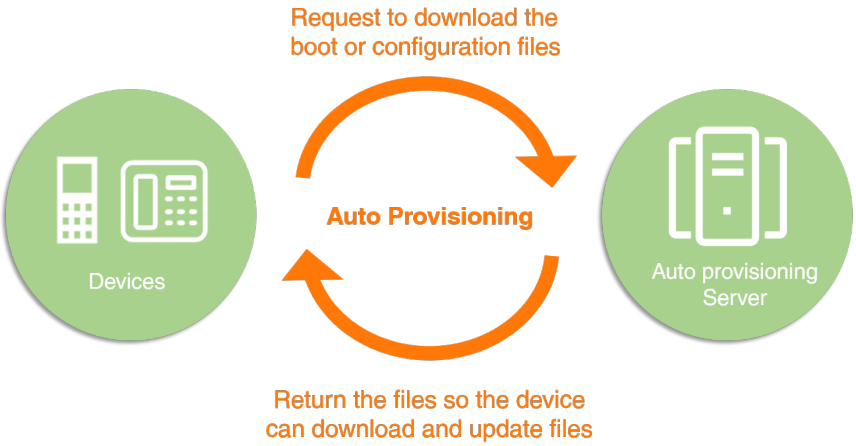
# Configuration Methods

## 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

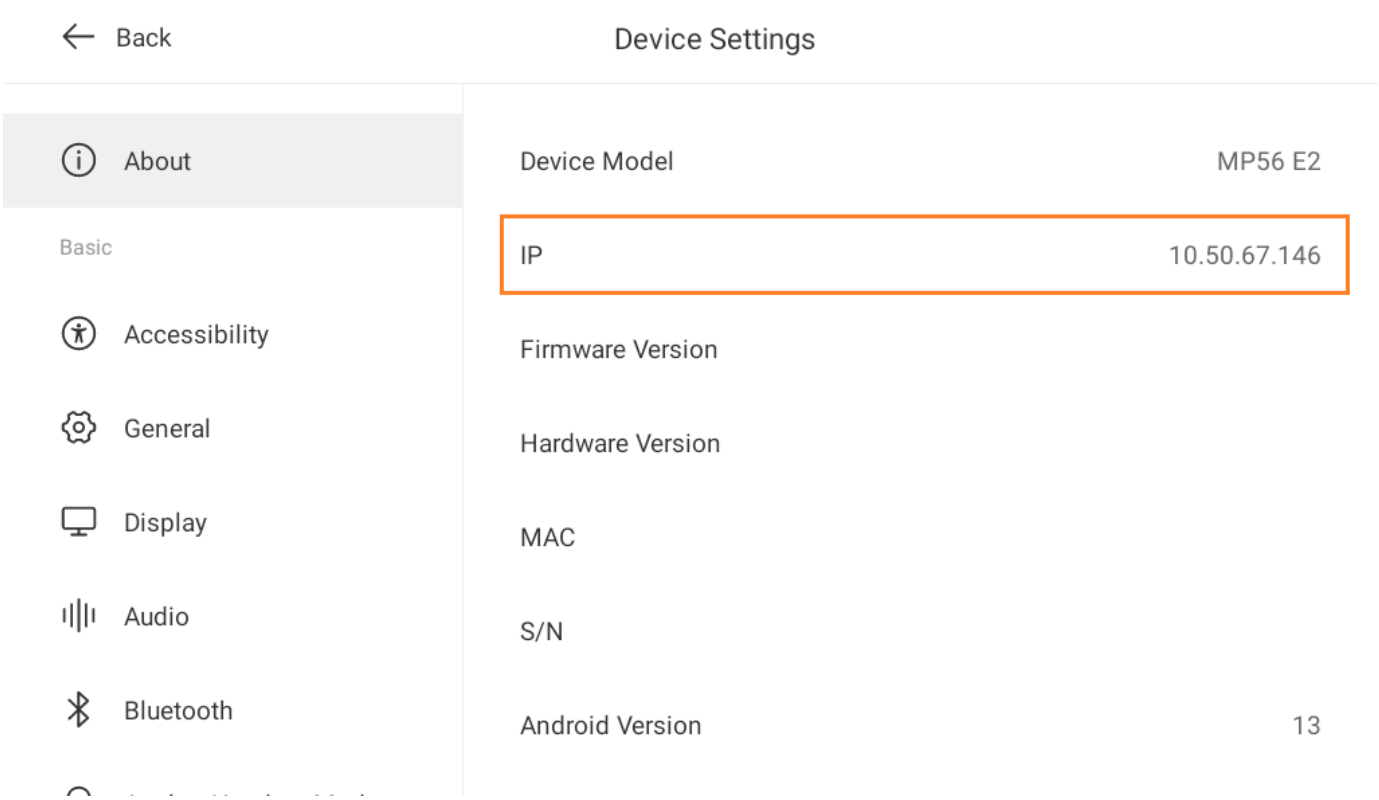
| Configuration Methods | Description | Applicable Scenarios |
|---|---|---|
| Auto provisioning | Auto provisioning is a process that allows you to make phones to request and download the boot or configuration files from the provisioning server. You can use this feature to change some configurations for bathes of phones.   | 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 configurations for the phone. | Single configuration |

## Access the Phone IP Address

You need to get the phone IP address before logging in to the phone web user interface.

**Procedure**

1. Go to **More** > **Settings** > **General** > **System Settings** > **About** > **IP**.




# Log In to the Web User Interface

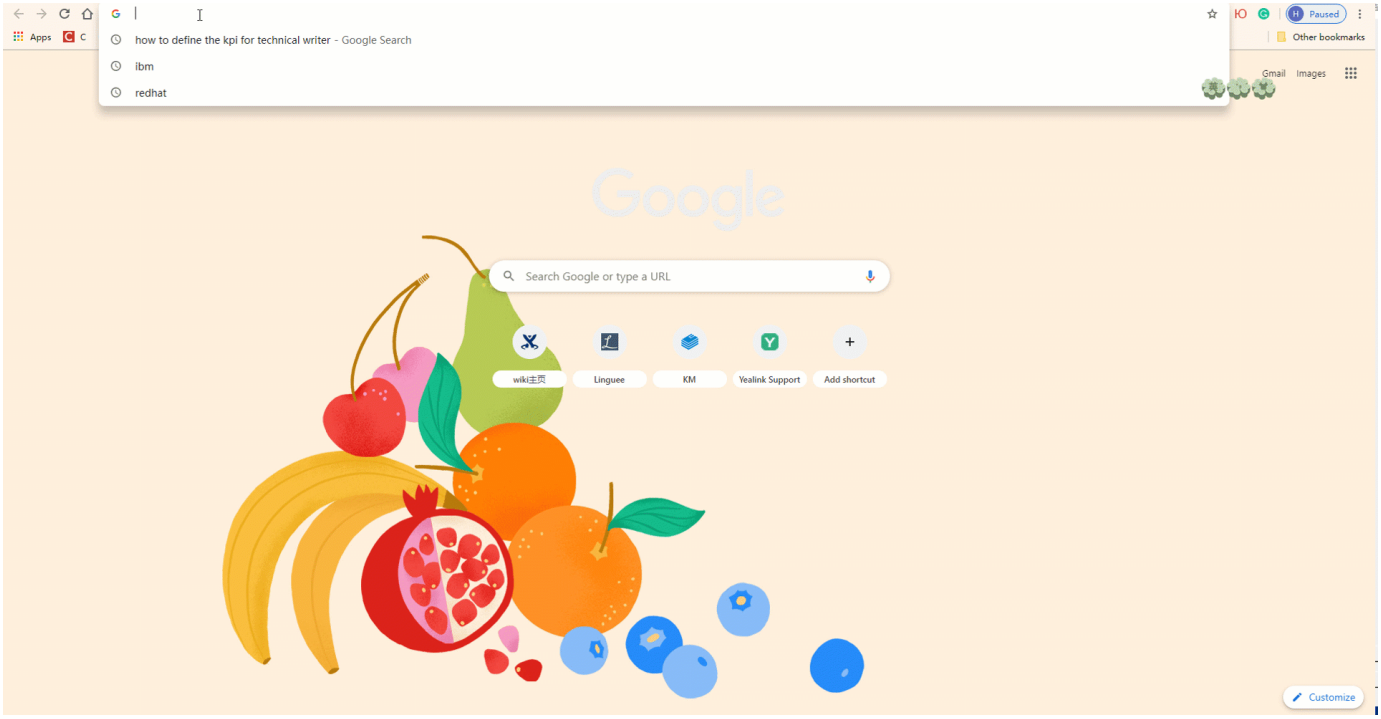
To use the phone web user interface to configure the phone, you need to log into the web user interface.

**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.


how to define the kpi for technical writer - Google Search
ibm
redhat
Apps
Paused
Other bookmarks
Gmail
Images
Google
Search Google or type a URL
wiki主页
Linguee
KM
Yealink Support
Add shortcut
Customize

# Enroll and Manage Zoom Phones on Zoom Device Management (ZDM)

See Zoom Phone Appliance admin guide.

# 802.1x Authentication

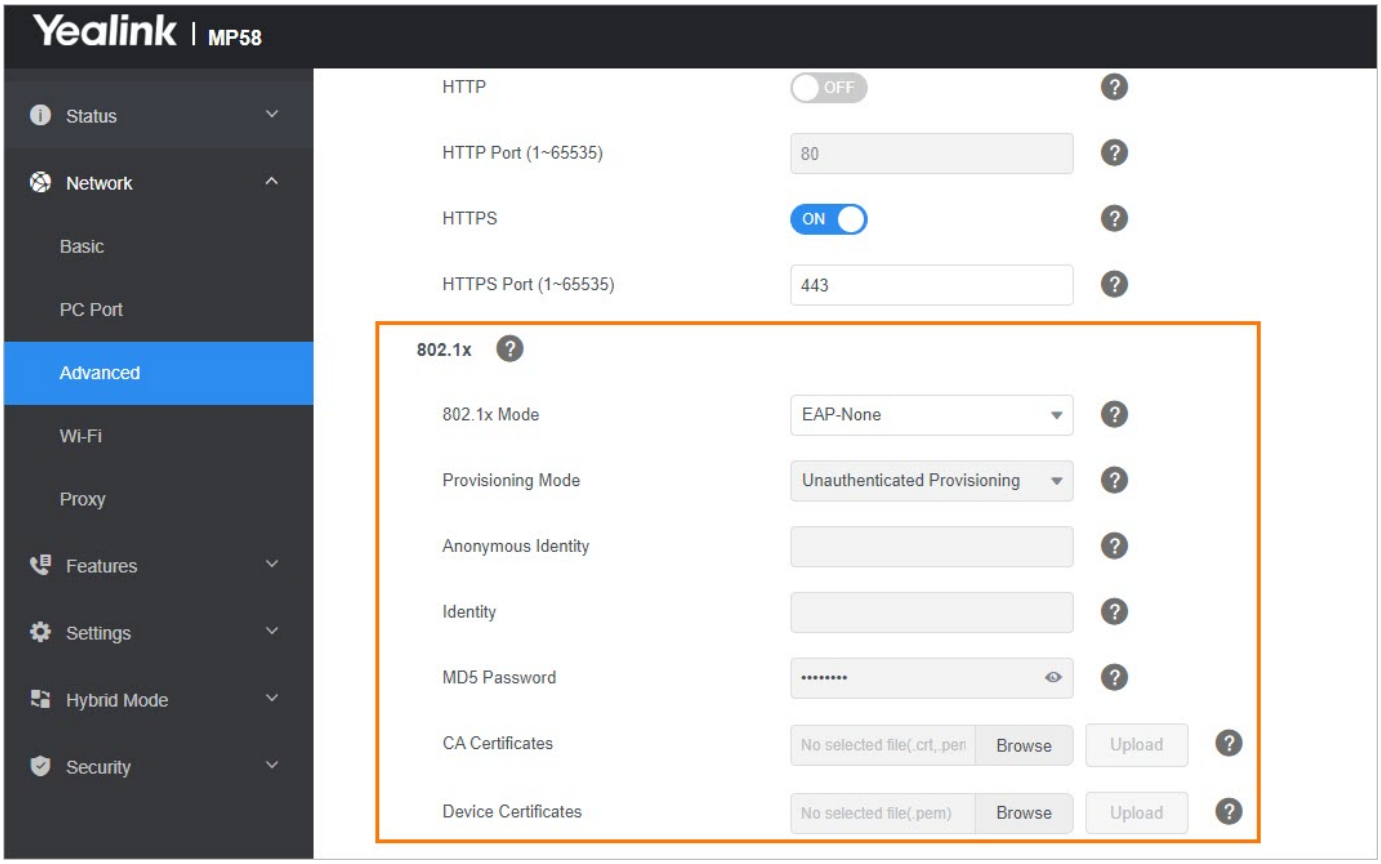
Yealink Zoom IP Phones support the following protocols for 802.1X authentication:

- 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**.

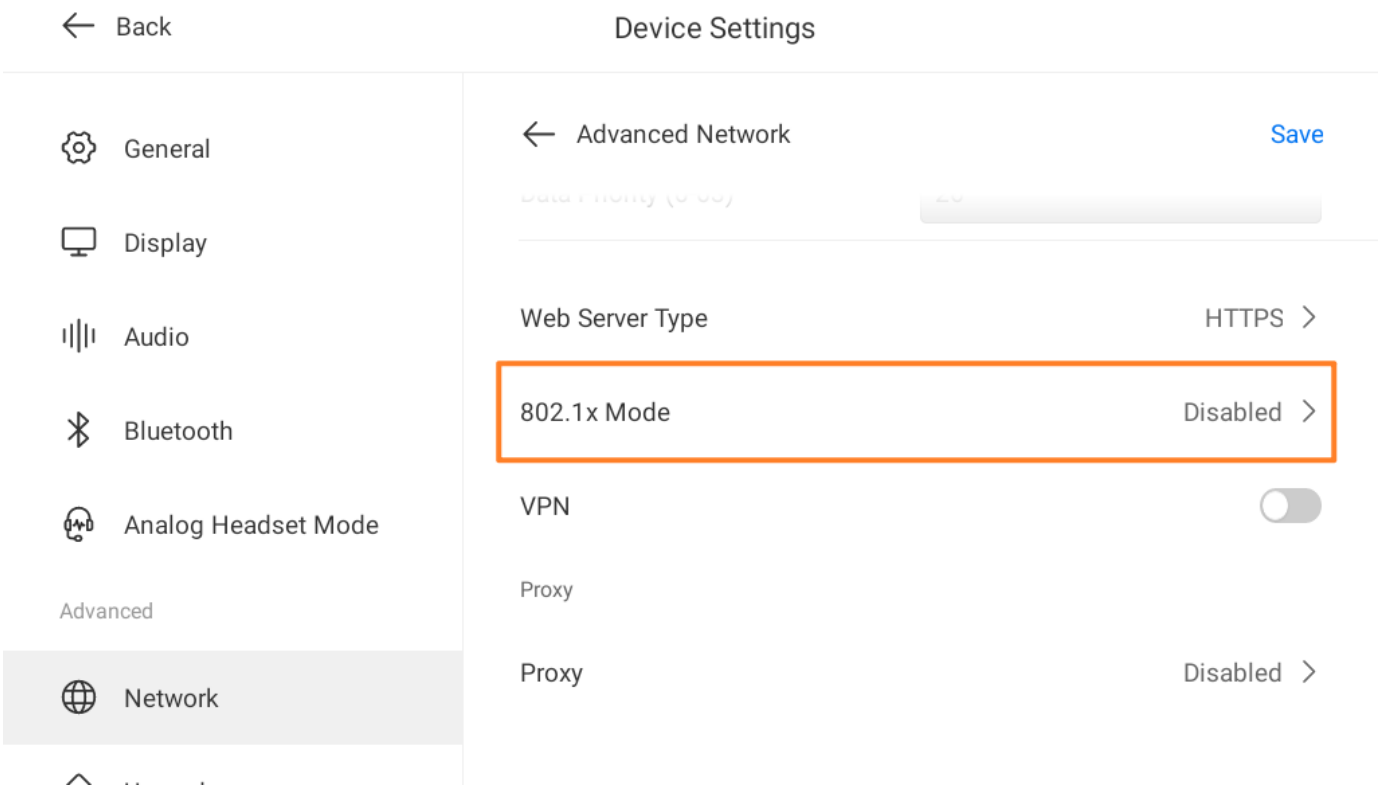



## Via Device User Interface

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. Go to **More** > **Settings** > **General** > **System Settings** > **Network** (Admin only, default password: admin) > **Advanced Network** > **802.1x Mode**.




# Via Auto Provisioning

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

network.802_1x.mode
network.802_1x.eap_fast_provision_mode
network.802_1x.anonymous_identity
network.802_1x.identity
network.802_1x.md5_password
network.802_1x.root_cert_url
network.802_1x.client_cert_url

| Parameter | Permitted Values | Default | Description |
|---|---|---|---|
| static.networ | **0-** EAP-None, 802.1x | 0 | It configures the 802.1x authentication method. |

| | | | |
|---|---|---|---|
| k.802_1x.mode [1] | authentication is not required.<br>**1-** EAP-MD5<br>**2-** EAP-TLS<br>**3-** EAP-PEAP/ MSCHAPv2<br>**4-** EAP-TTLS/EAP-MSCHAPv2<br>**5-** EAP-PEAP/GTC<br>**6-** EAP-TTLS/EAP-GTC<br>**7**-EAP-FAST | | |
| network.802_1x.eap_fast_provision_mode | **0**-Unauthenticated Provision<br>**1**-Authenticated Provision | 0 | It configures the EAP In-Band provisioning method for EAP-FAST.<br>**NOTE**<br>It works only if "static.network.802_1x.mode" is set to 7 (EAP-FAST). |
| network.802_1x.anonymous_identity | String within 32 characters | Blank | It configures the anonymous identity (user name) for 802.1X authentication.<br>It is used for constructing a secure tunnel for 802.1X authentication.<br>**NOTE**<br>It works only if "static.network.802_1x.mode" is set to 2, 3, 4, 5, 6 or 7. |
| static.network.802_1x.identity[1] | String within 32 characters | Blank | It configures the identity (user name) for 802.1x authentication.<br>**NOTE**<br>It works only if "static.network.802_1x.mode" is set to 1, 2, 3, 4, 5, 6, or 7. |
| static.networ | String within 32 | Bl | It configures the password for 802.1x |

| | | | |
|---|---|---|---|
| k.802_1x.md5_password[1] | characters | ank | authentication.<br>**NOTE**<br>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 *.pem,* .crt, *.cer or *.der.<br>**NOTE**<br>It works only if "static.network.802_1x.mode" is set to 2, 3, 4, 5, 6, or 7. |
| static.network.802_1x.client_cert_url | URL within 511 characters | Blank | It configures the access URL of the device certificate. The format of the certificate must be *.pem.<br>**NOTE**<br>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 Zoom 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/CP960.**

## Supported Transmission Methods

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

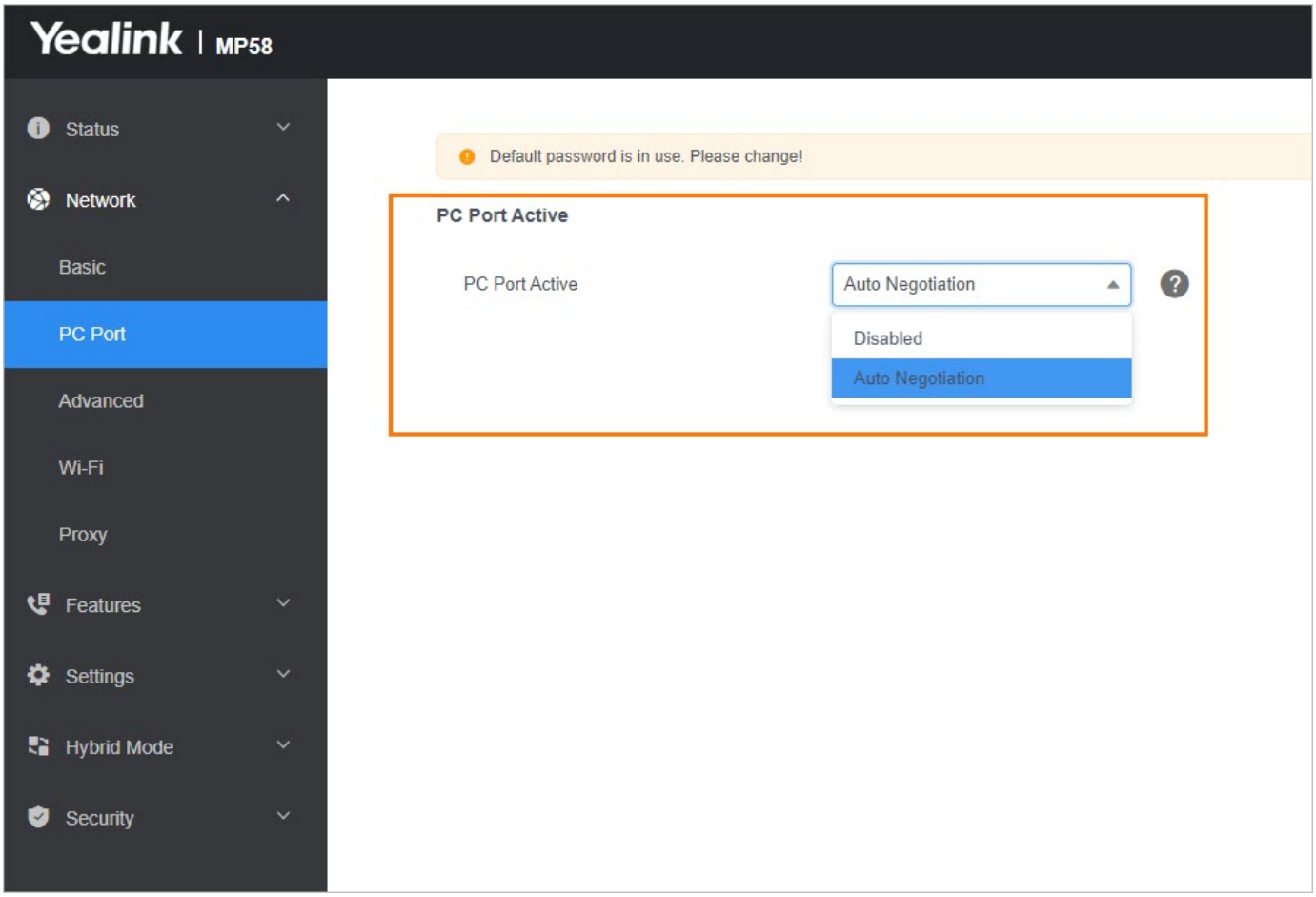
- Auto Negotiation
- Half-duplex (transmit in 10 Mbps or 100 Mbps)
- Full-duplex (transmit in 10 Mbps, 100 Mbps, or 1000 Mbps (unavailable to CP960/CP965)) Auto negotiation is configured for both Internet and PC ports on the device by default.

## Internet Port and PC Port Configuration

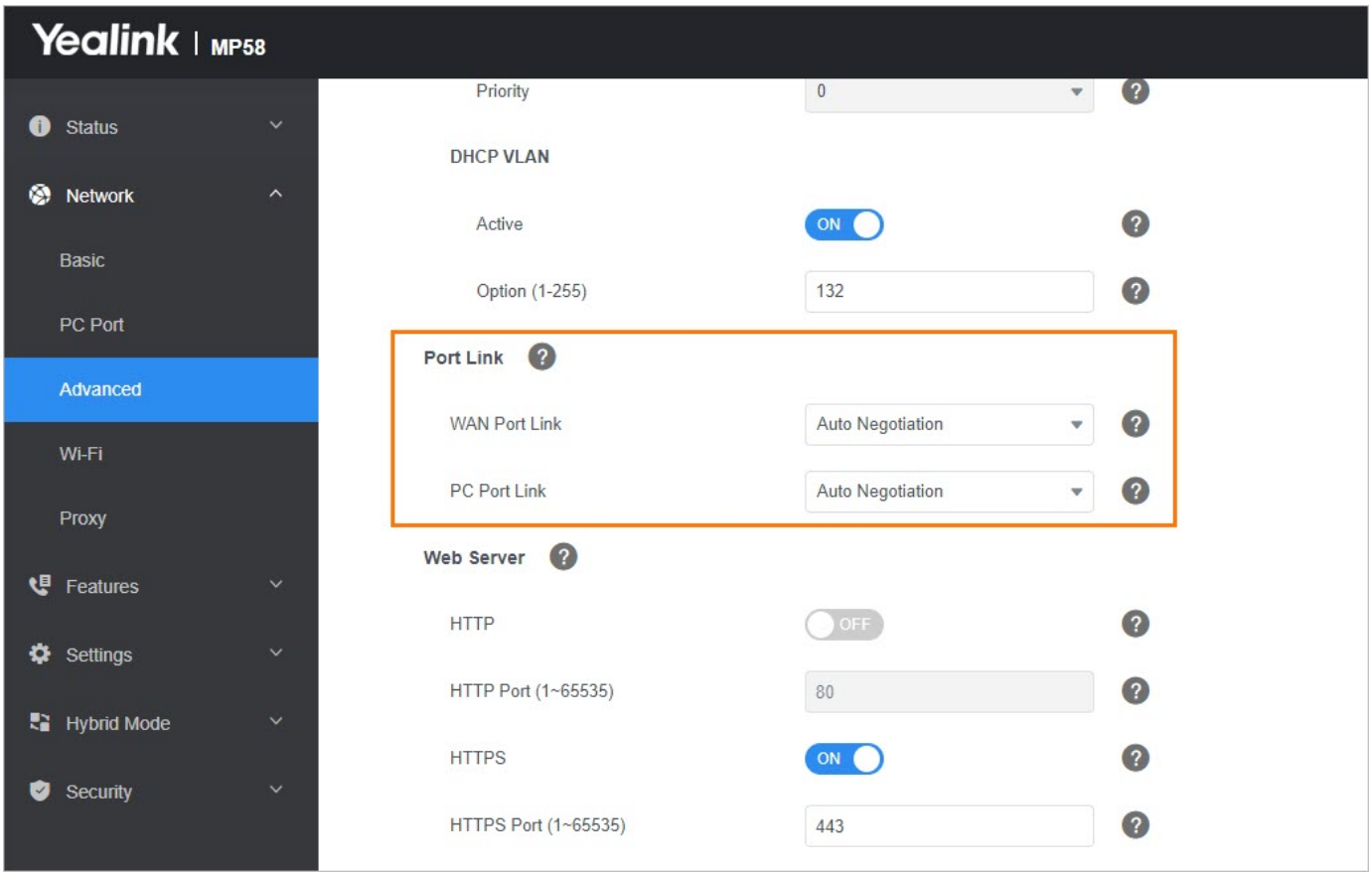
### Via Web User Interface

**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.




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

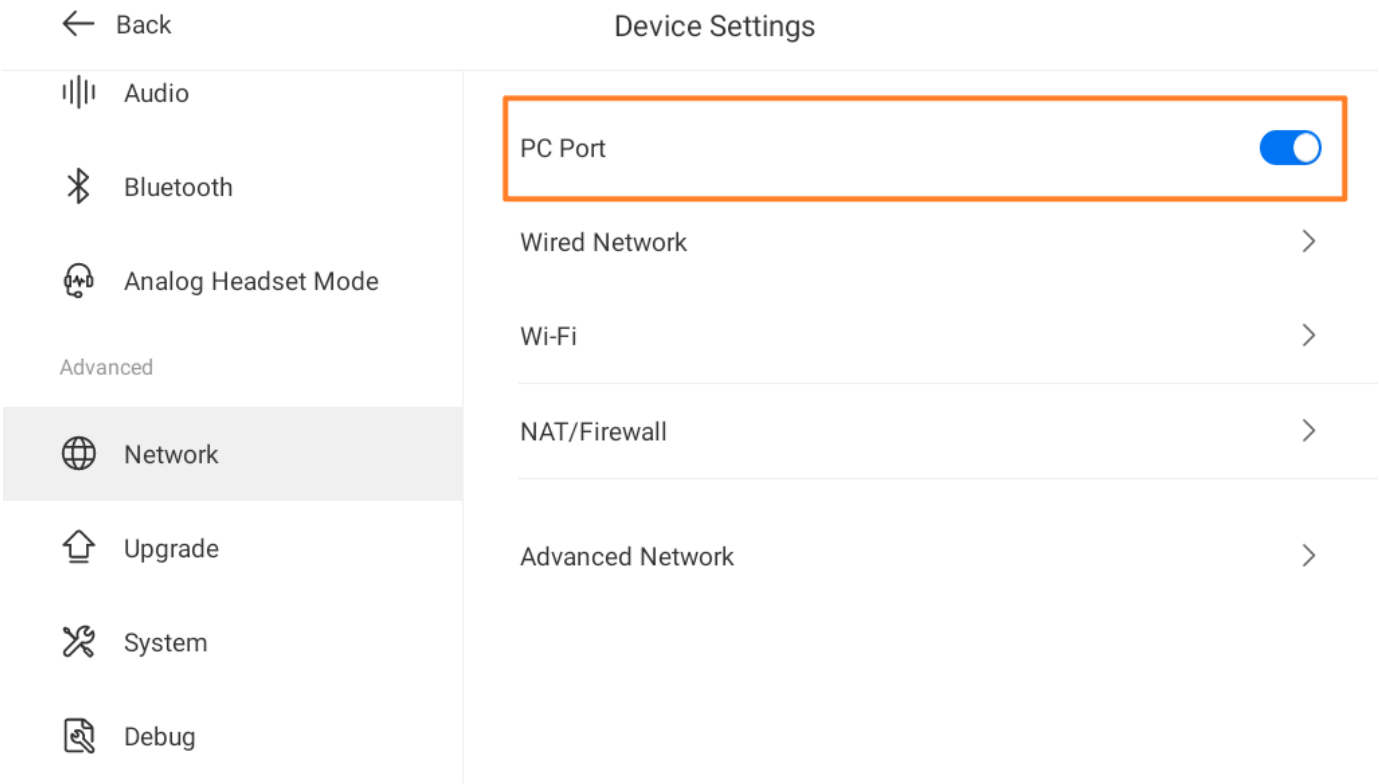


# Via Device User Interface

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. Go to **More** > **Settings** > **General** > **System Settings** > **Network** (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 | Default | Description |
|---|---|---|---|
| static.network.pc_port.en | **0**- Disabled<br>**1**-Auto Negotiation | 1 | It enables or disables the CDP feature.<br>**NOTE** |

| | | | |
|---|---|---|---|
| able[1] | | | This feature is unavailable to CP960/CP965. |
| static.network.internet_port.speed_duplex[1] | **0-** Auto Negotiation<br>**1-** Full Duplex 10Mbps<br>**2**-Full Duplex 100Mbps<br>**3**-Half Duplex 10Mbps<br>**4**-Half Duplex 100Mbps<br>**5**-Full Duplex 1000Mbps (unavailable to CP960/CP965) | 0 | It configures the transmission method of the Internet port.<br>**NOTE**<br>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<br>**1-** Full Duplex 10Mbps<br>**2**-Full Duplex 100Mbps<br>**3**-Half Duplex 10Mbps<br>**4**-Half Duplex 100Mbps<br>**5**-Full Duplex 1000Mbps | 0 | It configures the transmission method of the PC port.<br>**NOTE**<br>You can set the transmission speed to 1000Mbps/Auto Negotiation to transmit in 1000Mbps if the |

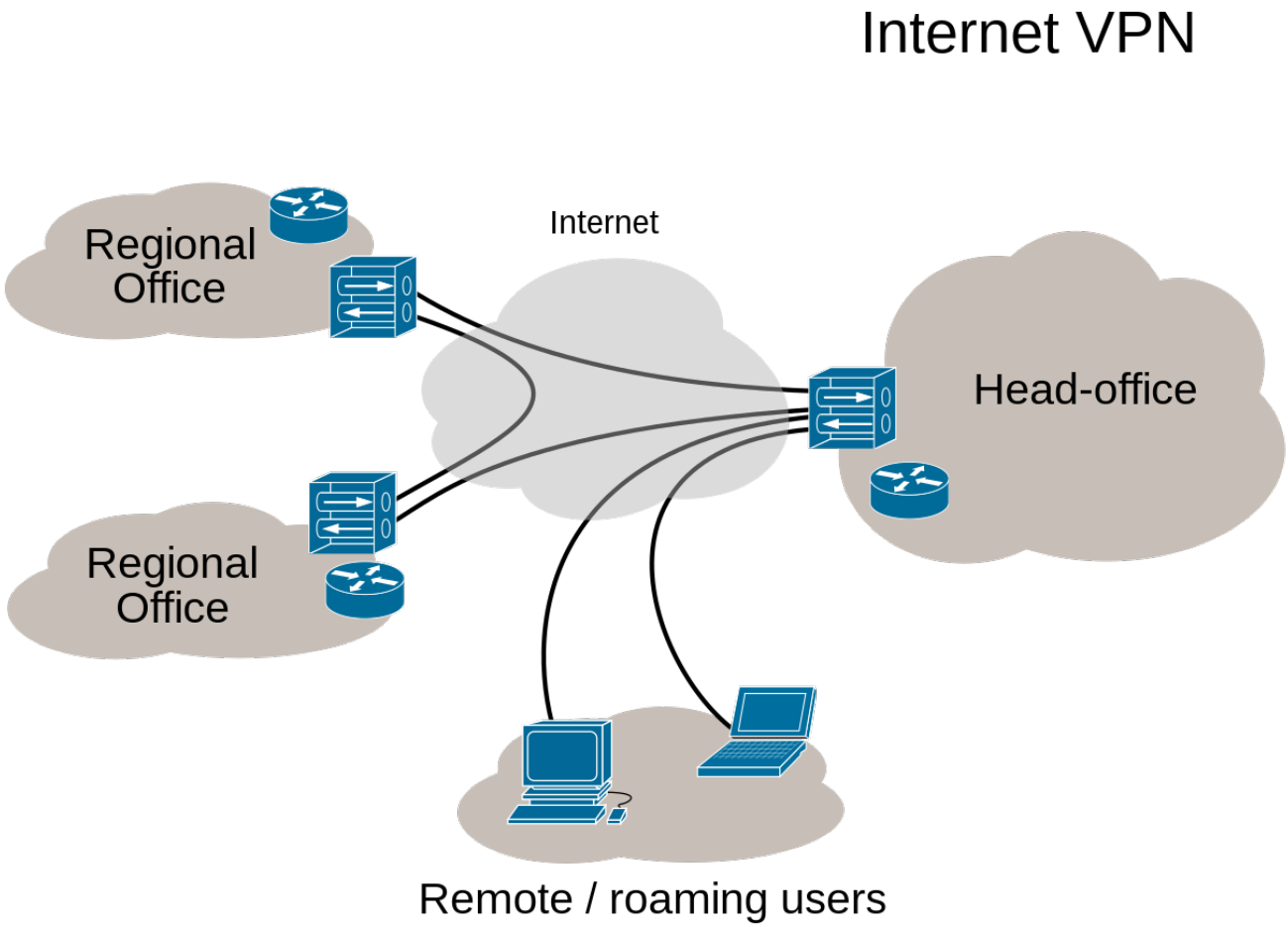
| | | | |
|---|---|---|---|
| | | | phone is connected to the switch which supports Gigabit Ethernet. We recommend that you do not change this parameter. This feature is unavailable to CP960/CP965. |
| static.network.vlan.pc_port_mode [1] | **0-** when packets are sent from the PC port to the Internet port, the phone will forward the packets directly.<br>**1**-when packets are sent from the PC port to the Internet port, and there is no VLAN tag in the packet, the phone will tag the packet with the configured tag for the PC port and then forward it. | 1 | It configures the way the phone processes packets for the PC port when VLAN is enabled on the PC port.<br>**NOTE**<br>When packets are sent from the Internet port to the PC port, remove the packet’ s tag if it is the same as the configured tag for the PC port, else forward the packets directly. This feature is unavailable to CP960/CP965. |

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

# Configure VPN

## About VPN

VPN (Virtual Private Network) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or traveling users with secure access to a central organizational network. VPN gives the organization the advantage of creating secure channels of communication, while at the same time reducing costs, improving security and increasing performance.




## Configure OpenVPN Feature on IP Phones

OpenVPN feature is disabled on IP phones by default. You can enable the OpenVPN feature using configuration files, via the web user interface or phone user interface. To use the OpenVPN feature, you also need to upload the OpenVPN TAR file to the IP phones.

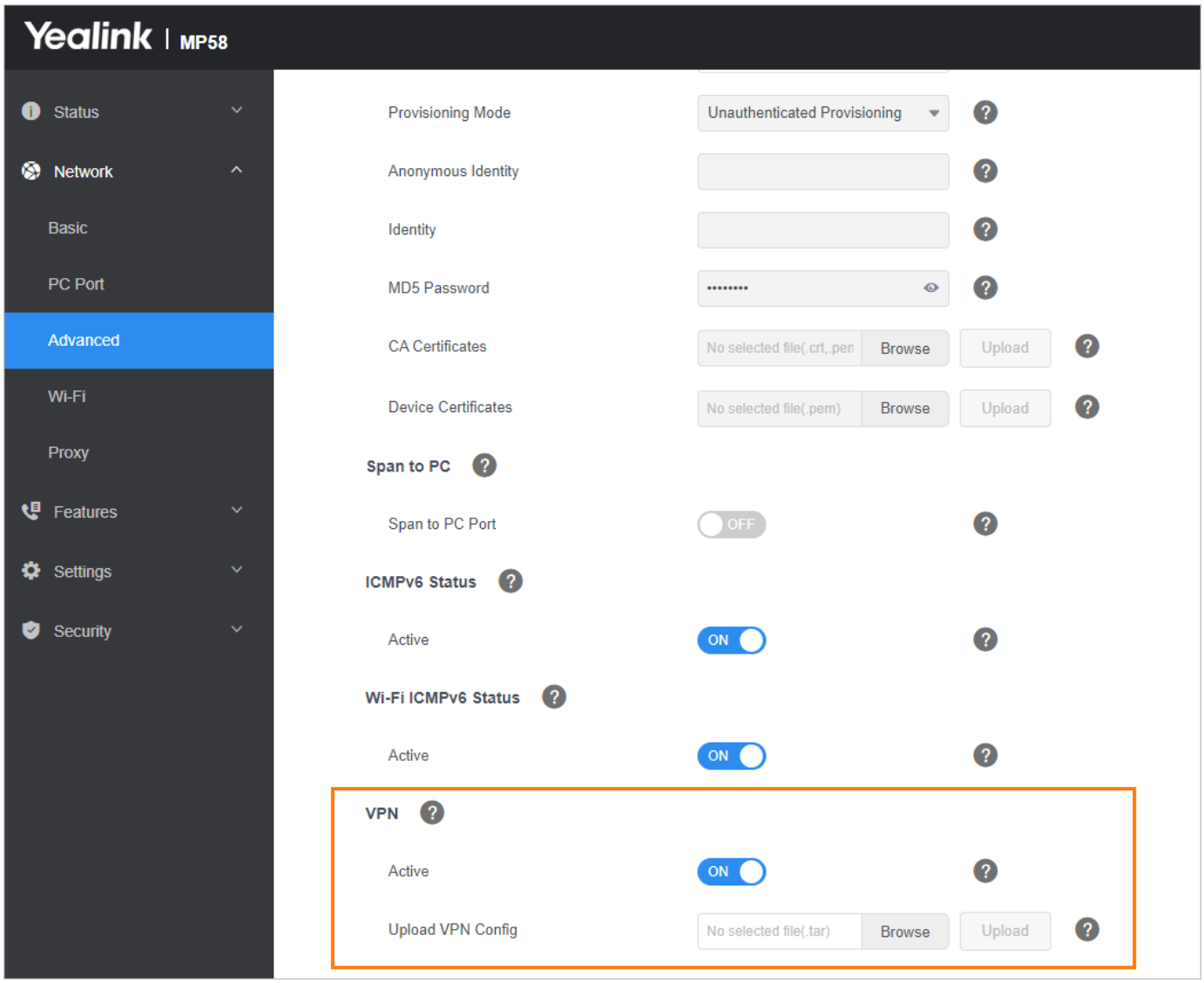
The configurations described in this section apply to the phones running the following firmware version.

- VP59: 91.30.0.45 or later.

- MP58/MP56/MP54: 122.30.0.30 or later.
- MP5X E2: 176.30.0.3

## Set via the Web User Interface

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




## Configuration parameter

static.network.vpn_enable
static.openvpn.url

| Parameter | Permitted Values | Default | Description |
|---|---|---|---|
| static.network.vpn_enable[1] | **0**-Disabled<br>**1**-Enabled | 0 | It enables or disables the OpenVPN feature. |

| | | | |
|---|---|---|---|
| static.openvpn.url | URL within 511 characters | Blank | It configures the access URL of the *.tar file for OpenVPN. |

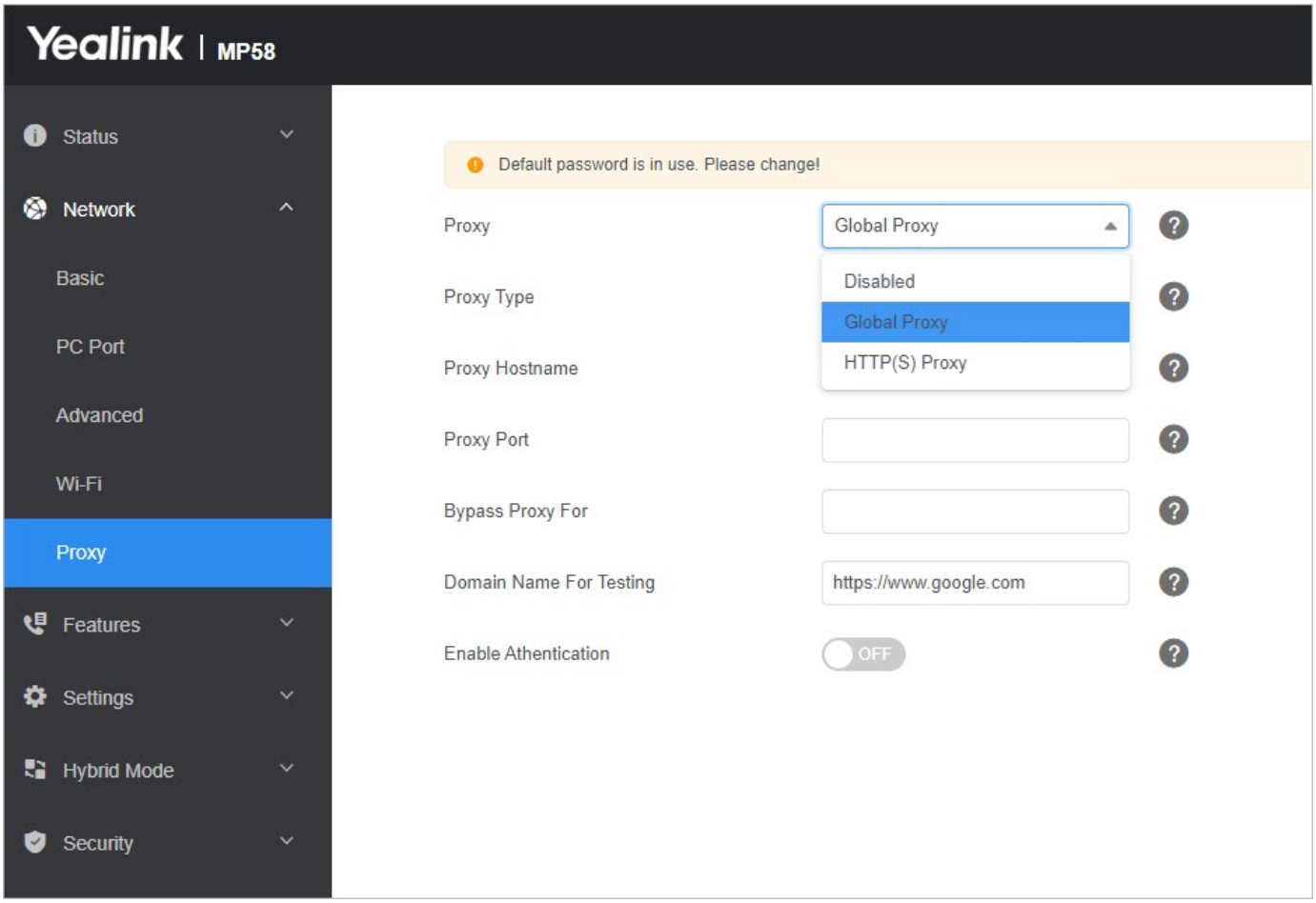
[1]If you change this parameter, the phone will reboot to make the change take effect.

# Configure Proxy Server

## Via Web User Interface

**Procedure**

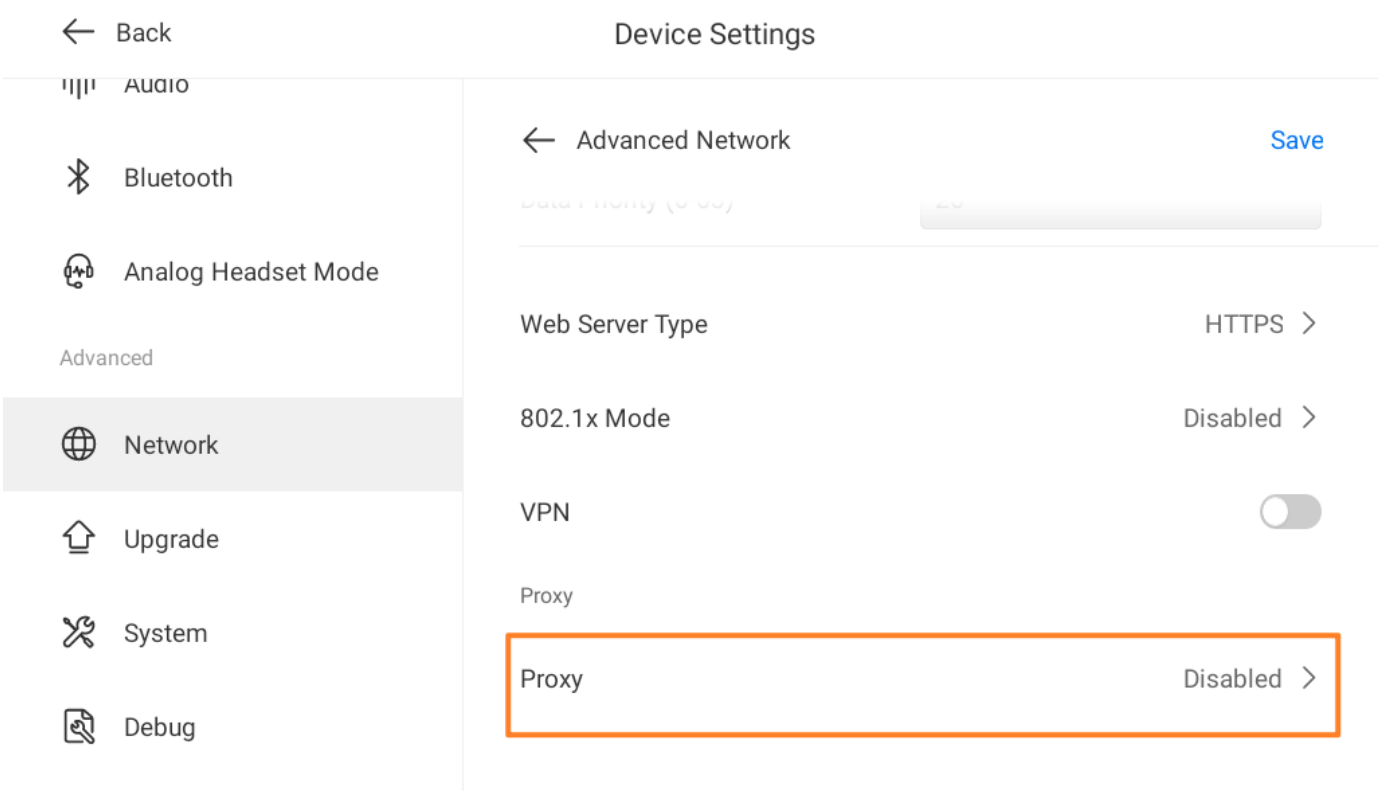
1. Log in to the phone web user interface as an admin.
2. Go to **Network** > **Proxy** > **Proxy**.




