Yealink

Skype for Business® HD IP Phone Administrator Guide

Version 9.26

Apr.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 Skype for Business 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/onepage_83.html.

About This Guide

Yealink administrator guide is intended for administrators who need to properly configure, customize, manage, and troubleshoot the Skype for Business phones 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 phones: central provisioning, web user interface and phone user interface. It will help you perform the following tasks:

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

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

The detailed information in this guide is applicable to the following firmware version for Skype for Business phones:

- For T48S/T46S/T42S/T41S Skype for Business phones: 66.9.0.25 or higher.
- For CP960 Skype for Business phones: 73.8.0.17 or higher.

Chapters in This Guide

This administrator guide includes the following chapters:

- Chapter 1, "Product Overview" describes the phones and expansion modules.
- Chapter 2, "Getting Started" describes how phones fit in your network and how to install and connect phones, and also gives you an overview of phone's initialization process.
- Chapter 3, "Setting Up Your System" describes some essential information on how to set up your phone network and set up your phone with a provisioning server.
- Chapter 4, "Configuring Basic Features" describes how to configure the basic features on phones.
- Chapter 5, "Configuring Advanced Features" describes how to configure the advanced features on phones.
- Chapter 6, "Configuring Audio Features" describes how to configure the audio features on phones.
- Chapter 7, "Configuring Security Features" describes how to configure the security features on phones.
- Chapter 8, "Troubleshooting" describes how to troubleshoot phones and provides some

common troubleshooting solutions.

- Chapter 9, "Appendix" provides the glossary, time zones, trusted certificates, auto provisioning flowchart, reference information about phones compliant with RFC 3261, SIP call flows and some other function lists (e.g., DSS keys, reading icons).

Related Documentations

This guide covers T48S/T46S/T42S/T41S/CP960 Skype for Business phones. The following related documents are available:

- Quick Start Guides, which describe how to assemble Skype for Business phones and configure the most basic features available on Skype for Business phones.
- User Guides, which describe the basic and advanced features available on Skype for Business phones.
- Auto Provisioning Guide, which describes how to provision Skype for Business phones using the configuration files.

  The purpose of *Auto Provisioning Guide* is to serve as a basic guidance for provisioning Yealink 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 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.
- <y0000000000xx>.cfg and <MAC>.cfg template configuration files.
- Deployment Guide, which describes how to deploy phones in a Microsoft Skype for Business Server environment.
- Updating Phone Firmware from Microsoft Skype for Business Server Guide, which describes how to upgrade firmware via Skype for Business Server.

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.

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

Convention	Description
Bold	Highlights the web/phone user interface items such as menus, menu selections, soft keys, or directory names when they are involved in a procedure or user action (e.g., Click on **Security**->**License**). Also used to emphasize text (e.g., **Configuration File**).
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 Skype for Business phone to Perform the Auto Provisioning*).
Blue Text	Used for cross references to other sections within this documentation (e.g., refer to Troubleshooting).
Blue Text in Italics	Used for hyperlinks to Yealink resources outside of this documentation such as the Yealink documentations (e.g., *Yealink_Skype_for_Business_HD_IP_Phones_Auto_Provisioning_Guide*).

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

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

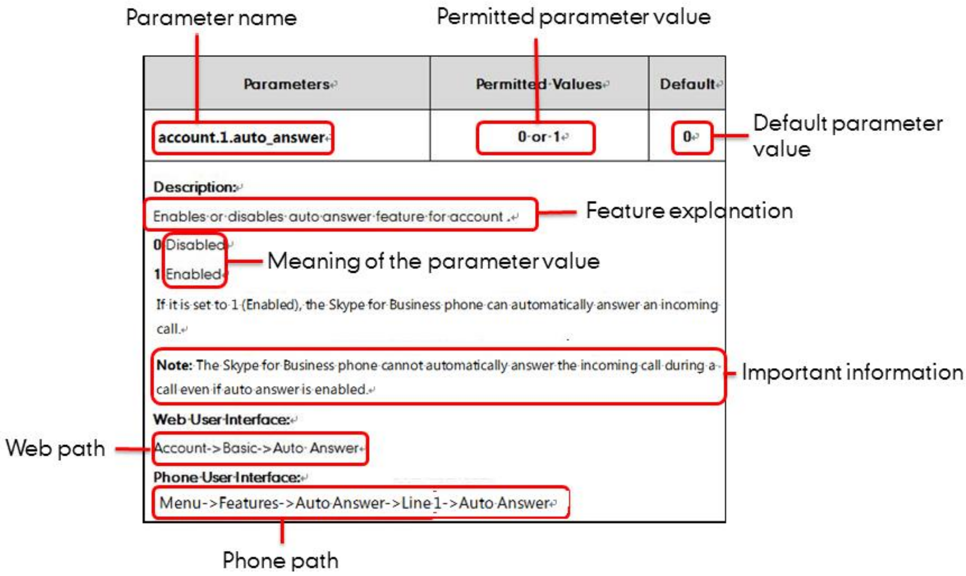
Reading the Configuration Parameter Tables

Most features described 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.

Configuration Parameter Table Format

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



Note

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

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

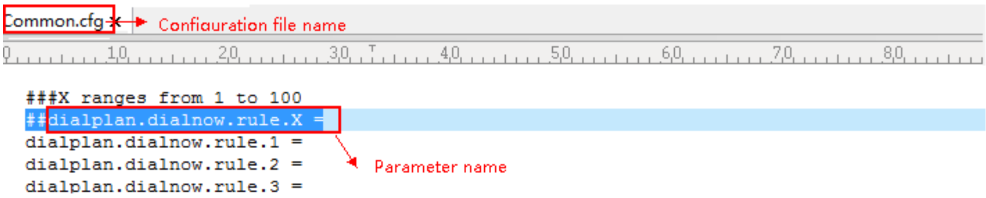
The above table also indicates three methods for configuring the feature.

Method 1: Central Provisioning

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

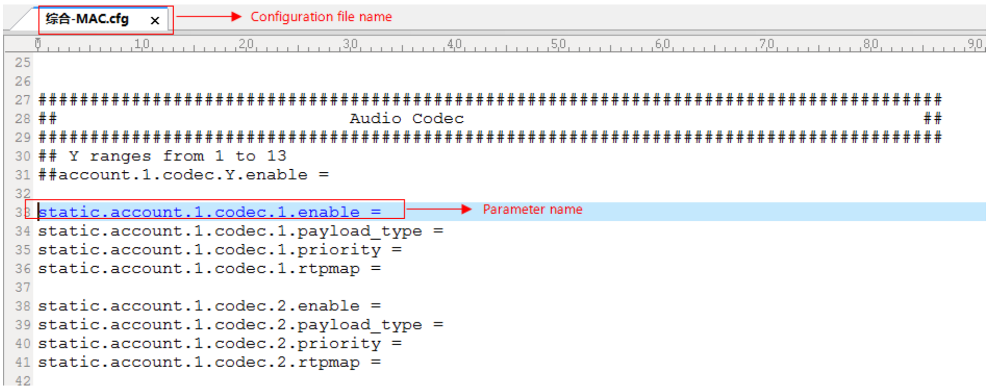
Note that some parameters described in this guide contain one or more variables (e.g., X or Y). But the variables in the parameters described in the CFG file are all replaced with specific value in the scope of variable. You may need to assign a value to the variable before you search and locate the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

For example, if you want to configure the dial-now rule, you need to locate the dialplan.dialnow.rule.X in the Common.cfg file and then configure it as required (e.g., dialplan.dialnow.rule.1 = 123).



If you want to enable the audio codec 1 for account 1, you can locate the static.account.1.codec.Y.enable in the MAC.cfg file and configure it as required (e.g., static.account.1.codec.1.enable = 1).

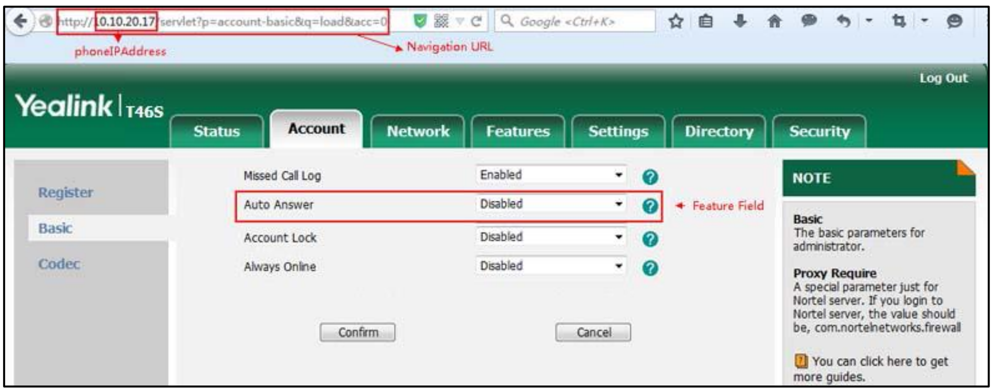
The following shows a segment of MAC.cfg file:



Method 2: Web User Interface

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

As shown in the following illustration:



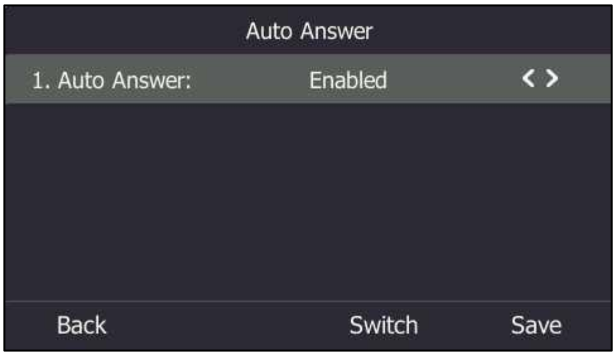
To successfully log into the web user interface, you may need to enter the user name (default: admin) and password (default: admin). For more information, refer to Web User Interface on

page 89.

Method 3: Phone User Interface

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

As shown in the following illustration:



Recommended References

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

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

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

This guide mainly takes the T46S Skype for Business phones as example for reference. For more details on other Skype for Business phones, refer to *Yealink Skype for Business phone-specific user guide*.

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

Understanding VoIP Principle and SIP Components

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

VoIP Principle

VoIP

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

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

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 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.

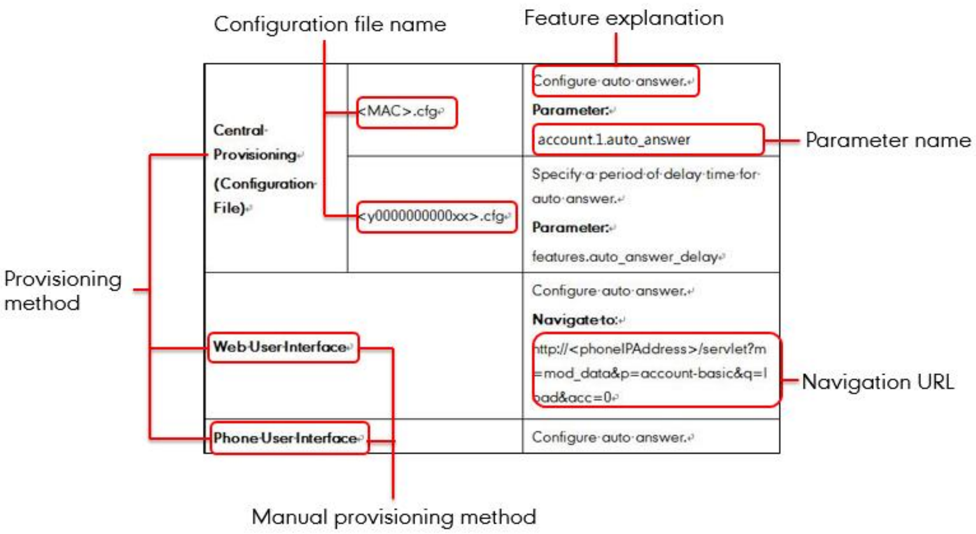
Summary Table Format

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

The central provisioning method requires you to configure parameters located in CFG format configuration files that Yealink provides. For more information on configuration files, refer to

Configuration Files on page 91. As shown below, the table specifies the configuration file name and the corresponding parameters. That is, the <MAC>.cfg file contains the *account.1.auto_answer* parameter, and the <y0000000000xx>.cfg file contains the *features.auto_answer_delay* parameter.

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



Summary of Changes

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

Changes for Release 8, Guide Version 9.26

Documentations of the newly released CP960 Skype for Business phones have been added.

Table of Contents

Product Overview

This chapter contains the following information about Skype for Business phones:

- Phone Models
- Expansion Module

Phone Models

This section introduces T48S/T46S/T42S/T41S/CP960 Skype for Business phone models. They are designed to work with Skype for Business Server. These phones are characterized by a large number of functions, which simplify business communication with a high standard of security.

The T48S/T46S/T42S/T41S/CP960 Skype for Business phones provide a powerful and flexible IP communication solution for Ethernet TCP/IP networks, delivering excellent voice quality. When these phones register Skype for Business accounts, you can interact with your Skype for Business contacts list on your phones through Microsoft's Active Directory.

Skype for Business phones comply with the SIP standard (RFC 3261), and they can only be used within a network that supports this model of phone.

For a list of key features available on Yealink Skype for Business phones running the latest firmware, refer to Physical Features of Skype for Business Phones on page 1.

Physical Features of Skype for Business Phones

This section lists the available physical features of T48S/T46S/T42S/T41S/CP960 Skype for Business phones.

T48S

Physical Features:

- 7" 800 x 480 pixel color touch screen with backlight
- 24 bit depth color
- 1 Skype for Business account
- HD Voice: HD Codec, HD Handset, HD Speaker
- 26 dedicated hard keys
- 1*RJ9 (4P4C) handset port
- 1*RJ9 (4P4C) headset port
- 2*RJ45 10/100/1000Mbps Ethernet ports
- 1*RJ12 (6P6C) expansion module port
- 4 LEDs: 1*power, 1*mute, 1*headset, 1*speakerphone
- Power adapter: AC 100~240V input and DC 5V/2A output
- Power over Ethernet (IEEE 802.3af)
- Built-in USB port, support USB flash drive, Bluetooth headset and Wi-Fi
- Wall Mount

T46S

Physical Features:

- 4.3" 480 x 272 pixel color display with backlight
- 24 bit depth color
- 1 Skype for Business account
- HD Voice: HD Codec, HD Handset, HD Speaker
- 36 dedicated hard keys and 4 context-sensitive soft keys
- 1*RJ9 (4P4C) handset port
- 1*RJ9 (4P4C) headset port

- 2*RJ45 10/100/1000Mbps Ethernet ports
- 1*RJ12 (6P6C) expansion module port
- 14 LEDs: 1*power, 10*line, 1*mute, 1*headset, 1*speakerphone
- Power adapter: AC 100~240V input and DC 5V/2A output
- Power over Ethernet (IEEE 802.3af)
- Built-in USB port, support USB flash drive and Bluetooth headset
- Wall Mount

T42S

Physical Features:

- 192 x 64 graphic LCD
- 1 Skype for Business account
- HD Voice: HD Codec, HD Handset, HD Speaker
- 30 dedicated hard keys and 4 context-sensitive soft keys
- 1*RJ9 (4P4C) handset port
- 1*RJ9 (4P4C) headset port
- 2*RJ45 10/100/1000Mbps Ethernet ports
- 1*RJ12 (6P6C) EHS36 headset adapter port
- 10 LEDs: 1*power, 6*line, 1*mute, 1*headset, 1*speakerphone
- Power adapter: AC 100~240V input and DC 5V/1.2A output
- Power over Ethernet (IEEE 802.3af)
- Built-in USB port and support USB flash drive
- Wall Mount

T41S

Physical Features:

- 192 x 64 graphic LCD
- 1 Skype for Business account
- HD Voice: HD Codec, HD Handset, HD Speaker
- 30 dedicated hard keys and 4 context-sensitive soft keys
- 1*RJ9 (4P4C) handset port
- 1*RJ9 (4P4C) headset port
- 2*RJ45 10/100Mbps Ethernet ports
- 1*RJ12 (6P6C) EHS36 headset adapter port
- 10 LEDs: 1*power, 6*line, 1*mute, 1*headset, 1*speakerphone
- Power adapter: AC 100~240V input and DC 5V/1.2A output
- Power over Ethernet (IEEE 802.3af)
- Built-in USB port and support USB flash drive
- Wall Mount

CP960

Physical Features:

- 5" 720 x 1280 pixel color touch screen with backlight
- 1 Skype for Business account
- HD Voice: HD Codec
- 5 Touch keys
- 1*RJ45 10/100Mbps Ethernet ports
- 2*EX mic ports
- 2*USB2.0 ports, support USB flash drive
- 1*3.5mm audio-out port, support external speaker
- 1*Micro USB port (It is unavailable for Skype for Business phones.)
- 2 LED indicators
- Security lock port
- Power over Ethernet (IEEE 802.3af)

Key Features of Skype for Business Phones

In addition to physical features introduced above, Skype for Business phones also support the following key features when running the latest firmware:

- **Phone Features**
  - **Call Options**: emergency call, call waiting, call hold, call mute, call forward, call transfer, group pickup and audio conference.
  - **Basic Features**: live dialpad, dial plan, hotline, caller identity, auto answer.

- **Codecs and Voice Features**
  - Wideband codec: G.722, SILK_WB
  - Narrowband codec: G.711, G.726, G.729, iLBC, G723, SILK_NB
  - VAD, CNG, AEC, PLC, AJB, AGC
  - Full-duplex speakerphone with AEC
  - Built in microphone array, 360 degree voice pickup (only applicable to CP960 Skype for Business phones)
- **Network Features**
  - SIP v1 (RFC2543), v2 (RFC3261)
  - NAT Traversal: STUN, TURN and ICE (TURN and ICE are not applicable to CP960 Skype for Business phones)
  - Proxy mode and peer-to-peer SIP link mode
  - IP assignment: Static/DHCP
  - VLAN assignment: LLDP/Static/DHCP/CDP
  - Bridge mode for PC port (not applicable to CP960 Skype for Business phones)
  - HTTP/HTTPS server
  - DNS client
  - DHCP server
  - IPv6 support
  - Wi-Fi (only applicable to T48S Skype for Business phones)
- **Management**
  - FTP/TFTP/HTTP/HTTPS auto-provision
  - Configuration: browser/phone/auto-provision
  - Dial number via SIP server
  - Dial URL via SIP server
- **Security**
  - HTTPS (server/client)
  - Transport Layer Security (TLS)
  - VLAN (802.1q), QoS
  - Digest authentication using MD5/MD5-sess
  - Secure configuration file via AES encryption

- Phone lock for personal privacy protection
- Admin/User configuration mode
- 802.1X authentication
- Incoming signaling validation

Expansion Module

This section introduces EXP40 expansion modules. EXP40 is only applicable to T48S/T46S Skype for Business phones.

The Yealink EXP40 Expansion Module, with a LCD display, is console you can connect to T48S/T46S Skype for Business phones. You can assign contacts to EXP keys on your EXP40, so that you can quickly call contacts by pressing the corresponding EXP key. You can also monitor your Skype for Business contacts' presence status from your Expansion Module. For more information on assigning contacts to EXP keys, refer to *Yealink_EXP40-Skype_for_Business_Edition_Quick_Start_Guide*.

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

EXP40

Physical Features:

- Rich visual experience with 160 x 320 graphic LCD
- 20 physical keys each with a dual-color LED
- 20 additional keys through page switch
- Supports up to 6 modules daisy-chain
- Expansion module (<=2) is powered by the host phone
- Expansion module (>2) is powered by the power adapter (AC 100~240V input and DC 5V/1.2A output)
- 2*RJ-12 (6P6C) ports for data in and out
- Wall Mount

Getting Started

This chapter provides basic information and installation instructions of Skype for Business phones.

This chapter provides the following sections:

What IP Phones Need to Meet

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

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

Initialization Process Overview

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

Once you connect your phone to the network and to an electrical supply, the 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 phone. The phone comes from the factory with a ROM file preloaded. During initialization, the phone runs a bootstrap loader that loads and executes the ROM file.

Configuring the VLAN

If the phone is connected to a switch, the switch notifies the phone of the VLAN information defined on the switch (if using LLDP or CDP). The 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 50.

Querying the DHCP (Dynamic Host Configuration Protocol) Server

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

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

You need to configure network parameters of the 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 28.

Contacting the provisioning server

If the phone is configured to obtain configurations from the provisioning server, it will connect to the provisioning server, download the configuration file(s) during startup. The phone will be able to resolve and update configurations written in the configuration file(s). If the phone does not obtain configurations from the provisioning server, the phone will use configurations stored in the flash memory. For more information, refer to Setting Up Your Phones with a Provisioning Server on page 86.

Updating firmware

If the access URL of firmware is defined in the configuration file, the 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 phone will perform a firmware update.

You can manually upgrade firmware if the phone does not download firmware from the provisioning server. For more information, refer to Upgrading Firmware on page 96.

Downloading the resource files

In addition to configuration file(s), the 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

For more information on resource files, refer to Resource Files on page 92.

Verifying Startup

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

1. The power LED indicator of T48S/T46S/T42S/T41S Skype for Business phones illuminates solid red.

   The mute touch key LED indicators of CP960 Skype for Business phones illuminate solid red

2. The message “Welcome Initializing… please wait” appears on the LCD screen of T48S/T46S/T42S/T41S Skype for Business phones when the phones start up.

   The message “Initializing…”appears on the touch screen of CP960 Skype for Business phones when the phones start up.

3. The phone enters the login screen.

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

In order to get your 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 phone.

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

- DHCP
- DHCP Option
- Configuring Network Parameters Manually
- Configuring Transmission Methods of the Internet Port and PC Port
- Configuring PC Port Mode
- Web Server Type
- Wi-Fi
- VLAN
- IPv6 Support
- 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. Skype for Business phones comply with the DHCP specifications documented in RFC 2131. If using DHCP, 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 configuration files or locally.

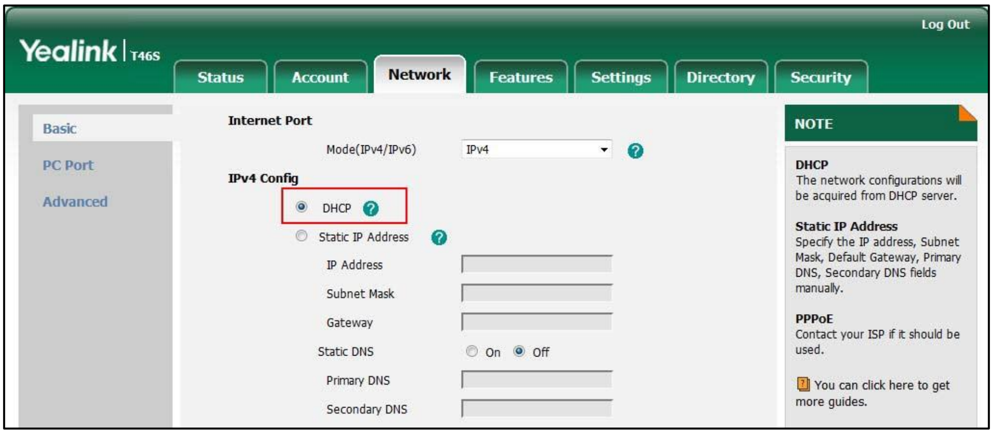
Central Provisioning (Configuration File)	<MAC>.cfg	Configure DHCP on the phone. **Parameter:** static.network.internet_port.type
Local	Web User Interface	Configure DHCP on the phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure DHCP on the phone.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.internet_port.type	**0 or 2**	**0**
Description: Configures the Internet (WAN) 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 phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->WAN Port->IPv4		

To configure DHCP via web user interface:

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



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

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

To configure DHCP via phone user interface:

1. Press **Menu->Advanced** (default password: admin) ->**Network**->**WAN Port**->**IPv4**.
2. Press ◀ or ▶, or the **Switch** soft key to select **DHCP** from the **Type** field.
3. Press the **Save** soft key to accept the change.

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

Static DNS

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

Procedure

Static DNS can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the static DNS feature. **Parameters:** static.network.static_dns_enable
	<MAC>.cfg	Configure static DNS address. **Parameters:** static.network.primary_dns static.network.secondary_dns
Local	Web User Interface	Configure the static DNS feature.

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

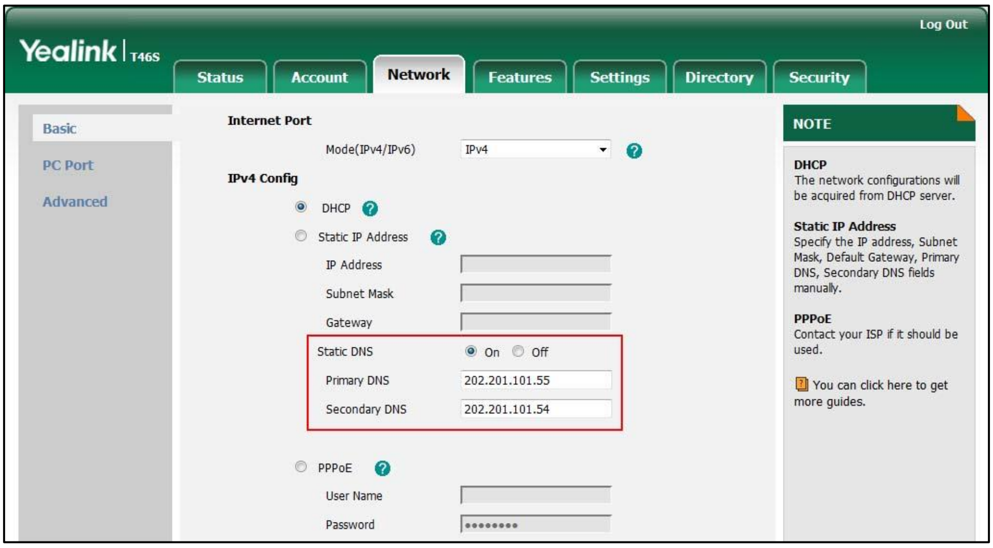
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.static_dns_enable	**0 or1**	**0**
Description: Triggers the static DNS feature to on or off. **0**-Off, the phone will use the IPv4 DNS obtained from DHCP. **1**-On, the 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 phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static DNS **Phone User Interface:** Menu->Advanced (default password: admin)->Network->WAN Port->IPv4->Type (DHCP)->Static DNS		
static.network.primary_dns	**IPv4 Address**	**Blank**
Description: Configures the primary IPv4 DNS server. **Example:** static.network.primary_dns = 202.101.103.55 **Note:** It works only if the value of the parameter "static.network.static_dns_enable" is set to 1 (On). If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->DHCP->Static DNS (On)->Primary DNS **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->WAN Port->IPv4->Type		

Parameters	Permitted Values	Default
(DHCP)->Static DNS (Enabled)->Primary DNS		
static.network.secondary_dns	**IPv4 Address**	**Blank**
Description: Configures the secondary IPv4 DNS server. **Example:** static.network.secondary_dns = 202.101.103.54 **Note:** It works only if the value of the parameter “static.network.static_dns_enable” is set to 1 (On). If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->DHCP->Static DNS (On)->Secondary DNS **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->WAN Port->IPv4->Type (DHCP)->Static DNS (Enabled)->Secondary DNS		

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

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



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

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

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

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

1. Press **Menu->Advanced** (default password: admin) ->**Network**->**WAN Port**->**IPv4**->**DHCP**.
2. Press or , or the **Switch** soft key to select **Enabled** from the **Static DNS** field.
3. Enter the desired values in the **Primary DNS** and **Secondary DNS** fields respectively.
4. Press the **Save** soft key to accept the change.

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

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 phone with the network. Skype for Business 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 phones.

Parameter	DHCP Option	Description
Subnet Mask	1	Specify the client’s subnet mask.
Time Offset	2	Specify the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).
Router	3	Specify a list of IP addresses for routers on the client’s subnet.
Time Server	4	Specify a list of time servers available to the client.
Domain Name Server	6	Specify a list of domain name servers available to the client.
Log Server	7	Specify a list of MIT-LCS UDP servers available to the client.
Host Name	12	Specify the name of the client.
Domain Server	15	Specify the domain name that client should use when resolving hostnames via DNS.
Broadcast Address	28	Specify the broadcast address in use on the client's subnet.

Parameter	DHCP Option	Description
Network Time Protocol Servers	42	Specify a list of NTP servers available to the client by IP address.
Vendor-Specific Information	43 (vendor class ID: CPE-OCPHONE)	Specify virtual local area network (VLAN) ID.
	43 (vendor class ID: MS-UC-Client)	Specify Skype for Business Server pool certificate provisioning service URL.
Vendor Class Identifier	60	Identify the vendor type.
TFTP Server Name	66	Identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.
Boot file Name	67	Identify a boot file when the 'file' field in the DHCP header has been used for DHCP options.
Skype for Business Server	120	Specify a list of Skype for Business Servers available to the client.

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

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

DHCP Option 66 and Option 43

Yealink Skype for Business phones support obtaining the provisioning server address by detecting DHCP options during startup.

The phone will automatically detect the option 66 for obtaining the provisioning server address. DHCP option 66 is used to identify the TFTP server. DHCP option 43 is a vendor-specific option, which is used to transfer the vendor-specific information.

The administrator can use vendor class identifier, specified by DHCP option 60, to send the phone a customized configuration in option 43. Depending on the vendor class ID it is configured for, the option 43 might have different values. Two vendor class identifiers are used when deploying with the Skype for Business Server: a VLAN ID request (vendor class ID: CPE-OCPHONE) and a certificate provisioning service URL request (vendor class ID: MS-UC-Client). For more information on DHCP option 60, refer to DHCP Option 60 on page 23.

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

Procedure

DHCP active can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure DHCP active. **Parameters:** static.auto_provision.dhcp_option.enable
Local	Web User Interface	Configure DHCP active. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-autop&q=load

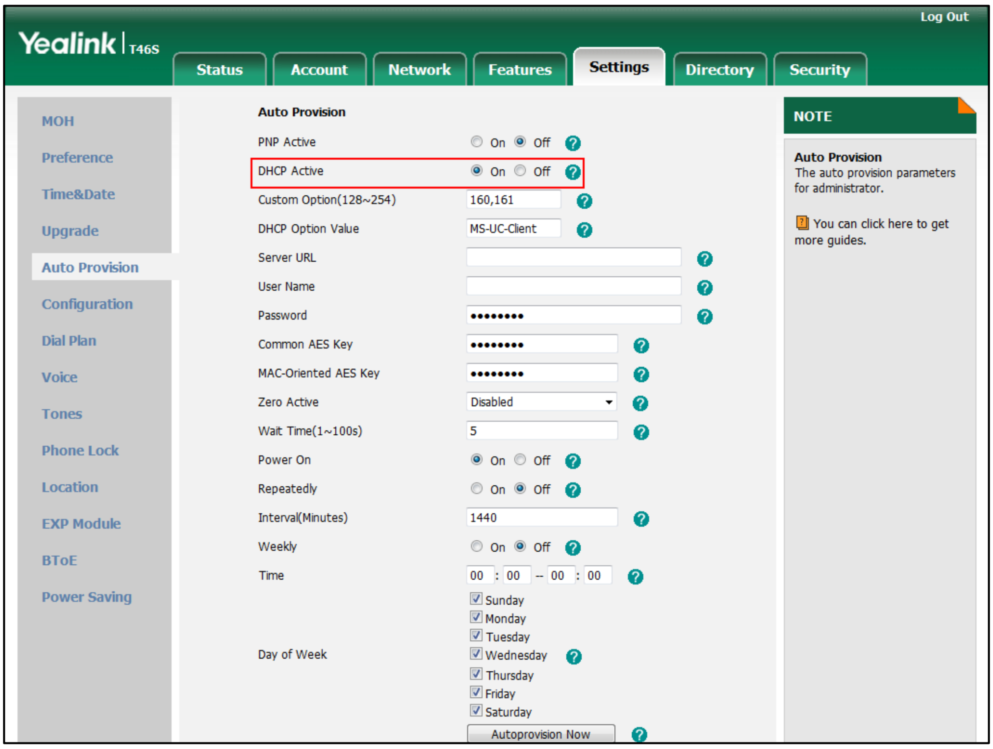
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.auto_provision.dhcp_option.enable	**0 or 1**	**1**
Description: Triggers the DHCP Active feature to on or off. **0**-Off **1**-On, the phone will obtain the provisioning server address by detecting DHCP options. **Web User Interface:** Settings->Auto Provision->DHCP Active **Phone User Interface:** None		

To configure the DHCP Active feature via web user interface:

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

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



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

DHCP Option 160 and Option 161

Yealink Skype for Business phones also support obtaining the provisioning server address by detecting DHCP custom option during startup.

If DHCP Option 66 is not available, you can use custom option (160 or 161) with the URL or IP address of the provisioning server. The phone will automatically detect the option 160 or 161 for obtaining the provisioning server address.

To use DHCP option 160 or option 161, make sure the DHCP Active feature is enabled and custom option is configured.

Procedure

DHCP active can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure DHCP active. **Parameters:** static.auto_provision.dhcp_option.enable
		Configures the custom DHCP option for requesting provisioning server address. static.auto_provision.dhcp_option.list_user_options

Local	Web User Interface	Configure the custom option. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-autop&q=load

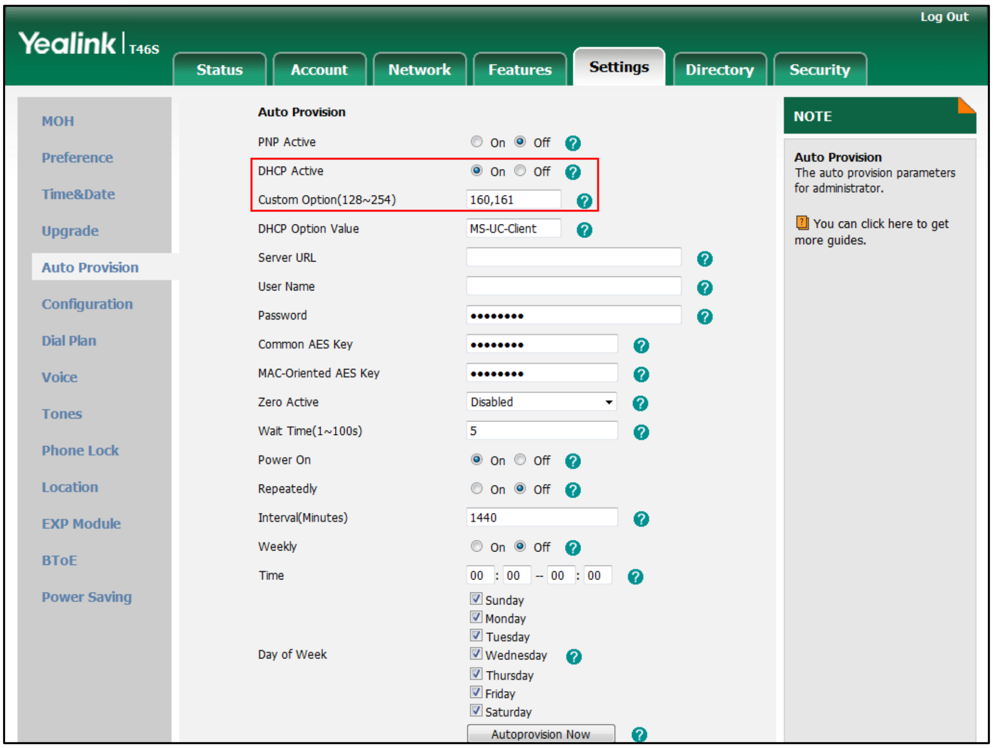
Details of Configuration Parameters:

<table>
<tr><th>Parameters</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 Option feature to on or off.
0-Off
1-On, the phone will obtain the provisioning server address by detecting DHCP options.
Web User Interface:
Settings->Auto Provision->DHCP Active
Phone User Interface:
None</td></tr>
<tr><td>static.auto_provision.dhcp_option.list_user_options</td><td>Integer from 128 to 254</td><td>160,161</td></tr>
<tr><td colspan="3">Configures the custom DHCP option for requesting provisioning server address. Multiple DHCP 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 custom option via web user interface:

1. Click on **Settings**->**Auto Provision**.
2. Mark the **On** radio box in the **DHCP Active** field.

3. Enter the custom option (160 or 161) in the **Custom Option(128~254)** field.



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

Note The phones also support obtaining the provisioning server address via Skype for Business Server (if configured) during sign-in process. This method for obtaining provisioning server address has higher priority than the DHCP option.

DHCP Option 60

DHCP option 60 is used to identify the vendor class ID. By default, the vendor class ID is MS-UC-Client (case-sensitive).

Procedure

DHCP option 60 can be configured using the configuration files or locally.

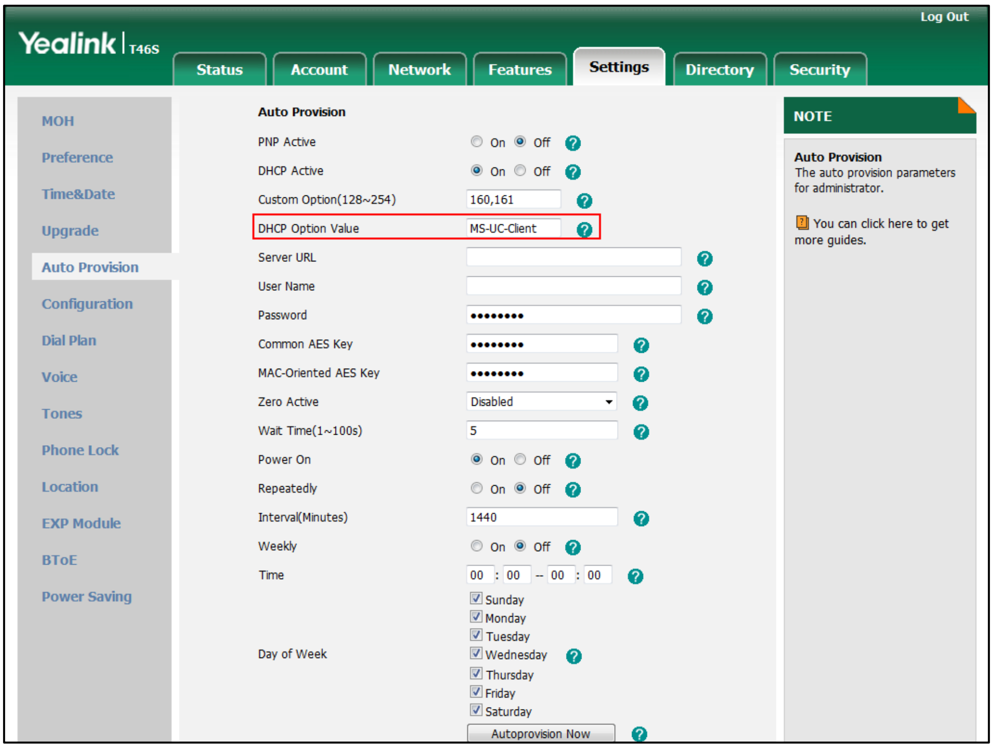
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure DHCP option 60. **Parameters:** static.auto_provision.dhcp_option.option60_value
Local	Web User Interface	Configure DHCP option 60. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-autop&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.auto_provision.dhcp_option.option60_value	**String within 99 characters**	**MS-UC-Client**
Description: Configures the value (vendor class ID) of DHCP option 60. **Web User Interface:** Settings->Auto Provision->DHCP Option Value **Phone User Interface:** None		

To configure DHCP option 60 on the phone via web user interface:

1. Click on **Settings**->**Auto Provision**.
2. Enter the desired host name in the **DHCP Option Value** filed.



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

DHCP Option 42 and Option 2

Yealink Skype for Business 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 path **Settings**->**Time & Date**->**DHCP Time**. For more information on how to configure DHCP time feature, refer to NTP Time Server on page 157.

DHCP Option 12 Hostname

This option specifies the host name of the phone. 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 configuration files or locally.

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

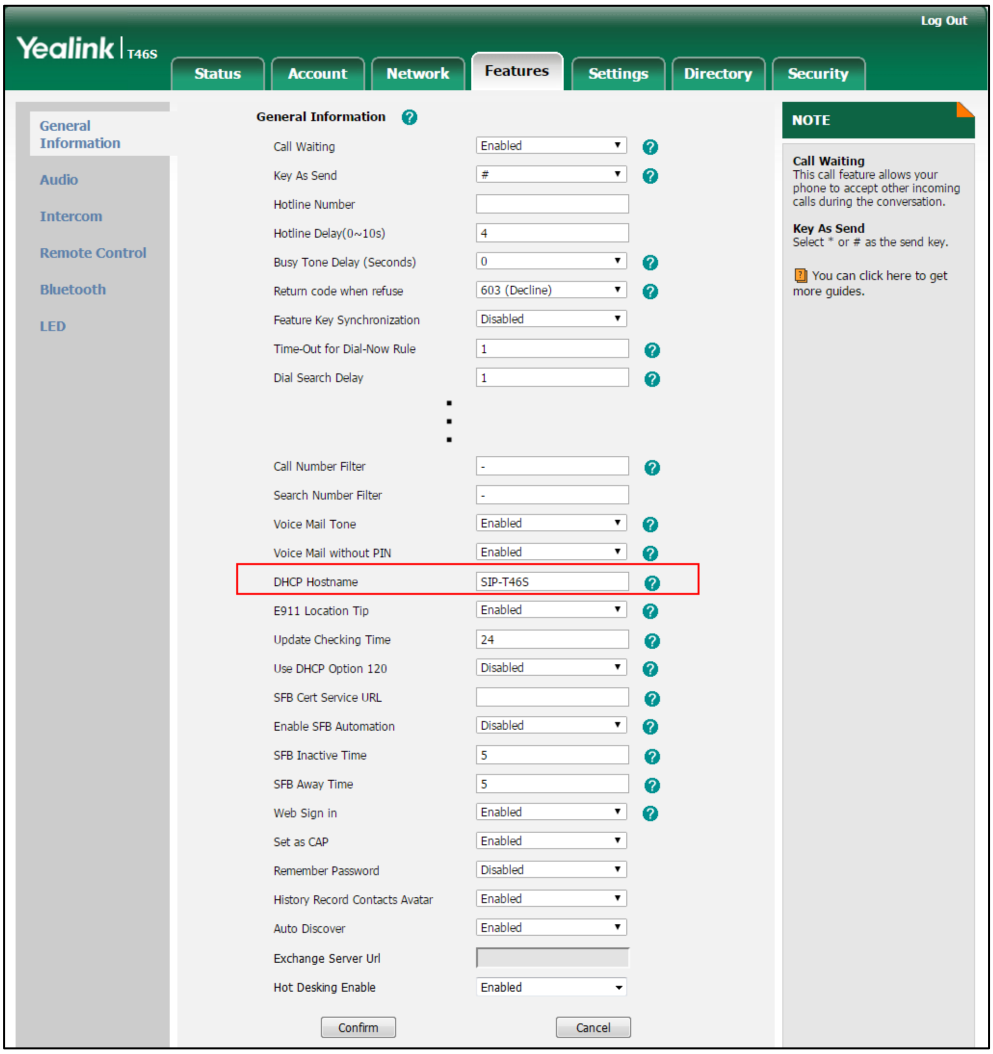
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.dhcp_host_name	**String within 99 characters**	**Refer to the following content**
Description: Configures the DHCP option 12 hostname on phone. **Default Value:** For T48S Skype for Business phones: SIP-T48S For T46S Skype for Business phones: SIP-T46S For T42S Skype for Business phones: SIP-T42S For T41S Skype for Business phones: SIP-T41S For CP960 Skype for Business phones: SIP-CP960 **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Features->General Information->DHCP Hostname **Phone User Interface:**		

Parameters	Permitted Values	Default
None		

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

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



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.

DHCP Option 120

Yealink Skype for Business phones support obtaining Skype for Business Server address from DHCP. DHCP option 120 is used to specify a list of Skype for Business Servers available to the client.

Procedure

DHCP option 120 can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure DHCP option 120. **Parameters:** sip.option120_get_lync_server.enable
Local	Web User Interface	Configure DHCP option 120. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

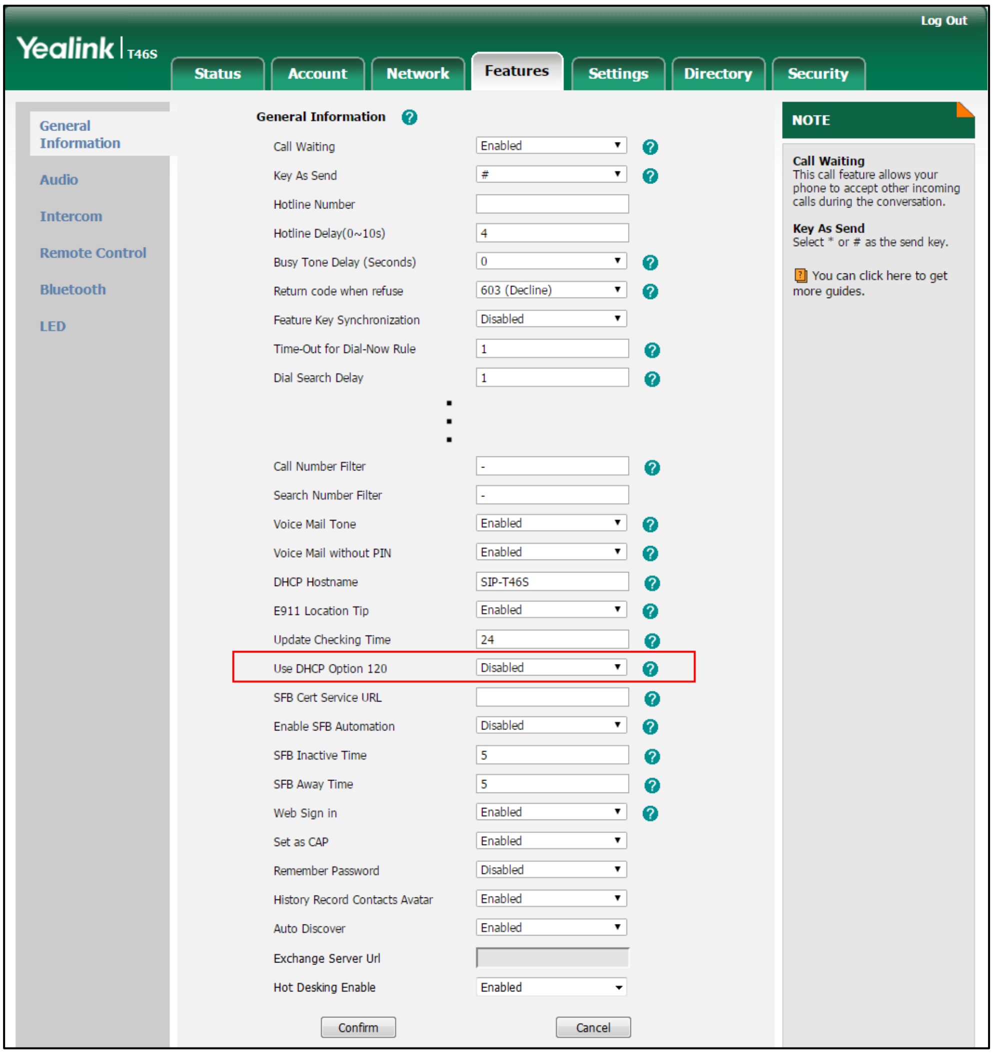
Details of Configuration Parameters:

Parameters	Permitted Values	Default
sip.option120_get_lync_server.enable	**0 or 1**	**0**
Description: Enables or disables phones to obtain the Skype for Business Server address from DHCP by detecting DHCP option 120. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Use DHCP Option 120 **Phone User Interface:** None		

To configure DHCP option 120 via web user interface:

1. Click on **Features->General Information**.

2. Select desired value from the pull-down list of **Use DHCP Option 120**.



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

Configuring Network Parameters Manually

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

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

Procedure

Network parameters can be configured manually using the configuration files or locally.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure network parameters of the 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
Local	Web User Interface	Configure network parameters of the phone manually. **Navigate to**: http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure network parameters of the phone manually.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.internet_port.type	**0 or 2**	**0**
Description: Configures the Internet (WAN) 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 phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config **Phone User Interface:** Menu->Advanced (default password: admin)->Network->WAN Port->IPv4->Type		
static.network.ip_address_mode	**0, 1 or 2**	**0**

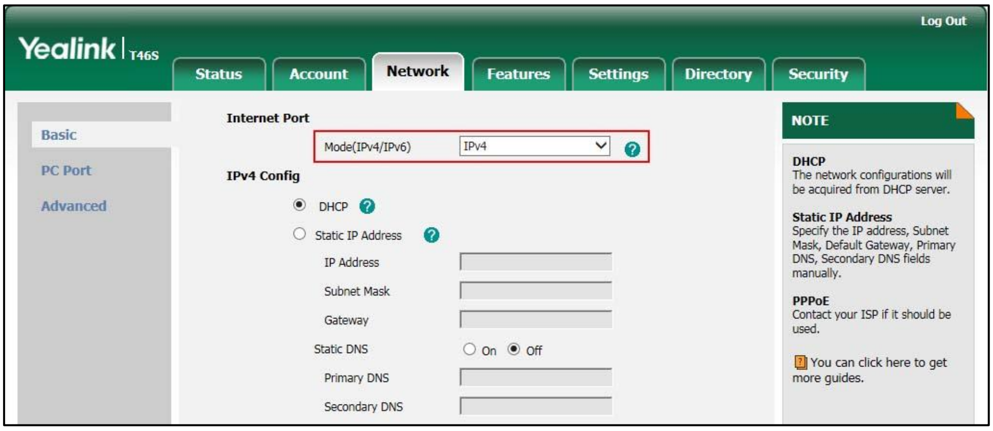
Parameters	Permitted Values	Default
Description: Configures the IP address mode. **0**-IPv4 **1**-IPv6 **2**-IPv4 & IPv6 **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->Internet Port->Mode(IPv4/IPv6) **Phone User Interface:**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

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

Parameters	Permitted Values	Default
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 phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv4 Config->Static IP Address->Static DNS (On)->Secondary DNS **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->WAN Port->IPv4->Type(Static IP) ->Secondary DNS		

To configure the IP address mode via web user interface:

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



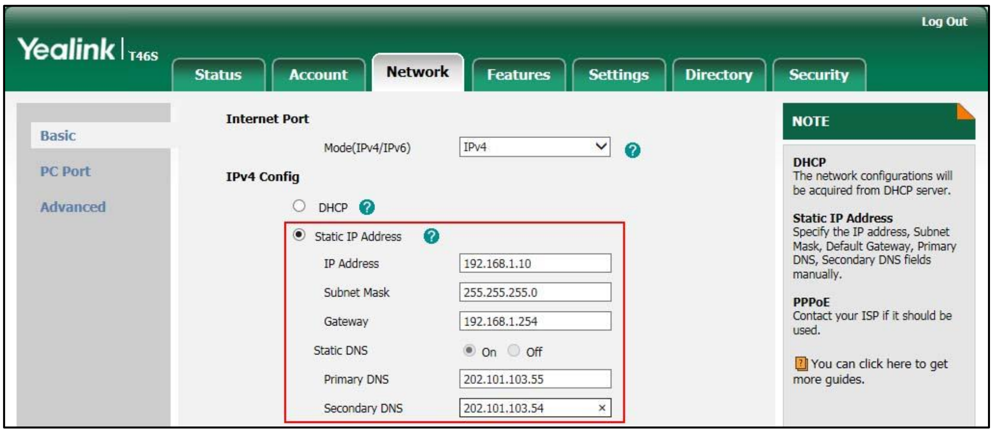
3. Click **Confirm** to accept the change.

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

To configure a static IPv4 address via web user interface:

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

3. Enter the desired values in the **IP Address**, **Subnet Mask**, **Gateway**, **Primary DNS** and **Secondary DNS** fields.



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

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

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

To configure the IP mode via phone user interface:

1. Press **Menu**->**Advanced** (default password: admin)->**Network**->**WAN Port**.
2. Press or , or the **Switch** soft key to select **IPv4**, **IPv6** or **IPv4 & IPv6** from the **IP Mode** field.
3. Press the **Save** soft key to accept the change.

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

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

To configure a static IPv4 address via phone user interface:

1. Press **Menu**->**Advanced** (default password: admin)->**Network**->**WAN Port**->**IPv4**.
2. Press or , or the **Switch** soft key to select the **Static IP** from the **Type** field.
3. Enter the desired value in the **IP Address**, **Subnet Mask**, **Gateway**, **Primary DNS** and **Secondary DNS** field respectively.
4. Press the **Save** soft key to accept the change.

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

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

Configuring Transmission Methods of the Internet Port and PC Port

Yealink T48S/T46S/T42S/T41S Skype for Business phones support two Ethernet ports: Internet port and PC port. The CP960 Skype for Business phones have Internet port only. Three optional methods of transmission configuration for phone Internet or PC Ethernet ports:

- Auto-negotiate
- Half-duplex
- Full-duplex

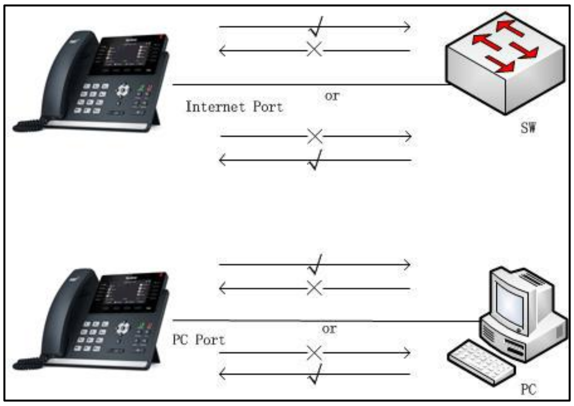
Auto-negotiate is configured for both Internet and PC ports on the phone by default.

Auto-negotiate

Auto-negotiate means that two connected devices choose common transmission parameters (e.g., speed and duplex mode) to transmit voice or data over Ethernet. This process entails devices first sharing transmission capabilities and then selecting the highest performance transmission mode supported by both. You can configure the Internet port and PC port on the phone to automatically negotiate during the transmission.

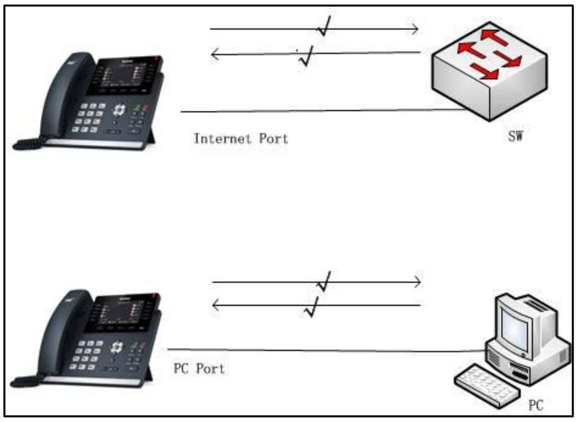
Half-duplex

Half-duplex transmission refers to transmitting voice or data in both directions, but in one direction at a time; this means one device can send data on the line, but not receive data simultaneously. You can configure the half-duplex transmission on both Internet port and PC port for the phone to transmit in 10Mbps or 100Mbps.



Full-duplex

Full-duplex transmission refers to transmitting voice or data in both directions at the same time; this means one device can send data on the line while receiving data. You can configure the full-duplex transmission on both Internet port and PC port for the phone to transmit in 10Mbps, 100Mbps or 1000Mbps (1000Mbps is only applicable to T48S/T46S/T42S Skype for Business phones).



Procedure

The transmission methods of Ethernet ports can be configured using the configuration files or locally.

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

Details of Configuration Parameters:

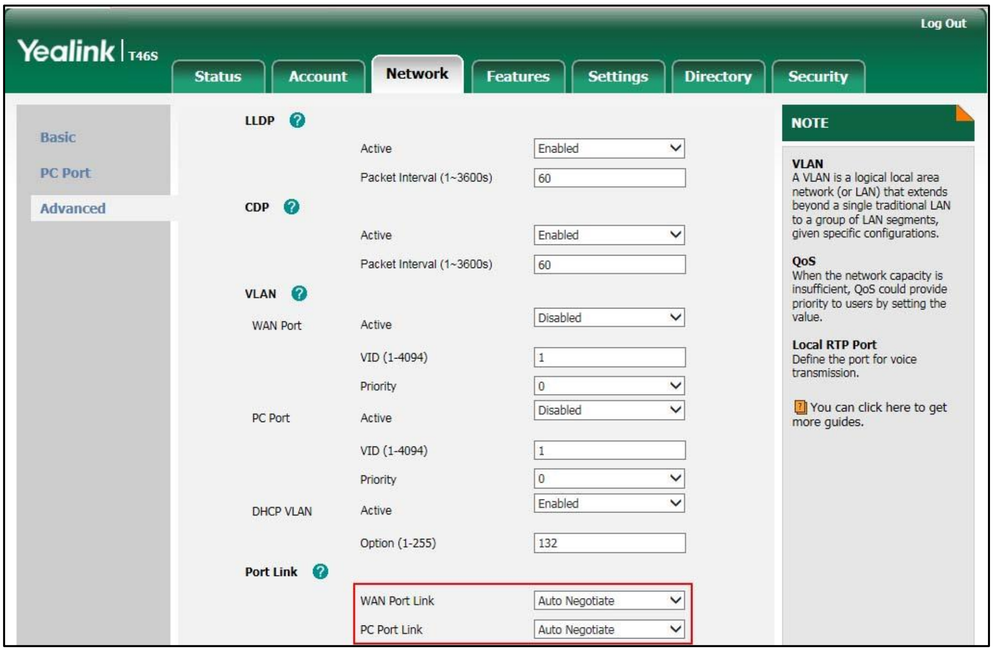
Parameters	Permitted Values	Default
static.network.internet_port.speed_duplex	**0, 1, 2, 3, 4 or 5**	**0**
Description: Configures the transmission method of the Internet (WAN) port.		

Parameters	Permitted Values	Default
0-Auto Negotiate **1**-Full Duplex 10Mbps **2**-Full Duplex 100Mbps **3**-Half Duplex 10Mbps **4**-Half Duplex 100Mbps **5**-Full Duplex 1000Mbps (only applicable to T48S/T46S/T42S Skype for Business phones) **Note**: For T48S/T46S/T42 Skype for Business phones, you can set the transmission speed to 1000Mbps/Auto Negotiation to transmit in 1000Mbps if the phone is connected to the switch supports Gigabit Ethernet. We recommend that you do not change this parameter. If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Port Link->WAN Port Link **Phone User Interface:** None		
static.network.pc_port.speed_duplex	**0, 1, 2, 3 ,4 or 5**	**0**
Description: Configures the transmission method of the PC (LAN) port. **0**-Auto Negotiate **1**-Full Duplex 10Mbps **2**-Full Duplex 100Mbps **3**-Half Duplex 10Mbps **4**-Half Duplex 100Mbps **5**-Full Duplex 1000Mbps (only applicable to T48S/T46S/T42S Skype for Business phones) **Note**: It works only if the value of the parameter "static.network.pc_port.enable" is set to 1 (Auto Negotiation). It is not applicable to CP960 Skype for Business phones. For T48S/T46S/T42 Skype for Business phones, you can set the transmission speed to 1000Mbps/Auto Negotiation to transmit in 1000Mbps if the phone is connected to the switch supports Gigabit Ethernet. We recommend that you do not change this parameter. If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Port Link->PC Port Link **Phone User Interface:** None		

To configure the transmission methods of Ethernet ports via web user interface:

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

2. Select the desired value from the pull-down list of **WAN Port Link**.
3. Select the desired value from the pull-down list of **PC Port Link**.



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

Configuring PC Port Mode

The PC port on the back of the phone is used to connect a PC. You can enable or disable the PC (LAN) port on the phones via web user interface or using configuration files. PC port is not applicable to CP960 Skype for Business phones.

Procedure

PC port mode can be configured using the configuration files or locally.

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

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.pc_port.enable	**0 or 1**	**1**
Description: Enables or disables the PC port. **0**-Disabled **1**-Auto Negotiation **Note:** If you change this parameter, the phone will reboot to make the change take effect. It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Network->PC Port->PC Port Active **Phone User Interface:** None		

To enable the PC port via web user interface:

1. Click on **Network**->**PC Port**.
2. Select **Auto Negotiate** from the pull-down list of **PC Port Active**.

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

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

To disable the PC port via web user interface:

1. Click on **Network**->**PC Port**.
2. Select **Disabled** from the pull-down list of **PC Port Active**.

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

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

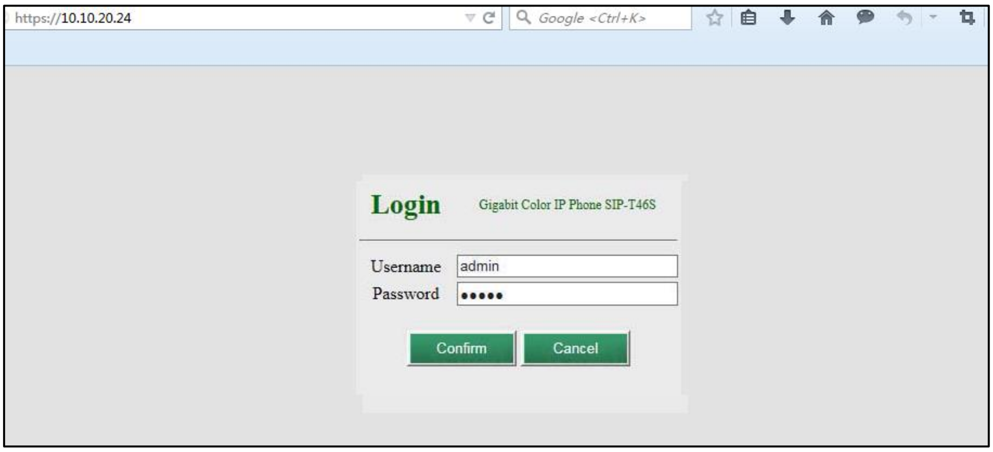
4. Click **OK** to reboot the phone.

Web Server Type

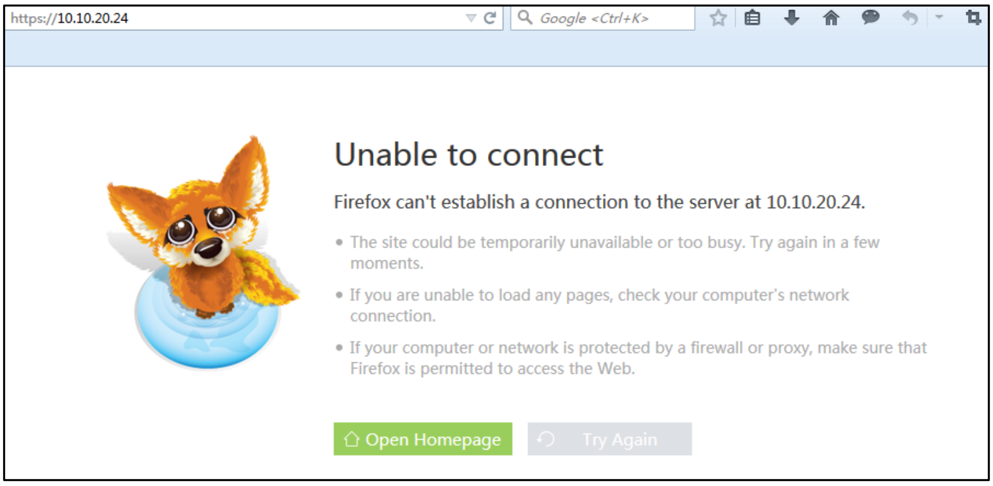
Web server type determines access protocol of the phone's web user interface. Skype for Business phones support both HTTP and HTTPS protocols for accessing the web user interface. This can be disabled when it is not needed or when it poses a security threat. For more information on accessing the web user interface, refer to Web User Interface on page 89.

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

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



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



Procedure

Web server type can be configured using the configuration files or locally.

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

Details of Configuration Parameters:

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

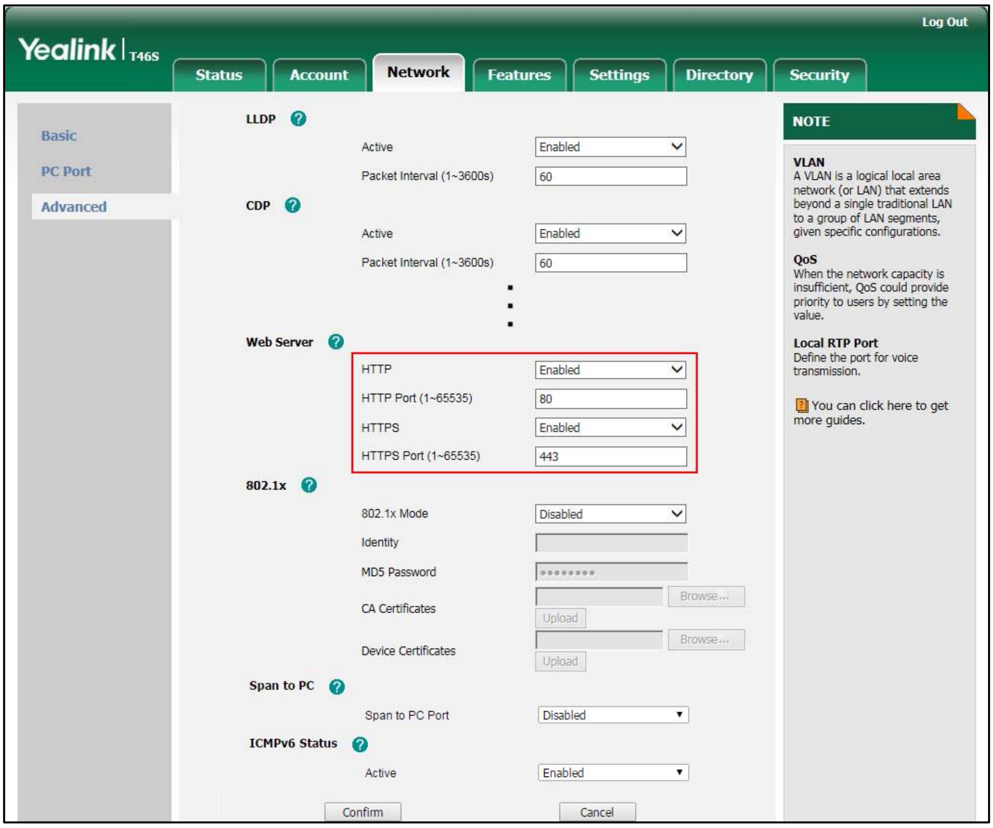
Parameters	Permitted Values	Default
Note: If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Web Server->HTTP Port(1~65535) **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->Webserver Type->HTTP Port		
static.wui.https_enable	**0 or 1**	**1**
Description: Enables or disables the user to access web user interface of the phone using the HTTPS protocol. **0**-Disabled **1**-Enabled **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Web Server->HTTPS **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->Webserver Type->HTTPS Status		
static.network.port.https	**Integer from 1 to 65535**	**443**
Description: Configures the HTTPS port for the user to access web user interface of the phone using the HTTPS protocol. **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Web Server->HTTPS Port (1~65535) **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->Webserver Type->HTTPS Port		

To configure web server type via web user interface:

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

   The default HTTP port number is 80.
4. Select the desired value from the pull-down list of **HTTPS**.
5. Enter the desired HTTPS port number in the **HTTPS Port (1~65535)** field.

The default HTTPS port number is 443.



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

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

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

To configure web server type via phone user interface:

1. Press **Menu**->**Advanced** (default password: admin)->**Network**->**Webserver Type**.
2. Press or , or the **Switch** soft key to select the desired value from the **HTTP Status** field.
3. Enter the desired HTTP port number in the **HTTP Port** field.
4. Press or , or the **Switch** soft key to select the desired value from the **HTTP Status** field.
5. Enter the desired HTTPS port number in the **HTTPS Port** field.
6. Press the **Save** soft key to accept the change.

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

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

Wi-Fi

Wi-Fi feature enables users to connect their phones to the organization's wireless network. The wireless network is more convenient and cost-effective than wired network. Wi-Fi feature is only applicable to T48S Skype for Business phones.

When the Wi-Fi feature is enabled, the phone will automatically scan the available wireless networks. All the available wireless networks will display in scanning list on the touch screen. You can store up to 5 frequently-used wireless networks on your phone and specify the priority for them.

Note

> To use Wi-Fi feature, make sure the Wi-Fi USB dongle is properly connected to the USB port on the back of the phone.
>
> When you connect the Ethernet cable, you can enable the Wi-Fi feature. But you have to disable the Wi-Fi feature if you want to use the wired network.

Procedure

Wi-Fi feature can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure Wi-Fi feature. **Parameter:** static.wifi.enable
		Configure the Wi-Fi settings. **Parameters:** static.wifi.X.label static.wifi.X.ssid static.wifi.X.priority static.wifi.X.security_mode static.wifi.X.cipher_type static.wifi.X.password static.wifi.X.eap_type static.wifi.X.eap_user_name static.wifi.X.eap_password
Web User Interface		Configure Wi-Fi feature. Configure the Wi-Fi settings. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-wifi&q=load
Phone User Interface		Configure Wi-Fi feature. Configure the Wi-Fi settings.

Details of the Configuration Parameters:

Parameters	Permitted Values	Default
static.wifi.enable	**0 or 1**	**0**
Description: Enables or disables the Wi-Fi feature. **0**-Disabled **1**-Enabled **Note:** It is only applicable to T48S Skype for Business phones. **Web User Interface:** Network->Wi-Fi->Wi-Fi Active **Phone User Interface:** Menu->Basic->Wi-Fi->Wi-Fi		
static.wifi.X.label (X ranges from 1 to 5)	**String within 32 characters**	**Blank**
Description: Configures the profile name of the wireless network X for the phone. **Note**: It works only if the value of the parameter "static.wifi.enable" is set to 1 (Enabled). It is only applicable to T48S Skype for Business phones. **Web User Interface:** Network->Wi-Fi->Profile Name **Phone User Interface:** Menu->Basic->Wi-Fi->Wi-Fi(On)->Add->Profile Name or Menu->Basic->Wi-Fi->Wi-Fi(On)->The storage network->Edit->Profile Name		
static.wifi.X.ssid (X ranges from 1 to 5)	**String within 32 characters**	**Blank**
Description: Configures the Service Set Identifier (SSID) of the wireless network X. SSID is a unique identifier for accessing wireless access points. **Note**: It works only if the value of the parameter "static.wifi.enable" is set to 1 (Enabled). It is only applicable to T48S Skype for Business phones. **Web User Interface:** Network->Wi-Fi->SSID **Phone User Interface:** Menu->Basic->Wi-Fi->Wi-Fi(On)->Add->SSID or		

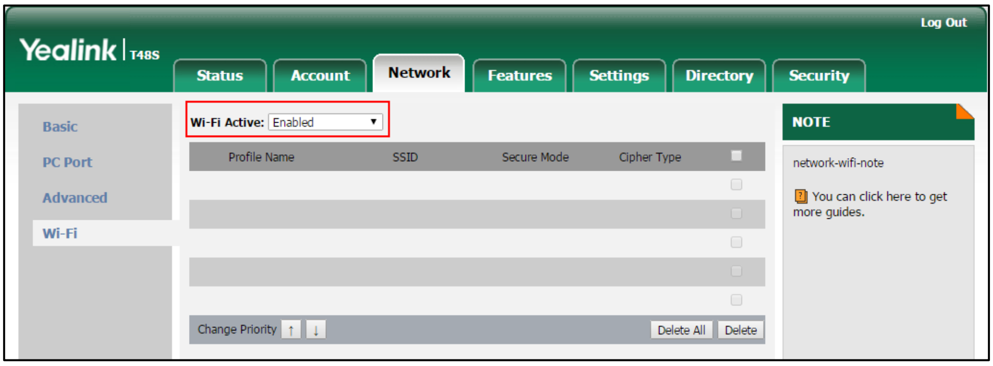
Parameters	Permitted Values	Default
Menu->Basic->Wi-Fi->Wi-Fi(On)->The storage network->Edit->SSID		
static.wifi.X.priority (X ranges from 1 to 5)	**Integer from 1 to 5**	**1**
Description: Configures the priority for the wireless network X for the Skype for Business phone. 5 is the highest priority, 1 is the lowest priority. **Note**: It works only if the value of the parameter "static.wifi.enable" is set to 1 (Enabled). It is only applicable to T48S Skype for Business phones. **Web User Interface:** Network->Wi-Fi->Change Priority **Phone User Interface:** Menu->Basic->Wi-Fi(On)->The storage network->Move Up/Move Down		
static.wifi.X.security_mode (X ranges from 1 to 5)	**NONE, WEP, WPA-PSK or WPA2-PSK, WPA-EAP or WPA2-EAP**	**NONE**
Description: Configures the security mode of the wireless network X. **Note**: It works only if the value of the parameter "static.wifi.enable" is set to 1 (Enabled). It is only applicable to T48S Skype for Business phones. **Web User Interface:** Network->Wi-Fi->Secure Mode **Phone User Interface:** Menu->Basic->Wi-Fi->Wi-Fi(On)->Add->Security Mode or Menu->Basic->Wi-Fi->Wi-Fi(On)->The storage network-> Edit->Security Mode		
static.wifi.X.cipher_type (X ranges from 1 to 5)	**NONE, WEP, TKIP, AES or TKIP AES**	**NONE**
Description: Configures the encryption type of the wireless network X. If the value of the parameter "static.wifi.X.security_mode" is set to **NONE**, the permitted value of this parameter is **NONE**. If the value of the parameter "static.wifi.X.security_mode" is set to **WEP**, the permitted value of this parameter is **WEP**. If the value of the parameter "static.wifi.X.security_mode" is set to other values, the permitted values of this parameter are **TKIP**, **AES** or **TKIP AES**.		

Parameters	Permitted Values	Default
Note: It works only if the value of the parameter "static.wifi.enable" is set to 1 (Enabled). It is only applicable to T48S Skype for Business phones. **Web User Interface:** Network->Wi-Fi->Cipher Type **Phone User Interface:** Menu->Basic->Wi-Fi->Wi-Fi(On)->Add->Cipher Type or Menu->Basic->Wi-Fi->Wi-Fi(On)->The storage network->Edit->Cipher Type		
static.wifi.X.password (X ranges from 1 to 5)	**String within 64 characters**	**Blank**
Description: Configures the password of the wireless network X. **Note**: It works only if the value of the parameter "static.wifi.enable" is set to 1 (Enabled) and "static.wifi.X.security_mode" is set to **WEP**, **WPA-PSK** or **WPA2-PSK**. It is only applicable to T48S Skype for Business phones. **Web User Interface:** Network->Wi-Fi->PSK **Phone User Interface:** Menu->Basic->Wi-Fi->Wi-Fi(On)->Add->WPA Shared Key or Menu->Basic->Wi-Fi->Wi-Fi(On)->The storage network->Edit->WPA Shared Key		
static.wifi.X.eap_type (X ranges from 1 to 5)	**TTLS, PEAP or TLS**	**Blank**
Description: Configures the EAP authentication mode of the wireless network X. **Note**: It works only if the value of the parameter "static.wifi.enable" is set to 1 (Enabled) and "static.wifi.X.security_mode" is set to **WPA-EAP** or **WPA2-EAP**. It is only applicable to T48S Skype for Business phones. **Web User Interface:** None **Phone User Interface:** None		
static.wifi.X.eap_user_name (X ranges from 1 to 5)	**String within 32 characters**	**Blank**
Description: Configures the EAP authentication username of the wireless network X.		

Parameters	Permitted Values	Default
Note: It works only if the value of the parameter "static.wifi.enable" is set to 1 (Enabled), "static.wifi.X.security_mode" is set to **WPA-EAP** or **WPA2-EAP** and the value of the parameter "static.wifi.X.eap_type" is set to **TTLS** or **PEAP**. It is only applicable to T48S Skype for Business phones. **Web User Interface:** Network->Wi-Fi->User Name **Phone User Interface:** Menu->Basic->Wi-Fi->Wi-Fi(On)->Add->User Name or Menu->Basic->Wi-Fi->Wi-Fi(On)->The storage network->Edit->User Name		
static.wifi.X.eap_password (X ranges from 1 to 5)	**String within 64 characters**	**Blank**
Description: Configures the EAP authentication password of the wireless network X. **Note**: It works only if the value of the parameter "static.wifi.enable" is set to 1 (Enabled) and "static.wifi.X.security_mode" is set to **WPA-EAP** or **WPA2-EAP**. It is only applicable to T48S Skype for Business phones. **Web User Interface:** Network->Wi-Fi->PSK **Phone User Interface:** Menu->Basic->Wi-Fi->Wi-Fi(On)->Add->WPA Shared Key or Menu->Basic->Wi-Fi->Wi-Fi(On)->The storage network-> Edit->WPA Shared Key		

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

1. Click on **Network**->**Wi-Fi**.
2. Select **Enabled** from the pull-down list of **Wi-Fi Active**.



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

o add a wireless network via web user interface:

1. Click on **Network**->**Wi-Fi**.
2. Enter the profile name of the wireless network in the **Profile Name** field.
3. Enter the Service Set Identifier (SSID) of the wireless network in the **SSID** field.
4. Select the security mode of the wireless network from the pull-down list of **Secure Mode**.

   - If you select **WEP**:

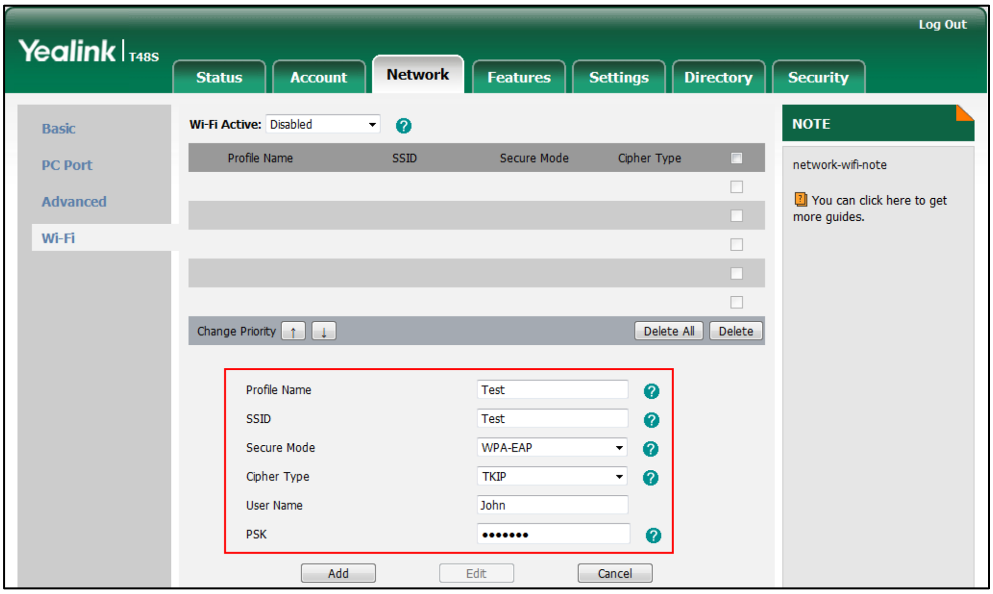
     1) Enter the password of the wireless network in the **PSK** field.

   - If you select **WPA-PSK** or **WPA2-PSK**:

     1) Select the encryption type of the wireless network (**TKIP**, **AES** or **TKIP AES**) from the pull-down list of the **Cipher Type**.
     2) Enter the password of the wireless network in the **PSK** field.

   - If you select **WPA-EAP** or **WPA2-EAP**:

     1) Select the encryption type of the wireless network (**TKIP**, **AES** or **TKIP AES**) from the pull-down list of the **Cipher Type**.
     2) Enter the desired username in the **User Name** field.
     3) Enter the password of the wireless network in the **PSK** field.

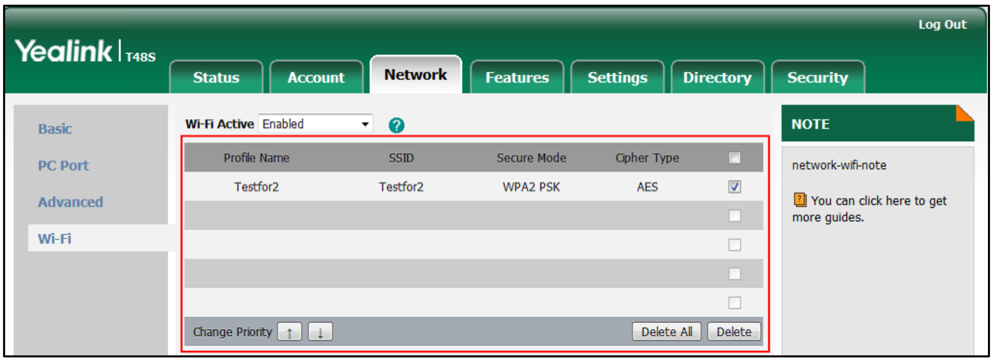


5. Click **Add** to accept the change.
6. Repeat steps 2 to 5 to add more wireless networks.

To adjust the priority of the added wireless network via web user interface:

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

2. Click to select the desired wireless network which you want to adjust the priority, and then click ↑ or ↓ .



3. Repeat the step 2 to adjust the priority of more wireless networks.

To activate the Wi-Fi mode via phone user interface:

1. Tap **Menu**->**Basic**->**Wi-Fi**.
2. Tap the **On** radio box of the **Wi-Fi** field.

   The phone scans the available wireless network automatically.

To add a wireless network:

1. Tap **Menu**->**Basic**->**Wi-Fi**.
2. Tap the **On** radio box of the **Wi-Fi** field.
3. The phone scans the available wireless network automatically.
4. Tap the **Add** soft key.
5. Use the WLAN settings obtained from your gateway/router to configure this WLAN Profile on the phone. Do the following:

   a) If you select **None** or **WEP** from the pull-down list of **Security Mode**:

      Enter the profile name, SSID and WPA shared key in the corresponding fields.

   b) If you select **WPA-PSK** or **WPA2-PSK** from the pull-down list of **Security Mode**:

      Select the desired Cipher type (**TKIP**, **AES** or **TKIP AES**) from the pull-down list of **Cipher Type**.

      Enter the profile name, SSID and WPA shared key in the corresponding fields.

   c) If you select **WPA-EAP** or **WPA2-EAP** from the pull-down list of **Security Mode**:

      Select the desired Cipher type (**TKIP**, **AES** or **TKIP AES**) from the pull-down list of **Cipher Type**.

      Enter the profile name, SSID, username and WPA shared key in the corresponding fields.

6. Tap the **Save** soft key to accept the change.

VLAN

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

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

VLAN on phones allows simultaneous access for a regular PC. This feature allows a PC to be daisy chained to a phone and the connection for both PC and phone to be trunked through the same physical Ethernet cable.

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

For more information on VLAN, refer to *VLAN Feature on Yealink Skype for Business phones*.

LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows the phone 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. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value (TLV) elements, each of which contains a particular type of information about the device or port transmitting it.

LLDP-MED (Media Endpoint Discovery)

LLDP-MED is published by the Telecommunications Industry Association (TIA). It is an extension to LLDP that operates between endpoint devices and network connectivity devices. LLDP-MED provides the following capabilities for the endpoint:

- Capabilities Discovery -- allows LLDP-MED endpoint to determine the capabilities that the connected switch supports and has enabled.
- Network Policy -- provides voice VLAN configuration to notify the phone which VLAN to use and QoS-related configuration for voice data. It provides a “plug and play” network environment.
- Power Management -- provides information related to how the phone is powered, power priority, and how much power the endpoint needs.
- Inventory Management -- provides a means to effectively manage the phone and its attributes, such as model number, serial number and software revision.

TLVs supported by the phone are summarized in the following table:

TLV Type	TLV Name	Description
Mandatory TLVs	Chassis ID	The network address of the phone.
	Port ID	The MAC address of the phone.
	Time To Live	Seconds until data unit expires. The default value is 180s.
	End of LLDPDU	Marks end of LLDPDU.
Optional TLVs	System Name	Name assigned to the phone. The default value is “SIP-T46S”.
	System Description	Description of the phone. Description includes firmware version of the phone.
	Capabilities	The supported and enabled phone capabilities. The Telephone capability is supported and enabled by default.
	Port Description	Description of port that sends data unit. The default value is “WAN PORT”.
IEEE Std 802.3 Organizationally Specific TLV	MAC/PHY Configuration/Status	Duplex mode and network speed settings of the phone. The Auto Negotiation is supported and enabled by default. The advertised capabilities of PMD. Auto-Negotiation is: 100BASE-TX (full duplex mode) 100BASE-TX (half duplex mode) 10BASE-T (full duplex mode) 10BASE-T (half duplex mode)
TIA Organizationally Specific TLVs	Media Capabilities	The MED device type of the phone and the supported LLDP-MED TLV type can be encapsulated in LLDPDU. The supported LLDP-MED TLV types are: LLDP-MED Capabilities, Network Policy, Extended Power via MDI-PD, Inventory.
	Network Policy	Port VLAN ID, application type, L2 priority and DSCP value.

TLV Type	TLV Name	Description
	Extended Power-via-MDI	Power type, source, priority and value.
	Inventory – Hardware Revision	Hardware revision of the phone.
	Inventory – Firmware Revision	Firmware revision of the phone.
	Inventory – Software Revision	Software revision of the phone.
	Inventory – Serial Number	Serial number of the phone.
	Inventory – Manufacturer Name	Manufacturer name of the phone. The default value is "Yealink".
	Inventory – Model Name	Model name of the phone. The default value is "T46S".
	Asset ID	Assertion identifier of the phone.

Procedure

LLDP can be configured using the configuration files or locally.

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

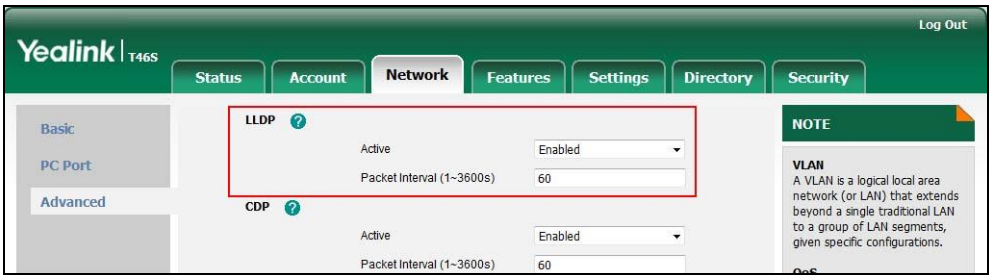
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.lldp.enable	**0 or 1**	**1**
Description: Enables or disables the LLDP (Linker Layer Discovery Protocol) feature on the phone.		

Parameters	Permitted Values	Default
0-Disabled **1**-Enabled, the phone will attempt to determine its VLAN ID through LLDP. **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->LLDP->Active **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->LLDP->LLDP Status		
static.network.lldp.packet_interval	**Integer from 1 to 3600**	**60**
Description: Configures the interval (in seconds) for the 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 phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->LLDP->Packet Interval (1~3600s) **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->LLDP->Packet Interval		

To configure LLDP via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **LLDP** block, select the desired value from the pull-down list of **Active**.
3. Enter the desired time interval in the **Packet Interval (1~3600s)** field.



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

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

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

To configure LLDP feature via phone user interface:

1. Press **Menu**->**Advanced** (default password: admin) ->**Network**->**LLDP**->**LLDP Status**.
2. Press or , or the **Switch** soft key to select the desired value from the **LLDP Status** field.
3. Enter the priority value (1-3600s) in the **Packet Interval** field.
4. Press the **Save** soft key to accept the change.

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

CDP

CDP (Cisco Discovery Protocol) allows phones to receive and/or transmit device-related information from/to directly connected devices on the network that are also using the protocol, and store the information about other devices.

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

Procedure

CDP can be configured using the configuration files or locally.

