Skype for Business® HD IP Phone Administrator Guide

Contents

Device Provisioning..38

Firmware Upgrade...52

Audio Features...53

Troubleshooting Methods..158

Troubleshooting Solutions...172

Introduction

Yealink administrator guide provides general guidance on setting up device network, provisioning and managing Skype for Business devices. This guide is not intended for end users, but administrators.

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

- Set up a provisioning server.
- Provision the device with features and settings.
- Troubleshoot, update, and maintain the devices.

The information detailed in this guide applies to the following Yealink devices running firmware:

- MP56 Skype for Business phones: 122.9.0.4 and later
- T48S/T46S/T42S/T41S Skype for Business phones: 66.9.0.80 or later.
- T58A/T56A/T55A Skype for Business phones: 55.9.0.14 or later.
- CP960 Skype for Business phones: 73.8.0.35 or later.

Read the *Yealink Products Regulatory Notices* guide for all regulatory and safety guidance.

- Related Documentations
- Typographic and Writing Conventions
- Recommended References

Related Documentations

The following related documents are available:

- Quick Start Guides, describe how to assemble Skype for Business devices and configure the most basic features available on the devices.
- User Guides, describe how to configure and use the basic and advanced features available on the devices via the phone user interface or web user interface.
- Auto Provisioning Guide, describes how to provision the devices using configuration files.

  The *Auto Provisioning Guide* is to serve as a basic guidance for provisioning Yealink Skype for Business devices with a provisioning server. If you are a novice, this guide is helpful for you.
- Description of Configuration Parameters in CFG Files, describes all configuration parameters in configuration files.

  Note that the Yealink administrator guide contains most parameters. If you want to find out more parameters which are not listed in the administrator guide, please refer to the Description of Configuration Parameters in CFG Files guide.
- Deployment Guide, which describes how to deploy phones in a Microsoft Skype for Business Server environment.
- Yealink CPW90 Quick Start Guide, which describes how to connect CPW90 wireless expansion microphones to CP960 Skype for Business phone.

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

Typographic and Writing Conventions

Yealink documentations contain a few typographic conventions and writing conventions.

You need to know the following basic typographic conventions to distinguish the 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 (for example, select **Settings** > **License**.
	Also used to emphasize text (for example, **Important!**).
Italics	Used to emphasize text, to show the example values or inputs (format of examples: http(s)://[*IPv6address*]).

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 device's 12-digit MAC address. If you see <deviceIPAddress>, enter your device's IP address.
>	Indicates that you need to select an item from a menu. For example, **Settings** > **Basic** indicates that you need to select **Basic** from the **Settings** menu.

Recommended References

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

To access the latest Release Notes or other guides for Yealink devices, refer to the Document Download page for your device 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 T56A Skype for Business phone as an example for reference. For more details on other Skype for Business devices, refer to *Yealink Skype for Business device-specific user guide*.

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

Getting Started

This chapter provides basic initialization instructions for Skype for Business devices.

- Initialization Process Overview
- Verifying Startup
- Skype for Business Feature License

Initialization Process Overview

The initialization process of the device is responsible for network connectivity and operation of the device in your local network. Once you connect your device to the network and to an electrical supply, the device begins its initialization process.

- Loading the ROM File
- Configuring the VLAN

- Querying the DHCP (Dynamic Host Configuration Protocol) Server
- Contacting the Provisioning Server
- Updating Firmware
- Downloading the Resource Files

Loading the ROM File

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

Configuring the VLAN

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

Querying the DHCP (Dynamic Host Configuration Protocol) Server

The device is capable of querying a DHCP server.

After network connectivity is established, the device can obtain the following network parameters from the DHCP server during initialization:

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

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

Contacting the Provisioning Server

If you configure the device to obtain configurations from the provisioning server, it will be connected to the provisioning server, and then download the configuration file(s) during startup. The device will be able to resolve and update configurations written in the configuration file(s). If the device does not obtain configurations from the provisioning server, the device will use the configurations stored in the flash memory.

Updating Firmware

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

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

Downloading the Resource Files

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

Verifying Startup

After connected to the power and network, the devices begin the initialization process:

1. The power LED indicators of MP56/T58A/T56A/T55A/T48S/T46S/T42S/T41S glow red.

   The mute touch key LED indicators of CP960 glow red.
2. The message "Initializing… Please wait" (or "Initializing…") appears on the LCD screen when the devices start up.
3. The phones enter the login screen.

Skype for Business Feature License

By default, the phone has a built-in Skype for Business feature license, which allows the user to use Yealink phones with Skype for Business features directly.

Any Open SIP build upgrades to Skype for Business build will be required to apply and import the license.

Any Skype for Business build will not be allowed to downgrade to the Open SIP from this release. If Skype for Business phones are under temporary license (for demo testing purpose) and want to get back to Open SIP, please contact the Yealink support team for technical support for an unlock license.

Once upgraded to the latest Skype for Business, it will not be allowed to downgrade to the previous Skype for Business version.

Please go to Yealink License Platform to apply for a license or unlock license.

📝 **Note:** When applying for the license, please pay attention to distinguishing between Teams and skype for business version, as well as the phone model you are applying for.

- Importing License via the Web User Interface
- Importing License Configuration

Importing License via the Web User Interface

If the device has not imported a license or the license is expired, you need to import the license manually.

Procedure

1. On your web user interface, go to **Security** > **License**.
2. Click **Browse** to select the license from your local system.
3. Click **Upload**.

Importing License Configuration

The following table lists the parameter you can use to import license.

Parameter	lync_license_dat.url [1]	<y0000000000xx>.cfg

Description	It configures the access URL of the Skype for Business feature license.
	Example:
	lync_license_dat.url = http://192.168.1.20/License_$MAC.dat
	The devices will replace the characters "$MAC" with their MAC addresses during auto provisioning. For example, the MAC address of one T56A Skype for Business device is 00156543EC97. When performing auto provisioning, the device will request to download the License_00156543ec97.dat file from the provisioning server address "http://192.168.1.20".
Permitted Values	String within 99 characters
Default	Blank
Web UI	**Security** > **License**

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

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 the 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 the 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 the 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 the On-Premises account and Online account.

📝 **Note:** If the phone reboots after successful login, the login credentials from the previous Sign-In will be cached. Users can sign in successfully without re-entering the credentials.

If the Active Directory Federation Services (ADFS) or Single Sign-On (SSO) authentication method is used in your environment, you can still use the user sign-in/sign in via pc/web sign-in method to sign into Skype for Business successfully.

- PIN Authentication
- User Sign-in
- Web Sign-in
- Signing Out of Skype for Business Configuration

Related information
BToE

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 option 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 support PIN Authentication sign-in method.

Contact your network administrator for more information.

- PIN Authentication Configuration

PIN Authentication Configuration

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

Parameter	features.pin_authentication.enable	<y0000000000xx>.cfg
Description	It enables or disables the user to sign into the phone using PIN Authentication method.	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Parameter	static.account.sfb.1.pin_number	<MAC>.cfg
Description	It configures the phone's extension for the PIN Authentication method.	
Permitted Values	String within 128 characters	
Default	Blank	
Web UI	**Account** > **Register** > **Extension**	
Phone UI	**Sign in** > **PIN Authentication** > **Extension**	
Parameter	static.account.sfb.1.pin_password	<MAC>.cfg
Description	It configures the PIN for the PIN Authentication method.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	**Account** > **Register** > **Pin**	
Phone UI	**Sign in** > **PIN Authentication** > **Pin**	
Parameter	features.remember_password.enable[1]	<y0000000000xx>.cfg
Description	It enables or disables a **Remember Password** option to appear on the phone login screen. **Note:** It is not applicable to CP960/T58A/T56A/MP56 phones.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	**Features** > **General Information** > **Remember Password**	

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

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.

- User Sign-in Configuration

User Sign-in Configuration

The following table lists the parameters you can use to configure the user sign-in method.

Parameter	features.user_sign_in.enable	<y0000000000xx>.cfg
Description	It enables or disables the user to sign into the phone using User Sign-in method.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Parameter	static.account.sfb.1.server	<MAC>.cfg
Description	It configures the sign-in address for the user sign-in method. The value format is username@domain.com.	
Permitted Values	SIP URI	
Default	Blank	
Web UI	**Account** > **Register** > **Login address**	
Phone UI	**Sign in** > **User Sign-in** > **Address**	
Parameter	static.account.sfb.1.user_name	<MAC>.cfg
Description	It 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.	
Permitted Values	String within 128 characters	
Default	Blank	
Web UI	**Account** > **Register** > **Register Name**	
Phone UI	**Sign in** > **User Sign-in** > **UserName**	
Parameter	static.account.sfb.1.password	<MAC>.cfg
Description	It configures the password for the user sign-in method.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	**Account** > **Register** > **Password**	
Phone UI	**Sign in** > **User Sign-in** > **Password**	

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.

- Web Sign-in Configuration

Web Sign-in Configuration

The following table lists the parameters you can use to configure the web sign-in method.

Parameter	features.web_sign_in.enable	<y0000000000xx>.cfg
Description	It enables or disables the user to sign into the phone using web sign-in method.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Features** > **General Information** > **Web Sign in**	
Parameter	features.device_pairing.url	<y0000000000xx>.cfg
Description	It configures the server URL for device pairing, so that you can sign into the phone using web sign-in method.	
Permitted Values	URL within 512 characters	
Default	https://bootstrap.pinauth.services.skypeforbusiness.com	
Parameter	features.remember_password.enable[1]	<y0000000000xx>.cfg
Description	It enables or disables a **Remember Password** option to appear on the phone login screen. **Note:** It is not applicable to CP960/T58A/T56A/MP56 phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Features** > **General Information** > **Remember Password**	

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

Signing Out of Skype for Business Configuration

The following table lists the parameters you can use to sign out of Skype for Business.

Parameter	phone_setting.idle_sign_out.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to sign out of Skype for Business Server from the idle screen. **Note:** It is only applicable to CP960/T58A/T56A/T55A/MP56 Skype for Business phones.	

Permitted Values	**0**-Disabled, you can only sign out of Skype for Business Server on your phone by navigating to **Menu** > **Setting** > **Advanced** > **Sign Out** or **More** > **Advanced** > **Sign Out**.
	1-Enabled, you can only sign out of Skype for Business Server by tapping your avatar, and then select **Sign Out**.
Default	For CP960: 0
	For T58A/T56A/T55A/MP56: 1

Device Network

Yealink Skype for Business devices operate on an Ethernet local area network (LAN). You can configure the local area network to accommodate many network designs, which varies by organizations and Yealink Skype for Business devices.

- IPv4 and IPv6 Network Settings
- DHCP Option for IPv4
- VLAN
- Wi-Fi
- Internet Port and PC Port
- Quality of Service (QoS)
- 802.1x Authentication

IPv4 and IPv6 Network Settings

Skype for Business devices support IPv4 addressing mode, IPv6 addressing mode, as well as an IPv4&IPv6 dual-stack addressing mode. After connected to the wired network, the devices can obtain the IPv4 or IPv6 network settings from a Dynamic Host Configuration Protocol (DHCP) server if your network supports it. To make it easier to manage IP settings, we recommend using automated DHCP which is possible to eliminate repetitive manual data entry. You can also configure IPv4 or IPv6 network settings manually.

📝 **Note:** Skype for Business devices comply with the DHCPv4 specifications documented in RFC 2131, and DHCPv6 specifications documented in RFC 3315.

- IP Addressing Mode Configuration
- IPv4 Configuration
- IPv6 Configuration

IP Addressing Mode Configuration

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

Parameter	static.network.ip_address_mode[1]	<MAC>.cfg
Description	It configures the IP addressing mode.	
Permitted Values	**0**-IPv4	
	1-IPv6	
	2-IPv4 & IPv6	

Default	0
Web UI	**Network** > **Basic** > **Internet Port** > **Mode(IPv4/IPv6)**
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IP Mode**

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

IPv4 Configuration

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

Parameter	static.network.internet_port.type[1]	<MAC>.cfg
Description	It configures the Internet port type for IPv4. **Note**: It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6).	
Permitted Values	**0**-DHCP **2**-Static IP	
Default	0	
Web UI	**Network** > **Basic** > **IPv4 Config**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv4** > **Type**	
Parameter	static.network.internet_port.ip[1]	<MAC>.cfg
Description	It configures the IPv4 address. **Note**: It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP).	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	**Network** > **Basic** > **IPv4 Config** > **Static IP Address** > **IP Address**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv4** > **Type(Static IP)** > **IP Address**	
Parameter	static.network.internet_port.mask[1]	<MAC>.cfg
Description	It configures the IPv4 subnet mask. **Note**: It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP).	
Permitted Values	Subnet Mask	
Default	Blank	

Web UI	Network > Basic > IPv4 Config > Static IP Address > Subnet Mask
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv4** > **Type(Static IP)** > **Subnet Mask**

Parameter	static.network.internet_port.gateway[1]	<MAC>.cfg
Description	It configures the IPv4 default gateway. **Note**: It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP).	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	**Network** > **Basic** > **IPv4 Config** > **Static IP Address** > **Default Gateway**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv4** > **Type(Static IP)** > **Default Gateway**	

Parameter	static.network.static_dns_enable[1]	<y0000000000xx>.cfg
Description	It triggers the static DNS feature to on or off. **Note:** It works only if "static.network.internet_port.type" is set to 0 (DHCP).	
Permitted Values	**0**-Off, the device will use the IPv4 DNS obtained from DHCP. **1**-On, the device will use manually configured static IPv4 DNS.	
Default	0	
Web UI	**Network** > **Basic** > **IPv4 Config** > **Static DNS**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv4** > **Type(DHCP)** > **Static DNS**	

Parameter	static.network.primary_dns[1]	<MAC>.cfg
Description	It configures the primary IPv4 DNS server. **Note**: It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure "static.network.static_dns_enable" is set to 1 (On).	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	**Network** > **Basic** > **IPv4 Config** > **DHCP** > **Static DNS (On)** > **Primary DNS** **Network** > **Basic** > **IPv4 Config** > **Static IP Address** > **Primary DNS**	

Phone UI	Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv4 > Type(Static IP) > Pri.DNS
	Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv4 > Type(DHCP) > Static DNS (Enabled) > Pri.DNS

Parameter	static.network.secondary_dns [1]	<MAC>.cfg
Description	It configures the secondary IPv4 DNS server. **Note**: It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure "static.network.static_dns_enable" is set to 1 (On).	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	Network > Basic > IPv4 Config > DHCP > Static DNS (On) > Secondary DNS	
	Network > Basic > IPv4 Config > Static IP Address > Secondary DNS	
Phone UI	Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv4 > Type(Static IP) > Sec.DNS	
	Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv4 > Type(DHCP) > Static DNS (Enabled) > Sec.DNS	

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

IPv6 Configuration

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

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

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

Parameter	static.network.ipv6_internet_port.type[1]	<MAC>.cfg
Description	It configures the Internet port type for IPv6. **Note**: It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6).	
Permitted Values	**0**-DHCP	
	1-Static IP	
Default	0	
Web UI	Network > Basic > IPv6 Config	
Phone UI	Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv6	
Parameter	static.network.ipv6_internet_port.ip[1]	<MAC>.cfg

Description	It configures the IPv6 address.
	Note: It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP).
Permitted Values	IPv6 Address
Default	Blank
Web UI	**Network** > **Basic** > **IPv6 Config** > **Static IP Address** > **IP Address**
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv6** > **Type(Static IP)** > **IP Address**

Parameter	static.network.ipv6_prefix[1]	<MAC>.cfg
Description	It configures the IPv6 prefix.	
	Note: It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP).	
Permitted Values	Integer from 0 to 128	
Default	64	
Web UI	**Network** > **Basic** > **IPv6 Config** > **Static IP Address** > **IPv6 Prefix(0~128)**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv6** > **Type(Static IP)** > **IPv6 IP Prefix**	

Parameter	static.network.ipv6_internet_port.gateway[1]	<MAC>.cfg
Description	It configures the IPv6 default gateway.	
	Note: It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP).	
Permitted Values	IPv6 Address	
Default	Blank	
Web UI	**Network** > **Basic** > **IPv6 Config** > **Static IP Address** > **Gateway**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv6** > **Type(Static IP)** > **Gateway**	

Parameter	static.network.ipv6_static_dns_enable[1]	<MAC>.cfg
Description	It triggers the static IPv6 DNS feature to on or off.	
	Note: It works only if "static.network.ipv6_internet_port.type" is set to 0 (DHCP).	
Permitted Values	**0**-Off, the device will use the IPv6 DNS obtained from DHCP.	
	1-On, the device will use manually configured static IPv6 DNS.	
Default	0	

Web UI	**Network** > **Basic** > **IPv6 Config** > **IPv6 Static DNS (or Static IPv6 DNS)**
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv6** > **Type(DHCP)** > **Static DNS**
Parameter	**static.network.ipv6_primary_dns**[1] **<MAC>.cfg**
Description	It configures the primary IPv6 DNS server. **Note**: It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure "static.network.ipv6_static_dns_enable" is set to 1 (On).
Permitted Values	IPv6 Address
Default	Blank
Web UI	**Network** > **Basic** > **IPv6 Config** > **Static IP Address** > **Primary DNS**
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv6** > **Type(Static IP)** > **Pri.DNS** **Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv6** > **Type(DHCP)** > **Static DNS(Enabled)** > **Pri.DNS**
Parameter	**static.network.ipv6_secondary_dns**[1] **<MAC>.cfg**
Description	It configures the secondary IPv6 DNS server. **Note**: It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure "static.network.ipv6_static_dns_enable" is set to 1 (On).
Permitted Values	IPv6 Address
Default	Blank
Web UI	**Network** > **Basic** > **IPv6 Config** > **Static IP Address** > **Secondary DNS**
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv6** > **Type(Static IP)** > **Sec.DNS** **Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv6** > **Type(DHCP)** > **Static DNS(Enabled)** > **Sec.DNS**
Parameter	**static.network.ipv6_icmp_v6.enable**[1] **<MAC>.cfg**
Description	It enables or disables the phone to obtain IPv6 network settings via SLAAC (Stateless Address Autoconfiguration). **Note**: It works only if "static.network.ipv6_internet_port.type" is set to 0 (DHCP).
Permitted Values	**0**-Disabled **1**-Enabled
Default	1
Web UI	**Network** > **Advanced** > **ICMPv6 Status** > **Active**

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

DHCP Option for IPv4

The Skype for Business device can obtain IPv4-related parameters in an IPv4 network via the DHCP option.

📝 **Note:** For more information on DHCP options, refer to RFC 2131 or RFC 2132.

- Supported DHCP Option for IPv4
- DHCP Option 160 and Option 161
- DHCP Option 66, Option 43 and Custom Option
- DHCP Option 42 and Option 2
- DHCP Option 12
- DHCP Option 60
- DHCP Option 120

Supported DHCP Option for IPv4

The following table lists common DHCP options for IPv4 supported by the devices.

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 the client should use when resolving hostnames via DNS.
Broadcast Address	28	Specify the broadcast address in use on the client's subnet.
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.

Parameter	DHCP Option	Description
TFTP Server Name	66	Identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.
Skype for Business Server	120	Specify a list of Skype for Business Servers available to the client.

DHCP Option 160 and Option 161

Yealink Skype for Business devices 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 device 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 the custom option is configured.

- DHCP Option 160 and Option 161 Configuration

DHCP Option 160 and Option 161 Configuration

The following table lists the parameters you can use to configure DHCP option 160 or 161.

Parameter	static.auto_provision.dhcp_option.enable[1]	<y0000000000xx>.cfg
Description	It triggers the DHCP Option feature to on or off.	
Permitted Values	**0**-Off **1**-On	
Default	1	
Web UI	**Settings** > **Auto Provision** > **DHCP Active**	

Parameter	static.auto_provision.dhcp_option.list_user_options[1]	<y0000000000xx>.cfg
Description	It configures the custom DHCP option for requesting provisioning server address. Multiple DHCP options are separated by commas. **Note**: It works only if "static.auto_provision.dhcp_option.enable" is set to 1 (On).	
Permitted Values	Integer from 128 to 254	
Default	160,161	
Web UI	**Settings** > **Auto Provision** > **Custom Option(128~254)**	

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

DHCP Option 66, Option 43 and Custom Option

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

The Skype for Business device can obtain the Auto Configuration Server (ACS) address by detecting option 43 during startup.

To obtain the server address via DHCP option, make sure you have configured the DHCP option on the device. The option must be in accordance with the one defined in the DHCP server.

> 📝 **Note:** If you fail to configure the DHCP options for discovering the provisioning server on the DHCP server, an alternate method of automatically discovering the provisioning server address is required. One possibility is that connecting to the secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server address. For more information, refer to RFC 3925. If a single alternate DHCP server responds, this is functionally equivalent to the scenario where the primary DHCP server responds with a valid provisioning server address. If no DHCP server responds, the INFORM query process will retry and until the time is out.

DHCP Option 42 and Option 2

Yealink Skype for Business devices can use the NTP server address offered by DHCP.

DHCP option 42 is used to specify a list of NTP servers available to the client by IP address. NTP servers should be listed in order of preference.

DHCP option 2 is used to specify the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).

Related information
NTP Settings

DHCP Option 12

You can specify a hostname for the device when using DHCP. The DHCP client uses option 12 to send a predefined hostname to the DHCP registration server. The name may or may not be qualified with the local domain name (based on RFC 2132). See RFC 1035 for character restrictions.

* DHCP Option 12 Hostname Configuration

DHCP Option 12 Hostname Configuration

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

Parameter	static.network.dhcp_host_name[1]	<y0000000000xx>.cfg
Description	It configures the DHCP option 12 hostname on the device.	
Permitted Values	String within 99 characters	
Default	For T58A: SIP-T58 For T56A: SIP-T56A For CP960: SIP-CP960 For T55A: SIP-T55A For MP56: MP56. For T48S: SIP-T48S For T46S: SIP-T46S For T42S: SIP-T42S For T41S: SIP-T41S	

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

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).

- DHCP Option 60 Configuration

DHCP Option 60 Configuration

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

Parameter	static.auto_provision.dhcp_option.option60_value[1]	<y0000000000xx>.cfg
Description	It configures the value (vendor name of the device) of DHCP option 60.	
Permitted Values	String within 99 characters	
Default	MS-UC-Client	
Web UI	**Settings** > **Auto Provision** > **DHCP Option Value**	

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

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.

- DHCP Option 120 Configuration

DHCP Option 120 Configuration

The following table lists the parameter you can use to configure DHCP option 120.

Parameter	sip.option120_get_lync_server.enable	<y0000000000xx>.cfg
Description	It enables or disables phones to obtain the Skype for Business Server address from DHCP by detecting DHCP option 120.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Features** > **General Information** > **Use DHCP Option 120**	

VLAN

The purpose of VLAN configurations on the device is to insert a tag with VLAN information to the packets generated by the device. When VLAN is properly configured for the ports (Internet port and PC port) on the device, the device 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 devices allows simultaneous access to a regular PC. This feature allows a PC to be daisy chained to a device and the connection for both PC and phone to be trunked through the same physical Ethernet cable.

In addition to manual configuration, the device also supports the 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.

- LLDP Configuration
- CDP Configuration
- Manual VLAN Configuration
- DHCP VLAN Configuration

LLDP Configuration

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

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

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

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

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

CDP Configuration

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

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

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

Parameter	static.network.cdp.enable[1]	<y0000000000xx>.cfg
Description	It enables or disables the CDP feature.	
Permitted Values	**0**-Disabled **1**-Enabled, the phone will attempt to determine its VLAN ID through CDP.	
Default	1	
Web UI	**Network** > **Advanced** > **CDP** > **Active**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **CDP** > **CDP Status**	
Parameter	static.network.cdp.packet_interval[1]	<y0000000000xx>.cfg
Description	It configures the interval (in seconds) at which the phone sends the CDP request. **Note**: It works only if "static.network.cdp.enable" is set to 1 (Enabled).	
Permitted Values	Integer from 1 to 3600	
Default	60	
Web UI	**Network** > **Advanced** > **CDP** > **CDP Interval (1~3600s)**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **CDP** > **Packet Interval**	

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

Manual VLAN Configuration

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

The PC port is not applicable to CP960, and you can only configure VLAN for the Internet port manually.

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

Parameter	static.network.vlan.internet_port_enable[1]	<y0000000000xx>.cfg
Description	It enables or disables the VLAN for the Internet port.	
Permitted Values	**0**-Disabled **1**-Enabled	

Default	0
Web UI	**Network** > **Advanced** > **VLAN** > **WAN Port** > **Active**
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **VLAN** > **WAN Port** > **VLAN Status**
Parameter	**static.network.vlan.internet_port_vid**[1] **<y0000000000xx>.cfg**
Description	It configures the VLAN ID for the Internet port. **Note**: It works only if "static.network.vlan.internet_port_enable" is set to 1 (Enabled).
Permitted Values	Integer from 1 to 4094
Default	1
Web UI	**Network** > **Advanced** > **VLAN** > **WAN Port** > **VID**
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **VLAN** > **WAN Port** > **VID Number**
Parameter	**static.network.vlan.internet_port_priority**[1] **<y0000000000xx>.cfg**
Description	It configures the VLAN priority for the Internet port. 7 is the highest priority, 0 is the lowest priority. **Note**: It works only if "static.network.vlan.internet_port_enable" is set to 1 (Enabled).
Permitted Values	Integer from 0 to 7
Default	1
Web UI	**Network** > **Advanced** > **VLAN** > **WAN Port** > **Priority**
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **VLAN** > **WAN Port** > **Priority**
Parameter	**static.network.vlan.pc_port_enable**[1] **<y0000000000xx>.cfg**
Description	It enables or disables the VLAN for the PC port. **Note**: It works only if "static.network.pc_port.enable" is set to 1 (Auto Negotiation).
Permitted Values	**0**-Disabled **1**-Enabled
Default	0
Supported Devices	All devices except CP960
Web UI	**Network** > **Advanced** > **VLAN** > **PC Port** > **Active**
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **VLAN** > **PC Port** > **VLAN Status**

Parameter	static.network.vlan.pc_port_vid[1]	**\<y0000000000xx\>.cfg**
Description	It configures the VLAN ID for the PC port. **Note**: It works only if "static.network.pc_port.enable" is set to 1 (Auto Negotiation) and "static.network.vlan.pc_port_enable" is set to 1 (Enabled).	
Permitted Values	Integer from 1 to 4094	
Default	1	
Supported Devices	All devices except CP960	
Web UI	**Network** > **Advanced** > **VLAN** > **PC Port** > **VID**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **VLAN** > **PC Port** > **VID Number**	
Parameter	**static.network.vlan.pc_port_priority**[1]	**\<y0000000000xx\>.cfg**
Description	It configures the VLAN priority for the PC port. 7 is the highest priority, 0 is the lowest priority. **Note**: It works only if "static.network.pc_port.enable" is set to 1 (Auto Negotiation) and "static.network.vlan.pc_port_enable" is set to 1 (Enabled).	
Permitted Values	Integer from 1 to 7	
Default	0	
Supported Devices	All devices except CP960	
Web UI	**Network** > **Advanced** > **VLAN** > **PC Port** > **Priority**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **VLAN** > **PC Port** > **Priority**	

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

DHCP VLAN Configuration

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

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

Parameter	static.network.vlan.dhcp_enable[1]	**\<y0000000000xx\>.cfg**
Description	It enables or disables the DHCP VLAN discovery feature on the device.	
Permitted Values	**0**-Disabled **1**-Enabled.	
Default	1	
Web UI	**Network** > **Advanced** > **DHCP VLAN** > **Active**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **VLAN** > **DHCP VLAN** > **DHCP VLAN**	
Parameter	**static.network.vlan.dhcp_option**[1]	**\<y0000000000xx\>.cfg**

Description	It configures the DHCP option from which the device obtains the VLAN settings. You can configure at most five DHCP options and separate them by commas.
Permitted Values	Integer from 1 to 255
Default	132
Web UI	**Network** > **Advanced** > **DHCP VLAN** > **Option(1-255)**
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **VLAN** > **DHCP VLAN** > **Option**

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

Wi-Fi

Wi-Fi feature enables you to connect the devices to the organization's wireless network. Wi-Fi feature is only applicable to MP56/CP960/T58A/T56A/T55A/T48S Skype for Business phones.