## Via Device User Interface

**Procedure**

1. Tap the account avatar and go to **More** > **Settings** > **General** > **System Settings** > **Network** (Admin only, default password: admin) > **Advanced Network** > **Proxy**.




# 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_addres
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.network.proxy.mode[1] | **0**- Disabled<br>**1**- Global proxy, you can manually configure the proxy server information.<br>**2**- HTTP(S) proxy, you can obtain proxy server information through PAC file. | 2 | It enables or disables the proxy server. |
| static.network.proxy.type | **0**- SOCKS5<br>**1**- HTTP CONNECT | 0 | It configures the proxy type.<br>**NOTE**<br>It works only if "static.network.proxy.mode" is set to 1 (Enabled). |
| static.network.proxy.hostname | String within 99 characters | Blank | It configures the IP address or domain name of the proxy server.<br>**NOTE**<br>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.<br>**NOTE**<br>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.<br>NOTE<br>It works only if "static.network.proxy.mode" is set to 1 (Enabled). |
| static. | URL within 511 | http | It configures the test URL for the proxy server. After |

| | | | |
|---|---|---|---|
| network.proxy.test_address | characters | s://www.google.com | connecting to the proxy server, the phones try to send a network request to the specified URL. If the URL cannot be accessed, the phone fails to connect to the proxy server.<br>NOTE<br>It works only if "static.network.proxy.mode" is set to 1 (Enabled). |
| static.network.proxy.enable | **0**-Disabled<br>**1**-Enabled | 0 | It enables or disables the proxy server authentication.<br>NOTE<br>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.<br>NOTE<br>It works only if "static.network.proxy.mode" is set to 2 (Enabled), "static.network.proxy.mode" is set to 1 (Disabled) and "static.network.proxy.http.set_from" is set to 1. |
| static.network.proxy.wpad | **0**-Disabled<br>**1**-Enabled | 1 | It enables or disables the WPAD to obtain the PAC file dynamically.<br>NOTE<br>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.<br>**1**- PAC URL, enter the PAC URL manually.<br>**2**- PAC File, upload PAC file directly. | 0 | It configures the sources where the proxy set comes.<br>NOTE<br>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[1] | String within 256 characters | Blank | It configures the username for proxy server authentication. |
| 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.<br>**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.

# Wi-Fi

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

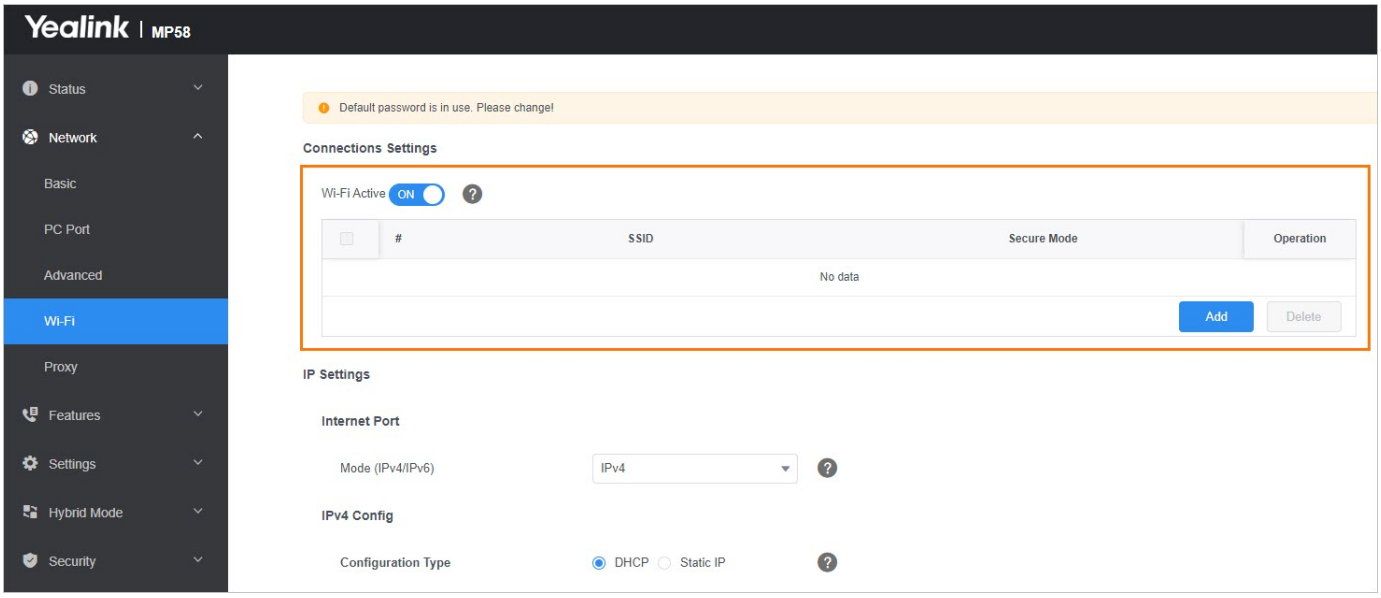
> TIP
> For MP54, make sure the Wi-Fi USB Dongle WF50 is connected to the device.

## 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)**.

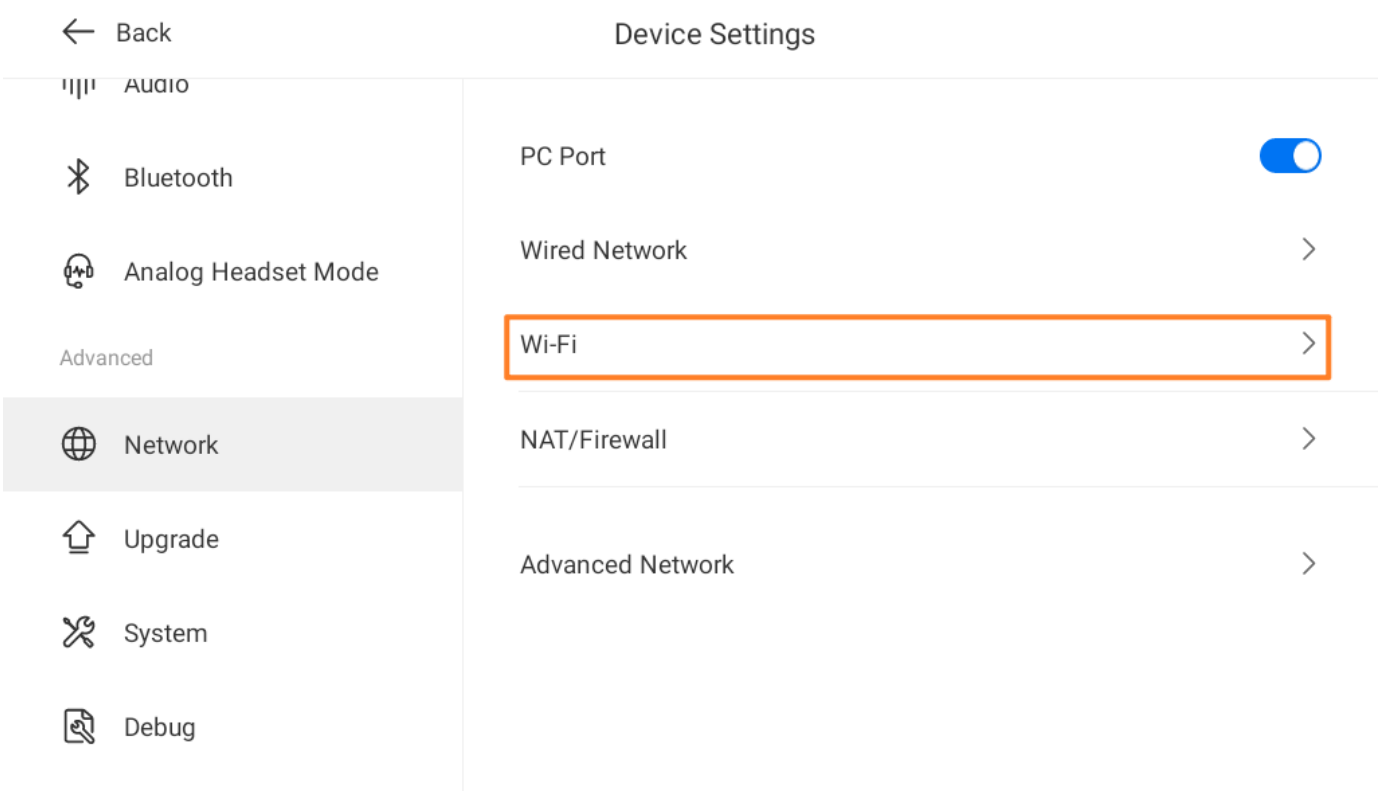



## Via Device User Interface

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. Go to **More** > **Settings** > **General** > **System Settings** > **Network** (Admin only, default password: admin) > **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<br>**1**-Enabled | 1 | It enables or disables the Wi-Fi feature. |

| | | | |
|---|---|---|---|
| static.wifi.enable | **0**-Disabled<br>**1**-Enabled | 0 | It activates or deactivates the Wi-Fi mode.<br>NOTE<br>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.<br>NOTE<br>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.<br>SSID is a unique identifier for accessing wireless access points.<br>NOTE<br>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.<br>5 is the highest priority, 1 is the lowest priority.<br>NOTE<br>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 | NONE | It configures the security mode of a specific wireless network. |

| | | | |
|---|---|---|---|
| | EAP | | NOTE<br>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 | NONE | It configures the encryption type of a specific wireless network.<br>If static.wifi.X.security_mode is set to NONE, the permitted value of this parameter is NONE.<br>If static.wifi.X.security_mode is set to 802.1x EAP, the permitted values of this parameter are PEAP, TLS, TTLS, or PWD.<br>NOTE<br>It works only if "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.<br>NOTE<br>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.<br>NOTE<br>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.<br>NOTE<br>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.<br>NOTE<br>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.

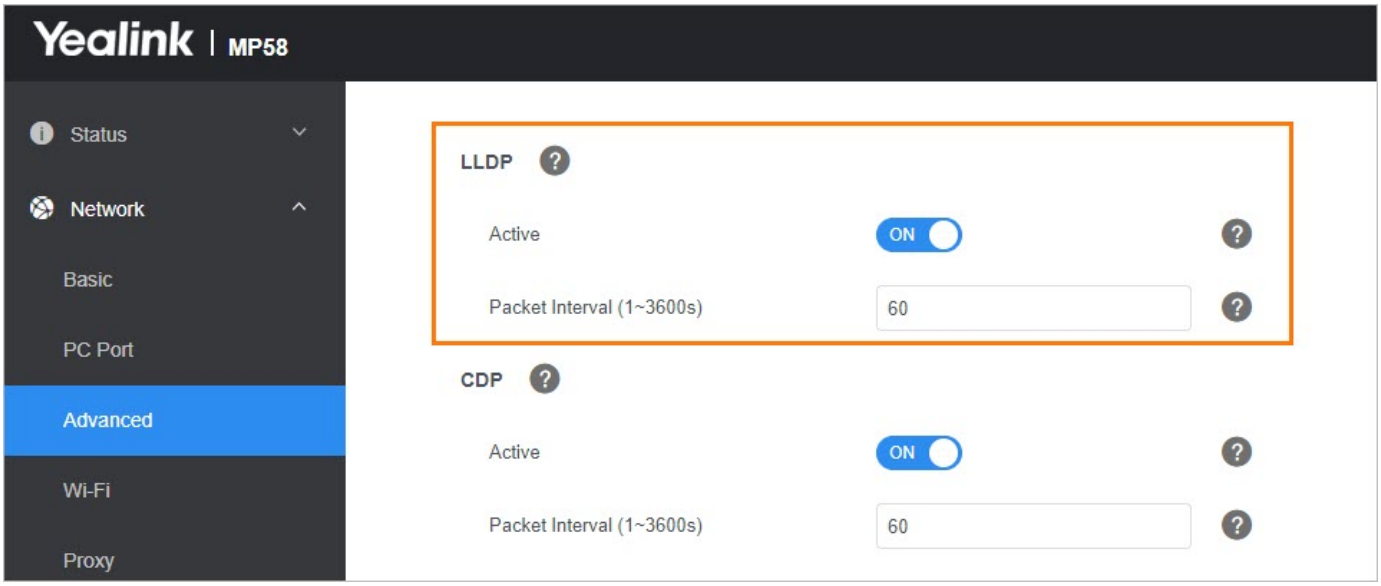
When the LLDP feature is enabled on the devices, the devices periodically advertise their information to the directly connected LLDP-enabled switch. The devices can also receive LLDP packets from the connected switch. When the application type is “voice”, the devices decide whether to update the VLAN

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**

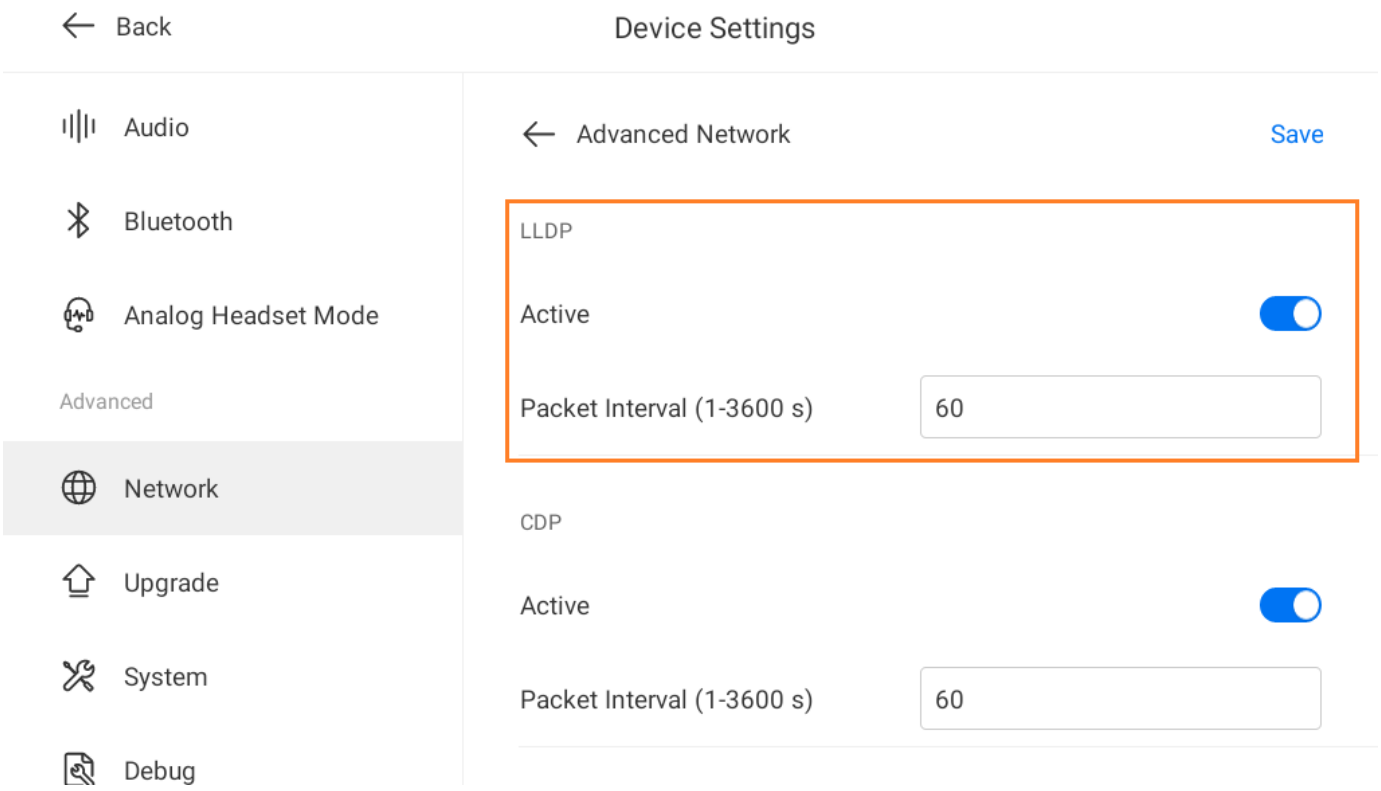
1. Log in to the phone web user interface as an admin.
2. Go to **Network** > **Advanced** > **LLDP**.




# Via Device User Interface

**Procedure**

1. Go to **More** > **Settings** > **General** > **System Settings** > **Network** (Admin only, default password: admin) > **Advanced Network** > **LLDP**.




# Via Auto Provisioning

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

| |
|---|
| static.network.lldp.enable<br>static.network.lldp.packet_interval |

| Parameter | Permitted Values | Default | Description |
|---|---|---|---|
| static.network.lldp.enable[1] | **0**- Disabled<br>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.<br>NOTE<br>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.

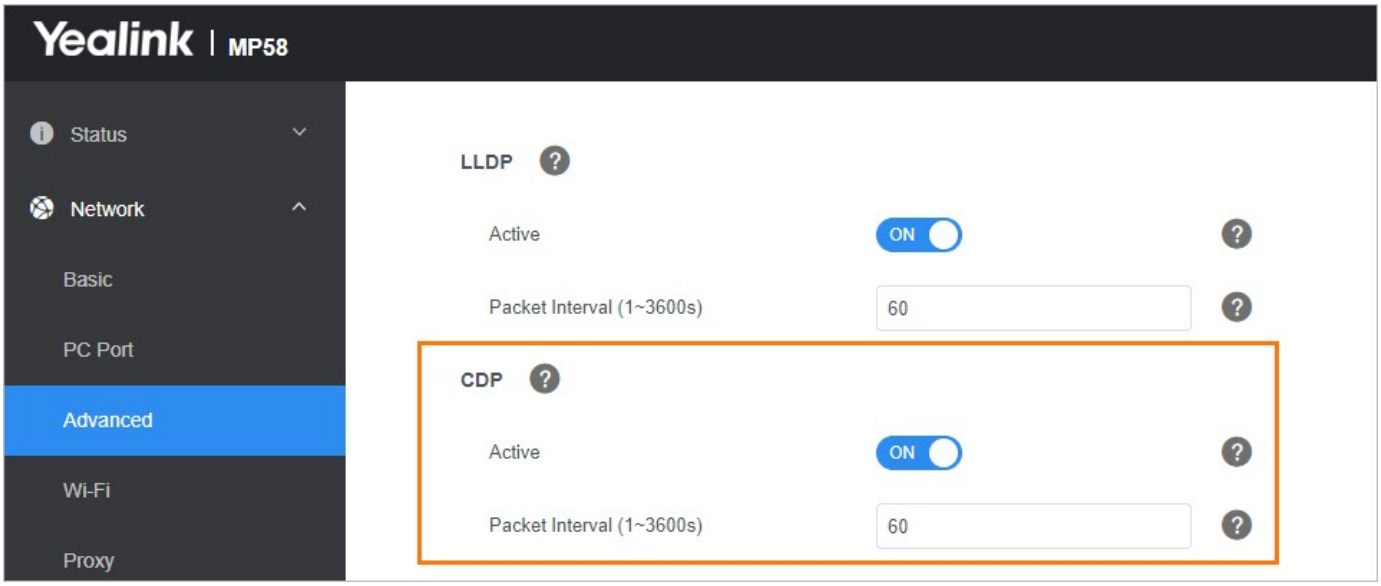
# Configure CDP

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.

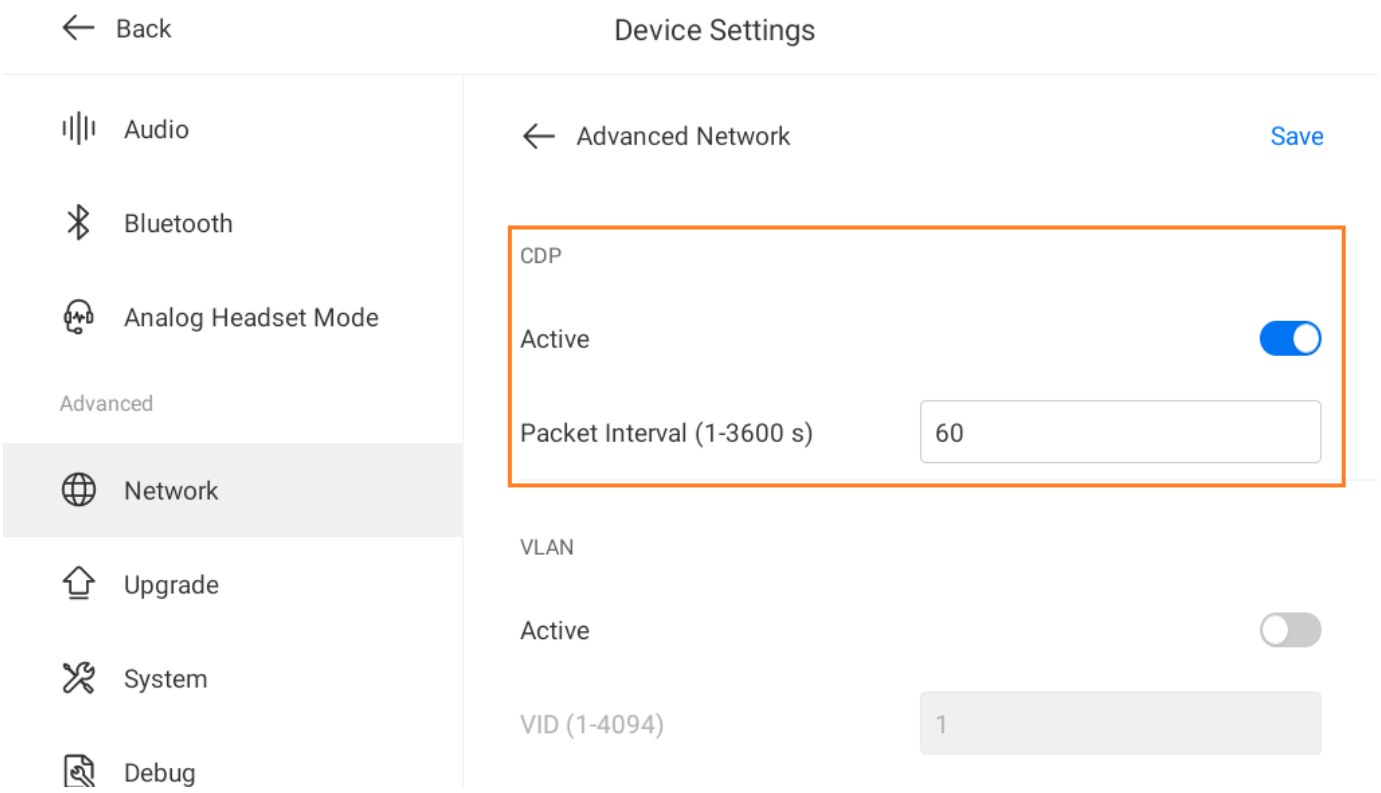
## Via Web User Interface

1. Log in to the phone web user interface as an admin.
2. Go to **Network** > **Advanced** > **CDP**.




## Via Device User Interface

1. Go to **More** > **Settings** > **General** > **System Settings** > **Network** (Admin only, default password: admin) > **Advanced Network** > **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<br>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.<br>NOTE<br>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.

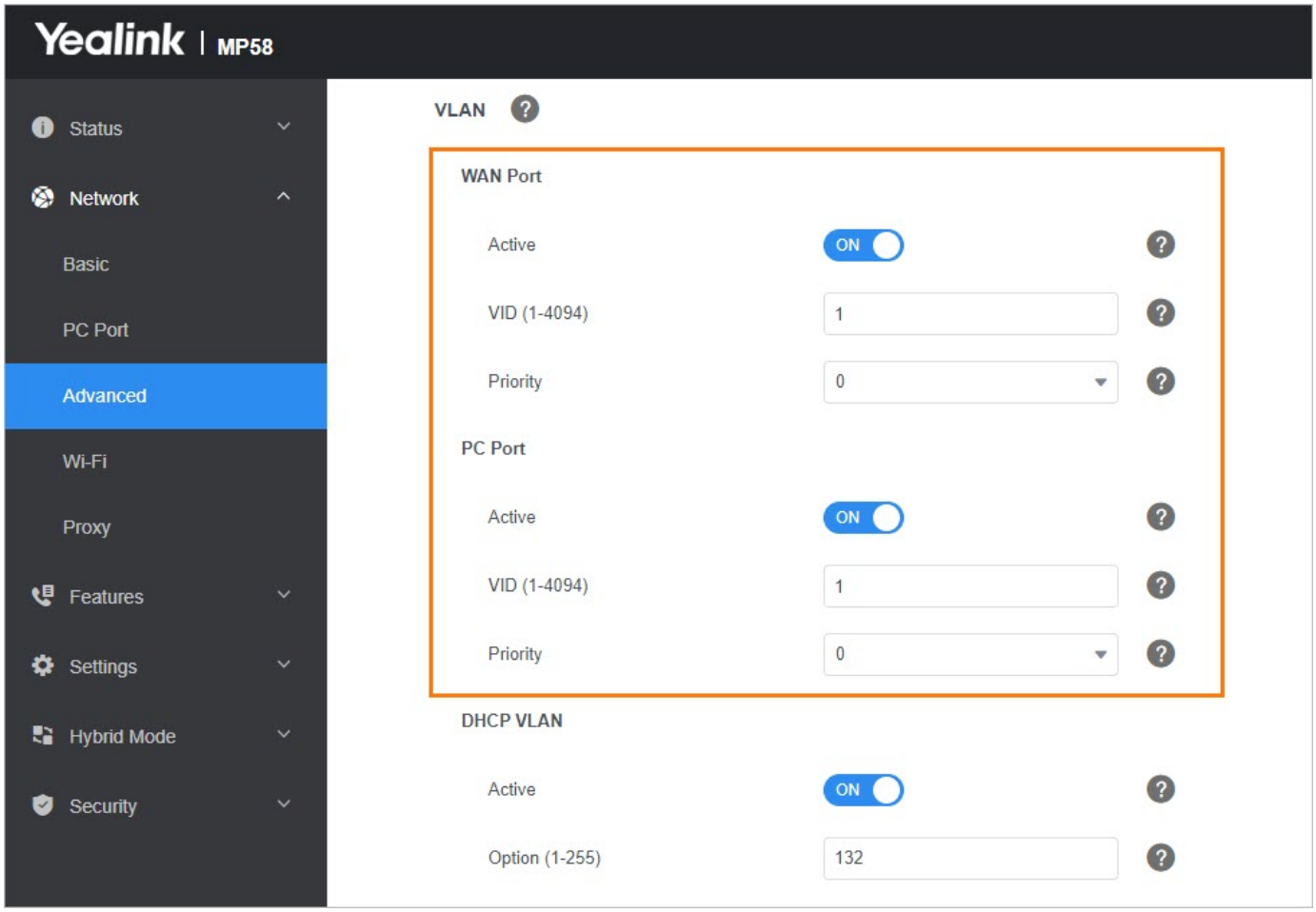
The PC port is unavailable to CP960/CP965, and you can only configure VLAN for the Internet port manually.

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

## Via Web User Interface

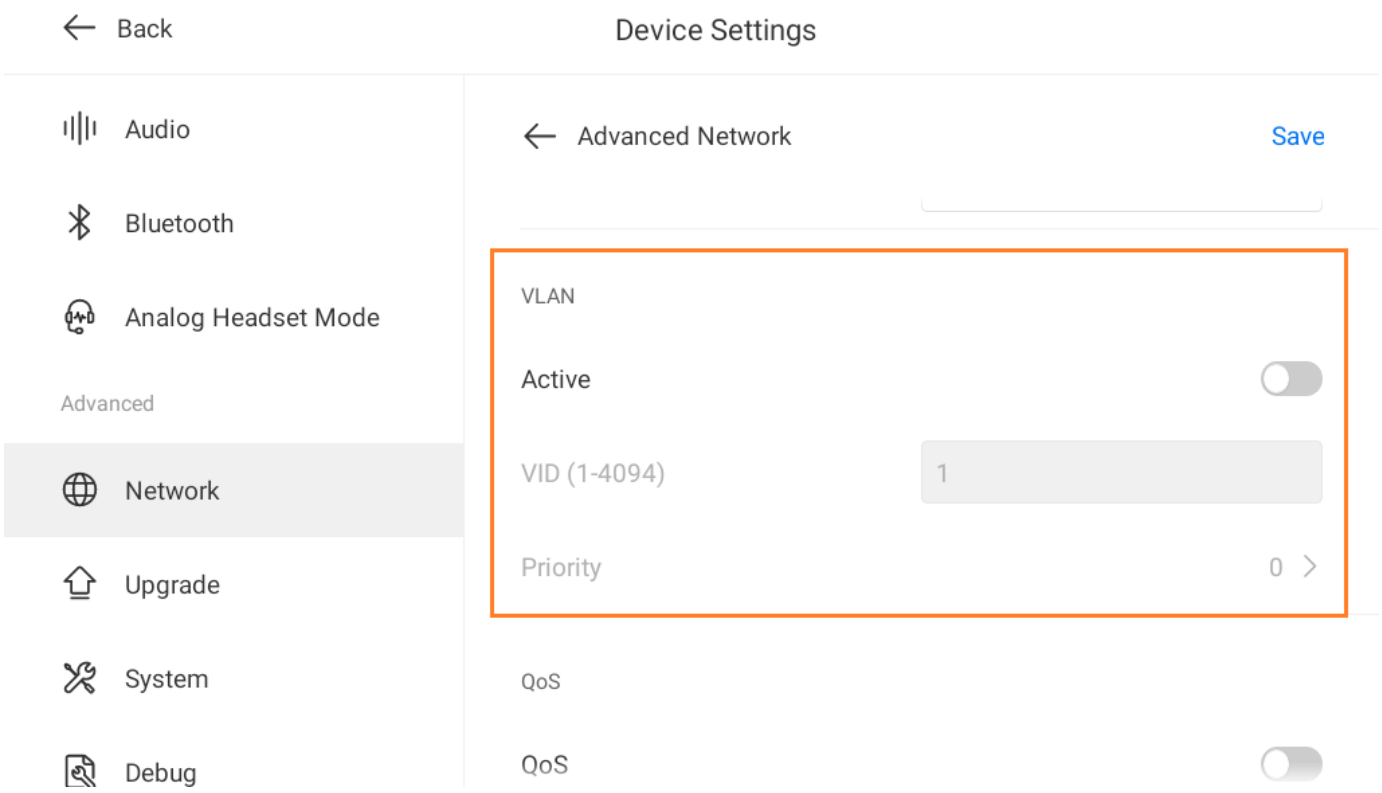
1. Log in to the phone web user interface as an admin.

2. Go to **Network** > **Advanced** > **VLAN** > **WAN Port**/**PC Port**.




# Via Device User Interface

1. Go to **More** > **Settings** > **General** > **System Settings** > **Network** (Admin only, default password: admin) > **Advanced Network** > **VLAN**.



# 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<br>**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.<br>NOTE<br>It works only if "static.network.vlan.internet_port_enable" is set to 1 (Enabled). |
| 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.<br>NOTE<br>It works only if "static.network.vlan.internet_port_enable" is set to 1 (Enabled). |
| static.network.vlan.pc_port_enable[1] | **0**-Disabled<br>**1**-Enabled | 0 | It enables or disables the VLAN for the PC port.<br>NOTE<br>It works only if "static.network.pc_port.enable" is set to 1 |

| | | | |
|---|---|---|---|
| | | | (Auto Negotiation).<br>This feature is not available to CP960/CP965. |
| static.network.vlan.pc_port_vid[1] | Integer from 1 to 4094 | 1 | It configures the VLAN ID for the PC port.<br>NOTE<br>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.<br>NOTE<br>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).<br>This feature is not available to CP960/CP965. |

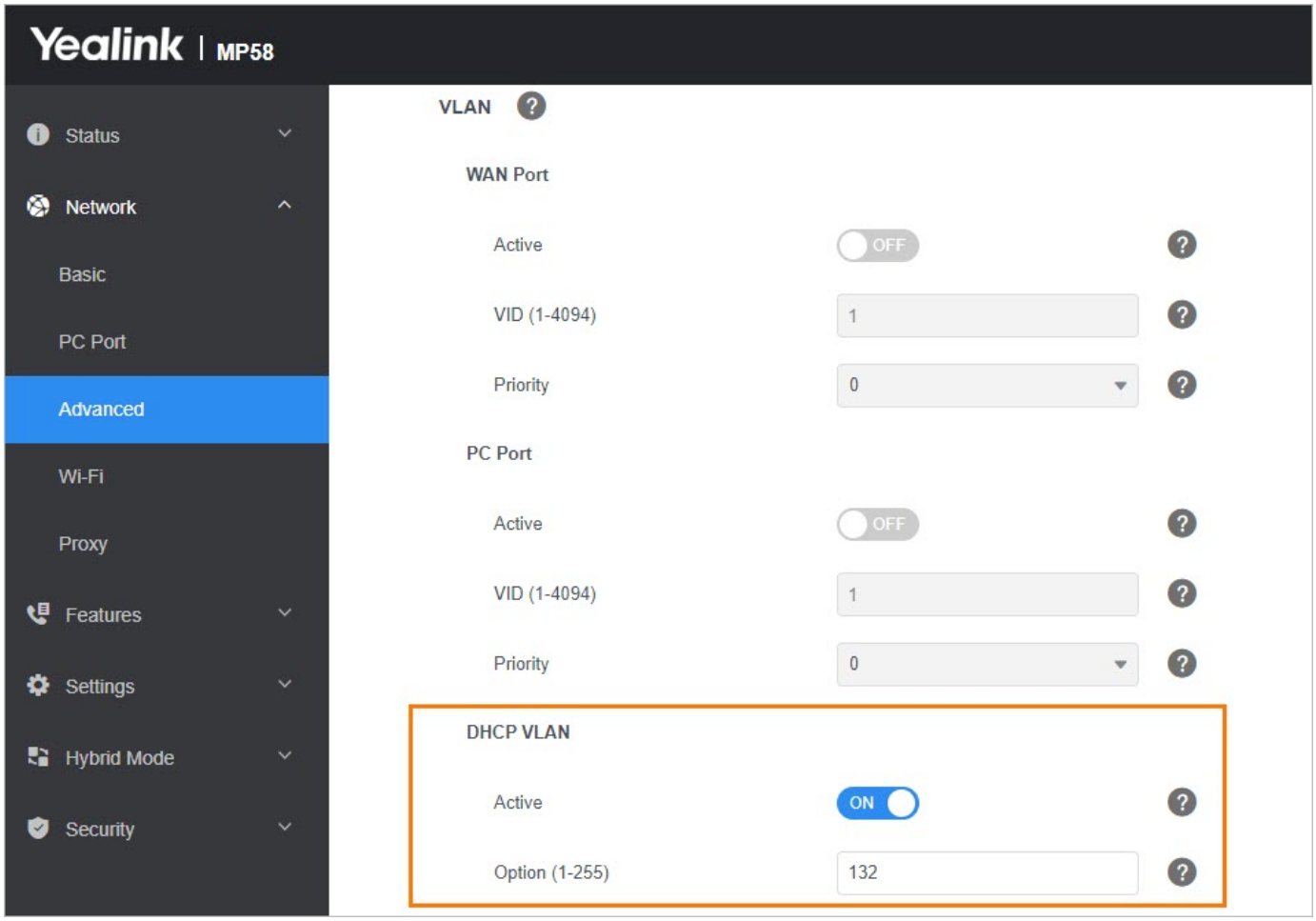
[1] If you change this parameter, the device will reboot to make the change take effect.

# Configure DHCP VLAN

Yealink Zoom 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 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<br>**1**-Enabled | 1 | It enables or disables the DHCP VLAN discovery feature on the device. |
| static.network.vlan.dhcp | Integer from 1 | 132 | It configures the DHCP option from which the device obtains the VLAN settings. You can configure at most five DHCP options and |

| | | | |
|---|---|---|---|
| _option | to 255 | | separate them by commas. |

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

# 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<br>**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 Zoom 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 Zoom 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 Zoom 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<br>**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.<br>Multiple DHCP options are separated by commas.<br>NOTE<br>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 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 that connecting to the secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server address. For more information, refer to RFC 3925.

If a single alternate DHCP server responds, this is functionally equivalent to the scenario where the primary DHCP server responds with a valid provisioning server address. If no DHCP server responds, the INFORM query process will retry and until the time is out.

# DHCP Option 42 and Option 2

Yealink 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. |

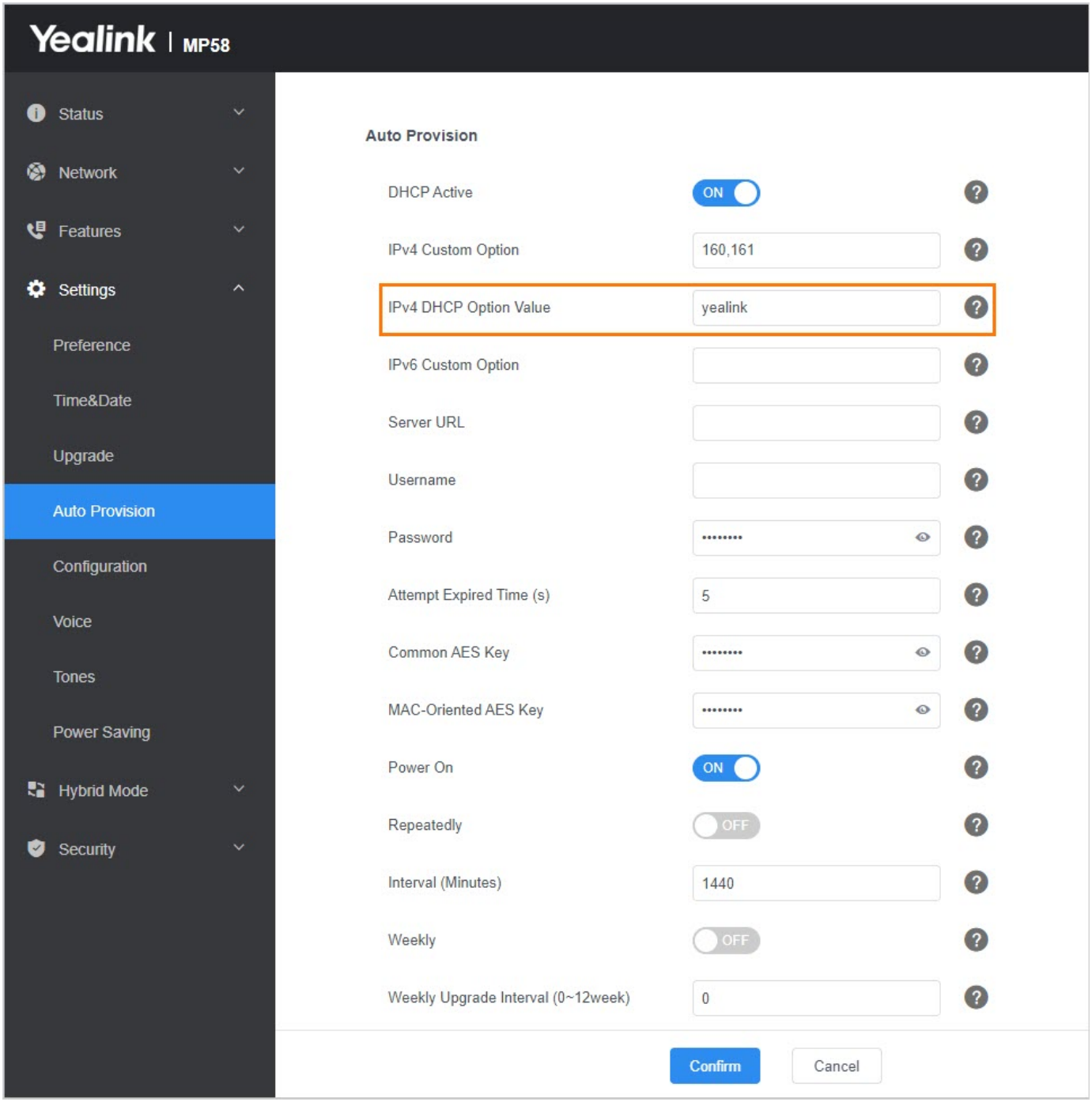
[1]If you change this parameter, the phone will reboot to make the change take effect.

