Yealink

AX83H Wi-Fi IP Phone
Administrator Guide

Oct. 2024

Network Configurations

Wi-Fi

Wi-Fi

You can configure the phones to operate in IPv4, IPv6, or dual-stack (IPv4/IPv6) mode and configure IPv4 or IPv6 wireless network settings manually.

Wi-Fi Configuration

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

Configuration parameter

```
static.wifi.function.enable
static.network.wifi.roaming_threshold
static.network.redundancy.mode
static.network.redundancy.failback.timeout
static.wifi.enable
static.wifi.X.ssid
static.wifi.X.priority
static.wifi.X.security_mode
static.wifi.X.password
static.wifi.X.eap_type
static.wifi.X.eap_user_name
static.wifi.X.802_1x.anonymous_identity
static.wifi.X.eap_password
static.wifi.show_scan_prompt
```

Parameter	Description	Permitted Values	Default
static.wifi.function.enable[1]	It enables or disables the Wi-Fi feature.	0-Disabled 1-Enabled	1
static.network.redundancy.mode	It configures the network connection mode to be used preferentially.	0-If Wi-Fi mode is activated, the wired network is unavailable; Wi-Fi mode must be deactivated if you want to use the wired network. 1-Use wireless network preferentially. 2-Use wired network preferentially.	2

static.network.wifi.roaming_threshold[1]	When the Wi-Fi signal strength of the device drops below this configured value, the device will scan for a hotpot above the threshold value and connect to it.	Integer from -100 to -30	-70
static.network.redundancy.failback.timeout	It configures the time to wait (minutes) for the phone to switch to the preferentially used network. **ⓘ NOTE** It works only if "static.network.redundancy.mode" is not set to 0 and there are multiple networks on the phone at the same time.	Integer from 0 to 1440 0-The phone will not switch as long as the current network is available. 1 to 1440–The phone will keep using the current network for the specified time after the preferentially used network becomes available. If the preferentially used network is still available after the specified time, the phone performs a network switch while the phone is not in use.	55
static.wifi.enable	It activates or deactivates the Wi-Fi mode. **ⓘ NOTE** It works only if "static.wifi.function.enable" is set to 1 (Enabled).	0-Disabled 1-Enabled	0
static.wifi.X.ssid[2]	It configures the SSID of a specific wireless network. SSID is a unique identifier for accessing wireless access points. **ⓘ NOTE** It works only if "static.wifi.enable" is set to 1 (Enabled).	ASCII code from 1 to 31 in length	Blank

static.wifi.X.priority[2]	It configures the priority for a specific wireless network. 5 is the highest priority, 1 is the lowest priority. **ⓘ NOTE** It works only if "static.wifi.enable" is set to 1 (Enabled).	Integer from 1 to 5	1
static.wifi.X.security_mode[2]	It configures the security mode of a specific wireless network. **ⓘ NOTE** It works only if "static.wifi.enable" is set to 1 (Enabled). If it is set to 802.1x EAP, the CA certificate can be uploaded by the parameter "static.network.802_1x.root_cert_url", the user certificate can be uploaded by the parameter "static.network.802_1x.client_cert_url".	NONE, WEP, WPA/WPA2 PSK, WPA3-Personal, 802.1x EAP	NONE
static.wifi.X.password[2]	It configures the password of a specific wireless network. **ⓘ NOTE** It works only if "static.wifi.enable" is set to 1 (Enabled).	String within 64 characters	Blank
static.wifi.X.eap_type[2]	It configures the EAP authentication mode of a specific wireless network. **ⓘ NOTE** It works only if "static.wifi.enable" is set to 1 (Enabled) and "static.wifi.X.security_mode" is set to 802.1x EAP.	Auto, PEAP, TLS, TTLS or PWD	Auto

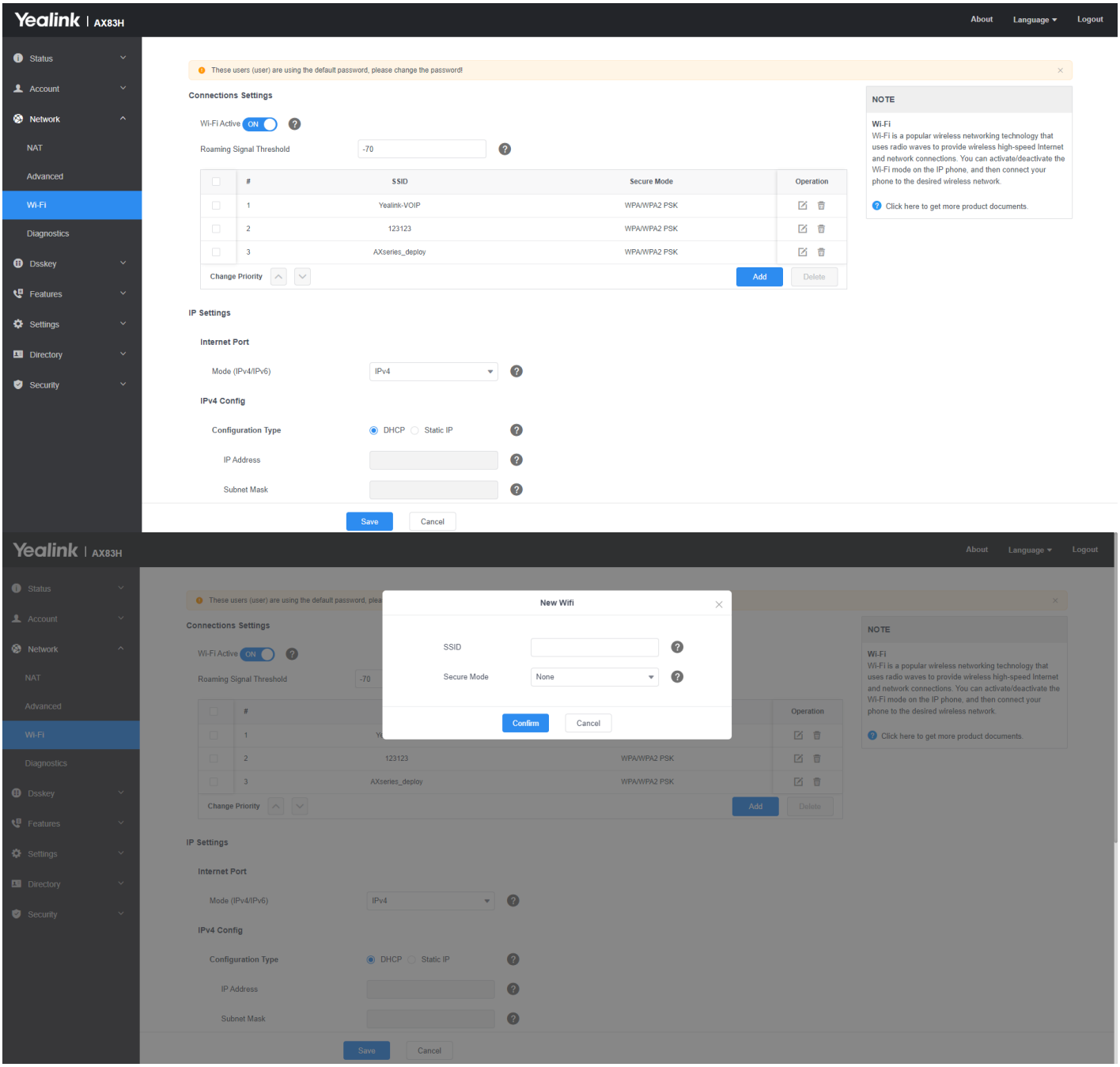
static.wifi.X.eap_user_name[2]	It configures the EAP authentication username of a specific wireless network. **NOTE** It works only if "static.wifi.enable" is set to 1 (Enabled) and "static.wifi.X.security_mode" is set to 802.1x EAP.	ASCII code from 1 to 32 in length	Blank
static.wifi.X.802_1x.anonymous_identity[2]	It configures the anonymous identity (user name) for Wi-Fi 802.1X authentication. **NOTE** It works only if "static.wifi.enable" is set to 1 (Enabled) and "static.wifi.X.security_mode" is set to 802.1x EAP.	String within 255 characters	Blank
static.wifi.X.eap_password[2]	It configures the EAP authentication password of a specific wireless network. **NOTE** It works only if "static.wifi.enable" is set to 1 (Enabled) and "static.wifi.X.security_mode" is set to 802.1x EAP.	String within 64 characters	Blank
static.wifi.show_scan_prompt	It enables or disables the phone to prompt you whether to scan Wi-Fi after connecting Wi-Fi USB dongle to the IP phone.	0-Disabled, the phone will enable the Wi-Fi feature and try to connect to the known wireless network (according to the priority) automatically. But if the phone fails to connect to any known wireless network, the phone will still display the Wi-Fi scanning prompt when connecting to the phone. 1-Enabled	1

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

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

Set via the Web User Interface

On the web user interface, go to: **Network** > **Wi-Fi** > **Wi-Fi Active**



Wireless Network IP Addressing Mode Configuration

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

Configuration parameter

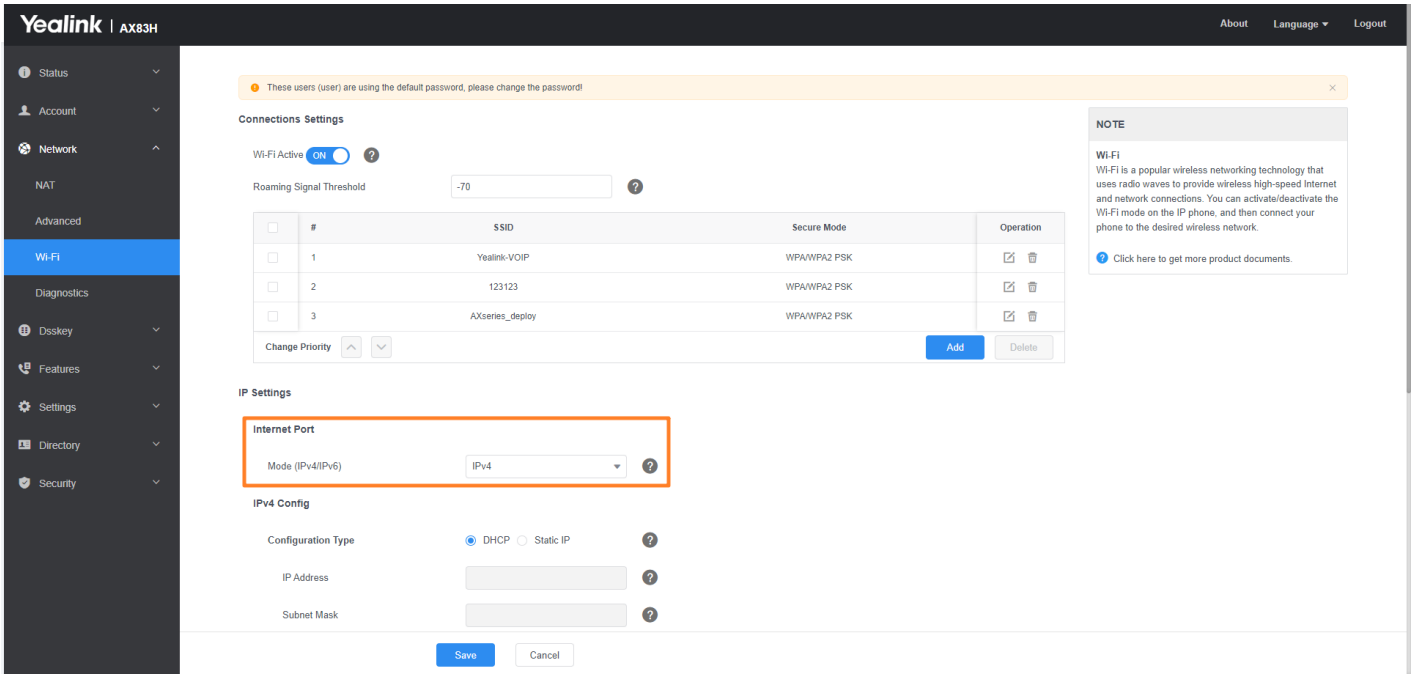
static.network.wifi.ip_address_mode
static.network.wifi.preference

Parameter	Description	Permitted Values	Default

static.network.wifi.ip_address_mode	It configures the IP addressing mode for the wireless network.	0-IPv4 1-IPv6 2-IPv4 & IPv6	0
static.network.wifi.preference	It specifies IPv4 or IPv6 as the preferred wireless network in a Dual-Stack mode. **ⓘ NOTE** It works only if "static.network.wifi.ip_address_mode" is set to 2 (IPv4 & IPv6).	0-IPv6 1-IPv4	0

Set via the Web User Interface

On the web user interface, go to: **Network** > **Wi-Fi** > **IP Settings** > **Internet port** > **Mode(IPv4/IPv6)**



IPv4 Wireless Network Configuration

The following table lists the parameters to configure the IPv4 wireless network.

Configuration parameter

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

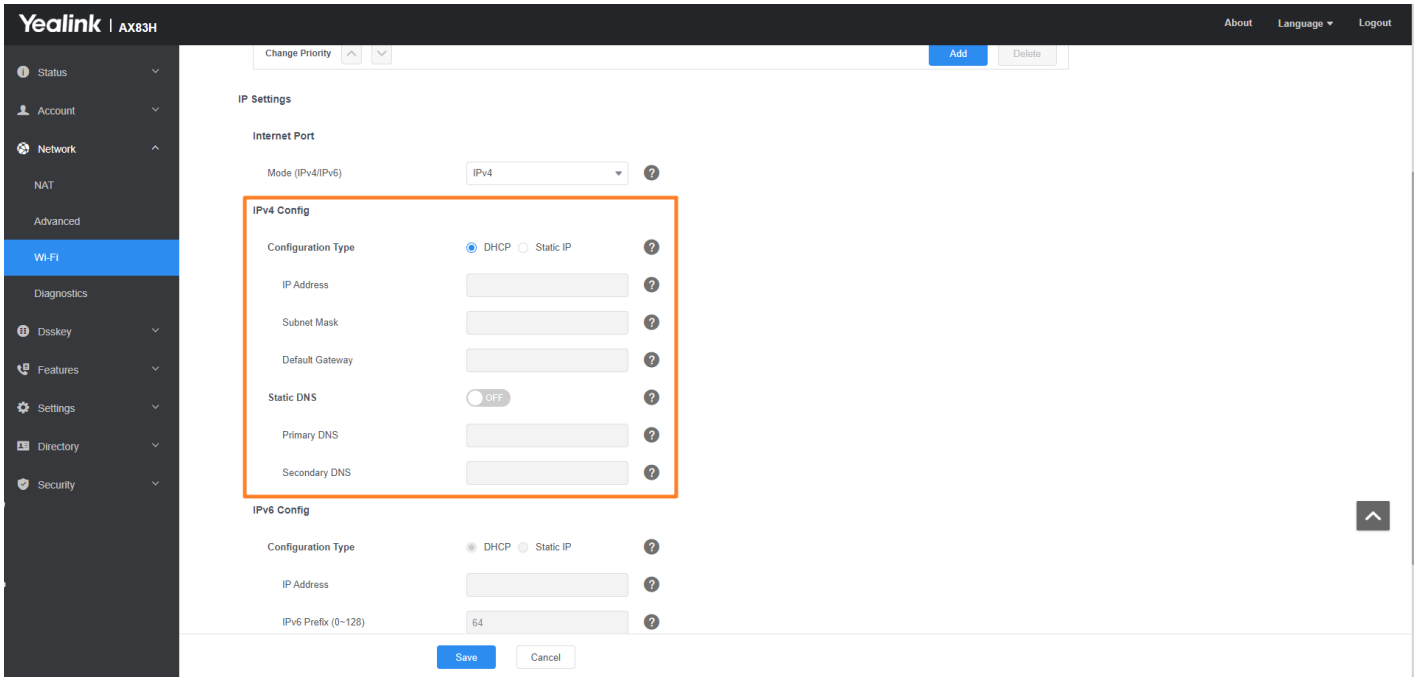
Parameter	Description	Permitted Values	Default

static.network.wifi.internet_port.type	It configures the Internet port type for the IPv4 wireless network. **NOTE** It works only if "static.network.wifi.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6).	0-DHCP 2-Static IP	0
static.network.wifi.internet_port.ip	It configures the IPv4 address for the wireless network. **NOTE** It works only if "static.network.wifi.internet_port.type" is set to 2 (Static IP).	IPv4 Address	Blank
static.network.wifi.internet_port.mask	It configures the IPv4 subnet mask for the wireless network. **NOTE** It works only if "static.network.wifi.internet_port.type" is set to 2 (Static IP).	IPv4 Address	Blank
static.network.wifi.internet_port.gateway	It configures the IPv4 default gateway for the wireless network. **NOTE** It works only if "static.network.wifi.internet_port.type" is set to 2 (Static IP).	IPv4 Address	Blank
static.network.wifi.static_dns_enable	It triggers the static DNS feature to on or off for the wireless network. **NOTE** It works only if "static.network.wifi.internet_port.type" is set to 0 (DHCP).	0-Off, the phone will use the IPv4 DNS obtained from DHCP. 1-On, the phone will use manually configured static IPv4 DNS.	0

static.network.wifi.primary_dns	It configures the primary IPv4 DNS server for the wireless network. **ⓘ NOTE** It works only if "static.network.wifi.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). In the DHCP environment, you also need to make sure "static.network.wifi.static_dns_enable" is set to 1 (On).	IPv4 Address	Blank
static.network.wifi.secondary_dns	It configures the secondary IPv4 DNS server for the wireless network. **ⓘ NOTE** It works only if "static.network.wifi.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). In the DHCP environment, you also need to make sure "static.network.wifi.static_dns_enable" is set to 1 (On).	IPv4 Address	Blank

Set via the Web User Interface

On the web user interface, go to: **Network** > **Wi-Fi** > **IP Settings** > **Internet port** > **IPv4 Config**



IPv6 Wireless Network Configuration

If you configure the network settings on the phone for an IPv6 network, you can set up an IP address for the phone

by using SLAAC (ICMPv6), DHCPv6, or by manually entering an IP address. Ensure that your network environment supports IPv6. Contact your ISP for more information.

When you enable both SLAAC and DHCPv6 on the phone, the server can specify the 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.

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

Configuration parameter

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

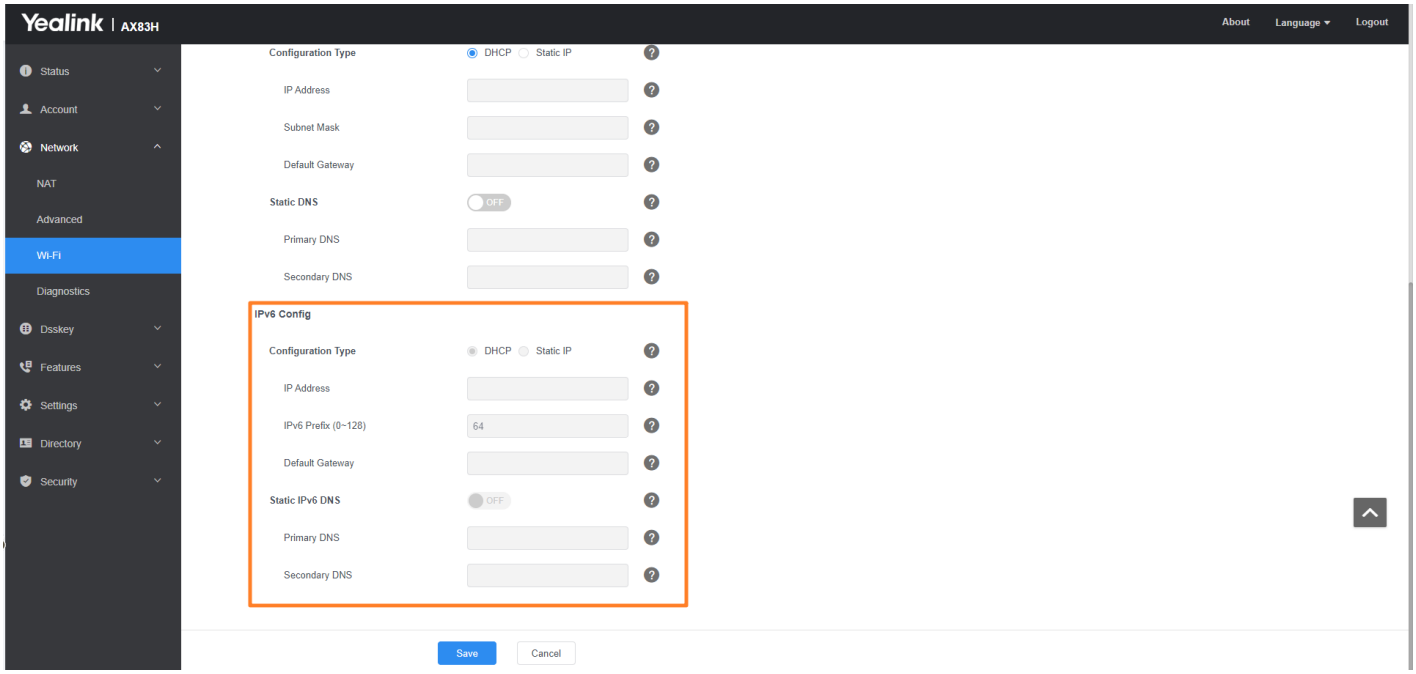
Parameter	Description	Permitted Values	Default
static.network.wifi.ipv6_internet_port.type	It configures the Internet port type for IPv6 wireless network. **NOTE** It works only if "static.network.wifi.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6).	0-DHCP 1-Static IP	0
static.network.wifi.ipv6_internet_port.ip	It configures the IPv6 address for the wireless network. **NOTE** It works only if "static.network.wifi.ipv6_internet_port.type" is set to 1 (Static IP).	IPv6 Address	Blank
static.network.wifi.ipv6_prefix	It configures the IPv6 prefix for the wireless network. **NOTE** It works only if "static.network.wifi.ipv6_internet_port.type" is set to 1 (Static IP).	Integer from 1 to 128	64

static.network.wifi.ipv6_internet_port.gateway	It configures the IPv6 default gateway for the wireless network. **NOTE** It works only if "static.network.wifi.ipv6_internet_port.type" is set to 1 (Static IP).	IPv6 Address	Blank
static.network.wifi.ipv6_static_dns_enable	It triggers the static IPv6 DNS feature to on or off for the wireless network. **NOTE** It works only if "static.network.wifi.ipv6_internet_port.type" is set to 0 (DHCP).	0-Off, the phone will use the IPv6 DNS obtained from DHCP. 1-On, the phone will use manually configured static IPv6 DNS.	0
static.network.wifi.ipv6_primary_dns	It configures the primary IPv6 DNS server for the wireless network. **NOTE** It works only if "static.network.wifi.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In the DHCP environment, you also need to make sure "static.network.wifi.ipv6_static_dns_enable" is set to 1 (On).	IPv6 Address	Blank
static.network.wifi.ipv6_secondary_dns	It configures the secondary IPv6 DNS server for the wireless network. **NOTE** It works only if "static.network.wifi.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In the DHCP environment, you also need to make sure "static.network.wifi.ipv6_static_dns_enable" is set to 1 (On).	IPv6 Address	Blank

static.network.wifi.ipv6_icmp_v6.enable	It enables or disables the phone to obtain IPv6 wireless network settings via SLAAC (Stateless Address Autoconfiguration). **NOTE** It works only if "static.network.wifi.ipv6_internet_port.type" is set to 0 (DHCP).	0-Disabled 1-Enabled	1

Set via the Web User Interface

On the web user interface, go to **Network** > **Wi-Fi** > **IP Settings** > **Internet port** > **IPv6 Config**.



How to access the web user interface

Introduction

You can access the web user interface using the IP address.
The switch or gateway distributes the IP address. It doesn't have a factory IP address.

How do you get the IP address of the Phone?

Go to **OK** > **Status** to check the device's IP address.

IPv4 and IPv6 Network Settings

Introduction

You can configure the devices to operate in IPv4, IPv6, or dual-stack (IPv4/IPv6) mode.
After establishing wired network connectivity, the devices obtain the IPv4 or IPv6 network settings from a Dynamic Host Configuration Protocol (DHCPv4 or DHCPv6) server. We recommend using DHCP where possible to eliminate repetitive manual data entry.
You can also configure IPv4 or IPv6 network settings manually.

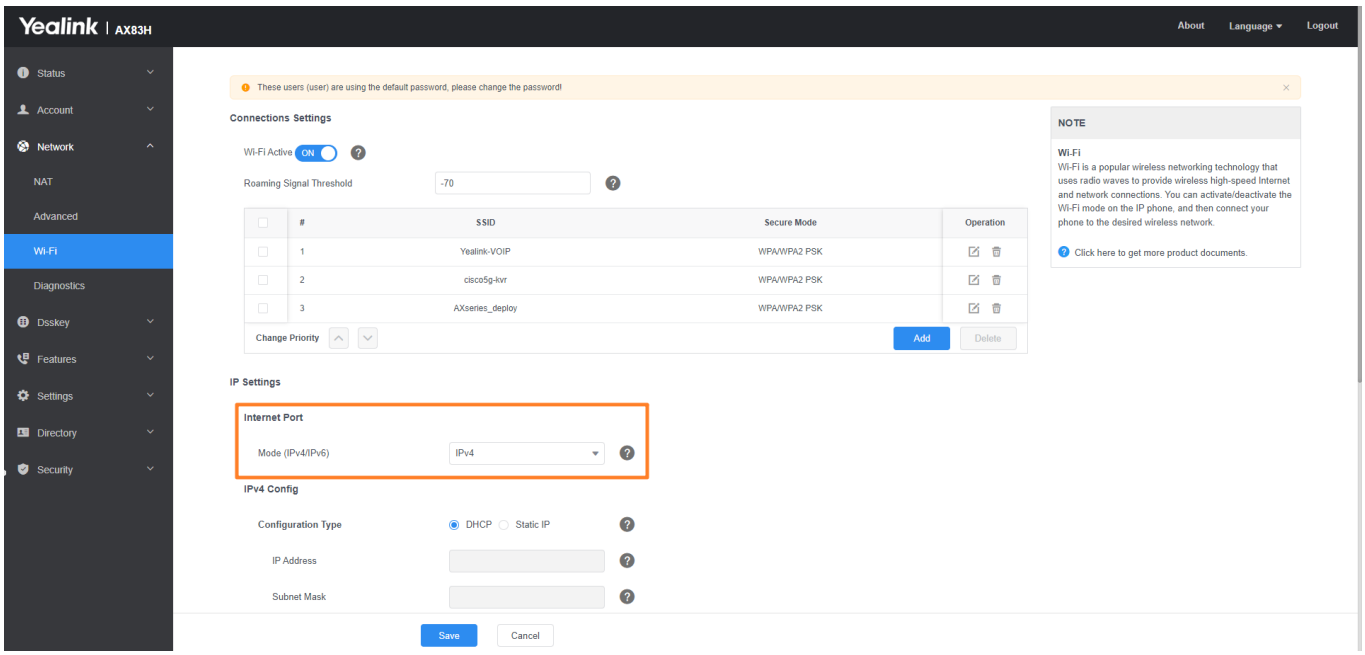
NOTE
Yealink devices comply with the DHCPv4 specifications documented in RFC 2131, and DHCPv6 specifications documented in RFC 4443.

IP Addressing Mode Configuration

You can configure IP addressing mode for the Wi-Fi network.

Set via the Web User Interface

1. On the web user interface, go to **Network** > **Wi-Fi** > **Internet Port**.



Configuration Parameter

```
static.network.wifi.ip_address_mode
static.network.wifi.preference
```

Parameter	Permitted Values	Default	Description
static.network.wifi.ip_address_mode[1]	**0**-IPv4 **1**-IPv6 **2**-IPv4 & IPv6	0	It configures the IP addressing mode.
static.network.wifi.preference[1]	**0**-IPv6 **1**-IPv4	0	It specifies IPv4 or IPv6 as the preferred wired network in a Dual-Stack mode. **NOTE** It works only if "static.network.wifi.ip_address_mode is set to 2 (IPv4 & IPv6).

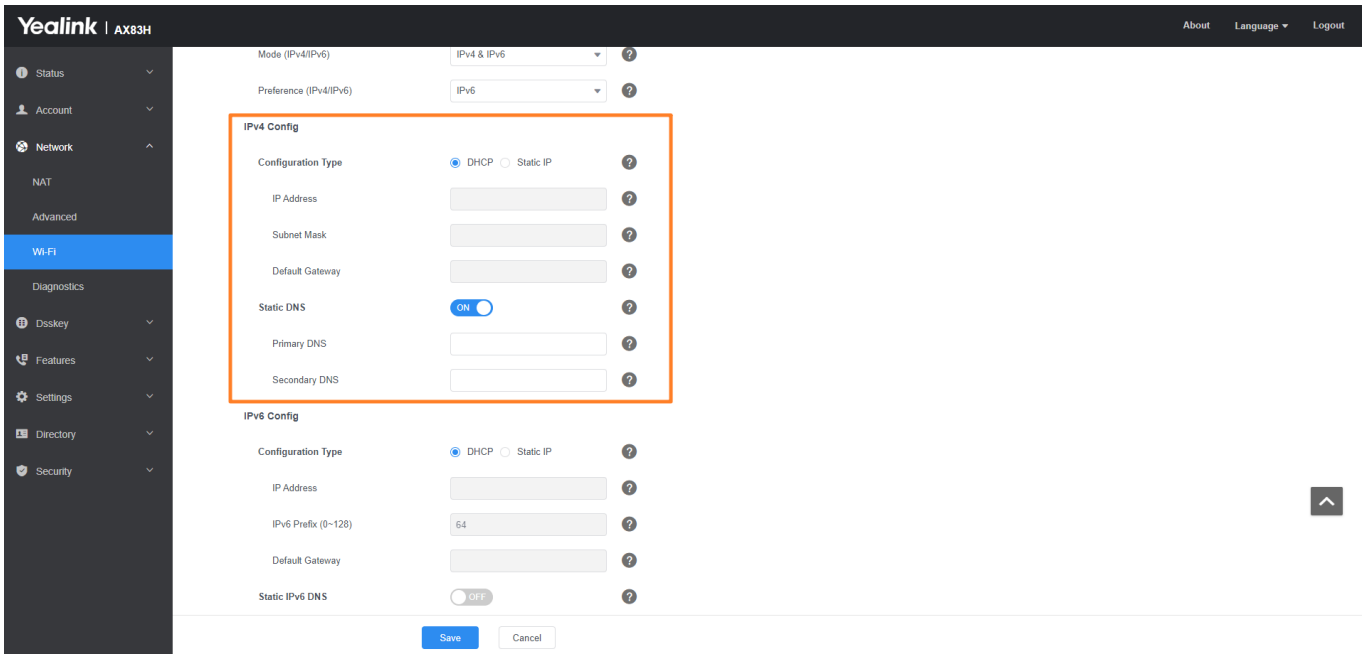
[1]If you change this parameter, the phone will reboot to make the change take effect.

IPv4 Configuration

You can configure the devices to operate in IPv4 mode.

Set via the Web User Interface

1. On the web user interface, go to **Network** > **Wi-Fi** > **IPv4 Config**.



Configuration Parameter

static.phone_setting.auto_switch_internet_port_type.enable
static.phone_setting.auto_switch_internet_port_type.time
static.network.wifi.internet_port.type
static.network.wifi.internet_port.ip
static.network.wifi.internet_port.mask
static.network.wifi.internet_port.gateway
static.network.wifi.static_dns_enable
static.network.wifi.primary_dns
static.network.wifi.secondary_dns

Parameter	Permitted Values	Default	Description
static.phone_setting.auto_switch_internet_port_type.enable[1]	**0**-Disabled **1**-Enabled, switching automatically	0	It enables or disables the feature of switching between DHCP and static IP mode automatically.
static.phone_setting.auto_switch_internet_port_type.time[1] [	Integer from 10 to 65535	60	It configures the overtime of switching between DHCP and static IP mode. **NOTE** It works only if `static.phone_setting.auto_switch_internet_port_type.enable` is set to 1.

static.network.wifi.internet_port.type[1]	**0**-DHCP **2**-Static IP	0	It configures the Internet port type for IPv4.
static.network.wifi.internet_port.ip[1]	IPv4 Address	Blank	It configures the IPv4 address. **NOTE** It works only if `static.network.wifi.internet_port.type` is set to 2 (Static IP).
static.network.wifi.internet_port.mask[1]	Subnet Mask	Blank	It configures the IPv4 subnet mask. **NOTE** It works only if `static.network.wifi.internet_port.type` is set to 2 (Static IP).
static.network.wifi.internet_port.gateway[1]	IPv4 Address	Blank	It configures the IPv4 default gateway. **NOTE** It works only if `static.network.wifi.internet_port.type` is set to 2 (Static IP).
static.network.wifi.static_dns_enable[1]	**0**-Off, the phone will use the IPv4 DNS obtained from DHCP. **1**-On, the phone will use manually configured static IPv4 DNS.	0	It triggers the static DNS feature to on or off. **NOTE** It works only if `static.network.wifi.internet_port.type` is set to 0 (DHCP).
static.network.wifi.primary_dns[1]	IPv4 Address	Blank	It configures the primary IPv4 DNS server. **NOTE** In the DHCP environment, you need to make sure `static.network.wifi.static_dns_enable` is set to 1 (On).

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

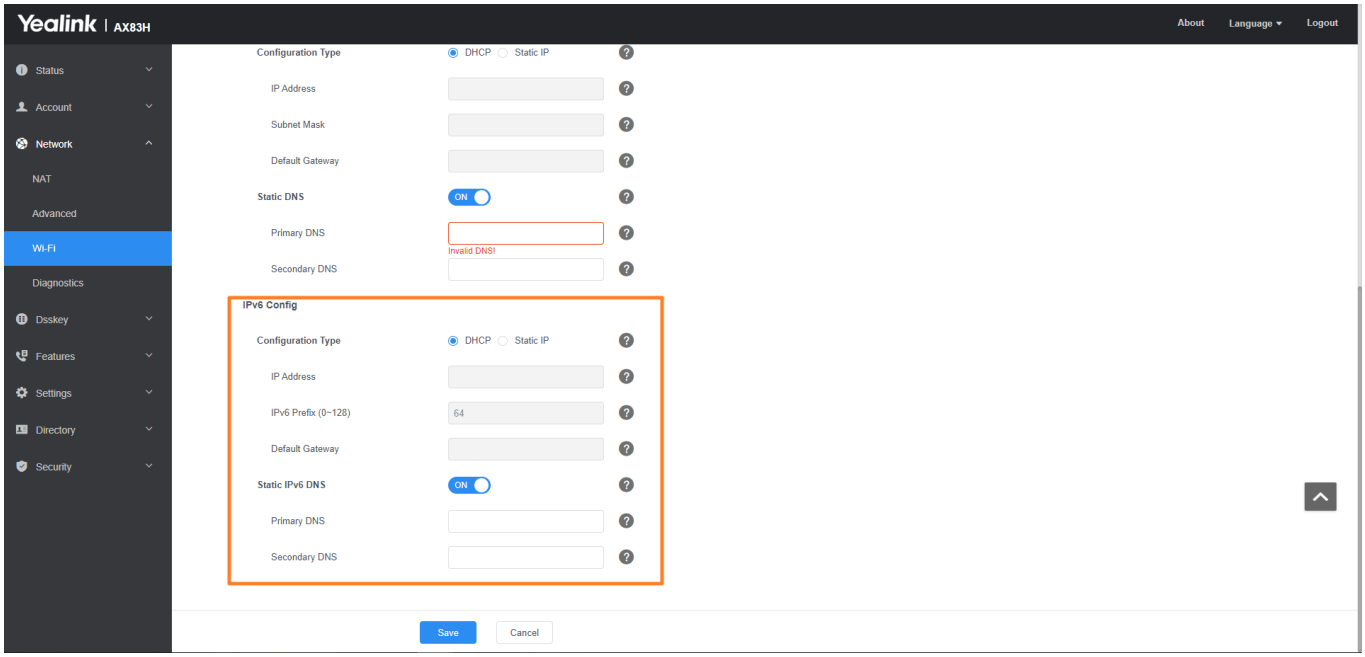
> [1]If you change this parameter, the phone will reboot to make the change take effect.

IPv6 Configuration

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.

Set via the Web User Interface

1. On the web user interface, go to **Network** > **Wi-Fi** > **IPv6 Config**.



Configuration Parameter

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

Parameter	Permitted Values	Default	Description

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

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

DHCP Option for IPv4

Introduction

The phone can obtain IPv4-related parameters in an IPv4 network via the DHCP option.
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 Mas	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.
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.
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 66, Option 43, and Custom Option

Description

During the startup, the phone automatically detects the DHCP option 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.

TIP

If you fail to configure the DHCP options for discovering the provisioning server on the DHCP server, enable the phone to automatically discover the provisioning server address. One possibility is connecting to the secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server address. For more information, refer to RFC 3925.

Related Topic

DHCP Provision Configuration

DHCP Option 42 and Option 2

Description

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).

Related Topic

NTP Settings

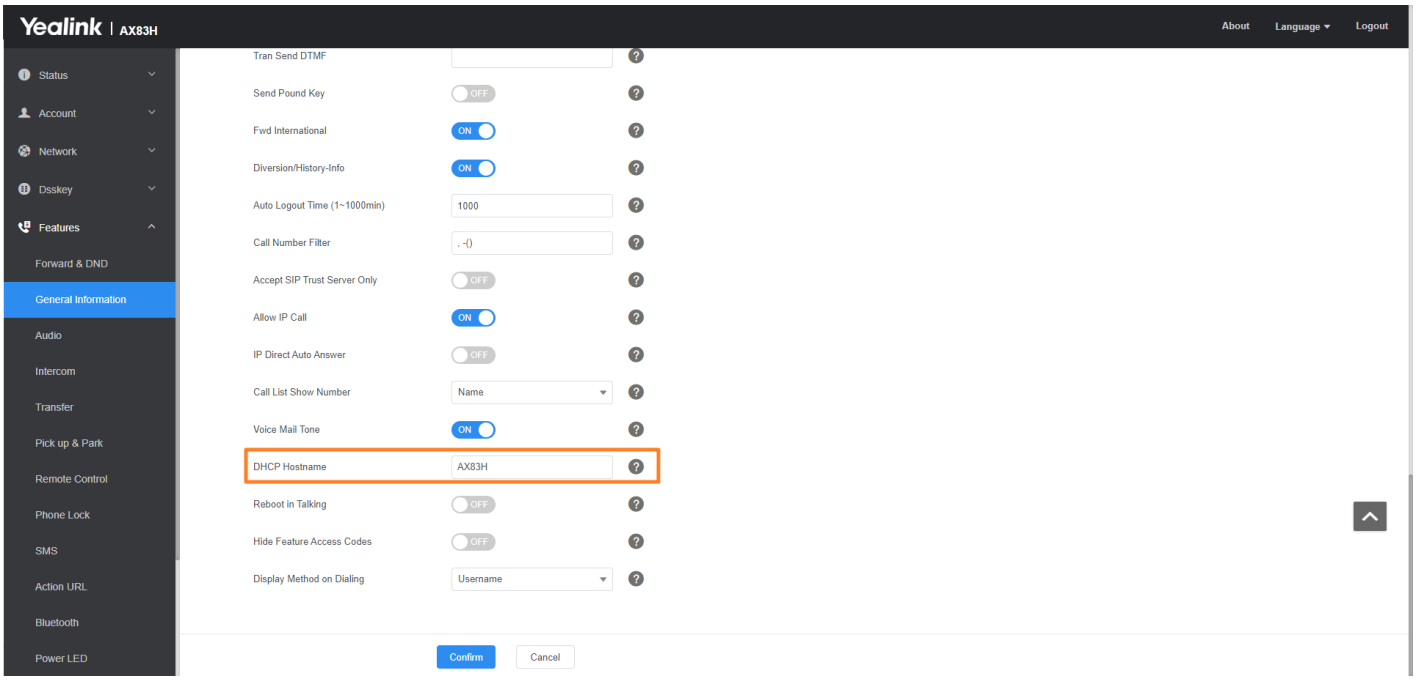
DHCP Option 12

Description

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.
See RFC 1035 for character set restrictions.

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **DHCP Hostname**.



Configuration parameter

static.network.dhcp_host_nam

Parameter	Permitted Values	Default	Description
static.network.dhcp_host_name[1]	String within 99 characters	SIP-Txx(you device model)	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

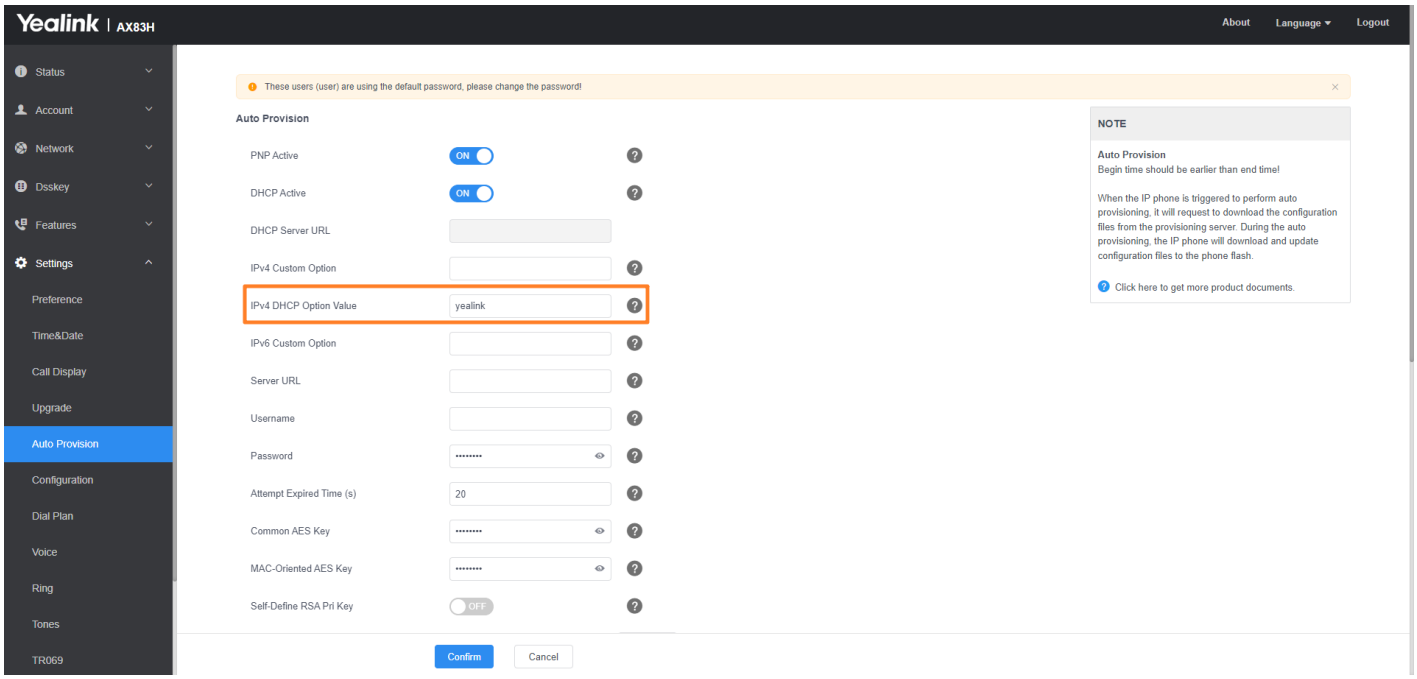
Description

DHCP option 60 is used to indicate the vendor type. Servers can use option 43 to return the vendor-specific information to the client.

You can set the DHCP option 60 type.

Set via the Web User Interface

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



Configuration parameter

```
static.network.dhcp.option60type
static.auto_provision.dhcp_option.option60_value
```

Parameter	Permitted Values	Default	Description
static.network.dhcp.option60type	**0**-ASCII, vendor-identifying information is in ASCII format. **1**-Binary, vendor-identifying information is in the format defined in RFC 3925.	0	It configures the DHCP option 60 type.
static.auto_provision.dhcp_option.option60_value	String within 99 characters	yealink	It configures the vendor class identifier string to use in the DHCP interaction.

Troubleshooting

To facilitate your confirmation of whether the phone has obtained the DHCP URL, T3X/T4XU/T5XW SIP phones have added a configuration option in versions x.86.0.129 and later to control whether to display the DHCP-obtained URL.

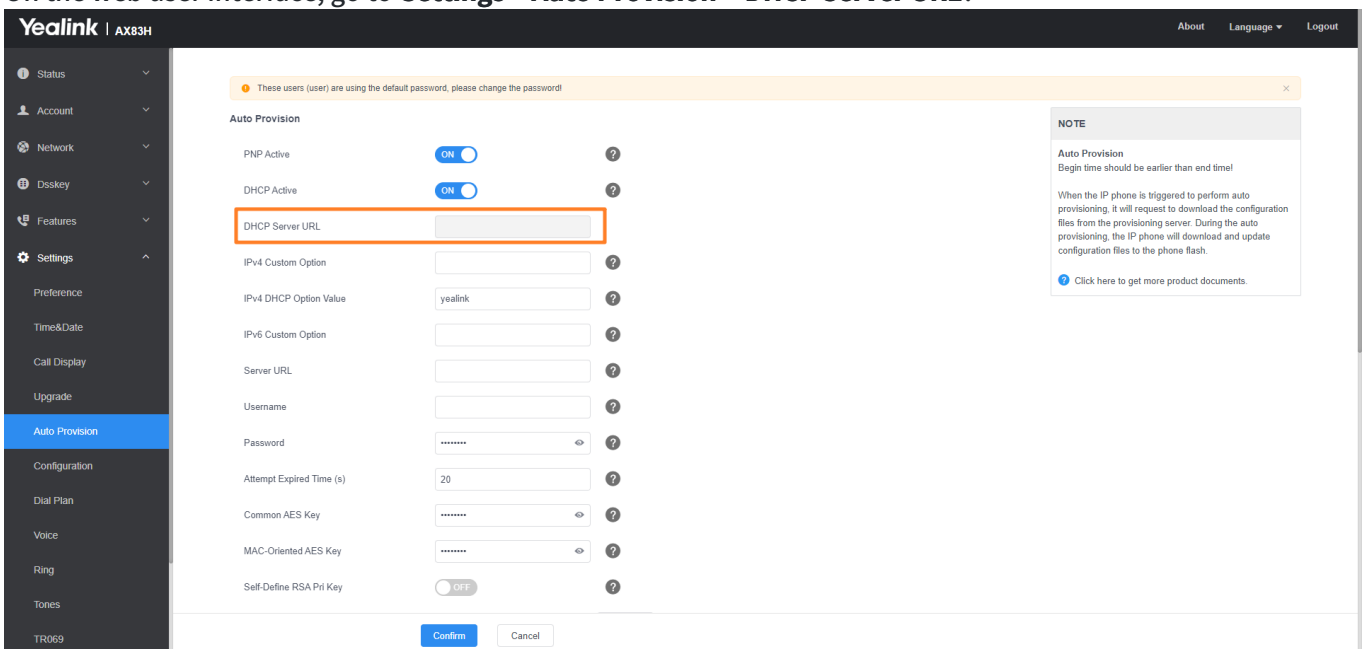
Configuration parameter

```
dhcp_server_url_display.enable
```

Parameter	Permitted Values	Default	Description
dhcp_server_url_display.enable	**0**-Disable **1**-Enable	0	It is used to configure whether to display the DHCP-obtained URL.

Set via the Web User Interface

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



ⓘ NOTE

DHCP Server URL can not be edited.

DHCP Option for IPv6

Introduction

The phone can obtain IPv6-related parameters in an IPv6 network via DHCP option.

Supported DHCP Option for IPv6

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.
59	Boot File URL	Specify a URL for the boot file to be downloaded by the client.

DHCP Option 59 and Custom Option

During the startup, the phone automatically detects the DHCP option for obtaining the provisioning server address. The priority is as follows: custom option > option 59.

Related Topic

DHCP Provision Configuration

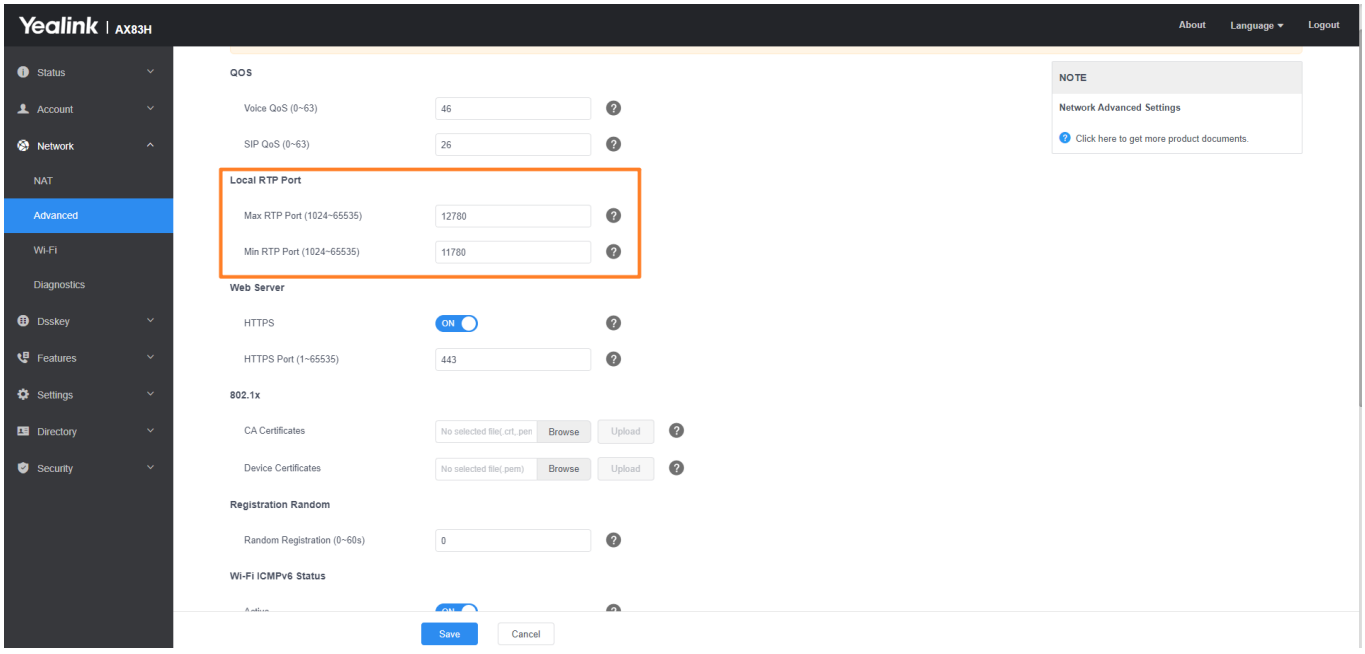
Real-Time Transport Protocol (RTP) Ports

Introduction

Since the phone supports conferencing and multiple RTP streams, it can use several ports concurrently. You can specify the phone’ s RTP port range.
The UDP port used for RTP streams is traditionally an even-numbered port. If port 11780 is used to send and receive RTP for the first voice session, additional calls would then use ports 11782, 11784, 11786, and so on. The phone is compatible with RFC 1889 - RTP: A Transport Protocol for Real-Time Applications and the updated RFC 3550.

Set via the Web User Interface

1. On the web user interface, go to **Network** > **Advanced** > **Local RTP Port**.



Configuration Parameter

```
static.network.port.min_rtpport
static.network.port.max_rtpport
static.dm.X.network.port.min_rtpport
static.dm.X.network.port.max_rtpport
features.rtp_symmetric.enable
```

Parameter	Permitted Values	Default	Description
static.network.port.min_rtpport[1]	Integer from 1024 to 65535	11780	t configures the minimum local RTP port.
static.network.port.max_rtpport[1]	Integer from 1024 to 65535	12780	It configures the maximum local RTP port.
static.dm.X.network.port.min_rtpport[1]	Integer from 1024 to 65535	11780	It configures the minimum local RTP port of the DM.
static.dm.X.network.port.max_rtpport[1]	Integer from 1024 to 65535	12780	It configures the maximum local RTP port of the DM.
features.rtp_symmetric.enable	**0**-Disabled **1**-reject RTP packets arriving from a non-negotiated IP address **2**-reject RTP packets arriving from a non-negotiated port **3**-reject RTP packets arriving from a non-negotiated IP address or a non-negotiated port	0	It configures the symmetrical RTP feature.

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

Network Address Translation (NAT)

Introduction

NAT enables phones with private unregistered addresses to communicate with devices with globally unique registered addresses.

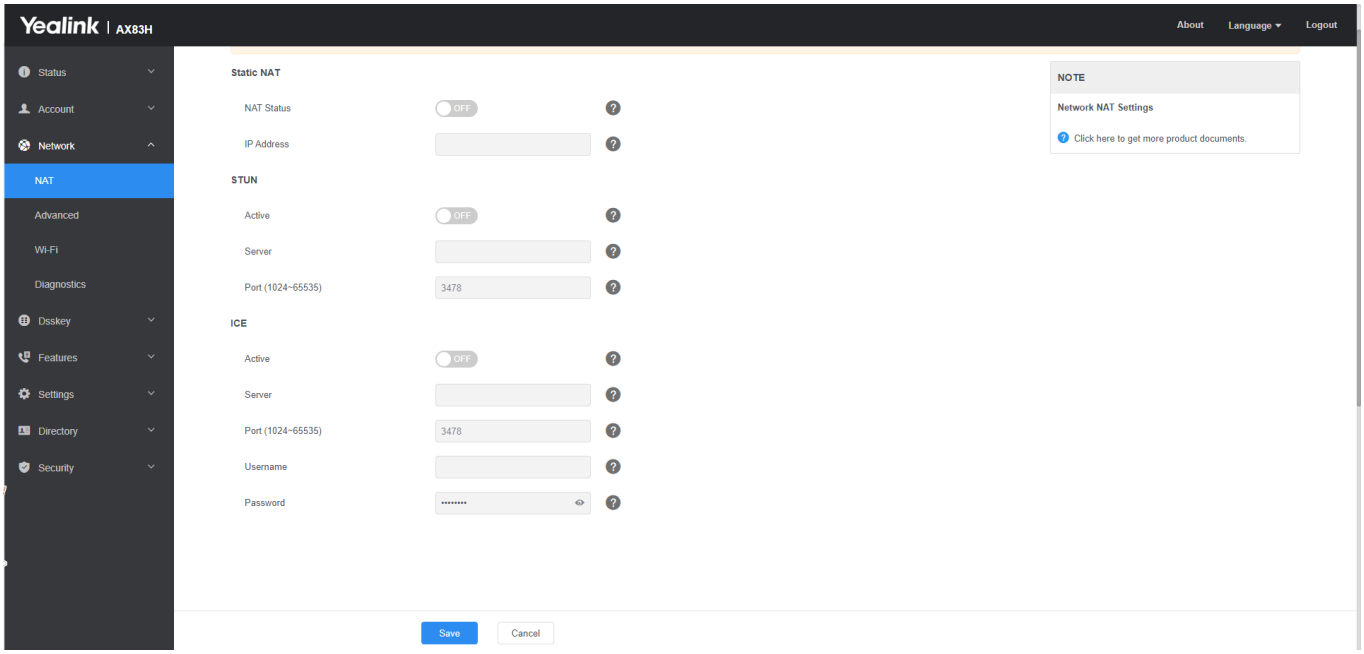
NAT Traversal

The phones can traverse NAT gateways to establish and maintain connections with external devices.
Yealink phones support three NAT traversal techniques: manual NAT, STUN, and ICE. If you enable manual NAT and STUN, the phone will use the manually configured external IP address for NAT traversal. The TURN protocol is used as part of the ICE approach to NAT traversal.

NAT Traversal Configuration

Set via the Web User Interface

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



Configuration Parameter

account.X.nat.nat_traversal
static.network.static_nat.enable
static.network.static_nat.addr
static.sip.nat_stun.enable
static.sip.nat_stun.server
static.sip.nat_stun.port
static.ice.enable[
static.sip.nat_turn.enable
static.sip.nat_turn.server
static.sip.nat_turn.port
static.sip.nat_turn.username
static.sip.nat_turn.password
features.media_transmit.enable
account.X.media_transmit.enable

Parameter	Permitted Values	Default	Description
account.X.nat.nat_traversal[1]	**0**-Disabled **1**-STUN **2**-Manual NAT	0	It enables or disables the NAT traversal for a specific account. **NOTE** If it is set to 1 (STUN), it works only if `static.sip.nat_stun.enable` is set to 1 (Enabled); if it is set to 2 (Manual NAT), it works only if `static.network.static_nat.enable` is set to 1 (Enabled).

static.network.static_nat.enable[2]	**0**-Disabled **1**-Enabled	0	It enables or disables the manual NAT feature.
static.network.static_nat.addr	IP Address	Blank	It configures the IP address to be advertised in SIP signaling. It should match the external IP address used by the NAT device. **NOTE** It works only if static.network.static_nat.enable is set to 1 (Enabled).
static.sip.nat_stun.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the STUN (Simple Traversal of UDP over NATs) feature.
static.sip.nat_stun.server	String	Blank	It configures the IP address or domain name of the STUN server. **NOTE** It works only if static.sip.nat_stun.enable is set to 1 (Enabled).
static.sip.nat_stun.port	Integer from 1024 to 65535	3478	It configures the port of the STUN server. **NOTE** It works only if static.sip.nat_stun.enable is set to 1 (Enabled).
static.ice.enable[2]	**0**-Disabled **1**-Enabled	0	It enables or disables the ICE (Interactive Connectivity Establishment) feature.
static.sip.nat_turn.enable[2]	**0**-Disabled **1**-Enabled	0	It enables or disables the TURN (Traversal Using Relays around NAT) feature.
static.sip.nat_turn.server[2]	IP Address or Domain Name	Blank	It configures the IP address or the domain name of the TURN server. **NOTE** It works only if static.sip.nat_turn.enable is set to 1 (Enabled).

static.sip.nat_turn.port[2]	Integer from 1024 to 65535	3478	It configures the port of the TURN server. **NOTE** It works only if `static.sip.nat_turn.enable` is set to 1 (Enabled).
static.sip.nat_turn.username[2]	String	Blank	It configures the user name to authenticate to the TURN server. **NOTE** It works only if `static.sip.nat_turn.enable` is set to 1 (Enabled).
static.sip.nat_turn.password[2]	String	Blank	It configures the password to authenticate to the TURN server. **NOTE** It works only if `static.sip.nat_turn.enable` is set to 1 (Enabled).
features.media_transmit.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the media stream to be forward forcibly on the DECT manager (DM) during a STUN/ICE call. **NOTE** The value configured by the parameter `account.X.media_transmit.enable` takes precedence over that configured by this parameter.
account.X.media_transmit.enable[1]	**0**-Disabled **1**-Enabled	Blank	It enables or disables the media stream to be forward forcibly on the DECT manager (DM) during a STUN/ICE call. **NOTE** The value configured by this parameter takes precedence over that configured by the parameter `features.media_transmit.enable`.

[1]X is the account ID.
[2]If you change this parameter, the phone will reboot to make the change take effect.

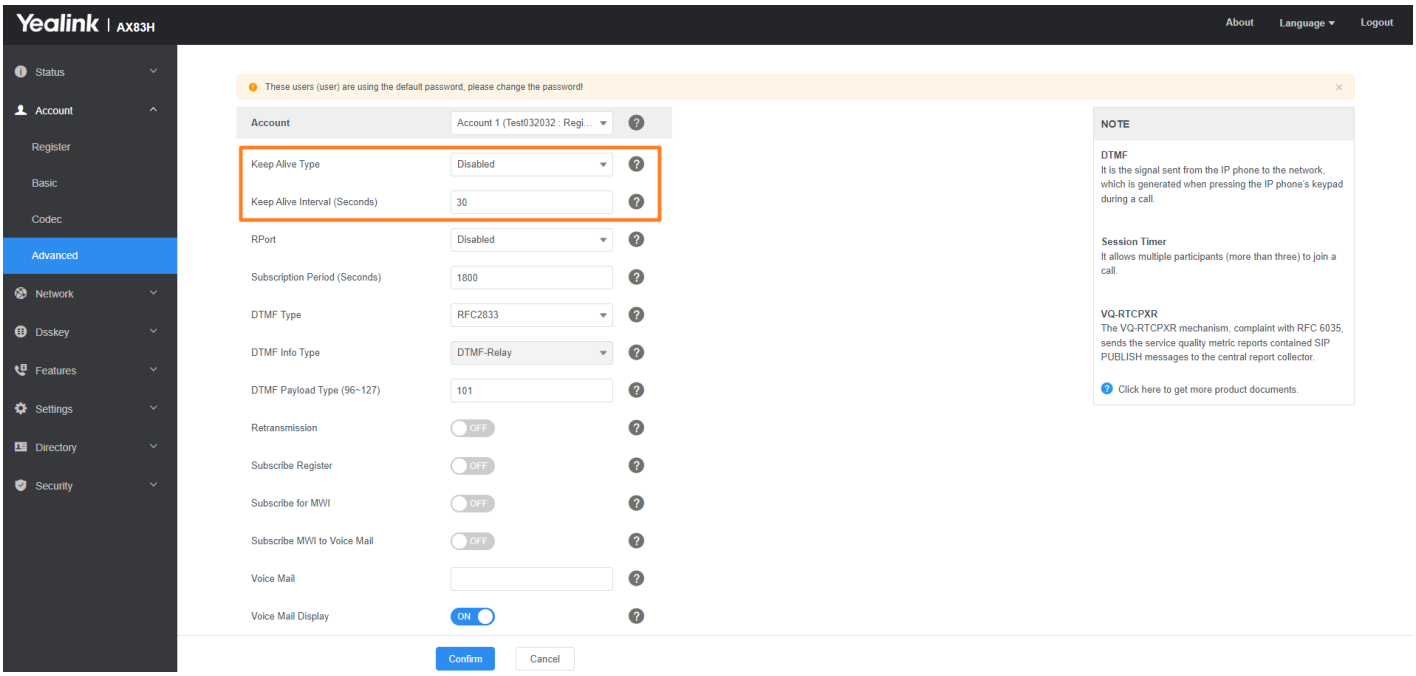
Keep Alive

Yealink phones can send keep-alive packets to the NAT device for keeping the communication port open.

Keep Alive Configuration

Set via the Web User Interface

On the web user interface, go to **Account** > **Advanced** > **Keep Alive Type**/**Keep Alive Interval(Seconds)**.



Configuration Parameter

```
account.X.nat.udp_update_enable
account.X.nat.udp_update_time
```

Parameter	Permitted Values	Default	Description
account.X.nat.udp_update_enable[1]	**0**-Disabled **1**-Default (the phone sends the corresponding packets according to the transport protocol) **2**-Options (the phone sends SIP OPTIONS packets to the server) **3**-Notify (the phone sends SIP NOTIFY packets to the server)	1	It sets the type of keep-alive packets sent by phone.
account.X.nat.udp_update_time[1]	Integer from 0 to 3600	30	It configures the interval (in seconds) at which the phone sends a keep-alive package. **NOTE** It works only if `account.X.nat.udp_update_enable` is set to 1, 2 or 3.

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

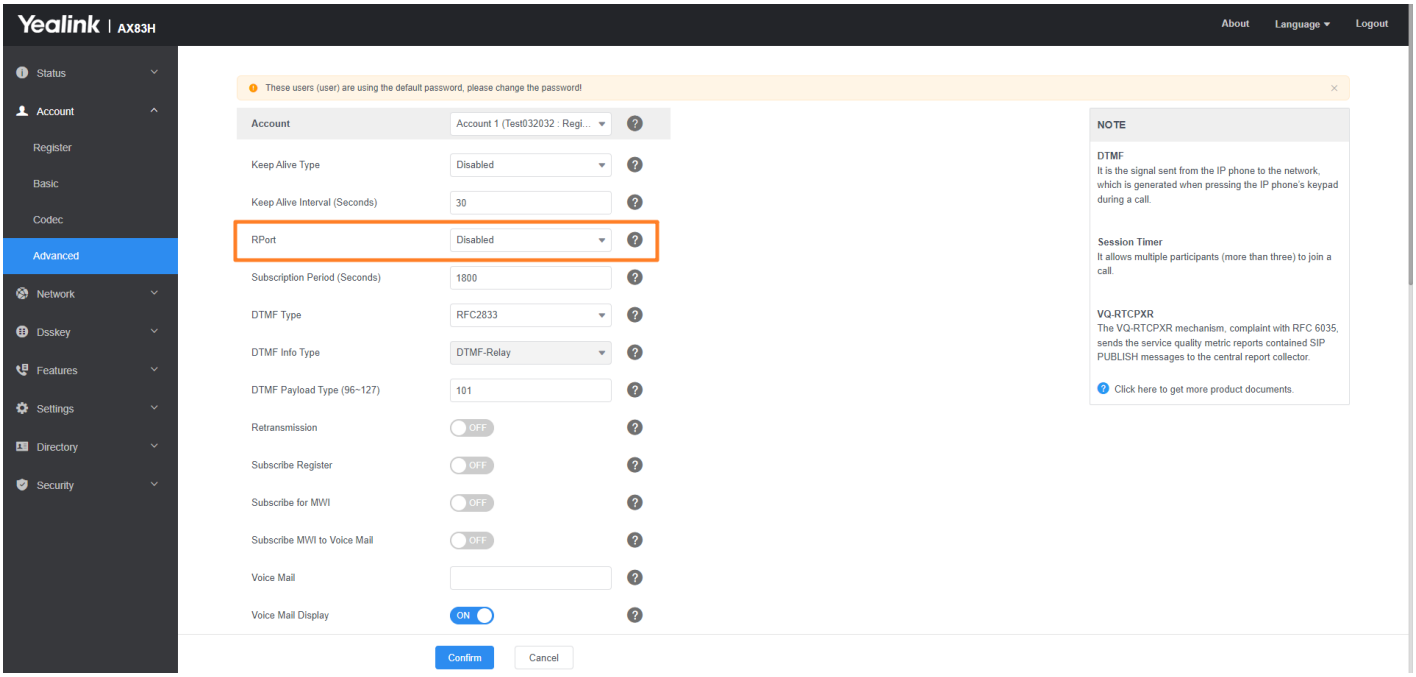
Rport

Rport allows a client to request that the server sends the response back to the source IP address and port from which the request originated. It helps the phone traverse symmetric NATs.
Rport feature depends on support from a SIP server. For more information, refer to RFC 3581.

Rport Configuration

Set via the Web User Interface

On the web user interface, go to **Account** > **Advanced** > **RPort**.



Configuration Parameter

```
account.X.nat.rport
```

Parameter	Permitted Values	Default	Description
account.X.nat.rport[1]	0-Disabled 1-Enabled, the INVITE Contact header uses the port in the "rport" parameter but does not use the source IP address in the "received" parameter in the Via header of server's response. 2-Enable Direct Process, the INVITE Contact header uses the port in the "rport" parameter and uses the source IP address in the "received" parameter in the Via header of server's response.	0	It enables or disables the phone to add the "rport" parameter in the Via header.

[1]X is the account ID.

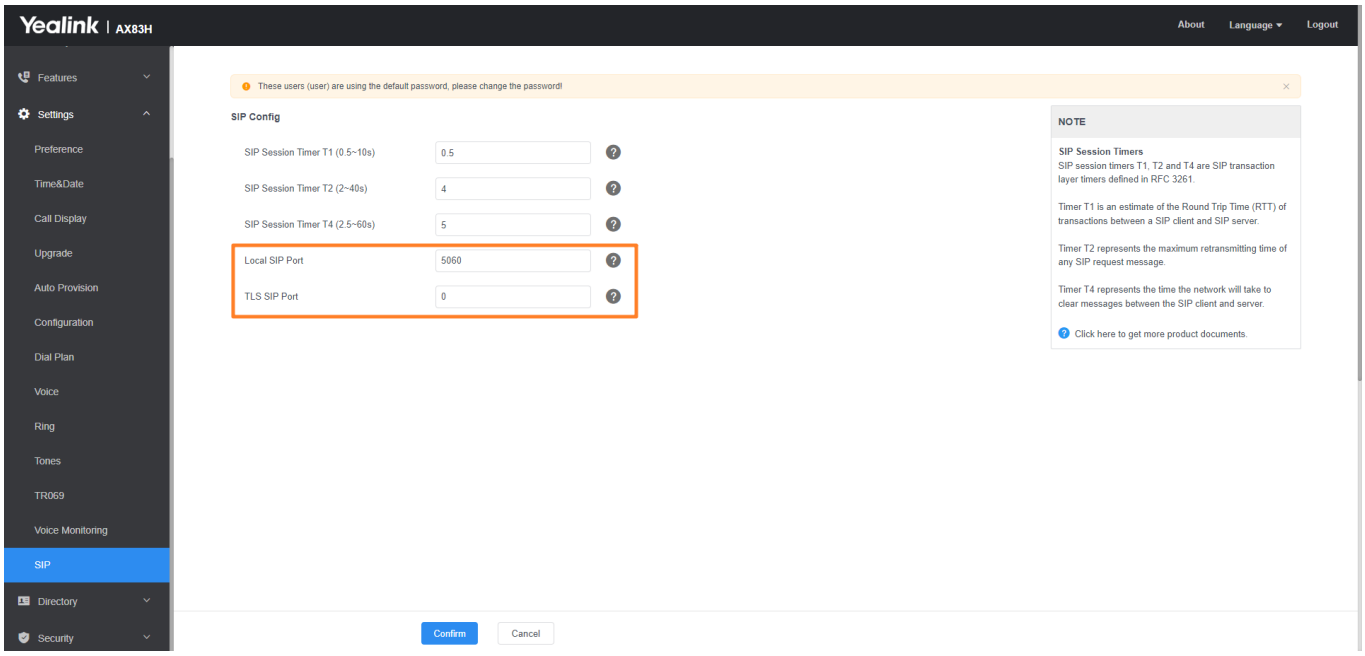
SIP Port and TLS Port

You can configure the SIP and TLS source ports on the phone. Otherwise, the phone uses default values (5060 for UDP/TCP and 5061 for TLS).
If NAT is disabled, the port number shows in the Via and Contact SIP headers of SIP messages. If NAT is enabled, the phone uses the NAT port number (and NAT IP address) in the Via and Contact SIP headers of SIP messages, but still using the configured source port.

SIP Port and TLS Port Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **SIP** > **Local SIP Port**/**TLS SIP Port**.



Configuration Parameter

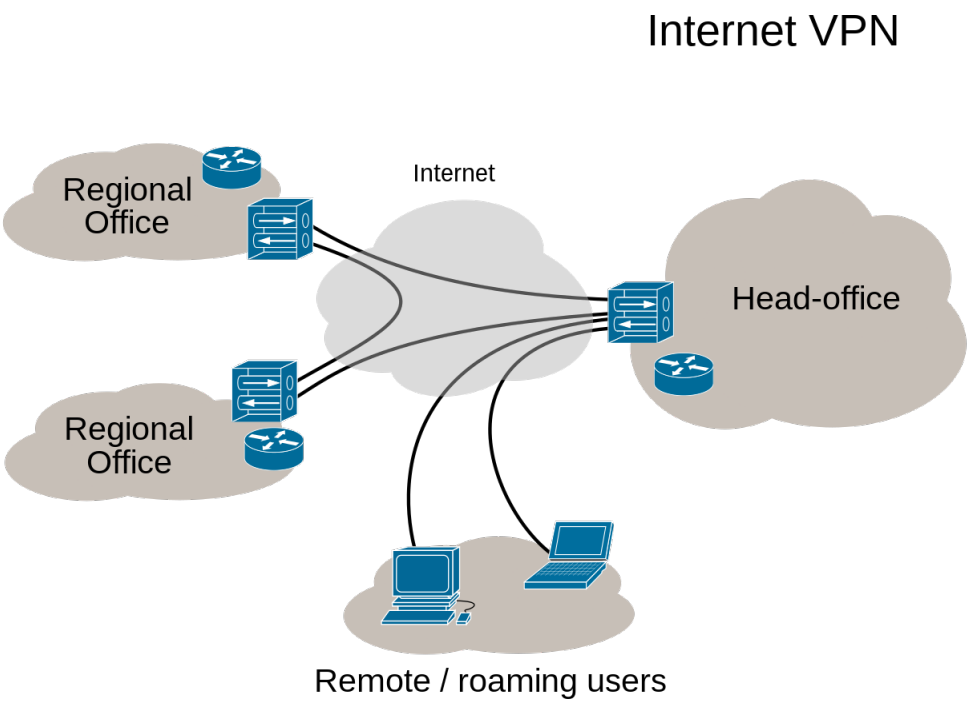
```
sip.listen_port
sip.tls_listen_port
```

Parameter	Permitted Values	Default	Description
sip.listen_port	0, Integer from 1024 to 65535	5060	It specifies the local SIP port. If it is set to 0, the phone will automatically listen to the local SIP port.
sip.tls_listen_port	0, Integer from 1024 to 65535	5061	It specifies the local TLS listen port. If it is set to 0, the phone will not listen to the TLS service.

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.



Types of VPN Access

Type	Description
Remote access VPN	Remote access VPN, also called a virtual private dial-up network (VPDN), is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations.
Site-to-site VPN	Site-to-site VPN connects entire networks, which means, site-to-site VPN can be used to connect a branch or remote office network to a company headquarters network. Each site is equipped with a VPN gateway, such as a router, firewall, VPN concentrator, or security appliance.

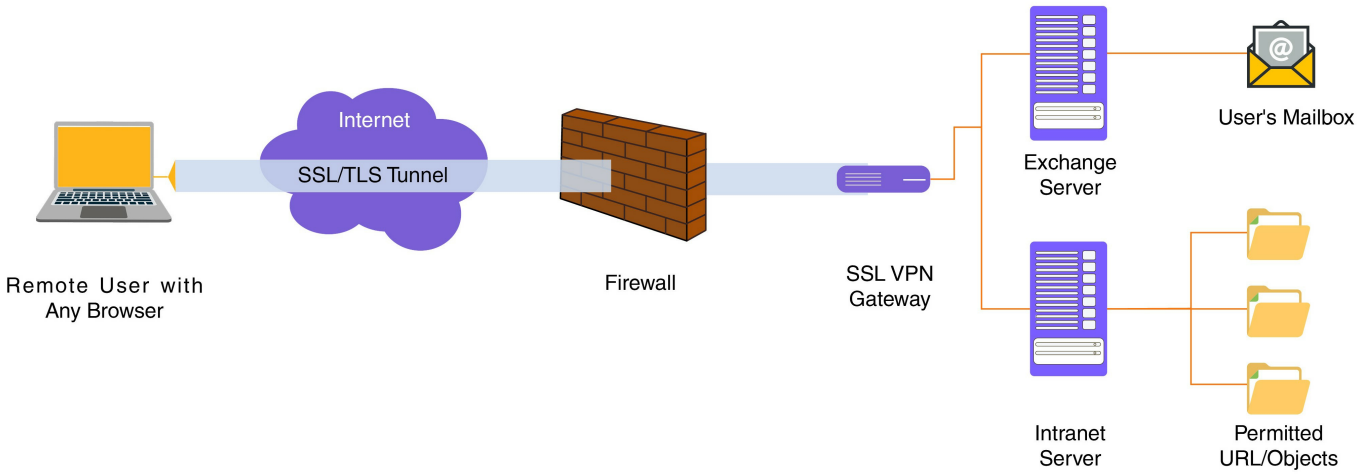
VPN Technology

VPN technology is based on the idea of tunneling. VPN tunneling involves establishing and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other bases or carrier protocols, then transmitted between the VPN client and the server, and finally de-encapsulated on the receiving side.

Several computer network protocols have been implemented specifically for use with VPN tunnels. The most two popular VPN tunneling protocols are **SSL** (Security Socket Layer) and **IPSec** (Internet Protocol Security).

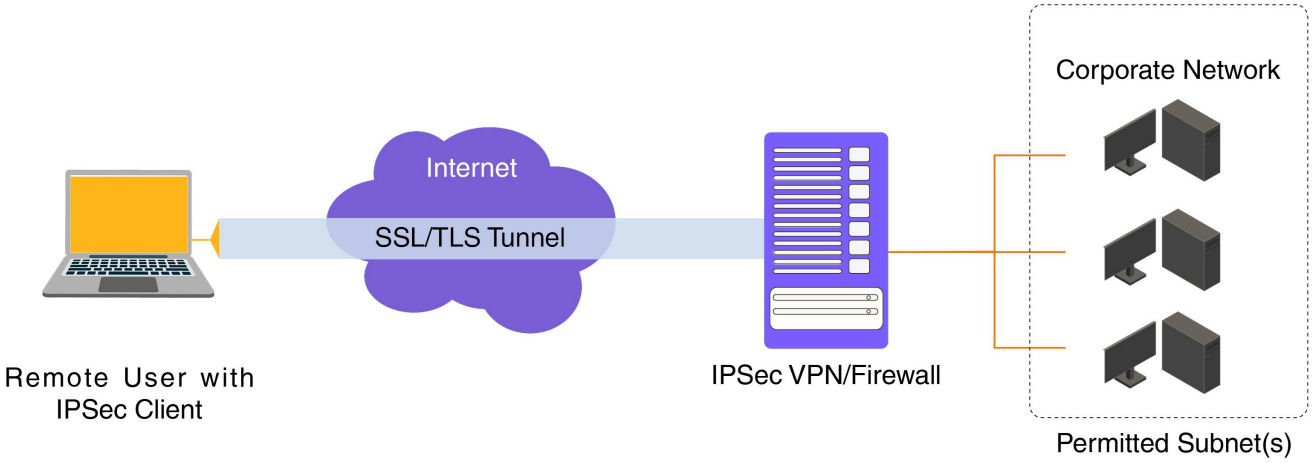
SSL VPN

SSL VPN uses the SSL protocol and Transport Layer Security (TLS) protocol to provide a secure connection between remote users and internal network resources. It can be used with a standard web browser and does not require the installation of specialized client software on the end user's device. An SSL VPN offers versatility, ease of use, and granular control for a range of users on a variety of devices, accessing resources from many locations.



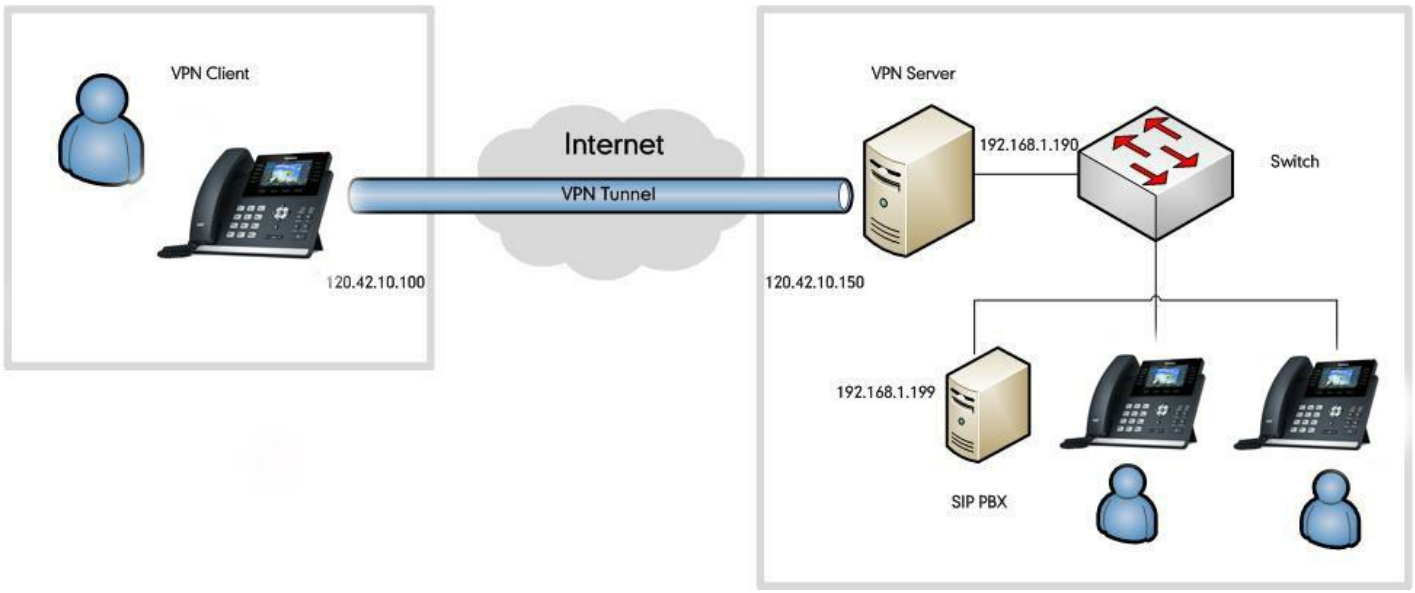
IPSec VPN

An IPSec VPN uses the standard IPSec mechanism to establish a VPN connection over the public Internet. IPSec is a framework for a set of protocols for security at the network or packet processing layer of network communication. IPSec VPN requires the installation of the IPSec client software on a client device before a connection can be established. IPSec can meet most security goals: authentication, integrity, and confidentiality.



Example Use of a VPN Tunnel

An employee has a phone with a public IP address 120.42.10.100 that wishes to connect to the SIP server inside a company network. The SIP server has an internal IP address of 192.168.1.199 and is not reachable publicly. Before reaching this server, the phone needs to go through a VPN server that has a public IP address 120.42.10.150 and an internal address 192.168.1.190. All data between the phone and the SIP server will need to be kept confidential, hence a secure VPN is used.



The following steps illustrate the principles of a VPN client-server interaction:

1. The VPN client connects to a VPN server via an external network interface.
2. The VPN server assigns an IP address to the VPN client from the VPN server's subnet. The client gets an internal IP address 192.168.1.192, for example, and creates a virtual network interface through which it will send encrypted packets to the other tunnel endpoint (the device at the other end of the tunnel).
3. When the VPN client wishes to communicate with the SIP server, it prepares a packet addressed to 192.168.1.199, encrypts it, and encapsulates it in an outer VPN packet. This packet is then sent to the VPN server at IP address 120.42.10.150 over the public Internet. The inner packet is encrypted so that even if someone intercepts the packet over the Internet, they cannot get any information from it. The inner encrypted packet has a source address of 192.168.1.192 and a destination address of 192.168.1.199. The outer packet has a source address of 120.42.10.100 and a destination address of 120.42.10.150.
4. When the packet reaches the VPN server from the Internet, the VPN server de-encapsulates the inner packet, decrypts it, finds the destination address to be 192.168.1.199, and forwards it to the intended SIP server at 192.168.1.199.
5. After some time, the VPN server receives a reply packet from 192.168.1.199, intended for 192.168.1.192. The VPN server consults its routing table and knows this packet is intended for a remote device (IP phone) that must go through a VPN.
6. The VPN server encrypts this reply packet, encapsulates it in a VPN packet, and sends it out over the Internet. The inner encrypted packet has a source address of 192.168.1.199 and a destination address of 192.168.1.192. The outer VPN packet has a source address of 120.42.10.150 and a destination address of 120.42.10.100.
7. The VPN client receives and de-encapsulates the packet, decrypts the inner packet, and passes it to the appropriate software at the upper layers.

Install the OpenVPN Server

If you already have a VPN server, you can skip this section.

OpenVPN server is a set of installation and configuration tools that simplifies the rapid deployment of a VPN remote access solution. It’ s supported on Linux, Windows, and MAC platforms.

Linux Platform

Install and Configure the OpenVPN Server

The OpenVPN server software is available for free. This section provides you with information on how to install the

OpenVPN server (e.g., OpenVPN 2.1.4.tar.gz) on the Linux platform (e.g., Centos 5.8 and kernel: 2.6.18 308.el5 i686). Before the installation, make sure the hardware and system meet the following requirements:

- Dual network cards.
- The system kernel supports the Universal TUN/TAP device driver (kernel 2.6.0 above) and the TUN/TAP module is loaded into the kernel.
- Install the required modules "OpenSSL and LZO".

To check if the TUN/TAP module is loaded into the kernel:

1. Open a terminal window.
2. Enter the following command.

```
[root@localhost~]# cat /dev/net/tun
```

- If the return information is "cat: /dev/net/tun: File descriptor in a bad state", it means that the TUN/TAP module has been loaded into the kernel.
- If the return information is "cat: /dev/net/tun: No such device", you need to execute the following commands to load the TUN/TAP module.

```
[root@localhost~]# cd /usr/src/kernels/2.6.18 308.el5 i686/

[root@localhost 2.6.18 308.el5 i686]# make menuconfig
```

In the pop-up configuration screen, select **Device Drivers**->**Network device support**->**Universal TUN/TAP device driver support** and set to **M**.

You can download the OpenSSL module online: http://www.openssl.org/. The following takes "openssl 1.0.0e.tar.gz" as an example. Download and store it in the root directory.

To install the OpenSSL module:

1. Open a terminal window.
2. Extract the installation package to the /etc directory.

```
[root@localhost~]# cd /etc/
[root@localhost etc]# tar zvxf /openssl 1.0.0e.tar.gz
```

3. Enter into the extracted directory.

```
[root@localhost etc]# cd openssl 1.0.0e
```

4. Enter the following commands to install the package.

```
[root@localhost openssl 1.0.0e]# ./config
[root@localhost openssl 1.0.0e]# make
[root@localhost openssl 1.0.0e]# make install
```

You can download the LZO module online: http://www.oberhumer.com/opensource/lzo/download/. The following takes "lzo 2.02.tar.gz" as an example. Download and store it in the root directory.

To install the LZO module:

1. Open a terminal window.
2. Extract the installation package to the /etc directory.

```
[root@localhost~]# cd /etc/
[root@localhost etc]# tar zvxf /lzo 2.02.tar.gz
```

3. Enter into the extracted directory.

```
[root@localhost etc]# cd lzo 2.02
```

4. Enter the following commands to install the package.

```
[root@localhost lzo 2.02]# ./configure
[root@localhost lzo 2.02]# make
[root@localhost lzo 2.02]# make install
```

You can download the OpenVPN software online: http://openvpn.net/index.php/open source/downloads.html. Download and store it in the root directory.

To install the OpenVPN server:

1. Open a terminal window.
2. Extract the installation package to the /etc directory

```
[root@localhost~]# cd /etc/
[root@localhost etc]# tar zvxf /openvpn 2.1.4.tar.gz
```

3. Enter into the extracted directory.

```
[root@localhost etc]# cd openvpn 2.1.4
```

4. Enter the following commands to install the package.

```
[root@localhost openvpn 2.1.4]# ./configure
[root@localhost openvpn 2.1.4]# make
[root@localhost openvpn 2.1.4]# make install
```

If the header and library files are not found, you should use the following command instead of the command "./configure" mentioned above.

```
./configure prefix=/usr/local with lzo headers=/usr/local/include with lzo lib=/usr/local/lib with ssl headers=/usr/local/ir
```

5. Add the OpenVPN service.

```
[root@localhost openvpn 2.1.4]# cp p sample scripts/openvpn.init /etc/init.d/openvpn
[root@localhost openvpn 2.1.4]# chkconfig add openvpn
```

To generate certificate files for the OpenVPN server and phones:

1. Enter into the directory used to generate the certificate files (may vary between different versions).

```
[root@localhost ~]# cd /etc/openvpn 2.1.4/easy rsa/2.0
```

2. Enter the following commands.

```
[root@localhost 2.0]# export D=pwd
[root@localhost 2.0]# export KEY_CONFIG=$D/openssl.cnf
[root@localhost 2.0]# export KEY_DIR=$D/keys
[root@localhost 2.0]# export KEY_SIZE=1024
[root@localhost 2.0]# export KEY_COUNTRY=CN
[root@localhost 2.0]# export KEY_PROVINCE=FJ
[root@localhost 2.0]# export KEY_CITY=XM
[root@localhost 2.0]# export KEY_ORG="yealink.com"
[root@localhost 2.0]# export KEY_EMAIL="admin@yealink.com"
```

3. Generate a CA certificate.

```
[root@localhost 2.0]# ./clean all
[root@localhost easy rsa]# ./build ca
```

The screen prompts the following information (if you don’t want to change the default settings, press the ENTER key, else enter the desired value and then press the ENTER key):

```
Generating a 1024 bit RSA private key
.............++++++
.............................++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated into your certificate request. What you are ab
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [FJ]:
Locality Name (eg, city) [XM]:
Organization Name (eg, company) [yealink.com]:
Organizational Unit Name (eg, section) []:yealink.com
Common Name (eg, your name or your server's hostname) [yealink.com CA]:server
Name []:
Email Address [admin@yealink.com]:
```

4. Generate a certificate for the OpenVPN server.

```
[root@localhost 2.0]# ./build key server server
```

The screen prompts the following information (if you don’ t want to change the default settings, press the ENTER key, else enter the desired value and then press the ENTER key):

```
Generating a 1024-bit RSA private key
.............++++++
.............................++++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [FJ]:
Locality Name (eg, city) [XM]:
Organization Name (eg, company) [yealink.com]:
Organizational Unit Name (eg, section) []:yealink.com
Common Name (eg, your name or your server's hostname) [yealink.com CA]:server
Name []:
Email Address [admin@yealink.com]: yealink.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abcd1234
An optional company name []:yealink.com
Using configuration from /root/openvpn-2.1.4/easy rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'FJ'
localityName :PRINTABLE:'XM'
organizationName :PRINTABLE:'yealink.com' organizationalUnitName:PRINTABLE:'yealink.com'
commonName :PRINTABLE:'server'
emailAddress :IA5STRING:'yealink.com'
Certificate is to be certified until May 18 11:53:36 2023 GMT (3650 days) Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

5. Generate a certificate for the client.

```
[root@localhost 2.0]# ./build key client
```

The screen prompts the following information (if you don’ t want to change the default settings, press the ENTER key, else enter the desired value and then press the ENTER key):

```
Generating a 1024 bit RSA private key
.............++++++
.............................++++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [FJ]:
Locality Name (eg, city) [XM]:
Organization Name (eg, company) [yealink.com]:
Organizational Unit Name (eg, section) []:yealink.com
Common Name (eg, your name or your server's hostname) [yealink.com CA]:server
Name []:
Email Address [admin@yealink.com]:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abcd1234
An optional company name []:yealink.com
Using configuration from /root/openvpn-2.1.4/easy rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'FJ'
localityName :PRINTABLE:'XM'
organizationName :PRINTABLE:'yealink.com' organizationalUnitName:PRINTABLE:'yealink.com'
commonName :PRINTABLE:'server'
emailAddress :IA5STRING:'yealink.com'
Certificate is to be certified until May 18 11:53:36 2023 GMT (3650 days) Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

6. Generate a dh1024.pem file for the server.

```
[root@localhost 2.0]# ./build dh
```

The screen prompts the following information:

```
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
```

If the screen prompts "./build dh: line 7: dhparam: command not found", you need to edit the file "build dh" in the /etc/openvpn 2.1.4/easy rsa/2.0 directory. Set "$OPENSSL" to "openssl" and save the file.

All the certificate files are generated in the directory "/openvpn 2.1.4/easy rsa/2.0/keys".

To configure the server's configuration file:

1. Create a new directory "openvpn" located in the path /etc.

```
[root@localhost ~]# mkdir /etc/openvpn
```

2. Create a new directory "keys" located in the path /etc/openvpn.

```
[root@localhost ~]# mkdir /etc/openvpn/keys
```

3. Enter into the installation directory of the OpenVPN server.

```
[root@localhost ~]# cd /etc/openvpn 2.1.4
```

4. Copy the certificate files required for the server to the directory "keys" created above.

```
[root@localhost openvpn 2.1.4]# cp easy rsa/2.0/keys/ca.crt /etc/openvpn/keys/
[root@localhost openvpn 2.1.4]# cp easy rsa/2.0/keys/dh1024.pem /etc/openvpn/keys/
[root@localhost openvpn 2.1.4]# cp easy rsa/2.0/keys/server.crt /etc/openvpn/keys/
[root@localhost openvpn 2.1.4]# cp easy rsa/2.0/keys/server.key /etc/openvpn/keys/
```

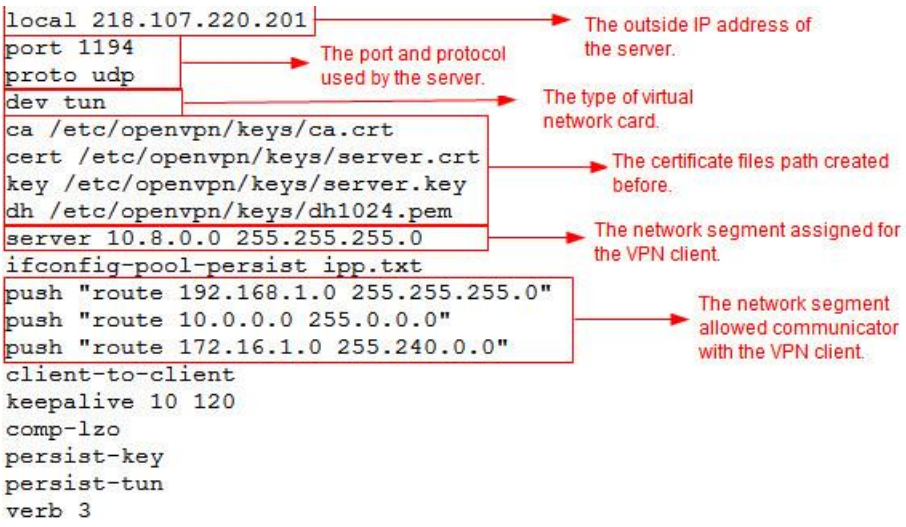
5. Copy the file "server.conf" in the sample config files directory to the directory "openvpn" created above.

```
[root@localhost openvpn 2.1.4]# cp sample config files/server.conf /etc/openvpn
```

6. Edit the file “server.conf” according to your actual network environment and save the change.

```
[root@localhost ~]# vi /etc/openvpn/server.conf
```

Press the “I” key to enter into the Insert Mode and modify the desired parameters, and then press the “Esc” key to return to the Command Mode and enter “wq!”.
The following shows an example:



According to the actual network environment, configure the network settings of the server, such as the TCP/IP forwarding feature and routing entries between the VPN clients and the Intranet.
For more information, contact your network administrator.

To enable the TCP/IP forwarding:

1. Open a terminal window.
2. Edit the file “sysctl.conf” in the /etc directory and save the change.

```
[root@localhost ~]# vi /etc/sysctl.conf
```

Press the “I” key to enter into the Insert Mode and Set “**net.ipv4.ip_forward**” to 1, and then press the “Esc” key to return to the Command Mode and enter “wq!”.

To start the OpenVPN service:

1. Enter into the installation directory of the OpenVPN server.

```
[root@localhost ~]# cd /etc/openvpn 2.1.4
```

2. Start the OpenVPN service.

```
[root@localhost openvpn 2.1.4]# service openvpn start
```

Create the OpenVPN TAR File for the VPN Client

OpenVPN requires using certificates to help establish the authenticity of clients connecting to an OpenVPN server. You need to obtain the files: ca.crt, client.crt, client.key, and vpn.cnf from the system, and then package these files

to TAR format.

To configure the client’s configuration file:

1. Create a new directory ”client” located in the path /etc/openvpn.

```
[root@localhost ~]# mkdir /etc/openvpn/client
```

2. Create a new directory ”keys” located in the path /etc/openvpn/client.

```
[root@localhost ~]# mkdir /etc/openvpn/client/keys
```

3. Enter into the installation directory of the OpenVPN server.

```
[root@localhost ~]# cd /etc/openvpn 2.1.4
```

4. Copy the certificate files required for the client to the directory “/etc/openvpn/client/keys” created before.

```
[root@localhost openvpn 2.1.4]# cp easy rsa/2.0/keys/ca.crt /etc/openvpn/client/keys/
[root@localhost openvpn 2.1.4]# cp easy rsa/2.0/keys/client.crt /etc/openvpn/client/keys/
[root@localhost openvpn 2.1.4]# cp easy rsa/2.0/keys/client.key /etc/openvpn/client/keys/
```

5. Copy the file “client.conf” in the sample config files directory to the directory “client” created above and rename it to vpn.cnf.

```
[root@localhost openvpn 2.1.4]# cp sample config files/client.conf /etc/openvpn/client/vpn.cnf
```

6. Edit the file “vpn.cnf” and save the change.

```
[root@localhost openvpn 2.1.4]# cd /etc/openvpn/client
[root@localhost client]# vi vpn.cnf
```

Press the “I” key to enter into the Insert Mode and modify the desired parameters, and then press the “Esc” key to return to the Command Mode and enter “wq!”.

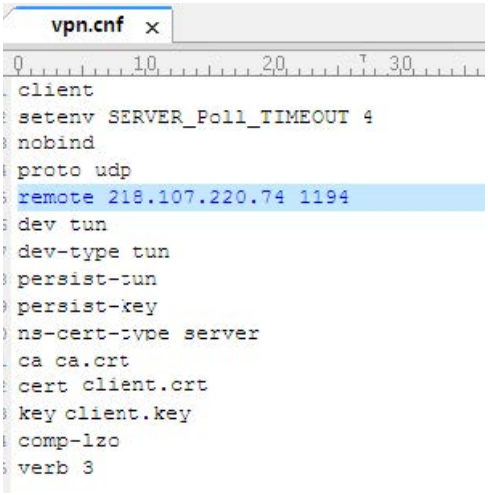
The following parameters should be configured as the same as that of the server.

```
remote 218.107.220.201 1194 udp
dev tun
dev type tun
```

The following defines the OpenVPN certificates and key for Yealink phones:

```
ca ca.crt
cert client.crt
key client.key
```

The following figure shows a portion of the vpn.cnf file for reference:



To package the TAR file on the Linux platform:

1. Enter the following commands to package the TAR file.

```
[root@localhost ~]# cd /etc/openvpn/client
[root@localhost client]# tar cvpf openvpn.tar *
```

An openvpn.tar file is generated in the client directory.

Windows Platform

Install and Configure the OpenVPN Server

The OpenVPN server software is available for free. You can download it for your Windows platform online.
This section provides you on how to install the OpenVPN server (e.g., openvpn 2.1.1 install.exe) on the Windows XP platform.
Before the installation, make sure the hardware and system meet the following requirements:

- Dual network cards.
- The system kernel supports the TUN/TAP module.

To install the OpenVPN server on the Windows XP platform:

1. Double-click the installation file on the local system.
2. Follow the prompts to finish the installation.
   The default installation directory is C:\Program Files\OpenVPN.

To generate certificate files for the OpenVPN server and phones:

1. Enter into the installation directory of the OpenVPN server.
2. Open the file vars.bat in the easy rsa folder and edit the following parameters:

```
set KEY_COUNTRY=US
set KEY_PROVINCE=CA
set KEY_CITY=SanFrancisco
set KEY_ORG=OpenVPN
set KEY_EMAIL=mail@host.domain
```

The following shows an example of configuring these parameters:

```
set KEY_COUNTRY=CN
set KEY_PROVINCE=FJ
set KEY_CITY=XM
set KEY_ORG=Yealink
set KEY_EMAIL=admin@yealink.com
```

3. Click **Start**–>**Run**.
4. Enter **cmd** in the pop-up dialogue box and click **OK** to open a command prompt screen.
5. Enter into the directory easy rsa located in the installation directory of the OpenVPN server.

```
C:\Documents and Settings\Administrator>cd \Program Files\OpenVPN\easy rsa
```

6. Enter the following commands.

```
C:\Program Files\OpenVPN\easy rsa>init config.bat
C:\Program Files\OpenVPN\easy rsa>vars
C:\Program Files\OpenVPN\easy rsa>clean all.bat
```

7. Generate a CA certificate.

```
C:\Program Files\OpenVPN\easy rsa>build ca.bat
```

The screen prompts the following information (if you don’ t want to change the default settings, press the ENTER key, else enter the desired value and then press the ENTER key):

```
Loading 'screen' into random state done
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [FJ]:
Locality Name (eg, city) [XM]:
Organization Name (eg, company) [Yealink]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []: CA
Email Address [admin@yealink.com]:
```

8. **Generate a dh1024.pem file for the server.**

```
C:\Program Files\OpenVPN\easy rsa>build dh.bat
```

The screen prompts the following information:

```
Loading 'screen' into random state done
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
```

9. **Generate a certificate for the OpenVPN server.**

```
C:\Program Files\OpenVPN\easy rsa>build key server.bat server
```

The screen prompts the following information (if you don’ t want to change the default settings, press the ENTER key, else enter the desired value and then press the ENTER key):

```
Loading 'screen' into random state done
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'keys\server.key'
-----
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [FJ]:
Locality Name (eg, city) [XM]:
Organization Name (eg, company) [Yealink]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []: Server
Email Address [admin@yealink.com]:
Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:serverpwd
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state-done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'FJ'
localityName :PRINTABLE:'XM'
organizationName :PRINTABLE:'Yealink'
organizationalUnitName:PRINTABLE:'EMB'
commonName :PRINTABLE:'Server'
emailAddress :IA5STRING:'admin@yealink.com'
Certificate is to be certified until Jan 20 13:10:22 2023 GMT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

10. Generate a certificate for the client.

```
C:\Program Files\OpenVPN\easy rsa>build key.bat client
```

The screen prompts the following information (if you don’t want to change the default settings, press the ENTER key, else enter the desired value and then press the ENTER key):

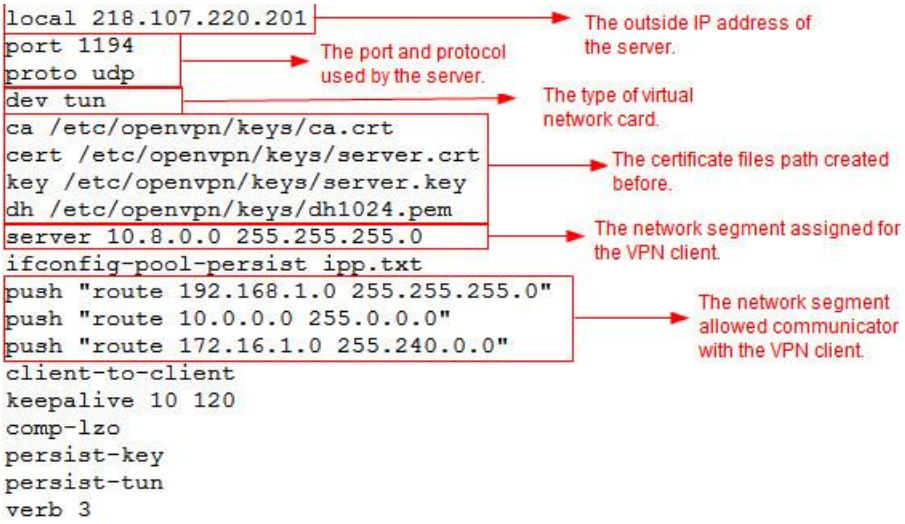
```
Loading 'screen' into random state done
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'keys\Client.key'
-----
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [FJ]:
Locality Name (eg, city) [XM]:
Organization Name (eg, company) [Yealink]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []: Client
Email Address [admin@yealink.com]:
Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:clientpwd
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state-done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'FJ'
localityName :PRINTABLE:'XM'
organizationName :PRINTABLE:'Yealink'
organizationalUnitName:PRINTABLE:'EMB'
commonName :PRINTABLE:'Client'
emailAddress :IA5STRING:'admin@yealink.com'
Certificate is to be certified until Jan 20 13:10:22 2023 GMT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

To configure the server’s configuration file:

1. Enter the installation directory of the OpenVPN server.
2. Create a new folder “serverconfig” in the directory.
3. Copy the file “server.ovpn” in the sample config folder to the serverconfig folder created above.

4. Edit the file "server.ovpn" according to your actual network environment and save the change.

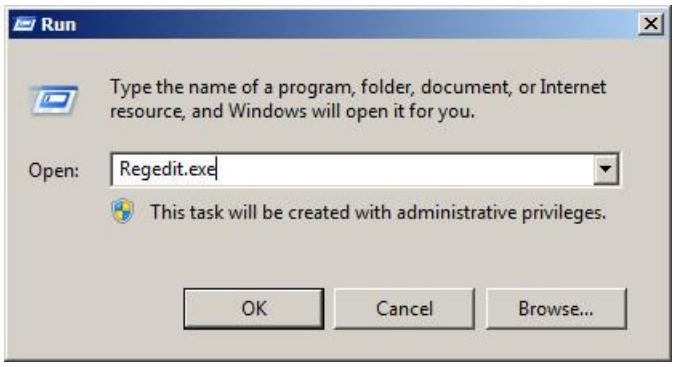
   The following shows an example:



   According to the actual network environment, configure the network settings of the server, such as the TCP/IP forwarding feature, Internet connection sharing feature and routing entries between the VPN clients and the Intranet. For more information, contact your network administrator.

