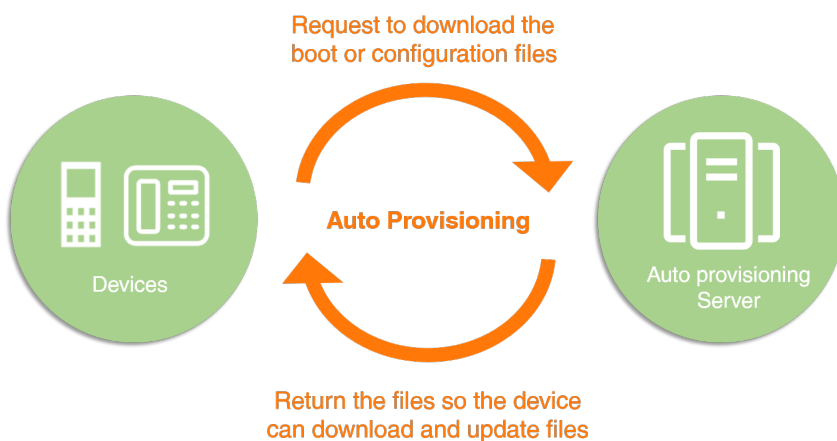


Configuration Methods

Introduction

Before we move on to how to administer the phone, you need to know the supported configuration methods.

- Auto Provisioning
- Web User Interface
- Device User Interface

Configuration Methods	Description	Applicable Scenarios
Auto provisioning	Auto provisioning is a process that allows you to make phones to request and download the boot or configuration files from the provisioning server. You can use this feature to change some configurations for batches of phones. For more information on how to set up an auto-provisioning server, see Auto provision guide. 	Mass configuration
Web user interface	You can use the phone web user interface to change some configurations for the phone.	Single configuration
Device user interface	You can use the phone screen to change some phone configurations.	Single configuration

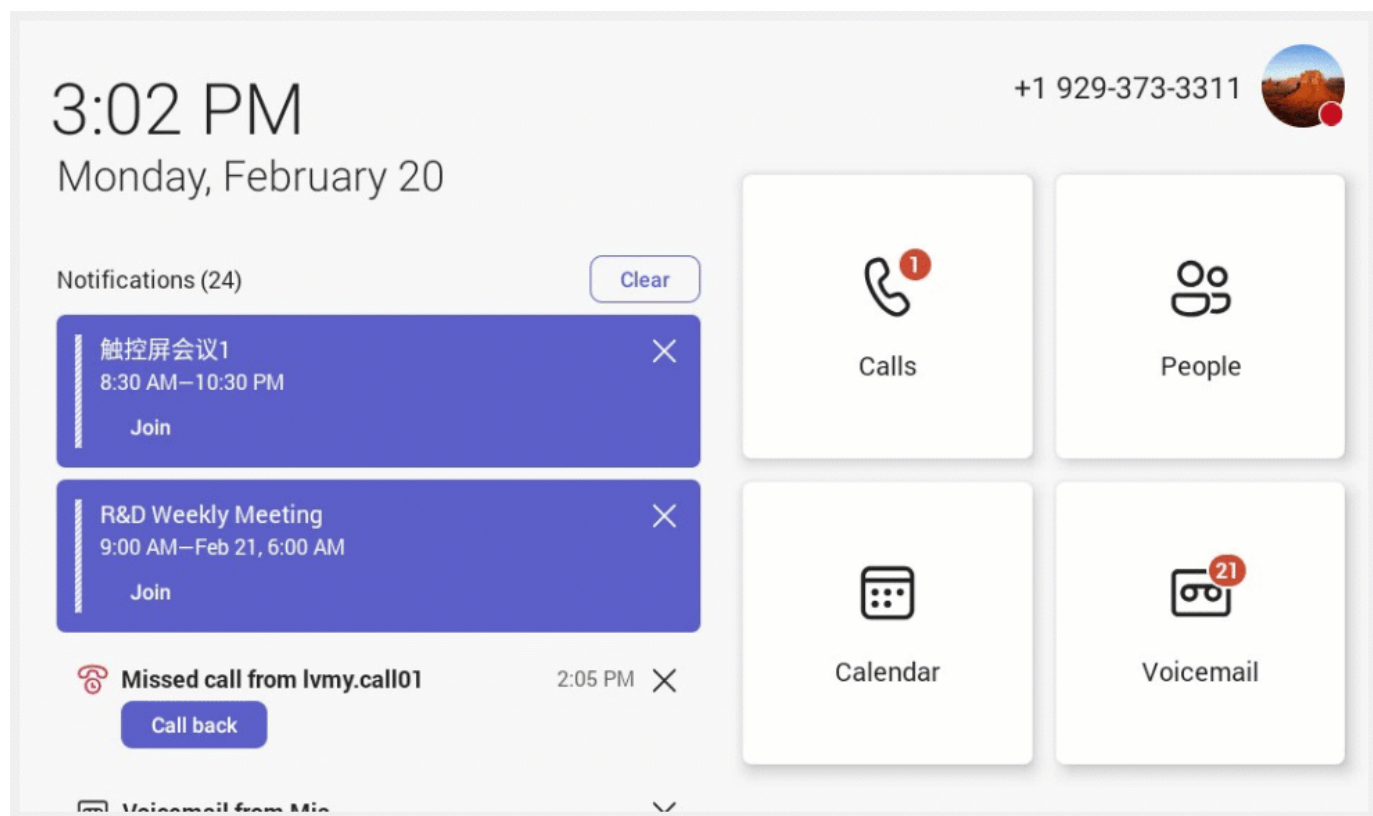
Access the Phone IP Address

You must get the IP address before logging in to the [phone web user interface](#).

Procedure

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > About > IPv4 , then you can get the phone IP address.	Go to  > Settings > Settings > Device Settings > About > IPv4 , then you can get the phone IP address.



Log In to the Web User Interface

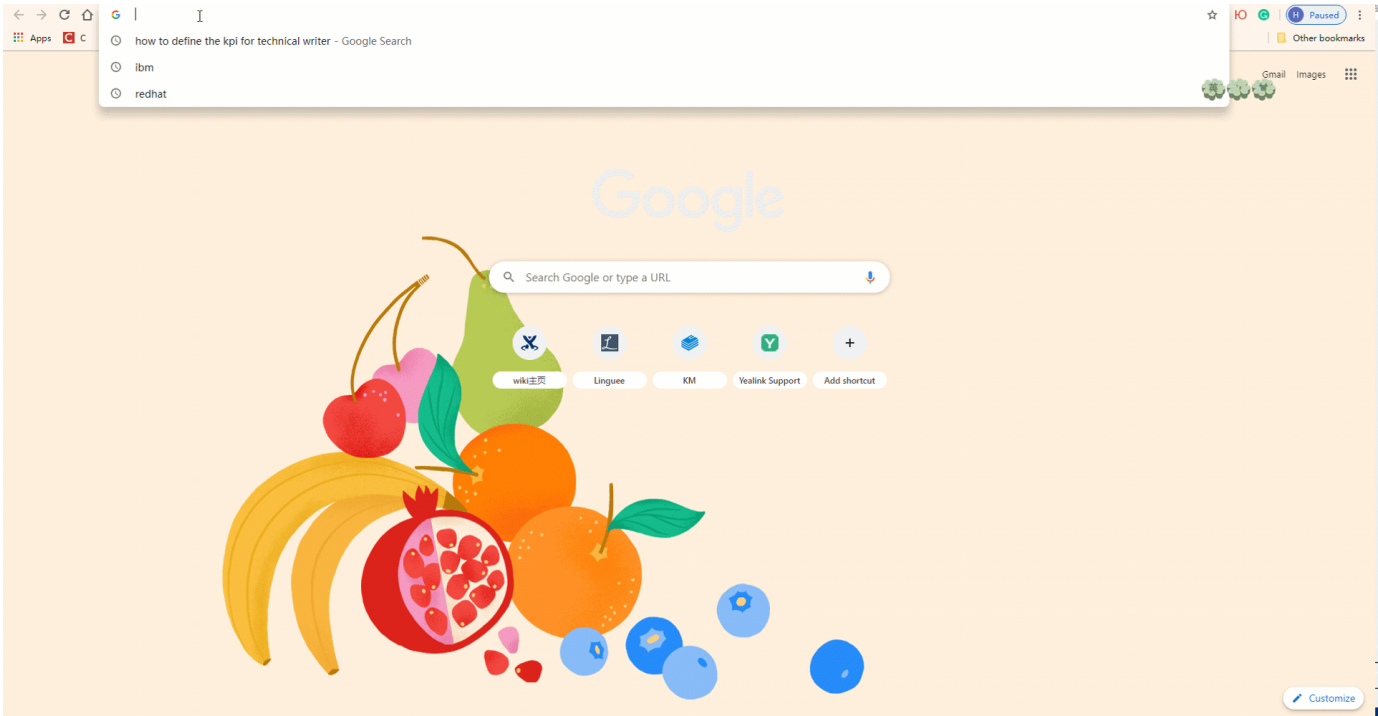
To use the phone web user interface to configure the phone, you need to log into the web user interface.

Before you begin

[Get the phone IP address.](#)

Procedure

1. Enter the "https:// IP address" in the address bar.
2. Enter the admin username and password (default username and password: **admin**) to log in.
3. After that, you can use the web user interface to configure the phone.

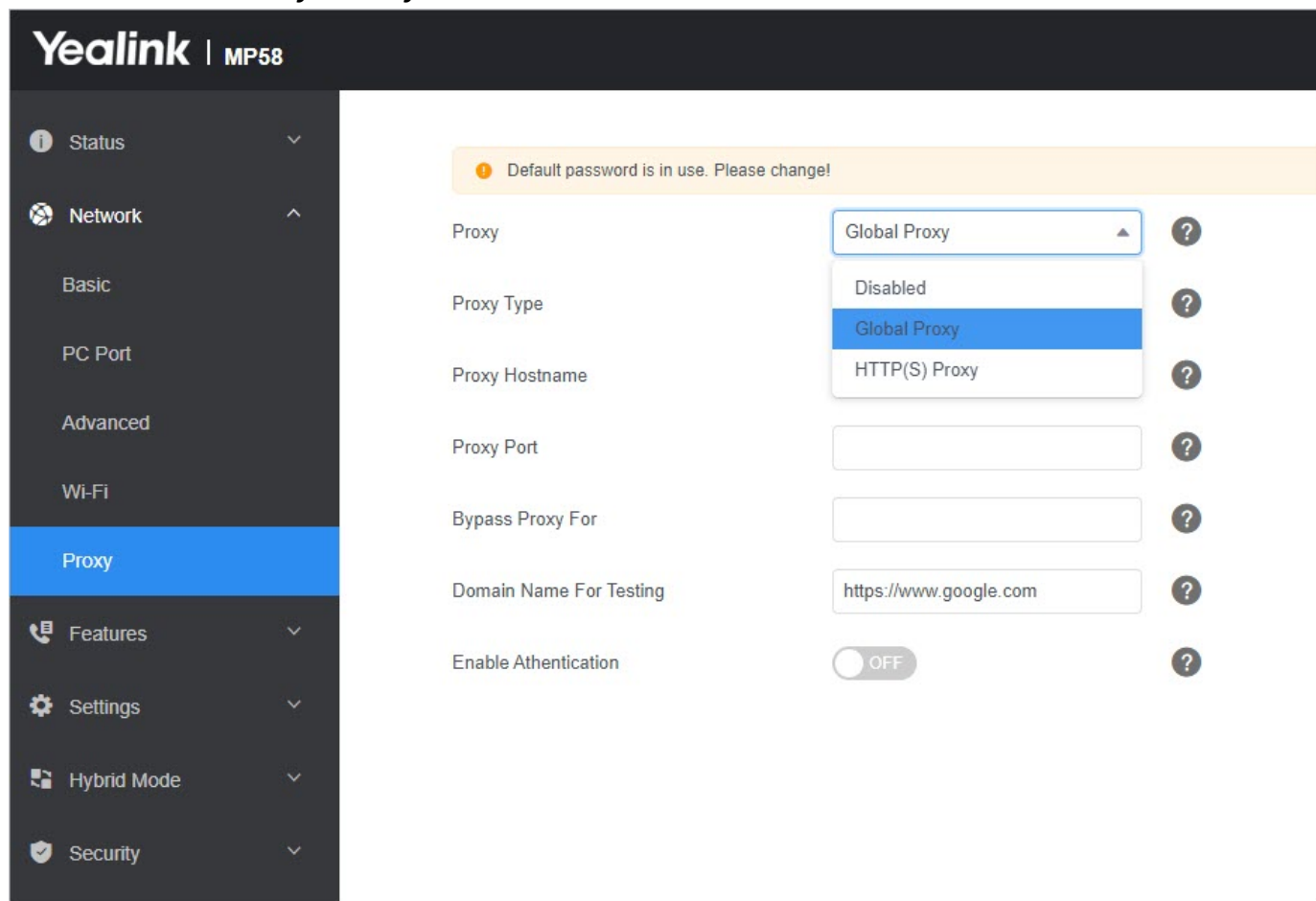


Configure Proxy Server

Via Web User Interface

Procedure

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Network > Proxy > Proxy**.



Via Device User Interface

Procedure

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Proxy (Admin only, default password: admin) > Proxy .	Go to  > Settings > Device Settings > Proxy (Admin only, default password: admin) > Proxy .

 Accessibility  Reboot  About  Upgrade Admin only  Network  Proxy  Debug  Admin Password	Proxy None
--	--

Via Auto Provisioning

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

```
static.network.proxy.mode
static.network.proxy.type
static.network.proxy.hostname
static.network.proxy.port
static.network.proxy.bypass_address
static.network.proxy.test_address
static.network.proxy.enable
static.network.proxy_pac.url
static.network.proxy.wpad
static.network.proxy.http.set_from
static.network.proxy.username
static.network.proxy.password
static.network.proxy.sip.enable
```

Parameters	Permitted Values	Default	Description
static.	0- Disabled	2	It enables or disables the proxy server.

network.proxy.mode[1]	1- Global proxy, you can manually configure the proxy server information. 2- HTTP(S) proxy, you can obtain proxy server information through PAC file.		
static.network.proxy.type	0- SOCKS5 1- HTTP CONNECT	0	It configures the proxy type.  NOTE It works only if "static.network.proxy.mode" is set to 1 (Enabled).
static.network.proxy.host.name	String within 99 characters	Blank	It configures the IP address or domain name of the proxy server.  NOTE It works only if "static.network.proxy.mode" is set to 1 (Enabled).
static.network.proxy.port[1]	Integer from 1 to 65535	Blank	It configures the port of the proxy server.  NOTE It works only if "static.network.proxy.mode" is set to 1 (Enabled).
static.network.proxy.bypass_address	URL within 511 characters	Blank	It configures the host name or IP address that does not apply to the proxy server to access. Multiple host names or IP addresses are separated by commas.  NOTE It works only if "static.network.proxy.mode" is set to 1 (Enabled).
static.network.proxy.	URL within 511 characters	http://www	It configures the test URL for the proxy server. After connecting to the proxy server, the phones try to send a network request to the specified URL. If the URL cannot be

test_address		.google.com	accessed, the phone fails to connect to the proxy server.  NOTE It works only if "static.network.proxy.mode" is set to 1 (Enabled).
static.network.proxy.enable	0 -Disabled 1 -Enabled	0	It enables or disables the proxy server authentication.  NOTE It works only if "static.network.proxy.mode" is set to 1 (Enabled).
static.network.proxy.pac.url	URL within 511 characters	Blank	It configures the URL for the PAC file location.  NOTE It works only if "static.network.proxy.mode" is set to 2 (Enabled), "static.network.proxy.wpad" is set to 1 (Disabled) and "static.network.proxy.http.set_from" is set to 1.
static.network.proxy.wpad	0 -Disabled 1 -Enabled	1	It enables or disables the WPAD to obtain the PAC file dynamically.  NOTE It works only if "static.network.proxy.mode" is set to 2 (Enabled).
static.network.proxy.http.set_from	0 - IP: Port, enter the IP address and port manually. 1 - PAC URL, enter the PAC URL manually. 2 - PAC File, upload PAC file directly.	0	It configures the sources which the proxy set comes.  NOTE It works only if "static.network.proxy.mode" is set to 2 (Enabled) and "static.network.proxy.wpad" is set to 1 (Disabled).
static.network.proxy.username	String within 256 characters	Blank	It configures the username for proxy server authentication.

y.user name[1]			
static. network. proxy. password[1]	String within 256 characters	Blank	It configures the password for proxy server authentication.
static. network. proxy. sip.enable	0 - Disabled, SIP UDP and outbound do not use proxy server. 1 - Enabled	0	It enables or disables all communications, including SIP to use a proxy server.

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

802.1x Authentication

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

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

Via Web User Interface

Procedure

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Network > Advanced > 802.1x**.

Yealink | MP58

802.1x ?

802.1x Mode	EAP-None	?
Provisioning Mode	Unauthenticated Provisioning	?
Anonymous Identity		?
Identity		?
MD5 Password		?
CA Certificates	No selected file(.crt,.pem) Browse Upload	?
Device Certificates	No selected file(.pem) Browse Upload	?

Via Device User Interface

You can only use the phone screen to enable the PC port (static.network.pc_port.enable). For other parameters, please use the auto provisioning method.

Procedure

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Network (Admin only, default password: admin) > 802.1x .	Go to  > Settings > Device Settings > Network (Admin only, default password: admin) > 802.1x .

←

Device Settings

ⓘ

Accessibility

↺

Reboot

ⓘ

About

⬆

Upgrade

Admin only

🌐

Network

🌐

Proxy

🔍

Debug

🔒

Admin Password

HTTPS Status

☒

HTTPS Port

443

802.1x

802.1x Mode

EAP-None

LLDP

LLDP Status

☒

Packet Interval

60

CDP

CDP Status

☒

Via Auto Provisioning

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

```
static.network.802_1x.mode
static.network.802_1x.identity
static.network.802_1x.md5_password
static.network.802_1x.root_cert_url
static.network.802_1x.client_cert_url
```

Parameter	Permitted Values	Def	Description
-----------	------------------	-----	-------------

		ault	
static.network.802_1x.mode[1]	0- EAP-None, 802.1x authentication is not required. 1- EAP-MD5 2- EAP-TLS 3- EAP-PEAP/MSCHAPv2 4- EAP-TTLS/EAP-MSCHAPv2 5- EAP-PEAP/GTC 6- EAP-TTLS/EAP-GTC 7- EAP-FAST	0	It configures the 802.1x authentication method.
static.network.802_1x.identity[1]	String within 32 characters	Blank	It configures the identity (user name) for 802.1x authentication.  NOTE It works only if "static.network.802_1x.mode" is set to 1, 2, 3, 4, 5, 6, or 7.
static.network.802_1x.md5_password[1]	String within 32 characters	Blank	It configures the password for 802.1x authentication.  NOTE It works only if "static.network.802_1x.mode" is set to 1, 2, 3, 4, 5, 6, or 7.
static.network.802_1x.root_cert_url	URL within 511 characters	Blank	It configures the access URL of the CA certificate. The format of the certificate must be <i>.pem</i> , <i>.crt</i> , <i>*.cer</i> or <i>*.der</i> .  NOTE It works only if "static.network.802_1x.mode" is set to

			1, 2, 3, 4, 5, 6, or 7.
static.network.802_1x.client_certificate_url	URL within 511 characters	Blank	It configures the access URL of the device certificate. The format of the certificate must be *.pem. ! NOTE It works only if "static.network.802_1x.mode" is set to 2 (EAP-TLS).

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

Internet Port and PC Port

Introduction

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

The PC port feature is unavailable to CP965.

Supported Transmission Methods

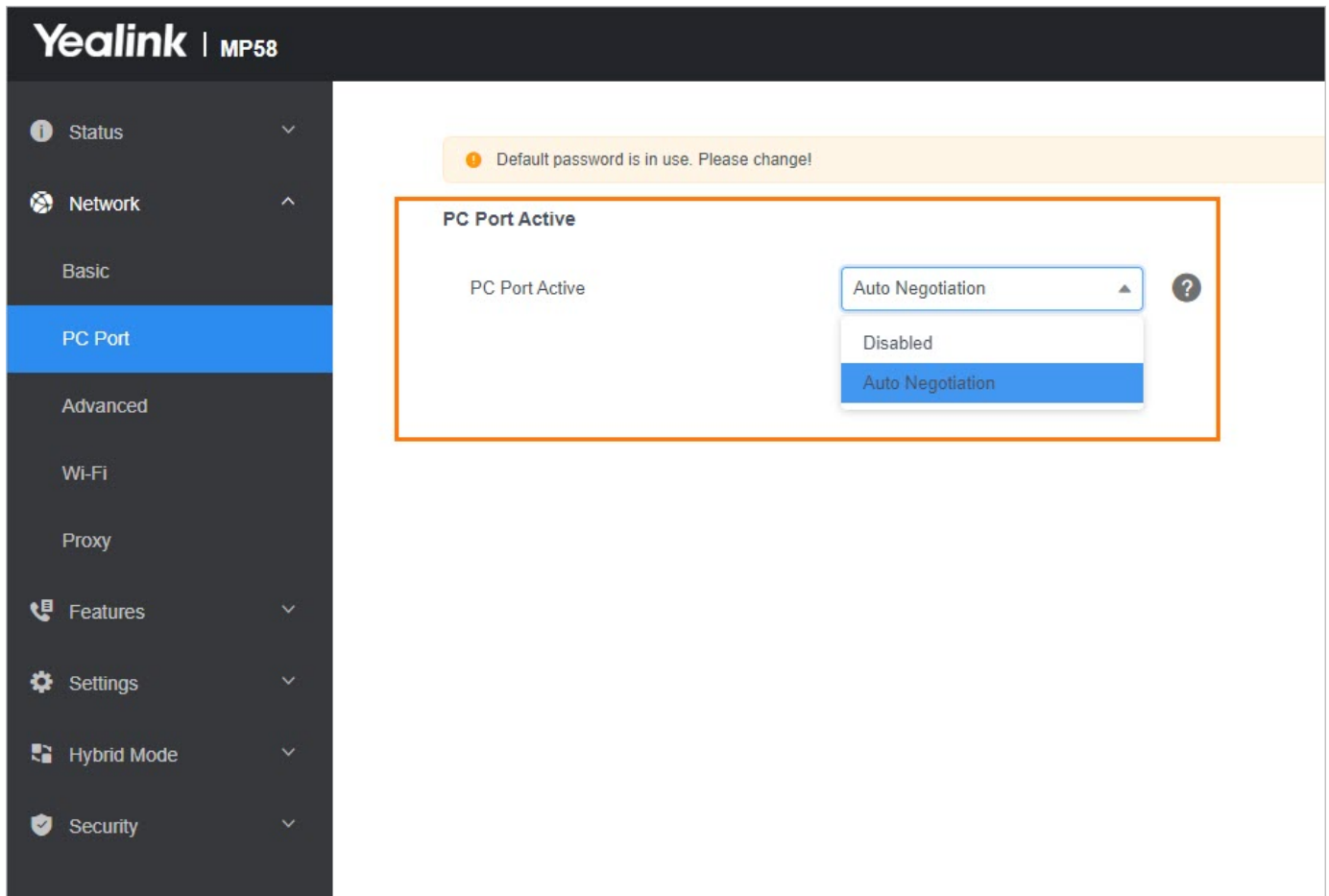
Three optional methods of transmission configuration for the device Internet port and PC port:

- Auto Negotiation
- Half-duplex (transmit in 10Mbps or 100Mbps)
- Full-duplex (transmit in 10Mbps, 100Mbps or 1000Mbps (unavailable to CP965)) Auto negotiation is configured for both Internet and PC ports on the device by default.

Internet Port and PC Port Configuration Via Web User Interface

Procedure

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Network > PC Port > PC Port Active** and set the corresponding parameters.



Yealink | MP58

Status

Network

Basic

PC Port

Advanced

Wi-Fi

Proxy

Features

Settings

Hybrid Mode

Security

Default password is in use. Please change!

PC Port Active

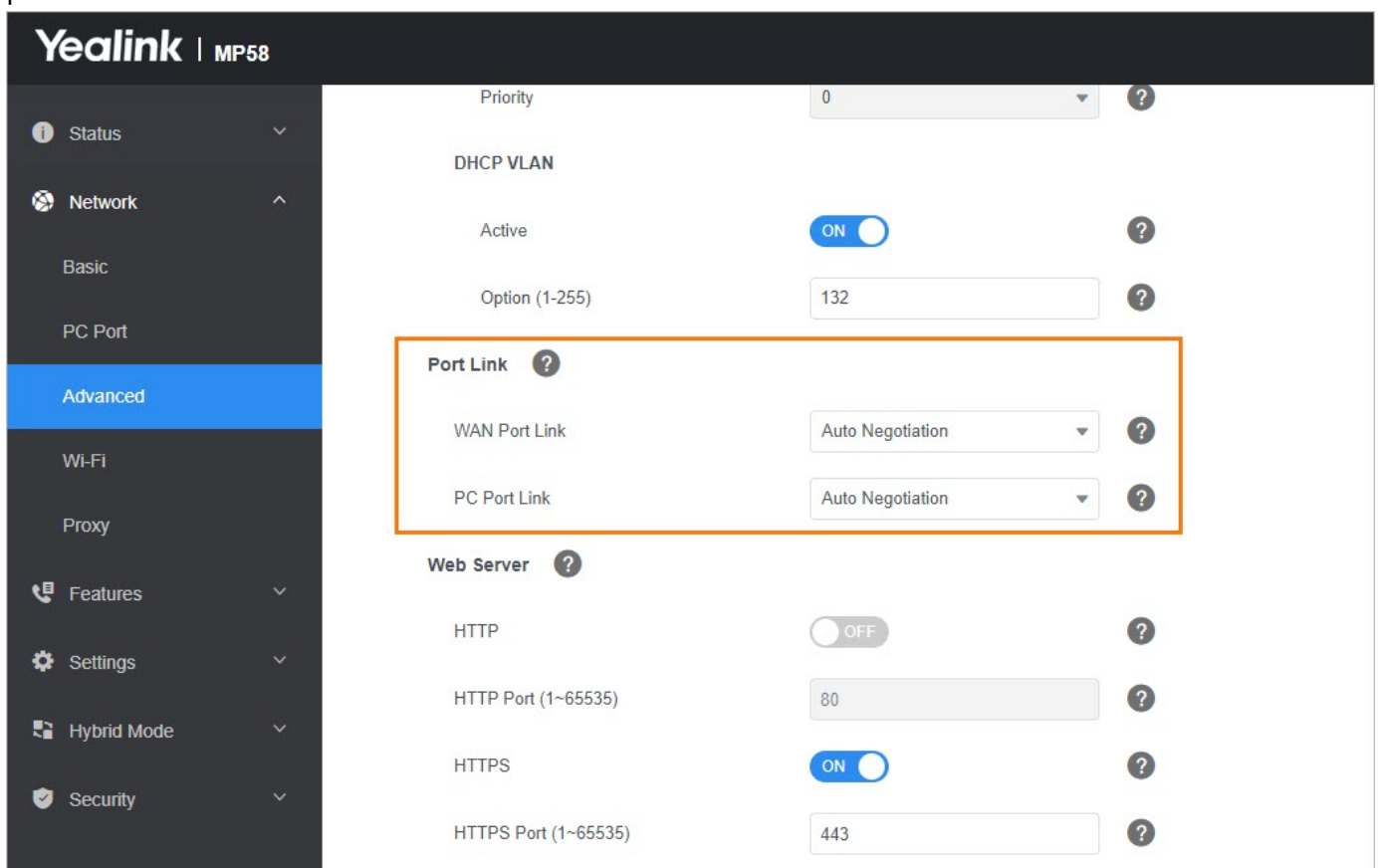
PC Port Active

Auto Negotiation

Disabled

Auto Negotiation

3. Go to **Network > Advanced > Port Link > WAN Port Link/PC Port Link** and set the corresponding parameters.



Yealink | MP58

Status

Network

Basic

PC Port

Advanced

Wi-Fi

Proxy

Features

Settings

Hybrid Mode

Security

Priority 0

DHCP VLAN

Active ON

Option (1-255) 132

Port Link

WAN Port Link Auto Negotiation

PC Port Link Auto Negotiation

Web Server

HTTP OFF

HTTP Port (1~65535) 80

HTTPS ON

HTTPS Port (1~65535) 443

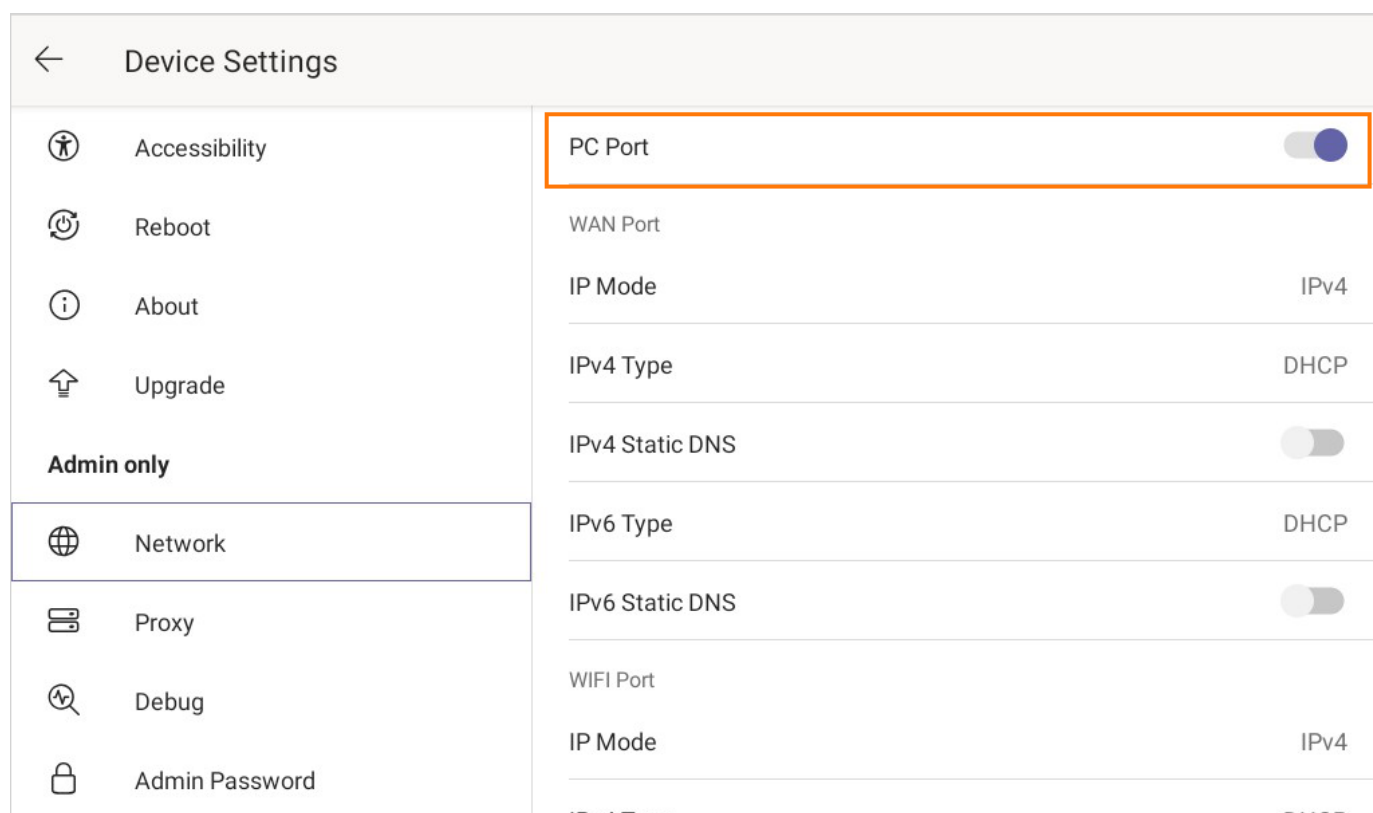
Via Device User Interface

You can only use the device user interface to enable PC port (static.network.pc_port.enable). For other parameters, please use the [auto provisioning method](#).

Procedure

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Network (default password: admin) > PC Port .	Go to  > Settings > Device Settings > Network (Admin only, default password: admin) > PC Port .



Via Auto Provisioning

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

```
static.network.pc_port.enable
static.network.internet_port.speed_duplex
static.network.pc_port.speed_duplex
static.network.vlan.pc_port_mode
```

Parameter	Permitted Values	Def	Description
-----------	------------------	-----	-------------

		ault	
static.network.pc_port.enable[1]	0 - Disabled 1 -Auto Negotiation	1	It enables or disables the CDP feature.  NOTE This feature is unavailable to CP965.
static.network.internet_port.speed_duplex[1]	0 - Auto Negotiation 1 - Full Duplex 10Mbps 2 -Full Duplex 100Mbps 3 -Half Duplex 10Mbps 4 -Half Duplex 100Mbps 5 -Full Duplex 1000Mbps (unavailable to CP965)	0	It configures the transmission method of the Internet port.  NOTE You can set the transmission speed to 1000Mbps/Auto Negotiation to transmit in 1000Mbps if the phone is connected to the switch which supports Gigabit Ethernet. We recommend that you do not change this parameter.
static.network.pc_port.speed_duplex[1]	0 - Auto Negotiation 1 - Full Duplex 10Mbps 2 -Full Duplex 100Mbps 3 -Half Duplex 10Mbps 4 -Half Duplex 100Mbps 5 -Full Duplex 1000Mbps	0	It configures the transmission method of the PC port.  NOTE You can set the transmission speed to 1000Mbps/Auto Negotiation to transmit in 1000Mbps if the phone is connected to the switch which supports Gigabit Ethernet. We recommend that you do not change this parameter. This feature is unavailable to CP965.
static.network.vlan.pc_port_mode[1]	0 - when packets are sent from the PC port to the Internet port, the phone will forward the packets directly. 1 -when packets are sent from the PC port to the	1	It configures the way the phone processes packets for the PC port when VLAN is enabled on the PC port.  NOTE When packets are sent from the Internet port to the PC port, remove the packet's tag if it is the same as

	Internet port, and there is no VLAN tag in the packet, the phone will tag the packet with the configured tag for the PC port and then forward it.		the configured tag for the PC port, else forward the packets directly. This feature is unavailable to CP965.
--	---	--	---

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

Wi-Fi

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

TIP

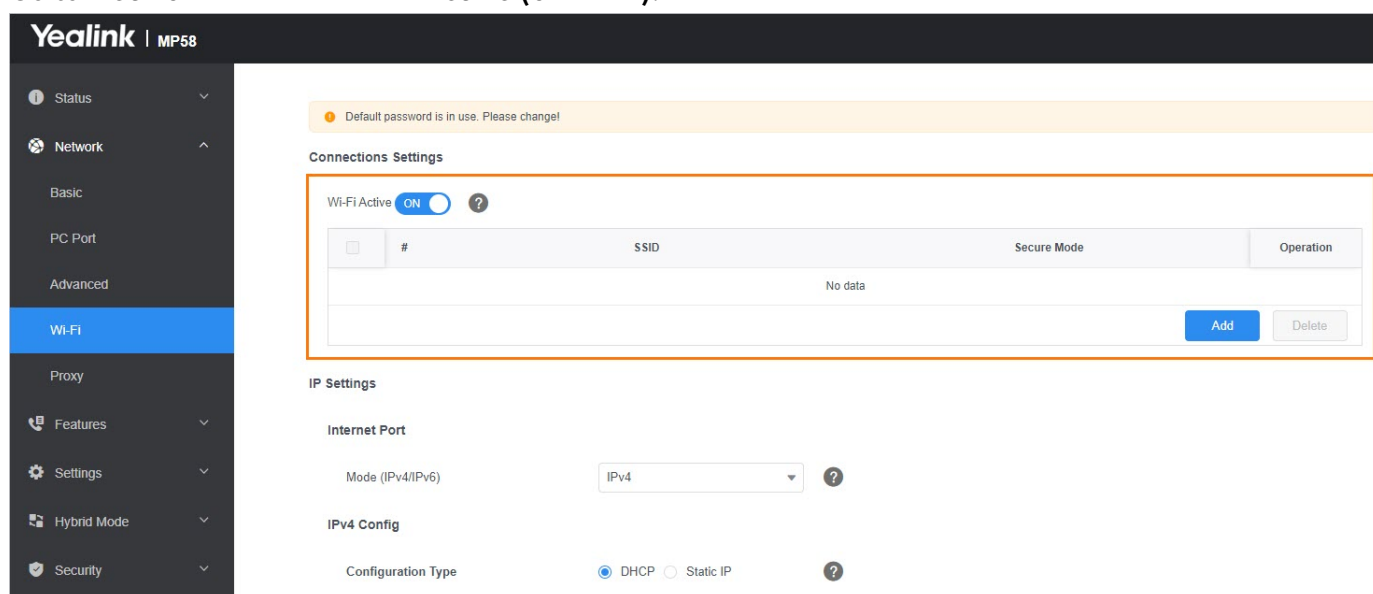
For T56A/T55A/MP54/MP52/MP52 E2, make sure the Wi-Fi USB Dongle WF50 is connected to the device.

Via Web User Interface

You can only use the phone screen to enable Wi-Fi (static.wifi.enable). For other parameters, please use the auto provisioning method.

Procedure

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Network > Wi-Fi > Wi-Fi Active (or Wi-Fi)**.



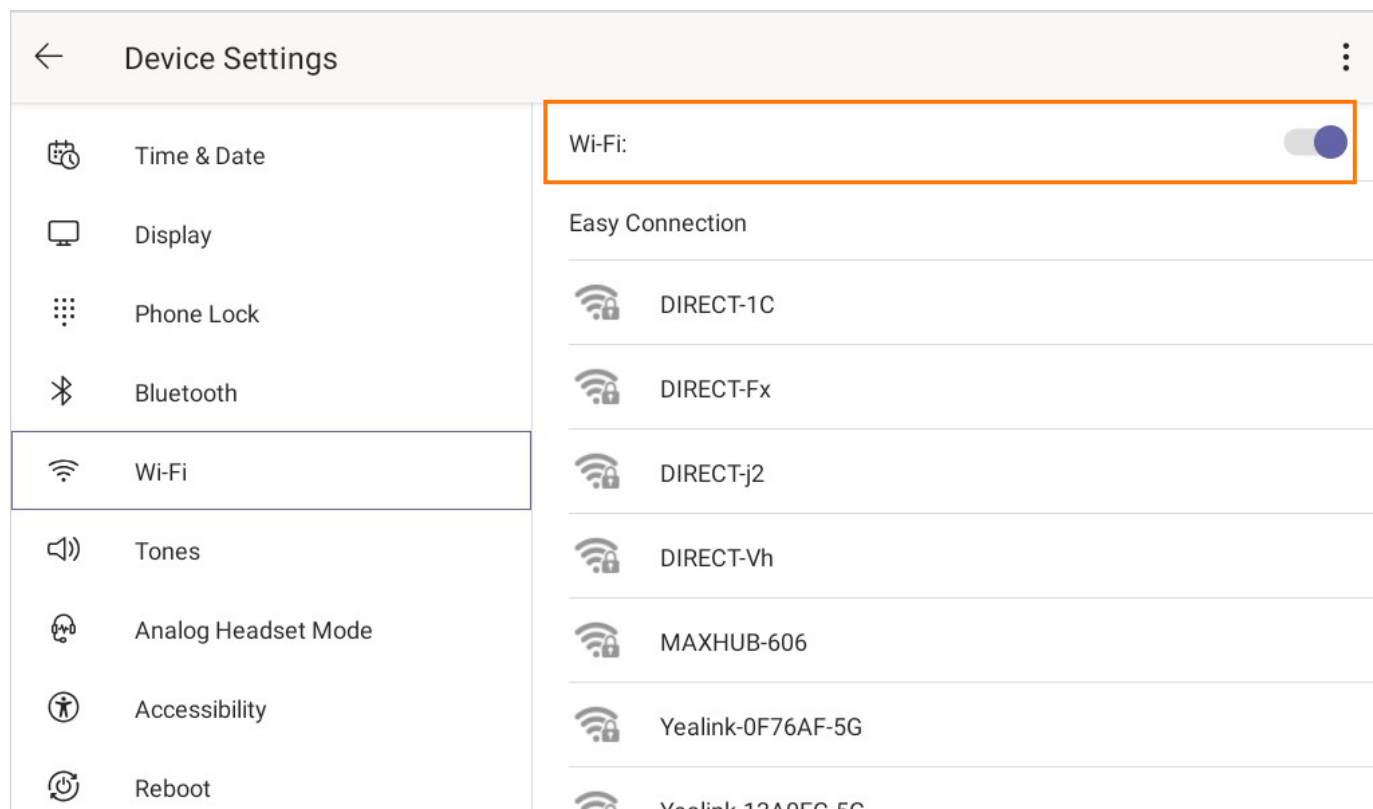
Via Device User Interface

You can only use the device user interface to enable Wi-Fi (static.wifi.enable). For other parameters, please use the [auto provisioning method](#).

Procedure

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Wi-Fi > Wi-Fi .	Go to  > Settings > Device Settings > Wi-Fi > Wi-Fi .



Via Auto Provisioning

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

```
static.wifi.function.enable
static.wifi.enable
static.wifi.X.label
static.wifi.X.ssid
static.wifi.X.priority
static.wifi.X.security_mode
static.wifi.X.cipher_type
static.wifi.X.password
static.wifi.X.eap_type
static.wifi.X.eap_user_name
static.wifi.X.eap_password
```

Parameter	Permitted Value	Default	Description
static.wifi.function.enable [1]	0-Disabled 1-Enabled	1	It enables or disables the Wi-Fi feature.

static.wifi.enable	0 -Disabled 1 -Enabled	0	It activates or deactivates the Wi-Fi mode.  NOTE It works only if "static.wifi.function.enable" is set to 1 (Enabled).
static.wifi.X.label [2]	String within 32 characters	Blank	It configures the profile name of a specific wireless network.  NOTE It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).
static.wifi.X.ssid[2]	String within 32 characters	Blank	It configures the SSID of a specific wireless network. SSID is a unique identifier for accessing wireless access points.  NOTE It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).
static.wifi.X.priority[2]	Integer from 1 to 5	1	It configures the priority for a specific wireless network. 5 is the highest priority, 1 is the lowest priority.  NOTE It works only if "static.wifi.function.enable and static.wifi.enable" are set to 1 (Enabled).
static.wifi.X.security_mode[2]	NONE, WEP, WPA/WPA2 PSK, 802.1x EAP	NONE	It configures the security mode of a specific wireless network.  NOTE

			It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).
static.wifi.X.cipher_type[2]	NONE, PEAP, TLS, TTLS, PWD	NO NE	It configures the encryption type of a specific wireless network. If static.wifi.X.security_mode is set to NONE, the permitted value of this parameter is NONE. If static.wifi.X.security_mode is set to 802.1x EAP, the permitted values of this parameter are PEAP, TLS, TTLS, or PWD. NOTE "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).
static.wifi.X.password[2]	String within 64 characters	Blank	It configures the password of a specific wireless network. NOTE It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).
static.wifi.X.eap_type[2]	TTLS, PEAP or TLS	Blank	It configures the EAP authentication mode of a specific wireless network. NOTE It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).
static.wifi.X.eap_user_name[2]	String within 64 characters	Blank	It configures the EAP authentication username of a specific wireless network.

			 NOTE It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).
static.wifi.X.eap_password[2]	String within 64 characters	Blank	It configures the EAP authentication password of a specific wireless network.  NOTE It works only if "static.wifi.function.enable" and "static.wifi.enable" are set to 1 (Enabled).

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

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

VLAN

Introduction

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

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

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

Configure LLDP

LLDP Configuration

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

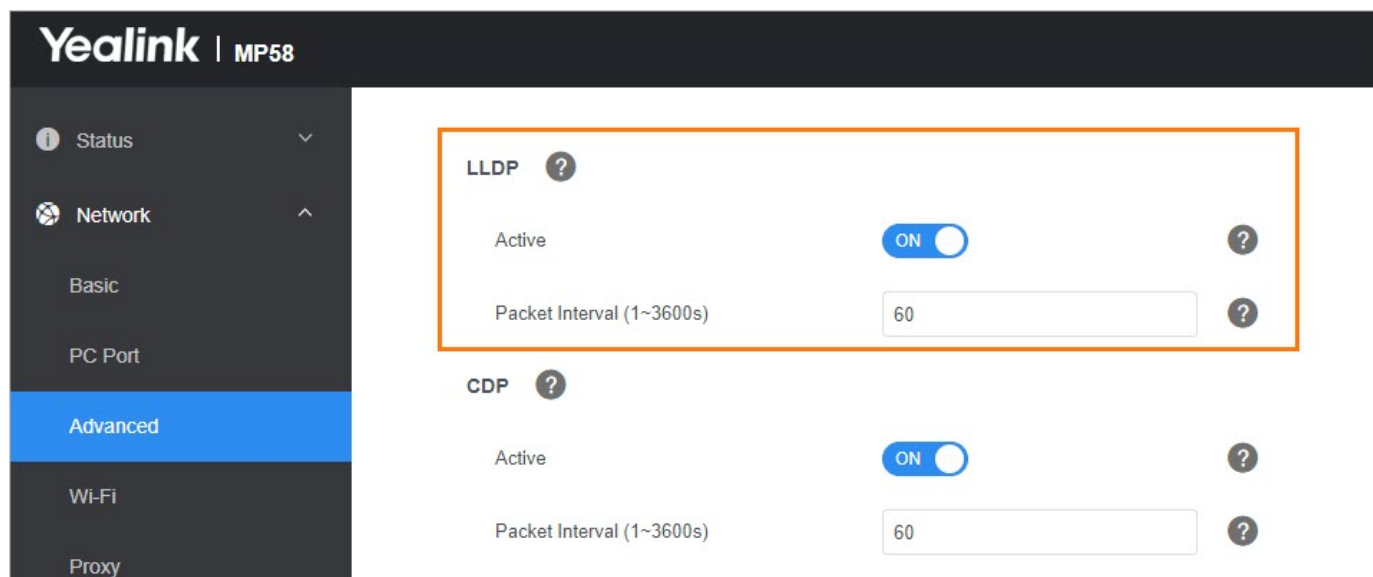
When the LLDP feature is enabled on the devices, the devices periodically advertise their information to the directly connected LLDP-enabled switch. The devices can also receive LLDP packets from the connected switch. When the application type is “voice”, the devices decide whether to update the VLAN

configurations obtained from the LLDP packets. When the VLAN configurations on the devices are different from the ones sent by the switch, the devices perform an update and reboot. This allows the devices to plug into any switch, obtain their VLAN IDs, and then start communications with the call control.

Via Web User Interface

Procedure

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Network > Advanced > LLDP**.

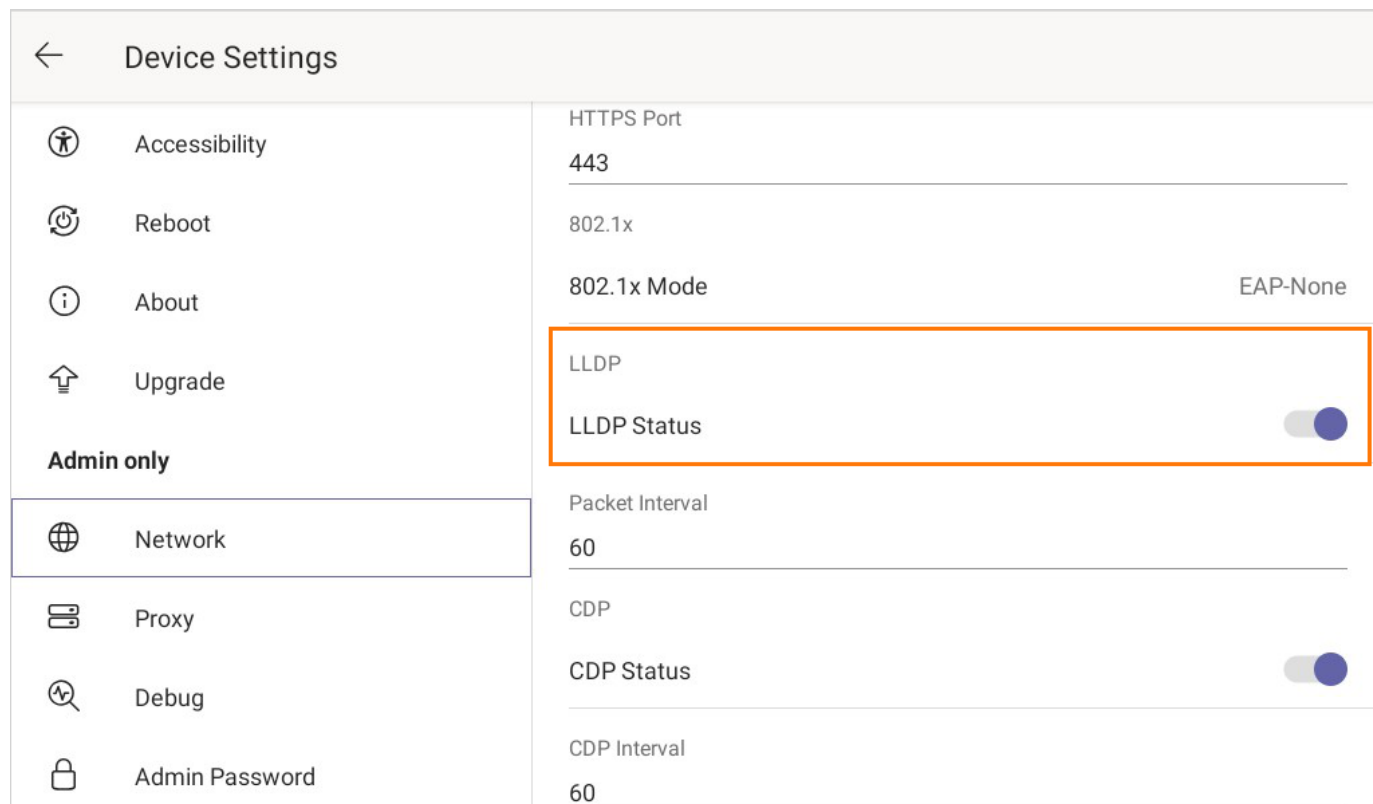


Via Device User Interface

Procedure

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Network (Admin only, default password: admin) > LLDP > LLDP Status .	Go to  > Settings > Device Settings > Network (Admin only, default password: admin) > LLDP > LLDP Status .



Via Auto Provisioning

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

```
static.network.lldp.enable
static.network.lldp.packet_interval
```

Parameter	Permitted Values	Default	Description
static.network.lldp.enable[1]	0- Disabled 1- Enabled, the device will attempt to determine its VLAN ID through LLDP.	1	It enables or disables the LLDP feature on the device.
static.network.lldp.packet_interval	Integer from 1 to 3600	60	It configures the interval (in seconds) that how often the device sends the LLDP request. NOTE It works only if “static.network.lldp.enable” is set to 1 (Enabled).

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

Configure CDP

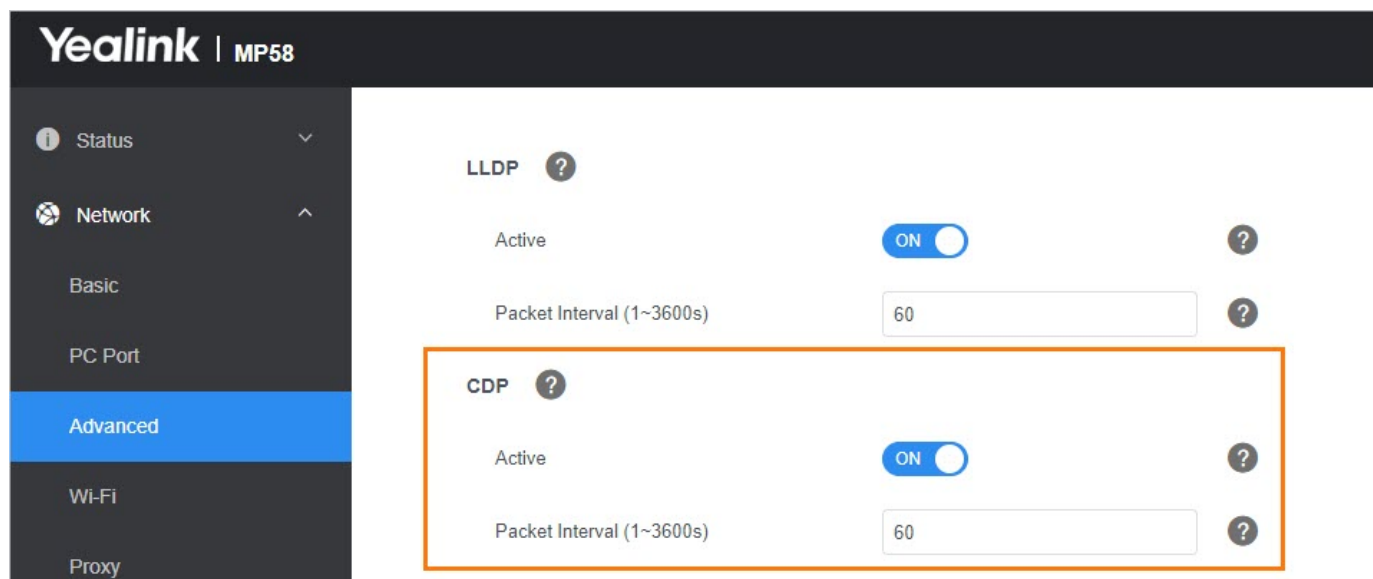
CDP (Cisco Discovery Protocol) allows devices to receive and/or transmit device-related information from/ to directly connected devices on the network that are also using the protocol, and store the information about other devices.

