

Administrator Guide

Teams Settings

Register Account

Introduction

If you do not have a Teams account, you need to register a Teams account in the Microsoft Management Center and configure related permissions for the account.

How to

To register a Teams account, please refer to [Yealink Teams Device Setup Guide with Microsoft Configuration Platforms](#).

FAQ

[Having trouble registering a device on Intune?](#)

[Which Teams licenses are required for A10/A20/A30 Teams?](#)

Microsoft Teams Admin Center

Introduction

After signing in to the Teams account on the MeetingBar AX0, the device will connect to the Microsoft Teams management center. You can manage the device in the management center, for example, remotely update or download logs.

How to Use

For more information, please refer to [Yealink Teams Device Setup Guide with Microsoft Configuration Platforms](#) .

Calling Settings

Introduction

Go to Teams administrator settings to set up calls.

How to Use

Go to **More > Settings > Device Settings > Teams Admin Settings** (default password: 0000) > **Call**.

For more information, please refer to [Manage your call settings in Microsoft Teams](#).

General Settings

Introduction

Change the wallpaper, enable HDMI content sharing, and other settings in the general settings.

How to Use

Wallpaper

Go to **More > Settings > Device Settings > Teams Admin Settings** (default password: 0000) > **General > Wallpaper** to change the wallpaper.

HDMI Content Sharing

On the MeetingBoard homepage, go to **More > Settings > Device Settings > Teams Admin Settings** (default password: 0000) > **General**.

After enabling **HDMI Content Sharing**, you can use a hardware device to share content.

After enabling **Include Audio**, audio can be shared during content sharing.

After enabling **Automatically share to conference room display**, the hardware device will automatically share the content immediately.

Meeting Settings

Introduction

Make some settings for the meeting.

How to Use

Go to **More > Settings > Device Settings > Teams Admin Settings** (default password: 0000) > **General > Meetings**.

You can do the following:

- **Display meeting name:** Display the meeting name in the list of scheduled meetings.
- **Allow Bluetooth Beacon:** Allow the use of the Proximity Join feature.
- **Allow conference room to enable whiteboard:** Enable local whiteboard.
- **Display chat bubbles:** Display chat bubbles in the meeting.
- **Display meeting chat:** Display chat content in the meeting.
- **Extend meeting room reservation:** Extend the reservation time of the meeting room.
- **Allow joining third-party meetings:** The meeting room can join third-party meetings.

Login & Update

Log In & Out Account

Introduction

If you boot the MeetingBar AX0 for the first time, restore it to factory settings or sign out of your account, you need to sign in to your Microsoft Teams account to use the relevant Teams features.

The MeetingBar A10/A20/A30 is hereinafter referred to as MeetingBar AX0.

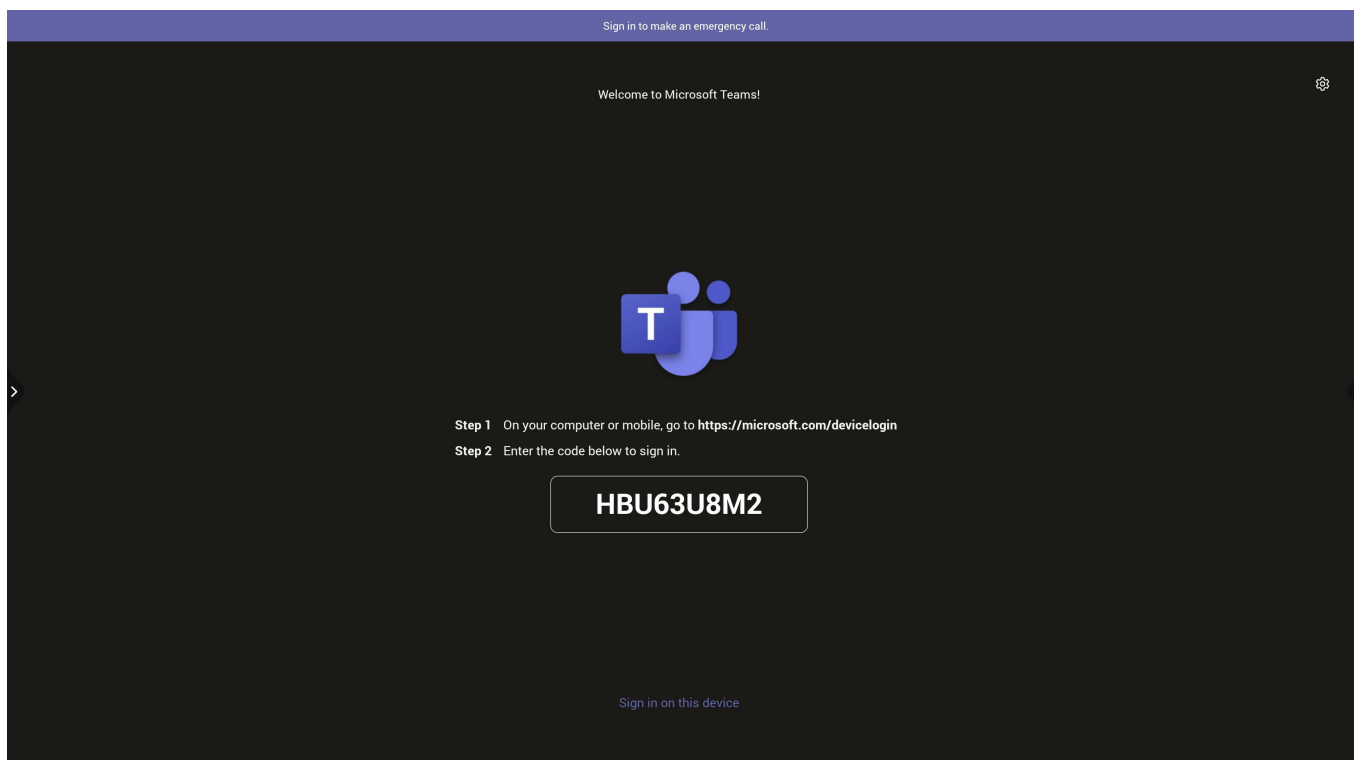
Log In to Account

NOTE

- Please contact the corresponding service provider to obtain an account.
- Sign in to the same account on CTP18 and MeetingBar AX0.

Login to Web User Interface

1. Visit this website <https://microsoft.com/devicelogin> on your PC or mobile phone.



2. Enter the pairing code displayed on the MeetingBoard AX0 or the CTP18 to the web interface and click **Next**.



Enter code

Enter the code displayed on your app or device.

Code

Next

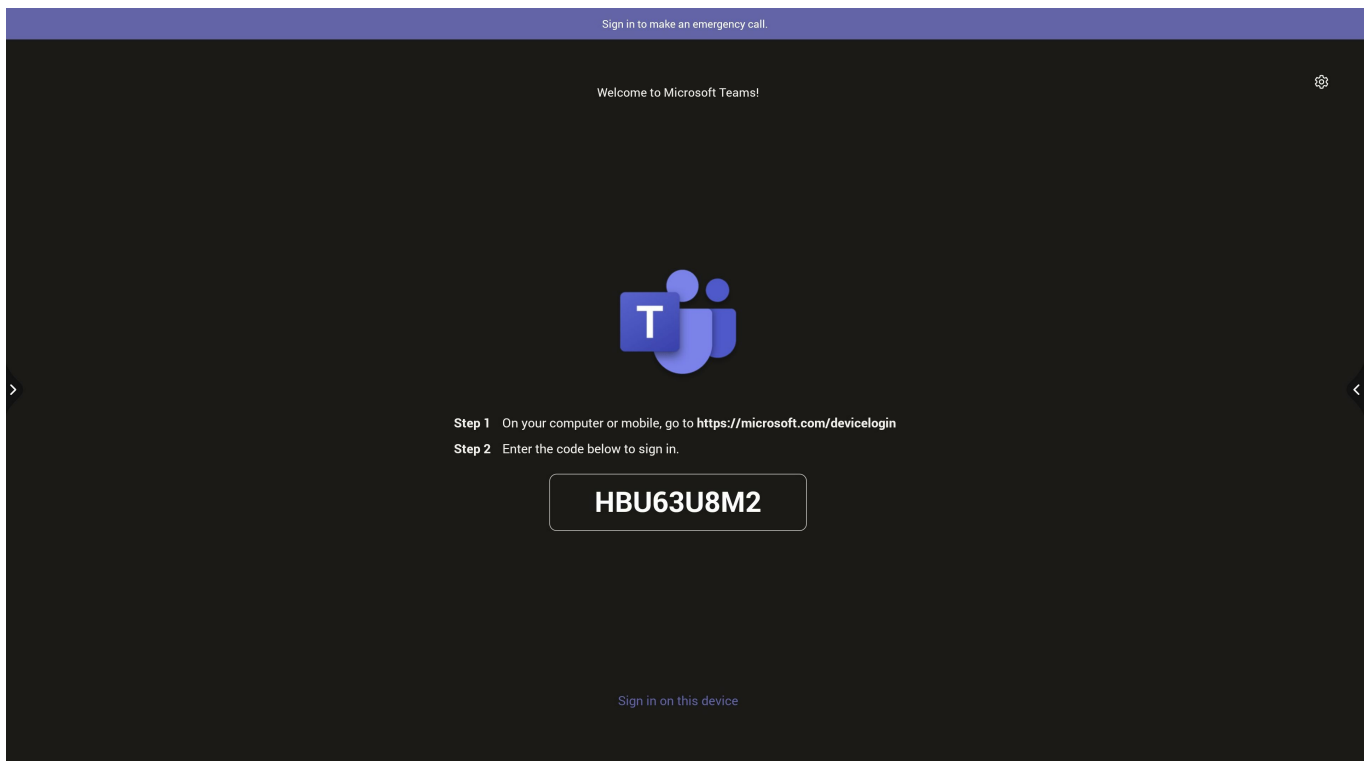
3. Enter the username and password to sign in.

Login to MeetingBar AX0

NOTE

If the TV display does not support touch, please use the remote control to operate the MeetingBar AX0.

1. Tap **Sign in on this device** on the MeetingBar screen.



2. Enter the account and password and tap **Sign in**.

Log Out of Account

You can sign out of your CTP18 and MeetingBar AX0 accounts respectively.

1. On the CTP18 or with the remote control, select **More > Settings > Sign out**.
2. Click **OK** to sign out of your account.

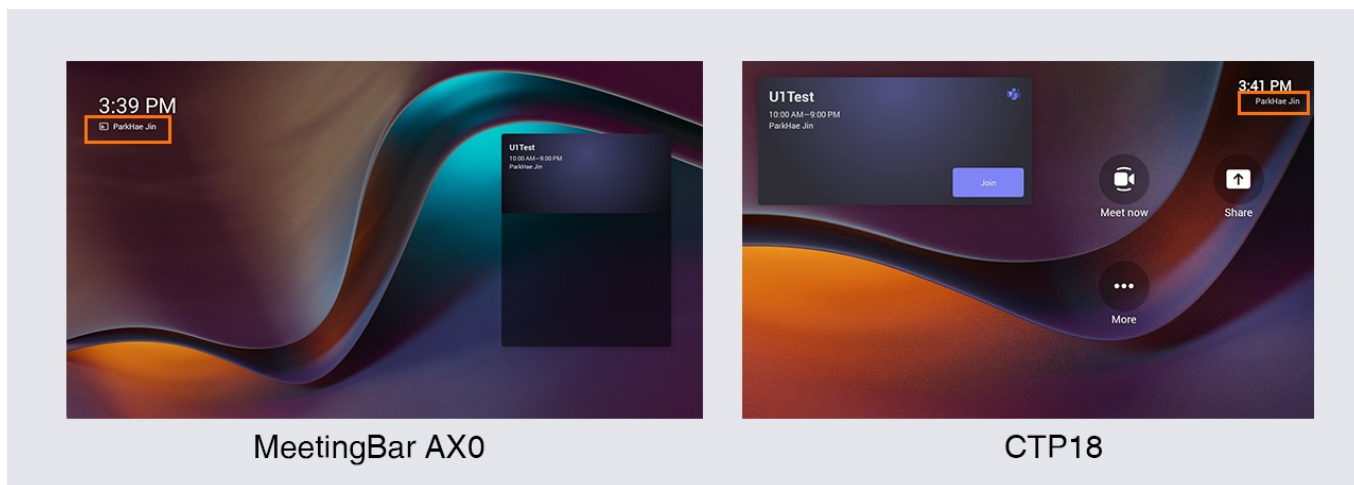
FAQ

Why can't I sign in to my account in MeetingBar A20&A30 Teams?

How to check whether CTP18 and MeetingBar AX0 have a login account?

- If the CTP18 and MeetingBar AX0 do not have a login account, their interface will display a login interface.

- If the CTP18 and MeetingBar AX0 have already signed in, the account will be displayed in the upper-right corner of CTP18 and the upper-left corner of MeetingBar AX0.



Firmware Update (MeetingBar)

Introduction

Three methods of firmware update:

- Check for updates through the MeetingBar AX0 interface.
- Update the MeetingBar AX0 through the **Automatic Update** of the MeetingBar AX0.
- Update the MeetingBar AX0 through the web user interface of MeetingBar AX0.
- Update the MeetingBar AX0 through a USB flash drive.
- Update the MeetingBar AX0 through the [Yealink Device Manage Platform](#).
- Update the MeetingBar AX0 in batches through the provisioning server.
- Update the MeetingBar AX0 in batches through the Microsoft Teams admin center.

NOTE

We recommend using the latest firmware. The new firmware version is compatible with the features of the old version. However, after you update your device to the latest version, you can not downgrade the device's firmware version.

Firmware Version

NOTE

Please update the CTP18 and MeetingBar AX0 respectively, and ensure their firmware versions match. If the firmware versions do not match, it may cause the functions to work abnormally or upgrade failure. Please refer to [Release Note](#) for the firmware version information.

The following table lists the firmware naming types for MeetingBar A10/A20/A30 (hereinafter referred to as MeetingBar AX0) and CTP18, with X denoting the actual firmware version.


Device Name	Firmware Type
MeetingBar A10	278.x.x.x.rom
MeetingBar A20/A30	133.x.x.x.rom
CTP18	137.x.x.x.rom

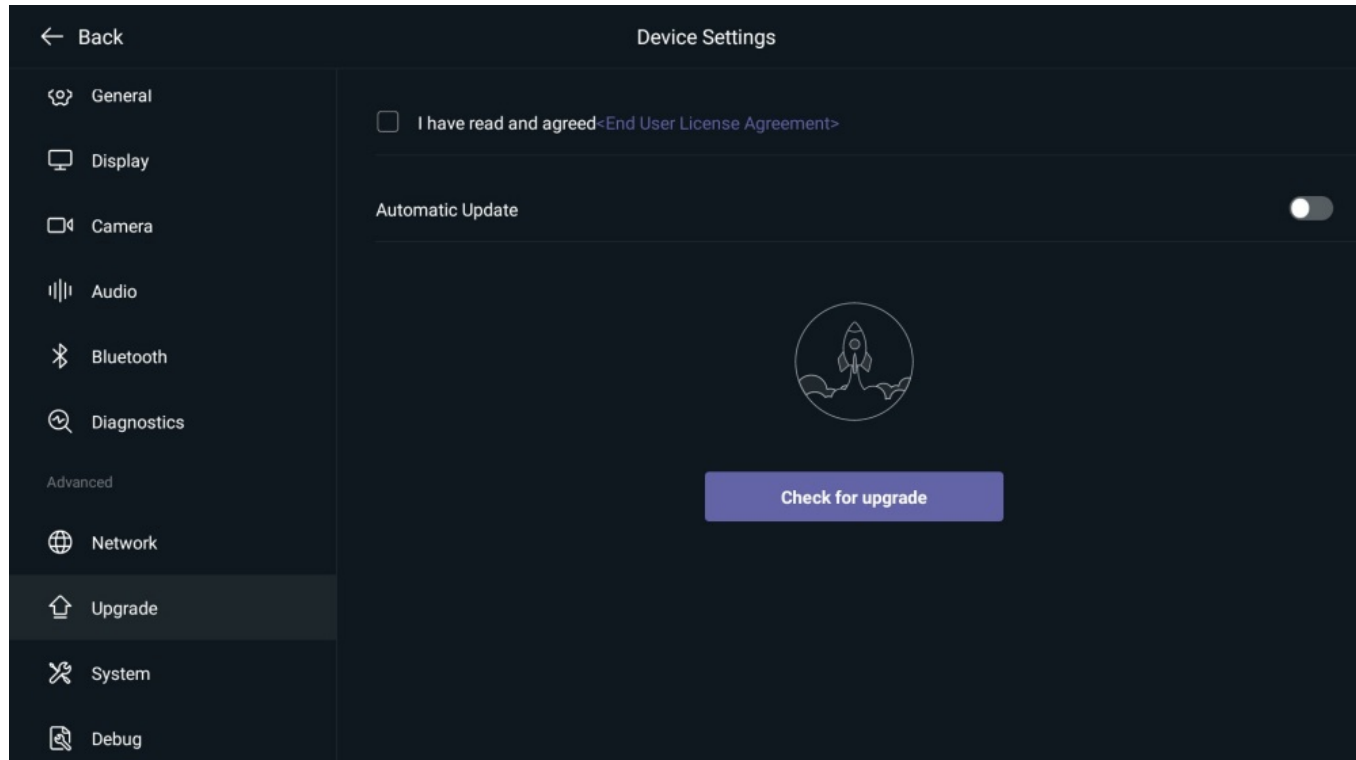
Firmware Update

Before updating the firmware:

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

Update via Check for Update

1. Go to the sidebar  **> Settings > Device Settings > Update** (default password: 0000) to check whether there is a newer version.
2. When MeetingBar AX0 detects that there is a new version, the MeetingBar AX0 will download and install the upgrade package.

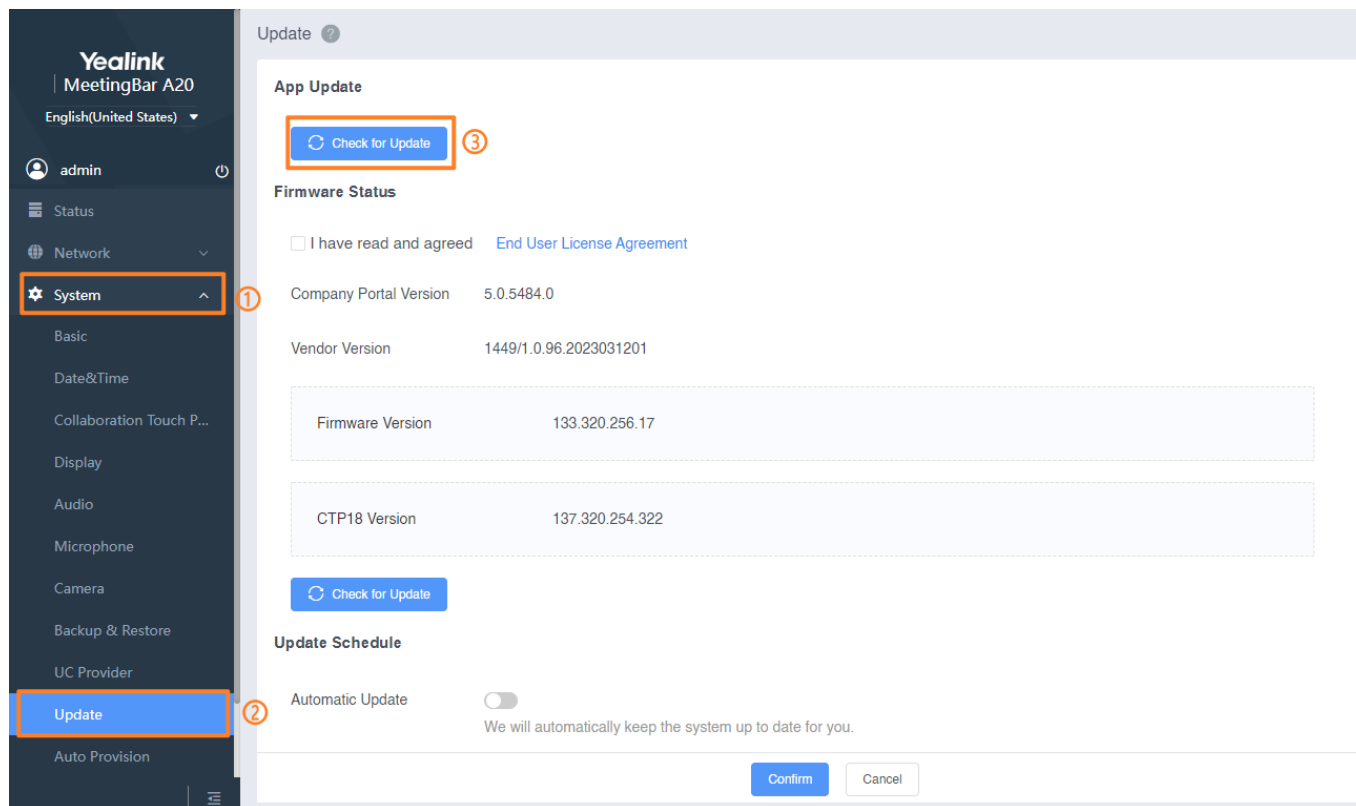


Update via Web User Interface

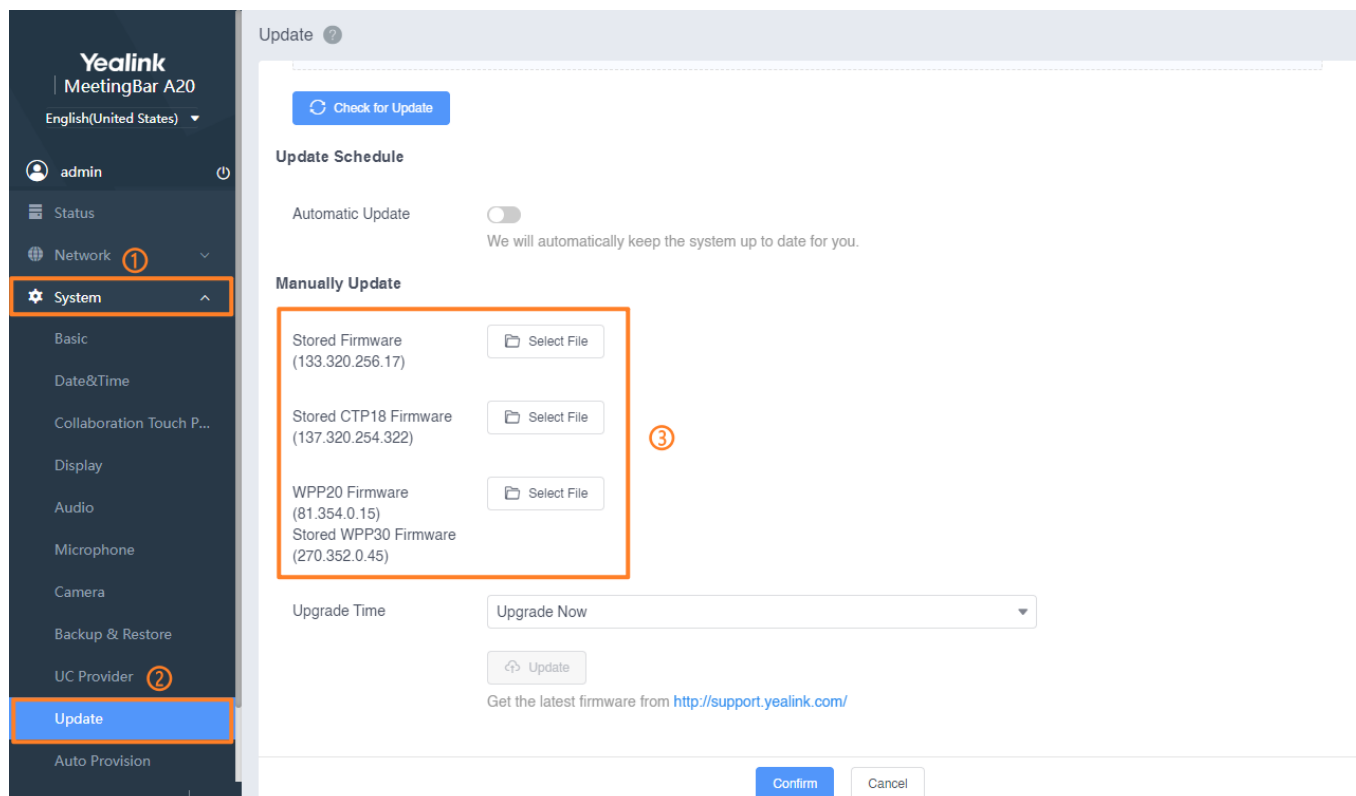
1. Go to **System > Update** in the [web user interface](#).

2. Do one of the following:

- Click **Check for Update**. If it is not the latest firmware version, the update icon will appear, and you can directly click **Check for Update** to update.



- Select the rom file in **Manually Update** and click **Update**.

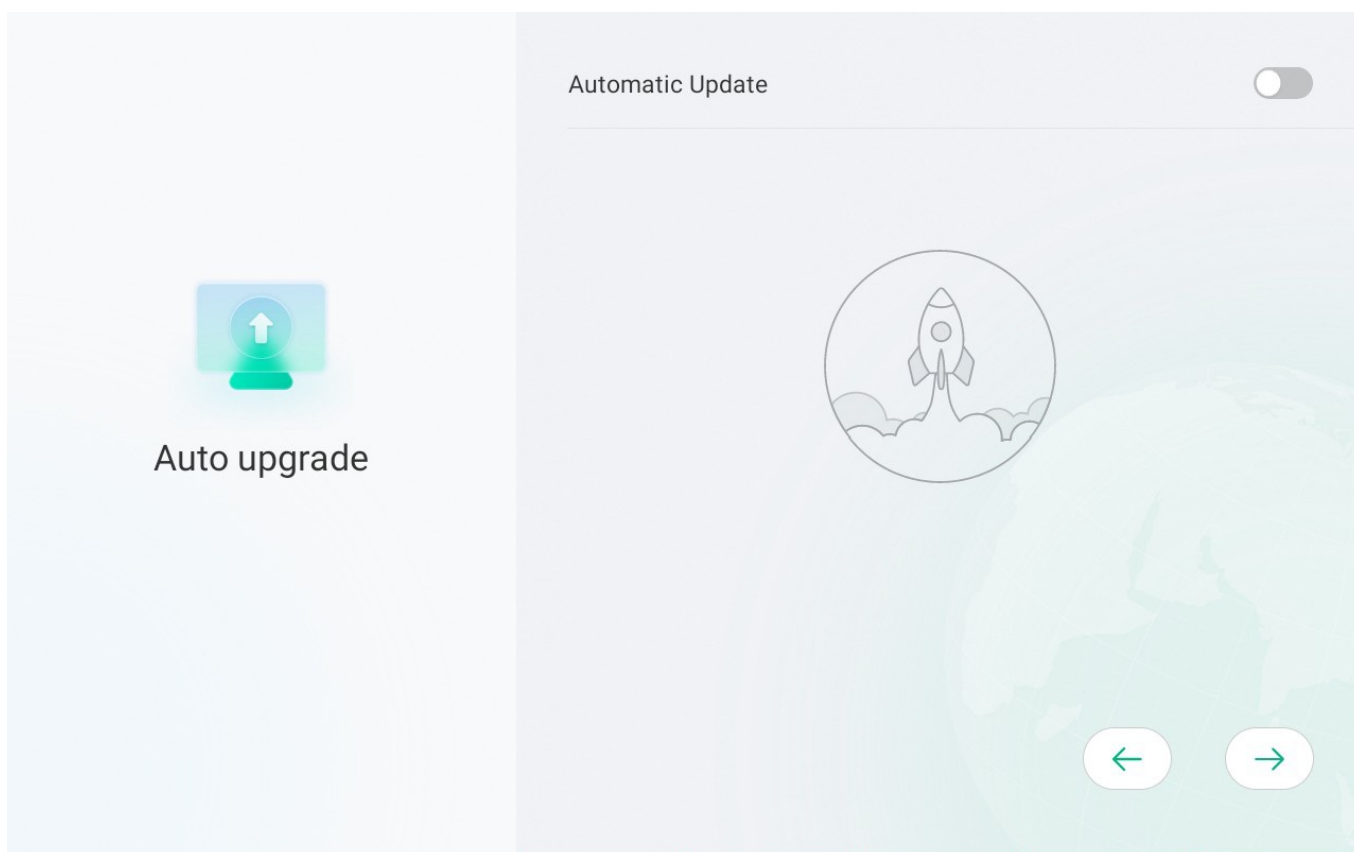


TIP

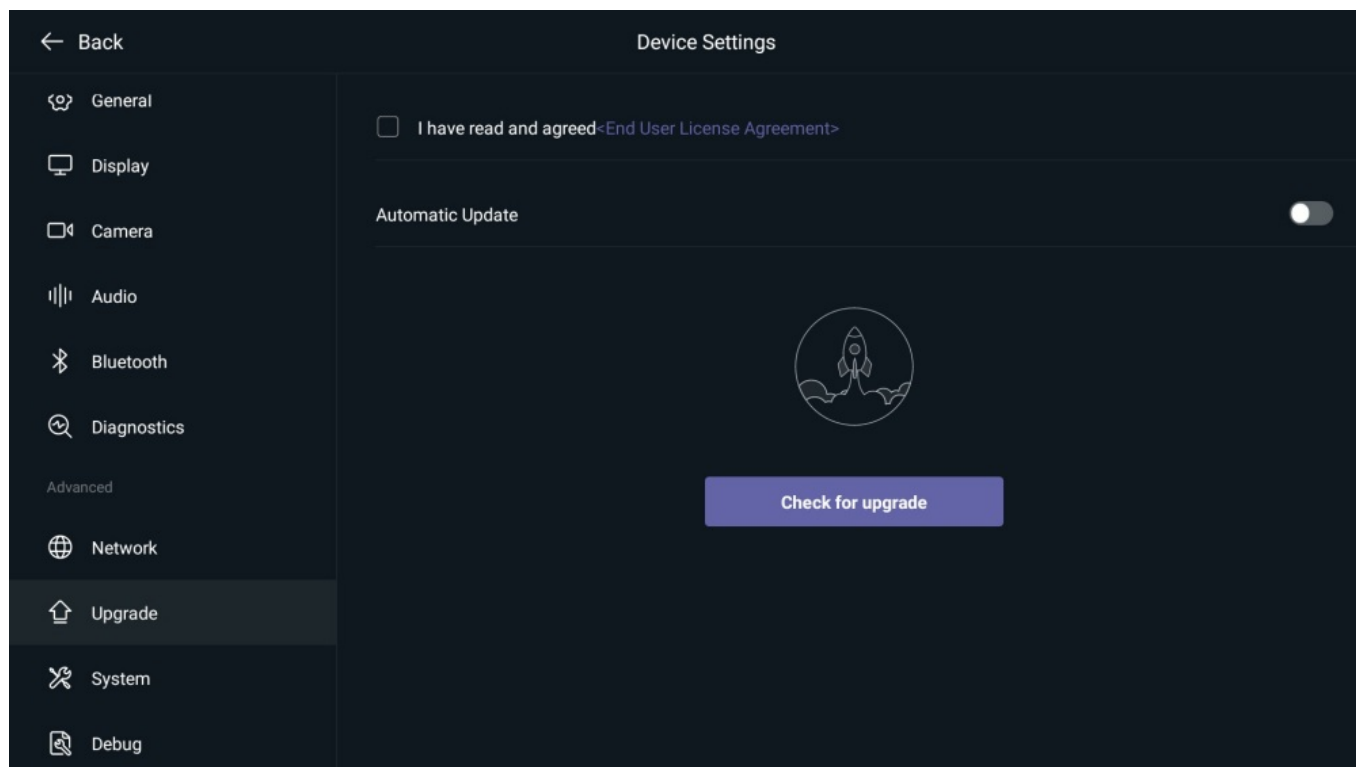
Update WPP20/WPP30: Normally, when using the WPP20/WPP30 after updating the MeetingBar AX0 to the latest terminal firmware, the firmware of the WPP20/WPP30 will be automatically updated.

Update via Automatic Update

- Enable **Auto Update** during initialization and the MeetingBar AX0 will be updated automatically.



- Go to the sidebar  > **Settings > Device Settings > Automatic Update** (default password: 0000) and the MeetingBar AX0 will be updated automatically.



Update via USB Flash Drive

- Download the latest firmware package of the MeetingBar AX0 and save it to the USB flash drive, and rename the firmware to *usb_firmware_upgrade.rom*.
- Put the firmware in the root directory of the USB flash drive.
- Insert the USB flash drive into the MeetingBar AX0. If the firmware package is suitable for the MeetingBar AX0 and the version is different from the current MeetingBar AX0 version, the MeetingBar AX0 will pop up an update prompt (it will automatically enter the upgrade after 10s).

Update via Auto Provisioning

Parameter	Description	Optional Value
static.firmw are.url	Auto provisioning deploys the server to perform firmware updates, and configures the complete url of the firmware storage address.	URL within 511 characters, empty by default.

Update via Teams Admin Center

For more information, please refer to [Microsoft Teams Admin Center](#).

FAQ

How do I update the MeetingBar A20/A30 System Firmware?

Firmware Update (CTP18)

Introduction

Two methods of firmware update:

- Update automatically through CTP18.
- Update through the web user interface of MeetingBar or the web user interface of the CTP18.

NOTE


When updating the CTP18 through the web user interface of MeetingBar, you can upload the CTP18 firmware to the web user interface of MeetingBar first. And the CTP18 will be automatically updated after pairing with the MeetingBar. For more information, please refer to [Quick Setup](#).

Firmware Version

Please download the corresponding CTP18 firmware version. For more information, please refer to [Release Note](#).

Firmware Update

Update via Check for Update

1. Tap  on the left or right side of the CTP18, go to **Settings > Update** (default password: 0000) > **Check for update** to check whether there is a new version.
2. When a new system version is available, download and install the package.

Update via Web User Interface

1. On the web user interface of the CTP18 or MeetingBar, go to **System > Update**.
2. Download the latest firmware version of the CTP18 to the local, select **Select File** next to **Endpoint Firmware** to upload firmware, and select **Update**.

Network Configuration

DHCP Option

Introduction

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

Supported DHCP Option for IPv4

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

Parameter	DHCP Option	Description
Subnet Mask	1	Specify the client' s subnet mask.
Time Offset	2	Specify the offset of the client' s subnet in seconds from Coordinated. Universal Time (UTC).
Router	3	Specify a list of IP addresses for routers on the client' s subnet.
Time Server	4	Specify a list of time servers available to the client.
Domain Name Server	6	Specify a list of domain name servers available to the client.
Log Server	7	Specify a list of MIT-LCS UDP servers available to the client.
Host Name	12	Specify the name of the client.
Domain Server	15	Specify the domain name that the client should use when resolving hostnames via DNS.
Broadcast Address	28	Specify the broadcast address in use on the client' s subnet.
Network Time Protocol Servers	42	Specify a list of NTP servers available to the client by IP address.
Vendor-Specific Information	43	Identify the vendor-specific information.
Vendor Class Identifier	60	Identify the vendor type.
TFTP Server Name	66	Identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.

DHCP Option 160 and Option 161

Configure via Web User Interface

1. Go to **System > Auto Provision** in the web user interface.

2. Enable **DHCP Active** to configure and click **Confirm**.

The screenshot shows the 'Auto Provision' configuration page for a Yealink MeetingBar A20 device. The left sidebar has 'System' selected. The main configuration area includes the following settings:

- DHCP Active:** Toggled 'On'.
- Custom Option:** 160,161.
- DHCP Option Value:** yealink.
- Server URL:** M7:features.slide_drawer.enable=0.
- Username:** (empty field).
- Password:** (masked field).
- Attempt Expired Time(s):** 5 (range 1-300).
- Common AES Key:** (masked field).
- MAC-Oriented AES Key:** (masked field).
- Power on:** Toggled 'On'.
- Repeatedly:** Toggled 'Off'.
- Interval(min):** 1440 (range 1-43200).

At the bottom right, there are 'Confirm' and 'Cancel' buttons.

Auto Provisioning

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

If the DHCP Option 66 is unavailable, you can use the custom option (160 or 161) with the URL or IP address of the provisioning server. The device will automatically detect 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.

Parameter	Description	Optional Value
static.auto_provision.dhcp_option.enable	It triggers the DHCP Option feature to on or off.	0: Disabled 1: Enabled (default)

<code>static.auto_provision.dhcp_option.list_user_options</code>	<p>It configures the custom DHCP option for requesting provisioning server address. Multiple DHCP options are separated by commas.</p> <div data-bbox="517 300 1123 517"> <p>NOTE</p> <p>It works only if “static.auto_provision.dhcp_option.enable” is set to 1 (Enabled).</p> </div>	<p>Integer from 128 to 254 (default: 160 and 161.)</p>
--	---	--

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 connecting to the secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server address. For more information, please 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 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).

For more information, please refer to [NTP Setting](#)

DHCP Option 12

Configure via Web Interface

1. Go to **Network > Wired Network** in the web user interface.

2. Configure **Host Name** and click **Confirm**.

The screenshot shows the Yealink MeetingBar A20 web interface. The left sidebar has a 'Network' menu item highlighted. The main content area is titled 'Wired Network'. Under the 'IPv4' section, the 'Network Connection Type' is set to 'Static IP'. The 'Host Name' field is highlighted with a red box and a circled '3', containing the text 'MeetingBar A20'. Other fields like Subnet Mask, Gateway, and DNS are also visible, with a circled '1' next to Subnet Mask and a circled '2' next to Gateway. The 'Confirm' button is at the bottom right.

Auto Provisioning

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](#)). Refer to [RFC 1035](#) for character restrictions.

DHCP Option 12 Hostname Configuration:

Parameter	Description	Optional Value
static.network.dhcp_host_name	It configures the DHCP option 12 hostname on the device.	String within 99 characters. Default: MeetingBar A20/MeetingBar A30

DHCP Option 60

Configure via Web User Interface

1. Go to **System > Auto Provision** in the web user interface.

2. Enable **DHCP Option Value** and click **Confirm**.

The screenshot shows the Yealink MeetingBar A20 web interface. On the left sidebar, the 'System' menu is expanded, and 'Auto Provision' is selected. The main content area is titled 'Auto Provision'. It contains several configuration fields: 'DHCP Active' (toggle on), 'Custom Option' (text field with '160,161'), 'DHCP Option Value' (text field with 'yealink', highlighted with an orange box and a circled '3'), 'Server URL' (text field with 'M7:features.slide_drawer.enable=0'), 'Username' (text field), 'Password' (password field), 'Attempt Expired Time(s)' (spinner with '5' and range '(1-300)'), 'Common AES Key' (password field), 'MAC-Oriented AES Key' (password field), 'Power on' (toggle on), 'Repeatedly' (toggle off), and 'Interval(min)' (spinner with '1440' and range '(1-43200)'). At the bottom right, there are 'Confirm' and 'Cancel' buttons.

Auto Provisioning

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:

Parameter	Description	Optional Value
static.auto_provision.dhcp_option.option60_value	It configures the value (vendor name of the device) of DHCP option 60.	String within 99 characters. Default: yealink.

Wi-Fi

Introduction

Connect the device to the wireless network or configure the device’ s wireless hotspot.

