Yealink

VC210 Teams® Collaboration Bar Administrator Guide



Version 15.47 | April. 2021

Contents

Introduction..... 6
Related Documentations..... 6
Typographic and Writing Conventions..... 6
Recommended References..... 7
Summary of Changes..... 7
Changes for Guide Version 15.47..... 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..... 9
Teams Feature License..... 9
Importing License via the Web User Interface..... 9
Importing License Configuration..... 9

Device 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..... 18
DHCP Option 42 and Option 2..... 18
DHCP Option 12..... 18
DHCP Option 60..... 19
DHCP Option for IPv6..... 19
Supported DHCP Option for IPv6..... 19
VLAN..... 19
LLDP Configuration..... 20
Manual VLAN Configuration..... 20
DHCP VLAN Configuration..... 21
VLAN Change Configuration..... 22
Wi-Fi..... 22
Wi-Fi Configuration..... 22
Internet Port..... 25
Supported Transmission Methods..... 25
Internet Port Configuration..... 25
802.1x Authentication..... 25
802.1x Authentication Configuration..... 26
Quality of Service (QoS)..... 27

QoS Configuration..... 27
Maximum Transmission Unit (MTU)..... 28
MTU Configuration..... 28

Device Provisioning..... 29
Provisioning Points to Consider..... 29
Boot Files, Configuration Files, and Resource Files..... 29
Boot Files..... 30
Configuration Files..... 32
Resource Files..... 34
Files Download Process..... 35
Provisioning Methods..... 36
Provisioning Methods Priority..... 36
Manual Provisioning..... 36
Central Provisioning..... 39
Setting Up a Provisioning Server..... 42
Supported Provisioning Protocols..... 42
Supported Provisioning Server Discovery Methods..... 43
Configuring a Provisioning Server..... 44

Provisioning Devices on the Microsoft Teams & Skype for Business Admin Center..... 44
Device Management..... 45
Editing Your Device Info..... 45
Customizing the Displayed Elements of Devices..... 45
Viewing the Device Details..... 45
Assigning Configuration Profile to Devices..... 46
Diagnostic Devices..... 46
Updating Device Software..... 46
Restarting Your Devices..... 47
Configuration Profiles Management..... 47
Creating a Configuration Profile..... 47
Editing a Configuration Profile..... 47
Assigning Configuration Profile to Devices..... 48

Firmware Upgrade..... 48
Firmware for Each Device Model..... 48
Firmware Upgrade Configuration..... 48

Device Customization..... 49
Language..... 49
Language Display Configuration..... 50
Language Customization..... 50
Example: Setting a Custom Language for Device Display..... 55
Screen Saver..... 55
Screensaver Configuration..... 55
Backlight..... 57
Backlight Brightness and Time Configuration..... 58
Time and Date..... 58
Time Zone..... 58
NTP Settings..... 60

DST Settings....62
Time and Date Manual Configuration....66
Time and Date Format Configuration....66

Security Features....67
User and Administrator Identification....67
User and Administrator Identification Configuration....68
Enabling the User Role....69
Transport Layer Security (TLS)....70
Supported Cipher Suites....70
Supported Trusted and Server Certificates....71
TLS Configuration....73
Encrypting Configuration Files....75
Configuration Files Encryption Tools....75
Configuration Files Encryption and Decryption....76
Encryption and Decryption Configuration....76
Example: Encrypting Configuration Files....77

Configuring Camera Settings....79
Camera Mode Configuration....79
Adjusting the White Balance....80
Adjusting the Exposure....80
Configuring Auto Exposure Mode....81
Configuring Manual Exposure Mode....82
Configuring the Mode of Shutter Priority....82
Configuring the Mode of Brightness Priority....83
Adjusting the Camera Display Image....84
Adjusting Hangup Mode and Camera Pan Direction....86
Reset Camera....86

Configuring Audio Settings....86
EQ Self Adaption....87
EQ Self Adaption Configuration....87
Noise Suppression....87
Noise Suppression Configuration....87

Troubleshooting Methods....88
Exporting All the Diagnostic Files....88
Log Files....88
Local Log....88
Syslog Log....93
Packets Capture....96
Capturing the Packets via Web User Interface....96
Ethernet Software Capturing Configuration....97
Analyzing Configuration Files....97
Exporting BIN Files from the Device....97
Importing BIN Files from the Device....97
Device Status....98
Viewing the Device Status....98
Resetting Device and Configuration....98
Resetting the Device to Default Factory Settings....98
Resetting the Device to Custom Factory Settings....99

Deleting the Custom Factory Settings Files....99
Device Reboot....100
Rebooting the Device via Endpoint....100
Rebooting the Device via Web User Interface....100
Capturing the Current Screen of the Device....100

Troubleshooting Solutions....100
IP Address Issues....101
The device does not get an IP address....101
IP Conflict....101
Specific format in configuring IPv6 on Yealink devices....101
Time and Date Issues....101
Display time and date incorrectly....101
Display Issues....102
The device LCD screen blank....102
The device displays “Offline”....102
Firmware and Upgrading Issues....102
Fail to upgrade the device firmware....102
The device does not update the configurations....102
System Log Issues....102
Fail to export the system log from a provisioning server (FTP/TFTP server)....103
Fail to export the system log from a syslog server....103
Password Issues....103
Restore the administrator password....103

Introduction

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

Yealink VC210 Microsoft Teams devices are the collaborative devices with Microsoft. As an administrator, you can do the following with this guide:

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

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

- VC210 Teams video collaboration bar: 118.15.0.47 or later

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

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

Related Documentations

The following related documents are available:

- Quick Start Guides, describe how to assemble Teams devices and configure the most basic features available on the devices.
- User Guides, describe how to configure and use the basic and advanced features available on the devices via the endpoint or web user interface.

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/endpoint items such as menus, menu selections, soft keys, or directory names when they are involved in a procedure or user action (for example, select **Settings** > **Device Settings**. Also used to emphasize text (for example, **Important!**).
Italics	Used to emphasize text, to show the example values or inputs (format of examples: http(s)://[*IPv6address*]).

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

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

Recommended References

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

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

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

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

Summary of Changes

- Changes for Guide Version 15.47

Changes for Guide Version 15.47

Major updates have occurred to the following sections:

- User and Administrator Identification
- TLS Configuration

The following features are be cancelled:

- Screen savers.

Getting Started

This chapter provides basic initialization instructions for Teams devices.

- Initialization Process Overview
- Verifying Startup
- Teams Feature License

Initialization Process Overview

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

- Loading the ROM File
- Configuring the VLAN
- Querying the DHCP (Dynamic Host Configuration Protocol) Server
- Contacting the Provisioning Server
- Updating Firmware
- Downloading the Resource Files

Loading the ROM File

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

Configuring the VLAN

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

Querying the DHCP (Dynamic Host Configuration Protocol) Server

The device is capable of querying a DHCP server.

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

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

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

Contacting the Provisioning Server

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

Updating Firmware

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

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

Downloading the Resource Files

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

Verifying Startup

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

The setup wizard appears on the monitor and you can select the language via your remote control or touch control.

Teams Feature License

Yealink offers VC210 devices configured for use with Microsoft Teams. By default, the device has a built-in Teams feature license, which allows users to use Yealink devices with Teams features directly. If the device has not imported a license yet, the screen will be shown as below:



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

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

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

Related information

Firmware Upgrade

Importing License via the Web User Interface

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

Procedure

1. On your web user interface, go to **Security** > **License**.
2. In the **Upload License File** block, click the white box to select the license from your local system.
3. Click **Upload**.

Importing License Configuration

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

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

Description	It configures the access URL of the Teams feature license. **Example**: lync_license_dat.url = http://192.168.1.20/License_$MAC.dat The devices will replace the characters “$MAC” with their MAC addresses during auto provisioning. For example, the MAC address of one VC210 Teams device is 00156543EC97. When performing auto provisioning, the device will request to download the License_00156543ec97.dat file from the provisioning server address “http://192.168.1.20”.
Permitted Values	String within 99 characters
Default	Blank
Web UI	**Security** > **License** > **Upload License File**

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

Device Network

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

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

IPv4 and IPv6 Network Settings

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

Note: Teams devices comply with the DHCPv4 specifications documented in RFC 2131, and DHCPv6 specifications documented in RFC 3315.

- IP Addressing Mode Configuration
- IPv4 Configuration
- IPv6 Configuration

IP Addressing Mode Configuration

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

Parameter	static.network.ip_address_mode[1]	<MAC>.cfg
Description	It configures the IP addressing mode.	
Permitted Values	**0**-IPv4 **1**-IPv6 **2**-IPv4 & IPv6	
Default	0	
Web UI	**Network** > **LAN Configuration** > **Internet Port** > **IPv4/IPv6**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IP Mode**	

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

IPv4 Configuration

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

Parameter	static.network.internet_port.type[1]	<MAC>.cfg
Description	It configures the Internet port type for IPv4. **Note**: It works only if “static.network.ip_address_mode” is set to 0 (IPv4) or 2 (IPv4 & IPv6).	
Permitted Values	**0**-DHCP **2**-Static IP	
Default	0	
Web UI	**Network** > **LAN Configuration** > **IPv4 Config** > **Configuration Type**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv4 Type** > **DHCP**	
Parameter	**static.network.internet_port.ip[1]**	**<MAC>.cfg**
Description	It configures the IPv4 address. **Note**: It works only if “static.network.ip_address_mode” is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP).	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	**Network** > **LAN Configuration** > **IPv4 Config** > **Configuration Type(Static IP)** > **IP Address**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv4 Type** > **DHCP (Off)** > **IP Address**	
Parameter	**static.network.internet_port.mask[1]**	**<MAC>.cfg**

Description	It configures the IPv4 subnet mask. **Note**: It works only if “static.network.ip_address_mode” is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP).	
Permitted Values	Subnet Mask	
Default	Blank	
Web UI	**Network** > **LAN Configuration** > **IPv4 Config** > **Configuration Type(Static IP)** > **Subnet Mask**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv4 Type** > **DHCP (Off)** > **Subnet Mask**	
Parameter	**static.network.internet_port.gateway**[1]	**<MAC>.cfg**
Description	It configures the IPv4 default gateway. **Note**: It works only if “static.network.ip_address_mode” is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP).	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	**Network** > **LAN Configuration** > **IPv4 Config** > **Configuration Type(Static IP)** > **Gateway**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv4 Type** > **DHCP (Off)** > **Gateway**	
Parameter	**static.network.static_dns_enable**[1]	**<y0000000000xx>.cfg**
Description	It triggers the static DNS feature to on or off. **Note:** It works only if “static.network.internet_port.type” is set to 0 (DHCP).	
Permitted Values	**0**-Off, the device will use the IPv4 DNS obtained from DHCP. **1**-On, the device will use manually configured static IPv4 DNS.	
Default	0	
Web UI	**Network** > **LAN Configuration** > **IPv4 Config** > **Static DNS**	
Phone UI	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv4 Type** > **IPv4 Static DNS**	
Parameter	**static.network.primary_dns**[1]	**<MAC>.cfg**
Description	It configures the primary IPv4 DNS server. **Note**: It works only if “static.network.ip_address_mode” is set to 0 (IPv4) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure “static.network.static_dns_enable" is set to 1 (On).	
Permitted Values	IPv4 Address	

Default	Blank	
Web UI	**Network** > **LAN Configuration** > **IPv4 Config** > **Configuration Type(Static IP)** > **Primary DNS** Or **Network** > **LAN Configuration** > **IPv4 Config** > **Configuration Type(DHCP)** > **Static DNS(On)** > **Primary DNS**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv4 Type** > **DHCP(Off)** > **IPv4 Pri DNS** Or **More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv4 Type** > **IPv4 Static DNS(On)** > **IPv4 Pri DNS**	
Parameter	**static.network.secondary_dns** [1]	**<MAC>.cfg**
Description	It configures the secondary IPv4 DNS server. **Note**: It works only if “static.network.ip_address_mode” is set to 0 (IPv4) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure “static.network.static_dns_enable" is set to 1 (On).	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	**Network** > **LAN Configuration** > **IPv4 Config** > **Configuration Type(Static IP)** > **Secondary DNS** Or **Network** > **LAN Configuration** > **IPv4 Config** > **Configuration Type(DHCP)** > **Static DNS(On)** > **Secondary DNS**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv4 Type** > **DHCP(Off)** > **IPv4 Sec DNS** Or **More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv4 Type** > **IPv4 Static DNS(On)** > **IPv4 Sec DNS**	

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

IPv6 Configuration

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

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

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

Parameter	**static.network.ipv6_internet_port.type**[1]	**<MAC>.cfg**

Description	It configures the Internet port type for IPv6. **Note**: It works only if “static.network.ip_address_mode” is set to 1 (IPv6) or 2 (IPv4 & IPv6).	
Permitted Values	**0**-DHCP **1**-Static IP	
Default	0	
Web UI	**Network** > **LAN Configuration** > **IPv6 Config** > **Configuration Type**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv6 Type**	
Parameter	**static.network.ipv6_internet_port.ip**[1]	**<MAC>.cfg**
Description	It configures the IPv6 address. **Note**: It works only if “static.network.ip_address_mode” is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP).	
Permitted Values	IPv6 Address	
Default	Blank	
Web UI	**Network** > **LAN Configuration** > **IPv6 Config** > **Configuration Type(Static IP)** > **IP Address**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv6 Type** > **DHCP (Off)** > **IP Address**	
Parameter	**static.network.ipv6_prefix**[1]	**<MAC>.cfg**
Description	It configures the IPv6 prefix. **Note**: It works only if “static.network.ip_address_mode” is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP).	
Permitted Values	Integer from 0 to 128	
Default	64	
Web UI	**Network** > **LAN Configuration** > **IPv6 Config** > **Configuration Type(Static IP)** > **IPv6 prefix(0~128)**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv6 Type** > **DHCP (Off)** > **IPv6 IP Prefix**	
Parameter	**static.network.ipv6_internet_port.gateway**[1]	**<MAC>.cfg**
Description	It configures the IPv6 default gateway. **Note**: It works only if “static.network.ip_address_mode” is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP).	
Permitted Values	IPv6 Address	
Default	Blank	