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

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)

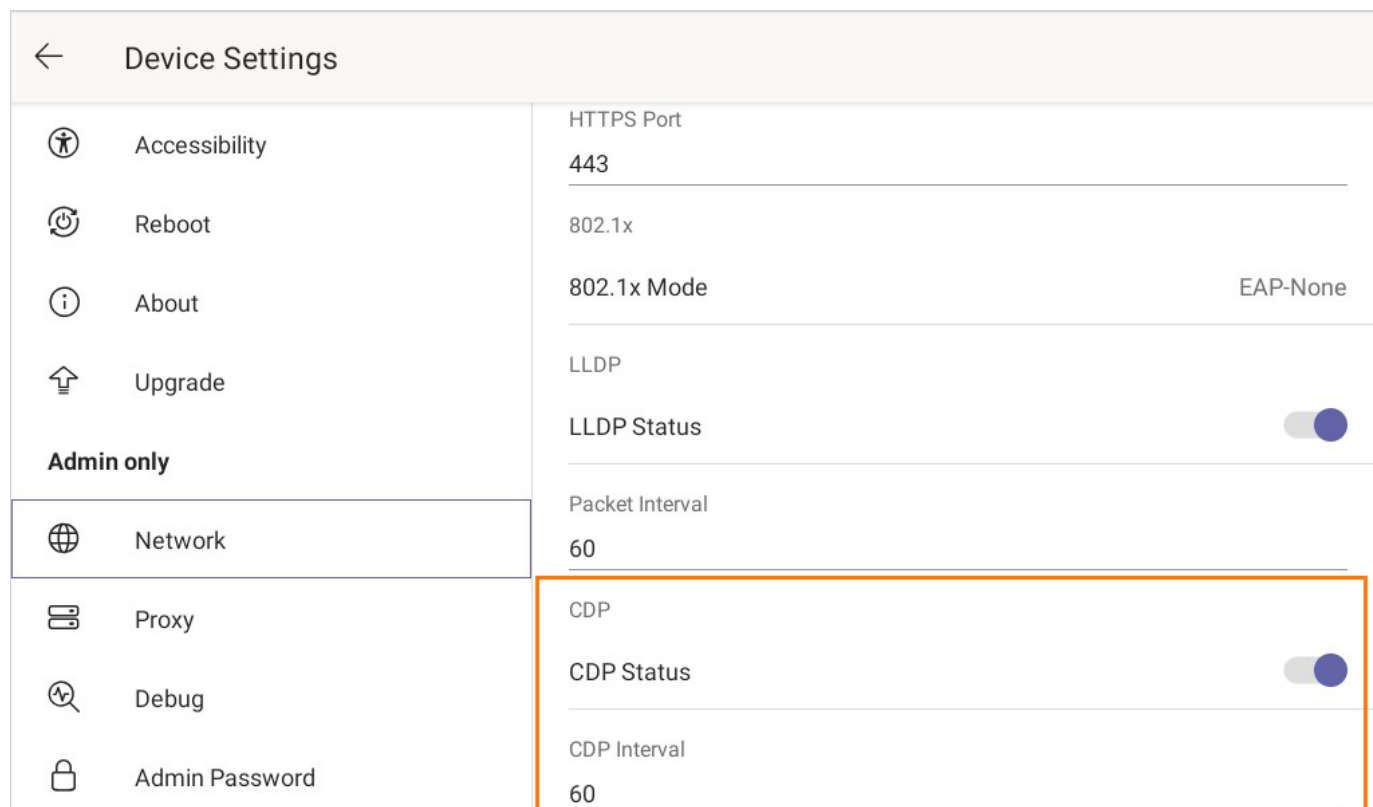
2. Go to **Network > Advanced > CDP**.



Via Device User Interface

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Network (Admin only, default password: admin) > CDP .	Go to  > Settings > Device Settings > Network (Admin only, default password: admin) > CDP .



Via Auto Provisioning

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

```
static.network.cdp.enable
static.network.cdp.packet_interval
```

Parameter	Permitted Values	Default	Description
static.network.cdp.enable[1]	0- Disabled 1- Enabled, the phone will attempt to determine its VLAN ID through CDP.	1	It enables or disables the CDP feature.
static.network.cdp.packet_interval[1]	Integer from 1 to 3600	60	It configures the interval (in seconds) at which the phone sends the CDP request.  NOTE It works only if “static.network.cdp.enable” is set to 1 (Enabled).

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

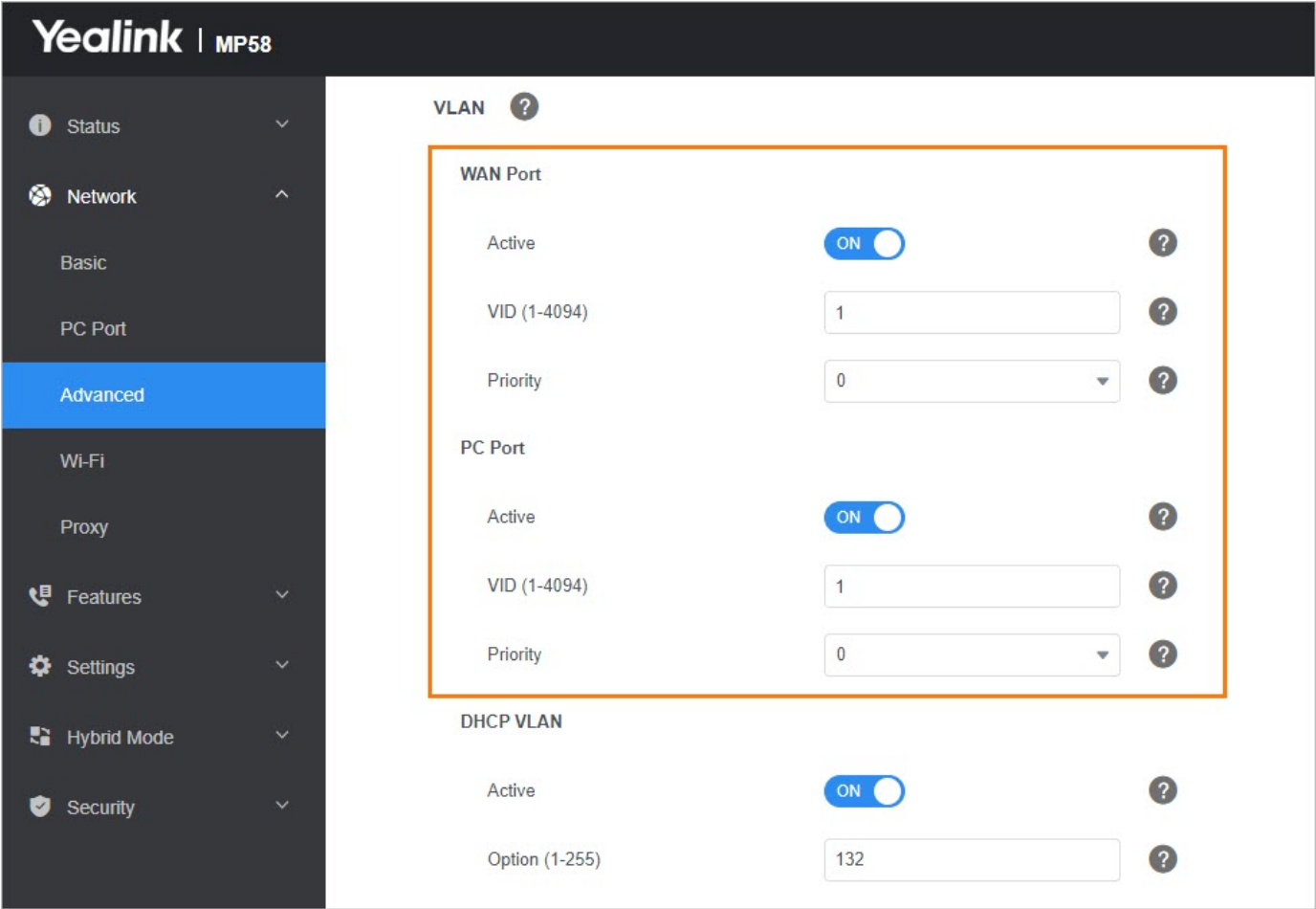
Configure Manual VLAN

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

The PC port is unavailable to CP965, and you can only configure VLAN for the Internet port manually. The following table lists the parameters you can use to configure VLAN manually.

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Network > Advanced > VLAN > WAN Port/PC Port**.



Via Device User Interface

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Network (Admin only, default password: admin) > VLAN > WAN Port/PC Port .	Go to  > Settings > Device Settings > Network (Admin only, default password: admin) > VLAN > WAN Port/PC Port .

Device Settings

- Accessibility
- Reboot
- About
- Upgrade

Admin only

- Network**
- Proxy
- Debug
- Admin Password

VLAN

WAN Port ☐

VID

1

Priority

0

PC Port ☐

VID

1

Priority

0

Via Auto Provisioning

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

static.network.vlan.internet_port_enable
 static.network.vlan.internet_port_vid
 static.network.vlan.internet_port_priority
 static.network.vlan.pc_port_enable
 static.network.vlan.pc_port_vid
 static.network.vlan.pc_port_priority

Parameter	Permitted Values	Default	Description
static.network.vlan.internet_port_enable[1]	0- Disabled 1- Enabled	0	It enables or disables the VLAN for the Internet port.
static.network.vlan.internet_port_vid[1]	Integer from 1 to 4094	1	It configures the VLAN ID for the Internet port.

static.network.vlan.internet_port_priority[1]	Integer from 0 to 7	1	It configures the VLAN priority for the Internet port. 7 is the highest priority, 0 is the lowest priority.  NOTE It works only if “static.network.vlan.internet_port_enable” is set to 1 (Enabled).
static.network.vlan.pc_port_enable[1]	0- Disabled 1- Enabled	0	It enables or disables the VLAN for the PC port.  NOTE It works only if “static.network.pc_port.enable” is set to 1 (Auto Negotiation). This feature is not available to CP965.
static.network.vlan.pc_port_vid[1]	Integer from 1 to 4094	1	It configures the VLAN ID for the PC port.  NOTE It works only if “static.network.pc_port.enable” is set to 1 (Auto Negotiation) and “static.network.vlan.pc_port_enable” is set to 1 (Enabled).
static.network.vlan.pc_port_priority[1]	Integer from 1 to 7	1	It configures the VLAN priority for the PC port. 7 is the highest priority, 0 is the lowest priority.  NOTE It works only if “static.network.pc_port.enable” is set to 1 (Auto Negotiation) and “static.network.vlan.pc_port_enable” is set to 1 (Enabled). This feature is not available to CP965.

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

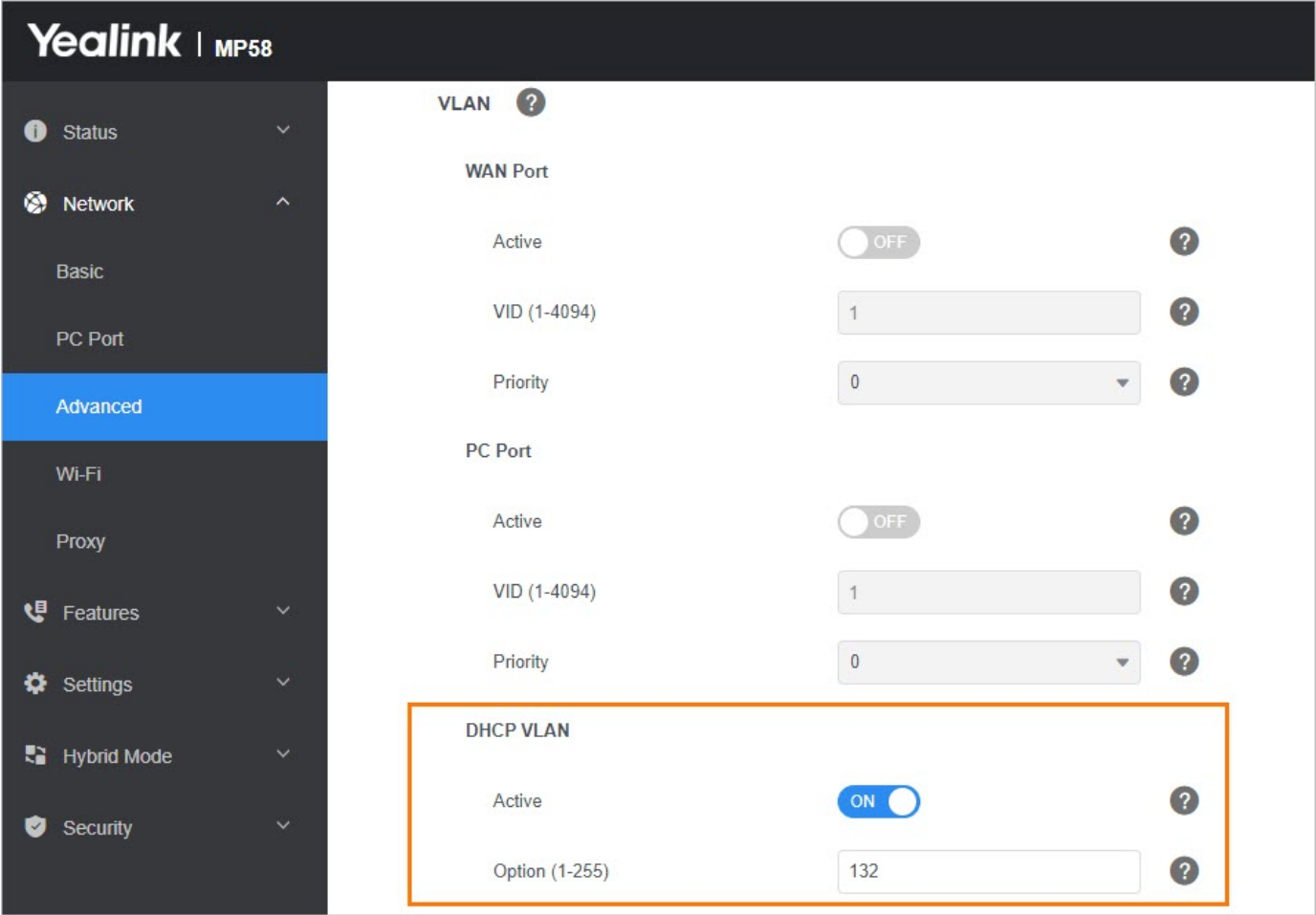
Configure DHCP VLAN

Yealink Teams devices support VLAN discovery via DHCP. When the VLAN discovery method is set to

DHCP, the device will examine the DHCP option for a valid VLAN ID. The predefined option 132 is used to supply the VLAN ID by default. You can customize the DHCP option used to request the VLAN ID.

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Network > Advanced > DHCP VLAN**.



Via Device User Interface

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Network (Admin only, default password: admin) > DHCP VLAN .	Go to  > Settings > Device Settings > Network (Admin only, default password: admin) > DHCP VLAN .

←

Device Settings

ⓘ

Accessibility

↺

Reboot

ⓘ

About

⬆

Upgrade

Admin only

🌐

Network

📡

Proxy

🔍

Debug

🔒

Admin Password

1

Priority

0

PC Port

VID

1

Priority

0

DHCP VLAN

Option

132

Web Server

Via Auto Provisioning

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

static.network.vlan.dhcp_enable
static.network.vlan.dhcp_option

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

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

10 / 11

Configure VLAN Change

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

static.network.vlan.vlan_change.enable

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

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

DHCP Option for IPv6

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

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

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

DHCP Option for IPv4

Introduction

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

**TIP**

For more information on DHCP options, refer to [RFC 2131](#) or [RFC 2132](#).

Supported DHCP Option for IPv4

The following table lists common DHCP options for IPv4 supported by Yealink phones.

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

	has been used for DHCP options.
--	---------------------------------

DHCP Options

DHCP Option 160 and Option 161

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

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

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

```
static.auto_provision.dhcp_option.enable
static.auto_provision.dhcp_option.list_user_options
```

Parameters	Permitted Value	Description
static.auto_provision.dhcp_option.enable[1]	0-Off 1 (default)-On	It triggers the DHCP Option feature to on or off.
static.auto_provision.dhcp_option.list_user_options[1]	Integer from 128 to 254	It configures the custom DHCP option for requesting provisioning server address. Multiple DHCP options are separated by commas. ! NOTE It works only if "static.auto_provision.dhcp_option.enable" is set to 1 (On).

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 is as follows: custom option > option 66 (identify the TFTP server) > option 43.

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

To obtain the server address via the 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.

TIP

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, 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 phones support using 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).

DHCP Option 12

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

See [RFC 1035](#) for character set restrictions.

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

```
static.network.dhcp_host_name
```

Parameter	Permitted Values	Description
static.network.dhcp_host_name[1]	String within 99 characters	It specifies a hostname for the phone when using DHCP.

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

DHCP Option 60

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

Configure DHCP Option 60 via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Auto Provisioning > IPv4 DHCP Option Value.**

The screenshot shows the Yealink MP58 web user interface. On the left is a dark sidebar with a menu containing: Status, Network, Features, Settings (expanded), Preference, Time&Date, Upgrade, Auto Provision (highlighted in blue), Configuration, Voice, Tones, Power Saving, Hybrid Mode, and Security. The main content area is titled 'Auto Provision' and contains various settings. The 'IPv4 DHCP Option Value' field is highlighted with an orange border and contains the text 'yealink'. Other settings include DHCP Active (ON), IPv4 Custom Option (160,161), IPv6 Custom Option, Server URL, Username, Password, Attempt Expired Time (5s), Common AES Key, MAC-Oriented AES Key, Power On (ON), Repeatedly (OFF), Interval (1440), Weekly (OFF), and Weekly Upgrade Interval (0). Each setting has a help icon (?) to its right. At the bottom right are 'Confirm' and 'Cancel' buttons.

Configure DHCP Option 60 via Auto Provisioning

```
static.auto_provision.dhcp_option.option60_value
```

Parameter	Permitted Values	Description
static.auto_provision.dhcp	String within	It configures the vendor class identifier string to

_option.option60_value	99 characters	use in the DHCP interaction.
------------------------	---------------	------------------------------

IPv4 and IPv6 Network Settings

IP Addressing Mode Configuration Via Web User Interface

Procedure

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Network > Basic > Internet Port > Mode(IPv4/IPv6)**.

Yealink | MP58

Default password is in use. Please change!

Internet Port

Mode (IPv4/IPv6) IPv4 ?

IPv4 Config

Configuration Type ☒ DHCP ☐ Static IP ?

IP Address ?

Subnet Mask ?

Default Gateway ?

Static DNS ☐ OFF ?

Primary DNS ?

Secondary DNS ?

IPv6 Config

Configuration Type ☒ DHCP ☐ Static IP ?

IP Address ?

IPv6 Prefix (0~128) 64 ?

Default Gateway ?

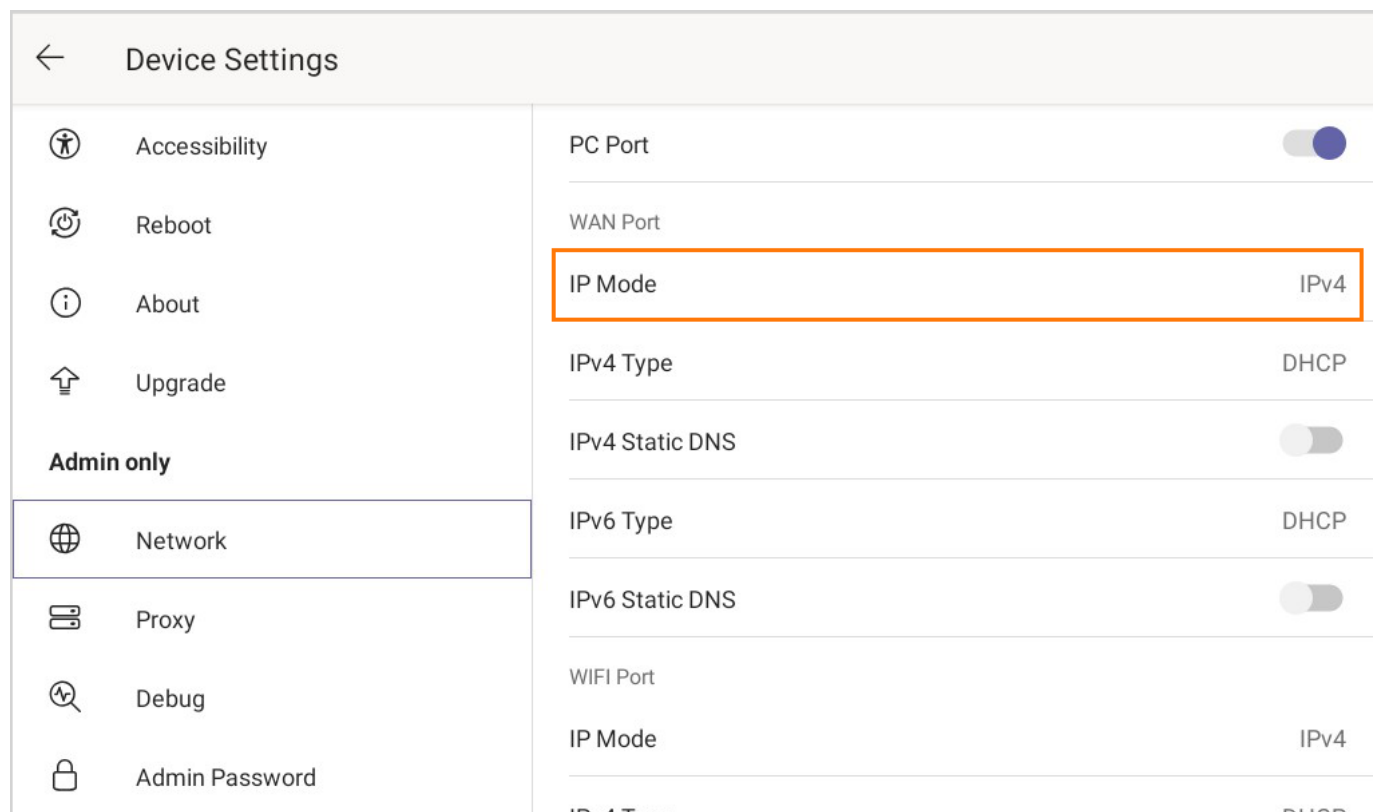
Confirm Cancel

Via Device User Interface

Procedure

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Network (Admin only, default password: admin) > WAN Port > IP Mode .	Go to  > Settings > Device Settings > Network (Admin only, default password: admin) > WAN Port > IP Mode .



← Device Settings

- Accessibility
- Reboot
- About
- Upgrade
- Admin only**
- Network**
- Proxy
- Debug
- Admin Password

PC Port ☒

WAN Port

IP Mode IPv4

IPv4 Type DHCP

IPv4 Static DNS ☐

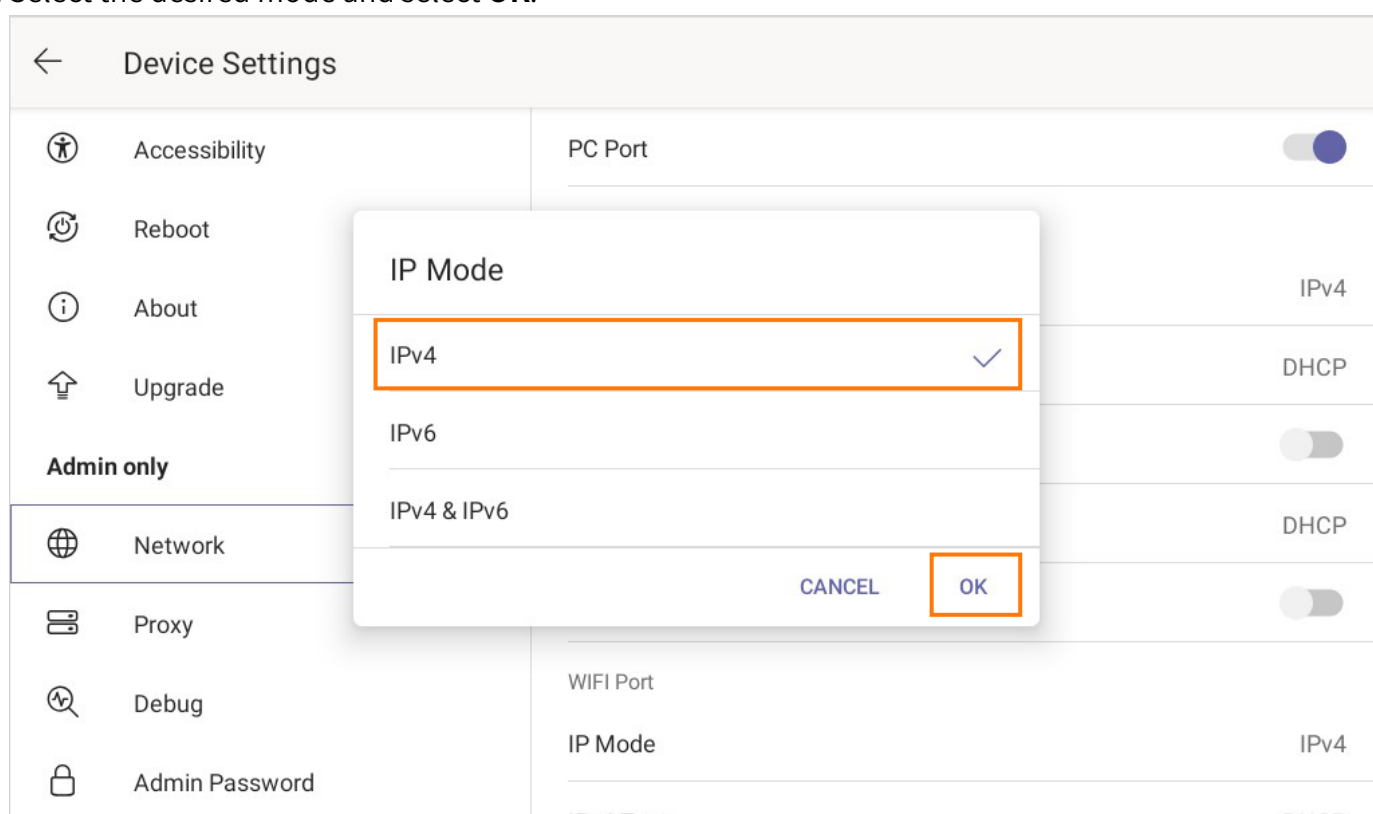
IPv6 Type DHCP

IPv6 Static DNS ☐

WIFI Port

IP Mode IPv4

2. Select the desired mode and select **OK**.



← Device Settings

- Accessibility
- Reboot
- About
- Upgrade
- Admin only**
- Network**
- Proxy
- Debug
- Admin Password

PC Port ☒

WAN Port

IP Mode

IPv4 ✓

IPv6

IPv4 & IPv6

CANCEL OK

WIFI Port

IP Mode IPv4

Auto Provisioning

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

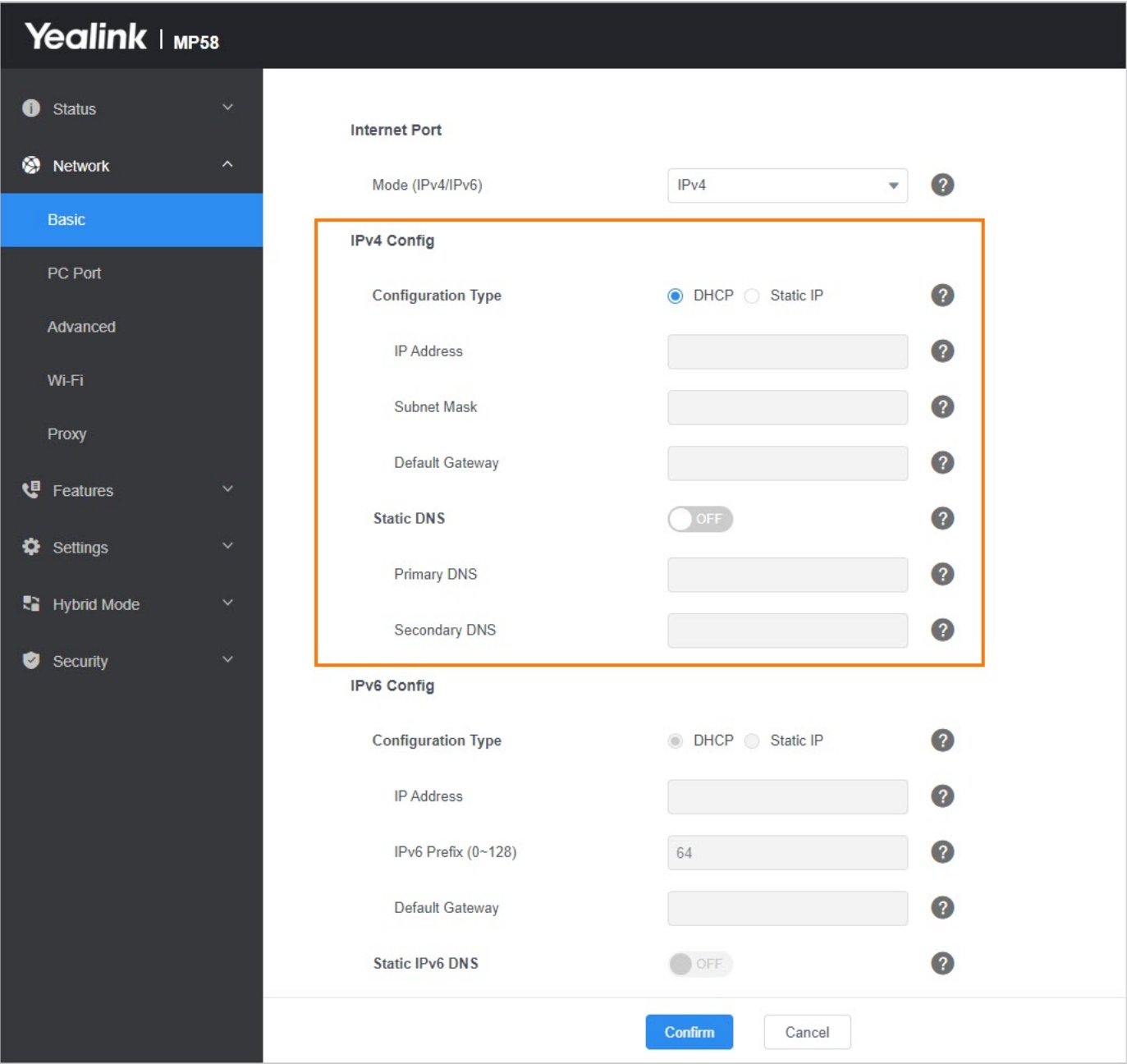
static.network.ip_address_mode

Parameters	Permitted Values	Default	Description
static.network.ip_address_mode	0-IPv4 1-IPv6 2-IPv4 & IPv6	0	It configures the IP addressing mode.

IPv4 Configuration Via Web User Interface

Procedure

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Network > Basic > IPv4 Config**.



Via Device User Interface

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Network (Admin only, default password: admin) > WAN Port > IPv4 Type/IPv4 Static DNS .	Go to  > Settings > Device Settings > Network (Admin only, default password: admin) > WAN Port > IPv4 Type/IPv4 Static DNS .

Device Settings

- Accessibility
- Reboot
- About
- Upgrade

Admin only

- Network**
- Proxy
- Debug
- Admin Password

PC Port ☒

WAN Port

IP Mode IPv4

IPv4 Type DHCP

IPv4 Static DNS ☒

Pri.DNS

Sec.DNS

IPv6 Type DHCP

IPv6 Static DNS ☐

2. Save the change.

Auto Provisioning

```
javastatic.network.internet_port.type
static.network.internet_port.ip
static.network.internet_port.mask
static.network.internet_port.gateway
static.network.static_dns_enable
static.network.primary_dns
static.network.secondary_dns
```

Parameter	Permitted Values	Default	Description
static.network.internet_port.type[1]	0 -DHCP 2 -Static IP	0	It configures the Internet port type for IPv4. NOTE It works only if "static.network.i

			p_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6).
static.network.internet_port.ip[1]	IPv4 Address	Blank	It configures the IPv4 address.  NOTE It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP).
static.network.internet_port.mask[1]	Subnet Mask	Blank	It configures the IPv4 subnet mask.  NOTE It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP).
static.network.internet_port.gateway[1]	IPv4 Address	Blank	It configures the IPv4 default gateway.  NOTE It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and

			"static.network.internet_port.type" is set to 2 (Static IP).
static.network.static_dns_enable[1]	0-Off, the phone will use the IPv4 DNS obtained from DHCP. 1-On, the phone will use manually configured static IPv4 DNS.	0	It triggers the static DNS feature to on or off. NOTE It works only if "static.network.internet_port.type" is set to 0 (DHCP).
static.network.primary_dns[1]	IPv4 Address	Blank	It configures the primary IPv4 DNS server. NOTE It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). In the DHCP environment, you need to make sure that "static.network.static_dns_enable" is set to 1 (On).
static.network.secondary_dns[1]	IPv4 Address	Blank	It configures the secondary IPv4 DNS server. NOTE It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). In

			the DHCP environment, you need to make sure that "static.network.static_dns_enable" is set to 1 (On).
--	--	--	---

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

IPv6 Configuration

Introduction

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

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

Via Web User Interface

Procedure

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Network > Basic > IPv6 Config**.

Yealink | MP58

Status

Network

Basic

PC Port

Advanced

Wi-Fi

Proxy

Features

Settings

Hybrid Mode

Security

IPv4 Config

Configuration Type

☒ DHCP ☐ Static IP

IP Address

Subnet Mask

Default Gateway

Static DNS

☐ OFF

Primary DNS

Secondary DNS

IPv6 Config

Configuration Type

☐ DHCP ☐ Static IP

IP Address

IPv6 Prefix (0~128)

64

Default Gateway

Static IPv6 DNS

☐ OFF

Primary DNS

Secondary DNS

Confirm

Cancel

Via Device User Interface

Procedure

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Network (Admin only, default password: admin) > WAN Port > IPv6 Type/IPv6 Static DNS .	Go to  > Settings > Device Settings > Network (Admin only, default password: admin) > WAN Port > IPv6 Type/IPv6 Static DNS .

Device Settings

- Accessibility
- Reboot
- About
- Upgrade
- Admin only**
- Network**
- Proxy
- Debug
- Admin Password

IPv4 Static DNS

IPv6 Type: DHCP

IPv6 Static DNS: ☒

Pri.DNS

Sec.DNS

WIFI Port

IP Mode: IPv4

IPv4 Type: DHCP

2. Save the change.

Via Auto Provisioning

```
static.network.ipv6_internet_port.type
static.network.ipv6_internet_port.ip
static.network.ipv6_prefix
static.network.ipv6_internet_port.gateway
static.network.ipv6_static_dns_enable
static.network.ipv6_primary_dns
static.network.ipv6_secondary_dns
static.network.ipv6_icmp_v6.enable
```

Parameter	Permitted Values	Default	Description
static.network.ipv6_internet_port.type[1]	0-DHCP 1-Static IP	0	It configures the Internet port type for IPv6. NOTE It works only if "static.network.ip_address_mode" is set to 1

			(IPv6) or 2 (IPv4 & IPv6).
static.network.ipv6_internet_port.ip[1]	IPv6 Address	Blank	It configures the IPv6 address.  NOTE It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP).
static.network.ipv6_prefix[1]	Integer from 0 to 128	64	It configures the IPv6 prefix.  NOTE It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP).
static.network.ipv6_internet_port.gateway[1]	IPv6 Address	Blank	It configures the IPv6 default gateway.  NOTE It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP).
static.network.ipv6_static_dns_enable[1]	0 -Off, the phone will use the IPv6 DNS obtained from DHCP. 1 -On, the phone will use manually configured	0	It triggers the static IPv6 DNS feature to turn on or off.  NOTE It works only if "static.network.ipv6_internet_port.type" is set to 0 (DHCP).

	static IPv6 DNS.		
static.network.ipv6_primary_dns[1]	IPv6 Address	Blank	It configures the primary IPv6 DNS server. NOTE It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure that "static.network.ipv6_static_dns_enable" is set to 1 (On).
static.network.ipv6_secondary_dns[1]	IPv6 Address	Blank	It configures the secondary IPv6 DNS server. NOTE It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure that "static.network.ipv6_static_dns_enable" is set to 1 (On).
static.network.ipv6_icmp_v6.enable[1]	0 -Disabled 1 -Enabled	1	It enables or disables the phone to obtain IPv6 network settings via SLAAC (Stateless Address Auto-configuration). NOTE It works only if "static.network.ipv6_internet_port.type" is set to 0 (DHCP).

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

Network Requirements

Before you set up Teams phone, make sure that your enterprise network meets the requirements of Microsoft Teams.

See Microsoft doc on [Prepare your organization's network for Microsoft Teams](#) for more information.

1. Do all your locations have Internet access (so they can connect to Microsoft 365 or Office 365)?
2. At a minimum, in addition to normal web traffic, make sure you've opened the following ports for all locations for media in Teams.

Ports	UDP ports 3478 through 3481
IP addresses	13.107.64.0/18, 52.112.0.0/14, and 52.120.0.0/14

If you need to federate with Skype for Business, either on-premises or online, you will need to configure some additional DNS records.

CNAME Records / Host name	TTL	Points to address or value
sip	3600	sipdir.online.lync.com
lyncdiscover	3600	webdir.online.lync.com

2. Do you have a verified domain for Microsoft 365 or Office 365 (for example, contoso.com)?
3. If your organization hasn't rolled out Microsoft 365 or Office 365, see [Get started](#).
4. If your organization hasn't added or configured a verified domain for Microsoft 365 or Office 365, see the [Domains FAQ](#).
3. Has your organization deployed Exchange Online and SharePoint Online?
4. If your organization doesn't have Exchange Online, see [Understand how Exchange and Microsoft Teams interact](#).
5. If your organization doesn't have SharePoint Online, see [Understand how SharePoint Online and OneDrive for Business interact with Microsoft Teams](#).

Once you've verified that you meet these network requirements, you may be ready to [Roll out Teams](#). If you're a large multinational enterprise, or if you know you've got some network limitations, read on to learn how to assess and optimize your network for Teams.

For educational institutions: If your organization is an educational institution and you use a Student Information System (SIS), [deploy School Data Sync](#) before you roll out Teams.

Running on-premises Skype for Business Server: If your organization is running on-premises Skype for Business Server (or Lync Server), you must [configure Azure AD Connect](#) to synchronize your on-

premises directory with Microsoft 365 or Office 365.

Set Up a Provisioning Server

Introduction

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

Supported Provisioning Protocols

Yealink phones support several transport protocols for provisioning:

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

TIP

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

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

Supported Provisioning Server Discovery Methods

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

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

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

Configure DHCP Provisioning Via the Web User Interface

Procedure

1. On the web user interface, go to **Settings > Auto Provision > DHCP Active / IPv4 Custom Option**.

Default password is in use. Please change!

Auto Provision

DHCP Active	☒	?
IPv4 Custom Option	160,161	?
IPv4 DHCP Option Value	yealink	?
IPv6 Custom Option		?
Server URL	http://192.168.1.100:8080	?
Username	admin	?
Password	*****	?
Attempt Expired Time (s)	5	?
Common AES Key	*****	?

Via Auto Provisioning

```
static.auto_provision.dhcp_option.enable
static.auto_provision.dhcp_option.list_user_options
```

Parameter	Permitted Values	Default	Description
static.auto_provision.dhcp_option.enable	0 -Off 1 -On, the phone obtains the provisioning server address by detecting DHCP options.	1	It triggers the DHCP Active feature to on or off.
static.auto_provision.dhcp_option.list_user_options	Integer from 128 to 254	Blank	It configures the IPv4 custom DHCP option for requesting provisioning server address. Multiple options are separated by commas.

**NOTE**

It works only if
"static.auto_provision.dhcp_option.enable" is set to 1 (On).

Configure Static Provisioning

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

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

**TIP**

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

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

Via the Web User Interface

Procedure

1. On the web user interface, go to **Settings > Auto Provision > Server URL / Username / Password**.

Auto Provision

Default password is in use. Please change!

DHCP Active ☒ ON ?

IPv4 Custom Option ?

IPv4 DHCP Option Value ?

IPv6 Custom Option ?

Server URL ?

Username ?

Password ?

Attempt Expired Time (s) ?

Common AES Key ?

Via Auto Provisioning

```
static.auto_provision.server.url
static.auto_provision.server.username
static.auto_provision.server.password
```

Parameter	Permitted Values	Default	Description
static.auto_provision.server.url	URL within 511 characters	Blank	It configures the access URL of the provisioning server.
static.auto_provision.server.username	String within 32 characters	Blank	It configures the user name for provisioning server access.
static.auto_provision.server.password	String within 32 characters	Blank	It configures the password for provisioning server access.

Configure a Provisioning Server

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

Procedure

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

TIP

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

Provisioning Methods

Introduction

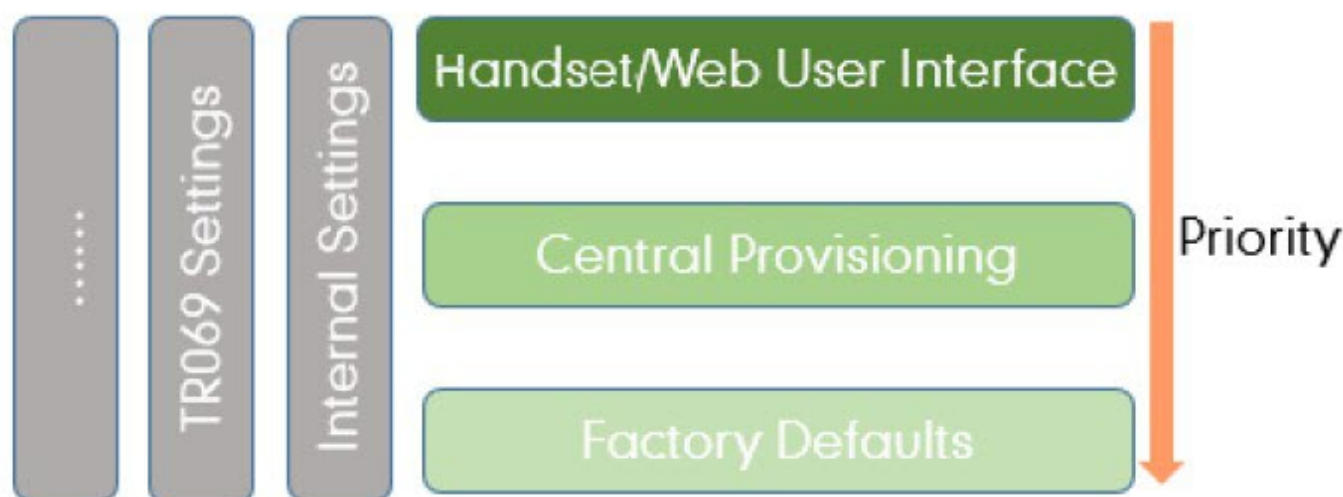
Teams devices can be configured using the following methods with your provisioning server:

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

Provisioning Methods Priority

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

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



NOTE

The provisioning priority mechanism takes effect only if `static.auto_provision.custom.protect` is set to 1. For more information on this parameter, refer to MAC-local CFG File Configuration . Static parameters have no priority. They take effect no matter what method (web user interface or phone user interface or configuration files) you are using for provisioning. Static parameters are the parameters that start with a prefix “static.” , for example, the parameters associated with auto provisioning/network/syslog, TR069 settings and internal settings (the temporary configurations to be used for program running).

Manual Provisioning

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

Web User Interface Access

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

Access the Web User Interface

See [Log In to the Web User Interface](#).

Configure Web Server Type

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

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

Via the Web User Interface

1. On the web user interface, go to **Network > Advanced > Web Server**.

The screenshot shows the Yealink Teams Web User Interface. On the left is a dark sidebar with a menu: Status, Network, Basic, PC Port, Advanced (highlighted in blue), Wi-Fi, Proxy, Features, Settings, Hybrid Mode, and Security. The main content area is titled 'Option (1-255)' with a value of '132'. Below this are 'Port Link' settings for WAN and PC, both set to 'Auto Negotiation'. The 'Web Server' section is highlighted with a red rectangle; it contains an 'HTTPS' toggle switch set to 'ON' and an 'HTTPS Port (1~65535)' field set to '443'. Below this is the '802.1x' section with settings for Mode (EAP-None), Provisioning Mode (Unauthenticated Provisioning), Anonymous Identity, and Identity.

Via Auto Provisioning

```
static.wui.https_enable
static.network.port.https
```

Parameter	Permitted Values	Default	Description
static.wui.https_enable	0-Disabled	1	It enables or disables to access the web user interface of

ps_enable[1]	1-Enabled		the phone over a secure tunnel (HTTPS).
static.network .port.https[1]	Integer from 1 to 65535	44 3	It configures the port used to access the web user interface of the phone over a secure tunnel (HTTPS).

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

Import CFG Configuration Files to Device

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

Procedure

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

Export CFG Configuration Files from Device

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

About this task

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

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

Procedure

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

Phone User Interface

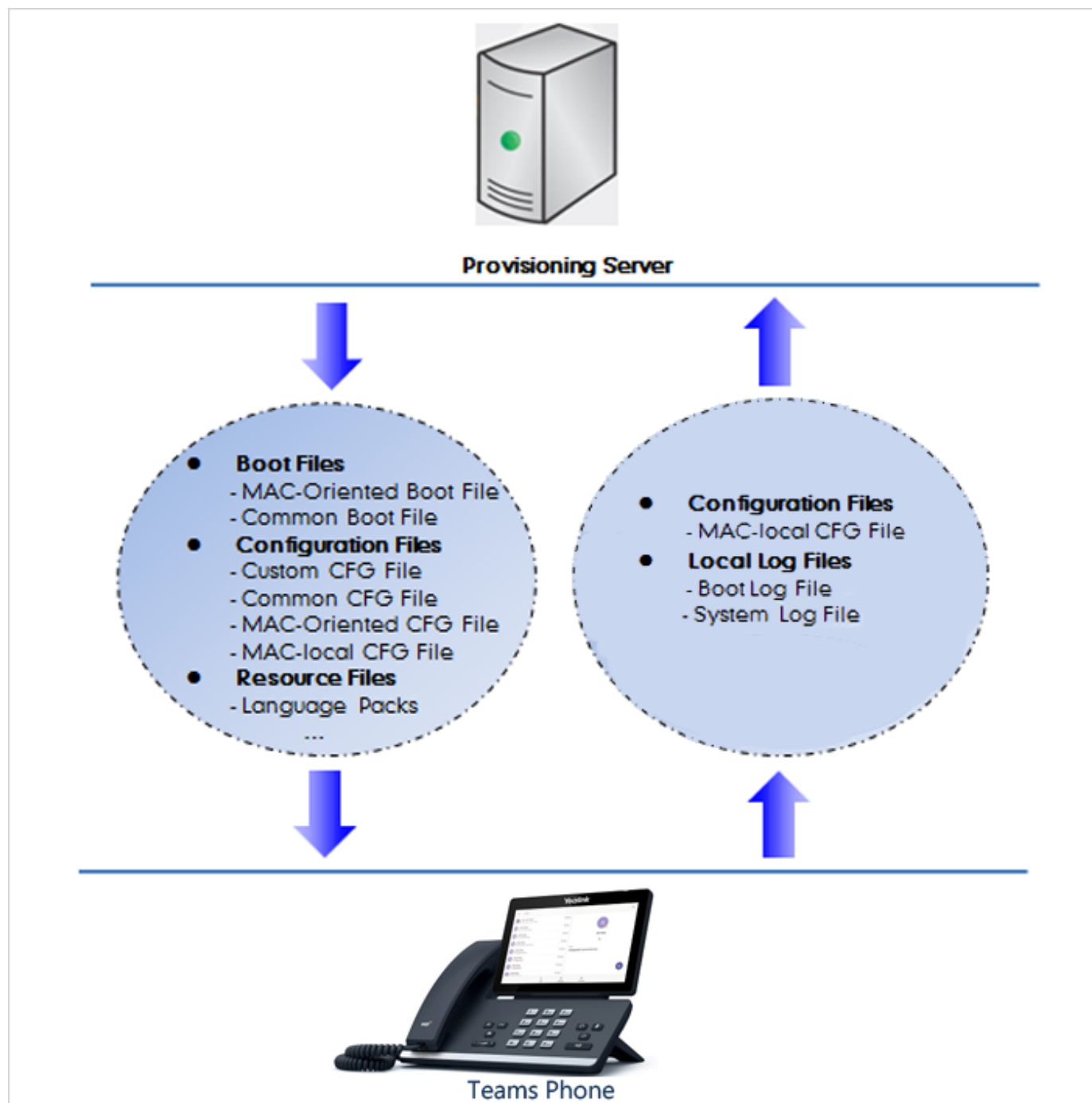
Phone user interface makes configurations available to users and administrators, but the  **Settings > Device Settings > Admin only** option is only available to administrators and requires an administrator password (default: admin).

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

Central Provisioning

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

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



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

Teams devices can obtain the provisioning server address during startup. Then devices download configuration files from the provisioning server, resolve and update the configurations written in configuration files. This entire process is called auto provisioning. For more information on auto provisioning, refer to [Yealink Teams HD IP Phones Auto Provisioning Guide](#).

Configure Auto Provisioning Settings

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

Via Auto Provisioning

```
static.network.attempt_expired_time
static.auto_provision.power_on
static.auto_provision.repeat.enable
static.auto_provision.repeat.minutes
static.auto_provision.weekly.enable
static.auto_provision.weekly.dayofweek
static.auto_provision.weekly.begin_time
static.auto_provision.weekly.end_time
```

Parameter	Permitted Values	Default	Description
static.network.attempt_expired_time[1]	Integer from 1 to 20	10	It configures the timeout (in seconds) to transfer a file for HTTP/HTTPS connection. ! NOTE It has a lower priority than the value defined by the parameter "static.auto_provision.attempt_expired_time".
static.auto_provision.power_on	0 -Off 1 -On, the phone performs auto provisioning when powered on.	1	It triggers the power on feature to on or off.
static.auto_provision.repeat.enable	0 -Off 1 -On	0	It triggers the repeatedly feature to on or off.
static.a	Integer from 1	14	It configures the interval (in minutes) for the phone to

uto_prov ision.repeat.minutes	to 43200	40	perform auto provisioning repeatedly.  NOTE It works only if "static.auto_provision.repeat.enable" is set to 1 (On).
static.auto_provision.weekly.enable	0 -Off 1 -On, the phone performs an auto provisioning process weekly.	0	It triggers the weekly feature to on or off.
static.auto_provision.weekly.dayofweek	0,1,2,3,4,5,6 or a combination of these digits 0 -Sunday 1 -Monday 2 -Tuesday 3 -Wednesday 4 -Thursday 5 -Friday 6 -Saturday	01 23 45 6	It configures the days of the week for the phone to perform auto provisioning weekly. Example: "static.auto_provision.weekly.dayofweek = 01" If "static.auto_provision.weekly_upgrade_interval" is set to 0, it means the phone performs auto provisioning every Sunday and Monday. If "static.auto_provision.weekly_upgrade_interval" is set to other value (for example, 3), it means the phone performs auto provisioning by randomly selecting a day from Sunday and Monday every three weeks.  NOTE It works only if "static.auto_provision.weekly.enable" is set to 1 (On).
static.auto_provision.weekly.begin_time	Time from 00:00 to 23:59	00:00	It configures the starting/ending time of the day for the phone to perform auto provisioning weekly.  NOTE It works only if

static.auto_provision.weekly.end_time			"static.auto_provision.weekly.enable" is set to 1 (On).
---------------------------------------	--	--	---

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

Boot Files, Configuration Files, and Resource Files

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

You can ask the distributor or Yealink FAE for template files. You can also obtain the template files online: <https://support.yealink.com/en/portal/home>.

Boot Files

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

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

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

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

TIP

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

Common Boot File

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

MAC-Oriented Boot File

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

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

**TIP**

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

Boot File Attributes

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

Attributes	Description
#! version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
include:config <xxx.cfg> include:config "xxx.cfg"	Each “include” statement can specify a location of a configuration file. The configuration file format must be <code>.cfg</code> . The locations in the angle brackets or double quotation marks support two forms: Relative path (relative to the boot file): <code>./sip.cfg</code> , <code>HTTP Directory/sip.cfg</code> for example Absolute path (or URL): <code>http://10.2.5.258/Teams.cfg</code> for example The location must point to a specific CFG file.
[\$MODEL]	The <code>[\$MODEL]</code> can be added to specify settings for specific phone models. <code>\$MODEL</code> represents the phone model name. The valid device model names are: MP58, MP56, MP54, MP52, CP965 and VP59. Multiple device models are separated by commas. For example, [T58A, T56A].
overwrite_mode	Enable or disable the overwrite mode. The overwrite mode applies to the configuration files specified in the boot file. It only affects the parameters pre-provisioned via central provisioning. 1-(Enabled) - If the value of a parameter in the configuration files is left blank, or if a non-static parameter in the configuration files is deleted or commented out, the factory default value takes effect. 0-(Disabled) -If the value of a parameter in the configuration files is left blank, deleted or commented out, the pre-configured value is kept.  NOTE Overwrite mode can only be used in boot files. If a boot file is used, but the value of the parameter “overwrite_mode” is not configured, the overwrite mode is enabled by default.
specific_mode	Enable or disable the exclude mode. The exclude mode applies to the

l.excluded_model	configuration files specified in the boot file. 0- Disabled (Append Mode), the device downloads its own model-specific configuration files and downloads other model-unspecified configuration files. 1- Enabled (Exclude Mode), the device attempts to download its own model-specific configuration files; if there are no own model-specific configuration files found on the server, it downloads model-unspecified configuration files. NOTE Exclude mode can only be used in boot files. If a boot file is used but the value of the parameter “specific_model.excluded_model” is not configured, the exclude mode is disabled by default.
------------------	--

TIP

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

Customize a Boot File

Procedure

1. Open a boot template file.
2. To add a configuration file, add `include:config <>` or `include:config “”` to the file. Each starts on a separate line.
3. Specify a configuration file for downloading.
4. For example: `include:config <configure/Teams.cfg>`, `include:config “http://10.2.5.206/configure/account.cfg”`
4. To specify configuration files for specific phone models, add specific phone models in front of `include:config <>*` or `*include:config “”`. Multiple phone model names are separated by commas.
5. For example:
 - `[CP965]include:config <configure/Teams.cfg>`
5. Specify the overwrite mode and exclude mode. For example: `overwrite_mode = 1`, `specific_model.excluded_model = 1`.
6. Save the boot file and place it on the provisioning server.

Configuration Files

Yealink devices support two configuration template files: Common CFG file and MAC-Oriented CFG file. These configuration files contain two kinds of parameters:

- Static: The parameters start with a prefix “static.”, for example, `static.network.ldap.enable`.

- Non-static: The parameters do not start with a prefix “static.” , for example, `phone_setting.phone_lock.enable`.

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

TIP

For protecting against unauthorized access, you can encrypt configuration files. For more information on encrypting configuration files, refer to [Encrypting Configuration Files](#).

Common CFG File

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

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

Device Model	Common CFG file
CP965	y000000000143.cfg
VP59	y000000000091.cfg
MP58/MP58-WH	y000000000135.cfg
MP56	y000000000122.cfg
MP54	y000000000134.cfg
MP52	y000000000145.cfg
MP58 E2	y000000000179.cfg
MP56 E2	y000000000178.cfg
MP54 E2	y000000000177.cfg
MP52 E2	y000000000176.cfg

MAC CFG Files

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

TIP

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

MAC-Oriented CFG Files

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

MAC-Local CFG Files

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

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

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

! TIP

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

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

Configure MAC-Local CFG File

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

Parameter	<code>static.auto_provision.custom.protect</code>
Description	It enables or disables the device to keep user's personalized settings after auto provisioning. ! NOTE The provisioning priority mechanism (phone user interface/web user interface > central provisioning > factory defaults) takes effect only if the value of this parameter is set to 1 (Enabled). If "overwrite_mode" is set to 1 in the boot file, the value of this parameter will be set to 1 (Enabled).
Permi	

tted Value s	0- Disabled 1- Enabled, the <code><MAC>-local.cfg</code> file is generated and personalized non-static settings configured via the web user interface or phone user interface will be kept after auto provisioning.
Default	1

Clear MAC-local CFG File

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

Procedure

1. Select the method according to your device:

Via Device User Interface	Via Web User Interface
• For VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965, tap the account avatar and go to Settings > Device Settings > Debug (default password: admin) > Reset user settings. • For MP52/MP55 E2, go to  > Settings > Device Settings > Debug (default password: admin) > Reset user settings.	Go to Settings > Upgrade > Reset User Settings



TIP

The **Reset user settings** option appears only if you set "static.auto_provision.custom.protect" = 1.

