Yealink Teams ® HD IP Phone Administrator Guide

Version 15.20 | Dec.2019

Contents

Introduction..... 6
Related Documentations..... 6
Typographic and Writing Conventions..... 6
Recommended References..... 7

Getting Started..... 7
Initialization Process Overview..... 7
Loading the ROM File..... 8
Configuring the VLAN..... 8
Querying the DHCP (Dynamic Host Configuration Protocol) Server..... 8
Contacting the Provisioning Server..... 8
Updating Firmware..... 8
Downloading the Resource Files..... 8
Verifying Startup..... 8
Teams Feature License..... 9
Importing license via Web User Interface..... 9
Importing license Configuration..... 9

Phone Network..... 10
IPv4 and IPv6 Network Settings..... 10
IP Addressing Mode Configuration..... 10
IPv4 Configuration..... 11
IPv6 Configuration..... 13
DHCP Option for IPv4..... 16
Supported DHCP Option for IPv4..... 16
DHCP Option 160 and Option 161..... 17
DHCP Option 66 , Option 43 and Custom Option..... 17
DHCP Option 42 and Option 2..... 18
DHCP Option 12..... 18
DHCP Option 60..... 18
DHCP Option for IPv6..... 19
Supported DHCP Option for IPv6..... 19
VLAN..... 19
LLDP Configuration..... 19
CDP Configuration..... 20
Manual VLAN Configuration..... 21
DHCP VLAN..... 23
VLAN Setting Configuration..... 23
Internet Port and PC Port..... 24
Supported Transmission Methods..... 24
Internet Port and PC Port Configuration..... 24
802.1x Authentication..... 25
802.1x Authentication Configuration..... 26

Phone Provisioning..... 27
Provisioning Points to Consider..... 28

Boot Files, Configuration Files and Resource Files....28
Boot Files....28
Configuration Files....31
Resource Files....34
Files Download Process....34
Provisioning Methods....35
Provisioning Methods Priority....35
Manual Provisioning....36
Central Provisioning....39
Setting Up a Provisioning Server....41
Supported Provisioning Protocols....41
Supported Provisioning Server Discovery Methods....42
Configuring a Provisioning Server....43

Provisioning Phone on the Microsoft Teams & Skype for Business Admin Center....44
Device Management....44
Editting Your Device Info....44
Customizing the Displayed Elements of Devices....44
Viewing the Device Details....45
Assigning Configuration Profile to Devices....45
Diagnostic Devices....45
Updating Device Software....45
Restarting Your Devices....46
Configuration Profiles Management....46
Creating a Configuration Profile....46
Editting a Configuration Profile....46
Assigning Configuration Profile to Devices....47

Firmware Upgrade....47
Firmware for Each Phone Model....47
Firmware Upgrade Configuration....48

Phone Customization....48
Language....48
Language Display Configuration....49
Screen Saver....49
Screensaver Configuration....50
Backlight....51
Backlight Brightness and Time Configuration....51
Time and Date....52
Time Zone....52
NTP Settings....54
DST Settings....55
Time and Date Manual Configuration....59
Time and Date Format Configuration....60
Tones....61
Supported Tones....61
Tones Configuration....61
Power Saving....62
Power Saving Configuration....63
Power LED Indicator....64

Power LED Indicator Configuration 65
Bluetooth 65
Bluetooth Configuration 66

Security Features 66
User and Administrator Identification 66
User and Administrator Identification Configuration 67
User Access Level Configuration 68
Phone Lock 68
Phone Lock Configuration 68
Transport Layer Security (TLS) 69
Supported Cipher Suites 69
Supported Trusted and Server Certificates 70
TLS Configuration 72
Encrypting Configuration Files 74
Configuration Files Encryption Tools 74
Configuration Files Encryption and Decryption 75
Encryption and Decryption Configuration 75
Example: Encrypting Configuration Files 77

Troubleshooting Methods 78
Log Files 78
Local Log 78
Syslog Log 83
Packets Capture 86
Capturing the Packets via Web User Interface 86
Ethernet Software Capturing Configuration 87
Analyzing Configuration Files 88
Exporting BIN Files from the Phone 88
Importing BIN Files from the Phone 88
Exporting All the Diagnostic Files 89
Phone Status 89
Viewing the Phone Status 89
Resetting Phone and Configuration 90
Resetting the phone to Default Factory Settings 90
Resetting the phone to Custom Factory Settings 90
Deleting the Custom Factory Settings Files 91
Phone Reboot 91
Rebooting the Phone via Phone User Interface 91
Rebooting the Phone via Web User Interface 91
Capturing the Current Screen of the Phone 92
Enabling the Screen Capture via Phone User Interface 92
Capturing the Current Screen of the Phone via Web User Interface 92

Troubleshooting Solutions 93
IP Address Issues 93
The IP phone does not get an IP address 93
IP Conflict 93
Specific format in configuring IPv6 on Yealink IP phones 94
Time and Date Issues 94
Display time and date incorrectly 94
Display Issues 94
The phone LCD screen blank 94

The phone displays “Offline”....94
Firmware and Upgrading Issues....95
Fail to upgrade the phone firmware....95
The phone does not update the configurations....95
System Log Issues....95
Fail to export the system log from a provisioning server (FTP/TFTP server)....95
Fail to export the system log from a syslog server....95
Password Issues....95
Restore the administrator password....96

Introduction

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

Yealink T58A/T56/CP960 Microsoft Teams IP phones are the collaborative phones with Microsoft. As an administrator, you can do the following with this guide:

- Manage the Teams IP Phones with Microsoft Teams & Skype for Business Admin Center
- Set up a provisioning server.
- Provision the phone with features and settings.
- Troubleshoot, update and maintain the phones.

The information detailed in this guide is applicable to the following Yealink devices running firmware version XX.15.0.20:

- T58A Teams IP Phones
- T56A Teams IP Phones
- CP960 Teams IP Phones

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

- *Related Documentations*
- *Typographic and Writing Conventions*
- *Recommended References*

Related Documentations

The following related documents are available:

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

  The *Auto Provisioning Guide* is to serve as a basic guidance for provisioning Yealink Teams IP Phones with a provisioning server. If you are the 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 (e.g., Tap **Settings**>**Device Settngs**). Also used to emphasize text (e.g., **Important!**).

Italics	Used to emphasize text, to show the example values or inputs (format of examples: http(s)://[IPv6address]) .
Blue Text	Used for cross references to other topics related to this topic (for example, Ring Tones), for hyperlinks toexternal sites and documents, for example, RFC 3315.

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

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

Recommended References

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

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

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

This guide mainly takes the T58A Teams phone as example for reference. For more details on other Teams IP Phones, refer to *Yealink Teams phone-specific user guide*.

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

Getting Started

This chapter describes where Teams IP Phones fit in your network, and provides basic initialization instructions for Teams IP Phones.

- *Initialization Process Overview*
- *Verifying Startup*
- *Teams Feature License*

Initialization Process Overview

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

- *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 phone. The phone comes from the factory with a ROM file preloaded. During initialization, the phone runs a bootstrap loader that loads and executes the ROM file.

Configuring the VLAN

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

Querying the DHCP (Dynamic Host Configuration Protocol) Server

The phone is capable of querying a DHCP server.

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

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

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

Contacting the Provisioning Server

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

Updating Firmware

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

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

Downloading the Resource Files

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

Verifying Startup

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

1. The power LED indicators of T58A/T56A Teams IP Phones glow red.

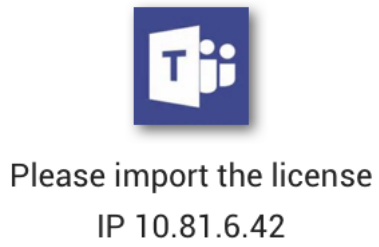
   The mute touch key LED indicators of CP960 Teams IP Phones glow red.

2. The message “Initializing… please wait” appears on the touch screen when the phones start up.

   The message “Initializing…”appears on the touch screen of CP960 Teams IP Phones when start up.
3. The phones enter the language selection interface.

Teams Feature License

Yealink offers T58A/T56A/CP960 IP phones configured for use with Microsoft Teams. Teams feature license allows user to use Yealink IP phones with Teams features directly. If the phone has not imported a license yet, the screen will be shown as below:



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

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

Note:

If the phone 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 upgrage to the Teams firmware.

- *Importing license via Web User Interface*
- *Importing license Configuration*

Related information

Firmware Upgrade

Importing license via Web User Interface

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

Procedure

1. From the web user interface, navigate to **Security** > **License** > **Import License**.
2. In the **Upload License File** block, click the white box to upload 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	<y0000000000xx>.cfg

Description	It configures the access URL of the Teams feature license. **Example**: lync_license_dat.url = http://192.168.1.20/License_$MAC.dat The phones will replace the characters “$MAC” with its MAC addresses during autoprovisioning. For example, the MAC address of one T58A Teams phone is 00156543EC97. When performing auto provisioning, the phone will request to downloadthe 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** > **Import License**

Phone Network

Yealink Teams IP Phones operate on an Ethernet local area network (LAN). You can configure the local area network to accommodate a number of network designs, which varies by organizations and Yealink Teams IP Phones.

- *IPv4 and IPv6 Network Settings*
- *DHCP Option for IPv4*
- *DHCP Option for IPv6*
- *VLAN*
- *Internet Port and PC Port*
- *802.1x Authentication*

IPv4 and IPv6 Network Settings

Teams IP Phones support IPv4 addressing mode, IPv6 addressing mode, as well as an IPv4&IPv6 dual-stack addressing mode.After connected to the wired network, the phones 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 IP Phones 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(Admin only, default password: admin)** > **WAN Port** > **IP Mode**

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

IPv4 Configuration

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

Parameter	**static.network.internet_port.type**[1]	**<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 Addres	
Default	0	
Web UI	**Network** > **Basic** > **IPv4 Config** > **Configuration Type**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, default password: admin)** > **WAN Port** > **IPv4 Type**	
Parameter	**static.network.internet_port.ip**[1]	**<MAC>.cfg**
Description	It configures the IPv4 address. **Example**: static.network.internet_port.ip = 192.168.1.20 **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 Address).	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	**Network** > **Basic** > **IPv4 Config** > **Configuration Type(Static IP)** > **IP Address**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, 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. **Example**: static.network.internet_port.mask = 255.255.255.0 **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 Address).	
Permitted Values	Subnet Mask	
Default	Blank	
Web UI	**Network** > **Basic** > **IPv4 Config** > **Configuration Type(Static IP)** > **Subnet Mask**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, 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. **Example**: static.network.internet_port.gateway = 192.168.1.254 **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 Address).	
Permitted Values	IPv4 gateway address	
Default	Blank	
Web UI	**Network** > **Basic** > **IPv4 Config** > **Configuration Type(Static IP)** > **Default Gateway**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, default password: admin)** > **WAN Port** > **IPv4 Type(Static IP)** > **Default Gateway**	
Parameter	**static.network.primary_dns**[1]	**<MAC>.cfg**
Description	It configures the primary IPv4 DNS server. **Example**: static.network.primary_dns = 202.101.103.55 **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	Primary IPv4 DNS server 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(Admin only, default password: admin)** > **WAN Port** > **IPv4 Type(Static IP)** > **Pri.DNS** Or ☰ > **Settings** > **Device Settings** > **Network(Admin only, 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. **Example**: static.network.secondary_dns = 202.101.103.54 **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	Secondary IPv4 DNS server 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(Admin only, default password: admin)** > **WAN Port** > **IPv4 Type(Static IP)** > **Sec.DNS** Or ☰ > **Settings** > **Device Settings** > **Network(Admin only, default password: admin)** > **WAN Port** > **IPv4 Type(DHCP)** > **IPv4 Static DNS(Enable)** > **Sec.DNS**	