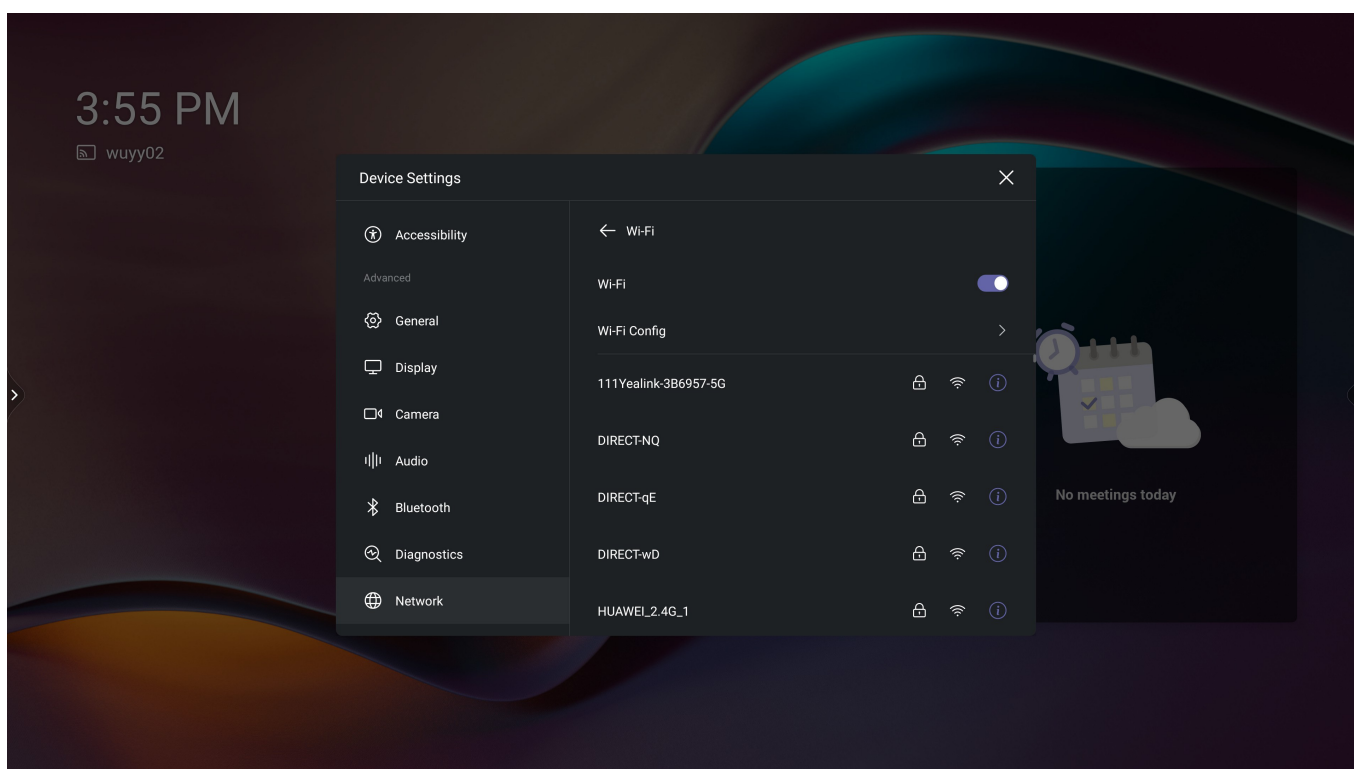
Wi-Fi Network

NOTE

- After connecting to the wireless network, the device will use the wireless network first.
- When connecting to a wireless network, both 2.4G/5G are supported.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **< Settings > Network (default password: 0000) > Wireless Network.**
2. Go to Wireless Networks under MeetingBar AX0 and CTP18.
3. Enable **Wi-Fi** to select a Wi-Fi to connect.

**Configure via Web User Interface**

1. Go to **Network > Wireless Network** on the web user interface.
2. Enable **Wi-Fi**.
3. Click **Scan Wireless Network** to start searching for the wireless networks in your area, or click **+** to add wireless networks manually.
4. Select a wireless network to connect. After the connection is successful, the status bar will display connected.

Parameter	Description
Connect to Existing Network	Enable or disable the Wi-Fi feature.
Scan Wireless Network	View the searchable wireless networks in the current area.
Wi-Fi Name	Displays the currently connected wireless network.
Disconnect network	Disconnected the currently connected wireless network.


Auto Provisioning

Parameter	Description	Optional Value
static.wifi.function.enable	It enables or disables the Wi-Fi feature.	0: Disable 1: Enable.
static.wifi.enable	It activates or deactivates the Wi-Fi mode.	0: Disable 1: Enable.
static.wifi.X.ssid	It configures the SSID of a specific wireless network. SSID is a unique identifier for accessing wireless access points.	ASCII codes of length 1-31
static.wifi.X.security_mode	It configures the security mode of a specific wireless network.	NONE WEP WPA/WPA2 PSK 802.1x EAP
static.wifi.X.password	It configures the password of a specific wireless network.	64 characters
static.wifi.X.eap_type	It configures the EAP authentication mode of a specific wireless network.	Auto TTLS PEAP TLS PWD

Configuration Wi-Fi

You can configure the MeetingBar to run in IPv4 or dual-stack (IPv4 and IPv6) mode and manually configure IPv4 or IPv6 wireless network settings.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to  **Settings > Network** (default password: 0000) > **Wireless Network**.
2. Configure the **Wireless Network** of the MeetingBar AX0 and CTP18.

Configure via Web User Interface

1. Go to **Network > Wireless Network** on the web user interface.
2. Configure **Wifi IPv4/Wifi IPv6**.

Parameter	Description
Network Connection Type (Wifi IPv4)	It configures the device to use DHCP to dynamically obtain network settings or manually configure the device' s IPv4 address.
Static IP (Wifi IPv4)	It triggers the static DNS feature to enable/disable.
Primary DNS (Wifi IPv4)	It configures the IPv4 address of the preferred DNS server.
Secondary DNS (Wifi IPv4)	It configures the IPv4 address of the secondary DNS server.
IP Address (Wifi IPv4)	It configures a static IPv4 address for the device.
Subnet mask (Wifi IPv4)	It configures the subnet mask assigned to the system.
Gateway (Wifi IPv4)	It configures the IPv4 default gateway.
IPv6 (Wifi IPv6)	It configures system for the IPv4 and IPv6 mode.
Network Connection Type (Wifi IPv6)	It configures the device to use DHCP to dynamically obtain network settings or manually configure the device' s IPv6 address.
Static IP (Wifi IPv6)	It triggers the static DNS feature to enable/disable.
Primary DNS (Wifi IPv6)	It configures the IPv6 address of the preferred DNS server.
Secondary DNS (Wifi IPv6)	It configures the IPv6 address of the secondary DNS server.
IPv6 Address(Wifi IPv6)	It configures a static IPv6 address for the device.
IPv6 prefix(Wifi IPv6)	It configures a static IPv6 prefix for the device. The IPv6 prefix is the number from left to right that converts the IPv6 address into binary.
Gateway (Wifi IPv6)	It configures the IPv6 default gateway.

Auto Provisioning

Parameter	Description	Optional Value
static.network.wifi.internet_port.type	It configures the device to use DHCP to dynamically obtain network settings or manually configure the device' s IPv4 address.	0: Disable 1: Enable.
static.network.wifi.static_dns_enable	It triggers the static DNS feature to enable/disable.	0: Disable 1: Enable.

static.network.wifi.primary_dns	It configures the IPv4 address of the preferred DNS server.	IPv4 Address
static.network.wifi.secondary_dns	It configures the IPv4 address of the secondary DNS server.	IPv4 Address
static.network.wifi.internet_port.ip	It configures a static IPv4 address for the device.	IPv4 Address
static.network.wifi.internet_port.mask	It configures the subnet mask assigned to the system.	Subnet Mask
static.network.wifi.internet_port.gateway	It configures the IPv4 default gateway.	IPv4 Address
static.network.wifi.ipv6_internet_port.type	It configures the device to use DHCP to dynamically obtain network settings or manually configure the device's IPv6 address.	0: Disable 1: Enable.
static.network.wifi.ipv6_static_dns_enable	It triggers the static DNS feature to enable/disable.	0: Disable 1: Enable.
static.network.wifi.ipv6_primary_dns	It configures the IPv6 address of the preferred DNS server.	IPv6 Address
static.network.wifi.ipv6_secondary_dns	It configures the IPv6 address of the secondary DNS server.	IPv6 Address
static.network.wifi.ipv6_internet_port.ip	It configures a static IPv6 address for the device.	IPv6 Address
static.network.wifi.ipv6_prefix	It configures a static IPv6 prefix for the device. The IPv6 prefix is the number from left to right that converts the IPv6 address into binary.	[1-128]
static.network.wifi.ipv6_internet_port.gateway	It configures the IPv6 default gateway.	IPv6 Address

Wireless AP

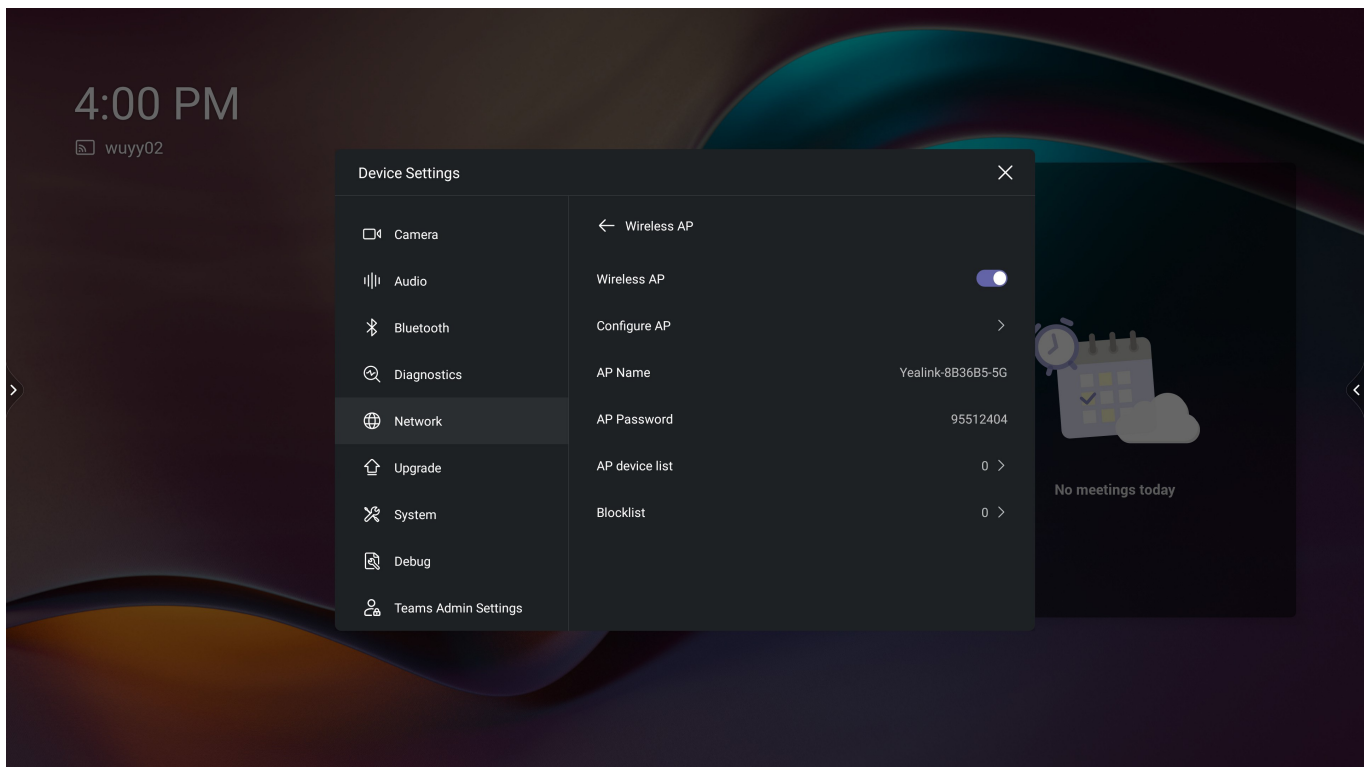
NOTE

When the wireless AP is enabled, the wireless network will be disabled.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to  > **Settings** > **Network** (default password: 0000) > **Wireless Network**.

2. Enable **Wireless AP** to configure the device parameters related.



Configure via Web User Interface

1. Go to **Network > Wireless Network** on the web user interface.

2. Enable **Wireless Hotspot** to configure the device parameters related.

The screenshot displays the Yealink MeetingBoard 65 web interface. In the left sidebar, the 'Network' menu item is highlighted with a red circle and the number 1, and the 'Wireless Network' sub-item is highlighted with a red circle and the number 2. The main content area shows the 'Wireless Network' configuration page. At the top, there is a toggle for 'Connect to Existing Network' and a 'Scan Wireless Network' button. Below this, the 'Network Name' is set to 'TPLINK_5G' and the status is 'Connected'. The 'Wi-Fi Hotspot' section is highlighted with a red box and contains the following settings:

- Wi-Fi Hotspot:** Enabled (toggle switch).
- Frequency:** 5G (selected), 2.4G.
- * Network Name:** Yealink-8B36B5-5G
- Encryption:** (dropdown menu)
- * Password:** 24078173
- Channel:** Auto
- LAN IP Address:** Auto (selected), Manually.
- Network Isolation:** Enabled (toggle switch).

A note at the bottom of the Wi-Fi Hotspot section states: 'After change Wi-Fi name and password, please remember to plug WPP20 to MeetingBoard 65 for Wi-Fi pairing.'

Parameter	Description
Frequency	It configures the frequency of the wireless AP. - 2.4G: Wide range. - 5G: Less interference, fast transmission.
Wi-Fi Name	It configures the network name of wireless AP. After modifying the configuration, please reconnect the WPP30 to the MeetingBar for pairing. Devices connected to the wireless AP of the MeetingBar need to reconnect to the wireless AP.
Encryption	It configures the security mode of the wireless AP. - None - WPA2-PSK: Enhanced encryption algorithm
Password	It configures the password of the wireless AP. After modifying the configuration, please reconnect the WPP30 to the MeetingBar for pairing. Devices connected to the wireless AP of the MeetingBar need to reconnect to the wireless AP.

Channel	<p>It configures the channel of the wireless AP. When the frequency band is 2.4G: Auto, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11.</p> <p>NOTE We recommend selecting Auto to avoid interference. If you want to select manually, we recommend selecting channels 1, 6, and 11 to reduce interference.</p> <p>When the frequency band is 5G: Auto, 36, 40, 44, 48, 149, 153, 157, 161, 165.</p> <p>NOTE We recommend selecting Auto to avoid interference. If you want to select manually, we recommend selecting more than 48 channels to ensure high power.</p>
Time	<p>It configures the default time to optimize wireless AP channels. You can choose a time from 00:00-23:00 on the hour.</p> <p>NOTE It needs to be configured when Channel is selected as Auto.</p>
Optimize Wireless AP	<p>The system will automatically take effect after clicking Optimize Wireless AP, and this configuration only takes effect after a specific time is set for the optimization time.</p>
LAN IP Address	<p>It configures the generation type of wireless AP address.</p> <ul style="list-style-type: none"> - Auto: Automatically assign the IP network segment of the Wireless AP. The default network segment is 192.168.144.X. - Manually: If automatically generated network segment conflicts with the one you use, you can change the network segment manually.
IP Address	<p>It configures the IP address of the wireless AP. It must conform to the IP format, such as 192.168.145.X.</p> <p>NOTE It needs to be configured only when the LAN IP address is configured manually.</p>
Network Isolation	<p>It enables or disables Network Isolation. After enabling, devices connected to the wireless AP cannot access the web user interface, applications, etc.</p>

Auto Provisioning

Parameter	Description	Optional Value
-----------	-------------	----------------

static.wifiap.enable	It enables or disables the Wireless AP.	0: Disabled 1: Enabled
static.wifiap.ssid	It configures the network name of wireless AP. Note: After modifying the configuration, please reconnect the [WPP20/WPP30] to the MeetingBar AX0 for pairing. Devices connected to the wireless AP of the MeetingBar AX0 need to reconnect to the wireless AP.	Support any combination of numbers, letters, Chinese characters, and special characters (such as @, #, %), and the length does not exceed 32 characters.
static.wifiap.security_mode	It configures the security mode of the wireless AP.	NONE WPA2-PSK
static.wifiap.password	It configures the password of the wireless AP.	Support any combination of numbers, letters, Chinese characters, and special characters (such as @, #, %), and the length is 8 - 64 characters.
static.wifiap.generation	It configures the Frequency of the wireless AP.	2.4-2.4G 5-5G
static.wifiap.channel	Configure the channel of the wireless AP.	For "static.wifiap.generation=2.4" : 0-Auto 1-1 2-2 3- 3 4-4 5-5 6-6 7-7 8-8 9-9 10-10 11-11 For "static.wifiap.generation=5" : 0-Auto 36-36 40-40 44-44 48-48 149-149 153-153 157-157 161-161 165-165

static.wifiap.dhcpd.mode	It configures the generation type of wireless AP address.	0: Auto 1: Manually
static.wifiap.dhcpd.segment	It configures the IP address of the wireless AP.	IPv4 Address

Wired Network

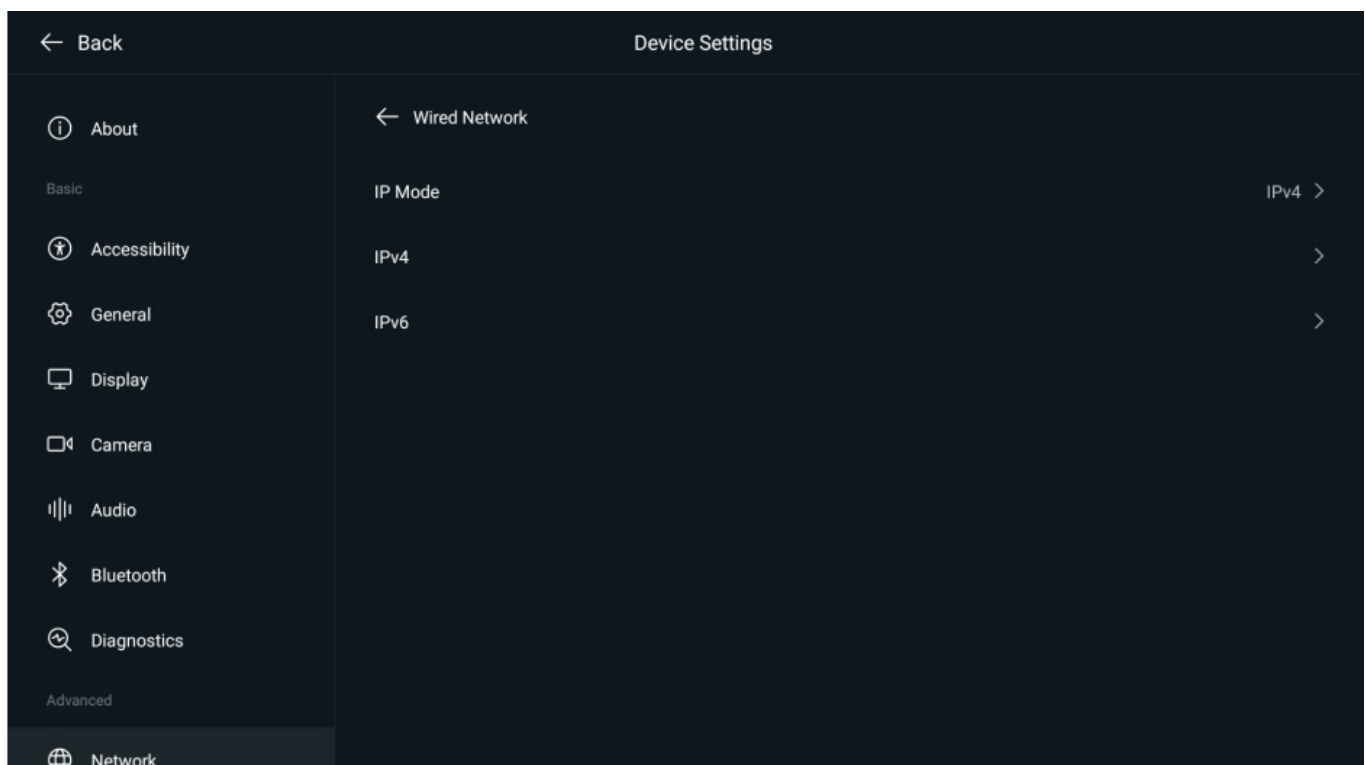
Introduction

Yealink Teams devices run on a local area network (LAN). You can configure your LAN to accommodate a variety of network designs, which vary by organization and device.

Select IP Mode

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Network > Wired Network** (default password: 0000).
2. Select **IPv4/IPv6/IP Mode** in the **IP Mode** of the MeetingBar AX0 and CTP18 respectively.



Configure via Web User Interface

The MeetingBar AX0 is configured to have IPv4 enabled by default. There is no IP mode option available on the web interface. If IPv6 is enabled, it will operate in **IPv4&IPv6** mode. If IPv6 is disabled, it will operate in **IPv4** mode.

1. Go to **Network > Wired Network** on the web user interface.
2. Enable/disable **IPv6** and click **Confirm**.

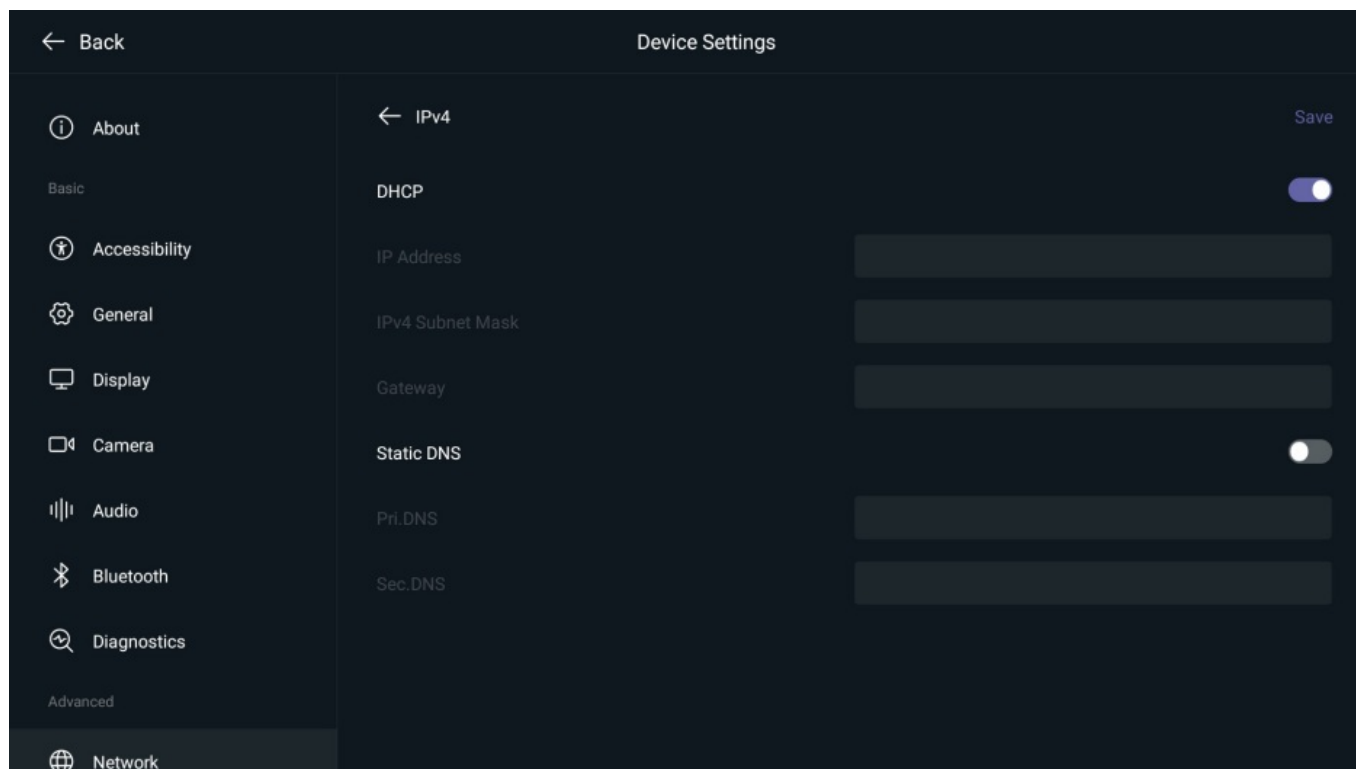
Auto Provisioning

Parameter	Description	Optional Value
static.network.ip_address_mode	It configures the IP mode of the wired network.	0: IPv4 2: IPv4 and IPv6

IPv4 Configuration

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Advanced > Network** (default password: 0000).
2. Enter **Wired Network** of the MeetingBar AX0 and CTP18 respectively, and select **IPv4**.



Configure via Web User Interface

1. Go to **Network > Wired Network** on the web user interface.

2. Configure IPv4 and click **Confirm**.

The screenshot displays the 'Wired Network' configuration page for a Yealink MeetingBar A20 device. The left-hand navigation menu shows 'Network' (1) and 'Wired Network' (2) as active options. The main configuration area for IPv4 (3) includes:

- Network Connection Type:** Radio buttons for 'Dynamic IP' (selected) and 'Static IP'.
- Static DNS:** A toggle switch currently turned off.
- Host Name:** A text field containing 'MeetingBar A20'.
- IPv6:** A toggle switch currently turned off.

'Confirm' and 'Cancel' buttons are located at the bottom right of the configuration area.

Parameter	Description
Network Connection Type	<p>It configures the device to use DHCP to obtain the network or manually configure the IPv4 address dynamically.</p> <ul style="list-style-type: none"> - Dynamic IP: The device automatically obtains the IP address through DHCP, and a DHCP server is required in the network. - Static IP: You need to configure the device' s IP address with the IP address, subnet mask, and gateway address.
Static DNS	<p>Enable or disable the DNS feature.</p> <p>When disabled, the device automatically obtains the DNS server address, and a DNS server is required in the network.</p> <div> <p>NOTE</p> <p>It can be configured when the network connection type is set to Dynamic IP.</p> </div>
DNS Primary Server	<p>It configures the IPv4 address of the preferred DNS server.</p> <div> <p>NOTE</p> <p>You can configure when the static DNS feature is enabled, or the network connection type is set to Static IP.</p> </div>

DNS Secondary Server	<p>It configures the IPv4 address of the secondary DNS server.</p> <p>NOTE You can configure when the static DNS feature is enabled, or the network connection type is set to Static IP.</p>
Host Name	<p>It configures the hostname of the system. When the system broadcasts DHCP DISCOVER messages, it will report the configured hostname to the DHCP server via DHCP option 12.</p>
IP Address	<p>It configures a static IPv4 address for the device.</p> <p>NOTE You can configure when the network connection type is set to Static IP.</p>
Subnet Mask	<p>It configures the subnet mask for the device. The subnet mask divides the IP address into the network and host addresses.</p> <p>NOTE You can configure when the network connection type is set to Static IP.</p>

Auto Provisioning

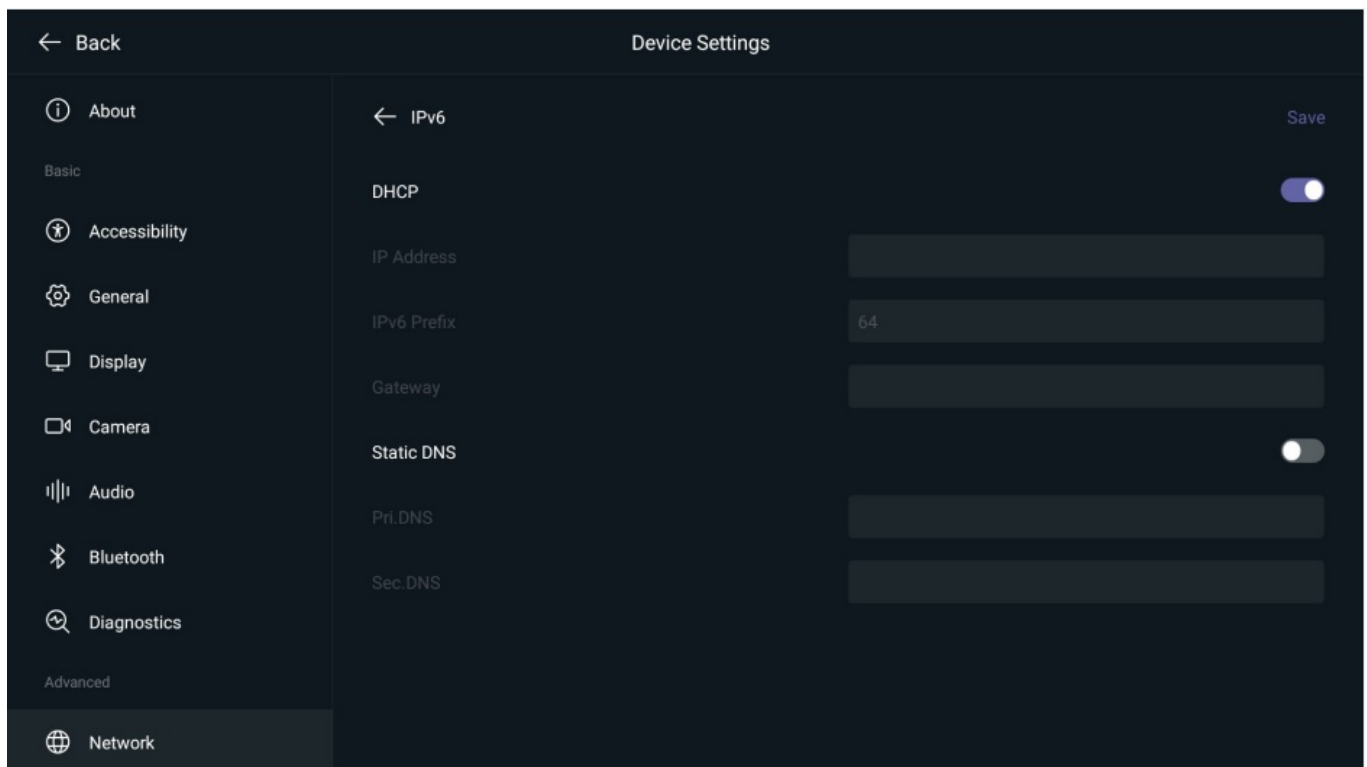
Parameter	Description	Optional Value
static.network.internet_port.type	It configures the device to use DHCP to dynamically obtain the network or manually configure the device's IP address.	<p>0: Dynamic IP. The device automatically obtains the IP address through DHCP, and a DHCP server is required in the network.</p> <p>1: Static IP. The device IP address must be manually configured.</p>
static.network.internet_port.ip	It configures the IPv4 address assigned to the system.	IPv4 Address

static.network.internet_port.mask	<p>It configures the subnet mask assigned to the system.</p> <p>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).</p>	Subnet Mask
static.network.internet_port.gateway	<p>It configures the IPv4 default gateway.</p> <p>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).</p>	IPv4 Address
static.network.static_dns_enable	<p>It triggers the static DNS feature to enable/disable.</p> <p>NOTE It works only if “static.network.internet_port.type” is set to 0 (DHCP).</p>	<p>0: Disabled. When disabled, the device automatically obtains the DNS server address, and a DNS server is required in the network.</p> <p>1: Enabled.</p>
static.network.primary_dns	It configures the primary IPv4 DNS server for the system.	IPv4 Address
static.network.secondary_dns	It configures the secondary DNS server for the system.	IPv4 Address

IPv6 Configuration

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Advanced > Network**(default password: 0000).
2. Enter **Wired Network** of the MeetingBar AX0 and CTP18 respectively, and select **IPv6**.



Configure via Web User Interface

1. Go to **Network > Wired Network** on the web user interface.

2. Configure IPv6 and click **Confirm**.

The screenshot shows the Yealink MeetingBar A20 web interface. On the left sidebar, the 'Network' menu item is circled with a red '1', and the 'Wired Network' sub-menu is highlighted with a blue bar and a red '2'. The main content area is titled 'Wired Network'. It contains two sections: 'IPv4' and 'IPv6'. The 'IPv6' section is highlighted with an orange box and a red '3'. Inside the 'IPv6' section, the 'IPv6' toggle switch is turned on. Below it, the 'Network Connection Type' has 'Dynamic IP' selected with a radio button, and 'Static IP' is unselected. The 'Static DNS' toggle switch is turned off. At the bottom of the page, there are 'Confirm' and 'Cancel' buttons.

Parameter	Description
Network Connection Type	<p>It configures the device to use DHCP to dynamically obtain the network or manually configure the device's IPv6 address.</p> <ul style="list-style-type: none"> - Dynamic IP: The device automatically obtains the IPv6 address through DHCP, and a DHCP server is required in the network. - Static IP: You need to configure the device's IPv6 address with the IP address, subnet mask, and gateway address.
Static DNS	<p>Enable or disable the DNS feature.</p> <p>When disabled, the device automatically obtains the DNS server address, and a DNS server is required in the network.</p> <div> <p>NOTE</p> <p>It can be configured when the network connection type is set to Dynamic IP.</p> </div>
DNS Primary Server	<p>It configures the IPv6 address of the preferred DNS server.</p> <div> <p>NOTE</p> <p>You can configure when the static DNS feature is enabled, or the network connection type is set to Static IP.</p> </div>

DNS Secondary Server	<p>It configures the IPv6 address of the secondary DNS server.</p> <p>NOTE You can configure when the static DNS feature is enabled, or the network connection type is set to Static IP.</p>
Host Name	<p>It configures the host name of the system. When the system broadcasts DHCP DISCOVER messages, it will report the configured host name to the DHCP server via DHCP option 12.</p>
IPv6 Address	<p>It configures a static IPv6 address for the device.</p> <p>NOTE It needs to be configured when the network connection type is set to Static IP.</p>
IPv6 Prefix	<p>It configures a static IPv6 prefix for the device. The IPv6 prefix is the number from left to right that converts the IPv6 address into binary.</p> <p>NOTE It needs to be configured when the network connection type is set to Static IP.</p>
Subnet Mask	<p>It configures the IPv6 default gateway. The subnet mask divides the IP address into the network and host addresses.</p> <p>NOTE It needs to be configured when the network connection type is set to Static IP.</p>

Auto Provisioning

Parameter	Description	Optional Value
static.network.ipv6_internet_port.type	It configures the device to use DHCP to dynamically obtain network or manually configure the device's IPv6 address.	0: Dynamic IP. The device automatically obtains the IPv6 address through DHCP, and a DHCP server is required in the network. 2: Static IP.
static.network.ipv6_internet_ip	It configures a static IPv6 address for the device.	IPv6 Address
static.network.ipv6_prefix	It configures the IPv6 prefix for the device.	0-128


static.network.ipv6_internet_port.gateway	It configures the IPv6 default gateway.	IPv6 Address
static.network.ipv6_static_dns_enable	It triggers the static DNS feature to enable/disable.	0: Disabled. When disabled, the device automatically obtains the DNS server address, and a DNS server is required in the network. 1: Enabled.
static.network.ipv6_primary_dns	It configures the IPv6 address of the preferred DNS server.	IPv6 Address
static.network.secondary_dns	It configures the IPv6 address of the secondary DNS server.	IPv6 Address

Wired Network Disabled

NOTE

The MeetingBar A10 version 278.321.0.20 and later is supported, but MeetingBar A20 and MeetingBar A30 are not.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to  **Settings** > **Network** (default password: 0000).
2. Enter the wired network settings to enable or disable the wired network. After disabling the wired network, the Meetingbar will be unable to access the network even if a network cable is connected. This configuration controls whether the A10 disables the wired network and the CTP18 wired network is not disabled.

Wireless Network

Introduction


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

Wireless Network


NOTE

- After connecting to the wireless network, the device will use the wireless network first.
- When connecting to a wireless network, both 2.4G/5G are supported.
- MeetingBar A10 with versions 278.321.0.20 and later support roaming between administrator-configured Wi-Fi LANs, A20 and A30 do not.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to  **> More > Settings > Device Settings > Network** (password: 0000) **> Wireless Network**.
2. Connect the MeetingBar AX0 and CTP18 to Wi-Fi respectively.

Configure via Web User Interface

1. Go to **Network > Wireless Network** on the web user interface.
2. Enable **Wireless Network**.
3. Click **Scan Wireless Network** to start searching for wireless networks in the area, or click  to manually add wireless network.
4. Select a wireless network to connect. After the connection is successful, the status bar will display connected.

Parameter	Description
Wireless Network	Enable or disable the wireless network.
Scan Wireless Network	View the searchable wireless networks in the current area.
Network Name	Displays the currently connected wireless network.
Disconnect network	Disconnected the currently connected wireless network.

Configure Wireless Network**Configure via Web User Interface**

1. Go to **Network > Wireless Network** on the web user interface.
2. Configure **Wifi IPv4/Wifi IPv6**.

Parameter	Description
Network Connection Type (Wifi IPv4)	It configures the device to use DHCP to dynamically obtain network settings or manually configure the device's IPv4 address.
Static IP (Wifi IPv4)	It triggers the static DNS feature to enable/disable.


Primary DNS (Wifi IPv4)	It configures the IPv4 address of the preferred DNS server.
Secondary DNS (Wifi IPv4)	It configures the IPv4 address of the secondary DNS server.
IP Address (Wifi IPv4)	It configures a static IPv4 address for the device.
Subnet mask (Wifi IPv4)	It configures the subnet mask assigned to the system.
Gateway (Wifi IPv4)	It configures the IPv4 default gateway.
IPv6 (Wifi IPv6)	It configures system for the IPv4 and IPv6 mode.
Network Connection Type (Wifi IPv6)	It configures the device to use DHCP to dynamically obtain network settings or manually configure the device' s IPv6 address.
Static IP (Wifi IPv6)	It triggers the static DNS feature to enable/disable.
Primary DNS (Wifi IPv6)	It configures the IPv6 address of the preferred DNS server.
Secondary DNS (Wifi IPv6)	It configures the IPv6 address of the secondary DNS server.
IPv6 Address(Wifi IPv6)	It configures a static IPv6 address for the device.
IPv6 prefix(Wifi IPv6)	It configures a static IPv6 prefix for the device. The IPv6 prefix is the number from left to right that converts the IPv6 address into binary.
Gateway (Wifi IPv6)	It configures the IPv6 default gateway.

Wireless AP

NOTE

When the wireless AP is enabled, the wireless network will be disabled.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to  **> More > Settings > Device Settings > Network** (password: 0000) **> Wireless AP**.
2. Enter **Wireless AP** of the MeetingBar AX0 and CTP18 respectively.

Configure via Web User Interface

1. Go to **Network > Wireless Network** on the web user interface.
2. Enable **Wireless Hotspot** to configure the device parameters related.

Parameter	Description
Frequency	<p>It configures the frequency of the wireless AP.</p> <ul style="list-style-type: none"> - 2.4G: Wide range. - 5G: Less interference, fast transmission.
Wi-Fi Name	<p>It configures the network name of the wireless AP.</p> <div> <p>NOTE</p> <p>After modifying the configuration, please reconnect the WPP20/WPP30 to the MeetingBar AX0 for pairing. Devices connected to the wireless AP of the MeetingBar AX0 need to reconnect to the wireless AP.</p> </div>
Encryption	<p>It configures the security mode of the wireless AP.</p> <ul style="list-style-type: none"> - None - WPA2-PSK: Enhanced encryption algorithm
Password	<p>It configures the password of the wireless AP.</p> <div> <p>NOTE</p> <p>After modifying the configuration, please reconnect the WPP20/WPP30 to the MeetingBar AX0 for pairing. Devices connected to the wireless AP of the MeetingBar AX0 need to reconnect to the wireless AP.</p> </div>
Channel	<p>It configures the channel of the wireless AP.</p> <ul style="list-style-type: none"> - When the frequency band is 2.4G: Auto, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11. We recommend selecting Auto to avoid interference. If you want to select manually, we recommend selecting channels 1, 6, and 11 to reduce interference. - When the frequency band is 5G: Auto, 36, 40, 44, 48, 149, 153, 157, 161, 165. We recommend selecting Auto to avoid interference. If you want to select manually, we recommend selecting more than 48 channels to ensure high power.
Time	<p>It configures the default time to optimize wireless AP channels. You can choose a time from 00:00-23:00 on the hour or disable the feature.</p> <div> <p>NOTE</p> <p>It needs to be configured when Channel is selected as Auto.</p> </div>
Optimize Wireless AP	<p>The system will automatically take effect after clicking Optimize Wireless AP, and this configuration only takes effect after a specific time is set for the optimization time.</p>

LAN IP Address	<p>It configures the generation type of wireless AP address.</p> <ul style="list-style-type: none">- Auto: Automatically assign the IP network segment of the Wireless AP. The default network segment is 192.168.144.X.- Manually: If the automatically generated network segment conflicts with the one you use, you can change the network segment manually.
IP address	<p>It configures the IP address of the wireless AP. It must conform to the IP format, such as 192.168.145.X.</p> <div><p>NOTE</p><p>It needs to be configured only when the LAN IP address is configured manually.</p></div>
Network Isolation	<p>It enables or disables Network Isolation. After enabling, devices connected to the wireless AP cannot access the web user interface, applications, etc.</p>

Advanced Network

Introduction

It configures parameters related to the advanced network.

LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows systems 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 systems, the systems periodically advertise their information to the directly connected LLDP-enabled switch.