# 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 **Network** > **Settings** > **IPv4 DHCP Option Value**.




# 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. |

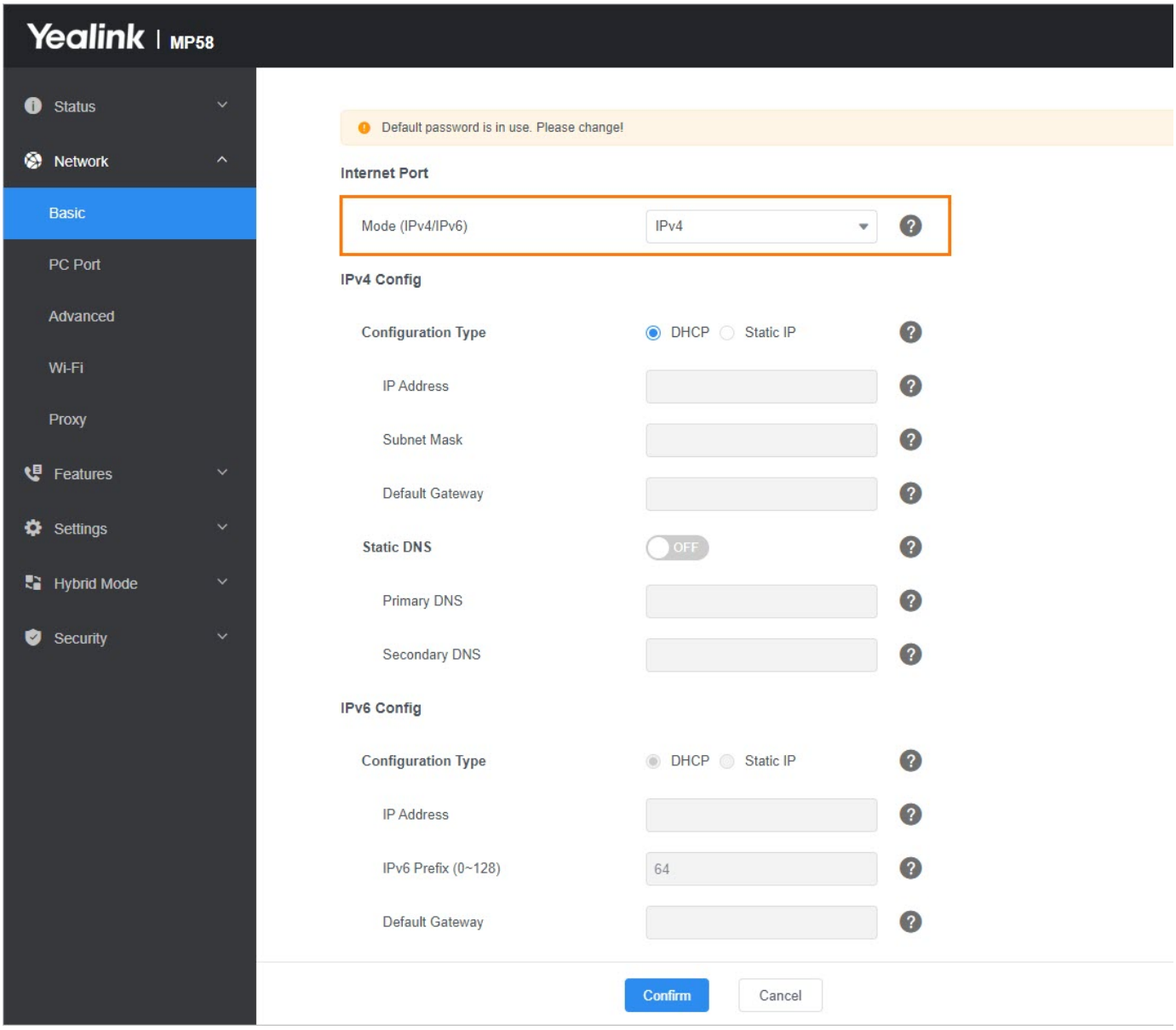
# IPv4 and IPv6 Network Settings

## IP Addressing Mode Configuration Edit

### 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)**.

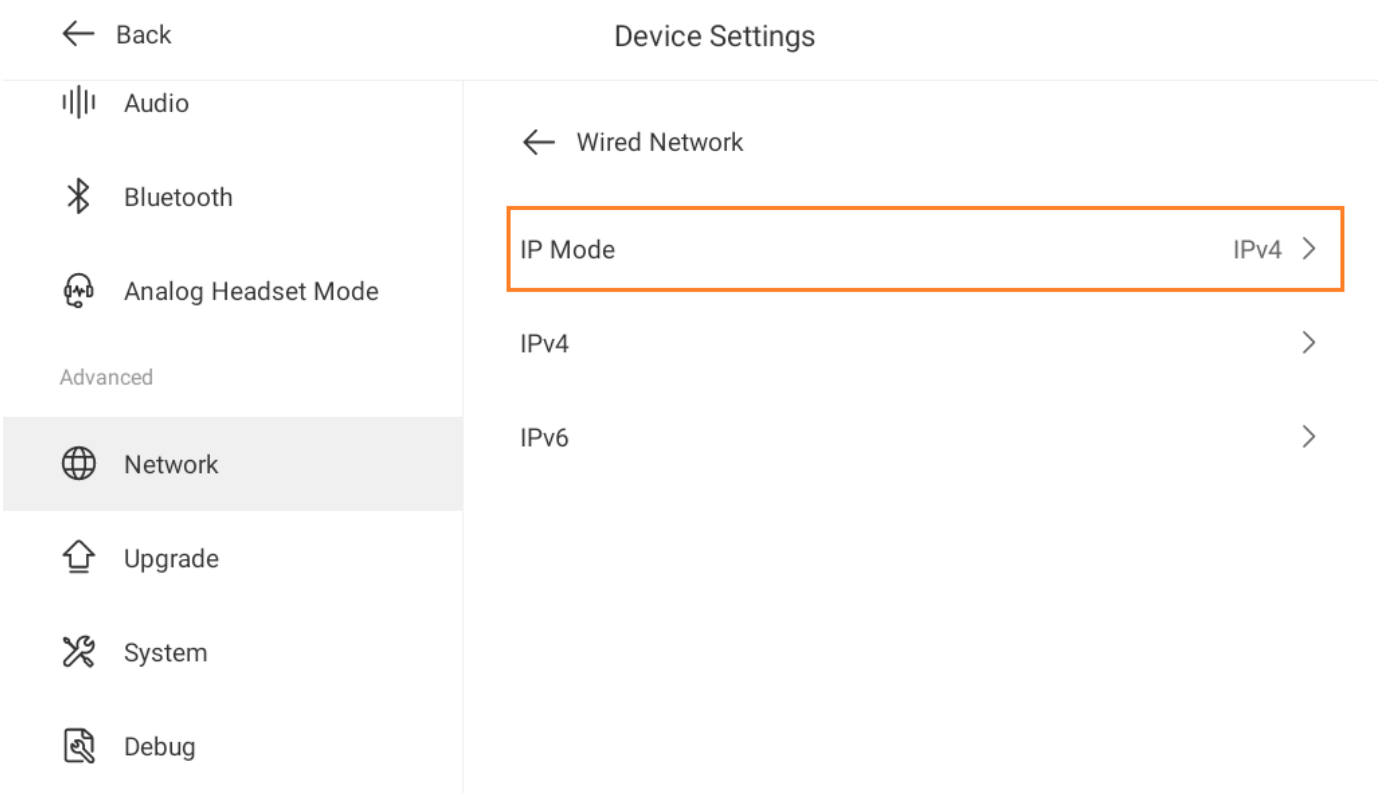



### Via Device User Interface

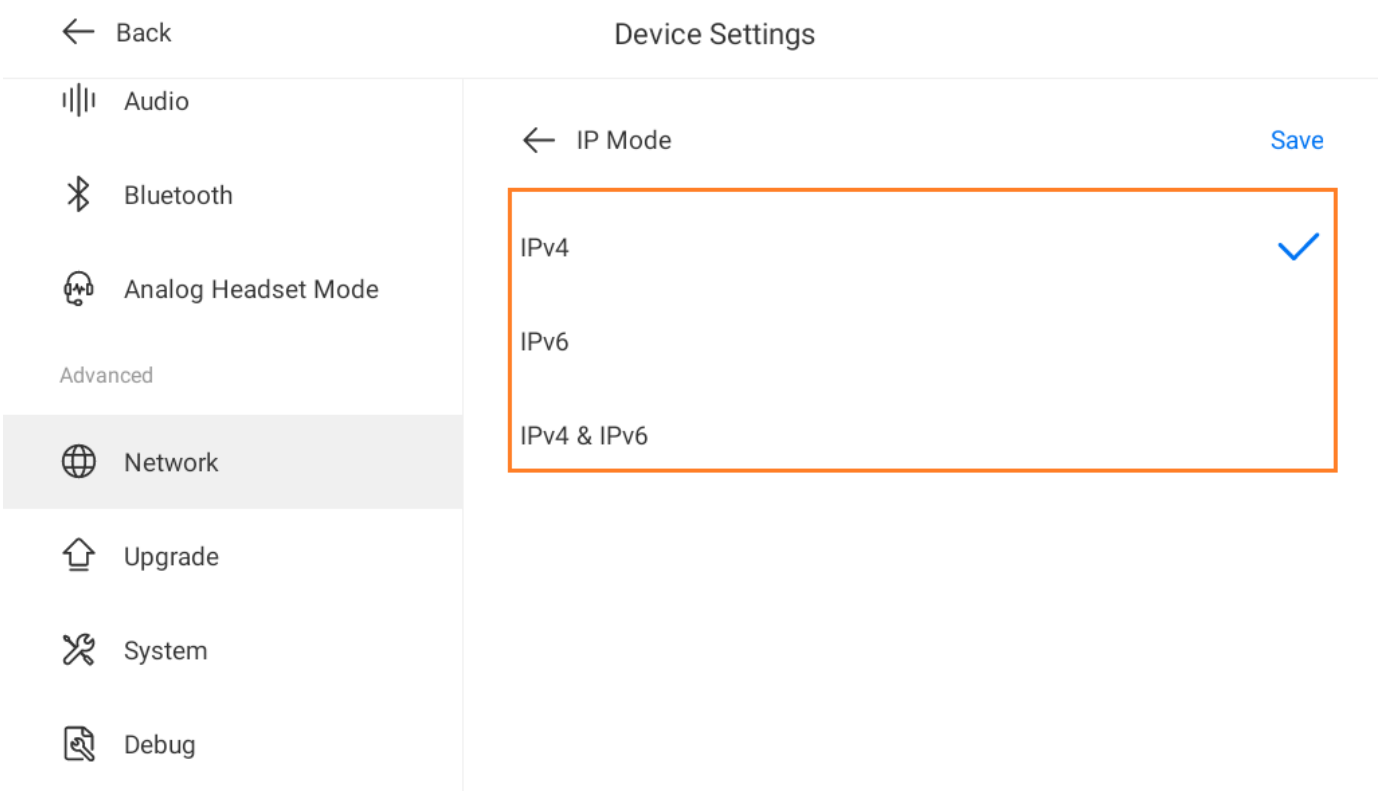
**Procedure**

1. Go to **More** > **Settings** > **General** > **System Settings** > **Network** (Admin only, default password:

admin) > **Wired Network** > **IP Mode**.




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




# Auto Provisioning

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

| |
|---|
| static.network.ip_address_mode |

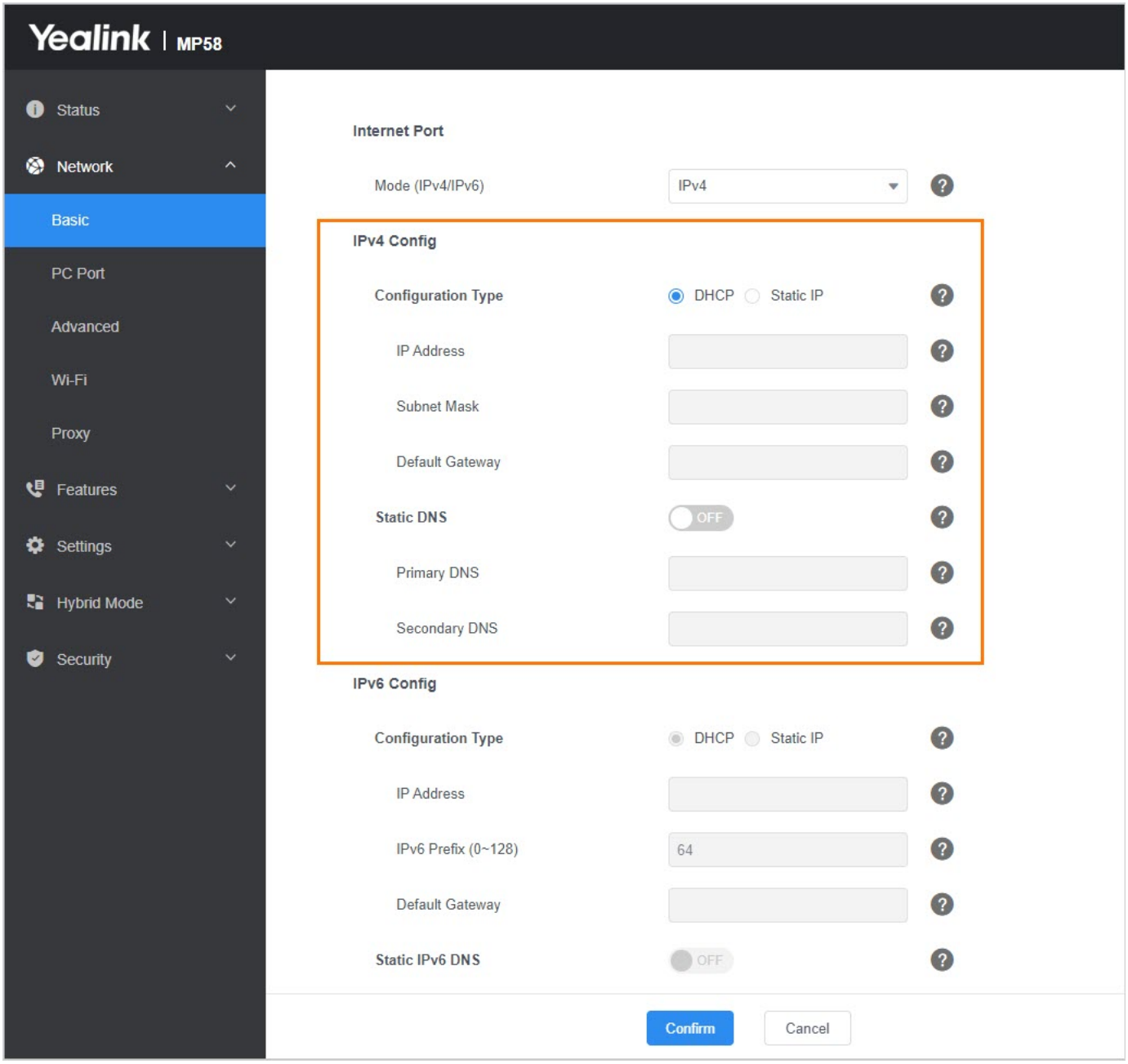
| Parameters | Permitted Values | Default | Description |
| --- | --- | --- | --- |
| static.network.ip_address_mode | **0**-IPv4<br>**1**-IPv6<br>**2**-IPv4 & IPv6 | 0 | It configures the IP addressing mode. |

# IPv4 Configuration

## Via Web User Interface

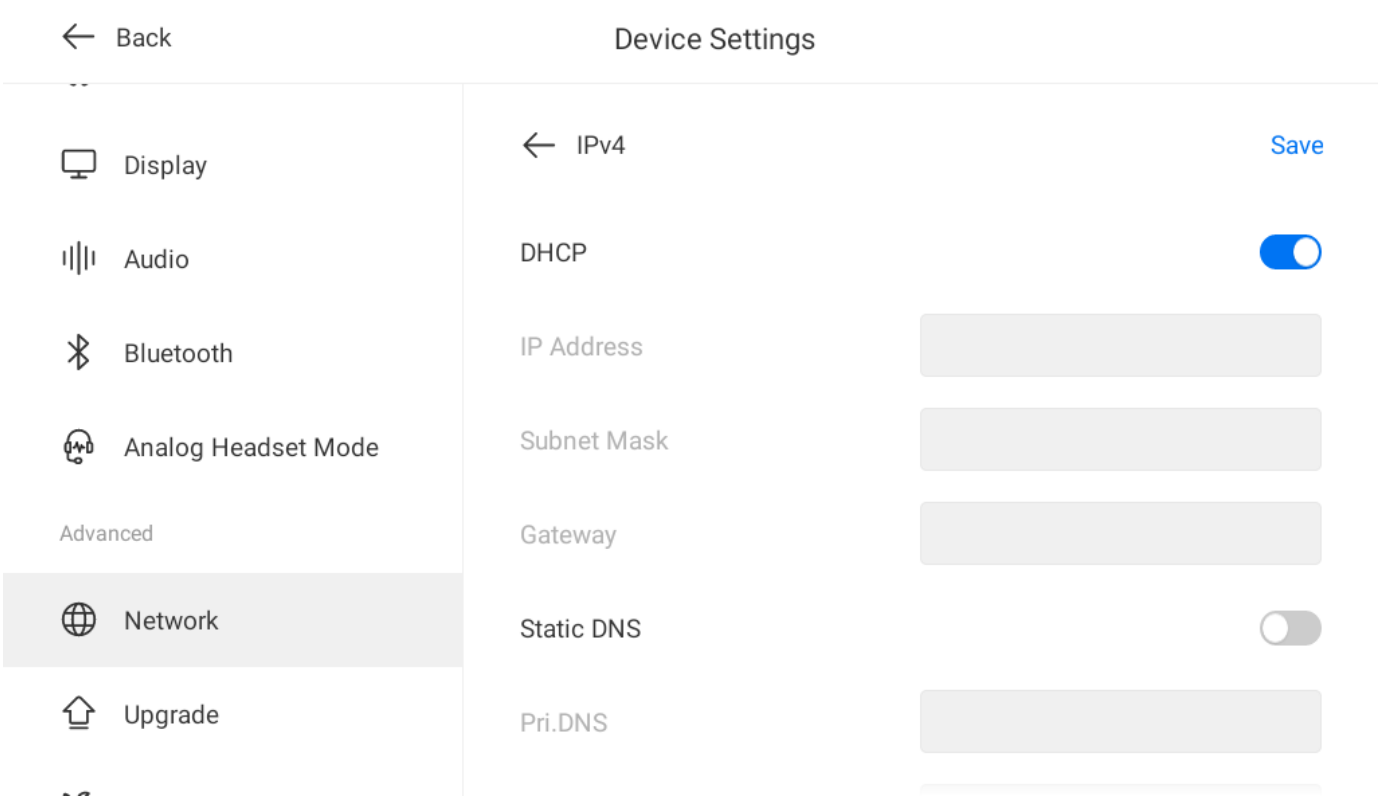
**Procedure**

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




# Via Device User Interface

1. Go to **More** > **Settings** > **General** > **System Settings** > **Network** (Admin only, default password: admin) > **Wired Network** > **IPv4**.




2. Save the change.

# Auto Provisioning

static.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<br>**2**-Static IP | 0 | It configures the Internet port type for IPv4.<br>NOTE<br>It works only if "static.network.ip_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.<br>NOTE<br>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.<br>NOTE<br>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.<br>NOTE<br>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.<br>**1**-On, the phone will use manually configured static IPv4 | 0 | It triggers the static DNS feature to on or off.<br>NOTE<br>It works only if "static.network.internet_port.type" is set to 0 (DHCP). |

| | | | |
|---|---|---|---|
| | DNS. | | |
| static.network.primary_dns[1] | IPv4 Address | Blank | It configures the primary IPv4 DNS server.<br>NOTE<br>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 "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.<br>NOTE<br>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 "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

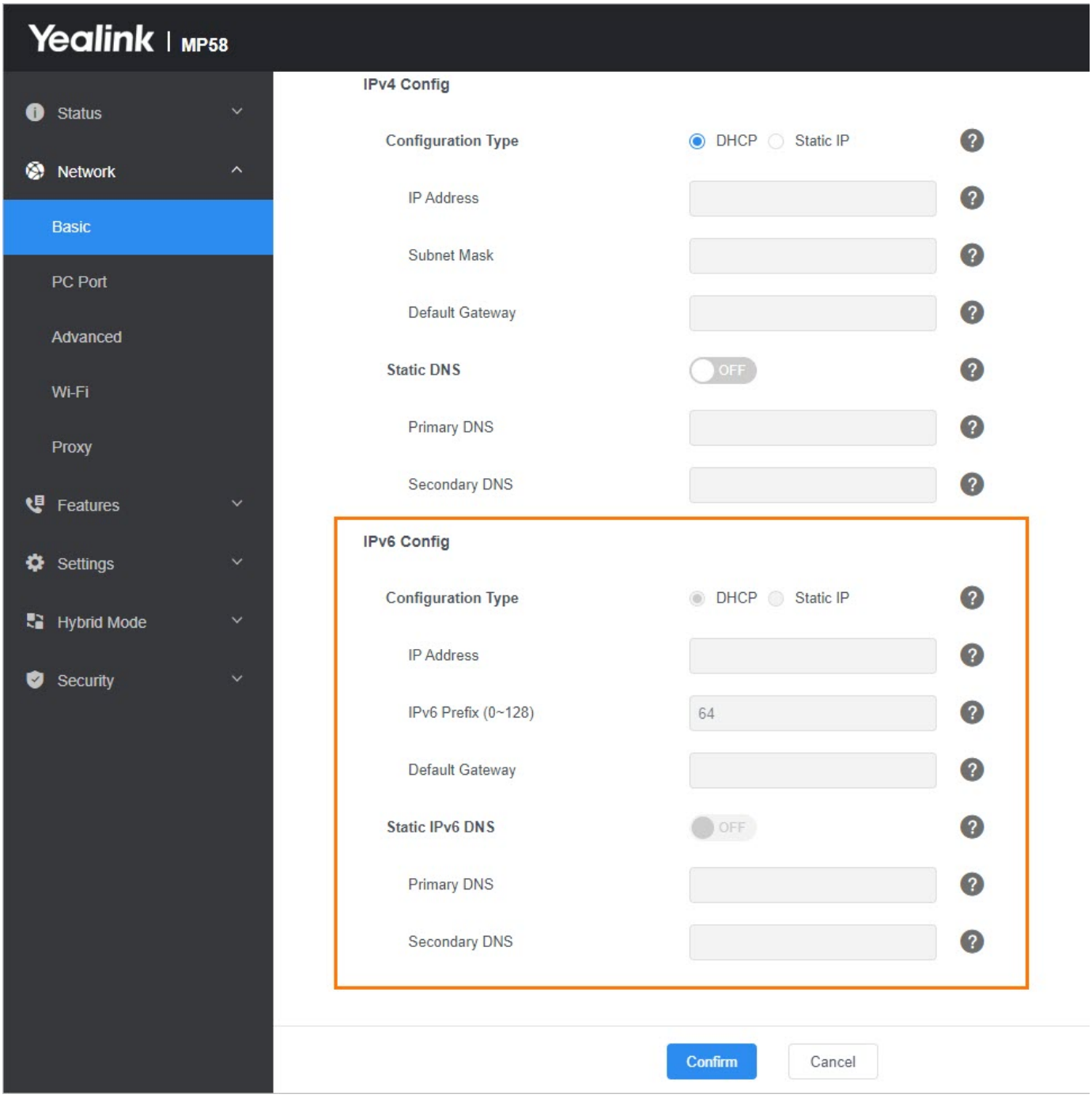
If you configure the network settings on the phone for an IPv6 wired network, you can set up an IP address for the phone by using SLAAC (ICMPv6), DHCPv6 or by manually entering an IP address. Ensure that your network environment supports IPv6. Contact your ISP for more information.

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**

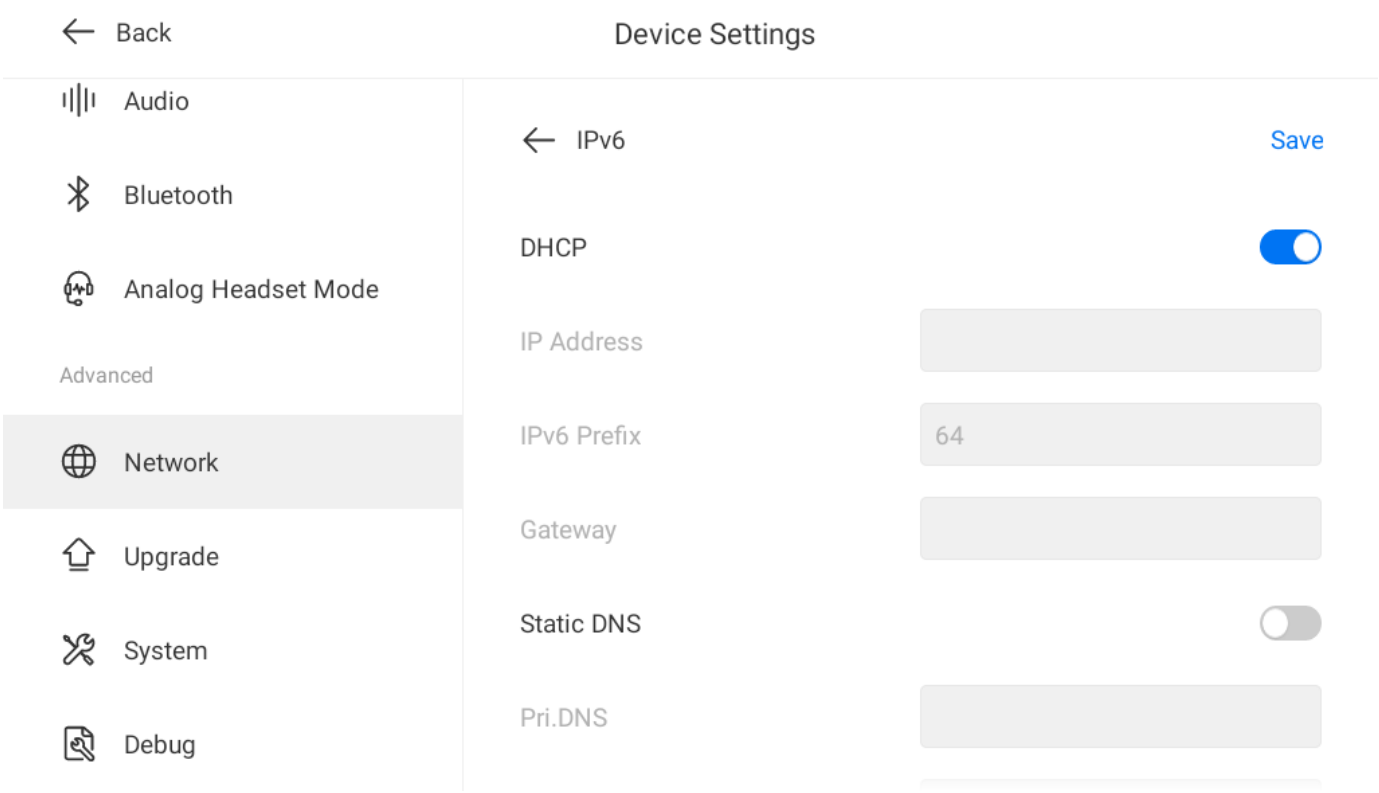
1. Log in to the phone web user interface as an admin.
2. Go to **Network** > **Basic** > **IPv6 Config**.




# Via Device User Interface

### Procedure

1. Go to **More** > **Settings** > **General** > **System Settings** > **Network** (Admin only, default password: admin) > **Wired Network** > **IPv6**.




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<br>**1**-Static IP | 0 | It configures the Internet port type for IPv6.<br>NOTE<br>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.<br>NOTE<br>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.<br>NOTE<br>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.<br>NOTE<br>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.<br>**1**-On, the phone | 0 | It triggers the static IPv6 DNS feature to turn on or off.<br>NOTE<br>It works only if "static.network.ipv6_internet_port.type" is set to 0 (DHCP). |

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

# 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:

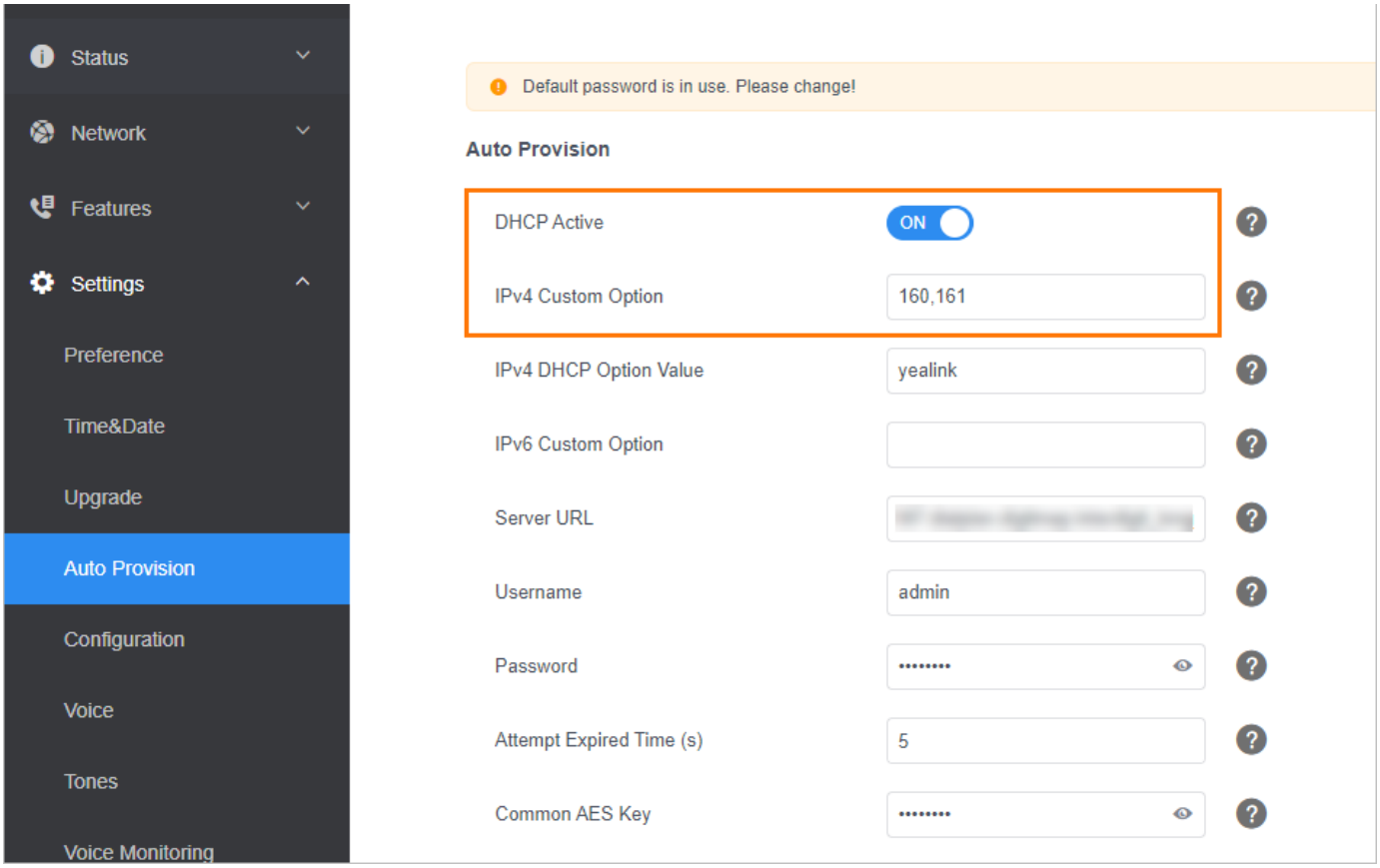
- **PnP**: PnP feature allows the phones to discover the provisioning server address by broadcasting the PnP SUBSCRIBE message during startup.
- **DHCP**: DHCP option can be used to provide the address or URL of the provisioning server to phones. When the IP phone requests an IP address using the DHCP 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**.




## 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<br>**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<br>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**

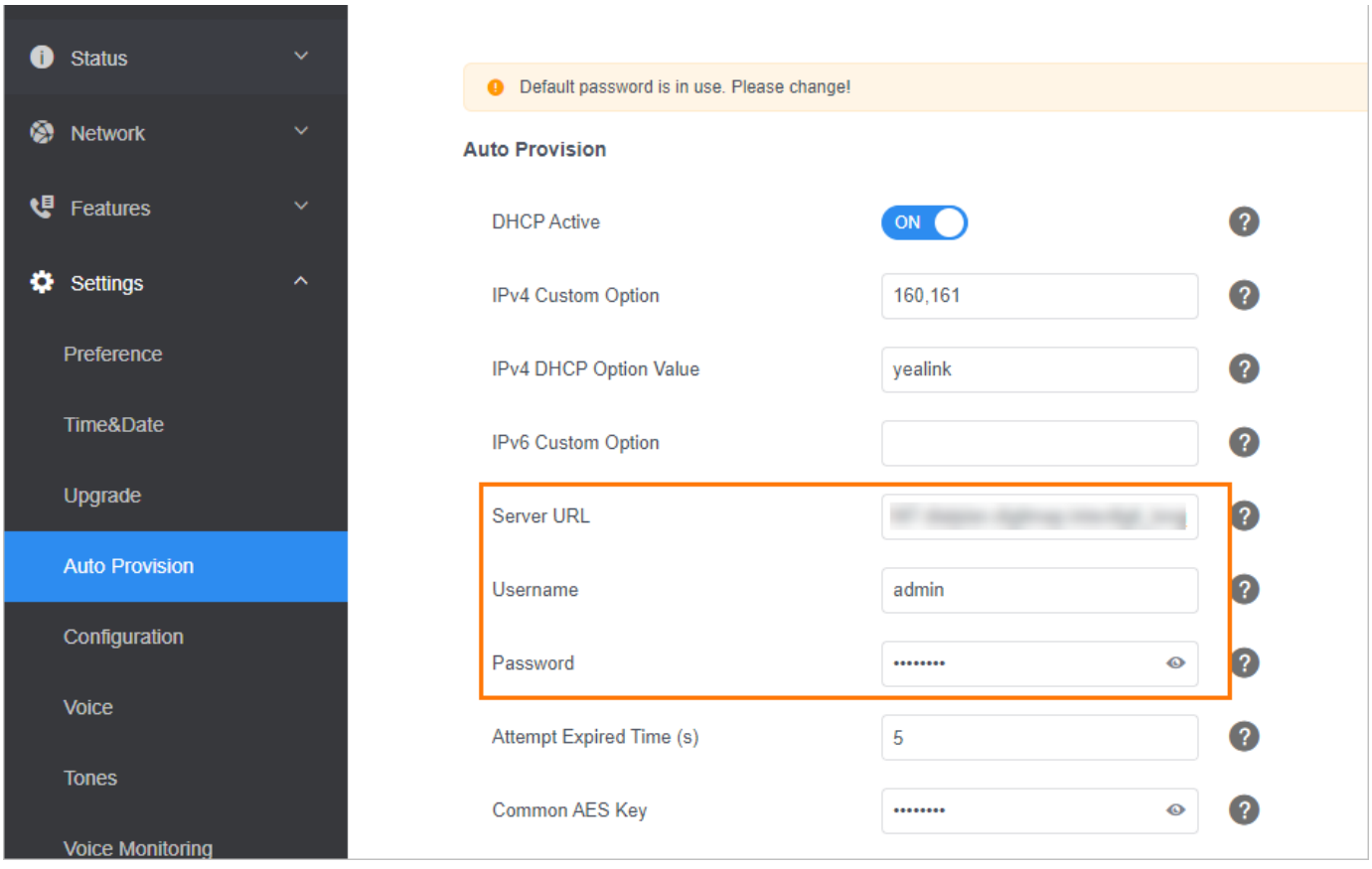
A URL should contain forward slashes instead of backslashes and should not contain spaces. Escape characters are not supported.

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**.



### 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

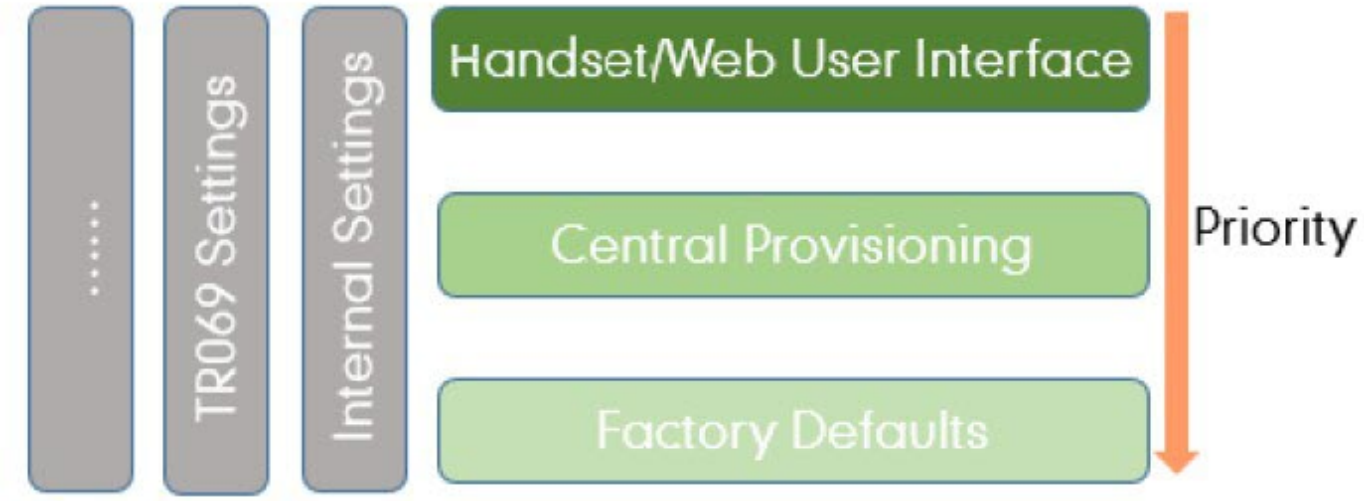
Zoom devices can be configured using the following methods with your provisioning server:

- **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.

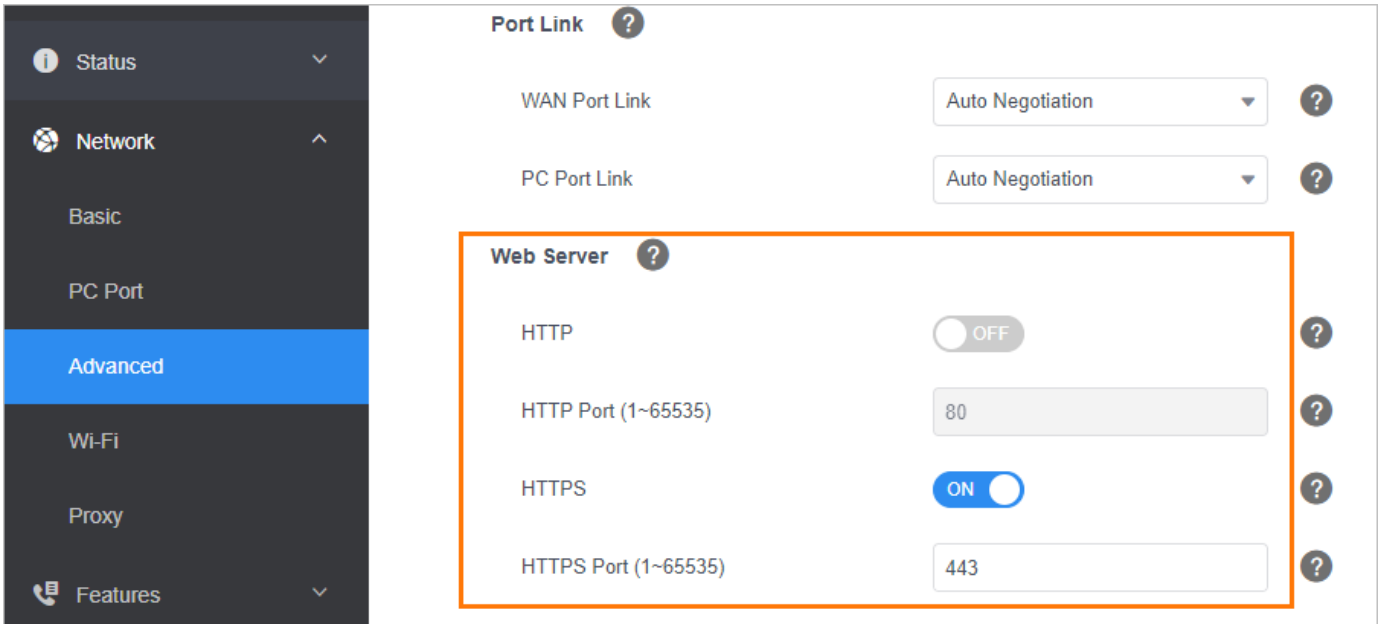
## Configure Web Server Type

Yealink Zoom 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**.




### Via Auto Provisioning

static.wui.http_enable
static.network.port.http
static.wui.https_enable
static.network.port.https

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

| | | | |
|---|---|---|---|
| static.wui.http_enable[1] | **0**-Disabled<br>**1**-Enabled | 1 | It enables or disables access to the web user interface of the phone over a non-secure tunnel (HTTP). |
| static.network.port.http[1] | Integer from 1 to 65535 | 80 | It configures the port used to access the web user interface of the phone over a non-secure tunnel (HTTP). |
| static.wui.https_enable[1] | **0**-Disabled<br>**1**-Enabled | 1 | It enables or disables access to the web user interface of the phone over a secure tunnel (HTTPS). |
| static.network.port.https[1] | Integer from 1 to 65535 | 443 | 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

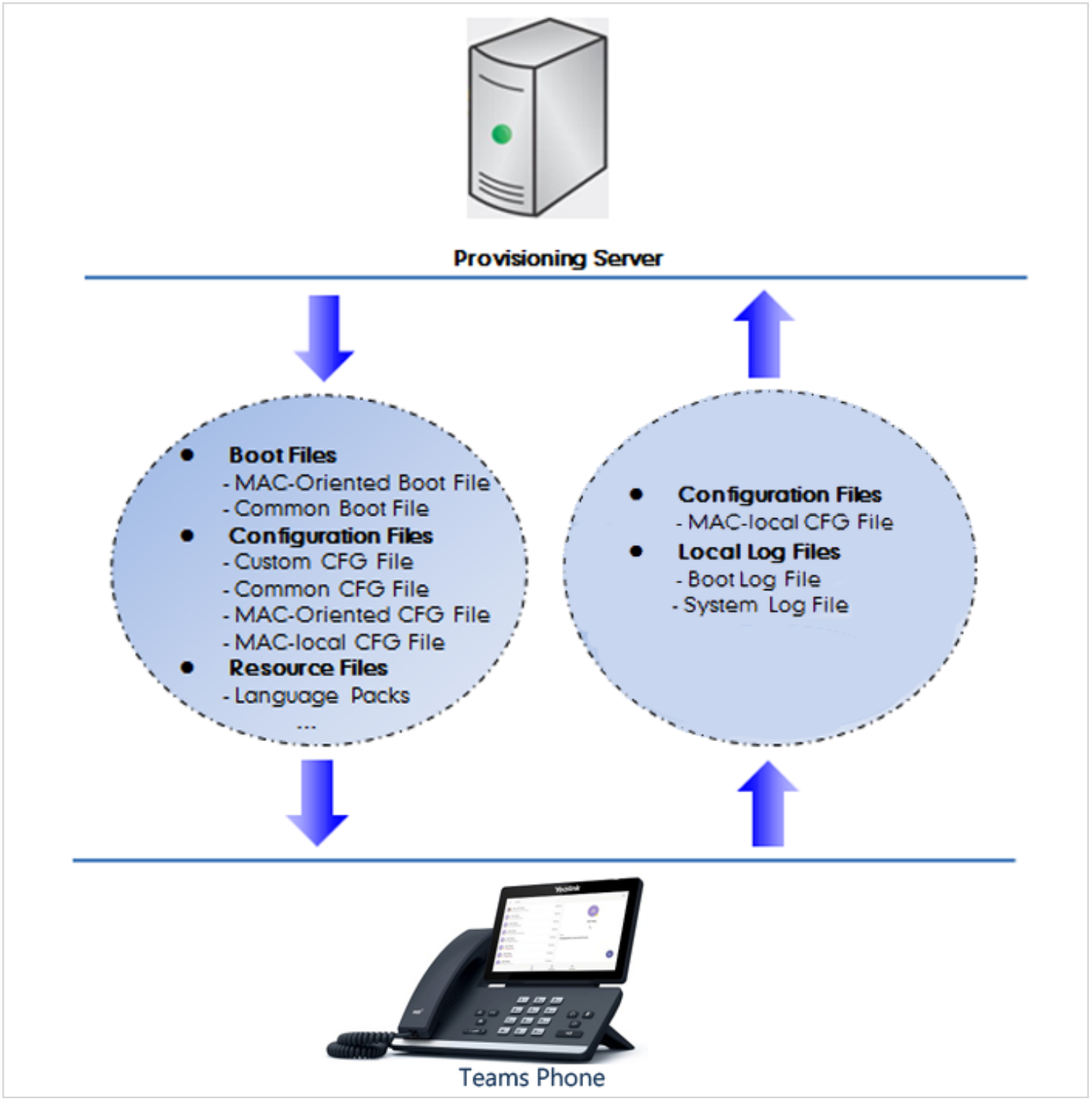
Phone user interface makes configurations available to users and administrators, but the > **Settings** > **Device Settings** > **Advanced** option is only available to administrators and requires an administrator password (default: admin).

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 the 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 the configuration files to a provisioning server. Zoom devices can be centrally provisioned from a provisioning server. For more information on the provisioning server, refer to Set Up a Provisioning Server.

Zoom devices can obtain the provisioning server address during startup. Then devices download configuration files from the provisioning server, and 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 Zoom 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.<br>**NOTE**<br>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<br>**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<br>**1**-On | 0 | It triggers the repeatedly feature to on or off. |
| static.au | Integer from 1 | 14 | It configures the interval (in minutes) for the phone to |

| | | | |
|---|---|---|---|
| to_provision.repeat.minutes | to 43200 | 40 | perform auto provisioning repeatedly.<br>**NOTE**<br>It works only if "static.auto_provision.repeat.enable" is set to 1 (On). |
| static.auto_provision.weekly.enable | **0**-Off<br>**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<br>**0**-Sunday<br>**1**-Monday<br>**2**-Tuesday<br>**3**-Wednesday<br>**4**-Thursday<br>**5**-Friday<br>**6**-Saturday | 01<br>23<br>45<br>6 | It configures the days of the week for the phone to perform auto provisioning weekly.<br><br>Example:<br>"static.auto_provision.weekly.dayofweek = 01"<br>If "static.auto_provision.weekly_upgrade_interval" is set to 0, it means the phone performs auto provisioning every Sunday and Monday.<br><br>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.<br>**NOTE**<br>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.<br>**NOTE**<br>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: Yealink Support.

## Boot Files

Zoom 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

Zoom 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 *.cfg.<br>The locations in the angle brackets or double quotation marks support two forms:<br>Relative path (relative to the boot file): "sip.cfg, HTTP Directory/sip.cfg" for example<br>Absolute path (or URL): "http://10.2.5.258/Zoom.cfg" for example<br>The location must point to a specific CFG file. |
| [$MODEL] | The [$MODEL] can be added to specify settings for specific phone models.<br>$MODEL represents the phone model name.<br>The valid device model names are: MP58, MP56, MP54, MP52, T58A, T56A, T55A, CP960, CP965 and VP59.<br>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.<br>**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.<br>**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.<br>NOTE<br>Overwrite mode can only be used in boot files. If a boot file is used, but the value of the parameter "overwrite_mode" is not configured, the overwrite mode is enabled by default. |

| | |
|---|---|
| specific_model.excluded_mode | Enable or disable the exclude mode. The exclude mode applies to the configuration files specified in the boot file.<br>**0- Disabled** (**Append Mode**), the device downloads its own model-specific configuration files and downloads other model-unspecified configuration files.<br>**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.<br>NOTE<br>Exclude mode can only be used in boot files. If a boot file is used but the value of the parameter "specific_model.excluded_mode" is not configured, the exclude mode is disabled by default. |

**TIP**

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

# 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/Zoom.cfg>, include:config "http://10.2.5.206/configure/account.cfg"
4. To specify configuration files for specific phone models, add specific phone modelsin front of include:config <>* or *include:config "". Multiple phone model names are separated by commas.
5. For example:
   - [T58A, CP960, CP965]include:config "<configure/Zoom.cfg> ""
   - [T56A]include:config "http://10.2.5.206/configure/account.cfg"
   - File "Zoom.cfg" only applies to T58A and CP960 phones, file "account.cfg" only applies to T56A phones
5. Specify the overwrite mode and exclude mode. For example: "overwrite_mode = 1", "specific_model.excluded_mode = 1".
6. Save the boot file and place it on the provisioning server.

# Configuration Files

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

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

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

**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 |
|---|---|
| T58A | y000000000058.cfg |
| T56A | y000000000056.cfg |
| T55A | y000000000099.cfg |
| CP960 | y000000000073.cfg |
| CP965 | y000000000073.cfg |
| VP59 | y000000000091.cfg |
| MP58/MP58-WH | y000000000135.cfg |
| MP56 | y000000000122.cfg |
| MP54 | y000000000134.cfg |
| MP52 | y000000000145.cfg |
| MP58-WH E2 | y000000000179.cfg |
| MP56 E2 | y000000000178.cfg |
| MP54 E2 | y000000000177.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** | **static.auto_provision.custom.protect** |
|---|---|
| **Descr** | It enables or disables the device to keep user’s personalized settings after auto |

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

## 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/MP56/MP54/ CP965, tap the account avatar and go to **Settings** > **Device Settings** > **Debug** (default password: admin) > **Reset user settings.**<br>• For MP52, 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, Zoom.cfg). You can rearrange the parameters in the configuration template file and create your own configuration files with the 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, Zoom.cfg.
2. Rearrange the parameters in the Zoom.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:
   - [T58A,CP960]phone_setting.phone_lock.enable= 1
   - [T58A]features.bluetooth_enable= 1
   - These parameters only apply to their own specific phone models.
4. Save the configuration file and place it on the provisioning server.

## Configuration File Attributes

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

| Attributes | Description |
|---|---|
| #!version:1.0.0.1 | It must be placed in the first line. Do not edit and delete. |
| Configuration Parameter=Valid Value (screensaver.wait_time =60) | Specify the parameters and values to apply specific settings to the devices.<br>• Separate each configuration parameter and value with an equal sign<br>• Set only one configuration parameter per line<br>• Put the configuration parameter and value on the same line, and do not break the line |
| [$MODEL] | The [$MODEL] can be added in front of the configuration parameter to specify the value for specific device models. $MODEL represents the phone model.<br>The valid device model names are: MP58, MP56, MP54, MP52, T58A, |

| | |
|---|---|
| | T56A, T55A, CP960, CP965 and VP59. Multiple phone models are separated by commas. For example, [T58A, CP960].<br>NOTE<br>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.