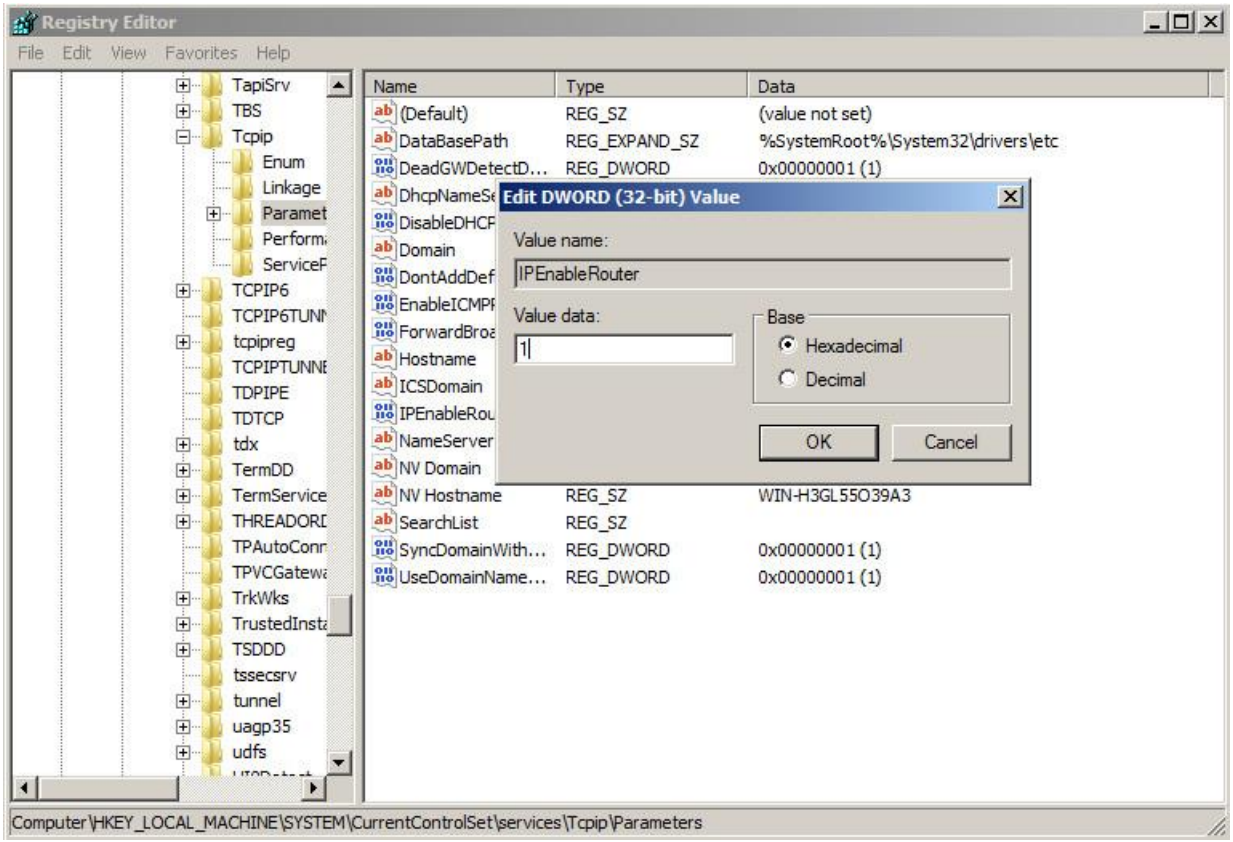
To enable the TCP/IP forwarding:

1. Click **Start**->**Run**.
2. Enter **Regedit.exe** in the pop up dialogue box and click **OK**.



3. Click **HKEY_LOCAL_MACHINE**->**SYSTEM**->**CurrentControlSet**->**Services**->**Tcpip**->**Parameters**.

4. Set **"IPEnableRouter"** to 1.



To enable Internet connection sharing for inside network card:

1. Open network connections.
2. Right click the local area network for the inside network card and select **Properties**.
3. On the **Advanced** tab, check the **Allow other network users to connect through this computer's Internet connection** check box.
4. Select the virtual network card of the server from the **Home networking connection** drop down menu.
5. Click **OK** to save the change.

Create the OpenVPN Tar File for the VPN Client

You can package the TAR file on the Windows platform using the tool 7 Zip or GnuWin32. You can download 7 Zip online: http://www.7 zip.org/ and GnuWin32 online: http://gnuwin32.sourceforge.net/packages/gtar.htm.
This section provides you on how to package the TAR file using 7 Zip on the Windows XP platform.

To configure the client' s configuration file:

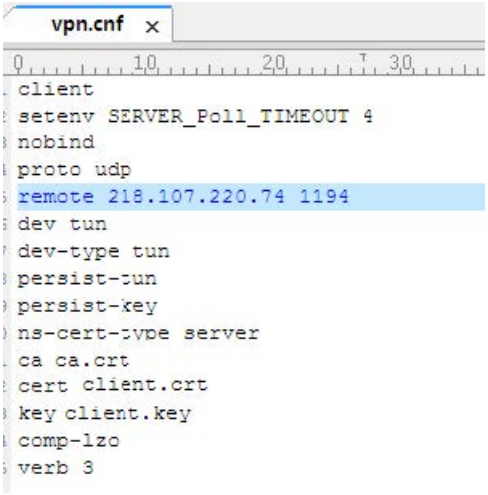
1. Create a new folder "openvpn" in the directory C:/.
2. Copy the file client.ovpn in the sample config folder to the openvpn folder.
3. Rename the file client.ovpn to vpn.cnf.
4. Create a new folder "keys" in the openvpn folder.
5. Copy ca.crt, client.crt and client.key files to the keys folder created above.

6. Edit the file vpn.cnf.

   The following parameters should be configured as the same as that of the server.

```
remote 218.107.220.201 1194 udp
dev tun
dev type tun
The following defines the OpenVPN certificates and key for Yealink phones:
ca ca.crt
cert client.crt
key client.key
```

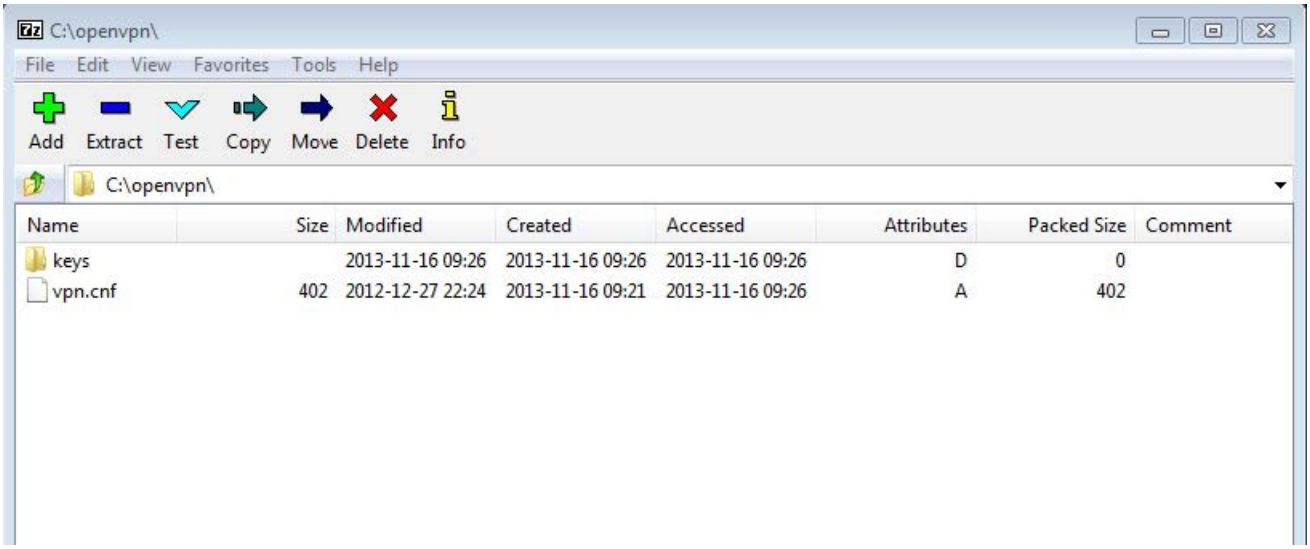
   The following figure shows a portion of the vpn.cnf file for reference:



7. Save the change.

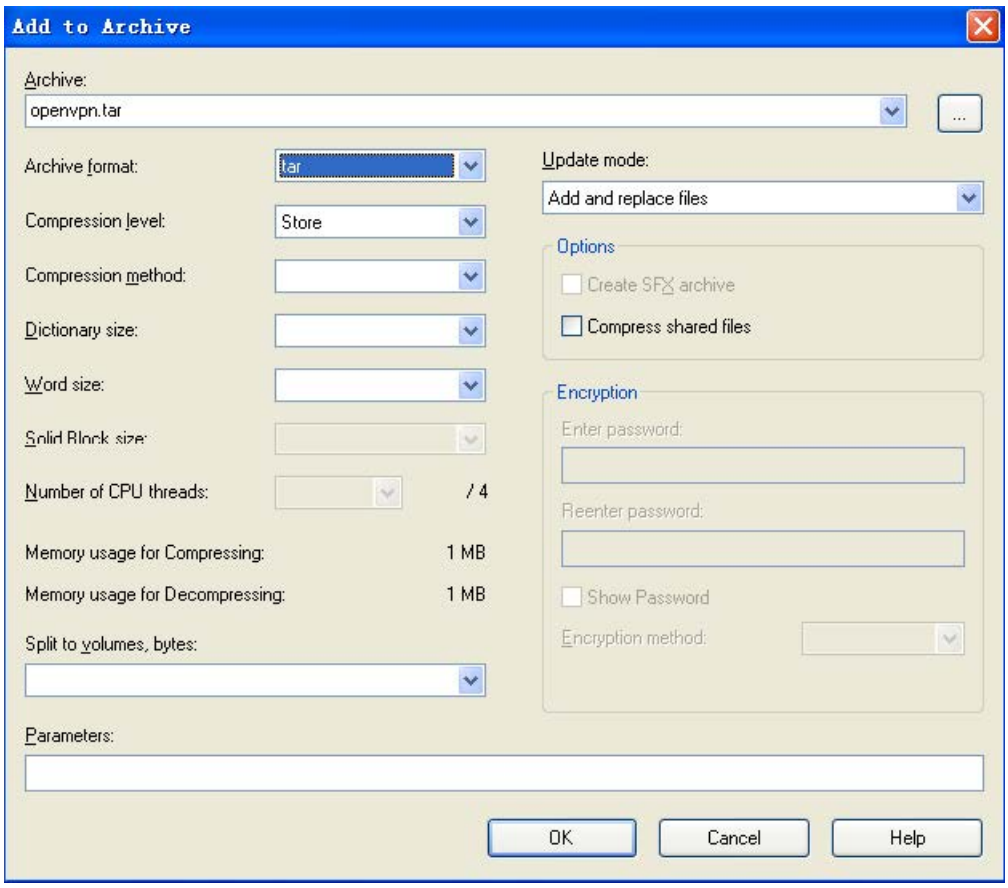
To package a TAR file using the tool 7-Zip on the Windows platform:

1. Download and install 7-Zip on the local system.
2. Start the 7-Zip file manager application.
3. Locate the openvpn folder from the local system.



4. Click the **Add** button.

5. Select tar from the Archive format drop down menu.



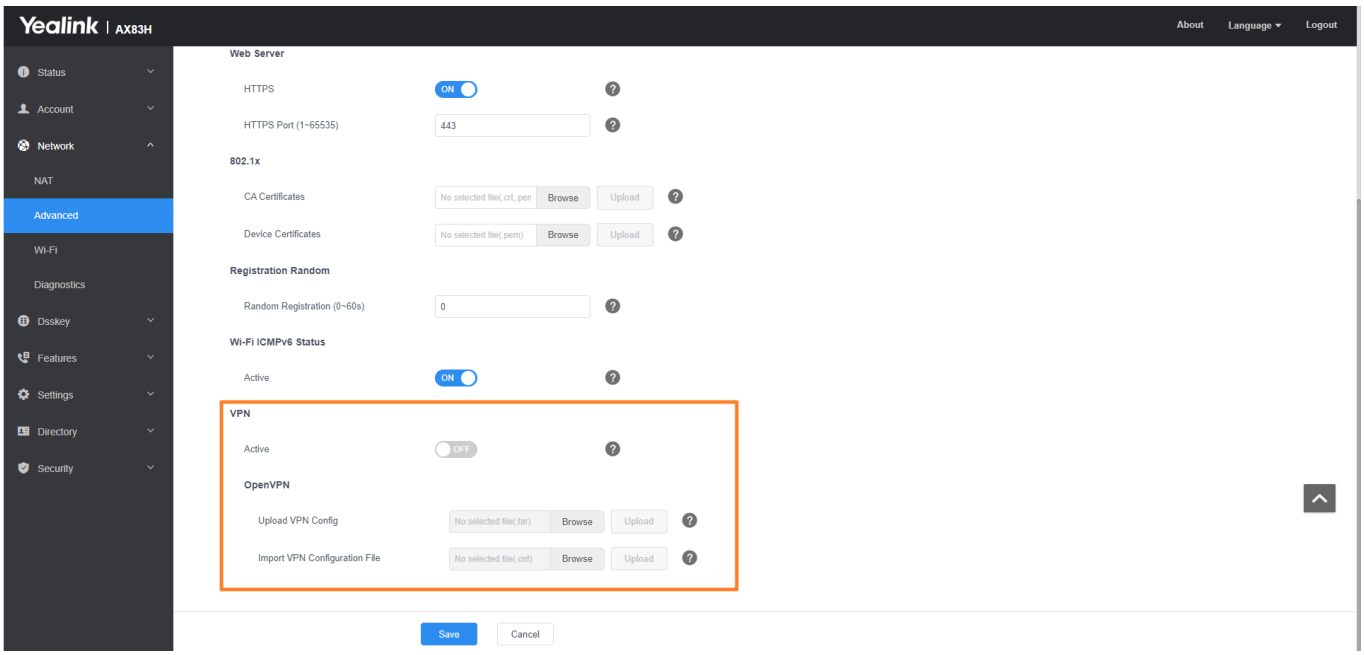
6. Click the **OK** button.
   An openvpn.tar file is generated in the directory C:/openvpn.

Configure OpenVPN Feature on Phones

OpenVPN feature is disabled on 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 phones.

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
static.network.openvpn_file.url
```

Parameter	Permitted Values	Default	Description
static.network.vpn_enable[1]	**0**-Disabled **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.
static.network.openvpn_file.url	String within 512 characters	Blank	It configures the URL for uploading the OpenVPN configuration file (vpn.cnf). **NOTE** It works only if `static.network.vpn.mode` is set to 1 (OpenVPN).

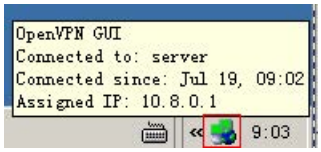
[1]If you change this parameter, the phone will reboot to make the change take effect.

Troubleshooting

Why does the phone fail to connect to the OpenVPN server?

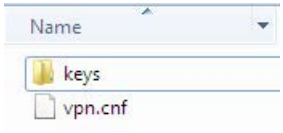
Do the following in sequence:

1. Ensure that the OpenVPN server is up and running.
   If the OpenVPN server is running properly, a virtual IP address assigning to the OpenVPN server will appear when you hover your mouse pointer over the VPN icon. The VPN icon in the notification area of the system tray is shown as below:



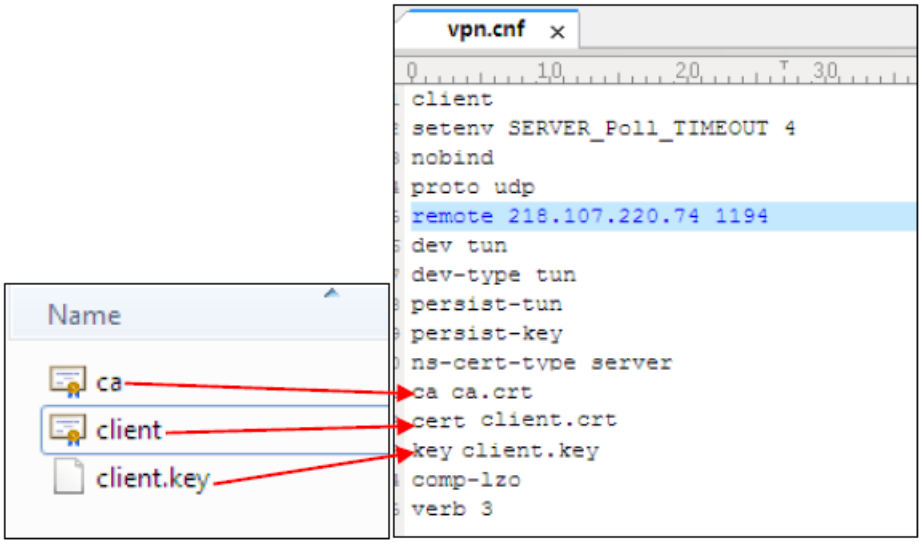
2. Ensure that the OpenVPN TAR file uploaded to the phone is correctly created.

   Extract the TAR file and ensure that the certificate folder is named as "keys" and the client configuration file is named as "vpn.cnf", as shown below:

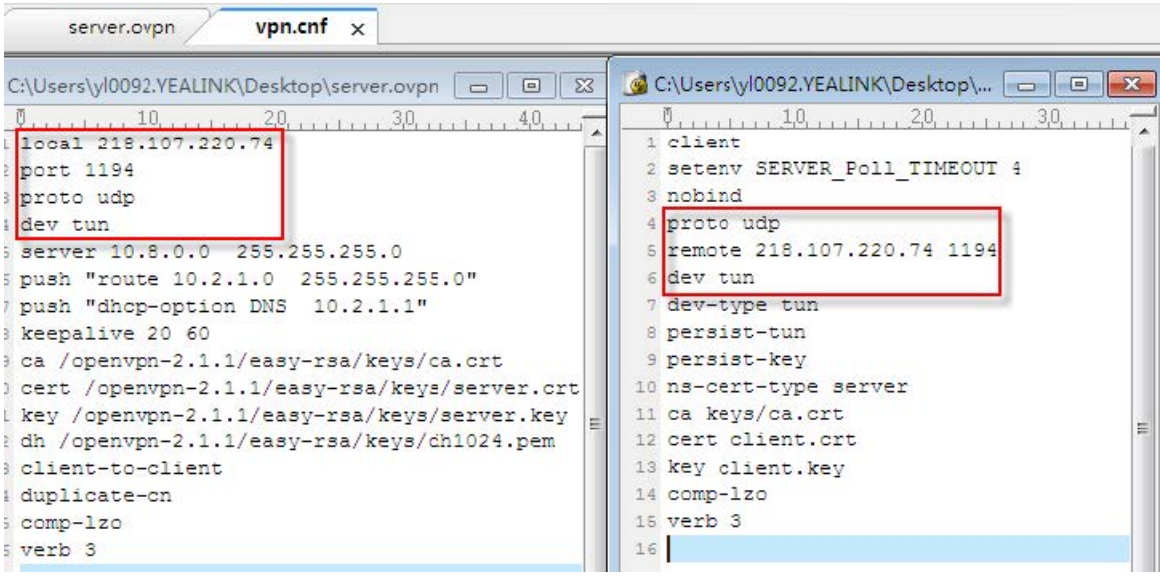


3. Ensure that the file names of the client certificates and key defined in the client configuration file are correct.

   Enter the "keys" directory to check the file names of client certificates and key.



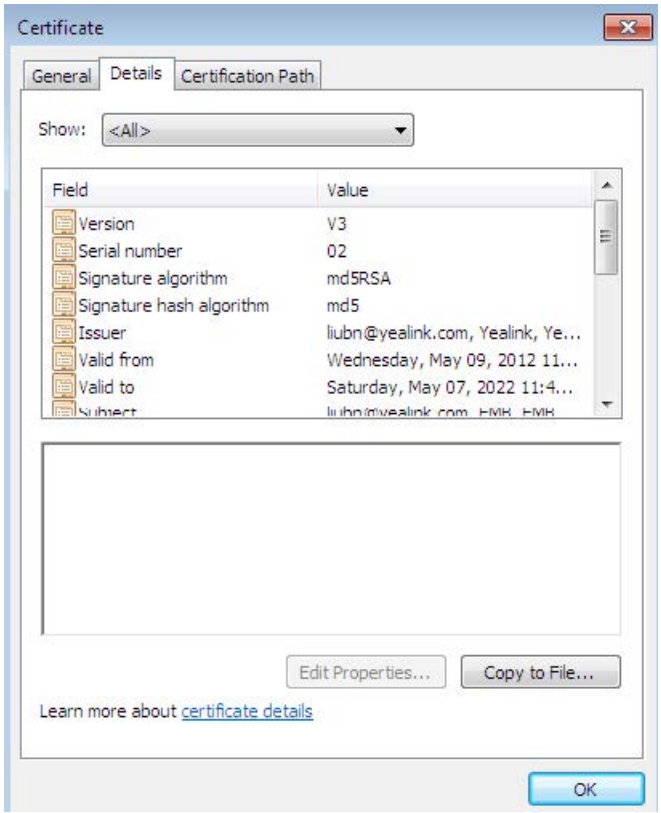
4. Ensure that the following configurations in the server configuration file and client configuration file are exactly matched.



5. Ensure that the time and date on the phone is within the validity time of the certificate.

6. Check if the signature algorithm of the client certificate is supported by the phone.

   Phones support MD5 and SHA 1 signature algorithms.
   Double click the client certificate file to check the validity time and signature algorithm of the certificate.



How to change the signature algorithm of the certificate?

If the signature algorithm of the client certificate is not supported by phones, you need to change the signature

algorithm and then re generate the client certificate.

Do the following:

1. Find the openssl.cnf file located in the folder easy rsa of the OpenVPN installation path.
   The file name and storage path may vary in your installation environment.
2. Configure the value of the parameter `default_md` to be md5 or sha1, as shown below:
   default_md = md5 or default_md = sha1
3. Re generate a client certificate following the steps introduced in the section Installing the OpenVPN Server.

Why does the phone fail to register to the SIP server after successfully connecting to the OpenVPN server?

Do the following in sequence:

1. Ensure that the OpenVPN server has dual network cards.
2. Ensure that the connection between the OpenVPN server and the SIP server is working correctly by the Ping command.
3. Ensure that Internet Connection Sharing and TCP/IP forwarding are enabled on the OpenVPN server on the Windows platform.
4. Ensure that access permission of the SIP server network segment has been assigned to the phone in the server configuration file.
   For example, the IP address of the SIP server is 192.168.3.6, the server configuration file must contain the configuration **push "route 192.168.3.0 255.255.255.0"**.

Why does the phone fail to register when the domain name of the SIP server is configured on the phone?

Do the following in sequence:

1. Ensure that the IP address of the DNS server has been added to the server configuration file.
   For example, the IP address of the DNS server is 192.1682.3.10, the server configuration file must contain the configuration **push "dhcp option DNS 192.1682.3.10"**.
2. Ensure that the connection between the DNS server and the phone is working correctly.

Why there is no sound during a call?

Do the following:

1. Ensure that the configuration **client-to-client** has been added to the server configuration file.
2. Reboot the OpenVPN server.

Why the voice quality is poor?

Do the following:

1. Network congestion, RTP packet loss or delay may result in poor call quality. In this case, you need to contact your network administrator.
2. Ensure that an appropriate log level is set in the client configuration file.
   Yealink recommends you to set the log level to 3 ("verb 3" in the client configuration file). If the log level is set too high, the phone will log phone events frequently. This may cause phone performance issues.

Example Configuration Files

The following lists example configuration files detailing how to configure the server and client configuration files.

Configurations may vary between different network environments.

Server Configuration File

```
local 218.107.220.74      #Outside IP address of the VPN server
port 1194                 #Port of the VPN server
proto udp                 #Transport protocol (udp or tcp) of the VPN server
dev tun                   #Virtual network interface (tun or tap)
server 10.8.0.0  255.255.255.0     #Virtual IP segment assigned to VPN clients
push "route 10.2.1.0  255.255.255.0"  # Inside network segment allowed to #be
                                      accessed by VPN clients
push "dhcp-option DNS  10.2.1.1"      #IP address of the DNS server #assigned
                                      to the VPN clients.
keepalive 20 60    #Ping the VPN server every 20 seconds. If the ping is not
                   #successfully within 60 seconds, reconnect the VPN server.
ca /openvpn-2.1.1/easy-rsa/keys/ca.crt          #CA certificate
cert /openvpn-2.1.1/easy-rsa/keys/server.crt    #Server certificate
key /openvpn-2.1.1/easy-rsa/keys/server.key     #Private key of the server
dh /openvpn-2.1.1/easy-rsa/keys/dh1024.pem
client-to-client      #Allow the connected VPN clients to communicate #directly,
                      rather than forwarding data by the VPN server.
duplicate-cn          #Allow VPN clients to use the same certificate to connect #the
                      VPN server.
comp-lzo              #Enable data compression
verb 3                #Log level
```

Client Configuration File

```
client
setenv SERVER_Poll_TIMEOUT 4
nobind
proto udp                          #Transport protocol (udp or tcp) of the VPN server
remote 218.107.220.74 1194         #Outside IP address and port of the VPN server
dev tun                            #Virtual network interface (tun or tap)
dev-type tun
persist-tun
persist-key
ns-cert-type server
ca ca.crt          #CA certificate
cert client.crt    #Client certificate
key client.key     #Private key of the client
verb 3                                    #Log level
comp-lzo
verb 3
```

Quality of Service (QoS)

Introduction

VoIP is extremely bandwidth and delay-sensitive. QoS is a major issue in VoIP implementations, regarding how to guarantee that packet traffic is not delayed or dropped due to interference from other lower priority traffic. VoIP can guarantee high-quality QoS only if the voice and the SIP packets are given priority over other kinds of network traffic. The phones support the DiffServ model of QoS.

Voice QoS

In order to make VoIP transmissions intelligible to receivers, voice packets should not be dropped, excessively delayed, or made to suffer varying delay. DiffServ model can guarantee high-quality voice transmission when the voice packets are configured to a higher DSCP value.

SIP QoS

The SIP protocol is used for creating, modifying, and terminating two-party or multi-party sessions. To ensure good voice quality, SIP packets emanated from the phones should be configured with a high transmission priority. DSCPs for voice and SIP packets can be specified respectively.

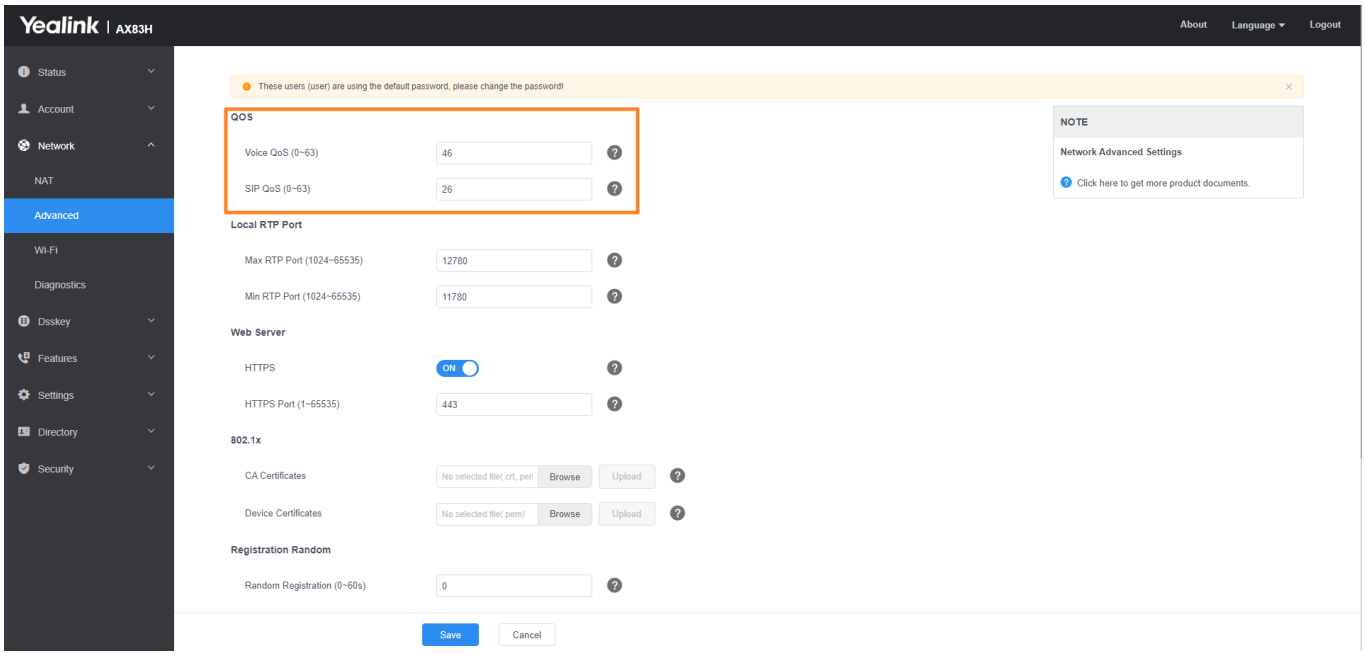
NOTE

For voice and SIP packets, the phone obtains DSCP info from the network policy if LLDP feature is enabled, which takes precedence over manual settings. For more information on LLDP, refer to LLDP Configuration.

Voice and SIP QoS Configuration

Set via the Web User Interface

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



Configuration Parameter

static.network.qos.audiotos
static.network.qos.signaltos

Parameter	Permitted Values	Default	Description
static.network.qos.audiotos[1]	Integer from 0 to 63	46	It configures the DSCP (Differentiated Services Code Point) for voice packets. The default DSCP value for RTP packets is 46 (Expedited Forwarding).
static.network.qos.signaltos[1]	Integer from 0 to 63	26	It configures the DSCP (Differentiated Services Code Point) for SIP packets. The default DSCP value for SIP packets is 26 (Assured Forwarding).

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

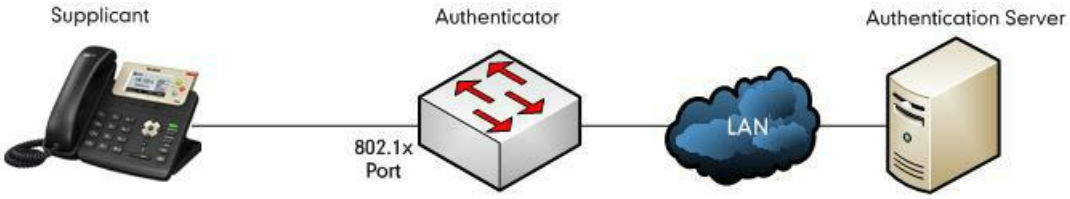
802.1x Authentication

About 802.1X

Introduction

The IEEE 802.1X standard defines a Port-based Network Access Control (PNAC) and authentication protocol that restricts unauthorized clients from connecting to a LAN. The IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) defined in RFC3748 which is known as “EAP over LAN” or EAPOL.

802.1x Components



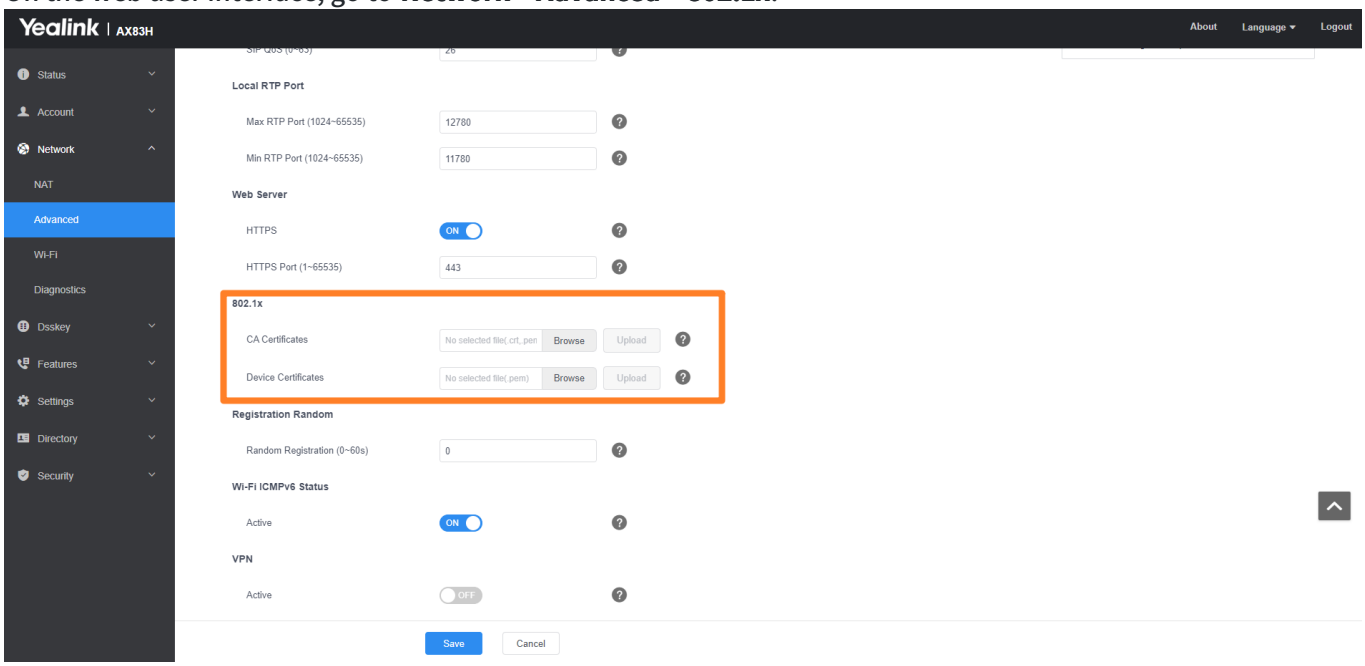
- **Supplicant**: The supplicant is a client device (such as an IP phone) that wishes to attach to the network.
- **Authenticator**: The authenticator is a network device, such as an Ethernet switch.
- **Authentication server**: The authentication server is typically a host running software supporting the RADIUS and EAP protocols.

802.1X Authentication Configuration

The configuration can be done either using the webGUI or Configuration Parameter.

Set via the Web User Interface

1. On the web user interface, go to **Network** > **Advanced** > **802.1x**.



Configuration Parameter

```
static.network.802_1x.root_cert_url
static.network.802_1x.client_cert_url
```

Parameter	Permitted Values	Default	Description
static.network.802_1x.root_cert_url	URL within 511 characters	Blank	It configures the URL for uploading the 802.1x CA certificate. The format of the certificate must be *.pem, *.crt, *.cer or *.der. **NOTE** It works only if static.network.802_1x.mode is set to 2, 3, 4, 5, 6 or 7. If the authentication method is EAP-FAST, you also need to set static.network.802_1x.eap_fast_provision_mode to 1 (Authenticated Provisioning).
static.network.802_1x.client_cert_url	URL within 511 characters	Blank	It configures the URL for uploading the 802.1x client certificate. The format of the certificate must be *.pem. **NOTE** It works only if static.network.802_1x.mode is set to 2 (EAP-TLS).

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

802.1X Authentication Flow

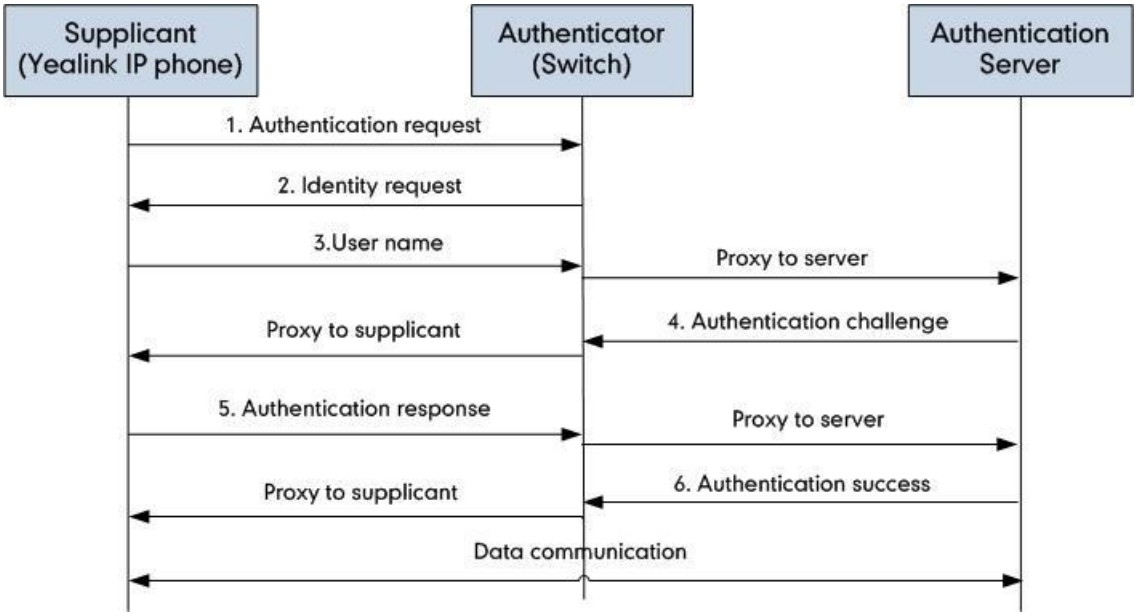
Reboot the phone to activate the 802.1X authentication on the phone. The 802.1X authentication process is divided into two basic stages:

Pre-authentication

The 802.1X pre-authentication process begins with the IP phone that contains a supplicant service used for negotiation and authentication. When the IP phone connects to an unauthorized port, the authenticator blocks the IP phone from connecting to the network. Using one of the authentication protocols, the authenticator establishes a security negotiation with the IP phone and creates an 802.1X session. The IP phone provides its authentication information for the authenticator, and then the authenticator forwards the information to the authentication server.

Authentication

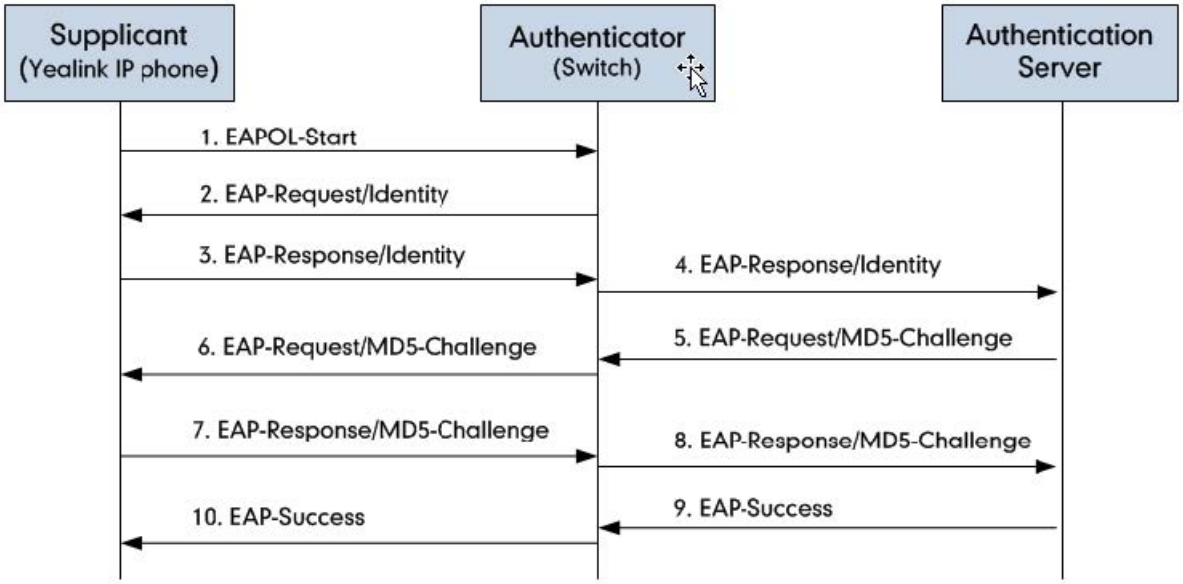
After the authentication server authenticates the IP phone, the authentication server initiates the authentication stage of the process. During this phase, the authenticator facilitates an exchange of keys between the IP phone and the authentication server. After these keys are established, the authenticator grants the IP phone access to the protected network on an authorized port. The following figure summarizes the implementation of the 802.1X authentication process using a RADIUS server as the authentication server:



Authentication Process Using EAP-MD5 Protocol

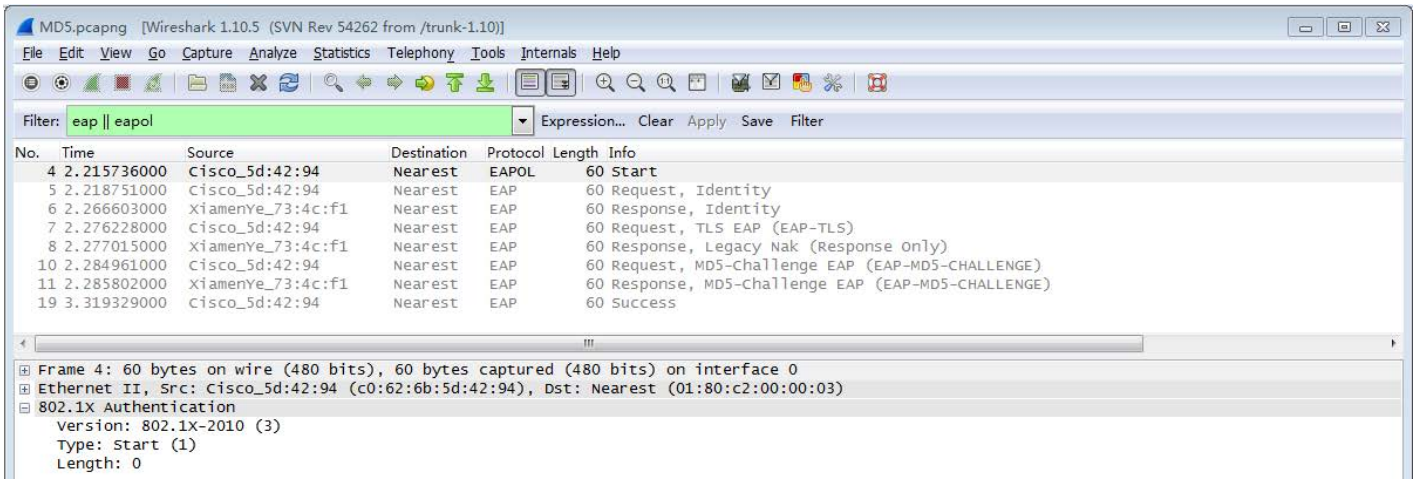
Authentication Process

The following figure illustrates the scenario of a successful 802.1X authentication process using the EAP-MD5 protocol.



1. The supplicant sends an “EAPOL-Start” packet to the authenticator.
2. The authenticator responds with an “EAP-Request/Identity” packet to the supplicant.
3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
4. The authenticator strips the Ethernet header and encapsulates the remaining EAP frame in the RADIUS format, and then sends it to the authentication server.
5. The authentication server recognizes the packet as an EAP-MD5 type and sends back a Challenge message to the authenticator.
6. The authenticator strips the authentication server’ s frame header, encapsulates the remaining EAP frame into the EAPOL format, and sends it to the supplicant.
7. The supplicant responds to the Challenge message.
8. The authenticator passes the response to the authentication server.
9. The authentication server validates the authentication information and sends an authentication success message.
10. The authenticator passes the successful message to the supplicant. After the supplicant is authenticated successfully, the authenticator provides network access permissions. If the supplicant does not provide proper identification, the
authentication server responds with a rejection message. The authenticator passes the message onto the supplicant and blocks access to the LAN. If the supplicant is disabled or reset after successful authentication, the supplicant sends an EAPOL-Logoff message, which prompts the authenticator to block access to the LAN.

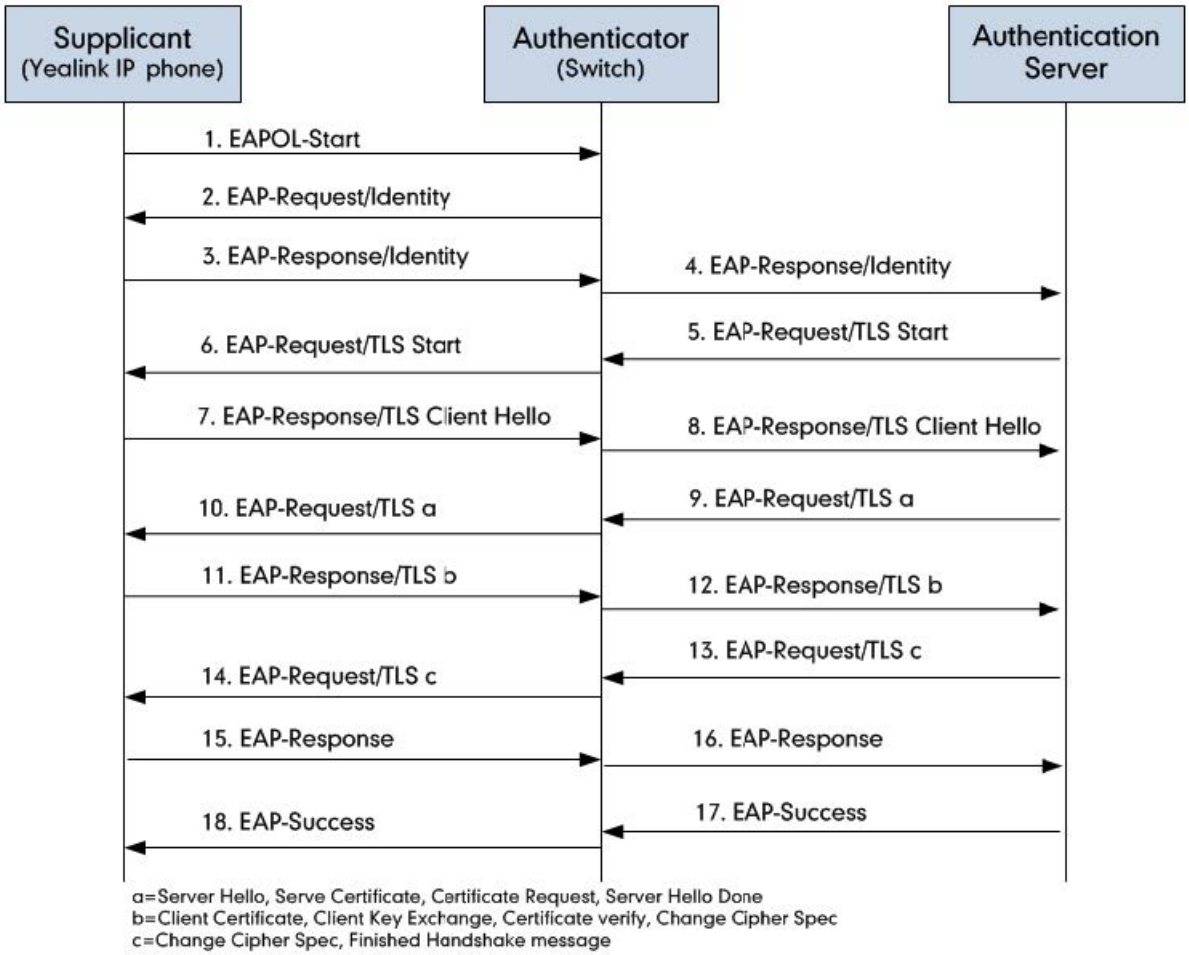
Sample Screenshot



Authentication Process Using EAP-TLS Protocol

Authentication Process

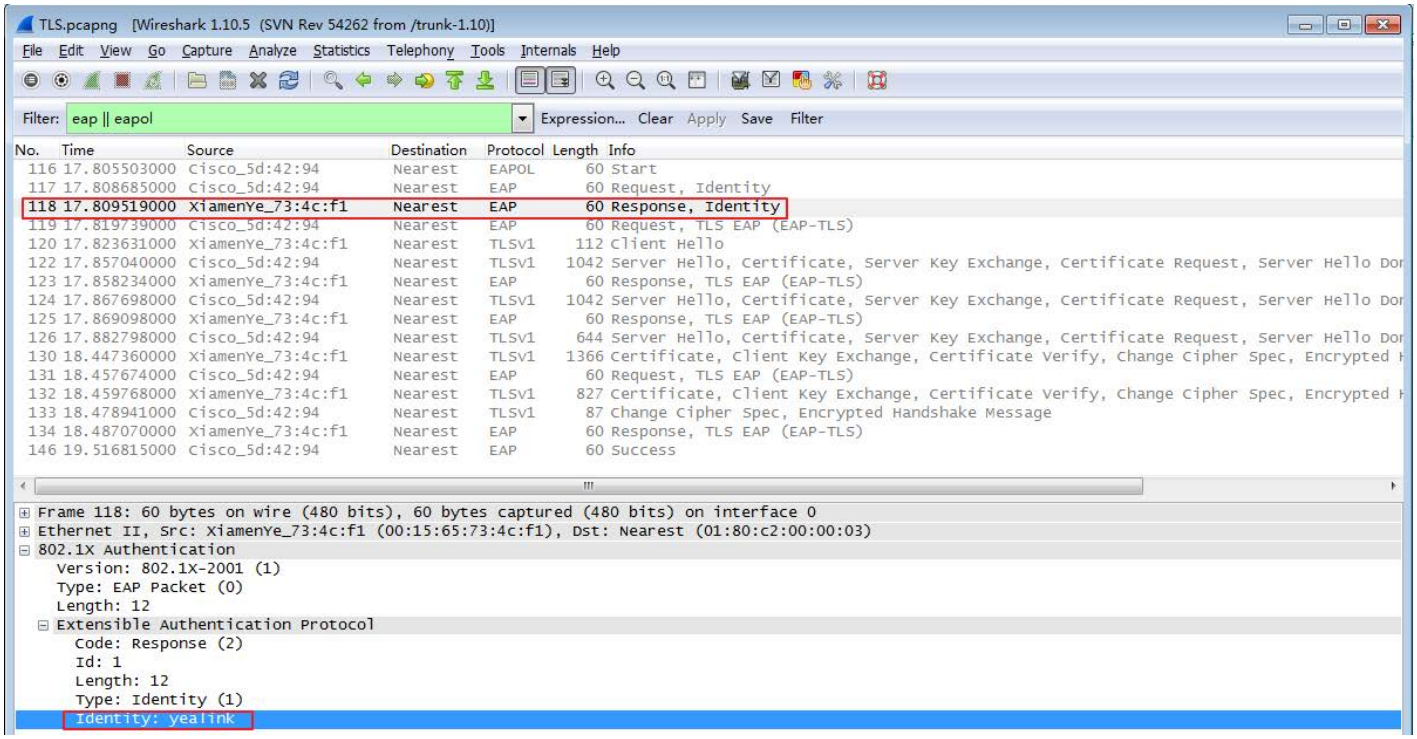
The following figure illustrates the scenario of a successful 802.1X authentication process using the EAP-TLS protocol.



1. The supplicant sends an “EAPOL-Start” packet to the authenticator.
2. The authenticator responds with an “EAP-Request/Identity” packet to the supplicant.
3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
4. The authenticator strips the Ethernet header encapsulates the remaining EAP frame in the RADIUS format, and then sends it to the authentication server.
5. The authentication server recognizes the packet as an EAP-TLS type and sends an “EAP-Request” packet with a TLS start message to the authenticator.
6. The authenticator strips the authentication server’s frame header, encapsulates the remaining EAP frame in the EAPOL format, and then sends it to the supplicant.
7. The supplicant responds with an “EAP-Response” packet containing a TLS client hello handshake message to the authenticator. The client hello message includes the TLS version supported by the supplicant, a session ID, a random number and a set of cipher suites.
8. The authenticator passes the response to the authentication server.
9. The authentication server sends an “EAP-Request” packet to the authenticator. The packet includes a TLS server hello handshake message, a server certificate message, a certificate request message, and a server hello done message.
10. The authenticator passes the request to the supplicant.

11. The supplicant responds with an "EAP-Response" packet to the authenticator. The packet includes a TLS change cipher spec message, a client certificate message, a client key exchange message, and a certificate verify message.
12. The authenticator passes the response to the authentication server.
13. The authentication server sends an "EAP-Request" packet to the authenticator. The packet includes a TLS change cipher spec message and a finished handshake message. The change cipher spec message is sent to notify the authenticator that subsequent records will be protected under the newly negotiated cipher spec.
14. The authenticator passes the request to the supplicant.
15. The supplicant responds with an "EAP-Response" packet to the authenticator.
16. The authenticator passes the response to the authentication server.
17. The authentication server responds with a success message indicating the supplicant and the authentication server have successfully authenticated each other.
18. The authenticator passes the message to the supplicant. After the supplicant is authenticated successfully, the authenticator provides network access permissions. If the supplicant does not provide proper identification, the authentication server responds with a rejection message. The authenticator passes the message to the supplicant and blocks access to the LAN. If the supplicant is disabled or reset after successful authentication, the supplicant sends an EAPOL-Logoff message, which prompts the authenticator to block access to the LAN.

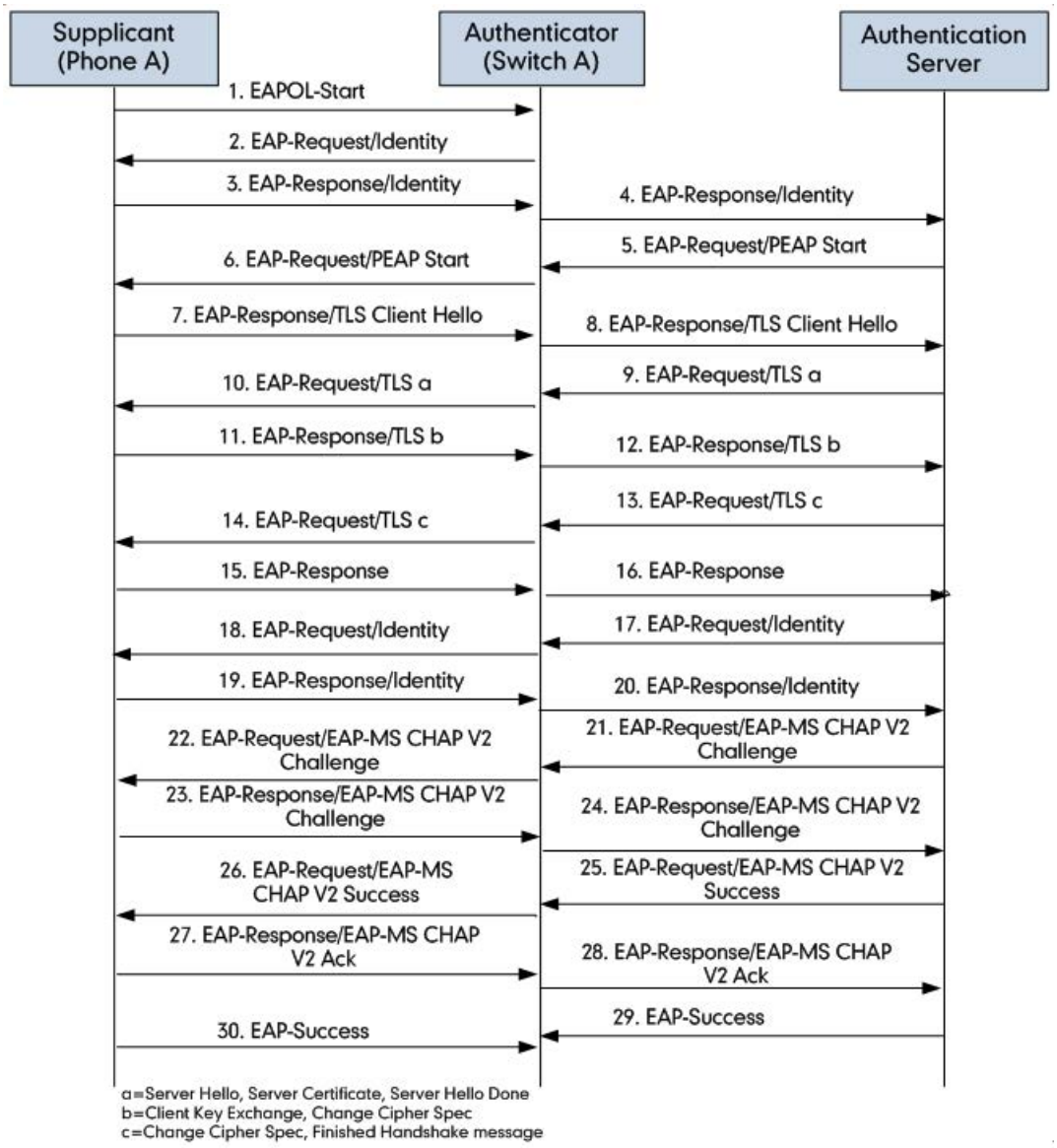
Sample Screenshot



Authentication Process Using EAP-PEAP/MSCHAPv2 Protocol

Authentication Process

The following figure illustrates the scenario of a successful 802.1X authentication process using the EAP-PEAP/MSCHAPv2 protocol.



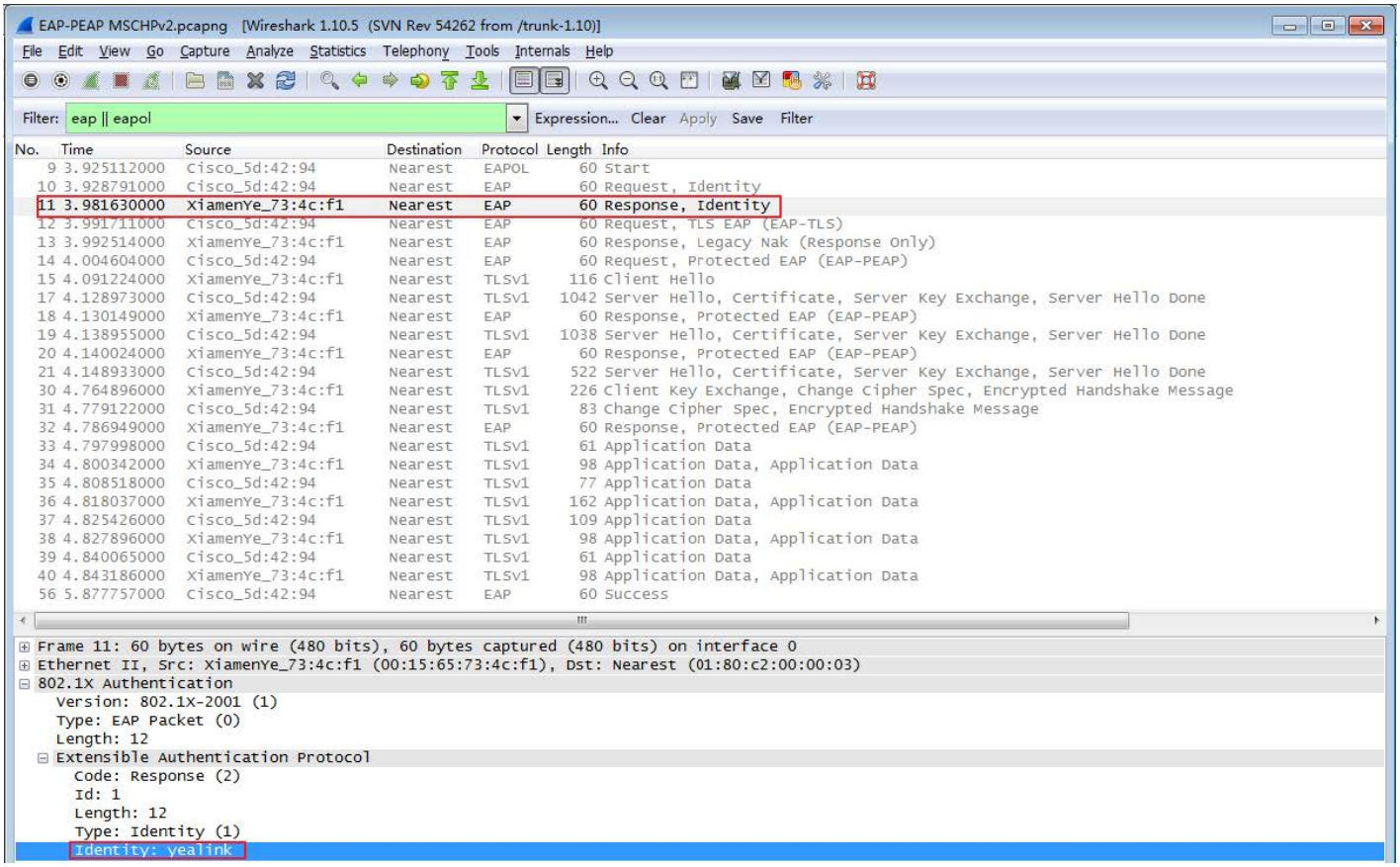
1. The supplicant sends an “EAPOL-Start” packet to the authenticator.
2. The authenticator responds with an “EAP-Request/Identity” packet to the supplicant.
3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
4. The authenticator strips the Ethernet header and encapsulates the remaining EAP frame in the RADIUS format, and then sends it to the authentication server.
5. The authentication server recognizes the packet as a PEAP type and sends an “EAP-Request” packet with a PEAP start message to the authenticator.
6. The authenticator strips the authentication server’s frame header, encapsulates the remaining EAP frame in the EAPOL format, and then sends it to the supplicant.
7. The supplicant responds with an “EAP-Respond” packet containing a TLS client hello handshake message to the authenticator. The TLS client hello message includes TLS version supported by the supplicant, a session ID, a random number and a set of cipher suites.
8. The authenticator passes the response to the authentication server.

9. The authentication server sends an “EAP-Request” packet to the authenticator. The packet includes a TLS server hello handshake message, a server certificate message, and a server hello done message.
10. The authenticator passes the request to the supplicant.
11. The supplicant responds with an “EAP-Response” packet to the authenticator. The packet includes a TLS change cipher spec message and a certificate verify message.
12. The authenticator passes the response to the authentication server.
13. The authentication server sends an “EAP-Request” packet to the authenticator. The packet includes a TLS change cipher spec message and a finished handshake message. The change cipher spec message is sent to notify the authenticator that subsequent records will be protected under the newly negotiated cipher spec.
14. The authenticator passes the request to the supplicant.
15. The supplicant responds with an “EAP-Response” packet to the authenticator.
16. The authenticator passes the response to the authentication server. The TLS tunnel is established.
17. The authentication server sends an “EAP-Request/Identity” packet to the authenticator.
18. The authenticator passes the request to the supplicant.
19. The supplicant responds with an “EAP-Response/Identity” packet to the authenticator.
20. The authenticator passes the response to the authentication server.
21. The authentication server sends an “EAP-Request” packet to the authenticator. The packet includes an MSCHAPv2 challenge message.
22. The authenticator passes the request to the supplicant.
23. The supplicant responds a challenge message to the authenticator.
24. The authenticator passes the message to the authentication server.
25. The authentication server sends a success message indicating that the supplicant provides proper identity.
26. The authenticator passes the message to the supplicant.
27. The supplicant responds with an ACK message to the authenticator.
28. The authenticator passes the response message to the authentication server.
29. The authentication server sends a successful message to the authenticator.

30. The authenticator passes the message to the supplicant.
    After the supplicant is authenticated successfully, the authenticator provides network access permissions. If the supplicant does not provide proper identification, the authentication server responds with a rejection message. The authenticator passes the message to the supplicant and blocks access to the LAN.

    If the supplicant is disabled or reset after successful authentication, the supplicant sends an EAPOL-Logoff message, which prompts the authenticator to block access to the LAN.

Sample Screenshot



Troubleshooting

Why doesn’ t the phone pass 802.1X authentication?

Do the following in sequence:

1. Ensure that the 802.1X authentication environment is operational.
    - a) Connect another device (e.g., a computer) to the switch port.
    - b) Check if the device is authenticated successfully, and an IP address is assigned to it.

      If the device fails the authentication, check the configurations on the switch and authentication server.

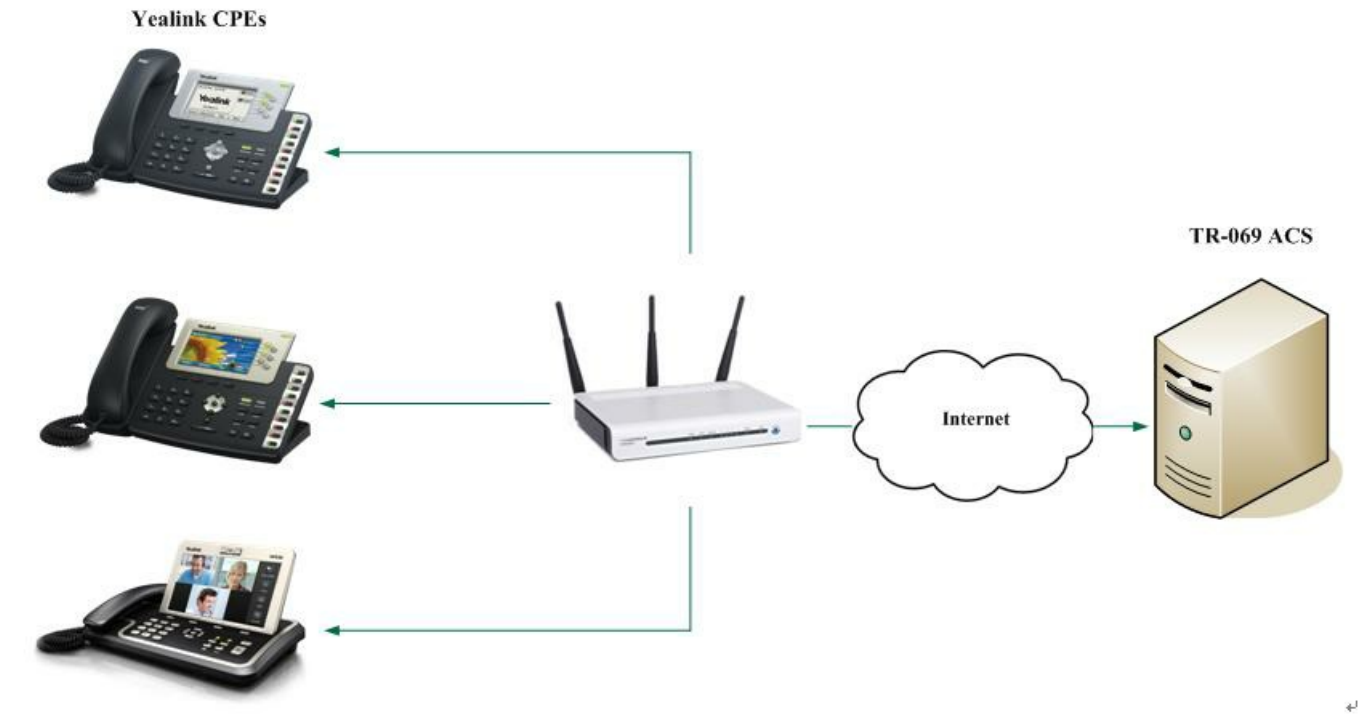
2. Ensure that the username and password configured on the phone are correct. If EAP-TLS, EAP-PEAP/MSCHAPv2, EAP-TTLS/EAP-MSCHAPv2, EAP-PEAP/GTC, EAP-TTLS/EAP-GTC, and EAP-FAST protocols are used, ensure that the certificate uploaded to the phone is valid.
   - a) Double-click the certificate to check the validity time.
   - b) Check if the time and date on the phone are within the validity time of the uploaded certificate. If not, re-generate a certificate and upload it to the phone.
3. Ensure that the failure is not caused by network settings.
   - a) Disable VLAN feature on the phone to check if the authentication passes successfully.

     If the phone is authenticated successfully, capture the packet and feed it back to your network administrator.
4. Contact Yealink FAE for support when the above steps cannot solve your problem.
   - a) Capture the packet and export configurations of the phone, switch, and authentication server.
   - b) Provide the related information to Yealink FAE.

TR069 Device Management

Introduction

TR-069 is a technical specification, which is defined by the Broadband Forum. It defines a mechanism that encompasses secure auto-configuration of a CPE (Customer-Premises Equipment), and also incorporates other CPE management functions into a common framework. TR-069 uses common transport mechanisms (HTTP and HTTPS) for communication between CPE and ACS (Auto Configuration Servers). The HTTP(S) messages contain XML-RPC methods defined in the standard for configuration and management of the CPE. The protocol addresses different Internet access devices such as modems, routers, gateways, set-top boxes, and VoIP phones for the end-users.



Why use TR-069?

TR-069 is an application layer protocol, which has broad applicability and no access restriction. TR-069 standard allows the subscriber to manage all devices on a common platform regardless of device type and manufacturer. Its specifications ensure that the device can be easily and securely configured, activated, and managed from a console in the service provider's network. This allows the service provider to provide an efficient and cost-effective deployment of services.

Supported RPC Methods

The RPC (Remote Procedure Call) method defines a generic mechanism that is used for bi-directional communication between a CPE and an ACS. An ACS can get or set parameters to configure and monitor the CPE by using the RPC methods. The following table provides a description of RPC methods supported by Yealink IP phones:

RPC Method	Description
GetRPCMethods	This method is used to discover the set of methods supported by the CPE.
SetParameterValues	This method is used to modify the value of one or more CPE parameters.
GetParameterValues	This method is used to obtain the value of one or more CPE parameters.
GetParameterNames	This method is used to discover the parameters accessible on a particular CPE.
GetParameterAttributes	This method is used to read the attributes associated with one or more CPE parameters.

SetParameterAttributes	This method is used to modify attributes associated with one or more CPE parameters.
Reboot	This method causes the CPE to reboot.
Download	This method is used to cause the CPE to download a specified file from the designated location. File types supported by the phones are: · Firmware Image · Configuration File
Upload	This method is used to cause the CPE to upload a specified file to the designated location. File types supported by the phones are: · Configuration File · Log File
ScheduleInform	This method is used to request the CPE to schedule a one-time Inform method call (separate from its periodic Inform method calls) sometime in the future.
FactoryReset	This method resets the CPE to its factory default state.
TransferComplete	This method informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.
AddObject	This method is used to add a new instance of an object defined on the CPE.
DeleteObject	This method is used to remove a particular instance of an object.

The ACS supports a variety of functionalities to manage a collection of phones using the above RPC methods, the following primary capabilities are included.

Auto-configuration and dynamic service provisioning

The ACS can provision a phone or collection of phones based on a variety of criteria. Different phone models can be configured using the uniform parameters. Phone can be provisioned at the initial connection and re-provisioned at any subsequent time. The ACS can also check the provision status (success or failure).

Firmware image management

Phone firmware can be upgraded or downgraded by downloading the firmware file from the ACS. TR-069 also provides mechanisms for version identification and file download initiation (ACS-initiated downloads and optional phone-initiated downloads). The ACS can be notified of the success or failure of a file downloading.

Status and performance monitoring

The ACS can use the GetParameterValues and GetParameterAttributes methods to monitor the phone’ s status and performance statistics. TR-069 also defines a set of mechanisms that allows the phone to actively notify the ACS of changes to its state.

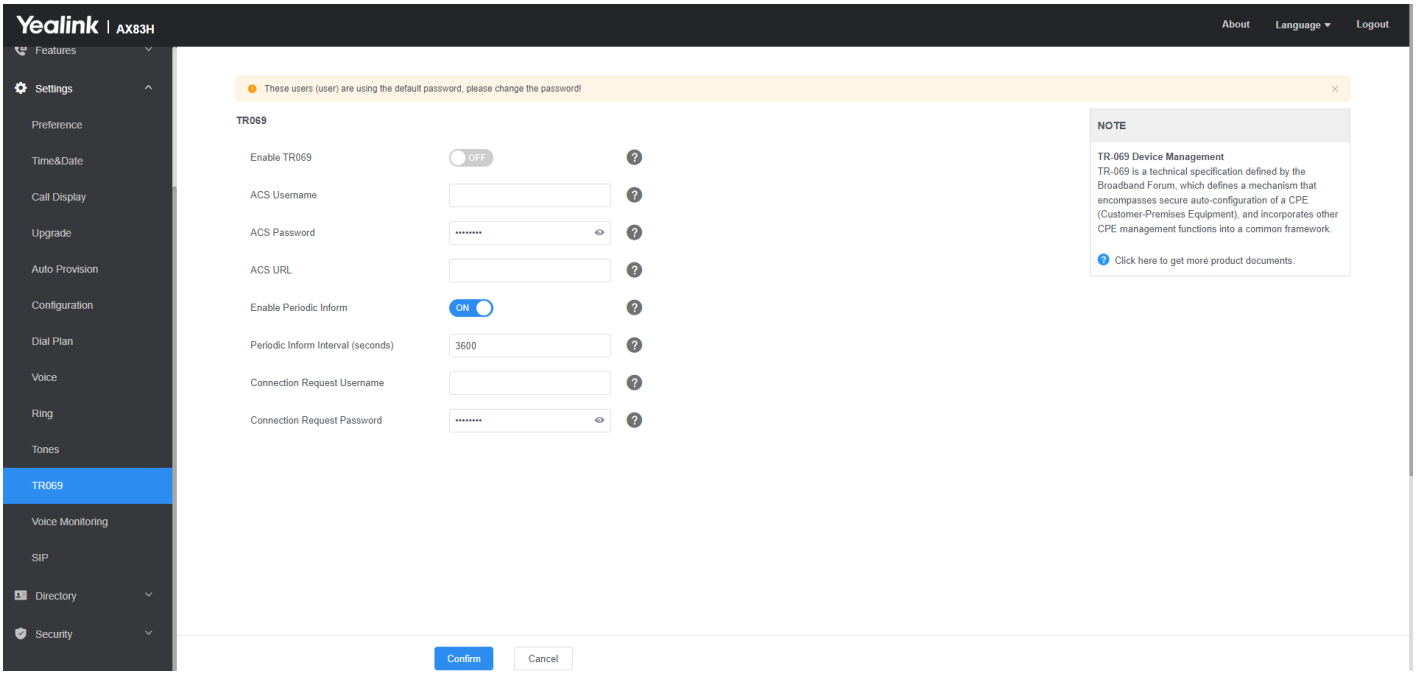
Diagnostics

For troubleshooting purposes, the phone can send diagnostic information such as network status to the ACS, or the ACS can execute the defined diagnostic tests to get the information from the phone.

TR-069 Cconfiguration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **TR069**.



Parameter	Description
Enable TR069	It enables or disables the TR-069 feature.
ACS Username	It configures the TR-069 ACS server user name used to authenticate the phone. Leave it blank if no authentication is required.
ACS Password	It configures the TR-069 ACS server password used to authenticate the phone. Leave it blank if no authentication is required.
ACS URL	It configures the access URL of the TR-069 ACS server.
Enable Periodic Inform	It enables or disables the phone to periodically report its configuration information to the ACS server.
Periodic Inform Interval (seconds)	It configures the interval (in seconds) at which the phone reports its configuration to the ACS server. The default value is **3600**.
Connection Request Username	It configures the user name used to authenticate the connection requests from the ACS server.
Connection Request Password	It configures the password used to authenticate the connection requests from the ACS server.

Configuration Parameter

```
static.managementserver.enable
static.managementserver.username
static.managementserver.password
static.managementserver.url
static.managementserver.connection_request_username
static.managementserver.connection_request_password
static.managementserver.periodic_inform_enable
static.managementserver.periodic_inform_interval
```

Parameter	Permitted Values	Default	Description
static.managementserver.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the TR-069 feature.
static.managementserver.username	String within 128 characters	Blank	It configures the TR-069 ACS server user name used to authenticate the phone. Leave it blank if no authentication is required.
static.managementserver.password	String within 64 characters	Blank	It configures the TR-069 ACS server password used to authenticate the phone. Leave it blank if no authentication is required.
static.managementserver.url	URL within 511 characters	Blank	It configures the access URL of the TR-069 ACS server.
static.managementserver.connection_request_username	String within 128 characters	Blank	It configures the user name used to authenticate the connection requests from the ACS server.
static.managementserver.connection_request_password	String within 64 characters	Blank	It configures the password used to authenticate the connection requests from the ACS server.
static.managementserver.periodic_inform_enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to periodically report its configuration information to the ACS server
static.managementserver.periodic_inform_interval	Integer from 5 to 4294967295	60	It configures the interval (in seconds) at which the phone reports its configuration to the ACS server. **NOTE** It works only if `static.managementserver.periodic_inform_enable` is set to 1 (Enabled).

TR-111 Support

TR-111 standard defines two mechanisms that extend the CWMP defined in TR-069 to enhance the ability to remotely manage devices, which are connected via a LAN through an Internet gateway.
The two mechanisms are briefly summarized as follows:

- **Device-Gateway Association**: Allows an ACS to manage a device to identify the associated gateway to which that device is connected.

- **Connection Request via NAT Gateway**: Allows an ACS to initiate a TR-069 Session with a device that is operating behind a NAT gateway.

ACS Specific Information

Yealink IP phones can work properly with various ACS. For more information about the supported ACS, contact Yealink technical support.

Data Model

Most of the configuration and diagnostics are performed through setting and retrieving the value of the phone parameters. They are organized in a well-defined hierarchical structure that is more or less common to all phone models. For more information about the common and customized phone parameters, refer to the phone-specific document *Yealink_TR-069_DataModel_V4.0.xlsx*.
Contact the Yealink technical support for the data model file. Each of the parameters is marked as writable or non-writable. The phone does not permit the change of any parameter marked as read-only. Values applicable for the parameter, their type, and meaning are also precisely defined in the document.

Normative References

TR-069: http://www.broadband-forum.org/technical/download/TR-069_Amendment-6.pdf
TR-104: http://www.broadband-forum.org/technical/download/TR-104.pdf
TR-106: http://www.broadband-forum.org/technical/download/TR-106_Amendment-3.pdf
TR-111: http://www.broadband-forum.org/technical/download/TR-111.pdf

Account Settings

Account Registration

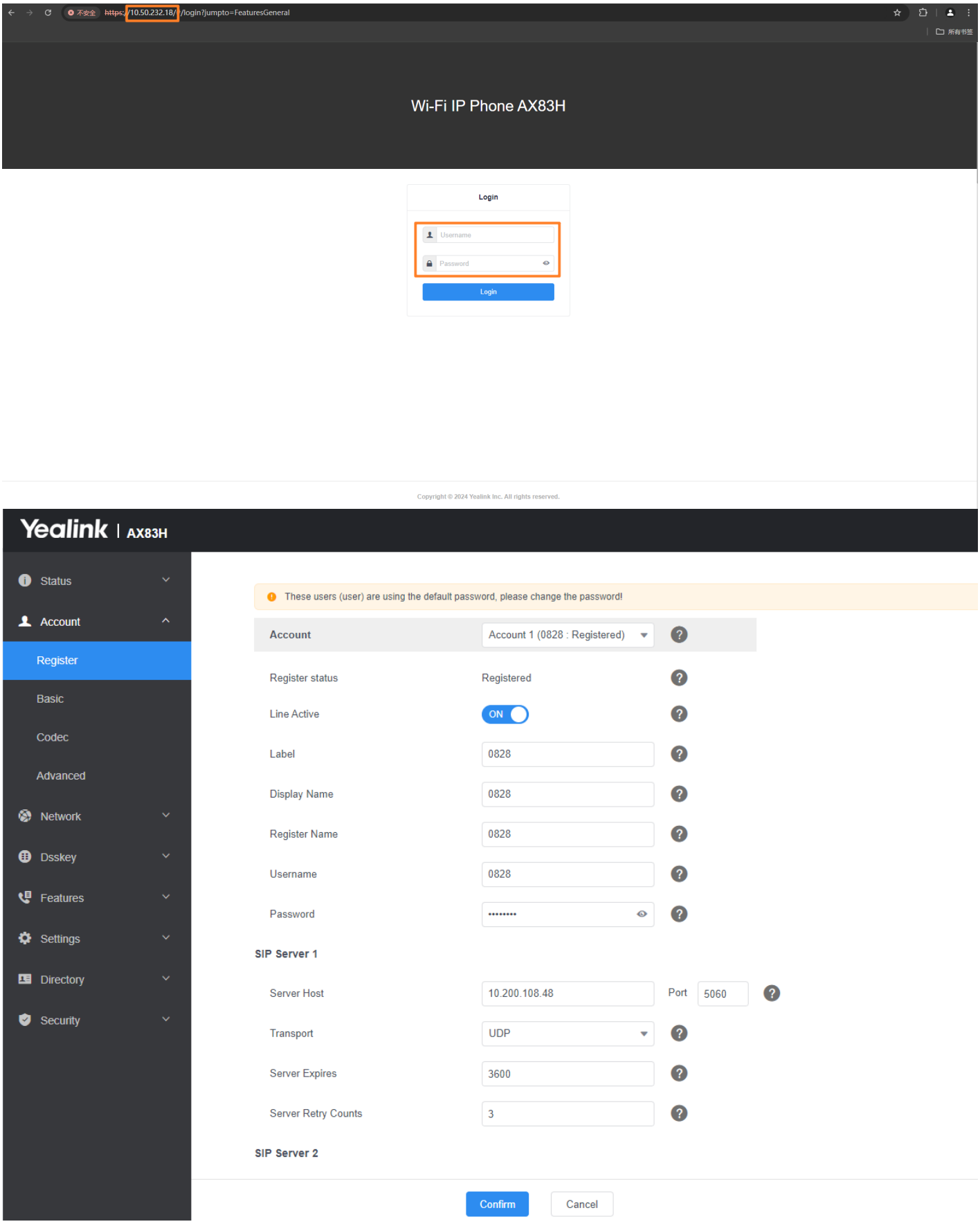
Introduction

Any handset must get assigned an individual SIP account. After registering the handset to the system, the handset can be assigned an account for receiving and sending VoIP connection.

Accounts Registration Configuration

Set via the Web User Interface

On the web user interface, go to **Account** > **Register**.



Register Status: It shows the registration status of the current account.

Line Active: You can enable/disable the account.

Label: It is shown on the LCD to identify the account.

Display Name: It is shown as a caller ID when placing a call.

User Name: It is provided by ITSP for registration (necessary). Please connect with your VOIP Service provider to get this information.
Register Name: It is an authenticated ID for authentication provided by ITSP (necessary) Please connect with your VOIP Service provider to get this information.
Password: It is provided by ITSP for registration (necessary). Please connect with your VOIP Service provider to get this information.
Server Host: It is provided by ITSP for registration (necessary). Please connect with your VOIP Service provider to get this information.

NOTE
The phone supports three SIP server configurations, allowing you to configure a third SIP server address through the web interface.

Configuration Parameter

```
account.X.enable
account.X.label
account.X.display_name
account.X.auth_name
account.X.user_name
account.X.password
account.X.sip_server.address
account.X.reg_fail_retry_interval
account.X.reg_failed_retry_min_time
account.X.reg_failed_retry_max_time
```

Parameter	Permitted Values	Default	Description
account.X.enable[1]	**0**-Disabled **1**-Enabled	0	It defines the activation status of the account.
account.X.label[1]	String within 99 characters	Blank	It configures the display label of the account.
account.X.display_name[1]	String within 99 characters	Blank	It configures the display name of the account.
account.X.auth_name[1]	String within 99 characters	Blank	It configures the user name for authentication registration.
account.X.user_name[1]	String within 99 characters	Blank	It configures the user name of the account.

account.X.password[1]	String within 99 characters	Blank	It configures password of the account.
account.X.sip_server.address	Integer from 1 to 10	1	It configures what SIP server to use for registering an account.
account.X.reg_fail_retry_interval[1]	Integer from 0 to 1800	30	It configures the re-registration period (in seconds) after the account registration fails. **NOTE** It works only if account.X.reg_failed_retry_min_time and account.X.reg_failed_retry_max_time are set to 0.
account.X.reg_failed_retry_min_time[1]	Integer greater than or equal to 0	0	It configures the base time to wait (in seconds) for the phone to retry to re-register after the account registration fails. **NOTE** It is used in conjunction with the parameter account.X.reg_failed_retry_max_time to determine how long to wait. The algorithm is defined in RFC 5626. We recommend that you set this value to an integer between 10 to 120 if needed. If the values of this parameter and the parameter account.X.reg_failed_retry_max_time are set to 0, the interval configured by account.X.reg_fail_retry_interval will be used.
account.X.reg_failed_retry_max_time[1]	Integer greater than or equal to 0	60	It configures the maximum time to wait (in seconds) for the phone to retry to re-register after the account registration fails. **NOTE** It is used in conjunction with the parameter account.X.reg_failed_retry_min_time to determine how long to wait. The algorithm is defined in RFC 5626. We recommend that you set this value to an integer between 60 to 1800 if needed. If the values of this parameter and the parameter account.X.reg_failed_retry_min_time are set to 0, the interval configured by account.X.reg_fail_retry_interval will be used.

[1]X is the account ID.
[2]Y is the server ID. Y=1-2.

Registration Settings Configuration

The following table lists the parameters you can use to change the registration settings.

Set via the Web User Interface

On the web user interface, go to **Account** > **Advanced**.

Configuration Parameter

```
account.X.enable_user_equal_phone
account.X.register_mac
account.X.register_line
account.X.unregister_on_reboot
account.X.sip_server_type
sip.reg_surge_prevention
account.X.subscribe_register
phone_setting.disable_account_without_username.enable
account.X.register_expires_overlap
account.X.subscribe_expires_overlap
```

Parameter	Permitted Values	Default	Description
account.X.enable_user_equal_phone[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to add "user=phone" to the SIP header of the INVITE message.
account.X.register_mac[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to add MAC address to the SIP header of the REGISTER message.
account.X.register_line[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to add a line number to the SIP header of the REGISTER message. 0-99 stand for line1-line100.
account.X.unregister_on_reboot[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to unregister first before re-registering account X after a reboot.
account.X.sip_server_type[1]	**0**-Default 2-BroadSoft (It works only if `bw.enable` is set to 1 (Enabled)) **8**-Genesys **10**-Genesys Advanced	0	It configures the type of SIP server.
sip.reg_surge_prevention[2]	Integer from 0 to 60	0	It configures the waiting time (in seconds) for account register after startup.

account.X.subscribe_register[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to subscribe to the registration state change notifications.
phone_setting.disable_account_without_username.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to disable the account whose username is empty.
account.X.register_expires_overlap[1]	Positive integer and -1	-1	It configures the renewal time (in seconds) away from the registration lease.
account.X.subscribe_expires_overlap[1]	Positive integer and -1	-1	It configures the renewal time (in seconds) away from the subscription lease.

[1]X is the account ID.
[2]If you change this parameter, the phone will reboot to make the change take effect.

Outbound Proxy in Dialog

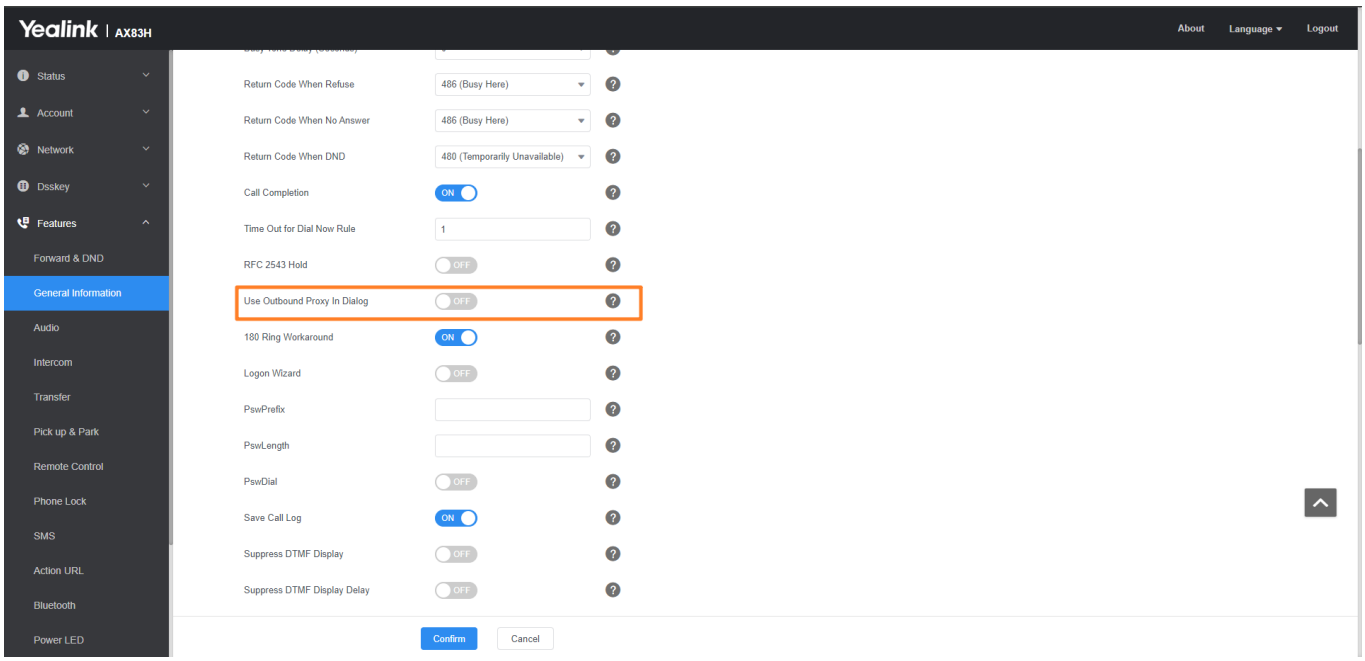
Introduction

An outbound proxy server can receive all initiating request messages and route them to the designated destination. If the device is configured to use an outbound proxy server within a dialog, all SIP request messages from the device will be sent to the outbound proxy server as a mandatory requirement.
To use this feature, make sure the outbound server has been correctly configured on the device. For more information on how to configure the outbound server, refer to Server Redundancy

Outbound Proxy in Dialog Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Use Outbound Proxy In Dialog**.



Configuration Parameter

```
sip.use_out_bound_in_dialog
```

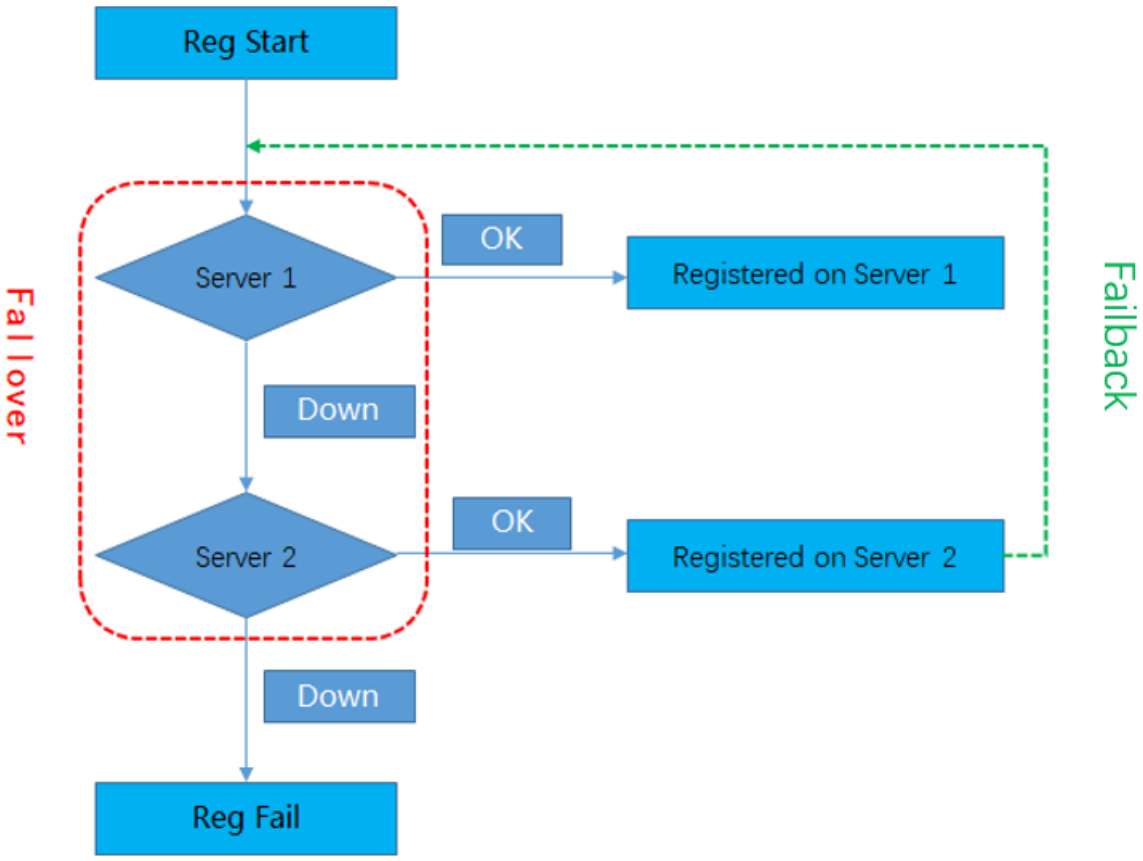
Parameter	Permitted Values	Default	Description
sip.use_out_bound_in_dialog	**0**-Disabled, only the new SIP request messages from the phone will be sent to the outbound proxy server in a dialog. **1**-Enabled, all the SIP request messages from the phone will be sent to the outbound proxy server in a dialog.	0	It enables or disables the phone to send all SIP requests to the outbound proxy server mandatorily in a dialog. **NOTE** It works only if `account.X.outbound_proxy_enable` is set to 1 (Enabled).

Server Redundancy

Introduction

Server redundancy is often required in VoIP deployments to ensure continuity of phone service, for example, take the call server offline for maintenance, the server fails, or the connection between the device and the server fails. Two types of redundancy are possible. In some cases, a combination of the two may be deployed:

- **Failover**: In this mode, the full phone system functionality is preserved by having a second equivalent capability call server take over from the one that has gone down/offline. This mode of operation should be done using the DNS mechanism from the primary to the secondary server. Therefore, if you want to use this mode, the server must be configured with a domain name.
- **Fallback**: In this mode, a second less-featured call server with SIP capability takes over call control to provide the basic calling capability, but without some advanced features (for example, shared line and MWI) offered by the working server. The phones support the configuration of two servers per SIP registration for the fallback purpose.

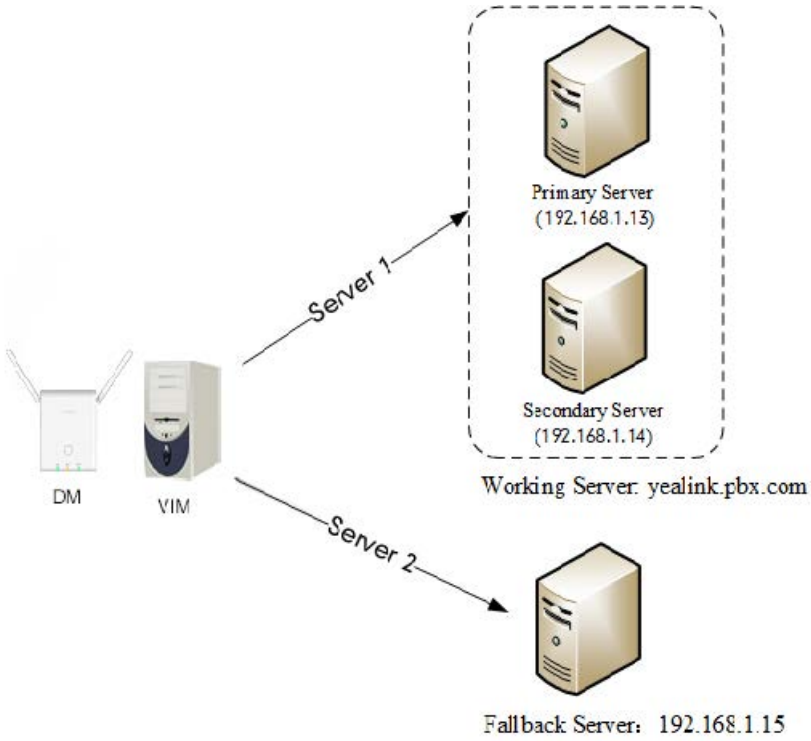


NOTE

For concurrent registration mode, it has a certain limitation when using some advanced features, and for successive registration mode, the phone service may have a brief interruption while the server fails. So we recommend that you use the failover mode for server redundancy because this mode can ensure the continuity of the phone service and you can use all the call features while the server fails.

Server Redundancy Implementation

To assist in explaining the redundancy behavior, an illustrative example of how a phone may be configured is shown below. In the example, server redundancy for fallback and failover purposes is deployed. Two separate servers (a working server and a fallback server) are configured for per-line registration.



- **Working Server**: Server 1 is configured with the domain name of the working server. For example yealink.pbx.com. The DNS mechanism is used such that the working server is resolved to multiple servers with different IP addresses for failover purposes. The working server is deployed in redundant pairs, designated as primary and secondary servers. The primary server (for example, 192.168.1.13) has the highest priority server in a cluster of servers resolved by the DNS server. The secondary server (for example, 192.168.1.14) backs up a primary server when the primary server fails and offers the same functionality as the primary server.
- **Fallback Server**: Server 2 is configured with the IP address of the fallback server. For example 192.168.1.15. A fallback server offers less functionality than a working server.

Yealink devices support Failover and Fallback server redundancy types. In some cases, you can deploy a combination of the two server redundancy types.

Behaviors When Working Server Connection Fails

When you initiate a call, the phone will go through the following steps to connect the call:

1. Send the INVITE request to the primary server.
2. If the primary server does not respond correctly to the INVITE (that is, the primary server responds to the INVITE with 503 messages or the request for responding with 100 Trying message times out (64*T1 seconds, defined in RFC 3261), then tries to make the call using the secondary server.
3. If the secondary server is also unavailable, the phone will try the fallback server until it either succeeds in making a call or exhausts all servers at which point the call will fail.
   At the start of a call, server availability is determined by SIP signaling failure. SIP signaling failure depends on the SIP protocol being used as described below:
   - If TCP is used, then the signaling fails if the connection or the send fails.
   - If UDP is used, then the signaling fails if ICMP is detected or if the signal times out. If the signaling has been attempted through all servers in the list (this list contains all the server addresses resolved by the DNS server) and this is the last server, then the signaling fails after the complete UDP timeout defined in RFC 3261 If it is not the last server in the list, the maximum number of retries depends on the configured retry counts (configured by `template.X.sip_server.Y.retry_counts`).

Registration Method of the Failover/Fallback Mode

1. **Registration method of the failover mode:**
   The phone must always register to the primary server first except in failover conditions. If this is unsuccessful, the phone will re-register as many times as configured until the registration is successful. When the primary server registration is unavailable, the secondary server will serve as the working server.

2. **Registration methods of the fallback mode**:

- **Concurrent registration (default)**: The phone registers to two SIP servers (working server and fallback server) at the same time. In a failure situation, a fallback server can take over the basic calling capability, but without some advanced features (for example, shared lines, call recording, and MWI) offered by the working server. It does not apply to outbound proxy servers.
- **Successive registration**: The phone only registers to one server at a time. The phone first registers to the working server. In a failure situation, the phone registers to the fallback server.

SIP Server Name Resolution

If a domain name is configured for a server, the IP address(es) associated with that domain name will be resolved through DNS as specified by RFC 3263. The DNS query involves NAPTR, SRV, and A queries, which allows the phone to adapt to various deployment environments. The phone performs the NAPTR query for the NAPTR pointer and transport protocol (UDP, TCP, and TLS), the SRV query on the record returned from the NAPTR for the target domain name and the port number, and the A query for the IP addresses.
If an explicit port (except 0) is specified and the transport type is set to DNS-NAPTR, A query will be performed only. If a server port is set to 0 and the transport type is set to DNS-NAPTR, NAPTR and SRV queries will be tried before falling to A query. If no port is found through the DNS query, 5060 will be used.
For more information, refer to Appendix A: SIP Server Name Resolution Configuration.
If your phone is not configured with a DNS server, or the DNS query returns no result from a DNS server, you can configure a static DNS cache for the phone. The phone will attempt to resolve the domain name of the server with a static DNS cache. For more information on static DNS cache, refer to Appendix B: Static DNS Cache.

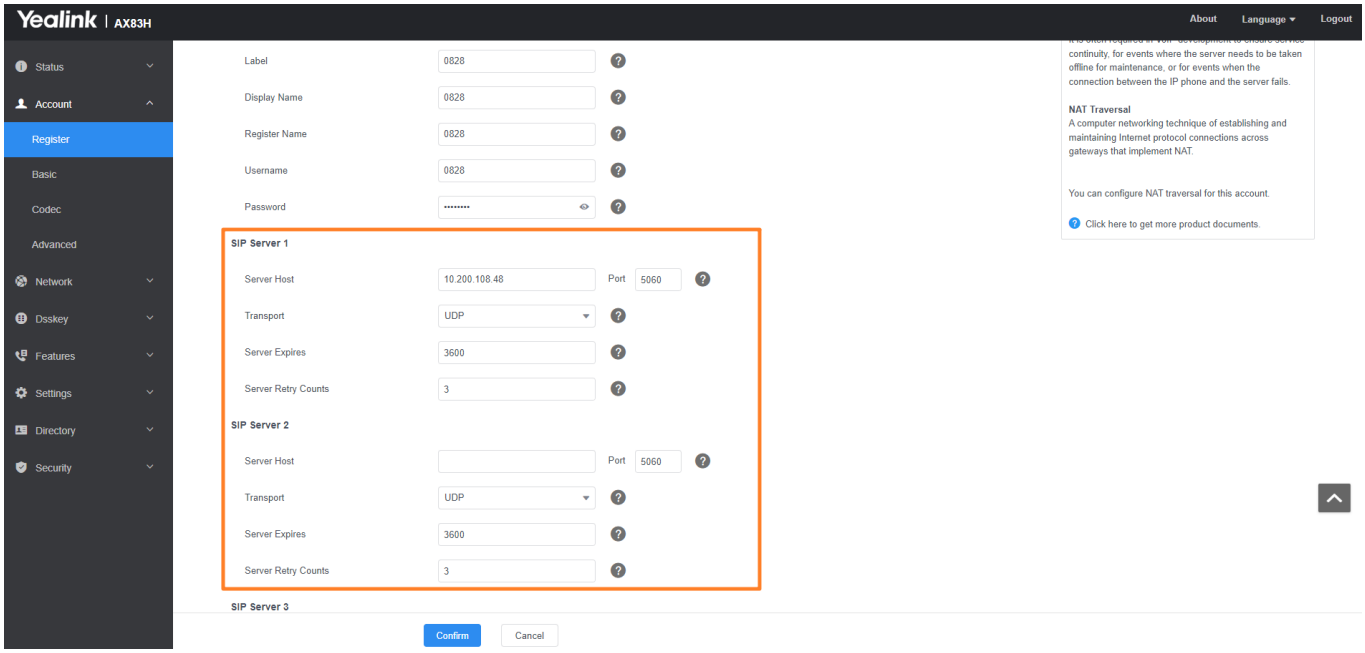
Configure Yealink Phones

Set via the Web User Interface

To configure server redundancy for fallback purpose Set via the Web User Interface:

1. Click **Account** > **Register**.
2. Select the desired account from the **Account** drop-down menu.
3. Configure the registration parameters of the selected account in the corresponding fields.

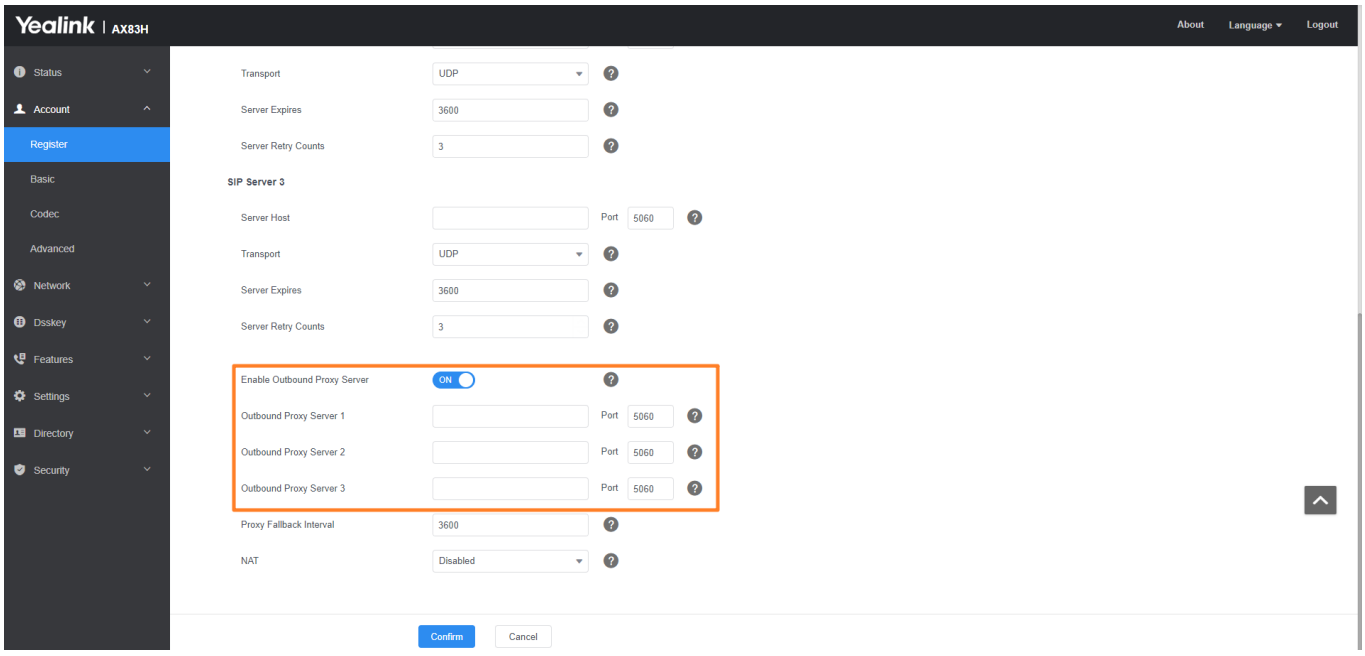
4. Configure the parameters of SIP server 1 and SIP server 2 in the corresponding fields.



5. If you use outbound proxy servers, do the following:

   1)Select **Enabled** from the **Enable Outbound Proxy Server** drop-down menu.

   2)Configure parameters of the outbound proxy server 1 and outbound proxy server 2 in the corresponding fields.

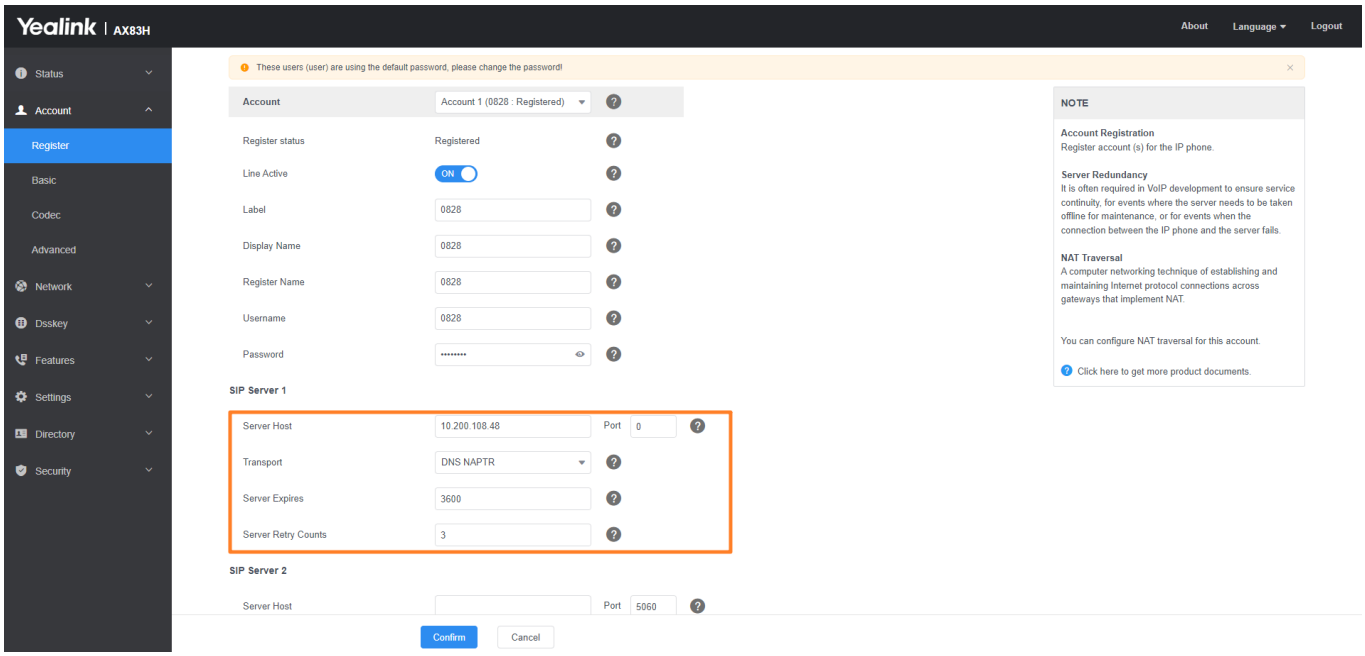


6. Click **Confirm** to accept the change.

To configure server redundancy for failover purposes Set via the Web User Interface:

1. Click **Account** > **Register**.
2. Select the desired account from the **Account drop-down** menu.

3. Configure the registration parameters of the selected account in the corresponding fields.
4. Configure the parameters of the SIP server 1 or SIP server 2 in the corresponding fields.
   You must set the port of the SIP server to 0 for NAPTR, SRV, and A queries.
5. Select **DNS-NAPTR** from the **Transport** drop-down menu.



6. If you use outbound proxy servers, do the following:

   1)Select **Enabled** from the **Enable Outbound Proxy Server** drop-down menu.

   2)Configure parameters of the outbound proxy server 1 and outbound proxy server 2 in the corresponding fields.

   You must set the port of the outbound proxy to 0 for NAPTR, SRV, and A queries.

7. Click **Confirm** to accept the change.

Configuration parameter

Fallback Server Redundancy Configuration