Web UI	**Network** > **LAN Configuration** > **IPv6 Config** > **Configuration Type(Static IP)** > **Gateway**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv6 Type** > **DHCP (Off)** > **Gateway**	
Parameter	**static.network.ipv6_static_dns_enable**[1]	**<MAC>.cfg**
Description	It triggers the static IPv6 DNS feature to on or off. **Note:** It works only if “static.network.ipv6_internet_port.type” is set to 0 (DHCP).	
Permitted Values	**0-**Off, the device will use the IPv6 DNS obtained from DHCP. **1-**On, the device will use manually configured static IPv6 DNS.	
Default	0	
Web UI	**Network** > **LAN Configuration** > **IPv6 Config** > **Static IPv6 DNS**	
Phone UI	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv6 Type** > **IPv6 Static DNS** **Menu** > **Setting** > **Advanced (default password: admin)** > **Network** > **WAN Port** > **IPv6** > **Type(DHCP)** > **Static DNS**	
Parameter	**static.network.ipv6_primary_dns**[1]	**<MAC>.cfg**
Description	It configures the primary IPv6 DNS server. **Note**: It works only if “static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure “static.network.ipv6_static_dns_enable" is set to 1 (On).	
Permitted Values	IPv6 Address	
Default	Blank	
Web UI	**Network** > **LAN Configuration** > **IPv6 Config** > **Configuration Type(Static IP)** > **Primary DNS** Or **Network** > **LAN Configuration** > **IPv6 Config** > **Configuration Type(DHCP)** > **Static IPv6 DNS(On)** > **Primary DNS**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv6 Type** > **DHCP(Off)** > **IPv6 Pri DNS** Or **More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv6 Type** > **DHCP(On)** > **IPv6 Static DNS(On)** > **IPv6 Pri DNS**	
Parameter	**static.network.ipv6_secondary_dns**[1]	**<MAC>.cfg**
Description	It configures the secondary IPv6 DNS server. **Note**: It works only if “static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure “static.network.ipv6_static_dns_enable" is set to 1 (On).	
Permitted Values	IPv6 Address	
Default	Blank	

Web UI	**Network** > **LAN Configuration** > **IPv6 Config** > **Configuration Type(Static IP)** > **Secondary DNS** Or **Network** > **LAN Configuration** > **IPv6 Config** > **Configuration Type(DHCP)** > **Static IPv6 DNS(On)** > **Secondary DNS**
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv6 Type** > **DHCP(Off)** > **IPv6 Sec DNS** Or **More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **Ethernet** > **IPv6 Type** > **DHCP(On)** > **IPv6 Static DNS(On)** > **IPv6 Sec DNS**

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

DHCP Option for IPv4

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

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

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

Supported DHCP Option for IPv4

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

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

Parameter	DHCP Option	Description
Network Time Protocol Servers	42	Specify a list of NTP servers available to the client by IP address.
Vendor-Specific Information	43	Identify the vendor-specific information.
Vendor Class Identifier	60	Identify the vendor type.
TFTP Server Name	66	Identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.

DHCP Option 160 and Option 161

Yealink Teams devices support obtaining the provisioning server address by detecting DHCP custom option during startup.

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

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

- DHCP Option 160 and Option 161 Configuration

DHCP Option 160 and Option 161 Configuration

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

Parameter	static.auto_provision.dhcp_option.enable[1]	<y0000000000xx>.cfg
Description	It triggers the DHCP Option feature to on or off.	
Permitted Values	**0**-Off **1**-On	
Default	1	
Web UI	**Setting** > **Auto Provision** > **DHCP Active**	
Parameter	**static.auto_provision.dhcp_option.list_user_options**[1]	**<y0000000000xx>.cfg**
Description	It configures the custom DHCP option for requesting provisioning server address. Multiple DHCP options are separated by commas. **Note**: It works only if “static.auto_provision.dhcp_option.enable” is set to 1 (On).	
Permitted Values	Integer from 128 to 254	
Default	160,161	
Web UI	**Setting** > **Auto Provision** > **Custom Option**	

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

DHCP Option 66, Option 43 and Custom Option

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

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

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

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

DHCP Option 42 and Option 2

Yealink Teams devices can use the NTP server address offered by DHCP.

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

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

Related information

NTP Settings

DHCP Option 12

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

- DHCP Option 12 Hostname Configuration

DHCP Option 12 Hostname Configuration

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

Parameter	static.network.dhcp_host_name[1]	<y0000000000xx>.cfg
Description	It configures the DHCP option 12 hostname on the device.	
Permitted Values	String within 99 characters	
Default	VC210	
Web UI	Network > LAN Configuration > Host Name	

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

DHCP Option 60

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

- DHCP Option 60 Configuration

DHCP Option 60 Configuration

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

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

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

DHCP Option for IPv6

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

- Supported DHCP Option for IPv6

Supported DHCP Option for IPv6

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

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

VLAN

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

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

- LLDP Configuration
- Manual VLAN Configuration
- DHCP VLAN Configuration
- VLAN Change Configuration

LLDP Configuration

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

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

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

Parameter	**static.network.lldp.enable**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the LLDP feature on the device.	
Permitted Values	**0**-Disabled **1**-Enabled, the device will attempt to determine its VLAN ID through LLDP.	
Default	1	
Web UI	**Network** > **Advanced** > **LLDP** > **Active**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **LLDP protocol** > **Activated**	
Parameter	**static.network.lldp.packet_interval**[1]	**<y0000000000xx>.cfg**
Description	It configures the interval (in seconds) that how often the device sends the LLDP request. **Note**: It works only if “static.network.lldp.enable” is set to 1 (Enabled).	
Permitted Values	Integer from 1 to 3600	
Default	60	
Web UI	**Network** > **Advanced** > **LLDP** > **Packet Interval(1-3600s)**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **LLDP protocol** > **Contracting interval(1-3600s)**	

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

Manual VLAN Configuration

VLAN is disabled on the devices by default. Before configuring VLAN on the device, you need to obtain the VLAN ID from your network administrator.

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** > **Internet Port** > **Active**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **VLAN** > **Activated**	
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** > **Internet Port** > **VID(1-4094)**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **VLAN** > **Activated(On)** > **VID(1-4094)**	
Parameter	**static.network.vlan.internet_port_priority**[1]	**<y0000000000xx>.cfg**
Description	It configures the VLAN priority for the Internet port. 7 is the highest priority, 0 is the lowest priority. **Note**: It works only if "static.network.vlan.internet_port_enable" is set to 1 (Enabled).	
Permitted Values	Integer from 0 to 7	
Default	1	
Web UI	**Network** > **Advanced** > **VLAN** > **Internet Port** > **Priority**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network (default password: 0000)** > **VLAN** > **Activated(On)** > **Priority**	

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

DHCP VLAN Configuration

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

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

Parameter	static.network.vlan.dhcp_enable[1]	<y0000000000xx>.cfg

Description	It enables or disables the DHCP VLAN discovery feature on the device.	
Permitted Values	**0**-Disabled **1**-Enabled.	
Default	1	
Web UI	**Network** > **Advanced** > **DHCP VLAN** > **Active**	
Parameter	**static.network.vlan.dhcp_option**[1]	**<y0000000000xx>.cfg**
Description	It configures the DHCP option from which the device obtains the VLAN settings. You can configure at most five DHCP options and separate them by commas.	
Permitted Values	Integer from 1 to 255	
Default	132	
Web UI	**Network** > **Advanced** > **DHCP VLAN** > **Option**	

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

VLAN Change Configuration

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

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

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

Wi-Fi

Wi-Fi feature enables you to connect the devices to the organization's wireless network.

- Wi-Fi Configuration

Wi-Fi Configuration

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

Parameter	**static.wifi.function.enable** [1]	**<y0000000000xx>.cfg**
Description	It enables or disables the Wi-Fi feature.	

Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Parameter	**static.wifi.enable**	**<y0000000000xx>.cfg**
Description	It activates or deactivates the Wi-Fi mode. **Note:** It works only if “static.wifi.function.enable” is set to 1 (Enabled).	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Network** > **Wi-Fi** > **Wi-Fi**	
Endpoint	**More** > **Settings** > **Device Settings** > **Wi-Fi (default password: 0000)** > **Wi-Fi**	
Parameter	**static.wifi.X.label**[2]	**<y0000000000xx>.cfg**
Description	It configures the profile name of a specific wireless network. **Note:** It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	String within 32 characters	
Default	Blank	
Parameter	**static.wifi.X.ssid**[2]	**<y0000000000xx>.cfg**
Description	It configures the SSID of a specific wireless network. SSID is a unique identifier for accessing wireless access points. **Note:** It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	String within 32 characters	
Default	Blank	
Parameter	**static.wifi.X.priority**[2]	**<y0000000000xx>.cfg**
Description	It configures the priority for a specific wireless network. 5 is the highest priority, 1 is the lowest priority. **Note:** It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	Integer from 1 to 5	
Default	1	
Parameter	**static.wifi.X.security_mode**[2]	**<y0000000000xx>.cfg**
Description	It configures the security mode of a specific wireless network. **Note:** It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	

Permitted Values	NONE, WEP, WPA/WPA2 PSK, 802.1x EAP	
Default	NONE	
Parameter	**static.wifi.X.cipher_type**[2]	**<y0000000000xx>.cfg**
Description	It configures the encryption type of a specific wireless network. If "static.wifi.X.security_mode" is set to **NONE**, the permitted value of this parameter is **NONE**. If "static.wifi.X.security_mode" is set to **802.1x EAP**, the permitted values of this parameter are **PEAP**, **TLS**, **TTLS**, or **PWD**. **Note:** It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	NONE, PEAP, TLS, TTLS, PWD	
Default	NONE	
Parameter	**static.wifi.X.password**[2]	**<y0000000000xx>.cfg**
Description	It configures the password of a specific wireless network. **Note:** It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	String within 64 characters	
Default	Blank	
Parameter	**static.wifi.X.eap_type**[2]	**<y0000000000xx>.cfg**
Description	It configures the EAP authentication mode of a specific wireless network. **Note:** It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	TTLS, PEAP or TLS	
Default	Blank	
Parameter	**static.wifi.X.eap_user_name**[2]	**<y0000000000xx>.cfg**
Description	It configures the EAP authentication username of a specific wireless network. **Note:** It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	String within 64 characters	
Default	Blank	
Parameter	**static.wifi.X.eap_password**[2]	**<y0000000000xx>.cfg**
Description	It configures the EAP authentication password of a specific wireless network. **Note:** It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).	
Permitted Values	String within 64 characters	
Default	Blank	

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

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

Internet Port

You can configure the transmission method for the Internet port.

- Supported Transmission Methods
- Internet Port Configuration

Supported Transmission Methods

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

- Auto Negotiation
- Half-duplex (transmit in 10Mbps or 100Mbps)
- Full-duplex (transmit in 10Mbps, 100Mbps)

Internet Port Configuration

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

Parameter	static.network.internet_port.speed_duplex[1]	<y0000000000xx>.cfg
Description	It configures the transmission method of the Internet port.	
Permitted Values	**0**-Auto Negotiation **1**-Full Duplex 10Mbps **2**-Full Duplex 100Mbps **3**-Half Duplex 10Mbps **4**-Half Duplex 100Mbps	
Default	0	
Web UI	**Network** > **Advanced** > **Speed** > **Network Speed**	

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

802.1x Authentication

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

- EAP-MD5
- EAP-TLS (requires Device and CA certificates, requires no password)
- EAP-PEAP/MSCHAPv2 (requires CA certificates)
- EAP-TTLS/EAP-MSCHAPv2 (requires CA certificates)
- EAP-PEAP/GTC (requires CA certificates)
- EAP-TTLS/EAP-GTC (requires CA certificates)
- EAP-FAST (supports EAP In-Band provisioning, requires CA certificates if the provisioning method is Authenticated Provisioning)

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

- 802.1x Authentication Configuration

802.1x Authentication Configuration

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

Parameter	**static.network.802_1x.mode**[1]	**<y0000000000xx>.cfg**
Description	It configures the 802.1x authentication method.	
Permitted Values	**0**-Disabled, 802.1x authentication is not required. **1**-EAP-MD5 **2**-EAP-TLS **3**-EAP-MSCHAPv2 **4**-EAP-TTLS/EAP-MSCHAPv2	
Default	0	
Web UI	**Network** > **Advanced** > **802.1x** > **802.1x Mode**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network(default password: 0000)** > **802.1x Mode**	
Parameter	**static.network.802_1x.identity**[1]	**<y0000000000xx>.cfg**
Description	It configures the user name for 802.1x authentication. **Note**: It works only if “static.network.802_1x.mode” is set to 1, 2, 3, 4.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	**Network** > **Advanced** > **802.1x** > **Identity**	
Parameter	**static.network.802_1x.md5_password**[1]	**<y0000000000xx>.cfg**
Description	It configures the password for 802.1x authentication. **Note**: It works only if “static.network.802_1x.mode” is set to 1, 3, 4.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	**Network** > **Advanced** > **802.1x** > **MD5 Password**	
Parameter	**static.network.802_1x.root_cert_url**[1]	**<y0000000000xx>.cfg**
Description	It configures the access URL of the CA certificate. The format of the certificate must be *.pem, *.crt, *.cer or *.der. **Note**: It works only if “static.network.802_1x.mode” is set to 2, 3, 4.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Network** > **Advanced** > **802.1x** > **CA Certificates**	
Parameter	**static.network.802_1x.client_cert_url**[1]	**<y0000000000xx>.cfg**

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

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

Quality of Service (QoS)

Teams video collaboration bar is subject to the bandwidth and the delay. Therefore, the QoS is very important for the network with limited bandwidth. QoS is a major issue in VoIP implementations, regarding how to guarantee that packet traffic is not delayed or dropped due to interference from other lower priority traffic. Your system supports the DiffServ model of QoS.

Audio QoS

The loss of audio packets, the delay and so on may cause poor audio quality. To solve this, you can configure DSCP priority for the audio packets.

Video QoS

Some issues, such as the video packet loss and delay may cause the video images distorted and unclear. To ensure acceptable visual quality for video, video packets emanated from the system should be configured with a high transmission priority.