Customize Configuration Files

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

Customize a Configuration File

Procedure

1. Copy and rename a configuration template file. For example, Teams.cfg.
2. Rearrange the parameters in the Teams.cfg, and set the valid values for them.
3. For example: `phone_setting.phone_lock.enable= 1`
3. To specify the parameters for specific phone models, add specific phone models in the front of the corresponding parameters. The names of different phone models are separated by commas.
4. For example:
 - `[CP965]phone_setting.phone_lock.enable= 1`
 - `[MP54]features.bluetooth_enable= 1`
 - These parameters only apply to their own specific phone models.
4. Save the configuration file and place it on the provisioning server.

Configuration File Attributes

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

Attributes	Description
<code>#!version:1.0.0.1</code>	It must be placed in the first line. Do not edit and delete.
Configuration Parameter=Valid Value (<code>screensaver.wait_time=60</code>)	Specify the parameters and values to apply specific settings to the devices. • Separate each configuration parameter and value with an equal sign • Set only one configuration parameter per line • Put the configuration parameter and value on the same line, and do not break the line
<code>[\$MODEL]</code>	The <code>[\$MODEL]</code> can be added in front of configuration parameter to specify the value for specific device models. <code>[\$MODEL]</code> represents the phone model. The valid device model names are: MP58, MP56, MP54, MP52, CP965 and VP59. Multiple phone models are separated by commas. For example, <code>[MP54, CP965]</code>.  NOTE The device updates model-specific configurations and those model- unspecified configurations.

The line beginning with `!` is considered to be a comment. You can use `!` to make any comment in the

boot file.

Resource Files

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

! TIP

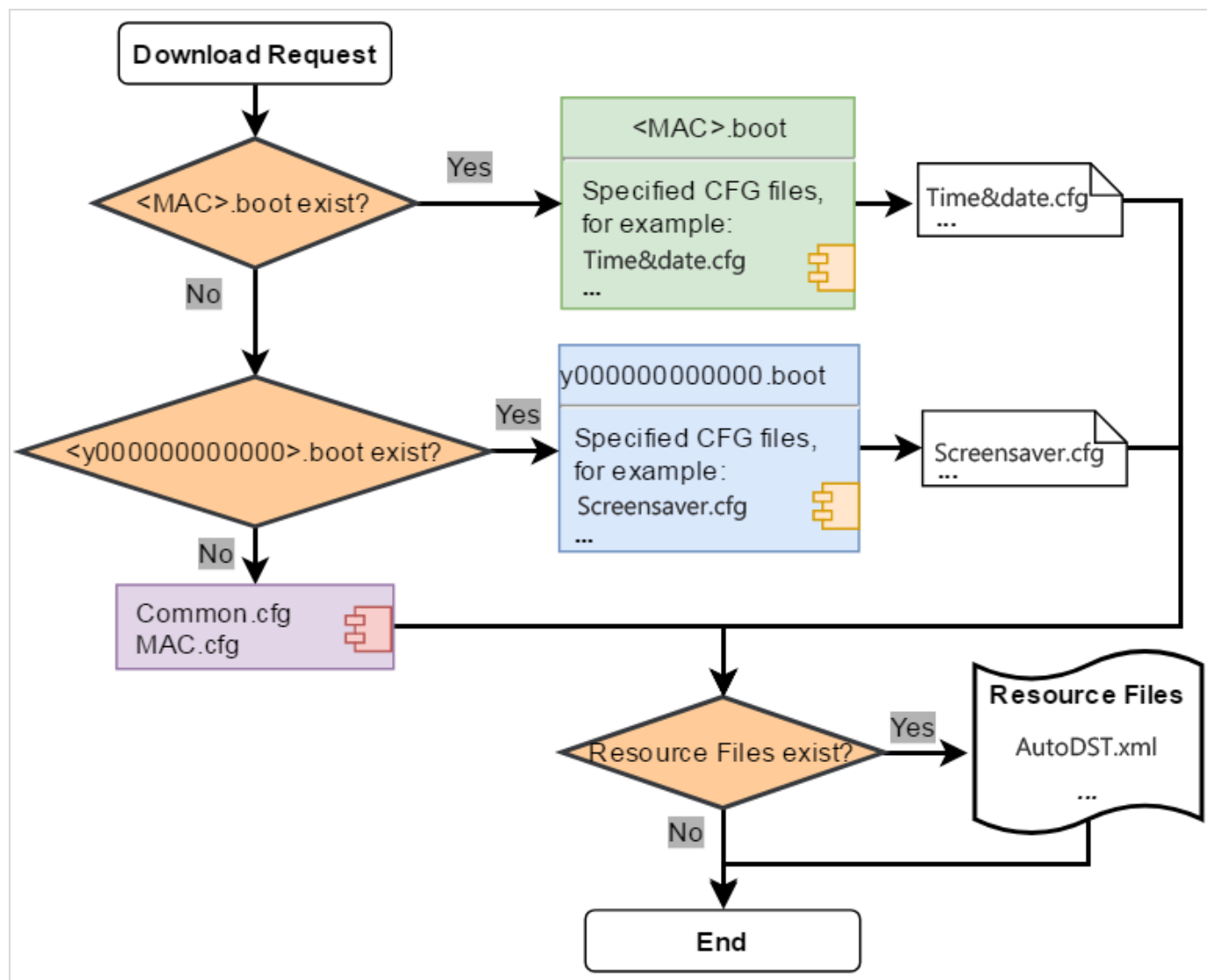
If you want to specify the desired device to use the resource file, the access URL of the resource file should be specified in the MAC-Oriented CFG file. During auto provisioning, the devices will request the resource files in addition to the configuration files.

Yealink supplies some template of resource files for you, so you can directly edit the files as required. The following table lists the resource files Yealink supplies:

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

Files Download Process

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



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

! TIP

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

Provisioning Points to Consider

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

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

This chapter provides basic instructions for setting up your devices with a provisioning server. For more information, refer to [Yealink Teams HD IP Phones Auto Provisioning Guide](#).

Sidetone

Introdcution

Sidetone is audible feedback to someone speaking or otherwise producing sound as an indication of active transmission.

Via Auto Provisioning

```
voice.side_tone
```

Parameter	Permitted Values	Default	Description
voice.side_tone[1]	Integer from -100 to 0	-25	It configures the volume of the sidetone.

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

Bluetooth

Bluetooth enables low-bandwidth wireless connections within a range of 10 meters (32 feet). The range with the best performance is 1 to 2 meters (3 to 6 feet).

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

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

Before You Begin

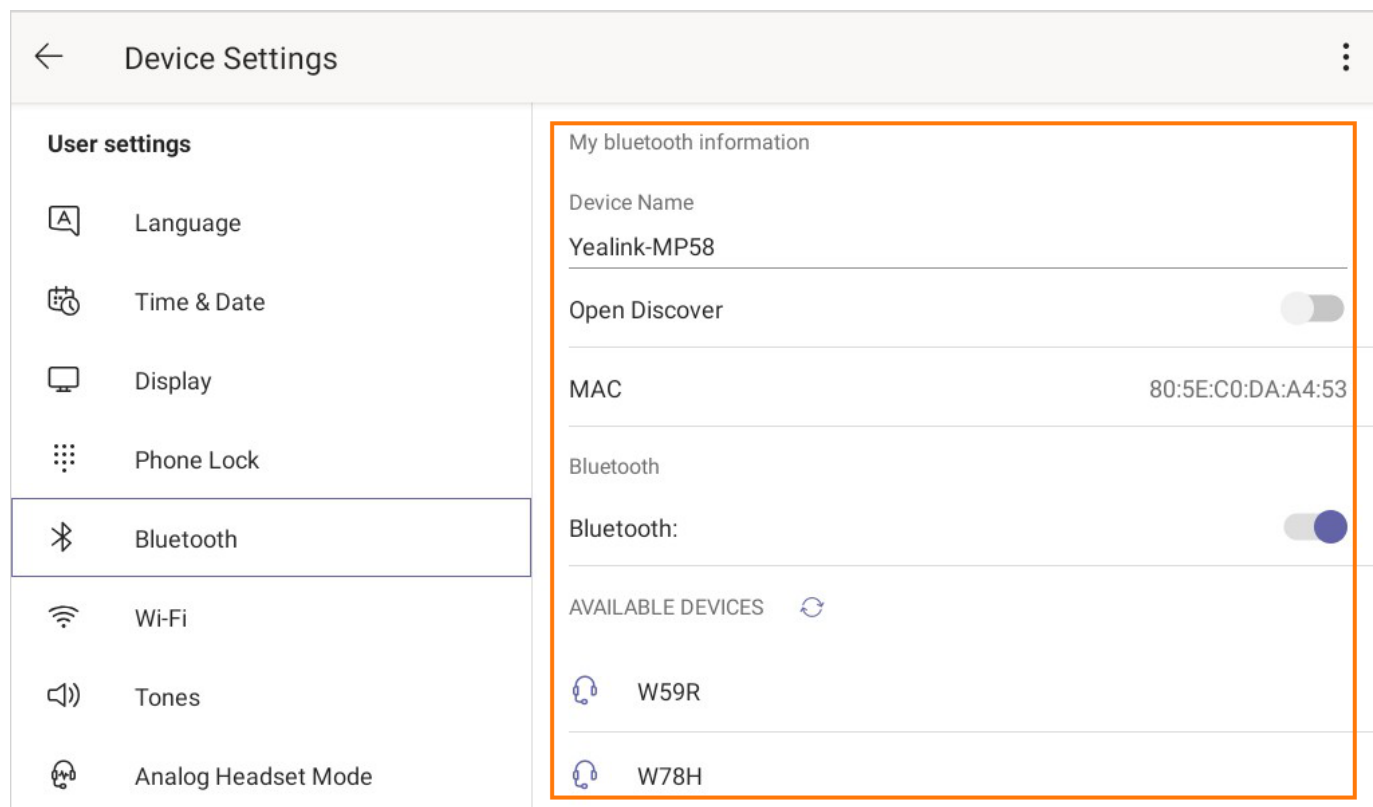
For MP54/MP52 Teams phones, make sure the Bluetooth USB Dongle BT41 is connected to the phone. For MP52 E2 Teams phone, Bluetooth is not supported.

Via Device User Interface

Procedure

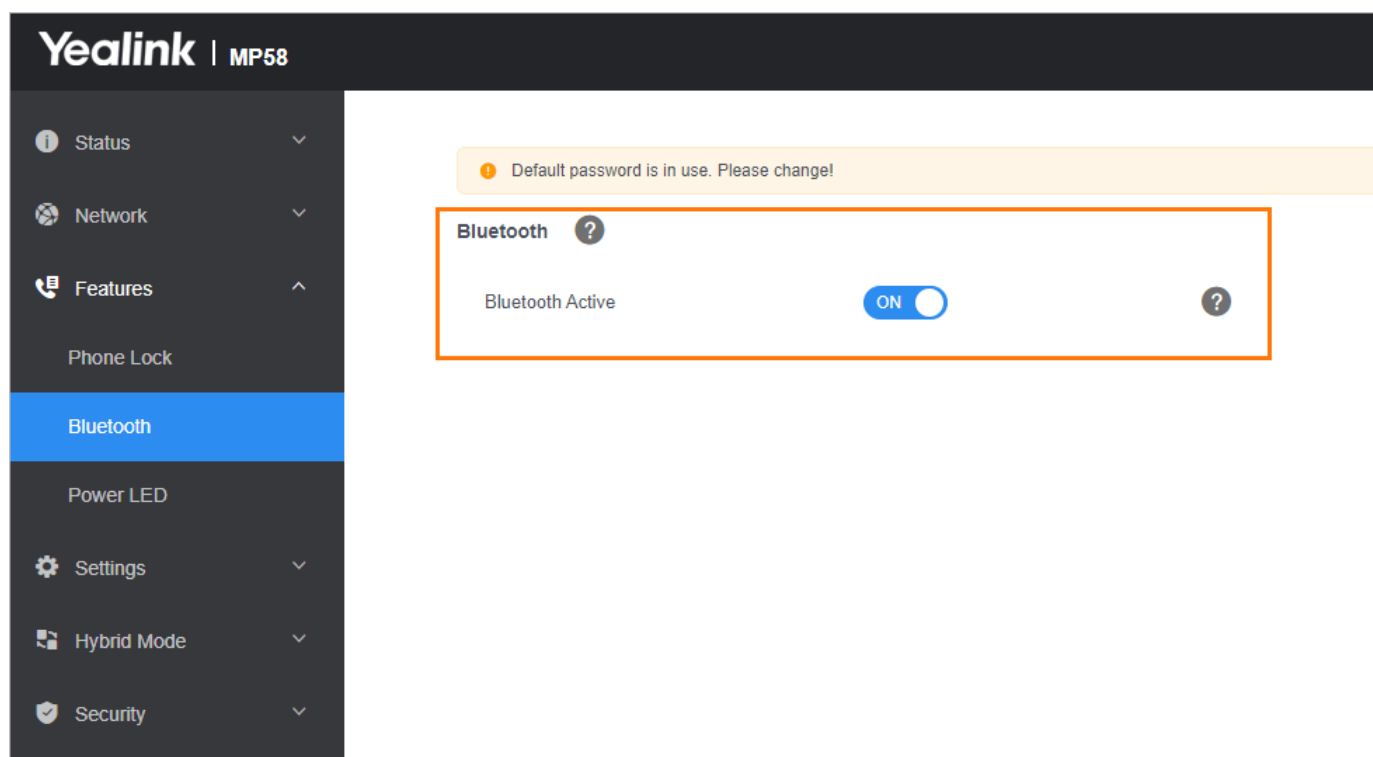
1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52/MP55 E2
Tap the account avatar and go to Settings > Device settings > Bluetooth .	Go to  > Settings > Device Settings > Bluetooth .



Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Features > Bluetooth**.



Via Auto Provisioning

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

--	--

```
static.bluetooth.function.enable[1]
features.bluetooth_enable
features.bluetooth_adapter_name
```

Parameter	Permitted Values	Default	Description
static.bluetooth.function.enable[1]	0 -Disabled 1 -Enabled	1	It enables or disables the ability to trigger the Bluetooth mode.
features.bluetooth_enable	0 -Off 1 -On	1 (0 for MP52/MP54)	It triggers the Bluetooth mode to on or off. ! NOTE It works only if “static.bluetooth.function.enable” is set to 1(Enabled).
features.bluetooth_adapter_name	String within 64 characters	For T58A: Yealink-T58 For T56A: Yealink-T56A For T55A: Yealink-T55A For VP59: Yealink-VP59 For CP965: Yealink-CP965 For MP52: Yealink-MP52 For MP54: Yealink-MP54 For MP56: Yealink-MP56 For MP58/MP58-WH: Yealink-MP58	It configures the Bluetooth device name. ! NOTE It works only if “features.bluetooth_enable” is set to 1 (On).

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

Analog Headset Mode

You can manually configure audio solutions for Yealink RJ headsets YHS36, YHS34, and YHS33.



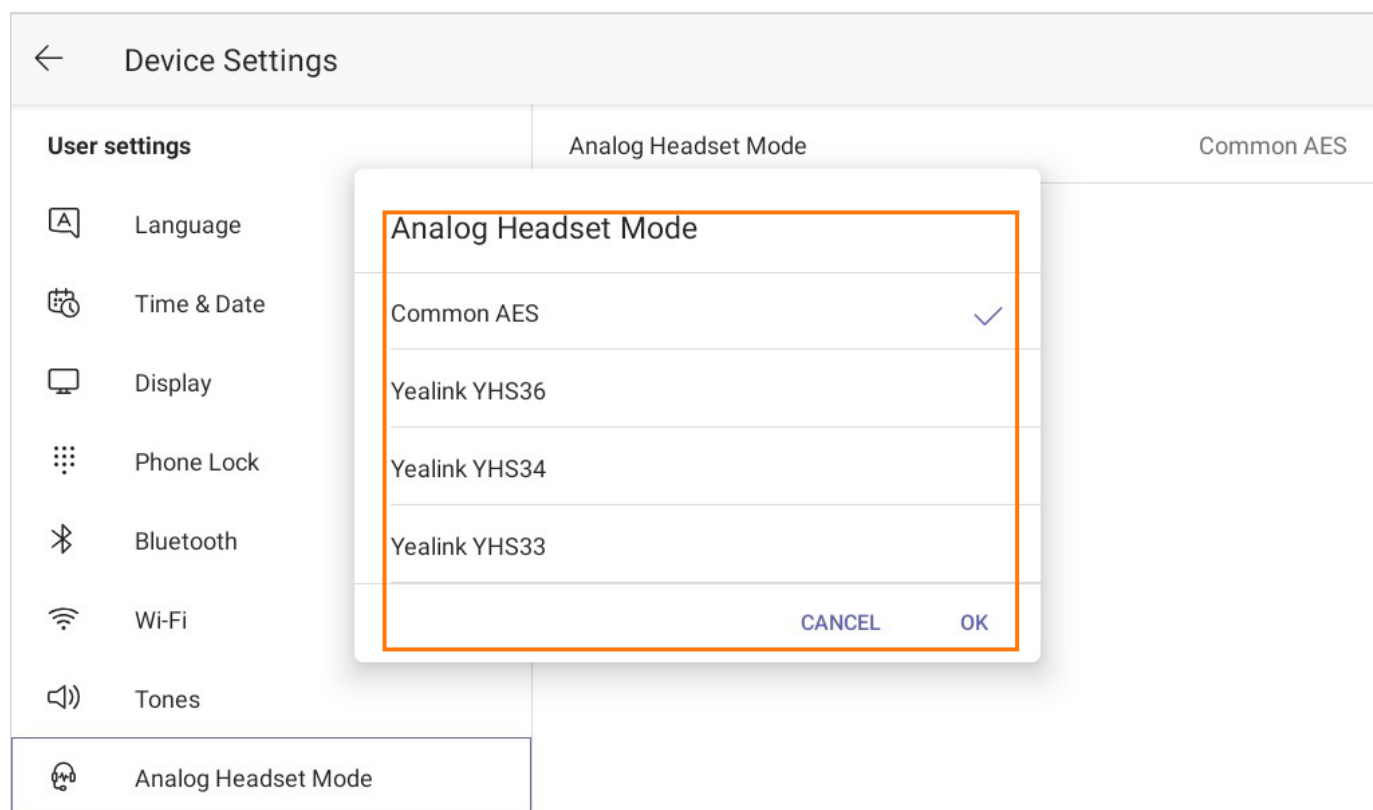
TIP

This feature is unavailable to CP965.

Via Device User Interface

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Analog Headset Mode > Analog Headset Mode .	Go to  > Settings > Device Settings > Analog Headset Mode > Analog Headset Mode .



Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Voice > Analog Headset > Analog Headset Mode**.

Yealink | MP58

Default password is in use. Please change!

Noise Proof

Noise Suppression ☒ ON ?

Smart Noise Block ☒ ON ?

Acoustic Shield ?

Acoustic Shield Mode Auto ?

Acoustic Shield Level 2 ?

Analog Headset

Analog Headset Mode Common ?

Common

Yealink YHS36

Yealink YHS34

Yealink YHS33

Via Auto Provisioning

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

features.analog_headset.mode

Parameter	Permitted Values	Default	Description
features.analog_headset.mode	Common, YHS36, YHS34, YHS33	Common	It sets the audio parameter mode of the analog headset.

Power LED Indicator

Power LED indicator indicates the power status and phone status.

**TIP**

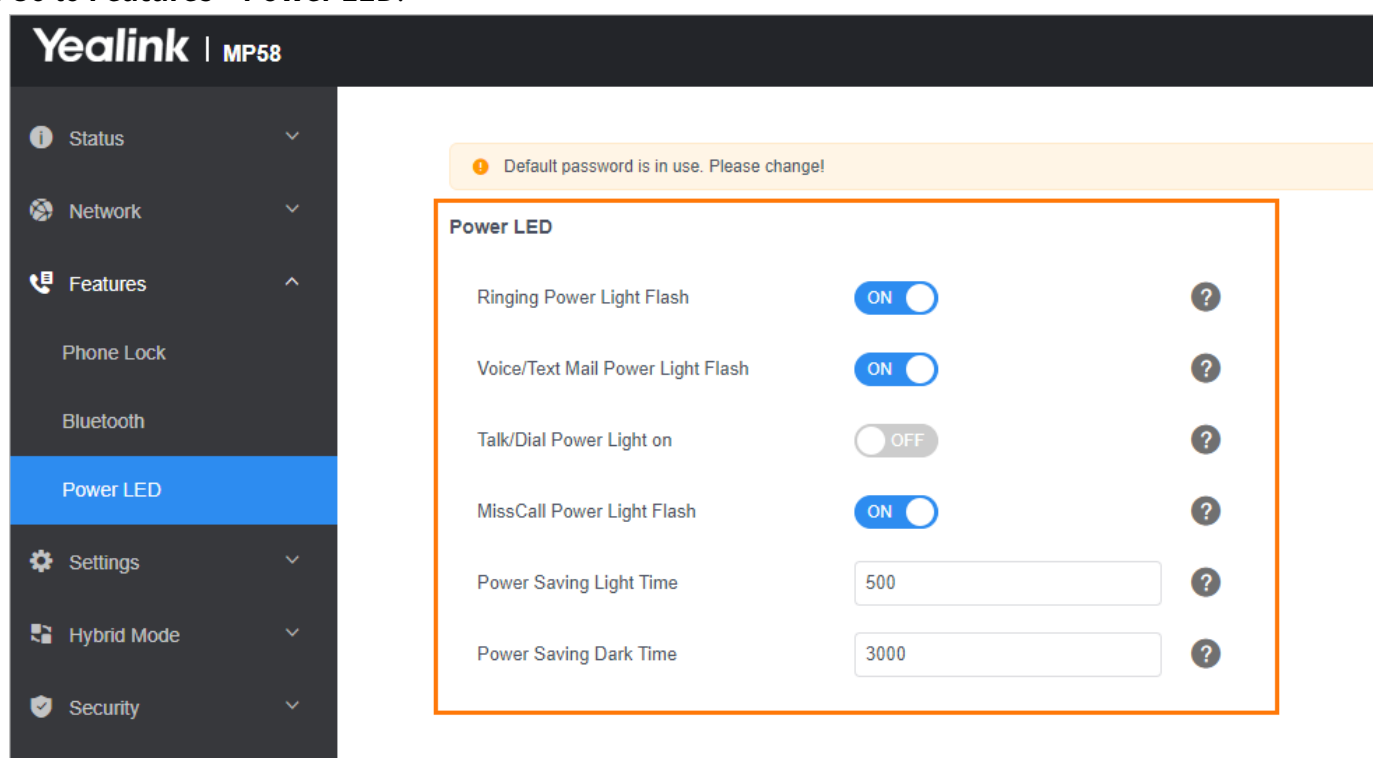
This feature is unavailable to CP965.

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

- The phone receives an incoming call
- The phone is busy
- The phone receives a voice mail
- The phone misses a call
- The phone in the power-saving mode.

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Features > Power LED**.



Via Auto Provisioning

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

phone_setting.ring_power_led_flash_enable

phone_setting.mail_power_led_flash_enable
 phone_setting.talk_and_dial_power_led_enable
 phone_setting.missed_call_power_led_flash.enable
 features.power_saving.power_led_flash.on_time
 features.power_saving.power_led_flash.off_time

Parameter	Permitted- Values	Default	Description
phone_setting.ring_power_led_flash_enable	0 - Disabled (power LED indicator- does not flash) 1 -Enabled (power LED indicator fast flashes (300ms)- red)	1	It enables or disables the power LED indicator to flash- when the phone receives an incoming call.
phone_setting.mail_power_led_flash_enable	0 - Disabled (power LED indicator- does not flash) 1 -Enabled (power LED indicator slowly flashes (1000ms) red)	1	It enables or disables the power LED indicator to flash- when the phone receives a voice mail.
phone_setting.talk_and_dial_power_led_enable	0 - Disabled (power LED indicator is- off) 1 -Enabled (power LED indicator glows red)	0	It enables or disables the power LED indicator to be- turned on when the phone is busy.
phone_setting.missed_call_power_led_flash.enable	0 - Disabled (power LED indicator- does not flash) 1 -Enabled (power LED indicator slowly flashes (1000ms) red)	1	It enables or disables the power LED indicator to flash- when the phone misses a call.
features.power_saving.power_led_flash.on_time	0 , integer from 100 to 10000	500	It configures the period of time (in milliseconds) when- the power LED indicator is on in the power-saving mode.  NOTE If it is set to 0 and

			“features.power_saving.power_led_flash.off_time” is not set to 0, the power LED indicator will be off when the phone enters the power-saving mode.
features.power_saving.power_led_flash.off_time	0, integer from 100 to 10000	3000	It configures the period of time (in milliseconds) when- the power LED indicator is off in the power-saving mode.  NOTE If it is set to 0, the power LED indicator will be on when the phone enters the power-saving mode.

Power Saving

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

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

Customized Power Saving

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

- **Office Hour:** specify the start time and end time of the office hour. You can change the office hours to avoid affecting your work.
- **Idle TimeOut (minutes):** specify the period of time before the phone enters the power-saving mode. You can specify the following three types of idle timeout:
 - **Office Hours Idle TimeOut:** specify the idle timeout for office hours.
 - **Off Hours Idle TimeOut:** specify the idle timeout for non-office hours.
 - **User Input Extension Idle TimeOut:** specify the idle timeout that applies after you use the IP phone (for example, press a key on the phone or pick up/hang up the handset).

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

TIP

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

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Power Saving**.

Yealink | MP58

- Status
- Network
- Features
- Settings
 - Preference
 - Time&Date
 - Upgrade
 - Auto Provision
 - Configuration
 - Voice
 - Tones
 - Power Saving**
 - Hybrid Mode
 - Security

Default password is in use. Please change!

Power Saving ON ?

Office Hour ?

Monday	7 -- 19	?
Tuesday	7 -- 19	?
Wednesday	7 -- 19	?
Thursday	7 -- 19	?
Friday	7 -- 19	?
Saturday	7 -- 7	?
Sunday	7 -- 7	?

Idle TimeOut (minutes) ?

Office Hour Idle TimeOut	120	?
Off Hour Idle TimeOut	10	?
User Input Extension Idle TimeOut	10	?

Via Auto Provisioning

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

```

features.power_saving.intelligent_mode
features.power_saving.enable
features.power_saving.office_hour.idle_timeout
features.power_saving.off_hour.idle_timeout
features.power_saving.user_input_ext.idle_timeout
features.power_saving.office_hour.monday
features.power_saving.office_hour.tuesday
features.power_saving.office_hour.wednesday
features.power_saving.office_hour.thursday
features.power_saving.office_hour.friday
  
```

features.power_saving.office_hour.saturday
 features.power_saving.office_hour.sunday

Parameter	Permitted Values	Default	Description
features.power_saving.intelligent_mode	0 - Disabled, the phone stays in power-saving mode even if the office hour arrives the next day. 1 -Enabled, the phone will automatically identify the office hour and exit power-saving mode once the office hour arrives the next day.	1	It enables or disables the power saving intelligent mode.
features.power_saving.enable	0 - Disabled, the phone automatically enters the power-saving mode to protect the screen when the phone is inactive for 72 hours. Image persistence may be caused on LCD. 1 -Enabled	1	It enables or disables the power saving feature.  NOTE Not applicable to CP965 or devices running Android 15 and above.

features.power_saving.office_hour.idle_timeout	Integer from 1 to 960	120	It configures the time (in minutes) that the phone waits in the idle state before the phone enters power-saving mode during office hours. Example: features.power_saving.office_hour.idle_timeout = 600 The phone will enter power-saving mode when it has been inactivated for 600 minutes (10 hours) during office hours.
features.power_saving.off_hour.idle_timeout	Integer from 1 to 10	10	It configures the time (in minutes) that the phone waits in the idle state before IP phone enters power-saving mode during the non-office hours. Example: features.power_saving.off_hour.idle_timeout = 5 The IP phone will enter power-saving mode when it has been inactivated for 5 minutes during the non-office hours.
features.power_saving.user_input_ext.idle_timeout	Integer from 1 to 30	10	It configures the minimum time (in minutes) that the phone waits in the idle state - after being inactive - before the phone enters power-saving mode. Example: features.power_saving.user_input_ext.idle_timeout = 5
features.power_saving.office_hour.monday	Integer from 0 to 23, Integer from 0	7,19 - for Monday,	It configures the start time and end time of the day's office

features.power_saving.office_hour.tuesday	to 23	Tuesday,	hour. Start time and end time are separated by a comma.
features.power_saving.office_hour.wednesday		Wednesday,	Example:
features.power_saving.office_hour.thursday		Thursday,	features.power_saving.office_hour.monday = 7,19
features.power_saving.office_hour.friday		Friday.	
features.power_saving.office_hour.saturday		7,7 - for	
features.power_saving.office_hour.sunday		Saturday,	
		Sunday.	

Maximum power saving & Intelligent power saving

Maximum Power Saving Mode: The feature reduces the power consumption of the phone. The phone will automatically enter sleep mode after 15 seconds of inactivity, and the screen brightness will be reduced accordingly.

Intelligent power saving: The feature is a new power-saving technology. This system automatically calculates and enters power-saving mode during idle times, standby periods, and screen inactivity. It reports the saved power to the server, providing a web-based overview of energy conservation. There's no need to manually set working hours or standby durations.

! NOTE

These two features are only applicable to Android 15 devices.

Via the Web User Interface

On the web user interface, go to: **Settings > Power Saving**

The screenshot shows the Yealink MP56 E2 web interface. On the left is a dark sidebar with a menu. The 'Settings' option is expanded, showing sub-items: Preference, Time&Date, Yealink Cloud Service, Upgrade, Auto Provision, Configuration, Voice, Tones, **Power Saving** (highlighted in blue), Hybrid Mode, and Security. The main content area displays the 'Power Saving' settings. A dropdown menu is open, showing four options: 'Maximum power saving' (selected and highlighted in blue), 'Off', 'Customized power saving', and 'Intelligent power saving'. A question mark icon is visible in the top right corner of the settings area.

Via Auto Provisioning

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

features.power_saving.mode

Parameter	Permitted Values	Default	Description
features.power_saving.mode	0 -OFF 1 -Customized power saving 2 -Maximum saving power saving 3 -Intelligent	1	It configures the power saving mode of the phone.

	power saving		
--	--------------	--	--

Acoustic Shield

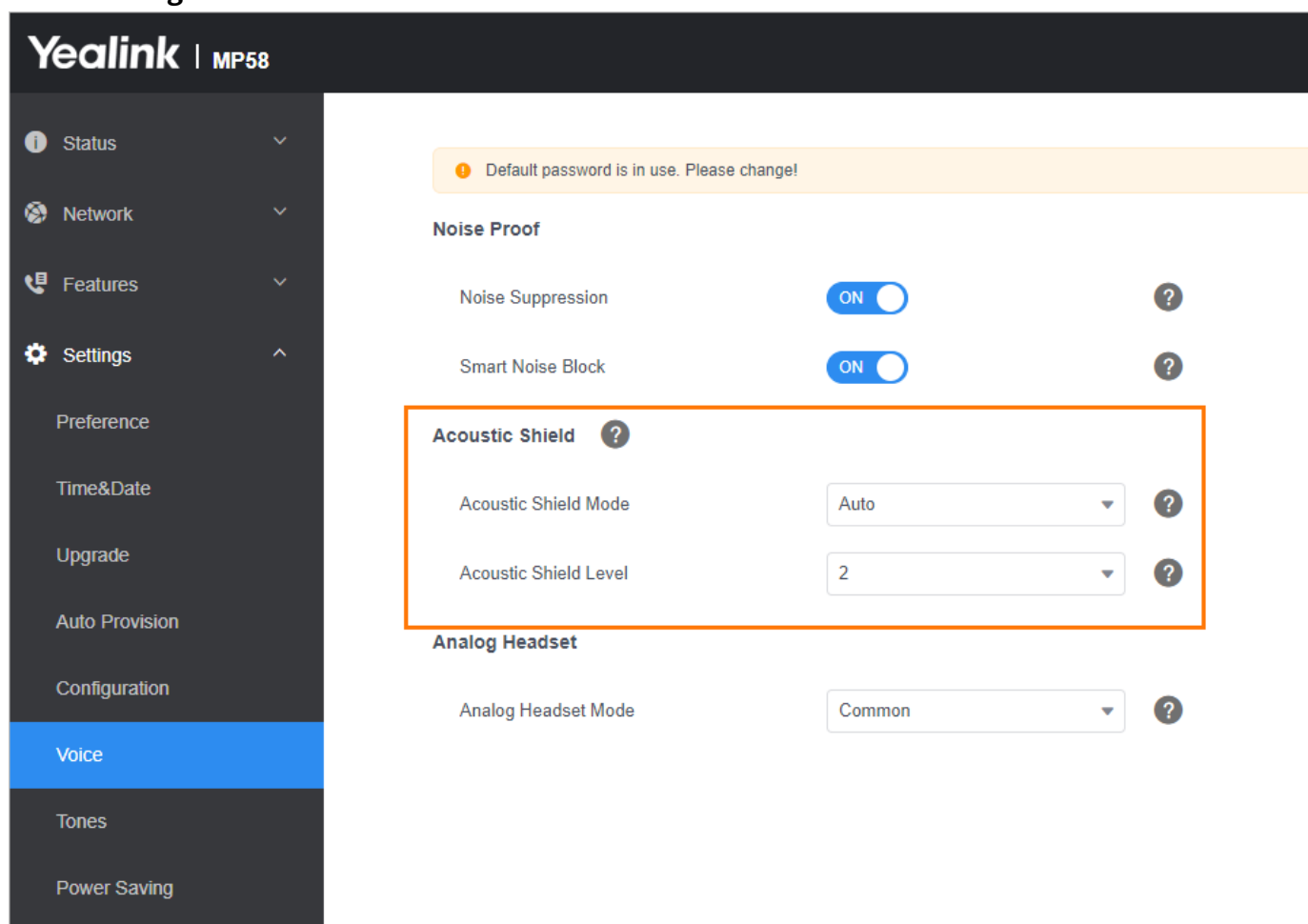
Introduction

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

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

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Voice > Acoustic Shield**.



Via Auto Provisioning

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

```
features.acoustic_shield.mode
```

Parameter	Permitted Values	Default	Description
features.acoustic_shield.mode	0 - Disabled 2 - Auto, the acoustic shield is automatically enabled when the call is set up.	2	It enables or disables the acoustic shield feature during the call.

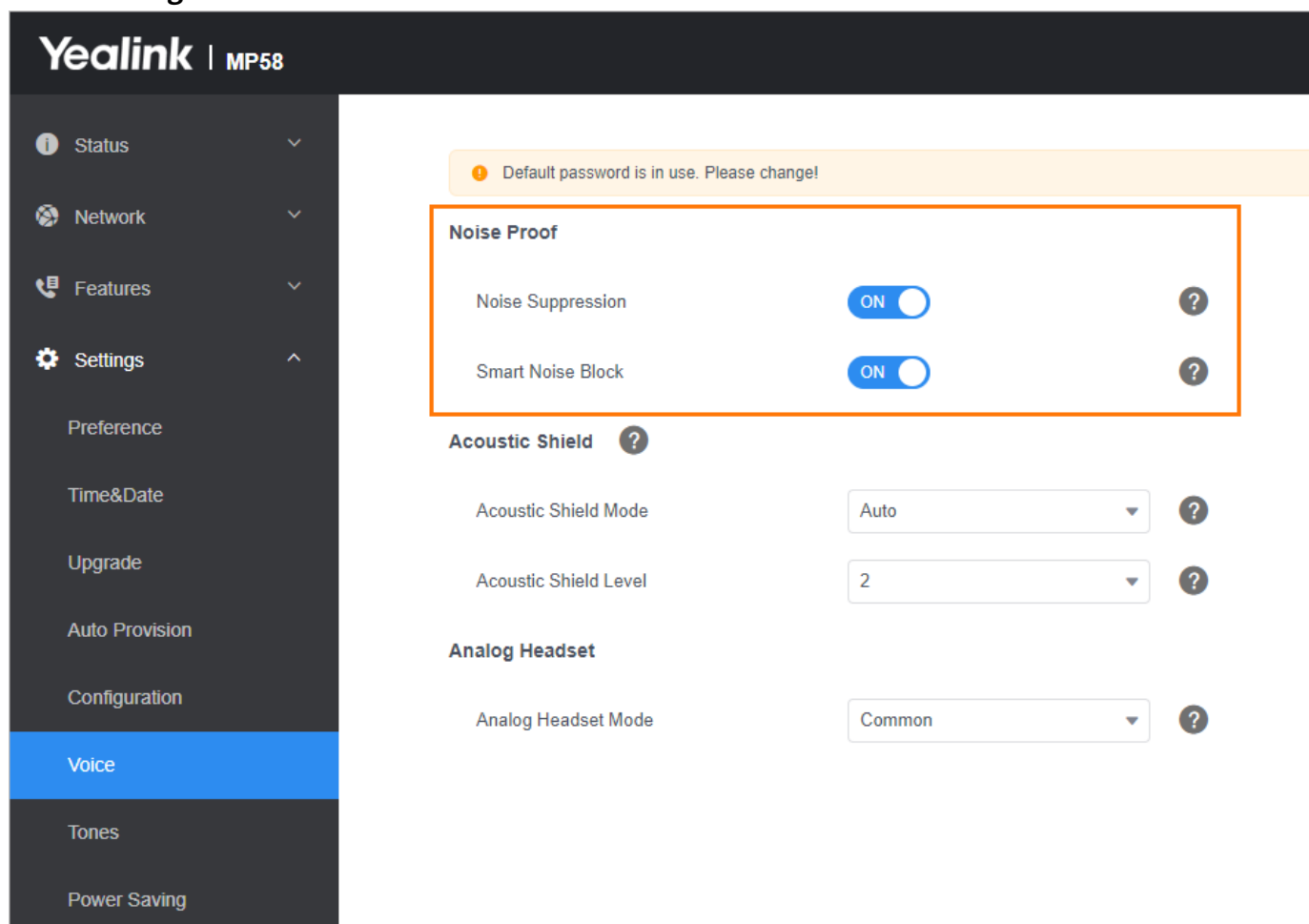
Smart Noise Block

Introduction

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

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Voice > Noise Proof > Smart Noise Block.**



Via Auto Provisioning

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

voice.ans_nb.enable

Parameter	Permitted Values	Default	Description
-----------	------------------	---------	-------------

voice.ans_nb.enable	0 -Disabled 1 -Enabled	1	It enables or disables the Smart Noise Block feature. ! NOTE It works only if “voice.tns.enable” is set to 1 (Enabled).
---------------------	---	---	---

Noise Suppression

Introduction

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

You can enable the Noise Suppression feature to suppress these noises.

Via Web User Interface

- For Android versions below 15: Go to **Settings** > **Voice** > **Noise Proof** > **Noise Suppression**.

The screenshot displays the Yealink MP58 web interface. On the left is a dark sidebar with a menu containing: Status, Network, Features, Settings (expanded), Preference, Time&Date, Upgrade, Auto Provision, Configuration, Voice (highlighted in blue), Tones, and Power Saving. The main content area has a dark header with the Yealink logo and 'MP58'. Below the header is a yellow warning banner that reads 'Default password is in use. Please change!'. The 'Noise Proof' section is highlighted with an orange border and contains two settings: 'Noise Suppression' and 'Smart Noise Block', both with blue 'ON' toggle switches and help icons. Below this is the 'Acoustic Shield' section with a help icon, containing 'Acoustic Shield Mode' (set to 'Auto') and 'Acoustic Shield Level' (set to '2'). The 'Analog Headset' section contains 'Analog Headset Mode' (set to 'Common'). All dropdown menus and toggle switches have associated help icons.

- For **Android 15** and above devices: Go to **Settings** > **Voice** > **Noise Proof Pro** > **Send**.

Yealink | MP56 E2

- Status
- Network
- Features
- Settings
 - Preference
 - Time&Date
 - Yealink Cloud Service
 - Upgrade
 - Auto Provision
 - Configuration
 - Voice**
 - Tones
 - Power Saving
- Hybrid Mode

Noise Proof Pro

Send ☒ ON ?

Receive ☐ OFF ?

Acoustic Shield ?

Acoustic Shield Settings Auto ?

Analog Headset

Analog Headset Mode Common ?

Via Auto Provisioning

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

voice.tns.enable

features.noise_filtering_rev.enable

Parameter	Per mit ted Val ues	Def aul t	Description
voice.tns.enable	0- Dis abl ed 1-	1	It enables or disables the Noise Suppression feature.

	Enabled		
features.noise_filtering_rev.enable	0- Disabled 1- Enabled	0	It enables or disables the phone to block out the slight noise from the far end when there is no speech in a call. Note: After smart noise filtering is enabled, if the far end is playing music or calling a voice service, the background music will also be eliminated when there is no speech in a call.  It is only applicable to Android 15 and above.

Volume

Via Auto Provisioning

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

```
voice.handset.tia4965.enable
voice.headset.tia4965.enable
force.voice.ring_vol
```

Parameter	Permitted Values	Default	Description
voice.handset.tia4965.enable	0 - Disabled 1 -Enabled, if the handset's volume level for the current call is adjusted to level 12/13/14/15, the volume level automatically resets to 11 after the call. That is, the initial volume level is 11 for the next call.	1	It enables or disables the handset's volume level to be reset to level 11 after the call if the volume level for the current call exceeds the standard.
voice.headset.tia4965.enable	0 - Disabled 1 - Enabled, if the headset's volume level for the current call is adjusted to level 12/13/14/15, the volume level automatically resets to 11 after the call. That is, the initial volume level is 11 for the next call.	1	It enables or disables the headset's volume level to be reset to level 11 after the call if the volume level for the current call exceeds the standard.
force.voice.vo	Blank -the user can adjust the ringer volume on the phone.	Blank	It configures the ring tone as a fixed volume.

ice. rin g_v ol	0 to 15 -the user cannot adjust the ringer volume on the phone; the ring tone is the configured volume.	k	 You can set the "force.voice.ring_vol">0 only if "custom.handset.silent_charging" is set to 1.
--------------------------	--	---	--

Tones

Introduction

When the device is in the dialing screen, it will play a warning tone. You can customize tones or select specialized tone sets (vary from country to country) to indicate different conditions of the device.

NOTE

This feature is unavailable to CP965.

Supported Tones

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

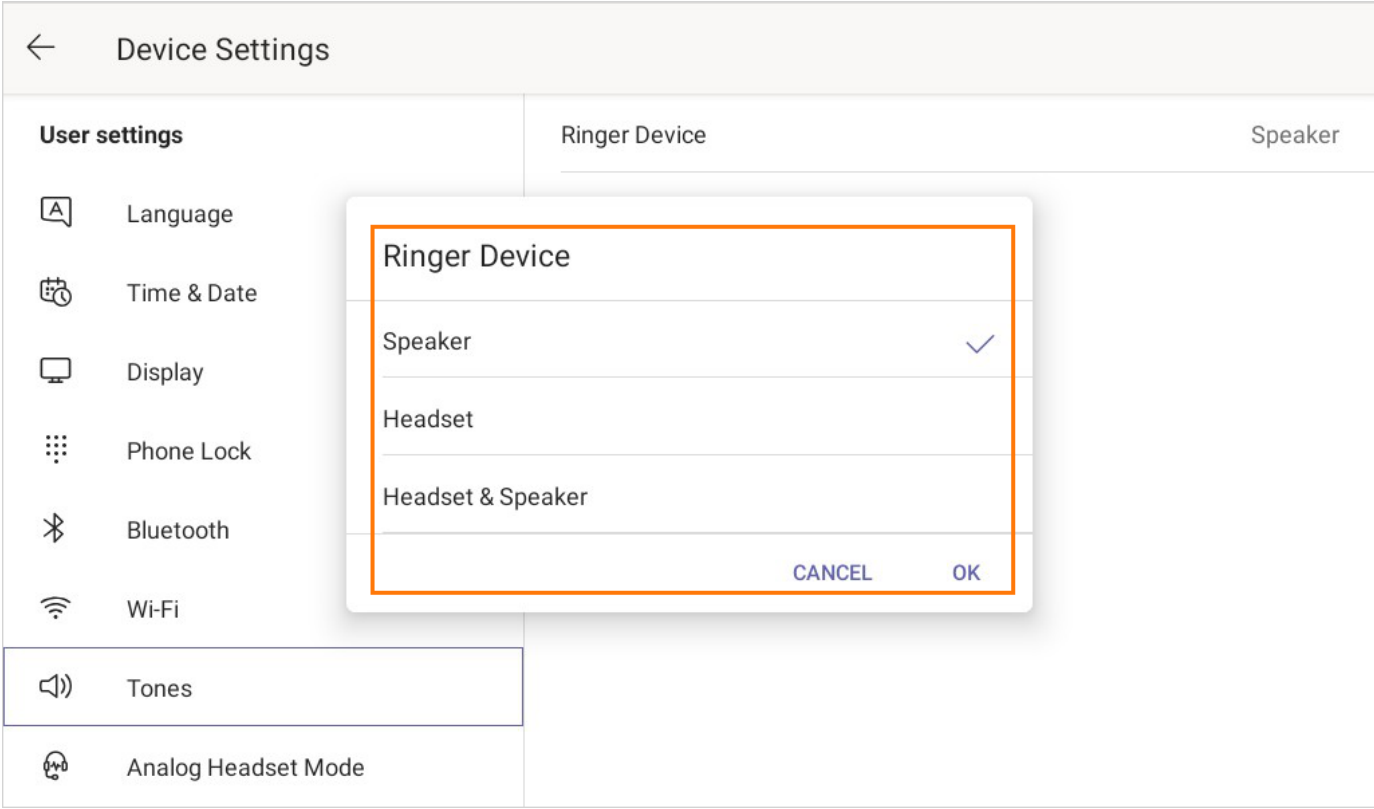
Supported Tones	Supported Tones
Australia	Lithuania
Austria	India
Brazil	Italy
Belgium	Japan
Chile	Mexico
China	New Zealand
Czech	Netherlands
Czech ETSI	Norway
Denmark	Portugal
Finland	Spain
France	Switzerland
Germany	Sweden
Great Britain	Russia
Greece	United States
Hungary	

Configure Tones

Configure Ringer Devices via Device User Interface

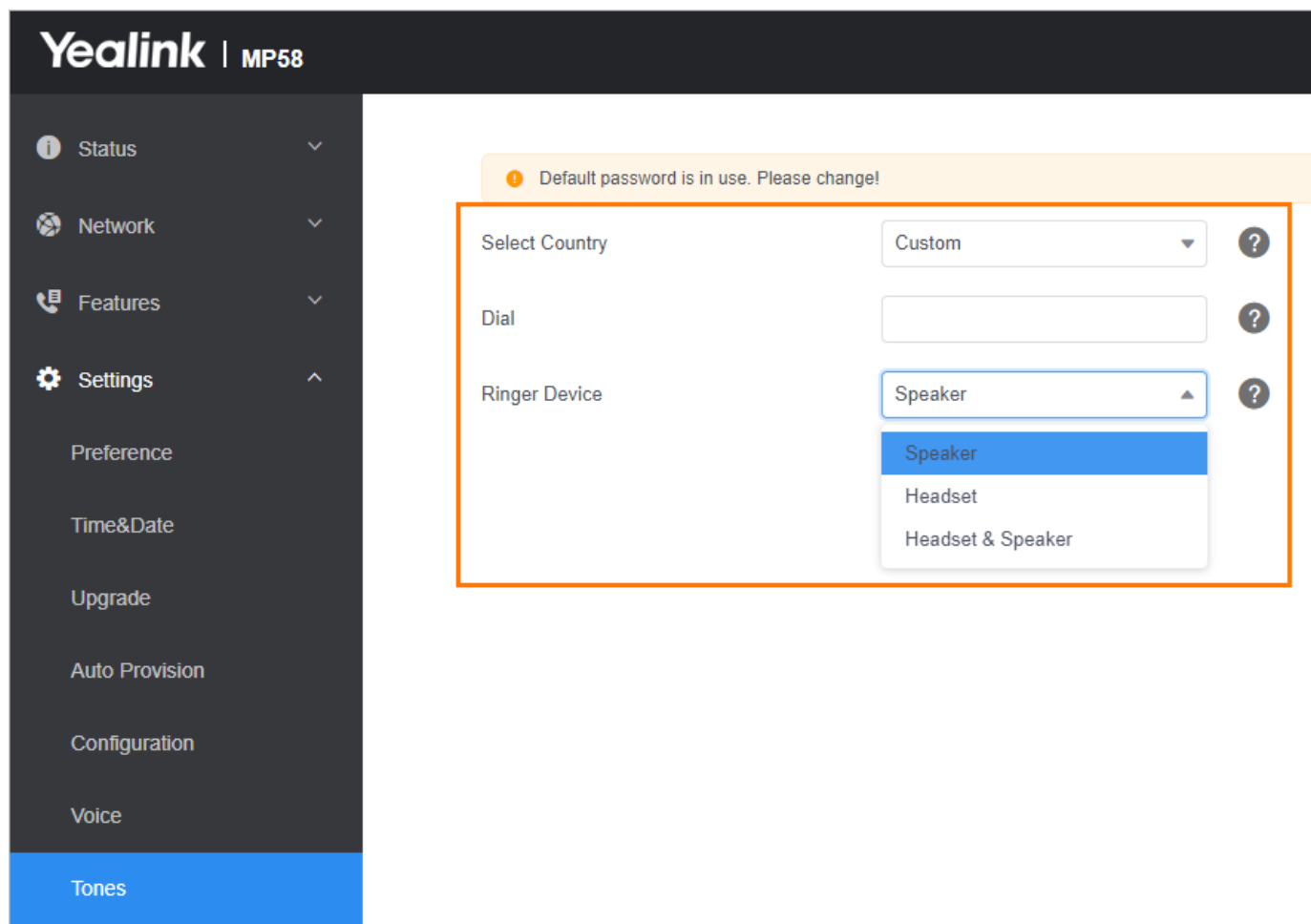
1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Tones.	Go to  > Settings > Device Settings > Tones.



Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Tones.**



Via Auto Provisioning

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

voice.tone.country
 voice.tone.dial
 features.ringer_device.is_use_headset

Parameter	Permitted Values	Default	Description
voice.tone.country	Custom, Australia, Austria, Brazil, Belgium, Chile, China, Czech, Czech ETSI, Denmark, Finland, France, Germany, Great Britain, Greece, Hungary, Lithuania, India, Italy, Japan, Mexico, New Zealand, Netherlands, Norway, Portugal, Spain, Switzerland, Sweden, Russia, United States	Custom	It configures the country tone for the phone.

voice.tone.dial	tone list = element[,element] [,element]... Where element = [!]Freq1[+Freq2][+Freq3][+Freq4] / Duration Freq: the frequency of the tone (ranges from 200 to 4000 Hz). If it is set to 0 Hz, it means the tone is not played. A tone is comprised of at most four different frequencies. Duration: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms. You can configure at most eight different tones for one condition, and separate them by commas. (for example, 250/200, 0/1000, 200+300/500, 200+500+800+1500/1000). If you want the phone to play tones once, add an exclamation mark “!” before tones (for example, ! 250/200,0/1000, 200+300/500,200+500+800+1500/1000).	/	It customizes the dial tone. ! NOTE It works only if “voice.tone.country” is set to Custom.
features.ringer_device.is_use_headset	0- Use Speaker 1- Use Headset 2- Use Headset & Speaker	0	It configures the ringer device for the phone.

Time and Date

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

Time Zone

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

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, La Paz, 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/	Mountain Time (US &	+4	Europe/	Izhevsk, Samara (RTZ

	Denver	Canada)		Samara	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)	+4:3 0	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/ Yekaterinbu rg	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	+5:3 0	Asia/ Calcutta	Chennai, Kolkata, Mumbai, New Delhi
-4	America/ Caracas	Caracas	+5:3 0	Asia/ Colombo	Sri Jayawardenepura
-4	America/ Cuiaba	Cuiaba	+5:4 5	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)
-2:3 0	America/ St_Johns	Newfoundland	+6:3 0	Asia/ Rangoon	Yangon (Rangoon)
-3	America/ Brasilia	Brasilia	+7	Asia/	Bangkok, Hanoi,

	Bahia			Bangkok	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_Lump ur	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	+9:3 0	Australia/ Adelaide	Adelaide
+1	Europe/ Dublin	Dublin, Edinburgh, Lisbon, London	+9:3 0	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	+12	Asia/	Petropavlovsk-

	Windhoek			Kamchatka	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	+8:4 5	Australia/ Eucla	Eucla
+2	Africa/Cairo	Cairo	+3	Asia/Gaza	Gaza
+3	Asia/ Damascus	Damascus	+2	Europe/ Luxembourg	Luxembourg
+3	Europe/ Chisinau	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	-9:3 0	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

Configure NTP

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

Via Device User Interface

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
---	--------------------------

Tap the account avatar and go to **Settings > Device Settings > Time & Date**.

Go to  > **Settings > Device Settings > Time & Date**.

← Device Settings

User settings

 Language

 Time & Date

 Display

 Bluetooth

 Wi-Fi

 Tones

 Analog Headset Mode

 Accessibility

General

Type

SNTP Settings

Time Zone

(UTC) Coordinated Universal Time

NTP Server1

north-america.pool.ntp.org

NTP Server2

pool.ntp.org

Date & Time Format

Date Format

WWW MMM DD

Time Format

12 Hour

Via Web User Interface

1. [Log in to the phone web user interface as an admin](#).
2. Go to **Settings > Time & Date**.

Yealink | MP58

Status

Network

Features

Settings

Preference

Time&Date

Upgrade

Auto Provision

Configuration

Voice

Tones

Default password is in use. Please change!

Time&Date

Manual Time

OFF

?

NTP by DHCP Priority

High

?

Primary Server

north-america.pool.ntp.org

?

Secondary Server

pool.ntp.org

?

Update Interval (15~86400s)

1000

?

Time Zone

(UTC) Coordinated Universal ...

?

Time Format

Hour 12

?

Date Format

WWW MMM DD

?

Via Auto Provisioning

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

local_time.manual_ntp_srv_prior
 local_time.ntp_server1
 local_time.ntp_server2
 local_time.interval
 local_time.android_time_zone

Parameter	Permitted Values	Default	Description
local_time.manual_ntp_srv_prior	0 - High (use the NTP server address offered by the DHCP server preferentially) 1 - Low (use the	0	It configures the priority for the device to use the NTP server address offered by the DHCP server.

	NTP server address configured manually preferentially)		
local_time.ntp_server1	IP address or domain name	time.windows.com	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.
local_time.ntp_server2	IP address or domain name	pool.ntp.org	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.
local_time.interval	Integer from 15 to 86400	1000	It configures the interval (in seconds) at which the device updates time and date from the NTP server.
local_time.android_time_zone	String within 64 characters	Asia/Shanghai	It configures the time zone in the tzdata 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)

DST Settings

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

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

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

Auto DST File Customization

Before customizing, you need to obtain the AutoDST file. You can ask the distributor or Yealink FAE for DST template.