```
account.X.fallback.redundancy_type
account.X.fallback.timeout
```

Parameter	Permitted Values	Default	Description

account.X.fallback.redundancy_type[1]	**0**-Concurrent registration **1**-Successive registration	0	It configures the registration mode in fallback mode. **NOTE** It is not applicable to outbound proxy servers.
account.X.fallback.timeout[1]	Integer from 10 to 2147483647	120	It configures the time interval (in seconds) for the phone to detect whether the working server is available by sending the registration request after the fallback server takes over call control. **NOTE** It is not applicable to outbound proxy servers.

[1] X is the account ID.

Failover Server Redundancy Configuration

```
account.X.sip_server.Y.register_on_enable
sip.skip_redundant_failover_addr
account.X.sip_server.Y.only_signal_with_registered
account.X.sip_server.Y.invite_retry_counts
account.X.sip_server.Y.failback_mode
account.X.sip_server.Y.failback_timeout
account.X.sip_server.Y.failback_subscribe.enable
sip.forbidden_failover_signal.list
```

Parameter	Permitted Values	Default	Description
account.X.sip_server.Y.register_on_enable[1] [2]	**0**-Disabled, the phone will not attempt to register to the secondary server, since the phone assumes that the primary and secondary servers share registration information. So the phone will directly send the requests to the secondary server. **1**-Enabled, the phone will register to the secondary server first, and then send the requests to it.	0	It enables or disables the phone to send registration requests to the secondary server when encountering a failover.
sip.skip_redundant_failover_addr	**0**-Disabled **1**-Enabled	1	It enables or disables the phone only to send requests to the servers with different IP addresses when encountering a failover.

account.X.sip_server.Y.only_signal_with_registered[1] [2]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to only send requests to the registered server when encountering a failover. **NOTE** It works only if account.X.sip_server.Y.register_on_enable is set to 1 (Enabled) and account.X.sip_server.Y.failback_mode is set to 1, 2 or 3.
account.X.sip_server.Y.invite_retry_counts[1] [2]	Integer from 1 to 10	3	It configures the number of retries attempted before sending requests to the next available server when encountering a failover.
account.X.sip_server.Y.failback_mode[1] [2]	**0**-newRequests: all requests are sent to the primary server first, regardless of the last server that was used. **1**-DNSTTL: the phone will send requests to the last registered server first. If the time defined by DNSTTL on the registered server expires, the phone will retry to send requests to the primary server. **2**-Registration: the phone will send requests to the last registered server first. If the registration expires, the phone will retry to send requests to the primary server. **3**-duration: the phone will send requests to the last registered server first. If the time defined by the account.X.sip_server.Y.failback_timeout parameter expires, the phone will retry to send requests to the primary server.	0	It configures the mode for the phone to retry the primary server in failover. **NOTE** It works only if template.X.sip_server.Y.address is set to the domain name of the SIP server.

account.X.sip_server.Y.failback_timeout[1] [2]	0, Integer from 60 to 65535	3600	It configures the timeout (in seconds) for the phone to retry to send requests to the primary server after failing over to the current working server. If you set the parameter to 0, the phone will not send requests to the primary server until a failover event occurs with the current working server. If you set the parameter between 1 and 59, the timeout will be 60 seconds. **NOTE** It works only if account.X.sip_server.Y.failback_mode is set to 3 (duration).
account.X.sip_server.Y.failback_subscribe.enable[1] [2]	**0**-Disabled **1**-Enabled, the phone will immediately re-subscribe to the secondary server, to ensure the normal use of the features associated with the subscription (for example, BLF, SCA).	0	It enables or disables the phone to retry to re-subscribe after registering to the secondary server with different IP addresses when encountering a failover. **NOTE** It works only if account.X.sip_server.Y.failback_mode is set to 1, 2 or 3.
sip.forbidden_failover_signal.list	PUBLISH INFO	Null	It configures whether RTCP can perform the failover.

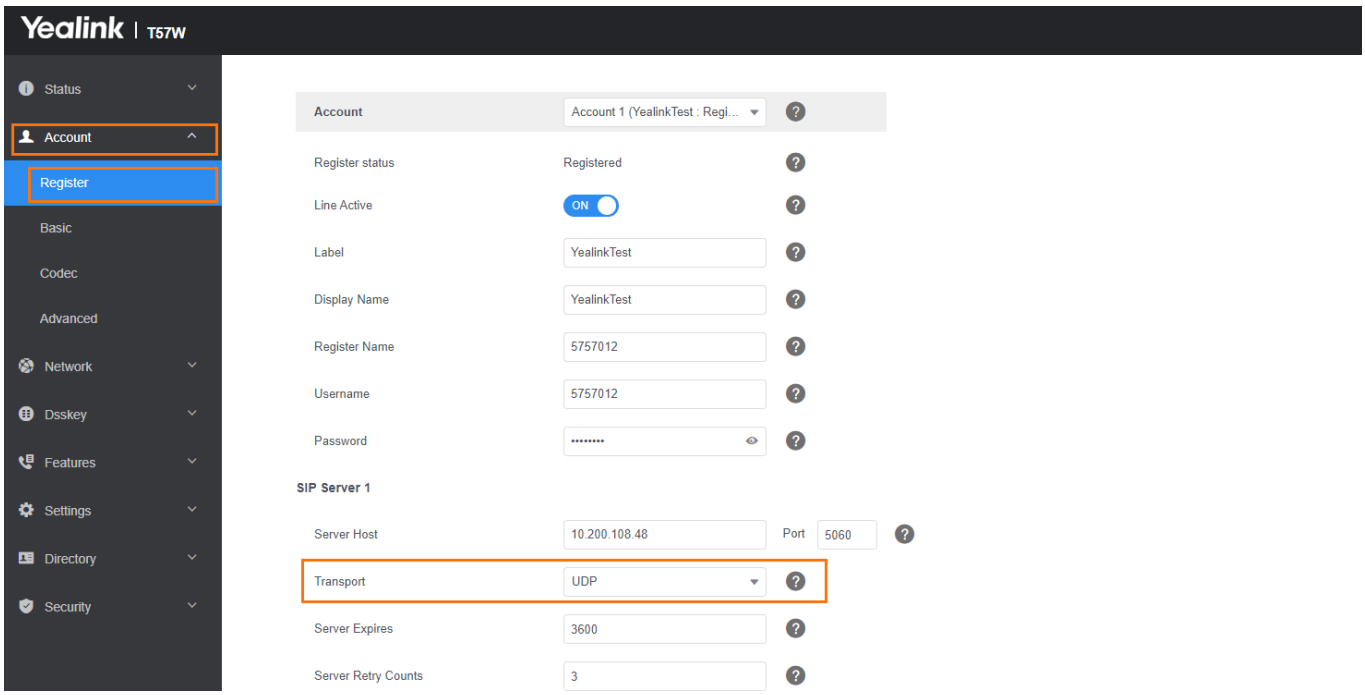
[1] X is the account ID.
[2] Y is the server ID. Y=1-2.

Appendix

Appendix A: SIP Server Name Resolution Configuration

- **Set via the Web User Interface**

  On the web user interface, go to **Account** > **Register** > **SIP Server Y** > **Transport**.



- **Configuration parameter**

```
account.X.sip_server.Y.transport_type
account.X.naptr_build
sip.dns_transport_type
static.network.dns.query_timeout
static.network.dns.retry_times
```

Parameter	Permitted Values	Default	Description
account.X.sip_server.Y.transport_type[1] [2]	**0**-UDP **1**-TCP **2**-TLS **3**-DNS NAPTR, if no server port is given, the device performs the DNS NAPTR and SRV queries for the service type and port.	0	It configures the type of transport protocol.
account.X.naptr_build[1]	**0**-SRV query using UDP only **1**-SRV query using UDP, TCP, and TLS.	0	It configures the way of SRV query for the phone to be performed when no result is returned from the NAPTR query.

sip.dns_transport_type	**0**-UDP **1**-TCP	0	It configures the transport protocol the phone uses to perform a DNS query.
static.network.dns.query_timeout[3]	Integer from 0 to 65535	3	It configures the interval (in seconds) at which the phone retries to resolve a domain name when the DNS server does not respond.
static.network.dns.retry_times[3]	Integer from 0 to 65535	2	It configures the retry times when the DNS server does not respond.

[1]X is the account ID.
[2]Y is the server ID. Y=1-2.
[3]If you change this parameter, the phone will reboot to make the change take effect.

Appendix B: Static DNS Cache

Failover redundancy can only be utilized when the configured domain name of the server is resolved to multiple IP addresses. If the phone is not configured with a DNS server, or the DNS query returns no result from a DNS server, you can statically configure a set of DNS NAPTR/SRV/A records into the phone. The phone will attempt to resolve the domain name of the SIP server with a static DNS cache.
Support for negative caching of DNS queries as described in RFC 2308 is also provided to allow faster failover when prior DNS queries have returned no results from the DNS server.

Behave with a Configured DNS Server

1. When the phone **is configured with a DNS server**, it will behave as follows to resolve the domain name of the server:
   - The phone performs a DNS query to resolve the domain name from the DNS server.
   - If the DNS query returns no results for the domain name or the returned record cannot be contacted, the values in the static DNS cache (if configured) are used when their configured time intervals are not elapsed.
   - If the configured time interval is elapsed, the phone will attempt to perform a DNS query again.
   - If the DNS query returns a result, the phone will use the returned record from the DNS server and ignore the statically configured cache values.
2. When the phone **is not configured with a DNS server**, it will behave as follows:
   - The phone attempts to resolve the domain name within the static DNS cache.
   - The phone will always use the results returned from the static DNS cache.

Static DNS Cache Configuration

Configuration parameter

dns_cache_naptr.X.service
account.X.static_cache_pri[1
account.X.dns_cache_type
dns_cache_naptr.X.name
dns_cache_naptr.X.order
dns_cache_naptr.X.preference
dns_cache_naptr.X.replace
dns_cache_naptr.X.ttl
dns_cache_srv.X.name
dns_cache_srv.X.port
dns_cache_srv.X.priority
dns_cache_srv.X.target
dns_cache_srv.X.weight
dns_cache_srv.X.ttl
dns_cache_a.X.name
dns_cache_a.X.ip
dns_cache_a.X.ttl
static.network.dns.ttl_enable
static.network.dns.last_cache_expired
static.network.dns.last_cache_expired.enable

Parameter	Permitted Values	Default	Description
account.X.dns_cache_type[1]	**0**-Perform real-time DNS query rather than using DNS cache. **1**-Use DNS cache, but do not record the additional records. **2**-Use DNS cache and cache the additional DNS records.	1	It configures whether the phone uses the DNS cache for domain name resolution of the SIP server and caches the additional DNS records.
account.X.static_cache_pri[1]	**0**-Use domain name resolution from server preferentially **1**-Use static DNS cache preferentially	0	It configures whether preferentially to use the static DNS cache for domain name resolution of the SIP server.
dns_cache_naptr.X.name[2]	Domain name	Blank	It configures the domain name to which NAPTR record X refers.
dns_cache_naptr.X.order[2]	Integer from 0 to 65535	0	It configures the order of NAPTR record X. NAPTR record with the lower order is more preferred.
dns_cache_naptr.X.preference[2]	Integer from 0 to 65535	0	It configures the preference of NAPTR record X. NAPTR record with lower preference is more preferred.
dns_cache_naptr.X.replace[2]	Domain name	Blank	It configures a domain name to be used for the next SRV query in NAPTR record X.

dns_cache_naptr.X.service[2]	**SIP+D2U**-SIP over UDP **SIP+D2T**-SIP over TCP **SIPS+D2T**-SIPS over TLS	Blank	It configures the transport protocol available for the SIP server in NAPTR record X.
dns_cache_naptr.X.ttl[2]	Integer from 30 to 2147483647	300	It configures the time interval (in seconds) that NAPTR record X may be cached before the record should be consulted again.
dns_cache_srv.X.name[2]	Domain name	Blank	It configures the domain name in SRV record X.
dns_cache_srv.X.port[2]	Integer from 0 to 65535	0	It configures the port to be used in SRV record X.
dns_cache_srv.X.priority[2]	Integer from 0 to 65535	0	It configures the priority for the target host in SRV record X. Lower priority is more preferred.
dns_cache_srv.X.target[2]	Domain name	Blank	It configures the domain name of the target host for an A query in SRV record X.
dns_cache_srv.X.weight[2]	Integer from 0 to 65535	0	It configures the weight of the target host in SRV record X. When priorities are equal, weight is used to differentiate the preference. Higher weight is more preferred.
dns_cache_srv.X.ttl[2]	Integer from 30 to 2147483647	300	It configures the time interval (in seconds) that SRV record X may be cached before the record should be consulted again.
dns_cache_a.X.name[2]	Domain name	Blank	It configures the domain name in A record X.
dns_cache_a.X.ip[2]	IP address	Blank	It configures the IP address that the domain name in A record X maps to.
dns_cache_a.X.ttl[2]	Integer from 30 to 2147483647	300	It configures the time interval (in seconds) that A record X may be cached before the record should be consulted again.
static.network.dns.ttl_enable[3]	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to use TTL (Time To Live) in the A record.

static.network.dns.last_cache_expired	Integer from 0 to 65535 **0**-the expired DNS cache can only be used once. After using, the phone will perform a DNS query again. **1 to 65535**-the phone will use the expired DNS cache during the specified period. After that, the phone will perform a DNS query again.	3600	It configures the validity period of the expired DNS cache. **NOTE** It works only if `static.network.dns.last_cache_expired.enable` is set to 1 (Enabled).
static.network.dns.last_cache_expired.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to use the DNS cache (even if the cache has expired) when the DNS server fails to resolve the domain name.

[1] X is the account ID.
[2]X is the record ID. X=1-12.
[3]If you change this parameter, the phone will reboot to make the change take effect.

Example Configuration

The following three examples show you how to configure the static DNS cache.

Example 1

This example shows how to configure a static DNS cache when your DNS server does not return A records. In this case, the static DNS cache on the phone provides A records.

When the static DNS cache is used, the configurations would look as below:

```
account.1.sip_server.1.address = yealink.pbx.com
account.1.sip_server.1.port = 5060
account.1.sip_server.1.transport_type = 3
dns_cache_a.1.name = yealink.pbx.com
dns_cache_a.1.ip = 192.168.1.13
dns_cache_a.1.ttl = 3600
dns_cache_a.2.name = yealink.pbx.com
dns_cache_a.2.ip = 192.168.1.14
dns_cache_a.2.ttl = 3600
```

Example 2

This example shows how to configure a static DNS cache when your DNS server returns A records but not SRV records. In this case, the static DNS cache on the phone provides SRV records.

When the static DNS cache is used, the configurations would look as below:

```
account.1.sip_server.1.address = yealink.pbx.com
account.1.sip_server.1.port = 0
account.1.sip_server.1.transport_type = 3

dns_cache_srv.1.name = _sip._tcp.yealink.pbx.com
dns_cache_srv.1.port = 5060
dns_cache_srv.1.priority = 0
dns_cache_srv.1.target = server1.yealink.pbx.com
dns_cache_srv.1.weight = 1
dns_cache_srv.1.ttl = 3600

dns_cache_srv.2.name = _sip._tcp.yealink.pbx.com
dns_cache_srv.2.port = 5060
dns_cache_srv.2.priority = 0
dns_cache_srv.2.target = server2.yealink.pbx.com
dns_cache_srv.2.weight = 2
dns_cache_srv.2.ttl = 3600
```

ⓘ NOTE

The parameter `account.1.sip_server.1.port` is set to 0 to force the SRV query.

Example 3

This example shows how to configure a static DNS cache when your DNS server returns A and SRV records but not NAPTR records. In this case, the static DNS cache on the phone provides NAPTR records.

When the static DNS cache is used, the configurations would look as below:

```
account.1.sip_server.1.address = yealink.pbx.com
account.1.sip_server.1.port = 0
account.1.sip_server.1.transport_type = 3

dns_cache_naptr.1.name = yealink.pbx.com
dns_cache_naptr.1.flags = S
dns_cache_naptr.1.order = 90
dns_cache_naptr.1.preference = 50
dns_cache_naptr.1.replace = _sip._tcp.yealink.pbx.com
dns_cache_naptr.1.service = SIP+D2T
dns_cache_naptr.1.ttl = 3600

dns_cache_naptr.2.name = yealink.pbx.com
dns_cache_naptr.2.flags = S
dns_cache_naptr.2.order = 100
dns_cache_naptr.2.preference = 50
dns_cache_naptr.2.replace = _sip._udp.yealink.pbx.com
dns_cache_naptr.2.service = SIP+D2U
dns_cache_naptr.2.ttl = 3600
```

ⓘ NOTE

The parameter `account.1.sip_server.1.port` is set to 0 to force NAPTR query.

Logon Wizard

Logon Wizard

Logon wizard allows the phones to provide the logon wizard during the first startup. It works only if there is no registered account on the IP phone.

Logon Wizard Configuration

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

Configuration Parameter

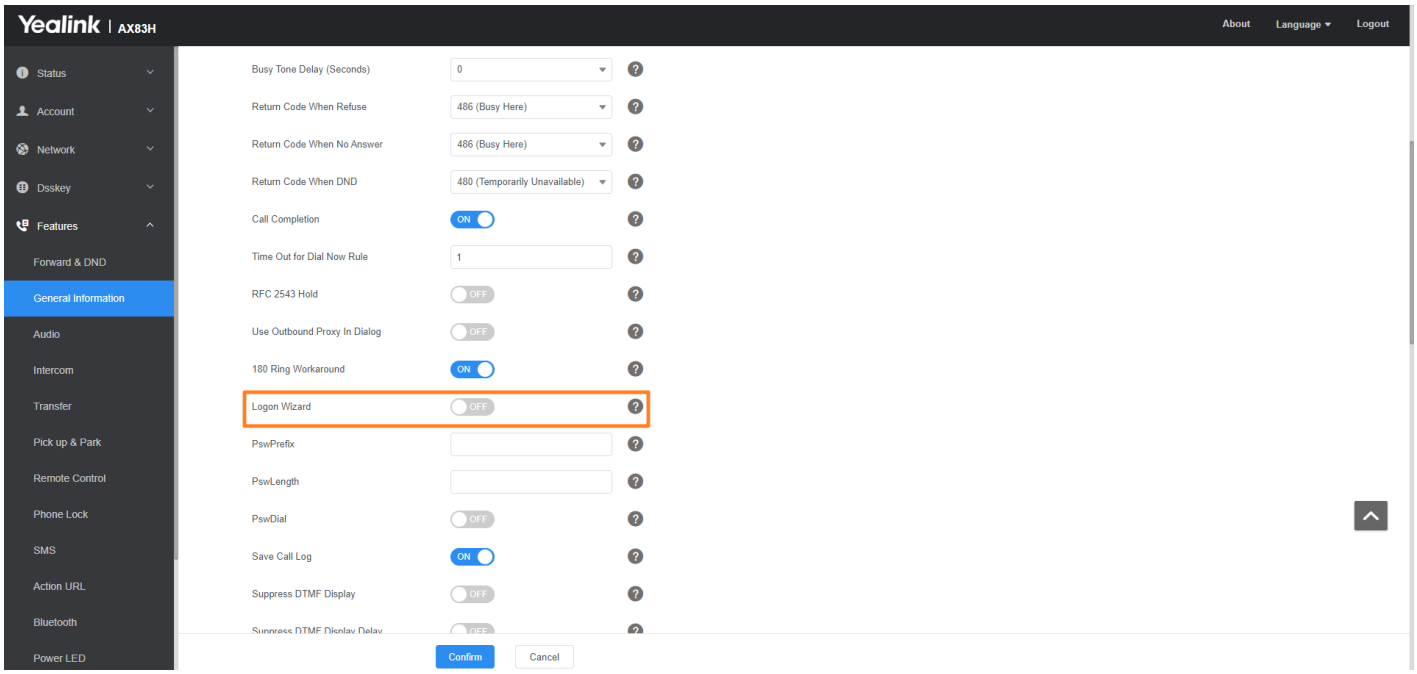
```
phone_setting.logon_wizard
hotdesking.startup_register_name_enable
hotdesking.startup_username_enable
hotdesking.startup_password_enable
hotdesking.startup_sip_server_enable
hotdesking.startup_outbound_enable
phone_setting.logon_wizard_forever_wait
```

Parameter	Description	Permitted Values	Default
phone_setting.logon_wizard	It enables or disables the phone to provide the logon wizard after startup when there is no registered account.	0-Disabled 1-Enabled	0
hotdesking.startup_register_name_enable	It enables or disables the phone to provide an input field of register name on the logon wizard after startup when there is no registered account. **ⓘ NOTE** It works only if "phone_setting.logon_wizard" is set to 1 (Enabled).	0-Disabled 1-Enabled	0
hotdesking.startup_username_enable	It enables or disables the phone to provide an input field of user name on the logon wizard after startup when there is no registered account. **ⓘ NOTE** It works only if "phone_setting.logon_wizard" is set to 1 (Enabled).	0-Disabled 1-Enabled	1

hotdesking.startup_password_enable	It enables or disables the phone to provide an input field of password on the logon wizard after startup when there is no registered account. **NOTE** It works only if "phone_setting.logon_wizard" is set to 1 (Enabled).	0-Disabled 1-Enabled	1
hotdesking.startup_sip_server_enable	It enables or disables the phone to provide an input field of SIP server on the logon wizard after startup when there is no registered account. **NOTE** It works only if "phone_setting.logon_wizard" is set to 1 (Enabled).	0-Disabled 1-Enabled	0
hotdesking.startup_outbound_enable	It enables or disables the phone to provide an input field of the outbound server on the logon wizard after startup when there is no registered account. **NOTE** It works only if "phone_setting.logon_wizard" is set to 1 (Enabled).	0-Disabled 1-Enabled	0
phone_setting.logon_wizard_forever_wait	It enables or disables the phone to remain at the hot desking logon wizard even though timeout.	0-Disabled 1-Enabled	0

Set via the Web User Interface

On the web user interface, go to: **Features** > **General Information** > **Logon Wizard**.



Directory and Call Log

Local Directory

Introduction

Yealink phones maintain a local directory that you can use to store contacts. The local directory can store up to 1000 contacts and 48 groups.
Contacts and groups can be added either one by one or in batches using a local contact file. Yealink phones support both *.xml and *.csv format contact files, but you can only customize the *.xml format contact file.

Local Contact File Customization

You can ask the distributor or Yealink FAE for a local contact template. You can also refer to the following template:

```
<?xml version="1.0" encoding="utf-8"?>
<root_group>
 <group display_name="All Contacts" ring="" />
 <group display_name="Blacklist" ring="" />
</root_group>
<root_contact>
 <contact display_name="Test1" office_number="2510" mobile_number="2511" other_number="3610" line="1" ring="" g
 <contact display_name="Test2" office_number="3510" mobile_number="3511" other_number="3620" line="2" ring="" g
</root_contact>
```

Local Contact File Elements and Attributes

The following table lists the elements and attributes you can use to add groups or contacts in the local contact file. We recommend that you do not edit these elements and attributes.

Elements	Attributes	Description
Contact	display_name	Specify the contact name. For example Some characters (for example, ") are key syntax markers and may never appear in the content. Non-standard name formats may cause XML parsing to fail. You can use the escape sequence instead. Error: display_name="Hurrell "&" Mclean" Correct 1: display_name="Hurrell & Mclean" Correct 2: display_name="Hurrell & amp; Mclean" **NOTE** The contact name cannot be blank.
	office_number	Specify the office number
	mobile_number	Specify the mobile number
	other_number	Specify the other number

Customize Local Contact File

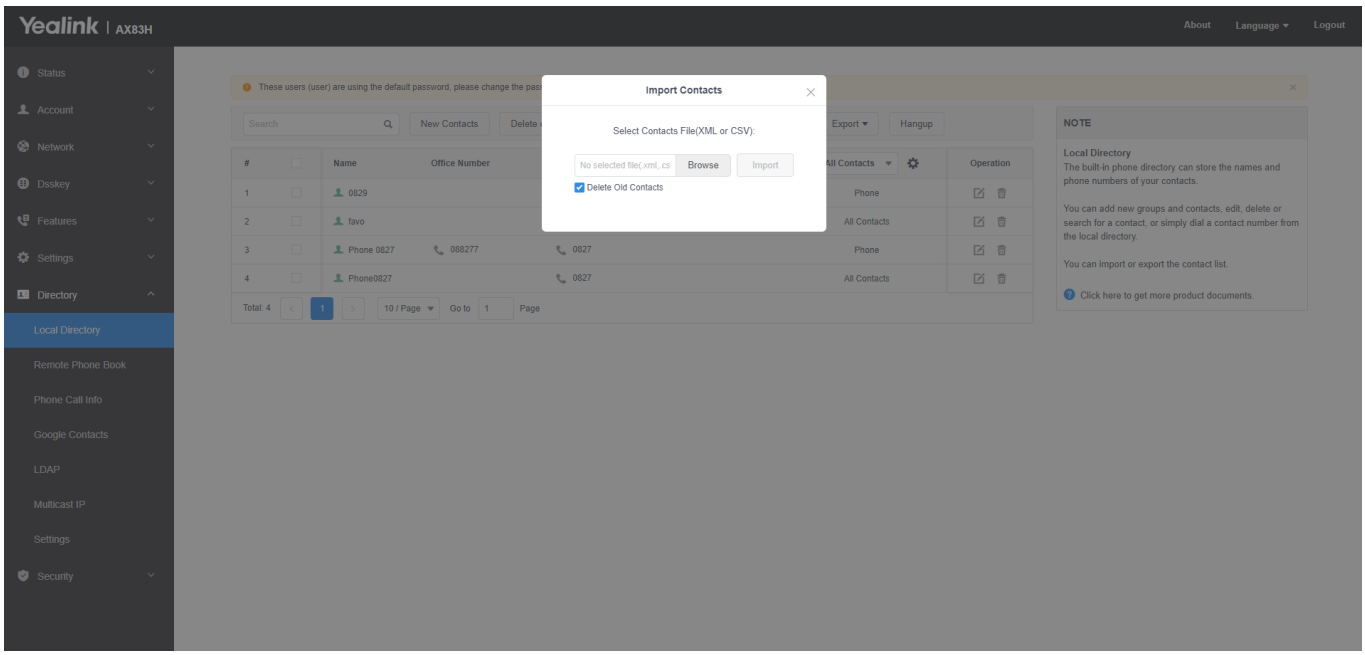
1. Open the local contact file.
2. To add a contact, add <contact display_name="" office_number="" mobile_number="" other_number=""/> to the file. Each starts on a new line.
3. Specify the values within double quotes.
   For example:
   <contact display_name="Lily"office_number="1020" mobile_number="1021" other_number="1112"/>
   <contact display_name="Tom" office_number="2020" mobile_number="2021" other_number="2112"/>
4. Save the changes and place this file to the provisioning server.

Local Contact Files and Resource Upload

You can upload local contact files to add multiple contacts at a time.

Set via the Web User Interface

1. On the web user interface, go to **Directory** > **Local Directory** > **Import** > **Import Contacts**



Configuration Parameter

```
handset.X.contact_list.url
features.local_directory_number.type
features.local_directory.overwrite
```

Parameter	Permitted Values	Default	Description
handset.X.contact_list.url[1]	URL within 511 characters	Blank	It configures the access URL of the contact file of a specific handset.
features.local_directory_number.type	1: No restrictions, can enter string type. 2: Only pure digits can be entered.	1	It is used to configure the required input content for manually adding local contacts.
features.local_directory.overwrite	**1**: Overwrite **0**: Not overwrite	1	It is used to configure whether to overwrite the existing address book on the phone when importing the local contact address book.

[1] X is the account ID.

Local Contacts Backup

Yealink phones support storing all local contacts to a contact file named `<MAC>-contact.xml`. You can back up this file to the server, avoiding data loss. Once the contacts update, the phone will automatically upload this file to the provisioning server or a specific server. If a contact file exists on the server, this file will be overridden. The phone will request to download the `<MAC>-contact.xml` file according to its MAC address from the server during auto

provisioning.The contact file is named after the MAC address of the IP phone. For example, if the MAC address of an IP phone is 00156574B150, the name of the contact file is 00156574B150-contact.xml (uppercase).

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

Configuration Parameter

The following table lists the parameters you can use to back up the local contacts.

```
static.auto_provision.local_contact.backup.enable
static.auto_provision.local_contact.backup.path
static.auto_provision.custom.upload_method
```

Parameter	Description	Permitted Values	Default
static.auto_provision.local_contact.backup.enable	It enables or disables the phone to upload the <MAC>-contact.xml file to the server each time the contacts update and download the <MAC>-contact.xml file from the server during auto provisioning. **NOTE** It does not affect the downloading of the contact avatar/icon files.	0-Disabled, the phone will not upload the contact file "<MAC>-contact.xml" to the server, so the IP phone downloads the contacts in the "contact.xml" from the access URL configured by the parameter "local_contact.data.url" or "local_contact.data_photo_tar.url" during auto-provisioning. 1-Enabled, the phone uploads the contact file "<MAC>-contact.xml" to the specific path configured by the parameter "static.auto_provision.local_contact.backup.path" each time the contacts update; and download the contacts in the "<MAC>-contact.xml" according to its MAC address from the specific path during auto-provisioning.	0

static.auto_provision.local_contact.backup.path	It configures a path or URL for the phone to upload/download the <MAC>-contact.xml file. If it is left blank, the phone connects to the provisioning server URL, and uploads/downloads the contact file "<MAC>-contact.xml". Example: static.auto_provision.local_contact.backup.path = http://192.168.1.20/contact%3Cbr />Once the contacts update, the phone will upload the contact file to the specified path "http://192.168.1.20/contact".%3Cbr />During auto-provisioning, the phone downloads the contact file "<MAC>-contact.xml" from the specified path "http://192.168.1.20/contact". **NOTE** It works only if "static.auto_provision.local_contact.backup.enable" is set to 1 (Enabled).	String	Blank
static.auto_provision.custom.upload_method	It configures the way the phone uploads the <MAC>-local.cfg file, <MAC>-calllog.xml file or <MAC>-contact.xml file to the provisioning server (for HTTP/HTTPS server only).	0-PUT 1-POST	0

Directory List for DirectoryDir Soft Key

Directory List for Directory/Dir Soft Key

Users can access frequently used directory lists by pressing the Directory/Dir soft key when the IP phone is idle. The lists include Local Directory, History, Remote Phone Book, and Blocklist by default.
You can add the desired lists to the directory list using a directory list file (favorite_setting.xml).

Directory List File Customization

You can ask the distributor or Yealink FAE for a directory template. You can also refer to the following template:

```
<?xml version="1.0"?>
<root_favorite_set>
   <item id_name="localdirectory" display_name="Local Directory" priority="1" enable="1" dev="common"/>
   <item id_name="history" display_name="History" priority="2" enable="0" dev="common"/>
   <item id_name="networkcalllog" display_name="Network Call Log" priority="3" enable="0" dev="common"/>
   <item id_name="remotedirectory" display_name="Remote Phone Book" priority="4" enable="0" dev="common"/>
   <item id_name="ldap" display_name="LDAP" priority="5" enable="0" dev="T19 T21 T23 T40 T40G T27 T27G T29 T41
   <item id_name="broadsoftdirectory" display_name="Network Directory" priority="6" enable="0" dev="common"/>
 <item id_name="plcmdirectory" display_name="Phonebook" priority="7" enable="0" />
 <item id_name="gabdirectory" display_name="Global Address Book" priority="8" enable="0" />
 <item id_name="pabdirectory" display_name="Personal Address Book" priority="9" enable="0" />
 <item id_name="metaswitchcontacts" display_name="Network Contacts" priority="10" enable="0" />
 <item id_name="metaswitchcalllog" display_name="Network Call List" priority="11" enable="0" />
 <item id_name="uc_buddies" display_name="Buddies" priority="12" enable="0" dev="T29 T46 T46S T54S T52 T48 T48S
 <item id_name="mobilecontant" display_name="Mobile Contacts" priority="13" enable="1" dev="T29 T46 T46S T54S T5
 <item id_name="blacklist" display_name="Blacklist" priority="14" enable="0" />
 <item id_name="googledirectory" display_name="Google Contacts" priority="15" enable="0" />
 <item id_name="sharedirectory" display_name="Shared Directory" priority="16" enable="0" dev="T54W T53W T53 T57
 <item id_name="dectintercom" display_name="Dect Intercom" priority="17" enable="0" dev="T54W T53W T53 T57W" /
 <item id_name="presencelist" display_name="Presence List" priority="18" enable="1"  />
 <item id_name="uc_calllog" display_name="Network CallLog" priority="19" enable="0"  />
</root_favorite_set>
```

The following table lists the attributes you can use to add contact lists to the directory list file. We recommend that you do not edit these attributes.

Attributes	Valid Values	Description

id_name	localdirectory history networkcalllog remotedirectory ldap broadsoftdirectory plcmdirectory gabdirectory pabdirectory metaswitchcontacts metaswitchcalllog uc_buddies mobilecontant blocklist googledirector presencelist	The existing directory list (For example, “localdirectory” for the local directory list). Note: Do not edit this field.

display_name	Local Directory History Network CallLog Remote Phone Book LDAP Network Directories PhoneBook Global Address Book Personal Address Book Network Contacts Network Call List Buddies Mobile Contacts Blocklist Google Contact Presence List	The display name of the directory list. Note: We recommend that you do not edit this field. Network Directories and Network CallLog lists are hidden for phones in GA firmware, GA firmware which is designed for the BroadWorks environment.
priority	1 to 18 1 is the highest priority.	The display priority of the directory list. Note: This attribute is not applicable for T57W/T48U/T48S/CP925/CP935W.
enable	0/1 0: Disabled 1: Enabled	Whether to display this list when you press Directory (Dir) on the phone.
dev	common	The applicable phone models of the directory list. Note: Do not edit this field.

Customizing Directory List File

1. Open the directory list XML file.

2. To configure each directory list, edit the values within double quotes in the corresponding field.
   For example, enable the local directory, disable the history and specify a priority.
   <item id_name="localdirectory" display_name="Local Directory" priority="1" enable="1" dev="common"/>
   <item id_name="history" display_name="History" priority="2" enable="0" dev="common"/>
   Save the change and place this file to the provisioning server.

Directory List Configuration

Configuration parameter

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

```
static.directory_setting.url
directory_setting.local_directory.enable
directory_setting.local_directory.priority
directory_setting.history.enable
directory_setting.history.priority
directory_setting.remote_phone_book.enable
directory_setting.remote_phone_book.priority
directory_setting.ldap.enable
directory_setting.ldap.priority
```

Parameter	Description	Permitted Values	Default
static.directory_setting.url	It configures the access URL of the custom directory file (favorite_setting.xml).	URL within 511 characters	Blank
directory_setting.local_directory.enable	It enables or disables the users to access the local directory by pressing the Directory/Dir soft key.	0-Disabled 1-Enabled	1
directory_setting.local_directory.priority	It configures the display priority of the local directory.	Integer greater than or equal to 0	1
directory_setting.history.enable	It enables or disables the users to access the history by pressing the Directory/Dir soft key.	0-Disabled 1-Enabled	0
directory_setting.history.priority	It configures the display priority of the call log list.	Integer greater than or equal to 0	2
directory_setting.remote_phone_book.enable	It enables or disables the users to access the remote phone book by pressing the Directory/Dir soft key.	0-Disabled 1-Enabled	0
directory_setting.remote_phone_book.priority	It configures the display priority of the remote phone book.	Integer greater than or equal to 0	4
directory_setting.ldap.enable	It enables or disables the users to access the LDAP by pressing the Directory/Dir soft key.	0-Disabled 1-Enabled	0

directory_setting.ldap.priority	It configures the display priority of the LDAP.	Integer greater than or equal to 0	5

Example: Configuring a Directory List

The following example shows the configuration for the directory list.

Customize the directory list file, and then place this file to the provisioning server “http://192.168.10.25”.

Example

static.directory_setting.url = http://192.168.10.25/favorite_setting.xml

After provisioning, you can press the Directory/Dir soft key to access the desired contact list quickly.

Enterprise Directory Configuration

Enterprise Directory Configuration

The following table lists the parameters that the phone can use to configure the enterprise directory.

Configuration Parameter

```
features.enterprise_directory.enable
features.enterprise_directory.host
features.enterprise_directory_photo.host
features.enterprise_directory.authentication_type
features.enterprise_directory.user
features.enterprise_directory.password
```

Parameter	Description	Permitted Values	Default
features.enterprise_directory.enable	It enables or disables the Huawei enterprise directory feature.	0-Disabled 1-Enabled	0

features.enterprise_directory.host	It configures the IP address of the enterprise directory server. You need to configure the complete address (port is required), such as https://11.11.182.202/ser vices:443. **NOTE** It works only if "features.enterprise_directory.enable" is set to 1 (Enabled).	String	Blank
features.enterprise_directory_photo.host	It configures the IP address of the contact avatars of the enterprise contacts. You need to configure the complete address, such as https://11.11.182.202/photo. **NOTE** It works only if "features.enterprise_directory.enable" is set to 1 (Enabled).	String	Blank
features.enterprise_directory.authentication_type	It configures the authentication type of the enterprise contact. **NOTE** It works only if "features.enterprise_directory.enable" is set to 1 (Enabled).	0-SIP authentication, use account 1 information to authenticate by default 1-Authentication information can be configured separately	0
features.enterprise_directory.user	It configures the user name used for authentication of the enterprise directory. **NOTE** It works only if "features.enterprise_directory.authentication_type" is set to 1.	String	Blank

features.enterprise_directory.password	It configures the password used for authentication of the enterprise directory. **ⓘ NOTE** It works only if "features.enterprise_directory.authentication_type" is set to 1.	String	Blank

Lightweight Directory Access Protocol (LDAP)

Introduction

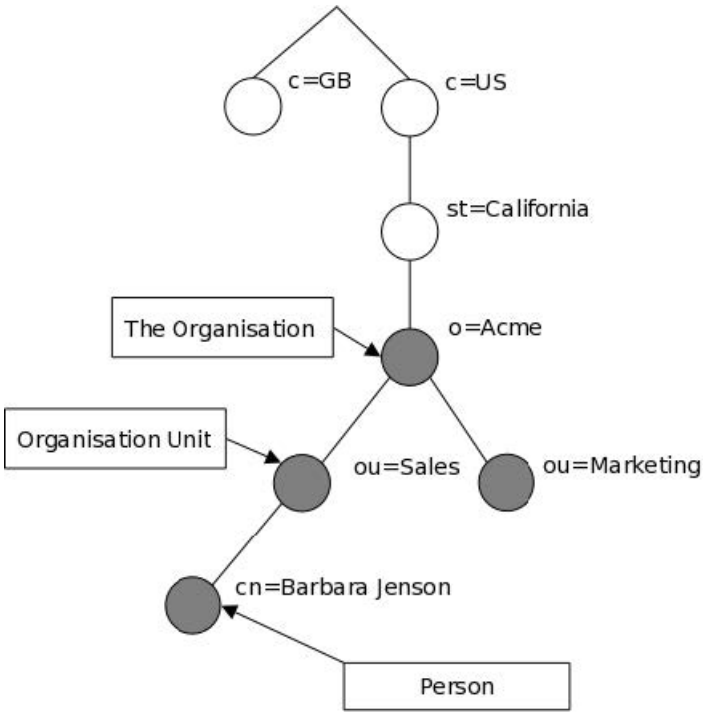
LDAP (Lightweight Directory Access Protocol) is a client/server protocol for accessing a directory service. LDAP is a directory service protocol that runs over TCP/IP.

What kind of information can be stored in the directory?

The LDAP information model is based on entries. An entry is a collection of attributes that has a globally unique Distinguished Name (DN). The DN is used to refer to the entry unambiguously. Each of the entry's attributes has a type and one or more values. The types are typically mnemonic strings, like "cn" for the common name, or "mail" for the email address. The syntax of values depends on the attribute type. For example, a cn attribute might contain the value “Babs Jensen”. A mail attribute might contain the value "babs@example.com".

How is the information arranged?

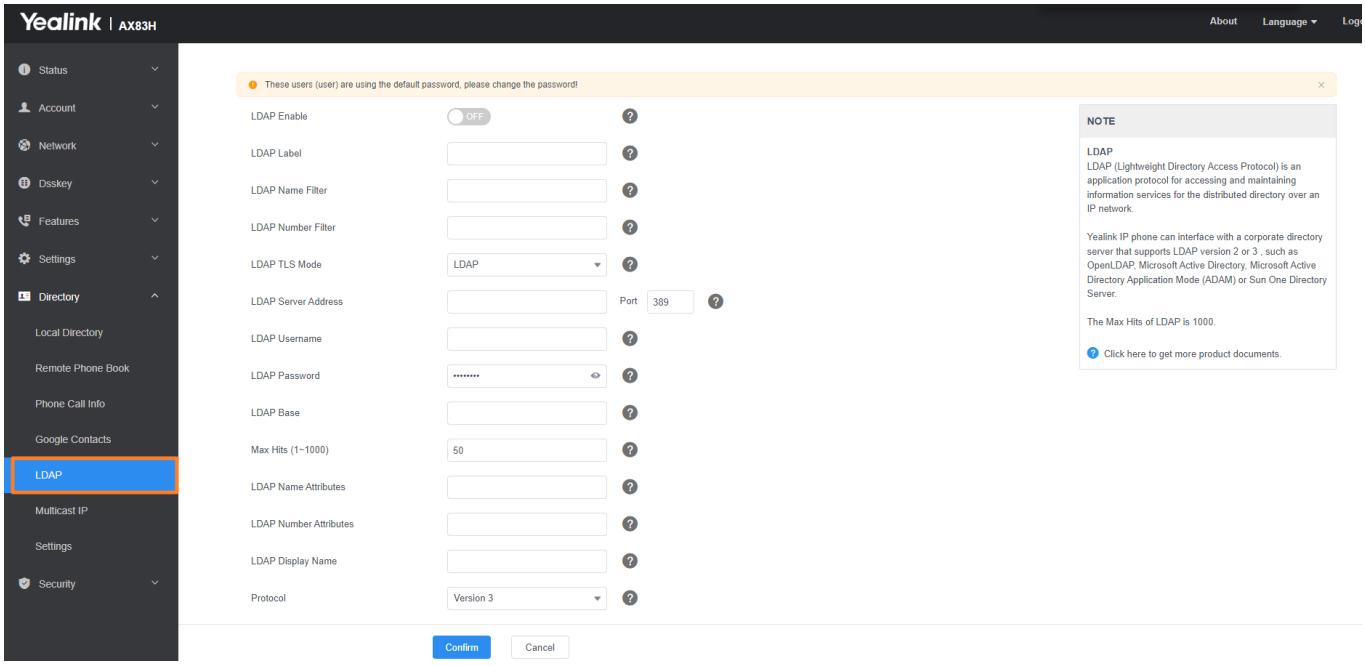
In LDAP, directory entries are arranged in a hierarchical tree-like structure. Traditionally, this structure reflected the geographic and/or organizational boundaries. Entries representing countries appear at the top of the tree. Below them are entries representing states and national organizations. Below them might be entries representing organizational units, people, printers, documents, or just about anything else you can think of. The following shows an example of an LDAP directory tree using traditional naming.



Configure Yealink Phones

Set via the Web User Interface

1. On the web user interface, go to **Directory** > **LDAP** > **LDAP enable**, and then enter the desired values in the corresponding fields.



Example for Web User Interface Configuration

You can use the following settings as a starting point and adjust the filter and display attributes according to your requirements. The following shows an example of OpenLDAP phone configurations.

```
Enable LDAP: Enabled
LDAP Name Filter: (|(cn=%)(sn=%))
LDAP Number Filter: (|(telephoneNumber=%)(mobile=%)(ipPhone=%))
LDAP TLS Mode: LDAP
Server Address: 10.3.6.128
Port: 389
Base: dc=yealink,dc=com
Username: cn=Manager,dc=yealink,dc=com
Password: secret
Max Hits (1~32000): 50
LDAP Name Attributes: cn sn
LDAP Number Attributes: mobile telephoneNumber ipPhone
LDAP Display Name: %cn
Protocol: Version 3
LDAP Lookup For Incoming Call: Enabled
LDAP Lookup For Callout: Enabled
LDAP Sorting Results: Enabled
```

Configuration Parameter

```
ldap.enable
ldap.name_filter
ldap.number_filter
ldap.tls_mode
ldap.host
ldap.port
ldap.base
ldap.user
ldap.password
ldap.max_hits
ldap.name_attr
ldap.numb_attr
ldap.display_name
ldap.version
ldap.call_in_lookup
ldap.call_out_lookup
ldap.ldap_sort
ldap.incoming_call_special_search.enable
ldap.customize_label
ldap.search_scope
ldap.search_scope
ldap.search_t9.enable
ldap.search_timeout
```

Parameter	Permitted Values	Default	Description
ldap.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the LDAP feature.

ldap.name_filter	String within 99 characters	Blank	It configures the search criteria for LDAP contact names lookup. The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the name entered by the user. **Example:** 1. `ldap.name_filter = (|(cn=%)(sn=%))` When the cn or sn of the LDAP contact matches the entered name, the record will be displayed on the phone screen. 2. `ldap.name_filter = (&(cn=*)(sn=%))` When the cn of the LDAP contact is set and the sn of the LDAP contact matches the entered name, the records will be displayed on the phone screen. 3. `ldap.name_filter = (!(cn=%))` When the cn of the LDAP contact does not match the entered name, the records will be displayed on the phone screen.
ldap.number_filter	String within 512 characters	Blank	It configures the search criteria for LDAP contact numbers lookup. The "*" symbol in the filter stands for any number. The "%" symbol in the filter stands for the number entered by the user. **Example:** 1. `ldap.number_filter = (|(telephoneNumber=%)(mobile=%)(ipPhone=%))` When the number of the telephoneNumber, mobile or ipPhone of the contact record matches the search criteria, the record will be displayed on the phone screen. 2. `ldap.number_filter = (&(telephoneNumber=*)(mobile=%))` When the telephoneNumber of the LDAP contact is set and the mobile of the LDAP contact matches the entered number, the record will be displayed on the phone screen.

ldap.tls_mode	**0**-LDAP—The unencrypted connection between the LDAP server and the IP phone (port 389 is used by default). **1**-LDAP TLS Start—The TLS/SSL connection between the LDAP server and the IP phone (port 389 is used by default). **2**-LDAPs—The TLS/SSL connection between the LDAP server and the IP phone (port 636 is used by default).	0	It configures the connection mode between the LDAP server and the phone.
ldap.host	IP address or domain name	Blank	It configures the IP address or domain name of the LDAP server.
ldap.port	Integer from 1 to 65535	389 (LDAPS: 636)	It configures the port of the LDAP server.
ldap.base	String within 512 characters	Blank	It configures the LDAP search base which corresponds to the location of the LDAP phonebook from which the LDAP search request begins. The search base narrows the search scope and decreases directory search time. **Example:** `ldap.base = dc=yealink,dc=cn`
ldap.user	String within 512 characters	Blank	It configures the user name used to log into the LDAP server. This parameter can be left blank in case the server allows anonymity to log into. Otherwise, you will need to provide the user name to log into the LDAP server. **Example:** `ldap.user = cn=manager,dc=yealink,dc=cn`
ldap.password	String within 512 characters	Blank	It configures the password to log into the LDAP server. This parameter can be left blank in case the server allows anonymous to log into. Otherwise, you will need to provide the password to log into the LDAP server.
ldap.max_hits	Integer from 1 to 1000	50	It configures the maximum number of search results to be returned by the LDAP server.

ldap.name_attr	String within 512 characters	Blank	It configures the name attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple name attributes separated by spaces. **Example:** ldap.name_attr = cn sn This requires the "cn" and "sn" attributes set for each contact record on the LDAP server.
ldap.numb_attr	String within 512 characters	Blank	It configures the number attributes of each record to be returned by the LDAP server. Multiple number attributes are separated by spaces. **Example:** ldap.numb_attr = mobile ipPhone This requires the "mobile" and "ipPhone" attributes set for each contact record on the LDAP server.
ldap.display_name	String within 512 characters	Blank	It configures the display name of the contact record displayed on the phone screen. The value must start with a "%" symbol. **Example:** ldap.display_name = %cn The cn of the contact record is displayed on the phone screen.
ldap.version	2 or 3	3	It configures the LDAP protocol version supported by the IP phone. The version must be the same as the version assigned on the LDAP server.
ldap.call_in_lookup	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to perform an LDAP search when receiving an incoming call.
ldap.call_out_lookup	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to perform an LDAP search when placing a call.
ldap.ldap_sort	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to sort the search results in alphabetical order or numerical order.

ldap.incoming_call_special_search.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to search the telephone numbers starting with ”+” symbol and “00” from the LDAP server if the incoming phone number starts with”+” or “00”. When completing the LDAP search, all the search results will be displayed on the phone screen. **Example:** If the phone receives an incoming call from the phone number 0044123456789, it will search 0044123456789 from the LDAP server first, if no result found, it will search +44123456789 from the server again. The phone will display all the search results. **NOTE** It works only if ldap.call_in_lookup is set to 1 (Enabled). You may need to set “ldap.name_filter” to be (|(cn=%)(sn=%)(telephoneNumber=%)(mobile=%)) for searching the telephone numbers starting with ”+” symbol.
ldap.customize_label	String within 512 characters	Blank	It configures the display name of the LDAP phone book. If it is left blank, LDAP is displayed. **NOTE** It works only if ldap.enable is set to 1 (Enabled).
ldap.search_scope	sub-A recursive search of all levels below the base domain name is performed. one-A search of one level below the base domain name is performed. base-A search at the base domain name level is performed.	sub	It controls the search scope when searching for LDAP contact.
ldap.search_t9.enable	**0**-Disabled **1**-Enabled	0	It is used to configure whether to enable LDAP T9 search.
ldap.search_timeout	int	15	It is used to configure the timeout duration for LDAP request server search results.

Errors and Solutions

Error	Description	Solution
0x00030000000060001 Operations error	Server error. The error code returned by the LDAP server is unknown.	Check the server.
0x00030000000060002 Protocol error	Phone compatibility error. The protocol version between the phone and the LDAP server does not match.	1. Puch the configuration line ***ldap.version=2*** to the phone to check whether the problem can be solved. 2. If the problem cannot be solved, please check the server or provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x00030000000060003 Time limit exceeded	Server error. Server processing timeout.	Check the server.
0x00030000000060004 Size limit exceeded	Server error. The number of attributes requested by the phone exceeds the server limits.	Change the server limits on the number of attributes.
0x00030000000060005 Compare False	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000060006 Compare True	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000060007 Authentication method not supported	Phone error. The server does not support the authentication method of the phone LDAP request.	1. Check whether the authentication password of the phone LDAP is correct. 2. Check the LDAP connection method. If it is LDAPS, you need to upload the server CA certificate from the phone end, and the CA's Common Name should be consistent with the LDAP server. 3. If the above methods do not solve the problem, please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x00030000000060008 Strong(er) authentication required	Phone compatibility error. The phone authentication methods do not meet the server requirements.	Check the server or please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.

0x000300000006000a Referral	Server error. The server is temporarily unavailable to handle this request.	Check the server.
0x000300000006000b Administrative limit exceeded	Server error. The time taken by the LDAP searching exceeds the maximum limit allowed by the server.	1. Change the maximum time limit of the server. 2. Reduce the phone filters to check whether the problem can be solved. 3. If the above methods do not solve the problem, please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x000300000006000c Critical extension is unavailable	Phone compatibility error. The server does not support some attribute items requested by the phone.	Please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x0003000000060010 No such attribute	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060011 Undefined attribute type	Server compatibility error. The server has not defined some attribute items requested by the phone.	1. Check the server. 2. Please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x0003000000060012 Inappropriate matching	Phone configuration error. The server does not support the filter requested by the phone.	1. Check whether the phone filter setting is correct. 2. Please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x0003000000060013 Constraint violation	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060014 Type or value exists	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060015 Invalid syntax	Phone configuration error. The phone LDAP filter syntax is invalid.	Please check the syntax format of the LDAP filter. For more information on the standards, see https://ldap.com/ldap-filters/.
0x0003000000060022 Invalid DN syntax	Phone configuration error. The DN format is invalid.	Please check the phone *ldap.abse* configuration. For more information on the standards, see https://ldap.com/ldap-dns-and-rdns/.

0x00030000000060024 Alias dereferencing problem	Server error.	Check the server.
0x00030000000060030 Inappropriate authentication	Phone error. The server does not support the authentication method of the phone LDAP request.	1. Check whether the authentication password of the phone LDAP is correct. 2. Check the LDAP connection method. If it is LDAPS, you need to upload the server CA certificate from the phone end, and the CA's Common Name should be consistent with the LDAP server. 3. If the above methods do not solve the problem, please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x00030000000060031 Invalid credentials	Phone configuration error, the authentication information carried in the LDAP request is invalid.	1. Please check that if the password of LDAP is correct. 2. If you use LDAPs, please upload the CA of the server to the phone.
0x00030000000060032 Insufficient access	Server error. The server refuses the phone access.	Check whether the server has enabled the access permission for the phone.
0x00030000000060033 Server is busy	Server error. The server is busy.	1. Try again 10 minutes later. 2. If the above method does not solve the problem, check the server.
0x00030000000060034 Server is unavailable	Server error. The server is unavailable.	1. Try again 10 minutes later. 2. If the above method does not solve the problem, check the server.
0x00030000000060035 Server is unwilling to perform	Server error. The server is unwilling to perform the action.	Check the server.
0x00030000000060036 Loop detected	Server error. The server takes the current request as a loop.	1. Check the server. 2. If the server can work as usual, please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x00030000000060050 Other (e.g., implementation specific) error	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.

0x00030000000600c7 Can't contact LDAP server	Phone configuration or compatibility error. The phone cannot connect to the LDAP server.	1. Check whether the server address, port number, and authentication password of the phone LDAP are correct. 2. When you use the LDAPS connection, you need to upload the server CA certificate from the phone end, and the CA's Common Name should be consistent with the LDAP server. 3. If the above methods do not solve the problem, please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x00030000000600c6 Local error	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600c5 Encoding error	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600c4 Decoding error	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600c3 Timed out	Server or network error. The phone exceeds the time limit when waiting for a response.	1. Push the configuration line ldap.connect_expires= to the phone to change the time limit (it defaults to 5 s). 2. If the phone stays in the time-out status for a long time, check whether the server works normally.
0x00030000000600c2 Unknown authentication method	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600c1 Bad search filter	Phone configuration error. The format of the phone LDAP Filter is incorrect.	Check the configuration format of the LDAP Filter. For more information on the standards, see https://ldap.com/ldap-filters/.
0x00030000000600c0 User cancelled operation	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600bf Bad parameter to an ldap routine	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.

0x000300000000600be Out of memory	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x000300000000600bd Connect error	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x000300000000600bc Not Supported	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x000300000000600ba No results returned	The server error. The server does not return the request result.	1. Check the server. 2. If the server can work as usual, provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x000300000000600b9 More results to return	Server error. The server returns too many results that exceed the limits.	Check the server (generally, this error does not happen).
0x000300000000600b8 Client Loop	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x000300000000600b7 Referral Limit Exceeded	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x000300000000600b7 Referral Limit Exceeded	Phone configuration error. The format of the LDAP attribute is invalid.	Check the configuration format of ldap.name_filter and ldap.number_filter. For more information on the standards, see https://ldap.com/ldap-filters/. **NOTE** The % symbol in the Yealink phone filter configuration equals *. Therefore, you need to configure the % symbol rather than *.
0x000300000000600b7 Referral Limit Exceeded	Certificate error. The certificate CN fails to be authenticated. The CN value in the server CA certificate is not consistent with the one in the LDAP server.	Keep the CN value in the phone LDAP server consistent with the one in the CA certificate.

0x000300000006012e Certificates error	Certificate error. The phone does not detect the correct CA certificate.	Upload the correct server CA certificate to the phone.
0x000300000006012f Domain name resolution failed	Phone configuration or network error. LDAP Server cannot be resolved.	1. If other devices can access the LDAP server, you can put the faulty phone under the same network of other devices to verify whether it is a network error. If it is, please check the network. 2. Change the IP address of the LDAP server to a static IP.
0x00030000000060130	Phone compatibility error. The phone and the server fail to negotiate a TLS algorithm when using LDAPS.	1. Adjust the server algorithm. 2. Yealink FAE will also do further analysis to give you a solution ASAP.
0x00030000000060131	Phone compatibility error. The phone and the server fail to negotiate a TLS protocol version when using LDAPS.	1. Change the phone TLS protocol version by pushing the configuration line `security.default_ssl_method`. The default value is 3. Auto adjustment to the version below 1. 2 is supported. 4 represents only supporting TlS 1.1; 5 represents only supporting TLS 1.2; 6 represents only supporting TLS 1.3. 2. If the above method does not solve the problem, please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.

Install and Configure the LDAP Server

An LDAP server is essentially a bit like an SQL server, which is mainly used for storing/retrieving information about people (such as contacts). The configuration settings on the phone will be altered depending on how the LDAP server is configured.
Before using the LDAP feature on IP phones, you must make sure the LDAP server is prepared properly, otherwise, you need to install and configure an LDAP server.

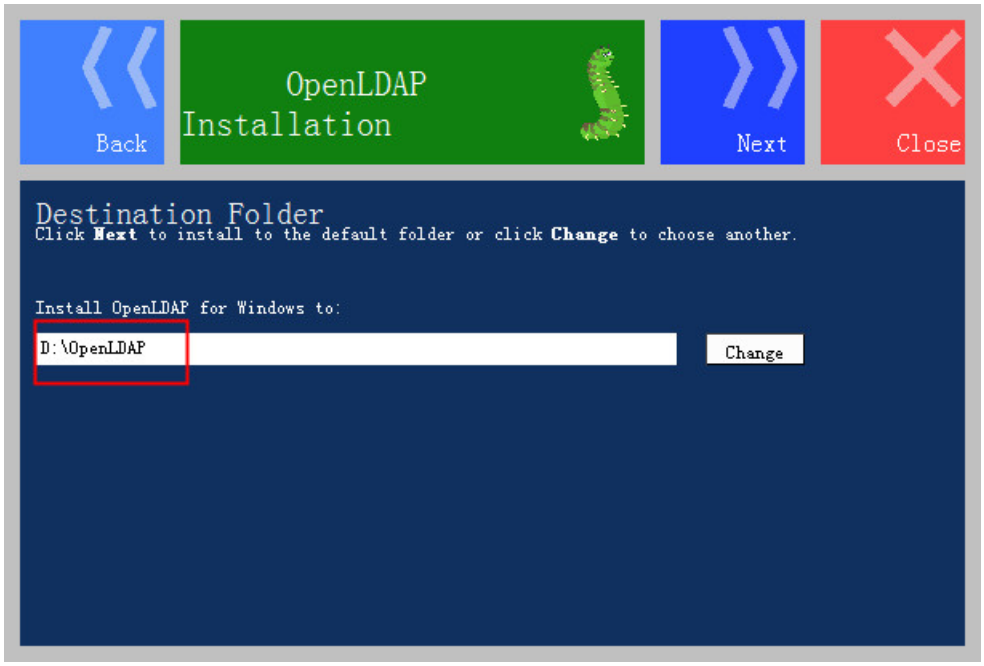
OpenLDAP

Install the OpenLDAP Server

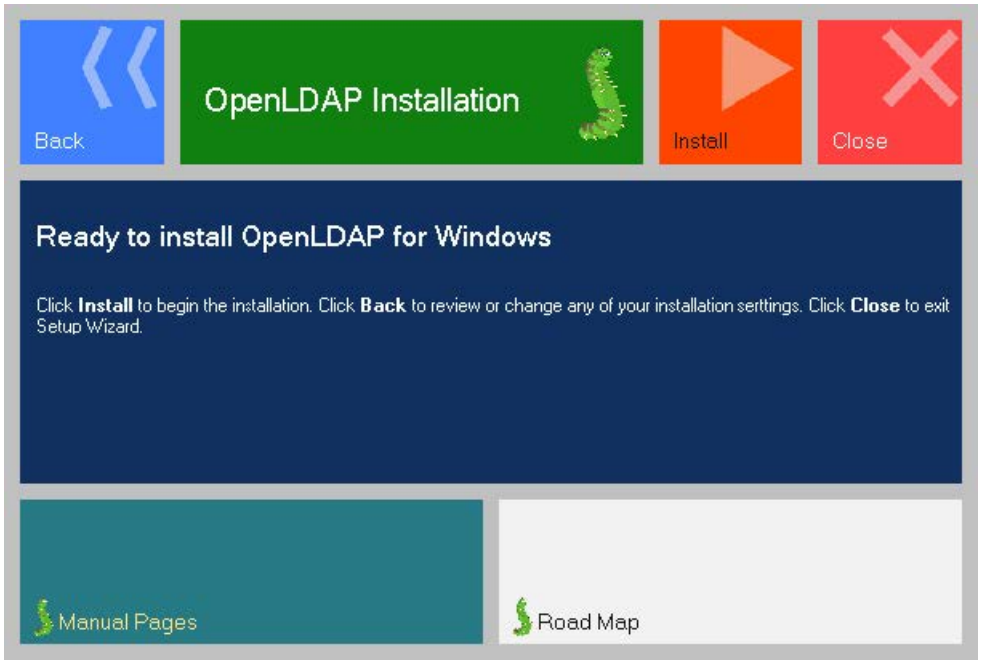
This section shows you how to install an OpenLDAP server on Microsoft Windows 2007 system. The OpenLDAP server software is available for free.
You can download it from http://www.userbooster.de/en/download/openldap-for-windows.aspx?l=en.
To install the OpenLDAP server:

1. Double-click the OpenLDAP application to start the installation. You will be prompted for the installation.

2. Click **Yes** to continue the installation.
3. Follow the default settings and click **Next** until the **Destination Folder** screen appears.
4. Click **Change** to locate the installation path from the local computer system and then click **Next**.
   You need to remember the installation path (e.g., D:\OpenLDAP) located here.
   The screenshot for reference is shown below:



5. Follow the default settings and click **Next** until the **Ready to install OpenLDAP for Windows** screen appears.



6. Click **Install** to start the installation.
7. Click **Close** to exit the Setup Wizard.

   For more information on how to install the OpenLDAP server for windows, refer to the website online: http://www.userbooster.de/en/support/feature-articles/openldap-for-windows-installation.aspx.

Configure the OpenLDAP Server

Edit the slapd.conf File

Access the OpenLDAP installation path. Edit the manager information for LDAP.

1. Open and edit the slapd.conf file using your favorite text editor.

   Find the commands

   ```
   Suffix "dc=maxcrc, dc=com"
   Rootdn "cn=Manager,dc=maxcrc,dc=com"
   ```

   Suffix defines the components of the domain name.

   Rootdn defines the manager as a management user for accessing the LDAP server.

   For example:

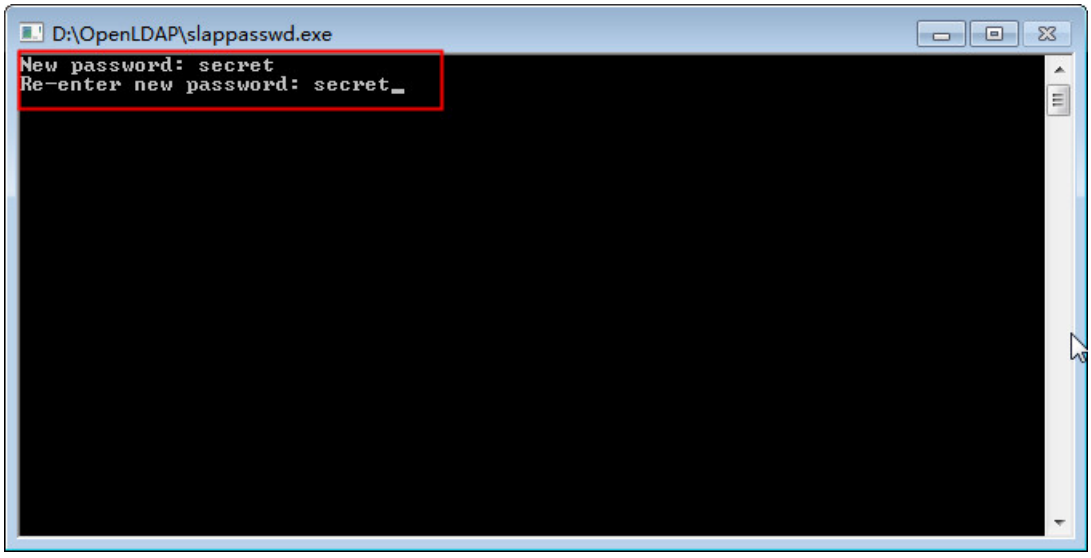
   ```
   Suffix "dc=yealink,dc=com"
   Rootdn "cn=Manager,dc=yealink,dc=com "
   ```

   The suffix line means that the domain name of the LDAP directory is yealink.com. The Rootdn line defines a management user named as Manager.

   If the domain name contains additional components, for example, yealink.com.cn, the suffix line will be edited as below:

   ```
   Suffix "dc=yealink,dc=com,dc=cn"
   Rootdn "cn=Manager,dc=yealink,dc=com,dc=cn"
   ```

2. Double-click slappasswd.exe to modify the user password for the management user. Type the new password twice.



Start the Slapd Service

To start the slapd service:

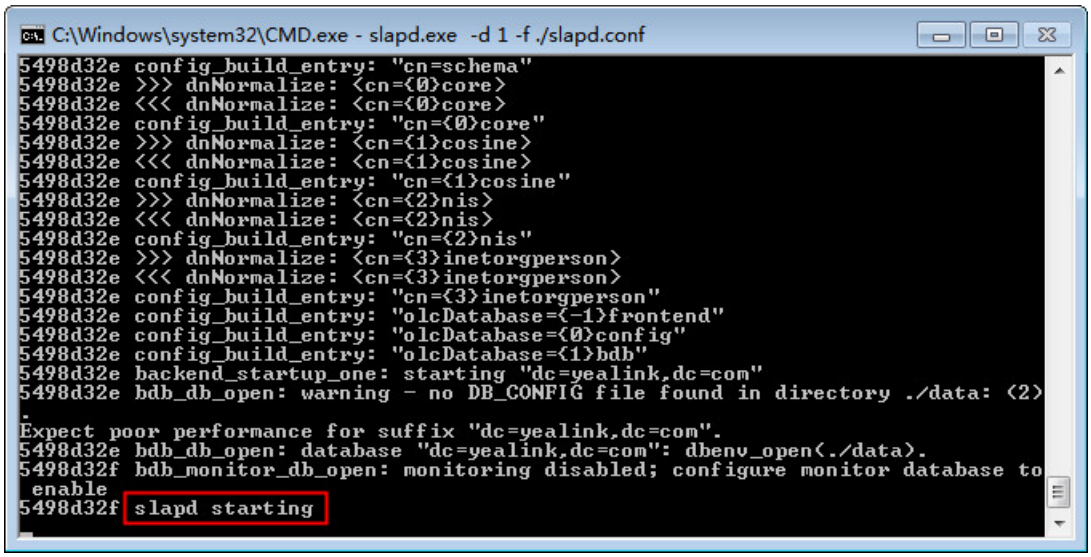
1. Click **Start** > **Run**.
2. Enter **cmd** in the dialog and click **OK** to enter the command line interface.

3. Access the server installation path. For example, execute the following commands to access the server installation path at **D:\OpenLDAP**.

4. Execute the command **slapd.exe -d 1 -f ./slapd.conf** to start the slapd service.

If the service runs successfully, you can find the prompt "**slapd starting**".

The screenshot for reference is shown below:



⊗ CAUTION

Please do not close this window to make sure the LDAP server keeps running.

Add the Initial Entry to the LDAP Directory

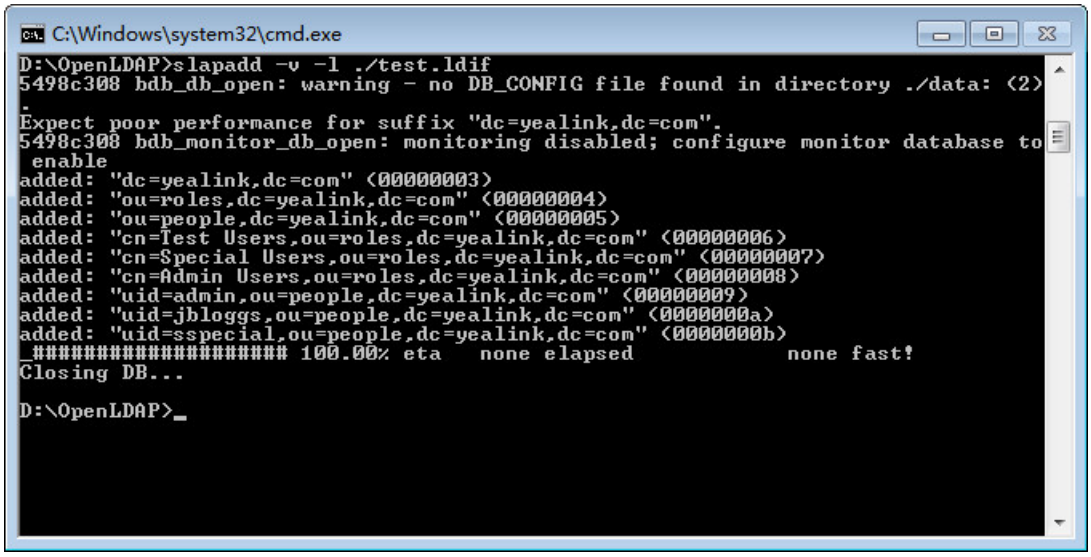
You can add the initial entry to the LDAP directory by using the LDIF file. Create a new text document, then modify the filename extension as ldif and place the document on the OpenLDAP installation path. For example, create a text document named as test.txt, right-click the test.txt document, and then select to rename it, modify the filename extension as ldif. Open the LDIF file with your favorite text editor and input the corresponding content. The following shows an example of the content of the LDIF file:

```
dn: dc=yealink,dc=com
objectClass: top
objectClass: dcObject
objectClass: domain
dc: yealink
```

```
dn: ou=roles,dc=yealink,dc=com
objectClass: top
objectClass: organizationalUnit
ou: roles

dn: ou=people,dc=yealink,dc=com
objectClass: top
objectClass: organizationalUnit
ou: people

dn: cn=Test Users,ou=roles,dc=yealink,dc=com
objectClass: groupOfUniqueNames
cn: Test Users
uniqueMember: uid=sspecial,ou=people,dc=yealink,dc=com
uniqueMember: uid=jbloggs,ou=people,dc=yealink,dc=com

dn: cn=Special Users,ou=roles,dc=yealink,dc=com
objectClass: groupOfUniqueNames
cn: Special Users
uniqueMember: uid=sspecial,ou=people,dc=yealink,dc=com

dn: cn=Admin Users,ou=roles,dc=yealink,dc=com
objectClass: groupOfUniqueNames
cn: Admin Users
uniqueMember: uid=admin,ou=people,dc=yealink,dc=com

dn: uid=admin,ou=people,dc=yealink,dc=com
objectClass: person
objectClass: inetOrgPerson
cn: State App
displayName: App Admin
givenName: App
mail: admin@fake.org
sn: Admin
uid: admin
userPassword: adminpassword

dn: uid=jbloggs,ou=people,dc=yealink,dc=com
objectClass: person
objectClass: inetOrgPerson
cn: Joe Bloggs
displayName: Joe Bloggs
givenName: Joe
mail: jbloggs@fake.org
sn: Bloggs
uid: jbloggs
userPassword: password

dn: uid=sspecial,ou=people,dc=yealink,dc=com
objectClass: person
objectClass: inetOrgPerson
cn: Super Special
displayName: Super Special
givenName: Super
mail: sspecial@fake.org
sn: Special
uid: sspecial
userPassword: password</span>
```

To add the initial entry using the test.ldif file:

1. Click **Start** > **Run**.
2. Execute **cmd** in the dialog and click **OK** to enter the command line interface.
3. Access the server installation path. For example, execute the following commands to access the server installation path at **D:\OpenLDAP**.
4. Execute the command **slapadd -v -l ./test.ldif** to add the initial entry.
   The screenshot for reference is shown as below:



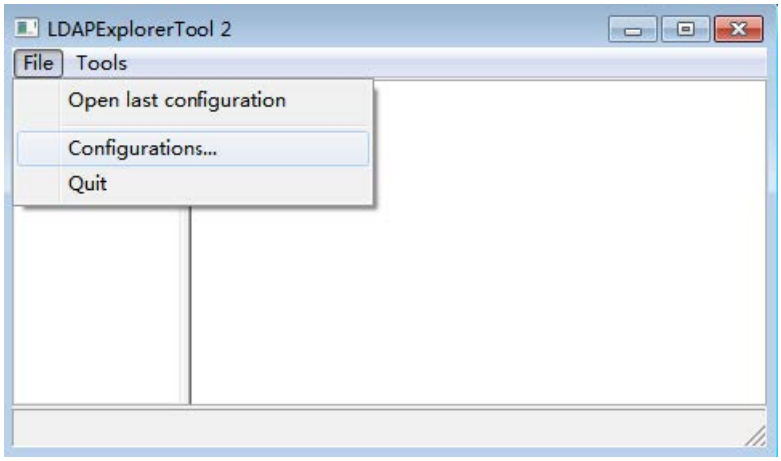
Configure the LDAPExploreTool2

The LDAPExploreTool2 application supports running on the Windows system. The application is a graphical LDAP tool that enables you to browse, modify, and manage contact entries on the LDAP server.
If you have an LDAPExploreTool2 application installed on your computer, open it now, otherwise, download the application from http://ldaptool.sourceforge.net/. And then complete the installation following the wizard.

Create a Configuration

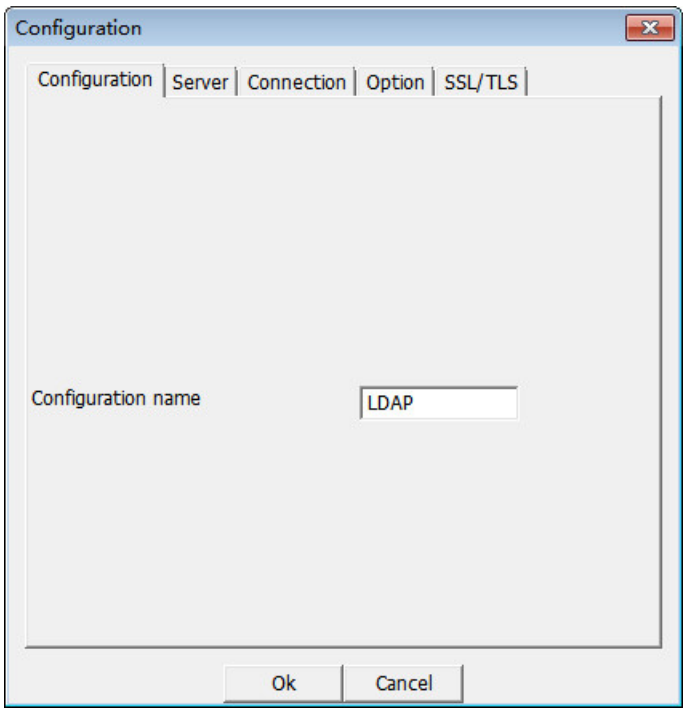
To create a configuration:

1. Double-click the LDAPExploreTool2.exe to run the application.
2. Click **File** > **Configurations**.

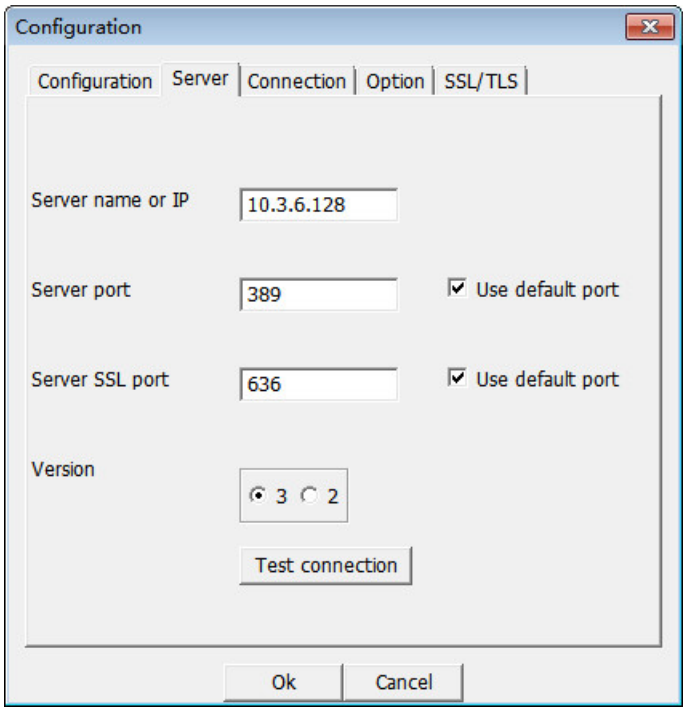


3. Click **New** to create a new configuration.

4. Enter a name in the **Configuration name** field under the **Configuration** tab.



5. Enter the domain name or IP address of the LDAP server in the **Server name or IP** field under the **Server** tab. Select the check box of **Use default port** for the **Server port** and **Server SSL port**.



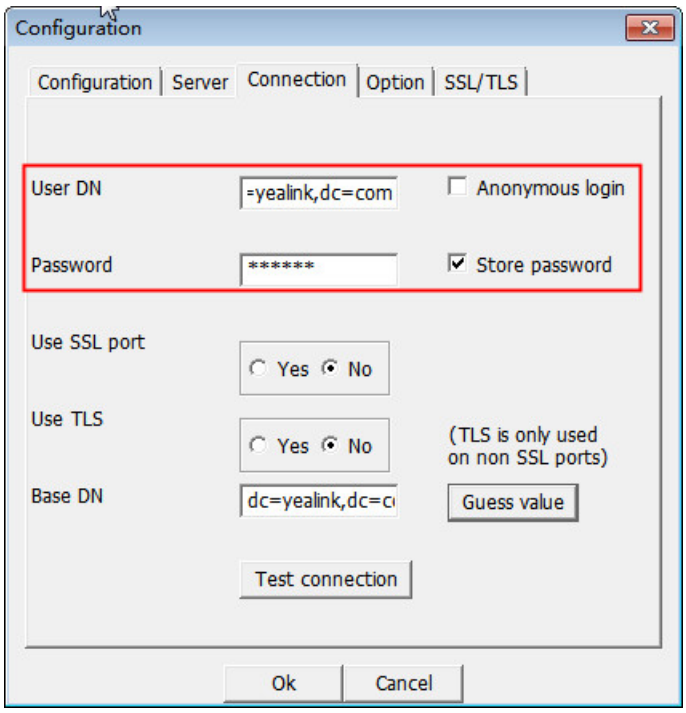
6. Enter the user DN and password in the **User DN** and **Password** field under the **Connection** tab.

   The user DN and password correspond with the Rootdn and Rootpw defined in the slapd.conf file.

   For example, according to the manager information defined in the slapd.conf file:

   ```
   Rootdn "cn=Manager,dc=yealink,dc=com"
   Rootpw secret
   ```

   Enter **cn=Manager,dc=yealink,dc=com** in the **User DN** field and **secret** in the **Password** field under the **Connection** tab.



7. Click **Guess value** to fill the **Base DN** automatically.

8. Click **Test connection** to test the connection to the LDAP server. If you encounter an error or warning during the test, you need to resolve the error or warning first according to the prompt, and then retry to test the connection.

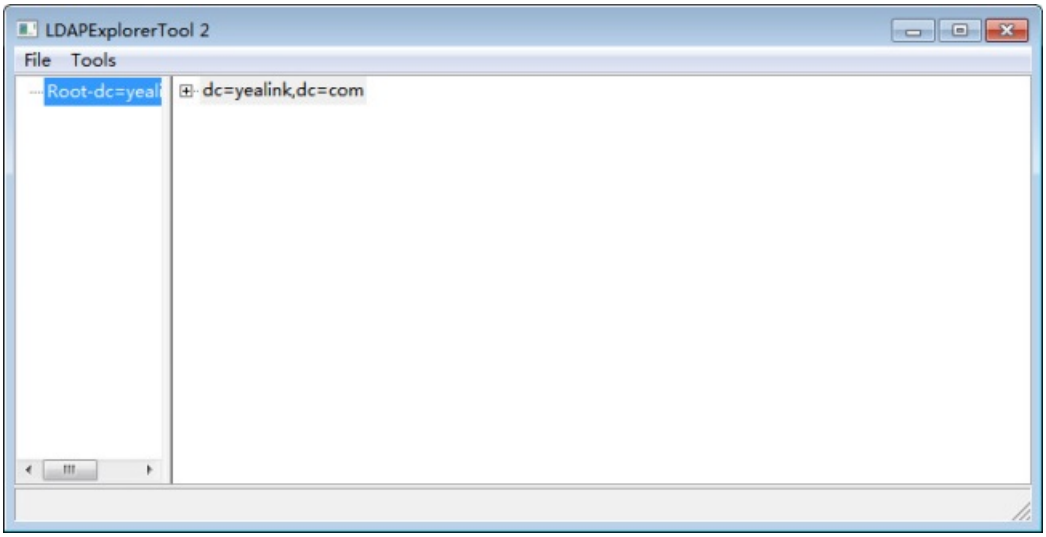
9. Click **OK** to accept the change.

Add Entries

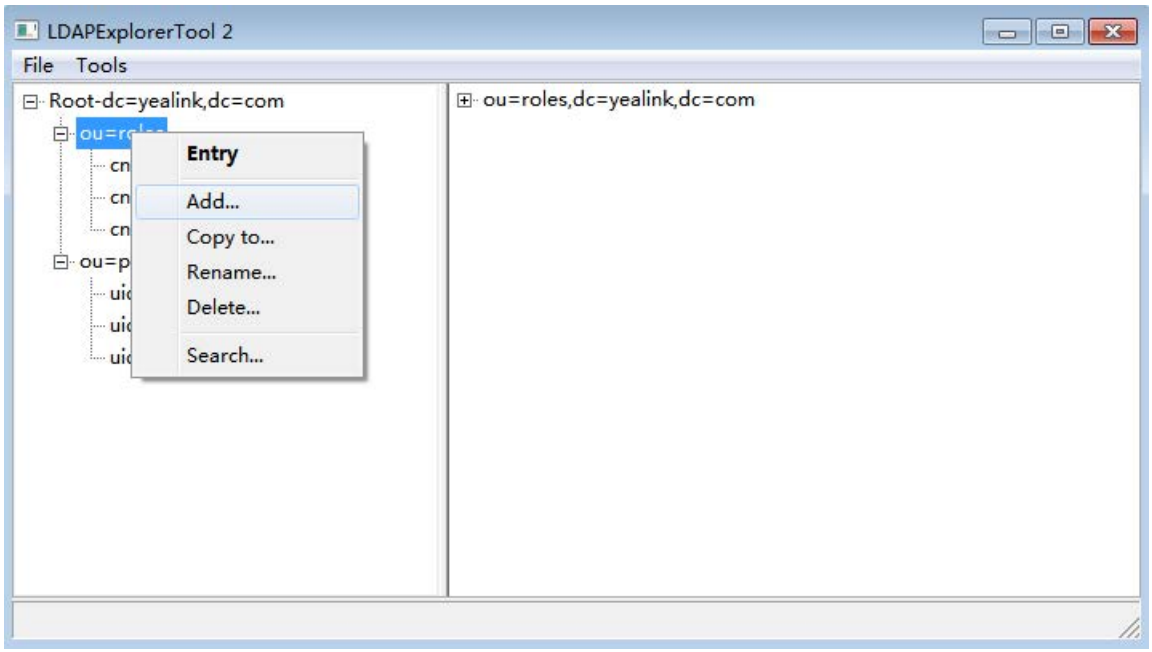
To add entries:

1. Click **File** > **Configurations**, select the configuration created above, and then click **Open**.

The screenshot for reference is shown below:



2. Right-click the root entry, and then select **Add** to add a new entry.



3. Enter the desired values in the corresponding fields.
   - **Parent DN**: It will be automatically generated according to the server configuration.
   - **Entry RDN**: The format is cn=XXX. This is a unique identifier for each entry.
   - **Object Class (from schema)**: Select the structure class to which the entry belongs. Each structure class has its must attributes and may attributes. For example, we select **person** from the **Object class (from schema)** drop-down menu.

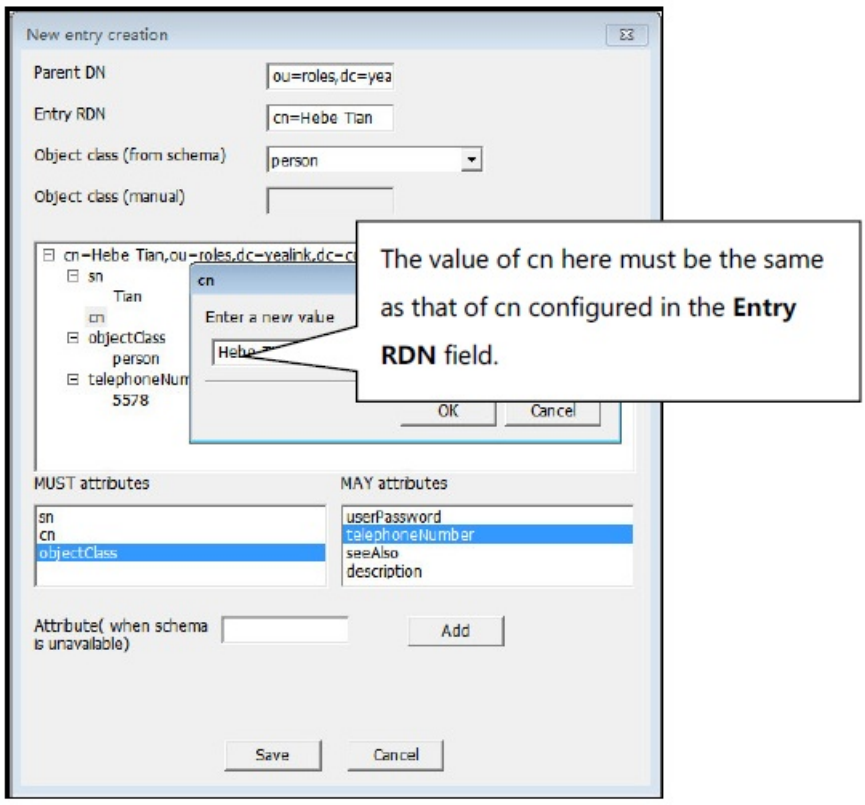
4. Select the desired attributes for the object class.
   - **Must attributes**: Double-click attributes to add them to the entry node. All attributes listed in the **Must attributes** field must be added and each value of the attribute must be set.
   - **May attributes**: Double-click the desired attributes to add them to the entry node. The attributes listed in the **May attributes** field are optional.

     Common attributes are listed in the following table:

Attribute	Name	Description
cn	commonName	Full name of the entry.
gn	givenName	The first name also called Christian name.
sn	surname	Surname, last name or family name.
telephoneNumber	telephoneNumber	Office phone number.
homePhone	homeTelephoneNumber	Home phone number.
mobile	mobileTelephoneNumber	Mobile or cellular phone number.
pager	pagerTelephoneNumber	Pager telephone number.
company	company	Company name.
o	organizationName	Organization name.
ou	organizationlUnitName	Usual department or any sub entity of larger entity.

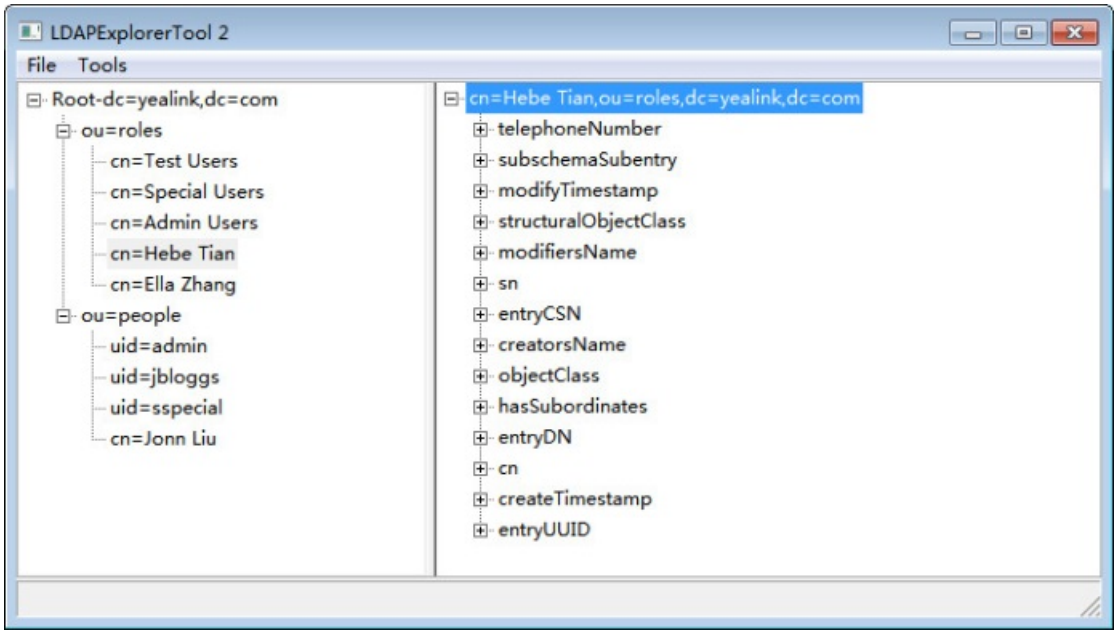
5. Right-click the selected attribute and then select **Add value**.

   The screenshot of adding a new entry is shown as below:



6. Click **Save** to confirm the configuration.

7. Repeat steps 2 to 6 to add more contact entries.
   You can find the added entries at the left of the LDAP catalog.



Microsoft Active Directory

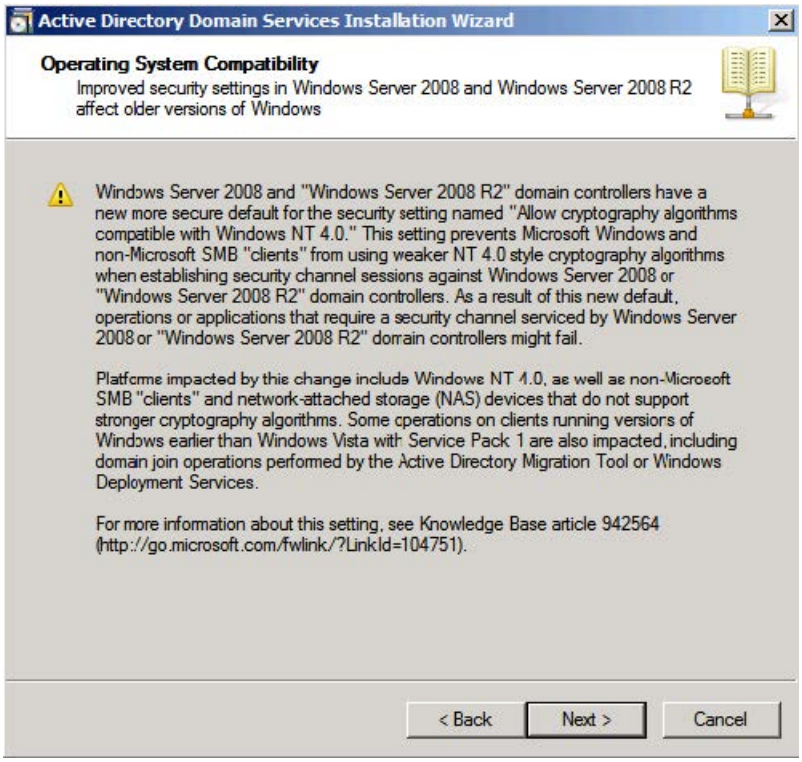
Install the Microsoft Active Directory Domain Services

This section shows you how to install an active directory on a Microsoft Windows Server 2008 R2 Enterprise 64-bit system.

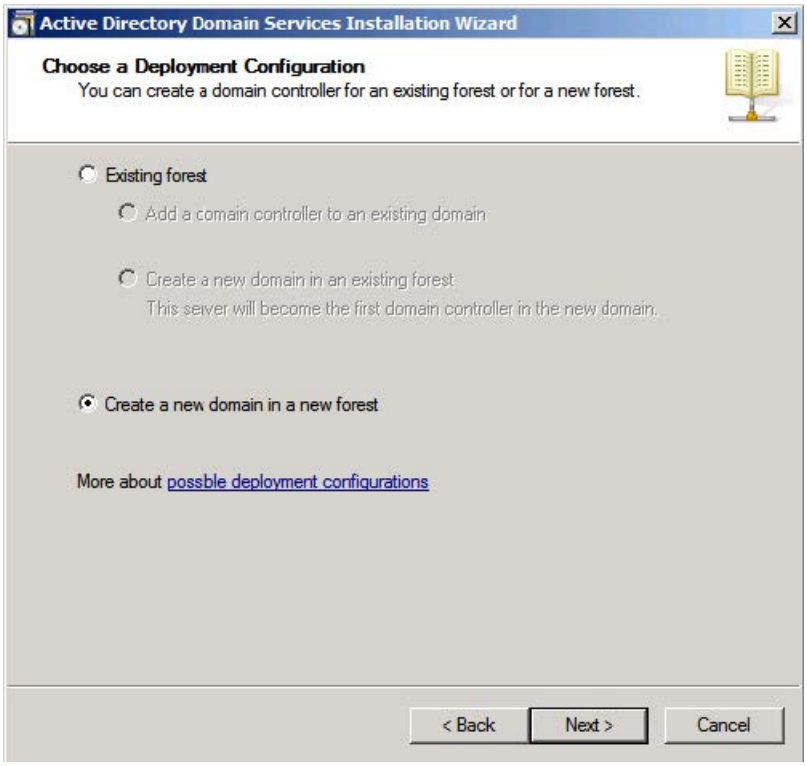
To install the Microsoft Active Directory Domain Services:

1. Click **Start** > **Run**.
2. Enter **dcpromo** in the dialog and click **OK**.
3. The Active Directory Domain Services Installation Wizard will appear after a short while, click **Next**.

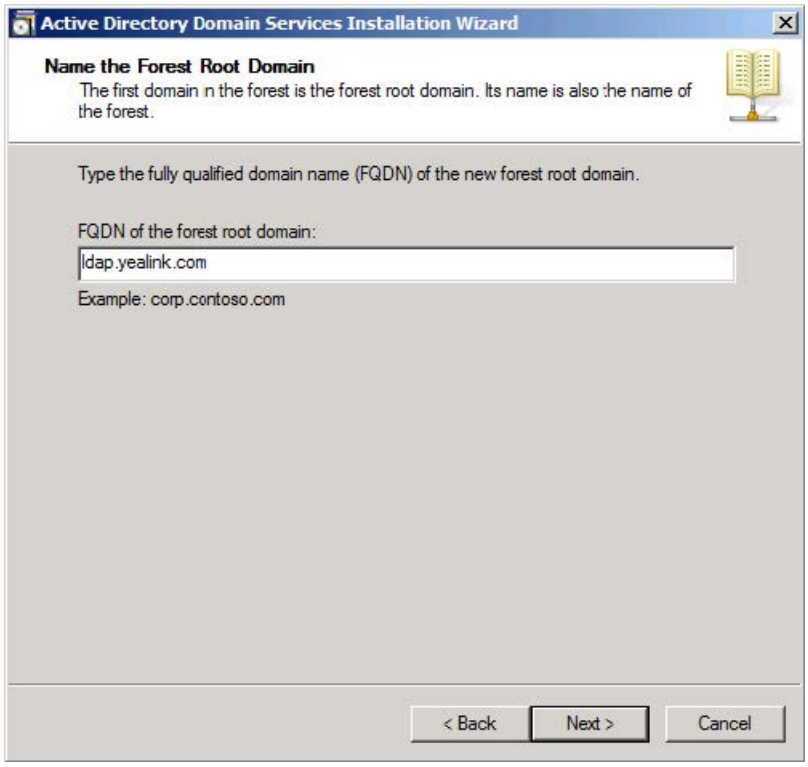
4. Read the provided information and click **Next**.



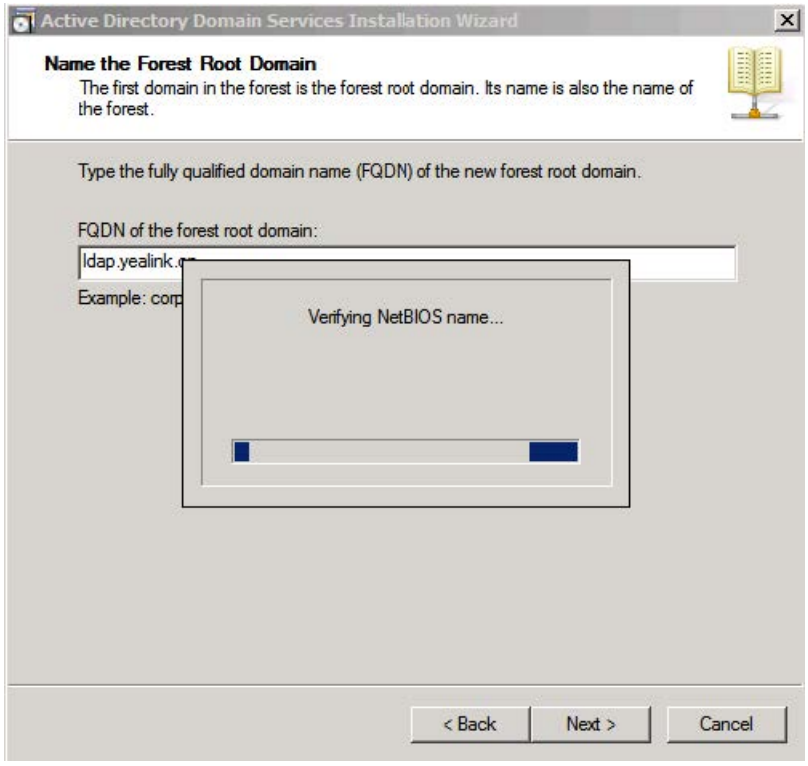
5. Select the **Create a new domain in a new forest** check box and click **Next**.



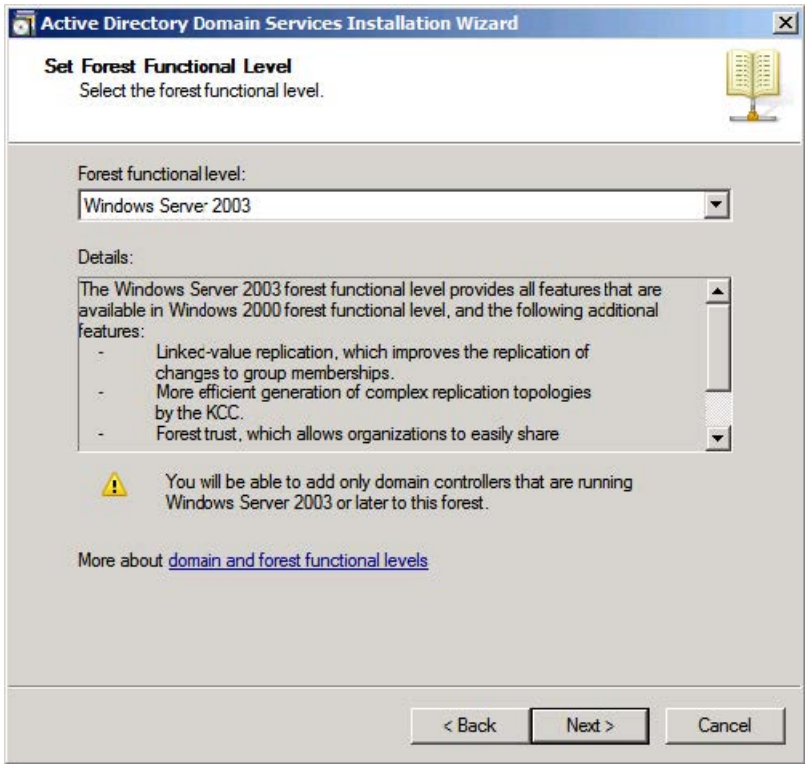
6. Enter an appropriate domain name for the forest root domain and click **Next**.



The wizard will check if the domain name is in use on the local network.

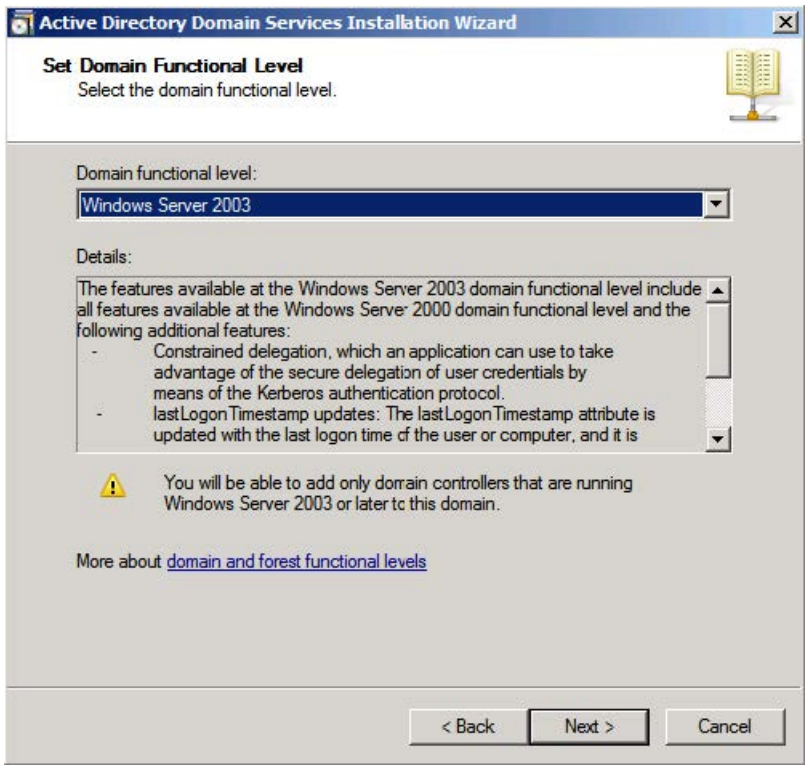


7. Select the desired forest functional level from the **Forest functional level** drop-down menu, and click **Next**.
   For more information, click **domain and forest functional levels**.



8. Select the desired domain functional level from the **Domain functional level** drop-down menu, and click **Next**.

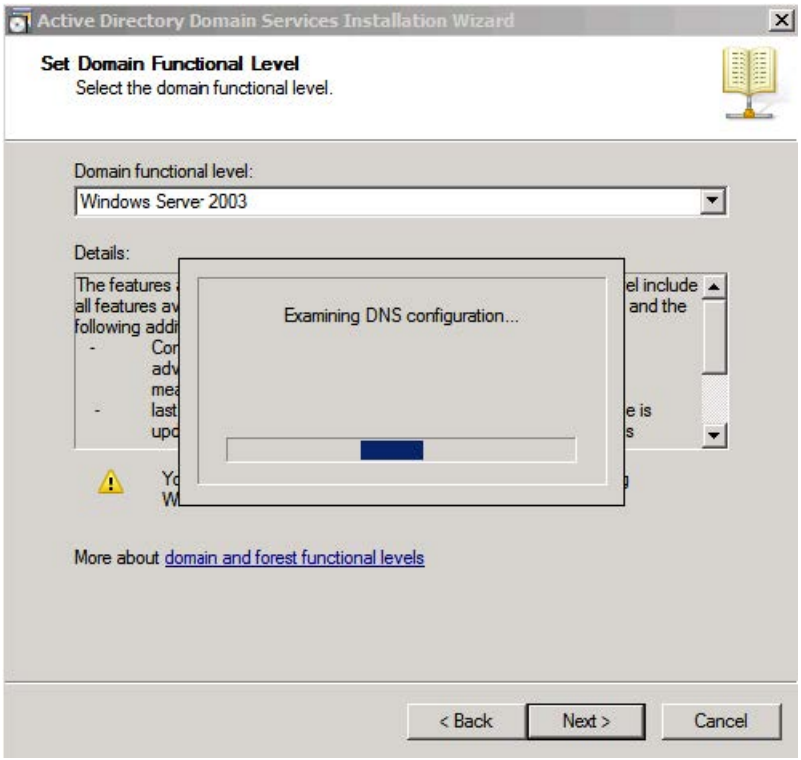
   For more information, click **domain and forest functional levels**.



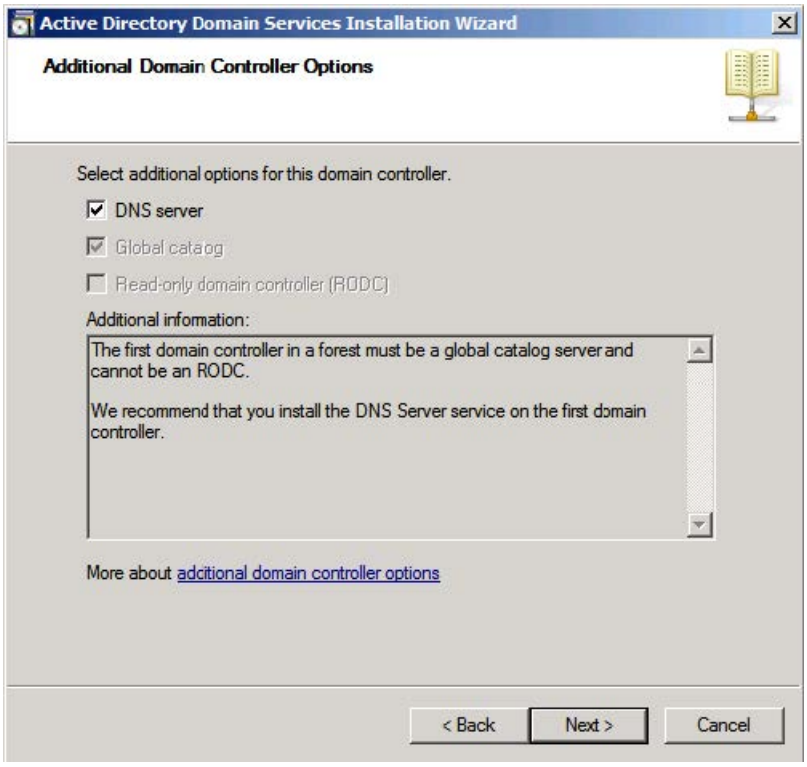
NOTE

If you select **Windows Server 2008 R2** for the forest functional level, you will not be prompted to select a domain functional level.

The wizard will check if the DNS is properly configured on the local network.



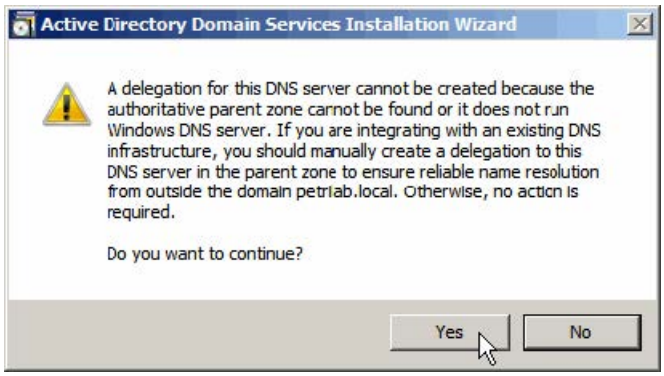
9. Select additional options for this domain controller if required, and click **Next**.



NOTE

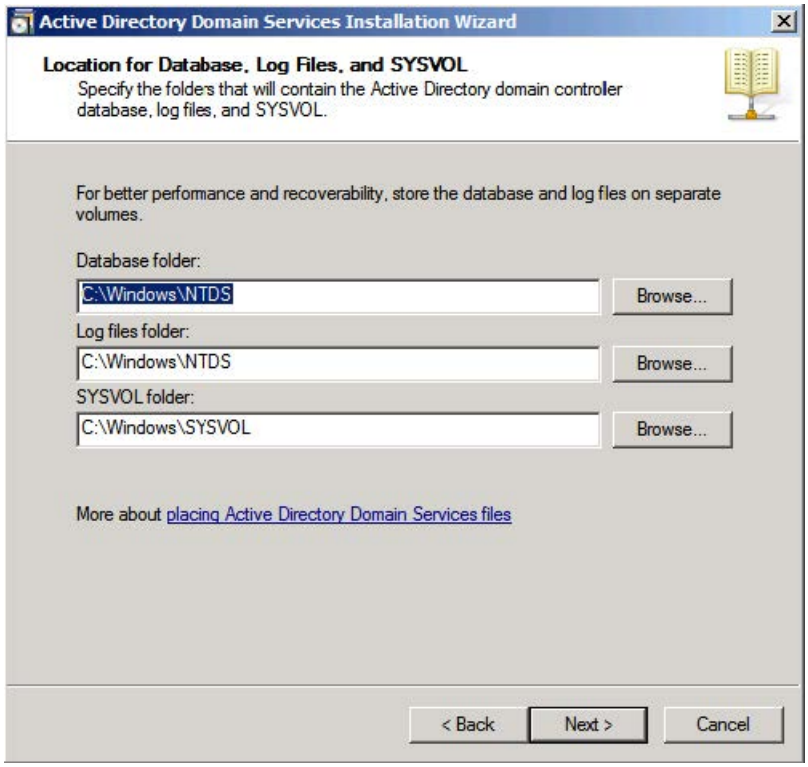
You may get a warning telling you that the server has one or more dynamic IP addresses. We recommend assigning a static IP address to the server.

10. The wizard will prompt a warning about DNS delegation. Since no DNS has been configured yet, you can ignore the message and click **Yes**.



11. Specify the desired paths for the database, log files, and SYSVOL folders, and click **Next**.

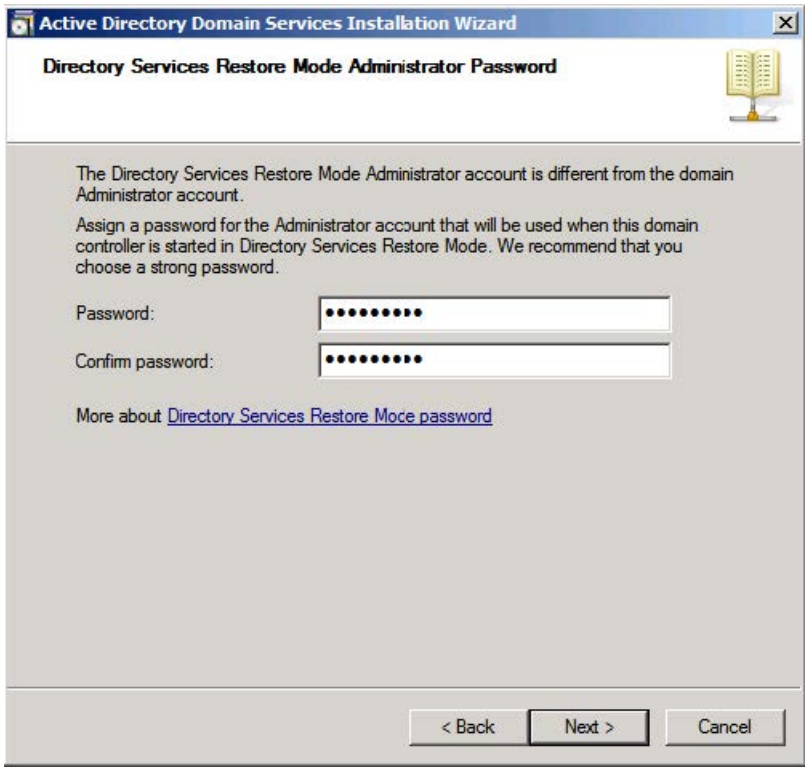
    For more information, click **placing Active Directory Domain Services files**.



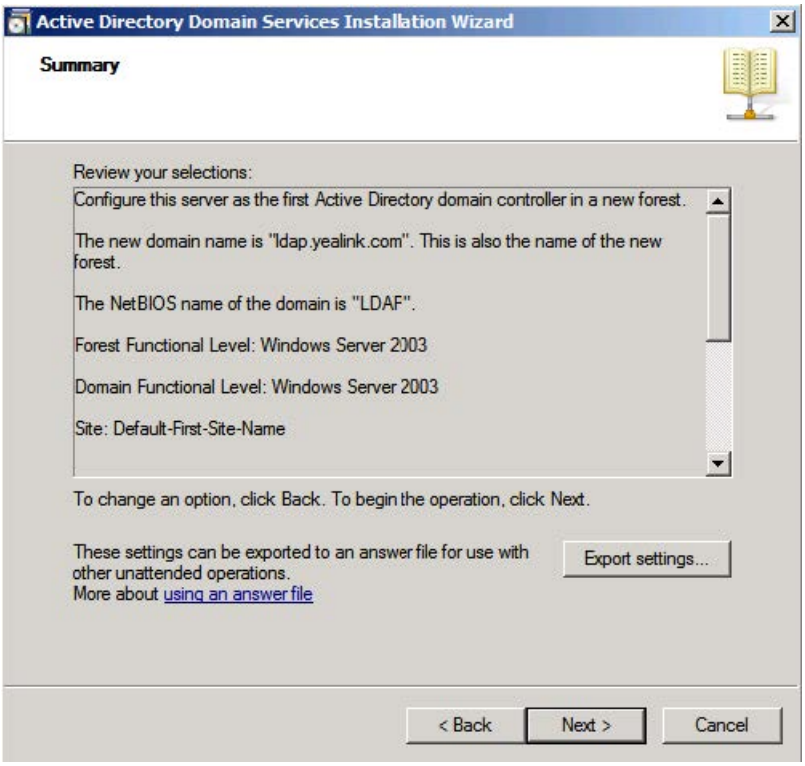
12. Configure the password for the active directory recovery mode, and click **Next**.

    For more information, click **Directory Services Restore Mode password**.

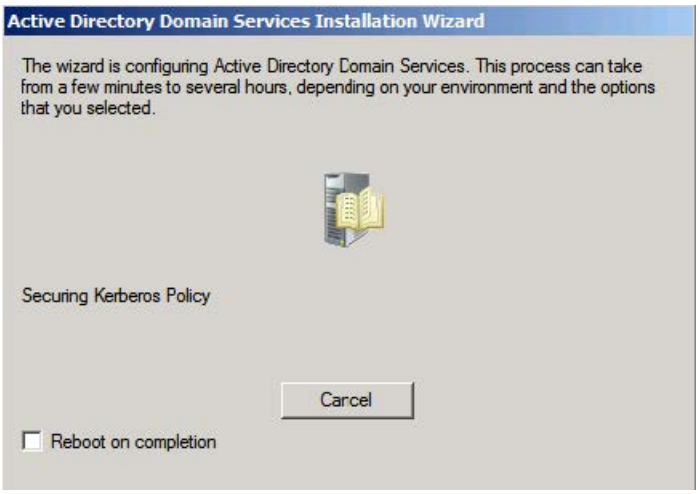
    The password should be complex and at least 7 characters long.



13. Review your selection and click **Next**.



The wizard will prompt that the system begins to create the Active Directory Domain Services.



14. Click **Finish** to complete the installation and exit the wizard.

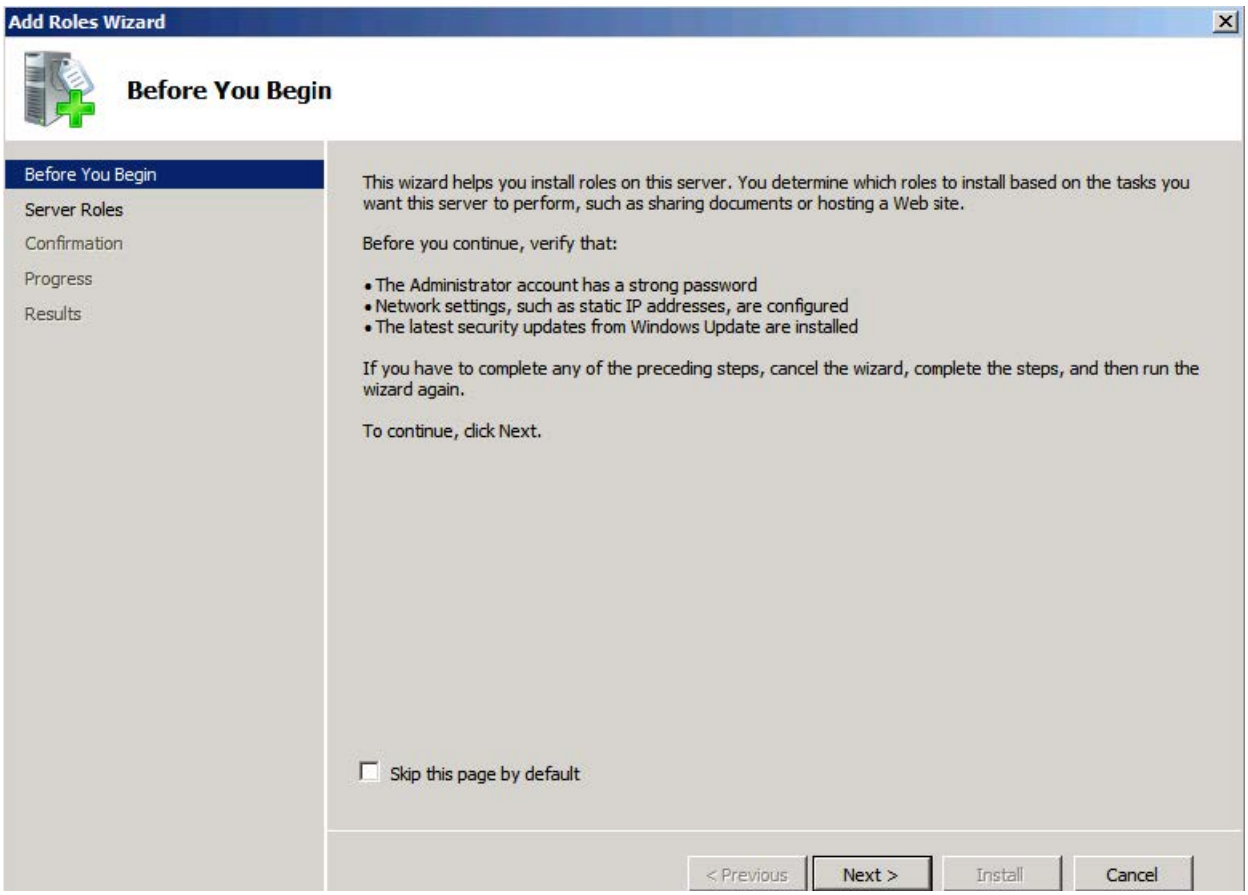
Install Active Directory Lightweight Directory Services Role

You should also install the Active Directory Lightweight Directory Services role on the Windows Server 2008 system.

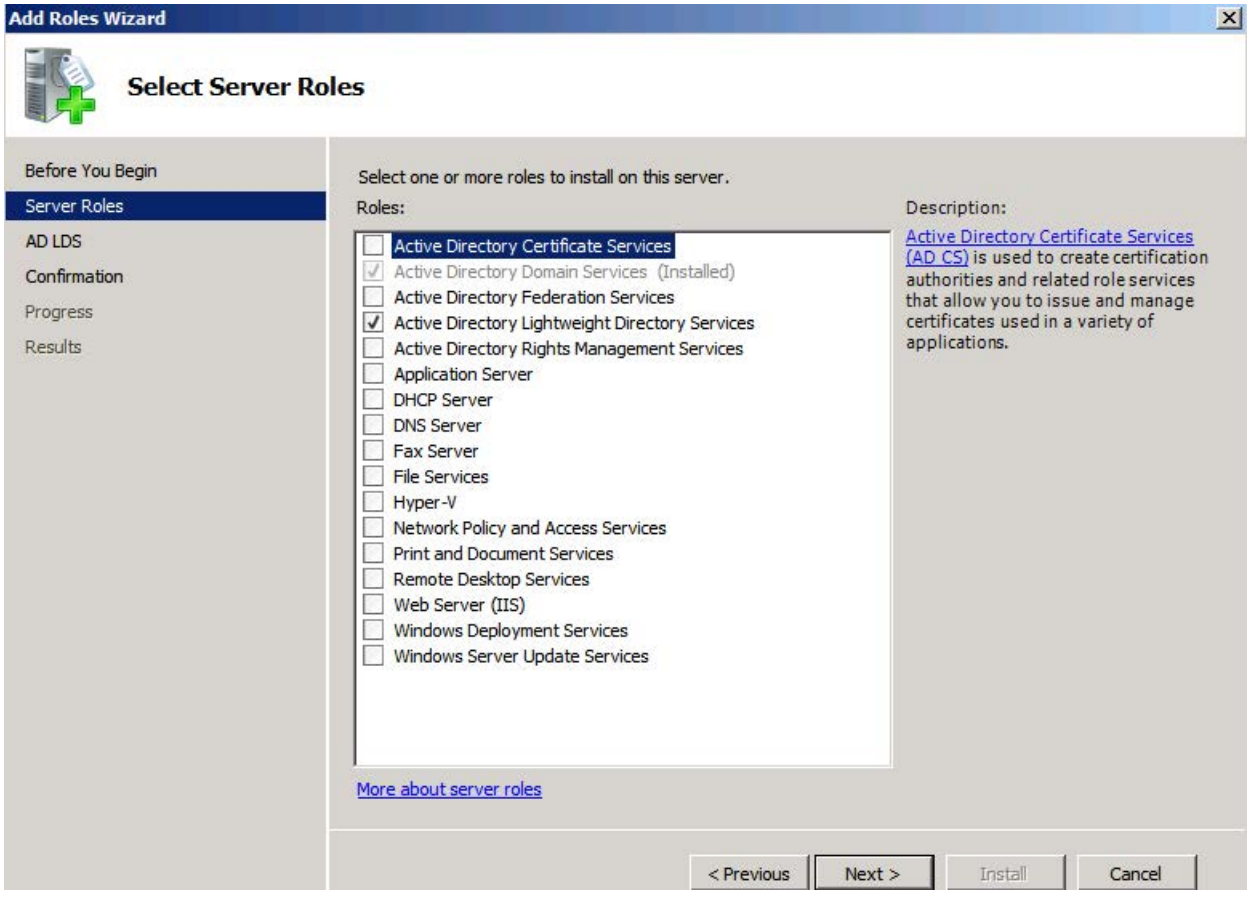
To install the Active Directory Lightweight Directory Services role:

1. Click **Start** > **Administrative Tools** > **Server Manager**.
2. Right-click **Roles**, and then select **Add Roles**.

3. The Add Roles Wizard will pop up, click **Next**.

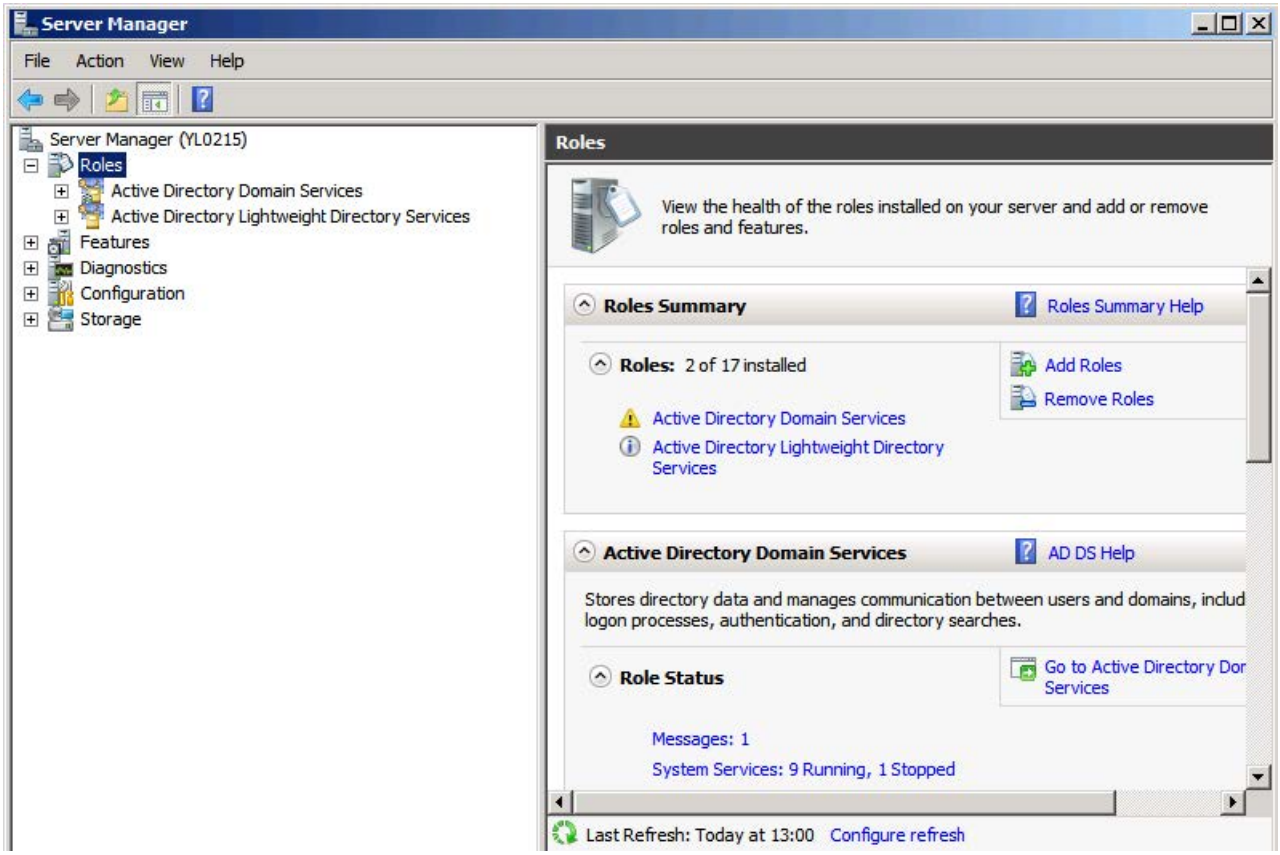


4. Select the **Active Directory Lightweight Directory Services** check box and click **Next**.



5. Follow the default settings and click **Next**.
6. When the installation is completed, click **Close**.

   After the installation succeeds, you will find the **Active Directory Lightweight Directory Services** role listed in the roles of the server manager.



Configure the Microsoft Active Directory Server

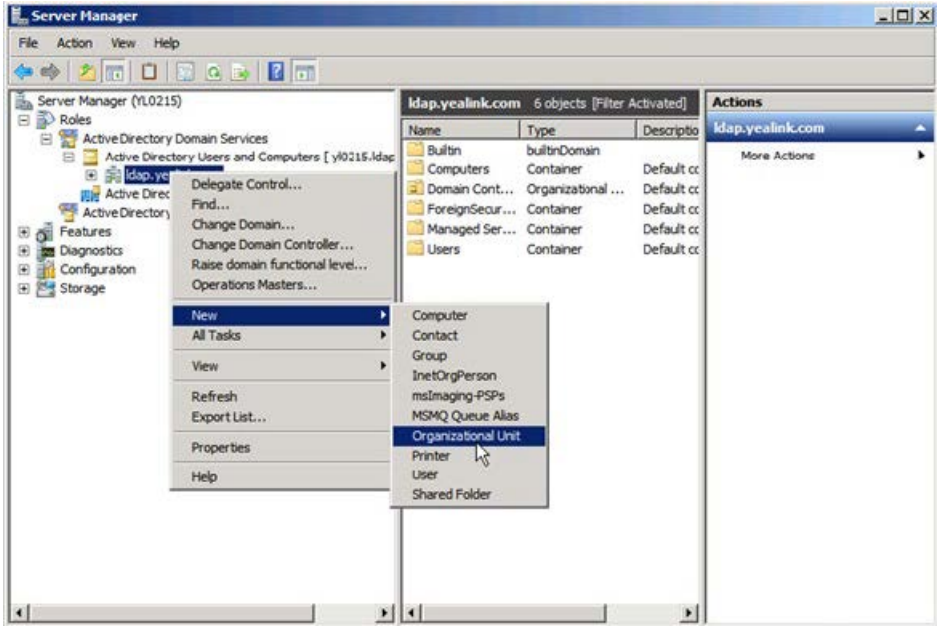
Add an Entry to the Active Directory

You can add entries to the active directory one by one in this way.

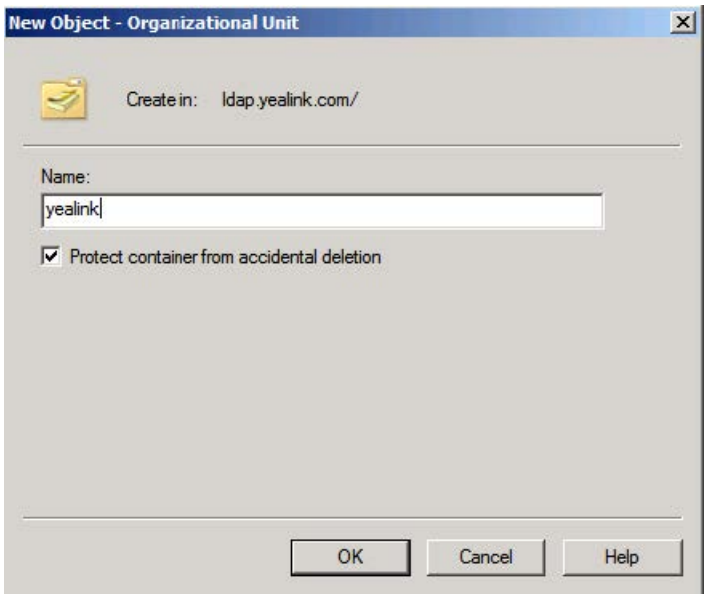
To add an entry to the Active Directory:

1. Click **Start** > **Administrative Tools** > **Server Manager**.
2. Double click **Roles** > **Active Directory Domain Services** > **Active Directory Users and Computers**.

3. Right-click the domain name created above (e.g., ldap.yealink.com), and then select **New** > **Organizational Unit**.

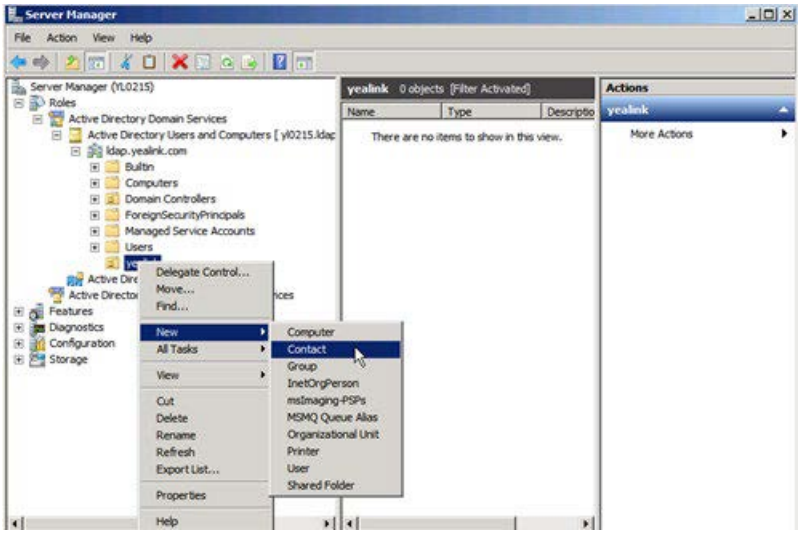


4. Enter the desired name of the organizational unit.

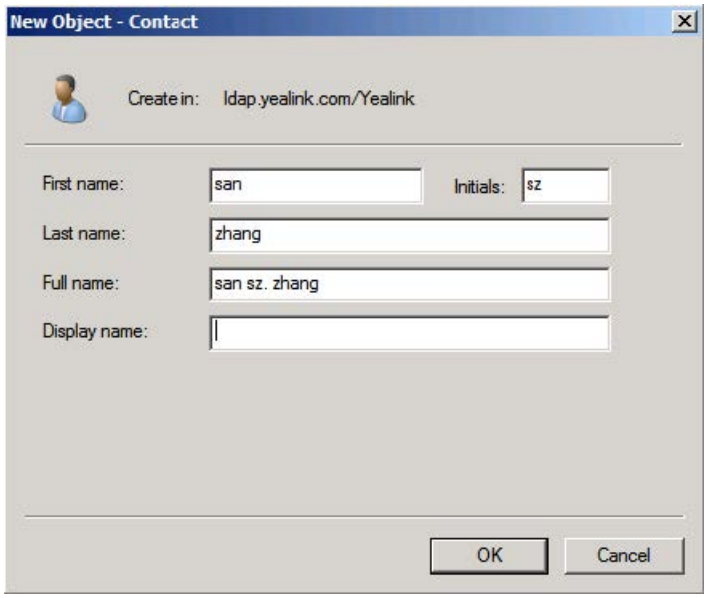


5. Click **OK** to accept the change.

6. Right-click the organizational unit created above, and then select **New** > **Contact**.



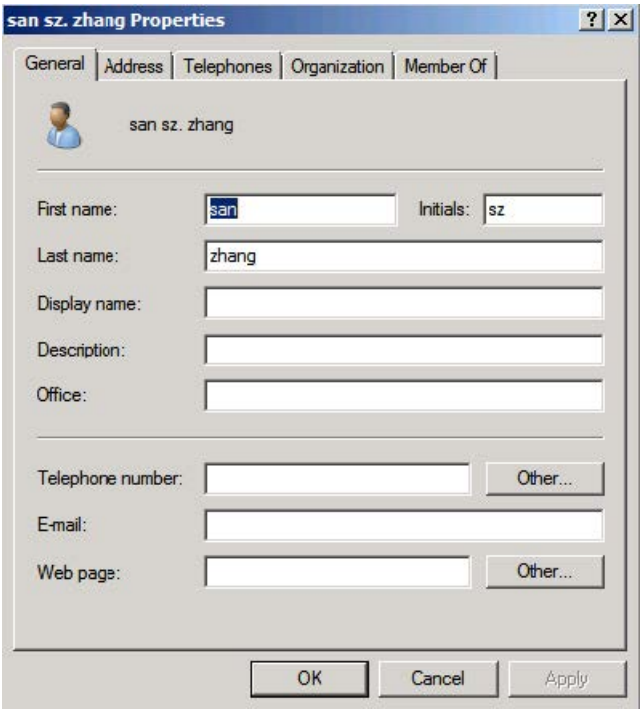
7. Enter the desired values in the corresponding fields.



8. Click **OK** to accept the change.

9. Double click the contact created above.

10. Configure more properties of the contact.



11. Click **OK** to accept the change.

Add Entries to the Active Directory Using the ldifde Tool

You can use an LDIF file to perform a batch import of all entries to the active directory.

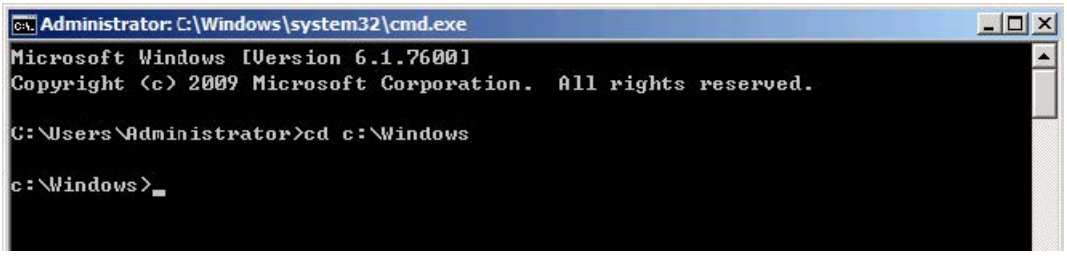
To create the LDIF file:

Create a new text document and then modify the filename extension as ldif. For example, create a text document named as test.txt, right-click the test.txt document and then select to rename it, modify the filename extension as ldif. Open the LDIF file with your favorite text editor and input the corresponding content. The following shows an example of the content of the LDIF file:

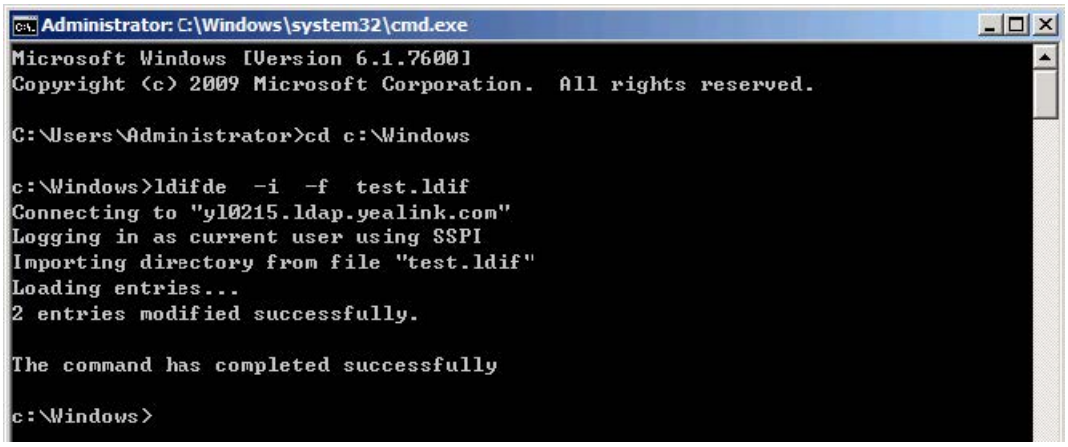
```
##Create a new organizational unit##
dn: OU=yealink,DC=ldap,DC=yealink,DC=com
changetype: add
objectClass: top
objectClass: organizationalUnit
ou: yealink
name: yealink