Data QoS

To ensure better presentation, data packets (PC content) emanated from the system should be configured with a high transmission priority.

DSCPs for audio, video and data packets can be specified respectively.

- QoS Configuration

QoS Configuration

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

Parameter	**static.network.qos.enable**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the QoS feature.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Network** > **Advanced** > **QoS** > **QoS Enable**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network** > **QoS** > **Quality of service**	
Parameter	**static.network.qos.audiotos**[1]	**<y0000000000xx>.cfg**
Description	It configures the DSCP (Differentiated Services Code Point) for audio packets.	

Permitted Values	Integer from 0 to 63	
Default	46	
Web UI	**Network** > **Advanced** > **QoS** > **Audio Priority**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network** > **QoS** > **Audio priority(0-63)**	
Parameter	**static.network.qos.videotos**[1]	**<y0000000000xx>.cfg**
Description	It configures the DSCP (Differentiated Services Code Point) for video packets.	
Permitted Values	Integer from 0 to 63	
Default	34	
Web UI	**Network** > **Advanced** > **QoS** > **Video Priority**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network** > **QoS** > **Video priority(0-63)**	
Parameter	**static.network.qos.signaltos**[1]	**<y0000000000xx>.cfg**
Description	It configures the DSCP (Differentiated Services Code Point) for data packets.	
Permitted Values	Integer from 0 to 63	
Default	26	
Web UI	**Network** > **Advanced** > **QoS** > **Data Priority**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network** > **QoS** > **Data priority(0-63)**	

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

Maximum Transmission Unit (MTU)

Data packets that exceed the maximum transmission unit (MTU) size for any router or segment along the network path may be fragmented or dropped, which may result in poor video quality. You can set the maximum MTU size of the data packets sent by the system.

Configure the MTU size used in calls based on the network bandwidth settings. If the video becomes blocky or network errors occur, packets may be too large; you should decrease the MTU. If the network is burdened with unnecessary overhead; packets may be too small, you should increase the MTU.

- MTU Configuration

MTU Configuration

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

Parameter	**static.network.mtu_value**[1]	**<y0000000000xx>.cfg**
Description	It configures the MTU (Maximum Transmission Unit) of network interface card.	
Permitted Values	Integer from 1000 to 1500	
Default	1500	
Web UI	**Network** > **Advanced** > **MTU** > **Network MTU(1000-1500)**	

Parameter	video.single_packet_mode.enable[1]	<y0000000000xx>.cfg
Description	It enables or disables the restricted single packet mode. **Note**: Some third-party devices only accept the data packets sent by single packet mode. If local system sends data packets by using multiple packets mode, the video call may be come with the mosaic. To avoid this situation, enable this Restricted Single Packet Mode.	
Permitted Values	**0**-Off, sends data packets by using multiple packets mode. **1**-On, sends data packets by using single packet mode.	
Default	1	
Web UI	**Network** > **Advanced** > **MTU** > **Restricted Single Packet Mode**	

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

Device Provisioning

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

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

Provisioning Points to Consider

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

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

Related information

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

Boot Files, Configuration Files, and Resource Files

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

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

- Boot Files
- Configuration Files

- Resource Files
- Files Download Process

Boot Files

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

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

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

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

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

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

Common Boot File

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

MAC-Oriented Boot File

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

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

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

Boot File Attributes

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

Attributes	Description
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.

Attributes	Description
include:config <xxx.cfg> include:config "xxx.cfg"	Each “include” statement can specify a location of a configuration file. The configuration file format must be *.cfg. The locations in the angle brackets or double quotation marks support two forms: • Relative path (relative to the boot file): For example, sip.cfg, HTTP Directory/sip.cfg • Absolute path (or URL): For example, http://10.2.5.258/Teams.cfg The location must point to a specific CFG file.
[$MODEL]	The [$MODEL] can be added to specify settings for specific phone models. $MODEL represents the device model name. The valid device model name is: VC210.
overwrite_mode	Enable or disable the overwrite mode. The overwrite mode applies to the configuration files specified in the boot file. Note that it only affects the parameters pre-provisioned via central provisioning. **1-(Enabled)** - If the value of a parameter in the configuration files is left blank, or if a non-static parameter in the configuration files is deleted or commented out, the factory default value takes effect. **0-(Disabled)** -If the value of a parameter in the configuration files is left blank, deleted or commented out, the pre-configured value is kept. **Note**: Overwrite mode can only be used in boot files. If a boot file is used, but the value of the parameter “overwrite_mode” is not configured, the overwrite mode is enabled by default.
specific_model.excluded_mode	Enable or disable the exclude mode. The exclude mode applies to the configuration files specified in the boot file. **0-Disabled** (**Append Mode**), the device downloads its own model-specific configuration files and downloads other model-unspecified configuration files. **1-Enabled** (**Exclude Mode**), the device attempts to download its own model-specific configuration files; if there are no own model-specific configuration files found on the server, it downloads model-unspecified configuration files. **Note**: Exclude mode can only be used in boot files. If a boot file is used but the value of the parameter “specific_model.excluded_mode” is not configured, the exclude mode is disabled by default.

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

Customizing a Boot File

Procedure

1. Open a boot template file.

2. To add a configuration file, add *include:config <>* or *include:config “”* to the file. Each starts on a separate line.
3. Specify a configuration file for downloading.
   For example:
   - include:config <configure/Teams.cfg>
   - include:config “http://10.2.5.206/configure/account.cfg”
4. Specify the overwrite mode and exclude mode.
   For example:
   - overwrite_mode = 1
   - specific_model.excluded_mode = 1
5. Save the boot file and place it on the provisioning server.

Related information

Boot File Attributes

Configuration Files

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

These configuration files contain two kinds of parameters:

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

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

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

- Common CFG File
- MAC CFG File
- Configuration File Customization

Common CFG File

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

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

Device Model	Common CFG file
VC210	y000000000118.cfg

MAC CFG File

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

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

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

MAC-Oriented CFG File

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

MAC-local CFG File

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

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

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

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

The provisioning priority mechanism is enabled by the parameter “static.auto_provision.custom.protect”.

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

MAC-local CFG File Configuration

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

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

Clearing MAC-local CFG File

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

- Via endpoint at the path: **More** > **Settings** > **Device Settings** > **Debug(Admin only, default password: 0000)** > **Reset user settings**.

- Via web user interface at the path: **Settings** > **Upgrade** > **Reset to Factory Setting** > **Reset Local Settings**.

  Note: The **Reset user settings/Reset Local Settings** option appears only if you set "static.auto_provision.custom.protect = 1".

Configuration File Customization

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

- Customizing a Configuration File
- Configuration File Attributes

Customizing a Configuration File

Procedure

1. Copy and rename a configuration template file. For example, Teams.cfg.
2. Rearrange the parameters in the Teams.cfg, and set the valid values for them.

   For example:

   phone_setting.phone_lock.enable= 1

3. 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	Specify the parameters and values to apply specific settings to the devices. • Separate each configuration parameter and value with an equal sign • Set only one configuration parameter per line • Put the configuration parameter and value on the same line, and do not break the line

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

Resource Files

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

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

- Supported Resource Files

Supported Resource Files

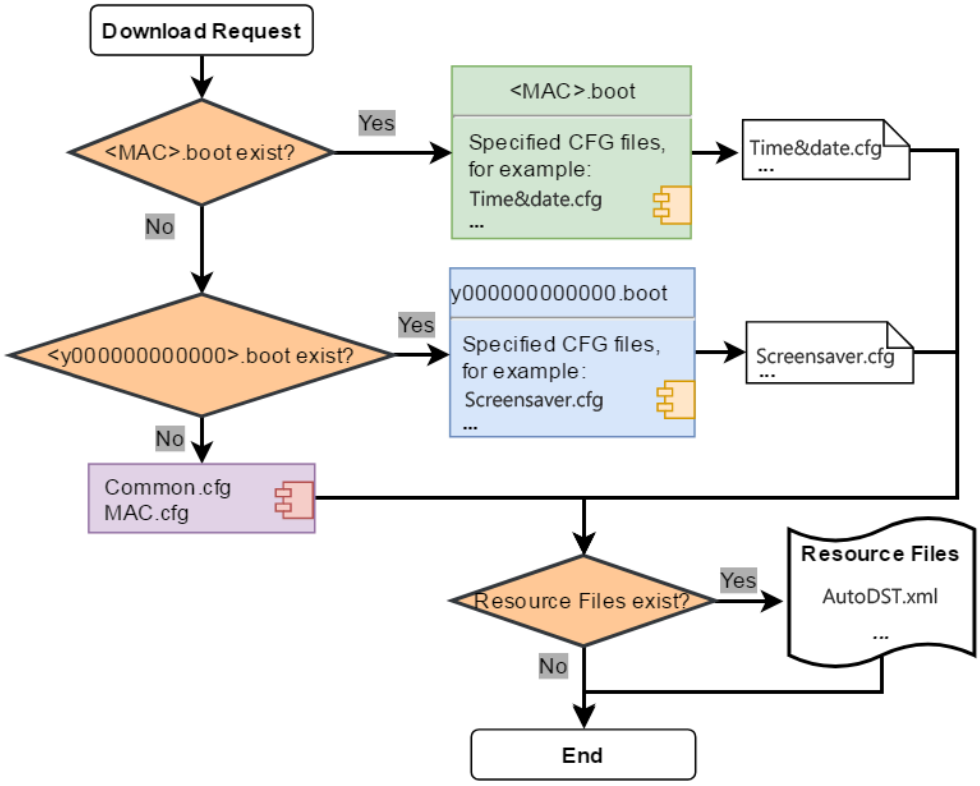
Yealink supplies some template of resource files for you, so you can directly edit the files as required.

The following table lists the resource files Yealink supplies:

Template File	File Name	Description	Reference in Section
AutoDST Template	AutoDST.xml	Add or modify the time zone and DST settings.	DST Settings
Language Packs	For example, 000.GUI.English.lang 1.English_note.xml 1.English.js	Customize the language file to display on the endpoint/web user interface.	Language Customization

Files Download Process

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



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

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

Provisioning Methods

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

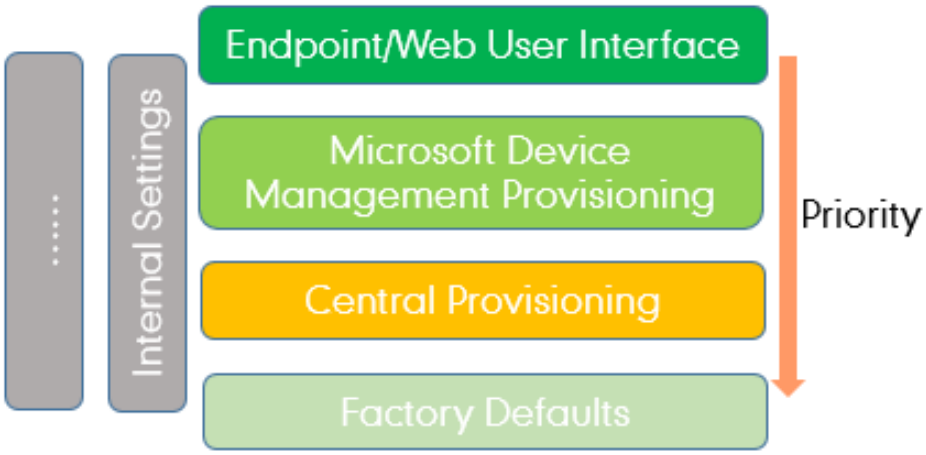
- **Central Provisioning**: configuration files stored on a central provisioning server.
- **Manual Provisioning:** operations on the web user interface or endpoint.

- 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 endpoint or configuration files) you are using for provisioning.

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

Related information

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

Manual Provisioning

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

- Web User Interface Access
- Endpoint

Web User Interface Access

When configuring the devices via the web user interface, you are required to have a user name and password for access. The default administrator username is “admin” (case-sensitive) and password is “0000”.

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

Accessing the Web User Interface

Procedure

1. Go to **More** > **Settings** > **Device Settings** > **About** > **IPv4**.
2. Enter the device IP address in the address bar of a web browser on your PC.
   For example, for IPv4: http://192.168.0.10 or 192.168.0.10; for IPv6: http://[2005:1:1:1:215:65ff:fe64:6e0a] or [2005:1:1:1:215:65ff:fe64:6e0a]
3. Enter the user name and password.
4. Click **Login**.

