
	static.security.user_name.var
	static.security.user_password
	static.phone_setting.reserve_certs_enable
	static.security.ca_cert

Function	Parameter
	static.security.dev_cert
	static.security.cn_validation
Certificates	static.trusted_certificates.url
	static.trusted_certificates.delete
	static.server_certificates.url
	static.server_certificates.delete
3-level Permissions	static.web_item_level.url
	static.security.var_enable
	static.security.default_access_level
WEB HTTP(S)	static.wui.https_enable
	static.wui.http_enable
Lang	static.lang.wui
Log	static.local_log.enable
	static.local_log.level
	static.local_log.max_file_size
	static.syslog.enable
	static.syslog.level
	static.syslog.server
	static.syslog.server_port
	static.syslog.transport_type
	static.syslog.prepend_mac_address.enable
	static.syslog.facility
	static.auto_provision.local_log.backup.enable
	static.auto_provision.local_log.backup.path
	static.auto_provision.local_log.backup.upload_period
	static.auto_provision.local_log.backup.append
	static.auto_provision.local_log.backup.append.limit_mode
	static.auto_provision.local_log.backup.append.max_file_size
	static.auto_provision.local_log.backup.bootlog.upload_wait_time
Autoprovision	static.auto_provision.power_on
	static.auto_provision.weekly_upgrade_interval

Function	Parameter
	static.auto_provision.inactivity_time_expire
	static.auto_provision.custom.sync
	static.auto_provision.custom.sync.path
	static.auto_provision.custom.protect
	static.auto_provision.custom.upload_method
	static.auto_provision.attempt_expired_time
	static.auto_provision.reboot_force.enable
	static.auto_provision.pnp_enable
	static.auto_provision.dhcp_option.enable
	static.auto_provision.dhcp_option.list_user_options
	static.auto_provision.dhcp_option.option60_value
	static.auto_provision.repeat.enable
	static.auto_provision.repeat.minutes
	static.auto_provision.server.type
	static.auto_provision.weekly.enable
	static.auto_provision.weekly.dayofweek
	static.auto_provision.weekly.begin_time
	static.auto_provision.weekly.end_time
	static.auto_provision.flexible.enable
	static.auto_provision.flexible.interval
	static.auto_provision.flexible.begin_time
	static.auto_provision.flexible.end_time
	static.auto_provision.user_agent_mac.enable
	static.auto_provision.server.url
	static.auto_provision.server.username
	static.auto_provision.server.password
	static.auto_provision.update_file_mode
	static.auto_provision.aes_key_in_file
	static.auto_provision.aes_key_16.com
	static.auto_provision.aes_key_16.mac
	static.auto_provision.encryption.config

Function	Parameter
	static.autoprovision.X.name
	static.autoprovision.X.code
	static.autoprovision.X.url
	static.autoprovision.X.user
	static.autoprovision.X.password
	static.autoprovision.X.com_aes
	static.autoprovision.X.mac_aes
	static.auto_provision.url_wildcard.pn
	static.auto_provision.attempt_before_failed
	static.auto_provision.retry_delay_after_file_transfer_failed
	static.auto_provision.dns_resolv_nosys
	static.auto_provision.dns_resolv_nretry
	static.auto_provision.dns_resolv_timeout
TR069	static.managementserver.enable
	static.managementserver.username
	static.managementserver.password
	static.managementserver.url
	static.managementserver.connection_request_username
	static.managementserver.connection_request_password
	static.managementserver.periodic_inform_enable
	static.managementserver.periodic_inform_interval
Watch Dog	static.watch_dog.enable
Custom Configuration	static.custom_mac_cfg.url
	static.configuration.url
Custom Factory Configuration	static.features.custom_factory_config.enable
	static.custom_factory_configuration.url
Other	static.firmware.url

Appendix F: SIP (Session Initiation Protocol)

This section describes how Yealink DECT IP phones comply with the IETF definition of SIP as described in RFC 3261.

This section contains compliance information in the following:

- RFC and Internet Draft Support
- SIP Request
- SIP Header
- SIP Responses
- SIP Session Description Protocol (SDP) Usage

RFC and Internet Draft Support

The following RFC's and Internet drafts are supported:

- RFC 1321—The MD5 Message-Digest Algorithm
- RFC 1889—RTP Media control
- RFC 2112—Multipart MIME
- RFC 2327—SDP: Session Description Protocol
- RFC 2387—The MIME Multipart/Related Content-type
- RFC 2543—SIP: Session Initiation Protocol
- RFC 2617—Http Authentication: Basic and Digest access authentication
- RFC 2782—A DNS RR for specifying the location of services (DNS SRV)
- RFC 2806—URLs for Telephone Calls
- RFC 2833—RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 2915—The Naming Authority Pointer (NAPTR) DNS Resource Record
- RFC 2976—The SIP INFO Method
- RFC 3087—Control of Service Context using SIP Request-URI
- RFC 3261—SIP: Session Initiation Protocol (replacement for RFC 2543)
- RFC 3262—Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3263—Session Initiation Protocol (SIP): Locating SIP Servers
- RFC 3264—An Offer/Answer Model with the Session Description Protocol (SDP)
- RFC 3265—Session Initiation Protocol (SIP) - Specific Event Notification
- RFC 3266—Support for IPv6 in Session Description Protocol (SDP)
- RFC 3310—HTTP Digest Authentication Using Authentication and Key Agreement (AKA)

- RFC 3311–The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3312–Integration of Resource Management and SIP
- RFC 3313–Private SIP Extensions for Media Authorization
- RFC 3323–A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3324–Requirements for Network Asserted Identity
- RFC 3325–SIP Asserted Identity
- RFC 3326–The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3361–DHCP-for-IPv4 Option for SIP Servers
- RFC 3372–SIP for Telephones (SIP-T): Context and Architectures
- RFC 3398–ISUP to SIP Mapping
- RFC 3420–Internet Media Type message/sipfrag
- RFC 3428–Session Initiation Protocol (SIP) Extension for Instant Messaging
- RFC 3455–Private Header (P-Header) Extensions to the SIP for the 3GPP
- RFC 3486–Compressing the Session Initiation Protocol (SIP)
- RFC 3489–STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 3515–The Session Initiation Protocol (SIP) Refer Method
- RFC 3550–RTP: Transport Protocol for Real-Time Applications
- RFC 3555–MIME Type Registration of RTP Payload Formats
- RFC 3581–An Extension to the SIP for Symmetric Response Routing
- RFC 3608–SIP Extension Header Field for Service Route Discovery During Registration
- RFC 3611–RTP Control Protocol Extended Reports (RTCP XR)
- RFC 3665–Session Initiation Protocol (SIP) Basic Call Flow Examples
- RFC 3666–SIP Public Switched Telephone Network (PSTN) Call Flows.
- RFC 3680–SIP Event Package for Registrations
- RFC 3702–Authentication, Authorization, and Accounting Requirements for the SIP
- RFC 3711–The Secure Real-time Transport Protocol (SRTP)
- RFC 3725–Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)
- RFC 3842–A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
- RFC 3856–A Presence Event Package for Session Initiation Protocol (SIP)
- RFC 3863–Presence Information Data Format
- RFC 3890–A Transport Independent Bandwidth Modifier for the SDP
- RFC 3891–The Session Initiation Protocol (SIP) "Replaces" Header