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

IPv6 Configuration

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

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

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

Parameter	**static.network.ipv6_internet_port.type**[1]	**<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 Address	
Default	0	
Web UI	**Network** > **Basic** > **IPv6 Config** > **Configuration Type**	

Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, default password: admin)** > **WAN Port** > **IPv6 Type**	
Parameter	**static.network.ipv6_internet_port.ip**[1]	**<MAC>.cfg**
Description	It configures the IPv6 address. **Example**: static.network.ipv6_internet_port.ip = 2026:1234:1:1:215:65ff:fe1f:caa **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 Address).	
Permitted Values	IPv6 Address	
Default	Blank	
Web UI	**Network** > **Basic** > **IPv6 Config** > **Configuration Type(Static IP)** > **IP Address**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, 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 Address).	
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(Admin only, 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. **Example**: static.network.ipv6_internet_port.gateway = 3036:1:1:c3c7:c11c:5447:23a6:255 **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 Address).	
Permitted Values	IPv6 gateway address	
Default	Blank	
Web UI	**Network** > **Basic** > **IPv6 Config** > **Configuration Type(Static IP)** > **Default Gateway**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, default password: admin)** > **WAN Port** > **IPv6 Type(Static IP)** > **Default Gateway**	
Parameter	**static.network.ipv6_primary_dns**[1]	**<MAC>.cfg**

Description	It configures the primary IPv6 DNS server. **Example**: static.network.ipv6_primary_dns = 3036:1:1:c3c7:c11c:5447:23a6:256 **Note**: It works only if "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	Primary IPv6 DNS server 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(Admin only, default password: admin)** > **WAN Port** > **IPv6 Type(Static IP)** > **Pri.DNS** Or ☰ > **Settings** > **Device Settings** > **Network(Admin only, default password: admin)** > **WAN Port** > **IPv6 Type(DHCP)** > **IPv6 Static DNS(Enable)** > **Pri.DNS**	
Parameter	**static.network.ipv6_primary_dns**[1]	**<MAC>.cfg**
Description	It configures the secondary IPv6 DNS server. **Example**: static.network.ipv6_secondary_dns = 2026:1234:1:1:c3c7:c11c:5447:23a6 **Note**: It works only if "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	Secondary IPv6 DNS server 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(Admin only, default password: admin)** > **WAN Port** > **IPv6 Type(Static IP)** > **Sec.DNS** Or ☰ > **Settings** > **Device Settings** > **Network(Admin only, 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 Teams 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 phone will reboot to make the change take effect.

DHCP Option for IPv4

The Teams phone can obtain IPv4-related parameters in an IPv4 network via DHCP option.

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

- *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 Teams IP Phones.

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

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

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

- *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	**Network** > **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 the value of the parameter "static.auto_provision.dhcp_option.enable" is set to 1 (On).	
Permitted Values	**Integer from 128 to 254**	
Default	**160,161**	
Web UI	**Network** > **Auto Provision** > **Custom Option(128~254)**	

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

DHCP Option 66 , Option 43 and Custom Option

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

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

To obtain the server address via DHCP option, make sure you have configured the DHCP option on the phone. 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 IP Phones 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 phone 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 phone.	
Permitted Values	String within 99 characters	
Default	For T58A Teams IP Phones: SIP-T58 For T56A Teams IP Phones: SIP-T56A For CP960 Teams IP Phones: SIP-CP960	

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

DHCP Option 60

DHCP option 60 is used to 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	**Network** > **Auto Provision** > **DHCP Option Value**	

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

DHCP Option for IPv6

The Teams phone can obtain IPv6-related parameters in an IPv6 network via 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 IP phones.

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

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

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

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

- *LLDP Configuration*
- *CDP Configuration*
- *Manual VLAN Configuration*
- *DHCP VLAN*
- *VLAN Setting Configuration*

LLDP Configuration

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

When LLDP feature is enabled on the phones, the phones periodically advertise their own information to the directly connected LLDP-enabled switch. The phones can also receive LLDP packets from the connected switch. When the application type is “voice”, the phones decide whether to update the VLAN configurations obtained from the LLDP packets. When the VLAN configurations on the phones are different from the ones sent by the switch, the phones

perform an update and reboot. This allows the phones 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 (Cisco Discovery Protocol) feature on the phone.	
Permitted Values	**0**-Disabled **1**-Enabled, the phone will attempt to determine its VLAN ID through LLDP.	
Default	1	
Web UI	**Network** > **Advanced** > **LLDP** > **Active**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, 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 phone sends the LLDP (Linker Layer Discovery Protocol) 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** > **LLDP Interval (1~3600s)**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, default password: admin)** > **LLDP** > **LLDP Interval**	

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

CDP Configuration

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

If the CDP feature is enabled on the phones, the phones will periodically advertise their own information to the directly connected CDP-enabled switch. The phones can also receive CDP packets from the connected switch. If the VLAN configurations on the phones are different from the ones sent by the switch, the phones will perform an update and reboot. This allows you to connect the phones 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 (Cisco Discovery Protocol) feature on the phone.	
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(Admin only, 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 (Cisco Discovery Protocol) 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(Admin only, default password: admin)** > **CDP** > **CDP Interval**	

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

Manual VLAN Configuration

VLAN is disabled on the phones by default. You can configure VLAN for the Internet port and PC port manually. Before configuring VLAN on the phone, you need to obtain the VLAN ID from your network administrator. PC port is not applicable to CP960, 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(Admin only, 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(Admin only, 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 1 to 7	
Default	0	
Web UI	**Network** > **Advanced** > **VLAN** > **WAN Port** > **Priority**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, 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). It is not applicable to CP960 Phones.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Network** > **Advanced** > **VLAN** > **PC Port** > **Active**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, 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). It is not applicable to CP960 Phones.	
Permitted Values	Integer from 1 to 4094	
Default	1	
Web UI	**Network** > **Advanced** > **VLAN** > **PC Port** > **VID**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, 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). It is not applicable to CP960 Phones.	
Permitted Values	Integer from 1 to 7	
Default	0	
Web UI	**Network** > **Advanced** > **VLAN** > **PC Port** > **Priority**	

Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, default password: admin)** > **VLAN** > **PC Port** > **Priority**

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

DHCP VLAN

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

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 phone.	
Permitted Values	**0**-Disabled **1**-Enabled.	
Default	1	
Web UI	**Network** > **Advanced** > **DHCP VLAN** > **Active**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, default password: admin)** > **DHCP VLAN**	
Parameter	**static.network.vlan.dhcp_option**[1]	**<y0000000000xx>.cfg**
Description	It configures the DHCP option from which the phone 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	6132	
Web UI	**Network** > **Advanced** > **DHCP VLAN** > **Option**	
Phone UI	☰ > **Settings** > **Device Settings** > **Network(Admin only, default password: admin)** > **DHCP VLAN** > **Option**	

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

VLAN Setting Configuration

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

Parameter	**static.network.vlan.vlan_change.enable**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to obtain VLAN ID using lower preference of VLAN assignment method or to close the VLAN feature when the phone cannot obtain VLAN ID using the current VLAN assignment method. The priority of each method is: LLDP/CDP>Manual>DHCP VLAN.	

Permitted Values	**0**-Disabled **1**-Enabled, the phone will attempt to use the lower priority method when failing to obtain the VLAN ID using higher priority method. If all the methods are attempted, the phone will disable VLAN feature.
Default	0

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

Internet Port and PC Port

Yealink Teams IP Phones support two Ethernet ports: Internet port and PC port. You can enable or disable the PC port on the phones. PC port is not applicable to CP960 Phones.

- *Supported Transmission Methods*
- *Internet Port and PC Port Configuration*

Supported Transmission Methods

Three optional methods of transmission configuration for the phone 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 phones))

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

Internet Port and PC Port Configuration

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

Parameter	**static.network.pc_port.enable**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the PC port. **Note**: It is not applicable to CP960 Phones.	
Permitted Values	**0**-Disabled **1**-Auto Negotiation	
Default	1	
Web UI	**Network** > **PC Port** > **PC Port Active**	
Parameter	**static.network.internet_port.speed_duplex**[1]	**<y0000000000xx>.cfg**
Description	It configures the 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 phones)	
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. It is not applicable to CP960 Phones.	
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	
Web UI	**Network** > **AdvancedPort 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 same as the configured tag for the PC port, else forward the packets directly. It is not to CP960 Phones.	
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	

[1]If you change this parameter, the phone 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(Admin only, 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. **Example**: static.network.802_1x.identity = yealink **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(Admin only, 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. **Example**: static.network.802_1x.md5_password = admin123 **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(Admin only, 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. **Example**: static.network.802_1x.root_cert_url = http://192.168.1.10/ca.pem **Note**: It works only if "static.network.802_1x.mode" is set to 2, 3, 4, 5, 6 or 7. If the authentication method is EAP-FAST, you also need to set "static.network.802_1x.eap_fast_provision_mode" to 1 (Authenticated Provisioning). The format of the certificate must be *.pem, *.crt, *.cer or *.der.	
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. **Example**: static.network.802_1x.client_cert_url = http://192.168.1.10/client.pem **Note**: It works only if "static.network.802_1x.mode" is set to 2 (EAP-TLS). The format of the certificate must be *.pem.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Network** > **Advanced** > **802.1x** > **Device Certificates**	

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

Phone Provisioning

This chapter provides basic instructions for setting up your IP phones 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 phones on the Microsoft Teams & Skype for Business Admin Center or using a provisioning server.

- Provisioning phones 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 phones, we recommend you to use central provisioning method as your primary configuration method. A provisioning server maximizes the flexibility when you install, configure, upgrade and manage the phones, 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 Phone 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 phone features and apply feature settings to phones. 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 IP Phones support boot files. The boot files maximize the flexibility to allow you to customize features and settings for multiple phones.

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

- For all phones
- For a group of phones
- For specific phone models
- For a single phone

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

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

- *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 phones. You can use a common boot file to apply common feature settings to all of the phones rather than a single phone.