> **Note:** For T56A/T55A/T48S Skype for Business phones, 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.

- Wi-Fi Configuration

Wi-Fi Configuration

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

Parameter	**static.wifi.function.enable** [1]	**<y0000000000xx>.cfg**
Description	It enables or disables the Wi-Fi feature. **Note**: It is only applicable to CP960/T58A/T56A/T55A/MP56 Skype for Business phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Parameter	**static.wifi.enable**	**<y0000000000xx>.cfg**
Description	It activates or deactivates the Wi-Fi mode. **Note:** It is only applicable to CP960/T58A/T56A/T55A/T48S/MP56 Skype for Business phones. For CP960/T58A/T56A/T55A/MP56, it works only if "static.wifi.function.enable" is set to 1 (Enabled).	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Network** > **Wi-Fi** > **Wi-Fi Active (or Wi-Fi)** (T48S only)	
Phone UI	**Menu** > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi**	

Parameter	static.wifi.X.label[2]	<y0000000000xx>.cfg
Description	It configures the profile name of a specific wireless network. **Note:** It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	**Network** > **Wi-Fi** > **Profile Name** (T48S only)	
Phone UI	**Menu** > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **Add** > **Profile Name** **Menu** > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **The storage network** > **Edit** > **Profile Name** (T48S only)	
Parameter	static.wifi.X.ssid[2]	<y0000000000xx>.cfg
Description	It configures the SSID of a specific wireless network. SSID is a unique identifier for accessing wireless access points. **Note:** It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	**Network** > **Wi-Fi** > **SSID** (T48S only)	
Phone UI	**Menu** > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **Add** > **SSID** **Menu** > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **The storage network** > **Edit** > **SSID**	
Parameter	static.wifi.X.priority[2]	<y0000000000xx>.cfg
Description	It configures the priority for a specific wireless network. 5 is the highest priority, 1 is the lowest priority. **Note:** It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	Integer from 1 to 5	
Default	1	
Web UI	**Network** > **Wi-Fi** > **Change Priority** (T48S only)	
Phone UI	**Menu** > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **The storage network** > **Move Up/ Move Down** (T48S only)	
Parameter	static.wifi.X.security_mode[2]	<y0000000000xx>.cfg
Description	It configures the security mode of a specific wireless network. **Note:** It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	

Permitted Values	**For T48S Skype for Business phone:**	
	NONE, WEP, WPA-PSK or WPA2-PSK, WPA-EAP or WPA2-EAP	
	For CP960/T58A/T56A/T55A/MP56 Skype for Business phone:	
	NONE, WEP, WPA/WPA2 PSK or 802.1x EAP	
Default	NONE	
Web UI	**Network** > **Wi-Fi** > **Secure Mode** (T48S only)	
Phone UI	**Menu** > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **Add** > **Security Mode**	
	Menu > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **The storage network** > **Edit** > **Security Mode**	
Parameter	static.wifi.X.cipher_type[2]	<y0000000000xx>.cfg
Description	It configures the encryption type of a specific wireless network.	
	If "static.wifi.X.security_mode" is set to **NONE**, the permitted value of this parameter is **NONE**.	
	If "static.wifi.X.security_mode" is set to **WEP**, the permitted value of this parameter is **WEP**.	
	If "static.wifi.X.security_mode" is set to other values, the permitted values of this parameter are **TKIP**, **AES** or **TKIP AES**.	
	Note: It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	NONE, PEAP, TLS, TTLS, PWD	
Default	NONE	
Web UI	**Network** > **Wi-Fi** > **Cipher Type** (T48S only)	
Phone UI	**Menu** > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **Add** > **Cipher Type**	
	Menu > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **The storage network** > **Edit** > **Cipher Type**	
Parameter	static.wifi.X.password[2]	<y0000000000xx>.cfg
Description	It configures the password of a specific wireless network.	
	Note: It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	**Network** > **Wi-Fi** > **PSK** (T48S only)	
Phone UI	**Menu** > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **Add** > **WPA Shared Key**	
	Menu > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **The storage network** > **Edit** > **WPA Shared Key**	
Parameter	static.wifi.X.eap_type[2]	<y0000000000xx>.cfg

Description	It configures the EAP authentication mode of a specific wireless network.
	Note: It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).
Permitted Values	**For T48S Skype for Business phone:** TTLS, PEAP or TLS **For CP960/T58A/T56A/T55A/MP56 Skype for Business phone:** PEAP, TLS, TTLS or PWD
Default	Blank

Parameter	static.wifi.X.eap_user_name[2]	<y0000000000xx>.cfg
Description	It configures the EAP authentication username of a specific wireless network.	
	Note: It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	**Network** > **Wi-Fi** > **User Name** (T48S only)	
Phone UI	**Menu** > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **Add** > **User Name** **Menu** > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **The storage network** > **Edit** > **User Name**	

Parameter	static.wifi.X.eap_password[2]	<y0000000000xx>.cfg
Description	It configures the EAP authentication password of a specific wireless network.	
	Note: It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	**Network** > **Wi-Fi** > **PSK** (T48S only)	
Phone UI	**Menu** > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **Add** > **WPA Shared Key** **Menu** > **Setting** > **Basic** > **Wi-Fi** > **Wi-Fi(On)** > **The storage network** > **Edit** > **WPA Shared Key**	

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

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

Internet Port and PC Port

Yealink Skype for Business devices support two Ethernet ports: Internet port and PC port. You can enable or disable the PC port on the devices.

The PC port is not applicable to CP960 devices.

- Supported Transmission Methods

- Internet Port and PC Port Configuration

Supported Transmission Methods

Three optional methods of transmission configuration for the device Internet port and PC port:

- Auto Negotiation
- Half-duplex (transmit in 10Mbps or 100Mbps)
- Full-duplex (transmit in 10Mbps, 100Mbps or 1000Mbps (not applicable to T41S/CP960))

Auto negotiation is configured for both Internet and PC ports on the device by default.

Internet Port and PC Port Configuration

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

Parameter	static.network.pc_port.enable[1]	<y0000000000xx>.cfg
Description	It enables or disables the PC port.	
Permitted Values	**0**-Disabled **1**-Auto Negotiation	
Default	1	
Supported Devices	All devices except CP960	
Web UI	**Network** > **PC Port** > **PC Port Active**	
Parameter	static.network.internet_port.speed_duplex[1]	<y0000000000xx>.cfg
Description	It configures the transmission method of the Internet port. **Note**: You can set the transmission speed to 1000Mbps/Auto Negotiation to transmit in 1000Mbps if the phone is connected to the switch which supports Gigabit Ethernet. We recommend that you do not change this parameter.	
Permitted Values	**0**-Auto Negotiation **1**-Full Duplex 10Mbps **2**-Full Duplex 100Mbps **3**-Half Duplex 10Mbps **4**-Half Duplex 100Mbps **5**-Full Duplex 1000Mbps (not applicable to T41S/CP960)	
Default	0	
Web UI	**Network** > **Advanced** > **Port Link** > **WAN Port Link**	
Parameter	static.network.pc_port.speed_duplex[1]	<y0000000000xx>.cfg
Description	It configures the transmission method of the PC port. **Note**: You can set the transmission speed to 1000Mbps/Auto Negotiation to transmit in 1000Mbps if the phone is connected to the switch which supports Gigabit Ethernet. We recommend that you do not change this parameter.	

Permitted Values	**0**-Auto Negotiation
	1-Full Duplex 10Mbps
	2-Full Duplex 100Mbps
	3-Half Duplex 10Mbps
	4-Half Duplex 100Mbps
	5-Full Duplex 1000Mbps (not applicable to T41S)
Default	0
Supported Devices	All devices except CP960
Web UI	**Network** > **Advanced** > **Port Link** > **PC Port Link**
Parameter	static.network.vlan.pc_port_mode[1]	**<y0000000000xx>.cfg**
Description	It configures the way the phone processes packets for the PC port when VLAN is enabled on the PC port.
	Note: When packets are sent from the Internet port to the PC port, remove the packet's tag if it is the same as the configured tag for the PC port, else forward the packets directly.
Permitted Values	**0**-when packets are sent from the PC port to the Internet port, the phone will forward the packets directly.
	1-when packets are sent from the PC port to the Internet port, and there is no VLAN tag in the packet, the phone will tag the packet with the configured tag for the PC port and then forward it.
Default	1
Supported Devices	All devices except CP960

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

Quality of Service (QoS)

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

Voice QoS

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

SIP QoS

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

DSCPs for voice and SIP packets can be specified respectively.

- QoS Configuration

QoS Configuration

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

Parameter	static.network.qos.audiotos[1]	<y0000000000xx>.cfg
Description	It configures the DSCP (Differentiated Services Code Point) for voice packets. The default DSCP value for RTP packets is 46 (Expedited Forwarding).	
Permitted Values	Integer from 0 to 63	
Default	46	
Web UI	**Network** > **Advanced** > **Voice QoS (0~63)**	
Parameter	static.network.qos.signaltos[1]	<y0000000000xx>.cfg
Description	It configures the DSCP (Differentiated Services Code Point) for SIP packets. The default DSCP value for SIP packets is 26 (Assured Forwarding).	
Permitted Values	Integer from 0 to 63	
Default	26	
Web UI	**Network** > **Advanced** > **SIP QoS (0~63)**	

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

802.1x Authentication

Yealink Skype for Business devices 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

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

- 802.1x Authentication Configuration

802.1x Authentication Configuration

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

Parameter	static.network.802_1x.mode[1]	<y0000000000xx>.cfg
Description	It configures the 802.1x authentication method.	

Permitted Values	0-EAP-None, 802.1x authentication is not required.
	1-EAP-MD5
	2-EAP-TLS
	3-EAP-PEAP/MSCHAPv2
	4-EAP-TTLS/EAP-MSCHAPv2
	5-EAP-PEAP/GTC
	6-EAP-TTLS/EAP-GTC
	7-EAP-FAST
Default	0
Web UI	**Network** > **Advanced** > **802.1x** > **802.1x Mode**
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **802.1x** > **802.1x Mode**

Parameter	static.network.802_1x.identity[1]	<y0000000000xx>.cfg
Description	It configures the user name for 802.1x authentication.	
	Note: It works only if "static.network.802_1x.mode" is set to 1, 2, 3, 4, 5, 6, or 7.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	**Network** > **Advanced** > **802.1x** > **Identity**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **802.1x** > **Identity**	

Parameter	static.network.802_1x.md5_password[1]	<y0000000000xx>.cfg
Description	It configures the password for 802.1x authentication.	
	Note: It works only if "static.network.802_1x.mode" is set to 1, 3, 4, 5, 6, or 7.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	**Network** > **Advanced** > **802.1x** > **MD5 Password**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **802.1x** > **MD5 Password**	

Parameter	static.network.802_1x.root_cert_url[1]	<y0000000000xx>.cfg
Description	It configures the access URL of the CA certificate.	
	The format of the certificate must be *.pem, *.crt, *.cer or *.der.	
	Note: It works only if "static.network.802_1x.mode" is set to 2, 3, 4, 5, 6, or 7.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Network** > **Advanced** > **802.1x** > **CA Certificates**	

Parameter	static.network.802_1x.client_cert_url[1]	<y0000000000xx>.cfg
Description	It configures the access URL of the device certificate. The format of the certificate must be *.pem. **Note**: It works only if "static.network.802_1x.mode" is set to 2 (EAP-TLS).	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Network** > **Advanced** > **802.1x** > **Device Certificates**	

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

Device Provisioning

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

For more information, refer to Yealink_Skype_for_Business_HD_IP_Phones_Auto_Provisioning_Guide.

- Provisioning Points to Consider
- Configuration Files, and Resource Files
- Provisioning Methods
- Setting Up a Provisioning Server

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.
- 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.
- 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.

Configuration Files, and Resource Files

You can use configuration files and resource files to configure device features and apply feature settings to devices. You can create or edit these files using a text editor such as UltraEdit.

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.

- Configuration Files
- Resource Files

Configuration Files

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

These configuration files contain two kinds of parameters:

- Static: The parameters start with a prefix "static.", for example, static.network.lldp.enable .
- Non-static: The parameters do not start with a prefix "static.", for example, phone_setting.phone_lock.enable.

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

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

- Common CFG File
- MAC-Oriented CFG File
- MAC-local CFG File
- Configuration File Customization

Common CFG File

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

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

Device Model	Common CFG file
T58A	y000000000058.cfg
T56A	y000000000056.cfg
T55A	y000000000099.cfg
CP960	y000000000073.cfg
MP56	y000000000122.cfg
T48S	y000000000065.cfg
T46S	y000000000066.cfg
T42S	y000000000067.cfg
T41S	y000000000068.cfg

MAC-Oriented CFG File

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

MAC-local CFG File

MAC-local CFG file, named <MAC>-local.cfg, contains the changes associated with a non-static parameter that you make via web user interface or phone user interface (for example, changes for time and date formats).

The MAC-local.cfg file uploads to the provisioning server each time the file updates. You can download the file via the web user interface.

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

> 📝 **Note:** The non-static changes that you made before enabling the provisioning priority mechanism are not saved in the generated MAC-local file, but the previous settings still take effect on the device. The static changes will never be saved to the <MAC>-local.cfg file.
>
> The provisioning priority mechanism is enabled by the parameter "static.auto_provision.custom.protect".

- MAC-local CFG File Configuration
- Clearing MAC-local CFG File

MAC-local CFG File Configuration

The following table lists the parameters you can use to generate the MAC-local CFG file.

Parameter	static.auto_provision.custom.protect	<y0000000000xx>.cfg
Description	It enables or disables the device to keep user's personalized settings after auto provisioning. **Note**: The provisioning priority mechanism (phone user interface/web user interface > In-band provisioning > central provisioning > factory defaults) takes effect only if the value of this parameter is set to 1 (Enabled).	
Permitted Values	**0**-Disabled **1**-Enabled, the <MAC>-local.cfg file is generated and personalized non-static settings configured via the web user interface or phone user interface will be kept after auto provisioning.	
Default	0	

Clearing MAC-local CFG File

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

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

  > 📝 **Note:** The **Reset local settings** option appears only if you set "static.auto_provision.custom.protect = 1".

Configuration File Customization

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

- Customizing a Configuration File
- Configuration File Attributes

Customizing a Configuration File

Procedure

1. Copy and rename a configuration template file. For example, SfB.cfg.

2. Rearrange the parameters in the SfB.cfg, and set the valid values for them.

For example:

phone_setting.phone_lock.enable= 1

screensaver.wait_time= 60

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

Configuration File Attributes

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

Attributes	Description
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
Configuration Parameter=Valid Value (screensaver.wait_time =60)	Specify the parameters and values to apply specific settings to the devices. • Separate each configuration parameter and value with an equal sign • Set only one configuration parameter per line • Put the configuration parameter and value on the same line, and do not break the line

> **ⓘ** **Tip:** The line beginning with "#" is considered to be a comment.

Resource Files

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

> **ⓘ** **Tip:** If you want to specify the desired device to use the resource file, the access URL of the resource file should be specified in the MAC CFG file. During auto provisioning, the devices will request the resource files in addition to the configuration files.

• Supported Resource Files

Supported Resource Files

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

The following table lists the resource files Yealink supplies:

Template File	File Name	Description	Reference in Section
AutoDST Template	AutoDST.xml	Add or modify the time zone and DST settings.	DST Settings
Language Packs	For example, 000.GUI.English.lang 1.English_note.xml 1.English.js	Customize the language file to display on the phone/web user interface.	Language Customization
Keypad Input Method File	ime.txt	Existing input methods. It is not applicable to CP960/T58A/T56A/T55A/MP56 phones.	/

Template File	File Name	Description	Reference in Section
Dial Now Template	dialnow.xml	Allows you to customize multiple dial now rules for the phone.	Dial Now
Local Contact File	contact.xml	Allows you to add or modify multiple local contacts at a time for your phone.	Local Directory Customization

Provisioning Methods

Skype for Business devices can be configured using the following methods with your provisioning server:

- **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.

- Provisioning Methods Priority
- Manual Provisioning
- Central Provisioning
- In-Band Provisioning

Provisioning Methods Priority

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

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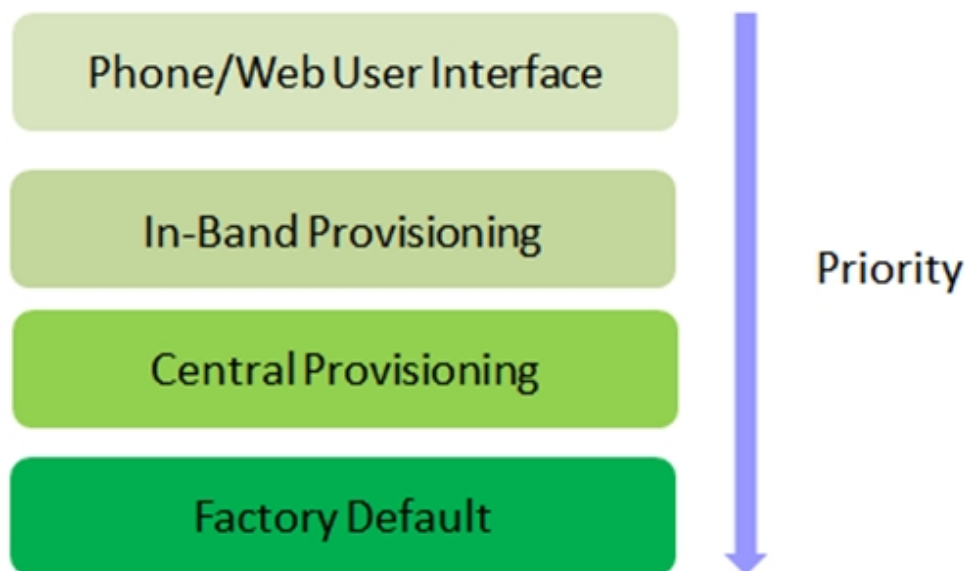
Note:

Static parameters have no priority. They take effect no matter what method (web user interface or phone user interface or configuration files) you are using for provisioning.

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

Manual Provisioning

This method enables you to perform configuration changes on a per-device basis.

- Web User Interface Access
- Phone User Interface

Web User Interface Access

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

- Accessing the Web User Interface
- Web Server Type Configuration
- Importing CFG Configuration Files to Device
- Exporting CFG Configuration Files from Device

Accessing the Web User Interface

Procedure

1. Navigate to **Menu** > **Status** > **General** > **IPv4**.
2. Enter the device IP address in the address bar of a web browser on your PC.

   For example, for IPv4: http://192.168.0.10 or 192.168.0.10; for IPv6: http://[2005:1:1:1:215:65ff:fe64:6e0a] or [2005:1:1:1:215:65ff:fe64:6e0a]
3. Enter the user name and password.
4. Click **Confirm**.

Web Server Type Configuration

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

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

Parameter	static.wui.http_enable[1]	<y0000000000xx>.cfg
Description	It enables or disables the user to access the web user interface of the device using the HTTP protocol.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Network** > **Advanced** > **Web Server** > **HTTP**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **Webserver Type** > **HTTP Status**	

Parameter	**static.network.port.http**[1]	**<y0000000000xx>.cfg**
Description	It configures the HTTP port for the user to access the web user interface of the device using the HTTP protocol.	
Permitted Values	Integer from 1 to 65535	
Default	80	
Web UI	**Network** > **Advanced** > **Web Server** > **HTTP Port (1~65535)**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **Webserver Type** > **HTTP Port**	
Parameter	**static.wui.https_enable**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the user to access the web user interface of the device using the HTTPS protocol.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Network** > **Advanced** > **Web Server** > **HTTPS**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **Webserver Type** > **HTTPS Status**	
Parameter	**static.network.port.https**[1]	**<y0000000000xx>.cfg**
Description	It configures the HTTPS port for the user to access the web user interface of the device using the HTTPS protocol.	
Permitted Values	Integer from 1 to 65535	
Default	443	
Web UI	**Network** > **Advanced** > **Web Server** > **HTTPS Port (1~65535)**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **Webserver Type** > **HTTPS Port**	

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

Importing CFG Configuration Files to Device
You can import the configuration files from local to the devices via the web user interface. The configuration files contain the changes for device features, and these changes will take effect immediately after the configuration files are imported.

Procedure

1. From the web user interface, navigate to **Settings** > **Configuration**.
2. In the **Import CFG Configuration File** block, click **Browse** to select a CFG configuration file from your local system.
3. Click **Import**.

Exporting CFG Configuration Files from Device

You can export the device's configuration file to local and make changes to the device's current feature settings. You can apply these changes to any device by importing the configuration files via the web user interface.

About this task

You can export six types of CFG configuration files to the local system:

- **<MAC>-local.cfg**: It contains the changes associated with non-static parameters made via the phone user interface and web user interface. It can be exported only if "static.auto_provision.custom.protect" is set to 1 (Enabled).
- <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>-all.cfg**: It contains all changes made via the phone user interface, web user interface and using configuration files.
- **<MAC>-static.cfg**: It contains all changes associated with the static settings (for example, network settings).
- **<MAC>-non-static.cfg**: It contains all changes associated with the non-static parameters made via the phone user interface, web user interface and using configuration files.
- **<MAC>-config.cfg**: It contains the changes associated with the non-static parameters made using configuration files. It can be exported only if "static.auto_provision.custom.protect" is set to 1 (Enabled).

Procedure

1. From the web user interface, navigate to **Settings** > **Configuration**.
2. In the **Export CFG Configuration File** block, click **Export** to open the file download window, and then save the file to your local system.

Phone 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).

You can configure the devices via the phone user interface on a per-device basis.

Central Provisioning

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

The following figure shows how the device interoperates with provisioning server when you use the centralized provisioning method:
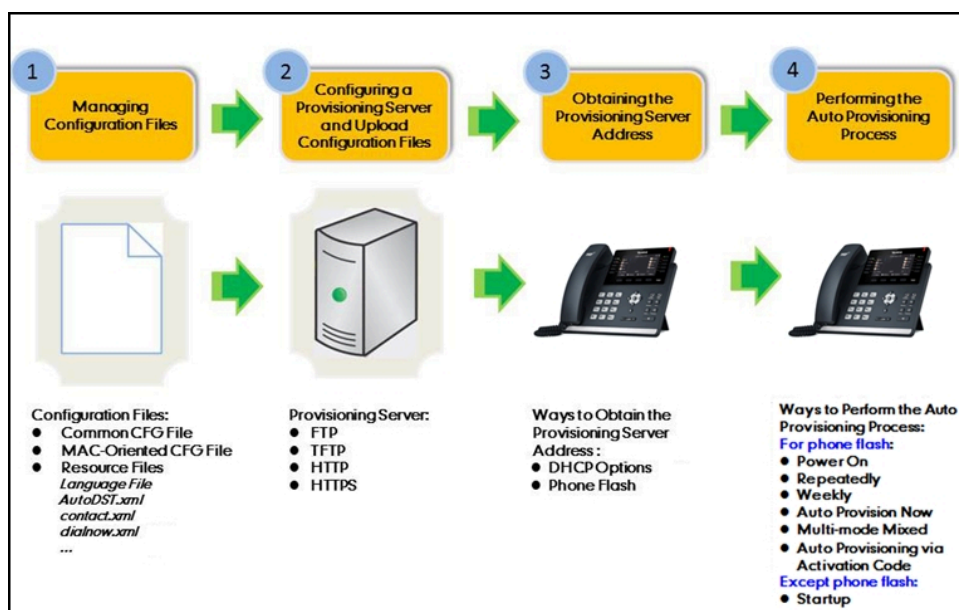
Using the configuration files to provision the devices and to modify features and configurations is called the central provisioning method. You can use a text-based editing application to edit configuration files, and then store configuration files to a provisioning server. Skype for Business devices can be centrally provisioned from a provisioning server. For more information on the provisioning server, refer to Setting Up a Provisioning Server .

Skype for Business devices can obtain the provisioning server address during startup. Then devices 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*.