Auto DST File Attributes

Attribute	Type	Values	Description
szTime	required	[+/-][X]:[Y], X=0-14, Y=0-59	Time Zone
szZone	required	String (if the content is more than one city, it is best to keep their daylight saving time the same)	Time Zone name
iType	optional	0/10: DST by Date 1: DST by Week	DST time type(This item is needed if you want to configure DST.)
szStart	optional	Month/Day/Hour (for iType=0) Month: 1-12 Day: 1-31 Hour: 0 (midnight)-23 Month/Week of Month/Day of Week/ Hour of Day (for iType=1) Month: 1-12 Week of Month: 1-5 (the last week) Day of Week: 1-7 Hour of Day: 0 (midnight)-23	Starting time of the DST
szEnd	optional	Same as szStart	Ending time of the DST
szOffset	optional	Integer from -300 to 300	The offset time (in minutes) of DST

Customize Auto DST File

Procedure

1. Open the AutoDST file.
2. To add a new time zone, add `<DST szTime="" szZone="" iType="" szStart="" szEnd="" szOffset="" />` between `<DSTData>` and `</DSTData>`.
3. Specify the DST attribute values within double quotes. For example:
4. Add a new time zone (+6 Paradise) with daylight saving time 30 minutes:
5. `<DST szTime="+6" szZone="Paradise" iType="1" szStart="3/5/7/2" szEnd="10/5/7/3" szOffset="30" />`

```

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

```

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

```

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

```

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

Configure DST via Auto Provisioning

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

```

local_time.summer_time
local_time.dst_time_type
local_time.start_time
local_time.end_time

```

local_time.offset_time
auto_dst.url

Parameter	Permitted Values	Default	Description
local_time.summer_time	0 - Disabled 1 - Enabled 2 - Automatic	2	It configures Daylight Saving Time (DST) feature.
local_time.dst_time_type	0 - DST by Date 1 - DST by Week	0	It configures the Daylight Saving Time (DST) type. NOTE It works only if “local_time.summer_time” is set to 1 (Enabled).
local_time.start_time	Month/Day/Hour-DST by Date, use the following mapping: Month: 1=January, 2=February,..., 12=December Day: 1=the first day in a month,..., 31=the last day in a month Hour: 0=0am, 1=1am,..., 23=11pm Month/Week of Month/Day of Week/ Hour of Day- DST by Week, use the following mapping: Month: 1=January, 2=February,..., 12=December Week of Month: 1=the first week in a month,..., 5=the last week in a month Day of Week: 1=Monday, 2=Tuesday,..., 7=Sunday Hour of Day: 0=0am, 1=1am,..., 23=11pm	1/1 /2 00 0	It configures the start time of the Daylight Saving Time (DST). NOTE It works only if the “local_time.summer_time” is set to 1 (Enabled).
local_time	Month/Day/Hour-DST by Date, use the	12	It configures the end time of the

e.end_time	following mapping: Month: 1=January, 2=February,..., 12=December Day: 1=the first day in a month,..., 31=the last day in a month Hour: 0=0am, 1=1am,..., 23=11pm Month/Week of Month/Day of Week/ Hour of Day- DST by Week, use the following mapping: Month: 1=January, 2=February,..., 12=December Week of Month: 1=the first week in a month,..., 5=the last week in a month Day of Week: 1=Monday, 2=Tuesday,..., 7=Sunday Hour of Day: 0=0am, 1=1am,..., 23=11pm	/31 /2 02 3	Daylight Saving Time (DST). ! NOTE It works only if “local_time.summer_time” is set to 1 (Enabled).
local_time.offset_time	Integer from -300 to 300	Blank	It configures the offset time (in minutes) of Daylight Saving Time (DST). ! NOTE It works only if “local_time.summer_time” is set to 1 (Enabled).
auto_dst.url	URL within 511 characters	Blank	It configures the access URL of the DST file (AutoDST.xml). ! NOTE It works only if “local_time.summer_time” is set to 2 (Automatic).

Manually Configure Time and Date

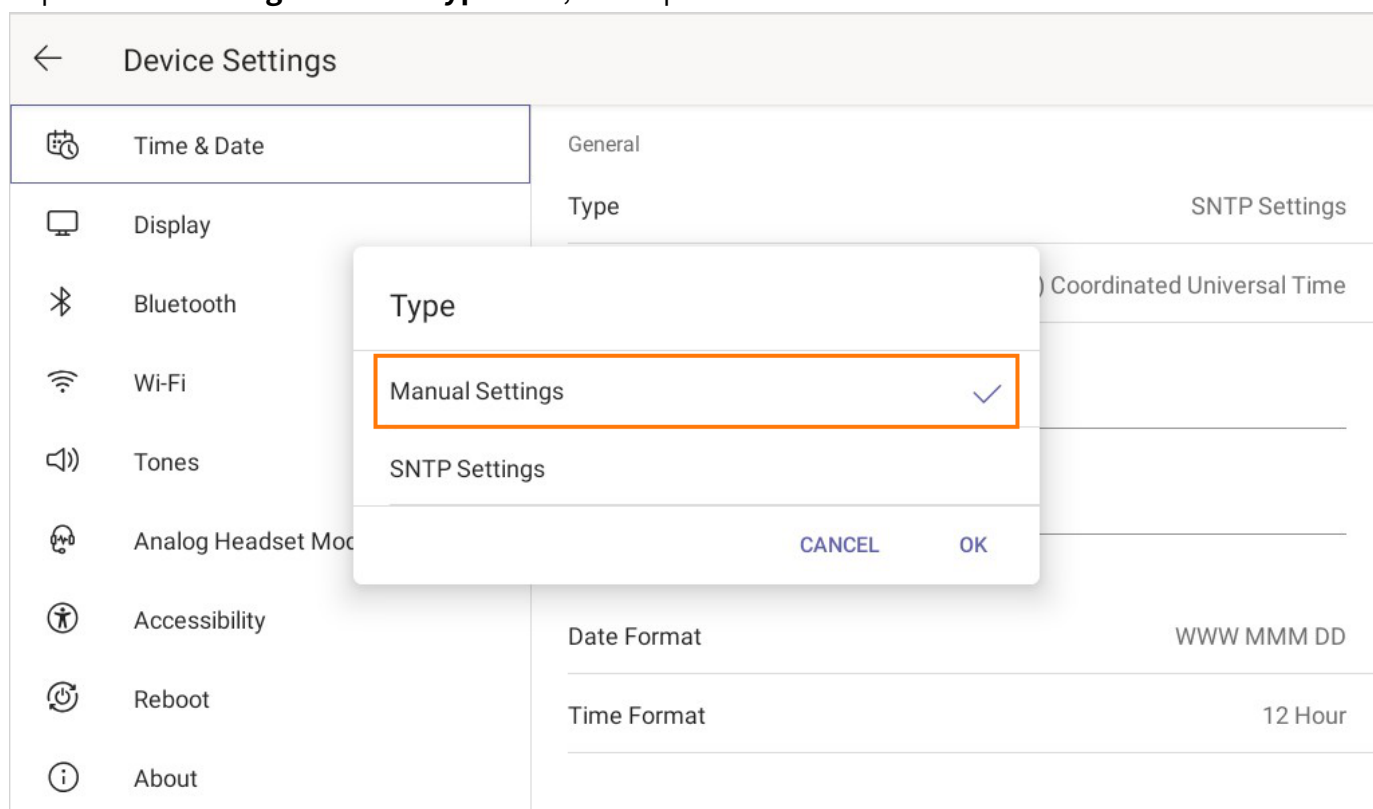
You can set the time and date manually when the devices cannot obtain the time and date from the NTP time server.

Via Device User Interface

1. Select the method according to your device:

VP59/MP5X (E2)	CP965
Go to  > Settings > Device Settings > Time & Date .	Tap the avatar in the top-right corner of the screen and go to Settings > Device Settings > Time & Date .

2. Tap **Manual Settings** from the **Type** field, and tap **OK**.



3. Enter the specific date and time in the **Date** and the **Time** fields respectively.

← Device Settings

- Time & Date
- Display
- Bluetooth
- Wi-Fi
- Tones
- Analog Headset Mode
- Accessibility
- Reboot
- About

General

Type Manual Settings

Date 2023-03-28

Time 06:36:24 AM

Date & Time Format

Date Format WWW MMM DD

Time Format 12 Hour

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Time & Date**.
3. Enable **Manual Time**.

Yealink | MP58

Default password is in use. Please change!

Time&Date

Manual Time ☒

Date 2023 Year 3 Month 28 Day

Time 6 Hour 35 Minute 42 Second

Time Format Hour 12

Date Format WWW MMM DD

Via Auto Provisioning

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

local_time.manual_time_enable

Parameters	Permitted Values	Default	Description
local_time_manual_time_enable	0 - Disabled (obtain time and date from NTP server) 1 - Enabled (obtain time and date from manual settings)	0	It enables or disables the device to obtain time and date from manual settings.

Configure the Format for Time and Date

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.

Via Device User Interface

1. Select the method according to your device:

VP59/MP5X (E2)	CP965
 1. Go to Settings > Device Settings > Time & Date > Time & Date Format .	Tap the avatar in the top-right corner of the screen and go to Settings > Device Settings > Time & Date > Time & Date Format .


Device Settings


Time & Date

 Display
  Bluetooth
  Wi-Fi
  Tones
  Analog Headset Mode
  Accessibility
  Reboot
  About

General

Type

Manual Settings

Date

2023-03-28

Time

06-36-24 AM

Date & Time Format

Date Format

WWW MMM DD

Time Format

12 Hour

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Time & Date.**
3. Enable **Manual Time.**

Yealink | MP58

Default password is in use. Please change!

Time&Date

Manual Time ☒ ON ?

Date 2023 Year 3 Month 28 Day ?

Time 6 Hour 35 Minute 42 Second ?

Time Format Hour 12 ?

Date Format WWW MMM DD ?

Via Auto Provisioning

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

local_time.time_format

local_time.date_format

Parameter s	Permitted Values	Def aul t	Description
local_time .time_form at	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).	1	It configures the time format.
local_time .date_form at	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	0	It configures the date format.

	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; YYY represents a four-digit year YY represents a two-digit year.		
--	--	--	--

Backlight

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

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

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

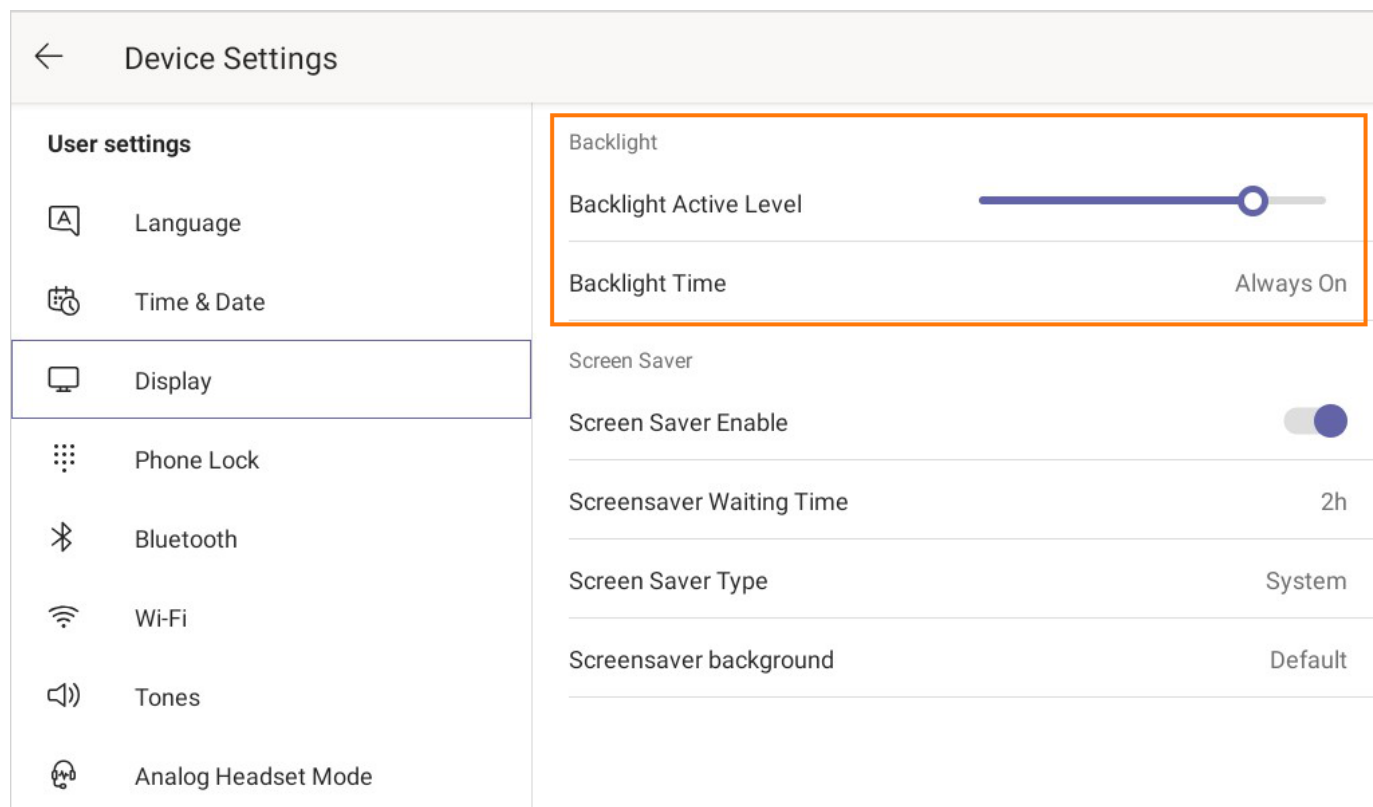
Backlight Time: The delay time to change the brightness of the LCD backlight when the device is inactive. Backlight time includes the following settings:

- **Always On:** Backlight is on permanently.
- (Via device or web user interfaces) **15 s, 30 s, 1 min, 2 min, 5 min, 10 min, 30 min,** or **1 h:** Backlight is turned off when the phone is inactive after the designated time.
- (Only via auto provisioning) **30 min, 1 h, 2 h, 4 h, 6 h, 8 h,** or **12 h:** Backlight is changed when the device is inactive after the designated time (in seconds).

Via Device User Interface

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Display > Backlight .	Go to  > Settings > Device Settings > Display > Backlight .



2. Slide the **Backlight Active Level** slider to change the brightness of the LCD backlight.
3. Select the desired time from the **Backlight Time** field.
4. Save the change.
5. If your phone is set as a common area phone, select the method according to your device:

VP59/MP58/MP56/MP54/CP965	MP52/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Display (admin only, default password: admin) > Screen Saver Enable to disable the screen saver.	Go to  > Settings > Device Settings > Display (admin only, default password: admin) > Screen Saver Enable to disable the screen saver.

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings** > **Preference** > **Backlight**.

Yealink | MP58

- Status
- Network
- Features
- Settings
- Preference**
- Time&Date
- Upgrade
- Auto Provision
- Configuration
- Voice
- Tones
- Power Saving

Backlight

Active Level: 8 ?

Backlight Time (seconds): Always On ?

Screensaver

Screensaver: ON ?

Screensaver Wait Time: 2 h ?

Screensaver Type: System ?

Screensaver Background: Default.jpg ?

Screen Capture

Screen Capture: OFF ?

Via Auto Provisioning

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

phone_setting.active_backlight_level
phone_setting.backlight_time

Parameter	Permitted Values	Default	Description
phone_setting.active_backlight_level	Integer from 1 to 10	8	It configures the intensity of the LCD backlight when the device is active.
phone_setting.backlight_time	0-Always On 1800-30	0	It configures the delay time (in seconds) to change the intensity of the LCD backlight when the device is inactive.

	min 3600-1 h 7200-2 h 14400-4 h 21600-6 h 28800-8 h 43200-1 2 h		
--	---	--	--

Screen Saver

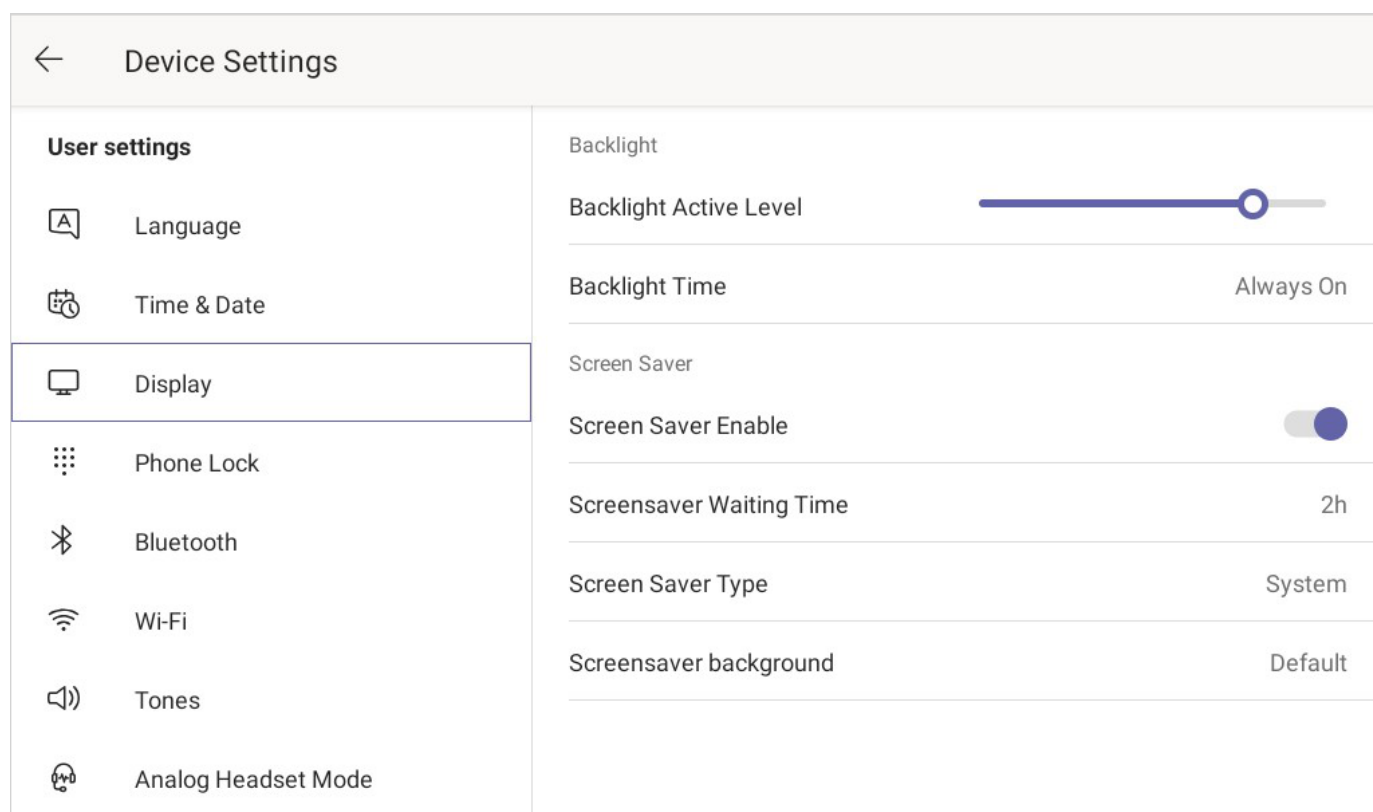
The screen saver will automatically start when the device is idle for the preset waiting time. You can stop the screen saver and return to the idle screen at any time by pressing a key on the device or tapping the touch screen. When your device is idle again for a preset waiting time, the screen saver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

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

Via Device User Interface

1. Select the method according to your device:

VP59 / MP58 / MP56 / MP54 / CP965	MP52/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Display > Screen Saver .	Go to  > Settings > Device Settings > Display > Screen Saver .



Via Web User Interface

1. [Log in to the phone web user interface as an admin](#).
2. Go to **Settings > Preference > Screensaver > Screensaver**.

The screenshot shows the Yealink MP58 web interface. On the left is a dark sidebar with a menu. The 'Preference' option is highlighted in blue. Below it are 'Time&Date', 'Upgrade', 'Auto Provision', 'Configuration', 'Voice', 'Tones', and 'Power Saving'. The main content area is white. At the top, it says 'Yealink | MP58'. Below this, there are sections for 'Backlight' and 'Screensaver'. The 'Backlight' section has 'Active Level' set to 8 and 'Backlight Time (seconds)' set to 'Always On'. The 'Screensaver' section is highlighted with an orange border and contains four settings: 'Screensaver' (ON), 'Screensaver Wait Time' (2 h), 'Screensaver Type' (System), and 'Screensaver Background' (Default.jpg). Below this is the 'Screen Capture' section with 'Screen Capture' set to OFF. Each setting has a help icon (question mark) to its right.

Via Auto Provisioning

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

screensaver.enable
 screensaver.wait_time
 screensaver.type
 screensaver.upload_url
 screensaver.background
 screensaver.delete

Parameter	Permitted Values	Default	Description
screensaver.enable	0-Disabled 1-Enabled	1	It enables or disables the screen saver.
screensaver.wait_time	30-30 s 60-1 min	900	It configures the time (in seconds) that the device waits

	120-2 min 300-5 min 600-10 min 900-15 min 1200-20 min 1800-30 min 2700-45 min 3600-1 h 7200-2 h		in the idle state before the screen saver starts.
screensaver.type	0 -System, the LCD screen will display the built-in picture. 4 -Custom, the LCD screen will display the custom screen saver images (configured by the parameter “screensaver.upload_url”). If multiple images are uploaded, the device will display all images alternately every 60 seconds.	Blank	It configures the type of screen saver to display.
screensaver.upload_url	URL within 511 characters	Blank	It configures the access URL of the custom screensaver background.
screensaver.background	Default.jpg 01.png 02.png 03.png 04.png 05.png 06.png 07.png 08.png	Default.jpg	It configures the background for the screen saver.
screensaver.delete	String	Blank	It deletes the specified or all custom screensaver backgrounds. Example:

		- Delete all custom screensaver backgrounds: screensaver.delete = http://localhost/all - Delete a custom screensaver background (for example, Screenshot.jpg): screensaver.delete = http://localhost/Screenshot.jpg
--	--	---

Language

Introduction

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

You can ask the distributor or Yealink FAE for language packs. You can also obtain the language packs online: <https://support.yealink.com/en/portal/home>

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

Device User Interface/Endpoint

Language	Language Pack
English (United States)	000.GUI.English.lang
English (United Kingdom)	001.GUI.English_UK.lang
Simplified Chinese	002.GUI.Chinese_S.lang
Traditional Chinese	003.GUI.Chinese_T.lang
French	004.GUI.French.lang
German	005.GUI.German.lang
Italian	006.GUI.Italian.lang
Polish	007.GUI.Polish.lang
Portuguese	008.GUI.Portuguese.lang
Spanish	009.GUI.Spanish.lang
Turkish	010.GUI.Turkish.lang
Russian	011.GUI.Russian.lang
Dutch	012.GUI.Netherlands.lang
Japanese	013.GUI.Japanese.lang

Web User Interface

Language	Language Pack	Note Language Pack
English (United States)	1.English.js	1.English_note.xml
English (United Kingdom)	2.English_UK.js	/

Chinese Simplified	3.Chinese_S.js	2.Chinese_S_note.xml
Chinese Traditional	4.Chinese_T.js	3.Chinese_T_note.xml
French	5.French.js	4.French_note.xml
German	6.German.js	5.German_note.xml
Italian	7.Italian.js	6.Italian_note.xml
Polish	8.Polish.js	7.Polish_note.xml
Portuguese	9.Portuguese.js	8.Portuguese_note.xml
Spanish	10.Spanish.js	9.Spanish_note.xml
Turkish	11.Turkish.js	10.Turkish_note.xml
Russian	12.Russian.js	11.Russian_note.xml
/	/	/
Japanese	13.Japanese.js	12.Japanese_note.xml

Configure Language Display

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

Via Auto Provisioning

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

lang.gui

lang.wui

Parameter	Permitted Values	Default	Description
lang.gui	English (United States), English (United Kingdom), Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian, Netherlands, Japanese or the custom language name.	English (United States)	It configures the language to display on the device.

lan g.w ui	English (United States), English (United Kingdom), Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian, Japanese or the custom language name.	Engli sh (Unit ed State s)	It configures the language to display on the web user interface.
------------------	--	---	--

Customize Language

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

You can ask the distributor or Yealink FAE for language packs. You can also obtain the language packs online: <https://support.yealink.com/en/portal/home>.

! NOTE

1. 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.
2. This feature is currently not available on the MP5X E2 series.

Language for Device Display Customization

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

For VP59/CP965/MP52/MP54/MP56/MP58:

Customize a Language Pack for Device Display

When you add a new language pack for the phone user interface, the language pack must be formatted as “X.GUI.name.lang” (X starts from 014, “name” is replaced with the language name). If the language name is the same as the existing one, the existing language pack will be overridden by the newly uploaded one. We recommend that the filename of the new language pack should not be the same as the existing one.

! NOTE

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

1. Open the desired language template file (for example, 000.GUI.English.lang).
2. Modify the characters within the double quotation marks on the right of the equal sign. Do not modify the item on the left of the equal sign.
3. The following shows a portion of the language pack “000.GUI.English.lang” for the phone user

interface:

000.GUI.English.lang x

10203040

```
1 [[Lang]
2 Name=English
3 FONT=Tahoma
4
5 [Translated]
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"
```

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

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

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

Configuration Via Auto Provisioning

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

```
gui_lang.url
gui_lang.delete
```

Paramet er	Permitted Values	Defaul t	Description
---------------	------------------	-------------	-------------

gui_lang .url	URL within 511 characters	Blank	It configures the access URL of the custom language pack for the phone user interface. You can also download multiple language packs to the device simultaneously.
gui_lang .delete	http://localhost/all or X.GUI.name.lang X starts from 014, “name” is replaced with the language name.	Blank	It deletes the specified or all custom language packs of the phone user interface.

Configuration Via Device User Interface

Procedure

1. Select the method according to your device:

VP59/MP5X	CP965	Common Area Phones
Go to  > Settings > Device Settings > Language .	Tap the avatar in the top-right corner of the screen and go to Settings > Device Settings > Language .	Go to  > Settings > Device Settings > Language (default password: admin).

For MP52 E2/MP54 E2/MP56 E2/MP58 E2/MP55 E2:

For the MP5X E2, you need to modify five translation modules: the first four are folders, and the last is standalone.

- com.android.systemui
- com.yealink.phone
- com.yealink.settings
- com.yealink.systemui
- lang



NOTE

- You can contact your administrator or <https://ticket.yealink.com> to obtain these files.
- The serial numbers for the same language within the five modules must be consistent. If new additions are needed, please append a new language file at the end of the module.
- The .lang file should use UTF-8 encoding; otherwise, the text may appear garbled.

Procedure

1. Open these desired language template files (for example, /com.yealink.settings/000.GUI.English.lang, /com.yealink.systemui/000.GUI.English.lang, /Lang/000.GUI.English.lang).
2. Modify the characters within the double quotation marks on the right of the equal sign. Do not modify the item on the left of the equal sign.

Example:

wifi_label = "Wi-Fi" → Change "Wi-Fi" but **preserve** "wifi_label" = " "

```

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"

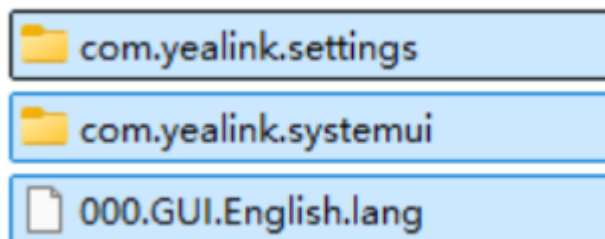
```

3. Save the file and compress it.
 - a. Save all modified files (for example, /com.yealink.settings/000.GUI.English.lang, /com.yealink.systemui/000.GUI.English.lang, /Lang/000.GUI.English.lang).

b. In each item:

- Delete ALL other language files
- Keep ONLY the modified .lang files

c. Compress the three parent folders into a ZIP file:



4. Upload the ZIP package to the provisioning server.

Configuration Via Auto Provisioning

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

```
gui_lang.url
gui.lang_custom.delete
```

Parameter	Permitted Values	Default	Description
gui_lang.url	URL within 511 characters	Blank	It configures the access URL of the custom language pack for the phone user interface.
gui.lang_custom.delete	all or X.GUI.name.language	Blank	It deletes the specified or all custom language packs of the phone user interface.

Language for Web Display Customization

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

Customize a Language Pack for Web Display

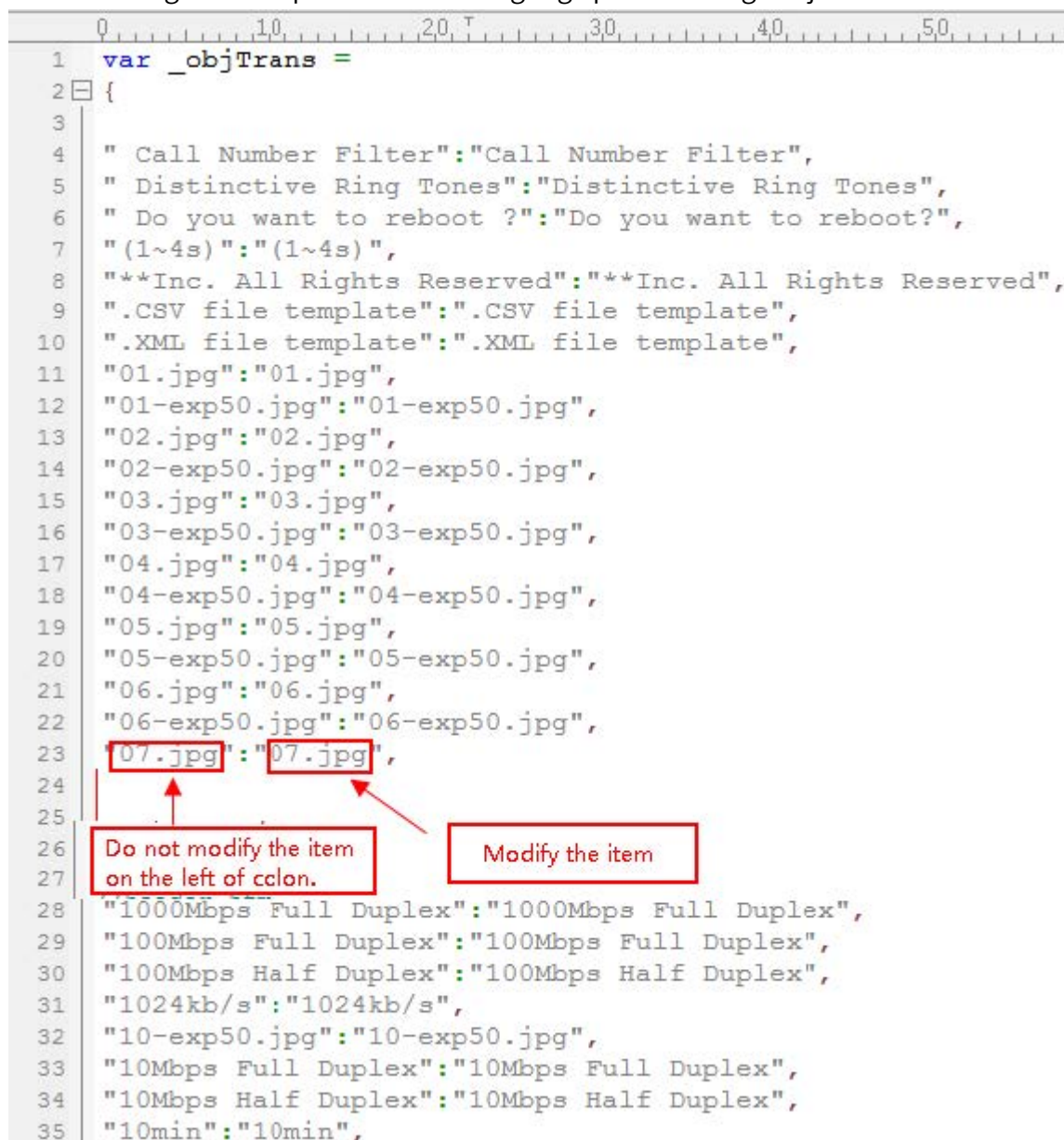
When you add a new language pack for the web user interface, the language pack must be formatted as “X.name.js” (X starts from 14, “name” is replaced with the language name). If the language name is the same as the existing one, the newly uploaded language file will override the existing one. We recommend that the filename of the new language pack should not be the same as the existing

one.

NOTE

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

1. Open the desired language template pack (for example, 1.English.js) using an ASCII editor.
2. Modify the characters within the double quotation marks on the right of the colon. Do not modify the translation item on the left of the colon.
3. The following shows a portion of the language pack “1.English.js” for the web user interface:



```

1  var _objTrans =
2  {
3
4  " Call Number Filter":"Call Number Filter",
5  " Distinctive Ring Tones":"Distinctive Ring Tones",
6  " Do you want to reboot ?":"Do you want to reboot?",
7  "(1~4s)":"(1~4s)",
8  "***Inc. All Rights Reserved":"***Inc. All Rights Reserved",
9  ".CSV file template":".CSV file template",
10 ".XML file template":".XML file template",
11 "01.jpg":"01.jpg",
12 "01-exp50.jpg":"01-exp50.jpg",
13 "02.jpg":"02.jpg",
14 "02-exp50.jpg":"02-exp50.jpg",
15 "03.jpg":"03.jpg",
16 "03-exp50.jpg":"03-exp50.jpg",
17 "04.jpg":"04.jpg",
18 "04-exp50.jpg":"04-exp50.jpg",
19 "05.jpg":"05.jpg",
20 "05-exp50.jpg":"05-exp50.jpg",
21 "06.jpg":"06.jpg",
22 "06-exp50.jpg":"06-exp50.jpg",
23 "07.jpg":"07.jpg",
24
25
26 "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

```

Do not modify the item on the left of colon.

Modify the item

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

Customize a Language Pack for Note Display

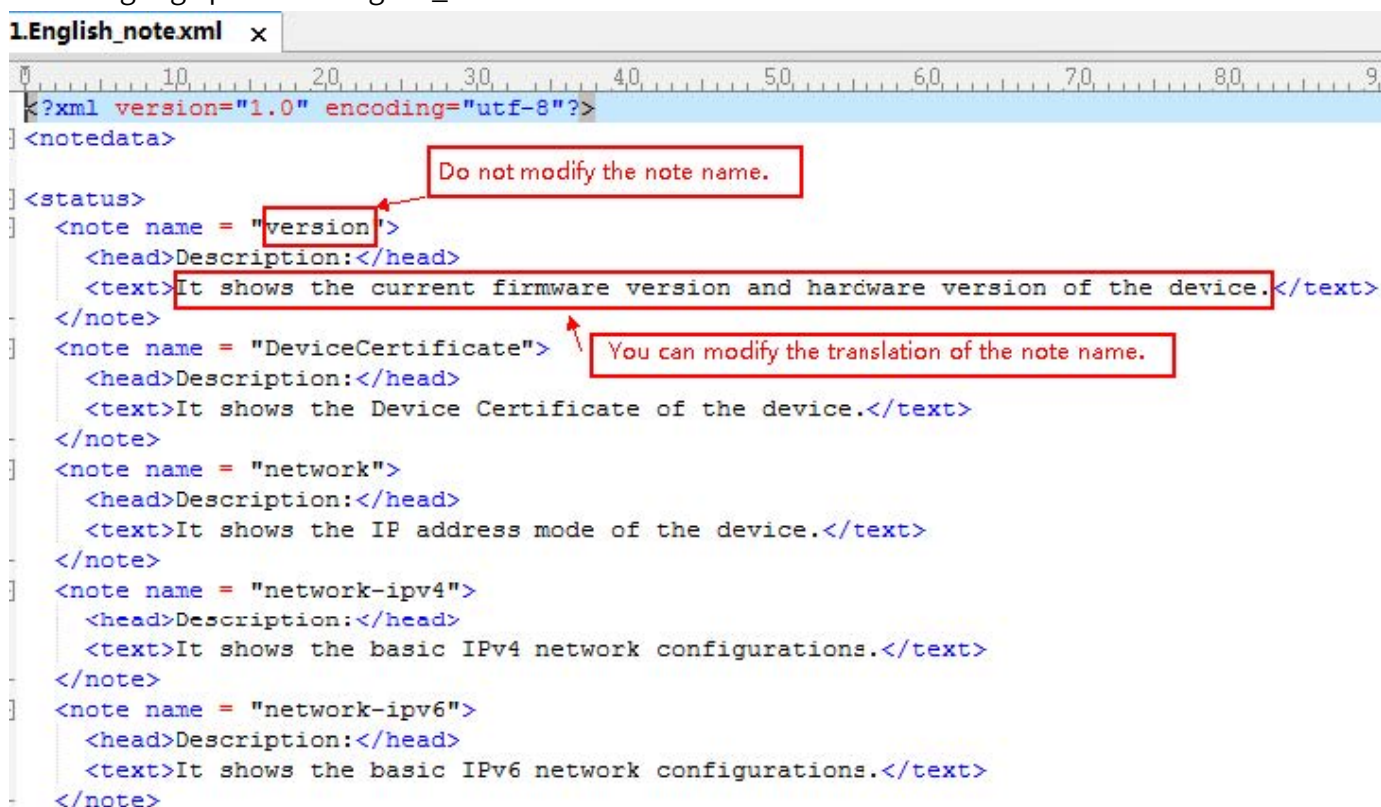
When you add a new language pack for the note, the note language pack must be formatted as

“X.name_note.xml” (X starts from 12, “name” is replaced with the language name). If the note language name is the same as the existing one, the new uploaded note language pack will override

the existing one.

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

1. Open the desired note language template pack (for example, 1.English_note.xml) using an XML editor.
2. Modify the text of the note field. Do not modify the note name. The following shows a portion of the note language pack “1.English_note.xml” for the web user interface:



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

Custom Language for Web and Note Display Configuration

If you want to add a new language (for example, Wuilan) to devices, prepare the language file named as “14.Wuilan.js” and “13.Wuilan_note.xml” for downloading. After the update, you will find a new language selection “Wuilan” at the top-right corner of the web user interface, and new note information is displayed in the icon when this new language is selected.

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

Parameter	Description	Permitted Values	Default
wui_lang.url	It configures the access URL of the custom language pack for	URL within 511 characters For example: http://localhost/	Blank

	the web user interface.	X.GUI.name.lang. X starts from 14, “name” is replaced with the language name	
wui_lang_note.url	It configures the access URL of the custom note language pack for the web user interface.	URL within 511 characters For example: http://localhost/X.name_note.xml X starts from 13, “name” is replaced with the language name	Blank
wui_lang_delete	It deletes the specified or all custom web language packs and note language packs of the web user interface.	http://localhost/all or http://localhost/Y.name.js	Blank

Example: Setting a Custom Language for Device Display

The following example shows the configuration for uploading custom language files

“015.GUI.English_15.lang” and “016.GUI.English_16.lang” , and then specify “015.GUI.English_15.lang” to display on the phone user interface. These language files are customized and placed on the provisioning server “192.168.10.25” .

```
gui_lang.url= http://192.168.10.25/015.GUI.English_15.lang
gui_lang.url= http://192.168.10.25/016.GUI.English_16.lang
lang.gui=English_15
```

After provisioning, the language on the phone user interface will change to the custom language you defined in **015.GUI.English_15.lang**. You can also find a new language selection English_15 and English_16 on the device user interface.

Set Up Voicemail

For Teams users, Cloud Voicemail is automatically set up and provisioned. *A Microsoft Teams Phone license is not required for Cloud Voicemail.*

For more information, see Microsoft docs on [Set up Cloud Voicemail](#).

Set Up Common Area Phone

A common area phone is typically placed in an area like a lobby or another area that is available to many people to make a call; for example, a reception area, lobby, or conference phone. Common area phones are signed in with accounts tied to a Common Area Phone license.

Prerequisites

Make sure you have purchased the **Common Area Phone** license [on Microsoft 365 admin center](#).

Step 1 - Create a User Account and Assign Licenses

See [Add Users and Assign Licenses Simultaneously](#) to learn how to create a user account and assign the Common Area Phone license.

Step 2 - Assign Phone Numbers

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Expand **Voice** and select **Phone numbers**.
3. Select a number and click **Edit**.
4. Assign the number to a user and click **Apply**.

Microsoft Teams admin center

Phone numbers

To set up calling features for users and services in your organization, you can get new numbers or port existing ones from a service provider. You can assign, unassign, and release phone numbers for people or for services, like audio conferencing, auto attendants, or call queues. [Learn more](#)

Get support for your phone numbers in the Phone Number Service Center

Create a new case [↗](#)
View my existing cases [↗](#)
View my existing company cases [↗](#)

Numbers Order history

+ Add ↓ Port Edit Release Change usage 63 items

Phone number	Number provider	Location	Available usages	Licensed usages	Number type
+1 213 458 8107	Microsoft	Los Angeles, United States	User, Conference, Voice app	User	Geographic
+1 213 458 8108	Microsoft	Los Angeles, United States	User, Conference, Voice app	User	Geographic
+1 408 791 0635	Microsoft	San Jose, United States	User, Conference, Voice app	Conference, Voice app	Geographic
+1 646 518 9925	Microsoft	New York City, United States	Conference, Voice app	Conference, Voice app	Geographic
+1 718 650 3667	Microsoft	New York City, United States	User, Conference, Voice app	User	Geographic
+1 912 446 5506	Microsoft	Savannah, United States	User, Conference, Voice app	User	Geographic
+1 912 446 5672	Microsoft	Savannah, United States	User, Conference, Voice app	User	Geographic

Assign/unassign

+1 213 458 8107

Number usages
User

Number type
CallingPlan

Number features

Assigned to
Select a person that you want to assign this phone number to

Yealink Amazon offic... [×](#)

Emergency location
Select a location within the country or region where emergency services must arrive when a call comes from this phone number.
If your organization has more than one physical location, it's likely that you'll need more than one emergency location. [Add a new emergency location.](#)

405 Hilgard Avenue, Los Angeles CA 90024, US. [×](#)

☐ Email user with phone number information

Apply **Cancel**

Set Up Auto Attendants

Auto attendants let people call your organization and navigate a menu system to speak to the right department, [call queue](#), person, or operator. You can create auto attendants for your organization with the Microsoft Teams admin center or [PowerShell](#).

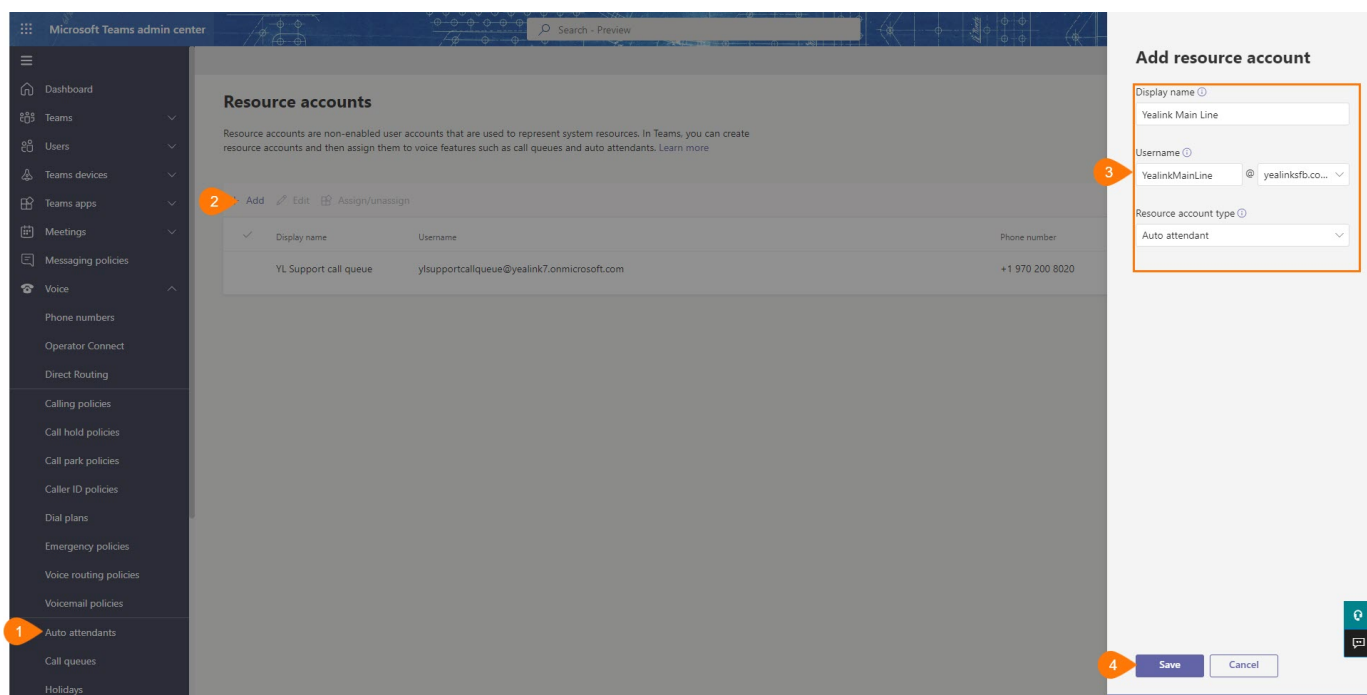
Prerequisites

- You have purchased the **Microsoft 365 Phone system** license. See [Prepare Your Teams Licenses](#).
- The person, operator, or call queue assigned in the auto attendant must be an **Enterprise Voice enabled** user.

For more detailed information, see the Microsoft docs on [prerequisites of creating auto attendants](#).

Step 1 - Create a Resource Account

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.
2. Expand **Voice** and select **Resource accounts**.
3. Select **Add**.
4. Enter the account information and select **Save**.



Step 2 - Assign a License to the Resource Account

1. Sign in to the [Microsoft 365 admin center](#) as an administrator.
2. Expand **Users** and select **Active users**.
3. Select the resource account to which you want to assign a license. The resource account's user pane

will appear.

4. Under the **Licenses and Apps** tab, select **Microsoft 365 Phone System**.

5. Select **Save changes**.

Step 3 - Enable Enterprise Voice

See [Enable Enterprise Voice for Agents](#).

Step 4 - Create an Auto Attendant

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.

2. Expand **Voice** and select **Auto attendants** > **Add**.

3. Set the general information and click **Next**.

The screenshot shows the 'Add auto attendant' page in the Microsoft Teams admin center. The left sidebar has a 'Voice' icon highlighted. The main content area is titled 'Auto attendants \ Add auto attendant' and has a 'General info' tab selected. The page is divided into sections: 'Yealink Main Line' (1), 'Operator (optional)' (2), 'Time zone' (3), 'Language' (4), and 'Voice inputs' (5). The 'Operator' section shows a dropdown for 'Person in organization' with a selection of Peter Parker. The 'Time zone' is set to '(UTC) Coordinated Universal Time'. The 'Language' is set to 'English (United States)'. The 'Voice inputs' toggle is turned 'On'. At the bottom, there is a 'Next' button (6) and a 'Cancel' button.

4. Set the call flow and click **Next**.

a. Set the greeting options. Callers can hear the greeting when they call the number. The system will read the text you set.

The screenshot shows the 'Add auto attendant' page in the Microsoft Teams admin center, with the 'Call flow' tab selected. The left sidebar shows 'General info' with a checkmark and 'Call flow' selected. The main content area is titled 'Auto attendants \ Add auto attendant' and has a 'Call flow' tab selected. The page is divided into sections: 'Call flow' and 'Greeting options'. The 'Greeting options' section has three radio buttons: 'No greeting', 'Play an audio file', and 'Add a greeting message'. The 'Add a greeting message' option is selected. Below the radio buttons is a text input field with the text 'Thanks for calling Yealink.' and a green circular icon with a 'G'.

b. Set the call routing options and click **Next**.

Auto attendants \ Add auto attendant

General info

Call flow

Advanced settings (optional)

1

Call routing options

☐ Disconnect

☐ Redirect call ⓘ

☒ Play menu options

Force Listen ☐ Off ⓘ

Set up the greeting and menu options.

☐ Play an audio file ⓘ

2

☒ Add a greeting message ⓘ

For Sales, press 1. For support, press 2. To speak to an operator, press 0. You can type or say the name of the person you are trying to reach at any time.

Set menu options ⓘ

3

+ Assign a dial key ⓘ Delete ⓘ

Dial key	Voice command	Redirect to	Destination	Transcription	Skip voicemail system message ⓘ
0	Operator	Operator	PP Peter Parker		
1		Voice app	YS Yealink Sales		
2		Voice app	Y YL Support call queue		

c. Set the directory search type.

d. If callers do not know the extension of the internal users, you can enable **Dial by name**.

Therefore, callers can say or type the name on the phone keypad.

Directory search

☐ None

☒ Dial by name

☐ Dial by extension

5. Set your company business hours.

- General info
- Call flow
- Advanced settings (optional)
 - Call flow for after hours**
 - Call flows during holidays
 - Dial scope
 - Resource accounts

Set business hours

By default, business hours are set to 24/7, Monday through Sunday. If you set custom business hours, all hours that aren't included in business hours are considered after business hours. [Learn more](#)

[Reset to default](#)
[Clear all hours](#)

Day	Start at	End at	
Sunday	Select start time	Select end time	+ Add new time
Monday	9:00 AM	5:30 PM	+ Add new time
Tuesday	9:00 AM	5:30 PM	+ Add new time
Wednesday	9:00 AM	5:30 PM	+ Add new time
Thursday	9:00 AM	5:30 PM	+ Add new time
Friday	9:00 AM	5:30 PM	+ Add new time
Saturday	Select start time	Select end time	+ Add new time

6. Set up after-hours call flow.

- General info
- Call flow
- Advanced settings (optional)
 - Call flow for after hours**
 - Call flows during holidays
 - Dial scope
 - Resource accounts

Set up after hours call flow

If you have business hours set up, you also need to set up a call flow for after business hours.

Greeting options

☐ No greeting
☐ Play an audio file [?](#)
☒ Add a greeting message [?](#)

Thank you for calling Yealink. Your call is important to us. Please leave your name and number, and we will call you back.

Call routing options

☐ Disconnect
☒ Redirect call [?](#)

Redirect to [?](#)

Voicemail

=

Y Yealink

Transcription

On

Skip voicemail system message [?](#)

Off

☐ Play menu options

3

Next

Submit

7. Click **Add** to add call flows during holidays. If you have not set a holiday, add one first.

1 **Christmas**

2 Holiday
Christmas

Greeting

☐ No greeting

☐ Play an audio file ⓘ

☒ Add a greeting message ⓘ

Thank you for calling Yealink. Our office is closed for the Christmas holiday. Please leave your name and number, and we will call you back.

Call routing options

☐ Disconnect

☒ Redirect call ⓘ

Redirect to ⓘ

Voicemail = Y Yealink X

Transcription Skip voicemail system message ⓘ

☐ Off ☐ Off

☐ Play menu options

5 **Save** **Cancel**

8. Set up a dial scope to include or exclude users or groups.

Auto attendants \ Add auto attendant

✓ General info

✓ Call flow

✓ Advanced settings (optional)

✓ Call flow for after hours

✓ Call flows during holidays

Dial scope

Resource accounts

Dial scope

Set up the users or groups that will be listed and available in your organization's directory when a caller dials in to this auto attendant. When callers use Dial by name and search for a person, they'll be transferred to a user who has the Teams app installed. [Learn more](#)

Include

Select which users will be included and available in your organization's directory. ⓘ

☒ All online users

☐ Custom user group

Exclude

Select which users or groups will be excluded from the organization's directory. ⓘ

☒ No one

☐ Custom user group

2 Next Submit

9. Add a resource account and click **Submit**.

Microsoft Teams admin center

Auto attendants \ Add auto attendant

✓ General info

✓ Call flow

✓ Advanced settings (optional)

✓ Call flow for after hours

✓ Call flows during holidays

✓ Dial scope

Resource accounts

When you create an auto attendant, you can add a new resource account and assign a phone number to that resource account. [Learn more](#)

You haven't added any resource accounts yet.

1 Add

2 Add accounts

Search for resource accounts you want to add.

Search by display or username

Accounts to add (1)

YL Yealink Main Line

3 Add Cancel

4 Submit

Step 5 - Assign a Call Number to the Resource Account

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.
2. Expand **Voice** and select **Resource accounts**.
3. Select the resource account to which you want to assign a number and click **Assign/unassign**.
4. Select the phone number type, a phone number and the auto attendant you created.
5. Click **Save**.

Assign/unassign

Yealink Main Line

To see a service number listed here, buy a Phone System or get a Teams Phone Resource Account license and make sure it's not assigned to any other voice services. [Learn more](#)

Phone number type

1

Assigned phone number

2

Assigned to

Your changes must be saved before making more changes.

Select an auto attendant

3

4

6.

Assign/unassign

Yealink Main Line

 To see a service number listed here, buy a Phone System or get a Teams Phone Resource Account license and make sure it's not assigned to any other voice services. [Learn more](#)

Phone number type

1

Calling Plan



Assigned phone number

2

+1 970 200 8021



Assigned to

 Your changes must be saved before making more changes.

Select an auto attendant

3

Yealink Main Line



4

Save

Cancel

Call Park and Retrieve

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

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

For more information on how to configure the call park and retrieve, refer to [Call park and retrieve in Microsoft Teams](#).

Supported Devices

This feature is available VP59/MP58/MP56/MP54/CP965/MP52 (E2)/MP55 E2.

Set Up Call Queue

Introduction

Call queues route callers to people in your organization who can help with a particular issue or question. Calls are distributed one at a time to the people (known as agents) in the queue.

For information on how to create a call queue, see Microsoft docs on [creating a call queue](#).

Supported Devices

This feature is only available to MP58/MP58-WH/MP56/MP54/T58A/T56A/T55A Teams phones.

Prerequisites

You need the following resources before creating call queues:

- The members in a call queue must be **Enterprise Voice enabled** users.
- If the members use the Microsoft Teams app for call queue calls, they need to be in **TeamsOnly** mode.
- You have purchased the **Microsoft 365 Phone system** license. See [Prepare Your Teams Licenses](#).

For more detailed information, see the Microsoft doc on [prerequisites of creating call queues](#).

Step 1 - Enable Enterprise Voice for Agents

Before you create a team for the call queue agents, you need to enable Enterprise Voice for each agent.

Prerequisite:

You have [downloaded and installed](#) the Teams PowerShell module.