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

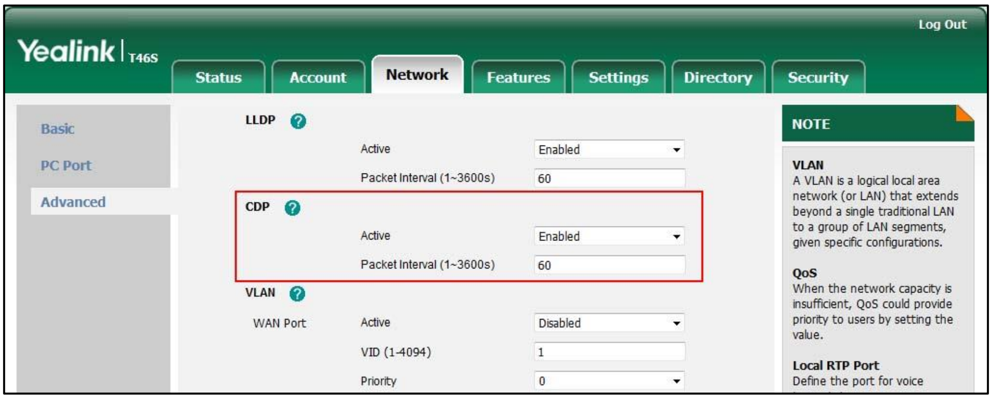
Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.cdp.enable	**0 or 1**	**1**

Parameters	Permitted Values	Default
Description: Enables or disables the CDP (Cisco Discovery Protocol) feature on the phone. **0**-Disabled **1**-Enabled, the phone will attempt to determine its VLAN ID through CDP. **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->CDP->Active **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->CDP->CDP Status		
static.network.cdp.packet_interval	**Integer from 1 to 3600**	**60**
Description: Configures the interval (in seconds) for the phone to send the CDP (Cisco Discovery Protocol) request. **Note:** It works only if the value of the parameter "network.cdp.enable" is set to 1 (Enabled). If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->CDP->Packet Interval (1~3600s) **Phone User Interface:** Menu->Advanced (default password: admin)->Network->CDP->Packet Interval		

To configure CDP via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **CDP** block, select the desired value from the pull-down list of **Active**.
3. Enter the desired time interval in the **Packet Interval (1~3600s)** field.



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

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

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

To configure CDP feature via phone user interface:

1. Press **Menu**->**Advanced** (default password: admin) ->**Network**->**CDP**->**CDP Status**.
2. Press or , or the **Switch** soft key to select the desired value from the **CDP Status** field.
3. Enter the priority value (1-3600s) in the **Packet Interval** field.
4. Press the **Save** soft key to accept the change.

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

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

Manual Configuration for VLAN in the Wired Network

VLAN is disabled on phones by default. You can configure VLAN for the Internet port and PC port manually. For CP960 Skype for Business phones, you can only configure VLAN for the Internet port manually, because they only have Internet port. Before configuring VLAN on the phone, you need to obtain the VLAN ID from your network administrator.

Procedure

VLAN can be configured using the configuration files or locally.

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

Details of Configuration Parameters:

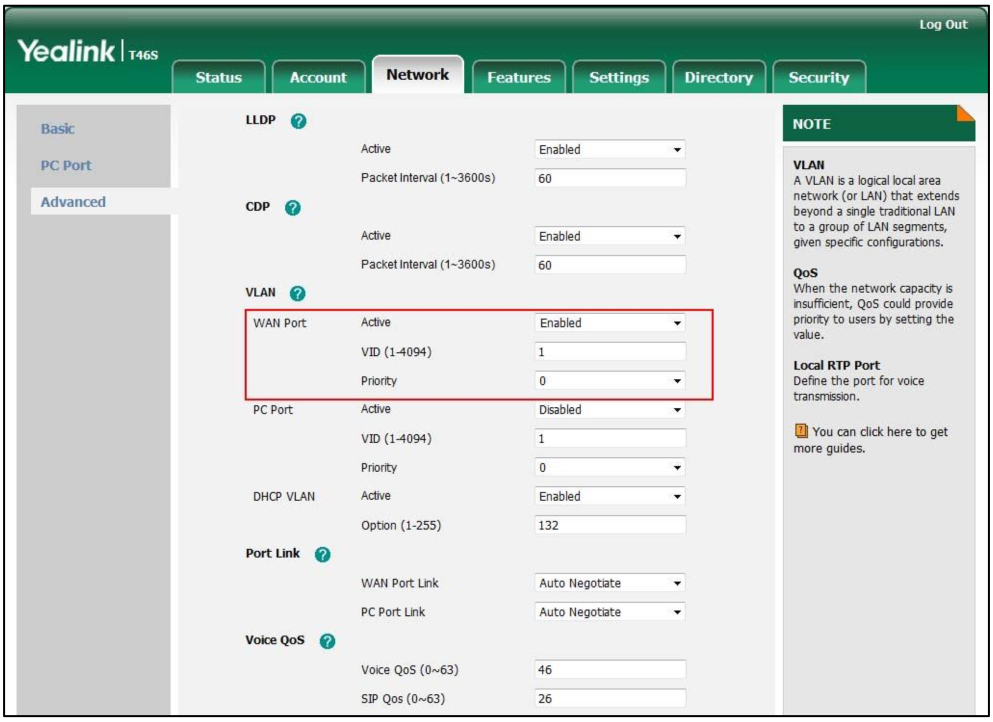
Parameters	Permitted Values	Default
static.network.vlan.internet_port_enable	**0 or 1**	**0**
Description: Enables or disables VLAN for the Internet (WAN) port. **0**-Disabled **1**-Enabled **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN->WAN Port->Active **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->VLAN->WAN Port->VLAN Status		
static.network.vlan.internet_port_vid	**Integer from 1 to 4094**	**1**
Description: Configures VLAN ID for the Internet (WAN) port. **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN->WAN Port->VID (1-4094) **Phone User Interface:** Menu->Advanced (default password: admin)->Network->VLAN->WAN Port->VID Number		
static.network.vlan.internet_port_priority	**Integer from 0 to 7**	**0**
Description: Configures VLAN priority for the Internet (WAN) port. 7 is the highest priority, 0 is the lowest priority. **Note:** It works only if the value of the parameter "static.network.vlan.internet_port_enable" is set to 1 (Enabled). If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN->WAN Port->Priority **Phone User Interface:**		

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

Parameters	Permitted Values	Default
It is not applicable to CP960 Skype for Business phones. If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN->PC Port->Priority **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->VLAN->PC Port->Priority		

To configure VLAN for Internet (WAN) port via web user interface:

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



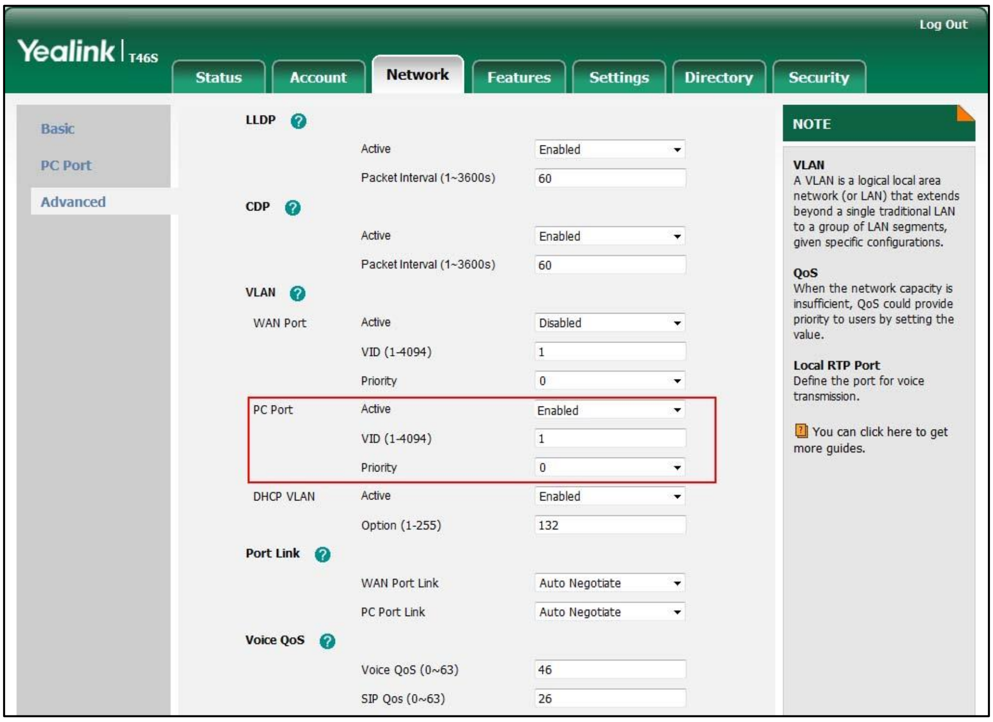
5. Click **Confirm** to accept the change.

   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 PC port via web user interface:

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

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



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

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

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

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

1. Press **Menu->Advanced** (default password: admin) ->**Network**->**VLAN**->**WAN Port** (or **PC Port**).
2. Press ◀ or ▶, or the **Switch** soft key to select the desired value from the **VLAN Status** field.
3. Enter the VLAN ID (1-4094) in the **VID Number** field.
4. Enter the priority value (0-7) in the **Priority** field.
5. Press the **Save** soft key to accept the change.

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

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

DHCP VLAN

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

Procedure

DHCP VLAN can be configured using the configuration files or locally.

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

Details of Configuration Parameters:

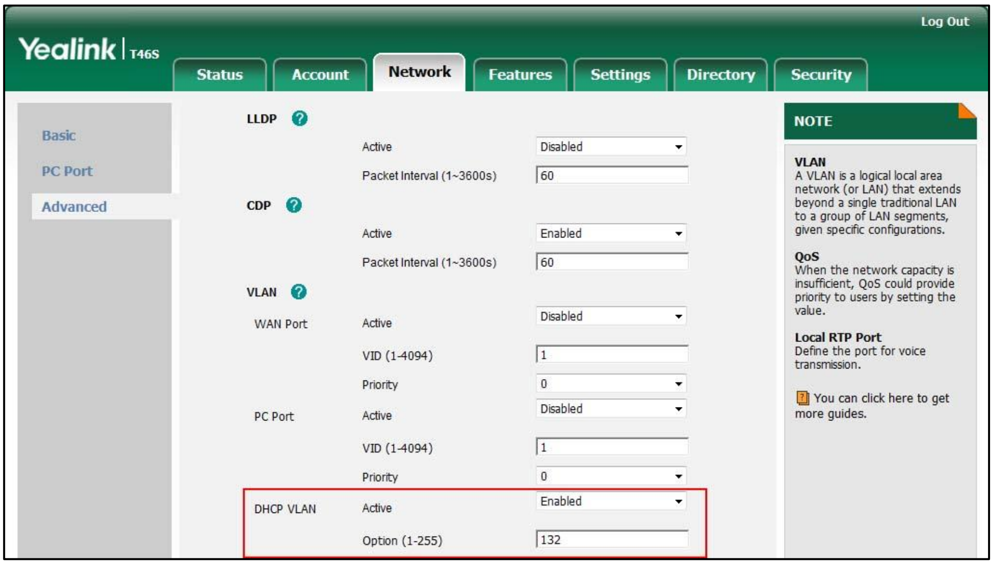
Parameters	Permitted Values	Default
static.network.vlan.dhcp_enable	**0 or 1**	**1**
Description: Enables or disables DHCP VLAN discovery feature on the phone. **0**-Disabled **1**-Enabled **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN->DHCP VLAN->Active **Phone User Interface:** Menu->Advanced (default password: admin)->Network->VLAN->DHCP VLAN->DHCP VLAN		
static.network.vlan.dhcp_option	**Integer from 1 to 255**	**132**
Description: Configures the DHCP option from which the 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 phone will reboot to make the change take effect. **Web User Interface:**		

Parameters	Permitted Values	Default
Network->Advanced->VLAN->DHCP VLAN->Option (1-255) **Phone User Interface:** Menu->Advanced (default password: admin)->Network->VLAN->DHCP VLAN->Option		

To configure DHCP VLAN discovery via web user interface:

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

   The default option is 132.



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

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

To configure DHCP VLAN discovery via phone user interface:

1. Press **Menu->Advanced** (default password: admin)->**Network**->**VLAN**->**DHCP VLAN**.
2. Press or , or the **Switch** soft key to select the desired value from the **DHCP VLAN** field.
3. Enter the desired option in the **Option** field.
4. Press the **Save** soft key to accept the change.

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

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 Skype for Business phone supports IPv4 addressing mode, IPv6 addressing mode, as well as an IPv4&IPv6 dual stack addressing mode. IPv4 uses a 32-bit address, consisting of four groups of three decimal digits separated by dots; for example, 192.168.1.100. IPv6 uses a 128-bit address, consisting of eight groups of four hexadecimal digits separated by colons; for example, 2026:1234:1:1:215:65ff:fe1f:caa.

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

If you configure the network settings on the phone for an IPv6 network, you can set up an IP address for the phone either by using SLAAC (ICMPv6), DHCPv6 or by manually entering an IP address. Ensure that your network environment supports IPv6. Contact your ISP for more information.

IPv6 Address Assignment Method

Supported IPv6 address assignment methods:

- **Manual Assignment:** An IPv6 address and other configuration parameters (e.g., DNS server) for the 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 phone, minimal (if any) configuration of routers, and no additional servers. To use IPv6 SLAAC, the 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 phone to configure itself with IPv6 address, as specified in RFC 4862.
- **Stateful DHCPv6:** The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has been standardized by the IETF through RFC 3315. DHCPv6 enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration" (RFC 2462), and can be used separately or concurrently with the latter to obtain configuration parameters.

How the phone obtains the IPv6 address and network settings?

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

DHCPv6	SLAAC (ICMPv6)	How the phone obtains the IPv6 address and network settings?
Disabled	Disabled	You have to manually configure the static IPv6 address and other network settings.
Enabled	Disabled	The phone can obtain the IPv6 address and other network settings via DHCPv6.
Enabled	Enabled	If the SLAAC server is working, the server can specify the phone to obtain the IPv6 address and other network settings either from DHCPv6 or SLAAC. If the SLAAC server is not working, the phone will try to obtain the IPv6 address and other network settings via DHCPv6.

Procedure

IPv6 can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the IPv6 address assignment method. **Parameters**: static.network.ip_address_mode static.network.ipv6_internet_port.type static.network.ipv6_internet_port.ip static.network.ipv6_prefix static.network.ipv6_internet_port.gateway static.network.ipv6_icmp_v6.enable
		Configure the IPv6 static DNS address. **Parameters**: static.network.ipv6_primary_dns static.network.ipv6_secondary_dns
	<y0000000000xx>.cfg	Configure the IPv6 static DNS. **Parameter:** static.network.ipv6_static_dns_enable
Local	Web User Interface	Configure the IPv6 address assignment method. Configure the IPv6 static DNS.

		Configure the IPv6 static DNS address. **Navigate to**: http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure the IPv6 address assignment method. Configure the IPv6 static DNS. Configure the IPv6 static DNS address.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.ip_address_mode	**0, 1 or 2**	**0**
Description: Configures the IP address mode. **0**-IPv4 **1**-IPv6 **2**-IPv4 & IPv6 **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->Internet Port->Mode (IPv4/IPv6) **Phone User Interface:** Menu->Advanced (default password: admin)->Network->WAN Port->IP Mode		
static.network.ipv6_internet_port.type	**0 or 1**	**0**
Description: Configures the Internet (WAN) 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 phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->WAN Port->IPv6		

Parameters	Permitted Values	Default
static.network.ipv6_static_dns_enable	**0 or 1**	**0**
Triggers the static IPv6 DNS feature to on or off. **0-**Off, the phone will use the IPv6 DNS obtained from DHCP. **1-**On, the 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 phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->IPv6 Static DNS **Phone User Interface:** Menu->Advanced (default: admin) ->Network->WAN Port->IPv6->Type(DHCP)->Static DNS		
static.network.ipv6_internet_port.ip	**IPv6 address**	**Blank**
Description: Configures the IPv6 address. **Example:** static.network.ipv6_internet_port.ip = 2026:1234:1:1:215:65ff:fe1f:caa **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP Address). If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->Static IP Address->IP Address **Phone User Interface:** Menu->Advanced (default password: admin)->Network->WAN Port->IPv6->Type(Static IP)->IP Address		
static.network.ipv6_prefix	**Integer from 0 to 128**	**64**
Description: Configures the IPv6 prefix. **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP Address). If you change this parameter, the phone will reboot to make the change take		

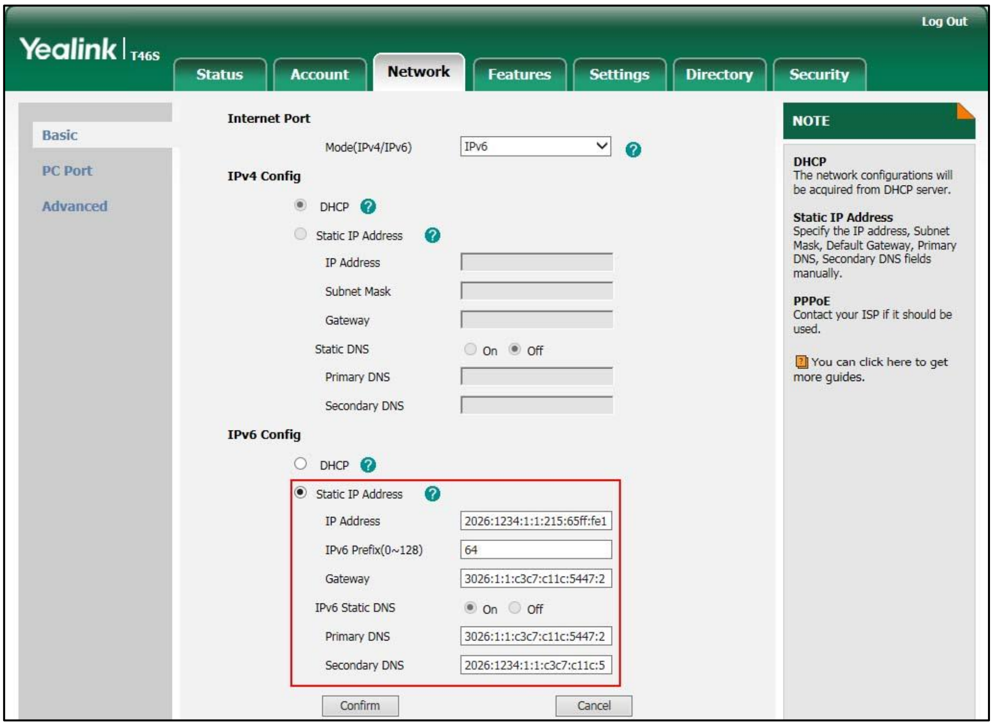
Parameters	Permitted Values	Default
effect. **Web User Interface:** Network->Basic->IPv6 Config->Static IP Address->IPv6 Prefix(0~128) **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->WAN Port->IPv6-> Type(Static IP)->IPv6 IP Prefix		
static.network.ipv6_internet_port.gateway	**IPv6 address**	**Blank**
Description: Configures the IPv6 default gateway. **Example:** static.network.ipv6_internet_port.gateway = 3036:1:1:c3c7:c11c:5447:23a6:255 **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP Address). If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->Static IP Address->Gateway **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->WAN Port->IPv6-> Type(Static IP)->Gateway		
static.network.ipv6_primary_dns	**IPv6 address**	**Blank**
Description: Configures the primary IPv6 DNS server. **Example:** static.network.ipv6_primary_dns = 3036:1:1:c3c7: c11c:5447:23a6:256 **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure the value of the parameter "static.network.ipv6_static_dns_enable" is set to 1 (On). If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->Static IP Address->Primary DNS **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->WAN Port->IPv6->Type(Static		

Parameters	Permitted Values	Default
IP)->Primary DNS **Or** Menu->Advanced (default password: admin) ->Network->WAN Port->IPv6-> Type(DHCP) ->Static DNS(Enabled)->Primary DNS		
static.network.ipv6_secondary_dns	**IPv6 address**	**Blank**
Description: Configures the secondary IPv6 DNS server. **Example:** static.network.ipv6_secondary_dns = 2026:1234:1:1:c3c7:c11c:5447:23a6 **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure the value of the parameter "static.network.ipv6_static_dns_enable" is set to 1 (On). If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->IPv6 Config->Static IP Address->Secondary DNS **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->WAN Port->IPv6-> Type(Static IP)->Secondary DNS **Or** Menu->Advanced (default password: admin) ->Network->WAN Port->IPv6-> Type(DHCP)->Static DNS(Enabled)->Secondary DNS		
static.network.ipv6_icmp_v6.enable	**0 or 1**	**1**
Description: Enables or disables the phone to obtain IPv6 network settings via SLAAC (Stateless Address Autoconfiguration) method. **0**-Disabled **1**-Enabled **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 phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->ICMPv6 Status->Active **Phone User Interface:** None		

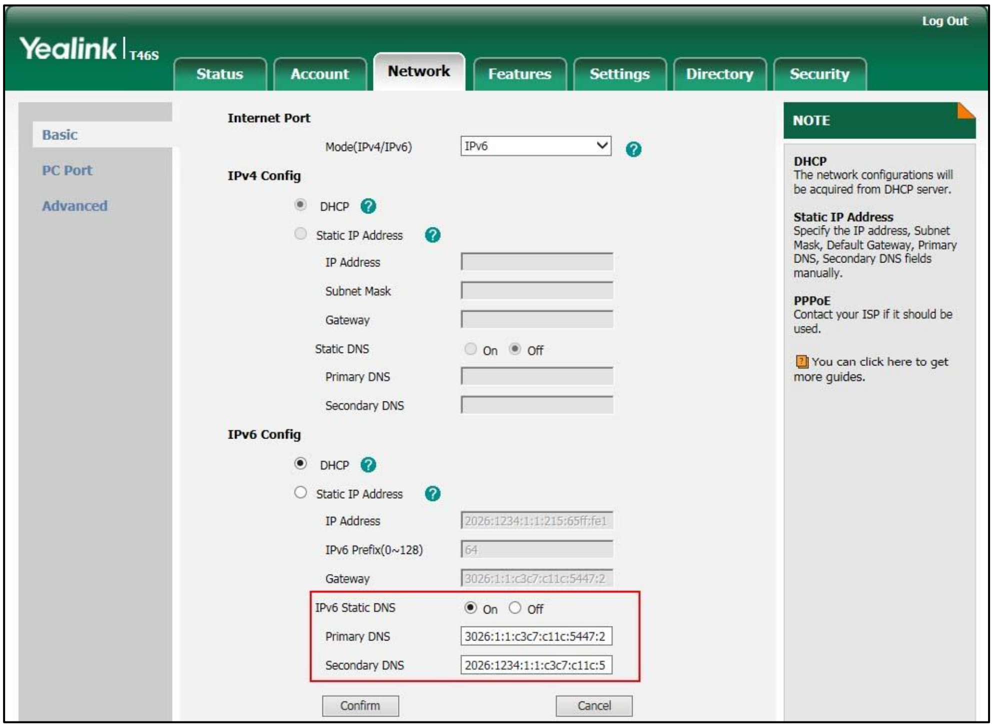
To configure IPv6 address assignment method via web user interface:

1. Click on **Network**->**Basic**.
2. Select the desired address mode (**IPv6** or **IPv4 & IPv6**) from the pull-down list of **Mode(IPv4/IPv6)**.
3. In the **IPv6 Config** block, mark the **DHCP** or the **Static IP Address** radio box.

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



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



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

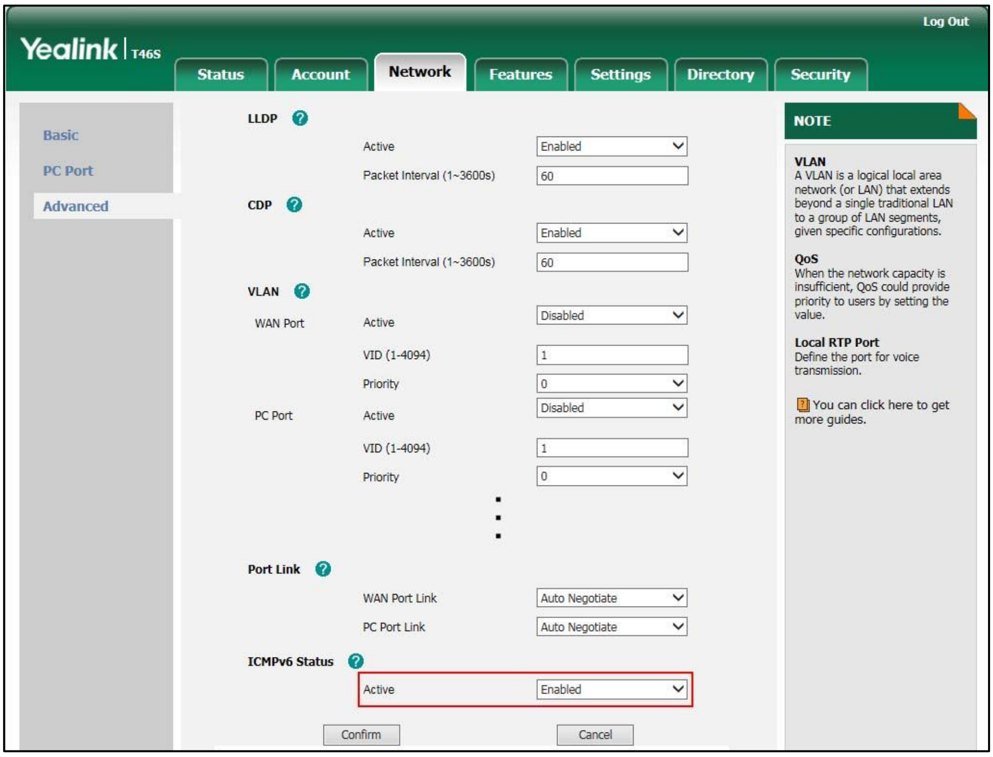
   A dialog box pops up to prompt that the settings will take effect after a reboot.

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

To configure SLAAC feature via web user interface:

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

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



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

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

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

To configure IPv6 address assignment method via phone user interface:

1. Press **Menu->Advanced** (default password: admin) ->**Network**->**WAN Port**.
2. Press or to select **IPv4 & IPv6** or **IPv6** from the **IP Mode** field.
3. Press or to highlight **IPv6** and press the **Enter** soft key.
4. Press or to select the desired IPv6 address assignment method.

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

5. Press the **Save** soft key to accept the change.

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

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

To configure IPv6 static DNS when DHCP is used via phone user interface:

1. Press **Menu**->**Advanced** (default password: admin) ->**Network**->**WAN Port**->**IPv6**.
2. Press or , or the **Switch** soft key to select the **DHCP** from the **Type** field.
3. Press or , or the **Switch** soft key to select **Enabled** from the **Static DNS** field.
4. Enter the desired values in the **Primary DNS** and **Second DNS** fields respectively.
5. Press the **Save** soft key to accept the change.

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

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

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. Skype for Business 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 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 Skype for Business 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 50.

Procedure

QoS can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the DSCPs for voice packets and SIP packets. **Parameters:** static.network.qos.audiotos static.network.qos.signaltos
Local	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:

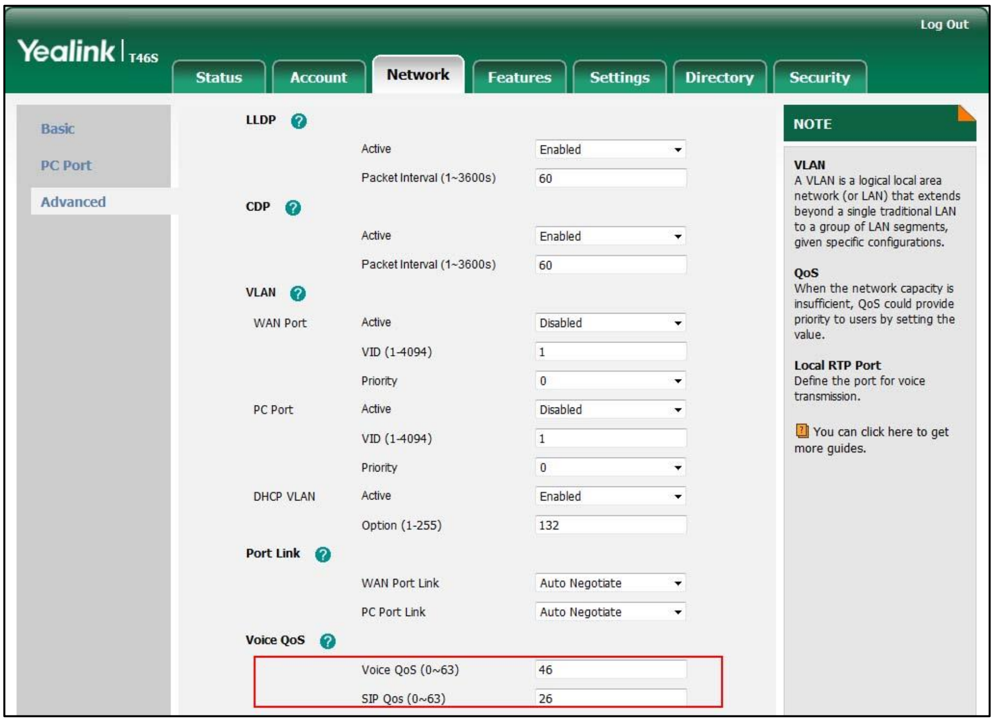
Parameters	Permitted Values	Default
static.network.qos.audiotos	**Integer from 0 to 63**	**46**
Description:		

Parameters	Permitted Values	Default
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 phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Voice QoS (0~63) **Phone 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 phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->SIP QoS (0~63) **Phone User Interface:** None		

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

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

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



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

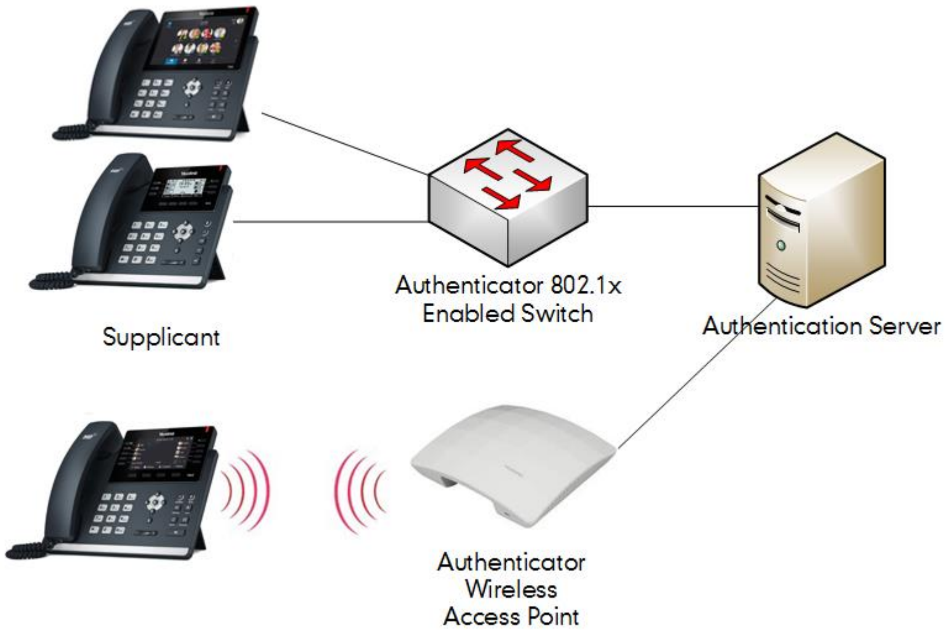
   A dialog box pops up to prompt that settings will take effect after a reboot.

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 phone that wishes to attach to the LAN or WLAN. With 802.1X port-based authentication, the 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 phone is allowed to access resources located on the protected side of the network.



Yealink Skype for Business 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 configuration files or locally.

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

		static.network.802_1x.identity static.network.802_1x.md5_password static.network.802_1x.root_cert_url static.network.802_1x.client_cert_url
Local	Web User Interface	Configure the 802.1X authentication. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure the 802.1X authentication.

Details of Configuration Parameters:

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

Parameters	Permitted Values	Default
Description: Configures the identity (or user name) for 802.1x authentication. **Example:** static.network.802_1x.identity = admin **Note:** It works only if the value of the parameter "static.network.802_1x.mode" is set to 1, 2, 3, 4, 5, 6 or 7. If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->802.1x->Identity **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->802.1x ->Identity		
static.network.802_1x.md5_password	**String within 32 characters**	**Blank**
Description: Configures the password for 802.1x authentication. **Example:** static.network.802_1x.md5_password = admin123 **Note:** It works only if the value of the parameter "static.network.802_1x.mode" is set to 1, 3, 4, 5, 6 or 7. If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->802.1x->MD5 Password **Phone User Interface:** Menu->Advanced (default password: admin) ->Network->802.1x ->MD5 Password		
static.network.802_1x.root_cert_url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the CA certificate. **Example:** static.network.802_1x.root_cert_url = http://192.168.1.10/ca.pem **Note:** It works only if the value of the parameter "static.network.802_1x.mode" is set to 2, 3, 4, 5, 6 or 7. The format of the certificate must be *.pem, *.crt, *.cer or *.der. **Web User Interface:** Network->Advanced->802.1x->CA Certificates **Phone User Interface:**		

Parameters	Permitted Values	Default
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 certificate must be *.pem. **Web User Interface:** Network->Advanced->802.1x->Device Certificates **Phone User Interface:** None		

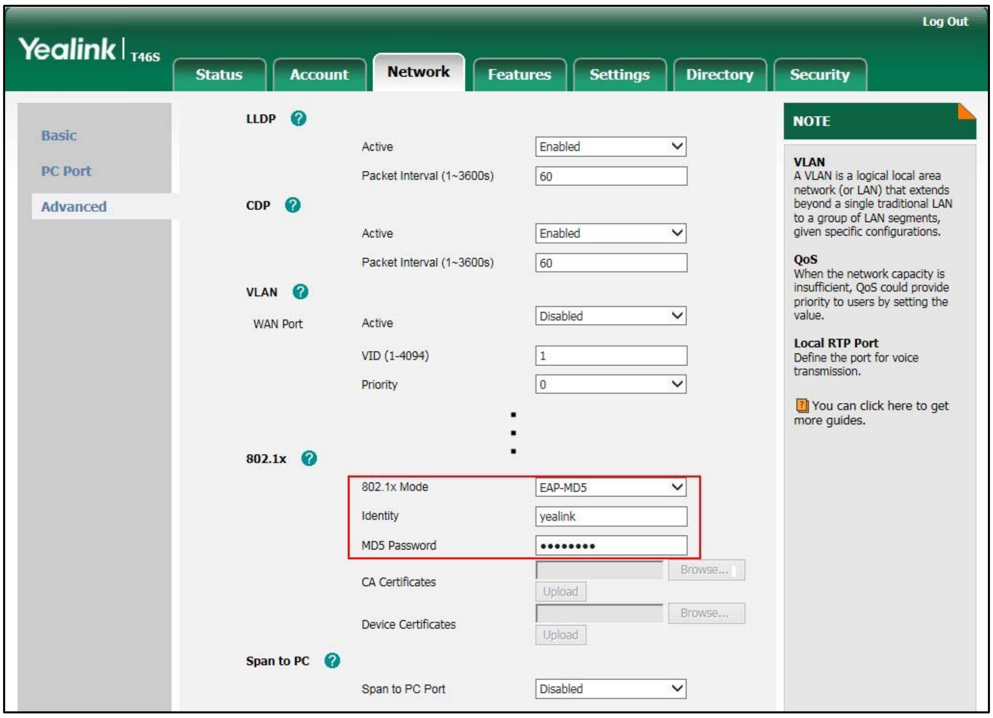
To configure the 802.1X authentication via web user interface:

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

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

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

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



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

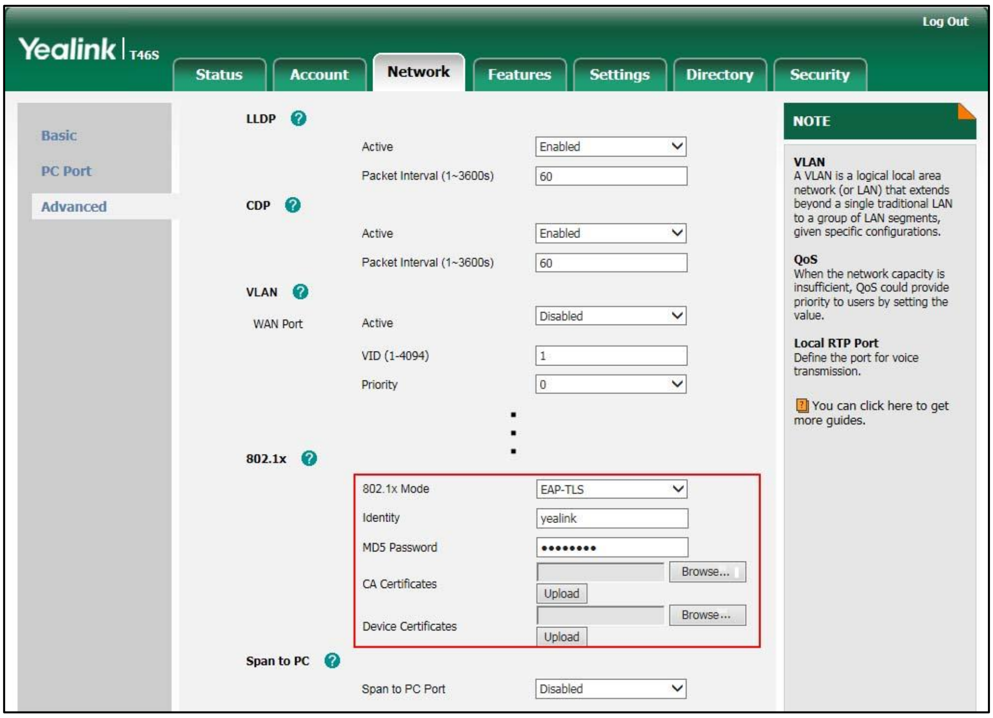
1) Enter the user name for authentication in the **Identity** field.

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

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

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

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



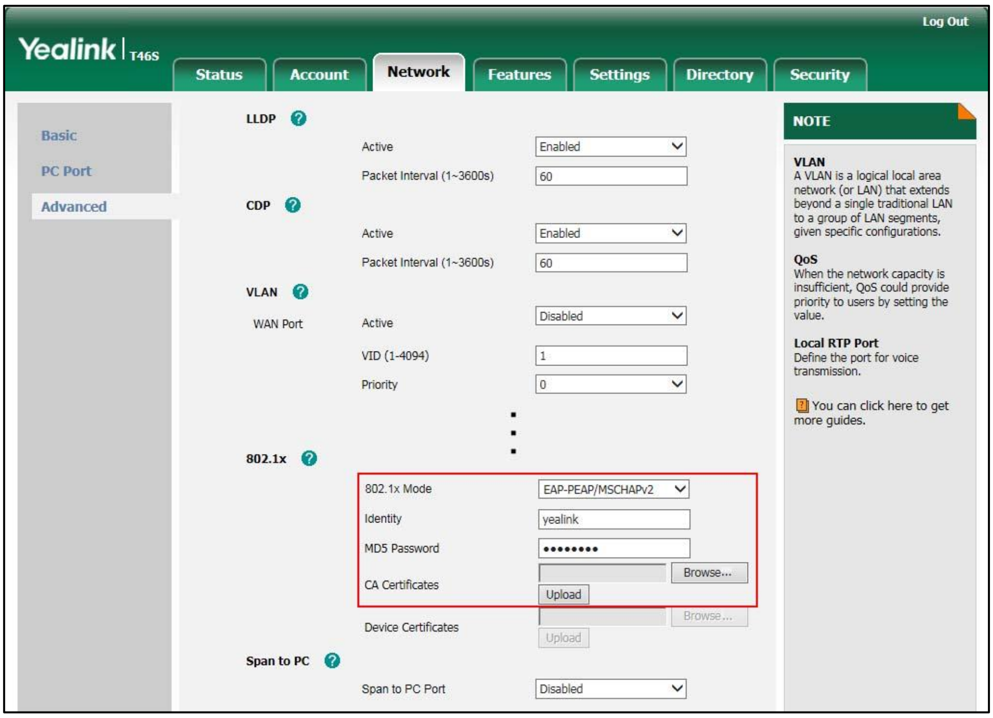
c) If you select **EAP-PEAP/MSCHAPv2**:

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

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

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

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



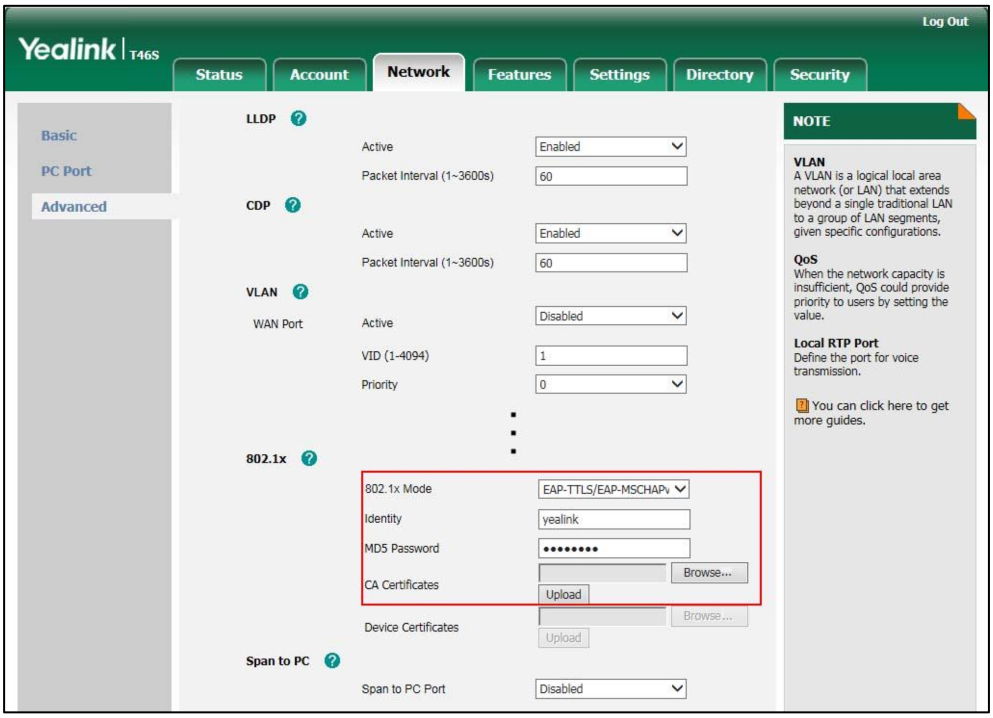
d) If you select **EAP-TTLS/EAP-MSCHAPv2**:

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

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

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

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

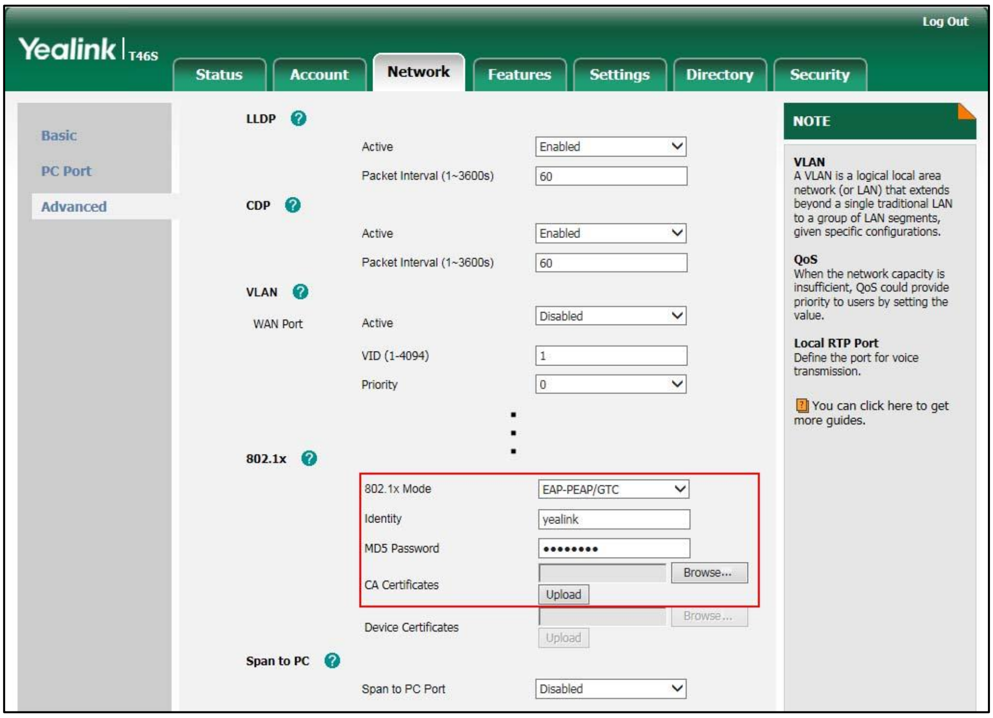


e) If you select **EAP-PEAP/GTC**:

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

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

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



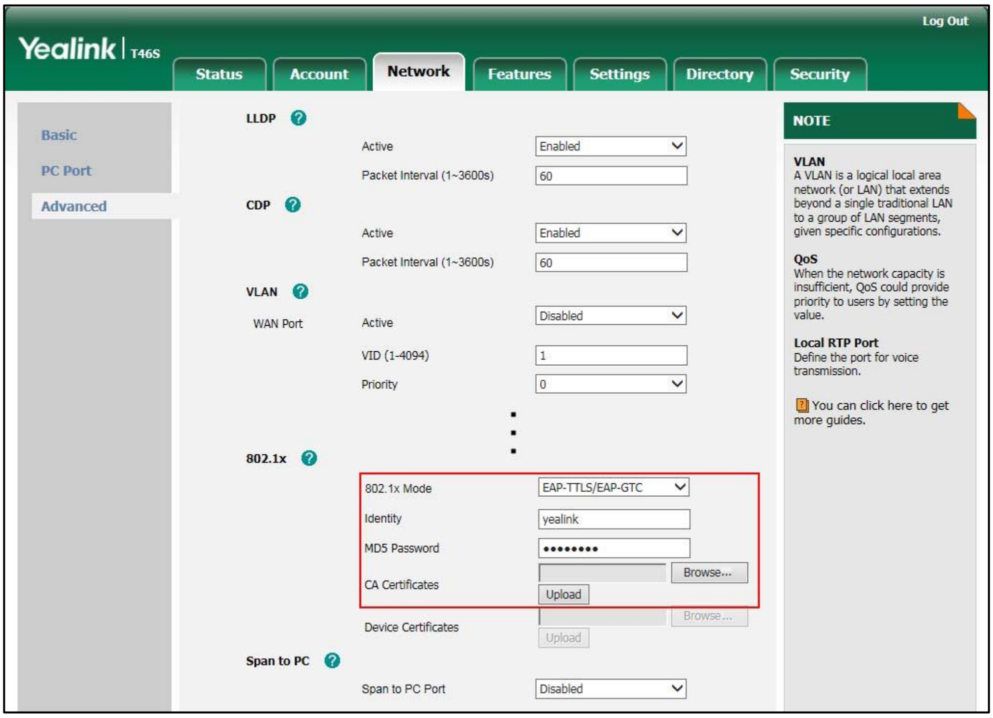
4) Click **Upload** to upload the certificate.

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

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

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

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



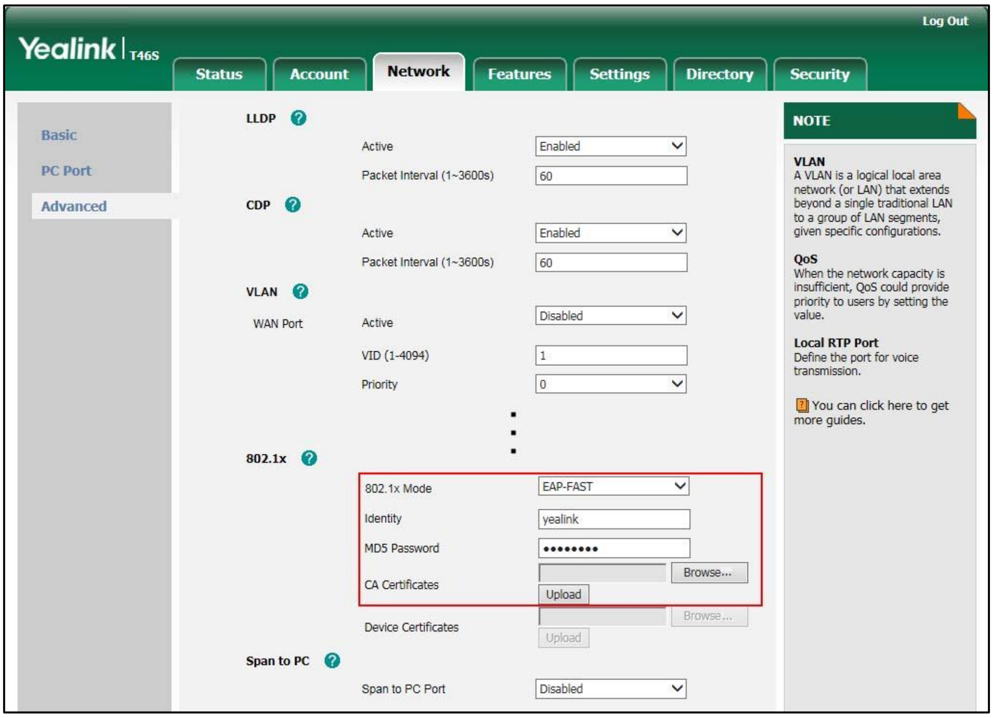
4) Click **Upload** to upload the certificate.

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

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

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

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



4) 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.

To configure the 802.1X authentication via phone user interface:

1. Press **Menu**->**Advanced** (default password: admin) ->**Network**->**802.1x**.
2. Press or or the **Switch** soft key to select the desired value from the **802.1x Mode** field.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Setting Up Your Phones with a Provisioning Server

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

This chapter consists of the following sections:

- Provisioning Points to Consider
- Provisioning Methods
- Configuration Files and Resource Files
- Setting up a Provisioning Server
- Upgrading Firmware

Provisioning Points to Consider

- If you are provisioning a mass of 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 87.
- A provisioning server maximizes the flexibility you have when installing, configuring, upgrading, and managing the phones, and enables you to store configuration 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 94.
- If the phone cannot obtain the address of a provisioning server during startup, and has not been configured with settings from any other source, the 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.

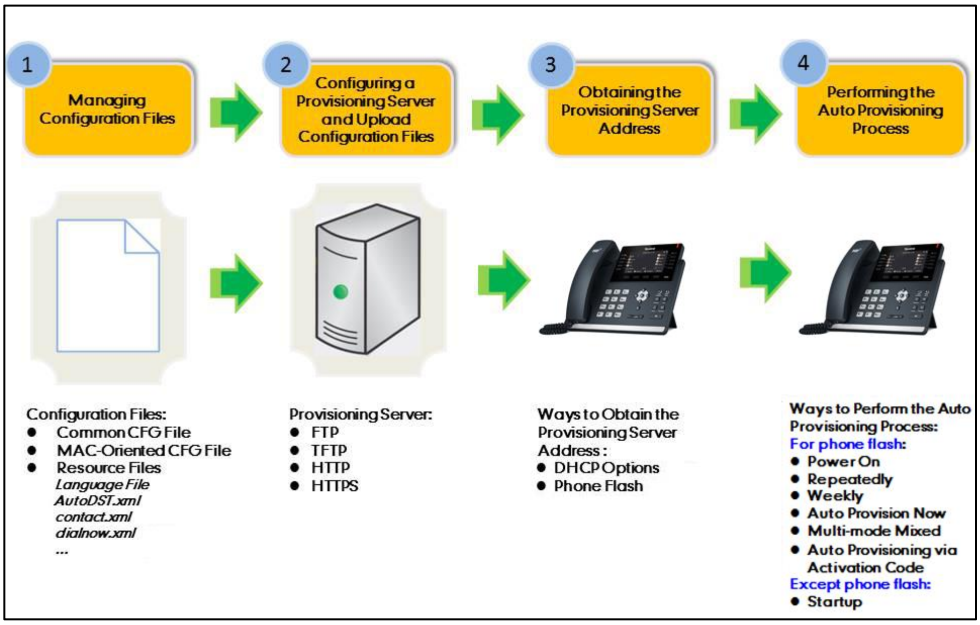
Provisioning Methods

Skype for Business phones can be configured using the following methods:

- **Central Provisioning**: configuration files stored on a central provisioning server.
- **In-band Provisioning:** settings from the Skype for Business server pool.
- **Manual Provisioning:** operations on the web user interface or phone user interface.
- Combination of the above methods.

Central Provisioning

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



Using the 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 configuration files, and then store configuration files to a provisioning server. Skype for Business 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 94. For more information on configuration files, refer to Configuration Files on page 91.

Skype for Business phones can obtain the provisioning server address during startup. Then phones download 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_Skype_for_Business_HD_IP_Phones_Auto_Provisioning_Guide*. In addition to the configuration files, the phones also download resource files during auto provisioning. For more information on resource files, refer to Resource Files on page 92.

In-Band Provisioning Settings

After the phone is signed in, the phone receives settings from the Skype for Business server pool through in-band provisioning.

Skype for Business in-band provisioning device settings take precedence over the same settings configured via central provisioning. To avoid configuration conflicts, ensure that the settings applied to phones are from one source or the other. If you are provisioning in-band, remove the parameters from the configuration files before using central provisioning method. If you are using central provisioning, it is best practice to disable in-band provisioning device settings.

Procedure

In-band provisioning device settings can be configured using the configuration files only.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configures in-band provisioning device settings sent from Skype for Business server. **Parameters:** static.phone_setting.receive_inband.enable

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.phone_setting.receive_inband.enable	**0 or 1**	**1**
Description: Enables or disables in-band provisioning device settings sent from Skype for Business server. **0**-Disabled, the phone blocks in-band provisioning device settings sent from Skype for Business server. **1**-Enabled, the phone accepts in-band provisioning device settings sent from Skype for Business server. **Note:** It is not applicable to CP960 Skype for Business phones. If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		

Manual Provisioning

There are two ways to manually provision phones:

- Web User Interface
- Phone User Interface

Web User Interface

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

An administrator or a user can configure 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 359.

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 other provisioning methods.

Phones support both HTTP and HTTPS protocols for accessing the web user interface. For more information, refer to Web Server Type on page 39.

Phone User Interface

You can configure phones via phone user interface on a per-phone basis. As with the web user interface, phone user interface makes configurations available to users and administrators; but the **Advanced/Advanced Settings** option is only available to administrators and requires an administrator password (default: admin). For more information on configuring password, refer to User and Administrator Passwords on page 359.

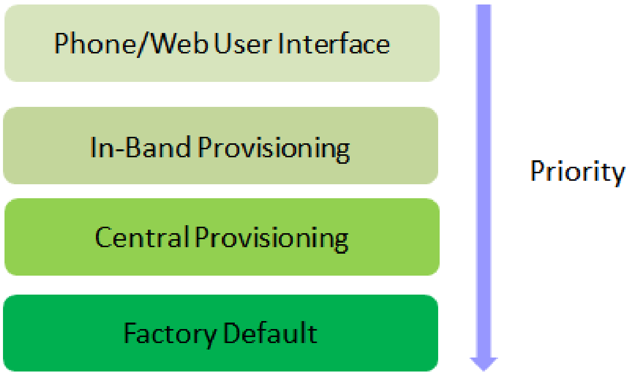
If you want to reset all settings made from the phone user interface to default, refer to *Yealink Skype for Business phone-specific user guide*.

Provisioning Methods Priority

By default, different provisioning methods (central provisioning, in-band Provisioning and manual Provisioning) have no priority. That is, the subsequent operations always override previous operations regardless of the provisioning method you are using.
For example, a user disables the phone lock feature via phone/web user interface manually, but the phone automatically receives in-band provisioning when the auto update timer expires, so that the phone lock feature is enabled automatically.
If users want to keep the personalized settings, the system administrator can enable the provisioning methods priority to ensure that provision with high priority will not be overwritten

by provision with low priority.

The provisioning methods priority is as follows (highest to lowest):



Note

Static settings are settings that related to network and central provisioning. Static settings have no priority. So no matter which provisioning method you are using to provision your phone, static settings always take effect. For more information on static settings, refer to Appendix D: Static Settings on page 437.

Procedure

Provisioning methods priority can be configured using the configuration files only.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configures the provisioning methods priority. **Parameters:** static.auto_provision.custom.protect

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.auto_provision.custom.protect	**0 or 1**	**0**
Description: Enables or disables the provisioning methods priority. **0**-Disabled, different provisioning methods (central provisioning, in-band Provisioning and manual Provisioning) have no priority. The subsequent operations always override previous operations regardless of the provisioning method you are using. **1**-Enabled, different provisioning methods have priority (phone/web user interface>in-band provisioning>central provisioning>factory defaults). Provision with high priority will not be overwritten by provision with low priority. **Web User Interface:**		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">None
Phone User Interface:
None
Note: It is not applicable to CP960 Skype for Business phones.</td></tr>
</table>

Configuration Files and Resource Files

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

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

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

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 phones automatically through configuration files stored on a provisioning server.

Yealink configuration files consist of:

- Common CFG File
- MAC-Oriented CFG File

Common CFG File

Common CFG file, named <y0000000000xx>.cfg, contains parameters that affect the basic operation of the phone, such as language and volume. It will be effectual for all phones of the same model. The common CFG file has a fixed name.

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

Phone Model	Common CFG file
T48S	y000000000065.cfg
T46S	y000000000066.cfg
T42S	y000000000067.cfg
T41S	y000000000068.cfg
CP960	y000000000073.cfg

MAC-Oriented CFG File

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

The MAC-Oriented CFG file is named after the MAC address of the 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 phone. For example, if the MAC address of a phone is 00156574B150, the name of the MAC-Oriented CFG file must be 00156574b150.cfg (case-sensitive).

Resource Files

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

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

The followings show examples of resource files:

- Language packs
- Ring tones
- Local contact file

For more information on resource files, refer to Obtaining Configuration Files/Resource Files on page 92.

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 phone to factory configuration settings. For more information, refer to Resetting Issues on page 422.

Obtaining 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:

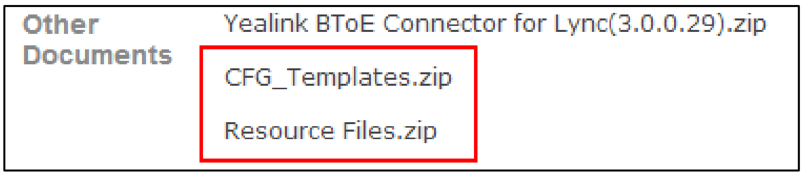
Template File		File Name	Description
Configuration	Common CFG File	Common.cfg	Allow you to deploy and maintain a mass of Yealink phones. For more

Template File		File Name	Description
Files	MAC-Oriented CFG File	MAC.cfg	information, refer to Common CFG File and MAC-Oriented CFG File on page 92.
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 170.
	Language Packs	For example, 000.GUI.English.lang 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 174.
	Keypad Input Method File	ime.txt	Existing input methods on Yealink phones. It is not applicable to CP960 Skype for Business phones.
	Dial Now Template	dialnow.xml	Allows you to customize multiple dial now rules for phone. For more information, refer to Customizing Dial-now Template File on page189.
	Local Contact File	contact.xml	Allows you to add or modify multiple local contacts at a time for your phone. For more information, refer to Customizing a Local Contact File on page 196.

To download template files:

1. Go to Yealink *Document Download* page and select the desired Skype for Business phone model.
2. Download and extract the combined files to your local system.

   For example, the following illustration shows the available template files.



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 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 phones. A provisioning server allows for flexibility in upgrading, maintaining and configuring the phone. Configuration files and resource files are normally located on this server.

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

Supported Provisioning Protocols

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

Note

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

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

There are two types of FTP methods—active and passive. The 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_Skype_for_Business_HD_IP_Phones_Auto_Provisioning_Guide*.

To set up the provisioning server:

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

For more information on how to deploy phones using configuration files, refer to Deploying Phones from the Provisioning Server on page 95.

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, the phones download the common configuration file first, and then the MAC-Oriented file. Therefore any parameter in the MAC-Oriented configuration file will override the same one in the common configuration file.

Yealink supplies configuration files for each phone model, which is delivered with the Skype for Business phone firmware. The configuration files, supplied with each firmware release, must be used with that release. Otherwise, configurations may not take effect, and the 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 Skype for Business phones from the provisioning server:

1. Create per-phone configuration files by performing the following steps:
   a) Obtain a list of phone MAC addresses (the bar code label on the back of the phone or on the outside of the box).
   b) Create per-phone <MAC>.cfg files by using the MAC-Oriented CFG file from the distribution as templates.
   c) Edit the parameters in the file as desired.
2. Create new common configuration files by performing the following steps:
   a) Create <y0000000000xx>.cfg files by using the Common CFG file from the distribution as templates.
   b) Edit the parameters in the file as desired.
3. Copy configuration files to the home directory of the provisioning server.
4. Reboot phones to trigger the auto provisioning process.

Skype for Business phones discover the provisioning server address, and then download the configuration files from the provisioning server.

For more information on configuration files, refer to Configuration Files on page 91. For protecting against unauthorized access, you can encrypt configuration files. For more information on encrypting configuration files, refer to Encrypting Configuration Files on page 376.

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

- **DHCP**: DHCP option can be used to provide the address or URL of the provisioning server to phones. When the phone requests an IP address using the DHCP protocol, the resulting response may contain option 66 or the custom option (if configured) that contains the provisioning server address.
- **Static**: You can manually configure the server address via phone user interface or web user interface.

For more information on the above methods, refer to *Yealink_Skype_for_Business_HD_IP_Phones_Auto_Provisioning_Guide*.

Upgrading Firmware

Yealink supports three methods to upgrade phone firmware:

- **Upgrade firmware via web user interface**: Download firmware in ROM format, and upload it to the phone via web user interface. This method can deploy a single phone.

- **Upgrade firmware from provisioning server**: Download firmware in ROM format, and use centralized provisioning method to upgrade the firmware. This method requires setting up a provisioning server, and uses configuration files to provision the phone.
- **Upgrade firmware from Skype for Business Server**: Download firmware in CAB file format, and place the firmware on Skype for Business Server to provision the phone.

The following table lists the associated and latest firmware name for Skype for Business phone model.

Phone Model	Associated Firmware Name	Firmware Name(.rom)	Firmware Name(.cab)
T48S/T46S/T42S/T41S	66.x.x.x.rom	66.9.0.25.rom	Yealink_ver_66.9.0.25.cab
CP960	73.x.x.x.rom	73.8.0.17.rom	Yealink_ver_73.8.0.17.cab

Note

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

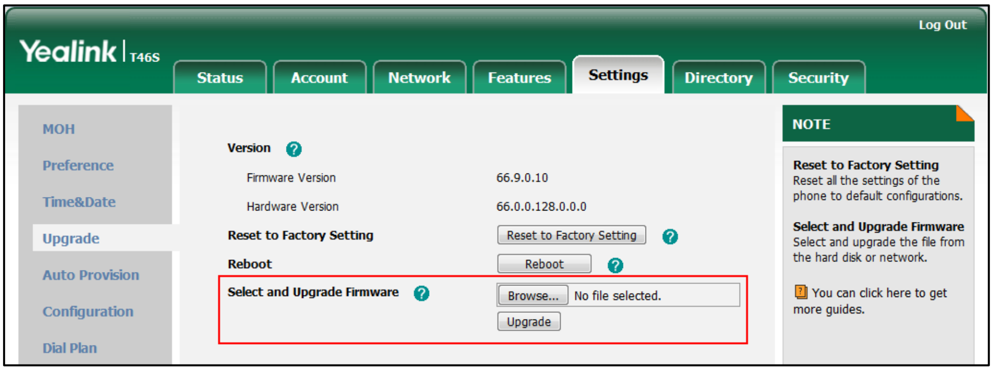
Do not unplug the network and power cables when the Skype for Business phone is upgrading firmware.

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**.



A dialog box pops up to prompt "Firmware of the SIP phone will be updated. It will take 5 minutes to complete. Please don't power off!".

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

Note

Do not close and refresh the browser when the Skype for Business phone is upgrading firmware via web user interface.

Upgrading Firmware from the Provisioning Server

Phones support using FTP, TFTP, HTTP and HTTPS protocols to download configuration files and firmware from the provisioning server, and then upgrade firmware automatically.

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 configuration files or locally.

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

Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>static.auto_provision.power_on</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Triggers the power on feature to on or off.
0-Off
1-On, the phone will perform an auto provisioning process when powered on.
Web User Interface:
Settings->Auto Provision->Power On
Phone User Interface:
None</td></tr>
<tr><td>static.auto_provision.repeat.enable</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Triggers the repeatedly feature to on or off.
0-Off
1-On, the phone will perform an auto provisioning process repeatedly.
Web User Interface:
Settings->Auto Provision->Repeatedly
Phone User Interface:
None</td></tr>
<tr><td>static.auto_provision.repeat.minutes</td><td>Integer from 1 to 43200</td><td>1440</td></tr>
<tr><td colspan="3">Description:
Configures the interval (in minutes) for the phone to perform an auto provisioning process repeatedly.
Note: It works only if the value of the parameter “static.auto_provision.repeat.enable” is set to 1 (On).
Web User Interface:
Settings->Auto Provision->Interval(Minutes)
Phone User Interface:
None</td></tr>
<tr><td>static.auto_provision.weekly.enable</td><td>0 or 1</td><td>0</td></tr>
</table>

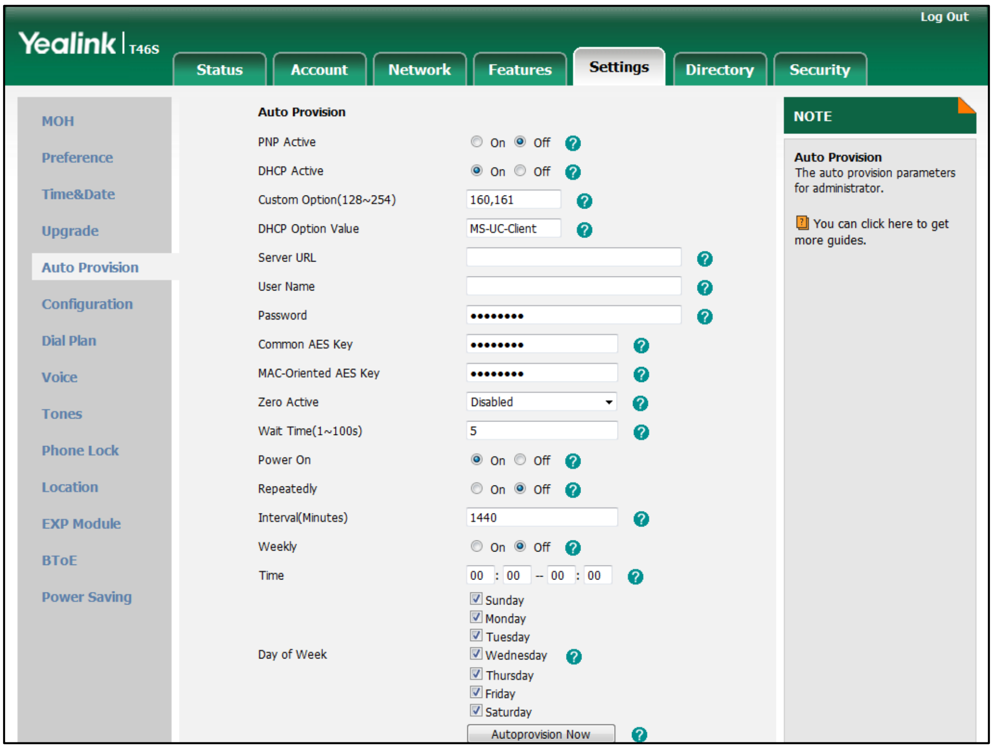
Parameters	Permitted Values	Default
Description: Triggers the weekly feature to on or off. **0**-Off **1**-On, the phone will perform an auto provisioning process weekly. **Web User Interface:** Settings->Auto Provision->Weekly **Phone User Interface:** None		
static.auto_provision.weekly.begin_time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

Parameters	Permitted Values	Default
weekly. **0**-Sunday **1**-Monday **2**-Tuesday **3-**Wednesday **4**-Thursday **5**-Friday **6**-Saturday **Example**: static.auto_provision.weekly.dayofweek = 01 It means the phone will perform an auto provisioning process every Sunday and Monday. **Note:** It works only if the value of the parameter "static.auto_provision.weekly.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Day of Week **Phone User Interface:** None		
static.firmware.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the firmware file. **Example:** static.firmware.url = http://192.168.1.20/66.9.0.25.rom **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Settings->Upgrade->Select and Upgrade Firmware **Phone User Interface:** None		
static.auto_provision.reset_factory.enable	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Enables or disables the phone to be reset to factory. **0**-Disabled **1**-Enabled **Note**: You can reset your phone to factory using this parameter once only.		

To configure the way for the Skype for Business 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 phone will check configuration files stored on the provisioning server during startup and then will download firmware from the server.

Updating Phone Firmware from Skype for Business Server

You can update firmware from Skype for Business Server. Before updating firmware from Skype for Business Server, you must upload the update package (*.CAB) to your Skype for Business Update Server in advance. For more information, refer to *Updating Phone Firmware from Microsoft Skype for Business Server*.

Automatic Update

Update checking time defines a period of time for the phone to automatically check a firmware update on Skype for Business Server.

Procedure

Update checking time can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure update checking time. **Parameters**: sfb.update_time
Local	Web User Interface	Configure update checking time. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

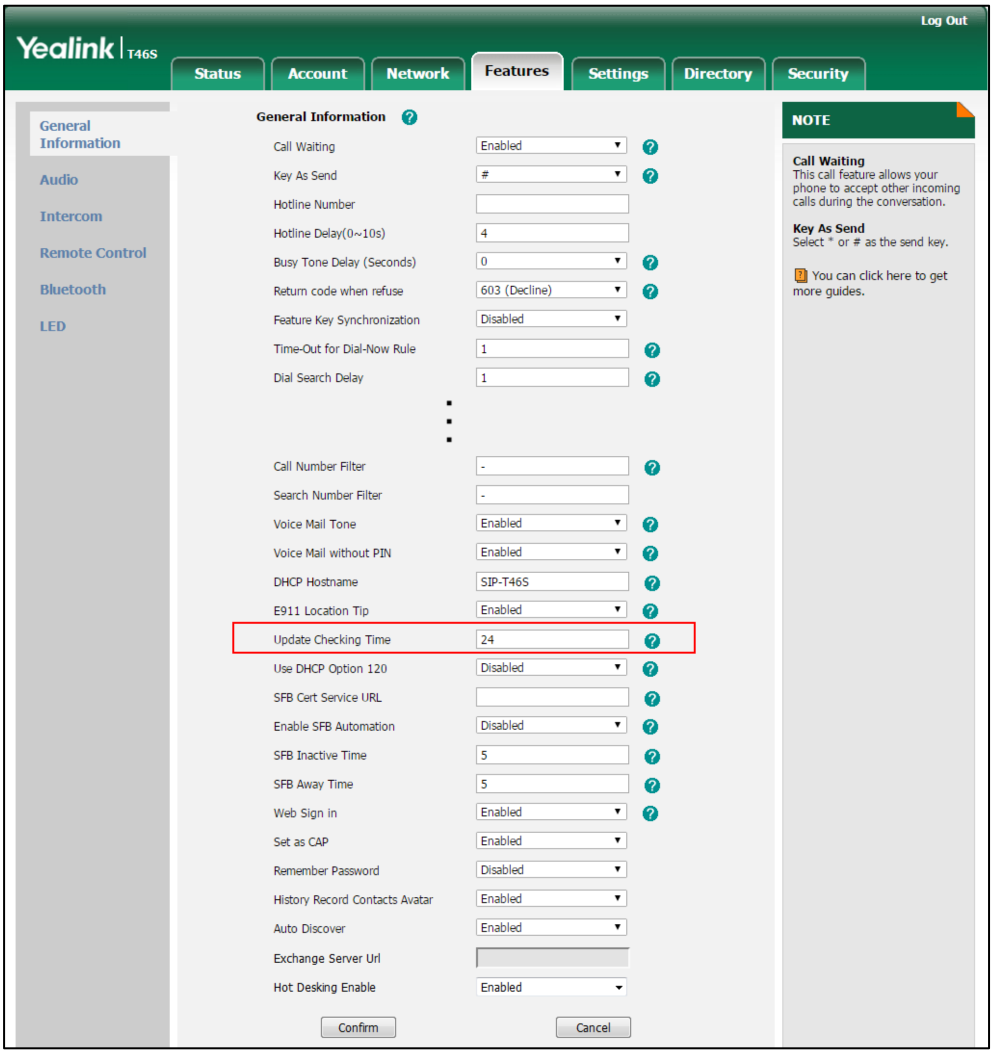
Details of Configuration Parameters:

Parameters	Permitted Values	Default
sfb.update_time	**Integer from 1 to 48**	**24**
Description: Configures the auto timer (in hours) for the phone to automatically check if there is a firmware update available on Skype for Business Server. If it is set to 24, the phone will check if a firmware update is available on the Skype for Business Server every 24 hours. **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Features->General Information->Update Checking Time **Phone User Interface:** None		

To configure update checking time via web user interface:

1. Click on **Features**->**General Information**.

2. Enter the desired value in the **Update Checking Time** field.



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

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

Manual Update

You can initiate an update immediately, just power off the phone and power on it again. The phone will boot up, check for updates and apply the updates. You can also trigger an update manually via phone user interface.

To trigger an update manually via phone user interface:

1. Press **Menu**-> **Advanced** (default password: admin)->**Firmware Update**.

2. Press the **Update** soft key.

3. Press the **OK** soft key to confirm the update.

If there is no update available on Skype for Business Server, the LCD screen prompts "The firmware is the latest".

Configuring Basic Features

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

- Signing into Skype for Business
- Signing Out of Skype for Business
- Microsoft Exchange Integration
- Updating Status Automatically
- Always Online
- Power LED indicator
- Contrast
- Screen Saver
- Power Saving
- Backlight
- Bluetooth
- Showing Full Name
- Time and Date
- Language
- Key As Send
- Send Tone
- Key Tone
- Dial Plan
- Dial Now
- Hotline
- Contact Management
- Call Log
- Dial Search Delay
- Live Dialpad
- Call Waiting
- Auto Answer
- Busy Tone Delay
- Return Code When Refuse
- Early Media

- 180 Ring Workaround
- Call Hold
- Call Forward
- Team-Call Group
- Response Group
- Call Queue
- Call Number Filter
- Search Number Filter
- Allow Mute
- Intercom
- USB Recording
- Voice Mail without PIN
- Shared Line Appearance(SLA)
- Boss-Admin Feature
- Calendar
- BToE
- EXP40 Expansion Module

Signing into Skype for Business

Skype for Business users are authenticated against Microsoft Active Directory Domain Service. The following four sign-in methods are available.

- **PIN Authentication**: This method uses the user's phone number (or extension) and personal identification number (PIN) to sign into Skype for Business server. This sign-in method is only applicable to On-Premises account.
- **User Sign-in**: This method uses the user's credentials (sign-in address, user name, and password) to sign into Skype for Business server. This sign-in method is applicable to On-Premises account and Online account.
- **Web Sign-in:** This method uses the unique website shown on the phone to sign in. This sign-in method is only applicable to Online account.
- **Sign in via PC**: when your phone is paired to your computer using Better Together over Ethernet (BToE), use the Skype for Business client to sign in. This sign-in method is applicable to On-Premises account and Online account. It is not applicable to CP960 Skype for Business phones.

Note If the phone reboots after successful login, the login credentials from the previous Sign-In will be cached. User can sign in successfully without reentering the credentials.

PIN Authentication

During startup, the phone can download a private CA root security certificate used by Skype for Business and obtain the Skype for Business server address by detecting the DHCP options 43. As a result, you can sign into Skype for Business on your phone with your PIN Authentication credentials. If the DHCP Option 43 is not configured in your network, your phone will not display PIN Authentication sign-in method.

Contact your system administrator for more information.

Procedure

PIN Authentication can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure PIN Authentication method. **Parameter:** features.pin_authentication.enable
	<MAC>.cfg	Configure PIN Authentication method. **Parameter:** static.account.1.sign_in.pin_number
		Configures the PIN for the PIN Authentication. **Parameter:** static.account.1.sign_in.pin_password
Local	Web User Interface	Configure PIN Authentication method. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-register-lync&q=load&acc=0
	Phone User Interface	Configure PIN Authentication.

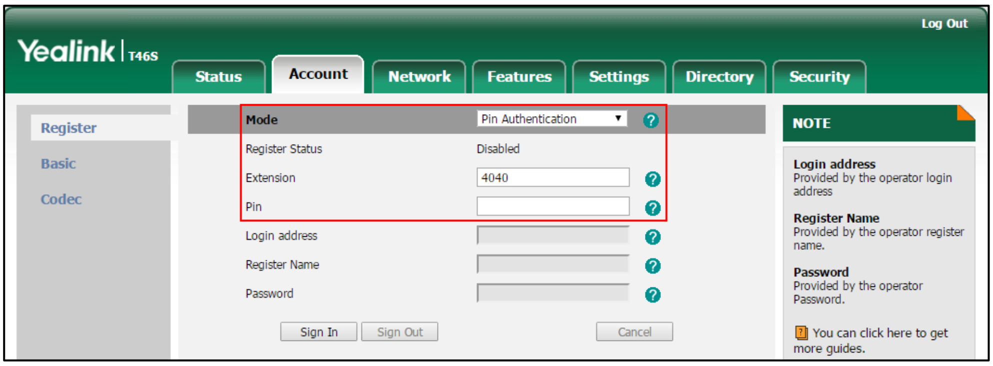
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.pin_authentication.enable	**0 or 1**	**1**
Description: Enables or disables the user to sign into the phone using PIN Authentication method. **0**-Disabled **1**-Enabled **Web User Interface:**		

Parameters	Permitted Values	Default
None **Phone User Interface:** None		
static.account.1.sign_in.pin_number	**String within 128 characters**	**Blank**
Description: Configures the phone's extension for the PIN Authentication method. **Web User Interface:** Account->Register->Extension **Phone User Interface:** Sign in->PIN Authentication->Extension		
static.account.1.sign_in.pin_password	**String within 99 characters**	**Blank**
Description: Configures the PIN for the PIN Authentication method. **Web User Interface:** Account->Register->Pin **Phone User Interface:** Sign in->PIN Authentication->PIN		

To sign into the Skype for Business Server using PIN Authentication method via web user interface:

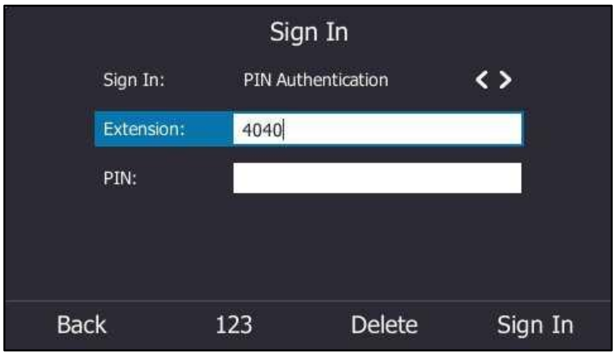
1. Click on **Account**->**Register**.
2. Select **Pin Authentication** from the pull-down list of **Mode**.
3. Enter your Skype for Business user's phone number or extension (e.g., 4040) in the **Extension** field.
4. Enter your personal identification number in the **Pin** field.



5. Click **Sign In** to accept the change.

To sign into Skype for Business server using PIN Authentication method via phone user interface:

1. Press the **Sign In** soft key.
2. Press or , or the **Switch** soft key to select **PIN Authentication**.
3. Enter your phone number or extension (e.g., 4040) in the **Extension** field.
4. Enter your personal identification number in the **PIN** field.



5. Press the **Sign In** soft key.

User Sign-in

You can sign into Microsoft Skype for Business on your phone with your login credentials, which includes your address, username, and password.

Procedure

User sign-in method can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure user sign-in method. **Parameter:** features.user_sign_in.enable
	<MAC>.cfg	Configure user sign-in method. **Parameters:** static.account.1.sign_in.server_address static.account.1.sign_in.user_name static.account.1.sign_in.password
Local	Web User Interface	Configure user sign-in method. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-register-

		lync&q=load&acc=0
	Phone User Interface	Configure user sign-in method.

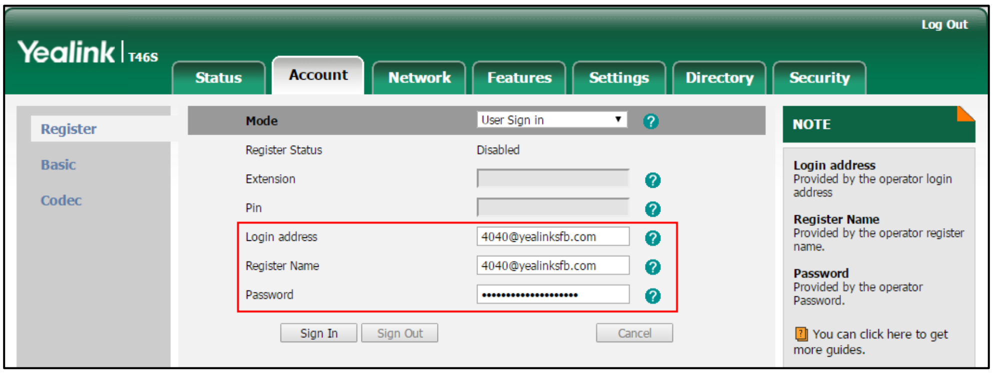
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.user_sign_in.enable	**0 or 1**	**1**
Description: Enables or disables the user to sign into the phone using User Sign-in method. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		
static.account.1.sign_in.server_address	**SIP URI**	**Blank**
Description: Configures the sign-in address for the user sign-in method. The value format is username@domain.com. **Example:** static.account.1.sign_in.server_address= 4040@yealinksfb.com **Web User Interface:** Account->Register->Login address **Phone User Interface:** Sign in->User Sign-in->Address		
static.account.1.sign_in.user_name	**String within 128 characters**	**Blank**
Description: Configures the user name for the user sign-in method. The value format is username@domain.com or username@domain, domain.com\username or domain\username. **Example:** static.account.1.sign_in.user_name= 4040@yealinksfb.com **Web User Interface:**		

Parameters	Permitted Values	Default
Account->Register->Register Name **Phone User Interface:** Sign in->User Sign-in->UserName		
static.account.1.sign_in.password	**String within 99 characters**	**Blank**
Description: Configures the password for the user sign-in method. **Web User Interface:** Account->Register->Password **Phone User Interface:** Sign in->User Sign-in->Password		

To sign into the Skype for Business server using User Sign-in method via web user interface:

1. Click on **Account**->**Register**.
2. Select **User Sign in** from the pull-down list of **Mode**.
3. Enter your Skype for Business user's sign-in address (e.g., 4040@yealinksfb.com) in the **Login address** field.
4. Enter your Skype for Business user name (e.g., 4040@yealinksfb.com) in the **Register Name** field.
5. Enter the sign-in password in the **Password** field.



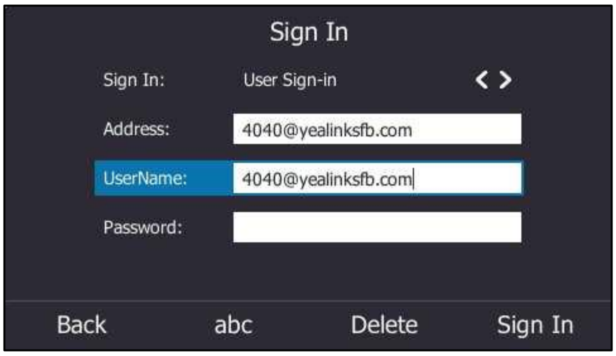
6. Click **Sign In** to accept the change.

To sign into the Skype for Business server using User Sign-in method via phone user interface:

1. Press the **Sign In** soft key.
2. Press or , or the **Switch** soft key to select **User Sign-in**.
3. Enter your Skype for Business user's sign-in address (e.g., 4040@yealinksfb.com) in the

Address field.

4. Enter your Skype for Business user name (e.g., 4040@yealinksfb.com) in the **UserName** field.



5. Enter the sign-in password in the **Password** field.

6. Press the **Sign in** soft key.

Web Sign-in

You can sign into your Skype for Business Online account using the Web Sign-In method, which allows you to sign into the phone with your Skype for Business Online account using a web browser.

Procedure

Web sign-in can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the web sign-in method. **Parameter:** features.web_sign_in.enable
		Configure the Server URL for device pairing. **Parameter:** features.device_pairing.url
Local	Web User Interface	Configure web sign-in method. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-register-lync&q=load&acc=0
	Phone User Interface	Configure web sign-in method.

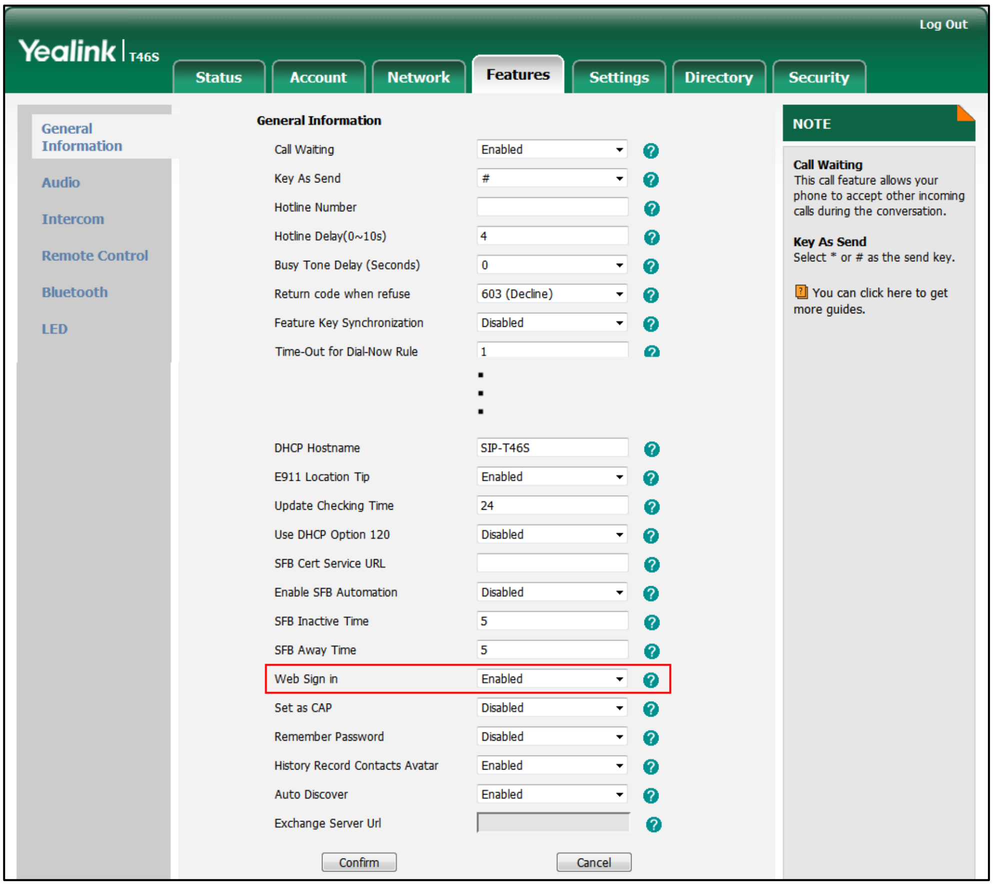
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.web_sign_in.enable	**0 or 1**	**1**
Description: Enables or disables the user to sign into the phone using web sign-in method. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Web Sign in **Phone User Interface:** None		
features.device_pairing.url	**URL within 512characters**	**https://bootstrap.pinauth.services.skypeforbusiness.com/**
Configures the Server URL for device pairing, so that you can sign into the phone using web sign-in method. **Example:** features.device_pairing.url= https://bootstrap.pinauth.services.skypeforbusiness.com/		

To enable the web sign-in via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Web Sign in**.
   - If it is enabled, you can sign into the Skype for Business Server using web sign-in method.

