Yealink

Yealink Teams ® HD IP Phone Administrator Guide

Version 15.1 | Mar. 2021

Contents

Introduction.......... 7
Related Documentations.......... 7
Typographic and Writing Conventions.......... 7
Recommended References.......... 8
Summary of Changes.......... 8
    Change for Guide Version 15.1.......... 8

Getting Started.......... 9
Initialization Process Overview.......... 9
    Loading the ROM File.......... 9
    Configuring the VLAN.......... 9
    Querying the DHCP (Dynamic Host Configuration Protocol) Server.......... 9
    Contacting the Provisioning Server.......... 10
    Updating Firmware.......... 10
    Downloading the Resource Files.......... 10
Verifying Startup.......... 10
    NET Probe Configuration.......... 10
Teams Feature License.......... 11
    Importing License via the Web User Interface.......... 12
    Importing License Configuration.......... 12

Device Network.......... 12
IPv4 and IPv6 Network Settings.......... 13
    IP Addressing Mode Configuration.......... 13
    IPv4 Configuration.......... 13
    IPv6 Configuration.......... 16
DHCP Option for IPv4.......... 19
    Supported DHCP Option for IPv4.......... 19
    DHCP Option 160 and Option 161.......... 20
    DHCP Option 66, Option 43 and Custom Option.......... 20
    DHCP Option 42 and Option 2.......... 21
    DHCP Option 12.......... 21
    DHCP Option 60.......... 21
DHCP Option for IPv6.......... 22
    Supported DHCP Option for IPv6.......... 22
VLAN.......... 22
    LLDP Configuration.......... 23
    CDP Configuration.......... 23
    Manual VLAN Configuration.......... 24
    DHCP VLAN Configuration.......... 26
    VLAN Change Configuration.......... 27
Wi-Fi.......... 27
    Wi-Fi Configuration.......... 27
Internet Port and PC Port.......... 30
    Supported Transmission Methods.......... 30
    Internet Port and PC Port Configuration.......... 30
802.1x Authentication.......... 31

802.1x Authentication Configuration........32
Proxy Server........33
Proxy Server Configuration........33

Device Provisioning........37

Provisioning Points to Consider........37
Boot Files, Configuration Files, and Resource Files........37
Boot Files........37
Configuration Files........40
Resource Files........43
Files Download Process........43
Provisioning Methods........44
Provisioning Methods Priority........44
Manual Provisioning........45
Central Provisioning........48
Setting Up a Provisioning Server........50
Supported Provisioning Protocols........50
Supported Provisioning Server Discovery Methods........51
Configuring a Provisioning Server........52

Provisioning Devices on the Microsoft Teams Admin Center........53

Device Management........53
Editing Your Device Info........53
Customizing the Displayed Elements of Devices........54
Viewing the Device Details........54
Assigning Configuration Profile to Devices........54
Updating Device Software........54
Restarting Your Devices........55
Configuration Profiles Management........55
Creating a Configuration Profile........55
Editing a Configuration Profile........55
Remote Provisioning and Sign in from Teams Admin Center........56
Step 1: Add a Device MAC Address........56
Step 2: Generate a Verification Code........56
Step 3: Provisioning on the Device........56
Step 4: Sign in Remotely........57

Firmware Upgrade........57

Firmware for Each Device Model........57
Firmware Upgrade Configuration........58

Using CP960 Cascaded Mode........58

Guidelines for Configuring Cascaded Mode........59
CP960 Cascaded Mode Configuration........60
Example: Configuring CP960 Cascaded Mode........61

Device Customization........61

Language........62
Language Display Configuration........62
Language Customization........63
Example: Setting a Custom Language for Device Display........67

- Screen Saver 67
  - Screensaver Configuration 68
- Backlight 70
  - Backlight Brightness and Time Configuration 71
- Time and Date 71
  - Time Zone 72
  - NTP Settings 75
  - DST Settings 76
  - Time and Date Manual Configuration 80
  - Time and Date Format Configuration 80
- Tones 81
  - Supported Tones 82
  - Tones Configuration 82
- Volume 83
  - Volume Configuration 83
- Noise Suppression 84
  - Noise Suppression Configuration 84
- Smart Noise Block 84
  - Smart Noise Block Configuration 84
- Acoustic Shield 85
  - Acoustic Shield Configuration 85
- Power Saving 85
  - Power Saving Configuration 85
- Power LED Indicator 88
  - Power LED Indicator Configuration 88
- Bluetooth 89
  - Bluetooth Configuration 89

Common Area Phone 90

Call Features 90

- Call Queue 90
- Call Park and Retrieve 91

Security Features 91

- User and Administrator Identification 91
  - User and Administrator Identification Configuration 92
  - User Access Level Configuration 93
- Phone Lock 93
  - Phone Lock Configuration 94
- Transport Layer Security (TLS) 94
  - Supported Cipher Suites 95
  - Supported Trusted and Server Certificates 95
  - TLS Configuration 98
- Encrypting Configuration Files 100
  - Configuration Files Encryption Tools 100
  - Configuration Files Encryption and Decryption 100
  - Encryption and Decryption Configuration 100
  - Example: Encrypting Configuration Files 102

Hybrid Mode 103

- Hybrid Mode Configuration 104

Paging Configuration........ 105
SIP Account Registration Configuration........ 109
Account Codec Configuration........ 111
Local Directory Configuration........ 114

Device Management........ 115
Device Management Configuration........ 115

Managing the USB Camera UVC30 Room........ 115
Upgrading UVC30 Camera........ 116
Exporting Camera Log........ 116

Troubleshooting Methods........ 116
Log Files........ 116
    Local Log........ 117
    Syslog Log........ 121
Packets Capture........ 124
    Capturing the Packets via Web User Interface........ 124
    Ethernet Software Capturing Configuration........ 125
Analyzing Configuration Files........ 126
    Exporting BIN Files from the Device........ 126
    Importing BIN Files from the Device........ 126
Exporting All the Diagnostic Files........ 127
Device Status........ 127
    Viewing the Device Status........ 127
Resetting Device and Configuration........ 128
    Resetting the Device to Default Factory Settings........ 128
    Resetting the Device to Custom Factory Settings........ 128
    Deleting the Custom Factory Settings Files........ 129
Device Reboot........ 129
    Rebooting the Device via Phone User Interface........ 129
    Rebooting the Device via Web User Interface........ 130
Capturing the Current Screen of the Phone........ 130
    Enabling the Screen Capture via Phone User Interface........ 130
    Capturing the Current Screen of the Device via Web User Interface........ 130

Troubleshooting Solutions........ 131
IP Address Issues........ 131
    The device does not get an IP address........ 131
    IP Conflict........ 131
    Specific format in configuring IPv6 on Yealink devices........ 132
Time and Date Issues........ 132
    Display time and date incorrectly........ 132
Display Issues........ 132
    The device LCD screen blank........ 132
    The device displays “Offline”........ 132
Firmware and Upgrading Issues........ 133
    Fail to upgrade the device firmware........ 133
    The device does not update the configurations........ 133
System Log Issues........ 133
    Fail to export the system log from a provisioning server (FTP/TFTP server)........ 133
    Fail to export the system log from a syslog server........ 133

Password Issues....133
    Restore the administrator password....134

Introduction

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

Yealink MP58/MP58-WH/MP56/MP54/T58A/T56A/T55A/CP960/VP59 Microsoft Teams devices are the collaborative devices with Microsoft. As an administrator, you can do the following with this guide:

- Manage the Teams devices with Microsoft Teams & Skype for Business Admin Center.
- 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:

- T58A/T56A/T55A Teams IP phones: 58.15.0.124 or later
- CP960 Teams IP phones: 73.15.0.117 or later
- VP59 Teams IP phones: 91.15.0.58 or later
- MP58/MP58-WH/MP56/MP54 Teams IP phones: 122.15.0.36 or later

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

- Related Documentations
- Typographic and Writing Conventions
- Recommended References
- Summary of Changes

Related Documentations

The following related documents are available:

- Quick Start Guides, describe how to assemble 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 the boot file and configuration files.

  The *Auto Provisioning Guide* is to serve as a basic guidance for provisioning Yealink Teams devices with a provisioning server. If you are a novice, this guide is helpful for you.

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** > **Device Settings**. 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** > **Device Settings** indicates that you need to select **Device Settings** 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 T58A Teams phone as an example for reference. For more details on other Teams devices, refer to *Yealink Teamsdevice-specific user guide*.

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

Summary of Changes

- Change for Guide Version 15.1

Change for Guide Version 15.1

The following sections are new for this version:

- NET Probe Configuration
- Noise Suppression
- Smart Noise Block
- Acoustic Shield
- Remote Provisioning and Sign in from Teams Admin Center

Major updates have occurred to the following sections:

- Proxy Server Configuration

- User and Administrator Identification
- User and Administrator Identification Configuration
- Hybrid Mode Configuration
- TLS Configuration
- Using CP960 Cascaded Mode
- Provisioning Devices on the Microsoft Teams Admin Center

Getting Started

This chapter provides basic initialization instructions for Teams devices.

- Initialization Process Overview
- Verifying Startup
- Teams 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
- Default 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 boot file and 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 MP58/MP58-WH/MP56/MP54/T58A/T56A/T55A/VP59 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 devices enter the language selection interface.

- NET Probe Configuration

NET Probe Configuration

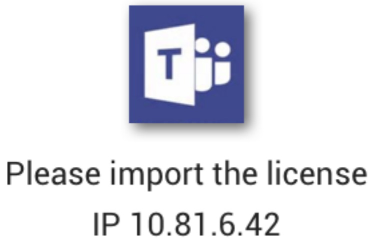
The following table lists the parameter you can use to detect network.

Parameter	**static.net.capportal.http.url**	**<y0000000000xx>.cfg**
Description	It configures the HTTP URL that detect the network connectivity. **Example**: *http://domain/generate_204*, *domain* is a complete domain name, such as www.g.cn.	
Permitted Values	String within 512 characters	
Default	http://www.g.cn/generate_204	
Parameter	**static.net.capportal.https.url**	**<y0000000000xx>.cfg**

Description	It configures the HTPPS URL that detect network connectivity. **Example**: *https://domain/generate_204*, *domain* is a complete domain name, such as www.g.cn.	
Permitted Values	String within 512 characters	
Default	http://www.g.cn/generate_204	
Parameter	**static.net.capportal.fallback.url**	**<y0000000000xx>.cfg**
Description	It configures the reserved http URL that detect network connectivity. **Example**: *http://domain/generate_204*, *domain* is a complete domain name, such as www.g.cn. **Note**: It can be set differently from "static.net.capportal.http.url".	
Permitted Values	String within 512 characters	
Default	http://www.g.cn/generate_204	

Teams Feature License

Yealink offers MP58/MP58-WH/MP56/MP54/T58A/T56A/T55A/CP960/VP59 devices configured for use with Microsoft Teams. By default, the device has a built-in Teams feature license, which allows users to use Yealink devices with Teams features directly. If the device has not imported a license yet, the screen will be shown as below:



Please import the license

IP 10.81.6.42

You need to upload the license to use the device normally.

For the Teams feature license and device version, you need to pay attention to the following points

- Any Open SIP build upgrades to Teams build will be required to apply and import the license.
- Any Teams upgrades to Skype for Business will not need to be required additional license. And vice versa.
- Any Teams will not be allowed to downgrade to the Open SIP from this release. If Teams phones are under temporary license (for demo testing purpose) and want to get back to Open SIP, please contact Yealink support team for technical support for an unlock license.
- Once upgraded to the latest Teams, it will not be allowed to downgrade to the previous Teams version.

For information about purchasing a Teams feature license, contact your reseller or sales representative.

Note: If the device running the Skype for Business firmware has been imported a Skype for Business feature license, you do not need to import the license after you upgrade to the Teams firmware.

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

Related information

Firmware Upgrade

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. In the **Load License File** (or **Upload License File**) block, click the white box 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 Teams 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 T58A Teams 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.

Device Network

Yealink Teams 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 Teams devices.

- IPv4 and IPv6 Network Settings
- DHCP Option for IPv4
- DHCP Option for IPv6

- VLAN
- Wi-Fi
- Internet Port and PC Port
- 802.1x Authentication
- Proxy Server

IPv4 and IPv6 Network Settings

Teams 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: Teams 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	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **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** > **Configuration Type**	
Phone UI	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **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** > **Configuration Type(Static IP)** > **IP Address**	
Phone UI	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **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** > **Configuration Type(Static IP)** > **Subnet Mask**	
Phone UI	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **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** > **Configuration Type(Static IP)** > **Default Gateway**	
Phone UI	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **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**	
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** > **Configuration Type(Static IP)** > **Primary DNS** Or **Network** > **Basic** > **IPv4 Config** > **Configuration Type(DHCP)** > **Static DNS(Enable)** > **Primary DNS**	
Phone UI	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **WAN Port** > **IPv4 Type(Static IP)** > **Pri.DNS** Or ≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **WAN Port** > **IPv4 Type(DHCP)** > **IPv4 Static DNS(Enable)** > **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** > **Configuration Type(Static IP)** > **Secondary DNS** Or **Network** > **Basic** > **IPv4 Config** > **Configuration Type(DHCP)** > **Static DNS(Enable)** > **Secondary DNS**
Phone UI	☰ > **Settings** > **Device Settings** > **Network (default password: admin)** > **WAN Port** > **IPv4 Type(Static IP)** > **Sec.DNS** Or ☰ > **Settings** > **Device Settings** > **Network (default password: admin)** > **WAN Port** > **IPv4 Type(DHCP)** > **IPv4 Static DNS(Enable)** > **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** > **Configuration Type**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network (default password: admin)** > **WAN Port** > **IPv6 Type**	
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** > **Configuration Type(Static IP)** > **IP Address**	

Phone UI	☰ > **Settings** > **Device Settings** > **Network (default password: admin)** > **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** > **Configuration Type(Static IP)** > **IPv6 Prefix(0~128)**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network (default password: admin)** > **WAN Port** > **IPv6 Type(Static IP)** > **IPv6 IP Prefix(0~128)**	
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** > **Configuration Type(Static IP)** > **Default Gateway**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network (default password: admin)** > **WAN Port** > **IPv6 Type(Static IP)** > **Default 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)**	
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** > **Configuration Type(Static IP)** > **Primary DNS** Or **Network** > **Basic** > **IPv6 Config** > **Configuration Type(DHCP)** > **Static DNS(Enable)** > **Primary DNS**	
Phone UI	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **WAN Port** > **IPv6 Type(Static IP)** > **Pri.DNS** Or ≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **WAN Port** > **IPv6 Type(DHCP)** > **IPv6 Static DNS(Enable)** > **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** > **Configuration Type(Static IP)** > **Secondary DNS** Or **Network** > **Basic** > **IPv6 Config** > **Configuration Type(DHCP)** > **Static DNS(Enable)** > **Secondary DNS**	
Phone UI	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **WAN Port** > **IPv6 Type(Static IP)** > **Sec.DNS** Or ≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **WAN Port** > **IPv6 Type(DHCP)** > **IPv6 Static DNS(Enable)** > **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 Teams 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

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	Identify the vendor-specific information.
Vendor Class Identifier	60	Identify the vendor type.
TFTP Server Name	66	Identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.

DHCP Option 160 and Option 161

Yealink Teams 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**	

[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 Teams 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 Teams 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 VP59: VP59 For MP54: MP54 For MP56: MP56 For MP58/MP58-WH: MP58	

[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 and functionality of a DHCP client. You can set the format for option 60. The default vendor class ID is “yealink”.

- 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	yealink	
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 for IPv6

The Teams device can obtain IPv6-related parameters in an IPv6 network via the DHCP option.

- Supported DHCP Option for IPv6

Supported DHCP Option for IPv6

The following table lists common DHCP options for IPv6 supported by Yealink Teams devices.

Parameters	DHCP Option	Description
DNS Server	23	Specify a list of DNS servers available to the client.
DNS Domain Search List	24	Specify a domain search list to a client.
SNTP Server	31	Specify a list of Simple Network Time Protocol (SNTP) servers available to the client.
Information Refresh Time	32	Specify an upper bound for how long a client should wait before refreshing information retrieved from DHCPv6.

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
- VLAN Change 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	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **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	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **LLDP** > **LLDP 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	☰ > **Settings** > **Device Settings** > **Network (default password: admin)** > **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	☰ > **Settings** > **Device Settings** > **Network (default password: admin)** > **CDP** > **CDP 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	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **VLAN** > **WAN Port**	
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	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **VLAN** > **WAN Port** > **VID**	
Parameter	**static.network.vlan.internet_port_priority**[1]	**<y0000000000xx>.cfg**
Description	It configures the VLAN priority for the Internet port. 7 is the highest priority, 0 is the lowest priority. **Note**: It works only if “static.network.vlan.internet_port_enable” is set to 1 (Enabled).	
Permitted Values	Integer from 0 to 7	
Default	1	
Web UI	**Network** > **Advanced** > **VLAN** > **WAN Port** > **Priority**	
Phone UI	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **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	≡ > **Settings** > **Device Settings** > **Network (default password: admin)** > **VLAN** > **PC Port**	
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	☰ > **Settings** > **Device Settings** > **Network (default password: admin)** > **VLAN** > **PC Port** > **VID**	
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	☰ > **Settings** > **Device Settings** > **Network (default password: admin)** > **VLAN** > **PC Port** > **Priority**	

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

DHCP VLAN Configuration

Yealink Teams 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	☰ > **Settings** > **Device Settings** > **Network (default password: admin)** > **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	☰ > **Settings** > **Device Settings** > **Network (default password: admin)** > **DHCP VLAN** > **Option**	

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

VLAN Change Configuration

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

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

[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.

Note: For T56A/T55A/MP54, make sure the Wi-Fi USB Dongle WF50 is connected to the device.

- 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.	
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 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)**	
Phone UI	☰ > **Settings** > **Device Settings** > **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	
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	
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	
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	NONE, WEP, WPA/WPA2 PSK, 802.1x EAP	
Default	NONE	

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

[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 Teams 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 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**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(default password: admin)** > **PC Port**	
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 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	
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.

802.1x Authentication

Yealink Teams IP Phones support the following protocols for 802.1X authentication:

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

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

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	☰ > **Settings** > **Device Settings** > **Network(default password: admin)** > **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	☰ > **Settings** > **Device Settings** > **Network(default password: admin)** > **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	☰ > **Settings** > **Device Settings** > **Network(default password: admin)** > **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.

Proxy Server

You can configure your network to use proxy servers.