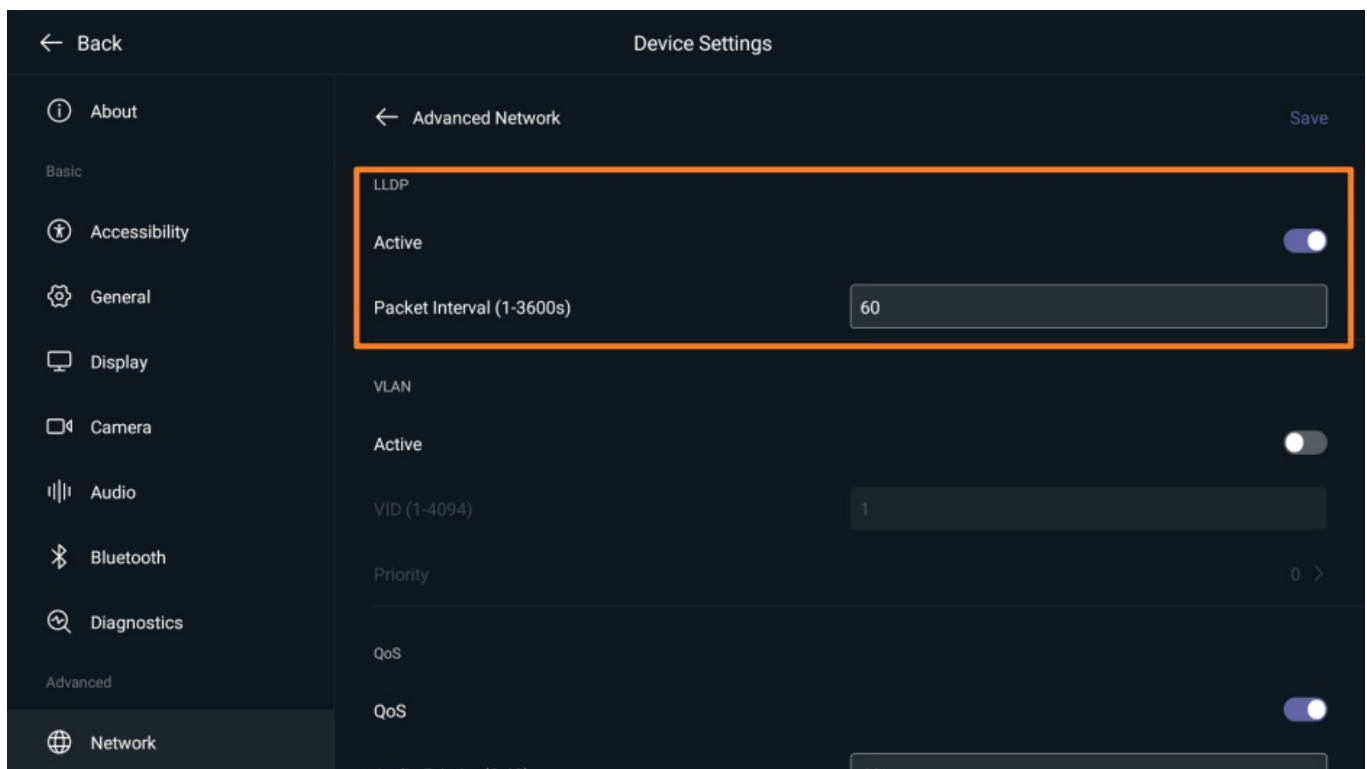
The systems can also receive LLDP packets from the connected switch and obtain their VLAN IDs, and then start communications with the call control.

The switch assigns a VLAN ID to the endpoint through the LLDP protocol.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Network** (default password: 0000).

2. Enter **Advanced Network > LLDP** of the MeetingBar AX0 and CTP18 respectively to configure it.



Configure via Web User Interface

1. Go to **Network > Advanced Network** on the web user interface.

2. Configure LLDP and click **Confirm**.

The screenshot shows the 'Advanced' configuration page for a Yealink MeetingBar A20. The left sidebar contains navigation options: Status, Network, Wireless Network, Wired Network, Advanced, Network Diagnostic, Proxy, System, and Security. The 'Advanced' option is selected and highlighted in blue. The main content area is titled 'Advanced' and contains three sections: LLDP, CDP, and VLAN. The LLDP section is highlighted with an orange box and includes a toggle for 'Active' (checked), a numeric input for 'Packet Interval (1-3600s)' set to 60, and a range of (1-3600). The CDP section includes a toggle for 'Active' (checked) and a numeric input for 'Packet Interval(1-3600s)' set to 60. The VLAN section includes a toggle for 'Internet Port' 'Active' (unchecked), a numeric input for 'VID(1-4094)' set to 1, a dropdown for 'Priority' set to 0, and a toggle for 'DHCP VLAN' 'Active' (checked). At the bottom right of the main content area are 'Confirm' and 'Cancel' buttons.

Auto Provisioning

Parameter	Description	Optional Value
static.network.lldp.enable	Enable or disable the LLDP feature.	0: Disabled 1: Enabled. The device will try to determine its VLAN ID through LLDP. Default: 1
static.network.lldp.packet_interval	It configures the frequency interval (in seconds) at which the device sends LLDP requests. <div> NOTE It works only if “static.network.lldp.enable” is set to 1 (Enable). </div>	Integer from 1 to 3600. Default: 60

VLAN

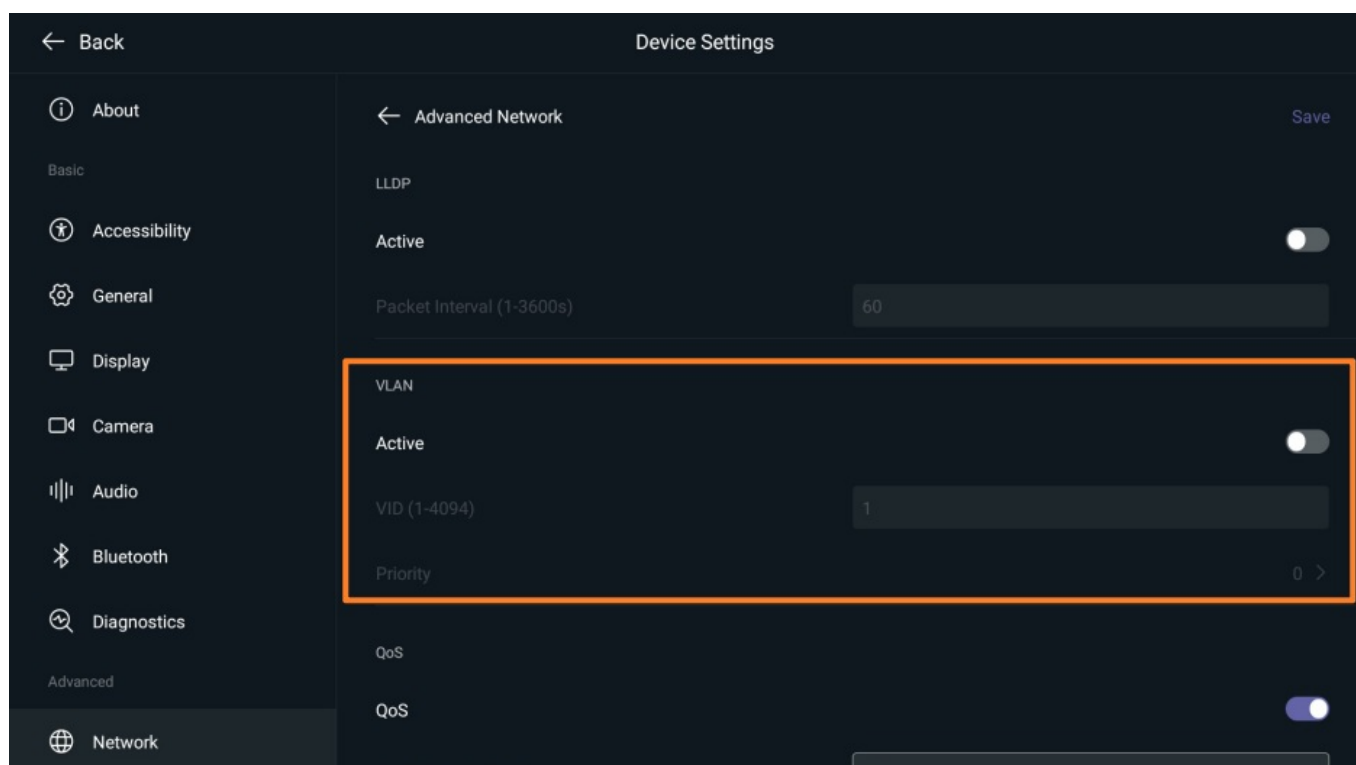
The purpose of VLAN configurations on the device is to insert a tag with VLAN information to the packets generated by the device. When VLAN is properly configured for the ports on the device, the device will tag all packets from

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.

Configure via Device Interface

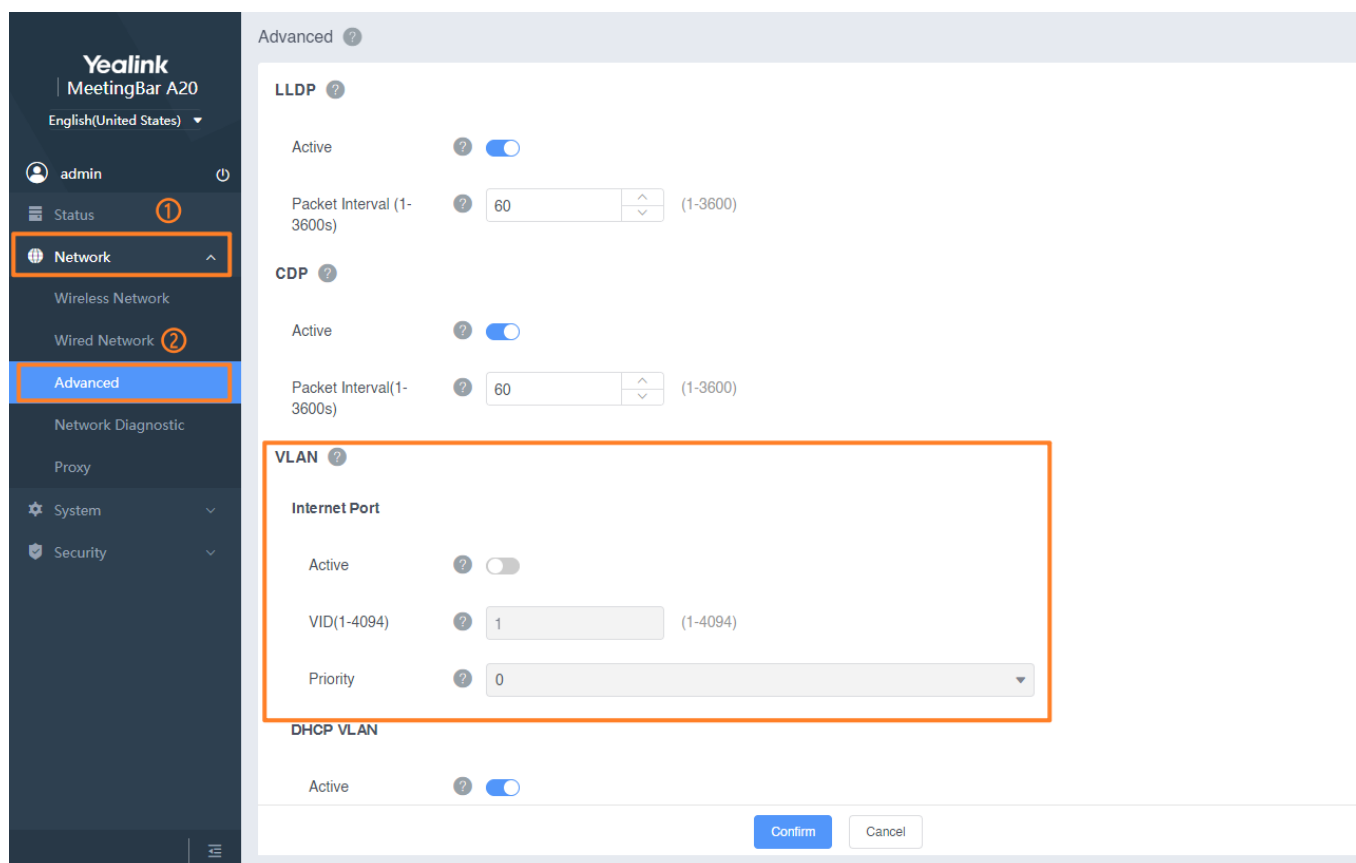
1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Network** (default password: 0000).
2. Enter **Advanced Network > VLAN** of the MeetingBar AX0 and CTP18 respectively to configure it.



Configure via Web User Interface

1. Go to **Network > Advanced** in the web user interface.

2. Enable VLAN to configure.



Auto Provisioning

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.

Parameter	Description
Activate (Internet Port)	Enable or disable VLAN for the Internet port.
VID(1-4094)	Configure the identification of the Virtual LAN. The last 12 bits of the VLAN are called the VLAN identifier VID, which uniquely marks which VLAN the Ethernet frame belongs to.
Priority	Configure the VLAN priority.

Activate (DHCP VLAN)	<p>Enable or disable the DHCP VLAN discovery feature on the system.</p> <p>Your system supports VLAN discovery via DHCP. When the VLAN discovery method is set to DHCP, the system will examine DHCP option for a valid VLAN ID.</p> <p>The predefined option 132 is used to supply the VLAN ID (it should be predefined on the DHCP server first) by default.</p> <p>The administrator can customize the DHCP option used to request the VLAN ID.</p>
Option	<p>Configure the DHCP option from which the system obtains the VLAN settings.</p> <p>You can configure at most 5 DHCP options and separate them by commas.</p> <p>Note: the value can be any integer from 1 to 255. The default value is 132.</p>

Parameter	Description	Optional Value
static.network.lldp.enable	It enables or disables the LLDP feature on the device.	0: Disabled 1: Enabled, the device will attempt to determine its VLAN ID through LLDP.
static.network.lldp.packet_interval	<p>It configures the interval (in seconds) that how often the device sends the LLDP request.</p> <div> <p>NOTE</p> <p>It works only if “static.network.lldp.enable” is set to 1 (Enabled).</p> </div>	Integer from 1 to 3600

CDP

CDP Parameters CDP (Cisco Discovery Protocol) enables MeetingBoard to receive and/or transmit device-related information from directly connected devices on the local network. When the CDP feature is enabled on the MeetingBoard, the MeetingBoard will periodically publish its own information to the directly connected switch enabled with CDP. The MeetingBoard can also receive CDP packets from the connected switch.

Configure via Web User Interface

1. Go to **Network > Advanced** on the web user interface.
2. Configure in the **CDP**.

Parameter	Description
Active	It configures MeetingBar to enable CDP.
Packet Interval(1-3600s)	It configures the interval for sending CDP packets.

Auto Provisioning

Parameter	Description	Optional Value
-----------	-------------	----------------

static.network.cdp.enable	It configures MeetingBoard whether to enable CDP.	0-Disable 1-Enable
static.network.cdp.packet_interval	It configures the interval for sending CDP packets.	1-3600

Port Link

Configure via Web User Interface

1. Go to **Network > Advanced** in the web user interface.
2. Configure in **Port Link** and click **Confirm**.

The screenshot shows the Yealink MeetingBar A20 web interface. The left sidebar contains the navigation menu with 'Network' selected and 'Advanced' highlighted. The main content area is titled 'Advanced' and contains several configuration sections:

- DHCP VLAN**: 'Active' is toggled on, and 'Option' is set to 132.
- Port Link**: 'WAN Port Link' is set to 'Auto Negotiation' (highlighted with an orange box).
- QoS**: 'QoS Enable' is toggled on. 'Audio Priority' is 46, 'Video Priority' is 34, and 'Data Priority' is 26, all with range (0-63).
- MTU**: 'Network MTU(1000-1500)' is 1500, and 'Restricted Single Packet Mode' is toggled on.

At the bottom right, there are 'Confirm' and 'Cancel' buttons.

Auto Provisioning

Parameter	Description	Optional Value
-----------	-------------	----------------

static.network.internet_port.speed_duplex	It configures the transmission method of the Internet port.	0: Auto Negotiation 1: Full Duplex 10Mbps 2: Full Duplex 100Mbps 3: Half Duplex 10Mbps 4: Half Duplex 100Mbps
---	---	--

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.

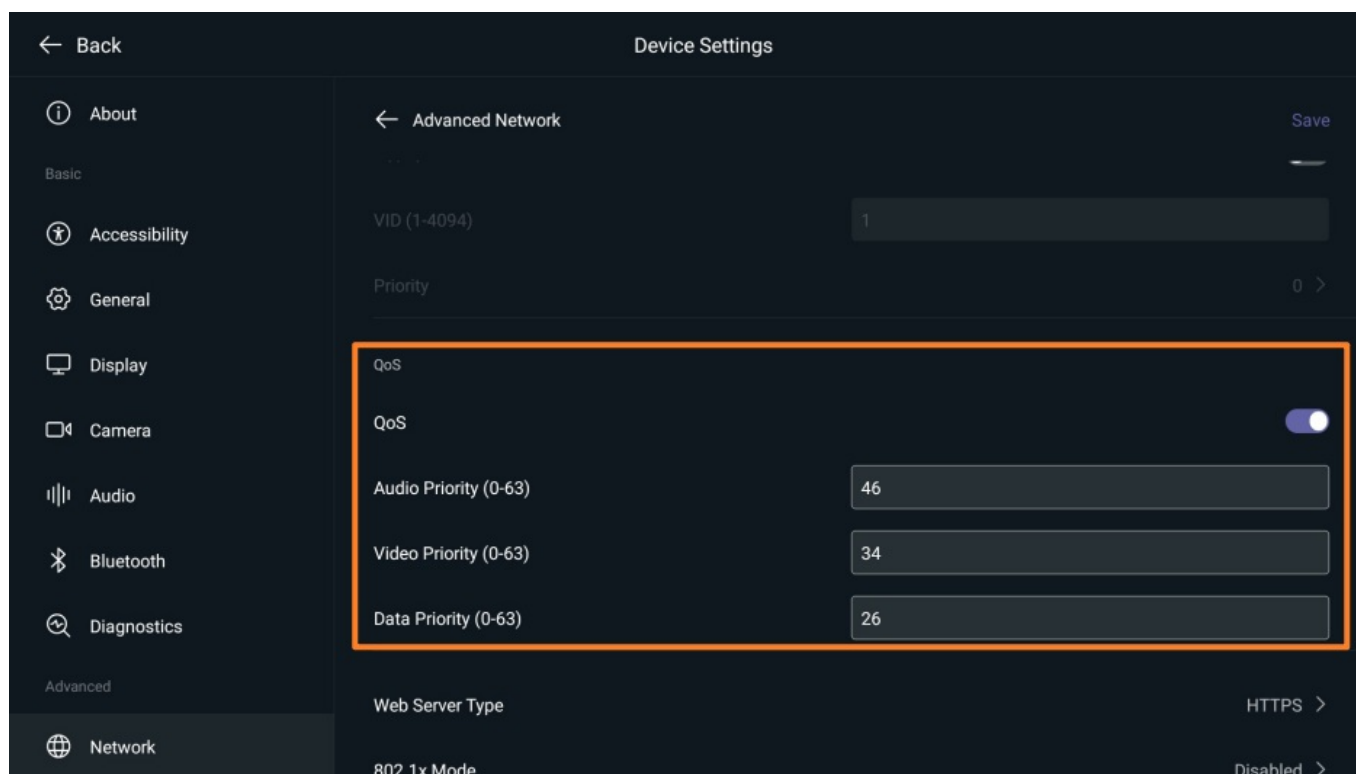
- **Data QoS**

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.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Network** (default password: 0000).

2. Enter **Advanced Network** > **QoS** of the MeetingBar AX0 and CTP18 respectively to configure it.



Configure via Web User Interface

1. Go to **Network** > **Advanced** in the web user interface.

2. Configuring QoS and click **Confirm**.

The screenshot displays the 'Advanced' configuration page for the Yealink MeetingBar A20. The left-hand navigation menu is visible, with 'Network' selected and 'Advanced' highlighted. The main configuration area is titled 'Advanced' and contains several sections. The 'QoS' section is highlighted with an orange box and includes a 'QoS Enable' toggle switch (turned on), 'Audio Priority' (46), 'Video Priority' (34), and 'Data Priority' (26), each with a range of (0-63). Below this is the 'MTU' section with 'Network MTU(1000-1500)' set to 1500 and 'Restricted Single Packet Mode' toggled on. The 'SNMP' section at the bottom has 'Active' toggled off. A 'Confirm' button is located at the bottom right of the configuration area.

Parameter	Description	Optional Value
static.network.qos.enable	It enables or disables the QoS feature.	0: Disabled 1: Enabled (default)
static.network.qos.audio	It configures the DSCP (Differentiated Services Code Point) for audio packets.	Integer from 0 to 63 (default: 46)
static.network.qos.video	It configures the DSCP (Differentiated Services Code Point) for video packets.	Integer from 0 to 63 (default: 34)
static.network.qos.signal	It configures the DSCP (Differentiated Services Code Point) for data packets.	Integer from 0 to 63 (default: 26)

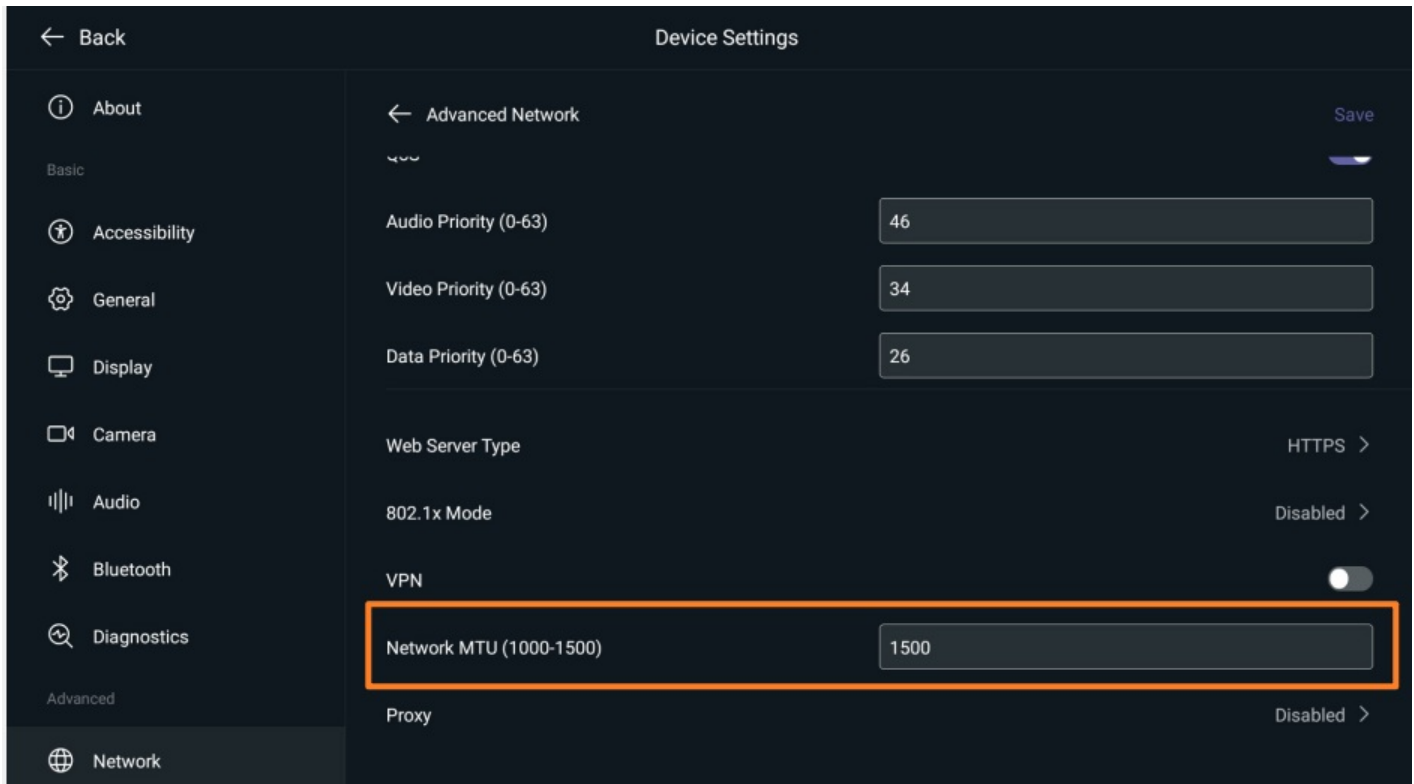
MTU

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.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Network** (default password: 0000).
2. Enter **Advanced Network > Video Priority** of the MeetingBar AX0 and CTP18 respectively to configure it.



Configure via Web User Interface

1. Go to **Network > Advanced** in the web user interface.

2. Configure in **MTU** and click **Confirm**.

The screenshot displays the 'Advanced' configuration page for the Yealink MeetingBar A20. The left-hand navigation menu has 'Network' selected, and 'Advanced' is highlighted. The main configuration area includes the following settings:

- Option:** 132
- Port Link:** Auto Negotiation
- QoS:**
 - QoS Enable: ☒
 - Audio Priority: 46 (range 0-63)
 - Video Priority: 34 (range 0-63)
 - Data Priority: 26 (range 0-63)
- MTU (highlighted with an orange box):**
 - Network MTU(1000-1500): 1500 (range 1000-1500)
 - Restricted Single Packet Mode: ☒
- SNMP:**
 - Active: ☐

'Confirm' and 'Cancel' buttons are located at the bottom right of the configuration area.

Auto Provisioning

Parameter	Description	Optional Value
static.network.mtu_value	It configures the MTU (Maximum Transmission Unit) of network interface card.	Integer from 1000 to 1500
video.single_packet_mode.enable	It enables or disables the restricted single packet mode. <div> 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. </div>	0: Off, sends data packets by using multiple packets mode. 1: On, sends data packets by using single packet mode (default).

SNMP

SNMP is a network management standard protocol widely used in TCP/IP networks. This protocol can support network management systems to monitor devices connected to the network for any management concerns.

Configure via Web User Interface

1. Go to **Network > Advanced** in the web user interface.
2. Configure in **SNMP** and click **Confirm**.

The screenshot displays the Yealink MeetingBar A20 web user interface. On the left, a dark sidebar contains the navigation menu. The 'Network' option is selected and highlighted with an orange box, and the 'Advanced' sub-option is also highlighted with an orange box. The main content area shows the 'Advanced' configuration page. The 'SNMP' section is highlighted with an orange box, showing the 'Active' toggle switch is disabled, the 'Port' is set to 161, and the 'Trusted Address' field is empty. The 'Web Server' section shows 'HTTP' is disabled, 'HTTP Port' is 80, 'HTTPS' is enabled, and 'HTTPS Port' is 443. The '802.1x' section is partially visible at the bottom. 'Confirm' and 'Cancel' buttons are located at the bottom right of the page.

Auto Provisioning

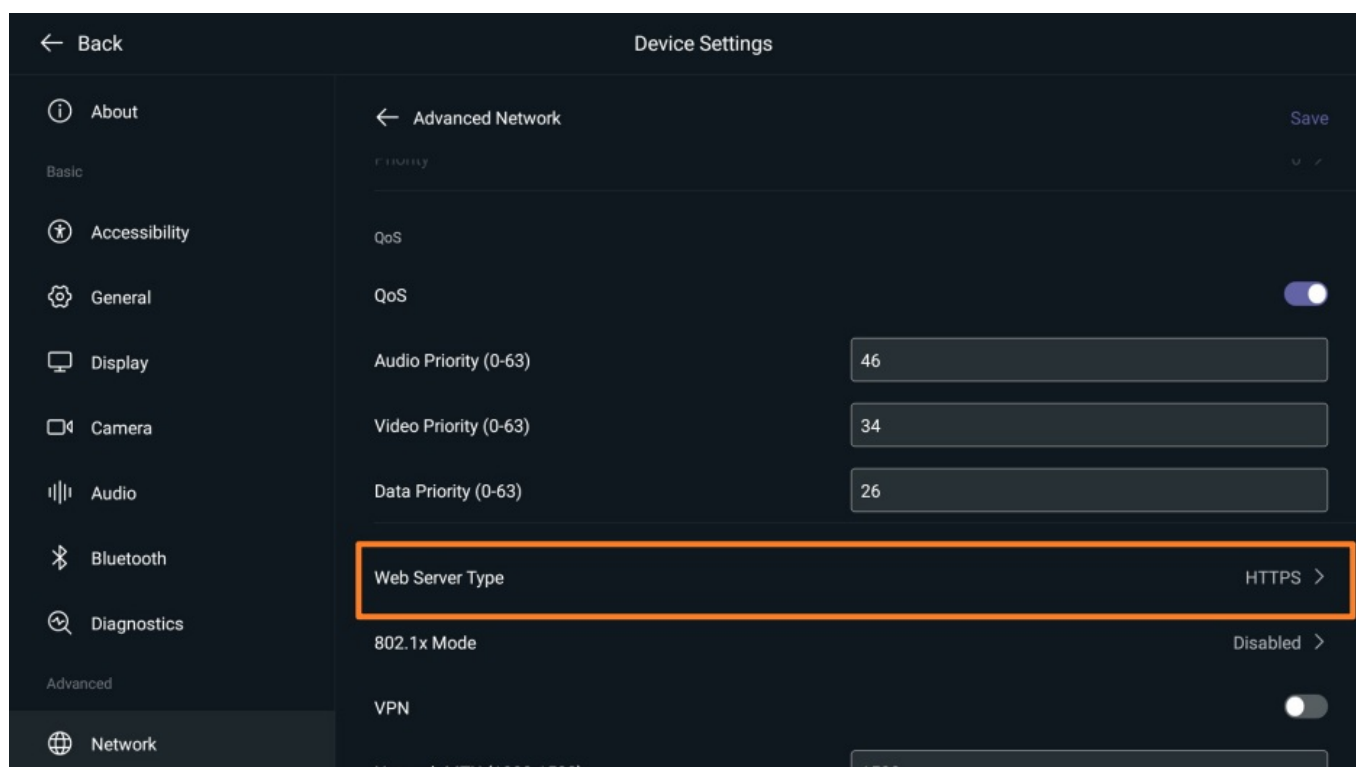
Parameter	Description	Optional Value
network.snmp.enable	Enable or disable the SNMP feature.	0: Disabled 1: Enabled Default: 0
network.snmp.port	Configure the SNMP port.	Integer from 1 to 65535. Default: 161
network.snmp.trust_ip	Configure SNMP trusted addresses.	URL within 511 characters. Null by default.

Web Server Type

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Network** (default password: 0000).

2. Enter **Advanced Network > Server Type** of the MeetingBar AX0 and CTP18 respectively to configure it.



Configure via Web User Interface

1. Go to **Network > Advanced** in the web user interface.

2. Configure in **Web Server** and click **Confirm**.

The screenshot shows the 'Advanced' configuration page for a Yealink MeetingBar A20. The left sidebar has 'Network' selected, with 'Advanced' highlighted. The main content area shows the 'Web Server' configuration, which is highlighted with an orange box. The 'Web Server' section includes:

- HTTP**: A toggle switch is turned off.
- HTTP Port**: Set to 80 (range 1-65535).
- HTTPS**: A toggle switch is turned on.
- HTTPS Port**: Set to 443 (range 1-65535).

 Below the 'Web Server' section is the '802.1x' section, which includes:

- 802.1x Mode**: Set to 'Disabled'.
- Identity**: An empty text field.
- MD5 Password**: A masked password field.
- CA Certificates**: An 'Import' button.
- Device Certificates**: An 'Import' button.

 At the bottom right, there are 'Confirm' and 'Cancel' buttons.

Auto Provisioning

Parameter	Description	Optional Value
wui.http_enable	It enables or disables the user to access the web user interface of the device using the HTTP protocol.	0: Disabled 1: Enabled Default: 0
network.port.http	It configures the HTTP port for the user to access the web user interface of the device using the HTTP protocol.	Integer from 1 to 65535. Default: 80
wui.https_enable	It enables or disables the user to access the web user interface of the device using the HTTPS protocol.	0: Disabled 1: Enabled Default: 0
network.port.https	It configures the HTTPS port for the user to access the web user interface of the device using the HTTPS protocol.	Integer from 1 to 65535. Default: 443

802.1X

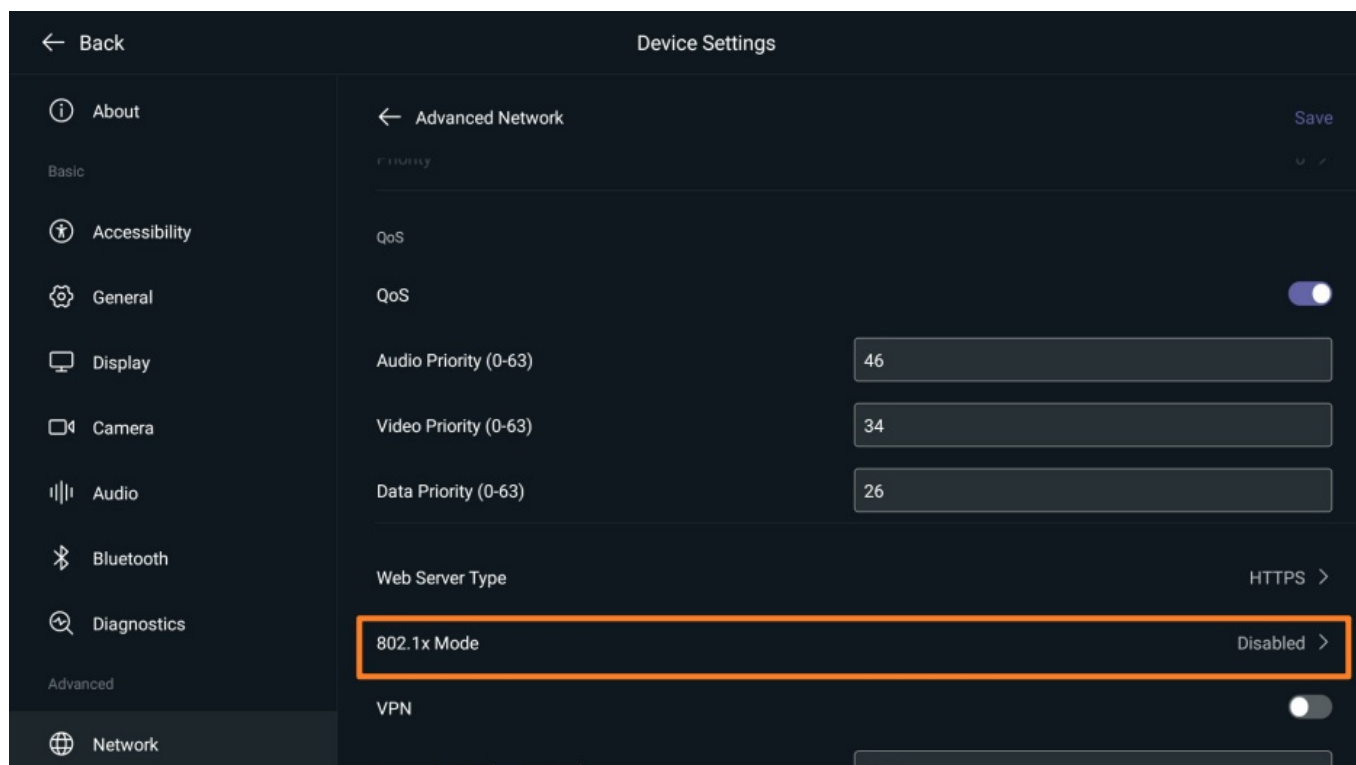
Yealink Teams IP Phones support the following protocols for 802.1X authentication:

- EAP-MD5

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

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Network** (default password: 0000).
2. Enter **Advanced Network > 802.1X** of the MeetingBar AX0 and CTP18 respectively to configure it.



Configure via Web User Interface

1. Go to **Network > Advanced** in the web user interface.

2. Configure in **802.1x** click **Confirm**.

The screenshot shows the Yealink MeetingBar A20 Advanced configuration page. The left sidebar has the 'Network' menu expanded, with 'Advanced' highlighted. The main content area shows the 'Web Server' section with 'HTTP' and 'HTTPS' settings. Below this, the '802.1x' section is highlighted with an orange box, showing '802.1x Mode' set to 'Disabled', 'Identity' field, 'MD5 Password' field, and 'CA Certificates' and 'Device Certificates' buttons. The 'VPN' section is also visible below.

Auto Provisioning


Parameter	Description	Optional Value
static.network.802_1x.mode	It configures the 802.1x authentication method.	0: Disabled, 802.1x authentication is not required. 1: EAP-MD5 2: EAP-TLS 3: EAP-MSCHAPv2 4: EAP-TTLS/EAP-MSCHAPv2 Default: 0
static.network.802_1x.i.identity	It configures the user name for 802.1x authentication. <div> <i>NOTE</i> It works only if “static.network.802_1x.mode” is set to 1, 2, 3, 4. </div>	String within 32 characters. Null by default.

static.network.802_1x.md5_password	<p>It configures the password for 802.1x authentication.</p> <p>NOTE It works only if “static.network.802_1x.mode” is set to 1, 3, 4.</p>	String within 32 characters. Null by default.
static.network.802_1x.root_cert_url	<p>It configures the access URL of the CA certificate. The format of the certificate must be *.pem, *.crt, *.cer or *.der.</p> <p>NOTE It works only if “static.network.802_1x.mode” is set to 2, 3, 4.</p>	URL within 511 characters. Null by default.
static.network.802_1x.client_cert_url	<p>It configures the access URL of the device certificate. The format of the certificate must be *.pem.</p> <p>NOTE It works only if “static.network.802_1x.mode” is set to 2 (EAP-TLS).</p>	URL within 511 characters. Null by default.

VPN

The VPN technology establishes a private tunnel on the public network through key exchange, encapsulation, authentication and encryption, to ensure the integrity, privacy, and validity of the transmitted data. To prevent disclosure of private information, tunnel endpoints must authenticate each other before the secure VPN tunnel is established. After you configure VPN feature on the system, the system will act as a VPN client and uses the certificates to authenticate with the VPN server.

Configure via Device Interface

1. On CTP18 or with remote control, go to  **> More > Settings > Device Settings > Network** (default password: 0000).
2. Enable **VPN** and select **Save**.

Configure via Web User Interface

1. Go to **Network > Advanced Network** on the web user interface.
2. Configure in the **VPN** field.

Parameter	Description
Active	Enable or disable the VPN feature on the system.
Upload VPN Config	Upload the compressed package of VPN-related files (*.tar) to the system. (refer to the table below)

To use VPN, you should upload the compressed package of VPN-related files to the system in advance. The file format of the compressed package must be tar. The related VPN files are certificates (ca.crt and client.crt), key (client.key), and the configuration file (vpn.cnf) of the VPN client.

The following table lists the directories of the OpenVPN certificates, the key and the configuration file:

VPN File	Description	Unified Directories
ca.crt	CA certificate	/config/openvpn/keys/ca.crt
client.crt	Client certificate	/config/openvpn/keys/client.crt
client.key	Private key of the client	/config/openvpn/keys/client.key

Proxy Server

Introduction

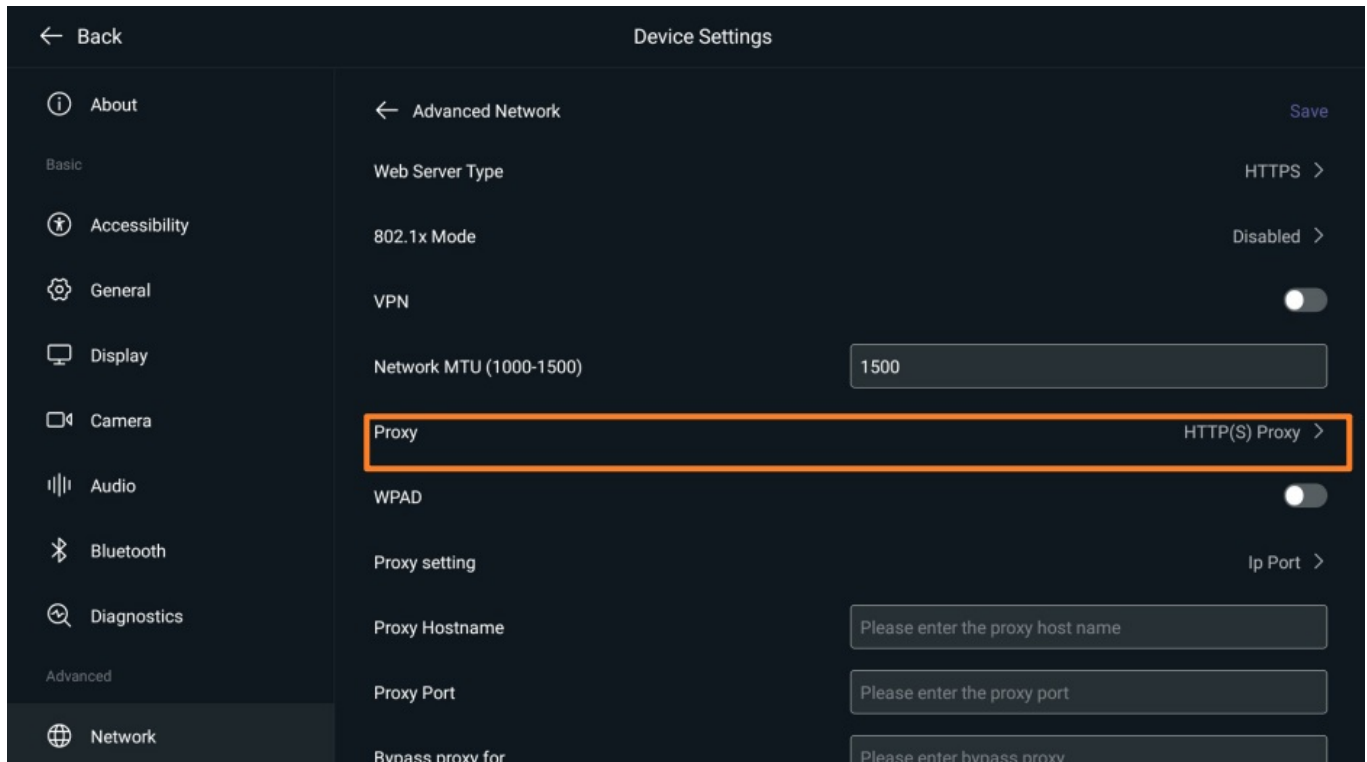
You can configure your network to use proxy servers.