Web Server Type Configuration

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

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

Parameter	**static.wui.http_enable**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the user to access the web user interface of the device using the HTTP protocol.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Network** > **Advanced** > **Web Server** > **HTTP**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network(default password: 0000)** > **Web service type (HTTP&HTTPS or HTTP)**	
Parameter	**static.network.port.http**[1]	**<y0000000000xx>.cfg**
Description	It configures the HTTP port for the user to access the web user interface of the device using the HTTP protocol.	
Permitted Values	Integer from 1 to 65535	
Default	80	
Web UI	**Network** > **Advanced** > **Web Server** > **HTTP Port**	
Parameter	**static.wui.https_enable**[1]	<y0000000000xx>.cfg

Description	It enables or disables the user to access the web user interface of the device using the HTTPS protocol.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	1	
Web UI	**Network** > **Advanced** > **Web Server** > **HTTPS**	
Endpoint	**More** > **Settings** > **Device Settings** > **Network(default password: 0000)** > **Web service type (HTTP&HTTPS or HTTPS)**	
Parameter	**static.network.port.https**[1]	**<y0000000000xx>.cfg**
Description	It configures the HTTPS port for the user to access the web user interface of the device using the HTTPS protocol.	
Permitted Values	Integer from 1 to 65535	
Default	443	
Web UI	**Network** > **Advanced** > **Web Server** > **HTTPS Port**	

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

Importing CFG Configuration Files to Device

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

Procedure

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

Exporting CFG Configuration Files from Device

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

About this task

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

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

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

Procedure

1. From the web user interface, go to **Setting** > **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.

Endpoint

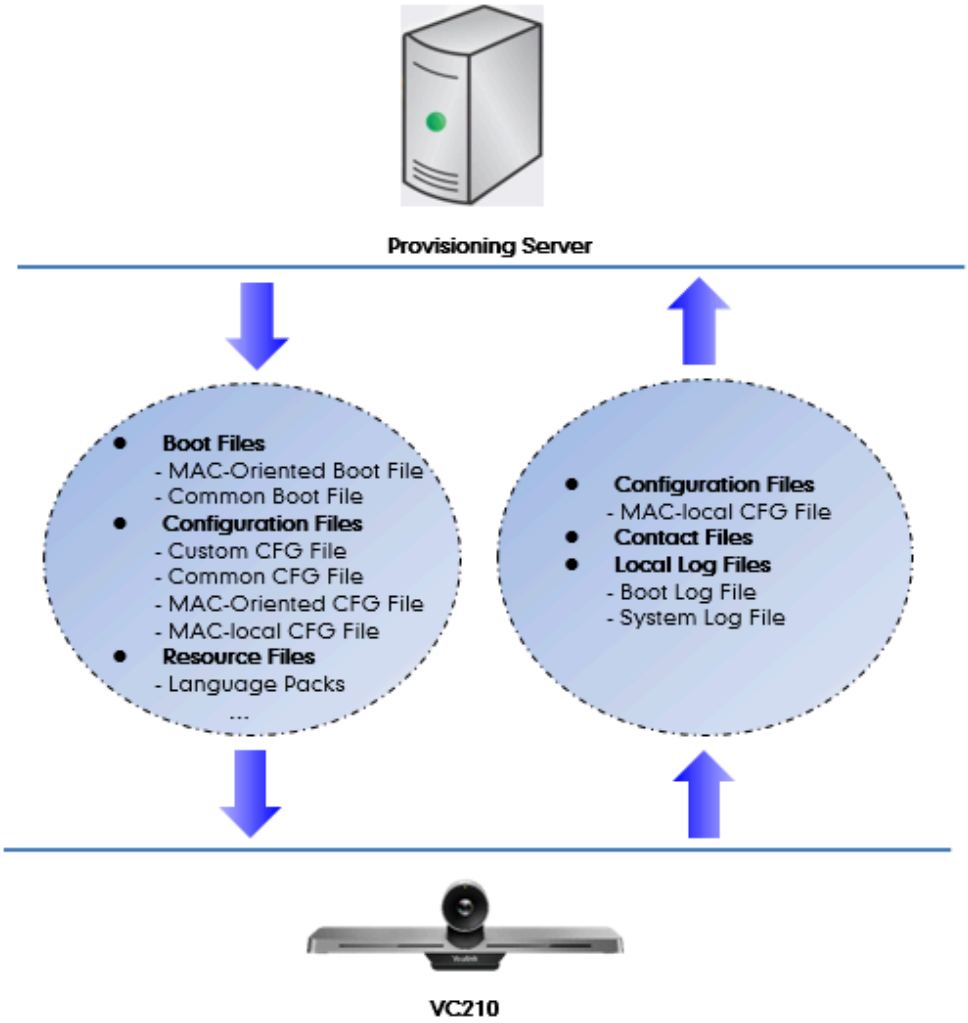
Endpoint makes configurations available to users and administrators, but the **More** > **Settings** > **Device Settings** > **Admin only** option is only available to administrators and requires an administrator password (default: 0000).

You can configure the devices via the endpoint on a per-device basis.

Central Provisioning

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

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



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

Teams devices can obtain the provisioning server address during startup. Then devices download configuration files from the provisioning server, resolve and update the configurations written in configuration files. This entire process is called auto provisioning.

- Auto Provisioning Settings Configuration

Auto Provisioning Settings Configuration

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

Parameter	**static.network.attempt_expired_time**[1]	**<y0000000000xx>.cfg**
Description	It configures the timeout interval (in seconds) to transfer a file for HTTP/HTTPS connection.	
Permitted Values	Integer from 1 to 20	
Default	10	
Parameter	**static.auto_provision.power_on**	**<y0000000000xx>.cfg**

Description	It configures the device whether to perform the auto provisioning when powered on.	
Permitted Values	**0**-Off **1**-On, the device will perform the auto provisioning when powered on.	
Default	1	
Web UI	**Setting** > **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	**Setting** > **Auto Provision** > **Repeatedly**	
Parameter	**static.auto_provision.repeat.minutes**	**<y0000000000xx>.cfg**
Description	It configures the interval (in minutes) for the device to perform the auto provisioning repeatedly. **Note**: It works only if “static.auto_provision.repeat.enable” is set to 1 (On).	
Permitted Values	Integer from 1 to 43200	
Default	1440	
Web UI	**Setting** > **Auto Provision** > **Interval(Minutes)**	
Parameter	**static.auto_provision.weekly.enable**	**<y0000000000xx>.cfg**
Description	It triggers the device to perform the auto provisioning weekly.	
Permitted Values	**0**-Off **1**-On, the device will perform an auto provisioning process weekly.	
Default	0	
Web UI	**Setting** > **Auto Provision** > **Weekly**	
Parameter	**static.auto_provision.weekly.dayofweek**	**<y0000000000xx>.cfg**
Description	It configures the days of the week for the device to perform the auto provisioning weekly. **Example**: static.auto_provision.weekly.dayofweek = 01 It means the device will perform an auto provisioning process every Sunday and Monday. **Note**: It works only if “static.auto_provision.weekly.enable” is set to 1 (On).	

Permitted Values	0,1,2,3,4,5,6 or a combination of these digits **0**-Sunday **1**-Monday **2**-Tuesday **3**-Wednesday **4**-Thursday **5**-Friday **6**-Saturday	
Default	0123456	
Web UI	**Setting** > **Auto Provision** > **Day of Week**	
Parameter	**static.auto_provision.weekly.begin_time** **static.auto_provision.weekly.end_time**	**<y0000000000xx>.cfg**
Description	It configures the start/end time of the day for the device to perform auto provisioning weekly. **Note**: It works only if "static.auto_provision.weekly.enable" is set to 1 (On).	
Permitted Values	Time from 00:00 to 23:59	
Default	00:00	
Web UI	**Setting** > **Auto Provision** > **Time**	

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

Setting Up a Provisioning Server

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

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

Supported Provisioning Protocols

Yealink devices support several transport protocols for provisioning:

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

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

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

Supported Provisioning Server Discovery Methods

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

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

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

- DHCP Provision Configuration
- Static Provision Configuration

DHCP Provision Configuration

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

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

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

Static Provision Configuration

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

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

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

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

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

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

Configuring a Provisioning Server

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

Procedure

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

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

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

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

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

- Editing 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

Editing Your Device Info

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

Procedure

1. Go 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. Go 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 information, software update status, and actions you performed.

Procedure

1. Go 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. Go 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 on the devices.

Related tasks

Creating a Configuration Profile

Diagnostic Devices

You can use the 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. Go 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. Go 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. Go 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, Russian and Netherlands are supported by the device. The language configuration does not take effect when you select other languages.

- Creating a Configuration Profile
- Editing a Configuration Profile
- Assigning Configuration Profile to Devices

Related information

Language

Creating a Configuration Profile

Procedure

1. Go 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 description.
4. Configure the general settings, device settings, or network settings.
5. Click **Save**.

Editing a Configuration Profile

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

Procedure

1. Go 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. Go 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 on the devices.

Firmware Upgrade

There are three methods of firmware upgrade:

- Manually, from the local system for a single device via the web user interface.
- Automatically, from the provisioning server for a mass of devices.
- Upgrade all device software to the latest version with one click on the Microsoft Teams & Skype for Business Admin Center. It is only applicable to devices running the Teams firmware.

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

It supports the bundle upgrade for audio pack when upgrading the firmware - no need for user to have a tool to manage CP900. Do not unplug the CP900 USB cable from VC210 when the device is upgrading firmware. If the upgrade fails, please contact the Yealink support team.

- Firmware for Each Device Model
- Firmware Upgrade Configuration

Related tasks

Updating Device Software

Firmware for Each Device Model

You can download the latest firmware online:

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

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

Device Model	Associated Firmware Name	Firmware Name
VC210	118.x.x.x.rom	118.15.0.47.rom

Firmware Upgrade Configuration

Before upgrading firmware, you need to know the following:

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

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

Parameter	static.firmware.url[1]	<y0000000000xx>.cfg
Description	It configures the access URL of the firmware file.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Setting > Upgrade > Upgrade Firmware	

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

Device Customization

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

- Language
- Screen Saver
- Backlight
- Time and Date

Language

Teams devices support multiple languages. Languages used on the endpoint 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 endpoint and the web user interface.

Phone User Interface/Endpoint		Web User Interface		
Language	Language Pack	Language	Language Pack	Note Language Pack
English	000.GUI.English.lang	English	1.English.js	1.English_note.xml
Chinese Simplified	001.GUI.Chinese_S.lang	Chinese Simplified	2.Chinese_S.js	2.Chinese_S_note.xml
Chinese Traditional	002.GUI.Chinese_T.lang	Chinese Traditional	3.Chinese_T.js	3.Chinese_T_note.xml
French	003.GUI.French.lang	French	4.French.js	4.French_note.xml
German	004.GUI.German.lang	German	5.German.js	5.German_note.xml
Italian	005.GUI.Italian.lang	Italian	6.Italian.js	6.Italian_note.xml
Polish	006.GUI.Polish.lang	Polish	7.Polish.js	7.Polish_note.xml
Portuguese	007.GUI.Portuguese.lang	Portuguese	8.Portuguese.js	8.Portuguese_note.xml
Spanish	008.GUI.Spanish.lang	Spanish	9.Spanish.js	9.Spanish_note.xml

Phone User Interface/Endpoint		Web User Interface		
Language	**Language Pack**	**Language**	**Language Pack**	**Note Language Pack**
Turkish	009.GUI.Turkish.lang	Turkish	10.Turkish.js	10.Turkish_note.xml
Russian	010.GUI.Russian.lang	Russian	11.Russian.js	11.Russian_note.xml
Netherlands	011.GUI.Netherlands.lang	Netherlands	12.Netherlands.js	12.Netherlands_note.xml

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

Language Display Configuration

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

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

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

Language Customization

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

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

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

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

Language for Device Display Customization

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

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

Customizing a Language Pack for Device Display

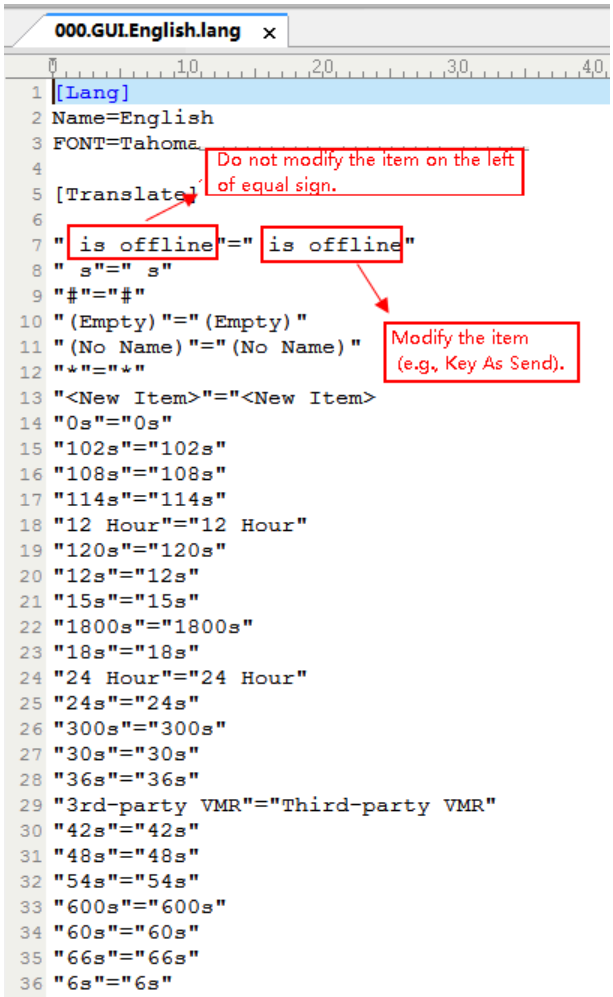
When you add a new language pack for the endpoint, the language pack must be formatted as “X.GUI.name.lang” (X starts from 012, “name” is replaced with the language name). If the language name is the same as the existing one, the existing language pack will be overridden by the newly uploaded one. We recommend that the filename of the new language pack should not be the same as the existing one.

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

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

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

   The following shows a portion of the language pack “000.GUI.English.lang” for the endpoint:



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

Custom Language for Device Display Configuration

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

Parameter	gui_lang.url	<y0000000000xx>.cfg
Description	It configures the access URL of the custom language pack for the endpoint. You can also download multiple language packs to the device simultaneously.	
Permitted Values	URL within 511 characters	
Default	Blank	
Parameter	**gui_lang.delete**	**<y0000000000xx>.cfg**
Description	It deletes the specified or all custom language packs of the endpoint.	
Permitted Values	http://localhost/all or X.GUI.name.lang X starts from 012, “name” is replaced with the language name.	
Default	Blank	

Language for Web Display Customization

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

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

Customizing a Language Pack for Web Display

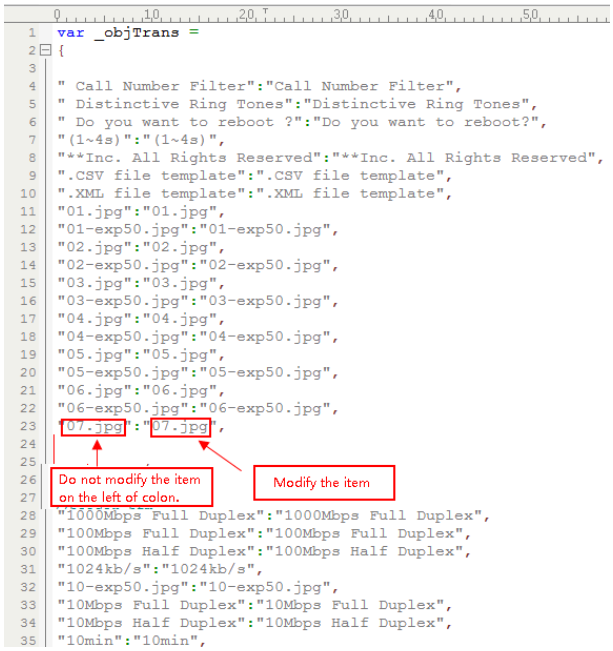
When you add a new language pack for the web user interface, the language pack must be formatted as “X.name.js” (X starts from 13, “name” is replaced with the language name). If the language name is the same as the existing one, the newly uploaded language file will override the existing one. We recommend that the filename of the new language pack should not be the same as the existing one.