- Proxy Server Configuration

Proxy Server Configuration

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

Parameter	**static.network.proxy.mode**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the proxy server.	
Permitted Values	**0**-Disabled **1**-Global proxy, you can manually configure the proxy server information. **2**-HTTP(S) proxy, you can obtain proxy server information through PAC file.	
Default	2	
Web UI	**Network** > **Proxy** > **Proxy**	
Phone UI	☰ > **Settings** > **Device Settings** > **Proxy (default password: admin)** > **Proxy**	
Parameter	**static.network.proxy.type**	**<y0000000000xx>.cfg**

Description	It configures the proxy type. **Note**: It works only if "static.network.proxy.mode" is set to 1 (Enabled).	
Permitted Values	**0**-SOCKS5 **1**-HTTP CONNECT	
Web UI	**Network** > **Proxy** > **Proxy** > **Proxy Type**	
Phone UI	☰ > **Settings** > **Device Settings** > **Proxy (default password: admin)** > **Proxy** > **Proxy Type**	
Default	0	
Parameter	**static.network.proxy.hostname**	**<y0000000000xx>.cfg**
Description	It configures the IP address or domain name of the proxy server. **Note**: It works only if "static.network.proxy.mode" is set to 1 (Enabled).	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	**Network** > **Proxy** > **Proxy** > **Proxy Hostname**	
Phone UI	☰ > **Settings** > **Device Settings** > **Proxy (default password: admin)** > **Proxy** > **Proxy hostname**	
Parameter	**static.network.proxy.port**[1]	**<y0000000000xx>.cfg**
Description	It configures the port of the proxy server. **Note**: It works only if "static.network.proxy.mode" is set to 1 (Enabled).	
Permitted Values	Integer from 1 to 65535	
Default	Blank	
Web UI	**Network** > **Proxy** > **Proxy** > **Proxy Port** (only for wired network)	
Phone UI	☰ > **Settings** > **Device Settings** > **Proxy (default password: admin)** > **Proxy** > **Proxy port**	
Parameter	**static.network.proxy.bypass_address**	**<y0000000000xx>.cfg**
Description	It configures the host name or IP address that does not apply to the proxy server to access. Multiple host names or IP addresses are seperated by commas. **Note**: It works only if "static.network.proxy.mode" is set to 1 (Enabled).	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Network** > **Proxy** > **Proxy** > **Bypass Proxy For** (only for wired network)	
Phone UI	☰ > **Settings** > **Device Settings** > **Proxy (default password: admin)** > **Proxy** > **Bypass proxy for**	
Parameter	**static.network.proxy.test_addres**	**<y0000000000xx>.cfg**

Description	It configures the test URL for the proxy server. After connecting to the proxy server, the phones try to send a network request to the specified URL. If the URL cannot be accessed, the phone fails to connect to the proxy server. **Note**: It works only if "static.network.proxy.mode" is set to 1 (Enabled).	
Permitted Values	URL within 511 characters	
Default	https://www.google.com	
Web UI	**Network** > **Proxy** > **Proxy** > **Domain Name For Testing** (only for wired network)	
Phone UI	☰ > **Settings** > **Device Settings** > **Proxy (default password: admin)** > **Proxy** > **Proxy domain name to test proxy configurations**	
Parameter	**static.network.proxy.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the proxy server authentication. **Note**: It works only if "static.network.proxy.mode" is set to 1 (Enabled).	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Network** > **Proxy** > **Enable Athentication**	
Phone UI	☰ > **Settings** > **Device Settings** > **Proxy (default password: admin)** > **Enable authentication**	
Parameter	**static.network.proxy_pac.url**	**<y0000000000xx>.cfg**
Description	It configures the URL for the PAC file location. **Note**: It works only if "static.network.proxy.mode" is set to 2 (Enabled), "static.network.proxy.wpad" is set to 1 (Disabled) and "static.network.proxy.http.set_from" is set to 1.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Network** > **Proxy** > **Proxy** > **WPAD** > **Proxy Set From** > **PAC URL**	
Phone UI	☰ > **Settings** > **Device Settings** > **Proxy (default password: admin)** > **Proxy** > **WPAD** > **Set From** > **PAC_URL**	
Parameter	**static.network.proxy.wpad**	**<y0000000000xx>.cfg**
Description	It enables or disables the WPAD to obtain the PAC file dynamically. **Note**: It works only if "static.network.proxy.mode" is set to 2 (Enabled).	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Network** > **Proxy** > **Proxy** > **WPAD**	

Phone UI	≡ > **Settings** > **Device Settings** > **Proxy (default password: admin)** > **Proxy** > **WPAD**	
Parameter	**static.network.proxy.http.set_from**	**<y0000000000xx>.cfg**
Description	It configures the sources where the proxy set comes. **Note**: It works only if "static.network.proxy.mode" is set to 2 (Enabled) and "static.network.proxy.wpad" is set to 1 (Disabled).	
Permitted Values	**0**-IP: Port, enter the IP address and port manually. **1**-PAC URL, enter the PAC URL manually. **2**-PAC File, upload PAC file directly.	
Default	0	
Web UI	**Network** > **Proxy** > **Proxy** > **WPAD** > **Proxy Set From**	
Phone UI	≡ > **Settings** > **Device Settings** > **Proxy (default password: admin)** > **Proxy** > **WPAD** > **Set From**	
Parameter	**static.network.proxy.username**[1]	**<y0000000000xx>.cfg**
Description	It configures the username for proxy server authentication.	
Permitted Values	String within 256 characters	
Default	Blank	
Web UI	**Network** > **Proxy** > **Proxy Username** (only for wired network)	
Phone UI	≡ > **Settings** > **Device Settings** > **Proxy (default password: admin)** > **Proxy username**	
Parameter	**static.network.proxy.password**[1]	**<y0000000000xx>.cfg**
Description	It configures the password for proxy server authentication.	
Permitted Values	String within 256 characters	
Default	Blank	
Web UI	**Network** > **Proxy** > **Proxy Password** (only for wired network)	
Phone UI	≡ > **Settings** > **Device Settings** > **Proxy (default password: admin)** > **Proxy password**	
Parameter	**static.network.proxy.sip.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables all communications including SIP to use a proxy server.	
Permitted Values	**0**-Disabled, SIP UDP and outbound do not use proxy server. **1**-Enabled	
Default	0	

[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 Teams HD IP Phones Auto Provisioning Guide.

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

Provisioning Points to Consider

You can deploy your devices on the Microsoft Teams & Skype for Business Admin Center or using a provisioning server.

- Provisioning devices on the Microsoft Teams & Skype for Business Admin Center, which allows you to efficiently realize centralized management for devices within the enterprise.
- If there is a provisioning server on your environment, and you want to deploy a mass of devices, we recommend you to use the central provisioning method as your primary configuration method. A provisioning server maximizes the flexibility when you install, configure, upgrade and manage the devices, and enables you to store the configuration on the server. You can set up a provisioning server on the local area network (LAN) or anywhere on the Internet.

Related information

Provisioning Devices on the Microsoft Teams & Skype for Business Admin Center

Boot Files, Configuration Files, and Resource Files

You can use boot files, 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.

- Boot Files
- Configuration Files
- Resource Files
- Files Download Process

Boot Files

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

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

- For all devices
- For a group of devices
- For specific device models
- For a single device

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

Note: You can select whether to use the boot file or not according to your deployment scenario. If you do not want to use the boot file, please go to Configuration Files.

- Common Boot File
- MAC-Oriented Boot File
- Boot File Attributes
- Customizing a Boot File

Common Boot File

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

MAC-Oriented Boot File

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

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

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

Boot File Attributes

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

Attributes	Description
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
include:config <xxx.cfg> include:config "xxx.cfg"	Each “include” statement can specify a location of a configuration file. The configuration file format must be *.cfg. The locations in the angle brackets or double quotation marks support two forms: • Relative path (relative to the boot file): For example, sip.cfg, HTTP Directory/sip.cfg • Absolute path (or URL): For example, http://10.2.5.258/Teams.cfg The location must point to a specific CFG file.
[$MODEL]	The [$MODEL] can be added to specify settings for specific phone models. $MODEL represents the phone model name. The valid device model names are: MP58, MP56, MP54, T58A, T56A, T55A, CP960 and VP59. Multiple device models are separated by commas. For example, [T58A, T56A].

Attributes	Description
overwrite_mode	Enable or disable the overwrite mode. The overwrite mode applies to the configuration files specified in the boot file. Note that it only affects the parameters pre-provisioned via central provisioning. **1-(Enabled)** - If the value of a parameter in the configuration files is left blank, or if a non-static parameter in the configuration files is deleted or commented out, the factory default value takes effect. **0-(Disabled)** -If the value of a parameter in the configuration files is left blank, deleted or commented out, the pre-configured value is kept. **Note**: Overwrite mode can only be used in boot files. If a boot file is used, but the value of the parameter “overwrite_mode” is not configured, the overwrite mode is enabled by default.
specific_model.excluded_mode	Enable or disable the exclude mode. The exclude mode applies to the configuration files specified in the boot file. **0-Disabled** (**Append Mode**), the device downloads its own model-specific configuration files and downloads other model-unspecified configuration files. **1-Enabled** (**Exclude Mode**), the device attempts to download its own model-specific configuration files; if there are no own model-specific configuration files found on the server, it downloads model-unspecified configuration files. **Note**: Exclude mode can only be used in boot files. If a boot file is used but the value of the parameter “specific_model.excluded_mode” is not configured, the exclude mode is disabled by default.

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

Customizing a Boot File

Procedure

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

   For example:

   - include:config <configure/Teams.cfg>
   - include:config “http://10.2.5.206/configure/account.cfg”
4. To specify configuration files for specific phone models, add specific phone modelsin front of *include:config <>* or *include:config “”*. Multiple phone model names are separated by commas.

   For example:

   - [T58A, CP960]include:config <configure/Teams.cfg>
   - [T56A]include:config “http://10.2.5.206/configure/account.cfg”
   - ## file *Teams.cfg* only applies to T58A and CP960 phones, file *account.cfg* only applies to T56A phones

5. Specify the overwrite mode and exclude mode.

   For example:

   - overwrite_mode = 1
   - specific_model.excluded_mode = 1
6. Save the boot file and place it on the provisioning server.

Related information

Boot File Attributes

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 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
VP59	y000000000091.cfg
MP58/MP58-WH	y000000000135.cfg
MP56	y000000000122.cfg
MP54	y000000000134.cfg

MAC CFG File

Yealink devices support two MAC CFG file: MAC-Oriented file and MAC-local CFG file, which are both named after the MAC address of the device. For example, if the MAC address of a device is 00156574B150, the name of MAC-Oriented CFG file is 00156574b150.cfg (lowercase), and the name of MAC-local CFG file is 00156574b150-local.cfg (lowercase).

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

- MAC-Oriented CFG File
- MAC-local CFG File

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 > central provisioning > factory defaults) takes effect only if the value of this parameter is set to 1 (Enabled). If "overwrite_mode" is set to 1 in the boot file, the value of this parameter will be set to 1 (Enabled).	
Permitted Values	**0**-Disabled **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	1	

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: ☰ > **Settings** > **Device Settings** > **Debug(default password: admin)** > **Reset user settings**.
- Via web user interface at the path: **Settings** > **Upgrade** > **Reset User Settings**.

Note: The **Reset user 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, Teams.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, Teams.cfg.
2. Rearrange the parameters in the Teams.cfg, and set the valid values for them.

   For example:

   phone_setting.phone_lock.enable= 1
3. To specify the parameters for specific phone models, add specific phone models in the front of the corresponding parameters. The names of different phone models are separated by commas.

   For example:

   [T58A,CP960]phone_setting.phone_lock.enable= 1

   [T58A]features.bluetooth_enable= 1

   ## These parameters only apply to their own specific phone models.
4. 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

Attributes	Description
[$MODEL]	The [$MODEL] can be added in front of configuration parameter to specify the value for specific device models. $MODEL represents the phone model. The valid device model names are: MP58, MP56, MP54, T58A, T56A, T55A, CP960 and VP59. Multiple phone models are separated by commas. For example, [T58A, CP960]. **Note**: The device updates model-specific configurations and those model-unspecified configurations.

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

Resource Files

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

- Supported Resource Files

Supported Resource Files

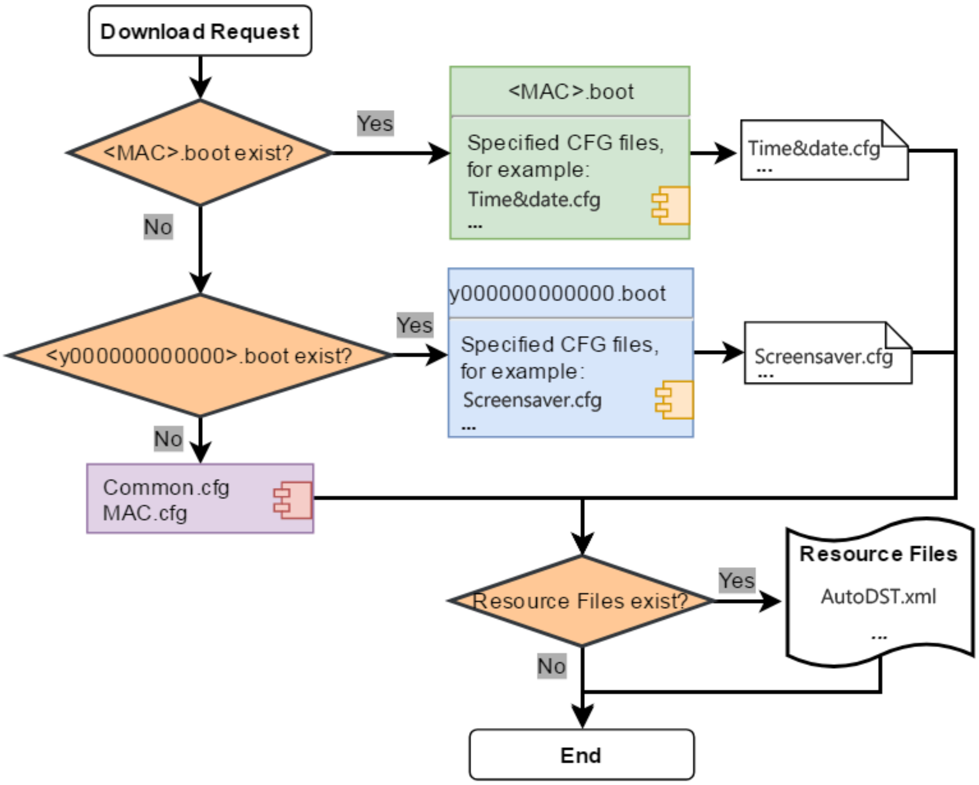
Yealink supplies some template of resource files for you, so you can directly edit the files as required.

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

Files Download Process

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


Download Request
<MAC>.boot exist?
Yes
No
<MAC>.boot
Specified CFG files, for example:
Time&date.cfg
...
Time&date.cfg
...
<y000000000000>.boot exist?
Yes
No
y000000000000.boot
Specified CFG files, for example:
Screensaver.cfg
...
Screensaver.cfg
...
Common.cfg
MAC.cfg
Resource Files exist?
Yes
No
Resource Files
AutoDST.xml
...
End

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

Note: The parameter “specific_model.excluded_mode” determines which configuration files referenced in the boot file to be downloaded.

Provisioning Methods

Teams devices can be configured using the following methods with your provisioning server:

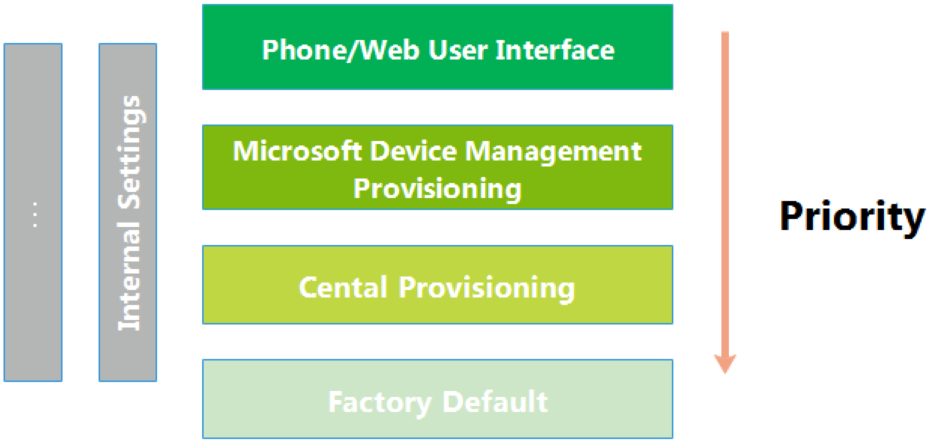
- **Central Provisioning**: configuration files stored on a central provisioning server.
- **Manual Provisioning:** operations on the web user interface or phone user interface.

- Provisioning Methods Priority
- Manual Provisioning
- Central 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: The provisioning priority mechanism takes effect only if “static.auto_provision.custom.protect” is set to 1. For more information on this parameter, refer to MAC-local CFG File Configuration.

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

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

Related information

Provisioning Devices on the Microsoft Teams & Skype for Business Admin Center

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. Go to ☰ > **Settings** > **Device Settings** > **About**.
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 **Login**.

Web Server Type Configuration

Yealink Teams 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	≡ > **Settings** > **Device Settings** > **Network(default password: admin)** > **Web Server** > **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	≡ > **Settings** > **Device Settings** > **Network(default password: admin)** > **Web Server** > **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	≡ > **Settings** > **Device Settings** > **Network(default password: admin)** > **Web Server** > **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	≡ > **Settings** > **Device Settings** > **Network(default password: admin)** > **Web Server** > **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, go to **Settings** > **Configuration** > **CFG Configuration**.
2. In the **Import CFG Configuration File** block, click the white box 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 five 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>-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, go to **Settings** > **Configuration** > **CFG 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

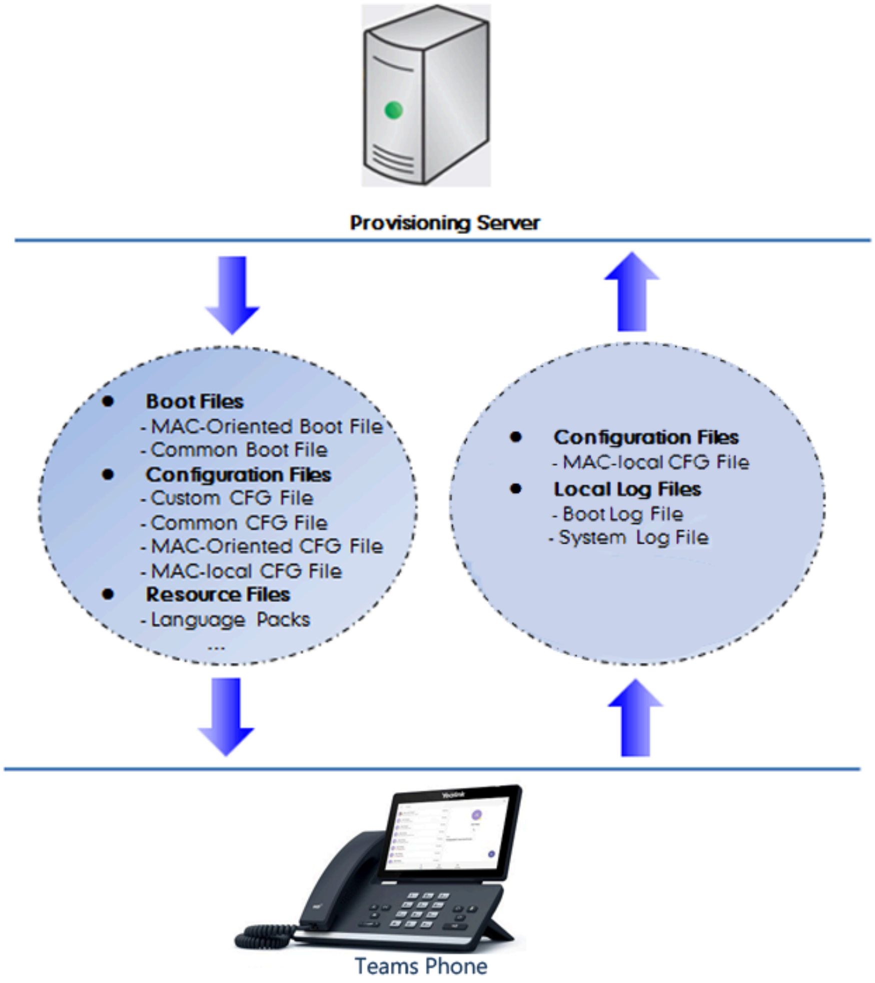
Phone user interface makes configurations available to users and administrators, but the ☰ > **Settings** > **Device Settings** > **Admin only** option is only available to administrators and requires an administrator password (default: admin).