- RFC 3892—The Session Initiation Protocol (SIP) Referred-By Mechanism
- RFC 3959—The Early Session Disposition Type for SIP
- RFC 3960—Early Media and Ringing Tone Generation in SIP
- RFC 3966—The tel URI for telephone number
- RFC 3968—IANA Registry for SIP Header Field
- RFC 3969—IANA Registry for SIP URI
- RFC 4028—Session Timers in the Session Initiation Protocol (SIP)
- RFC 4083—3GPP Release 5 Requirements on SIP
- RFC 4235—An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
- RFC 4244—An Extension to the SIP for Request History Information
- RFC 4317—Session Description Protocol (SDP) Offer/Answer Examples
- RFC 4353—A Framework for Conferencing with the SIP
- RFC 4458—SIP URIs for Applications such as Voicemail and Interactive Voice Response (IVR)
- RFC 4475—Session Initiation Protocol (SIP) Torture
- RFC 4485—Guidelines for Authors of Extensions to the SIP
- RFC 4504—SIP Telephony Device Requirements and Configuration
- RFC 4566—SDP: Session Description Protocol.
- RFC 4568—Session Description Protocol (SDP) Security Descriptions for Media Streams
- RFC 4575—A SIP Event Package for Conference State
- RFC 4579—SIP Call Control - Conferencing for User Agents
- RFC 4583—Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams
- RFC 4662—A SIP Event Notification Extension for Resource Lists
- RFC 4730—Event Package for KPML
- RFC 5009—P-Early-Media Header
- RFC 5079—Rejecting Anonymous Requests in SIP
- RFC 5359—Session Initiation Protocol Service Examples
- RFC 5589—Session Initiation Protocol (SIP) Call Control – Transfer
- RFC 5630—The Use of the SIPS URI Scheme in SIP
- RFC 5806—Diversion Indication in SIP
- RFC 5954—Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261
- RFC 6026—Correct Transaction Handling for 2xx Responses to SIP INVITE Requests
- RFC 6141—Re-INVITE and Target-Refresh Request Handling in SIP

- draft-ietf-sip-cc-transfer-05.txt–SIP Call Control - Transfer
- draft-anil-sipping-bla-02.txt–Implementing Bridged Line Appearances (BLA) Using Session Initiation Protocol (SIP)
- draft-anil-sipping-bla-03.txt–Implementing Bridged Line Appearances (BLA) Using Session Initiation Protocol (SIP)
- draft-ietf-sip-privacy-00.txt–SIP Extensions for Caller Identity and Privacy, November
- draft-ietf-sip-privacy-04.txt–SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks
- draft-levy -sip-diversion-08.txt–Diversion Indication in SIP
- draft-ietf-sipping-cc-conferencing-03.txt–SIP Call Control - Conferencing for User Agents
- draft-ietf-sipping-cc-conferencing-05.txt–Connection Reuse in the Session Initiation Protocol (SIP)
- draft-ietf-sipping-rtcp-summary-02.txt–Session Initiation Protocol Package for Voice Quality Reporting Event
- draft-ietf-sip-connect-reuse-06.txt–Connection Reuse in the Session Initiation Protocol (SIP)
- draft-ietf-bliss-shared-appearances-15.txt–Shared Appearances of a Session Initiation Protocol (SIP) Address of Record (AOR)

To find the applicable Request for Comments (RFC) document, go to http://www.ietf.org/rfc.html and enter the RFC number.

SIP Request

The following SIP request messages are supported:

Method	Supported	Notes
REGISTER	Yes	
INVITE	Yes	Yealink DECT IP phones support mid-call changes such as placing a call on hold as signaled by a new INVITE that contains an existing Call-ID.
ACK	Yes	
CANCEL	Yes	
BYE	Yes	
OPTIONS	Yes	

Method	Supported	Notes
SUBSCRIBE	Yes	
NOTIFY	Yes	
REFER	Yes	
PRACK	Yes	
INFO	Yes	
MESSAGE	Yes	
UPDATE	Yes	
PUBLISH	Yes	

SIP Header

The following SIP request headers are supported:

Note In the following table, a "Yes" in the Supported column means the header is sent and properly parsed.

Method	Supported	Notes
Accept	Yes	
Alert-Info	Yes	
Allow	Yes	
Allow-Events	Yes	
Authorization	Yes	
Call-ID	Yes	
Call-Info	Yes	
Contact	Yes	
Content-Length	Yes	
Content-Type	Yes	
CSeq	Yes	
Diversion	Yes	
History-Info	Yes	
Event	Yes	
Expires	Yes	

Method	Supported	Notes
From	Yes	
Max-Forwards	Yes	
Min-SE	Yes	
P-Asserted-Identity	Yes	
P-Preferred-Identity	Yes	
Proxy-Authenticate	Yes	
Proxy-Authorization	Yes	
RAck	Yes	
Record-Route	Yes	
Refer-To	Yes	
Referred-By	Yes	
Remote-Party-ID	Yes	
Replaces	Yes	
Require	Yes	
Route	Yes	
RSeq	Yes	
Session-Expires	Yes	
Subscription-State	Yes	
Supported	Yes	
To	Yes	
User-Agent	Yes	
Via	Yes	

SIP Responses

The following SIP responses are supported:

Note

In the following table, a "Yes" in the Supported column means the header is sent and properly parsed. The phone may not actually generate the response.

1xx Responses—Provisional

1xx Response	Supported	Notes
100 Trying	Yes	
180 Ringing	Yes	
181 Call Is Being Forwarded	Yes	
182 Queued	Yes	
183 Session Progress	Yes	

2xx Responses—Successful

2xx Response	Supported	Notes
200 OK	Yes	
202 Accepted	Yes	In REFER transfer.

3xx Responses—Redirection

3xx Response	Supported	Notes
300 Multiple Choices	Yes	
301 Moved Permanently	Yes	
302 Moved Temporarily	Yes	
305 Use Proxy	Yes	
380 Alternative Service	No	

4xx Responses—Request Failure

4xx Response	Supported	Notes
400 Bad Request	Yes	
401 Unauthorized	Yes	
402 Payment Required	Yes	
403 Forbidden	Yes	
404 Not Found	Yes	
405 Method Not Allowed	Yes	
406 Not Acceptable	No	

4xx Response	Supported	Notes
407 Proxy Authentication Required	Yes	
408 Request Timeout	Yes	
409 Conflict	No	
410 Gone	No	
411 Length Required	No	
413 Request Entity Too Large	No	
414 Request-URI Too Long	Yes	
415 Unsupported Media Type	Yes	
416 Unsupported URI Scheme	No	
420 Bad Extension	No	
421 Extension Required	No	
423 Interval Too Brief	Yes	
480 Temporarily Unavailable	Yes	
481 Call/Transaction Does Not Exist	Yes	
482 Loop Detected	Yes	
483 Too Many Hops	No	
484 Address Incomplete	Yes	
485 Ambiguous	No	
486 Busy Here	Yes	
487 Request Terminated	Yes	
488 Not Acceptable Here	Yes	
491 Request Pending	No	
493 Undecipherable	No	

5xx Responses—Server Failure

5xx Response	Supported	Notes
500 Server Internal Error	Yes	
501 Not Implemented	Yes	
502 Bad Gateway	No	

5xx Response	Supported	Notes
503 Service Unavailable	Yes	
504 Server Time-out	No	
505 Version Not Supported	No	
513 Message Too Large	No	

6xx Response—Global Failures

6xx Response	Supported	Notes
600 Busy Everywhere	Yes	
603 Decline	Yes	
604 Does Not Exist Anywhere	No	
606 Not Acceptable	No	

SIP Session Description Protocol (SDP) Usage

SDP Headers	Supported
v–Session Description Protocol Version	Yes
o–Owner/Creator, Session Id	Yes
a–Media Attribute	Yes
c–Connection Information	Yes
b–Bandwidth Information	Yes
m–Media Description, name and address	Yes
s–Session Name	Yes
t–Time Description, active time	Yes

Appendix G: SIP Call Flows

SIP uses six request methods:

INVITE–Indicates a user is being invited to participate in a call session.

ACK–Confirms that the client has received a final response to an INVITE request.

BYE–Terminates a call and can be sent by either the caller or the callee.

CANCEL–Cancels any pending searches but does not terminate a call that has already been accepted.

OPTIONS−Queries the capabilities of servers.

REGISTER−Registers the address listed in the To header field with a SIP server.