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

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

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

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



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

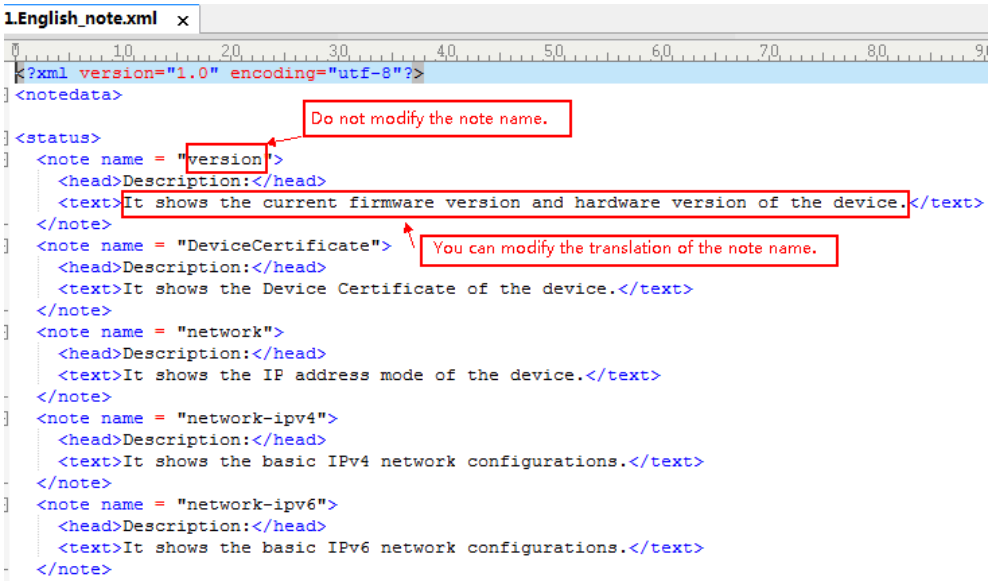
Customizing a Language Pack for Note Display

When you add a new language pack for the note, the note language pack must be formatted as “X.name_note.xml” (X starts from 12, “name” is replaced with the language name). If the note language name is the same as the existing one, the new uploaded note language pack will override the existing one. We recommend that the filename of the new note language pack should not be the same as the existing one.

1. Open the desired note language template pack (for example, 1.English_note.xml) using an XML editor.

2. Modify the text of the note field. Do not modify the note name.

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



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

Custom Language for Web Display Configuration

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

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

Parameter	**wui_lang.url**	**<y0000000000xx>.cfg**
Description	It configures the access URL of the custom language pack for the web user interface.	
Permitted Values	URL within 511 characters For example: http://localhost/X.GUI.name.lang X starts from 012, “name” is replaced with the language name	
Default	Blank	
Parameter	**wui_lang_note.url**	**<y0000000000xx>.cfg**
Description	It configures the access URL of the custom note language pack for web user interface.	
Permitted Values	URL within 511 characters For example: http://localhost/X.name_note.xml X starts from 13, “name” is replaced with the language name	
Default	Blank	
Parameter	**wui_lang.delete**	**<y0000000000xx>.cfg**

Description	It deletes the specified or all custom web language packs and note language packs of the web user interface.
Permitted Values	http://localhost/all or http://localhost/*Y.name.js*
Default	Blank

Example: Setting a Custom Language for Device Display

The following example shows the configuration for uploading custom language files "015.GUI.English_15.lang" and "016.GUI.English_16.lang", and then specify "015.GUI.English_15.lang" to display on the endpoint. These language files are customized and placed on the provisioning server "192.168.10.25".

Example

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

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

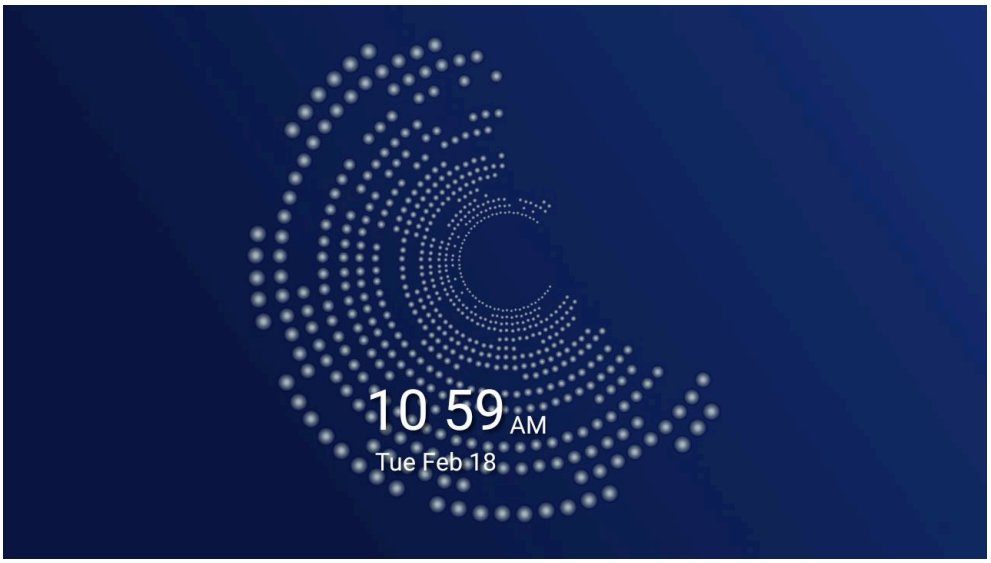
lang.gui=English_15

After provisioning, the language on the endpoint will change to the custom language you defined in "*015.GUI.English_15.lang"*. You can also find a new language selection "*English_15*" and "*English_16*" on the endpoint: **More** > **Settings** > **Device Settings** > **Language**.

Screen Saver

The screen saver will automatically start when the device is idle for the preset waiting time.

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



- Screensaver Configuration

Screensaver Configuration

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

Parameter	screensaver.wait_time	<y0000000000xx>.cfg
Description	It configures the time (in seconds) that the device waits in the idle state before the screen saver starts.	
Permitted Values	**30**-30s **60**-1min **300**-5min **600**-10min **900**-15min **1800**-30min **3600**-1h **7200**-2h	
Default	900	
Web UI	**Setting** > **General** > **Screensaver** > **Screensaver Wait Time**	
Endpoint	**More** > **Settings** > **Device Settings** > **Display** > **Screensaver Waiting Time**	
Parameter	**screensaver.type**	**<y0000000000xx>.cfg**
Description	It configures the type of screen saver to display.	
Permitted Values	**0**-System, the LCD screen will display the built-in picture. **4**-Custom, the LCD screen will display the custom screen saver images (configured by the parameter “screensaver.upload_url”). If multiple images are uploaded, the device will display all images alternately every 60 seconds.	
Default	Blank	
Web UI	**Setting** > **General** > **Screensaver** > **Screensaver Type**	
Endpoint	**More** > **Settings** > **Device Settings** > **Display** > **Screen Saver Type**	
Parameter	**screensaver.upload_url**	**<y0000000000xx>.cfg**
Description	It configures the access URL of the custom screensaver background.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Setting** > **General** > **Screensaver** > **Screensaver Type(Custom)** > **Upload Screensaver**	
Parameter	**screensaver.background**	**<y0000000000xx>.cfg**
Description	It configures the background for the screen saver.	

Permitted Values	Default.jpg 01.png 02.png 03.png 04.png 05.png 06.png 07.png 08.png	
Default	Default.jpg	
Web UI	**Setting** > **General** > **Screensaver** > **Screensaver Type(System)** > **Screensaver Background** **Setting** > **General** > **Screensaver** > **Screensaver Type(Custom)** > **Screensaver**	
Endpoint	**More** > **Settings** > **Device Settings** > **Display** > **Screensaver Type(System)** > **Screensaver background**	
Parameter	**screensaver.delete**	**<y0000000000xx>.cfg**
Description	It deletes the specified or all custom screensaver background. **Example**: Delete all custom screensaver background: screensaver.delete = http://localhost/all Delete a custom screensaver background (for example, Screencapture.jpg): screensaver.delete = http://localhost/Screencapture.jpg	
Permitted Values	String	
Default	Blank	

Backlight

You can change the brightness of LCD backlight when the device is active (in use). The brightness of LCD backlight automatically changes when the device is idle for a specified time.

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

Backlight Active Level: The brightness level of the LCD backlight when the device is active.

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

- **Always On**: Backlight is on permanently.
- **15s**, **30s**, **1min**, **2min**, **5min**, **10min**,**30min**, **45min** or **1h**: Backlight is changed when the device is inactive after the designated time (in seconds).

- Backlight Brightness and Time Configuration

Backlight Brightness and Time Configuration

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

Parameter	phone_setting.backlight_time	<y0000000000xx>.cfg
Description	It configures the delay time (in seconds) to change the intensity of the LCD backlight when the device is inactive.	
Permitted Values	**0**-Always On **15**-15s **30**-30s **60**-1min **120**-2min **300**-5min **600**-10min **1800**-30min **2700**-45min **3600**-1h	
Default	0	
Web UI	**Setting** > **General** > **General Information** > **Backlight Time**	
Endpoint	**More** > **Settings** > **Device Settings** > **Display** > **Backlight Time**	

Time and Date

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

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

Time Zone

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

Time Zone	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)

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

Time Zone	Time Zone Name	Time Zone	Time Zone Name
+1	Albania(Tirane), Austria(Vienna), Belgium(Brussels), Caicos, Chad, Croatia(Zagreb), Czech Republic(Prague), Denmark(Kopenhagen), France(Paris), Germany(Berlin), Hungary(Budapest), Italy(Rome), Luxembourg(Luxembourg), Macedonia(Skopje), Namibia(Windhoek), Netherlands(Amsterdam), Spain(Madrid)	+12:45	New Zealand(Chatham Islands)
+2	Estonia(Tallinn), Finland(Helsinki), Gaza Strip(Gaza), Greece(Athens), Harare,Pretoria,Israel(Tel Aviv), Jordan(Amman), Latvia(Riga), Lebanon(Beirut), Moldova(Kishinev), Romania(Bucharest), Russia(Kaliningrad), Syria(Damascus), Turkey(Ankara), Ukraine(Kyiv, Odessa)	+13	Tonga(Nukualofa)
+3	East Africa Time, Iraq(Baghdad), Russia(Moscow)	+13:30	Chatham Islands
+3:30	Iran(Teheran)	+14	Kiribati
+4	Armenia(Yerevan), Azerbaijan(Baku), Georgia(Tbilisi), Kazakhstan(Aktau), Russia(Samara)		

NTP Settings

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

- NTP Configuration

NTP Configuration

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

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

Description	It enables or disables the device to update time with the offset time offered by the DHCP server. **Note**: It is only available to offset time from Greenwich Mean Time GMT 0.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Setting** > **Date&Time** > **DHCP Time**	
Endpoint	**More** > **Settings** > **Device Settings** > **Time & Date** > **DHCP Time** > **DHCP Time**	
Parameter	**local_time.ntp_server1**	**<MAC>.cfg**
Description	It configures the IP address or the domain name of the NTP server 1. The device will obtain the current time and date from the NTP server 1.	
Permitted Values	IP address or domain name	
Default	cn.pool.ntp.org	
Web UI	**Setting** > **Date&Time** > **Primary Server**	
Endpoint	**More** > **Settings** > **Device Settings** > **Time & Date** > **General** > **NTP Server1**	
Parameter	**local_time.ntp_server2**	**<MAC>.cfg**
Description	It configures the IP address or the domain name of the NTP server 2. If the NTP server 1 is not configured (configured by the parameter "local_time.ntp_server1") or cannot be accessed, the device will request the time and date from the NTP server 2.	
Permitted Values	IP address or domain name	
Default	pool.ntp.org	
Web UI	**Setting** > **Date&Time** > **Secondary Server**	
Endpoint	**More** > **Settings** > **Device Settings** > **Time & Date** > **General** > **NTP Server2**	
Parameter	**local_time.interval**	**<MAC>.cfg**
Description	It configures the interval (in seconds) at which the device updates time and date from the NTP server.	
Permitted Values	Integer from 15 to 86400	
Default	1000	
Web UI	**Setting** > **Date&Time** > **Synchronism (15~86400s)**	
Parameter	**local_time.time_zone**	**<MAC>.cfg**

Description	It configures the interval (in seconds) at which the device updates time and date from the NTP server.	
Permitted Values	-12 to +14 For available time zones, refer to Time Zone.	
Default	+8	
Web UI	**Setting** > **Date&Time** > **Time Zone**	
Endpoint	**More** > **Settings** > **Device Settings** > **Time&Date** > **General** > **Time Zone**	
Parameter	**local_time.time_zone_name**	**<MAC>.cfg**
Description	It configures the time zone name. **Note**: It works only if "local_time.summer_time" is set to 2 (Automatic) and the parameter "local_time.time_zone" should be configured in advance.	
Permitted Values	String within 32 characters The available time zone names depend on the time zone configured by "local_time.time_zone". For available time zone names, refer to Time Zone.	
Default	China(Beijing)	
Web UI	**Setting** > **Date&Time** > **Location**	
Endpoint	**More** > **Settings** > **Device Settings** > **Time & Date** > **General** > **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 device obtains the DST configuration from the AutoDST file.

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

- Auto DST File Customization
- DST Configuration

Auto DST File Customization

Before customizing, you need to obtain the AutoDST file. You can ask the distributor or Yealink FAE for DST template. You can also obtain the DST template online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage.