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:


Provisioning Server
Boot Files
- MAC-Oriented Boot File
- Common Boot File
Configuration Files
- Custom CFG File
- Common CFG File
- MAC-Oriented CFG File
- MAC-local CFG File
Resource Files
- Language Packs
...
Configuration Files
- MAC-local CFG File
Local Log Files
- Boot Log File
- System Log File
Teams Phone

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. Teams devices can be centrally provisioned from a provisioning server. For more information on the provisioning server, refer to Setting Up a Provisioning Server.

Teams 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 Teams HD IP Phones Auto Provisioning Guide*.

- Auto 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.

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 boot files and configuration files, and then edit them as desired.
5. Copy the boot files, configuration files, and resource files to the provisioning server.
6. If performing static provisioning, obtain the provisioning server address.

Tip: Typically, all 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.

Provisioning Devices on the Microsoft Teams Admin Center

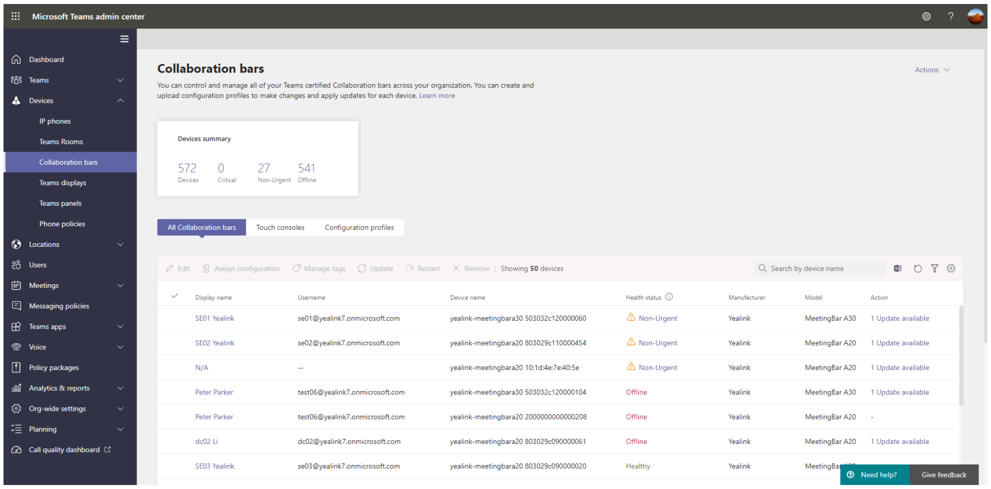
Microsoft Teams Admin Center allows administrators to efficiently realize centralized management for Yealink Teams devices. With the device management platform, you can customize configuration profiles and update all of your devices that are used.

Note: You can only manage the devices that login with the online accounts which has opened Microsoft Teams Admin Center services.

- Device Management
- Configuration Profiles Management
- Remote Provisioning and Sign in from Teams Admin Center

Device Management

You can monitor and manage your devices directly on the Microsoft Teams Admin Center.


Microsoft Teams admin center
Dashboard
Teams
Devices
IP phones
Teams Rooms
Collaboration bars
Teams displays
Teams panels
Phone policies
Locations
Users
Meetings
Messaging policies
Teams apps
Voice
Policy packages
Analytics & reports
Org-wide settings
Planning
Call quality dashboard
Actions
All Collaboration bars
Touch consoles
Configuration profiles
Edit
Assign configuration
Manage tags
Update
Restart
Remove
Search by device name
Need help?
Give feedback

Collaboration bars

You can control and manage all of your Teams certified Collaboration bars across your organization. You can create and upload configuration profiles to make changes and apply updates for each device. Learn more

Devices summary

572	0	27	541
Devices	Critical	Non-Urgent	Offline

Showing **50** devices

Display name	Username	Device name	Health status	Manufacturer	Model	Action
SE01 Yealink	se01@yealink7.onmicrosoft.com	yealink-meetingbara30 503032c120000060	⚠ Non-Urgent	Yealink	MeetingBar A30	1 Update available
SE02 Yealink	se02@yealink7.onmicrosoft.com	yealink-meetingbara20 803029c110000454	⚠ Non-Urgent	Yealink	MeetingBar A20	1 Update available
N/A	--	yealink-meetingbara20 10:1d:4e:7e:40:5e	⚠ Non-Urgent	Yealink	MeetingBar A20	1 Update available
Peter Parker	test06@yealink7.onmicrosoft.com	yealink-meetingbara30 503032c120000104	Offline	Yealink	MeetingBar A30	1 Update available
Peter Parker	test06@yealink7.onmicrosoft.com	yealink-meetingbara20 2000000000000208	Offline	Yealink	MeetingBar A20	-
dc02 Li	dc02@yealink7.onmicrosoft.com	yealink-meetingbara20 803029c090000061	Offline	Yealink	MeetingBar A20	1 Update available
SE03 Yealink	se03@yealink7.onmicrosoft.com	yealink-meetingbara20 803029c090000020	Healthy	Yealink	MeetingBar	

- Editing Your Device Info
- Customizing the Displayed Elements of Devices
- Viewing the Device Details
- Assigning Configuration Profile to Devices
- Updating Device Software
- Restarting Your Devices

Editing Your Device Info

You can edit the device name, organization asset tag, or add notes for the device. Note that you can only edit one device at a time.

Procedure

1. Select **Devices**.
2. Select a desired classification of devices.
3. Click a desired device in the **All xxx** list.
4. Click **Edit** at the top left of the device list.
5. Edit device info from the right side of the pop-up menu.

6. Click **Apply**.

Customizing the Displayed Elements of Devices

You can customize your table elements displayed in the device list.

Procedure

1. Select **Devices**.
2. Select a desired classification of devices.
3. Click ⚙at the top-right of the device list.
4. Turn on or turn off the table elements.
5. Click **Apply**.

Viewing the Device Details

You can view the device basic information, update information, software update status, and actions you performed.

Procedure

1. Select **Devices**.
2. Select a desired classification of devices.
3. Click the corresponding display name in the **All xxx** list to enter the device details page.

   You can click **Details** to view software update status or click **History** to view actions you performed for the device.

Assigning Configuration Profile to Devices

Before assigning configuration profile to devices, make sure there are configuration profiles on the platform.

Procedure

1. Select **Devices**.
2. Select a desired classification of devices.
3. Click desired devices in the **All xxx** list.
4. Click **Assign configuration** at the top left of the device list.
5. Search for the configuration profile from the right side of the pop-up menu.
6. Click **Apply**.
   The configuration profile will take effect on the devices.

Updating Device Software

You can update all software for your devices to the latest version with one click on the Microsoft Teams Admin Center.

About this task
All software on the selected devices will be updated.

Procedure

1. Select **Devices**.
2. Select a desired classification of devices.
3. Click desired devices in the **All xxx** list.

4. Click **Update** at the top of the device list.
5. Select **Firmware auto-update** or **Manual updates** from the right side of the pop-up menu.
6. Click **Update**.
   The current firmware of the devices will be updated automatically after a few minutes.

Restarting Your Devices

Procedure

1. Select **Devices**.
2. Select a desired classification of devices.
3. Click desired devices in the **All xxx** list.
4. Click **Restart** at the top of the device list.

   It will prompt "The selected device will be restarted. Restart puts devices temporarily out of reach. To restart later, you can select to schedule the restart at a preferred date and time and then Confirm."
5. Click **Restart now**.
   The devices will be restarted.

Configuration Profiles Management

You can configure the devices by using configuration profiles. Configuration profiles provide general settings, device settings, and network settings to manage devices. This makes it easy to realize centralized device deployment. All configurations are sent to devices according to the profiles deployment configuration. The configuration not supported by the device will not be pushed to the device.

Note: For the language settings, only English(United States), Chinese_S(Simplified, PRC), Chinese_T(Traditional, Taiwan), French(France), German, Italian, Polish, Portuguese(Portugal), Spanish, Turkish, Russian, Netherlands and Japanese are supported by the device. The language configuration does not take effect when you select other languages.

- Creating a Configuration Profile
- Editing a Configuration Profile

Related information

Language

Creating a Configuration Profile

Procedure

1. Select **Devices**.
2. Select a desired classification of devices and select **Configuration profiles**.
3. Click **Add** at the top left of the configuration profiles list.
4. Edit the configuration profile name and description.
5. Configure the general settings, device settings, or network settings.

   If you enable the phone lock feature for the device, the user cannot disable it.
6. Click **Save**.

Editing a Configuration Profile

You can edit the name, description, and configurations of the configuration file.

Procedure

1. Select **Devices**.
2. Select a desired classification of devices and select **Configuration profiles**.
3. Click a desired configuration file in the **Configuration file** list.
4. Click **Edit** at the top left of the configuration profiles list.
5. Edit the configuration profile.
6. Click **Save**.

Remote Provisioning and Sign in from Teams Admin Center

IT admins can remotely provision and sign in to a Teams device. To provision a device remotely, the admin needs to upload the MAC IDs of the devices being provisioned and create a verification code. The entire process can be completed remotely from the Teams admin center.

- Step 1: Add a Device MAC Address
- Step 2: Generate a Verification Code
- Step 3: Provisioning on the Device
- Step 4: Sign in Remotely

Step 1: Add a Device MAC Address

Provision the device by imprinting a MAC address on it.

Procedure

1. Select **Devices** > **IP phones**.
2. Select **Provision new device** from the **Actions** tab.
3. Do one of the following:
   - Manually add a device MAC address: select **Add MAC address**, enter the **MAC address** and **Location**, and select **Apply**.
   - Upload a file to add a device MAC address: select **Upload MAC addresses**, select a file, and select **Apply**.

Step 2: Generate a Verification Code

You need to generate a verification code for the devices. The verification code is generated in bulk or at the device level and is valid for 24 hours.

Procedure

1. Select an existing **MAC address** from the **Waiting on activation** tab.
2. Select **Generate verification code**.
   A password is created for the MAC address and is shown in the Verification Code column.

Step 3: Provisioning on the Device

Once the device is powered up and connected to network, the technician provisions the device by choosing the Settings gear on the top right of the new Sign in page and selecting **Provision phone**.

Procedure

1. Select ⚙ > **Provision phone** on the device.

2. Enter **verification code** in the **Type the verification code** field.

Step 4: Sign in Remotely

The provisioned device appears in the **Waiting for sign in** tab. Initiate the remote sign-in process by selecting the individual device.

Procedure

1. Select a device from the **Waiting for sign in** tab.
2. Select **Sign in a user** and follow the instructions.

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 all device software to the latest version with one click on the Microsoft Teams & Skype for Business Admin Center. It is only applicable to devices running the Teams firmware.

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.

Note: For T58A/T56A Teams devices, if you upgrade the firmware from 58.15.0.20 to 58.15.0.41 (or later), you need to upgrade to 58.15.0.26 first and then upgrade the firmware to 58.15.0.41(or later).

- Firmware for Each Device Model
- Firmware Upgrade Configuration

Related tasks

Updating Device Software

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
T58A/T56A/T55A	58.x.x.x.rom	58.15.0.124.rom
CP960	73.x.x.x.rom	73.15.0.117.rom
VP59	91.x.x.x.rom	91.15.0.58.rom
MP58/MP58-WH/MP56/ MP54	122.x.x.x.rom	122.15.0.36.rom

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	**over_the_air.url.bth58**	**<y0000000000xx>.cfg**
Description	It configures the access URL of the BTH58 handset firmware file.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Settings** > **Upgrade** > **Upgrade Firmware**	

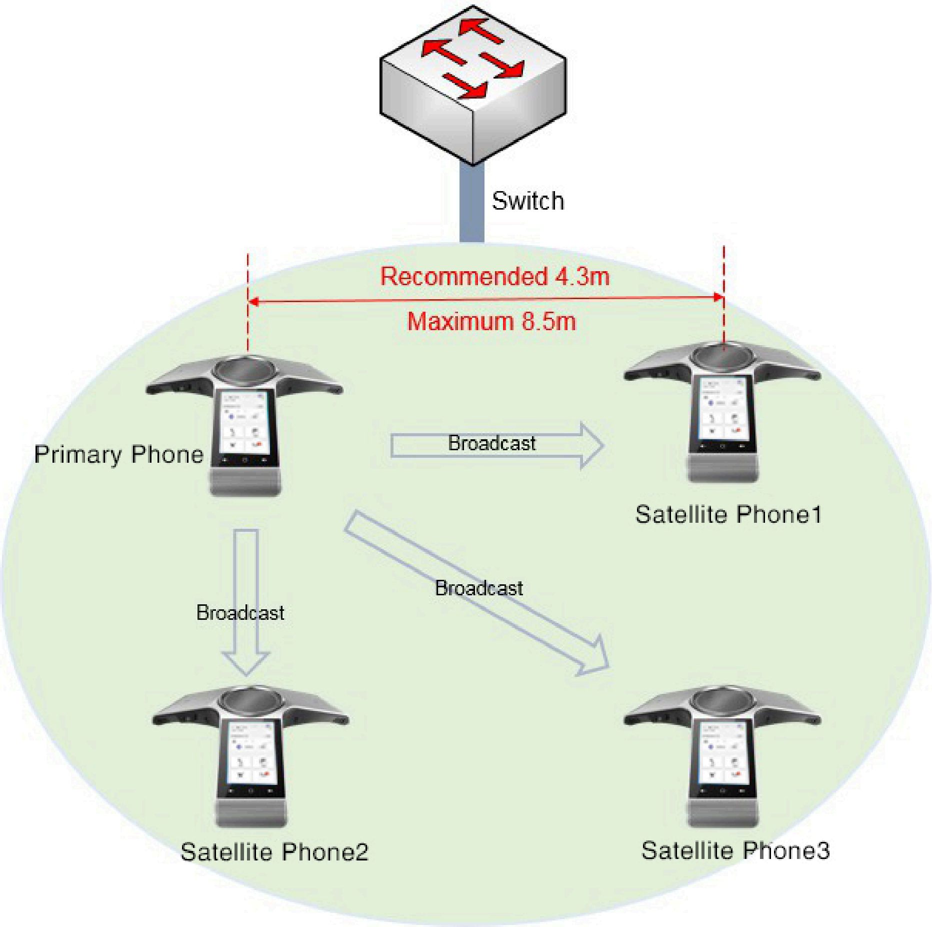
[1] If you change this parameter, the device will reboot to make the change take effect.

Using CP960 Cascaded Mode

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

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

The following shows an example for setting up a cascaded group:


Switch
Recommended 4.3m
Maximum 8.5m
Primary Phone
Broadcast
Satellite Phone1
Broadcast
Broadcast
Satellite Phone2
Satellite Phone3

- Guidelines for Configuring Cascaded Mode
- CP960 Cascaded Mode Configuration
- Example: Configuring CP960 Cascaded Mode

Guidelines for Configuring Cascaded Mode

The following instructions you need to know when configuring cascaded mode for CP960:

- Ensure all the phones are deployed in the same subnet.
- Ensure all the phones are running the same firmware versions.
- You can only deploy the CP960 phones in a star layout in the wired network.
- If the primary phone is not in the broadcast status, the satellite phones will not reconnect automatically after reboot.
- The satellite phones are unable to sync some custom features of primary phone, for example, wallpaper or contact avatar.
- You cannot access the web user interface of the satellite phones.
- If you upgrade firmware via the web user interface for the primary phone, only the primary phone will be upgraded. After upgrading, the satellite phones are disconnected from the primary phone because of the different firmware version.
- If you upgrade firmware via auto provisioning, both the primary phone and satellite phones will be upgraded.

CP960 Cascaded Mode Configuration

The following table lists the parameters you can use to configure CP960 cascaded mode.

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

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

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

Related information

Example: Configuring CP960 Cascaded Mode

Example: Configuring CP960 Cascaded Mode

Scenario Conditions

The MAC address of phone A is 805EC0092F33.

The MAC address of phone B is 805EC0092F4B.

The MAC address of phone C is 805EC009223B.

The MAC address of phone D is 805EC0033E2B.

All the phones are in the same subnet, and are running the same firmware versions.

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

The following example shows configuration for the phones:

Example

```
######For Phone A (primary phone)######

features.cp_star_connection.master.enable=1

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

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

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

######For Phones B, C, D (satellite phones)######

features.cp_star_connection.master.enable=0

features.cp_star_connection.master.mac=805EC0092F33
```

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

Device Customization

You can make the Teams device more personalized by customizing various settings.