Procedure

1. Start Windows PowerShell as an administrator.
2. Type the following and press Enter to connect to the Microsoft Teams PowerShell session:
3. `powershell`
4. `Import-Module MicrosoftTeams $credential = Get-Credential Connect-MicrosoftTeams -Credential $credential`
3. Run the command below to assign the `$EnterpriseVoiceEnabled` and `$HostedVoiceMail` properties to the account:
4. `powershell`
5. `Set-CsUser -Identity "<User name>" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true //`
change <user name> to the actual user name

6. Example:

7. `powershell`

8. `Set-CsUser -Identity "Peter Parker" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true`

4. Run the command below to see the status:

5. If it is true, the Enterprise Voice feature is enabled.

6. `powershell`

7. `Get-CsOnlineUser -Identity "<user name>" | fl EnterpriseVoiceEnabled`

```
PS D:\Users\yl2886\Desktop\direct routing tool> Set-CsUser -Identity test06@yealink7.onmicrosoft.com -EnterpriseVoiceEnabled $true

PS D:\Users\yl2886\Desktop\direct routing tool> Get-CsOnlineUser -Identity test06 | fl EnterpriseVoiceEnabled

EnterpriseVoiceEnabled : True

PS D:\Users\yl2886\Desktop\direct routing tool>
```

Step 2 - Create a Team for the Call Queue Agents

Procedure

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.
2. Expand **Teams** and select **Manage teams** > **Add**.
3. Enter the team information and click **Apply**.

The screenshot shows the Microsoft Teams admin center interface. On the left is a navigation pane with options like Dashboard, Teams, Teams settings, Teams policies, Team templates, Templates policies, Teams update policies, Teams upgrade settings, Users, Teams devices, Teams apps, Meetings, Messaging policies, Voice, Locations, Enhanced encryption p..., Policy packages, Planning, Analytics & reports, Notifications & alerts, and Other settings. The main area is titled 'Manage teams' and includes a 'Users summary' card showing 3,334 Total users, 2,291 Internal users, and 1,043 Guests. Below this is a table of existing teams. On the right, the 'Add a new team' dialog box is open, with an orange border around its input fields. The 'Name' field contains 'YL technical support', the 'Description' field contains 'YL technical support', and the 'Team owners' field lists 'Peter Parker (TEST06)'. The 'Privacy' dropdown is set to 'Private'. At the bottom of the dialog are 'Apply' and 'Cancel' buttons.

4. Click the name of the created team to view the team's members, channels, and settings.

Manage teams

Teams and channels are collections of people, content, and tools used for projects or outcomes within your organization. You can manage all teams and channels, and create new ones. Go to the [Admin center > Groups](#) to manage Microsoft 365 groups. Learn more

Users summary

3,334 Total users 2,291 Internal users 1,043 Guests

Name	Standard channels	Private channels	Shared channels	Team members	Owners	Guests
YL technical support	1	0	0	1	1	0
Yealink Technical Support - TD Synnex	1	0	0	8	1	2
Comtel & Yealink Technical Support	1	0	0	1	1	0
Asit&Yealink Technical support Team	1	0	0	7	1	1

5. Under the **Members** tab, click **Add**, add members, and click **Apply**.

YL technical support

YL technical support

Team members

Privacy: Private

Email: YLtechnicalsupport@yealink...

Members Channels Settings

+ Add × Remove | 2 items

Display name	Username	Title	Location	Role
Peter Parker	test06@yealink7.onmicros...	-	-	Owner

Add members

Search members: test07

Team members to add 3

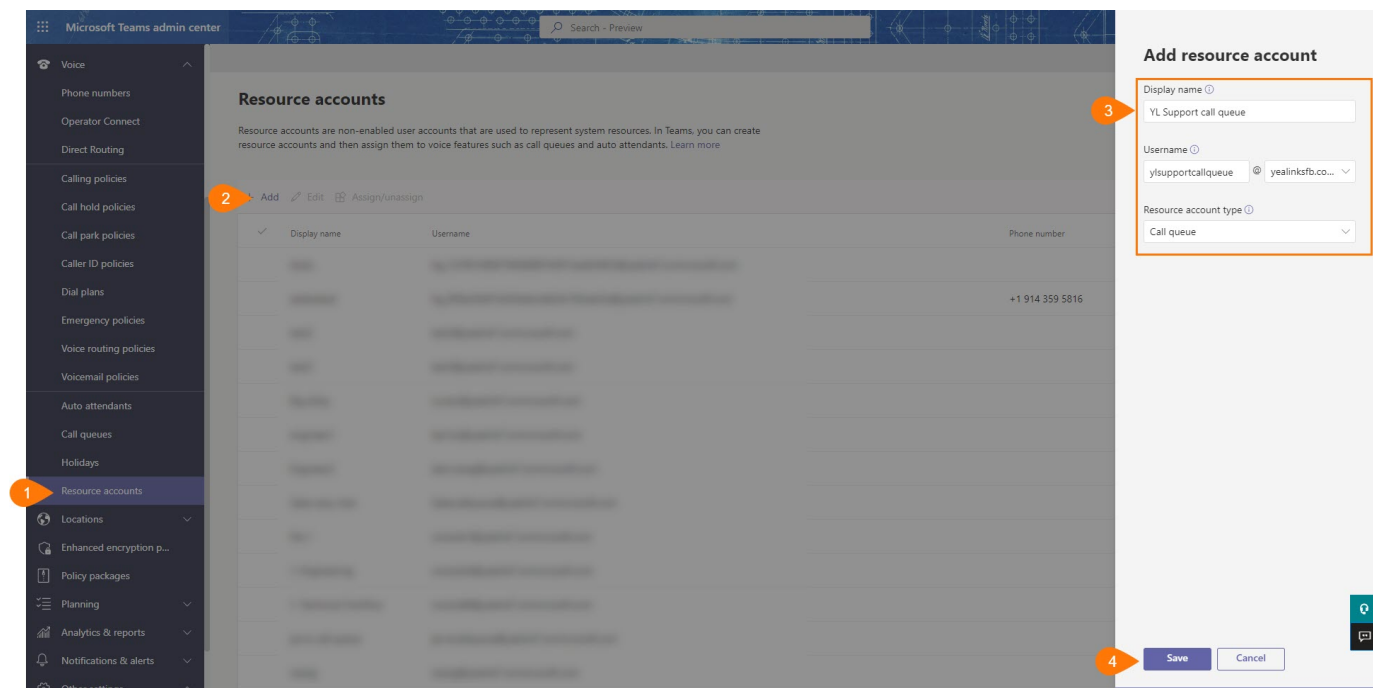
- Wang Siri (TEST01)
- Xiao nana (TEST03)
- ParkHae Jin (TEST07) SALES ENGINEER

Apply Cancel

Step 3 - Create a Resource Account

Procedure

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.
2. Expand **Voice** and select **Resource accounts**.
3. Select **Add**.
4. Enter the account information and select **Save**.



Step 4 - Assign a License to the Resource Account

Procedure

1. Sign in to the [Microsoft 365 admin center](#) as an administrator.
2. Expand **Users** and select **Active users**.
3. Select the resource account to which you want to assign a license. The resource account's user pane will appear.
4. Under the **Licenses and Apps** tab, select **Microsoft 365 Phone System**.
5. Select **Save changes**.

Step 5 - Create a Call Queue

Procedure

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.
2. Expand **Voice** and select **Call queues** > **Add**.
3. Set the general information and click **Next**.

Microsoft Teams admin center

Call queues \ Add a call queue

YL Support call queue

General info

Greeting and music
Call answering
Agent selection
Call overflow handling
Call timeout handling

Resource accounts

Add or remove resource accounts. You can assign a phone number to a resource account you're adding.

+ Add X Remove 1 item

✓	Resource account	Phone number
	YL Support call queue	

Assign calling ID

Agents can make outbound calls using the phone numbers on the following resource accounts.

You haven't added any resource accounts yet.

Add

Language

This lets you set the language used to transcribe voicemail messages and play system prompts to the caller.

English (United States)

Next

Cancel

4. Set the greeting and music and click **Next**.

Microsoft Teams admin center

Call queues \ Add a call queue

Greeting and music

Greetings and music keep your caller informed about their call while waiting to be answered by an agent. Learn more

Greeting

☐ No greeting

☒ Play an audio file

hello.wav

Accepted file formats are MP3, WAV, and WMA. Files must be less than 5 MB.

☐ Add a greeting message

Music on hold

☒ Play default music

☐ Play an audio file

Next

Submit

Cancel

5. Set up call answering and click **Next**.

Microsoft Teams admin center Search - Preview

Call queues \ Add a call queue

Call answering

You can choose either a channel, or groups and individual users to answer incoming calls for this call queue.

Call answering

Agent selection

Call overflow handling

Call timeout handling

Conference mode

On

Call agents who use the Skype for Business client won't receive calls when conference mode is enabled.

Add a channel

To select a channel for call agents, first select the team, then select the channel.

Selected team

YL technical support 4 members

Select the channel

General

Next **Submit** **Apply** **Cancel**

- [Conference mode](#): it reduces the time it takes for a caller to be connected to an agent after the agent accepts the call. For conference mode to work, agents in the call queue must use one of the following clients:
 - The latest version of the Microsoft Teams desktop client, Android app, or iOS app
 - Microsoft Teams Phone version 1449/1.0.94.2020051601 or later

6. Choose and assign agents and click **Next**.

Microsoft Teams admin center

Search - Preview

Call queues \ Add a call queue

- General info
- Greeting and music
- Call answering
- Agent selection**
- Call overflow handling
- Call timeout handling

Agent selection

Routing method

- ☐ Attendant routing
- ☒ Serial routing
- ☐ Round robin
- ☐ Longest idle

Presence-based routing

☒ On

Agents who use the Skype for Business client will not receive calls when longest idle or presence-based routing is enabled.

Call agents can opt out of taking calls

☒ On

Call agent alert time (seconds)

Next Submit Cancel

- [Serial routing](#): it brings each agent one by one in the order specified in the **Call agents** list. If an agent dismisses or doesn't pick up a call, the call will ring to the next agent. This will repeat until the call is picked up or times out.
- [Presence-based routing](#): call agents whose availability status is set to **Available** can receive the

call.

- [Call agents can opt out of taking calls](#): call agents can opt out of taking calls or not.
- [Agent alert time](#): it specifies how long an agent's phone will ring before the queue redirects the call to the next agent. The recommended alert time is 20 seconds.

7. Set call overflow handling and click **Next**.

8. Set call timeout handling and click **Submit**.

- [Maximum wait time](#): it specifies the maximum time a call can be on hold in the queue before it is redirected or disconnected.

Step 6 - Assign a Call Number to the Resource

Account

Procedure

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.
2. Expand **Voice** and select **Resource accounts**.
3. Select the resource account to which you want to assign a number and click **Assign/unassign**.
4. Select the phone number type, a phone number and the call queue you created.
5. Click **Save**.

Assign/unassign

YL Support call queue

To see a service number listed here, buy a Phone System or get a Teams Phone Resource Account license and make sure it's not assigned to any other voice services. [Learn more](#)

Phone number type

1 Calling Plan

Assigned phone number

2 +1 970 200 8021

Assigned to

Your changes must be saved before making more changes.

Select a call queue

3 YL support call queue

4 **Save** Cancel

6.

Assign/unassign

YL Support call queue

 To see a service number listed here, buy a Phone System or get a Teams Phone Resource Account license and make sure it's not assigned to any other voice services. [Learn more](#)

Phone number type

1

Calling Plan

Assigned phone number

2

+1 970 200 8021

Assigned to

 Your changes must be saved before making more changes.

Select a call queue

3

YL support call queue

4

Save

Cancel

Auto Answer

Teams phone supports automatically answer the incoming call. If you use the ringer device, the phone will automatically answer the incoming call and connect to the ringer device.

Via Auto Provisioning

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

features.auto_answer.enable

Parameter	Description	Permitted Values	Default
features.auto_answer.enable	It enables or disables auto answer a call.	0 -Disabled 1 -Enabled, the phone can automatically answer an incoming call.	0

Prepare Your Teams Licenses

Prepare the Apps or Services for Teams Users

! TIP

- The apps or services will be included in the [Microsoft cloud-based suite for Office 365 and Microsoft 365](#). You can go to **Billing > Purchase services** on the [Microsoft 365 admin center](#) to buy the license suite.
- The license takes effect **10** minutes after your assignment or modification.
- If you need other license types, please see the [Microsoft Teams add-on licenses](#) or contact Microsoft.

Features you need	Services or apps you need
Sign in to Teams	Ensure that the selected license (e.g., the Common Area Phone) includes the Microsoft Teams app. Apps (6)  Show apps for: All licenses  ☒ Select all ☒ Azure Active Directory Premium P1 Common Area Phone ☒ Exchange Online (Plan 2) Common Area Phone ☒ Microsoft 365 Phone System Common Area Phone ☒ Microsoft Intune Common Area Phone ☒ Microsoft Teams Common Area Phone ☒ Skype for Business Online (Plan 2) Common Area Phone
Common Area Phone	Common Area Phone license

	Licenses (1)*  ☒ Assign user a product license ☐ Audio Conferencing for non-China users 35 of 35 licenses available ☐ Azure Active Directory Basic The prepaid subscription for this product is no longer active. You need to buy a subscription before you can assign a license. ☐ Business Apps (free) 1 of 6 licenses available ☒ Common Area Phone You're out of licenses. If you turn this on, we'll try to buy an additional license for you.
Calendar feature	Ensure that the selected license (e.g., the Common Area Phone) includes the Exchange Online app. Apps (6)  Show apps for: All licenses  ☒ Select all ☒ Azure Active Directory Premium P1 Common Area Phone ☒ Exchange Online (Plan 2) Common Area Phone ☒ Microsoft 365 Phone System Common Area Phone ☒ Microsoft Intune Common Area Phone ☒ Microsoft Teams Common Area Phone ☒ Skype for Business Online (Plan 2) Common Area Phone
Intune (manage device and apply policies on Intune)	Ensure that the selected license (e.g., Microsoft 365 E3) includes the Microsoft Intune app.

	☒ Microsoft Defender for Endpoint Plan 1 Microsoft 365 E3 ☒ Microsoft Forms (Plan E3) Microsoft 365 E3 ☒ Microsoft Intune Microsoft 365 E3 ☒ Microsoft Kaizala Pro Microsoft 365 E3
Call queue	Ensure that the selected license (e.g., the Office 365 E5 without Audio Conferencing) includes the Microsoft 365 Phone System app. ☒ Microsoft 365 Apps for Enterprise Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Communication Compliance Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Defender Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Phone System Office 365 E5 without Audio Conferencing ☒ Microsoft Bookings Office 365 E5 without Audio Conferencing ☒ Microsoft Communications DLP Office 365 E5 without Audio Conferencing ! NOTE You need a follow-up configuration to enable the call queue feature.
Auto Attendant	Ensure that the selected license (e.g., the Office 365 E5 without Audio Conferencing) includes the Microsoft 365 Phone System app.

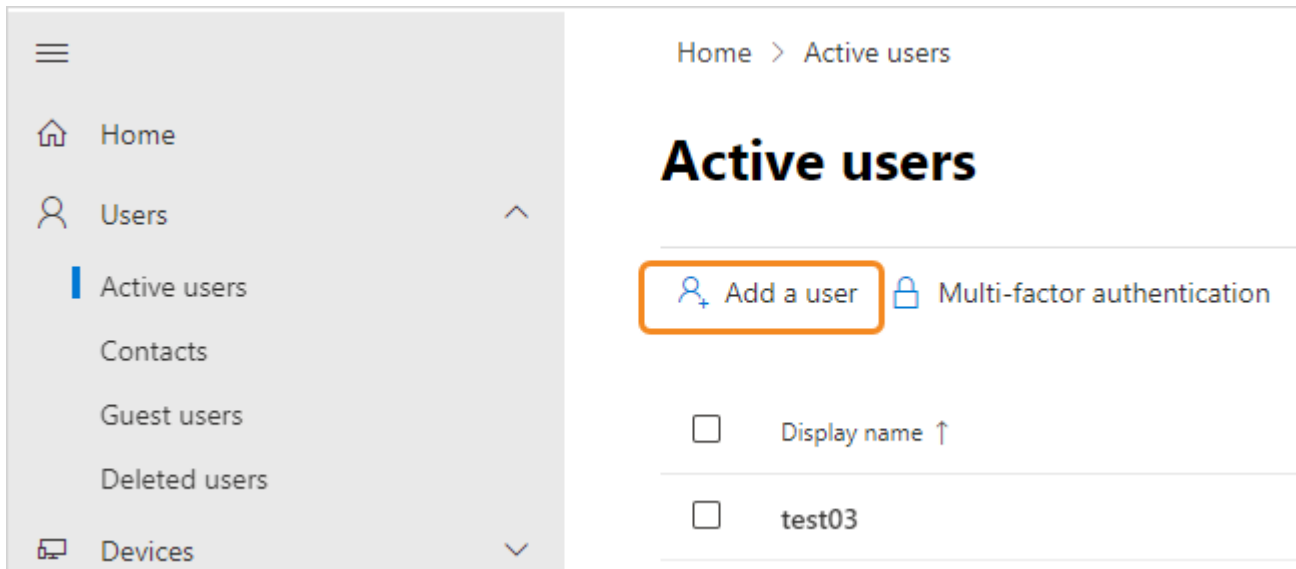
	☒ Microsoft 365 Apps for Enterprise Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Communication Compliance Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Defender Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Phone System Office 365 E5 without Audio Conferencing ☒ Microsoft Bookings Office 365 E5 without Audio Conferencing ☒ Microsoft Communications DLP Office 365 E5 without Audio Conferencing NOTE You need a follow-up configuration to enable the call queue feature.
PSTN	1. Microsoft Teams Domestic or Domestic and International Calling Plan. ☐ Microsoft Stream Trial Unlimited licenses available ☒ Microsoft Teams Domestic Calling Plan 0 of 42 licenses available ☐ Microsoft Teams Domestic and International Calling Plan You're out of licenses. If you turn this on, we'll try to buy an additional license for you. ☐ Microsoft Teams Exploratory 3 of 500 licenses available 2. Ensure that the selected license (e.g., the Office 365 E5 without Audio Conferencing) includes the Microsoft 365 Phone System app.

	☒ Microsoft 365 Apps for Enterprise Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Communication Compliance Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Defender Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Phone System Office 365 E5 without Audio Conferencing ☒ Microsoft Bookings Office 365 E5 without Audio Conferencing ☒ Microsoft Communications DLP Office 365 E5 without Audio Conferencing NOTE You need a follow-up configuration to set up the PSNT feature.
Voice Mail	Not require any service or apps.
Skype for Business	Ensure that the selected license (e.g., the Office 365 E3) includes the Skype for Business Online (Plan 2) app. ☒ SharePoint (Plan 2) Microsoft 365 E3 ☒ Skype for Business Online (Plan 2) Microsoft 365 E3 ☒ Sway Microsoft 365 E3

Add Users and Assign Licenses Simultaneously

People on your team need a user account before signing in to Teams phone and using the supported features. After this step, your users have Microsoft 365 licenses, sign-in credentials, and Microsoft 365 mailboxes. You can also assign the corresponding licenses to users.

1. Sign in to the [Microsoft 365 admin center](#) as an administrator.
2. Go to **Users > Active users > Add a user**.



3. Set the basic information and click **Next**.

Add a user

- Basics
- Product licenses
- Optional settings
- Finish

Set up the basics

To get started, fill out some basic information about who you're adding as a user.

First name

Last name

Display name *

Username *

Domains

Automatically create a password

Password *

Require this user to change their password when they first sign in

Send password in email upon completion

Monica

Zhang

Monica Zhang

test01_

@ yealink7.onmicrosoft.com

☐

..... Strong

☐

☐

Next

4. Assign product licenses and apps for the user and click **Next**.

Add a user

Licenses

- ☐ **Dynamics 365 Marketing Business Edition**
9999 of 10000 licenses available
- ☐ **Enterprise Mobility + Security E3**
The prepaid subscription for this product is no longer active. You need to [buy a subscription](#) before you can assign a license.
- ☒ **Microsoft 365 Audio Conferencing**
4 of 100 licenses available
- ☐ **Microsoft 365 E3**
86 of 300 licenses available
- ☐ **Microsoft Power Apps Plan 2 Trial**
9990 of 10000 licenses available
- ☐ **Microsoft Power Automate Free**
9557 of 10000 licenses available
- ☐ **Microsoft Stream Trial**
Unlimited licenses available
- ☒ **Microsoft Teams Domestic Calling Plan**
0 of 42 licenses available
- ☐ **Microsoft Teams Domestic and International Calling Plan**
You're out of licenses. If you turn this on, we'll try to buy an additional license for you.
- ☐ **Microsoft Teams Exploratory**
3 of 500 licenses available
- ☐ **Microsoft Teams Rooms Standard**
You're out of licenses. If you turn this on, we'll try to buy an additional license for you.
- ☐ **Office 365 E1**
59 of 215 licenses available
- ☒ **Office 365 E5 without Audio Conferencing**
11 of 135 licenses available
- ☐ **Power BI (free)**
Unlimited licenses available

Back
Next

Apps

Licenses (3)*

Apps (55)

Show apps for:
All licenses

- ☒ Select all
- ☒ **Azure Rights Management**
Office 365 E5 without Audio Conferencing
- ☒ **Common Data Service**
Office 365 E5 without Audio Conferencing
- ☒ **Common Data Service for Teams**
Office 365 E5 without Audio Conferencing
- ☒ **Customer Lockbox**
Office 365 E5 without Audio Conferencing
- ☒ **Data Classification in Microsoft 365**
Office 365 E5 without Audio Conferencing
- ☒ **Exchange Online (Plan 2)**
Office 365 E5 without Audio Conferencing
- ☒ **Graph Connectors Search with Index**
Office 365 E5 without Audio Conferencing
- ☒ **Information Barriers**
Office 365 E5 without Audio Conferencing
- ☒ **Information Protection and Governance Analytics - Premium**
Office 365 E5 without Audio Conferencing
This app is assigned at the organization level. It can't be assigned per user.
- ☒ **Information Protection and Governance Analytics - Standard**
Office 365 E5 without Audio Conferencing

Back
Next

5. Check the information and click **Finish adding**.

Add a user

Review and finish

Assigned Settings

Review all the info and settings for this user before you finish adding them.

Display and username

Monica Zhang
test01_@yealink7.onmicrosoft.com
[Edit](#)

Password

Type: Auto-generated
[Edit](#)

Product licenses

Location: United States
Licenses: Microsoft Teams Domestic Calling Plan, Office 365 E5 without Audio Conferencing, Microsoft 365 Audio Conferencing
Apps: Viva Learning Seeded, Nucleus, Information Protection and Governance Analytics – Standard, 52 more
[Edit](#)

Roles (default)

User (no admin center access)
[Edit](#)

Profile info

[Edit](#)

Back
Finish adding

Simple Certificate Enrollment Protocol

SCEP is an industry-standard protocol and technology. It mainly issues certificates for device through the internal CA of the enterprise, which can provide digital certificates for device online safely and reliably.

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

static.scep.enable
static.scep.url
static.scep.user
static.scep.password
static.scep.enroll.retry_count
static.scep.enroll.retry_interval
static.scep.renewal.threshold
static.scep.renewal.time
static.scep.challenge_password
static.scep.csr.common_name
static.scep.csr.organization
static.scep.csr.email
static.scep.csr.state
static.scep.csr.country

Parameter	Permitted Values	Default	Description
static.scep.enable	0-Disabled 1-Enabled	0	It enables or disables using SCEP to obtain or update certificate.
static.scep.url	String within 256 characters	Blank	It configures the SCEP server address. The process of obtaining the certificate will be triggered when the certificate is updated.
static.scep.user	String within 256 characters	Blank	It configures the user name of SCEP server.

static.scep.password	String within 256 characters	Blank	It configures the password of SCEP server.
static.scep.enroll.retry_count	Integer from 1 to 12	3	It configures the retries count of the phone registration to the SCEP server error/waiting and certificate acquisition failure.
static.scep.enroll.retry_interval	Integer from 300 to 3600	300	It configures the seconds between retry attempts for phone registration to the SCEP server error/wait and certificate acquisition failure.
static.scep.renewal.threshold	Integer from 50 to 100	80	It configures the percentage of the certificate validity period when the phone initiates an update from the SCEP server.
static.scep.renewal.time	The first two digits represent the clock: 00-23; The last two digits represent the minute: 00-59;	100	It configures starts time when the phone initiates the certificate update to the SCEP server.
static.scep.challenge_password	String within 256 characters	Blank	It configures the verification password when the phone requests a certificate from the SCEP server.
static.scep.csr.common_name	String within 64 characters	Blank	It configures the common name used to generate the CSR (Certificate Signing Request).
static.scep.csr.organization	String within 64 characters	Blank	It configures the legal name used to generate the CSR organization.
static.scep.csr.email	String within 64 characters	Blank	It configures the email address used to generate the CSR.
static.scep.csr.state	String within 64 characters	Blank	It configures the state/province name used to generate the CSR.  NOTE It can not be abbreviated and

			should included suffixes such as Inc, Corp or LLC.
static.scep.csr.country	String within 2 characters	Blank	It configures the country name used to generate the CSR. ! NOTE The ISO code of the country/region where the organization is located.

Encrypt Configuration Files

Introduction

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

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

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

! TIP

AES keys must be 16 characters. The supported characters contain: digits, upper-case letters, lower-case letters, and special characters: `# $ % * + , - . : = ? @ [ ] ^ _ { } ~ .`

Configuration Files Encryption Tools

Yealink provides three encryption tools for configuration files:

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

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

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

Configuration Files Encryption and Decryption

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

For security reasons, you should upload encrypted configuration files, `<xx>_Security.enc` files to the root directory of the provisioning server. During auto provisioning, the device requests to download

the boot file first and then download the referenced configuration files. For example, the device downloads an encrypted account.cfg file. The device will request to download `<account_Security>.enc` file (if enabled) and decrypt it into the plaintext key (for example, key2) using the built-in key (for example, key1). Then the device decrypts account.cfg file using key2. After decryption, the device resolves configuration files and updates configuration settings onto the device system.

Encryption and Decryption Configuration

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

static.auto_provision.update_file_mode

static.auto_provision.aes_key_in_file

static.auto_provision.aes_key_16.com

static.auto_provision.aes_key_16.mac

Parameter	Permitted Values	Default	Description
static.auto_provision.update_file_mode	0- Disabled, the device will download the configuration files (for example, sip.cfg, account.cfg, <MAC>-local.cfg) and <MAC>-contact.xml file from the server during auto provisioning no matter whether the files are encrypted or not. And then the device resolves these files and updates the settings onto the device system. 1-Enabled, the device will only download the encrypted configuration files (for example, sip.cfg, account.cfg, <MAC>-local.cfg) or <MAC>-	0	It enables or disables the device only to download the encrypted files.

	contact.xml file from the server during auto provisioning, and then resolve these files and update settings onto the device system.		
static.auto_provision.aes_key_in_file	0- Disabled, the device will decrypt the encrypted configuration files using plaintext AES keys configured on the device. 1-Enabled, the device will download <code><xx_Security>.enc</code> files (for example, <code><sip_Security>.enc</code>, <code><account_Security>.enc</code>) during auto provisioning, and then decrypts these files into the plaintext keys (for example, key2, key3) respectively using the device built-in key (for example, key1). The device then decrypts the encrypted configuration files using corresponding key (for example, key2, key3).	0	It enables or disables the device to decrypt configuration files using the encrypted AES keys.
static.auto_provision.aes_key_16.com	16 characters	Blank	It configures the plaintext AES key for encrypting/decrypting the Common CFG/ Custom CFG file. The valid characters contain: digits, upper-case letters, lower-case letters and the following special characters are also supported: <code># \$ % * + , - . : = ? @ [] ^ _ { } ~ .</code>

			Example: <pre>static.auto_provision.aes_key_16.com = 0123456789abcdef</pre> NOTE For decrypting, it works only if "static.auto_provision.aes_key_in_file" is set to 0 (Disabled). If the downloaded MAC-Oriented file is encrypted and the parameter "static.auto_provision.aes_key_16.mac" is left blank, the device will try to encrypt/decrypt the MAC-Oriented file using the AES key configured by the parameter "static.auto_provision.aes_key_16.com".
static.auto_provision.aes_key_16.mac	16 characters	Blank	It configures the plaintext AES key for encrypting/decrypting the MAC-Oriented files (<MAC>.cfg, <MAC>-local.cfg and <MAC>-contact.xml). The valid characters contain: digits, upper-case letters, lower-case letters and the following special characters are also supported: # \$ % ^ + , - . : = ? @ [] ^ _ { } ~. Example: <pre>static.auto_provision.aes_key_16.mac = 0123456789abmins</pre> NOTE For decrypting, it works only if "static.auto_provision.aes_key_in_file" is set to 0 (Disabled). If the downloaded MAC-Oriented file is encrypted and the parameter

"static.auto_provision.aes_key_16.mac" is left blank, the device will try to encrypt/decrypt the MAC-Oriented file using the AES key configured by the parameter "static.auto_provision.aes_key_16.com".

Example: Encrypting Configuration Files

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

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

Procedure

1. Double click "Config_Encrypt_Tool.exe" to start the application tool.
2. The screenshot of the main page is shown below:



2. When you start the application tool, a file folder named "Encrypted" is created automatically in the directory where the application tool is located.
3. Click **Browse** to locate configuration file(s) (for example, account.cfg) from your local system in the **Select File(s)** field.
4. To select multiple configuration files, you can select the first file and then press and hold the **Ctrl** key and select other files.
4. (Optional.) Click **Browse** to locate the target directory from your local system in the **Target Directory** field.
5. The tool uses the file folder "Encrypted" as the target directory by default.
5. (Optional.) Mark the desired radio box in the **AES Model** field.
6. If you mark the **Manual** radio box, you can enter an AES KEY in the **AES KEY** field or click **Re-**

Generate to generate an AES KEY in the **AES KEY** field. The configuration file(s) will be encrypted using the AES KEY in the **AES KEY** field.

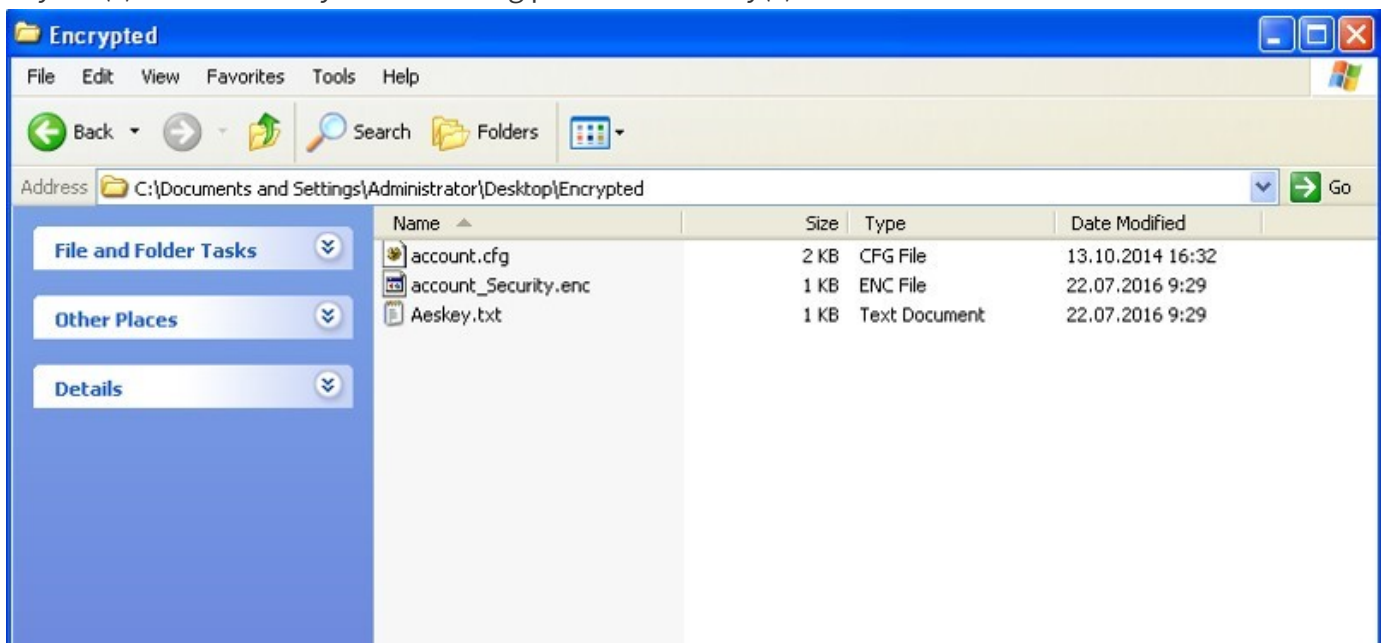
7. If you mark the **Auto Generate** radio box, the configuration file(s) will be encrypted using a random **AES KEY**. The AES keys of configuration files are different.

6. Click **Encrypt** to encrypt the configuration file(s).



7. Click **OK**.

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



Transport Layer Security (TLS)

Introduction

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

Yealink devices support TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.

Supported Cipher Suites

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

Yealink devices support the following cipher suites:

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

Supported Trusted and Server Certificates

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

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

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

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

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

Supported Trusted Certificates

Yealink Teams devices trust the following CAs by default.

! IMPORTANT

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

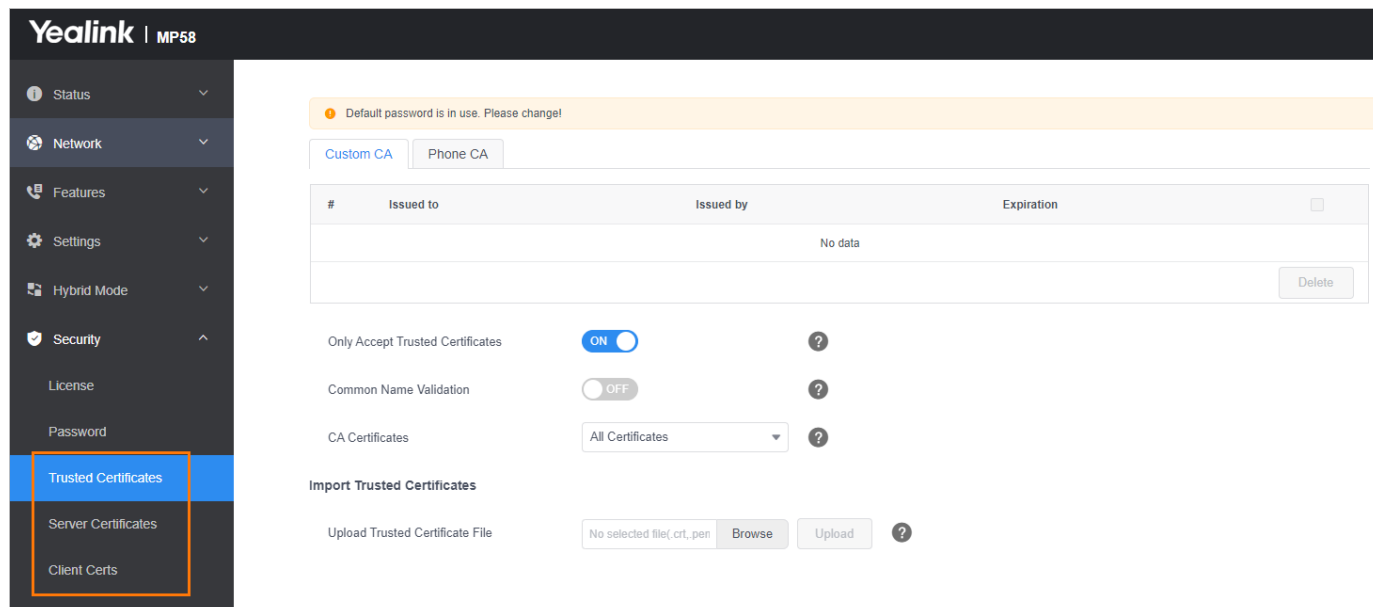
Supported CAs	Supported CAs
DigiCert High Assurance EV Root CA	DigiCert Assured ID Root G2

Deutsche Telekom Root CA-2	DigiCert Assured ID Root G3
Equifax Secure Certificate Authority	DigiCert Assured ID Root CA
Equifax Secure eBusiness CA-1	DigiCert Global Root G2
Equifax Secure Global eBusiness CA-1	DigiCert Global Root G3
GeoTrust Global CA	DigiCert Global Root CA
GeoTrust Global CA2	DigiCert Trusted Root G4
GeoTrust Primary Certification Authority	Entrust Root Certification Authority
GeoTrust Primary Certification Authority G2	Entrust Root Certification Authority - G2
GeoTrust Universal CA	Entrust.net Certification Authority (2048)
GeoTrust Universal CA2	GeoTrust Primary Certification Authority - G3
Thawte Personal Freemail CA	GlobalSign Root CA
Thawte Premium Server CA	GlobalSign Root CA - R2
Thawte Primary Root CA	Starfield Root Certificate Authority - G2
Thawte Primary Root CA - G2	TC TrustCenter Class 2 CA II
Thawte Primary Root CA - G3	TC TrustCenter Class 3 CA II
Thawte Server CA	TC TrustCenter Class 4 CA II
VeriSign Class 1 Public Primary Certification Authority	TC TrustCenter Universal CA I
VeriSign Class 1 Public Primary Certification Authority - G2	TC TrustCenter Universal CA III
VeriSign Class 1 Public Primary Certification Authority - G3	Thawte Universal CA Root
VeriSign Class 2 Public Primary Certification Authority - G2	VeriSign Class 3 Secure Server CA - G2
VeriSign Class 2 Public Primary Certification Authority - G3	VeriSign Class 3 Secure Server CA - G3
VeriSign Class 3 Public Primary Certification Authority	Thawte SSL CA
VeriSign Class 3 Public Primary Certification Authority - G2	StartCom Certification Authority
VeriSign Class 3 Public Primary Certification	StartCom Certification Authority G2

Authority - G3	
VeriSign Class 3 Public Primary Certification Authority - G4	Starfield Services Root Certificate Authority - G2
VeriSign Class 3 Public Primary Certification Authority - G5	RapidSSL CA
VeriSign Class 4 Public Primary Certification Authority - G2	Go Daddy Root Certificate Authority - G2
VeriSign Class 4 Public Primary Certification Authority - G3	Cybertrust Global Root
VeriSign Universal Root Certification Authority	COMODOSSLCA
ISRG Root X1 (Let's Encrypt Authority X1 and Let's Encrypt Authority X2 certificates are signed by the root certificate ISRG Root X1.)	COMODO RSA Domain Validation Secure Server CA
Baltimore CyberTrust Root	COMODO RSA Certification Authority
DST Root CA X3	AmazonRootCA4
Verizon Public SureServer CA G14-SHA2	AmazonRootCA3
AddTrust External CA Root	AmazonRootCA2
Go Daddy Class 2 Certification Authority	AmazonRootCA1
Class 2 Primary CA	Yealink Root CA
Cybertrust Public SureServer SV CA	Yealink Equipment Issuing CA
SIP Core	

Configure TLS Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Security > Trusted Certificates/Server Certificates/Client Certs.**
3. Configure the certificate parameters and upload the corresponding certificate.



Via Auto Provisioning

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

```
static.security.trust_certificates[1]
static.security.ca_cert[1]
static.security.cn_validation[1]
static.trusted_certificates.url
static.trusted_certificates.delete
static.security.dev_cert[1]
static.server_certificates.url
static.server_certificates.delete
static.phone_setting.reserve_certs_enable
```

Parameter	Permitted Values	Default	Description
static.security.trust_certificates[1]	0 - Disabled, the device will trust the server no matter whether the certificate sent by the server is valid or not. 1 -Enabled, the device will authenticate the server certificate based on the	1	It enables or disables the device to only trust the server certificates listed in the Trusted Certificates list.

	trusted certificates list. Only when the authentication succeeds, will the device trust the server.		
static.security.ca_cert [1]	0 -Default Certificates 1 -Custom Certificates 2 -All Certificates	2	It configures the type of certificates in the Trusted Certificates list for the device to authenticate for TLS connection.
static.security.cn_validation[1]	0 -Disabled 1-Enabled	0	It enables or disables the device to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server.
static.trusted_certificates.url	URL within 511 characters	Blank	It configures the access URL of the custom trusted certificate used to authenticate the connecting server. Example: <pre>static.trusted_certificates.url = http://192.168.1.20/tc.crt</pre> ! NOTE The certificate you want to upload must be in *.pem, *.crt, *.cer, or *.der format.
static.trusted_certificates.delete	http://localhost/all	Blank	It deletes all uploaded trusted certificates.
static.security.dev_cert[1]	0 - Default Certificates 1- Custom Certificates	0	It configures the type of device certificates for the device to send for TLS authentication.
static.server_certificates.url	URL within 511 characters	Blank	It configures the access URL of the certificate the device sends for authentication. ! NOTE The certificate you want to

			upload must be in *.pem or *.cer format.
static.server_certificates.delete	http://localhost/all	Blank	It deletes all uploaded server certificates.
static.phone_setting.reserve_certs_enable	0 -Disabled 1 -Enabled	0	It enables or disables the device to reserve custom certificates after it is reset to factory defaults.

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

Phone Lock

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

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

If you want to use the phone lock feature, see [Phone Lock](#).

NOTE

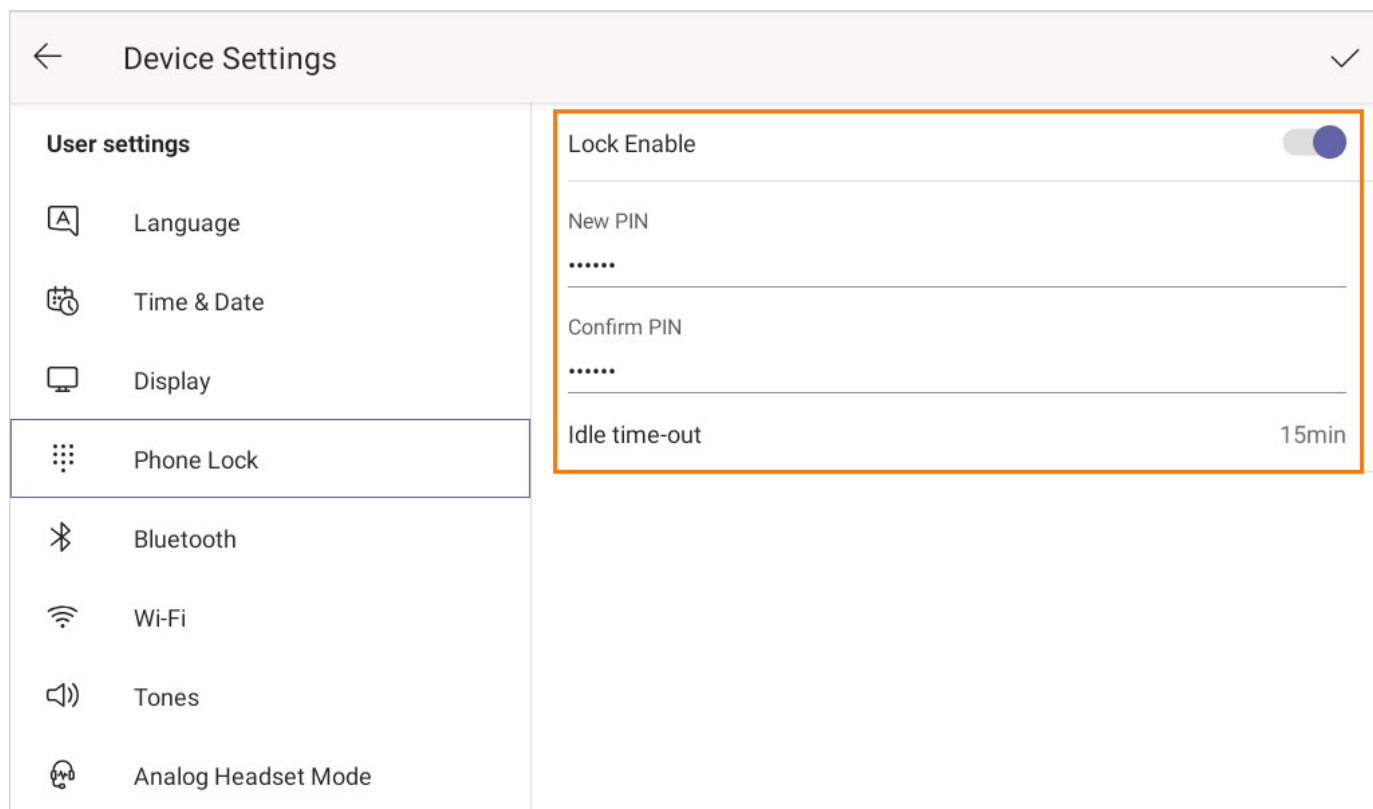
The Phone Lock feature is unavailable to Common Area Phones.

Phone Lock Configuration Via Device User Interface

1. Select the method according to your device:

VP59/MP58/MP56/MP54/CP965	MP52/MP55 E2
Tap the account avatar and go to Settings > Device Settings > Phone Lock .	Go to  > Settings > Lock Screen & PIN .

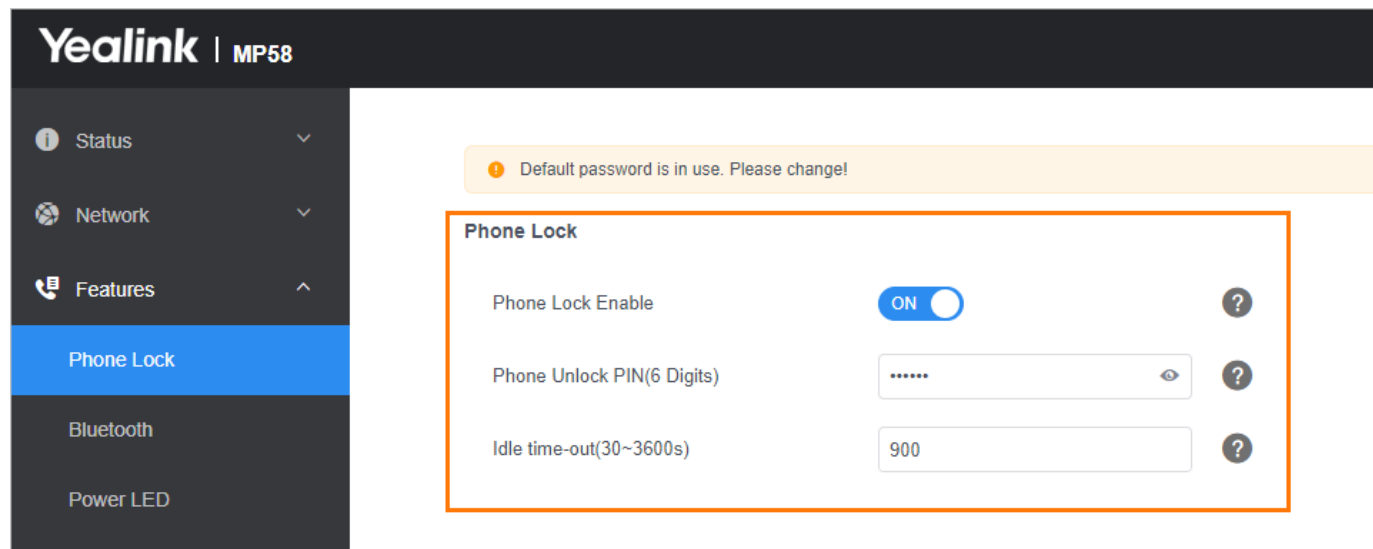
2. Set the corresponding parameters.



The screenshot shows the 'Device Settings' app interface. On the left, a list of settings includes 'User settings', 'Language', 'Time & Date', 'Display', 'Phone Lock' (highlighted with a purple box), 'Bluetooth', 'Wi-Fi', 'Tones', and 'Analog Headset Mode'. On the right, the 'Phone Lock' configuration screen is shown, enclosed in an orange box. It contains the following fields: 'Lock Enable' (a toggle switch turned on), 'New PIN' (a field with six dots), 'Confirm PIN' (a field with six dots), and 'Idle time-out' (set to '15min').

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Features > Phone Lock**.



Via Auto Provisioning

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

```
phone_setting.phone_lock.enable
phone_setting.phone_lock.unlock_pin
phone_setting.phone_lock.lock_time_out
phone_setting.phone_lock.complex_pin_enable
phone_setting.phone_lock.complex_pin_rule.X
```

Parameter	Permitted Values	Default	Description
phone_setting.phone_lock.enable	0- Disabled 1- Enabled	0	It enables or disables the phone lock feature.
phone_setting.phone_lock.unlock_pin	Characters within 6 digits	Blank	It configures the password for unlocking the phone.
phone_setting.phone_lock.lock_time_out	Integer from 30 to 3600	900	It configures the interval (in seconds) to automatically lock the phone.

phone_setting.phone_lock.complex_pin_enable	0- Disabled 1- Enabled	0	It enables or disables complex password rules for locking the phone.  NOTE It works only if “phone_setting.phone_lock.enable” is set to 1.
phone_setting.phone_lock.complex_pin_rule.X[2]	String within 511 characters	See the following to get the default value*.	Example: <pre>phone_setting.phone_lock.complex_pin_rule.1 = ^((?!(((9(?=8) 8(?=7) 7(?=6) 6(?=5) 5(?=4) 4(?=3) 3(?=2) 2(?=1) 1(?=0)) (0(?=1) 1(?=2) 2(?=3) 3(?=4) 4(?=5) 5(?=6) 6(?=7) 7(?=8) 8(?=9)))){2}\d)).*\$</pre> means not allowed three consecutive numbers. <pre>phone_setting.phone_lock.complex_pin_rule.2 = ^((?!(\d)\1{2}).)*\$</pre> means not allowed three repeated numbers. <pre>phone_setting.phone_lock.complex_pin_rule.3 = ^((?!((admin) (administrator) (var) (user) (test))).)*\$</pre> means not contain 'admin', 'administrator', 'var', 'user', 'test' strings. <pre>phone_setting.phone_lock.complex_pin_rule.4 = (?!(^(\d+ [a-zA-Z]+ [\`~!@#\$%^&*()\_-=\+\\\\\\[\]\{\};:\"",<.>/?]+)\$)^\[w`~!@#\$%^&*()_-=\+\\\\\\[\]\{\};:\"",<.>/?]{6,20}\$</pre> means includes at least two characters: letters, numbers or special characters.

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

[2]X ranges from 1 to 10.

The default value is: (?!(^(\d+|[a-zA-Z]+|[\`~!@#\$%^&\*()\\_-=\+\\\\\\[\]\{\};:\"",<.>/?]+)\$)^\[w`~!@#\$%^&()_-=\+\\\\\\[\]\{\};:\"",<.>/?]{6,20}\$

User and Administrator Identification

Introduction

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

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

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

If you enable the feature of complex passwords, when you sign in on the web interface more than 5 times with the default password, you will be forced to change your password.

The modified password must comply with the following rules:

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

Configure User and Administrator Identification

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

```
static.security.user_name.user
static.security.user_name.admin
static.security.user_name.var
static.security.user_password
static.security.custom_password_rule.X
```

Parameter	Permitted Values	Default	Description
static.security.user_name.user	String within 32 characters	user	It configures the user name for the device' s web user interface access.
static.security.user_name.admin	String within 32 characters	admin	It configures the user name of the administrator for the device' s web user interface access.
static.security.user_name.var	String within 32 characters	var	It configures the user name of the var for the device' s web user interface access.  NOTE It works only if "static.security.var_enable" is set to 1 (Enabled).
static.security.user_password	String within 32 characters	user	It configures the password of the user or administrator. The device uses “user” as the default user password and “admin” as the default administrator password. The valid value format is "<username>: <new password>". Example: static.security.user_password = user:123 means setting the password of the user to 123. static.security.user_password = admin:456 means setting the password of the administrator to 456.  NOTE The devices support ASCII characters 32-126(0x20-0x7E) in passwords. You can set the password to be empty via the web user interface only.
static.security.custom_password_rule.X [1]	String within 511 characters	Blank	It configures the regular expression rules of the password, and the result is the AND operation of multiple regular expressions (up to 10). Example: static.security.custom_password_rule.1 = .{8,} means length of the password more than 8 digits.

		static.security.custom_password_rule.2 = ^((?!.*(000\\ 111\\ 222\\ 333\\ 444\\ 555\\ 666\\ 777\\ 888\\ 999).*)).* \$ means not allowed three consecutive identical numbers. static.security.custom_password_rule.3 = ^((?!\\d(?:?<=0)1\\(?:<=1)2\\(?:<=2)3\\(?:<=3)4\\(?:<=4)5\\(?:<=5)6\\(?:<=6)7\\(?:<=7)8\\(?:<=8)9){2,}).*) \$ means not allowed three consecutive incremental numbers. static.security.custom_password_rule.4 = ^((?!\\d(?:?<=9)8\\(?:<=8)7\\(?:<=7)6\\(?:<=6)5\\(?:<=5)4\\(?:<=4)3\\(?:<=3)2\\(?:<=2)1\\(?:<=1)0){2,}).*) \$ means not allowed three consecutive diminishing numbers. static.security.custom_password_rule.5 = ^((?!.*(admin\\ administrator\\ var\\ user\\ test).*)).* \$ means not allowed to contain xxx. NOTE When you set "static.security.custom_password_rule.X" (X=1-10) to be blank, the feature of complex password is disabled.
--	--	--

[1] X ranges from 1 to 10.

Configure User Access Level

For more information, refer to the [Yealink SIP IP Phones Configuration Guide for User Access Level](#).

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

```
static.security.var_enable[1]
static.web_item_level.url[1]
```

Parameter	Permitted Values	Default	Description
static.security.var_enable[1]	0-Disabled 1-Enabled	0	It enables or disables the 3-level access permissions (admin, user, var).
static.web_item_level	URL within 511	Bl	It configures the file's access URL, which defines 3-

vel.url[1]	characters	an k	level access permissions.
------------	------------	---------	---------------------------

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

Overview

Introduction

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

Supported Devices

This feature is available VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965/MP52 E2/MP55 E2 but unavailable to MP52.