- Auto Provisioning Settings Configuration
- User-Triggered Provisioning Settings Configuration

Auto Provisioning Settings Configuration

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

Parameter	static.network.attempt_expired_time[1]	<y0000000000xx>.cfg
Description	It configures the timeout interval (in seconds) to transfer a file for HTTP/HTTPS connection.	
Permitted Values	Integer from 1 to 20	
Default	10	
Parameter	static.auto_provision.power_on	<y0000000000xx>.cfg
Description	It configures the device whether to perform the auto provisioning when powered on.	
Permitted Values	**0**-Off **1**-On, the device will perform the auto provisioning when powered on.	
Default	1	
Web UI	**Settings** > **Auto Provision** > **Power On**	
Parameter	static.auto_provision.repeat.enable	<y0000000000xx>.cfg

Description	It triggers the repeatedly feature to on or off.	
Permitted Values	**0**-Off **1**-On	
Default	0	
Web UI	**Settings** > **Auto Provision** > **Repeatedly**	
Parameter	**static.auto_provision.repeat.minutes**	**<y0000000000xx>.cfg**
Description	It configures the interval (in minutes) for the device to perform the auto provisioning repeatedly. **Note**: It works only if "static.auto_provision.repeat.enable" is set to 1 (On).	
Permitted Values	Integer from 1 to 43200	
Default	1440	
Web UI	**Settings** > **Auto Provision** > **Interval(Minutes)**	
Parameter	**static.auto_provision.weekly.enable**	**<y0000000000xx>.cfg**
Description	It triggers the device to perform the auto provisioning weekly.	
Permitted Values	**0**-Off **1**-On, the device will perform an auto provisioning process weekly.	
Default	0	
Web UI	**Settings** > **Auto Provision** > **Weekly**	
Parameter	**static.auto_provision.weekly.dayofweek**	**<y0000000000xx>.cfg**
Description	It configures the days of the week for the device to perform the auto provisioning weekly. **Example**: static.auto_provision.weekly.dayofweek = 01 It means the device will perform an auto provisioning process every Sunday and Monday. **Note**: It works only if "static.auto_provision.weekly.enable" is set to 1 (On).	
Permitted Values	0,1,2,3,4,5,6 or a combination of these digits **0**-Sunday **1**-Monday **2**-Tuesday **3**-Wednesday **4**-Thursday **5**-Friday **6**-Saturday	
Default	0123456	
Web UI	**Settings** > **Auto Provision** > **Day of Week**	

Parameter	static.auto_provision.weekly.begin_time static.auto_provision.weekly.end_time	<y0000000000xx>.cfg
Description	It configures the start/end time of the day for the device to perform auto provisioning weekly. **Note**: It works only if "static.auto_provision.weekly.enable" is set to 1 (On).	
Permitted Values	Time from 00:00 to 23:59	
Default	00:00	
Web UI	**Settings** > **Auto Provision** > **Time**	

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

User-Triggered Provisioning Settings Configuration

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

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

Permitted Values	String within 64 characters	
Default	Blank	
Parameter	**static.autoprovision.X.password**[1][2]	**<y0000000000xx>.cfg**
Description	It the password for authentication during auto provisioning which is triggered by the activation code.	
Permitted Values	String within 32 characters	
Default	Blank	
Parameter	**static.autoprovision.X.com_aes**[1][2]	**<y0000000000xx>.cfg**
Description	It configures the plaintext AES key for decrypting the Common CFG file. If it is configured, it has a higher priority than the value configured by the parameter "static.auto_provision.aes_key_16.com".	
Permitted Values	String within 16 characters	
Default	Blank	
Parameter	**static.autoprovision.X.mac_aes**[1][2]	**<y0000000000xx>.cfg**
Description	It configures the plaintext AES key for decrypting the MAC-Oriented CFG file. If it is configured, it has a higher priority than the value configured in the parameter "static.auto_provision.aes_key_16.mac".	
Permitted Values	String within 32 characters	
Default	Blank	

[1]X is an activation code ID. X=1-50.

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

In-Band Provisioning

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 the central provisioning method. If you are using central provisioning, it is best practice to disable in-band provisioning device settings.

• In-band Provisioning Settings Configuration

In-band Provisioning Settings Configuration

The following table lists the parameter you can use to configure settings for in-band provisioning.

Parameter	**static.phone_setting.receive_inband.enable**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables in-band provisioning device settings sent from Skype for Business server.	

Permitted Values	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.
Default	1

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

Setting Up a Provisioning Server

You can use a provisioning server to configure your devices. A provisioning server allows for flexibility in upgrading, maintaining, and configuring the device. Configuration files are normally located on this server.

- Supported Provisioning Protocols
- Supported Provisioning Server Discovery Methods
- Configuring a Provisioning Server

Supported Provisioning Protocols

Yealink devices support several transport protocols for provisioning:

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

📝 **Note:** There are two types of FTP methods—active and passive. The devices are not compatible with active FTP.

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

Supported Provisioning Server Discovery Methods

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

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

- DHCP Provision Configuration
- Static Provision Configuration

DHCP Provision Configuration

You can select to use IPv4 or custom DHCP option according to your network environment. The IPv4 or custom DHCP option must be in accordance with the one defined in the DHCP server.

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

Parameter	static.auto_provision.dhcp_option.enable	<y0000000000xx>.cfg

Description	It triggers the DHCP Active feature to on or off.
Permitted Values	**0**-Off **1**-On, the device will obtain the provisioning server address by detecting DHCP options.
Default	1
Web UI	**Settings** > **Auto Provision** > **DHCP Active**
Parameter	**static.auto_provision.dhcp_option.list_user_option** **<y0000000000xx>.cfg**
Description	It configures the custom DHCP option for requesting provisioning server address. Multiple DHCP options are separated by commas. **Note**: It works only if "static.auto_provision.dhcp_option.enable" is set to 1 (On).
Permitted Values	Integer from 128 to 254
Default	Blank
Web UI	**Settings** > **Auto Provision** > **Custom Option**

Static Provision Configuration

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

The provisioning server address can be IP address, domain name, or URL. If a user name and password are specified as part of the provisioning server address, for example, http://user:pwd@server/dir, they will be used only if the server supports them.

> **Note:** A URL should contain forward slashes instead of 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 device will be used.

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

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

Default	Blank
Web UI	**Settings** > **Auto Provision** > **Password**

Configuring a Provisioning Server

The provisioning server can be set up on the local LAN or anywhere on the Internet. Use the following procedure as a recommendation if this is your first provisioning server setup.

Procedure

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

   ⓘ **Tip:** Typically, all devices 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.

Firmware Upgrade

There are three methods of firmware upgrade:

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

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

- Firmware for Each Device Model
- Firmware Upgrade Configuration

Firmware for Each Device Model

You can download the latest firmware online:

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

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

Device Model	Associated Firmware Name	Firmware Name(.rom)	Firmware Name(.cab)
MP56	122.x.x.x.rom	122.9.0.4.com	Yealink_ver_122.9.0.4.cab
T58A/T56A	55.x.x.x.rom	55.9.0.14.rom	Yealink_ver_55.9.0.14.cab
CP960	73.x.x.x.rom	73.8.0.35.rom	Yealink_ver_73.8.0.35.cab

Device Model	Associated Firmware Name	Firmware Name(.rom)	Firmware Name(.cab)
T48S/T46S/T42S/ T41S	66.x.x.x.rom	66.9.0.80.rom	Yealink_ver_66.9.0.80.cab

Firmware Upgrade Configuration

Before upgrading firmware, you need to know the following:

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

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

Parameter	static.firmware.url[1]	<y0000000000xx>.cfg
Description	It configures the access URL of the firmware file.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Settings** > **Upgrade** > **Upgrade Firmware**	
Parameter	static.auto_provision.reset_factory.enable[1]	<y0000000000xx>.cfg
Description	It enables or disables the device to be reset to factory after the upgrade.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Parameter	sfb.update_time[1]	<y0000000000xx>.cfg
Description	It configures the auto timer (in hours) for the device to automatically check if there is a firmware update available on Skype for Business Server. If it is set to 24, the device will check if a firmware update is available on the Skype for Business Server every 24 hours.	
Permitted Values	Integer from 1 to 48	
Default	24	
Web UI	**Features** > **General Information** > **Update Checking Time**	

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

Audio Features

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

- Send Tone
- Key Tone

- [Pre Dial Tone](#)
- [Phone Ring Tones](#)
- [Muting the Ringtone](#)
- [Private Line Tones](#)
- [Redial Tone](#)
- [Tones](#)
- [Voice Mail Tone](#)
- [Busy Tone Delay](#)
- [Early Media](#)
- [Headset Prior](#)
- [Ringer Device for Headset](#)
- [Dual Headset](#)
- [Sending Volume](#)
- [Audio Codecs](#)
- [Acoustic Clarity Technology](#)
- [DTMF](#)
- [Quality of Experience (QoE)](#)

Send Tone

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

- [Send Tone Configuration](#)

Send Tone Configuration

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

Parameter	features.send_key_tone	<y0000000000xx>.cfg
Description	It enables or disables the phone to play a key tone when a user presses a send key. **Note**: It works only if "features.key_tone" is set to 1 (Enabled).	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Features** > **Audio** > **Send Sound**	

Key Tone

Key tone allows the phone to play a key tone when a user presses any key.

- [Key Tone Configuration](#)

Key Tone Configuration

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

Parameter	features.key_tone	<y0000000000xx>.cfg
Description	It enables or disables the phone to play a key tone when a user presses any key on your phone keypad.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Features** > **Audio** > **Key Tone**	
Phone UI	**Menu** > **Setting** > **Basic** > **Sounds** > **Key Tone** > **Key Tone**	

Pre Dial Tone

Pre dial tone allows phones to play key tone in the following situations:

- Enter phone numbers without picking up the handset (applicable to MP56/T58A/T56A/T55A/T48S/T46S/T42S/T41S phones).
- Tap (**Search** icon) to enter the pre-dialing screen, and then enter phone numbers without picking up the handset (only applicable to MP56/T58A/T56A/T48S phones).

Pre dial tone is not applicable to CP960 phones.

- Pre Dial Tone Configuration

Pre Dial Tone Configuration

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

Parameter	sfb.pre_dial_tone.enable	<y0000000000xx>.cfg
Description	It enables or disables the phones to play key tone in the following situations: **For MP56/T58A/T56A/T55A/T48S/T46S/T42S/T41S Skype for Business phones:** Enter phone numbers without picking up the handset. **For MP56/T58A/T56A/T48S Skype for Business phones:** Tap (**Search** icon) to enter the pre-dialing screen, and then enter the phone numbers without picking up the handset. **Note:** It is not applicable to CP960 Skype for Business phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Features** > **Audio** > **Pre Dial Tone**	

Phone Ring Tones

Phone ring tones are the sound to indicate incoming calls. Users can select a built-in system ring tone or a custom ring tone for the phone or a registered 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:

Phone Model	Format	Total File Size	Note
MP56/CP960/T58A/T56A/T55A/T48S/T46S	.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.

- Phone Ring Tones Configuration

Phone Ring Tones Configuration

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

Parameter	phone_setting.ring_type	<y0000000000xx>.cfg
Description	It configures a ring tone for the phone.	
Permitted Values	Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring.wav).	
Default	Ring1.wav	
Web UI	**Settings** > **Preference** > **Ring Type**	
Phone UI	**Menu** > **Setting** > **Basic** > **Sounds** > **Ring Tones** > **Normal**	
Parameter	account.1.ringtone.ring_type	<MAC>.cfg
Description	It configures a ring tone for the account 1.	
Permitted Values	Common, Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring.wav).	
Default	Common	
Parameter	phone_setting.ringtone.url	<y0000000000xx>.cfg
Description	It configures the access URL of the custom ring tone file.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Settings** > **Preference** > **Upload Ringtone**	
Parameter	ringtone.delete	<y0000000000xx>.cfg

Description	It deletes all custom ring tone files.
Permitted Values	http://localhost/all
Default	Blank

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.

- Ringtone Mute Configuration

Ringtone Mute Configuration

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

Parameter	**phone_setting.soundsmin.busy_enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to mute the ringtone when account status is busy (in a call).	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Parameter	**phone_setting.soundsmin.dnd_enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to mute the ringtone when account status is Do Not Disturb.	
Permitted Values	**0**-Disabled, the phone plays a ringtone for incoming calls from the working group when account status is Do Not Disturb. **1**-Enabled, the phone does not play a ringtone for incoming calls from the working group when account status is Do Not Disturb.	
Default	1	

Private Line Tones

The Skype for Business Server allows the system administrator to give the user a second, but private telephone line in addition to their primary telephone line. Private line is often assigned to the boss who wants an unlisted telephone number which they can be reached directly. When the boss receives a private call, the private line will bypass call delegation and only the 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.

- Private Line Tones Configuration

Private Line Tones Configuration

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

Parameter	phone_setting.private_line_ring.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to set a distinct ring tone for the private line.	
Permitted Values	**0**-Disabled, the 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.	
Default	1	
Parameter	phone_setting.private_line_ring_type	<y0000000000xx>.cfg
Description	It 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).	
Default	Ring6.wav	
Web UI	**Settings** > **Preference** > **Private line ring**	
Phone UI	**Menu** > **Setting** > **Basic** > **Sound** > **Ring Tones** > **Private Line**	

Redial Tone

Redial tone allows the phone to continue to play the dial tone after inputting the preset numbers on the pre-dialing screen.

Redial tone is not applicable to CP960 Skype for Business phones.

- Redial Tone Configuration

Redial Tone Configuration

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

Parameter	features.redial_tone	<y0000000000xx>.cfg
Description	It configures the phone to continue to play the dial tone after inputting the preset numbers on the pre-dialing screen. **Example**: features.redial_tone = 125 The phone will continue to play the dial tone after inputting "125" on the pre-dialing screen. If it is left blank, the phone will not play the dial tone after inputting numbers on the pre-dialing screen. **Note:** It is not applicable to CP960 Skype for Business phones.	
Permitted Values	Integer within 6 digits	
Default	Blank	
Web UI	**Features** > **Audio** > **Redial Tone**	

Tones

When the device is in the dialing screen, it 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 device.

- Supported Tones
- Tones Configuration

Supported Tones

The default tones used on Skype for Business devices are the US tone sets. Available tone sets for the devices:

- 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

Tones Configuration

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

Parameter	voice.tone.country	<y0000000000xx>.cfg
Description	It configures the country tone for the 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	
Default	Custom	
Web UI	**Settings** > **Tones** > **Select Country**	
Parameters	**voice.tone.dial**	**<y0000000000xx>.cfg**
Permitted Values	It customizes the dial tone. tone list = element[,element] [,element]… Where **element** = [!]Freq1[+Freq2][+Freq3][+Freq4] /Duration **Freq**: the frequency of the tone (ranges from 200 to 4000 Hz). If it is set to 0 Hz, it means the tone is not played. 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. (for example, 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 (for example, !250/200,0/1000, 200+300/500,200+500+800+1500/1000). **Note**: It works only if "voice.tone.country" is set to Custom. It is not applicable to CP960 phones.	
Supported Devices		
Web UI	**Settings** > **Tones** > **Dial**	
Parameter	**voice.tone.ring**	**<y0000000000xx>.cfg**
Description	It customizes the ringback tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** It works only if "voice.tone.country" is set to Custom.	
Permitted Values	String	
Default	Blank	
Web UI	**Settings** > **Tones** > **Ring Back**	
Parameter	**voice.tone.busy**	**<y0000000000xx>.cfg**
Description	It customizes the tone when the callee is busy. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** It works only if "voice.tone.country" is set to Custom.	
Permitted Values	String	
Default	Blank	

Web UI	Settings > Tones > Busy	
Parameter	**voice.tone.congestion**	**<y0000000000xx>.cfg**
Description	It customizes the tone when the network is congested.	
	The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".	
	Note: It works only if "voice.tone.country" is set to Custom.	
Permitted Values	String	
Default	Blank	
Web UI	Settings > Tones > Congestion	
Parameter	**voice.tone.callwaiting**	**<y0000000000xx>.cfg**
Description	It 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 "voice.tone.country" is set to Custom.	
Permitted Values	String	
Default	Blank	
Web UI	Settings > Tones > Call Waiting	
Parameter	**voice.tone.dialrecall**	**<y0000000000xx>.cfg**
Description	It 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 "voice.tone.country" is set to Custom.	
Permitted Values	String	
Default	Blank	
Web UI	Settings > Tones > Dial Recall	
Parameter	**voice.tone.info**	**<y0000000000xx>.cfg**
Description	It customizes the info tone. The phone will play the info tone with the special information, for example, the number you are calling is not in service.	
	The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".	
	Note: It works only if "voice.tone.country" is set to Custom.	
Permitted Values	String	
Default	Blank	
Web UI	Settings > Tones > Info	
Parameter	**voice.tone.stutter**	**<y0000000000xx>.cfg**

Description	It 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 "voice.tone.country" is set to Custom.
Permitted Values	String
Default	Blank
Web UI	**Settings** > **Tones** > **Stutter**

Parameter	**voice.tone.autoanswer**	**<y0000000000xx>.cfg**
Description	It customizes the warning tone for the 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 "voice.tone.country" is set to Custom.	
Permitted Values	String	
Default	Blank	
Web UI	**Settings** > **Tones** > **Auto Answer**	

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.

- Voice Mail Tone Configuration

Voice Mail Tone Configuration

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

Parameter	**features.voice_mail_tone_enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to play a warning tone when it receives a new voice mail.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Features** > **General Information** > **Voice Mail Tone**	

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.

- Busy Tone Delay Configuration

Busy Tone Delay Configuration

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

Parameter	features.busy_tone_delay	<y0000000000xx>.cfg
Description	It configures the duration (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.	
Permitted Values	**0**-0s, the phone will not play a busy tone. **3**-3s, a busy tone plays for 3 seconds on the phone. **5**-5s	
Default	0	
Web UI	**Features** > **General Information** > **Busy Tone Delay (Seconds)**	

Early Media

Early media refers to media (for example, 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.

You can also configure 180 ring workaround which defines whether to deal with the 180 message received after the 183 message. When the caller receives a 183 message, it suppresses any local ringback tone and begins to play the media received. 180 ring workaround allows the phones to resume and play the local ringback tone upon a subsequent 180 message received.

- Early Media Configuration

Early Media Configuration

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

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

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.

- Headset Prior Configuration

Headset Prior Configuration

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

Parameter	features.headset_prior	<y0000000000xx>.cfg
Description	It enables or disables to preferentially use the headset mode for all incoming calls and outgoing calls.	
Permitted Values	**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.	
Default	0	
Web UI	**Features** > **General Information** > **Headset Prior**	

Ringer Device for Headset

Skype for Business phones support either or both speaker and headset ringer devices. You can configure which ringer device to be used when receiving an incoming call. For example, if the ringer device is set to Headset, ring tone will be played through your headset.

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.

Ringer Device for Headset feature is not applicable to CP960 Skype for Business phones.

- Ringer Device for Headset Configuration

Ringer Device for Headset Configuration

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

Parameter	features.ringer_device.is_use_headset	<y0000000000xx>.cfg
Description	It configures the ringer device for the phone. **Note:** Itis not applicable to CP960 Skype for Business phones.	
Permitted Values	**0**-Use Speaker **1**-Use Headset **2**-Use Headset & Speaker	
Default	0	

Web UI	**Features** > **Audio** > **Ringer Device for Headset**

Dual Headset

Redial tone allows the phone to continue to play the dial tone after inputting the preset numbers on the pre-dialing screen.

Redial tone is not applicable to CP960 Skype for Business phones.

- Dual Headset Configuration

Dual Headset Configuration

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

Parameter	features.headset_training	<y0000000000xx>.cfg
Description	It enables or disables dual headset feature. **Note:** It is not applicable to CP960 Skype for Business phones.	
Permitted Values	**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.	
Default	0	
Web UI	**Features** > **General Information** > **Dual-Headset**	

Sending Volume

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

- Sending Volume Configuration

Sending Volume Configuration

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

Parameter	voice.handfree_send[1]	<y0000000000xx>.cfg
Description	It 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.	
Permitted Values	Integer from -50 to 50	
Default	0	
Parameter	voice.handset_send[1]	<y0000000000xx>.cfg

Description	It 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. It is not applicable to CP960 Skype for Business phones.
Permitted Values	Integer from -50 to 50
Default	0

Parameter	**voice.headset_send**[1]	**<y0000000000xx>.cfg**
Description	It 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. It is not applicable to CP960 Skype for Business phones.	
Permitted Values	Integer from -50 to 50	
Default	0	

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

Audio Codecs

CODEC is an abbreviation of COmpress-DECompress, capable of coding or decoding a digital data stream or signal by implementing an algorithm. The object of the algorithm is to represent the high-fidelity audio signal with a minimum number of bits while retaining the quality. This can effectively reduce the frame size and the bandwidth required for audio transmission.

The audio codec that the phone uses to establish a call should be supported by the SIP server. When placing a call, the phone will offer the enabled audio codec list to the server and then use the audio codec negotiated with the called party according to the priority.

- Supported Audio Codecs
- Audio Codec Configuration

Supported Audio Codecs

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 Ksps	20ms
PCMA	G.711 a-law	RFC 3551	64 Kbps	8 Ksps	20ms
PCMU	G.711 u-law	RFC 3551	64 Kbps	8 Ksps	20ms
G729	G.729	RFC 3551	8 Kbps	8 Ksps	20ms
G726-16	G.726	RFC 3551	16 Kbps	8 Ksps	20ms
G726-24	G.726	RFC 3551	24 Kbps	8 Ksps	20ms
G726-32	G.726	RFC 3551	32 Kbps	8 Ksps	20ms
G726-40	G.726	RFC 3551	40 Kbps	8 Ksps	20ms

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
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
SILK_NB	SILK_NB	draft-vos-silk-01	12kbps	8 Ksps	20ms
SILK_WB	SILK_WB	draft-vos-silk-01	20kbp	16 Ksps	20ms

Audio Codec Configuration

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

Parameter	static.account.1.codec.Y.enable[1]	<MAC>.cfg
Description	It enables or disables the specified codec for the account.	
Permitted Values	**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; When Y=5, the default value is 1; When Y=6, the default value is 1; When Y=7-13, the default value is 0;	
Web UI	**Account** > **Codec**	
Parameter	static.account.1.codec.Y.payload_type[1]	<MAC>.cfg
Description	It configures the codec for the account.	
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;
Web UI	**Account** > **Codec**
Parameter	**static.account.1.codec.Y.priority**[1] **<MAC>.cfg**
Description	It configures the priority of the enabled codec for the account.
Permitted Values	Integer from 0 to 12
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=7-13, the default value is 0;
Web UI	**Account** > **Codec**
Parameter	**static.account.1.codec.Y.rtpmap**[1] **<MAC>.cfg**
Description	It configures the rtpmap of the audio codec for the account.
Permitted Values	Integer from 0 to 127

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;

[1]Y ranges from 1 to 13.

Acoustic Clarity Technology

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

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

Acoustic Echo Cancellation (AEC)

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

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

- AEC Configuration

AEC Configuration

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

Parameter	voice.echo_cancellation	<y0000000000xx>.cfg

Description	It enables or disables AEC (Acoustic Echo Canceller) feature on the phone.
Permitted Values	**0**-Disabled **1**-Enabled
Default	1
Web UI	**Settings** > **Voice** > **Echo Cancellation** > **ECHO**

Background Noise Suppression (BNS)

Background noise suppression (BNS) is designed primarily for hands-free operation and reduces background noise to enhance communication in noisy environments.

Automatic Gain Control (AGC)

Automatic Gain Control (AGC) is applicable to the hands-free operation and is used to keep audio output at nearly a constant level by adjusting the gain of signals in 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) can avoid unnecessary coding or transmission of silence packets in VoIP applications, saving on computation and network bandwidth.

- VAD Configuration

VAD Configuration

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

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

Comfort Noise Generation (CNG)

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

- CNG Configuration

CNG Configuration

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

Parameter	voice.cng	<y0000000000xx>.cfg
Description	It enables or disables CNG (Comfortable Noise Generation) feature on the phone.	

Permitted Values	**0**-Disabled **1**-Enabled
Default	1
Web UI	**Settings** > **Voice** > **Echo Cancellation** > **CNG**

Jitter Buffer

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

- [Jitter Buffer Configuration](#)

Jitter Buffer Configuration

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

Parameter	voice.jib.adaptive	<y0000000000xx>.cfg
Description	It configures the type of jitter buffer.	
Permitted Values	**0**-Fixed **1**-Adaptive	
Default	1	
Web UI	**Settings** > **Voice** > **JITTER BUFFER** > **Type**	
Parameter	**voice.jib.min**	**<y0000000000xx>.cfg**
Description	It configures the minimum delay time (in milliseconds) of jitter buffer. **Note:** It works only if "voice.jib.adaptive" is set to 1 (Adaptive).	
Permitted Values	Integer from 0 to 400	
Default	60	
Web UI	**Settings** > **Voice** > **JITTER BUFFER** > **Min Delay**	
Parameter	**voice.jib.max**	**<y0000000000xx>.cfg**
Description	It configures the maximum delay time (in milliseconds) of jitter buffer. **Note:** It works only if "voice.jib.adaptive" is set to 1 (Adaptive).	
Permitted Values	Integer from 0 to 400	
Default	240	
Web UI	**Settings** > **Voice** > **JITTER BUFFER** > **Max Delay**	
Parameter	**voice.jib.normal**	**<y0000000000xx>.cfg**
Description	It configures the normal delay time (in milliseconds) of jitter buffer. **Note:** It works only if "voice.jib.adaptive" is set to 0 (Fixed).	
Permitted Values	Integer from 0 to 400	
Default	120	

Web UI	Settings > Voice > JITTER BUFFER > Normal

Noise Suppression

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

It is only applicable to MP56/T58A/T56A/T55A phones.

• Noise Suppression Configuration

Noise Suppression Configuration

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

Parameter	voice.tns.enable	<y0000000000xx>.cfg
Description	It enables or disables the Noise Suppression feature on the phones. **Note:** It is only applicable to MP56/T58A/T56A/T55A phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	Features > Voice > Noise Proof > Noise Suppression	

Smart Noise Block

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

It is only applicable to MP56/T58A/T56A/T55A phones.

• Smart Noise Block Configuration

Smart Noise Block Configuration

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

Parameter	voice.ans_nb.enable	<y0000000000xx>.cfg
Description	It enables or disables the Smart Noise Block feature on the IP phones. **Note**: It works only if "voice.tns.enable" is set to 1 (Enabled). It is only applicable to MP56/T58A/T56A/T55A phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	Features > Voice > Noise Proof > Smart Noise Block	

DTMF

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.

- DTMF Keypad
- Transmitting DTMF Digit
- Suppress DTMF Display
- Transfer via DTMF
- Play Local DTMF Tone

DTMF Keypad

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

DTMF Keypad Frequencies:

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

Transmitting DTMF Digit

Three methods of transmitting DTMF digits on SIP calls:

- **RFC 2833** -- DTMF digits are transmitted by RTP Events compliant with RFC 2833. You can configure the payload type and sending times of the end RTP Event packet. The RTP Event packet contains 4 bytes. The 4 bytes are distributed over several fields denoted as Event, End bit, R-bit, Volume, and Duration. If the End bit is set to 1, the packet contains the end of the DTMF event. You can configure the sending times of the end RTP Event packet.
- **INBAND** -- DTMF digits are transmitted in the voice band. It uses the same codec as your voice and is audible to conversation partners.
- **SIP INFO** -- DTMF digits are transmitted by SIP INFO messages. DTMF digits are transmitted by the SIP INFO messages when the voice stream is established after a successful SIP 200 OK-ACK message sequence. The SIP INFO message can transmit DTMF digits in three ways: DTMF, DTMF-Relay, and Telephone-Event.

- Transmitting DTMF Digit Configuration

Transmitting DTMF Digit Configuration

The following table lists the parameters you can use to configure the transmitting DTMF digit.