MAC-Oriented Boot File

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

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

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

Boot File Attributes

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

Attributes	Description
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
include:config <xxx.cfg> 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): **Note:** For example, sip.cfg, HTTP Directory/sip.cfg • Absolute path (or URL): **Note:** 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 phone model names are: T58A, T56A and CP960. Multiple phone models are separated by commas. For example, [T58A, T56A].

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 configuration files is left blank, or if a non-static parameter in configuration files is deleted or commented out, the factory default value takes effect. **0-(Disabled)** -If the value of a parameter in 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** (**AppendMode**), the phone downloads its own model-specific configuration files, and downloads other model-unspecified configuration files. **1-Enabled** (**ExcludeMode**), the phone attempts to download its own model-specific configuration files; if there is 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"
   - include:config "http://10.2.5.206/configure/screensaver.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 T58S 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 supports two configuration template files: Common CFG file and MAC-Oriented CFG file.

These configuration files contain two kinds of parameters:

- Static: The parameters start with a prefix “static.”, for example, static.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 Yealink Teams IP Phones automatically through configuration files stored in a provisioning server.

Note: For protecting against unauthorized access, you can encrypt configuration files. For more information on encrypting configuration files, refer to *Encrypting 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 phone, such as language and volume. It will be effective for all phones in the same model. The common CFG file has a fixed name for each phone model.

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

Phone Model	Common CFG file
T58A	y000000000058.cfg
T56A	y000000000056.cfg
T48G	y000000000073.cfg

MAC CFG File

Yealink supports two MAC CFG file: MAC-Oriented file and MAC-local CFG file, which are both named after the MAC address of the phone. For example, if the MAC address of an phone 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 phone. You can obtain it from the bar code on the back of the phone.

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

MAC-Oriented CFG File

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

MAC-local CFG File

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

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

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

Note: The non-static changes that you made before enabling the provisioning priority mechanism are not saved in the generated MAC-local file, but the previous settings still take effect on the phone. The static changes 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

By default, the MAC-local.cfg file is stored on the phone. You can configure the phone to upload this file to the provisioning server each time the file updates.

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 phone to keep user’s personalized settings after auto provisioning. **Note**: The provisioning priority mechanism (phone/web user interface >central provisioning >factory defaults) takes effect only if the value of this parameter is set to 1 (Enabled). If “overwrite_mode” is set to 1 in the boot file, the value of this parameter will be set to 1 (Enabled).	
Permitted Values	**0**-Disabled **1**-Enabled, the <MAC>-local.cfg file is generated and personalized non-static settings configured via web or phone user interface will be kept after auto provisioning.	
Default	1	

Clearing MAC-local CFG File

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

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

Note: The **Reset user settings** option on the web/phone user interface 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, screensaver.cfg). You can rearrange the parameters in the configuration template file and create your own

configuration files with parameters you want. This flexibility is especially useful when you want to apply specific settings to a group of phones.

- *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

   screensaver.wait_time= 60
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 phones. • 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
[$MODEL]	The [$MODEL] can be added in front of configuration parameter to specify the value for specific phone models. $MODEL represents the phone model. The valid names of the phone model are: T58A, T56A and CP960. Multiple phone models are separated by commas. For example, [T58A, CP960]. **Note**: The phone updates model-specific configurations and those model-unspecified configurations.

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

Resource Files

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

Tip: If you want to specify the desired phone to use the resource file, the access URL of resource file should be specified in the MAC-Oriented CFG file. During auto provisioning, the phones will request the resource files in addition to the configuration files.

- *Supported Resource Files*

Supported Resource Files

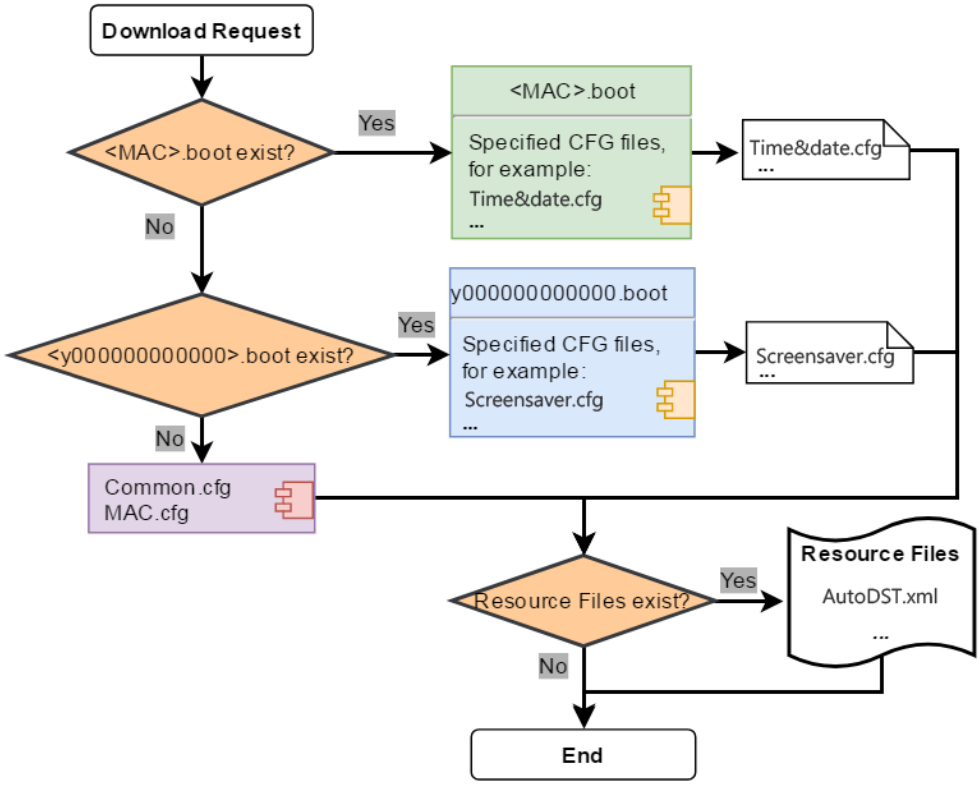
Yealink supplies some template of resource files for you, so you can directly edit the files as required.

The following table lists the resource files Yealink supplies:

Template File	File Name	Description	Reference in Section
AutoDST Template	AutoDST.xml	Add or modify time zone and DST settings.	DST Settings
Language Packs	For example, 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 phones, the phones will request to download the boot files, configuration files and resource files from the provisioning server according to the following flowchart:



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

Note: "specific_model.excluded_mode" determines which configuration files referenced in the boot file to be downloaded.

Provisioning Methods

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

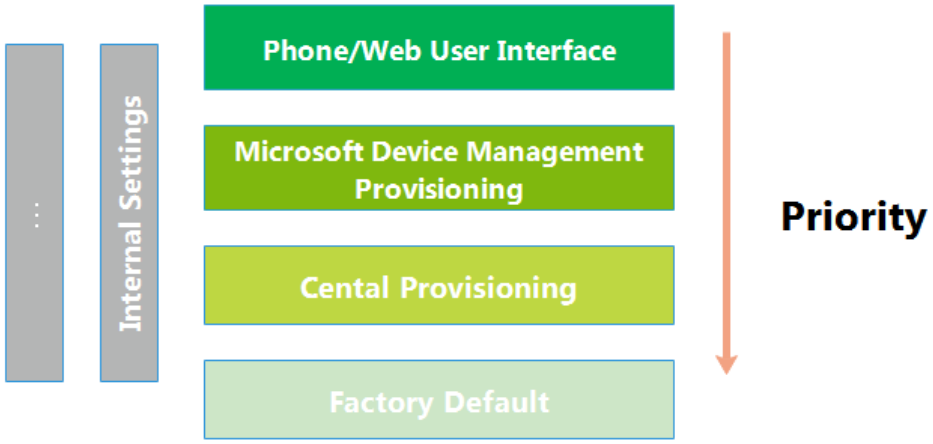
- **Central Provisioning**: configuration files stored on a central provisioning server.
- **Manual Provisioning:**operations on the web user interface or phone user interface.

- *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 Phone on the Microsoft Teams & Skype for Business Admin Center

Manual Provisioning

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

- *Web User Interface Access*
- *Phone User Interface*

Web User Interface Access

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

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

Accessing the Web User Interface

Procedure

1. Find the phone IP address. Tap ☰ > **Settings** > **Device Settings** > **Language** on the phone.
2. Enter the IP address in the address bar of a web browser on your PC.

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

Web Server Type Configuration

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

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

Parameter	static.wui.http_enable[1]	<y0000000000xx>.cfg
Description	It enables or disables the user to access the web user interface of the phone 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(Admin only, 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 phone 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(Admin only, 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 phone 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(Admin only, default password: admin)** > **Web Server** > **HTTPS 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 phone using the HTTP 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(Admin only, default password: admin)** > **Web Server** > **HTTPS Port**

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

Importing CFG Configuration Files to Phone

You can import the configuration files from local to the phones via the web user interface. The configuration files contain the changes for phone features, and these changes will take effect immediately after the configuration files are imported.

Procedure

1. From the web user interface, navigate 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** to import the configuration file.

Exporting CFG Configuration Files from Phone

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

About this task

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

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

Procedure

1. From the web user interface, navigate to **Settings** > **Configuration** > **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

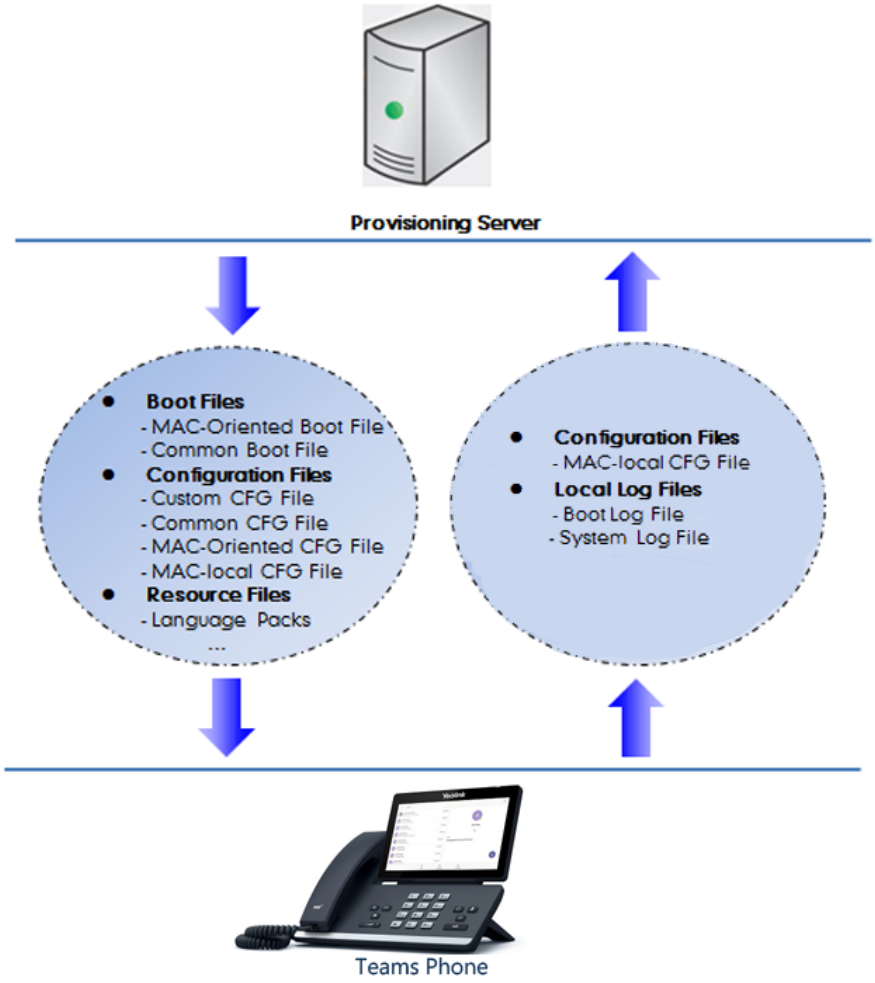
Phone user interface makes configurations available to users and administrators; but the ☰ > **Settings** > **Device Settings** > **Admin only** option is only available to administrators and requires an administrator password (default: admin).