- Language
- Screen Saver
- Backlight
- Time and Date
- Tones
- Volume
- Noise Suppression
- Smart Noise Block
- Acoustic Shield
- Power Saving
- Power LED Indicator
- Bluetooth

Language

Teams 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/Endpoint		**Web User Interface**		
Language	**Language Pack**	**Language**	**Language Pack**	**Note Language Pack**
English	000.GUI.English.lang	English	1.English.js	1.English_note.xml
Chinese Simplified	001.GUI.Chinese_S.lang	Chinese Simplified	2.Chinese_S.js	2.Chinese_S_note.xml
Chinese Traditional	002.GUI.Chinese_T.lang	Chinese Traditional	3.Chinese_T.js	3.Chinese_T_note.xml
French	003.GUI.French.lang	French	4.French.js	4.French_note.xml
German	004.GUI.German.lang	German	5.German.js	5.German_note.xml
Italian	005.GUI.Italian.lang	Italian	6.Italian.js	6.Italian_note.xml
Polish	006.GUI.Polish.lang	Polish	7.Polish.js	7.Polish_note.xml
Portuguese	007.GUI.Portuguese.lang	Portuguese	8.Portuguese.js	8.Portuguese_note.xml
Spanish	008.GUI.Spanish.lang	Spanish	9.Spanish.js	9.Spanish_note.xml
Turkish	009.GUI.Turkish.lang	Turkish	10.Turkish.js	10.Turkish_note.xml
Russian	010.GUI.Russian.lang	Russian	11.Russian.js	11.Russian_note.xml
Netherlands	011.GUI.Netherlands.lang	Netherlands	12.Netherlands.js	12.Netherlands_note.xml
Japanese	012.GUI.Japanese.lang	Japanese	13.Japanese.js	13.Japanese_note.xml

- 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	English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian, Netherlands, Japanese or the custom language name.	

Default	English	
Phone UI	☰ > **Settings** > **Device Settings** > **Language** For Common Area Phones: ☰ > **Settings** > **Device Settings** > **Language** **(default password: admin)**	
Parameter	**lang.wui**	**<y0000000000xx>.cfg**
Description	It configures the language to display on the web user interface.	
Permitted Values	English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian, Netherlands, Japanese or the custom language name.	
Default	English	
Web UI	On the top right corner of the web user interface	

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” (X starts from 012, “name” is replaced with the language name). If the language name is the same as the existing one, the existing language pack will be overridden by the newly uploaded one. We recommend that the filename of the new language pack should not be the same as the existing one.

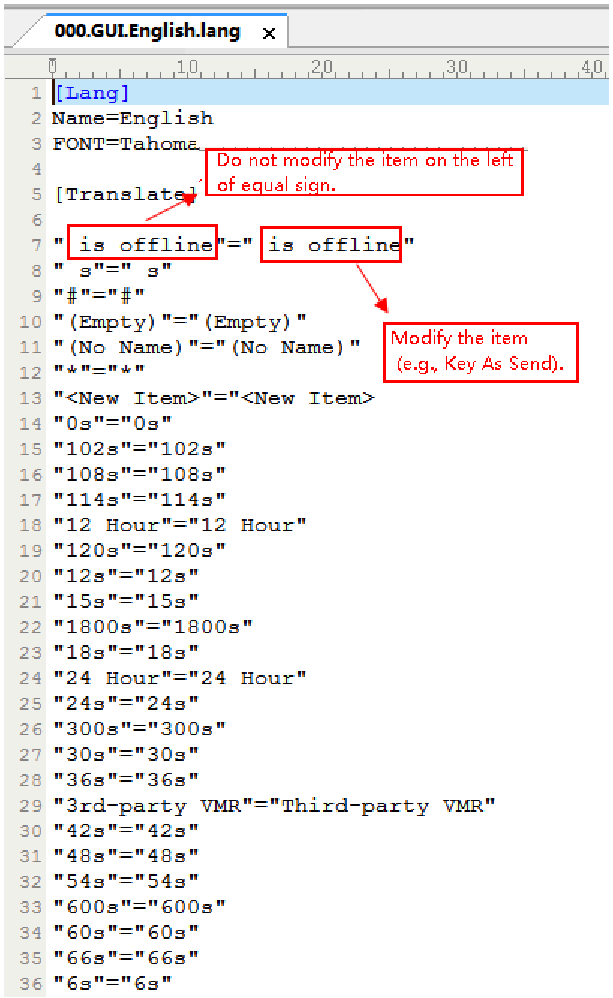
Note: To modify language file, do not rename the language pack.

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:



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

Modify the item (e.g., Key As Send).

```
[Lang]
Name=English
FONT=Tahoma

[Translate]

" is offline"=" is offline"
" s"=" s"
"#"="#"
"(Empty)"="(Empty)"
"(No Name)"="(No Name)"
"*"="*"
"<New Item>"="<New Item>
"0s"="0s"
"102s"="102s"
"108s"="108s"
"114s"="114s"
"12 Hour"="12 Hour"
"120s"="120s"
"12s"="12s"
"15s"="15s"
"1800s"="1800s"
"18s"="18s"
"24 Hour"="24 Hour"
"24s"="24s"
"300s"="300s"
"30s"="30s"
"36s"="36s"
"3rd-party VMR"="Third-party VMR"
"42s"="42s"
"48s"="48s"
"54s"="54s"
"600s"="600s"
"60s"="60s"
"66s"="66s"
"6s"="6s"
```

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 X starts from 012, “name” is replaced with the language name.
Default	Blank

Language for Web Display Customization

You can modify the language file or add a new language for web display. You can also customize the note language pack. The note information is displayed in the icon ? of the web user interface.

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

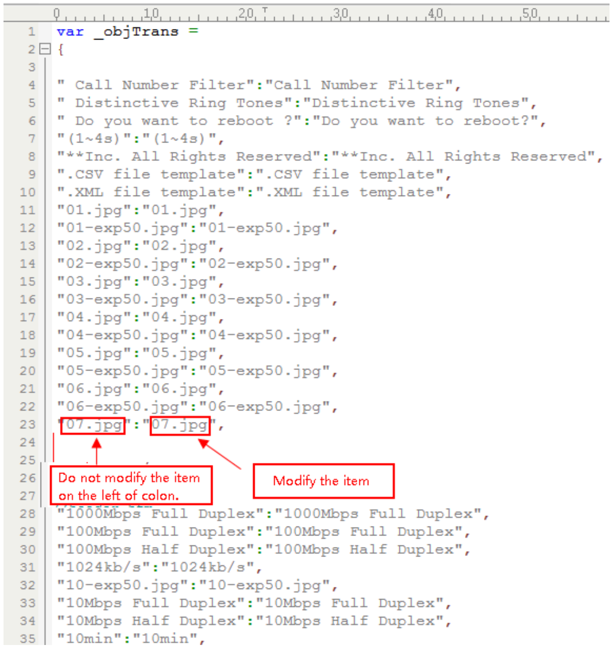
Customizing a Language Pack for Web Display

When you add a new language pack for the web user interface, the language pack must be formatted as “X.name.js” (X starts from 13, “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:



```
var _objTrans =
{

" Call Number Filter":"Call Number Filter",
" Distinctive Ring Tones":"Distinctive Ring Tones",
" Do you want to reboot ?":"Do you want to reboot?",
"(1~4s)":"(1~4s)",
"**Inc. All Rights Reserved":"**Inc. All Rights Reserved",
".CSV file template":".CSV file template",
".XML file template":".XML file template",
"01.jpg":"01.jpg",
"01-exp50.jpg":"01-exp50.jpg",
"02.jpg":"02.jpg",
"02-exp50.jpg":"02-exp50.jpg",
"03.jpg":"03.jpg",
"03-exp50.jpg":"03-exp50.jpg",
"04.jpg":"04.jpg",
"04-exp50.jpg":"04-exp50.jpg",
"05.jpg":"05.jpg",
"05-exp50.jpg":"05-exp50.jpg",
"06.jpg":"06.jpg",
"06-exp50.jpg":"06-exp50.jpg",
"07.jpg":"07.jpg",




"1000Mbps Full Duplex":"1000Mbps Full Duplex",
"100Mbps Full Duplex":"100Mbps Full Duplex",
"100Mbps Half Duplex":"100Mbps Half Duplex",
"1024kb/s":"1024kb/s",
"10-exp50.jpg":"10-exp50.jpg",
"10Mbps Full Duplex":"10Mbps Full Duplex",
"10Mbps Half Duplex":"10Mbps Half Duplex",
"10min":"10min",
```

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

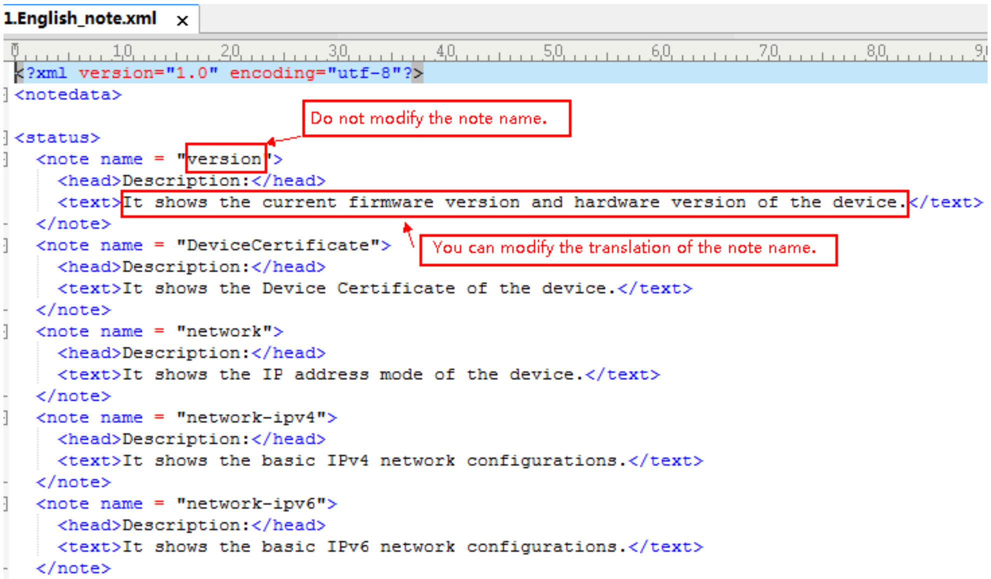
Customizing a Language Pack for Note Display

When you add a new language pack for the note, the note language pack must be formatted as “X.name_note.xml” (X starts from 12, “name” is replaced with the language name). If the note language name is the same as the existing one, the new uploaded note language pack will override the existing one.

We recommend that the filename of the new note language pack should not be the same as the existing one.

1. Open the desired note language template pack (for example, 1.English_note.xml) using an XML editor.
2. Modify the text of the note field. Do not modify the note name.