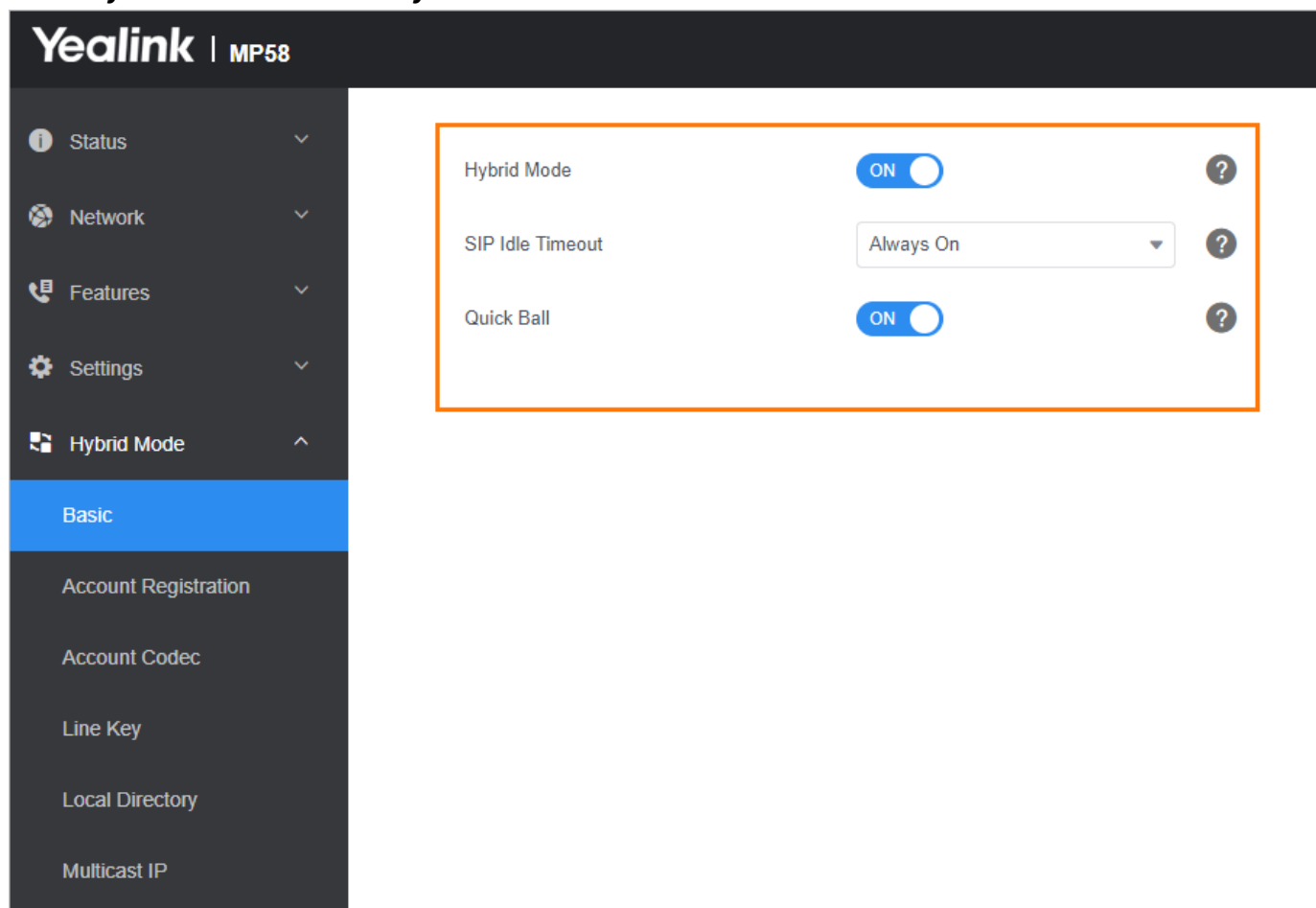
What Features Can You Use When Hybrid Mode Is Enabled?

- Register SIP account on MP Teams phones.
- [Set Up Multicast Paging](#)
- [Configure Account Codec](#)
- [Configure Local Directory](#)

Enable and Configure Hybrid Mode

Configure Hybrid Mode Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Hybrid Mode > Basic > Hybrid Mode**.



Via Auto Provisioning

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

```
features.hybrid_mode.enable  
features.hybrid_mode.quick_ball.enable  
features.hybrid_mode.sip_idle_timeout  
features.hybrid_mode.sip_callwaiting.enable
```

Parameter	Permitted Values	Default	Description
-----------	------------------	---------	-------------

features.hybrid_mode.enable	0 - Disabled, the Hybrid Mode configuration does not display on the phone user interface and the Account and Directory configurations do not display on the web user interface. 1 -Enabled	0	It enables or disables the hybrid mode feature. For touch phones (VP59/CP965/MP54 (E2)...): The quick ball is used to switch between apps in Teams/Survivability. For non-touch phones (MP52 E2/MP55 E2): The quick ball indicates that there is an ongoing call in a background app.
features.hybrid_mode.quick_ball.enable	0 -Disabled 1 -Enabled	0	It enables or disables the quick ball for quickly switching between Teams APP and Survivability APP.
features.hybrid_mode.sip_idle_timeout	0-Always on 60-1 min 120-2 min 300-5 min 600-10 min 900-15 min 1800-30 min 3600-1 h	0	It configures the waiting time of returning to the Teams APP when the user has no operation in Survivability APP.
features.hybrid_mode.sip_callwaiting.enable	0 -Disabled 1 -Enabled	0	It configures that puts an incoming SIP call to waiting mode and has a pop-up prompt during a Teams call.

To achieve quick switching between Teams and Survivability App:

- For touchscreen devices: after configuring the following settings, tap the **quick ball** for quick switching.

```
features.hybrid_mode.enable = 1
features.hybrid_mode.quick_ball.enable = 1
```

- For keypad devices, configure: after configuring the following settings, long-press the **cancel key** for quick switching.

```
features.hybrid_mode.enable = 1
```

Set Up Multicast Paging

Multicast Paging Introduction

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

Multicast Paging allows you to send instant audio announcements to groups of phones listening to the same multicast IP address of the PBX directly.

With multicast paging, phones are programmed to listen to a broadcast address. The multicast paging is a single SIP call instead of a multiple-party conference call. This greatly reduces the workload placed on the PBX, especially when many devices are involved.

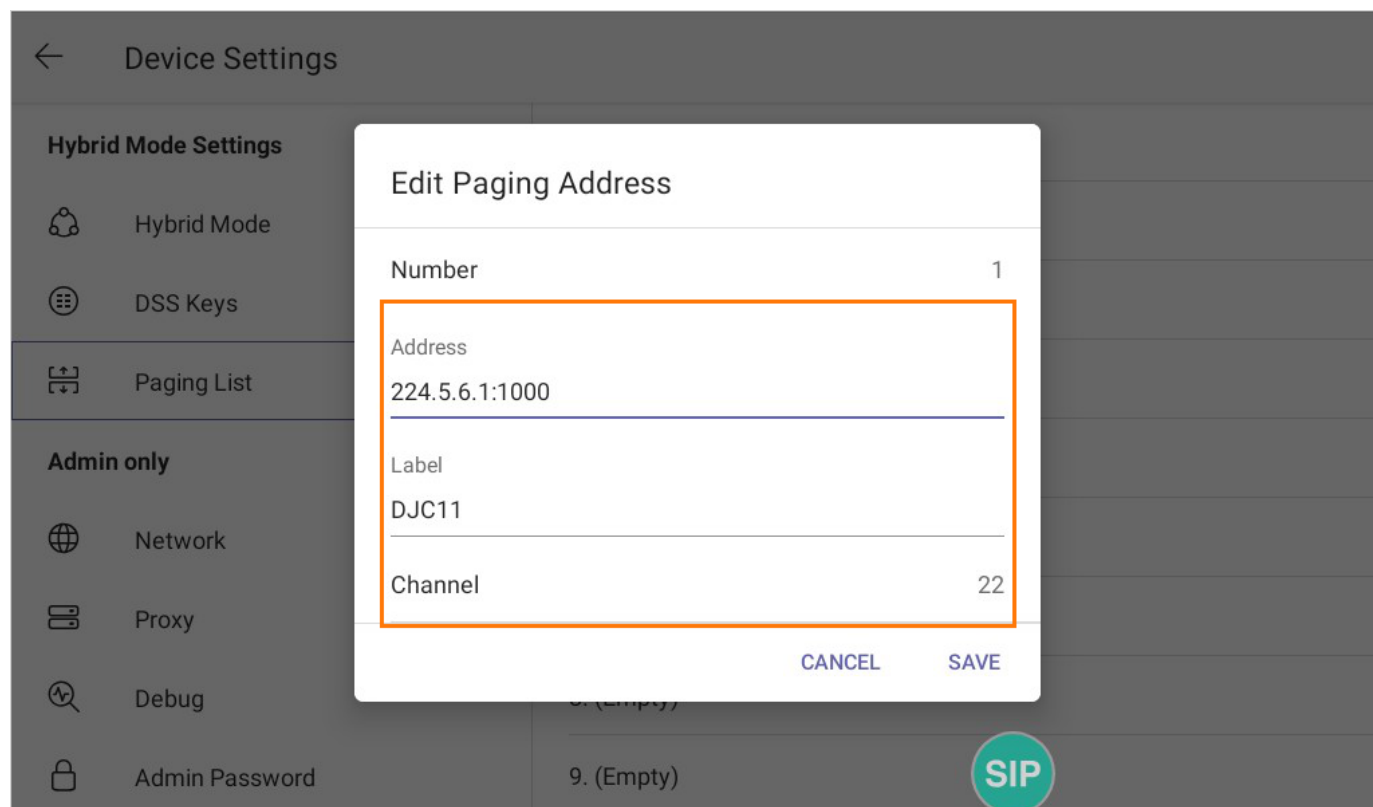
NOTE

- All phones you want to include in the multicast paging group must be **on the same network** since a network broadcast protocol is used.

Set a Paging Group Via Device User Interface

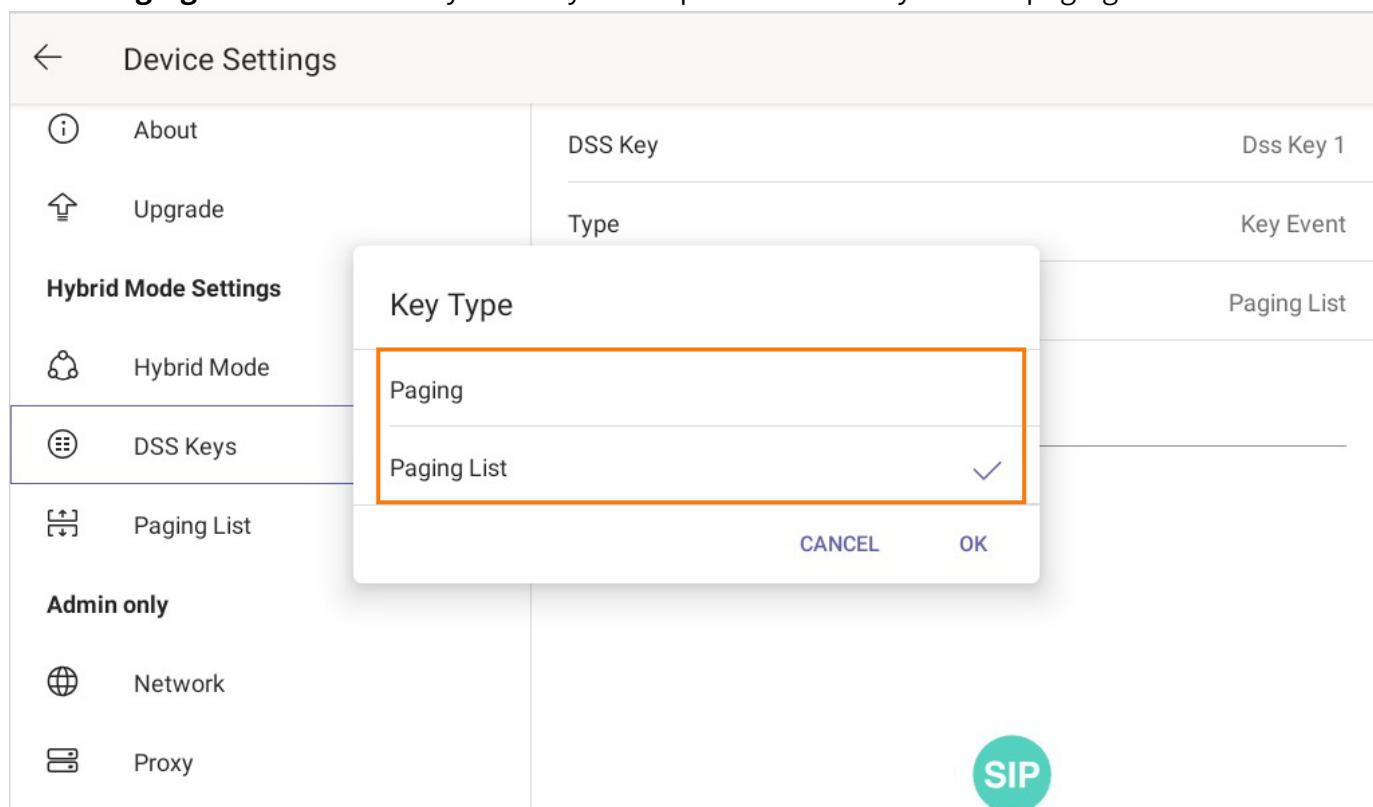
1. Tap the account avatar and go to **Settings > Device Settings > Hybrid Mode Settings > Paging List**.
2. Edit the paging address.

Parameter	Description
Address	It configures the IP address and port number of the multicast paging group in the paging list. Make sure that you use the same IP address as the receiver.
Label	It configures the name of the multicast paging group to be displayed in the paging list. It will be displayed on the phone screen when placing the multicast paging calls.
Channel	It configures the channel of the multicast paging group in the paging list. Make sure that you use the same channel as the receiver.



3. Tap the account avatar and go to **Settings > Device Settings > Hybrid Mode Settings > DSS Keys**.

4. Select **Paging List** for the line key so that you can press the line key to send paging.



Via Web User Interface

1. [Log in to the phone web user interface as an admin](#).
2. Go to **Hybrid Mode > Multicast IP > Paging List**.

3. Set the paging address, the label and the channel.

Parameter	Description
Address	It configures the IP address and port number of the multicast paging group in the paging list. Make sure that you use the same IP address as the receiver.
Label	It configures the name of the multicast paging group to be displayed in the paging list. It will be displayed on the phone screen when placing the multicast paging calls.
Channel	It configures the channel of the multicast paging group in the paging list. Make sure that you use the same channel as the receiver.

Yealink | MP58

- Status
- Network
- Features
- Settings
- Hybrid Mode
 - Basic
 - Account Registration
 - Account Codec
 - Line Key
 - Local Directory
 - Multicast IP**

6 IP Address			0	6
7 IP Address			0	7
8 IP Address			0	8
9 IP Address			0	9
10 IP Address			0	10
Total: 31 < 1 2 3 4 > 10 / Page Goto 1 Page				

Paging List ?

Index	Paging Address	Label	Channel
1	224.5.6.1:1000	Paging List	22
2			0
3			0
4			0
5			0

4. Go to **Hybrid Mode > Line Key**.

5. Select **Paging List** for the line key so that you can press the line key to send paging.

Yealink | MP58

Status Network Features Settings Hybrid Mode Basic Account Registration Account Codec **Line Key** Local Directory Multicast IP Security

Enable Page Tips ☒

Line Key 1-10 Line Key 11-20 Line Key 21-27

Key	Type	Value	Label	Line	Extension
Line Key1	Paging List		Group PAG	N/A	
Line Key2	Paging	224.5.6.0:1008	Paging	N/A	22
Line Key3	N/A			N/A	
Line Key4	Line			Line4	
Line Key5	Line			Line5	
Line Key6	Line			Line6	
Line Key7	Line			Line7	
Line Key8	Line			Line8	
Line Key9	Line			Line9	
Line Key10	Line			Line10	

Via Auto Provisioning

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

linekey.X.type
 linekey.X.line
 linekey.X.value
 linekey.X.label
 linekey.X.extension
 features.auto_linekeys.enable
 account.X.number_of_linekey
 multicast.codec
 multicast.paging_address.X.ip_address
 multicast.paging_address.X.label
 multicast.paging_address.X.channel
 multicast.listen_address.X.ip_address
 multicast.listen_address.X.label
 multicast.listen_address.X.channel
 multicast.receive_priority.enable
 multicast.receive_priority.priority

Parameter	Permitted Values	Default	Description
linekey.X.type[1]	0-N/A	15	It configures the key feature.

	15 -Line 24 -Paging 66 -Paging List	(VP59/MP58 / MP58-WH) 0 (MP54)	
linekey.X.line[1]	1	1	It configures the desired line to apply the line key feature.
linekey.X.value[1]	String within 99 characters	Blank	It configures the value for line key features.
linekey.X.label[1]	String within 99 characters	Blank	It configures the label displayed on the phone screen. This is an optional configuration.
linekey.X.extension [1]	0 to 31	Blank	It configures the channel of the multicast paging group.
features.auto_linekeys.enable	0-Disabled 1-Enabled	0	It enables or disables to assign multiple line keys to associate with a specific account. NOTE The number of the line keys is determined by "account.X.number_of_linekey".
account.X.number_of_linekey[2]	Integer from 1 to 999	1	It configures the number of line keys to be assigned with a specific account from the first unused one. If a line key is in used, the phone will skip to the next unused DSS key.
multicast.codec	PCMU, PCMA, G729, G722	G722	It configures the codec for multicast paging.
multicast.paging_a	IP address: port	Blank	It configures the IP address and port

ddress.X.ip_addresses [3]	(224.0.0.1-239.255.255.255 port: 0-65535)	k	number of the multicast paging group in the paging list.
multicast.paging_address.X.label[3]	String	Blank	It configures the name of the multicast paging group to be displayed in the paging list. It will be displayed on the phone screen when placing the multicast paging calls.
multicast.paging_address.X.channel[3]	0-all the Yealink phones running old firmware version or Yealink phones listen to channel 0 or third-party available devices in the paging group can receive the RTP stream. 1 to 25-the phones pre-configured to listen to the channel can receive the RTP stream. 26 to 30-the Yealink phones pre-configured to listen to the channel can receive the RTP stream.	0	It configures the channel of the multicast paging group in the paging list.
multicast.receive_priority.enable	0- Disabled, the phone will ignore the incoming multicast paging calls when there is an active multicast paging call on the phone. 1-Enabled, the phone will receive the incoming multicast paging call with a higher priority and ignore the one with a lower priority.	1	It enables or disables the phone to handle the incoming multicast paging calls when there is an active multicast paging call on the phone.
multicast.receive_p	0-Disabled, all incoming	31	It configures the priority of the voice

priority.priority	multicast paging calls will be automatically ignored when a voice call is in progress. 1-1 2-2 3-3 ... 3 1-31 If it is set to other values, the phone will receive the incoming multicast paging call with a higher or equal priority and ignore the one with a lower priority when a voice call is in progress.		call (a normal phone call rather than a multicast paging call) in progress. 1 is the highest priority, 31 is the lowest priority.
multicast.listen_address.X.ip_addresses[3]	IP address: port (224.0.0.1-239.255.255.255 port: 0-65535)	Blank	It configures the multicast address and port number that the phone listens to.
multicast.listen_address.X.channel[3]	0-the phone can receive an RTP stream of the pre-configured multicast address from the phones running old firmware version, from the phones listen to the channel 0, or from the available third-party devices. 1 to 25-the phone can receive an RTP stream of the pre-configured multicast address on the channel 1 to 25 respectively from Yealink phones. 26 to 30-the phone can	0	It configures the channel that the phone listens to.

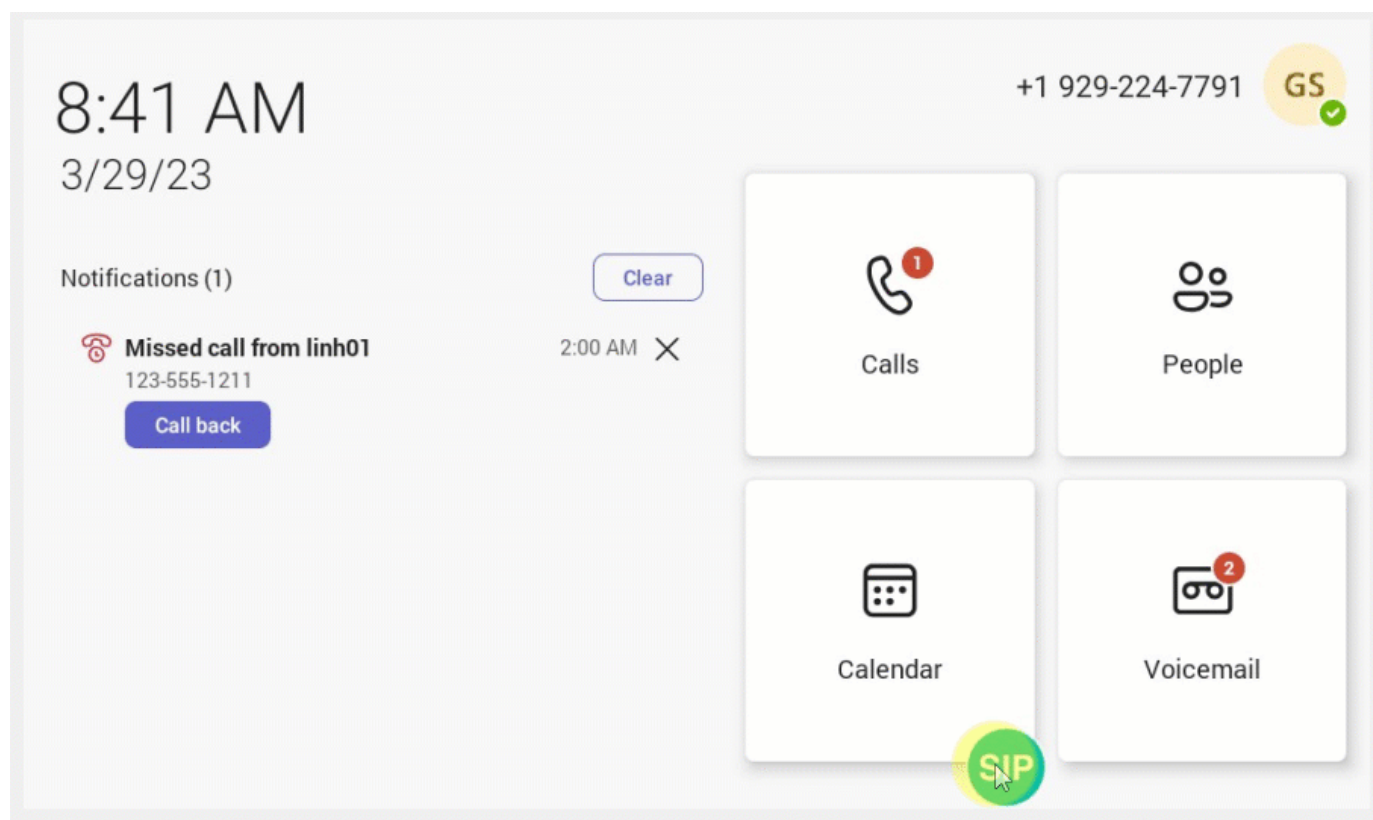
	receive the RTP stream of the pre-configured multicast address on the channel 26 to 30 respectively from Yealink phones.		
multicast.listen_address.X.label[3]	String within 99 characters	Blank	It configures the label to be displayed on the phone screen when receiving the multicast paging calls.

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

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

[3]X ranges from 1 to 31.

You can see your phone screen displaying the line key you set. Press the line key you can send the paging.



Set a Paging Via Device User Interface

1. Select the method according to your device:

VP59/MP5X E2	CP965
--------------	-------

Go to  > Settings > Device Settings > Hybrid Mode Settings > DSS Keys.	Tap the avatar in the top-right corner of the screen and go to Settings > Device Settings > Hybrid Mode Settings > DSS Keys.
---	--

2. Edit the following parameters and save the change.

Parameter	Description
Label	It configures the name of the multicast paging group to be displayed in the paging list. It will be displayed on the phone screen when placing the multicast paging calls.
Value	It configures the IP address and port number of the multicast paging group in the paging list. Make sure that you use the same IP address as the receiver.
Channel	It configures the channel of the multicast paging group in the paging list. Make sure that you use the same channel as the receiver.

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)

2. Go to **Hybrid Mode > Line Key.**

Parameter	Description
Value	It configures the IP address and port number of the multicast paging group in the paging list. Make sure that you use the same IP address as the receiver.
Label	It configures the name of the multicast paging group to be displayed in the paging list. It will be displayed on the phone screen when placing the multicast paging calls.
Extension	It configures the channel of the multicast paging group in the paging list. Make sure that you use the same channel as the receiver.

Yealink | MP58

Status

Network

Features

Settings

Hybrid Mode

Basic

Account Registration

Account Codec

Line Key

Local Directory

Multicast IP

Security

Enable Page Tips ON

Line Key 1-10

Line Key 11-20

Line Key 21-27

Key	Type	Value	Label	Line	Extension
Line Key1	Paging List		Group PAG	N/A	
Line Key2	Paging	224.5.6.0:1008	Paging	N/A	22
Line Key3	N/A			N/A	
Line Key4	Line			Line4	
Line Key5	Line			Line5	
Line Key6	Line			Line6	
Line Key7	Line			Line7	
Line Key8	Line			Line8	
Line Key9	Line			Line9	
Line Key10	Line			Line10	

Via Auto Provisioning

See [setting paging group via auto provisioning](#).

FAQ

[How to use multicast paging on MP Teams phones?](#)

Configure Account Codec

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

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Hybrid Mode > Account Codec**.

Via Auto Provisioning

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

```
account.X.codec.<payload_type>.enable
account.X.codec.<payload_type>.priority
```

Parameter	Permitted Values	Default	Description
account.X.codec.<payload_type>.enable[1]	0-Disabled 1-Enabled	When the audio codec is G.722.1c (48kb/s), the default value is 1; When the audio codec is G.722.1c (32kb/s), the default value is 1; When the audio codec is G.722.1c (24kb/s), the default value is 1; When the audio codec is G.722.1 (48kb/s), the default value is 1; When the audio codec is G722, the default value is 1; When the audio codec is PCMU, the default value is 1; When the audio codec is PCMA, the default value is 1; When the audio codec is G729, the default value is 1; When the audio codec is G726-16, the	It enables or disables the specified audio codec. The name (payload_type) of the audio codec: Ares codec g722_1c_48kpbs-G.722.1c (48kb/s) g722_1c_32kpbs-G.722.1c (32kb/s) g722_1c_24kpbs-G.722.1c (24kb/s) g722_1_24kpbs-G.722.1 (24kb/s) g722-G722 pcmu-PCMU pcma-PCMA g729-G729 g726_16-G726-16

		default value is 0; When the audio codec is G726-24, the default value is 0; When the audio codec is G726-32, the default value is 0; When the audio codec is G726-40, the default value is 0; When the audio codec is G723_53, the default value is 0; When the audio codec is G723_63, the default value is 0; When the audio codec is iLBC, the default value is 0; When the audio codec is Ares codec, the default value is 0.	g726_24-G726-24 g726_32-G726-32 g726_40-G726-40 g723_53-G723_53 g723_63-G723_63 ilbc-iLBC
account.X.code c.<payload_type>.priority[1]	Integer from 0 to 16	When the audio codec is G722.1c (48kb/s), the default value is 1; When the audio codec is G722.1c (32kb/s), the default value is 2; When the audio codec is G722.1c (24kb/s), the default value is 3; When the audio codec is G722.1 (24kb/s), the default value is 4; When the audio codec is G722, the default value is 5; When the audio codec is PCMU, the default value is 6; When the audio codec is PCMA, the default value is 7; When the audio codec is G729, the default value is 8; When the audio codec is Ares codec, the default value is 9; When the audio codec is G726_16, the default value is 0;	It configures the priority of the enabled audio codec. The name (payload_type) of the audio codec: Ares codec g722_1c_48kpbs-G.722.1c (48kb/s) g722_1c_32kpbs-G.722.1c (32kb/s) g722_1c_24kpbs-G.722.1c (24kb/s) g722_1_24kpbs-G.722.1 (24kb/s) g722-G722 pcmu-PCMU pcma-PCMA g729-G729 g726_16-G726-16 g726_24-G726-24 g726_32-G726-32 g726_40-

		When the audio codec is G726_24, the default value is 0; When the audio codec is G726_32, the default value is 0; When the audio codec is G726_40, the default value is 0; When the audio codec is G723_53, the default value is 0; When the audio codec is G723_63, the default value is 0; When the audio codec is iLBC, the default value is 0.	G726-40 g723_53-G723_53 g723_63-G723_63 ilbc-iLBC
--	--	--	---

[1]X is the account ID. For MP58 (E2)/MP56 (E2)/VP59, X=1-16; for MP54 (E2), X=1.

Configure Local Directory

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

Via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Hybird Mode > Local Directory > Import.**

The screenshot shows the Yealink MP58 web interface. On the left is a sidebar menu with options: Status, Network, Features, Settings, Hybrid Mode (expanded), Basic, Account Registration, Account Codec, Line Key, Local Directory (selected), Multicast IP, and Security. The main content area is titled 'Local Directory' and contains a table of contacts. Above the table are buttons for 'New Contacts', 'Delete Contacts', 'Move to', 'Import' (highlighted with an orange box), and 'Export'. The table has columns for #, Name, Office Number, Mobile Number, Other Number, All Contacts, and Operation. It lists 10 contacts, all with Office Number 50031 and Mobile Number 60031. The bottom of the table shows 'Total: 10' and pagination controls.

Via Auto Provisioning

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

local_contact.data.url

Parameter	Permitted Values	Default	Description
local_contact.data.url	URL within 511 characters	Blank	It configures the access URL of the local contact file (*.xml).

Connect MP Teams Phone to YMCS or YDMP

Introduction

You can enable the device management feature to connect devices and report device information to the Yealink Device Management Platform (YDMP)/Yealink Management Cloud Service (YMCS), where you can realize mass device management, including but not limited to:

- Update the firmware for one or multiple groups of devices
- Change the configuration for one or multiple groups of devices
- Diagnose devices remotely

How to Connect MP Teams Phone to YMCS/YDMP

You can connect MP Teams phones to YMCS in the following ways:

Add Devices to the Phone

1. Select the method according to your device:

MP58 (E2)/MP56 (E2)/MP54 (E2)	MP52 (E2)/MP55 E2
1. Tap the account avatar and go to Settings > Device Settings > Yealink Cloud Service. 2. Enter the admin password and tap OK.	Go to  > Settings > Yealink Cloud Service .

2. Enable the **Cloud Platform Device Management** and tap **Device Manage Platform**.

3. Enter the related information and then tap **Save**.

← Back

Device Settings

Wi-Fi

Analog Headset Mode

Microsoft privacy settings

Advanced

Network

Yealink Cloud Service

System

Debug

← Device Manage Platform Save

Connection Status

Device Management Server Yealink Device Management Platform ▾

Platform Address

Port number

Deployment ID

Device Name

Add Devices on the Phone Web User Interface

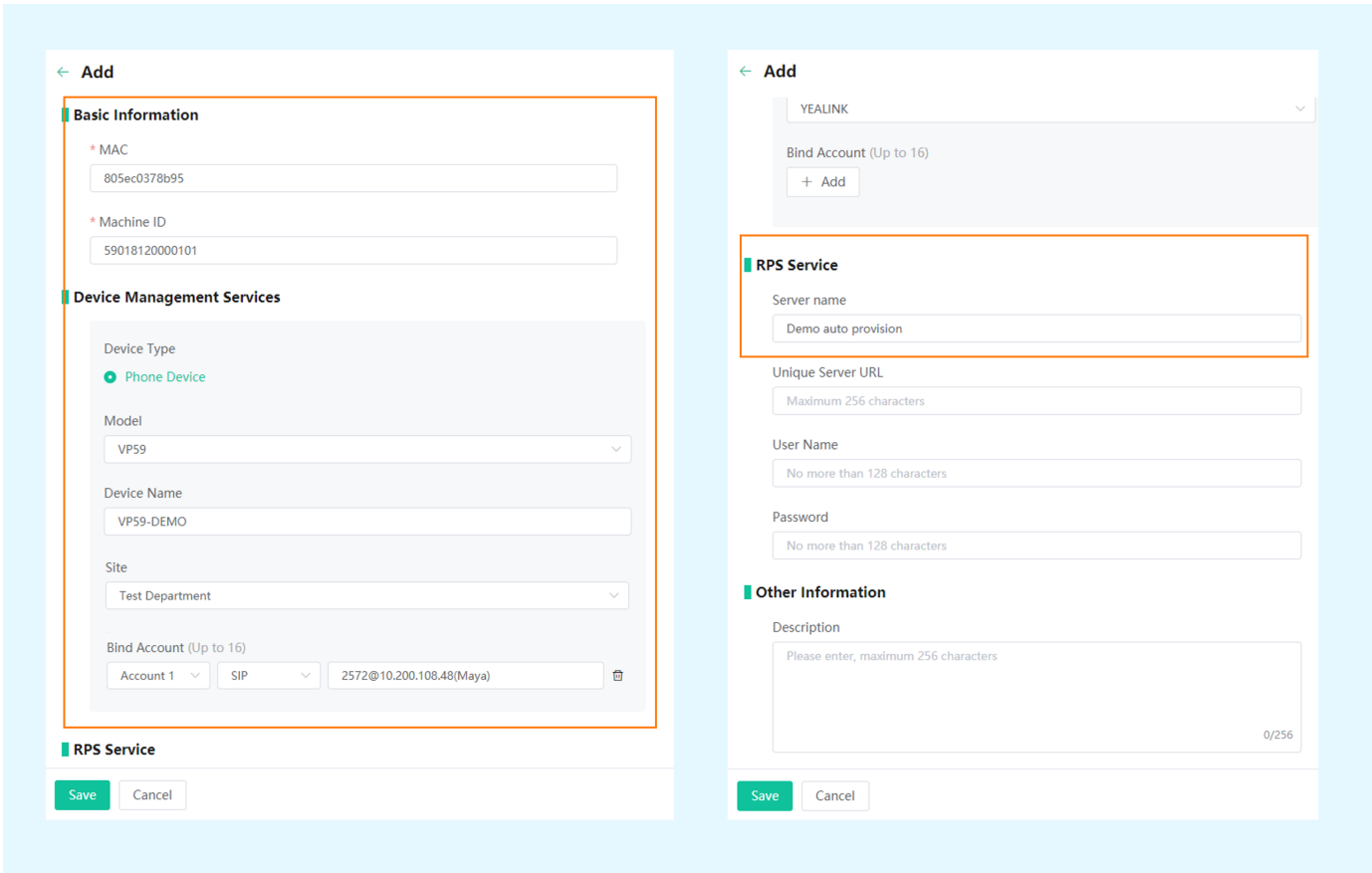
1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Yealink Cloud Service**.
3. Enable the **Cloud Platform Device Management**, then read and agree the *Yealink Cloud Service Agreement*.
4. Enter the related information and click **Confirm**.

The screenshot shows the Yealink Cloud Service configuration page. On the left is a dark sidebar menu with options: Status, Network, Features, Settings (expanded), Preference, Time&Date, Yealink Cloud Service (highlighted), Upgrade, Auto Provision, Configuration, Voice, Tones, Power Saving, Hybrid Mode, and Security. The main content area has a yellow warning banner at the top: "These users (user) are using the default password, please change the password!". Below this, the "Yealink Cloud Service" toggle is set to "ON". A link to "Check 《Yealink Cloud Service Agreement》" is provided. The "Device Management" section has a "Cloud Platform Management Server" toggle set to "ON". The "Device Manage Platform" section contains the following fields: "Connection Status" (Connected), "Device Management Server" (Yealink Device Management Platform), "Platform Address" (Please enter (required)), "Platform Port" (Please enter (required)), "Deployment ID" (Please enter (optional)), and "Device Name" (MP56 E2). At the bottom right are "Confirm" and "Cancel" buttons.

Add Devices to the Device List (YMCS/YDMP Portal)

Add a Single Device

1. Sign in to [YMCS](#)/YDMP as an enterprise administrator.
2. Go to **Device > Phone Device > Add**.
3. Set the parameters and click **Save**.



5.

Parameter	Introduction
MAC	Enter the device MAC address.
Machine ID	Enter the device machine ID.
Device Type	Select the device type.
Model	Select the device model.
Device Name	Enter a descriptive name for the device.
Site	Select a site for the device.
Bind Account	Select an account to bind with this device.
Server name	Select the server you add from the drop-down list. NOTE If you do not connect devices via Yealink RPS, you do not need to set this parameter.
Unique Server URL	If you do not add a server, you can add a server URL. NOTE

	! - If you select an added server and set the unique server URL, the unique server has a higher priority than the added server. Therefore, YMCS will send the unique server URL to the device. - If you do not connect devices via Yealink RPS, you do not need to set this parameter.
User Name	Enter the user name that can access the unique server.
Password	Enter the user password.
Description	Enter the description.

Add Multiple Devices

1. Go to **Device > Phone Device > Import**.
2. Select **Yes** under **Import Server** and select the server name from the **Server name** drop-down menu.
3. Click **Download template** to download the template.
4. Enter the device information in the template.
5. Upload the template and click **Upload**.

Import device

Import Server
☒ Yes ☐ No
 * Server name
 Demo auto provision

Tips: Please download the template and import the data as required
[Download template](#)

* Upload File
 Drag the file here, or [Click here](#)
 Note: The file extension must be .xls or .xlsx (Excel format), and the maximum number of imported data cannot exceed 5000
 device_import_template.xlsx
[Upload](#) [Cancel](#)

Excel Template Data:

*MAC	*Machine ID	Model	Device Name	Site	Unique URL	User Name
80E0C4A57F	00119C0000000101(MPS4Team)	MPS4-TEST				
80E0C4A462	00119C0000000202(MPS8Team)	MPS8-TEST				

Configure Parameters via Auto Provisioning

See the following image to see how your auto provisioning server works to connect the devices to YMCS:

How it Works?



If your device firmware versions are too low, you need to update them to the latest versions. You can visit [Yealink Support](#) to download the latest firmware version.

For convenience, you can use the following command to update the device firmware:

```
static.firmware.url=http://192.168.1.20/150.86.0.5.rom
```

NOTE

Set the Device Autop URL address to your auto provisioning URL.

1. Configure the following commands:

```
features.cloud_services.enable
dm.enable
dm.server.address
dm.server.port
```

NOTE

Change the value of dm.server.address according to your enterprise's location:

- EU region: eu-device-scheduler.ymcs.yealink.com
- US region: us-device-scheduler.ymcs.yealink.com
- AU region: au-device-scheduler.ymcs.yealink.com

Parameters	Description	Permitted Values	Default

features.cloud_services.enable	It enables or disables the Yealink cloud services.	0- Disabled 1-Enabled	0
dm.enable	It enables or disables the device management feature.	0- Disabled 1-Enabled	0
dm.server.address	It configures the server address of the YDMP/YMCS.	String within 512 characters	Blank
dm.server.port	It configures the server port of the YDMP/YMCS.	Integer from 0 to 65535	443

Manage Devices on Intune

Manage Device Compliance and Conditional Access

Compliance Policy and Conditional Access are two different features inside of Microsoft Intune. We can use them cooperatively to manage devices and improve device security.

What are Device Compliance and Conditional Access?

- Device Compliance: Tells you if your device is compliant or not.
- Conditional Access: Determines what to do with these devices depending on their compliant status.

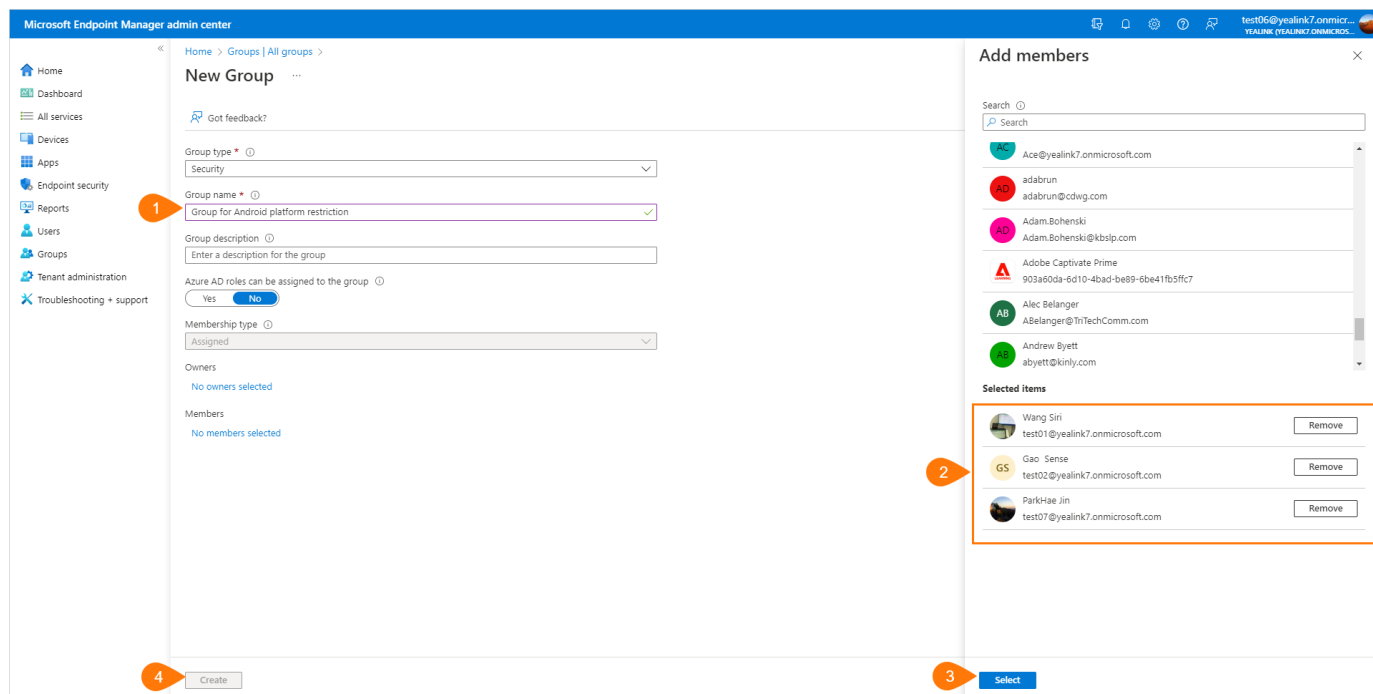
For example, restrict users from enrolling on Intune unless their Android OS versions are later than 9.0.

Step 1 - Create a Group

Skip this step if you already have a group that includes the user. Or you can add the user to the existing group.

Procedure

1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.
2. Go to **Groups** > **New group** to create a group that includes the users whose device platform is restricted.

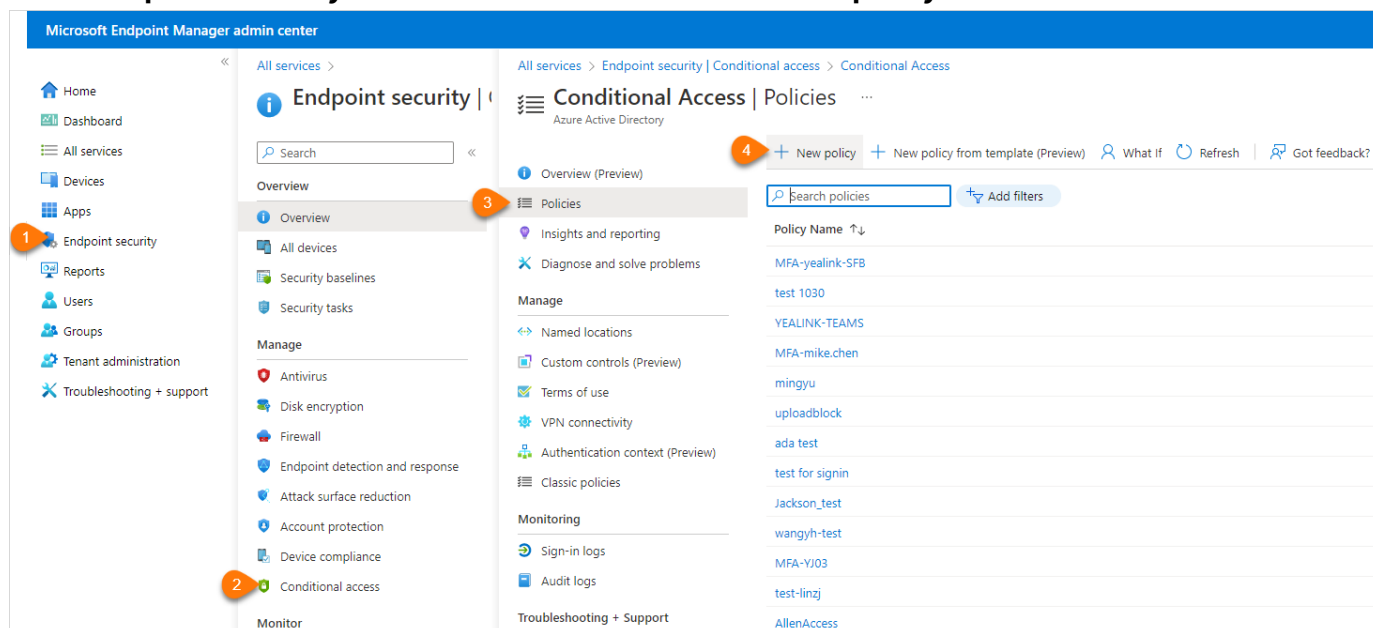


Step 2 - Set Conditional Access

Procedure

1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.

2. Go to **Endpoint security** > **Conditional access** > **Policies** > **New policy**.



3. Enter the policy name.

4. Under the **Users or workload identities** field, select the users or groups to which the policy applies.

NOTE

- Do not select the check box of **All users**. Otherwise, the administrator is locked out.
- Select the users who will use their account to log into Teams phones and do the Intune authentication after you complete setting conditional access and device compliance.
- After you select the users, you can also click **...** > Remove to delete the selected users.

[All services](#) > [Endpoint security](#) | [Conditional access](#) > [Conditional Access](#) | [Policies](#) >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
Sample policy ✓

Assignments

Users or workload identities ⓘ

1 Specific users included

2 *Select users and groups" must be configured

Cloud apps or actions ⓘ

3 No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

4 0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

What does this policy apply to?
Users and groups

Include Exclude

☐ None

☐ All users

☒ Select users and groups

☐ All guest and external users ⓘ

☐ Directory roles ⓘ

☒ Users and groups

Enable policy

Report-only On Off

Create

Select users and groups

test07

ParkHae Jin
test07@yealink7.onmicrosoft.com

test07
test07@yealink7.onmicrosoft.com
Selected

Test07 CAP
test07cap@yealink7.onmicrosoft.com

Selected items

Wang Siri
test01@yealink7.onmicrosoft.com Remove

GS Gao Sense
test02@yealink7.onmicrosoft.com Remove

TE test07
test07@yealink7.onmicrosoft.com Remove

Select

5. Under the **Cloud apps or actions** field, select the desired apps or actions to which this policy applies.

[Home](#) >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
Sample policy ✓

Assignments

Users or workload identities ⓘ

2 Specific users included

Cloud apps or actions ⓘ

1 No cloud apps, actions, or authentication contexts selected

3 *Select apps" must be configured

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Select what this policy applies to
Cloud apps

Include Exclude

☐ None

☐ All cloud apps

☒ Select apps

Select

None

Select at least one app.

Select

Cloud apps

team

☒ Microsoft Teams
cc15fd57-2c6c-4117-a88c-83b1d56b4bbe

☐ Teams Device Store
4b8f5d40-29b0-4950-b174-a2df72363942

Selected items

4 Microsoft Teams
cc15fd57-2c6c-4117-a88c-83b1d56b4bbe Remove

Select

6. Under the **Conditions** field, set the device platform to which this policy applies.

NOTE

- If you want to restrict the login location, you can set the Locations under the Conditions tab.
- Select Android as the device platform because the operating system of Teams phone is Android.

Home > New ...
Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
Sample policy

Assignments
Users or workload identities
Specific users included

Cloud apps or actions
1 app included

Conditions
0 conditions selected

Access controls
Grant
0 controls selected

Session
0 controls selected

Device platforms
Not configured

Locations
Not configured

Client apps
Not configured

Filter for devices
Not configured

Enable policy
Report-only On Off
Create

Device platforms

Apply policy to selected device platforms. [Learn more](#)

Configure
Yes No

Include Exclude

☐ Any device

☒ Select device platforms

☒ Android

☐ iOS

☐ Windows Phone

☐ Windows

☐ macOS

☐ Linux

Done

7. Under the **Grant** field, select the controls to be enforced.

NOTE

- You must select the check boxes of **Require device to be marked as compliant** and **Require approved client app**. Therefore, these two rules will be verified when the policy verifies Yealink Teams phones.
- If your company has other restrictions on the controls, for example MFA, you can select the

check box of Require multi-factor authentication.

Home >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Sample policy ✓

Assignments

Users or workload identities ⓘ

[Specific users included](#)

Cloud apps or actions ⓘ

[1 app included](#)

Conditions ⓘ

[1 condition selected](#)

Access controls

Grant ⓘ

1 controls selected

Session ⓘ

[0 controls selected](#)

Enable policy

Report-only On Off

Create

Grant

Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☐ Require multifactor authentication ⓘ

☒ Require device to be marked as compliant ⓘ

⚠ Don't lock yourself out! Make sure that your device is compliant.

☐ Require Hybrid Azure AD joined device ⓘ

☒ Require approved client app ⓘ
[See list of approved client apps](#)

☐ Require app protection policy ⓘ
[See list of policy protected client apps](#)

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

Select

8. Enable this policy and click **Create**.

Enable policy

Report-only On Off

Create

Step 3 - Set Device Compliance

Procedure

1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.
2. Go to **Endpoint security > Device compliance > Policies > Create policy**.

3. Select a **Platform** for this policy and click **Create**.
4. You can choose a platform according to your enterprise [enrollment methods for Android devices](#).
4. Under the **Basics** tab, specify a **Name** that helps you identify it later and click **Next**.
5. Under the **Compliance settings** tab, set the following settings and click **Next**.
 - a. Set the device health:

b. Set the operating system version:

^ Device Properties

Operating System Version

Minimum OS version ⓘ

5.0.0 ✓

Maximum OS version ⓘ

9.1.0 ✓

c. Set the system security:

System Security

Encryption

Require encryption of data storage on device. ⓘ

Require

Not configured

Device Security

Block apps from unknown sources ⓘ

Block

Not configured

Company Portal app runtime integrity ⓘ

Require

Not configured

Block USB debugging on device ⓘ

Block

Not configured

Minimum security patch level ⓘ

Not configured

Restricted apps ⓘ

Export

App name

App bundle ID

ⓘ Beginning in October 2020, some settings will not be supported on Android devices that are running Android 10 and later and are not Samsung Knox. These settings are labeled with Android 9 and earlier or Samsung Knox. Click to learn more.

All Android devices

These settings work for all Android OS versions and manufacturers.

Maximum minutes of inactivity before password is required ⓘ

Not configured

Require a password to unlock mobile devices ⓘ

Require

Not configured

Android 10 and later

These settings work for devices running Android 10 or later.

Password complexity ⓘ

None

Android 9 and earlier or Samsung Knox

6. Under the **Assignments** tab, assign this policy to the desired groups to which the users belong and click **Next**.

! CAUTION

Do not assign this policy to all users. Otherwise, the administrator is blocked out.

7. Click **Create**.

Check the Status of the Compliance Policy

After you apply your policy, you can see the device sign-in status.

Procedure

1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.
2. Go to **Devices > Compliance**.
3. Click the name of the policy you create.

Policy name	Platform
vivi11	Android Enterprise
rooted device compliance	Android device administrator
Mark Yealink MP5X series as compliant	Android device administrator
test	Android device administrator
testplan for teams	Android device administrator

4. Click **Device status** or **User status** to check the corresponding compliance status.

Search	Refresh	Export	Columns
Overview	Search		
Manage			
Properties			
Monitor			
Device status			
User status			
Per-setting status			
Device	User Principal Name	Compliance status	Last status update
test05_Android_8/16/2022_6:47 ...	None	Not evaluated	
test01_Android_9/22/2022_1:14 ...	test01@yealink7.onmicrosoft.com	Compliant	09/22/2022 09:29 AM
test09_Android_9/21/2022_3:18 ...	None	Not evaluated	
test01_Android_9/8/2022_7:06 AM	None	Not evaluated	
test09_Android_8/24/2022_2:07 ...	None	Not evaluated	
test09_Android_9/21/2022_12:25...	None	Not evaluated	
test05_Android_9/8/2022_9:11 AM	None	Not evaluated	
test09_Android_9/20/2022_12:44...	None	Not evaluated	
test01_Android_9/20/2022_12:01...	test01@yealink7.onmicrosoft.com	Compliant	09/21/2022 02:00 PM

Search	Refresh	Export	Columns
Overview	Search		
Manage			
Properties			
Monitor			
Device status			
User status			
Per-setting status			
User Principal Name	Device count	Compliance status	Last status update
test01@yealink7.onmicrosoft.com	4	Compliant	09/22/2022 11:43 AM

Check the Sign-In Logs

After you apply your policy, you can see the device sign-in status.

Procedure

1. Sign in to the [Azure Active Directory admin center](#) as an admin.
2. Go to **Azure Active Directory > Monitoring > Sign-in logs**.

Download

Export Data Settings

Troubleshoot

Refresh

Columns

Got feedback?

This view will be soon replaced with a view that includes refresh tokens and application sign-ins. Try out our new sign-ins preview. →

9/22/2022, 9:57:23 AM	232f2d4d-c652-4bfe-9...	vcs01 Yealink	Office 365 Exchange O...	Failure	46.101.140.131	Frankfurt Am Main, He...	Not Applied	Single-factor authentic...
9/22/2022, 9:57:00 AM	0f46549b-d53a-4ff2-a...	vcs01 Yealink	Office 365 Exchange O...	Failure	46.101.140.131	Frankfurt Am Main, He...	Not Applied	Single-factor authentic...
9/22/2022, 9:56:59 AM	08bba69f-376a-4409-8...	vcs01 Yealink	Office 365 Exchange O...	Failure	46.101.140.131	Frankfurt Am Main, He...	Not Applied	Single-factor authentic...
9/22/2022, 9:56:58 AM	1ab86cbd-1d15-4e26-...	vcs01 Yealink	Office 365 Exchange O...	Failure	46.101.140.131	Frankfurt Am Main, He...	Not Applied	Single-factor authentic...
9/22/2022, 9:56:22 AM	dbffc97b-4dd4-4043-b...	Peter Parker	Azure Portal	Success	117.28.234.43	Fuzhou, Fujian, CN	Not Applied	Single-factor authentic...
9/22/2022, 9:56:18 AM	b0089bce-04c8-460b-...	ParkHae Jin	Office 365 Exchange O...	Success	170.114.10.202	San Jose, California, US	Not Applied	Single-factor authentic...
9/22/2022, 9:56:15 AM	307eb0ba-f7ce-431d-9...	vcs01 Yealink	Office 365 Exchange O...	Failure	46.101.140.131	Frankfurt Am Main, He...	Not Applied	Single-factor authentic...
9/22/2022, 9:55:38 AM	6f74519e-f1f6-4782-ae...	Gao Sense	Microsoft Authenticati...	Success	117.28.234.43	Fuzhou, Fujian, CN	Not Applied	Single-factor authentic...
9/22/2022, 9:55:09 AM	cec73cbe-589f-4f92-a...	MiMi Pan	Microsoft Authenticati...	Success	117.28.234.43	Fuzhou, Fujian, CN	Not Applied	Single-factor authentic...
9/22/2022, 9:54:56 AM	3afe47f3-ec85-482a-8...	MiMi Pan	Microsoft Authenticati...	Failure	117.28.234.43	Fuzhou, Fujian, CN	Not Applied	Single-factor authentic...
9/22/2022, 9:53:22 AM	69bf7fa9-1182-40dd-8...	Peter Parker	Microsoft Authenticati...	Success	117.28.234.43	Fuzhou, Fujian, CN	Not Applied	Single-factor authentic...
9/22/2022, 9:53:19 AM	6df55d07-c45b-449c-a...	Peter Parker	Microsoft Authenticati...	Failure	117.28.234.43	Fuzhou, Fujian, CN	Not Applied	Single-factor authentic...
9/22/2022, 9:53:11 AM	65b1827b-7a06-4ade-...	Zoey	Microsoft Teams Web ...	Interrupted	117.28.234.43	Fuzhou, Fujian, CN	Not Applied	Single-factor authentic...
9/22/2022, 9:52:27 AM	d9fe933d-1ad3-45a8-...	lh12	Microsoft Teams	Success	117.28.234.43	Fuzhou, Fujian, CN	Not Applied	Single-factor authentic...
9/22/2022, 9:52:00 AM	0f46549b-d53a-4ff2-a...	Wang Siri	Microsoft Authenticati...	Success	117.28.234.43	Fuzhou, Fujian, CN	Not Applied	Single-factor authentic...