Proxy Server Configuration

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Proxy** (default password: 0000).

2. Configure **Disable/Global Proxy (Manual)/HTTP(S) Proxy** in **Proxy**



Configure via Web User Interface

1. Go to **Network > Proxy** in the web user interface.

2. Select **Disable/Global Proxy/HTTP(S) Proxy** in **Proxy** and click **Confirm**.

The screenshot shows the Yealink MeetingBar A20 web interface. On the left sidebar, the 'Network' menu is expanded, and the 'Proxy' option is highlighted with an orange box and a circled '2'. The 'Proxy' configuration page is displayed, showing various settings. The 'Proxy' dropdown is set to 'Global Proxy'. The 'Proxy Type' is set to 'Socks5'. The 'Proxy Hostname' field is empty. The 'Proxy Port' field is empty. The 'Bypass Proxy For' field is empty. The 'Domain Name For Testing' field is set to 'https://www.google.com'. The 'Enable Authentication' toggle is turned off. At the bottom right, there are 'Confirm' and 'Cancel' buttons.

Auto Provisioning

Parameter	Description	Optional Value
static.network.proxy.mode	It enables or disables the proxy server.	0: Disabled 1: Global proxy. You can manually configure the proxy server information. 2: HTTP(S) proxy. You can obtain proxy server information through PAC file. Default: 2
static.network.proxy.type	It configures the proxy type.	0: SOCKS5 1: HTTP CONNECT Default: 1
static.network.proxy.hostname	It configures the IP address or domain name of the proxy server.	String within 99 characters. Null by default.
static.network.proxy.port	It configures the port of the proxy server.	Integer from 1 to 65535. Null by default.

static.network.proxy.bypass_address	It configures the host name or IP address that does not apply to the proxy server to access.	URL within 511 characters. Null by default. Multiple host names or IP addresses are separated by commas.
static.network.proxy.test_address	After connecting to the proxy server, the phones try to send a network request to the specified URL. If the URL cannot be accessed, the phone fails to connect to the proxy server.	URL within 511 characters.
static.network.proxy.enable	It enables or disables the proxy server authentication.	0: Disabled 1: Enabled Default: 0
static.network.proxy.username	It configures the proxy server authentication account, which is consistent with the server information.	String within 256 characters.
static.network.proxy.password	It configures the proxy server authentication password, which is consistent with the server information.	String within 256 characters.

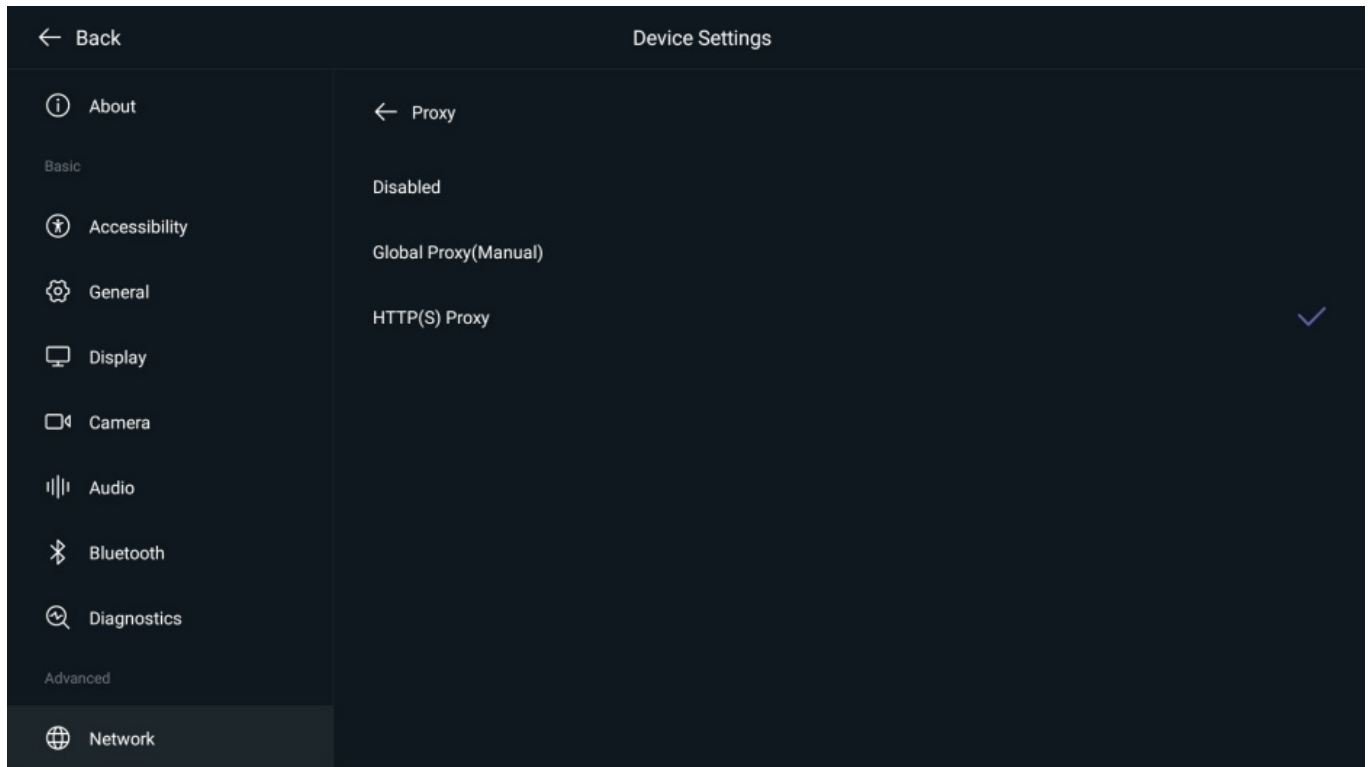
HTTP(S) Proxy

You can obtain proxy server information through PAC file.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Network** (default password: 0000).

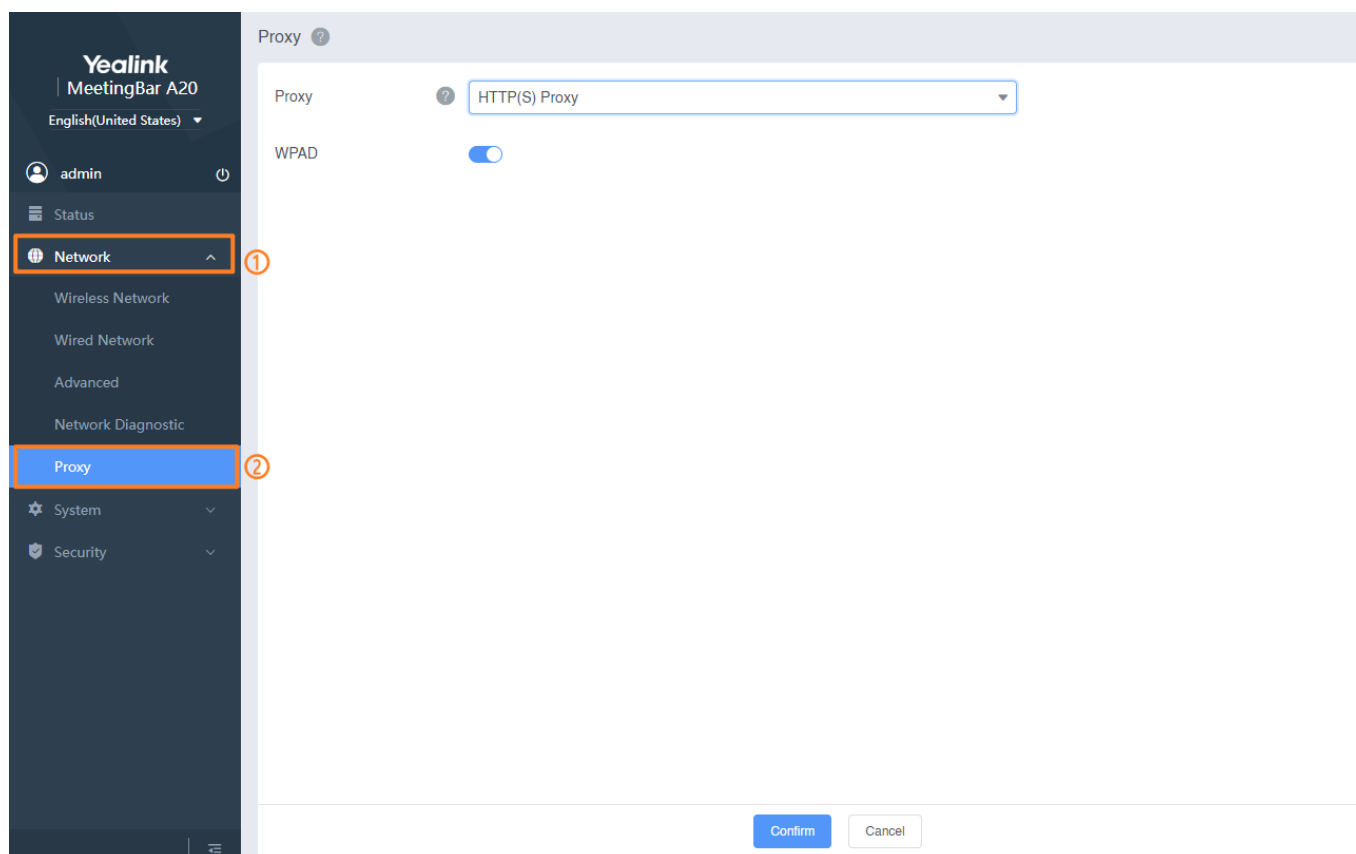
2. Enter **Advanced Network > Proxy** of the MeetingBar AX0 and CTP18 respectively to select **HTTP(S) Proxy**.



Configure via Web User Interface

1. Go to **Network > Proxy** on the web user interface.

2. Configure **HTTP(S) Proxy** and click **Confirm**.



Parameter	Description
WPAD	Configure the proxy type. - SOCKS5 : The proxy server adopts the SOCKS5 protocol, supports TCP/UDP protocol, and supports various authentication mechanisms and other protocols. - HTTP Connect : Mainly to proxy browsers to access pages.
Proxy Configuration	Configure proxy mode. - IP Port - PAC address: Manually configure the URL of the PAC. - PAC File: Upload the PAC file directly.
Proxy Address	Configure the domain name or the IP address of the proxy server.
Port Number	Configure the port of the proxy server.
Bypass Proxy For	The configuration does not apply to the proxy's hostname or IP. Multiple host names are supported, and the host names are separated by commas.

PAC Address	<p>Configure the URL where the PAC file is placed, and the device obtains the PAC file through autop.</p> <div> NOTE Proxy settings need to be configured when self-configuring as a PAC path. </div>
Import PAC file	<p>Upload the PAC file locally.</p> <div> NOTE It needs to be configured when the proxy setting self-configuration is PAC File. </div>

Auto Provisioning

Parameter	Description	Optional Value
static.network.proxy.mode	It enables or disables the proxy server.	0: Disabled 1: Global proxy. You can manually configure the proxy server information. 2: HTTP(S) proxy. You can obtain proxy server information through the PAC file Default: 2
static.network.proxy.wpad	Enable or disable WPAD to obtain PAC files dynamically.	0: Disabled 1: Enabled
static.network.proxy.http.set_from	Configure proxy mode.	0-IP Port, manually enter the proxy server' s IP address and port number. 1-PAC URL, manually configure the PAC URL. 2-PAC File, directly upload the PAC file.
static.network.proxy.hostname	Configure the domain name or the IP address of the proxy server.	String within 99 characters.
static.network.proxy.port	Configure the port proxy server' s port	Integer from 1 to 65535. Null by default.
static.network.proxy.bypass_address	It configures the host name or IP address that does not apply to the proxy server to access.	URL within 511 characters. Multiple host names or IP addresses are separated by commas.
static.network.proxy.pac.url	Configure the URL where the PAC file is placed, and the device obtains the PAC file through autop.	URL String within 511 characters.

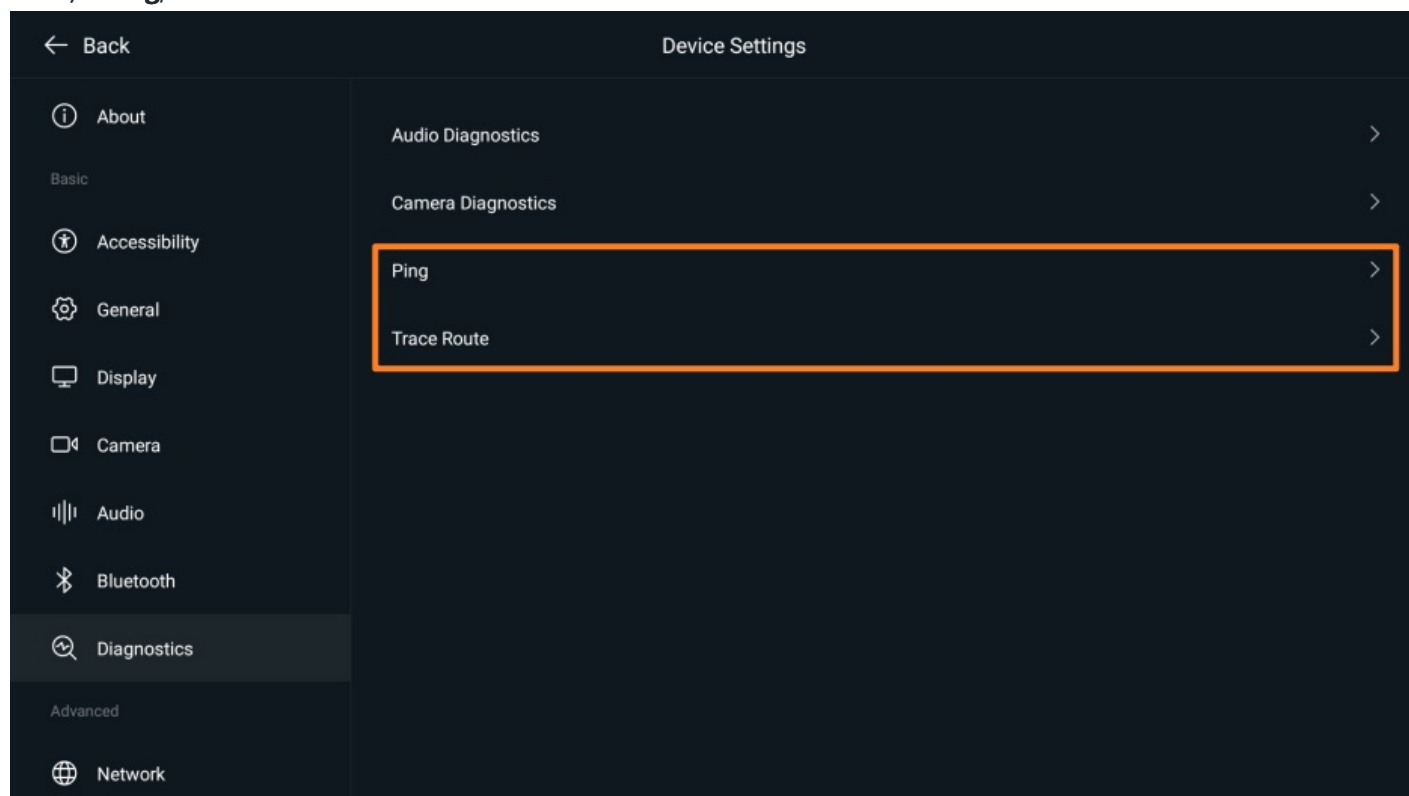
Network Diagnostics

Introduction

The wrong network may result in the inaccessibility of your system and poor network performance. You can use the ping or traceroute to troubleshoot network connectivity problems. The Ping method can check whether the system can be connected to the IP address of the remote device. You can use the traceroute method to diagnose the network. If the test is successful, the system lists the hops between the system and the IP address you entered. You can check whether the congestion happens by viewing the time cost among the hops.

Configure via Device Interface

On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Diagnostics** (default password: 0000) > **Ping/Trace Route**.

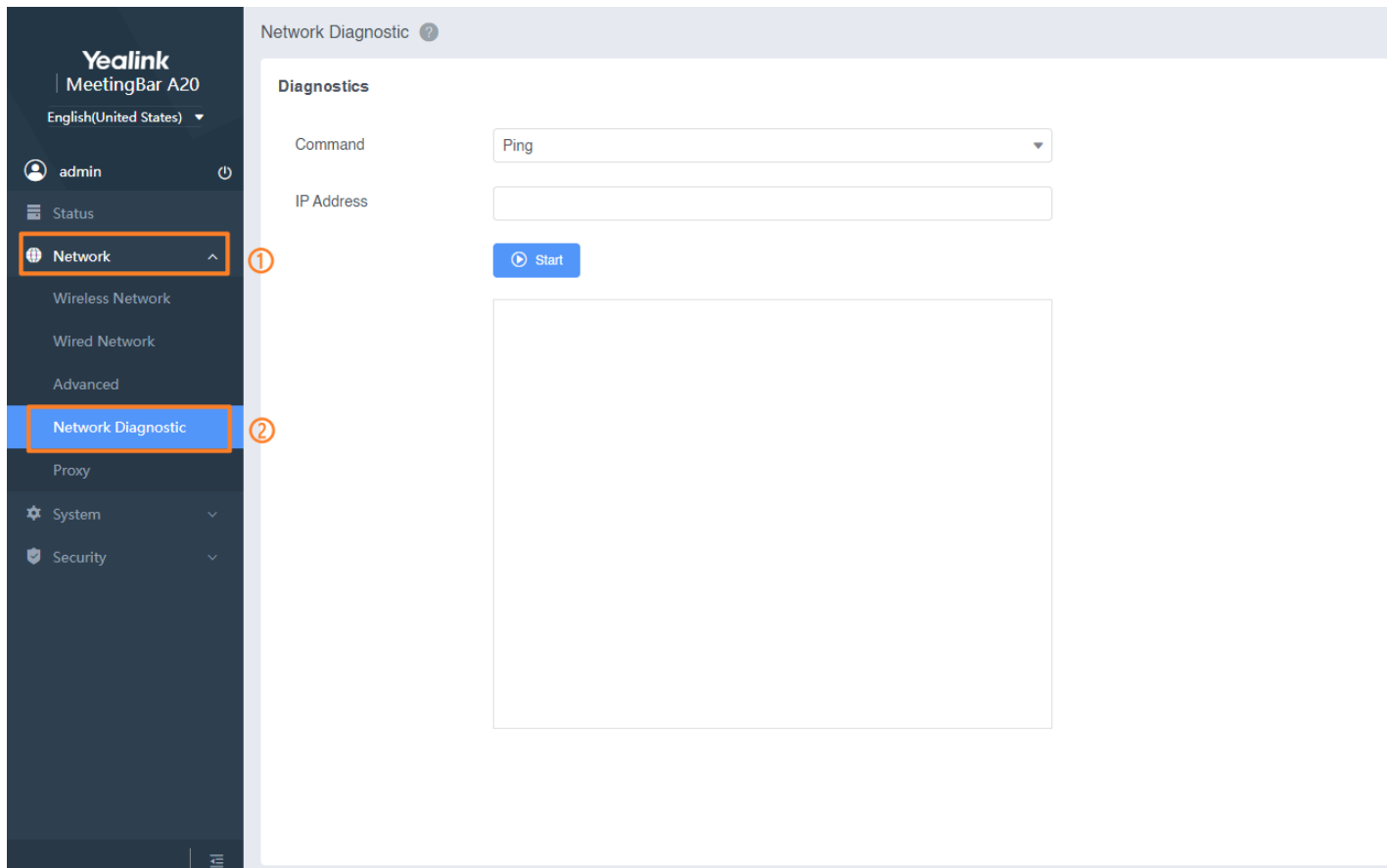


Configure via Web User Interface

1. Go to **Network > Network Diagnostic** on the web user interface.
2. Select **Ping** or **Trace Route** to diagnose the network.
3. Fill in the address that needs to be pinged or tracked in the **IP Address**.
4. Click **Start** to ping or trace and **Stop** for a while.

NOTE

If you select Ping in the command and the packet loss rate is 0%, the network is normal.



Audio & Video

Audio Input/Out

Introduction

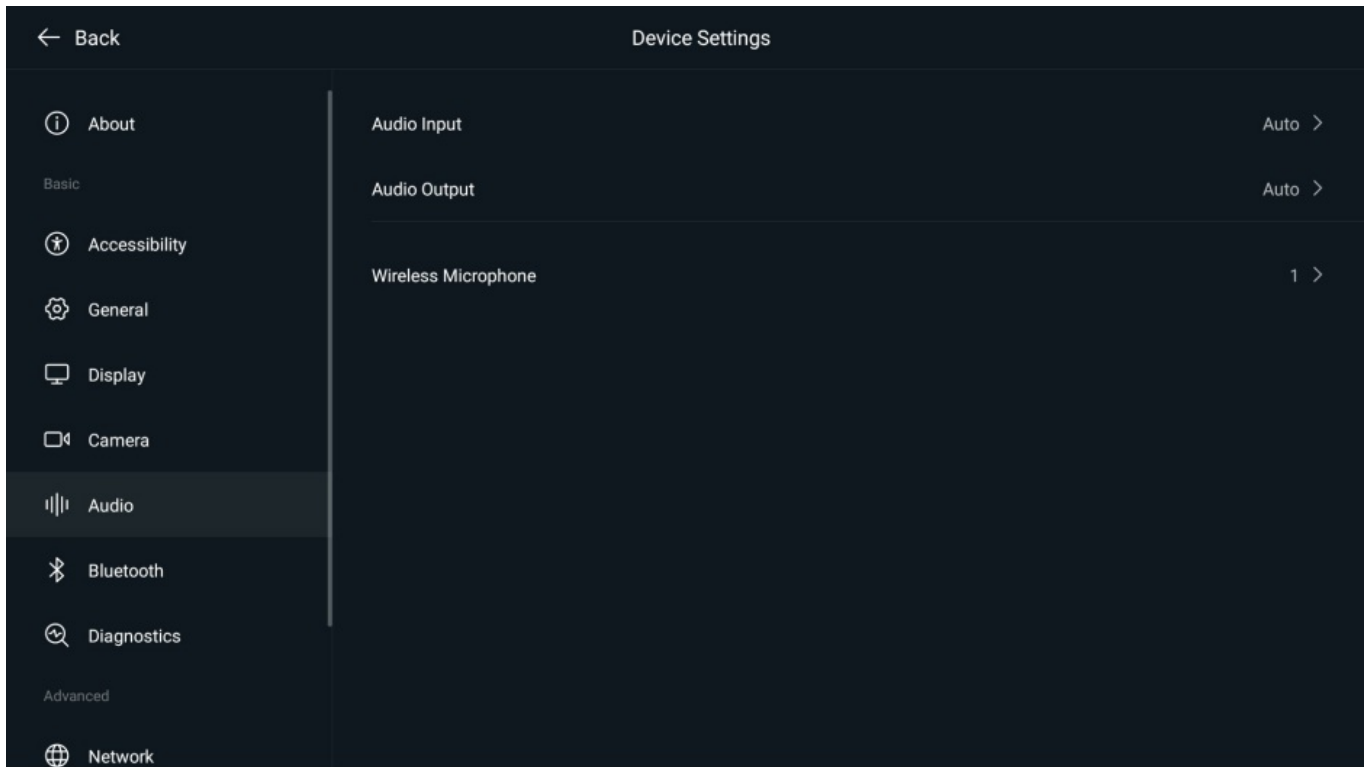
Configure the audio input and output devices used by MeetingBar AX0 and related parameters.

Audio Input

Configure via Device Interface

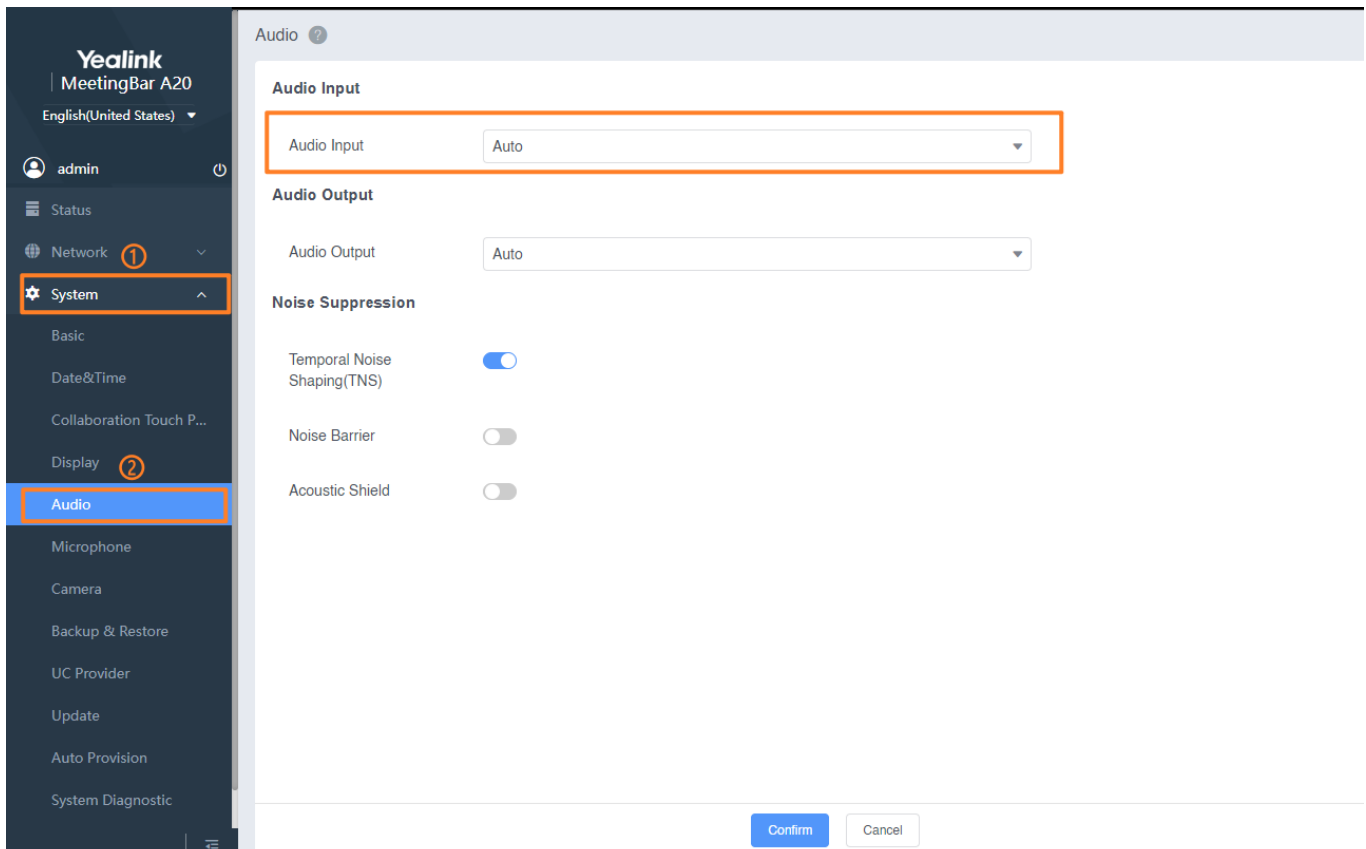
1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Audio Input Device**.

2. Configure the audio input device for the system.



Configure via Web User Interface

1. Go to **Settings > Audio** on the web user interface.
2. Configure **Audio Input** for the system and click **Confirm**.



Parameter	Description
Audio input device	<p>Configure the audio input device for the system.</p> <ul style="list-style-type: none"> - Auto: Use the audio input device with the highest priority. Priority order: VCM38 > VCM35 > VCM34 > VCM36-W > CPW90 > Built-in microphone > Line In. - Built-in microphone: Use the device's built-in microphone. - VCM38/VCM35/VCM34/VCM36-W/CPW90: After connecting the microphone to the endpoint, the corresponding microphone option will appear. For example, when the endpoint is connected to VCM35, the VCM35 option will appear. - Line in: A line in the device connected to the Line In port of the device. This option will appear after the MeetingBar A10/A30 is connected to the device through the Line In port, and the MeetingBar A20 has no Line In port.
Audio line in volume	<p>Configure the volume of the line input device.</p> <div> <p>NOTE</p> <p>Required when the audio input device is set to Line in. The default value of 0 means that the default volume is used. The set value indicates that the volume is subtracted or added to the default volume.</p> </div>

Auto Provisioning

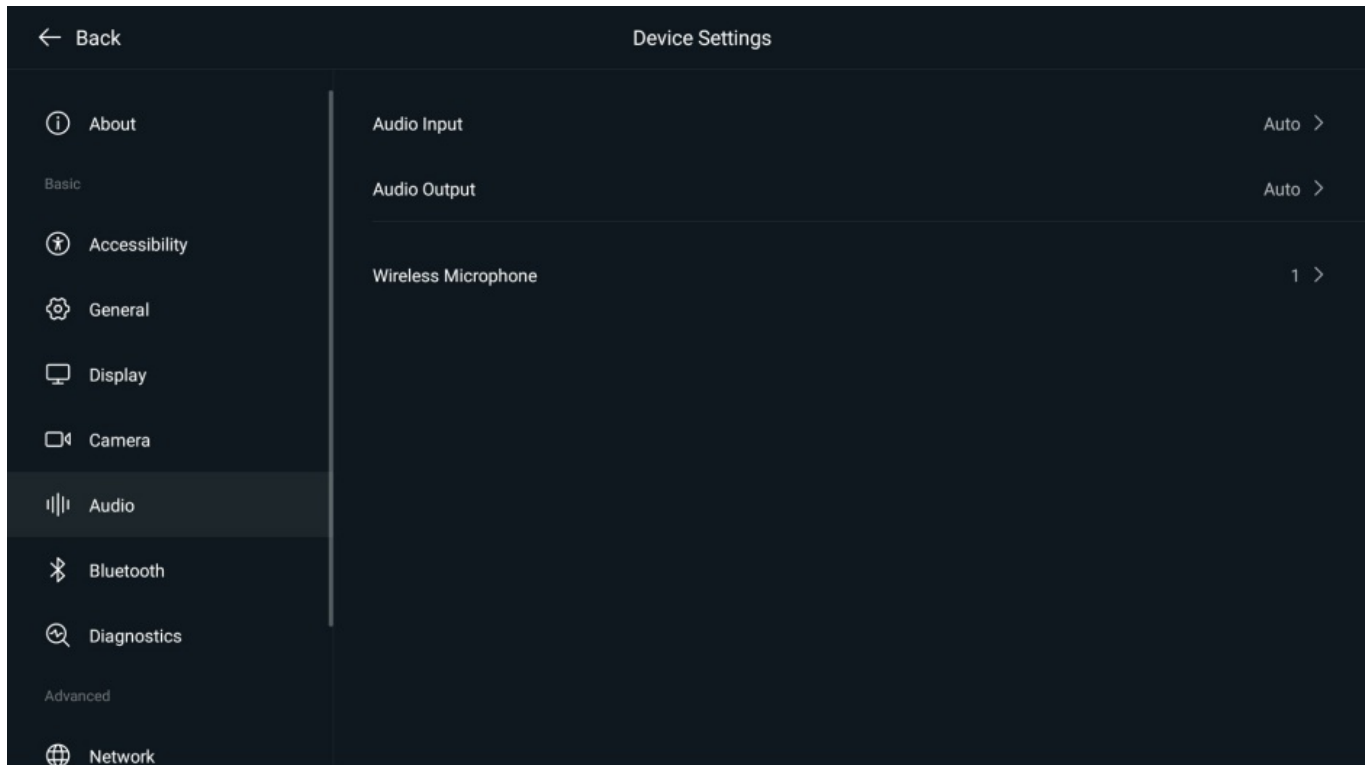
Parameter	Description	Optional Value
audio.active mic	Configure the audio input device for the system.	<p>0: Auto. Priority order: Built-in microphone > line in.</p> <p>4: Built-in microphone.</p> <p>5: Line in.</p>
audio.line_in_vol	<p>Configure the volume of the line input device.</p> <div> <p>NOTE</p> <p>Required when the audio input device is set to Line in. The default value of 0 means that the default volume is used. The set value indicates that the volume is subtracted or added to the default volume.</p> </div>	-50-50

Audio Output

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Audio output Device**.

2. Configure the audio output device for the system.



Configure via Web User Interface

1. Go to **Settings > Audio** on the web user interface.

2. Configure **Audio output** for the system and click **Confirm**.

The screenshot shows the Yealink MeetingBar A20 configuration interface. On the left sidebar, the 'System' menu is expanded, and 'Audio' is selected. The main panel displays the 'Audio' settings. Under the 'Audio Output' section, the 'Audio Output' dropdown menu is set to 'Auto' and is highlighted with an orange box. Below this, the 'Noise Suppression' section shows three settings: 'Temporal Noise Shaping(TNS)' is enabled (toggle on), 'Noise Barrier' is disabled (toggle off), and 'Acoustic Shield' is disabled (toggle off). At the bottom right of the panel are 'Confirm' and 'Cancel' buttons.

Parameter	Description
Audio output device	<p>Configure the audio output device for the system.</p> <p>The supported types are as follows:</p> <ul style="list-style-type: none"> - Auto: Use the audio input device with the highest priority. Priority order: Built-in speaker > Line out. - Built-in speaker: Use the device's built-in speaker. - Line out: A line out device connected to the Line out port of the device.
Audio Line out volume	<p>Configure the volume of the line out device.</p> <div> <p>NOTE</p> <p>Required when the audio input device is set to Line out. The default value of 0 means that the default volume is used. The set value indicates that the volume is subtracted or added to the default volume.</p> </div>

Auto Provisioning

Parameter	Description	Optional Value
-----------	-------------	----------------

audio.output_type	Configure the audio output to be used by the device.	0: Auto. Priority order: Built-in speaker > Line out 3: Line out 7: Built-in speaker
audio.line_out_vol	Configure the volume of line out device. <div> <i>NOTE</i> Required when the audio input device is set to Line out. The default value of 0 means that the default volume is used. The set value indicates that the volume is subtracted or added to the default volume. </div>	-50-50

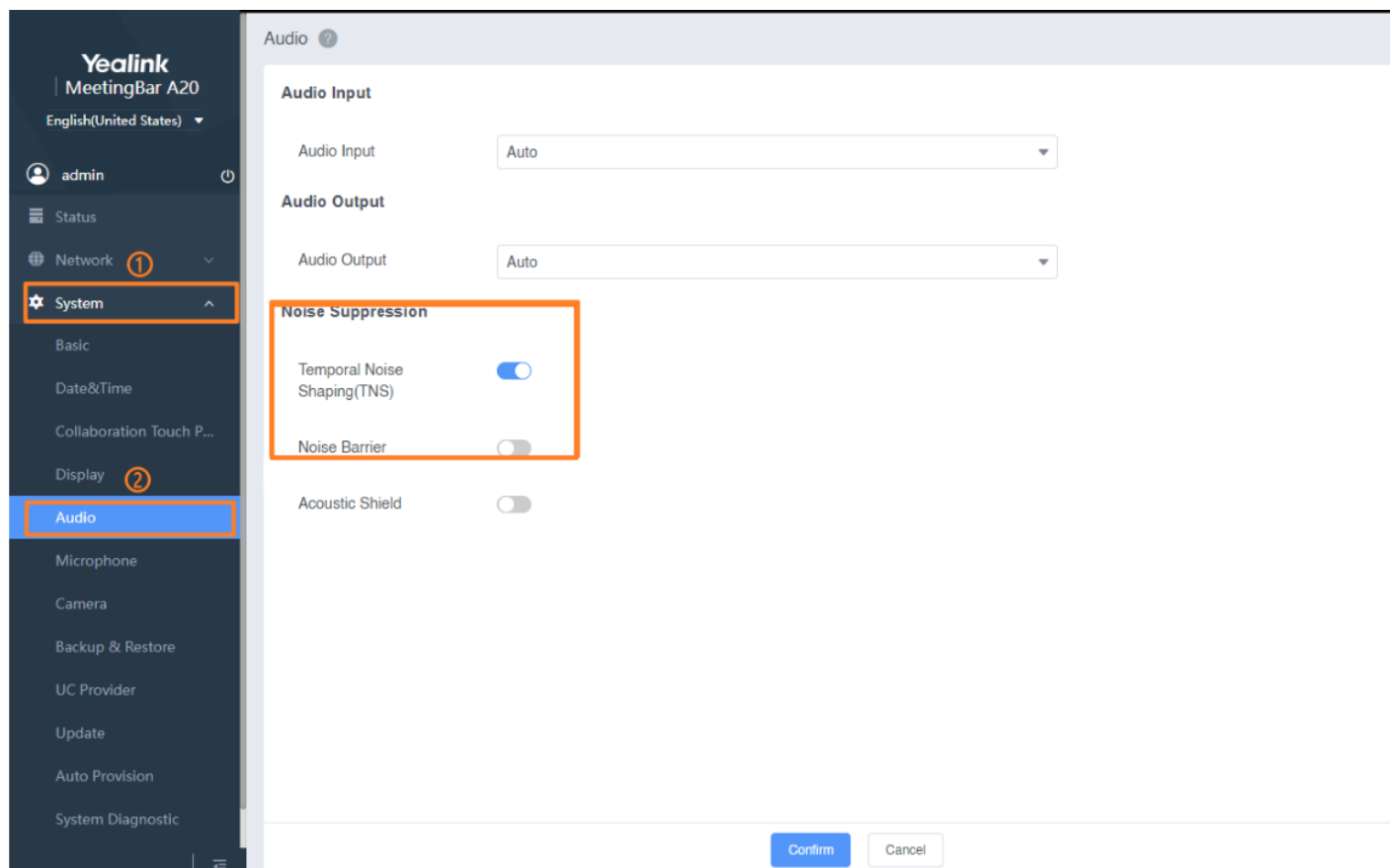
Noise Suppression Configuration

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.

Configure via Web User Interface

1. Go to **Settings > Audio** on the web user interface.
2. Enable/disable **Temporal Noise Shaping(TNS)/Noise Barrier** and click **Confirm**.



Auto Provisioning

Parameter	Description	Optional Value
voice.tns.enable	It enables or disables the Transient Noise Suppressor (TNS).	0: Off 1: On, it can reduce the noise volume temporarily and block the noise in the voice. Default: 1
voice.ans_nb.enable	It enables or disables the noise barrier feature.	0: Off. 1: On, it can block the noise when there is no speech in a call. Default: 0

Acoustic Shield

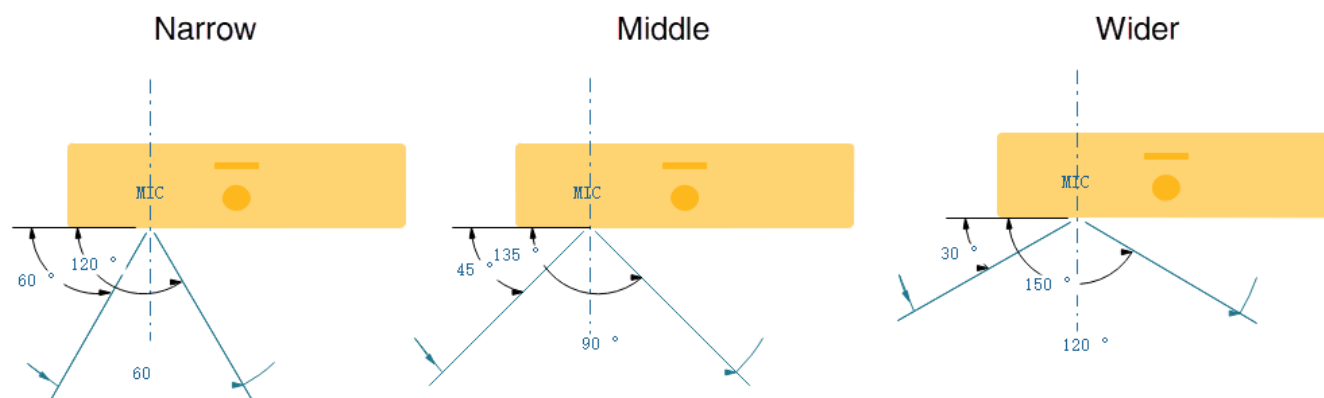
In an open meeting scenario, the sound pickup device may pick up the surrounding environment noise during the meeting since there is no physical barrier between the meeting place and the outside, resulting in a bad experience. In this case, you can use this feature to adjust the sound pickup range, and the microphone will only pick up audio signals within the set range to reduce the interference caused by noise in the meeting. The Acoustic Shield feature does not provide a preview of the effect. If you need to verify the setting effect, you can initiate a meeting and verify it remotely.

The MeetingBar A20/A30 version 133.321.0.1 and later, MeetingBar A10 version 278.321.0.20 and later support the setting of sound enclosures. Please refer to the [release note](#) and download the latest firmware version for detailed instructions.

For the operation video, please refer to [Acoustic Shield](#).