The following types of responses are used by SIP and generated by the DECT IP phone or the SIP server:

SIP 1xx−Provisional Responses

SIP 2xx−Successful Responses

SIP 3xx−Redirection Responses

SIP 4xx−Request Failure Responses

SIP 5xx−Server Failure Responses

SIP 6xx−Global Failures Responses

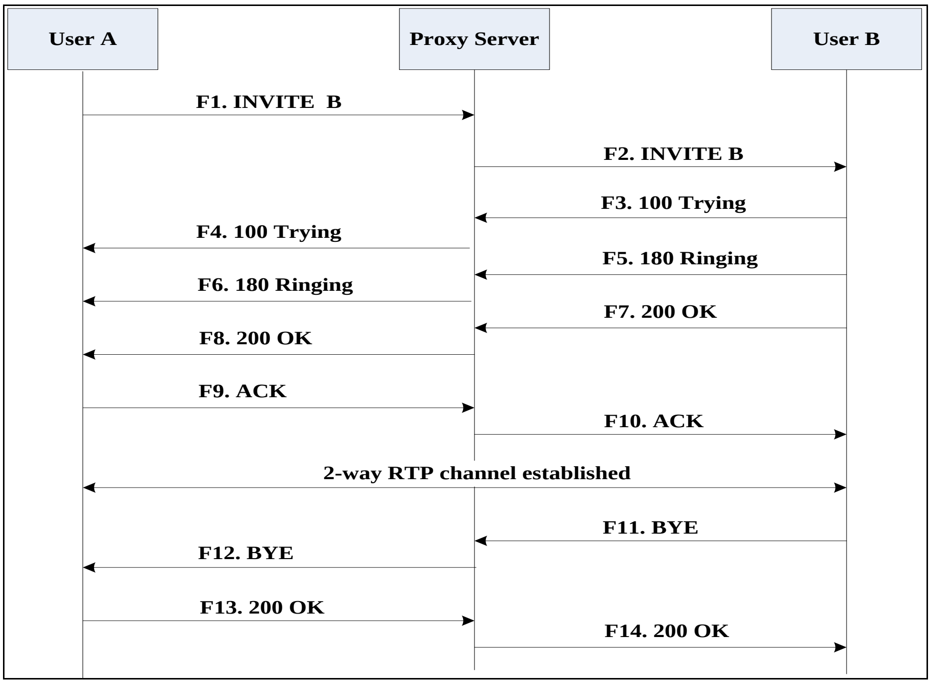
For more information on SIP Responses, refer to SIP Responses on page 484.

Successful Call Setup and Disconnect

The following figure illustrates the scenario of a successful call. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP DECT IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B hangs up.



Step	Action	Description
F1	INVITE−User A to Proxy Server	User A sends a SIP INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: ● The IP address of User B is inserted in the Request-URI field. ● User A is identified as the call session initiator in the From field. ● A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ● The transaction number within a single call leg is identified in the CSeq field. ● The media capability User A is ready to receive is specified. ● The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE−Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	100 Trying−User B to Proxy Server	User B sends a SIP 100 Trying response to the proxy server. The 100 Trying response indicates that the INVITE request has been received by User B.
F4	100 Trying−Proxy Server to User A	The proxy server forwards the SIP 100 Trying to User A to indicate that the INVITE request has been received by User B.
F5	180 Ringing−User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the User B is being alerted.
F6	180 Ringing−Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.

Step	Action	Description
F7	200 OK– User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F8	200OK–Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
F9	ACK–User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F10	ACK–Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F11	BYE–User B to Proxy Server	User B terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User B wants to release the call.
F12	BYE–Proxy Server to User A	The proxy server forwards the SIP BYE request to User A to notify that User B wants to release the call.
F13	200 OK–User A to Proxy Server	User A sends a SIP 200 OK response to the proxy server. The 200 OK response indicates that User A has received the BYE request. The call session is now terminated.
F14	200 OK–Proxy Server to User B	The proxy server forwards the SIP 200 OK response to User B to indicate that User A has received the BYE request. The call session is now terminated.

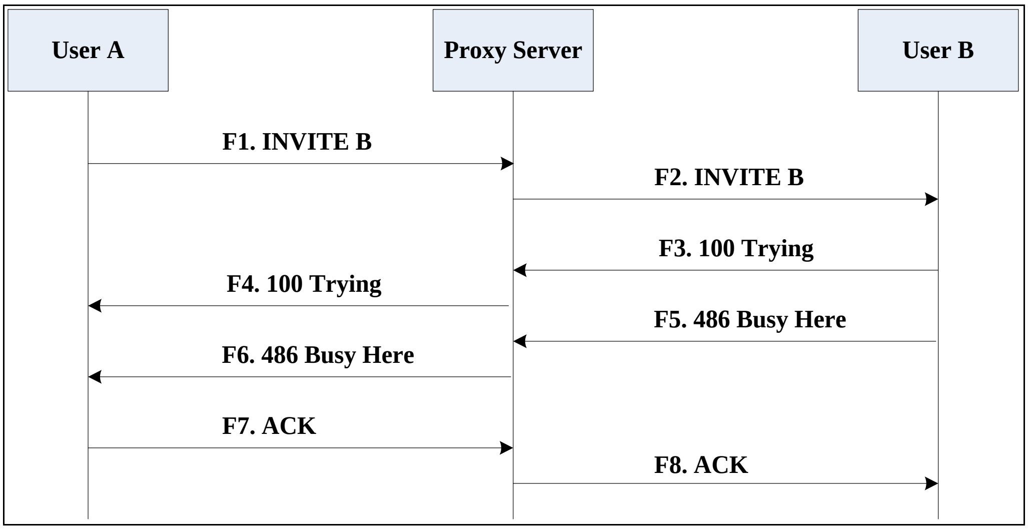
Unsuccessful Call Setup—Called User is Busy

The following figure illustrates the scenario of an unsuccessful call caused by the called user's being busy. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP DECT IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B is busy on the DECT IP phone and unable or unwilling to take another call.

The call cannot be set up successfully.



Step	Action	Description
F1	INVITE—User A to Proxy Server	User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: ● The IP address of User B is inserted in the Request-URI field. ● User A is identified as the call session initiator in the From field. ● A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ● The transaction number within a single call leg is identified in the CSeq field. ● The media capability User A is ready to receive is specified. ● The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	100 Trying—User B to Proxy Server	User B sends a SIP 100 Trying response to the proxy server. The 100 Trying response indicates that the INVITE request has been

Step	Action	Description
		received by User B.
F4	100 Trying–Proxy Server to User A	The proxy server forwards the SIP 100 Trying to User A to indicate that the INVITE request has already been received.
F5	486 Busy Here–User B to Proxy Server	User B sends a SIP 486 Busy Here response to the proxy server. The 486 Busy Here response is a client error response indicating that User B is successfully connected but User B is busy on the DECT IP phone and unable or unwilling to take the call.
F6	486 Busy Here–Proxy Server to User A	The proxy server forwards the 486 Busy Here response to notify User A that User B is busy.
F7	ACK–User A to Proxy Server	User A sends a SIP ACK to the proxy server. The SIP ACK message indicates that User A has received the 486 Busy Here message.
F8	ACK–Proxy Server to User B	The proxy server forwards the SIP ACK to User B to indicate that the 486 Busy Here message has already been received.

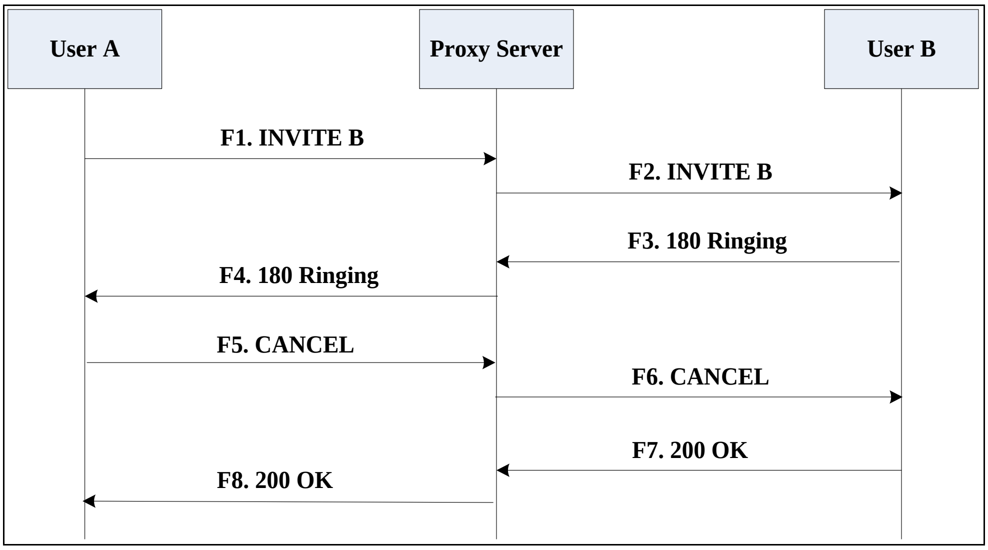
Unsuccessful Call Setup—Called User Does Not Answer

The following figure illustrates the scenario of an unsuccessful call caused by the called user's no answering. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP DECT IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B does not answer the call.
3. User A hangs up.