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



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

<status>
  <note name = "version">
    <head>Description:</head>
    <text>It shows the current firmware version and hardware version of the device.</text>
  </note>
  <note name = "DeviceCertificate">
    <head>Description:</head>
    <text>It shows the Device Certificate of the device.</text>
  </note>
  <note name = "network">
    <head>Description:</head>
    <text>It shows the IP address mode of the device.</text>
  </note>
  <note name = "network-ipv4">
    <head>Description:</head>
    <text>It shows the basic IPv4 network configurations.</text>
  </note>
  <note name = "network-ipv6">
    <head>Description:</head>
    <text>It shows the basic IPv6 network configurations.</text>
  </note>
```

Do not modify the note name.

You can modify the translation of the note name.

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

Custom Language for Web and Note Display Configuration

If you want to add a new language (for example, Wuilan) to devices, prepare the language file named as “13.Wuilan.js” and “13.Wuilan_note.xml” for downloading. After the update, you will find a new language selection “Wuilan” at the top-right corner of the web user interface, and new note information is displayed in the icon when 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 For example: http://localhost/X.GUI.name.lang X starts from 012, “name” is replaced with the language name	
Default	Blank	
Parameter	**wui_lang_note.url**	**<y0000000000xx>.cfg**
Description	It configures the access URL of the custom note language pack for web user interface.	

Permitted Values	URL within 511 characters For example: http://localhost/X.name_note.xml X starts from 13, “name” is replaced with the language name	
Default	Blank	
Parameter	**wui_lang.delete**	**<y0000000000xx>.cfg**
Description	It deletes the specified or all custom web language packs and note language packs of the web user interface.	
Permitted Values	http://localhost/all or http://localhost/*Y.name.js*	
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

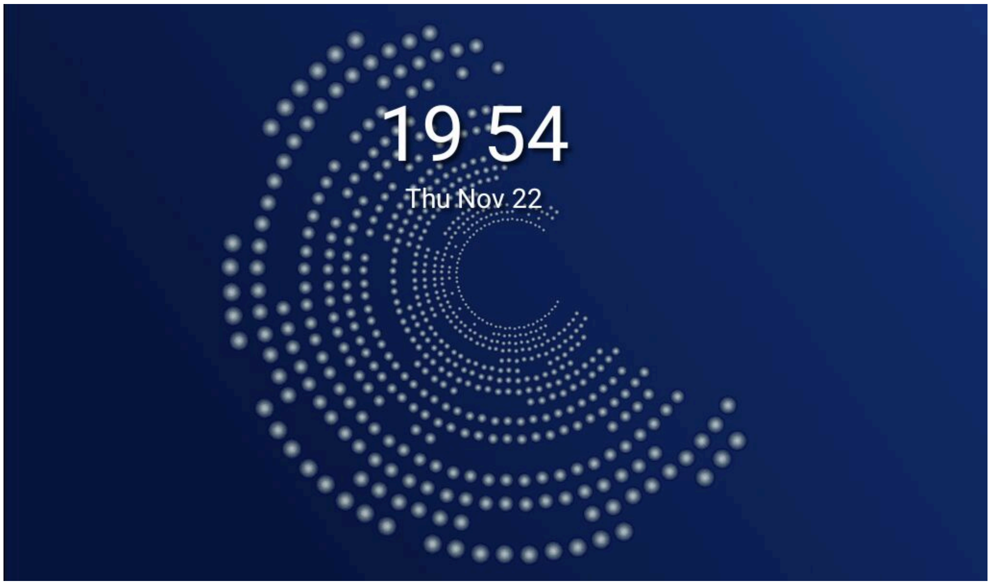
lang.gui=English_15

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: ☰ > **Settings** > **Device Settings** > **Language**.

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.

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. The following shows the built-in screen saver displayed on T58A Teams devices:



- Screensaver Configuration

Screensaver Configuration

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

Parameter	**screensaver.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the screen saver.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Settings** > **Preference** > **Screensaver** > **Screensaver**	
Phone UI	☰ > **Settings** > **Device Settings** > **Display** > **Screen saver** > **Screen Saver Enable** For Common Area Phones: ☰ > **Settings** > **Device Settings** > **Screen Saver (default password: admin)** > **Screen Saver Enable**	
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	**30**-30s **60**-1min **300**-5min **600**-10min **900**-15min **1800**-30min **3600**-1h **7200**-2h	

Default	900	
Web UI	**Settings** > **Preference** > **Screensaver** > **Screensaver Wait Time**	
Phone UI	☰ > **Settings** > **Device Settings** > **Display** > **Screen saver** > **Screensaver Waiting Time** For Common Area Phones: ☰ > **Settings** > **Device Settings** > **Screen Saver (default password: admin)** > **Screensaver Waiting Time**	
Parameter	**screensaver.type**	**<y0000000000xx>.cfg**
Description	It configures the type of screen saver to display.	
Permitted Values	**0**-System, the LCD screen will display the built-in picture. **4**-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 every 60 seconds.	
Default	Blank	
Web UI	**Settings** > **Preference** > **Screensaver Type**	
Phone UI	☰ > **Settings** > **Device Settings** > **Display** > **Screen Saver Type** For Common Area Phones: ☰ > **Settings** > **Device Settings** > **Screen Saver (default password: admin)** > **Screen Saver 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** > **Screensaver** > **Screensaver Type(Custom)** > **Upload Screensaver**	
Parameter	**screensaver.background**	**<y0000000000xx>.cfg**
Description	It configures the background for the screen saver.	

Permitted Values	Default.jpg 01.png 02.png 03.png 04.png 05.png 06.png 07.png 08.png	
Default	Default.jpg	
Web UI	**Settings** > **Preference** > **Screensaver** > **Screensaver Type(System)** > **Screensaver Background** **Settings** > **Preference** > **Screensaver** > **Screensaver Type(Custom)** > **Screensaver**	
Phone UI	☰ > **Settings** > **Device Settings** > **Display** > **Screen saver** > **Screensaver Type(System)** > **Screensaver background** For Common Area Phones: ☰ > **Settings** > **Device Settings** > **Screen Saver (default password: admin)** > **Screensaver Type(System)** > **Screensaver background**	
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	

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.

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.

Backlight Time: The delay time to change the brightness of the LCD backlight when the device is inactive. Backlight time includes the following settings:

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

- Backlight Brightness and Time Configuration

Backlight Brightness and Time Configuration

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

Parameter	**phone_setting.active_backlight_level**	**<y0000000000xx>.cfg**
Description	It configures the intensity of the LCD backlight when the device is active.	
Permitted Values	Integer from 1 to 10	
Default	8	
Web UI	**Settings** > **Preference** > **Backlight** > **Backlight Active Level**	
Phone UI	☰ > **Settings** > **Device Settings** > **Display** > **Backlight** > **Backlight Active Level**	
Parameter	**phone_setting.backlight_time**	**<y0000000000xx>.cfg**
Description	It configures the delay time (in seconds) to change the intensity of the LCD backlight when the device is inactive.	
Permitted Values	**0**-Always On **15**-15s **30**-30s **60**-1min **120**-2min **300**-5min **600**-10min **1800**-30min	
Default	0	
Web UI	**Settings** > **Preference** > **Backlight** > **Backlight Time(seconds)** **Setting** > **General** > **General Information** > **Backlight Time**	
Phone UI	☰ > **Settings** > **Device Settings** > **Display** > **Backlight** > **Backlight Time**	

Time and Date

Teams 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 Id	Time Zone Name	Time Zone Id	Time Zone Name
Etc/GMT+12	International Date Line West	Europe/Moscow	Moscow, St. Petersburg, Volgograd (RTZ 2)
Etc/GMT+11	Coordinated Universal Time-11	Africa/Nairobi	Nairobi
Pacific/ Honolulu	Hawaii	Asia/Tehran	Tehran
America/ Anchorage	Alaska	Asia/Muscat	Abu Dhabi, Muscat
America/ Los_Angeles	Pacific Time (US & Canada)	Asia/Baku	Baku
America/ Tijuana	Baja California	Europe/Samara	Izhevsk, Samara (RTZ 3)
America/ Mazatlan	Chihuahua, La Paz, Mazatlan	Indian/Mauritius	Port Louis
America/ Phoenix	Arizona	Asia/Tbilisi	Tbilisi
America/ Edmonton, America/ Denver	Mountain Time (US & Canada)	Asia/Yerevan	Yerevan
America/ Guatemala	Central America	Asia/Kabul	Kabul
America/ Mexico_City	Guadalajara, Mexico City, Monterrey	Asia/Tashkent, Asia/ Ashgabat	Ashgabat, Toshkent
America/ Regina	Saskatchewan	Asia/Yekaterinburg	Ekaterinburg (RTZ 4)
America/ Chicago	Central Time (US & Canada)	Asia/Karachi	Islamabad, Karachi
America/ Cancun	Chetumal	Asia/Calcutta	Chennai, Kolkata, Mumbai, New Delhi
America/ New_York	Eastern Time (US & Canada)	Asia/Colombo	Sri Jayawardenepura
America/ Indianapolis	Indiana (East)	Asia/Kathmandu	Kathmandu

Time Zone Id	Time Zone Name	Time Zone Id	Time Zone Name
America/ Rio_Branco, America/ Bogota	Bogota, Lima, Quito, Rio Branco	Asia/Almaty	Astana
America/ Caracas	Caracas	Asia/Dhaka	Dhaka
America/ Cuiaba	Cuiaba	Asia/Novosibirsk	Novosibirsk (RTZ 5)
America/ La_Paz	Georgetown, La Paz, Manaus, San Juan	Asia/Rangoon	Yangon (Rangoon)
America/ Asuncion	Asuncion	Asia/Bangkok, Asia/ Jakarta	Bangkok, Hanoi, Jakarta
America/ Halifax	Atlantic Time (Canada)	Asia/Krasnoyarsk	Krasnoyarsk (RTZ 6)
America/ St_Johns	Newfoundland	Asia/Shanghai, Asia/ Hong_Kong	Beijing, Chongqing, Hong Kong, Urumqi
America/Bahia	Brasilia	Asia/Irkutsk	Irkutsk (RTZ 7)
America/ Buenos_Aires	Buenos Aires	Asia/Singapore, Asia/ Kuala_Lumpur	Kuala Lumpur, Singapore
America/ Cayenne, America/ Fortaleza	Cayenne, Fortaleza	Australia/Perth	Perth
America/ Godthab	Greenland	Asia/Taipei	Taipei
America/ Montevideo	Montevideo	Asia/Ulaanbaatar	Ulaanbaatar
America/Bahia	Salvador	Asia/Tokyo	Osaka, Sapporo, Tokyo
America/ Santiago	Santiago	Asia/Seoul	Seoul
Etc/GMT+2	Coordinated Universal Time-02	Asia/Yakutsk	Yakutsk (RTZ 8)
America/ Noronha	Mid-Atlantic - Old	Australia/Adelaide	Australia/Adelaide
Atlantic/ Azores	Azores	Australia/Darwin	Darwin
Atlantic/ Cape_Verde	Cabo Verde Is	Australia/Brisbane	Brisbane
Africa/ Casablanca	Casablanca	Australia/Sydney	Canberra, Melbourne, Sydney
Etc/GMT	Coordinated Universal Time	Pacific/Port_Moresby, Pacific/Guam	Guam, Port Moresby

Time Zone Id	Time Zone Name	Time Zone Id	Time Zone Name
Europe/London, Europe/Dublin, Europe/Lisbon	Dublin, Edinburgh, Lisbon, London	Australia/Hobart	Hobart
Atlantic/Reykjavik, Europe/Stockholm	Monrovia, Reykjavik	Asia/Magadan	Magadan
Europe/Berlin, Europe/Rome, Europe/Stockholm	Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	Asia/Vladivostok	Vladivostok, Magadan (RTZ 9)
Europe/Budapest, Europe/Belgrade	Belgrade, Bratislava, Budapest, Ljubljana, Prague	Asia/Srednekolymsk	Chokurdakh (RTZ 10)
Europe/Paris, Europe/Madrid, Europe/Brussels	Brussels, Copenhagen, Madrid, Paris	Pacific/Guadalcanal, Pacific/Noumea	Solomon Is., New Caledonia
Europe/Warsaw, Europe/Skopje	Sarajevo, Skopje, Warsaw, Zagreb	Asia/Anadyr	Anadyr, Petropavlovsk-Kamchatsky (RTZ 11)
Africa/Lagos	West Central Africa	Pacific/Auckland	Auckland, Wellington
Africa/Windhoek	Windhoek	Etc/GMT-12	Coordinated Universal Time+12
Asia/Amman	Amman	Pacific/Fiji	Fiji
Europe/Bucharest, Europe/Athens	Athens, Bucharest	Asia/Kamchatka	Petropavlovsk-Kamchatsky - Old
Asia/Beirut	Beirut	Pacific/Tongatapu	Nuku'alofa
Africa/Cairo	Cairo	Pacific/Pago_Pago	Samoa
Asia/Damascus	Damascus	Pacific/Kiritimati	Kiritimati Island
Europe/Chisinau	E. Europe	Australia/Eucla	Eucla
Africa/Harare	Harare, Pretoria	Asia/Gaza	Gaza
Europe/Kiev	Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	Europe/Luxembourg	Luxembourg
Europe/Istanbul	Istanbul	Atlantic/Canary	Spain-Canary Islands

Time Zone Id	Time Zone Name	Time Zone Id	Time Zone Name
Asia/ Jerusalem	Jerusalem	America/Havana	Havana
Europe/ Kaliningrad	Kaliningrad	America/Nassau	Nassau
Africa/Tripoli	Tripoli	Atlantic/Bermuda	Bermuda
Asia/Baghdad	Baghdad	Pacific/Marquesas	French Polynesia
Asia/Riyadh, Asia/Kuwait	Kuwait, Riyadh	Australia/Lord_Howe	Lord Howe Island
Europe/Minsk	Minsk	Pacific/Chatham	Chatham Islands

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	≡ > **Settings** > **Device Settings** > **Time&Date** > **DHCP 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	☰ > **Settings** > **Device Settings** > **Time&Date** > **General** > **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	☰ > **Settings** > **Device Settings** > **Time&Date** > **General** > **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.android_time_zone**	**<MAC>.cfg**
Description	It configures the time zone name in the tzdata standard.	
Permitted Values	String within 64 characters For available time zones, refer to Time Zone.	
Default	Asia/Beijing	
Web UI	**Settings** > **Time & Date** > **Time Zone**	
Phone UI	**More** > **Settings** > **Device Settings** > **Time&Date** > **General** > **Time Zone**	

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.)
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

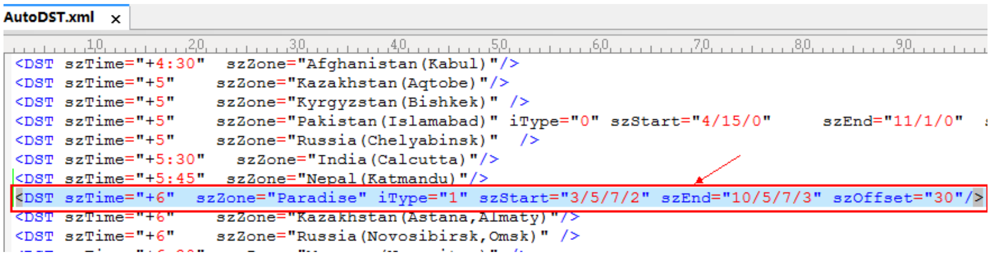
1. Open the AutoDST file.

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:

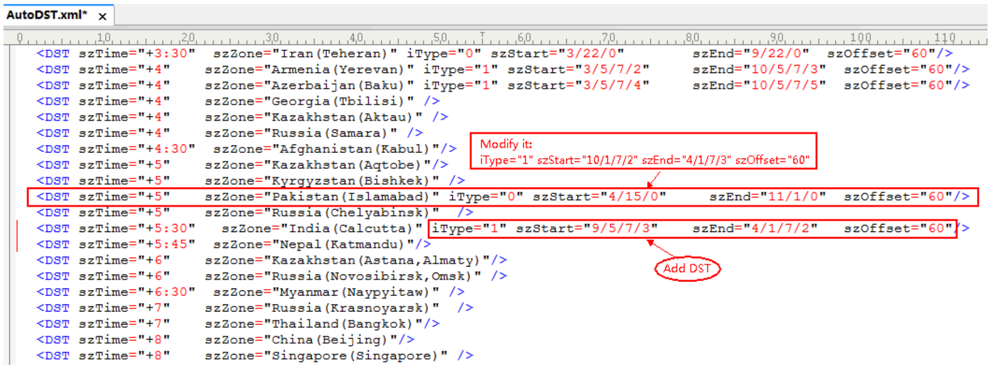
   Add a new time zone (+6 Paradise) with daylight saving time 30 minutes:

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



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

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



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

Modify it:
iType="1" szStart="10/1/7/2" szEnd="4/1/7/3" szOffset="60"

Add DST

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	≡ > **Settings** > **Device Settings** > **Time&Date** > **General** > **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**	
Phone UI	☰ > **Settings** > **Device Settings** > **Time & Date** > **General** > **Type** > **Manual Settings**	

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	☰ > **Settings** > **Device Settings** > **Time&Date** > **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 **7**-MM/DD/YYYY Use the following mapping: “WWW” represents the abbreviation of the week; “DD” represents a two-digit day; “MM” represents a two-digit month; “MMM” represents the first three letters of the month; “YYYY” represents a four-digit year, and “YY” represents a two-digit year.	
Default	0	
Web UI	**Settings** > **Time & Date** > **Date Format**	
Phone UI	☰ > **Settings** > **Device Settings** > **Time&Date** > **Time & Date Format** > **Date Format**	

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. It is not applicable to CP960 phones.

- Supported Tones
- Tones Configuration

Supported Tones

The default tones used on Teams 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. **Note**: It is not applicable to CP960 phones.	
Permitted Values	Custom, Australia, Austria, Brazil, Belgium, Chile, China, Czech, Czech ETSI, Denmark, Finland, France, Germany, Great Britain, Greece, Hungary, Lithuania, India, Italy, Japan, Mexico, New Zealand, Netherlands, Norway, Portugal, Spain, Switzerland, Sweden, Russia, United States	
Default	Custom	
Web UI	**Settings** > **Tones** > **Select Country**	

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.	
Web UI	**Settings** > **Tones** > **Dial**	
Parameter	**features.ringer_device.is_use_headset**	**<y0000000000xx>.cfg**
Description	It configures the ringer device for the phone.	
Permitted Values	**0**-Use Speaker **1**-Use Headset **2**-Use Headset & Speaker	
Default	0	
Web UI	**Settings** > **Tones** > **Ringer Device**	
Phone UI	☰ > **Settings** > **Device settings** > **Tones**	

Volume

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

- Volume Configuration

Volume Configuration

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

Parameter	**voice.handset.tia4965.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the handset's volume level to be reset to level 11 after the call if the volume level for the current call exceeds the standards.	

Permitted Values	**0**-Disabled **1**-Enabled, if the handset's volume level for the current call is adjusted to level 12/13/14/15, the volume level automatically resets to 11 after the call. That is, the initial volume level is 11 for the next call.	
Default	1	
Parameter	**voice.headset.tia4965.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the headset's volume level to be reset to level 11 after the call if the volume level for the current call exceeds the standards.	
Permitted Values	**0**-Disabled **1**-Enabled, if the headset's volume level for the current call is adjusted to level 12/13/14/15, the volume level automatically resets to 11 after the call. That is, the initial volume level is 11 for the next call.	
Default	1	

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.

- Noise Suppression Configuration

Noise Suppression Configuration

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

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

Smart Noise Block

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

- Smart Noise Block Configuration

Smart Noise Block Configuration

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

Parameter	**voice.ans_nb.enable**	**<y0000000000xx>.cfg**

Description	It enables or disables the Smart Noise Block feature. **Note**: It works only if “voice.tns.enable” is set to 1 (Enabled).
Permitted Values	**0**-Disabled **1**-Enabled
Default	1
Web UI	**Settings** > **Voice** > **Noise Proof** > **Smart Noise Block**

Acoustic Shield

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

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

- Acoustic Shield Configuration

Acoustic Shield Configuration

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

Parameter	**features.acoustic_shield.mode**	**<y0000000000xx>.cfg**
Description	It enables or disables the acoustic shield feature during the call.	
Permitted Values	**0**- Disabled **2**- Auto, the acoustic shield is automatically enabled when the call is set up.	
Default	2	
Web UI	**Settings** > **Voice** > **Acoustic Shield** > **Acoustic Shield Mode**	

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.

Note: For VP59/MP54/MP58/MP58-WH Teams phones, if you disable the power saving feature, the phone will automatically enter power-saving mode to protect the screen when the phone is inactive for 72 hours. Image persistence may be caused on LCD if power saving is disabled.

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, the phone automatically enters the power-saving mode to protect the screen when the phone is inactive for 72 hours. Image persistence may be caused on LCD. **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	120	
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.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/Text Mail Power Light Flash**	
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.missed_call_power_led_flash.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the power LED indicator to flash when the phone misses a call.	
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** > **MissCall Power Light Flash**

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).

You can pair and connect a Bluetooth headset or Bluetooth handset with the device.

For T56A/T55A/MP54 Teams phones, make sure the Bluetooth USB Dongle BT41 is connected to 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/MP58/MP58-WH/MP56/MP54 Skype for Business phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Parameter	**features.bluetooth_enable**	**<y0000000000xx>.cfg**
Description	It triggers the Bluetooth mode to on or off.	
Permitted Values	**0**-Off **1**-On	
Default	1 (0 for MP56)	
Phone UI	☰**(More)** > **Settings** > **Device Settings** > **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 VP59: Yealink-VP59 For CP960: Yealink-CP960 For MP54: Yealink-MP54 For MP56: Yealink-MP56 For MP58/MP58-WH: Yealink-MP58
Phone UI	☰**(More)** > **Settings** > **Device Settings** > **Bluetooth** > **Device Name**

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

Common Area Phone

A common area phone is typically placed in an area like a lobby or another area which is available to many people to make a call; for example, a reception area, lobby, or conference phone. Common area phones are set up as devices rather than users, and can automatically sign into a network.

You need to set up an account for the phone system to deploy common area phones for your organization.

You have access to certain features for the common area phones:

- **CAP account**: You have calls capability. You also have searching capability if your system administrator enables it on the Microsoft Teams & Skype for Business Admin Center.
- **Meeting account**: You can only join the scheduled meeting.

For more information on how to set up an account for common area phones, refer to Set up the Common Area Phone license for Microsoft Teams.

Call Features

This chapter shows you how to configure the call feature on Teams devices.

- Call Queue
- Call Park and Retrieve

Call Queue

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.

You can set the greeting and music played while on hold and choose either **Attendant**, **Serial**, or **Round Robin** for your call queue distribution method. All new and existing call queues will have attendant routing selected by default. When attendant routing is used, the first call in the queue rings all call agents at the same time. The first call agent to pick up the call gets the call.

Call queue feature is only applicable to MP58/MP58-WH/MP56/MP54/T58A/T56A/T55A Teams phones.

For information on how to create a call queue, refer to Create a Cloud call queue.

Call Park and Retrieve

Call park and retrieve is a feature that lets a user place a call on hold in the Teams service in the cloud. When a call is parked, the service generates a unique code for call retrieval. The user who parked the call or someone else can then use that code to retrieve the call.

Call park and retrieve feature is disabled by default. You can enable it for users and create user groups using the call park policy. When you apply the same policy to a set of users, they can park and retrieve calls.

For more information on how to configure call park and retrieve, refer to Call park and retrieve in Microsoft Teams.

Security Features

- User and Administrator Identification
- Phone 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 accessing 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.

When you sign in on the web interface more than 5 times with the default password, you will be forced to change your password. The modified password must comply with the following rules:

- The password must be at least 8 digits in length.
- The password must contain a combination of at least two characters:
  - Lowercase letters
  - Uppercase letters
  - Numbers
  - Special characters: ` ~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- User and Administrator Identification Configuration

- User Access Level Configuration

User and Administrator Identification Configuration

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

Parameter	**static.security.user_name.user**	**<y0000000000xx>.cfg**
Description	It configures the user name of the user for the 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_name.var**	**<y0000000000xx>.cfg**
Description	It configures the user name of the var for device's web user interface access. **Note**: It works only if "static.security.var_enable" is set to 1 (Enabled).	
Permitted Values	String within 32 characters	
Default	var	
Parameter	**static.security.user_password**	**<y0000000000xx>.cfg**
Description	It configures the password 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	≡ > **Settings** > **Device Settings** > **Admin Password(default password: admin)** **Note**: You cannot change the user password via the phone user interface.	

Parameter	**static.security.custom_password_rule.X**[1]	**<y0000000000xx>.cfg**
Description	It configures the regular expression rules of the password, and the result is the AND operation of multiple regular expressions (up to 10). **Example**: static.security.custom_password_rule.1 = .{8,} means length of the password more than 8 digits. static.security.custom_password_rule.2 = ^((?!.*(000|111|222|333|444|555|666|777|888|999).*).)*$ means not allowed three consecutive identical numbers. static.security.custom_password_rule.3 = ^((?!\d(?:(?<=0)1|(?<=1)2|(?<=2)3|(?<=3)4|(?<=4)5|(?<=5)6|(?<=6)7|(?<=7)8|(?<=8)9){2,}).)*$ means not allowed three consecutive incremental numbers. static.security.custom_password_rule.4 = ^((?!\d(?:(?<=9)8|(?<=8)7|(?<=7)6|(?<=6)5|(?<=5)4|(?<=4)3|(?<=3)2|(?<=2)1|(?<=1)0){2,}).)*$ means not allowed three consecutive diminishing numbers. static.security.custom_password_rule.5 = ^((?!.*(admin|administrator|var|user|test).*).)*$ means not allowed to contain xxx.	
Permitted Values	String within 511 characters	
Default	Blank	

[1] X ranges from 1 to 31.

User Access Level Configuration

For more information, refer to Yealink SIP IP Phones Configuration Guide for User Access Level.

The following table lists the parameters you can use to configure the user access level.

Parameter	**static.security.var_enable**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the 3-level access permissions (admin, user, var).	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Parameter	**static.web_item_level.url**[1]	**<y0000000000xx>.cfg**
Description	It configures the access URL of the file, which defines 3-level access permissions.	
Permitted Values	URL within 511 characters	
Default	Blank	

Phone Lock

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

For users with high security requirements, you can enable the phone lock for them by Microsoft Teams & Skype for Business Admin Center so that they cannot disable it by themselves.

Note: Phone Lock feature is not available to Common Area Phones.

- Phone Lock Configuration

Related tasks

Creating a Configuration Profile

Related information

Provisioning Devices on the Microsoft Teams & Skype for Business Admin Center

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	**Features** > **Phone Lock** > **Phone Lock Enable**	
Phone UI	☰ > **Settings** > **Device Settings** > **Phone Lock** > **Lock Enable**	
Parameter	**phone_setting.phone_lock.lock_time_out**	**<y0000000000xx>.cfg**
Description	It configures the interval (in seconds) to automatically lock the phone.	
Permitted Values	Integer from 30 to 3600	
Default	900	
Web UI	**Features** > **Phone Lock** > **Idle time-out(30~3600s)**	
Phone UI	☰ > **Settings** > **Device Settings** > **Phone Lock** > **Idle time-out**	

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

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 Teams devices trust the following CAs by default:

- DigiCert High Assurance EV Root CA
- Deutsche Telekom Root CA-2
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure Global eBusiness CA-1
- GeoTrust Global CA
- GeoTrust Global CA2
- GeoTrust Primary Certification Authority
- GeoTrust Primary Certification Authority G2
- GeoTrust Universal CA
- GeoTrust Universal CA2
- Thawte Personal Freemail CA
- Thawte Premium Server CA
- Thawte Primary Root CA
- Thawte Primary Root CA - G2
- Thawte Primary Root CA - G3
- Thawte Server CA
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Universal Root Certification Authority
- ISRG Root X1 (Let’s Encrypt Authority X1 and Let’s Encrypt Authority X2 certificates are signed by the root certificate ISRG Root X1.)
- Baltimore CyberTrust Root
- DST Root CA X3

- Verizon Public SureServer CA G14-SHA2
- AddTrust External CA Root
- Go Daddy Class 2 Certification Authority
- Class 2 Primary CA
- Cybertrust Public SureServer SV CA
- DigiCert Assured ID Root G2
- DigiCert Assured ID Root G3
- DigiCert Assured ID Root CA
- DigiCert Global Root G2
- DigiCert Global Root G3
- DigiCert Global Root CA
- DigiCert Trusted Root G4
- Entrust Root Certification Authority
- Entrust Root Certification Authority - G2
- Entrust.net Certification Authority (2048)
- GeoTrust Primary Certification Authority - G3
- GlobalSign Root CA
- GlobalSign Root CA - R2
- Starfield Root Certificate Authority - G2
- TC TrustCenter Class 2 CA II
- TC TrustCenter Class 3 CA II
- TC TrustCenter Class 4 CA II
- TC TrustCenter Universal CA I
- TC TrustCenter Universal CA III
- Thawte Universal CA Root
- VeriSign Class 3 Secure Server CA - G2
- VeriSign Class 3 Secure Server CA – G3
- Thawte SSL CA
- StartCom Certification Authority
- StartCom Certification Authority G2
- Starfield Services Root Certificate Authority - G2
- RapidSSL CA
- Go Daddy Root Certificate Authority - G2
- Cybertrust Global Root
- COMODOSSLCA
- COMODO RSA Domain Validation Secure Server CA
- COMODO RSA Certification Authority
- AmazonRootCA4
- AmazonRootCA3
- AmazonRootCA2
- AmazonRootCA1
- Yealink Root CA
- Yealink Equipment Issuing CA
- SIP Core

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** > **Upload Trusted Certificate 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** > **Upload Server Certificate 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	
Parameter	**static.client_certificates.url**	**<y0000000000xx>.cfg**