3. Click the log to see more detailed information. For example, check the sign-in error code to find out

why a user failed to sign in.

Dashboard > Yealink

Yealink | Sign-in logs

Azure Active Directory

Download Export Data Settings Troubleshoot Refresh Columns

This view will be soon replaced with a view that includes refresh tokens and application sign-ins.1

9/22/2022, 9:57:23 AM	232f2d4d-c652-4bfe-9...	vcs01 Yealink	Office 365 Exch
9/22/2022, 9:57:00 AM	0f46549b-d53a-4ff2-a...	vcs01 Yealink	Office 365 Exch
9/22/2022, 9:56:59 AM	08bba69f-376a-4409-8...	vcs01 Yealink	Office 365 Exch
9/22/2022, 9:56:58 AM	1ab86cbd-1d15-4e26-...	vcs01 Yealink	Office 365 Exch
9/22/2022, 9:56:22 AM	dbffc97b-4dd4-4043-b...	Peter Parker	Azure Portal
9/22/2022, 9:56:18 AM	b0089bce-04c8-460b-...	ParkHae Jin	Office 365 Exch
9/22/2022, 9:56:15 AM	307eb0ba-f7ce-431d-9...	vcs01 Yealink	Office 365 Exch
9/22/2022, 9:55:38 AM	6f74519e-f1f6-4782-ae...	Gao Sense	Microsoft Auth
9/22/2022, 9:55:09 AM	cec73cbe-589f-4f92-a...	MiMi Pan	Microsoft Auth
9/22/2022, 9:54:56 AM	3afe47f3-ec85-482a-8...	MiMi Pan	Microsoft Auth
9/22/2022, 9:53:22 AM	69bf7fa9-1182-40dd-8...	Peter Parker	Microsoft Auth
9/22/2022, 9:53:19 AM	6df55d07-c45b-449c-a...	Peter Parker	Microsoft Auth
9/22/2022, 9:53:11 AM	65b1827b-7a06-4ade-...	Zoezy	Microsoft Team
9/22/2022, 9:52:27 AM	d9fe933d-1ad3-45a8-...	lh12	Microsoft Team
9/22/2022, 9:52:00 AM	0f46549b-d53a-4ff2-a...	Wang Siri	Microsoft Auth
9/22/2022, 9:51:41 AM	2f4965ec-3fc8-46d7-b...	Wang Siri	Microsoft Auth
9/22/2022, 9:51:34 AM	12e4727d-cba1-4fbc-b...	Peter Parker	Azure Portal
9/22/2022, 9:51:24 AM	cea8ee51-e6cd-4bfe-b...	Wang Siri	Microsoft Auth
9/22/2022, 9:51:00 AM	bbd14cd1-06d1-4a91-...	vcs01 Yealink	Office 365 Exch
9/22/2022, 9:50:22 AM	59931d25-b8d2-4a62-...	Wang Siri	Microsoft Team
9/22/2022, 9:50:21 AM	d4d34033-35d5-423e-...	Wang Siri	Microsoft Team
9/22/2022, 9:49:42 AM	02d7684f-c40f-46b8-b...	vcs01 Yealink	Office 365 Exch

Activity Details: Sign-ins

Basic info Location Device info Authentication Details Conditional Access Report-only

Date 9/22/2022, 9:51:41 AM

Request ID 2f4965ec-3fc8-46d7-b664-d29485bc0f01

Correlation ID 83f4f75a-471e-41cc-8fd7-66c753c1b2b9

Authentication requirement Single-factor authentication

Status Failure

Continuous access evaluation No

Sign-in error code 50126

Failure reason Error validating credentials due to invalid username or password.

Additional Details The user didn't enter the right credentials. It's expected to see some number of these errors in your logs due to users making mistakes.

Troubleshoot Event Follow these steps:
[Launch the Sign-in Diagnostic.](#)
1. Review the diagnosis and act on suggested fixes.

User Wang Siri

Username test01@yealink7.onmicrosoft.com

User ID 53732d9e-d85e-4d40-93cd-61baf6f1f3c6

Sign-in identifier test01@yealink7.onmicrosoft.com

User type Member

Cross tenant access type None

Application Microsoft Authentication Broker

Application ID 29d9ed98-a469-4536-ade2-f981bc1d605e

Resource Device Registration Service

Resource ID 01cb2876-7ebd-4aa4-9cc9-d28bd4d359a9

Resource tenant ID da574a7f-d308-4fe7-93d7-f055275b863d

Home tenant ID da574a7f-d308-4fe7-93d7-f055275b863d

5. For other activity details, see the Microsoft's doc on [Sign-in logs in Azure Active Directory](#).

Enroll Devices to Intune

Generally, Yealink Teams phone has pre-installed the Company Portal app.

Therefore, the devices of Intune-licensed users will be enrolled on Intune automatically when they sign in to their Teams account on their devices.

For more information about Microsoft Intune, refer to [Microsoft Intune Documentation](#).

Manage Devices on Teams Admin Center

After users sign in to Teams accounts on their devices, the devices are connected to the Teams admin center. You can manage them, for example, by updating devices remotely or downloading device logs.

Update Devices Remotely on Teams Admin Center

With the Microsoft Teams admin center, you can update your Teams phones.

You can update the following for your device on the Teams admin center:

- Teams app and teams admin agent
- Company portal app
- OEM agent app
- Device firmware

NOTE

You cannot select the desired firmware version to update. If you want to update the device to the desired firmware, you update it from the web browser.

Automatic Update

Procedure

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Go to **Teams Devices > Phones**.
3. Select one or more devices and then select **Update**.

✓	Display name	Username	Device name	Health status	Manufacturer	Model	IP address	Tags
	Xiao nana	test03@yealink7.onmicrosoft.com	yealink-vp59 515901812000041	Non-urgent	yealink	vp59	10.50.69.130	--
✓	Xiao nana	test03@yealink7.onmicrosoft.com	yealink-mp54 301198d070000410	Non-urgent	yealink	mp54	10.50.67.14	--
✓	Xiao nana	test03@yealink7.onmicrosoft.com	yealink-vp59 803050b080001348	Offline	yealink	vp59	10.50.151.25	--
	Xiao nana	test03@yealink7.onmicrosoft.com	yealink-t58a 8158117057000890	Offline	yealink	t58a	10.81.56.193	--
	Xiao nana	test03@yealink7.onmicrosoft.com	yealink-t58a 80:5ec0:31:96:88	Offline	yealink	t58a	10.81.20.29	--

4. Select one of the following:
 - **As soon as available:** Second-newest device firmware update is applied on the first weekend after the latest update is released.
 - **Defer 30 days:** Second-newest device firmware update is applied 30 days after the latest update is released.

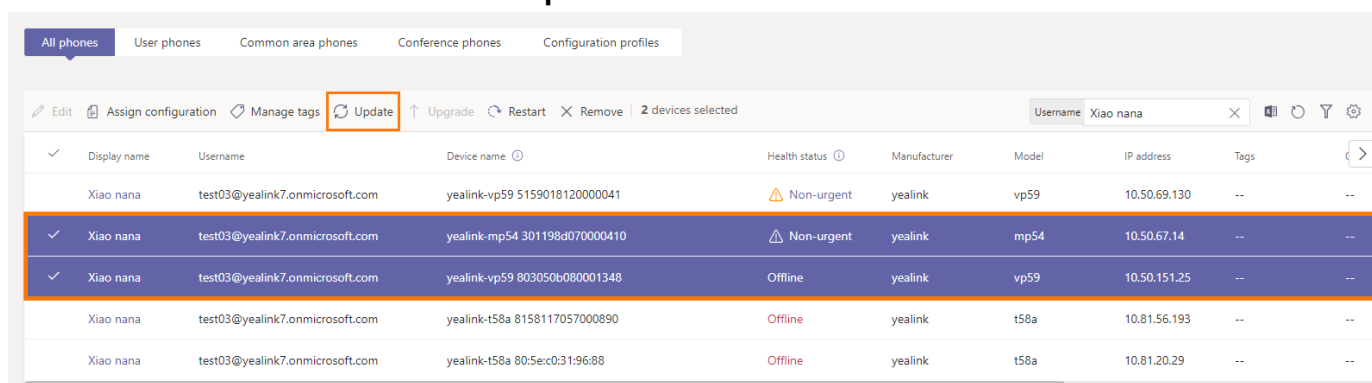
- **Defer 90 days:** Second-newest device firmware update is applied 90 days after the latest update is released.

5. Select **Update**.

Manual Update

Procedure

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Navigate **Teams Devices > Phones**.
3. Select one or more devices and select **Update**.



All phones									
User phones									
Common area phones									
Conference phones									
Configuration profiles									
Edit Assign configuration Manage tags Update Upgrade Restart Remove 2 devices selected Username: Xiao nana									
✓	Display name	Username	Device name	Health status	Manufacturer	Model	IP address	Tags	
	Xiao nana	test03@yealink7.onmicrosoft.com	yealink-vp59 5159018120000041	Non-urgent	yealink	vp59	10.50.69.130	--	--
✓	Xiao nana	test03@yealink7.onmicrosoft.com	yealink-mp54 301198d070000410	Non-urgent	yealink	mp54	10.50.67.14	--	--
✓	Xiao nana	test03@yealink7.onmicrosoft.com	yealink-vp59 803050b080001348	Offline	yealink	vp59	10.50.151.25	--	--
	Xiao nana	test03@yealink7.onmicrosoft.com	yealink-t58a 8158117057000890	Offline	yealink	t58a	10.81.56.193	--	--
	Xiao nana	test03@yealink7.onmicrosoft.com	yealink-t58a 80:5ec0:31:96:88	Offline	yealink	t58a	10.81.20.29	--	--

4. **Optional:** Select **Schedule** if you want to schedule the update for a future date and time. The updates are applied at the date and time in the timezone selected in **Timezone**.
5. Select the available firmware or apps you want to update and click **Update**.
 - If you select a single device:

Update status

yealink-mp54 301198d070000410

Firmware auto-update 

Manual updates 

Schedule  Off

Software component

☒ **Firmware**

Current version

122.15.0.80

New version

122.15.0.91

Published on

Jul 29, 2022, 9:20 PM

Software component

☒ **Teams app**

Current version

1449/1.0.94.2022072801

New version

1449/1.0.94.2022082401

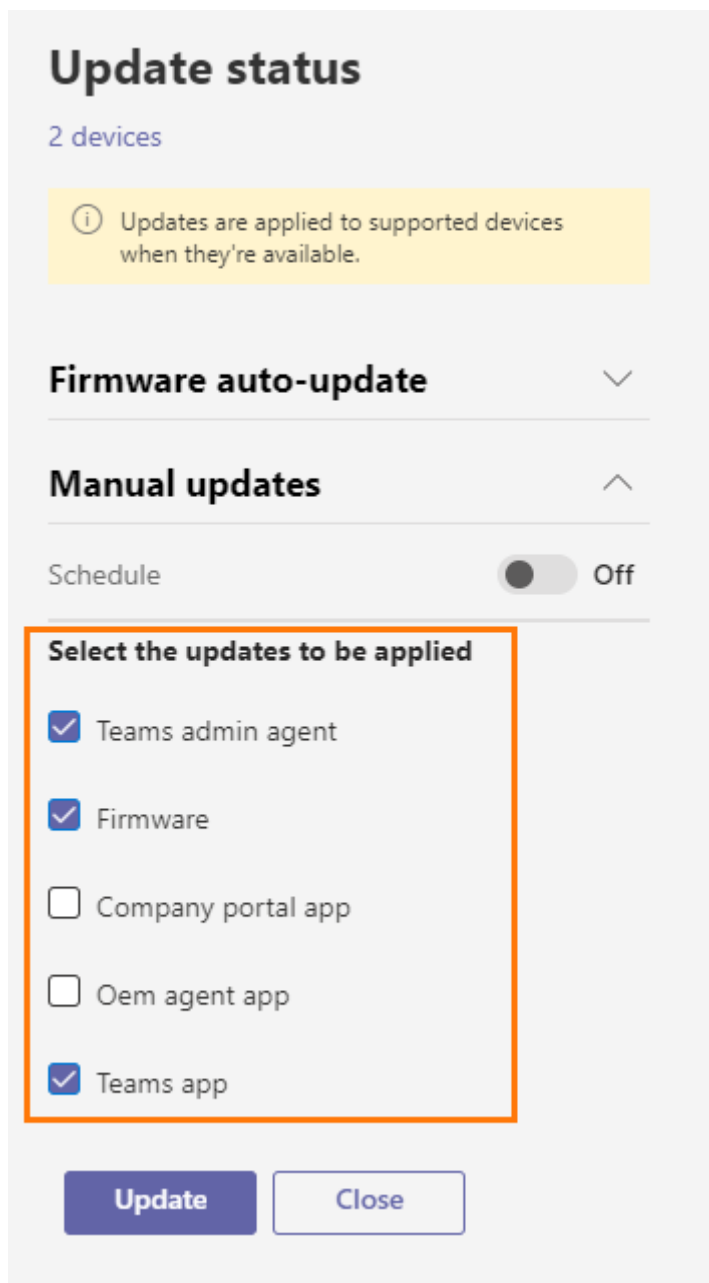
Published on

Aug 29, 2022, 8:30 PM

Update

Close

- If you select multiple devices:

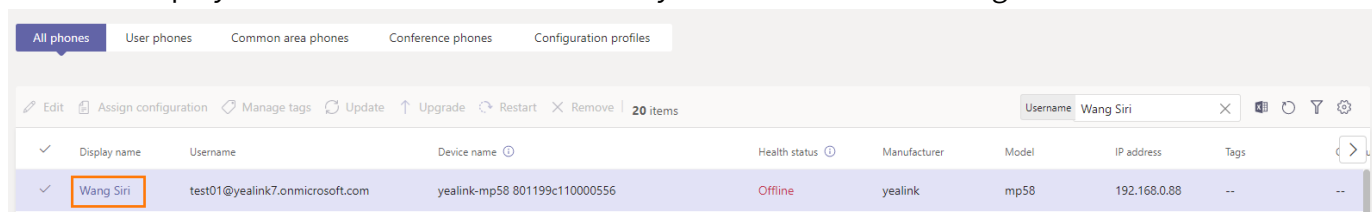


Download Device Logs on Teams Admin Center

You can download a copy of a device's diagnostic log files if requested to do so by Microsoft support.

Procedure

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Go to **Teams Devices > Phones**.
3. Click the display name of the device from which you want to download logs.



4. Select **Download device logs**. It can take several minutes for device logs to become available.

Wang Siri
yealink mp58

Health status
Offline
Offline since
Aug 26, 2022, 4:18 AM
Device name
yealink-mp58 801199c11000...
Username
test01@yealink7.onmicrosof...

7-DAY QUALITY

7-DAY ACTIVITY

21 Meetings
173 Calls

Health Details Activity History

5. Select the **History** tab, then click **Download** to download the log file under the **Diagnostics file** column.

6. If the diagnostic log files are available to download, the status will change to "Successful".

History

✓	Action	Status	Scheduled at	Modified on	Diagnostics file	Initiated by
	DeviceDiagnostics	Successful	-	Sep 19, 2022, 6:59 PM	Download	Peter Parker

Use Configuration Files on Teams Admin Center

Use configuration profiles to manage settings and features for different Teams phones in your organization.

Add a Configuration File

Procedure

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Go to **Teams Devices > Phones > Configuration profiles > Add**.

Teams devices

Store

Teams Rooms on Windo...

Teams Rooms on Android

Surface Hubs

Panels

Phones

Displays

All phones User phones Common area phones Conference phones Configuration profiles

+ Add Edit Assigned devices Delete 16 items

✓	Name	Description	Modified by	Modified on
	hyt-test		Peter Parker	Aug 25, 2022, 3:09 PM
	10.50.70.69		Peter Parker	Aug 30, 2022, 8:41 AM
	Phone lock test		Peter Parker	Aug 22, 2022, 4:17 PM

3. Enter a name for the profile and optionally add a friendly description.
4. Specify the settings you want for the profile, and then click **Save**.

For Yealink MP series

MP58, MP56, MP54, CP965

General

Device lock ☒ On

Timeout 30 seconds

Device lock PIN 123456

Language Chinese (Simplified, PRC)

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

Date format DD/MM/YYYY

Time format 12 Hours (AM/PM)

Calling settings

Advanced calling ☐ Off

ⓘ This setting may not be applicable if the device isn't updated.

6. The newly created configuration profile is displayed in the list of profiles.

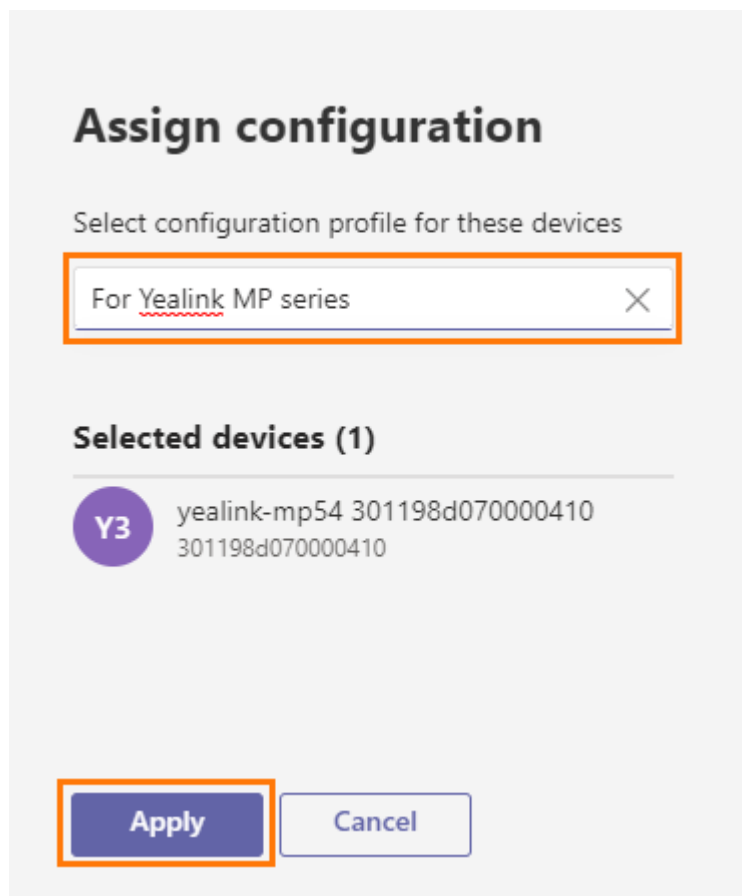
Assign Configuration File to Devices

Procedure

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Go to **Teams Devices > Phones**.
3. Select one or more devices and click **Assign configuration**.

All phones User phones Common area phones Conference phones Configuration profiles								
Edit Assign configuration Manage tags Update Upgrade Restart Remove 1 device selected Username: Xiao nana								
✓	Display name	Username	Device name ⓘ	Health status ⓘ	Manufacturer	Model	IP address	Tags
	Xiao nana	test03@yealink7.onmicrosoft.com	yealink-vp59 5159018120000041	⚠ Non-urgent	yealink	vp59	10.50.69.130	--
✓	Xiao nana	test03@yealink7.onmicrosoft.com	yealink-mp54 301198d070000410	⚠ Non-urgent	yealink	mp54	10.50.67.14	--

4. Search for a configuration profile to assign to the selected devices and click **Apply**.



Assign configuration

Select configuration profile for these devices

For Yealink MP series

Selected devices (1)

Y3 yealink-mp54 301198d070000410
301198d070000410

Apply Cancel

6. For the devices to which you applied the configuration policy, the **Action** column displays **Config Update** and the **Configuration profile** column displays the configuration profile name.

Restart Devices on Teams Admin Center

You can directly restart devices on the Teams admin center.

Procedure

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Go to **Teams Devices > Phones**.
3. Select one or more devices, and click **Update**.
4. The device will restart automatically and immediately.

Remove Devices from Teams Admin Center

When you remove a device, all the associated data will be removed. Any user or resource accounts must be signed out of any device before it's removed. If this is the only device the account is used for, delete it from the [Microsoft 365 admin center](#).

Procedure

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Go to **Teams Devices > Phones**.
3. Select one or more devices, and click **Remove**.

Provision Device on Teams Admin Center

You can remotely provision and sign in to a Teams Android device.

Device Firmware Requirements

Supported device models:

Device model	Firmware version
Yealink VP59	91.15.0.58 or later
Yealink MP56/MP54/MP58	122.15.0.36 or later
Yealink MP52	145.15.0.4 or later
Yealink CP965	143.15.0.7 or later
Yealink MP52 E2/MP54 E2/MP56 E2/MP58 E2	176.15.0.16 or later

Add Device MAC Addresses

Procedure

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Expand **Teams devices** and select **Phones**.
3. Select **Provision new device** from the **Actions** tab.

You can either manually add the MAC address or upload a file to add in batch in the **Provision new devices** window.

- **Manually add a device MAC address:**
 - a. Under the Waiting on activation tab, click **Add**.
 - b. Enter the MAC address, set the location, and click **Save**.

Provision devices

Add one or more MAC addresses or hardware IDs for your devices to start provisioning them. When you add your devices, they can be remotely signed in and then deployed in your organization. [Learn more](#)

Provisioning summary

6 MAC addresses or hardware IDs | 2 Verification codes expired | 2 Waiting to sign in

New device provisioning steps

1. Manually add or upload a file with new MAC addresses or hardware IDs.
2. Generate a verification code.
3. Export the verification codes for your devices.

Waiting on activation | Waiting for sign in

1 + Add Upload Generate verification code + Edit Delete 4 items

ID	ID type	Location	Verification code
02-10-00-04-00-05:999	Hardware ID (analog)	India	--
02-10-00-04-00-05	MAC address	US	--
80-5e-c0-60-3b-e3	MAC address	--	Expired
00-02-91-c6-d3-e8	MAC address	--	Expired

Add MAC addresses or hardware IDs

ID type: MAC address | Enter MAC address: 80-5E-C0-DA-A4-52

Location: Xiamen, China

4 Save Cancel

- **Upload a file to add a device MAC address:**
 - a. From the **Waiting on activation** tab, select **Upload**.
 - b. Download the file template.
 - c. Enter the MAC ID and location, and then save the file.
 - d. Click **Select a file** and then select **Upload**.

Pre-Configure Devices

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

Procedure

1. From the **Waiting on activation** tab, select an existing MAC ID and click **Generate verification code**.
2. A password is created for the MAC address and is shown in the **Verification Code** column.

Provision devices

Add one or more MAC addresses or hardware IDs for your devices to start provisioning them. When you add your devices, they can be remotely signed in and then deployed in your organization. [Learn more](#)

Provisioning summary

7	2	2
MAC addresses or hardware IDs	Verification codes expired	Waiting to sign in

New device provisioning steps

1. Manually add or upload a file with new MAC addresses or hardware IDs.
2. Generate a verification code.
3. Export the verification codes for your devices.

Waiting on activation | Waiting for sign in

+ Add | Upload | **Generate verification code** | Edit | Delete | 1 item selected

Search by MAC address or hardw...

ID	ID type	Location	Verification code
✓ 80-5e-c0-da-a4-52	MAC address	Xiamen, China	362671
02-10-00-04-00-05:999	Hardware ID (analog)	India	--
02-10-00-04-00-05	MAC address	US	--
80-5e-c0-60-3b-e3	MAC address	--	Expired
00-02-91-c6-d3-e8	MAC address	--	Expired

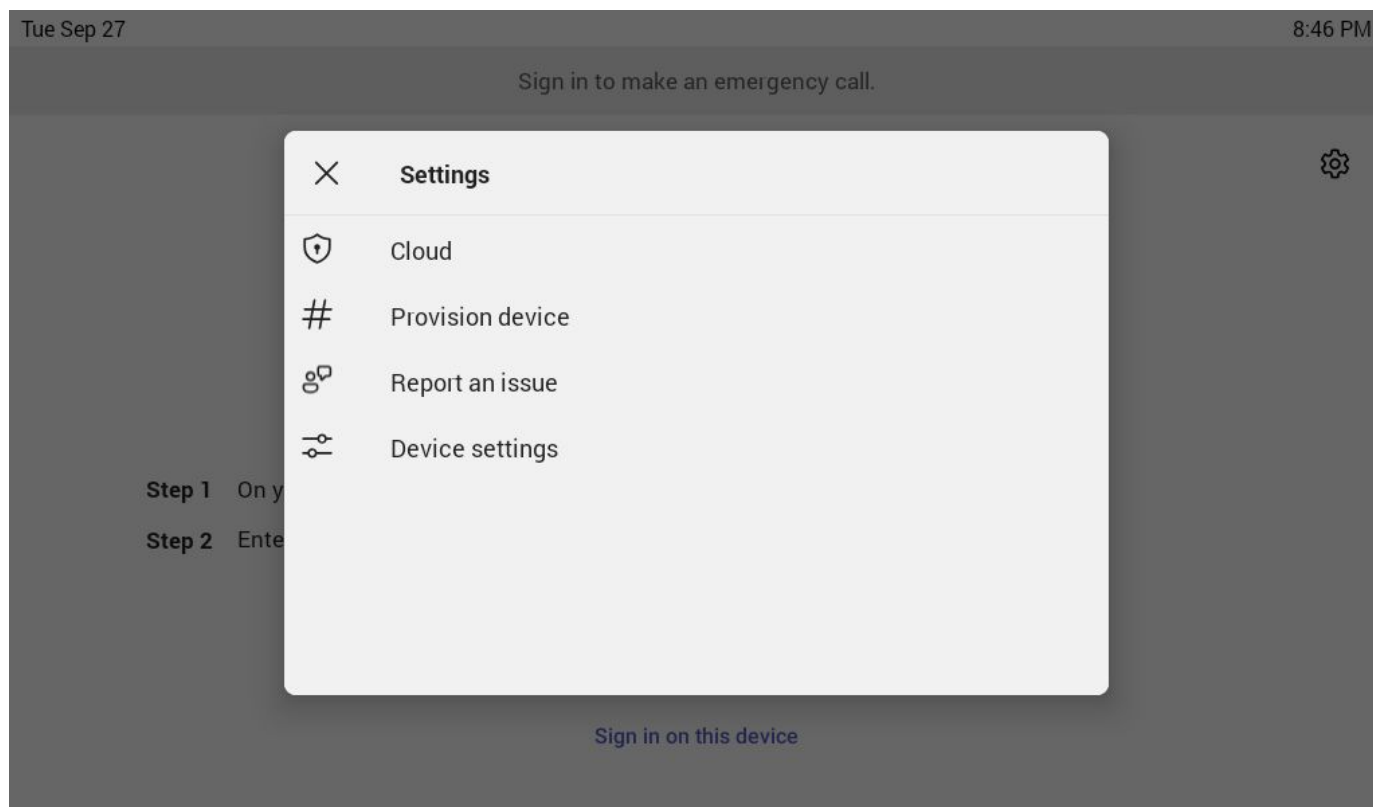
4. You can also provide the list of MAC IDs and verification codes to the field technicians. You can export the detail directly in a file and share the file with the technician who is doing the actual installation work.

Provision Devices

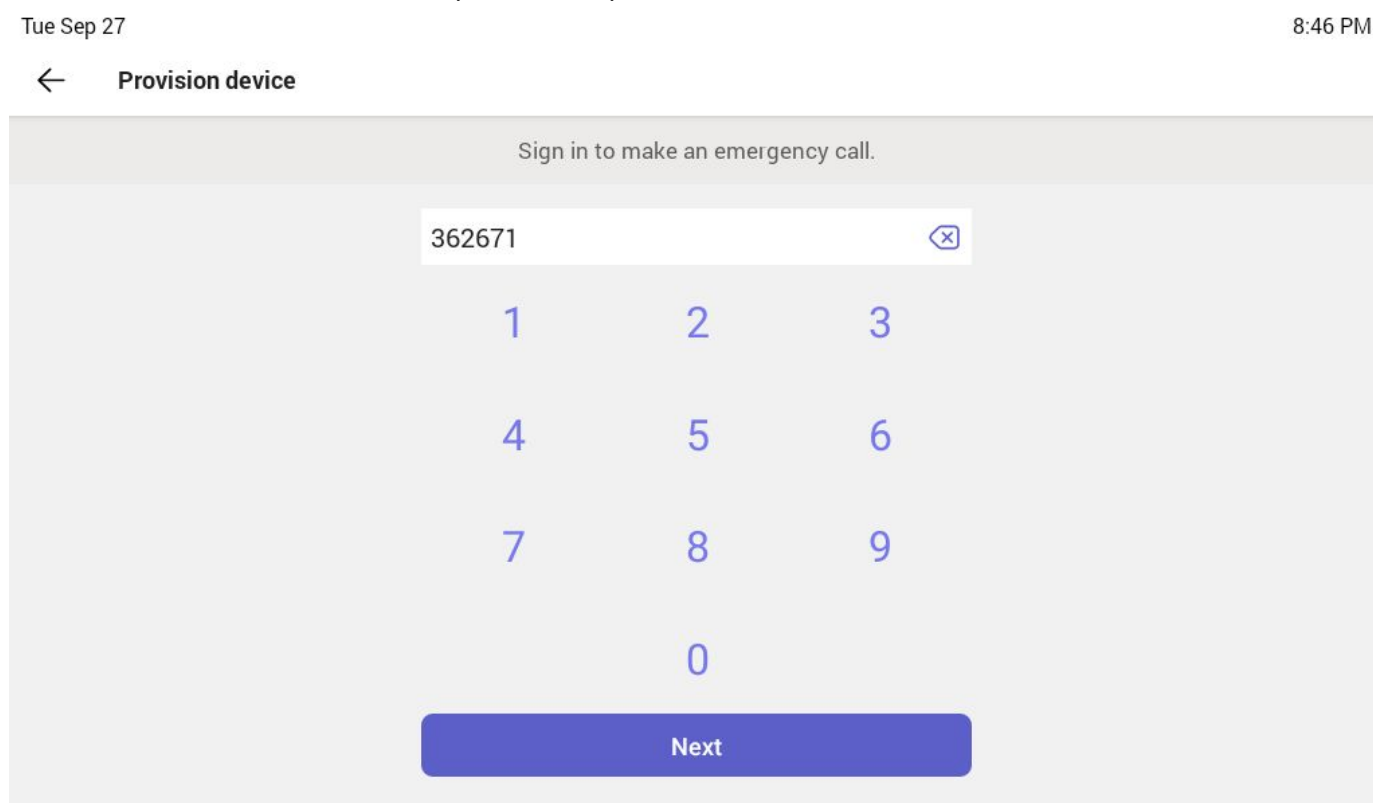
When the device is powered on and connected to the network, you can provision the device. These steps are completed on the Teams device.

Procedure

1. Click the **Settings** icon and select **Provision device** from the **Settings**.



2. Enter the verification code in the provided input field.



4. Once the device is provisioned successfully, the tenant name appears on the sign-in page.

Remote Sign In

Procedure

1. Select a device from the **Waiting for sign in** tab.

2. Follow the instructions in **Sign in a user**, and then select **Close**.

Update Firmware

Introduction

A Firmware update improves the functionality and features of your device. It can provide fixes to any performance issues that may occur.

Therefore, we recommend that you update the firmware of Teams phones to the latest version.

The following sections introduce how to update firmware from the phone's web user interface. If you want to update the firmware from the Teams Admin Center, see [Manage Devices on Teams Admin Center](#) for more information.

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

Step 1: Check the Firmware Version

Procedure

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > About .	Go to  > Settings > Device Settings > About .

2. You can see the detailed version information of the firmware and the Teams app.

← Device Settings	
 Reboot	IPv4 10.50.67.7
 About	License Status Eternal
 Upgrade	MAC 80:5E:C0:37:8B:95
 Mic-BT	Machine ID 5159018120000101
Admin only	Firmware 91.15.0.119
 Network	Partner APP Version 1.15.0.22111722
 Proxy	Company Portal Version 5.0.5484.0
 Debug	Teams Version 1449/1.0.94.2022110803
 Admin Password	Admin Agent Version 1.0.0.202209060820.product

Step 2: Download the Latest Device Firmware

1. Go to [Yealink Support](#).
2. Navigate to the device model you want (you can also search the desired device model by keyword search).
3. Click the **Firmware** tab and download the latest firmware version.

Yealink | Support Ticket Warranty Service License Knowledge Base Resource Center Prime Care Help Desk

Home > Microsoft/ZOOM/RingCentral/BlueJeans Devices > Teams Phones > VP59 Teams Video Phone

VP59 Teams Video Phone [subscribe](#)

Document **Firmware** Tool Video FAQ

Firmware

All

Firmware & Release Notes

Firmware & Release Notes (19)

Yealink VP59 Teams Video Phone Release Notes of Version 20	NEW	1.67MB	Download	2022-12-01
VP59_9.0-91.15.0.118	NEW	745.99MB	Download	2022-12-01
VP59_9.0-91.15.0.102		731.05MB	Download	2022-08-10
VP59_9.0-91.15.0.90		690.82MB	Download	2022-05-06
VP59_9.0-91.15.0.87		678.88MB	Download	2022-02-08
Yealink VP59 Teams Video Phone Release Notes of Version 17		1.03MB	Download	2022-03-01

5.

Step 3 (Option 1): Update via Web User Interface

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Upgrade > Upgrade Firmware > Browse.**
3. Select the latest firmware and click **Upload.**



Do not close and refresh the browser when upgrading firmware via the web user interface.

Yealink | MP58

- Status
- Network
- Features
- Settings
 - Preference
 - Time&Date
 - Upgrade**
 - Auto Provision
 - Configuration
 - Voice
 - Tones
 - Power Saving
 - Hybrid Mode
 - Security

Version ?

Firmware Version	122.15.0.91
Hardware Version	135.0.0.0.0.0.0
Company Portal Version	5.0.5484.0
Teams Version	1449/1.0.94.2022062103
Admin Agent Version	1.0.0.202205230848.product

Reset

Reset User Settings	Reset User Settings ?
Reset to Factory	Reset to Factory ?

Reboot

Reboot	Reboot ?
--------	----------

Upgrade

Check for Updates Check for Updates

Upgrade Firmware Browse Upload ?

Step 3 (Option 2): Update via Auto Provisioning

For enterprise administrators, you can update the firmware for multiple devices via auto provisioning.

Before you begin

You have downloaded the latest firmware for each device and placed the firmware file on the auto provisioning server.

! Do not unplug the network cables and power cables when upgrading firmware.

Parameter	Description	Permitted Values
static.firmware.url	It configures the access URL of the firmware file. If you change this parameter, the device will reboot to make the change take effect.	URL within 511 characters
over_the_air.u	It configures the access URL of the BTH58 handset firmware	URL within 511

rl.bth58	file.	characters
----------	-------	------------

```
static.firmware.url = https://10.50.60.70/firmwarefile  
over_the_air.url.bth58 = https://10.50.60.70/firmwarefile
```

Step 3 (Option 3): Update via Teams Admin Center

See [Manage Devices on Teams Admin Center](#) to update the firmware via the Teams Admin Center.

FAQ

Forgot the admin default password?

Generally, the admin default password is *admin*.

If you forgot the password, you can reset the phone to factory settings by pressing the pound key (#) and the star key (*) for about 6 seconds when the phone is idle.

If the default admin password is managed by your company administrator, please contact them.

How to convert the Teams firmware into a SIP/Zoom/VCS version?

See the following:

- [Convert between Teams and SIP Versions](#)
- [Convert between Teams and Zoom Versions](#)
- [Convert between Teams and VCS Versions](#)

Update to the Latest Teams App

You can update the Teams app of the MP Teams phone by the following methods:

- Update the Teams app on your MP Teams phone.
- Update the Teams app on the Teams admin center.

Step 1: Check the Teams App Version

Procedure

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the account avatar and go to Settings > Device Settings > About .	Go to  > Settings > Device Settings > About .

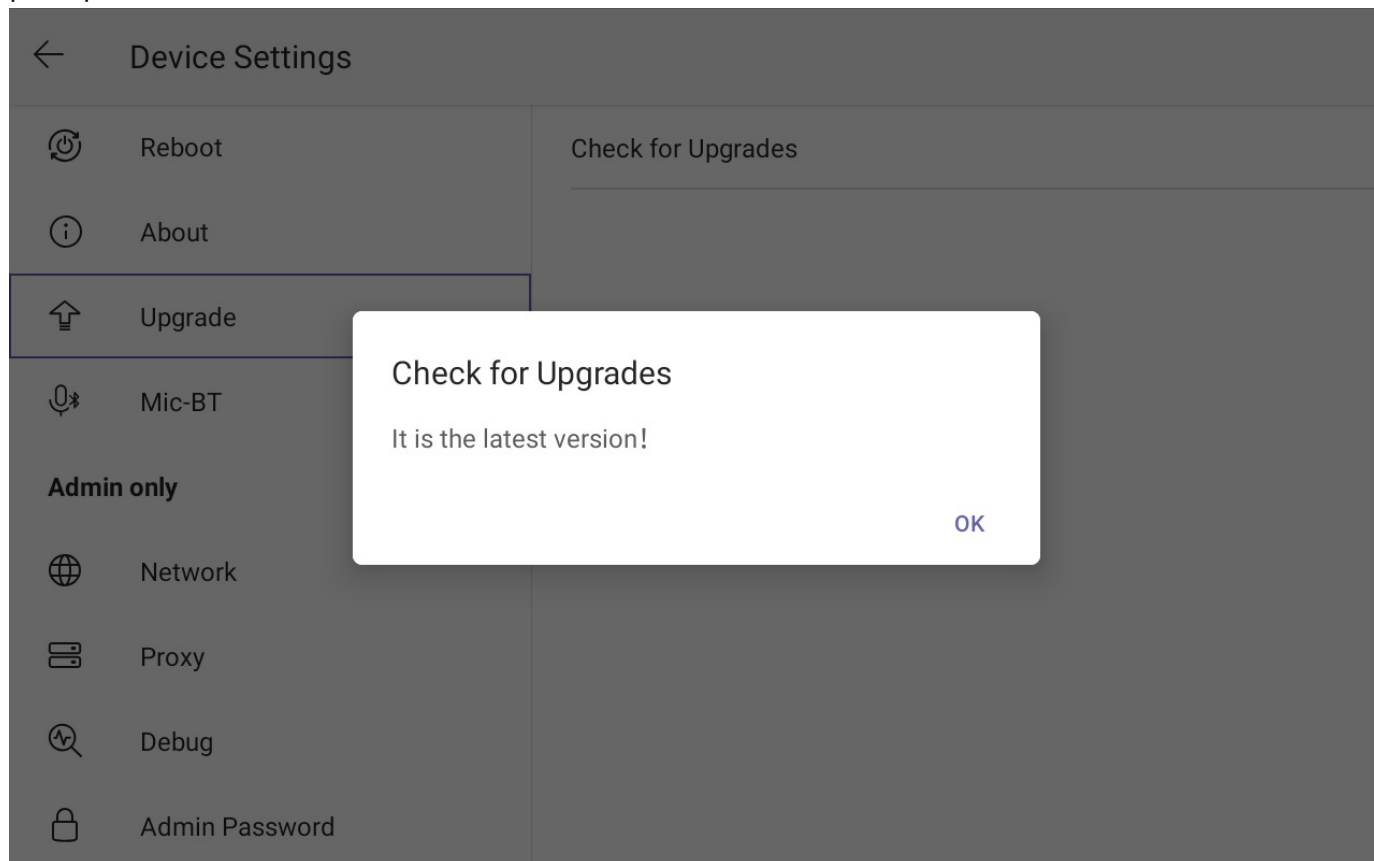
2. You can see the detailed version information of the firmware and the Teams app.

← Device Settings	
 Reboot	IPv4 10.50.67.7
 About	License Status Eternal
 Upgrade	MAC 80:5E:C0:37:8B:95
 Mic-BT	Machine ID 5159018120000101
Admin only	Firmware 91.15.0.119
 Network	Partner APP Version 1.15.0.22111722
 Proxy	Company Portal Version 5.0.5484.0
 Debug	Teams Version 1449/1.0.94.2022110803
 Admin Password	Admin Agent Version 1.0.0.202209060820.product

Step 2 (Optional): Update Teams App on Your MP

Teams Phone

3. On your MP Teams phone, go to **Settings > Device Settings > Upgrade > Check for Updates**.
4. If a new version is available, you can update it according to the on-screen prompts. Otherwise, it will prompt that it is the latest version.



Step 2 (Optional): Update the Teams App on the Teams Admin Center

See [Manage Devices on Teams Admin Center](#) to update your Teams app on Teams admin center.

Version Converting Introduction

You can also convert MP Teams phones into other versions, for example, SIP or Zoom versions, as listed below:

- To convert from the Teams version to other versions, you need to apply the device license of the target version.
- To convert from other versions to the Teams version, you need to apply for the Teams device license.

Device	Can be Converted To
VP59 (Teams version)	SIP, Zoom, VCS
MP58 (E2) (Teams version)	Zoom
MP56 (E2) (Teams version)	Zoom
MP55 E2 (Teams version)	/ (Only Teams version)
MP54 (E2) (Teams version)	Zoom
MP52 (E2) (Teams version)	/ (Only Teams version)
MP50 (Teams version)	/ (Only Teams version)
CP965 (Teams version)	SIP

💡 For MP5X E2, the conversion can be performed after the official release of the Zoom version.

Convert between Teams and VCS Versions

Available Devices

- VP59

! MP series do not support converting between VCS and Teams versions.

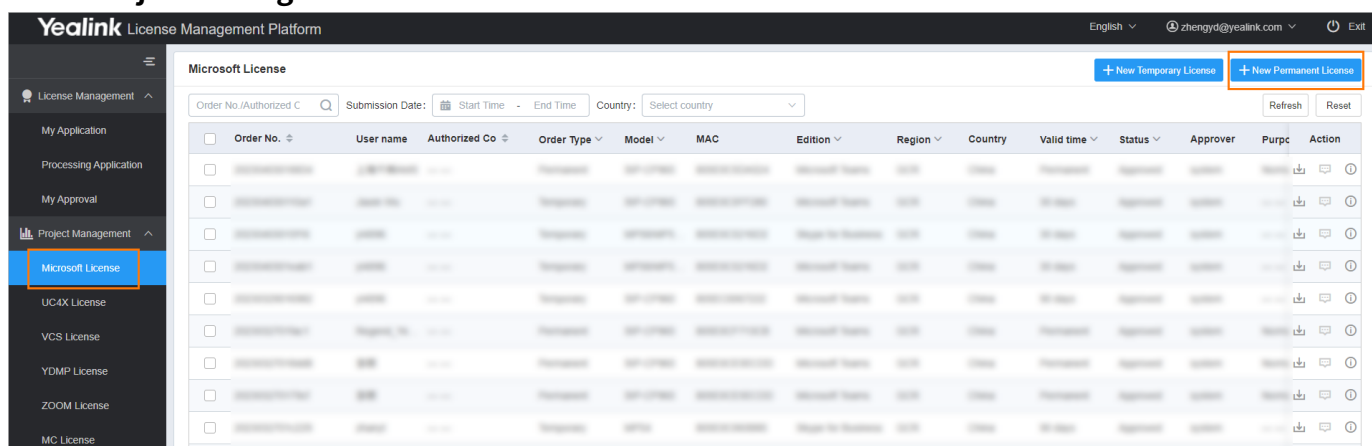
Upgrade from Teams to VCS Version

Step 1: Apply for a License for Unlocking

Before you begin

Make sure that you have signed up for the Yealink License Management Platform.

1. Go to page <https://license.yealink.com/manage/micro>.
2. Go to **Project Management > Microsoft License > New Permanent License**.



3. Set the parameters as shown below.

New Permanent License

Advanced

☒ Unlock License

* Purpose: Normal Delivery

* MAC: 8...5

* Edition: Microsoft Teams

* Model: VP59

* Valid time: Permanent

* Purpose: I want to convert from Teams to VCS edition.

OK Cancel

4. Click **OK** to submit. The system will approve and send your application to your reserved email address after some time.

! If any errors occur after clicking OK, take a screenshot of the error message and submit a ticket for consultation. Our technical support engineers will help you solve the problem.

5. Download the license file from the email attachment or the [Yealink License Application Platform](#).

6. Go to **License Management > My Application** on the platform to download your license.

Yealink License Management Platform

English | Aloys.gan@yealink.com | Administrator | Exit

License List | Device List

+ New Temporary License | + New Permanent License

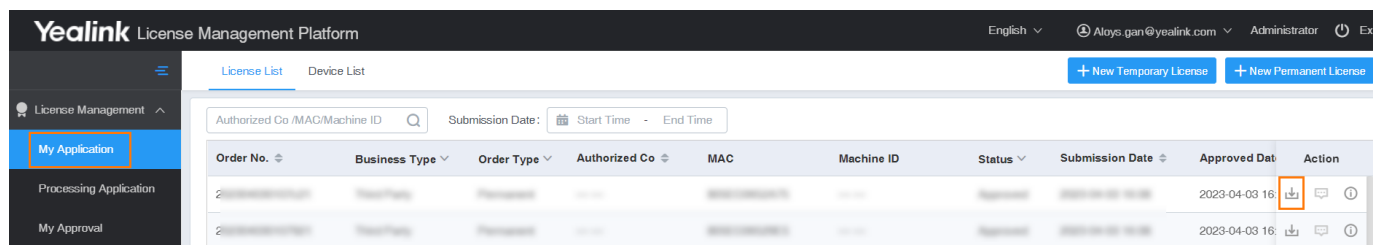
Authorized Co./MAC/Machine ID | Submission Date: Start Time - End Time

Order No.	Business Type	Order Type	Authorized Co.	MAC	Machine ID	Status	Submission Date	Approved Date	Action
2...	Team/Pro	Purchase	...	8...	...	Approved	2023-04-03 16:...	2023-04-03 16:...	Download Chat Info
2...	Team/Pro	Purchase	...	8...	...	Approved	2023-04-03 16:...	2023-04-03 16:...	Download Chat Info

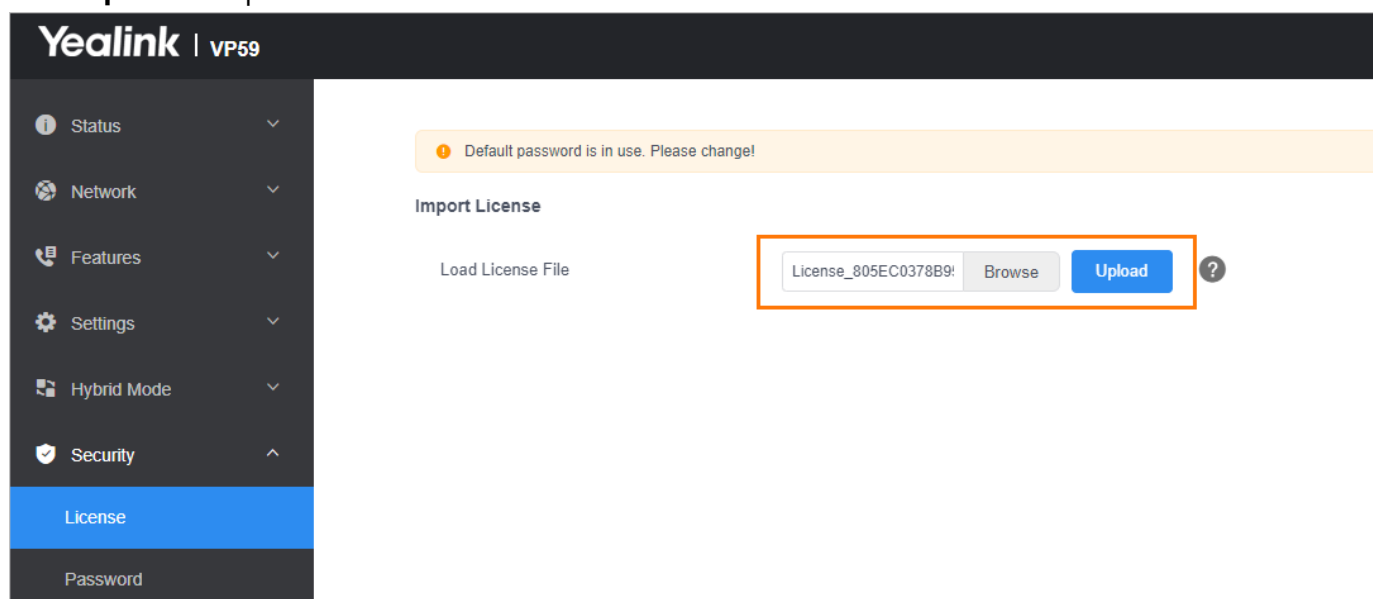
Step 2: Import the Unlocking License

1. Download the license file from the email attachment or the [Yealink License Application Platform](#).

2. Go to **License Management > My Application** on the platform to download your license.



2. [Log in to the phone web user interface as an admin.](#)
3. Go to **Security > License**.
4. Click **Browser** to select the license.
5. Click **Upload** to upload the license.



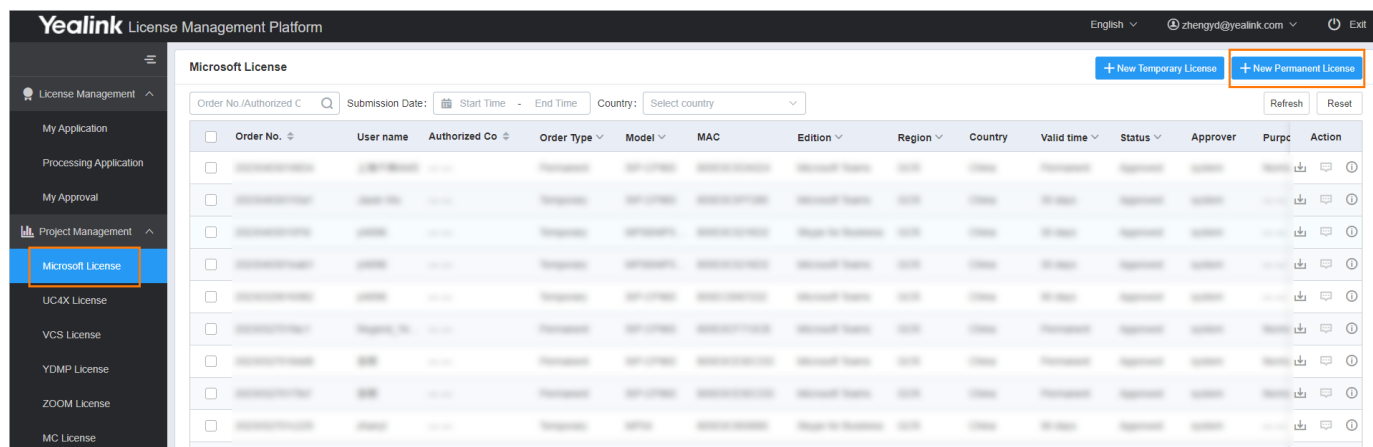
Step 3: Upgrade from Teams to VCS Firmware

1. Go to Yealink Support to download the latest device firmware.
2. [Log in to the phone web user interface as an admin.](#)
3. Go to **Settings > Upgrade > Upgrade Firmware > Browse**.
4. Select the latest firmware and click **Upload**.

Upgrade from VCS to Teams Version

Step 1: Apply for a Teams License

1. Go to page <https://license.yealink.com/manage/micro>.
2. Go to **Project Management > Microsoft License > New Permanent License**.



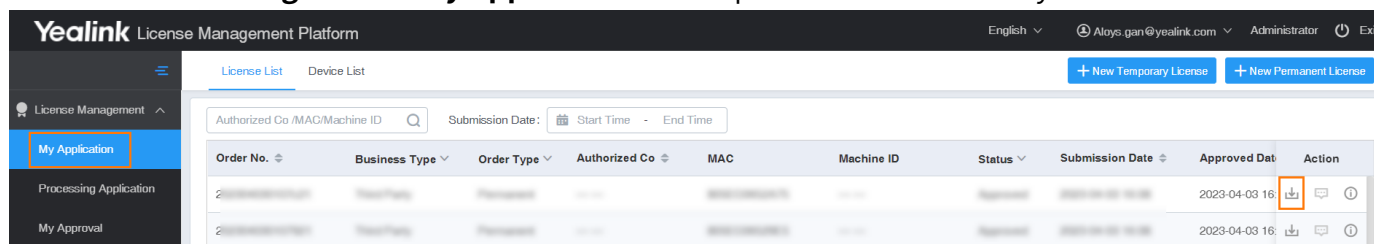
3. Set the parameters as shown below.

4. Click **OK** to submit. The system will approve and send your application to your reserved email address after some time.

! If any errors occur after clicking OK, take a screenshot of the error message and submit a ticket for consultation. Our technical support engineers will help you solve the problem.

5. Download the license file from the email attachment or the [Yealink License Application Platform](#).

6. Go to **License Management > My Application** on the platform to download your license.



Step 2: Upgrade from VCS to Teams Firmware

See [Upgrade from Teams to VCS Firmware](#) to import the Teams firmware.

Step 3: Import the Teams License

See [Import the Unlocking License](#) to import the Teams license.

Convert between Teams and Zoom Versions

Introduction

The phone cannot be used as both Teams and Zoom phones simultaneously. This is the strategy of Microsoft and Zoom.

There is no **license requirement** for converting Teams and Zoom versions. You can directly upgrade the device firmware to the desired version.

Available Devices

- VP59
- MP58 (E2)
- MP56 (E2)
- MP54 (E2)

Upgrade the Teams or Zoom Firmware

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Upgrade > Upgrade Firmware > Browse.**
3. Select the latest firmware and click **Upload.**



Do not close and refresh the browser when upgrading firmware via the web user interface.

Yealink | MP58

Status

Network

Features

Settings

Preference

Time&Date

Upgrade

Auto Provision

Configuration

Voice

Tones

Power Saving

Hybrid Mode

Security

Default password is in use. Please change!

Version

Firmware Version

122.15.0.91

Hardware Version

135.0.0.0.0.0.0

Company Portal Version

5.0.5484.0

Teams Version

1449/1.0.94.2022062103

Admin Agent Version

1.0.0.202205230848.product

Reset

Reset User Settings

Reset User Settings

Reset to Factory

Reset to Factory

Reboot

Reboot

Reboot

Upgrade

Check for Updates

Check for Updates

Upgrade Firmware

MP58(MP54,Teams_MF

Browse

Upload

Convert between Teams and SIP Versions

Available Devices

- VP59
- CP965



- MP series do not support converting between SIP and Teams versions.
- For CP965 running Android 12 or later, direct conversion from SIP to Teams is not supported. A transition firmware is required before upgrading to the Teams firmware. Please contact Yealink Support to obtain the transition firmware.