Parameter	features.dtmf.repetition	<y0000000000xx>.cfg
Description	It configures the repetition times for the phone to send the end RTP Event packet during an active call.	
Permitted Values	1, 2 or 3	
Default	3	

Web UI	**Features** > **Features** > **DTMF Repetition**

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. Suppress DTMF display delay defines whether to display the DTMF digits for a short period of time before displaying as "*".

• Suppress DTMF Display Configuration

Suppress DTMF Display Configuration

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

Parameter	features.dtmf.hide	<y0000000000xx>.cfg
Description	It enables or disables the phone to suppress the display of DTMF digits during an active call.	
Permitted Values	**0**-Disabled **1**-Enabled, the DTMF digits are displayed as asterisks.	
Default	0	
Web UI	**Features** > **General Information** > **Suppress DTMF Display**	
Parameter	features.dtmf.hide_delay	<y0000000000xx>.cfg
Description	It enables or disables the phone to display the DTMF digits for a short period before displaying asterisks during an active call. **Note:** It works only if "features.dtmf.hide" is set to 1 (Enabled).	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Features** > **General Information** > **Suppress DTMF Display Delay**	

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.

• Transfer via DTMF Configuration

Transfer via DTMF Configuration

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

Parameter	features.dtmf.replace_tran	<y0000000000xx>.cfg
Description	It enables or disables the phone to send DTMF sequences for transfer function when pressing a Transfer/Bind Transfer soft key or TRANSFER key.	

Permitted Values	**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 the **Transfer**/**Bind Transfer** soft key or TRANSFER key during a call.
Default	0
Web UI	**Features** > **General Information** > **DTMF Replace Tran**
Parameter	**features.dtmf.transfer** **<y0000000000xx>.cfg**
Description	It configures the DTMF digits to be transmitted to perform call transfer.
	Valid values are: 0-9, *, # and A-D.
	Note: It works only if "features.dtmf.replace_tran" is set to 1 (Enabled).
Permitted Values	String within 32 characters
Default	Blank
Web UI	**Features** > **General Information** > **Tran Send DTMF**

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 during a call.

- Play Local DTMF Tone Configuration

Play Local DTMF Tone Configuration

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

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

Quality of Experience (QoE)

Quality of Experience (QoE) metrics track the quality of audio calls made in your organization, including how many network packets lost, the amount of "jitter" (differences in packet delay) and the background noise.

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).

- QoE Configuration

QoE Configuration

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

Parameter	phone_setting.qoe.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to send Quality of Experience (QoE) metrics to a server.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Parameter	features.report_qoe.when_bad_quality.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to send Quality of Experience (QoE) metrics to a server for monitoring and diagnostics when voice quality is poor. **Note:** It works only if "phone_setting.qoe.enable" is set to 1 (Enabled).	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	

Device Customization

You can make the Skype for Business device more personalized by customizing various settings.

- Language
- Contrast
- Screen Saver
- Backlight
- Time and Date
- Power Saving
- Power LED Indicator
- Bluetooth
- Showing Full Name
- Always Online
- Key As Send
- Common Area Phone
- BToE
- Microsoft Exchange Integration
- Updating Status Automatically
- Calendar
- Boss-Admin

- EXP40/EXP50 Expansion Module

Language

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

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

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

Phone User Interface		Web User Interface	
Language	**Language Pack**	**Language**	**Language Pack**
English	000.GUI.English.lang	English	1.English.js
Chinese Simplified	001.GUI.Chinese_S.lang	Chinese Simplified	2.Chinese_S.js
Chinese Traditional	002.GUI.Chinese_T.lang	Chinese Traditional	3.Chinese_T.js
French	003.GUI.French.lang	French	4.French.js
German	004.GUI.German.lang	German	5.German.js
Italian	005.GUI.Italian.lang	Italian	6.Italian.js
Polish	006.GUI.Polish.lang	Polish	7.Polish.js
Portuguese	007.GUI.Portuguese.lang	Portuguese	8.Portuguese.js
Spanish	008.GUI.Spanish.lang	Spanish	9.Spanish.js
Turkish	009.GUI.Turkish.lang	Turkish	10.Turkish.js
Korean	010.GUI.Korean.lang (not applicable to MP56/CP960/T58A/T56A/T55A Skype for Business phones)	Korean	11.Korean.js (not applicable to MP56/CP960/T58A/T56A/T55A Skype for Business phones)
Russian	011.GUI.Russian.lang(not applicable to MP56/CP960/T58A/T56A/T55A Skype for Business phones)	Russian	12.Russian.js (not applicable to MP56/CP960/T58A/T56A/T55A Skype for Business phones)

- Language Display Configuration
- Language Customization
- Example: Setting a Custom Language for Device Display

Language Display Configuration

The default language displayed on the phone user interface depends on the language chosen by the user during startup. If your web browser displays a language not supported by the device, the web user interface will display English by default. You can specify the languages for the phone user interface and web user interface respectively.

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

Parameter	lang.gui	<y0000000000xx>.cfg
Description	It configures the language to display on the device.	
Permitted Values	**For T48S/T46S/T42S/T41S:** English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Korean, Russian or the custom language name. **For MP56/CP960/T58A/T56A/T55A:** English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, or the custom language name.	
Default	English	
Phone UI	**Menu** > **Setting** > **Basic** > **Language**	
Parameter	**lang.wui**	**<y0000000000xx>.cfg**
Description	It configures the language to display on the web user interface.	
Permitted Values	**For T48S/T46S/T42S/T41S:** English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Korean, Russian or the custom language name. **For MP56/CP960/T58A/T56A/T55A:** English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, or the custom language name.	
Default	English	
Web UI	**Settings** > **Preference** > **Language**	

Language Customization

You can customize the language file to display on the phone user interface or web user interface.

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

> **Note:** The newly added language must be supported by the font library on the device. If the characters in the custom language file are not supported by the device, the device will display "?" instead.

- Language for Device Display Customization
- Language for Web Display Customization

Language for Device Display Customization

Available languages depend on the language packs currently loaded to the device. You can also add new languages (not included in the available language list) available for device display by loading language packs to the device.

- Customizing a Language Pack for Device Display
- Custom Language for Device Display Configuration

Customizing a Language Pack for Device Display

When you add 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 phones, X starts from 012, for MP56/CP960/T58A/T56A/T55A phones, X starts from 010). If the language name is the same as the existing one, the existing language pack will be overridden by the newly uploaded one. We recommend that the filename of the new language pack should not be the same as the existing one.

Note: To modify language file, do not rename the language pack.

1. Open the desired language template file (for example, 000.GUI.English.lang).
2. Modify the characters within the double quotation marks on the right of the equal sign.

   Do not modify the item on the left of the equal sign.

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

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

Custom Language for Device Display Configuration

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

Parameter	gui_lang.url	<y0000000000xx>.cfg

Description	It configures the access URL of the custom language pack for the phone user interface. You can also download multiple language packs to the device simultaneously.	
Permitted Values	URL within 511 characters	
Default	Blank	
Parameter	**gui_lang.delete**	**<y0000000000xx>.cfg**
Description	It deletes the specified or all custom language packs of the phone user interface.	
Permitted Values	http://localhost/all or X.GUI.name.lang	
Default	Blank	

Language for Web Display Customization

You can modify the language file or add a new language for web display.

- Customizing a Language Pack for Web Display
- Custom Language for Web Display Configuration

Customizing a Language Pack for Web Display

When you add a new language pack for the web user interface, the language pack must be formatted as "X.name.js" (For T48S/T46S/T42S/T41S Skype for Business phones, Y starts from 13. For MP56/CP960/T58A/T56A/T55A Skype for Business phones, X starts from 11, "name" is replaced with the language name). If the language name is the same as the existing one, the newly uploaded language file will override the existing one. We recommend that the filename of the new language pack should not be the same as the existing one.
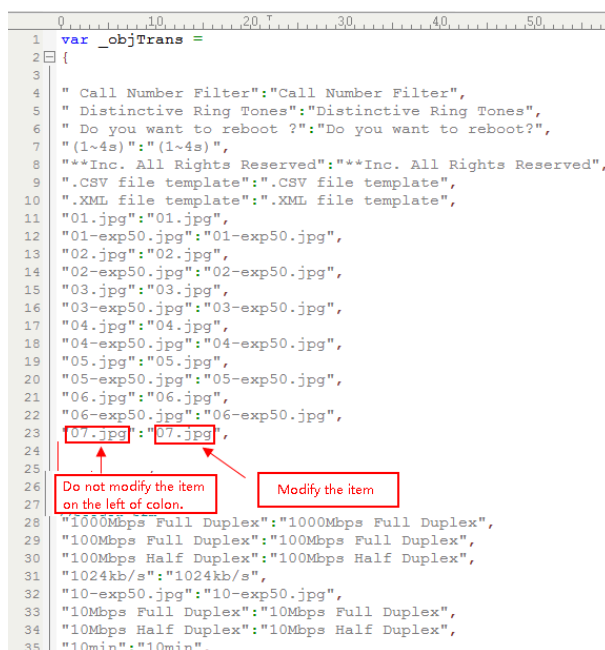
> **Note:** To modify the language file, do not rename the language pack.

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

2. Modify the characters within the double quotation marks on the right of the colon. Do not modify the translation item on the left of the colon.

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

```
 1   var _objTrans =
 2   {
 3
 4   " Call Number Filter":"Call Number Filter",
 5   " Distinctive Ring Tones":"Distinctive Ring Tones",
 6   " Do you want to reboot ?":"Do you want to reboot?",
 7   "(1~4s)":"(1~4s)",
 8   "**Inc. All Rights Reserved":"**Inc. All Rights Reserved",
 9   ".CSV file template":".CSV file template",
10   ".XML file template":".XML file template",
11   "01.jpg":"01.jpg",
12   "01-exp50.jpg":"01-exp50.jpg",
13   "02.jpg":"02.jpg",
14   "02-exp50.jpg":"02-exp50.jpg",
15   "03.jpg":"03.jpg",
16   "03-exp50.jpg":"03-exp50.jpg",
17   "04.jpg":"04.jpg",
18   "04-exp50.jpg":"04-exp50.jpg",
19   "05.jpg":"05.jpg",
20   "05-exp50.jpg":"05-exp50.jpg",
21   "06.jpg":"06.jpg",
22   "06-exp50.jpg":"06-exp50.jpg",
23   "07.jpg":"07.jpg",
24
25
26       Do not modify the item              Modify the item
27       on the left of colon.
28   "1000Mbps Full Duplex":"1000Mbps Full Duplex",
29   "100Mbps Full Duplex":"100Mbps Full Duplex",
30   "100Mbps Half Duplex":"100Mbps Half Duplex",
31   "1024kb/s":"1024kb/s",
32   "10-exp50.jpg":"10-exp50.jpg",
33   "10Mbps Full Duplex":"10Mbps Full Duplex",
34   "10Mbps Half Duplex":"10Mbps Half Duplex",
35   "10min":"10min",
```

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

Custom Language for Web Display Configuration

If you want to add a new language (for example, Wuilan) to devices, prepare the language file named as "13.Wuilan.js" for downloading. After the update, you will find a new language selection "Wuilan" at the top-right corner of the web user interface, and new note information is displayed in the icon when this new language is selected.

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

Parameter	wui_lang.url	<y0000000000xx>.cfg
Description	It configures the access URL of the custom language pack for the web user interface.	
Permitted Values	URL within 511 characters	
Default	Blank	
Parameter	wui_lang.delete	<y0000000000xx>.cfg
Description	It deletes the specified or all custom web language packs and note language packs of the web user interface.	
Permitted Values	http://localhost/all or http://localhost/*Y.name.js*	
Default	Blank	

Example: Setting a Custom Language for Device Display

The following example shows the configuration for uploading custom language files "015.GUI.English_15.lang" and "016.GUI.English_16.lang", and then specify "015.GUI.English_15.lang" to

display on the phone user interface. These language files are customized and placed on the provisioning server "192.168.10.25".

Example

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

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

lang.gui=English_15

After provisioning, the language on the phone user interface will change to the custom language you defined in *"015.GUI.English_15.lang"*. You can also find a new language selection*"English_15"* and *"English_16"* on the phone user interface: **Menu** > **Setting** > **Basic** > **Language**.

Contrast

Contrast determines the readability of the texts displayed on the LCD screen. Adjusting the contrast to a comfortable level can optimize the screen viewing experience.

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 MP56/CP960/T58A/T56A/T55A/T42S/T41S phones.

- Contrast Configuration

Contrast Configuration

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

Parameter	phone_setting.contrast	<y0000000000xx>.cfg
Description	It configures the contrast of the LCD screen. For T48S/T46S phones, it configures the LCD's contrast of the connected EXP40 only. **Note:** We recommend that you set the contrast of the LCD screen to 6 as a more comfortable level. It is not applicable to MP56/CP960/T58A/T56A/T55A/T42S/T41S phones.	
Permitted Values	Integer from 1 to 10	
Default	6	
Phone UI	**Menu** > **Setting** > **Basic** > **Display** > **Contrast**	

Screen Saver

The screen saver will automatically start when the device is idle for the preset waiting time. You can stop the screen saver and return to the idle screen at any time by pressing a key on the device or tapping the touch screen. When your device is idle again for a preset waiting time, the screen saver starts again.

The screen saver is only applicable to MP56/CP960/T58A/T56A/T55A/T48S/T46S phones.

By default, the device screen displays a built-in picture when the screen saver starts. You can set the device to display the other built-in screensaver background. You can also set the device to display the custom screensaver background.

- Screensaver Configuration

Screensaver Configuration

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

Parameter	screensaver.wait_time	<y0000000000xx>.cfg
Description	It configures the time (in seconds) that the device waits in the idle state before the screen saver starts.	
Permitted Values	**15**-15s **30**-30s **60**-1min **120**-2min **300**-5min **600**-10min **900**-15min **1800**-30min **3600**-1h (not applicable to MP56/CP960/T58A/T56A/T55A) **7200**-2h (not applicable to MP56/CP960/T58A/T56A/T55A) **10800**-3h (not applicable to MP56/CP960/T58A/T56A/T55A) **21600**-6h (not applicable to MP56/CP960/T58A/T56A/T55A)	
Default	600	
Web UI	**Settings** > **Preference** > **Screensaver Wait Time**	
Phone UI	**Menu** > **Setting** > **Basic** > **Display** > **Screensaver** > **Wait Time**	
Parameter	screensaver.type	<y0000000000xx>.cfg
Description	It configures the type of screen saver to display.	
Permitted Values	**For T48S/T46S Skype for Business phones:** **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 device will display all images alternately. The time interval is configured by the parameter "screensaver.picture_change_interval". **For MP56/T58A/T56A/T55A phones:** **0**-Clock **1**-Colors **2**-Photo Frame **3**-Photo Table	
Default	Blank	
Web UI	**Settings** > **Preference** > **Screensaver Type**	

Phone UI	**Menu** > **Setting** > **Basic** > **Display** > **Screensaver** > **Screensaver Type**	
Parameter	**screensaver.upload_url**	**<y0000000000xx>.cfg**
Description	It configures the access URL of the custom screensaver background.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Settings** > **Preference** > **Upload Screensaver**	
Parameter	**screensaver.delete**	**<y0000000000xx>.cfg**
Description	It deletes the specified or all custom screensaver background. **Example**: Delete all custom screensaver background: screensaver.delete = http://localhost/all Delete a custom screensaver background (for example, Screencapture.jpg): screensaver.delete = http://localhost/Screencapture.jpg	
Permitted Values	String	
Default	Blank	
Web UI	**Settings** > **Preference** > **Screensaver Type (Custom)** > **Del**	
Parameter	**screensaver.display_clock.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to display the clock and icons when the screen saver starts. **Note**: It is only applicable to T48S/T46S Skype for Business phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Settings** > **Preference** > **Display Clock**	
Phone UI	**Menu** > **Setting** > **Basic** > **Display** > **Screensaver** > **Display Clock**	
Parameter	**screensaver.picture_change_interval**	**<y0000000000xx>.cfg**
Description	It configures the interval (in seconds) for the phone to change the pictures when the screen saver starts. **Note**: It works only if "screensaver.type" is set to 1 (Custom) and "screensaver.upload_url" should be configured in advance. It is only applicable to T48S/T46S Skype for Business phones.	
Permitted Values	Integer from 5 to 1200	
Default	60	

Parameter	screensaver.clock_move_interval	<y0000000000xx>.cfg
Description	It configures the interval (in seconds) for the phone to move the clock and icons when the screen saver starts. **Note**: It works only if "screensaver.display_clock.enable" is set to 1 (Enabled). It is only applicable to T48S/T46S Skype for Business phones.	
Permitted Values	Integer from 5 to 1200	
Default	60	

Backlight

You can change the brightness of LCD backlight when the device is active (in use). The brightness of LCD backlight automatically changes when the device is idle for a specified time. Backlight time is applicable to MP56/CP960/T58A/T56A/T55A/T48S/T46S phones and connected EXP40/EXP50.

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

Backlight Active Level: The brightness level of the LCD backlight when the device is active. It is applicable to MP56/CP960/T58A/T56A/T55A/T48S/T46S phones and the connected EXP40.

Inactive Level is used to adjust the backlight intensity of the LCD screen when the phone is inactive. It is only applicable to T48S/T46S phones and the connected EXP40.

Backlight Time: The delay time to change the brightness of the LCD backlight when the device is inactive. For T48S/T46S phones, backlight time is configurable on Skype for Business Server only.

- Backlight Brightness Configuration

Backlight Brightness Configuration

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

Parameter	phone_setting.active_backlight_level	<y0000000000xx>.cfg
Description	It configures the intensity of the LCD backlight when the device is active. For T48S/T46S phones, it configures the LCD's intensity of the phone and the connected EXP40. For MP56/CP960/T58A/T56A/T55A phones, it configures the intensity of the touch screen.	
Permitted Values	Integer from 1 to 10	
Default	8	
Web UI	**Settings** > **Preference** > **Backlight Active Level**	
Phone UI	**Menu** > **Setting** > **Basic** > **Display** > **Backlight** > **Backlight Active Level**	
Parameter	phone_setting.inactive_backlight_level	<y0000000000xx>.cfg
Description	It configures the intensity of the LCD screen when the device is inactive. **Note:** It is only applicable to T48S and T46S Skype for Business phones and the connected EXP40.	

Permitted Values	**0**-Off
	1-Low
Default	0
Phone UI	**Menu** > **Setting** > **Basic** > **Display** > **Backlight** > **Inactive Level**

Time and Date

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

- Time Zone
- NTP Settings
- DST Settings
- Time and Date Manual Configuration
- Time and Date Format Configuration

Time Zone

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

Time Zone	Time Zone Name	Time Zone	Time Zone Name
-11	Samoa	+4:30	Afghanistan(Kabul)
-10	United States-Hawaii-Aleutian, United States-Alaska-Aleutian	+5	Kazakhstan(Aqtobe), Kyrgyzstan(Bishkek), Pakistan(Islamabad), Russia(Chelyabinsk)
-9:30	French Polynesia	+5:30	India(Calcutta)
-9	United States-Alaska Time	+5:45	Nepal(Katmandu)
-8	Canada(Vancouver,Whitehorse), Mexico(Tijuana,Mexicali), United States-Pacific Time	+6	Kazakhstan(Astana, Almaty), Russia(Novosibirsk,Omsk)
-7	Canada(Edmonton,Calgary), Mexico(Mazatlan,Chihuahua), United States-MST no DST, United States-Mountain Time	+6:30	Myanmar(Naypyitaw)
-6	Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Belize, Canada-Manitoba(Winnipeg), Chile(Easter Islands), Mexico(Mexico City,Acapulco), United States-Central Time	+7	Russia(Krasnoyarsk), Thailand(Bangkok)

Time Zone	Time Zone Name	Time Zone	Time Zone Name
-5	Peru, Bahamas(Nassau), Canada(Montreal,Ottawa,Quebec), Cuba(Havana), United States-Eastern Time	+8	Australia(Perth), China(Beijing), Russia(Irkutsk, Ulan-Ude), Singapore(Singapore)
-4:30	Venezuela(Caracas)	+8:45	Eucla
-4	Canada(Halifax,Saint John), Chile(Santiago), Paraguay(Asuncion), United Kingdom-Bermuda(Bermuda), United Kingdom(Falkland Islands), Trinidad&Tobago	+9	Japan(Tokyo), Korea(Seoul), Russia(Yakutsk,Chita)
-3:30	Canada-New Foundland(St.Johns)	+9:30	Australia(Adelaide), Australia(Darwin)
-3	Argentina(Buenos Aires), Brazil(DST), Brazil(no DST), Denmark-Greenland(Nuuk)	+10	Australia(Brisbane), Australia(Hobart), Australia(Sydney,Melbourne,Canberra), Russia(Vladivostok)
-2:30	Newfoundland and Labrador	+10:30	Australia(Lord Howe Islands)
-2	Brazil(no DST)	+11	New Caledonia(Noumea), Russia(Srednekolymsk Time)
-1	Portugal(Azores)	+11:30	Norfolk Island
0	Denmark-Faroe Islands(Torshavn), GMT, Greenland, Ireland(Dublin), Morocco, Portugal(Lisboa,Porto,Funchal), Spain-Canary Islands(Las Palmas), United Kingdom(London)	+12	New Zealand(Wellington,Auckland), Russia(Kamchatka Time)
+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),	+12:45	New Zealand(Chatham Islands)
+2	Estonia(Tallinn), Finland(Helsinki), Gaza Strip(Gaza), Greece(Athens), Harare,Pretoria,Israel(Tel Aviv), Jordan(Amman), Latvia(Riga), Lebanon(Beirut), Moldova(Kishinev), Romania(Bucharest), Russia(Kaliningrad), Syria(Damascus), Turkey(Ankara), Ukraine(Kyiv, Odessa)	+13	Tonga(Nukualofa)

Time Zone	Time Zone Name	Time Zone	Time Zone Name
+3	East Africa Time, Iraq(Baghdad), Russia(Moscow)	+13:30	Chatham Islands
+3:30	Iran(Teheran)	+14	Kiribati
+4	Armenia(Yerevan), Azerbaijan(Baku), Georgia(Tbilisi), Kazakhstan(Aktau), Russia(Samara)		

NTP Settings

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

- NTP Configuration

NTP Configuration

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

Parameter	local_time.manual_ntp_srv_prior	<MAC>.cfg
Description	It configures the priority for the device to use the NTP server address offered by the DHCP server.	
Permitted Values	**0**- High (use the NTP server address offered by the DHCP server preferentially) **1**- Low (use the NTP server address configured manually preferentially)	
Default	0	
Web UI	**Settings** > **Time & Date** > **NTP By DHCP Priority**	

Parameter	local_time.dhcp_time	<MAC>.cfg
Description	It enables or disables the device to update time with the offset time offered by the DHCP server. **Note**: It is only available to offset time from Greenwich Mean Time GMT 0.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Settings** > **Time & Date** > **DHCP Time**	
Phone UI	**Menu** > **Setting** > **Basic** > **Date & Time** > **DHCP Time**	

Parameter	local_time.ntp_server1	<MAC>.cfg
Description	It configures the IP address or the domain name of the NTP server 1. The device will obtain the current time and date from the NTP server 1.	
Permitted Values	IP address or domain name	

Default	cn.pool.ntp.org
Web UI	**Settings** > **Time & Date** > **Primary Server**
Phone UI	**Menu** > **Setting** > **Basic** > **Date & Time** > **General** > **SNTP Settings** > **NTP Server1**

Parameter	**local_time.ntp_server2**	**<MAC>.cfg**
Description	It configures the IP address or the domain name of the NTP server 2. If the NTP server 1 is not configured (configured by the parameter "local_time.ntp_server1") or cannot be accessed, the device will request the time and date from the NTP server 2.	
Permitted Values	IP address or domain name	
Default	pool.ntp.org	
Web UI	**Settings** > **Time&Date** > **Secondary Server**	
Phone UI	**Menu** > **Setting** > **Basic** > **Date & Time** > **General** > **SNTP Settings** > **NTP Server2**	

Parameter	**local_time.interval**	**<MAC>.cfg**
Description	It configures the interval (in seconds) at which the device updates time and date from the NTP server.	
Permitted Values	Integer from 15 to 86400	
Default	1000	
Web UI	**Settings** > **Time & Date** > **Update Interval (15~86400s)**	

Parameter	**local_time.time_zone**	**<MAC>.cfg**
Description	It configures the interval (in seconds) at which the device updates time and date from the NTP server.	
Permitted Values	-11 to +14 For available time zones, refer to Time Zone .	
Default	+8	
Web UI	**Settings** > **Time & Date** > **Time Zone**	

Parameter	**local_time.time_zone_name**	**<MAC>.cfg**
Description	It configures the time zone name. **Note**: It works only if "local_time.summer_time" is set to 2 (Automatic) and the parameter "local_time.time_zone" should be configured in advance.	
Permitted Values	String within 32 characters The available time zone names depend on the time zone configured by "local_time.time_zone". For available time zone names, refer to Time Zone .	
Default	China(Beijing)	

Web UI	Settings > Time & Date > Location	
Phone UI	Menu > Setting > Basic > Date & Time > General > SNTP Settings > Location	
Parameter	phone_setting.hide_ntp_server.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to hide NTP Server configurations on the LCD screen. **Note**: It is not applicable to T42S/T41S Skype for Business phones.	
Permitted Values	**0**-Disabled **1**-Enabled, the NTP Server configurations on the LCD screen will be hidden, so that you cannot configure NTP Server address manually.	
Default	0	

DST Settings

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

The time zone and corresponding DST pre-configurations exist in the AutoDST file. If the DST is set to Automatic, the device 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 the time zone and DST settings for your area each year.

- Auto DST File Customization
- DST Configuration

Auto DST File Customization

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.

- Auto DST File Attributes
- Customizing Auto DST File

Auto DST File Attributes

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

Attributes	Type	Values	Description
szTime	required	[+/-][X]:[Y], X=0~14, Y=0~59	Time Zone
szZone	required	String (if the content is more than one city, it is the best to keep their daylight saving time the same)	Time Zone name
iType	optional	0/1 **0**: DST by Date **1**: DST by Week	DST time type (This item is needed if you want to configure DST.)

Attributes	Type	Values	Description
szStart	optional	**Month/Day/Hour** (for **iType=0**) Month: 1~12 Day: 1~31 Hour: 0 (midnight)~23 **Month/Week of Month/Day of Week/ Hour of Day** (for **iType=1**) Month: 1~12 Week of Month: 1~5 (the last week) Day of Week: 1~7 Hour of Day: 0 (midnight)~23	Starting time of the DST
szEnd	optional	Same as szStart	Ending time of the DST
szOffset	optional	Integer from -300 to 300	The offset time (in minutes) of DST

Customizing Auto DST File

Procedure

1. Open the AutoDST file.
2. To add a new time zone, add <DST szTime="" szZone="" iType="" szStart="" szEnd="" szOffset=""/> between <DSTData> and </DSTData>.