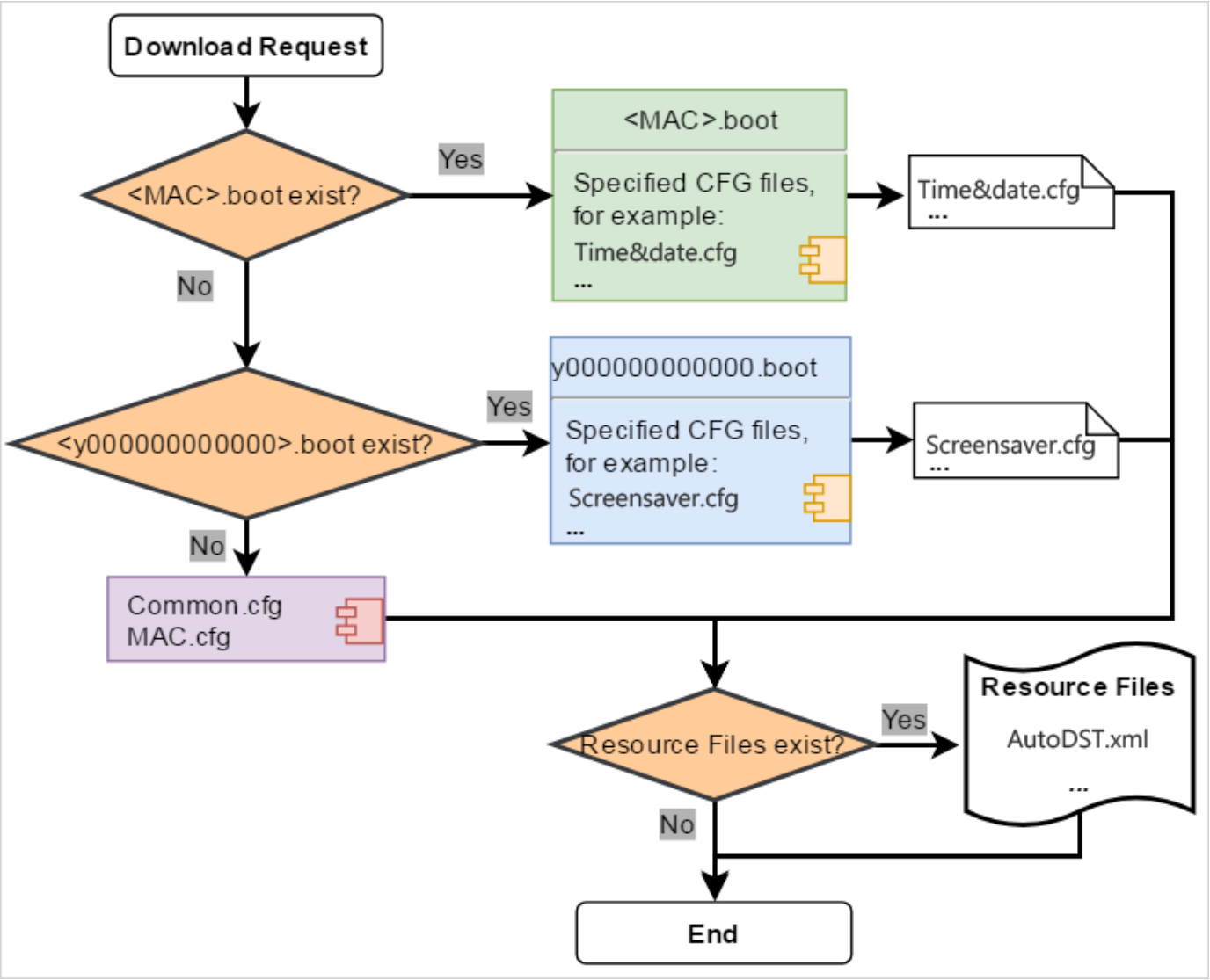
**TIP**
If you want to specify the desired device to use the resource file, the access URL of the resource file should be specified in the MAC-Oriented CFG file. During auto provisioning, the devices will request the resource files in addition to the configuration files.

Yealink supplies some templates 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 the files downloaded before.

**TIP**

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

# Provisioning Points to Consider

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

- Provisioning devices on the Zoom 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.

# 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.

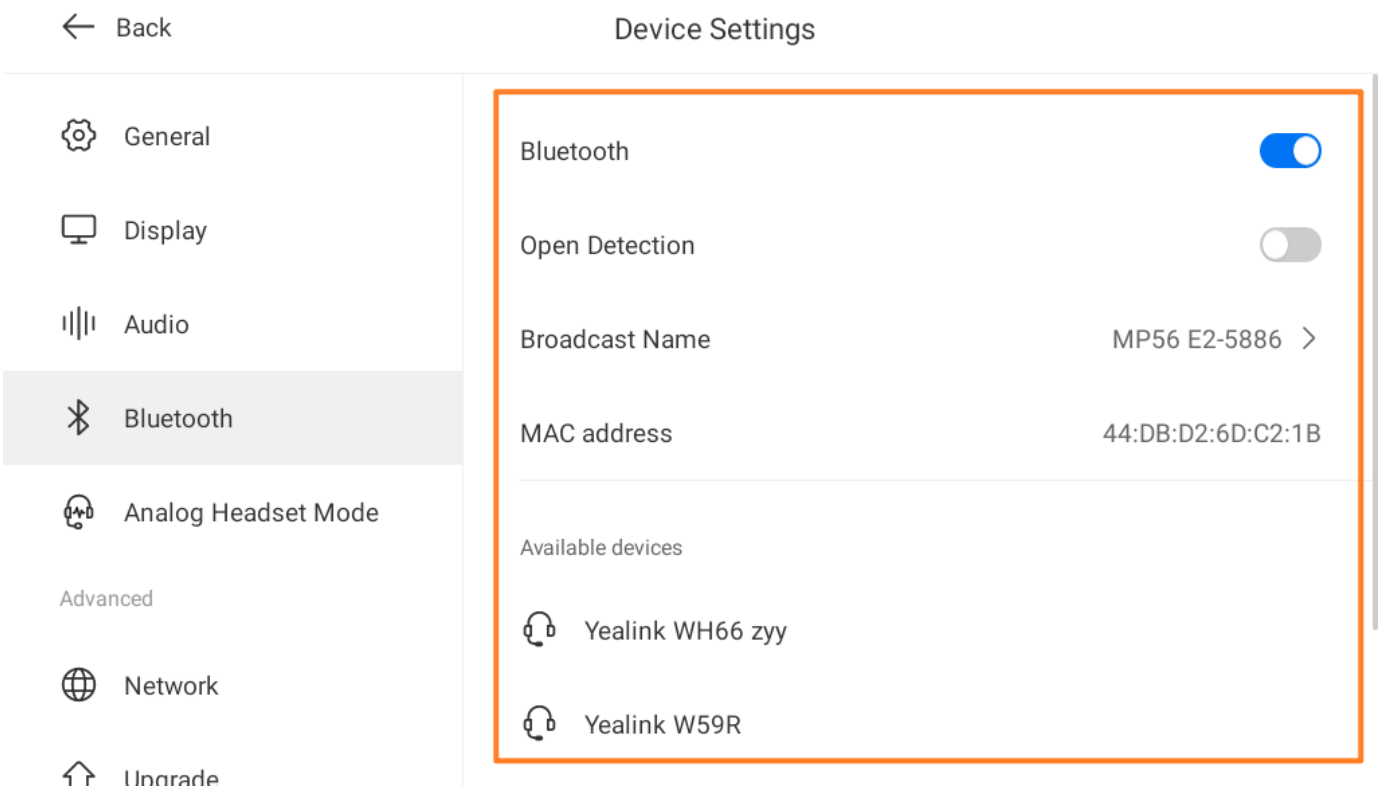
## Before You Begin

For MP54/MP52 Zoom phones, make sure the Bluetooth USB Dongle BT41 is connected to the phone.

## Via Device User Interface

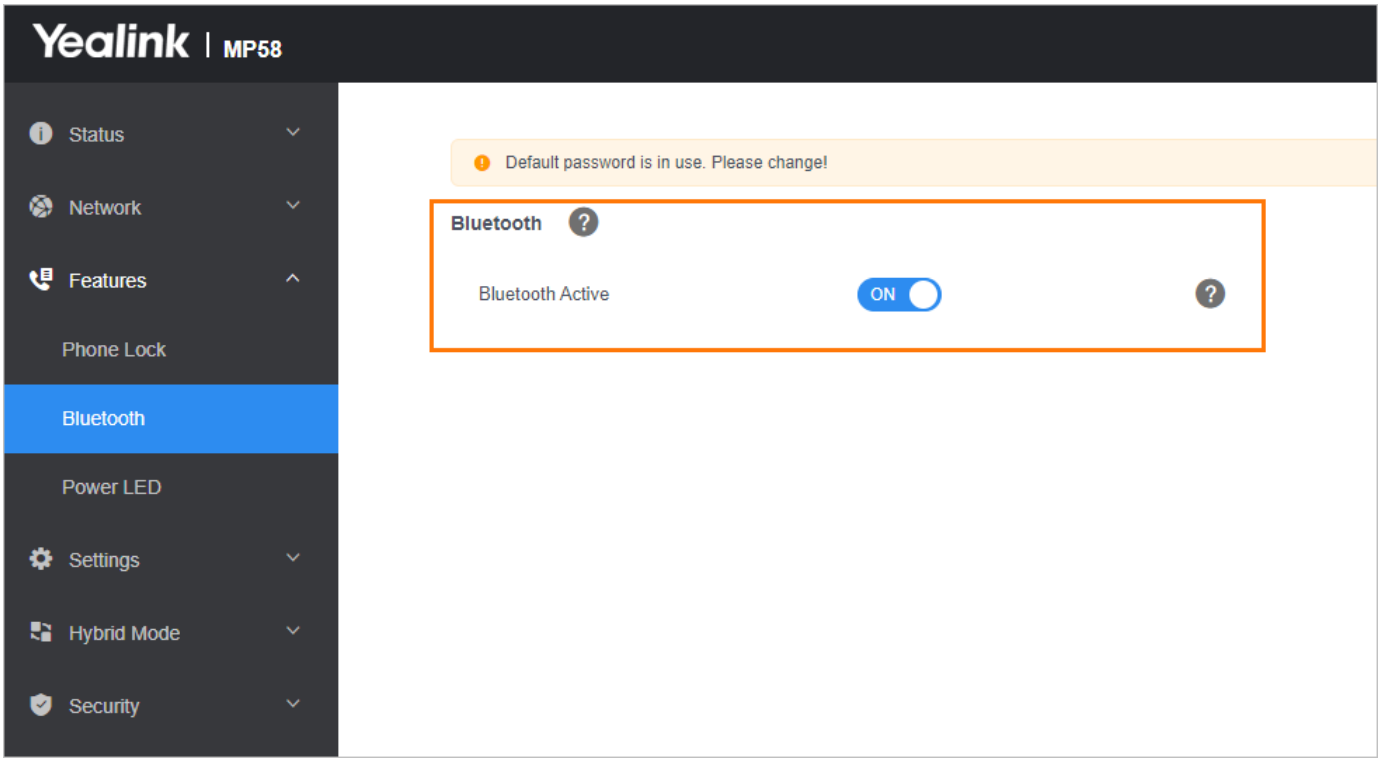
**Procedure**

1. Go to **More** > **Settings** > **General** > **System 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<br>**1**-Enabled | 1 | It enables or disables the Bluetooth feature. |
| features.bluetooth_enable | **0**-Off<br>**1**-On | 1 (0 for MP52/ MP56) | It triggers the Bluetooth mode to on or off.<br>NOTE<br>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 | It configures the Bluetooth device name. |

| | | | |
|---|---|---|---|
| | | For T56A: Yealink-T56A<br>For T55A: Yealink-T55A<br>For VP59: Yealink-VP59<br>For CP965: Yealink-CP96<br>For MP52: Yealink-MP52<br>For MP54: Yealink-MP54<br>For MP56: Yealink-MP56<br>For MP58/MP58-WH: Yealink-MP58 | NOTE<br>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

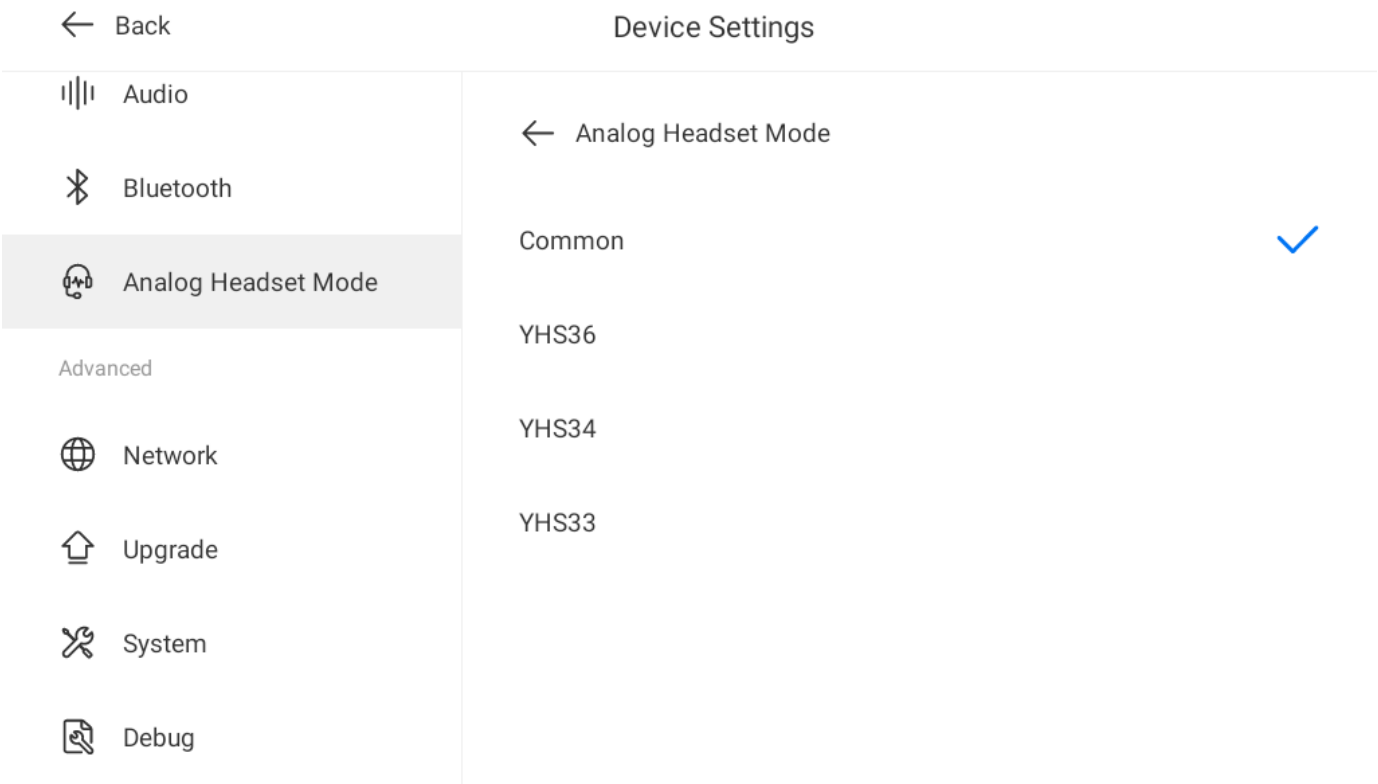
You can manually configure audio solutions for Yealink RJ headsets YHS36, YHS34, YHS33.

**TIP**

This feature is unavailable to CP965.

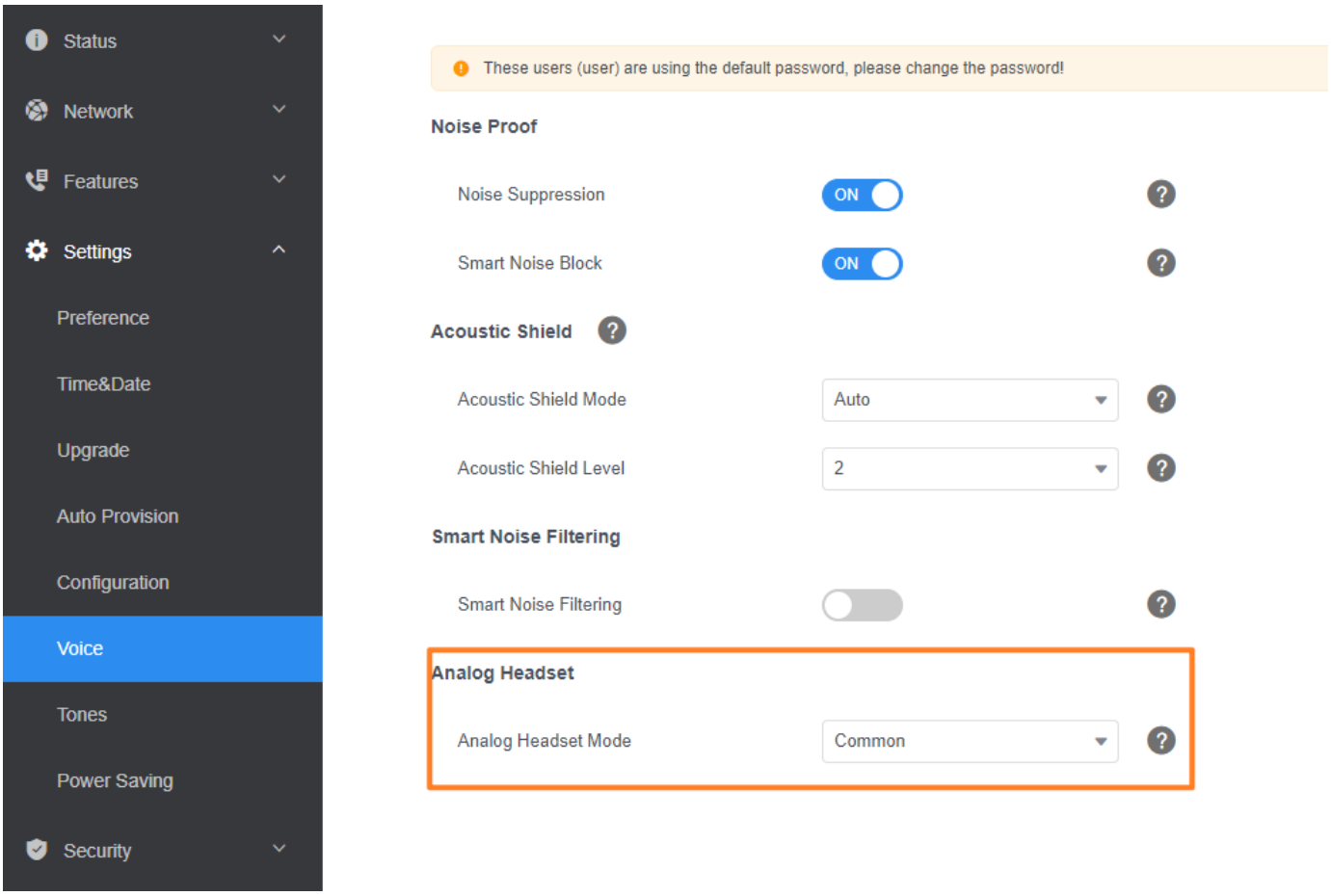
## Via Device User Interface

1. Go to **More** > **Settings** > **General** > **System Settings** > **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**.




# 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. |

# Smart Noise Filtering

## Introduction

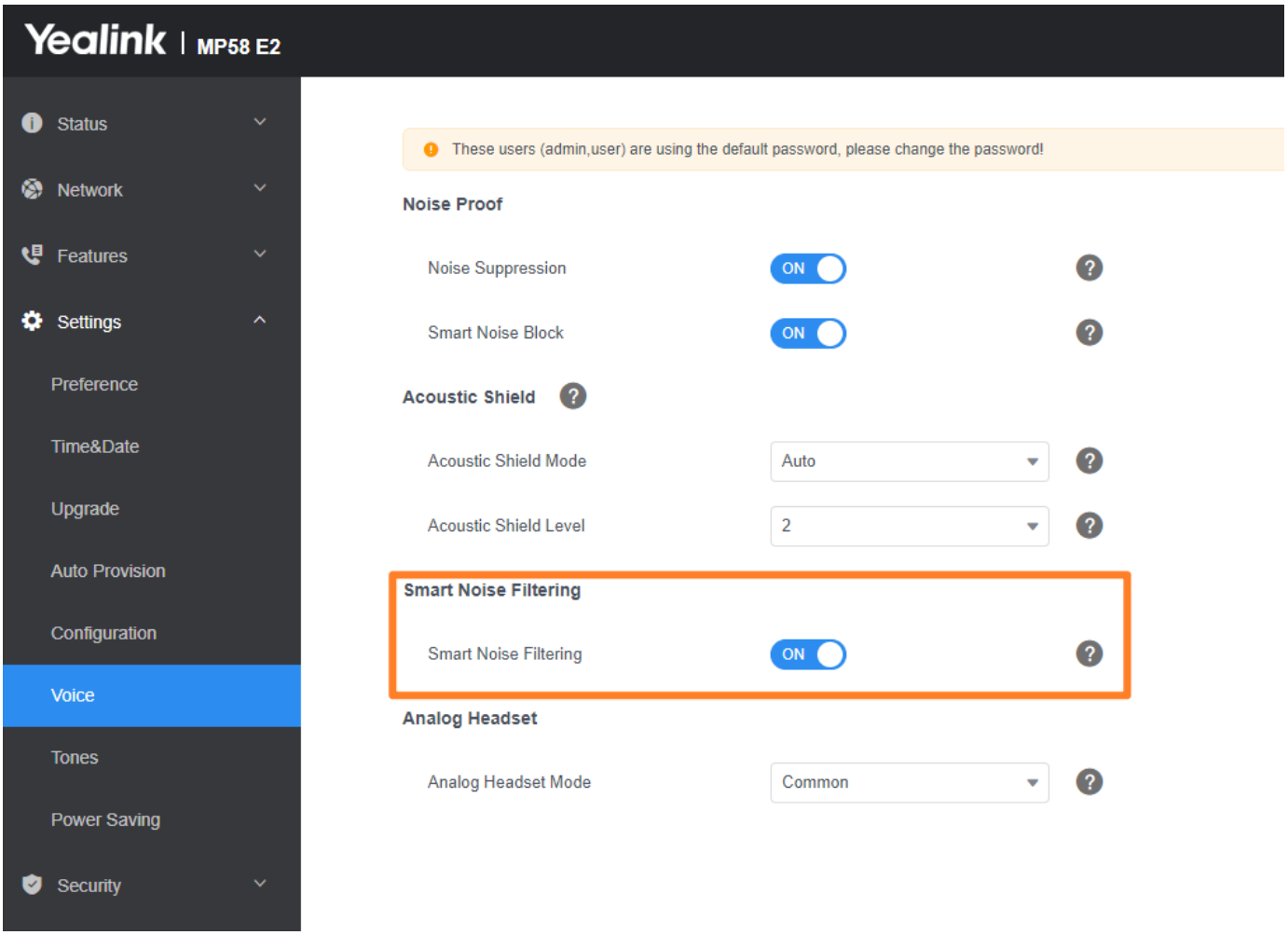
The phones can block out the slight noise from the far party when there is no speech in a call, and at the same time filter out the common transient noise (door closing, table knocking, and so on).

**NOTE**

Only applicable to MP5X E2.

## Via Web User Interface

On the web user interface, go to: **Settings** > **Voice** > **Smart Noise Filtering**




## Via Auto Provisioning

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

| features.noise_filtering_rev.enable |
|---|

| Parameter | Description | Permitted Values | Default |
|---|---|---|---|
| features.noise_filtering_rev.enable | It enables or disables the phone to block out the slight noise from the far end when there is no speech in a call.<br>**NOTE**<br>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. | 0-Disabled<br>1-Enabled | 0 |

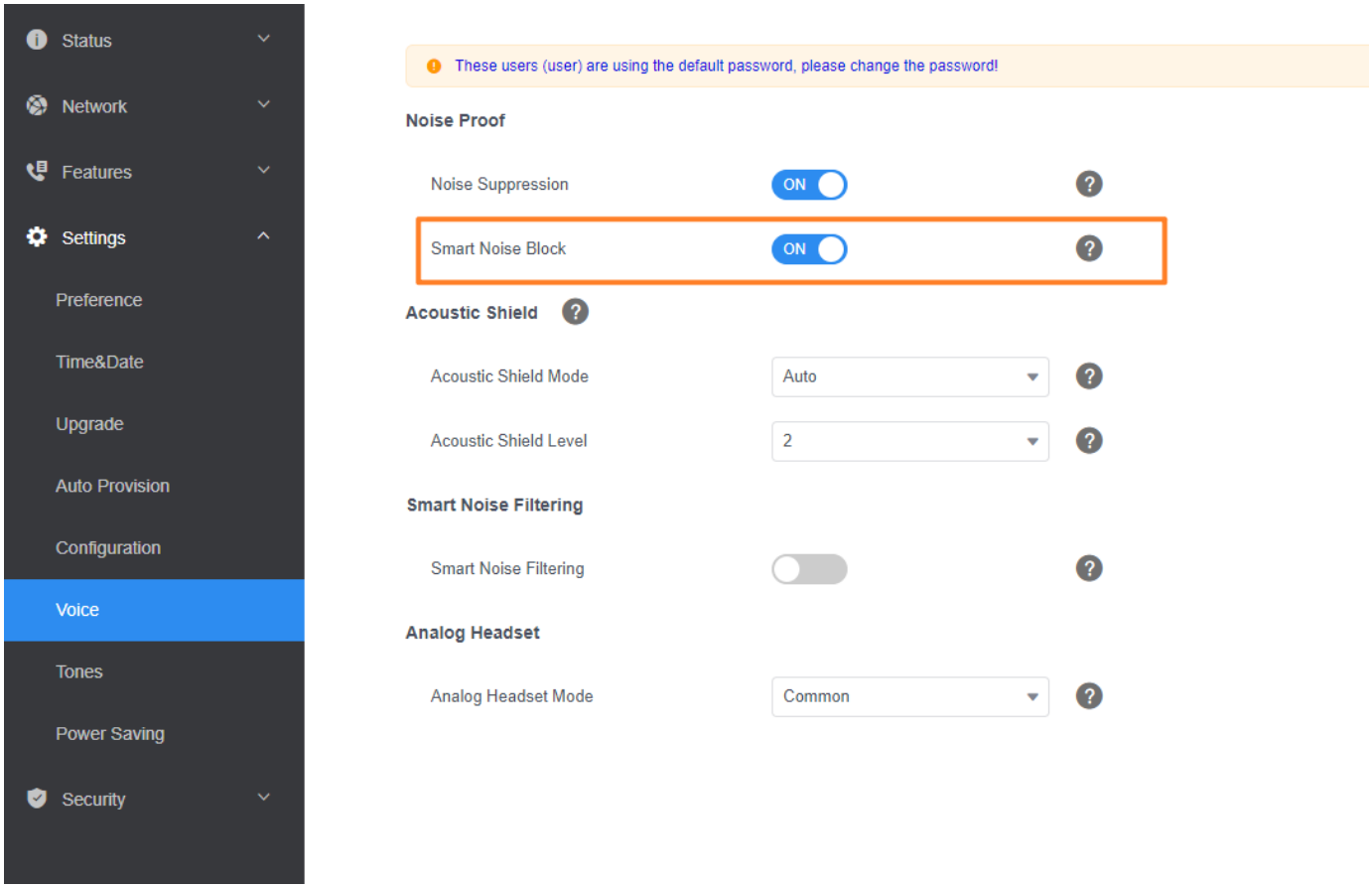
# Smart Noise Block

## 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 the smart noise block.

voice.ans_nb.enable

| Parameter | Permitted Values | Default | Description |
|---|---|---|---|
| voice.ans_nb.enable | **0**-Disabled | 1 | It enables or disables the Smart Noise Block |

| | | | |
|---|---|---|---|
| | **1**-Enabled | | feature.<br>**NOTE**<br>It works only if "voice.tns.enable" is set to 1 (Enabled). |

# Noise Suppression

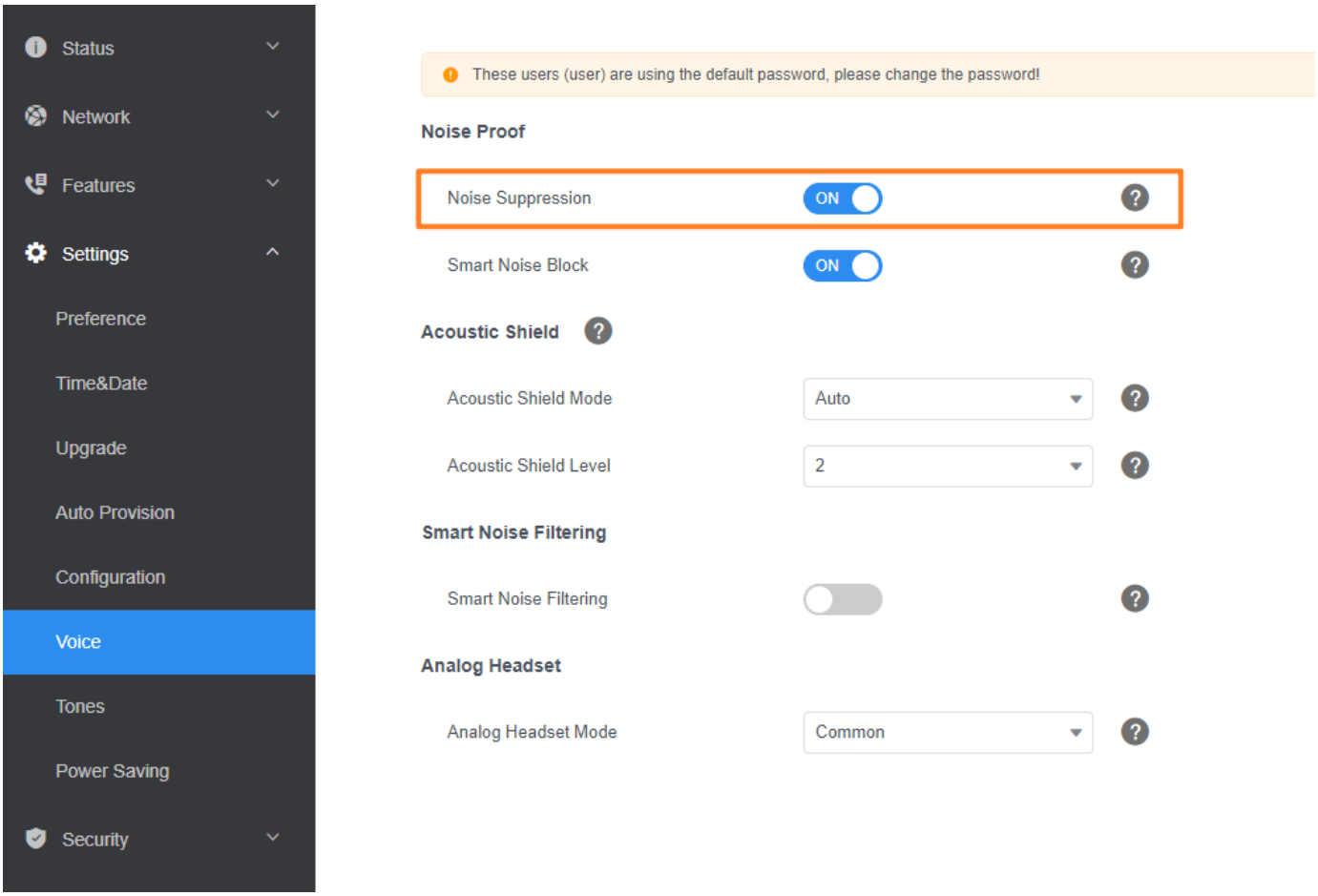
## Introduction

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

1. Log in to the phone web user interface as an admin.
2. Go to **Settings** > **Voice** > **Noise Proof** > **Noise Suppression**.




## Via Auto Provisioning

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

voice.tns.enable

| Parameter | Permitted | Defa | Description |
|---|---|---|---|

| | Values | ult | |
|---|---|---|---|
| voice.tns.enable | **0**-Disabled<br>**1**-Enabled | 1 | It enables or disables the **Noise Suppression** feature. |

# Acoustic Shield

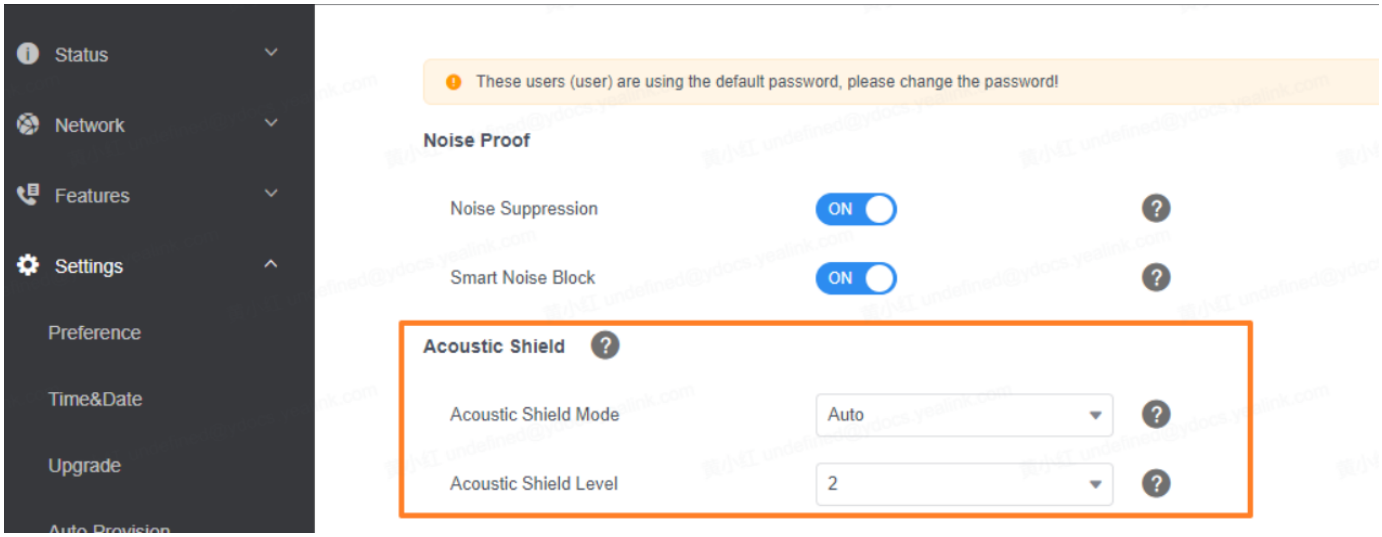
## Introduction

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
features.acoustic_shield.level

| Parameter | Permitted Values | Default | Description |
|---|---|---|---|
| features.acoustic_shield.mode | **0**- Disabled<br>**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. |

| | | | |
|---|---|---|---|
| features.acoustic_shield.level | Integer from 1 to 3 | 2 | It configures the level of call with the acoustic shield function. |

# Volume

## Configure the Headset Volume via Auto Provisioning

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

voice.handset.tia4965.enable
voice.headset.tia4965.enable

| Parameter | Permitted Values | Default | Description |
|---|---|---|---|
| voice.handset.tia4965.enable | **0**- Disabled<br>**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 standards. |
| voice.headset.tia4965.enable | **0**- Disabled<br>**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 standards. |

# Set Ringer Devices

## Introduction

When the device is on 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/CP960.

## Supported Tones

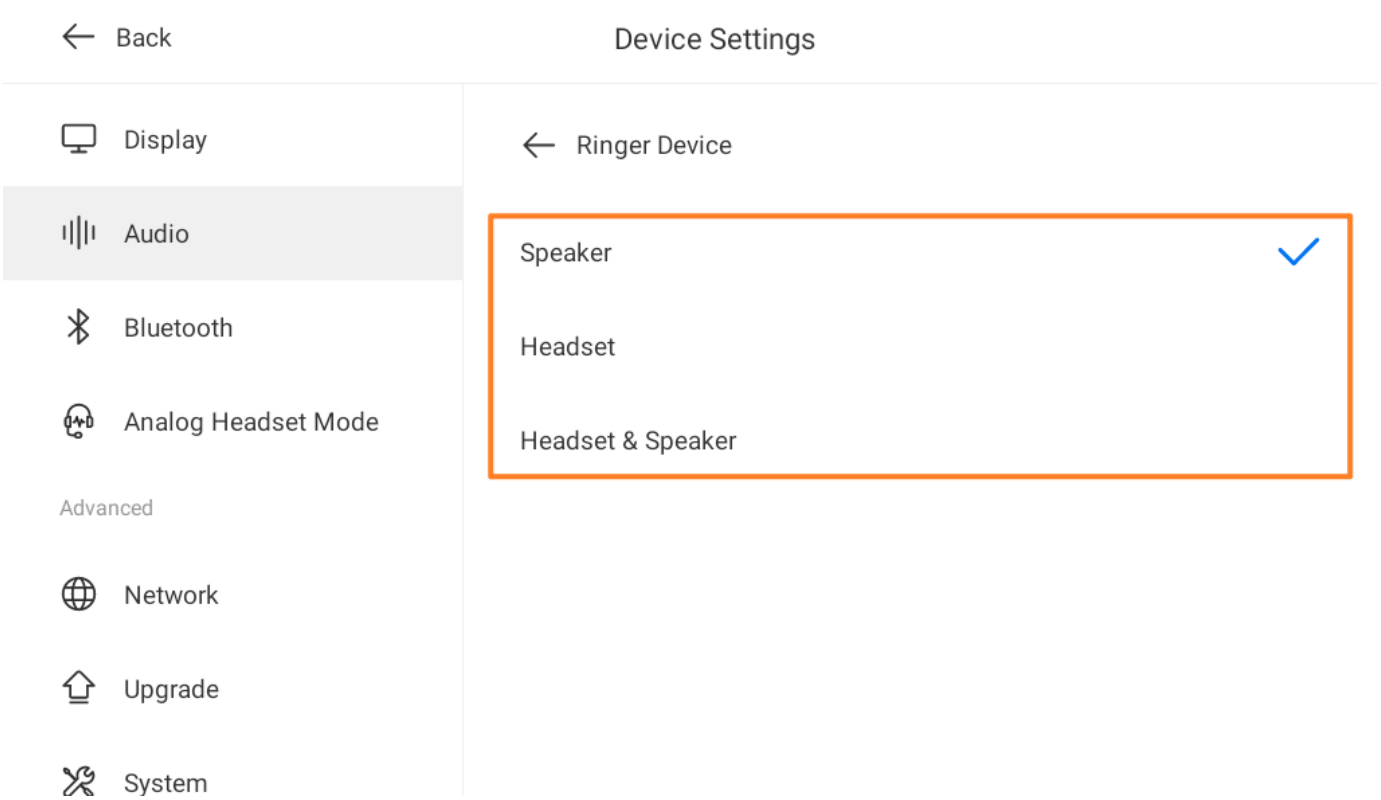
The default tones used on Zoom devices are the US tone sets. Available tone sets for the devices:

| 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

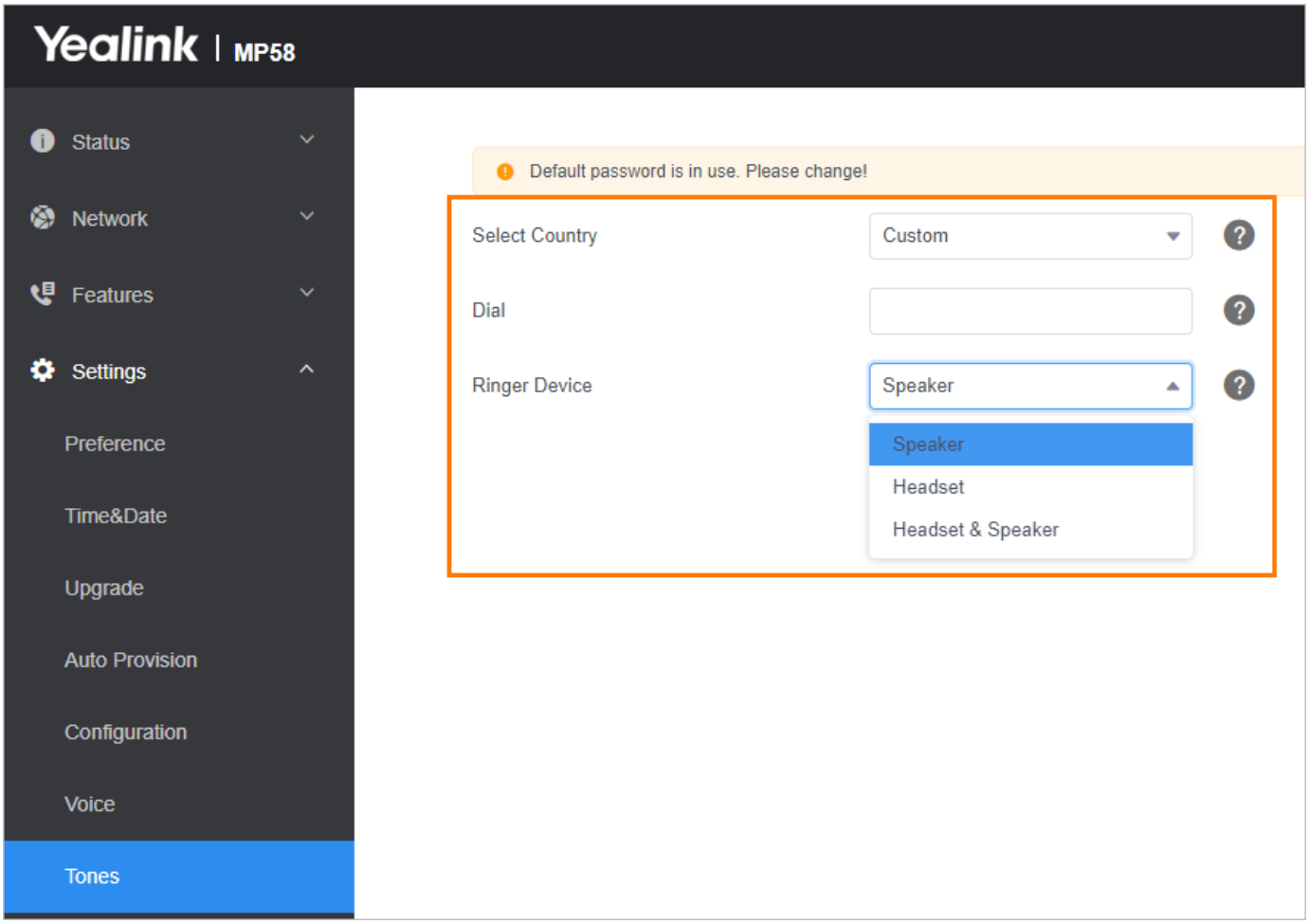
### Configure Ringer Devices via Device User Interface

1. Go to **More** > **Settings** > **General** > **System Settings** > **Audio**.




# 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
voice.tone.stutterdial
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]…<br>Where<br>**element** = [!]Freq1[+Freq2][+Freq3][+Freq4] / Duration<br>**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.<br>**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.<br>**NOTE**<br>It works only if "voice.tone.country" is set to Custom. |
| voice.tone. | String | Bl | It configures the |

| | | | |
|---|---|---|---|
| stutterdial | | an k | frequency and the period of Stutter Dial Tone. |
| features.ringer_device.is_use_headset | **0**- Use Speaker<br>**1**- Use Headset<br>**2**- Use Headset & Speaker | 0 | It configures the ringer device for the phone. |

# Time and Date

Zoom 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 3) |

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

| | | | | | |
|---|---|---|---|---|---|
| | Bahia | | | Bangkok | |
| -3 | America/ Buenos_Aires | Buenos Aires | +7 | Asia/ Jakarta | Bangkok, Hanoi, Jakarta |
| -3 | America/ Cayenne | Cayenne, Fortaleza | +7 | Asia/ Krasnoyarsk | Krasnoyarsk (RTZ 6) |
| -3 | America/ Fortaleza | Cayenne, Fortaleza | +8 | Asia/ Shanghai | Beijing, Chongqing, Hong Kong, Urumqi |
| -2 | America/ Godthab | Greenland | +8 | Asia/ Hong_Kong | Beijing, Chongqing, Hong Kong, Urumqi |
| -3 | America/ Montevideo | Montevideo | +8 | Asia/Irkutsk | Irkutsk (RTZ 7) |
| -3 | America/ Bahia | Salvador | +8 | Asia/ Singapore | Kuala Lumpur, Singapore |
| -4 | America/ Santiago | Santiago | +8 | Asia/ Kuala_Lumpur | Kuala Lumpur, Singapore |
| -2 | Etc/GMT+2 | Coordinated Universal Time-02 | +8 | Australia/ Perth | Perth |
| -2 | America/ Noronha | Mid-Atlantic - Old | +8 | Asia/Taipei | Taipei |
| 0 | Atlantic/ Azores | Azores | +8 | Asia/ Ulaanbaatar | Ulaanbaatar |
| -1 | Atlantic/ Cape_Verde | Cabo Verde Is | +9 | Asia/Tokyo | Osaka, Sapporo, Tokyo |
| +1 | Africa/ Casablanca | Casablanca | +9 | Asia/Seoul | Seoul |
| 0 | Etc/GMT | Coordinated Universal Time | +9 | Asia/ Yakutsk | Yakutsk (RTZ 8) |
| +1 | Europe/ London | Dublin, Edinburgh, Lisbon, London | +9:30 | Australia/ Adelaide | Adelaide |

| | | | | | |
|---|---|---|---|---|---|
| +1 | Europe/ Dublin | Dublin, Edinburgh, Lisbon, London | +9:30 | Australia/ Darwin | Darwin |
| +1 | Europe/ Lisbon | Dublin, Edinburgh, Lisbon, London | +10 | Australia/ Brisbane | Brisbane |
| 0 | Atlantic/ Reykjavik | Monrovia, Reykjavik | +10 | Australia/ Sydney | Canberra, Melbourne, Sydney |
| 0 | Europe/ Stockholm | Monrovia, Reykjavik | +10 | Pacific/ Port_Moresby | Guam, Port Moresby |
| +2 | Europe/ Berlin | Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna | +10 | Pacific/ Guam | Guam, Port Moresby |
| +2 | Europe/ Rome | Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna | +10 | Australia/ Hobart | Hobart |
| +2 | Europe/ Stockholm | Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna | +11 | Asia/ Magadan | Magadan |
| +2 | Europe/ Budapest | Belgrade, Bratislava, Budapest, Ljubljana, Prague | +10 | Asia/ Vladivostok | Vladivostok, Magadan (RTZ 9) |
| +2 | Europe/ Belgrade | Belgrade, Bratislava, Budapest, Ljubljana, Prague | +11 | Asia/ Srednekolymsk | Chokurdakh (RTZ 10) |
| +2 | Europe/ Paris | Brussels, Copenhagen, Madrid, Paris | +11 | Pacific/ Guadalcanal | Solomon Is., New Caledonia |
| +2 | Europe/ Madrid | Brussels, Copenhagen, Madrid, Paris | +11 | Pacific/ Noumea | Solomon Is., New Caledonia |
| +2 | Europe/ Brussels | Brussels, Copenhagen, Madrid, Paris | +12 | Asia/Anadyr | Anadyr, Petropavlovsk-Kamchatsky (RTZ 11) |
| +2 | Europe/ | Sarajevo, Skopje, | +12 | Pacific/ | Auckland, Wellington |