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

Central Provisioning

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

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



Using the configuration files to provision the phones and to modify features and configurations is called the central provisioning method. You can use a text-based editing application to edit configuration files, and then store configuration files to a provisioning server. Teams IP Phones can be centrally provisioned from a provisioning server. For more information on the provisioning server, refer to *Setting Up a Provisioning Server*.

Teams IP Phones can obtain the provisioning server address during startup. Then phones download configuration files from the provisioning server, resolve and update the configurations written in configuration files. This entire process is called auto provisioning. For more information on auto provisioning, refer to *Yealink_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 phone whether to perform the auto provisioning when powered on.	
Permitted Values	**0**-Off **1**-On, the phone 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 phone 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 phone to perform the auto provisioning weekly.	
Permitted Values	**0**-Off **1**-On, the phone 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 phone to perform the auto provisioning weekly. **Example**: static.auto_provision.weekly.dayofweek = 01 It means the phone will perform an auto provisioning process every Sunday and Monday. **Note**: It works only if "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 phone 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 phone will reboot to make the change take effect.

Setting Up a Provisioning Server

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

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

Supported Provisioning Protocols

Yealink Teams IP Phones support several transport protocols for provisioning:

- Trivial File Transfer Protocol (TFTP)
- File Transfer Protocol (FTP)

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

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

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

Supported Provisioning Server Discovery Methods

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

The phone supports the following methods to discover the provisioning server address:

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

- *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 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 IP phone 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_options**	**<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 phone will be used.

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

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

Configuring a Provisioning Server

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

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

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

Microsoft Teams & Skype for Business Admin Center allows administrators to efficiently realize centralized management for Yealink Teams IP Phones. 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 & Skype for Business Admin Center services.

- *Device Management*
- *Configuration Profiles Management*

Device Management

You can monitor and manage your devices directly on the Microsoft Teams & Skype for Business Admin Center.

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

Editting 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. Navigate to **Device** > **Manage Devices** > **All device**.
2. Click a desired device in the **All devices** list.
3. Click **Edit** at the top left of the device list.
4. Edit device info from the right side of the pop-up menu.
5. Click **Save**.

Customizing the Displayed Elements of Devices

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

Procedure

1. Navigate to **Device** > **Manage Devices** > **All device**.
2. Click  at the top-right of the device list.
3. Turn on or turn off the table elements.
4. Click **Save**.

Viewing the Device Details

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

Procedure

1. Navigate to **Device** > **Manage Devices** > **All device**.
2. Click the corresponding device name in the **All devices** 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. Navigate to **Device** > **Manage Devices** > **All device**.
2. Click desired devices in the **All devices** list.
3. Click **Assign configuration** at the top left of the device list.
4. Search for the configuration profile from the right side of the pop-up menu.
5. Click **Save**.
   The configuration profile will take effect to the devices.

Related tasks

Creating a Configuration Profile

Diagnostic Devices

You can use diagnostic feature to quickly find the root cause of the problem and troubleshoot the problem. After diagnostic devices, you should download and check the diagnostics file.

Procedure

1. Navigate to **Device** > **Manage Devices** > **All device**.
2. Click desired devices in the **All devices** list.
3. Click **Diagnostics** at the top of the device list.

   It will prompt " Log files will be retrieved from the selected device(s). Would you like to proceed?"
4. Click **Proceed**.
   Log files will be retrieved from the selected device(s) if diagnosing successfully.
5. Click the corresponding device name in the **All devices** list to enter the device details page.
6. Select **History** and then click **Download** to download the log file.

Updating Device Software

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

About this task

All software on the selected devices will be updated .

Procedure

1. Navigate to **Device** > **Manage Devices** > **All device**.
2. Click desired devices in the **All devices** list.

3. Click **Update** at the top of the device list.
   It will prompt " All software on the selected devices will be updated to the latest versions. Would you like to proceed?"
4. Click **Update anyway**.
   The current firmware of the devices will be updated automatically after a few minutes.

Restarting Your Devices

Procedure

1. Navigate to **Device** > **Manage Devices** > **All device**.
2. Click desired devices in the **All devices** list.
3. Click **Restart** at the top of the device list.
   It will prompt " The selected devices will be restarted. Would you like to proceed?"
4. Click **Restart anyway**.
   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 and Russian are supported by the phone. The language configuration does not take effect when you select other languages.

- *Creating a Configuration Profile*
- *Editting a Configuration Profile*
- *Assigning Configuration Profile to Devices*

Related information

Language

Creating a Configuration Profile

Procedure

1. Navigate to **Device** > **Manage Devices** > **Configuration profiles**.
2. Click **New configuration profiles** at the top left of the configuration profiles list.
3. Edit the configuration profile name and discription.
4. Configure the general settings,device settings or network settings.
   If you enable phone lock feature for the device, the user cannot disable it.
5. Click **Save**.

Editting a Configuration Profile

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

Procedure

1. Navigate to **Device** > **Manage Devices** > **Configuration profiles**.
2. Click a desired configuration file in the **Configuration file** list.
3. Click **Edit** at the top left of the configuration profiles list.
4. Edit the configuration profile.
5. Click **Save**.

Assigning Configuration Profile to Devices

Procedure

1. Navigate to **Device** > **Manage Devices** > **Configuration profiles**.
2. Click a desired configuration file in the **Configuration file** list.
3. Click **Assigned to devices** at the top of the configuration profiles list.
4. Search for the devices from the right side of the pop-up menu.
5. Click **Save**.
   The configuration profile will take effect to the devices.

Firmware Upgrade

There are three methods of firmware upgrade:

- Manually, from the local system for a single phone via web user interface.
- Automatically, from the provisioning server for a mass of phones.
- 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 IP Phones running the Teams firmware.

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

- *Firmware for Each Phone Model*
- *Firmware Upgrade Configuration*

Related tasks

Updating Device Software

Firmware for Each Phone Model

You can download the latest firmware online:

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

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

IP Phone Model	Associated Firmware Name	Firmware Name
T58A/T56A	58.x.x.x.rom	58.15.0.20.rom
CP960	73.x.x.x.rom	73.15.0.20.rom

Firmware Upgrade Configuration

Before upgrading firmware, you need to know the following:

- Do not close and refresh the browser when the phone is upgrading firmware via web user interface.
- Do not unplug the network cables and power cables when the phone 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. **Example**: static.firmware.url = http://192.168.1.20/58.15.0.20.rom	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Settings** > **Upgrade** > **Select And Upgrade Firmware**	

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

Phone Customization

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

- *Language*
- *Screen Saver*
- *Backlight*
- *Time and Date*
- *Tones*
- *Power Saving*
- *Power LED Indicator*
- *Bluetooth*

Language

Teams IP Phones support multiple languages. Languages used on the phone user interface and web user interface can be specified respectively as required.

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

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

Phone User Interface		**Web User Interface**		
Language	**Language Pack**	**Language**	**Language Pack**	**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

- *Language Display Configuration*

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 phone, the web user interface will display English by default. You can specify the languages for the phone user interface and web user interface respectively.

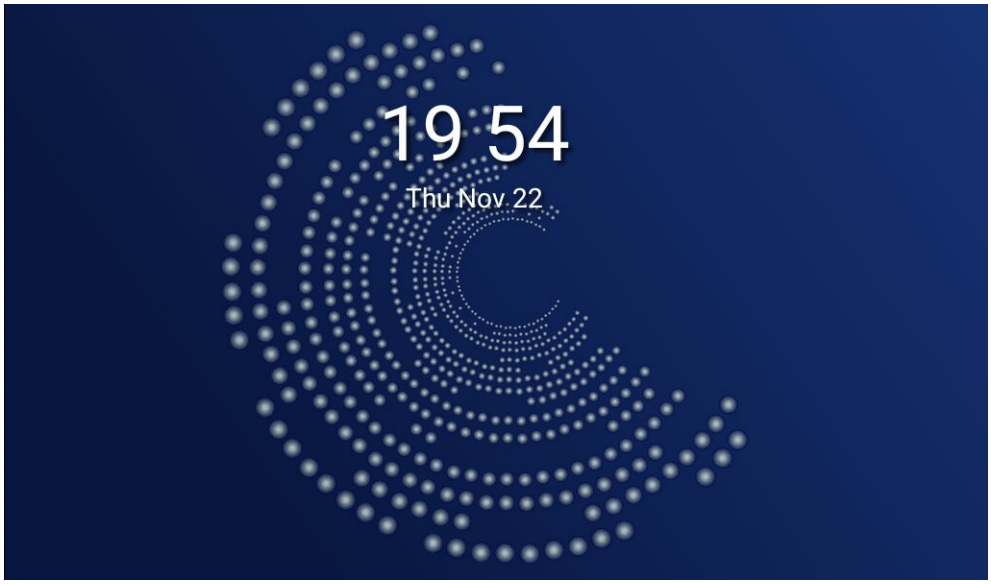
The following table lists the parameters you can use to configure language display.

Parameter	**lang.gui**	**<y0000000000xx>.cfg**
Description	It configures the language to display on the phone user interface.	
Permitted Values	English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian or the custom language name.	
Default	English	
Phone UI	☰ > **Settings** > **Device Settings** > **Language**	
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 or the custom language name.	
Default	English	
Web UI	On the top right corner of the web user interface	

Screen Saver

The screen saver will automatically start when the phone 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 phone or tapping the touch screen. When your phone is idle again for a preset waiting time,the screen saver starts again.