Description	It configures the access URL of the custom client certificate used to specify the PC that can access the web user interface. **Note**: • The certificate you want to upload must be in *.pem, *.cer, *.crt or *.der format. • Only can import one certificate. The new certificate will overwrite the old. • Install the certificate on the PC or Mobile manually after importing the certificate to the device.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Security** > **Client Certs** > **Import Client Certificates**	

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

Encrypting Configuration Files

Yealink Teams 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), MAC-local CFG file (<MAC>-local.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, <MAC>-local.cfg) and <MAC>-contact.xml file from the server during auto provisioning no matter whether the files are encrypted or not. And then 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, <MAC>-local.cfg) or <MAC>-contact.xml file 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/ Custom 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 **Note**: For decrypting, it works only if “static.auto_provision.aes_key_in_file” is set to 0 (Disabled). If the downloaded MAC-Oriented file is encrypted and the parameter “static.auto_provision.aes_key_16.mac” is left blank, the device will try to encrypt/ decrypt the MAC-Oriented file using the AES key configured by the parameter “static.auto_provision.aes_key_16.com”.	
Permitted Values	16 characters	
Default	Blank	
Web UI	**Settings** > **Auto Provision** > **Common AES Key**	
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 **Note**: For decrypting, it works only if "static.auto_provision.aes_key_in_file" is set to 0 (Disabled). If the downloaded MAC-Oriented file is encrypted and the parameter "static.auto_provision.aes_key_16.mac" is left blank, the device will try to encrypt/ decrypt the MAC-Oriented file using the AES key configured by the parameter "static.auto_provision.aes_key_16.com".
Permitted Values	16 characters
Default	Blank
Web UI	**Settings** > **Auto Provision** > **MAC-Oriented AES Key**

Example: Encrypting Configuration Files

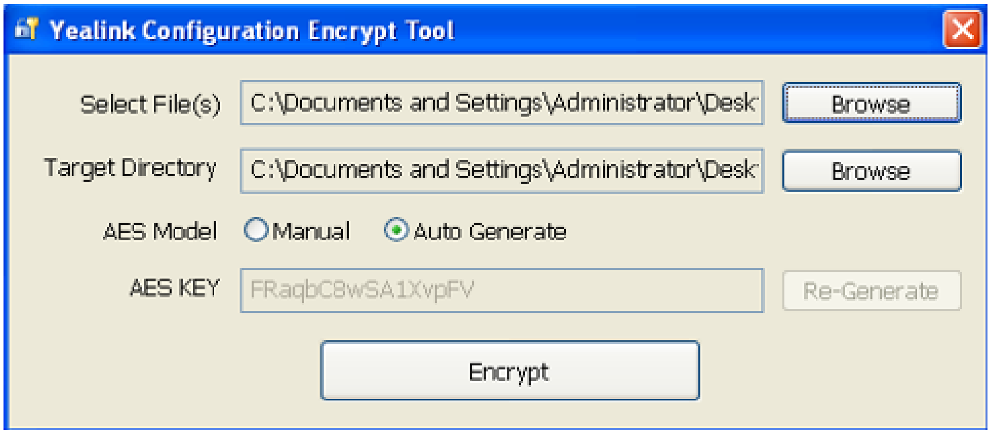
The following example describes how to use "Config_Encrypt_Tool.exe" to encrypt the account.cfg file. For more information on the other two encryption tools, refer to Yealink Configuration Encryption Tool User Guide.

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:



Select File(s) C:\Documents and Settings\Administrator\Desk

Target Directory C:\Documents and Settings\Administrator\Desk

AES Model ○ Manual ● Auto Generate

AES KEY FRaqbC8wSA1XvpFV

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.

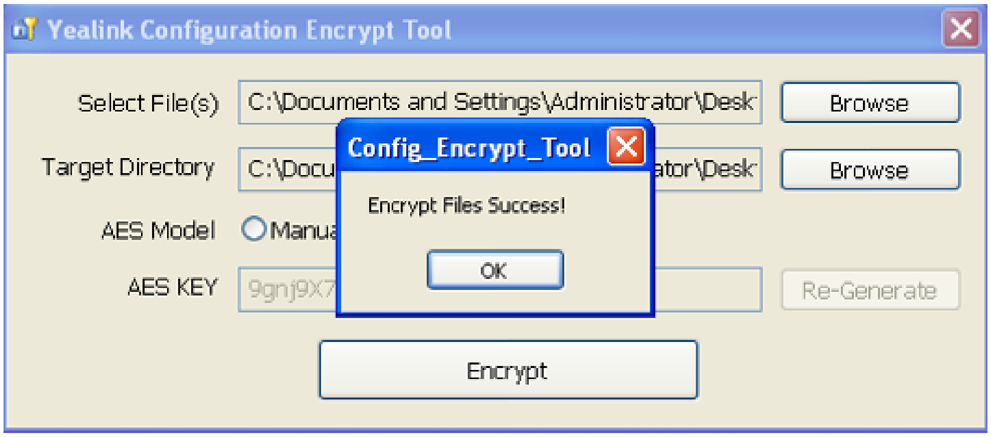
   To select multiple configuration files, you can select the first file and then press and hold the **Ctrl** key and select other files.
4. (Optional.) Click **Browse** to locate the target directory from your local system in the **Target Directory** field.

   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).


Yealink Configuration Encrypt Tool
Browse
Browse
Re-Generate
Encrypt
Config_Encrypt_Tool
OK

Select File(s) C:\Documents and Settings\Administrator\Desk

Target Directory C:\Docu ator\Desk

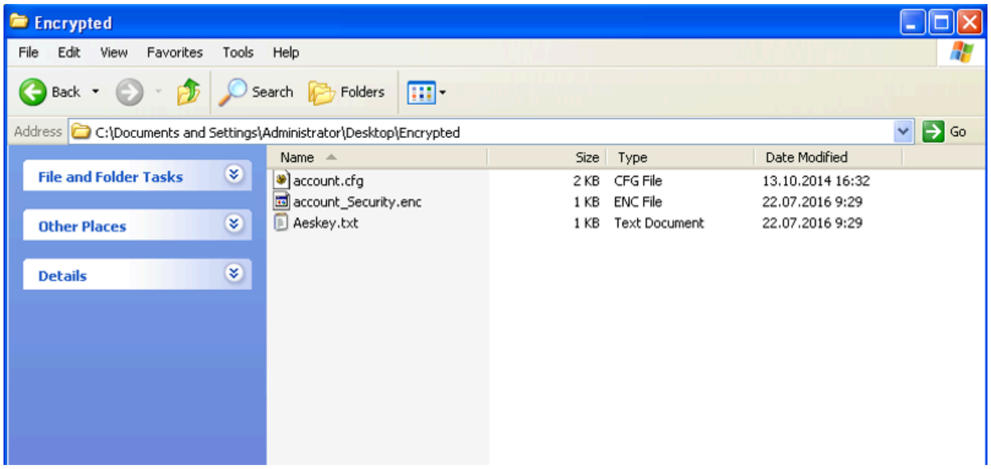
AES Model ○ Manua

AES KEY 9gnj9X7

Encrypt Files Success!

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).


Encrypted
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
Go
File and Folder Tasks
Other Places
Details

Address C:\Documents and Settings\Administrator\Desktop\Encrypted

Name	Size	Type	Date Modified
account.cfg	2 KB	CFG File	13.10.2014 16:32
account_Security.enc	1 KB	ENC File	22.07.2016 9:29
Aeskey.txt	1 KB	Text Document	22.07.2016 9:29

Hybrid Mode

Team devices support hybrid mode: survivability app mode and teams app mode. This feature is suitable for the scenario of disconnection with the local MS server. Also, it can be applied to customers who migrate from SIP solutions to Teams solutions. During the transition period, there will be both SIP account users and Teams account users within the enterprise, and we will make it possible for these two groups to communicate with each other in their groups.

- Hybrid Mode Configuration
- Paging Configuration

- SIP Account Registration Configuration
- Account Codec Configuration
- Local Directory Configuration

Hybrid Mode Configuration

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

Parameter	**features.hybrid_mode.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the hybrid mode feature.	
Permitted Values	**0**-Disabled, the Hybrid Mode configuration does not display on the phone user interface and the Account and Directory configurations do not display on the web user interface. **1**-Enabled	
Default	0	
Web UI	**Hybrid Mode** > **Basic** > **Hybrid Mode**	
Parameter	**features.hybrid_mode.quick_ball.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the quick ball for quickly switching between Teams APP and Survivability APP.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Hybrid Mode** > **Basic** > **Quick Ball**	
Phone UI	☰ > **Settings** > **Device Settings** > **Hybrid Mode** > **Quick Ball**	
Parameter	**features.hybrid_mode.sip_idle_timeout**	**<y0000000000xx>.cfg**
Description	It configures the waiting time of returning to the Teams APP when the user has no operation in Survivability APP.	
Permitted Values	**0**-Always on **60**-1min **120**-2min **300**-5min **600**-10min **900**-15min **1800**-30min **3600**-1h	
Default	0	
Web UI	**Hybrid Mode** > **Basic** > **SIP Idle Timeout**	
Phone UI	☰ > **Settings** > **Device Settings** > **Hybrid Mode** > **SIP Idle Timeout**	

Parameter	**features.hybrid_mode.sip_callwaiting.enable**	**<y0000000000xx>.cfg**
Description	It configures that put an incoming SIP call to waiting mode and has a pop-up prompt during a Teams call.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	

Paging Configuration

When the hybrid mode is enabled, you can use paging feature on the phone.

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

Parameter	**linekey.X.type**[1]	**<y0000000000xx>.cfg**
Description	It configures the key feature.	
Permitted Values	**0**-N/A **15**-Line **24**-Paging **66**-Paging List	
Default	15 (VP59/MP58/MP58-WH/T58A/T56A: X= 1-16; MP54/T55A/CP960: 1) 0 (other line keys)	
Web UI	**Dsskey** > **Line Key** > **Line KeyX** > **Type**	
Phone UI	☰ > **Settings** > **Device Settings** > **DSS Keys** > **DSS Keys X** > **Type**	
Parameter	**linekey.X.line**[1]	**<y0000000000xx>.cfg**
Description	It configures the desired line to apply the line key feature.	
Permitted Values	1	
Default	1	
Web UI	**Dsskey** > **Line Key** > **Line KeyX** > **Line**	
Phone UI	☰ > **Settings** > **Device Settings** > **DSS Keys** > **DSS Keys X** > **Account ID**	
Parameter	**linekey.X.value**[1]	**<y0000000000xx>.cfg**
Description	It configures the value for line key features.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	**Dsskey** > **Line Key** > **Line KeyX** > **Value**	
Phone UI	☰ > **Settings** > **Device Settings** > **DSS Keys** > **DSS Keys X** > **Value**	
Parameter	**linekey.X.label**[1]	**<y0000000000xx>.cfg**

Description	It configures the label displayed on the phone screen. This is an optional configuration.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	**Dsskey** > **Line Key** > **Line KeyX** > **Label**	
Phone UI	☰ > **Settings** > **Device Settings** > **DSS Keys** > **DSS Keys X** > **Label**	
Parameter	**linekey.X.extension**[1]	**<y0000000000xx>.cfg**
Description	It configures the channel of the multicast paging group.	
Permitted Values	0 to 31	
Default	Blank	
Web UI	**Dsskey** > **Line Key** > **Line KeyX** > **Extension**	
Phone UI	☰ > **Settings** > **Device Settings** > **DSS Keys** > **DSS Keys X** > **Extension**	
Parameter	**features.auto_linekeys.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables to assign multiple line keys to associate with a specific account. **Note**: The number of the line keys is determined by “account.X.number_of_linekey”.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Parameter	**account.X.number_of_linekey**[2]	**<y0000000000xx>.cfg**
Description	It configures the number of line keys to be assigned with a specific account from the first unused one. If a line key is in used, the phone will skip to the next unused DSS key.	
Permitted Values	Integer from 1 to 999	
Default	1	
Parameter	**multicast.codec**	**<y0000000000xx>.cfg**
Description	It configures the codec for multicast paging.	
Permitted Values	PCMU, PCMA, G729, G722	
Default	G722	
Parameter	**multicast.paging_address.X.ip_address** [3]	**<y0000000000xx>.cfg**
Description	It configures the IP address and port number of the multicast paging group in the paging list.	
Permitted Values	IP address: port (224.0.0.1-239.255.255.255 port: 0-65535)	
Default	Blank	
Web UI	**Directory** > **Multicast IP** > **Paging List** > **Paging Address**	

Phone UI	☰ > **Settings** > **Device Settings** > **Paging List** > **Edit** > **Address**	
Parameter	**multicast.paging_address.X.label**[3]	**<y0000000000xx>.cfg**
Description	It configures the name of the multicast paging group to be displayed in the paging list. It will be displayed on the phone screen when placing the multicast paging calls.	
Permitted Values	String	
Default	Blank	
Web UI	**Directory** > **Multicast IP** > **Paging List** > **Label**	
Phone UI	☰ > **Settings** > **Device Settings** > **Paging List** > **Edit** > **Label**	
Parameter	**multicast.paging_address.X.channel**[3]	**<y0000000000xx>.cfg**
Description	It configures the channel of the multicast paging group in the paging list.	
Permitted Values	**0**-all the Yealink phones running old firmware version or Yealink phones listen to channel 0 or third-party available devices in the paging group can receive the RTP stream. **1 to 25**-the phones pre-configured to listen to the channel can receive the RTP stream. **26 to 30**-the Yealink phones pre-configured to listen to the channel can receive the RTP stream.	
Default	0	
Web UI	**Directory** > **Multicast IP** > **Paging List** > **Channel**	
Phone UI	☰ > **Settings** > **Device Settings** > **Paging List** > **Edit** > **Channel**	
Parameter	**multicast.listen_address.X.ip_address**[3]	**<y0000000000xx>.cfg**
Description	It configures the multicast address and port number that the phone listens to.	
Permitted Values	IP address: port (224.0.0.1-239.255.255.255 port: 0-65535)	
Default	Blank	
Web UI	**Directory** > **Multicast IP** > **Multicast Listening** > **Listening Address**	
Parameter	**multicast.listen_address.X.label**[3]	**<y0000000000xx>.cfg**
Description	It configures the label to be displayed on the phone screen when receiving the multicast paging calls.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	**Directory** > **Multicast IP** > **Multicast Listening** > **Label**	
Parameter	**multicast.listen_address.X.channel**[3]	**<y0000000000xx>.cfg**
Description	It configures the channel that the phone listens to.	

Permitted Values	**0**-the phone can receive an RTP stream of the pre-configured multicast address from the phones running old firmware version, from the phones listen to the channel 0, or from the available third-party devices. **1 to 25**-the phone can receive an RTP stream of the pre-configured multicast address on the channel 1 to 25 respectively from Yealink phones. **26 to 30**-the phone can receive the RTP stream of the pre-configured multicast address on the channel 26 to 30 respectively from Yealink phones.	
Default	0	
Web UI	**Directory** > **Multicast IP** > **Multicast Listening** > **Channel**	
Parameter	**multicast.receive_priority.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to handle the incoming multicast paging calls when there is an active multicast paging call on the phone.	
Permitted Values	**0**-Disabled, the phone will ignore the incoming multicast paging calls when there is an active multicast paging call on the phone. **1**-Enabled, the phone will receive the incoming multicast paging call with a higher priority and ignore the one with a lower priority.	
Default	1	
Web UI	**Directory** > **Multicast IP** > **Multicast Listening** > **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, 31 is the lowest priority.	
Permitted Values	**0**-Disabled, all incoming multicast paging calls will be automatically ignored when a voice call is in progress. **1**-1 **2**-2 **3**-3 ... **31**-31 If it is set to other values, the phone will receive the incoming multicast paging call with a higher or equal priority and ignore the one with a lower priority when a voice call is in progress.	
Default	31	
Web UI	**Directory** > **Multicast IP** > **Multicast Listening** > **Paging Barge**	

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

[2] X is the account ID. For VP59/MP58/MP58-WH/MP56/T58A/T56A, X=1-16; for MP54/T55A/CP960, X=1.

[3] X ranges from 1 to 31.

SIP Account Registration Configuration

In survivability app mode, you can register SIP accounts on the phone.

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

Parameter	**account.X.enable**[1]	**<MAC>.cfg**
Description	It enables or disables a specific account.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Account** > **Register** > **Line Active**	
Parameter	**account.X.label**[1]	**<MAC>.cfg**
Description	It configures the label to be displayed on the LCD screen.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	**Account** > **Register** > **Label**	
Parameter	**account.X.display_name**[1]	**<MAC>.cfg**
Description	It configures the display name for a specific account.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	**Account** > **Register** > **Display Name**	
Parameter	**account.X.auth_name**[1]	**<MAC>.cfg**
Description	It configures the user name for register authentication for a specific account.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	**Account** > **Register** > **Register Name**	
Parameter	**account.X.user_name**[1]	**<MAC>.cfg**
Description	It configures the register user name for a specific account.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	**Account** > **Register** > **User Name**	
Parameter	**account.X.password**[1]	**<MAC>.cfg**
Description	It configures the password for register authentication for a specific account.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	**Account** > **Register** > **Password**	

Parameter	**account.X.outbound_proxy_enable**[1]	**<MAC>.cfg**
Description	It enables or disables the phone to send requests to the outbound proxy server.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Account** > **Register** > **Enable Outbound Proxy Server**	
Parameter	**account.X.outbound_proxy.Y.address**[1][2]	**<MAC>.cfg**
Description	It configures the IP address (or domain name) of the outbound proxy server Y.	
Permitted Values	String within 256 characters	
Default	Blank	
Web UI	**Account** > **Register** > **Outbound Proxy Server**	
Parameter	**account.X.outbound_proxy.Y.port**[1][2]	**<MAC>.cfg**
Description	It configures the port of the outbound proxy server Y.	
Permitted Values	Integer from 0 to 65535	
Default	5060	
Web UI	**Account** > **Register** > **Outbound Proxy Server Y** > **Port**	
Parameter	**account.X.outbound_proxy_fallback_interval**[1]	**<MAC>.cfg**
Description	It configures the time interval (in seconds) for the phone to detect whether the working outbound proxy server is available by sending the registration request after the fallback server takes over call control.	
Permitted Values	Integer from 0 to 65535	
Default	3600	
Web UI	**Account** > **Register** > **Proxy Fallback Interval**	
Parameter	**account.X.sip_server.Y.address**[1][2]	**<MAC>.cfg**
Description	It configures the IP address (or domain name) of the SIP server Y.	
Permitted Values	String within 256 characters	
Default	Blank	
Web UI	**Account** > **Register** > **SIP Server Y** > **Server Host**	
Parameter	**account.X.sip_server.Y.port**[1][2]	**<MAC>.cfg**
Description	It configures the port of the SIP server Y.	
Permitted Values	Integer from 0 to 65535	
Default	5060	
Web UI	**Account** > **Register** > **SIP Server Y** > **Port**	
Parameter	**account.X.sip_server.Y.expires**[1][2]	**<MAC>.cfg**
Description	It configures the registration expiration time (in seconds) of SIP server Y.	
Permitted Values	Integer from 30 to 2147483647	

Default	3600	
Web UI	**Account** > **Register** > **SIP Server Y** > **Server Expires**	
Parameter	**account.X.sip_server.Y.retry_counts**[1][2]	**<MAC>.cfg**
Description	It configures the retry times for the phone to resend requests when the SIP server Y is unavailable or there is no response from the SIP server Y.	
Permitted Values	Integer from 0 to 20	
Default	3	
Web UI	**Account** > **Register** > **SIP Server Y** > **Server Retry Counts**	
Parameter	**account.X.sip_server.Y.transport_type**[1][2]	**<MAC>.cfg**
Description	It configures the type of transport protocol for a specific account.	
Permitted Values	**0**-UDP **1**-TCP **2**-TLS **3**-DNS-NAPTR, if no server port is given, the phone performs the DNS NAPTR and SRV queries for the service type and port.	
Default	0	
Web UI	**Account** > **Register** > **SIP Server Y** > **Transport**	

[1] X is the account ID. For MP58/MP58-WH/MP56/VP59/T58A/T56A, X=1-16; for MP54/T55A/CP960, X=1.

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

Account Codec Configuration

In survivability app mode, you can enable codecs for a specific account.

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

Parameter	**account.X.codec.<payload_type>.enable**[1]	**<MAC>.cfg**

Description	It enables or disables the specified audio codec. The name (payload_type) of the audio codec: **g722_1c_48kpbs**-G.722.1c (48kb/s) **g722_1c_32kpbs**-G.722.1c (32kb/s) **g722_1c_24kpbs**-G.722.1c (24kb/s) **g722_1_24kpbs**-G.722.1 (24kb/s) **g722**-G722 **pcmu**-PCMU **pcma**-PCMA **g729**-G729 **g726_16**-G726-16 **g726_24**-G726-24 **g726_32**-G726-32 **g726_40**-G726-40 **g723_53**-G723_53 **g723_63**-G723_63 **opus**-Opus **ilbc**-iLBC
Permitted Values	**0**-Disabled **1**-Enabled
Default	When the audio codec is G.722.1c (48kb/s), the default value is 1; When the audio codec is G.722.1c (32kb/s), the default value is 1; When the audio codec is G.722.1c (24kb/s), the default value is 1; When the audio codec is G.722.1 (48kb/s), the default value is 1; When the audio codec is G722, the default value is 1; When the audio codec is PCMU, the default value is 1; When the audio codec is PCMA, the default value is 1; When the audio codec is G729, the default value is 1; When the audio codec is G726-16, the default value is 0; When the audio codec is G726-24, the default value is 0; When the audio codec is G726-32, the default value is 0; When the audio codec is G726-40, the default value is 0; When the audio codec is G723_53, the default value is 0; When the audio codec is G723_63, the default value is 0; When the audio codec is Opus, the default value is 0; When the audio codec is iLBC, the default value is 0.

Web UI	**Account** > **Codec** > **Audio Codec**	
Parameter	**account.X.codec.<payload_type>.priority**[1]	**<MAC>.cfg**
Description	It configures the priority of the enabled audio codec. The name (payload_type) of the audio codec: **g722_1c_48kpbs**-G.722.1c (48kb/s) **g722_1c_32kpbs**-G.722.1c (32kb/s) **g722_1c_24kpbs**-G.722.1c (24kb/s) **g722_1_24kpbs**-G.722.1 (24kb/s) **g722**-G722 **pcmu**-PCMU **pcma**-PCMA **g729**-G729 **g726_16**-G726-16 **g726_24**-G726-24 **g726_32**-G726-32 **g726_40**-G726-40 **g723_53**-G723_53 **g723_63**-G723_63 **opus**-Opus **ilbc**-iLBC	
Permitted Values	Integer from 0 to 16	

Default	When the audio codec is G722.1c (48kb/s), the default value is 1; When the audio codec is G722.1c (32kb/s), the default value is 2; When the audio codec is G722.1c (24kb/s), the default value is 3; When the audio codec is G722.1 (24kb/s), the default value is 4; When the audio codec is G722, the default value is 5; When the audio codec is PCMU, the default value is 6; When the audio codec is PCMA, the default value is 7; When the audio codec is G729, the default value is 8; When the audio codec is G726_16, the default value is 0; When the audio codec is G726_24, the default value is 0; When the audio codec is G726_32, the default value is 0; When the audio codec is G726_40, the default value is 0; When the audio codec is G723_53, the default value is 0; When the audio codec is G723_63, the default value is 0; When the audio codec is Opus, the default value is 0; When the audio codec is iLBC, the default value is 0.	
Web UI	**Account** > **Codec** > **Audio Codec**	
Parameter	**account.X.codec.opus.para**[1]	**<MAC>.cfg**
Description	It configures the sample rate of the Opus audio codec.	
Permitted Values	**opus-fb**-Opus-FB (48KHz) **opus-swb**-Opus-SWB (24KHz) **opus-wb**-Opus-WB (16KHz) **opus-mb**-Opus-MB (12KHz) **opus-nb**-Opus-NB (8KHz)	
Default	opus-fb	
Web UI	**Account** > **Codec** > **Opus Sample Rate**	

[1] X is the account ID. For MP58/MP58-WH/MP56/VP59/T58A/T56A, X=1-16; for MP54/T55A/CP960, X=1.

Local Directory Configuration

In the survivability app mode, you can import the local contact files. The local directory can store up to 1000 contacts and 48 groups.

The following table lists the parameters you can use to import the local contact files.

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 Directory File**

Device Management

You can enable the device management feature to report phones information to the Yealink Device Management Platform, where you can view phones information and manage phones.

- Device Management Configuration

Device Management Configuration

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

Parameter	**static.dm.enable**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the device management feature.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Parameter	**static.dm.server.address**[1]	**<y0000000000xx>.cfg**
Description	It configures the server address of the Device Management Platform.	
Permitted Values	String	
Default	Blank	
Parameter	**static.dm.server.port**[1]	**<y0000000000xx>.cfg**
Description	It configures the port of the Device Management Platform.	
Permitted Values	Integer from 0 to 65535	
Default	443	

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

Managing the USB Camera UVC30 Room

Users can connect a UVC30 Room to the VP59 Teams phone to make video calls. After connected, you can upgrade the camera firmware or export the camera log.

- Upgrading UVC30 Camera
- Exporting Camera Log

Upgrading UVC30 Camera

You can update the connected UVC30 to the latest version.

Procedure

1. From the web user interface, go to **Camera** > **Upgrade**.
2. In the **Upgrade** block, click the white box to select a latest firmware from your local system.
3. Click **Upload**.

   It will prompt "It will take a few minutes to update the uvc firmware. Please do not power off!"
4. Click **OK**.

   The current firmware of the camera will be updated automatically after a few minutes.

Exporting Camera Log

You can export the camera log to help analyze camera problem.

Procedure

1. From the web user interface, go to **Camera** > **Upgrade**.
2. In the **Log** block, click **Export** to open the file download window, and then save the file to your local system.

Troubleshooting Methods

Yealink Teams 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
- Analyzing Configuration Files
- Exporting All the Diagnostic Files
- Device Status
- Resetting Device and Configuration
- Device Reboot
- Capturing the Current Screen of the Phone

Log Files

Yealink Teams 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
- 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 (<MAC>-boot.log and <MAC>-sys.log) 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 (<MAC>-boot.log and <MAC>-sys.log) locally. You can upload the local log files to the provisioning server or a specific server or export them to the local system.	
Default	1	
Web UI	**Settings** > **Configuration** > **Enable Local Log**	
Phone UI	☰ > **Settings** > **Device Settings** > **Debug(default password: admin)** > **Log enable**	
Parameter	**static.local_log.level**	**<y0000000000xx>.cfg**
Description	It configures the lowest level of local log information to be rendered to the <MAC>-sys.log file. When you choose a log level, it includes all events of an equal or higher severity level and excludes events of a lower severity level. The logging level you choose determines the lowest severity of events to log.	
Permitted Values	**0**-system is unusable **1**-action must be taken immediately **2**-critical condition **3**-error conditions **4**-warning conditions **5**-normal but significant condition **6**-informational	
Default	6	
Web UI	**Settings** > **Configuration** > **Local Log Level**	
Phone UI	☰ > **Settings** > **Device Settings** > **Debug(default password: admin)** > **Log level**	
Parameter	**static.local_log.max_file_size**	**<y0000000000xx>.cfg**

Description	It configures the maximum size (in KB) of the log files (<MAC>-boot.log and <MAC>-sys.log) 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 2048 to 20480	
Default	20480	
Web UI	**Settings** > **Configuration** > **Max Log File Size (2048-20480KB)**	
Parameter	**static.auto_provision.local_log.backup.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the device to upload the local log files (<MAC>-boot.log and <MAC>-sys.log) 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	
Parameter	**static.auto_provision.local_log.backup.upload_period**	**<y0000000000xx>.cfg**
Description	It configures the period (in seconds) of the local log files (<MAC>-boot.log and <MAC>-sys.log) uploads to the provisioning server or a specific server. **Note**: It works only if "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled).	
Permitted Values	Integer from 30 to 86400	
Default	30	
Parameter	**static.auto_provision.local_log.backup.path**	**<y0000000000xx>.cfg**

Description	It configures the upload path of the local log files (<MAC>-boot.log and <MAC>-sys.log). 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	
Parameter	**static.auto_provision.local_log.backup.append**	**<y0000000000xx>.cfg**
Description	It configures whether the uploaded local log files (<MAC>-boot.log and <MAC>-sys.log) overwrite the existing files or are appended to the existing files.	
Permitted Values	**0**-Overwrite **1**-Append (not applicable to TFTP Server)	
Default	0	
Parameter	**static.auto_provision.local_log.backup.append.limit_mode**	**<y0000000000xx>.cfg**
Description	It configures the behavior when local log files (<MAC>-boot.log and <MAC>-sys.log) on the provisioning server or a specific server reach the maximum file size.	
Permitted Values	**0**-Append Delete, the server will delete the old log, and the device will continue uploading log. **1**-Append Stop, the device will stop uploading log.	
Default	0	
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 (<MAC>-boot.log and <MAC>-sys.log) can be stored on the provisioning server or a specific server.	
Permitted Values	Integer from 200 to 65535	
Default	1024	
Parameter	static.auto_provision.local_log.backup.bootlog.upload_wait_tim	**<y0000000000xx>.cfg**
Description	It configures the waiting time (in seconds) before the device uploads the local log file (<MAC>-boot.log) to the provisioning server or a specific server after startup.	
Permitted Values	Integer from 1 to 86400	
Default	120	

Exporting the Log Files to a Local PC

Procedure

1. From the web user interface, go to **Settings** > **Configuration** > **Local Log**.
2. Turn on **Enable Local Log**
3. Select the desired value from the **Local Log Level** drop-down menu.
   The default local log level is “6”.
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.

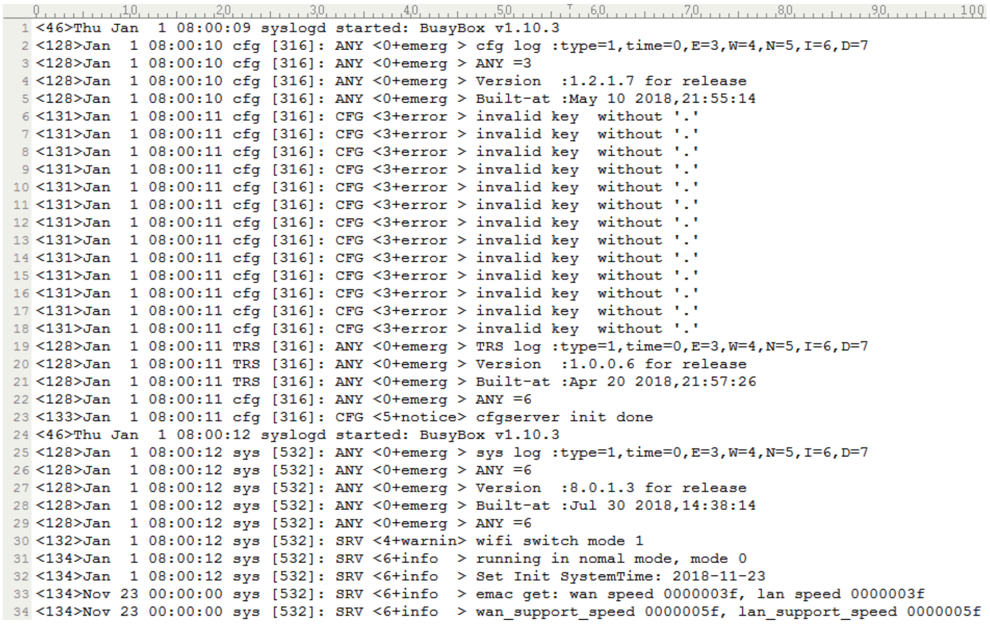
Viewing the Log Files

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

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

The default local log level is 6.

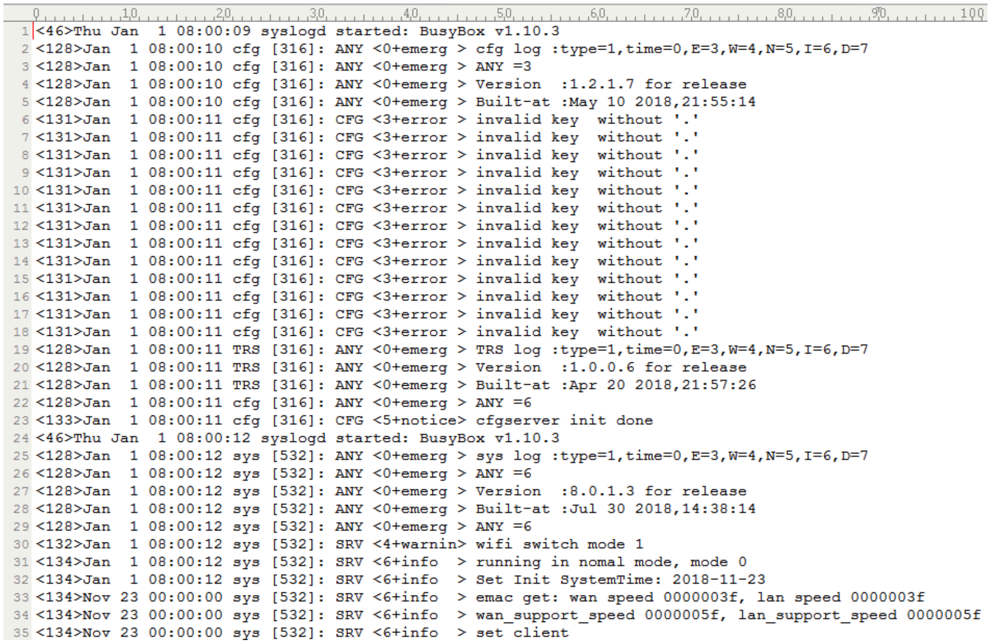
The following figure shows a portion of a boot log file (for example, 805EC031960A-boot.log):