- Auto DST File Attributes
- Customizing Auto DST File

Auto DST File Attributes

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

Attributes	Type	Values	Description
szTime	required	[+/-][X]:[Y], X=0~14, Y=0~59	Time Zone

Attributes	Type	Values	Description
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

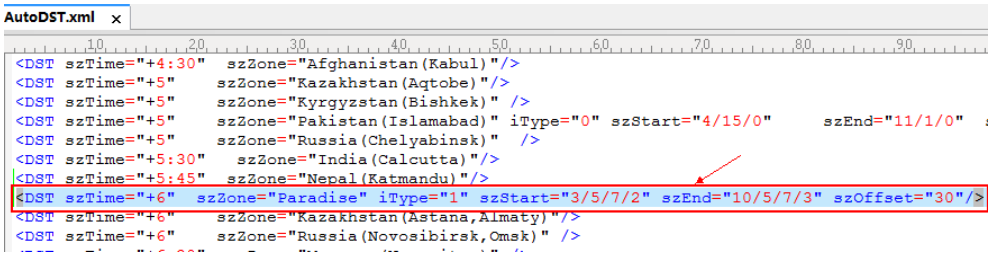
1. Open the AutoDST file.
2. To add a new time zone, add <DST szTime="" szZone="" iType="" szStart="" szEnd="" szOffset=""/> between <DSTData> and </DSTData>.

3. Specify the DST attribute values within double quotes.

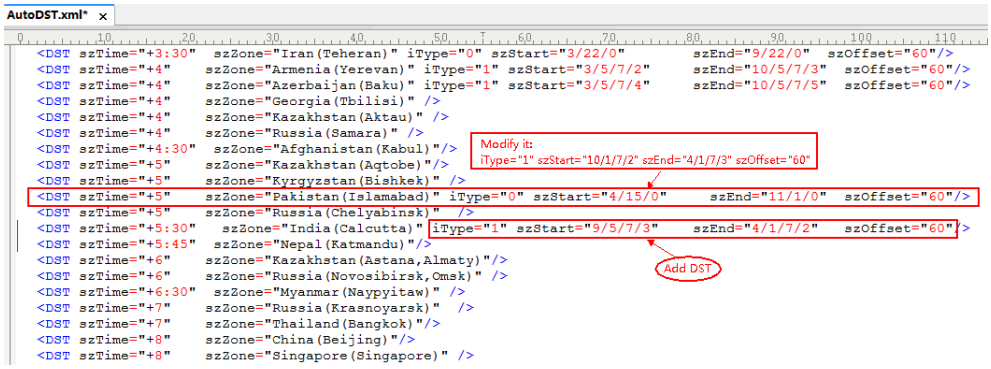
   For example:

   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	
Web UI	**Setting** > **Date&Time** > **Daylight Saving Time**	
Endpoint	**More** > **Settings** > **Device Settings** > **Time & Date** > **General** > **Daylight Saving**	
Parameter	**local_time.dst_time_type**	**<MAC>.cfg**
Description	It configures the Daylight Saving Time (DST) type. **Note**: It works only if “local_time.summer_time” is set to 1 (Enabled).	

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

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

Time and Date Manual Configuration

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

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

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

Time and Date Format Configuration

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

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

format as required.

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

Parameters	**local_time.time_format**	**<MAC>.cfg**
Description	It configures the time format.	
Permitted Values	**0**-Hour 12, the time will be displayed in 12-hour format with AM or PM specified. **1**-Hour 24, the time will be displayed in 24-hour format (for example, 2:00 PM displays as 14:00).	

Default	1	
Web UI	**Setting** > **Date&Time** > **Time Format**	
Endpoint	**More** > **Settings** > **Device Settings** > **Time&Date** > **Time & Date Format** > **Time Format**	
Parameter	**local_time.date_format**	**<MAC>.cfg**
Description	It configures the date format.	
Permitted Values	**0**-WWW MMM DD **1**-DD-MMM-YY **2**-YYYY-MM-DD **3**-DD/MM/YYYY **4**-MM/DD/YY **5**-DD MMM YYYY **6**-WWW DD MMM **7**-MM/DD/YYYY Use the following mapping: “WWW” represents the abbreviation of the week; “DD” represents a two-digit day; “MM” represents a two-digit month; “MMM” represents the first three letters of the month; “YYYY” represents a four-digit year, and “YY” represents a two-digit year.	
Default	0	
Web UI	**Setting** > **Date&Time** > **Date Format**	
Endpoint	**More** > **Settings** > **Device Settings** > **Time&Date** > **Time & Date Format** > **Date Format**	

Security Features

- User and Administrator Identification
- 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 endpoint.

When logging into the web user interface or accessing the advanced settings on the device, as an administrator, you need an administrator password to access various menu options. The default administrator name is “admin” and the administrator password is “0000”. The default user name is “user” and the password 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 the administrator, users can configure them only if they have administrator privileges.

When you sign in on the web interface more than 5 times with the default password, you will be forced to change your password.

The modified password must comply with the following rules:

- The password must be at least 8 digits in length.
- The password must contain at least one number.
- The password must contain any uppercase letter.
- The password must contain any lowercase letter.
- At most 3 consecutive repeating characters.
-

- User and Administrator Identification Configuration
- Enabling the User Role

User and Administrator Identification Configuration

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

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

Description	It configures the password of the user or administrator. The device uses “user” as the default user password and “0000” as the default administrator password. The valid value format is <username> : <new password>. **Example**: static.security.user_password = user:123 means setting the password of user to 123. static.security.user_password = admin:456 means setting the password of administrator to 456. **Note**: The devices support ASCII characters 32-126(0x20-0x7E) in passwords. You can set the password to be empty via the web user interface only. The user role is disabled by default.	
Permitted Values	String within 32 characters	
Default	user	
Web UI	**Security** > **Security**	
Endpoint	**More** > **Settings** > **Device Settings** > **Admin Password(default password: 0000)** **Note**: You cannot change the user password via the endpoint.	
Parameter	**security.complex_password.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables complex password rules.	
Permitted Values	**0**- Disabled **1**- Enabled	
Default	1	

Enabling the User Role

If you enable the user role, users can access basic configurations such as contacts. The default user name is “user” and the password is “user”.

Procedure

1. On your web user interface, go to **Security** > **Security**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
User Type	Select user.	Web user interface
User Mode	Enables the user role. **Default**: Disabled.	Web user interface

Related information

User and Administrator Identification Configuration

Transport Layer Security (TLS)

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

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

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

Supported Cipher Suites

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

Yealink devices support the following cipher suites:

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

Supported Trusted and Server Certificates

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

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

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

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

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

- Supported Trusted Certificates

Supported Trusted Certificates

Yealink Teams devices trust the following CAs by default:

- DigiCert High Assurance EV Root CA
- Deutsche Telekom Root CA-2
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure Global eBusiness CA-1
- GeoTrust Global CA
- GeoTrust Global CA2
- GeoTrust Primary Certification Authority
- GeoTrust Primary Certification Authority G2
- GeoTrust Universal CA
- GeoTrust Universal CA2
- Thawte Personal Freemail CA
- Thawte Premium Server CA
- Thawte Primary Root CA
- Thawte Primary Root CA - G2
- Thawte Primary Root CA - G3
- Thawte Server CA
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority

- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Universal Root Certification Authority
- ISRG Root X1 (Let's Encrypt Authority X1 and Let's Encrypt Authority X2 certificates are signed by the root certificate ISRG Root X1.)
- Baltimore CyberTrust Root
- DST Root CA X3
- Verizon Public SureServer CA G14-SHA2
- AddTrust External CA Root
- Go Daddy Class 2 Certification Authority
- Class 2 Primary CA
- Cybertrust Public SureServer SV CA
- DigiCert Assured ID Root G2
- DigiCert Assured ID Root G3
- DigiCert Assured ID Root CA
- DigiCert Global Root G2
- DigiCert Global Root G3
- DigiCert Global Root CA
- DigiCert Trusted Root G4
- Entrust Root Certification Authority
- Entrust Root Certification Authority - G2
- Entrust.net Certification Authority (2048)
- GeoTrust Primary Certification Authority - G3
- GlobalSign Root CA
- GlobalSign Root CA - R2
- Starfield Root Certificate Authority - G2
- TC TrustCenter Class 2 CA II
- TC TrustCenter Class 3 CA II
- TC TrustCenter Class 4 CA II
- TC TrustCenter Universal CA I
- TC TrustCenter Universal CA III
- Thawte Universal CA Root
- VeriSign Class 3 Secure Server CA - G2
- VeriSign Class 3 Secure Server CA – G3
- Thawte SSL CA
- StartCom Certification Authority
- StartCom Certification Authority G2
- Starfield Services Root Certificate Authority - G2
- RapidSSL CA
- Go Daddy Root Certificate Authority - G2
- Cybertrust Global Root
- COMODOSSLCA
- COMODO RSA Domain Validation Secure Server CA
- COMODO RSA Certification Authority
- AmazonRootCA4
- AmazonRootCA3

- AmazonRootCA2
- AmazonRootCA1
- Yealink Root CA
- Yealink Equipment Issuing CA
- SIP Core

Note: Yealink endeavors to maintain a built-in list of most commonly used CA Certificates. Due to memory constraints, we cannot ensure a complete set of certificates. If you are using a certificate from a commercial Certificate Authority but is not in the list above, you can send a request to your local distributor. At this point, you can upload your particular CA certificate into your device.

TLS Configuration

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

Parameter	**static.security.trust_certificates**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the device to only trust the server certificates listed in the Trusted Certificates list.	
Permitted Values	**0**-Disabled, the device will trust the server no matter whether the certificate sent by the server is valid or not. **1**-Enabled, the device will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, will the device trust the server.	
Default	1	
Web UI	**Security** > **Trusted Certs** > **Only Accept Trusted Certificates**	
Parameter	**static.security.ca_cert**[1]	**<y0000000000xx>.cfg**
Description	It configures the type of certificates in the Trusted Certificates list for the device to authenticate for TLS connection.	
Permitted Values	**0**-Default Certificates **1**-Custom Certificates **2**-All Certificates	
Default	2	
Web UI	**Security** > **Trusted Certs** > **CA Certificates**	
Parameter	**static.security.cn_validation**[1]	**<y0000000000xx>.cfg**
Description	It enables or disables the device to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Security** > **Trusted Certs** > **Common Name Validation**	
Parameter	**static.trusted_certificates.url**	**<y0000000000xx>.cfg**

Description	It configures the access URL of the custom trusted certificate used to authenticate the connecting server. **Example**: static.trusted_certificates.url = http://192.168.1.20/tc.crt **Note**: The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Security** > **Trusted Certs** > **Upload Trusted Certificate File**	
Parameter	**static.trusted_certificates.delete**	**<y0000000000xx>.cfg**
Description	It deletes all uploaded trusted certificates.	
Permitted Values	http://localhost/all	
Default	Blank	
Parameter	**static.security.dev_cert**[1]	**<y0000000000xx>.cfg**
Description	It configures the type of the device certificates for the device to send for TLS authentication.	
Permitted Values	**0**-Default Certificates **1**-Custom Certificates	
Default	0	
Web UI	**Security** > **Server Certs** > **Device Certificates**	
Parameter	**static.server_certificates.url**	**<y0000000000xx>.cfg**
Description	It configures the access URL of the certificate the device sends for authentication. **Note**: The certificate you want to upload must be in *.pem or *.cer format.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Security** > **Server Certs** > **Upload Server Certificate File**	
Parameter	**static.server_certificates.delete**	**<y0000000000xx>.cfg**
Description	It deletes all uploaded server certificates.	
Permitted Values	http://localhost/all	
Default	Blank	
Parameter	**static.phone_setting.reserve_certs_enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the device to reserve custom certificates after it is reset to factory defaults.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	

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

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

Encrypting Configuration Files

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

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

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

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

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

Configuration Files Encryption Tools

Yealink provides three encryption tools for configuration files:

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

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

These tools also encrypt the plaintext 16-character symmetric keys using a fixed key, which is the same as the one built in the device, and generate new files named as <xx_Security>.enc (xx is the name of the configuration file, for example, y000000000118_Security.enc for y000000000118.cfg file, account_Security.enc for account.cfg). These tools generate another new file named as Aeskey.txt to store the plaintext 16-character symmetric keys for each configuration file.

Configuration Files Encryption and Decryption

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

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

Encryption and Decryption Configuration

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

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

Description	It configures the plaintext AES key for encrypting/decrypting the Common CFG/ Custom CFG file. The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ _ { } ~. **Example**: static.auto_provision.aes_key_16.com = 0123456789abcdef **Note**: For decrypting, it works only if "static.auto_provision.aes_key_in_file" is set to 0 (Disabled). If the downloaded MAC-Oriented file is encrypted and the parameter "static.auto_provision.aes_key_16.mac" is left blank, the device will try to encrypt/ decrypt the MAC-Oriented file using the AES key configured by the parameter "static.auto_provision.aes_key_16.com".	
Permitted Values	16 characters	
Default	Blank	
Web UI	**Setting** > **Auto Provision** > **Common AES Key**	
Parameter	**static.auto_provision.aes_key_16.mac**	**<y0000000000xx>.cfg**
Description	It configures the plaintext AES key for encrypting/decrypting the MAC-Oriented files (<MAC>.cfg, <MAC>-local.cfg and <MAC>-contact.xml). The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ _ { } ~. **Example**: static.auto_provision.aes_key_16.mac = 0123456789abmins **Note**: For decrypting, it works only if "static.auto_provision.aes_key_in_file" is set to 0 (Disabled). If the downloaded MAC-Oriented file is encrypted and the parameter "static.auto_provision.aes_key_16.mac" is left blank, the device will try to encrypt/ decrypt the MAC-Oriented file using the AES key configured by the parameter "static.auto_provision.aes_key_16.com".	
Permitted Values	16 characters	
Default	Blank	
Web UI	**Setting** > **Auto Provision** > **MAC-Oriented AES Key**	

Example: Encrypting Configuration Files

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

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

Procedure

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

   The screenshot of the main page is shown below:



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.