By default, the phone screen displays a built-in picture when the screen saver starts. You can set the phone to display the other built-in screensaver background. The following shows the built-in screen saver displayed on T58A Teams IP Phones:



- *Screensaver Configuration*

Screensaver Configuration

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

Parameter	**screensaver.wait_time**	**<y0000000000xx>.cfg**
Description	It configures the time (in seconds) that the phone waits in the idle state before the screen saver starts.	
Permitted Values	**15**-15s **30**-30s **60**-1min **120**-2min **300**-5min **600**-10min **900**-15min **1800**-30min **3600**-1h **7200**-2h	
Default	900	
Phone UI	☰ > **Settings** > **Device Settings** > **Display** > **Screen saver** > **Screensaver Waiting Time**	
Web UI	**Settings** > **Preference** > **Screen saver**	
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
Phone UI	☰ > **Settings** > **Device Settings** > **Display** > **Screen saver** > **Screensaver background**
Web UI	**Settings** > **Preference** > **Screen saver** > **Screensaver Background**

Backlight

You can change the brightness of LCD backlight when the phone is active (in use). The brightness of LCD backlight automatically changes when the phone 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 phone is active.

Backlight Time: The delay time to change the brightness of the LCD backlight when the phone 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 phone 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 phone is active.	
Permitted Values	Integer from 1 to 10	
Default	8	
Phone UI	☰ > **Settings** > **Device Settings** > **Display** > **Backlight** > **Backlight Active Level**	
Web UI	**Settings** > **Preference** > **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 phone is inactive.
Permitted Values	**0**-Always On **15**-15s **30**-30s **60**-1min **120**-2min **300**-5min **600**-10min **1800**-30min
Default	0
Phone UI	☰ > **Settings** > **Device Settings** > **Display** > **Backlight** > **Backlight Time**
Web UI	**Settings** > **Preference** > **Backlight** > **Backlight Time(seconds)**

Time and Date

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

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

Time Zone

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

Time Zone	Time Zone Name	Time Zone	Time Zone Name
-12	International Date Line West	+4	Armenia(Yerevan), Azerbaijan(Baku), Georgia(Tbilisi) , Kazakhstan(Aktau), Russia(Samara)
-11	Samoa	+4:30	Afghanistan(Kabul)
-10	United States-Hawaii-Aleutian, United States-Alaska-Aleutian	+5	Kazakhstan(Aqtobe), Kyrgyzstan(Bishkek), Pakistan(Islamabad), Russia(Chelyabinsk)
-9:30	French Polynesia	+5:30	India(Calcutta)
-9	United States-Alaska Time	+5:45	Nepal(Katmandu)
-8	Canada(Vancouver,Whitehorse), Mexico(Tijuana,Mexicali), United States-Pacific Time	+6	Kazakhstan(Astana, Almaty), Russia(Novosibirsk,Omsk)

Time Zone	Time Zone Name	Time Zone	Time Zone Name
-7	Canada(Edmonton,Calgary), Mexico(Mazatlan,Chihuahua), United States-MST no DST, United States-Mountain Time	+6:30	Myanmar(Naypyitaw)
-6	Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Belize, Canada-Manitoba(Winnipeg), Chile(Easter Islands), Mexico(Mexico City,Acapulco), United States-Central Time	+7	Russia(Krasnoyarsk), Thailand(Bangkok)
-5	Peru, Bahamas(Nassau), Canada(Montreal,Ottawa,Quebec), Cuba(Havana), United States-Eastern Time	+8	Australia(Perth), China(Beijing), Russia(Irkutsk, Ulan-Ude), Singapore(Singapore)
-4:30	Venezuela(Caracas)	+8:45	Eucla
-4	Canada(Halifax,Saint John), Chile(Santiago), Paraguay(Asuncion), United Kingdom-Bermuda(Bermuda), United Kingdom(Falkland Islands), Trinidad&Tobago	+9	Japan(Tokyo), Korea(Seoul), Russia(Yakutsk,Chita)
-3:30	Canada-New Foundland(St.Johns)	+9:30	Australia(Adelaide), Australia(Darwin)
-3	Argentina(Buenos Aires), Brazil(DST), Brazil(no DST), Denmark-Greenland(Nuuk)	+10	Australia(Brisbane), Australia(Hobart), Australia(Sydney,Melbourne,Canberra), Russia(Vladivostok)
-2:30	Newfoundland and Labrador	+10:30	Australia(Lord Howe Islands)
-2	Brazil(no DST)	+11	New Caledonia(Noumea), Russia(Srednekolymsk Time)
-1	Portugal(Azores)	+11:30	Norfolk Island
0	Denmark-Faroe Islands(Torshavn), GMT, Greenland, Ireland(Dublin), Morocco, Portugal(Lisboa,Porto,Funchal), Spain-Canary Islands(Las Palmas), United Kingdom(London)	+12	New Zealand(Wellington,Auckland), Russia(Kamchatka Time)
+1	Albania(Tirane), Austria(Vienna), Belgium(Brussels), Caicos, Chad, Croatia(Zagreb), Czech Republic(Prague), Denmark(Kopenhagen), France(Paris), Germany(Berlin), Hungary(Budapest), Italy(Rome), Luxembourg(Luxembourg), Macedonia(Skopje), Namibia(Windhoek), Netherlands(Amsterdam), Spain(Madrid),	+12:45	New Zealand(Chatham Islands)
+2	Estonia(Tallinn), Finland(Helsinki), Gaza Strip(Gaza), Greece(Athens), Harare,Pretoria,Israel(Tel Aviv), Jordan(Amman), Latvia(Riga), Lebanon(Beirut), Moldova(Kishinev), Romania(Bucharest), Russia(Kaliningrad),	+13	Tonga(Nukualofa)

Time Zone	Time Zone Name	Time Zone	Time Zone Name
	Syria(Damascus), Turkey(Ankara), Ukraine(Kyiv, Odessa)		
+3	East Africa Time, Iraq(Baghdad), Russia(Moscow)	+13:30	Chatham Islands
+3:30	Iran(Teheran)	+14	Kiribati

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 phone to use the NTP server address offered by the DHCP server.	
Permitted Values	**0**- High (use the NTP server address offered by the DHCP server preferentially) **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 phone 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	
Phone UI	☰ > **Settings** > **Device Settings** > **Time&Date** > **DHCP Time** > **DHCP Time**	
Web UI	**Settings** > **Time & Date** > **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 phone will obtain the current time and date from the NTP server 1.	
Permitted Values	IP address or domain name	
Default	cn.pool.ntp.org	
Phone UI	☰ > **Settings** > **Device Settings** > **Time&Date** > **General** > **NTP Server1**	
Web UI	**Settings** > **Time & Date** > **Primary Server**	

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 phone will request the time and date from the NTP server 2.	
Permitted Values	IP address or domain name	
Default	pool.ntp.org	
Phone UI	> **Settings** > **Device Settings** > **Time&Date** > **General** > **NTP Server2**	
Web UI	**Settings** > **Time&Date** > **Secondary Server**	
Parameter	**local_time.interval**	**<MAC>.cfg**
Description	It configures the interval (in seconds) at which the phone updates time and date from the NTP server.	
Permitted Values	Integer from 15 to 86400	
Default	1000	
Web UI	**Settings** > **Time & Date** > **Update Interval (15~86400s)**	
Parameter	**local_time.time_zone**	**<MAC>.cfg**
Description	It configures the interval (in seconds) at which the phone updates time and date from the NTP server.	
Permitted Values	-12 to +14 For available time zones, refer to *Time Zone*.	
Default	+8	
Web UI	**Settings** > **Time & Date** > **Time Zone**	
Parameter	**local_time.time_zone_name**	**<MAC>.cfg**
Description	It configures the time zone name. **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 2 (Automatic) and the parameter "local_time.time_zone" should be configured in advance.	
Permitted Values	String within 32 characters The available time zone names depend on the time zone configured by the parameter "local_time.time_zone". For available time zone names, refer to *Time Zone*.	
Default	China(Beijing)	
Phone UI	> **Settings** > **Device Settings** > **Time&Date** > **General** > **Location**	
Web UI	**Settings** > **Time & Date** > **Location**	

DST Settings

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

The time zone and corresponding DST pre-configurations exist in the AutoDST file. If the DST is set to Automatic, the phone obtains the DST configuration from the AutoDST file.

You can customize the AutoDST file if required. The AutoDST file allows you to add or modify time zone and DST settings for your area each year.

- *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 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

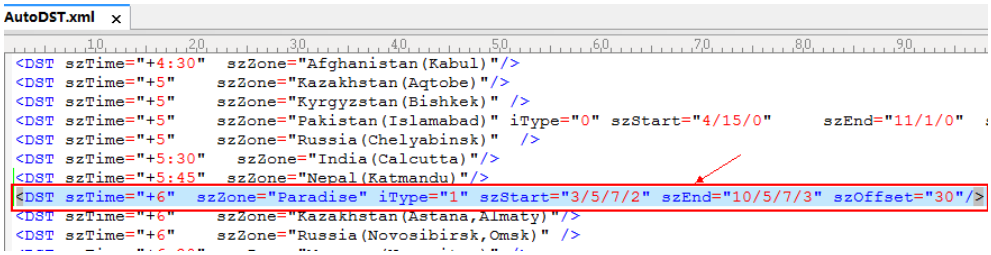
Procedure

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.