3. Specify the DST attribute values within double quotes.

For example:

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

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

Modify the DST settings for the existing time zone "+5 Pakistan(Islamabad)" and add DST settings for the existing time zone "+5:30 India(Calcutta)".

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

Related information

Time Zone

DST Configuration

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

Parameter	local_time.summer_time	<MAC>.cfg
Description	It configures Daylight Saving Time (DST) feature.	
Permitted Values	**0**-Disabled **1**-Enabled **2**-Automatic	
Default	2	
Web UI	**Settings** > **Time & Date** > **Daylight Saving Time**	
Phone UI	**Menu** > **Setting** > **Basic** > **Date & Time** > **General** > **SNTP Settings** > **Daylight Saving**	
Parameter	local_time.dst_time_type	<MAC>.cfg

Description	It configures the Daylight Saving Time (DST) type.
	Note: It works only if "local_time.summer_time" is set to 1 (Enabled).
Permitted Values	**0**-DST by Date
	1-DST by Week
Default	0
Web UI	**Settings** > **Time & Date** > **Fixed Type**

Parameter	**local_time.start_time**	**<MAC>.cfg**
Description	It configures the start time of the Daylight Saving Time (DST).	
	Note: It works only if the "local_time.summer_time" is set to 1 (Enabled).	
Permitted Values	Month/Day/Hour-DST by Date, use the following mapping:	
	Month: 1=January, 2=February,…, 12=December	
	Day: 1=the first day in a month,…, 31= the last day in a month	
	Hour: 0=0am, 1=1am,…, 23=11pm	
	Month/Week of Month/Day of Week/Hour of Day- DST by Week, use the following mapping:	
	Month: 1=January, 2=February,…, 12=December	
	Week of Month: 1=the first week in a month,…, 5=the last week in a month	
	Day of Week: 1=Monday, 2=Tuesday,…, 7=Sunday	
	Hour of Day: 0=0am, 1=1am,…, 23=11pm	
Default	1/1/0	
Web UI	**Settings** > **Time & Date** > **Start Date**	

Parameter	**local_time.end_time**	**<MAC>.cfg**
Description	It configures the end time of the Daylight Saving Time (DST).	
	Note: It works only if "local_time.summer_time" is set to 1 (Enabled).	
Permitted Values	Month/Day/Hour-DST by Date, use the following mapping:	
	Month: 1=January, 2=February,…, 12=December	
	Day: 1=the first day in a month,…, 31= the last day in a month	
	Hour: 0=0am, 1=1am,…, 23=11pm	
	Month/Week of Month/Day of Week/Hour of Day- DST by Week, use the following mapping:	
	Month: 1=January, 2=February,…, 12=December	
	Week of Month: 1=the first week in a month,…, 5=the last week in a month	
	Day of Week: 1=Monday, 2=Tuesday,…, 7=Sunday	
	Hour of Day: 0=0am, 1=1am,…, 23=11pm	
Default	12/31/23	

Web UI	Settings > Time & Date > End Date	
Parameter	**local_time.offset_time**	**<MAC>.cfg**
Description	It configures the offset time (in minutes) of Daylight Saving Time (DST). **Note**: It works only if "local_time.summer_time" is set to 1 (Enabled).	
Permitted Values	Integer from -300 to 300	
Default	Blank	
Web UI	Settings > Time&Date > Offset(minutes)	
Parameter	**auto_dst.url**	**<MAC>.cfg**
Description	It configures the access URL of the DST file (AutoDST.xml). **Note**: It works only if "local_time.summer_time" is set to 2 (Automatic).	
Permitted Values	URL within 511 characters	
Default	Blank	

Time and Date Manual Configuration

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

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

Parameters	local_time.manual_time_enable	<MAC>.cfg
Description	It enables or disables the device to obtain time and date from manual settings.	
Permitted Values	**0**-Disabled (obtain time and date from NTP server) **1**-Enabled (obtain time and date from manual settings)	
Default	0	
Web UI	Settings > Time & Date > Manual Time	

Time and Date Format Configuration

You can customize the time and date with a variety of time and date formats, including options to

date format with the day, month, or year, and time format in 12 hours or 24 hours, or you can also custom the date

format as required.

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

Parameters	local_time.time_format	<MAC>.cfg
Description	It configures the time format.	

Permitted Values	**0**-Hour 12, the time will be displayed in 12-hour format with AM or PM specified.
	1-Hour 24, the time will be displayed in 24-hour format (for example, 2:00 PM displays as 14:00).
Default	1
Web UI	**Settings** > **Time & Date** > **Time Format**
Phone UI	**Menu** > **Setting** > **Basic** > **Date & Time** > **Time&Date Format** > **Time Format**

Parameter	local_time.date_format		<MAC>.cfg
Description	It configures the date format.		
Permitted Values	**0**-WWW MMM DD		
	1-DD-MMM-YY		
	2-YYYY-MM-DD		
	3-DD/MM/YYYY		
	4-MM/DD/YY		
	5-DD MMM YYYY		
	6-WWW DD MMM		
	Use the following mapping:		
	"WWW" represents the abbreviation of the week;		
	"DD" represents a two-digit day;		
	"MMM" represents the first three letters of the month;		
	"YYYY" represents a four-digit year, and "YY" represents a two-digit year.		
Default	0		
Web UI	**Settings** > **Time & Date** > **Date Format**		
Phone UI	**Menu** > **Setting** > **Basic** > **Date & Time** > **Time&Date Format** > **Date Format**		

Power Saving

The power-saving feature turns off LCD backlight and LCD display to conserve energy. The device enters power-saving mode after the device has been idle for a certain period of time. And the device will exit power-saving mode if a device event occurs - for example, the device receives an incoming call, or you press a key on the device or tap the touch screen.

📝 **Note:** If the Screen Saver is enabled on your device, power-saving mode will still occur. For example, if a screen saver is configured to start after the device 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 after the screen saver has been on for 10 minutes.

- Power Saving Configuration

Power Saving Configuration

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

- **Office Hour**: specify the start time and end time of the office hour. You can change the office hours to avoid affecting your work.
- **Idle TimeOut (minutes)**: specify the period of time before the phone enters the power-saving mode.

You can specify the following three types of idle timeout:

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

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

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

Parameter	features.power_saving.intelligent_mode	<y0000000000xx>.cfg
Description	It enables or disables the power saving intelligent mode.	
Permitted Values	**0**-Disabled, the phone stays in power-saving mode even if the office hour arrives the next day. **1**-Enabled, the phone will automatically identify the office hour and exit power-saving mode once the office hour arrives the next day.	
Default	1	
Param eter	features.power_saving.enable	<y0000000000xx>.cfg
Description	It enables or disables the power saving feature.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Settings** > **Power Saving** > **Power Saving**	
Parameters	features.power_saving.office_hour.idle_timeout	<y0000000000xx>.cfg
Description	It configures the time (in minutes) that the phone waits in the idle state before the phone enters power-saving mode during 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 hours) during office hours.	
Permitted Values	Integer from 1 to 960	
Default	960	
Web UI	**Settings** > **Power Saving** > **Office Hour Idle TimeOut**	

Parameters	**features.power_saving.off_hour.idle_timeout**	**<y0000000000xx>.cfg**
Description	It configures the time (in minutes) that the phone waits in the idle state before IP phone enters power-saving mode during the non-office hours. **Example**: features.power_saving.off_hour.idle_timeout = 5 The IP phone will enter power-saving mode when it has been inactivated for 5 minutes during the non-office hours.	
Permitted Values	Integer from 1 to 10	
Default	10	
Web UI	**Settings** > **Power Saving** > **Off Hour Idle TimeOut**	
Parameters	**features.power_saving.user_input_ext.idle_timeout**	**<y0000000000xx>.cfg**
Description	It configures the minimum time (in minutes) that the phone waits in the idle state - after being inactive - before the phone enters power-saving mode. **Example**: features.power_saving.user_input_ext.idle_timeout = 5	
Permitted Values	Integer from 1 to 30	
Default	10	
Web UI	**Settings** > **Power Saving** > **User Input Extension Idle TimeOut**	
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**	**<y0000000000xx>.cfg**
Description	It configures the start time and end time of the day's office hour. Start time and end time are separated by a comma. **Example**: features.power_saving.office_hour.monday = 7,19	
Permitted Values	Integer from 0 to 23, Integer from 0 to 23	
Default	7,19 - for Monday, Tuesday, Wednesday, Thursday, Friday. 7,7 - for Saturday, Sunday.	
Web UI	**Settings** > **Power Saving** > **Monday/Tuesday/Wednesday/Thursday/Friday/Saturday/ Sunday**	

Power LED Indicator

Power LED indicator indicates power status and phone status.

It is not applicable to CP960.

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

- The phone receives an incoming call
- The phone is busy
- The phone receives a voice mail
- The phone misses a call

- Power LED Indicator Configuration

Power LED Indicator Configuration

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

Parameter	**phone_setting.common_power_led_enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the power LED indicator to be turned on.	
Permitted Values	**0**-Disabled (power LED indicator is off) **1**-Enabled (power LED indicator glows red)	
Default	0	
Web UI	**Features** > **Power LED** > **Common Power Light On**	
Parameter	**phone_setting.ring_power_led_flash_enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the power LED indicator to flash when the phone receives an incoming call.	
Permitted Values	**0**-Disabled (power LED indicator does not flash) **1**-Enabled (power LED indicator fast flashes (300ms) red)	
Default	1	
Web UI	**Features** > **Power LED** > **Ringing Power Light Flash**	
Parameter	**phone_setting.mail_power_led_flash_enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the power LED indicator to flash when the phone receives a voice mail.	
Permitted Values	**0**-Disabled (power LED indicator does not flash) **1**-Enabled (power LED indicator slowly flashes (1000ms) red)	
Default	1	
Web UI	**Features** > **Power LED** > **Voice Mail Power Light Flash**	
Parameter	**phone_setting.mute_power_led_flash_enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the power LED indicator to be turned on.	
Permitted Values	**0**-Disabled (power LED indicator does not flash) **1**-Enabled (power LED indicator fast flashes (300ms) red)	
Default	0	

Web UI	**Features** > **Power LED** > **Mute Power Light On**	
Parameter	**phone_setting.hold_and_held_power_led_flash_enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the power LED indicator to flash when a call is placed on hold or is held.	
Permitted Values	**0**-Disabled (power LED indicator does not flash) **1**-Enabled (power LED indicator fast flashes (500ms) red)	
Default	0	
Web UI	**Features** > **Power LED** > **Hold/Held Power Light On**	
Parameter	**phone_setting.talk_and_dial_power_led_enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the power LED indicator to be turned on when the phone is busy.	
Permitted Values	**0**-Disabled (power LED indicator is off) **1**-Enabled (power LED indicator glows red)	
Default	0	
Web UI	**Features** > **Power LED** > **Talk/Dial Power Light On**	
Parameter	**phone_setting.boss_admin.talk_power_light.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the power LED indicator to be turned on when using the Boss-Admin feature.	
Permitted Values	**0**-Disabled (power LED indicator is off) **1**-Enabled (power LED indicator glows red)	
Default	0	
Web UI	**Features** > **Power LED** > **Boss/Admin Power Light On**	

Bluetooth

Bluetooth enables low-bandwidth wireless connections within a range of 10 meters (32 feet). The range with the best performance is 1 to 2 meters (3 to 6 feet). It is not applicable to T42S/T41S Skype for Business phones.

For T48S/T46S Skype for Business phones, you can pair and connect the Bluetooth headset. For CP960/ T58A/T56A/T55A/MP56 Skype for Business phones, you can use your Skype for Business phone as a Bluetooth speaker for your mobile phone and manage calls for your mobile phone.

📝 **Note:** To use this feature on T48S/T46S/T56A/T55A Skype for Business phones, make sure the Bluetooth USB dongle is properly connected to the USB port on the back of the phone.

• Bluetooth Configuration

Bluetooth Configuration

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

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

Parameter	**static.bluetooth.function.enable**[1]	**<y0000000000xx>.cfg**

Description	It enables or disables the Bluetooth feature.
	Note: It is only applicable to T58A/T56A/T55A/MP56 Skype for Business phones.
Permitted Values	**0**-Disabled
	1-Enabled
Default	1
Parameter	**features.bluetooth.fast_entrance** **<y0000000000xx>.cfg**
Description	It enables or disables the phone to display a Bluetooth entry on the menu screen.
	Note: It is only applicable to CP960/T58A/T56A/T55A/MP56 Skype for Business phones. For T58A/T56A/T55A/MP56 Skype for Business phone, it works only if "static.bluetooth.function.enable" is set to 1(Enabled).
Permitted Values	**0**-Disabled
	1-Enabled
Default	0
Parameter	**features.bluetooth_enable** **<y0000000000xx>.cfg**
Description	It triggers the Bluetooth mode to on or off.
	Note: It is only applicable to CP960/T58A/T56A/T55A/MP56 Skype for Business phones. For T58A/T56A/T55A/MP56 Skype for Business phone, it works only if "static.bluetooth.function.enable" is set to 1(Enabled).
Permitted Values	**0**-Off
	1-On
Default	0
Phone UI	**Menu** > **Setting** > **Basic** > **Bluetooth** > **Bluetooth**
Web UI	**Features** > **Bluetooth** > **Bluetooth Active**
Parameter	**features.bluetooth_adapter_name** **<y0000000000xx>.cfg**
Description	It configures the Bluetooth device name.
	Note: It works only if "features.bluetooth_enable" is set to 1 (On).
Permitted Values	String within 64 characters
Default	For T58A: Yealink-T58
	For T56A: Yealink-T56A
	For T55A: Yealink-T55A
	For CP960: Yealink-CP960
	For MP56: Yealink-MP56
	For T48S: Yealink T48S
	For T46S: Yealink T46S

Phone UI	Menu > Setting > Basic > Bluetooth > Bluetooth (On) > Edit My Device Information > Device Name	
Parameter	**bluetooth.a2dp_sink**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to display the Media audio option for the connected Bluetooth device. **Note:** It is only applicable to CP960 Skype for Business phones. It works only if "features.bluetooth_enable" is set to 1 (On).	
Permitted Values	**0**-Disabled **1**-Enabled, the phone displays the Media audio option, but this option is disabled. **2**-Enabled, the phone displays the Media audio option, and this option is enabled.	
Default	1	

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

Showing Full Name

Showing full name allows the phone to extend the display length of the contact's name. 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.

- Showing Full Name Configuration

Showing Full Name Configuration

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

Parameter	**phone_setting.name_full_display.mode**[1]	**<y0000000000xx>.cfg**
Description	It configures the display mode of the contact's name. **Note**: It is only applicable to T48S/T46S Skype for Business phones.	
Permitted Values	**0**-Off, the phone does not extend the display length of the contact's name. **1**-On, the phone extends the display length of the contact's name. More characters can be displayed in a line. **2**-On (only applicable to T48S), the phone extends the display length of the contacts' names. More characters (about 15 characters) can be displayed in a line. If the contact's name includes a dot, the dot breaks a line into two lines.	
Default	6	
Phone UI	Menu > Setting > Basic > Display > Show full name	

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

Always Online

Always on line feature allows 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.

- Always Online Configuration

Always Online Configuration

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

Parameter	sfb.always_online.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to maintain online status when it is idle until you manually change it.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Account** > **Basic** > **Always Online**	
Phone UI	**Menu** > **Setting** > **Basic** > **Always Online** (not applicable to CP960/T55A)	

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 the key tone is enabled.

- Key As Send Configuration

Key As Send Configuration

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

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

Description	It enables or disables the phone not to send any pound key when pressing double #.
Permitted Values	**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.
Default	0
Web UI	**Features** > **General Information** > **Send Pound Key**

Common Area Phone

Common area phones(CAPs) are those Skype for Business phones that are not associated with an individual user. Instead of being deployed in someone's office, CAPs are typically deployed in building lobbies, cafeterias, employee lounges, conference rooms, and other places 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.

- Common Area Phone Configuration

Common Area Phone Configuration

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

Parameter	features.set_as_cap.enable[1]	<y0000000000xx>.cfg
Description	It enables or disables the phone to work as a common area phone.	
Permitted Values	**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).	
Default	0	
Web UI	**Features** > **General Information** > **Set as CAP**	
Phone UI	**Menu** > **Setting** > **Advanced(default password: admin)** > **Common Area Phone** > **Set as CAP**	
Parameter	features.cap_presence.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to display presence status of the Skype for Business contacts.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Parameter	features.voice_mail.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to use the voice mail feature.	

Permitted Values	0-Disabled	
	1-Enabled	
Default	For MP56/T58A/T56A/T55A/T48S/T46S/T42S/T41S Skype for Business phones: 1	
	For CP960 Skype for Business phones: 0	
	For common area phone: 0	
Parameter	**features.redial.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to dial out a last dialed number.	
	Note: It is not applicable to CP960/T55A Skype for Business phones.	
Permitted Values	0-Disabled	
	1-Enabled	
Default	For individual phone: 1	
	For common area phone: 0	
Parameter	**features.exchange_connect.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to use Microsoft Exchange integration feature.	
Permitted Values	0-Disabled	
	1-Enabled	
Default	For individual phone: 1	
	For common area phone: 0	
Parameter	**features.sfb_directory.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to display the Skype for Business contacts.	
Permitted Values	0-Disabled	
	1-Enabled	
Default	For individual phone: 1	
	For common area phone: 0	
Parameter	**phone_setting.search_contacts.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables you to search for contacts on the phone.	
Permitted Values	0-Disabled	
	1-Enabled	
Default	For individual phone: 1	
	For common area phone: 0	
Parameter	**features.call_history.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to display call history.	

Permitted Values	**0**-Disabled	
	1-Enabled	
Default	For individual phone: 1	
	For common area phone: 0	
Parameter	**features.paging.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to configure the multicast paging feature.	
	Note: It is not applicable to CP960 Skype for Business phones.	
Permitted Values	**0**-Disabled, the phone hides multicast paging configurations.	
	1-Enabled, the phone displays multicast paging configurations.	
Default	For individual phone: 1	
	For common area phone: 0	
	For T55A Skype for Business phones: 0	

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

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.

- [BToE Configuration](#)

BToE Configuration

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

Parameter	**sip.btoe.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the BToE (Better Together over Ethernet) feature.	
Permitted Values	**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.	
Default	For MP56/T58A/T56A/T55A/T48S/T46S/T42S/T41S Skype for Business phones: 1	
	For CP960 Skype for Business phones: 0	
Web UI	**Settings** > **BToE** > **BToE**	
Phone UI	**Menu** > **Setting** > **Features** > **BToE** > **BToE**	
Parameter	**features.sign_in_via_btoe.enable**	**<y0000000000xx>.cfg**

Description	It enables or disables the BToE (Better Together over Ethernet) feature.
	Note: It works only if "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, so that you can sign into the phone via PC.
Permitted Values	**0**-Disabled
	1-Enabled
Default	1
Parameter	**sip.btoe.pairing_mode** **<y0000000000xx>.cfg**
Description	It configures the BToE pairing mode.
	Note: It works only if "sip.btoe.enable" is set to 1 (Enabled).
Permitted Values	**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 with the Skype for Business client.
Default	0
Web UI	**Settings** > **BToE** > **BToE paring Mode**
Phone UI	**Menu** > **Setting** > **Features** > **BToE** > **BToE Pairing Mode**

Microsoft Exchange Integration

The Skype for Business phone can obtain Microsoft Exchange Server address automatically. This feature enables visual voicemail setting up, 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.

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 features. You may need to enter Exchange authentication information manually when your login password expires, or is changed by system administrator.

- Microsoft Exchange Server Configuration
- Exchange Authentication Configuration

Microsoft Exchange Server Configuration

The following table lists the parameters you can use to configure the Microsoft Exchange Server.

Parameter	phone_setting.ews_autodiscover.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to obtain the Microsoft Exchange Server address automatically via Auto discover request.	

Permitted Values	**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.
Default	1
Web UI	**Features** > **General Information** > **Auto Discover**

Parameter	**phone_setting.ews_url**	**<y0000000000xx>.cfg**
Description	It specifies the Microsoft Exchange Server address manually. **Note:** It works only if "phone_setting.ews_autodiscover.enable" is set to 0 (Disabled).	
Permitted Values	String	
Default	Blank	
Web UI	**Features** > **General Information** > **Exchange Server Url**	

Exchange Authentication Configuration

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

Parameter	**static.account.sfb.1.ews.auth_address**[1]	**<MAC>.cfg**
Description	It configures the Exchange address for accessing the Microsoft Exchange Server.	
Permitted Values	String within 128 characters	
Default	Blank	
Phone UI	**On the authentication dialog box** > **Sign in address**	
Parameter	**static.account.sfb.1.ews.auth_user**[1]	**<MAC>.cfg**
Description	It configures the user name for accessing the Microsoft Exchange Server.	
Permitted Values	String within 128 characters	
Default	Blank	
Phone UI	**On the authentication dialog box** > **User**	
Parameter	**static.account.sfb.1.password**[1]	**<MAC>.cfg**
Description	It configures the password for accessing the Microsoft Exchange Server.	
Permitted Values	String within 128 characters	
Default	Blank	
Phone UI	**On the authentication dialog box** > **Password**	
Parameter	**phone_setting.ews_auth_popup.enable**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to pop up a reminder about if the Exchange authentication failed. **Note:** It is not applicable to CP960 Skype for Business phones.	

Permitted Values	**0**-Disabled
	1-Enabled
Default	1

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

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 turns to **Inactive** when your phone has been idle for the designated time. Phone status will change from **Inactive** to **Away** after another designated time.

- Updating Status Automatically Configuration

Updating Status Automatically Configuration

The following table lists the parameters you can use to configure updating status automatically.

Parameter	**sfb.presence.inactive_time**[1]	**<y0000000000xx>.cfg**
Description	It configures the inactive time (in minutes) of the phone, after which the phone will change its status to Inactive automatically.	
	Note: It works only if "sfb.always_online.enable" is set to 0 (Disabled).	
Permitted Values	Integer from 5 to 360	
Default	5	
Web UI	**Features** > **General Information** > **SFB Inactive Time**	
Parameter	**sfb.presence.away_time**[1]	**<y0000000000xx>.cfg**
Description	It configures the inactive time (in minutes) of the phone, after which the phone will change its status from Inactive to Away automatically.	
	Note: It works only if "sfb.always_online.enable" is set to 0 (Disabled).	
Permitted Values	Integer from 5 to 360	
Default	5	
Web UI	**Features** > **General Information** > **SFB Away Time**	

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

Calendar

Yealink Skype for Business phones integrate with the Microsoft Exchange calendar feature. If your phone is configured to connect to the Microsoft Exchange Server, and the Microsoft® Outlook® is installed at your site, you can view Skype conference, appointment, meeting and event, or join the Skype conference from your phone.

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.

- Calendar Configuration

Related information
User Sign-in
Web Sign-in
Sign in via PC

Calendar Configuration

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

Parameter	sfb.calendar.enable	<y0000000000xx>.cfg
Description	It enables or disables the calendar feature.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	For individual phone: 1 For common area phone: 0	
Parameter	phone_setting.calendar_reminder	<y0000000000xx>.cfg
Description	It enables or disables the meeting reminder.	
Permitted Values	**0**-Disabled, the phone will not display reminders for any meeting. **1**-Enabled, the phone will display reminders for all meetings.	
Default	For MP56/T58A/T56A/T55A/T48S/T46S/T42S/T41S: 1 For CP960: 0	
Web UI	**Settings** > **Calendar** > **Reminder** (only for MP56/CP960/T58A/T56A/T55A)	
Phone UI	**Menu** > **Setting** > **Basic** > **Calendar Settings** > **Reminder**	
Parameter	phone_setting.calendar_reminder.interval	<y0000000000xx>.cfg
Description	It 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 "phone_setting.calendar_reminder" is set to 1 (Enabled).	
Permitted Values	Integer from 1 to 15	
Default	5	
Web UI	**Settings** > **Calendar** > **Reminder Interval(mins)** (only for MP56/CP960/T58A/T56A/T55A)	
Phone UI	**Menu** > **Setting** > **Basic** > **Calendar Settings** > **Reminder Interval**	
Parameter	phone_setting.calendar.update_time[1]	<y0000000000xx>.cfg
Description	It 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 update the calendars.	

Permitted Values	Integer from 0 to 1000
Default	For CP960: 180
	For MP56/T58A/T56A/T55A/T48S/T46S/T42S/T41S: 300

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

Boss-Admin

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.

- Boss-Line Ringtone Configuration
- Delegates-call Ringtone Configuration

Boss-Line Ringtone Configuration

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.

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

Parameter	phone_setting.boss_line_ring.enable	<y0000000000xx>.cfg
Description	It enables or disables the delegate to set a distinct ringtone for assigned bosses' lines. **Note**: It is not applicable to CP960 Skype for Business phones.	
Permitted Values	**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 the delegate receives incoming calls from assigned bosses or assigned bosses to receive incoming calls, the delegate's phone will play the distinct ringtone.	
Default	1	

Delegates-call Ringtone Configuration

As a boss, you can set a distinct ringtone for incoming calls from your assigned delegates' lines. Delegate-line ringtone is not applicable to CP960 Skype for Business phones.

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

Parameter	phone_setting.delegates_call_ring.enable	<y0000000000xx>.cfg
Description	It enables or disables the boss to set a distinct ringtone for incoming calls from the assigned delegates' lines. **Note**: It is not applicable to CP960 Skype for Business phones.	

Permitted Values	**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.
Default	1

EXP40/EXP50 Expansion Module

The Yealink EXP40/EXP50 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.

EXP40/EXP50 can display local contacts or Skype for Business contacts, but you can only use EXP40/EXP50 to monitor Skype for Business contacts for status changes. For example, you can assign a Skype for Business contact to the EXP40/EXP50 to monitor the status of his line (busy or idle). The EXP key LED indicator glows red when his line is busy.

- EXP key LED Indicators
- EXP key LED Indicator Configuration

EXP key LED Indicators

The EXP key LED indicators on the EXP40/EXP50 expansion module:

LED Status	Description
Green	The Skype for Business contact is available.
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.
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.

EXP key LED Indicator Configuration

The following table lists the parameters you can use to configure the EXP key LED indicator.