Configure via Web User Interface

1. Go to **Settings > Audio** on the web user interface.
2. Enable/disable **Acoustic Shield** to set **Acoustic Shield Sensitivity**.
3. Configure the **Acoustic Shield Sensitivity** by selecting either **Narrow**, **Medium**, or **Wide**, which correspond to picking angles of 60°, 90°, and 120° respectively. When the Acoustic Shield Sensitivity is set to Narrow (60°), the microphone picks up audio signals within the smallest range. Disabling the noise suppression feature allows the microphone to pick up audio signals within the widest range.



Auto Provisioning

Parameter	Description	Option Value
features.acoustic_shield.enable	Disable or enable Acoustic Shield.	0: Disable 1: Enable
features.acoustic_shield.degree	Configure Acoustic Shield degree.	1: Narrow 2: Middle 3: Wider

FAQ

[How does MeetingBar A20/A30 export audio diagnostic files?](#)

[How do I troubleshoot a MeetingBar A20/A30 microphone \(VCM34/VCM38\) problem?](#)

Camera


Introduction

You can customize the camera configuration: camera mode, white balance, exposure, graphics, subject boundary (video wall), adjust the camera pan direction, and reset the camera.


CTP18, VCR11, and VCR20 can be used to operate MeetingBar A20/A30, while CTP18 and VCR11 can be used to operate MeetingBar A10.

Camera Control

Configure via Device Interface

On the CTP18 or with the remote control, go to  > **Camera Control**.

Configure via Web User Interface

1. On the Meetingbar interface, go to  > **Settings** > **Debug** (default password: 0000).
2. Enable the **Web Remote Screen Capture**.
3. Go to **Device Control** on the web user interface.

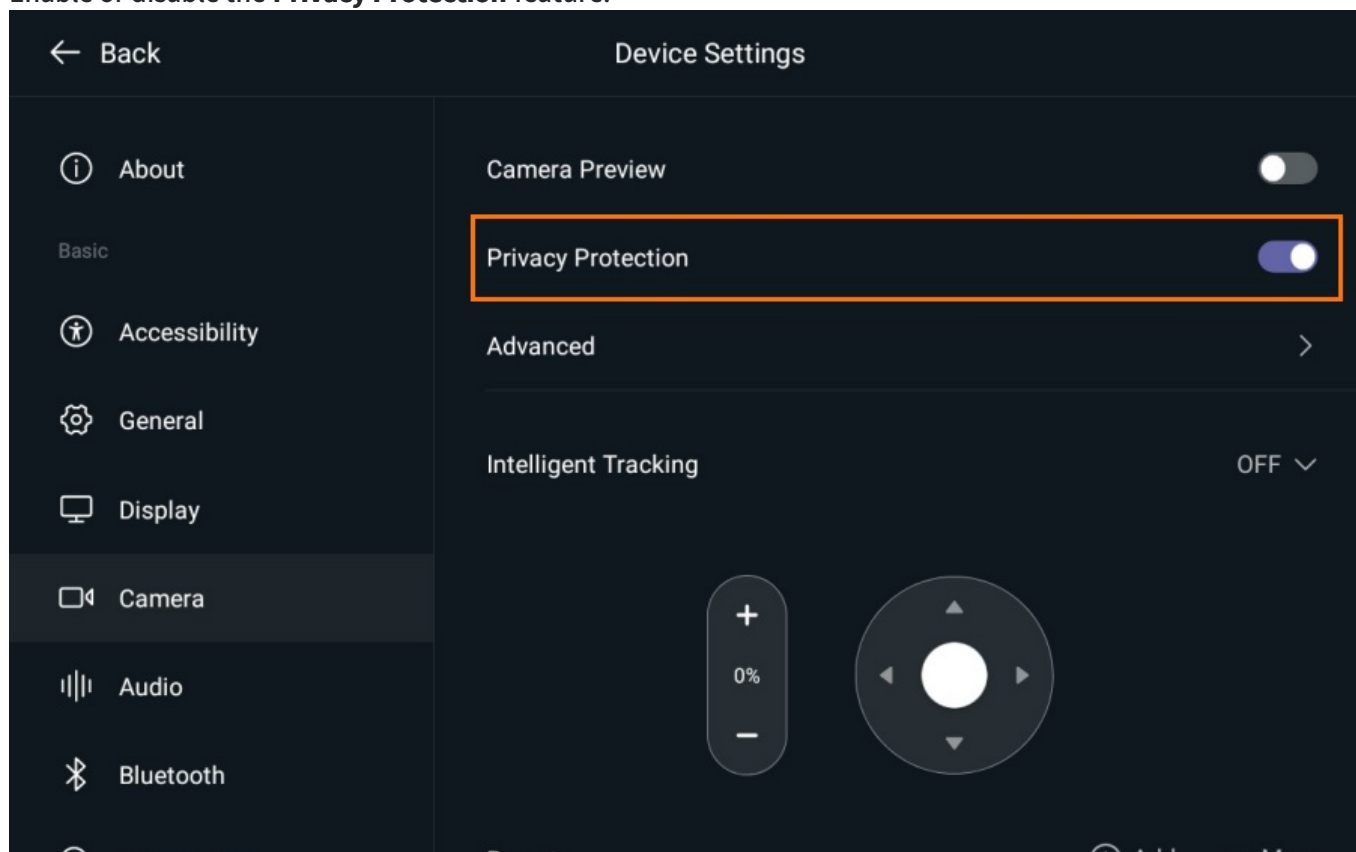
Privacy Protection

After enabling it, the camera privacy cover will automatically close when not in a meeting or without camera control.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More** > **Settings** > **Device Settings** > **Camera** (default password: 0000).

2. Enable or disable the **Privacy Protection** feature.



Parameter	Description
Screen Preview	Enable screen preview; the display will show the preview screen.
Camera	Configure the camera's Intelligent Tracking mode. The camera cannot be adjusted manually when Intelligent Tracking is turned on. For more information, please refer to Camera Controls .
Intelligent Tracking	Choose the camera preset you have set. For more information, please refer to Camera Preset .

Camera Mode

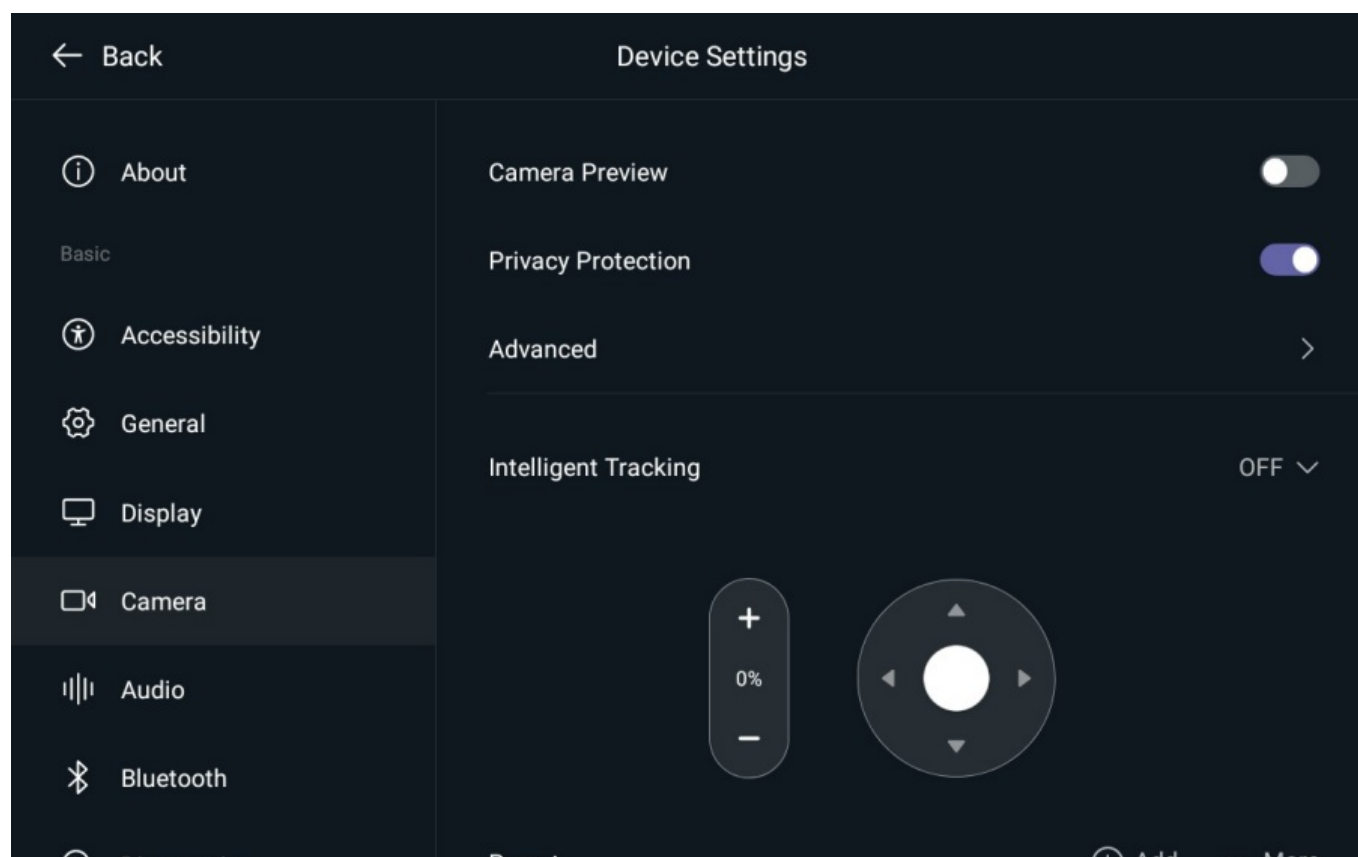
Configure via Device Interface

NOTE

When using the CTP18 to Configure the Tracking Feature in the idle state, it prompts "Please turn on the camera first". Go to **More > Settings > Device Settings > Camera** to enable **Camera Preview**.

1. Do one of the following:
 - Use the remote control, go to **More > Settings > Device Settings > Camera Settings**.
 - On the CTP18, go to **More > Settings > Device Settings > Camera Settings > Camera**.

2. Configure **Intelligent Feature**.



Configure via Web User Interface

1. Go to **System > Camera** on the web user interface.

2. Configure Camera and click **Confirm**.

The screenshot shows the Yealink MeetingBar A20 web interface. On the left sidebar, the 'System' menu is expanded, and the 'Camera' option is highlighted with an orange box. The main content area is titled 'Camera' and contains several configuration sections:

- Camera:** A dropdown menu set to 'MeetingBarA20 Camera' and a text field for 'Camera Name' also containing 'MeetingBarA20 Camera'. This section is highlighted with an orange box.
- Camera Mode:** A dropdown menu set to 'OFF'.
- Exposure:** A dropdown menu set to 'Auto Exposure' and a dropdown menu set to '50Hz'.
- White Balance:** A dropdown menu set to 'Auto'.
- Graphics:** A dropdown menu set to 'Standard', a 'Saturation' slider set to 5 (range 0-10), and a 'Sharpness' slider set to 3 (range 0-6).

At the bottom right of the configuration area are 'Confirm' and 'Cancel' buttons.

Auto Provisioning

Parameter	Description	Optional Value
features.framing_mode.enable	It configures to enable or disable the Tracking Mode.	0: Disabled 1: Enabled Default: 0
features.video_framing.mode	It configures the framing mode of the camera. <div> <i>NOTE</i> It works only when “features.framing_mode.enable” is set to 1 (Enabled). </div>	1: Auto Framing 2: Speaker Tracking 3: Small FoV Mode 6: Smart Garlley: This feature is only available to the Zoom version. 7: Allows setting to Multi-focus Framing or Picture in Picture Mode.

features.multi_focus.type	<p>It configures the camera mode to Multi-focus Framing or Picture in Picture mode.</p> <p>NOTE It works only when “features.video_framing.mode” is set to 7 (Enabled).</p>	<p>0: Multi-focus Framing 1: Picture in Picture Mode</p>
features.video_framing.speed_mode	<p>It configures the tracking speed for the Auto Frame.</p> <p>NOTE It works only when “features.framing_mode.enable” is set to 1 (Enabled) and “features.video_framing.mode” is set to 1 (Auto Framing).</p>	<p>- realtime - quick - normal - slow</p>
features.talkers_tracking_mode	<p>It configures Talkers Tracking Settings and Talkers Tracking Timer.</p> <p>NOTE It works only when features.framing_mode.enable is set to 1 (Enabled) and features.video_framing.mode is set to 2 (Speaker Tracking).</p>	<p>0: Disable the Talkers Tracking Settings. 3: Set the Talkers Tracking Timer for 3s. 5: Set the Talkers Tracking Timer for 5s. 7: Set the Talkers Tracking Timer for 7s.</p>
features.audio_framing.speed_mode	<p>It configures the Speaker Tracking Speed.</p> <p>NOTE It works only when features.framing_mode.enable is set to 1 (Enabled) and features.video_framing.mode is set to 2 (Speaker Tracking).</p>	<p>- quick - normal - slows</p>
features.video_framing.field_of_view	<p>It configures the viewing angle of Small FoV Mode.</p> <p>NOTE It works only if “features.video_framing.mode” is set to 1 (Auto Framing) and features.video_framing.mode is set to 3 (Small FoV Mode).</p>	<p>1: 70° 2: 90° Default: 2</p>

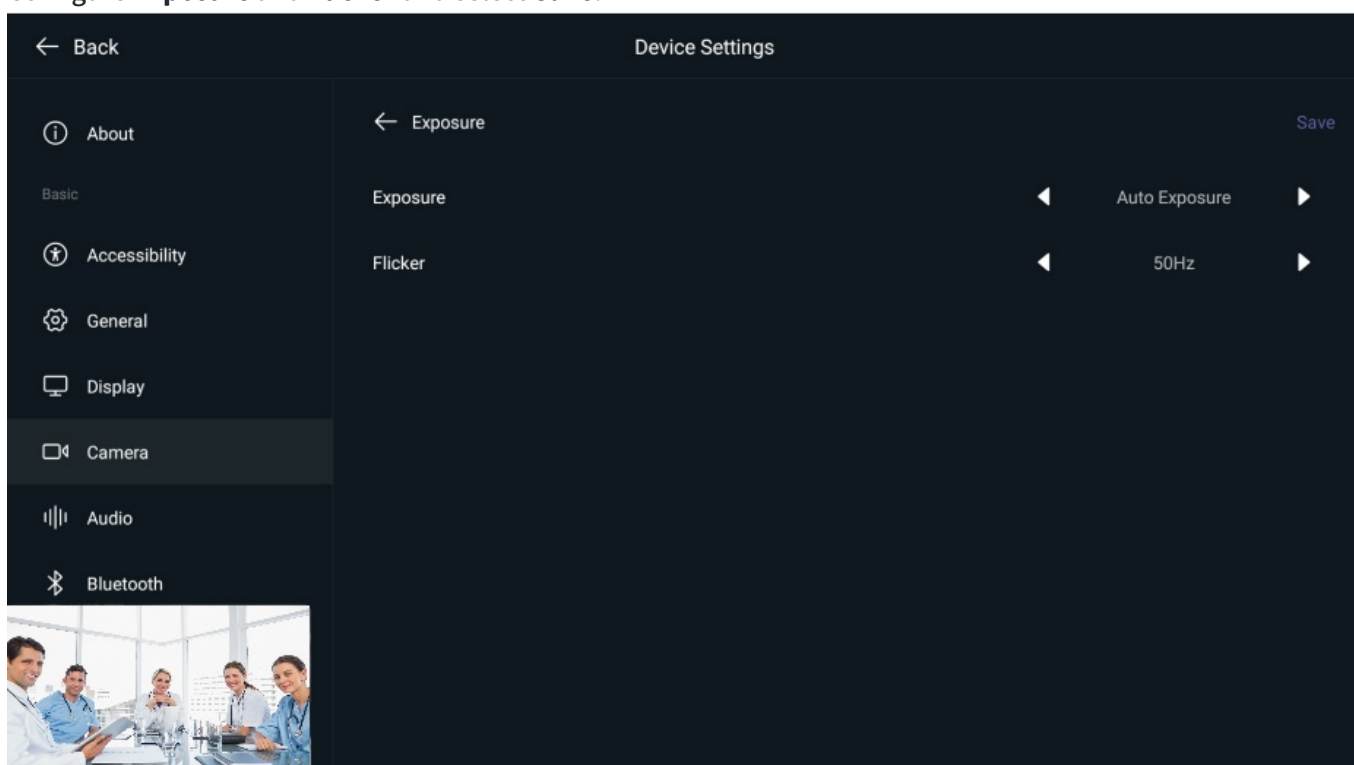
features.video_framing.pip_mode	<p>Set the screen displayed in the small floating window. The small floating window is set to display the panoramic view by default.</p> <div> <p>NOTE</p> <p>It is available when the Intelligent Tracking is set to PiP Mode.</p> </div>	<p>0: Panoramic First 1: Feature First</p>
features.video_framing.pip_position	<p>Set the position where the small floating window in PiP Mode.</p> <div> <p>NOTE</p> <p>It is available when the Intelligent Tracking is set to PIP Mode.</p> </div>	<p>0: Upper Right 1: Lower Right 2: Upper Left 3: Lower Left Default: 0</p>

Exposure

Auto-exposure aims to achieve desired brightness level, or so-called target brightness level in different lighting conditions and scenes, so the videos or images captured are neither too dark nor too bright.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Camera > Advanced > Exposure**.
2. Configure **Exposure** and **Flicker** and select **Save**.



Configure via Web User Interface

1. Go to **System** > **Camera** on the web user interface.
2. Select **Auto** under **Exposure** and click **Confirm**.

The screenshot shows the Yealink MeetingBar A20 web interface. On the left sidebar, 'System' and 'Camera' are highlighted. The main content area is titled 'Camera'. It contains several sections: 'Camera' with a dropdown menu set to 'MeetingBarA20 Camera'; 'Camera Name' with a text field containing 'MeetingBarA20 Camera'; 'Camera Mode' with 'Tracking Mode' set to 'OFF'; 'Exposure' (highlighted with an orange box) with 'Exposure' set to 'Auto Exposure' and 'Flicker' set to '50Hz'; 'White Balance' with 'White Balance Mode' set to 'Auto'; and 'Graphics' with 'Display Mode' set to 'Standard', 'Saturation' at 5 (0-10), and 'Sharpness' at 3 (0-6). At the bottom right are 'Confirm' and 'Cancel' buttons.

Parameter	Description
Exposure	<p>It configures the exposure mode.</p> <ul style="list-style-type: none"> - Auto Exposure: Achieve a desired or target brightness level under different lighting conditions and scenes so that the captured video or image is neither too dark nor too bright. - Manual Exposure: Achieve a combined camera aperture value and shutter speed exposure. - Shutter Priority: The shutter speed needs to be adjusted manually, and then the camera selects the appropriate aperture value. - Brightness Priority: Brightness priority lets the camera's automatic light metering system calculate the exposure value and then automatically determine the shutter value according to the aperture value. <div> <p>NOTE</p> <p>We recommend setting it to Auto Exposure, the camera will automatically adjust the exposure.</p> </div>

Flicker	<p>It configures the value of the camera flicker frequency.</p> <p>The indoor lights powered by a 50Hz or 60Hz power source may produce a flicker in the camera. You can adjust the camera flicker frequency according to your needs.</p> <p>The AC frequency is 50Hz, so choosing a 50Hz shoot light will avoid light flickering.</p> <p>The refresh rate of an ordinary TV display is 60Hz, so you can choose a 60Hz TV display to avoid flickering.</p>
Gain Limit	<p>It adjusts the value of the brightness gain.</p> <p>In poor light, we recommend using a higher gain.</p> <div> <p>NOTE</p> <p>This configuration needs to be set when the exposure mode is configured as Manual Exposure.</p> </div>
Shutter	<p>It configures the value of the shutter.</p> <p>You can not use the high-speed shutter in dark scenes. In this case, you need to increase the aperture value.</p> <div> <p>NOTE</p> <p>This configuration needs to be set when the exposure mode is configured as Shutter Priority.</p> </div>
Brightness	<p>It configures the value of brightness.</p> <div> <p>NOTE</p> <p>This configuration needs to be set when the exposure mode is configured as Brightness Priority.</p> </div>

Auto Provisioning

Parameter	Description	Optional Value
camera.ae_mode	It configures the value of exposure compensation.	0: Auto Exposure 1: Manual Exposure 2: Shutter Priority 4: Brightness Priority
camera.ae_mode.auto_mode.flick	It configures the stroboscopic parameters in auto exposure mode.	0: 50hz 1: 60hz 2: Off

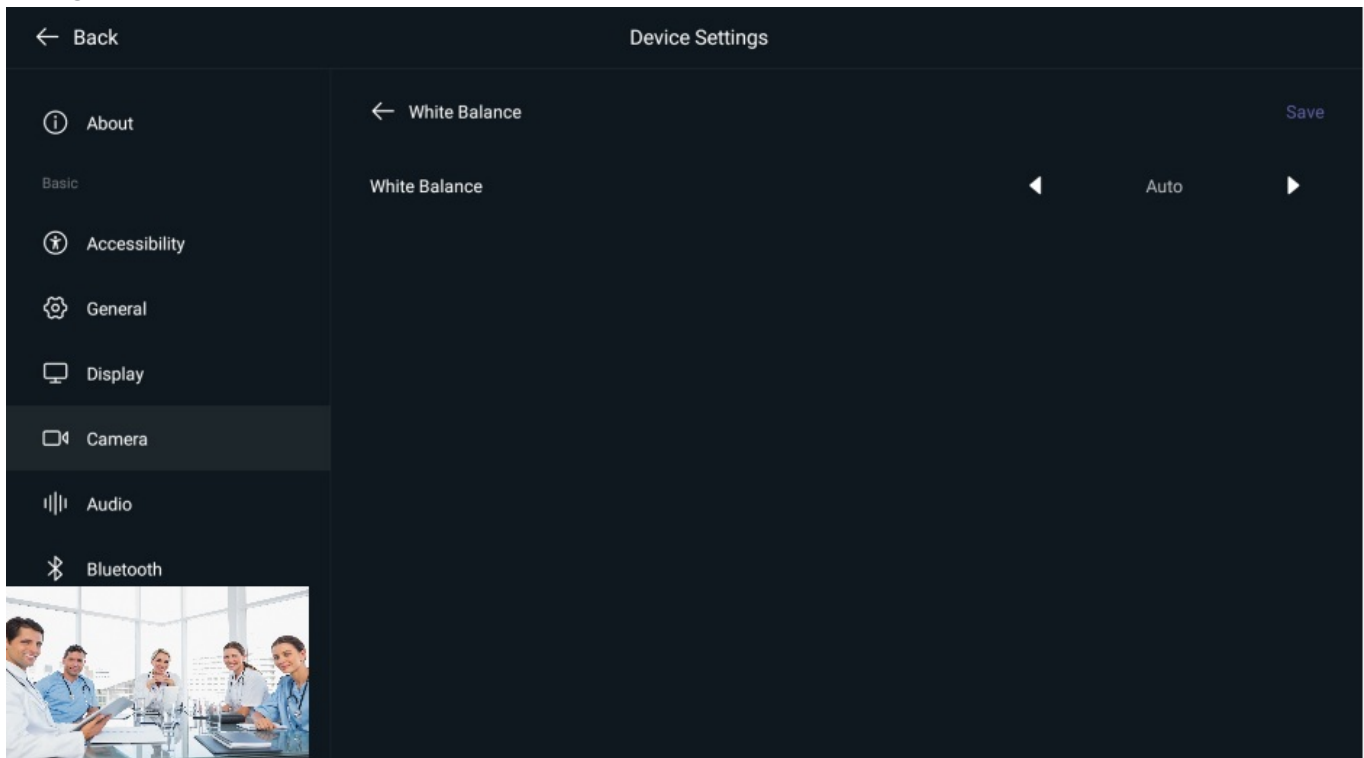
camera.ae_mode.manual_mode .bright	It configures the gain parameters manual exposure mode.	1-15 Default: 1
camera.ae_mode.manual_mode .shutter	It configures the shutter parameter in manual exposure mode.	0-1/60 1-1/90 2-1/1001-15 (default) 3-1/125 4-1/180 5-1/250 6-1/350 7-1/500 8-1/725 9-1/1000 10-1/1500 11-1/2000 12-1/3000 13-1/4000 14-1/6000 15-1/10000
camera.ae_mode.shutter_mode. shutter	It configures the shutter parameter in shutter priority mode.	0-1/60 1-1/90 2-1/100 (default) 3-1/125 4-1/180 5-1/250 6-1/350 7-1/500 8-1/725 9-1/1000 10-1/1500 11-1/2000 12-1/3000 13-1/4000 14-1/6000 15-1/10000
camera.ae_mode.bright_mode. bright	It configures the brightness parameter in brightness priority mode.	1-15 (default:6)

White Balance

The white balance mode is mainly a camera mode set up to adapt to various scenes to make the color temperature of the image captured by the camera normal.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Camera Settings > White Balance Settings**.
2. Configure **White Balance** and select **Save**.



Configure via Web User Interface

1. Go to **System > Camera** on the web user interface.

2. Configure **White Balance Mode** under **White Balance** and click **Confirm**.

The screenshot shows the Yealink MeetingBar A20 web interface. On the left sidebar, the 'System' menu is expanded, and the 'Camera' option is highlighted. The main content area displays the 'Camera' settings page. The 'White Balance' section is highlighted with an orange box, showing 'White Balance Mode' set to 'Auto'. Other settings visible include Tracking Mode (OFF), Exposure (Auto Exposure), Flicker (50Hz), Display Mode (Standard), Saturation (5), Sharpness (3), Noise Reduction (2D) (disabled), and Camera Pan Direction (Normal). At the bottom right, there are 'Confirm' and 'Cancel' buttons.

Auto Provisioning

Parameter	Description	Optional Value
White Balance Setting	It configures the white balance mode of the camera.	<ul style="list-style-type: none"> - Auto: It calculates the best white balance setting based on lighting conditions in the room. We recommend using this setting for most situations. - Incandescent - Fluorescent - Daylight - Cloudy Light - Shade

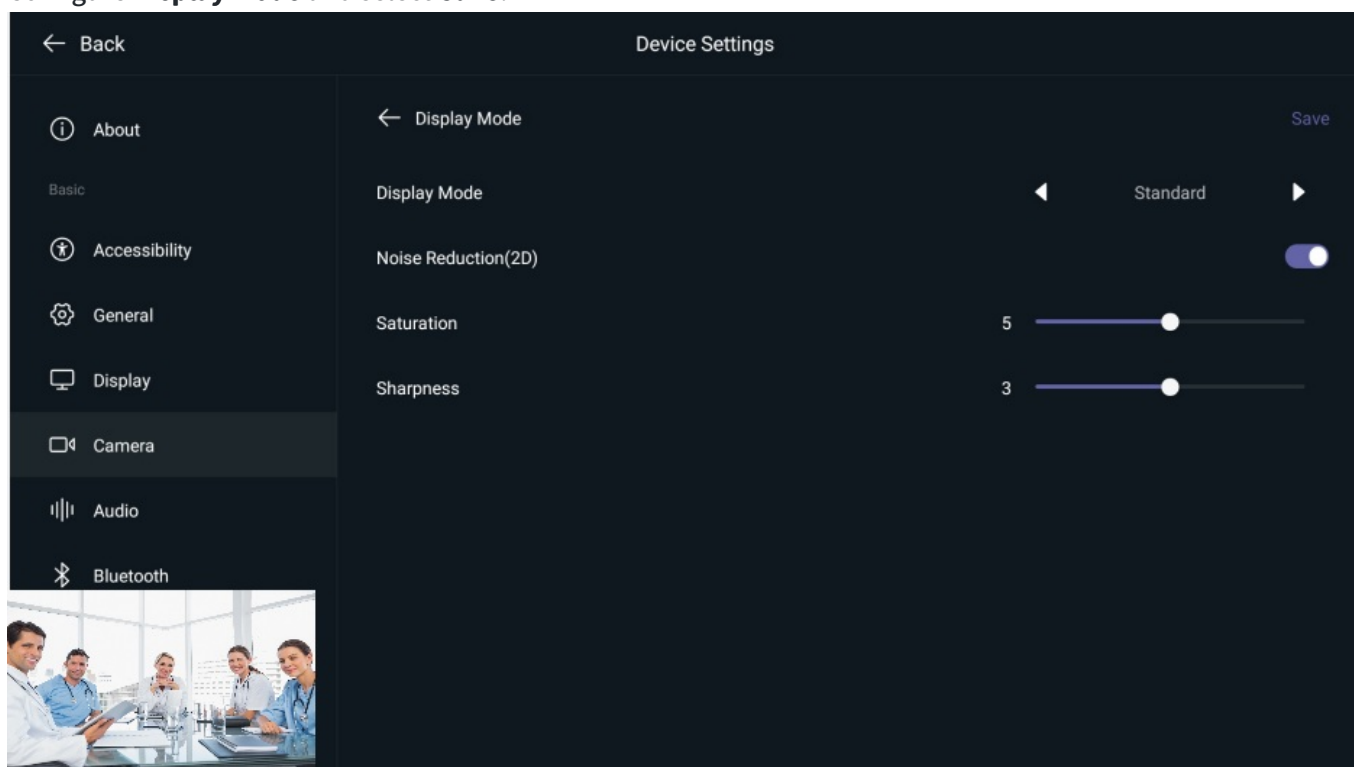
Display Mode

It configures parameters related to the graphics display.

Configure via Device Interface

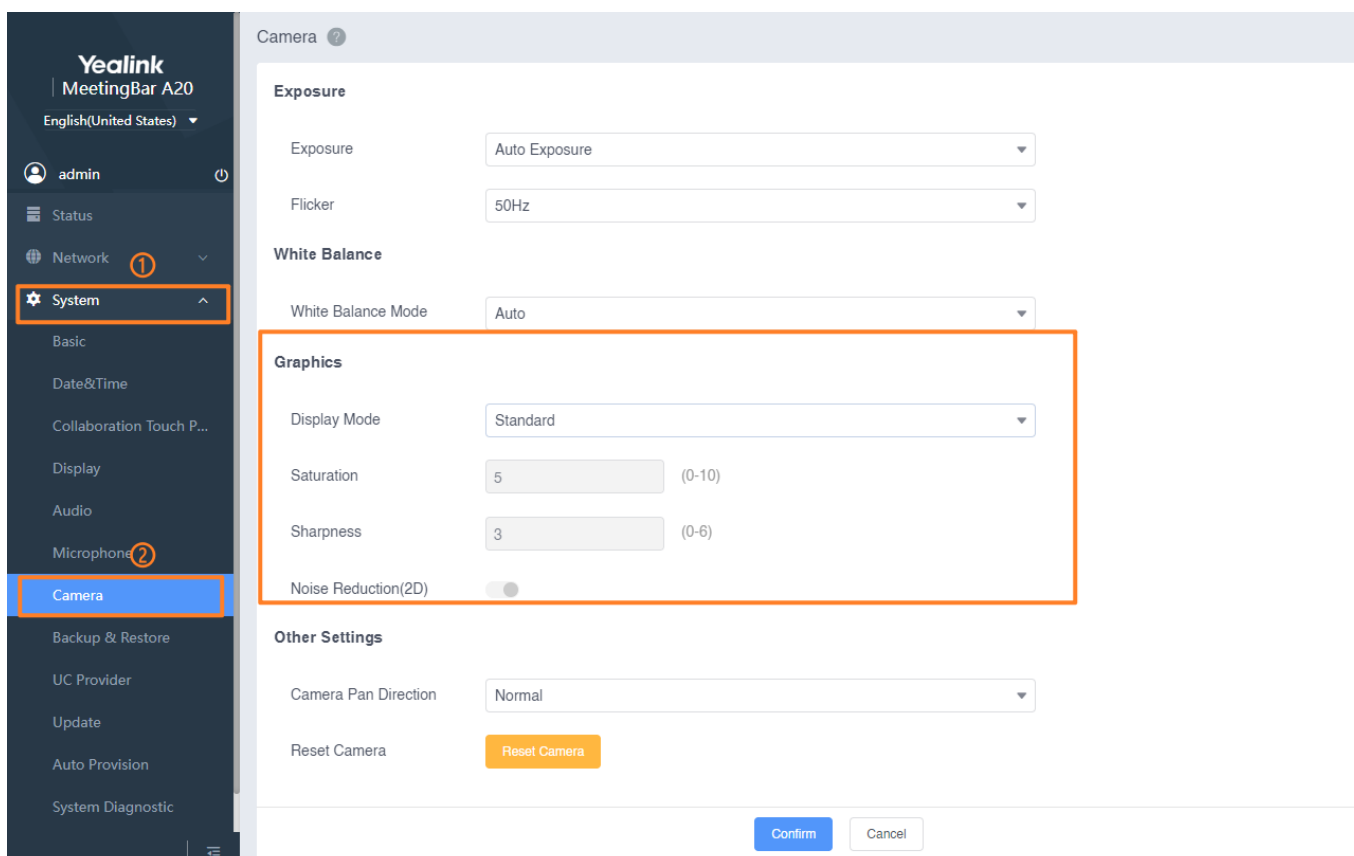
1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Camera > Advanced > Display Mode**.

2. Configure **Display Mode** and select **Save**.



Configure via Web User Interface

1. Go to **System > Camera** on the web user interface.
2. Configure **Graphics** and click **Confirm**.



Auto Provisioning

Parameter	Description	Optional Value
Display Mode (camera.displaymode)	It configures the display mode.	0: High Definition 1: Standard 2: Mild 3: Custom Default: 1
Saturation	It configures the image saturation of the camera. The saturation means the maximum intensity of color in the image.	The value is from 0 to 100. The default value is 50.
Sharpness	It configures the image sharpness of the camera. The sharpness is an indicator that reflects the image plane's definition and the image edge's sharpness. Increasing the sharpness will improve the definition of the image. However, if the sharpness is too high, the image will look distorted and glaring.	The value is from 0 to 6. The default value is 3.
Noise Reduction (2D)	Specify the noise reduction (2D) mode.	- Enable - Disable Default: Enable.

Image-pickup Range (Video Fence)

In some meeting scenarios with glass walls or open spaces in the background, participants reflected on the glass walls or outside the meeting range may be detected. In this case, you can use this feature to adjust the subject boundary (video wall), and the camera will not detect participants beyond the set range. You can now start adjusting the width and depth of the boundary and walk around the room to check if the boundary you have set is as desired. The green square will turn red once you are outside the pickup range. This means that auto framing will not detect a participant in this part of the room as they are outside the configured boundary. AI features like Auto Framing only track members within the range.

Version 133.321.0.1 and later of MeetingBar A20/A30 and version 278.321.0.20 and later of MeetingBar A10 support setting the image-picking range. Please refer to [Release Note](#) and download the latest firmware version.

For the operation video: coming soon.



Configure via Device Interface

NOTE

When using the CTP18 for operation, the screen will automatically display a preview of the image-pickup range's effect. When using the remote control, the screen's bottom-left corner will show the camera view.

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Camera > Advanced > Video Wall**.
2. Configure **Width/Depth**.

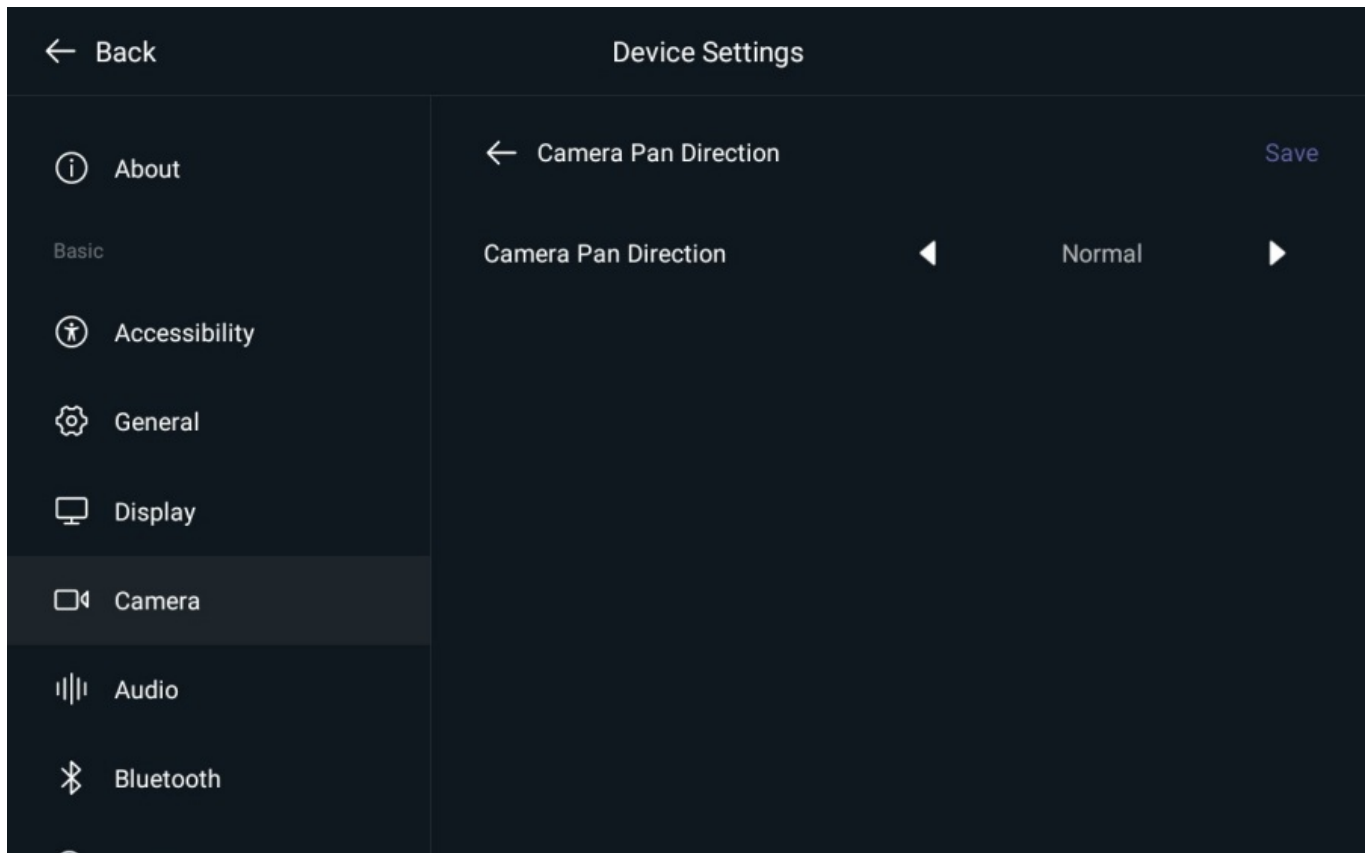
Auto Provisioning

Parameter	Description	Option Value
features.video_fence.width	Configure the width of the Subject Boundary (Video Wall)	An integer from 0 to 20, the default is 20.
features.video_fence.depth	Configure the depth of the Subject Boundary (Video Wall)	An integer from 0 to 20, the default is 20.

Other Settings

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Camera > Advanced**.
2. Configure **Camera Pan Direction/Factory Reset**.



Configure via Web User Interface

1. Go to **System > Camera** on the web user interface.

2. Configure **Camera Pan Direction/Reset Camera** under **Other Settings** and click **Confirm**.

The screenshot shows the Yealink MeetingBar A20 web interface. On the left sidebar, the 'System' menu item is highlighted with an orange box and a circled '1', and the 'Camera' menu item is highlighted with an orange box and a circled '2'. The main content area is titled 'Camera' and contains several sections: 'Exposure' with 'Auto Exposure' and '50Hz' settings; 'White Balance' with 'Auto' mode; 'Graphics' with 'Standard' display mode, 'Saturation' at 5, 'Sharpness' at 3, and 'Noise Reduction(2D)' turned off; and 'Other Settings' where 'Camera Pan Direction' is set to 'Normal' (highlighted with an orange box) and there is a 'Reset Camera' button. At the bottom right, there are 'Confirm' and 'Cancel' buttons.

Parameter	Description
Camera Pan Direction	Configure the pan direction of the camera. - Normal - Reversed Note: When setting the camera to reverse, use the remote control or the CTP18 to adjust the camera to the right, but the camera will turn to the left.
Reset Camera	Restore the camera's settings to factory settings. Note: After resetting, your camera settings will be restored to factory settings.

Auto Provisioning

Parameter	Description	Optional Value
camera.pandirection	Configure the pan direction of the camera.	0: Normal 1: Reversed

FAQ

What should I do if the remote video screen of the MeetingBar A20/A30 is black?