– If it is disabled, you cannot sign into the Skype for Business Server using web sign-in method.



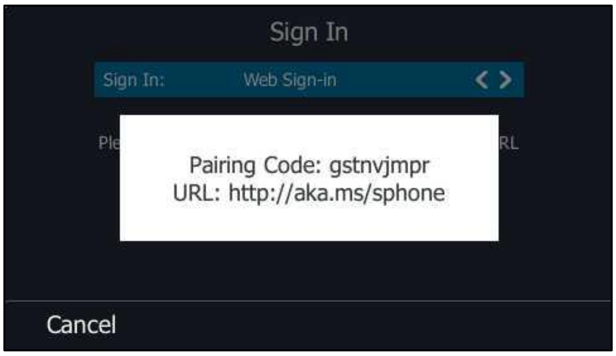
3. Click **Confirm** to accept the change.

To sign into Skype for Business server using Web Sign-In method via phone user interface:

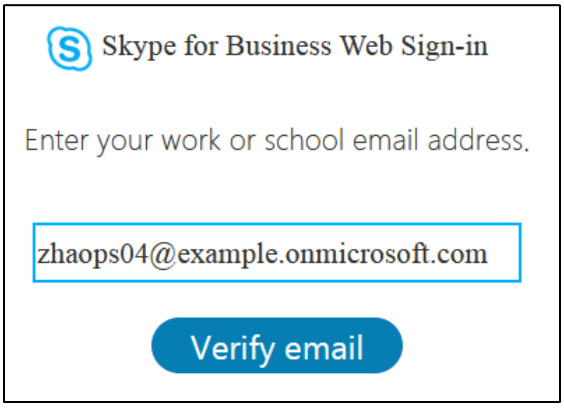
1. Press the **Sign In** soft key.
2. Press , or the **Switch** soft key to select **Web Sign-in**.

3. Press the **Sign In** soft key.

The screen will show the pairing code and URL.

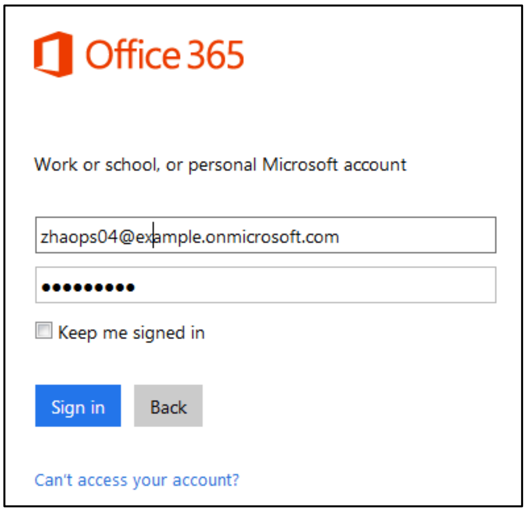


4. On your computer, enter the URL into your web browser.
5. On the Skype for Business Authentication website, enter your email address (e.g., zhaops04@example.onmicrosoft.com) in the **Email address** field.



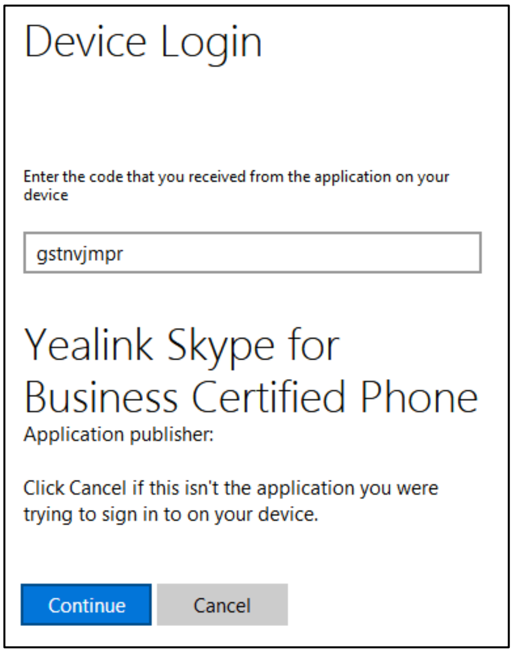
6. Click **Verify email** to check the validity of the email address.

   The sign-in screen will appear if the email address is valid.
7. Enter your Online account and password.



8. (Optional) Check the **Keep me signed in** checkbox, so that you don't need to enter a password next time.

9. Click **Sign in**.
10. Enter the pairing code generated on the phone (e.g., gstnvjmpr) into the web browser.



11. Click **Continue**.
12. Click the account to sign in.

    A confirmation message is displayed when your phone successfully signs into Skype for Business.

Sign in via PC

When your phone and your computer are paired using Better Together over Ethernet (BToE), you can sign into your phone using the Skype for Business client on your computer. For more information, refer to BToE on page 268. It is not applicable to CP960 Skype for Business phones.

Remember Password

You can enable the remember password feature, so that a **Remember Password** option will appear at the phone login screen.

Note Remember password feature is only applicable to **PIN Authentication** and **User Sign-in** method.

Procedure

Remember password can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the remember password feature. **Parameters:** features.remember_password.enable
Local	Web User Interface	Configure the remember password feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

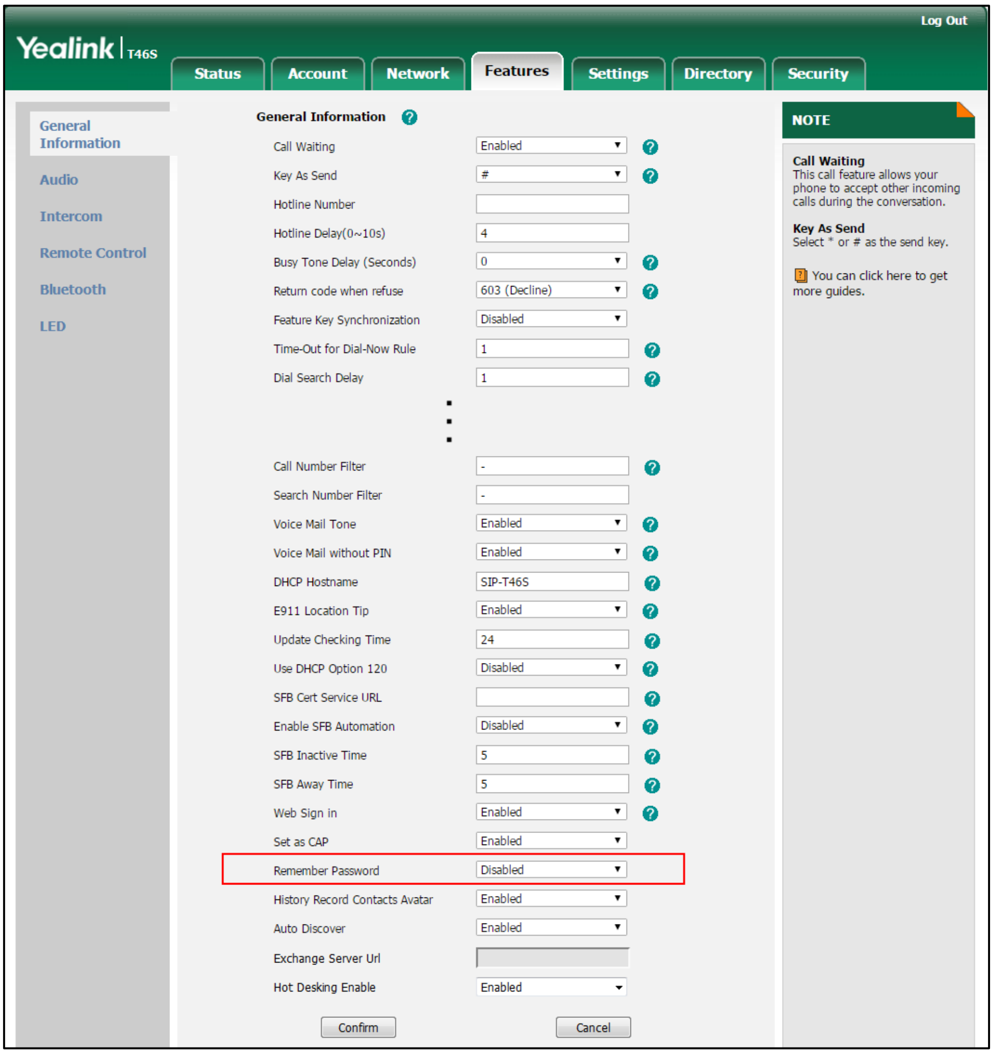
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.remember_password.enable	**0 or 1**	**0**
Description: Enables or disables a **Remember Password** option to appear at the phone login screen. **0**-Disabled **1**-Enabled, a **Remember Password** option will appear at the phone login screen. **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->General Information->Remember Password		

To configure remember password feature via web user interface:

1. Click on **Features**->**General Information**.

2. Select **Enabled** from the pull-down list of **Remember Password.**



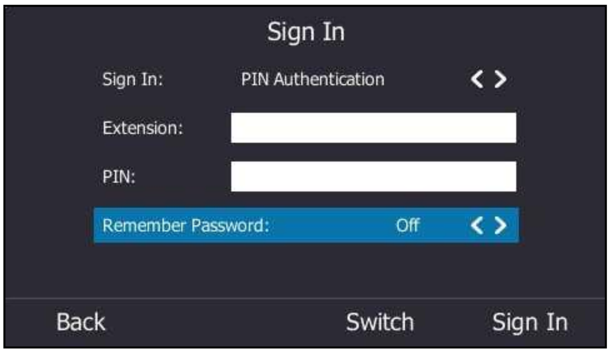
3. Click **Confirm** to accept the change.

   A dialog box pops up to prompt you that this configuration will take effect after a reboot.

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

The login screen will be shown as below:

(User Sign-in method)



(PIN Authentication method)

Signing Out of Skype for Business

Procedure

Sign-out can be configured using the configuration files or locally.

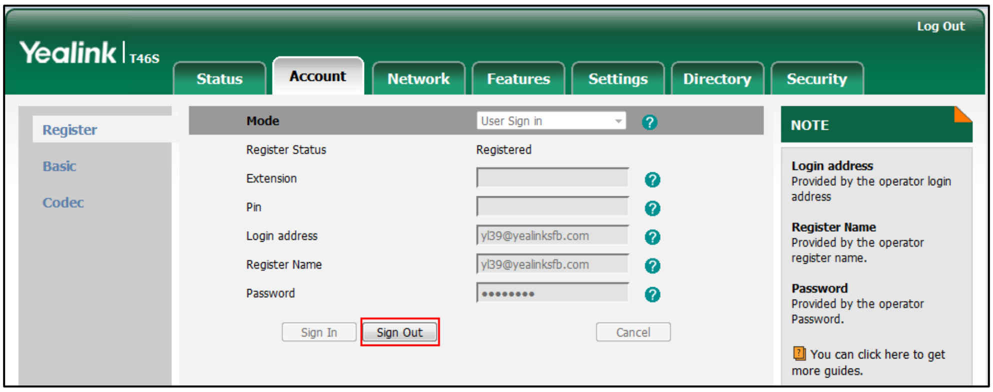
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the sign out feature. **Parameters:** phone_setting.idle_sign_out.enable
Local	Web User Interface	Sign out of Skype for Business Server. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-register-lync&q=load&acc=0
	Phone User Interface	Sign out of Skype for Business Server.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.idle_sign_out.enable	**0 or 1**	**0**
Description: Enables or disables the phone to sign out of Skype for Business Server from the idle screen. **0**-Disabled, users can sign out of Skype for Business Server from the menu **More**->**Advanced**->**Sign Out**. **1**-Enabled, users can sign out of Skype for Business Server by tapping the avatar and then selecting **Sign Out** from the idle screen. **Note:** It is only applicable to CP960 Skype for Business phones.		

To sign out of Skype for Business Server via web user interface:

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



2. Click **Sign Out** to accept the change.

To sign out of Skype for Business Server via phone user interface:

1. Press the **Status** soft key.
2. Press or to select **Sign Out**.

   The phone signs out of Skype for Business Server.

   After you sign out of Skype for Business, the account-related features (call or view your Skype for Business contacts, etc.) are not available. However, you can still use other available features.

For more information on how to sign out of Skype for Business Server, refer to *Yealink Skype for Business phone-specific user guide*.

Microsoft Exchange Integration

The Skype for Business phone can obtain Microsoft Exchange Server address automatically via

Auto discover request. This feature enables set up of visual voicemail, call log synchronization, Outlook contact search, and calendar retrieval.

If your phone fails to obtain the Microsoft Exchange Server address automatically, you can manually configure the address.

Procedure

Microsoft Exchange Server can be configured using the configuration files or locally.

<table>
<tr><td rowspan="2">Central Provisioning (Configuration File)</td><td rowspan="2"><y0000000000xx>.cfg</td><td>Configures the way to obtain Microsoft Exchange Server address.
Parameter:
phone_setting.ews_autodiscover.enable</td></tr>
<tr><td>Specify the Microsoft Exchange Server address manually.
Parameter:
phone_setting.ews_url</td></tr>
<tr><td>Local</td><td>Web User Interface</td><td>Configures the way to obtain Microsoft Exchange Server address.
Specify the Microsoft Exchange Server address.
Navigate to:
http://<phoneIPAddress>/servlet?p=features-general&q=load</td></tr>
</table>

Details of Configuration Parameters:

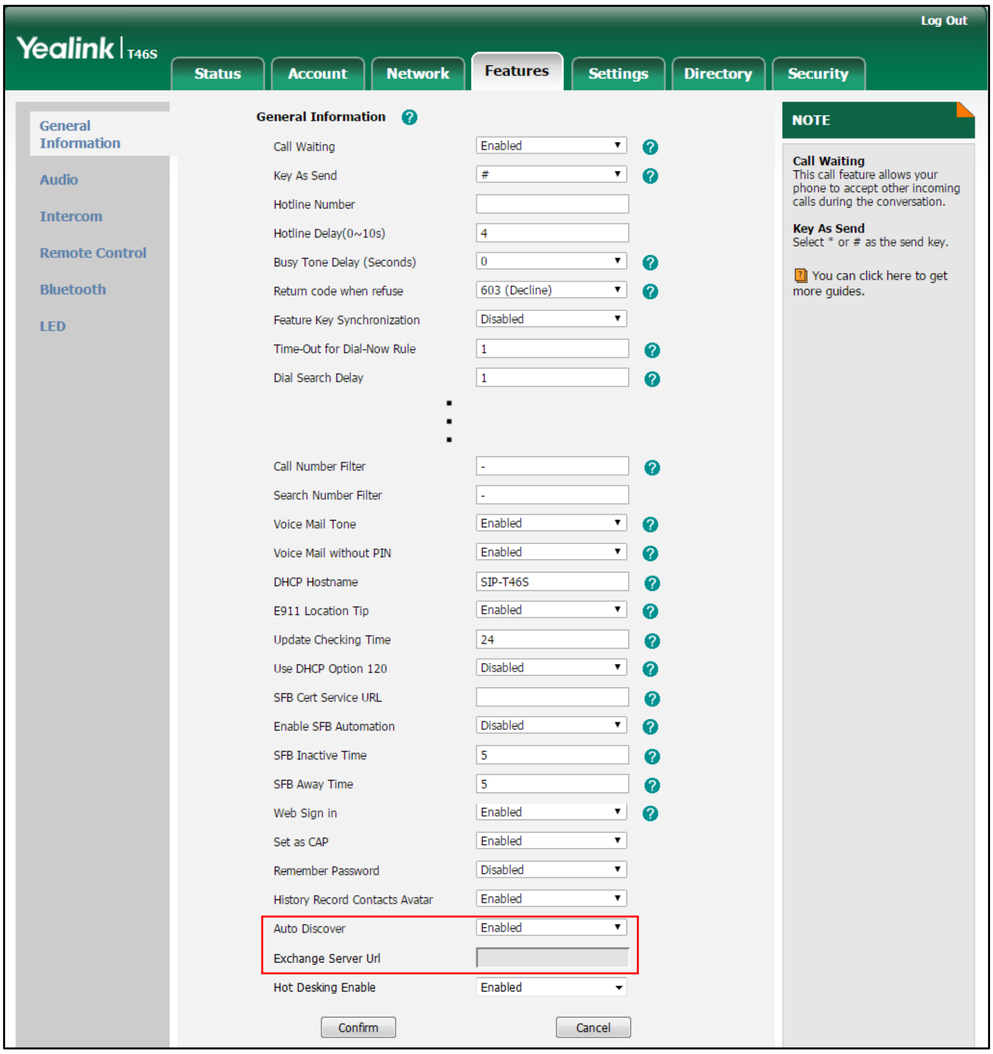
<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>phone_setting.ews_autodiscover.enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Description:
Enables or disables the phone to obtain the Microsoft Exchange Server address automatically via Auto discover request.
0-Disabled, the phone does not obtain Microsoft Exchange Server address automatically via Auto discover request. You need to configure the Microsoft Exchange Server address manually.
1-Enabled, the phone will obtain Microsoft Exchange Server address automatically via Auto discover request.
Web User Interface:
Features->General Information->Auto Discover</td></tr>
</table>

Parameters	Permitted Values	Default
Phone User Interface: None		
phone_setting.ews_url	**String**	**Blank**
Specify the Microsoft Exchange Server address manually**.** **Note:** It works only if the value of the parameter "phone_setting.ews_autodiscover.enable" is set to 0 (Disabled). **Web User Interface:** Features->General Information->Exchange Server Url **Phone User Interface:** None		

To configure the Microsoft Exchange Server via web user interface:

1. Click on **Features**->**General Information**.
2. Do one of the following:
   - If you select **Enabled** from the pull-down list of **Auto Discover**, the phone can obtain Microsoft Exchange Server address automatically.

- If you select **Disabled** in the pull-down list of **Auto Discover**, you should enter the Microsoft Exchange Server address in the **Exchange Server Url** field.



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

Exchange Authentication

You need to pass Exchange authentication to access features that associated with the Microsoft Exchange Server (history records, voice mail, Outlook contacts and calendars). By default, your phone will pass Exchange authentication automatically when you access these feature. You may need to enter Exchange authentication information manually when your login password expires, or changed by system administrator.

Procedure

Exchange authentication can be configured using the configuration files only.

Central	<MAC>.cfg	Configures the Exchange address for accessing the Microsoft Exchange

Provisioning (Configuration File)		Server. **Parameter:** static.account.1.ews.auth_address
		Configures the user name for accessing the Microsoft Exchange Server. **Parameter:** static.account.1.ews.auth_user
		Configures the password for accessing the Microsoft Exchange Server. **Parameter:** static.account.1.ews.auth_pwd
Local	Phone User Interface	Configure the Exchange authentication information.

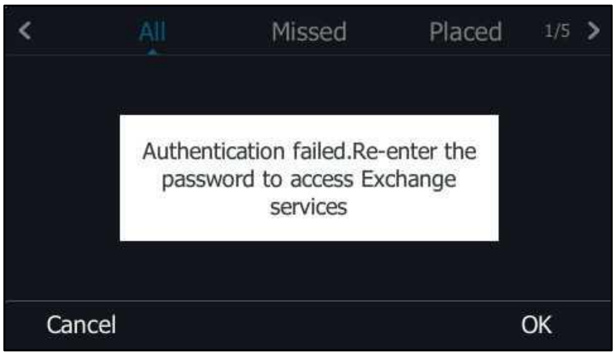
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.account.1.ews.auth_address	**String within 128 characters**	**Blank**
Description: Configures the Exchange address for accessing the Microsoft Exchange Server. **Example:** static.account.1.ews.auth_address = yl39@redmond.yealinksfb.com **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** On the authentication dialog box->Sign in address		
static.account.1.ews.auth_user	**String within 129 characters**	**Blank**
Description: Configures the user name for accessing the Microsoft Exchange Server. **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Example:** static.account.1.ews.auth_user = yl39@yealinksfb.com **Web User Interface:** None		

Parameters	Permitted Values	Default
Phone User Interface: On the authentication dialog box->User name		
static.account.1.sign_in.password	**String within 130 characters**	**Blank**
Description: Configures the password for accessing the Microsoft Exchange Server. **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** On the authentication dialog box->Password		

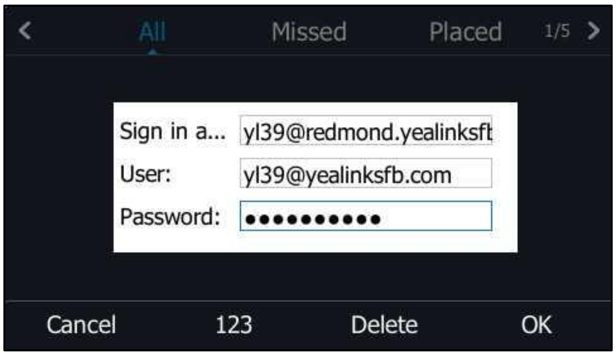
To configure Exchange authentication via phone user interface:

1. When your login password has expired, or changed by your system administrator, and you access history records, voice mail or calendar features that are associated with the Microsoft Exchange Server, a message is displayed on the LCD screen:



2. Press **OK**.

3. Enter authentication credentials in corresponding fields.



4. Press **OK** to accept the change.

Updating Status Automatically

The Skype for Business Server helps you keep your presence information up-to-date by monitoring idle time of your phone. Phone status will be Inactive when your phone has been idle for the designated time. Phone status will change from Inactive to Away after another designated time.

Procedure

Updating status automatically can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configures the inactive time (in minutes) of the phone. **Parameters:** sfb.presence.inactive_time sfb.presence.away_time
Local	Web User Interface	Configures the inactive time (in minutes) of the phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameters:

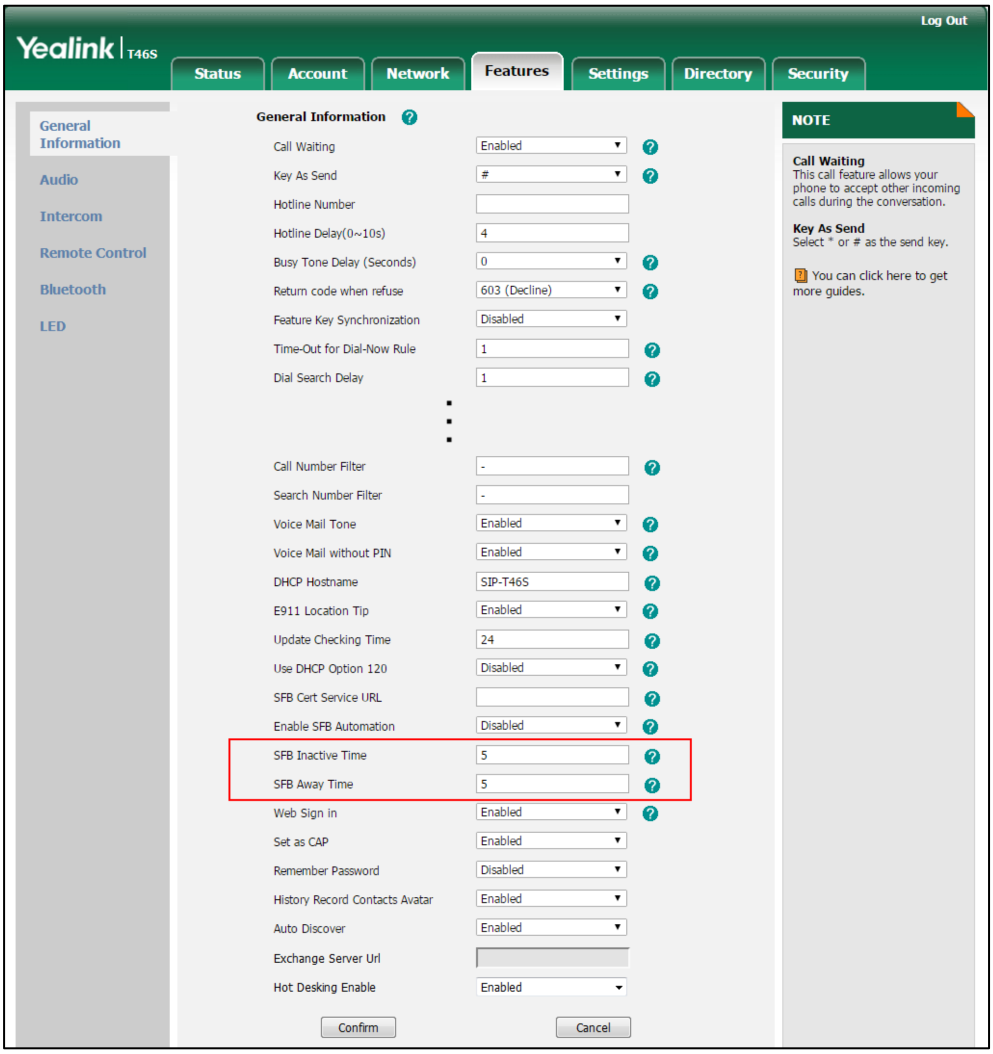
Parameters	Permitted Values	Default
sfb.presence.inactive_time	**Integer from 5 to 360**	**5**
Description: Configures the inactive time (in minutes) of the phone, after which the phone will change its status to Inactive automatically.		

Example: If it is set to 5, the phone will change its status to Inactive automatically when inactive time reaches 5 minutes. **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Features->General Information->SFB Inactive Time **Phone User Interface:** None		
sfb.presence.away_time	**Integer from 5 to 360**	**5**
Description: Configures the inactive time (in minutes) of the phone, after which the phone will change its status from Inactive to Away automatically. **Example**: If it is set to 5, the phone whose status is Inactive will change to Away automatically after 5 minutes. **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Features->General Information->SFB Away Time **Phone User Interface:** None		

To configure the automatic status updating time via web user interface:

1. Click on **Features**->**General Information**.
2. Enter the desired time in the **SFB Inactive Time** field.

3. Enter the desired time in the **SFB Away Time** field.



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

Always Online

Always on line feature allow the phone to maintain the current status until you manually change it. For example, the current status of the phone is Available, if the always online feature is enabled, then the phone status will stay Available until you manually change it.

Procedure

Always on line can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure always on line. **Parameter:** sfb.always_online.enable

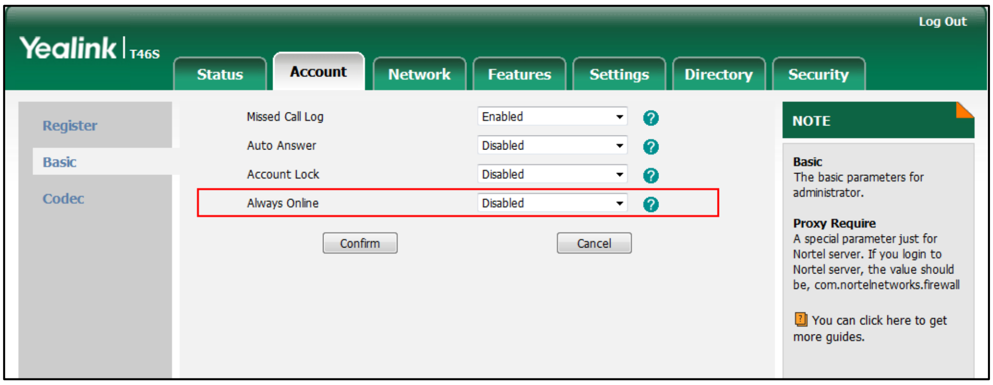
Local	Web User Interface	Configure always on line. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sfb.always_online.enable	**0 or 1**	**0**
Description: Enables or disables the phone to maintain current status until you manually change it. **0**-Disabled **1**-Enabled **Note:** If your phone status is DND before dialing an emergency number, then the phone status will be changed to available after the emergency call even if the value of this parameter is set to 1 (Enabled). **Web User Interface:** Account->Basic->Always Online **Phone User Interface:** Menu->Basic->Always Online (It is not applicable to CP960 Skype for Business phones.)		

To configure always on line via web user interface:

1. Click on **Account**->**Basic**.
2. Select the desired value from the pull-down list of **Always Online**.



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

To configure always online via phone user interface:

1. Press **Menu->Basic->Always Online**.

2. Press or , or the **Switch** soft key to select the desired value from the **Always Online** field.
3. Press the **Save** soft key to accept the change.

Power LED indicator

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

There are six configuration options for power LED indicator:

Common Power Light On

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

Ring Power Light Flash

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

Voice Mail Power Light Flash

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

Mute Power Light On

Mute Power Light On allows the power LED indicator to flash when a call is mute.

Hold/Held Power Light On

Hold/Held Power Light On allows the power LED indicator to flash when a call is placed on hold or is held.

Talk/Dial Power Light On

Talk/Dial Power Light On allows the power LED indicator to be turned on when the phone is busy.

Boss/Admin Power Light On

Boss/Admin Power Light On allows the power LED indicator to be turned on when using the Boss-Admin Feature.

Procedure

Power LED indicator can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the power LED indicator. **Parameters:** phone_setting.common_power_led_enable

		phone_setting.ring_power_led_flash_enable phone_setting.mail_power_led_flash_enable phone_setting.mute_power_led_flash_enable phone_setting.hold_and_held_power_led_flash_enable phone_setting.talk_and_dial_power_led_enable phone_setting.boss_admin.talk_power_light.enable
Local	Web User Interface	Configure the power LED indicator. **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 power LED indicator to be turned on. **0**-Disabled (power LED indicator is off) **1**-Enabled (power LED indicator is solid red) **Note**: It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->LED->Common Power Light On **Phone User Interface:** None		
phone_setting.ring_power_led_flash_enable	**0 or 1**	**1**
Description: Enables or disables the power LED indicator to flash when the phone receives an incoming call. **0**-Disabled (power LED indicator does not flash) **1**-Enabled (power LED indicator fast flashes (300ms) red) **Note**: It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->LED->Ring Power Light Flash **Phone User Interface:** None		

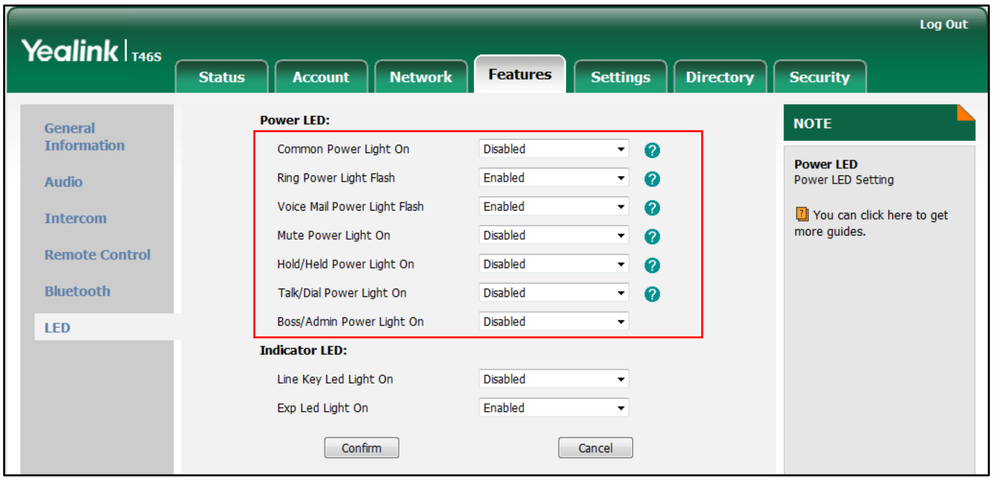
Parameters	Permitted Values	Default
phone_setting.mail_power_led_flash_enable	**0 or 1**	**0**
Description: Enables or disables the power LED indicator to flash when the phone receives a voice mail. **0**-Disabled (power LED indicator does not flash) **1**-Enabled (power LED indicator slow flashes (1000ms) red) **Note**: It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->LED->Voice Mail Power Light Flash **Phone User Interface:** None		
phone_setting.mute_power_led_flash_enable	**0 or 1**	**0**
Description: Enables or disables the power LED indicator to flash when a call is mute. **0**-Disabled (power LED indicator does not flash) **1**-Enabled (power LED indicator fast flashes (300ms) red) **Note**: It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->LED->Mute Power Light On **Phone User Interface:** None		
phone_setting.hold_and_held_power_led_flash_enable	**0 or 1**	**0**
Description: Enables or disables the power LED indicator to flash when a call is placed on hold or is held. **0**-Disabled (power LED indicator does not flash) **1**-Enabled (power LED indicator fast flashes (500ms) red) **Note**: It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->LED->Hold/Held Power Light On **Phone User Interface:** None		
phone_setting.talk_and_dial_power_led_enable	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Enables or disables the power LED indicator to be turned on when the phone is busy. **0**-Disabled (power LED indicator is off) **1**-Enabled (power LED indicator is solid red) **Note**: It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->LED->Talk/Dial Power Light On **Phone User Interface:** None		
phone_setting.boss_admin.talk_power_light.enable	**0 or 1**	**0**
Description: Enables or disables the power LED indicator to be turned on when using the Boss-Admin feature. **0**-Disabled (power LED indicator is off) **1**-Enabled (power LED indicator is solid red) **Note**: It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->LED->Boss/Admin Power Light On **Phone User Interface:** None		

To configure the power LED indicator via web user interface:

1. Click on **Features**->**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 Mail Power Light Flash**.
5. Select the desired value from the pull-down list of **Mute Power Light Flash**.
6. Select the desired value from the pull-down list of **Hold/Held Power Light Flash**.
7. Select the desired value from the pull-down list of **Talk/Dial Power Light On**.

8. Select the desired value from the pull-down list of **Boss/Admin Power Light On**.



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

Contrast

Contrast determines the readability of the texts displayed on the LCD screen/touch screen. Adjusting the contrast to a comfortable level can optimize the screen viewing experience. When configured properly, contrast allows users to read the LCD's display with minimal eyestrain. You can configure the LCD's contrast of EXP40 that is connected to T48S/T46S phones. Make sure the expansion module has been connected to the phone before adjustment.

Contrast is not applicable to T42S/T41S/CP960 Skype for Business phones.

Procedure

Contrast can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the contrast of the LCD screen/touch screen. **Parameter:** phone_setting.contrast
Local	Web User Interface	Configure the contrast of the LCD screen/touch screen. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Configure the contrast of the LCD screen/touch screen.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.contrast	**Integer from 1 to 10**	**6**
Description: Configures the contrast of the LCD screen/touch screen. For T48S/T46S Skype for Business phones, it configures the LCD's contrast of the connected EXP40 only. **Note:** We recommend that you set the contrast of the LCD screen/touch screen to 6 as a more comfortable level. It is not applicable to T42S/T41S/CP960 Skype for Business phones. **Web User Interface:** None **Phone User Interface:** Menu->Basic->Display->Contrast		

To configure the contrast via phone user interface:

1. Press **Menu**->**Basic**->**Display**->**Contrast**.

   If EXP40 is not connected to the phone, the Contrast Setting screen displays "No EXP".

2. Press  or , or the **Switch** soft key to increase or decrease the intensity of contrast.

   The default contrast level is "6".

3. Press the **Save** soft key to accept the change.

Screen Saver

The screen saver will automatically start when the phone has been idle for a certain amount of time if you have configured the screensaver wait time. You can stop the screen saver and return to the idle screen at any time by pressing a key on the phone or tapping the touch screen. The screen saver is only applicable to T48S/T46S/CP960 Skype for Business phones.

Users can select to display the built-in screen saver or a custom screen saver (not applicable to CP960 Skype for Business phones). To set the custom screen saver for the phone, you need to upload the custom screen saver in advance. If multiple pictures are uploaded, all pictures are displayed in slide-show style when screen saver starts.

For CP960 Skype for Business phone supports four screen saver types: Clock, Colors, Photo Frame and Photo Table, you can only configure the screen saver via phone user interface.

The screen saver image format must meet the following:

Phone Model	Format	Resolution	Single File Size	Note
T48S	*.jpg/*.png/*.bmp/*.jpeg	<=2.0 megapixels	<=5MB	2MB of space should be reserved for the phone
T46S		<=1.8 megapixels	<=5MB	

The following shows that the built-in screen saver is displaying on the phone:

Procedure

Screen saver can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the time to wait in the idle state before the screen saver starts. **Parameter:** screensaver.wait_time
		Configure the type of screen saver to display. **Parameter:** screensaver.type
		Specify the access URL of the custom screen saver image. **Parameter:** screensaver.upload_url
		Delete custom screen saver image. **Parameter:** screensaver.delete
		Configure the phone to display the clock

		and icons when the screen saver starts. **Parameter:** screensaver.display_clock.enable
		Configure the interval for the phone to change the picture when the screen saver starts. **Parameter:** screensaver.picture_change_interval
		Configure the interval for the phone to move the clock and icons when the screen saver starts. **Parameter:** screensaver.clock_move_interval
Web User Interface		Configure the idle time before the screen saver starts. Configure the type of screen saver to be displayed. Upload the custom screen saver image. Delete custom screen saver images. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load
Phone User Interface		Configure the screen saver.

Details of the Configuration Parameters:

Parameters	Permitted Values	Default
screensaver.wait_time	**15, 30, 60, 120, 300, 600, 1800, 3600, 7200, 10800, 21600**	**21600**
Description: Configures the time (in seconds) to wait in the idle state before the screen saver starts. **15**-15s **30**-30s **60**-1min **120**-2min		

Parameters	Permitted Values	Default
300-5min **600**-10min **1800**-30min **3600**-1h **3200**-2h **10800**-3h **21600**-6h **Note**: It is only applicable to T48S/T46S/CP960 Skype for Business phones. **Web User Interface:** Settings->Preference->Screensaver Wait Time (not applicable to CP960 Skype for Business phones.) **Phone User Interface:** Menu->Basic->Display->Screensaver->Wait Time		
screensaver.type	**0 or 1**	**0**
Description: Configures the type of screen saver to display. **0**-System, the LCD screen will display the built-in picture. **1**-Custom, the LCD screen will display the custom screen saver images (configured by the parameter "screensaver.upload_url"). If multiple images are uploaded, the phone will display all images alternately. The time interval is configured by the parameter "screensaver.picture_change_interval". **Note**: It is only applicable to T48S/T46S Skype for Business phones. **Web User Interface:** Settings->Preference->Screensaver Type **Phone User Interface:** Menu->Basic->Display->Screensaver->Screensaver Type **Note**: It is configurable only if you have uploaded custom image file(s) to the phone.		
screensaver.upload_url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom screen saver image. **Example:** screensaver.upload_url = http://192.168.10.25/Screencapture.jpg During the auto provisioning process, the phone connects to the HTTP provisioning server		

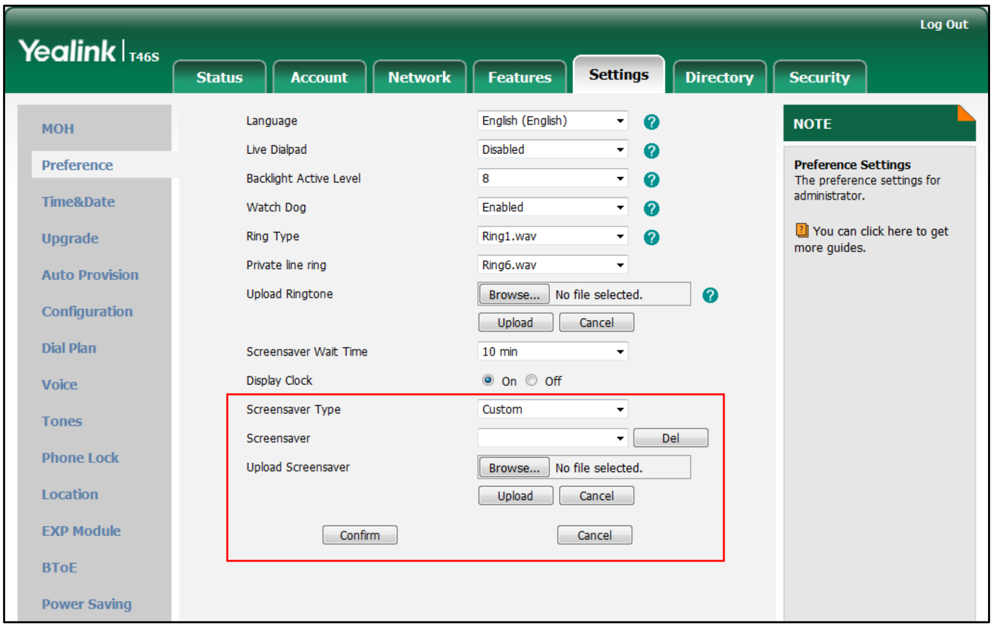
Parameters	Permitted Values	Default
"192.168.10.25", and downloads the screen saver image "Screencapture.jpg". If you want to download multiple screen saver images to the phone simultaneously, you can configure as following: screensaver.upload_url = http://192.168.10.25/Screencapture.jpg screensaver.upload_url = http://192.168.10.25/Screensaver.jpg **Note**: It works only if the value of the parameter "screensaver.type" is set to 1 (Custom). It is only applicable to T48S/T46S Skype for Business phones. **Web User Interface:** Settings->Preference->Upload Screensaver **Phone User Interface:** None		
screensaver.delete	**http://localhost/all or http://localhost/*name.(jpg/png/bmp)***	**Blank**
Description: Deletes the specified or all custom screen saver images. **Example:** Delete all custom screen saver images: screensaver.delete = http://localhost/all Delete a custom screen saver image (e.g., Screencapture.jpg): screensaver.delete = http://localhost/Screencapture.jpg **Note**: It is only applicable to T48S/T46S Skype for Business phones. **Web User Interface:** Settings->Preference->Del **Phone User Interface:** None		
screensaver.display_clock.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display the clock and icons when the screen saver starts. **0**-Disabled **1**-Enabled **Note**: It is only applicable to T48S/T46S Skype for Business phones. **Web User Interface:**		

Parameters	Permitted Values	Default
Settings->Preference->Display Clock **Phone User Interface:** Menu->Basic->Display->Screensaver->Display Clock		
screensaver.picture_change_interval	**Integer from 5 to 1200**	**60**
Description: Configures the interval (in seconds) for the phone to change the pictures when the screen saver starts. **Note**: It works only if the value of the parameter "screensaver.type" is set to 1 (Custom) and the parameter "screensaver.upload_url" should be configured in advance. It is only applicable to T48S/T46S Skype for Business phones. **Web User Interface:** None **Phone User Interface:** None		
screensaver.clock_move_interval	**Integer from 5 to 1200**	**600**
Description: Configures the interval (in seconds) for the phone to move the clock and icons when the screen saver starts. **Note**: It works only if the value of the parameter "screensaver.display_clock.enable" is set to 1 (Enabled). It is only applicable to T48S/T46S Skype for Business phones. **Web User Interface:** None **Phone User Interface:** None		

To upload custom screen saver via web user interface:

1. Click on **Settings**->**Preference**.
2. Select **Custom** from the pull-down list of **Screensaver Type**.
3. In the **Upload Screensaver** field, click **Browse** to locate the custom picture from your local system.
4. Click **Upload** to upload the file.

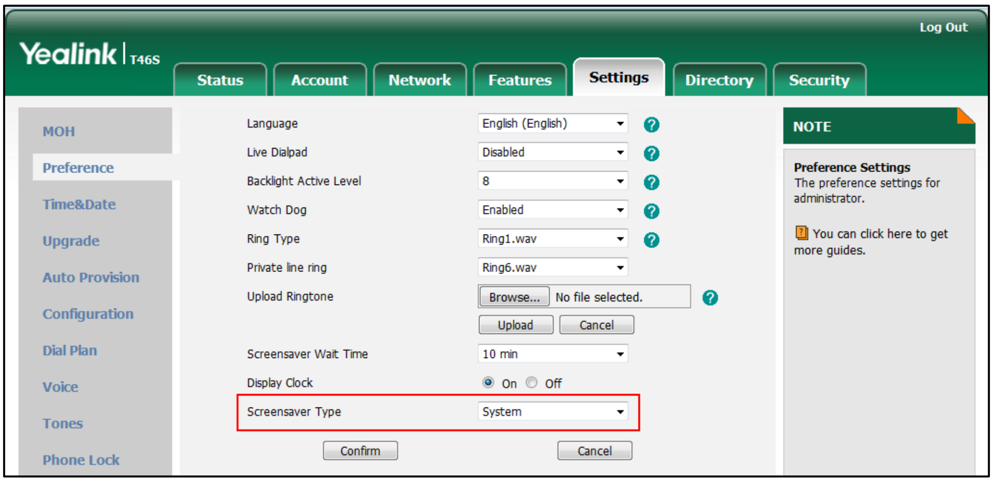
The **Upload Screensaver** field appears only if **Screensaver Type** is set to **Custom**.



The custom screen saver appears in the pull-down list of **Screensaver**. The **Screensaver** field appears only if **Screensaver Type** is set to **Custom**.

To set the system screen saver via web user interface:

1. Click on **Settings**->**Preference**.
2. Select **System** from the pull-down list of **Screensaver Type**.

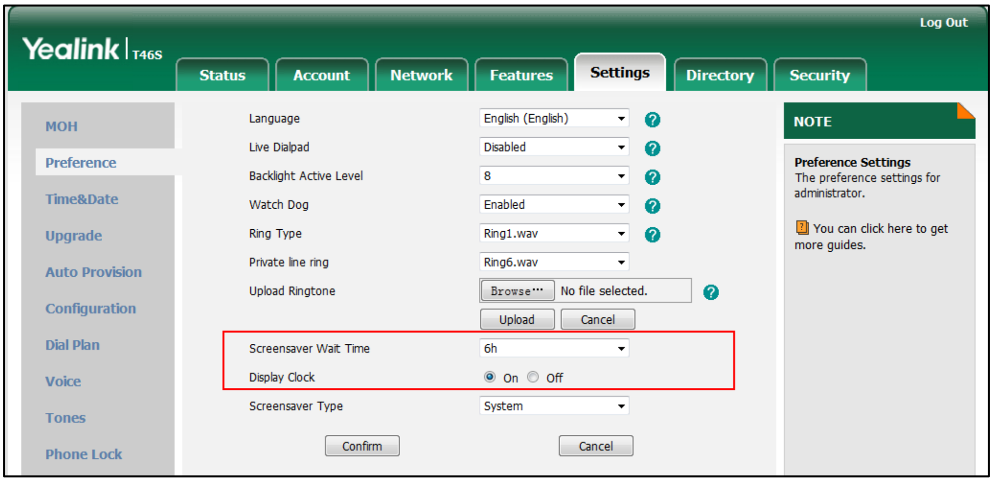


3. Click **Confirm** to accept the change.

To configure the screen saver wait time and screensaver display clock via web user interface:

1. Click on **Settings**->**Preference**.
2. Select the desired time from the pull-down list of **Screensaver Wait Time**.

3. Mark the desired radio box in the **Display Clock** field.



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

To configure the screen saver via phone user interface:

1. Press **Menu**->**Basic**->**Display**->**Screensaver**.
2. Press or , or the **Switch** soft key to select the desired wait time from the **Wait Time** field.
3. Press or , or the **Switch** soft key to select the desired value from the **Display Clock** field.
4. Press or , or the **Switch** soft key to select the desired value from the **Screensaver Type** field.

   This field is available only if you have uploaded custom image file(s) via web user interface.
5. Press the **Save** soft key to accept the change.

Power Saving

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

For T46S/T48S Skype for Business phones, if you connect an expansion module EXP40 to the phone, the phone and EXP40 will enter or exit power-saving mode synchronously.

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

You can configure the following power-saving settings:

- **Office Hour**: When you start work and how long you work each day.
- **Idle TimeOut (minutes)**: The period of time the phone should be idle before the screen turns off.

  You can specify different timeouts for office hours (Office Hour Idle Timeout) and non-office hours (Off Hour Idle Timeout). By default, the Office Hours Idle Timeout is much longer than the Off Hours Idle Timeout.

  You can also specify a separate timeout period that applies after you press a key or tap the screen. This is called the User Input Extention Idle TimeOut. You can choose to set a higher User Input Extention Idle TimeOut than the Office Hours and Off Hours Idle Timeouts, so that when you're actively using the phone, power-saving mode won't initiate as often.

Note To determine which idle timeout applies：If you press a key or tap the screen, the idle timeout period that applies (User Input Extention Idle TimeOut or Office Hours/Off Hours Idle Timeout) will be the timeout with the highest value.

Procedure

Power saving can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the power-saving feature. **Parameter:** features.power_saving.enable
		Configure the office hour. **Parameters:** features.power_saving.office_hour.monday features.power_saving.office_hour.tuesday features.power_saving.office_hour.wednesday features.power_saving.office_hour.thursday features.power_saving.office_hour.friday features.power_saving.office_hour.saturday features.power_saving.office_hour.sunday
		Configures idle time before the phone enters power-saving mode. **Parameters:** features.power_saving.office_hour.idle_timeout features.power_saving.off_hour.idle_timeout features.power_saving.user_input_ext.idle_timeout

Web User Interface	Configure the power-saving feature. Configure the office hour. Configures idle time before the phone enters power-saving mode. **Navigate to:** http://<phoneIPAddress/servlet?p=settings-powersaving&q=load

Details of the Configuration Parameters:

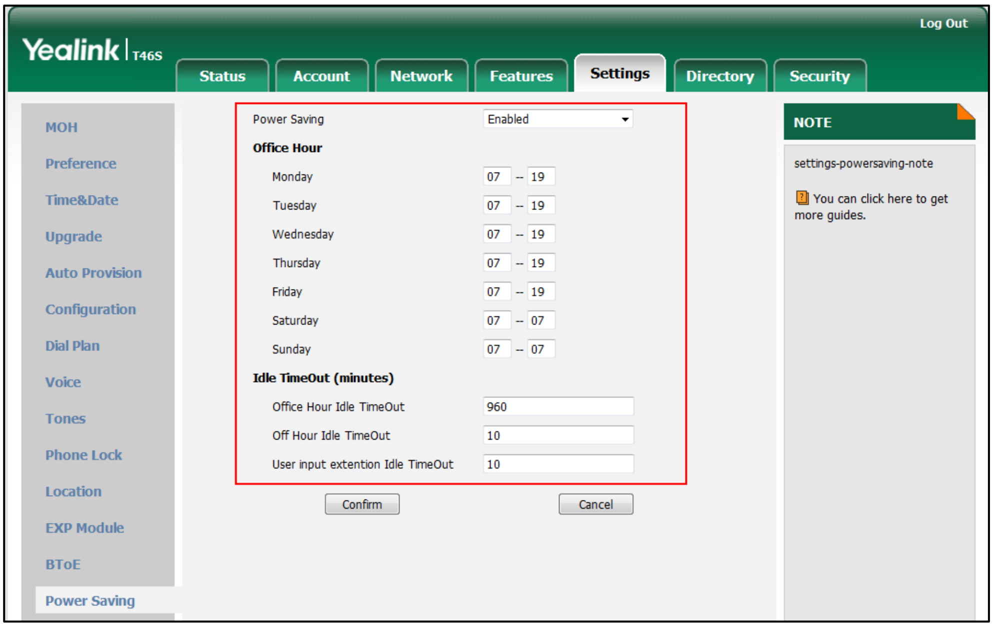
Parameters	Permitted Values	Default
features.power_saving.enable	**0 or 1**	**1**
Description: Enables or disables the power-saving feature. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Power Saving->Power Saving **Phone User Interface:** None		
features.power_saving.office_hour.idle_timeout	**Integer from 1 to 960**	**960**
Description: Configures the time (in minutes) to wait in the idle state before the phone enters power-saving mode during the office hours. **Example**: features.power_saving.office_hour.idle_timeout = 600 The phone will enter power-saving mode when it has been inactivated for 600 minutes (10 hour) during the office hours. **Web User Interface:** Settings->Power Saving->Office Hour Idle TimeOut **Phone User Interface:** None		
features.power_saving.off_hour.idle_timeout	**Integer from 1 to 10**	**10**

Parameters	Permitted Values	Default
Description: Configures the time (in minutes) to wait in the idle state before the phone enters power-saving mode during the non-office hours. **Example**: features.power_saving.off_hour.idle_timeout = 10 The phone will enter power-saving mode when it has been inactivated for 10 minutes during the non-working hours. **Web User Interface:** Settings->Power Saving->Off Hour Idle TimeOut **Phone User Interface:** None		
features.power_saving.user_input_ext.idle_timeout	**Integer from 1 to 30**	**10**
Description: Configures the minimum time (in minutes) to wait in the idle state - after using the phone - before the phone enters power-saving mode. **Example**: features.power_saving.user_input_ext.idle_timeout = 10 **Web User Interface:** Settings->Power Saving->User input extension Idle TimeOut **Phone User Interface:** None		
features.power_saving.office_hour.monday **features.power_saving.office_hour.tuesday** **features.power_saving.office_hour.wednesday** **features.power_saving.office_hour.thursday** **features.power_saving.office_hour.friday** **features.power_saving.office_hour.saturday** **features.power_saving.office_hour.sunday**	**Integer from 0 to 23, Integer from 0 to 23**	**7,19** **7,19** **7,19** **7,19** **7,19** **7,7** **7,7**
Description: Configures the starting time and ending time of the day's office hour. Starting time and ending time are separated by a comma. **Example**: features.power_saving.office_hour.monday = 7,19		

Parameters	Permitted Values	Default
Web User Interface: Settings->Power Saving->Monday/Tuesday/Wednesday/Thursday/Friday/Saturday/Sunday **Phone User Interface**: None		

To configure the power-saving feature via web user interface:

1. Click on **Settings**->**Power Saving**.
2. Enter the start time and end time respectively in the desired field.
3. Enter the desired value (1-960) in the **Office Hours Idle TimeOut** field.
4. Enter the desired value (1-10) in the **Off Hours Idle TimeOut** field.
5. Enter the desired value (1-30) in the **User input extension Idle TimeOut** field.



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

Backlight

Backlight determines the brightness of the screen display, allowing users to read easily in dark environments. Backlight time specifies the delay time to change the intensity of the screen when the phone is inactive. Backlight turns off quickly if a short backlight time is configured, this may not give users enough time to read messages.

Backlight Active Level is used to adjust the backlight intensity of the screen when the phone is active. It is applicable to CP960 Skype for Business phones, T48S/T46S Skype for Business phones and the connected EXP40 and.

Backlight Inactive Level is used to adjust the backlight intensity of the LCD screen/touch screen when the phone is inactive. It is only applicable to T48S/T46S Skype for Business phones.

Backlight Time is used to specify the delay time to turn off the backlight when the phone is inactive.

Note

> Before you adjust the LCD's backlight of expansion module, make sure the expansion module has been connected to the Skype for Business phone.

The following table lists available methods and configuration options to configure the backlight of phone models.

Phone Model (and the connected expansion module)	Configuration Methods	Configuration Options
T48S/T46S	Configuration Files Phone User Interface	Inactive Level
T48S/T46S/EXP40	Configuration Files Web User Interface Phone User Interface	Backlight Active Level
CP960	Configuration Files Web User Interface Phone User Interface	Backlight Active Level
	Phone User Interface	Backlight Time

Procedure

Backlight can be configured using the configuration files or locally.

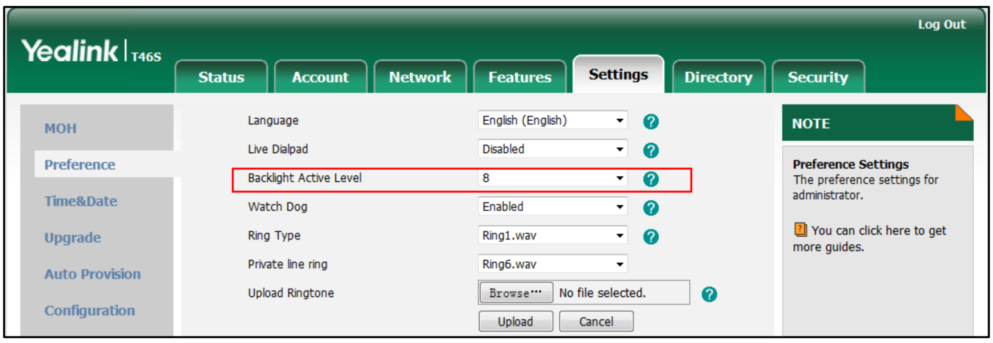
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the backlight of the LCD screen/touch screen. **Parameters:** phone_setting.active_backlight_level phone_setting.inactive_backlight_level
Local	Web User Interface	Configure the backlight of the LCD screen/touch screen. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Configure the backlight of the LCD screen/touch screen.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.active_backlight_level	**Integer from 1 to 10**	**10**
Description: Configures the intensity of the LCD screen/touch screen when the phone is active. 10 is the highest intensity. For T48S/T46S Skype for Business phones, it configures the LCD's intensity of the phone and the connected EXP40. **Note:** It is applicable to CP960 Skype for Business phones, T48S/T46S Skype for Business phones and the connected EXP40. **Web User Interface:** Settings->Preference->Backlight Active Level **Phone User Interface:** Menu->Basic->Display->Backlight->Backlight Active Level		
phone_setting.inactive_backlight_level	**0 or 1**	**1**
Description: Configures the intensity of the LCD screen/touch screen when the phone is inactive. **0**-Off **1**-Low **Note:** It is only applicable to T48S and T46S Skype for Business phones. **Web User Interface:** None **Phone User Interface:** Menu->Basic->Display->Backlight->Inactive Level		

To configure the backlight via web user interface:

1. Click on **Settings**->**Preference**.
2. Select the desired value from the pull-down list of **Backlight Active Level**.



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

To configure the backlight via phone user interface:

1. Press **Menu**->**Basic**->**Display**->**Backlight**.
2. Press or , or the **Switch** soft key to select the desired level from the **Backlight Active Level** field.
3. Press or , or the **Switch** soft key to select the desired value from the **Inactive Level** field.
4. Press the **Save** soft key to accept the change.

Bluetooth

Bluetooth enables low-bandwidth wireless connections within a range of 10 meters (32 feet). The best performance is in the 1 to 2 meters (3 to 6 feet) range. You can activate/deactivate the Bluetooth mode and then pair and connect the Bluetooth headset with your phone. For more information, refer to *Yealink Skype for Business phone-specific user guide*. It is only applicable to T48S/T46S Skype for Business phones.

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

Note To use this feature on T48S/T46S Skype for Business phones, make sure the Bluetooth USB dongle is properly connected to the USB port on the back of the phone.

Procedure

Bluetooth mode can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure Bluetooth mode. **Parameter:** features.bluetooth_enable
		Configure the Bluetooth device name. **Parameter:** features.bluetooth_adapter_name
Local	Web User Interface	Configure Bluetooth mode. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-bluetooth&q=load
	Phone User Interface	Configure Bluetooth mode. Configure the Bluetooth device

		name.

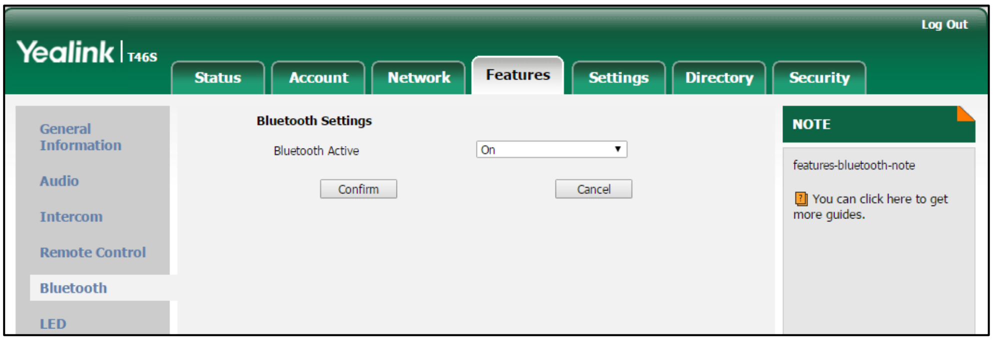
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.bluetooth_enable	**0 or 1**	**0**
Description: Triggers Bluetooth mode to on or off. **0**-Off **1**-On **Note:** It is only applicable to T48S/T46S Skype for Business phones. **Web User Interface:** Features->Bluetooth->Bluetooth Active **Phone User Interface:** Menu->Basic->Bluetooth->Bluetooth		
features.bluetooth_adapter_name	**String within 64 characters**	**Refer to the following content**
Description: Configures the Bluetooth device name. **For T48S Skype for Business phones:** The default value is Yealink T48S. **For T46S Skype for Business phones:** The default value is Yealink T46S. **Note**: It works only if the value of the parameter "features.bluetooth_enable" is set to 1 (On). It is only applicable to T48S/T46S Skype for Business phones. **Web User Interface:** None **Phone User Interface:** Menu->Basic->Bluetooth->Bluetooth (On)->Edit My Device Information->Device Name		

To active the Bluetooth mode via web user interface:

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

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



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

To active the Bluetooth mode via phone user interface:

1. Press **Menu**->**Basic**->**Bluetooth**.
2. Press or , or the **Switch** soft key to select **On** from the **Bluetooth** field.
3. Press the **Save** soft key to accept the change.

To edit device information via phone user interface:

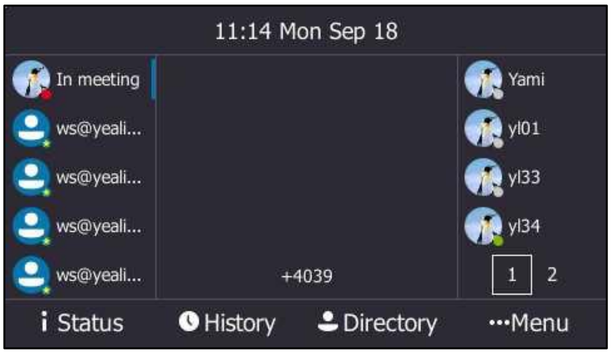
1. Press **Menu**->**Basic**->**Bluetooth**.
2. Press or , or the **Switch** soft key to select **On** from the **Bluetooth** field.
3. Press the **Save** soft key to accept the change.
4. Select **Edit My Device Information** and then press the **Enter** soft key.

   The LCD screen displays the device name and MAC address. The MAC address cannot be edited.
5. Enter the desired name in the **Device Name** field.
6. Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

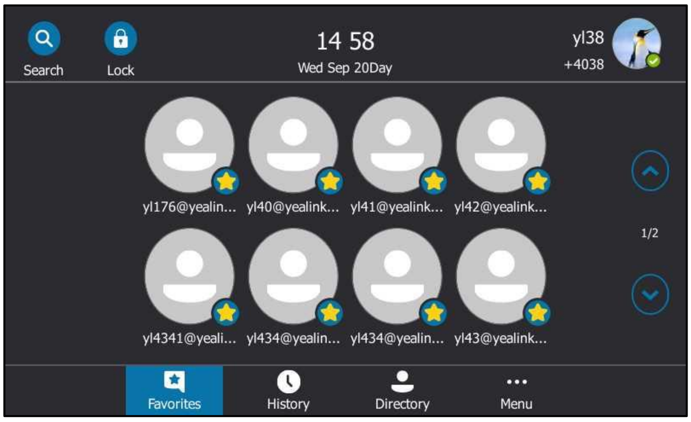
Showing Full Name

Showing full name allows the phone to extend the display length of the line key (For T46S) or display length of the favorites' names on the **Favorites** screen (For T48S). If the showing full name feature is enabled, more characters can be displayed. Showing full name feature is only applicable to T48S/T46S Skype for Business phones.

When showing full name feature is set to **Off**:



T46S Skype for Business phone



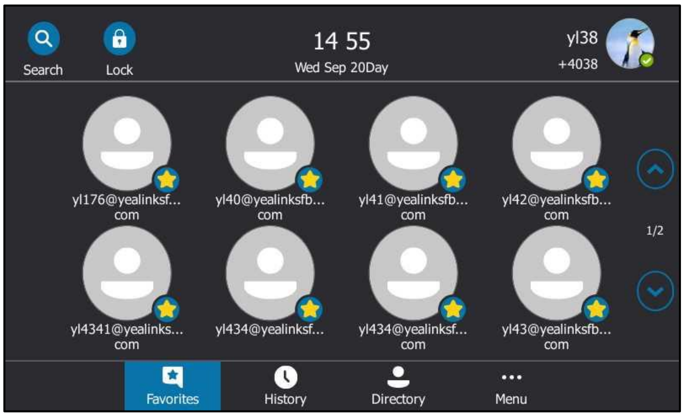
T48S Skype for Business phone

When showing full name feature is set to **On**:

For T46S Skype for Business phones, the display length of the line key label is extended and more characters can be displayed:

T46S Skype for Business phone

For T48S Skype for Business phones, the display length of the favorites' names on the **Favorites** screen are extended and characters can be displayed in two lines.



T48S Skype for Business phone

Procedure

Showing full name can be configured using the following methods.

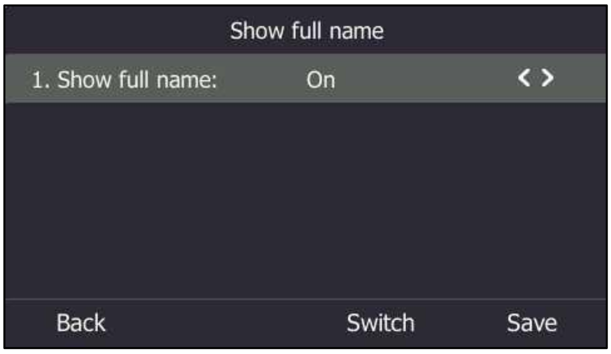
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the idle screen to show full name. **Parameter:** phone_setting.name_full_display.enable
Phone User Interface		Configure the idle screen to show full name.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.name_full_display.enable	**0 or 1**	**0**
Description: Enables or disables the phone to extend the display length of the line key (For T46S) or display length of the favorites' names on the **Favorites** screen (For T48S). **0**-Off **1**-On **Note**: It is only applicable to T48S/T46S Skype for Business phones. If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** Menu->Basic->Display->Show full name		

To configure the idle screen to display full name via phone user interface:

1. Press **Menu**->**Basic**->**Display**->**Show full name**.
2. Press or , or the **Switch** soft key to select **On** from the **Show full name** field.



3. Press the **Save** soft key to accept the change.

   The phone will reboot to make the change take effect.

Time and Date

Phones maintain a local clock and calendar. Time and date are displayed on the idle screen of phones.

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

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

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

NTP Time Server

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

The 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 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 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 configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the NTP server. **Parameters:** phone_setting.hide_ntp_server.enable
	<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

Local	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
	Phone User Interface	Configure DHCP time feature. Configure the NTP server and time zone.

Details of Configuration Parameters:

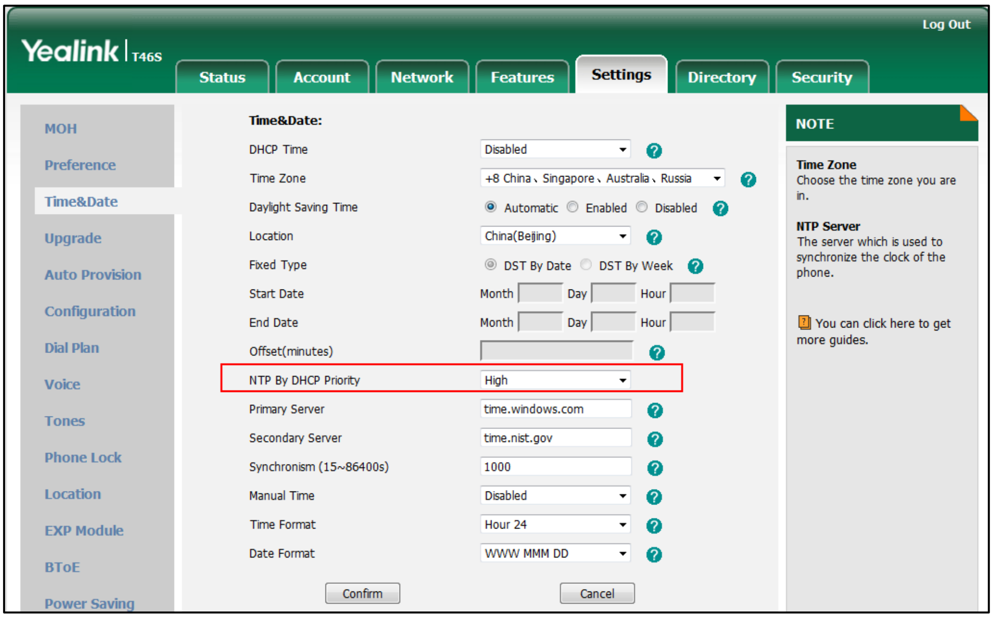
Parameters	Permitted Values	Default
local_time.manual_ntp_srv_prior	**0 or 1**	**0**
Description: Configures the priority for the phone to use the NTP server address offered by the DHCP server. **0**-High, use the NTP server address offered by the DHCP server preferentially **1**-Low, use the NTP server address configured manually preferentially **Web User Interface:** Settings->Time & Date->NTP by DHCP Priority **Phone User Interface:** None		
local_time.dhcp_time	**0 or 1**	**0**
Description: Enables or disables the 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 GMT 0. **Web User Interface:** Settings->Time & Date->DHCP Time **Phone User Interface:** Menu->Basic->Date & Time->DHCP Time		
phone_setting.hide_ntp_server.enable	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: It enables or disables the phone to hide NTP Server configurations on the LCD screen/touch screen. **0**-Disabled **1**-Enabled, the NTP Server configurations on the LCD screen/touch screen will be hidden, so that you cannot configure NTP Server address manually. **Web User Interface:** None **Phone 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. **Example:** local_time.ntp_server1 = 192.168.0.5 **Web User Interface:** Settings->Time & Date->Primary Server **Phone User Interface:** Menu->Basic->Date & Time->General->SNTP Settings->NTP Server1		
local_time.ntp_server2	**IP Address or Domain Name**	**cn.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 or cannot be accessed, the 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 **Phone User Interface:** Menu->Basic->Date & Time->General->SNTP Settings->NTP Server2		
local_time.interval	**Integer from 15 to 86400**	**1000**

Parameters	Permitted Values	Default
Description: Configures the interval (in seconds) to update time and date from the NTP server. **Example:** local_time.interval = 1000 **Web User Interface:** Settings->Time & Date->Synchronism (15~86400s) **Phone User Interface:** None		
local_time.time_zone	**-11 to +14**	**+8**
Description: Configures the time zone. **Example:** local_time.time_zone = +8 For more available time zones, refer to Appendix B: Time Zones on page 434. **Web User Interface:** Settings->Time & Date->Time Zone **Phone User Interface:** Menu->Basic->Date & Time->General->SNTP Settings->Time Zone		
local_time.time_zone_name	**String within 32 characters**	**China(Beijing)**
Description: Configures the time zone name. The available time zone names depend on the time zone configured by the parameter "local_time.time_zone". For more information on the available time zone names for each time zone, refer to Appendix B: Time Zones on page 434. **Example:** local_time.time_zone_name = China(Beijing) **Note:** It works only if the value of the parameter "local_time.summer_time" is set to 2 (Automatic) and the parameter "local_time.time_zone" should be configured in advance. **Web User Interface:** Settings->Time & Date->Location **Phone User Interface:** Menu->Basic->Date & Time->General->SNTP Settings->Location		

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

1. Click on **Settings**->**Time & Date**.
2. Select the desired value from the pull-down list of **NTP by DHCP Priority**.

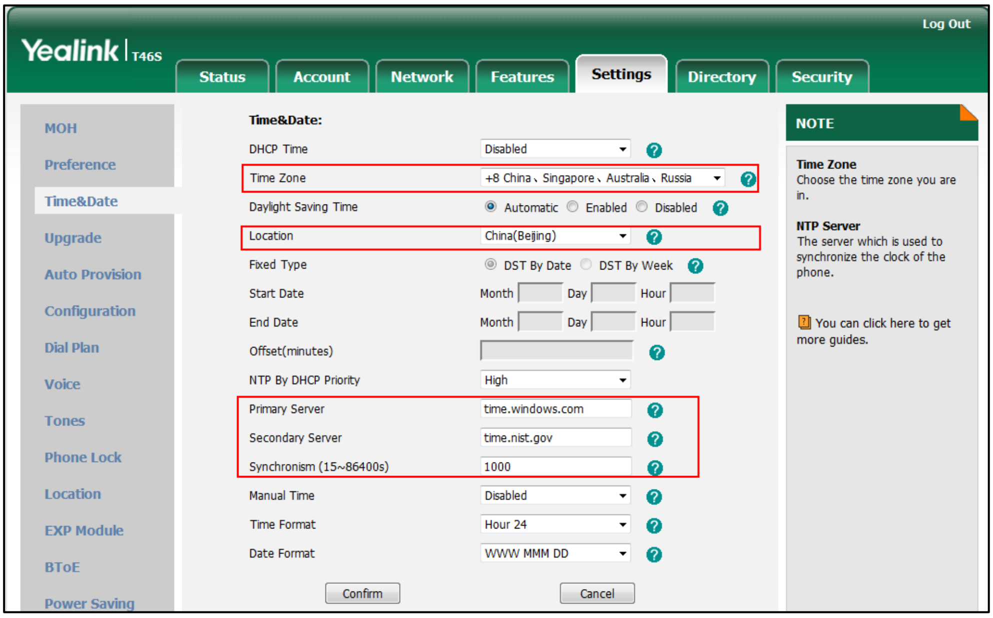


3. Click **Confirm** to accept the change.

To configure the NTP server, time zone via web user interface:

1. Click on **Settings**->**Time & Date**.
2. Select **Disabled** from the pull-down list of **Manual Time**.
3. Select the desired time zone from the pull-down list of **Time Zone**.
4. Select the desired location from the pull-down list of **Location**.
5. Enter the domain name or IP address in the **Primary Server** and **Secondary Server** field respectively.

6. Enter the desired time interval in the **Synchronism (15~86400s)** field.



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

To configure the SNTP settings via phone user interface:

1. Press **Menu**->**Basic**->**Date & Time**->**General**->**SNTP Settings**.
2. Press or , or the **Switch** soft key to select the time zone that applies to your area from the **Time Zone** field.

   The default time zone is "GMT+8".
3. Enter the domain name or IP address of SNTP server in the **NTP Server1** and **NTP Server2** field respectively.
4. Press or , or the **Switch** soft key to select automatic, enabled and disabled from the **Daylight Saving** field.
5. Press or , or the **Switch** soft key to select the desired location from the **Location** field.
6. Press the **Save** soft key to accept the change.

Time and Date Settings

You can set the time and date manually when phones cannot obtain the time and date from the NTP time server. The time and date display can use one of several different formats.

Procedure

Time and date can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the time and date manually.

		Parameter: local_time.manual_time_enable Configure the time and date formats. **Parameters:** local_time.time_format local_time.date_format
Local	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
	Phone User Interface	Configure the time and date manually. Configure the time and date formats.

Details of Configuration Parameters:

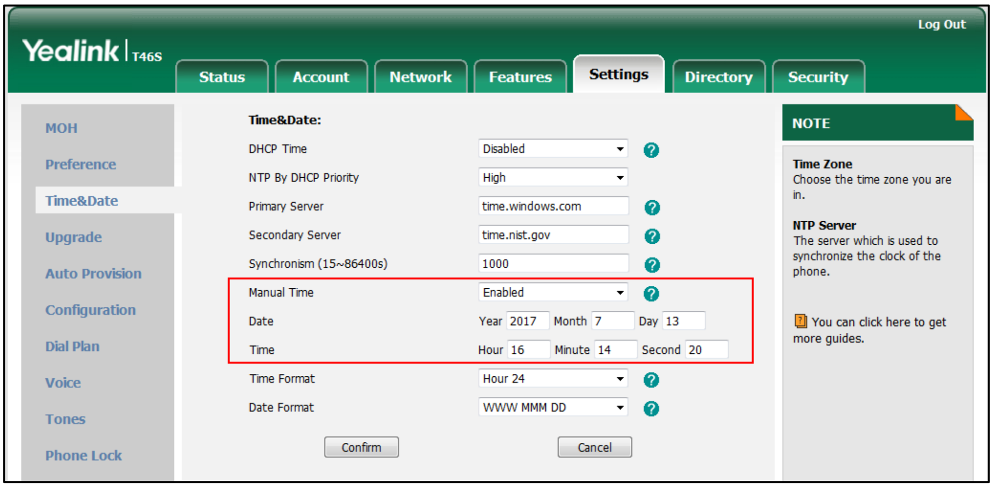
Parameters	Permitted Values	Default
local_time.manual_time_enable	**0 or 1**	**0**
Description: Enables or disables the phone to obtain time and date from manual settings. **0**-Diabled, obtain time and date from NTP server **1**-Enabled, obtain time and date from manual settings **Web User Interface:** Settings->Time & Date->Manual Time **Phone User Interface:** None		
local_time.time_format	**0 or 1**	**1**
Description: Configures the time format. **0**-Hour 12, the time will be displayed in 12-hour format with AM or PM specified. **1**-Hour 24, the time will be displayed in 24-hour format (for example, 2:00 PM displays as		

Parameters	Permitted Values	Default
14:00). **Web User Interface:** Settings->Time & Date->Time Format **Phone User Interface:** Menu->Basic->Date & Time->Time & Date Format->Time Format		
local_time.date_format	**0, 1, 2, 3, 4, 5 or 6**	**0**
Description: Configures the date format. **Valid values are:** **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. **Web User Interface:** Settings->Time & Date->Date Format **Phone User Interface:** Menu->Basic->Date & Time->Time & Date Format->Date Format		

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

1. Click on **Settings**->**Time & Date**.
2. Select **Enabled** from the pull-down list of **Manual Time**.

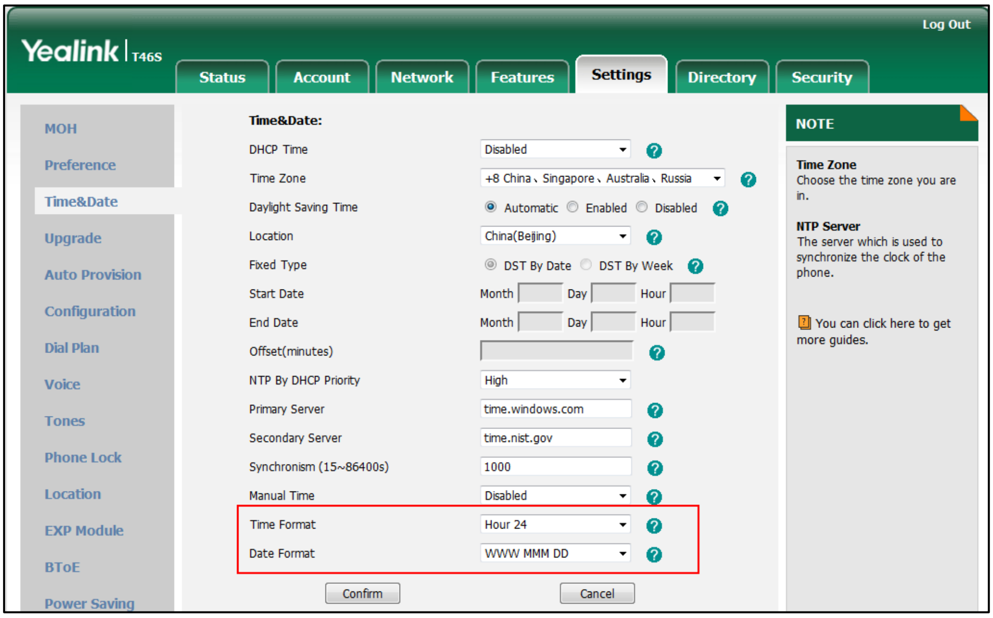
3. Enter the time and date in the corresponding fields.



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

To configure the time and date format via web user interface:

1. Click on **Settings**->**Time & Date**.
2. Select the desired value from the pull-down list of **Time Format**.
3. Select the desired value from the pull-down list of **Date Format**.



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

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

1. Press **Menu**->**Basic**->**Date &Time**->**General**->**Manual Settings**.
2. Enter the specific date and time or press or to edit specific date and time in the corresponding fields.
3. Press **Save** to accept the change.

The time and date displayed on the LCD screen/touch screen will change accordingly.

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

1. Press **Menu** ->**Basic**->**Date &Time** ->**Time & Date Format**.
2. Press or , or the **Switch** soft key to select the desired date format from the **Date Format** field.
3. Press or , or the **Switch** soft key to select the desired time format (**12 Hour** or **24 Hour**) from the **Time Format** field.
4. Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

Daylight Saving Time

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 configuration files or locally.

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
Local	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:		

Parameters	Permitted Values	Default
Configures Daylight Saving Time (DST) feature. **0**-Disabled **1**-Enabled **2**-Automatic **Web User Interface:** Settings->Time & Date->Daylight Saving Time **Phone User Interface:** Menu->Basic->Date & Time->General->SNTP Settings->Daylight Saving		
local_time.dst_time_type	**0 or 1**	**0**
Description: Configures the 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 **Phone User Interface:** None		
local_time.start_time	**Time**	**1/1/0**
Description: Configures the start time of the DST. **Value formats are:** ● Month/Day/Hour (for DST By Date) ● Month/Day of Week Last in 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 If "local_time.dst_time_type" is set to 1 (DST By Week), use the mapping: **Month:** 1=January, 2=February,..., 12=December **Day of Week Last in Month:** 1=the first week in a month,..., 5=the last week in a month **Day of Week:** 1=Monday, 2=Tuesday,..., 7=Sunday		

Parameters	Permitted Values	Default
Hour of Day: 0=0am, 1=1am,..., 23=11pm **Note:** It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings->Time & Date->Start Date **Phone User Interface:** None		
local_time.end_time	**Time**	**12/31/23**
Description: Configures the end time of the DST. **Value formats are:** ● Month/Day/Hour (for DST By Date) ● Month/Day of Week Last in 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 If "local_time.dst_time_type" is set to 1 (DST By Week), use the mapping: **Month:** 1=January, 2=February,..., 12=December **Day of Week Last in 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 **Note:** It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings->Time & Date->End Date **Phone User Interface:** None		
local_time.offset_time	**Integer from -300 to 300**	**Blank**
Description: Configures the offset time (in minutes) of DST. **Note:** It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled).		

Parameters	Permitted Values	Default
Web User Interface: Settings->Time & Date->Offset(minutes) **Phone User Interface:** None		

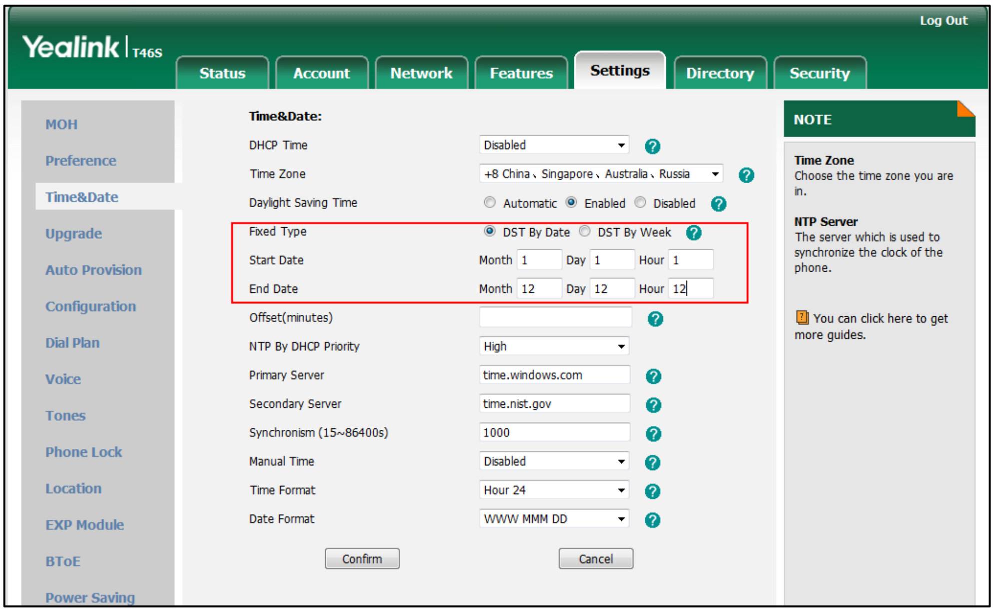
To configure the DST via web user interface:

1. Click on **Settings**->**Time & Date**.
2. Select **Disabled** from the pull-down list of **Manual Time**.
3. Select the desired time zone from the pull-down list of **Time Zone**.
4. Enter the domain name or IP address in the **Primary Server** and **Secondary Server** field respectively.
5. Enter the desired time interval in the **Synchronism (15~86400s)** field.
6. Mark the **Enabled** radio box in the **Daylight Saving Time** field.

   - Mark the **DST by Date** radio box in the **Fixed Type** field.

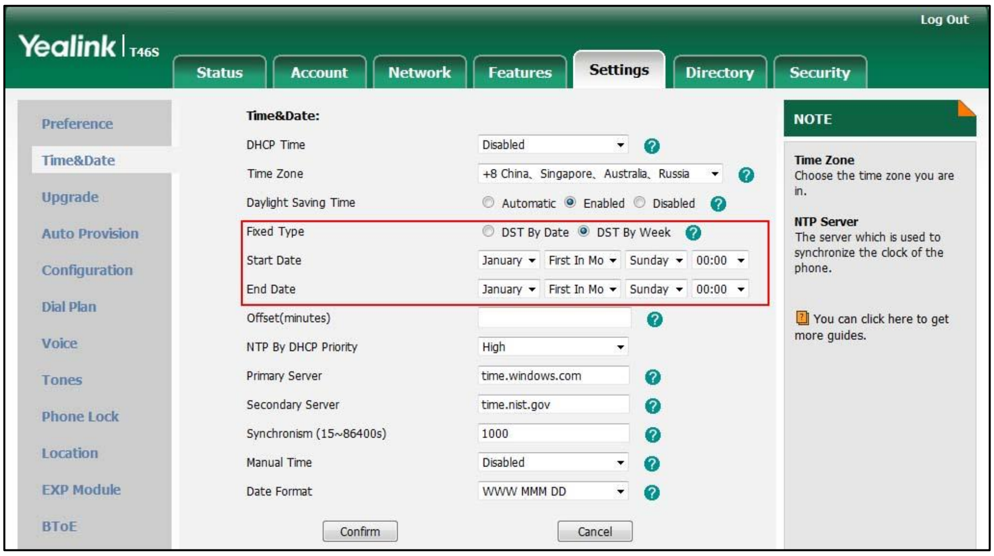
     Enter the start time in the **Start Date** field.

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



   - Mark the **DST by Week** radio box in the **Fixed Type** field.

Select the desired values of DST Start Month, DST Start Week of Month, DST Start Day of Week, Start Hour of Day; DST Stop Month, DST Stop Week of Month, DST Stop Day of Week and End Hour of Day from the pull-down lists.



7. Enter the desired offset time in the **Offset(minutes)** field.
8. Click **Confirm** to accept the change.

Customizing an AutoDST Template File

The time zone and corresponding DST pre-configurations exist in the AutoDST file. If the DST is set to Automatic, the phone obtains the DST configuration from the AutoDST file. You can customize the AutoDST file if required. The AutoDST file allows you to add or modify time zone and DST settings for your area each year.

Before customizing, you need to obtain the AutoDST file. You can ask the distributor or Yealink FAE for DST template. You can also obtain the DST template online: *http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage*. For more information on obtaining the template file, refer to Obtaining Configuration Files/Resource Files on page 92.