```
<46>Thu Jan  1 08:00:09 syslogd started: BusyBox v1.10.3
<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
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > ANY =3
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Version  :1.2.1.7 for release
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Built-at :May 10 2018,21:55:14
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<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
<128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > Version  :1.0.0.6 for release
<128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > Built-at :Apr 20 2018,21:57:26
<128>Jan  1 08:00:11 cfg [316]: ANY <0+emerg > ANY =6
<133>Jan  1 08:00:11 cfg [316]: CFG <5+notice> cfgserver init done
<46>Thu Jan  1 08:00:12 syslogd started: BusyBox v1.10.3
<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
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > Version  :8.0.1.3 for release
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > Built-at :Jul 30 2018,14:38:14
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
<132>Jan  1 08:00:12 sys [532]: SRV <4+warnin> wifi switch mode 1
<134>Jan  1 08:00:12 sys [532]: SRV <6+info  > running in nomal mode, mode 0
<134>Jan  1 08:00:12 sys [532]: SRV <6+info  > Set Init SystemTime: 2018-11-23
<134>Nov 23 00:00:00 sys [532]: SRV <6+info  > emac get: wan speed 0000003f, lan speed 0000003f
<134>Nov 23 00:00:00 sys [532]: SRV <6+info  > wan_support_speed 0000005f, lan_support_speed 0000005f
```

The boot.log file reports the logs with all severity levels.

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