Device Customization

Language

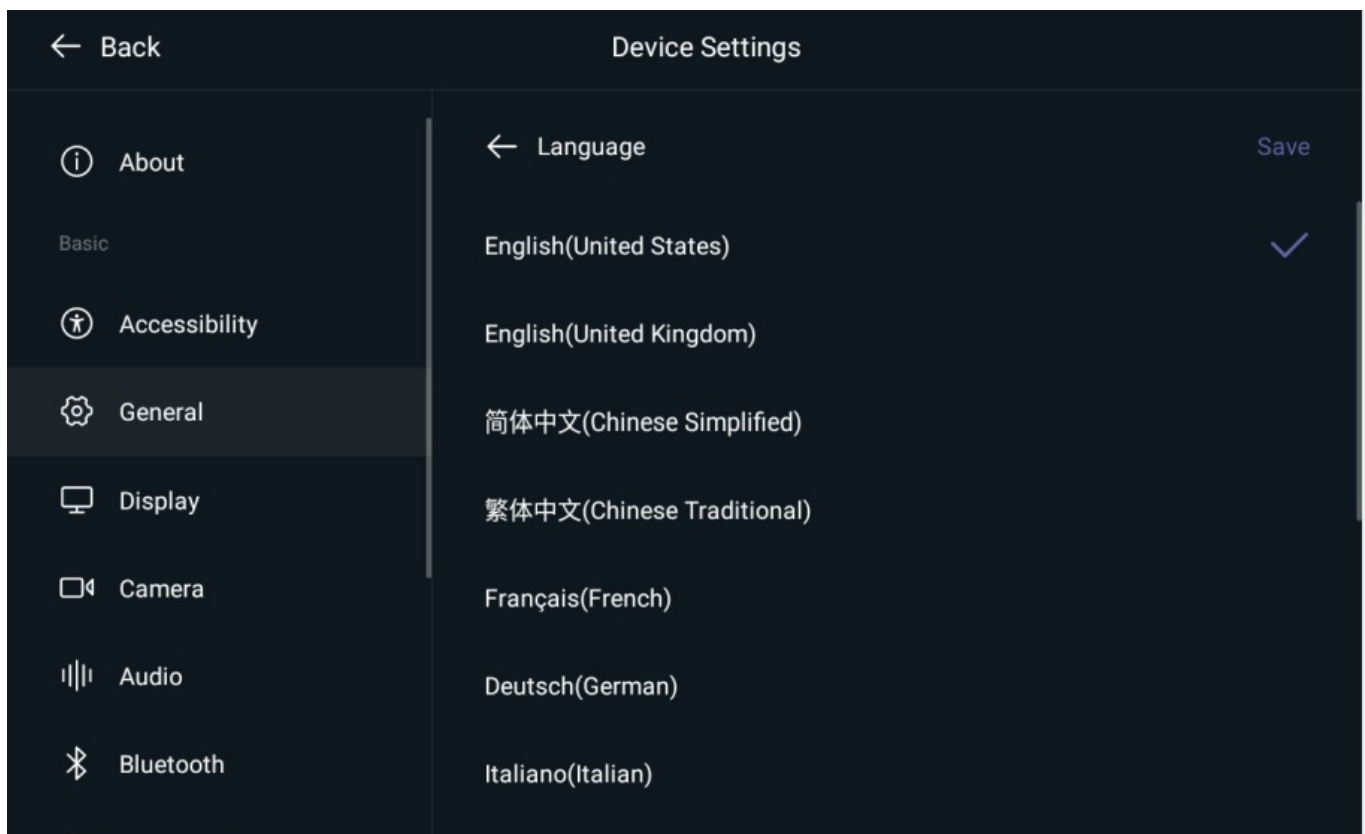
Introduction

Support changing the display language of the device interface or the web interface's display language.

Change Language

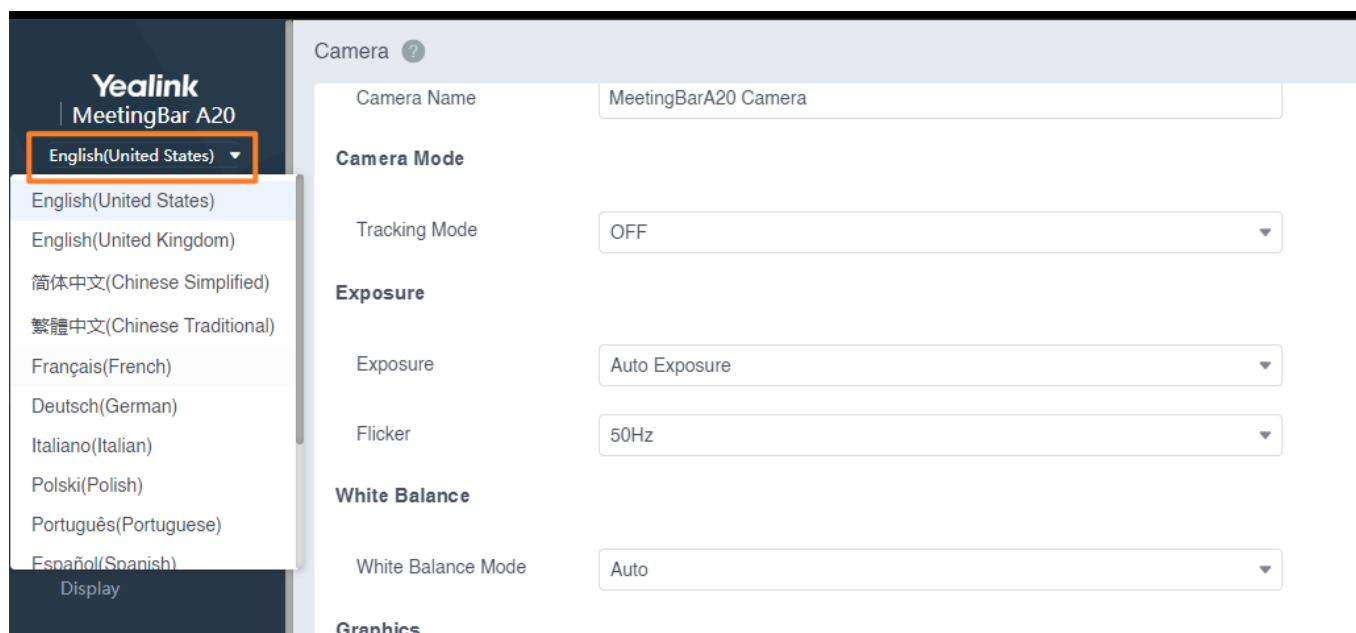
Change Device Interface Language

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > General**.
2. Choose the desired language and select **Save**.



Configure Web Interface Language

1. Click **Language** in the upper-left corner of the web user interface to select a language as required.



Auto Provisioning

Parameter	Description	Optional Value
lang.gui	Configure the language to display on the device.	English (United States) (default)/ English (United Kingdom) / Chinese_S / Chinese_T / French / German / Italian / Polish / Portuguese / Spanish / Turkish / Russian / Netherlands / Japanese / Customize language name.
lang.wui	Configure the language to display on the web user interface.	English (United States) (default)/ English (United Kingdom) / Chinese_S / Chinese_T / French / German / Italian / Polish / Portuguese / Spanish / Turkish / Russian / Japanese / Customize language name.

Customize Language Packs

You can customize the language files displayed on the device or web user interface. Please contact Yealink technical support to get the language pack template.

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.

Customize Device Language File

Available languages depend on the language packs currently loaded into 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.

When you add a new language pack for the endpoint, the language pack must be formatted as “X.GUI.name.lang” (X starts from 014, and “name” is replaced with the language name).

NOTE

We recommend that the filename of the new language pack should not be the same as the existing one. If the language name is the same as the existing one, the existing language pack will be overridden by the newly uploaded one.

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.

NOTE

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

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


```

000.GUI.English.lang x
1 [Lang]
2 Name=English
3 FONT=Tahoma
4
5 [Translate]
6
7 "is offline"="is offline"
8 "s"="s"
9 "#"="#"
10 "(Empty)"="(Empty)"
11 "(No Name)"="(No Name)"
12 "*"="*"
13 "<New Item>"="<New Item>"
14 "0s"="0s"
15 "102s"="102s"
16 "108s"="108s"
17 "114s"="114s"
18 "12 Hour"="12 Hour"
19 "120s"="120s"
20 "12s"="12s"
21 "15s"="15s"
22 "1800s"="1800s"
23 "18s"="18s"
24 "24 Hour"="24 Hour"
25 "24s"="24s"
26 "300s"="300s"
27 "30s"="30s"
28 "36s"="36s"
29 "3rd-party VMR"="Third-party VMR"
30 "42s"="42s"
31 "48s"="48s"
32 "54s"="54s"
33 "600s"="600s"
34 "60s"="60s"
35 "66s"="66s"
36 "6s"="6s"
  
```

Parameter	Description	Optional Value
-----------	-------------	----------------

gui_lang.url	It configures the access URL of the custom language pack for the endpoint.	URL within 511 characters, empty is the default. For example http://localhost/X.GUI.name.lang X starts from 014, “name” is replaced with the language name.
gui_lang.delete	It deletes the specified or all custom language packs of the device.	http://localhost/all or X.GUI.name.lang\ X starts from 014, and “name” is replaced with the language name. Default null.

Customize Web Interface Language File

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

Customizing the Web Interface Language

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 14, and “name” is replaced with the language name).

NOTE

We recommend that the filename of the new language pack should not be the same as the existing one. If the language name is the same as the existing one, the existing language pack will be overridden by the newly uploaded one.

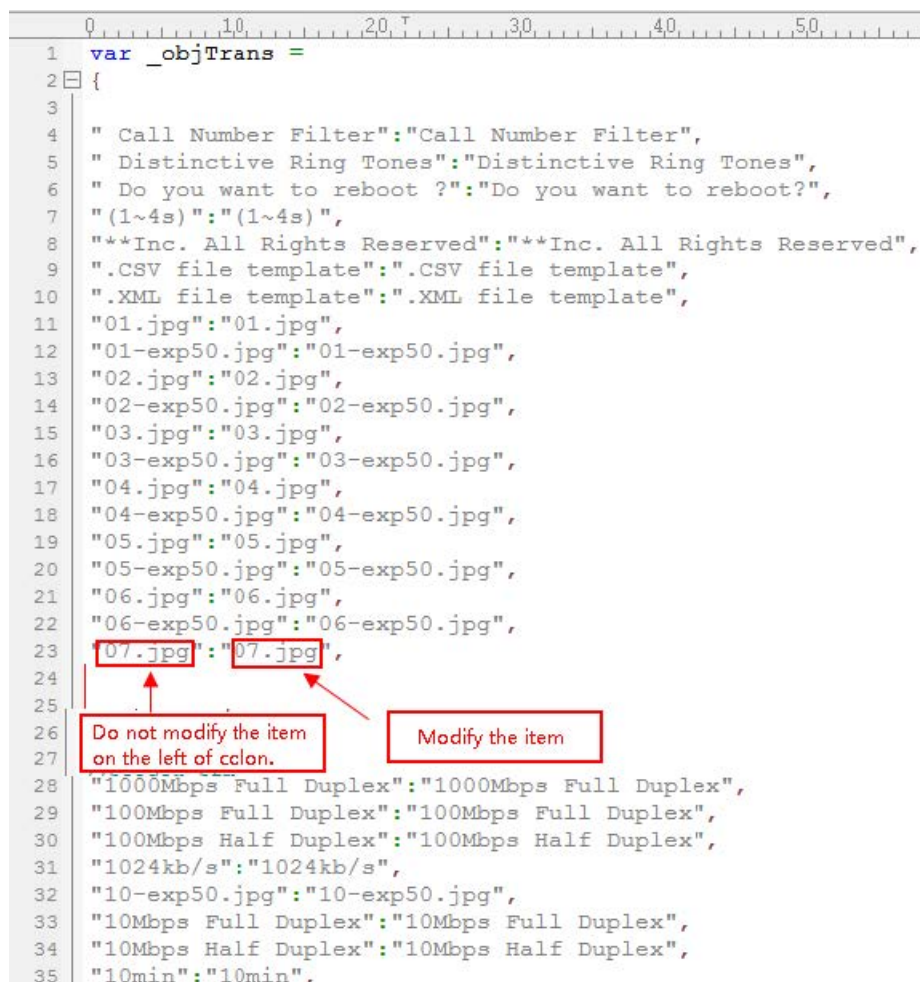
1. Use the ASCII editor to open the desired language template file (for example, 1.English.js).

2. Modify the characters within the double quotation marks on the right of the colon.

NOTE

Do not modify the translation item on the left of the colon.

Save the language pack and place it on the provisioning server.



```

1  var _objTrans =
2  {
3
4  " Call Number Filter":"Call Number Filter",
5  " Distinctive Ring Tones":"Distinctive Ring Tones",
6  " Do you want to reboot ?":"Do you want to reboot?",
7  "(1~4s)":"(1~4s)",
8  "***Inc. All Rights Reserved":"***Inc. All Rights Reserved",
9  ".CSV file template":".CSV file template",
10 ".XML file template":".XML file template",
11 "01.jpg":"01.jpg",
12 "01-exp50.jpg":"01-exp50.jpg",
13 "02.jpg":"02.jpg",
14 "02-exp50.jpg":"02-exp50.jpg",
15 "03.jpg":"03.jpg",
16 "03-exp50.jpg":"03-exp50.jpg",
17 "04.jpg":"04.jpg",
18 "04-exp50.jpg":"04-exp50.jpg",
19 "05.jpg":"05.jpg",
20 "05-exp50.jpg":"05-exp50.jpg",
21 "06.jpg":"06.jpg",
22 "06-exp50.jpg":"06-exp50.jpg",
23 "07.jpg":"07.jpg",
24
25
26 "1000Mbps Full Duplex":"1000Mbps Full Duplex",
27 "100Mbps Full Duplex":"100Mbps Full Duplex",
28 "100Mbps Half Duplex":"100Mbps Half Duplex",
29 "1024kb/s":"1024kb/s",
30 "10-exp50.jpg":"10-exp50.jpg",
31 "10Mbps Full Duplex":"10Mbps Full Duplex",
32 "10Mbps Half Duplex":"10Mbps Half Duplex",
33 "10min":"10min",
34
35

```

Customizing Language Pack for Note

When you add a new language pack, the language pack must be formatted as “X.name_.xml” (X starts from 12, and “name” is replaced with the language name).

NOTE

We recommend that the filename of the new language pack should not be the same as the existing one. If the language name is the same as the existing one, the newly uploaded language pack will override the existing one.

1. Use the XML editor to open the language template file (for example, 1.English_.xml).
2. Modify the text of the field.

NOTE

Do not modify the name.

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

```
<?xml version="1.0" encoding="utf-8"?>
<notedata>
<status>
  <note name = "version">
    <head>Description:</head>
    <text>It shows the current firmware version and hardware version of the device.</text>
  </note>
  <note name = "DeviceCertificate">
    <head>Description:</head>
    <text>It shows the Device Certificate of the device.</text>
  </note>
  <note name = "network">
    <head>Description:</head>
    <text>It shows the IP address mode of the device.</text>
  </note>
  <note name = "network-ipv4">
    <head>Description:</head>
    <text>It shows the basic IPv4 network configurations.</text>
  </note>
  <note name = "network-ipv6">
    <head>Description:</head>
    <text>It shows the basic IPv6 network configurations.</text>
  </note>
</status>
</notedata>
```

Parameter	Description	Optional Value
wui_lang.url	It configures the access URL of the custom language pack for the web user interface.	URL within 511 characters For example http://localhost/X.GUI.name.lang X starts from 14, and “name” is replaced with the language Name. Default null.
wui_lang_.url	It configures the access URL of the custom language pack for the web user interface.	URL within 511 characters For example: http://localhost/X.name_.xml X starts from 13, and “name” is replaced with the language Name. Default null.
wui_lang.delete	It deletes the specified or all language packs of the web user interface and s the language packs for the web user interface.	http://localhost/all or http://localhost/Y.name.js. Default null.

Basic Settings


Introduction

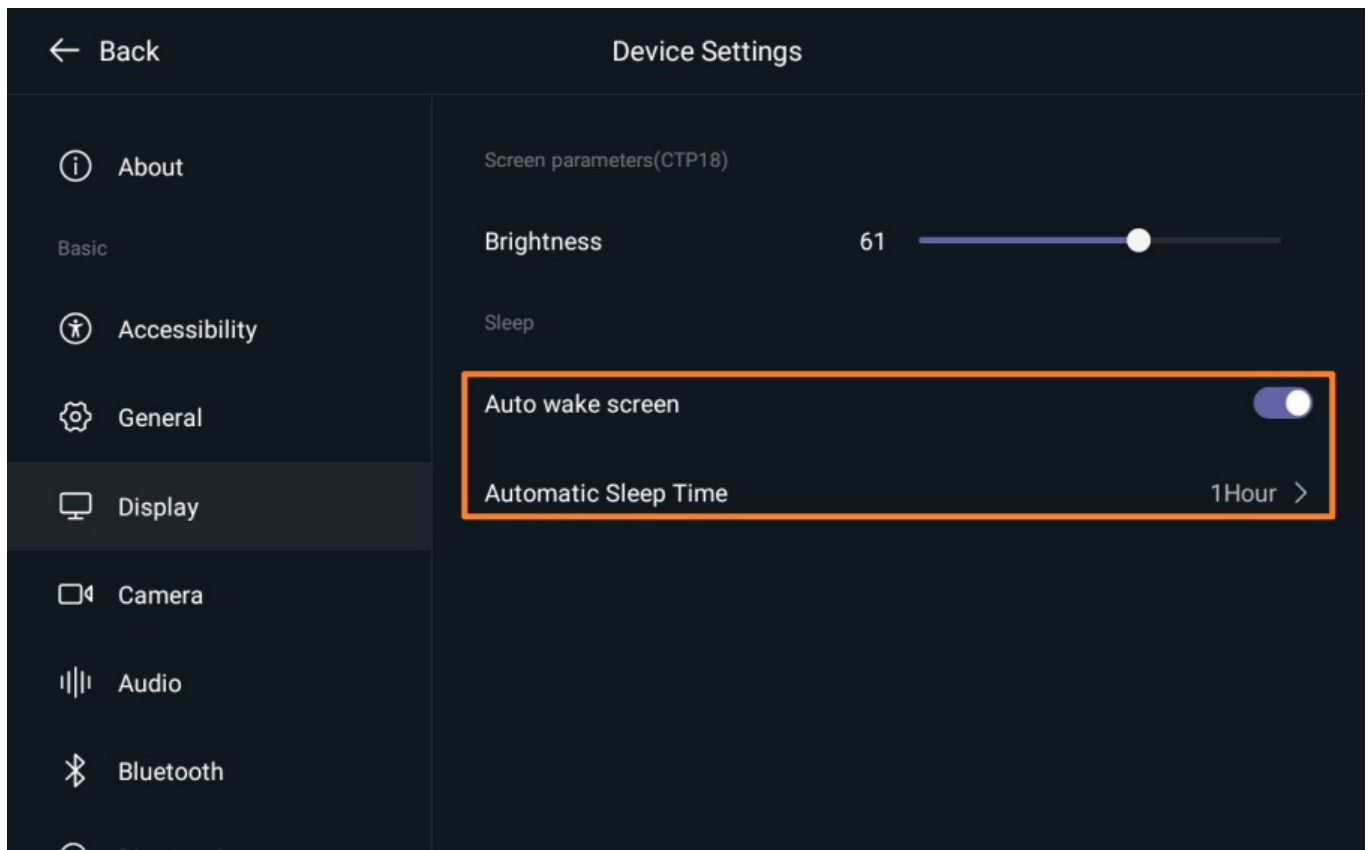
It configures the basic settings of the MeetingBar.

Automatic Sleep

The device automatically enters sleep mode after a period of standby.

Configure via Device Interface

1. On the CTP18, go to  > **Settings** > **General**.
2. Configure **Sleep**.



Configure via Web User Interface

1. Go to **System** > **Basic** on the web user interface.

2. Configure **Auto Wake Screen/Automatic Sleep Time** and click **Confirm**.

The screenshot shows the Yealink MeetingBar A20 Basic configuration page. The left sidebar has the 'System' menu expanded, with 'Basic' selected. The main area shows the 'Basic' configuration page. The 'Automatic Sleep Time' is set to '1 h' and 'Automatic Wake Up' is enabled. The 'ReLogOffTime(1-1000min)' is set to '500' and the 'Remote Controller Model' is 'VCR11'. The 'Confirm' button is at the bottom right.

Parameter	Description
Automatic Sleep Time	<p>Configure the inactive time (minutes) before the system enters sleep mode.</p> <div> <p>NOTE</p> <p>Tap the screen to manually exit sleep mode. The device will not automatically enter sleep mode during the setup wizard, and the display will always be on. To protect the monitor, you should complete the setup wizard immediately.</p> </div>
Auto Wake Screen	Enable or disable the device automatically wakes up the screen when someone approaches.

Basic Settings

Adjust the basic configuration of the MeetingBar AX0.

Configure via Device Interface

- On the CTP18, go to  > **Settings** > **General**.

Configure via Web User Interface

1. Go to **System > Basic** in the web user interface.
2. Configure in the **Basic**.

Parameter	Description
Device Name	To configure the site name of the endpoint and customize the name of the endpoint, which will be displayed on remote devices' screens during a call.
ReLogOffTime(1-1000min)	To configure the logout time for the web user interface when it is idle.

Remote Controller Model

Configure the model of the remote control used by the endpoint.

Configure via Web User Interface

1. Go to **System > Basic** in the web user interface.
2. Configure in the **Remote Controller Model**.

Parameter	Description
Remote Controller Model	Configure the model of the remote control used by the endpoint.

Time & Date

Introduction

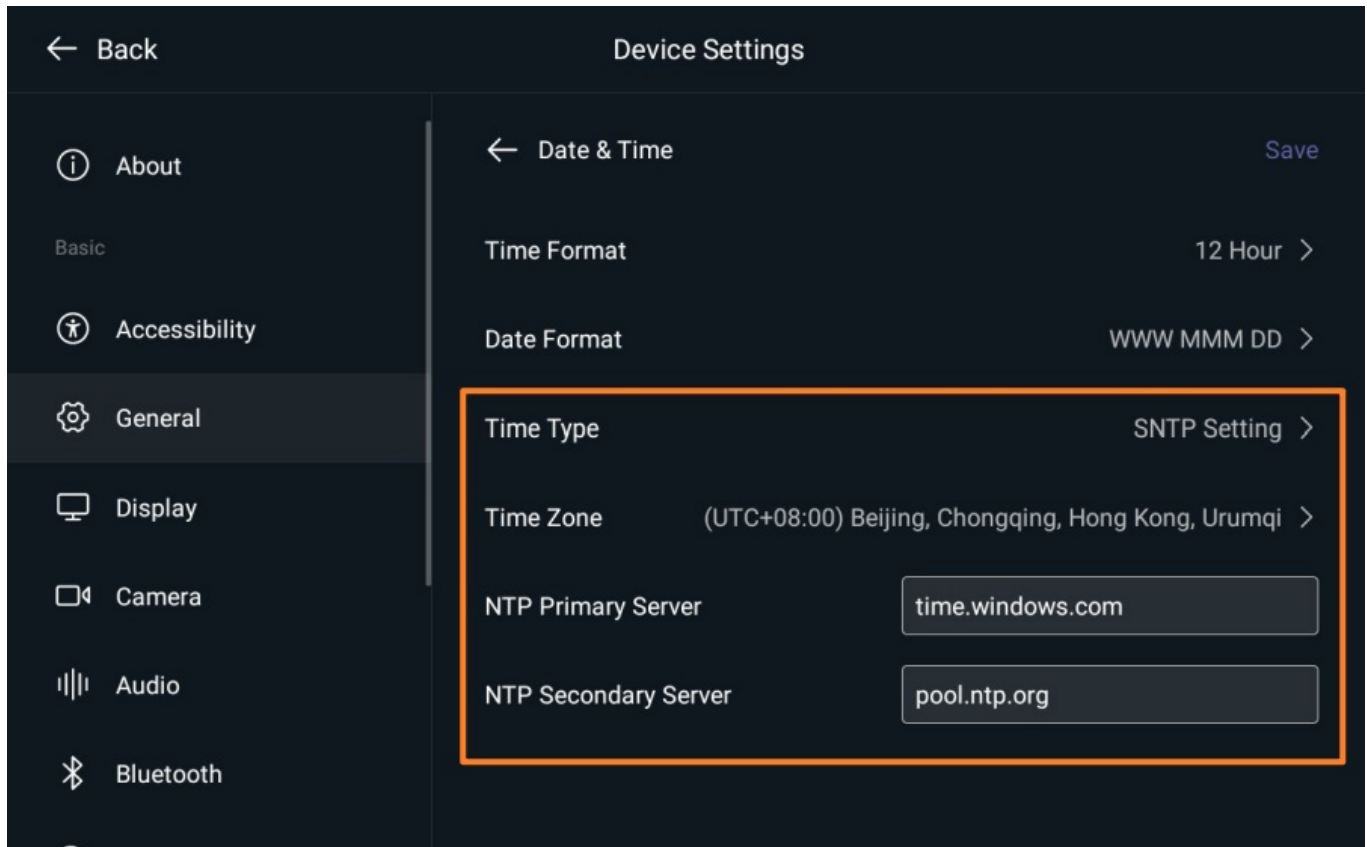
It configures the date and time of the device.

NTP Settings

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > General > Date & Time**.

2. Configure **Time/Zone/NTP Primary Server/NTP Secondary Server** and select **Save**.



Configure via Web User Interface

1. Go to **System > Date&Time** on the web user interface.

2. Configure **Date & Time** and click **Confirm**.

Date&Time ?

Date&Time

Current Time 3:48:26 PM Thu Apr 20

Set Time ☒ Use NTP ☐ Manually

Time Zone (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

* Primary Server time.windows.com

Secondary Server pool.ntp.org

Update Interval (Sec) 1000 (15-86400)

Format Settings

Date Format WWW MMM DD

Time Format Hour 12

Confirm Cancel

Parameter	Description
Current Time	Displays the date and time of the current time zone.
Set Time	<p>Choose to use NTP to obtain the time or set the time manually automatically.</p> <p>- Use NTP: The device automatically updates the system time within a period to keep consistent with the time of the NTP server. You need to configure the time zone, NTP primary server, and update interval.</p> <p>- Manually: Set the device time manually. You need to configure the date and time.</p>
Time Zone	Configure the time zone for the device.
NTP Primary Server	Configure the NTP primary server for the device.
NTP Secondary Server	Configure the NTP secondary server for the device.
Update Interval (Sec)	Configure the interval for the device to synchronize time and date from the NTP server.

Auto Provisioning

You can set up an NTP time server for the desired locale as needed. The NTP time server address can be provided by

the DHCP server or manually configured.

Parameter	Description	Optional Value
local_time. manual_ntp _srv_prior	It configures the priority for the device to use the NTP server address offered by the DHCP server.	0: Disabled. (use the NTP server address offered by the DHCP server preferentially) (default) 1: Enabled. (use the NTP server address configured manually preferentially) Default: 0
local_time. ntp_server1	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.	IP address or domain name. Default: time.windows.com
local_time. ntp_server2	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.	IP address or domain name. Default: pool.ntp.org
local_time.i nterval	It configures the interval (in seconds) at which the device updates the time and date from the NTP server.	Integer from 15 to 86400. Default: 1000
local_time. android_ti me_zone	It configures the time zone in the data standard. Example: “local_time.android_time_zone=Asia/Shanghai” means configures the time zone as “Beijing, Chongqing, Hong Kong, Urumqi” ; “local_time.android_time_zone=Pacific/Honolulu” means configures the time zone as “Hawaii” ; “local_time.android_time_zone=America/Chicago” means configures the time zone as “Central Time (US & Canada)” For available time zones, refer to Time Zone.	String within 64 characters. Default: America/Los_Angeles

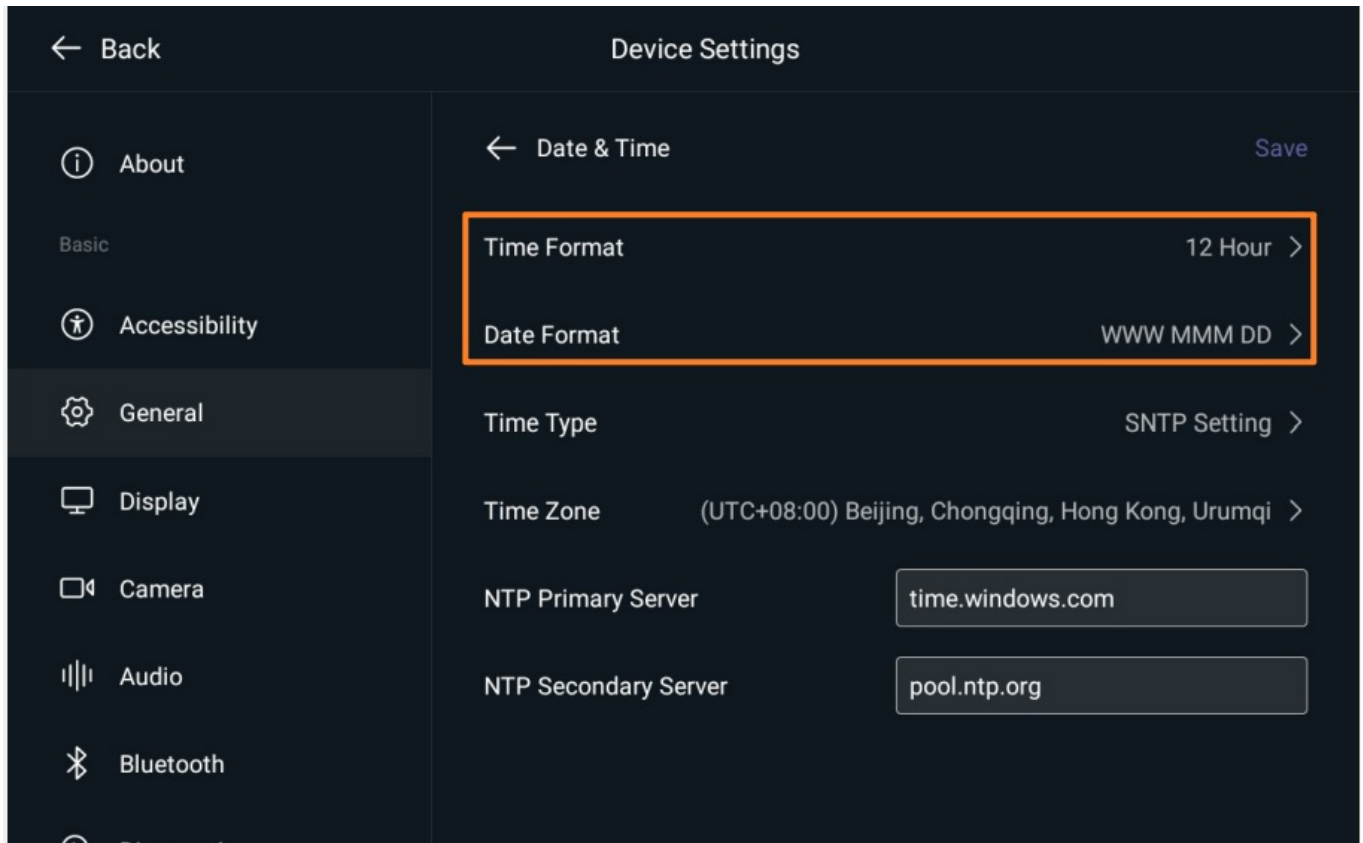
Configure Format

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.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > General > Date & Time**.

2. Configure **Date & Time Format** and select **Save**.



Configure via Web User Interface

1. Go to **System > Date & Time** on the web user interface.

2. Configure **Date** or **Time** and click **Confirm**.

Yealink
MeetingBar A20
English(United States) ▼

admin

Status

Network ①

System ②

Basic

Date&Time

Collaboration Touch P...

Display

Audio

Microphone

Camera

Backup & Restore

UC Provider

Update

Auto Provision

System Diagnostic

hl

Date&Time ?

Date&Time

Current Time 3:48:28 PM Thu Apr 20

Set Time ☒ Use NTP ☐ Manually

Time Zone (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi ▼

* Primary Server time.windows.com

Secondary Server pool.ntp.org

Update Interval (Sec) 1000 (15-86400)

Format Settings

Date Format WWW MMM DD ▼ ③

Time Format Hour 12 ▼

Confirm Cancel

Auto Provisioning

Parameter	Description	Optional Value
local_time.time_format	It configures the time format.	0: Hour 12, the time will be displayed in 12-hour format with AM or PM specified. 1: Hour 24, the time will be displayed in 24-hour format (for example, 2:00 PM displays as 14:00). Default: 1

local_time.date _format	It configures the date format.	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.
----------------------------	--------------------------------	--

Zones

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

Time Zone	Time Zone ID	Time Zone Name	Time Zone	Time Zone ID	Time Zone Name
-12	Etc/GMT+12	International Date Line West	+3	Asia/Baghdad	Baghdad
-11	Etc/GMT+11	Coordinated Universal Time-11	+3	Asia/Riyadh	Kuwait, Riyadh
-10	Pacific/Honolulu	Hawaii	+3	Asia/Kuwait	Kuwait, Riyadh
-8	America/Anchorage	Alaska	+3	Europe/Minsk	Minsk
-7	America/Los_Angeles	Pacific Time (US & Canada)	+3	Europe/Moscow	Moscow, St.Petersburg, Volgograd (RTZ 2)
-7	America/Tijuana	Baja California	+3	Africa/Nairobi	Nairobi
-6	America/Mazatlan	Chihuahua, LaPaz, Mazatlan	+4:30	Asia/Tehran	Tehran
-7	America/Phoenix	Arizona	+4	Asia/Muscat	Abu Dhabi, Muscat
-6	America/Edmonton	Mountain Time (US & Canada)	+4	Asia/Baku	Baku

-6	America/Denver	Mountain Time (US & Canada)	+4	Europe/Samara	Izhevsk, Samara (RTZ 3)
-6	America/Guatemala	Central America	+4	Indian/Mauritius	Port Louis
-5	America/Mexico_City	Guadalajara, Mexico City, Monterrey	+4	Asia/Tbilisi	Tbilisi
-6	America/Regina	Saskatchewan	+4	Asia/Yerevan	Yerevan
-5	America/Chicago	Central Time (US & Canada)	+4:30	Asia/Kabul	Kabul
-5	America/Cancun	Chetumal	+5	Asia/Tashkent	Ashgabat, Toshkent
-4	America/New_York	Eastern Time (US & Canada)	+5	Asia/Ashgabat	Ashgabat, Toshkent
-4	America/Indianapolis	Indiana (East)	+5	Asia/Yekaterinburg	Ekaterinburg (RTZ 4)
-5	America/Rio_Branco	Bogota, Lima, Quito, Rio Branco	+5	Asia/Karachi	Islamabad, Karachi
-5	America/Bogota	Bogota, Lima, Quito, Rio Branco	+5:30	Asia/Calcutta	Chennai, Kolkata, Mumbai, New Delhi
-4	America/Caracas	Caracas	+5:30	Asia/Colombo	Sri Jayawardenepura
-4	America/Cuiaba	Cuiaba	+5:45	Asia/Kathmandu	Kathmandu
-4	America/La_Paz	Georgetown, La Paz, Manaus, San Juan	+6	Asia/Almaty	Astana
-4	America/Asuncion	Asuncion	+6	Asia/Dhaka	Dhaka
-3	America/Halifax	Atlantic Time (Canada)	+7	Asia/Novosibirsk	Novosibirsk (RTZ 5)
-2:30	America/St_Johns	Newfoundland	+6:30	Asia/Rangoon	Yangon (Rangoon)
-3	America/Bahia	Brasilia	+7	Asia/Bangkok	Bangkok, Hanoi, Jakarta
-3	America/Buenos_Aires	Buenos Aires	+7	Asia/Jakarta	Bangkok, Hanoi, Jakarta

-3	America/Cayenne	Cayenne, Fortaleza	+7	Asia/Krasnoyarsk	Krasnoyarsk (RTZ 6)
-3	America/Fortaleza	Cayenne, Fortaleza	+8	Asia/Shanghai	Beijing, Chongqing, Hong Kong, Urumqi
-2	America/Godthab	Greenland	+8	Asia/Hong Kong	Beijing, Chongqing, Hong Kong, Urumqi
-3	America/Montevideo	Montevideo	+8	Asia/Irkutsk	Irkutsk (RTZ 7)
-3	America/Bahia	Salvador	+8	Asia/Singapore	Kuala Lumpur, Singapore
-4	America/Santiago	Santiago	+8	Asia/Kuala Lumpur	Kuala Lumpur, Singapore
-2	Etc/GMT+2	Coordinated Universal Time-02	+8	Australia/Perth	Perth
-2	America/Noronha	Mid-Atlantic-Old	+8	Asia/Taipei	Taipei
0	Atlantic/Azores	Azores	+8	Asia/Ulaanbaatar	Ulaanbaatar
-1	Atlantic/Cape Verde	Cabo Verde Is	+9	Asia/Tokyo	Osaka, Sapporo, Tokyo
+1	Africa/Casablanca	Casablanca	+9	Asia/Seoul	Seoul
0	Etc/GMT	Coordinated Universal Time	+9	Asia/Yakutsk	Yakutsk (RTZ 8)
+1	Europe/London	Dublin, Edinburgh, Lisbon, London	+9:30	Australia/Adelaide	Adelaide
+1	Europe/Dublin	Dublin, Edinburgh, Lisbon, London	+9:30	Australia/Darwin	Darwin
+1	Europe/Lisbon	Dublin, Edinburgh, Lisbon, London	+10	Australia/Brisbane	Brisbane
0	Atlantic/Reykjavik	Monrovia, Reykjavik	+10	Australia/Sydney	Canberra, Melbourne, Sydney
0	Europe/Stockholm	Monrovia, Reykjavik	+10	Pacific/Port Moresby	Guam, Port Moresby

+2	Europe/Berlin	Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	+10	Pacific/Guam	Guam, Port Moresby
+2	Europe/Rome	Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	+10	Australia/Hobart	Hobart
+2	Europe/Stockholm	Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	+11	Asia/Magadan	Magadan
+2	Europe/Budapest	Belgrade, Bratislava, Budapest, Ljubljana, Prague	+10	Asia/Vladivostok	Vladivostok, Magadan (RTZ 9)
+2	Europe/Belgrade	Belgrade, Bratislava, Budapest, Ljubljana, Prague	+11	Asia/Srednekolymsk	Chokurdakh (RTZ 10)
+2	Europe/Paris	Brussels, Copenhagen, Madrid, Paris	+11	Pacific/Guadalcanal	Solomon Is., New Caledonia
+2	Europe/Madrid	Brussels, Copenhagen, Madrid, Paris	+11	Pacific/Noumea	Solomon Is., New Caledonia
+2	Europe/Brussels	Brussels, Copenhagen, Madrid, Paris	+12	Asia/Anadyr	Anadyr, Petropavlovsk-Kamchatsky (RTZ 11)
+2	Europe/Warsaw	Sarajevo, Skopje, Warsaw, Zagreb	+12	Pacific/Auckland	Auckland, Wellington
+2	Europe/Skopje	Sarajevo, Skopje, Warsaw, Zagreb	+12	Etc/GMT-12	Coordinated Universal Time+12
+1	Africa/Lagos	West Central Africa	+12	Pacific/Fiji	Fiji
+2	Africa/Windhoek	Windhoek	+12	Asia/Kamchatka	Petropavlovsk-Kamchatsky-Old
+3	Asia/Amman	Amman	+13	Pacific/Tongatapu	Nuku'alofa
+3	Europe/Bucharest	Athens, Bucharest	-11	Pacific/Pago_Pago	Samoa
+3	Europe/Athens	Athens, Bucharest	+14	Pacific/Kiritimati	Kiritimati Island
+3	Asia/Beirut	Beirut	+8:45	Australia/Eucla	Eucla
+2	Africa/Cairo	Cairo	+3	Asia/Gaza	Gaza
+3	Asia/Damascus	Damascus	+2	Europe/Luxembourg	Luxembourg

+3	Europe/China	E. Europe	+1	Atlantic/Canary	Spain-Canary Islands
+2	Africa/Harare	Harare, Pretoria	-4	America/Havana	Havana
+3	Europe/Kiev	Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	-4	America/Nassau	Nassau
+3	Europe/Istanbul	Istanbul	-3	Atlantic/Bermuda	Bermuda
+3	Asia/Jerusalem	Jerusalem	-9:30	Pacific/Marquesas	French Polynesia
+2	Europe/Kaliningrad	Kaliningrad	+10:30	Australia/Lord_Howe	Lord Howe Island
+2	Africa/Tripoli	Tripoli	+12:45	Pacific/Chatham	Chatham Islands

Display

Introduction

It configures the parameters displayed on the device screen.