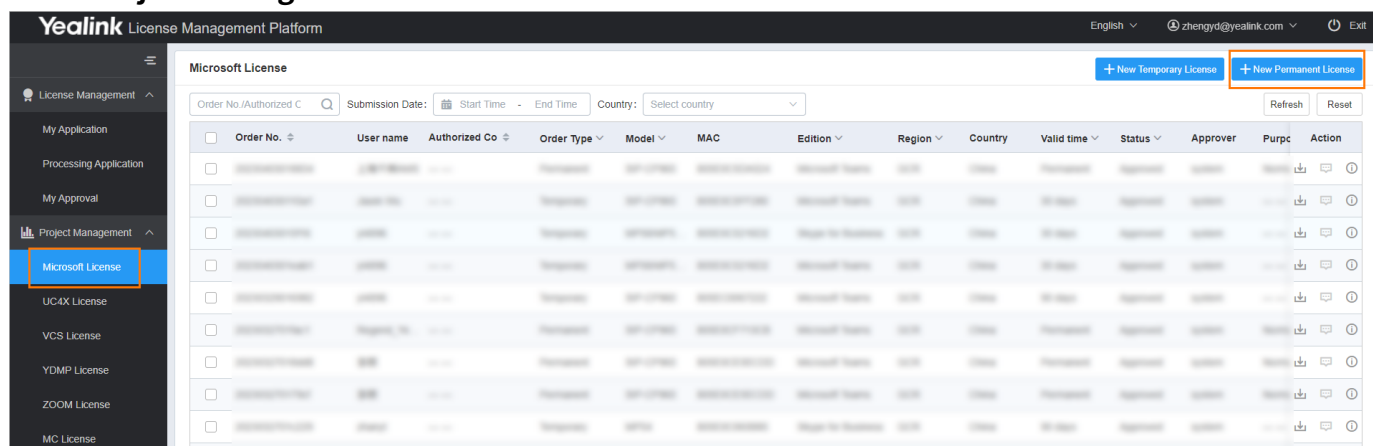
Upgrade from Teams to the SIP Version

Step 1: Apply for a License for Unlocking

Before you begin

Make sure that you have signed up for the Yealink License Management Platform.

1. Go to page <https://license.yealink.com/manage/micro>.
2. Go to **Project Management > Microsoft License > New Permanent License**.



3. Set the parameters as shown below.

New Permanent License

Advanced

☒ Unlock License

* Purpose: Normal Delivery

* MAC: 8...2

* Edition: Microsoft Teams

* Model: MP58/MP58-WH

* Valid time: Permanent

* Purpose: I want to convert Teams edition to SIP.

OK Cancel

4. Click **OK** to submit. The system will approve and send your application to your reserved email address after some time.

💡 If any errors occur after clicking OK, take a screenshot of the error message and submit a ticket for consultation. Our technical support engineers will help you solve the problem.

5. Download the license file from the email attachment or the [Yealink License Application Platform](#).
6. Go to **License Management > My Application** on the platform to download your license.

Yealink License Management Platform

English | Aloys.gan@yealink.com | Administrator | Exit

License List | Device List

+ New Temporary License | + New Permanent License

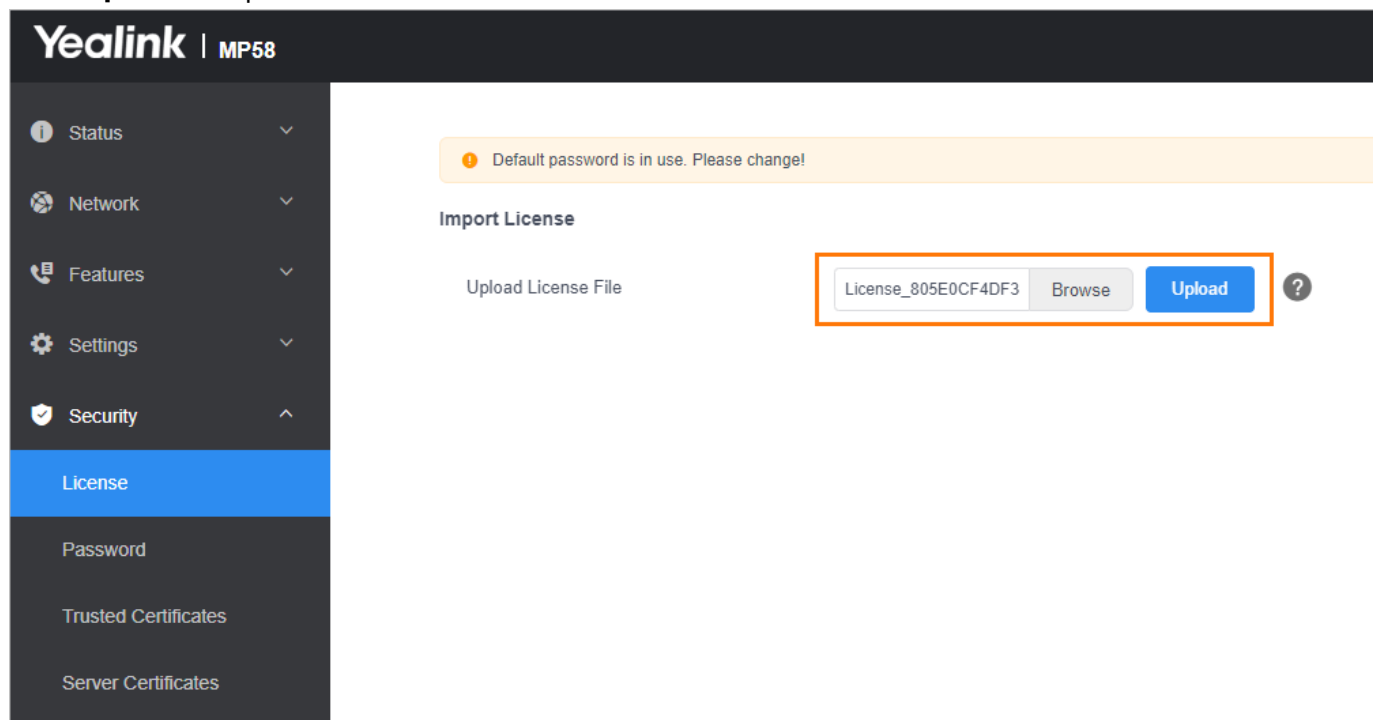
Authorized Co./MAC/Machine ID | Submission Date: Start Time - End Time

Order No.	Business Type	Order Type	Authorized Co.	MAC	Machine ID	Status	Submission Date	Approved Date	Action
2	TeamPhone	Permanent	...	...	...	Approved	2023-04-03 16:00	2023-04-03 16:00	Download Chat Help
2	TeamPhone	Permanent	...	...	...	Approved	2023-04-03 16:00	2023-04-03 16:00	Download Chat Help

Step 2: Import the Unlocking License

1. [Log in to the phone web user interface as an admin.](#)

2. Go to **Security** > **License**.
3. Click **Browser** to select the license.
4. Click **Upload** to upload the license.



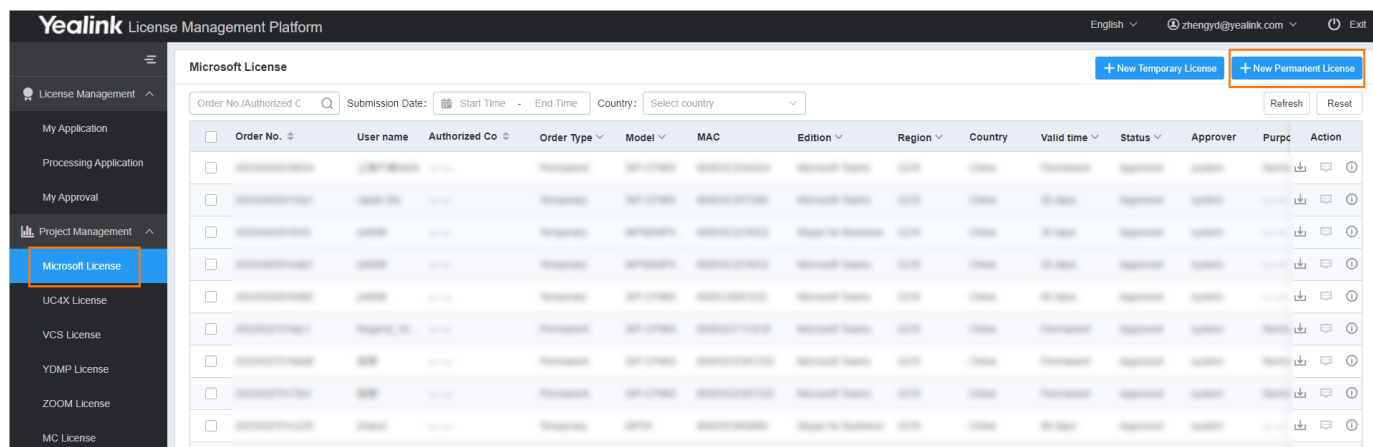
Step 3: Upgrade from Teams to SIP Firmware

1. Go to Yealink Support to download the latest device firmware.
2. [Log in to the phone web user interface as an admin.](#)
3. Go to **Settings** > **Upgrade** > **Upgrade Firmware** > **Browse**.
4. Select the latest firmware and click **Upload**.

Upgrade from SIP to Teams Version

Step 1: Apply for and Download a Teams License

1. Go to page <https://license.yealink.com/manage/micro>.
2. Go to **Project Management** > **Microsoft License** > **New Permanent License**.



3. Set the parameters as shown below.

New Permanent License

Advanced

☒ Unlock License

* Purpose: Normal Delivery

* MAC: E-52

* Edition: Microsoft Teams

* Model: MP58/MP58-WH

* Valid time: Permanent

Authorized Co: Please enter authorized company

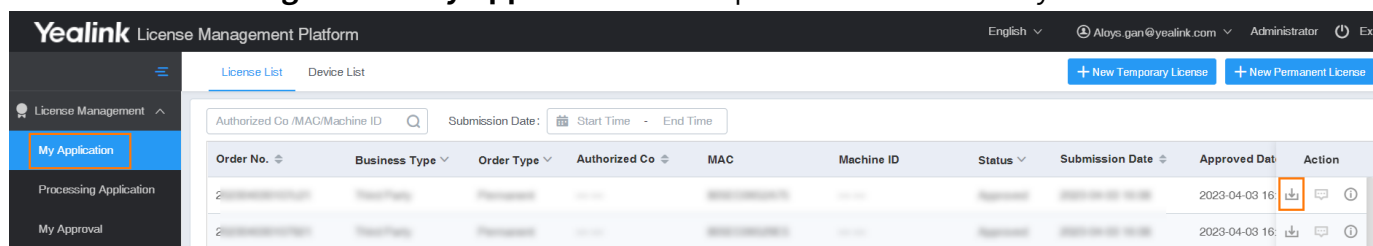
Email: test@yealink.com

OK Cancel

4. Click **OK** to submit. The system will approve and send your application to your reserved email address after some time.

! If any errors occur after clicking OK, take a screenshot of the error message and submit a ticket for consultation. Our technical support engineers will help you solve the problem.

5. Download the license file from the email attachment or the [Yealink License Application Platform](#).
6. Go to **License Management > My Application** on the platform to download your license.

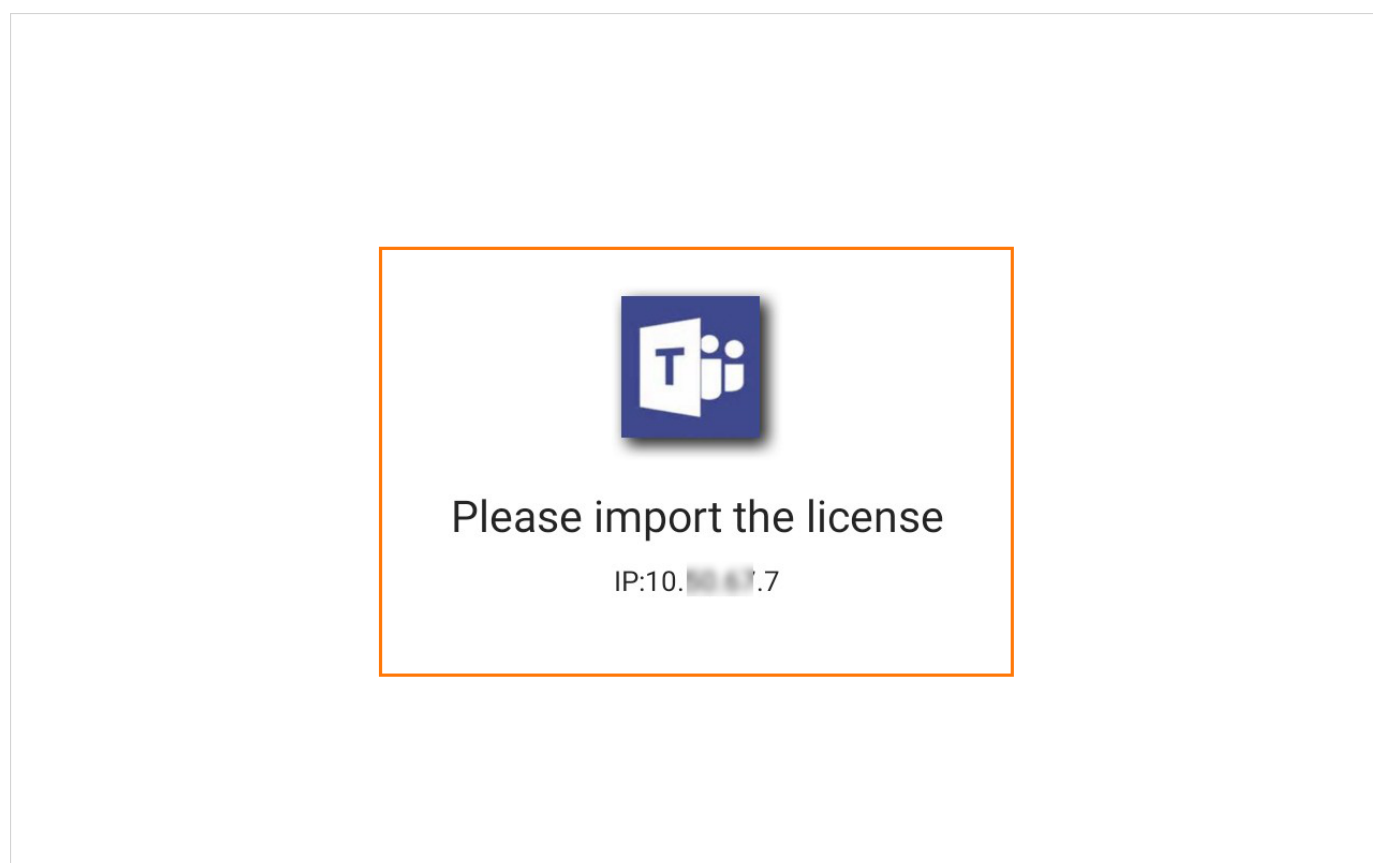


Step 2: Upgrade from SIP to Teams Firmware

See [Upgrade from Teams to SIP Firmware](#) to import the Teams firmware.

Step 3: Import the Teams License

After you upgrade the device from SIP to Teams firmware, the screen will prompt "Please import the license" and the device IP address as below:



See [Import the Unlocking License](#) to import the Teams license.

Take a Screenshot

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

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

Before capturing the phone's current screen, ensure that the IP address of the computer is included in the trusted IP address for Action URI on the phone. When you capture the screen display, the IP phone may prompt you to enter the user name and password of the administrator if the web browser does not remember the user name and password for the web user interface login.

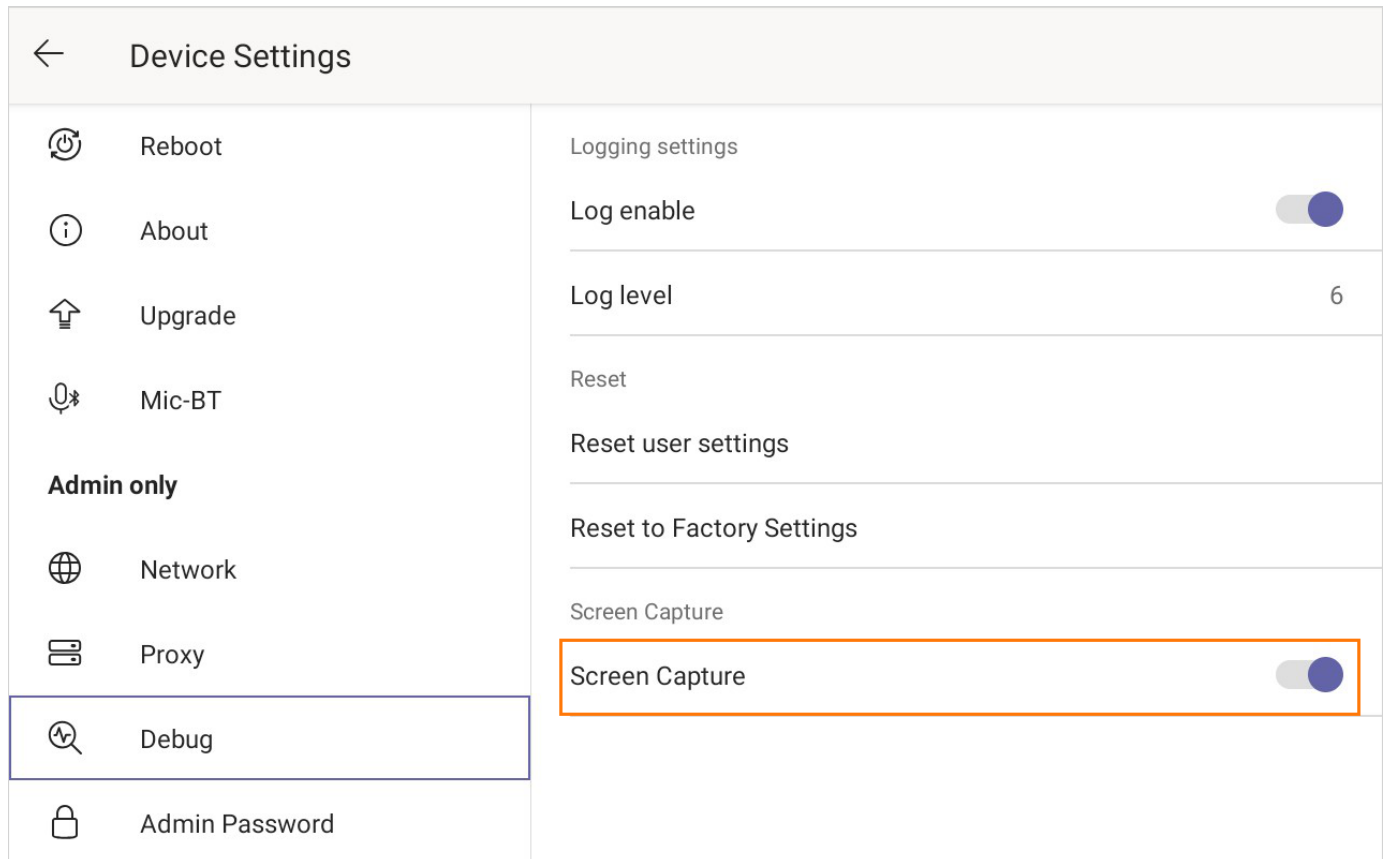
Enable the Screen Capture Feature Via Device User Interface

Procedure

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the avatar in the top-right corner of the screen and go to Settings > Device Settings > Debug (default password: admin) > Screen Capture .	Go to  > Settings > Device Settings > Debug (default password: admin) > Screen Capture .

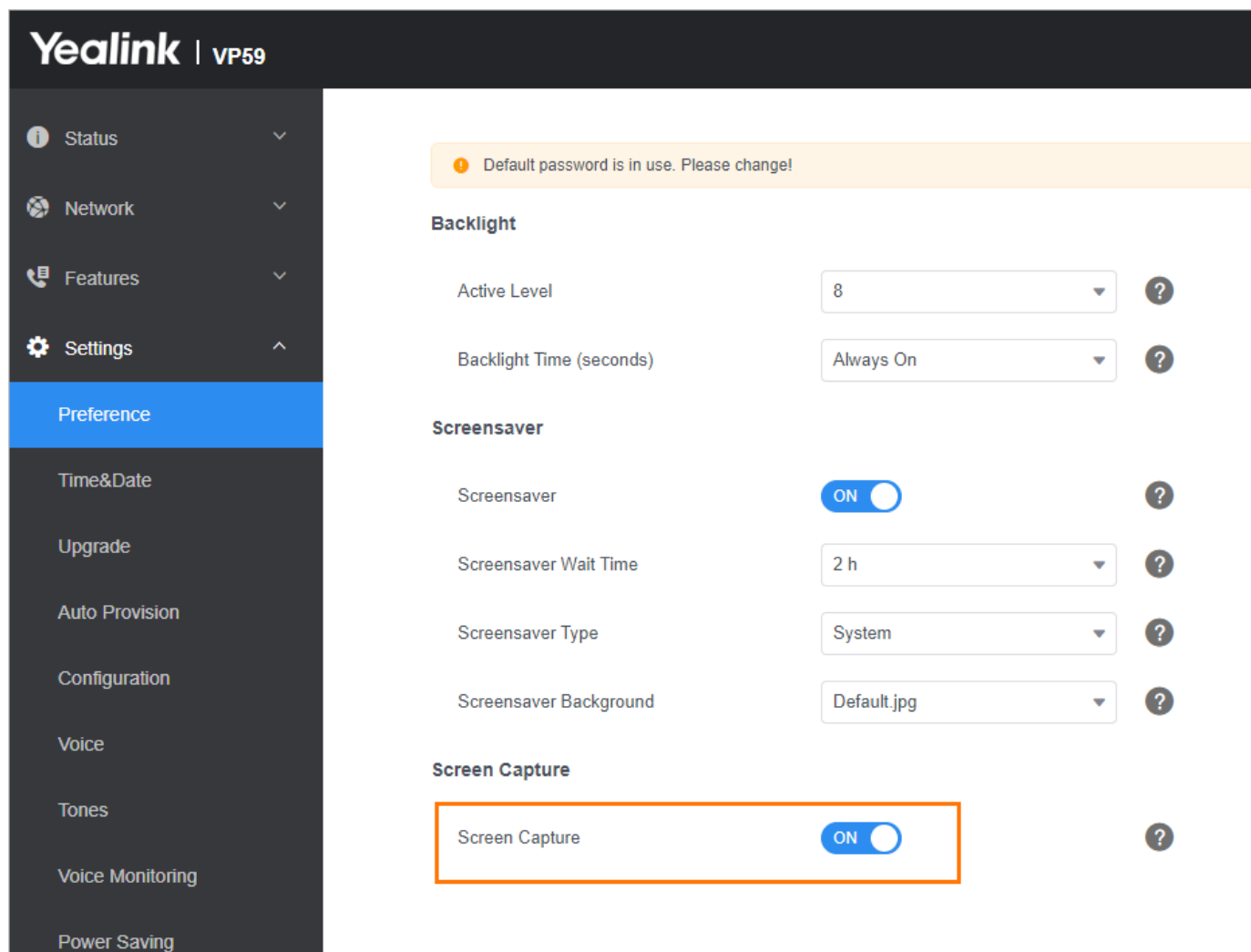
2. Enable **Screen Capture**.



Via Web User Interface

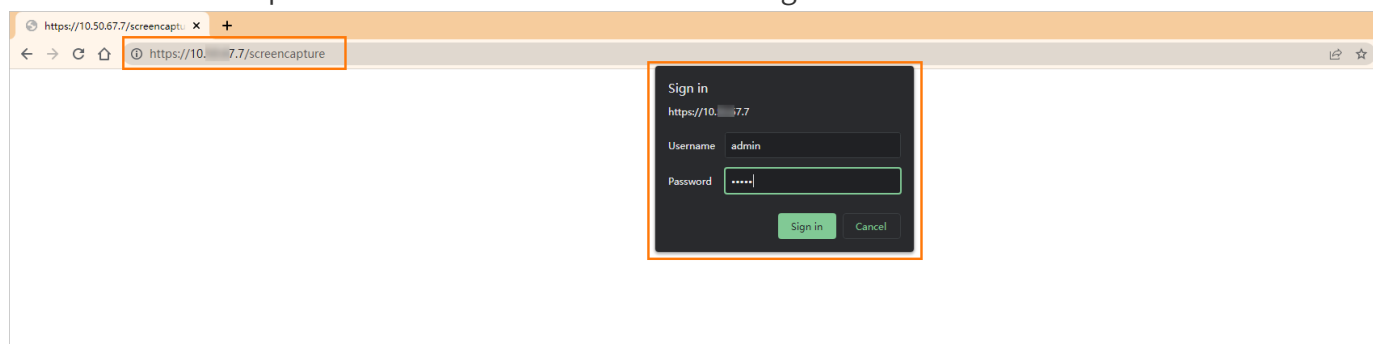
Procedure

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Preference > Screen Capture**.
3. Enable **Screen Capture**.

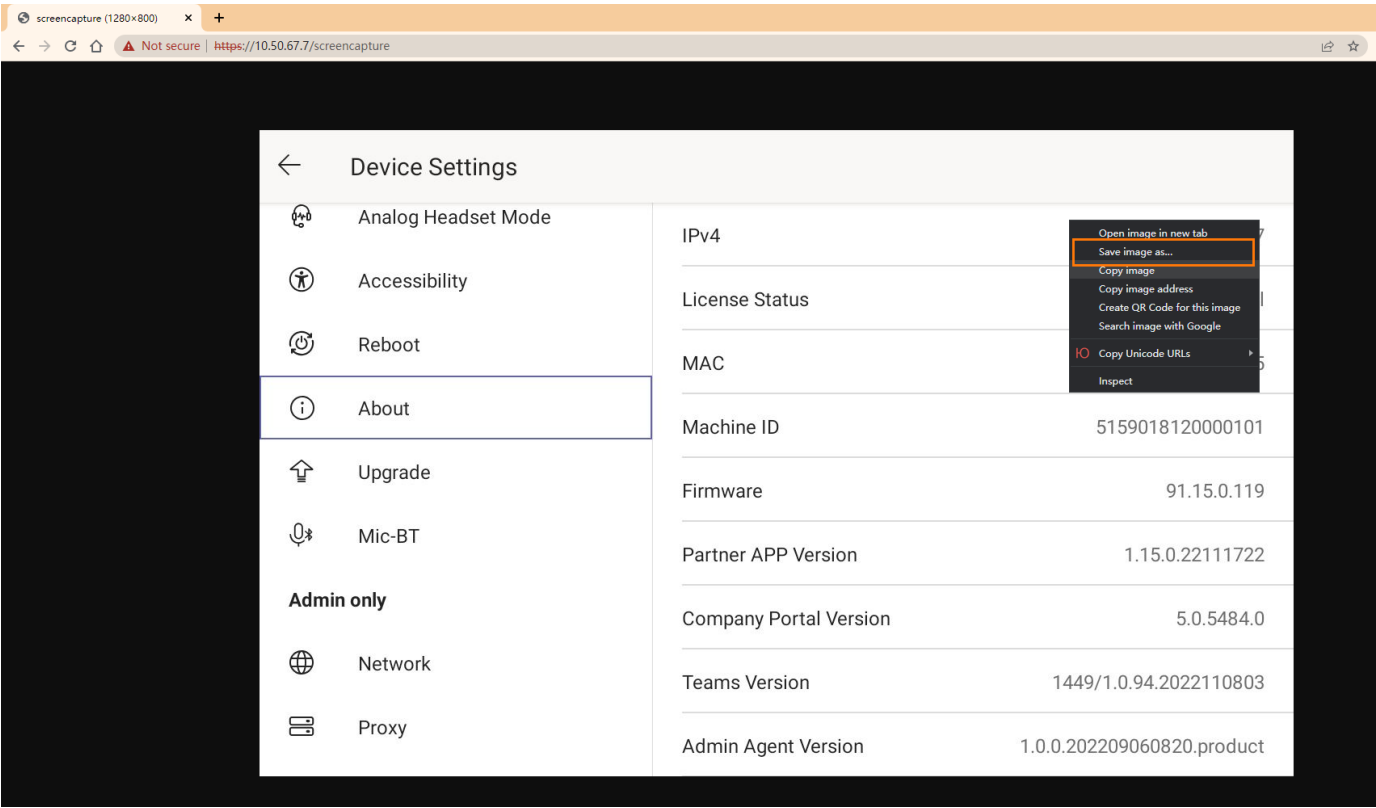


Take a Screenshot via Web User Interface

1. Enter request URI (for example, <http://10.2.20.252/screenshot>) in the browser's address bar and press the Enter key on the keyboard.
2. If it is the first time you capture the phone's current screen using the computer, it will prompt you to enter the user name and password of the administrator if the web browser does not remember the user name and password for the web user interface login.



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



Analyze Configuration Files

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

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

Exporting BIN Files from the Device

Procedure

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

Importing BIN Files from the Device

Procedure

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

Configure BIN File Import URL

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

static.configuration.url

Parameter	Permitted Values	Default	Description
static.configuration.url[1]	URL within 511 characters	Blank	It configures the access URL for the custom configuration files.  NOTE The file format of the custom configuration file must be *.bin.

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

Capture Packets

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

Capture the Packets via Web User Interface

For Yealink Teams devices, you can export the packets file to the local system and analyze it. Yealink Teams devices support the following two modes for capturing the packets:

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

Capture the Packets in a Normal Way

Procedure

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

Yealink | VP59

Default password is in use. Please change!

BIN Configuration

Import Configuration: No selected file(.bin) [Browse] [Import] [?]

Export Configuration: [Export] [?]

CFG Configuration

Import CFG Configuration File: No selected file(.cfg) [Browse] [Import] [?]

Export CFG Configuration File: All Settings [Export] [?]

Pcap

Pcap Type: Normal [?]

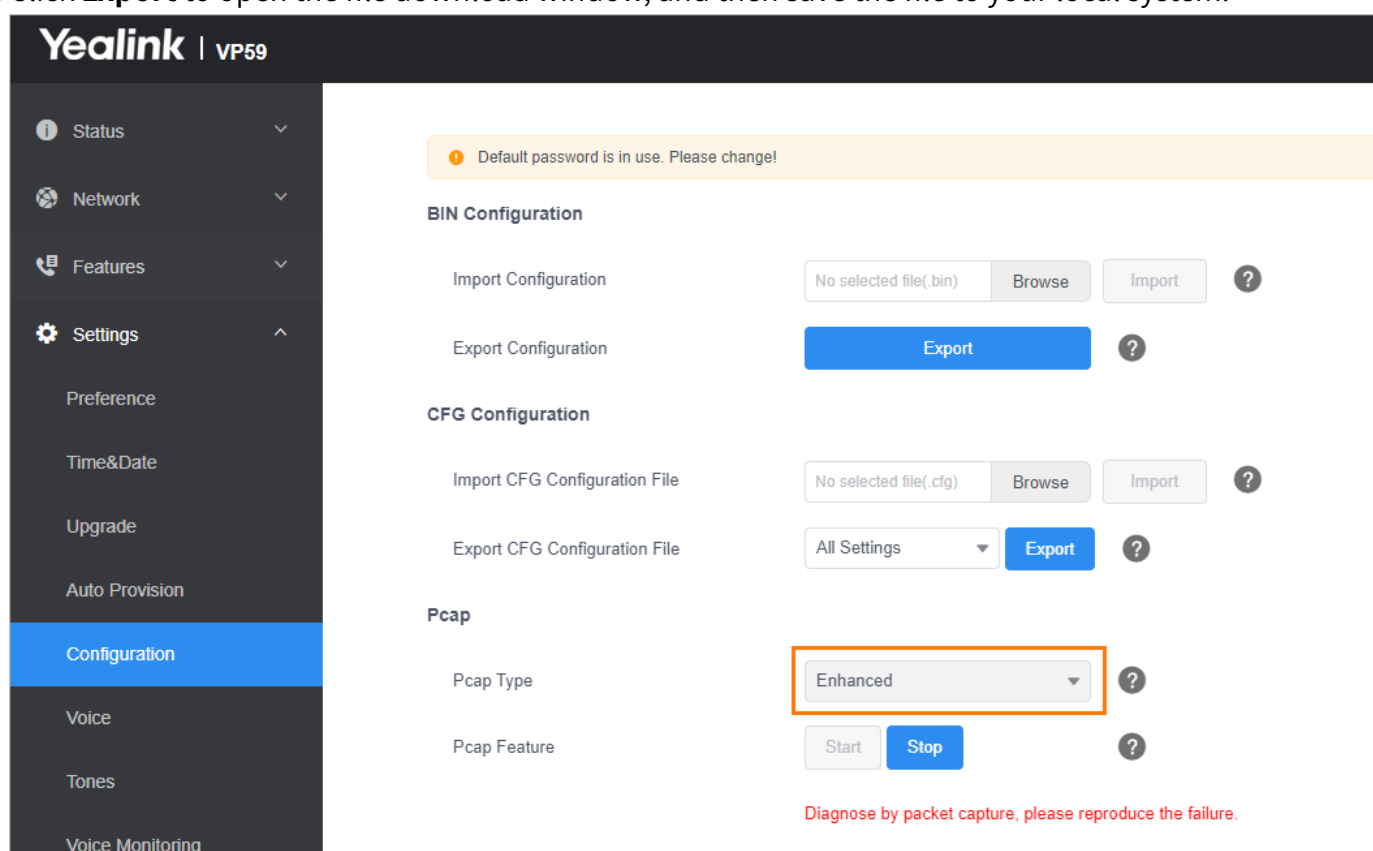
Pcap Feature: [Start] [Stop] [Export] [?]

Diagnose by packet capture, please reproduce the failure.

Capture the Packets in Enhanced Way

Procedure

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



Configure Ethernet Software Capturing

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

- **Receiving data packets from the HUB:** Connect the Internet port of the device and the PC to the same HUB, and then use Sniffer, Ethereal, or Wireshark software to capture the signal traffic.
- **Receiving data packets from PC port:** Connect the Internet port of the phone to the Internet and the PC port of the phone to a PC. Before capturing the signal traffic, make sure the phone can span data packets received from the Internet port to the PC port. It is unavailable for CP960/CP965 phones.

Span to PC Port Configuration

The following table lists the parameter you can use to configure the span to the PC port.

--	--

static.network.span_to_pc_port

Parameter	Permitted Values	Default	Description
static.network.span_to_pc_port[1]	0 - Disabled 1 -Enabled, all data packets from the Internet port can be received by PC port.	0	It enables or disables the device to span data packets received from the WAN port to the PC port. ! NOTE It works only if "static.network.pc_port.enable" is set to 1 (Auto Negotiation).

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

Reboot Teams Phones

Via Device User Interface

1. Select the method according to your device:

VP59/MP58/MP56/MP54/MP52/CP965	MP58 E2/MP56 E2/MP54 E2/MP52 E2/MP55 E2
Go to Settings > Device Settings > Reboot.	Go to Settings > Device Settings > General > Reboot.

2. Select **Reboot phone.**
3. It prompts if you are sure to reboot the device.
3. Select **OK.**

Via Web User Interface

Procedure

1. [Log in to the phone web user interface as an admin.](#)
2. Click **Settings > Upgrade.**
3. Click **Reboot** to reboot the device.
4. The web user interface prompts the message “Reboot the system?”
4. Click **OK** to confirm the reboot.
5. The device begins at rebooting. Any reboot of the device may take a few minutes.

Reset Teams Phones and Configuration

Generally, some common issues may occur while using the device. You can reset your device to factory configurations after you have tried all troubleshooting suggestions but still do not solve the problem.

Resetting the device to factory configurations clears the flash parameters, removes log files, user data, and cached data, and resets the administrator password to admin. All custom settings will be overwritten after resetting.

Reset Teams Phones to Factory Via Device User Interface

Procedure

1. Select the method according to your device:

VP59/MP58/MP56/MP54/MP52/CP965	MP58 E2/MP56 E2/MP54 E2/MP52 E2
Go to Settings > Device Settings > Debug > Reset to Factory Settings .	Go to Settings > Device Settings > System > Reset to Factory .

It prompts if you are sure to reset to factory default.

2. Tap **OK**.

Via Hardware Key

If you want to reset the device to factory settings but your screen cannot work or is frozen, you can use the hardware key to reset the device to factory.

Procedure

1. For MP, long press the pound key (#) and the star key (*) for a while.
2. For CP, press and hold the two Mute keys for a while.

Via Web User Interface

Procedure

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

**TIP**

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

Reset Custom Factory Settings

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

Procedure

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

Configure Custom Factory

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

static.features.custom_factory_config.enable
static.custom_factory_configuration.url

Parameter	Permitted Values	Default	Description
static.features.custom_factory_config.enable	0 - Disabled 1 -Enabled, Import Factory Configuration item will be displayed on the device's web user interface at the path Settings > Configuration. You can import a custom factory configuration file or delete the user-defined factory configuration via web user interface.	0	It enables or disables the Custom Factory Configuration feature.
static.custom_fac	URL within 511 characters	Bl	It configures the access URL of the

tory_configuration.url		ank	custom factory configuration files.  NOTE It works only if "static.features.custom_factory_config.enable" is set to 1 (Enabled) and the file format of the custom factory configuration file must be *.bin.
------------------------	--	-----	---

Delete the Custom Factory Settings Files

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

Procedure

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

Export All Diagnostic Files for MP Teams Phones

Export All Diagnostic Files

Procedure

1. From the web user interface, go to **Settings > Configuration**.
2. (Optional) Go to **Audio Diagnostic > Start** if you also want to export the audio diagnostic files.
3. Click **Start** in the **Export All Diagnostic Files** field to begin capturing signal traffic. The system log level will be automatically set to 6.
4. Reproduce the issue by doing the steps that will cause the problem.
5. (☒Important) Please also record the issue timestamp, like `July 1st 12:00-12:05`.
6. (Optional) Go to **Audio Diagnostic > Stop** to stop the audio diagnostic.
7. Click **Stop** in the **Export All Diagnostic Files** field to stop the capture.
8. Click **Export** to open the file download window, and then save the diagnostic file to your local system. A diagnostic file named `<MAC>-DiagnoseInfo.tar` is successfully exported to your local system.

! NOTE

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

Export the Audio Diagnostic File Only

Procedure

1. From the web user interface, go to **Settings > Configuration**.
2. Go to **Audio Diagnostic > Start**.
3. Reproduce the issue by doing the steps that will cause the problem.
4. (☒Important) Please also record the issue timestamp, like `July 1st 12:00-12:05`.
5. (Optional) Go to **Audio Diagnostic > Stop** to stop the audio diagnostic.
6. Click **Export** to open the file download window, and then save the diagnostic file to your local system. A diagnostic file named `<MAC>-DiagnoseInfo.tar` is successfully exported to your local

system.

! NOTE

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

Configure Syslog

Configure Syslog

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.

Via Web User Interface

Procedure

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Configuration > Syslog**.
3. Enable **Syslog**.
4. Enter the server URL in the **Syslog Server** field.
5. Select a desired transport type from the drop-down menu of **Syslog Transport Type**.
6. Select **6** from the drop-down menu of **Syslog Level**.

The screenshot shows the Yealink VP59 web interface. On the left is a dark sidebar with a menu. The 'Configuration' option is highlighted in blue. The main content area is titled 'Audio Diagnostic' and 'Local Log'. Below these, there are settings for 'Enable Local Log' (ON), 'Local Log Level' (6), 'Max Log File Size (2048-20480KB)' (20480), and 'Export Local Log' (Export button). A section titled 'Syslog' is highlighted with an orange border. It contains settings for 'Enable Syslog' (ON), 'Syslog Server' (http://19/), 'Port' (514), 'Syslog Transport Type' (UDP), 'Syslog Level' (6), 'Syslog Facility' (Local Use 0 (Local0)), and 'Syslog Prepend MAC' (OFF). Each setting has a help icon (question mark) to its right.

Via Auto Provisioning

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

```
static.syslog.enable
static.syslog.server
static.syslog.server_port
static.syslog.transport_type
static.syslog.level
static.syslog.facility
static.syslog.prepend_mac_address.enable
```

Parameter	Permitted Values	Default	Description
static.syslog.	0-Disabled 1-Enabled	0	It enables or disables the

enable			device to upload log messages to the syslog server in real time.
static.syslog.server	IP address or domain name	Blank	It configures the IP address or domain name of the syslog server when exporting log to the syslog server.
static.syslog.server_port	Integer from 1 to 65535	514	It configures the port of the syslog server. Example: static.syslog.port = 515
static.syslog.transport_type	0 - UDP 1 -TCP 2 -TLS	0	It configures the transport protocol that the device uses when uploading log messages to the syslog server.
static.syslog.level	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	6	It configures the lowest level of syslog information that displays in the syslog. When you choose a log level, it includes all events of an equal or higher severity level and excludes events of a lower severity level. The logging level you choose determines the lowest severity of events to log.
static.syslog.facility	0 -kernel messages 1 -user-level messages 2 -mail system 3 -system daemons 4 -security/authorization messages (note 1) 5 -messages generated internally by syslogd 6 -line printer subsystem 7 -network news subsystem 8 -UUCP subsystem	16	It configures the facility that generates the log messages. For more information, refer to RFC 3164.

	9 -clock daemon (note 2) 10 -security/authorization messages (note 1) 11 -FTP daemon 12 -NTP subsystem 13 -log audit (note 1) 14 -log alert (note 1) 15 -clock daemon (note 2) 16 -local use 0 (local0) 17 -local use 1 (local1) 18 -local use 2 (local2) 19 -local use 3 (local3) 20 -local use 4 (local4) 21 -local use 5 (local5) 22 -local use 6 (local6) 23 -local use 7 (local7)		
static.syslog. prepend_mac _address.enable	0 -Disabled 1 -Enabled	0	It enables or disables the device to prepend the MAC address to the log messages exported to the syslog server.

View the Syslog Messages on Your Syslog Server

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

The following figure shows a portion of the syslog:

```

Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http2.Http2Connection.newStream(Http2Connection.java:239)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http2.Http2Connection.newStream(Http2Connection.java:222)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http2.Http2Codec.writeRequestHeaders(Http2Codec.java:111)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http.CallServerInterceptor.intercept(CallServerInterceptor.java:50)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:121)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at com.microsoft.skyeye.teams.data.proxy.GlobalRequestInterceptor.intercept(GlobalRequestInterceptor.java:291)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.connection.ConnectInterceptor.intercept(ConnectInterceptor.java:45)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:121)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.cache.CacheInterceptor.intercept(CacheInterceptor.java:93)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:121)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http.BridgeInterceptor.intercept(BridgeInterceptor.java:93)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http.RetryAndFollowUpInterceptor.intercept(RetryAndFollowUpInterceptor.java:126)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:121)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:121)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.RealCall.getResponseWithInterceptorChain(RealCall.java:200)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at okhttp3.RealCall.execute(RealCall.java:77)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at retrofit2.OkHttpCall.execute(OkHttpCall.java:180)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at retrofit2.ExecutorCallAdapterFactory$ExecutorCallbackCall.execute(ExecutorCallAdapterFactory.java:91)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at com.microsoft.skyeye.teams.data.HttpCallExecutor$RetrofitRequestExecutor.execute(HttpCallExecutor.java:459)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at com.microsoft.skyeye.teams.data.HttpCallExecutor.execute(HttpCallExecutor.java:216)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at com.microsoft.skyeye.teams.data.HttpCallExecutor.execute(HttpCallExecutor.java:147)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at com.microsoft.skyeye.teams.data.HttpCallExecutor.execute(HttpCallExecutor.java:129)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at com.microsoft.skyeye.teams.data.HttpCallExecutor.execute(HttpCallExecutor.java:118)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at com.microsoft.skyeye.teams.services.files.PresenceServiceAppData.setUnifiedPresence(PresenceServiceAppData.java:299)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at com.microsoft.skyeye.teams.data.AppData.setResponseStatus(AppData.java:2240)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at com.microsoft.skyeye.teams.calling.call.CallPresence1.handleMessage(CallPresence.java:66)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at android.os.Handler.dispatchMessage(Handler.java:98)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at android.os.Looper.loop(Looper.java:135)
Nov 22 00:09:35 ap1c:[590]: ANDR3+error > 1155 1524 E SetUnifiedPresence: at android.os.HandlerThread.run(HandlerThread.java:61)

```

Configure Local Logs

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

Configure Local Log

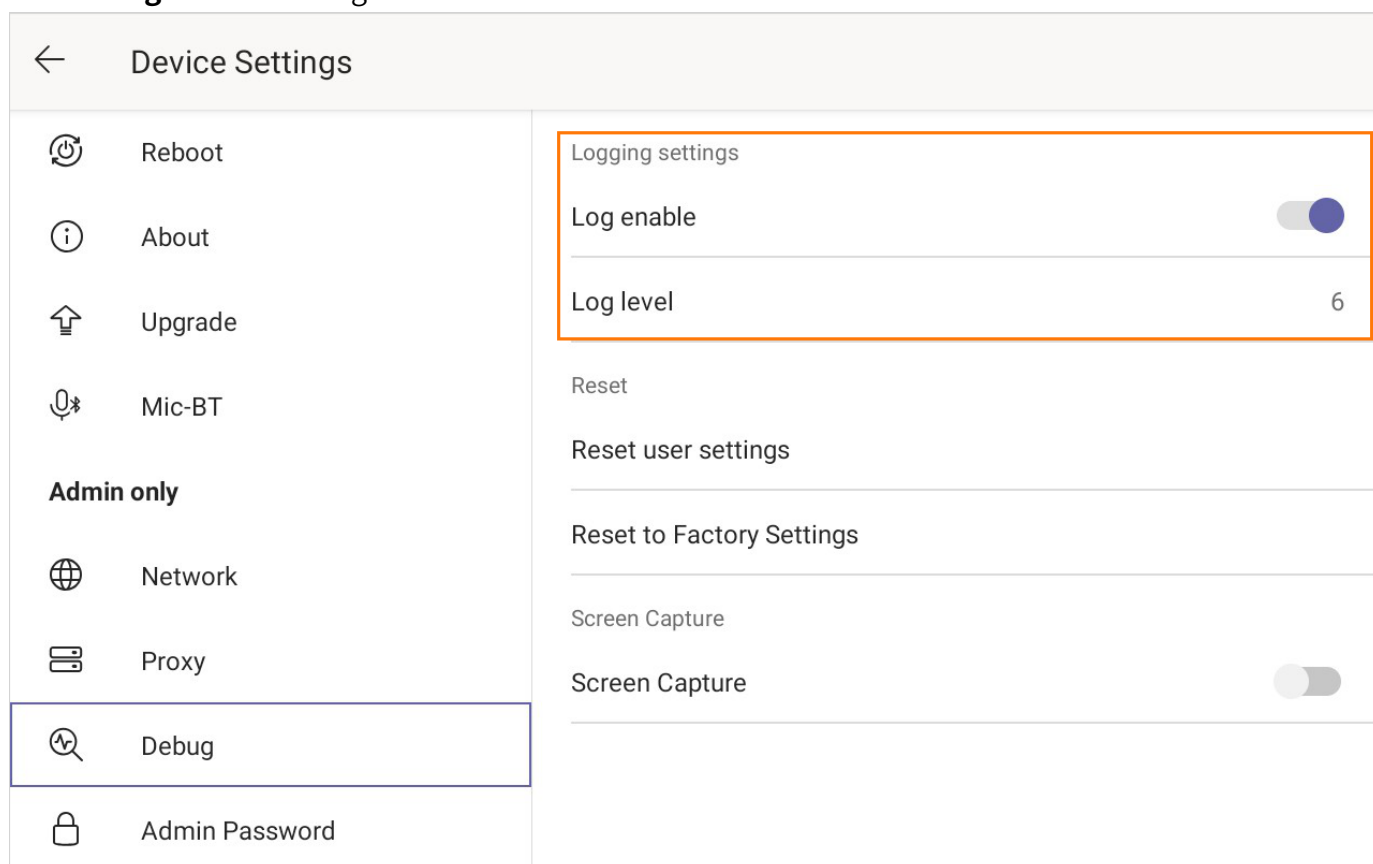
You can enable the local log, specify the severity level, and choose to keep the log locally or upload the local log files to the provisioning server. The local log files can be exported via the web user interface simultaneously.

Via Device User Interface

1. Select the method according to your device:

VP59/MP58 (E2)/MP56 (E2)/MP54 (E2)/CP965	MP52 (E2)/MP55 E2
Tap the avatar in the top-right corner of the screen and go to Settings > Device Settings > Debug (default password: admin).	Go to  > Settings > Device Settings > Debug (default password: admin).

2. Enable **Log** and set the log level as 6.



Via Web User Interface

Procedure

1. [Log in to the phone web user interface as an admin.](#)
2. Go to **Settings > Configuration > Local Log**.
3. Enable **Local Log** and set the log level as 6.
4. (Optional) Click **Export** to export the local log.

The screenshot shows the Yealink VP59 web interface. On the left is a navigation menu with options: Status, Network, Features, Settings, Preference, Time&Date, Upgrade, Auto Provision, Configuration (highlighted in blue), Voice, and Tones. The main content area is titled 'Export CFG Configuration File' with a dropdown set to 'All Settings' and an 'Export' button. Below this are sections for 'Pcap' (with 'Pcap Type' set to 'Enhanced' and 'Pcap Feature' buttons 'Start' and 'Stop'), 'Audio Diagnostic' (with 'Audio Diagnostic' buttons 'Start' and 'Stop'), and 'Local Log' (highlighted with an orange box). The 'Local Log' section contains: 'Enable Local Log' (ON), 'Local Log Level' (6), 'Max Log File Size (2048-20480KB)' (20480), and an 'Export Local Log' button.

Via Auto Provisioning

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

```
static.local_log.enable
static.local_log.level
static.local_log.max_file_size
static.auto_provision.local_log.backup.enable
static.auto_provision.local_log.backup.upload_period
static.auto_provision.local_log.backup.path
static.auto_provision.local_log.backup.append
static.auto_provision.local_log.backup.append.limit_mode
static.auto_provision.local_log.backup.append.max_file_size
```

static.auto_provision.local_log.backup.bootlog.upload_wait_time

Parameter	Permitted Values	Default	Description
static.local_log.enable	0- Disabled, the device will stop recording logs to the log files (<MAC>-boot.log and <MAC>-sys.log) locally. The log files recorded before are still kept on the device. 1-Enabled, the device will continue to record logs to the log files (<MAC>-boot.log and <MAC>-sys.log) locally. You can upload the local log files to the provisioning server or a specific server or export them to the local system.	1	It enables or disables the device from recording logs locally.  NOTE We recommend that you not disable this feature.
static.local_log.level	0- system is unusable 1-action must be taken immediately 2-critical condition 3-error conditions 4-warning conditions 5-normal but significant condition 6-informational	6	It configures the lowest level of local log information to be rendered to the <MAC>-sys.log file. When you choose a log level, it includes all events of an equal or higher severity level and excludes events of a lower severity level. The logging level you choose determines the lowest severity of events to log.
static.local_log.max_file_size	Integer from 2048 to 20480	20480	It configures the maximum size (in KB) of the log files (<MAC>-boot.log and <MAC>-sys.log) that can be stored on the device. When this size is about to be exceeded,

			If the local log files are configured to be uploaded to the server by the parameter <code>static.auto_provision.local_log.backup.enable</code>, the device will clear all the local log files on the device once successfully backing up. If <code>static.auto_provision.local_log.backup.enable</code> is set to 0 (Disabled), the device will erase half of the logs from the oldest log information on the device.
<code>static.auto_provision.local_log.backup.enable</code>	0- Disabled 1-Enabled, the device will upload the local log files to the provisioning server or the specific server to back up these files when one of the following happens: Auto provisioning is triggered; The size of the local log files reaches the maximum configured by the parameter <code>static.local_log.max_file_size</code>; It's time to upload local log files according to the upload period configured by the parameter <code>static.auto_provision.local_log.backup.upload_period</code>.	0	It enables or disables the device to upload the local log files (<code><MAC>-boot.log</code> and <code><MAC>-sys.log</code>) to the provisioning server or a specific server. ! NOTE The upload path is configured by the parameter <code>"static.auto_provision.local_log.backup.path"</code>.
<code>static.auto_provision.local_log.backup.upload_period</code>	Integer from 30 to 86400	30	It configures the period (in seconds) of the local log files (<code><MAC>-boot.log</code> and <code><MAC>-sys.log</code>) uploads to the provisioning server or a specific server.

			NOTE It works only if "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled).
static.auto_provision.local_log.backup.path	URL within 1024 characters	Blank	It configures the upload path of the local log files (<MAC>-boot.log and <MAC>-sys.log). If you leave it blank, the device will upload the local log files to the provisioning server. If you configure a relative URL (for example, /upload), the device will upload the local log files by extracting the root directory from the access URL of the provisioning server. If you configure an absolute URL with protocol (for example, tftp), the device will upload the local log files using the desired protocol. If no protocol, the device will use the same protocol with auto provisioning for uploading files. Example: <pre>static.auto_provision.local_log.backup.path = tftp://10.3.6.133/upload.</pre> NOTE It works only if "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled).
static.auto_provision.local_log.backup.append	0- Overwrite 1-Append (unavailable to TFTP Server)	0	It configures whether the uploaded local log files (<MAC>-boot.log and <MAC>-sys.log) overwrite the existing files or are appended to the existing files.
static.auto_provision.local_log.backup.delete	0 - Append Delete, the server	0	It configures the behavior when local

ision.local_log. backup.append. limit_mode	will delete the old log, and the device will continue uploading log. 1 -Append Stop, the device will stop uploading log.		log files (<MAC>-boot.log and <MAC>-sys.log) on the provisioning server or a specific server reach the maximum file size.
static.auto_provision.local_log. backup.append.max_file_size	Integer from 200 to 65535	10 24	It configures the maximum size (in KB) of the local log files (<MAC>-boot.log and <MAC>-sys.log) can be stored on the provisioning server or a specific server.
static.auto_provision.local_log. backup.bootlog.upload_wait_time	Integer from 1 to 86400	12 0	It configures the waiting time (in seconds) before the device uploads the local log file (<MAC>-boot.log) to the provisioning server or a specific server after startup.

View the Log Files

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

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

The default local log level is 6.

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

```

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

```

The <MAC>-sys.log file reports the logs with a configured severity level and higher. For example, if you

have configured the severity level of the log to be reported to the `<MAC>-sys.log` file to 4, then the log with a severity level of 0 to 4 will all be reported.

Troubleshooting Guidance

This section provides some troubleshooting tips to help you solve the problem:

- Generally, you can configure the log for future troubleshooting needs:
 - [Configure Local Logs](#)
 - [Configure Syslog](#)
- When some problems occur with your phone, you can use the following troubleshooting methods to solve the problem.
 - [Reboot Devices](#)
 - [Update to the Latest Teams App](#)
 - [Update to the Latest Firmware](#)
 - [Reset Device to Factory](#)
- If the preceding methods CANNOT solve the problem, you need to [create a ticket](#) to Yealink support and provide the following diagnostic files.
 - [Export All Diagnostic Files \(log files, audio diagnostic files, captured packets, and configuration files\)](#)
 - [Export Audio Diagnostic Files only](#)
 - [Capture Packets](#)