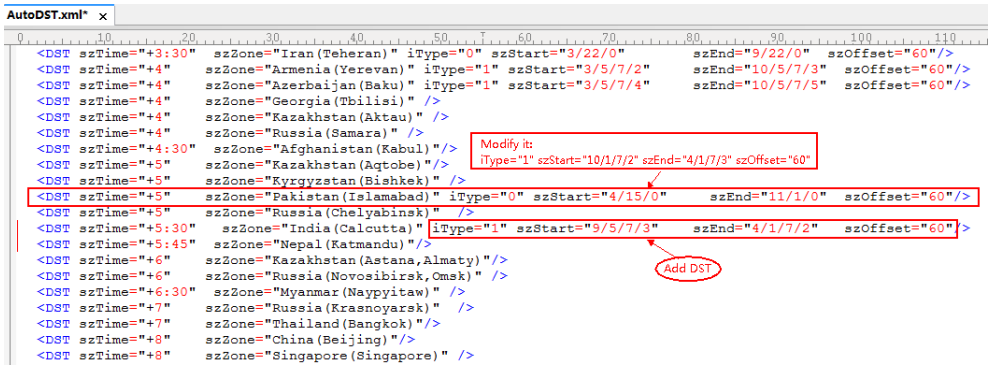
   For example:

   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"/>



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



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

Related information

Time Zone

DST Configuration

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

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

Web UI	**Settings** > **Time & Date** > **Daylight Saving Time**	
Parameter	**local_time.dst_time_type**	**<MAC>.cfg**
Description	It configures the Daylight Saving Time (DST) type.**Note**: It works only if the value of the parameter "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). It works only if the value of the parameter "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 the value of the parameter "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 the value of the parameter "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 For example, tftp://192.168.1.100/AutoDST.xml	
Default	Blank	

Time and Date Manual Configuration

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

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

Parameters	**local_time.manual_time_enable**	**<MAC>.cfg**
Description	It enables or disables the IP phone 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** > **Tpye** > **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 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	
Phone UI	☰ > **Settings** > **Device Settings** > **Time&Date** > **Time & Date Format** > **Time Format**	
Web UI	**Settings** > **Time & Date** > **Time Format**	
Parameter	**local_time.date_format**	**<MAC>.cfg**
Description	It configures the date format. The value configured by the parameter "lcl.datetime.date.format" takes precedence over that configured by this parameter.	
Permitted Values	**0**-WWW MMM DD **1**-DD-MMM-YY **2**-YYYY-MM-DD **3**-DD/MM/YYYY **4**-MM/DD/YY **5**-DD MMM YYYY **6**-WWW DD MMM Use the following mapping: "WWW" represents the abbreviation of the week; "DD" represents a two-digit day; "MMM" represents the first three letters of the month; "YYYY" represents a four-digit year, and "YY" represents a two-digit year.	
Default	0	
Phone UI	☰ > **Settings** > **Device Settings** > **Time&Date** > **Time & Date Format** > **Date Format**	
Web UI	**Settings** > **Time & Date** > **Date Format**	

Tones

When the phone is in the dialing interface, 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 phone. It is not applicable to CP960 Phones.

- *Supported Tones*
- *Tones Configuration*

Supported Tones

The default tones used on Teams IP Phones are the US tone sets. Available tone sets for the phones:

- Australia
- Austria
- Brazil
- Belgium
- Chile
- China
- Czech
- Czech ETSI
- Denmark
- Finland
- France
- Germany
- Great Britain
- Greece
- Hungary
- Lithuania
- India
- Italy
- Japan
- Mexico
- New Zealand
- Netherlands
- Norway
- Portugal
- Spain
- Switzerland
- Sweden
- Russia
- United States

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. **Example**: voice.tone.country = Custom 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.	

Power Saving

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

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

- *Power Saving Configuration*

Power Saving Configuration

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

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

You can specify the following three types of idle timeout:

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

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

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

Parameter	**features.power_saving.intelligent_mode**	**<y0000000000xx>.cfg**
Description	It enables or disables the power saving intelligent mode.	
Permitted Values	**0**-Disabled, the phone stays in power-saving mode even if the office hour arrives the next day. **1**-Enabled, the phone will automatically identify the office hour and exit power-saving mode once the office hour arrives the next day.	
Default	1	
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 phone enters power-saving mode during the office hours. **Example**: features.power_saving.office_hour.idle_timeout = 600 The phone will enter power-saving mode when it has been inactivated for 600 minutes (10 hour) during the office hours.	
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 enter 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 Teams IP Phones.

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 power LED indicator.

Parameter	phone_setting.ring_power_led_flash_enable	<y0000000000xx>.cfg
Description	It enables or disables the power indicator LED 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). It is only applicable to T58A Teams IP Phones and only the Bluetooth headset is supported.

- *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 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	**features.bluetooth_enable**	**<y0000000000xx>.cfg**
Description	It triggers the Bluetooth mode to on or off. **Note**: It is only applicable to T58A Phones.	
Permitted Values	**0**-Off **1**-On	
Default	0	
Phone UI	☰ > **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). It is only applicable to T58A IP phones.	
Permitted Values	String within 64 characters	
Default	Yealink-T58	
Phone UI	☰ > **Settings** > **Device Settings** > **Bluetooth** > **Device Name**	

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/handset user interface. Yealink Teams IP Phones support the access levels of admin, var and user.

When logging into the web user interface or access the advanced settings on the phone, as an administrator, you need administrator password to access various menu options. The default username and password for administrator is "admin". Both you and the user can log into the web user interface, and you will see all of the user options. The default username and password for user is "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 administrator, users can configure them only if they have administrator privileges.

- *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 phone'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 phone'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 phone'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 phone uses "user" as the default user password and "admin" as the default administrator password. The valid value format is <username> : <new password>. **Example**: static.security.user_password = user:123 means setting the password of user to 123. static.security.user_password = admin:456 means setting the password of administrator to 456. **Note**: The phones support ASCII characters 32-126(0x20-0x7E) in passwords. You can set the password to be empty via web user interface only.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	**Security** > **Password**	

Phone UI	☰ > **Settings** > **Device Settings** > **Admin Password(Admin only, default password: admin)** **Note**: You cannot change the user password via phone user interface.

User Access Level Configuration

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

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

Parameter	**static.security.var_enable**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the 3-level access permissions (admin, user, var).	
Permitted Values	**0**-Disabled **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 can not diable it by themselves.

- *Phone Lock Configuration*

Related tasks

Creating a Configuration Profile

Related information

Provisioning Phone 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**	

Transport Layer Security (TLS)

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

Yealink Teams IP phones 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 Teams IP phones support the following *cipher suites*:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- AES256-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- 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 phone 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 phone requests a TLS connection with a server, the phone should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The phone has 77 built-in trusted certificates. You can upload 10 custom certificates at most. The format of the trusted certificate files must be *.pem,*.cer,*.crt and *.der and the maximum file size is 5MB.
- **Server Certificate**: When clients request a TLS connection with the phone, the phone sends the server certificate to the clients for authentication. The phone has two types of built-in server certificates: a unique server certificate and a generic server certificate. You can only upload one server certificate to the phone. The old server certificate will be overridden by the new one. The format of the server certificate files must be *.pem and *.cer and the maximum file size is 5MB.
- **A unique server certificate**: It is unique to a phone (based on the MAC address) and issued by the Yealink Certificate Authority (CA).
- **A generic server certificate**: It is issued by the Yealink Certificate Authority (CA). Only if no unique certificate exists, the phone may send a generic certificate for authentication.

The phone can authenticate the server certificate based on the trusted certificates list. The trusted certificates list and the server certificates list contain the default and custom certificates. You can specify the type of certificates the phone accepts: default certificates, custom certificates or all certificates.

Common Name Validation feature enables the phone 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 IP phones trust the following CAs by default:

- DigiCert High Assurance EV Root CA
- Deutsche Telekom Root CA 2
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure Global eBusiness CA-1
- GeoTrust Global CA
- GeoTrust Global CA2
- GeoTrust Primary Certification Authority
- GeoTrust Primary Certification Authority G2
- GeoTrust Universal CA
- GeoTrust Universal CA2
- Thawte Personal Freemail CA

- Thawte Premium Server CA
- Thawte Primary Root CA
- Thawte Primary Root CA - G2
- Thawte Primary Root CA - G3
- Thawte Server CA
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Universal Root Certification Authority
- ISRG Root X1 (Let’s Encrypt Authority X1 and Let’s Encrypt Authority X2 certificates are signed by the root certificate ISRG Root X1.)
- Baltimore CyberTrust Root
- DST Root CA X3
- Verizon Public SureServer CA G14-SHA2
- AddTrust External CA Root
- Go Daddy Class 2 Certification Authority
- Class 2 Primary CA
- Cybertrust Public SureServer SV CA
- DigiCert Assured ID Root G2
- DigiCert Assured ID Root G3
- DigiCert Assured ID Root CA
- DigiCert Global Root G2
- DigiCert Global Root G3
- DigiCert Global Root CA
- DigiCert Trusted Root G4
- Entrust Root Certification Authority
- Entrust Root Certification Authority - G2
- Entrust.net Certification Authority (2048)
- GeoTrust Primary Certification Authority - G3
- GlobalSign Root CA
- GlobalSign Root CA - R2
- Starfield Root Certificate Authority - G2
- TC TrustCenter Class 2 CA II
- TC TrustCenter Class 3 CA II
- TC TrustCenter Class 4 CA II
- TC TrustCenter Universal CA I
- TC TrustCenter Universal CA III
- Thawte Universal CA Root
- VeriSign Class 3 Secure Server CA - G2
- VeriSign Class 3 Secure Server CA – G3
- Thawte SSL CA

- StartCom Certification Authority
- StartCom Certification Authority G2
- Starfield Services Root Certificate Authority - G2
- RapidSSL CA
- Go Daddy Root Certificate Authority - G2
- Cybertrust Global Root
- COMODOSSLCA
- COMODO RSA Domain Validation Secure Server CA
- COMODO RSA Certification Authority
- AmazonRootCA4
- AmazonRootCA3
- AmazonRootCA2
- AmazonRootCA1
- Yealink Root CA
- Yealink Equipment Issuing CA
- SIP Core

Note:

Yealink endeavors to maintain a built-in list of most common used CA Certificates. Due to memory constraints, we cannot ensure a complete set of certificates. If you are using a certificate from a commercial Certificate Authority 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 phone.

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 phone to only trust the server certificates listed in the Trusted Certificates list.	
Permitted Values	**0**-Disabled, the phone will trust the server no matter whether the certificate sent by the server is valid or not. **1**-Enabled, the phone will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, will the IP phone 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 phone 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 phone 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.security.dev_cert**[1]	**<y0000000000xx>.cfg**
Description	It configures the type of the device certificates for the phone to send for TLS authentication.	
Permitted Values	**0**-Default Certificates **1**-Custom Certificates	
Default	0	
Web UI	**Security** > **Server Certificates** > **Device Certificates**	
Parameter	**static.trusted_certificates.url**	**<y0000000000xx>.cfg**
Description	It configures the access URL of the custom trusted certificate used to authenticate the connecting server. **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. **Example**: static.trusted_certificates.delete = http://localhost/all	
Permitted Values	*http://localhost/all*	
Default	Blank	
Parameter	**static.server_certificates.url**	**<y0000000000xx>.cfg**
Description	It configures the access URL of the certificate the phone sends for authentication. **Example**: static.server_certificates.url = http://192.168.1.20/ca.pem **Note**: The certificate you want to upload must be in *.pem or *.cer format.	
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. **Example**: static.server_certificates.delete = http://localhost/all	
Permitted Values	*http://localhost/all*	
Default	Blank	
Parameter	**static.phone_setting.reserve_certs_enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to reserve custom certificates after it is reset to factory defaults.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	

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

Encrypting Configuration Files

Yealink Teams IP phones 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, sip.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 phone, and generate new files named as <xx_Security>.enc (xx is the name of the configuration file, for

example, y000000000058_Security.enc for y000000000058.cfg file, account_Security.enc for account.cfg). These tools generate another new file named as Aeskey.txt to store the plaintext 16-character symmetric keys for each configuration file.