The call cannot be set up successfully.



Step	Action	Description
F1	INVITE−User A to Proxy Server	User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: ● The IP address of User B is inserted in the Request-URI field. ● User A is identified as the call session initiator in the From field. ● A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ● The transaction number within a single call leg is identified in the CSeq field. ● The media capability User A is ready to receive is specified. ● The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE−Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	180 Ringing−User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing

Step	Action	Description
		response indicates that the user is being alerted.
F4	180 Ringing−Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	CANCEL−User A to Proxy Server	User A sends a SIP CANCEL request to the proxy server after not receiving an appropriate response within the time allocated in the INVITE request. The SIP CANCEL request indicates that User A wants to disconnect the call.
F6	CANCEL−Proxy Server to User B	The proxy server forwards the SIP CANCEL request to notify User B that User A wants to disconnect the call.
F7	200 OK−User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The SIP 200 OK response indicates that User B has received the CANCEL request.
F8	200 OK−Proxy Server to User A	The proxy server forwards the SIP 200 OK response to notify User A that the CANCEL request has been processed successfully.

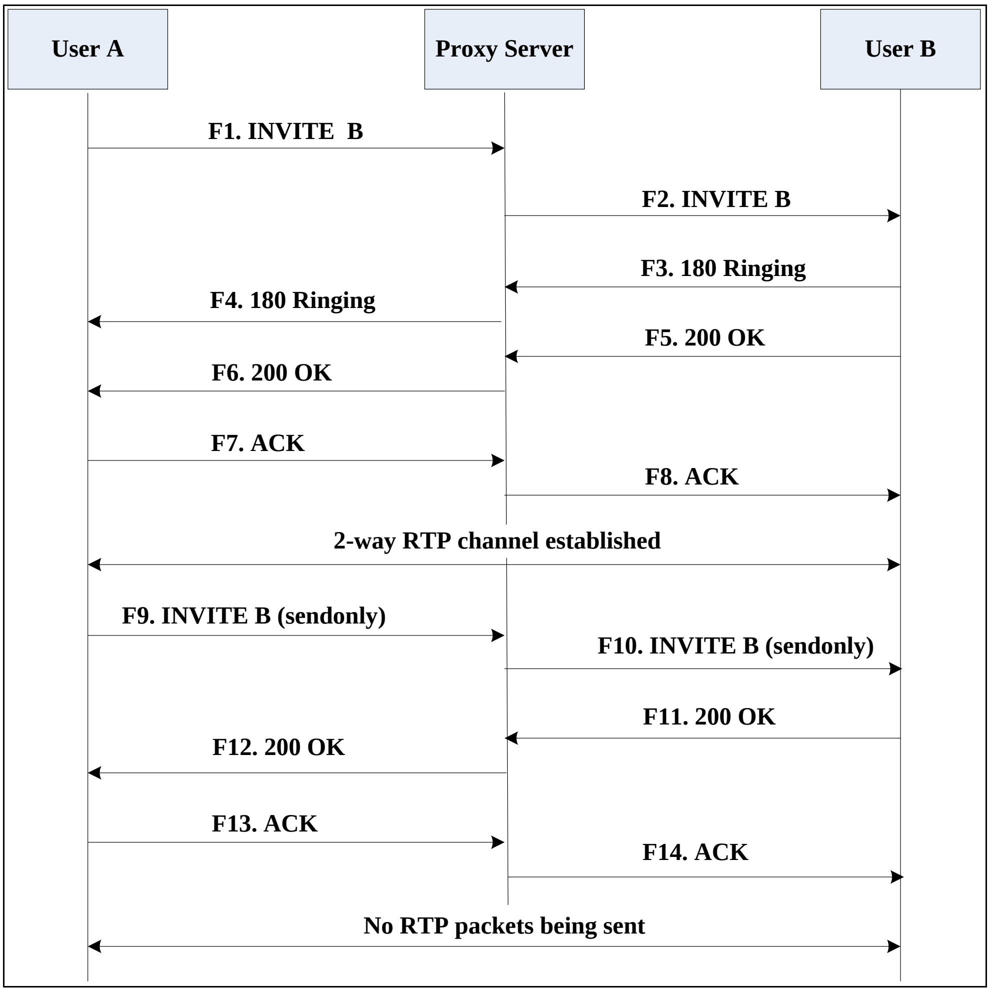
Successful Call Setup and Call Hold

The following figure illustrates a successful call setup and call hold. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP DECT IP phones.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.

3. User A places User B on hold.



Step	Action	Description
F1	INVITE−User A to Proxy Server	User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: ● The IP address of User B is inserted in the Request-URI field. ● User A is identified as the call session initiator in the From field. ● A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ● The transaction number within a single call leg is identified in the

Step	Action	Description
		CSeq field. ● The media capability User A is ready to receive is specified. ● The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies the proxy server that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.

Step	Action	Description
F11	200 OK−User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE is successfully processed.
F12	200 OK−Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully placed on hold.
F13	ACK−User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK−Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.