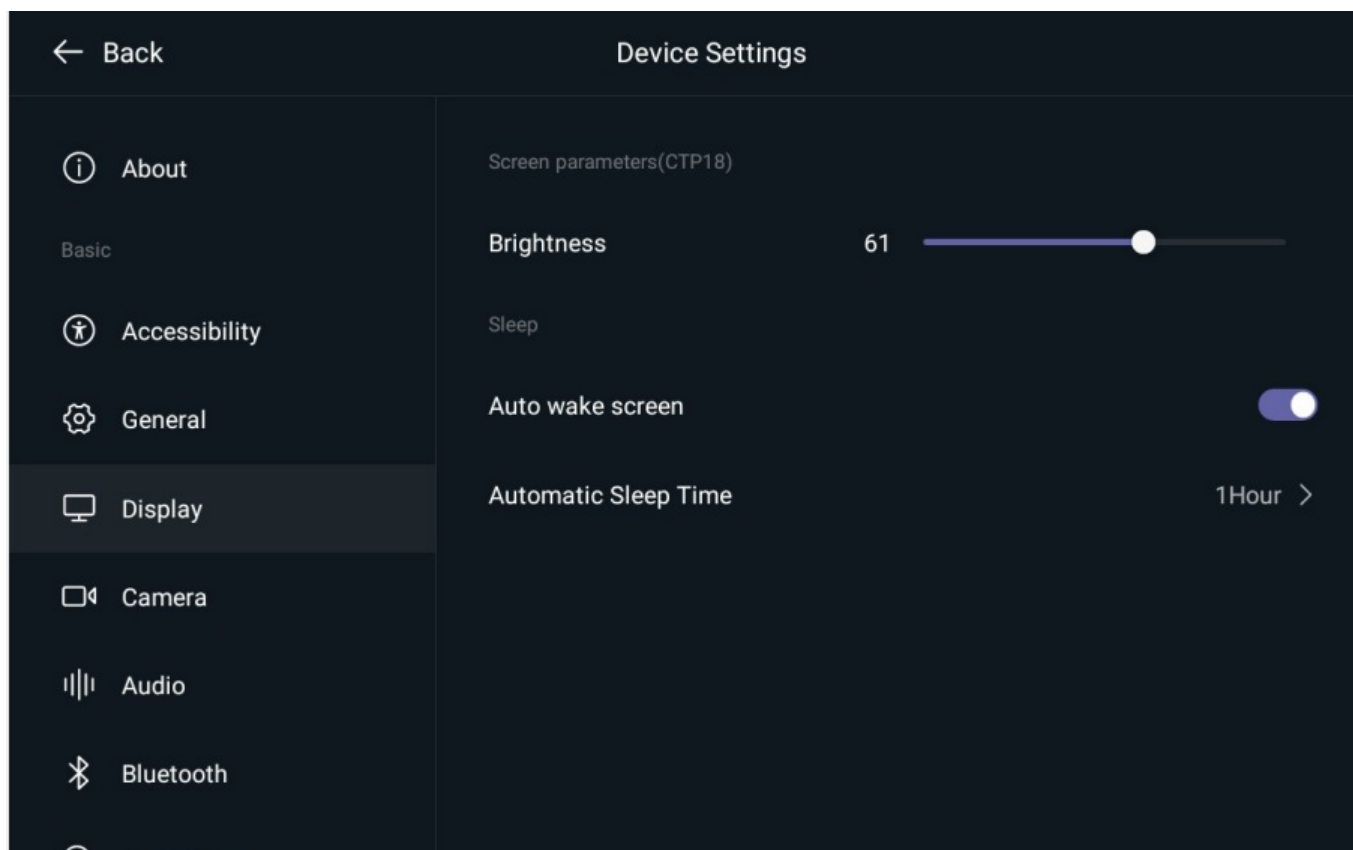
Adjust CTP18 Brightness

It can only be configured after MeetingBar AX0 is connected to CTP18.

Configure via the CTP18

1. On the CTP18, go to **More > Settings > Device Settings > Display**.

2. Adjust **Brightness** in **Screen parameters**.




CEC

The MeetingBar will automatically synchronize standby and wake with the connected display when enabled.

Configure via Device Interface

NOTE

The MeetingBar A10 is supported in version 278.321.0.20 and later. MeetingBar A20/A30 is not supported.

1. On the CTP18 or with the remote control, go to  **> Settings > Display**.
2. Enable **HDMI CEC**.

Configure via Web User Interface

1. Go to **System > Display** on the web user interface.
2. Enable **HDMI CEC**.

Parameter	Description
HDMI CEC	The MeetingBar will automatically synchronize standby and wake with the connected display when enabled.

Output Resolution

You can configure the resolution to meet the needs of different display screens.

NOTE

The MeetingBar A10 is supported in version 278.321.0.20 and later. MeetingBar A20/A30 is not supported.

Configure via Web User Interface

1. Go to **System > Display** on the web user interface.
2. Configure **Output Resolution**.

Parameter	Description
Output Resolution	The main screen supports up to 4K30 resolution, and the secondary screen supports up to 1080P60 resolution, depending on whether the display you connect supports it or not.

Bluetooth

Introduction

When Bluetooth is enabled, the Proximity Join meeting feature can be used.

Bluetooth Settings

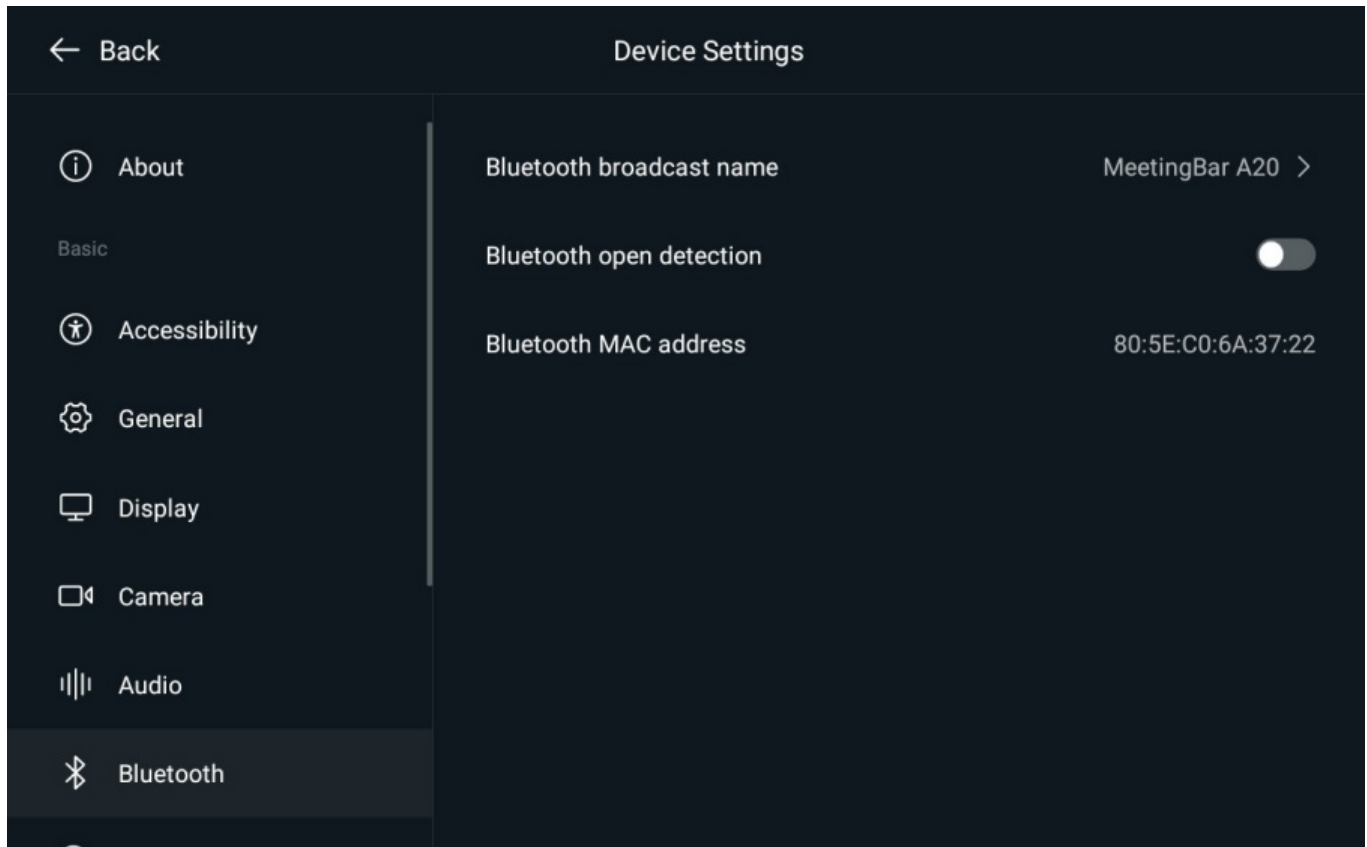
Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Bluetooth**.

2. Enable **Bluetooth open detection** to search for devices.

NOTE

If you want the device to be searched by other Bluetooth devices, you need to enable **Bluetooth open detection**.



Auto Provisioning

Parameter	Description	Optional Value
static.bluetooth.function.enable	It configures whether to enable Bluetooth.	0: Disabled. You will not be able to activate Bluetooth mode. 1: Enabled
features.bluetooth_enable	It configures whether to activate Bluetooth.	0: Disabled 1: Enabled
features.bluetooth_adapter_name	It customizes the name of the Bluetooth device.	64 characters

Accessibility

Introduction

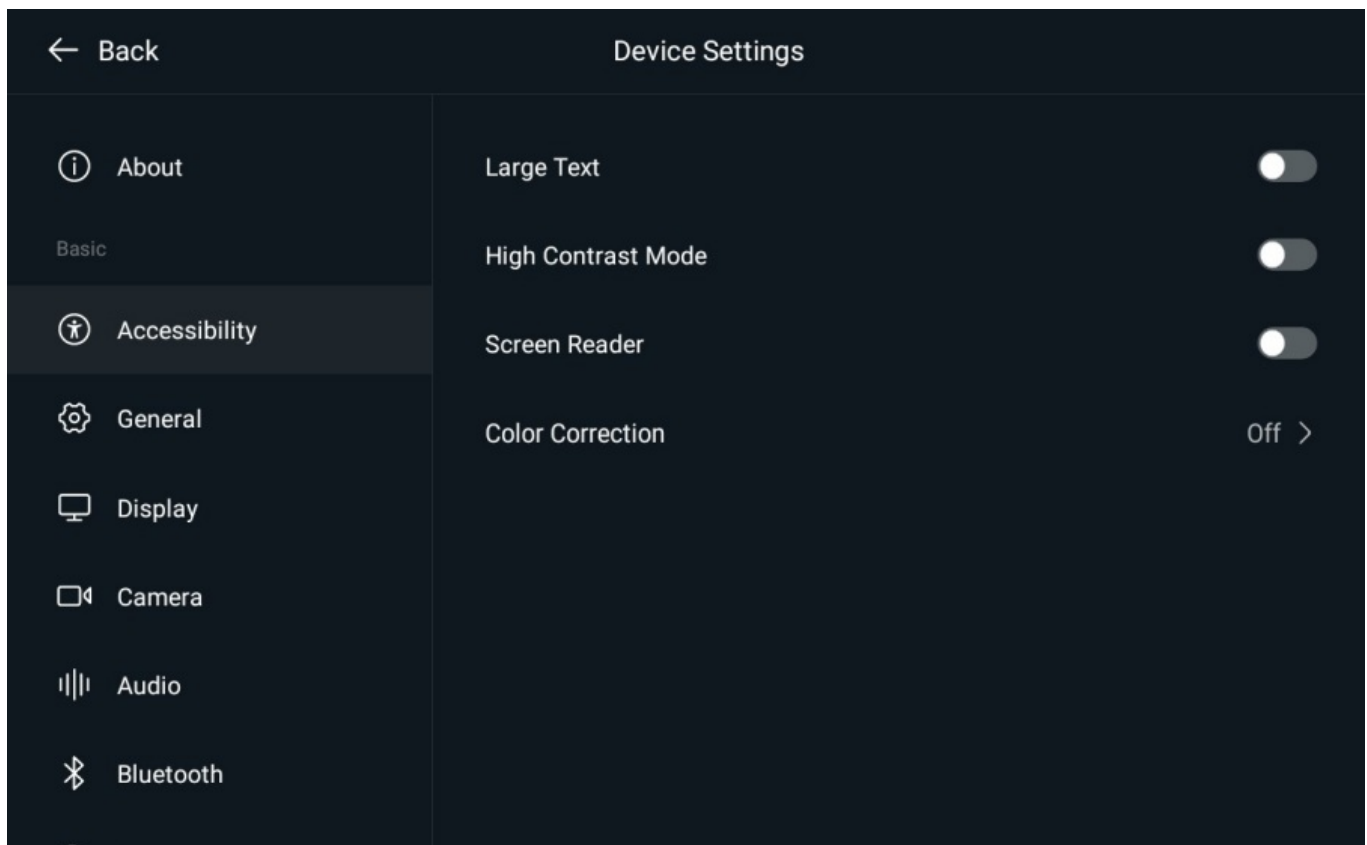
The device provides the appropriate accessibility functions for visually impaired users.

NOTE

After enabling the Screen Reader feature, you need to double-tap to select features and swipe with two fingers to move the progress bar.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Accessibility**.
2. Enable the required accessibility features.



Auto Provisioning

Parameter	Description	Optional Value
features.accessibility.large_text.enable	It enables or disables the large text feature.	0: Disabled 1: Enabled
features.accessibility.high_text_contrast.enable	It enables or disables the high-contrast text feature.	0: Disabled 1: Enabled

features.accessibility.display_daltonizer	It enables or disables color correction.	0: Disabled 1: Deuteranomaly (red-green) 2: Protanomaly (red-green) 3: Tritanomaly (blue-yellow)
features.screen_reader.enable	It enables or disables the screen reader features.	0: Disabled 1: Enabled

Screenshot

Introduction

Use the screenshot feature to capture the screen you need.

Screenshot

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Debug** (default password: 0000) to open the **web remote screen capture** under the corresponding device. If the default password (0000) is used at this time, you will be prompted to change the password first. Please change the password according to the prompt, then enable this setting.
2. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > About** to get the IP address of the device.
3. Enter *[https://device IP address/api#/screencapture](https://device IP address/api#%2Fscreencapture)* on the browser, for example, <https://10.50.67.1/api#/screencapture>. And enter the administrator account (default account: admin) and password (please enter the new password).

System Configuration

Reboot Device

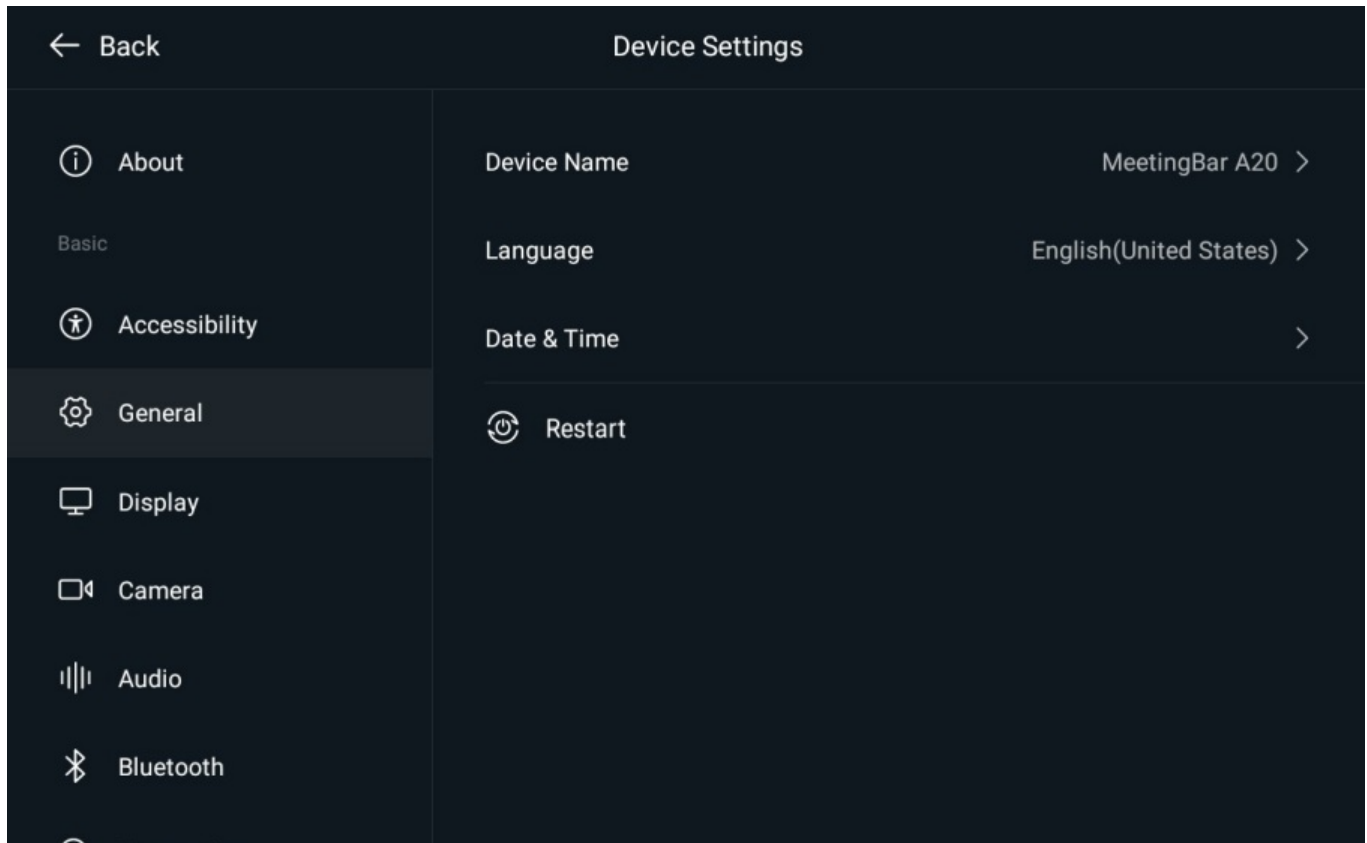
Introduction

Reset your system.

Reboot System

Configure via Device Interface

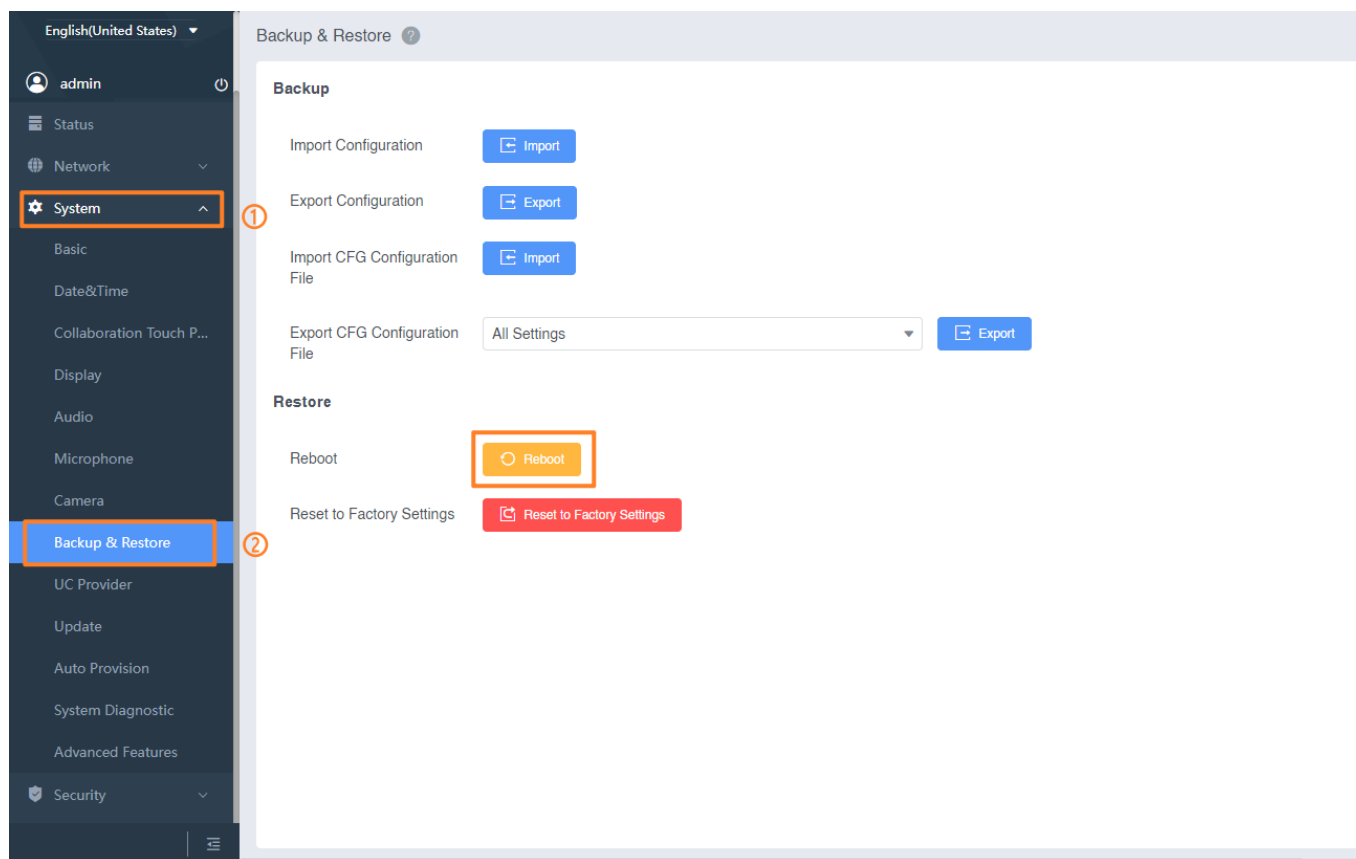
1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > General > Restart**.
2. Select **Restart**. After successful pairing between CTP18 and AX0, rebooting the CTP18 device will result in both devices rebooting.



Configure via Web User Interface

1. Go to **System > Backup & Restore** on the web user interface.

2. Click **Restore**.



Backup & Reset

Introduction

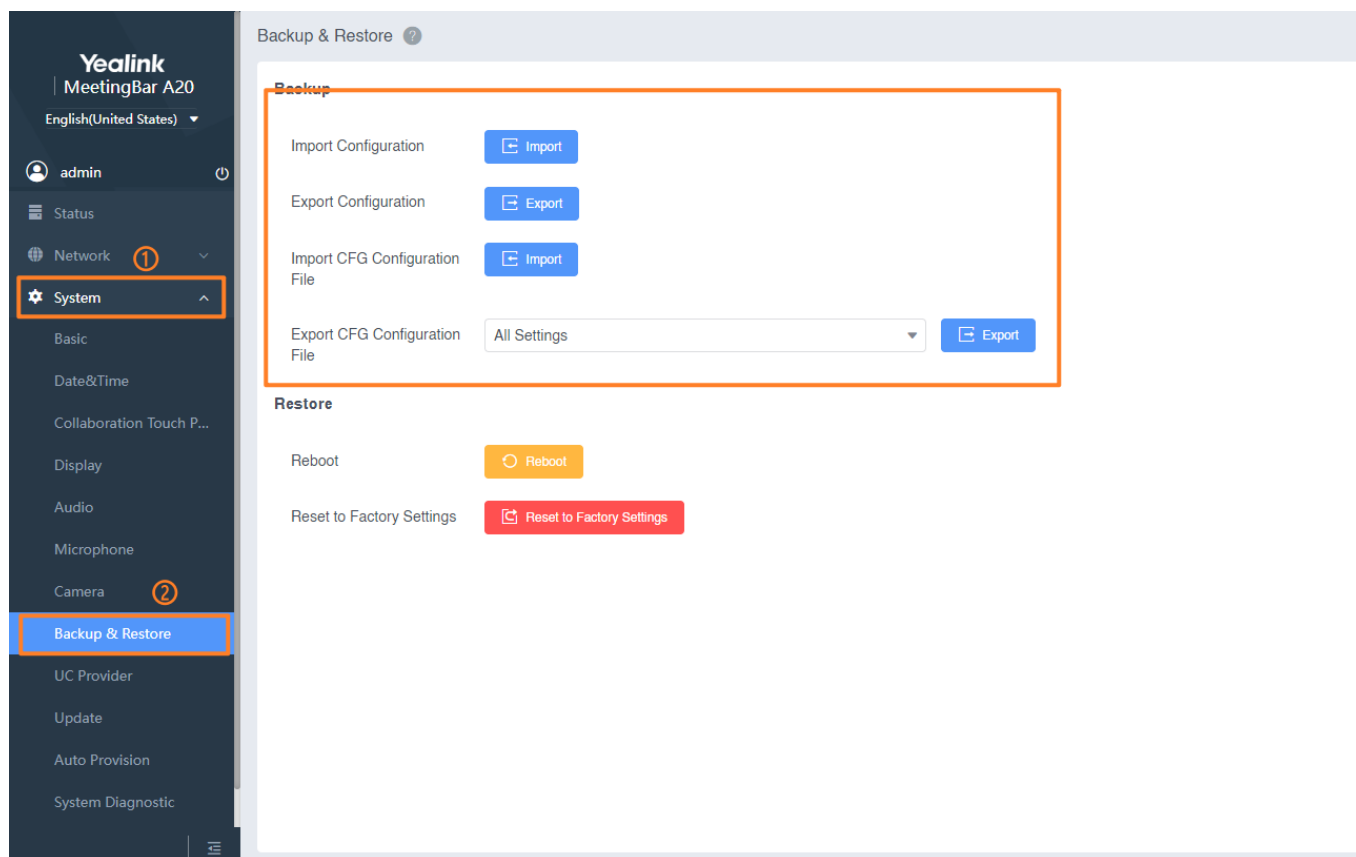
Import system configuration and configure multiple devices in batches. Export the configuration before restoring the terminal to factory settings, and re-import the configuration file after restoring the factory to restore the pre-factory state quickly.

Backup

Configure via Web User Interface

1. Go to **System > Backup & Restore** on the web user interface.

2. Click **Export** under **Export Configuration**.



Parameter	Description
Import Configuration	<p>Import a configuration file for the device to configure quickly.</p> <p>NOTE The file format of the custom configuration file must be *.bin.</p>
Export Configuration	<p>When the device encounters a problem, you can export the device configuration for backup or assist Yealink technical support in analyzing the problem.</p> <p>NOTE The exported configuration file contains modified non-factory configuration values and resource files (such as contacts).</p>
Import CFG Configuration	<p>When you want to apply specific settings to devices in bulk, you can create your own CFG profile with custom parameters.</p> <p>NOTE The imported configuration file must be in .cfg format. You can get the template of the CFG profile by Export CFG Configuration File.</p>

Export CFG Configuration	<p>To export the CFG file of the terminal configuration, you can optionally export the file:</p> <ul style="list-style-type: none"> - Static Settings: Export parameters are static parameters, and the parameter prefixes are static, such as network configuration. - Non-static settings: Export parameters are non-static parameters without static prefixes, such as contacts and display settings. - All Settings: Export all static and non-static settings. <p>NOTE The exported CFG configuration file contains modified non-factory configuration values.</p>
--------------------------	--

Auto Provisioning

Parameter	Description	Optional Value
static.configuration.url	<p>It configures the access URL for the custom configuration files.</p> <p>NOTE The file format of the custom configuration file must be *.bin.</p>	URL within 511 characters, empty is the default.

Reset System

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.

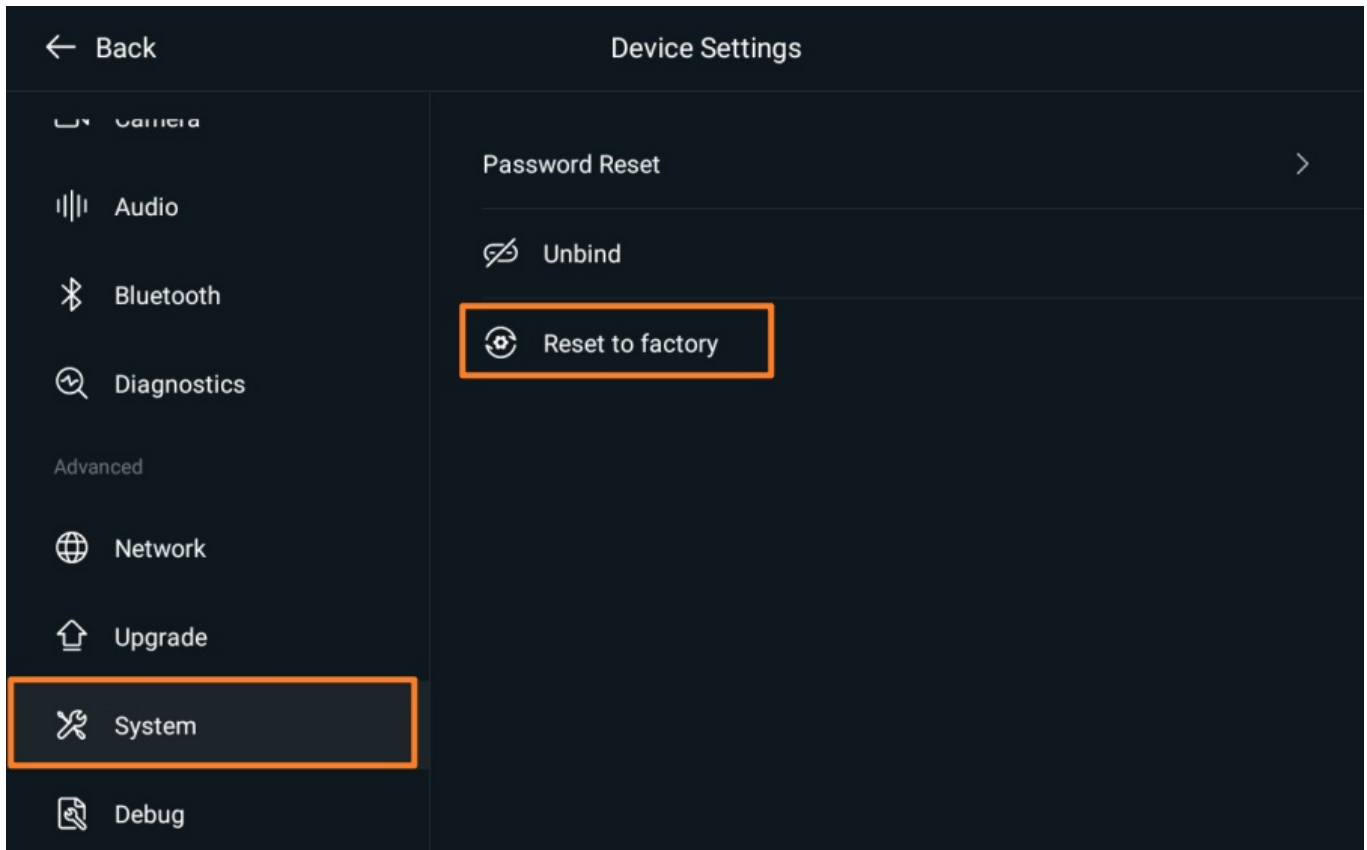
NOTE

- Dates such as call logs and local logs cannot be recovered after a factory reset.
- You can export the configuration before the factory reset (the exported configuration file contains modified non-factory configuration values and resource files (such as contacts)) to facilitate system recovery after the factory reset.

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > Advanced > System** (default password: 0000).

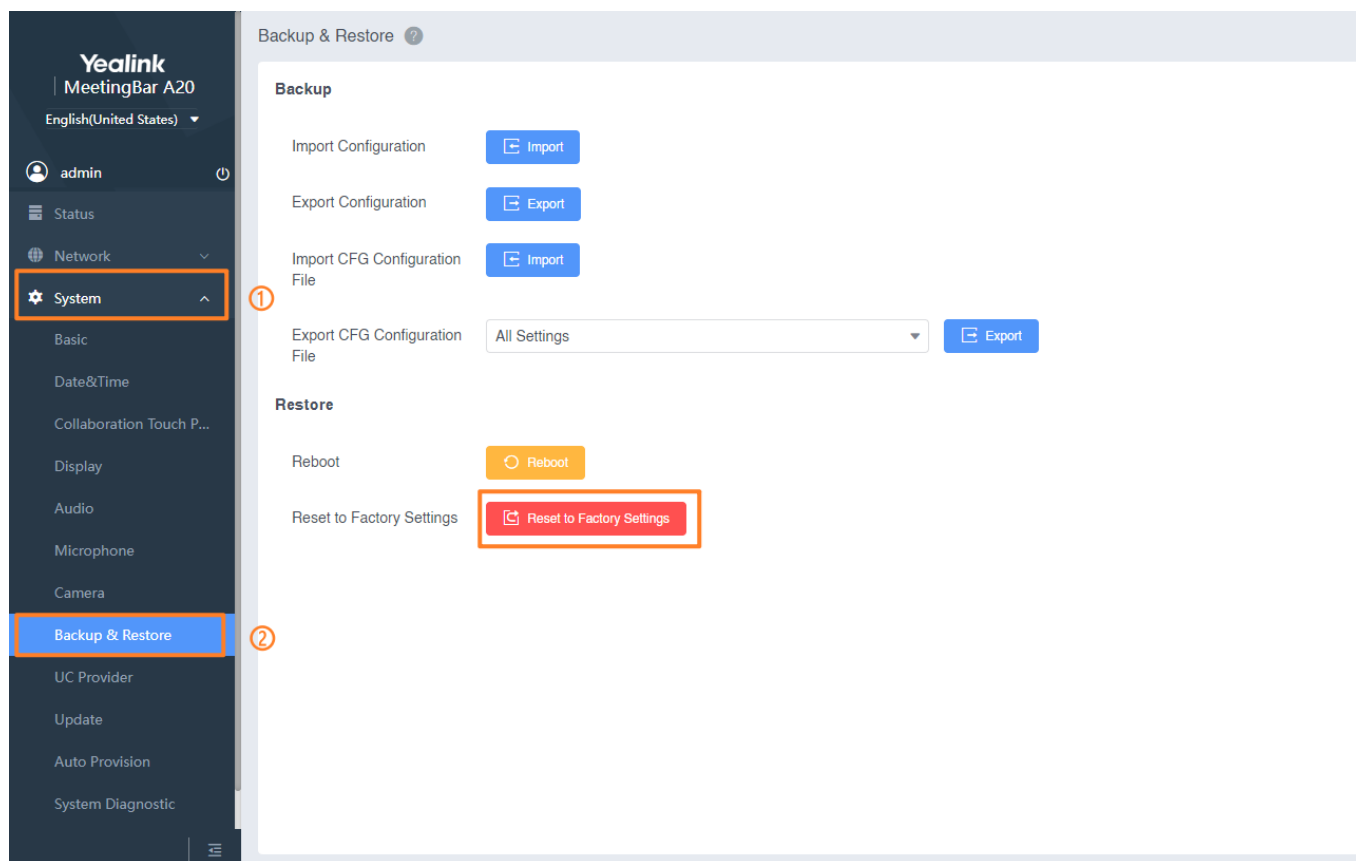
2. Select **Reset to factory**.



Configure via Web User Interface

1. Go to **System > Backup & Restore** on the web user interface.

2. Select **Reset to Factory Settings**.



Reset via Rest Hole

If you forget the password and cannot restore the factory settings on the LCD screen, you can use a paper clip or toothpick to press and hold the Reset hole on the back of the MeetingBar AX0 or CTP18 for 10 seconds. For more information about the position of the Reset hole, please refer to [Hardware Introduction](#).

FAQ

How to enter the recovery mode of A10/A20/A30/CTP18?

If the device system cannot be used, you can enter the recovery mode and switch to the backup system. The MeetingBar AX0 and CTP18 are independent and can be operated separately as required. For more information, please refer to [How to recover A20/A30/CTP18](#).

System Diagnostic & Export Log

Introduction

You can capture packets in two ways: capturing the packets via the web user interface or using the Ethernet software. You can analyze the captured packets for troubleshooting purposes.

Capture Packets

Configure via Web User Interface

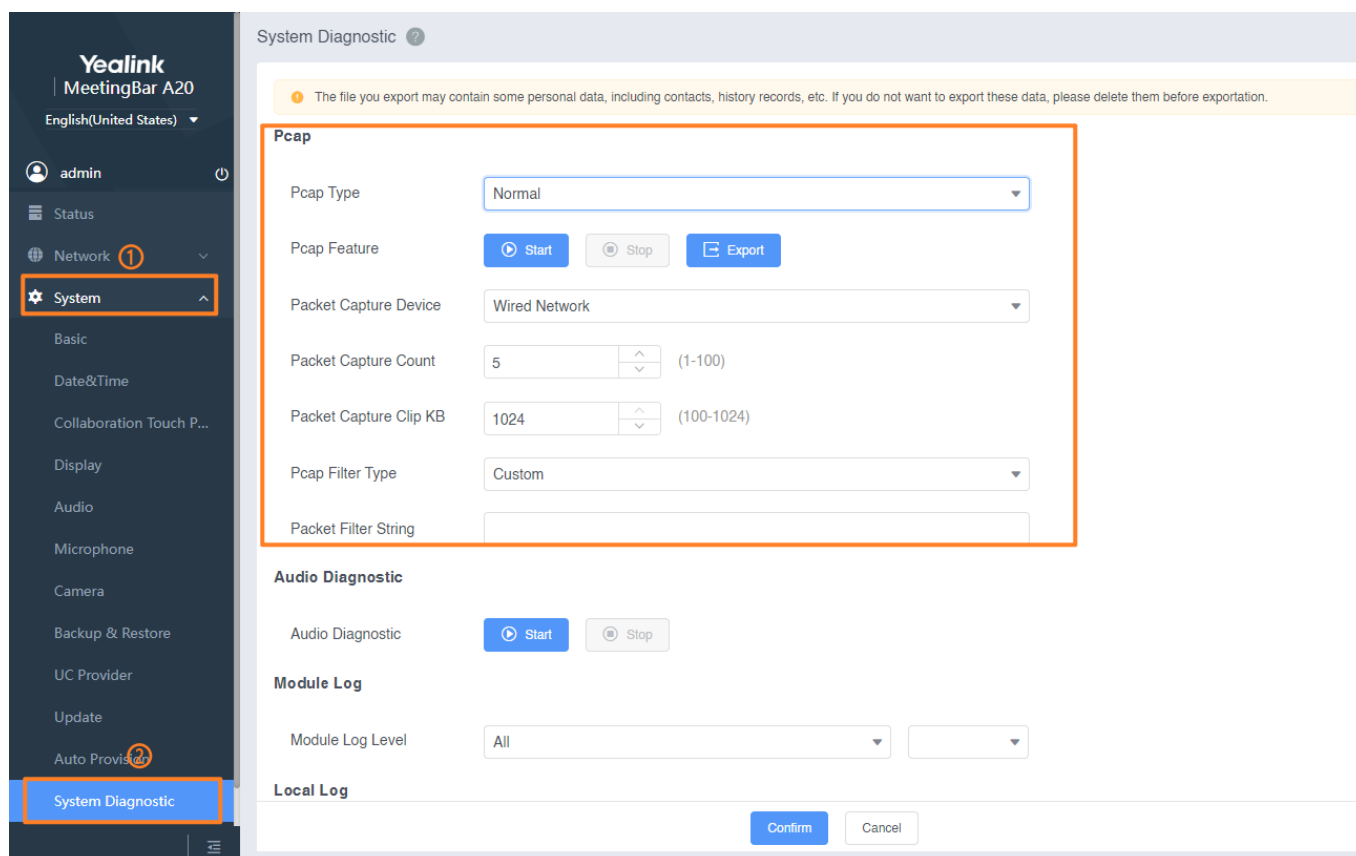
1. Go to **System > System Diagnostic** on the web user interface.
2. Select **Normal/Enhanced** from **Pcap Type** drop-down menu.

NOTE

Selecting normal or enhanced packet capture has the same content. Enhanced packet capture can continue to capture packets with no capacity limit, and the maximum capacity of normal packet capture is 1MB.

In the **Pcap Feature** field, click **Start** to start capturing signal traffic.

3. Reproduce the issue to get stack traces.
4. Click **Stop** in the **Pcap Feature** field to stop capturing.
5. Click **Export** to save the file to your local system.



Capture String

You can customize the packet capture string to capture specific packets.

The syntax of the captured string is:

Protocol + Direction + Host(s) + Value + Logical Operations + Other Expression Protocol

Related syntax:

Syntax	Description
Protocol	<p>Possible values: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp If no protocol type is specified, the default is to capture all supported protocols.</p> <div> <p>NOTE</p> <p>The packet capture string does not support application layer protocols, such as http, dns, sip, etc.</p> </div>
Direction	<p>Possible values: src, dst, src and dst, src or dst If no direction is specified, the default is to use “src or dst” as the key. “host 10.2.2.2” is equivalent to “src or dst host 10.2.2.2” .</p>
Host(s)	<p>Possible values: net, port, host, port range The “host” keyword is used by default, and “src 10.1.1.1” is equivalent to “src host 10.1.1.1” .</p>
Logical Operations	<p>Possible values: not, and, or Not (“not”) has the highest priority. Or (“or”) and (“and”) have the same precedence, and operations are performed from left to right. For example, “not tcp port 3128 and TCP port 23” is equivalent to “(not tcp port 3128) and TCP port 23” , “not tcp port 3128 and TCP port 23” is not equal to “not (tcp port 3128 and tcp port 23)” .</p>

For example: host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst port range 10000 and dst net 10.0.0.0/8 means that the captured IP is 10.4.1.12 or the source IP is located in the network 10.6.0.0/16, and the TCP of the destination IP All packets whose port number is between 200 and 10000 and whose destination IP is within the network 10.0.0.0/8.