Configuration Files Encryption and Decryption

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

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

Encryption and Decryption Configuration

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

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

Permitted Values	**0**-Disabled, the phone will decrypt the encrypted configuration files using plaintext AES keys configured on the phone. **1**-Enabled, the phone will download <xx_Security>.enc files (for example, <sip_Security>.enc, <account_Security>.enc) during auto provisioning, and then decrypts these files into the plaintext keys (for example, key2, key3) respectively using the phone built-in key (for example, key1). The phone then decrypts the encrypted configuration files using 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 phone will try to encrypt/decrypt the MAC-Oriented file using the AES key configured by the parameter "static.auto_provision.aes_key_16.com".	
Permitted Values	16 characters	
Default	Blank	
Web UI	**Settings** > **Auto Provision** > **Common AES Key**	
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 phone will try to encrypt/decrypt the MAC-Oriented file using the AES key configured by the parameter "static.auto_provision.aes_key_16.com".	
Permitted Values	16 characters	
Default	Blank	
Web UI	**Settings** > **Auto Provision** > **MAC-Oriented AES Key**	

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 phone processes other configuration files is the same as that of the account.cfg file.

Procedure

1. Double click “Config_Encrypt_Tool.exe” to start the application tool.

   The screenshot of the main page is shown as below:

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

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

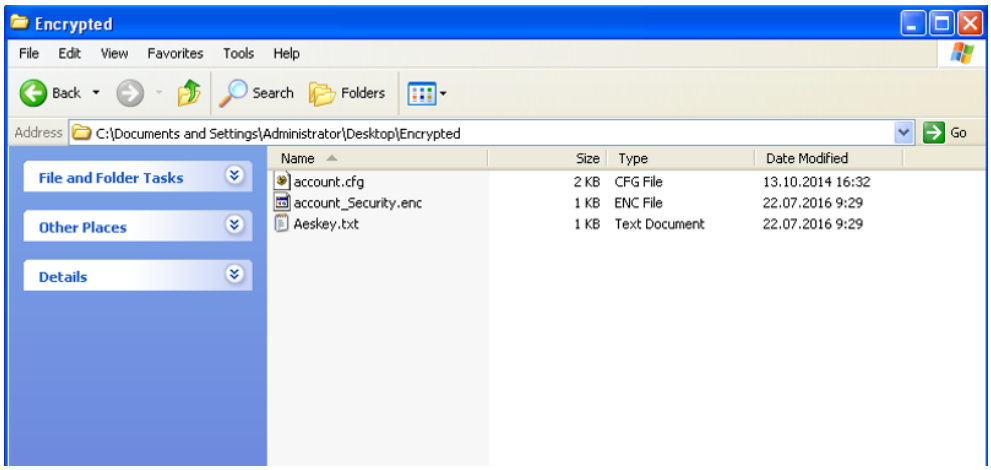
   The tool uses the file folder “Encrypted” as the target directory by default.
5. (Optional.) Mark the desired radio box in the **AES Model** field.

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

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

7. Click **OK**.

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



Troubleshooting Methods

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

- *Log Files*
- *Packets Capture*
- *Analyzing Configuration Files*
- *Exporting All the Diagnostic Files*
- *Phone Status*
- *Resetting Phone and Configuration*
- *Phone Reboot*
- *Capturing the Current Screen of the Phone*

Log Files

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

- *Local Log*
- *Syslog Log*

Local Log

You can enable 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 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 local log.

Parameter	**static.local_log.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to record log locally. **Note**: We recommend you not to disable this feature.	
Permitted Values	**0**-Disabled, the phone will stop recording log to the log files (<MAC>-boot.log and <MAC>-sys.log) locally. The log files recorded before are still kept on the phone. **1**-Enabled, the phone will continue to record log to the log files (<MAC>-boot.log and <MAC>-sys.log) locally. You can upload the local log files to the provisioning server or a specific server or export them to the local system.	
Default	1	
Web UI	**Settings** > **Configuration** > **Enable Local Log**	
Phone UI	☰ > **Settings** > **Device Settings** > **Debug(Admin only, 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(Admin only, 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) can be stored on the phone. When this size is about to be exceeded, (1) If the local log files are configured to be uploaded to the server by the parameter "static.auto_provision.local_log.backup.enable", the phone will clear all the local log files on the phone once successfully backing up. (2) If "static.auto_provision.local_log.backup.enable" is set to 0 (Disabled), the phone will erase half of the logs from the oldest log information on the phone. Example: static.local_log.max_file_size = 1024	
Permitted Values	Integer from 2048 to 20480	
Default	20480	
Web UI	**Settings** > **Configuration** > **Max Log File Size (2048-20480KB)**	
Parameter	**static.auto_provision.local_log.backup.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the phone to upload the local log files (<MAC>-boot.log and <MAC>-sys.log) to the provisioning server or a specific server. **Note**: The upload path is configured by the parameter "static.auto_provision.local_log.backup.path".	
Permitted Values	**0**-Disabled **1**-Enabled, the phone will upload the local log files to the provisioning server or the specific server to back up these files when one of the following happens: - Auto provisioning is triggered; - The size of the local log files reaches 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. **Example**: static.auto_provision.local_log.backup.upload_period = 60 **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 phone will upload the local log files to the provisioning server. If you configure a relative URL (for example, /upload), the IP phone will upload the local log files by extracting the root directory from the access URL of the provisioning server. If you configure an absolute URL with protocol (for example, tftp), the phone will upload the local log files using the desired protocol. If no protocol, the phone will use the same protocol with auto provisioning for uploading files. **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 IP phone will continue uploading log. **1**-Append Stop, the phone will stop uploading log.	
Default	0	
Parameter	**static.auto_provision.local_log.backup.append.max_file_size**	**<y0000000000xx>.cfg**
Description	It configures the maximum size (in KB) of the local log files (<MAC>-boot.log and <MAC>-sys.log) can be stored on the provisioning server or a specific server. **Example**: static.auto_provision.local_log.backup.append.max_file_size = 1025	
Permitted Values	Integer from 200 to 65535	
Default	1024	
Parameter	**static.auto_provision.local_log.backup.bootlog.upload_wait_time**	**<y0000000000xx>.cfg**
Description	It configures the waiting time (in seconds) before the phone uploads the local log file (<MAC>-boot.log) to the provisioning server or a specific server after startup. **Example**: static.auto_provision.local_log.backup.bootlog.upload_wait_time = 121	

Permitted Values	Integer from 1 to 86400
Default	120

Exporting the Log Files to a Local PC

Procedure

1. From the web user interface, navigate to **Settings** > **Configuration** > **Local Log**.
2. Turn on **Enable Local Log**.
3. Select a desired value from the pull-down list of **Local Log Level** .

   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 then save the file to your local system.

Viewing the Log Files

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

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

The default local log level is 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 (for example, 805EC031960A-sys.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
<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 Teams phone to send syslog messages to a syslog server in real time.

You can specify syslog details such as IP address or host name, server type, facility, and the severity level of events youwant to log. You can also choose to prepend the phone'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 phone 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. **Example**: static.syslog.server = 192.168.1.100	

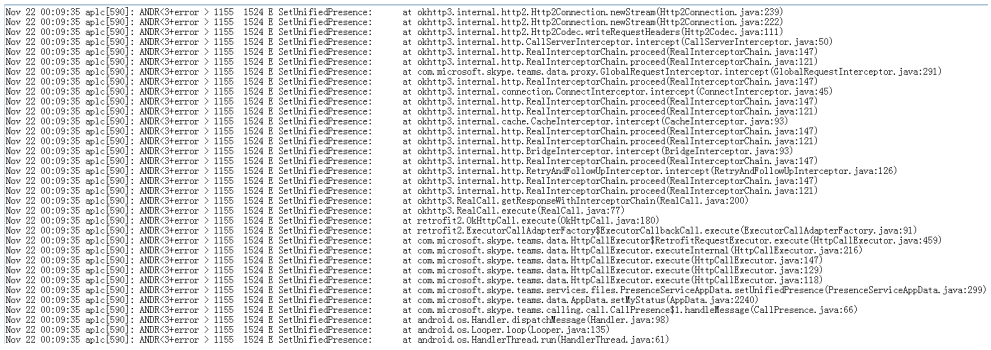
Permitted Values	IP address or domain name	
Default	Blank	
Web UI	**Settings** > **Configuration** > **Syslog** > **Syslog Server**	
Parameter	**static.syslog.server_port**	**<y0000000000xx>.cfg**
Description	It configures the port of the syslog server. **Example**: static.syslog.port = 515	
Permitted 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 phone 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 phone 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:



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 purpose.

- *Capturing the Packets via Web User Interface*
- *Ethernet Software Capturing Configuration*

Capturing the Packets via Web User Interface

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

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

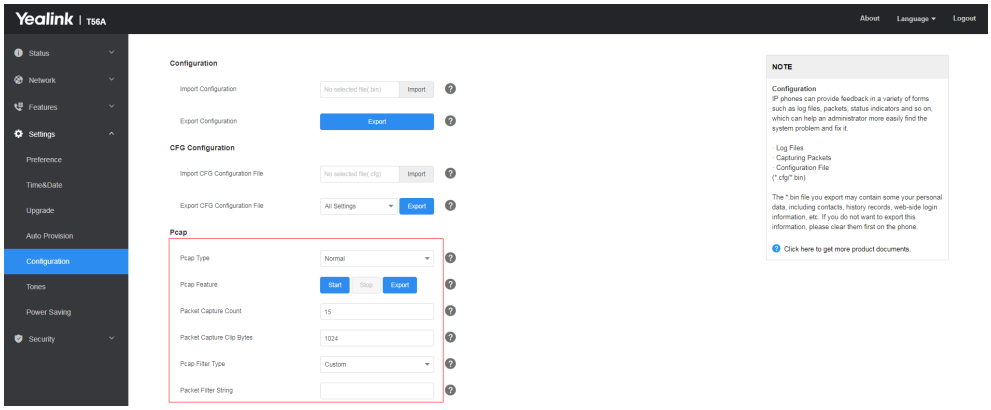
- **Normal**: Export the packets file after stopping capturing.
- **Enhanced**: Export the packets file while capturing.