```
<46>Thu Jan  1 08:00:09 syslogd started: BusyBox v1.10.3
<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
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > ANY =3
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Version  :1.2.1.7 for release
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Built-at :May 10 2018,21:55:14
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<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
<128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > Version  :1.0.0.6 for release
<128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > Built-at :Apr 20 2018,21:57:26
<128>Jan  1 08:00:11 cfg [316]: ANY <0+emerg > ANY =6
<133>Jan  1 08:00:11 cfg [316]: CFG <5+notice> cfgserver init done
<46>Thu Jan  1 08:00:12 syslogd started: BusyBox v1.10.3
<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
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > Version  :8.0.1.3 for release
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > Built-at :Jul 30 2018,14:38:14
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
<132>Jan  1 08:00:12 sys [532]: SRV <4+warnin> wifi switch mode 1
<134>Jan  1 08:00:12 sys [532]: SRV <6+info  > running in nomal mode, mode 0
<134>Jan  1 08:00:12 sys [532]: SRV <6+info  > Set Init SystemTime: 2018-11-23
<134>Nov 23 00:00:00 sys [532]: SRV <6+info  > emac get: wan speed 0000003f, lan speed 0000003f
<134>Nov 23 00:00:00 sys [532]: SRV <6+info  > wan_support_speed 0000005f, lan_support_speed 0000005f
<134>Nov 23 00:00:00 sys [532]: SRV <6+info  > set client
```

The <MAC>-sys.log file reports the logs with a configured severity level and the higher. For example, if you have con\u0002figured the severity level of the log to be reported to the <MAC>-sys.log file to 4, then the log with a severity level of 0 to 4 will all be reported.

Syslog 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
- 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** > **Enable Syslog**	
Parameter	**static.syslog.server**	**<y0000000000xx>.cfg**
Description	It configures the IP address or domain name of the syslog server when exporting log to the syslog server.	
Permitted Values	IP address or domain name	

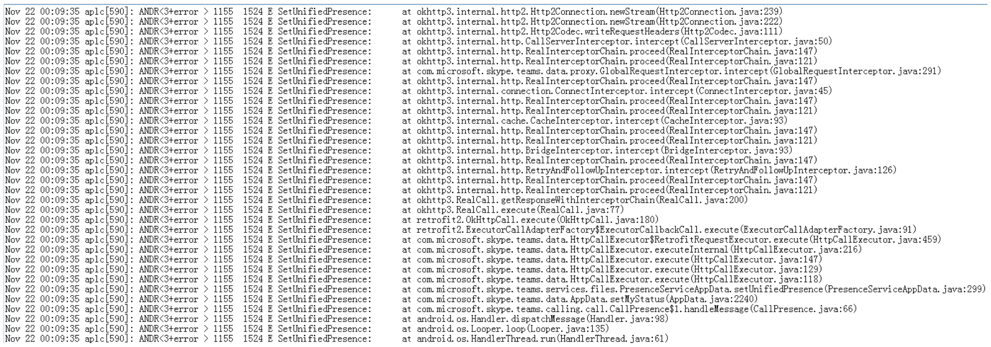
Default	Blank	
Web UI	**Settings** > **Configuration** > **Syslog** > **Syslog Server**	
Parameter	**static.syslog.server_port**	**<y0000000000xx>.cfg**
Description	It configures the port of the syslog server. **Example**: static.syslog.port = 515	
Permitted Values	Integer from 1 to 65535	
Default	514	
Web UI	**Settings** > **Configuration** > **Syslog** > **Syslog Server** > **Port**	
Parameter	**static.syslog.transport_type**	**<y0000000000xx>.cfg**
Description	It configures the transport protocol that the device uses when uploading log messages to the syslog server.	
Permitted Values	**0**-UDP **1**-TCP **2**-TLS	
Default	0	
Web UI	**Settings** > **Configuration** > **Syslog** > **Syslog Transport Type**	
Parameter	**static.syslog.level**	**<y0000000000xx>.cfg**
Description	It configures the lowest level of syslog information that displays in the syslog. When you choose a log level, it includes all events of an equal or higher severity level and excludes events of a lower severity level. The logging level you choose determines the lowest severity of events to log.	
Permitted Values	**0**-Emergency: system is unusable **1**-Alert: action must be taken immediately **2**-Critical: critical conditions **3**-Critical: error conditions **4**-Warning: warning conditions **5**-Warning: normal but significant condition **6**-Informational: informational messages	
Default	6	
Web UI	**Settings** > **Configuration** > **Syslog** > **Syslog Level**	
Parameter	**static.syslog.facility**	**<y0000000000xx>.cfg**
Description	It configures the facility that generates the log messages. **Note**: For more information, refer to RFC 3164.	

Permitted Values	**0**-kernel messages **1**-user-level messages **2**-mail system **3**-system daemons **4**-security/authorization messages (note 1) **5**-messages generated internally by syslogd **6**-line printer subsystem **7**-network news subsystem **8**-UUCP subsystem **9**-clock daemon (note 2) **10**-security/authorization messages (note 1) **11**-FTP daemon **12**-NTP subsystem **13**-log audit (note 1) **14**-log alert (note 1) **15**-clock daemon (note 2) **16**-local use 0 (local0) **17**-local use 1 (local1) **18**-local use 2 (local2) **19**-local use 3 (local3) **20**-local use 4 (local4) **21**-local use 5 (local5) **22**-local use 6 (local6) **23**-local use 7 (local7)	
Default	16	
Web UI	**Settings** > **Configuration** > **Syslog** > **Syslog Facility**	
Parameter	**static.syslog.prepend_mac_address.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the device to prepend the MAC address to the log messages exported to the syslog server.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Settings** > **Configuration** > **Syslog** > **Syslog Prepend MAC**	

Viewing the Syslog Messages on Your Syslog Server

You can view the syslog file in the desired folder on the syslog server. The location of the folder may differ from the syslog server. For more information, refer to the network resources.

The following figure shows a portion of the syslog:



```
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http2.Http2Connection.newStream(Http2Connection.java:239)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http2.Http2Connection.newStream(Http2Connection.java:222)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http2.Http2Codec.writeRequestHeaders(Http2Codec.java:111)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http.CallServerInterceptor.intercept(CallServerInterceptor.java:50)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:121)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at com.microsoft.skype.teams.data.proxy.GlobalRequestInterceptor.intercept(GlobalRequestInterceptor.java:291)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.connection.ConnectInterceptor.intercept(ConnectInterceptor.java:45)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:121)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.cache.CacheInterceptor.intercept(CacheInterceptor.java:93)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:121)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http.BridgeInterceptor.intercept(BridgeInterceptor.java:93)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http.RetryAndFollowUpInterceptor.intercept(RetryAndFollowUpInterceptor.java:126)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:121)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.RealCall.getResponseWithInterceptorChain(RealCall.java:200)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at okhttp3.RealCall.execute(RealCall.java:77)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at retrofit2.OkHttpCall.execute(OkHttpCall.java:180)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at retrofit2.ExecutorCallAdapterFactory$ExecutorCallbackCall.execute(ExecutorCallAdapterFactory.java:91)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at com.microsoft.skype.teams.data.HttpCallExecutor$RetrofitRequestExecutor.execute(HttpCallExecutor.java:459)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at com.microsoft.skype.teams.data.HttpCallExecutor.executeInternal(HttpCallExecutor.java:216)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at com.microsoft.skype.teams.data.HttpCallExecutor.execute(HttpCallExecutor.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at com.microsoft.skype.teams.data.HttpCallExecutor.execute(HttpCallExecutor.java:129)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at com.microsoft.skype.teams.data.HttpCallExecutor.execute(HttpCallExecutor.java:118)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at com.microsoft.skype.teams.services.files.PresenceServiceAppData.setUnifiedPresence(PresenceServiceAppData.java:299)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at com.microsoft.skype.teams.data.AppData.setMyStatus(AppData.java:2240)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at com.microsoft.skype.teams.calling.call.CallPresence$1.handleMessage(CallPresence.java:66)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at android.os.Handler.dispatchMessage(Handler.java:98)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at android.os.Looper.loop(Looper.java:135)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:      at android.os.HandlerThread.run(HandlerThread.java:61)
```

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 Teams devices, you can export the packets file to the local system and analyze it.

Yealink Teams 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.

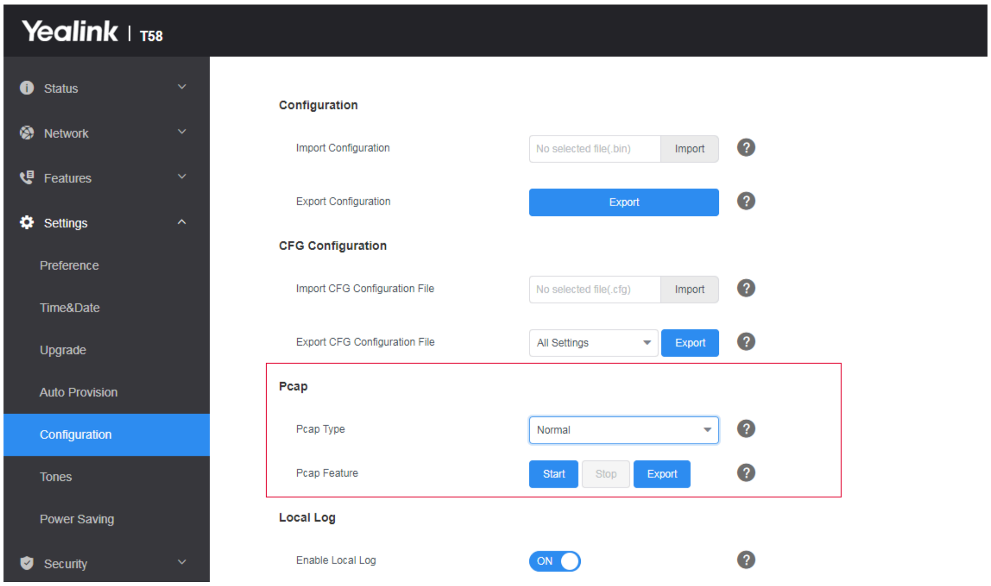
- Capturing the Packets in Normal Way
- Capturing the Packets in Enhanced Way

Capturing the Packets in Normal Way

Procedure

1. From the web user interface, go to **Settings** > **Configuration**.
2. Select **Normal** from the **Pcap Type** drop-down menu.
3. In the **Pcap Feature** field, click **Start** to start capturing signal traffic.
4. Reproduce the issue to get stack traces.
5. Click **Stop** in the **Pcap Feature** field to stop capturing.

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


Yealink | T58
Status
Network
Features
Settings
Preference
Time&Date
Upgrade
Auto Provision
Configuration
Tones
Power Saving
Security
Configuration
Import Configuration
No selected file(.bin)
Import
Export Configuration
Export
CFG Configuration
Import CFG Configuration File
No selected file(.cfg)
Import
Export CFG Configuration File
Export
Pcap
Pcap Type
Pcap Feature
Start
Stop
Export
Local Log
Enable Local Log

Export CFG Configuration File: All Settings

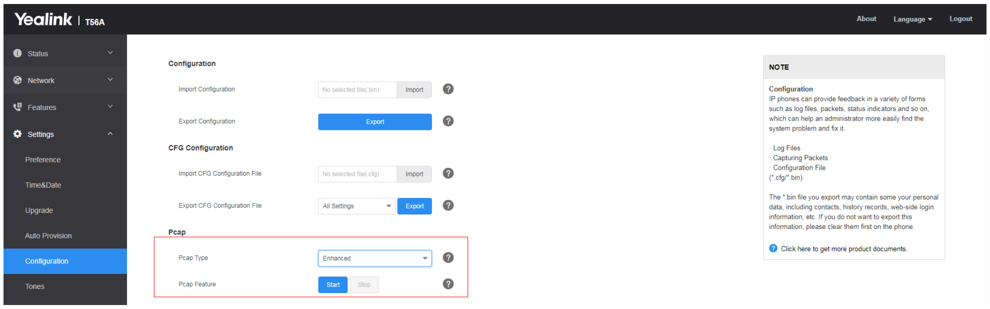
Pcap Type: Normal

Enable Local Log: ON

Capturing the Packets in Enhanced Way

Procedure

1. From the web user interface, go to **Settings** > **Configuration**.
2. Select **Enhanced** from the **Pcap Type** drop-down menu.
3. Click **Start** in the **Pcap Feature** field to start capturing signal traffic.
4. Reproduce the issue to get stack traces.
5. Click **Stop** in the **Pcap Feature** field to stop capturing.
6. Click **Export** to open the file download window, and then save the file to your local system.


Yealink | T56A
About
Language
Logout
Status
Network
Features
Settings
Preference
Time&Date
Upgrade
Auto Provision
Configuration
Tones
Configuration
Import Configuration
No selected file(.bin)
Import
Export Configuration
Export
CFG Configuration
Import CFG Configuration File
No selected file(.cfg)
Import
Export CFG Configuration File
Export
Pcap
Pcap Type
Pcap Feature
Start
Stop

Export CFG Configuration File: All Settings

Pcap Type: Enhanced

NOTE

Configuration

IP phones can provide feedback in a variety of forms such as log files, packets, status indicators and so on, which can help an administrator more easily find the system problem and fix it.

· Log Files
· Capturing Packets
· Configuration File
(*.cfg/*.bin)

The *.bin file you export may contain some your personal data, including contacts, history records, web-side login information, etc. If you do not want to export this information, please clear them first on the phone.

Click here to get more product documents.

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.

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 BIN Files from the Device
- Importing BIN Files from the Device

Exporting BIN Files from the Device

Procedure

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

Importing BIN Files from the Device

Procedure

1. From the web user interface, go to **Settings** > **Configuration** > **Configuration**.
2. In the **Import Configuration** block, click the white box to select 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** > **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 *.tar.

Procedure

1. From the web user interface, go 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 <MAC>-DiagnoseInfo.tarDiagnoseInfo.tar 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:

-
- Version information (Firmware Version, Hardware Version, Partner APP Version, Company Portal Version and Teams 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 ☰ > **Settings** > **Device Settings** > **About**. 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 **Login** 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. Go to ☰ > **Settings** > **Device Settings** > **Reboot**.
2. Select **Reboot phone**.

   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.

   The web user interface prompts the message “Reboot the system?"
3. Click **OK** to confirm the rebooting.

   The device begins at rebooting. Any reboot of the device may take a few minutes.

Capturing the Current Screen of the Phone

You can capture the screen display of the phone using the action URI. The phones can handle an HTTP or HTTPS GET request. The URI format is http(s)://<deviceIPAddress>/screencapture. The captured picture is saved as a BMP or JPEG file.

You can also use the URI “http(s)://<deviceIPAddress>/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 computer is included in the trusted IP address for Action URI on the phone. When you capture the screen display, the IP 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 the web user interface login.

- Enabling the Screen Capture via Phone User Interface
- Capturing the Current Screen of the Device via Web User Interface

Enabling the Screen Capture via Phone User Interface

Procedure

1. Go to ☰ > **Settings** > **Device Settings** > **Debug(default password: admin)** > **Screen Capture**.
2. Enable **Screen Capture**.

Capturing the Current Screen of the Device via Web User Interface

Before you begin

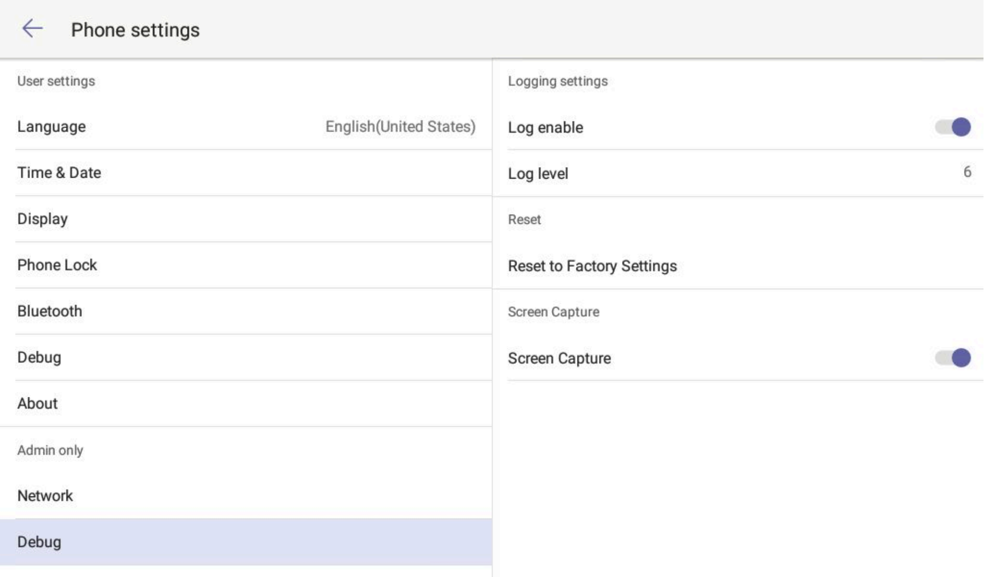
Before capturing the phone’s current screen, ensure that the Screen Capture feature is enabled via phone user interface.

Procedure

Enter request URI (for example, http://10.2.20.252/screencapture) in the browser's address bar and press the Enter key on the keyboard.

If it is the first time you capture the phone’s current screen using the computer, it will prompt you to enter the user name and password of the administrator if web browser does not remember the user name and password for web user interface login.

Then the browser will display an image of the phone’s current screen directly. You can save the image to your local system.



Phone settings
User settings
Language
English(United States)
Time & Date
Display
Phone Lock
Bluetooth
Debug
About
Admin only
Network
Debug
Logging settings
Log enable
Log level
6
Reset
Reset to Factory Settings
Screen Capture
Screen Capture

Troubleshooting Solutions

This section describes the solutions to common issues that may occur while using the Teams 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 ☰ > **Settings** > **Device Settings** > **Network(default password: admin)** > **WAN Port** > **IPv4 Type(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 Teams 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 displays "Offline"

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.

The device displays "Offline"

The device displays "Offline" when there is no available network on the device. Ensure that your device has connected to the wired network.

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.

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 provisioning server (FTP/TFTP server)
- Fail to export the system log from a syslog server

Fail to export the system log from a provisioning server (FTP/TFTP server)

Do one of the following:

- Ensure that the FTP/TFTP server is downloaded and installed on your local system.
- Ensure that you have configured the FTP/TFTP server address correctly via the web user interface on your device.
- Reboot the device. The configurations require a reboot to take effect.

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.