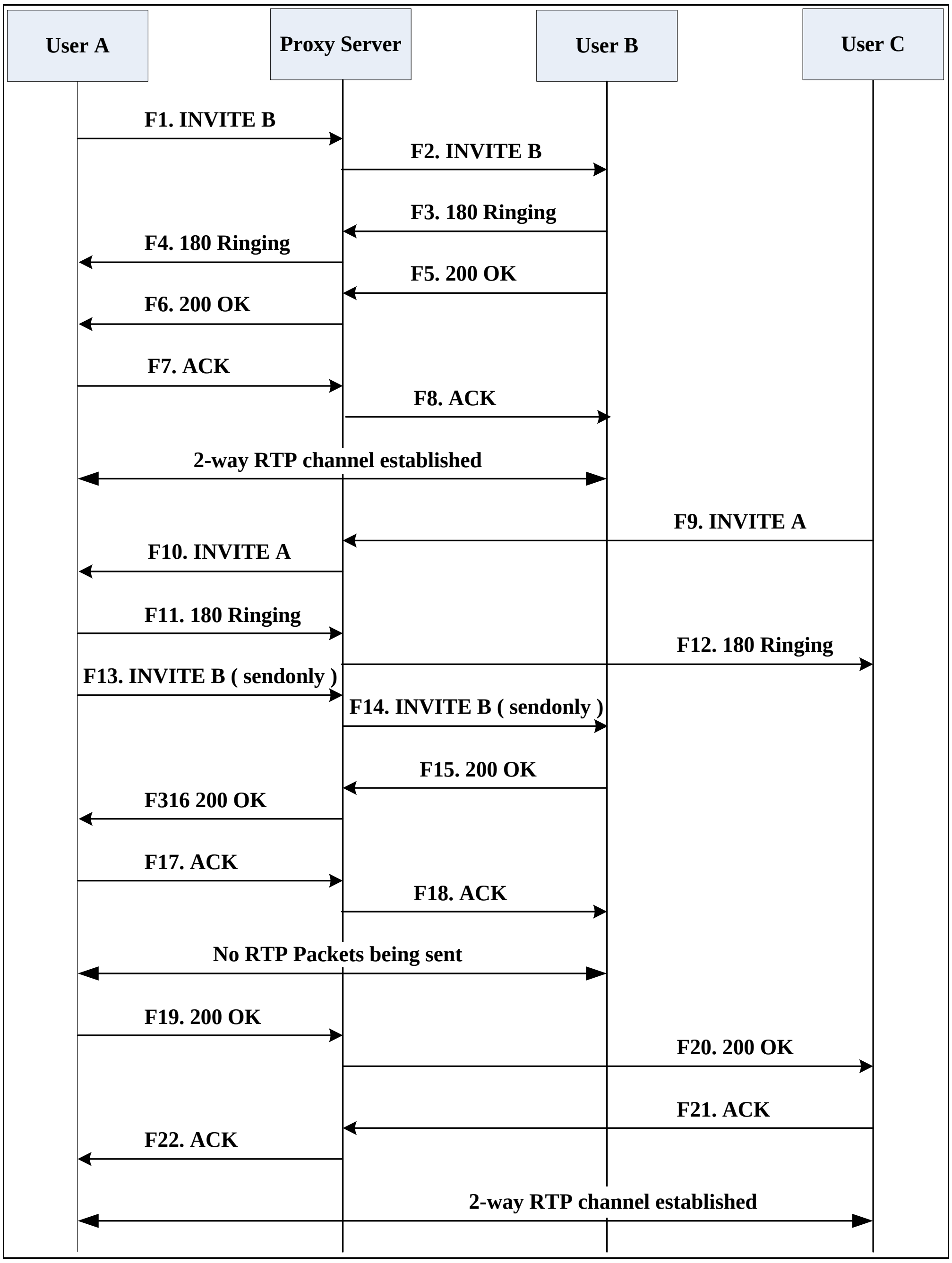
Successful Call Setup and Call Waiting

The following figure illustrates a successful call between Yealink SIP DECT IP phones in which two parties are in a call, one of the participants receives and answers an incoming call from a third party. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP DECT IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User C calls User B.

4. User B accepts the call from User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: ● The IP address of User B is inserted in the Request-URI field. ● User A is identified as the call

Step	Action	Description
		session initiator in the From field. ● A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ● The transaction number within a single call leg is identified in the CSeq field. ● The media capability User A is ready to receive is specified. ● The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE−Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing−User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing−Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK−User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies proxy server that the connection has been made.
F6	200 OK−Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
F7	ACK−User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK−Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.

Step	Action	Description
F9	INVITE−User C to Proxy Server	User C sends a SIP INVITE message to the proxy server. The INVITE request is an invitation to User A to participate in a call session. In the INVITE request: ● The IP address of User A is inserted in the Request-URI field. ● User C is identified as the call session initiator in the From field. ● A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ● The transaction number within a single call leg is identified in the CSeq field. ● The media capability User C is ready to receive is specified. ● The port on which User A is prepared to receive the RTP data is specified.
F10	INVITE−Proxy Server to User A	The proxy server maps the SIP URI in the To field to User A. The proxy server sends the INVITE message to User A.
F11	180 Ringing−User A to Proxy Server	User A sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F12	180 Ringing−Proxy Server to User C	The proxy server forwards the 180 Ringing response to User C. User C hears the ring-back tone indicating that User A is being alerted.
F13	INVITE−User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F14	INVITE−Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F15	200 OK−User B to Proxy Server	User B sends a 200 OK to the proxy server. The 200 OK response indicates that the

Step	Action	Description
		INVITE was successfully processed.
F16	200 OK–Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully placed on hold.
F17	ACK–User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F18	ACK–Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F19	200 OK–User A to Proxy Server	User A sends a 200 OK response to the proxy server. The 200 OK response notifies that the connection has been made.
F20	200 OK–Proxy Server User C	The proxy server forwards the 200 OK message to User C.
F21	ACK–User C to Proxy Server	User C sends a SIP ACK to the proxy server. The ACK confirms that User C has received the 200 OK response. The call session is now active.
F22	ACK–Proxy Server to User A	The proxy server forwards the SIP ACK to User A to confirm that User C has received the 200 OK response.

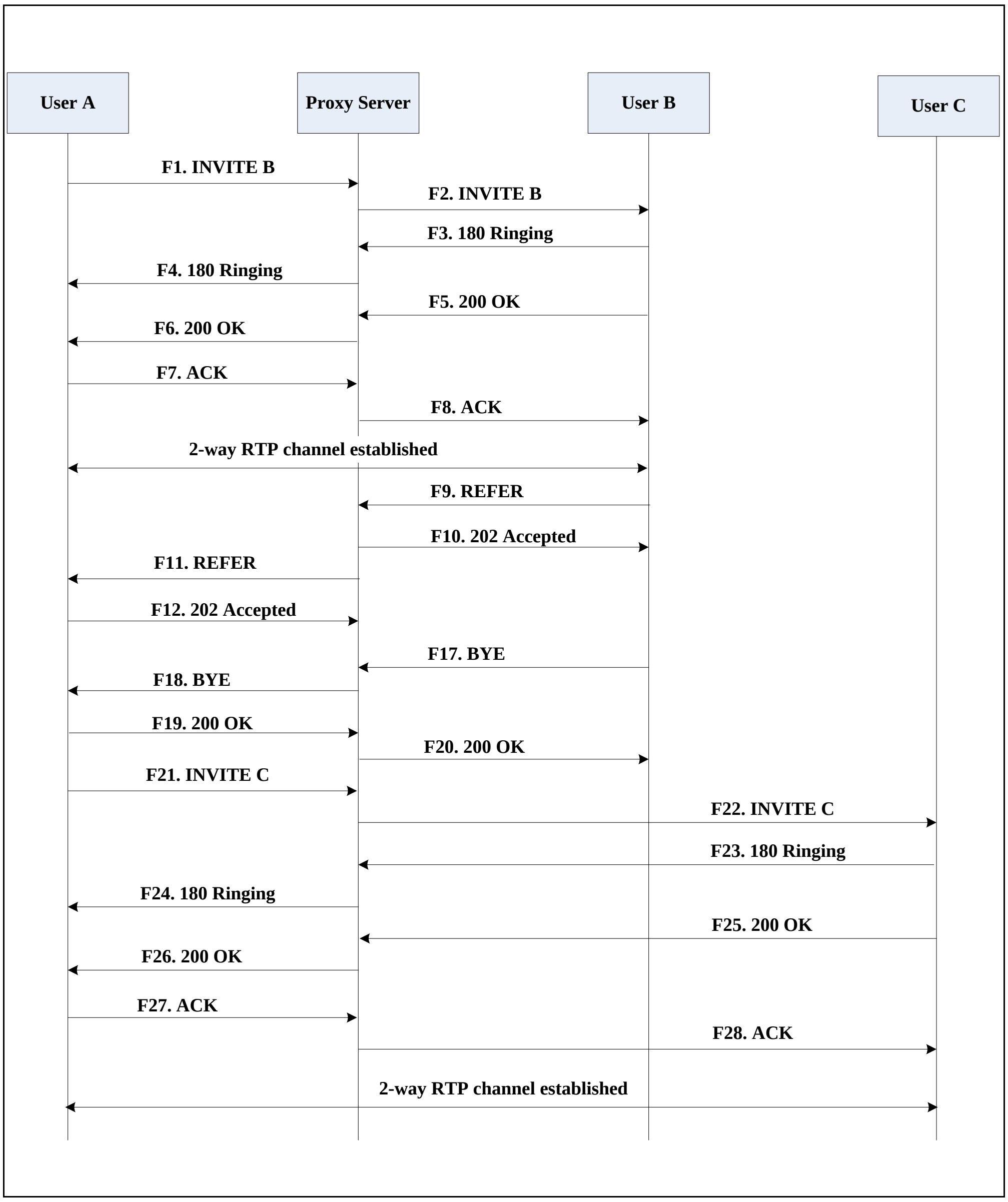
Call Transfer without Consultation

The following figure illustrates a successful call between Yealink SIP DECT IP phones in which two parties are in a call and then one of the parties transfers the call to a third party without consultation. This is called a blind transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP DECT IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B transfers the call to User C.
4. User C answers the call.

   Call is established between User A and User C.