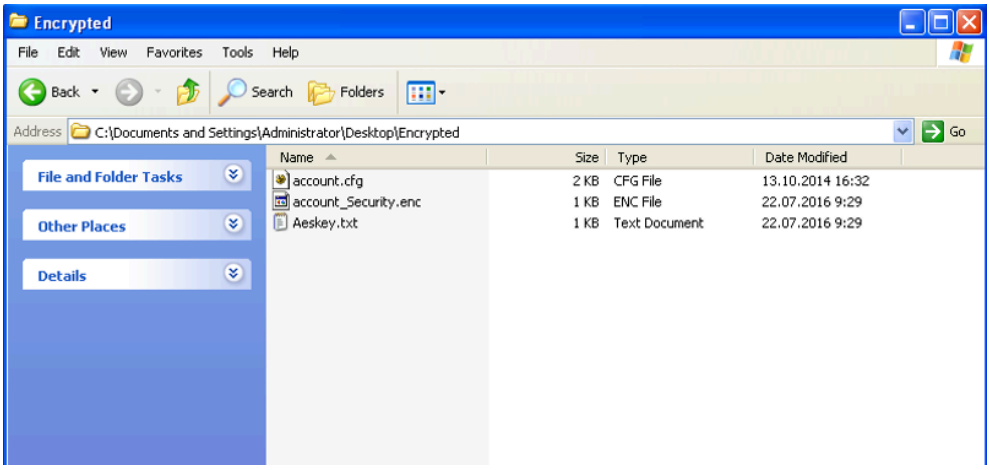
   If you mark the **Manual** radio box, you can enter an AES KEY in the **AES KEY** field or click **Re-Generate** to generate an AES KEY in the **AES KEY** field. The configuration file(s) will be encrypted using the AES KEY in the **AES KEY** field.

   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).



Configuring Camera Settings

You can customize the camera settings.

- Camera Mode Configuration
- Adjusting the White Balance
- Adjusting the Exposure
- Adjusting the Camera Display Image
- Adjusting Hangup Mode and Camera Pan Direction
- Reset Camera

Camera Mode Configuration

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

Parameter	**features.video_framing.mode**	**<y0000000000xx>.cfg**
Description	It configures the framing mode of the camera.	
Permitted Values	**0**-Manual **1**-Auto Framing, the camera automatically locates and frames participants in the room without moving the camera.	
Default	0	
Web UI	**Setting** > **Camera** > **Camera Mode** > **Framing mode**	
Endpoint	**More** > **Settings** > **Device Settings** > **Others** > **Auto Framing**	
Parameter	**features.video_framing.move_effect_enable**	**<y0000000000xx>.cfg**

Description	It configures the video switching mode. **Note**: It works only if "features.video_framing.mode" is set to 1 (Auto Framing).
Permitted Values	**0**-Direct Switching **1**-Smooth Switching
Default	0
Web UI	**Setting** > **Camera** > **Camera Mode** > **Video Switching Mode**

Adjusting the White Balance

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **White Balance**.
   - On your VC210, go to **More** > **Settings** > **Device Settings** > **Camera Settings** > **White Balance Settings**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
White Balance Mode	Configure the white balance mode of the camera. • **Auto**—Yealink recommends that you use this setting for most situations. It calculates the best white balance setting based on lighting conditions in the room. • **InDoor** • **OutDoor** • **OnePush** • **ATW**—automatically adjust the white balance according to the picture taken by the camera. • **Manual**—manually set a fixed value for color temperature. **Default**: ATW.	Web user interface Endpoint
Color Temperature	Configure the value of the color temperature. **Note**: the value is from 2800K to 6800K. The default value is the color temperature tested in your current environment. You can set this parameter only when the white balance mode is configured to **Manual**.	Web user interface Endpoint

Adjusting the Exposure

- Configuring Auto Exposure Mode
- Configuring Manual Exposure Mode
- Configuring the Mode of Shutter Priority

- Configuring the Mode of Brightness Priority

Configuring Auto Exposure Mode

The goal of auto-exposure is to achieve desired brightness level, or so-called target brightness level in different lighting conditions and scenes, so that the videos or images captured are neither too dark nor too bright.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - On your VC210, go to **More** > **Settings** > **Device Settings** > **Camera Settings** > **Exposure Settings**.
2. Select **Auto** from the **Exposure** drop-down menu.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Exposure Compensation	Configure the value of exposure compensation. The exposure compensation is used to compensate the camera effectively when the camera is shooting in the backlighting. If the environment light is dark, you can increase the compensation value. **Valid value**: from -6 to 6. The default value is 0.	Web user interface Endpoint
Flicker	Configure the value of camera flicker frequency. The supported types are as follows: • 50 Hz • 60 Hz The indoor lights powered by a 50Hz or 60Hz power source may produce a flicker. You can adjust the camera flicker frequency according to the power source that the light is powered by. **Default**: 50 Hz.	Web user interface Endpoint
Gain Limit	Specify the value. **Note**: the valid value is 1 to 15. The default value is 4.	Web user interface Endpoint
Wide Dynamic Range	Off or Specify the WDR. The value represents the compression degree of the dynamic range Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balance different lighting, so that you can identify the details. • **Off**- do not use WDR. • 1~5 **Default**: 2.	Web user interface Endpoint

Parameter	Description	Configuration Method
Photometry	Configure the value of metering. • Equal NxN • Central • Bottom • Top **Default**: Equal NxN.	Web user interface Endpoint

Configuring Manual Exposure Mode

Manual exposure mode allows you to achieve a combined exposure of the camera's aperture size and shutter speed.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - On your VC210, go to **More** > **Settings** > **Device Settings** > **Camera Settings** > **Exposure Settings**.
2. Select **Manual** from the **Exposure** drop-down menu.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Shutter	Configure the value of the shutter. **Value**: 1/60, 1/90, 1/100, 1/125, 1/180, 1/250, 1/350, 1/500, 1/725 1/1000, 1/1500, 1/2000, 1/3000, 1/4000, 1/6000, 1/10000 **Default**: 1/100.	Web user interface Endpoint
Gain Limit	Specify the value. **Note**: the valid value is 1 to 15. The default value is 2.	Web user interface Endpoint
Wide Dynamic Range	Off or Specify the WDR. The value represents the compression degree of the dynamic range Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balances different lighting, so that you can identify the details. • **Off**- do not use WDR. • 1~5 **Default**: 2.	Web user interface Endpoint

Configuring the Mode of Shutter Priority

Shutter priority allows you to choose a specific shutter speed while the camera adjusts the aperture to ensure adequate exposure.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - On your VC210, go to **More** > **Settings** > **Device Settings** > **Camera Settings** > **Exposure Settings**.
2. Select **Shutter Priority** from the **Exposure** drop-down menu.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Shutter	Configure the value of the shutter. **Valid Value**: 1/60, 1/90, 1/100, 1/125, 1/180, 1/250, 1/350, 1/500, 1/725, 1/1000, 1/1500, 1/2000, 1/3000, 1/4000, 1/6000, 1/10000 **Default**: 1/100.	Web user interface Endpoint
Exposure Compensation	Configure the value of exposure compensation. The exposure compensation is used to compensate the camera effectively when the camera is shooting in the backlighting. If the environment light is dark, you can increase the compensation value. **Valid value**: from -6 to 6. The default value is 0.	Web user interface Endpoint
Gain Limit	Specify the value. **Note**: the valid value is 1 to 15. The default value is 4.	Web user interface Endpoint
Wide Dynamic Range	Off or Specify the WDR. The value represents the compression degree of the dynamic range Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balance different lighting, so that you can identify the details. • **Off**- do not use WDR. • 1~5 **Default**: 2.	Web user interface Endpoint
Photometry	Configure the value of metering. • Equal NxN • Central • Bottom • Top **Default**: Equal NxN.	Web user interface Endpoint

Configuring the Mode of Brightness Priority

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - On your VC210, go to **More** > **Settings** > **Device Settings** > **Camera Settings** > **Exposure Settings**.
2. Select **Brightness Priority** from the **Exposure** drop-down menu.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Brightness	Configure the value of brightness. **Note**: the valid value is from 0 to 14 and the default value is 6.	Web user interface Endpoint
Flicker	Configure the value of camera flicker frequency. The supported types are as follows: • 50 Hz • 60 Hz The indoor lights powered by a 50Hz or 60Hz power source may produce a flicker. You can adjust the camera flicker frequency according to the power source that the light is powered by. **Default**: 50 Hz.	Web user interface Endpoint
Wide Dynamic Range	Off or Specify the WDR. The value represents the compression degree of the dynamic range Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balances different lighting, so that you can identify the details. • **Off**- do not use WDR. • 1~5 **Default**: 2.	Web user interface Endpoint
Photometry	Configure the value of metering. • Equal NxN • Central • Bottom • Top **Default**: Equal NxN.	Web user interface Endpoint

Adjusting the Camera Display Image

You can adjust display mode of the camera or customize the image display.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Graphics**.
   - On your VC210, go to **More** > **Settings** > **Device Settings** > **Camera Settings** > **Graphics**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Display Mode	Configure the display mode of the camera. • High Definition • Standard • Mild • Custom Definition **Default**: Standard	Web user interface Endpoint
Saturation	Configure the image saturation of the camera. The saturation means the maximum intensity of color in the image. **Note**: the value is from 0 to 100. The default value is 50.	Web user interface Endpoint
Sharpness	Configure the image sharpness of the camera. The sharpness is an indicator that reflects the definition of the image plane and the sharpness of image edge. Increasing the sharpness will improve the definition of the image. However, if the sharpness is set too high, the image will look distorted and glaring. **Note**: the value is from 0 to 100. The default value is 15.	Web user interface Endpoint
Brightness	Configure the image brightness of the camera. **Note**: the value is from 0 to 100. The default value is 50.	Web user interface Endpoint
Contrast	Configure the image contrast of the camera. **Valid value**: 0 - 100. The default value is 49. **Note**: It is only applicable to MeetingBar A20.	Web user interface Endpoint
Noise Reduction (2D)	Specify the noise reduction (2D) mode. The available modes are described below: • Off • Low • Middle • High **Default**: Middle.	Web user interface Endpoint

Adjusting Hangup Mode and Camera Pan Direction

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Other Settings**.
   - On your VC210, go to **More** > **Settings** > **Device Settings** > **Camera Settings** > **Others**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Hangup Mode	Enable or disable the camera to flip the image view when camera is hung at up-side-down position. If this mode is enabled, the picture took by the camera is upside down. This mode is applicable when you install the camera on the meeting room ceiling. **Default**: Off.	Web user interface Endpoint
Camera Pan Direction	Configure the pan direction of the camera. • Normal • Reversed If the camera reversed mode is enabled, the camera pan direction will be reversed when pressing the left and right navigation keys on the remote control. In this case, you can set the camera pan direction to **Reversed**. **Default**: Normal.	Web user interface Endpoint

Reset Camera

You can reset the camera to factory defaults.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Other Settings**.
   - On your VC210, go to **More** > **Settings** > **Device Settings** > **Camera Settings**.
2. Select **Reset Camera**.
   The system prompts whether or not you are sure to reset.
3. Confirm the action.

Configuring Audio Settings

You can configure the audio settings.

- EQ Self Adaption
- Noise Suppression

EQ Self Adaption

The EQ self adaption allows the device to optimize the acoustic effect. The EQ self adaption is enabled by default. System supports manual EQ self adaption adjustment.

- EQ Self Adaption Configuration

EQ Self Adaption Configuration

The following table lists the parameters you can use to configure the EQ self adaption.

Parameter	audio.eq_self-adaption.enable	<y0000000000xx>.cfg
Description	It enables or disables the EQ self adaption feature on the device.	
Permitted Values	**0**-Off **1**-On	
Default	1	
Web UI	**Setting** > **Audio** > **EQ Self Adaption** > **EQ Self Adaption**	

Noise Suppression

The noises in the room may be picked-up, including paper rustling, coffee mugs, coughing, typing and silverware striking plates. These noises, when transmitted to remote participants, can be very distracting. You can enable the Transient Noise Suppressor (TNS) to suppress these noises. You can also enable the Noise Barrier feature to block these noises when there is no speech in a call.

- Noise Suppression Configuration

Noise Suppression Configuration

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

Parameter	voice.tns.enable	<y0000000000xx>.cfg
Description	It enables or disables the Transient Noise Suppressor (TNS).	
Permitted Values	**0**-Off **1**-On, it can reduce the noise volume temporarily and block the noise in the voice.	
Default	1	
Web UI	**Setting** > **Audio** > **Noise Suppression** > **Temporal Noise Shaping(TNS)**	
Parameter	voice.ans_nb.enable	<y0000000000xx>.cfg
Description	It enables or disabled the noise barrier feature.	
Permitted Values	**0**-Off **1**-On, it can block the noise when there is no speech in a call.	
Default	0	

Web UI	**Setting** > **Audio** > **Noise Suppression** > **Noise Barrier**

Troubleshooting Methods

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

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

Exporting All the Diagnostic Files

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

Procedure

1. From the web user interface, go to **Setting** > **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 DiagnoseInfo.tar is successfully exported to your local system.

Note: After exporting the diagnostic files, you can create a ticket and describe your problem at ticket.yealink.com. After that Yealink support team will help you locate the root cause.

Log Files

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

- Local Log
- Syslog Log

Local Log

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

- Local Log Configuration
- Exporting the Log Files to a Local PC
- Viewing the Log Files

Local Log Configuration

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

Parameter	static.local_log.enable	<y0000000000xx>.cfg
Description	It enables or disables the device to record log locally. **Note**: We recommend you not to disable this feature.	
Permitted Values	**0**-Disabled, the device will stop recording log to the log files locally. The log files recorded before are still kept on the device. **1**-Enabled, the device will continue to record log to the log files locally. You can upload the local log files to the provisioning server or a specific server or export them to the local system.	
Default	1	
Web UI	**Setting** > **Configuration** > **Enable Local Log**	
Parameter	**static.local_log.level**	**<y0000000000xx>.cfg**
Description	It configures the lowest level of local log information to be rendered to the sys.log file. When you choose a log level, it includes all events of an equal or higher severity level and excludes events of a lower severity level. The logging level you choose determines the lowest severity of events to log.	
Permitted Values	**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	**Setting** > **Configuration** > **Local Log Level**	
Parameter	**static.local_log.max_file_size**	**<y0000000000xx>.cfg**
Description	It configures the maximum size (in KB) of the log files that can be stored on the device. When this size is about to be exceeded, (1) If the local log files are configured to be uploaded to the server by the parameter “static.auto_provision.local_log.backup.enable”, the device will clear all the local log files on the device once successfully backing up. (2) If “static.auto_provision.local_log.backup.enable” is set to 0 (Disabled), the device will erase half of the logs from the oldest log information on the device.	