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 keep their daylight saving time the same)	Time Zone name

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

When customizing an AutoDST file, learn the following:

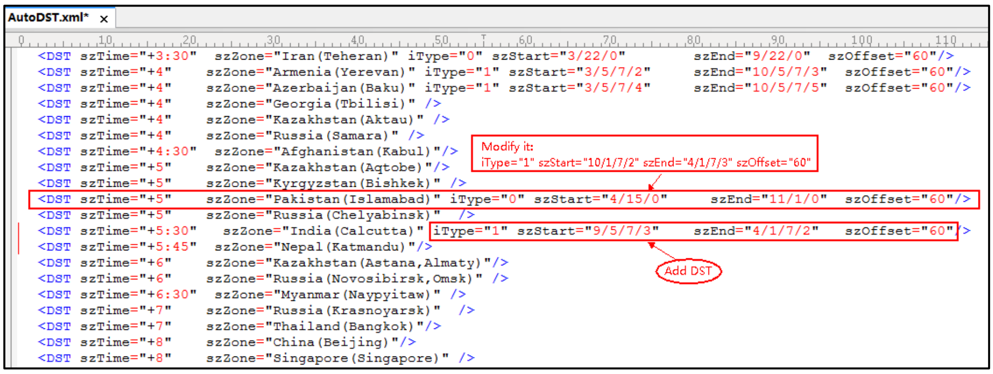
- <DSTData> indicates the start of a template and </DSTData> indicates the end of a template.
- Add or modify time zone and DST settings between <DSTData> and </DSTData>.
- The display order of time zone is corresponding to the szTime order specified in the AutoDST.xml file.
- If the start time of DST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

Customizing an AutoDST file:

1. Open the AutoDST file using an ASCII editor.
2. Add or modify time zone and DST settings as you want in the AutoDST file.

   Example 1:

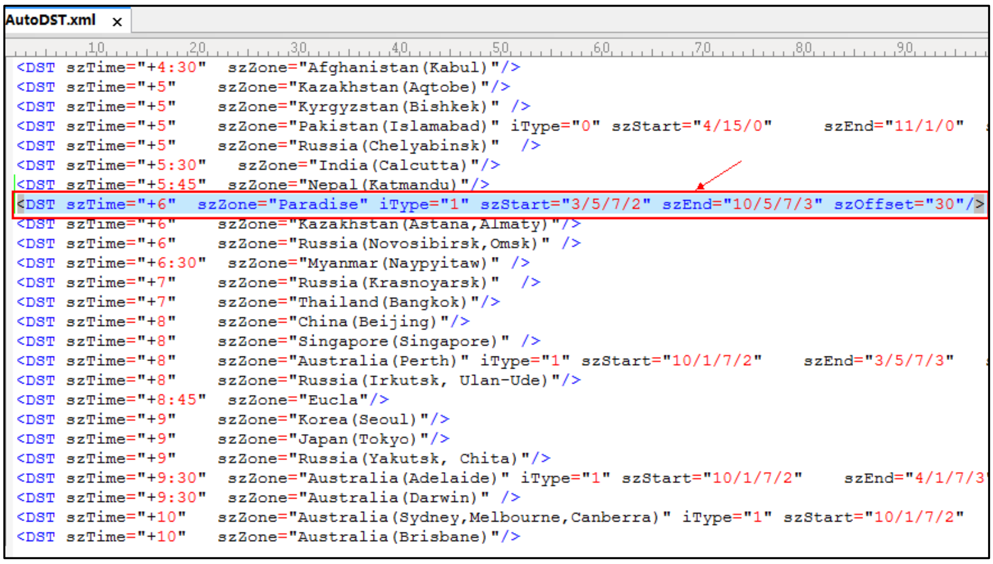
To modify the DST settings for the existing time zone “+5 Pakistan(Islamabad)” and add DST settings for the existing time zone “+5:30 India(Calcutta)”.




```
<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)" />
```

Example 2:

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




```
<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. **Parameters:** auto_dst.url

Details of Configuration Parameters:

Parameters	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 phone connects to the provisioning server "192.168.1.100", and downloads the AutoDST file "AutoDST.xml". After update, you will find a new time zone "Paradise" and updated DST of "Pakistan (Islamabad)" and "India (Calcutta)" via web user interface: **Settings**->**Time & Date**->**Time Zone**. **Note:** It works only if the value of the parameter "local_time.summer_time" is set to 2 (Automatic). **Web User Interface:** None **Phone User Interface:** None		

Language

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

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

Phone/Web User Interface
English
Chinese Simplified
Chinese Traditional
French
German
Italian
Polish
Portuguese
Spanish
Turkish

Phone/Web User Interface
Korean (not applicable to CP960 Skype for Business phones) Russian

Loading Language Packs

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

You can ask the distributor or Yealink FAE for language packs. You can also obtain the language packs online: *http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage*. For more information on obtaining the language packs, refer to Obtaining Configuration Files/Resource Files on page 92.

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 Skype for Business phone. If the characters in the custom language file are not supported by the Skype for Business phone, the phone will display "?" instead.

Customizing a Language for Phone User Interface

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

Available Language	Associated Language Pack
English	000.GUI.English.lang
Chinese Simplified	001.GUI.Chinese_S.lang
Chinese Traditional	002.GUI.Chinese_T.lang
French	003.GUI.French.lang
German	004.GUI.German.lang
Italian	005.GUI.Italian.lang
Polish	006.GUI.Polish.lang
Portuguese	007.GUI.Portuguese.lang
Spanish	008.GUI.Spanish.lang
Turkish	009.GUI.Turkish.lang

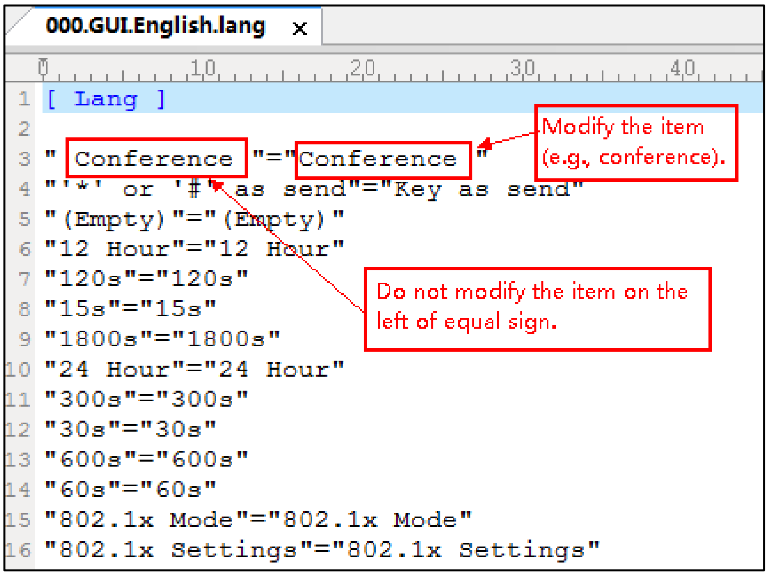
Available Language	Associated Language Pack
Korean	010.GUI.Korean.lang (not applicable to CP960 Skype for Business phones)
Russian	011.GUI.Russian.lang

When adding a new language pack for the phone user interface, the language pack must be formatted as "X.GUI.name.lang" (For T48S/T46S/T42S/T41S Skype for Business phones, X starts from 012, for CP960 Skype for Business phones, X starts from 011), "name" is replaced with the language name). If the language name is the same as the existing one, the existing language pack will be overridden by the new uploaded one. We recommend that the filename of the new language pack should not be the same as the existing one.

To customize a language file:

1. Open the desired language template file (e.g., 000.GUI.English.lang) using an ASCII editor.
2. Modify the characters within the double quotation marks on the right of the equal sign. Don't modify the translation item on the left of the equal sign.

   The following shows a portion of the language pack "000.GUI.English.lang" for the phone user interface (take T46S Skype for Business phones for example):



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

If you want to add a new custom language (e.g., Guilan) to your phone (e.g., T46S), prepare the language file named as "012.GUI.Guilan.lang" for downloading. After update, you will find a new language selection "Guilan" on the phone user interface: **Menu->Basic**->**Language**.

Procedure

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

<table>
<tr><td rowspan="2">Central Provisioning (Configuration File)</td><td rowspan="2"><y0000000000xx>.cfg</td><td>Specify the access URL of the phone user interface language pack.
Parameter:
gui_lang.url</td></tr>
<tr><td>Delete custom LCD language packs of the phone user interface.
Parameter:
gui_lang.delete</td></tr>
</table>

Details of the Configuration Parameter:

<table>
<tr><th>Parameter</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>gui_lang.url</td><td>URL within 511 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the access URL of the custom LCD language pack for the phone user interface.
Example:
gui_lang.url = http://192.168.10.25/000.GUI.English.lang
During the auto provisioning process, the phone connects to the HTTP provisioning server “192.168.10.25”, and downloads the language pack “000.GUI.English.lang”. The English language translation will be changed accordingly if you have modified the language template file.
If you want to download multiple language packs to the phone simultaneously, you can configure as following:
gui_lang.url = http://192.168.10.25/000.GUI.English.lang
gui_lang.url = http://192.168.10.25/001.GUI.Chinese_S.lang
Web User Interface:
None
Phone User Interface:
None</td></tr>
<tr><td>gui_lang.delete</td><td>http://localhost/all or
http://localhost/Y.GUI.name.lang</td><td>Blank</td></tr>
<tr><td colspan="3">Description:</td></tr>
</table>

Parameter	Permitted Values	Default
Deletes the specified or all custom LCD language packs of the phone user interface. **Example:** Delete all custom language packs of the phone user interface: gui_lang.delete = http://localhost/all Delete a custom language pack of the phone user interface (e.g., 001.GUI.Chinese_S.lang): gui_lang.delete = http://localhost/001.GUI.Chinese_S.lang **Web User Interface:** None **Phone User Interface:** None		

Customizing a Language for Web User Interface

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

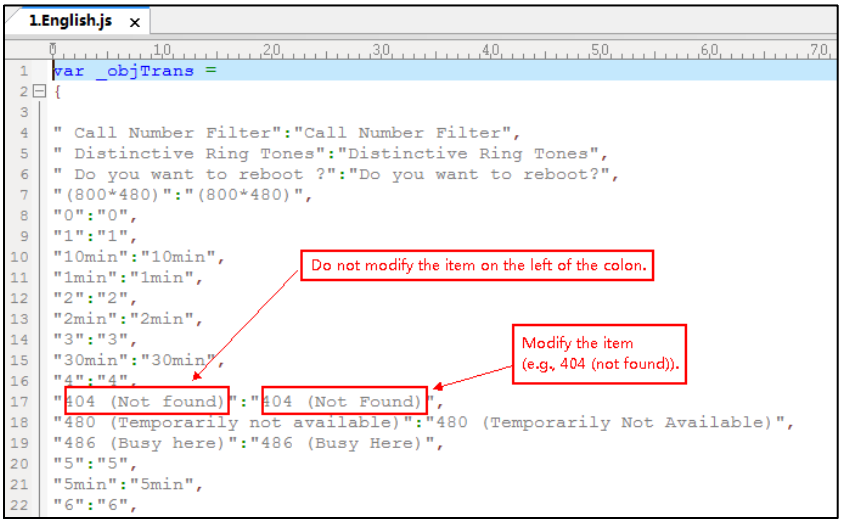
Available Language	Associated Language Pack
English	1.English.js
Chinese Simplified	2.Chinese_S.js
Chinese Traditional	3.Chinese_T.js
French	4.French.js
German	5.German.js
Italian	6.Italian.js
Polish	7.Polish.js
Portuguese	8.Portuguese.js
Spanish	9.Spanish.js
Turkish	10.Turkish.js
Korean	11.Korean.js (not applicable to CP960 Skype for Business phones)
Russian	12.Russian.js

When adding a new language pack for the web user interface, the language pack must be formatted as "Y.name.js" (For T48S/T46S/T42S/T41S Skype for Business phones, Y starts from 13, for CP960 Skype for Business phones, X starts from 12), "name" is replaced with the language name). If the language name is the same as the existing one, the existing language file will be overridden by the new uploaded one. We recommend that the name of the new language file should not be the same as the existing languages.

To customize a language file:

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

   The following shows a portion of the language pack "1.English.js" for the web user interface (take T46S Skype for Business phones for example):



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.

If you want to add a new language (e.g., Wuilan) to phones, prepare the language file named as "13.Wuilan.js" for downloading. After update, you will find a new language selection "Wuilan" on the web user interface: **Settings**->**Preference**->**Language**.

Procedure

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

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

Details of the Configuration Parameter:

Parameter	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 phone connects to the HTTP provisioning server "192.168.10.25", and downloads the language pack "1.English.js". The English language translation will be changed accordingly if you have modified the language template file. If you want to download multiple language packs to the web user interface simultaneously, you can configure as following: wui_lang.url = http://192.168.10.25/1.English.js wui_lang.url = http://192.168.10.25/11.Russian.js **Web User Interface:** None **Phone User Interface:** None		
wui_lang.delete	**http://localhost/all or http://localhost/*Y.name.js***	**Blank**
Description: Delete the specified or all custom web language packs of the web user interface. **Example:** Delete all custom language packs of the web user interface: wui_lang.delete = http://localhost/all Delete a custom language pack of the web user interface (e.g., 11.Russian.js): wui_lang.delete = http://localhost/11.Russian.js **Web User Interface:** None **Phone User Interface:** None		

Specifying the Language to Use

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

Procedure

Specify the language for the phone user interface or the web user interface using the configuration files or locally.

<table>
<tr><td>Central Provisioning (Configuration File)</td><td><y0000000000xx>.cfg</td><td>Specify the languages for the phone user interface and the web user interface.
Parameters:
For T48S/T46S/T42S/T41S Skype for Business phones:
static.lang.gui
static.lang.wui</td></tr>
<tr><td rowspan="2">Local</td><td>Web User Interface</td><td>Specify the language for the web user interface.
Navigate to:
http://<phoneIPAddress>/servlet?p=settings-preference&q=load</td></tr>
<tr><td>Phone User Interface</td><td>Specify the language for the phone user interface.</td></tr>
</table>

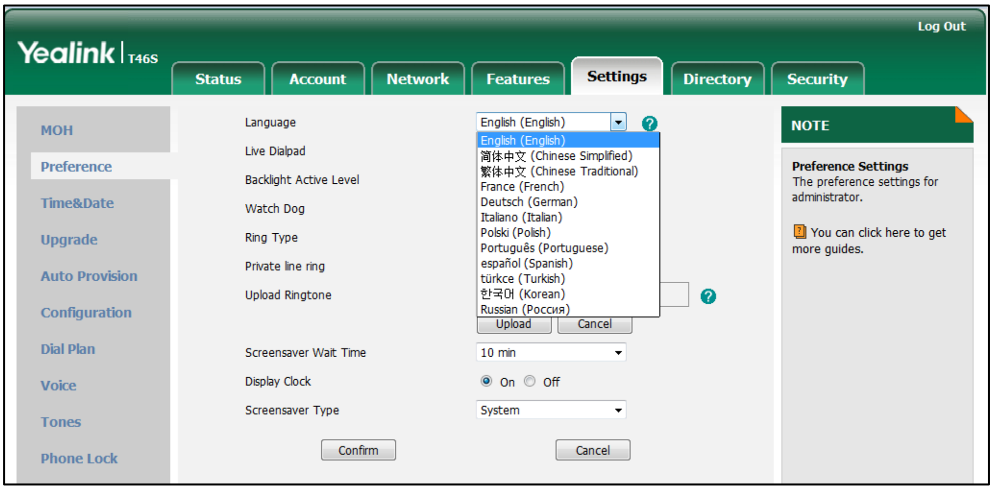
Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>static.lang.gui</td><td>Refer to the following content</td><td>English</td></tr>
<tr><td colspan="3">Description:
Configures the language used on the phone user interface.
Permitted Values:
English, Chinese Simplified, Chinese Traditional, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Korean, Russian or the custom language name.
Example:
static.lang.gui = English
If you want to use the custom language (e.g., Guilan) for the phone, configure the parameter “static.lang.gui = Guilan”.
Web User Interface:
None
Phone User Interface:</td></tr>
</table>

Parameters	Permitted Values	Default
Menu->Basic->Language		
static.lang.wui (lang.wui)	**Refer to the following content**	**English**
Description: Configures the language used on the web user interface. **Permitted Values**: English, Chinese Simplified, Chinese Traditional, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Korean, Russian or the custom language name. **Example:** static.lang.wui = English If the language of your browser is not supported by the phone, the web user interface will use English by default. **Web User Interface:** Settings->Preference->Language **Phone User Interface:** None		

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

1. Click on **Settings**->**Preference**.
2. Select the desired language from the pull-down list of **Language**.



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

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

1. Press **Menu->Basic**->**Language**.
2. Press or to select the desired language.

3. Press the **Save** soft key to accept the change.

Key As Send

Key as send allows assigning the pound key ("#") or asterisk key ("*") as the send key.

Send tone allows the phone to play a key tone when a user presses the send key. Key tone allows the phone to play a key tone when a user presses any key. Send tone works only if key tone is enabled.

Procedure

Key as send can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure a send key. **Parameter:** features.key_as_send
		Configure send pound key. **Parameter:** features.send_pound_key
Local	Web User Interface	Configure a send key. Configure send pound key. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
		Configure a send key. Configure send pound key. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure a send key.

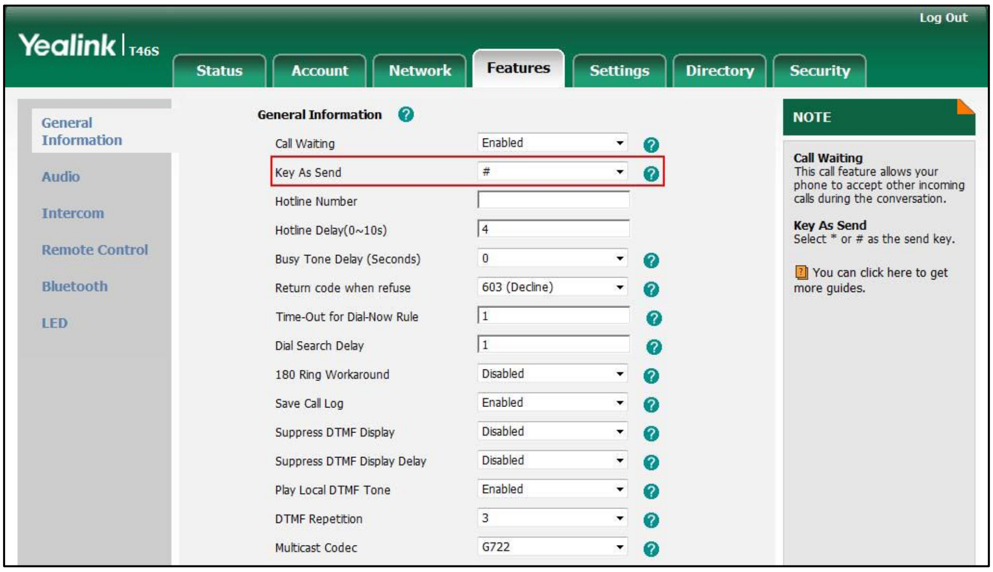
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.key_as_send	**0, 1 or 2**	**1**
Description: Configures the "#" or "*" key as the send key. **0**-Disabled, neither "#" nor "*" can be used as the send key.		

Parameters	Permitted Values	Default
1-# key, the pound key is used as the send key. **2**-* key, the asterisk key is used as the send key. **Web User Interface:** Features->General Information->Key As Send **Phone User Interface:** Menu->Features->Key as send		
features.send_pound_key	**0 or 1**	**0**
Description: Enables or disables the phone not to dial out "##" when the user presses double # key on dialing screen or pre-dialing screen. **0**-Disabled, the phone will dial out "#" when the user presses the # key for the second time. **1**-Enabled, the phone will dial out "##" when the user presses the # key for the third time. **Note**: It works only if the value of the parameter "features.key_as_send" is set to 1 (Enabled). **Web User Interface:** Features->General Information->Send Pound Key **Phone User Interface:** None		

To configure a send key via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Key As Send**.



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

To configure a send key via phone user interface:

1. Press **Menu**->**Features**->**Key as Send**.
2. Press or , or the **Switch** soft key to select **#** or ***** from the **Key as Send** field, or select **Disabled** to disable this feature.
3. Press the **Save** soft key to accept the change.

Send Tone

Send tone allows the phone to play a key tone when a user presses the send key. It works only if key tone is enabled. For more information on key tone, refer to Key Tone on page 185.

Procedure

Send tone can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure a send tone. **Parameter:** features.send_key_tone
Web User Interface		Configure a send tone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-audio&q=load

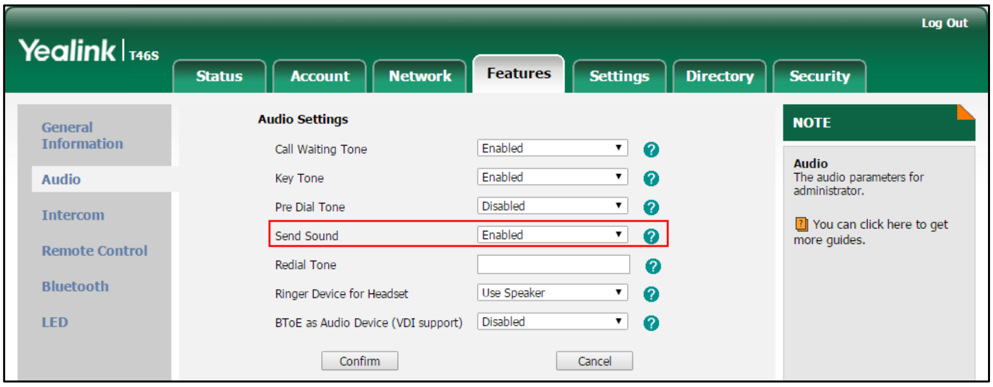
Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.send_key_tone	**0 or 1**	**1**
Description: Enables or disables the phone to play a key tone when a user presses a send key. **0**-Disabled **1**-Enabled **Note**: It works only if the value of the parameter "features.key_tone" is set to 1 (Enabled). **Web User Interface:** Features->Audio->Send Sound **Phone User Interface:** None		

To configure a send sound via web user interface:

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

2. Select the desired value from the pull-down list of **Send Sound**.



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

Key Tone

Key tone allows the phone to play a key tone when a user presses any key on the phone keypad or taps any key on the onscreen dial pad.

Procedure

Key tone can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure a key tone. **Parameter:** features.key_tone
Web User Interface		Configure a key tone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-audio&q=load
Phone User Interface		Configure a key tone.

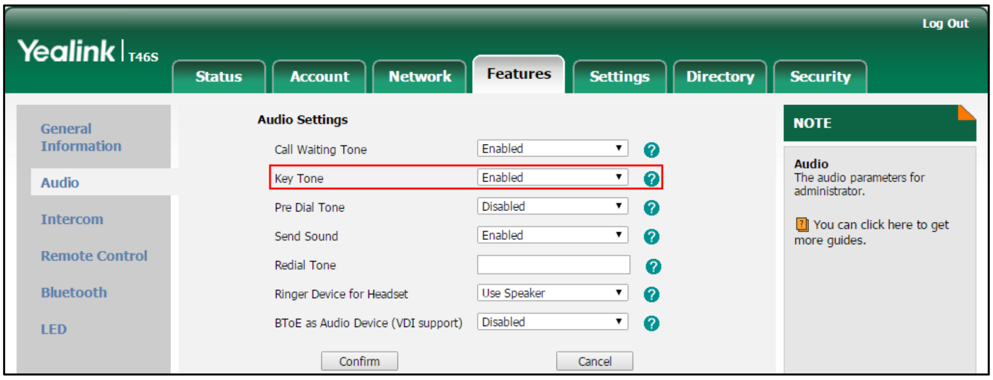
Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.key_tone	**0 or 1**	**1**
Description: Enables or disables the phone to play a key tone when a user presses any key on your phone keypad or taps any key on the onscreen dial pad. **0**-Disabled **1**-Enabled		

Parameter	Permitted Values	Default
If it is set to 1 (Enabled), the Skype for Business phone will play a key tone when a user presses any key on your phone keypad or taps any key on the onscreen dial pad. **Web User Interface:** Features->Audio->Key Tone **Phone User Interface:** Menu->Basic->Sounds->Key Tone		

To configure a key tone via web user interface:

1. Click on **Features**->**Audio**.
2. Select the desired value from the pull-down list of **Key Tone**.



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

To configure a key tone via web user interface:

1. Press **Menu**->**Basic**->**Sound**->**Key Tone**.
2. Press or , or the **Switch** soft key to select the desired value from the **Key Tone** field.
3. Press the **Save** soft key to accept the change.

Dial Plan

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

The dial plan is configured on the Skype for Business server by your system administrator. The phone can use the dial plan received from the Skype for Business server via In-band provisioning method. When user enters digits in the dialing screen, the phone will match the digits to a dial plan.

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 phone will automatically dial out the numbers without pressing the send key. Skype for Business phones support up to 100 dial-now rules, which can be created either one by one or in batch using a dial-now rule template. For more information on how to customize a dial-now template, refer to Customizing Dial-now Template File on page 189.

Time Out for Dial Now Rule

The 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 configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Create the dial-now rule for the phone. **Parameters:** dialplan.dialnow.rule.X
		Configure the delay time for the dial-now rule. **Parameters:** phone_setting.dialnow_delay
Local	Web User Interface	Create the dial-now rule for the 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:

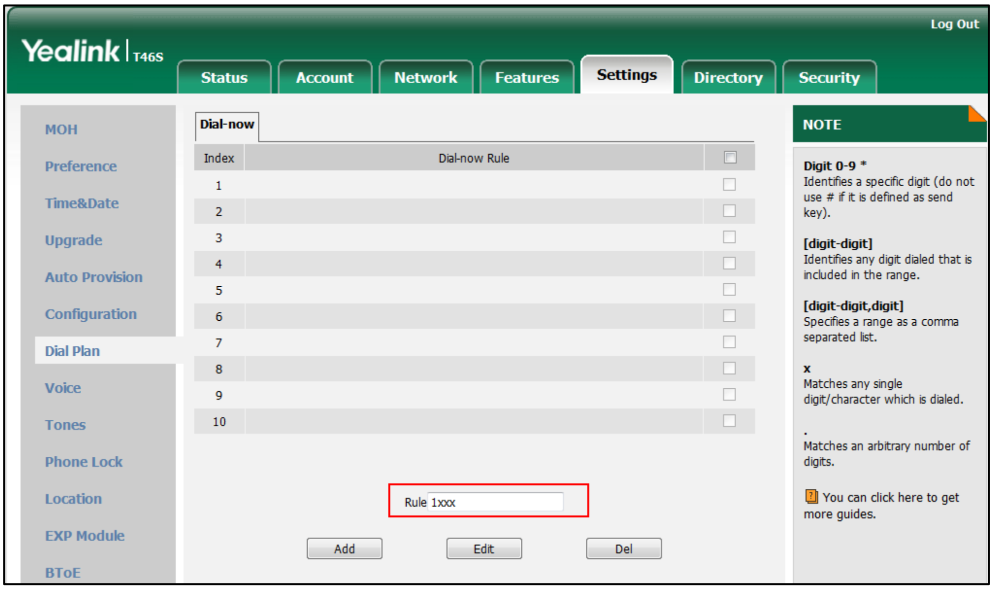
Parameters	Permitted Values	Default
dialplan.dialnow.rule.X (X ranges from 1 to 100)	**String within 511 characters**	**Blank**

Parameters	Permitted Values	Default
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 phone will automatically dial out the numbers without pressing the send key. **Example:** dialplan.dialnow.rule.1 = 123 **Web User Interface:** Settings->Dial Plan->Dial-now->Rule **Phone User Interface:** None		
phone_setting.dialnow_delay	**Integer from 0 to 14**	**1**
Description: Configures the delay time (in seconds) for the dial-now rule. When entered numbers match the predefined dial-now rule, the phone will automatically dial out the entered number after the designated delay time. **Web User Interface:** Features->General Information->Time-Out for Dial-Now Rule **Phone User Interface:** None		

To create a dial-now rule via web user interface:

1. Click on **Settings**->**Dial Plan**->**Dial-now**.

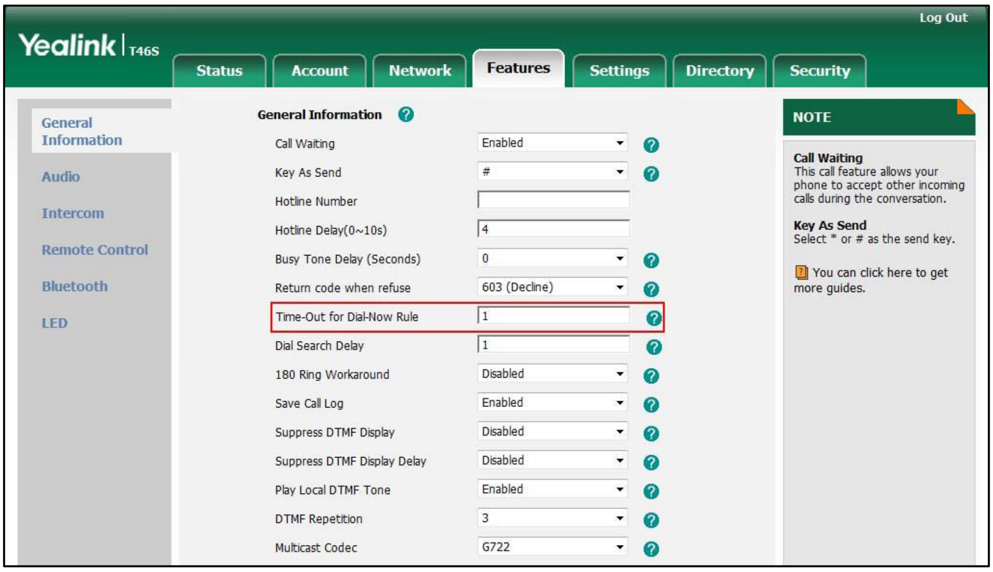
2. Enter the desired value in the **Rule** field.



3. Click **Add** to add the dial-now rule.

To configure the delay time for the dial-now rule via web user interface:

1. Click on **Features**->**General Information**.
2. Enter the desired time within 0-14 (in seconds) in the **Time-Out for Dial-Now Rule** field.



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

Customizing Dial-now Template File

The dial-now template helps with the creation of multiple dial-now rules. After setup, place the dial-now template to the provisioning server and specify the access URL in the configuration files.

You can ask the distributor or Yealink FAE for dial-now template. You can also obtain the dial-now template online:

http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the dial-now template, refer to Obtaining Configuration Files/Resource Files on page 92.

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 line for the dial-now rule, the valid value is 0 or 1. No matter you leave it blank or set it to 0 or 1, the dial-now rule will all be applied to account 1.
- At most 100 rules can be added to the 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="99" LineID="1" />

   Where:

   DialNowRule="" specifies the dial-now rule.

   LineID="" specifies the desired line for this rule. When you leave it blank or enter 0 or enter 1, this dial-now rule will all apply to account 1.

```
<?xml version="1.0" encoding="UTF-8"?>
<DialNow>
  <data DialNowRule="11" LineID="1" />
  <Data DialNowRule="22" LineID="" />
<data DialNowRule="*xx" LineID="1" />
<data DialNowRule="#xx" LineID="1" />
<data DialNowRule="000" LineID="1" />
<data DialNowRule="106" LineID="1" />
<data DialNowRule="101" LineID="1" />
<data DialNowRule="11xx" LineID="1" />
<data DialNowRule="12[23]x" LineID="1" />
<data DialNowRule="124xx" LineID="1" />
<data DialNowRule="1251xx" LineID="1" />
<data DialNowRule="1[38]xxxxxxxx" LineID="1" />
<data DialNowRule="13[1-9]xxx" LineID="1" />
<data DialNowRule="1345xxxx" LineID="1" />
<data DialNowRule="0[2-9]xxxxxxxx" LineID="1" />
<data DialNowRule="2xxx" LineID="1" />
<data DialNowRule="[3-9]xxxxxxx" LineID="1" />
<data DialNowRule="99" LineID="1" />
</DialNow>
```

Add a new dial-now rule

   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 configuration files.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the access URL of the dial-now template. **Parameter:** dialplan_dialnow.url

Details of Configuration Parameters:

Parameters	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 phone connects to the provisioning server "192.168.10.25", and downloads the dial-now rule file "dialnow.xml". **Web User Interface:** None **Phone User Interface:** None		

Hotline

Hotline, sometimes referred to as hot dialing, is a point-to-point communication link in which a call is automatically directed to the preset hotline number. The phone automatically dials out the hotline number after a specified time interval when you lift the handset, press the Speakerphone key, the line key or tap **New Call**. Skype for Business phones only support one hotline number.

Procedure

Hotline can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the hotline number. **Parameter:** features.hotline_number

		Specify the time (in seconds) the phone waits before automatically dialing out the hotline number. **Parameter:** features.hotline_delay
Local	Web User Interface	Configure the hotline number. Specify the time (in seconds) the phone waits before automatically dial out the hotline number. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure the hotline number. Specify the time (in seconds) the phone waits before automatically dialing out the hotline number.

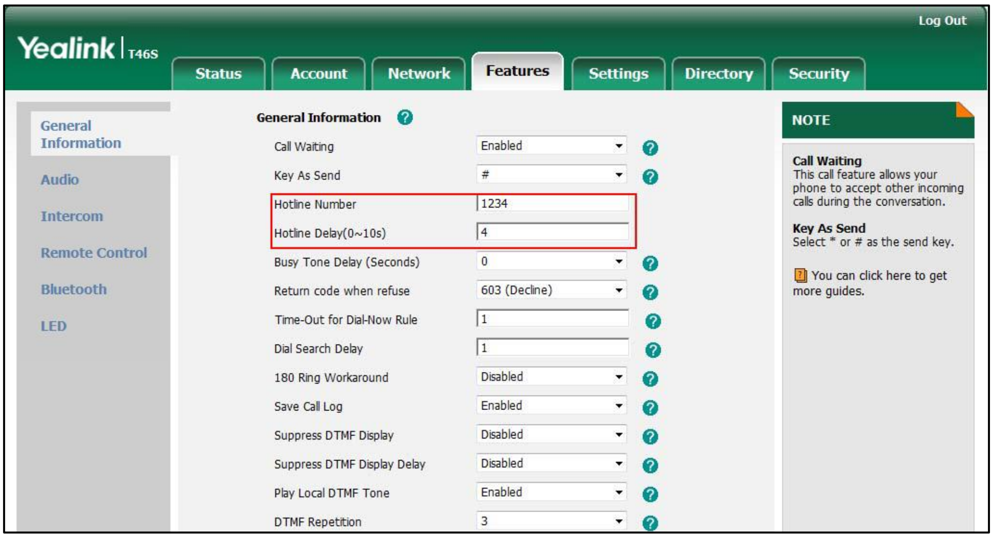
Details of Configuration Parameters:

Parameter	Permitted Values	Default
features.hotline_number	**String within 32 characters**	**Blank**
Description: Configures the hotline number that the phone automatically dials out when in the dialing screen. Leaving it blank disables hotline feature. **Example:** features.hotline_number = 1234 **Web User Interface:** Features->General Information->Hotline Number **Phone User Interface:** Menu->Features->Hotline->Hot Number		
features.hotline_delay	**Integer from 0 to 10**	**4**
Description: Configures the waiting time (in seconds) for the phone to automatically dial out the hotline number.		

Parameter	Permitted Values	Default
If it is set to 0 (0s), the phone will immediately dial out the preconfigured hotline number when in the dialing screen. If it is set to a value greater than 0, the phone will wait the designated seconds before dialing out the predefined hotline number when in the dialing screen. **Web User Interface:** Features->General Information->Hotline Delay(0~10s) **Phone User Interface:** Menu->Features->Hotline->HotLine Delay		

To configure hotline via web user interface:

1. Click on **Features**->**General Information**.
2. Enter the hotline number in the **Hotline Number** field.
3. Enter the delay time in the **Hotline Delay(0~10s)** field.



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

To configure hotline via phone user interface:

1. Press **Menu**->**Features**->**Hot Line**.
2. Enter the hotline number in the **Hot Number** field.
3. Enter the waiting time (in seconds) in the **Hotline Delay** field.
4. Press the **Save** soft key to accept the change.

Contact Management

Your phone can display local contacts, Skype for Business contacts and Outlook contacts.

Skype for Business Directory

The Skype for Business directory on your phone displays all Skype for Business contacts. You can store up to 1000 Skype for Business contacts in your phone's Skype for Business directory. For T41S/T42S/T46S/T48S, you can search, add, view or delete Skype for Business contacts using your phone or Skype for Business client.

Monitoring Status Changes using Line Key LED Indicator

The line key LEDs on your phone can monitor Skype for Business favorites for status changes on the phone. For example, you can view the line key LED on the phone to monitor the status of a friend's line (busy or idle). The line key LED illuminates solid red when the friend's line is busy.

It is not applicable to T48S/CP960 Skype for Business phones.

Procedure

Line key LED indicator can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the line key LED indicator. **Parameter:** phone_setting.line_key_led.enable
Local	Web User Interface	Configure the line key LED indicator. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-powerled&q=load

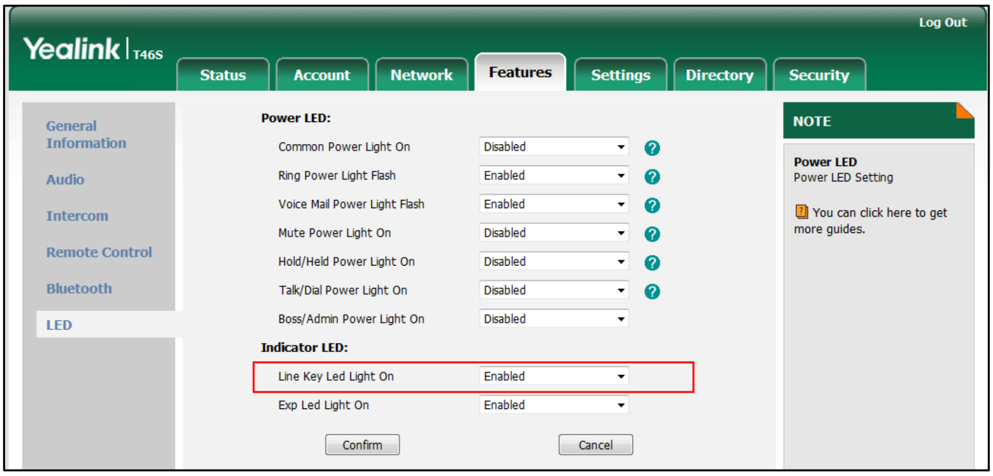
Details of Configuration Parameters:

Parameter	Permitted Values	Default
phone_setting.line_key_led.enable	**0 or 1**	**0**
Description: Enables or disables the line key LED indicators on the phone to monitor the status of the Skype for Business favorites. **0**-Disabled, the line key LED indicators corresponding to your Skype for Business favorites are off. **1**-Enabled, the line key LED indicators vary depending on the status of your Skype for Business favorites. **Note:** It is only applicable to T46S/T42S/T41S Skype for Business phones. **Web User Interface:**		

Parameter	Permitted Values	Default
Features->LED-> Line Key Led Light On **Phone User Interface:** None		

To configure the line key LED indicator via web user interface:

1. Click on **Features**->**LED**.
2. Select the desired value from the pull-down list of **Line Key Led Light On**.



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

Line key LED indicator on your phone (when configured as Skype for Business favorites)

LED Status	Description
Solid green	The Skype for Business favorite is available.
Solid red	The Skype for Business favorite is busy. The Skype for Business favorite is Do Not Disturb. The call of your Skype for Business favorite is parked. The call of your Skype for Business favorite is placed on hold. The held call of your Skype for Business favorite is resumed. The Skype for Business favorite is in a conference.
Solid yellow	The Skype for Business favorite is right back. The Skype for Business favorite is off work. The Skype for Business favorite is away.
Off	The Skype for Business favorite is unknown. The Skype for Business favorite is offline. Your phone is locked.

Local Directory

Yealink Skype for Business phones also maintain a local directory. The Skype for Business phones can store up to 1000 local contacts. When adding a contact to the local directory, in addition to name and phone numbers, you can also specify the ring tone and group for the local contact. Contacts can be added either one by one or in batch using a local contact file. Yealink Skype for Business phones support both *.xml and *.csv format contact files.

Hiding the Local Directory

If you do not want to display the local directory, you can hide the local directory. It is only applicable to CP960 Skype for Business phones.

Procedure

Local directory can be configured using the configuration files only.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configures the phone to display a directory called Local Directory. **Parameter:** features.local_directory.enable

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.local_directory.enable	**0 or 1**	**1**
Description: It enables or disables the phone to display a directory called Local Directory. **0**-Disabled **1**-Enabled **Note:** It is only applicable to CP960 Skype for Business phones. **Web User Interface:** None **Phone User Interface:** None		

Customizing a Local Contact File

You can add contacts one by one on the phone directly. You can also add multiple contacts at a time and/or share contacts between phones using the local contact template file. After setup, place the template file to the provisioning server and specify the access URL of the template file in the configuration files. The existing local contacts on the phones will be overridden by the downloaded local contacts.

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

For more information on obtaining the local contact file, refer to refer to Obtaining Configuration Files/Resource Files on page 92.

The following table lists meaning of each variable in the local contact template file:

Element	Values	Description
root_group	no	Group list's root element.
group	no	Group's root element.
display_name	All Contacts Favoritelist	An element of group. Group name.
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.
address	String	Contact's address.
line	Valid Value: -1 or 0 - -1 stands for Auto (the first registered line) - 0 stands for line1	Since the Skype for Business phones only support 1 account, so no matter -1 or 0 is selected, the contact will all be added to account 1.
ring	Format of the value: System ring tone: - **Auto** - **Resource:Silent.wav** - **Resource:Splash.wav** - **Resource:RingN.wav** (integer N ranges from 1 to 8) Custom ring tone: **Custom:Name.wav**	An element of contact. Contact ring tone.
email	String	Contact's email address.
title	String	Contact's title.
priority	**For T48S/CP960 Skype for**	It is only applicable to local

Element	Values	Description
	Business phones: 0~32. **For T46S Skype for Business phones**: 0~27. **For T42S/T41S Skype for Business phones:** 0~15.	favorites. Favorites display consecutively, according to their priority. The favorite with the lowest number displays first.
group_id_name	Valid Value: All Contacts, Favoritelist	Group name of a contact.

The following shows the procedure of customizing a local contact file for Skype for Business phones:

To customize a local contact file:

1. Open the template file using an ASCII editor.
2. For each contact that you want to add, add the following string to the file. Each starts on a separate line:

   <contact display_name="" office_number=" mobile_number="" other_number="" address=" " line="" ring="" email="" title="" priority="" group_id_name="" />
3. Specify the values within double quotes.

   For example:

   <contact display_name="Yealink" office_number="123" mobile_number="234" other_number="345" address="china" line="-1" ring="Auto" email="456@yealink.com" title="manager" priority="0" group_id_name="All Contacts" />