Step	Action	Description
F1	INVITE−User A to Proxy Server	User A sends an INVITE message to the proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request:

Step	Action	Description
		● The IP address of User B is inserted in the Request-URI field. ● User A is identified as the call session initiator in the From field. ● A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ● The transaction number within a single call leg is identified in the CSeq field. ● The media capability User A is ready to receive is specified. ● The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE−Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing−User B to Proxy server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing−Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK−User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK−Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
F7	ACK−User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK−Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy

Step	Action	Description
		server has received the 200 OK response. The call session is now active.
F9	REFER–User B to Proxy Server	User B sends a REFER message to the proxy server. User B performs a blind transfer of User A to User C.
F10	202 Accepted–Proxy Server to User B	The proxy server sends a SIP 202 Accept response to User B. The 202 Accepted response notifies User B that the proxy server has received the REFER message.
F11	REFER–Proxy Server to User A	The proxy server forwards the REFER message to User A.
F12	202 Accepted–User A to Proxy Server	User A sends a SIP 202 Accept response to the proxy server. The 202 Accepted response indicates that User A accepts the transfer.
F13	BYE–User B to Proxy Server	User B terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User B wants to release the call.
F14	BYE–Proxy Server to User A	The proxy server forwards the BYE request to User A.
F15	200OK–User A to Proxy Server	User A sends a SIP 200 OK response to the proxy server. The 200 OK response confirms that User A has received the BYE request.
F16	200OK–Proxy Server to User B	The proxy server forwards the SIP 200 OK response to User B.
F17	INVITE–User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F18	INVITE–Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C.
F19	180 Ringing–User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.

Step	Action	Description
F20	180 Ringing−Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted
F21	200OK−User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies the proxy server that the connection has been made.
F22	200OK−Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.
F23	ACK− User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F24	ACK−Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that User A has received the 200 OK response. The call session is now active.

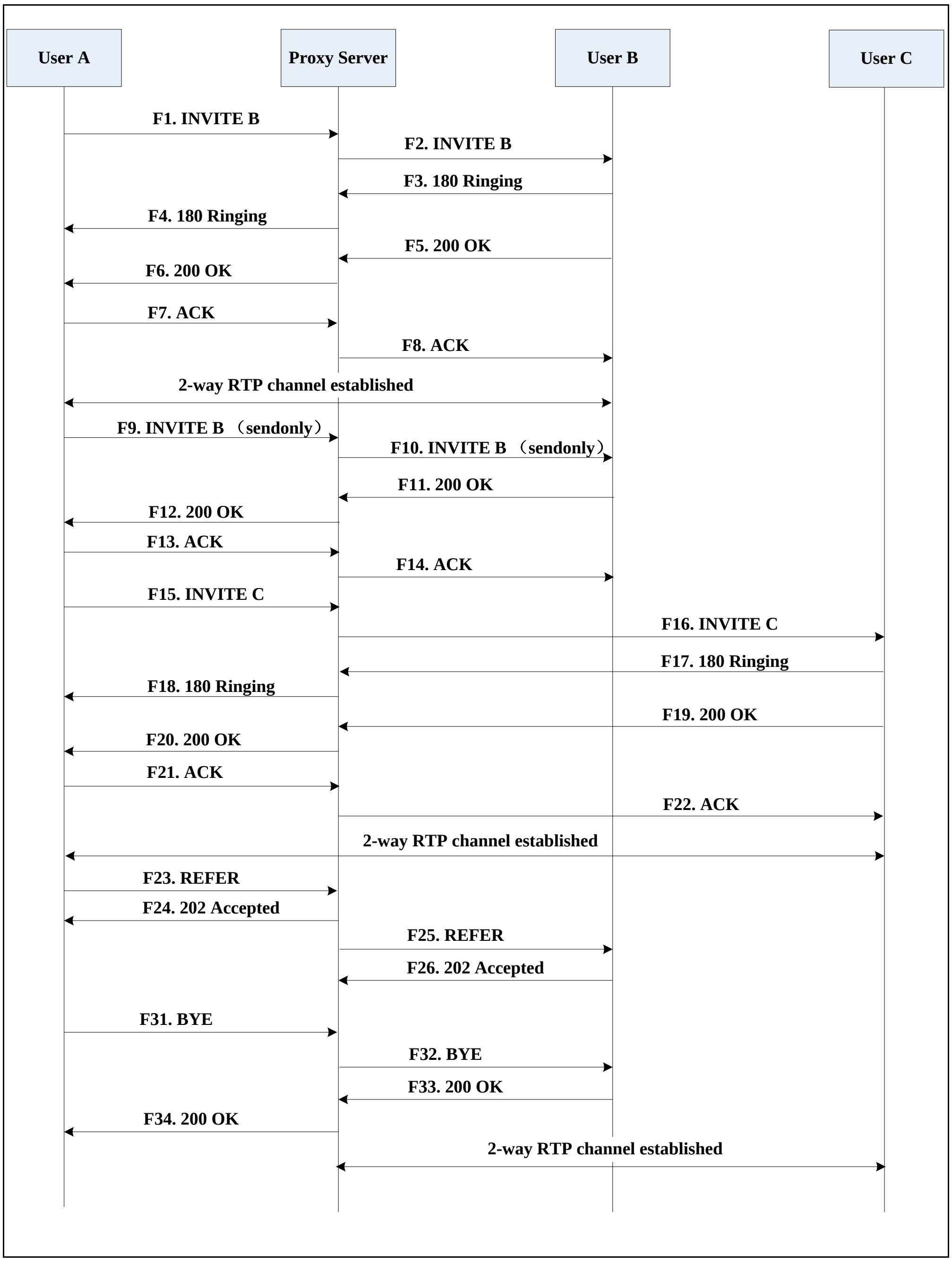
Call Transfer with Consultation

The following figure illustrates a successful call between Yealink SIP DECT IP phones in which two parties are in a call and then one of the parties transfers the call to the third party with consultation. This is called attended transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP DECT IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A calls User C.
4. User C answers the call.
5. User A transfers the call to User C.

Call is established between User B and User C.



Step	Action	Description
F1	INVITE−User A to Proxy Server	User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: ● The IP address of User B is inserted in the Request-URI field.

Step	Action	Description
		• User A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE−Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing−User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing−Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK−User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK−Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
F7	ACK−User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK−Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.

Step	Action	Description
F9	INVITE−User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE−Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK−User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE was successfully processed.
F12	200 OK−Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully placed on hold.
F13	ACK−User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK−Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F15	INVITE−User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F16	INVITE−Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C. The proxy server sends the INVITE request to User C.
F17	180 Ringing−User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F18	180 Ringing−Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being

Step	Action	Description
		alerted.
F19	200OK−User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F20	200OK−Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F21	ACK− User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F22	ACK−Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F23	REFER−User A to Proxy Server	User A sends a REFER message to the proxy server. User A performs a transfer of User B to User C.
F24	202 Accepted−Proxy Server to User A	The proxy server sends a SIP 202 Accepted response to User A. The 202 Accepted response notifies User A that the proxy server has received the REFER message.
F25	REFER−Proxy Server to User B	The proxy server forwards the REFER message to User B.
F26	202 Accepted−User B to Proxy Server	User B sends a SIP 202 Accept response to the proxy server. The 202 Accepted response indicates that User B accepts the transfer.
F27	BYE−User A to Proxy Server	User A terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User A wants to release the call.
F28	BYE−Proxy Server to User B	The proxy server forwards the BYE request to User B.
F29	200OK−User B to Proxy Server	User B sends a SIP 200 OK response to the

Step	Action	Description
		proxy server. The 200 OK response notifies User A that User B has received the BYE request.
F30	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.