Permitted Values	Integer from 2048 to 20480	
Default	20480	
Web UI	**Setting** > **Configuration** > **Max Log File Size**	
Parameter	**static.auto_provision.local_log.backup.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the device to upload the local log files to the provisioning server or a specific server. **Note**: The upload path is configured by the parameter "static.auto_provision.local_log.backup.path".	
Permitted Values	**0**-Disabled **1**-Enabled, the device will upload the local log files to the provisioning server or the specific server to back up these files when one of the following happens: - Auto provisioning is triggered; - The size of the local log files reaches the maximum configured by the parameter "static.local_log.max_file_size"; - It's time to upload local log files according to the upload period configured by the parameter "static.auto_provision.local_log.backup.upload_period".	
Default	0	
Parameter	**static.auto_provision.local_log.backup.upload_period**	**<y0000000000xx>.cfg**
Description	It configures the period (in seconds) of the local log files uploads to the provisioning server or a specific server. **Note**: It works only if "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled).	
Permitted Values	Integer from 30 to 86400	
Default	30	
Parameter	**static.auto_provision.local_log.backup.path**	**<y0000000000xx>.cfg**
Description	It configures the upload path of the local log files. If you leave it blank, the device will upload the local log files to the provisioning server. If you configure a relative URL (for example, /upload), the device will upload the local log files by extracting the root directory from the access URL of the provisioning server. If you configure an absolute URL with protocol (for example, tftp), the device will upload the local log files using the desired protocol. If no protocol, the device will use the same protocol with auto provisioning for uploading files. **Example**: static.auto_provision.local_log.backup.path = tftp://10.3.6.133/upload/ **Note**: It works only if "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled).	
Permitted Values	URL within 1024 characters	

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

Exporting the Log Files to a Local PC

Procedure

1. From the web user interface, go to **Setting** > **Configuration** > **Local Log**.
2. Turn on **Enable Local Log**
3. Select the desired value from the **Local Log Level** drop-down menu.
   The default local log level is “6”.
4. Enter the limit size of the log files in the **Max Log File Size** field.
5. Click **Confirm** to accept the change.
6. Reproduce the issue.
7. Click **Export** to open the file download window and save the file to your local system.

Viewing the Log Files

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

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

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

```
<46>Thu Jan  1 08:00:09 syslogd started: BusyBox v1.10.3
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > cfg log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > ANY =3
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Version  :1.2.1.7 for release
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Built-at :May 10 2018,21:55:14
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<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 following figure shows a portion of a sys log file:

```
<46>Thu Jan  1 08:00:09 syslogd started: BusyBox v1.10.3
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > cfg log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > ANY =3
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Version  :1.2.1.7 for release
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Built-at :May 10 2018,21:55:14
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<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
```

Syslog Log

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

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

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

Syslog Logging Configuration

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

Parameter	**static.syslog.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the device to upload log messages to the syslog server in real time.	
Permitted Values	**0**-Disabled **1**-Enabled	
Default	0	
Web UI	**Setting** > **Configuration** > **Syslog** > **Enable Syslog**	
Parameter	**static.syslog.server**	**<y0000000000xx>.cfg**
Description	It configures the IP address or domain name of the syslog server when exporting log to the syslog server.	
Permitted Values	IP address or domain name	
Default	Blank	
Web UI	**Setting** > **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	**Setting** > **Configuration** > **Syslog** > **Syslog Server** > **Port**	
Parameter	**static.syslog.transport_type**	**<y0000000000xx>.cfg**
Description	It configures the transport protocol that the device uses when uploading log messages to the syslog server.	
Permitted Values	**0**-UDP **1**-TCP **2**-TLS	
Default	0	
Web UI	**Setting** > **Configuration** > **Syslog** > **Syslog Transport Type**	

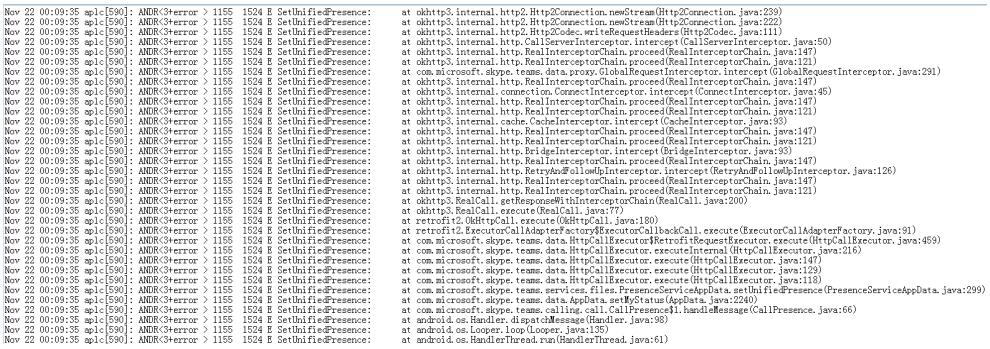
Parameter	**static.syslog.level**	**<y0000000000xx>.cfg**
Description	It configures the lowest level of syslog information that displays in the syslog.	
Permitted Values	**0**-Emergency: system is unusable **1**-Alert: action must be taken immediately **2**-Critical: critical conditions **3**-Critical: error conditions **4**-Warning: warning conditions **5**-Warning: normal but significant condition **6**-Informational: informational messages	
Default	6	
Web UI	**Setting** > **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	**Setting** > **Configuration** > **Syslog** > **Syslog Facility**
Parameter	**static.syslog.prepend_mac_address.enable** **<y0000000000xx>.cfg**
Description	It enables or disables the device to prepend the MAC address to the log messages exported to the syslog server.
Permitted Values	**0**-Disabled **1**-Enabled
Default	0
Web UI	**Setting** > **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 purposes.

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

Capturing the Packets via Web User Interface

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

Yealink devices support the following two modes for capturing the packets:

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

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

Capturing the Packets in Normal Way

Procedure

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

Capturing the Packets in Enhanced Way

Procedure

1. From the web user interface, go to **Setting** > **Configuration**.
2. Click **Start** in the **Pcap Feature** field to start capturing signal traffic.
3. Reproduce the issue to get stack traces.
4. Click **Stop** in the **Pcap Feature** field to stop capturing.

Ethernet Software Capturing Configuration

You can choose to capture the packets using the following way:

- **Receiving data packets from the HUB**: Connect the Internet port of the device and the PC to the same HUB, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic.

Analyzing Configuration Files

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

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

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

Exporting BIN Files from the Device

Procedure

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

Importing BIN Files from the Device

Procedure

1. From the web user interface, go to **Setting** > **Configuration** > **Configuration**.
2. In the **Import Configuration** block, click the white box to select a BIN configuration file from your local system.
3. Click **Import** to import the configuration file.

- BIN Files Import URL Configuration

BIN Files Import URL Configuration

The following table lists the parameter you can use to configure the BIN files import URL.

Parameter	**static.configuration.url**[1]	**<y0000000000xx>.cfg**
Description	It configures the access URL for the custom configuration files. **Note**: The file format of the custom configuration file must be *.bin.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Setting** > **Configuration** > **Import Configuration**	

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

Device Status

Available information on device status includes:

-
- Version information (Firmware Version, Hardware Version, Partner APP Version, Company Portal Version and Teams Version).
- Network status (IPv4 status or IPv6 status, and IP mode).
- Device Certificate
- Device status (MAC address and device type)

- Viewing the Device Status

Viewing the Device Status

You can view device status via the endpoint by navigating to **More** > **Settings** > **Device Settings** > **Other Settings** > **About**. You can also view the device status via the web user interface.

Procedure

1. Open a web browser on your computer.
2. Enter the IP address in the browser's address bar and then press the **Enter** key.
   For example, "http://192.168.0.10" for IPv4 or "http://[2005:1:1:1:215:65ff:fe64:6e0a]" for IPv6.
3. Enter the user name (admin) and password (0000) in the login page.
4. Click **Login** to login.
   The device status is displayed on the first page of the web user interface.

Resetting Device and Configuration

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

- Resetting the Device to Default Factory Settings
- Resetting the Device to Custom Factory Settings
- Deleting the Custom Factory Settings Files

Resetting the Device to Default Factory Settings

Procedure

1. From the web user interface, click **Setting** > **Upgrade**.
2. Click **Reset to Factory** in the **Reset to Factory Setting** field.
   The web user interface prompts the message "Do you want to reset to factory?".
3. Click **OK** to confirm the resetting.
   The device will be reset to the factory successfully after startup.

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

Resetting the Device to Custom Factory Settings

After you enable the custom factory feature, you can import the custom factory configuration file, and then reset the device to custom factory settings.

Procedure

1. From the web user interface, click **Setting** > **Configuration** > **Factory Configuration**.
2. In the **Import Factory Configuration** field, click the white box to select the custom factory configuration file from your local system.
3. Click **Import**.
   After the custom factory configuration file is imported successfully, you can reset the device to custom factory settings.

- Custom Factory Configuration

Custom Factory Configuration

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

Parameter	**static.features.custom_factory_config.enable**	**<y0000000000xx>.cfg**
Description	It enables or disables the Custom Factory Configuration feature.	
Permitted Values	**0**-Disabled **1**-Enabled, **Import Factory Configuration** item will be displayed on the device's web user interface at the path Setting > **Configuration**. You can import a custom factory configuration file or delete the user-defined factory configuration via web user interface.	
Default	0	
Parameter	**static.custom_factory_configuration.url**	**<y0000000000xx>.cfg**
Description	It configures the access URL of the custom factory configuration files. **Note**: It works only if “static.features.custom_factory_config.enable” is set to 1 (Enabled) and the file format of the custom factory configuration file must be *.bin.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	**Setting** > **Configuration** > **Import Factory Configuration**	

Deleting the Custom Factory Settings Files

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

Procedure

1. From the web user interface, click **Setting** > **Configuration** > **Factory Configuration**.
2. Click **Delete** from the **Delete Factory Configuration** field.
   The web user interface prompts the message “Are you sure delete user-defined factory configuration?”.
3. Click **OK** to delete the custom factory configuration files.
   The imported custom factory file will be deleted. The device will be reset to default factory settings after resetting.

Device Reboot

You can reboot the device locally.

- Rebooting the Device via Endpoint
- Rebooting the Device via Web User Interface

Rebooting the Device via Endpoint

Procedure

1. Go to **More** > **Settings** > **Device Settings** > **Other Settings** > **Debug**.
2. Select **Reboot phone**.
   It prompts if you are sure to reboot the device.
3. Select **OK**.

Rebooting the Device via Web User Interface

Procedure

1. Click **Setting** > **Upgrade**.
2. Click **Reboot** to reboot the device.
   The web user interface prompts the message “Reboot the system?"
3. Click **OK** to confirm the rebooting.
   The device begins at rebooting. Any reboot of the device may take a few minutes.

Capturing the Current Screen of the Device

You can capture the screen display of the device via the web user interface.

Procedure

1. On your web user interface, go to **Home** > **Screenshot**.
2. Save the screenshot to your local system.

Troubleshooting Solutions

This section describes the solutions to common issues that may occur while using the Teams device. Upon encountering a case not listed in this section, contact your Yealink reseller for further support.

- IP Address Issues
- Time and Date Issues
- Display Issues
- Firmware and Upgrading Issues
- System Log Issues
- Password Issues

IP Address Issues

- The device does not get an IP address
- IP Conflict
- Specific format in configuring IPv6 on Yealink devices

The device does not get an IP address

Do one of the following:

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

IP Conflict

Do one of the following:

- Reset another available IP address for the device.
- Check network configuration via the endpoint at the path **More** > **Settings** > **Device Settings** > **Network(default password: 0000)** > **IPv4 Type(or IPv6 Type)**. If the Static IP is selected, select DHCP instead.

Specific format in configuring IPv6 on Yealink devices

Scenario 1:

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

Scenario 2:

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

When provisioning your device to obtain an IPv6 address, the provisioning server should support IPv6 and the format of the access URL of the provisioning server can be "*tftp://[IPv6 address or domain name]*". For example, if the provisioning server address is "2001:250:1801::1", the access URL of the provisioning server can be "tftp://[2001:250:1801::1]/".

Time and Date Issues

- Display time and date incorrectly

Display time and date incorrectly

Check if the device is configured to obtain the time and date from the NTP server automatically. If your device is unable to access the NTP server, configure the time and date manually.

Display Issues

- The device LCD screen blank
- The device displays “Offline”

The device LCD screen blank

Do one of the following:

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

The device displays “Offline”

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

Firmware and Upgrading Issues

- Fail to upgrade the device firmware
- The device does not update the configurations

Fail to upgrade the device firmware

Do one of the following:

- Ensure that the target firmware is not the same as the current firmware.
- Ensure that the target firmware is applicable to the device model.
- Ensure that the current or the target firmware is not protected.
- Ensure that the power is on and the network is available during upgrading.
- Ensure that the web browser is not closed or refreshed when upgrading firmware via the web user interface.

The device does not update the configurations

Do one of the following:

- Ensure that the configuration is set correctly.
- Reboot the device. Some configurations require a reboot to take effect.
- Ensure that the configuration is applicable to the device model.
- The configuration may depend on the support from a server.

System Log Issues

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

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

Do one of the following:

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

Fail to export the system log from a syslog server

Do one of the following:

- Ensure that the syslog server can save the syslog files exported from the device.
- Ensure that you have configured the syslog server address correctly via the web user interface on your device.
- Reboot the device. The configurations require a reboot to take effect.

Password Issues

- Restore the administrator password

Restore the administrator password

Factory reset can restore the default password. All custom settings will be overwritten after reset.