##create a new contact##
dn: CN=san zhang,OU=yealink,DC=ldap,DC=yealink,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: contact
cn: san zhang
sn: zhang
givenName: san
initials: zs
name: san zhang
ipPhone: 2336
mobile: 15557107369
```

To import the test.ldif file:

1. Click **Start** > **Run**.
2. Enter **cmd** in the pop-up dialogue box and click **OK** to enter the command line interface.
3. Execute the command **cd** to access the path of the test.ldif file. For example, execute **cd c:\Windows** to access the path of the test.ldif file at **c:\Windows**.



4. Execute the command **ldifde -i -f test.ldif** to import the file.
   If the entries are added successfully, you can find the prompt "**n entries modified successfully**" ("n" indicates the number of the added entries).
   The screenshot for reference is shown as below:



   You can also export the existing entries on the active directory into a *.ldif file first, modify the file, and then import the modified file into the active directory. For more information, refer to the network resource.

Add Entries to the Active Directory Using the Csvde Tool

You can also use a CSV file to perform a batch import of all entries to the active directory. Create a new document using a spreadsheet application (e.g., Microsoft Excel) and then save the document to your local computer using "Save as" in the format "*.csv". For example, create a document named as test.xls, click "Save as" to save the document as test.csv. Open the CSV file with the spreadsheet application and input the corresponding content. The following shows an example of the CSV file content:

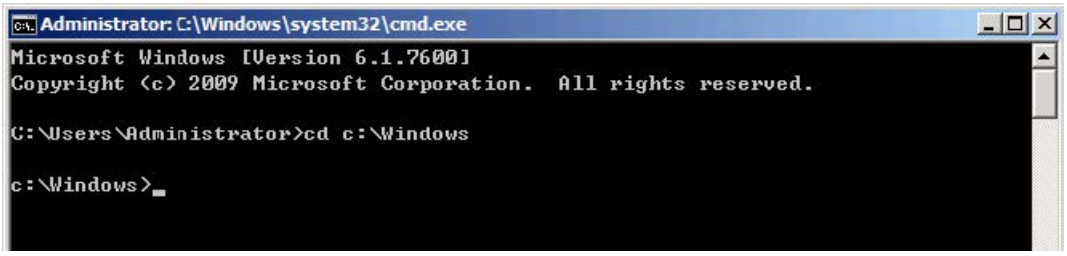
test.csv *

	A	B	C	D	E	F	G	H	I	J
1	DN	objectClass	ou	name	cn	sn	givenName	initials	ipPhone	mobile
2	OU=yealink,DC=ldap,DC=yealink,DC=com	organizationalUnit	yealink	yealink						
3	CN=san zhang,OU=yealink,DC=ldap,DC=yealink,DC=com	contact		san zhang	san zhang	san	zhang	sz	1111	123456789001
4	CN=si li,OU=yealink,DC=ldap,DC=yealink,DC=co	contact		si li	si li	li	si	sl	2222	123456789002
5	CN=wu wang,OU=yealink,DC=ldap,DC=yealink,DC=com	contact		wu wang	wu wang	wang	wu	ww	3333	123456789003

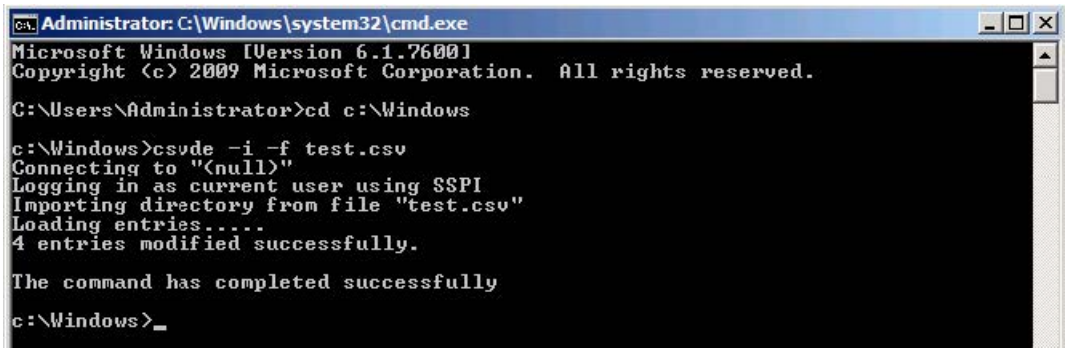
- The first line lists the attributes of the entries.
- The second line lists the values of an organizational unit in the corresponding attribute columns.
- The other lines list the values of contacts in the corresponding attribute columns.

To import the test.csv file:

1. Click **Start** > **Run**.
2. Enter **cmd** in the pop-up dialogue box and click **OK** to enter the command line interface.
3. Execute the command cd to access the path of the test.csv file. For example, execute **cd c:\Windows** to access the path of the test.csv file at **c:\Windows**.



4. Execute the command **csvde -i -f test.csv** to import the file.
   If the entries are added successfully, you can find the prompt "**n entries modified successfully**" ("n" indicates the number of the added entries).
   The screenshot for reference is shown as below:



NOTE

· The csvde tool cannot edit or delete the existing entries on the active directory.

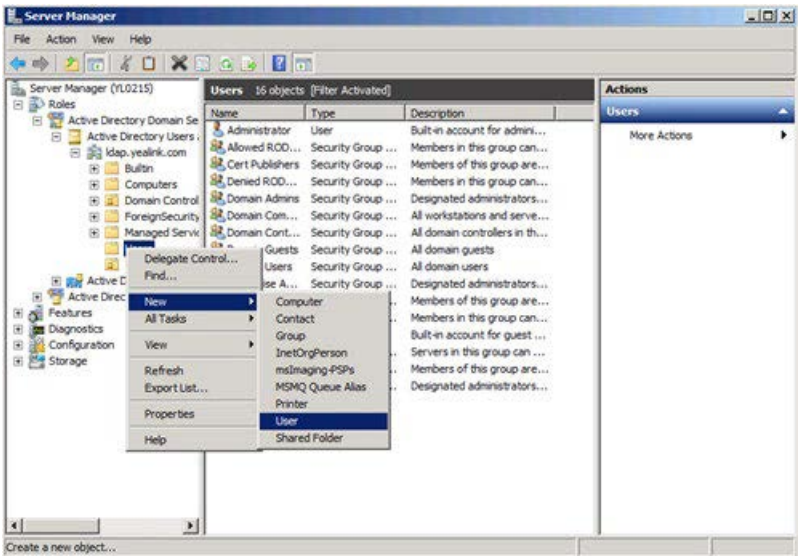
· You can also export the existing entries on the active directory into a *.csv file first, modify the file, and then import the modified file into the active directory. For more information, refer to the network resource.

Create User Accounts

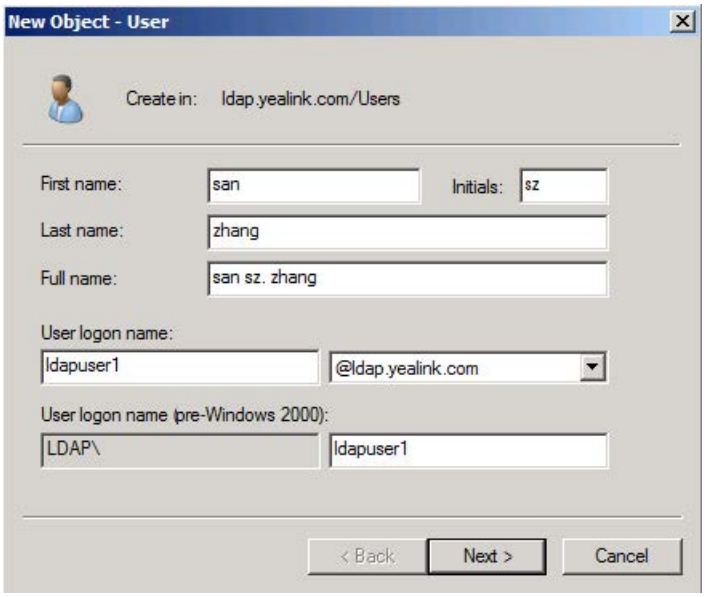
You can create user accounts to allow access to resources on the active directory. User accounts are very important and useful.

To create a user account:

1. Click **Start** > **Administrative Tools** > **Server Manager**.
2. Double click **Server Manager** > **Roles** > **Active Directory Domain Services** > **Active Directory Users and Computers**.
3. Select the domain name created above (e.g., ldap.yealink.com).
4. Right click **Users**, and then select **New** > **User**.

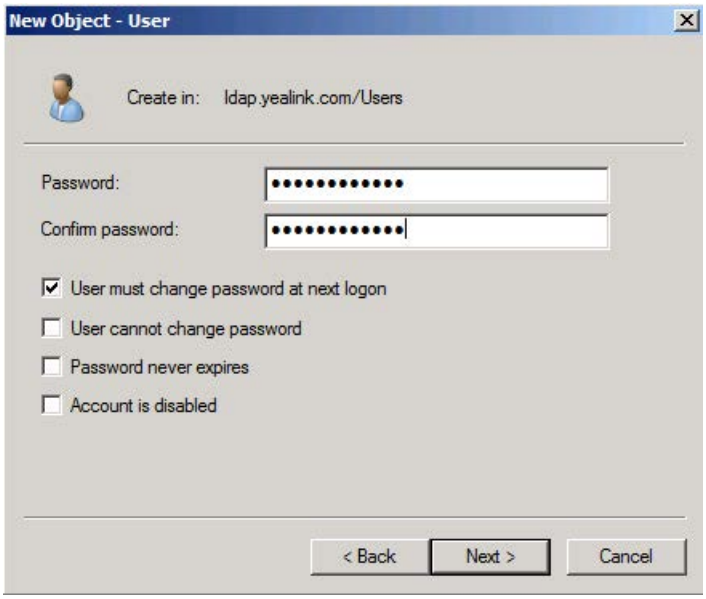


5. Enter desired values in the corresponding fields and click **Next**.

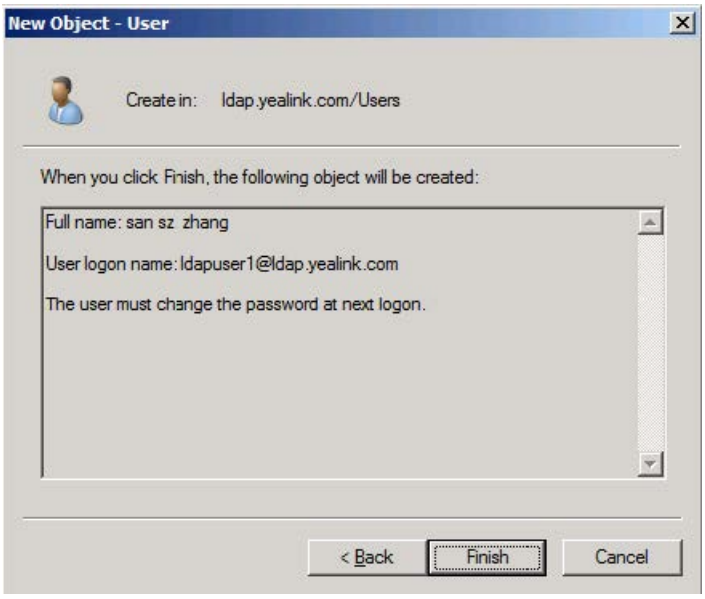


6. Enter the password for the user, select the appropriate options and click **Next**.

   The password should be a combination of upper case letters, lower case letters, numbers, and special characters.



7. Click **Finish** to complete the creation of the user account.



Microsoft Active Directory Application Mode

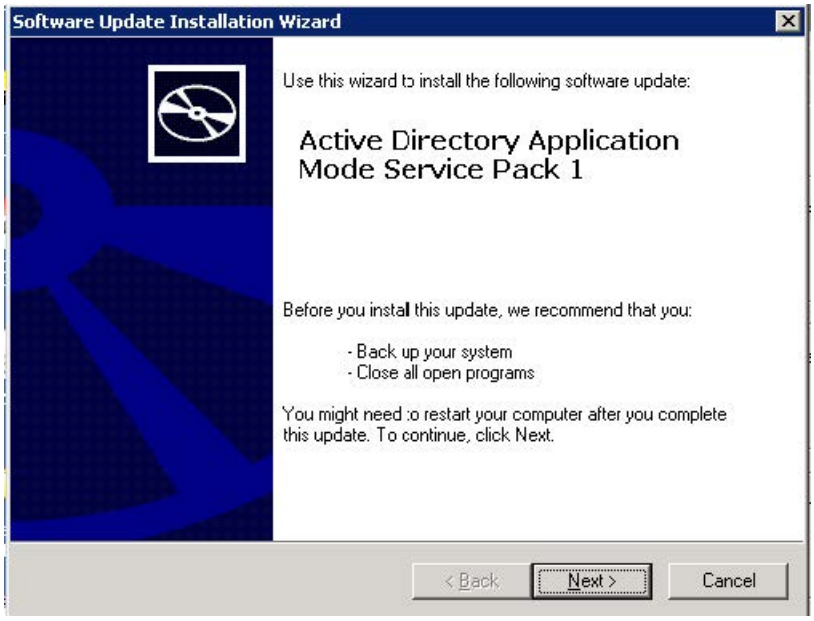
Microsoft Active Directory Application Mode (ADAM) is a new mode of Active Directory that is designed specifically for directory-enabled applications. ADAM is a Lightweight Directory Access Protocol (LDAP) directory service that runs as a user service, rather than as a system service. You can run ADAM on servers and domain controllers running operating systems in the Windows Server 2003 family. This section shows you how to install Active Directory Application Mode (ADAM) on Microsoft Windows Server 2003 SP2 Enterprise 32-bit system. You can download Active Directory Application Mode (ADAM) online:
http://www.microsoft.com/en-us/download/confirmation.aspx?id=4201.

Install the Active Directory Application Mode

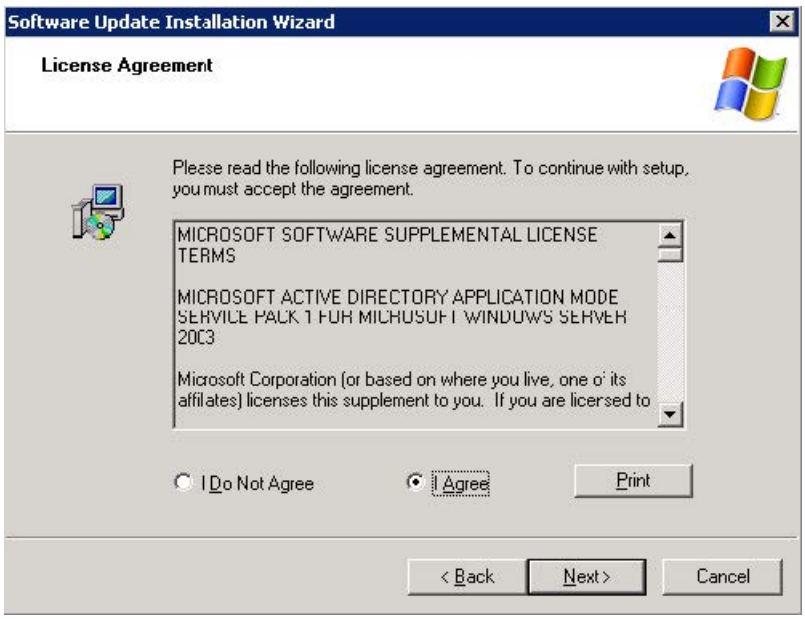
To install the Active Directory Application Mode:

1. Double click ADAMSP1_x86_English.exe to run the application.

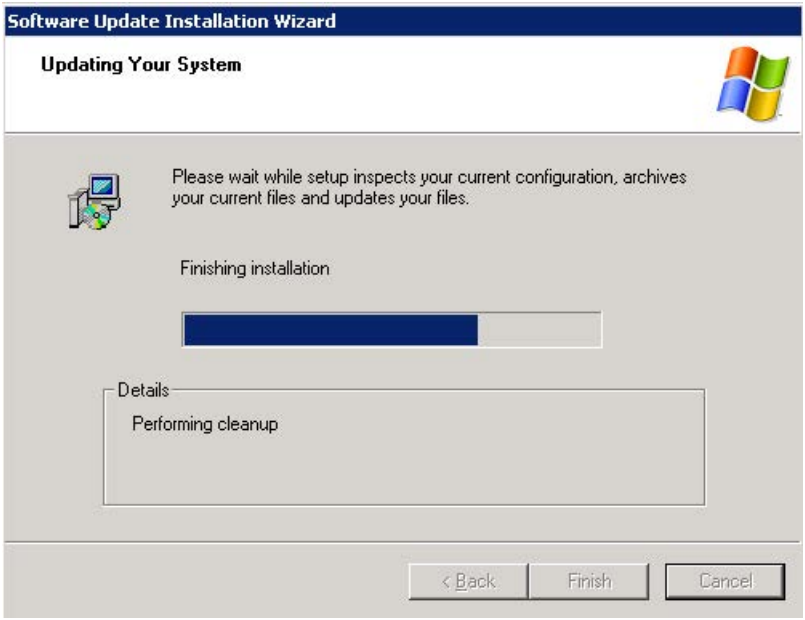
2. The Active Directory Application Mode Service Park 1 Installation Wizard will appear after a short while, click **Next**.



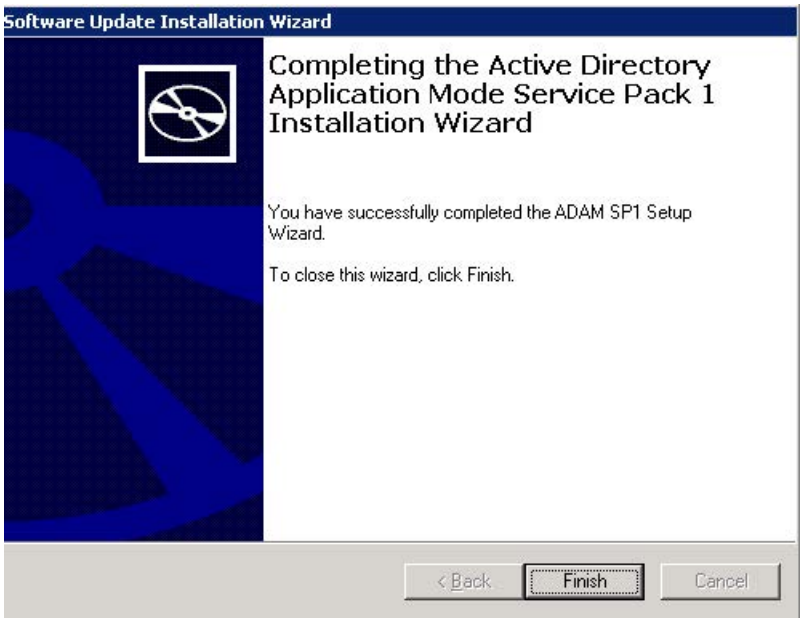
3. Read the software license agreement and select **I Agree** check box. And then click **Next**.



The installation progress screen will be shown as below:



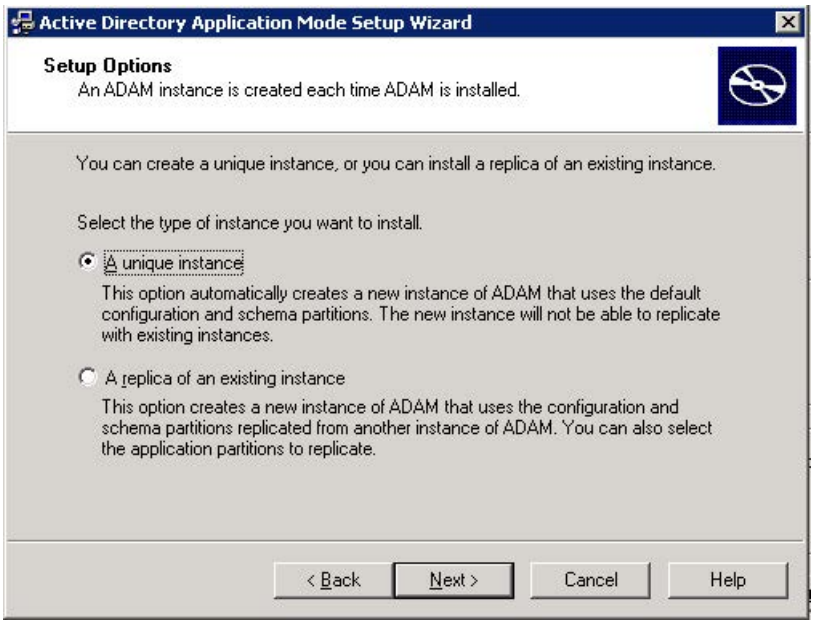
4. Click **Finish** to complete the installation and exit the wizard.



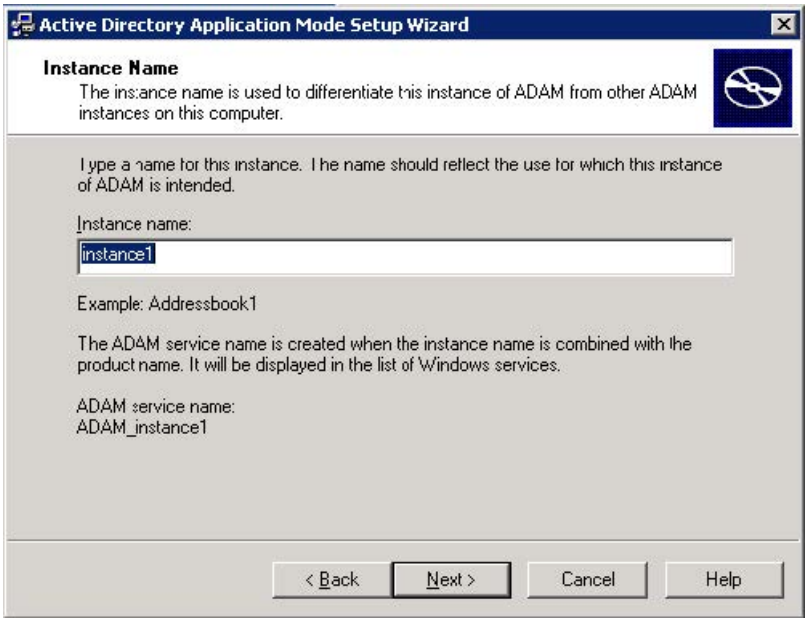
To create an ADAM instance:

1. Click **Start** > **Programs** > **ADAM** > **Create an ADAM instance**.
   It will prompt the following interface and click **Next**.

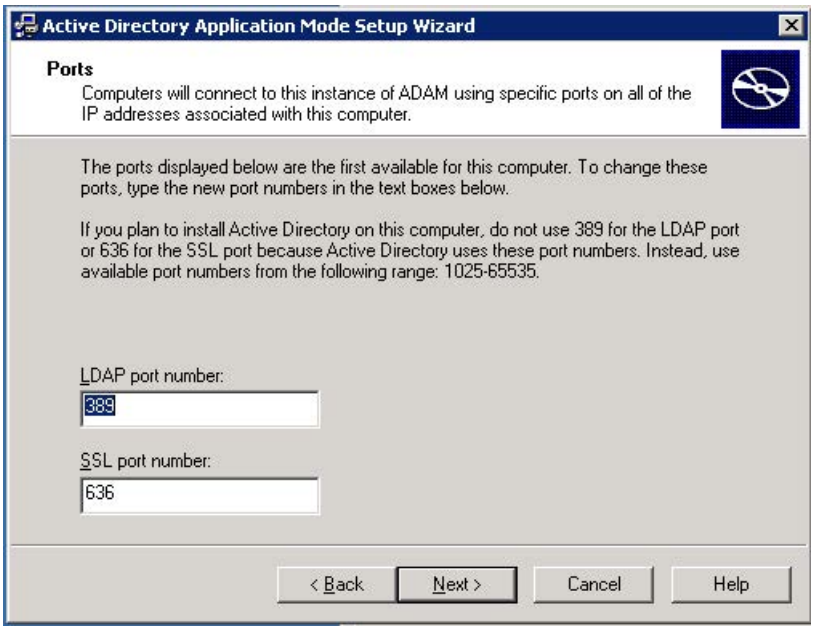
2. Mark the **A unique instance** check box and click **Next**.



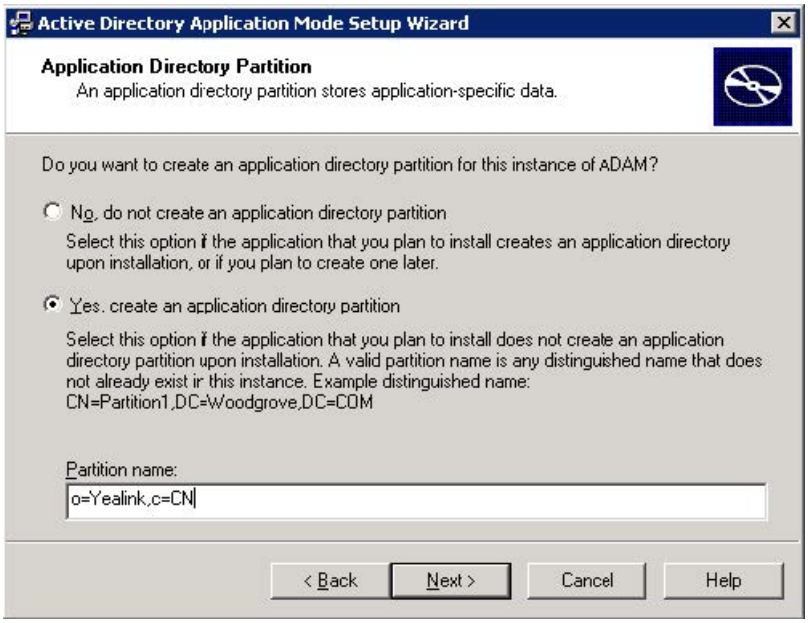
3. Enter the desired name in the **Instance name** field and click **Next**.



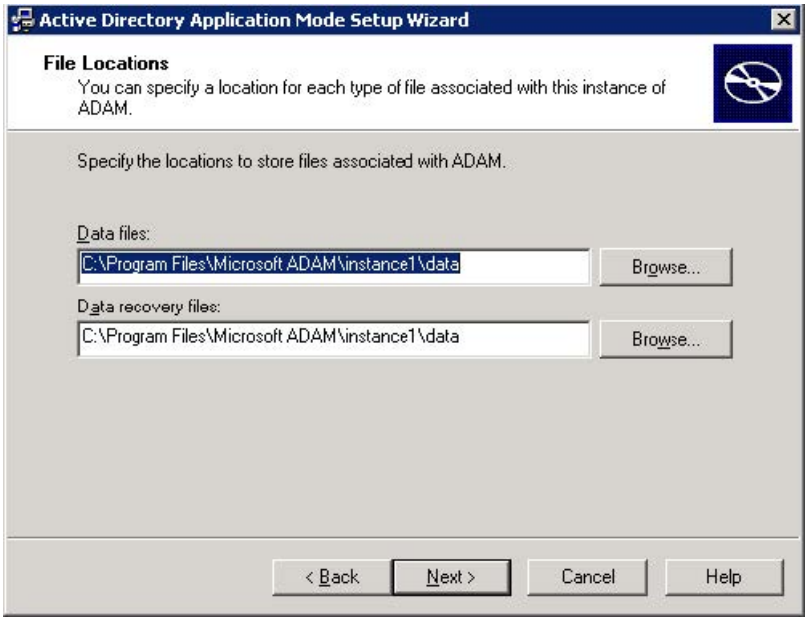
4. Keep the default ports and click **Next**.



5. Select the **Yes, create an application directory partition** check box and enter the desired name (e.g., o=Yealink,c=CN) in the **Partition name** field, and then click **Next**.

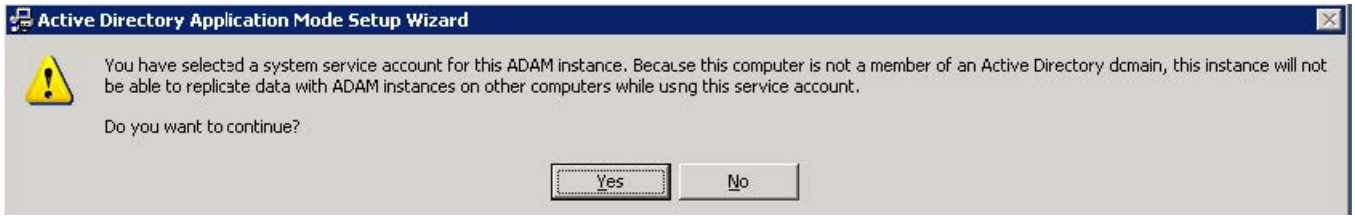


6. Specify the desired paths for the data and data recovery files, and click **Next**.

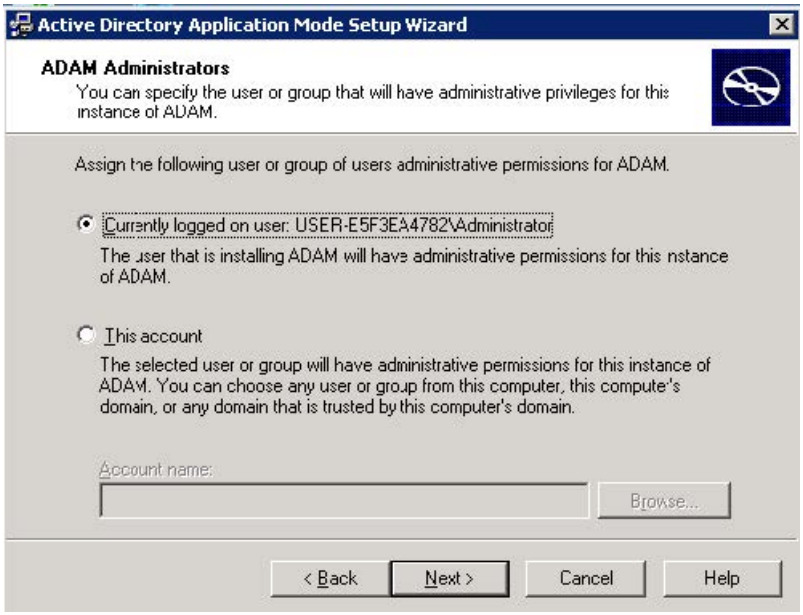


7. Mark the **Network service account** check box and click **Next**.

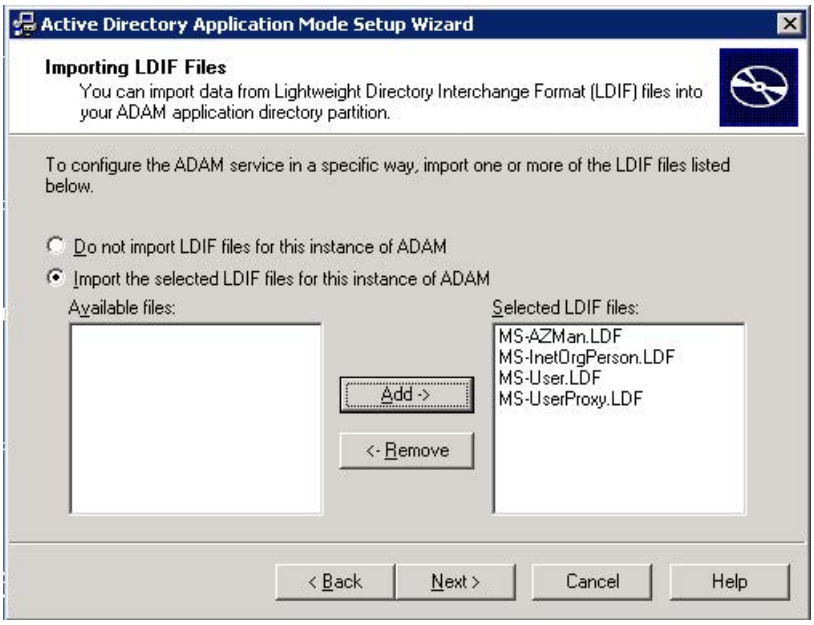
It will pop up the following prompt box. Read the provided information and click **Yes**.



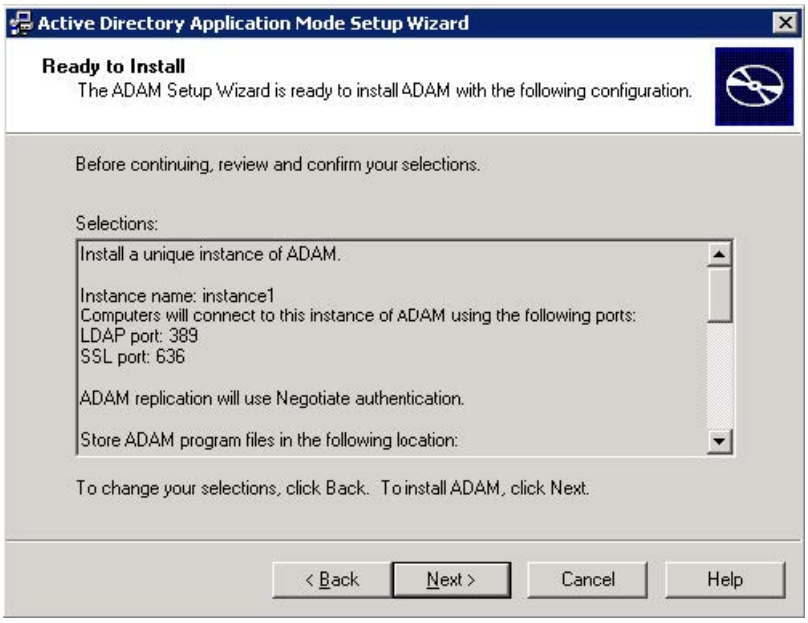
8. Select the first check box to assign the administrative permissions for ADAM to the currently logged on user (e.g., USER-E5F3EA4782) and click **Next**.



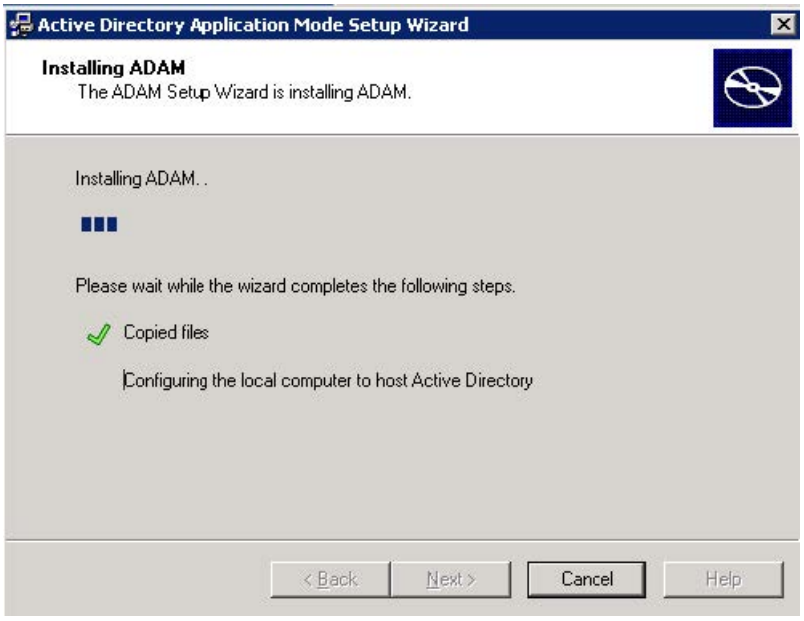
9. Select the **Import the selected LDIF files for this instance of ADAM** check box.
10. In the **Available** files box, select the desired LDF files and then click **Add->**, and then click **Next**.



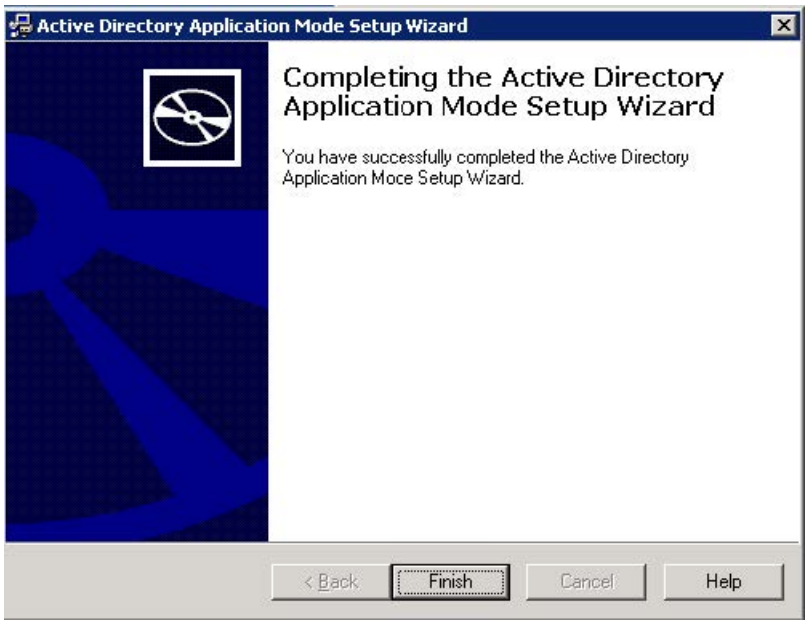
11. Review your selection and click **Next**.



The installing progress is shown as below:



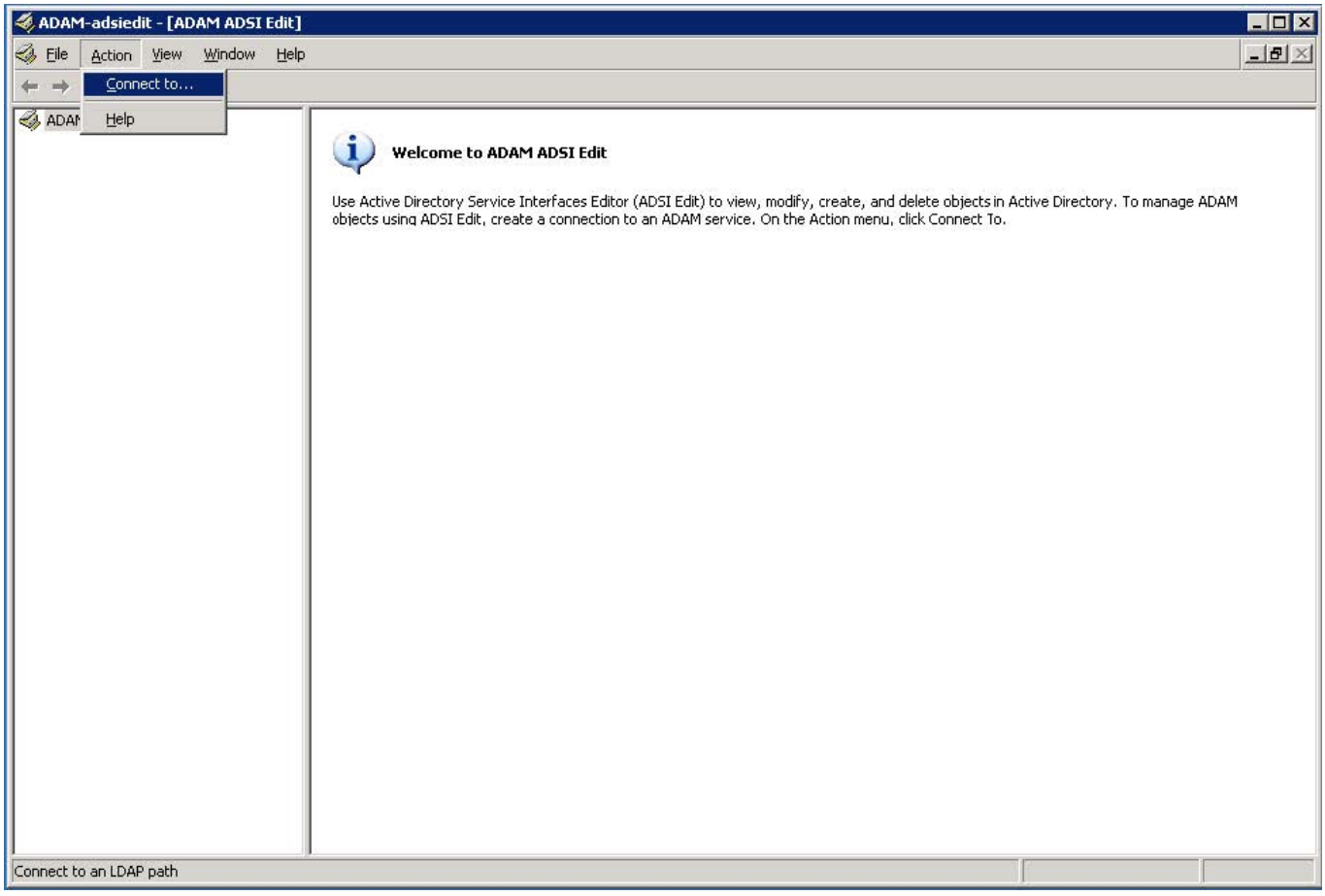
12. Click **Finish** to complete the installation and exit the wizard.



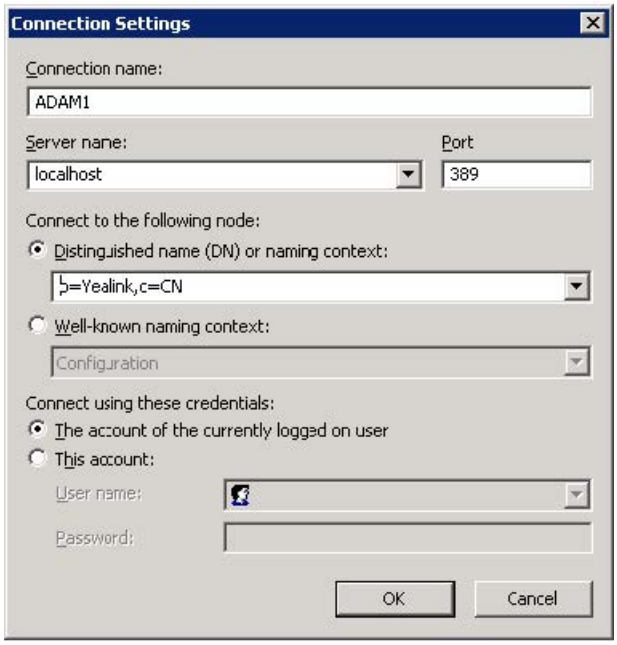
Configure the ADAM ADSI Edit

To configure the ADAM ADSI Edit:

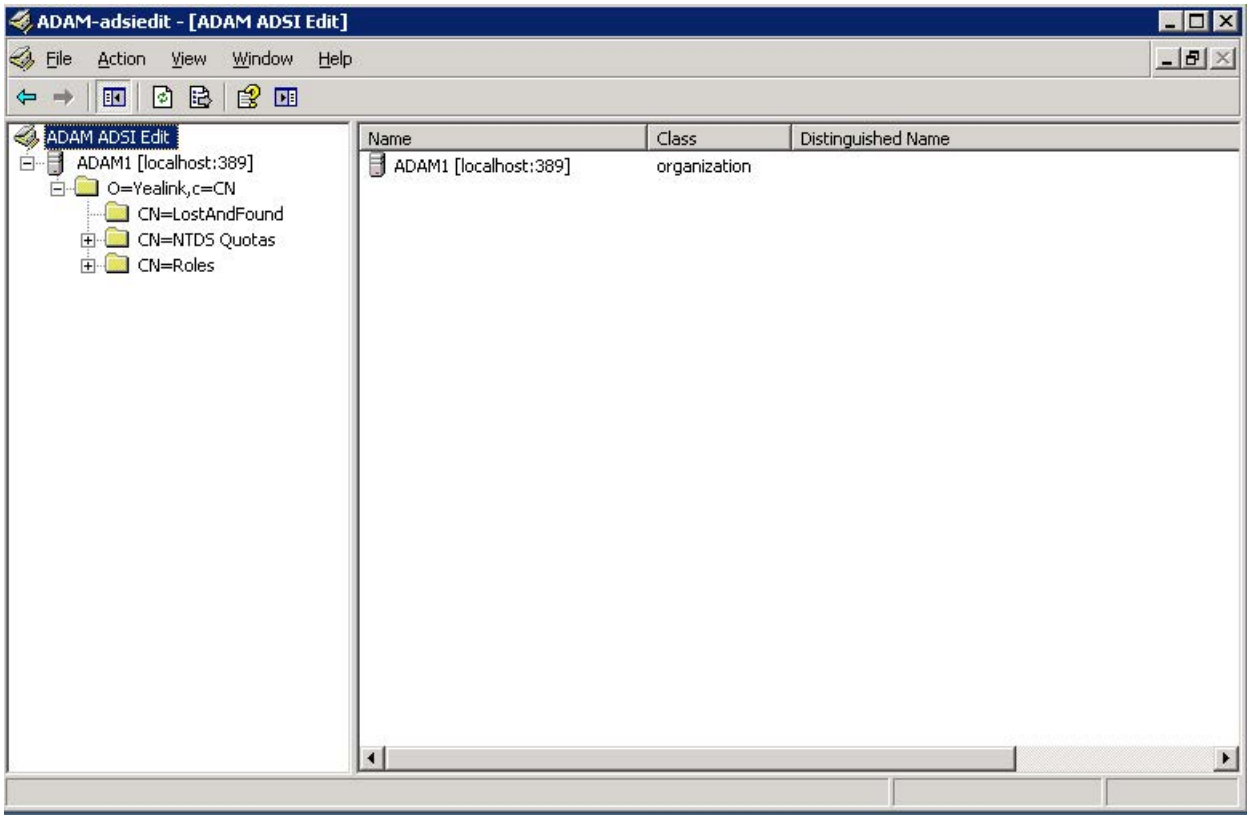
1. Click **Start** > **Programs** > **ADAM** > **ADAM ADSI Edit**.
2. Click **Action** > **Connect to**.



3. Enter the desired name (e.g., ADAM1) in the **Connection name** field.
4. Select the **Distinguished name (DN) or naming context** check box and enter the desired value (e.g., o=Yealink,c=CN) in the following field.
5. Click **OK**.

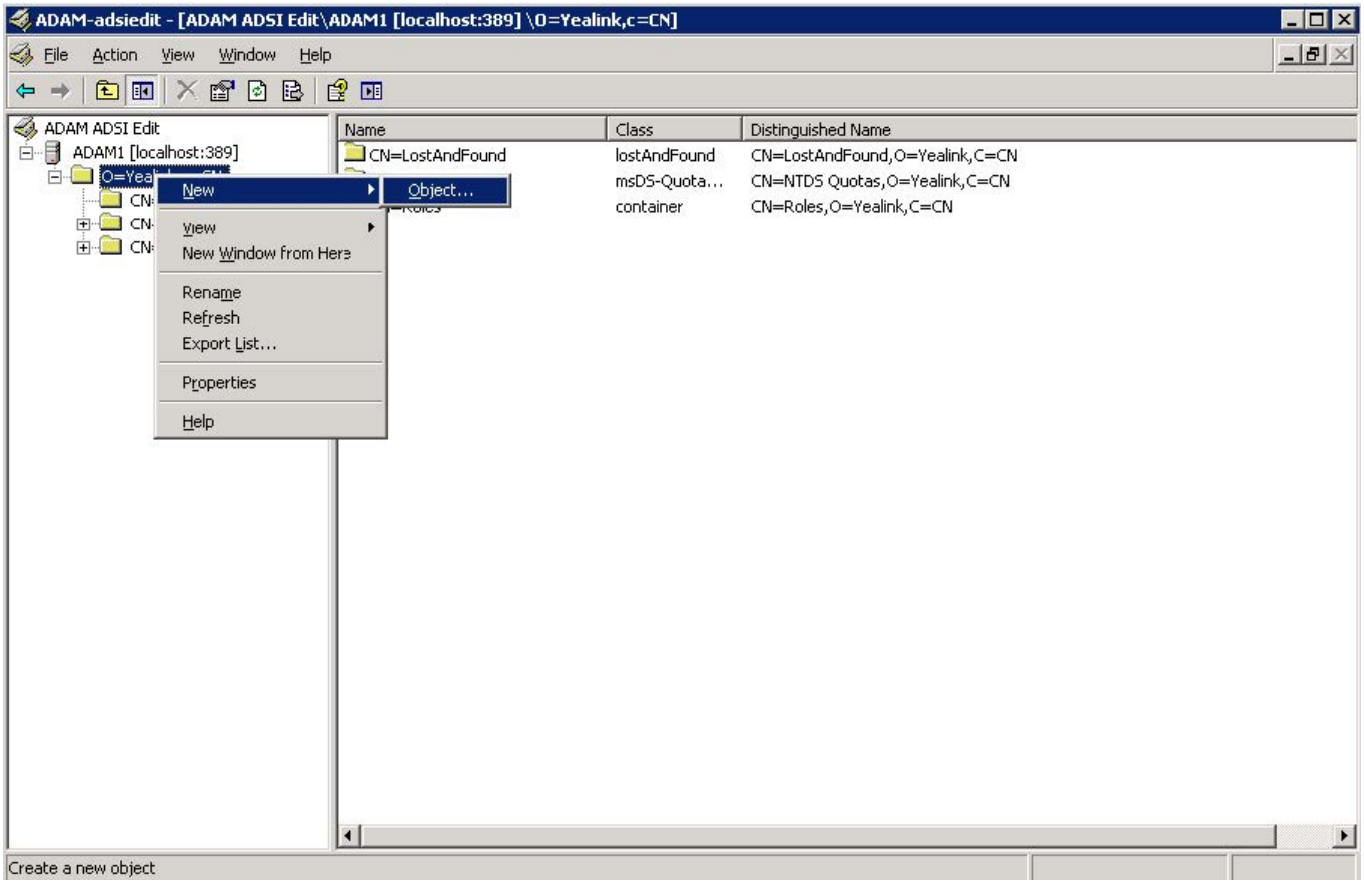


When the ADAM ADSI Edit connects an application directory partition (e.g., o=Yealink,c=CN) successfully, it will show as below:

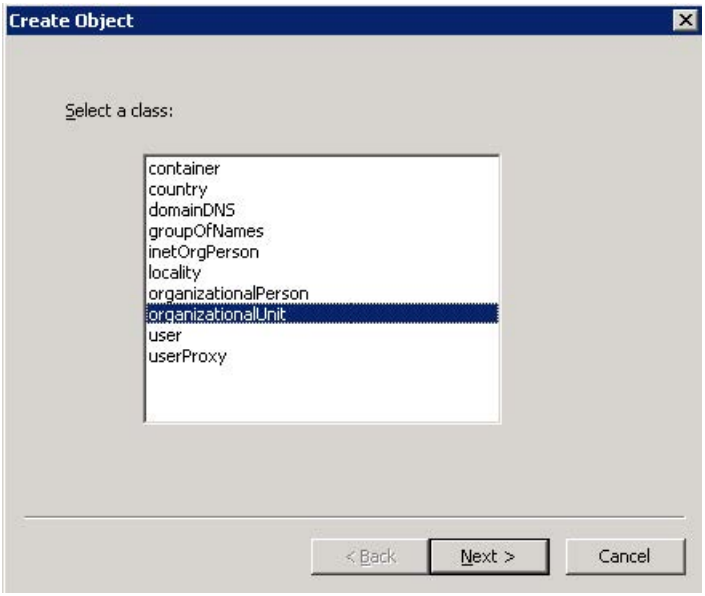


To create the object for ADAM:

1. Select and right click **O=Yealink,c=CN**, and then select **New** > **Object**.



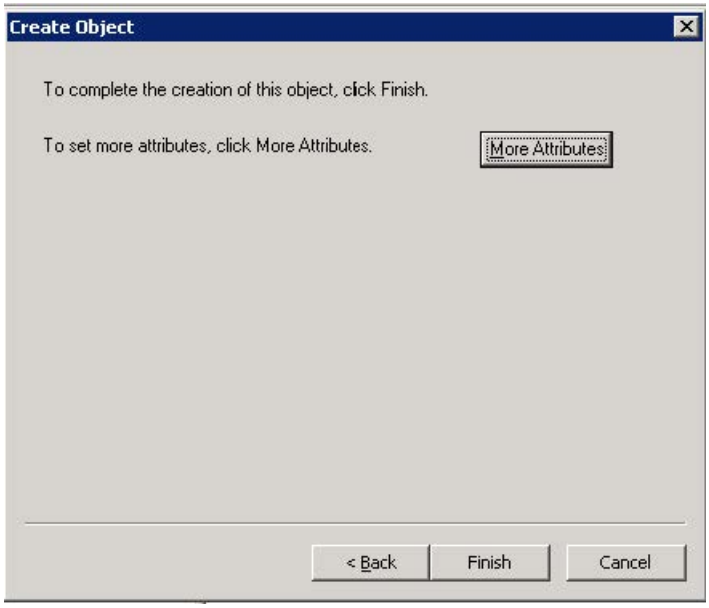
2. Select **organizationalUnit** and click **Next**.



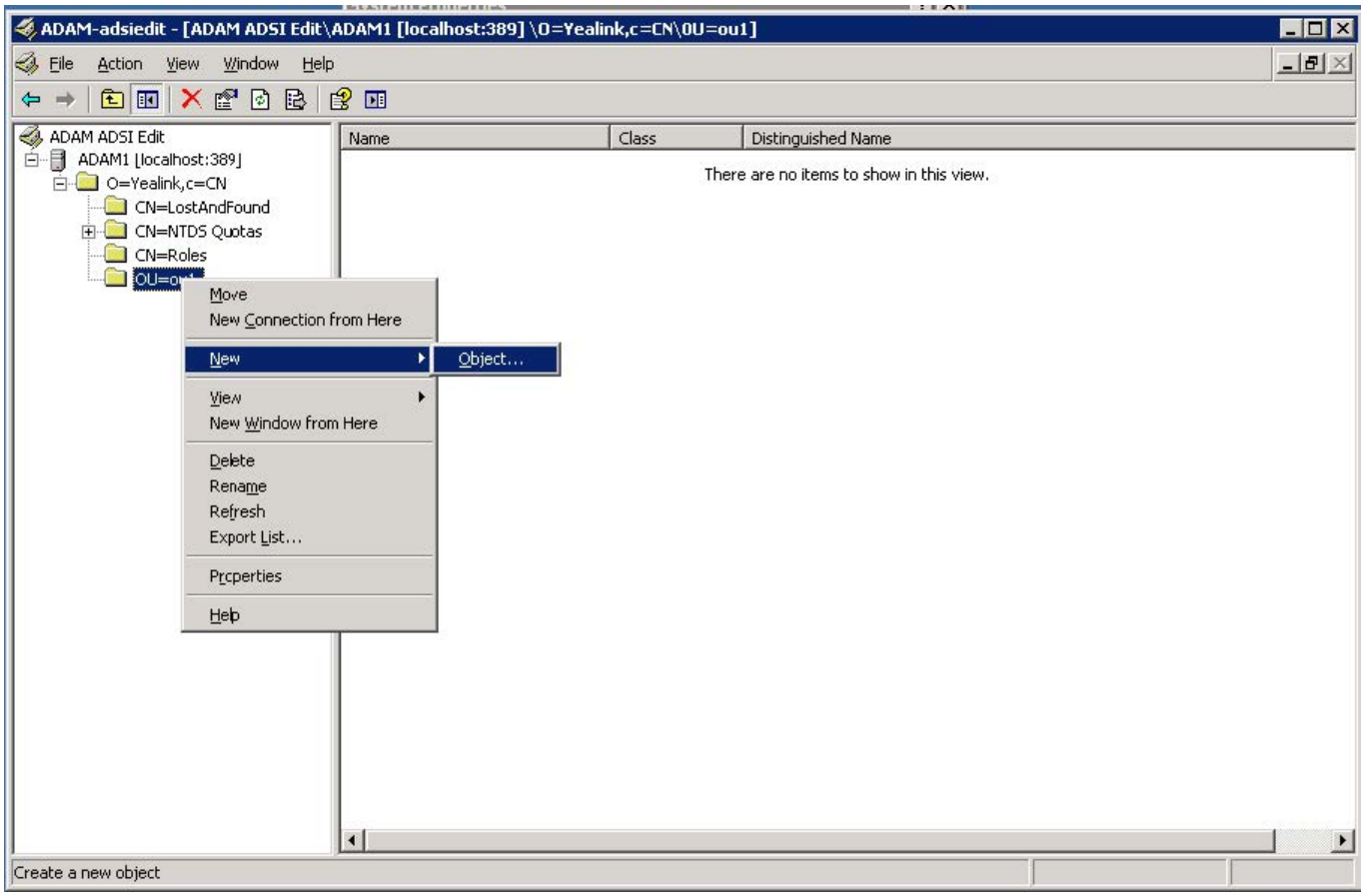
3. Enter the desired value (e.g., ou1) in the **Value** field and click **Next**.

   ![](resource/Enter the desired value (e.g., ou1) in the Value field and click Next…jpg)

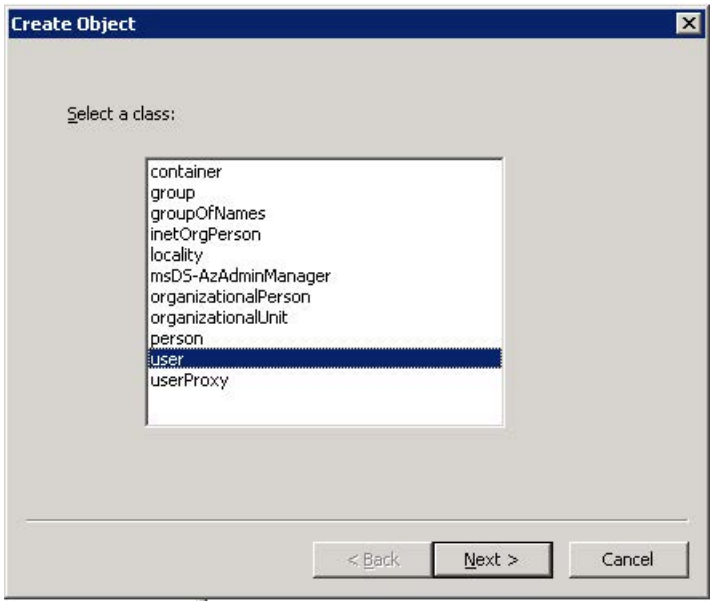
4. Click **Finish** to complete the creation of this object.
   You can also click **More Attributes** to set more attributes for this object.



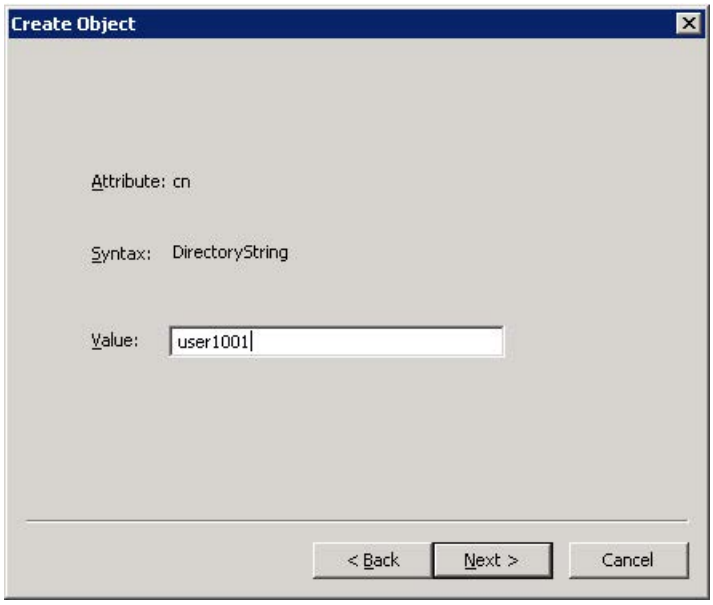
5. Select and right click **OU=ou1**, and then select **New** > **Object**.



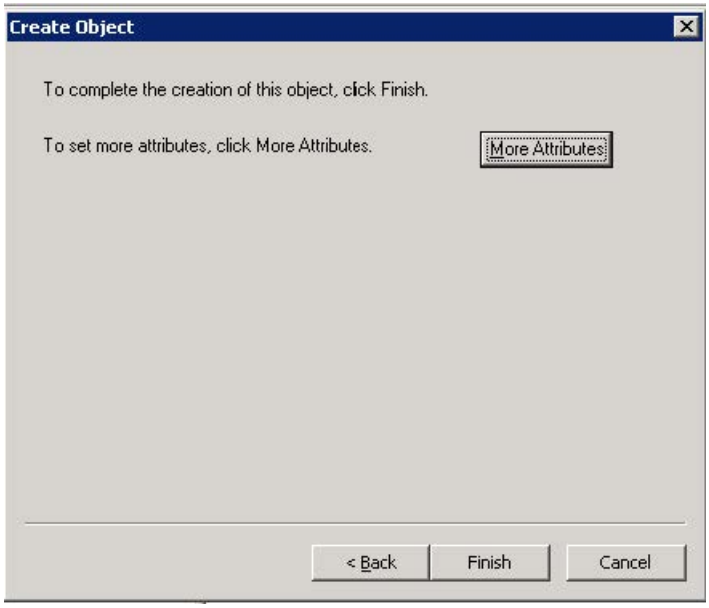
6. Select **user** and click **Next**.



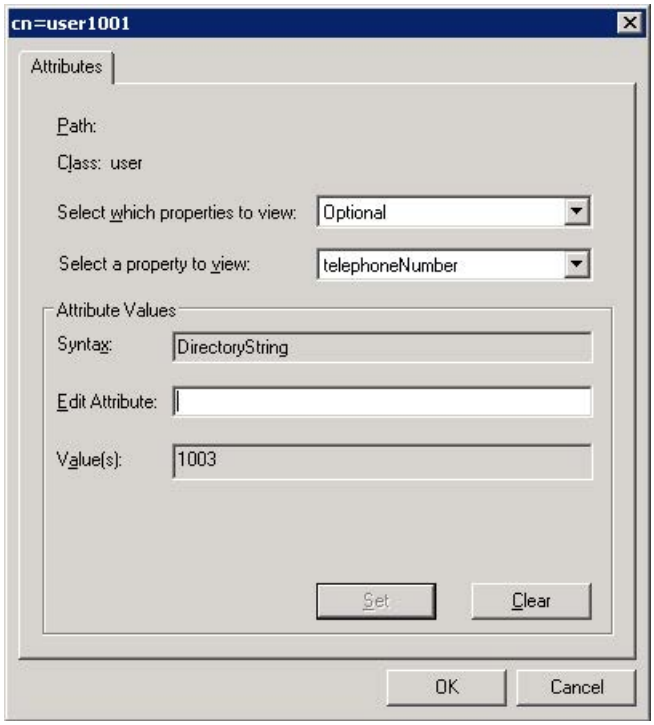
7. Enter the desired value (e.g., user1001) in the **Value** field and click **Next**.



8. Click **More Attributes** to set more attributes for this user.



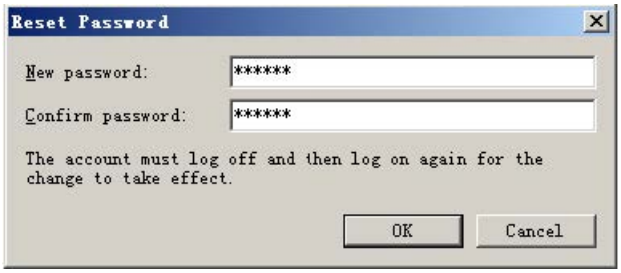
9. In the dialog of Attributes, select the **telephoneNumber** from the **Select a property to view** drop-down menu. Enter the desired telephone number (e.g., 1003) in the **Edit Attribute** field and click **Set**. The entered telephone number will be shown in the **Value(s)** field.



10. Click **OK** to close the Attributes dialog, and click **Finish** to complete the creation of this user.

11. Select and right click the user created above, and then select **Reset Password**.

12. Enter the password for the user created above in the **New password** field and **Confirm password** field respectively.

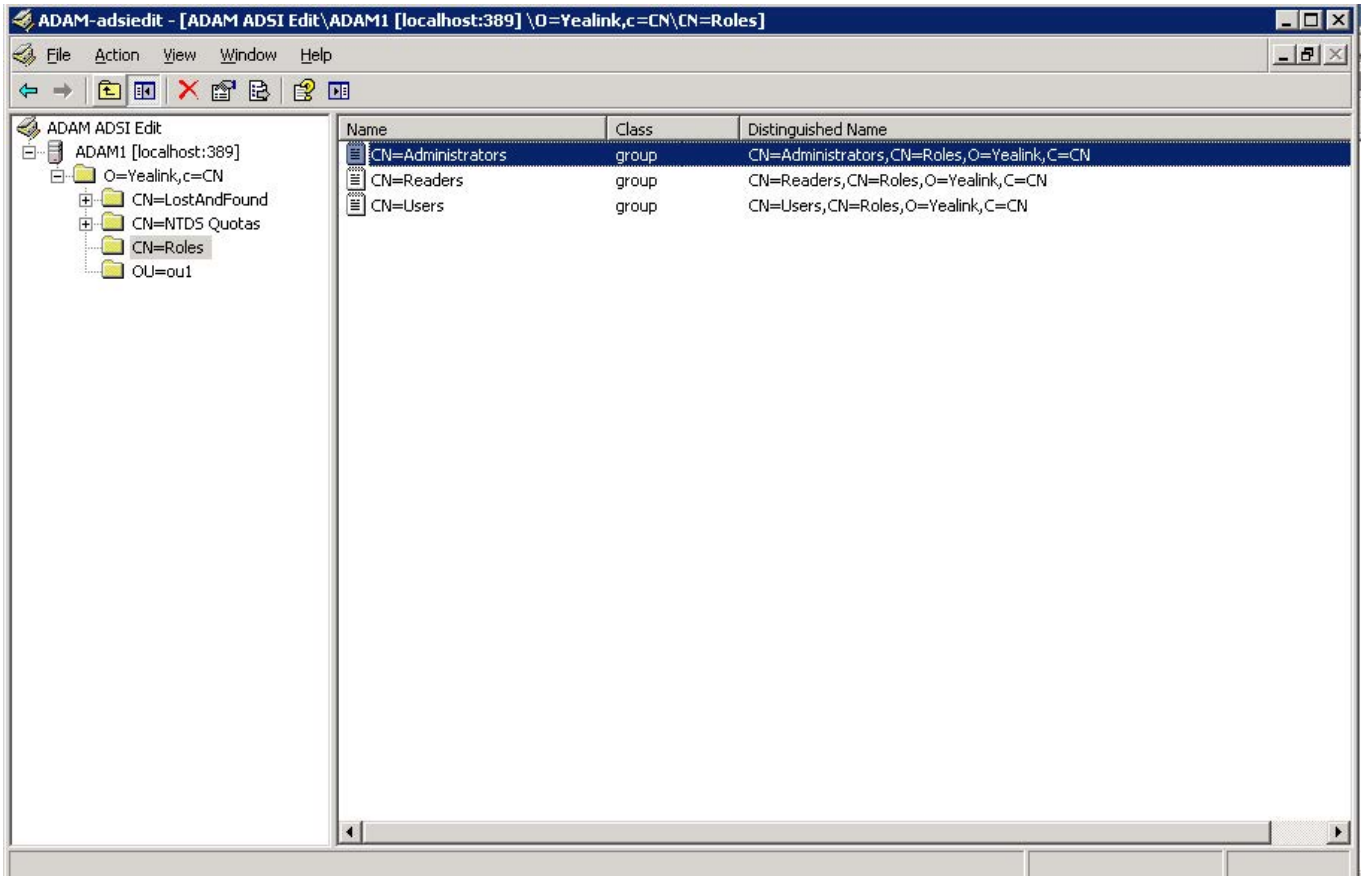


13. Click **OK** to accept the change.

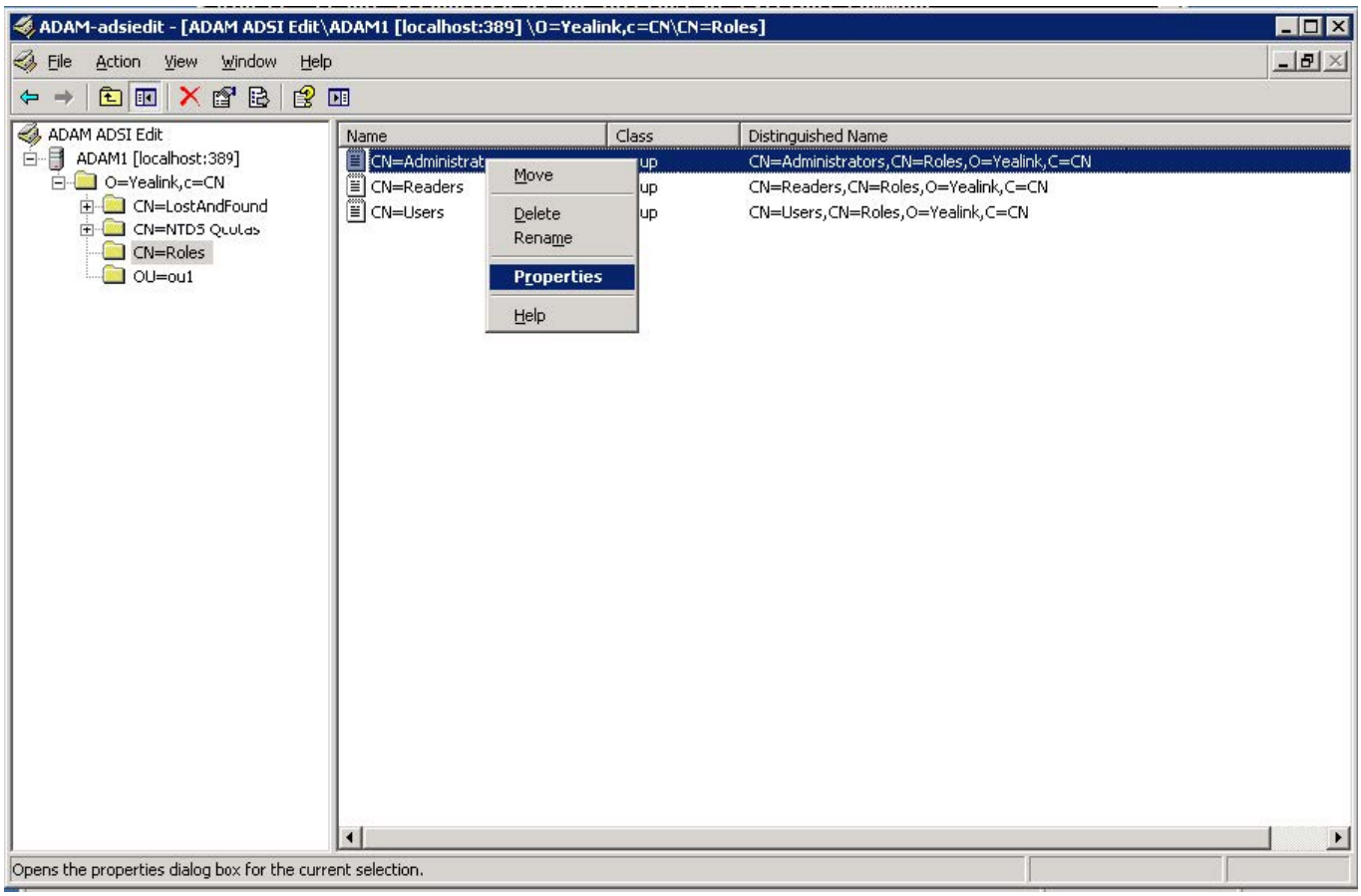
If you want to use the user created above to manage and search for information of LDAP, you need to add the user to the administrator group in advance.

To add the user to the administrator group:

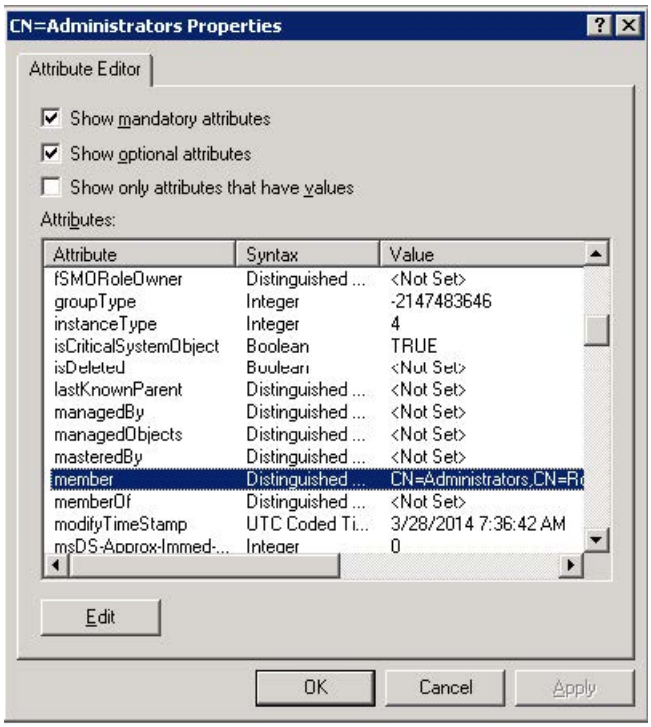
1. Click **ADAM1** > **O=Yealink, c=CN** > **CN=Roles**.



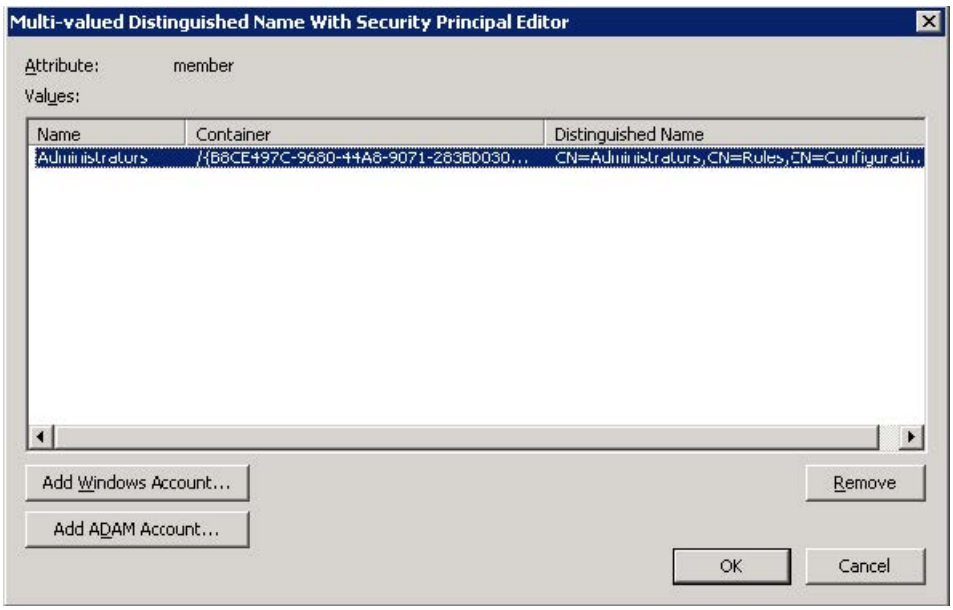
2. Select and right click **CN=Administrators**, and then select **Properties**.



3. Select the **member** attribute in the **Attributes** box and click **Edit**.



4. In the dialog of the member attribute, click **Add ADAM Account**.



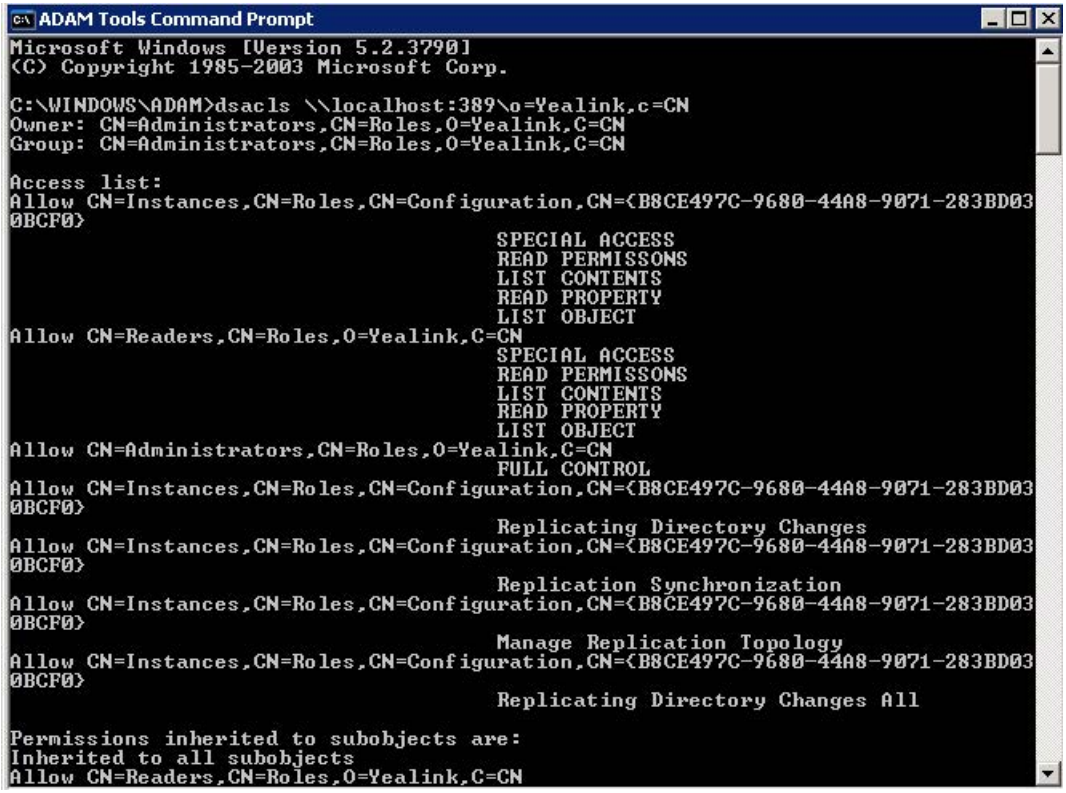
5. In the dialog of adding the ADAM account, enter the desired distinguished name (e.g., CN=user1001,OU=ou1,o=Yealink,c=CN) in the field.
6. Click **OK** to accept the change and close the dialog of adding the ADAM account.
7. Click **OK** to accept the change and close the dialog of the member attribute.
8. Click **OK** to accept the change and close the Administrators Properties interface.

You can also view the permissions of ADAM using the command.

To view permissions using the command:

1. Click **Start** > **Programs** > **ADAM** > **ADAM Tools Command Prompt**.

2. Execute the command `dsacls \\localhost:389\o=Yealink,c=CN` view permissions of o=Yealink,c=CN.



Sun One Directory Server

Sun One Directory Server, also known as Sun Java System Directory Server, is a component of the Java Enterprise System. Sun One Directory Server can be installed on multiple platforms, such as Windows, Linux, Solaris and so on. This section shows you how to install Sun One Directory Server version 5.2 on Microsoft Windows Server 2003 SP2 Enterprise 32-bit system. You can download it online: http://download.csdn.net/download/wbsoso/6439291.

Before the installation, you should prepare as follows:

- Modify the hosts file of your computer.
- Install the Java Development Kit (JDK) 5 or later.

To modify the hosts file of your computer:

1. Locate the hosts file in the path “C:\WINDOWS\system32\drivers\etc\hosts”.
2. Open and edit the hosts.dz file using your favorite text editor.
3. Add FQCN (Fully Qualified Computer Name) of your computer to the file. For example, the FQCN of your computer is ldapsun.yealinktest.com. Add the following mapping:

```
127.0.0.1               ldapsun.yealinktest.com
```

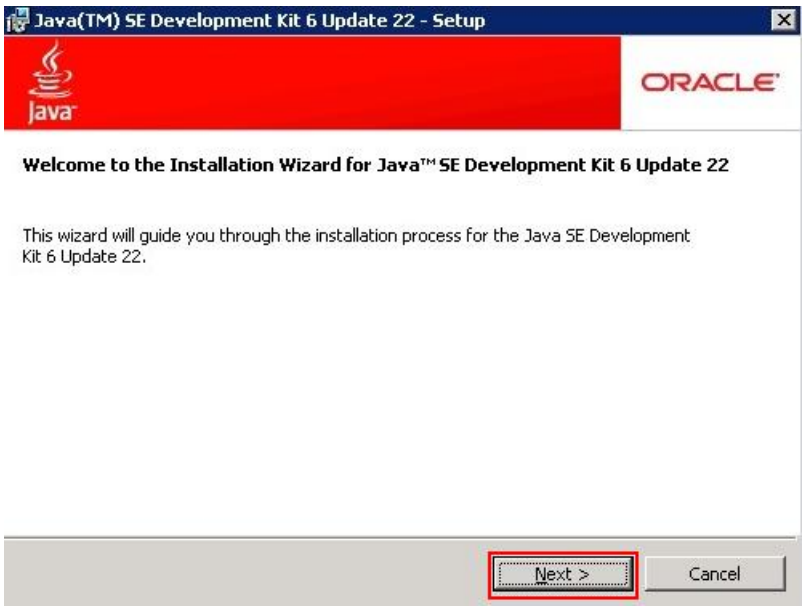
```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
127.0.0.1       ldapsun.yealinktest.com
```

4. Save the hosts file.

The following shows you how to install the Java Development Kit (JDK) 6 on your computer. You can download it online: http://www.oracle.com/technetwork/java/javase/downloads/index.html.

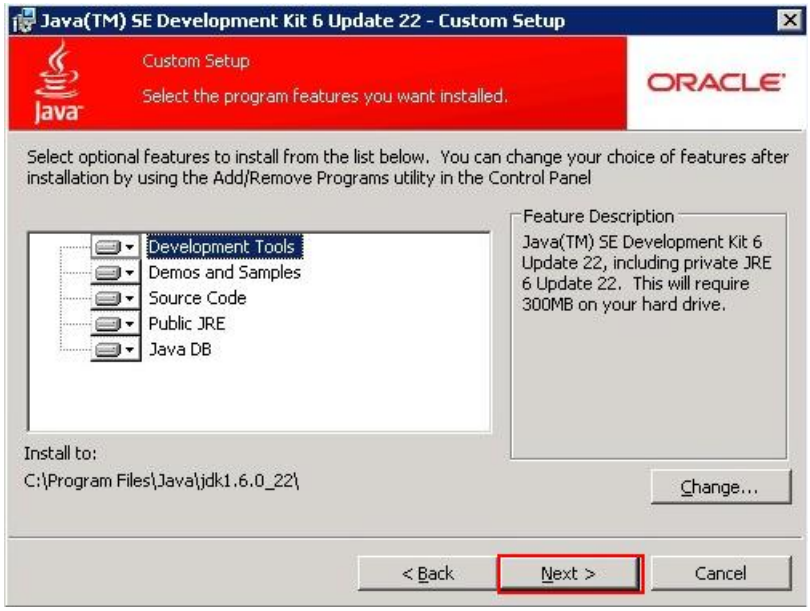
To install the Java Development Kit (JDK) 6:

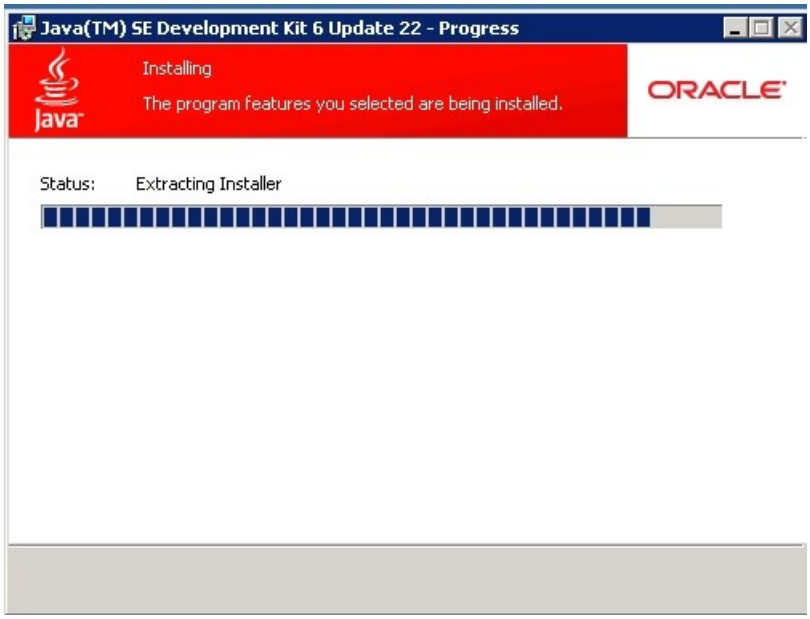
1. Double click jdk-6u22-windows-i586.exe to run the application.
2. The Java ™ SE Development Kit 6 Update 22 Installation Wizard will appear after a short while, click **Next**.

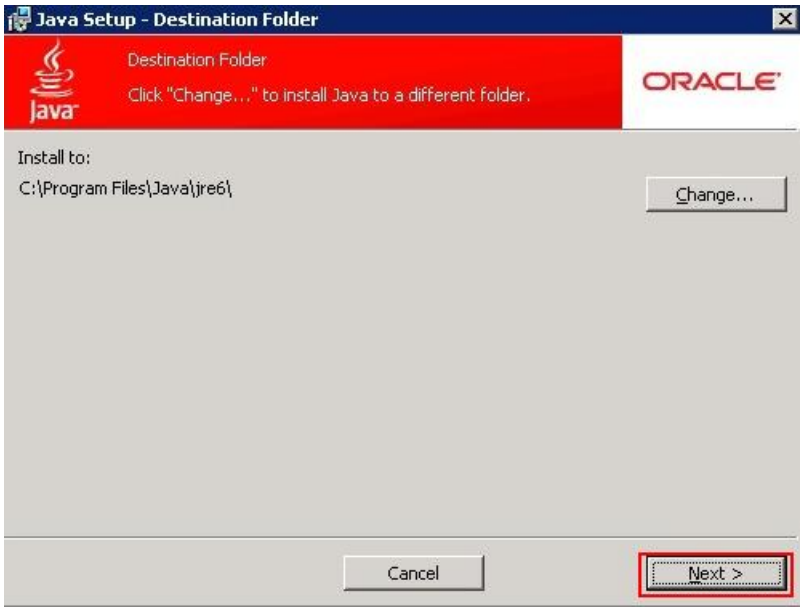


3. Click **Change** to locate the installation path from the local computer system and then click **Next**.

   You need to remember the installation path (e.g., C:\Program Files\Java\jdk1.6.0_22) located here.
   The screenshot for reference is shown as below:


Java(TM) SE Development Kit 6 Update 22 - Custom Setup
Custom Setup
Select the program features you want installed.
ORACLE
Select optional features to install from the list below. You can change your choice of features after installation by using the Add/Remove Programs utility in the Control Panel
Development Tools
Demos and Samples
Source Code
Public JRE
Java DB
Feature Description
Java(TM) SE Development Kit 6 Update 22, including private JRE 6 Update 22. This will require 300MB on your hard drive.
Install to:
C:\Program Files\Java\jdk1.6.0_22\
Change...
< Back
Next >
Cancel


Java(TM) SE Development Kit 6 Update 22 - Progress
Installing
The program features you selected are being installed.
ORACLE
Status: Extracting Installer

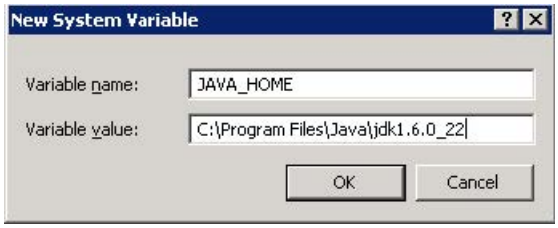

Java Setup - Destination Folder
Destination Folder
Click "Change..." to install Java to a different folder.
ORACLE
Install to:
C:\Program Files\Java\jre6\
Change...
Cancel
Next >

4. Click **Finish** to finish the installation.
   After the installation, you need to configure environment variables.

To configure environment variables:

1. Right click the **My Computer** icon and select **Properties**.
2. Click the **Advanced** tab.
3. Click the **Environment Variables** button.
4. Add the following variables, click **New** under **System Variables**.
5. Enter the variable name as JAVA_HOME.

6. Enter the variable value as the installation path (e.g., C:\Program Files\Java\jdk1.6.0_22) for the Java Development Kit.

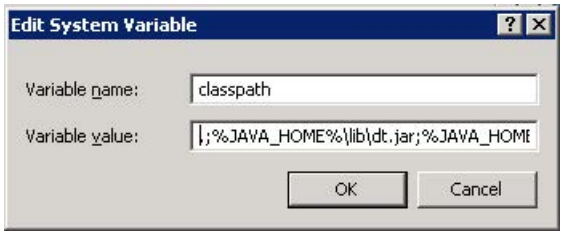


7. Click **OK**.

8. Repeat steps 4-7 to create a new system variable.

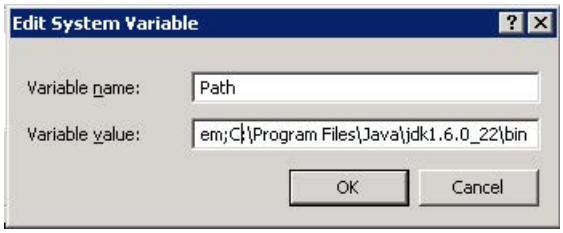
   Variable name: classpath
   Variable value: .;%JAVA_HOME%\lib\dt.jar;%JAVA_HOME%\lib\tools.jar
   The dot "." stands for the current path and it can't be deleted.

   %JAVA_HOME% references the value of the specified JAVA_HOME variable created before.



9. Under **System Variables**, select the **Path** variable and click **Edit**.

10. In the **Variable value** field, append the Java bin directory (e.g., C:\ProgramFiles\Java\jdk1.6.0_22\bin) to the end of the existing path (e.g.,%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;). If the end of the existing path has no semicolon, you should add a semicolon to the end of the existing path and then append the Java bin directory.



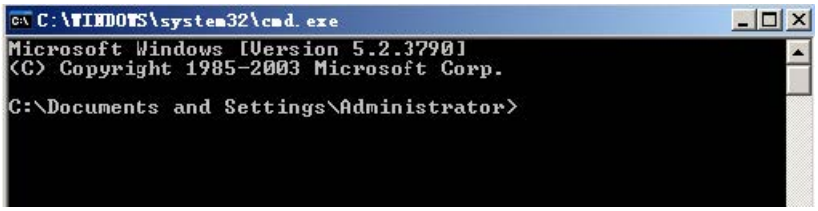
11. Click **OK**.

12. Click **Apply Changes**.

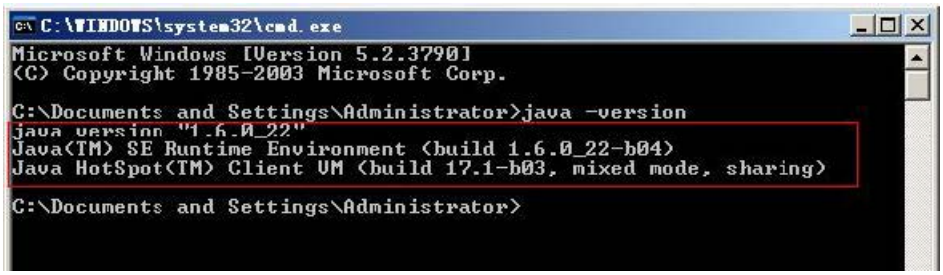
To verify the configuration of environment variables:

1. Click **Start** > **Run**.

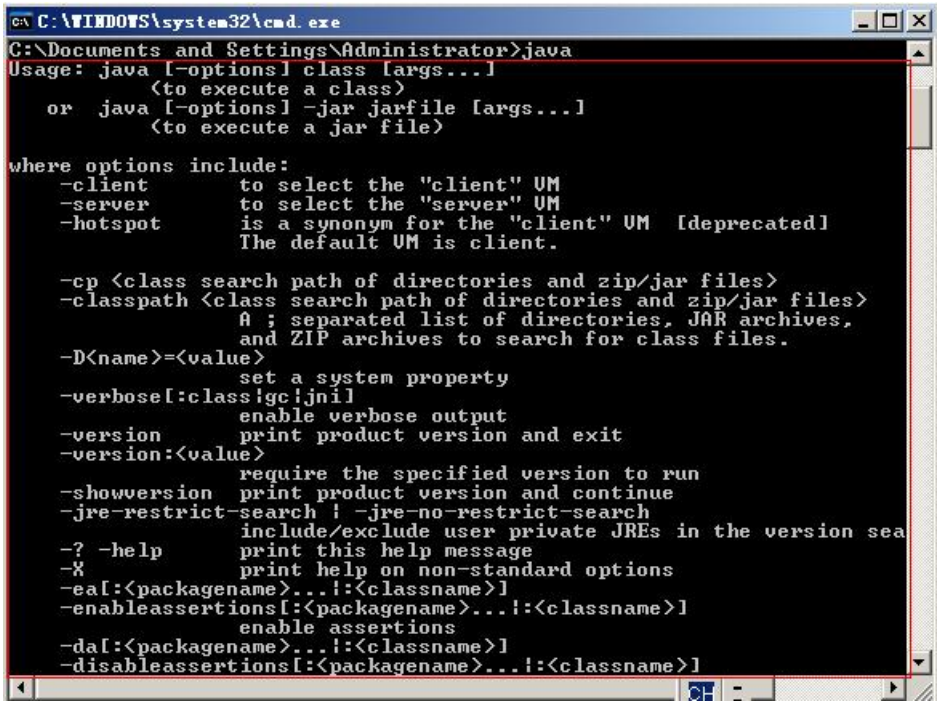
2. Enter **cmd** in the dialog and click **OK** to enter the command line interface.



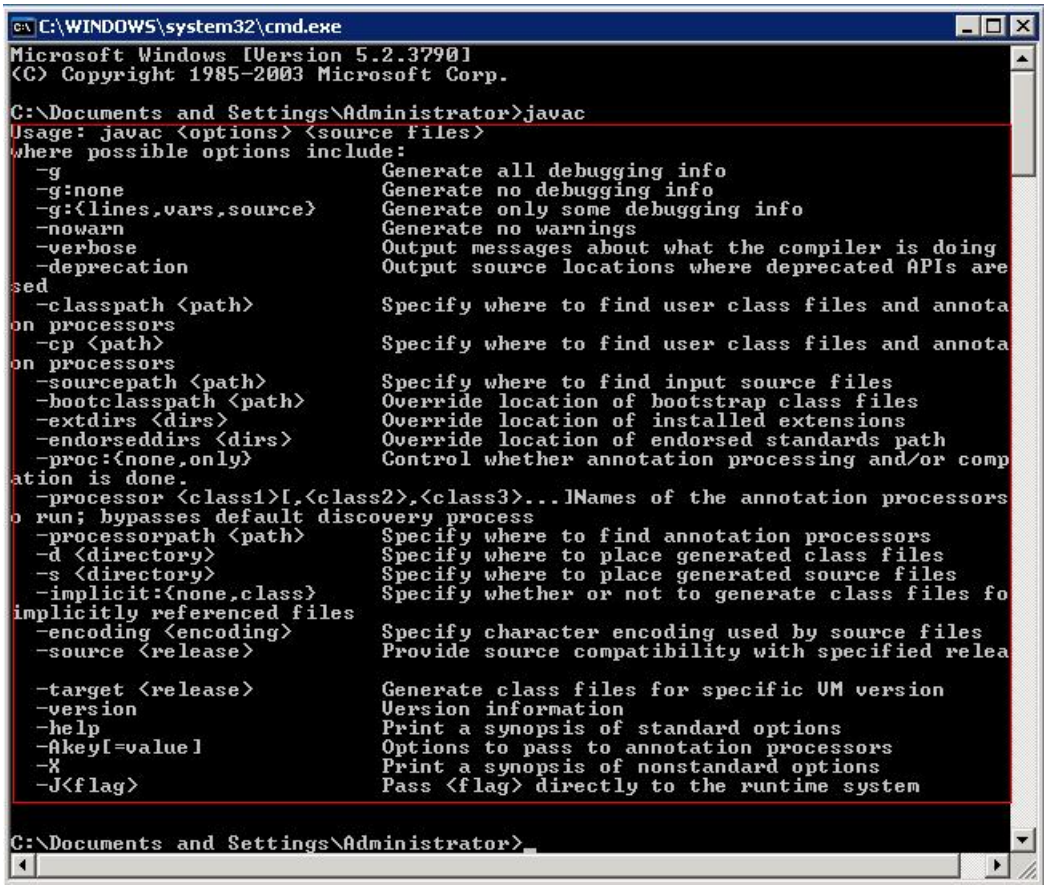
3. Execute the command **java -version** to check the java version.



4. Execute the command **java** to run the application.



5. Execute the command **javac** to compile java files into class files.

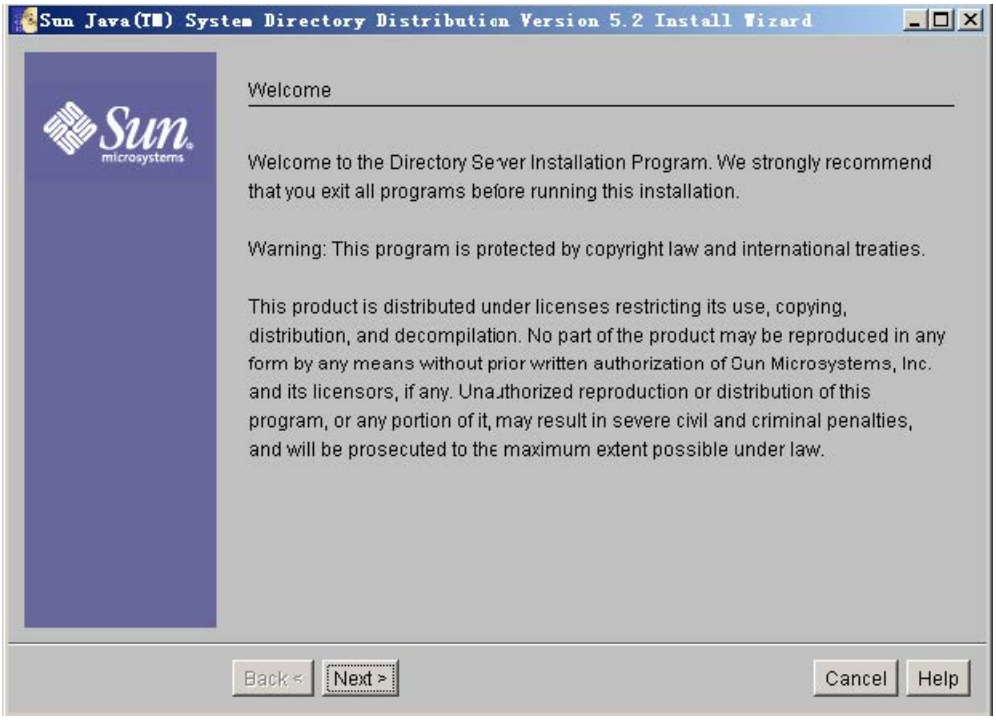


Install the Sun One Directory

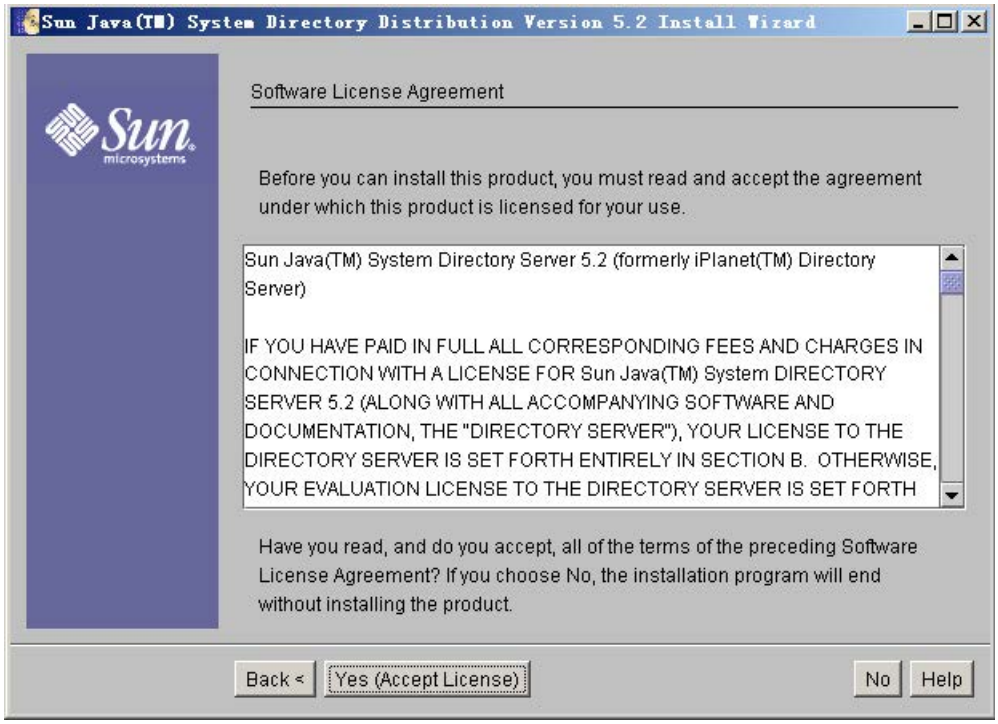
To install the Sun One Directory:

1. Unpack the compressed files named Sun Java System Directory Server.5.2.P4.Windows.full.rar.
2. Double click setup.exe to run the application.

3. The Sun Java™ System Directory Distribution Version 5.2 Install Wizard will appear after a short while, click **Next**.

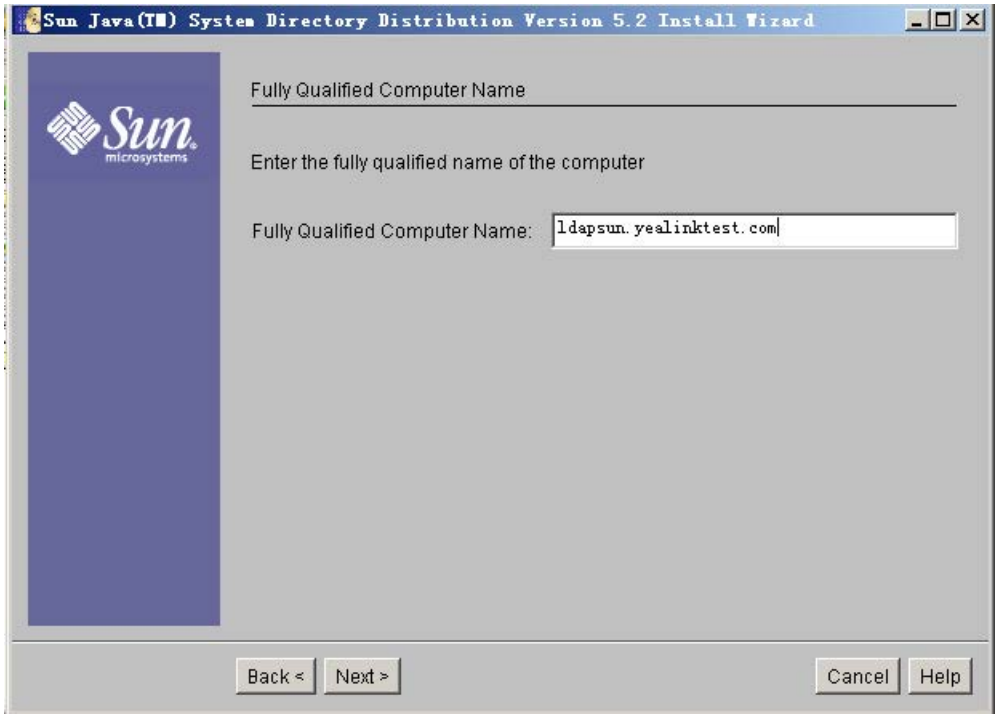


4. Read the software license agreement and click **Yes (Accept License)**.

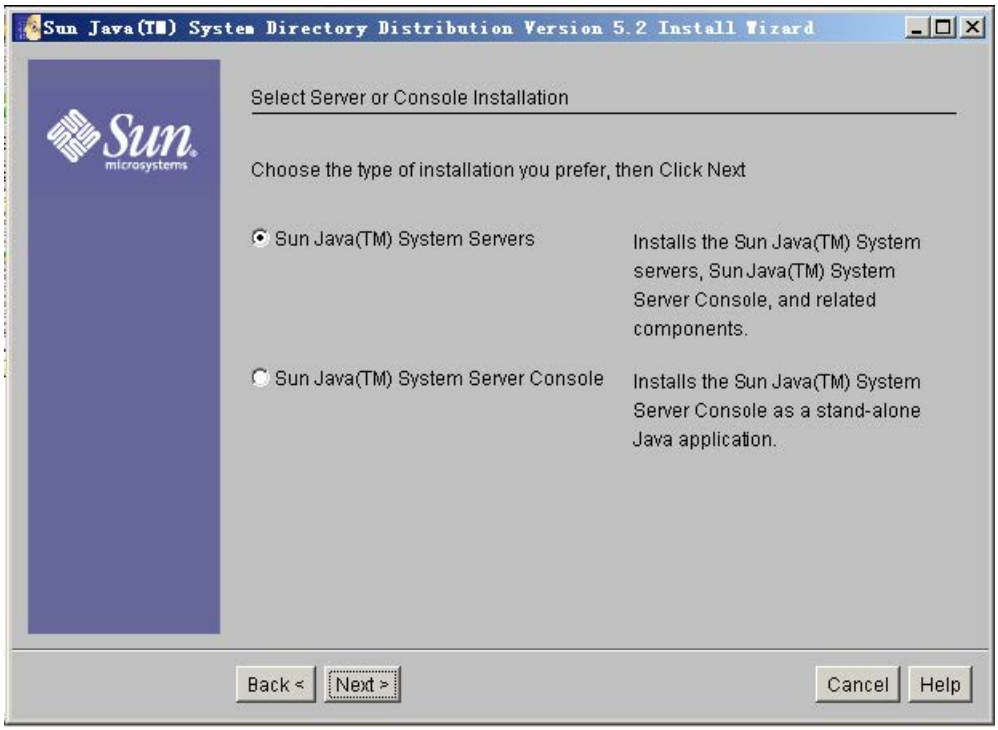


5. Enter the fully qualified name of the computer (e.g., ldapsun.yealinktest.com) in the **Fully Qualified Computer Name** field and click **Next**.

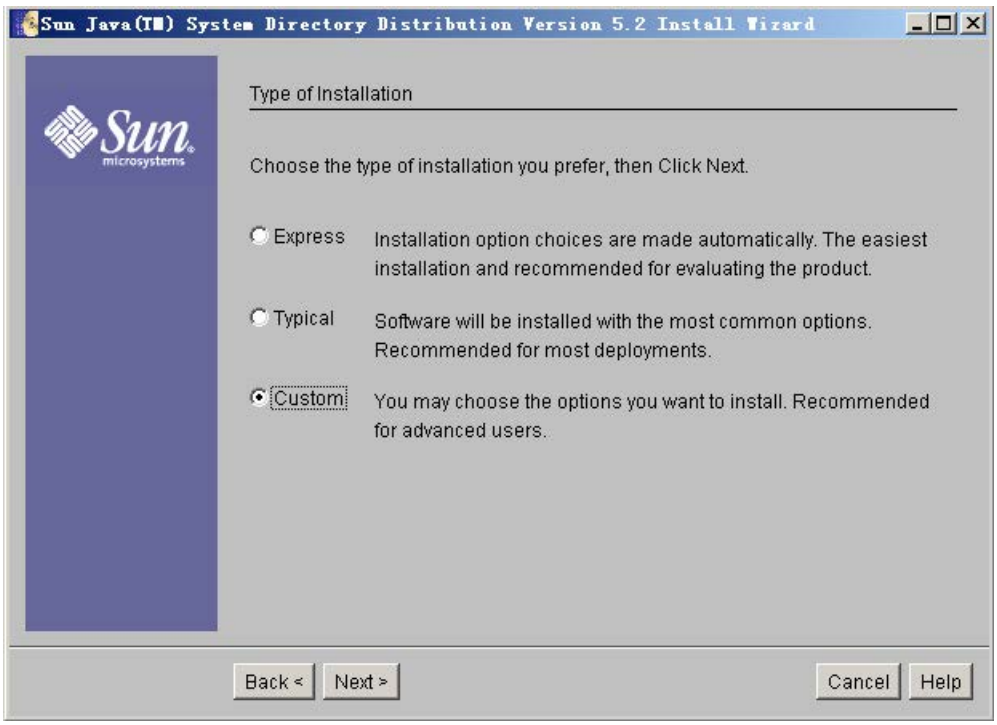
   The fully qualified name of the computer was planned before. For more information, refer to modify the hosts file of your computer.



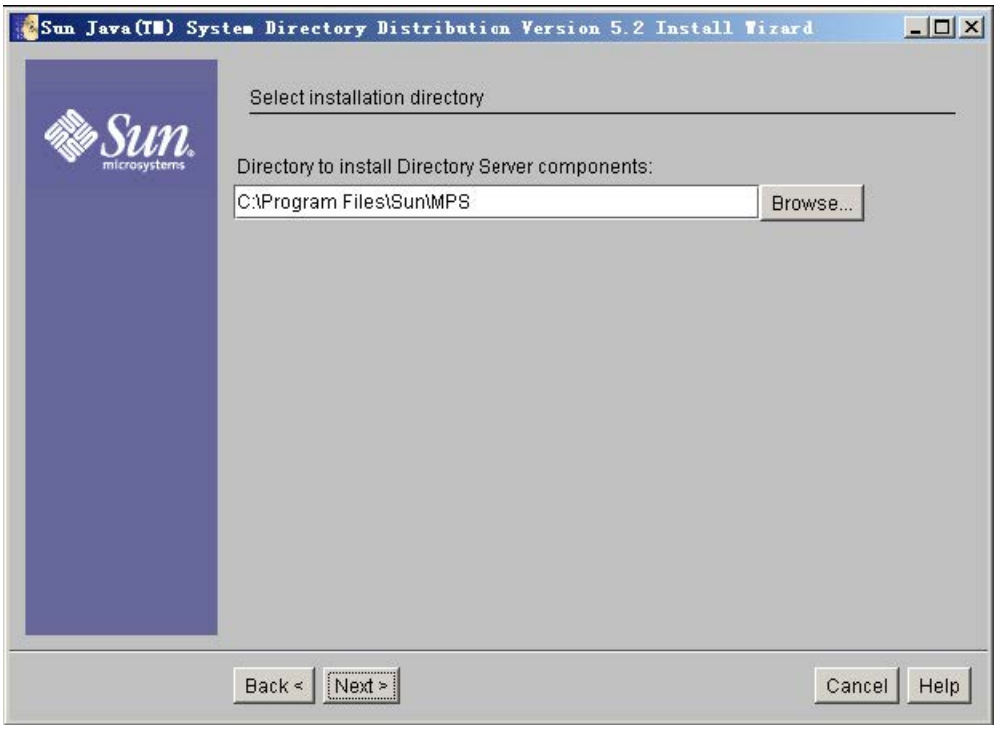
6. Select the **Sun Java ™ System Servers** check box and click **Next**.



7. Select the **Custom** check box and click **Next**.

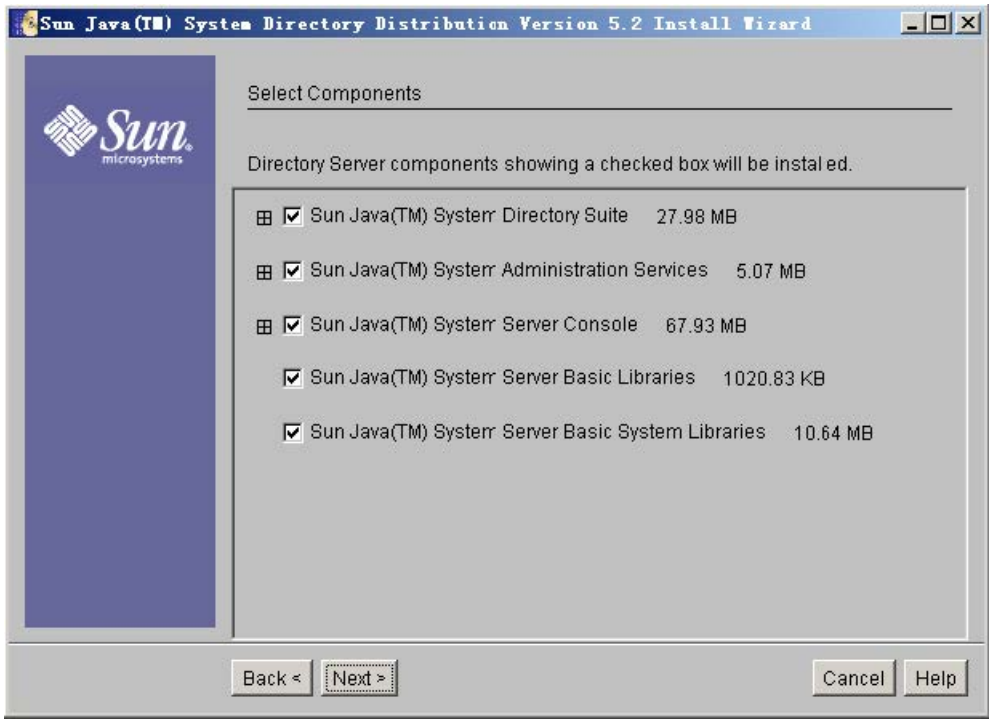


8. Specify the desired installation directory and click **Next**.

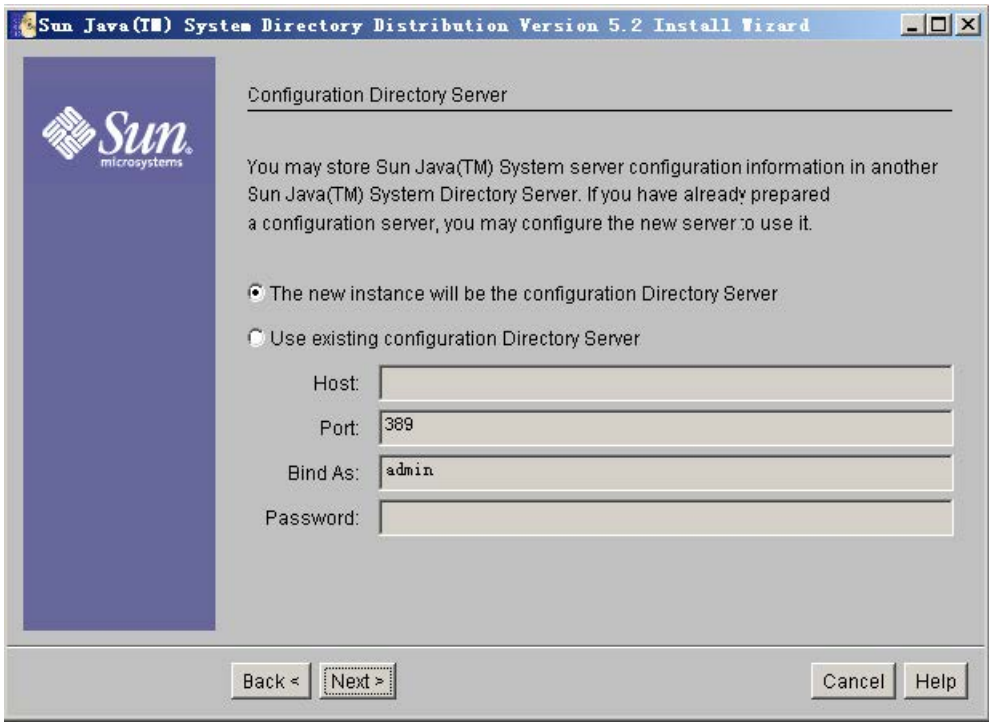


It prompts the following window. And you can click **Create Directory** to create the directory or click **Choose New** to select another path.

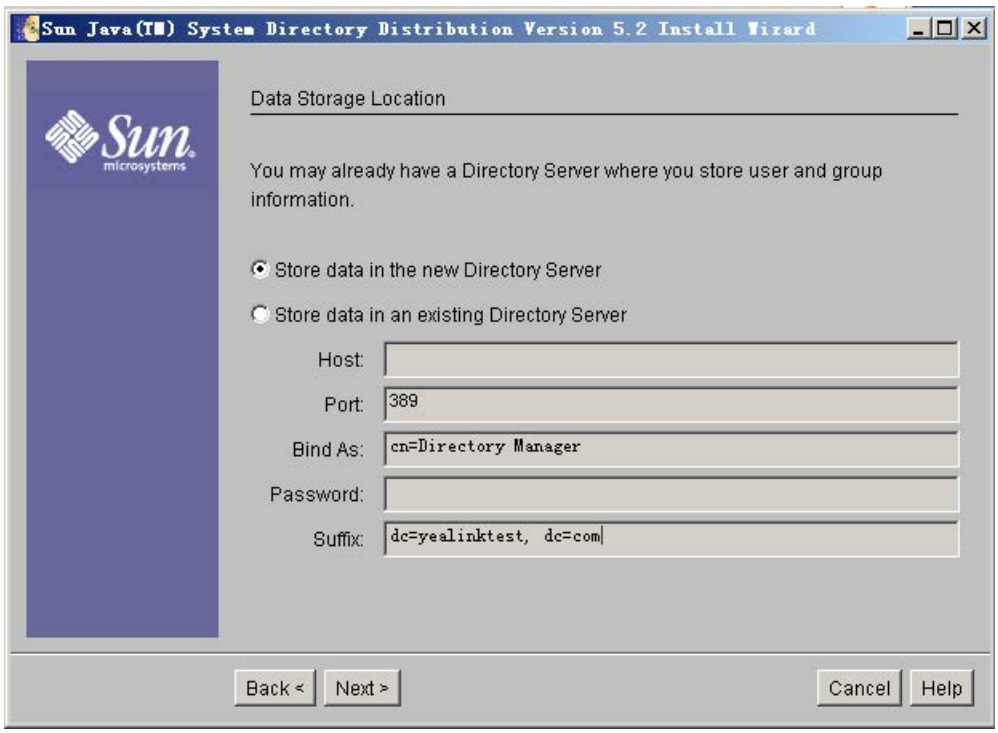
9. Select the desired installation components and click **Next**.



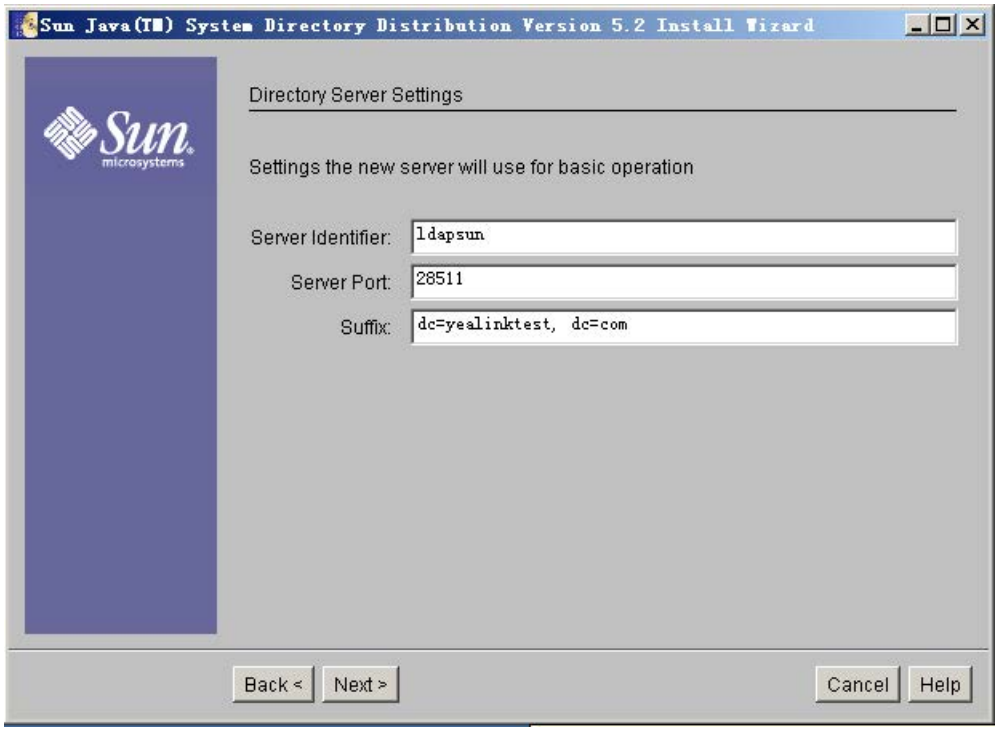
10. Select **The new instance will be the configuration Directory Server** check box and click **Next**.



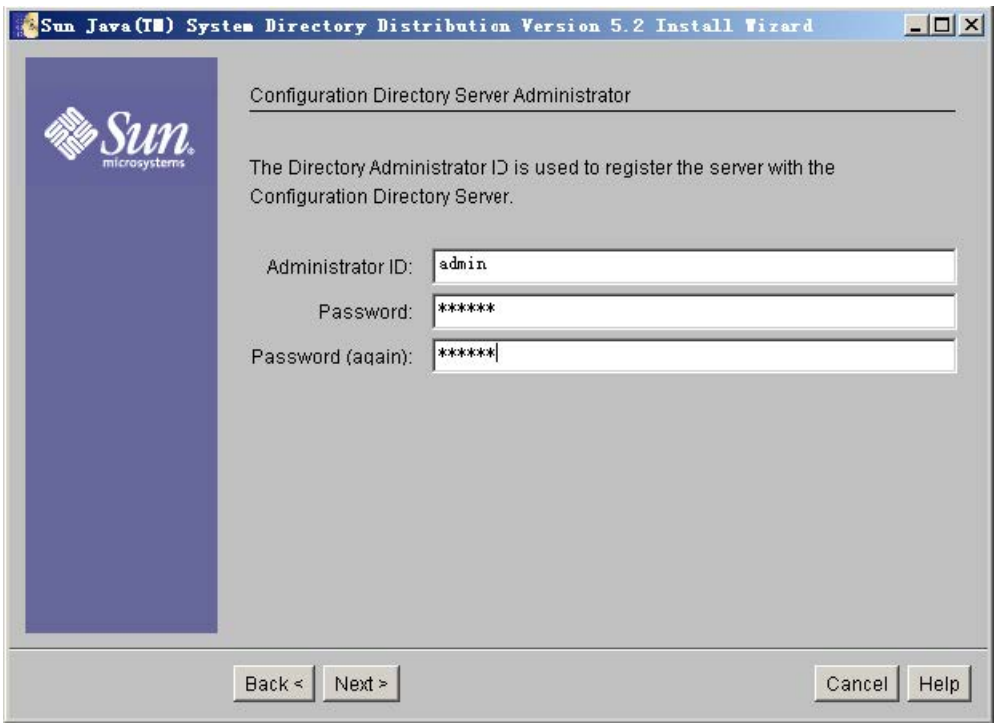
11. Select the **Store data in the new Directory Server** check box and click **Next**.



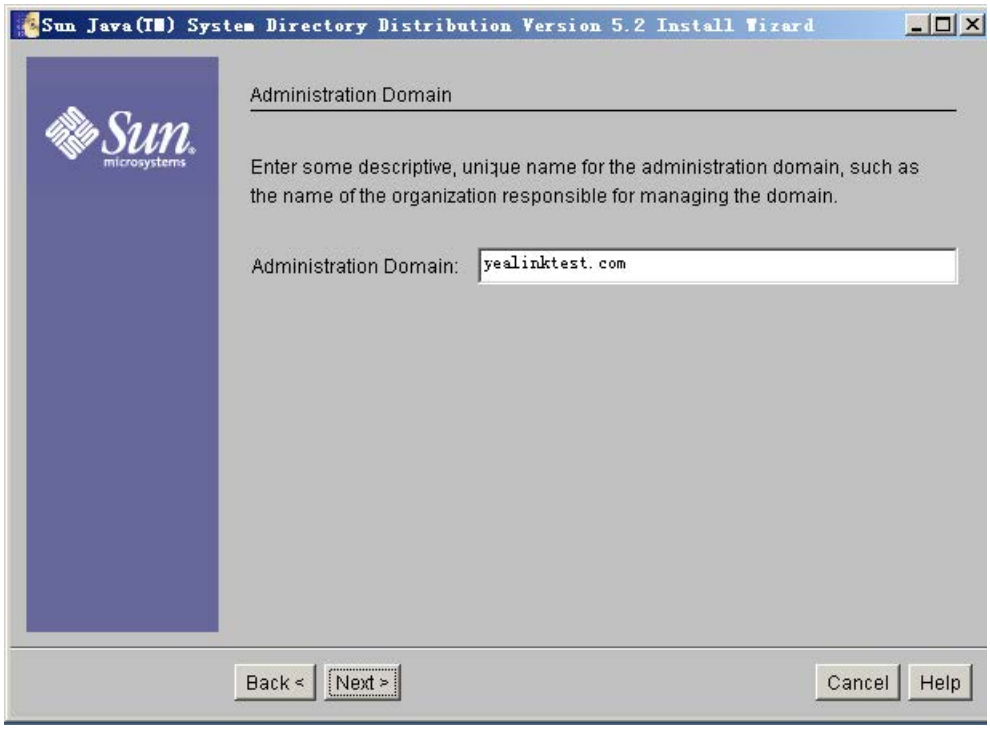
12. Enter the value "ldapsun" in the **Server Identifier** field and keep the default values in the other two fields. And then click **Next**.



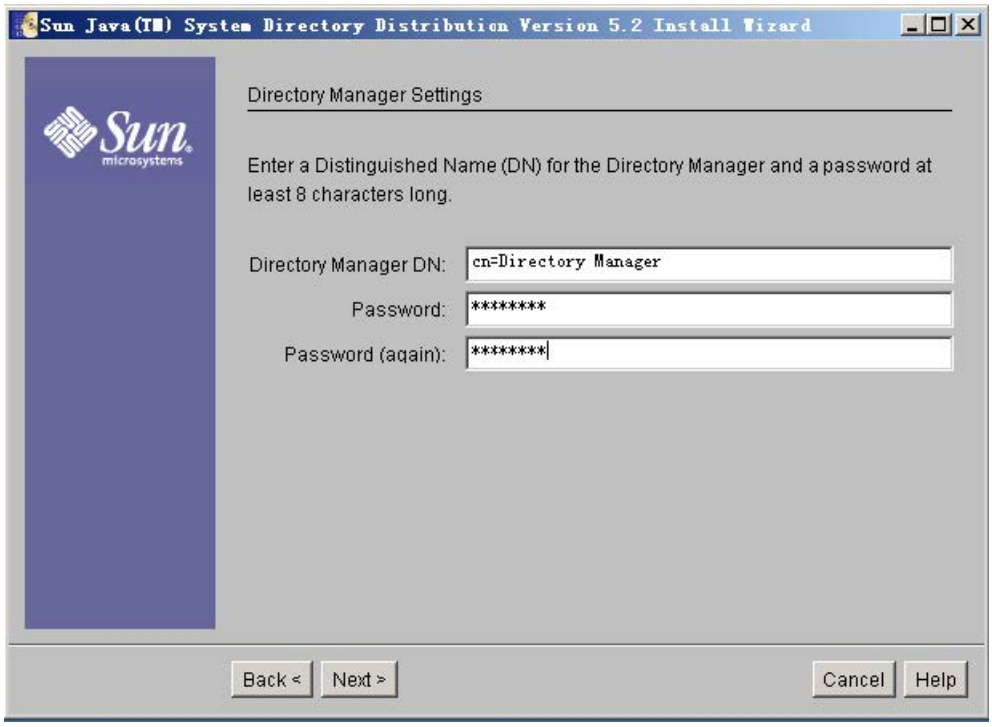
13. Configure the password for the Directory Server Administrator and click **Next**.



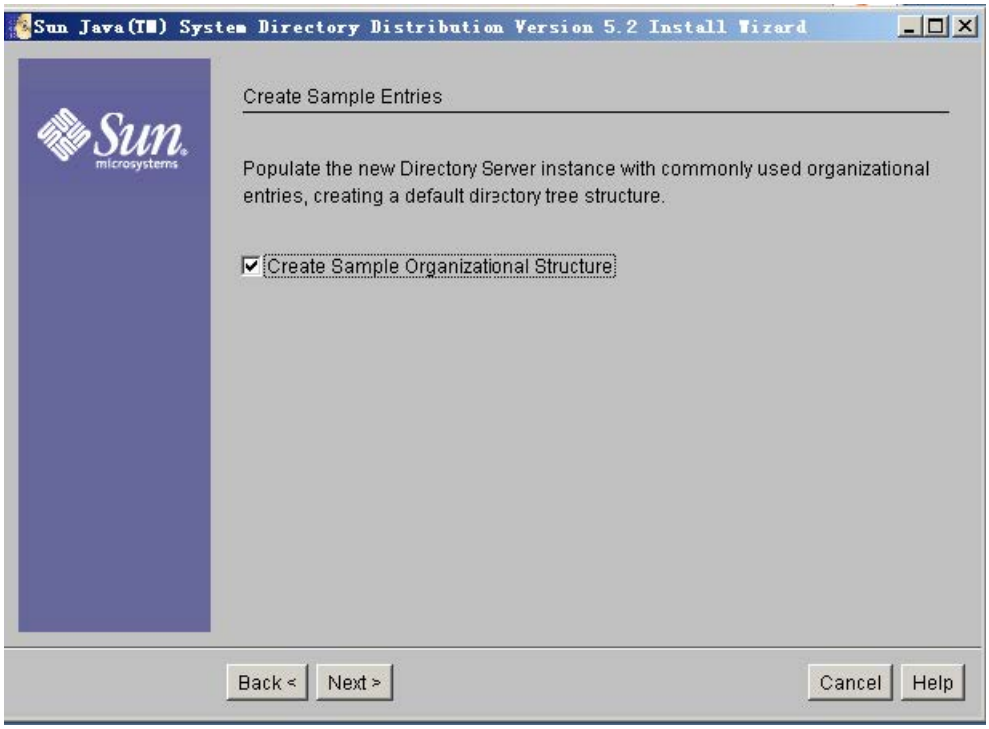
14. Follow the default setting and click **Next**.



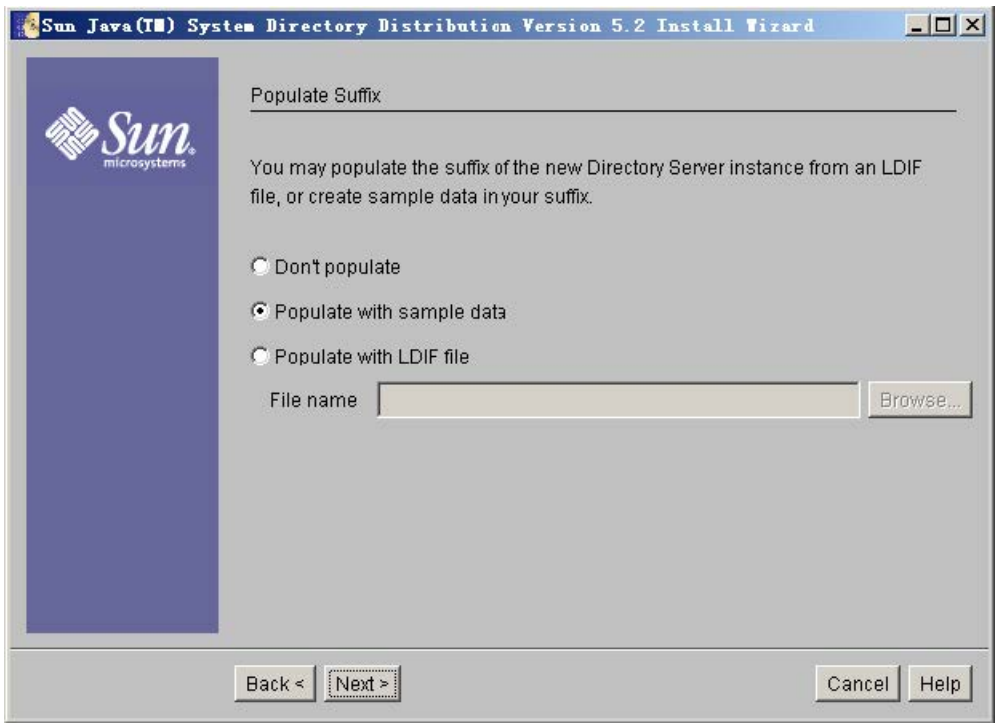
15. Configure the password for the Directory Manager and click **Next**.
    The password must be at least 8 characters long.



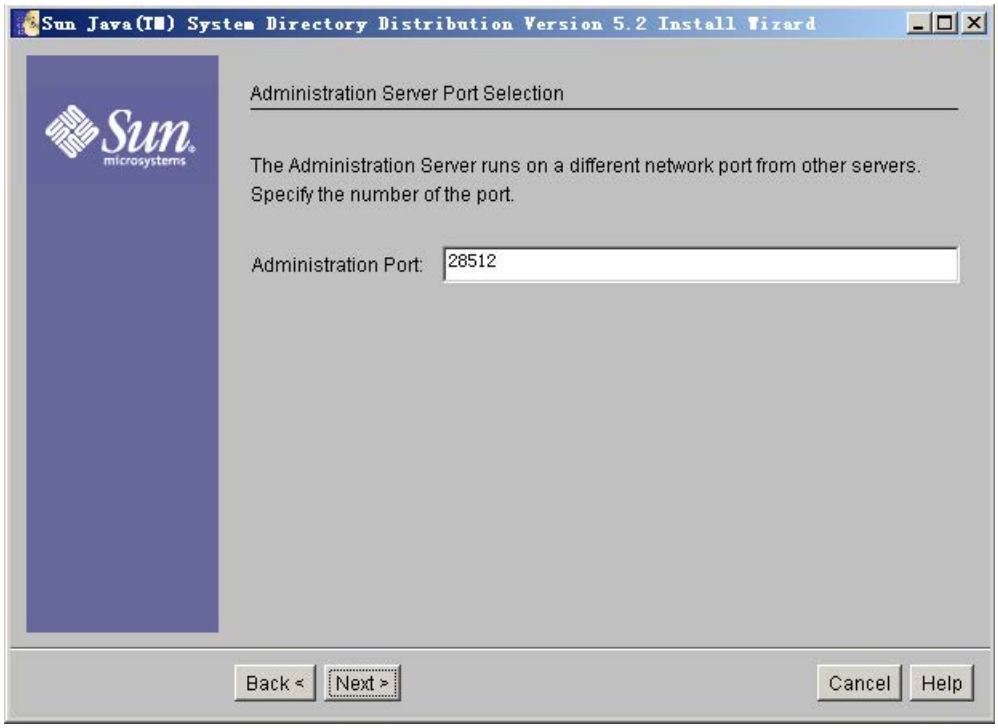
16. Select the **Create Sample Organizational Structure** check box and click **Next**.



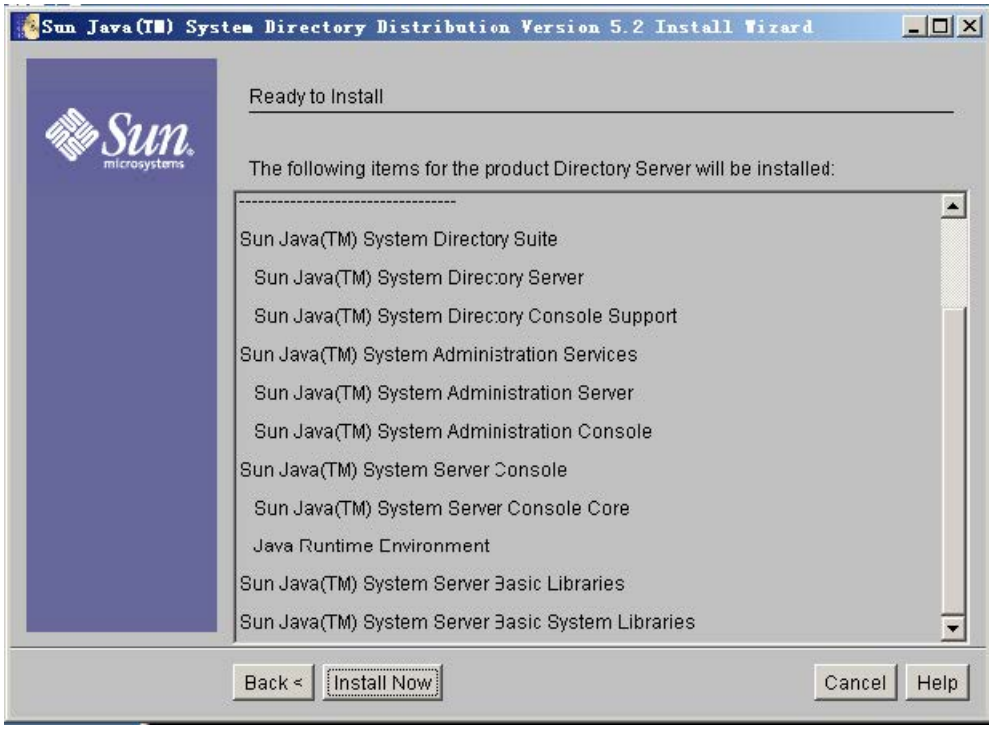
17. Select the **Populate with sample date** check box and click **Next**.



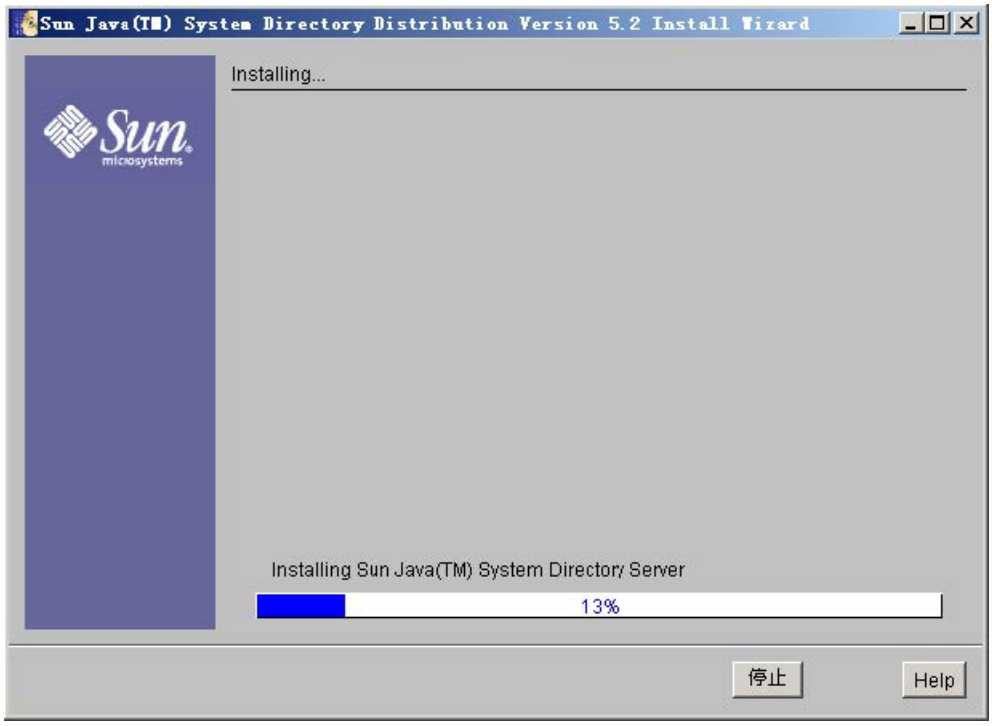
18. Follow the default settings and click **Next** for the following two steps.



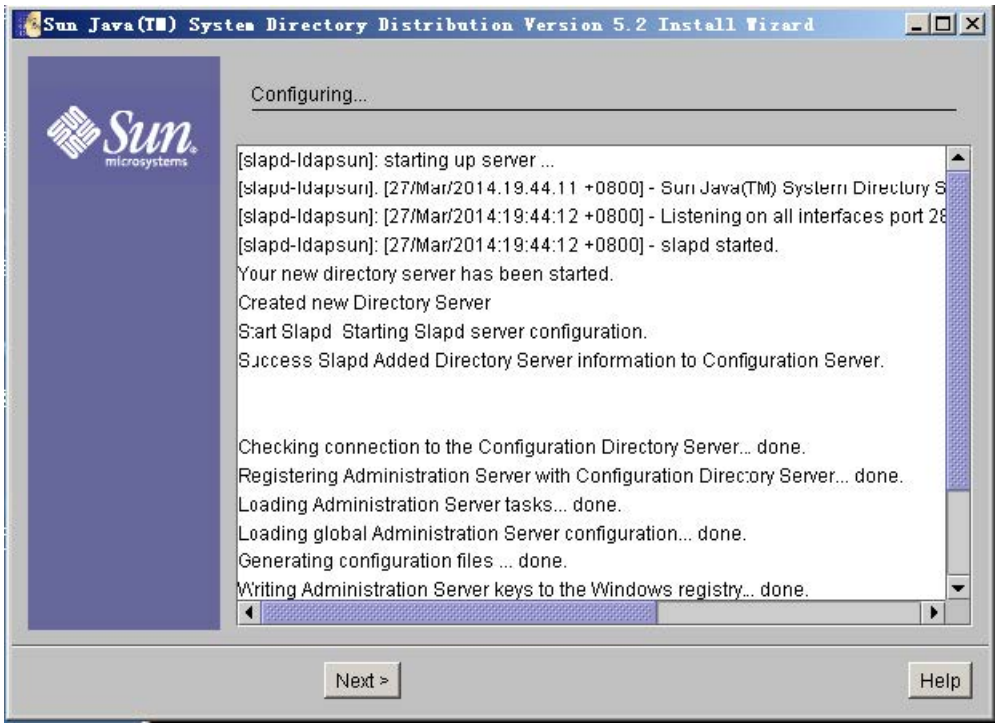
19. View the items to be installed and click **Install Now**.



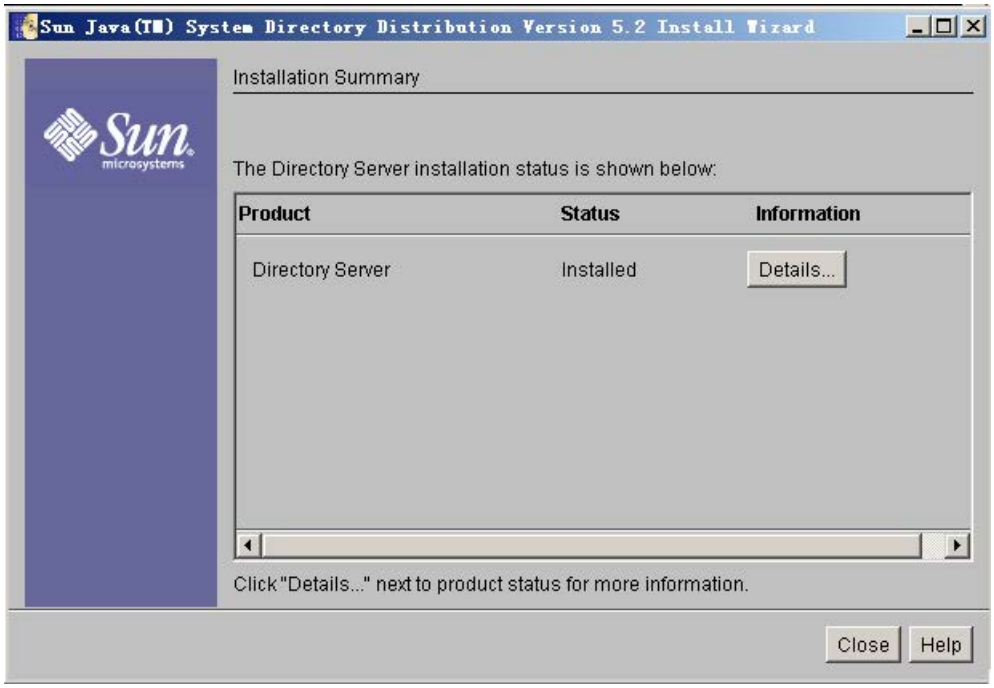
The installing progress is shown as below:



After the installation, it will enter the configuring screen.



20. After the configuration, click **Next** to enter the installation summary screen. You can view the directory server installation status and click **Details** for more information. You can also click **Close** to close the Sun Java™ System Directory Distribution Version 5.2 Install Wizard.



Configure the Sun Java™ System Server Console

Add an Entry to the Directory Server

You can add entries to the Directory Server one by one in this way.

To add an entry to the Directory Server:

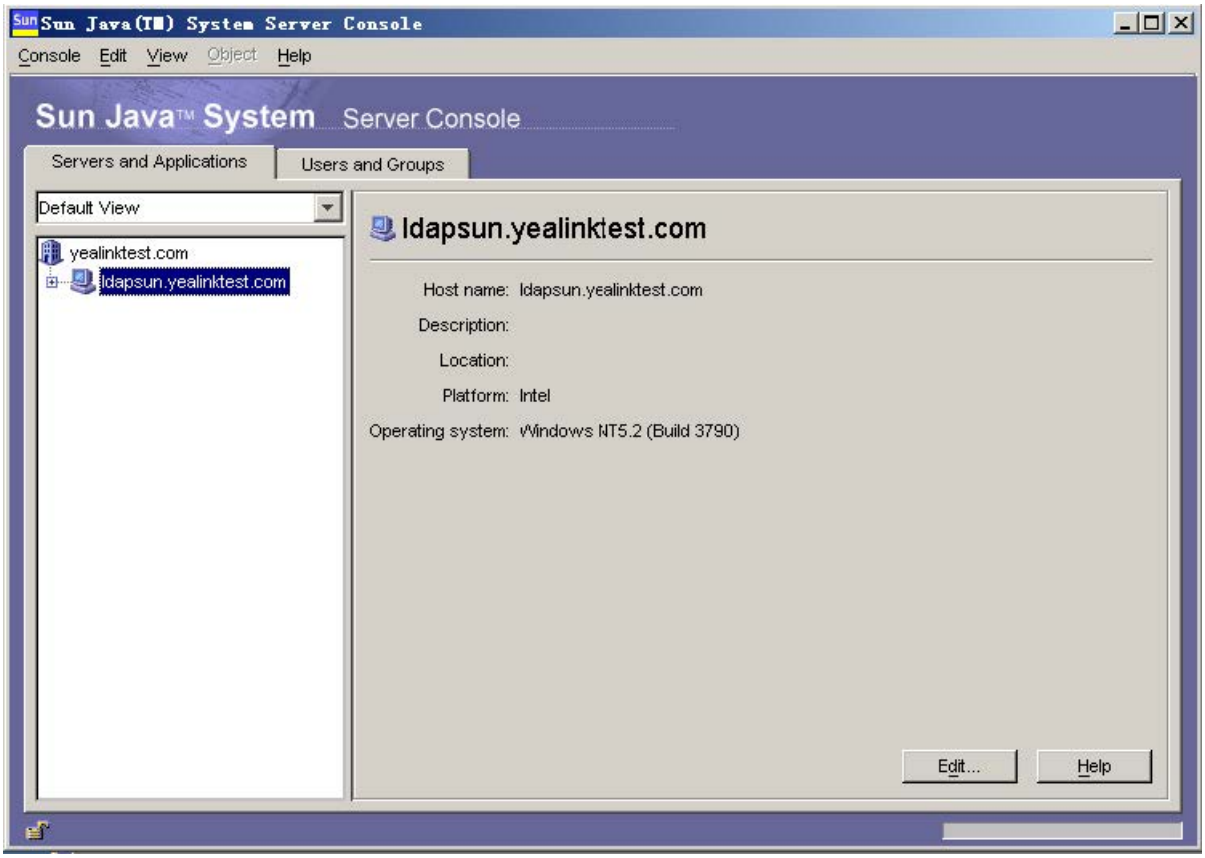
1. Click **Start** > **Program** > **Sun Java™ System Server Products** > **Sun Java™ System Server Console 5.2.**

   It will enter the login screen. You should enter the administrator user name and its password in the **User ID** field and **Password** field respectively.

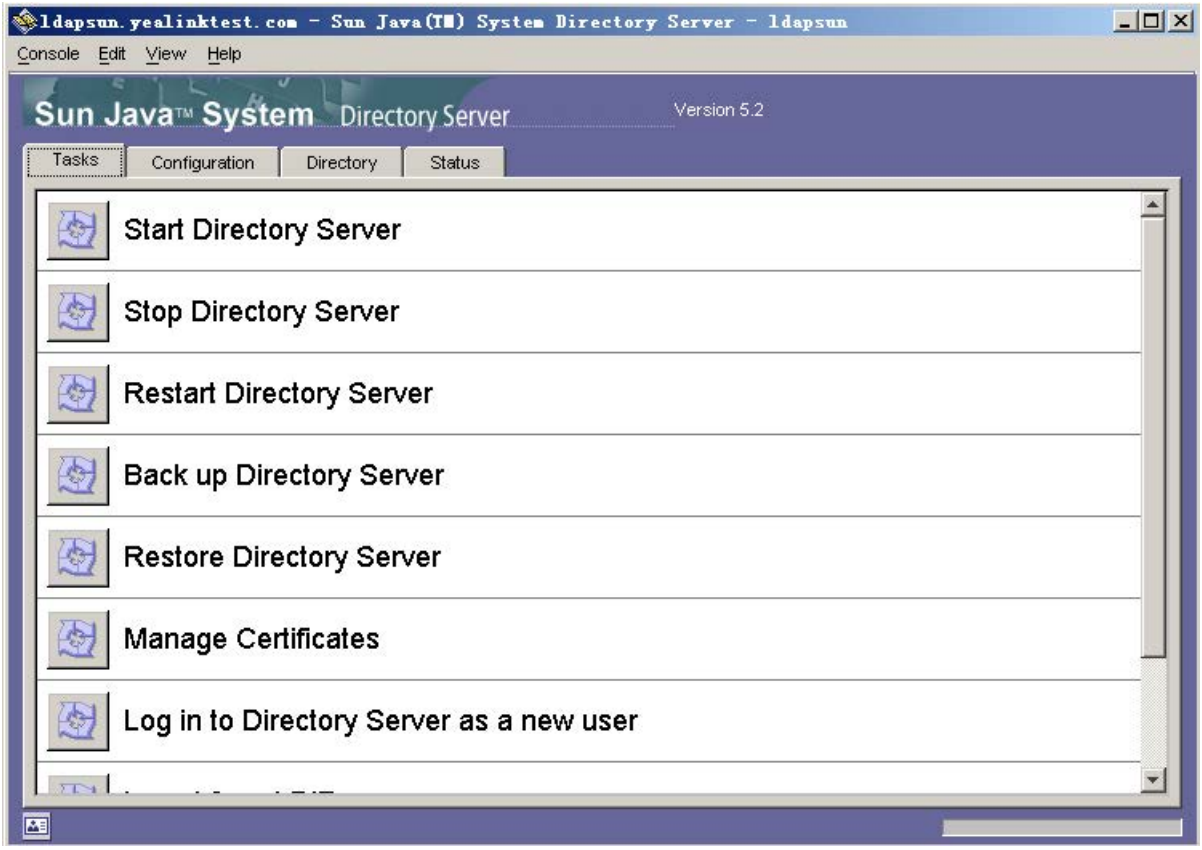
NOTE

The system default administrator is **cn=Directory Manager** and its password which must be at least 8 characters long has already been set during the installation process.

Then click **OK** to enter the home page.

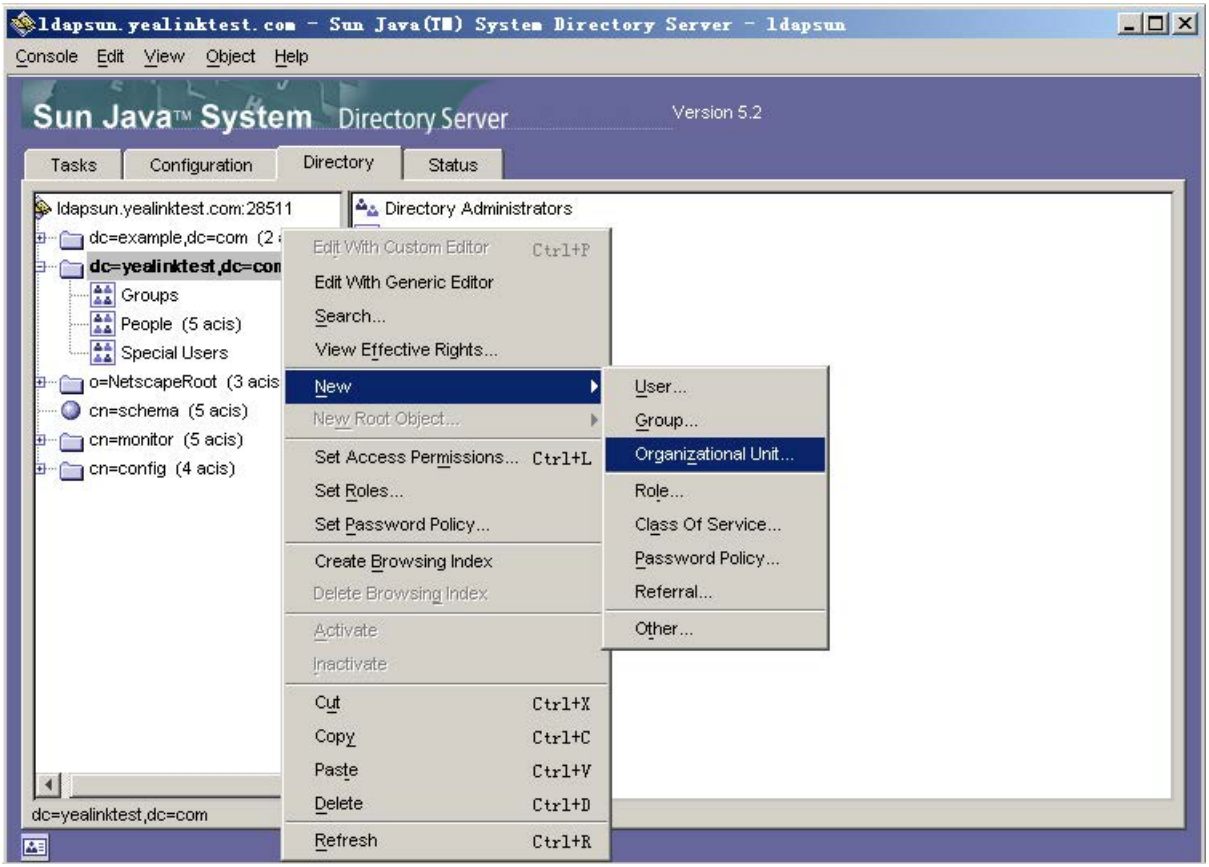


2. Double click **ldapsun.yealinktest.com** > **Server Group** > **Directory Server(ldapsun)**. It will enter the Directory Tasks interface.

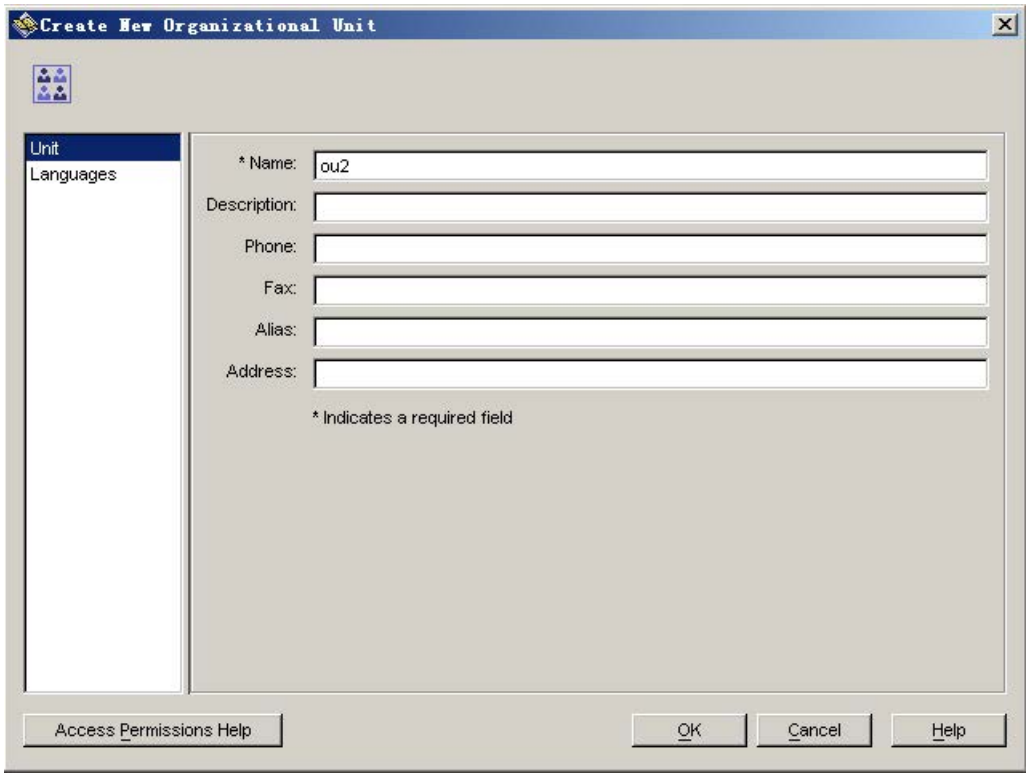


3. Click the **Directory** tab.

4. Select and right click the **dc=yealinktest,dc=com (6 acis)**, and then select **New** > **Organizational Unit**.

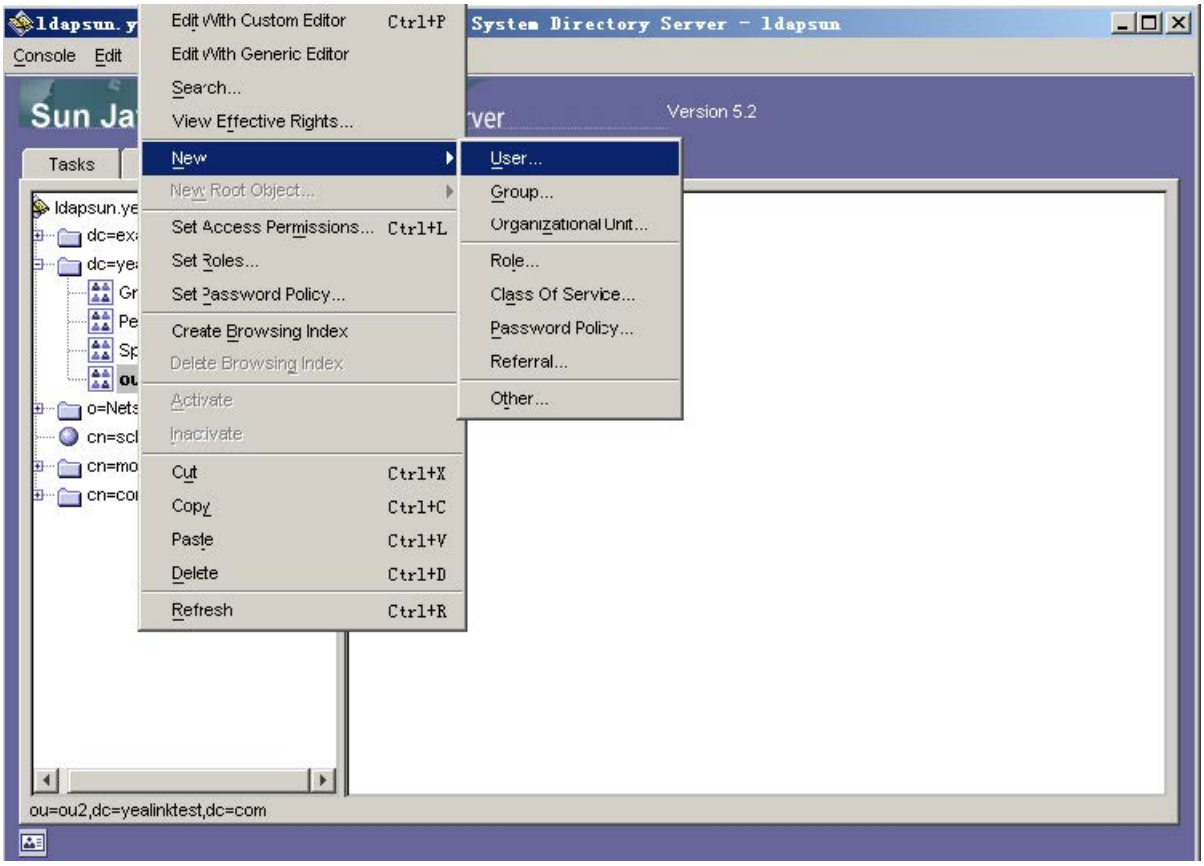


5. Enter the desired name of the organizational unit.

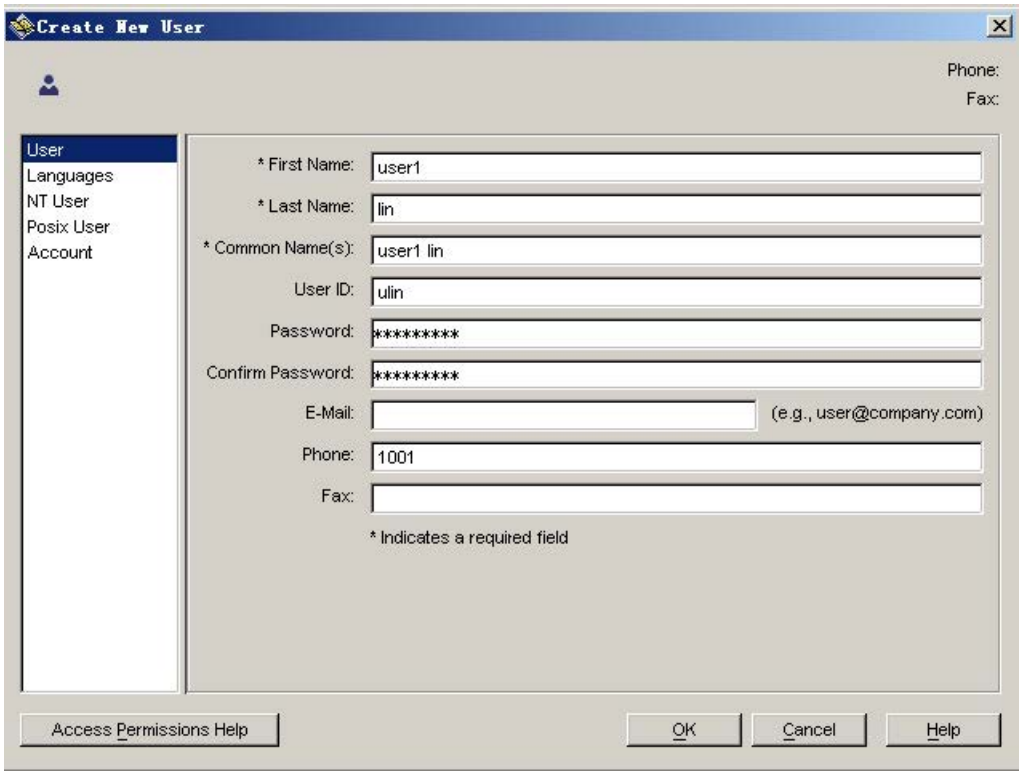


6. Click **OK** to accept the change.

7. Select and right click the organizational unit created above, and then select **New** > **User**.

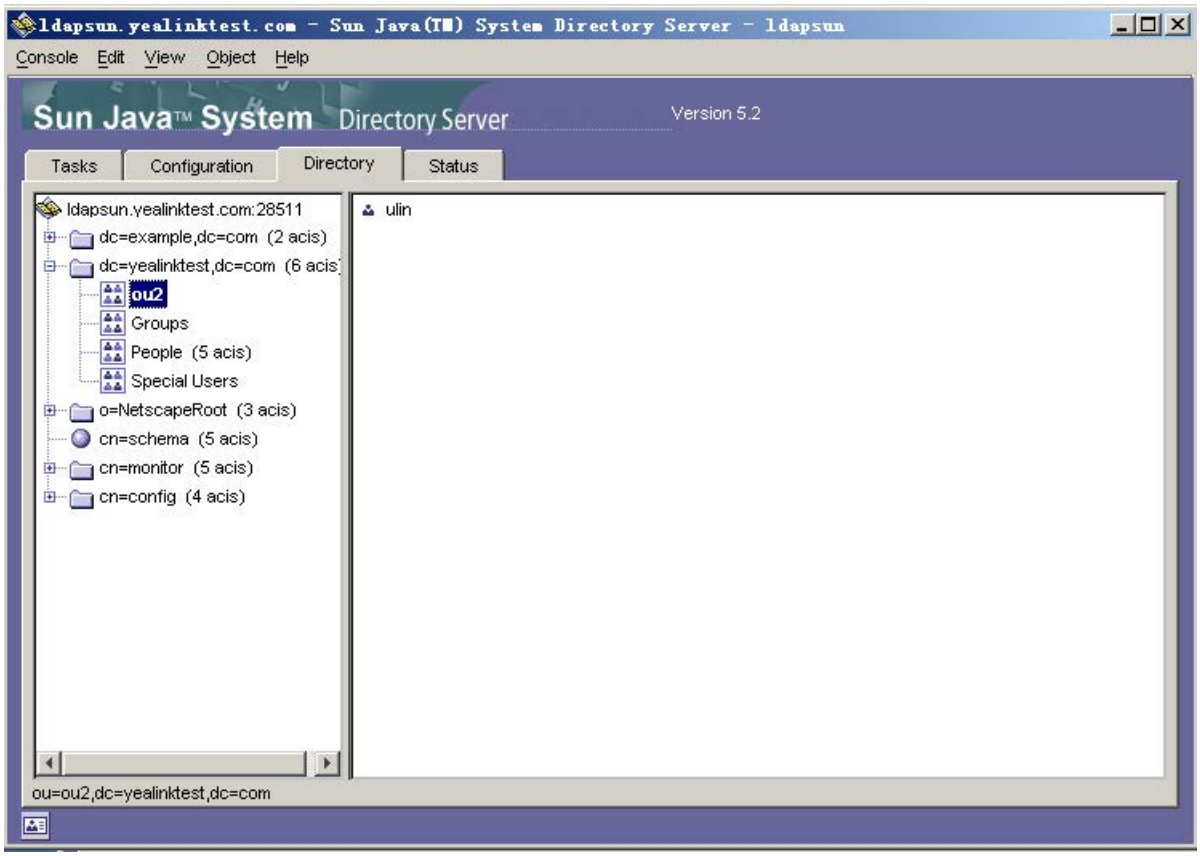


8. Enter the desired values in the corresponding fields.



9. Click **OK** to accept the change.

   You can view the user (User ID is ulin) created above under the organizational unit named ou2.



Add Entries to the Directory Server Using the ldifde Tool

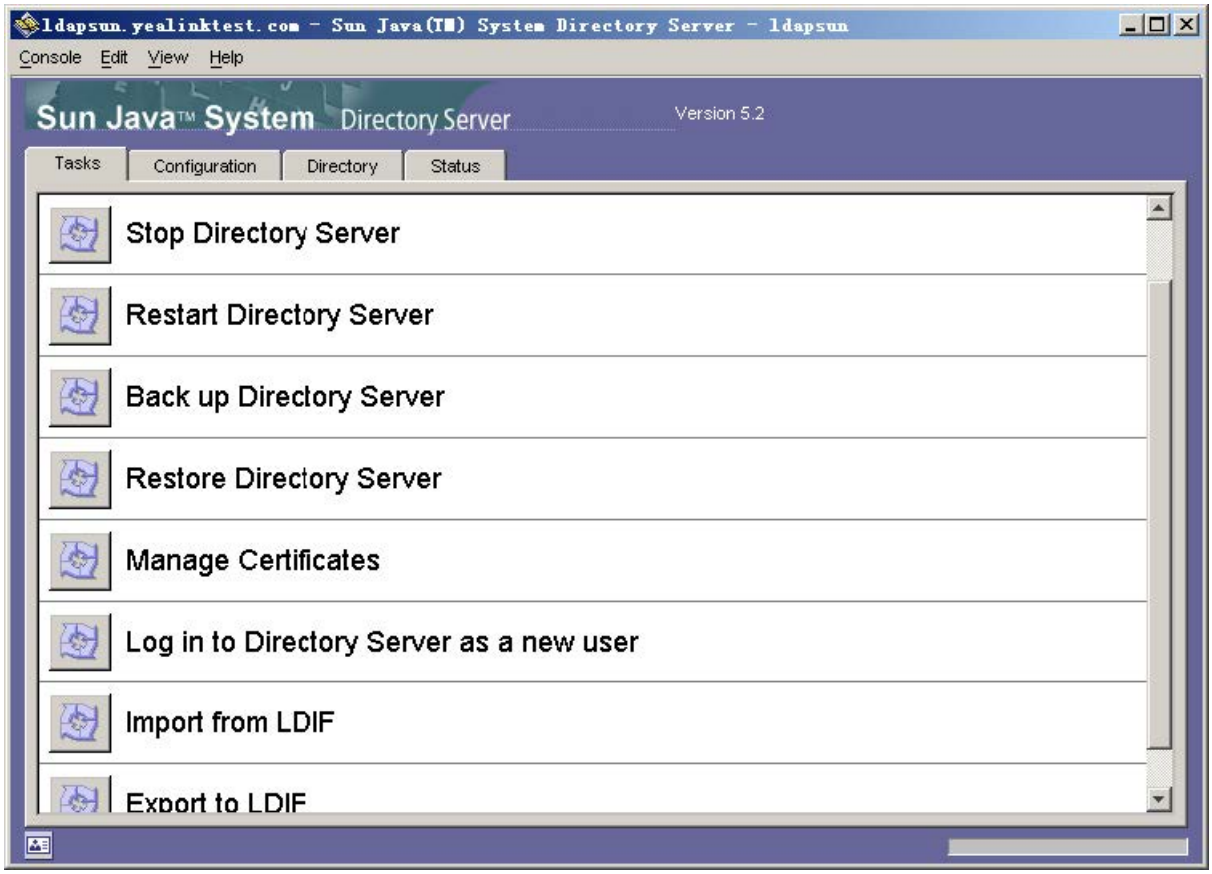
You can use an LDIF file to perform a batch import of all entries to the Directory Server. For more information, refer to create the LDIF file. The following shows an example of the content of the LDIF file for the Directory Server:

```
##Create a new organizational unit##
dn: ou=ou3,dc=yealinktest,dc=com
ou: ou3
objectClass: top
objectClass: organizationalunit
creatorsname: cn=directory manager
modifiersname: cn=directory manager
parentid: 1
entryid: 15
entrydn: ou=ou3,dc=yealinktest,dc=com

##create a new user##
dn: uid=utest,ou=ou3,dc=yealinktest,dc=com
uid: utest
facsimileTelephoneNumber: 11002
givenName: user4
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
sn: test
cn: user4 test
```

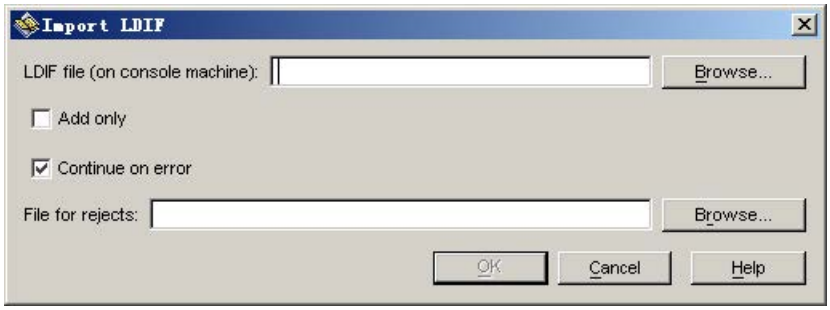
To import the test.ldif file:

1. On the home page of Sun Java™ System Server Console, double click **ldapsun.yealinktest.com** > **Server Group** > **Directory Server(ldapsun)**.

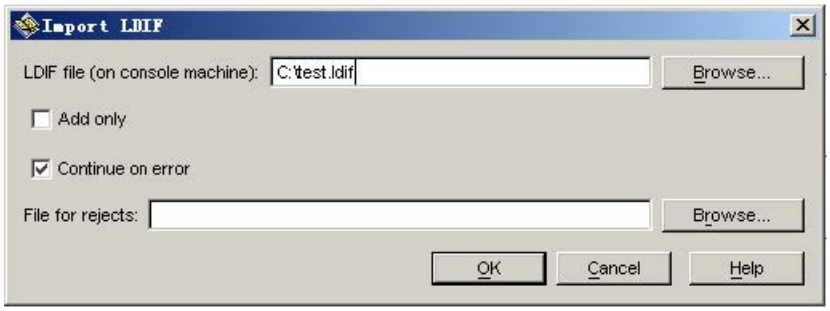
It will enter the Directory **Tasks** interface.



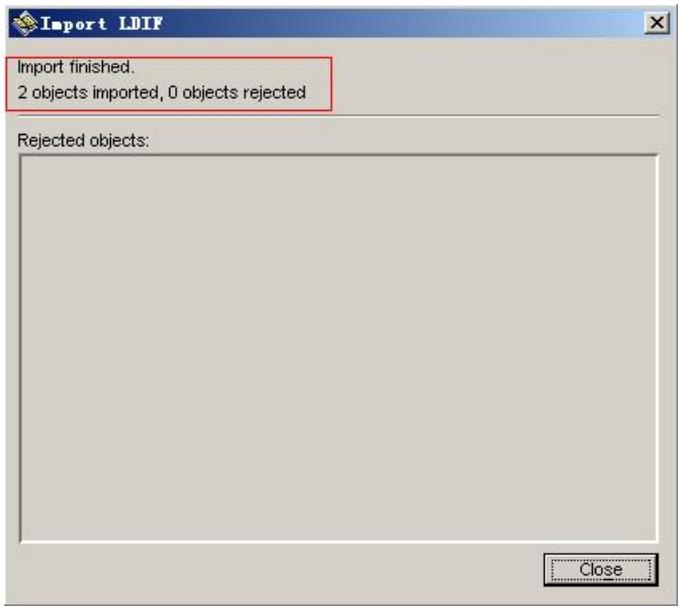
2. Click **Import from LDIF**.



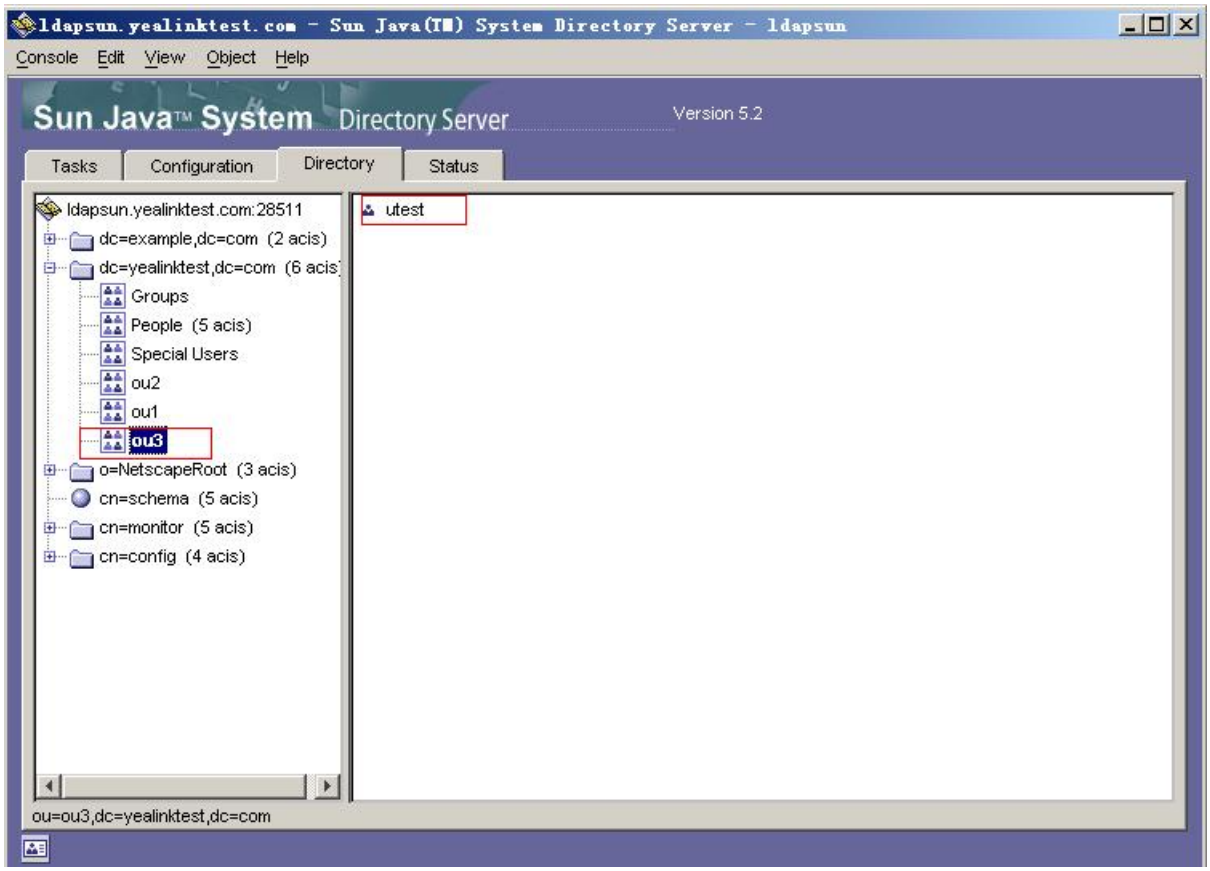
3. Click **Browse** to locate the test.ldif file from your local system, and then click **OK**.



After importing the test.ldif file, it will show the status of importing. If the entries are added successfully, you can view the information "n objects imported, 0 objects rejected". You can click **Close** to close it.



You can view the imported the organizational unit (e.g., ou3) and user (e.g., uid=utest) under the path: **Directory** > **dc=yealinktest,dc=com (6 acis)**.



Remote Phone Book

Introduction

The remote phone book is a centrally maintained phone book, stored on the remote server. Users only need the access URL of the remote phone book. The phone can establish a connection with the remote server download the phone book, and then display the remote phone book entries on the phone.
Yealink phones support up to 5 remote phone books. The remote phone book is customizable.

ⓘ NOTE
We recommend that you download less than 5000 remote contacts from the remote server.

Remote Phone Book File Customization

Yealink phones support remote phone book contact customization.
You can add multiple contacts at a time and/or share contacts between the phones using the supplied template files (Menu.xml and Department.xml).
You can ask the distributor or Yealink FAE for a remote phone book template. You can also refer to the following template:

```
<YealinkIPPhoneDirectory>
<DirectoryEntry><Name>Tom</Name><Telephone>66000</Telephone></DirectoryEntry>
<DirectoryEntry><Name>Jensen</Name><Telephone>29000</Telephone><Telephone>42</Telephone></DirectoryEntry>
<DirectoryEntry><Name>Phil</Name><Telephone>49880</Telephone></DirectoryEntry>
<DirectoryEntry><Name>Boss</Name><Telephone>10.10.32.147</Telephone></DirectoryEntry>
</YealinkIPPhoneDirectory>
```

Remote Phone Book File Elements

Yealink phones support two template files: Menu.xml and Department.xml.
The Menu.xml file defines the group/department of a remote phone book. The Department.xml file defines contact lists for a department/group, which is nested in Menu.xml file.
The following table lists the elements you can use to add groups or contacts in the remote phone book file. We recommend that you do not edit these elements.

Template	Element	Valid Values
Department.xml	`<DirectoryEntry ><Name > Contact Name</Name ><Telephone > Contact Number</Telephone ><DirectoryEntry >`	Add a contact in a department/group: Specify the contact name between `<Name >` and `</Name >` ; Specify the contact number between `<Telephone >` and `</Telephone>` .
Menu.xml	`<MenuItem><Name>Department</Name><URL>Department URI</URL></MenuItem>`	Add a contact department/group file: Specify the department/group name between `<Name>` and `</Name>` ; Specify the department/group access URL between `<URL>` and `</URL>` .

Menu.xml	<SoftKeyItem> <Name>#</Name> <URL>http://10.2.9.1:99/Department.xml</URL> </SoftKeyItem>	Specify a department/group file for a key: Specify *key, # key or digit key between <Name> and </Name>; Specify the department/group access URL between <URL> and </URL>.

Customize Remote Phone Book File

1. Add contacts in a Department.xml file. Each starts on a new line.

   For example,

   ```
   <DirectoryEntry>
       <Name>Lily</Name>
       <Telephone>123456</Telephone>
   </DirectoryEntry>
   <DirectoryEntry>
       <Name>Jim</Name>
       <Telephone>654321</Telephone>
   </DirectoryEntry>
   ```

2. You can create multiple department.xml files, rename these files and specify multiple contacts in these files. For example, Market.xml with contact Lily and Jim, Propaganda.xml with other contacts and so on.

3. Save these files and place them on the provisioning server.

4. Copy the department files URLs and specify them in the Menu.xml file.

   For example,

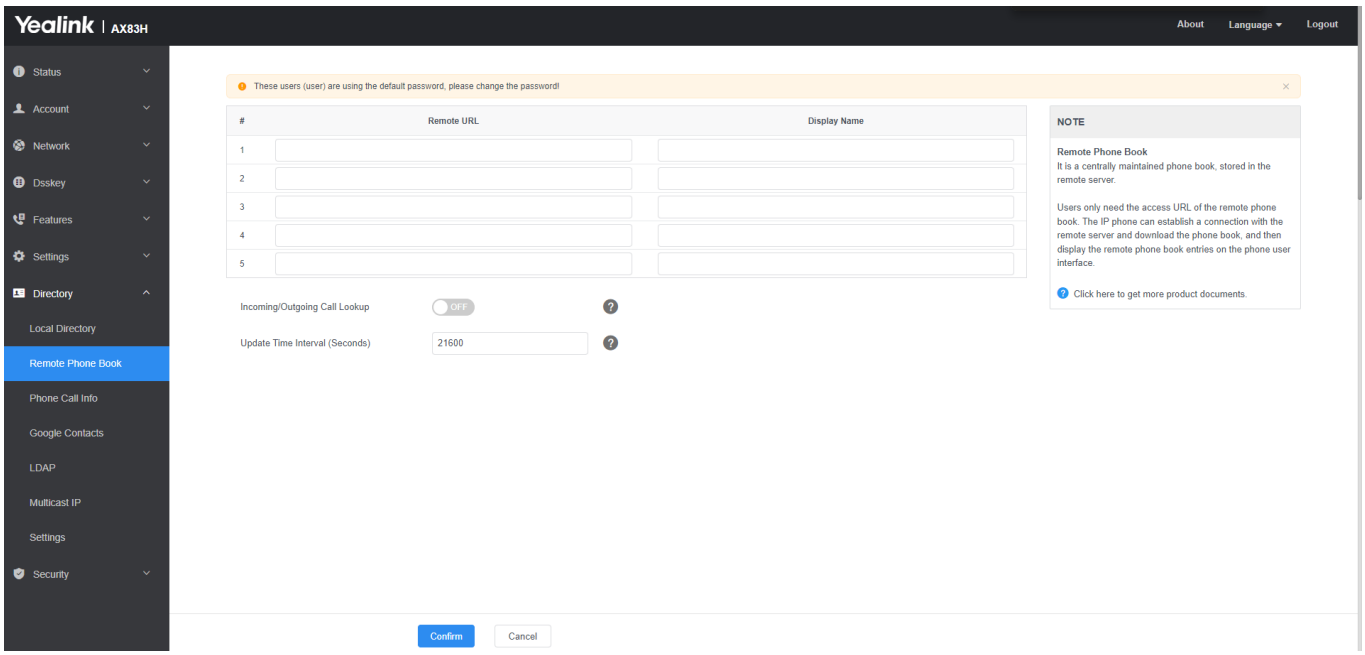
   ```
   <MenuItem>
      <Name > Market</Name>
      <URL > http://192.168.0.1:99/Market.xml</URL>
   </MenuItem>
   <SoftKeyItem>
      <Name>1</Name>
      <URL>http://192.168.0.1:99/Propaganda.xml</URL>
   </SoftKeyItem>
   ```

5. Save Menu.xml file and place it to the provisioning server.

Remote Phone Book Configuration

Set via the Web User Interface

1. On the web user interface, go to **Directory** > **Remote Phone Book**.



Configuration Parameter

remote_phonebook.data.X.url
remote_phonebook.data.X.name
remote_phonebook.data.X.username
remote_phonebook.data.X.password
remote_phonebook.display_name
features.remote_phonebook.enable
features.remote_phonebook.flash_time
remote_phonebook.assignment.enable
handset.X.remote_phonebook_access

Parameter	Permitted Values	Default	Description
remote_phonebook.data.X.url[1]	URL within 511 characters	Blank	It configures the access URL of the remote phone book. **ⓘ NOTE** The size of a remote phone book file should be less than 1.5 M.
remote_phonebook.data.X.name[1]	String within 99 characters	Blank	It configures the display name of the remote phone book item.
remote_phonebook.data.X.username[1]	String	Blank	It configures the user name used to access the remote phone book X.
remote_phonebook.data.X.password[1]	String	Blank	It configures the password used to access the remote phone book X.

remote_phonebook.display_name	String within 99 characters	Blank	It configures the display name of the remote phone book. If it is left blank, "Remote Phone Book" will be the display name.
features.remote_phonebook.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to perform a remote phone book search for an incoming or outgoing call and display the matched results on the phone screen.
features.remote_phonebook.flash_time	0, Integer from 3600 to 1296000	21600	It configures how often to refresh the local cache of the remote phone book. If it is set to 3600, the phone will refresh the local cache of the remote phone book every 3600 seconds (1 hour). If it is set to 0, the phone will not refresh the local cache of the remote phone book.
remote_phonebook.assignment.enable	**0**-Disabled **1**-Enabled	0	It configures whether the remote phone book can be allocated.
handset.X.remote_phonebook_access[2]	Integer from 1 to 10	X	It sets the remote phonebook that handset can access. Multiple values are separated by commas. **ⓘ NOTE** It works only if `remote_phonebook.assignment.enable` is set to 1.

[1] X is the phone book ID.
[2]X is the handset ID. X=1-10.

Example: Configure a Remote Phone Book

The following example shows the configuration for the remote phone book.
Customize the “Department.xml “and “Menu.xml “ files, and then place these files to the provisioning server “http://192.168.10.25”.

Example

```
remote_phonebook.data.1.url = http://192.168.10.25/Menu.xml
remote_phonebook.data.1.name = Yealink
remote_phonebook.data.2.url = http://192.168.10.25/Market.xml
remote_phonebook.data.2.name = Market
```

Errors and Solutions

Error	Description	Solution
0x00090000 01060000 Remote dir download fail	Remote Phone Book downloading failure.	1. Refer to the corresponding error code to find out the solution. 2. If the above method does not solve the problem, please provide the diagnostic file in the working scenario for comparison so that Yealink FAE could do further analysis.
0x00090000 01060001 Download file format error	XML file format error.	Change the XML file format to the correct one. For more information, see https://www.cnblogs.com/codingmengmeng/p/7245625.html.
0x00090000 01060002 Download limit exceeded	Phone performance limits. The contact files you download exceed the maximum limit.	Generally, the color screen phones allow file downloading up to 1.5 M. However, the phones with black and white LCD display allow file downloading up to 768KB. Therefore, you need to control the size of the file to be downloaded, for example, the resource file uploaded by users.
0x00090000 01060003 Auth Error	Phone configuration error. XML file authentication failed.	1. Choose one of the following methods to configure the correct authentication information for the phone: - Set the user name and password: `remote_phonebook.data.x.username=` and `remote_phonebook.data.x.password=` - Bring the authentication information in the URL. For example, http://user:password@IP/RemotePhonebook.xml 2. If the above method does not solve the problem, please provide the diagnostic file in the working scenario for comparison so that Yealink FAE could do further analysis.
0x00090000 01060004 network unavailable	Network error, causing downloading failure.	Check whether the network between the phone and the server is available by using the phone Ping feature.
0x00090000 01060005 load remote dir error	Phone error. The phone has problems when loading the contacts.	Yealink FAE will also do further analysis to give you a solution ASAP.

XML Phonebook Configuration

Introduction

You can get contacts by searching an XML phonebook in real time.
For more information about XML Browser, please refer to XML Browser .

XML Phonebook Configuration

Configuration Parameter

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

```
xml_phonebook.data.X.url
xml_phonebook.data.X.name
xml_phonebook.data.X.username
xml_phonebook.data.X.password
xml_phonebook.data.max_hits
```

Parameter	Permitted Values	Default	Description
xml_phonebook.data.X.url[1]	String within 512 characters	Blank	It configures the requested URL of the XML phonebook. **NOTE** The contacts in the XML phonebook are all in the first level, and any nesting is not allowed.
xml_phonebook.data.X.name[1]	String within 64 characters	Blank	It configures the name of the XML phonebook to be displayed on the handset. If it is left blank, XML Dir x is displayed.
xml_phonebook.data.X.username[1]	String within 64 characters	Blank	It configures the authentication user name to request the XML phonebook.
xml_phonebook.data.X.password[1]	String within 64 characters	Blank	It configures the authentication password to request the XML phonebook.
xml_phonebook.data.max_hits	Integer from 1 to 800	50	It configures the maximum number of contacts returned by the server when you perform an XML phonebook search. **NOTE** Contacts with multiple numbers are counted as only one contact.

[1]X is the XML phonebook ID. X=1-10.

Directory Search Settings

Introduction

You can configure how the phones search contacts.

Directory Search Settings Configuration

Configuration Parameter

```
directory.search_type
directory.containing_search.additional_sorting_mode
```

Parameter	Permitted Values	Default	Description
directory.search_type	**0**-Approximate string matching, the phone will search the contact numbers or names containing the entered character(s). **1**-Prefix matching, the phone will search the contact numbers or names starting with the entered character(s).	0	It configures the search type when searching the contact in the Local Directory, Remote Phone Book, Network, Directory or Blocklist.
directory.containing_search.additional_sorting_mode	**0**-Sort by ASCII code order. **1**-The contacts starting with the searched content are displayed first, and the remaining contacts are displayed in the ASCII code order.	0	It configures the sorting mode in the search results. **NOTE** It works only if `directory.search_type` is set to 0 (Approximate string matching).

Number Matching Settings

Introduction

You can configure the pattern to match the contact numbers with the caller's phone number. The numbers stored in your phone's contact memory do not include country or area codes, such as 7812967549, while the incoming call number carries the country code +17812967549. In this case, the contact name cannot be matched. Therefore, you

need to use regular expression matching to associate the incoming call number with the contact information.

Number Matching Settings Configuration

Configuration Parameter

```
phone_setting.reverse_lookup.contact_list.replace.pattern
phone_setting.reverse_lookup.contact_list.replace.with
phone_setting.reverse_lookup.incoming_call.replace.pattern
phone_setting.reverse_lookup.incoming_call.replace.with
phone_setting.call_number_display.replace.pattern
phone_setting.call_number_display.replace.with
```

Parameter	Permitted Values	Default	Description
phone_setting.reverse_lookup.contact_list.replace.pattern	Regular Expression	Blank	It configures the matching pattern used to identify the replaced string of the contact number.
phone_setting.reverse_lookup.contact_list.replace.with	String within 512 characters	Blank	It configures the string used to replace the certain matched one of the contact numbers.
phone_setting.reverse_lookup.incoming_call.replace.pattern	Regular Expression	Blank	It configures the matching pattern used to identify the replaced string of the caller's phone number.
phone_setting.reverse_lookup.incoming_call.replace.with	String within 512 characters	Blank	It configures the string used to replace the certain matched one of the caller's phone numbers.
phone_setting.call_number_display.replace.pattern	Regular Expression	Blank	It configures the matching pattern used to identify the replaced string of the caller's phone display number.
phone_setting.call_number_display.replace.with	String within 512 characters	Blank	It configures the string used to replace the certain matched one of the caller's phone display numbers.

Example: Configure Number Matching Settings

For example, in your region, the area code is +123, and the incoming call number is +123987654. On your phone, you have a contact named "Test" with the number 0987654. If you want the incoming call number to be correctly matched and display the correct contact name, you need to configure the following:

Method One:

```
phone_setting.reverse_lookup.incoming_call.replace.pattern = ^\+123
phone_setting.reverse_lookup.incoming_call.replace.with = 0
```

The meaning is to replace the "+123" in the incoming call number with "0". By doing so, the incoming call number will match exactly with "0987654", allowing the correct contact name to be displayed.

Method Two:

You can also choose to match the stored contact information instead of modifying the incoming call number. Here's how:

```
phone_setting.reverse_lookup.contact_list.replace.pattern = ^0
phone_setting.reverse_lookup.contact_list.replace.with = \+123
```

It means replacing the "0" in the contact number 0987654 with "+123" can also achieve a complete match with the incoming call number, thereby displaying the correct contact information.

Method Three:

You can also choose to manipulate both the local contact number and the incoming call number simultaneously.