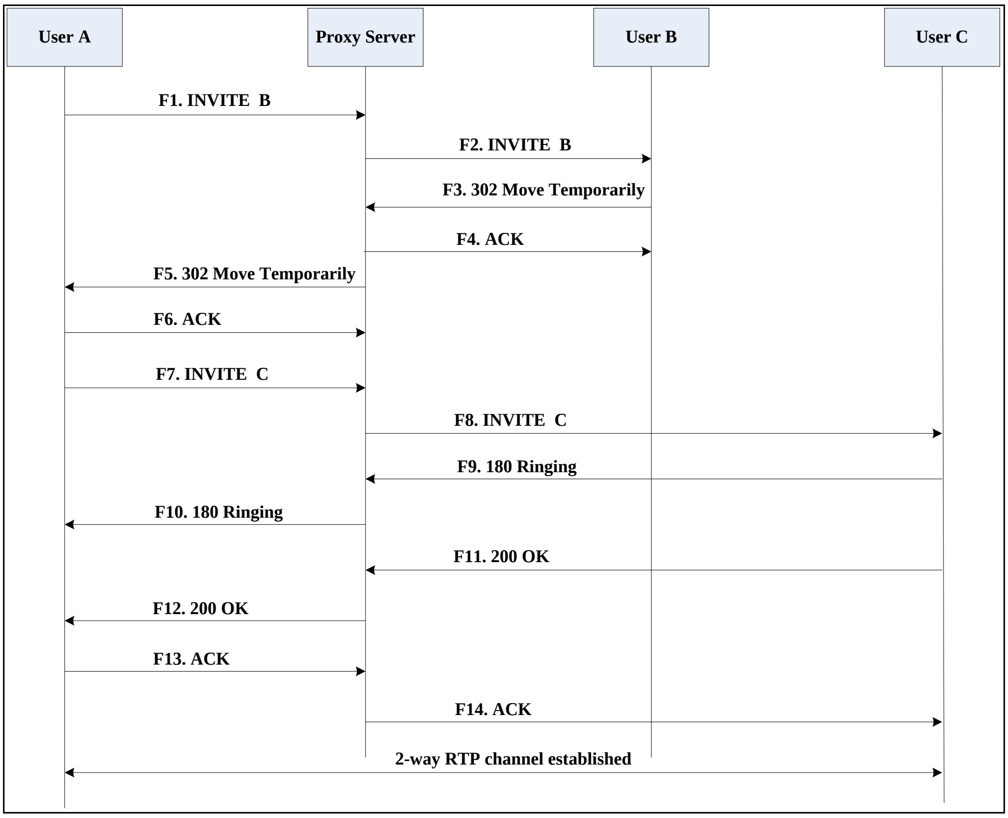
Always Call Forward

The following figure illustrates successful call forwarding between Yealink SIP DECT IP phones in which User B has enabled always call forward. The incoming call is immediately forwarded to User C when User A calls User B. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP DECT IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables always call forward, and the destination number is User C.
2. User A calls User B.
3. User B forwards the incoming call to User C.
4. User C answers the call.

   Call is established between User A and User C.



Step	Action	Description
F1	INVITE−User A to Proxy Server	User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: ● The IP address of the User B is inserted in the Request-URI field. ● User A is identified as the call session initiator in the From field. ● A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ● The transaction number within a single call leg is identified in the CSeq field. ● The media capability User A is ready to receive is specified. ● The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE−Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	302 Move Temporarily−User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SDECT IP phone B. User B rewrites the contact-URI.
F4	ACK−Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the 302 Move Temporarily message.
F5	302 Move Temporarily−Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F6	ACK−User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the 302 Move Temporarily message.
F7	INVITE−User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a

Step	Action	Description
		unique Call-ID is generated and the Contact-URI field indicates that User A requested the call.
F8	INVITE−Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C. The proxy server sends the SIP INVITE request to User C.
F9	180 Ringing−User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F10	180 Ringing−Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F11	200OK−User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F12	200OK−Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F13	ACK−User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F14	ACK−Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.

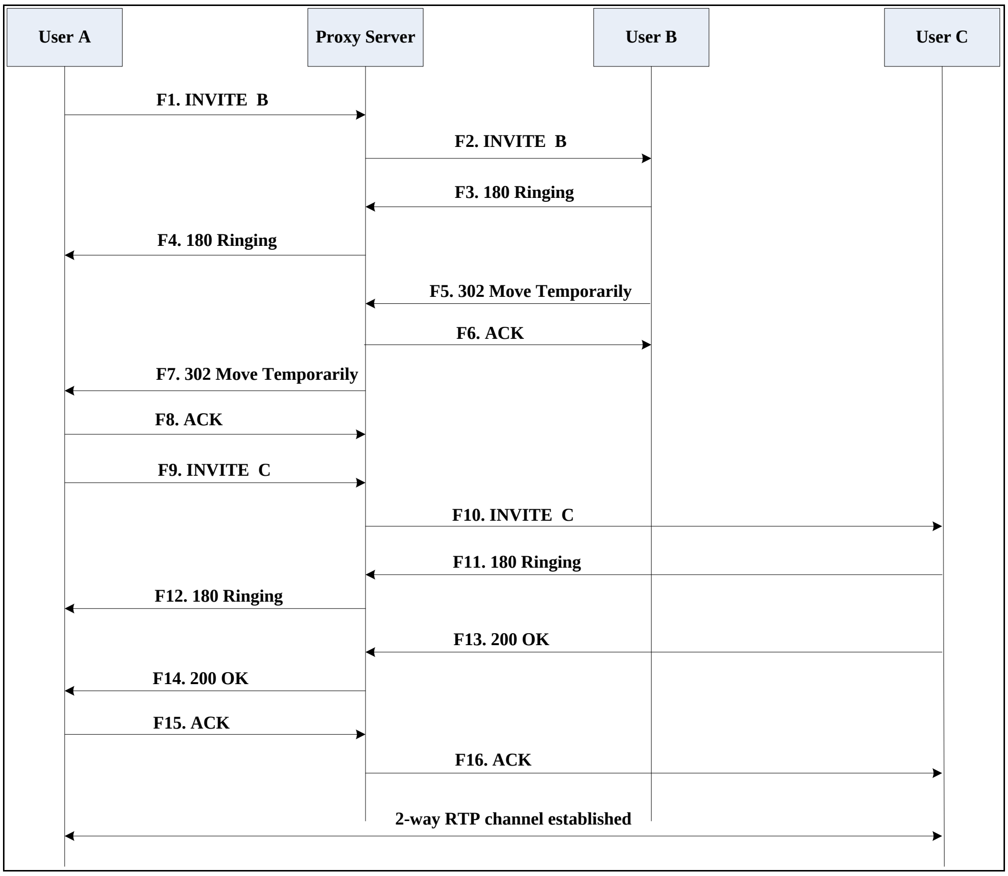
Busy Call Forward

The following figure illustrates successful call forwarding between Yealink SIP DECT IP phones in which User B has enabled busy call forward. The incoming call is forwarded to User C when User B is busy. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP DECT IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables busy call forward, and the destination number is User C.
2. User A calls User B.
3. User B is busy.
4. User B forwards the incoming call to User C.
5. User C answers the call.

Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: ● The IP address of User B is inserted in the Request-URI field. ● User A is identified as the call session initiator in the From field. ● A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ● The transaction number within a single call leg is identified in the CSeq field. ● The media capability User A is ready to receive is specified.

Step	Action	Description
		● The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE−Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing−User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing−Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	302 Move Temporarily−User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SDECT IP phone B. User B rewrites the contact-URI.
F6	ACK−Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the ACK message.
F7	302 Move Temporarily−Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F8	ACK−User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the ACK message.
F9	INVITE−User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F10	INVITE−Proxy Server to User C	The proxy server forwards the SIP INVITE request to User C.
F11	180 Ringing−User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being

Step	Action	Description
		alerted.
F12	180 Ringing−Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F13	200OK−User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F14	200OK−Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.
F15	ACK− User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F16	ACK−Proxy Server to User C	The proxy server sends the ACK message to User C.