Parameter	phone_setting.exp40_led.enable	<y0000000000xx>.cfg
Description	It enables or disables the EXP key LED indicator on the expansion module to monitor the status of the Skype for Business contacts. **Note:** It is only applicable to MP56/T58A/T56A/T48S/T46S Skype for Business phones.	
Permitted Values	**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.	
Default	1	
Web UI	**Features** > **(Power)LED** > **Exp Led Light On**	

Call Log

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

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

- Call Log Configuration
- Exporting Call Log

Call Log Configuration

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

Parameter	features.save_call_history	<y0000000000xx>.cfg
Description	It enables or disables the phone to save the local call log.	
Permitted Values	**0**-Disabled, the phone cannot save the missed calls, placed calls, received calls and the forwarded calls in the call log lists. **1**-Enabled	
Default	1	
Web UI	**Features** > **General Information** > **Save Call Log**	
Phone UI	**Menu** > **Setting** > **Features** > **History Setting** > **History Record**	
Parameter	account.1.missed_calllog	<MAC>.cfg
Description	It enables or disables the phone to indicate and record missed calls. **Note:**It works only if "features.save_call_history" is set to 1 (Enabled).	

Permitted Values	**0**-Disabled, the phone does not display indicator on the idle screen and does not log the missed call in the Missed Calls list when missed calls.
	1-Enabled, the phone displays an indicator icon on the idle screen and logs the missed call in the Missed Calls list when missed calls.
Default	1
Web UI	**Account** > **Basic** > **Missed Call Log**
Parameter	**features.call_history_contacts_avator.enable** **<y0000000000xx>.cfg**
Description	It enables or disables the phone to display the contact avatars for history records.
	Note: It is only applicable to MP56/CP960/T58A/T56A/T55A/T48S/T46S Skype for Business phones.
Permitted Values	**0**-Disabled, the phone only displays default avatars for history records.
	1-Enabled, the phone displays contact avatars for history records.
Default	1
Web UI	**Features** > **General Information** > **History Record Contacts Avatar**
Phone UI	**Menu** > **Setting** > **Features** > **History Setting** > **Contacts Avatar**

Exporting Call Log

You can download the call logs to the local system to check the phone events.

Procedure

1. Click **Settings** > **Configuration**.
2. In the **Export Call Log** field, click **Export** to open the file download window, and then save the file to your local system.

Contact Management

Your phone can store local contacts, Skype for Business contacts and Outlook contacts.

- Skype for Business Directory
- Local Directory
- Local Favorites
- Outlook Contacts

Skype for Business Directory

The Skype for Business directory on your phone stores all Skype for Business contacts (up to 1000 skype for Business contacts). You can search, add, view or delete Skype for Business contacts either by your phone or by the Skype for Business client.

- Line Key LED Indicators

- Line Key Led Light On Configuration

Line Key LED Indicators

Line key LED indicator on your phone (when configured as Skype for Business favorites):

LED Status	Description
Green	The Skype for Business favorite is available.
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.
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.

Line Key Led Light On Configuration

The following table lists the parameters you can use to configure the line key LED indicator.

Parameter	phone_setting.line_key_led.enable	<y0000000000xx>.cfg
Description	It enables or disables the line key LED indicators on the phone to monitor the status of the Skype for Business favorites. **Note:** It is only applicable to T46S/T42S/T41S Skype for Business phones.	
Permitted Values	**0**-Disabled, the line key LED indicators do not change according to the status changes of the monitored Skype for Business favorites. **1**-Enabled, the line key LED indicators change according to the status changes of the monitored Skype for Business favorites.	
Default	0	
Web UI	**Features** > **LED** > **Line Key Led Light On**	

Local Directory

Yealink Skype for Business phones also maintain a local directory. The Skype for Business phones can store up to 1000 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, and the file format must be *.xml or *.csv.

- Local Directory Configuration
- Local Directory Customization

Local Directory Configuration

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

Parameter	features.local_directory.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to display a directory called Local Directory. **Note:** It is only applicable to CP960 Skype for Business phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Parameter	local_contact.data.url	<y0000000000xx>.cfg
Description	It configures the access URL of the local contact file (*.xml).	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Directory** > **Local Directory** > **Import Local Contact File**	

Local Directory Customization

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.

- Local Contact File Attributes
- Customizing the Local Contact File

Local Contact File Attributes

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.

Element	Values	Description
root_contact	no	Contact list's root element.
contact	no	Contact's root element.
display_name	String	An element of contact. Contact name. **Note:** This value cannot be blank or duplicated.
office_number	String	Office number of the contact.
mobile_number	String	Mobile number of the contact.
other_number	String	Other number of the contact.
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 MP56/CP960/T58A/T56A/ T55A/T48S Skype for Business phones**: 0~32. **For T46S Skype for Business phones**: 0~27. **For T42S/T41S Skype for Business phones:** 0~15.	It is only applicable to local 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.

Customizing the Local Contact File

Procedure

1. Open the local contact file.
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" />
4. Save the changes and place this file to the provisioning server

Local Favorites

Local favorites and Skype for Business favorites of the phone are displayed on the idle screen. By default, local favorites are displayed before the Skype for Business favorites.

You can configure whether to display local favorites on the idle screen and configure the display order of the local favorites.

For MP56/CP960/T58A/T56A/T55A/T48S/T46S Skype for Business phones: local favorite is indicated

by ⭐ icon. For T42S/T41S Skype for Business phones: local favorite is indicated by ★ icon. Skype for Business favorite is indicated by the presence status icon. The following figure shows a sample Favorites list.
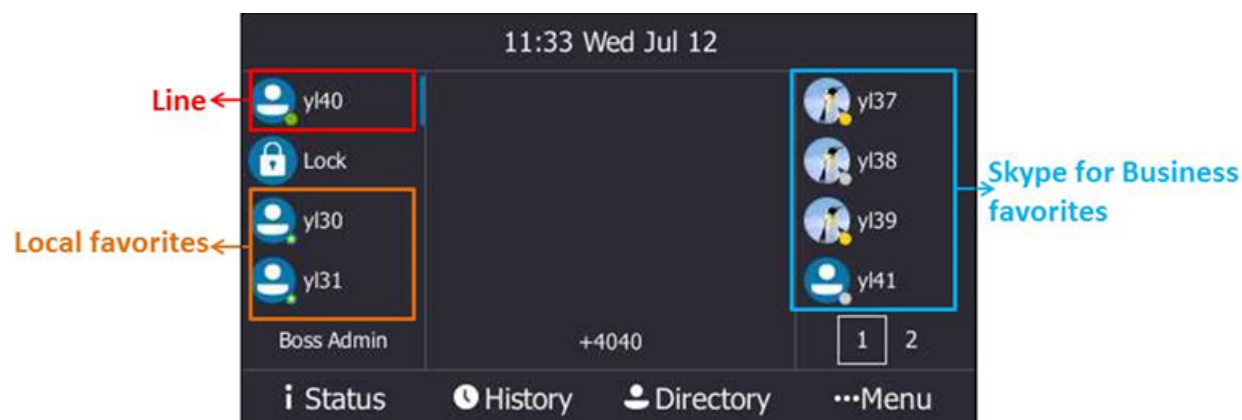
📝   **Note:** Only Skype for Business favorites have presence status.

- Local Favorites Configuration

Local Favorites Configuration

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

Parameter	sfb.local_favorite.enable	<y0000000000xx>.cfg

Description	It enables or disables the phone to display local favorites on the idle screen (on the **Favorites** screen for MP56/T58A/T56A/T55A/CP960 Skype for Business phones).
Permitted Values	**0**-Disabled, local favorites are not displayed on the idle screen, only Skype for Business favorites are displayed on the idle screen (on the **Favorites** screen for MP56/T58A/T56A/T55A/CP960 Skype for Business phones). **1**-Preferential, the local favorites will be displayed before the Skype for Business favorites on the idle screen (on the **Favorites** screen for MP56/T58A/T56A/T55A/CP960 Skype for Business phones).
Default	1
Web UI	**Directory** > **Settings** > **Local Favorite**

Parameter	**sfb.local_favorite.sort**	**<y0000000000xx>.cfg**
Description	It configures the order of the local favorites on the idle screen. **Note:** It works only if "sfb.local_favorite.enable" is set to 1 (Enabled).	
Permitted Values	**1**-Preferential, the local favorites will be displayed before the Skype for Business favorites on the idle screen (on the **Favorites** screen for MP56/T58A/T56A/T55A/CP960 Skype for Business phones). **2**-General, the local favorites will be displayed after the Skype for Business favorites on the idle screen (on the **Favorites** screen for MP56/T58A/T56A/T55A/CP960 Skype for Business phones).	
Default	1	
Web UI	**Directory** > **Settings** > **Local Favorite**	

Outlook Contacts

Skype for Business Server and Exchange Server are integrated. You can add Outlook contacts on the Microsoft Outlook only. You can view and search Outlook contacts on your phones.

- Outlook Contacts Configuration

Outlook Contacts Configuration

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

Parameter	**exchange.outlook_contact.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to display a directory called Outlook Contacts. This directory will include your Outlook contacts.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Parameter	**phone_setting.search_outlook_contacts.return_numb**	**<y0000000000xx>.cfg**

Description	It defines the maximum number of Outlook contacts to be displayed when you perform a search in the dialing screen.
Permitted Values	Integer from 0 to 1000
Default	20

Parameter	**exchange.outlook_contact_sync.enable**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to synchronize outlook contacts from the Exchange Server.	
Permitted Values	**0-**Disabled **1-**Enabled	
Default	1	

Parameter	**phone_setting.outlook_contacts.update_time**[1]	**<y0000000000xx>.cfg**
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.	
Permitted Values	Integer from 0 to 100	
Default	10	

Parameter	**exchange.outlook_contact.request_number**[1]	**<y0000000000xx>.cfg**
Description	It configures the maximum outlook contacts that can be downloaded from the Exchange Server.	
Permitted Values	Integer from 1 to 5000	
Default	**For MP56/T58A/T56A/T55A/T48S/T46S:** The default value is 500. **For CP960/T42S/T41S:** The default value is 300.	

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

Call Features

This chapter shows you how to configure the call feature on Skype for Business devices.

- Dial Plan
- Dial Search Delay
- Live Dialpad
- Call Waiting

- Auto Answer
- Incoming Call Display
- Call Hold
- Call Forward
- Return Code When Refuse
- Call Number Filter
- Search Number Filter
- Allow Mute
- Audio Recording
- Voice Mail without PIN
- Call Queue
- Hotline
- Multicast Paging
- Response Group
- Team-Call Group

Dial Plan

Dial plan is a string of characters that governs the way the phone processes 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 with the method of In-band provisioning. When user enters digits on the dialing screen, the phone will match the digits to a dial plan.

- Dial Now
- Dial Now File Customization

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.

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.

- Dial Now Configuration

Dial Now Configuration

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

Parameter	dialplan.dialnow.rule.X[1]	<y0000000000xx>.cfg
Description	It configures the dial-now rule (the string used to match the numbers entered by the user). When entered numbers match the predefined dial-now rule, the phone will automatically dial out the numbers without pressing the send key.	
Permitted Values	String within 511 characters	
Default	Blank	

Web UI	Settings > Dial Plan > Dial-now > Rule	
Parameter	**phone_setting.dialnow_delay**	**<y0000000000xx>.cfg**
Description	It 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.	
Permitted Values	Integer from 0 to 14	
Default	1	
Web UI	**Features** > **General Information** > **Time-Out for Dial-Now Rule**	
Parameter	**dialplan_dialnow.url**	**<y0000000000xx>.cfg**
Description	It configures the access URL of the dial-now rule template file.	
Permitted Values	URL within 511 characters	
Default	Blank	

[1]X ranges from 1 to 100.

Dial Now File Customization

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.

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.

- Dial Now File Attributes
- Customizing the Dial-now File

Dial Now File Attributes

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

Attributes	Description
DialNowRule	Specify the dial-now number.
LineID	Specify a registered line to apply the dial-now rule. Valid Values: 0, 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. Multiple line IDs are separated by commas.

Customizing the Dial-now File

Procedure

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

   For example,

   <Data DialNowRule="1001" LineID="0" / >
4. Save the changes and place this file to the provisioning server

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 you search for contacts on the dialing screen.

- Dial Search Delay Configuration

Dial Search Delay Configuration

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

Parameter	sfb.search_delay_time	<y0000000000xx>.cfg
Description	It configures the delay time (in seconds) for the phone to automatically display the search results on the dialing screen.	
Permitted Values	Integer from 1 to 10	
Default	1	
Web UI	**Features** > **General Information** > **Dial Search Delay**	

Live Dialpad

Live dialpad allows the phone to automatically dial out the entered phone number after a specified period of time.

- Live Dialpad Configuration

Live Dialpad Configuration

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

Parameter	phone_setting.predial_autodial	<y0000000000xx>.cfg
Description	It enables or disables live dialpad feature.	
Permitted Values	**0**-Disabled **1**-Enabled, the phone will automatically dial out the entered phone number on the dialing screen without pressing a send key.	
Default	0	

Web UI	Settings > Preference > Live Dialpad	
Parameter	**phone_setting.inter_digit_time**	**<y0000000000xx>.cfg**
Description	It configures the delay time (in seconds) for the phone to automatically dial out the entered digits without pressing a send key. **Note:** It works only if "phone_setting.predial_autodial" is set to 1 (Enabled).	
Permitted Values	Integer from 1 to 14	
Default	8	

Call Waiting

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

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

- Call Waiting Configuration

Call Waiting Configuration

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

Parameter	call_waiting.enable	<y0000000000xx>.cfg
Description	It enables or disables call waiting feature.	
Permitted Values	**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 will present a new incoming call while during a call.	
Default	1	
Web UI	Features > General Information > Call Waiting	
Phone UI	Menu > Setting > Features > Call Waiting > Call Waiting	
Parameter	**call_waiting.tone**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to play the call waiting tone when the phone receives an incoming call during a call. **Note:** It works only if "call_waiting.enable" is set to 1 (Enabled).	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	Features > Audio > Call Waiting Tone	
Phone UI	Menu > Setting > Features > Call Waiting > Play Tone	

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 the auto answer is enabled. Auto-Answer delay defines a period of delay time before the phone automatically answers incoming calls.

- Auto Answer Configuration

Auto Answer Configuration

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

Parameter	account.1.auto_answer	<MAC>.cfg
Description	It enables or disables auto answer feature. **Note:** The phone cannot automatically answer the incoming call during a call even if auto answer is enabled.	
Permitted Values	**0**-Disabled **1**-Enabled, the phone can automatically answer an incoming call.	
Default	0	
Web UI	**Account** > **Basic** > **Auto Answer**	
Phone UI	**Menu** > **Setting** > **Features** > **Auto Answer** > **Auto Answer**	
Parameter	features.auto_answer_delay	<y0000000000xx>.cfg
Description	It configures the delay time (in seconds) before the phone automatically answers an incoming call.	
Permitted Values	Integer from 1 to 4	
Default	1	
Web UI	**Features** > **General Information** > **Auto-Answer Delay(1~4s)**	

Incoming Call Display

You can configure whether the phone preferentially shows the incoming call even the phone is in use.

- Incoming Call Display Configuration

Incoming Call Display Configuration

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

Parameter	phone_setting.incoming_call.priority	<y0000000000xx>.cfg
Description	It enables or disables the phone to focus on the incoming call when the phone is during a call.	
Permitted Values	**0**-Disabled **1**-Enabled	

Default	1	
Parameter	**phone_setting.incoming_call_when_dialing.priority**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to preferentially show incoming calls when you are dialing a call. **Note:** It works only if "phone_setting.incoming_call.priority" is set to 1 (Enabled).	
Permitted Values	**0**-Disabled, the phone shows the incoming call only when the phone is not in the dialing screen. **1**-Enabled, the phone shows the incoming call even though you are dialing a call.	
Default	1	

Call Hold

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

- Call Hold Configuration
- Music on Hold Configuration

Call Hold Configuration

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

Parameter	**features.play_hold_tone.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to play a warning tone when there is a call on hold.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Features** > **General Information** > **Play Hold Tone**	
Parameter	**features.play_hold_tone.delay**	**<y0000000000xx>.cfg**
Description	It configures the interval (in seconds) at which the phone plays 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 "features.play_hold_tone.enable" is set to 1 (Enabled).	

Permitted Values	Integer from 3 to 3600
Default	30
Web UI	**Features** > **General Information** > **Play Hold Tone Delay**

Music on Hold Configuration

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

Parameter	**sfb.music_on_hold.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to play a music for the held party.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Settings** > **MOH** > **MOH Enable**	
Parameter	**sfb.music_on_hold.mode**	**<y0000000000xx>.cfg**
Description	It configures the source of the music played for the held party. **Note:**It works only if "sfb.music_on_hold.enable" is set to 1 (Enabled).	
Permitted Values	**0**-Inband Provision, your phone will play the music received from the Skype for Business Server (via Inband provisioning method) to the held party. **1**-Local Custom, your phone will play the custom music to the held party.	
Default	1	
Web UI	**Settings** > **MOH** > **MOH Mode**	
Parameter	**sfb.music_on_hold.url**	**<y0000000000xx>.cfg**
Description	It configures the access URL of the custom music file. **Note:**It works only if "sfb.music_on_hold.enable" and parameter "sfb.music_on_hold.mode" are set to 1 (Enabled).	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Settings** > **MOH** > **MOH File**	
Parameter	**sfb.music_on_hold.delete**	**<y0000000000xx>.cfg**
Description	It delete all custom music files.	
Permitted Values	http://localhost/all	
Default	Blank	
Web UI	**Settings** > **MOH** > **Delete**	

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.

Call forwarding has the 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.
- **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 a team-call group assigned to your line, you can enable your team-call members' phones to simultaneously ring when you receive incoming calls.

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 where the call was from, and from which phone number it was forwarded.

It is not applicable to MP56/CP960/T58A/T56A/T55A Skype for Business phones.

- Call Forwarding Configuration

Call Forwarding Configuration

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

Parameter	features.fwd_diversion_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to present the diversion information when an incoming call is forwarded to your phone. **Note:** It is not applicable to MP56/CP960/T58A/T56A/T55A Skype for Business phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Features** > **General Information** > **Diversion/History-Info**	

Return Code When Refuse

Return code when refuse defines the return code and reason of the SIP response message for the refused call. The caller's phone LCD screen displays the reason according to the received return code. Available return codes and reasons are:

- 404 (Not Found)

- 480 (Temporarily Not Available)
- 486 (Busy Here)
- 603 (Decline)

- Return Code When Refuse Configuration

Return Code When Refuse Configuration

The following table lists the parameters you can use to configure the return code for the refused call.

Parameter	features.normal_refuse_code	<y0000000000xx>.cfg
Description	It configures a return code and reason of SIP response messages when the phone rejects an incoming call. A specific reason is displayed on the caller's phone LCD screen.	
Permitted Values	**404**-Not Found **480**-Temporarily Not Available **486**-Busy Here, the caller's phone LCD screen will display the message "Busy Here" when the callee rejects the incoming call. **603**-Decline	
Default	603	
Web UI	**Features** > **General Information** > **Return code when refuse**	

Call Number Filter

Call number filter feature allows the phone to automatically filter out particular characters when dialing a number.

- Call Number Filter Configuration

Call Number Filter Configuration

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

Parameter	features.call_num_filter	<y0000000000xx>.cfg
Description	It configures the characters that the phone filters out when dialing a number. If the dialed number contains the configured characters, the phone will automatically filter out those characters when dialing. But if the dialed SIP address contains the configured characters, the phone will not filter out those characters when dialing. **Note**: If it is left blank, the phone will not automatically filter out 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).	
Permitted Values	String within 99 characters	
Default	()-	
Web UI	**Features** > **General Information** > **Call Number Filter**	

Search Number Filter

Search number filter feature allows the phone to automatically filter out the particular characters when searching for contacts.

* Search Number Filter Configuration

Search Number Filter Configuration

The following table lists the parameters you can use to configure the search number filter.

Parameter	features.search_num_filter[1]	<y0000000000xx>.cfg
Description	It configures the characters that the phone filters out from the contact number when searching it. **Note**: If it is left blank, the phone will not automatically filter out any characters when searching for contacts. If you want to filter out just a space, you have to set the value to " ," (a space first followed by a comma).	
Permitted Values	String within 99 characters	
Default	()-	
Web UI	**Features** > **General Information** > **Search Number Filter**	

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

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.

* Allow Mute Configuration

Allow Mute Configuration

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

Parameter	features.allow_mute	<y0000000000xx>.cfg
Description	It enables or disables the phone to mute an active call.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Features** > **General Information** > **Allow Mute**	

Audio Recording

Yealink Skype for Business phones support recording active calls, but only MP56/CP960/T58A/T56A/T55A Skype for Business phones support recording local audio when the phone is idle.

For MP56/CP960/T58A/T56A/T55A Skype for Business phones, if you connect a USB flash drive to the phone, you can choose to save the recorded files to the Internal SD card or USB flash drive.

For T48S/T46S/T42S/T41S Skype for Business phones, you must connect a USB flash drive to save the recorded files.

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.

- Audio Recording Configuration

Audio Recording Configuration

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

Parameter	features.usb_call_recording.enable	<y0000000000xx>.cfg
Description	It enables or disables the call recording feature for the phone. **Note:** It is not applicable to CP960 Skype for Business phones. And local audio recording is only applicable for MP56/T58A/T56A/T55A Skype for Business phones with the value of the parameter "features.call_recording.fast_entrance" set to 1.	
Permitted Values	**0**-Disabled, you cannot record the local audio or active call. **1**-Enabled, you can record the local audio or active call (For T48S/T46S/T42S/T41S Skype for Business phones, the recorded calls will be saved to the USB flash drive.)	
Default	0	
Web UI	**Features** > **General Information** > **Allow Mute**	
Parameter	features.call_recording.enable	<y0000000000xx>.cfg
Description	It enables or disables the call recording feature for the phone. **Note:** It is only applicable to CP960 Skype for Business phones.	
Permitted Values	**0**-Disabled, you cannot record the local audio or active call. **1**-Enabled, you can record the local audio or active call.	
Default	0	
Parameter	features.call_recording.fast_entrance	<y0000000000xx>.cfg
Description	It enables or disables the phone to display a Recording entry on the menu screen so that you can view the recorded calls or audios quickly. **Note:** It is only applicable to MP56/CP960/T58A/T56A/T55A Skype for Business phones. For MP56/T58A/T56A/T55A Skype for Business phones, if it is disabled, you cannot record the local audio.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	

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 the voice mail box without entering a PIN. It is especially useful for users who often access mailbox from the phone in their own offices.

- Voice Mail without PIN Configuration

Voice Mail without PIN Configuration

The following table lists the parameters you can use to configure the voice mail without PIN.

Parameter	account.1.voice_mail.skip_pin.enable	<MAC>.cfg
Description	It enables or disables the phone to access the voice mail box without entering a PIN.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	

Call Queue

If you sign into the device using an Online account, you can use the call queue feature. On-Premises environment does not support this feature.

A call queue is a feature that route and queue incoming calls to group numbers, called agents, such as for a help desk or a customer service desk.

When someone calls into a phone number that is set 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 and waiting. After a call agent accepts the call, other agents' phones stop ringing.

For information on creating a call queue, refer to *Create a Phone System call queue* on Microsoft TechNet.

Hotline

Hotline, sometimes referred to as hot dialing, is a point-to-point communication link in which a call is automatically directed to the preset hotline number. If you lift the handset, press the Speakerphone key or the line key (line key is not applicable to MP56/CP960/T58A/T56A/T55A/T48S phones), and do nothing for a specified time interval, the IP phone will automatically dial out the hotline number. Skype for Business phones only support one hotline number.

- Hotline Configuration

Hotline Configuration

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

Parameter	features.hotline_number	<y0000000000xx>.cfg

Description	It configures the hotline number that the phone automatically dials out when you lift the handset, press the Speakerphone/off-hook key or the line key. Leaving it blank disables hotline feature. **Note:** Line key is not applicable to MP56/T58A/T56A/T55A/T48S Skype for Business phones.
Permitted Values	String within 32 characters
Default	Blank
Web UI	**Features** > **General Information** > **Hotline Number**
Phone UI	**Menu** > **Setting** > **Features** > **Hotline** > **Hot Number**
Parameter	**features.hotline_delay** **<y0000000000xx>.cfg**
Description	It configures the waiting time (in seconds) for the phone to automatically dial out the hotline number. If it is set to 0 (0s), the phone will immediately dial out the preconfigured hotline number when you lift the handset, press the Speakerphone/off-hook key or press the line key. 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 you lift the handset, press the Speakerphone/off-hook key or press the line key. **Note:** Line key is not applicable to MP56/T58A/T56A/T55A/T48S Skype for Business phones.
Permitted Values	Integer from 0 to 10
Default	4
Web UI	**Features** > **General Information** > **Hotline Delay(0~10s)**
Phone UI	**Menu** > **Setting** > **Features** > **Hotline** > **HotLine Delay**

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**.**

- Multicast Paging Group Configuration
- Multicast Listening Group Configuration
- Multicast Paging Settings

Multicast Paging Group Configuration

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

Parameter	**multicast.paging_address.X.ip_address**[1] **<y0000000000xx>.cfg**

Description	It configures the IP address and port number of the multicast paging group in the paging list.
	It will be displayed on the LCD screen when placing the multicast paging call.
	Note: It is not applicable to CP960 Skype for Business phones. The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.
Permitted Values	String
Default	Blank
Web UI	**Directory** > **Multicast IP** > **Paging List** > **Paging Address**
Phone UI	**Menu** > **Setting** > **Features** > **Paging List** > **Option** > **Edit** > **Address**
Parameter	**multicast.paging_address.X.label**[1] **<y0000000000xx>.cfg**
Description	It configures the name of the multicast paging group to be displayed in the paging list.
	It will be displayed on the LCD screen when placing the multicast paging calls.
	Note: It is not applicable to CP960 Skype for Business phones.
Permitted Values	String
Default	Blank
Web UI	**Directory** > **Multicast IP** > **Paging List** > **Label**
Phone UI	**Menu** > **Setting** > **Features** > **Paging List** > **Option** > **Edit** > **Label**

[1]X ranges from 1 to 10.

Multicast Listening Group Configuration

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

Parameter	**multicast.listen_address.X.ip_address**[1] **<y0000000000xx>.cfg**
Description	It configures the multicast address and port number that the phone listens to.
	Note: It is not applicable to CP960/T55A Skype for Business phones. The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.
Permitted Values	IP address: port
Default	Blank
Web UI	**Directory** > **Multicast IP** > **Multicast Listening** > **Listening Address**
Parameter	**multicast.listen_address.X.label**[1] **<y0000000000xx>.cfg**
Description	(Optional.) It configures the label to be displayed on the LCD screen when receiving the multicast paging calls.
	Note: It is not applicable to CP960/T55A Skype for Business phones.
Permitted Values	String within 99 characters

Default	Blank
Web UI	**Directory** > **Multicast IP** > **Multicast Listening** > **Label**

[1]X ranges from 1 to 10.