```
phone_setting.reverse_lookup.contact_list.replace.pattern = ^0
phone_setting.reverse_lookup.incoming_call.replace.pattern = ^\+123
```

This means removing the "+123" from the incoming call number "+123987654" and removing the "0" from the local contact number "0987654" to achieve a complete match using "987654," thereby displaying the correct contact information.

ⓘ NOTE

The above methods are just simple examples, please choose the appropriate method based on your specific situation.

Call Log

Introduction

Yealink phones record and maintain phone events to a call log, also known as a call list.
Call log consists of four lists: Missed Calls, Placed Calls, Received Calls, and All Calls.
Each call log list supports up to 100 entries.

Call Log Display

The following table describes the detailed call log information:
When there is only one menu under the "History" directory, clicking on "History" will directly enter that menu.
For example, if you have enabled only the "Local Call Log" menu, clicking on "History" will directly enter the "Local Call Log" without displaying the "Call Log" directory.

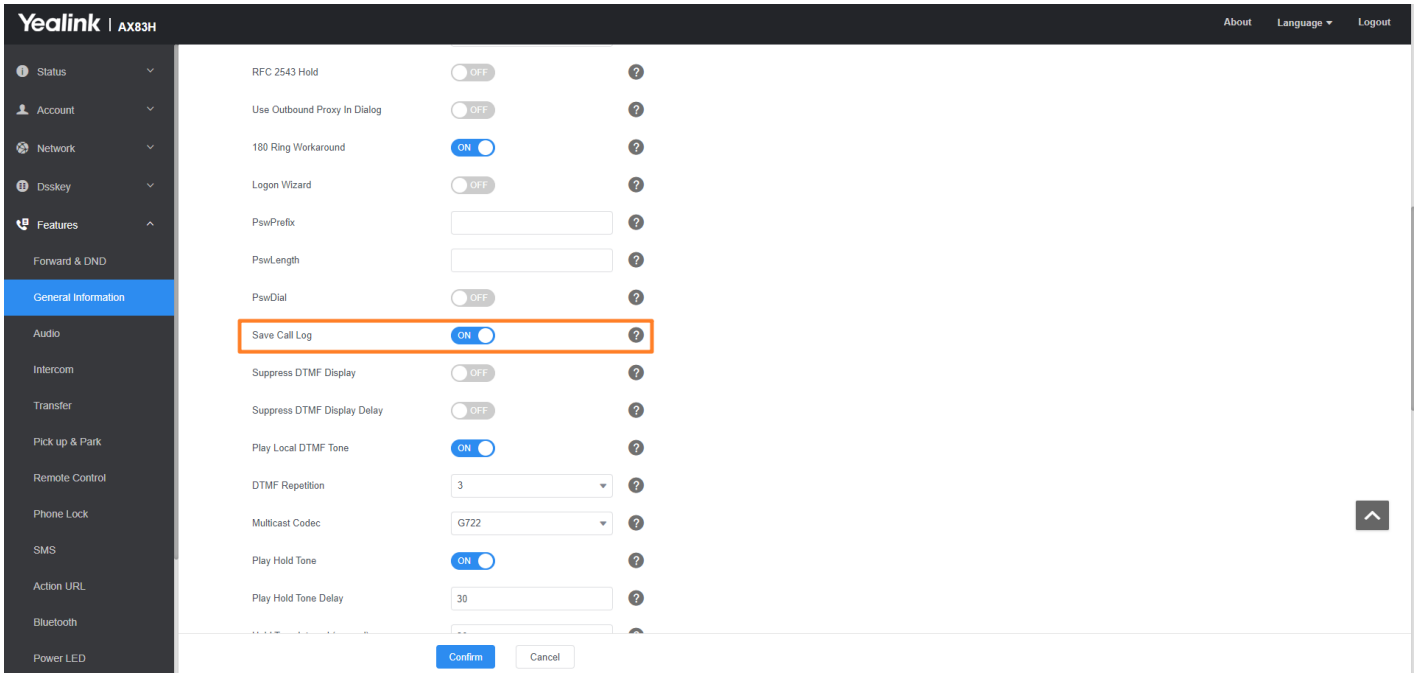
Display Field	Description

Name	Shows the name of the remote party.
Number	Shows the number of the remote party.
Time	Shows the call initiation time.
Duration	Shows the duration of the call.
Relation	Shows what happened to the call. The valid display contents are: · **Rejected**: Reject an incoming call. · **Forward to X**: Forward an incoming call to X. For example, Forward to 1048 means you forward an incoming call to 1048. · **Busy**: The outgoing call is rejected. · **Transfer to X**: Transfer a call to X. For example, **Transfer to 1048** means you transfer a call to 1048. · **X**: Answer a transferred/forwarded call from remote party X; your call is transferred/forwarded to X. For example, **1048** means you answer a transferred/forwarded call from remote party 1048. It is configurable by `features.calllog_detailed_information`.

Call Log Configuration

Set via the Web User Interface

On the web user interface, go to **Features** > **General Information** > **Save Call Log**.



Configuration Parameter

features.save_call_history
account.X.missed_calllog
pstn.account.X.missed_calllog
features.call_log_show_num
features.calllog_detailed_information
features.save_init_num_to_history.enable
features.call_out_history_by_off_hook.enable
features.call_log_merge.enable
features.local_calllog.received.replace_rule

Parameter	Description	Permitted Values	Default
features.save_call_history	It enables or disables the phone to log the call history (missed calls, placed calls, received calls and forwarded calls) in the call lists. **NOTE** To log the missed calls, "account.X.missed_calllog" should be set to 1 (Enabled).	0-Disabled, the phone cannot log the placed calls, received calls, missed calls and the forwarded calls in the call lists. 1-Enabled	1
account.X.missed_calllog[1]	It enables or disables the phone to record missed calls for account X. **NOTE** It works only if "features.save_call_history" is set to 1 (Enabled).	0-Disabled 1-Enabled	1
pstn.account.X.missed_calllog[2]	It enables or disables the phone to indicate and record missed calls for PSTN account X. **NOTE** It works only if "features.save_call_history" is set to 1 (Enabled). The prompt message displays only if "features.missed_call_popup.enable" is set to 1 (Enabled).	0-Disabled, the phone does not display a prompt message and an indicator icon on the idle screen and log the missed call in the Missed Calls list when it misses calls. 1-Enabled, the phone displays a prompt message and an indicator icon on the idle screen and logs the missed call in the Missed Calls list when it misses calls.	1

features.call_log_show_num	It configures the display type of the other parties' information in the call log lists. **NOTE** It works only if "features.save_call_history" is set to 1 (Enabled).	0-Name, the name is displayed preferentially; if there is no name, the number is displayed 1-Number 2-Name & Number, the name and number are displayed; if there is no name, the number is displayed	0
features.calllog_detailed_information	It enables or disables the phone to indicate what happened to the call in the call log lists. It is applicable to the following scenarios: Reject an incoming call Forward an incoming call The outgoing call is rejected Transfer a call Answer a transferred/forwarded call from the remote party; your call is transferred/forwarded to another party. **NOTE** It works only if "features.save_call_history" is set to 1 (Enabled).	0-Disabled 1-Enabled, you can get the detailed call-disposition information . at the path via the phone user interface: History > Option > Detail > Relation.	1
features.save_init_num_to_history.enable	It enables or disables the phone to log the transfer party's phone number in the call history list.	0-Disabled, the phone will log the transfer-to party's phone number in the call history list. 1-Enabled	1
features.call_out_history_by_off_hook.enable	It enables or disables the phone to dial out automatically once you go off-hook or press the Speakerphone key in the call history list.	0-Disabled 1-Enabled	0

features.call_log_merge.enable	It enables or disables the phone to merge the same history records. **NOTE** The merged entry only displays the initiation time of the last call.	0-Disabled, each call is logged individually in the calls list. 1-Enabled, consecutive incomplete calls to/from the same party and in the same direction are merged into one record in the calls list. The merged entry displays the number of consecutive calls.	0
features.local_calllog.received.replace_rule	It configures the string of the digit map to be applied to the numbers dialed from the call history list. Example: features.local_calllog.received.replace_rule = <00:+>x.|<5:1>xx When you call the contact 001234567 from the call history list, the number +1234567 will be dialed out because "001234567" matches the "<00:+>x." in the digit map; When you call the contact 532 from the call history list, the number 132 will be dialed out because "532" matches the "<5:1>xx" in the digit map. **NOTE** The records in the Placed Calls are not matched.	String	Blank

[1]X is the account ID.

Call Logs Backup

Yealink phones support storing all call logs to a call log file named `<MAC>-calllog.xml`. You can back up this file to the server, avoiding data loss. Once the call logs update, the phone will automatically upload this file to the provisioning server or a specific server. If a call log file exists on the server, it will be overridden. The phone will request to download the `<MAC>-calllog.xml` file according to its MAC address from the server during auto provisioning.

The call log file is named after the MAC address of the phone. For example, if the MAC address of an phone is 00156574B150, the name of the call log file is 00156574B150-calllog.xml (uppercase).

TIP

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

The following table lists the parameters you can use to back up the call log.

Configuration Parameter

```
static.auto_provision.local_calllog.backup.enable
static.auto_provision.local_calllog.backup.path
static.auto_provision.local_calllog.write_delay.terminated
static.auto_provision.custom.upload_method
```

Parameter	Description	Permitted Values	Default
static.auto_provision.local_calllog.backup.enable	It enables or disables the phone to upload the <MAC>-calllog.xml file to the server each time the call logs update and download the <MAC>-calllog.xml file from the server during auto provisioning.	0-Disabled, the phone does not upload/download the call log file "<MAC>-calllog.xml" to the server. 1-Enabled, the phone uploads the call log file "<MAC>-calllog.xml" to the specific path configured by the parameter "static.auto_provision.local_calllog.backup.path" each time the call logs update; and downloads the call logs in the "<MAC>-calllog.xml" according to its MAC address from the specific path during auto provisioning.	0

static.auto_provision.local_calllog.backup.path	It configures a path or URL for the phone to upload/download the `<MAC>-calllog.xml` file. If it is left blank, the phone connects to the provisioning server URL, and uploads/downloads the contact file "`<MAC>-calllog.xml`". Example: static.auto_provision.local_calllog.backup.path = http://192.168.1.20/calllog Once the call logs update, the phone will upload the call log file to the specified path "http://192.168.1.20/calllog". During auto provisioning, the phone downloads the call log file "`<MAC>-calllog.xml`" from the specified path "http://192.168.1.20/calllog". **NOTE** It works only if "static.auto_provision.local_calllog.backup.enable" is set to 1 (Enabled).	String	Blank

static.auto_provision.local_calllog.write_delay.terminated	It configures the delay time (in seconds) for the phone to upload the <MAC>-calllog.xml file each time the call logs update. **NOTE** It works only if "static.auto_provision.local_calllog.backup.enable" is set to 1 (Enabled).	Integer from 10 to 600	60
static.auto_provision.custom.upload_method	It configures the way the phone uploads the <MAC>-local.cfg file, <MAC>-calllog.xml file or <MAC>-contact.xml file to the provisioning server (for HTTP/HTTPS server only).	0-PUT 1-POST	

Google Contacts

Google Contacts

Google contact is a phone book that is stored on the Google Contact Server. You can sign in to the Google Contact Server on your phone, and then the phone can establish a connection with the Google Contact Server and download the phone book. As a result, Google contacts appear in the phone directory.

Google Contacts Configuration

The following table lists the parameters that the phone can use to connect to the Google Contact Server.

Configuration Parameter

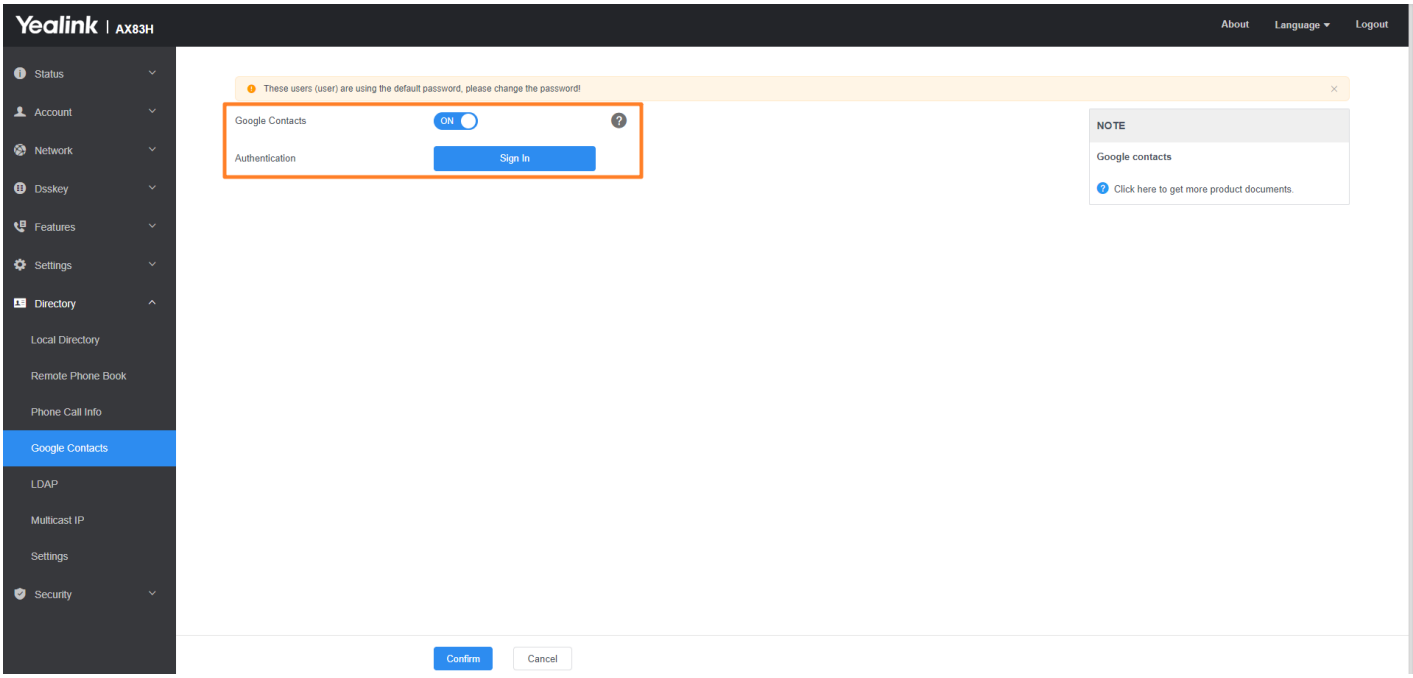
```
google_contact_server.enable
google_contact_server.display_mode
```

Parameter	Description	Permitted Values	Default

google_contact_server.enable	It enables or disables the phone to connect to the Google Contact Server.	0-Disabled 1-Enabled	0
google_contact_server.display_mode	It configures the display mode of the Google contacts. **NOTE** It works only if "google_contact_server.enable" is set to 1 (Enabled).	0-All downloaded Google contacts will be displayed on the phone. 1-Only the Google contacts whose number fields are not empty will be displayed on the phone.	1

Set via the Web User Interface

On the web user interface, go to: **Directory** > **Google Contacts**



Signing in to the Google Contact Server

After you allow the IP phone to connect to the Google Contact Server, you can sign in to the Google Contact Server via the web user interface, so that the Google contacts will appear in the phone directory.

Procedure

1. On your web user interface, select **Directory** > **Google Contacts**.
2. In the Authentication field, click **Sign In**.

A pop-up window and a code are displayed.

1. Enter the code generated on the web user interface into the pop-up window.
2. Enter your email address and password.

3. Allow contact tests to access your Google account.

Comparison of different contacts

Comparison of different contacts

Yealink supports multiple contact formats, and you may want to understand the differences, advantages, and disadvantages of different contact storage methods. This chapter aims to present the distinctions between various contact formats as comprehensively as possible.

Different scenarios for Directory

	Max contacts	Support avatars	Advantages	Disadvantages
Local Directory	1000	√	high-speed query	small storage capacity; inconvenient to update
LDAP	1000 at a time,(the total quantity depends on the LDAP server)	√	lightweight; high-speed query; Easy to modify	Requires dedicated server
Remote Phone Book	10000	√	Shared; Low cost	Inconvenient updates
XML Phonebook	10000	√	Easy deployment; User-friendly	Limited display content
Google Contacts	1000	√	Cloud synchronization; Easy to operate	Not shareable
Network Directory	Requires complementary development	× (Requires complementary development)	Shared; User-friendly; Easy deployment;	Requires complementary development, such as Broadsoft, Meta.

Different usage scenarios for Directory

Scenario 1:
If you need to frequently communicate with certain contacts and your contact list is relatively small (e.g., within 500 people)
Recommended contact method: Local Directory
Scenario 2:

- You are a minimalist and only need contact names and their phone numbers.
- You have a micro download server.

Recommended contact method: XML PhoneBook
Scenario 3:

- If your company is large and has a significant number of shared contacts.
- If you have a comprehensive IT team and a dedicated maintenance server for downloads.
- If you want your team's contacts to be synchronized and updated.
- If your company has a complex organizational structure.

If you meet 2-3 of the above points.

Recommended contact method: LDAP PhoneBook, Remote Phone Book.

Scenario 4:

If you frequently use Google Contacts.

Recommended contact method: Google Contacts.

Scenario 5:

If your account is registered on Broadsoft or Meta servers and you use their network contacts feature.

Recommended contact method: Network Directory

Troubleshooting for Directory

Troubleshooting for Directory

During the regular use of the functionality, you may encounter various issues. This article will primarily address common problems and provide corresponding solutions. If this article does not resolve your issue, please contact technical support for further assistance. https://ticket.yealink.com/index

> ⓘ **NOTE**
> The suggestions are for troubleshooting purposes and may or may not solve the issue.

Local Directory

Why is the contact avatar not displaying correctly?

1. Please check the format of your avatar. The supported formats for local contact avatars are jpg/JPG/JPEG/jpeg. If you are uploading in bulk, make sure your compressed file format is tar.
2. It is possible that your resolution does not meet the requirements. The correct resolution for avatars is 110*110, with a size not exceeding 5MB.

Why is my device lagging and the operation not smooth?

The number of contacts occupies the available memory space of the phone. When the number of contacts exceeds the limit, the available memory of the phone decreases, which may result in lagging response and unsmooth operation of the phone, especially for older models. You can consider deleting some less frequently used contacts or using alternative methods to store contacts, such as LDAP.

Why did the existing contacts disappear after uploading new contacts?

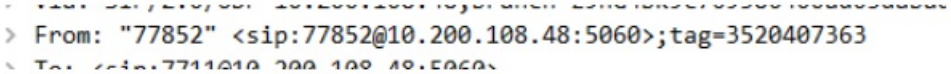
This is normal in such cases. If you uploaded contacts using Autop or imported an XML file through the web interface, it will overwrite the existing contact data. Make sure that the newly uploaded file includes the existing contact data. If you are importing a CSV file through the web interface, there will be a pop-up asking if you want to delete the existing contact data.

Why does the contact upload fail?

1. Your phone's memory space may be insufficient, which is a common issue with older devices. You can try restarting the phone or deleting unnecessary files to free up memory for importing contacts.
2. There might be errors in your contact file, as described above. Please refer to the mentioned description for more details.
3. The autop server address you set may have firewall restrictions, certificate errors, incorrect URL, or configuration statement errors, preventing the phone from accessing the server. Please double-check these aspects.

Why isn't the caller's name correctly matched with the local contact in incoming calls?

Incoming call matching is typically done using the number information in the SIP signaling "From" header, such as:



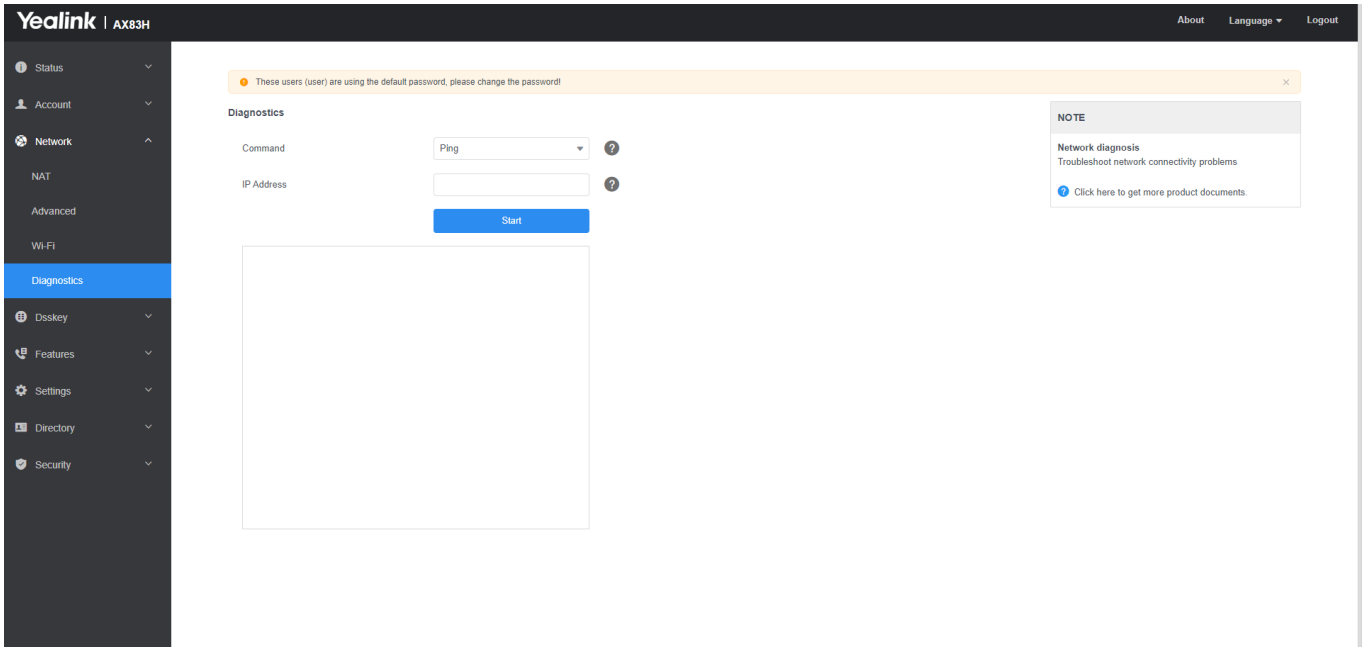
Please confirm if the number carried in the incoming call information is correct.

XML Phonebook

Why is the XML Phonebook unable to display contact information and shows a "Network Unavailable" message?

The proper functioning of XML Phonebook relies on the ability of the phone to interact with the server. If you encounter an "Network Unavailable" message, the main causes and possible solutions are as follows:

1. Check network connectivity: Ensure that the phone can successfully ping the server's IP address. On the web user interface, go to **Network** > **Diagnostics**.



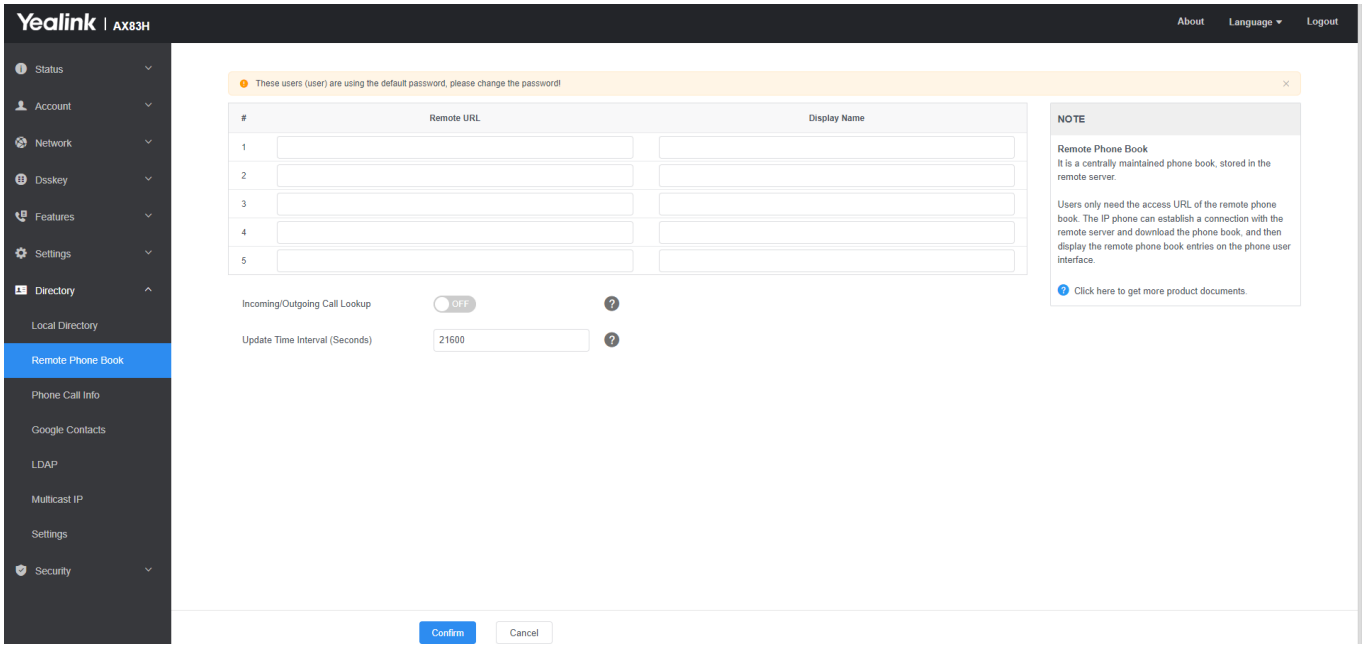
2. Verify certificate settings: Confirm that the device and server have the correct certificate settings (HTTPS). Both the server and the phone should have uploaded the appropriate certificates.

Remote Phone Book

Why is it that after updating the content of the Remote Phone Book on the server, the changes are not reflected on the phone?

This is normal behavior. The Remote Phone Book is not synchronized with the server in real-time. To trigger an update, you can try one of the following methods:

1. Log in to the phone's web interface, go to the Remote Phone Book section, and click **Confirm** to trigger an update.



2. Restart the phone to trigger an update.
3. Set a scheduled update time for the device to update periodically.
4. On the phone's UI, go to the Remote Phone Book section and click **Update**.

Why is the phone unable to access via HTTPS?

The common reasons for the phone being unable to access via HTTPS are related to the connection with the server. You can first try accessing the server via HTTP to check if it works properly. If HTTP works fine but there are issues with HTTPS, you can try the following solutions:

1. The phone may not have uploaded the server certificate. You can try disabling certificate verification on the phone by going to Web UI > Security > Trusted Certificates > Only Accept Trusted Certificates, or uploading the server certificate to the phone.
2. Poor network conditions can cause SSL authentication timeout and result in failure. You can try increasing the timeout duration by adjusting the configuration. For example, set "static.network.attempt_expired_time = 20" to see if the issue is resolved.
3. Mismatched TLS versions or unsupported encryption algorithms can cause issues. Yealink devices default to supporting TLS 1.2. If you're using V81 firmware and unable to use TLS 1.2, please contact Yealink technical support for assistance.

Bluetooth contacts

Why can't I view my phone's contact information on the phone?

After successfully connecting your Bluetooth phone to the phone, the phone will automatically create a phone contact group and, once the phone contacts are downloaded, the functionality will be the same as that of local

contacts. If you are unable to view your phone's contact information on the phone, please check the following aspects for any possible misconfigurations:

1. Check if the contacts on your Bluetooth phone are stored on the SIM card rather than the phone itself. The phone cannot synchronize contacts from the SIM card.
2. The phone currently supports Bluetooth contact formats in VCF (vCard) format. For non-VCF formatted Bluetooth contacts, the phone will treat them as synchronization failures.
3. Verify that the "Mobile contact sync" switch on your Bluetooth phone is enabled. If it is disabled, the phone will not download phone contacts.
4. If the Bluetooth connection is interrupted during the synchronization process, the download will not be successful.
5. If you have a large number of contacts, exceeding 500, some contacts may not be displayed. The phone can only download up to 500 contacts.

Google Contacts

Why can't I sign in to my Google contacts and receive the message "Sign in with Google temporarily disabled for this app"?

1. This issue is commonly caused by the expiration of the client authorization for the built-in client account on the device. You can try creating your own Google account's Client ID to resolve this issue. For detailed instructions on how to create a Client ID, please refer to the Google official website.
2. You can also contact Yealink technical support for assistance and they can provide you with a solution.

Google Contacts login abnormality, with the same account, may require two login attempts to be successful.

If the Google Cloud Platform does not have the Contact API enabled, it can cause abnormal behavior in Google Contacts. To resolve this issue, you can try the following steps:

1. Go to the console and click on the left-side main menu.
2. Navigate to API & Services and select Library.
3. Search for "Contact API" in the library and enable it.

Console Link: https://console.cloud.google.com/apis/library?project=formal-landing-280613

LDAP

LDAP incoming and outgoing calls do not match the contacts.

You can try the following methods to identify the cause and possibly resolve the issue:

1. Make sure you have enabled LDAP incoming and outgoing call matching. The corresponding configuration should be ldap.call_in_lookup=1 and ldap.call_out_lookup=1.
2. Verify that your search criteria are correct and not empty. For example, the ldap.name_filter=(|(cn=%)(sn=%)) rule allows you to input characters in the % position and search the server. If your server does not have the corresponding attributes, it may result in a failed match.
3. Check if your regular expression (regex) matching configuration is set correctly. If your incoming call number includes an area code or other prefixes, you need to use regex matching to remove the additional information. Refer to the "Number Matching Settings" for detailed instructions on how to use regex for matching.

The LDAP contact number display type does not correspond to the number type provided by the server.

The issue you are experiencing is as follows: For example, you have stored a contact on the server as follows:
Jim
telephoneNumber = 123
mobile = 456
homePhone = 789
However, the phone displays it as:
Jim
office: 456
mobile: 789
Other: 123
This behavior is normal. Currently, the LDAP number display does not have a strong association with the content on the LDAP server because different users have different naming conventions. It is challenging for the terminal devices to be compatible with all situations. Therefore, Yealink provides only three fields on the device to display the numbers in the order they are returned by the server. As a result, the displayed numbers may not match your expected display.ll situations. Therefore, Yealink provides only three fields on the device to display the numbers in the order they are returned by the server.

Audio Features

Alert Tone

Introduction

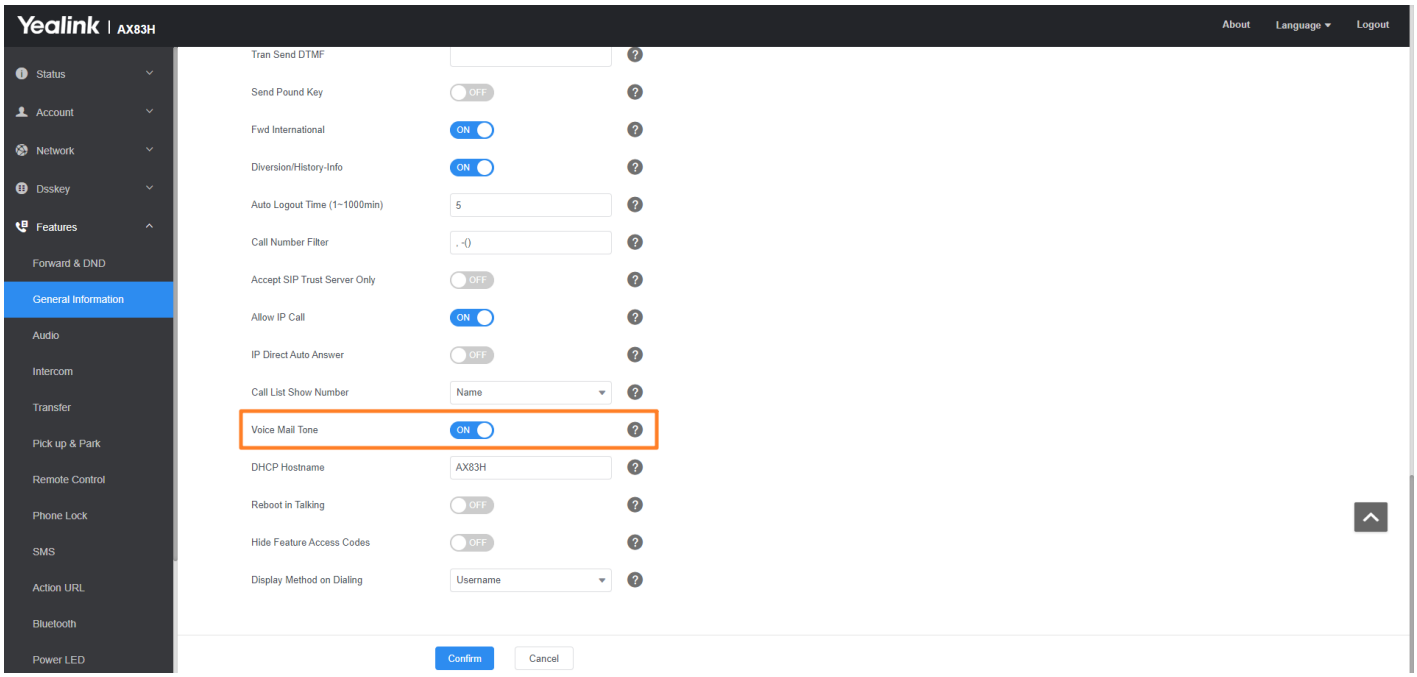
You can configure the following audio alert for the phone:

- **Redial tone**: allow the phones to continue to play the dial tone after inputting the preset numbers on the dialing
  screen.
- **Voice mail tone**: allow the IP phone to play a warning tone when receiving a new voicemail. You can customize the warning tone or select specialized tone sets (vary from country to country) for your IP phone.
- **Dial tone**: allow the IP phone to play a specific dial tone for a specified time.
- **Key tone**: allow the IP phone to play a key tone when you press any key.

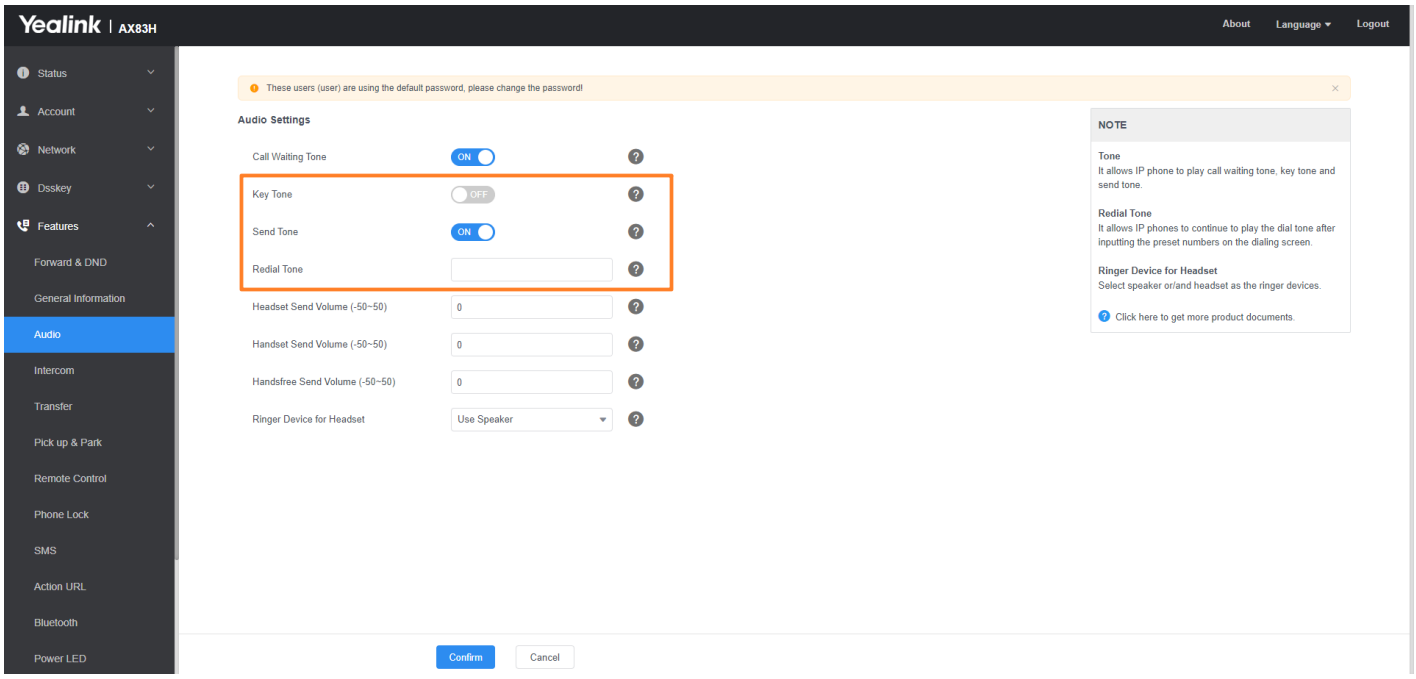
Alert Tone Configuration

Set via the Web User Interface

On the web user interface, go to **Features** > **General Information** > **Voice Mail Tone**.



On the web user interface, go to **Features** > **Audio** > **Redial Tone**/**Key Tone**/**Send Tone**.



Configuration Parameter

features.call.dialtone_time_out
phone_setting.outgoing_call_answer_tone.enable
features.voice_mail_tone_enable

Parameter	Permitted Values	Default	Description
features.redial_tone	Integer within 6 digits	Blank	It configures that after you enter a specific number on the dialing screen, the phone will replay the dial tone.

account.X.dial_tone	**0**-Default (depend on the country tone by "voice.tone.country") **1**-440/250,0/250 **2**-1000/250,0/250	0	It configures the dial tone for the phone.
features.call.dialtone_time_out	Integer from 0 to 65535	15	It configures the duration time (in seconds) that a dial tone plays before a call is dropped. If it is set to 0, the call is not dropped.
features.voice_mail_tone_enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to play a warning tone when it receives a new voicemail. **NOTE** It works only if "account.X.display_mwi.enable" is set to 1 (Enabled).
features.send_key_tone	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to play a key tone when a user presses any key on your phone keypad.
features.call.dialtone_time_out	Integer from 0 to 65535	15	It configures the duration time (in seconds) that a dial tone plays before a call is dropped. If it is set to 0, the call is not dropped.
phone_setting.outgoing_call_answer_tone.enable	**0**-Disabled **1**-Enabled	1	It configures the handsets to have a prompt sound (Beep) after the call is answered by the remote end.
features.voice_mail_tone_enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to play a warning tone when it receives a new voicemail. **NOTE** It works only if `account.X.display_mwi.enable` is set to 1 (Enabled).

Tones

Introduction

When receiving a message, the phone 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 IP phone.

Supported Tones

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

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

Configured tones can be heard on the phones in the following conditions.

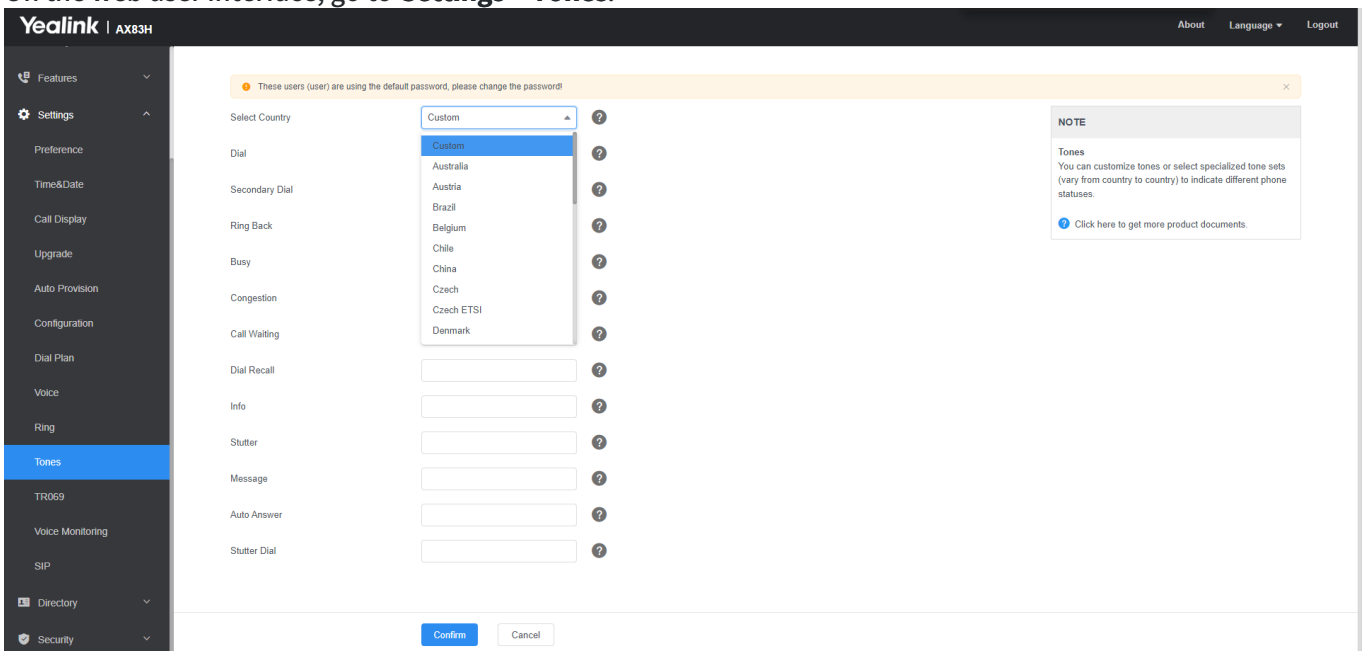
Condition	Description
Dial	When in the dialing interface
Ring Back	Ring-back tone

Busy	When the callee is busy
Call Waiting	Call waiting tone (For more information on call waiting, refer to Call Waiting)

Tones Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Tones**.



Configuration Parameter

Configuration Parameter

voice.tone.country
voice.tone.dial
features.partition_tone
voice.tone.secondary_dial
voice.tone.ring
voice.tone.busy
voice.tone.congestion
features.congestion_tone.codelist
voice.tone.callwaiting
voice.tone.dialrecall
voice.tone.info
voice.tone.stutter
voice.tone.message
voice.tone.autoanswer
voice.tone.stutterdial
voice.tone.stutter_dial_tone.apply_to_dnd.enable
voice.tone.stutter_dial_tone.apply_to_fwd.enable
voice.tone.stutter_dial_tone.apply_to_vm.enable

Parameter	Description	Permitted Values	Default

voice.tone.country	It configures the country tone for the phones.	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
voice.tone.dial	It customizes the dial tone. tone list = element[,element][,element]… Where element = [!]Freq1[+Freq2][+Freq3][+Freq4] /Duration Freq: the frequency of the tone (ranges from 200 to 4000 Hz). If it is set to 0 Hz, it means the tone is not played. **ⓘ NOTE** It works only if "voice.tone.country" is set to Custom.	String	Blank
features.partition_tone[1]	It enables or disables the phone to play the different dial tones when there is no active account. **ⓘ NOTE** It works only if "voice.tone.dial" is configured.	0-Disabled 1-Enabled. If there is an active account, the phone will play the default dial tone. If there is no active account, the phone will play the dial tone configured by "voice.tone.dial".	0
voice.tone.secondary_dial	It customizes the secondary dial tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **ⓘ NOTE** It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.	String	350+440/3000

voice.tone.ring	It customizes the ringback tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **NOTE** It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.	String	Blank
voice.tone.busy	It customizes the tone when the callee is busy. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **NOTE** It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.	String	Blank
voice.tone.congestion	It customizes the tone when the network is congested or no available accounts (SIP account&IP call account) on the phone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **NOTE** It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.	String	Blank

features.congestion_tone.codelist	It configures the return code to play the congestion tone. Multiple codes are separated by commas. Example: features.congestion_tone.codelist = 403,503,603 **NOTE** The congestion tone can be customized by "voice.tone.congestion".	any code that the server can return	Blank
voice.tone.callwaiting	It customizes the call waiting tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **NOTE** It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.	String	Blank
voice.tone.dialrecall	It customizes the callback tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **NOTE** It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.	String	Blank

voice.tone.info	It customizes the info tone. The phone will play the info tone with the special information, for example, the number you are calling is not in service. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **ⓘ NOTE** It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.	String	Blank
voice.tone.stutter	It customizes the tone when the IP phone receives a voicemail. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **ⓘ NOTE** It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.	String	Blank

voice.tone.message	It customizes the tone when the phone receives a text message. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **NOTE** It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.	String	Blank
voice.tone.autoanswer	It customizes the warning tone for the auto answer. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **NOTE** It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.	String	Blank

voice.tone.stutterdial	It customizes the dial tone when DND or call forward is activated or the phone has a new voice message. The value format is Freq/Duration. For more information on the value format, refer to the parameter “voice.tone.dial”. **NOTE** It works only if “voice.tone.country” is set to Custom and "voice.tone.stutter_dial_tone.apply_to_dnd.enable"/"voice.tone.stutter_dial_tone.apply_to_fwd.enable"/"voice.tone.stutter_dial_tone.apply_to_vm.enable" is set to 1 (Enabled). If you want to disable this warning tone, set it to 0.	String within 512 characters	Blank
voice.tone.stutter_dial_tone.apply_to_dnd.enable	It enables or disables the phone to play a specified dial tone when DND is activated on the phone. The dial tone is configured by "voice.tone.stutterdial". **NOTE** It works only if “voice.tone.country” is set to Custom.	0-Disabled 1-Enabled	0
voice.tone.stutter_dial_tone.apply_to_fwd.enable	It enables or disables the phone to play a specified dial tone when call forward is activated on the phone. The dial tone is configured by "voice.tone.stutterdial". **NOTE** It works only if “voice.tone.country” is set to Custom.	0-Disabled 1-Enabled	0

voice.tone.stutter_dial_tone.apply_to_vm.enable	It enables or disables the phone to play a specified dial tone when the phone has a new voice message. The dial tone is configured by "voice.tone.stutterdial". **NOTE** It works only if "voice.tone.country" is set to Custom.	0-Disabled 1-Enabled	0
features.touch_tone	It enables or disables the touch tone.	0-Disabled 1-Enabled	1

Ringer Device

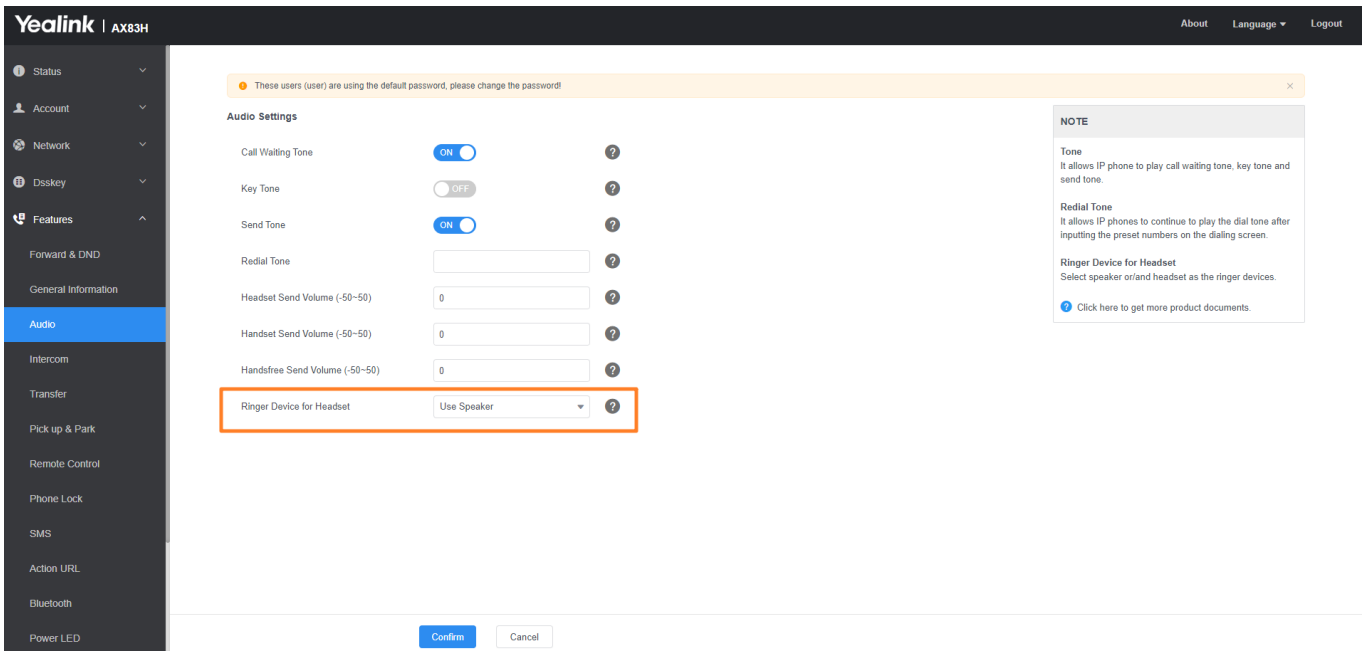
Introduction

You can use either or both the speaker and the headset as the ringer devices. You can configure which ringer device to be used when receiving an incoming call. For example, if the ringer device is set to Headset, ring tone will be played through your headset.

Ringer Device Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **Audio** > **Ringer Device for Headset.**



Configuration Parameter

```
features.ringer_device.is_use_headset
```

Parameter	Permitted Values	Default	Description
features.ringer_device.is_use_headset	**0**-Use Speaker **1**-Use Headset	0	It configures the ringer device for the phone.

Audio Volume

Introduction

You can configure the sending volume and ringer volume for the phone.

Ringer Volume Configuration

You can configure the ringer volume as a fixed level so the user cannot adjust the ringer volume on the phone. This feature avoids missing calls when the user turns down the ringer volume.

```
force.voice.ring_vol
```

Parameter	Permitted Values	Default	Description

force.voice.ring_vol	**Blank**-the user can adjust the ringer volume on the phone. **0 to 15**-the user cannot adjust the ringer volume on the phone; the ring tone is the configured volume.	Blank	It configures the ring tone as a fixed volume. **NOTE** You can set the `force.voice.ring_vol>0` only if `custom.handset.silent_charging` is set to 1.

Distinctive Ring Tones

Introduction

The feature of distinctive ring tones allows certain incoming calls to trigger the phones to play distinctive ring tones.
The phone inspects the INVITE request for an "Alert-Info" header when receiving an incoming call. If the INVITE request contains an "Alert-Info" header, the phone strips out the URor keyword parameter and maps it to the appropriate ring tone.

NOTE
If the caller already exists in the local directory, the ring tone assigned to the caller should be preferentially played.
The distinctive ring tone priority is higher than the normal incoming calling tone setting.

Supported Alert-Info Headers Format

Yealink phones support Alert-Info headers in four formats: Bellcore-drN, ringtone-N (or MyMelodyN), and info=info text;x-line-id=0.

TIP
If the Alert-Info header contains multiple types of keywords, the phone will process the keywords in the following order:
AutoAnswer > UR > info text/Bellcore-drN/ringtone-N (ringtone-RingN) > MyMelodyN (MyMelodyRingN).

Alert-Info: Bellcore-drN

When the Alter-Info header contains the keyword “Bellcore-drN”, the phone will play the desired ring tone.
The following table identifies the corresponding ring tones:

Value of N	Ring Tone (features.alert_info_tone = 1)	Ring Tone (features.alert_info_tone = 0)
1	Bellcore-dr1	Ring1.wav
2	Bellcore-dr2	Ring2.wav
3	Bellcore-dr3	Ring3.wav
4	Bellcore-dr4	Ring4.wav
5	Bellcore-dr5	Ring5.wav
6	Ring6.wav	
7	Ring7.wav	
8	Ring8.wav	
9	Silent.wav	
10	Splash.wav	
N<1 or N>10	Ring1.wav	

Examples:

```
Alert-Info: http://127.0.0.1/Bellcore-dr1
Alert-Info: test/Bellcore-dr1
Alert-Info: Bellcore-dr1
Alert-Info: Bellcore-dr1;x-line-id=1
Alert-Info: <http://10.1.0.31>;info=Bellcore-dr1
```

The following table identifies the different Bellcore ring tone patterns and cadences. These ring tones are designed for the BroadWorks server.

Bellcore Tone	Pattern ID	Pattern	Cadence	Minimum Duration (ms)	NominaDuration (ms)	Maximum Duration (ms)
Bellcore-dr1 (standard)	1	Ringing	2s On	1800	2000	2200
		Silent	4s Off	3600	4000	4400
Bellcore-dr2	2	Ringing	Long	630	800	1025
		Silent		315	400	525
		Ringing	Long	630	800	1025
		Silent		3475	4000	4400
Bellcore-dr3	3	Ringing	Short	315	400	525
		Silent		145	200	525
		Ringing	Short	315	400	525
		Silent		145	200	525

		Ringing	Long	630	800	1025
		Silent		2975	4000	4400
Bellcore-dr4	4	Ringing	Short	200	300	525
		Silent		145	200	525
		Ringing	Long	800	1000	1100
		Silent		145	200	525
		Ringing	Short	200	300	525
		Silent		2975	4000	4400
Bellcore-dr5	5	Ringing		450	500	550

NOTE
If the user is waiting for a call, "Bellcore-dr5" is a splash ring tone reminding the user that the DND or Always CalForward feature is enabled on the server side.

Alert-Info: ringtone-N/Alert-Info: ringtone-RingN.wav (or Alert-Info: MyMelodyN/Alert-Info: MyMelodyRingN.wav)

When the Alter-Info header contains the keyword "ringtone-N/ringtone-RingN" or "MyMolodyN/MyMelodyRingN", the phone will play the corresponding local ring tone (RingN.wav), or play the first local ring tone (Ring1.wav) for about 10 seconds if "N" is greater than 10 or less than 1.

Examples:

```
Alert-Info: ringtone-2
Alert-Info: ringtone-Ring2.wav
Alert-Info: ringtone-2;x-line-id=1
Alert-Info: <http://10.1.0.31>;info=ringtone-2
Alert-Info: <http://127.0.0.1/ringtone-2>
Alert-Info: MyMelody2
Alert-Info: MyMelodyRing2.wav
Alert-Info: MyMelody2;x-line-id=1
Alert-Info: <http://10.1.0.31>;x-line-id=0;info=MyMelody2
```

The following table identifies the corresponding local ring tones:

Value of N	Ring Tone
1 Ring1.wav	Ring1.wav
2 Ring2.wav	Ring2.wav
3 Ring3.wav	Ring3.wav

4 Ring4.wav	Ring4.wav
5 Ring5.wav	Ring5.wav
6 Ring6.wav	Ring6.wav
7 Ring7.wav	Ring7.wav
8 Ring8.wav	Ring8.wav
9 Silent.wav	Silent.wav
10 Splash.wav	Splash.wav
N<1 or N>10	Ring1.wav

Alert-Info: < URL >

When the Alert-Info header contains a remote URL, the phone will try to download the WAV ring tone file from the URL and then play the remote ring tone if `account.X.alert_info_url_enable` is set to 1 (or the item called **Distinctive Ring Tones** on the web user interface is Enabled), or play the preconfigured local ring tone in about 10 seconds if `account.X.alert_info_url_enable` is set to 0 or if the phone fails to download the remote ring tone.

Example:

```
Alert-Info: http://192.168.0.12:8080/Custom.wav
```

Alert-Info: info=info text;x-line-id=0

When the Alert-Info header contains an info text, the phone will map the text with the InternaRinger Text preconfigured (or `distinctive_ring_tones.alert_info.X.text` is configured) on the phone, and then play the ring tone associated with the InternaRinger Text (the ring tone can be configured by the parameter `distinctive_ring_tones.alert_info.X.ringer`). If no internal ringer text maps, the phone will play the preconfigured local ring tone for about 10 seconds.

Example:

```
Alert-Info: info=family;x-line-id=0
Alert-Info: <http://10.1.0.31>;info=family
Alert-Info: <http://10.1.0.31>;info=family;x-line-id=0
```

Auto Answer

If the INVITE request contains the following string types, the phone will answer incoming calls automatically without playing the ring tone:

- Alert-Info: Auto Answer

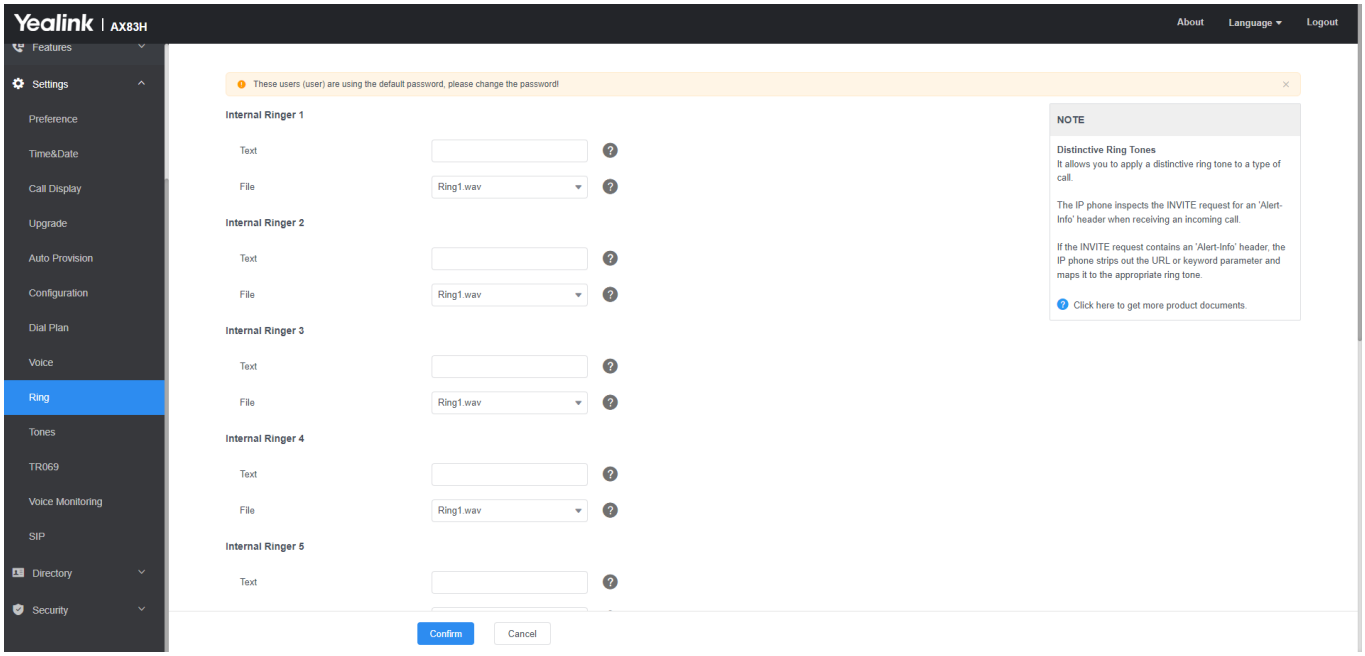
- Alert-Info: info = alert-autoanswer
- Alert-Info: answer-after = 0 (or Alert-Info: Answer-After = 0)
- Alert-Info: Intercom

If the auto answer tone feature is enabled, the phone plays a warning tone to alert you before answering an incoming call.

Distinctive Ring Tones Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Ring** > **Internal Ringer[x]**.



Configuration Parameter

```
distinctive_ring_tones.alert_info.X.text
distinctive_ring_tones.alert_info.X.ringer
```

Parameter	Permitted Values	Default	Description
distinctive_ring_tones.alert_info.X.text[1]	String within 32 characters	Blank	It configures the internal ringer text to map the keywords contained in the Alert-Info header.

distinctive_ring_tones.alert_info.X.ringer[1]	Integer from 1 to 10 (the digit stands for the appropriate ring tone) or ring tone name: **1** or **Ring1.wav** **2** or **Ring2.wav** 3 or **Ring3.wav** **4** or **Ring4.wav** **5** or **Ring5.wav** **6** or **Ring6.wav** **7** or **Ring7.wav** **8** or **Ring8.wav** **9** or **Ring9.wav** **10** or **Ring10.wav** **11** or **Ring11.wav** **12** or **Ring12.wav** **13** or **Ring13.wav** **14** or **Silent.wav** **15** or **Splash.wav** · Custom ring tone name (for example, Customring.wav)	1	It configures the desired ring tone for each internal ringer text.

[1]X is the ringtone ID. X=1-10.

Audio Codecs

Introduction

CODEC is an abbreviation of COmpress-DECompress, capable of coding or decoding a digital data stream or signal by implementing an algorithm. The object of the algorithm is to represent the high-fidelity audio signal with a minimum number of bits while retaining the quality. This can effectively reduce the frame size and the bandwidth required for audio transmission.
The audio codec that the phone uses to establish a call should be supported by the SIP server. When placing a call, the phone will offer the enabled audio codec list to the server and then use the audio codec negotiated with the called party according to the priority.

Supported Audio Codecs

The following table summarizes the supported audio codecs on the phones:

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
G722	G.722	RFC 3551	64 Kbps	16 Ksps	20 ms

PCMA(G.711A)	G.711 a-law	RFC 3551	64 Kbps	8 Ksps	20 ms
PCMU(G.711μ)	G.711 u-law	RFC 3551	64 Kbps	8 Ksps	20 ms
G729(G729A)	G.729	RFC 3551	8 Kbps	8 Ksps	20 ms
G726-16	G.726	RFC 3551	16 Kbps	8 Ksps	20 ms
G726-24	G.726	RFC 3551	24 Kbps	8 Ksps	20 ms
G726-32	G.726	RFC 3551	32 Kbps	8 Ksps	20 ms
G726-40	G.726	RFC 3551	40 Kbps	8 Ksps	20 ms
iLBC	iLBC	RFC 3952	15.2 Kbps 13.33 Kbps	8 Ksps	20 ms 30 ms

NOTE
The network bandwidth necessary to send the encoded audio is typically 5~10% higher than the bit rate due to packetization overhead. For example, a two-way G.722 audio call at 64 Kbps consumes about 135 Kbps of network bandwidth.

The codec supports various audio bandwidths, defined as follows:

Abbreviation	Audio Bandwidth	Sample Rate (Effective)
NB (narrowband)	4 kHz	8 kHz
MB (medium-band)	6 kHz	12 kHz
WB (wideband)	8 kHz	16 kHz
SWB (super-wideband)	12 kHz	24 kHz
FB (fullband)	20 kHz	48 kHz

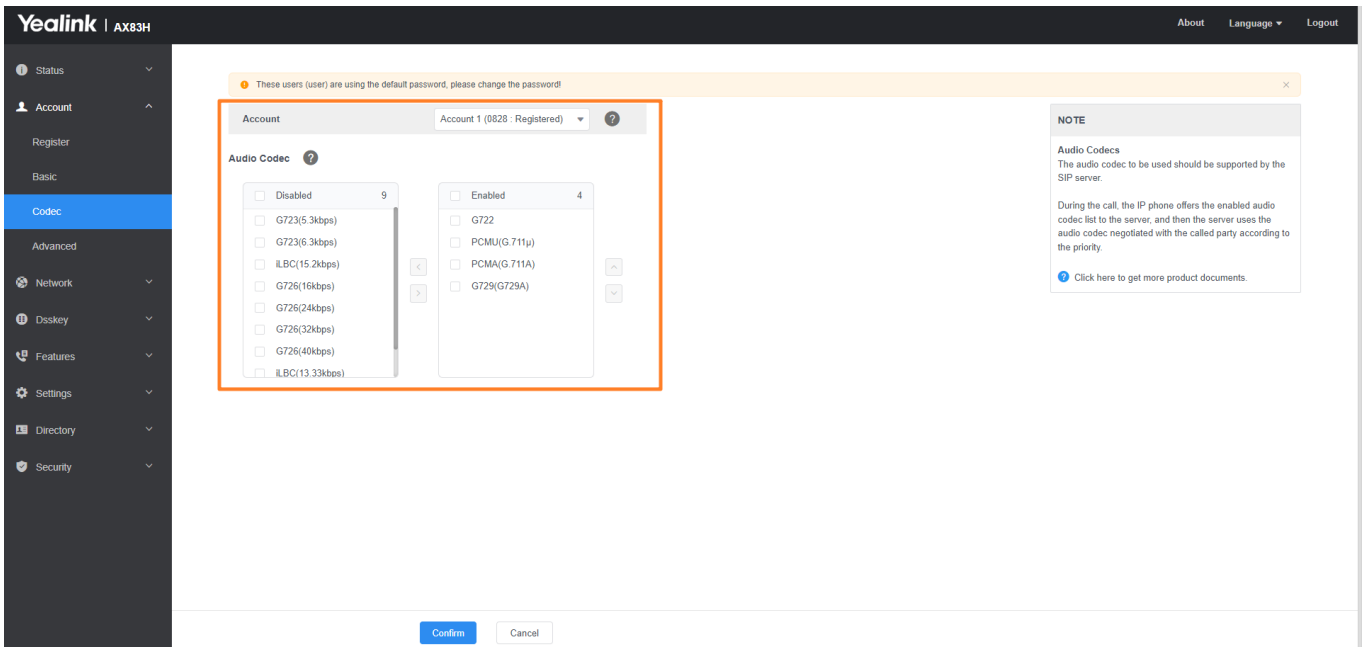
The following table lists the audio codecs supported by each phone model:

Supported Audio Codecs	Default Audio Codecs
G722, PCMA(G.711A), PCMU(G.711μ), G729(G729A), G726-16, G726-24, G726-32, G726-40, iLBC	G722, PCMA(G.711A), PCMU (G.711μ), G729(G729A)

Audio Codecs Configuration

Set via the Web User Interface

1. On the web user interface, go to **Account** > **Codec** > **Audio Codec**.



Configuration Parameter

account.X.codec.<payload_type>.enable
account.X.codec.<payload_type>.priority
phone_setting.talking_codec_display

Parameter	Permitted Values	Default	Description
		When the audio codec is G722, the default value is 1; When the audio codec is PCMU(G.711μ), the default value is 1; When the audio codec is PCMA(G.711A), the default value is 1; When the	It enables or disables the specified audio codec. The name (payload_type) of the audio codec: **g722**-G722 **pcmu**-PCMU(G.711μ) **pcma**-PCMA(G.711A)

account.X.codec.<payload_type>.enable[1]	**0**-Disabled **1**-Enabled	audio codec is G729(G729A), the default value is 1; When the audio codec is G726-16, the default value is 0; When the audio codec is G726-24, the default value is 0; When the audio codec is G726-32, the default value is 0; When the audio codec is G726-40, the default value is 0; When the audio codec is iLBC, the default value is 0;	**g729**-G729(G729A) **g726_16**-G726-16 **g726_24**-G726-24 **g726_32**-G726-32 **g726_40**-G726-40 **ilbc**-iLBC **Example**: account.1.codec.g722.enable = 1 **NOTE** The name of the audio codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect.
		When the audio codec is G722, the default value is 1; When the audio codec is PCMU(G.711μ), the default value is 2; When the audio codec is PCMA(G.711A), the default	It configures the priority of the enabled audio codec. The name of the audio codec: **g722**-G722 **pcmu**-PCMU(G.711μ)

account.X.codec.<payload_type>.priority[1]	Integer from 0 to 10	value is 3; When the audio codec is G729(G729A), the default value is 4; When the audio codec is G726-16, the default value is 0; When the audio codec is G726-24, the default value is 0; When the audio codec is G726-32, the default value is 0; When the audio codec is G726-40, the default value is 0; When the audio codec is iLBC, the default value is 0;	**pcma**-PCMA(G.711A) **g729**-G729(G729A) **g726_16**-G726-16 **g726_24**-G726-24 **g726_32**-G726-32 **g726_40**-G726-40 **ilbc**-iLBC **Example**: account.1.codec.g722.priority = 1 **NOTE** The priority of the codec in the disable codec list is not specified, and numerical value 1 is defined as the highest priority in the enable codec list. The name of the audio codec in this parameter should be the correct one as listed in the above example, otherwise, the corresponding configuration will not take effect.
phone_setting.talking_codec_display	amr	AMR: Display AMR icon during AMR calls Both can be configured simultaneously, separated by commas.	It is used to configure whether the corresponding codec should display the corresponding icon.

[1] X is the account ID.

Packetization Time (PTime)

Introduction

PTime is a measurement of the duration (in milliseconds) of how long the audio data in each RTP packet is sent to the destination, and defines how much the network bandwidth is used for the RTP stream transfer. Before establishing a conversation, codec and ptime are negotiated through SIP signaling. The valid values of ptime range from 10 to 60, in increments of 10 milliseconds. The default ptime is 20 ms. You can also disable the ptime negotiation.

Supported PTime of Audio Codec

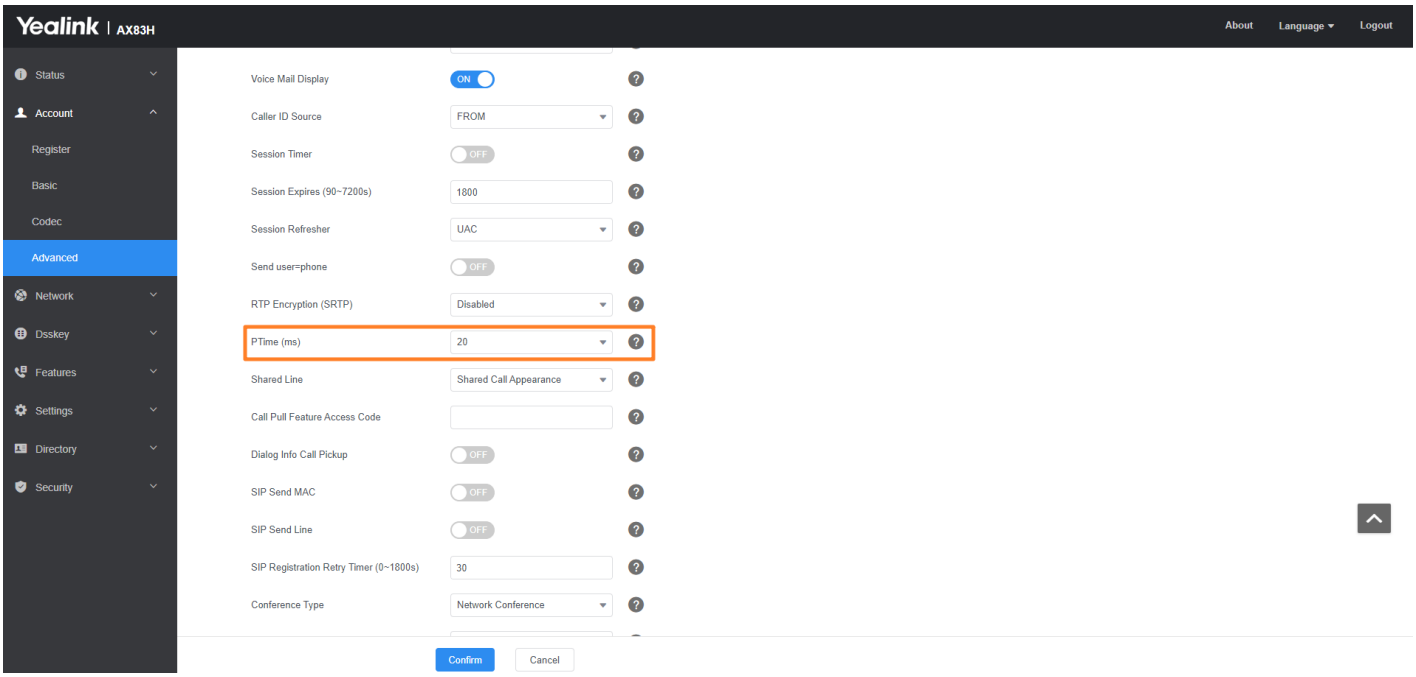
The following table summarizes the valid values of ptime for each audio codec:

Codec	Packetization Time (Minimum)	Packetization Time (Maximum)
G722	10 ms	40 ms
PCMA	10 ms	40 ms
PCMU	10 ms	40 ms
G729	10 ms	80 ms
G726-16	10 ms	30 ms
G726-24	10 ms	30 ms
G726-32	10 ms	30 ms
G726-40	10 ms	30 ms
iLBC	20 ms	30 ms

PTime Configuration

Set via the Web User Interface

On the web user interface, go to **Account** > **Advanced** > **PTime (ms)**.



Configuration Parameter

account.X.ptime

Parameter	Permitted Values	Default	Description
account.X.ptime[1]	**0**-Disabled **10**-10 **20**-20 **30**-30 **40**-40 **50**-50 **60**-60	20	It configures the ptime (in milliseconds) for the codec.

Early Media

Introduction

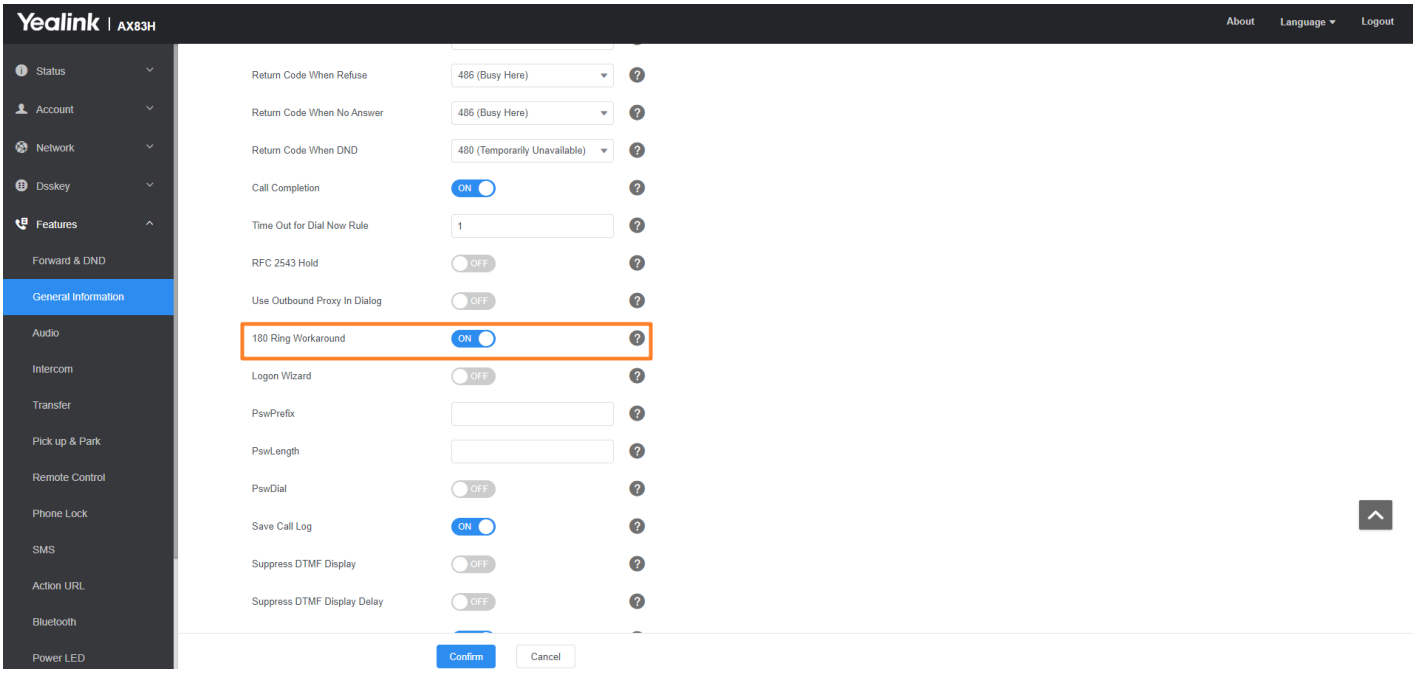
The early media refers to the media (for example, audio and video) played to the caller before a SIP call is actually established.

You can also configure a 180 ring workaround which defines whether to deal with the 180 messages received after the 183 messages. When the caller receives a 183 message, it suppresses any local ringback tone and begins to play the media received. 180 ring workaround allows the phones to resume and play the local ringback tone upon a subsequent 180 message received.

Early Media Configuration

Set via the Web User Interface

On the web user interface, go to **Features** > **General Information** > **180 Ring Workaround**.



Configuration Parameter

```
phone_setting.is_deal180
```

Parameter	Permitted Values	Default	Description
phone_setting.is_deal180	**0**-Disabled **1**-Enabled, the phone will resume and play the local ringback tone upon a subsequent 180 message received.	1	It enables or disables the phone to deal with the 180 SIP messages received after the 183 SIP messages.

Acoustic Clarity Technology

Introduction

To optimize the audio quality in your network, Yealink phones support acoustic clarity technology: Background Noise Suppression (BNS), Automatic Gain Control (AGC), Voice Activity Detection (VAD), Comfort Noise Generation (CNG), and jitter buffer.

Noise Suppression

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.

Noise Suppression Configuration

voice.tns.enable

Parameter	Permitted Values	Default	Description
voice.tns.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the Noise Suppression feature.

Background Noise Suppression (BNS)

Background noise suppression (BNS) is designed primarily for hands-free operation and reduces background noise to enhance communication in noisy environments.

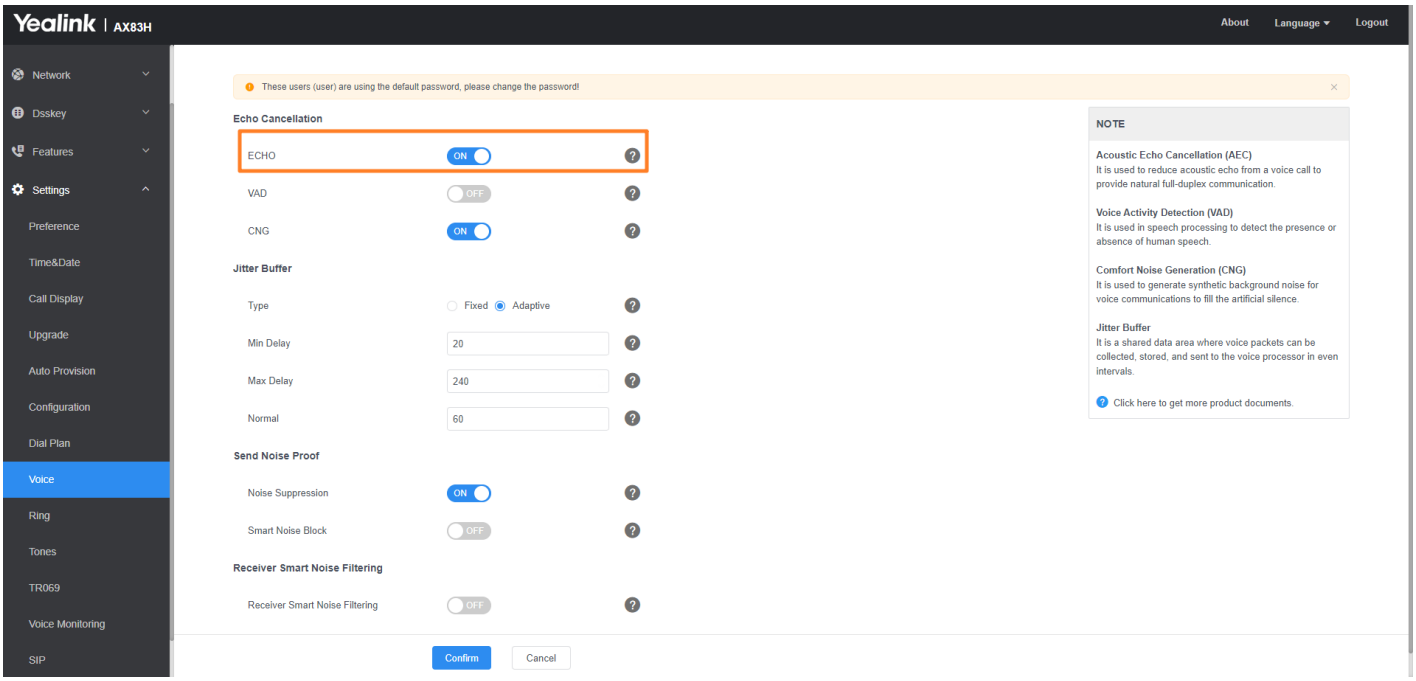
Acoustic Echo Canceller（AEC）

Acoustic Echo Canceller（AEC）can eliminate echo during hands-free calls.

AEC Configuration

Set via the Web User Interface

On the web user interface, go to **Settings** > **Voice** > **Echo Cancellation** > **ECHO**.



Configuration Parameter

voice.echo_cancellation

Parameter	Permitted Values	Default	Description
voice.vad	**0**-Disabled **1**-Enabled	1	It enables or disables the AEC (Acoustic Echo Canceller) feature.

Automatic Gain Control (AGC)

Automatic Gain Control (AGC) applies to the hands-free operation and is used to keep audio output at nearly a constant level by adjusting the gain of signals in some circumstances. This increases the effective user-phone radius and helps with the intelligibility of soft-talkers.

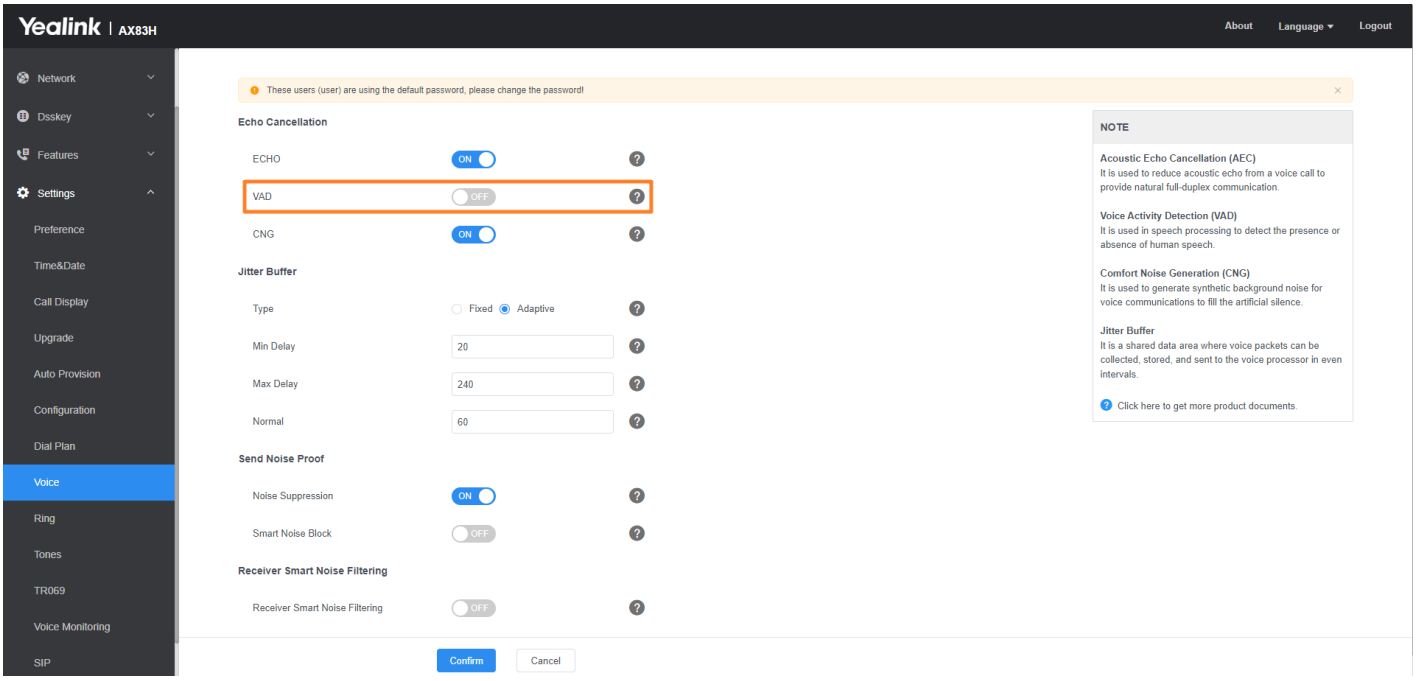
Voice Activity Detection (VAD)

VAD can avoid unnecessary coding or transmission of silence packets in VoIP applications, saving on computation and network bandwidth.

VAD Configuration

Set via the Web User Interface

On the web user interface, go to **Settings** > **Voice** > **Echo Cancellation** > **VAD**.



Configuration Parameter

voice.vad

Parameter	Permitted Values	Default	Description
voice.vad	**0**-Disabled **1**-Enabled	0	It enables or disables the VAD (Voice Activity Detection) feature.

Comfort Noise Generation (CNG)

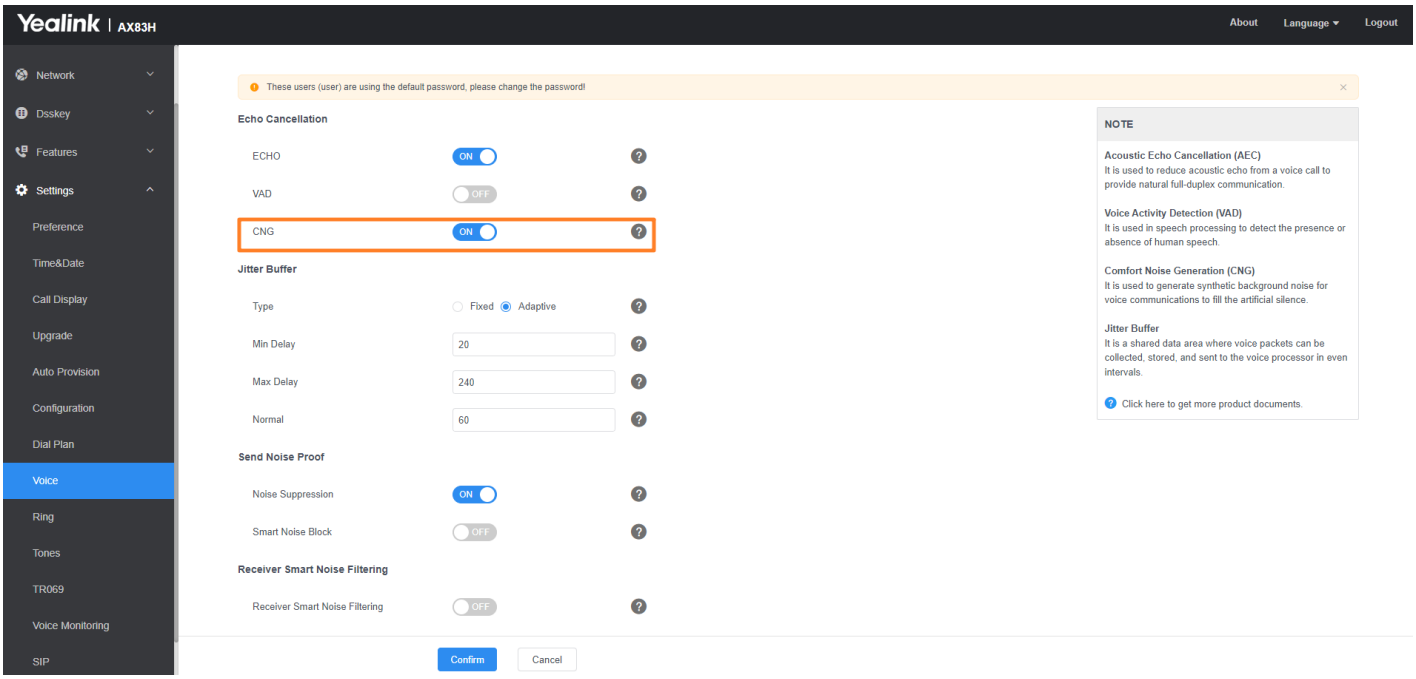
Comfort Noise Generation (CNG) is used to generate background noise for voice communications during periods of silence in a conversation.

> **NOTE**
> VAD is used to send CN packets when the phone detects a "silence" period; CNG is used to generate comfortable noise when the phone receives CN packets from the other side.

CNG Configuration

Set via the Web User Interface

On the web user interface, go to **Settings** > **Voice** > **Echo Cancellation** > **CNG**.



Configuration Parameter

```
voice.cng
```

Parameter	Permitted Values	Default	Description
voice.cng	**0**-Disabled **1**-Enabled	0	It enables or disables the CNG (Comfortable Noise Generation) feature.

Jitter Buffer

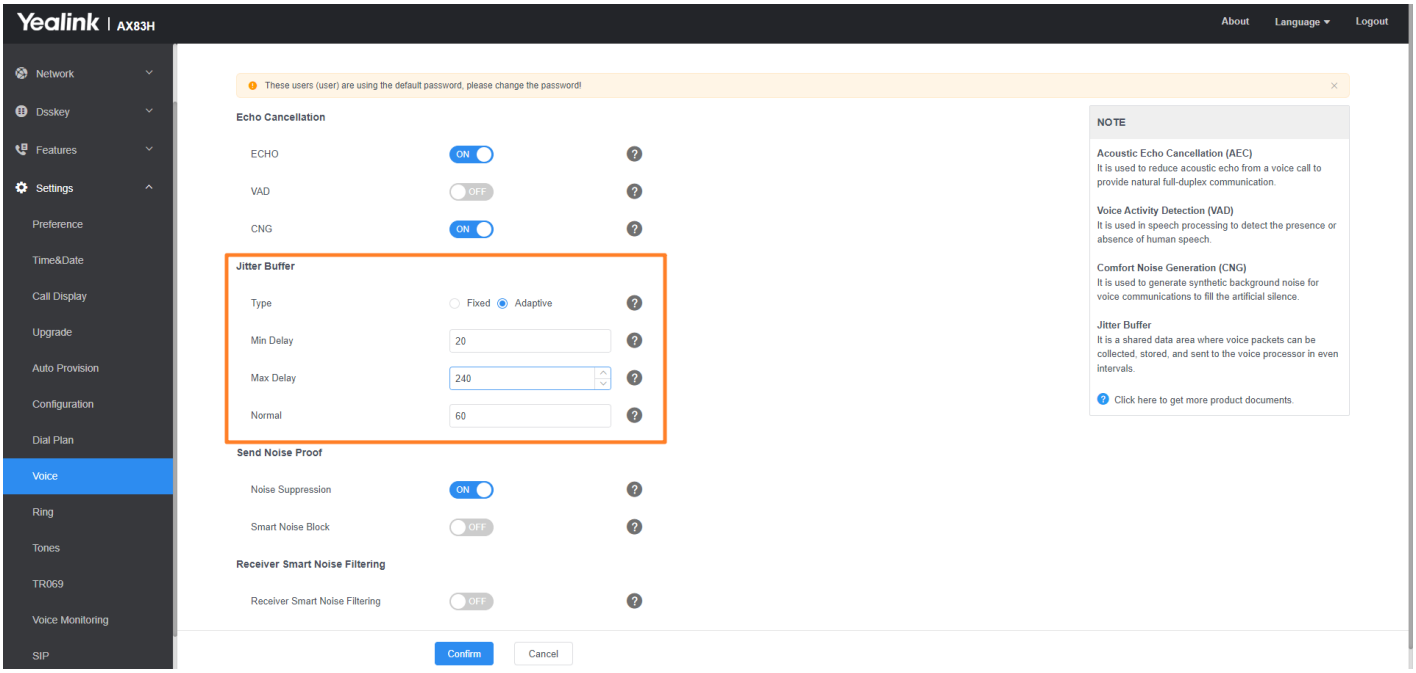
Yealink phones support two types of jitter buffers: **fixed** and **adaptive**. A fixed jitter buffer adds the fixed delay to voice packets. You can configure the delay time for the static jitter buffer on the phones. An adaptive jitter buffer is capable of adapting to the changes in the network's delay. The range of the delay time for the dynamic jitter buffer

added to packets can be also configured on the phones.

Jitter Buffer Configuration

Set via the Web User Interface

On the web user interface, go to **Settings** > **Voice** > **Jitter Buffer**.



Configuration Parameter