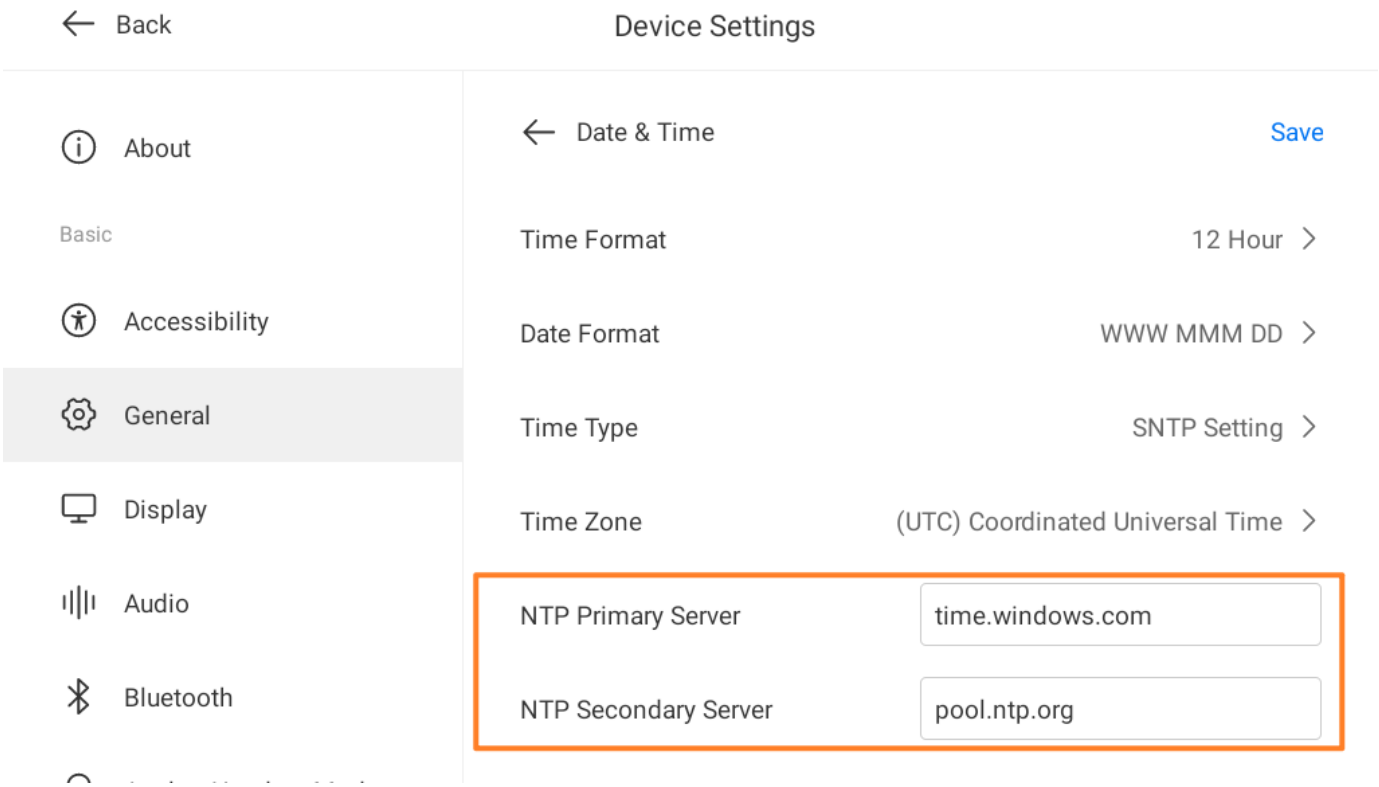
| | | | | | |
|---|---|---|---|---|---|
| | Warsaw | Warsaw, Zagreb | | Auckland | |
| +2 | Europe/ Skopje | Sarajevo, Skopje, Warsaw, Zagreb | +12 | Etc/GMT-12 | Coordinated Universal Time+12 |
| +1 | Africa/ Lagos | West Central Africa | +12 | Pacific/Fiji | Fiji |
| +2 | Africa/ Windhoek | Windhoek | +12 | Asia/ Kamchatka | Petropavlovsk-Kamchatsky - Old |
| +3 | Asia/ Amman | Amman | +13 | Pacific/ Tongatapu | Nuku'alofa |
| +3 | Europe/ Bucharest | Athens, Bucharest | -11 | Pacific/ Pago_Pago | Samoa |
| +3 | Europe/ Athens | Athens, Bucharest | +14 | Pacific/ Kiritimati | Kiritimati Island |
| +3 | Asia/Beirut | Beirut | +8:45 | Australia/ Eucla | Eucla |
| +2 | Africa/Cairo | Cairo | +3 | Asia/Gaza | Gaza |
| +3 | Asia/ Damascus | Damascus | +2 | Europe/ Luxembourg | Luxembourg |
| +3 | Europe/ 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 | -9:30 | Pacific/ Marquesas | French Polynesia |
| +2 | Europe/ Kaliningrad | Kaliningrad | +10:30 | Australia/ Lord_Howe | Lord Howe Island |
| +2 | Africa/ Tripoli | Tripoli | +12:45 | Pacific/ Chatham | Chatham Islands |

# 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.

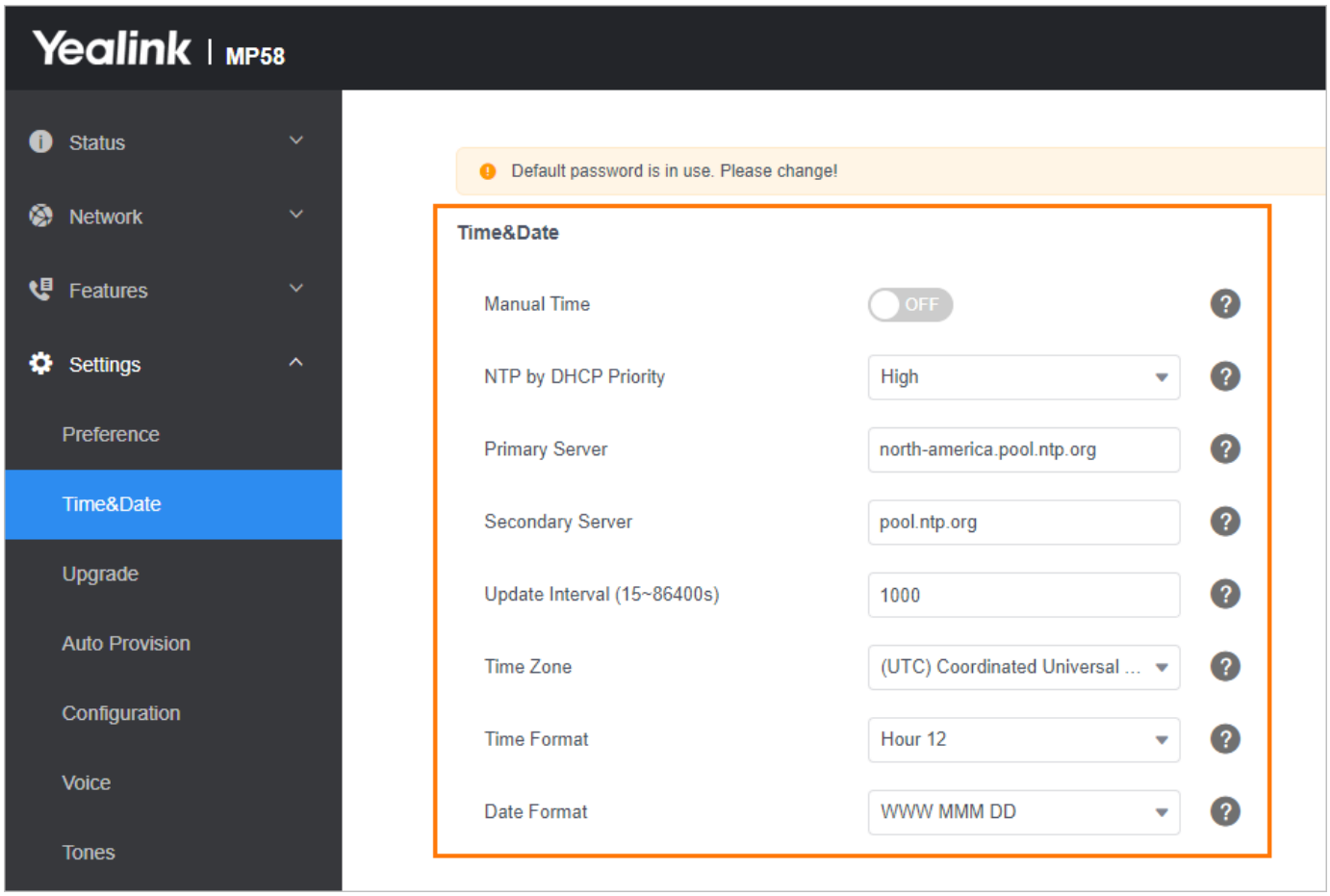
## Via Device User Interface

1. Go to **More** > **Settings** > **General** > **System Settings** > **General** >**Time & Date**.




## Via Web User Interface

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




# 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 | 0 | It configures the priority for the device to use the NTP server address offered by the DHCP server. |

| | | | |
|---|---|---|---|
| | by the DHCP server preferentially) **1**-Low (use the 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_zo | String within 64 characters | Asia/Shangha | 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/ |

| | | | |
|---|---|---|---|
| ne | | i | 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. You can also obtain the DST template online: http://supportx.yealink.com/documentFront/ .

## Auto DST File Attributes

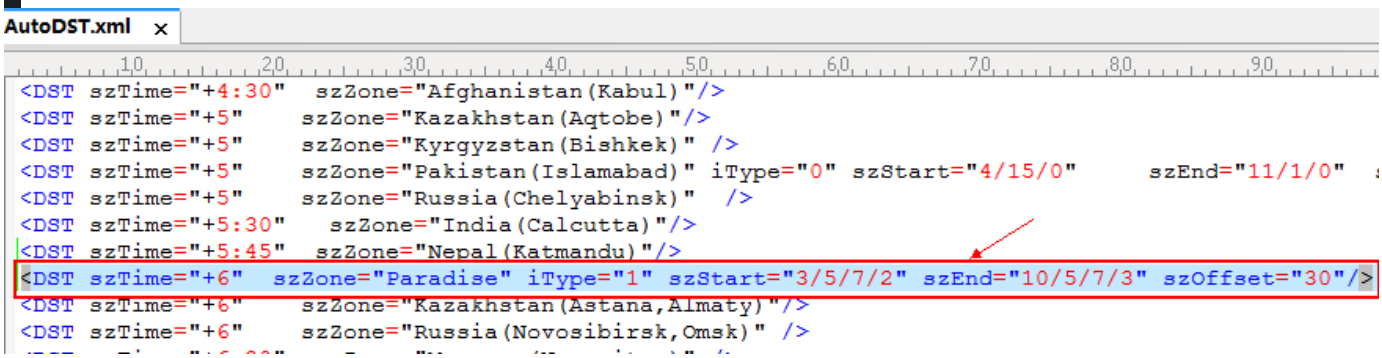
| Attributes | Type | Values | Description |
|---|---|---|---|
| **szTime** | required | [+/-][X]:[Y], X=0-14, Y=0-59 | Time Zone |
| **szZone** | required | String (if the content is more than one city, it is the best to keep their daylight saving time the same) | Time Zone name |
| **iType** | optional | 0/1**0**: DST by Date**1**: DST by Week | DST time type(This item is needed if you want to configure DST.) |
| **szStart** | optional | **Month/Day/Hour** (for **iType=0**)<br>Month: 1-12<br>Day: 1-31<br>Hour: 0 (midnight)-23<br>**Month/Week of Month/Day of Week/ Hour of Day** (for **iType=1**) | Starting time of the DST |

| | | | |
|---|---|---|---|
| | | Month: 1-12<br>Week of Month: 1-5 (the last week)<br>Day of Week: 1-7<br>Hour of Day: 0 (midnight)-23 | |
| **szEnd** | optional | Same as szStart | Ending time of the DST |
| **szOffset** | optional | Integer from -300 to 300 | The offset time (in minutes) of DST |

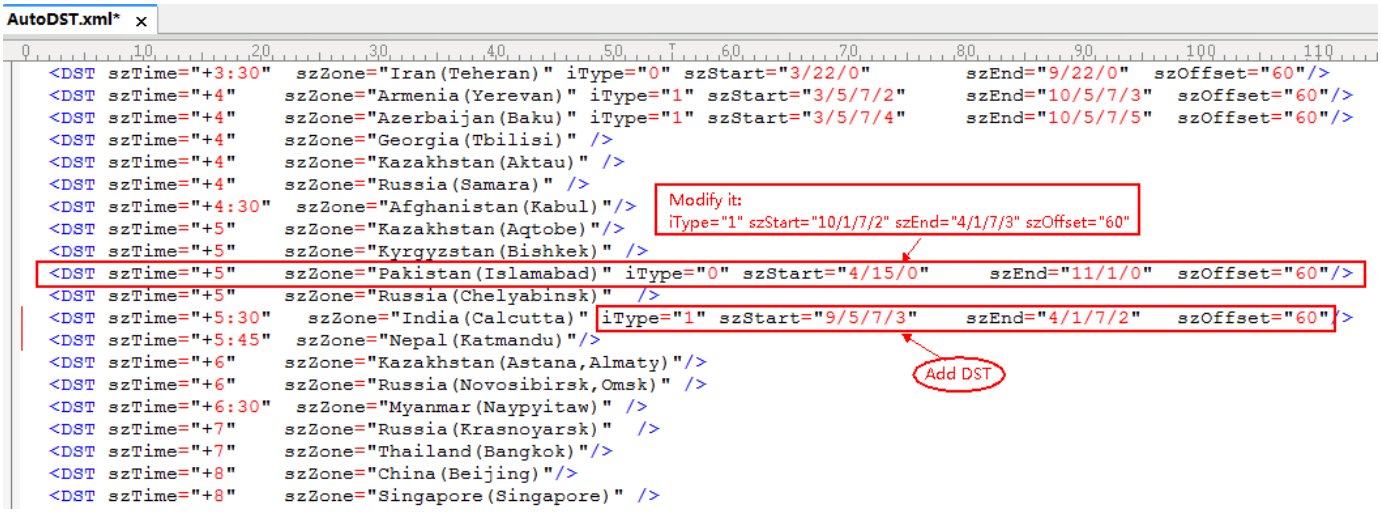
## Customize Auto DST File

**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"/>`




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)”.




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<br>**1**- Enabled<br>**2**- Automatic | 2 | It configures Daylight Saving Time (DST) feature. |
| local_time.dst_time_type | **0**- DST by Date<br>**1**- DST by Week | 0 | It configures the Daylight Saving Time (DST) type.<br>NOTE<br>It works only if "local_time.summer_time" is set to 1 (Enabled). |
| local_time.start_tim | Month/Day/Hour-DST by Date, use the | 1/1/2 | It configures the start time of the |

| | | | |
|---|---|---|---|
| e | following mapping:<br>**Month**: 1=January, 2=February,…, 12=December<br>**Day**: 1=the first day in a month,…, 31= the last day in a month<br>**Hour**: 0=0am, 1=1am,…, 23=11pm<br>Month/Week of Month/Day of Week/ Hour of Day- DST by Week, use the following mapping:<br>**Month**: 1=January, 2=February,…, 12=December<br>**Week of Month**: 1=the first week in a month,…, 5=the last week in a month<br>**Day of Week**: 1=Monday, 2=Tuesday,…, 7=Sunday<br>**Hour of Day**: 0=0am, 1=1am,…, 23=11pm | 000 | Daylight Saving Time (DST).<br>NOTE<br>It works only if the "local_time.summer_time" is set to 1 (Enabled). |
| local_time.end_time | Month/Day/Hour-DST by Date, use the following mapping:<br>**Month**: 1=January, 2=February,…, 12=December<br>**Day**: 1=the first day in a month,…, 31= the last day in a month<br>**Hour**: 0=0am, 1=1am,…, 23=11pm<br>Month/Week of Month/Day of Week/ Hour of Day- DST by Week, use the following mapping:<br>**Month**: 1=January, 2=February,…, 12=December<br>**Week of Month**: 1=the first week in a month,…, 5=the last week in a month<br>**Day of Week**: 1=Monday, 2=Tuesday,…, 7=Sunday<br>**Hour of Day**: 0=0am, 1=1am,…, 23=11pm | 12/31/2023 | It configures the end time of the Daylight Saving Time (DST).<br>NOTE<br>It works only if "local_time.summer_time" is set to 1 (Enabled). |

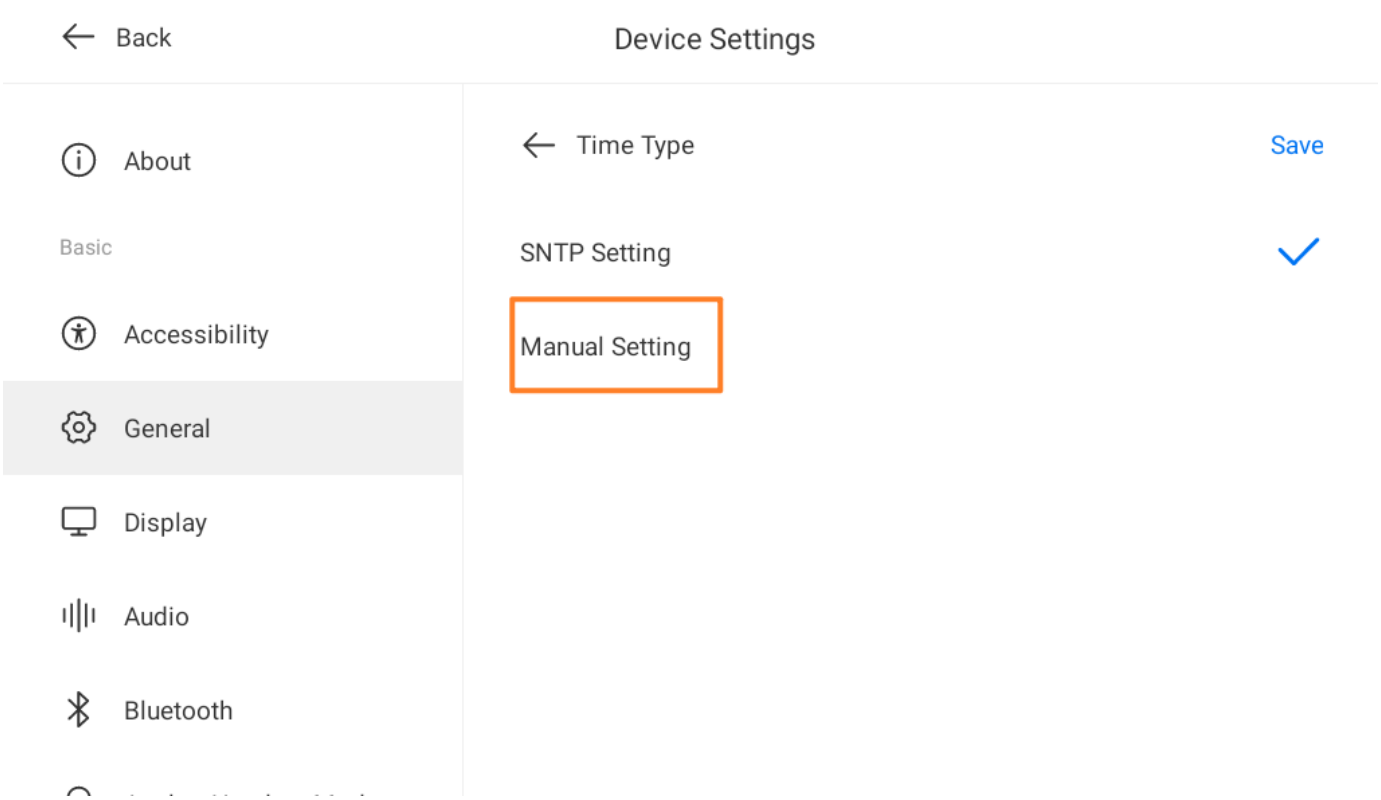
| | | | |
|---|---|---|---|
| local_time.offset_time | Integer from -300 to 300 | Blank | It configures the offset time (in minutes) of Daylight Saving Time (DST).<br>NOTE<br>It works only if "local_time.summer_time" is set to 1 (Enabled). |
| auto_dst.url | URL within 511 characters | Blank | It configures the access URL of the DST file (AutoDST.xml).<br>NOTE<br>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

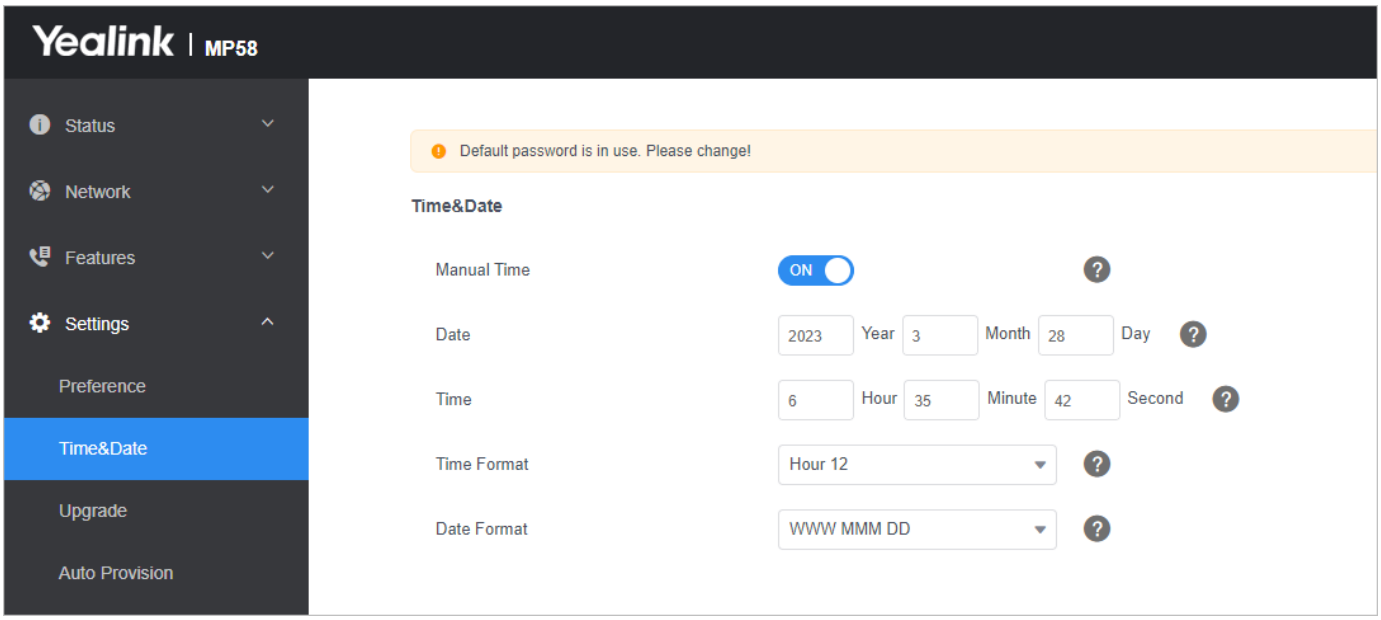
1. Go to **More** > **Settings** > **General** > **System Settings** > **General** >**Time & Date**.
2. Tap **Manual Settings** from the **Type** field, and tap **Save**.




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

# 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**.




# Via Auto Provisioning

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

| |
|---|
| local_time.manual_time_enable |

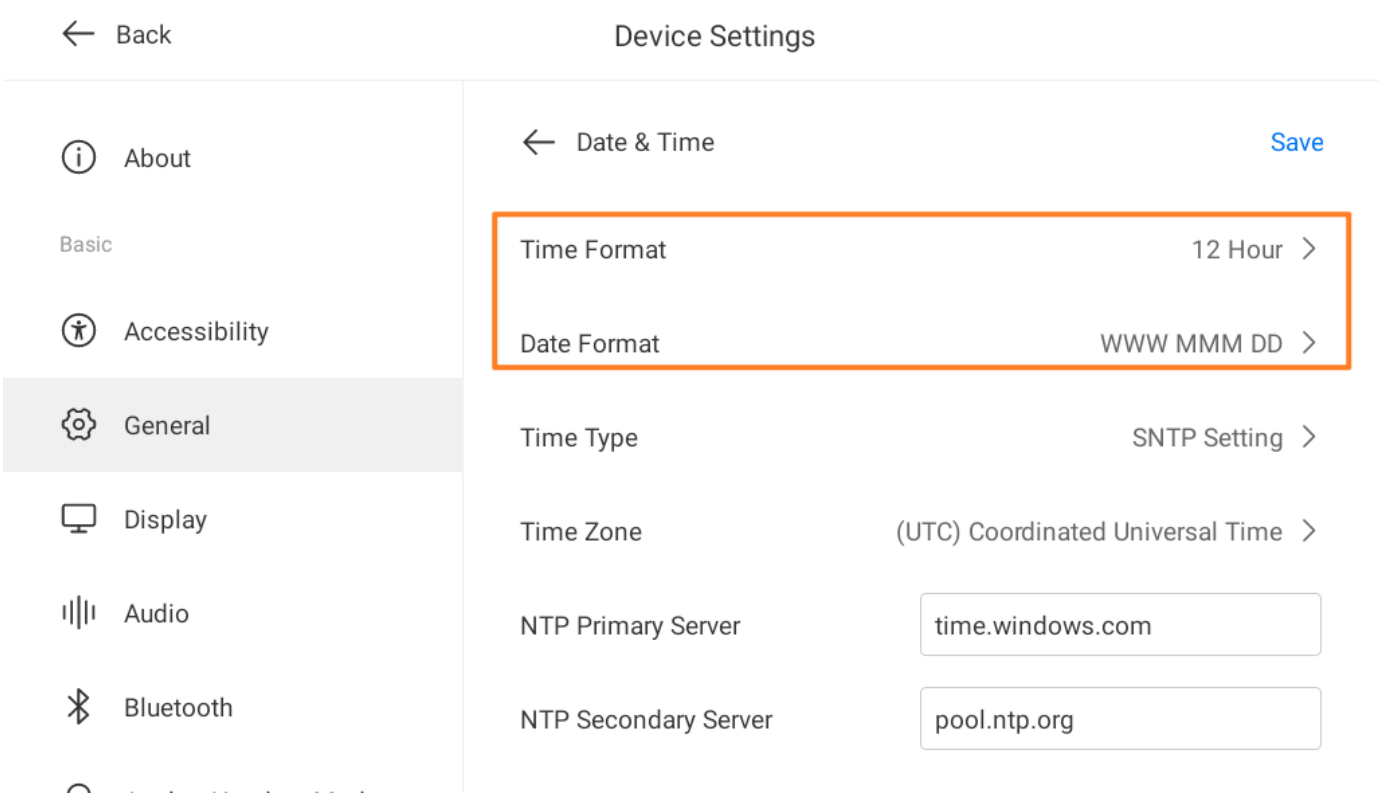
| Parameters | Permitted Values | Default | Description |
|---|---|---|---|
| local_time.manual_time_enable | **0**- Disabled (obtain time and date from NTP server)<br>**1**- Enabled (obtain time and date from manual settings) | 0 | It enables or disables the device to obtain time and date from manual 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 customize the date format as required.

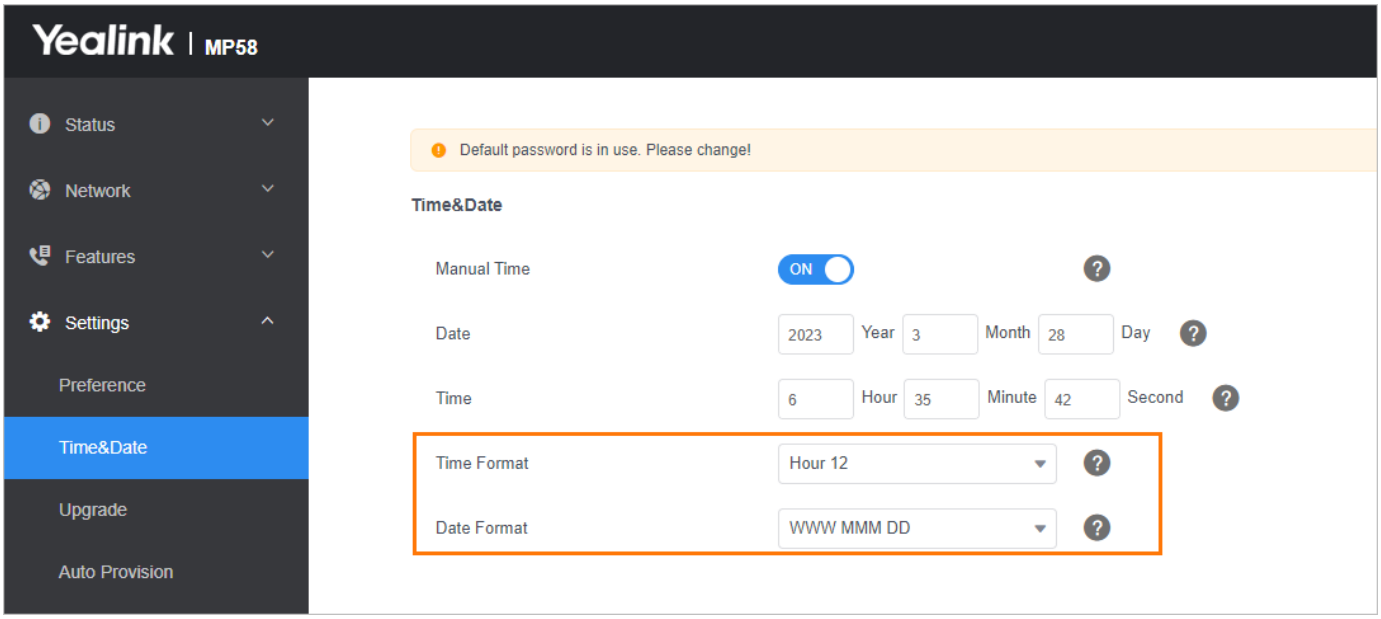
## Via Device User Interface

1. Go to **More** > **Settings** > **General** > **System Settings** > **General** > **Time & Date** > **Time Format**/**Date Format**.




## 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**.




# 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

| Parameters | Permitted Values | Default | Description |
|---|---|---|---|
| local_time.time_format | **0**-Hour 12, the time will be displayed in 12-hour format with AM or PM specified.<br>**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_format | **0-** WWW MMM DD<br>**1-** DD-MMM-YY<br>**2-** YYYY-MM-DD<br>**3-** DD/MM/YYYY<br>**4-** MM/DD/YY<br>**5-** DD MMM YYYY<br>**6-** WWW DD MMM<br>**7-** MM/DD/YYYY<br>Use the following mapping:<br>WWW represents the abbreviation of the week; | 0 | It configures the date format. |

| | | | |
|---|---|---|---|
| | DD represents a two-digit day;<br>MM represents a two-digit month;<br>MMM represents the first three letters of the month;<br>YYYY represents a four-digit year<br>YY represents a two-digit year. | | |

# Backlight

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

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

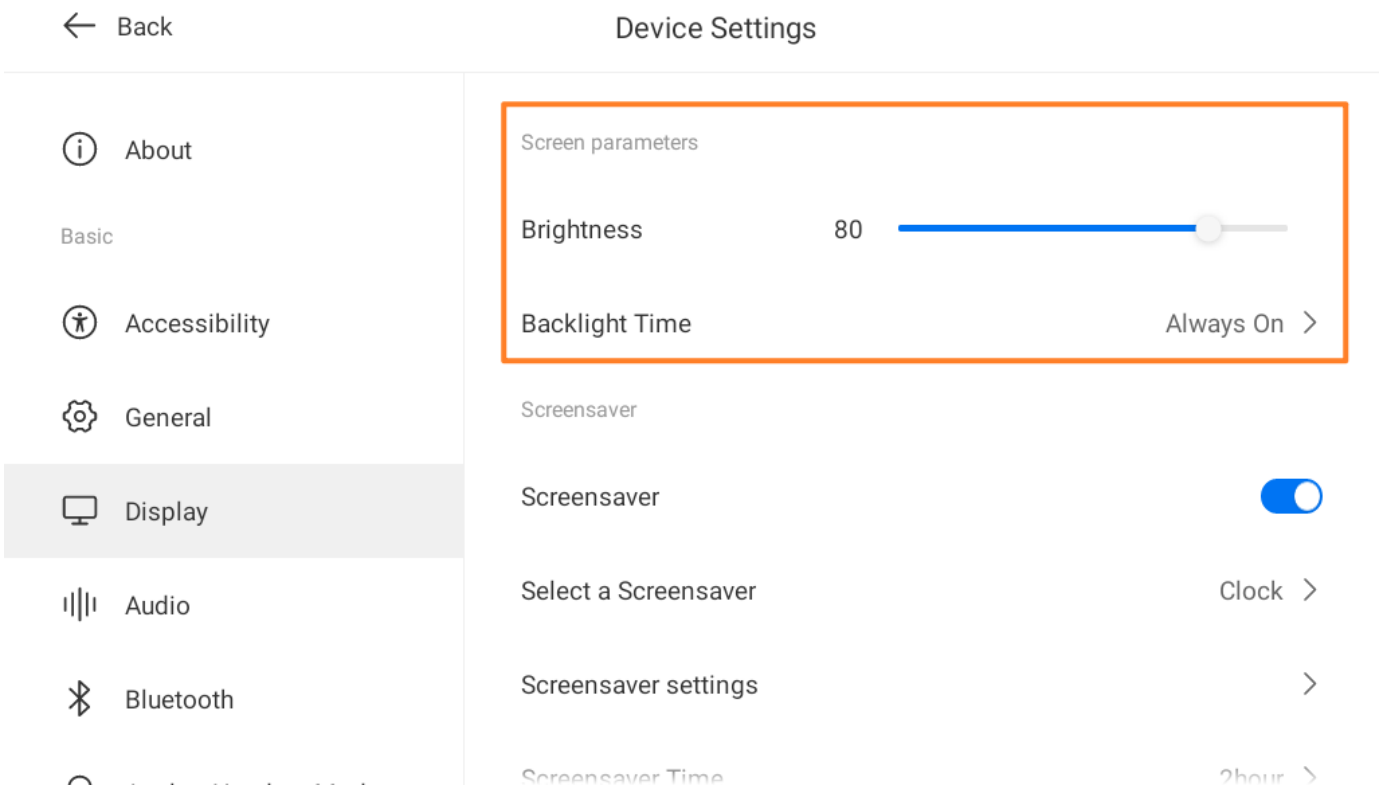
**Backlightness**: The brightness level of the LCD backlight when the device is active.

**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.
- 30min, 1h, 2h, 4h, 6h, 8h, or 12h: Backlight is changed when the device is inactive after the designated time (in seconds).

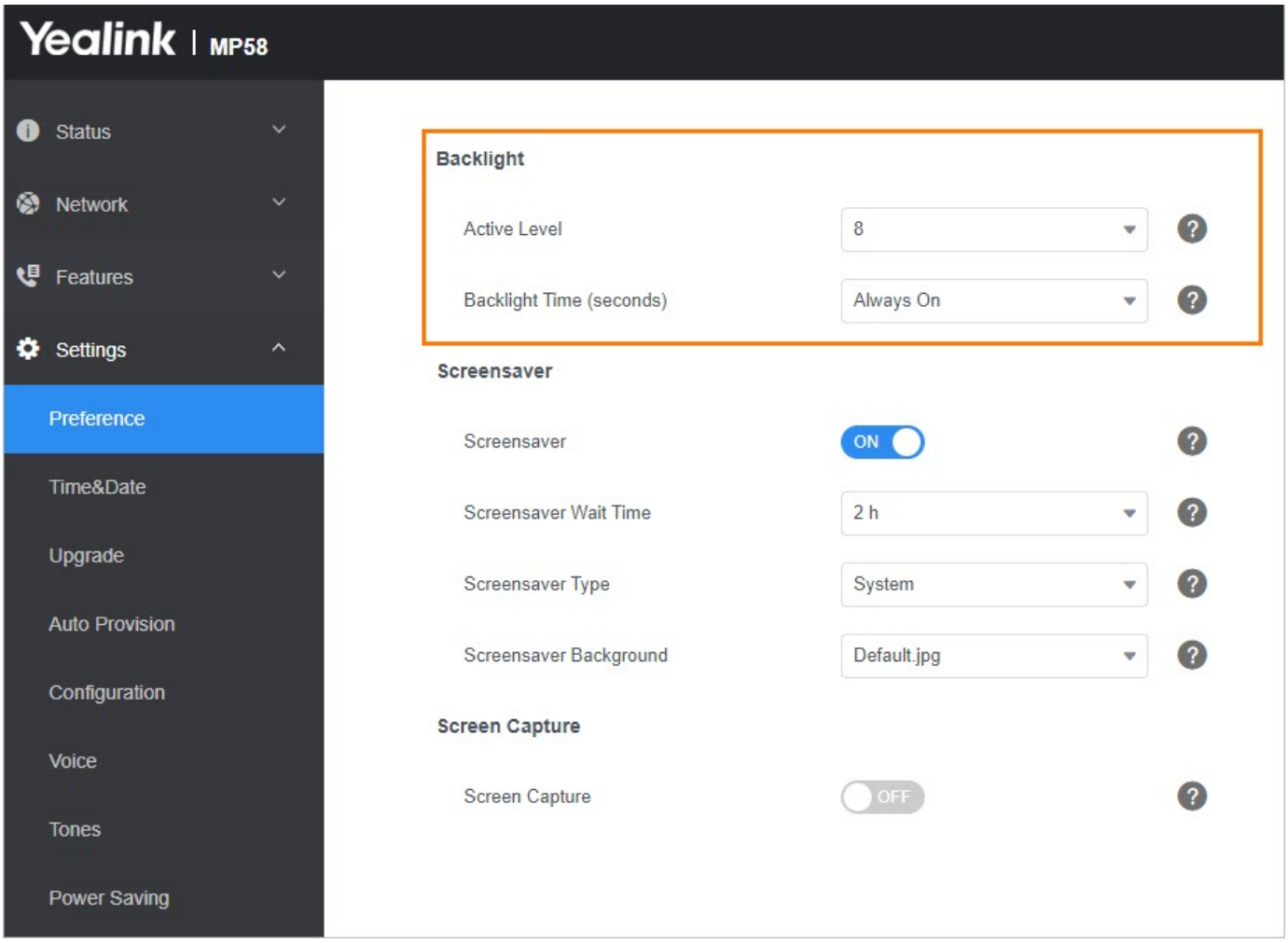
## Via Device User Interface

1. Go to **More** > **Settings** > **General** > **System Settings** > **Display** > **Screen parameters**.




## Via Web User Interface

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




# 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<br>3600-1<br>h<br>7200-2<br>h<br>14400-4<br>h<br>21600-6<br>h<br>28800-8<br>h<br>43200-1<br>2 h | | |

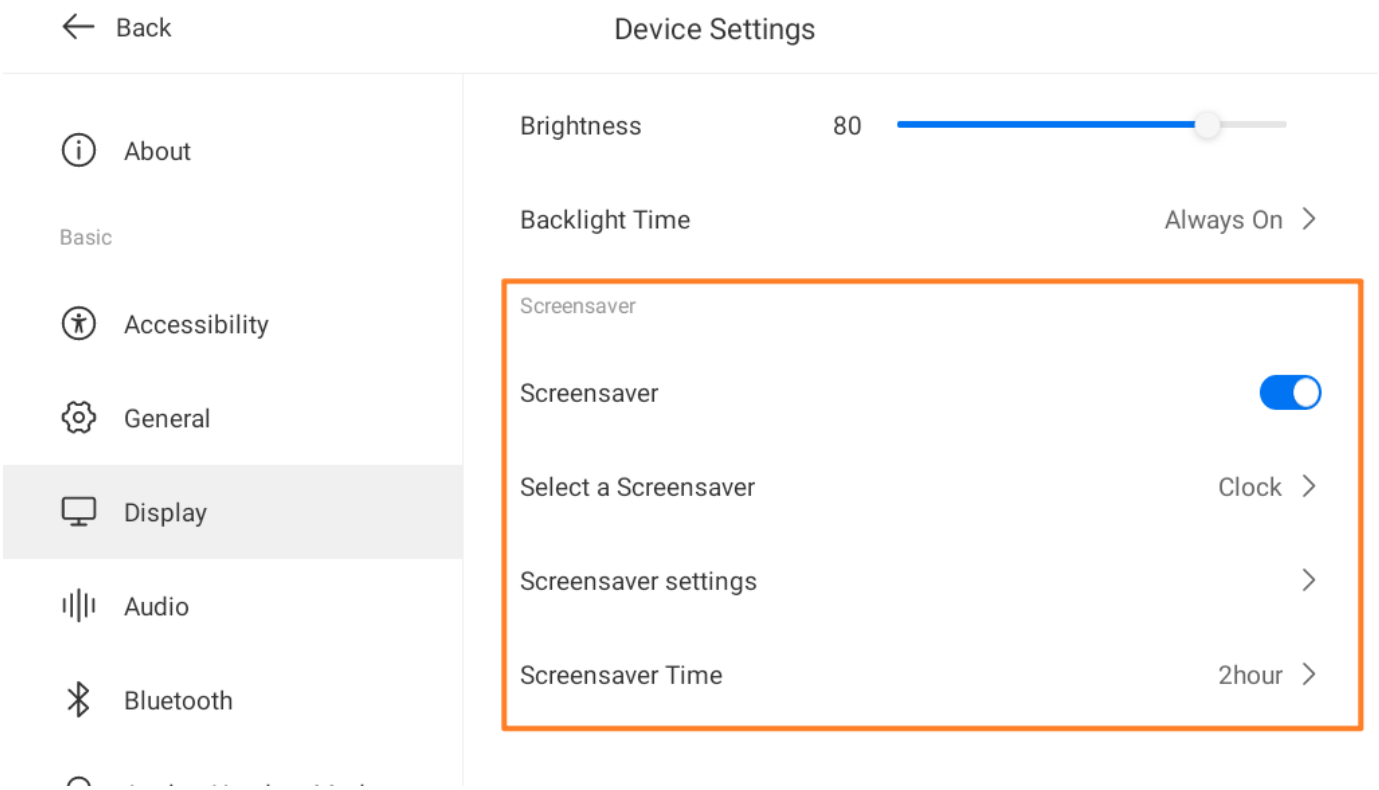
# Screen Saver

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.

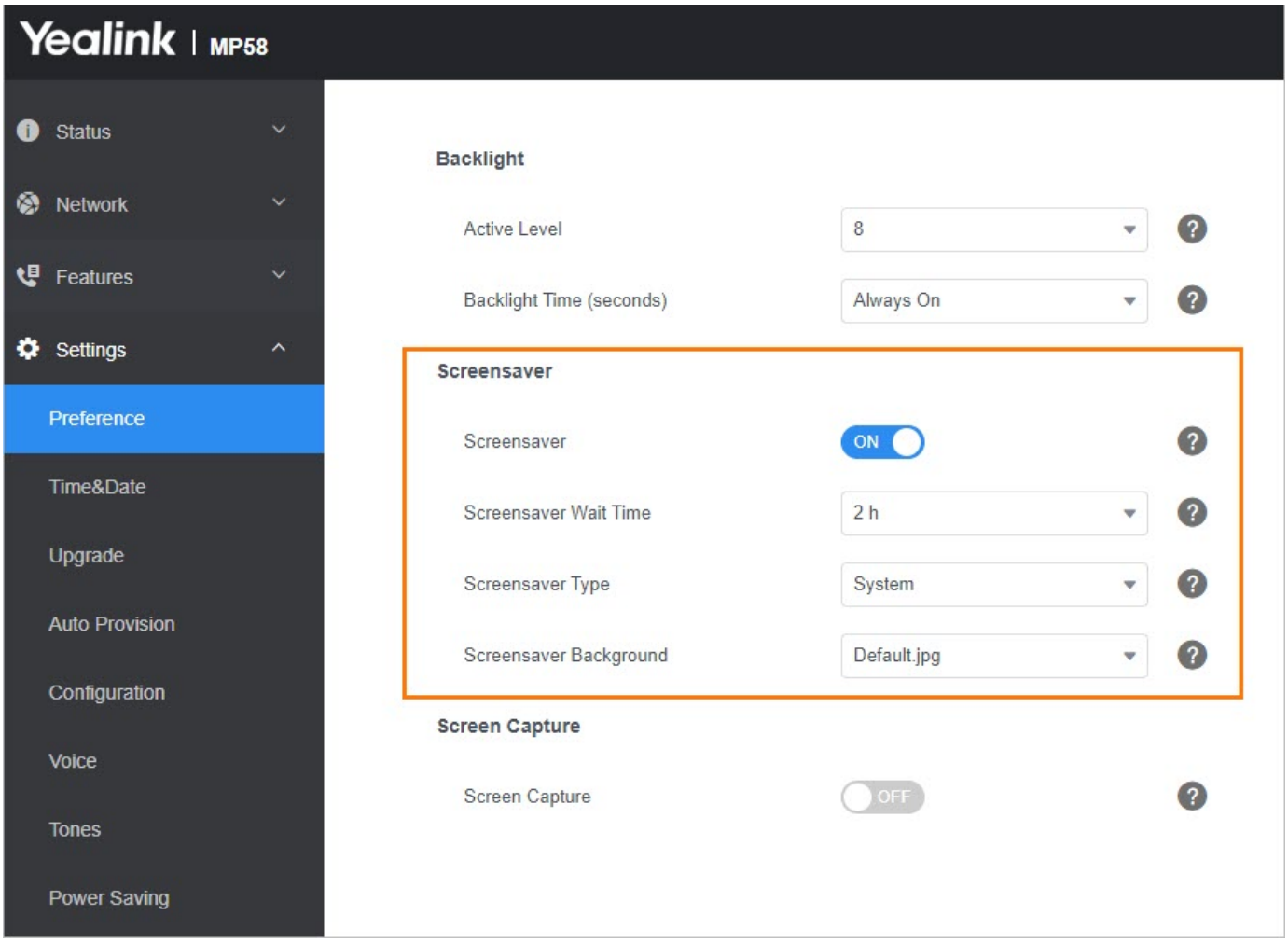
## Via Device User Interface

1. Go to **More** > **Settings** > **General** > **System Settings** > **Display** > **Screensaver**.




## Via Web User Interface

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




# 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<br>**1**-Enabled | 1 | It enables or disables the screen saver. |
| screensaver.wait_time | 30-30 s<br>60-1 min | 900 | It configures the time (in seconds) that the device waits in |

| | | | |
|---|---|---|---|
| | 120-2 min<br>300-5 min<br>600-10 min<br>900-15 min<br>1200-20 min<br>1800-30 min<br>2700-45 min<br>3600-1 h<br>7200-2 h | | the idle state before the screen saver starts. |
| screensaver.type | **0**-System, the LCD screen will display the built-in picture.<br>**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<br>01.png<br>02.png<br>03.png<br>04.png<br>05.png<br>06.png<br>07.png<br>08.png | Default.jpg | It configures the background for the screen saver. |
| screensaver.delete | String | Blank | It deletes the specified or all custom screensaver background.<br>Example: |

| | | | |
|---|---|---|---|
| | | | - Delete all custom screensaver background: "screensaver.delete = http://localhost/all"<br>- Delete a custom screensaver background (for example, Screencapture.jpg): "screensaver.delete = http://localhost/Screencapture.jpg" |

# Language

## Introduction

Zoom 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.