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

Capturing the Packets in Normal Way

Procedure

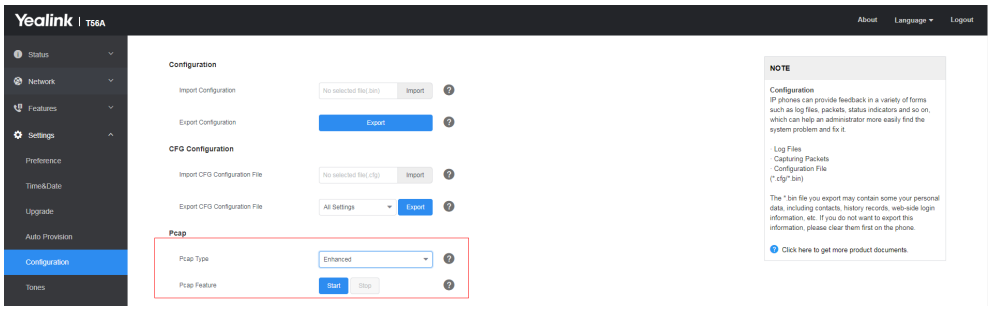
1. From the web user interface, navigate to **Settings** > **Configuration**.
2. Select **Normal** from the pull-down list of **Pcap Type**.
3. Enter the desired value in the **Packet Capture Count** field.
4. Enter the desired value in the **Packet Capture Clip Bytes** field.
5. Select the desired value from the pull-down list of **Pcap Filter Type**.
6. Enter the desired value in the **Packet Filter String** field.
7. In the **Pcap Feature** field,click **Start** to start capturing signal traffic.
8. Reproduce the issue to get stack traces.
9. Click **Stop** in the **Pcap Feature** field to stop capturing.
10. Click **Export** to open the file download window, and then save the file to your local system.



Capturing the Packets in Enhanced Way

Procedure

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



Ethernet Software Capturing Configuration

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

- Receiving data packets from the HUB: Connect the Internet port of the phone and the PC to the same HUB, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic.
- Receiving data packets from PC port: Connect the Internet port of the phone to the Internet and 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. It is not applicable to CP960 Phones.

Parameter	static.network.span_to_pc_port[1]	<y0000000000xx>.cfg

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

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

Analyzing Configuration Files

Wrong configurations may a poor impact on the phone. You can export configuration file(s) to check the current configuration of the phone and troubleshoot if necessary. You can also import configuration files for a quick and easy configuration.

We recommend you to edit the exported CFG file instead of the BIN file to change the phone's current settings. The config.bin file is an encrypted file. For more information on config.bin file, contact your Yealink reseller.

- *Exporting BIN Files from the Phone*
- *Importing BIN Files from the Phone*

Exporting BIN Files from the Phone

Procedure

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

Importing BIN Files from the Phone

Procedure

1. From the web user interface, navigate 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 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 phone will reboot to make the change take effect.

Exporting All the Diagnostic Files

Yealink Teams IP Phones support three types of diagnostic files (including Pcap trace, log files (boot.log and sys.log) and BIN configuration files) to help analyze your problem. You can export these files at a time and troubleshoot if necessary. The file format of the exported diagnostic file is *.tar.

Procedure

1. From the web user interface, navigate to **Settings** > **Configuration**.
2. Click **Start** in the **Export All Diagnostic Files** field to begin capturing signal traffic.
   The system log level will be automatically set to 6.
3. Reproduce the issue.
4. Click **Stop** in the **Export All Diagnostic Files** field to stop the capture.
5. Click **Export** to open the file download window, and then save the diagnostic file to your local system.
   A diagnostic file named allconfig.tgz is successfully exported to your local system.

Phone Status

Available information on phone status includes:

- 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
- Phone status(MAC address and device type)
- *Viewing the Phone Status*

Viewing the Phone Status

You can view phone status via phone user interface by navigating to ☰ > **Settings** > **Device Settings** > **About**. You can also view the phone status via 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 phone status is displayed on the first page of the web user interface.

Resetting Phone and Configuration

Generally, some common issues may occur while using the phone. You can reset your phone to factory configurations after you have tried all troubleshooting suggestions, but still do not solve the problem. Resetting the phone to factory configurations clears the flash parameters, removes log files, user data, and cached data, and resets the administrator password to admin. All custom settings will be overwritten after resetting.

- *Resetting the phone to Default Factory Settings*
- *Resetting the phone to Custom Factory Settings*
- *Deleting the Custom Factory Settings Files*

Resetting the phone 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 phone will be reset to factory sucessfully after startup.

Note: Reset of your phone may take a few minutes. Do not power off until the phone starts up successfully.

Resetting the phone to Custom Factory Settings

After you enable the custom factory feature, you can import the custom factory configuration file, and then reset the phone 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 custom factory configuration file is imported successfully, you can reset the phone to custom factory settings.

- *Custom Factory Configuration*

Custom Factory Configuration

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

Parameter	**static.features.custom_factory_config.enable**	<y0000000000xx>.cfg
Description	It enables or disables the Custom Factory Configuration feature.	
Permitted Values	**0**-Disabled **1**-Enabled, Import Factory Configuration item will be displayed on the phone's web user interface at the path **Settings->Configuration**. You can import a custom factory configuration file or delete the user-defined factory configuration via web user interface.	
Default	0	
Parameter	**static.custom_factory_configuration.url**	**<y0000000000xx>.cfg**

Description	It configures the access URL of the custom factory configuration files. **Note**: It works only if "static.features.custom_factory_config.enable" is set to 1 (Enabled) and the file format of custom factory configuration file must be *.bin.
Permitted Values	URL within 511 characters
Default	Blank
Web UI	**Settings** > **Configuration** > **Import Factory Configuration**

Deleting the Custom Factory Settings Files

You can delete the user-defined factory configurations via web user interface.

Procedure

1. From the web user interface, click **Settings** > **Configuration** > **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 phone will be reset to default factory settings after resetting.

Phone Reboot

You can reboot the phone locally.

- *Rebooting the Phone via Phone User Interface*
- *Rebooting the Phone via Web User Interface*

Rebooting the Phone via Phone User Interface

Procedure

1. Navigate to ☰ > **Settings** > **Device Settings** > **Debug**.
2. Tap **Reboot phone**.
   It prompts if you are sure to reboot the phone.
3. Tap **OK**.

Rebooting the Phone via Web User Interface

Procedure

1. Click **Settings** > **Upgrade**.
2. Click **Reboot** to reboot the phone.
   The web user interface prompts the message "Reboot the system?"
3. Click **OK** to confirm the rebooting.
   The phone begins rebooting. Any reboot of the phone 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)://<phoneIPAddress>/screencapture. The captured picture is saved as a BMP or JPEG file.

You can also use the URI “http(s)://<phoneIPAddress>/screencapture/download” to capture the screen display first, and then download the image (which is saved as a JPG file and named with the phone model and the capture time) to the local system.

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 web browser does not remember the user name and password for web user interface login.

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

Enabling the Screen Capture via Phone User Interface

Procedure

1. Navigate to ☰ > **Settings** > **Device Settings** > **Debug(Admin only, default password: admin)** > **Screen Capture**.
2. Enable **Screen Capture**.

Capturing the Current Screen of the Phone via Web User Interface

Before you begin

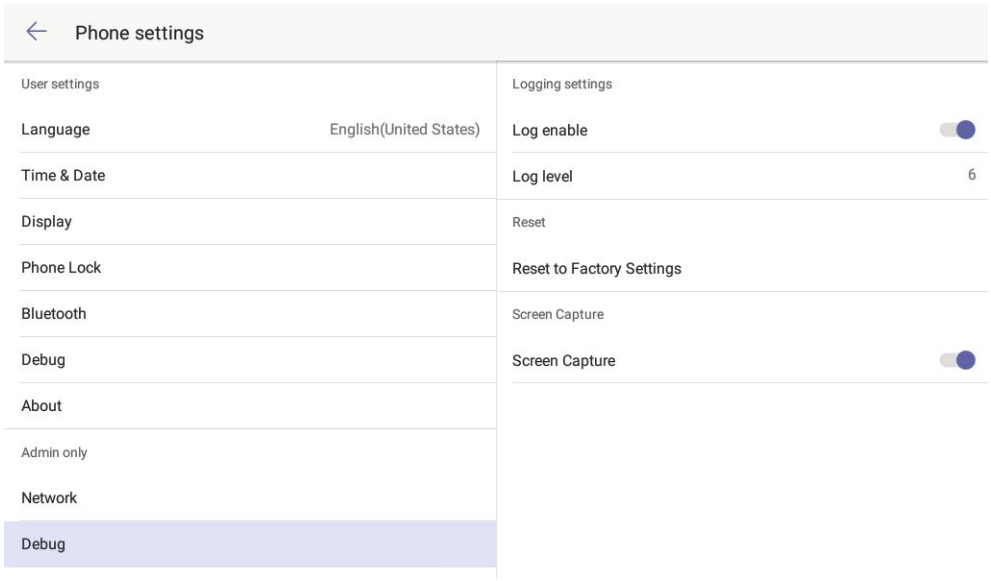
Before capturing the phone’s current screen, ensure that the Screen Capture feature is enabled via phone user interface.

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.



Troubleshooting Solutions

This section describes the solutions to common issues that may occur while using the Teams phone. 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 IP phone does not get an IP address*
- *IP Conflict*
- *Specific format in configuring IPv6 on Yealink IP phones*

The IP phone does not get an IP address

Do one of the following:

- Ensure that the Ethernet cable is plugged into the Internet port on the phone and the Ethernet cable is not loose.
- Ensure that the Ethernet cable is not damaged.
- Ensure that the IP address and related network parameters are set correctly.
- Ensure that your network switch or hub is operational.

IP Conflict

Do one of the following:

- Reset another available IP address for the phone.

- Check network configuration via phone user interface at the path ☰ > **Settings** > **Device Settings** > **Network(Admin only, 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 IP phones

Scenario 1:

If the IP phone obtains the IPv6 address, the format of the URL to access the web user interface is "*[IPv6 address]*" or "*http(s):///[IPv6 address]*". For example, if the IPv6 address of your phone is "fe80::204:13ff:fe30:10e", you can enter the URL (for example, "[fe80::204:13ff:fe30:10e]" or "http(s)://[fe80::204:13ff:fe30:10e])" in the address bar of a web browser on your PC to access the web user interface.

Scenario 2:

Yealink IP phones support using FTP, TFTP, HTTP and HTTPS protocols to download configuration files or resource files. You can use one of these protocols for provisioning.

When provisioning your IP phone 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 IP phone is configured to obtain the time and date from the NTP server automatically. If your phone is unable to access the NTP server, configure the time and date manually.

Display Issues

- *The phone LCD screen blank*
- *The phone displays "Offline"*

The phone LCD screen blank

Do one of the following:

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

The phone displays "Offline"

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

Firmware and Upgrading Issues

- *Fail to upgrade the phone firmware*
- *The phone does not update the configurations*

Fail to upgrade the phone firmware

Do one of the following:

- Ensure that the target firmware is not the same as the current firmware.
- Ensure that the target firmware is applicable to the phone 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 web user interface.

The phone does not update the configurations

Do one of the following:

- Ensure that the configuration is set correctly.
- Reboot the phone. Some configurations require a reboot to take effect.
- Ensure that the configuration is applicable to the phone 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 web user interface on your phone.
- Reboot the phone. 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 phone.
- Ensure that you have configured the syslog server address correctly via web user interface on your phone.
- Reboot the phone. 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.