```
voice.jib.adaptive
voice.jib.min
voice.jib.max
voice.jib.normal
```

Parameter	Permitted Values	Default	Description
voice.jib.adaptive	**0**-Fixed **1**-Adaptive	1	It configures the type of jitter buffer in the wired network
voice.jib.min	Integer from 0 to 400	60	It configures the minimum delay time (in milliseconds) of the jitter buffer in the wired network. **NOTE** It works only if `voice.jib.adaptive` is set to 1 (Adaptive). The value of this parameter should be less than or equal to that of "voice.jib.normal".

voice.jib.max	Integer from 0 to 400	240	It configures the maximum delay time (in milliseconds) of the jitter buffer in the wired network. **NOTE** It works only if `voice.jib.adaptive` is set to 1 (Adaptive). The value of this parameter should be less than or equal to that of "voice.jib.normal".
voice.jib.normal	Integer from 0 to 400	120	It configures the normal delay time (in milliseconds) of the jitter buffer in the wired network. **NOTE** It works only if `voice.jib.adaptive` is set to 1 (Adaptive). The value of this parameter should be less than or equal to that of "voice.jib.normal".

DTMF

Introduction

DTMF (Dual Tone Multi-frequency) tone, better known as touch tone. DTMF is the signal sent from the IP phone to the network, which is generated when pressing the IP phone's keypad during a call. Each key pressed on the IP phone generates one sinusoidal tone of two frequencies. One is generated from a high-frequency group and the other from a low-frequency group.

DTMF Keypad

The DTMF keypad is laid out in a 4×4 matrix, with each row representing a low frequency, and each column representing a high frequency. Pressing a digit key (such as '1') will generate a sinusoidal tone for each of the two frequencies (697 and 1209 hertz (Hz)).

DTMF Keypad Frequencies:

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

NOTE

The phones will not send the DTMF sequence when the call is placed on hold or is held.

Transmit DTMF Digit

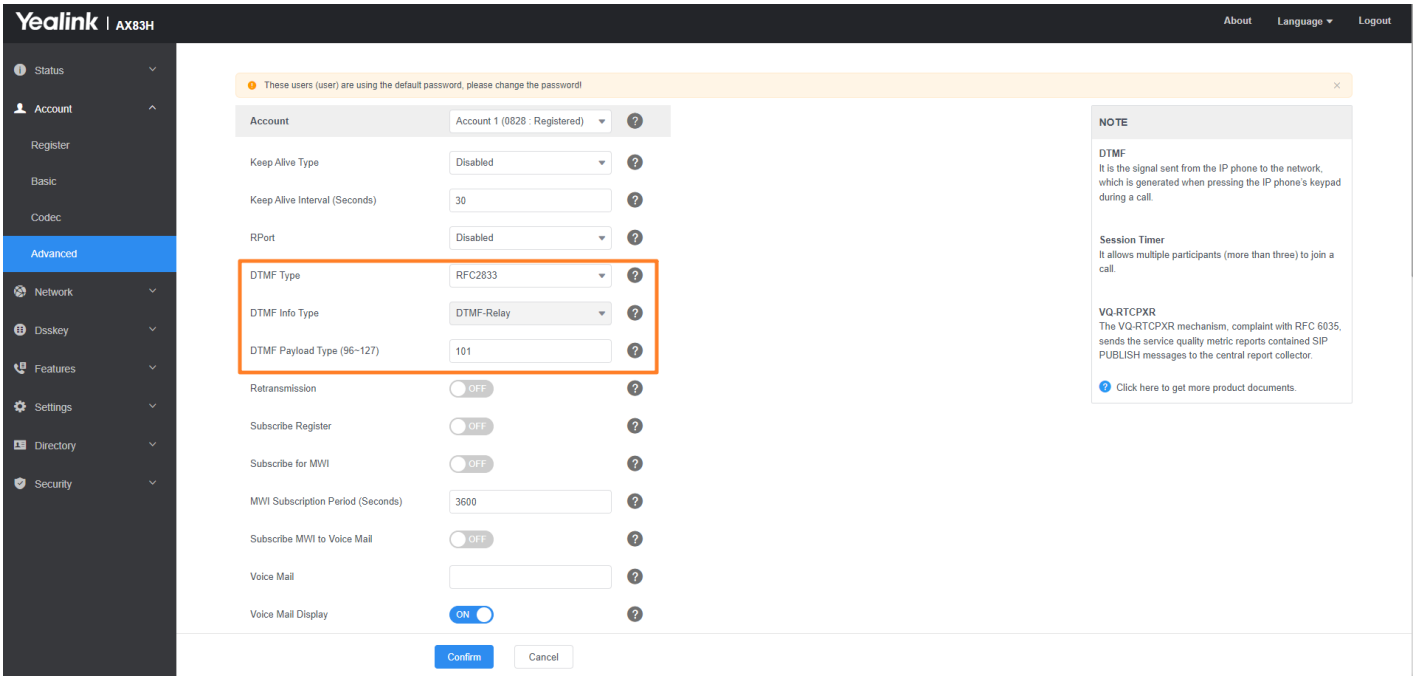
Three methods of transmitting DTMF digits on SIP calls:

- **RFC 2833** – DTMF digits are transmitted by RTP Events compliant with RFC 2833. You can configure the payload type and sending times of the end RTP Event packet. The RTP Event packet contains 4 bytes. The 4 bytes are distributed over several fields denoted as Event, End bit, R-bit, Volume, and Duration. If the End bit is set to 1, the packet contains the end of the DTMF event. You can configure the sending times of the end RTP Event packet.
- **INBAND** – DTMF digits are transmitted in the voice band. It uses the same codec as your voice and is audible to conversation partners.
- **SIP INFO** – DTMF digits are transmitted by SIP INFO messages. DTMF digits are transmitted by the SIP INFO messages when the voice stream is established after a successful SIP 200 OK-ACK message sequence. The SIP INFO message can transmit DTMF digits in three ways: DTMF, DTMF-Relay, and Telephone-Event.

Transmit DTMF Digit Configuration

Set via the Web User Interface

On the web user interface, go to **Account** > **Advanced** > **DTMF Type/DTMF Payload Type(96~127)/DTMF Info Type**.



Configuration Parameter

account.X.dtmf.type
account.X.dtmf.dtmf_payload
account.X.dtmf.info_type
features.dtmf.repetition
features.dtmf.duration
features.dtmf.volume

Parameter	Permitted Values	Default	Description
account.X.dtmf.type[1]	**0**-INBAND, DTMF digits are transmitted in the voice band. **1**-RFC2833, DTMF digits are transmitted by RTP Events compliant to RFC 2833. **2**-SIP INFO, DTMF digits are transmitted by the SIP INFO messages. **3**-RFC2833 + SIP INFO, DTMF digits are transmitted by RTP Events compliant to RFC 2833 and the SIP INFO messages.	1	It configures the DTMF type.
account.X.dtmf.dtmf_payload[1]	Integer from 96 to 127	101	It configures the value of DTMF payload. **NOTE** It works only if `account.X.dtmf.type` is set to 1 (RFC2833) or 3 (RFC2833 + SIP INFO).
account.X.dtmf.info_type[1]	**1**-DTMF-Relay **2**-DTMF **3**-Telephone-Event	1	It configures the DTMF info type. **NOTE** It works only if `account.X.dtmf.type` is set to 1 (RFC2833) or 3 (RFC2833 + SIP INFO).
features.dtmf.repetition	1, 2 or 3	3	It configures the repetition times for the phone to send the end RTP Event packet during an active call.

features.dtmf.duration [2]	Integer from 0 to 700	100	It configures the duration time (in milliseconds) for each digit when a sequence of DTMF tones is played out automatically. **NOTE** If the time interval between two DTMF digits is less than this value, two or more same DTMF digits could be identified as one DTMF digit. This may cause the loss of one or more DTMF digits. For example, 2662 may be identified as 262. If so, you can modify the value of this parameter to a little lower than the default value.
features.dtmf.volume	Integer from -33 to 0	-10	It configures the volume of the DTMF tone (in dB).

[1] X is the account ID.
[2]If you change this parameter, the phone will reboot to make the change take effect.

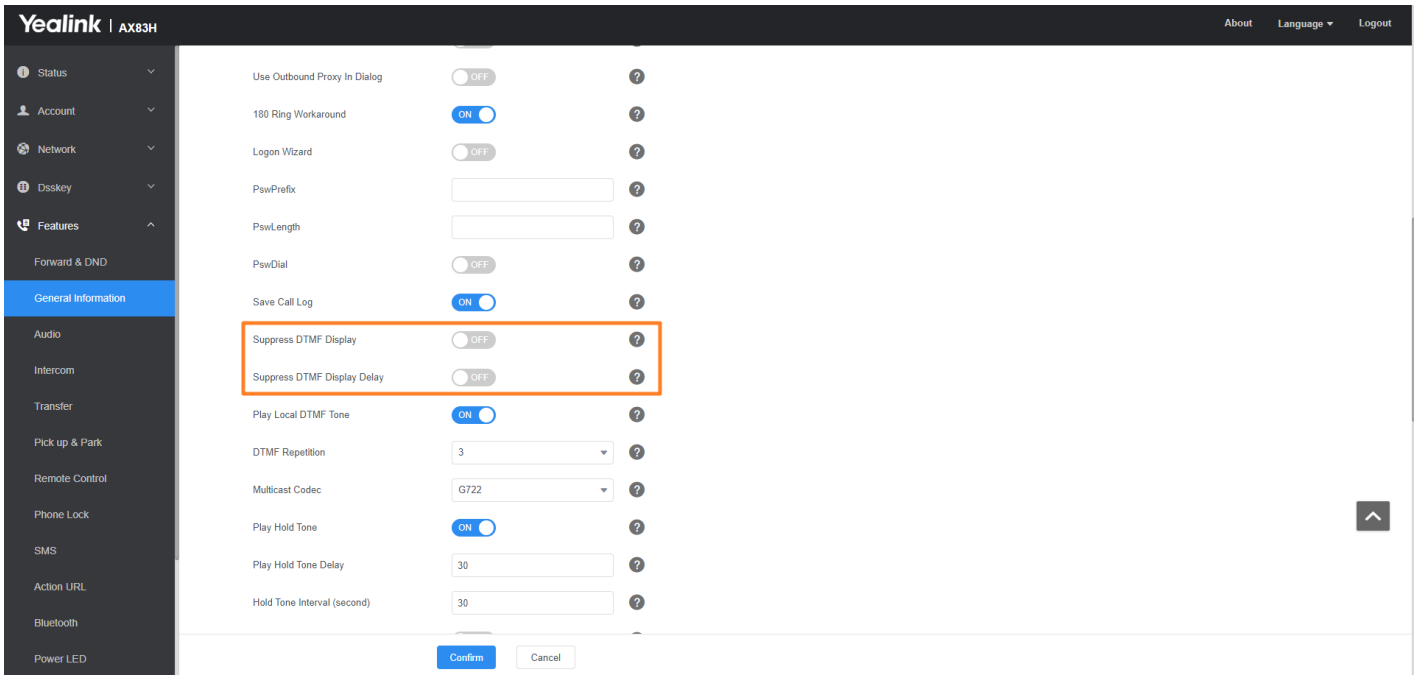
Suppress DTMF Display

Suppress DTMF display allows the phones to suppress the display of DTMF digits during an active call. DTMF digits are displayed as “*” on the phone screen. Suppress DTMF display delay defines whether to display the DTMF digits for a short period of time before displaying as “*”.

Suppress DTMF Display Configuration

Set via the Web User Interface

On the web user interface, go to **Features** > **General Information** > **Suppress DTMF Display/Suppress DTMF Display Delay**.



Configuration Parameter

```
features.dtmf.hide
features.dtmf.hide_delay
```

Parameter	Permitted Values	Default	Description
features.dtmf.hide	**0**-Disabled **1**-Enabled, the DTMF digits are displayed as asterisks.	0	It enables or disables the phone to suppress the display of DTMF digits during an active call.
features.dtmf.hide_delay	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to display the DTMF digits for a short period before displaying asterisks during an active call. **NOTE** It works only if `features.dtmf.hide` is set to 1 (Enabled).

Voice Quality Monitoring (VQM)

Introduction

Voice quality monitoring feature allows the phones to generate various quality metrics for listening quality and conversational quality. These metrics can be sent between the phones in RTCP-XR packets. These metrics can also be sent in SIP PUBLISH messages to a central voice quality report collector. Yealink phones support two

mechanisms for voice quality monitoring: **RTCP-XR** and **VQ-RTCPXR**.

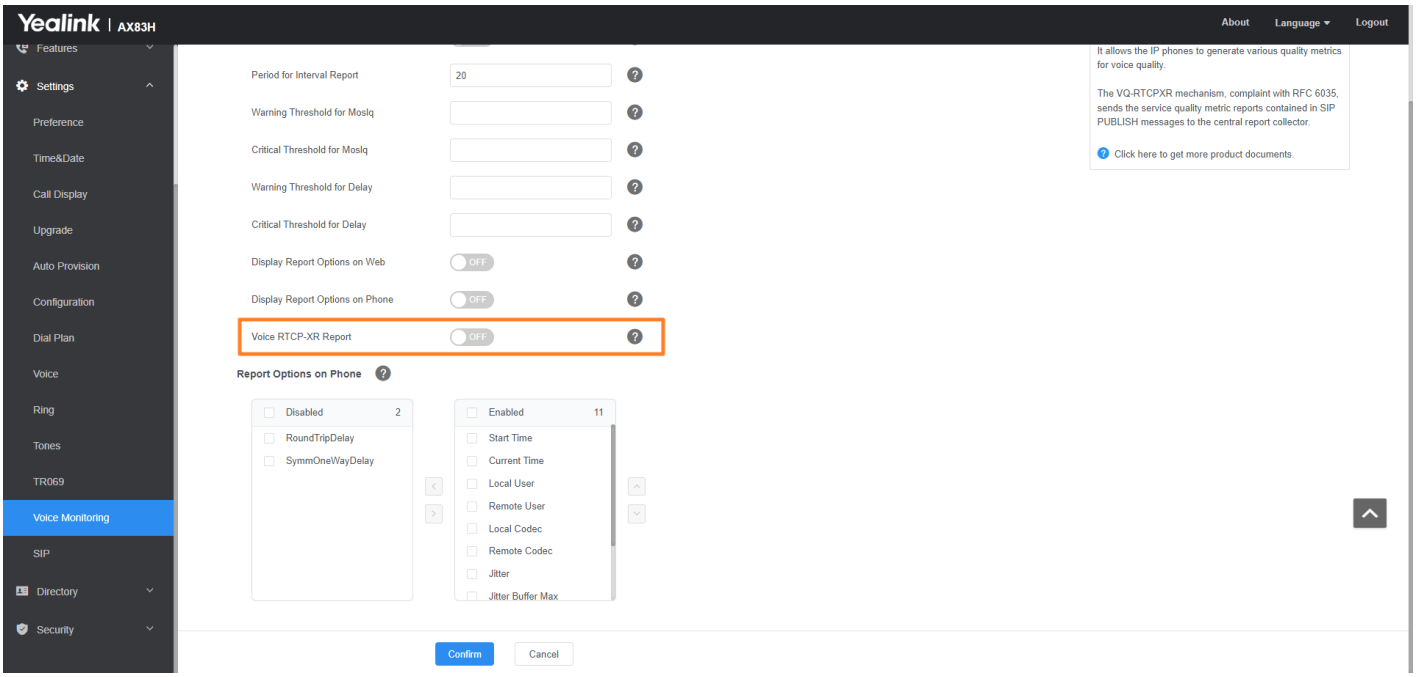
RTCP-XR

The RTCP-XR mechanism, compliant with RFC 3611-RTP ControExtended Reports (RTCP XR) , provides the metrics contained in RTCP-XR packets for monitoring the quality of calls. These metrics include network packet loss, delay metrics, analog metrics, and voice quality metrics.

RTCP-XR Configuration

Set via the Web User Interface

On the web user interface, go to **Settings** > **Voice Monitoring** > **Voice RTCP-XR Report**.



Configuration Parameter

```
voice.rtcp_xr.enable
voice.rtcp.enable
voice.rtcp_cname
```

Parameter	Permitted Values	Default	Description
voice.rtcp_xr.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to send RTCP-XR packets.
voice.rtcp.enable[1]	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to send RTCP packets.
voice.rtcp_cname[1]	String	Blank	It configures the cname of the RTCP packets.

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

VQ-RTCPXR

The VQ-RTCPXR mechanism, compliant with RFC 6035, sends the service quality metric reports contained in SIP PUBLISH messages to the central report collector.

A wide range of performance metrics are generated in the following three ways:

- Based on current values, such as jitter, jitter buffer max, and round trip delay.
- Covers the time period from the beginning of the call until the report is sent, such as network packet loss.
- Computed using other metrics as input, such as listening Mean Opinion Score (MOS-LQ) and conversationaMean Opinion Score (MOS-CQ).

Voice Quality Reports

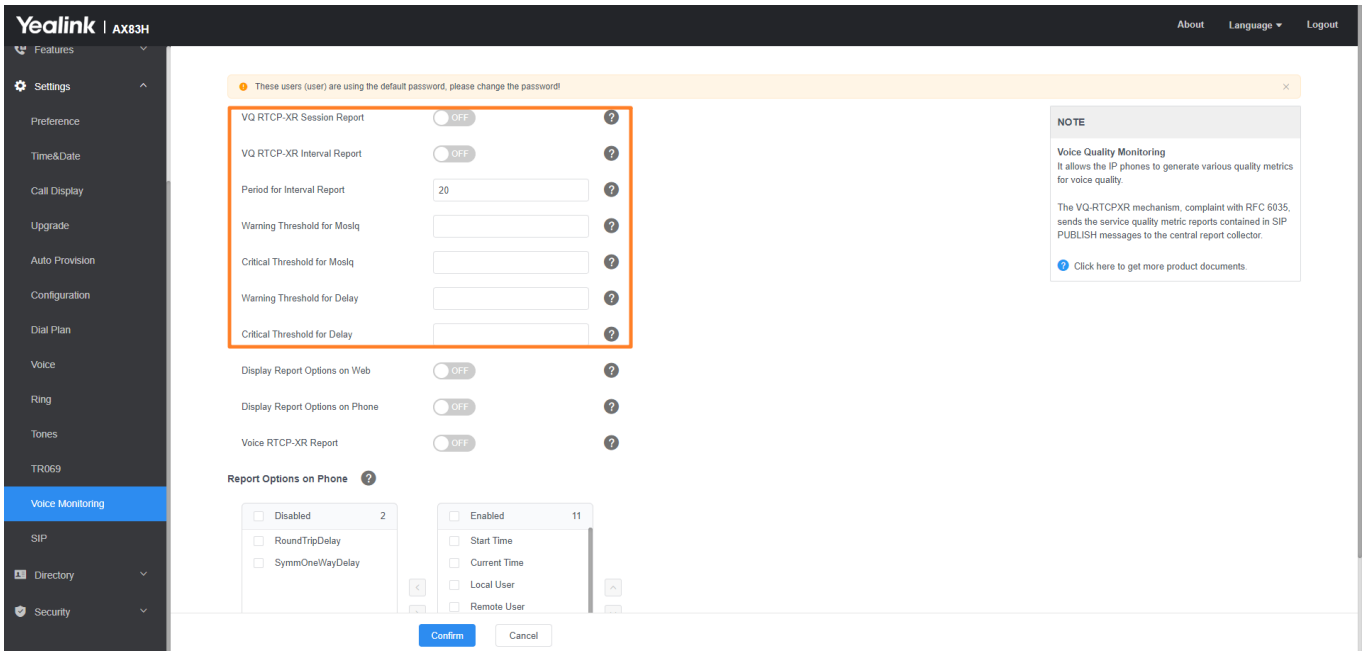
Three types of quality reports can be enabled:

- **Session**: Generated at the end of a call.
- **Interval**: Generated during a cal lat a configurable period.
- **Alert**: Generated when the call quality degrades below a configurable threshold.

Voice Quality Reports Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Voice Monitoring** > **VQ RTCP-XR Session Report/VQ RTCP-XR Interval Report/Period for Interval Report/Warning Threshold for Moslq/Critical Threshold for Moslq/Warning Threshold for Delay/Critical Threshold for Delay**.



Configuration Parameter

```
phone_setting.vq_rtcpxr.session_report.enable
phone_setting.vq_rtcpxr.interval_report.enable
phone_setting.vq_rtcpxr_interval_period
phone_setting.vq_rtcpxr_moslq_threshold_warning
phone_setting.vq_rtcpxr_moslq_threshold_critical
phone_setting.vq_rtcpxr_delay_threshold_warning
phone_setting.vq_rtcpxr_delay_threshold_critical
```

Parameter	Permitted Values	Default	Description
phone_setting.vq_rtcpxr.session_report.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to send a session quality report to the central report collector at the end of each call.
phone_setting.vq_rtcpxr.interval_report.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to send an interval quality report to the central report collector periodically throughout a call.
phone_setting.vq_rtcpxr_interval_period	Integer from 5 to 20	20	It configures the interval (in seconds) for the phone to send an interval quality report to the central report collector periodically throughout a call. **NOTE** It works only if `phone_setting.vq_rtcpxr.interval_report.enable` is set to 1 (Enabled).
phone_setting.vq_rtcpxr_moslq_threshold_warning	Integer from 15 to 40	Blank	It configures the threshold value of the listening MOS score (MOS-LQ) multiplied by 10. The threshold value of MOS-LQ causes the phone to send a warning alert quality report to the central report collector. For example, a configured value of 35 corresponds to the MOS score 3.5. When the MOS-LQ value computed by the phone is less than or equal to 3.5, the phone will send a warning alert quality report to the central report collector. When the MOS-LQ value computed by the phone is greater than 3.5, the phone will not send a warning alert quality report to the central report collector. If it is set to blank, warning alerts are not generated due to MOS-LQ.

phone_setting.vq_rtcpxr_moslq_threshold_critical	Integer from 15 to 40	Blank	It configures the threshold value of the listening MOS score (MOS-LQ) multiplied by 10. The threshold value of MOS-LQ causes the phone to send a critical alert quality report to the central report collector. For example, a configured value of 28 corresponds to the MOS score 2.8. When the MOS-LQ value computed by the phone is less than or equal to 2.8, the phone will send a critical alert quality report to the central report collector. When the MOS-LQ value computed by the phone is greater than 2.8, the phone will not send a critical alert quality report to the central report collector. If it is set to blank, critical alerts are not generated due to MOS-LQ.
phone_setting.vq_rtcpxr_delay_threshold_warning	10 to 2000	Blank	It configures the threshold value of one-way delay (in milliseconds) that causes the phone to send a warning alert quality report to the central report collector. For example, if it is set to 500, when the value of one way delay computed by the phone is greater than or equal to 500, the phone will send a warning alert quality report to the central report collector; when the value of one way delay computed by the phone is less than 500, the phone will not send a warning alert quality report to the central report collector. If it is set to blank, warning alerts are not generated due to one-way delay. The one-way delay includes both network delay and end system delay.
phone_setting.vq_rtcpxr_delay_threshold_critical	10 to 2000	Blank	It configures the threshold value of one-way delay (in milliseconds) that causes the phone to send a critical alert quality report to the central report collector. For example, if it is set to 500, when the value of one-way delay computed by the phone is greater than or equal to 500, the phone will send a critical alert quality report to the central report collector; when the value of one way delay computed by the phone is less than 500, the phone will not send a critical alert quality report to the central report collector. If it is set to blank, critical alerts are not generated due to one-way delay. The one-way delay includes both network delay and end system delay.

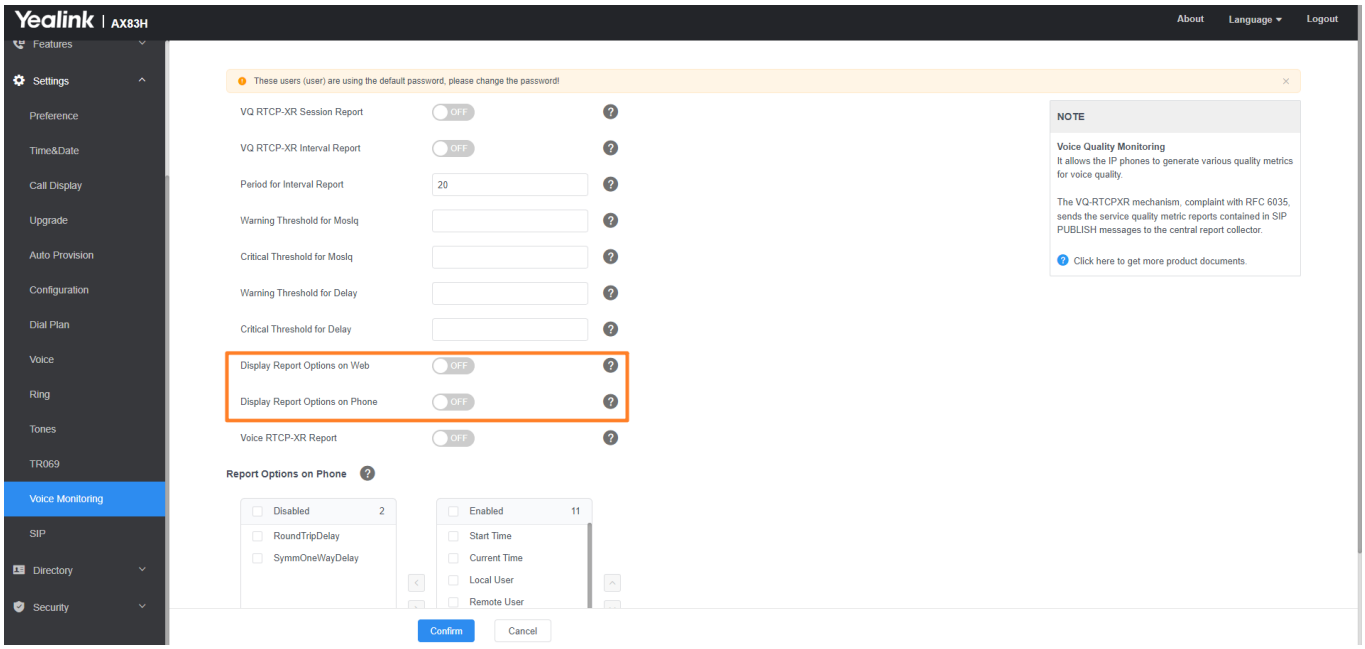
VQ-RTCPXR Display

You can check the voice quality data of the last call via the web user interface.

VQ-RTCPXR Display Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Voice Monitoring** > **Display Report Options on Web**.



Configuration Parameter

```
phone_setting.vq_rtcpxr.states_show_on_web.enable
phone_setting.vq_rtcpxr.states_show_on_gui.enable
```

Parameter	Permitted Values	Default	Description
phone_setting.vq_rtcpxr.states_show_on_web.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the voice quality data of the last call to be displayed on the web interface at the path **Status** > **RTP Status**.
phone_setting.vq_rtcpxr.states_show_on_gui.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the voice quality data of the last call or current call to be displayed on the phone screen. You can view the voice quality data of the last call on the phone at the path **Menu** > **Status** >**More** > **RTP (RTP Status)**. You can view the voice quality data of the current call by pressing RTP/RTP Status soft key during a call.

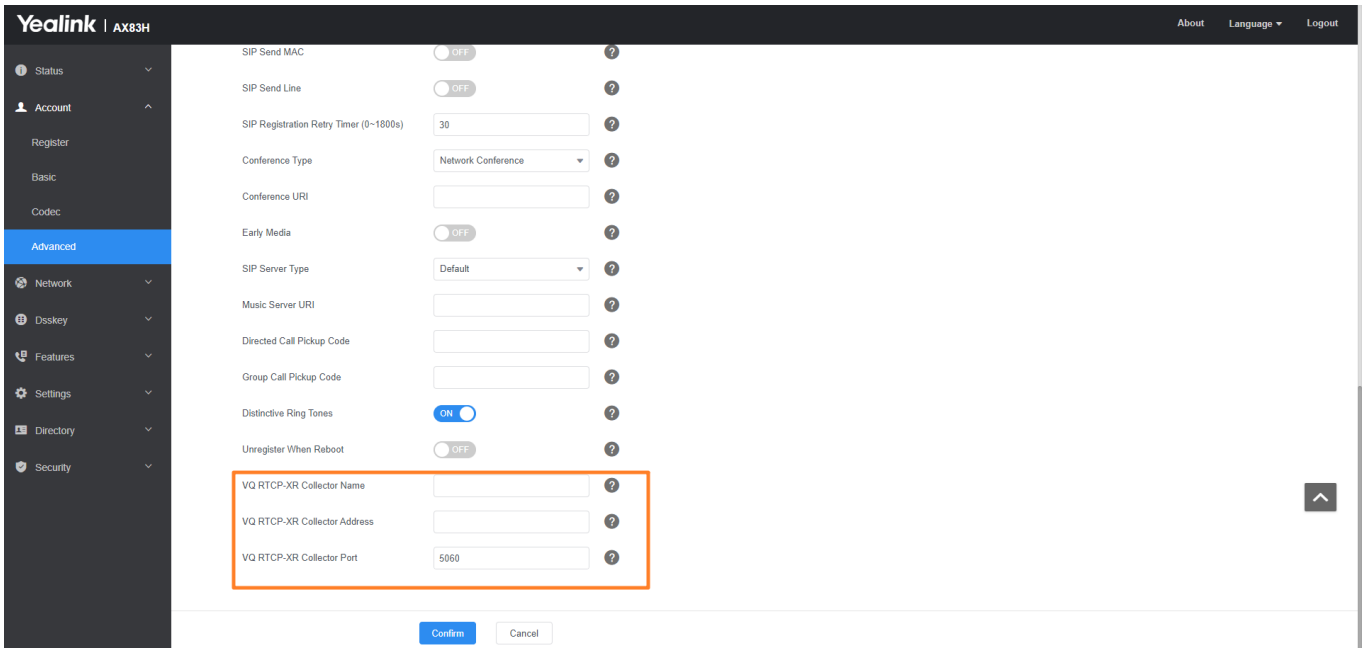
Central Report Collector

To operate with the central report collector, the phones must be configured to forward their voice quality reports to the specified report collector. You can specify the report collector on a per-line basis.

Central Report Collector Configuration

Set via the Web User Interface

1. On the web user interface, go to **Account** > **Advanced** > **VQ RTCP-XR Collector Name/VQ RTCP-XR Collector Address/VQ RTCP-XR Collector Port**.



Configuration Parameter

```
account.X.vq_rtcpxr.collector_name
account.X.vq_rtcpxr.collector_server_host
account.X.vq_rtcpxr.collector_server_port
```

Parameter	Permitted Values	Default	Description
account.X.vq_rtcpxr.collector_name[1]	String within 32 characters	Blank	It configures the hostname of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.
account.X.vq_rtcpxr.collector_server_host[1]	IPv4 Address/FQDN	Blank	It configures the IP address of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.
account.X.vq_rtcpxr.collector_server_port[1]	Integer from 0 to 65535	5060	It configures the port of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.

> [1]X is the account ID

Ring Tones

Ring Tones

Ring tones are used to play for incoming calls. You can select a built-in ringtone or a custom ringtone for the phone

system or specific line registration. To set the custom ring tones, you need to upload the custom ring tones to the IP phone in advance.
You can also specify a period after which the phone will stop ringing if the call is not answered.

Custom Ringtone Limit

The ringtone format must meet the following:

Phone Model	Format	Single File Size
Phones	.wav	<=8MB

NOTE
The ring tone file must be in PCMU/PCMA audio format, mono channel, 8K sample rate, and 16-bit resolution.

Ringtone Configuration

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

Configuration Parameter

```
phone_setting.ring_type
account.X.ringtone.ring_type
pstn.account.X.ring_type
ringtone.url
ringtone.delete
phone_setting.ringing_timeout
phone_setting.ring_for_tranfailed
```

Parameter	Description	Permitted Values	Default
phone_setting.ring_type	It configures a ring tone for the phone.	Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (for example, Custom ring.wav) For T3 phones: Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Silent.wav, Splash.wav or custom ring tone name (for example, Customring.wav)	Ring1.wav

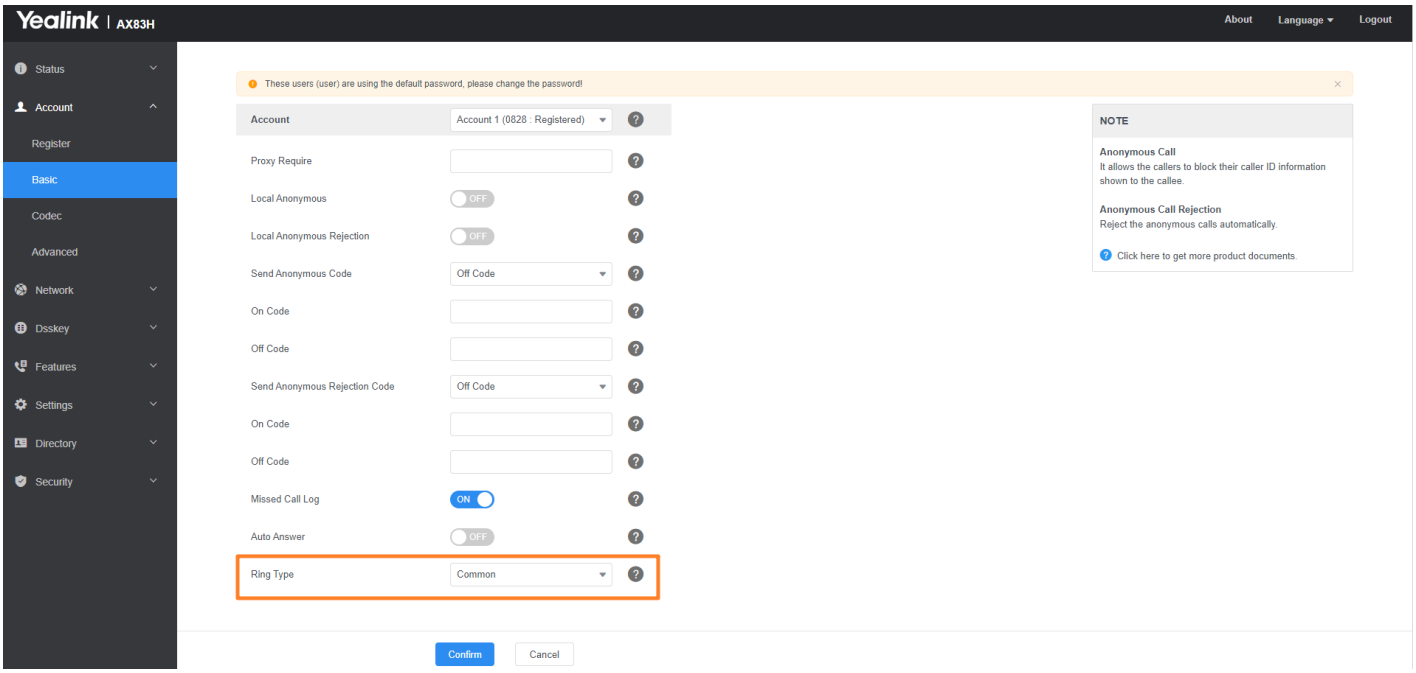
account.X.ringtone.ring_type[1]	It configures a ring tone. Example: account.1.ringtone.ring_type = Ring3.wav It means configuring Ring3.wav for account1. account.1.ringtone.ring_type = Common It means account1 will use the ring tone selected for the phone configured by the parameter "phone_setting.ring_type".	Common, Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (for example, Custom ring.wav) For T3 phones: Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Silent.wav, Splash.wav or custom ring tone name (for example, Customring.wav)	Common
pstn.account.X.ring_type[2]	It configures a ring tone for PSTN account X. Example: pstn.account.1.ring_type = Ring3.wav It means PSTN account 1 will use the Ring3.wav as the ring tone. pstn.account.1.ring_type = Common It means PSTN account 1 will use the ring tone selected for the IP phone configured by the parameter “phone_setting.ring_type”.	Common, Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (for example, Customring.wav)	Common
ringtone.url	It configures the access URL of the custom ringtone file.	URL within 511 characters	Blank
ringtone.delete	It deletes all custom ringtone files.	http://localhost/all	Blank
phone_setting.ringing_timeout	It configures the duration time (in seconds) in the ringing state. If it is set to 180, the phone will stop ringing if the call is not answered within 180 seconds.	Integer from 1 to 3600	120
phone_setting.ring_for_tranfailed	It configures the ring tone when the phone fails to transfer a call and displays "Transfer failed" on the screen.	Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav or Splash.wav For T3 phones: Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Silent.wav, Splash.wav	Ring1.wav

> [1]X is the account ID.

> [2]X is the PSTN account ID. X=1-2.

Set via the Web User Interface

On the web user interface, go to: **Account** > **Basic** > **Ring Type**



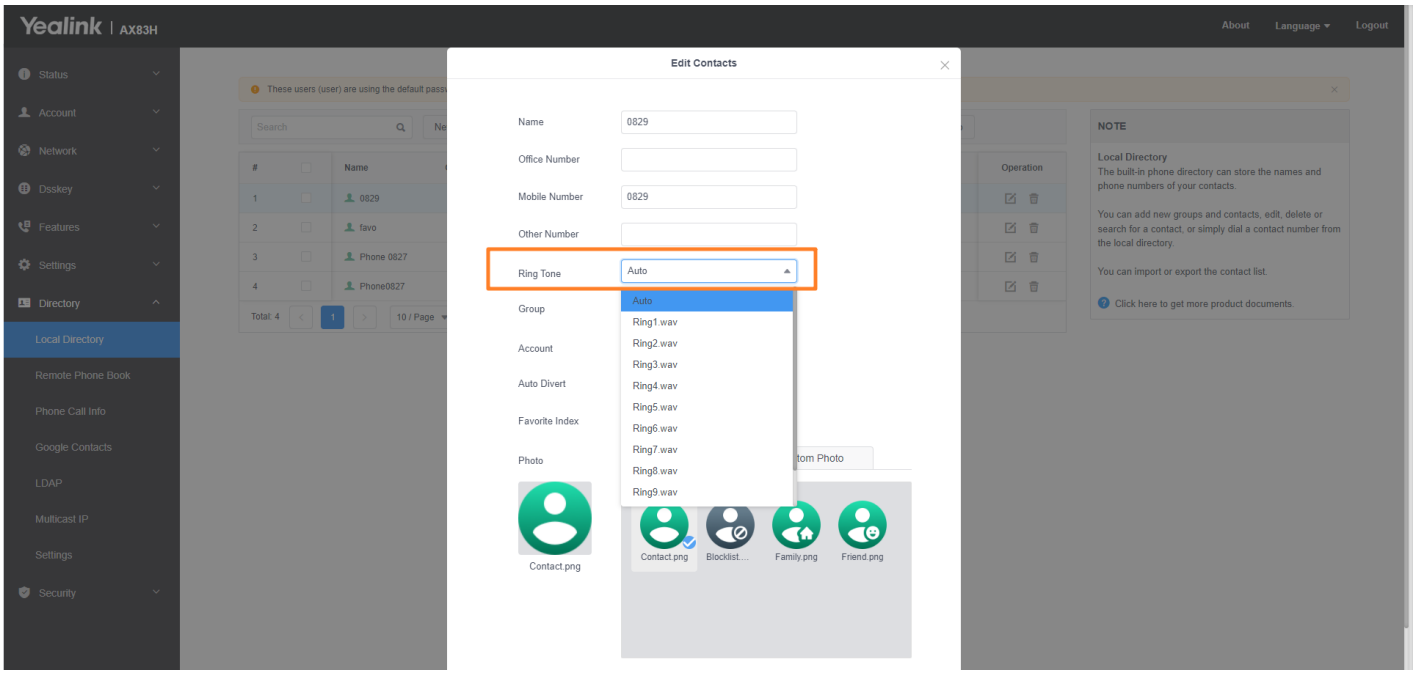
FAQ

The priority of ringtone.

There are several ringtone settings in the phone, the priority from high to low shown below.
You can change the ringtone according to the priority.

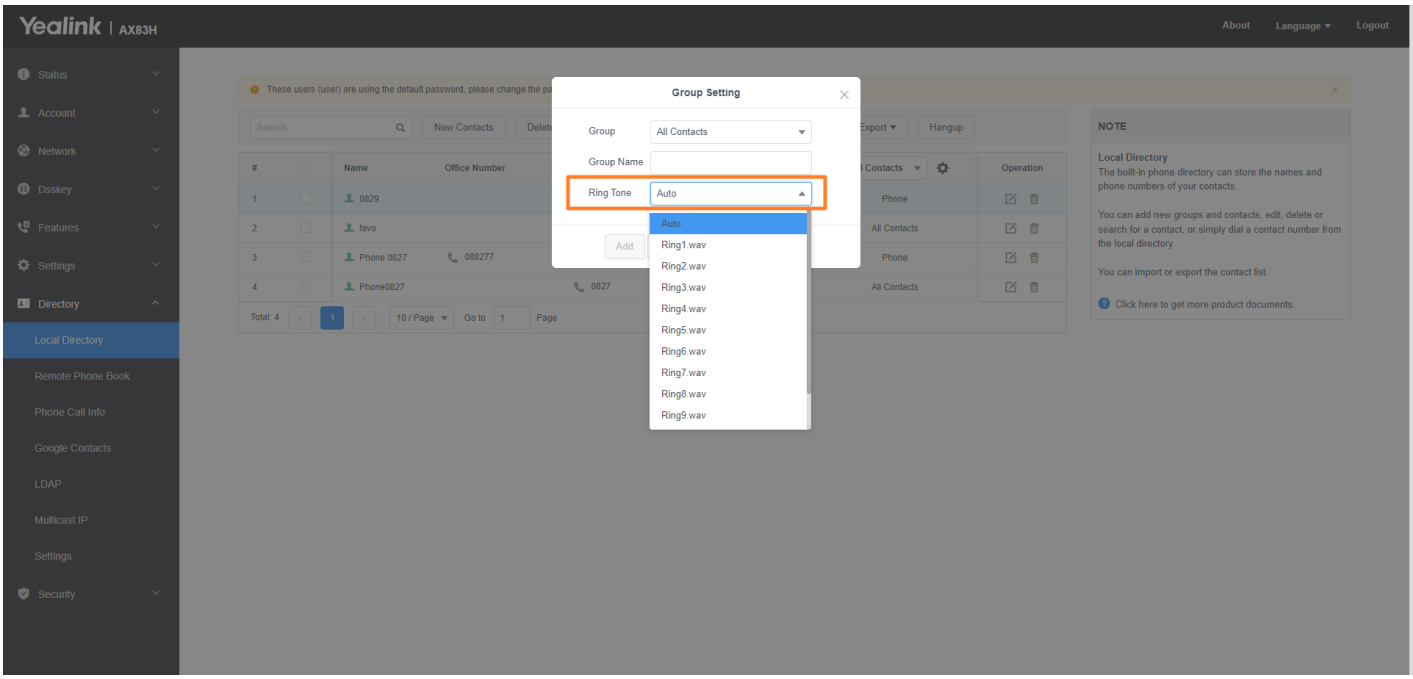
1. Contact Ringtone

On the web user interface, go to **Directory** > **Local Directory** >  > Ring Tone.



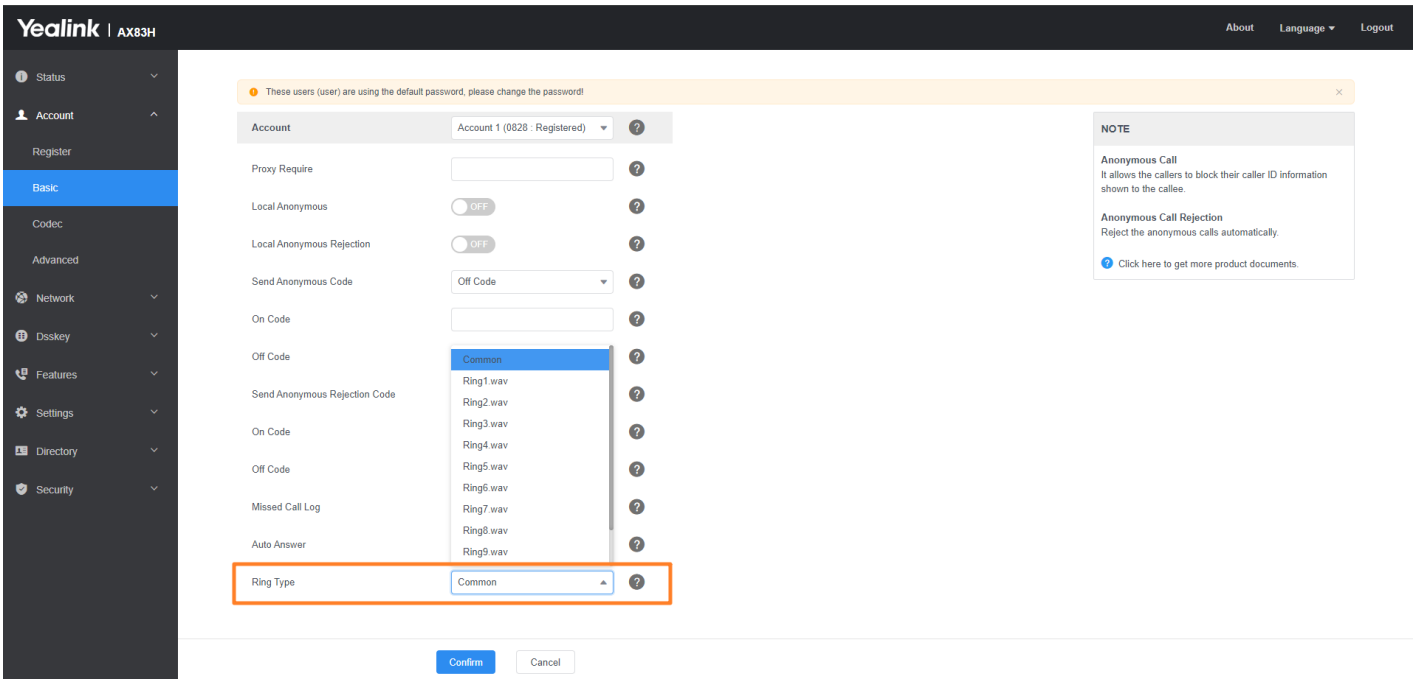
2. Group Ringtone

On the web user interface, go to **Directory** > **Local Directory** > > Group Setting.



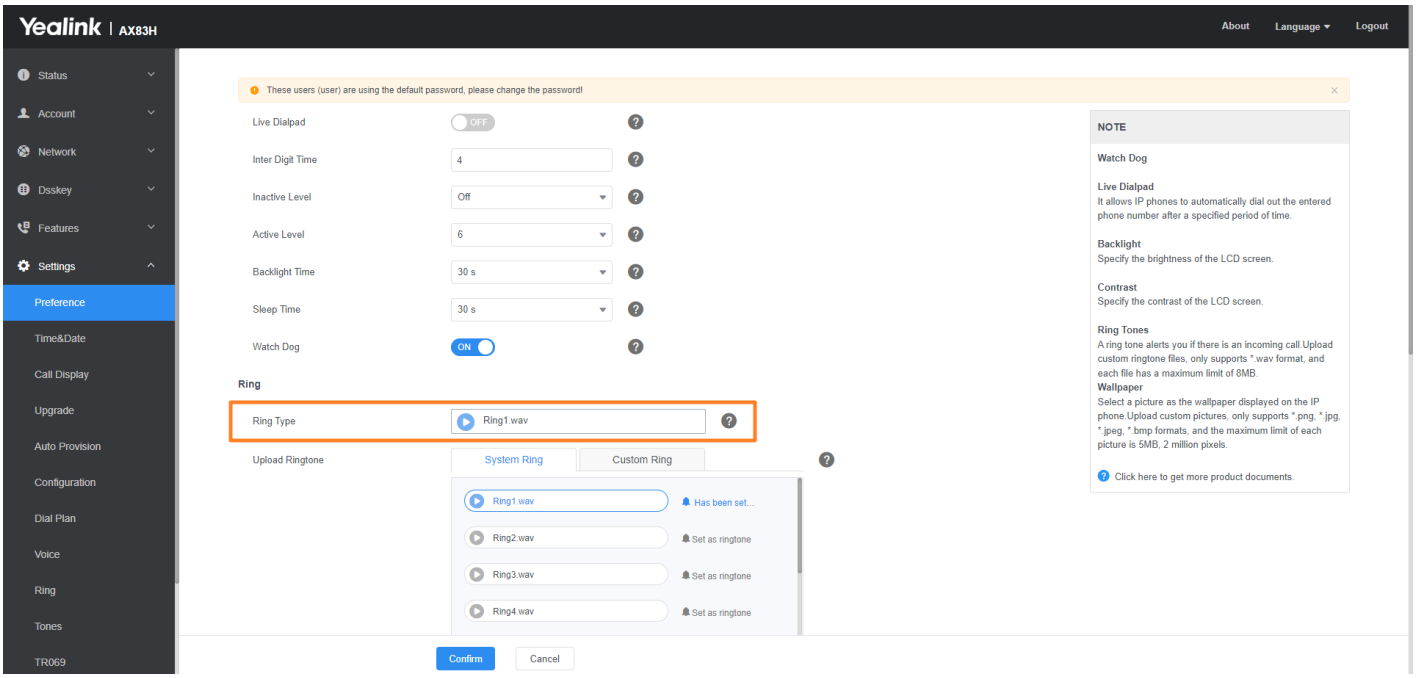
3. Account Ringtone

On the web user interface, go to **Account** > **Basic** > **Ring Type**.



4. Default Ringtone

On the web user interface, go to **Settings** > **Preference** > **Ring Type**.



Smart Noise Filtering

Smart Noise Filtering

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).

Smart Noise Filtering Configuration

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

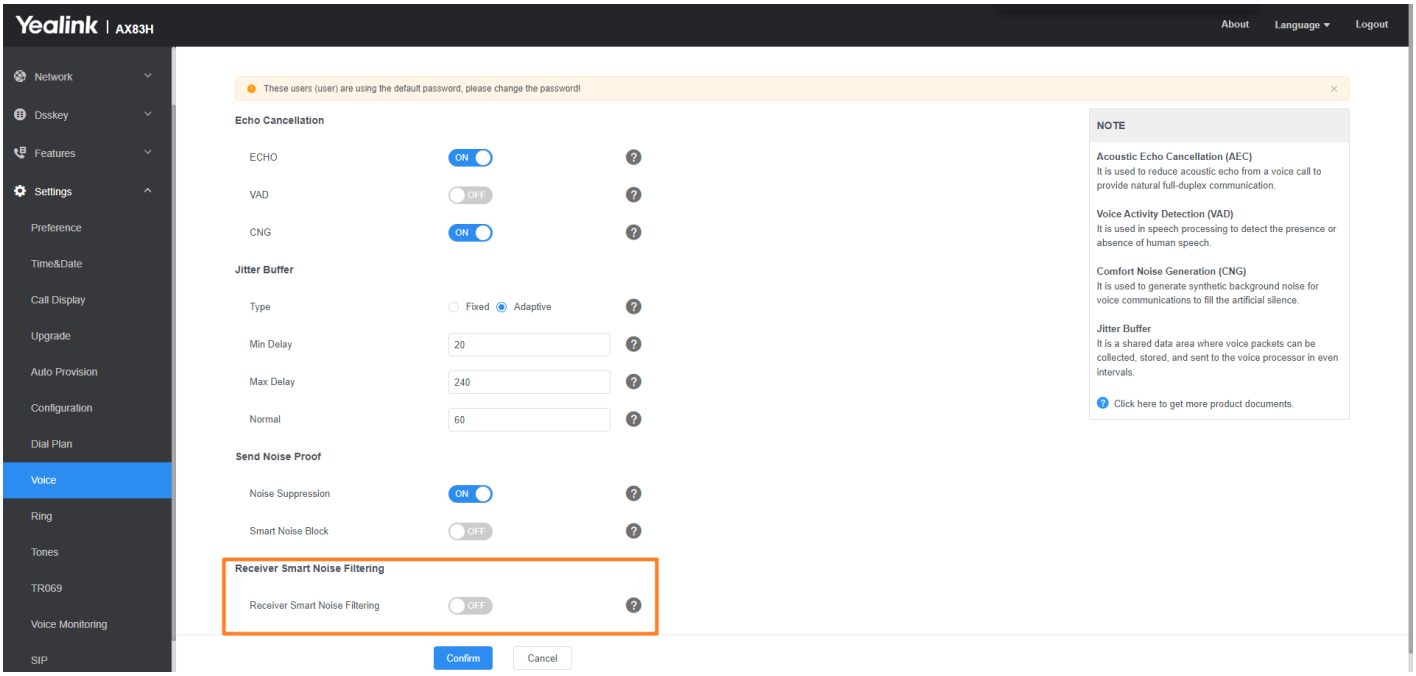
Configuration Parameter

```
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. Note: After smart noise filtering is enabled, if the far end is playing music or calling a voice service, the background music will also be eliminated when there is no speech in a call.	0-Disabled 1-Enabled	0

Set via the Web User Interface

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



Call Features

Dial Plan

Introduction

Dial plan is a string of characters that governs the way how the phones process the inputs received from the IP phone’ s keypads. You can use the regular expression to define the dial plan.

Yealink phones support four patterns:

Pattern	Description
Replace rule	an alternative string that replaces the numbers entered by the user. Yealink phones support up to 100 replace rules.
Dial now	a string used to match numbers entered by the user. When entered numbers match the predefined dial now rule, the phone will automatically dial out the numbers without pressing the send key. Yealink phones support up to 20 dial now rules.
Area code	also known as Numbering Plan Areas (NPAs). They usually indicate geographical areas in one country. When entered numbers match the predefined area code rule, the phone will automatically add the area code before the numbers when dialing them. Yealink phones only support 1 area code rule.
Block out	prevents users from dialing out specific numbers. When entered numbers match the predefined block-out rule, the phone screen prompts "Forbidden Number". Yealink phones support up to 10 block-out rules.

NOTE
You can configure these four patterns via the web user interface or auto-provisioning. For replace rule and dial now, you can select to add the rule one by one or use the template file to add multiple rules at a time.

Basic Regular Expression Syntax for Four Patterns

You need to know the following basic regular expression syntax when creating a dial plan:

Regular Expression	Description
.	The dot "." can be used as a placeholder or multiple placeholders for any string. **Example**: "12." would match "123", "1234", "12345", "12abc", and so on.
x	The "x" can be used as a placeholder for any character. **Example**: "12x" would match "121", "122", "123", "12a", and so on.
-	The dash "-" can be used to match a range of characters within the brackets. **Example**: "[5-7]" would match the number "5", "6" or "7".
,	The comma "," can be used as a separator within the bracket. **Example**: "[2,5,8]" would match the number "2", "5" or "8".
[]	The square bracket "[]" can be used as a placeholder for a single character that matches any of a set of characters. **Example**: "91[5-7]1234"would match "9151234", "9161234", "9171234".
()	The parenthesis "( )" can be used to group together patterns, for instance, to logically combine two or more patterns. **Example**: "([1-9])([2-7])3" would match "923", "153", "673", and so on.

$	The "$" followed by the sequence number of a parenthesis means the characters placed in the parenthesis. The sequence number stands for the corresponding parenthesis. **Example**: A replace rule configuration, Prefix: "001(xxx)45(xx)", Replace: "9001$1$452". When you dial out "0012354599" on your phone, the phone will replace the number with "90012354599". "$1" means 3 digits in the first parenthesis, that is, "235". "$2" means 2 digits in the second parenthesis, that is, "99".

Replace Rule File Customization

The replace rule file helps create multiple replace rules. At most 100 replace rules can be added to the IP phone. You can ask the distributor or Yealink FAE for the replacement rule file template. You can also refer to the following template:

```
<?xml version="1.0" encoding="UTF-8"?>
<dialrule>
<Data Prefix="2512" Replace="05922512" LineID="1"/>
</dialrule>
```

Replace Rule File Attributes

The following table lists the attributes you can use to add replace rules to the replace rule file:

Attributes	Description
Prefix	Specify the number to be replaced.
Replace	Specify the alternate string instead of what the user enters.
LineID	Specify a registered line to apply the replace rule. Valid Values: **0-10** **0** stands for all lines; **1-10** stand for line1-line10 Multiple line IDs are separated by commas.

Customize the Replace Rule File

1. Open the replace rule file.
2. To add a replace rule, add `<Data Prefix="" Replace="" LineID=""/>` to the file. Each starts on a new line.
3. Specify the values within double quotes.
   For example,
   `<Data Prefix="2512" Replace="05922512" LineID="1"/>`
4. Save the changes and place this file on the provisioning server.

Dial Now File Customization

The dial now file helps create multiple dial now rules. At most 20 dial-now rules can be added to the IP phone.

You can ask the distributor or Yealink FAE for the dial now file template. You can also refer to the following template:

```
<?xml version="1.0" encoding="UTF-8"?>
<dialnow>
<Data DialNowRule="1001" LineID="0" />
</dialnow>
```

Dial Now File Attributes

The following table lists the attributes you can use to add dial-now rules to the dial-now file:

Attributes	Description
DialNowRule	Specify the dial-now number.
LineID	Specify a registered line to apply the replace rule. Valid Values: **0-10** **0** stands for all lines; **1-10** stand for line1-line10 Multiple line IDs are separated by commas.

Customize the Dial Now File

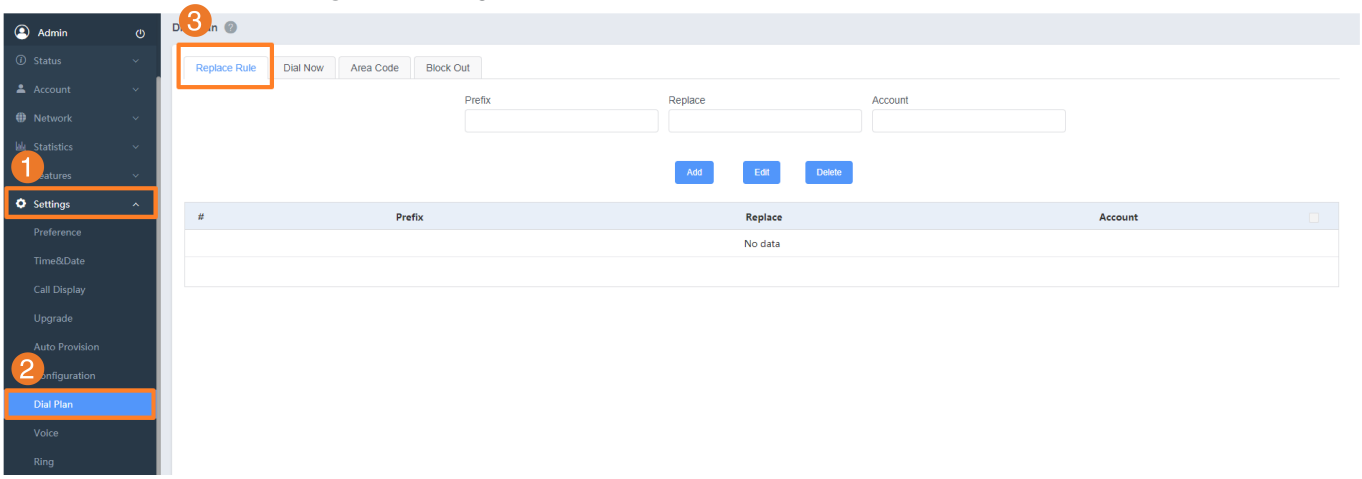
1. Open the dial now file.
2. To add a dial-now rule, add `<Data DialNowRule="" LineID="" />` to the file. Each starts on a new line.
3. Specify the values within double quotes.
   For example,
   `<Data DialNowRule="1001" LineID="0" />`
4. Save the changes and place this file to the provisioning server.

Replace Rule Configuration

You can configure replace rules either one by one or in batch using a replace rule template.

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Dial Plan** > **Replace Rule**.



Configuration Parameter

```
dialplan.replace.prefix.X
dialplan.replace.replace.X
dialplan.replace.line_id.X
dialplan_replace_rule.url
```

Parameter	Permitted Values	Default	Description
dialplan.replace.prefix.X[1]	String within 32 characters	Blank	It configures the entered number to be replaced.
dialplan.replace.replace.X[1]	String within 32 characters	Blank	It configures the alternate number to replace the entered number. The entered number is configured by `dialplan.replace.prefix.X`.
dialplan.replace.line_id.X[1]	0 to 250	Blank	It configures the desired line to apply the replace rule. The digit 0 stands for all lines. If it is left blank, the replace rule will apply to all lines on the phone. **NOTE** Multiple line IDs are separated by commas.
dialplan_replace_rule.url	URL within 511 characters	Blank	It configures the access URL of the replace rule template file. For customizing replace rule template file, refer to Replace Rule File Customization.

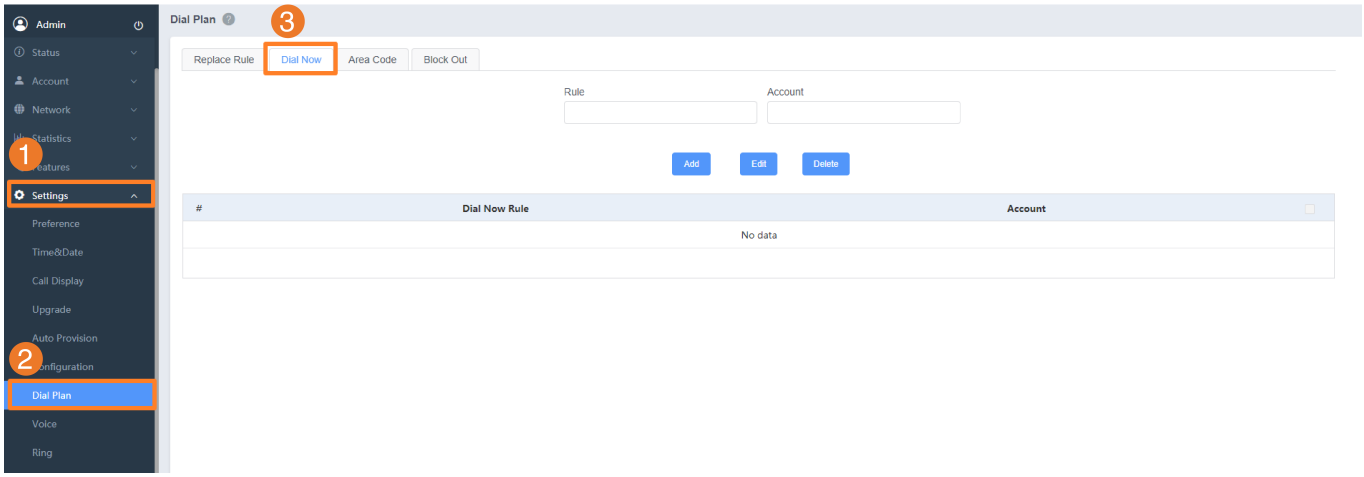
[1] 0-99

Dial Now Configuration

You can configure dial now rules either one by one or in batches using a dial now template.

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Dial Plan** > **Dial Now**.



Configuration Parameter

```
dialplan.dialnow.rule.X
dialplan.dialnow.line_id.X
phone_setting.dialnow_delay
dialplan_dialnow.url
```

Parameter	Permitted Values	Default	Description
dialplan.dialnow.rule.X[1]	String within 511 characters	Blank	It configures the dial now rule (the string used to match the numbers entered by the user). When entered numbers match the predefined dial now rule, the phone will automatically dial out the numbers without pressing the send key. **Example:** `dialplan.dialnow.rule.1 = 123`
dialplan.dialnow.line_id.X[1]	0 to 10	Blank	It configures the desired line to apply the dial now rule. The digit 0 stands for all lines. If it is left blank, the dial-now rule will apply to all lines on the phone. **NOTE** Multiple line IDs are separated by commas.

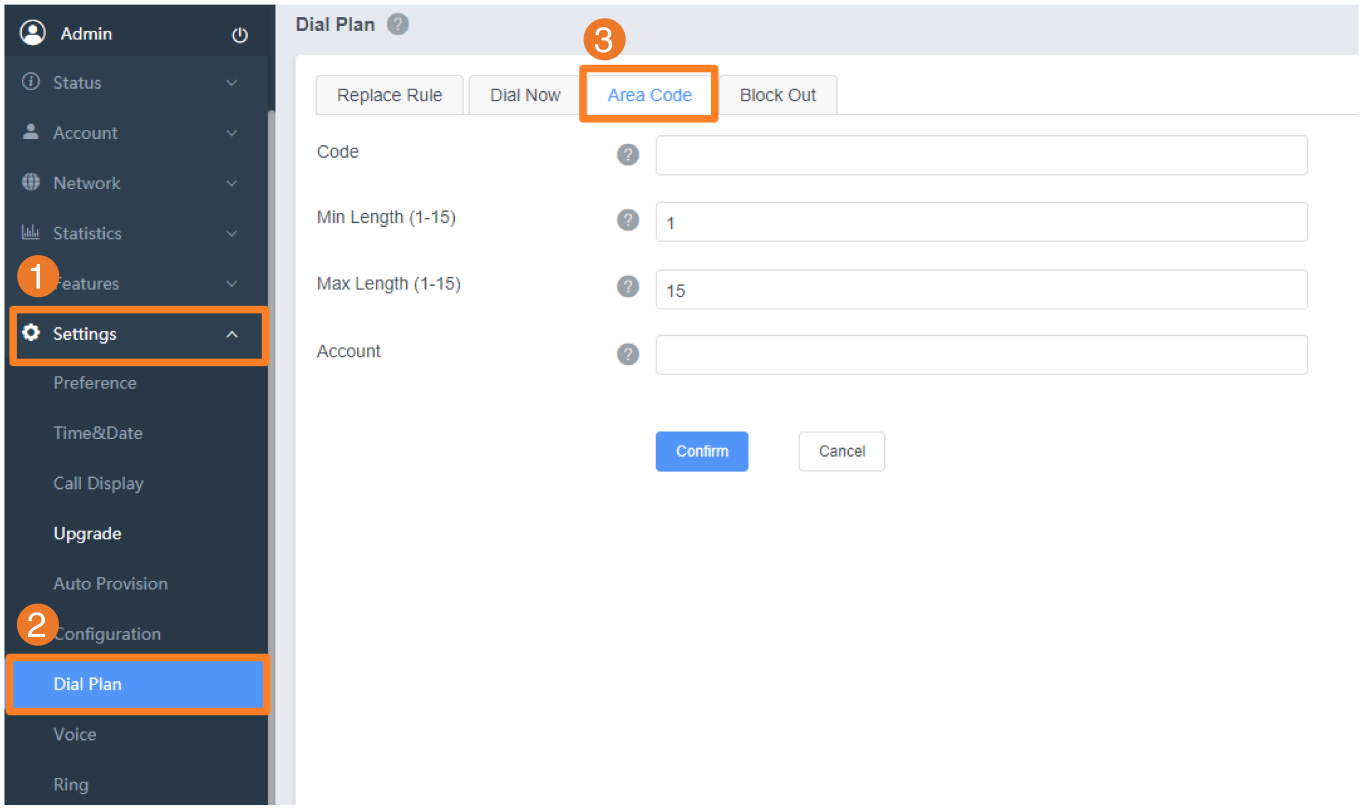
phone_setting.dialnow_delay	Integer from 0 to 14	1	It configures the delay time (in seconds) for the dial now rule. When entered numbers match the predefined dial now rule, the phone will automatically dial out the entered number after the designated delay time. If it is set to 0, the phone will automatically dial out the entered number immediately.
dialplan_dialnow.url	String within 511 characters	Blank	It configures the access URL of the dial now template file. For customizing dial now template file, refer to Dial Now File Customization.

[1] X is from 1 to 20.

Area Code Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Dial Plan** > **Area Code**.



Configuration Parameter

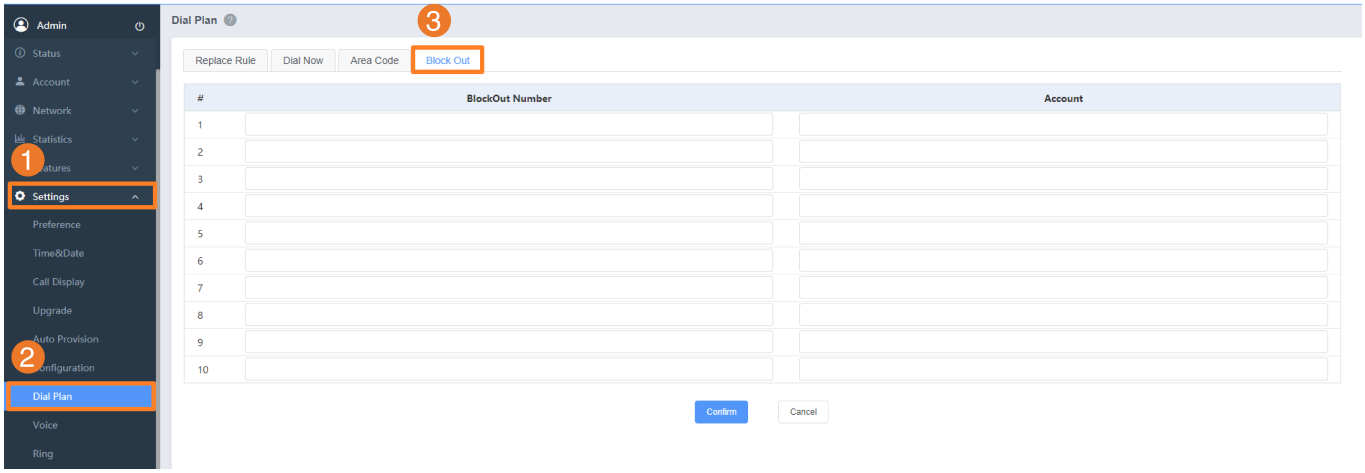
```
dialplan.area_code.code
dialplan.area_code.min_len
dialplan.area_code.max_len
dialplan.area_code.line_id
```

Parameter	Permitted Values	Default	Description
dialplan.area_code.code	String within 16 characters	Blank	It configures the area code to be added before the entered numbers when dialing out. **NOTE** The length of the entered number must be between the minimum length configured by the parameter `dialplan.area_code.min_len` and the maximum length configured by the parameter `dialplan.area_code.max_len`.
dialplan.area_code.min_len	Integer from 1 to 15	1	It configures the minimum length of the entered number.
dialplan.area_code.max_len	Integer from 1 to 15	15	It configures the maximum length of the entered number. **NOTE** The value must be larger than the minimum length.
dialplan.area_code.line_id	0 to 250	Blank	It configures the desired line to apply the area code rule. The digit 0 stands for all lines. If it is left blank, the area code rule will apply to all lines on the IP phone. **NOTE** Multiple line IDs are separated by commas.

Block Out Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Dial Plan** > **Block Out**.



Configuration Parameter

```
dialplan.block_out.number.X
dialplan.block_out.line_id.X
```

Parameter	Permitted Values	Default	Description
dialplan.block_out.number.X[1]	String within 32 characters	Blank	It configures the block out numbers. **Example:** `dialplan.block_out.number.1 = 4321` When you dial the number “4321” on your phone, the dialing will fail and the phone screen will prompt "Forbidden Number".
dialplan.block_out.line_id.X[2]	0 to 250	Blank	It configures the desired line to apply the block out rule. The digit 0 stands for all lines. If it is left blank, the block out rule will apply to all lines on the IP phone. **NOTE** Multiple line IDs are separated by commas.

[1]X is from 1 to 10.
[2]X is the account id.

Example: Add Replace Rules Using a Replace Rule File

The following example shows the configuration for adding replace rules.
Customize the replace rule template file and place this file to the provisioning server “http://192.168.10.25”.

Example

```
dialplan_replace_rule.url = http://192.168.10.25/DialPlan.xml
```

After provisioning, the rules defined in this file are added to the IP phone, and you can use the replace rules on the phone.

Auto Redial

Auto Redial

You can set the phone to automatically redial the last dialed number when the callee is temporarily unavailable. Both the number of attempts and waiting time between redials are configurable.

Auto Redial Configuration

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

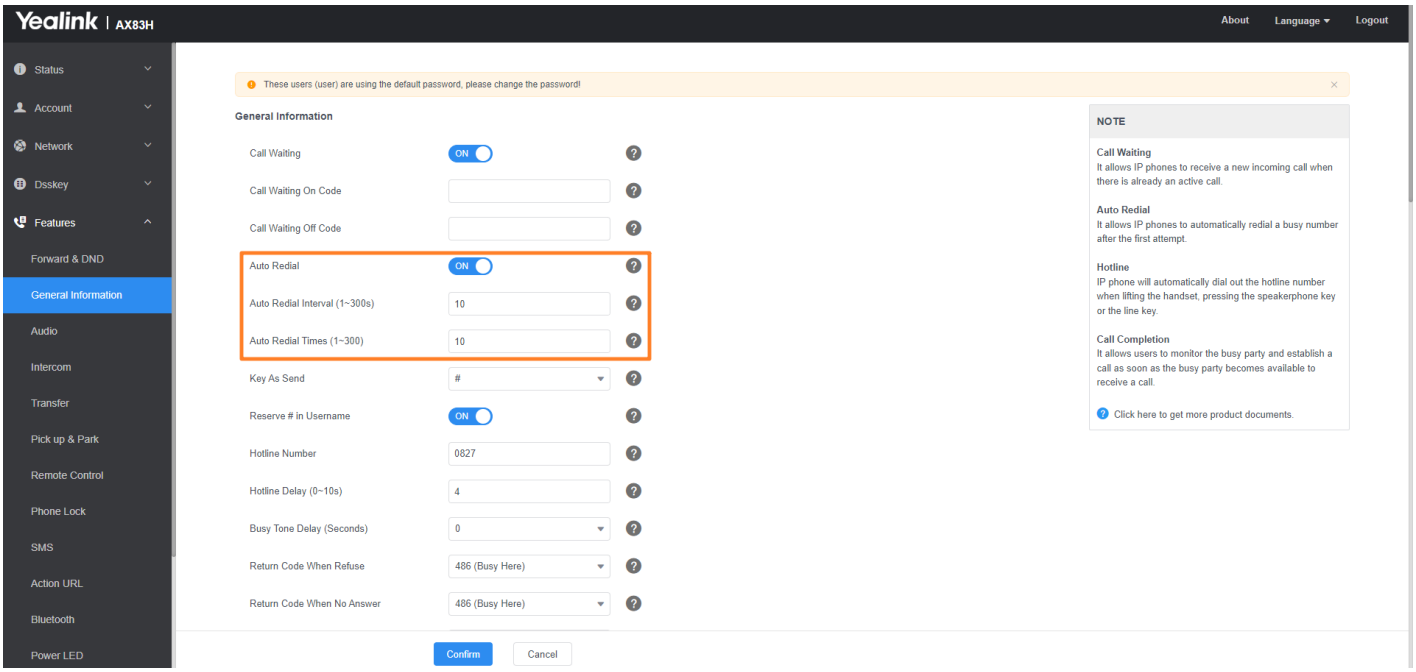
Configuration Parameter

```
auto_redial.enable
auto_redial.interval
auto_redial.times
features.redial_via_local_sip_server.enable
```

Parameter	Description	Permitted Values	Default
auto_redial.enable	It enables or disables the phone to automatically redial the last dialed number when the callee is temporarily unavailable.	0-Disabled 1-Enabled	0
auto_redial.interval	It configures the interval (in seconds) for the phone to wait between redials. The phone redials the last dialed number at regular intervals until the callee answers the call.	Integer from 1 to 300	10
auto_redial.times	It configures the auto redial times when the callee is temporarily unavailable. The phone tries to redial the callee as many times as configured till the callee answers the call.	Integer from 1 to 300	10
features.redial_via_local_sip_server.enable	It configures the phone to redial via a local SIP server or remote SIP server.	0-Remote SIP Server 1-Local SIP Server	1

Set via the Web User Interface

On the web user interface, go to **Features** > **General Information** > **Auto Redial/Auto Redial Interval (1~300s)/Auto Redial Times (1~300)**.



Live Dialpad

Live Dialpad

Live Dialpad allows the phones to automatically dial out the entered phone number without pressing the send key after a designated period of time.

Live Dialpad Configuration

The following table lists the parameters you can use to configure a live dialpad.

Configuration Parameter

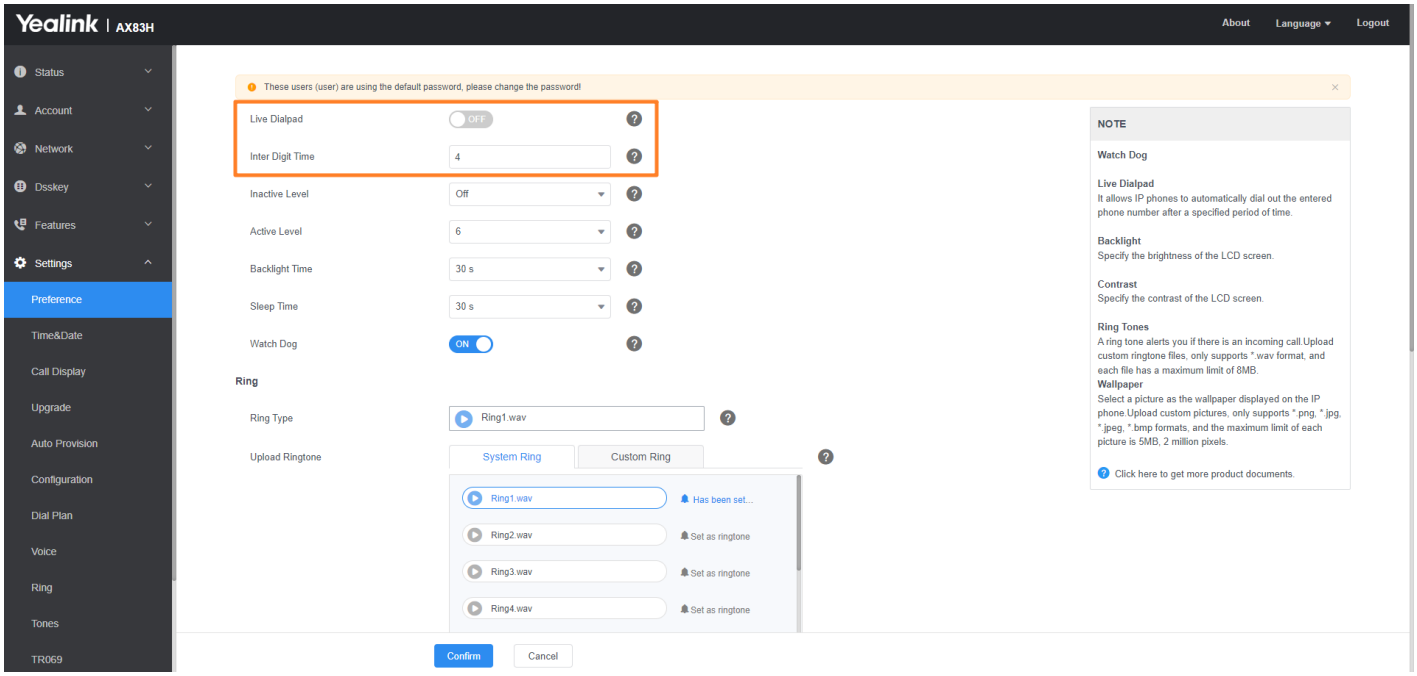
```
phone_setting.predial_autodial
phone_setting.inter_digit_time
```

Parameter	Description	Permitted Values	Default
phone_setting.predial_autodial	It enables or disables the phone to automatically dial out the entered phone number on the pre-dialing screen without pressing a send key. To enter the pre-dialing screen, directly enter numbers when the phone is idle.	0-Disabled 1-Enabled	0

phone_setting.inter_digit_time	It configures the delay time (in seconds) for the phone to automatically dial out the entered phone number without pressing a send key. For the pre-dialing screen, it works only if "phone_setting.predial_autodial" is set to 1 (Enabled).	Integer from 1 to 14	4

Set via the Web User Interface

On the web user interface, go to **Settings** > **Preference** > **Live Dialpad/Inter Digit Time**.



Emergency Dialplan and Enhanced 911

Introduction

You can dial the emergency telephone number (emergency services number) at any time when the phone is powered on and has been connected to the network. It is available even if your phone keypad is locked or no SIP account is registered.

Yealink phones support emergency dialplan and enhanced 911.

Emergency Dial Plan

You can configure the emergency dial plan for the phone (for example, emergency number, and emergency routing).

The phone determines if this is an emergency number by checking the emergency dial plan. When placing an emergency call, the call is directed to the configured emergency server. Multiple emergency servers may need to be configured for emergency routing to prevent emergency calls from getting through because of server failure. If the phone is not locked, it checks against the regular dial plan. If the phone is locked, it checks against the emergency dial plan.

Enhanced 911

E911 (Enhanced 911) is a location technology that enables the called party to identify the geographical location of

the calling party. For example, if a caller makes an emergency call to E911, the feature extracts the caller's information for the police department to identify the caller's location immediately.

Emergency Dialplan Configuration

Configuration parameter

```
dialplan.emergency.enable
dialplan.emergency.asserted_id_source
dialplan.emergency.custom_asserted_id
dialplan.emergency.server.X.address
dialplan.emergency.server.X.port
dialplan.emergency.server.X.transport_type
dialplan.emergency.X.value
dialplan.emergency.X.server_priority
```

Parameter	Permitted Values	Default	Description
dialplan.emergency.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the Emergency dialplan feature.
dialplan.emergency.asserted_id_source	**ELIN**-The outbound identity used in the P-Asserted-Identity (PAI) header of the SIP INVITE request is taken from the network using an LLDP-MED Emergency Location Identifier Number (ELIN). The custom outbound identity configured by `dialplan.emergency.custom_asserted_id` will be used if the phone fails to get the LLDP-MED ELIN value. **CUSTOM**-The custom outbound identity configured by `dialplan.emergency.custom_asserted_id` will be used; if `dialplan.emergency.custom_asserted_id` is left blank, the LLDP-MED ELIN value will be used.	ELIN	It configures the precedence of the source of emergency outbound identities when placing an emergency call. **NOTE** If the obtained LLDP-MED ELIN value is blank and no custom outbound identity, the PAI header will not be included in the SIP INVITE request. It works only if `dialplan.emergency.enable` is set to 1 (Enabled).

dialplan.emergency.custom_asserted_id	**A number with 10 to 25 digits** - for example, 1234567890. The SIP URI constructed from the number and SIP server (for example, abc.com) is included in the P-Asserted-Identity (PAI) header (for example, <sip:1234567890@abc.com >). **SIP URI** - for example, sip:1234567890123@abc.com. The full URI is included in the P-Asserted-Identity (PAI) header and the address will be replaced by the emergency server (for example, <sip:1234567890123@emergency.com >). **TEL URI** - for example, tel:+16045558000. The full URI is included in the P-Asserted-Identity (PAI) header (for example, <tel:+16045558000 >).	Blank	It configures the custom outbound identity when placing an emergency call. **NOTE** It works only if `dialplan.emergency.enable` is set to 1 (Enabled).
dialplan.emergency.server.X.address[1]	IP address or domain name	Blank	It configures the IP address or domain name of the emergency server X to be used for routing calls. **NOTE** If the account information has been configured (no matter whether the account registration succeeds or fails), the emergency calls will be dialed using the following priority: SIP server > emergency server; if not, the emergency server will be used. It works only if `dialplan.emergency.enable` is set to 1 (Enabled).

dialplan.emergency.server.X.port[1]	Integer from 0 to 65535	5060	It configures the port of emergency server X to be used for routing calls. **NOTE** It works only if dialplan.emergency.enable is set to 1 (Enabled).
dialplan.emergency.server.X.transport_type[1]	**0**-UDP **1**-TCP **2**-TLS **3**-DNS-NAPTR	0	It configures the transport protocol the phones use to communicate with the emergency server X. **NOTE** It works only if dialplan.emergency.enable is set to 1 (Enabled).
dialplan.emergency.X.value[2]	Number or SIP URI	When X = 1, the default value is 911; When X = 2-255, the default value is Blank.	It configures the emergency number to use on your phones so a caller can contact emergency services in the local area when required. **NOTE** It works only if dialplan.emergency.enable is set to 1 (Enabled).

[1] X is from 1 to 3.
[2] X is from 1 to 255.

Enhanced 911 Configuration

Configuration parameter

dialplan.emergency.held.server_url
dialplan.emergency.held.secondary.server_url
dialplan.emergency.held.request_type
dialplan.emergency.held.request_element.X.name
dialplan.emergency.held.request_element.X.value
dialplan.emergency.held.username
dialplan.emergency.held.password
dialplan.emergency.held.secondary.username
dialplan.emergency.held.secondary.password
dialplan.emergency.held.nai.enable
dialplan.emergency.held.location_retry_timer
dialplan.emergency.held.prompt_enable
dialplan.emergency.sip_header.geolocation_routing.enable
sip.emgr.header
dialplan.emergency.held.non_lldp.chassisid_portid_enable
dialplan.emergency.held.resync_period

Parameter	Permitted Values	Default	Description
dialplan.emergency.held.server_url	String	Blank	It configures the primary Location Information Server URL for the phone to send HELD location request. **NOTE** It works only if "dialplan.emergency.enable" is set to 1 (Enabled) and `dialplan.emergency.asserted_id_source` is set to **HELD**.
dialplan.emergency.held.secondary.server_url	String	Blank	It configures the secondary Location Information Server URL for the phone to send HELD location request. **NOTE** It works only if `dialplan.emergency.enable` is set to 1 (Enabled) and `dialplan.emergency.asserted_id_source` is set to **HELD**.

dialplan.emergency.held.request_type	**SIMPLE** or **REDSKY** or **YEALINK** If it is set to **SIMPLE**, the phone will send the location request message defined in RFC5985. If it is set to **REDSKY**, the phone will send the location request message defined by REDSKY.	SIMPLE	It configures the type of location request message. **NOTE** It works only if `dialplan.emergency.enable` is set to 1 (Enabled) and `dialplan.emergency.asserted_id_source` is set to **HELD**.

dialplan.emergency.held.request_element.X.name[2]	String	Blank	It configures the custom element name to be sent in a location request message.
			Example:
			`dialplan.emergency.held.request_element.1.name = mac`
			`dialplan.emergency.held.request_element.2.name = companyID`
			`dialplan.emergency.held.request_element.3.name = nai`
			
			NOTE
			It works only if `dialplan.emergency.enable` is set to 1 (Enabled) and `dialplan.emergency.asserted_id_source` is set to **HELD**.

dialplan.emergency.held.request_element.X.value[2]	String	Blank	It configures the custom element value to be sent in a location request message.
			Example:
			`dialplan.emergency.held.request_element.1.value = 001565B38ECB`
			`dialplan.emergency.held.request_element.2.value = 6f2f2d50-c385-4b72-b84a-ce0ca3a77cb7`
			`dialplan.emergency.held.request_element.3.value = 8611@pbx.yealink.com`
			
			NOTE
			It works only if `dialplan.emergency.enable` is set to 1 (Enabled) and `dialplan.emergency.asserted_id_source` is set to **HELD**.

dialplan.emergency.held.username	String	Blank	It configures the user name authentication when the phone sends location information to the E911 Location Information Server. **NOTE** It works only if `dialplan.emergency.held.request_type` is set to `YEALINK`.
dialplan.emergency.held.password	String	Blank	It configures the password authentication when the phone sends location information to the E911 Location Information Server. **NOTE** It works only if `dialplan.emergency.held.request_type` is set to **YEALINK** or **REDSKY**.
dialplan.emergency.held.secondary.username	String	Blank	It configures the user name authentication when the phone sends location information to the secondary E911 Location Information Server. **NOTE** It works only if `dialplan.emergency.held.request_type` is set to **YEALINK** or **REDSKY**.

dialplan.emergency.held.secondary.password	String	Blank	It configures the password authentication when the phone sends location information to the secondary E911 Location Information Server. **NOTE** It works only if dialplan.emergency.held.request_type is set to **YEALINK** or **REDSKY**.
dialplan.emergency.held.nai.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to send Network Access Identifier (nai) information to the E911 Location Information Server. **NOTE** It works only if dialplan.emergency.held.request_type is set to **YEALINK** or **REDSKY**.
dialplan.emergency.held.location_retry_timer	**0**-The phone does not report the location to the E911 Location Information Server again when failed to report the location to the server. **60 to 86400**-The phone reports the location to the E911 Location Information Server within the specified time interval.	0	It configures the time interval (seconds) for the phone to report location information to the E911 Location Information Server when the phone fails to report the location to the server. **NOTE** It works only if dialplan.emergency.held.request_type is set to **YEALINK** or **REDSKY**.

dialplan.emergency.held.prompt_enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to pop up the "Set E911 location failed! Please contact your administrator." prompt when the phone failed to report location information to the server. **NOTE** It works only if dialplan.emergency.held.request_type is set to **YEALINK** or **REDSKY**.
dialplan.emergency.sip_header.geolocation_routing.enable	**0**-The information "Geolocation-Routing: no" exists in the E911 INVITE message, and the information "geolocation", "Supported: geolocation" do not exist. **1**-The information "Geolocation-Routing: yes" exists in the E911 INVITE message, and the information "geolocation", "Supported: geolocation" also exist.	1	It enables or disables the phone to carry the geolocation-routing header information in the E911 INVITE message when the phone calls the emergency number. **NOTE** It works only if dialplan.emergency.held.request_type is set to **YEALINK** or **REDSKY**.
sip.emgr.header	**priority:emergency**-The E911 INVITE header field contains priority: emergency. **String**-The INVITE header field can be customized.	priority: emergency	It configures the content of E911 INVITE header field when the phone calls the emergency number.
dialplan.emergency.held.non_lldp.chassisid_portid_enable	**0**-The phone does not send the ChassisID and PortID fields to the server. **1**-The phone sends the ChassisID and PortID fields to the server, ChassisID field is the mac of the gateway, and PortID field is the mac of the phone.	0	It configures the contents of held requests when the phone cannot connect to LDAP switch.
dialplan.emergency.held.resync_period	**0**-The phone will not periodically send held requests to the server. **Integer from 1 to 10800**-The phone sends held request to the server within the specified time interval.	0	It configures the time interval (minutes) for the phone to send held requests regularly to the E911 Location Information Server.

[1] X is from 1 to 3.
[2] X is from 1 to 255.

Hotline&Off Hook Hot Line Dialing

Hotline

Hotline, sometimes referred to as hot dialing, is a point-to-point communication link in which a call is automatically directed to the preset hotline number. If you lift the handset, press the Speakerphone key or the off-hook key, and do nothing for a specified time interval, the phone will automatically dial out the hotline number. Yealink phones only support one hotline number.

ⓘ NOTE
If you do not specify a line, the phone uses the first available line to dial out the hotline number by default. This feature works only if the Off Hook Hot Line Dialing feature is disabled. For more information, refer to Off Hook Hot Line Dialing.

Hotline Configuration

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

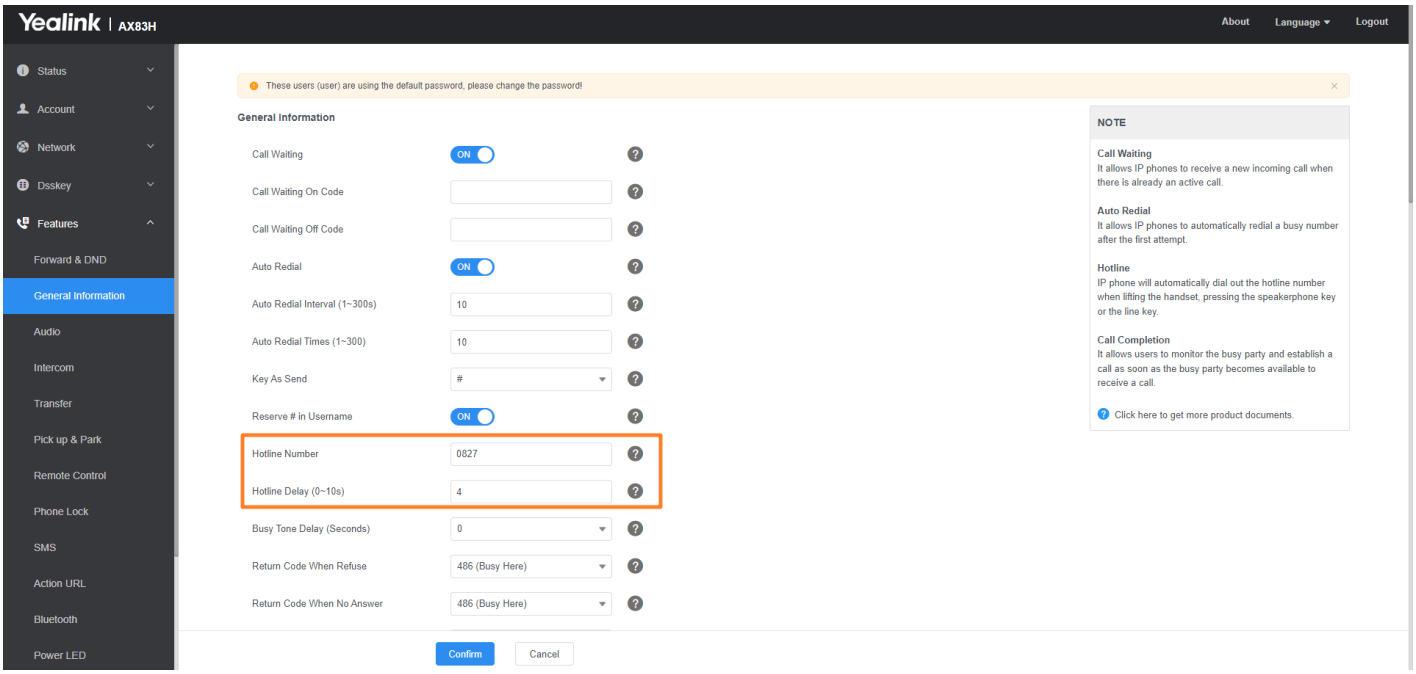
Configuration Parameter

```
features.hotline_number
features.hotline_delay
```

Parameter	Description	Permitted Values	Default
features.hotline_number	It configures the hotline number that the phone automatically dials out when you lift the handset, and press the Speakerphone/off-hook key. Leaving it blank disables the hotline feature.	String within 32 characters	Blank
features.hotline_delay	It configures the waiting time (in seconds) for the phone to automatically dial out the preset hotline number. If it is set to 0 (0s), the phone will immediately dial out the preset hotline number when you lift the handset, press the Speakerphone/off-hook key, or press the line key. If it is set to a value greater than 0, the phone will wait the designated seconds before dialing out the preset hotline number when you lift the handset, press the Speakerphone/off-hook key, or press the line key.	Integer from 0 to 10	4

Set via the Web User Interface

On the web user interface, go to **Features** > **General Information** > **Hotline Number/Hotline Delay(0~10s)**.



Off Hook Hot Line Dialing

For security reasons, the phones support off hook hotline dialing feature, which allows the phone to automatically dial out the pre-configured number when you call any number. The SIP server may then prompt you to enter an activation code for call service. Only if you enter a valid activation code, the phone will use this account to dial out a call successfully.

Off hook hotline dialing feature is configurable on a per-line basis and depends on support from a SIP server. The server actions may vary from different servers.

It is also applicable to the IP call and intercom call.

ⓘ NOTE

Off hook hotline dialing feature limits the call-out permission of this account and disables the hotline feature. For example, when the phone goes off-hook using the account with this feature enabled, the configured hotline number will not be dialed out automatically.

Off Hook Hot Line Dialing Configuration

Configuration Parameter

```
account.X.auto_dial_enable
account.X.auto_dial_num
```

Parameter	Permitted Values	Default	Description

account.X.auto_dial_enable[1]	**0**-Disabled **1**-Enabled, the phone will dial out the pre-configured number (configured by `account.X.auto_dial_num`).	0	It enables or disables the phone to automatically dial out a pre-configured number when a user calls any number.
account.X.auto_dial_num[1]	String within 1024 characters	Blank	It configures the number that the phone automatically dials out when a user calls any number. **NOTE** It works only if `account.X.auto_dial_enable` is set to 1 (Enabled)

[1] X is the account ID.

Speed Dial

Speed Dial

Speed dial allows you to speed up dialing contacts on the phone’s idle screen using keypad 1-9.

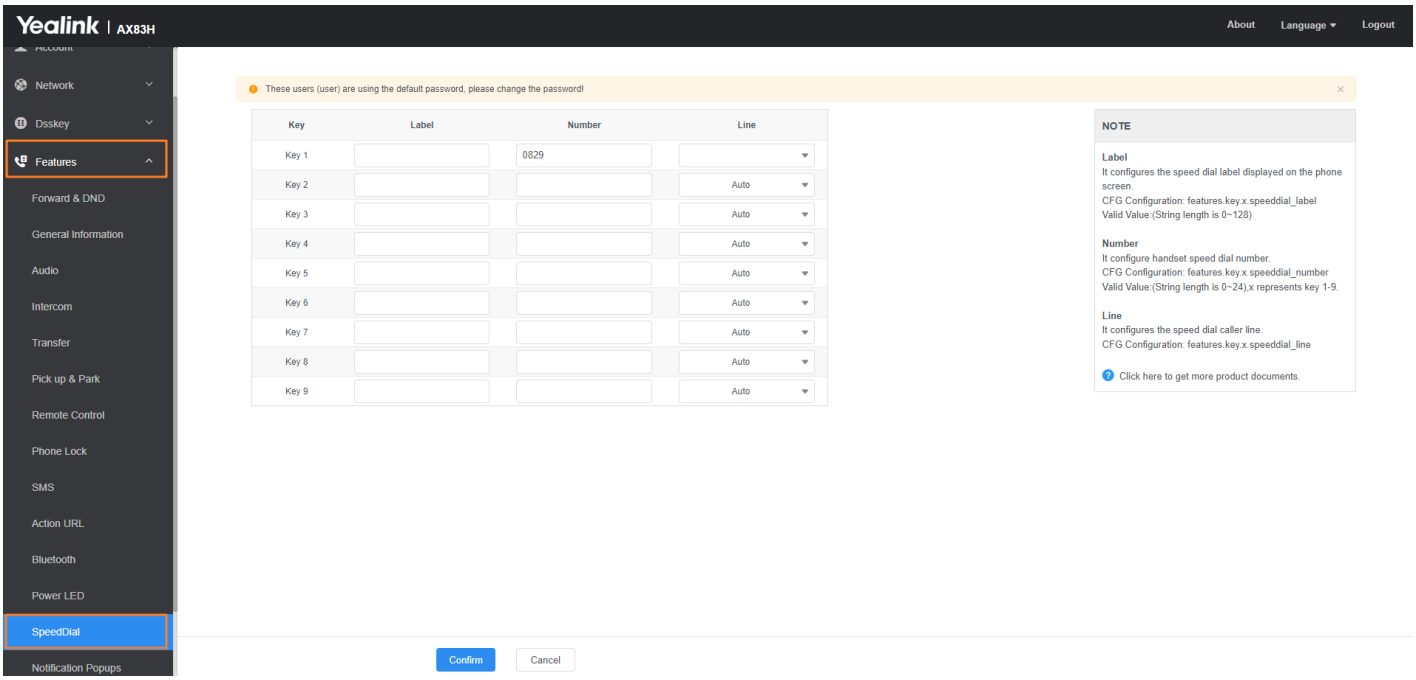
Speed Dial Key Configuration

Set via the Device Interface

For detailed information, see Place Call with Speed Dial.

Set via the Web User Interface

On the web user interface, go to **Features** > **SpeedDial**.



Configuration Parameter

```
features.key.x.speeddial_label
features.key.x.speeddial_number
features.key.x.speeddial_line
```

Parameter	Description	Permitted Values	Default
features.key.x.speeddial_label	It configures the speed dial number identification of the numeric keys.	String within 128 characters	Blank
features.key.x.speeddial_number	It configures the corresponding speed dial number of the numeric keys.	X =1-9.	Blank
features.key.x.speeddial_line	It configures the line for speed dial outgoing calls.	Handset registered line. X =1-9.	Auto

Call Timeout

Introduction

Call timeout defines a specific period of time after which the phone will cancel the dialing if the call is not answered.

Call Timeout Configuration

Configuration parameter

```
phone_setting.ringback_timeout
phone_setting.ringing_timeout
```

Parameter	Permitted Values	Default	Description
phone_setting.ringback_timeout	Integer from 1 to 3600	180	It configures the duration time (in seconds) in the ringback state. If it is set to 180, the phone will cancel the dialing if the call is not answered after 180 seconds.
phone_setting.ringing_timeout	Integer from 1 to 3600	120	It configures the duration time (in seconds) in the ringing state. If it is set to 180, the phone will stop ringing if the call is not answered within 180 seconds.

Anonymous Call

Introduction

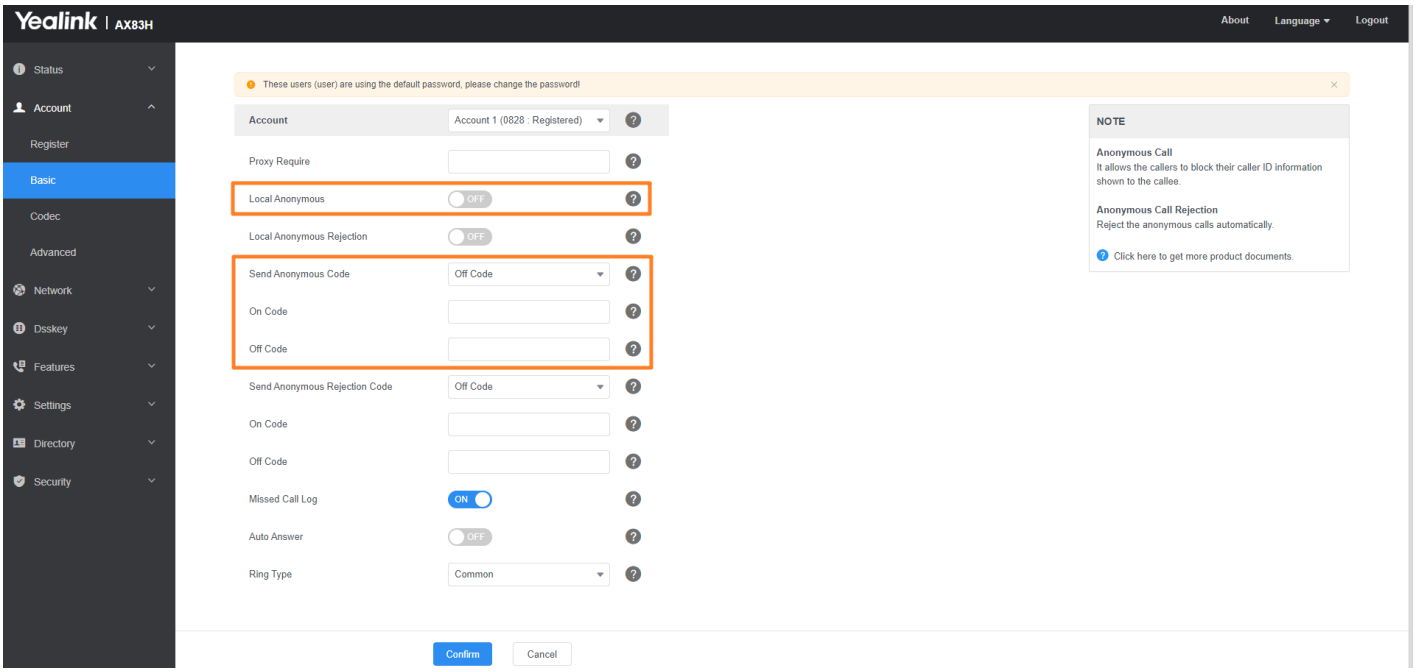
An anonymous call allows the caller to cancel the identity information shown to the callee. The callee’ s phone LCD screen prompts an incoming call from anonymity.
Anonymous calls can be performed locally or on the server. When performing an anonymous call on locally, the phone sends an INVITE request with a call source "From: "Anonymous" sip:anonymous@anonymous.invalid” . If performing an Anonymous call on a specific server, you may need to configure anonymous call on code and off code to activate and deactivate the server-side anonymous call feature.

ⓘ NOTE
After receiving an anonymous call, you will be unable to make a callback to that number. The device will display a "Network Unavailable" message.

Anonymous Call Configuration

Set via the Web User Interface

On the web user interface, go to **Account** > **Basic** > **Local Anonymous**/**Send Anonymous Code**.



Configuration parameter

account.X.anonymous_call
account.X.send_anonymous_code
account.X.anonymous_call_oncode
account.X.anonymous_call_offcode
features.anonymous.feature_key_sync.enable

Parameter	Permitted Values	Default	Description
account.X.anonymous_call[1]	**0**-Off **1**-On, the phone will block its identity from showing to the callee when placing a call. The callee’ s phone screen presents “Anonymous” instead of the caller’ s identity.	0	It triggers the anonymous call feature to on or off.
account.X.send_anonymous_code[1]	**0**-Off Code, the phone will send anonymous off code to the server when you deactivate the anonymous call feature. **1**-On Code, the phone will send anonymous on code to the server when you activate the anonymous call feature.	0	It configures the phone to send anonymous on/off code to activate/deactivate the server-side anonymous call feature for a specific account.
account.X.anonymous_call_oncode[1]	String within 32 characters	Blank	It configures the anonymous call on code. The phone will send the code to activate the anonymous call feature on server-side when you activate it on the phone.

account.X.anonymous_call_offcode[1]	String within 32 characters	Blank	It configures the anonymous call off code. The phone will send the code to deactivate the anonymous call feature on server-side when you deactivate it on the phone.
features.anonymous.feature_key_sync.enable	**0**-Disabled **1**-Enabled	0	It enables or disables synchronizing the anonymous call status between the IP phone and the server.

Call Number Filter

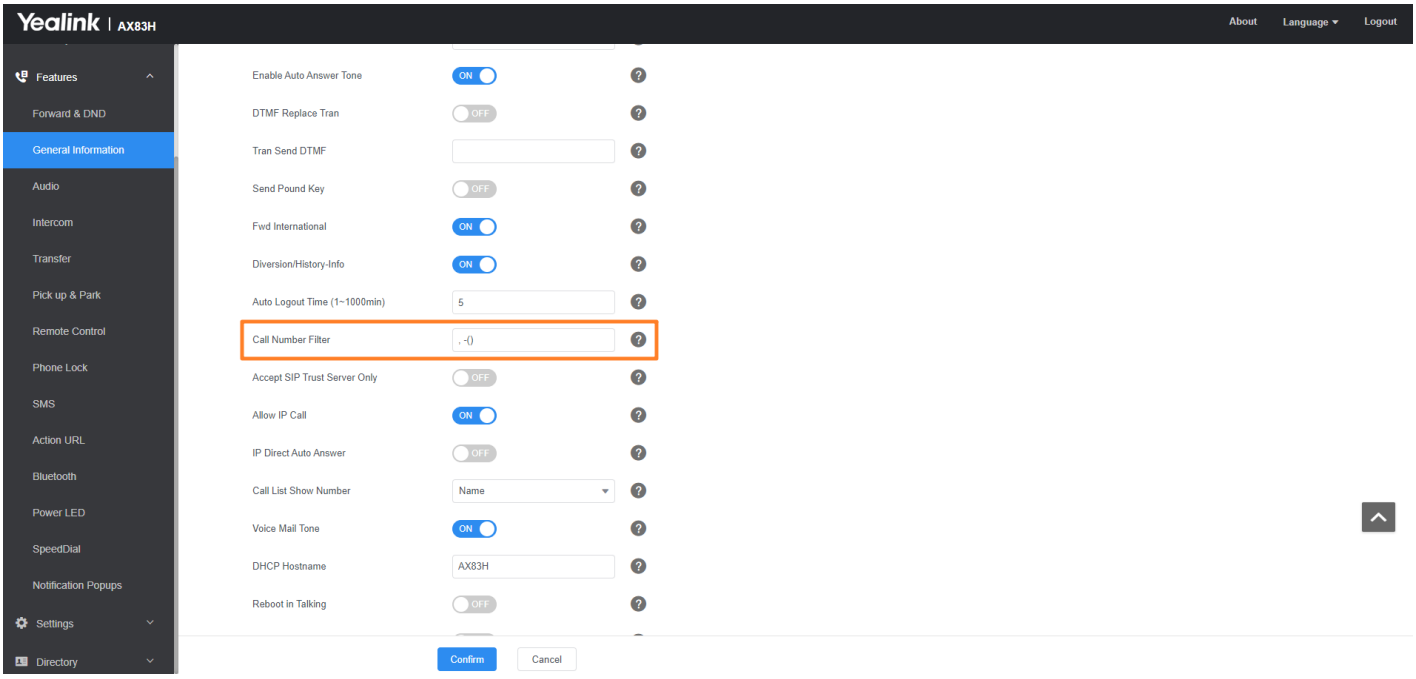
Introduction

The call number filter feature allows phones to filter designated characters automatically when dialing.

Call Number Filter Configuration

Set via the Web User Interface

On the web user interface, go to **Features** > **General Information** > **Call Number Filter**.



Configuration Parameter

```
features.call_num_filter
```

Parameter	Permitted Values	Default	Description
features.call_num_filter	String within 99 characters	, -()	It configures the characters the phone filters when dialing. If the dialed number contains configured characters, the phone will automatically filter these characters when dialing. **Example**: `features.call_num_filter = -` If you dial 3-61, the phone will filter the character - and then dial out 361. **NOTE** If it is left blank, the phone will not automatically filter any characters when dialing.