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 | English (United States), English (United Kingdom), | Engli | It configures the |

| | | | |
|---|---|---|---|
| g.wui | Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian, Japanese or the custom language name. | sh (United States) | 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: Yealink Support.

**NOTE**

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

# Language for Device Display Customization

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.

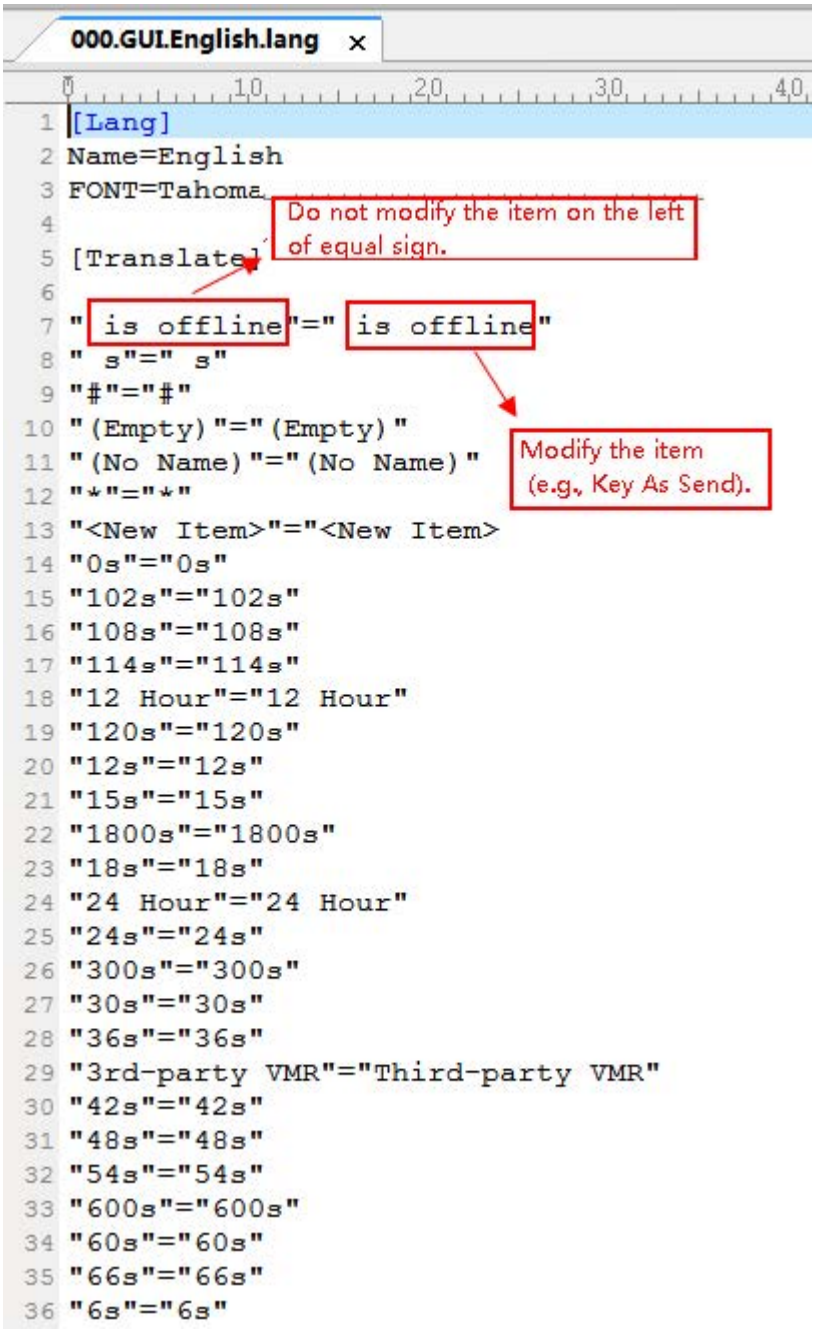
## Customize a Language Pack for Device Display

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 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:




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

## Customize Language for Device Display 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

| Para | Permitted Values | Default | Description |
|---|---|---|---|

| meter | | t | |
|---|---|---|---|
| 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. |

## Via Device User Interface

**Procedure**

1. Select the method according to your device:

| VP59/MP5X/CP960 | 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). |

# 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:

```
var _objTrans =
{

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

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

Do not modify the item on the left of cclon.

Modify the item

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

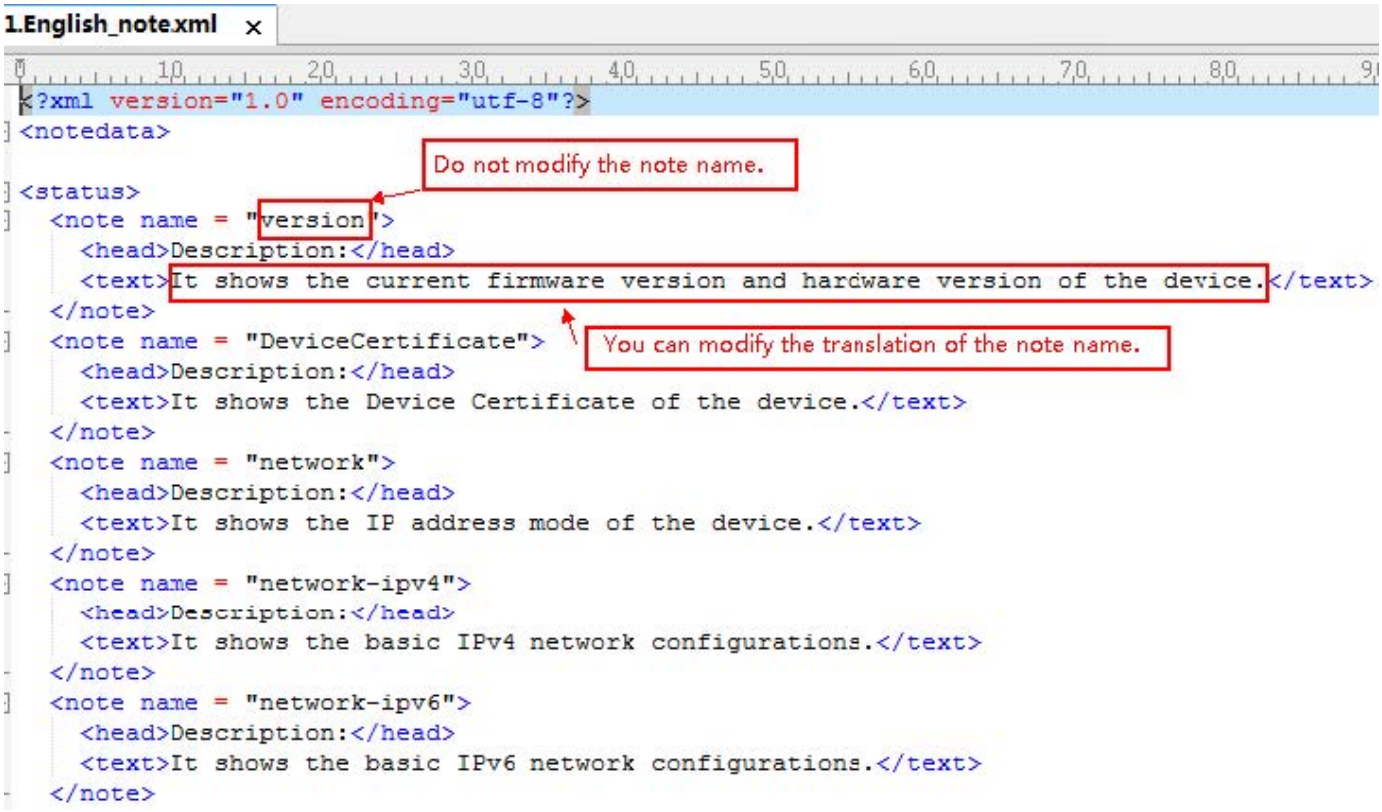
## Customize a Language Pack for Note Display

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 to the provisioning server.

## Custom Language for Web and Note Display Configuration

If you want to add a new language (for example, Wuilan) to devices, prepare the language file named as "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 the web user interface. | URL within 511 characters<br>For example: "http://localhost/X.GUI.name.lang".<br>X starts from 14, "name" is replaced with the language name | Blank |
| wui_lang_note.ur | It configures the access URL of the custom note language pack for web user | URL within 511 characters<br>For example: "http://localhost/ | Blan |

| | | | |
|---|---|---|---|
| l | interface. | X.name_note.xml"<br>X starts from 13, "name" is replaced with the language name | k |
| 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 Shared Line Groups

If you want to set up shared line groups, please refer to the following Zoom docs:

- Setting up shared line groups
- Changing shared line group settings
- Setting up and using group call pickup

# Manage Voicemails

Phone users, auto receptionists, call queues, and shared line groups can have their own dedicated voicemail/videomail inbox. You can allow callers to leave voicemails by change the extension's routing options to route to the extension's voicemail.

Admins can access a voicemail/videomail inbox for a phone user, auto receptionist, call queue, or shared line groups. You can view, play, or delete messages. Please refer to the Zoom doc: Viewing extensions' voicemail or videomail.

# Set Up Hot Desking

Phone users, auto receptionists, call queues, and shared line groups can have their own dedicated voicemail/videomail inbox. You can allow callers to leave voicemails by change the extension's routing options to route to the extension's voicemail.

Admins can access a voicemail/videomail inbox for a phone user, auto receptionist, call queue, or shared line groups. You can view, play, or delete messages. Please refer to the Zoom doc: Viewing extensions' voicemail or videomail.

# Set Up Auto Receptionist

If you want to set up auto receptionist, please refer to the following Zoom docs:

- Managing auto receptionists
- Changing auto receptionist settings

# Call Park and Retrieve

Call park allows phone users to place a call on hold and let another phone user resume the call from any phone or Zoom client. After parking a call, Zoom Phone generates a retrieval code. Any other phone user can use the retrieval code to resume the call. Admins can set routing rules if parked calls are not answered after a specified amount of time.

Please refer to Zoom doc How to change call park settings (admin).

# Set Up Call Queue

If you want to set up call queue, please refer to the following Zoom docs:

- Managing call queues
- Changing call queue settings
- Setting up and using the call queue pickup code

# 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<br>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 | Blan | It configures the user name of SCEP server. |

| | | | |
|---|---|---|---|
| | | k | |
| 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.sc ep.csr.st ate | String within 64 characters | Bl an k | It configures the state/province name used to generate the CSR.<br>**NOTE**<br>It can not be abbreviated and should included suffixes such as Inc, Corp or LLC. |
| static.sc ep.csr.c ountry | String within 2 characters | Bl an k | It configures the country name used to generate the CSR.<br>**NOTE**<br>The ISO code of the country/region where the organization is located. |

# Encrypt Configuration Files

## Introduction

Yealink Zoom 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, Zoom.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)
- yealinkencrypt (for Linux platform)

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

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

## Configuration Files Encryption and Decryption

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

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

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

# Encryption and Decryption Configuration

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

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 | 0 | It enables or disables the device only to download the encrypted files. |

| | | | |
|---|---|---|---|
| | whether the files are encrypted or not. And then the device resolves these files and updates the settings onto the device system.<br>**1**-Enabled, the device will only download the encrypted configuration files (for example, sip.cfg, account.cfg, <MAC>-local.cfg) or <MAC>-contact.xml file from the server during auto provisioning, and then resolve these files and update settings onto | | |

| | | | |
|---|---|---|---|
| | the device system. | | |
| 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.<br>**1**-Enabled, the device will download <xx_Security>.enc files (for example, <sip_Security>.enc, <account_Security>.enc) during auto provisioning, and then decrypts these files into the plaintext keys (for example, key2, key3) | 0 | It enables or disables the device to decrypt configuration files using the encrypted AES keys. |

| | | | |
|---|---|---|---|
| | 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). | | |
| 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: # $ % * + , - . : = ? @ [ ] ^ _ { } ~.<br>**Example**: static.auto_provision.aes_key_16.com = 0123456789abcdef<br>NOTE<br>For decrypting, it works only if "static.auto_provision.aes_key_in_file" is set to 0 (Disabled).<br>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_provis | 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). |

| | | | |
|---|---|---|---|
| ion.aes_key_16.mac | | | The valid characters contain: digits, upper-case letters, lower-case letters and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ _ { } ~.<br>Example: static.auto_provision.aes_key_16.mac = 0123456789abmins<br>NOTE<br>For decrypting, it works only if "static.auto_provision.aes_key_in_file" is set to 0 (Disabled).<br>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.

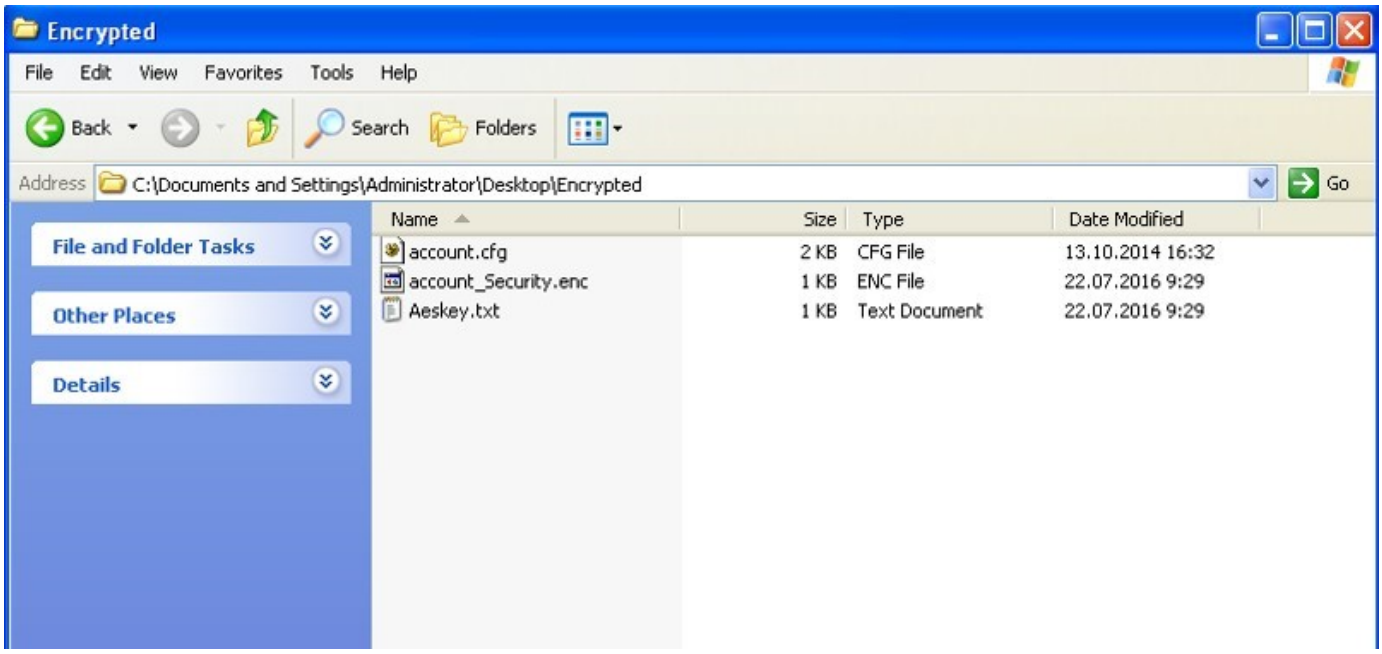
4. (Optional.) Click **Browse** to locate the target directory from your local system in the **Target Directory** field.
5. The tool uses the file folder "Encrypted" as the target directory by default.

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 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).


Encrypted
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\Administrator\Desktop\Encrypted
Go
File and Folder Tasks
Other Places
Details
Name Size Type Date Modified
account.cfg 2 KB CFG File 13.10.2014 16:32
account_Security.enc 1 KB ENC File 22.07.2016 9:29
Aeskey.txt 1 KB Text Document 22.07.2016 9:29

# 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, and TLS 1.2.

## 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 Zoom phones 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 |

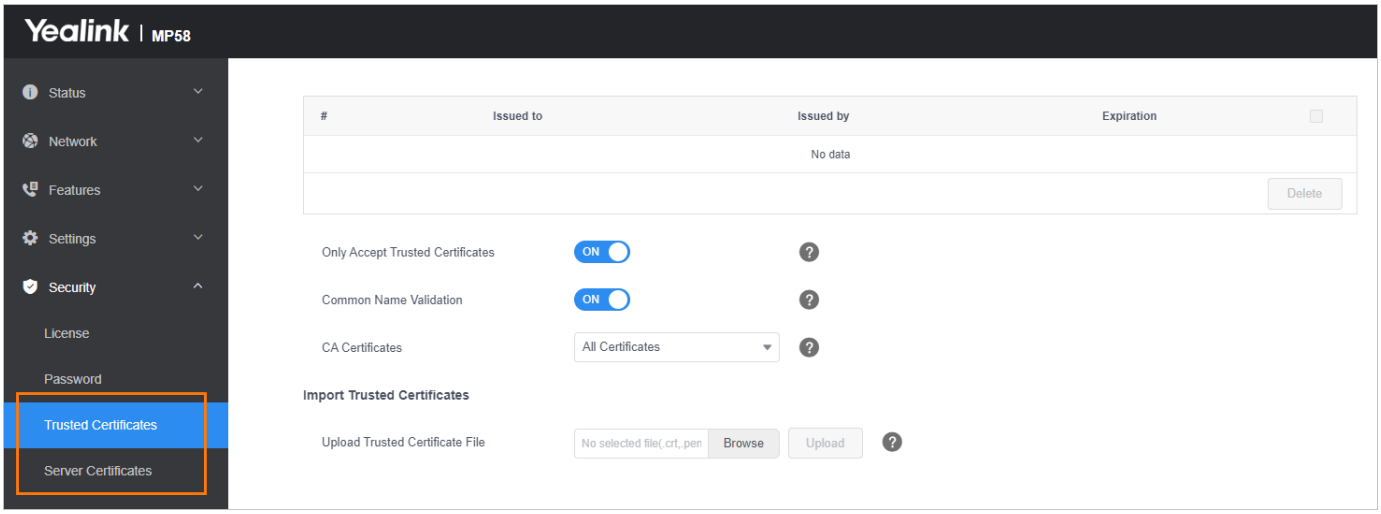
| | |
|---|---|
| Deutsche Telekom Root CA-2 | DigiCert Assured ID Root G3 |
| Equifax Secure Certificate Authority | DigiCert Assured ID Root CA |
| Equifax Secure eBusiness CA-1 | DigiCert Global Root G2 |
| Equifax Secure Global eBusiness CA-1 | DigiCert Global Root G3 |
| GeoTrust Global CA | DigiCert 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**.
3. Configure the certificate parameters and upload the correspondinf 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.<br>**1**-Enabled, the device will authenticate the server certificate based on the trusted certificates list. Only | 1 | It enables or disables the device to only trust the server certificates listed in the Trusted Certificates list. |

| | | | |
|---|---|---|---|
| | when the authentication succeeds will the device trust the server. | | |
| static.security.ca_cert[1] | **0**-Default Certificates<br>**1**-Custom Certificates<br>**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.<br>**Example**:<br>"static.trusted_certificates.url = http://192.168.1.20/tc.crt"<br>NOTE<br>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.<br>NOTE<br>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<br>**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.

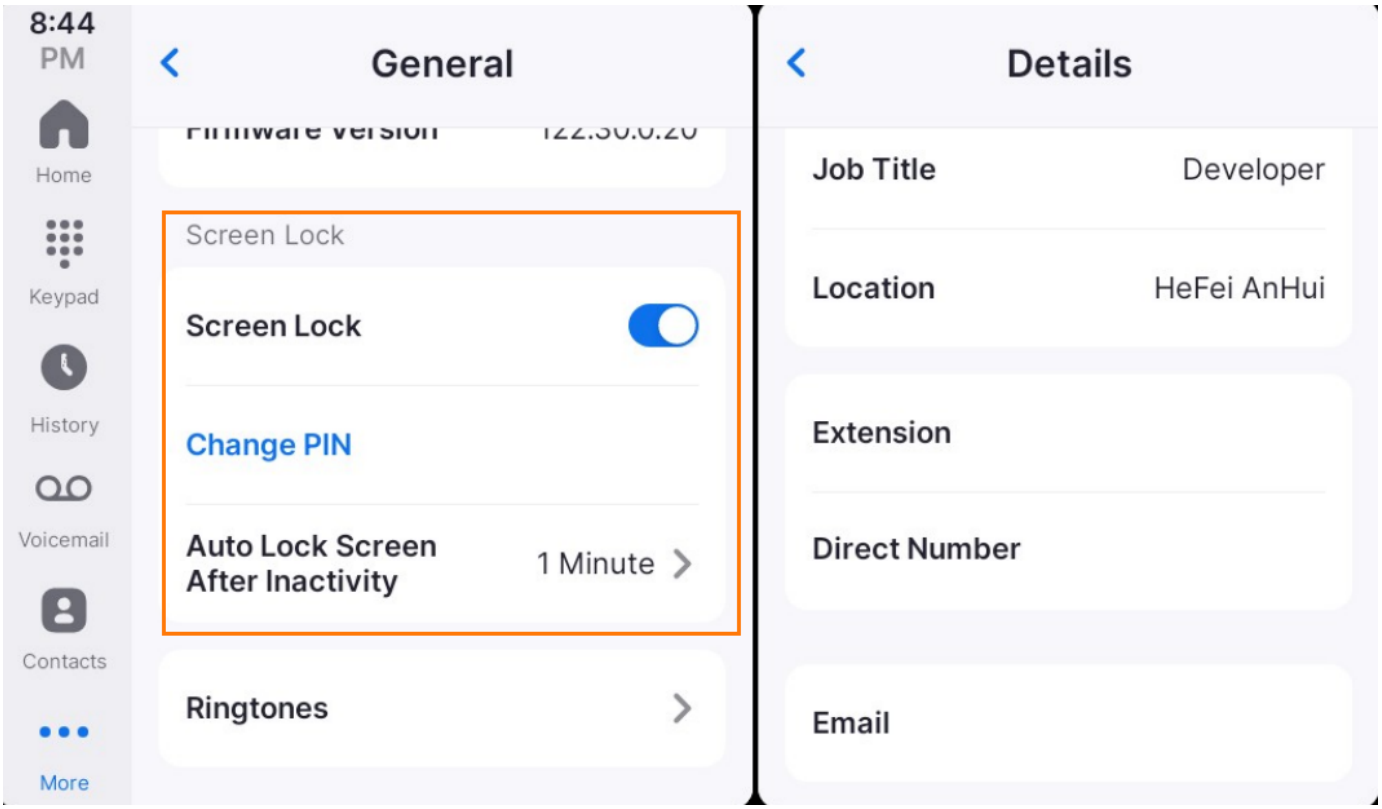
# Phone Lock

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

## Phone Lock Configuration

### Via Device User Interface

1. Go to **More** > **Settings** > **General** > **Screen Lock**.
2. Set the corresponding parameters.




### 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

| Parame | Per | Defaul | Description |
|---|---|---|---|

| ter | mitted Values | t | |
|---|---|---|---|
| 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.<br>NOTE<br>It works only if “phone_setting.phone_lock.enable” is set to 1. |
| phone_ | Stri | See | Example: "phone_setting.phone_lock.complex_pin_rule.1 =^((?!(((9(? |

| | | | |
|---|---|---|---|
| setting.phone_lock.complex_pin_rule.X[2] | ng with in 511 characters | the following to get the default value*. | =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)).)*$" means not allowed three consecutive numbers.<br>"phone_setting.phone_lock.complex_pin_rule.2 = ^((?!(\d)\1{2}).)*$ "means not allowed three repeated numbers.<br>"phone_setting.phone_lock.complex_pin_rule.3 = ^((?!((admin)\|(administrator)\|(var)\|(user)\|(test))).)*$" means not contain 'admin', 'administrator', 'var', 'user','test' strings.<br>"phone_setting.phone_lock.complex_pin_rule. 4 = (?!^(\d+\|[a-zA-Z]+\|[~!@#$%^&*?]+)$)^[\w~!@#$%^&*?]{7,20}$" 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}$

# FAQ

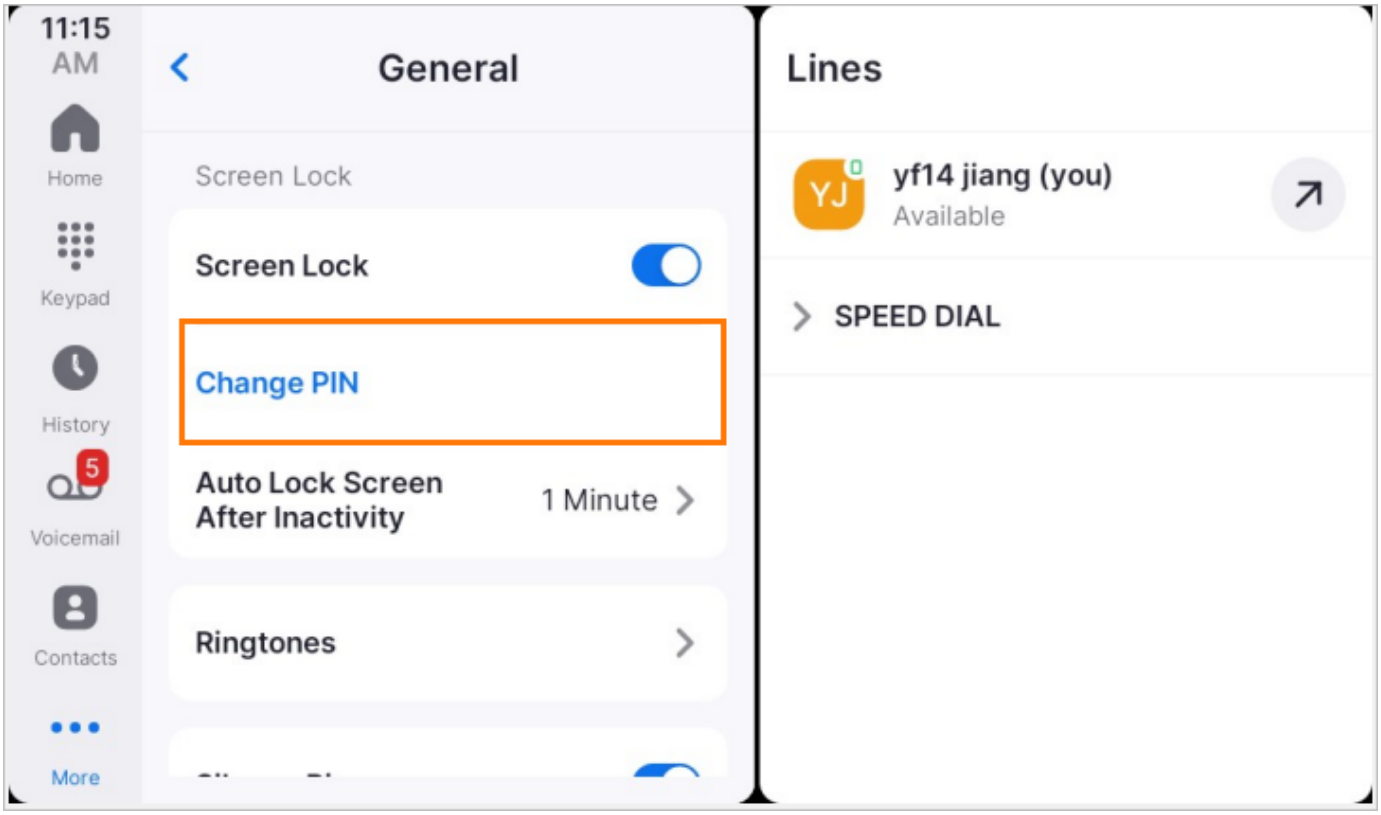
## Can I change the unlock PIN length?

Currently, the default PIN length should include 6 digits and cannot be changed.

## Can I change the screen lock PIN?

Yes.

1. Go to **More** > **Settings** > **General** > **Screen Lock** > **Change PIN**.




2. Enter your old PIN, enter your new PIN, and confirm the new PIN.

## What should I do if I forget the screen lock PIN?

If you forget your screen lock PIN, you need to reset your phone to factory settings.

Long press the pound key (#) and the star key ( * ) for about 6 seconds when the phone is idle.

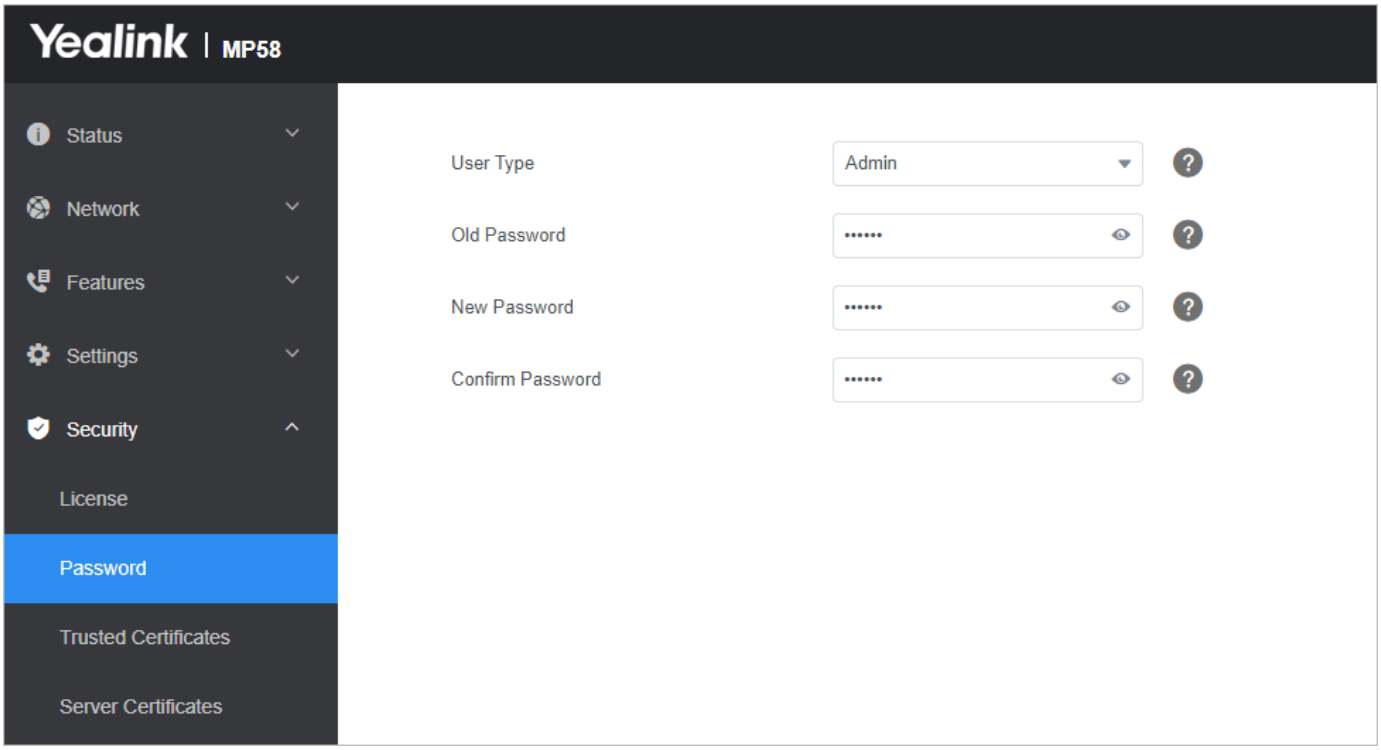
# Administrator Password

## Change Default Administrator Password

The default administrator password is "admin" and you can change it.

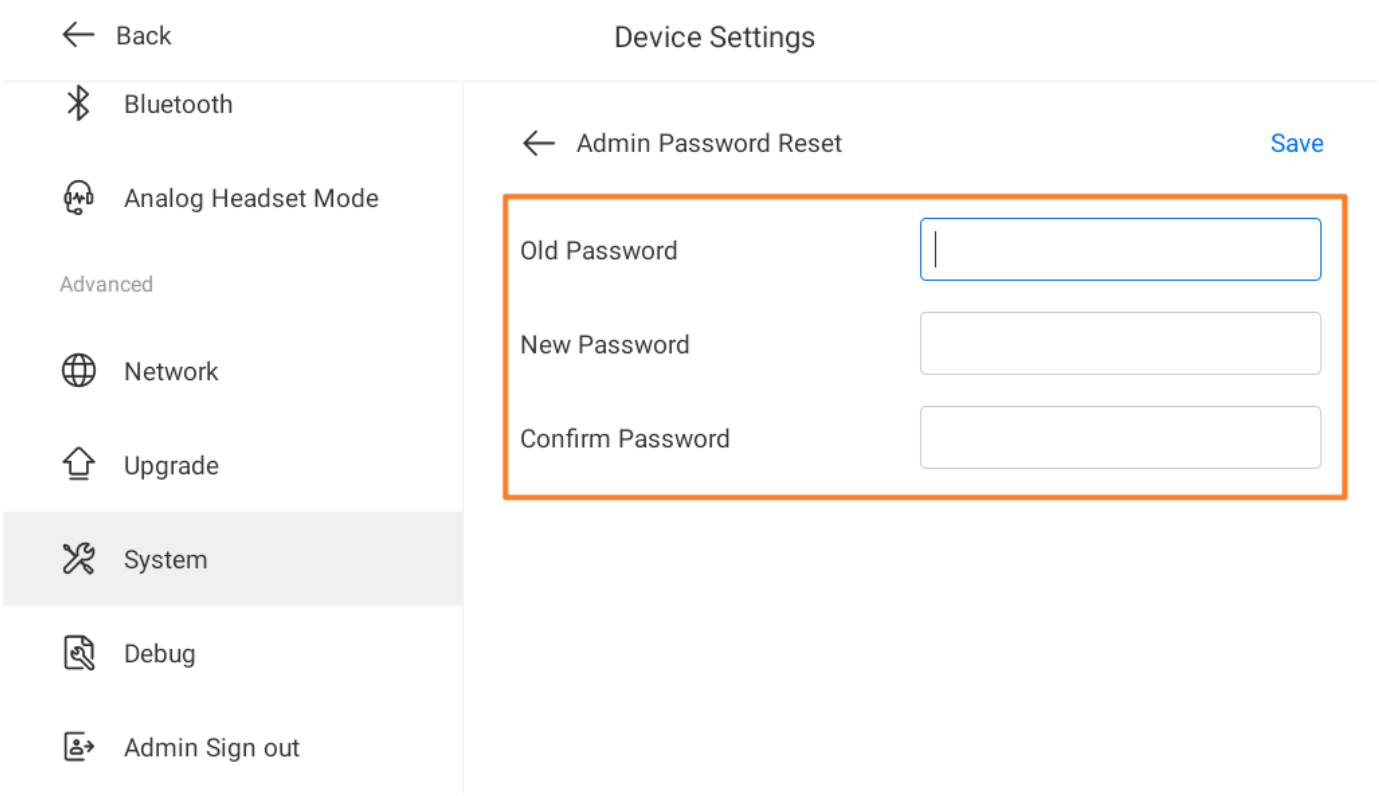
### Via Web User Interface

1. Log in to the phone web user interface as an admin.
2. Go to **Security** > **Password**.
3. Enter the old password, the new password, and the confirm password.
4. Click **Confirm** to change the password.




### Via Device User Interface

1. Go to **More** > **Settings** > **General** > **System Settings** > **System** (default password: admin) > **Admin Password Reset**.
2. Enter the old password, the new password, and the confirm password.
3. Click **Save** to change the password.




# Via Auto Provisioning

static.security.user_name.admin
static.security.user_password

| Parameter | Permitted Values | Default | Description |
|---|---|---|---|
| static.security.user_n | String within 32 characters | admin | It configures the user name of the administrator for the device’ s web user interface access. |

| | | | |
|---|---|---|---|
| name.admin | | | |
| 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 user to 123. "static.security.user_password = admin:456" means setting the password of administrator to 456.<br>NOTE<br>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. |

# Forgot Administrator Password?

If you forgot your administrator password, you can reset your phone to reset the password to the default one "admin".

# 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 permission for configurations on the web user interface and phone user interface. Yealink phones support the access levels of admin, var and user.

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

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

If you enable the feature of complex password, 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 of the user 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.<br>NOTE<br>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.<br>The valid value format is <username> : <new password>.<br>Example:<br>static.security.user_password = user:123 means setting the password of user to 123.<br>static.security.user_password = admin:456 means setting the password of the administrator to 456.<br>NOTE<br>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_ | String within 511 | Blank | It configures the regular expression rules of the password, and the result is the AND operation of multiple regular expressions (up to |

| | | | |
|---|---|---|---|
| rule.X[1] | characters | | 10).<br>**Example**:<br>static.security.custom_password_rule.1 = .{8,} means length of the password more than 8 digits.<br>static.security.custom_password_rule.2 = ^((?!.*(000\|111\|222\|333\|444\|555\|666\|777\|888\|999).*).)*$ means not allowed three consecutive identical numbers.<br>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.<br>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.<br>static.security.custom_password_rule.5 = ^((?!.*(admin\|administrator\|var\|user\|test).*).)*$ means not allowed to contain xxx.<br>NOTE<br>When you set "static.security.custom_password_rule.X" (X=1-10) to be blank, the the feature of complex password is disabled. |

[1] X ranges from 1 to 10.

# Configure User Access Level

For more information, refer to Yealink SIP IP Phones Configuration Guide for User Access Level. The following table lists the parameters you can use to configure the user access level.

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

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

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

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

# Connect Zoom Phone to YMCS or YDMP

## Introduction

You can enable the device management feature to connect device 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

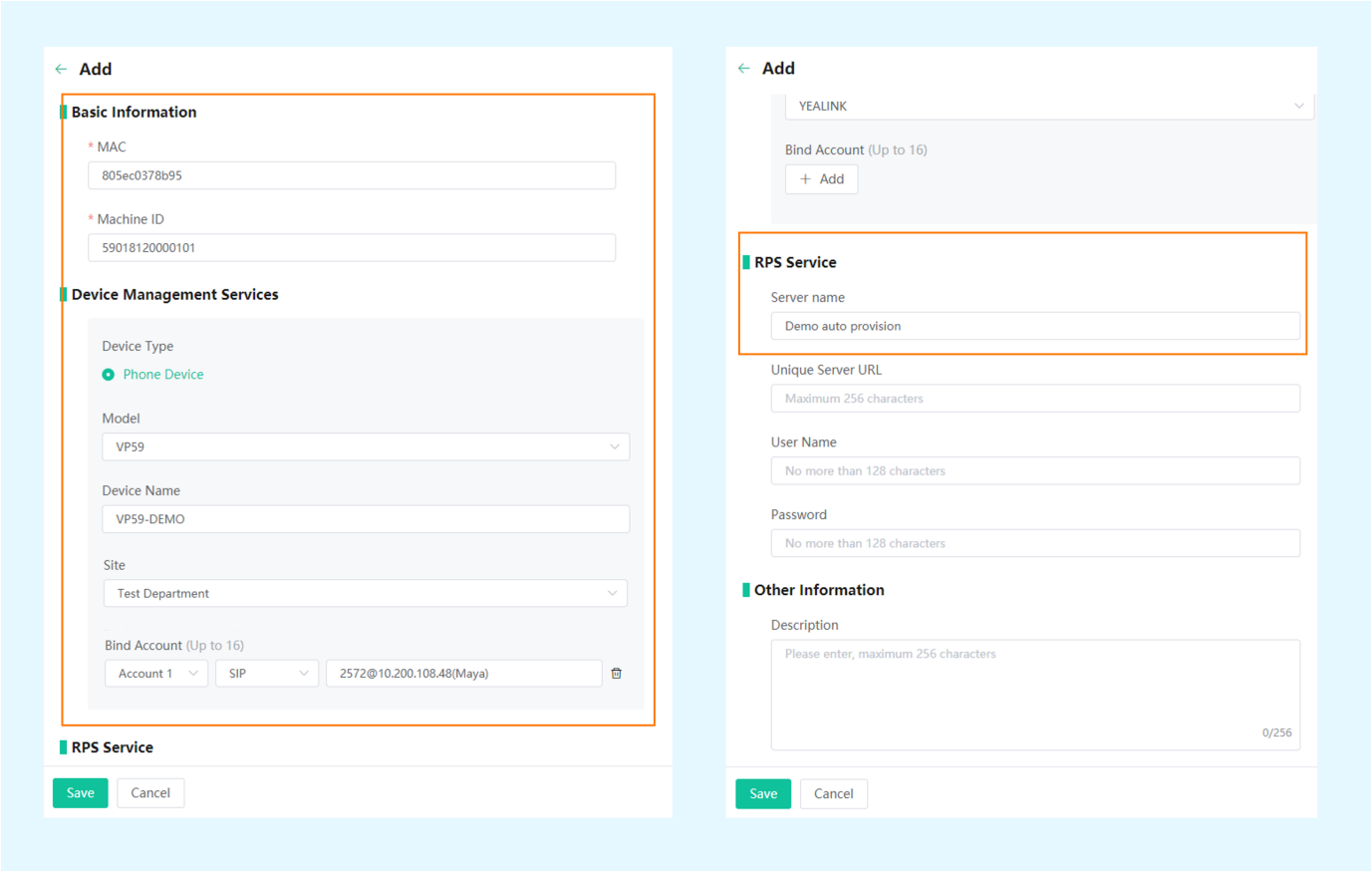
## How to Connect Zoom Phones to YMCS/YDMP

You can connect Zoom phones to YMCS by the following methods:

### 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**.

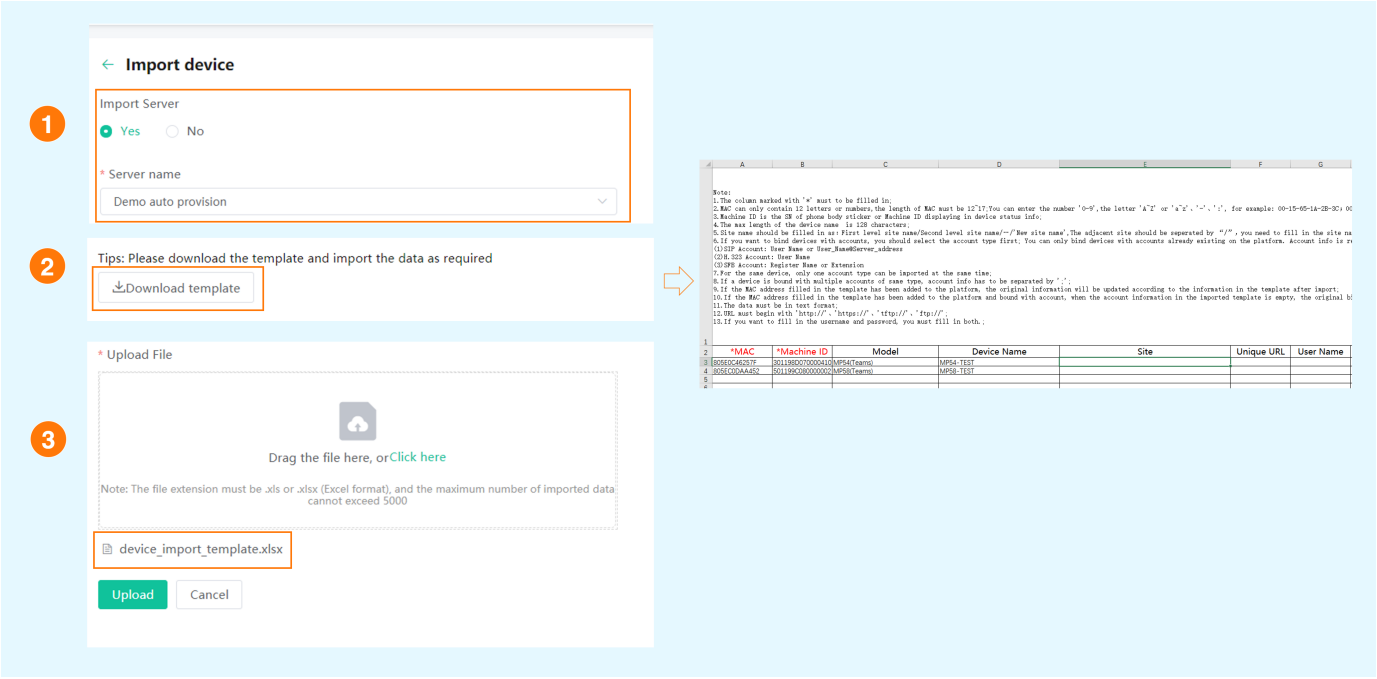


5.

| 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.<br>NOTE<br>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.<br>NOTE<br>• 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.<br>• 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. |

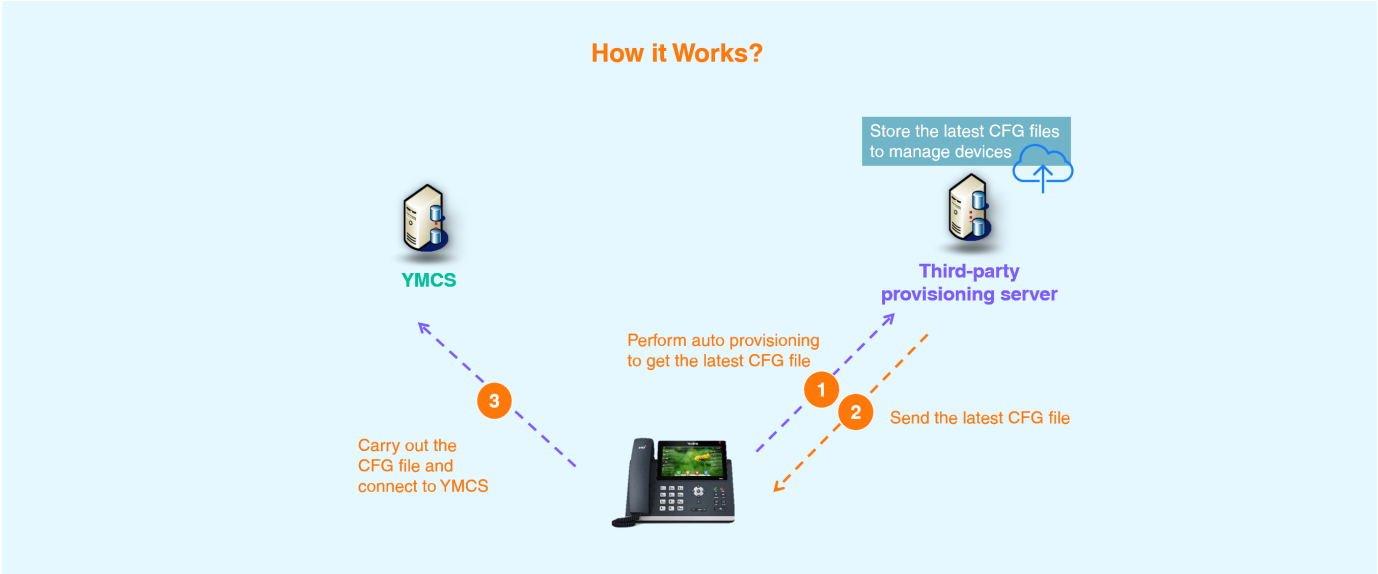
## Add Multiple Devices

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**.




# Configure Parameters via Auto Provisioning

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




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
```

**TIP**

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

1. Configure the following commands:

```
dm.enable =
dm.server.address =
dm.server.port = 9448
```

**TIP**

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 |
|---|---|---|---|
| dm.enable | It enables or disables the device management feature. | 0- Disabled<br>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 |

# Update to the Latest Zoom App

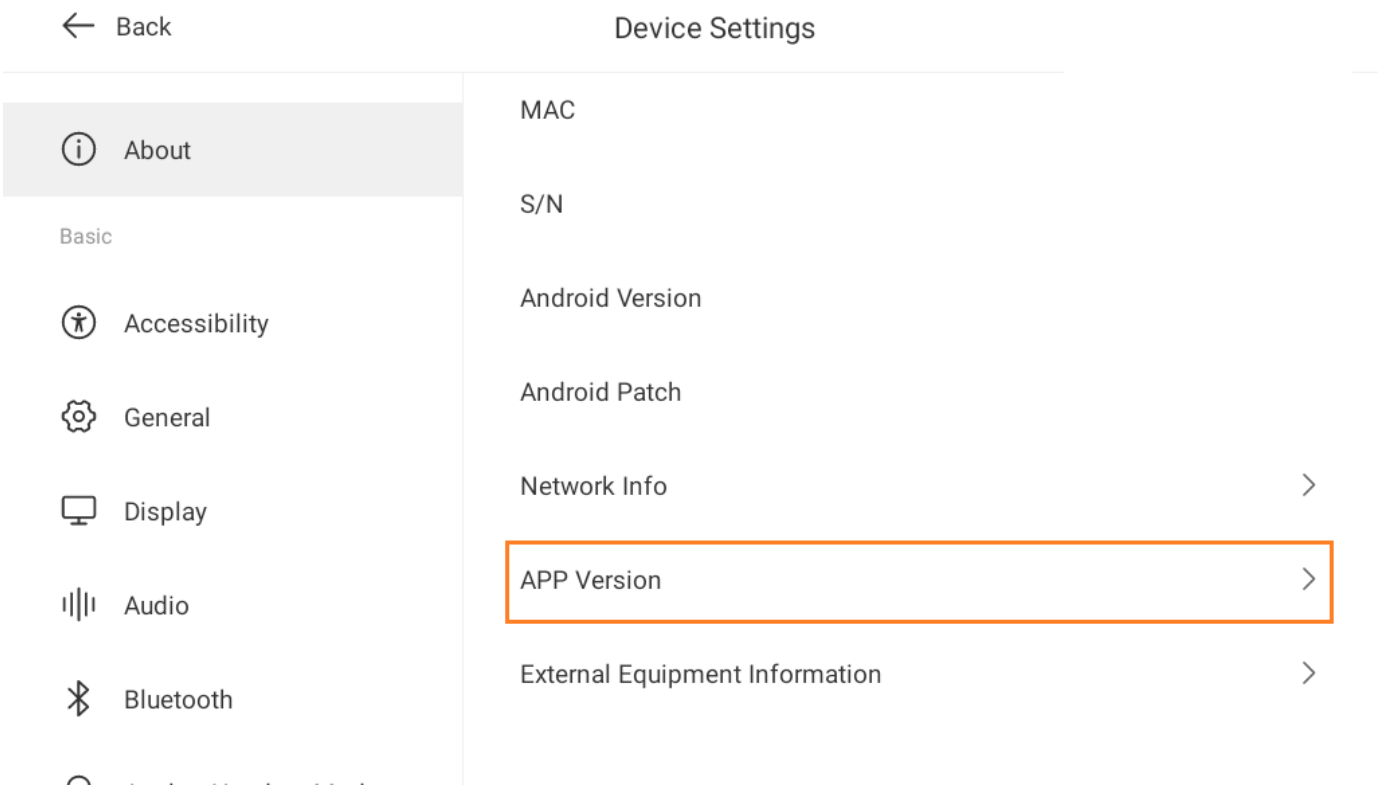
You can update the Zoom app of the MP Zoom phone by the following methods:

- Update the Zoom app on your MP Zoom phone.
- Update the Zoom app on the Zoom admin center.