Multicast Paging Settings

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

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

Paging Barge

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.

- Multicast Paging Settings Configuration

Multicast Paging Settings Configuration

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

Parameter	**multicast.codec**	**<y0000000000xx>.cfg**
Description	It configures the codec of multicast paging. **Note**: It is not applicable to CP960 Skype for Business phones.	
Permitted Values	PCMU, PCMA, G729, G722	
Default	G722	
Web UI	**Features** > **General Information** > **Multicast Codec**	
Parameter	**multicast.receive_priority.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to handle the incoming multicast paging calls when there is an active multicast paging call on the phone. **Note:** It is not applicable to CP960/T55A Skype for Business phones.	

Permitted Values	**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.
Default	1
Web UI	**Directory** > **Multicast IP** > **Paging Priority Active**

Parameter	**multicast.receive_priority.priority**	**<y0000000000xx>.cfg**
Description	It configures the priority of the voice call (a normal phone call rather than a multicast paging call) in progress.	
	1 is the highest priority, 10 is the lowest priority.	
	Note: It is not applicable to CP960/T55A Skype for Business phones.	
Permitted Values	**0**-Disabled, all incoming multicast paging calls will be automatically ignored when a voice call is in progress.	
	1-1	
	...	
	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.	
Default	10	
Web UI	**Directory** > **Multicast IP** > **Paging Barge**	

[1]X ranges from 1 to 10.

Response Group

If you sign into the phone using an On-Premises account, you can use the response group feature. But the current Online environment does not support this feature.

A response group is a feature that route and queue incoming calls to group numbers, called agents, such as to 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 available 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 as 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* on Microsoft TechNet.

You can configure whether to display a missed call on the group members' phone when the response group call was not answered.

- Response Group Configuration

Response Group Configuration

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

Parameter	features.response_group_history.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to display a missed call when the response group call was not answered. **Note:** It is only applicable to MP56/CP960/T58A/T56A/T55A Skype for Business phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Parameter	phone_setting.rsg_call_ring.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to play a distinct ringtone for response group calls.	
Permitted Values	**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 ringtone for response group calls.	
Default	1	
Parameter	phone_setting.rsg_call_ring_type	<y0000000000xx>.cfg
Description	It 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).	
Default	Ring1.wav	
Phone UI	**Menu** > **Setting** > **Basic** > **Sounds** > **Ring Tones** > **Response Group**	

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 configure 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 any team member picks up the phone, the other phones stop ringing.

- Team-Call Ringtone Configuration

Team-Call Ringtone Configuration

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

Parameter	**phone_setting.team_call_ring.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to play a distinct ringtone for team-call.	
Permitted Values	**0**-Disabled, incoming calls to the 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 ringtone for team-call.	
Default	1	
Parameter	**phone_setting.team_call_ring_type**	**<y0000000000xx>.cfg**
Description	It configures a ring tone for the team-call.	
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).	
Default	Ring1.wav	
Phone UI	**Menu** > **Setting** > **Basic** > **Sounds** > **Ring Tones** > **Team Call**	

Advanced Features

The advanced features require server support. Consult your server partner to find out if these features are supported.

- E911
- Action URI
- Shared Line Appearance (SLA)
- Intercom
- Hot Desking

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:

*   MAC address
*   IP address
*   Subnet
*   SIP URI
*   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.

*   LIS URI
*   Enhanced Emergency Enabled
*   Location Required
*   Emergency Dial String
*   Emergency Dial String Mask
*   Secondary Location Source
*   Notify URI
*   Conf URI
*   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>
```

When user dials an emergency number, you can configure whether the number should be applied the dial plan configured on the Skype for Business server.

> 📝 **Note:** If the user's presence status is DND before dialing an emergency number, it will reset to Available from DND when an E911 number is dialed.

- E911 Emergency Call Translation Configuration
- E911 Location Tip
- Adding the Location Information

E911 Emergency Call Translation Configuration

The following table lists the parameters you can use to configure the E911 emergency call translation.

Parameter	phone_setting.e911.translation_enable[1]	<y0000000000xx>.cfg
Description	It enables or disables the phone to apply the dial plan configured on the Skype for Business server when user dials emergency numbers. **Note:** It is only applicable to MP56/CP960/T58A/T56A/T55A Skype for Business phones.	
Permitted Values	**0**-Disabled, the phone adds a prefix "+" to the emergency number automatically when dialing. The dialed emergency number ignores the dial plan configured on the Skype for Business server. **1**-Enabled, the dialed emergency number applies the dial plan configured on the Skype for Business server.	
Default	1	

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

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 enabling users to either ignore the notification or edit the location information.
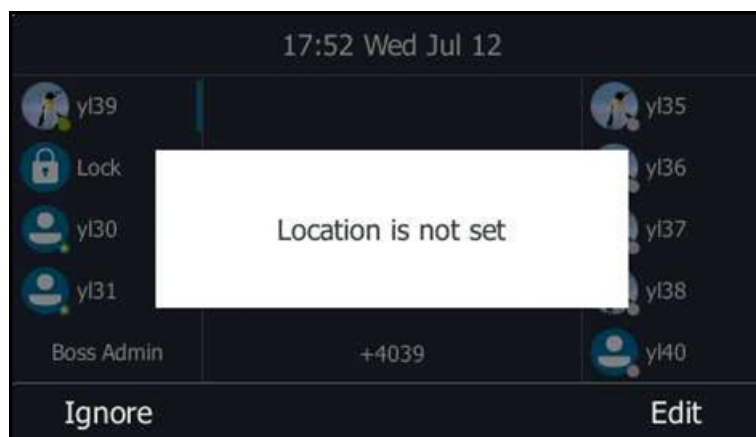
- E911 Location Tip Configuration

E911 Location Tip Configuration

The following table lists the parameters you can use to configure the E911 emergency call translation.

Parameter	sfb.E911_location_tip[1]	<y0000000000xx>.cfg
Description	It enables or disables the idle screen to display the notification "Location is not set" when the location of the phone is not set. **Note:** It is only applicable to MP56/CP960/T58A/T56A/T55A Skype for Business phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Features** > **General Information** > **E911 Location Tip**	

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

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

1. Click **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 drop-down menu of **Country**.
9. Click **Confirm** to accept the change.

Action URI

Yealink phones can perform the specified action by receiving and handling an HTTP or HTTPS GET request or accept a SIP NOTIFY message with the "Event: ACTION-URI" header from a SIP proxy server.

- Supported HTTP/HTTPS GET Request
- Action URI Configuration
- Example: Capturing the Current Screen of the Phone

Supported HTTP/HTTPS GET Request

Action URI allows phones to interact with a 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.

Action URI Configuration

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

Parameter	features.action_uri.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to receive the action URI requests.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Parameter	features.action_uri_limit_ip	<y0000000000xx>.cfg
Description	It 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. **Note**: It works only if "features.action_uri.enable" is set to 1 (Enabled).	
Permitted Values	IP address or any	
Default	Blank	
Web UI	**Features** > **Remote Control** > **Action URI allow IP List**	

Example: Capturing the Current Screen of the Phone

You can capture the screen display of the 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 the web browser does not remember the user name and password for web user interface login.

> **Note:** You can also use the old URI "http://<phoneIPAddress>/servlet?command=screenshot" to capture the screen display.

Procedure

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:
3. 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 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.

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 an 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 progress, 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 T55A Skype for Business phones.

> **Note:** A user can be assigned to be one SLA group only.

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 Configuration
- Incoming Intercom Configuration

Outgoing Intercom Configuration

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

Parameter	features.intercom.enable	<y0000000000xx>.cfg
Description	It enables or disables the intercom feature. **Note**: It is not applicable to CP960 Skype for Business phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	For individual phone: 1 For common area phone: 0	
Web UI	**Features** > **Audio** > **Send Sound**	
Parameter	features.intercom.outgoing	<y0000000000xx>.cfg
Description	It enables or disables the phone to place an outgoing intercom call from the intercom list. **Note**: It is not applicable to CP960 Skype for Business phones. It works only if "features.intercom.enable" is set to 1 (Enabled).	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Features** > **Intercom** > **Outgoing Intercom**	
Phone UI	**Menu** > **Setting** > **Features** > **Intercom** > **Outgoing Intercom**	
Parameter	intercom.x.label[1]	<y0000000000xx>.cfg
Description	(Optional.) It configures the label displayed on the intercom list. **Note:** It is not applicable to CP960 Skype for Business phones. It works only if "features.intercom.enable" and "features.intercom.outgoing" are set to 1 (Enabled).	
Permitted Values	String	
Default	Blank	
Web UI	**Features** > **Intercom** > **Label**	

Phone UI	**Menu** > **Setting** > **Features** > **Intercom List** > **Option** > **Edit** > **Label**	
Parameter	**intercom.x.value**[1]	**<y0000000000xx>.cfg**
Description	It configures the intercom number displayed on the intercom list. **Note:** It is not applicable to CP960 Skype for Business phones. It works only if "features.intercom.enable" and "features.intercom.outgoing" are set to 1 (Enabled).	
Permitted Values	String	
Default	Blank	
Web UI	**Features** > **Intercom** > **Value**	
Phone UI	**Menu** > **Setting** > **Features** > **Intercom List** > **Option** > **Edit** > **Value**	

[1]x ranges from 1 to 10.

Incoming Intercom Configuration

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

Parameter	**features.intercom.allow**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to answer an incoming intercom call. **Note**: It is not applicable to CP960 Skype for Business phones. It works only if "features.intercom.enable" is set to 1 (Enabled).	
Permitted Values	**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.	
Default	1	
Web UI	**Features** > **Intercom** > **Intercom Allow**	
Phone UI	**Menu** > **Setting** > **Features** > **Intercom** > **Intercom Allow**	
Parameter	**features.intercom.mute**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to mute the microphone when answering an intercom call. **Note:** It is not applicable to CP960 Skype for Business phones. It works only if "features.intercom.allow" is set to 1 (Enabled).	
Permitted Values	**0**-Disabled **1**-Enabled, the microphone is muted for intercom calls, and then the other party cannot hear you.	
Default	0	
Web UI	**Features** > **Intercom** > **Intercom Mute**	

Phone UI	Menu > Setting > Features > Intercom > Intercom Mute	
Parameter	**features.intercom.tone**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to play a warning tone when answering an intercom call. **Note:** It is not applicable to CP960 Skype for Business phones. It works only if "features.intercom.allow" is set to 1 (Enabled).	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Features** > **Intercom** > **Intercom Tone**	
Phone UI	**Menu** > **Setting** > **Features** > **Intercom** > **Intercom Tone**	
Parameter	**features.intercom.barge**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to answer an incoming intercom call while there is already an active call on the phone. **Note:** It is not applicable to CP960 Skype for Business phones. It works only if "features.intercom.allow" and "call_waiting.enable" are set to 1 (Enabled).	
Permitted Values	**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.	
Default	0	
Web UI	**Features** > **Intercom** > **Intercom Barge**	
Phone UI	**Menu** > **Setting** > **Features** > **Intercom** > **Intercom Barge**	

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, as a result, the offices would often be vacant and consumes valuable space and resources.

Hot desking allows a Guest to clear the Host's registration configurations on the phone, and then register his own account.

- Hot Desking Configuration

Hot Desking Configuration

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

Parameter	**sfb.hot_desking.enable**	**<y0000000000xx>.cfg**

Description	It enables or disables the hot desking feature.
Permitted Values	**0**-Disabled **1**-Enabled
Default	1
Web UI	**Features** > **General Information** > **Hot Desking Enable**
Phone UI	**Menu** > **Setting** > **Features** > **Hot-Desking**

Security Features

- User and Administrator Identification
- Auto-Logout Time
- Phone Lock
- Account Lock
- Transport Layer Security (TLS)
- Encrypting Configuration Files

User and Administrator Identification

By default, some menu options are protected by the privilege levels: user and administrator, each with its own password. You can also customize the access permission for configurations on the web user interface and phone user interface. Yealink phones support the access levels of admin, var and user.

When logging into the web user interface or access the advanced settings on the device, as an administrator, you need an administrator password to access various menu options. The default username and password for administrator are "admin". Both you and the user can log into the web user interface, and you will see all of the user options. The default username and password for the user are "user".

For security reasons, you should change the default user or administrator password as soon as possible. Since the advanced menu options are strictly used by the administrator, users can configure them only if they have administrator privileges.

- User and Administrator Identification Configuration

User and Administrator Identification Configuration

The following table lists the parameters you can use to configure the user and administrator identification.

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

Default	admin	
Parameter	**static.security.user_password**	**<y0000000000xx>.cfg**
Description	It configures the password of the user or administrator. The device 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 to 123. static.security.user_password = admin:456 means setting the password of administrator to 456. **Note**: The devices support ASCII characters 32-126(0x20-0x7E) in passwords. You can set the password to be empty via the web user interface only.	
Permitted Values	String within 32 characters	
Default	user	
Web UI	**Security** > **Password**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Set Password** **Note**: You cannot change the user password via the phone user interface.	

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 the web user interface. Once logging out, you must re-enter username and password for web access authentication.

- Auto-Logout Time Configuration

Auto-Logout Time Configuration

The following table lists the parameters you can use to configure auto-logout time.

Parameter	**features.relog_offtime**[1]	**<y0000000000xx>.cfg**
Description	It configures the timeout interval (in minutes) for web access authentication. **Note**: It is only applicable to T48S/T46S Skype for Business phones.	
Permitted Values	Integer from 1 to 1000	
Default	5	
Web UI	**Features** > **General Information** > **Auto-Logout Time(1~1000min)**	

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

Phone Lock

If system administrator sets the policy "ucEnforcePinLock" = true on the Skype for Business Fronted Server, user can use the phone lock feature to lock the phone to prevent it from unauthorized use. And the phone will prompt the user to configure an unlock PIN at the initial sign-in.

- Phone Lock Configuration

Phone Lock Configuration

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

Parameter	phone_setting.phone_lock.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone lock feature.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Settings** > **Phone Lock** > **Phone Lock**	
Phone UI	**Menu** > **Setting** > **Basic** > **Phone Lock** > **Phone Lock**	
Parameter	phone_setting.phone_lock.lock_time_out	<y0000000000xx>.cfg
Description	It configures the interval (in minutes) to automatically lock the phone.	
Permitted Values	Integer from 1 to 1440	
Default	10	
Web UI	**Features** > **Phone Lock** > **Idle time-out(1~1440mins)**	
Phone UI	**Menu** > **Setting** > **Basic** > **Phone Lock** > **Idle time-out**	
Parameter	sfb.phone_lock.max_attempts	<y0000000000xx>.cfg
Description	It 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.	
Permitted Values	Integer from 3 to 10	
Default	5	
Web UI	**Settings** > **Phone Lock** > **Max attempts of unlock**	
Phone UI	**Menu** > **Setting** > **Basic** > **Phone Lock** > **Unlock attempts**	
Parameter	sfb.phone_lock_with_pc.enable	<y0000000000xx>.cfg
Description	It enables or disables your phone to be locked and unlocked automatically when you lock and unlock your computer. **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.	

Permitted Values	**0**-Disabled	
	1-Enabled	
Default	1	
Web UI	**Settings** > **Phone Lock** > **Phone Lock with PC**	
Phone UI	**Menu** > **Setting** > **Basic** > **Phone Lock** > **Phone Lock with PC**	
Parameter	**sfb.phone_lock.sign_out_auto.enable**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to be automatically signed out when you do not create a lock PIN within 5 minutes when prompted.	
Permitted Values	**0**-Disabled	
	1-Enabled	
Default	0	

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

Account Lock

You can lock your account to prevent your account from being signed in or signed out by someone else. If the 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 MP56/CP960/T58A/T56A/T55A Skype for Business phones.

- Account Lock Configuration

Account Lock Configuration

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

Parameter	**sfb.account_lock.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to lock the account to prevent the account from being signed in or signed out by someone else.	
	Note: It is not applicable to MP56/CP960/T58A/T56A/T55A Skype for Business phones.	
Permitted Values	**0**-Disabled	
	1-Enabled, the phone needs an administrator password to sign in or sign out.	
Default	0	
Web UI	**Account** > **Basic** > **Account Lock**	
Phone UI	**Menu** > **Setting** > **Advanced (default password: admin)** > **Account Lock**	

Transport Layer Security (TLS)

TLS is a commonly-used protocol that provides communications privacy and manages the security of message transmission, allowing the devices to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent eavesdropping and tampering.

Yealink devices support TLS 1.0, TLS 1.1, and TLS 1.2.

- Supported Cipher Suites
- Supported Trusted and Server Certificates
- TLS Configuration

Supported Cipher Suites

A cipher suite is a named combination of authentication, encryption, and message authentication code (MAC) algorithms used to negotiate the security settings for a network connection using the TLS/SSL network protocol.

Yealink devices support the following cipher suites:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- AES256-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- DES-CBC3-MD5
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- RC2-CBC-MD5
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- RC4-64-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- DES-CBC-MD5
- EXP1024-DHE-DSS-RC4-SHA
- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC2-CBC-MD5
- EXP-RC4-MD5

Supported Trusted and Server Certificates

The device can serve as a TLS client or a TLS server. In TLS feature, we use the terms trusted and the server certificate. These are also known as CA and device certificates.

The TLS requires the following security certificates to perform the TLS handshake:

- **Trusted Certificate**: When the device requests a TLS connection with a server, the device should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. You can upload 10 custom certificates at most. The format of the trusted certificate files must be *.pem,*.cer,*.crt, and *.der, and the maximum file size is 5MB.
- **Server Certificate**: When clients request a TLS connection with the device, the device sends the server certificate to the clients for authentication. The device 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 device. 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 device (based on the MAC address) and issued by the Yealink Certificate Authority (CA).
   - **A generic server certificate**: It is issued by the Yealink Certificate Authority (CA). Only if no unique certificate exists, the device may send a generic certificate for authentication.

The device 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 device accepts: default certificates, custom certificates, or all certificates.

Common Name Validation feature enables the device to mandatorily validate the common name of the certificate sent by the connecting server. The security verification rules are compliant with RFC 2818.

- Supported Trusted Certificates

Supported Trusted Certificates

Yealink Skype for Business devices 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 commonly 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 but is 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 device.

TLS Configuration

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

Parameter	static.security.trust_certificates[1]	<y0000000000xx>.cfg
Description	It enables or disables the device to only trust the server certificates listed in the Trusted Certificates list.	
Permitted Values	**0**-Disabled, the device will trust the server no matter whether the certificate sent by the server is valid or not. **1**-Enabled, the device will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, will the device trust the server.	
Default	1	
Web UI	**Security** > **Trusted Certificates** > **Only Accept Trusted Certificates**	
Parameter	static.security.ca_cert[1]	<y0000000000xx>.cfg

Description	It configures the type of certificates in the Trusted Certificates list for the device to authenticate for TLS connection.	
Permitted Values	**0**-Default Certificates **1**-Custom Certificates **2**-All Certificates	
Default	2	
Web UI	**Security** > **Trusted Certificates** > **CA Certificates**	
Parameter	**static.security.cn_validation**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the device to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Security** > **Trusted Certificates** > **Common Name Validation**	
Parameter	**static.trusted_certificates.url**	**<y0000000000xx>.cfg**
Description	It 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.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Security** > **Trusted Certificates** > **Load trusted certificates file**	
Parameter	**static.trusted_certificates.delete**	**<y0000000000xx>.cfg**
Description	It deletes all uploaded trusted certificates.	
Permitted Values	http://localhost/all	
Default	Blank	
Parameter	**static.security.dev_cert**[1]	**<y0000000000xx>.cfg**
Description	It configures the type of the device certificates for the device to send for TLS authentication.	
Permitted Values	**0**-Default Certificates **1**-Custom Certificates	
Default	0	
Web UI	**Security** > **Server Certificates** > **Device Certificates**	
Parameter	**static.server_certificates.url**	**<y0000000000xx>.cfg**

Description	It configures the access URL of the certificate the device sends for authentication.
	Note: The certificate you want to upload must be in *.pem or *.cer format.
Permitted Values	URL within 511 characters
Default	Blank
Web UI	**Security** > **Server Certificates** > **Load server cer file**
Parameter	**static.server_certificates.delete**	**<y0000000000xx>.cfg**
Description	It deletes all uploaded server certificates.
Permitted Values	http://localhost/all
Default	Blank
Parameter	**static.phone_setting.reserve_certs_enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the device to reserve custom certificates after it is reset to factory defaults.
Permitted Values	**0**-Disabled
	1-Enabled
Default	0

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

Encrypting Configuration Files

Yealink Skype for Business device can download encrypted files from the server and encrypt files before/when uploading them to the server.

You can encrypt the following configuration files: MAC-Oriented CFG file (<MAC>.cfg), Common CFG file (y0000000000xx.cfg), or other custom CFG files (for example, Teams.cfg, account.cfg)

To encrypt/decrypt files, you may have to configure an AES key.

> 📝 **Note:** AES keys must be 16 characters. The supported characters contain: 0 ~ 9, A ~ Z, a ~ z and special characters: # $ % * + , - . : = ? @ [ ] ^ _ { } ~.

- Configuration Files Encryption Tools
- Configuration Files Encryption and Decryption
- Encryption and Decryption Configuration
- Example: Encrypting Configuration Files

Configuration Files Encryption Tools

Yealink provides three encryption tools for configuration files:

- Config_Encrypt_Tool.exe (via graphical tool for Windows platform)
- Config_Encrypt.exe (via DOS command line for Windows platform)
- yealinkencrypt (for Linux platform)

The encryption tools encrypt plaintext configuration files (for example, account.cfg, <y0000000000xx>.cfg, <MAC>.cfg) (one by one or in batch) using 16-character symmetric keys (the same or different keys for configuration files) and generate encrypted configuration files with the same file name as before.

These tools also encrypt the plaintext 16-character symmetric keys using a fixed key, which is the same as the one built in the device, and generate new files named as <xx_Security>.enc (xx is the name of the configuration file, for example, y000000000058_Security.enc for y000000000058.cfg file, account_Security.enc for account.cfg). These tools generate another new file named as Aeskey.txt to store the plaintext 16-character symmetric keys for each configuration file.

Configuration Files Encryption and Decryption

Encrypted configuration files can be downloaded from the provisioning server to protect against unauthorized access and tampering of sensitive information (for example, login passwords, registration information).

For security reasons, you should upload encrypted configuration files, <xx_Security>.enc files to the root directory of the provisioning server. During auto provisioning, the device requests to download the boot file first and then download the referenced configuration files. For example, the device downloads an encrypted account.cfg file. The device will request to download <account_Security>.enc file (if enabled) and decrypt it into the plaintext key (for example, key2) using the built-in key (for example, key1). Then the device decrypts account.cfg file using key2. After decryption, the device resolves configuration files and updates configuration settings onto the device system.

Encryption and Decryption Configuration

The following table lists the parameters you can use to configure the encryption and decryption.

Parameter	static.auto_provision.update_file_mode	<y0000000000xx>.cfg
Description	It enables or disables the device only to download the encrypted files.	
Permitted Values	**0**-Disabled, the device will download the configuration files (for example, sip.cfg, account.cfg) from the server during auto provisioning no matter whether the files are encrypted or not. And then the device resolves these files and updates the settings onto the device system. **1**-Enabled, the device will only download the encrypted configuration files (for example, sip.cfg, account.cfg,) from the server during auto provisioning, and then resolve these files and update settings onto the device system.	
Default	0	
Parameter	static.auto_provision.aes_key_in_file	<y0000000000xx>.cfg
Description	It enables or disables the device to decrypt configuration files using the encrypted AES keys.	
Permitted Values	**0**-Disabled, the device will decrypt the encrypted configuration files using plaintext AES keys configured on the device. **1**-Enabled, the device 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 device built-in key (for example, key1). The device then decrypts the encrypted configuration files using corresponding key (for example, key2, key3).	
Default	0	
Parameter	static.auto_provision.aes_key_16.com	<y0000000000xx>.cfg

Description	It configures the plaintext AES key for encrypting/decrypting the Common CFG 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
Permitted Values	16 characters
Default	Blank
Web UI	**Settings** > **Auto Provision** > **Common AES Key**
Phone UI	**Menu** > **Setting** > **Advanced** > **Auto Provision** > **Common AES**
Parameter	**static.auto_provision.aes_key_16.mac**	**<y0000000000xx>.cfg**
Description	It configures the plaintext AES key for encrypting/decrypting the MAC-Oriented files (<MAC>.cfg, <MAC>-local.cfg and <MAC>-contact.xml).
	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
Permitted Values	16 characters
Default	Blank
Web UI	**Settings** > **Auto Provision** > **MAC-Oriented AES Key**
Phone UI	**Menu** > **Setting** > **Advanced** > **Auto Provision** > **MAC-Oriented AES**

Example: Encrypting Configuration Files

The following example describes how to use "Config_Encrypt_Tool.exe" to encrypt the account.cfg file.
For more information on the other two encryption tools, refer to Yealink Configuration Encryption Tool User Guide.

The way the device processes other configuration files is the same as that of the account.cfg file.

Procedure

1. Double click "Config_Encrypt_Tool.exe" to start the application tool.

    The screenshot of the main page is shown below:

2. When you start the application tool, a file folder named "Encrypted" is created automatically in the directory where the application tool is located.
3. Click **Browse** to locate configuration file(s) (for example, account.cfg) from your local system in the **Select File(s)** field.

    To select multiple configuration files, you can select the first file and then press and hold the **Ctrl** key and select other files.
4. (Optional.) Click **Browse** to locate the target directory from your local system in the **Target Directory** field.

    The tool uses the file folder "Encrypted" as the target directory by default.
5. (Optional.) Mark the desired radio box in the **AES Model** field.

    If you mark the **Manual** radio box, you can enter an AES KEY in the **AES KEY** field or click **Re-Generate** to generate an AES KEY in the **AES KEY** field. The configuration file(s) will be encrypted using the AES KEY in the **AES KEY** field.

    If you mark the **Auto Generate** radio box, the configuration file(s) will be encrypted using random **AES KEY**. The AES keys of configuration files are different.
6. Click **Encrypt** to encrypt the configuration file(s).

7. Click **OK**.

The target directory will be automatically opened. You can find the encrypted CFG file(s), encrypted key file(s) and an Aeskey.txt file storing plaintext AES key(s).
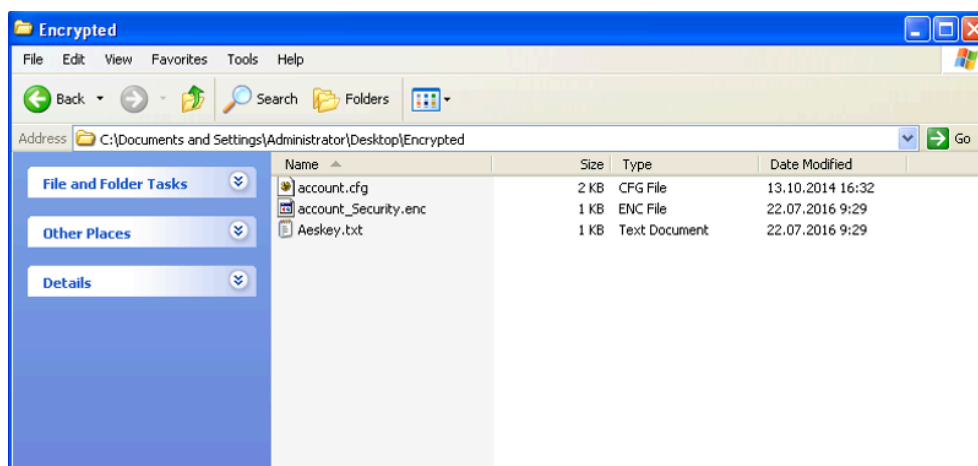
Troubleshooting Methods

Yealink Skype for Business devices provide feedback in a variety of forms such as log files, packets, status indicators and so on, which can help you more easily find the system problem and fix it.

- Log Files
- Packets Capture
- Watch Dog
- Analyzing Configuration Files
- Exporting All the Diagnostic Files
- Device Status
- Resetting Device and Configuration
- Device Reboot

Log Files

Yealink Skype for Business devices can log events into two different log files: boot log and system log. You can choose to generate the log files locally or sent to the syslog server in real time, and use these log files to generate informational, analytic, and troubleshoot devices.

- Local Log
- Syslog Log

Local Log

You can enable the local log, specify the severity level, and choose to keep the log locally or upload the local log files to the provisioning server. The local log files can be exported via the web user interface simultaneously.

- Local Log Configuration
- Exporting the Log Files to a Local PC
- Exporting the Log File to the Skype for Business Server

- Exporting the Log Files to a USB Flash Drive
- Viewing the Log Files

Local Log Configuration

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

Parameter	static.local_log.enable	<y0000000000xx>.cfg
Description	It enables or disables the device to record log locally. **Note**: We recommend you not to disable this feature.	
Permitted Values	**0**-Disabled, the device will stop recording log to the log files locally. The log files recorded before are still kept on the device. **1**-Enabled, the device will continue to record log to the log files locally. You can upload the local log files to the provisioning server or a specific server or export them to the local system.	
Default	1	
Web UI	**Settings** > **Configuration** > **Local Log Switch**	
Parameter	static.local_log.level	<y0000000000xx>.cfg
Description	It configures the lowest level of local log information to be rendered to the sys.log file. When you choose a log level, it includes all events of an equal or higher severity level and excludes events of a lower severity level. The logging level you choose determines the lowest severity of events to log.	
Permitted Values	**5**-Normal **6**-Debug	
Default	For T48S/T46S/T42S/T41S: 5 For MP56/CP960/T58A/T56A/T55A: 6	
Web UI	**Settings** > **Configuration** > **Local Log Level**	
Parameter	static.local_log.max_file_size	<y0000000000xx>.cfg
Description	It configures the maximum size (in KB) of the log files that can be stored on the device. 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 device will clear all the local log files on the device once successfully backing up. (2) If "static.auto_provision.local_log.backup.enable" is set to 0 (Disabled), the device will erase half of the logs from the oldest log information on the device.	
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 CP960/T48S) Integer from 2048kb to 20480kb (for MP56/T58A/T56A/T55A)	

Default	1024 kb for T46S/T42S/T41S
	5120 kb for CP960/T48S
	15360 kb for MP56/T58A/T56A/T55A
Web UI	**Settings** > **Configuration** > **Max Log File Size**

Parameter	**static.auto_provision.local_log.backup.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the device to upload the local log files to the provisioning server or a specific server.	
	Note: The upload path is configured by the parameter "static.auto_provision.local_log.backup.path".	
Permitted Values	**0**-Disabled	
	1-Enabled, the device 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 the maximum configured by the parameter "static.local_log.max_file_size";	
	- It's time to upload local log files according to the upload period configured by the parameter "static.auto_provision.local_log.backup.upload_period".	
Default	0	
Web UI	**Settings** > **Configuration** > **Enable log backup**	

Parameter	**static.auto_provision.local_log.backup.upload_period**	**<y0000000000xx>.cfg**
Description	It configures the period (in seconds) of the local log files uploads to the provisioning server or a specific server.	
	Note: It works only if "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled).	
Permitted Values	Integer from 30 to 86400	
Default	30	
Web UI	**Settings** > **Configuration** > **Log backup interval**	

Parameter	**static.auto_provision.local_log.backup.path**	**<y0000000000xx>.cfg**

Description	It configures the upload path of the local log files.
	If you leave it blank, the device will upload the local log files to the provisioning server.
	If you configure a relative URL (for example, /upload), the device 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 (for example, tftp), the device will upload the local log files using the desired protocol. If no protocol, the device 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 "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled).
Permitted Values	URL within 1024 characters
Default	Blank
Web UI	**Settings** > **Configuration** > **Backup Server URL**
Parameter	**static.auto_provision.local_log.backup.append** **<y0000000000xx>.cfg**
Description	It configures whether the uploaded local log files overwrite the existing files or are appended to the existing files.
Permitted Values	**0**-Overwrite
	1-Append (not applicable to TFTP Server)
Default	0
Web UI	**Settings** > **Configuration** > **Backup Mode**
Parameter	**static.auto_provision.local_log.backup.append.limit_mode** **<y0000000000xx>.cfg**
Description	It configures the behavior when local log files on the provisioning server or a specific server reach the maximum file size.
Permitted Values	**0**-Delete, the server will delete the old log and the phone will continue to uploading log.
	1-Stet, the phone will stop uploading log.
Default	0
Web UI	**Settings** > **Configuration** > **Backup limit mode**
Parameter	**static.auto_provision.local_log.backup.append.max_file_s** **<y0000000000xx>.cfg**
Description	It configures the maximum size (in KB) of the local log files can be stored on the provisioning server or a specific server.
Permitted Values	Integer from 200 to 65535
Default	1024
Web UI	**Settings** > **Configuration** > **Max size for backup log**
Parameter	static.auto_provision.local_log.backup.bootlog.upload_wait_tim **<y0000000000xx>.cfg**

Description	It configures the waiting time (in seconds) before the device uploads the local log file to the provisioning server or a specific server after startup.
Permitted Values	Integer from 1 to 86400
Default	120
Web UI	**Settings** > **Configuration** > **Bootlog backup time**

Exporting the Log Files to a Local PC

Procedure

1. From the web user interface, navigate to **Settings** > **Configuration**.
2. Select **Enabled** from the **Local Log Switch** drop-down menu.
3. Select **Debug** from the **Local Log Level** drop-down menu.

   The default local log level is **Normal**.
4. Enter the limit size of the log files in the **Max Log File Size** field.
5. Click **Confirm** to accept the change.
6. Reproduce the issue.
7. Click **Export** to open the file download window and save the file to your local system.

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 uploading a log, The HTTP POST sent from the 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:

- VendorName-phone manufacturer name
- DeviceModel-phone model
- Firmware version
- MAC address

Sample:

UCDevice_ID: Yealink_SIP-T46S_66.9.0.30_00156574B1D6E\r\n
UCDevice_Type: 3PIP\r\n

Procedure

1. Press **Menu** > **Setting** > **Basic** > **Log Upload**.
2. Press **Log 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.

Exporting the Log Files to a USB Flash Drive

You can upload your local log to the connected USB flash drive instead of your phone flash. The phone will automatically adjust the log level to the debug level and record the complete log.

The following table lists the parameters you can use to export the log files to the USB flash drive.

Parameter	static.phone_setting.logging_to_usb_drive.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to record local log messages to the connected USB flash drive. **Note**: It is not applicable to MP56/T58A/T56A/T55A Skype for Business phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Settings** > **Configuration** > **Logging to USB drive**	

Viewing the Log Files

You can verify whether you got the correct log through the following key fields:

- <0+emerg>
- <1+alert>
- <2+crit>
- <3+error>
- <4+warning>
- <5+notice>
- <6+info>

The following figure shows a portion of a boot log file:

```
     0........10........20........30........40........50.......60........70........80........90........100
 1 <46>Thu Jan  1 08:00:09 syslogd started: BusyBox v1.10.3
 2 <128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > cfg log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
 3 <128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > ANY =3
 4 <128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Version  :1.2.1.7 for release
 5 <128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Built-at :May 10 2018,21:55:14
 6 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
 7 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
 8 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
 9 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
10 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
11 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
12 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
13 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
14 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
15 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
16 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
17 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
18 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
19 <128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > TRS log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
20 <128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > Version  :1.0.0.6 for release
21 <128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > Built-at :Apr 20 2018,21:57:26
22 <128>Jan  1 08:00:11 cfg [316]: ANY <0+emerg > ANY =6
23 <133>Jan  1 08:00:11 cfg [316]: CFG <5+notice> cfgserver init done
24 <46>Thu Jan  1 08:00:12 syslogd started: BusyBox v1.10.3
25 <128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
26 <128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
27 <128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > Version  :8.0.1.3 for release
28 <128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > Built-at :Jul 30 2018,14:38:14
29 <128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
30 <132>Jan  1 08:00:12 sys [532]: SRV <4+warnin> wifi switch mode 1
31 <134>Jan  1 08:00:12 sys [532]: SRV <6+info  > running in nomal mode, mode 0
32 <134>Jan  1 08:00:12 sys [532]: SRV <6+info  > Set Init SystemTime: 2018-11-23
33 <134>Nov 23 00:00:00 sys [532]: SRV <6+info  > emac get: wan speed 0000003f, lan speed 0000003f
34 <134>Nov 23 00:00:00 sys [532]: SRV <6+info  > wan_support_speed 0000005f, lan_support_speed 0000005f
```

The following figure shows a portion of a sys log file (for example, 805EC031960A-sys.log):

```
          0         10        20        30        40        50        60        70        80        90        100
  1 <46>Thu Jan  1 08:00:09 syslogd started: BusyBox v1.10.3
  2 <128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > cfg log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
  3 <128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > ANY =3
  4 <128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Version   :1.2.1.7 for release
  5 <128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Built-at :May 10 2018,21:55:14
  6 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
  7 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
  8 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
  9 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
 10 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
 11 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
 12 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
 13 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
 14 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
 15 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
 16 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
 17 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
 18 <131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
 19 <128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > TRS log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
 20 <128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > Version   :1.0.0.6 for release
 21 <128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > Built-at :Apr 20 2018,21:57:26
 22 <128>Jan  1 08:00:11 cfg [316]: ANY <0+emerg > ANY =6
 23 <133>Jan  1 08:00:11 cfg [316]: CFG <5+notice> cfgserver init done
 24 <46>Thu Jan  1 08:00:12 syslogd started: BusyBox v1.10.3
 25 <128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
 26 <128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
 27 <128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > Version   :8.0.1.3 for release
 28 <128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > Built-at :Jul 30 2018,14:38:14
 29 <128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
 30 <132>Jan  1 08:00:12 sys [532]: SRV <4+warnin> wifi switch mode 1
 31 <134>Jan  1 08:00:12 sys [532]: SRV <6+info  > running in nomal mode, mode 0
 32 <134>Jan  1 08:00:12 sys [532]: SRV <6+info  > Set Init SystemTime: 2018-11-23
 33 <134>Nov 23 00:00:00 sys [532]: SRV <6+info  > emac get: wan speed 0000003f, lan speed 0000003f
 34 <134>Nov 23 00:00:00 sys [532]: SRV <6+info  > wan_support_speed 0000005f, lan_support_speed 0000005f
 35 <134>Nov 23 00:00:00 sys [532]: SRV <6+info  > set client
```

Syslog Log

You can also configure the device to send syslog messages to a syslog server in real time.

You can specify syslog details such as IP address or host name, server type, facility, and the severity level of events you want to log. You can also choose to prepend the device's MAC address to log messages.

- Syslog Logging Configuration
- BToE Logging Configuration
- Viewing the Syslog Messages on Your Syslog Server

Syslog Logging Configuration

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

Parameter	static.syslog.enable	<y0000000000xx>.cfg
Description	It enables or disables the device to upload log messages to the syslog server in real time.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Settings** > **Configuration** > **Syslog** > **Syslog Switch**	
Parameter	static.syslog.server	<y0000000000xx>.cfg
Description	It configures the IP address or domain name of the syslog server when exporting log to the syslog server.	
Permitted Values	IP address or domain name	
Default	Blank	
Web UI	**Settings** > **Configuration** > **Syslog** > **Syslog Server**	

Parameter	static.syslog.level	<y0000000000xx>.cfg
Description	It configures the lowest level of syslog information that displays in the syslog.	
Permitted Values	**5**-Normal **6**-Debug	
Default	6	
Web UI	**Settings** > **Configuration** > **Syslog** > **Syslog Level**	

BToE Logging Configuration

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

Parameter	static.phone_setting.logging_to_btoe.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to upload syslog messages to the paired PC using the BToE. The log files will be saved at the root directory of BToE on your computer.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Settings** > **Configuration** > **Logging to BToE**	

Viewing the Syslog Messages on Your Syslog Server

You can view the syslog file in the desired folder on the syslog server. The location of the folder may differ from the syslog server. For more information, refer to the network resources.

The following figure shows a portion of the syslog:

Packets Capture

You can capture packet in two ways: capturing the packets via web user interface or using the Ethernet software. You can analyze the captured packets for troubleshooting purposes.

- Capturing the Packets via Web User Interface
- Ethernet Software Capturing Configuration

Capturing the Packets via Web User Interface

For Yealink Skype for Business devices, you can export the packets file to the local system and analyze it.

Yealink Skype for Business devices support the following two modes for capturing the packets:

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

- Capturing the Packets in Normal Way
- Capturing the Packets in Enhanced Way

Capturing the Packets in Normal Way

Procedure

1. From the web user interface, navigate to **Settings** > **Configuration**.
2. In the **Pcap Feature** field, click **Start** to start capturing signal traffic.
3. Reproduce the issue to get stack traces.
4. Click **Stop** in the **Pcap Feature** field to stop capturing.
5. Click **Export** to open the file download window, and then save the file to your local system.
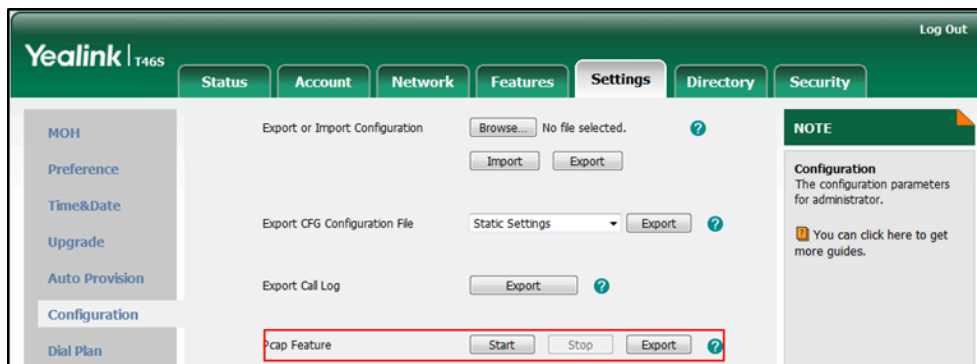
Capturing the Packets in Enhanced Way
If you capture packets in enhanced way, the packets file that include more message than the normal mode will be saved on PC directly. This way is not applicable to MP56/CP960/T58A/T56A/T55A Skype for Business phones.

Procedure

1. From the web user interface, navigate to **Settings** > **Configuration**.
2. Click **Start** in the **Enhanced Pcap Feature** field to start capturing signal traffic.
3. Reproduce the issue to get stack traces.
4. Click **Stop** in the **Enhanced Pcap Feature** field to stop capturing.

Ethernet Software Capturing Configuration

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

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

- Span to PC Port Configuration

Span to PC Port Configuration

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

Parameter	static.network.span_to_pc_port[1]	<y0000000000xx>.cfg
Description	It enables or disables the device to span data packets received from the WAN port to the PC port. **Note**: It works only if "static.network.pc_port.enable" is set to 1 (Auto Negotiation).	
Permitted Values	**0**-Disabled **1**-Enabled, all data packets from the Internet port can be received by PC port.	
Default	0	
Web UI	**Network** > **Advanced** > **Span to PC** > **Span to PC Port**	

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

Watch Dog

The Skype for Business phone provides a troubleshooting feature called "Watch Dog", which helps you monitor the phone status and 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.

- Watch Dog Configuration

Watch Dog Configuration

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

Parameter	static.watch_dog.enable[1]	<y0000000000xx>.cfg
Description	It enables or disables the Watch Dog feature.	
Permitted Values	**0**-Disabled **1**-Enabled, the phone will reboot automatically when the system crashed.	
Default	1	
Web UI	**Settings** > **Preference** > **Watch Dog**	

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

Analyzing Configuration Files

Wrong configurations may a poor impact on the device. You can export configuration file(s) to check the current configuration of the device and troubleshoot if necessary. You can also import configuration files for a quick and easy configuration.

We recommend you to edit the exported CFG file instead of the BIN file to change the device's current settings. The config.bin file is an encrypted file. For more information on the config.bin file, contact your Yealink reseller.

Exporting CFG Configuration Files from Phone

You can export the following CFG configuration files:

- **<MAC>-local.cfg**: It contains changes associated with non-static settings made via the phone user interface and web user interface. It can be exported only if "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 "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 "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.

Procedure

1. Click **Settings** > **Configuration**.
2. Select the desired CFG configuration file from the **Export CFG** > **Configuration File** drop-down menu.
3. Click **Export** to open the file download window, and then save the file to your local system.

Importing CFG Configuration Files to Phone

Procedure

1. From the web user interface, navigate to **Settings** > **Configuration**.
2. In the **Export or Import Configuration** block, click **Browse** to locate a CFG configuration file from your local system.
3. Click **Import** to import the configuration file.

Exporting BIN Files from the Device

Procedure

1. From the web user interface, navigate to **Settings** > **Configuration**.
2. In the **Export or Import Configuration** block, click **Export** to open the file download window, and then save the file to your local system.

Importing BIN Files from the Device

Procedure

1. From the web user interface, navigate to **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.

- BIN Files Import URL Configuration

BIN Files Import URL Configuration

The following table lists the parameter you can use to configure the BIN files import URL.

Parameter	static.configuration.url[1]	<y0000000000xx>.cfg
Description	It configures the access URL for the custom configuration files. **Note**: The file format of the custom configuration file must be *.bin.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Settings** > **Configuration** > **Export or Import Configuration**	

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

Exporting All the Diagnostic Files

Yealink devices support three types of diagnostic files (including Pcap trace, log files (boot.log and sys.log) and BIN configuration files) to help analyze your problem. You can export these files at a time and troubleshoot if necessary. The file format of the exported diagnostic file is *.tgz.

Procedure

1. From the web user interface, navigate to **Settings** > **Configuration**.
2. Click **Start** in the **Export All Diagnostic Files** field to begin capturing signal traffic.
   The system log level will be automatically set to 6.
3. Reproduce the issue.
4. Click **Stop** in the **Export All Diagnostic Files** field to stop the capture.
5. Click **Export** to open the file download window, and then save the diagnostic file to your local system.
   A diagnostic file named allconfig.tgz is successfully exported to your local system.

   > **Note:** After exporting the diagnostic files, you can create a ticket and describe your problem at ticket.yealink.com. After that Yealink support team will help you locate the root cause.

Device Status

Available information on device status includes:

- General information (IPv4 address or IPv6 address, phone MAC address, Machine ID, and firmware version).
- Network status (IPv4 status or IPv6 status, and IP mode).
- Device Certificate
- Device status (MAC address and device type)

- Viewing the Device Status

Viewing the Device Status

You can view device status via the phone user interface by navigating to **Menu** > **Status**. You can also view the device status via the web user interface.

Procedure

1. Open a web browser on your computer.
2. Enter the IP address in the browser's address bar and then press the **Enter** key.
   For example, "http://192.168.0.10" for IPv4 or "http://[2005:1:1:1:215:65ff:fe64:6e0a]" for IPv6.
3. Enter the user name (admin) and password (admin) in the login page.
4. Click **Confirm** to login.
   The device status is displayed on the first page of the web user interface.

Resetting Device and Configuration

Generally, some common issues may occur while using the device. You can reset your device to factory configurations after you have tried all troubleshooting suggestions, but still do not solve the problem. Resetting the device 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.

- Resetting the Device to Default Factory Settings
- Resetting the Device to Custom Factory Settings
- Deleting the Custom Factory Settings Files

Resetting the Device to Default Factory Settings

Procedure

1. From the web user interface, click **Settings** > **Upgrade**.
2. Click **Reset to Factory** in the **Reset to Factory** field.
   The web user interface prompts the message "Do you want to reset to factory?".
3. Click **OK** to confirm the resetting.
   The device will be reset to the factory successfully after startup.

   📝 **Note:** Reset of your device may take a few minutes. Do not power off until the device starts up successfully.

Resetting the Device to Custom Factory Settings

After you enable the custom factory feature, you can import the custom factory configuration file, and then reset the device to custom factory settings.

Procedure

1. From the web user interface, click **Settings** > **Configuration** > **Factory Configuration**.
2. In the **Import Factory Configuration** field, click the white box to select the custom factory configuration file from your local system.
3. Click **Import**.
   After the custom factory configuration file is imported successfully, you can reset the device to custom factory settings.

- Custom Factory Configuration

Custom Factory Configuration

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

Parameter	static.features.custom_factory_config.enable	<y0000000000xx>.cfg

Description	It enables or disables the Custom Factory Configuration feature.
Permitted Values	**0**-Disabled **1**-Enabled, **Import Factory Configuration** item will be displayed on the device's web user interface at the path **Settings** > **Configuration**. You can import a custom factory configuration file or delete the user-defined factory configuration via web user interface.
Default	0
Parameter	**static.custom_factory_configuration.url** `<y0000000000xx>.cfg`
Description	It configures the access URL of the custom factory configuration files. **Note**: It works only if "static.features.custom_factory_config.enable" is set to 1 (Enabled) and the file format of the custom factory configuration file must be *.bin.
Permitted Values	URL within 511 characters
Default	Blank
Web UI	**Settings** > **Configuration** > **Import Factory Configuration**

Deleting the Custom Factory Settings Files

You can delete the user-defined factory configurations via the web user interface.

Procedure

1. From the web user interface, click **Settings** > **Configuration** > **Factory Configuration**.
2. Click **Delete** from the **Delete Factory Configuration** field.
   The web user interface prompts the message "Are you sure delete user-defined factory configuration?".
3. Click **OK** to delete the custom factory configuration files.
   The imported custom factory file will be deleted. The device will be reset to default factory settings after resetting.

Device Reboot

You can reboot the device locally.

- Rebooting the Device via Phone User Interface
- Rebooting the Device via Web User Interface

Rebooting the Device via Phone User Interface

Procedure

1. Navigate to **Menu** > **Setting** > **Advanced**.
2. Select **Reboot**.
   It prompts if you are sure to reboot the device.
3. Select **OK**.

Rebooting the Device via Web User Interface

Procedure

1. Click **Settings** > **Upgrade**.
2. Click **Reboot** to reboot the device.
3. Click **OK** to confirm the rebooting.
   The device begins at rebooting. Any reboot of the device may take a few minutes.

Troubleshooting Solutions

This section describes the solutions to common issues that may occur while using the Skype for Business device. Upon encountering a case not listed in this section, contact your Yealink reseller for further support.

- IP Address Issues
- Time and Date Issues
- Display Issues
- Firmware and Upgrading Issues
- System Log Issues
- Password Issues

IP Address Issues

- The device does not get an IP address
- IP Conflict
- Specific format in configuring IPv6 on Yealink devices

The device does not get an IP address

Do one of the following:

- Ensure that the Ethernet cable is plugged into the Internet port on the device 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.

IP Conflict

Do one of the following:

- Reset another available IP address for the device.
- Check network configuration via the phone user interface at the path **Menu** > **Setting** > **Advanced** > **Network** > **WAN Port** > **IPv4 (or IPv6)**. If the Static IP is selected, select DHCP instead.

Specific format in configuring IPv6 on Yealink devices

Scenario 1:

If the device obtains the IPv6 address, the format of the URL to access the web user interface is "*[IPv6 address]" or "http(s)://[IPv6 address]*". For example, if the IPv6 address of your device is "fe80::204:13ff:fe30:10e", you can enter the URL (for example, "[fe80::204:13ff:fe30:10e]" or "http(s)://

[fe80::204:13ff:fe30:10e])" in the address bar of a web browser on your PC to access the web user interface.

Scenario 2:

Yealink devices support using FTP, TFTP, HTTP, and HTTPS protocols to download configuration files or resource files. You can use one of these protocols for provisioning.

When provisioning your device to obtain an IPv6 address, the provisioning server should support IPv6 and the format of the access URL of the provisioning server can be "*tftp://[IPv6 address or domain name]*". For example, if the provisioning server address is "2001:250:1801::1", the access URL of the provisioning server can be "tftp://[2001:250:1801::1]/". For more information on provisioning, refer to Yealink_Skype for Business_HD_IP_Phones_Auto_Provisioning_Guide.

Time and Date Issues

- Display time and date incorrectly

Display time and date incorrectly

Check if the device is configured to obtain the time and date from the NTP server automatically. If your device is unable to access the NTP server, configure the time and date manually.

Display Issues

- The device LCD screen blank

The device LCD screen blank

Do one of the following:

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

Firmware and Upgrading Issues

- Fail to upgrade the device firmware
- The device does not update the configurations

Fail to upgrade the device firmware

Do one of the following:

- Ensure that the target firmware is not the same as the current firmware.
- Ensure that the target firmware is applicable to the device model.
- Ensure that the current or the target firmware is not protected.
- Ensure that the power is on and the network is available during upgrading.
- Ensure that the web browser is not closed or refreshed when upgrading firmware via the web user interface.
- Ensure that the target firmware on the Skype for Business Server is available.

The device does not update the configurations

Do one of the following:

- Ensure that the configuration is set correctly.
- Reboot the device. Some configurations require a reboot to take effect.
- Ensure that the configuration is applicable to the device model.
- The configuration may depend on the support from a server.

System Log Issues

- Fail to export the system log from a syslog server

Fail to export the system log from a syslog server

Do one of the following:

- Ensure that the syslog server can save the syslog files exported from the device.
- Ensure that you have configured the syslog server address correctly via the web user interface on your device.
- Reboot the device. The configurations require a reboot to take effect.

Password Issues

- Restore the administrator password

Restore the administrator password

Factory reset can restore the default password. All custom settings will be overwritten after reset.