```
<root_group>
  <group display_name="All Contacts" />
  <group display_name="Favoritelist" />
  <group />
</root_group>
<root_contact>
  <contact display_name="Yealink" office_number="123" mobile_number="234" other_number="345" address="china"
   line="-1" ring="Auto" email="456@yealink.com" title="manager" priority="0" group_id_name="All Contacts" />
</root_contact>
```

4. Save the change and place this file to the provisioning server.
5. Specify the access URL of the custom local contact template in the configuration files.

   For example:

   local_contact.data.url = tftp://192.168.10.25/contact.xml

   During the auto provisioning process, the phone connects to the provisioning server “192.168.10.25”, and downloads the contact file “contact.xml”.

Procedure

Local directory can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the access URL of the local contact file (*.xml). **Parameter:** local_contact.data.url
Local	Web User Interface	Add a new contact to the local directory. To import or export the local contact file. **Navigate to**: http://<phoneIPAddress>/servlet?p=contactsbasic&q=load&num=1&group=
	Phone User Interface	Add a new contact to the local directory.

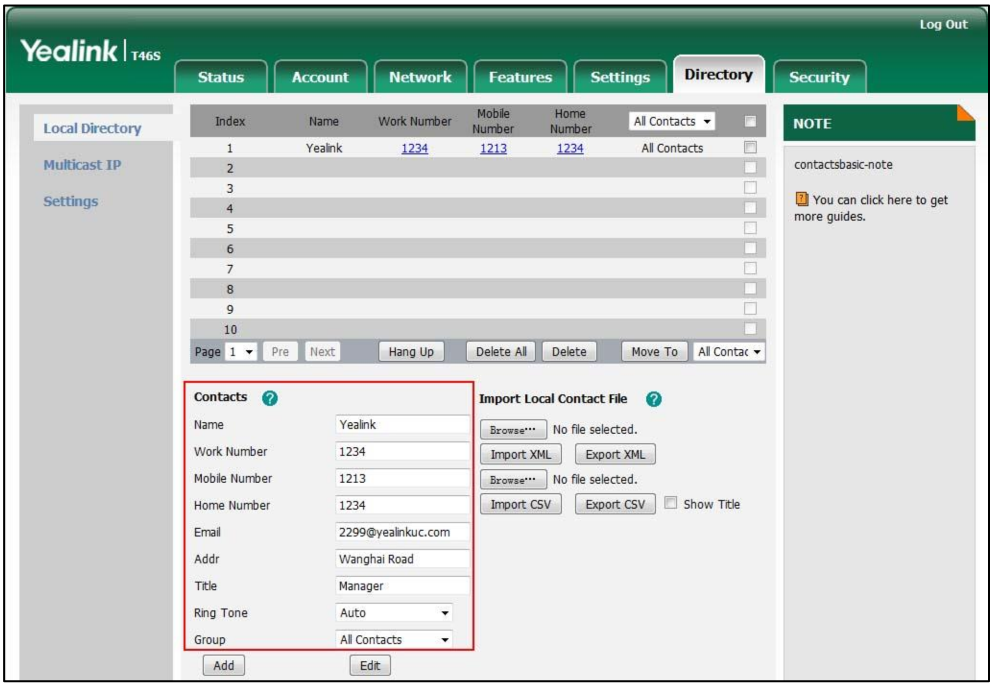
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
local_contact.data.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the local contact file (*.xml). **Example:** local_contact.data.url = http://192.168.10.25/contact.xml **Web User Interface:** Directory->Local Directory->Import Local Contact File **Phone User Interface:** None		

To add a contact to the local directory via web user interface:

1. Click on **Directory**->**Local Directory**.
2. In the **Contacts** block, enter name, work number, mobile number, home numbers, email, address and title in the corresponding fields.
3. Select the desired ring tone from the pull-down list of **Ring Tone**.

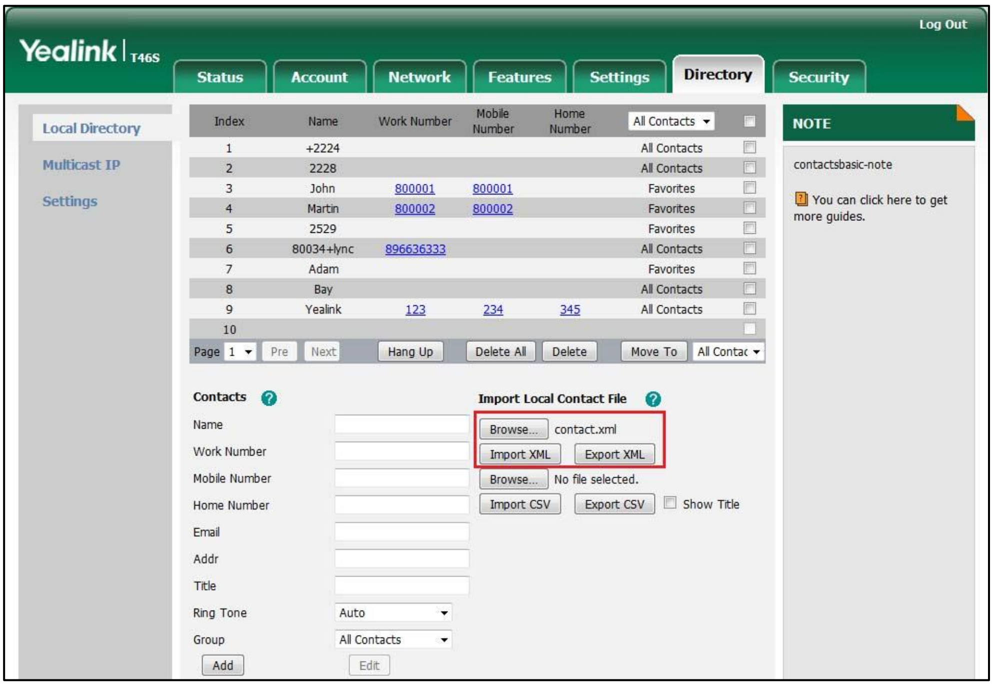
4. Select **All Contacts** from the pull-down list of **Ring Tone**.



5. Click **Add** to add the contact.

To import an XML contact list file via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Click **Browse** to locate a contact list file (the file format must be *.xml) from your local system.



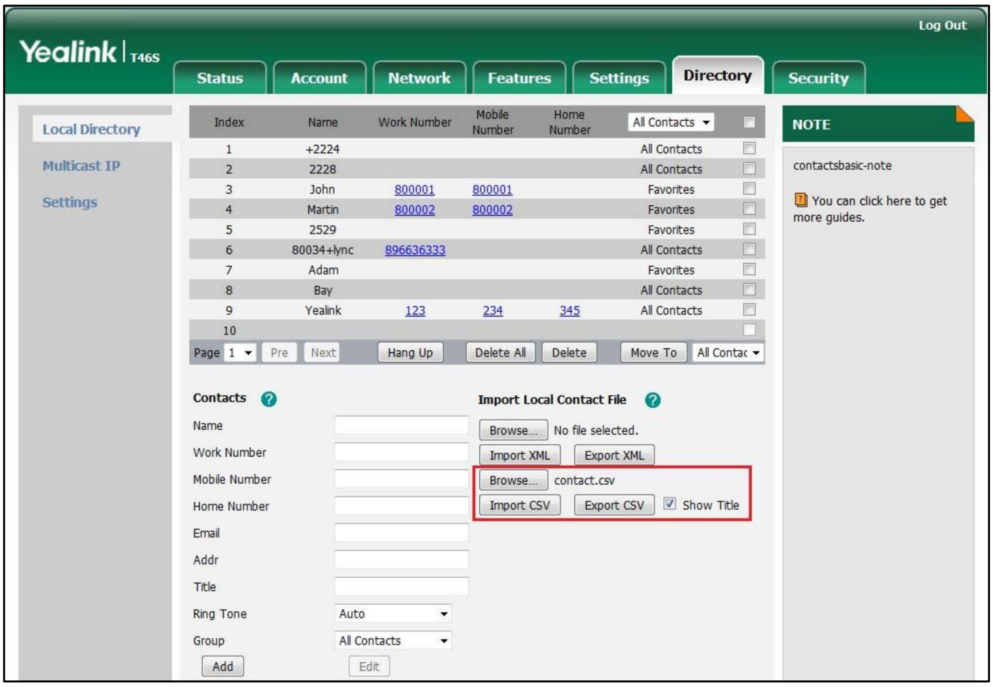
3. Click **Import XML** to import the contact list.

The web user interface prompts "The original contact will be covered, Continue?".

4. Click **OK** to complete importing the contact list.

To import a CSV contact list file via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Click **Browse** to locate a contact list file (the file format must be *.csv) from your local system.



3. (Optional.) Check the **Show Title** checkbox.

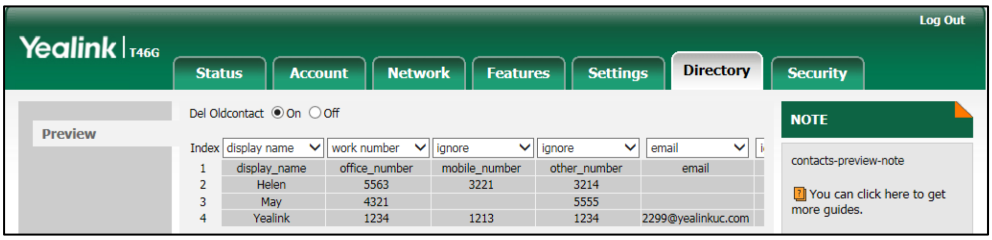
   It will prevent importing the title of the contact information which is located in the first line of the CSV file.

4. Click **Import CSV** 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.



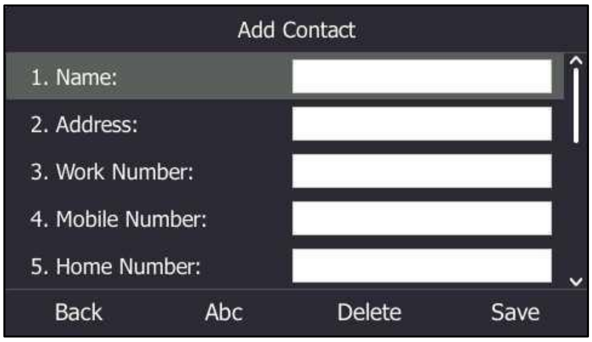
7. Click **Import** to complete importing the contact list.

To export a contact list via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Click **Export XML** (or **Export CSV**).
3. Click **Save** to save the contact list to your local system.

To add a contact to the local directory via phone user interface:

1. Press **Directory**->**Local Directory**->**All Contacts**.
2. Press the **Add** soft key.
3. Enter name, address, work number, mobile number, home number, title and email in the corresponding fields.



4. Press or , or the **Switch** soft key to select the desired ring tone from the **Ring** field.
5. Press the **Save** soft key to accept the change.

Note

If the contact name already exists in the directory, the LCD screen will prompt "Contact name existed!".

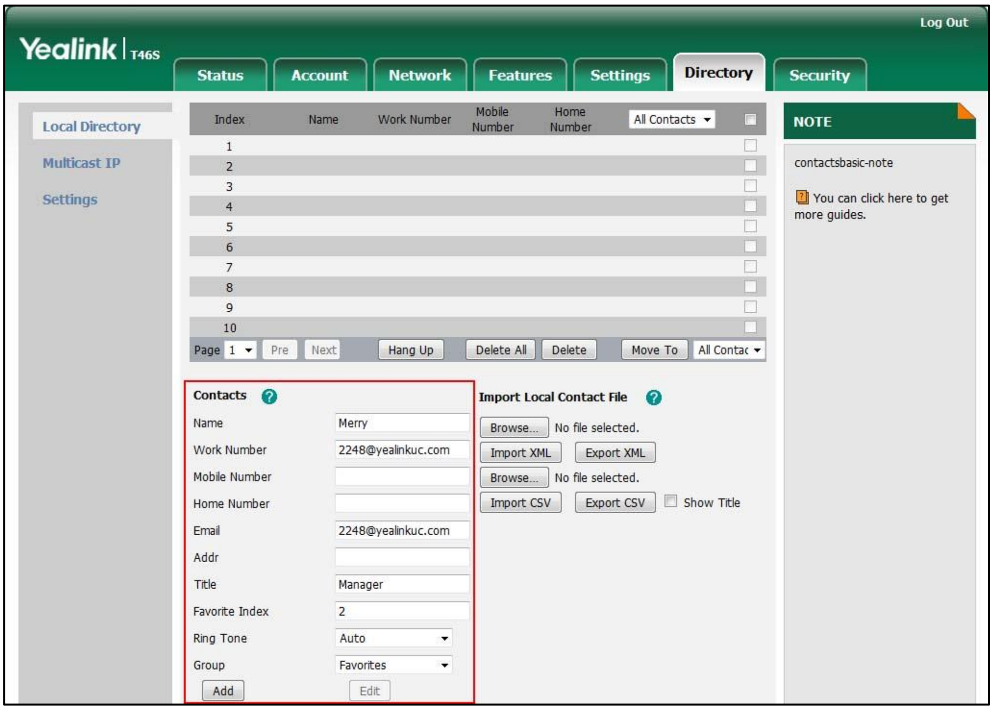
Local Favorites

You can add local contacts as favorites on the phone. You can also reorder your favorites by assigning the contact a different index number.

To add a local favorite via web user interface:

1. Click on **Directory**->**Local Directory**.
2. In the **Contacts** block, enter the contact name, office, mobile, other numbers, Email, address and title in the corresponding fields.
3. Select the desired ring tone from the pull-down list of **Ring Tone**.
4. Select the **Favorites** group from the pull-down list of **Group**.
5. Enter the index number in the **Favorite Index** fields.

Favorites display consecutively, according to their index numbers. The contact with the lowest number displays first.



6. Click **Add** to add the contact.

To add a local favorite via phone user interface:

1. Press **Directory**->**Local Directory**->**Favorites**.
2. Press **Add** soft key.
3. Enter the contact name, address, work number, mobile number, home number, title and email in the corresponding fields.
4. Press or , or the **Switch** soft key to select the desired ring tone from the **Ring** field.
5. Press or , or the **Switch** soft key to select the index number from the **Index** field.

   The contact with the lowest priority number displays first. For more information on the number of priority, refer to priority on page197.
6. Press the **Save** soft key to accept the change.

Managing Local Favorites

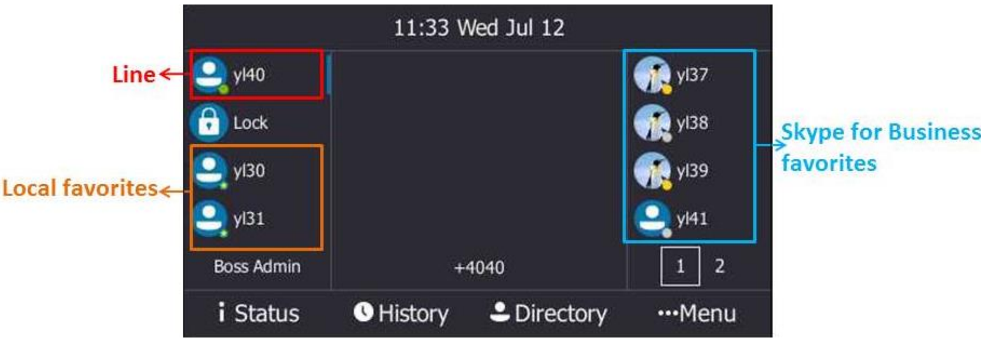
Local favorites and Skype for Business favorites are displayed on the idle screen/favorites screen. By default, local favorites are displayed before the Skype for Business favorites.

Local favorite is indicated by an icon (T48S/T46S/CP960) or an icon (T42S/T41S). Skype for Business favorite is indicated by the presence status icon. The following figures show sample Favorites lists.

For T48S:

You can tap or to turn pages to view more favorites.

For T46S:

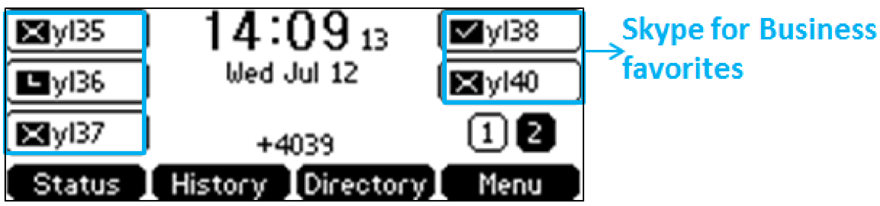


The line key located in the bottom right corner of the screen is used to turn pages. Press it to view more favorites.

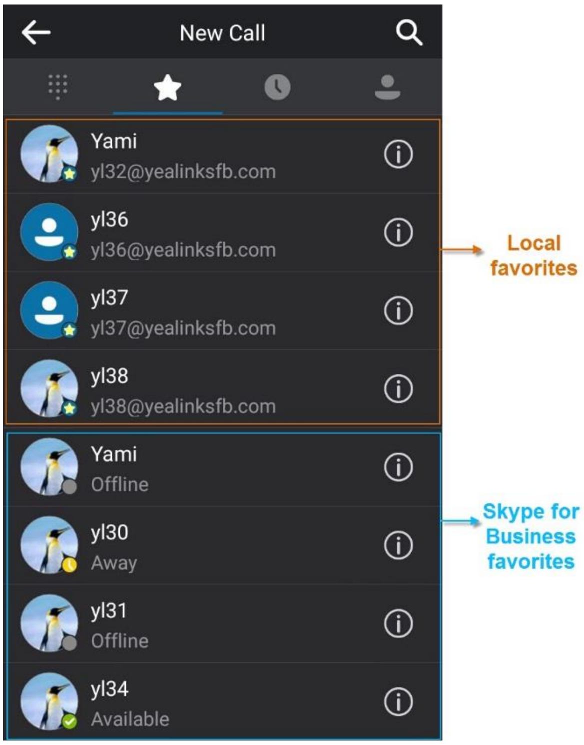
For T42S/T41S:

The following figure shows a sample Favorites list.

Press the key located in the bottom right corner of the screen to turn page.



For CP960:



Slide up and down to view more favorites.

Note Only Skype for Business favorites have presence status.

You can configure whether to display local favorites on the idle screen/favorites screen and configure the display order of the local favorites.

Procedure

Local favorites can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure whether to display local favorites on the idle screen/favorites screen. **Parameter:** sfb.local_favorite.enable Configure the display order of the local favorites on the idle screen/favorites screen. **Parameter:** sfb.local_favorite.sort
Local	Web User Interface	Configure whether to display local favorites on the idle

		screen/favorites screen. Configure the display order of the local favorites on the idle screen/favorites screen. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-settings&q=load

Details of the Configuration Parameter:

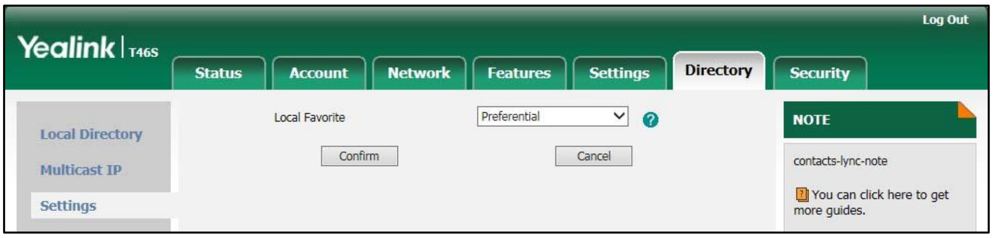
Parameter	Permitted Values	Default
sfb.local_favorite.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display local favorites on the idle screen/favorites screen. **0**-Disabled, local favorites are not displayed on the idle screen/favorites screen, only Skype for Business favorites are displayed on the idle screen/favorites screen. **1**-Enabled, local favorites and Skype for Business favorites are displayed on the idle screen/favorites screen. **Web User Interface:** Directory->Settings->Local Favorite **Phone User Interface:** None		
Parameter	**Permitted Values**	**Default**
sfb.local_favorite.sort	**1 or 2**	**1**
Description: Configures the order of the local favorites on the idle screen/favorites screen. **1**-Preferential, the local favorites will be displayed before the Skype for Business favorites on the idle screen/favorites screen. **2**-General, the local favorites will be displayed after the Skype for Business favorites on the idle screen/favorites screen. **Note:** It works only if the value of the parameter "sfb.local_favorite.enable" is set to 1 (Enabled). **Web User Interface:** Directory->Settings->Local Favorite **Phone User Interface:**		

Parameter	Permitted Values	Default
None		

To configure the display order of local favorites via web user interface:

1. Click on **Directory**>**Settings**.
2. Select the desired value from the pull-down list of **Local Favorite**.
3. Depending on your selection:

   - If **Disabled** is selected, only Skype for Business favorites are displayed on the idle screen/favorites screen.
   - If **Preferential** is selected, local favorites will be displayed before the Skype for Business favorites on the idle screen/favorites screen.
   - If **General** is selected, the local favorites will be displayed after the Skype for Business favorites on the idle screen/favorites screen.



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

Outlook Contacts

Skype for Business Server and Exchange Server are integrated. You can add Outlook contacts on the Microsoft Outlook software only. You can view and search Outlook contacts on your phones.

Procedure

Outlook contacts can be configured using the configuration files only.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configures the phone to display a directory called Outlook Contacts. **Parameter:** exchange.outlook_contact.enable
		Configures the number of Outlook contacts that can be displayed when you perform a search.

		Parameter: phone_setting.search_outlook_contacts.return_number
		Configures the phone to synchronize outlook contacts from the Microsoft Exchange Server. **Parameter:** exchange.outlook_contact_sync.enable
		Configures the interval (in minutes) for the phone to automatically check if any outlook contacts update available on Microsoft Exchange Server. **Parameter:** phone_setting.outlook_contacts.update_time
		Configure the maximum outlook contacts that can be downloaded from the Microsoft Exchange Server. **Parameter:** exchange.outlook_contact.request_number

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
exchange.outlook_contact.enable	**0 or 1**	**0**
Description: It enables or disables the phone to display a directory called Outlook Contacts. This directory will include your Outlook contacts. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		
phone_setting.search_outlook_contacts.return_number	**20**	**Refer to the following content**
Description:		

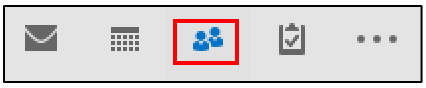
Parameter	Permitted Values	Default
It configures the number of results searched from the Outlook Directory when you perform a search. **Web User Interface:** None **Phone User Interface:** None		
exchange.outlook_contact_sync.enable	**0 or 1**	**1**
Description: It enables or disables the phone to synchronize outlook contacts from the Exchange Server. **0-**Disabled **1-**Enabled **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		
phone_setting.outlook_contacts.update_time	**Integer from 0 to 100**	**10**
Description: It configures the interval (in minutes) for the phone to automatically check if any outlook contacts update available on Microsoft Exchange Server. If it is set to 10 (in minutes), the phone will check if any outlook contact update available on the Microsoft Exchange Server every 10 minutes. If an update is available, the phone will download the outlook contacts. **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		
exchange.outlook_contact.request_number	**Integer from 1 to 5000**	**100**
Description:		

Parameter	Permitted Values	Default
Configures the maximum outlook contacts that can be downloaded from the Exchange Server. **For T48S/T46S**: The maximum value is 500. **For T42S/T41S**: The maximum value is 300. **For CP960**: The maximum value is 300. **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		

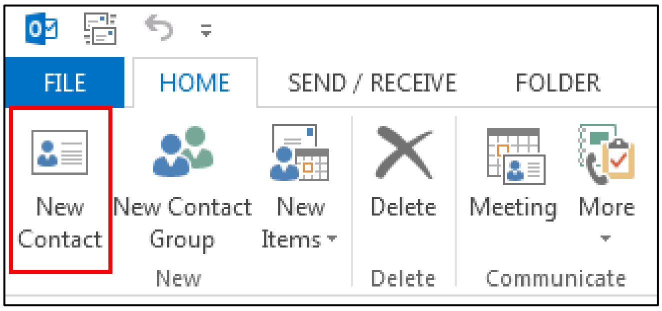
Adding Outlook Contacts

To add an Outlook contact via Microsoft Outlook software:

1. Click **People** at the bottom of the screen.



2. Click **HOME**->**New Contacts**.



3. Enter a name and any other information that you want to include for the contact.
4. If you want to immediately create another contact, click **Save & New** (this way, you don't have to start over for each contact). After you have added new contacts, click **Save & Close**.

Searching Outlook Contacts

You can only search outlook contacts on the pre-dialing screen.

Note

Make sure that you sign into the phone using User Sign-in or Web Sign-in or Sign in via PC method, so that the phone can connect to the Microsoft Exchange Server to obtain the outlook contacts.

To search for Outlook contacts on the pre-dialing screen:

1. On the pre-dialing screen, enter the first few continuous characters of the Outlook contact name or number. The phone performs an Intelligent search (e.g., press the digit key 2 to search the letters "2, a, b and c").

   The entries whose name or phone number matches the characters entered will appear on the LCD screen/touch screen. The search results include your Skype for Business contacts, local contacts and Microsoft Outlook contacts.

Viewing Outlook Contacts

If you have configured the phones to display a directory named **Outlook Contacts** using parameter "exchange.outlook_contact.enable", the **Outlook Contacts** directory will include your Outlook contacts.

To view Outlook contacts via the phone user interface:

1. Press **Directory->Outlook Contacts**.

Call Log

Save Call Log

Call log contains call information such as remote party identification, time and date, 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.

Skype for Business phones maintain a local call log. Call log consists of four lists: Missed Calls, Placed Calls, Received Calls, and Forwarded Calls (Forwarded Calls are not applicable to T48S Skype for Business phones). Each call log list supports up to 100 entries. To store call information, you must enable save call log feature in advance. You can access the call history information via phone user interface only.

Procedure

Call log can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure call log feature. **Parameter:** features.save_call_history
Local	Web User Interface	Configure call log feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure call log feature.

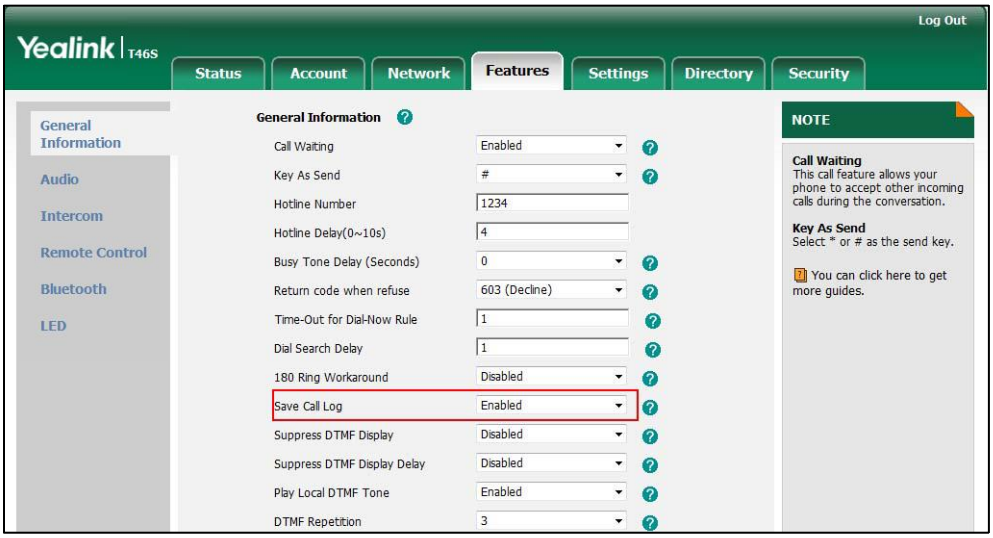
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.save_call_history	**0 or 1**	**1**
Description: Enables or disables the phone to save the local call log. **0**-Disabled, the phone cannot save the missed calls, placed calls, received calls and the forwarded calls in the call log lists. **1**-Enabled **Web User Interface:** Features->General Information->Save Call Log **Phone User Interface:** Menu->Features->History Setting->History Record		

To save call log feature via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **Save Call Log**.



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

To configure call log feature via phone user interface:

1. Press **Menu**->**Features**->**History Setting**.
2. Press or , or the **Switch** soft key to select the desired value from the **History Record** field.
3. Press the **Save** soft key to accept the change.

Exporting Call Log

User or administrator can access call logs by downloading them to the local system for diagnosis purpose.

Procedure

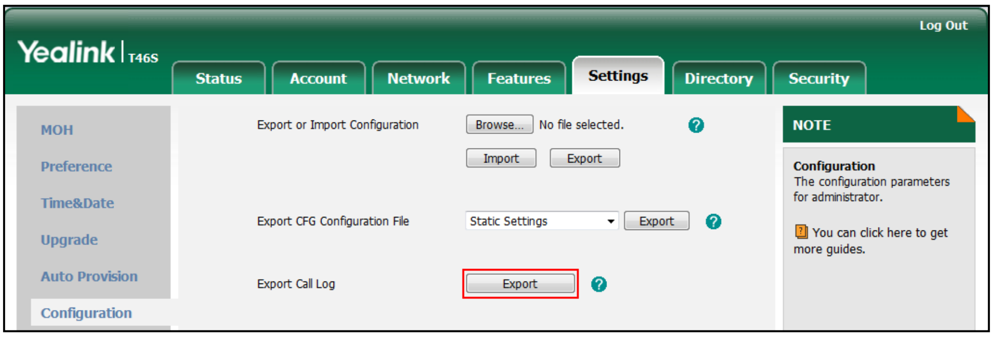
Exporting call log can be configured locally.

Local	Web User Interface	Export the call log. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-config&q=load

To export the call logs via web user interface:

1. Click on **Settings**->**Configuration**->**Export Call Log**.

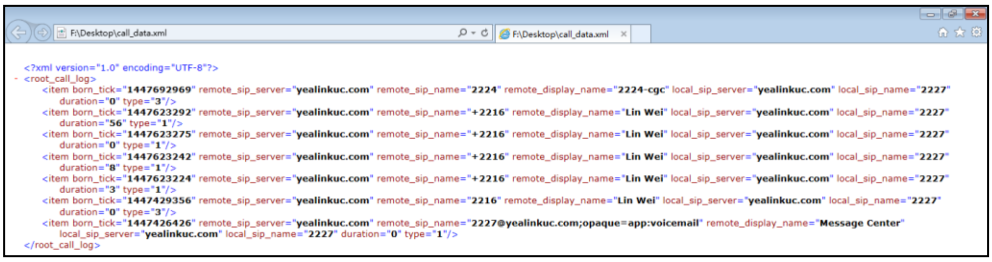
2. Click **Export** to open file download window, and then save the file to your local system.



To view the call logs on your local system:

1. Open the folder where you save the call logs.
2. Double-click the call logs file that is in .xml format.

   The following figure shows a portion of a call logs file:



Missed Call Log

Missed call log allows the phone to display a missed call icon on the idle screen, and to log missed calls in the Missed Calls list when the phone misses calls. Once the user accesses the Missed Calls list, the missed call icon on the idle screen disappears.

Procedure

Missed call log can be configured using the configuration files or locally.

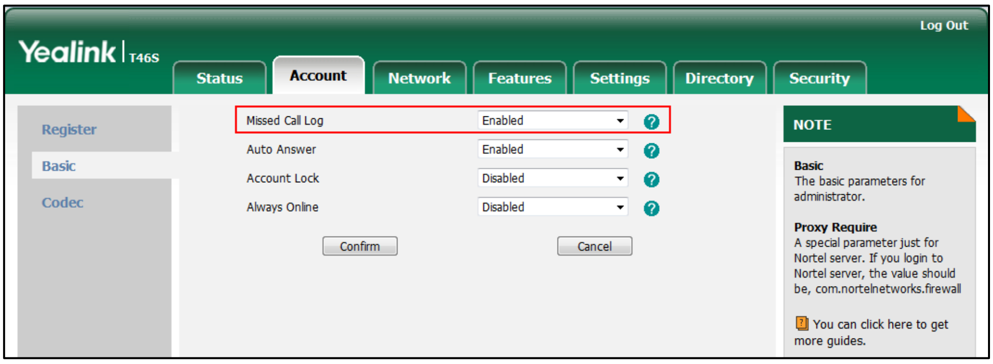
Central Provisioning (Configuration File)	<MAC>.cfg	Configure missed call log feature. **Parameter:** account.1.missed_calllog
Local	Web User Interface	Configure missed call log feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.1.missed_calllog	**0 or 1**	**1**
Description: Enables or disables the phone to indicate and record missed calls for the account. **0**-Disabled, the phone does not display a missed call on the idle screen and does not log the missed call in the Missed Calls list when missed calls. **1**-Enabled, the phone displays a missed call icon on the idle screen and logs the missed call in the Missed Calls list when missed calls. **Note:** It works only if the value of the parameter "features.save_call_history" is set to 1 (Enabled). **Web User Interface:** Account->Basic->Missed Call Log **Phone User Interface:** None		

To configure missed call log via web user interface:

1. Click on **Account**->**Basic**.
2. Select the desired value from the pull-down list of **Missed Call Log**.



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

History Record Contacts Avatar

History record contacts avatar allows the history record to display the contact avatars. It is only applicable to T48S/T46S/CP960 Skype for Business phones.

Procedure

History record contacts avatar can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the contacts avatar for history record. **Parameter:** features.call_history_contacts_avator.enable
Local	Web User Interface	Configure the contacts avatar for history record. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

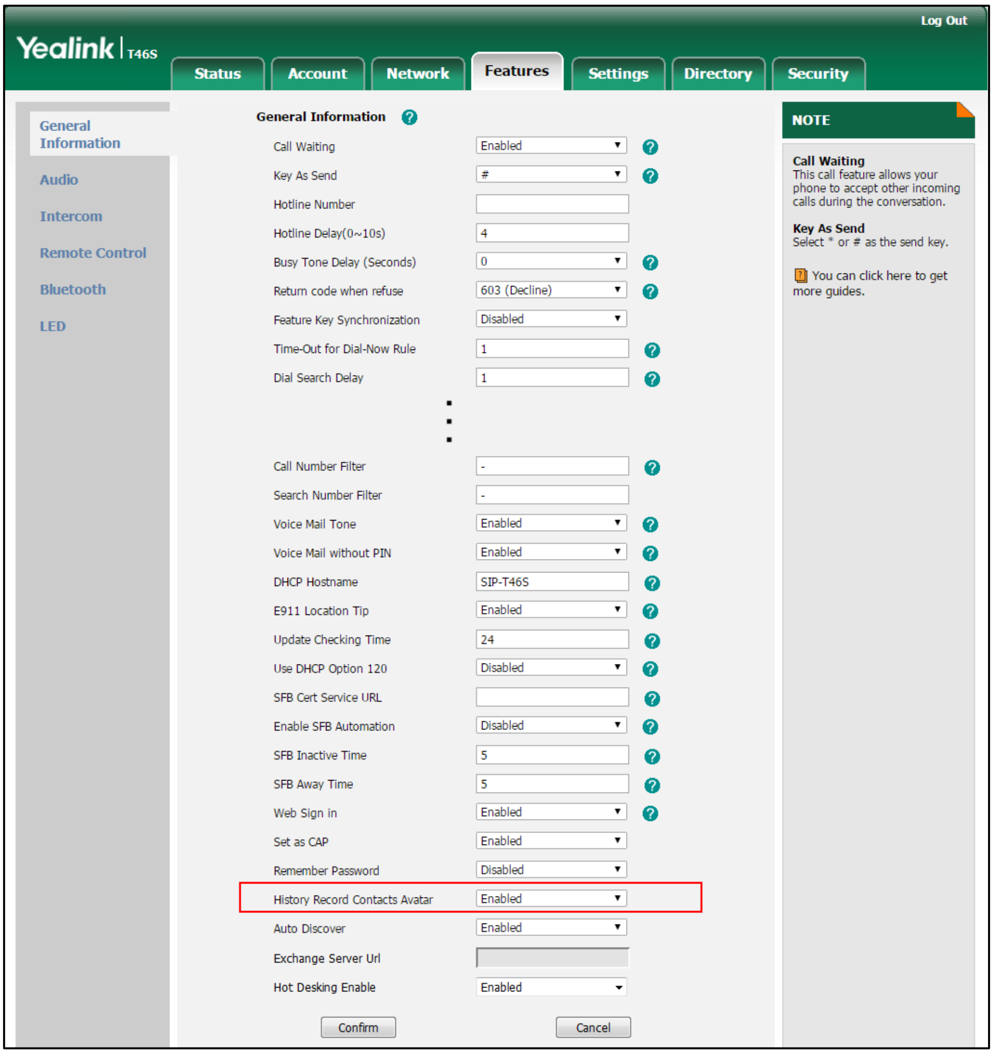
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.call_history_contacts_avator.enable	**0 or 1**	**1**
Description: Enables or disables the history record to display the contact avatars. **0**-Disabled, the history records do not display contact avatars. **1**-Enabled, the history records display contact avatars. **Note:** It is only applicable to T48S/T46S Skype for Business phones. **Web User Interface:** Features->General Information->History Record Contacts Avatar **Phone User Interface:** Menu->Features->History Setting->Contacts Avatar		

To configure contacts avatar feature via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **History Record Contacts Avatar**.



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

To configure contacts avatar feature via phone user interface:

1. Press **Menu**->**Features**->**History Setting**.
2. Press or , or the **Switch** soft key to select the desired value from the **Contacts Avatar** field.
3. Press the **Save** soft key to accept the change.

Dial Search Delay

Dial search delay defines a period of delay time before the phones automatically displays the search results. It is applicable only when searching for contacts on the dialing screen.

Procedure

Dial search delay can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure dial search delay feature. **Parameter:** sfb.search_delay_time
Local	Web User Interface	Configure dial search delay feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

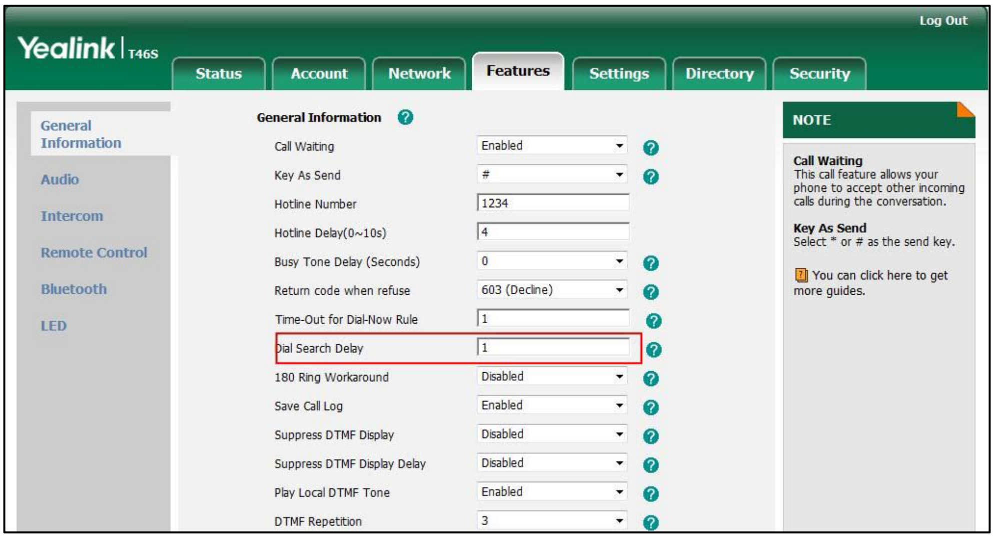
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sfb.search_delay_time	**Integer from 1 to 10**	**1**
Description: Configures the delay time (in seconds) for the phone to automatically display the search results on the dialing screen. **Example:** sfb.search_delay_time = 1 **Web User Interface:** Features->General Information->Dial Search Delay **Phone User Interface:** None		

To configure dial search delay via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **Dial Search Delay**.



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

Live Dialpad

Live dialpad allows the phone to automatically dial out the entered phone number after a specified period of time.

Procedure

Live dialpad can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure live dialpad. **Parameters:** phone_setting.predial_autodial phone_setting.inter_digit_time
Local	Web User Interface	Configure live dialpad. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-preference&q=load

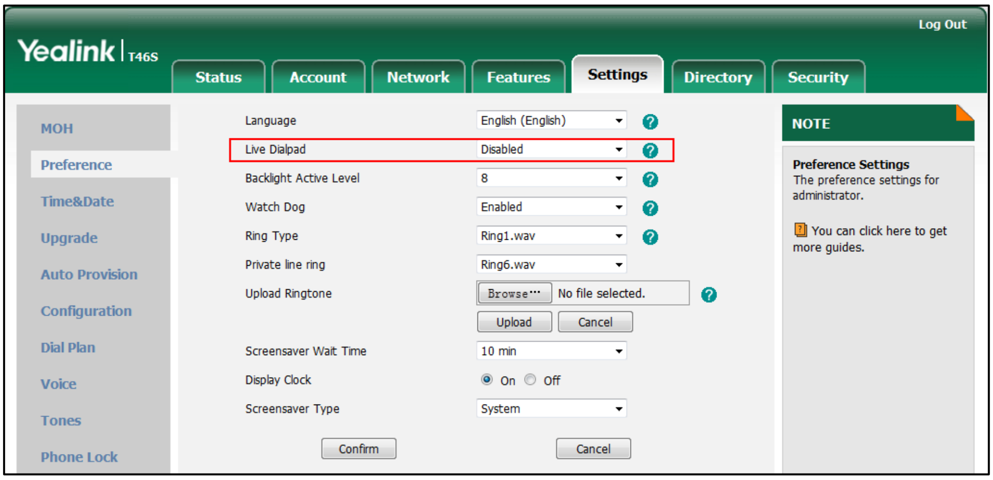
Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.predial_autodial	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Enables or disables live dialpad feature. **0**-Disabled **1**-Enabled, the phone will automatically dial out the entered phone number on the dialing screen without pressing a send key. **Web User Interface:** Settings->Preference->Live Dialpad **Phone User Interface:** None		
phone_setting.inter_digit_time	**Integer from 1 to 14**	**8**
Description: Configures the delay time (in seconds) for the phone to automatically dial out the entered digits without pressing a send key. **Note:** It works only if the value of the parameter “phone_setting.predial_autodial” is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		

To configure live dialpad via web user interface:

1. Click on **Settings**->**Preference**.
2. Select the desired value from the pull-down list of **Live Dialpad**.



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

Call Waiting

Call waiting allows the phone 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/touch screen. Call waiting tone allows the 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 phone. For more information, refer to Tones on page 319.

Procedure

Call waiting and call waiting tone can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure call waiting and call waiting tone. **Parameters:** call_waiting.enable call_waiting.tone
Local	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
	Phone User Interface	Configure call waiting and call waiting tone.

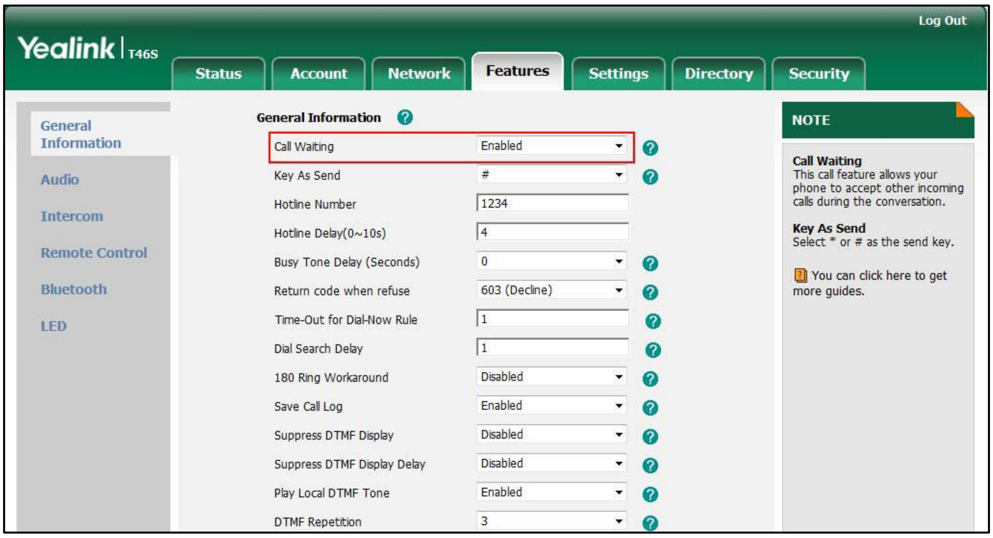
Details of Configuration Parameters:

Parameters	Permitted Values	Default
call_waiting.enable	**0 or 1**	**1**
Description: Enables or disables call waiting feature. **0**-Disabled, a new incoming call is automatically rejected by the phone with a busy message while during a call. **1**-Enabled, the LCD screen/touch screen will present a new incoming call while during a call.		

Parameters	Permitted Values	Default
Web User Interface: Features->General Information->Call Waiting **Phone User Interface:** Menu->Features->Call Waiting->Call Waiting		
call_waiting.tone	**0 or 1**	**1**
Description: Enables or disables the phone to play the call waiting tone when the phone receives an incoming call during a call. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "call_waiting.enable" is set to 1 (Enabled). **Web User Interface:** Features->Audio->Call Waiting Tone **Phone User Interface:** Menu->Features->Call Waiting->Play Tone		

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**.

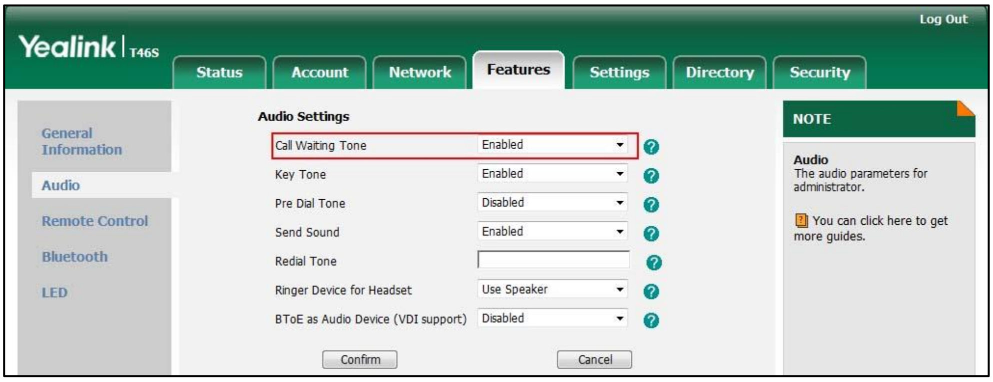


3. Click **Confirm** to accept the change.

To configure call waiting tone via web user interface:

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

2. Select the desired value from the pull-down list of **Call Waiting Tone**.



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

To configure call waiting and call waiting tone via phone user interface:

1. Press **Menu**->**Features**->**Call Waiting**.
2. Press or , or the **Switch** soft key to select the desired value from the **Call Waiting** field.
3. Press or , or the **Switch** soft key to select the desired value from the **Play Tone** field.
4. Press the **Save** soft key to accept the change.

Auto Answer

Auto answer allows the phone to automatically answer an incoming call. Skype for Business phones will not automatically answer the incoming call during a call even if auto answer is enabled. Auto-Answer delay defines a period of delay time before the phone automatically answers incoming calls.

Auto Answer Tone

Auto answer tone allows the phones to play a tone when an incoming call is automatically answered. You can customize the auto answer tone or select specialized tone sets (vary from country to country) for your phone. For more information, refer to Tones on page 319.

Procedure

Auto answer can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure auto answer. **Parameter:** account.1.auto_answer
	<y0000000000xx>.cfg	Specify a period of delay time for auto answer. **Parameter:** features.auto_answer_delay
Local	Web User Interface	Configure auto answer. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0 Specify a period of delay time for auto answer. **Navigate to**: http://<phoneIPAddress>servlet?p=features-general&q=load

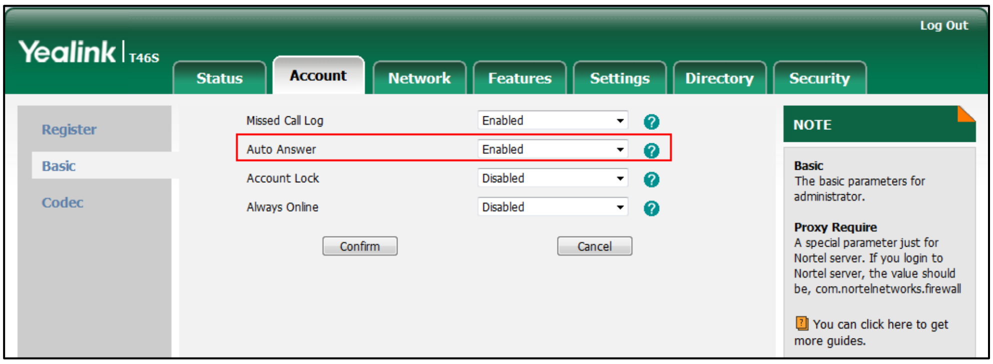
Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.1.auto_answer	**0 or 1**	**0**
Description: Enables or disables auto answer feature for the account. **0**-Disabled **1**-Enabled, the phone can automatically answer an incoming call. **Note:** The phone cannot automatically answer the incoming call during a call even if auto answer is enabled. **Web User Interface:** Account->Basic->Auto Answer **Phone User Interface:** Menu->Features->Auto Answer->Line 1->Auto Answer		
features.auto_answer_delay	**Integer from 1 to 4**	**1**

Parameters	Permitted Values	Default
Description: Configures the delay time (in seconds) before the phone automatically answers an incoming call. **Web User Interface:** Features->General Information->Auto-Answer Delay(1~4s) **Phone User Interface:** None		

To configure auto answer via web user interface:

1. Click on **Account**->**Basic**.
2. Select the desired value from the pull-down list of **Auto Answer**.

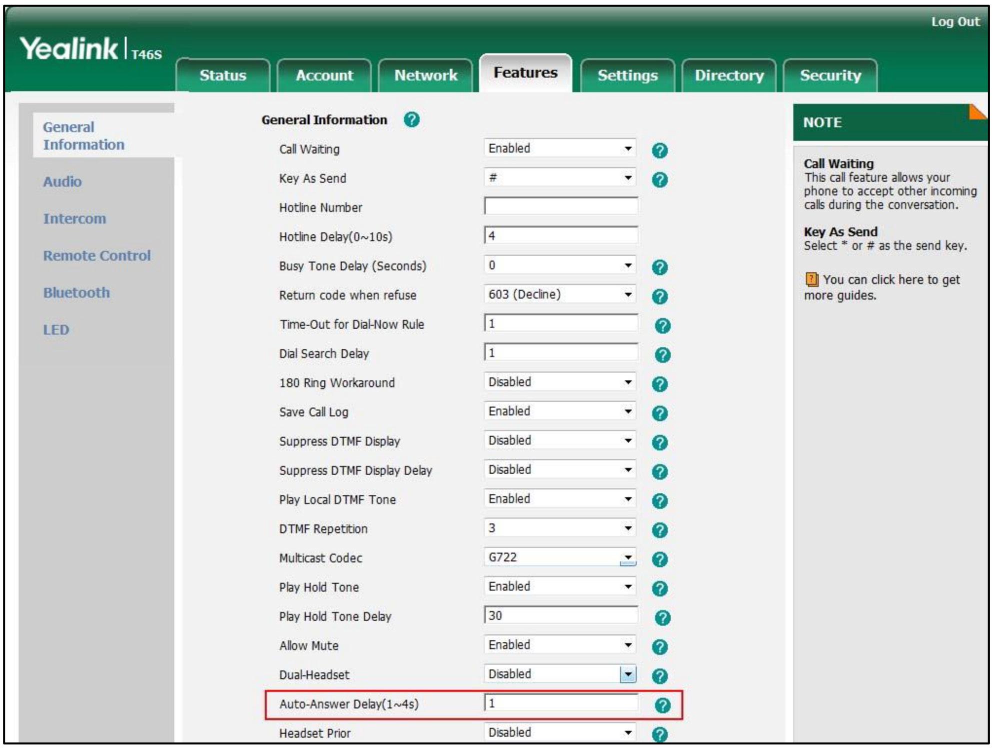


3. Click **Confirm** to accept the change.

To configure a period of delay time for auto answer via web user interface:

1. Click on **Features**->**General Information**.

2. Enter the desired time in the **Auto-Answer Delay(1~4s)** field.



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

To configure auto answer via phone user interface:

1. Press **Menu**->**Features**->**Auto Answer**->**Line 1**-> **Auto Answer**.
2. Press or , or the **Switch** soft key to select the desired value from the **Auto Answer** field.
3. Press the **Save** 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 configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure busy tone delay. **Parameter:** features.busy_tone_delay
Local	Web User Interface	Configure busy tone delay. **Navigate to**: http://<phoneIPAddress>/servlet?p

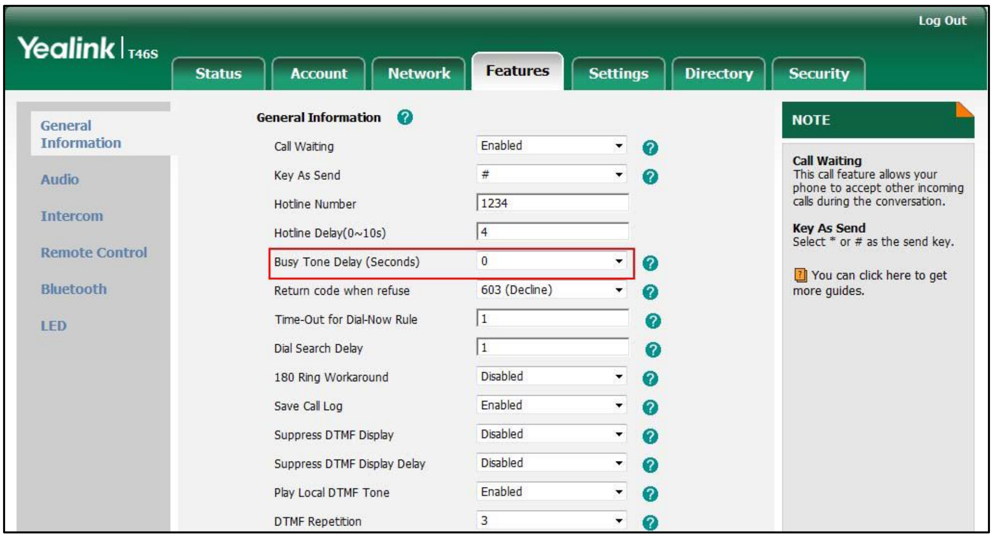
		=features-general&q=load

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, the phone will not play a busy tone. **3**-3s, a busy tone is audible for 3 seconds on the phone. **5**-5s **Web User Interface:** Features->General Information->Busy Tone Delay (Seconds) **Phone User Interface:** None		

To configure busy tone delay via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Busy Tone Delay (Seconds)**.



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

Return Code When Refuse

Return code when refuse defines the return code and reason of the SIP response message for the refused call. The caller's phone LCD screen/touch screen displays the reason according to the received return code. Available return codes and reasons are:

- 404 (Not Found)
- 480 (Temporarily Not Available)
- 486 (Busy Here)
- 603 (Decline)

Procedure

Return code for refused call can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the return code and the reason of the SIP response message when refusing a call. **Parameter:** features.normal_refuse_code
Local	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

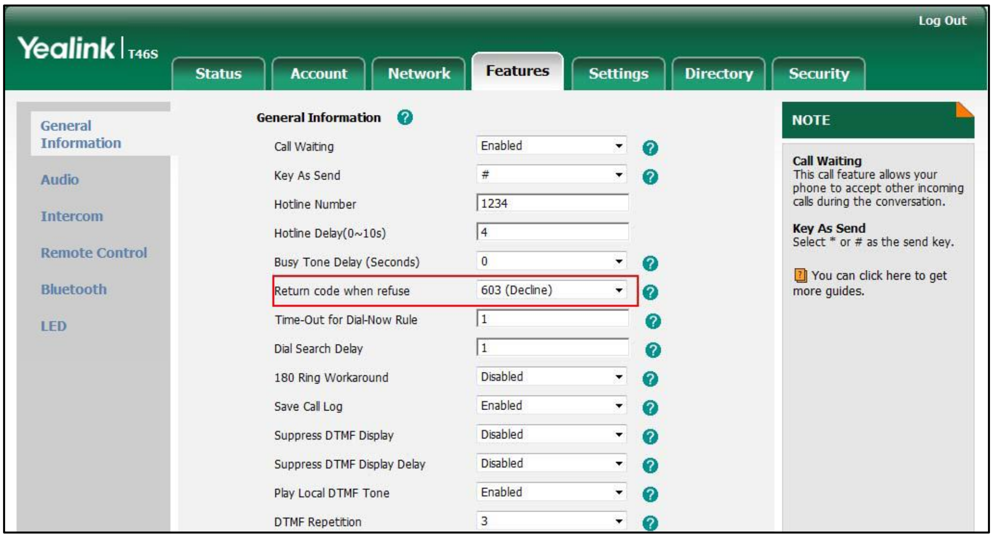
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.normal_refuse_code	**404, 480, 486 or 603**	**603**
Description: Configures a return code and reason of SIP response messages when the phone rejects an incoming call. A specific reason is displayed on the caller's phone LCD screen/touch screen. **404**-Not Found **480**-Temporarily Not Available **486**-Busy Here, the caller's phone LCD screen/touch screen will display the message "Busy Here" when the callee rejects the incoming call. **603**-Decline **Web User Interface:**		

Parameter	Permitted Values	Default
Features->General Information->Return Code When Refuse **Phone User Interface:** None		

To specify the return code and the reason when refusing a call via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Return Code When Refuse**.



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

Early Media

Early media refers to media (e.g., audio and video) played to the caller before a SIP call is actually established. Current implementation supports early media through the 183 message. When the caller receives a 183 message with SDP before the call is established, a media channel is established. This channel is used to provide the early media stream for the caller.

180 Ring Workaround

180 ring workaround defines whether to deal with the 180 message received after the 183 message. When the caller receives a 183 message, it suppresses any local ringback tone and begins to play the media received. 180 ring workaround allows the phone to resume and play the local ringback tone upon a subsequent 180 message received.

Procedure

180 ring workaround can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure 180 ring workaround. **Parameter:** phone_setting.is_deal180
Local	Web User Interface	Configure 180 ring workaround. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

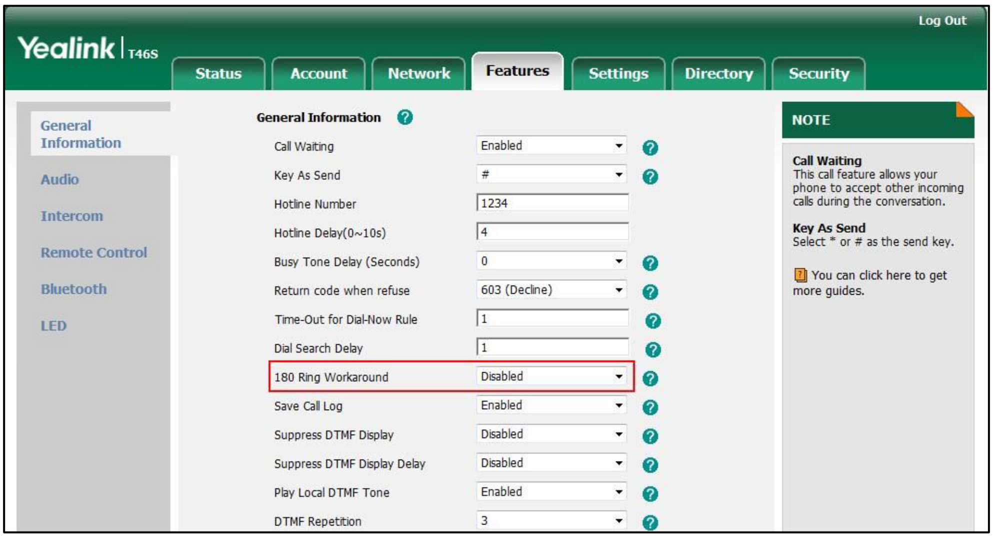
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.is_deal180	**0 or 1**	**0**
Description: Enables or disables the phone to deal with the 180 SIP message received after the 183 SIP message. **0**-Disabled **1**-Enabled, the phone will resume and play the local ringback tone upon a subsequent 180 message received. **Web User Interface:** Features->General Information->180 Ring Workaround **Phone User Interface:** None		

To configure 180 ring workaround via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **180 Ring Workaround**.



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

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 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. Skype for Business phones support two call hold methods, one is RFC 3264, which sets the "a" (media attribute) in the SDP to sendonly, recvonly or inactive (e.g., a=sendonly). The other is RFC 2543, which sets the "c" (connection addresses for the media streams) in the SDP to zero (e.g., c=0.0.0.0).

Call hold tone allows phones to play a warning tone at regular intervals when there is a call on hold. The warning tone is played through the speakerphone.

Procedure

Call hold can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the call hold tone and call hold tone delay. **Parameters:** features.play_hold_tone.enable features.play_hold_tone.delay
Local	Web User Interface	Configure the call hold tone and call hold tone delay. **Navigate to**:

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

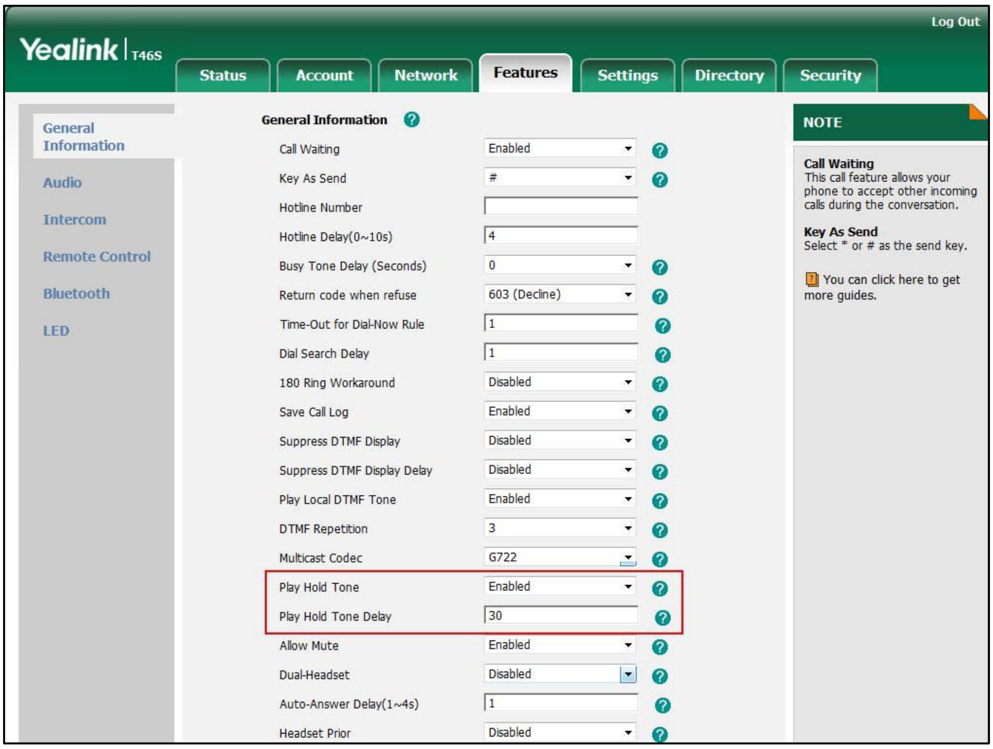
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.play_hold_tone.enable	**0 or 1**	**1**
Description: Enables or disables the phone to play a warning tone when there is a call on hold. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Play Hold Tone **Phone User Interface:** None		
features.play_hold_tone.delay	**Integer from 3 to 3600**	**30**
Description: Configures the interval (in seconds) at which the phone play a warning tone when there is a call on hold. If it is set to 30 (30s), the phone will play a warning tone every 30 seconds when there is a call on hold. **Note:** It works only if the value of the parameter "features.play_hold_tone.enable" is set to 1 (Enabled). **Web User Interface:** Features->General Information->Play Hold Tone Delay **Phone User Interface:** None		

To configure call hold tone and call hold tone delay via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Play Hold Tone**.

3. Enter the desired time in the **Play Hold Tone Delay** field.



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

Music on Hold

Music on Hold (MoH) is the business practice of playing recorded music to fill the silence that would be heard by the party who has been placed on hold. When a call is placed on hold, the phone will play a ring tone to the held party. Music on Hold is not applicable to CP960 Skype for Business phones.

Users can upload a custom music to the phone or use the music sent from the Skype for Business via In-band provisioning method.

The uploaded music format must meet the following:

Format	Single File Size	Duration
.wav	1~500K	1~30S

Note

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

Procedure

Music on hold can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the music on hold feature. **Parameter**: sfb.music_on_hold.enable
		Configure the music on hold mode. **Parameter**: sfb.music_on_hold.mode
		Specify the access URL of the custom ring tone. **Parameter**: sfb.music_on_hold.url
		Delete the custom music files. **Parameter:** sfb.music_on_hold.delete
Local	Web User Interface	Configure the music on hold feature. Configure the music on hold mode. Specify the access URL of the custom ring tone. Delete the custom music files. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-moh&q=load

Details of the Configuration Parameters:

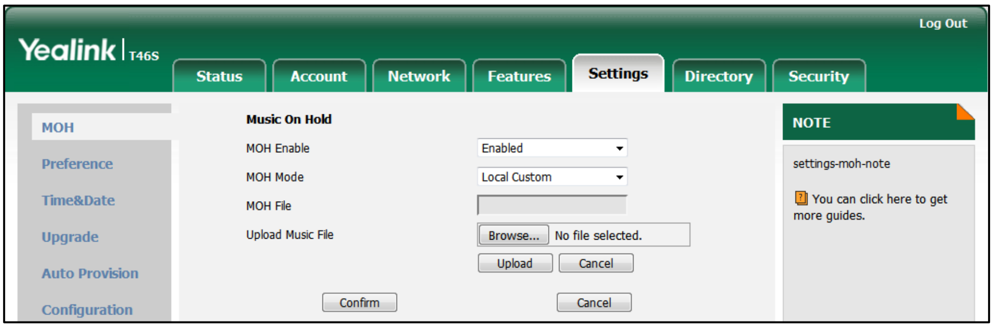
Parameters	Permitted Values	Default
sfb.music_on_hold.enable	**0 or 1**	**0**
Description: Enables or disables the phone to play music for the held party. **0**-Disabled **1**-Enabled **Note**: It is not applicable to CP960 Skype for Business phones.		

Parameters	Permitted Values	Default
Web User Interface: Settings->MOH->MOH Enable **Phone User Interface:** None		
sfb.music_on_hold.mode	**0 or 1**	**1**
Description: Configures the source of the music played for the held party. **0**-Inband Provision **1**-Local Custom **Note:** It works only if the value of the parameter "sfb.music_on_hold.enable" is set to 1 (Enabled). It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Settings->MOH->MOH Mode **Phone User Interface:** None		
sfb.music_on_hold.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom music file. **Example:** sfb.music_on_hold.url = tftp://192.168.1.100/Customring.wav **Note:** It works only if the values of the parameter "sfb.music_on_hold.enable" and parameter "sfb.music_on_hold.mode" are set to 1 (Enabled). It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Settings->MOH->MOH File **Phone User Interface:** None		
sfb.music_on_hold.delete	**http://localhost/all**	**Blank**
Description: Delete all custom music files. **Example:**		

Parameters	Permitted Values	Default
sfb.music_on_hold.delete = http://localhost/all **Note**: It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Settings->MOH->Delete **Phone User Interface:** None		

To configure music on hold via web user interface:

1. Click on **Settings**->**MOH**.
2. Select **Enabled** from the pull-down list of **MOH Enable**.



3. Select the desired mode from the pull-down list of **MOH Mode**.
   - If you select **Inband provision**, your phone will play the music sent from the Skype for Business Server to the held party.
   - If you select **Local Custom**, you can click **Browse** in the **Upload Music File** field to select a music file saved in your local computer.

     Click **Upload** to upload the custom music.

     The held party will hear your custom music
4. Click **Confirm** to accept the change.

Call Forward

The phone provides a flexible call forwarding feature that enables you to forward incoming calls to another destination. Skype for Business phones redirect an incoming INVITE message by responding with a 303 Moved See Other message, which contains a Contact header with a new URI that should be tried.

Call forwarding has following types:

- **Forward Calls to a Contact**: Incoming calls are forwarded to your preset number or contact.
- **Simultaneously Ring to a Contact**: The preset number will ring simultaneously when

your phone receives an incoming call.

- **Forward to Voice Mail**: Incoming calls are forwarded to your voicemail.
- **Forward to Delegates**: If you have delegates assigned to your line, you can forward all incoming calls directly to your delegates. For more information on how to assign a delegate, refer to Assigning Delegates on page 259.
- **Simultaneously Ring to Delegates**: If you have delegates assigned to your line, you can enable your delegates' phones to simultaneously ring when you receive incoming calls.
- **Simultaneously Ring to Team Call**: If you have team-call group assigned to your line, you can enable your team-call members' phones to simultaneously ring when you receive incoming calls. For more information on how to configure a team-call group, refer to Setting up Team-call Group on page 240.

Diversion/History-Info

Skype for Business phones support the redirected call information sent by the SIP server with Diversion header, per draft-levy-sip-diversion-08, or History-info header, per RFC 4244. The Diversion/History-info header is used to inform the phone of a call’s history. For example, when a phone has been set to enable call forward, the Diversion/History-info header allows the receiving phone to indicate who the call was from, and from which phone number it was forwarded.

Procedure

Call forward can be configured using the configuration files or locally.

Procedure

Call forward can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure diversion/history-info feature. **Parameter:** features.fwd_diversion_enable
Local	Web User Interface	Configure diversion/history-info feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure call forward.

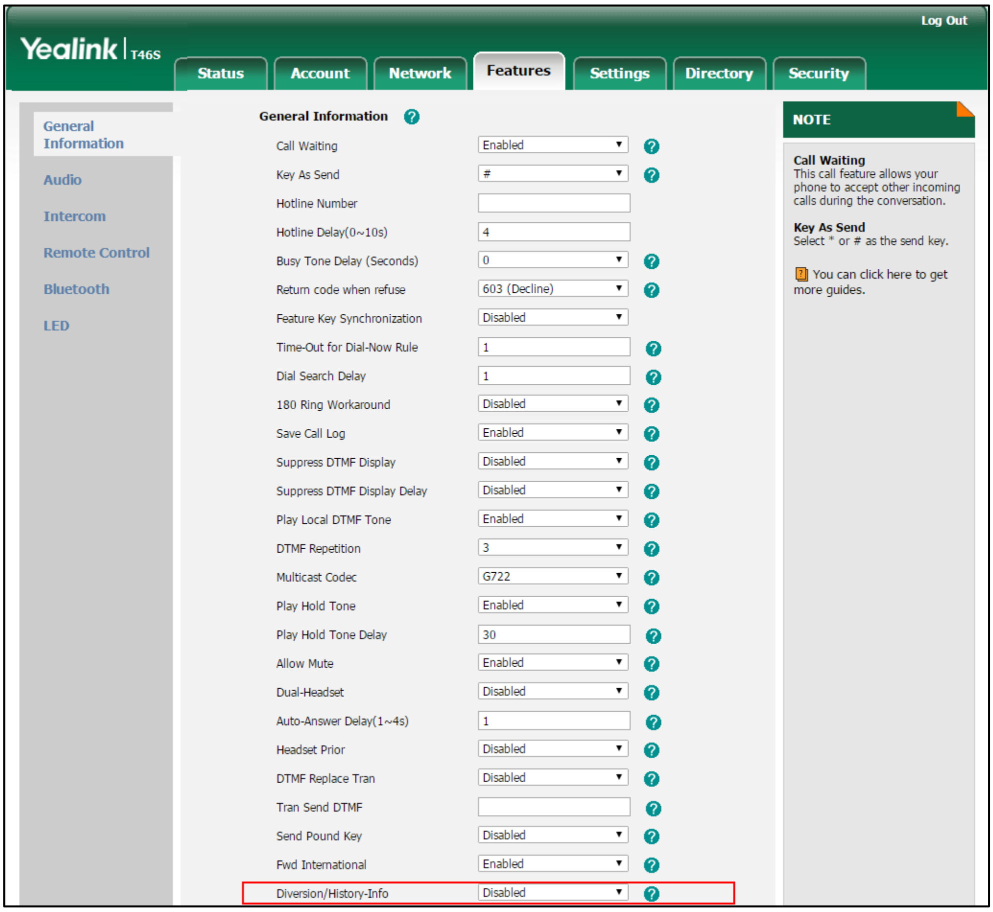
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.fwd_diversion_enable	**0 or 1**	**0**
Description: Enables or disables the phone to present the diversion information when an incoming call is forwarded to your phone. **0**-Disabled **1**-Enabled **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->General Information->Diversion/History-Info **Phone User Interface:** None		

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 enable call forward:

1. Press **Menu**->**Features**->**Call Forward**.
2. Press or , or the **Switch** soft key to select **On** from the **Call Forward** field.
3. Select the desired value.
4. Press the **Save** soft key.

Team-Call Group

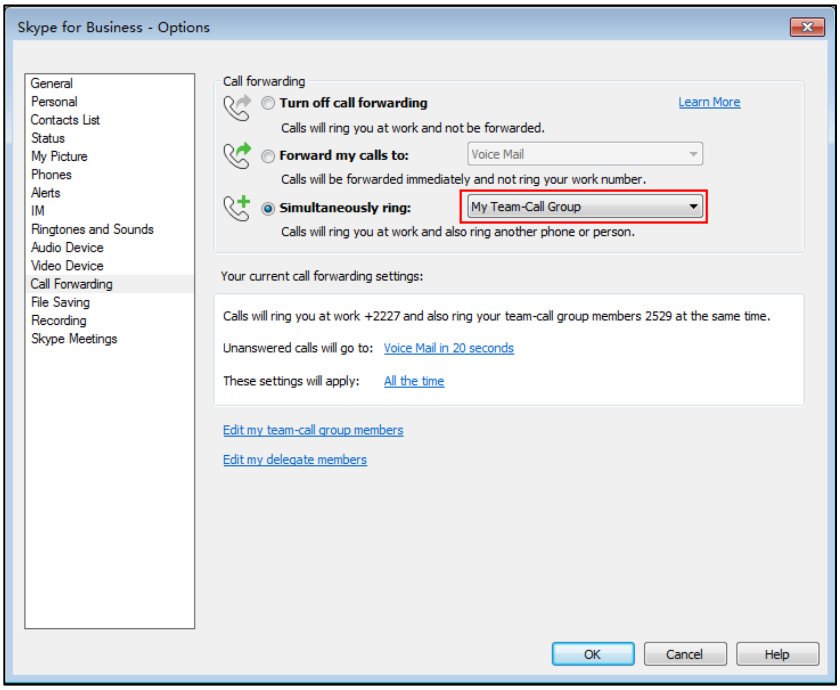
A team-call group is a team of people who can answer your work calls. You can add or remove members, and select when they can answer calls for you. Team-call group can be configured via Skype for Business client only.

Assume that you have a team of people working on the same project or tasks. If you are away from your desk and your phone rings, anyone in the team-call group can answer the call for you. As soon as a team member picks up the phone, the other phones stop ringing.

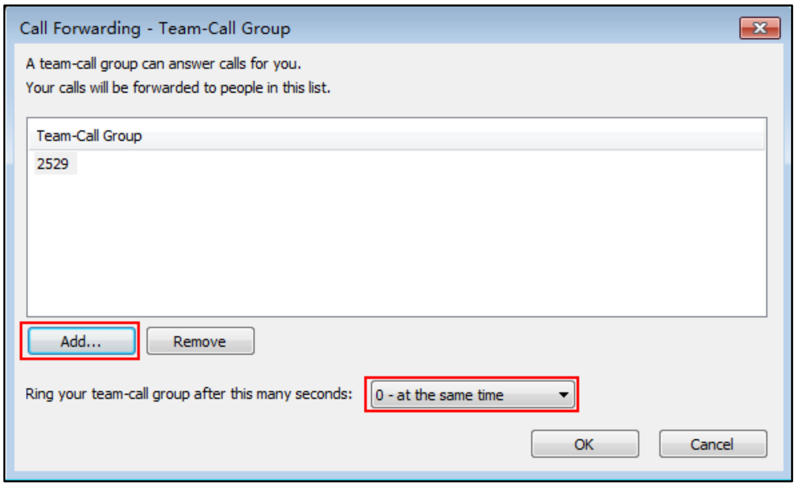
Setting up Team-call Group

To set up team-call group using Skype for Business client:

1. Open Skype for Business client.
2. Sign into Skype for Business client.
3. Click the button, and then click **Call Forwarding Settings**.
4. Mark the radio box in **Simultaneously ring** field.
5. Select **My Team-Call Group** from the pull-down list of **Simultaneously ring**.



6. In the **Team-Call Group** dialog box, click **Add** to choose team-call group members.
7. Click the **Ring your team-call group after this many seconds** pull-down list to determine when your team-call group members' phones ring.



8. Click **OK**.
9. Click **OK** in the **My Team-Call Group** dialog box.
10. Click **OK** in the **Options** dialog box.

    Simultaneous ringing is enabled for all assigned team-call members. If your line receives an incoming call, other phones in the team-call group will ring too.

Team-Call Ringtone

Team-call ring tone feature allows the phone to play a distinct ringtone when receiving a team-call.

Procedure

Team-call ring tone can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure a ring tone for the team-call. **Parameter:** phone_setting.team_call_ring.enable phone_setting.team_call_ring_type
Local	Phone User Interface	Configure a ring tone for the team-call.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.team_call_ring.enable	**0 or 1**	**1**
Description: Enables or disables the phone to play a distinct ringtone for team-call. **0**-Disabled, incoming calls to team-call group will use the phone's ring tone. The phone's ring tone is configured by the parameter "phone_setting.ring_type". **1**-Enabled, you can set a distinct ringtones for team-call. **Web User Interface:** None **Phone User Interface:** None		
phone_setting.team_call_ring_type	**Refer to the following content**	**Ring1.wav**
Description: Configures a ring tone for the team-call.		

Parameter	Permitted Values	Default
Permitted Values: Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring.wav). **Example:** To configure a phone built-in ring tone (e.g., Ring1.wav): phone_setting.team_call_ring_type = Ring1.wav To configure a custom ring tone (e.g., Customring.wav): phone_setting.team_call_ring_type = Customring.wav **Web User Interface:** None **Phone User Interface:** Menu->Basic->Sounds->Ring Tones->Team Call		

To set a ringtone for the team-call via phone user interface:

1. Press **Menu**->**Basic**->**Sounds**->**Ring Tones**->**Team Call**.
2. Press or to select a ring tone.
3. Press the **Save** soft key to accept the change.

Response Group

If you sign into the phone using On-Premises account, you can use response group feature. Current Online environment does not support this feature.

A response group is a feature that route and queue incoming calls to groups of people, called agents, such as for a help desk or a customer service desk.

When someone calls a response group, the call is routed to an agent based on a hunt group or the caller's answers to interactive voice response (IVR) questions. The Response Group application uses standard response group routing methods to route the call to the next available agent. After a call agent accepts the call, other agents' phones stop ringing.

The routing methods of response group are as follows:

- LongestIdle - Calls are routed to the agent who has been idle (that is, not involved in a Skype for Business activity) for the longest period of time.
- RoundRobin - Calls are routed to the next agent on the list.
- Serial - Calls are always routed to the first agent on the list, and are only routed to other agents if this person is not available or does not answer within the allotted time.
- Parallel - Calls are routed to all agents at the same time, except for agents whose presence status indicates that they are in a call or otherwise unavailable.
- Attendant - Calls are routed to all agents at the same time, even if the agent's presence

status indicates that he or she is in a call or otherwise unavailable. The only exception occurs when an agent has set his or her presence to Do Not Disturb.

The default routing method is Parallel.

For information on creating a response group, refer to *Deployment process for Response Group in Skype for Business 2015* on Microsoft TechNet.

Response Group Ringtone

Response group ring tone feature allows the phone to play a distinct ringtone when receiving a response group call.

Procedure

Response group ring tone can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure a ring tone for the response group calls. **Parameter:** phone_setting.rsg_call_ring.enable phone_setting.rsg_call_ring_type
Local	Phone User Interface	Configure a ring tone for the response group calls.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.rsg_call_ring.enable	**0 or 1**	**1**
Description: Enables or disables the phone play a distinct ringtone for response group calls. **0**-Disabled, incoming calls to response group will use the phone's ring tone. The phone's ring tone is configured by the parameter "phone_setting.ring_type". **1**-Enabled, you can set a distinct ringtones for response group calls. **Web User Interface:** None **Phone User Interface:** None		
phone_setting.rsg_call_ring_type	**Refer to the following content**	**Ring1.wav**

Parameter	Permitted Values	Default
Description: Configures a ring tone for response group calls. **Permitted Values:** Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring.wav). **Example:** To configure a phone built-in ring tone (e.g., Ring6.wav): phone_setting.rsg_call_ring_type = Ring6.wav To configure a custom ring tone (e.g., Customring.wav): phone_setting.rsg_call_ring_type = Customring.wav **Web User Interface:** None **Phone User Interface:** Menu->Basic->Sounds->Ring Tones->Response Group		

To set a ringtone for the response group via phone user interface:

1. Press **Menu**->**Basic**->**Sounds**->**Ring Tones**->**Response Group**.
2. Press ▲ or ▼ to select a ring tone.
3. Press the **Save** soft key to accept the change.

Call Queue

If you sign into the phone using Online account, you can use call queue feature. On-Premises environment does not support this feature.

A call queue is a feature that route and queue incoming calls to groups of people, called agents, such as for a help desk or a customer service desk.

When someone calls in to a phone number that is setup up with a call queue, they will hear a greeting first (if any is setup), and then they will be put in the queue and wait for the available call agent. The person calling in will hear music while they are on hold waiting, and the call in the queue will ring all call agents at the same time. After a call agent accepts the call, other agents' phones stop ringing.

For information on creating a call queue, refer to *Create an Office 365 Phone System call queue* on Microsoft TechNet.

Call Number Filter

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

Procedure

Call number filter can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the characters that the phone filters when dialing a number. **Parameters:** features.call_num_filter
Local	Web User Interface	Configure the characters that the phone filters when dialing a number. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

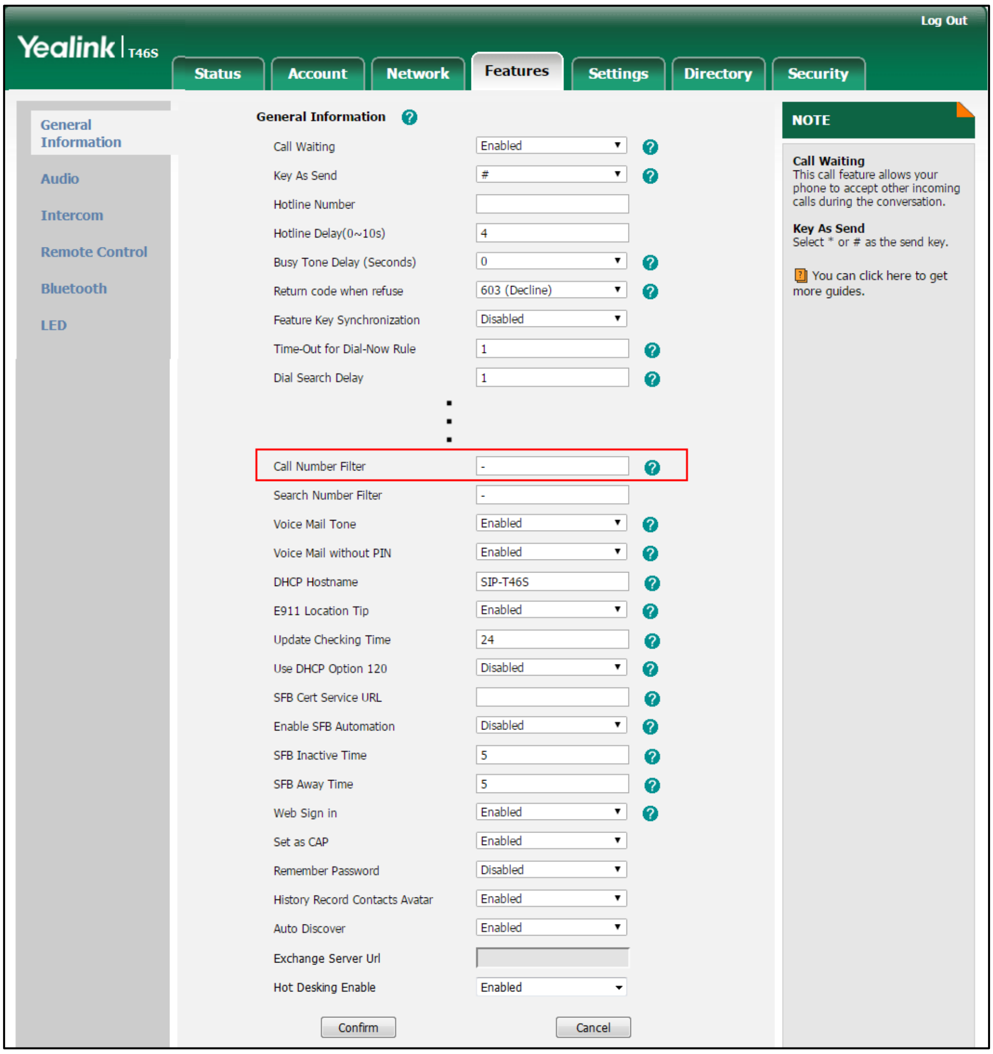
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.call_num_filter	**String within 99 characters**	**()-**
Description: Configures the characters that the phone filters when dialing a number. If the dialed number contains configured characters, the phone will automatically filter these characters when dialing. If the dialed SIP address contains configured characters, the phone will not filter these characters when dialing. **Example:** features.call_num_filter = . If you dial 3.61, the phone will filter the character ".", and then dial out 361. If you dial ralf.siebken@yealinksfb.com, the phone will not filter the character "." in the SIP address. **Note**: If it is left blank, the phone will not automatically filter any characters when dialing a number. If you want to filter just a space, you have to set the value to " ," (a space first followed by a comma). **Web User Interface:** Features->General Information->Call Number Filter **Phone User Interface:** None		

To configure the characters the phone filters when dialing via web user interface:

1. Click on **Features->General Information**.

2. Enter the desired character in the **Call Number Filter** field.



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

Search Number Filter

Search number filter feature allows the phone to automatically filter designated characters when searching for contacts.

Procedure

Search number filter can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the characters that the phone filters when searching for contacts. **Parameters:** features.search_num_filter
Local	Web User Interface	Configure the characters that the phone filters when searching for contacts. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

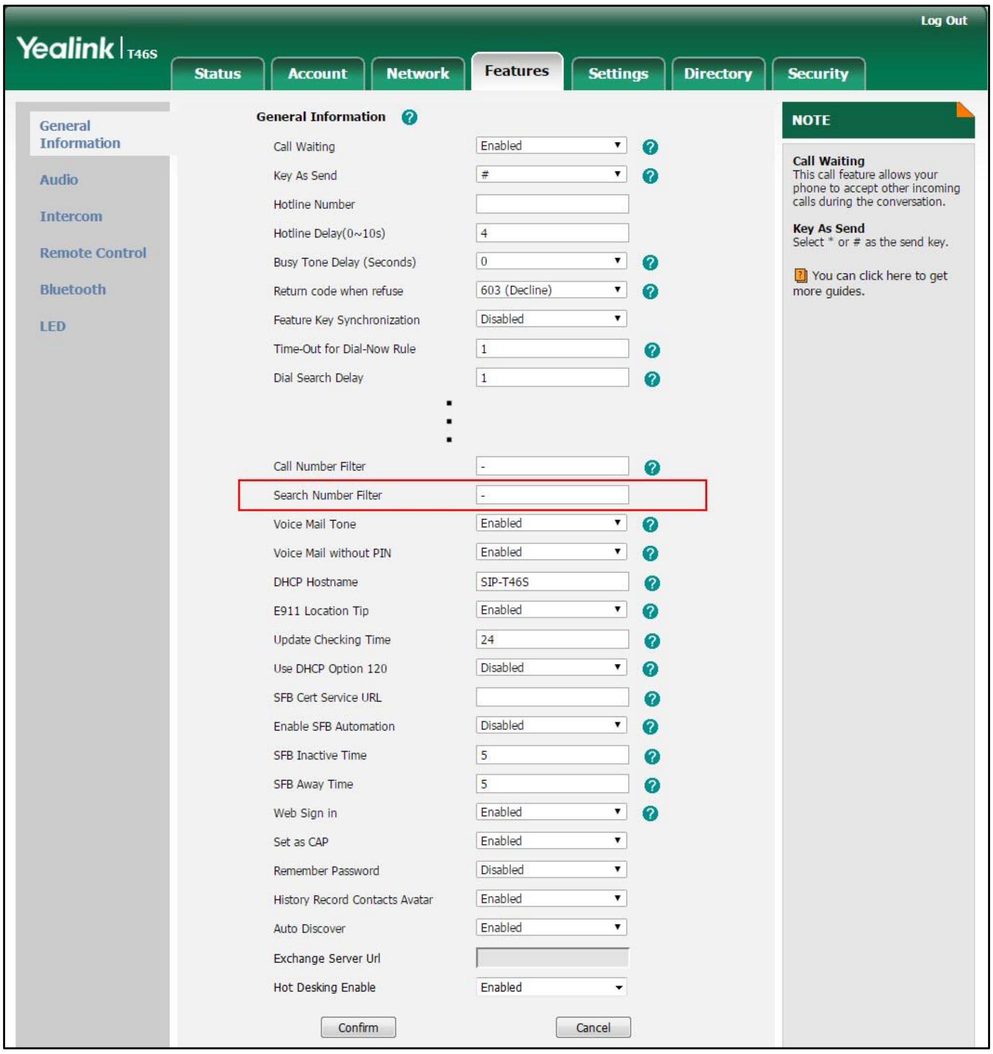
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.search_num_filter	**String within 255 characters**	**Blank**
Description: Configures the characters that the phone filters when searching for contacts. If the entered number contains configured characters, the phone will automatically filter these characters when searching for contacts. **Example:** features.search_num_filter = - If you enter 40-38, the phone will filter the character -, and then search 4038. **Note**: If it is left blank, the phone will not automatically filter any characters when searching for contacts. 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->Search Number Filter **Phone User Interface:** None		

To configure the characters the phone filters when searching for contacts via web user interface:

1. Click on **Features->General Information**.

2. Enter the desired character in the **Search Number Filter** field.



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

Allow Mute

You can mute the microphone of the active audio device during an active call, and then the other party cannot hear you. If allow mute feature is disabled, you cannot mute an active call.

Procedure

Allow mute can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure allow mute feature. **Parameters:** features.allow_mute
Local	Web User Interface	Configure allow mute feature.

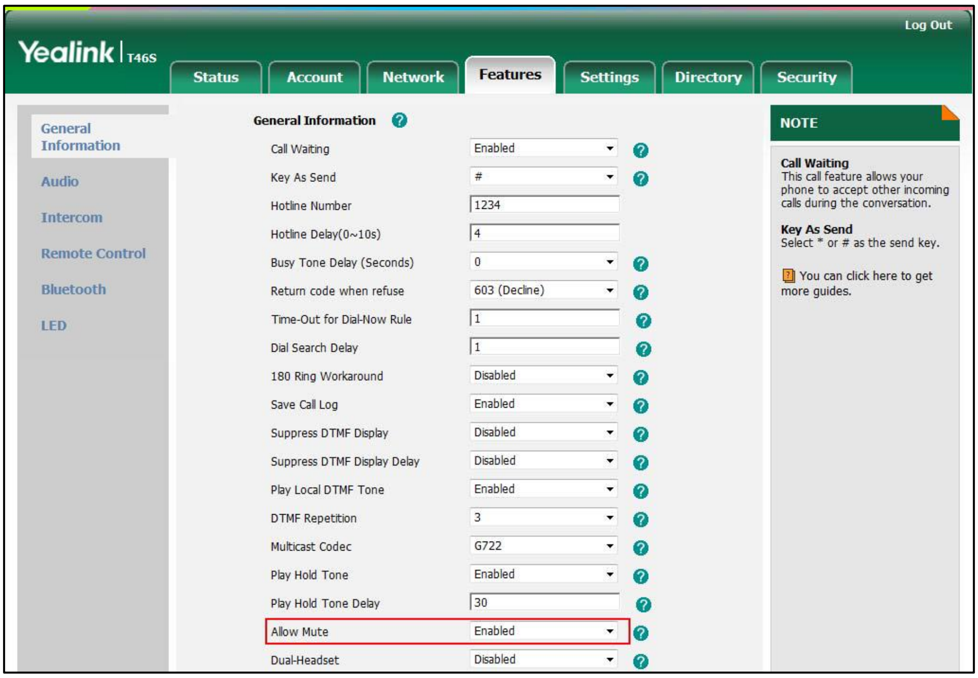
		Navigate to: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.allow_mute	**0 or 1**	**1**
Description: Enables or disables the phone to mute an active call. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Allow Mute **Phone User Interface:** None		

To configure allow mute via web user interface:

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



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

Intercom

Intercom allows establishing an audio conversation directly. The phone can answer intercom calls automatically.

Intercom is not applicable to CP960 Skype for Business phones.

Outgoing Intercom Calls

Intercom is a useful feature in office environments to quickly connect with an operator or secretary. Users can press an intercom key to view the intercom list, and then place an outgoing intercom call from the intercom list.

Procedure

Outgoing intercom calls can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the outgoing intercom calls feature. **Parameters:** features.intercom.enable features.intercom.outgoing intercom.x.label intercom.x.value
Web User Interface		Configure the outgoing intercom calls feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-intercom&q=load
Phone User Interface		Configure the outgoing intercom calls feature.

Details of Configuration Parameters:

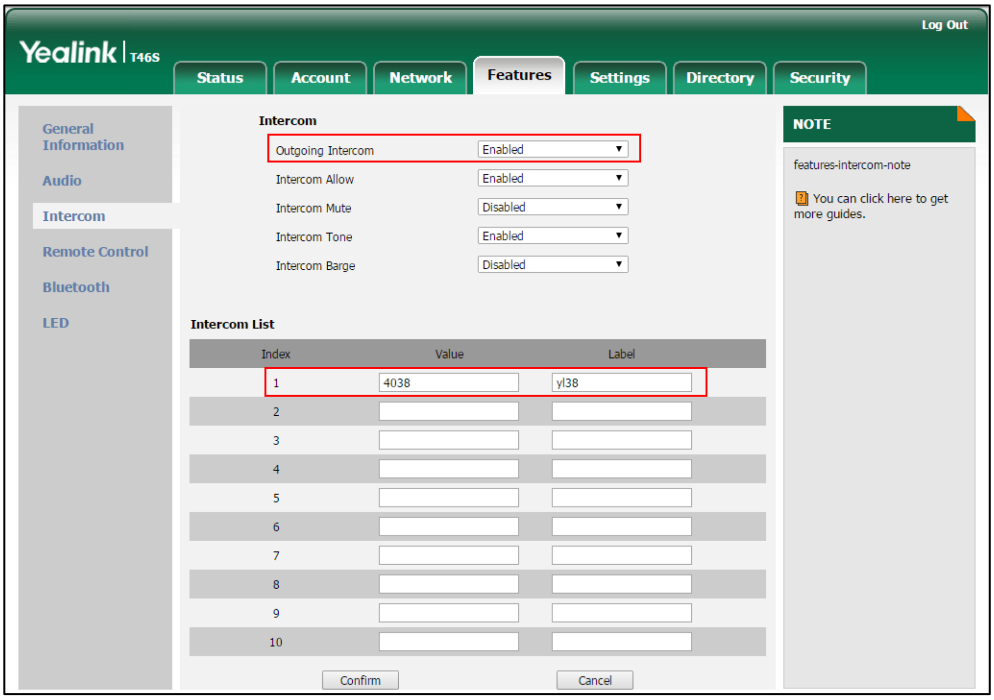
Parameters	Permitted Values	Default
features.intercom.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display intercom configurations. **0**-Disabled **1**-Enabled		

Parameters	Permitted Values	Default
Note: It is not applicable to CP960 Skype for Business phones. **Web User Interface:** None **Phone User Interface:** None		
features.intercom.outgoing	**0 or 1**	**0**
Description: Enables or disables the phone to place an outgoing intercom call from the intercom list. **0**-Disabled **1**-Enabled **Note**: It works only if the value of the parameter "features.intercom.enable" is set to 1 (Enabled). It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->Intercom->Outgoing Intercom **Phone User Interface:** Menu->Features->Intercom->Outgoing Intercom		
intercom.x.label (x ranges from 1 to 10)	**String**	**Blank**
Description: (Optional.) Configures the label displayed on the intercom list. **Note:** It works only if the values of parameters "features.intercom.enable" and "features.intercom.outgoing" are set to 1 (Enabled). **Example:** **intercom.1.label** = Test **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->Intercom->Label **Phone User Interface:** Menu->Features->Intercom List->Option->Edit->Label		
intercom.x.value (x ranges from 1 to 10)	**String**	**Blank**
Description: Configures the intercom number displayed on the intercom list.		

Parameters	Permitted Values	Default
Note: It works only if the values of parameters “features.intercom.enable” and “features.intercom.outgoing” are set to 1 (Enabled). **Example:** **intercom.1.value** = 4038 **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->Intercom->Value **Phone User Interface:** Menu->Features->Intercom List->Option->Edit->Value		

To configure outgoing intercom calls via web user interface:

1. Click on **Features**->**Intercom**.
2. Select the **Enabled** from the pull-down lists of **Outgoing Intercom**.
3. (Optional.) Enter the string that will appear on the intercom list in the **Label** field.
4. Enter the target extension number in the **Value** field.



5. Repeat steps 3 to 4, you can add more target extension numbers.
6. Click **Confirm** to accept the change.

To configure outgoing intercom via phone user interface:

1. Press **Menu**->**Features**->**Intercom**.
2. Press or , or the **Switch** soft key to **On** from the **Outgoing Intercom** fields.

3. Press the **Save** soft key to accept the change.

To configure the target extension number via phone user interface:

1. Do one of the following to enter the intercom list:

   - Press the Intercom key.

   - Press **Menu**->**Features**->**Intercom List**.

2. Press or to select a desired item.

   The default tag is Empty if it is not configured before.

3. Press the **Option** soft key, and then press the **Edit** soft key.

4. (Optional.) Enter the string that will appear on the intercom list in the **Label** field.

5. Enter the target extension number in the **Value** field.

6. Press the **Save** soft key to accept the change.

7. Repeat steps 2 to 6, you can add more target extension numbers.

Incoming Intercom Calls

The phone can process incoming calls differently depending on settings. There are four configuration options for incoming intercom calls:

Intercom Allow

Intercom Allow allows the phone to answer an incoming intercom call.

If you disable this feature, the phone will handle an incoming intercom call like a normal incoming call.

Intercom Mute

Intercom Mute allows the phone to mute the microphone for incoming intercom calls.

Intercom Tone

Intercom Tone allows the phone to play a warning tone before answering an intercom call.

Intercom Barge

Intercom Barge allows the phone to automatically answer an incoming intercom call while an active call is in progress. The active call will be placed on hold.

If you disable this feature, the phone will handle an incoming intercom call like a normal incoming call while there is already an active call on the phone.

Procedure

Incoming intercom calls can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure incoming intercom call feature. **Parameters:** features.intercom.allow features.intercom.mute features.intercom.tone features.intercom.barge
Web User Interface		Configure incoming intercom call feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-intercom&q=load
Phone User Interface		Configure incoming intercom call feature.

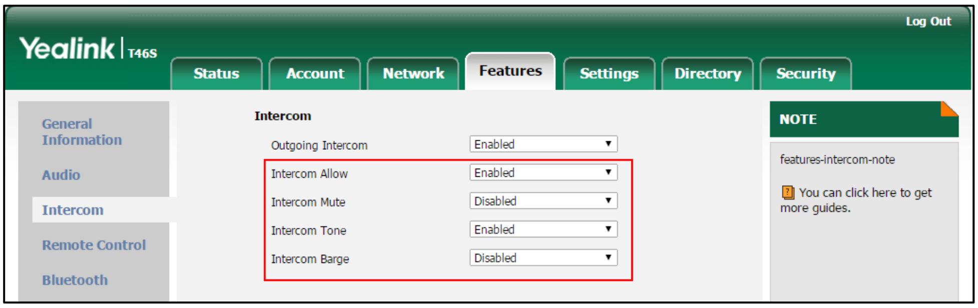
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.intercom.allow	**0 or 1**	**1**
Description: Enables or disables the phone to answer an incoming intercom call. **0**-Disabled, the phone will handle an incoming intercom call like a normal incoming call. **1**-Enabled, the phone will automatically answer an incoming intercom call. **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->Intercom->Intercom Allow **Phone User Interface:** Menu->Features->Intercom->Intercom Allow		
features.intercom.mute	**0 or 1**	**0**
Description: Enables or disables the phone to mute the microphone when answering an intercom call. **0**-Disabled **1**-Enabled, the microphone is muted for intercom calls, and then the other party cannot		

Parameters	Permitted Values	Default
hear you. **Note:** It works only if the value of the parameter "features.intercom.allow" is set to 1 (Enabled). It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->Intercom->Intercom Mute **Phone User Interface:** Menu->Features->Intercom->Intercom Mute		
features.intercom.tone	**0 or 1**	**1**
Description: Enables or disables the phone to play a warning tone when answering an intercom call. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "features.intercom.allow" is set to 1 (Enabled). It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->Intercom->Intercom Tone **Phone User Interface:** Menu->Features->Intercom->Intercom Tone		
features.intercom.barge	**0 or 1**	**0**
Description: Enables or disables the phone to answer an incoming intercom call while there is already an active call on the phone. **0**-Disabled, the phone will handle an incoming intercom call like a normal incoming call while there is already an active call on the phone. **1**-Enabled, the phone will automatically answer the intercom call while there is already an active call on the phone and place the active call on hold. **Note:** It works only if the values of parameters "features.intercom.allow" and "call_waiting.enable" are set to 1 (Enabled). It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->Intercom->Intercom Barge **Phone User Interface:** Menu->Features->Intercom->Intercom Barge		

To configure incoming intercom via web user interface:

1. Click on **Features**->**Intercom**.
2. Select the desired values from the pull-down lists of **Intercom Allow**, **Intercom Mute**, **Intercom Tone** and **Intercom Barge**.



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

To configure incoming intercom via phone user interface:

1. Press **Menu**->**Features**->**Intercom**.
2. Press or , or the **Switch** soft key to select the desired values from the **Intercom Allow**, **Intercom Mute**, **Intercom Tone** and **Intercom Barge** fields.
3. Press the **Save** soft key to accept the change.

USB Recording

Yealink phones support recording during a call. Before recording, ensure that the USB flash drive has been inserted into the USB port of the phone.

You need to press the **Start REC** soft key during a call to record the audio call or conference. USB recording is not applicable to CP960 Skype for Business phones.

Note

Before recording any call, especially those involving PSTN, it is necessary to know about the rules and restrictions of any governing call-recording in the place where you are. It is also very important to have the consent of the person you are calling before recording the conversation.

The recorded calls are saved in *.wav format and include a date/time stamp, other party's information (number, name or a conference call), duration of the call and the recording file size. For example, 20170920-1953-yl38 was created on Sep. 20, 2017, at 19:53 and you have a call with yl38. Recorded calls can be played on either the phone itself or on a computer using an application capable of playing *.wav files.

For more information, refer to *Yealink Skype for Business phone-specific user guide*.

Procedure

USB recording feature can be only configured using the configuration file.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the USB recording feature on a phone basis. **Parameter:** features.usb_call_recording.enable

Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.usb_call_recording.enable	**0 or 1**	**0**
Description: Enables or disables the the call recording (using a USB flash drive) feature for the phone. **0**-Disabled, disable audio call recording. **1**-Enabled, you can record the active audio call for the phone by pressing the **Start REC** soft key, and the recorded calls will be saved to the USB flash drive. **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** None **Phone User Interface:** None		

Voice Mail without PIN

Generally, users have to enter a PIN before they access the voice mail box. If voice mail without PIN feature is enabled, users can access voice mail box without entering PIN. It is especially useful for users who often access mailbox from the phone in a secure office.

Procedure

Voice mail without PIN can be configured using the configuration files.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure voice mail without PIN. **Parameters:** account.1.voice_mail.skip_pin.enable

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.1.voice_mail.skip_pin.enable	**0 or 1**	**1**
Description: Enables or disables the phone to access voice mail box without entering PIN. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		

Shared Line Appearance(SLA)

Shared Line Appearance is a feature in Skype for Business for handling multiple calls on a specific number called a shared number. The system administrator assigns members to a SLA group. When users call the shared number, the calls are not actually received on the shared number, instead they are forwarded to SLA groups members.

Any SLA group member can place, answer, hold, or resume calls on the lines, and all group members can view the status of a call on the shared line on their phones. Each line supports up to 25 call appearances. Only one call at a time can be active on the shared line appearance. If a call is placed to the shared line with an active call in place, the incoming call is sent to another shared line.

For information on creating a Shared Line Appearance in Skype for Business Server, refer to *Deploy Shared Line Appearance in Skype for Business Server 2015* on Microsoft TechNet.

Shared Line Appearance is not applicable to CP960 Skype for Business phones.

Note

A user can be assign to be one SLA group only. If the user has to be a delegate for multiple shared numbers, refer to Boss-Admin Feature on page 258 for more information.

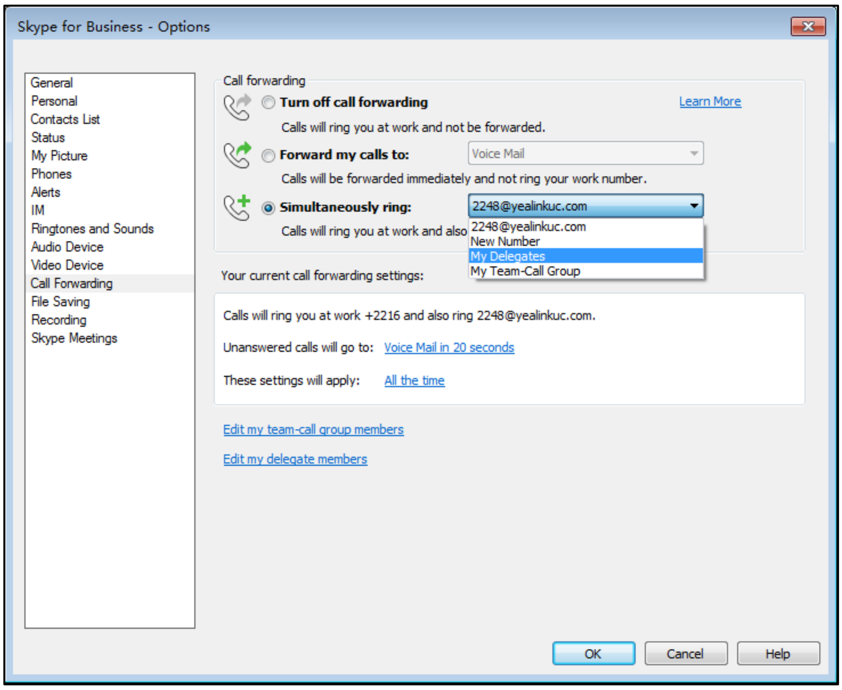
Boss-Admin Feature

When your phone is registered with Skype for Business server, you can use the Boss-Admin feature to manage shared lines. The boss-admin feature, which is also called boss-delegate feature, enables a "boss" phone and delegates' phones to ring simultaneously when a user calls the boss. When one party answers the call, the other phone will stop ringing. A boss can assign delegates and delegates can manage calls on behalf of the boss's line. For more information, refer to *Yealink Skype for Business phone-specific user guide*.

Assigning Delegates

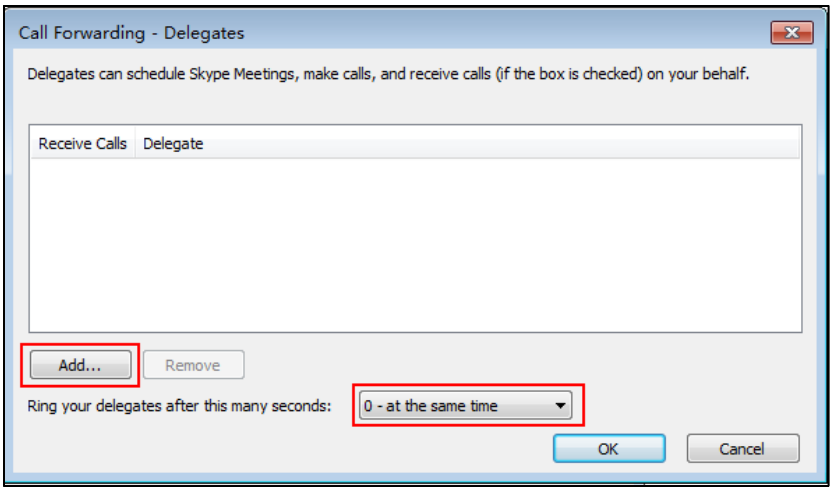
To assign delegates using Skype for Business client:

1. Open Skype for Business client.
2. Sign into Skype for Business client as the person who wants to assign a delegate.
3. Click the  button, and then click **Call Forwarding Settings**.
4. Mark the radio box in **Simultaneously ring** field.
5. Select **My Delegates** from the pull-down list of **Simultaneously ring**.



6. In the **Delegate**s dialog box, click **Add**. Each delegate must be a Skype for Business contact.

7. Click the **Ring your delegates after this many seconds** pull-down list to determine when your delegates' phones ring.



8. Click **OK**.
9. Click **OK** in the **Delegates** dialog box.
10. Click **OK** in the **Options** dialog box.

The boss's phone is able to accept the response (200 OK) to initial SUBSCRIBE and the response contains the current list of provisioned delegates and indication (in <flags>) that delegate ringing is currently enabled.

For example, when a user calls the boss (extension: 2227), the boss's line and his delegates (2216 and 2529) will ring simultaneously.

```
<flags name="clientflags" value="delegate_ring forward_audio_app_invites"></flags>
<list name=" delegates "><target uri="sip:2529@yealinkuc.com"></target><target
uri="sip:2216@yealinkuc.com"></target></list>
```

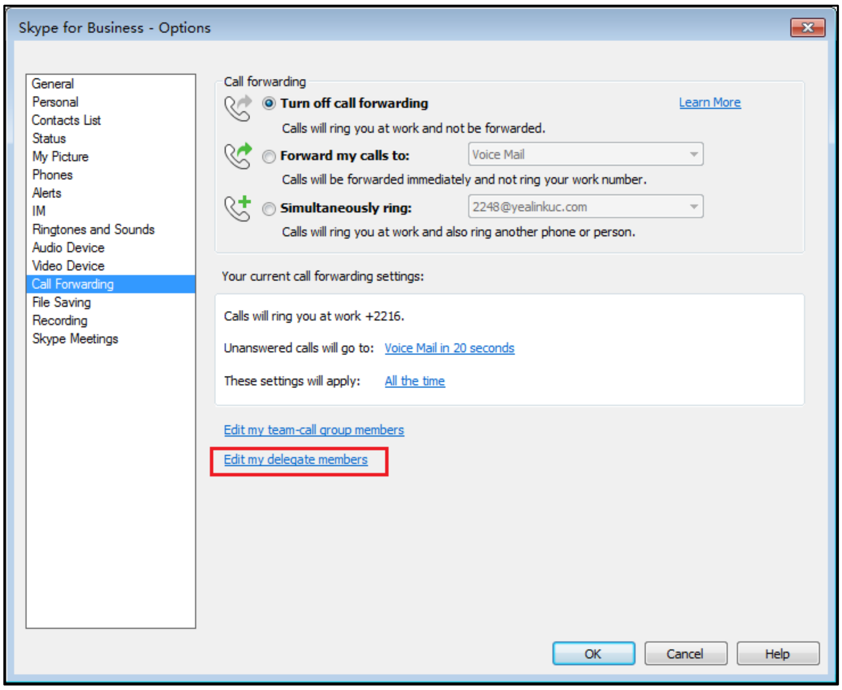
Removing Delegates

To remove a delegate from Skype for Business client:

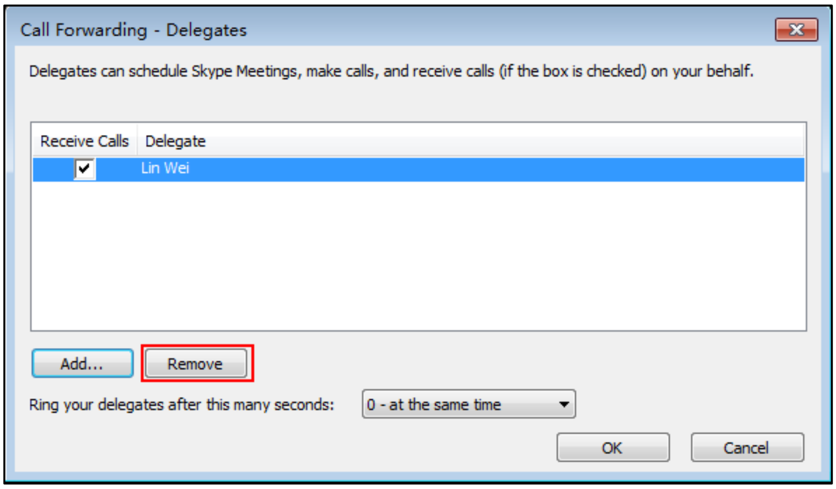
1. Open Skype for Business client.
2. Sign into Skype for Business client as the person who wants to remove a delegate.

   Make sure **My Delegates** option is not selected in either the **Simultaneously ring** or **Forward my calls to** list.

3. Click **Edit my delegate members**.



4. Check the checkbox of the delegate you want to remove.



5. Click **Remove**.
6. Click **OK** in the **Delegates** dialog box.
7. Click **OK** in the **Options** dialog box.

For example, if the boss removes the delegate whose extension is 2216, then the phone is able to accept a Notification of modified delegate list and the NOTIFY contains a list of current provisioned delegate:

```
<list name="delegates"><target uri="sip:2529@yealinkuc.com"></target>
```

Boss-Line Ringtone

As a delegate, you can set a distinct ringtone for your assigned bosses' lines. When you receive incoming calls from your assigned bosses or your assigned bosses receive incoming calls, your phone will play this ringtone. Boss-line ringtone is not applicable to CP960 Skype for Business phones.

Procedure

Boss-line ringtone can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure a distinct ringtone for assigned bosses' lines. **Parameter:** phone_setting.boss_line_ring.enable
Local	Phone User Interface	Configure a distinct ringtone for assigned bosses' lines.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.boss_line_ring.enable	**0 or 1**	**1**
Description: Enables or disables the delegate to set a distinct ringtone for assigned bosses' lines. **0**-Disabled, ringtone for assigned bosses' lines will use the phone's ringtone. The phone's ringtone is configured by the parameter "phone_setting.ring_type". **1**-Enabled, the delegate can set a distinct ringtone for assigned bosses' lines. When delegate receives incoming calls from assigned bosses or assigned bosses receive incoming calls, delegate's phone will play the distinct ringtone. **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** None **Phone User Interface:** None		

To set a ringtone for assigned bosses' lines via phone user interface:

1. Press **Menu**->**Basic**->**Sounds**->**Ring Tones**->**Boss**.
2. Press or to select a boss.
3. Press or to select a ring tone.
4. Press the **Save** soft key to accept the change.

Delegates-call Ringtone

As a boss, you can set a distinct ringtone for incoming calls from your assigned delegates' lines. It is not applicable to CP960 Skype for Business phones.

Procedure

Delegates-call ringtone can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure a distinct ringtone for incoming calls from the assigned delegates' lines. **Parameter:** phone_setting.delegates_call_ring.enable
Local	Phone User Interface	Configure a distinct ringtone for incoming calls from the assigned delegates' lines.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.delegates_call_ring.enable	**0 or 1**	**1**
Description: Enables or disables the boss to set a distinct ringtone for incoming calls from the assigned delegates' lines. **0**-Disabled, incoming calls from the assigned delegates' lines will use the phone’s ringtone. The phone's ringtone is configured by the parameter "phone_setting.ring_type". **1**-Enabled, the boss can set a distinct ringtone for incoming calls from the assigned delegates' lines. **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** None **Phone User Interface:** None		

To set a ringtone for the assigned delegates' lines via phone user interface:

1. Press **Menu**->**Basic**->**Sounds**->**Ring Tones**->**Delegate call**.
2. Press or to select a delegate.
3. Press or to select a ring tone.
4. Press the **Save** soft key to accept the change.

Calendar

Yealink Skype for Business phones integrates with the Microsoft Exchange calendar feature. If your phone is configured to connect to the Microsoft Exchange Server, and the Microsoft® Outlook® application is installed at your site, you can view Skype conference, appointment, meeting and event, or join the Skype conference from your phone.

For more information on how to set up a Skype conference, appointment, meeting and event via the Microsoft Exchange Server, refer to *Yealink Skype for Business phone-specific user guide*.

To use the calendar feature on your phone, you must sign into the phone using User Sign-in or Web Sign-in or Sign in via PC method. So the phones can display the Microsoft Exchange calendar which gives you quick access to Skype conference, appointment, meeting and event.

Procedure

Calendar can be configured using the configuration files only.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure calendar feature. **Parameters:** sfb.calendar.enable
		Configure the meeting reminder. **Parameters:** phone_setting.calendar_reminder
		Configure the interval of meeting reminder. **Parameters:** phone_setting.calendar_reminder.interval
		Configures the interval (in seconds) for the phone to automatically check if any calendars update available on Microsoft Exchange Server. **Parameters:** phone_setting.calendar.update_time
		Configure the calendar to dispaly all schedules. **Parameters:** phone_setting.calendar_view_all.enable
		Configure the time to display the next meeting before it begins. **Parameters:**

		phone_setting.calendar_home.start_time
		Configure the information to be displayed on the private meeting. **Parameters:** phone_setting.calendar_private_attendees.enable phone_setting.calendar_private_content.enable phone_setting.calendar_private_location.enable phone_setting.calendar_private_subject.enable phone_setting.calendar_private_organizer.enable
		Configure the information to be displayed on the public meeting. **Parameters:** phone_setting.calendar_public_attendees.enable phone_setting.calendar_public_content.enable phone_setting.calendar_public_location.enable phone_setting.calendar_public_subject.enable phone_setting.calendar_public_organizer.enable

Details of Configuration Parameters:

Parameters	Permitted Values	Default
sfb.calendar.enable	**0 or 1**	**1**
Description: Enables or disables the calendar feature. **0**-Disabled, user cannot use calendar feature on the phone. **1**-Enabled, user can use calendar feature on the phone. **Web User Interface:**		

Parameters	Permitted Values	Default
None **Phone User Interface:** None		
phone_setting.calendar_reminder	**0 or 1**	**1(T42S/T42S/T46S/ T48S);** **0(CP960)**
Description: Enables or disables the meeting reminder. **0**-Disabled, the phone will not display reminders for any meeting. **1**-Enabled, the phone will display reminders for all meetings. **Web User Interface:** None **Phone User Interface:** Menu->Basic->Calendar Settings->Reminder		
phone_setting.calendar_reminder.interval	**Integer from 1 to 15**	**5**
Description: Configures the interval (in minutes) for the phone to display the next meeting reminder after you temporarily remove the reminder. **Note:** It works only if the value of the parameter "phone_setting.calendar_reminder" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** Menu->Basic->Calendar Settings->Reminder Interval		
phone_setting.calendar.update_time	**Integer from 0 to 1000**	**300**
Description: Configures the interval (in seconds) for the phone to automatically check if any calendars update available on Microsoft Exchange Server. If it is set to 300 (in seconds), the phone will check if any calendar update available on the Microsoft Exchange Server every 300 seconds. If an update is available, the phone will download the calendars. **Note:** This configuration will take effect after a reboot.		

Parameters	Permitted Values	Default
Web User Interface: None **Phone User Interface:** None		
phone_setting.calendar_view_all.enable	**0 or 1**	**0**
Description: Enables or disables the calendar to display all schedules. **0**-Disabled, the phone will display the schedules of today only. **1**-Enabled, the phone will display all schedules. **Web User Interface:** None **Phone User Interface:** None		
phone_setting.calendar_home.start_time	**Integer from 30 to 360**	**30**
Description: Configures the time (in minutes) to display the next meeting before it begins. **Web User Interface:** None **Phone User Interface:** None		
phone_setting.calendar_private_attendees.enable **phone_setting.calendar_private_content.enable** **phone_setting.calendar_private_location.enable** **phone_setting.calendar_private_subject.enable**	**0 or 1**	**0**
phone_setting.calendar_private_organizer.enable		**1**
Description: Enables or disables the phone to display conference attendees, content, location, subject or organizer of the private meeting when receiving the reminder. **0**-Disabled **1**-Enabled **Note:** It is not applicable to T48S/T46S/T42S/T41S Skype for Business phones. You can set		

Parameters	Permitted Values	Default
up a private meeting in Outlook. **Web User Interface:** None **Phone User Interface:** None		
phone_setting.calendar_public_attendees.enable **phone_setting.calendar_public_content.enable** **phone_setting.calendar_public_location.enable** **phone_setting.calendar_public_subject.enable** **phone_setting.calendar_public_organizer.enable**	**0 or 1**	**1**
Description: Enables or disables the phone to display conference attendees, content, location, subject or organizer of the public meeting when receiving the reminder. **0**-Disabled **1**-Enabled, the phone will display conference attendees, content, location, subject or organize. **Web User Interface:** None **Phone User Interface:** None		

To configure the reminder interval via phone user interface:

1. Press **Menu**->**Basic**->**Calendar Settings**.
2. Press , or the **Switch** soft key to select **Enabled** in the **Reminder** field.
3. Enter the interval in the **Reminder Interval** field.

   The interval is 5 minutes by default.

BToE

Better Together over Ethernet (BToE) feature on Yealink Skype for Business phones enables you to control call activity from your phones and your computer using your Skype for Business client. You can also use BToE to sign into your phone using your Skype for Business credentials. In order to use BToE, you need to download and install the Yealink BToE Connector application.

It is not applicable to CP960 Skype for Business phones.

Procedure

BToE can be configured using the configuration files.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure BToE feature. **Parameters:** sip.btoe.enable features.sign_in_via_btoe.enable
		Configures the BToE pairing mode. **Parameters:** sip.btoe.pairing_mode
Local	Web User Interface	Configure BToE feature. Configures the BToE pairing mode. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-btoe&q=load
	Phone User Interface	Configure BToE feature. Configures the BToE pairing mode.

Details of Configuration Parameters:

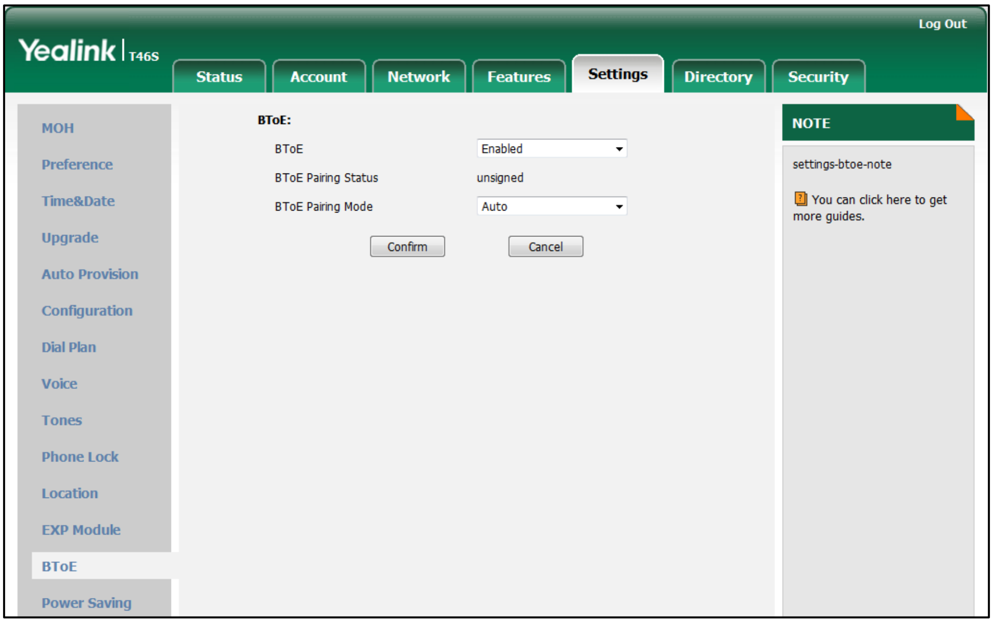
Parameters	Permitted Values	Default
sip.btoe.enable	**0 or 1**	**1**
Description: Enables or disables the BToE (Better Together over Ethernet) feature. **0**-Disabled, BToE is disabled on the phone. Your phone cannot pair with Skype for Business Client. **1**-Enabled), BToE is enabled on the phone. Your phone can pair with Skype for Business Client. **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Settings->BToE->BToE **Phone User Interface:** Menu->Features->BToE->BToE		
features.sign_in_via_btoe.enable	**0 or 1**	**1**
Description:		

Parameters	Permitted Values	Default
Enables or disables the user to sign into the phone via PC. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter “sip.btoe.enable” is set to 1 (Enabled). If it is set to 1 (Enabled), make sure your phone has paired with the Skype for Business client using BToE software, so that you can sign into the phone via PC. It is not applicable to CP960 Skype for Business phones. **Web User Interface:** None **Phone User Interface:** None		
sip.btoe.pairing_mode	**0 or 1**	**0**
Description: Configures the BToE pairing mode. **0**-Auto, you can pair your phone and PC automatically without a pairing code. **1**-Maunal, your phone will generate a pairing code when pairing with Skype for Business client. You need to enter the pairing code on your BToE software to manually to pair your phone and Skype for Business client. **Note:** It works only if the value of the parameter “sip.btoe.enable” is set to 1 (Enabled). It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Settings->BToE->BToE paring Mode **Phone User Interface:** Menu->Features->BToE->BToE Pairing Mode		

To configure BToE feature via web user interface:

1. Click on **Settings**->**BToE**.
2. Select the desired value from the pull-down list of **BToE**.

3. Select the desired generation from the pull-down list of **BToE Pairing Mode**.



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

To configure BToE feature via phone user interface:

1. Press **Menu**-> **Features**->**BToE**.
2. Press or , or the **Switch** soft key to select **Enabled** from the **BToE** field.
3. Press or , or the **Switch** soft key to select the desired pairing mode from the **BToE Pairing Mode** field.

   The default value is **Auto**.

4. Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

To use the BToE feature and sign in:

1. Download and install the Yealink BToE Connector application to your computer.
2. Sign into the Skype for Business client.
3. Enable BToE and pair your phone with your computer. For more information on how to pair, refer to *Better Together over Ethernet* chapter in *Yealink Skype for Business phone-specific user guide*.

When no user signs into the phone, a logon dialog will pop up on the Skype for Business client on your computer to prompt you to enter the password.

4. Enter your password and sign in.

   Now you will sign into your phone with the same account on your client. You can manage calls on your phone using the Skype for Business client.

EXP40 Expansion Module

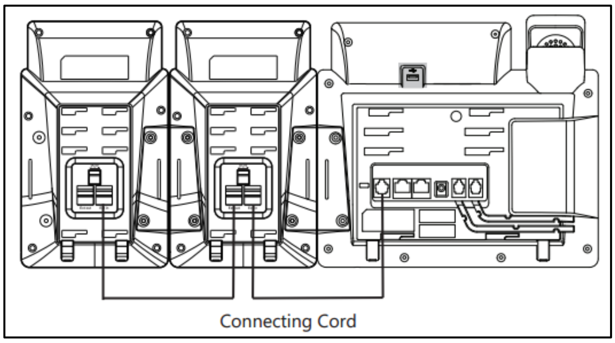
The Yealink EXP40 expansion module is an ideal choice for receptionists, administrative assistants, call center agents, power-users, and executives who need to handle large call volumes on a daily basis.

Assigning Contacts to EXP40

You can connect an EXP40 expansion module to T48S/T46S Skype for Business phones only. When your T48S/T46S is registered with a Skype for Business account, you can assign contacts to EXP keys on your EXP40 expansion module, so that you can quickly call contact by pressing the corresponding EXP key.

You can also monitor your Skype for Business contacts' presence status from your expansion module.

To use EXP40 expansion modules, connect the Ext jack of the phone and the Ext in jack of the expansion module using one supplied cord. If you need to connect multiple expansion modules, connect the Ext out jack of the previous expansion module and the Ext in jack of the next expansion module using another supplied cord.



Each EXP40 expansion module provides you with 20 EXP keys and 2 display pages, supporting a total of 40 EXP keys that you can set up as contacts. You can connect up to 6 EXP40 expansion modules to your phone to support a maximum of 240 EXP keys per phone.

Procedure

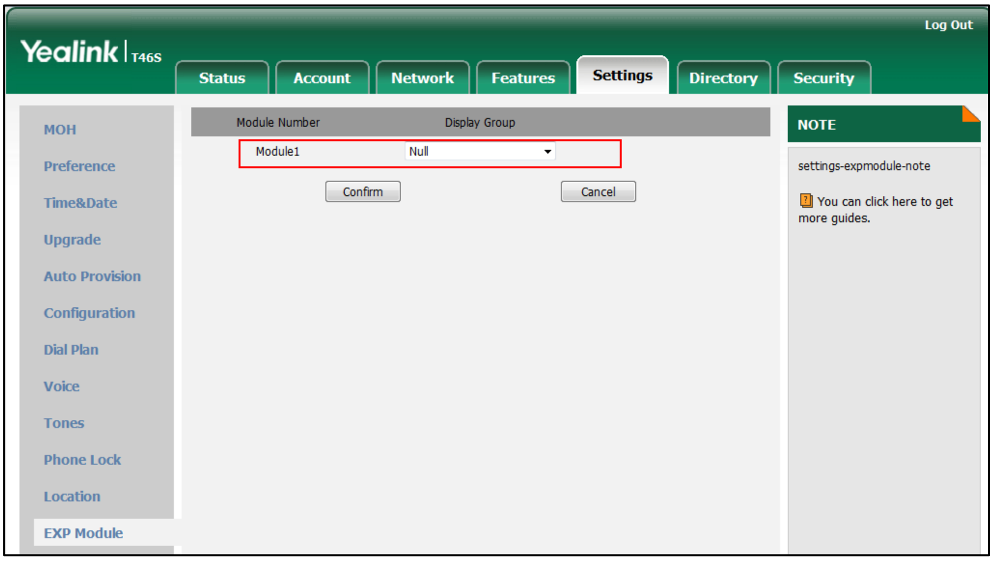
EXP40 expansion module can be configured locally.

Locally	Web User Interface	Configure the desired contact group to be displayed on the EXP40 expansion

		module. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-expmodule&q=load
	Phone user Interface	Configure the desired contact group to be displayed on the EXP40 expansion module.

To assign contact group to the EXP40 expansion module via web user interface:

1. Click on **Settings**->**EXP Module**.
2. Select the desired contact group from the pull-down list of **ModuleX** (X ranges from 1 to 6 depending on the amount of the connected EXP40).



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

   The selected contact group will be displayed on the selected expansion module.

To assign contact group to the EXP40 expansion module via phone user interface:

1. Press **Menu**->**Basic**->**Exp Module**.
2. Press or , or the **Switch** soft key to select the desired contact group from the **ModuleX** field (X ranges from 1 to 6 depending on the amount of the connected EXP40).
3. Press the **Save** soft key to accept the change.

   The selected contact group will be displayed on the selected expansion module.

Monitoring Status Changes using EXP Key LED Indicator

EXP40 can display local contacts or Skype for Business contacts, but you can only use EXP40 to monitor Skype for Business contacts for status changes. For example, you can assign a Skype for Business contact to the EXP40 to monitor the status of his line (busy or idle). The EXP key

LED indicator illuminates solid red when his line is busy.

Procedure

EXP key LED indicator can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the EXP key LED indicator. **Parameter:** phone_setting.exp40_led.enable
Local	Web User Interface	Configure the EXP key LED indicator. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-powerled&q=load

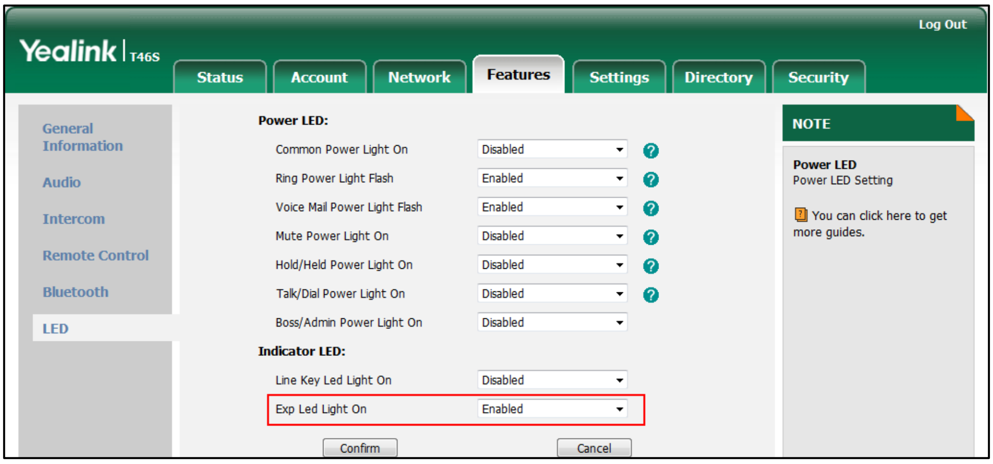
Details of Configuration Parameters:

Parameter	Permitted Values	Default
phone_setting.exp40_led.enable	**0 or 1**	**1**
Description: Enables or disables the EXP key LED indicator on the expansion module to monitor the status of the Skype for Business contacts. **0**-Disabled, the EXP key LED indicators corresponding to your Skype for Business contacts are off. **1**-Enabled, the EXP key LED indicators vary depending on the status of your Skype for Business contacts. **Note:** It is only applicable to T48S/T46S Skype for Business phones. **Web User Interface:** Features->LED->Exp Led Light On **Phone User Interface:** None		

To configure the EXP key LED indicators via web user interface:

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

2. Select the desired value from the pull-down list of **Exp Led Light On**.



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

The EXP key LED indicators on the EXP40 expansion module:

LED Status	Description
Solid green	The Skype for Business contact is available.
Solid red	The Skype for Business contact is busy. The Skype for Business contact is Do Not Disturb. The call of your Skype for Business contact is parked. The call of your Skype for Business contact is placed on hold. The held call of your Skype for Business contact is resumed. The Skype for Business contact is in a Skype for Business conference.
Solid yellow	The Skype for Business contact is right back. The Skype for Business contact is off work. The Skype for Business contact is away.
Stay the original LED status	The Skype for Business contact is placing a call. The Skype for Business contact is receiving a call. The parked call of your Skype for Business contact is retrieved.
Off	The Skype for Business contact is unknown. The Skype for Business contact is offline. Your phone is locked.

Configuring Advanced Features

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

- E911
- Multicast Paging
- Hot Desking
- Common Area Phone
- Branch Office Resiliency
- Action URI
- Quality of Experience

E911

E911 (Enhanced 911) is a location technology that enables the called party to identify the geographical location of the calling party. For example, if a caller makes an emergency call to E911, the feature extracts the caller's information for the police department to immediately identify the caller's location. For more information, refer to *https://technet.microsoft.com/en-us/library/dn951423.aspx*.

System administrator can configure multiple emergency numbers via the Skype for Business Server.

The phone sends the following attributes to LIS to get back the location information:

1. MAC address
2. IP address
3. Subnet
4. SIP URI
5. Chassis ID / Port ID of L2 switch (This information is obtained using LLDP)

During in-band provisioning, the following have been sent from the Frontend server to the phone.

1. LIS URI
2. Enhanced Emergency Enabled
3. Location Required
4. Emergency Dial String
5. Emergency Dial String Mask
6. Secondary Location Source
7. Notify URI

8. Conf URI
9. Conf Mode

Sample:

```
ms-subnet: 192.168.1.0.
<provisionGroup name="locationPolicy" >
<propertyEntryList >
<property name="EnhancedEmergencyServicesEnabled" >true</property>
<property name="LocationPolicyTagID" >user-tagid</property>
<property name="LocationRequired" >yes</property>
<property name="UseLocationForE911Only" >true</property>
<property name="EmergencyDialString" >910086</property>
<property name="EmergencyDialMask" >911;912</property>
<property
name="NotificationUri" >sip:7000@yealinkuc.com,sip:80040@yealinkuc.com</property>
<property name="ConferenceMode" >oneway</property>
```

When user dials an emergency number, the location of the user set in phone and the phone number are sent out as a part of INVITE message.

Sample:

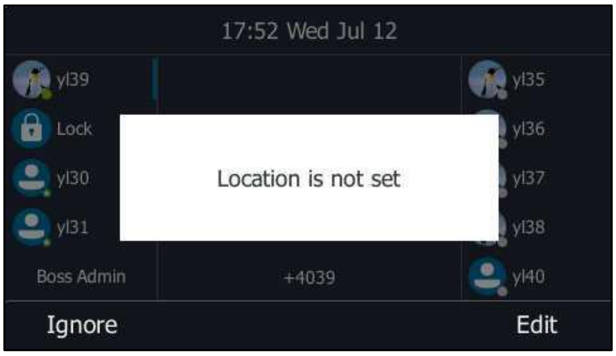
```
INVITE sip:+119@bor-ee.com;user=phone SIP/2.0
<location-info>
        <civicAddress xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
            <PC>361008</PC>
            <country>CN</country>
            <STS />
            <PRD />
            <HNS />
            <POD />
            <HNO />
            <RD>Wanghailu</RD>
            <A3>Xiamen</A3>
            <A1>Fujian</A1>
            <NAM />
            <LOC>63</LOC>
        </civicAddress>
    </location-info>
```

Note If user's presence status is DND before dialing an emergency number, it will reset to Available from DND when a 911 number is dialed.

E911 Location Tip

The network administrator configures geographical location on Skype for Business Server for users. After user signs in, the geographical location is downloaded via in-band provisioning.

If geographical location is not provisioned by the server and the LocationRequired property of in-band LocationPolicy is set to 'yes' or 'disclaimer' on the Skype for Business Server, a popup opens in the phone's LCD screen/touch screen enabling users to either ignore the notification or edit the location information.



Procedure

E911 location tip can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure E911 location tip. **Parameters:** sfb.E911_location_tip
Local	Web User Interface	Configure E911 location tip. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

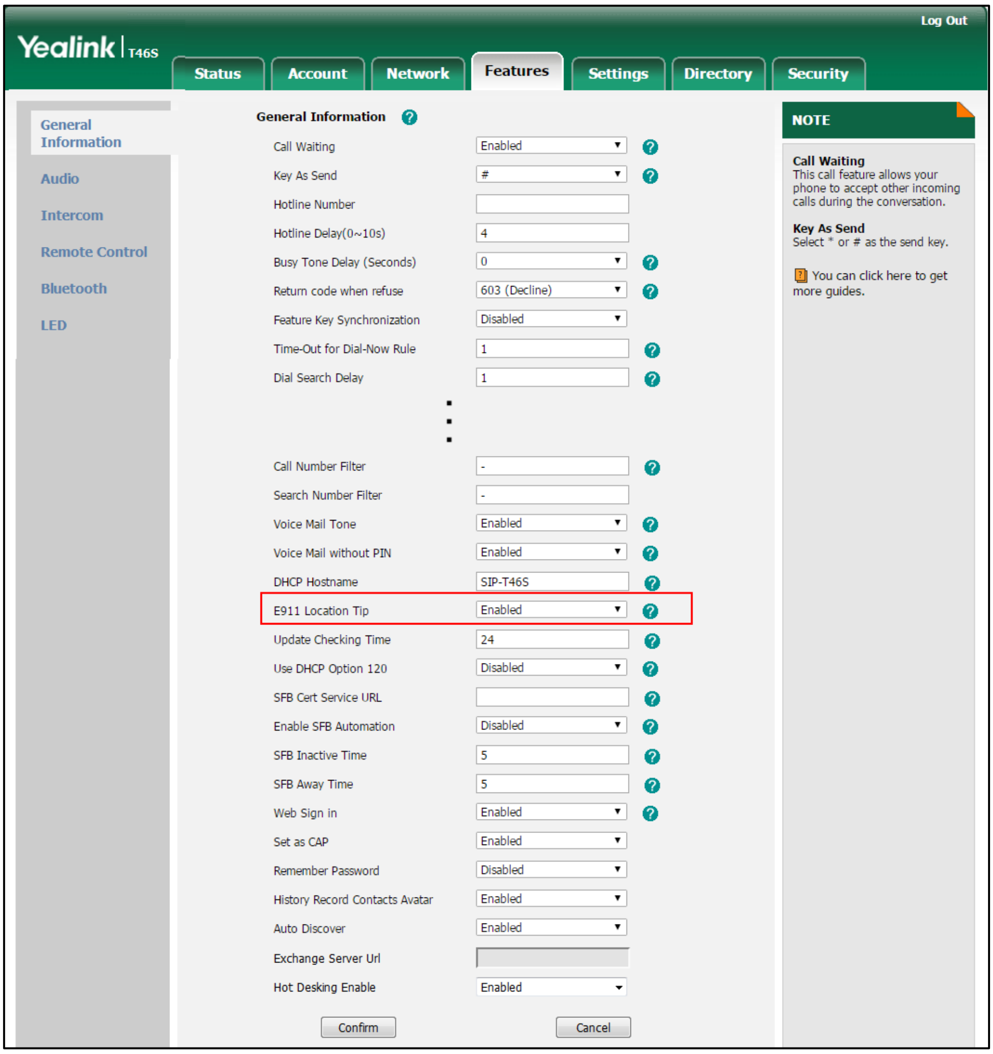
Details of Configuration Parameters:

Parameters	Permitted Values	Default
sfb.E911_location_tip	**0 or 1**	**1**

Parameters	Permitted Values	Default
Description: Enables or disables the idle screen to display the notification “Location is not set” when the location of the phone is not set. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->E911 Location Tip **Phone User Interface:** None		

To configure E911 location tip via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **E911 Location Tip**.



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

Adding the Location Information

If the location is not set on the Skype for Business Server, users can also add the location information manually via web user interface or phone user interface.

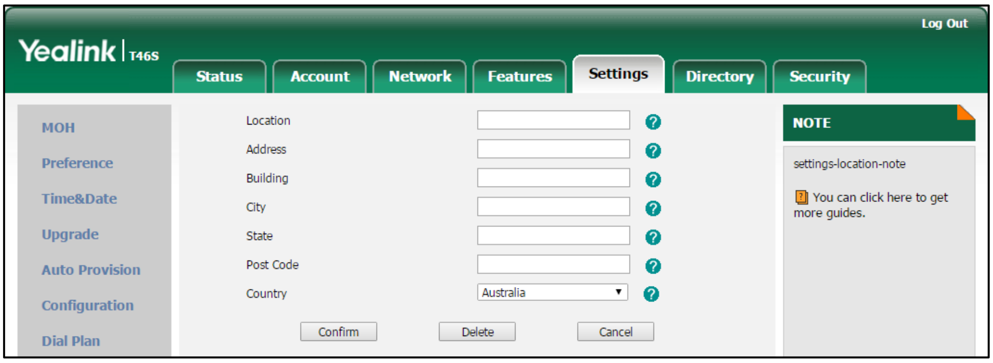
Procedure

Location information can be configured locally.

Local	Web User Interface	Configure the location information. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-location&q=load
	Phone User Interface	Configure the location information.

To add the location information manually via web user interface:

1. Click on **Settings**->**Location**.
2. Enter the location name in the **Location** field.
3. Enter the address name in the **Address** field.
4. Enter the building name in the **Building** field.
5. Enter the city name in the **City** field.
6. Enter the state name in the **State** field.
7. Enter the postcode in the **Post Code** field.
8. Select the desired country from the pull-down list of **Country**.



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

To add the location information manually via phone user interface:

1. Press **Menu**->**Basic**->**Location**.

2. Press the **Edit** soft key.
3. Enter the location name in the **Set Location** field.
4. Enter the address name in the **Set Address** field.
5. Enter the building name in the **Set Building** field.
6. Enter the city name in the **Set City** field.
7. Enter the state name in the **Set State** field.
8. Enter the postcode in the **Set Postcode** field.
9. Press or , or the **Switch** soft key to select the country from the **Set Country** field.
10. Press the **Save** soft key to accept the change.

Location is configurable via web user interface at the path **Settings**->**Location**.

Multicast Paging

Multicast paging allows the phone to send/receive Real-time Transport Protocol (RTP) streams to/from the pre-configured multicast address(es) without involving SIP signaling. Up to 10 listening multicast addresses can be specified on the phone.

Multicast paging is not applicable to CP960 Skype for Business phones.

Sending RTP Stream

Users can send an RTP stream without involving SIP signaling by pressing a **Paging** soft key. A multicast address (IP: Port) should be assigned to the multicast paging key, which is defined to transmit RTP stream to a group of designated phones. When the phone sends the RTP stream to a pre-configured multicast address, each phone preconfigured to listen to the multicast address 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 configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify a multicast codec for the 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
Local	Web User Interface	Specify a multicast codec for the phone to send the RTP stream. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
		Configure the multicast IP address and port number for a paging list key. Configure the multicast paging group name for a paging list key. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-multicastIP&q=load
	Phone User Interface	Configure the multicast IP address and port number for a paging list key. Configure the multicast paging group name for a paging list key.

Details of the Configuration Parameter:

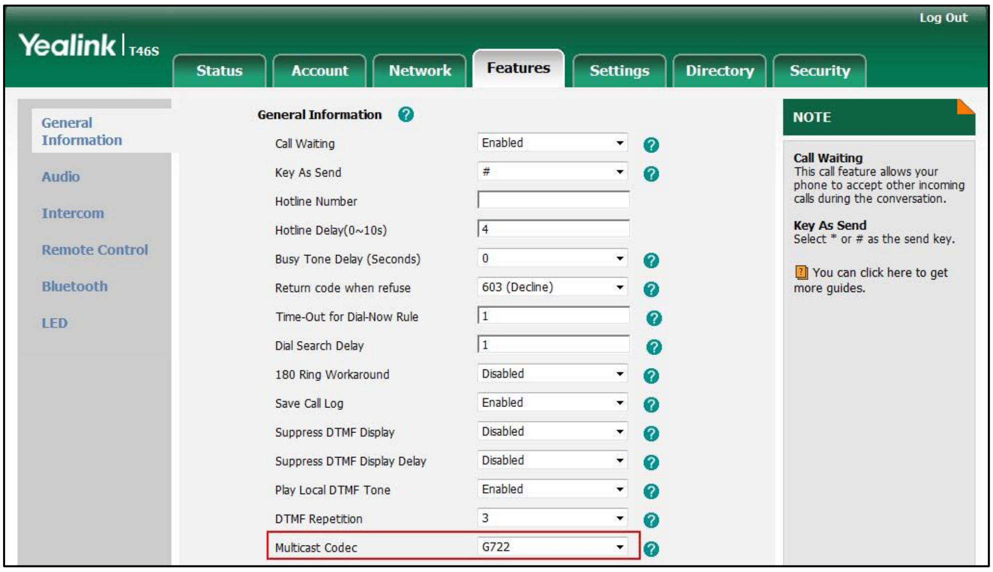
Parameters	Permitted Values	Default
multicast.codec	**PCMU, PCMA, G729, G722**	**G722**
Description: Configures the codec of multicast paging. **Example:** multicast.codec = G722 **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->General Information->Multicast Codec **Phone User Interface:** None		
multicast.paging_address.X.ip_address (X ranges from 1 to 10)	**String**	**Blank**

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">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/touch screen when placing the multicast paging call.
Example:
multicast.paging_address.1.ip_address = 224.5.6.20:10008
multicast.paging_address.2.ip_address = 224.1.6.25:1001
Note: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255. It is not applicable to CP960 Skype for Business phones.
Web User Interface:
Directory->Multicast IP->Paging List->Paging Address
Phone User Interface:
Menu->Features->Paging List->Option->Edit->Address</td></tr>
<tr><td>multicast.paging_address.X.label
(X ranges from 1 to 10)</td><td>String</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the name of the multicast paging group to be displayed in the paging list.
It will be displayed on the LCD screen/touch screen when placing the multicast paging calls.
Example:
multicast.paging_address.1.label = Product
multicast.paging_address.2.label = Sales
Note: It is not applicable to CP960 Skype for Business phones.
Web User Interface:
Directory->Multicast IP->Paging List->Label
Phone User Interface:
Menu->Features->Paging List->Option->Edit->Label</td></tr>
</table>

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.

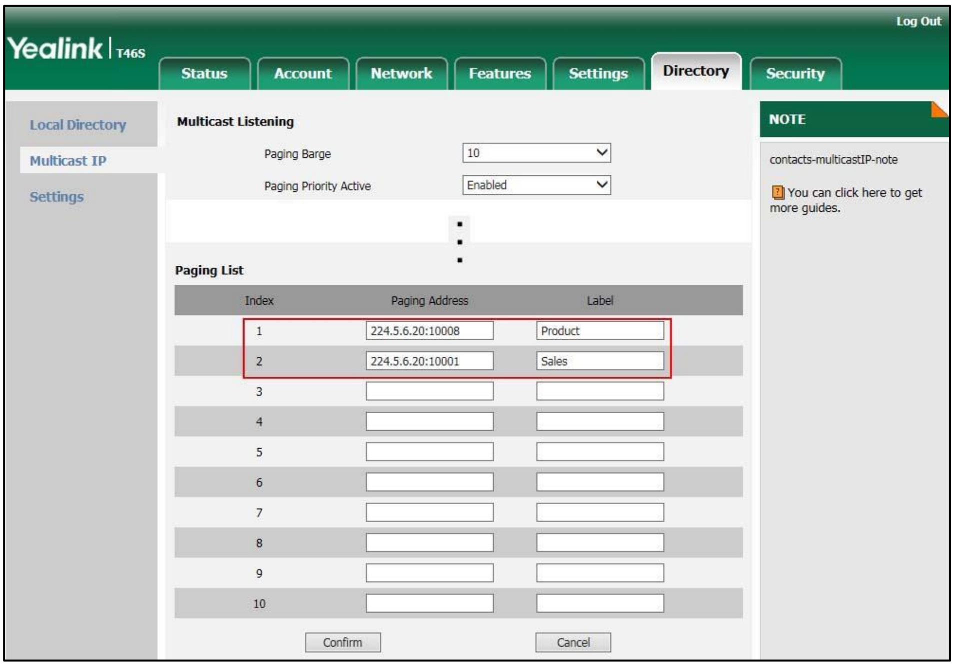
To configure two sending multicast addresses via web user interface:

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/touch screen when sending the RTP multicast.



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

To configure paging list via phone user interface:

1. Press **Menu**->**Features**->**Paging List**.

2. Press or to select a desired paging group.
3. The default tag is Empty if it is not configured before.
4. Press the **Option** soft key, and then press the **Edit** soft key.
5. Enter the multicast IP address and port number (e.g., 224.5.6.20:10008) in the **Address** field.
6. The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.
7. Enter the group name in the **Label** field.
8. Press the **Save** soft key to accept the change.
9. Repeat steps 2 to 6, you can add more paging groups.

   For T46S/T42S/T41S Skype for Business phones, the second line key will change to be a Paging key automatically. When the phone is idle, you can press the Paging key to access the paging list.

   For T48S Skype for Business phones, an icon appears on the screen title area. You can tap it or tap **Menu**->**Features**->**Paging list** to access the paging list.

Receiving RTP Stream

Skype for Business phones can receive an RTP stream from the pre-configured multicast address(es) without involving SIP signaling, and can handle the incoming multicast paging calls differently depending on the configurations of Paging Barge and Paging Priority Active.

Paging Barge

This parameter defines the priority of the voice call in progress, and decides how the phone handles the incoming multicast paging calls when there is already a voice call in progress. If the value of the parameter is configured as disabled, all incoming multicast paging calls will be automatically ignored. If the value of the parameter is the priority value, the incoming multicast paging calls with higher or equal priority are automatically answered and the ones with lower priority are ignored.

Paging Priority Active

This parameter decides how the phone handles the incoming multicast paging calls when there is already a multicast paging call in progress. If the value of the parameter is configured as disabled, the phone will automatically ignore all incoming multicast paging calls. If the value of the parameter is configured as enabled, an incoming multicast paging call with higher priority or equal is automatically answered, and the one with lower priority is ignored.

Procedure

Configuration changes can be performed using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the listening multicast address. **Parameters:** multicast.listen_address.X.ip_address multicast.listen_address.X.label
		Configure Paging Barge and Paging Priority Active features. **Parameters:** multicast.receive_priority.enable multicast.receive_priority.priority
Local	Web User Interface	Configure the listening multicast address. Configure Paging Barge and Paging Priority Active features. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-multicastIP&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
multicast.listen_address.X.ip_address (X ranges from 1 to 10)	**IP address: port**	**Blank**
Description: Configures the multicast address and port number that the 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. It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Directory->Multicast IP->Multicast Listening->Listening Address **Phone User Interface:** None		
multicast.listen_address.X.label (X ranges from 1 to 10)	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label to be displayed on the LCD screen/touch screen when receiving the multicast paging calls.		

Parameters	Permitted Values	Default
Example: multicast.listen_address.1.label = Paging1 **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Directory->Multicast IP->Multicast Listening->Label **Phone User Interface:** None		
multicast.receive_priority.enable	**0 or 1**	**1**
Description: Enables or disables the phone to handle the incoming multicast paging calls when there is an active multicast paging call on the phone. **0**-Disabled, the phone will ignore the incoming multicast paging calls when there is an active multicast paging call on the phone. **1**-Enabled, the phone will receive the incoming multicast paging call with a higher or equal priority and ignore that with a lower priority. **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Directory->Multicast IP->Paging Priority Active **Phone User Interface:** None		
multicast.receive_priority.priority	**Integer from 0 to 10**	**10**
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, 10 is the lowest priority. **0**-Disabled, all incoming multicast paging calls will be automatically ignored when a voice call is in progress. **1**-1 **2**-2 **3**-3 **4**-4 **5**-5 **6**-6		

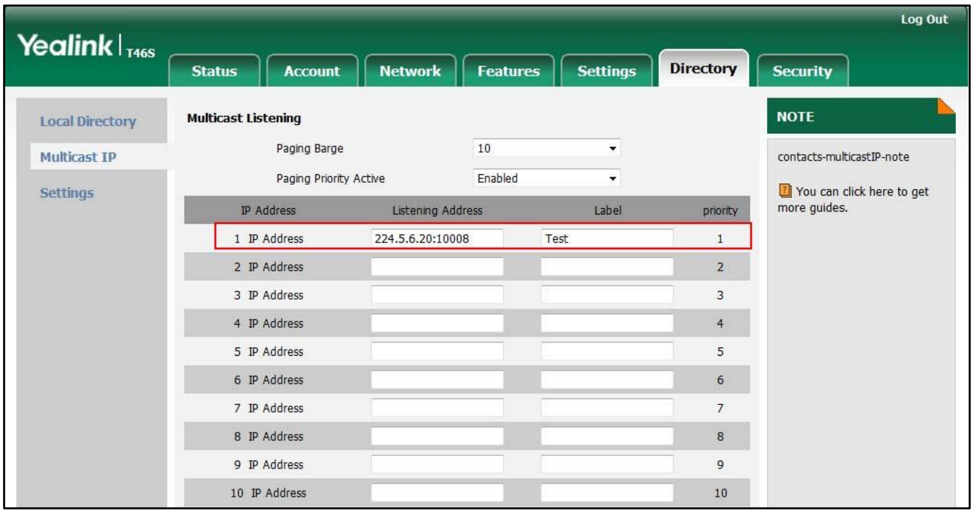
Parameters	Permitted Values	Default
7-7 **8**-8 **9**-9 **10**-10 If it is set to other values, the phone will receive the incoming multicast paging call with a higher or equal priority and ignore that with a lower priority when a voice call is in progress. **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Directory->Multicast IP->Paging Barge **Phone User Interface:** None		

To configure a listening multicast address via web user interface:

1. Click on **Directory**->**Multicast IP**.
2. Enter the listening multicast address and port number in the **Listening Address** field.

   1 is the highest priority and 10 is the lowest priority.
3. Enter the label in the **Label** field.

   The label will appear on the LCD screen/touch screen when receiving the RTP multicast.

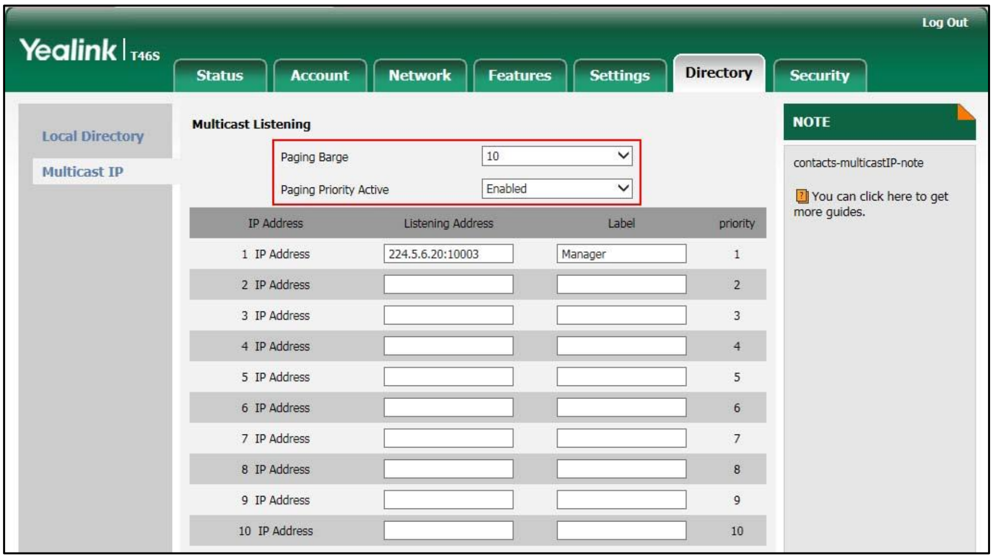


4. Click **Confirm** to accept the change.

To configure paging barge and paging priority active features 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. Click **Confirm** to accept the change.

Hot Desking

Hot desking originates from the definition of being the temporary physical occupant of a work station or surface by a particular employee. A primary motivation for hot desking is cost reduction. Hot desking is regularly used in places where not all employees are in the office at the same time, or not in the office for a long time, which means actual personal offices would often be vacant, consuming valuable space and resources.

Hot desking allows a Guest to clear registration configurations of the Host on the phone, and then register his own account.

Procedure

Hot desking feature can be configured using the configuration files or locally.

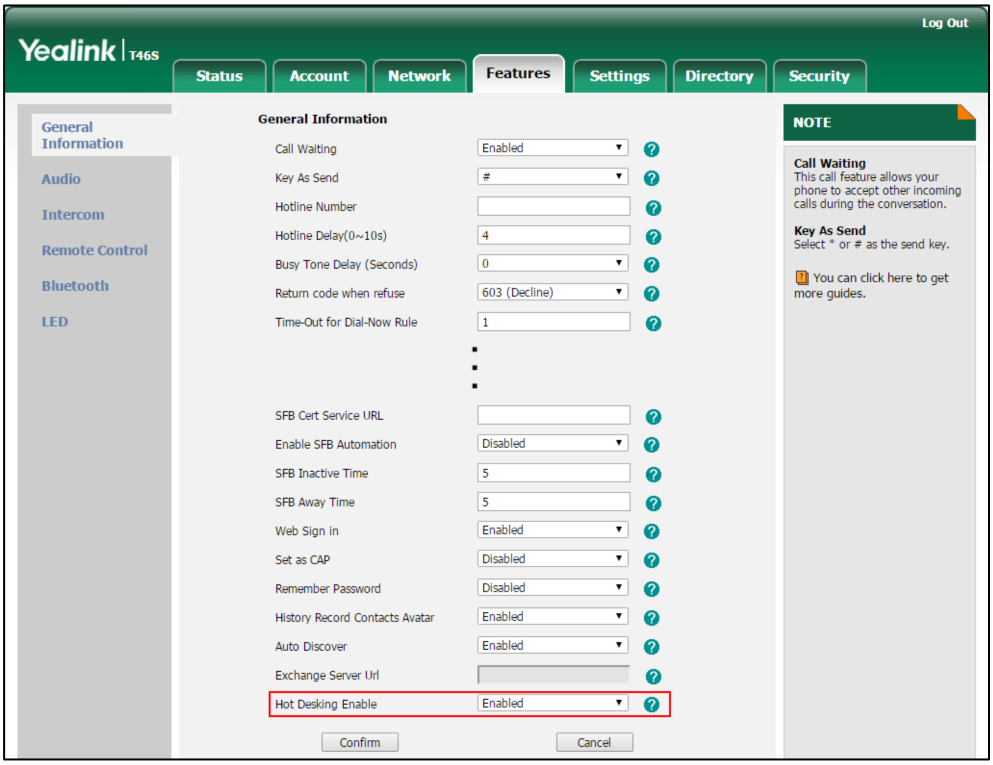
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the hot desking feature. **Parameters:** sfb.hot_desking.enable
Local	Web User Interface	Configure the hot desking feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure the hot desking feature.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
sfb.hot_desking.enable	**0 or 1**	**1**
Description: Enables or disables the hot desking feature. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Hot Desking Enable **Phone User Interface:** Menu->Features->Hot-Desking		

To configure hot desking via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Hot Desking Enable**.



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

To configure hot desking feature via phone user interface:

1. Press **Menu**->**Features**->**Hot-Desking**.

2. Press , or **Switch** soft key to select the desired value in the **Hot-Desking** field.
3. Press the **Save** soft key to accept the change or the **Back** soft key to cancel.

For more information on how to use the hot desking feature, refer to *Yealink Skype for Business phone-specific user guide*.

Common Area Phone

Common area phones(CAPs) are Skype for Business phones that are not associated with an individual user. Instead of being located in someone's office, CAPs are typically located in building lobbies, cafeterias, employee lounges, conference rooms, and other locations where a large number of people are likely to gather. Unlike other phones on the Skype for Business server, which are typically maintained by using voice policies and dial plans that are assigned to individual users, CAPs do not have individual users assigned to them.

Procedure

Common area phone can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the common area phone feature. **Parameters:** features.set_as_cap.enable features.voice_mail.enable features.cap_presence.enable features.redial.enable features.exchange_connect.enable features.sfb_directory.enable phone_setting.search_contacts.enable features.call_history.enable features.paging.enable
Web User Interface		Configure the common area phone feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
Phone User Interface		Configure the common area phone feature.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.set_as_cap.enable	**0 or 1**	**0**
Description: Enables or disables the phone to work as a common area phone. **0**-Disabled, the phone will work as an individual phone. **1**-Enabled, the phone will work as a common area phone (with limited features enabled). **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Features->General Information->Set as CAP **Phone User Interface:** Menu->Advanced(default password: admin)->Common Area Phone->Set as CAP		
features.cap_presence.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display presence status of the Skype for Business contacts. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		
features.voice_mail.enable	**0 or 1**	**Refer to the following content**
Enables or disables the phone to use the voice mail feature. **0**-Disabled **1**-Enabled **Default Values**: For individual phone: The default value of T41S/T42S/T46S/T48S are 1 and CP960 is 0. For common area phone: 0 **Web User Interface:** None **Phone User Interface:** None		

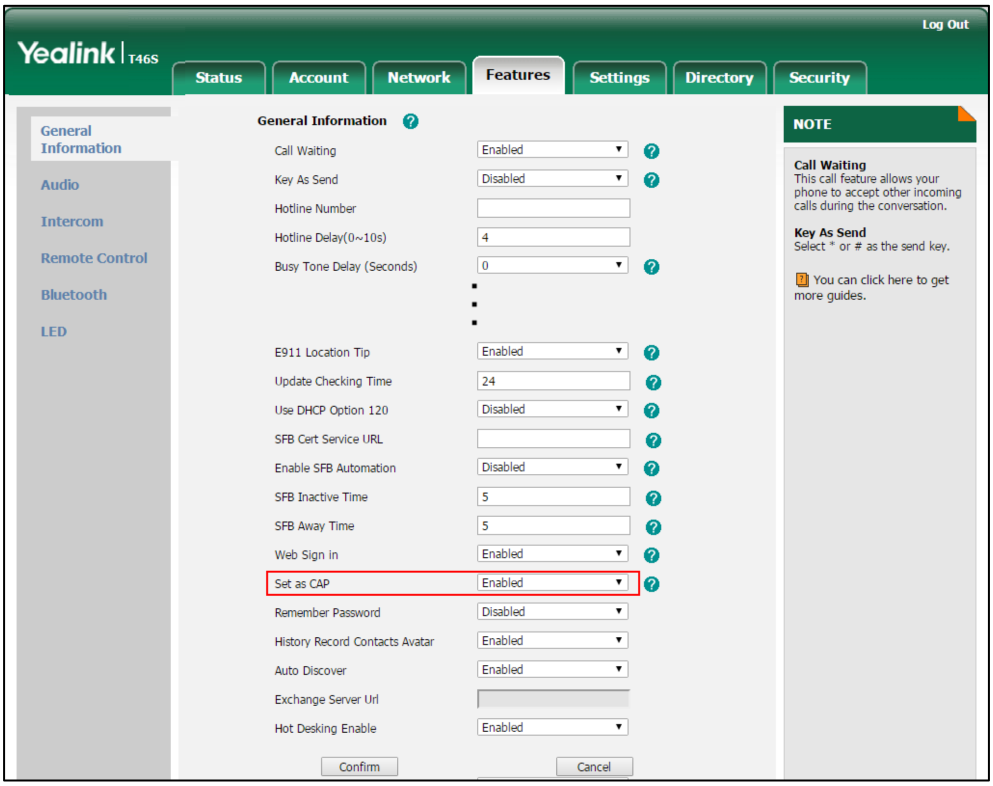
<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>features.redial.enable</td><td>0 or 1</td><td>Refer to the following content</td></tr>
<tr><td colspan="3">Enables or disables the phone to redial a previously dialed number by pressing the redial key.
0-Disabled
1-Enabled
Default Values:
For individual phone: 1
For common area phone: 0
Note: It is not applicable to CP960 Skype for Business phones.
Web User Interface:
None
Phone User Interface:
None</td></tr>
<tr><td>features.exchange_connect.enable</td><td>0 or 1</td><td>1</td></tr>
<tr><td colspan="3">Enables or disables Microsoft Exchange integration.
0-Disabled
1-Enabled
Web User Interface:
None
Phone User Interface:
None</td></tr>
<tr><td>features.sfb_directory.enable</td><td>0 or 1</td><td>Refer to the following content</td></tr>
<tr><td colspan="3">Enables or disables the phone to display the Skype for Business contacts.
0-Disabled
1-Enabled
Default Values:
For individual phone: 1
For common area phone: 0
Web User Interface:
None
Phone User Interface:
None</td></tr>
</table>

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>phone_setting.search_contacts.enable</td><td>0 or 1</td><td>Refer to the following content</td></tr>
<tr><td colspan="3">Enables or disables the phone search contacts.
0-Disabled
1-Enabled
Default Values:
For individual phone: 1
For common area phone: 0
Web User Interface:
None
Phone User Interface:
None</td></tr>
<tr><td>features.call_history.enable</td><td>0 or 1</td><td>Refer to the following content</td></tr>
<tr><td colspan="3">Enables or disables the phone display call history.
0-Disabled
1-Enabled
Default Values:
For individual phone: 1
For common area phone: 0
Web User Interface:
None
Phone User Interface:
None</td></tr>
<tr><td>features.paging.enable</td><td>0 or 1</td><td>Refer to the following content</td></tr>
<tr><td colspan="3">Enables or disables the phone to configure the multicast paging feature.
0-Disabled, the phone hides multicast paging configurations.
1-Enabled, the phone displays multicast paging configurations.
Note: It is not applicable to CP960 Skype for Business phones.
Default Values:
For individual phone: 1
For common area phone: 0
Web User Interface:</td></tr>
</table>

Parameters	Permitted Values	Default
None **Phone User Interface:** None		

To configure a phone to be a CAP via phone user interface:

1. Click on **Features**->**General Information**.
2. Select **Enabled** from the pull-down lists of **Set as CAP**.



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

To configure a phone to be a CAP via phone user interface:

1. Press **Menu**->**Advanced** (default password: admin)->**Common Area Phone**.
2. Press , or the **Switch** soft key to select **Enabled** from the **Set as CAP** field.
3. Press the **Save** soft key.

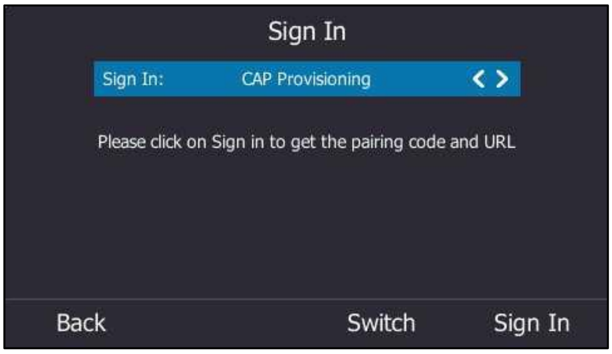
   A dialog box pops up to prompt you that this configuration will take effect after a reboot.

CAP Provisioning Sign-in Method

If you are a technician who is given permission to provision CAP accounts. You can use a web browser to provision numerous CAPs quickly.

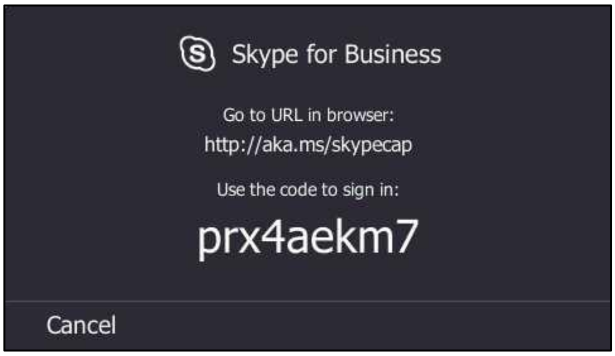
To sign into a CAP using the CAP Provisioning method via phone user interface:

1. Press the **Sign In** soft key.
2. Press , or the **Switch** soft key to select **CAP Provisioning**.

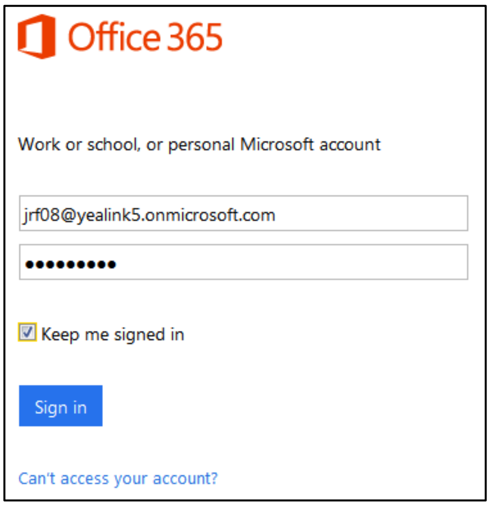


3. Press the **Sign In** soft key.

   The screen will show the pairing code and URL.



4. On your computer, enter the URL into your web browser.
5. Enter your Online account (make sure it has permission to provision CAP accounts) and password.



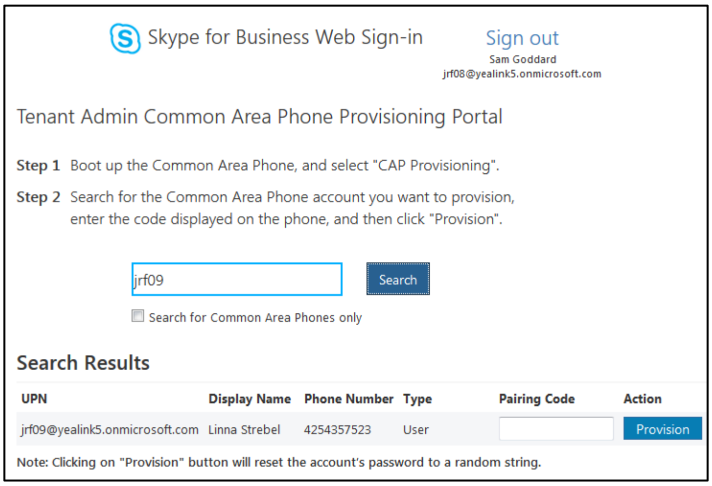
6. (Optional) Check the **Keep me signed in** checkbox, so that you don't need to enter a

password next time.

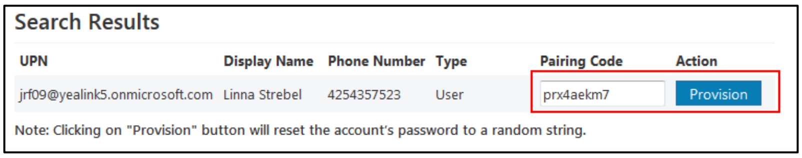
7. Click **Sign in**.

8. Search for the Online account you want to provision, and then click **Search**.

   The entry matches the characters entered will appear.



9. Enter the pairing code generated on the phone (e.g.,prx4aekm7) into the web browser.



10. Click **Provision**.

    The phone will sign into this CAP account automatically.

Note

You can also sign into the common area phone using other sign-in methods. For more information, refer to Signing into Skype for Business on page 108.

Branch Office Resiliency

Branch office resiliency is critical for multi-site deployments of Skype for Business where the control servers are located at a central site or data center. It allows branch site users to continue to have Enterprise Voice service and voice mail (if voice mail rerouting settings are configured) when the branch site loses the connection to the central site.

When the WAN connection between the branch site and central site is unavailable, the phone goes into resiliency mode:

- Branch site user on the phone stays signed in with an indication of “Limited service due to outage”.
- Presence icon on the phone LCD screen/touch screen is displayed as Unknown (T46S/T48S/CP960)/ ? (T42S/T41S).

- Call between branch site users is established successfully with 2-way audio.
- Conference between branch site users can be established successfully.
- The call history cannot get modified. (Already downloaded call log entries will not be deleted)
- Calls can be placed from the call history on the Skype for Business phone.
- Contact list is unavailable but you can search for a contact on the Skype for Business phone.
- User is not able to change his presence state manually.
- User is not able to use calendar feature.
- User is not able to receive the voice mail as exchange is unreachable and when Skype for Business phone comes out of resiliency mode, it downloads the yet undownloaded voice mail items and updates the voice mail screen.
- Calls between the branch office phones can be transferred to another branch site user.
- Call forward settings cannot be changed.
- By default, the phone can still download location information configured on the Skype for Business Server.

When the WAN connection between the branch site and central site becomes available, the phone comes out of resiliency mode automatically. Notification of resiliency is automatically dismissed, and you can use phone features as normal.

Note	For more information on branch office resiliency, contact your system administrator.

Action URI

HTTP/HTTPS GET Request

Action URI allows phones to interact with web server application by receiving and handling an HTTP or HTTPS GET request. When receiving a GET request, the phone will perform the specified action and respond with a 200 OK message. A GET request may contain variable named as “key” and variable value, which are separated by “=”. The valid URI format is: *http(s)://<phoneIPAddress>/servlet?key=variable value*. For example: http://10.3.20.10/servlet?key=OK.

Configuring Trusted IP Address for Action URI

For security reasons, phones do not handle HTTP/HTTPS GET requests by default. You need to specify the trusted IP address for action URI. When the phone receives a GET request from the trusted IP address for the first time, the LCD screen/touch screen prompts the message “Allow Remote Control?”. Press the **OK** soft key on the phone to allow remote control. You can specify one or more trusted IP addresses on the phone, or configure the phone to receive and handle the URI from any IP address.

You can use action URI feature to capture the phone's current screen. For more information, refer to Capturing the Current Screen of the Phone on page 302.

Procedure

Specify the trusted IP address for action URI using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the phone to receive the action URI requests. **Parameter:** features.action_uri.enable
		Specify the trusted IP address(es) for sending the action URI to the phone. **Parameter:** features.action_uri_limit_ip
Local	Web User Interface	Specify the trusted IP address(es) for sending the action URI to the phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-remotecontrl&q=load

Details of the Configuration Parameter:

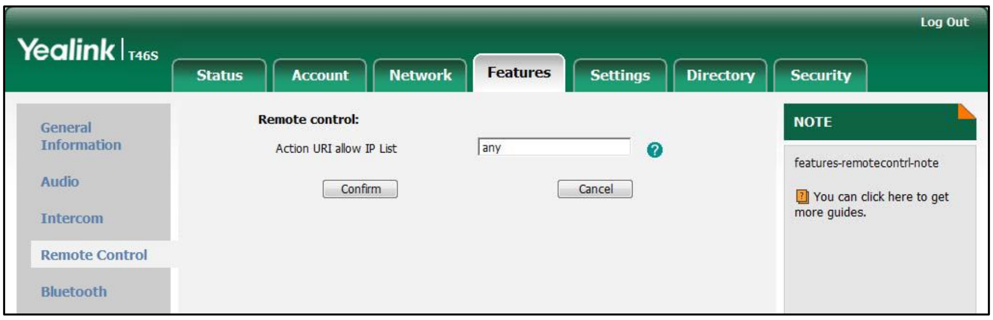
Parameter	Permitted Values	Default
features.action_uri.enable	**0 or 1**	**0**
Description: Enables or disables the phone to receive the action URI requests. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		
features.action_uri_limit_ip	**IP address or any**	**Blank**
Description:		

Parameter	Permitted Values	Default
Configures the IP address of the server from which the phone receives the action URI requests. For discontinuous IP addresses, multiple IP addresses are separated by commas. For continuous IP addresses, the format likes *.*.*.* and the “*” stands for the values 0~255. For example: 10.10.*.* stands for the IP addresses that range from 10.10.0.0 to 10.10.255.255. If left blank, the phone will reject any HTTP GET request. If it is set to “any”, the phone will accept and handle HTTP GET requests from any IP address. **Example:** features.action_uri_limit_ip = any **Note**: It works only if the value of the parameter “features.action_uri.enable” is set to 1 (Enabled). **Web User Interface:** Features->Remote Control->Action URI allow IP List **Phone User Interface:** None		

To configure the trusted IP address(es) for action URI via web user interface:

1. Click on **Features**->**Remote Control**.
2. Enter the IP address or any in the **Action URI allow IP List** field.

   Multiple IP addresses are separated by commas. If you enter “any” in this field, the phone can receive and handle GET requests from any IP address. If you leave the field blank, the phone cannot receive or handle any HTTP GET request.



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

Capturing the Current Screen of the Phone

You can capture the screen display of the phone using the action URI. Skype for Business phones support handling an HTTP or HTTPS GET request. The URI format is http(s)://<phoneIPAddress>/screencapture. The captured picture can be saved as a BMP or JPEG file.

You can also use the URI "http(s)://<phoneIPAddress>/screencapture/download" to capture the screen display first, and then download the image (which is saved as a JPG file and named with the phone model and the capture time) to the local system. Before capturing the phone's current screen, ensure that the IP address of the PC is included in the trusted IP address for Action URI on the phone.

When you capture the screen display, the phone may prompt you to enter the user name and password of the administrator if web browser does not remember the user name and password for web user interface login.

Note

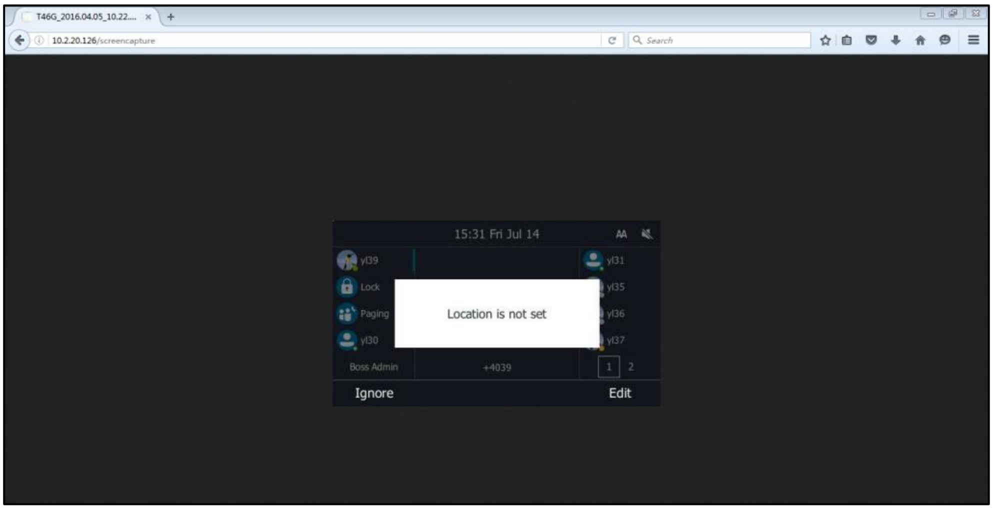
Skype for Business phones also support capturing the screen display using the old URI "http://<phoneIPAddress>/servlet?command=screenshot".

To capture the current screen of the phone:

1. Enter request URI (e.g., http://10.2.20.126/screencapture) in the browser's address bar and press the Enter key on the keyboard.
2. Do one of the following:
   - If it is the first time you capture the phone's current screen using the computer, the browser will display "Remote control forbidden", and the LCD screen/touch screen will prompt the message "Allow remote control?".

     Press the OK soft key on the phone to allow remote control. The phone will return to the previous screen. Refresh the web page.

The browser will display an image showing the phone's current screen. You can save the image to your local system.



- Else, the browser will display an image showing the phone's current screen directly. You can save the image to your local system.

Note Frequent capture may affect the Skype for Business phone performance. Yealink recommend you to capture the phone screen display within a minimum interval of 4 seconds.

Quality of Experience

Quality of Experience (QoE) metrics track the quality of audio calls made in your organization, including such things as the number of network packets lost, background noise, and the amount of "jitter" (differences in packet delay).

The phone calculates QoE metrics and then sends them to a server for monitoring and diagnostics purposes.

The phone will send QoE metrics every 30 seconds during a call or once a call ends (the call should last at least 5 seconds).

Procedure

QoE can be configured using the configuration files only.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the QoE feature. **Parameters:** features.report_qoe.when_bad_quality.enable

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.report_qoe.when_bad_quality.enable	**0 or 1**	**1**

Description:

Enables or disables the phone to send Quality of Experience (QoE) metrics to a server for monitoring and diagnostics purposes when voice quality on phone calls is poor.

0-Disabled

1-Enabled

Web User Interface:

None

Phone User Interface:

None

In QoE Metrics, the following formation will be reported:

Fields	Element	Attribute
VQReportEvent	VQSessionReport	
	VQSessionIntervalReport	
VQSessionReport		
	Endpoint	SessionId
	DialogInfo	
	MediaLine	
VQSessionReport:Endpoint		
		xmlns
		xmlns:v2
		xmlns:v3
		Name
		v2:OS
		v2:CPUName
		v2:CPUNumberOfCores
		v2:CPUProcessorSpeed(fixed value: 498)
		v2:VirtualizationFlag
VQSessionReport:DialogInfo		
	DialogCategory	CallId
	CorrelationID	FromTag
	FromURI	ToTag
	ToURI	Start
	Caller	End
	LocalContactURI	
	RemoteContactURI	

Fields	Element	Attribute
	LocalUserAgent	
	RemoteUserAgent	
	LocalPAI	
	RemotePAI	
	ConfURI	
	v2:CallPriority	
	v2:MediationServerBypass Flag	
	v2:TrunkingPeer	
	v2:MediaBypassWarningFl ag	
	v2:RegisteredInside	
	CallId	
	FromTag	
	ToTag	
	Start	
	End	
VQSessionReport:MediaLine		
	Description	xmlns
	InboundStream	xmlns:v2
	OutboundStream	xmlns:v3
		Label
MediaLine:Description	Connectivity	
	Security	
	Offerer	
	Transport	
	NetworkConnectivityInfo	
	LocalAddr	
	RemoteAddr	
	CaptureDev	
	RenderDev	
	ReflexiveLocalIPAddress	
	v3:ReflexiveLocalIPAddress	
	v3:MidCallReport	
Description:Connectivity	Ice	
	IceWarningFlags	
	RelayAddress	
Connectivity:RelayAddress	IPAddr	
	Port	
Description:NetworkConnectivityInfo	NetworkConnection	
	VPN	
	LinkSpeed	

Fields	Element	Attribute
	v3:NetworkConnectionDetails	
Description:LocalAddr	IPAddr	
	Port	
	SubnetMask	
	v2:MACAddr	
Description:RemoteAddr	IPAddr	
	Port	
Description:CaptureDev	Name	
	Driver	
Description:RenderDev	Name	
	Driver	
Description:ReflexiveLocalIPAddress	IPAddr	
	Port	
MediaLine:InboundStream	Network	ID
	Payload	
	QualityEstimates	
InboundStream:Network	Jitter	
	PacketLoss	
	BurstGapLoss	
	Delay	
	Utilization	
Network:Jitter	InterArrival	
	InterArrivalSD	
	InterArrivalMax	
Network:PacketLoss	LossRate	
	LossRateMax	
Network:Delay	RelativeOneWay	
Delay:RelativeOneWay	Average	
	Max	
	Gap	
Delay:RelativeOneWay:Gap	Occurrences	
	Density	
	Duration	
Network:Utilization	Packets	
InboundStream:Payload:Audio	PayloadType	
	PayloadDescription	
	SampleRate	
	Signal	
	v4:JitterBufferSizeAvg	
	v4:JitterBufferSizeMax	
	v4:JitterBufferSizeMin	

Fields	Element	Attribute
	v4:NetworkJitterAvg	
	v4:NetworkJitterMax	
	v4:NetworkJitterMin	
Audio:Signal	SignalLevel	
	NoiseLevel	
	SpeakerGlitchRate	
	v2:RxAvgAGCGain	
	v3:RecvSignalLevelCh1	
	v3:RecvNoiseLevelCh1	
	v4:RenderSignalLevel	
	v4:RenderNoiseLevel	
	v4:RenderLoopbackSignalLevel	
QualityEstimates:Audio	RecvListenMOS	
	RecvListenMOSMin	
	RecvListenMOSAlg (fixed value for Yealink device: P.564)	
	NetworkMOS	
Audio:NetworkMOS	OverallAvg	
	OverallMin	
MediaLine:OutboundStream	Network	ID
	Payload	
	QualityEstimates	
OutboundStream:Network	Jitter	
	PacketLoss	
	Delay	
	Utilization	
Network:Jitter	InterArrival	
	InterArrivalMax	
Network:PacketLoss	LossRate	
	LossRateMax	
Network:Delay	RoundTrip	
	RoundTripMax	
Network:Utilization	Packets	
	BandwidthEst	
OutboundStream:Payload:Audio	PayloadType	
	PayloadDescription	
	SampleRate	
	Signal	
Audio:Signal	SignalLevel	
	NoiseLevel	

Fields	Element	Attribute
	MicGlitchRate	
	EchoPercentMicIn	
	EchoPercentSend	
	SendSignalLevelCh1	
	SendNoiseLevelCh1	

You can log into the QoE Monitoring Server to view intuitive QoE information.

Configuring Audio Features

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

- Pre Dial Tone
- Phone Ring Tones
- Private Line Tones
- Redial Tone
- Tones
- Voice Mail Tone
- Headset Prior
- Ringer Device for Headset
- Dual Headset
- Sending Volume
- Audio Codecs
- Acoustic Clarity Technology
- DTMF

Pre Dial Tone

Pre dial tone allows phones to play key tone in following situations:

- Enter phone numbers without picking up the handset (applicable to T48S/T46S/T42S/T41S Skype for Business phones).
- Tap (**Search** icon) to enter the pre-dialing screen, and then enter phone numbers without picking up the handset (only applicable to T48S Skype for Business phones).

Pre dial tone is not applicable to CP960 Skype for Business phones.

Procedure

Pre dial tone can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure pre dial tone feature. **Parameters:** sfb.pre_dial_tone.enable
Local	Web User Interface	Configure pre dial tone feature. **Navigate to**:

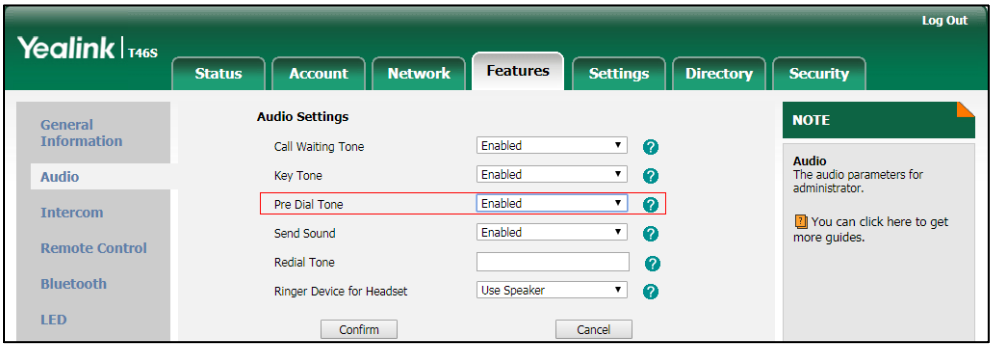
		http://<phoneIPAddress>/servlet?p=features-audio&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
sfb.pre_dial_tone.enable	**0 or 1**	**0**
Description: Enables or disables the phones to play key tone in following situations: **For T48S/T46S/T42S/T41S Skype for Business phones:** Enter phone numbers without picking up the handset. **For T48S Skype for Business phones:** Tap (**Search** icon) to enter the pre-dialing screen, and then enter phone numbers without picking up the handset. **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->Audio->Pre Dial Tone **Phone User Interface:** None		

To configure pre dial tone via web user interface:

1. Click on **Features**->**Audio**.
2. Select the desired value from the pull-down list of **Pre Dial Tone**.



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

Phone Ring Tones

Phone ring tones are used to indicate incoming calls acoustically. Users can select a built-in system ring tone or a custom ring tone for the phone or account. To set the custom ring tones, you need to upload the custom ring tones to the phone in advance.

The ring tone format must meet the following:

Skype for Business phone Model	Format	Total File Size	Note
T48S/T46S/CP960	.wav	<=8MB	2MB of space should be reserved for the phone.
T42S/T41S	.wav	<=100k	2MB of space should be reserved for the phone.

Note

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

Procedure

Ring tones can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure a ring tone for the phone. **Parameter:** phone_setting.ring_type
		Specify the access URL of the custom ring tone. **Parameter:** phone_setting.ringtone.url
		Delete all custom ring tone files. **Parameter:** ringtone.delete
	<MAC>.cfg	Configure a ring tone on a per-line basis. **Parameters:** account.1.ringtone.ring_type
Local	Web User Interface	Upload the custom ring tones. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load
		Configure a ring tone for the phone.

		Navigate to: http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Configure a ring tone for the phone.

Details of the Configuration Parameter:

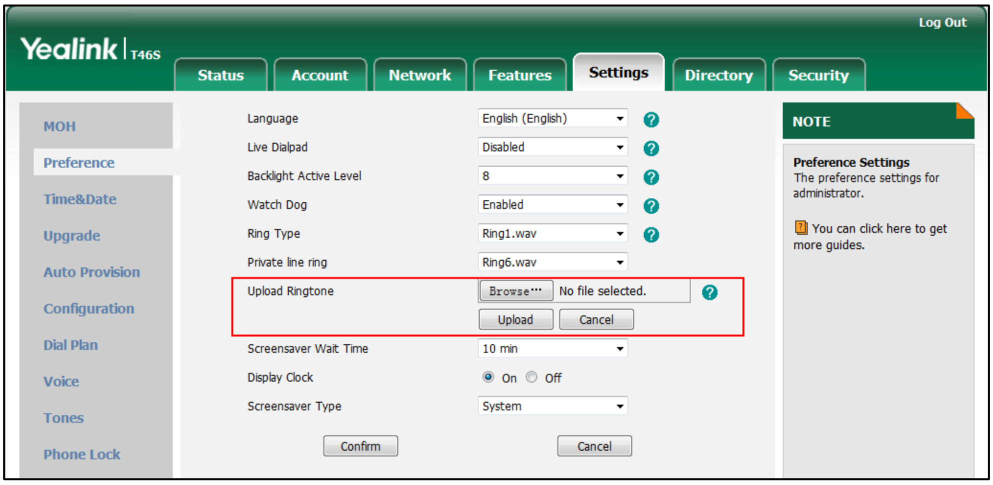
Parameters	Permitted Values	Default
phone_setting.ring_type	**Refer to the following content**	**Ring1.wav**
Description: Configures a ring tone for the phone. **Permitted Values:** Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring.wav). **Example:** To configure a phone built-in ring tone (e.g., Ring1.wav): phone_setting.ring_type = Ring1.wav To configure a custom ring tone (e.g., Customring.wav): phone_setting.ring_type = Customring.wav **Web User Interface:** Settings->Preference->Ring Type **Phone User Interface:** Menu->Basic->Sounds->Ring Tones->Normal		
account.1.ringtone.ring_type	**Refer to the following content**	**Common**
Description: Configures a ring tone for the account 1. **Example**: account.1.ringtone.ring_type = Ring3.wav It means configuring Ring3.wav for the account. account.1.ringtone.ring_type = Common It means the account will use the ring tone selected for the phone configured by the parameter "phone_setting.ring_type". **Permitted Values:**		

Parameters	Permitted Values	Default
Common, Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring.wav). **Web User Interface:** None **Phone User Interface:** None		
phone_setting.ringtone.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom ring tone file. **Example:** phone_setting.ringtone.url = tftp://192.168.1.100/Customring.wav **Web User Interface:** Settings->Preference->Upload Ringtone **Phone User Interface:** None		
ringtone.delete	**http://localhost/all**	**Blank**
Description: Deletes all custom ring tone files. **Example:** ringtone.delete = http://localhost/all **Web User Interface:** None **Phone User Interface:** None		

To upload a custom ring tone via web user interface:

1. Click on **Settings**->**Preference**.
2. In the **Upload Ringtone** field, click **Browse** to locate a ring tone file (the file format must be *.wav) from your local system.

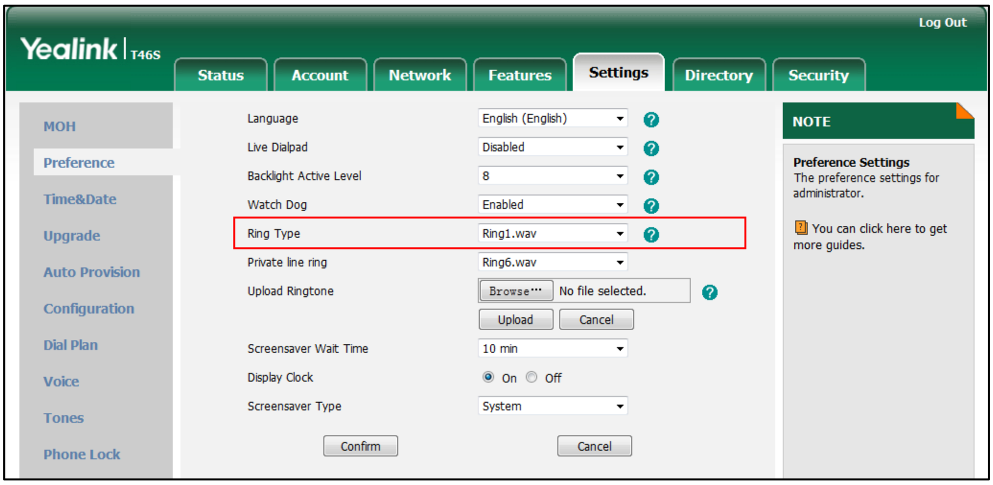
3. Click **Upload** to upload the file.



The custom ring tone appears in the pull-down list of **Ring Type**.

To change the ring tone for the phone via web user interface:

1. Click on **Settings**->**Preference**.
2. Select the desired ring tone from the pull-down list of **Ring Type**.



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

To select a ring tone for the phone via phone user interface:

1. Press **Menu**->**Basic**->**Sounds**->**Ring Tones**->**Normal**.
2. Press or to select the desired ring tone.
3. Press the **Save** soft key to accept the change.

Muting the Ringtone

If you do not want to be disturbed by the phone ringtone, you can choose to mute the ringtone when you set account status to Busy (in a call) or Do Not Disturb.

Procedure

Muting the ringtone can be configured using the configuration files only.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the phone to mute the ringtone. **Parameters:** phone_setting.soundsmin.busy_enable phone_setting.soundsmin.dnd_enable

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.soundsmin.busy_enable	**0 or 1**	**0**
Description: Enables or disables the phone to mute the ringtone when account status is busy (in a call). **0**-Disabled, the phone plays a ringtone for incoming calls when account status is busy (in a call). **1**-Enabled, the phone does not play a ringtone for incoming calls when account status is busy (in a call). **Web User Interface:** None **Phone User Interface:** None		
phone_setting.soundsmin.dnd_enable	**0 or 1**	**1**
Description: Enables or disables the phone to mute the ringtone when account status is Do not Disturb. **0**-Disabled, the phone plays a ringtone for incoming calls from work group when account status is Do not Disturb. **1**-Enabled, the phone does not play a ringtone for incoming calls from work group when account status is Do not Disturb. **Web User Interface:** None **Phone User Interface:** None		

Private Line Tones

The Skype for Business Server allows the system administrator to give user a second, private telephone line in addition to their primary telephone line. Private lines are often assigned to bosses who want an unlisted telephone number at which they can be reached directly.

When the boss receives a private call, the private line will bypass call delegation and only boss's phone rings. Private line can be configured via Skype for Business Server only.

Private line tones feature allows the phone to play a distinct ring tone when receiving a private call.

Procedure

Private line tones can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure a ring tone for the private line. **Parameter:** phone_setting.private_line_ring.enable phone_setting.private_line_ring_type
Local	Web User Interface	Configure a ring tone for the private line. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Configure a ring tone for the private line.

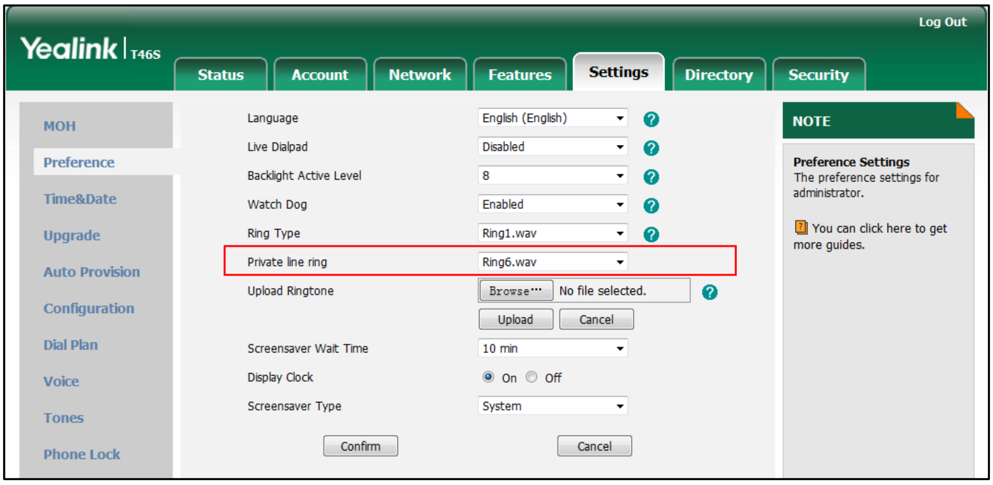
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.private_line_ring.enable	**0 or 1**	**1**
Description: Enables or disables the phone to set a distinct ring tone for the private line. **0**-Disabled, private call will use the phone's ring tone. The phone's ring tone is configured by the parameter "phone_setting.ring_type". **1**-Enabled, a distinct ring tone can be assigned to the private line. **Web User Interface:** None **Phone User Interface:** None		
phone_setting.private_line_ring_type	**Refer to the following**	**Ring6.wav**

Parameter	Permitted Values	Default
	content	
Description: Configures a ring tone for the private line. **Permitted Values:** Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring.wav). **Example:** To configure a phone built-in ring tone (e.g., Ring6.wav): phone_setting.private_line_ring_type = Ring6.wav To configure a custom ring tone (e.g., Customring.wav): phone_setting.private_line_ring_type = Customring.wav **Web User Interface:** Settings->Preference->Private line ring **Phone User Interface:** Menu->Basic->Sounds->Ring Tones->Private Line		

To change the ring tone for the private line via web user interface:

1. Click on **Settings**->**Preference**.
2. Select the desired ring tone from the pull-down list of **Private line ring**.



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

To select a ring tone for the private line via phone user interface:

1. Press **Menu**->**Basic**->**Sounds**->**Ring Tones**->**Private Line**.
2. Press or to select the desired ring tone.
3. Press the **Save** soft key to accept the change.

Redial Tone

Redial tone allows phone to continue to play the dial tone after inputting the preset numbers on the dialing screen.

Redial tone is not applicable to CP960 Skype for Business phones.

Procedure

Redial tone can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure redial tone feature. **Parameters:** features.redial_tone
Local	Web User Interface	Configure redial tone feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-audio&q=load

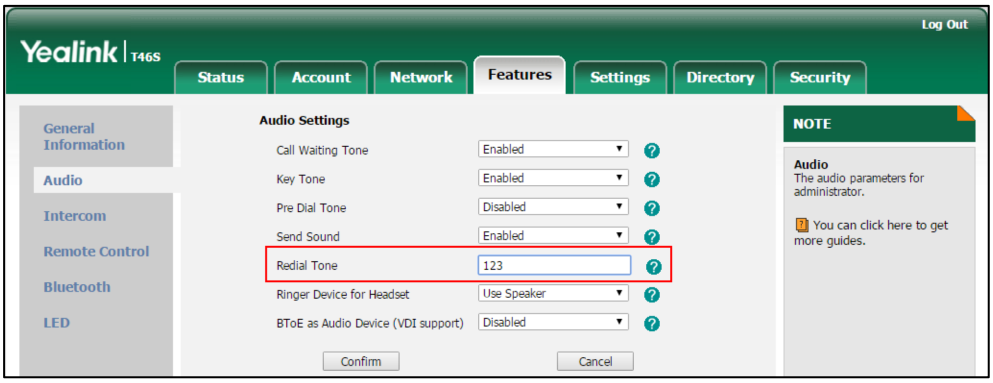
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.redial_tone	**Integer within 6 digits**	**Blank**
Description: Configures the phone to continue to play the dial tone after inputting the preset numbers on the dialing screen. **Example**: features.redial_tone = 125 The phone will continue to play the dial tone after inputting “125” on the dialing screen. If it is left blank, the phone will not play the dial tone after inputting numbers on the dialing screen. **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->Audio->Redial Tone **Phone User Interface:**		

Parameters	Permitted Values	Default
None		

To configure redial tone via web user interface:

1. Click on **Features**->**Audio**.
2. Enter the desired value in the **Redial Tone** field.



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

Tones

When receiving a message, the phone will play a warning tone. You can customize tones or select specialized tone sets (vary from country to country) to indicate different conditions of the phone. The default tones used on phones are the US tone sets. Available tone sets for phones:

- 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

Configured tones can be heard on phones for the following conditions.

Condition	Description
Dial	When in the pre-dialing interface
Ring Back	Ring-back tone
Busy	When the callee is busy
Congestion	When the network is congested
Call Waiting	Call waiting tone (For more information on call waiting, refer to Call Waiting)
Dial Recall	When receiving a call back
Info	When receiving a special message
Stutter	When receiving a voice mail
Auto Answer	When automatically answering a call (For more information on auto answer, refer to Auto Answer)

Procedure

Tones can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the tones for the phone. **Parameters:** voice.tone.country voice.tone.dial voice.tone.ring

		voice.tone.busy voice.tone.congestion voice.tone.callwaiting voice.tone.dialrecall voice.tone.info voice.tone.stutter voice.tone.autoanswer
Local	Web User Interface	Configure the tones for the 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 phone. **Permitted Values:** Custom, Australia, Austria, Brazil, Belgium, Chile, China, Czech, Czech ETSI, Denmark, Finland, France, Germany, Great Britain, Greece, Hungary, Lithuania, India, Italy, Japan, Mexico, New Zealand, Netherlands, Norway, Portugal, Spain, Switzerland, Sweden, Russia, United States. **Example:** voice.tone.country = Custom **Web User Interface:** Settings->Tones->Select Country **Phone User Interface:** None		
voice.tone.dial	**String**	**Blank**
Description: Customizes the dial tone. tonelist = element[,element] [,element]… Where **element** = [!]Freq1[+Freq2][+Freq3][+Freq4] /Duration		

Parameters	Permitted Values	Default
Freq: the frequency of the tone (ranges from 200 to 4000Hz). If it is set to 0Hz, it means the tone is not played. A tone is comprised of at most four different frequencies. **Duration**: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms. You can configure at most eight different tones for one condition, and separate them by commas. (e.g., 250/200,0/1000,200+300/500,200+500+800+1500/1000). If you want the 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. It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Settings->Tones->Dial **Phone User Interface:** None		
voice.tone.ring	**String**	**Blank**
Description: Customizes the ringback tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** It works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings->Tones->Ring Back **Phone User Interface:** None		
voice.tone.busy	**String**	**Blank**
Description: Customizes the tone when the callee is busy. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** It works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings->Tones->Busy **Phone User Interface:**		

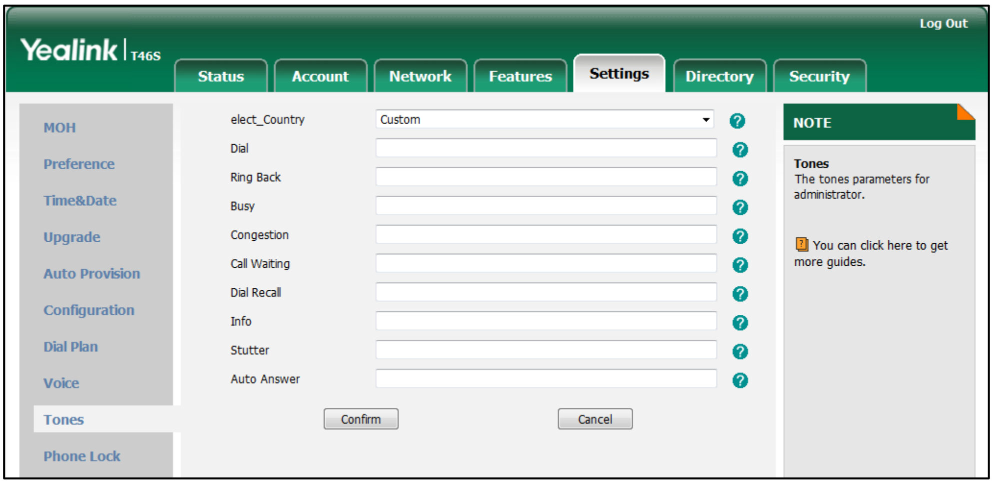
Parameters	Permitted Values	Default
None		
voice.tone.congestion	**String**	**Blank**
Description: Customizes the tone when the network is congested. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** It works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings->Tones->Congestion **Phone User Interface:** None		
voice.tone.callwaiting	**String**	**Blank**
Description: Customizes the call waiting tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** It works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings->Tones->Call Waiting **Phone User Interface:** None		
voice.tone.dialrecall	**String**	**Blank**
Description: Customizes the call back tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** It works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings->Tones->Dial Recall **Phone User Interface:** None		

Parameters	Permitted Values	Default
voice.tone.info	**String**	**Blank**
Description: Customizes the info tone. The phone will play the info tone with the special information, for example, the number you are calling is not in service. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** It works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings->Tones->Info **Phone User Interface:** None		
voice.tone.stutter	**String**	**Blank**
Description: Customizes the tone when the phone receives a voice mail. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** It works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings->Tones->Stutter **Phone User Interface:** None		
voice.tone.autoanswer	**String**	**Blank**
Description: Customizes the warning tone for auto answer. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** It works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings->Tones->Auto Answer **Phone User Interface:** None		

To configure tones via web user interface:

1. Click on **Settings**->**Tones**.
2. Select the desired value from the pull-down list of **Select Country**.

   If you select **Custom**, you can customize a tone for each condition of the phone.



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

Voice Mail Tone

Voice mail tone feature allows the 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 phone. For more information, refer to Voice Mail Tone on page 325.

Procedure

Voice mail tone can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure whether to play a warning tone when the phone receives a new voice mail. **Parameters:** features.voice_mail_tone_enable
Local	Web User Interface	Configure whether to play a warning tone when the phone receives a new voice mail. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

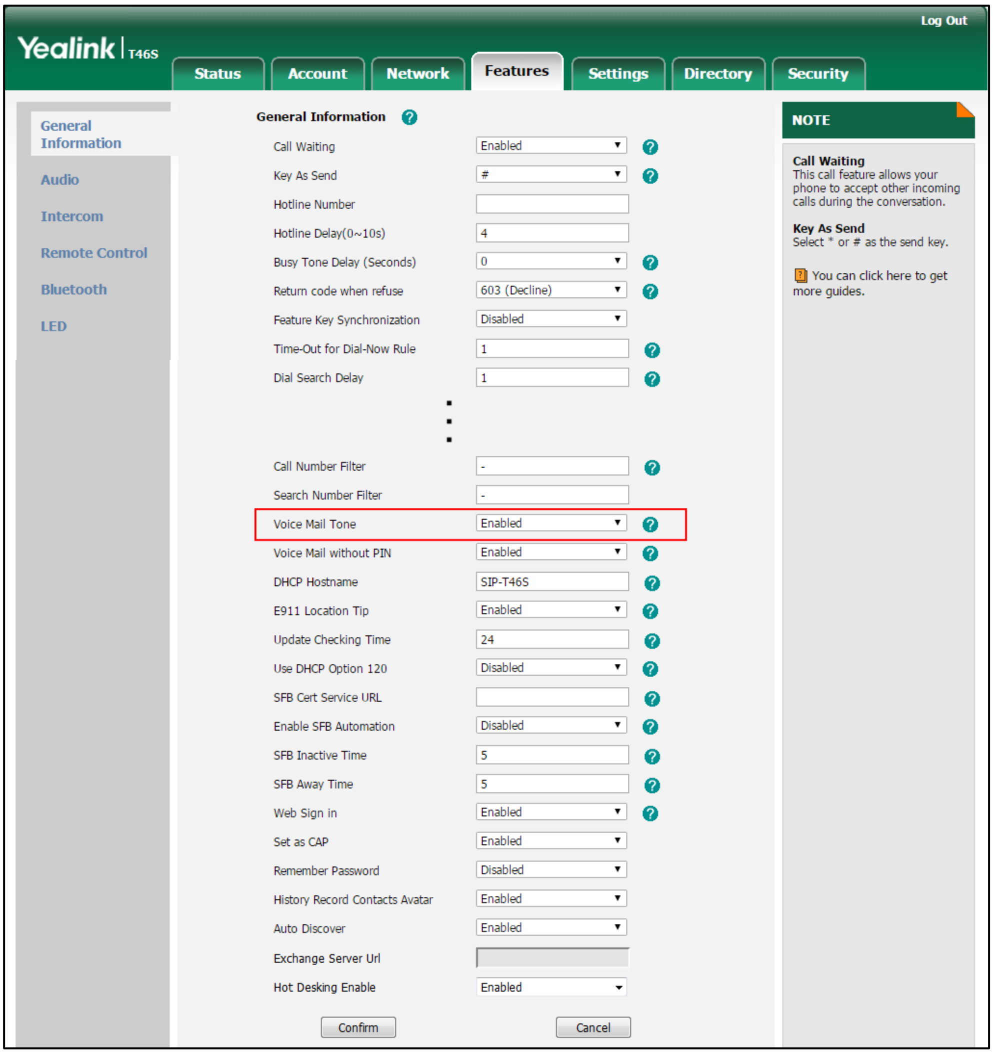
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.voice_mail_tone_enable	**0 or 1**	**1**
Description: Enables or disables the phone to play a warning tone when it receives a new voice mail. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Voice Mail Tone **Phone User Interface:** None		

To configure voice mail tone via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **Voice Mail Tone**.



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

Headset Prior

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

Headset prior is not applicable to CP960 Skype for Business phones.

Procedure

Headset prior can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure headset prior. **Parameter:** features.headset_prior
Local	Web User Interface	Configure headset prior.

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

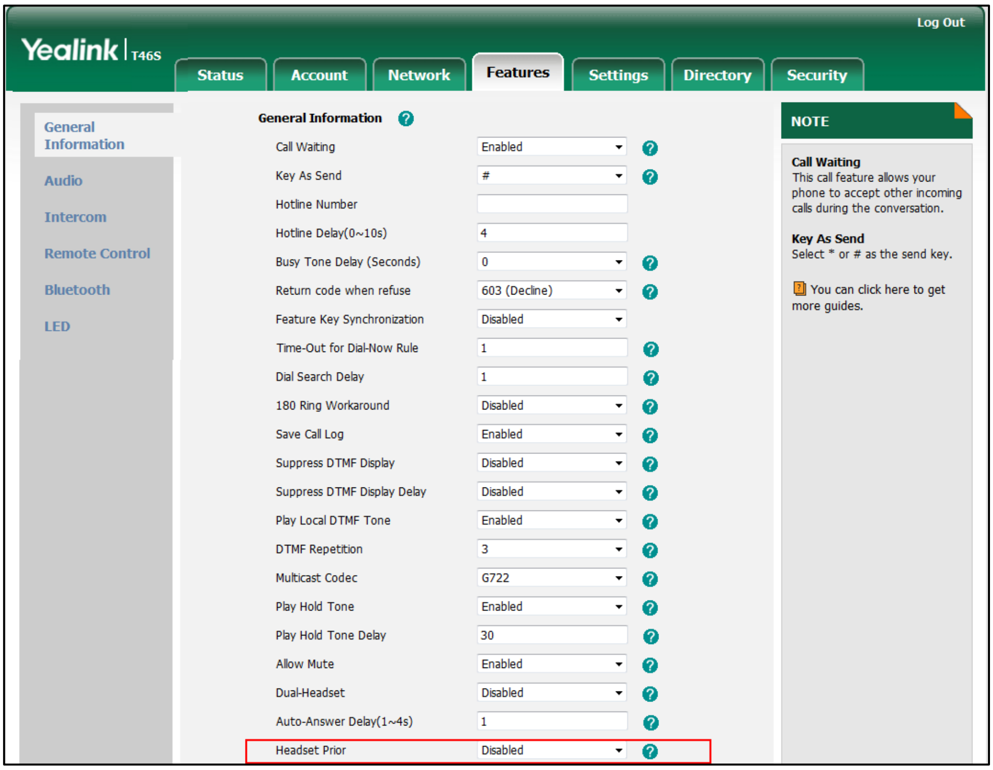
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.headset_prior	**0 or 1**	**0**
Description: Enables or disables headset prior feature. You need to press the HEADSET key to activate the headset mode in advance. **0**-Disabled, the headset mode can be deactivated by pressing the speakerphone key or the HEADSET key except the HANDSET key. **1**-Enabled, the headset mode will not be deactivated until the user presses the HEADSET key again. **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->General Information->Headset Prior **Phone User Interface:** None		

To configure headset prior via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **Headset Prior**.



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

Ringer Device for Headset

The Skype for Business phones support either or both speaker and headset ringer devices. Ringer Device for Headset feature allows users to configure which ringer device to be used when receiving an incoming call. For example, if the ringer device is set to Headset, ring tone will be played through your headset.

If the ringer device is set to Headset or Headset&Speaker, the headset should be connected to the phone and the headset mode also should be activated in advance. You can press the HEADSET key to activate the headset mode. For more information, refer to *Yealink Skype for Business phone-specific user guide*.

Ringer Device for Headset feature is not applicable to CP960 Skype for Business phones.

Procedure

Ringer device for headset can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the ringer device for the phone. **Parameters:** features.ringer_device.is_use_headset
Local	Web User Interface	Configure the ringer device for the

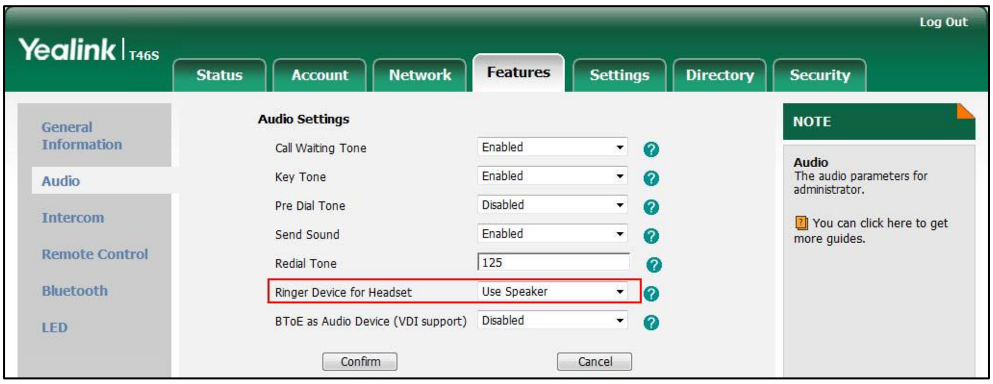
		phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-audio&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.ringer_device.is_use_headset	**0, 1 or 2**	**0**
Description: Configures the ringer device for the phone. **0**-Use Speaker **1**-Use Headset **2**-Use Headset & Speaker If the ringer device is set to Headset or Headset&Speaker, the headset should be connected to the phone and the headset mode also should be activated in advance. **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->Audio->Ringer Device for Headset **Phone User Interface:** None		

To configure ringer device for headset via web user interface:

1. Click on **Features**->**Audio**.
2. Select the desired value from the pull-down list of **Ringer Device for Headset**.



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

Dual Headset

Dual headset allows users to use two headsets on one phone. To use this feature, users need to physically connect two headsets to the headset and handset jacks respectively. Once the phone connects to a call, the user with the headset connected to the headset jack has full-duplex capabilities, while the user with the headset connected to the handset jack is only able to listen.

Dual headset is not applicable to CP960 Skype for Business phones.

Procedure

Dual headset can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure dual headset. **Parameter:** features.headset_training
Local	Web User Interface	Configure dual headset. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

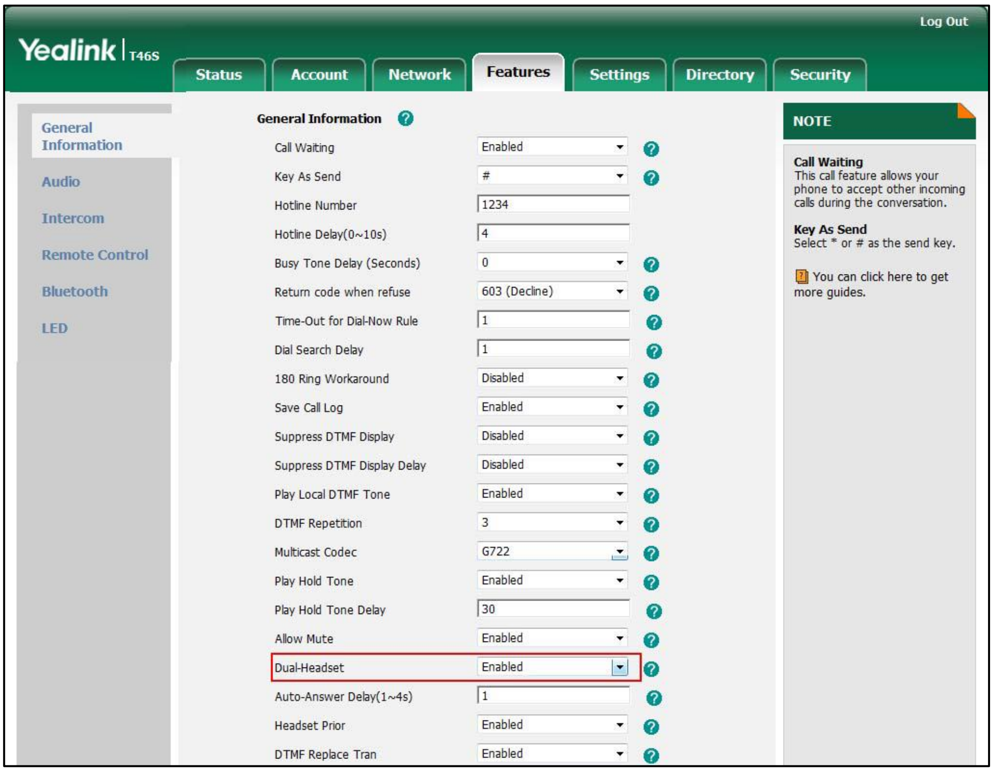
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.headset_training	**0 or 1**	**0**
Description: Enables or disables dual headset feature. **0**-Disabled **1**-Enabled, users can use two headsets on one phone. When the phone joins in a call, the users with the headset connected to the headset jack have a full-duplex conversation, while the users with the headset connected to the handset jack are only allowed to listen to. **Note:** It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Features->General Information->Dual-Headset **Phone User Interface:** None		

To configure dual headset via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **Dual-Headset**.



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

Sending Volume

Sending volume allows user to adjust the sending volume of currently engaged audio devices (handset, speakerphone or headset) when the phone is in use.

Procedure

Sending volume can be configured using the configuration files only.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the sending volume of the speaker. **Parameter:** voice.handfree_send
		Configure the sending volume of the handset. **Parameter:** voice.handset_send

		Configure the sending volume of the headset. **Parameter:** voice.headset_send

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.handfree_send	**Integer from -50 to 50**	**0**
Description: Configures the sending volume of the speaker. **Note:** We recommend that you modify this parameter cautiously. An unreasonable value may render the voice quality bad. If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		
voice.handset_send	**Integer from -50 to 50**	**0**
Description: Configures the sending volume of the handset. **Note:** We recommend that you modify this parameter cautiously. An unreasonable value may render the voice quality bad. If you change this parameter, the phone will reboot to make the change take effect. It is not applicable to CP960 Skype for Business phones. **Web User Interface:** None **Phone User Interface:** None		
voice.headset_send	**Integer from -50 to 50**	**0**
Description: Configures the sending volume of the headset. **Note:** We recommend that you modify this parameter cautiously. An unreasonable value may render the voice quality bad. If you change this parameter, the phone will reboot to make the change take effect. It is not applicable to CP960 Skype for Business phones.		

Parameter	Permitted Values	Default
Web User Interface: None **Phone User Interface:** None		

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 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.

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

Supported Audio Codecs	Default Audio Codecs
G722, PCMA, PCMU, G729, G726-16, G726-24, G726-32, G726-40, iLBC, G723_53, G723_63, SILK_NB, SILK_WB	G722, PCMA, PCMU, G729

The following table summarizes the supported audio codecs on phones:

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
G722	G.722	RFC 3551	64 Kbps	16	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
G723_53/ G723_63	G.723.1	RFC 3551	5.3kbps 6.3kbps	8 Ksps	30ms
iLBC	iLBC	RFC 3952	15.2 Kbps 13.33 Kbps	8 Ksps	20ms 30ms

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
SILK_NB	SILK_NB	draft-vos-silk-01	12kbps	8 Ksps	20ms
SILK_WB	SILK_WB	draft-vos-silk-01	20kbp	16 Ksps	20ms

Packetization Time

Ptime (Packetization Time) 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 attribute "rtpmap" is used to define a mapping from RTP payload codes to a codec, clock rate and other encoding parameters.

The corresponding attributes of the codec are listed as follows:

Codec	Configuration	Priority	RTPmap
G722	Configuration Files Web User Interface	1	9
PCMU	Configuration Files Web User Interface	2	0
PCMA	Configuration Files Web User Interface	3	8
G729	Configuration Files Web User Interface	4	18
G723_53	Configuration Files Web User Interface	0	4
G723_63	Configuration Files Web User Interface	0	4
G726-16	Configuration Files Web User Interface	0	103
G726-24	Configuration Files Web User Interface	0	104
G726-32	Configuration Files Web User Interface	0	102

Codec	Configuration	Priority	RTPmap
G726-40	Configuration Files Web User Interface	0	105
iLBC	Configuration Files Web User Interface	0	106
SILK_WB	Configuration Files Web User Interface	0	119
SILK_NB	Configuration Files Web User Interface	0	120

Procedure

Configuration changes can be performed using the configuration files or locally.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the codecs to be used. **Parameters:** static.account.1.codec.Y.enable static.account.1.codec.Y.payload_type
		Configure the priority and rtpmap for the enabled codec. **Parameters:** static.account.1.codec.Y.priority static.account.1.codec.Y.rtpmap
Local	Web User Interface	Configure the codecs to be used. 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
static.account.1.codec.Y.payload_type (Y ranges from 1 to 13)	**Refer to the following content**	**Refer to the following content**
Description: Configures the codec for the account.		

Parameters	Permitted Values	Default
Permitted Values: G722, PCMU, PCMA, G729, G726-16, G726-24, G726-32, G726-40, iLBC, G723_53, G723_63, SILK_NB, SILK_WB **Default:** When Y=1, the default value is PCMU; When Y=2, the default value is PCMA; When Y=3, the default value is G723_53; When Y=4, the default value is G723_63; When Y=5, the default value is G729; When Y=6, the default value is G722; When Y=7, the default value is iLBC; When Y=8, the default value is G726-16; When Y=9, the default value is G726-24; When Y=10, the default value is G726-32; When Y=11, the default value is G726-40; When Y=12, the default value is SILK_WB; When Y=13, the default value is SILK_NB; **Example:** static.account.1.codec.1.payload_type = PCMU **Web User Interface:** Account->Codec **Phone User Interface:** None		
static.account.1.codec.Y.enable (Y ranges from 1 to 13)	**0 or 1**	**Refer to the following content**
Description: Enables or disables the specified codec for the account. **0**-Disabled **1**-Enabled **Default:** When Y=1, the default value is 1; When Y=2, the default value is 1; When Y=3, the default value is 0; When Y=4, the default value is 0;		

Parameters	Permitted Values	Default
When Y=5, the default value is 1; When Y=6, the default value is 1; When Y=7, the default value is 0; When Y=8, the default value is 0; When Y=9, the default value is 0; When Y=10, the default value is 0; When Y=11, the default value is 0; When Y=12, the default value is 0; When Y=13, the default value is 0; **Example:** static.account.1.codec.1.enable = 1 It means that the codec PCMU is enabled on the account. **Web User Interface:** Account->Codec **Phone User Interface:** None		
static.account.1.codec.Y.priority (Y ranges from 0 to 13)	**Integer from 0 to 12**	**Refer to the following content**
Description: Configures the priority of the enabled codec for the account. **Default:** When Y=1, the default value is 2; When Y=2, the default value is 3; When Y=3, the default value is 0; When Y=4, the default value is 0; When Y=5, the default value is 4; When Y=6, the default value is 1; When Y=7, the default value is 0; When Y=8, the default value is 0; When Y=9, the default value is 0; When Y=10, the default value is 0; When Y=11, the default value is 0; When Y=12, the default value is 0; When Y=13, the default value is 0;		

Parameters	Permitted Values	Default
Example: static.account.1.codec.1.priority = 2 **Web User Interface:** Account->Codec **Phone User Interface:** None		
static.account.1.codec.Y.rtpmap (Y ranges from 1 to 13)	**Integer from 0 to 127**	**Refer to the following content**
Description: Configures the rtpmap of the audio codec for the account. **Default:** When Y=1, the default value is 0; When Y=2, the default value is 8; When Y=3, the default value is 4; When Y=4, the default value is 4; When Y=5, the default value is 18; When Y=6, the default value is 9; When Y=7, the default value is 106; When Y=8, the default value is 103; When Y=9, the default value is 104; When Y=10, the default value is 102; When Y=11, the default value is 105; When Y=12, the default value is 119; When Y=13, the default value is 120; **Example:** static.account.1.codec.1.rtpmap = 0 **Web User Interface:** None **Phone User Interface:** None		

To configure the codecs to be used 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**.

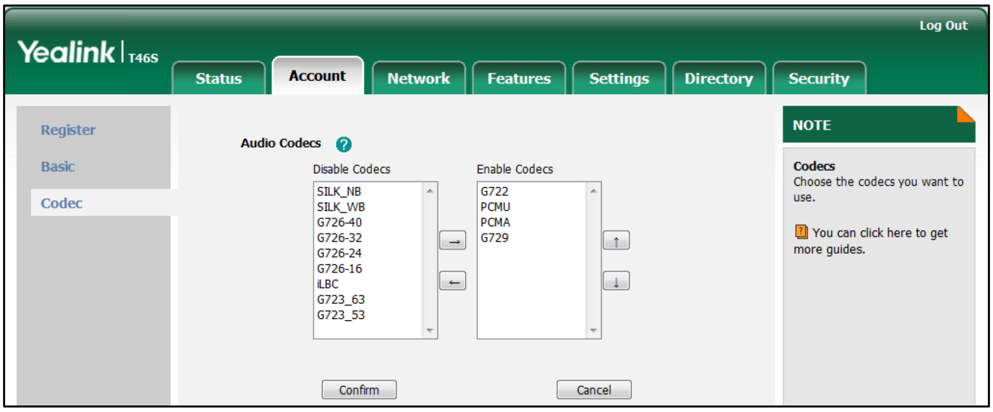
3. Select the desired codec from the **Disable Codecs** column and then click →.

   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.

Acoustic Clarity Technology

Acoustic Echo Cancellation

Acoustic Echo Cancellation (AEC) is used to reduce acoustic echo from a voice call to provide natural full-duplex communication patterns. It also increases the capacity achieved through silence suppression by preventing echo from traveling across a network. Skype for Business phones employ advanced AEC for hands-free operation. AEC is not normally required for calls via the handset. In certain situation, where echo is experienced by the remote party, AEC may be used to reduce/avoid echo when the user uses the handset.

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

Procedure

AEC can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure AEC. **Parameter:** voice.echo_cancellation
Local	Web User Interface	Configure AEC.

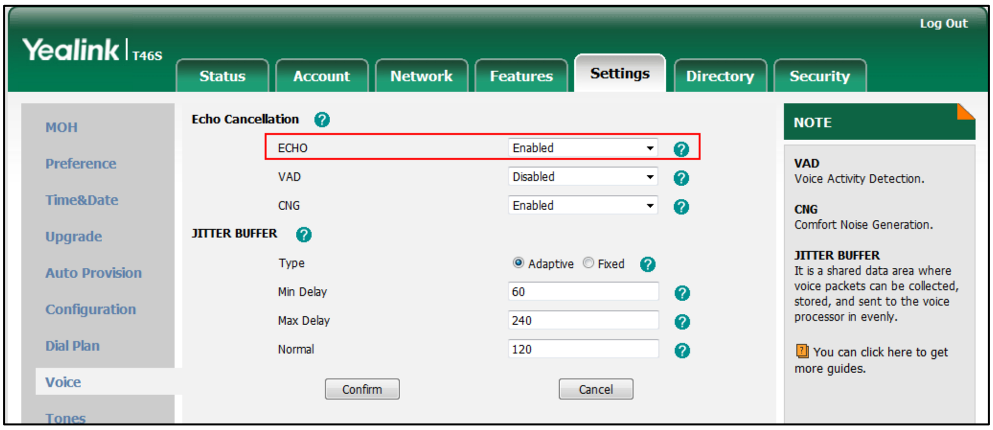
		Navigate to: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.echo_cancellation	**0 or 1**	**1**
Description: Enables or disables AEC (Acoustic Echo Canceller) feature on the phone. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Voice->Echo Cancellation->ECHO **Phone User Interface:** None		

To configure AEC via web user interface:

1. Click on **Settings**->**Voice**.
2. Select the desired value from the pull-down list of **ECHO**.



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

Background Noise Suppression (BNS)

Background noise suppression (BNS) is designed primarily for hands-free operation and reduces background noise to enhance communication in noisy environments.

Automatic Gain Control (AGC)

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

Voice Activity Detection (VAD)

Voice Activity Detection (VAD) is used in speech processing to detect the presence or absence of human speech. When detecting period of “silence”, VAD replaces that silence efficiently with special packets that indicate silence is occurring. It can facilitate speech processing, and deactivate some processes during non-speech section of an audio session. VAD can avoid unnecessary coding or transmission of silence packets in VoIP applications, saving on computation and network bandwidth.

Procedure

VAD can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure VAD. **Parameter:** voice.vad
Local	Web User Interface	Configure VAD. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

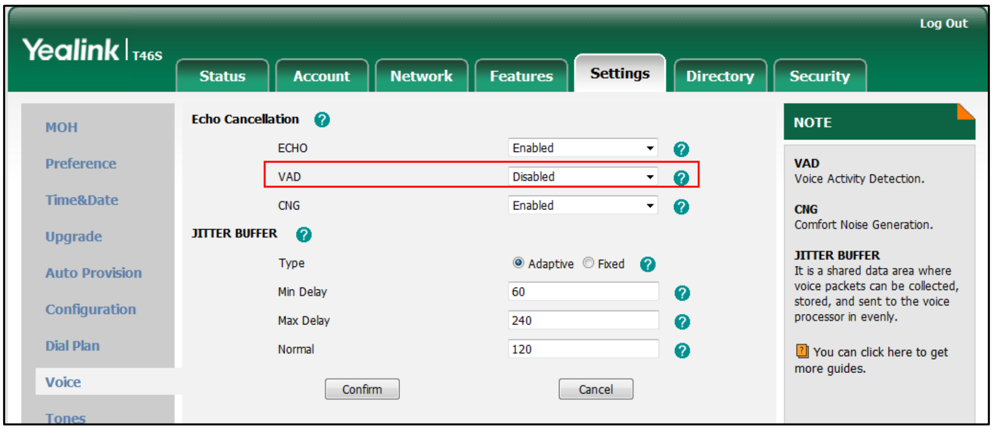
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.vad	**0 or 1**	**0**
Description: Enables or disables VAD (Voice Activity Detection) feature on the phone. **0**-Disabled **1**-Enabled **Web User Interface**: Settings->Voice->Echo Cancellation->VAD **Phone User Interface:**		

Parameter	Permitted Values	Default
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 configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure CNG. **Parameter:** voice.cng
Local	Web User Interface	Configure CNG. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

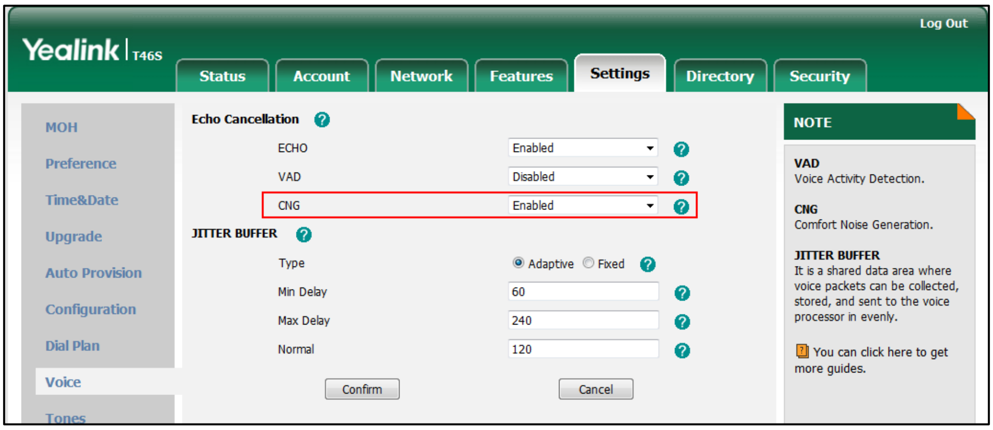
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.cng	**0 or 1**	**1**
Description: Enables or disables CNG (Comfortable Noise Generation) feature on the phone. **0**-Disabled **1**-Enabled **Web User Interface**: Settings->Voice->Echo Cancellation->CNG **Phone User Interface:** None		

To configure CNG via web user interface:

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

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



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

Jitter Buffer

Jitter buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in even intervals. Jitter is a term indicating variations in packet arrival time, which can occur because of network congestion, timing drift or route changes. The jitter buffer, located at the receiving end of the voice connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very little sound distortion. Skype for Business 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 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 phones.

Procedure

Jitter buffer can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the mode of jitter buffer and the delay time for jitter buffer. **Parameters:** voice.jib.adaptive voice.jib.min voice.jib.max voice.jib.normal
Local	Web User Interface	Configure the mode of jitter buffer and the delay time for jitter buffer.

		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. **0**-Fixed **1**-Adaptive **Web User Interface:** Settings->Voice->JITTER BUFFER->Type **Phone User Interface:** None		
voice.jib.min	**Integer from 0 to 400**	**60**
Description: Configures the minimum delay time (in milliseconds) of jitter buffer. **Note:** It works only if the value of the parameter "voice.jib.adaptive" is set to 1 (Adaptive). **Web User Interface:** Settings->Voice->JITTER BUFFER->Min Delay **Phone User Interface:** None		
voice.jib.max	**Integer from 0 to 400**	**240**
Description: Configures the maximum delay time (in milliseconds) of jitter buffer. **Note:** It works only if the value of the parameter "voice.jib.adaptive" is set to 1 (Adaptive). **Web User Interface:** Settings->Voice->JITTER BUFFER->Max Delay **Phone User Interface:** None		

Parameters	Permitted Values	Default
voice.jib.normal	**Integer from 0 to 400**	**120**
Description: Configures the normal delay time (in milliseconds) of jitter buffer. **Note:** It works only if the value of the parameter "voice.jib.adaptive" is set to 0 (Fixed). **Web User Interface:** Settings->Voice->JITTER BUFFER->Normal **Phone User Interface:** None		

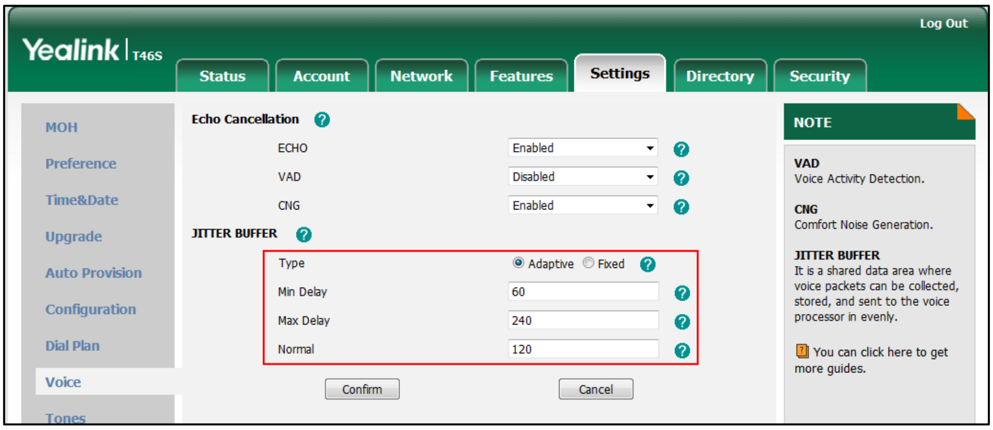
To configure Jitter Buffer via web user interface:

1. Click on **Settings**->**Voice**.
2. Mark the desired radio box in the **Type** field.
3. Enter the minimum delay time for adaptive jitter buffer in the **Min Delay** field.

   The valid value ranges from 0 to 300.
4. Enter the maximum delay time for adaptive jitter buffer in the **Max Delay** field.

   The valid value ranges from 0 to 300.
5. Enter the fixed delay time for fixed jitter buffer in the **Normal** field.

   The valid value ranges from 0 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 phone to the network, which is generated when pressing the phone's keypad during a call. Each key pressed on the phone generates one sinusoidal tone of two frequencies. One is generated from a high frequency group and the other from a low frequency group.

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

DTMF Keypad Frequencies:

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

Methods of Transmitting DTMF Digit

RFC 2833

DTMF digits are transmitted using the RTP Event packets that are sent along with the voice path. These packets use RFC 2833 format and must have a payload type that matches what the other end is listening for. The payload type for RTP Event packets is configurable. The default payload type for RTP Event packets is 101 and the payload type is configurable. The 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.

Procedure

Configuration changes can be performed using the configuration files or locally.

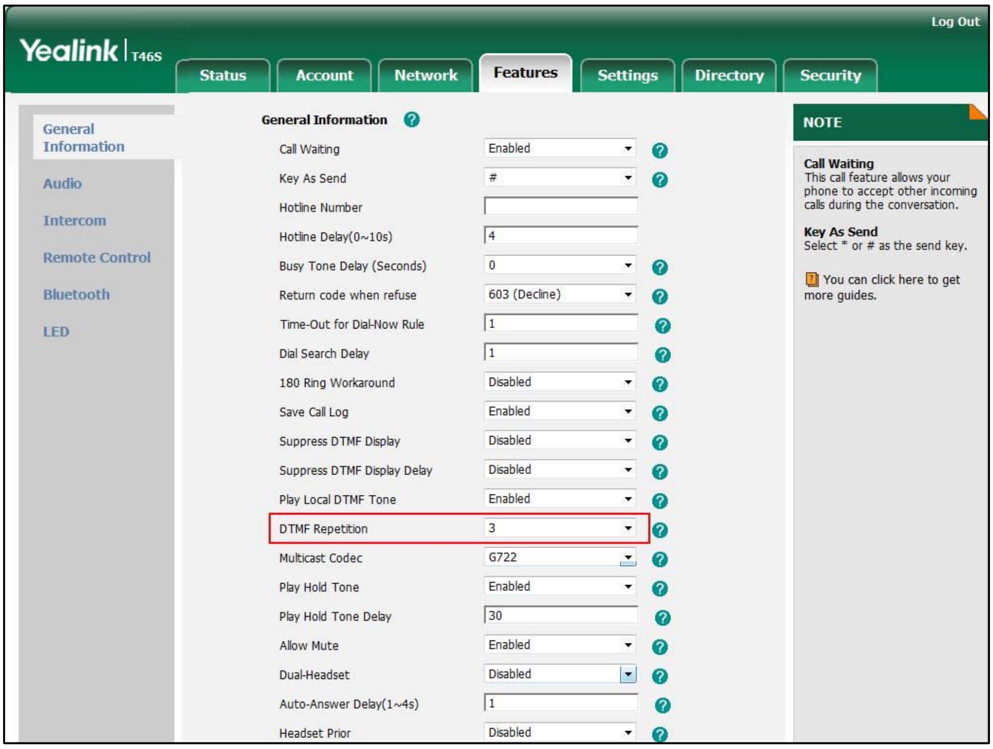
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the number of times for the phone to send the end RTP Event packet. **Parameter**: features.dtmf.repetition
Local	Web User Interface	Configure the number of times for the phone to send the end RTP Event packet. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.dtmf.repetition	**1, 2 or 3**	**3**
Description: Configures the repetition times for the phone to send the end RTP Event packet during an active call. **Web User Interface:** Features->General Information->DTMF Repetition **Phone User Interface:** None		

To configure the number of times to send the end RTP Event packet via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value (1-3) from the pull-down list of **DTMF Repetition**.



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

Suppress DTMF Display

Suppress DTMF display allows phones to suppress the display of DTMF digits during an active call. DTMF digits are displayed as "*" on the LCD screen/touch screen. Suppress DTMF display delay defines whether to display the DTMF digits for a short period of time before displaying as "*".

Procedure

Configuration changes can be performed using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure suppress DTMF display and suppress DTMF display delay. **Parameters:** features.dtmf.hide features.dtmf.hide_delay
Local	Web User Interface	Configure suppress DTMF display and suppress DTMF display delay. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

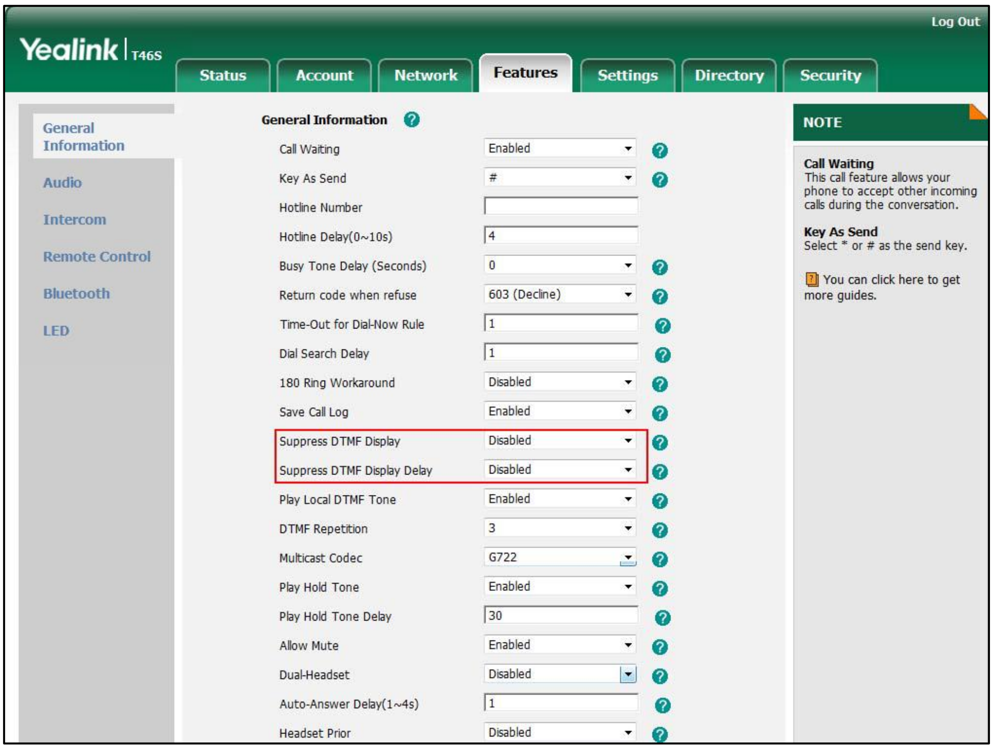
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.dtmf.hide	**0 or 1**	**0**
Description: Enables or disables the phone to suppress the display of DTMF digits during an active call. **0**-Disabled **1**-Enabled, the DTMF digits are displayed as asterisks. **Web User Interface:** Features->General Information->Suppress DTMF Display **Phone User Interface:** None		
features.dtmf.hide_delay	**0 or 1**	**0**
Description: Enables or disables the 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).		

Parameters	Permitted Values	Default
Web User Interface: Features->General Information->Suppress DTMF Display Delay **Phone User Interface:** None		

To configure suppress DTMF display and suppress DTMF display delay via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Suppress DTMF Display**.
3. Select the desired value from the pull-down list of **Suppress DTMF Display Delay**.



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

Transfer via DTMF

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

Procedure

Configuration changes can be performed using the configuration files or locally.

Central Provisioning	<y0000000000xx>.cfg	Configure transfer via DTMF.

(Configuration File)		**Parameters:** features.dtmf.replace_tran features.dtmf.transfer
Local	Web User Interface	Configure transfer via DTMF. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

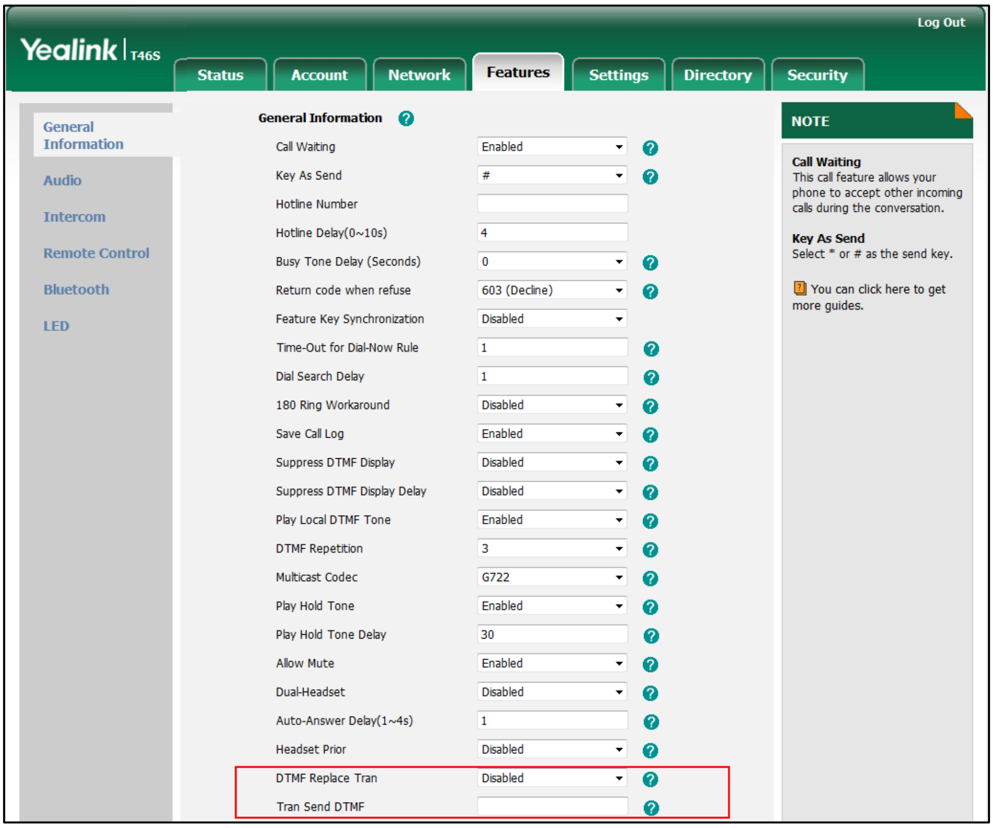
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.dtmf.replace_tran	**0 or 1**	**0**
Description: Enables or disables the phone to send DTMF sequences for transfer function when pressing a Transfer/Bind Transfer soft key or TRANSFER key. **0**-Disabled, the phone will perform the transfer as normal when pressing a Transfer/Bind Transfer soft key or TRANSFER key during a call. **1**-Enabled, the phone will transmit the designated DTMF digits to the server for performing call transfer when pressing t a Transfer/Bind Transfer soft key or TRANSFER key during a call. **Web User Interface:** Features->General Information->DTMF Replace Tran **Phone User Interface:** None		
features.dtmf.transfer	**String within 32 characters**	**Blank**
Description: Configures the DTMF digits to be transmitted to perform call transfer. Valid values are: 0-9, *, # and A-D. **Example:** features.dtmf.transfer = 123 **Note:** It works only if the value of the parameter "features.dtmf.replace_tran" is set to 1 (Enabled). **Web User Interface:** Features->General Information->Tran Send DTMF **Phone User Interface:**		

Parameters	Permitted Values	Default
None		

To configure transfer via DTMF via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **DTMF Replace Tran**.
3. Enter the specified DTMF digits in the **Tran Send DTMF** field.



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

Play Local DTMF Tone

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

Procedure

Configuration changes can be performed using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure play local DTMF tone. **Parameters:** features.play_local_dtmf_tone_enable
Local	Web User Interface	Configure play local DTMF tone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

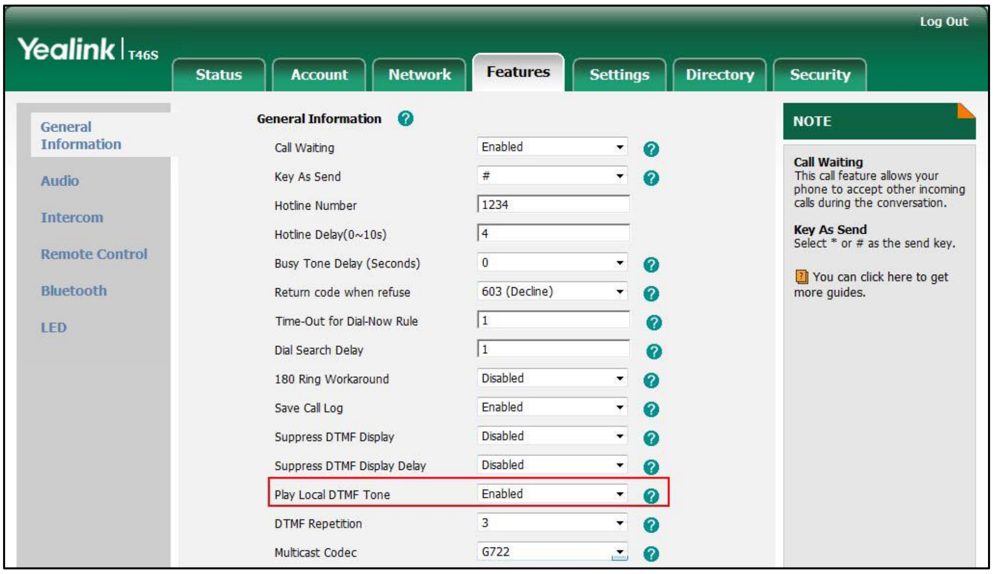
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.play_local_dtmf_tone_enable	**0 or 1**	**1**
Description: Enables or disables the phone to play a local DTMF tone during a call. **0**-Disabled **1**-Enabled, you can hear the DTMF tone when pressing the phone's keypad or onscreen dial pad during a call. **Web User Interface:** Features->General Information->Play Local DTMF Tone **Phone User Interface:** None		

To configure play local DTMF tone via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **Play Local DTMF Tone**.



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

Configuring Security Features

This chapter provides information for making configuration changes for the following security-related features:

- Skype for Business Feature License
- User and Administrator Passwords
- Auto-Logout Time
- Phone Lock
- Account Lock
- Transport Layer Security
- Encrypting Configuration Files

Skype for Business Feature License

By default, the phone has a built-in Skype for Business feature license, which allows user to use Yealink phones with Skype for Business features directly.

If users purchase phones which aren't running Skype for Business firmware, while the user wants to upgrade firmware to a Skype for Business firmware, then a Skype for Business feature license is needed to be uploaded to the phone after the update. Contact Yealink resellers to purchase the license.

Procedure

Skype for Business feature license can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the access URL of Skype for Business feature license. **Parameter:** lync_license_dat.url
Local	Web User Interface	Specify the access URL of Skype for Business feature license. **Navigate to:** http://<phoneIPAddress>/servlet?p=security-license&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
lync_license_dat.url	**String within 99 characters**	**Blank**
Description: Configures the access URL of the Skype for Business feature license. **Example:** lync_license_dat.url = http://192.168.1.20/License_$MAC.dat **Example:** The phones will replace the characters “$MAC” with its MAC addresses during auto provisioning. For example, the MAC address of one T46S Skype for Business phone is 00156543EC97. When performing auto provisioning, the phone will request to download the License_00156543ec97.dat file from the provisioning server address “http://192.168.1.20”. **Web User Interface:** Security->License **Phone User Interface:** None **Note:** If you change this parameter, the phone will reboot to make the change take effect.		

To upload the Skype for Business feature license via web user interface:

1. Click on **Security**->**License**.
2. Click **Browse** to select the license from your local system.

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

You can view the Skype for Business Server license status via web user interface. For more information, refer to Skype for Business Status on page 384.

User and Administrator Passwords

Some menu options are protected by two privilege levels, user and administrator, each with its own password. When logging into the web user interface, you need to enter the user name and password to access various menu options. The default user password is "user" and the default administrator password is "admin".

For security reasons, the user or administrator should change the default user or administrator password as soon as possible. A user or an administrator can change the user password. The administrator password can only be changed by an administrator.

Advanced menu options are strictly used by administrators. Users can configure them only if they have administrator privileges.

Procedure

User or administrator password can be changed using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Change the user or administrator password of the phone. **Parameter:** static.security.user_password
Local	Web User Interface	Change the user or administrator password of the phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=security&q=load
	Phone User Interface	Change the administrator password of the phone.

Details of the Configuration Parameter:

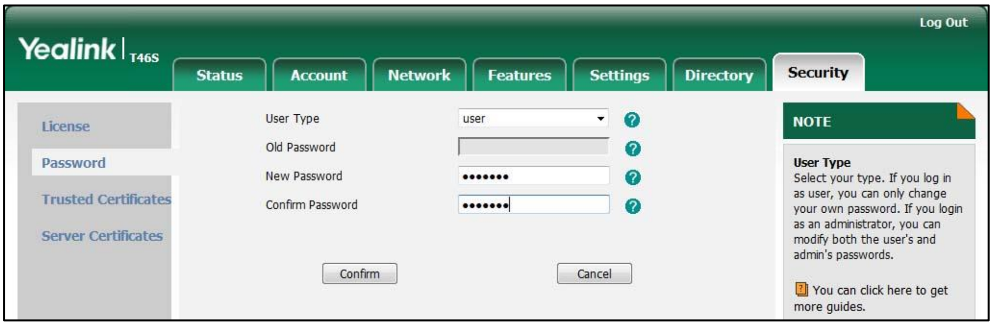
Parameter	Permitted Values	Default
static.security.user_password	**String within 32 characters**	**user**
Description: Configures the password of the user or administrator for phone's web user interface access. The phone uses "user" as the default user password and "admin" as the default administrator 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.		

Parameter	Permitted Values	Default
static.security.user_password = admin:456 means setting the password of administrator (current user name is "admin") to password 456. **Note**: Phones support ASCII characters 32-126(0x20-0x7E) in passwords. You can set the password to be empty via web user interface only. **Web User Interface:** Security->Password **Phone User Interface:** Menu->Advanced (default password: admin)->Set Password **Note**: You cannot change the user password via phone user interface.		

To change the user or administrator password via web user interface:

1. Click on **Security**->**Password**.
2. Select the desired value (**user** or **admin**) from the pull-down list of **User Type**.
3. Enter new password in the **New Password** and **Confirm Password** fields.

   Valid characters are ASCII characters 32-126(0x20-0x7E) except 58(3A).



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

Note

If logging into the web user interface of the phone with the user credential, you need to enter the old user password in the **Old Password** field.

To change the administrator password via phone user interface:

1. Press **Menu**-> **Advanced** (default password: admin) ->**Set Password**.
2. Enter the current administrator password in the **Current PWD** field.
3. Enter new password in the **New PWD** field and **Confirm PWD** field.

   Valid characters are ASCII characters 32-126(0x20-0x7E).

4. Press the **Save** soft key to accept the change.

Auto-Logout Time

Auto-logout time defines a specific period of time during which the 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 configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure auto-logout time. **Parameter**: features.relog_offtime
Local	Web User Interface	Configure auto-logout time. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

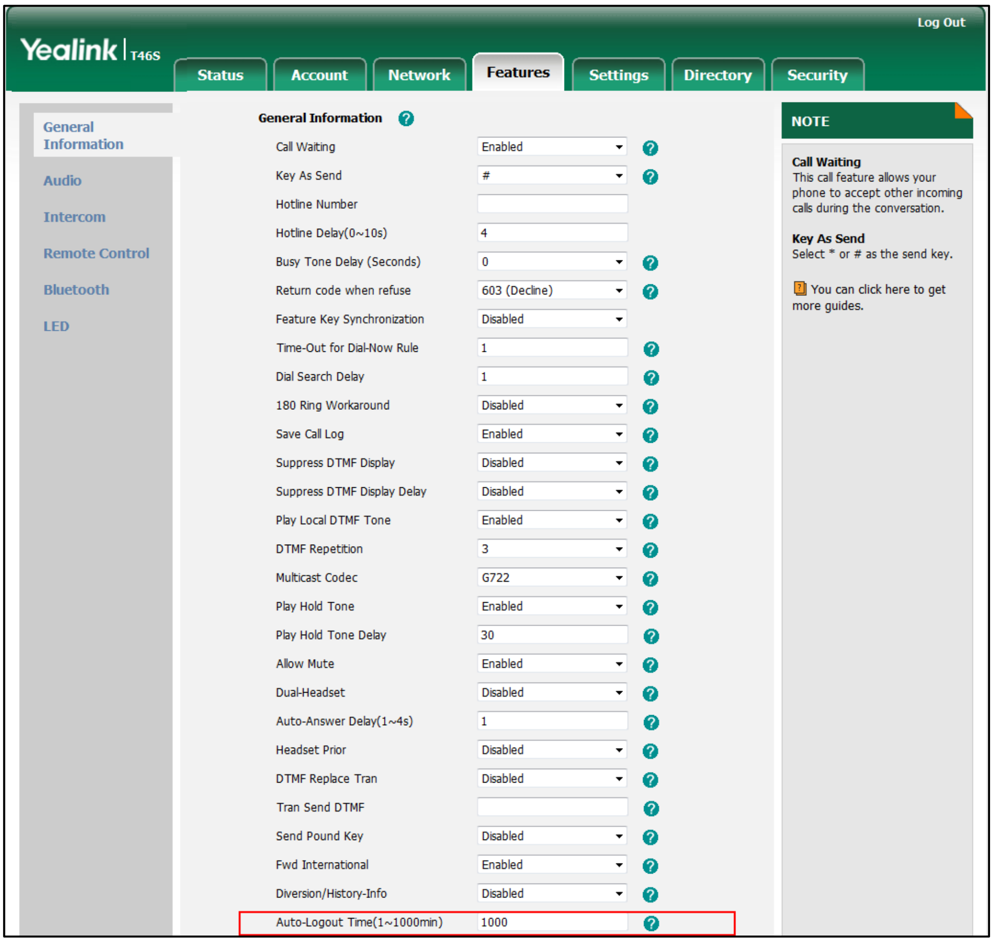
Details of the Configuration Parameter:

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. **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Features->General Information->Auto-Logout Time(1~1000min) **Phone 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.

Phone Lock

If system administrator sets the policy "ucEnforcePinLock" =true on the Skype for Business Fronted Server, user can use phone lock feature to lock the phone to prevent it from unauthorized use. And the phone will prompt the user to configure an n-digit lock PIN at the initial sign-in.

Procedure

Phone lock configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configures the time (in minutes) the phone can be idle before it automatically locks. **Parameter**: phone_setting.phone_lock.enable sfb.phone_lock.time_out

		Configures the unlock attempts. **Parameter**: sfb.phone_lock.max_attempts
		Configures the phone to be locked and unlocked automatically with the paired PC. sfb.phone_lock_with_pc.enable
		Configures the phone to be automatically signed out when you do not create a lock PIN when prompted. sfb.phone_lock.sign_out_auto.enable
Local	Web User Interface	Configures the time (in minutes) the phone can be idle before it automatically locks. Configures the unlock attempts. Configures the phone to be locked and unlocked automatically with the paired PC. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-phonelock&q=load
	Phone User Interface	Configures the time (in minutes) the phone can be idle before it automatically locks. Configures the unlock attempts. Configures the phone to be locked and unlocked automatically with the paired PC.

Details of Configuration Parameter:

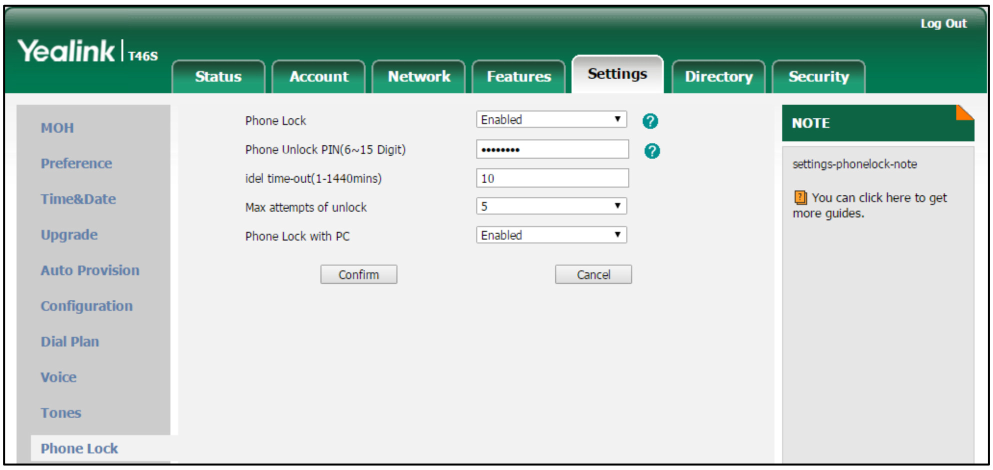
Parameters	Permitted Values	Default
phone_setting.phone_lock.enable	**0 or 1**	**0**
Enables or disables the phone lock feature. 0-Disabled 1-Enabled If it is set to 1 (Enabled), the IP phone will prompt the user to configure an n-digit unlock		

Parameters	Permitted Values	Default
PIN at the initial sign-in. **Web User Interface:** Settings->Phone Lock->Phone Lock **Phone User Interface:** Menu->Basic->Phone Lock->Phone Lock-		
sfb.phone_lock.time_out(CP960) **phone_setting.phone_lock.lock_time_out(T41S/T42S/T46S/T48S)**	**1 to 1440**	**10**
Configures the time (in minutes) the phone can be idle before it automatically locks. **Web User Interface:** Settings->Phone Lock->Idle time-out(1~1440mins) **Phone User Interface:** Menu->Basic->Phone Lock->Idle time-out		
sfb.phone_lock.max_attempts	**3 to 10**	**5**
Configures the maximum number of unsuccessful unlock attempts for a locked phone that is not during a call. You will be automatically signed out of the phone when the unsuccessful unlock attempts exceeds the limit. **Web User Interface:** Settings->Phone Lock->Max attempts of unlock **Phone User Interface:** Menu->Basic->Phone Lock->Unlock attempts		
sfb.phone_lock_with_pc.enable	**0 or 1**	**1**
Enables or disables your phone to be locked and unlocked automatically when you lock or unlock your computer. **0**-Enabled **1**-Disabled **Note**: It works only when your phone is paired with your computer using the BToE (Better Together over Ethernet) application and the BToE status is Paired (Sign In). It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Settings->Phone Lock->Phone Lock with PC **Phone User Interface:**		

Parameters	Permitted Values	Default
Menu->Basic->Phone Lock->Phone Lock with PC		
sfb.phone_lock.sign_out_auto.enable	**0 or 1**	**0**
Enables or disables the phone to be automatically signed out when you do not create a lock PIN within 5 minutes when prompted. **0**-Disabled **1**-Enabled **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		

To configure phone lock via web user interface:

1. Click on **Settings**->**Phone Lock**.
2. Select the **Enabled** from the pull-down list of **Phone Lock**.
3. Enter the lock PIN in the **Phone Unlock PIN(6~15 Digit)** field.
4. Enter the desired time in the **Idle time-out(1~1440mins)** field.
5. Select the desired value from the pull-down list of **Max attempts of unlock**.
6. Select the desired value from the pull-down list of **Phone Lock with PC**.



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

To configure phone lock via phone user interface:

1. Press **Menu**-> **Basic**->**Phone Lock**->**Phone Lock**.
2. Configures the desired fields.

3. Press the **Save** soft key to accept the change.

Account Lock

You can lock your account to prevent your account being signed in or signed out randomly. If account lock feature is enabled, users are prompted for administrator password to sign in or sign out. This feature is especially useful for public area telephone users.

Account lock is not applicable to CP960 Skype for Business phones.

Procedure

Account lock can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure account lock. **Parameters:** sfb.account_lock.enable
Local	Web User Interface	Configure account lock. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0
	Phone User Interface	Configure account lock.

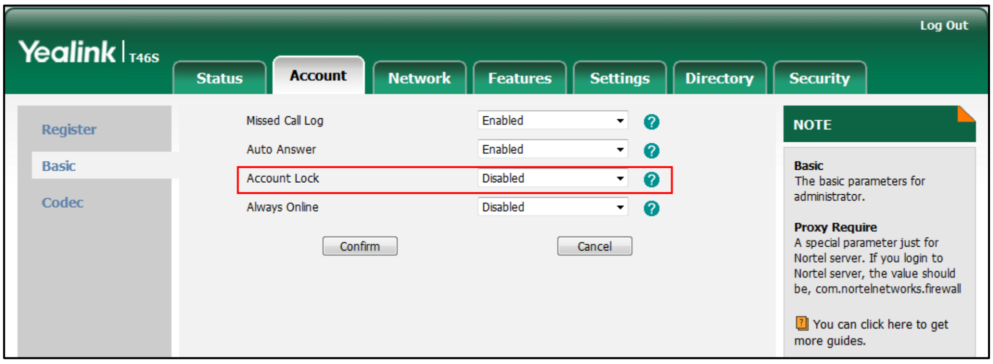
Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>sfb.account_lock.enable</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables the phone to lock the account to prevent the account being signed in or signed out randomly.
0-Disabled
1-Enabled, the phone needs an administrator password to sign in or sign out.
Note: It is not applicable to CP960 Skype for Business phones.
Web User Interface:
Account->Basic->Account Lock
Phone User Interface:
Menu->Advanced (default password: admin)->Account Lock</td></tr>
</table>

To configure account lock feature via web user interface:

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

2. Select the desired value from the pull-down list of **Account Lock**.



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

To configure the account lock feature via phone user interface:

1. Press **Menu**->**Advanced** (default password: admin) ->**Account Lock**.
2. Press or , or the **Switch** soft key to select **On** from the **Account Lock** field.
3. Press the **Save** soft key to accept the change.

Transport Layer Security

TLS is a commonly-used protocol for providing communications privacy and managing the security of message transmission, allowing Skype for Business 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.

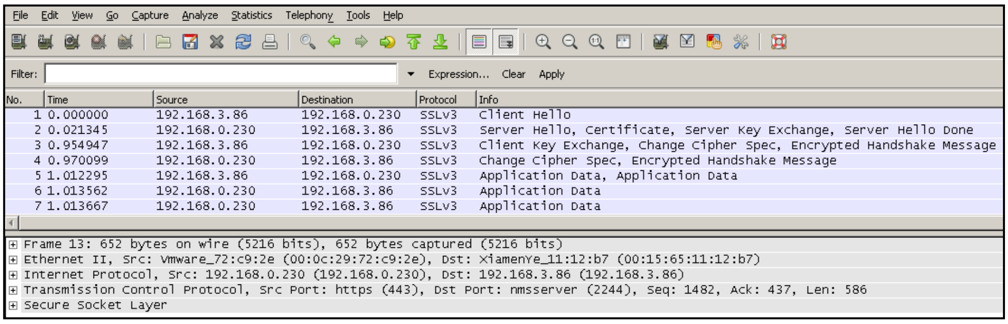
The TLS protocol uses asymmetric encryption for authentication of key exchange, symmetric encryption for confidentiality, and message authentication codes for integrity.

- **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.

Skype for Business 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. Skype for Business phones support the following cipher suites:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- AES256-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- DES-CBC3-MD5
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- RC2-CBC-MD5
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- RC6-64-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- DES-CBC-MD5
- EXP1024-DHE-DSS-RC4-SHA
- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC2-CBC-SHA
- EXP-RC4-MD5

The following figure illustrates the TLS messages exchanged between the Skype for Business phone and TLS server to establish an encrypted communication channel:



Step1: Skype for Business 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: Skype for Business 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.

Skype for Business 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/touch screen after the successful TLS negotiation.

Certificates

The Skype for Business 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 Skype for Business phone requests a TLS connection with a server, the Skype for Business phone should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The Skype for Business phone has 51 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 51 built-in trusted certificates, refer to Appendix C: Trusted Certificates on page 436.
- **Server Certificate**: When clients request a TLS connection with the Skype for Business phone, the Skype for Business phone sends the server certificate to the clients for authentication. The Skype for Business 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 Skype for Business 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 a Skype for Business 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 Skype for Business phone may send a generic certificate for authentication.

The Skype for Business 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 Skype for Business phone accepts: default certificates, custom certificates or all certificates.

Common Name Validation feature enables the Skype for Business 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 Skype for Business 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 configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure trusted certificates feature. **Parameters:** static.security.trust_certificates static.security.ca_cert static.security.cn_validation
		Configure server certificates feature. **Parameters:** 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_enabl e
Local	Web User Interface	Configure trusted certificates feature. Upload the trusted certificates. **Navigate to**: http://<phoneIPAddress>/servlet?p=tru sted-cert&q=load
		Configure server certificates feature. Upload the server certificates. **Navigate to**: http://<phoneIPAddress>/servlet?p=ser ver-cert&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.security.trust_certificates	**0 or 1**	**1**
Description: Enables or disables the phone to only trust the server certificates in the Trusted Certificates list. **0**-Disabled, the phone will trust the server no matter whether the certificate sent by the server is valid or not. **1**-Enabled, the phone will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, the phone will trust the server. **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Security->Trusted Certificates->Only Accept Trusted Certificates **Phone User Interface:** None		
static.security.ca_cert	**0, 1 or 2**	**2**

Parameters	Permitted Values	Default
Description: Configures the type of certificates in the Trusted Certificates list for the Skype for Business phone to authenticate for TLS connection. **0**-Default Certificates **1**-Custom Certificates **2**-All Certificates **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Security->Trusted Certificates->CA Certificates **Phone User Interface:** None		
static.security.cn_validation	**0 or 1**	**0**
Description: Enables or disables the Skype for Business 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 phone will reboot to make the change take effect. **Web User Interface:** Security->Trusted Certificates->Common Name Validation **Phone User Interface:** None		
static.security.dev_cert	**0 or 1**	**0**
Description: Configures the type of the device certificates for the Skype for Business phone to send for TLS authentication. **0**-Default Certificates **1**-Custom Certificates **Note:** If you change this parameter, the phone will reboot to make the change take effect. **Web User Interface:** Security->Server Certificates->Device Certificates **Phone User Interface:**		

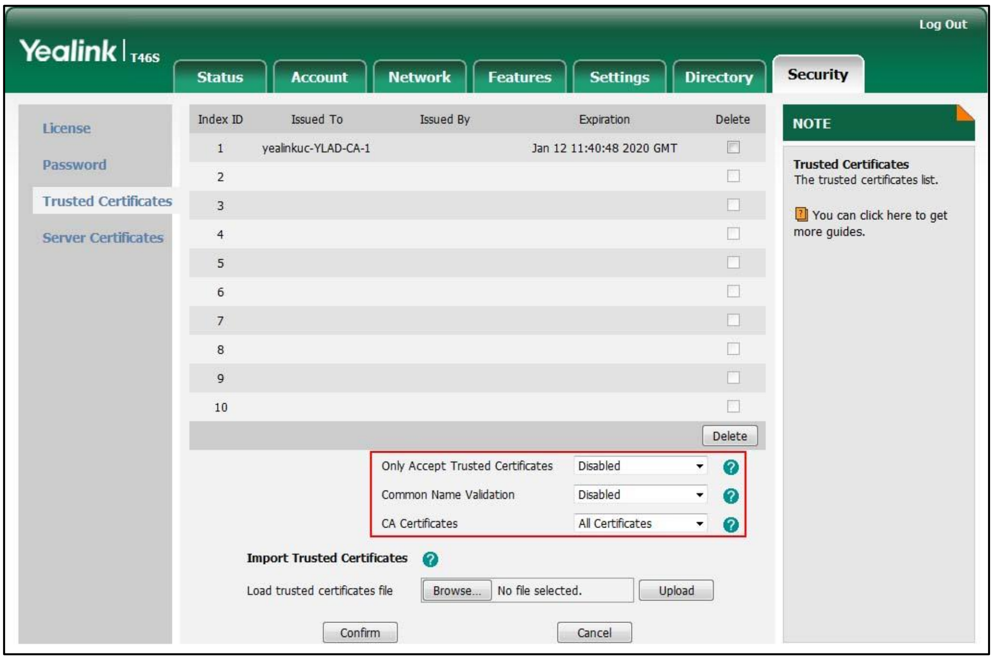
Parameters	Permitted Values	Default
None		
static.trusted_certificates.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom trusted certificate used to authenticate the connecting server. **Example:** static.trusted_certificates.url = http://192.168.1.20/tc.crt **Note:** The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format. **Web User Interface:** Security->Trusted Certificates->Load trusted certificates file **Phone User Interface:** None		
static.trusted_certificates.delete	**http://localhost/all**	**Blank**
Description: Deletes all uploaded trusted certificates. **Example:** static.trusted_certificates.delete = http://localhost/all **Web User Interface:** None **Phone User Interface:** None		
static.server_certificates.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the certificate the 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		

Parameters	Permitted Values	Default
Phone User Interface: None		
static.server_certificates.delete	**http://localhost/all**	**Blank**
Description: Deletes all uploaded server certificates. **Example:** static.server_certificates.delete = http://localhost/all **Web User Interface:** None **Phone User Interface:** None		
static.phone_setting.reserve_certs_enable	**0 or 1**	**0**
Description: Enables or disables the phone to reserve custom certificates after it is reset to factory defaults. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		

To configure the trusted certificates via web user interface:

1. Click on **Security**->**Trusted Certificates**.

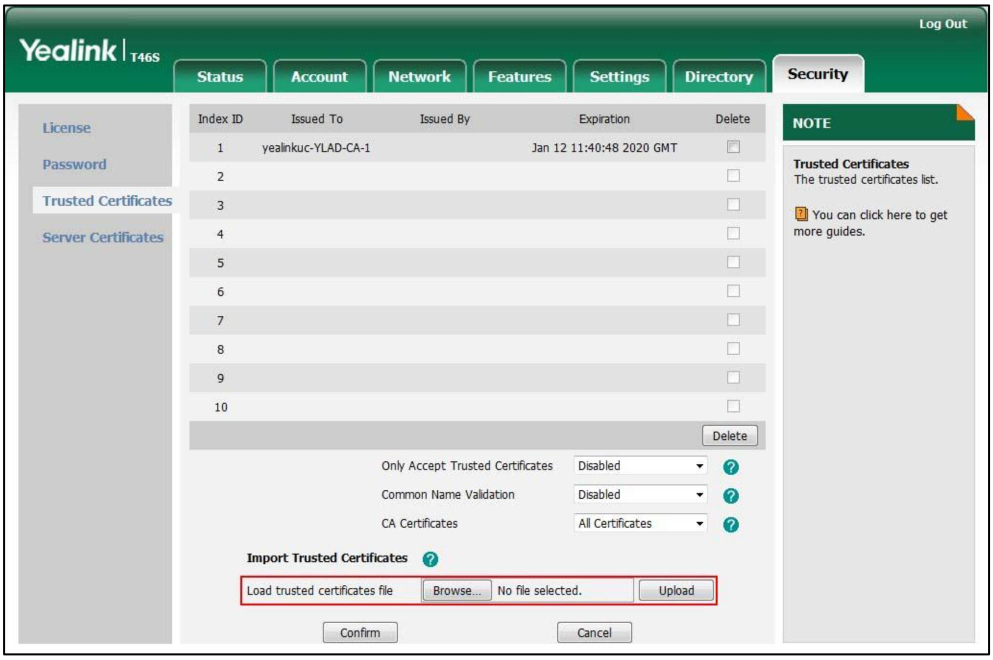
2. Select the desired values from the pull-down lists of **Only Accept Trusted Certificates**, **Common Name Validation** and **CA Certificates**.



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

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.

   A dialog box pops up to prompt "Success: The Server Certificate has been loaded! Rebooting, please wait...".

Encrypting 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 <y0000000000xx>.cfg and <MAC>.cfg files (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. This tool also encrypts the plaintext 16-character symmetric keys using a fixed key, which is the same as the one built in the phone, and generates new files named as <xx_Security>.enc (xx indicates the name of the configuration file, for example, y000000000066_Security.enc for y000000000066.cfg file). 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 <y0000000000xx>.cfg and <MAC>.cfg 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, <y0000000000xx_Security>.enc and/or <MAC_Security>.enc files to the root directory of the provisioning server. During auto provisioning, the phone requests to download <y0000000000xx>.cfg file first. If the downloaded configuration file is encrypted, the phone will request to download <y0000000000xx_Security>.enc file (if enabled) and decrypt it into the plaintext key (e.g., key2) using the built-in key (e.g., key1). Then the phone decrypts <y0000000000xx>.cfg file using key2. After decryption, the phone resolves configuration files and updates configuration settings onto the phone system.

The way the phone processes the <MAC>.cfg file is the same to that of the<y0000000000xx>.cfg file.

Procedure to Encrypt Configuration Files

To encrypt the <y0000000000xx>.cfg file:

1. Double click "Config_Encrypt_Tool.exe" to start the application tool.

   The screenshot of the main page is shown as below:

   When you start the application tool, a file folder named "Encrypted" is created automatically in the directory where the application tool is located.

2. Click **Browse** to locate configuration file(s) (e.g., y000000000066.cfg) from your local system in the **Select File(s)** field.

   To select multiple configuration files, you can select the first file and then press and hold the **Ctrl** key and select the next files.

3. (Optional.) Click **Browse** to locate the target directory from your local system in the

Target Directory field.

The tool uses the file folder "Encrypted" as the target directory by default.

4. (Optional.) Mark the desired radio box in the **AES Model** field.

   If you mark the **Manual** radio box, you can enter an AES key in the **AES KEY** field or click **Re-Generate** to generate an AES key in the **AES KEY** field. The configuration file(s) will be encrypted using the AES key in the **AES KEY** field.

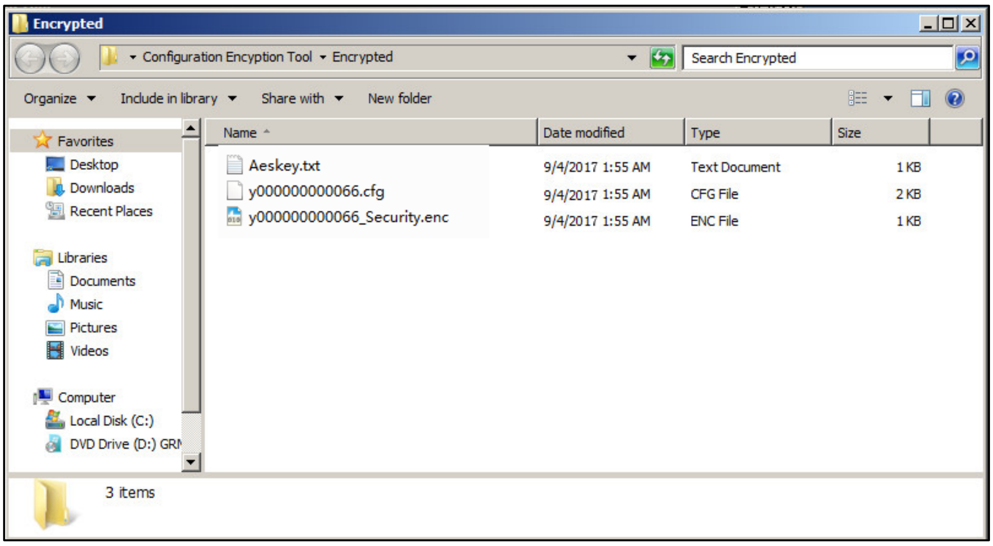
   If you mark the **Auto Generate** radio box, the configuration file(s) will be encrypted using random AES key. The AES keys of configuration files are different.

Note AES keys must be 16 characters and the supported characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ { } ~.

5. Click **Encrypt** to encrypt the configuration file(s).

6. Click **OK**.

The target directory will be automatically opened. You can find the encrypted CFG file(s), encrypted key file(s) and an Aeskey.txt file storing plaintext AES key(s).



Procedure

AES keys can be configured using the configuration files.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	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
Local	Web User Interface	Configure AES keys. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-autop&q=load
	Phone User Interface	Configure AES keys.

Details of Configuration Parameters:

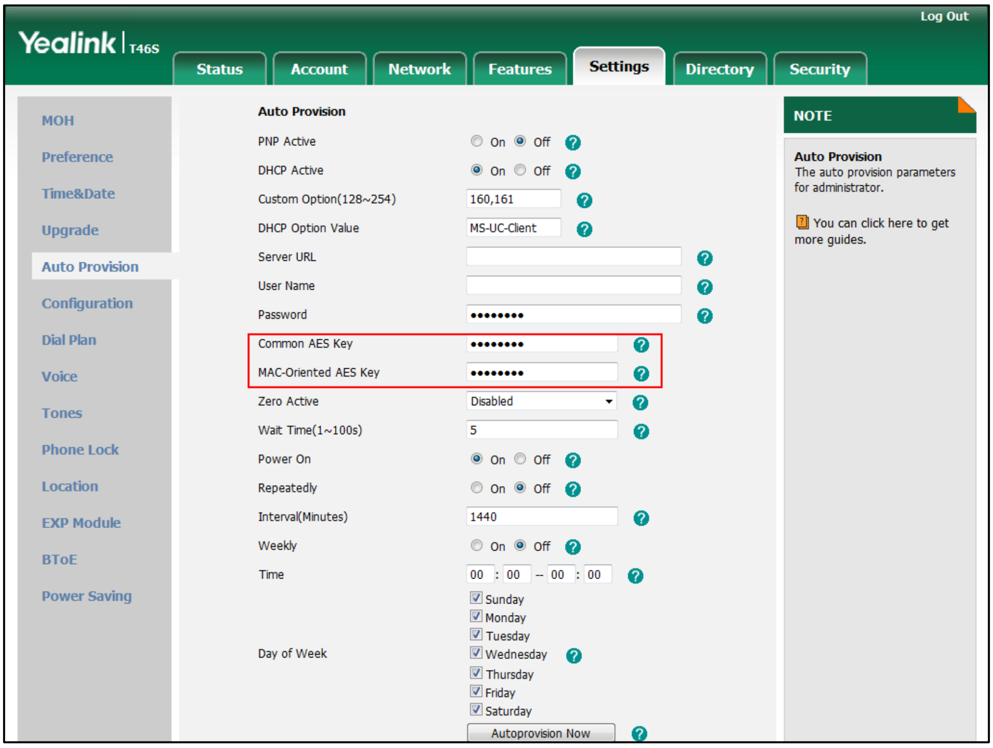
Parameters	Permitted Values	Default
static.auto_provision.aes_key_in_file	**0 or 1**	**0**
Description: Enables or disables the phone to decrypt configuration files using the encrypted AES keys. **0**-Disabled, the phone will decrypt the encrypted configuration files using plaintext AES keys configured on the phone. **1**-Enabled, the phone will download <xx_Security>.enc files (for example, <sip_Security>.enc, <account_Security>.enc) during auto provisioning, and then decrypts these files into the plaintext keys (for example, key2, key3) respectively using the phone built-in key (for example, key1). The phone then decrypts the encrypted configuration files using corresponding key (for example, key2, key3). **Web User Interface:** None **Phone User Interface:** None		
static.auto_provision.aes_key_16.com	**16 characters**	**Blank**
Description:		

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">Configures the plaintext AES key for decrypting the Common CFG file.
The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ _ { } ~.
Example:
static.auto_provision.aes_key_16.com = 0123456789abcdef
Web User Interface:
Settings->Auto Provision->Common AES Key
Phone User Interface:
For T48S/T46S/T42S/T41S: Menu->Advanced ->Set AES Key->Common
For CP960: More->Advanced->Auto Provision->Common AES</td></tr>
<tr><td>static.auto_provision.aes_key_16.mac</td><td>16 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the plaintext AES key for decrypting the MAC-Oriented CFG file.
The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ _ { } ~.
Example:
static.auto_provision.aes_key_16.mac = 0123456789abmins
Web User Interface:
Settings->Auto Provision->MAC-Oriented AES Key
Phone User Interface:
For T48S/T46S/T42S/T41S: Menu-> Advanced ->Set AES Key->MAC-Oriented
For CP960: More->Advanced ->Auto Provision->MAC-Oriented AES</td></tr>
</table>

To configure AES keys via web user interface:

1. Click on **Settings**->**Auto Provision**.
2. Enter the values in the **Common AES Key** and **MAC-Oriented AES Key** fields.

AES keys must be 16 characters and the supported characters contain: 0-9, A-Z, a-z and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ _ { } ~.



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

To configure AES keys via phone user interface:

1. Press **Menu**->**Advanced** (default password: admin) ->**Set AES Key**.
2. Enter the values in the **Common** and **MAC-Oriented** 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. Press the **Save** soft key to accept the change.

Troubleshooting

This chapter provides an administrator with general information for troubleshooting some common problems that he (or she) may encounter while using phones.

Troubleshooting Methods

Skype for Business 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 phone.

- Memory Information
- Skype for Business Status
- Log Files
- Capturing Packets
- Enabling Watch Dog Feature
- Getting Information from Status Indicators
- Analyzing Configuration Files
- Exporting All the Diagnostic Files

Memory Information

You can understand phone process, memory occupancy and CPU utility via the web user interface.

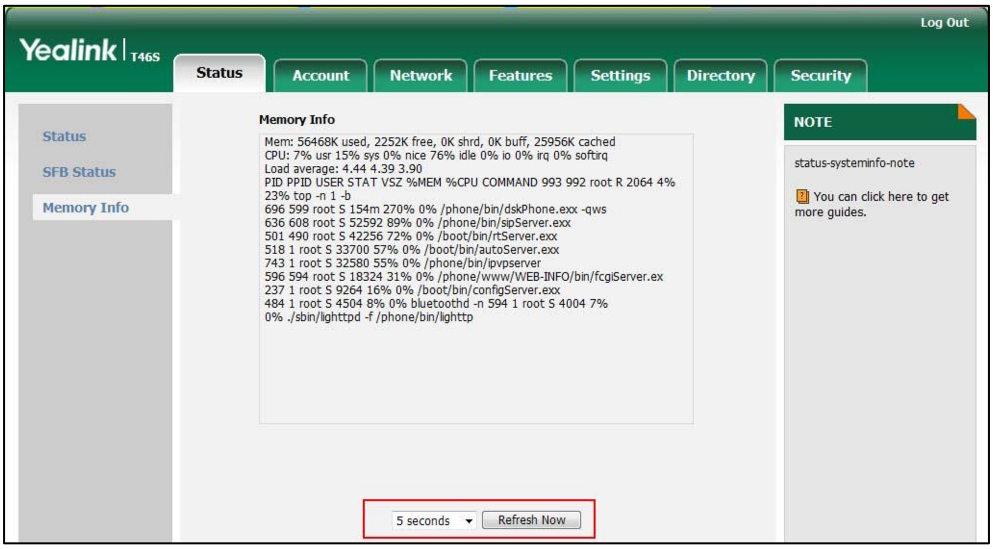
Procedure

Memory information can be configured locally.

Local	Web User Interface	Configure memory information feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=status-systeminfo&q=load

To configure memory information via web user interface:

1. Click on **Status**->**Memory Info**.
2. Select the desired refresh interval from the pull-down list.
3. If **Disabled** is selected, the page will not be refreshed.



4. Click **Refresh Now** to refresh the page and accept the change.

Skype for Business Status

You can troubleshoot phone issues by viewing the Skype for Business status.

To view Skype for Business status via web user interface:

1. Click on **Status**->**SFB Status**.

Status	Display Name	Description
License	License Status	Indicates whether the Skype for Business feature license is imported to your phone. Values: • Installed • None
	Expire Date	Validity period of the license.
Authentication info	User Type	Indicates the account type. Values: • UNKNOW • PIN • ONPREM

Status	Display Name	Description
		● MANAGED ● FEDERATED
	SIP Authentication	Indicates the SIP authentication type. Values: ● UNSET ● NTLM ● KERBEROS ● NEGOTIATE ● TLS_DSK
	Sign-in Authentication Type	Indicates the Sign-in authentication type. Values: ● NONE ● ORG_ID ● OAUTH ● NTLM ● DEV_PAIRING ● BASIC ● CACHE ● CERT ● ALL_METHOD
	Exchange Authentication Type	Indicates the Exchange authentication type. Values: ● NONE ● ORG_ID ● OAUTH ● NTLM ● DEV_PAIRING ● BASIC ● CACHE ● CERT ● ALL_METHOD
Server Status	Update Server URL	Indicates the Updates Server URL.

Status	Display Name	Description
	Edge Server	Indicates the Edge Server address.
	Voice Mail URI	Indicates the Voice Mail URI of your account
	Email URI	Indicates the Email URI of your account
	ABS URL	Indicates the ABS (Address Book Server) URL
	LIS URL	Indicates the LIS URL for obtaining address information
	STS URI	Indicates the URI of the Security token service.
	Focus Factory URI	Indicates the URI of the Focus Factory.
	Home Server URL	Indicates the URL of the Home server.
	MRAS URL	Indicates the URL of the Media Relay Authentication Service.
	CallPark Server URI	Indicates the CallPark Server URI.
QoE	QoE Status	Indicates the QOE status
	QoE URI	Indicates the address where to send Quality of Experience (QoE) report.
	In-Call QoE Status	Indicates the QOE status during a call.
	In-Call QoE Interval	Indicates the interval the phone sends Quality of Experience (QoE) report to the server during a call.
BToE (not applicable to CP960)	BToE Status	Indicates whether the BToE feature is enabled
	Pairing Mode	Indicates the BToE paring mode. ● Auto ● Manually
	Pairing Status	Indicates the BToE paring status.
Hot desking	Hot desking Status	Indicates whether the phone is in hot-desking mode.
	Hot desking Time out	Indicates the idle time (in seconds) before the phone exit the hot-desking mode automatically.
	CAP Status	Indicates whether the phone is in CAP (common area phone) mode.
Features Status	Simultaneous ringing	Indicates whether the simultaneous ringing

Status	Display Name	Description
		feature is enabled
	Call forwarding	Indicates whether the call forwarding feature is enabled
	Call Park	Indicates whether the call park feature is enabled
	Call transfer	Indicates whether the call transfer feature is enabled
	Delegation	Indicates whether the Delegation (assign a delegate or being assigned to be a delegate) feature is enabled.
	Teamcall	Indicates whether the Teamcall (your phone and your team-call group will ring simultaneously when you receive a call) feature is enabled
Data	Calendar Number	Indicates the total number of calendars downloaded from the server.
	Contact Number	Indicates the total number of your Skype for Business contacts.
	Outlook Contacts Number	Indicates the total number of your Outlook contacts.
	Calllog Number	Indicates the total number of call logs downloaded from the server.
	Visual Voicemail Number	Indicates the total number of voice mails downloaded from the server.
Exchange	Calendar Status	Indicates whether the Exchange calendar feature is enabled. If it is enabled, calendar on the phone is synchronized with the Exchange server.
	Contact Status	Indicates whether to download Outlook contact from the Exchange server to the phone.
	Calllog Status	Indicates whether the Exchange call log feature is enabled. If it is enabled, call logs on the phone are synchronized with the Exchange server.

Status	Display Name	Description
	VoiceMail Status	Indicates whether the Exchange voice mail feature is enabled. If it is enabled, user can retrieve voicemails stored on the Exchange server
	EWS URL	Indicates the Microsoft Exchange server address.

Log Files

If your 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 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 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 Log

Procedure

Local log can be configured using the configuration files or locally.

<table>
<tr><td rowspan="4">Central Provisioning (Configuration File)</td><td rowspan="4"><y0000000000xx>.cfg</td><td>Configure Local log feature.
Parameter:
static.local_log.enable</td></tr>
<tr><td>Configure the severity level of the logs to be reported to the <MAC>-sys.log file.
Parameter:
static.local_log.level</td></tr>
<tr><td>Configure the maximum size of the log files to be stored on the phone.
Parameter:
static.local_log.max_file_size</td></tr>
<tr><td>Configure the maximum size of the local log</td></tr>
</table>

		files to be stored on the server. **Parameter:** static.auto_provision.local_log.backup.append.max_file_size
		Configure the 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 log feature. **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 phone to record log to the log files locally. **0**-Disabled, the phone will stop recording log to the log files (<MAC>-boot.log and <MAC>-sys.log) locally. The log files recorded before are still kept on the phone. **1**-Enabled, the phone will continue to record log to the log files (<MAC>-boot.log and <MAC>-sys.log) locally. You can upload the local log files to the provisioning server or a specific server or export them to the local system. **Note**: We recommend you not to disable this feature. **Web User Interface:** Settings->Configuration->Local Log Switch **Phone User Interface:** None		
static.local_log.level	**Integer from 0 to 6**	**6**
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		

Parameters		Permitted Values	Default
Web User Interface: Settings->Configuration->Local Log Level **Phone User Interface:** None			
static.local_log.max_file_size	**Refer to the following content**		**Refer to the following content**
Description: Configures the maximum size (in KB) of the log files (<MAC>-boot.log and <MAC>-sys.log) to be stored on the 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 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 phone will erase half of the logs from the oldest log information on the phone. **Permitted Values**: Integer from 1 kb to 1024 kb (for T42S/T41S) Integer from 1 kb to 3072 kb (for T46S) Integer from 1 kb to 5120 kb (for T48S/CP960) **Default Values**: 1024 kb for T46S/T42S/T41S 5120 kb for T48S/CP960 **Example:** static.local_log.max_file_size = 1024 **Web User Interface:** Settings->Configuration->Max Log File Size **Phone User Interface:** None			
static.auto_provision.local_log.backup.enable		**0 or 1**	**0**
Description: Enables or disables the phone to upload the local log files (<MAC>-boot.log and <MAC>-sys.log) to the provisioning server or a specific server. **0**-Disabled			

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">1-Enabled, the phone will upload the local log files to the provisioning server or the specific server to back up these files when one of the following happens:
- 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:
Settings->Configuration->Enable log backup
Phone User Interface:
None</td></tr>
<tr><td>static.auto_provision.local_log.backup.path</td><td>URL within 1024 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the upload path of the local log files (<MAC>-boot.log and <MAC>-sys.log).
If you leave it blank, the phone will upload the local log files to the provisioning server.
If you configure a relative URL (e.g., /upload), the 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 phone will upload the local log files using the desired protocol. If no protocol, the phone will use the same protocol with auto provisioning for uploading files.
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:
Settings->Configuration->Backup Server URL
Phone User Interface:
None</td></tr>
<tr><td>static.auto_provision.local_log.backup.upload_period</td><td>Integer from 30 to 86400</td><td>180</td></tr>
<tr><td colspan="3">Description:
Configures the period (in seconds) of the local log files (<MAC>-boot.log and <MAC>-</td></tr>
</table>

Parameters	Permitted Values	Default
sys.log) uploads to the provisioning server or a specific server. **Example:** static.auto_provision.local_log.backup.upload_period = 180 **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:** Settings->Configuration->Log backup interval **Phone 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:** Settings->Configuration->Backup Mode **Phone User Interface:** None		
static.auto_provision.local_log.backup.append.max_file_size	**Integer from 200 to 65535**	**1024**
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 = 1024 **Web User Interface:** Settings->Configuration->Max size for backup log **Phone User Interface:** None		
static.auto_provision.local_log.backup.append.limit_mode	**0 or 1**	**0**

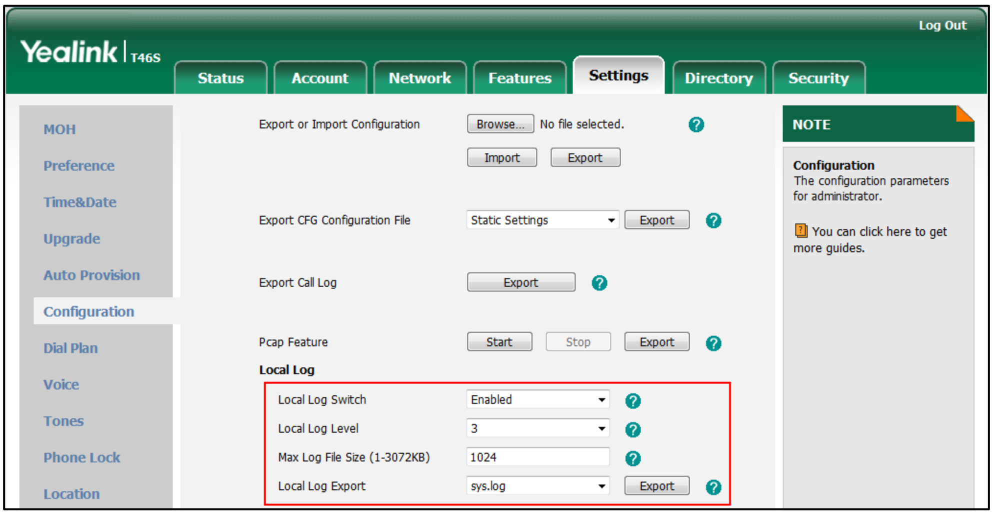
Parameters	Permitted Values	Default
Description: Configures the behavior when local log files (<MAC>-boot.log and <MAC>-sys.log) on the provisioning server or a specific server reach the maximum size. **0**-Append Delete, the server will delete the old log and the phone will continue to uploading log. **1**-Append Stop, the phone will stop uploading log. **Web User Interface:** Settings->Configuration->Backup limit mode **Phone User Interface:** None		
static.auto_provision.local_log.backup.bootlog.upload_wait_time	**Integer from 1 to 86400**	**120**
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:** Settings->Configuration->Bootlog backup time **Phone 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 **Local Log Switch**.
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.

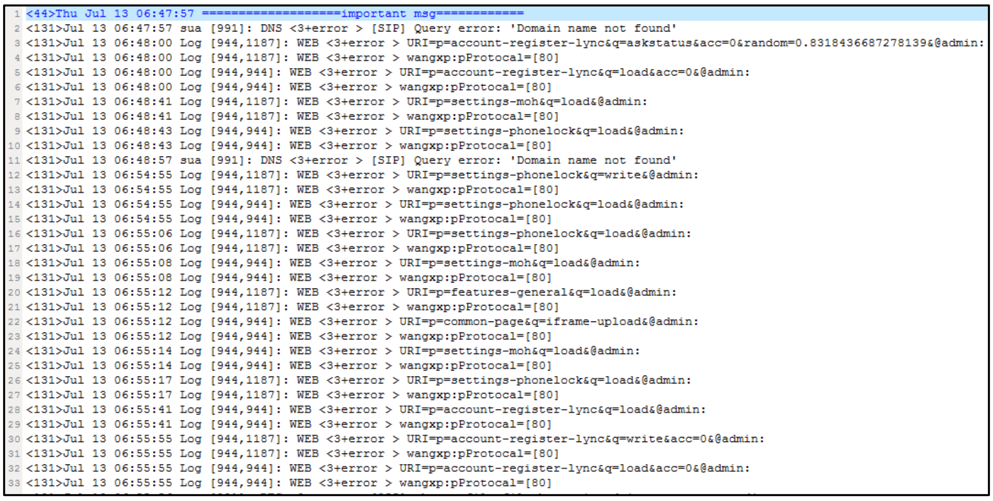


7. Reproduce the issue.

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

To view the syslog files on your local system:

The following figure shows a portion of a <MAC>-sys.log (e.g., 00156574b150-sys.log):