## Check the Zoom App Version

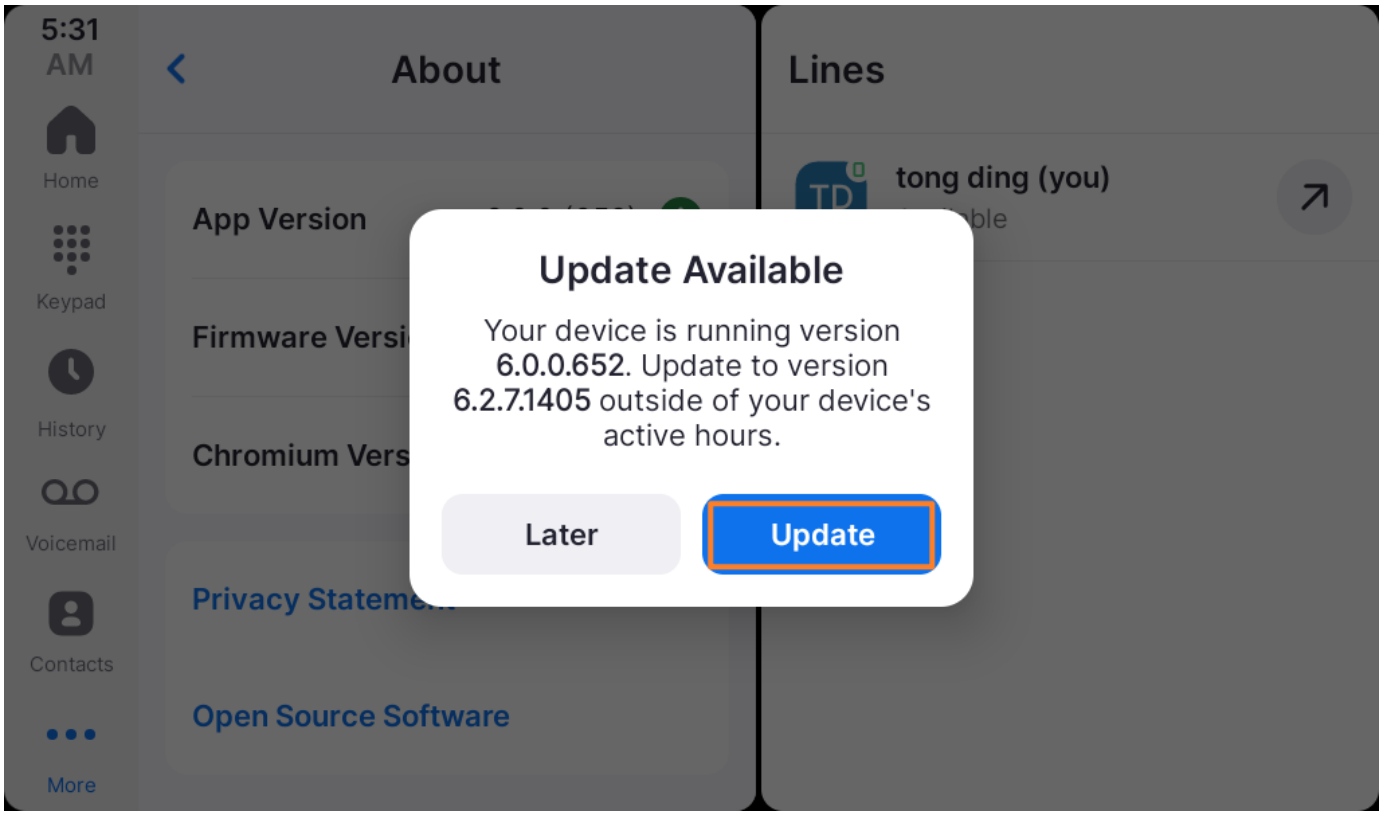
**Procedure**

1. Go to **More** > **Settings** > **General** > **System Settings** > **About** > **App Version**.
2. You can see the detailed version information of the Zoom app.




## Update Zoom App on Your Zoom Phone

1. Go to **More** > **Settings** > **About**.
2. Tap **App Version**. If a new version is available, you can update the Zoom app directly.




# Update Zoom App on Zoom Web Portal

See Zoom doc Remotely upgrading Zoom Room devices with ZDM.

# 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 can update the firmware of Zoom phones to the latest version.

The following sections introduce how to update firmware from the phone web user interface.

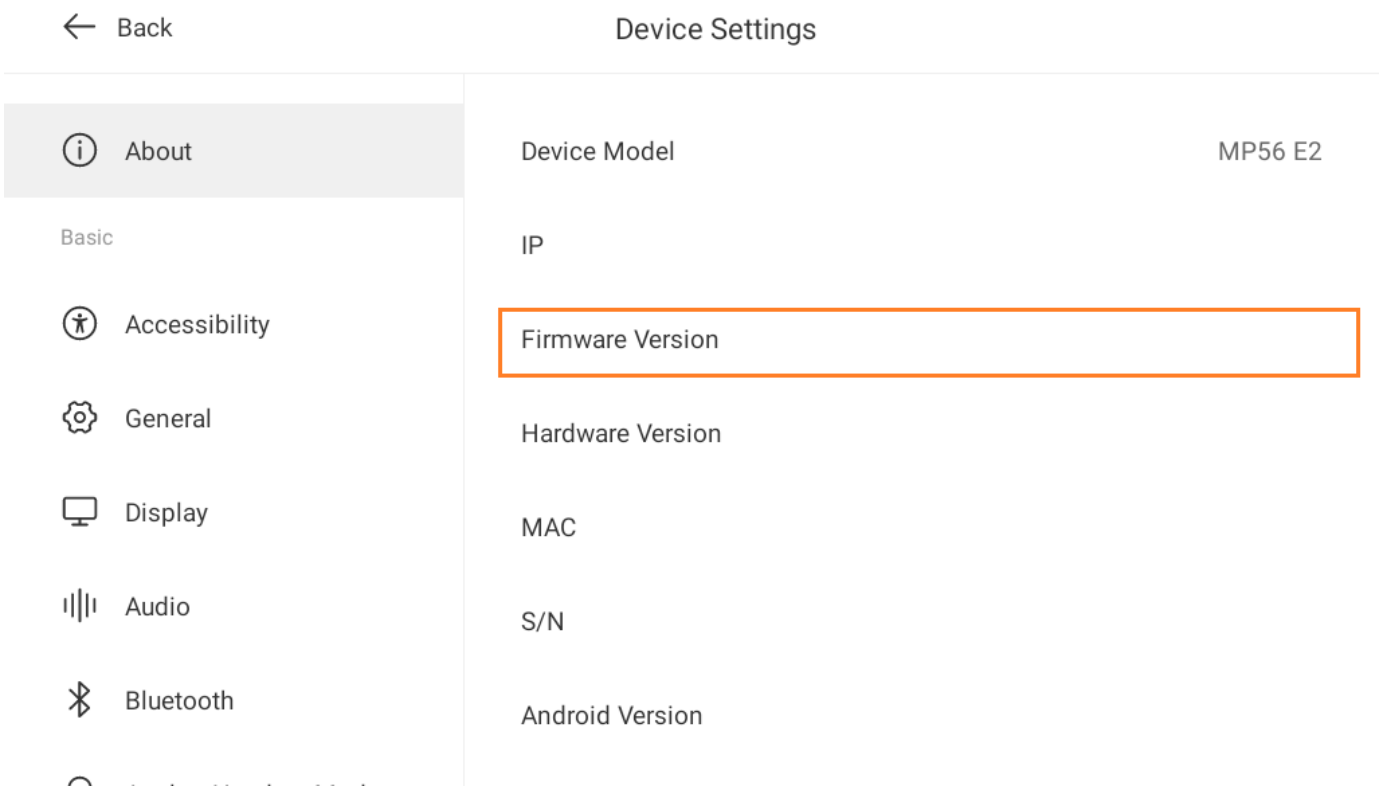
**NOTE**

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

## Step 1: Check the Firmware Version

**Procedure**

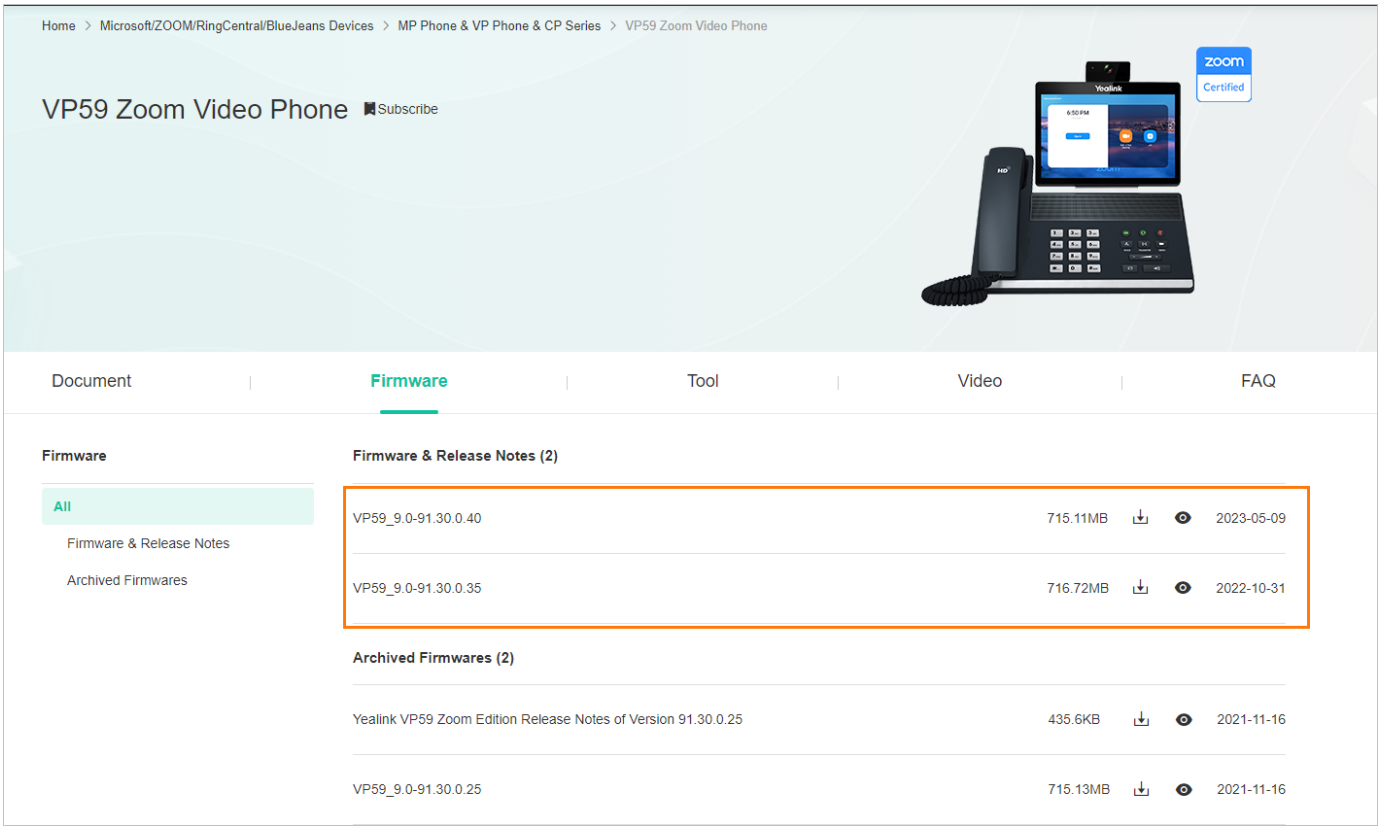
1. Go to **More** > **Settings** > **General** > **System Settings** > **About**.
2. You can see the detailed firmware version information.




## 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.

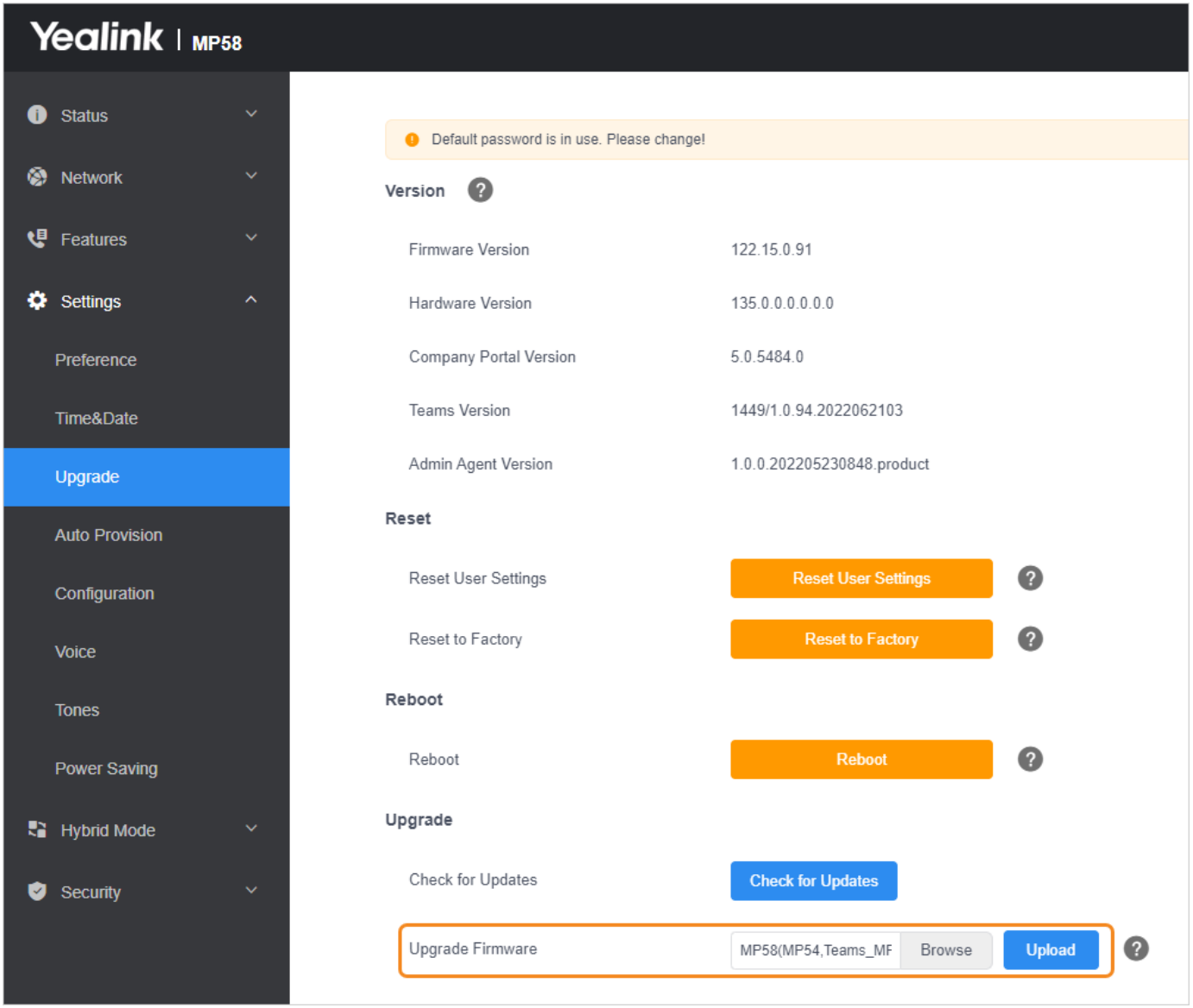



5.

# 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**.

> **CAUTION**
> Do not close and refresh the browser when upgrading firmware via the web user interface.




# 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.

**CAUTION**

Do not unplug the network cables and power cables when upgrading firmware.

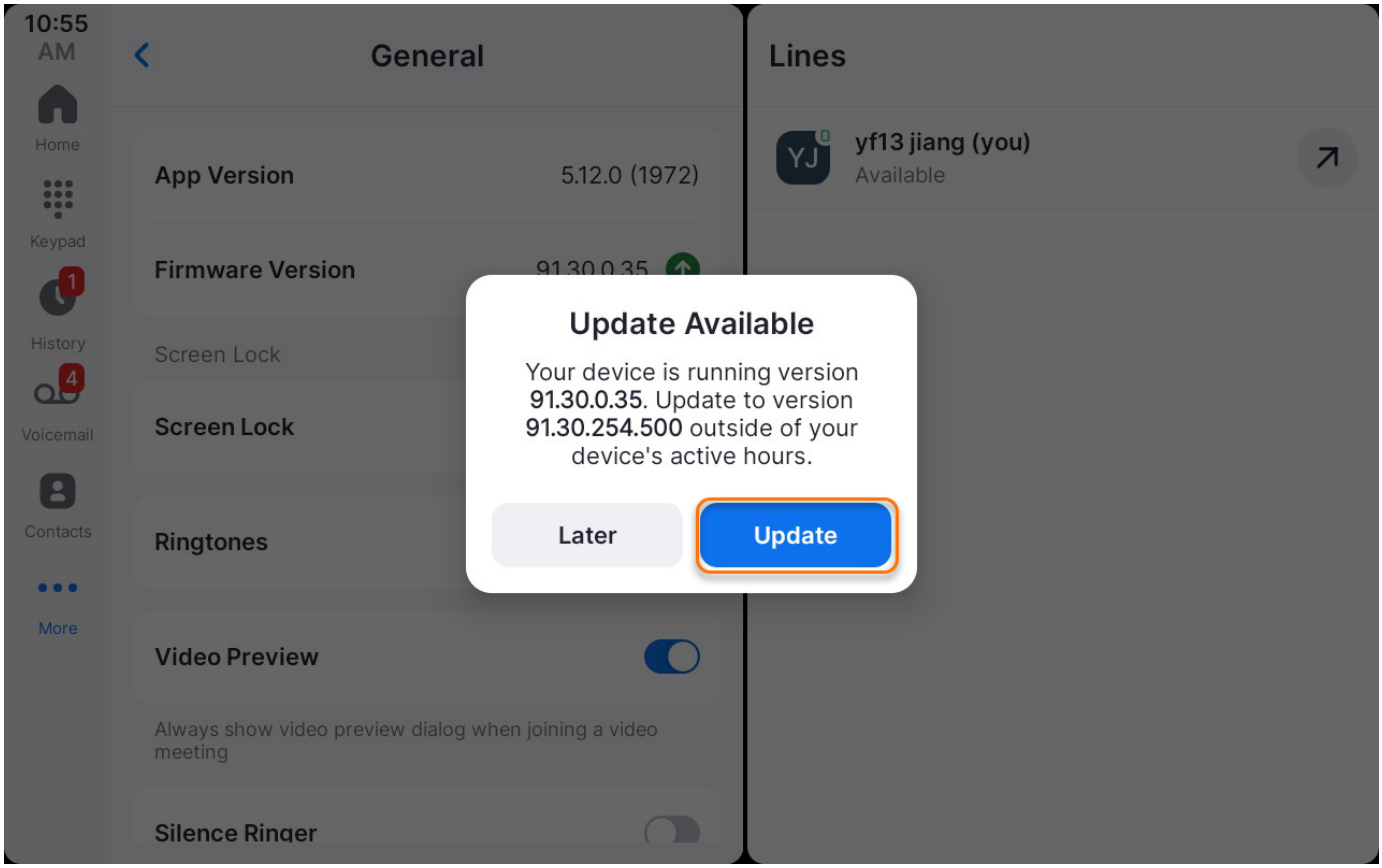
| Parameter | Description | Permitted Values |
|---|---|---|
| static.firmware.url | It configures the access URL of the firmware file.<br>If you change this parameter, the device will reboot to make the change take effect. | URL within 511 characters |

| | | |
|---|---|---|
| over_the_air.url.bth58 | It configures the access URL of the BTH58 handset firmware file. | URL within 511 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 on Your Zoom Phone

1. Go to **More** > **Settings** > **About** > **Firmware Version**.
2. If a new firmware is available, you can update it.




# Step 3 (Option 4): Update Firmware on Zoom Web Portal

See Zoom doc How to upgrade the OS/firmware from with ZDM.

# FAQ

## Forgot the admin default password?

Generally, the admin default password is admin.

If you forgot the password, you can reset the phone to the factory 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.

# Version Converting Introduction

You can also convert Zoom phones into other versions, for example SIP or Teams version, as listed as below:

- To convert from Zoom version to other versions, you need to apply the device license of the target version.
- To convert from other versions to Zoom version, you need to apply the Zoom device license.

| Device | Can be Converted To |
| --- | --- |
| VP59 (Zoom version) | SIP, Zoom, VCS |
| MP58 (Zoom version) | Teams |
| MP56 (Zoom version) | Teams |
| MP54 (Zoom version) | Teams |

# 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.

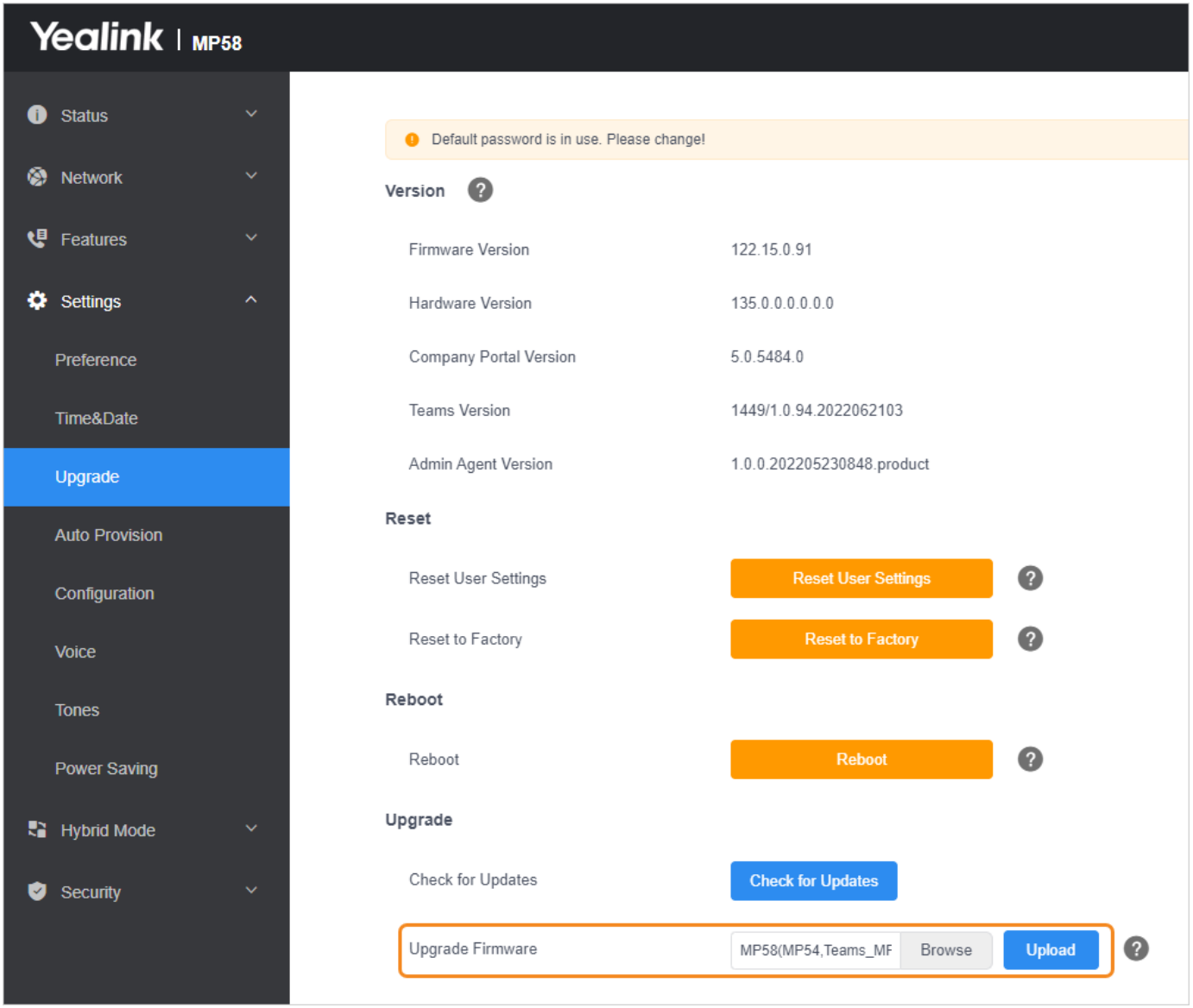
## Available Devices

- 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

# Perform Recovery Mode on Zoom Phones

## Overview

This guide shows how to use recovery mode to get your phone ready when it fails to start up.

There are four recovery modes:

1. Using HTTP server
2. Using TFTP server
3. Running backup system

Generally, when a Yealink IP phone is powered and connected to the network properly, it will start up successfully and get ready for you to use. In case, the IP phone is accidentally powered off when upgrading, the system data in the flash may be damaged and this makes the IP phone fail to start up. **Therefore, we strongly recommend that do not unplug or remove the power when the phone is updating firmware or configurations**.

## Getting Started

Before using recovery mode to get the IP phone ready, the following steps are required:

1. Preparing the Firmware and other Resource Files
2. Configuring the HTTP Server, Configuring the TFTP Server or Connecting the USB Flash Drive to the IP Phone

## Prepare the Firmware (rom file) and Other Resource Files

For the firmware and other resource files, you can ask your Yealink reseller.

Different phone models require different resource files to be used for recovery mode. Some just need the firmware, while others need extra files like "**.bin**" or "**.rfs**" in addition to the firmware.

The filename of the firmware used for recovery mode is strictly required. For example, to use recovery mode on MP58, you must rename the firmware file as MP58.rom.

For more details about the firmware name and required resource files, refer to the following table:

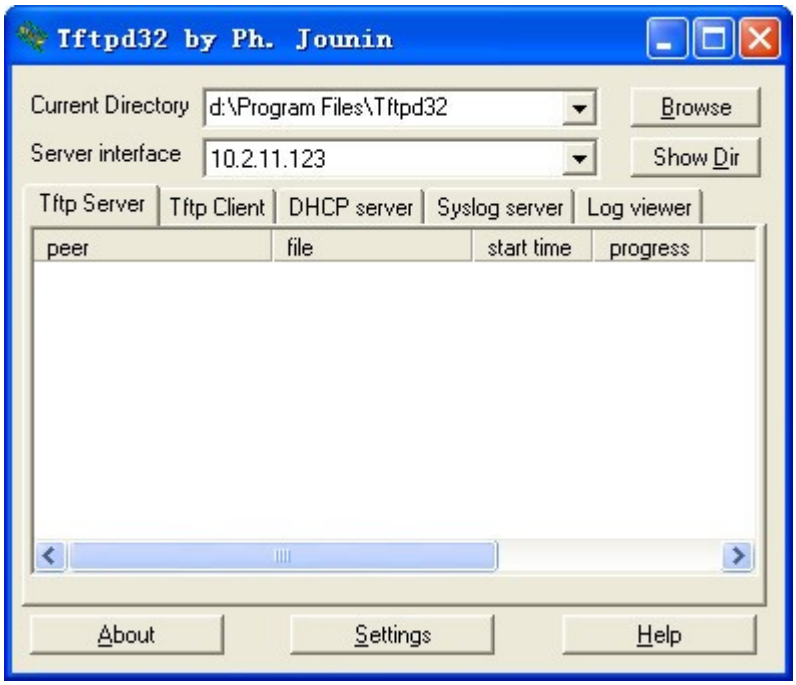
| Phone Model | The Resource Files Required |
|---|---|
| MP58 | MP58.rom, MP58.bin |
| MP56 | MP56.rom, MP56.bin |
| MP54 | MP54.rom, MP54.bin |
| VP59 | VP59.bin, VP59.rfs |

# Configure the TFTP Server

This section shows how to configure a TFTP server for the windows system using the tftpd32 application. You can download the tftpd32 application online: http://tftpd32.jounin.net/tftpd32_download.html. If there is a TFTP server installed on your local system, you can skip this section and go to the next.

**Procedure**

1. Create a TFTP root directory on the local system.
2. Place resource files to this root directory.
3. Double click the **tftpd32.exe** to start the application.
4. Click the Browse button to locate the TFTP root directory from the local system.
5. Select the local IP address from the **Server interface** drop-down menu.
6. Take a note of the server IP address (e.g., 10.2.11.123) which is used at the later stage.



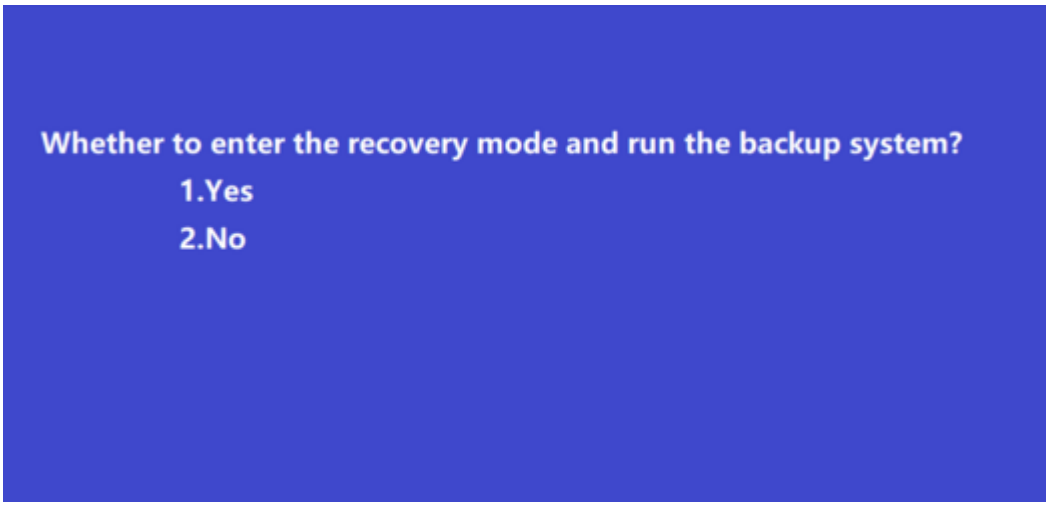

# Use Recovery Mode and Running Backup System on VP59

**TIP**

The firmware version of VP59 should be later than 91.15.0.68.

**Procedure**

1. Long press the **Speakerphone** key to trigger the recovery mode. Do not release the **Speakerphone** key until the recovery mode wizard appears on the phone LCD screen.




2. Press 1 to run the backup system.

# Use Recovery Mode on Yealink IP Phones (TFTP Server)

This section introduces how to perform recovery mode using the TFTP server on Yealink IP phones step by step.

**Procedure**

1. Long press (Speakerphone key) and reconnect the power adapter to trigger the recovery mode. the Speakerphone Key until the recovery mode wizard appears on the phone LCD screen.
2. For MP54/MP56/MP58, you need to press 1 on the recovery mode selection screen to use TFTP server.
2. Enter the desired values in the **IP Address**, **Netmask**, **IP Gateway** and **TFTP Server** fields respectively.
3. The IP phone must be configured in the same subnet as the TFTP server.
4. For MP56/MP58, you need to press press / / as up/down/left/right navigation key.
5. For MP54 IP phones, you need to press / / as up/down/left/right navigation key.
3. Press the OK key to complete the recovery mode.
4. The IP phone will download and upgrade the firmware from the TFTP server. After upgrading, the IP phone will initialize successfully and get ready for use.
5. The LCD screen prompts “Initializing…Please Wait” when upgrading successfully.
6. You need to press (for MP56/MP58/VP59 IP phones)/ (for MP54 IP phones) to complete the recovery mode since there is no OK key.
4. If the IP phone fails to upgrade, the LCD screen will indicate the failure. You need to check and make sure:
5. The connectivity between the TFTP server and the IP phone works well.

6. The resource files are correctly renamed and placed in the TFTP root directory.
7. Repeat the recovery mode procedures to try again.
8. The LCD screen prompts “Update Fail…Please reboot” when failing to upgrade:

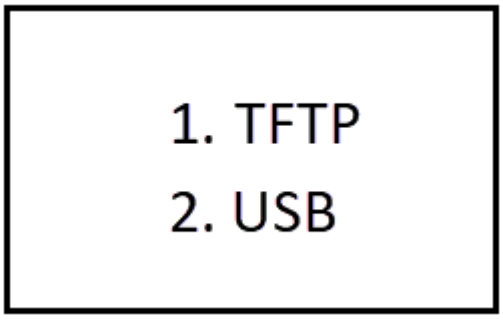
5. Press the OK key to verify the current firmware version after upgrading successfully.

# Use Recovery Mode on Yealink IP Phones (USB Flash Drive)

This section introduces how to perform recovery mode using USB flash drive on Yealink IP phones step by step.

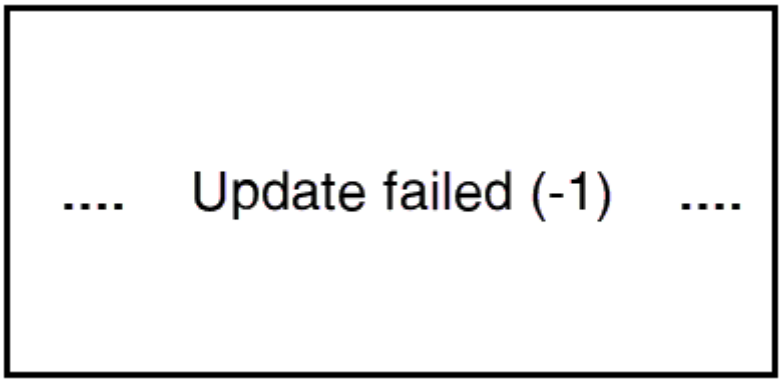
**Procedure**

1. Long press the Speakerphone Key and reconnect the power adapter to trigger the recovery mode. Do not release the Speakerphone Key until the recovery mode selection screen appears on the phone LCD screen.




2. Press 2 on the phone keypad to use USB flash drive.
3. The IP phone will read and upgrade the firmware from the USB flash drive.
4. After upgrading, the IP phone will initialize successfully and get ready for use. The LCD screen prompts “Initializing…Please wait” when upgrading successfully.

3. If the IP phone fails to upgrade, the LCD screen will indicate the failure. You need to check and make sure:
   - The file system of the USB flash drive should be FAT32.
   - The USB flash drive has been successfully connected to the IP phone.
   - The resource files are correctly renamed and placed on the USB flash drive.
   - Repeat the recovery mode procedures to try again.
   - The LCD screen prompts “Update failed (-1)” when failing to upgrade:




4. Press the OK key to verify the current firmware version after upgrading successfully.

# Take a Screencapture

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

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

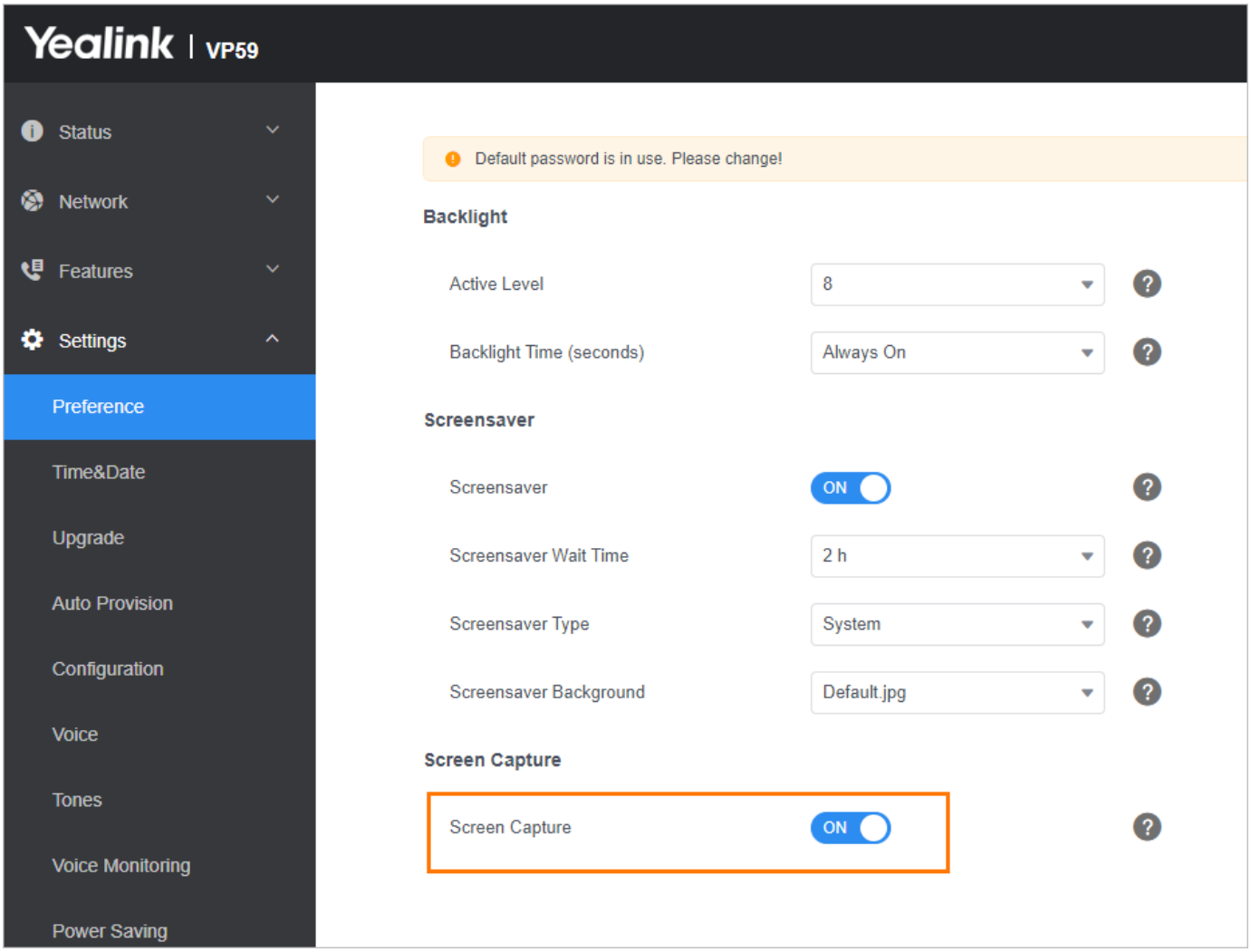
Before capturing the phone’ s current screen, ensure that the IP address of the computer is included in the trusted IP address for Action URI on the phone. When you capture the screen display, the IP phone may prompt you to enter the username and password of the administrator if the web browser does not remember the username and password for the web user interface login.

## Enable the Screen Capture Feature

### Via Web User Interface

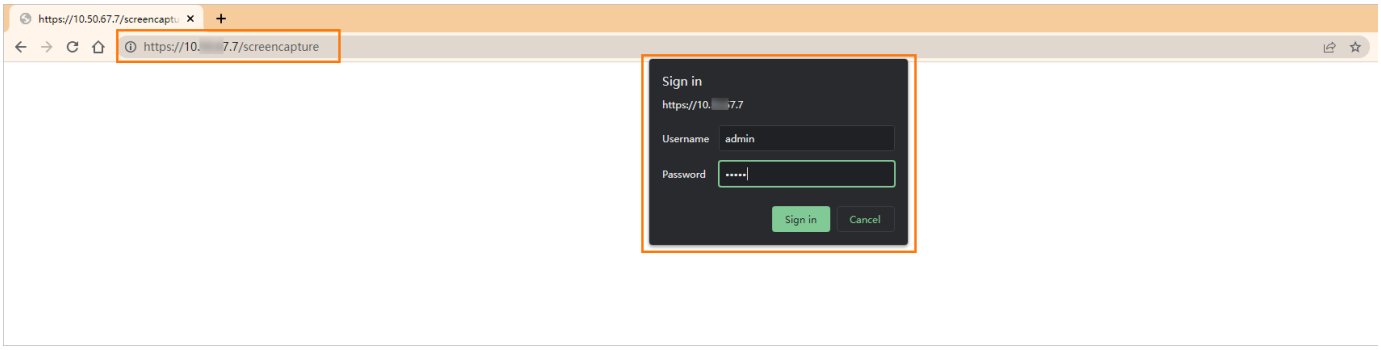
**Procedure**

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 Screencapture via Web User Interface

1. Enter request URI (for example, "http://10.2.20.252/screencapture") in the browser's address bar and press the Enter key on the keyboard.
2. If it is the first time you capture the phone’ s current screen using the computer, it will prompt you to enter the username and password of the administrator if the web browser does not remember the username 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.