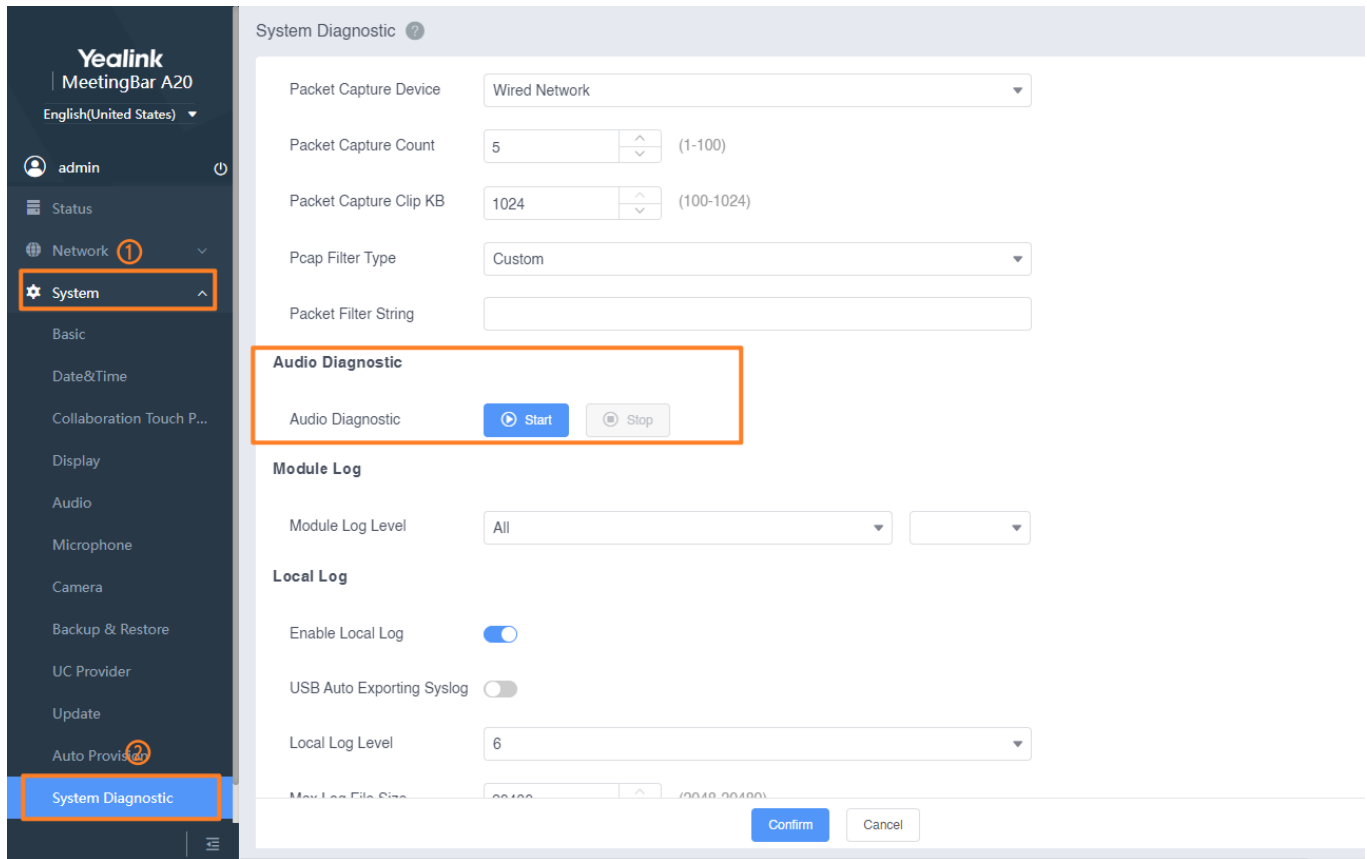
Audio Collection

Check whether the audio output device and audio input device of the device are normal.

Configure via Web User Interface

1. Go to **System > System Diagnostic** on the web user interface.
2. Click **Start** in **Audio Diagnostic**.
3. Speak to the microphone connected to the device.

4. Click **Stop** to stop collecting audio data and automatically generate .dat file to the local PC.

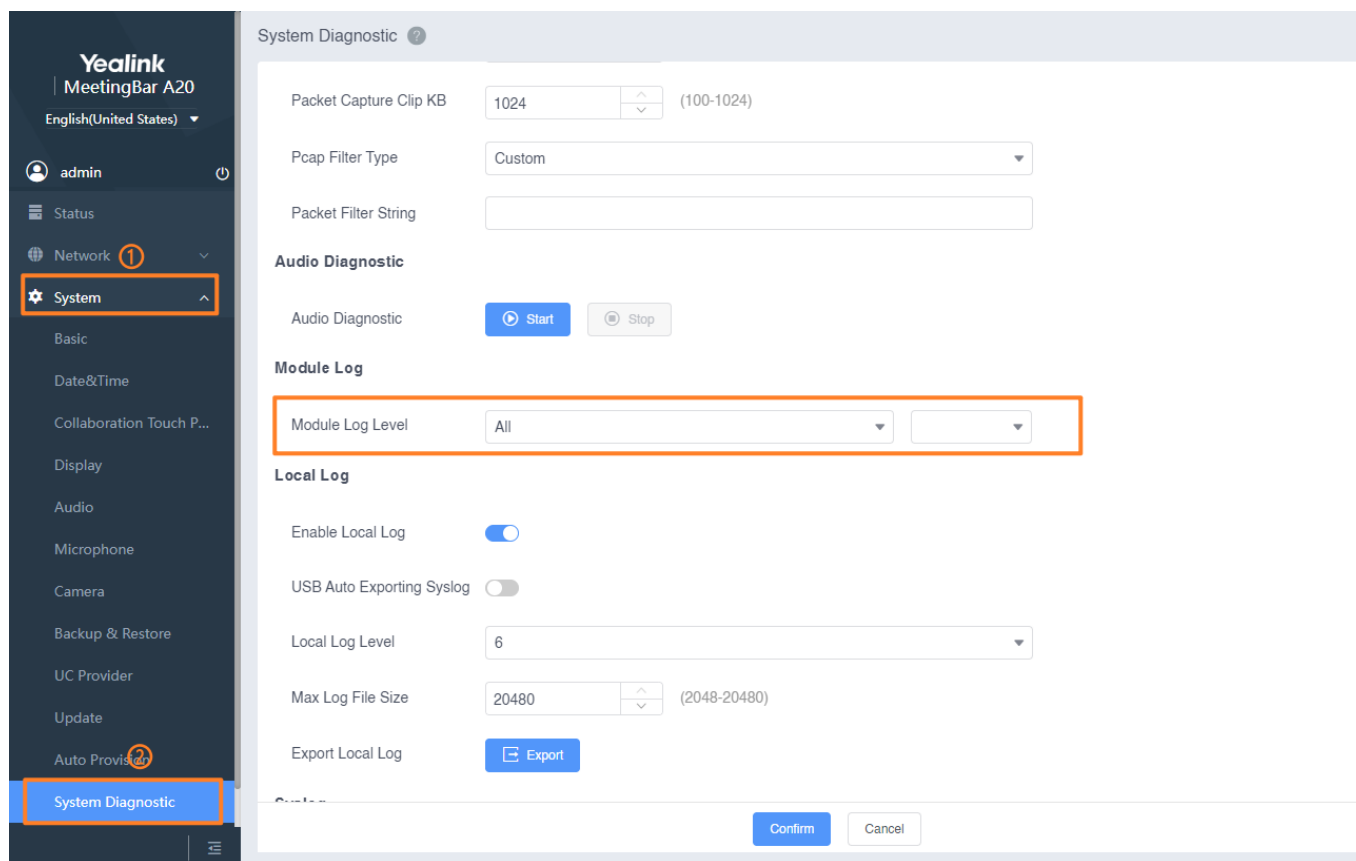


Module Log

Configure via Web User Interface

1. Go to **System > System Diagnostic** on the web user interface.

2. Set Module Log Level.



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

Configure via Web Interface

1. Go to **System > System Diagnostic** on the web user interface.
2. Set **Local Log Level** to 6.
3. If there is a problem with audio (such as noise or voice delay), click **Start** on the right side of **Audio Diagnostic** to reproduce the problem. And click **Stop** to export the diagnostic file automatically after completing the reproduction.
4. Click **Start** on the right side of **Export All Diagnostic Files** to reproduce the problem. And click **Stop** to export all diagnostic files after completing the reproduction.

5. Click **Export** to download the diagnostic file to your local system.

Auto Provisioning

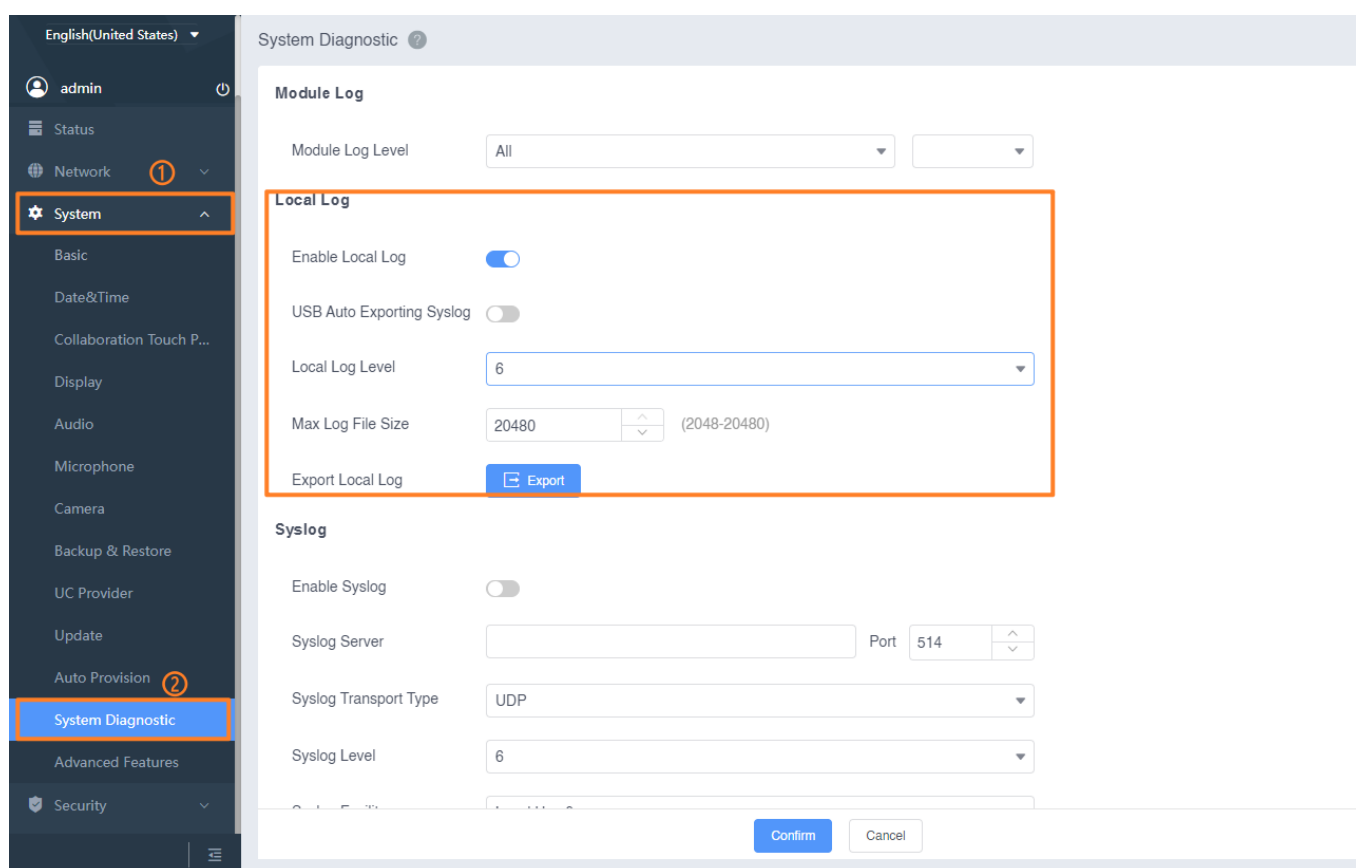
Parameter	Description	Optional Value
static.local_log.enable	<p>It enables or disables the device to record logs locally.</p> <div> NOTE We recommend you not disable this feature. </div>	<p>0: Disabled, the device will stop locally recording logs to the log files. The log files recorded before are still kept on the device.</p> <p>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.</p> <p>Default: 1</p>
static.local_log.level	<p>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.</p>	<p>0: the system is unusable</p> <p>1: action must be taken immediately</p> <p>2: critical condition</p> <p>3: error conditions</p> <p>4: warning conditions</p> <p>5: normal but significant condition</p> <p>6: informational</p> <p>Default: 6</p>

static.local_log.max_file_size	<p>It configures the maximum size (in KB) of the log files that can be stored on the device.</p> <p>When this size is about to be exceeded,</p> <p>(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 backed up.</p> <p>(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.</p>	<p>Integer from 2048 to 20480.</p> <p>Default: 20480</p>
static.auto_provision.local_log.backup.enable	<p>It enables or disables the device to upload the local log files to the provisioning server or a specific server.</p> <div> <p>NOTE</p> <p>The upload path is configured by the parameter “static.auto_provision.local_log.backup.path” .</p> </div>	<p>0: Disabled</p> <p>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:</p> <ul style="list-style-type: none"> - 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” . <p>Default: 0</p>
static.auto_provision.local_log.backup.upload_period	<p>It configures the period (in seconds) of the local log files uploads to the provisioning server or a specific server.</p> <div> <p>NOTE</p> <p>It works only if “static.auto_provision.local_log.backup.enable” is set to 1 (Enabled).</p> </div>	<p>Integer from 30 to 86400.</p> <p>Default: 30</p>

static.auto_provision.local_log.backup.path	<p>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 the 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.</p> <p>Example: static.auto_provision.local_log.backup.path = tftp://10.3.6.133/upload/</p> <div> <p>NOTE</p> <p>It works only if “static.auto_provision.local_log.backup.enable” is set to 1 (Enabled).</p> </div>	URL within 1024 characters, null by default.
static.auto_provision.local_log.backup.append	<p>It configures whether the uploaded local log files overwrite the existing files or are appended to the existing files.</p>	<p>0: Overwrite 1: Append (not applicable to TFTP Server) Default: 0</p>
static.auto_provision.local_log.backup.append.limit_mode	<p>It configures the behavior when local log files on the provisioning server or a specific server reach the maximum file size.</p>	<p>0: Append Delete; the server will delete the old log, and the device will continue uploading the log. 1: Append Stop; the device will stop uploading the log. Default: 0</p>
static.auto_provision.local_log.backup.append.max_file_s	<p>It configures the maximum size (in KB) of the local log files that can be stored on the provisioning server or a specific server.</p>	<p>Integer from 200 to 65535. Default: 1024</p>
static.auto_provision.local_log.backup.bootlog.upload_wait_tim	<p>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.</p>	<p>Integer from 1 to 86400. Default: 120</p>

Export Log Files to Local PC

1. Go to **System > System Diagnostic > Local Log** on the web user interface.
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 value 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 save the file to your local system.



View Local Log Files

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

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

- <6+info>

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

```

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

```

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

```

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

```

Syslog Log

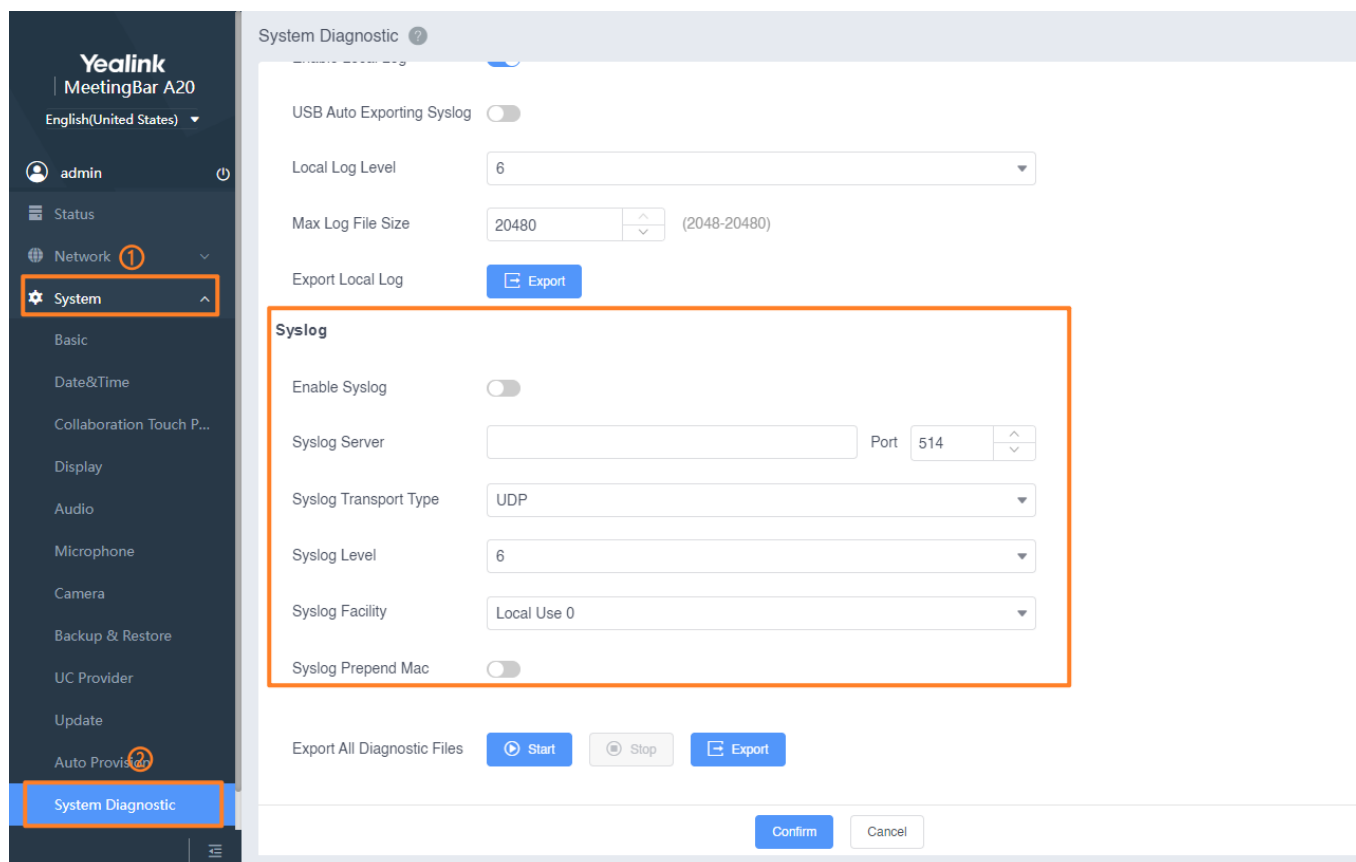
You can also configure the device to send Syslog messages to a Syslog server in real-time.

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

Syslog Logging Configuration

Configure via Web Interface

1. Go to **System > System Diagnostic** on the web user interface.
2. Set the **System Log Level** to 6.
3. If there is a problem with audio (such as noise or voice delay), click **Start** on the right side of **Audio Diagnostic** to reproduce the problem. And click **Stop** to export the diagnostic file automatically after completing the reproduction.
4. Click **Start** on the right side of **Export All Diagnostic Files** to reproduce the problem. And click **Stop** to export all diagnostic files after completing the reproduction.
5. Click **Export** to download the diagnostic file to your local PC and provide the file to Yealink technical support.



Auto Provisioning

Parameter	Description	Optional Value
-----------	-------------	----------------

static.syslog.enable	It enables or disables the device to upload log messages to the Syslog server in real-time.	0: Disabled 1: Enabled Default: 0
static.syslog.server	It configures the IP address or domain name of the Syslog server when exporting logs to the Syslog server.	IP address or domain name, empty is the default.
static.syslog.server_port	It configures the port of the Syslog server. Example: static.syslog.port = 515	Integer from 1 to 65535. Default: 514
static.syslog.transport_type	It configures the transport protocol that the device uses when uploading log messages to the Syslog server.	0: UDP 1: TCP 2: TLS Default: 0
static.syslog.level	It configures the lowest level of Syslog information that displays in the Syslog.	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

static.syslog.facility	<p>It configures the facility that generates the log messages.</p> <div> <p>NOTE</p> <p>For more information, refer to RFC 3164.</p> </div>	<p>0: kernel messages 1: user-level messages 2: mail system 3: system daemons 4: security/authorization messages (1) 5: messages generated internally by syslogd 6: line printer subsystem 7: network news subsystem 8: UUCP subsystem 9: clock daemon (2) 10: security/authorization messages (1) 11: FTP daemon 12: NTP subsystem 13: log audit (1) 14: log alert (1) 15: clock daemon (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)</p>
static.syslog.prepend_mac_address.enable	It enables or disables the device to prepend the MAC address to the log messages exported to the Syslog server.	<p>0: Disabled 1: Enabled Default: 0</p>

View System Log

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:

FAQ

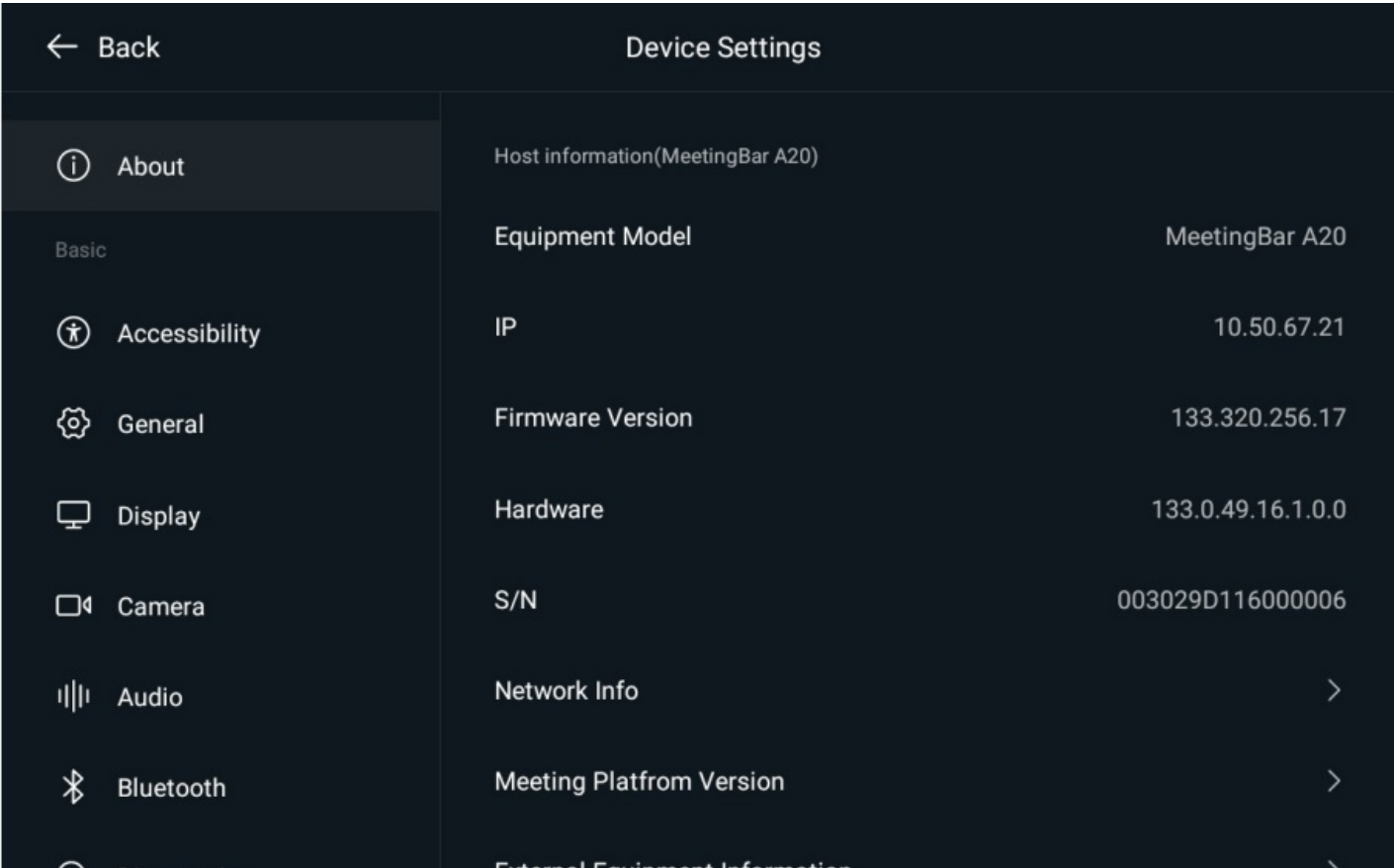
How to Export Audio Diagnostic Files

Introduction

- 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)

View via Device Interface

129



View via Web User Interface

- 1. Open a web browser on your computer.

Enter the IP address in the browser’ s address bar and press **Enter**.

For example, “http://192.168.0.10” for IPv4.
- 2. Enter the user name (admin) and password (0000) on the login page.
- 3. Click **Login**.
The device status is displayed on the first page of the web user interface.

Yealink

MeetingBar A20

English(United States)

admin

Status

Network

System

Security

Status ?

System

Model	MeetingBar A20	MAC Address	80:5E:C0:6A:37:21
Android OS	10	S/N	003029D116000006
Firmware Version	133.320.256.17	Wi-Fi Mac Address	00:0A:F5:8E:12:5A
Hardware Version	133.0.49.16.1.0.0	Uptime	2 Day 07 Hour 36 Min
Product ID	202304061034	Available Storage	45.28 G
Vendor Version	1449/1.0.96.2023031201		
Company Portal Version	5.0.5484.0		
Partner Version	v1.1.252.187-2-g9d576b79.20230404181036		

Wired Network

Status	Connected	Protocol Version	IPv4
IPv4			
IP Type	DHCP	Gateway	10.50.67.254
IP Address	10.50.67.21	Primary DNS	10.100.1.10
Subnet Mask	255.255.255.0	Secondary DNS	192.168.1.22


Touch Panel Configuration

Introduction

You can view the touch panel that is paired with the current MeetingBar A10/A20/A30.

CTP18 Configuration

Configure via Web User Interface

1. On the web user interface, go to **System > Collaboration Touch Panel**.
2. Configure the **Connected Devices**.
3. You can view the MAC address, connection method, and connection status of the paired touch panel (CTP18).
4. Click  to unpair the touch panel from the MeetingBar.

Security Configuration

Administrator Password

Introduction

The default administrator username is “admin” and the password is “0000”. Only users with administrator privileges can modify the administrator password. For security reasons, we recommend you change the administrator password as soon as possible. The administrator password for the MeetingBar supports ASCII characters 32-126 (0x20-0×7E).

Configure via Device Interface

1. On the CTP18 or with the remote control, go to **More > Settings > Device Settings > System > Password Reset** (default password: 0000).
2. Enter the current password, new password, and confirm the password and select **Save** to complete the configuration.

The screenshot shows the 'Device Settings' menu with a left sidebar containing options: Camera, Audio, Bluetooth, Diagnostics, Advanced, Network, Upgrade, System (highlighted), and Debug. The main area is titled 'Password Reset' and includes a 'Save' button in the top right. It contains three input fields: 'Current Password' (placeholder: Please enter current password), 'New Password' (placeholder: Please enter new password), and 'Confirm Password' (placeholder: Please enter confirm password). Below these fields, a message states: 'Please use a password that complies with complex password rules, as follows:' followed by a list of requirements: '* 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;', and '* At most 3 consecutive repeating characters .'.

Configure via Web User Interface

1. Go to **Security > Password** on the web user interface.

2. Enter the current password, new password, and confirm the password and click **Confirm** to complete the configuration.

Yealink
MeetingBar A20
English

admin

Status

Network

System

Security

Password

Trusted Certs

Server Certs

Client Certs

Password ?

User Type: admin

Old Password

New Password

Confirm Password

Please use a password that complies with complex password rules, as follows:

- 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.

Auto Provisioning

Parameter	Description	Optional Value
static.security.user_name.admin	It configures the administrator's user name for the device's web user interface access.	String within 32 characters. Default: Admin
static.security.user_password	It configures the password of the user or administrator.	String within 32 characters.

FAQ

How to push the admin password to MeetingBar A20/A30 in TAC?

Forgot your admin password?

You can reset user settings or restore factory settings, and the default password is 0000.

To ensure device security, please change the password in time.

The default password is 0000. If you forget the password, please refer to the [Backup & Reset](#) to restore the device to factory settings. To ensure device security, please change the password in time.

License

Introduction

Terminal device licenses are divided into:

- License for converting demo machines to official machines: If the current device you are using is a demo machine, which is used for demonstrating features to clients, the display will show “Not for sale, for demonstration only, no after-sales service!” You can contact Yealink’s technical support team to obtain a permanent license. Importing the device type license can transform the demo machine into an official machine for customer use.
- License for switchable system version: If you need to switch system versions, you need to import the certificate that can switch the system version before upgrading. For example, if you’re switching from the VCS version to the Teams version, you need to import the Teams version certificate and then upgrade the firmware to the Teams version.

i NOTE

- If there is no license or the license expires, you can enter the web user interface to configure parameters, upload licenses, and upgrade firmware.
- When the device prompts that the device expires and needs to import licenses, please contact Yealink technical support to obtain a new license.
- Do not modify the license arbitrarily, otherwise the license file will be unusable.

License

Configure via Web Interface

1. Save the license on your PC.
2. Go to **Security > Certs** on the web user interface.
3. Click **Import** to upload the license.

Auto Provisioning

Parameter	Description	Optional Value
lync_license_dat.url	It configures the URL for uploading licenses.	String within 99 characters.

Certificate

Introduction

Certificates include trusted certificates, server certificates and client certificates. Ensure the normal and safe use of

the device by configuring and uploading certificates.

Trusted certificates

When the system serves as a TLS client and requests a TLS connection with a server, the system should verify the server certificate sent by the server to decide whether it is trusted based on the trusted certificates list.

The trusted certificates list contains the default and the custom certificates.

- **Default Certificate:** The commonly used CA Certificates built-in Yealink video conferencing system.
- **Custom Certificate:** You can upload up to 10 trusted certificates with a size of no more than 5 MB to the system. The CA certificate types supported by the device are: *.pem*, *.cer*, *.crt* and *.der*.

NOTE

- Before adding a certificate, please confirm the security of the certificate. We recommend you import a certificate issued by a security authority to avoid risks.
- Yealink devices have the most commonly used CA certificates built-in. We cannot cover all CA certificates due to memory limits. If the certificate you use does not appear in the default certificate list, you can contact your local distributor to provide and upload the certificate to your device.

For the common trusted CA certificates built-in device, please refer to, please refer to Built-in Trusted CA Certificates.

Configure via Web User Interface

1. Save the obtained certificate locally on your PC.
2. Go to **Security > Trusted Certs** on the web interface.
3. Click **Import** to import the certificate.

NOTE

The format of the trusted certificate files must be *.pem* or *.cer*, and the maximum file size is 5 MB. You can upload up to 10 certificates.

4. Configure the parameters related to the trusted certificate.

The screenshot displays the 'Trusted Certs' configuration page in the Yealink MeetingBar A20 admin interface. The left-hand navigation menu shows 'Security' and 'Trusted Certs' as active sections. The main content area includes an 'Import' button, tabs for 'Custom CA' and 'Phone CA', and a table for managing certificates. The table has columns for '#', 'Issued to', 'Issued by', and 'Expiration', but it is currently empty. Below the table, there are three configuration options: 'Only Accept Trusted Certificates' (a toggle switch that is turned on), 'Common Name Validation' (a toggle switch that is turned off), and 'CA Certificates' (radio buttons for 'Default Certificates', 'Custom Certificates', and 'All Certificates', with 'All Certificates' selected).

Parameter	Description
Only Accept Trusted Certificates	It enables or disables the IP phone to only trust the server certificates in the Trusted Certificates list. If disabled, devices can connect to the server regardless of whether the server certificate sent by the server is valid. If enabled, devices verify that the server certificate is trusted based on the list of trusted CA certificates. Only the authentication is passed, the device can connect to the server.
Common Name Validation	It enables or disables the IP phone to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server.
CA Certificates	It configures the type of certificates in the Trusted Certificates list for the IP phone to authenticate for TLS connection. - Default Certificate: The device uses the built-in CA certificate to verify that the server is trusted. - Custom Certificate: The device uses the uploaded CA certificate to verify that the server is trusted. - All Certificates: The device uses the built-in and custom CA certificates to verify that the server is trusted.

Auto Provisioning

Parameter	Description	Optional Value
static.security.trust_certificates	It enables or disables the device to only trust the server certificates listed in the Trusted Certificates list.	0: Disabled 1: Enabled Default: 1

static.security.ca_cert	It configures the type of certificates in the Trusted Certificates list for the device to authenticate for TLS connection.	0: Default Certificates 1: Custom Certificates 2: All Certificates Default: 2
static.security.cn_validation	It enables or disables the device to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server.	0: Disabled 1: Enabled Default: 0
static.trusted_certificates.url	It configures the access URL of the custom trusted certificate used to authenticate the connecting server.	URL within 511 characters, empty is default.

Built-in Trusted CA Certificates

1. Save the obtained certificate locally on your PC.
2. Go to **Security > Trusted Certs** on the web user interface.
3. Click **Phone CA** to view the trusted CA certificate built-in the device.

Trusted Certs ?

Import

Custom CA Phone CA

#	Issued To	Issued By
1	E-Tugra Certification Authority	E-Tugra Certification Authority
2	Hongkong Post Root CA 1	Hongkong Post Root CA 1
3	Security Communication RootCA1	Security Communication RootCA1
4	Symantec Class 3 Secure Server CA - G4	VeriSign Class 3 Public Primary Certification Authority - G5
5	HydrantID SSL ICA G2	QuoVadis Root CA 2
6	Trustis FPS Root CA	Trustis FPS Root CA
7	Zultys	Zultys
8	Trusted Secure Certificate Authority 5	USERTrust RSA Certification Authority
9	InCommon RSA Server CA	USERTrust RSA Certification Authority
10	RILROOTCA	RILROOTCA

Total: 167 < 1 2 3 ... 17 > 10 / Page GoTo 1 Page

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 server certificate contains the default and User certificates. You can customize the certificate type sent by the system to the client for authentication.

- **Default certificate:** The terminal has two built-in default certificates: a unique server certificate (a certificate issued by the Yealink Certificate Authority based on an individual MAC address of the terminal) and a generic server certificate (a certificate issued by the Yealink Certificate Authority). A unique server certificate is

preferred on the terminal to authenticate the client.

- **User Certificate:** You can upload up to 1 trusted size of no more than 5 MB Custom the system. The new one will override the old server certificate. The format of the server certificate files must be *.pem or, and cer.

NOTE

- Contact your system administrator or local dealer to download the certificate. Before you add a certificate, confirm the security of the certificate.
- We recommend you import certificates issued by security authorities to avoid risks.

Configure via Web User Interface

1. Save the obtained certificate locally on your PC.
2. Go to **Security > Server Certs** on the web user interface.
3. Click **Import** to import the custom certificate.

NOTE

The format of the trusted certificate files must be *.pem* or *.cer*, and the maximum file size is 5 MB. You can upload up to one server certificate.

The screenshot displays the Yealink MeetingBar A20 web user interface. On the left is a dark sidebar with the Yealink logo and 'MeetingBar A20'. Below this, it shows 'English(United States)' and a user profile for 'admin'. A menu lists 'Status', 'Network', 'System', 'Security' (highlighted with an orange box), 'Password', 'Trusted Certs', 'Server Certs' (highlighted with an orange box), and 'Client Certs'. The main content area is titled 'Server Certs' with a help icon. It features a blue 'Import' button and a table with columns '#', 'Issued to', and 'Issued by'. Below the table, there are three radio button options: 'Device Certificates' (disabled), 'Default Certificates' (selected), and 'Custom Certificates' (disabled).

Auto Provisioning

Parameter	Description	Optional Value
static.security.dev_cert	It configures the type of device certificates for the device to send for TLS authentication.	0: Default Certificates 1: Custom Certificates
static.server_certificates.url	It configures the access URL of the certificate the device sends for authentication.	URL within 511 characters
static.phone_setting.reserve_certs_enable	It enables or disables the device to reserve custom certificates after it is reset to factory defaults.	0: Disabled 1: Enabled

Client Certificate

The device supports users to install custom client certificates, and only computers and smartphones that install the corresponding certificates can log in to the web user interface of the device.

NOTE

If the device does not upload a custom client certificate, the web user interface can be freely accessed.

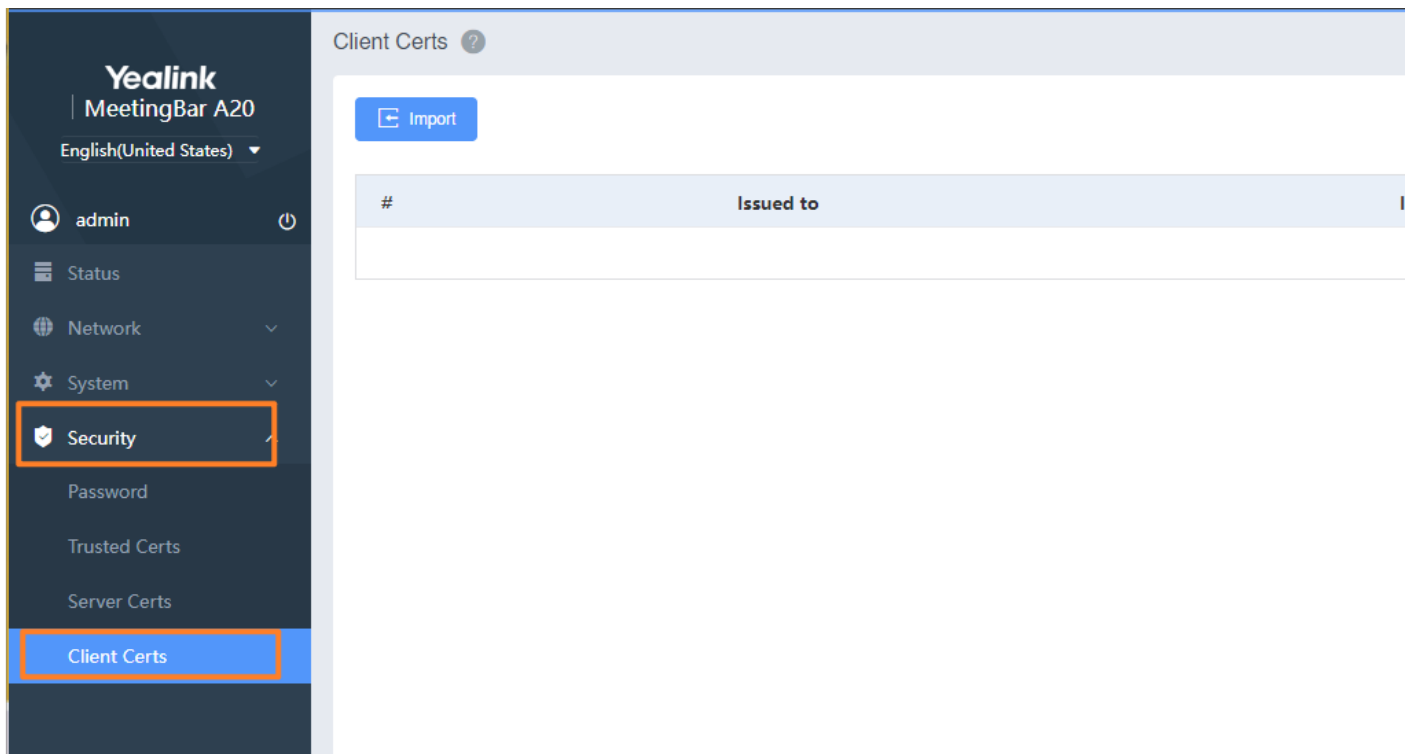
Configure via Web User Interface

1. Save the obtained certificate locally on your system.
2. Go to **Security** > **Client Certs** on the web user interface.
3. Click **Import** to import the client certificate.

Install the same certificate on your PC or smartphone.

NOTE

The format of the trusted certificate files must be .pem, .cer, .crt, and *.der, and the maximum file size is 5 MB. You can upload up to one server certificate.



Auto Provisioning

Parameter	Description	Optional Value
static.client_certificates.url	It configures the URL to upload the client certificate.	URL within 511 characters

YMCS Platform

YMCS Platform

Introduction

Yealink Management Cloud Service (YMCS) integrates device deployment, management, analysis, active monitoring, fault diagnosis, account registration, RPS service, order management and other functions. Enterprise administrators can centrally configure and update Yealink products deployed on the platform or use the RPS redirection function provided by the platform to manage devices.

How to Use

NOTE

Please ensure all devices are powered on and connected to the network before starting.

You can register MeetingBar A10/A20/A30 to the Yealink Management Cloud Service platform for unified management. For more information, please refer to [AX0 Registration to YMCS](#).