```
<44>Thu Jul 13 06:47:57 ===================important msg============
<131>Jul 13 06:47:57 sua [991]: DNS <3+error > [SIP] Query error: 'Domain name not found'
<131>Jul 13 06:48:00 Log [944,1187]: WEB <3+error > URI=p=account-register-lync&q=askstatus&acc=0&random=0.8318436687278139&@admin:
<131>Jul 13 06:48:00 Log [944,1187]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:48:00 Log [944,944]: WEB <3+error > URI=p=account-register-lync&q=load&acc=0&@admin:
<131>Jul 13 06:48:00 Log [944,944]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:48:41 Log [944,1187]: WEB <3+error > URI=p=settings-moh&q=load&@admin:
<131>Jul 13 06:48:41 Log [944,1187]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:48:43 Log [944,944]: WEB <3+error > URI=p=settings-phonelock&q=load&@admin:
<131>Jul 13 06:48:43 Log [944,944]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:48:57 sua [991]: DNS <3+error > [SIP] Query error: 'Domain name not found'
<131>Jul 13 06:54:55 Log [944,1187]: WEB <3+error > URI=p=settings-phonelock&q=write&@admin:
<131>Jul 13 06:54:55 Log [944,1187]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:54:55 Log [944,944]: WEB <3+error > URI=p=settings-phonelock&q=load&@admin:
<131>Jul 13 06:54:55 Log [944,944]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:55:06 Log [944,1187]: WEB <3+error > URI=p=settings-phonelock&q=load&@admin:
<131>Jul 13 06:55:06 Log [944,1187]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:55:08 Log [944,944]: WEB <3+error > URI=p=settings-moh&q=load&@admin:
<131>Jul 13 06:55:08 Log [944,944]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:55:12 Log [944,1187]: WEB <3+error > URI=p=features-general&q=load&@admin:
<131>Jul 13 06:55:12 Log [944,1187]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:55:12 Log [944,944]: WEB <3+error > URI=p=common-page&q=iframe-upload&@admin:
<131>Jul 13 06:55:12 Log [944,944]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:55:14 Log [944,944]: WEB <3+error > URI=p=settings-moh&q=load&@admin:
<131>Jul 13 06:55:14 Log [944,944]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:55:17 Log [944,1187]: WEB <3+error > URI=p=settings-phonelock&q=load&@admin:
<131>Jul 13 06:55:17 Log [944,1187]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:55:41 Log [944,944]: WEB <3+error > URI=p=account-register-lync&q=load&@admin:
<131>Jul 13 06:55:41 Log [944,944]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:55:55 Log [944,1187]: WEB <3+error > URI=p=account-register-lync&q=write&acc=0&@admin:
<131>Jul 13 06:55:55 Log [944,1187]: WEB <3+error > wangxp:pProtocal=[80]
<131>Jul 13 06:55:55 Log [944,944]: WEB <3+error > URI=p=account-register-lync&q=load&acc=0&@admin:
<131>Jul 13 06:55:55 Log [944,944]: WEB <3+error > wangxp:pProtocal=[80]
```

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.

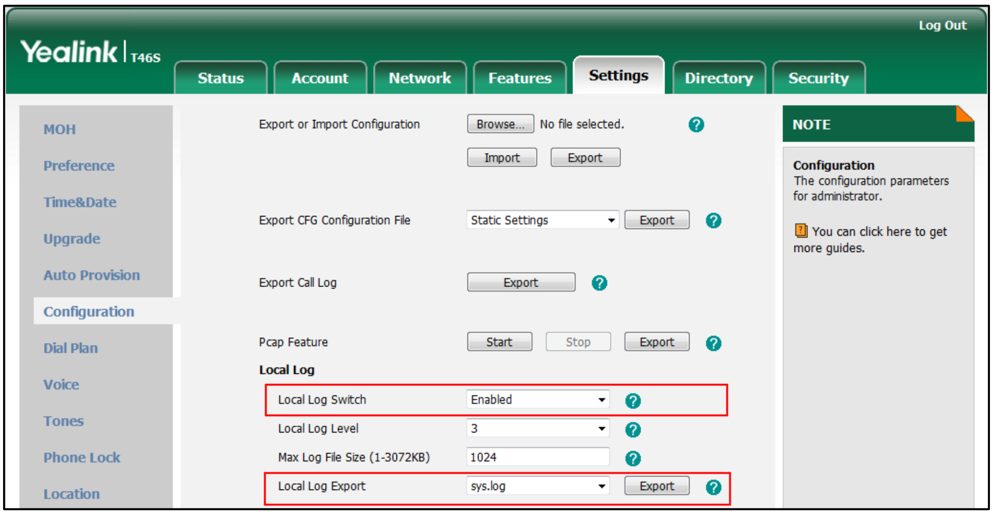
You can verify whether you got the correct log through the following key fields:

- <0+emerg>
- <1+alert>
- <2+crit>
- <3+error>
- <4+warning>

- <5+notice>
- <6+info>

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 **Local Log Switch**.
3. Select **boot.log** from the pull-down list of **Export Local Log**.

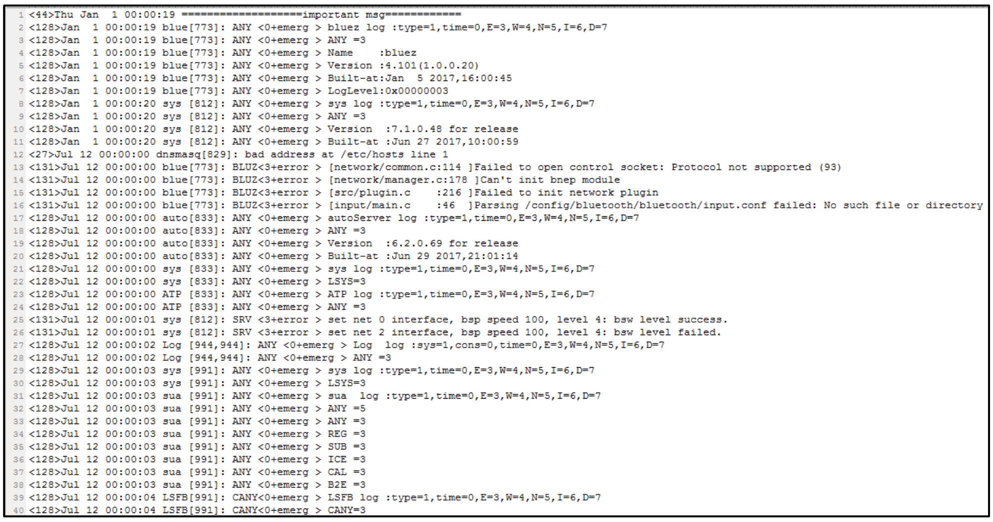


4. Click **Confirm** to accept the change.
5. Click **Export** to open the file download window, and then save the file to your local system.

To view the boot 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):