# 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

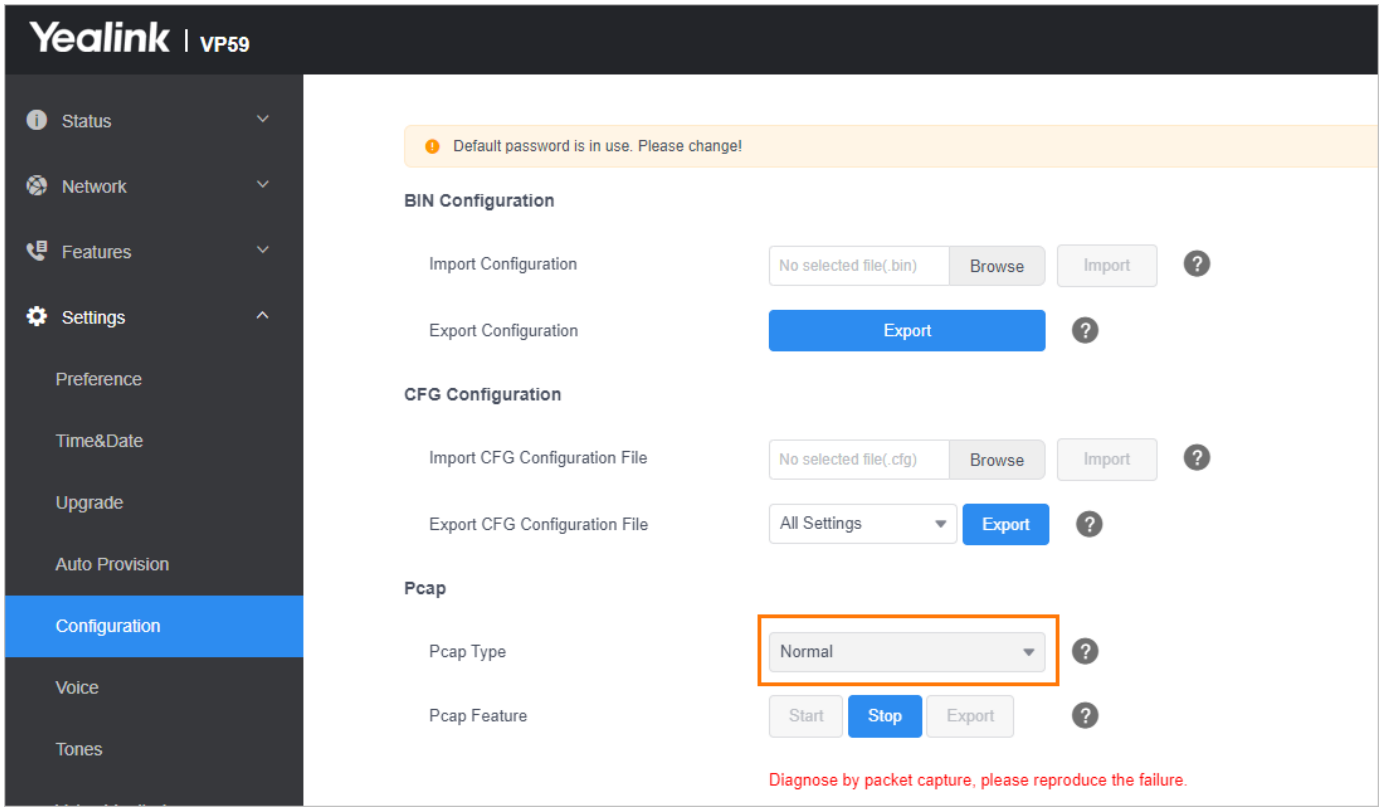
For Yealink Zoom devices, you can export the packets file to the local system and analyze it. Yealink Zoom devices support the following two modes for capturing the packets:

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

## Capture the Packets in Normal Way

**Procedure**

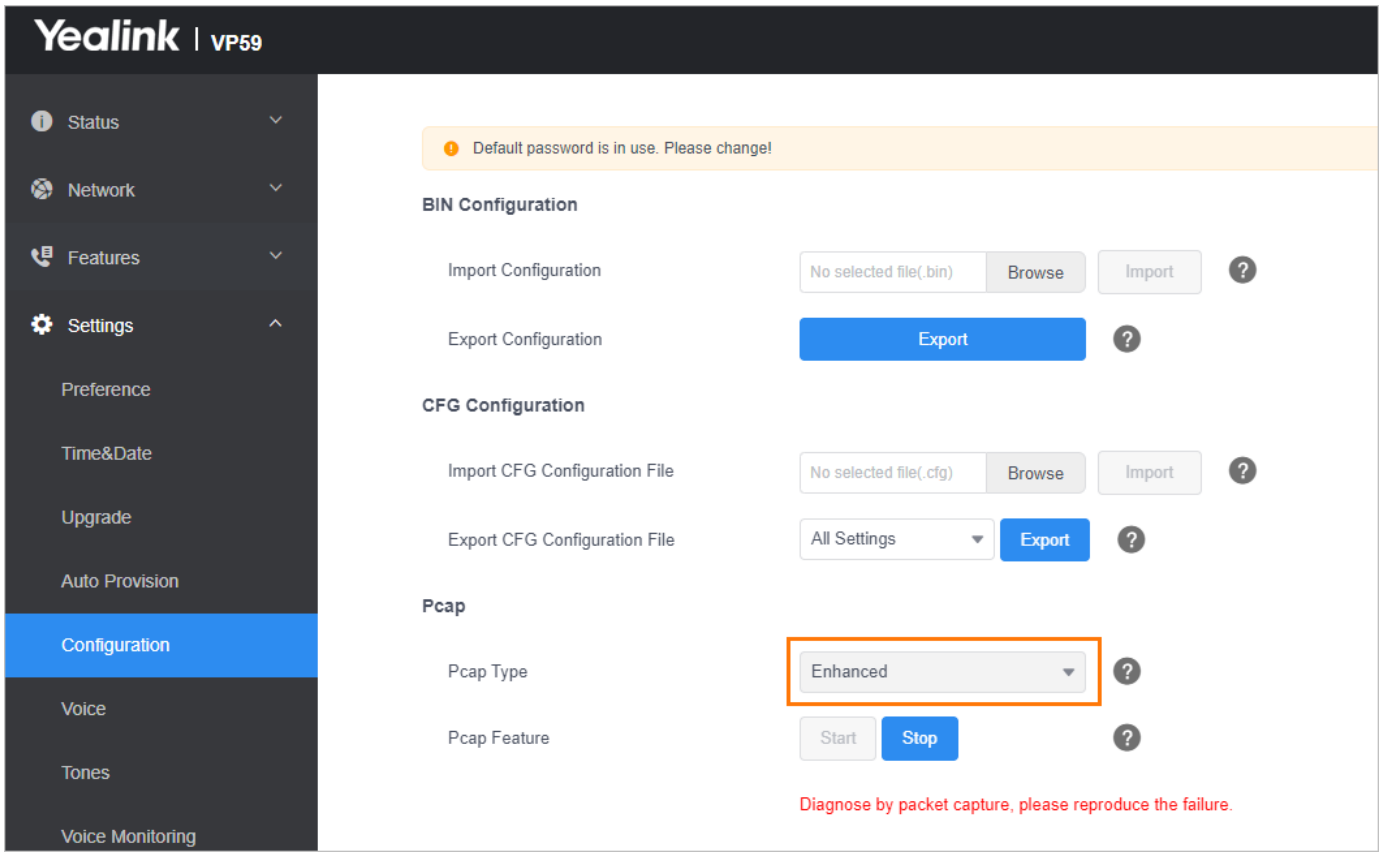
1. From the web user interface, go to **Settings** > **Configuration**.
2. Select **Normal** from the **Pcap Type** drop-down menu.
3. In the **Pcap Feature** field, click **Start** to start capturing signal traffic.
4. Reproduce the issue to get stack traces.
5. Click **Stop** in the **Pcap Feature**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



# 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 to CP960/CP965 phones.

# Span to PC Port Configuration

The following table lists the parameter you can use to configure span to PC port.

static.network.span_to_pc_port

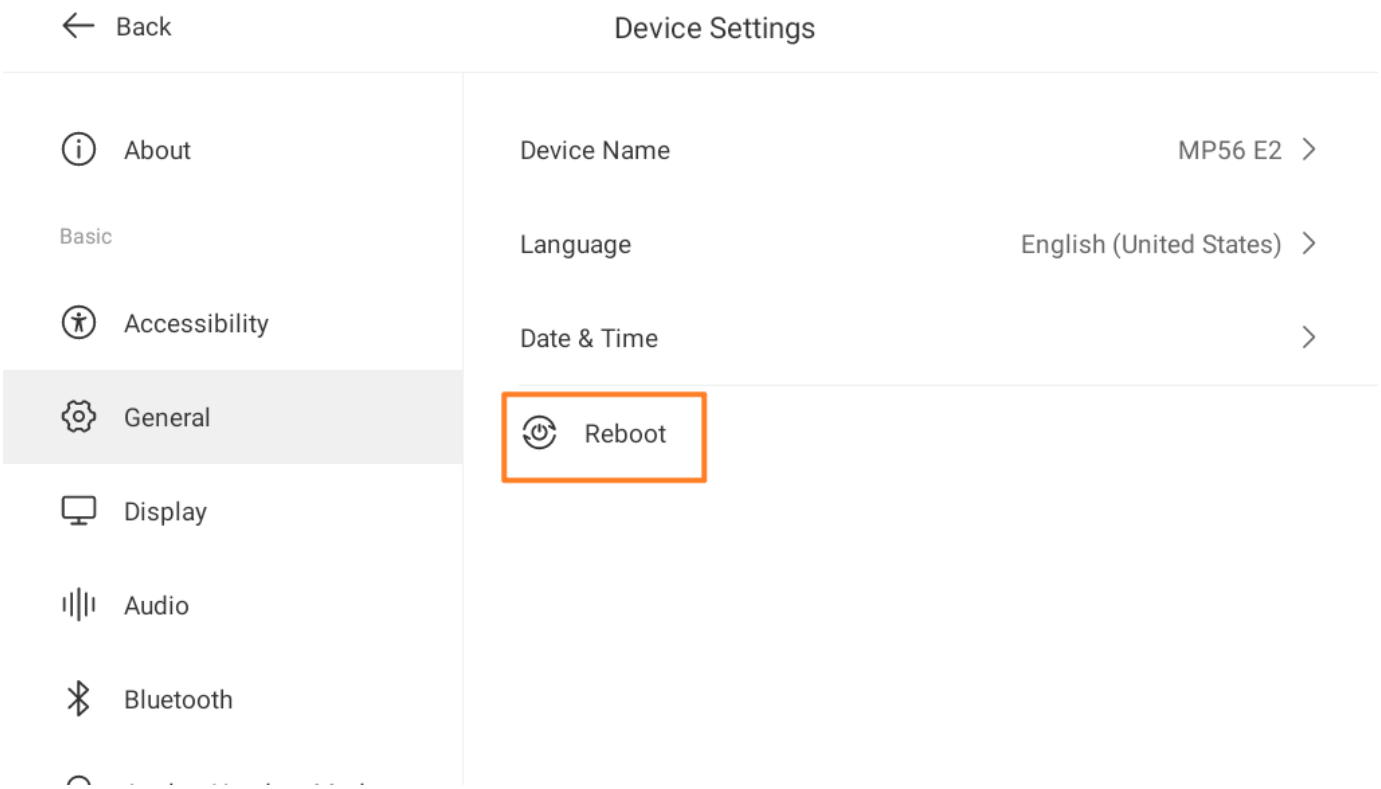
| Parameter | Permitted Values | Default | Description |
|---|---|---|---|
| static.network.span_to_pc_port[1] | **0**- Disabled<br>**1**-Enabled, all data packets from the Internet port can be received by PC port. | 0 | It enables or disables the device to span data packets received from the WAN port to the PC port.<br>NOTE<br>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 Zoom Phones

## Via Device User Interface

1. Go to **More** > **Settings** > **General** > **Reboot**.
2. It prompts if you are sure to reboot the device.

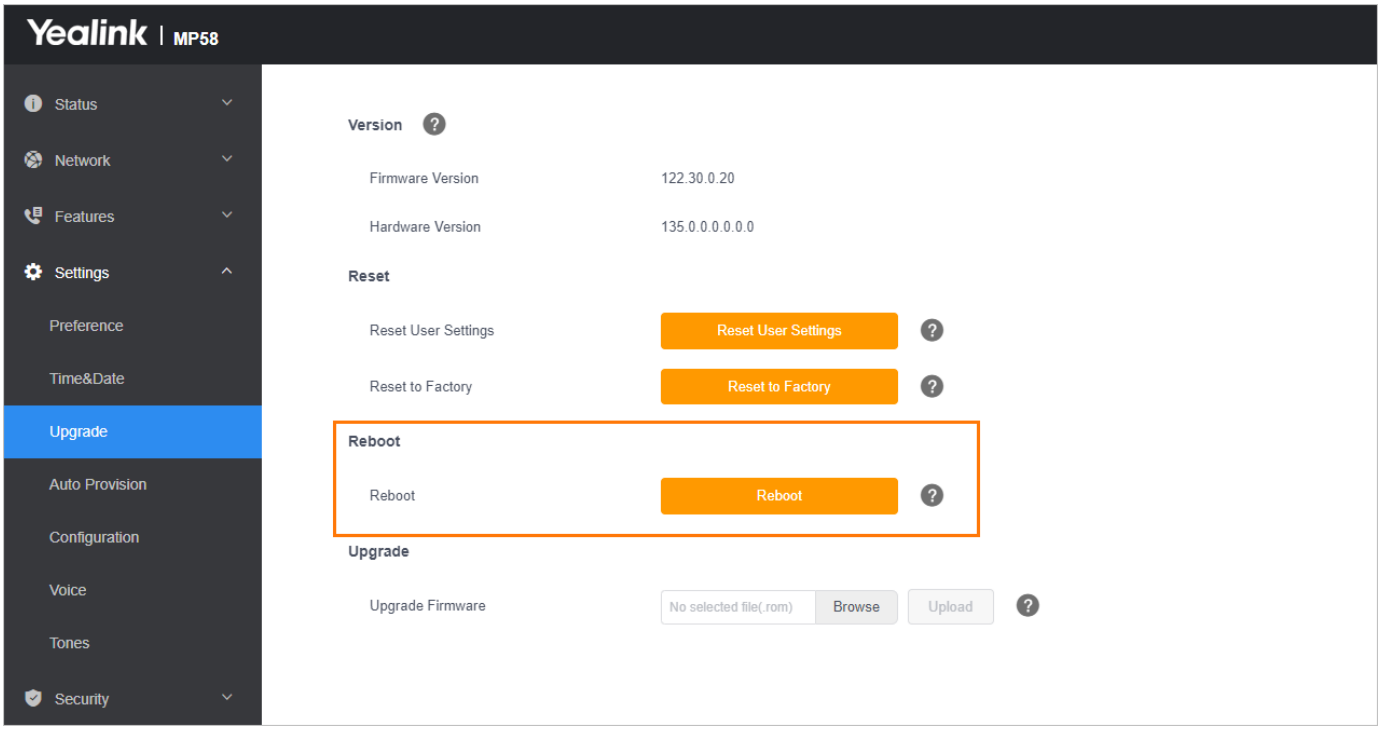



2. Select **OK**.

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

# Reset Zoom 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.

**NOTE**

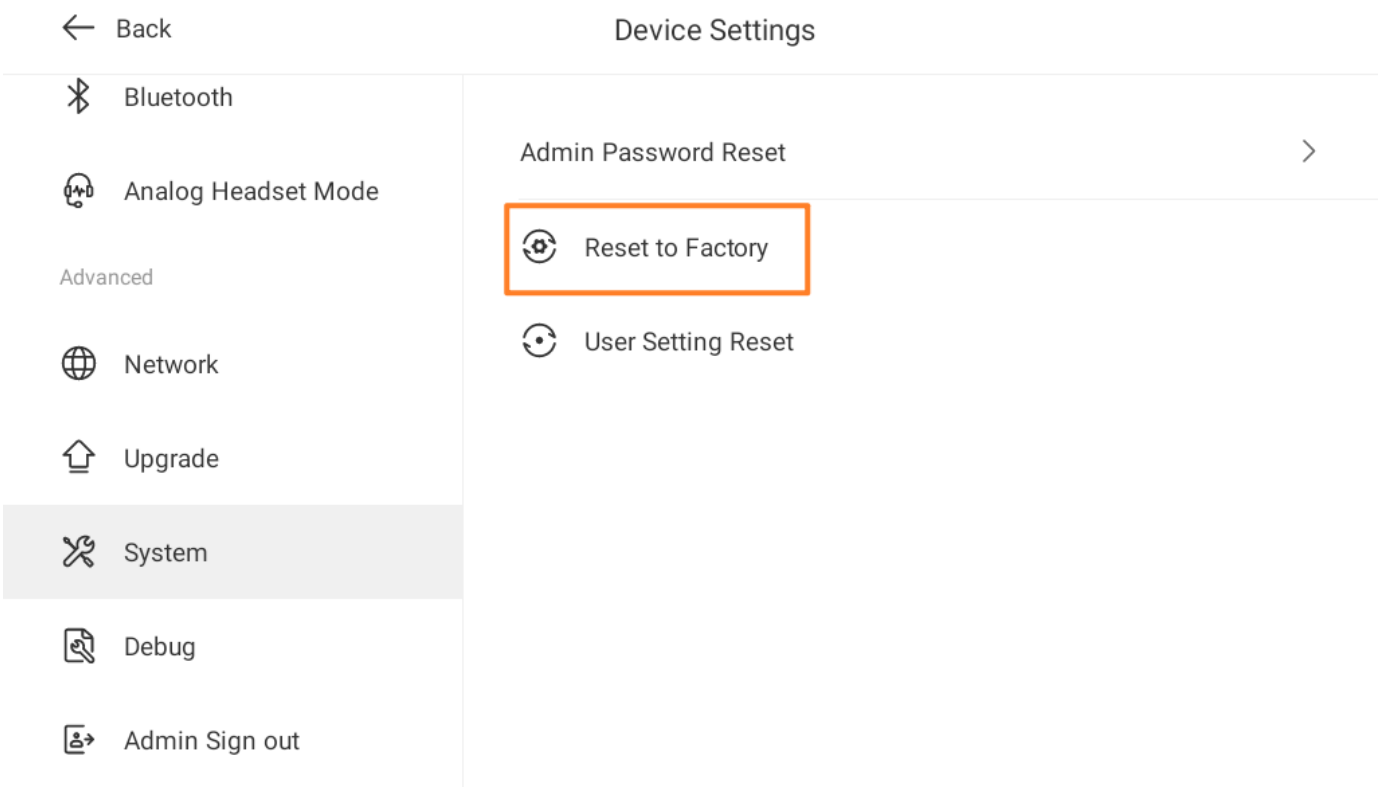
The license you apply from the Yealink license platform for version converting will not be cleared after the factory reset.

## Reset Zoom Phones to Factory

### Via Device User Interface

**Procedure**

1. Go to **More** > **Settings** > **General** > **System Settings** > **System** (default password: admin) > **Reset to Factory Settings**.
2. It prompts if you are sure to reset to factory default.




2. Tap **Reset**.

# 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.

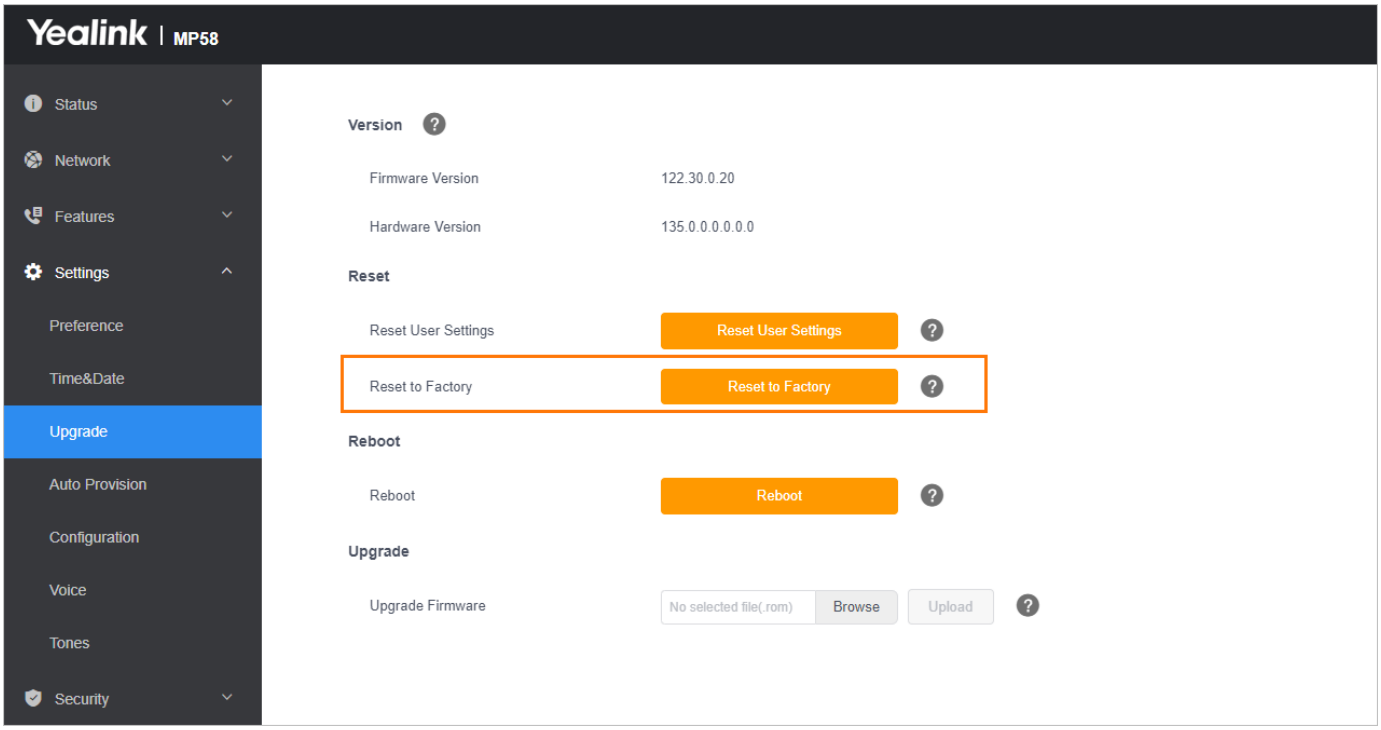
**Procedure**

1. Long press the pound key (#) and the star key (*) for about 6 seconds when the phone is idle.

# 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<br>**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 the web user interface. | 0 | It enables or disables the Custom Factory Configuration feature. |
| static.custom_factory_configuration.url | URL within 511 characters | Blank | It configures the access URL of the custom factory configuration files.<br>NOTE It works only if "static.features.c |

| | | | |
|---|---|---|---|
| | | | ustom_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**

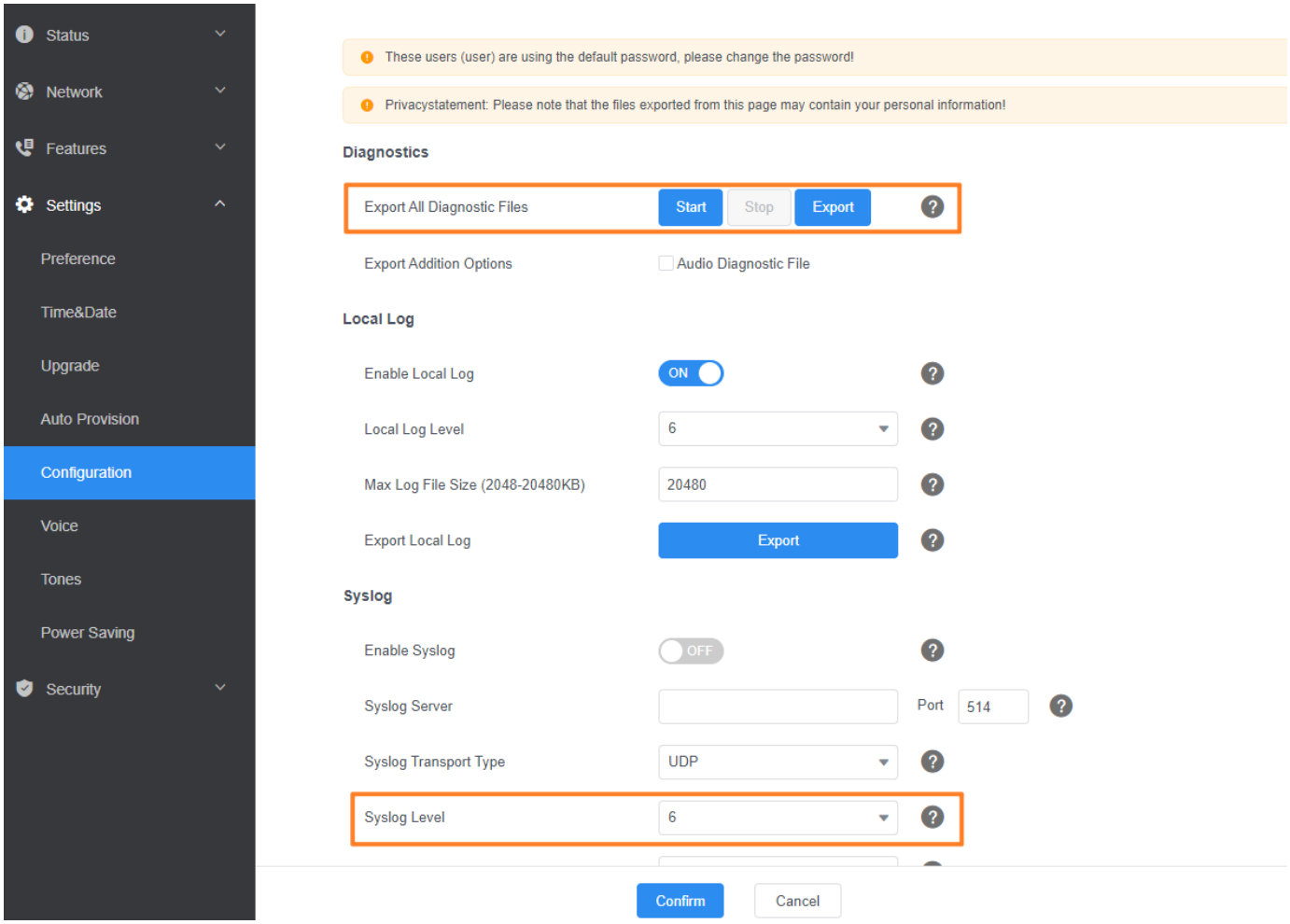
1. From the web user interface, click **Settings** > **Configuration** > **Factory Configuration**.
2. Click **Delete** from the **Delete Factory Configuration** field.
3. The web user interface prompts the message “Are you sure to delete user-defined factory configuration?”.
3. Click **OK** to delete 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 Zoom Phones

## Export All Diagnostic Files

**Procedure**

1. From the web user interface, go to **Settings** > **Configuration**.
2. Click **Start** in the **Export All Diagnostic Files** field to begin capturing signal traffic. The system log level will be automatically set to 6.




3. Reproduce the issue 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. Click **Stop** in the **Export All Diagnostic Files** field to stop the capture.
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.

> **TIP**
>
> 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

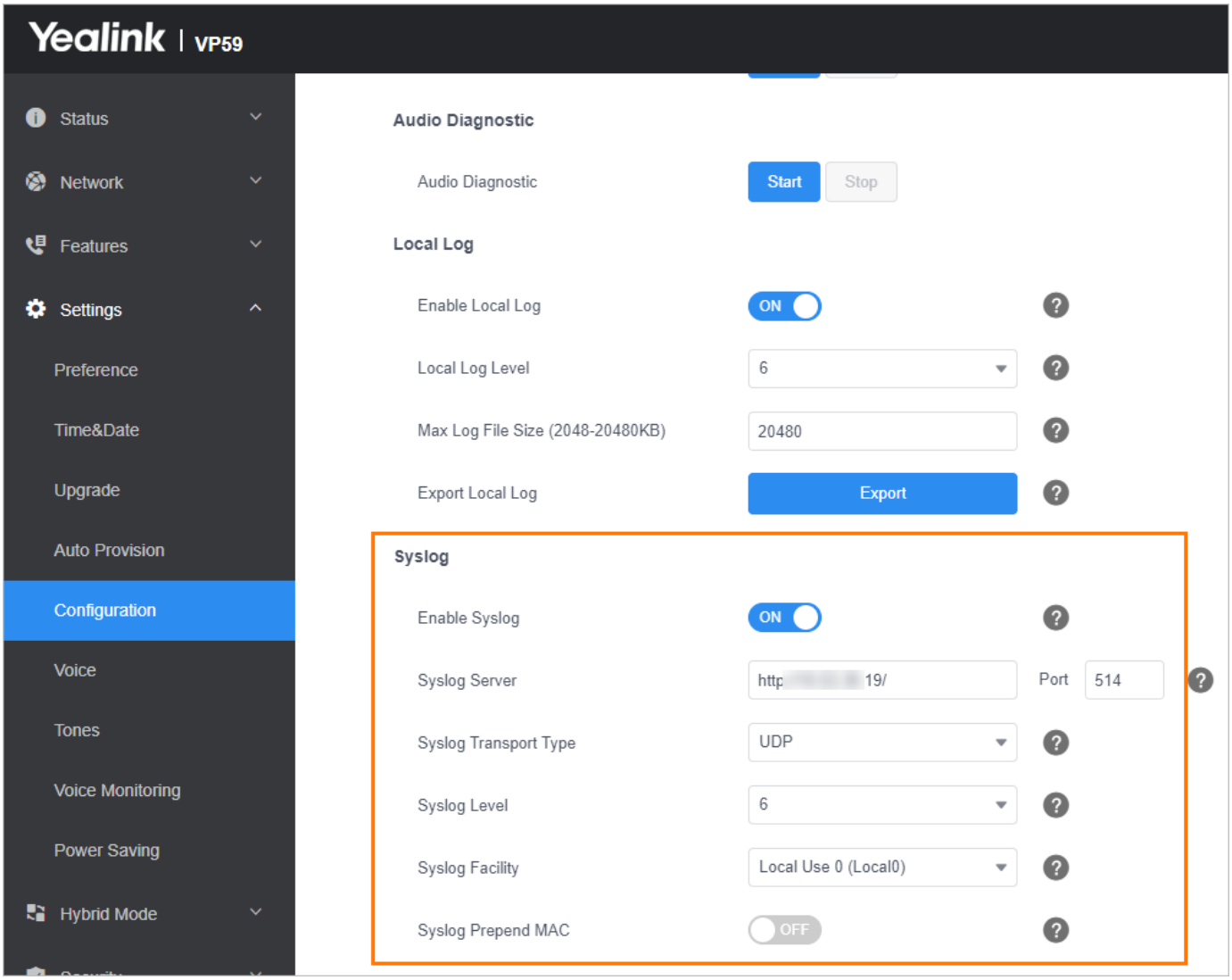
You can also configure the device to send syslog messages to a syslog server in real time.

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**.




# 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.enable | 0-Disabled 1-Enabled | 0 | It enables or disables the 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<br>1-Alert: action must be taken immediately<br>**2**-Critical: critical conditions<br>**3**-Critical: error conditions<br>**4**-Warning: warning conditions<br>**5**-Warning: normal but significant condition<br>**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<br>**1**-user-level messages<br>**2**-mail system<br>**3**-system daemons<br>**4**-security/authorization messages (note 1)<br>**5**-messages generated internally by syslogd<br>**6**-line printer subsystem<br>**7**-network news | 16 | It configures the facility that generates the log messages. For more information, refer to RFC 3164. |

| | | | |
|---|---|---|---|
| | subsystem<br>**8**-UUCP subsystem<br>**9**-clock daemon (note 2)<br>**10**-security/authorization messages (note 1)<br>**11**-FTP daemon<br>**12**-NTP subsystem<br>**13**-log audit (note 1)<br>**14**-log alert (note 1)<br>**15**-clock daemon (note 2)<br>**16**-local use 0 (local0)<br>**17**-local use 1 (local1)<br>**18**-local use 2 (local2)<br>**19**-local use 3 (local3)<br>**20**-local use 4 (local4)<br>**21**-local use 5 (local5)<br>**22**-local use 6 (local6)<br>**23**-local use 7 (local7) | | |
| static.syslog.prepend_mac_address.enable | **0**-Disabled<br>**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 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http2.Http2Connection.newStream(Http2Connection.java:239)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http2.Http2Connection.newStream(Http2Connection.java:222)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http2.Http2Codec.writeRequestHeaders(Http2Codec.java:111)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http.CallServerInterceptor.intercept(CallServerInterceptor.java:50)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:121)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at com.microsoft.skype.teams.data.proxy.GlobalRequestInterceptor.intercept(GlobalRequestInterceptor.java:291)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.connection.ConnectInterceptor.intercept(ConnectInterceptor.java:45)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:121)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.cache.CacheInterceptor.intercept(CacheInterceptor.java:93)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:121)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http.BridgeInterceptor.intercept(BridgeInterceptor.java:93)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http.RetryAndFollowUpInterceptor.intercept(RetryAndFollowUpInterceptor.java:126)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.internal.http.RealInterceptorChain.proceed(RealInterceptorChain.java:121)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.RealCall.getResponseWithInterceptorChain(RealCall.java:200)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at okhttp3.RealCall.execute(RealCall.java:77)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at retrofit2.OkHttpCall.execute(OkHttpCall.java:180)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at retrofit2.ExecutorCallAdapterFactory$ExecutorCallbackCall.execute(ExecutorCallAdapterFactory.java:91)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at com.microsoft.skype.teams.data.HttpCallExecutor$RetrofitRequestExecutor.execute(HttpCallExecutor.java:459)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at com.microsoft.skype.teams.data.HttpCallExecutor.executeInternal(HttpCallExecutor.java:216)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at com.microsoft.skype.teams.data.HttpCallExecutor.execute(HttpCallExecutor.java:147)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at com.microsoft.skype.teams.data.HttpCallExecutor.execute(HttpCallExecutor.java:129)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at com.microsoft.skype.teams.data.HttpCallExecutor.execute(HttpCallExecutor.java:118)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at com.microsoft.skype.teams.services.files.PresenceServiceAppData.setUnifiedPresence(PresenceServiceAppData.java:299)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at com.microsoft.skype.teams.data.AppData.setMyStatus(AppData.java:2240)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at com.microsoft.skype.teams.calling.call.CallPresence$1.handleMessage(CallPresence.java:66)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at android.os.Handler.dispatchMessage(Handler.java:98)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at android.os.Looper.loop(Looper.java:135)
Nov 22 00:09:35 aplc[590]: ANDR<3+error > 1155  1524 E SetUnifiedPresence:       at android.os.HandlerThread.run(HandlerThread.java:61)
```

# Configure Local Logs

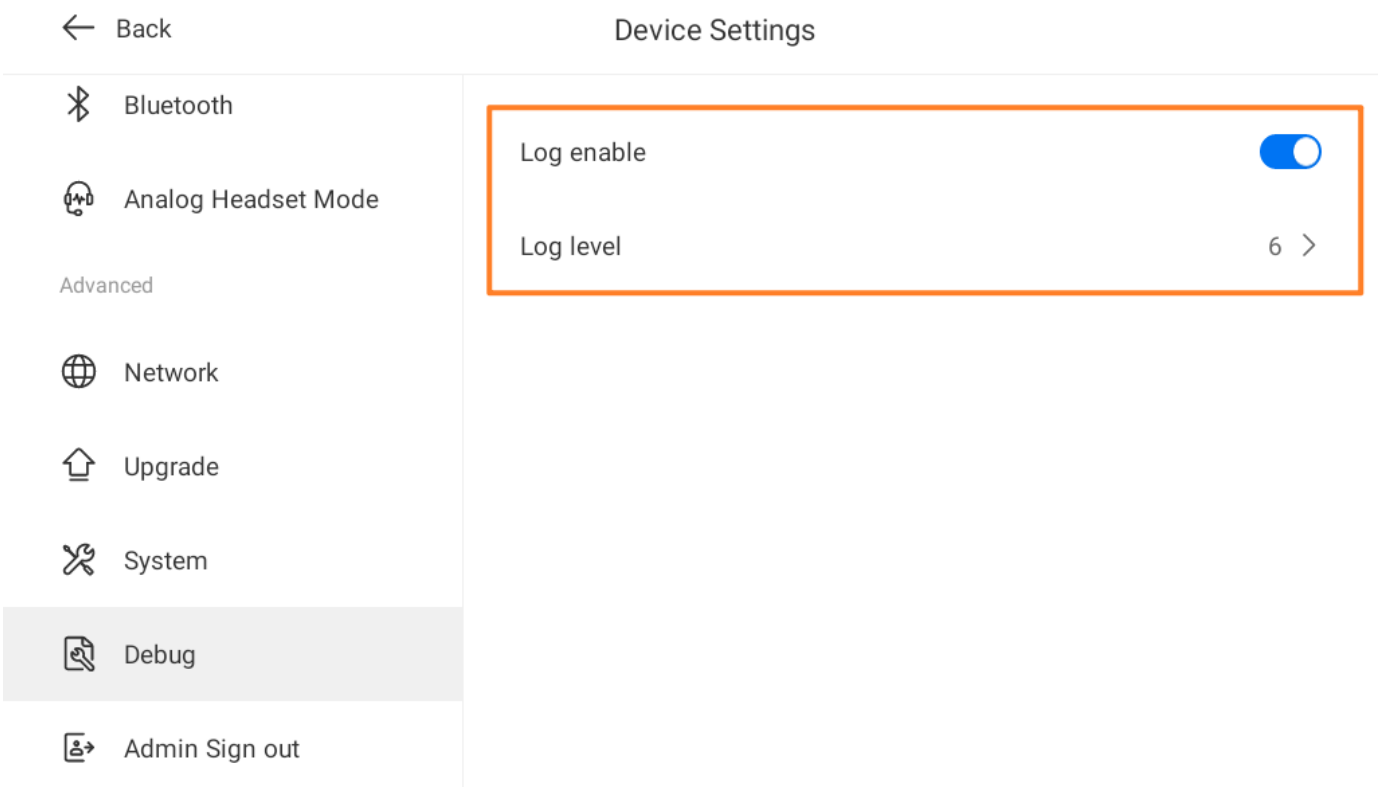
Yealink Zoom devices can log events into two different log files: boot log and system log. You can choose to generate the log files locally or send to the Syslog server in real-time, and use these log files to generate informational, analytic, and troubleshooting devices.

## 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

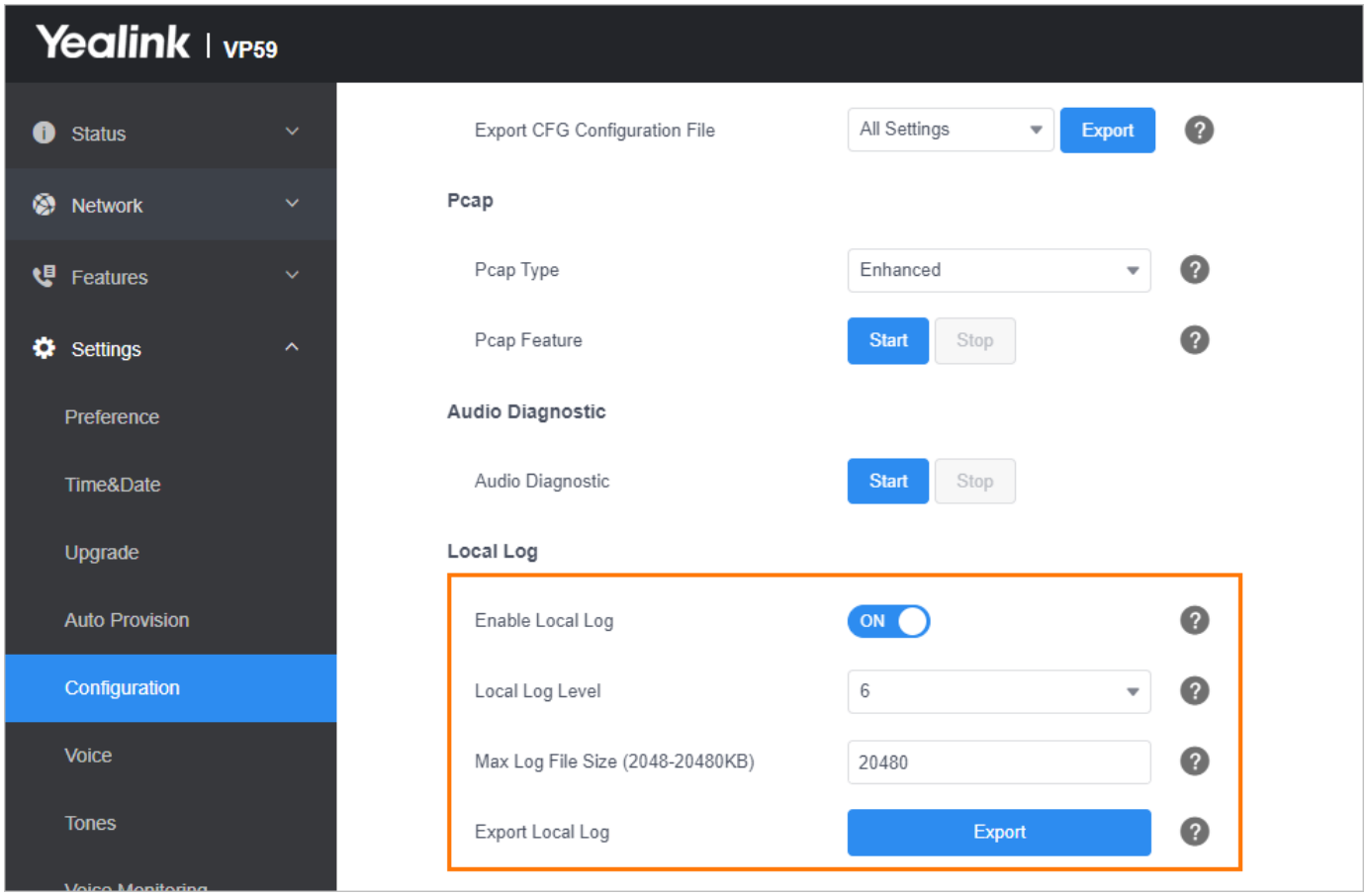
1. Go to **More** > **Settings** > **General** > **System Settings** > **Debug** (default password: admin).
2. Enable **Log** and set the log level as 6.




### 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.




# 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 log to the log files (<MAC>-boot.log and <MAC>-sys.log) locally. The log | 1 | It enables or disables the device to record log locally.<br>NOTE<br>We recommend you not to disable this feature. |

| | | | |
|---|---|---|---|
| | files recorded before are still kept on the device. **1**-Enabled, the device will continue to record log to the log files (<M[redacted]AC> | | |

| | | | |
|---|---|---|---|
| | [redacted] and [redacted] locally. You can upload the local log files to the provisioning server or a specific ser | | |

| | | | |
|---|---|---|---|
| | ver or exp ort the m to the loca l sys tem . | | |
| sta tic .lo cal _lo g.l eve l | **0**- sys tem is unu sab le **1**- act ion mus t be tak en imm edi ate ly **2**- crit ical con | 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. |

| | | | |
|---|---|---|---|
| | dition **3**-error conditions **4**-warning conditions **5**-normal but significant condition **6**-informational | | |
| static | Integer | 2048 | 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. |

| | | | |
|---|---|---|---|
| .local_log.max_file_size | from 2048 to 20480 | 0 | When this size is about to be exceeded, If the local log files are configured to be uploaded to the server by the parameter static.auto_provision.local_log.backup.enable, the device will clear all the local log files on the device once successfully backing up.<br>If static.auto_provision.local_log.backup.enable is set to 0 (Disabled), the device will erase half of the logs from the oldest log information on the device. |
| static.auto_provision.local_log.backup.enable | **0**-Disabled **1**-Enabled, the device will upload the local log files to the provisioning server | 0 | It enables or disables the device to upload the local log files (<MAC>-boot.log and <MAC>-sys.log) to the provisioning server or a specific server.<br>NOTE<br>The upload path is configured by the parameter "static.auto_provision.local_log.backup.path" . |

| | | | |
|---|---|---|---|
| | 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 [redacted]; It's tim | | |

| | | | |
|---|---|---|---|
| | e to upl oad<br><br>loca l log file s acc ord ing to the upl oad<br><br>per iod con fig ure d by the par ame ter [redacted] | | |

| | | | |
|---|---|---|---|
| | [redacted] | | |
| static.auto_provision.local_log.backup.upload_period | Integer from 30 to 86400 | 30 | It configures the period (in seconds) of the local log files ([redacted] and [redacted]) uploads to the provisioning server or a specific server.<br>NOTE<br>It works only if "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled). |
| static.auto_provision | URL within 1024 cha | Blank | It configures the upload path of the local log files ([redacted] and [redacted]). 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 |

| | | | |
|---|---|---|---|
| .local_log.backup.path | characters | | protocol with auto provisioning for uploading files.<br>Example: static.auto_provision.local_log.backup.path = tftp://10.3.6.133/upload/.<br>NOTE<br>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_l | **0**-Append Delete, the server will | 0 | It configures the behavior when local log files (<MAC>-boot.log and <MAC>-sys.log) on the provisioning server or a specific server reach the maximum file size. |

| | | | |
|---|---|---|---|
| og.backup.append.limit_mode | delete the old log, and the device will continue uploading log.<br>**1**-Append<br>Stop, the device will stop uploading log. | | |
| static | Integer | 1024 | 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 |

| | | | |
|---|---|---|---|
| .auto_provision.local_log.backup.append.max_file_size | r from 200 to 65535 | | server. |
| static.auto_provision.local_log.backup.bootlog.upl | Integer from 1 to 86400 | 120 | 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. |

| | | | |
|---|---|---|---|
| ad_wait_time | | | |

# 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):

```
<46>Thu Jan  1 08:00:09 syslogd started: BusyBox v1.10.3
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > cfg log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > ANY =3
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Version  :1.2.1.7 for release
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Built-at :May 10 2018,21:55:14
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > TRS log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > Version  :1.0.0.6 for release
<128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > Built-at :Apr 20 2018,21:57:26
<128>Jan  1 08:00:11 cfg [316]: ANY <0+emerg > ANY =6
<133>Jan  1 08:00:11 cfg [316]: CFG <5+notice> cfgserver init done
<46>Thu Jan  1 08:00:12 syslogd started: BusyBox v1.10.3
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > Version  :8.0.1.3 for release
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > Built-at :Jul 30 2018,14:38:14
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
<132>Jan  1 08:00:12 sys [532]: SRV <4+warnin> wifi switch mode 1
<134>Jan  1 08:00:12 sys [532]: SRV <6+info  > running in nomal mode, mode 0
<134>Jan  1 08:00:12 sys [532]: SRV <6+info  > Set Init SystemTime: 2018-11-23
<134>Nov 23 00:00:00 sys [532]: SRV <6+info  > emac get: wan speed 0000003f, lan speed 0000003f
<134>Nov 23 00:00:00 sys [532]: SRV <6+info  > wan_support_speed 0000005f, lan_support_speed 0000005f
```

The boot.log file reports the logs with all severity levels. The following figure shows a portion of a sys

log file:

```
<46>Thu Jan  1 08:00:09 syslogd started: BusyBox v1.10.3
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > cfg log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > ANY =3
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Version  :1.2.1.7 for release
<128>Jan  1 08:00:10 cfg [316]: ANY <0+emerg > Built-at :May 10 2018,21:55:14
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<131>Jan  1 08:00:11 cfg [316]: CFG <3+error > invalid key  without '.'
<128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > TRS log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > Version  :1.0.0.6 for release
<128>Jan  1 08:00:11 TRS [316]: ANY <0+emerg > Built-at :Apr 20 2018,21:57:26
<128>Jan  1 08:00:11 cfg [316]: ANY <0+emerg > ANY =6
<133>Jan  1 08:00:11 cfg [316]: CFG <5+notice> cfgserver init done
<46>Thu Jan  1 08:00:12 syslogd started: BusyBox v1.10.3
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > Version  :8.0.1.3 for release
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > Built-at :Jul 30 2018,14:38:14
<128>Jan  1 08:00:12 sys [532]: ANY <0+emerg > ANY =6
<132>Jan  1 08:00:12 sys [532]: SRV <4+warnin> wifi switch mode 1
<134>Jan  1 08:00:12 sys [532]: SRV <6+info  > running in nomal mode, mode 0
<134>Jan  1 08:00:12 sys [532]: SRV <6+info  > Set Init SystemTime: 2018-11-23
<134>Nov 23 00:00:00 sys [532]: SRV <6+info  > emac get: wan speed 0000003f, lan speed 0000003f
<134>Nov 23 00:00:00 sys [532]: SRV <6+info  > wan_support_speed 0000005f, lan_support_speed 0000005f
<134>Nov 23 00:00:00 sys [532]: SRV <6+info  > set client
```

The <MAC>-sys.log file reports the logs with a configured severity level and the higher. For example, if you have 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 to your phone, you can use the following troubleshooting methods to solve the problem.
  - Reboot Devices
  - Update to the Latest Zoom 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)
  - Capture Packets
- If you need to perform recovery mode to recover the device, please see Perform Recovery Mode.