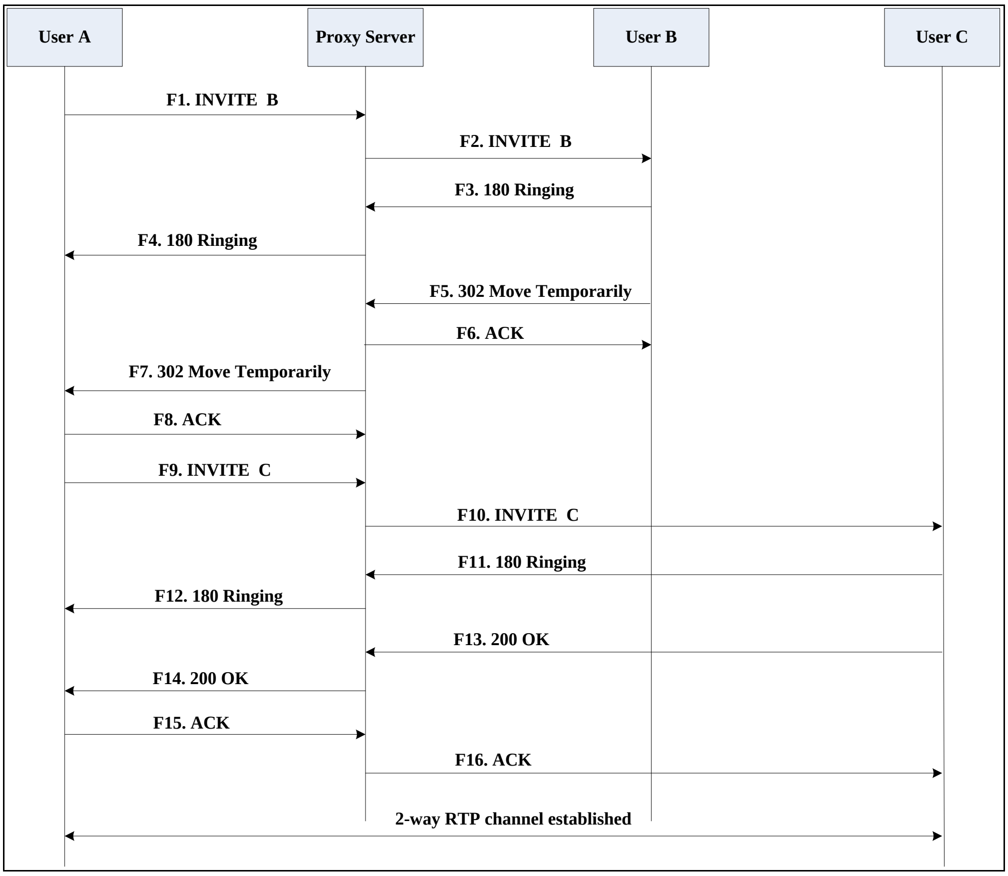
No Answer Call Forward

The following figure illustrates successful call forwarding between Yealink SIP DECT IP phones in which User B has enabled no answer call forward. The incoming call is forwarded to User C when User B does not answer the incoming call after a period of time. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP DECT IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B enables no answer call forward, and the destination number is User C.
2. User A calls User B.
3. User B does not answer the incoming call.
4. User B forwards the incoming call to User C.
5. User C answers the call.

Call is established between User A and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: ● The IP address of User B is inserted in the Request-URI field. ● User A is identified as the call session initiator in the From field. ● A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ● The transaction number within a single call leg is identified in the CSeq field. ● The media capability User A is ready to receive is specified.

Step	Action	Description
		● The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE−Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing−User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing−Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	302 Move Temporarily−User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SDECT IP phone B. User B rewrites the contact-URI.
F6	ACK−Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the ACK message.
F7	302 Move Temporarily−Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F8	ACK−User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the ACK message.
F9	INVITE−User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F10	INVITE−Proxy Server to User C	The proxy server forwards the SIP INVITE request to User C.
F11	180 Ringing−User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being

Step	Action	Description
		alerted.
F12	180 Ringing–Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F13	200OK–User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F14	200OK–Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F15	ACK– User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F16	ACK–Proxy Server to User C	The proxy server sends the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response.

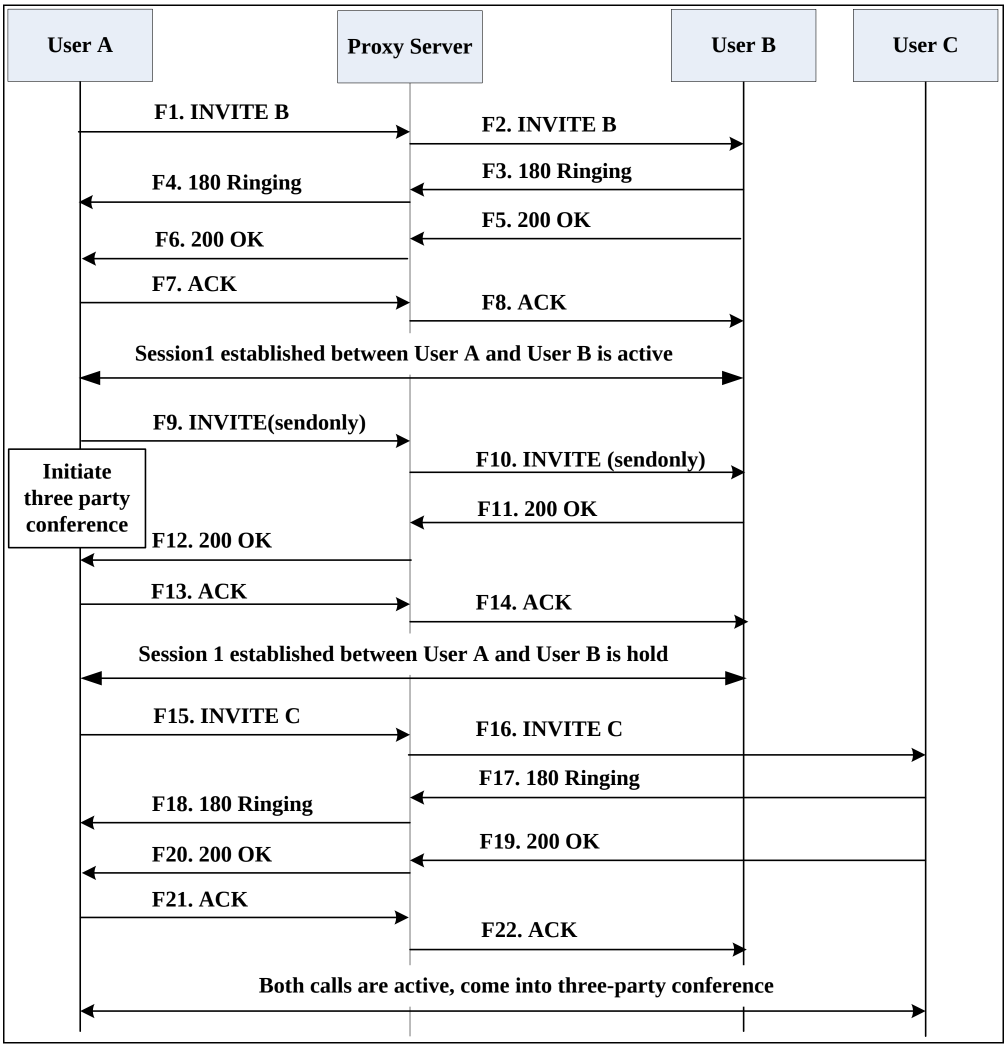
Call Conference

The following figure illustrates successful 3-way calling between Yealink DECT IP phones in which User A mixes two RTP channels and therefore establishes a conference between User B and User C. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP DECT IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User A places User B on hold.
4. User A calls User C.
5. User C answers the call.

6. User A mixes the RTP channels and establishes a conference between User B and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: ● The IP address of User B is inserted in the Request-URI field. ● User A is identified as the call session initiator in the From field. ● A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ● The transaction number within a

Step	Action	Description
		single call leg is identified in the CSeq field. ● The media capability User A is ready to receive is specified. ● The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE−Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	180 Ringing−User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing−Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK−User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK−Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
F7	ACK−User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK−Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE−User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE−Proxy Server to User B	The proxy server forwards the mid-call

Step	Action	Description
		INVITE message to User B.
F11	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE is successfully processed.
F12	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User A that User B is successfully placed on hold.
F13	ACK—User A to Proxy Server	User A sends the ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F15	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F16	INVITE—Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C. The proxy server sends the SIP INVITE request to User C.
F17	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F18	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F19	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.

Step	Action	Description
F20	200OK−Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F21	ACK− User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F22	ACK−Proxy Server to User C	The proxy server sends the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response.

Index

M

N

O

P

Q

R

S