```
<44>Thu Jan  1 00:00:19 ===================important msg============
<128>Jan  1 00:00:19 blue[773]: ANY <0+emerg > bluez log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jan  1 00:00:19 blue[773]: ANY <0+emerg > ANY =3
<128>Jan  1 00:00:19 blue[773]: ANY <0+emerg > Name    :bluez
<128>Jan  1 00:00:19 blue[773]: ANY <0+emerg > Version :4.101(1.0.0.20)
<128>Jan  1 00:00:19 blue[773]: ANY <0+emerg > Built-at:Jan  5 2017,16:00:45
<128>Jan  1 00:00:19 blue[773]: ANY <0+emerg > LogLevel:0x00000003
<128>Jan  1 00:00:20 sys [812]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jan  1 00:00:20 sys [812]: ANY <0+emerg > ANY =3
<128>Jan  1 00:00:20 sys [812]: ANY <0+emerg > Version  :7.1.0.48 for release
<128>Jan  1 00:00:20 sys [812]: ANY <0+emerg > Built-at :Jun 27 2017,10:00:59
<27>Jul 12 00:00:00 dnsmasq[829]: bad address at /etc/hosts line 1
<131>Jul 12 00:00:00 blue[773]: BLUZ<3+error > [network/common.c:114 ]Failed to open control socket: Protocol not supported (93)
<131>Jul 12 00:00:00 blue[773]: BLUZ<3+error > [network/manager.c:178 ]Can't init bnep module
<131>Jul 12 00:00:00 blue[773]: BLUZ<3+error > [src/plugin.c    :216 ]Failed to init network plugin
<131>Jul 12 00:00:00 blue[773]: BLUZ<3+error > [input/main.c    :46  ]Parsing /config/bluetooth/bluetooth/input.conf failed: No such file or directory
<128>Jul 12 00:00:00 auto[833]: ANY <0+emerg > autoServer log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jul 12 00:00:00 auto[833]: ANY <0+emerg > ANY =3
<128>Jul 12 00:00:00 auto[833]: ANY <0+emerg > Version  :6.2.0.69 for release
<128>Jul 12 00:00:00 auto[833]: ANY <0+emerg > Built-at :Jun 29 2017,21:01:14
<128>Jul 12 00:00:00 sys [833]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jul 12 00:00:00 sys [833]: ANY <0+emerg > LSYS=3
<128>Jul 12 00:00:00 ATP [833]: ANY <0+emerg > ATP log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jul 12 00:00:00 ATP [833]: ANY <0+emerg > ANY =3
<131>Jul 12 00:00:01 sys [812]: SRV <3+error > set net 0 interface, bsp speed 100, level 4: bsw level success.
<131>Jul 12 00:00:01 sys [812]: SRV <3+error > set net 2 interface, bsp speed 100, level 4: bsw level failed.
<128>Jul 12 00:00:02 Log [944,944]: ANY <0+emerg > Log  log :sys=1,cons=0,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jul 12 00:00:02 Log [944,944]: ANY <0+emerg > ANY =3
<128>Jul 12 00:00:03 sys [991]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jul 12 00:00:03 sys [991]: ANY <0+emerg > LSYS=3
<128>Jul 12 00:00:03 sua [991]: ANY <0+emerg > sua  log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jul 12 00:00:03 sua [991]: ANY <0+emerg > ANY =5
<128>Jul 12 00:00:03 sua [991]: ANY <0+emerg > ANY =3
<128>Jul 12 00:00:03 sua [991]: ANY <0+emerg > REG =3
<128>Jul 12 00:00:03 sua [991]: ANY <0+emerg > SUB =3
<128>Jul 12 00:00:03 sua [991]: ANY <0+emerg > ICE =3
<128>Jul 12 00:00:03 sua [991]: ANY <0+emerg > CAL =3
<128>Jul 12 00:00:03 sua [991]: ANY <0+emerg > B2E =3
<128>Jul 12 00:00:04 LSFB[991]: CANY<0+emerg > LSFB log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jul 12 00:00:04 LSFB[991]: CANY<0+emerg > CANY=3
```

The <MAC>-boot.log file is forced to report the logs with all severity levels.

To back up the local log files to a server via web user interface:

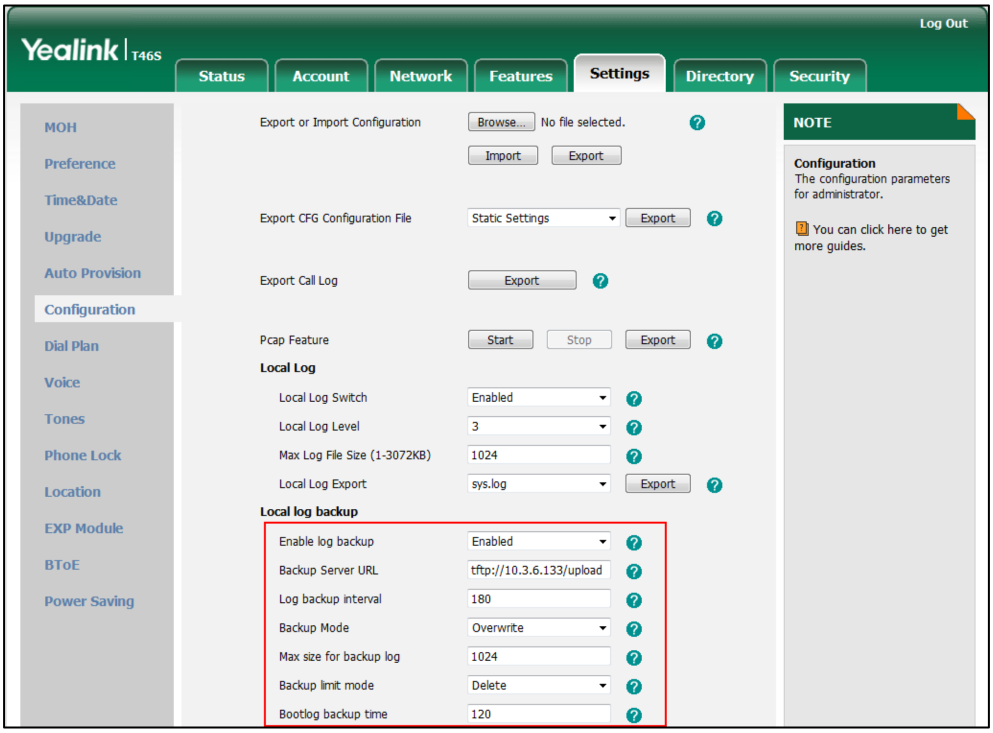
1. Click on **Settings**->**Configuration**.
2. Select **Enabled** from the pull-down list of **Enable log backup**.
3. Enter the desired path in the **Backup Server URL** field.
4. Enter the desired interval (in seconds) in the **Log backup interval** field.

   The local log files (<MAC>-boot.log and <MAC>-sys.log) will be uploaded to the server at intervals.
5. Select desired mode from the pull-down list of **Backup Mode**.

   - If you select **Overwrite**, the new uploaded local log files will overwrite the old local log files.
   - If you select **Append** (not applicable to TFTP Server), the new uploaded local log files will append to the existing local log files.
6. Enter the limit size of the local log files that can be stored on the server in the **Max size for backup log** field.
7. Select desired mode from the pull-down list of **Backup limit mode**.

   - If you select **Delete**, the phone will delete the old local log and start over when the server reaches its capacity.
   - If you select **Stet**, the phone will stop uploading local log when the server reaches its capacity.
8. Enter the desired time (in seconds) in the **Bootlog backup** time field.

   It configures the waiting time (in seconds) before the phone uploads the <MAC>-boot.log file to the server after startup.



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

Syslog

Procedure

Syslog logging can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.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 Skype for Business 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 Skype for Business 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. **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 phone to upload log messages to the syslog server in real time. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Configuration->Syslog Switch **Phone 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 **Phone User Interface:** None		
static.syslog.server_port	**Integer from 1 to 65535**	**514**
Description: Configures the port of the syslog server. **Example:** static.syslog.port = 515 **Web User Interface:** Settings->Configuration->Port **Phone User Interface:** None		
static.syslog.transport_type	**0, 1 or 2**	**0**

Parameters	Permitted Values	Default
Description: Configures the transport protocol that the Skype for Business phone uses when exporting log messages to the syslog server. **0**-UDP **1**-TCP **2**-TLS **Web User Interface:** Settings->Configuration->Syslog Transport Type **Phone User Interface:** None		
static.syslog.level	**Integer from 0 to 6**	**6**
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 **6**-Informational: informational messages **Web User Interface:** Settings->Configuration->Syslog Level **Phone 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		

Parameters	Permitted Values	Default
2-mail system **3**-system daemons **4**-security/authorization messages (note 1) **5**-messages generated internally by syslog **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) **Note**: For more information, refer to RFC 3164. **Web User Interface:** Settings->Configuration->Syslog Facility **Phone User Interface:** None		
static.syslog.prepend_mac_address.enable	**0 or 1**	**0**
Description: Enables or disables the Skype for Business phone to prepend the MAC address to the log messages exported to the syslog server. **0**-Disabled **1**-Enabled **Web User Interface:**		

Parameters	Permitted Values	Default
Settings->Configuration->Syslog Prepend MAC **Phone User Interface:** None		

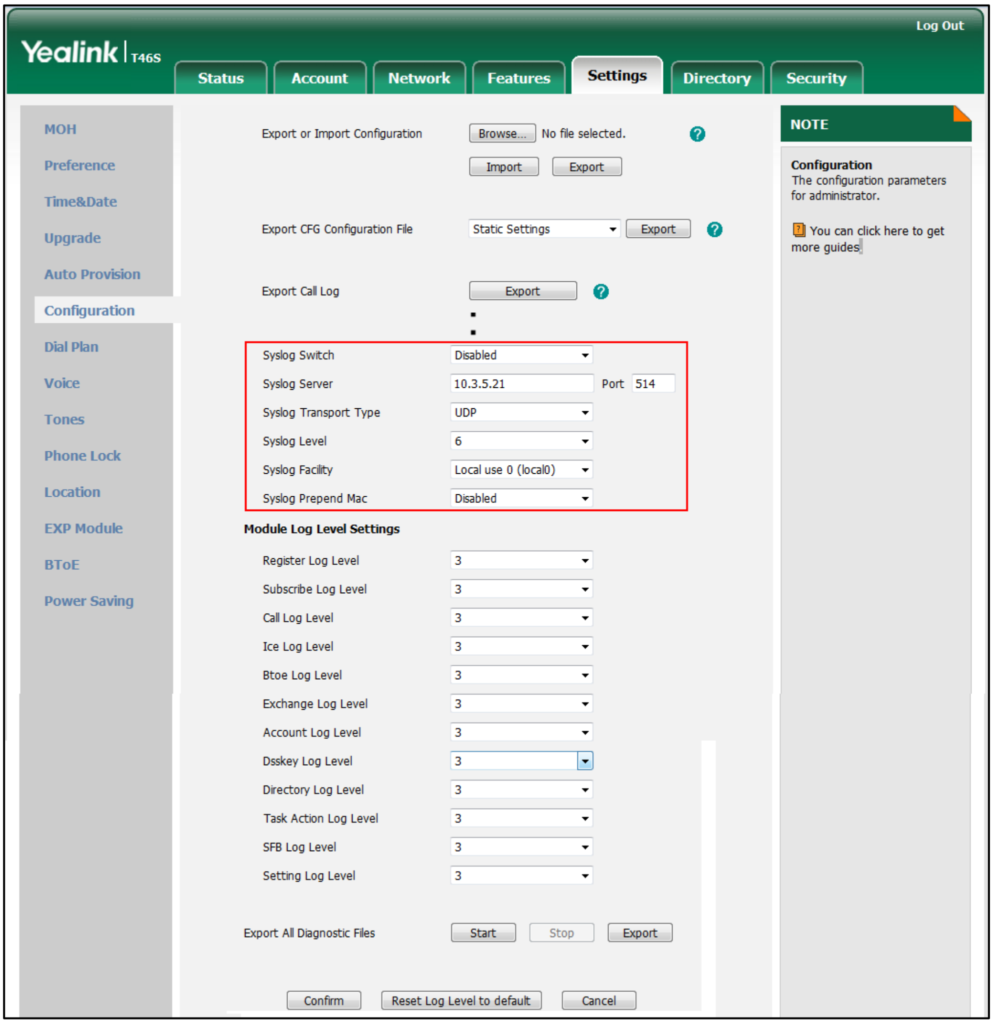
To configure the phone to export the system log to a syslog server via web user interface:

1. Click on **Settings**->**Configuration**.
2. Select the desired value from the pull-down list of **Syslog Switch**.
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**.

   It configures the transport protocol that the phone uses when exporting log messages to the syslog server.
6. Select the desired log level from the pull-down list of **Syslog Level**.
7. 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.
8. Select the desired facility from the pull-down list of **Syslog Facility**.

   It configures the facility that generates the log messages.
9. Select the desired value from the pull-down list of **Syslog Prepend MAC**.

It configures whether the uploaded log messages has phone MAC address or not.



10. 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:

```
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek read (0,256) ret 256 [sgfc]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek read (0,256) ret 256 [sgfc]
Jul 14 03:38:48 cfg [451]: CFG <4+warnin> write all 0, len 40960, offset 8346, changed 4, used 124, node_set 1021 to 1021
Jul 14 03:38:48 cfg [451]: CFG <4+warnin> 1462 buf remain 667054
Jul 14 03:38:48 cfg [451]: CFG <4+warnin> 1489 buf remain 667054
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write cnt 4
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [3363,44] [syslog.log_level]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [4942,49] [syslog.server]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [5158,40] [syslog.level]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [6884,41] [syslog.enable]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [0,256] [sgfc]
Jul 14 03:38:48 cfg [451]: CFG <4+warnin> backup cfg
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [0,256] [sgfc]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write cnt 4
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [3363,44] [syslog.log_level]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [4942,49] [syslog.server]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [5158,40] [syslog.level]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [6884,41] [syslog.enable]
```

Module Log

You can configure severity level of each module.

The severity level of the exported Module Log will not be greater than the total level (Local Log Level or Syslog Level). For example:

If you set Local Log Level to 3 and set ICE log Level to 6, the exported ICE log Level will still be 3 in your exported local log.

If you set Syslog Level to 3 and set ICE log Level to 6, the exported ICE log Level will still be 3 in your exported syslog.

Procedure

Module log can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the severity level of each module. **Parameters:** syslog.reg_loglevel syslog.sub_loglevel syslog.call_loglevel syslog.ice_loglevel syslog.btoe_loglevel syslog.exchange_loglevel

		syslog.account_module.log_level syslog.dsskey_module.log_level syslog.directory_module.log_level syslog.taskaction_module.log_level syslog.sfb_feature.log_level syslog.setting_module.log_level
Local	Web User Interface	Configure the severity level of each module. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-config&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
syslog.reg_loglevel	**Integer from 0 to 6**	**3**
Description: Configures the severity level of the register log. **Web User Interface:** Settings->Configuration->Register Log Level **Phone User Interface:** None		
syslog.sub_loglevel	**Integer from 0 to 6**	**3**
Description: It configures the severity level of the subscribe log. **Web User Interface:** Settings->Configuration->Subscribe Log Level **Phone User Interface:** None		
syslog.ice_loglevel	**Integer from 0 to 6**	**3**
Description: Configures the severity level of the ICE log. **Web User Interface:** Settings->Configuration->Ice Log Level		

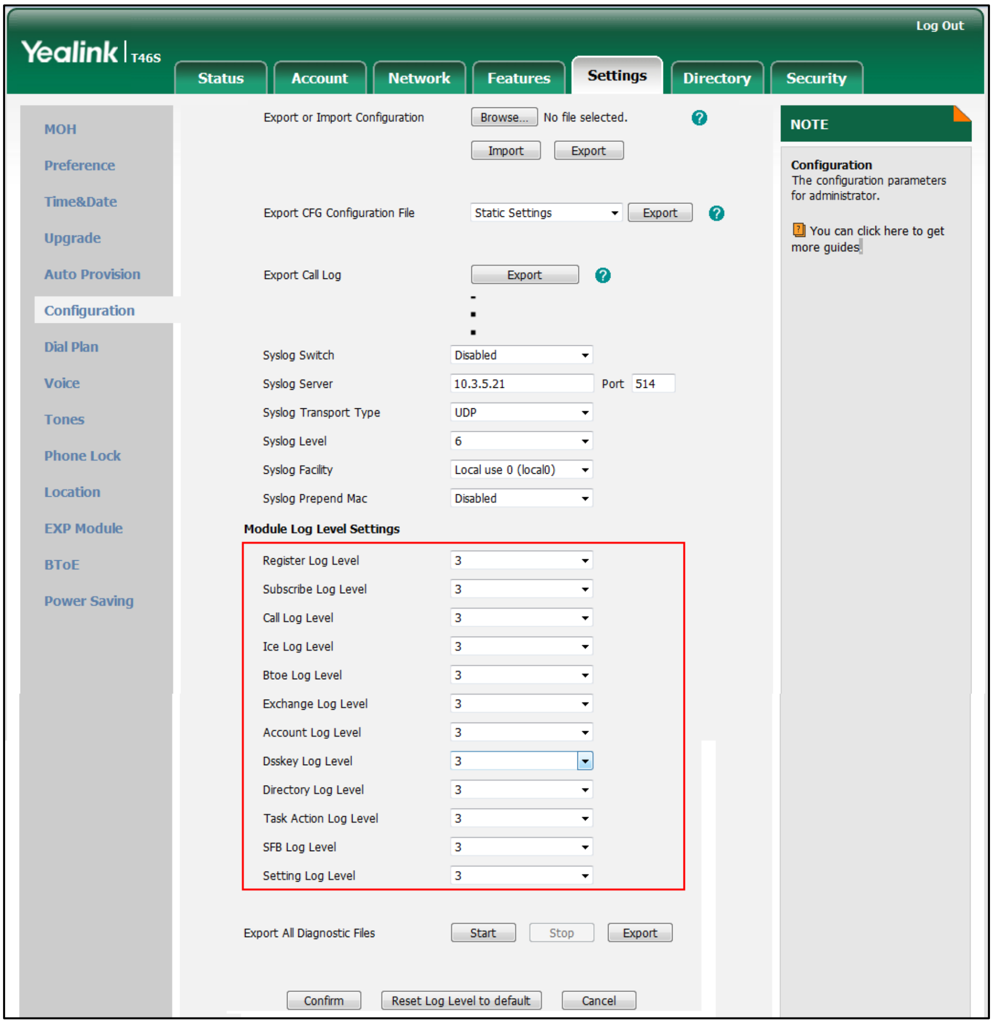
Parameters	Permitted Values	Default
Phone User Interface: None		
syslog.btoe_loglevel	**Integer from 0 to 6**	**3**
Description: Configures the severity level of the BToE (Better Together over Ethernet) log. **Web User Interface:** Settings->Configuration->Btoe Log Level **Note:** It is not applicable to CP960 Skype for Business phones. **Phone User Interface:** None		
syslog.exchange_loglevel	**Integer from 0 to 6**	**3**
Description: Configures the severity level of the Exchange log. **Web User Interface:** Settings->Configuration->Exchange Log Level **Phone User Interface:** None		
syslog.account_module.log_level	**Integer from 0 to 6**	**6**
Description: Configures the severity level of the account logs. **Web User Interface:** Settings->Configuration->Account Log Level **Phone User Interface:** None		
syslog.dsskey_module.log_level	**Integer from 0 to 6**	**3**
Description: Configures the severity level of Dsskey log. **Web User Interface:** Settings->Configuration->Dsskey Log Level **Phone User Interface:** None		

Parameters	Permitted Values	Default
syslog.directory_module.log_level	**Integer from 0 to 6**	**6**
Description: Configures the severity level of the logs related to calling feature. **Web User Interface:** Settings->Configuration->Directory Log Level **Phone User Interface:** None		
syslog.taskaction_module.log_level	**Integer from 0 to 6**	**3**
Description: Configures the severity level of the logs related to calling feature. **Web User Interface:** Settings->Configuration->Task Action Log Level **Phone User Interface:** None		
syslog.sfb_feature.log_level	**Integer from 0 to 6**	**3**
Description: Configures the severity level of the logs related to calling feature. **Web User Interface:** Settings->Configuration->SFB Log Level **Phone User Interface:** None		
syslog.setting_module.log_level	**Integer from 0 to 6**	**3**
Description: Configures the severity level of setting log **Web User Interface:** Settings->Configuration->Setting Log Level **Phone User Interface:** None		

To configure the severity level of the module logs via web user interface:

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

2. Select the desired level from the pull-down list of corresponding module logs.



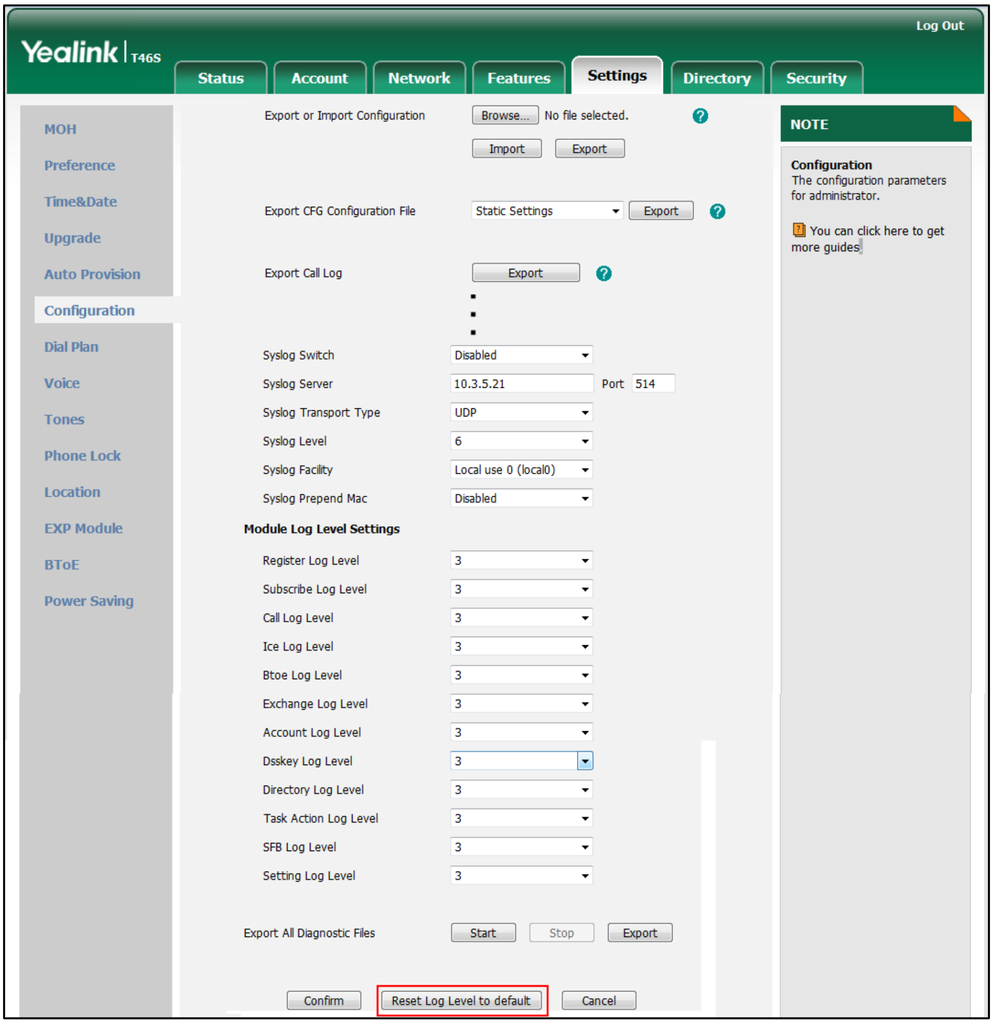
3. Click **Confirm** to accept the change.

High level may make some sensitive information accessible (e.g., password and dial number), we recommend that you reset the module logs level to 3 after providing the log for troubleshooting purpose.

To reset severity level of module logs via web user interface:

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

2. Click **Reset Log Level to Default**.



3. All module log level will reset to 3.

Exporting the Log File to the Skype for Business Server

You can upload the log file to the Skype for Business Server via phone user interface only.

When performing a log upload, The HTTP POST sent from phone has following Headers:

UCDevice_Type: “with a value of “3PIP”.

UCDevice_ID: containing a unique string identifying the phone.

The UCDevice_ID contains at minimum the following entries:

1. VendorName-phone manufacturer name
2. DeviceModel-phone model
3. Firmware version
4. MAC address

Sample:

```
UCDevice_ID: Yealink_SIP-T46S_66.9.0.25_00156574B1D6E\r\n
UCDevice_Type: 3PIP\r\n
```

To export a log file to the Skype for Business Server via phone user interface:

1. Press **Menu**->**Basic**->**Log Upload**.
2. Press **Upload**.

   A dialog box pops up to prompt "Log Uploaded Successfully！".

   The log file can be found on the Skype for Business Server at %ocsfilestore%\%domain%-WebServices-1\DeviceUpdateLogs\Cient.

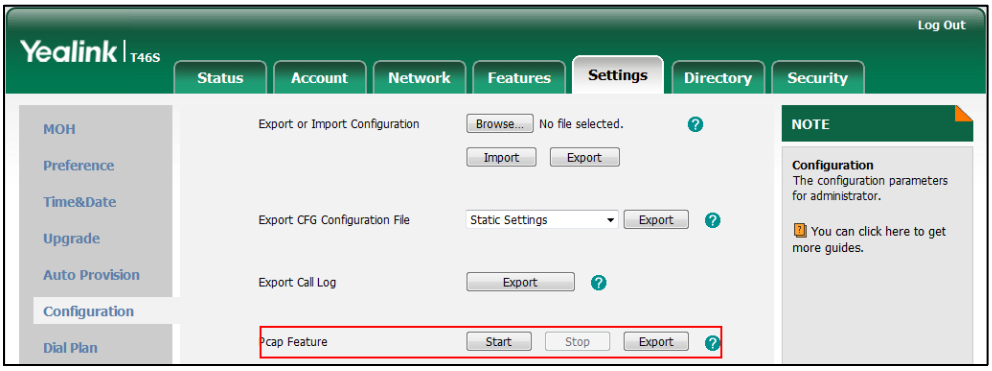
Capturing Packets

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

To capture packets via web user interface:

1. Click on **Settings**->**Configuration**.
2. Click **Start** to start capturing signal traffic.
3. Reproduce the issue to get stack traces.
4. Click **Stop** to stop capturing.
5. Click **Export** to open the file download window, and then save the file to your local system.



Capture the Packets Using the Ethernet Software

Receiving data packets from the HUB

Connect the Internet port of the phone and the PC to the same HUB, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic.

Receiving data packets from PC port

Connect the Internet port of the phone to the Internet, and then connect the PC port of the phone to a PC. Before capturing the signal traffic, make sure the data packets can be received from the WAN (Internet) port to the PC (LAN) port.

It is not applicable to CP960 Skype for Business phones.

Procedure

Span to PC Port can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure span to PC Port. **Parameter:** static.network.span_to_pc_port
Local	Web User Interface	Configure span to PC Port. **Navigate to:** http://<phoneIPAddress/servlet?p=network-adv&q=load

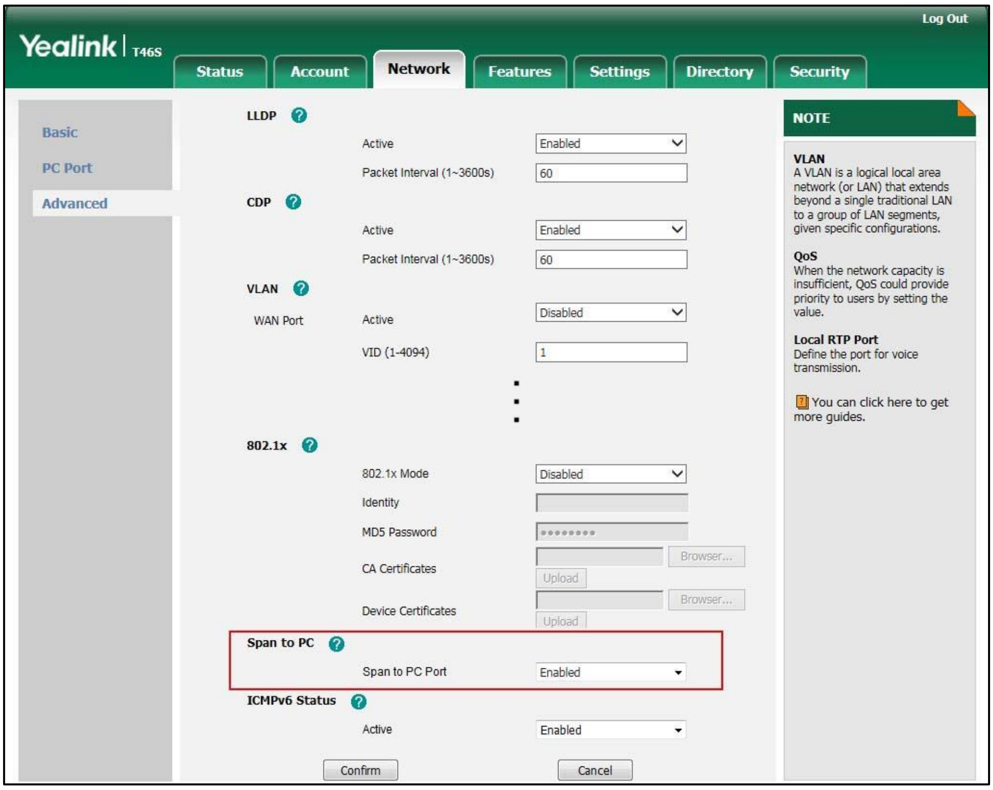
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
static.network.span_to_pc_port	**0 or 1**	**0**
Description: Enables or disables the phone to span data packets received from the WAN (Internet) port to the PC (LAN) port. **0**-Disabled **1**-Enabled, all data packets from WAN (Internet) port can be received by PC port. **Note:** It works only if the value of the parameter “static.network.pc_port.enable” is set to 1 (Auto Negotiate). If you change this parameter, the phone will reboot to make the change take effect. It is not applicable to CP960 Skype for Business phones. **Web User Interface:** Network->Advanced->Span to PC->Span to PC Port **Phone User Interface:** None		

To enable span to pc port via web user interface:

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

2. Select **Enabled** from the pull-down list of **Span to PC Port**.



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

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

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

   Then you can use Sniffer, Ethereal or Wireshark software to capture the signal traffic.

Enabling Watch Dog Feature

The Skype for Business phone provides a troubleshooting feature called "Watch Dog", which helps you monitor the phone status and provides the ability to get stack traces from the last time the phone failed. If Watch Dog feature is enabled, the phone will automatically reboot when it detects a fatal failure. This feature can be configured using the configuration files or via web user interface.

Procedure

Watch dog can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure watch dog feature. **Parameter:** static.watch_dog.enable
Local	Web User Interface	Configure watch dog

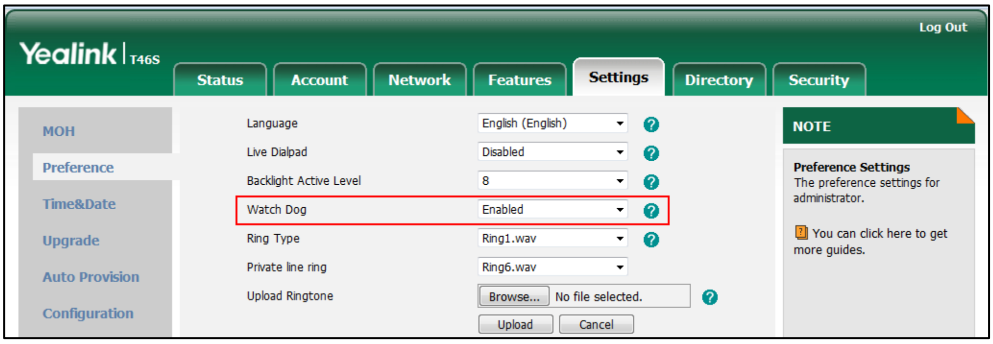
		feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-preference&q=load

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, the phone will reboot automatically when the system is broken down. **Web User Interface:** Settings->Preference->Watch Dog **Phone User Interface:** None		

To configure watch dog feature via web user interface:

1. Click on **Settings**->**Preference**.
2. Select the desired value from the pull-down list of **Watch Dog**.



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

Getting Information from Status Indicators

Status indicators may consist of the power LED, MESSAGE key LED, line key indicator, headset key indicator, the mute touch key and the on-screen icons.

The following shows two examples of obtaining the phone information from status indicators on T46S Skype for Business phones:

- If a LINK failure of the phone is detected, a prompting message “Network unavailable” will appear on the LCD screen/touch screen.
- If a voice mail is received, the power LED indicator slowly flashes red.
- If a Skype for Business favorite is during a call, the line key LED indicator is solid red.

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 phone and troubleshoot if necessary. You can also import configuration files for a quick and easy configuration.

You can export BIN or CFG configuration files to your local system.

BIN Configuration Files

The config.bin file is an encrypted file. For more information on config.bin file, contact your Yealink reseller.

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the access URL for the custom configuration files. **Parameter:** static.configuration.url
Web User Interface		Export or import the custom configuration files. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-config&q=load

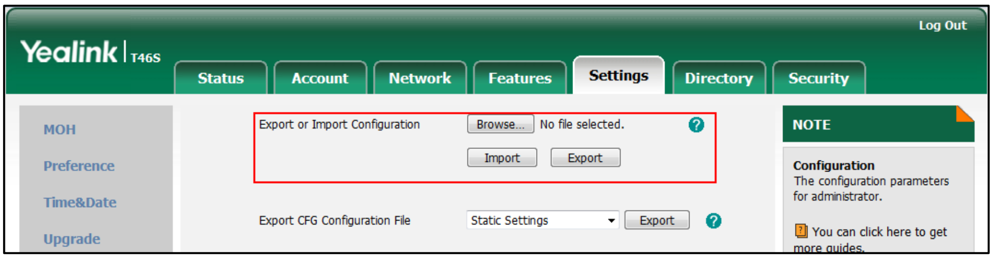
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
static.configuration.url	**URL within 511 characters**	**Blank**

<table>
<tr><th>Parameter</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td colspan="3">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 phone will reboot to make the change take effect.
Web User Interface:
Settings->Configuration->Export or Import Configuration
Phone User Interface:
None</td></tr>
</table>

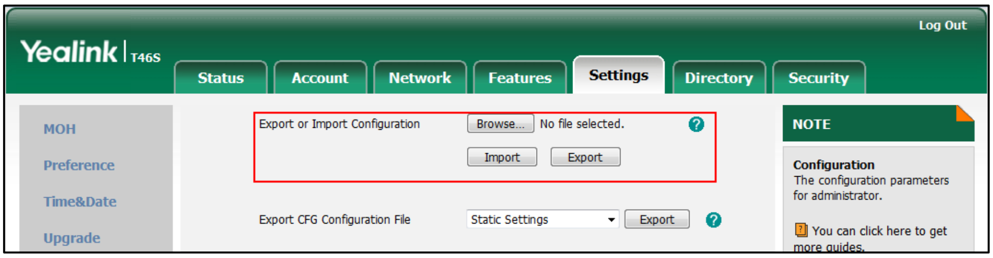
To export BIN configuration files via web user interface:

1. Click on **Settings**->**Configuration**.
2. In the **Export or Import Configuration** block, click **Export** to open the file download window, and then save the file to your local system.



To import a BIN configuration files 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

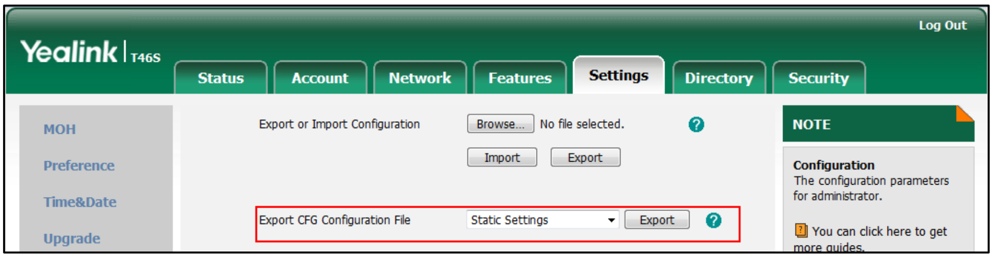
You can export the following CFG configuration files for T48S/T46S/T42S/T1S Skype for Business phones:

- **<MAC>-local.cfg**: It contains changes associated with non-static settings made via phone user interface and web user interface. It can be exported only if the value of the parameter “static.auto_provision.custom.protect” is set to 1.
- **<MAC>-inband.cfg:** It contains configurations sent from Skype for Business server. It can be exported only if the value of the parameter “static.auto_provision.custom.protect” is set to 1.
- **<MAC>-config.cfg**: It contains changes associated with non-static settings made using configuration files. It can be exported only if the value of the parameter “static.auto_provision.custom.protect” is set to 1.
- **<MAC>-static.cfg**: It contains all changes associated with static settings (for example, network settings).
- **<MAC>-non-static.cfg**: It contains all changes associated with non-static settings.
- **<MAC>-all.cfg**: It contains all changes made via phone user interface, web user interface, configuration files and in-band provisioning.

  It is not applicable to CP960 Skype for Business phones.

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.



4. Click **Import** to import the configuration file.

Exporting All the Diagnostic Files

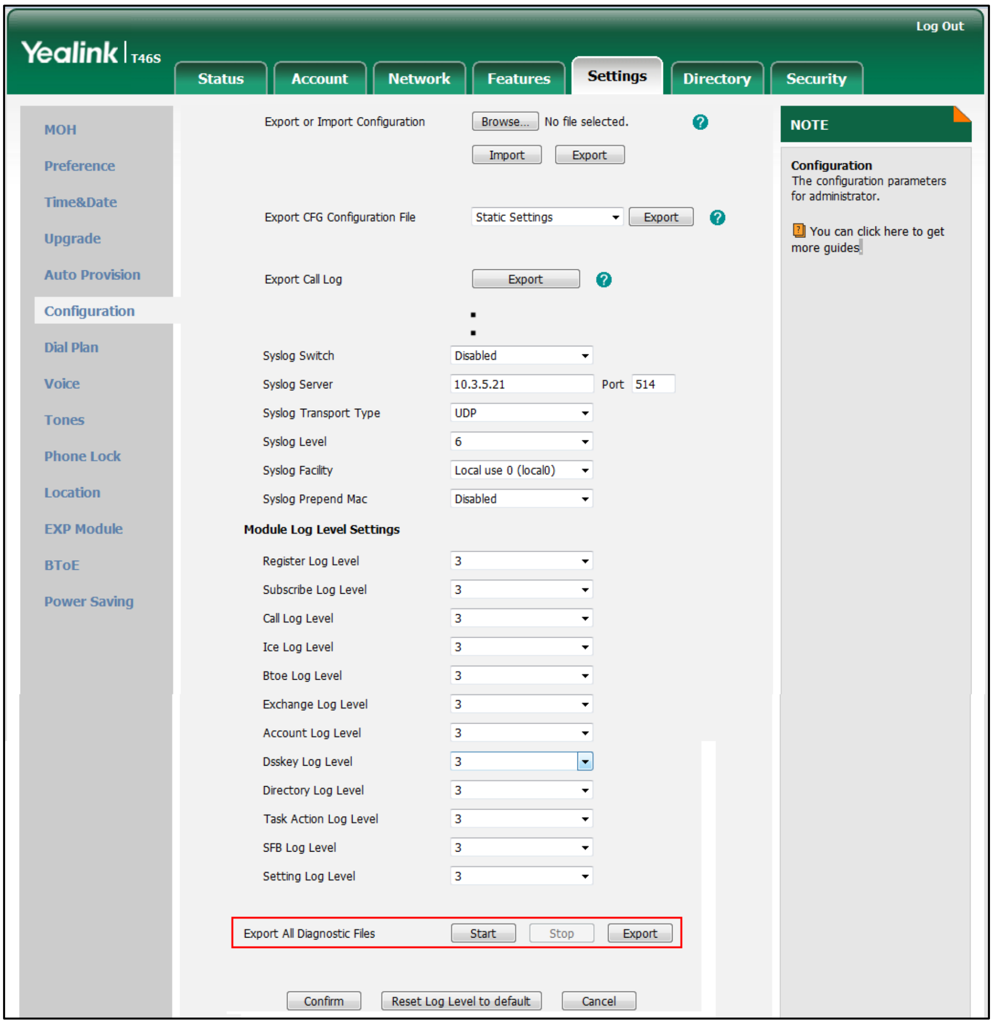
Yealink phones support three types of diagnostic files (including Pcap trace, log files (boot.log and sys.log) and BIN configuration files) to help analyze your problem. You can export these files at a time and troubleshoot if necessary. The file format of exported diagnostic file is *.tar.

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 local 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 local log level will be automatically set to the previous setting.
5. Click **Export** to open file download window, and then save the diagnostic file to your local system.



A diagnostic file named **allconfig.tgz** is successfully exported to your local system.

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 410, Log Files on page388 and Analyzing Configuration Files on page 414.

Troubleshooting Solutions

This section describes solutions to common issues that may occur while using the phone. Upon encountering a scenario not listed in this section, contact your Yealink reseller for further support.

IP Address Issues

Why doesn't the phone get an IP address?

Do one of the following:

- Ensure that the Ethernet cable is plugged into the Internet port on the phone and the Ethernet cable is not loose.
- Ensure that the Ethernet cable is not damaged.
- Ensure that the IP address and related network parameters are set correctly.
- Ensure that your network switch or hub is operational.

How to solve the IP conflict problem?

Do one of the following:

- Reset another available IP address for the phone.
- Check network configuration via phone user interface at the path **Menu->Advanced**->**Network**->**WAN Port**->**IPv4** (or **IPv6**). If the Static IP is selected, select DHCP instead.

Time and Date Issues

Why doesn't the phone display time and date correctly?

Check if the phone is configured to obtain the time and date from the NTP server automatically. If your phone is unable to access the NTP server, configure the time and date manually.

Display Issues

Why is the LCD screen/touch screen blank?

Do one of the following:

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

Directory Issues

What is the difference between a Skype for Business directory and a local directory?

The Skype for Business directory on your phone displays all Skype for Business contacts on your Skype for Business client. While a local directory is placed on the phone flash. When you sign into different phones using the same account, the phone will display the same Skype for Business contacts, while a local directory can only be used by a specific phone.

Audio Issues

How to increase or decrease the volume?

Press the volume key to increase or decrease the ringer volume when the phone is idle or ringing, or to adjust the volume of engaged audio device (handset, speakerphone or headset) 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 PC or a fan, may cause voice interference. Turn off any noisy equipment.
- Line issues can also cause this problem; disconnect the old line and redial the call to ensure another line may provide better connection.

Why is there no sound when the other party picks up the call?

If the caller and receiver cannot hear anything - there is no sound at all when the other party picks up the call, the possible reason could be: the phone cannot send the real-time transport protocol (RTP) streams, in which audio data is transmitted, to the connected call.

Try to disable the 180 ring workaround feature. For more information, refer to 180 Ring Workaround on page 229.

Why does the 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 229.

Bluetooth Issues

Why can't I connect the Bluetooth device with my phone all the time?

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

Why does the Bluetooth headset affect the phone's voice quality？

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

Firmware and Upgrading Issues

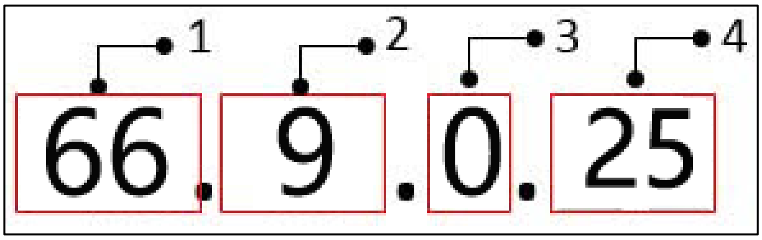
Why doesn't the phone upgrade firmware successfully?

Do one of the following:

- Ensure that the target firmware is not the same as the current firmware.
- Ensure that the target firmware is applicable to the 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.
- Ensure that the target firmware on the Skype for Business Server is available.

How can I verify the firmware generation and version of the phone?

Press the **OK** key when the phone is idle to check the firmware version. For example: 66.9.0.25.



	Item	Description
1	66	A fixed number for each phone model.
2	9	Firmware generation. **Note:** The larger it is, the newer the firmware generation is.
3	0	A fixed number.
4	25	Firmware version. **Note:** With the same firmware generation, the larger it is, the newer the firmware version is.

Why doesn't the phone update the configuration?

Do one of the following:

- Ensure that the configuration is set correctly.
- Reboot the phone. Some configurations require a reboot to take effect.
- Ensure that the configuration is applicable to the phone model.
- The configuration may depend on support from a server.

Provisioning Issues

What is auto provisioning?

Auto provisioning refers to the update of phones, including update on configuration parameters, local phone book, firmware and so on. You can use auto provisioning on a single phone, but it makes more sense in mass deployment.

System Log Issues

Why cannot I export the log to a syslog server?

Do one of the following:

- Ensure that the syslog server supports saving the syslog files exported from phone.

- Ensure that you have configured the syslog server address correctly via web user interface on your phone.

Resetting Issues

Generally, some common issues may occur while using the 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.

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. It is not applicable to CP960 Skype for Business phones.
CP960 Skype for Business phones can reset all configurations to factory only.

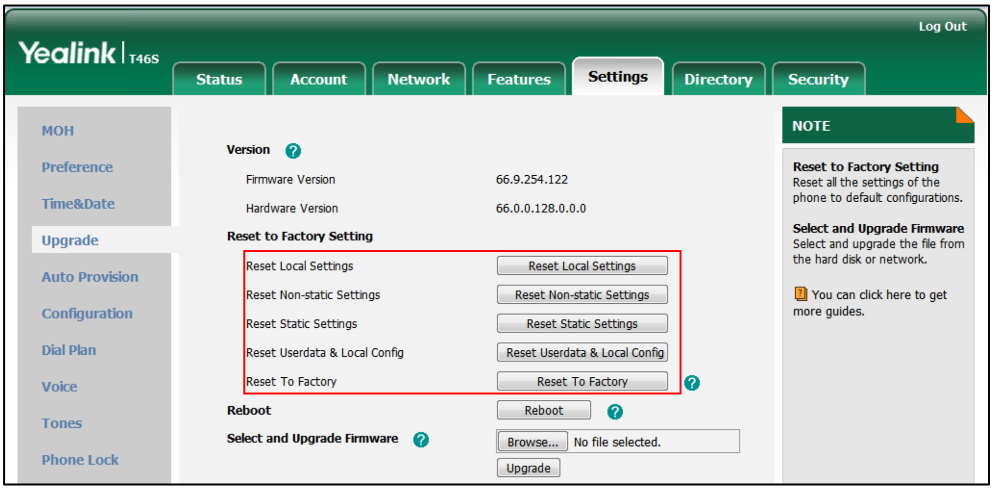
- **Reset Local settings**: All configurations saved in the <MAC>-local.cfg file on the phone will be reset. Changes associated with non-static settings made via web user interface and phone user interface are saved in the <MAC>-local.cfg file.
- **Reset Non-static Settings**: All non-static settings on the phone will be reset.
- **Reset StaticSettings**: All static settings on the phone will be reset.
- **Reset Userdata &Local config**: All the local cache data (for example, userdata, history, local directory) will be cleared. And all configurations saved in the <MAC>-local.cfg configuration file on the phone will be reset.
- **Reset To Factory**: Reset the phone to default factory configurations. The default factory configurations are the settings that reside on the phone after it has left the factory.

How to reset the phone?

To reset the phone via web user interface:

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

2. In the **Reset** block, click the desired value to reset the corresponding settings.



Note

Reset of your phone may take a few minutes. The phone will be reset to factory sucessfully after a reboot, do not power off until the phone starts up successfully.

How to reset the phone to custom factory configurations?

You can also reset the phone to custom factory configurations if required.

You can change some values in the default factory configurations file to generate a custom factory configurations file, and then import the custom factory configuration files to the phone. As a result, the custom factory configurations defined by you can be kept even if you reset the phone.

Procedure

Custom factory configurations can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the Custom Factory Configuration feature. **Parameter:** static.features.custom_factory_config.enable
		Configure the access URL of the custom factory configuration file. **Parameter:** static.custom_factory_configuration.url
Web User Interface		Configure the access URL of the custom factory configuration file. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-config&q=load

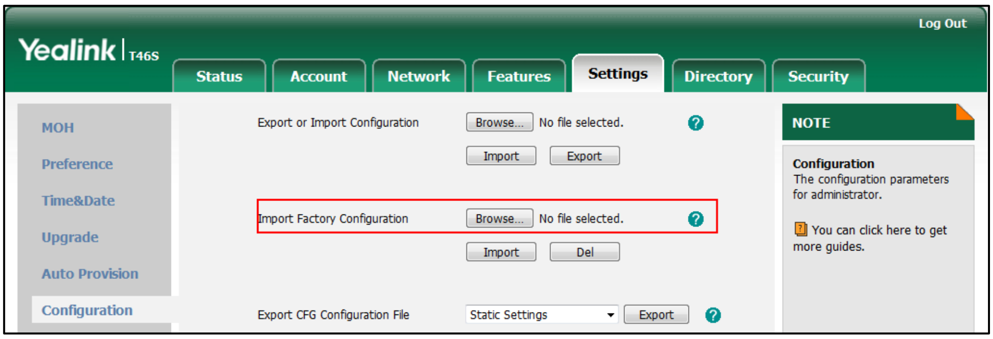
Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>static.features.custom_factory_config.enable</td><td>0 or 1</td><td>0</td></tr>
<tr><td colspan="3">Description:
Enables or disables the phone to be imported a custom factory configuration file.
0-Disabled
1-Enabled, Import Factory Configuration item will be displayed on the phone's web user interface at the path Settings->Configuration. You can import or delete a custom factory configuration file via web user interface.
Web User Interface:
None
Phone User Interface:
None</td></tr>
<tr><td>static.custom_factory_configuration.url</td><td>URL within 511 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the access URL of the custom factory configuration file.
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 phone will reboot to make the change take effect.
Web User Interface:
Settings->Configuration->Import Factory Config
Phone User Interface:
None</td></tr>
</table>

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.



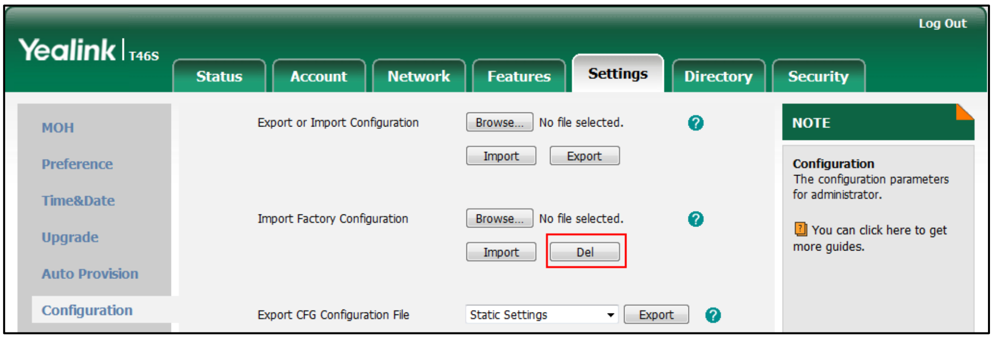
3. Click **Import**.

When the custom factory configuration file is imported successfully, you can reset the 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 phone? on page 422.

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 Config** field.



The web user interface prompts the message “Are you sure delete user-defined factory configuration?”.

3. Click **OK** to delete the custom factory configuration files.

The imported custom factory file will be deleted. The phone will be reset to default factory configurations after resetting.

Rebooting Issues

How to reboot the phone via web/phone user interface?

You can reboot your phone via web/phone user interface.

To reboot the phone via phone user interface:

1. Press **Menu**->**Advanced** (default password: admin).

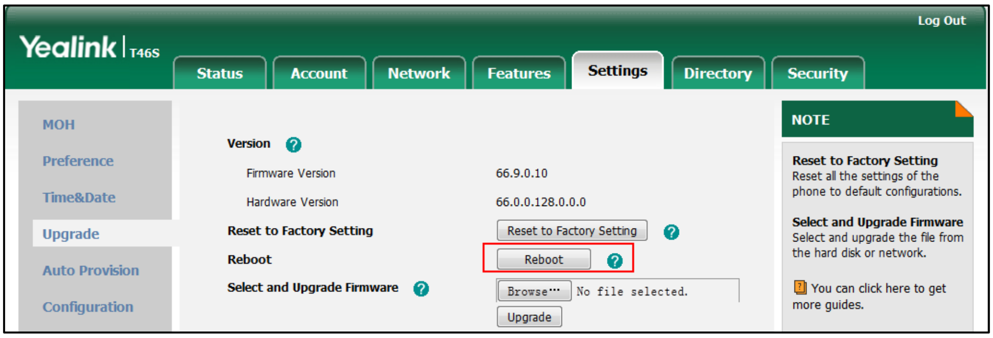
2. Press or to scroll to **Reboot**, and then press the **Enter** soft key.
3. Press **Reboot** soft key.

   The LCD screen prompts "Reboot the phone?".
4. Press the **OK** soft key to reboot the phone.

   The phone begins rebooting. Any reboot of the phone may take a few minutes.

To reboot the phone via web user interface:

1. Click on **Settings**->**Upgrade**.
2. Click **Reboot** to reboot the 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 Skype for Business phones support?

Source Device	Source IP	Source Port	Destination Device	Destination IP	Destination Port (Listening port)	Protocol	Description of destination port
Skype for Business phones	IP address of Skype for Business phones	2~65535	Skype for Business phone or voice gateway	IP address of Skype for Business 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	File server	IP address of file server	Determined by destination device.	TCP	HTTP protocol port, it is used to download file.
		1024~65535	AA	IP address of AA	Determined by destination device.	TCP	HTTP protocol port, it is used for AA communication.
		68	DHCP Server	IP address of DHCP server	67	UDP	DHCP protocol port, it is used to obtain IP address from DHCP server.
		1024~65535	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 Skype for Business phones

Source Device	Source IP	Source Port	Destination Device	Destination IP	Destination Port (Listening port)	Protocol	Description of destination port
							to upload syslog information to syslog server.
PC	IP address of PC	Determined by the destination device.	Skype for Business phones	IP address of Skype for Business phones	1~65535	TCP	HTTP port (default value: 80)
					1~65535	TCP	HTTP port (default value: 443)
SIP Server	IP address of SIP Server				1024~65534	UDP/TCP	SIP protocol port, it is used for signaling interaction with SIP server.
Skype for Business phone of voice gateway	Skype for Business phone or voice gateway				2~65535	UDP	RTP protocol port, it is used by destination device to send or receive audio stream.

Password Issues

How to reset the administrator password?

Factory reset can reset the original password. All custom settings will be overwritten after reset.

Power and Startup Issues

What will happen if I connect both PoE cable and power adapter? Which has the higher priority?

Phones use the PoE preferentially.

Why does the phone have no power?

If no lights appear on the phone when it is powered up, do one of the following:

- Reboot your phone.
- Replace the power adapter.

Why is the LCD screen black?

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

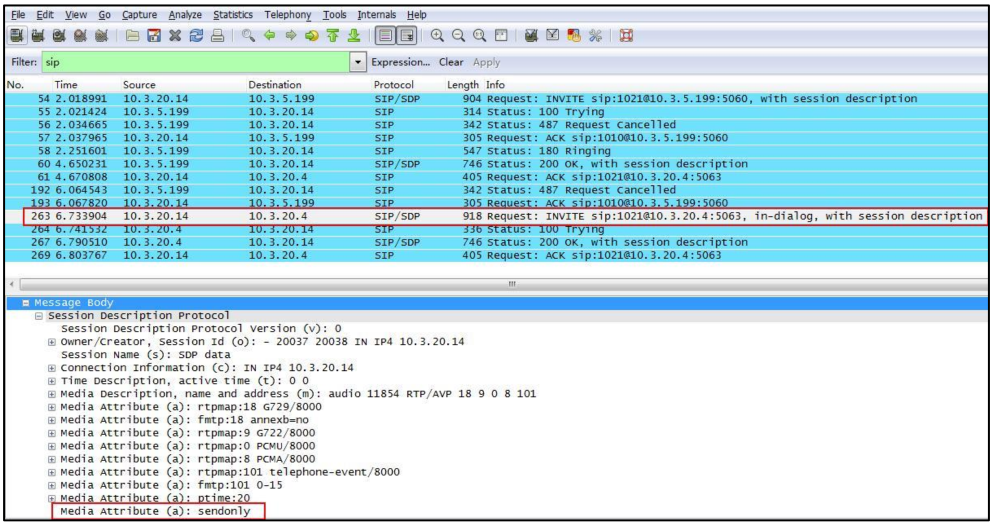
Other Issues

How can I find the basic information of the phone?

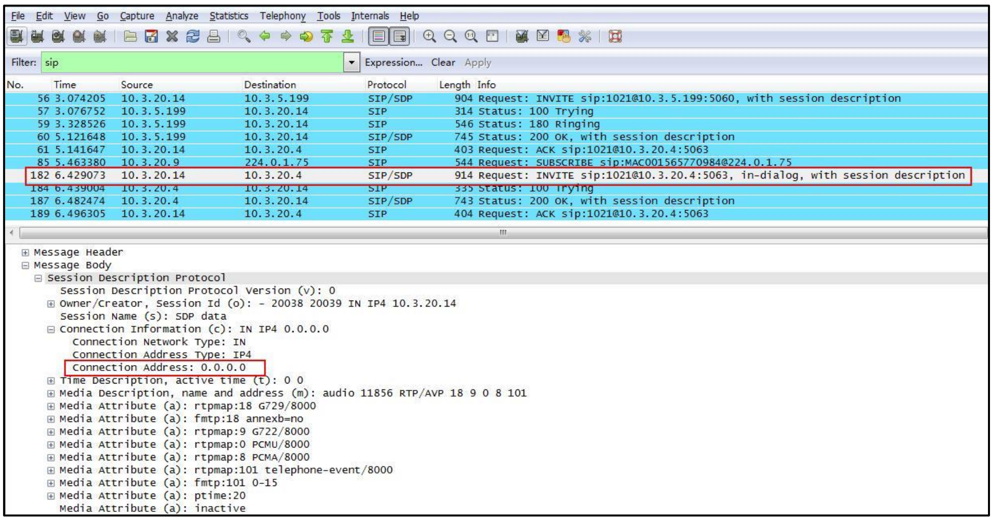
Press **Menu**-> **Status** when the phone is idle to check the basic information (e.g., IP address, MAC address and firmware version).

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 231. For more information on capturing packets, refer to Capturing Packets on page 410.

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 PC, 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 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, PC 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.

ROM (Read-only Memory)**--**a class of storage medium used in PC 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	Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Belize, Canada-Manitoba(Winnipeg), Chile(Easter Islands), Mexico(Mexico City,Acapulco), United States-Central Time

Time Zone	Time Zone Name
-5	Peru, 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), Switzerland(Bern), Sweden(Stockholm)
+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), Abu Dhabi， Kazakhstan(Aktau), Russia(Samara)
+4:30	Afghanistan(Kabul)
+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)

Time Zone	Time Zone Name
+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 Skype for Business phones trust the following CAs by default:

- DigiCert High Assurance EV Root CA
- Deutsche Telekom AG 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 CA
- GeoTrust Primary CA G2 ECC
- GeoTrust Universal CA
- GeoTrust Universal CA2
- Thawte Personal Freemail CA
- Thawte Premium Server CA
- Thawte Primary Root CA - G1 (EV)
- Thawte Primary Root CA - G2 (ECC)
- Thawte Primary Root CA - G3 (SHA256)
- 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
- Microsoft_IT_SSL_SHA2.cer
- CNNIC_Root.cer
- baltimoreCyberTrust.cer
- UserTrust.cer
- AAA Certificate Services.cer
- DigiCert Assured ID Root CA.cer
- Entrust.net Certification Authority (2048).cer
- Entrust Root Certification Authority
- Entrust.net Secure Server Certification Authority
- GTE CyberTrust Global Root.cer
- Starfield Class 2 Certification Authority.cer
- AddTrust External CA Root
- Go Daddy Class 2 Certification Authority
- StartCom Certification Authority
- DST Root CA X3
- ISRG Root X1 (intermediate certificates: Let's Encrypt Authority X1 and Let's Encrypt Authority X2 are signed by the root certificate ISRG Root X1.)
- Baltimore CyberTrust Root
- DigiCert Cloud Services CA-1
- D-Trust Root Class 3 CA 2 2009
- AddTrust External CA Root
- Starfield Root Certificate Authority - G2

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 on page

Appendix D: 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, phone user interface, configuration files or In-band provisioning) 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 file.

For more information on static settings, refer to the Static Settings sheet in *Yealink_Skype_for_Business_Edition_HD_IP_Phones_Description_of_Configuration_Parameters_in_CFG_Files*.

Appendix E: SIP (Session Initiation Protocol)

This section describes how Yealink 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 Skype for Business 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	

Method	Supported	Notes
BYE	Yes	
OPTIONS	Yes	
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	

Method	Supported	Notes
Event	Yes	
Expires	Yes	
From	Yes	
Max-Forwards	Yes	
Min-SE	Yes	
P-Asserted-Identity	Yes	
P-Preferred-Identity	Yes	
Proxy-Authenticate	Yes	
Proxy-Authorization	Yes	
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 Response—Information Responses

1xx Response	Supported	Notes
100 Trying	Yes	
180 Ringing	Yes	
181 Call Is Being Forwarded	Yes	
183 Session Progress	Yes	

2xx Response—Successful Responses

2xx Response	Supported	Notes
200 OK	Yes	
202 Accepted	Yes	In REFER transfer.

3xx Response—Redirection Responses

3xx Response	Supported	Notes
300 Multiple Choices	Yes	
301 Moved Permanently	Yes	
302 Moved Temporarily	Yes	

4xx Response—Request Failure Responses

4xx Response	Supported	Notes
400 Bad Request	Yes	
401 Unauthorized	Yes	
402 Payment Required	Yes	
403 Forbidden	Yes	
404 Not Found	Yes	
405 Method Not Allowed	Yes	
406 Not Acceptable	No	
407 Proxy Authentication Required	Yes	
408 Request Timeout	Yes	
409 Conflict	No	

4xx Response	Supported	Notes
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 Response—Server Failure Responses

5xx Response	Supported	Notes
500 Internal Server Error	Yes	
501 Not Implemented	Yes	
502 Bad Gateway	No	
503 Service Unavailable	No	
504 Gateway Timeout	No	
505 Version Not Supported	No	

6xx Response—Global Responses

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–Protocol version	Yes
o–Owner/creator and session identifier	Yes
a–Media attribute	Yes
c–Connection information	Yes
m–Media name and transport address	Yes
s–Session name	Yes
t–Active time	Yes

Appendix F: 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 phone or the SIP server:

SIP 1xx–Informational Responses

SIP 2xx–Successful Responses

SIP 3xx–Redirection Responses

SIP 4xx–Client Failure Responses

SIP 5xx–Server Failure Responses

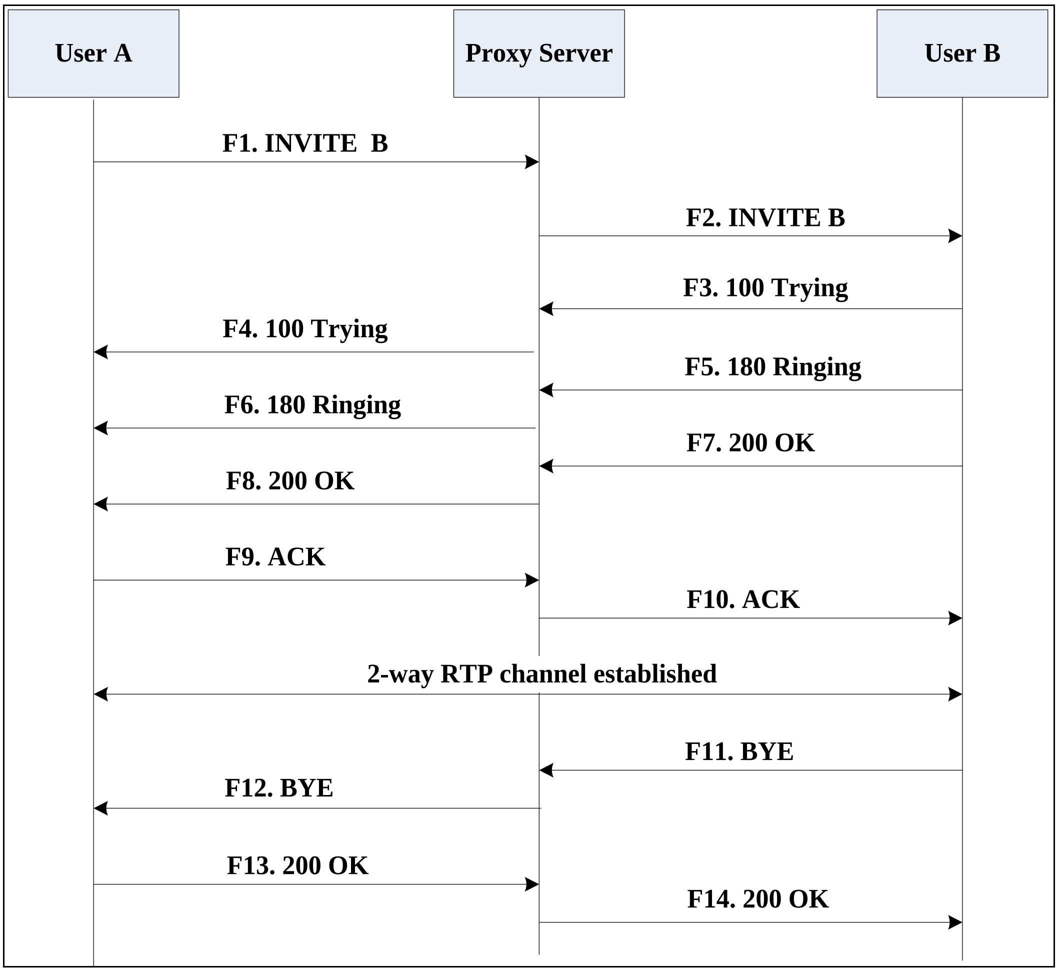
SIP 6xx–Global Failure Responses

Successful Call Setup and Disconnect

The following figure illustrates the scenario of a successful call. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink 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

Step	Action	Description
		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.
F7	200 OK− User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response

Step	Action	Description
		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

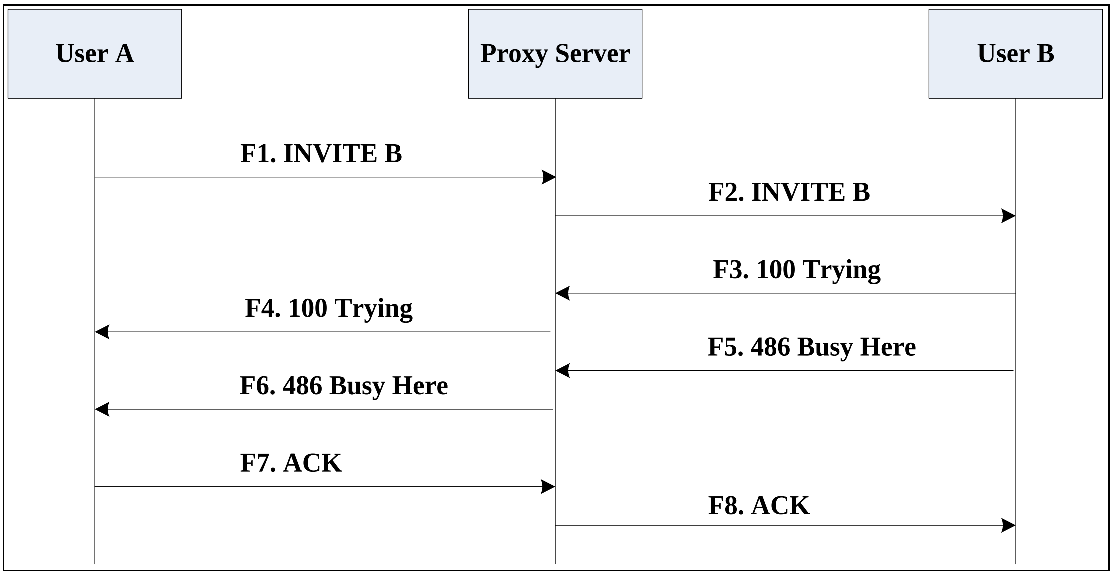
The following figure illustrates the scenario of an unsuccessful call caused by the called user's being busy. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink phones.

The call flow scenario is as follows:

1. User A calls User B.

2. User B is busy on the 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	User B sends a SIP 100 Trying response to

Step	Action	Description
	Server	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 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 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.

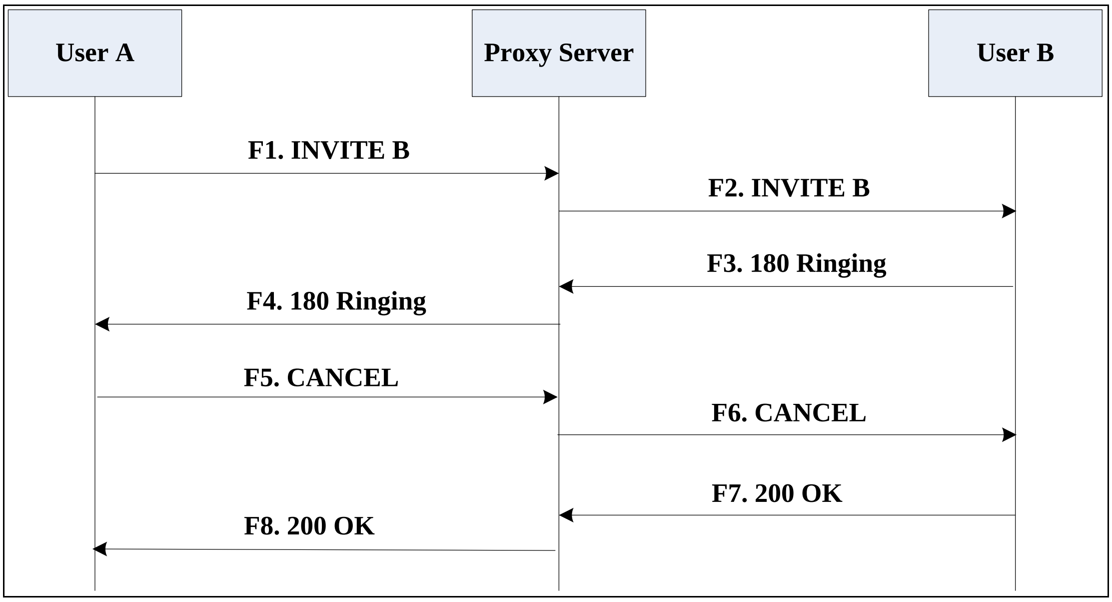
Unsuccessful Call Setup—Called User Does Not Answer

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 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

Step	Action	Description
		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	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.

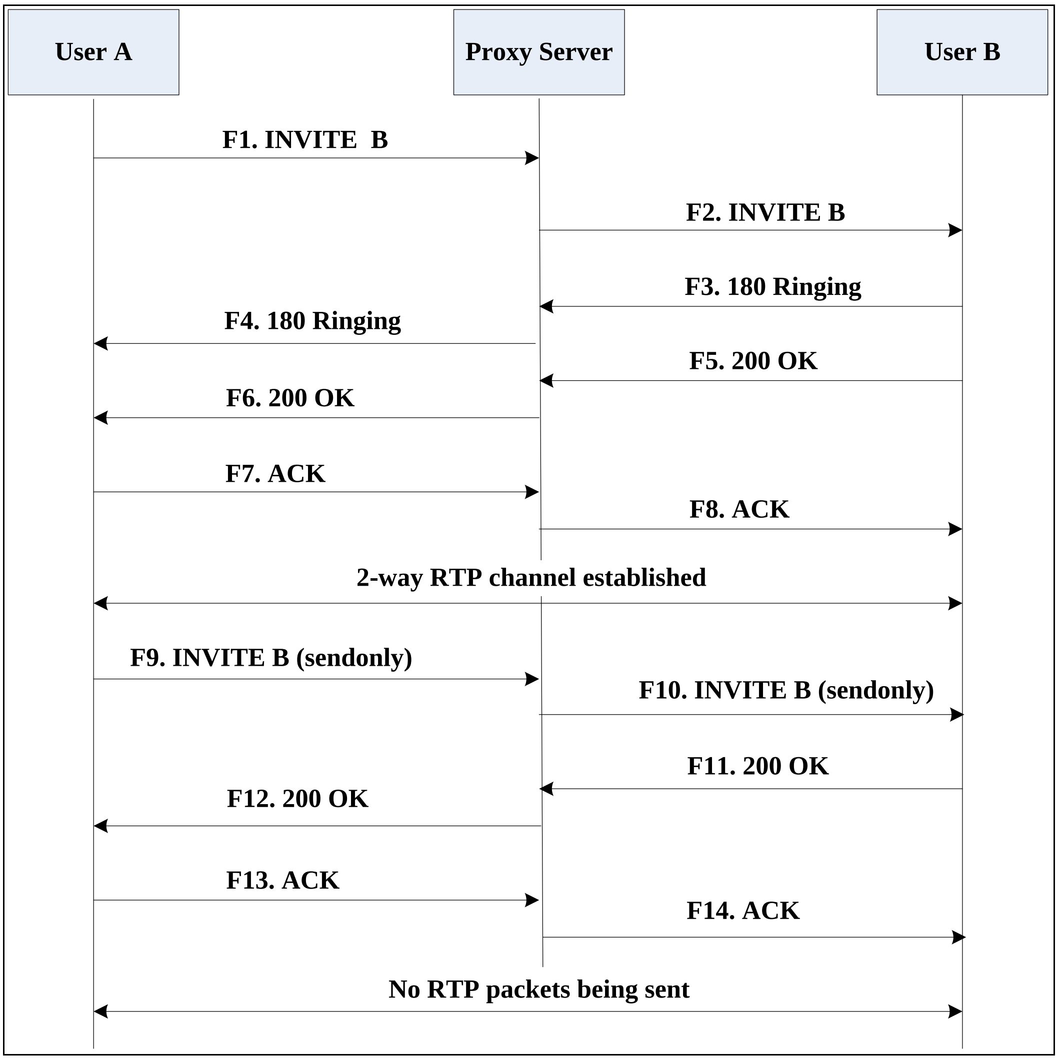
Successful Call Setup and Call Hold

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 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.

Step	Action	Description
		• 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 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.

Step	Action	Description
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 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.

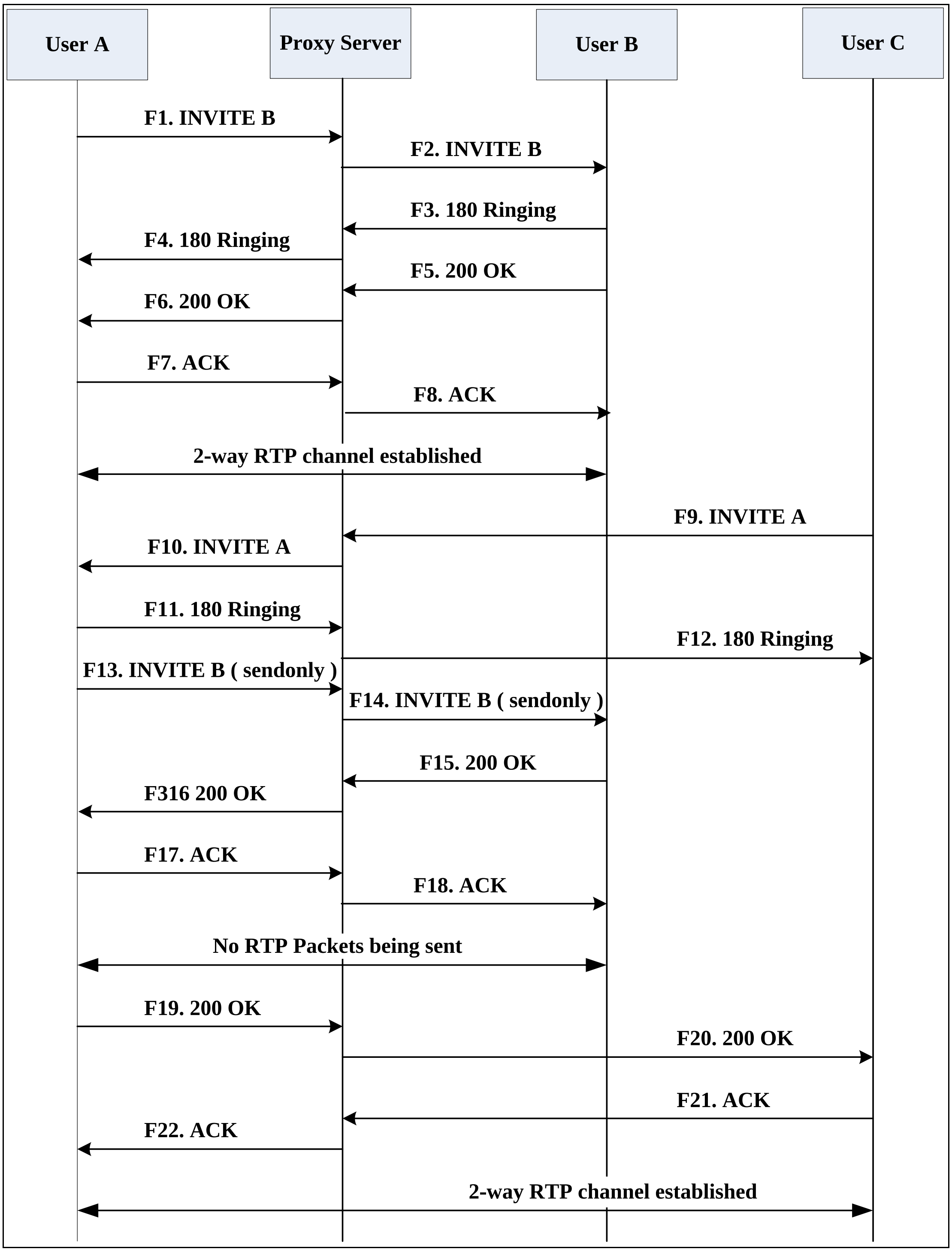
Successful Call Setup and Call Waiting

The following figure illustrates a successful call between Yealink 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 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.

Step	Action	Description
		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	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.

Step	Action	Description
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User C to Proxy Server	User C sends a SIP INVITE message to the proxy server. The INVITE request is an invitation to User A to participate in a call 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.

Step	Action	Description
F14	INVITE−Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F15	200 OK−User B to Proxy Server	User B sends a 200 OK to the proxy server. The 200 OK response indicates that the INVITE was successfully processed.
F16	200 OK−Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully placed on 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 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 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.

Step	Action	Description
F1	INVITE—User A to Proxy Server	User A sends an INVITE message to the proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: ● The IP address of User B is inserted in the Request-URI field. ● User A is identified as the call session initiator in the From field. ● A unique numeric identifier is assigned to the call and is inserted in 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

Step	Action	Description
		been made.
F6	200 OK−Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
F7	ACK−User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK−Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	REFER−User B to Proxy Server	User B sends a REFER message to the proxy server. User B performs a blind transfer of User A to User C.
F10	202 Accepted−Proxy Server to User B	The proxy server sends a SIP 202 Accept response to User B. The 202 Accepted 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.

Step	Action	Description
F17	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F18	INVITE—Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C.
F19	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F20	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted
F21	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies the proxy server that the connection has been made.
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

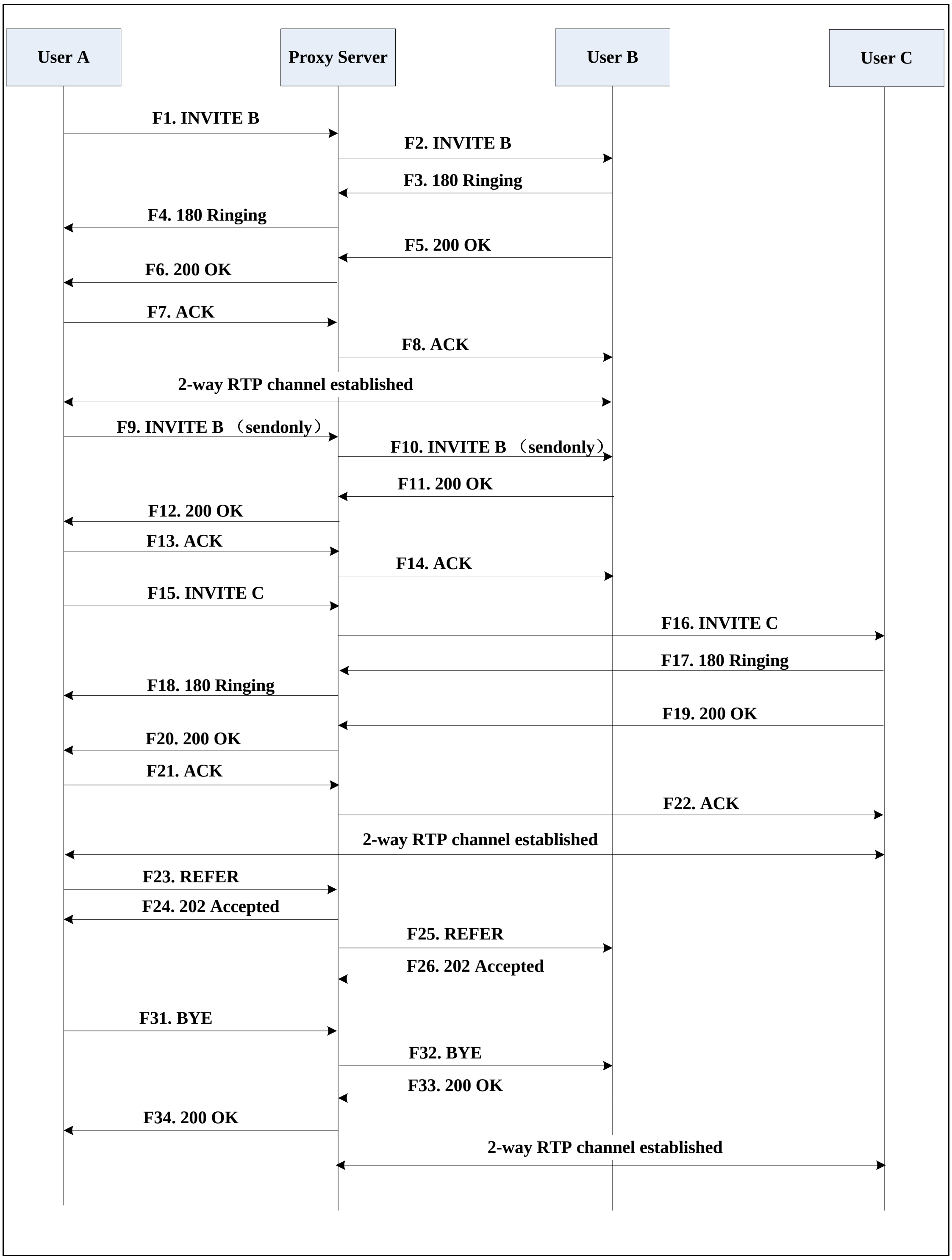
The following figure illustrates a successful call between Yealink phones in which two parties are in a call and then one of the parties transfers the call to the third party with consultation. This is called consultative transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.

2. User B answers the call.
3. User A calls User C.
4. User C answers the call.
5. User A transfers the call to User C.

Call is established between User B and User C.



Step	Action	Description
F1	INVITE−User A to Proxy Server	User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: ● The IP address of User B is inserted in the Request-URI field. ● User A is identified as the call session 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.

Step	Action	Description
F7	ACK–User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK–Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE–User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE–Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK–User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies 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

Step	Action	Description
		the INVITE request to User C.
F17	180 Ringing−User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F18	180 Ringing−Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F19	200OK−User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F20	200OK−Proxy Server to User A	The proxy server forwards the SIP 200 OK 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

Step	Action	Description
		transfer.
F27	BYE−User A to Proxy Server	User A terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User A wants to release the call.
F28	BYE−Proxy Server to User B	The proxy server forwards the BYE request to User B.
F29	200OK−User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that User B has received the BYE request.
F30	200OK−Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.

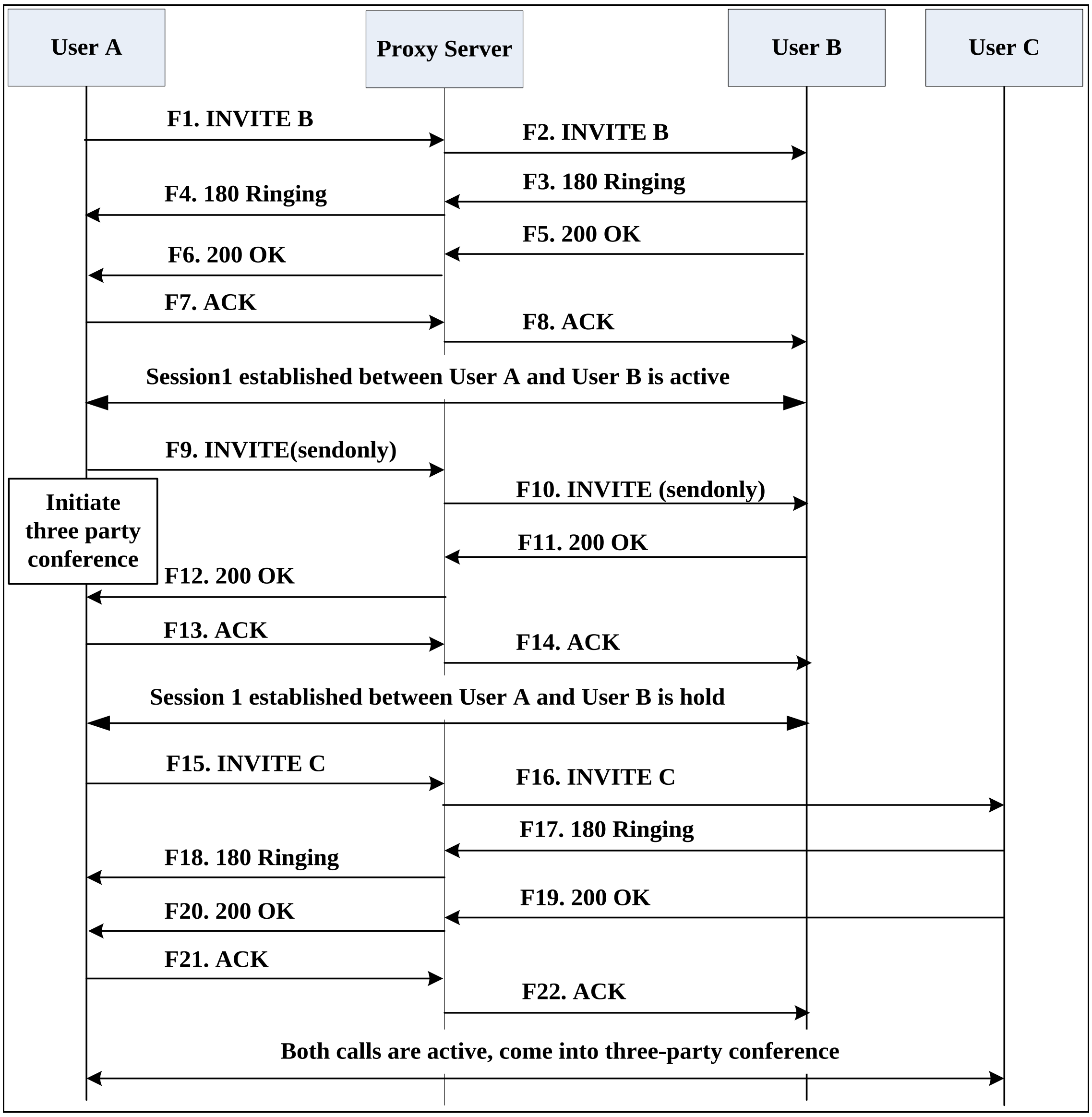
Call Conference

The following figure illustrates successful 3-way calling between Yealink 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 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

Step	Action	Description
		assigned to the call and is inserted in the Call-ID field. ● The transaction number within a single call leg is identified in the CSeq field. ● The media capability User A is ready to receive is specified. ● The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE−Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	180 Ringing−User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
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

Step	Action	Description
		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 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

Step	Action	Description
		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 sends the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response.