IP Address Call

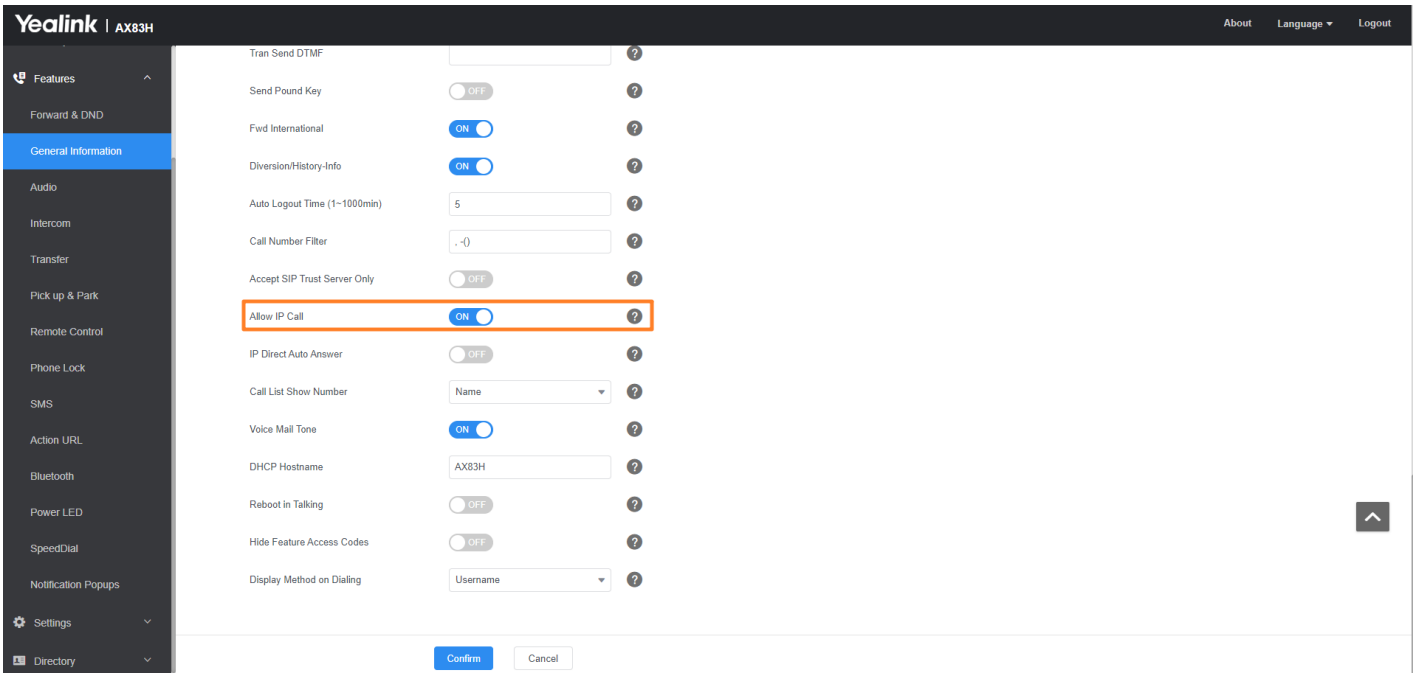
Introduction

You can set the phone to receive or place an IP call. You can neither receive nor place an IP call if you disable this feature.

IP Address Call Configuration

Set via the Web User Interface

On the web user interface, go to **Features** > **General Information** > **Allow IP Call**.



Configuration Parameter

features.direct_ip_call_enable

Parameter	Permitted Values	Default	Description
features.direct_ip_call_enable	**0**-Disabled **1**-Enabled	1	It enables or disables to allow IP address call. **NOTE** If you want to receive an IP address call, make sure sip.trust_ctrl is set to 0 (Disabled).

FAQ

1. Can't Disable the IP Call Feature

Auto Answer

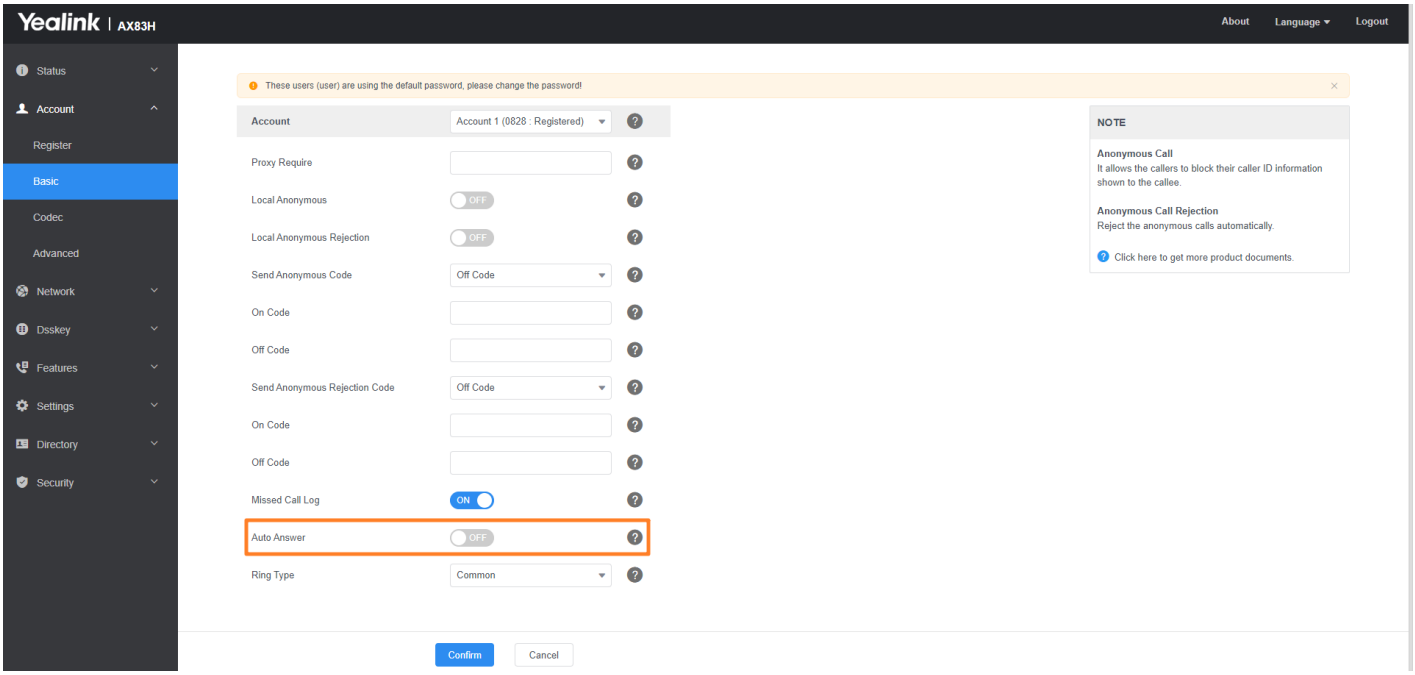
Introduction

Auto answer allows the handset to automatically answer an incoming call by picking up it from the charger cradle without having to press the off-hook key. The handset will not automatically answer the incoming call during a call even if the auto answer is enabled.
The auto answer feature works only if the handset is placed in the charger cradle.

Auto Answer Configuration

Set via the Web Interface

On the web user interface, go to: **Account** > **Basic** > **Account** > **Auto Answer**



Configuration Parameter

account.x.auto_answer

Parameter	Permitted Values	Default	Description
account.x.auto_answer	0-Disabled 1-Enabled, the phone can automatically answer an incoming call.	-1	It enables or disables auto-answer a SIP call. **NOTE** The phone cannot automatically answer the incoming call during a call or while dialing even if the auto answer is enabled.
features.intercom.allow_string	Numbers. Multiple numbers are separated by commas.	Blank	It is used to configure whether incoming calls from specified numbers are treated as intercom calls. **NOTE** Only support x.86.0.112 or later

X is the account ID.

Anonymous Call Rejection

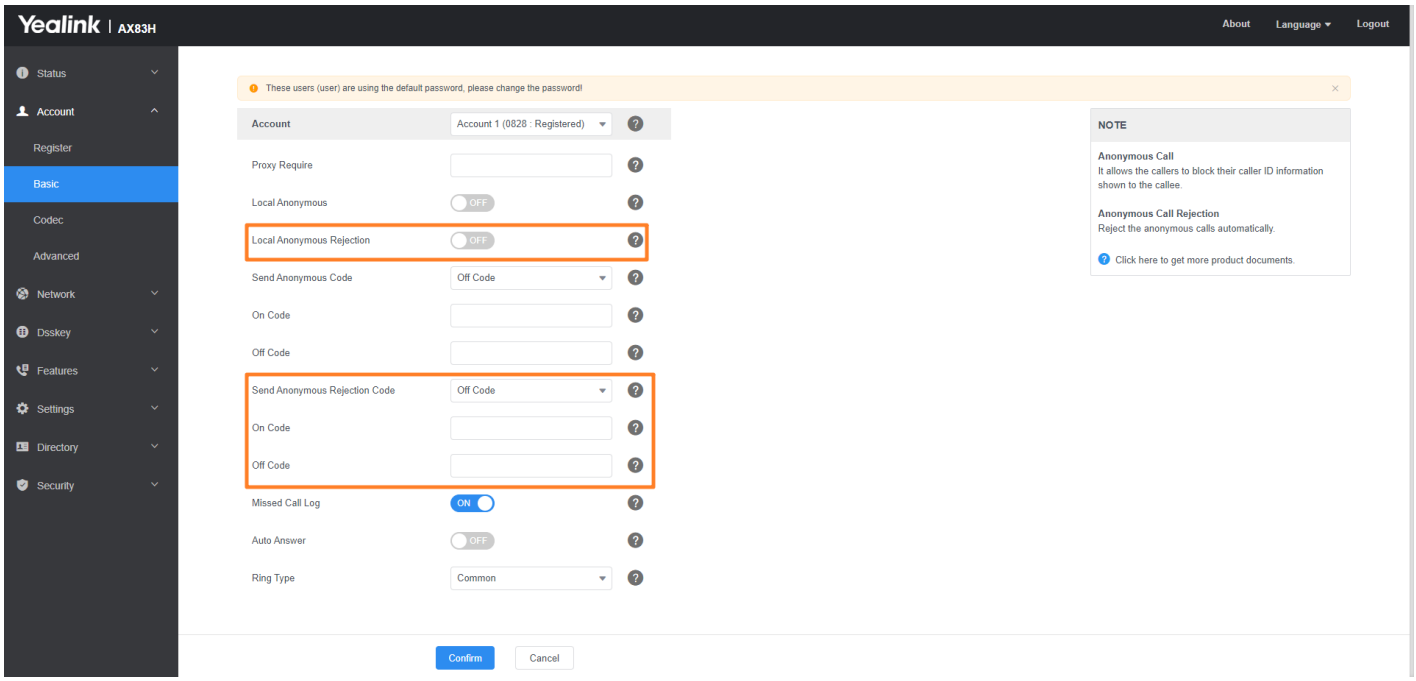
Introduction

Anonymous call rejection allows phones to automatically reject incoming calls from callers whose identity has been deliberately concealed.
Anonymous call rejection can be performed locally or on the server. When performing anonymous call rejection locally, the phone sends the server a status message ” Status-Line: SIP/2.0 433 Anonymity Disallowed” . If performing anonymous call rejection on a specific server, you may need to configure anonymous call rejection on code and off code to activate and deactivate server-side anonymous call rejection feature.

Anonymous Call Rejection Configuration

Set via the Web User Interface

On the web user interface, go to **Account** > **Basic** > **Local Anonymous Rejection**/**Send Anonymous Rejection Code**.



Configuration Parameter

account.X.reject_anonymous_call
account.X.anonymous_reject_oncode
account.X.send_anonymous_rejection_code
account.X.anonymous_reject_offcode

Parameter	Permitted Values	Default	Description

account.X.reject_anonymous_call[1]	**0**-Off **1**-On, the phone will automatically reject incoming calls from users enabled anonymous call feature. The anonymous user's phone screen presents "**Forbidden**".	0	It triggers the anonymous call rejection feature to on or off.
account.X.anonymous_reject_oncode[1]	String within 32 characters	Blank	It configures the anonymous call rejection on code. The phone will send the code to activate the anonymous call rejection feature on server-side when you activate it on the phone.
account.X.send_anonymous_rejection_code[1]	**0**-Off Code, the phone will send an anonymous rejection off code to the server when you deactivate the anonymous call rejection feature. **1**-On Code, the phone will send anonymous rejection on code to the server when you activate the anonymous call rejection feature.	0	It configures the IP phone to send anonymous call rejection on/off code to activate/deactivate the server-side anonymous call rejection feature for account X.
account.X.anonymous_reject_offcode[1]	String within 32 characters	Blank	It configures the anonymous call rejection off code. The phone will send the code to deactivate the anonymous call rejection feature on server-side when you deactivate it on the phone.

[1] X is the account ID.

Call Waiting

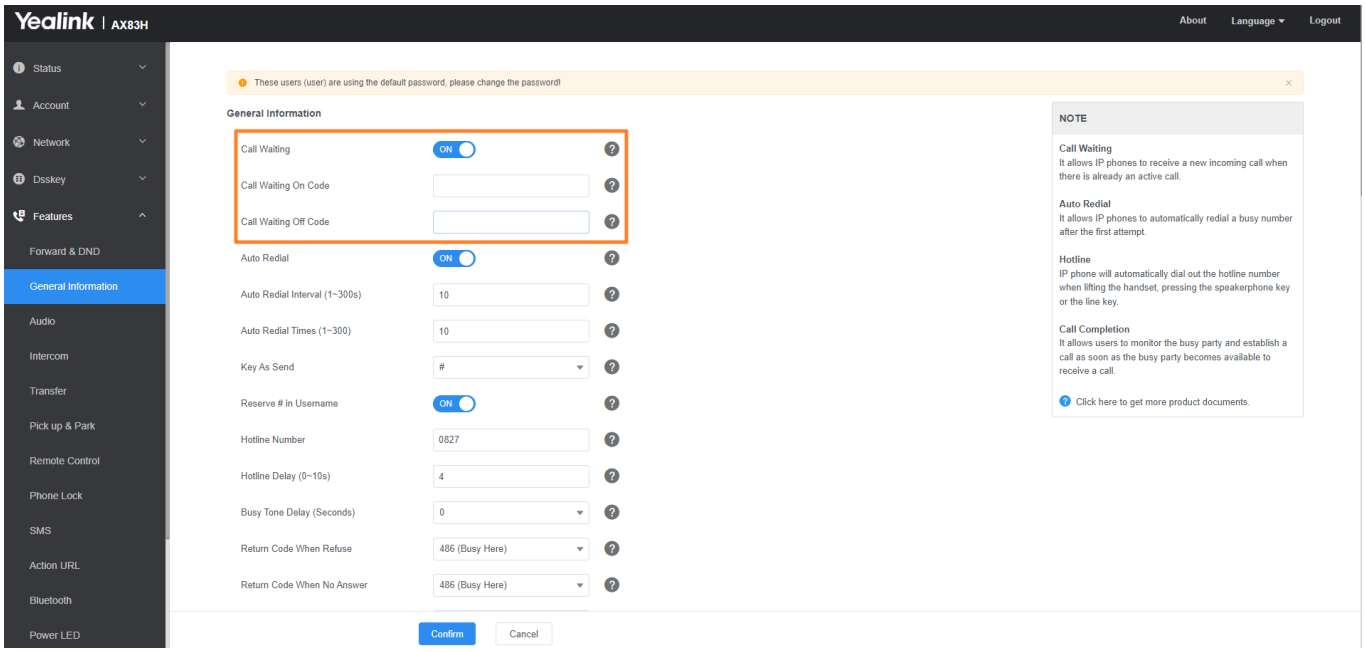
Introduction

Call waiting enables you to receive another call when there is already an active call on your phone. If it is disabled, the new incoming call will be rejected automatically.
You can enable call waiting feature and set the phone to play a warning tone to avoid missing important calls during a call.
Yealink phones also support call waiting on code and off code to activate and deactivate server-side call waiting feature. They may vary on different servers.

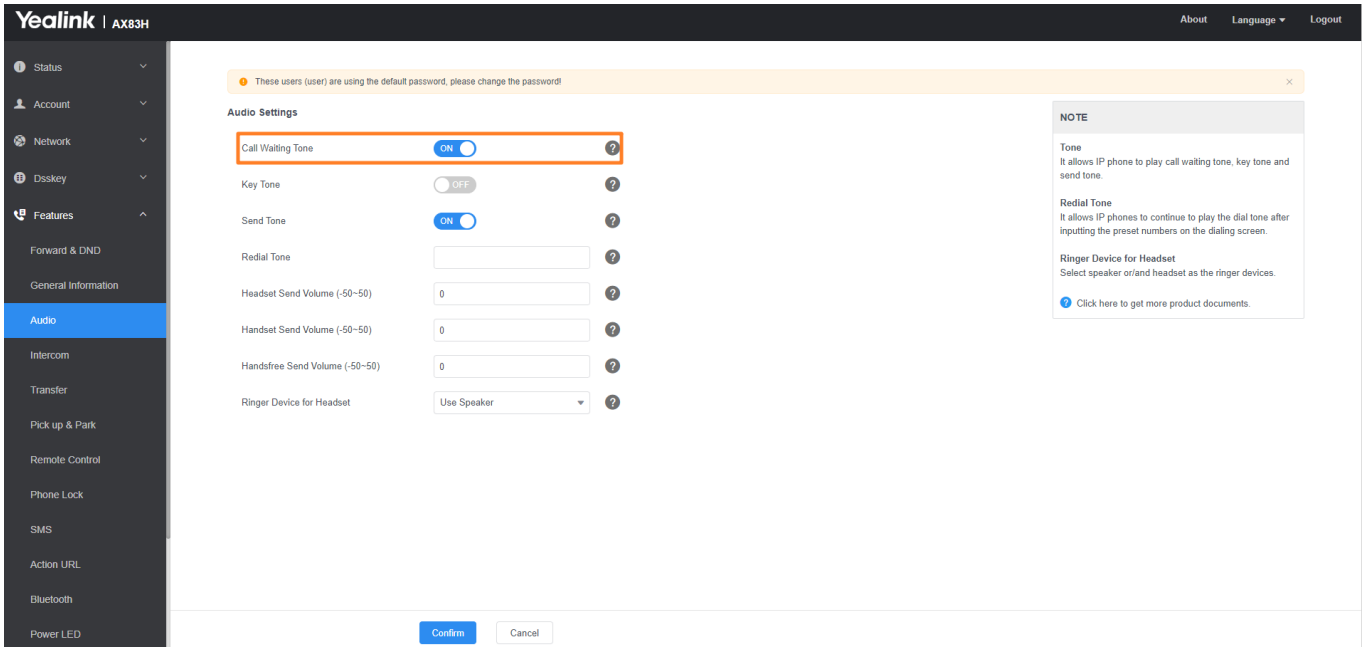
Call Waiting Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Call Waiting**.



2. On the web user interface, go to **Features** > **Audio** > **Call Waiting Tone**.



Configuration Parameter

```
call_waiting.enable
call_waiting.tone
call_waiting.on_code
call_waiting.off_code
```

Parameter	Permitted Values	Default	Description

call_waiting.enable	**0**-Disabled, a new incoming call is automatically rejected by the phone with a busy message during a call. **1**-Enabled, the phone screen will present a new incoming call during a call.	1	It enables or disables the call-waiting feature.
call_waiting.tone	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to play the call waiting tone when the phone receives an incoming call during a call. **NOTE** It works only if `call_waiting.enable` is set to 1 (Enabled).
call_waiting.on_code	String within 32 characters	Blank	It configures the call waiting on code. The phone will send the code to activate the call waiting on the server side when you activate it on the phone.
call_waiting.off_code	String within 32 characters	Blank	It configures the call waiting off code. The phone will send the code to deactivate the call waiting on the server side when you deactivate it on the phone.

Call Hold

Introduction

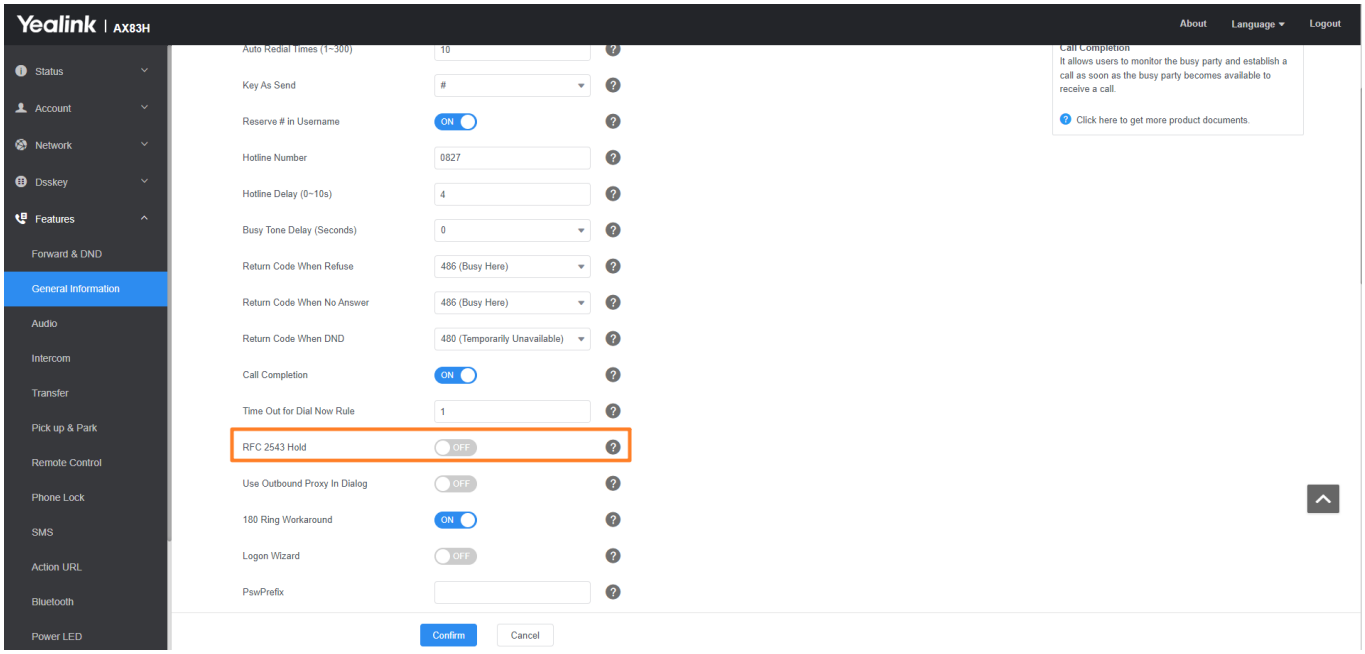
Call hold provides a service of placing an active call on hold. It enables you to pause activity on an active call so that you can use the phone for another task, for example, to place or receive another call.
When a call is placed on hold, the phones send an INVITE request with HOLD SDP to request remote parties to stop sending media and to inform them that they are being held.
The phones support two call hold methods:

- RFC 3264, which sets the "a" (media attribute) in the SDP to sendonly, recvonly or inactive (for example, a=seendonly).
- RFC 2543, which sets the "c" (connection addresses for the media streams) in the SDP to zero (for example, c=0.0.0.0).

Call Hold Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **RFC 2543 Hold/Play Hold Tone/Play Hold Tone Delay/Held Tone Interval**.



Configuration Parameter

```
sip.rfc2543_hold
account.X.hold_use_inactive[1]
```

Parameter	Permitted Values	Default	Description
sip.rfc2543_hold	**0**-Disabled, SDP media direction attributes (such as a=sendonly) per RFC 3264 is used when placing a call on hold. **1**-Enabled, SDP media connection address c=0.0.0.0 per RFC 2543 is used when placing a call on hold.	0	It enables or disables the phone to use RFC 2543 (c=0.0.0.0) outgoing hold signaling.

account.X.hold_use_inactive[1]	**0**-Disabled, SDP media direction attribute "a=sendonly" is used when placing a call on hold. **1**-Enabled, SDP media direction attribute "a=inactive" is used when placing a call on hold. RTP packets will not be sent or received.	0	It enables or disables the phone to use inactive outgoing hold signaling. **NOTE** It works only if `sip.rfc2543_hold` is set to 0 (Disabled).
features.play_hold_tone.enable	0-Disabled 1-Enabled	1	It enables or disables the phone to play the call hold tone when you place a call on hold.
features.play_hold_tone.delay	Integer from 3 to 3600	30	It configures the time (in seconds) to wait for the phone to play the initial call hold tone. If it is set to 30 (30s), the phone will wait 30 seconds to play the initial call hold tone after you place a call on hold. **NOTE** It works only if "features.play_hold_tone.enable" is set to 1 (Enabled).
features.play_hold_tone.interval	Integer from 3 to 3600	30	It configures the time (in seconds) between subsequent call hold tones. If it is set to 3 (3s) and "features.play_hold_tone.delay" is set to 30 (30s), the phone will begin to play a hold tone after you place a call on hold for 30 seconds and repeat the call hold tone every 3 seconds. **NOTE** It works only if "features.play_hold_tone.enable" is set to 1 (Enabled).
features.play_held_tone.enable	0-Disabled 1-Enabled	0	It enables or disables the phone to play the call held tone when a call is held by the other party.

features.play_held_tone.delay	Integer from 3 to 3600	30	It configures the time (in seconds) to wait for the phone to play the initial call held tone. If it is set to 30 (30s), the phone will wait 30 seconds to play the initial call held tone after you are held by the other party. **NOTE** It works only if the Music on Hold feature is disabled and "features.play_held_tone.enable" is set to 1 (Enabled).
features.play_held_tone.interval	Integer from 3 to 3600	60	It configures the time (in seconds) between subsequent call held tones. If it is set to 3 (3s) and "features.play_held_tone.delay" is set to 30 (30s), the phone will begin to play a held tone after a call is held by the other party for 30 seconds and repeat the call held tone every 3 seconds. **NOTE** It works only if the Music on Hold feature is disabled and "features.play_held_tone.enable" is set to 1 (Enabled).
phone_setting.hold_or_swap.mode	**0**-Only display the Swap soft key. **1**-Only display the Hold soft key. **2**-Display the Hold and Swap soft keys.	0	It configures the time (in seconds) between subsequent call held tones. If it is set to 3 (3s) and "features.play_held_tone.delay" is set to 30 (30s), the phone will begin to play a held tone after a call is held by the other party for 30 seconds and repeat the call held tone every 3 seconds. **NOTE** It works only if the Music on Hold feature is disabled and "features.play_held_tone.enable" is set to 1 (Enabled).

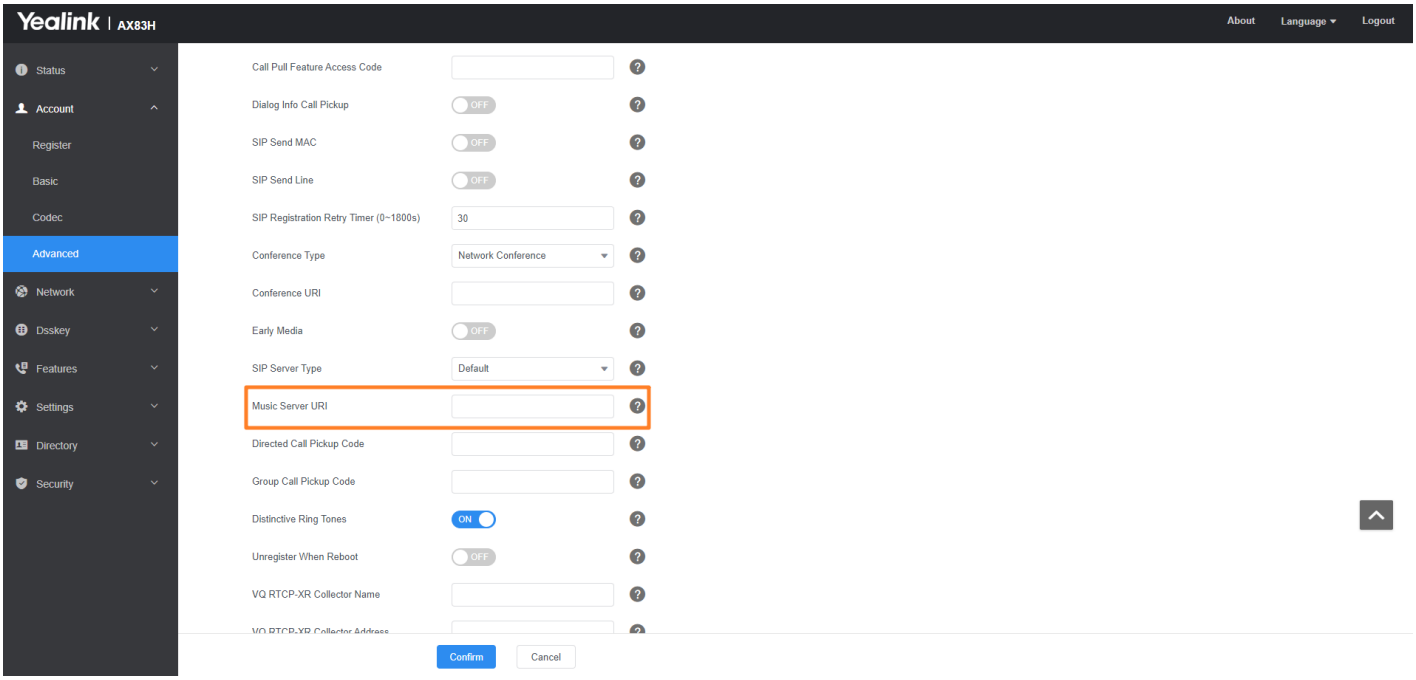
[1] X is the account ID.

Music on Hold (MoH) Configuration

When a call is placed on hold, the phone will send an INVITE message to the specified MoH server account according to the SIP URI. The MoH server account automatically responds to the INVITE message and immediately plays audio from some source located anywhere (LAN, Internet) to the held party. For more information, refer to draft RFC draft-worley-service-example.

Set via the Web User Interface

On the web user interface, go to **Account** > **Advanced** > **Music Server URI**.



Configuration parameter

account.X.music_server_uri
account.X.music_on_hold_type

Parameter	Permitted Values	Default	Description
account.X.music_server_uri [1]	SIP URI within 256 characters	Blank	It configures the address of the Music On Hold server. Examples for valid values: <10.1.3.165>, 10.1.3.165, sip:moh@sip.com, sip:moh@sip.com <yealink.com > or yealink.com. **NOTE** The DNS query in this parameter only supports A query.

account.X.music_on_hold_type[1]	**0**-Calling the Music On Hold server before holding the call **1**-Calling the Music On Hold server after holding the call	0	It configures the way to process Music On Hold when placing an active call on hold.

[1] X is the account ID.

Call Forward

Introduction

You can forward calls in special situations, such as when the phone is busy or there is no answer, or forward all incoming calls to a contact immediately.

Call Forward Settings Configuration

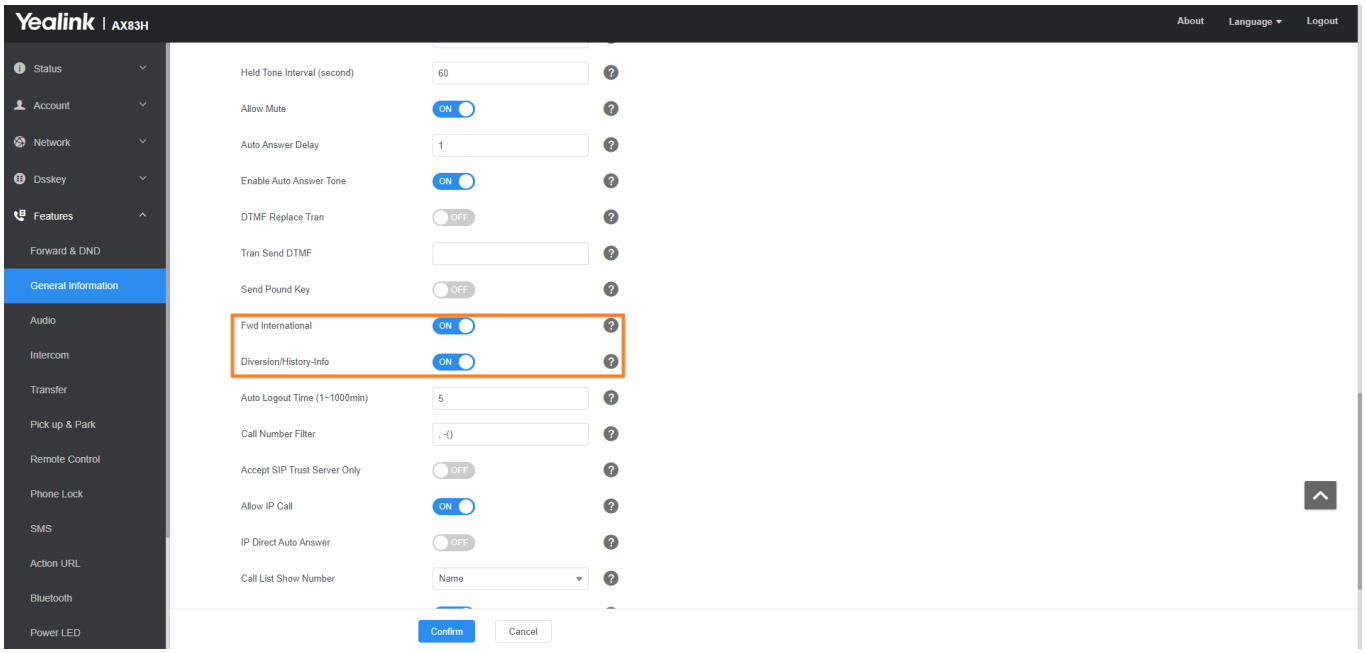
You can change the following call forward settings:

- Enable or disable the call forward feature. If disabled, the users cannot configure call forward on their phones.
- Allow or disallow users to forward an incoming call to an international telephone number (the prefix is 00).
- Enable or disable the display of the Diversion header. The Diversion header allows the phone that receives a forwarded call to indicate where the call was from.

The following table lists the parameters to change the call forward settings.

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Fwd International**/**Diversion/History-Info**.



Configuration Parameter

```
features.fwd.allow
forward.international.enable
features.fwd_diversion_enable
features.forward_call_popup.enable
```

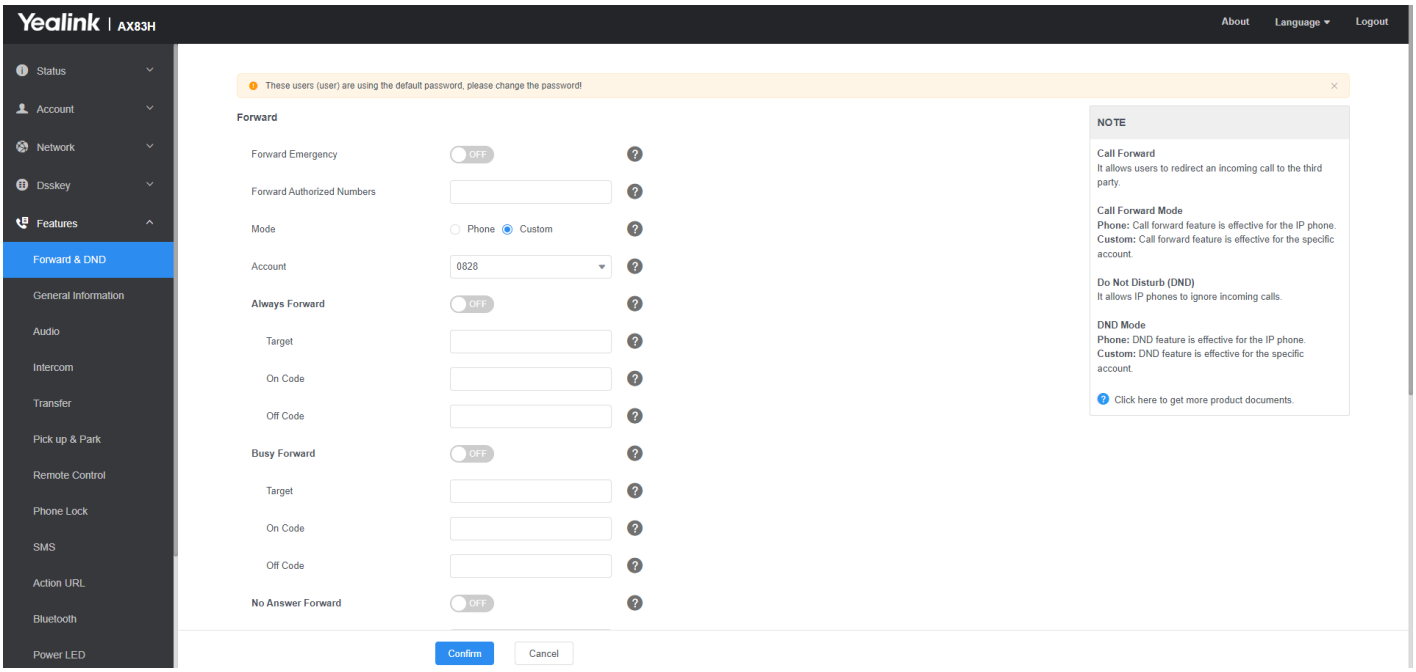
Parameter	Permitted Values	Default	Description
features.fwd.allow	**0**-Disabled, call forward feature is not available to the users. **1**-Enabled	1	It enables or disables the call forward feature.
forward.international.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to forward incoming calls to international numbers (the prefix is 00).
features.fwd_diversion_enable	**0**-Disabled **1**-Enabled, the server can use the Diversion field with an SIP header to inform the phone of a call' s history.	1	It enables or disables the phone to present the diversion information when an incoming call is forwarded to the IP phone.
features.forward_call_popup.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to pop up the message when you forward an incoming call to another party.

Call Forward Feature Configuration

Yealink phones support call forward on code and off code to activate and deactivate server-side call forward feature.
They may vary on different servers.

Set via the Web User Interface

1. On the web user interface, go to **Features** > **Forward&DND** > **Forward**.



Configuration parameter

account.X.always_fwd.enable
account.X.always_fwd.target
account.X.always_fwd.on_code
account.X.always_fwd.off_code
account.X.busy_fwd.enable
account.X.busy_fwd.target
account.X.busy_fwd.on_code
account.X.busy_fwd.off_code
account.X.timeout_fwd.enable
account.X.timeout_fwd.target
account.X.timeout_fwd.timeout
account.X.timeout_fwd.on_code
account.X.timeout_fwd.off_code
account.x.fwd_diversion_hdr.enable

Parameter	Permitted Values	Default	Description
account.X.always_fwd.enable[1]	**0**-Off **1**-On, incoming calls to the account X are forwarded to the destination number (configured by the parameter account.X.always_fwd.target) immediately.	0	It triggers always forward feature to on or off. **NOTE** It works only if features.fwd.allow is set to 1 (Enabled) and features.fwd_mode is set to 1 (Custom).

account.X.always_fwd.target[1]	String within 32 characters	Blank	It configures the destination number of the always forward. **NOTE** It works only if features.fwd.allow is set to 1 (Enabled) and features.fwd_mode is set to 1 (Custom).
account.X.always_fwd.on_code[1]	String within 32 characters	Blank	It configures the always forward on code to activate the server-side always forward feature. The phone will send the always forward on code, and the pre-configured destination number (configured by the parameter account.X.always_fwd.target) to the server when you activate always forward feature on the phone. **NOTE** It works only if features.fwd.allow is set to 1 (Enabled) and features.fwd_mode is set to 1 (Custom).
account.X.always_fwd.off_code[1]	String within 32 characters	Blank	It configures the always forward off code to deactivate the server-side always forward feature. The phone will send the always forward off code to the server when you deactivate always forward feature on the phone. **NOTE** It works only if features.fwd.allow is set to 1 (Enabled) and features.fwd_mode is set to 1 (Custom).

account.X.busy_fwd.enable[1]	**0**-Off **1**-On, incoming calls to the account X are forwarded to the destination number (configured by the parameter account.X.busy_fwd.target) when the callee is busy.	0	It triggers the busy forward feature to on or off.
account.X.busy_fwd.target[1]	String within 32 characters	Blank	It configures the destination number of the busy forward. **NOTE** It works only if features.fwd.allow is set to 1 (Enabled) and features.fwd_mode is set to 1 (Custom).
account.X.busy_fwd.on_code[1]	String within 32 characters	Blank	It configures the busy forward on code to activate the server-side busy forward feature. The phone will send the busy forward on code and the pre-configured destination number (configured by the parameter account.X.busy_fwd.target) to the server when you activate the busy forward feature on the phone. **NOTE** It works only if features.fwd.allow is set to 1 (Enabled) and features.fwd_mode is set to 1 (Custom).

account.X.busy_fwd.off_code[1]	String within 32 characters	Blank	It configures the busy forward off code to deactivate the server-side busy forward feature. The phone will send the busy forward off code to the server when you deactivate the busy forward feature on the phone. **NOTE** It works only if features.fwd.allow is set to 1 (Enabled) and features.fwd_mode is set to 1 (Custom).
account.X.timeout_fwd.enable[1]	**0**-Off **1**-On, incoming calls to the account X are forwarded to the destination number (configured by the parameter account.X.timeout_fwd.target) after a period of ring time.	0	It triggers no answer forward feature to on or off. **NOTE** It works only if features.fwd.allow is set to 1 (Enabled) and features.fwd_mode is set to 1 (Custom).
account.X.timeout_fwd.target[1]	String within 32 characters	Blank	It configures the destination number of the no answer forward. **NOTE** It works only if features.fwd.allow is set to 1 (Enabled) and features.fwd_mode is set to 1 (Custom).
account.X.timeout_fwd.timeout[1]	Integer from 0 to 20	2	It configures ring times (N) to wait before forwarding incoming calls. **NOTE** It works only if features.fwd.allow is set to 1 (Enabled) and features.fwd_mode is set to 1 (Custom).

account.X.timeout_fwd.on_code[1]	String within 32 characters	Blank	It configures the no answer forward on code to activate the server-side no answer forward feature. The phone will send the no answer forward on code and the pre-configured destination number (configured by the parameter account.X.timeout_fwd.target) to the server when you activate the no answer forward feature on the phone. **NOTE** It works only if features.fwd.allow is set to 1 (Enabled) and features.fwd_mode is set to 1 (Custom).
account.X.timeout_fwd.off_code[1]	String within 32 characters	Blank	It configures the no answer forward off code to deactivate the server-side no answer forward feature. The phone will send the no answer forward off code to the server when you deactivate the no answer forward feature. **NOTE** It works only if features.fwd.allow is set to 1 (Enabled) and features.fwd_mode is set to 1 (Custom).
account.x.fwd_diversion_hdr.enable	**0**: Do not carry the Diversion header field. **1**:Carry the Diversion header field.	1	Used to control whether the forward feature of account X carries the Diversion header field. **NOTE** It works only if you version is x.86.0.118 or later

[1] X is the account ID.

Call Forward Synchronization for Server-side Configuration

The call forward synchronization feature provides the capability to synchronize the status of the call forward

features between the IP phone and the server.
If the call forward is activated in phone mode, the forward status changing locally will be synchronized to all registered accounts on the server; but if the forward status of the specific account is changed on the server, the forward status locally will be changed.

Configuration parameter

```
features.feature_key_sync.enable
account.X.forward.feature_key_sync.enable
```

Parameter	Permitted Values	Default	Description
features.feature_key_sync.enable	**0**-Disabled **1**-Enabled, the phone sends a SUBSCRIBE message with event "as-feature-event" to the server.	0	It enables or disables synchronizing the feature status between the IP phone and the server.
account.X.forward.feature_key_sync.enable[1]	**0**-Disabled **1**-Enabled, server-based call forward is enabled. The server and local phone call forward are synchronized.	Blank	It enables or disables the forward feature synchronization for account X. **NOTE** The value configured by this parameter takes precedence over that configured by the parameter `features.forward.feature_key_sync.enable`. It works only if `account.X.feature_key_sync.enable` is set to 1 (Enabled).

[1] X is the account ID.

Call Transfer

Introduction

Call transfer enables the phones to transfer an existing call to a third party. For example, if party A is in an active call with party B, party A can transfer this call to party C (the third party). Then, party B will begin a new call with party C, and party A will disconnect.
Yealink phones support call transfer using the REFER method specified in RFC 3515 and offer three types of transfer:

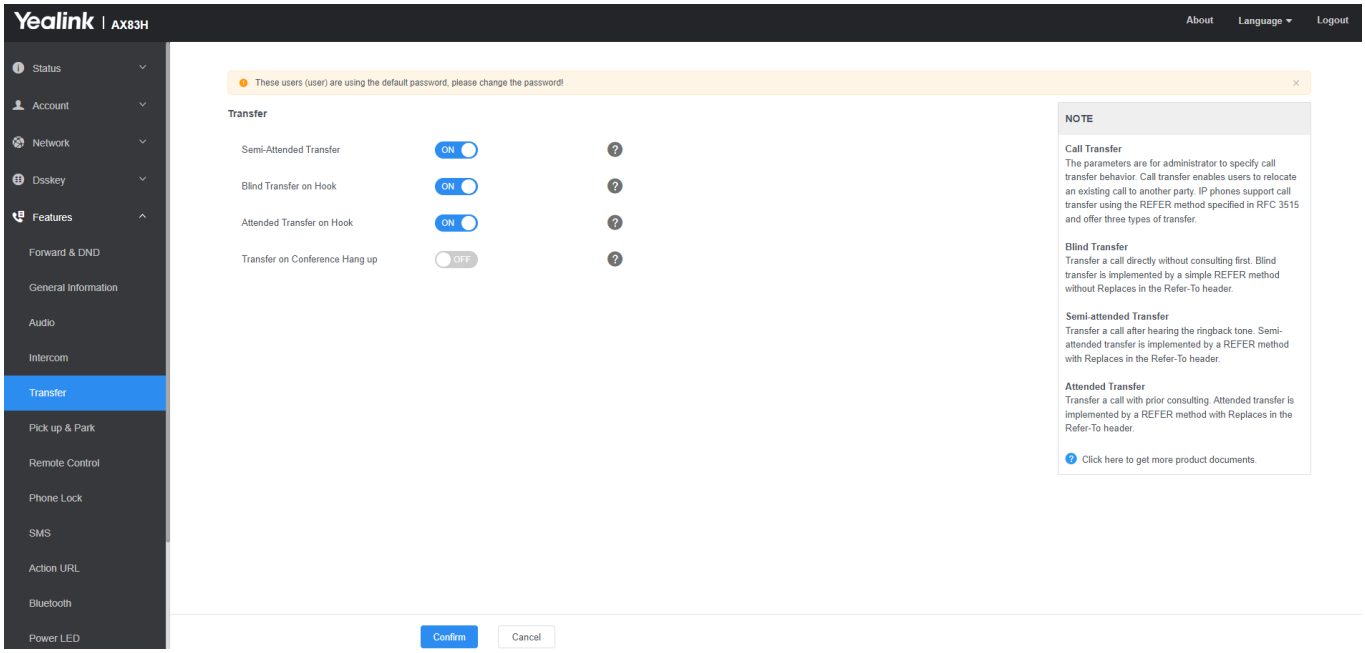
Type	Description

Blind Transfer	Transfer a call directly to another party without consulting. Blind transfer is implemented by a simple REFER method without replacing the Refer-To header.
Semi-attended Transfer	Transfer a call after hearing the ringback tone. The semi-attended transfer is implemented by a REFER method with Replaces in the Refer-To header. The semi-attended transfer is applicable to when users do not want to consult with the third party after hearing the ringback tone, and the third party has not answered the call, the users can cancel the transfer or implement the transfer.
Attended Transfer (Consultative Transfer)	Transfer a call with prior consulting. Attended transfer is implemented by a REFER method with Replaces in the Refer-To header.

Call Transfer Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **Transfer**.



Configuration Parameter

features.transfer.allow
transfer.semi_attend_tran_enable
account.X.transfer_refer_to_contact_header.enable
features.transfer_keep_session2_after_failed.enable
transfer.blind_tran_on_hook_enable
transfer.on_hook_trans_enable
transfer.tran_others_after_conf_enable

Parameter	Permitted Values	Default	Description

features.transfer.allow	**0**-Disabled, call transfer feature is not available to users. **1**-Enabled	1	It enables or disables the call transfer feature.
transfer.semi_attend_tran_enable	**0**-Disabled, when the user presses the TRAN key after hearing the ringback tone, the phone will blind transfer the call. **1**-Enabled, when the user presses the TRAN key after hearing the ringback tone, the phone will transfer the call after the transferee answers the call.	1	It enables or disables the semi-attended transfer.
account.X.transfer_refer_to_contact_header.enable[1]	**0**-Disabled **1**-Enabled	1	It enables or disables the Refer-To header to use the information of the Contact header in the second 200 OK message when attended transfer.
features.transfer_keep_session2_after_failed.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to keep the original call status after the server rejects the semi-attended/attended transfer.
transfer.blind_tran_on_hook_enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to complete the blind transfer through on-hook besides pressing the TRAN key. **NOTE** Blind transfer means transferring a call directly to another party without consulting.
transfer.on_hook_trans_enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to complete the semi-attended/attended transfer through on-hook besides pressing the TRAN key. **NOTE** Semi-attended transfer means transferring a call after hearing the ringback tone; Attended transfer means transferring a call with prior consulting.

transfer.tran_others_after_conf_enable	**0**-Disabled **1**-Enabled	0	1.It enables or disables the phone to transfer the local conference call to the other two parties after the conference initiator drops the local conference call. **NOTE** It works only if "account.X.conf_type" is set to 0 (Local Conference)

[1] X is the account ID.

Do Not Disturb (DND)

Introduction

DND feature enables the phone to reject incoming calls automatically when you do not want to be interrupted. You can choose to implement DND locally on the phone or on the server-side.

DND Settings Configuration

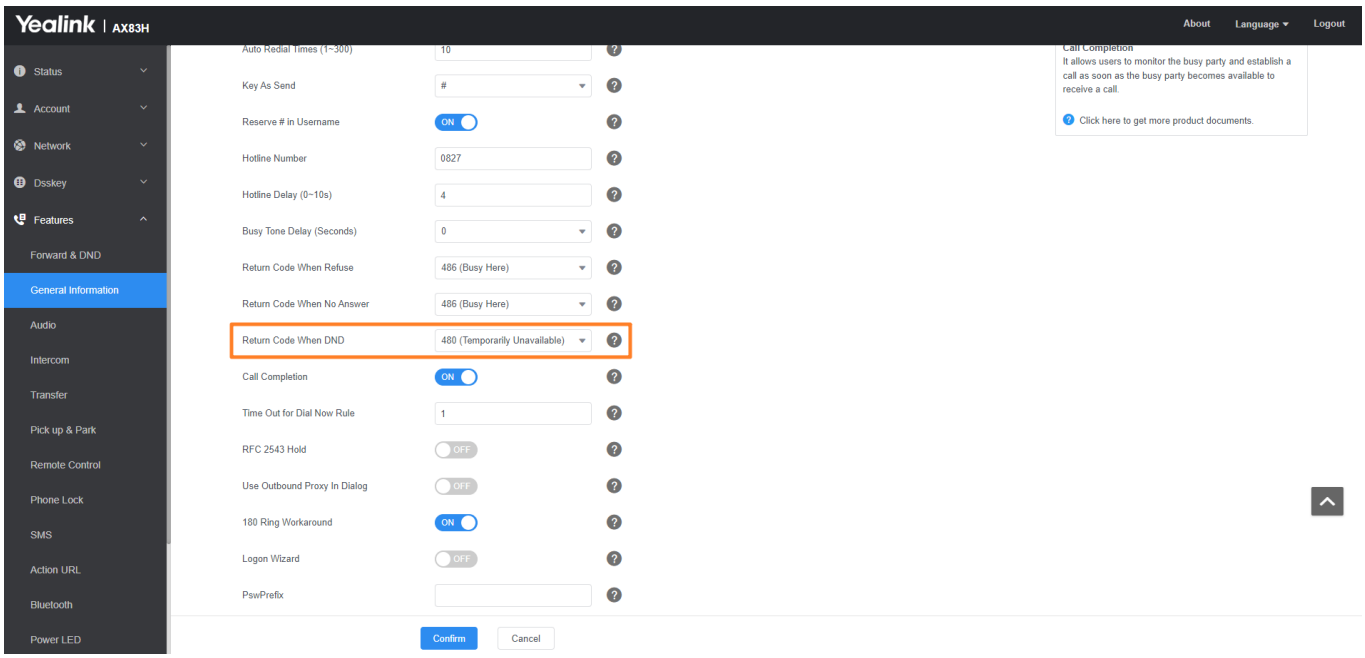
You can change the following DND settings:

- Enable or disable the DND feature. If disabled, the users have no permission to configure DND on their phones.
- Define the return code and the reason of the SIP response message for a rejected incoming calwhen DND is activated. The caller’ s phone screen displays the received return code.

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

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Return Code When DND**.



Configuration Parameter

```
features.dnd.allow
features.dnd_refuse_code
```

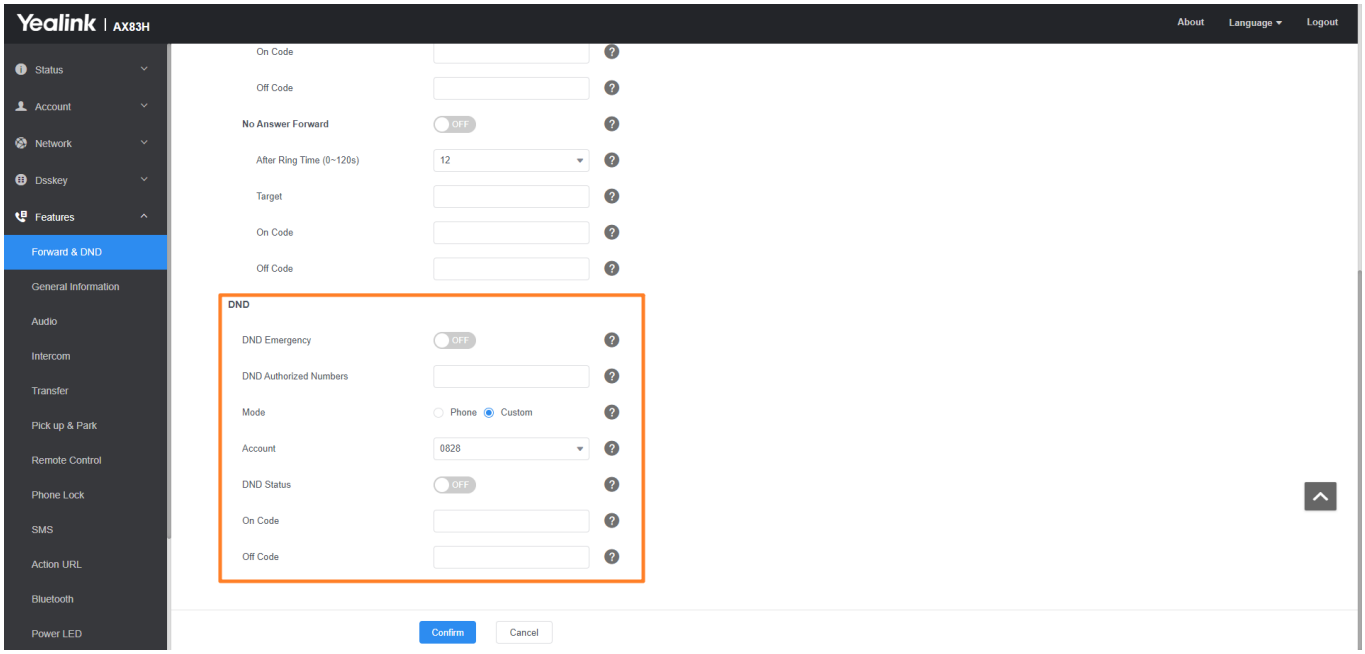
Parameter	Permitted Values	Default	Description
features.dnd.allow	**0**-Disabled, DND cannot be activated and users are not allowed to configure DND on the phone. **1**-Enabled	1	It enables or disables the DND feature.
features.dnd_refuse_code	**404**-Not Found **480**-Temporarily Unavailable **486**-Busy Here, the caller’ s phone screen will display the reason “Busy Here” when the callee enables DND feature. **603**-Decline	480	It configures a return code and reason of SIP response messages when rejecting an incoming call by DND. A specific reason is displayed on the caller’ s phone screen. **ⓘ NOTE** It works only if `features.dnd.allow` is set to 1 (Enabled).

DND Feature Configuration

Yealink phones support DND on code and off code to activate and deactivate server-side DND features. They may vary on different servers.
The following table lists the parameters you can use to configure DND.

Set via the Web User Interface

1. On the web user interface, go to **Features** > **Forward & DND** > **DND**.



Configuration Parameter

```
account.X.dnd.enable
account.X.dnd.on_code
account.X.dnd.off_code
```

Parameter	Permitted Values	Default	Description
account.X.dnd.enable[1]	**0**-Off **1**-On, the phone will reject incoming calls on account X.	0	It triggers the DND feature to on or off. **ⓘ NOTE** It works only if `features.dnd.allow` is set to 1 (Enabled) and `features.dnd_mode` is set to 1 (Custom).

account.X.dnd.on_code[1]	String within 32 characters	Blank	It configures the DND on code to activate the server-side DND feature. The phone will send the DND on code to the server when you activate the DND feature on the phone. **NOTE** It works only if features.dnd.allow is set to 1 (Enabled) and features.dnd_mode is set to 1 (Custom).
account.X.dnd.off_code[1]	String within 32 characters	Blank	It configures the DND off code to deactivate the server-side DND feature. The phone will send the DND off code to the server when you deactivate the DND feature on the phone. **NOTE** It works only if features.dnd.allow is set to 1 (Enabled) and features.dnd_mode is set to 1 (Custom).

[1] X is the account ID.

DND Synchronization for Server-side Configuration

DND synchronization feature provides the capability to synchronize the status of the DND features between the IP phone and the server.
If the DND is activated in phone mode, the DND status changing locally will be synchronized to all registered accounts on the server; but if the DND status of a specific account is changed on the server, the DND status locally will be changed.
The following table lists the parameters you can use to configure DND synchronization for server-side.

Configuration Parameter

```
features.feature_key_sync.enable
account.X.dnd.feature_key_sync.enable
```

Parameter	Permitted Values	Default	Description

features.feature_key_sync.enable	**0**-Disabled **1**-Enabled, the phone sends a SUBSCRIBE message with event "as-feature-event".	0	It enables or disables to synchronize the feature status between the IP phone and the server.
account.X.dnd.feature_key_sync.enable[1]	**0**-Disabled **1**-Enabled, server-based DND is enabled. Server and local phone DND are synchronized.	Blank	It enables or disables the DND feature synchronization for account X. **NOTE** The value configured by this parameter takes precedence over that configured by the parameter `features.dnd.feature_key_sync.enable`. It works only if `account.X.feature_key_sync.enable` is set to 1 (Enabled).

[1] X is the account ID.

No Answer

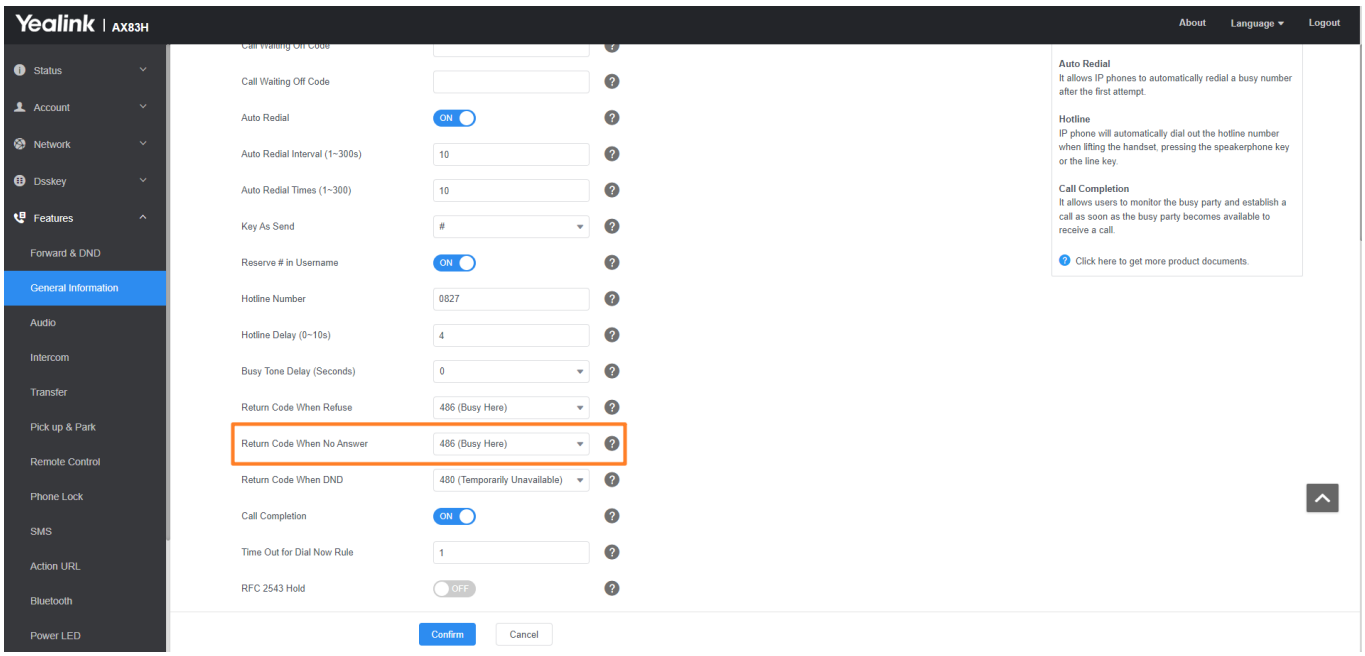
Introduction

No answer enables the phone to reply to the caller with the return code and reason when the handset does not answer an incoming call.

No Answer Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Return Code When No Answer**.



Configuration Parameter

Permitted Values	Default	Description
404-Not Found **480**-Temporarily Unavailable **486**-Busy Here **600**-Busy Everywhere **603**-Decline	486	It configures a return code and reason of response messages when the handset does not answer an incoming call.

Conference

Introduction

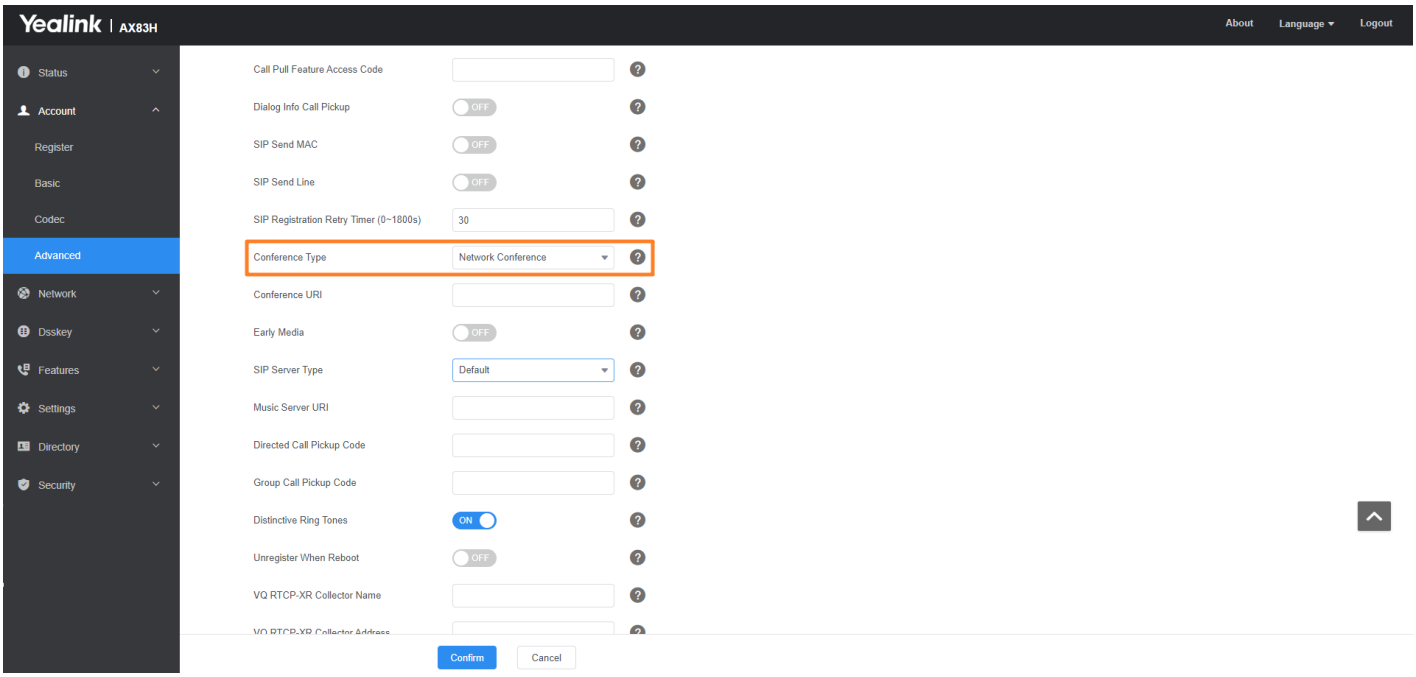
The Yealink phones support local conferences and network conferences.

Conference Type Configuration

You can specify which type of conference to establish.

Set via the Web User Interface

1. On the web user interface, go to **Account** > **Advanced** > **Conference Type**.



Configuration Parameter

account.X.conf_type

Parameter	Permitted Values	Default	Description
account.X.conf_type[1]	**0**-Local Conference **2**-Network Conference	0	It configures the conference type for a specific account.
account.x.local_conf.transfer_mode	**0**-Disabled **1**-Enabled	0	It is used to configure whether to enable the Transfer on Conference Hang up feature for 4-way and above.

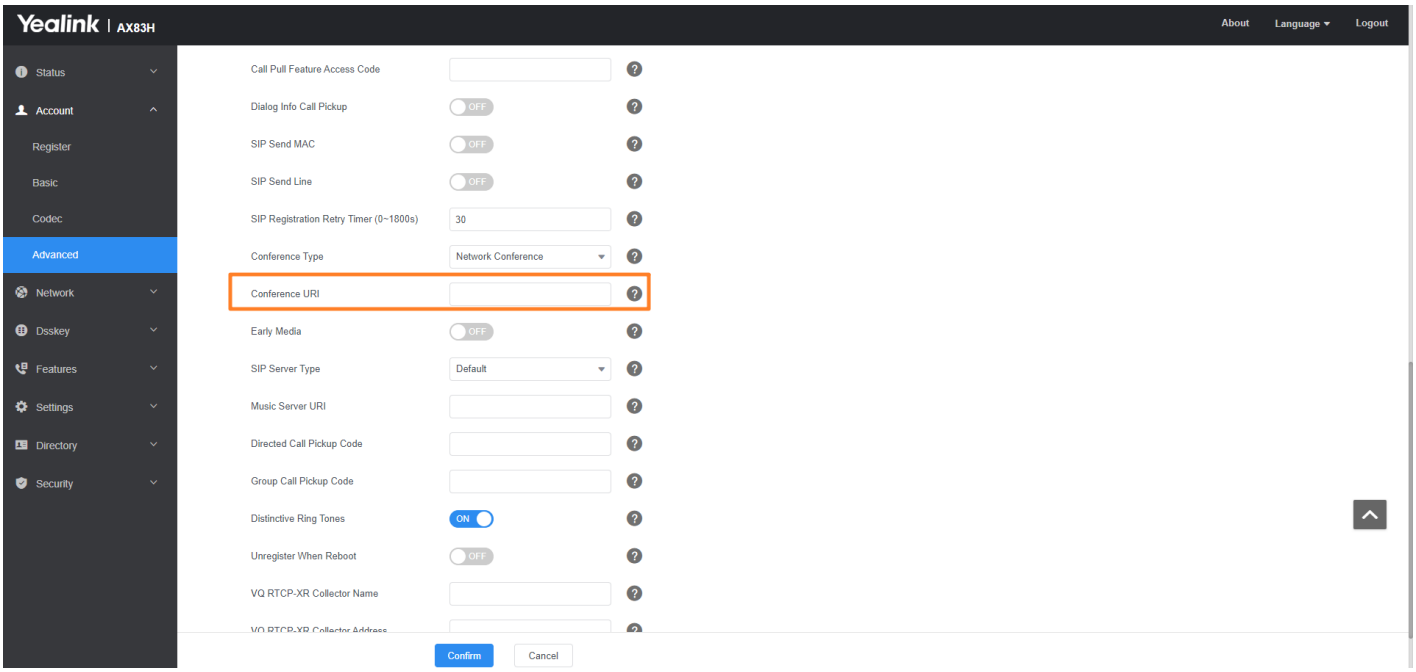
[1] X is the account ID.

Network Conference Configuration

Network conference, also known as a centralized conference, provides you with the flexibility of calling multiple participants (more than three). The phones implement network conferences using the REFER method specified in RFC 4579. This feature depends on the support from a SIP server.
For network conferences, if any party leaves the conference, the remaining parties are still connected.

Set via the Web User Interface

1. On the web user interface, go to **Account** > **Advanced** > **Conference URI**.



Configuration Parameter

account.X.conf_uri

Parameter	Permitted Values	Default	Description
account.X.conf_uri[1]	SIP URI within 511 characters	Blank	It configures the network conference URI for a specific account. **NOTE** It works only if account.X.conf_type is set to 2 (Network Conference).
account.x.conf_member.mode	0: Does not retrieve participant information. 1: Retrieves participant information through subscription.	0	Methods of retrieving participant information. You can enable this configuration to enable the function of kicking out participants.

Local Conference Configuration

The local conference requires a host phone to process the audio of all parties. Yealink phones support up to 3 parties (5 parties for CP930W/CP935W)(including yourself) in a local conference call.

Configuration Parameter

```
transfer.tran_others_after_conf_enable
```

Parameter	Permitted Values	Default	Description
transfer.tran_others_after_conf_enable	**0**-Disabled, all parties are disconnected when the conference initiator drops the conference call. **1**-Enabled, the other two parties remain connected when the conference initiator drops the conference call.	0	It enables or disables the phone to transfer the local conference call to the other two parties after the conference initiator exits the local conference call. **NOTE** It works only if `account.X.conf_type` is set to 0 (Local Conference).

Multicast Paging

Introduction

Multicast Paging allows you to easily and quickly broadcast instant audio announcements to users who are listening to a specific multicast group on a specific channel.
Yealink phones support the following 31 channels:

- **0**: Broadcasts are sent to channel 0. Note that the Yealink phones running old firmware versions (an old paging mechanism) can be regarded as listening to channel 0. It is the default channel.
- **1 to 25**: Broadcasts are sent to channels 1 to 25. We recommend that you specify these channels when broadcasting with Polycom phones which have 25 channels you can listen to.
- **26 to 30**: Broadcasts are sent to channels 26 to 30.

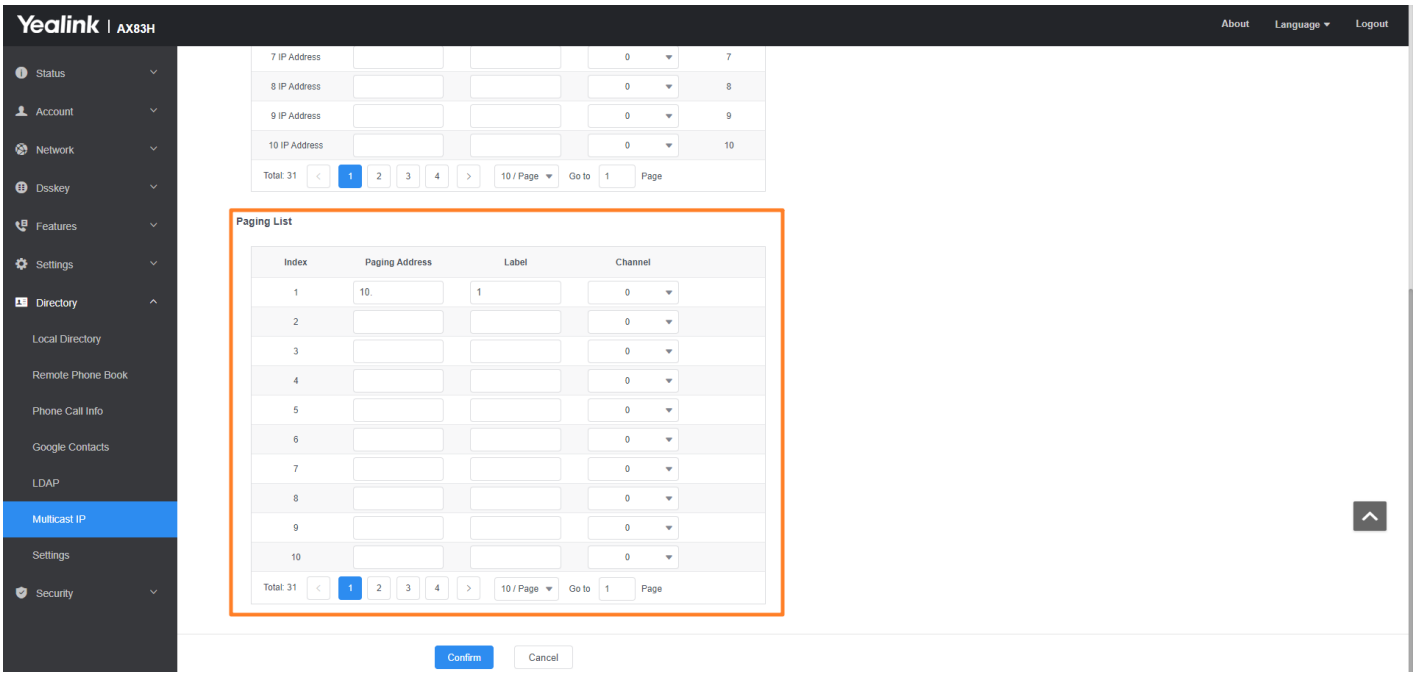
The phones can only send and receive broadcasts to/from the listened channels. Other channels' broadcasts will be ignored automatically by the IP phone.

Multicast Paging Group Configuration

Yealink phones support up to 31 groups for paging. You can assign a multicast IP address with a channel for each group, and specify a label to each group to identify the phones in the group, such as All, Sales, or HR.

Set via the Web User Interface

1. On the web user interface, go to **Directory** > **Multicast IP** > **Paging List** > **Paging Address**/**Label**/**Channel**.



Configuration Parameter

features.send_paging.enable
multicast.paging_address.X.ip_address
multicast.paging_address.X.label
multicast.paging_address.X.channel

Parameter	Permitted Values	Default	Description
features.send_paging.enable	**0**: Disable **1**: Enable	1	Configure whether to enable Paging and Paging List features. **NOTE** If set to 0, it will synchronize the hiding of functionality entrances on both the LCD interface and the web interface.
multicast.paging_address.X.ip_address[1]	IP address: port (224.0.0.1-239.255.255.255 port: 0-65535)	Blank	It configures the IP address and port number of the multicast paging group in the paging list.
multicast.paging_address.X.label[1]	String	Blank	It configures the name of the multicast paging group to be displayed in the paging list. It will be displayed on the phone screen when placing the multicast paging calls.

multicast.paging_address.X.channel[1]	**0**-all the Yealink phones running old firmware version or Yealink phones listen to channel 0 or third-party available devices in the paging group can receive the RTP stream. **1 to 25**-the Polycom or Yealink phones preconfigured to listen to the channel can receive the RTP stream. **26 to 30**-the Yealink phones preconfigured to listen to the channel can receive the RTP stream.	0	It configures the channel of the multicast paging group in the paging list.

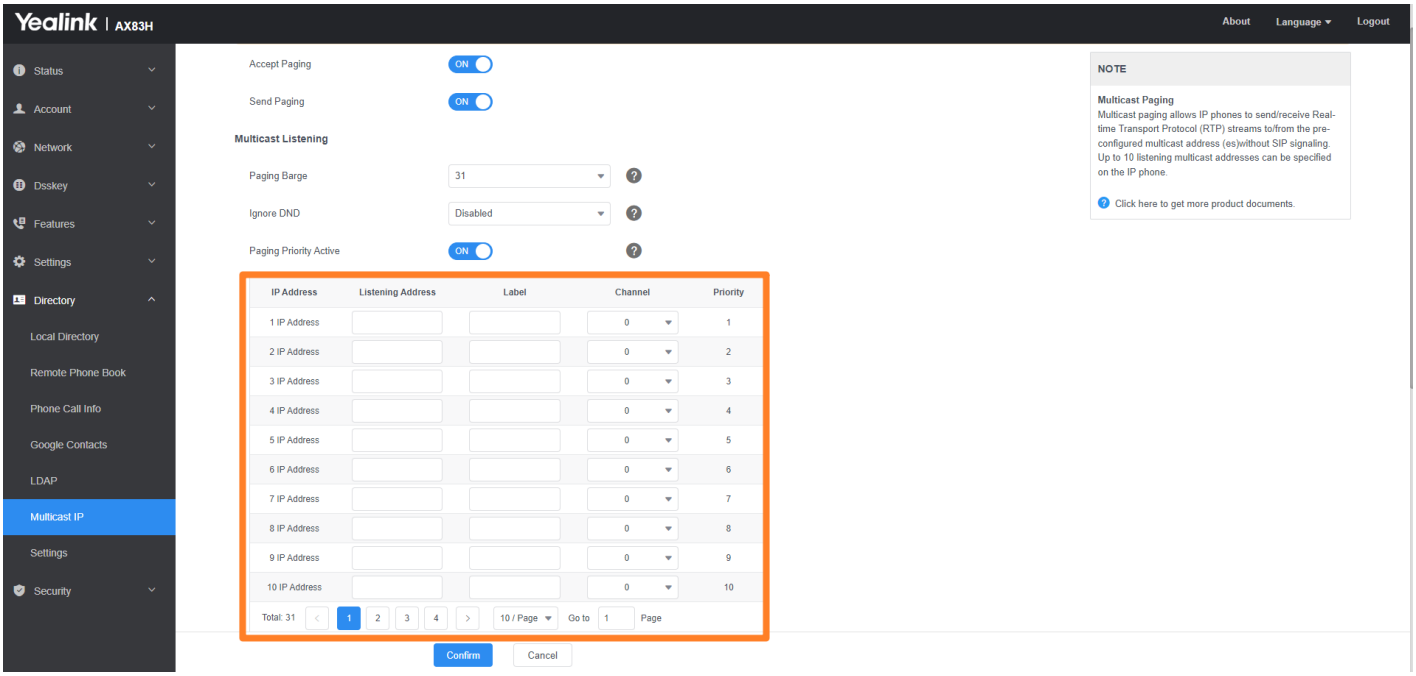
[1]X ranges from 1 to 31.

Multicast Listening Group Configuration

Yealink phones support up to 31 groups for listening. You can assign a multicast IP address with a channel for each group, and specify a label for each group to identify the phones in the group, such as All, Sales, or HR.

Set via the Web User Interface

1. On the web user interface, go to **Directory** > **Multicast IP** > **Multicast Listening**.



Configuration Parameter

```
features.accept_paging.enable
multicast.listen_address.X.ip_address
multicast.listen_address.X.label
multicast.listen_address.X.channel
```

Parameter	Permitted Values	Default	Description
features.accept_paging.enable	**0**-Disabled **1**-Enabled	1	It configure whether to enable the Multicast Listening feature. **NOTE** If set to 0, it will synchronize the hiding of functionality entrances on both the LCD interface and the web interface.
multicast.listen_address.X.ip_address[1]	IP address: port (224.0.0.1-239.255.255.255 port: 0-65535)	Blank	It configures the multicast address and port number that the phone listens to.
multicast.listen_address.X.label[1]	String within 99 characters	Blank	It configures the label to be displayed on the phone screen when receiving the multicast paging calls.
multicast.listen_address.X.channel[1]	**0**-the phone can receive an RTP stream of the pre-configured multicast address from the phones running old firmware version, from the phones listen to the channel 0, or from the available third-party devices. **1 to 25**-the phone can receive an RTP stream of the pre-configured multicast address on the channel 1 to 25 respectively from Yealink or Polycom phones. **26 to 30**-the phone can receive the RTP stream of the pre-configured multicast address on the channel 26 to 30 respectively from Yealink phones.	0	It configures the channel that the phone listens to.

[1]X ranges from 1 to 31.

Multicast Paging Settings

You can configure some general settings for multicast paging, for example, specify a codec, and configure the volume and audio device for listening to a paging call.

By default, all the listening groups are considered with a certain priority from 1 (lower priority) to 31 (higher priority). If you neither want to receive some paging calls nor miss urgent paging calls when there is a voice call or paging call, or when DND is activated, you can use the priority to define how your phone handles different incoming paging calls.

Paging Barge

You can set your phone to see whether an incoming paging call interrupts an active call.

The **Paging Barge** defines the lowest priority of the paging group from which the phone can receive a paging call when there is a voice call (a normal phone call rather than a multicast paging call) in progress. You can specify a priority so that the incoming paging calls with higher or equal priority are automatically answered, and the lower ones are ignored.

If it is disabled, all incoming paging calls will be automatically ignored.

Paging Priority

You can set your phone to see whether a new incoming paging call interrupts a current paging call.

The **Paging Priority** feature decides how the phone handles incoming paging calls when there is already a paging call on the phone. If enabled, the phone will ignore incoming paging calls with lower priorities, otherwise, the phone will answer incoming paging calls automatically and place the previous paging call on hold. If disabled, the phone will automatically ignore all incoming paging calls.

Ignore DND

If you do not want to miss some urgent paging calls when DND is activated. You can use the Ignore DND feature to define the lowest priority of the paging group from which the phone can receive an urgent paging call when DND is activated. You can specify a priority so that the incoming paging calls with higher or equal priority are automatically

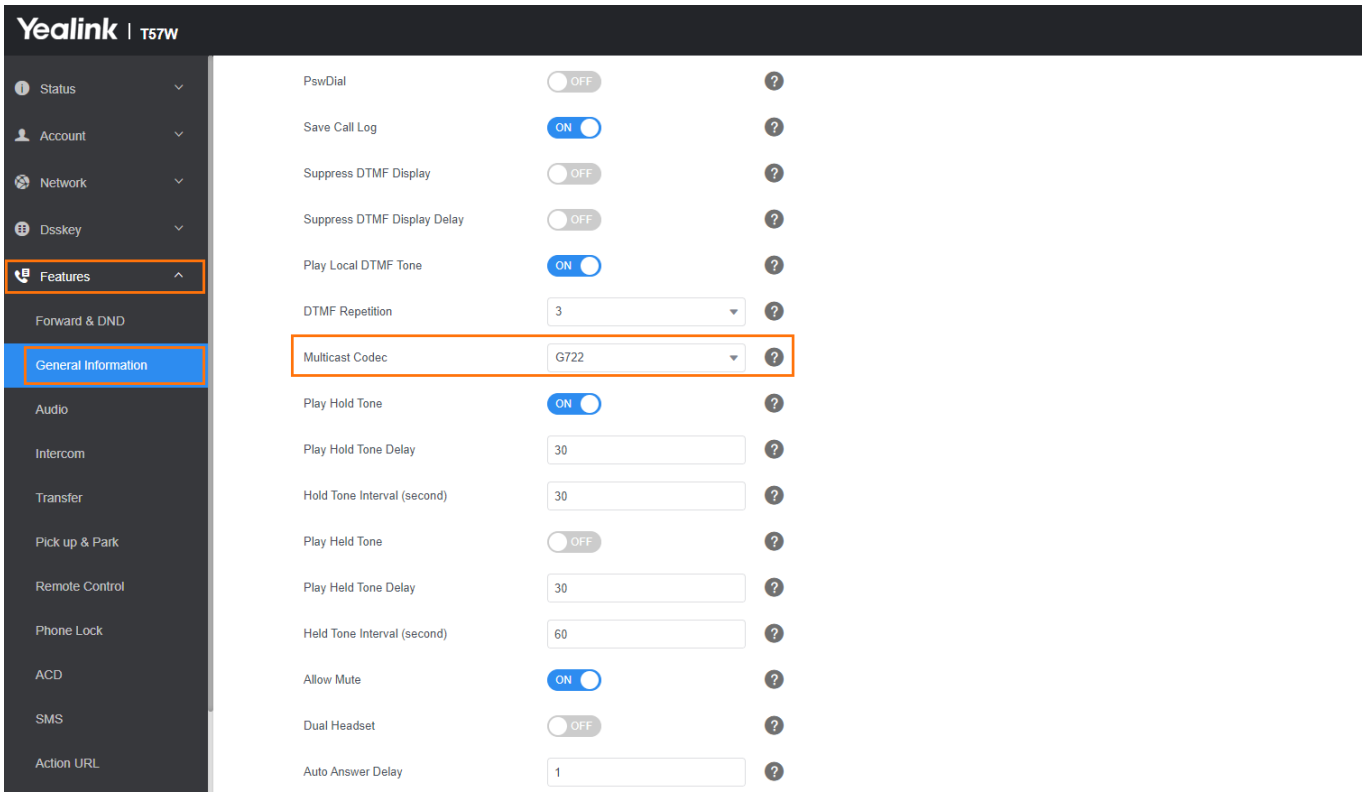
answered, and the lower ones are ignored.

If it is disabled, all the incoming paging calls will be ignored when DND is activated in phone mode.

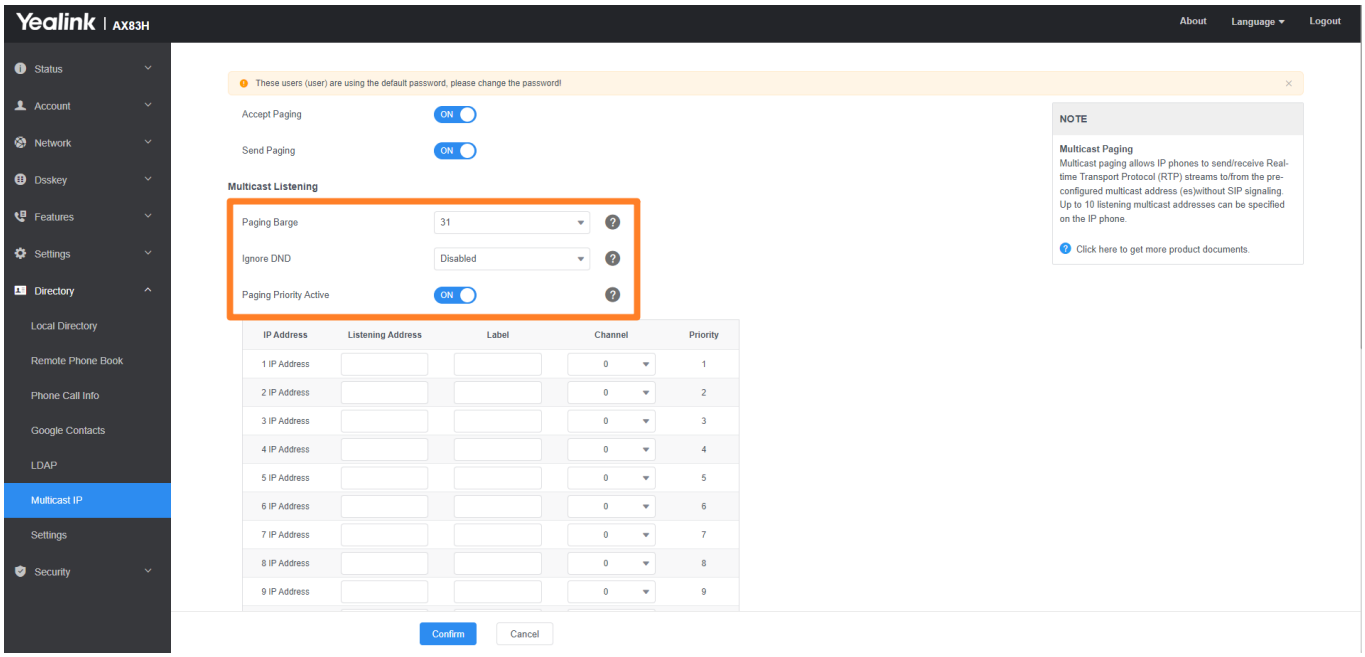
Multicast Paging Settings Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Multicast Codec**.



2. On the web user interface, go to **Directory** > **Multicast IP** > **Ignore DND**/**Paging Priority Active**/**Paging Barge**.



Configuration Parameter

multicast.codec
multicast.receive_priority.enable
multicast.receive_priority.priority
multicast.receive.ignore_dnd.priority
multicast.listen_address.X.volume
multicast.receive.use_speaker
multicast.paging.timeout
multicast.auto_end.popup_timeout

Parameter	Permitted Values	Default	Description
multicast.codec	PCMU, PCMA, G729, G722	G722	It configures the codec for multicast paging.
multicast.receive_priority.enable	**0**-Disabled, the phone will ignore the incoming multicast paging calls when there is an active multicast paging call on the phone. **1**-Enabled, the phone will receive the incoming multicast paging call with a higher priority and ignore the one with a lower priority.	1	It enables or disables the phone to handle the incoming multicast paging calls when there is an active multicast paging call on the phone.
multicast.receive_priority.priority	**0**-Disabled, all incoming multicast paging calls will be automatically ignored when a voice call is in progress. **1**-1 **2**-2 **3**-3 … **31**-31 If it is set to other values, the phone will receive the incoming multicast paging call with a higher or equal priority and ignore the one with a lower priority when a voice call is in progress.	31	It configures the priority of the voice call (a normal phone call rather than a multicast paging call) in progress. 1 is the highest priority, 31 is the lowest priority.
multicast.receive.ignore_dnd.priority	**0**-Disabled, all incoming multicast paging calls will be automatically ignored when DND is activated in phone mode. **1**-1 **2**-2 **3**-3 … **31**-31 If it is not set to 0 (Disabled), the phone will receive the incoming multicast paging call with a higher or same priority than this value and ignore that with a lower priority than this value when DND is activated in phone mode.	0	It configures the lowest priority of the multicast paging call that can be received when DND is activated in phone mode. 1 is the highest priority, and 31 is the lowest priority.

multicast.listen_address.X.volume [1]	Integer from 0 to 15	0	It configures the volume of the speaker when receiving the multicast paging calls. If it is set to 0, the current volume of the speaker takes effect. The volume of the speaker can be adjusted by pressing the Volume key in advance when the phone is on a call. You can also adjust the volume of the speaker during the paging call. If it is set to 1 to 15, the configured volume takes effect and the current volume of the speaker will be ignored. You are not allowed to adjust the volume of the speaker during the paging call.
multicast.receive.use_speaker	**0**-Disabled, the engaged audio device will be used when receiving the multicast paging calls. **1**-Enabled	0	It enables or disables the phone to always use the speaker as the audio device when receiving multicast paging calls.
multicast.paging.timeout	**0**-Disabled **1-1440:** Customize the timeout duration, with a maximum of 1 day, in minutes (min).	0	Control the timeout duration for multicast paging. After reaching the timeout duration, a pop-up window will prompt the user to turn off multicast.
multicast.auto_end.popup_timeout	**0-3600:** In second (s) **NOTE** If configured as 0, the multicast will be exited directly without any pop-up window.	60s	Configure the duration of the multicast timeout pop-up window. If the time exceeds this duration and the user does not choose to continue with multicast, the multicast will be automatically closed.>

[1]X ranges from 1 to 31.

FAQ

1. How to set paging priority when DND

Call Mute

Call Mute

You can mute the microphone of the active audio device (handset, headset or speakerphone) on Yealink phones during an active call or when the phone is on the pre-dialing/dialing/calling/ringing screen. The call is automatically muted when setting up successfully. Muting before a call is answered prevents the other party from hearing the local discussion.
You can activate the mute feature by pressing the MUTE key. Normally, the mute feature is automatically deactivated when the active call ends. You can use the keep mute feature to keep the mute state persisting across the calls.

Microphone Mute Configuration

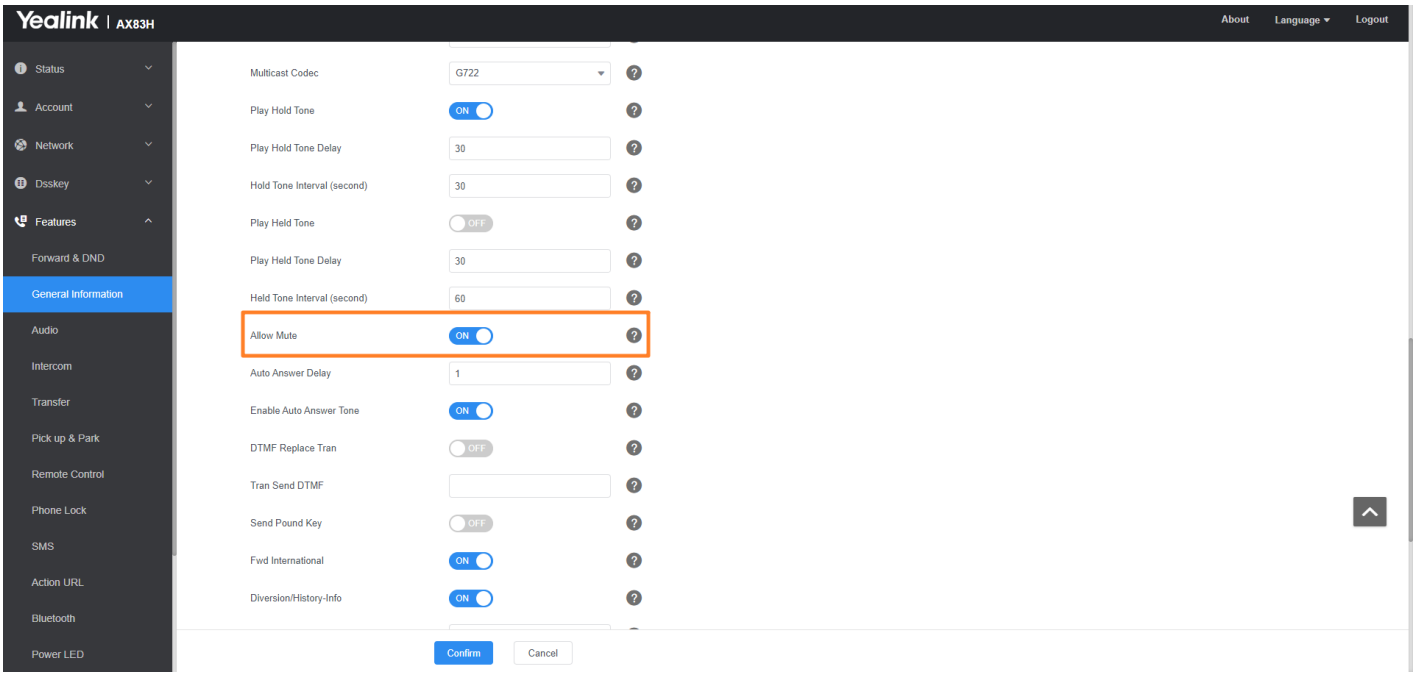
The following table lists the parameters you can use to configure the microphone mute feature.
Configuration Parameter

```
features.allow_mute
```

Parameter	Description	Permitted Values	Default
features.allow_mute	It enables or disables the allow mute feature for the phone.	**0**-Disabled **1**-Enabled, you are allowed to mute an active call or activate the mute feature on the pre-dialing/dialing/calling/ringing screen.	1

Set via the Web User Interface

On the web user interface, go to: **Features** > **General Information** > **Allow Mute**



Keep Mute

Keep mute, also known as persistent mute, allows you to keep the mute state persisting across calls.
In a call center or meeting room, if incoming calls are answered automatically, the callers may hear the local discussion. Therefore, you can mute the phone in an idle state to prevent an unintended situation. The mute state persists across calls until you unmute the microphone manually or until the phone restarts.
You can activate the mute feature by pressing the MUTE key in the idle/pre-dialing/dialing/ringing/calling/talking state.

Keep Mute Configuration

The following table lists the parameters you can use to enable or disable keep mute.

Configuration Parameter

```
features.keep_mute.enable
features.keep_mute.mode
```

Parameter	Description	Permitted Values	Default
features.keep_mute.enable	It configures the keep mute feature. **NOTE** It works only if "features.allow_mute" is set to 1 (Enabled).	**0**-The mute feature is automatically deactivated when the active call ends. **1**-The mute state is kept until you change the mute state manually or the phone restarts.	0
features.keep_mute.mode	It configures the keep mute mode.	**1**-Represents entering the continuous mute mode, but the Mute key can still be operated to enter or exit continuous mute mode on the idle screen. **2**- Represents entering the permanent mute mode, which means that users cannot exit continuous mute mode through the Mute key on the idle screen. However, during a call, the call is initially muted by default, and pressing the Mute key can unmute the call. Pressing the Mute key again will return to mute mode. After the call ends, it returns to continuous mute mode.	0

Mute Alert Tone

You can configure the phone to play an audible tone if the mute status of the phone is changed. This allows you to know if your phone is in the mute or un-mute state. In addition, you can set a periodic reminder which plays the audible tone periodically when the phone is in the mute state. The time interval must not be less than 3 seconds.

Mute Alert Tone Configuration

The following table lists the parameters you can use to configure the mute alert tone feature.

Configuration Parameter

```
features.play_mute_tone.enable
features.play_mute_tone.interval
```

Parameter	Description	Permitted Values	Default
features.play_mute_tone.enable	It enables or disables the phone to play an audible tone when the mute status is changed.	**0**-Disabled **1**-Enabled	0
features.play_mute_tone.interval	It configures a time interval (in seconds) for playing an audible tone when the phone is in the mute state during the call.	Integer from 3 to 3600	5

Security Features

User and Administrator Identification

Introduction

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

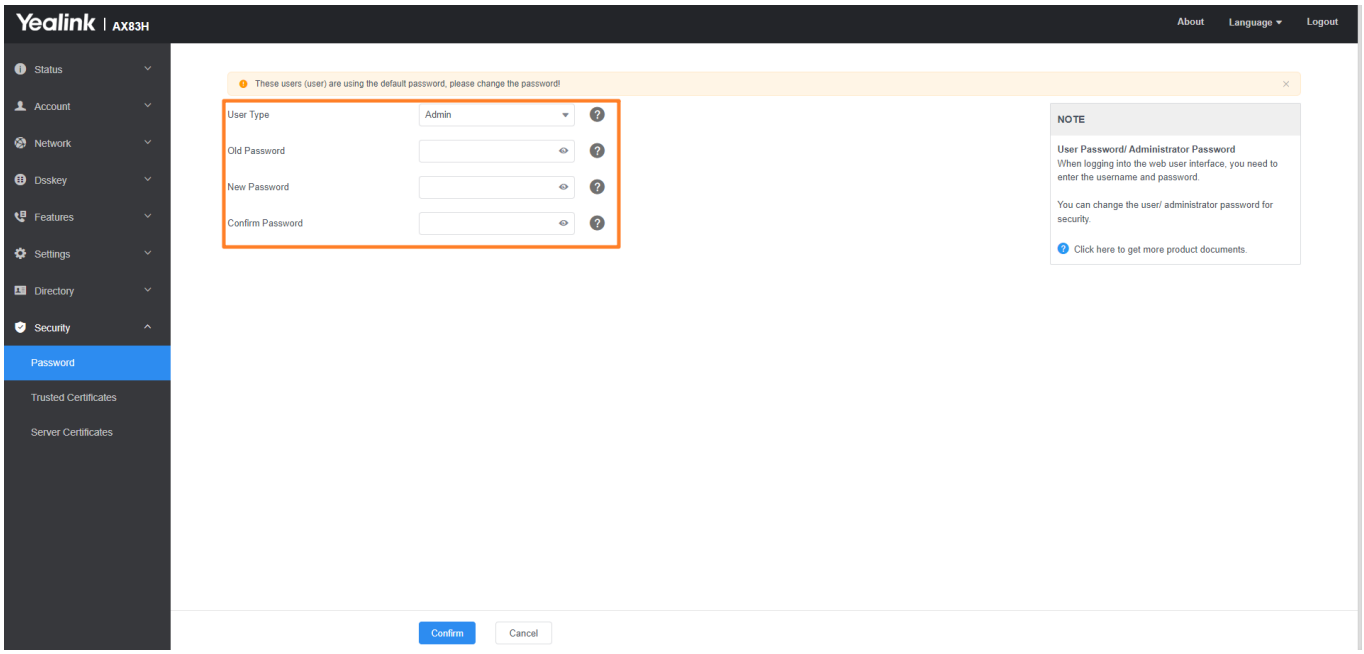
When logging into the web user interface or accessing advanced settings on the phone, as an administrator, you need an administrator password to access various menu options. The default username and password for administrator is "**admin**". Both you and the user can log into the web user interface,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

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

User and Administrator Identification Configuration

Set via the Web User Interface

1. On the web user interface, go to **Security** > **Password**.



Configuration Parameter

```
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
static.security.password_use_default.mode
```

Parameter	Permitted Values	Default	Description
static.security.user_name.user	String within 32 characters	user	It configures the user name for the user to access the phone's web user interface.
static.security.user_name.admin	String within 32 characters	admin	It configures the user name for the administrator to access the phone's web user interface.
static.security.user_name.var	String within 32 characters	var	It configures the user name for the var to access the phone's web user interface. **NOTE** It works only if "static.security.var_enable" is set to 1 (Enabled).

static.security.user_password	String within 32 characters	Blank	It configures the password. The phone uses “user” as the default user password, "var" as the default var password and “admin” as the default administrator password. The valid value format is :. **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. `static.security.user_password = var:789` means setting the password of var to 789. **NOTE** The phones support ASCII characters 32-126(0x20-0x7E) in passwords. If you want to set space and colon characters in the password, you need to configure it via the web user interface. You can set the password to be empty via the web user interface only.
static.security.custom_password_rule.X	regular expression（x:1-10）	Blank	The regular expression rules for user-defined security passwords, if there are multiple rules, require the password to satisfy all rules simultaneously.

static.security.password_use_default.mode	0: Default mode, allows users to use default passwords. 1: Force mode, mandates users to change default passwords; both web and LCD interfaces require password modification before use. 2: Semi-force mode, compels users to change the default password when logging in via the web interface; the LCD interface can be used without changing the password. 3: Semi-force mode, requires users to change the default password when logging in via the web interface; the LCD interface enforces password change only upon entering advanced settings.	0	Used to configure whether administrators and users can utilize default passwords.

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

User Access Level Configuration

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

Configuration Parameter

```
static.security.var_enable
static.web_item_level.url
static.security.default_access_level
```

Parameter	Permitted Values	Default	Description
static.security.var_enable[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the 3-level access permissions (admin, user, var).
static.web_item_level.url[1]	URL within 511 characters	Blank	It configures the access URL of the file, which defines 3-level access permissions.
static.security.default_access_level[1]	**0**-user **1**-var **2**-admin	0	It configures the default access level to access the handset user interface. **NOTE** It works only if `static.security.var_enable` is set to 1 (Enabled).

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

Auto Logout Time

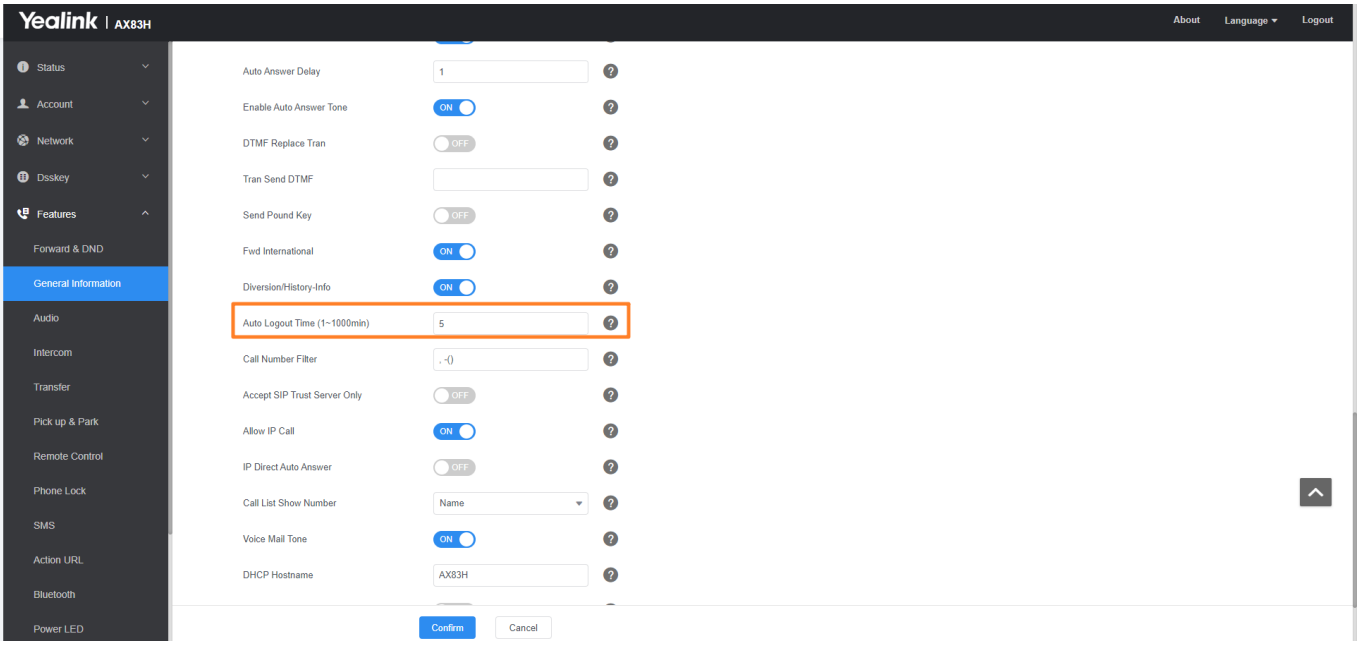
Introduction

Auto logout time defines how long the phone will log out of the web user interface automatically when you do not perform any actions on the web user interface. Once logging out, you must re-enter your username and password for web access authentication.

Auto Logout Time Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Auto Logout Time(1~1000min)**.



Configuration Parameter

features.relog_offtime

Parameter	Permitted Values	Default	Description
features.relog_offtime	Integer from 1 to 1000	5	It configures the timeout interval (in minutes) for web access authentication

wui.login_wait_time	Integer from 1 to 120	15	It is used to configure the allowed duration before logging into the Web GUI configuration interface.
wui.stay_active_wait_time	Integer from 1 to 120	15	It is used to configure the allowed duration of inactivity after logging into the Web GUI configuration interface (unit: minutes).
wui.operate_wait_time	Integer from 1 to 120	15	t is used to configure the maximum allowed duration for operations after logging into the Web GUI configuration interface.

Phone Lock

Phone Lock

You can lock the phone to prevent it from unauthorized use. Once the IP phone is locked, anyone must enter the password to unlock it.
You can set a waiting time, after which the phone is locked automatically. If the waiting time is set to 0, the phone will not be automatically locked. You need to lock the phone manually.
When the phone is locked, you can still answer incoming calls and make emergency calls.

NOTE
The key and Speakerphone key are always available even when you lock the phone.

Phone Lock Configuration

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

Configuration Parameter

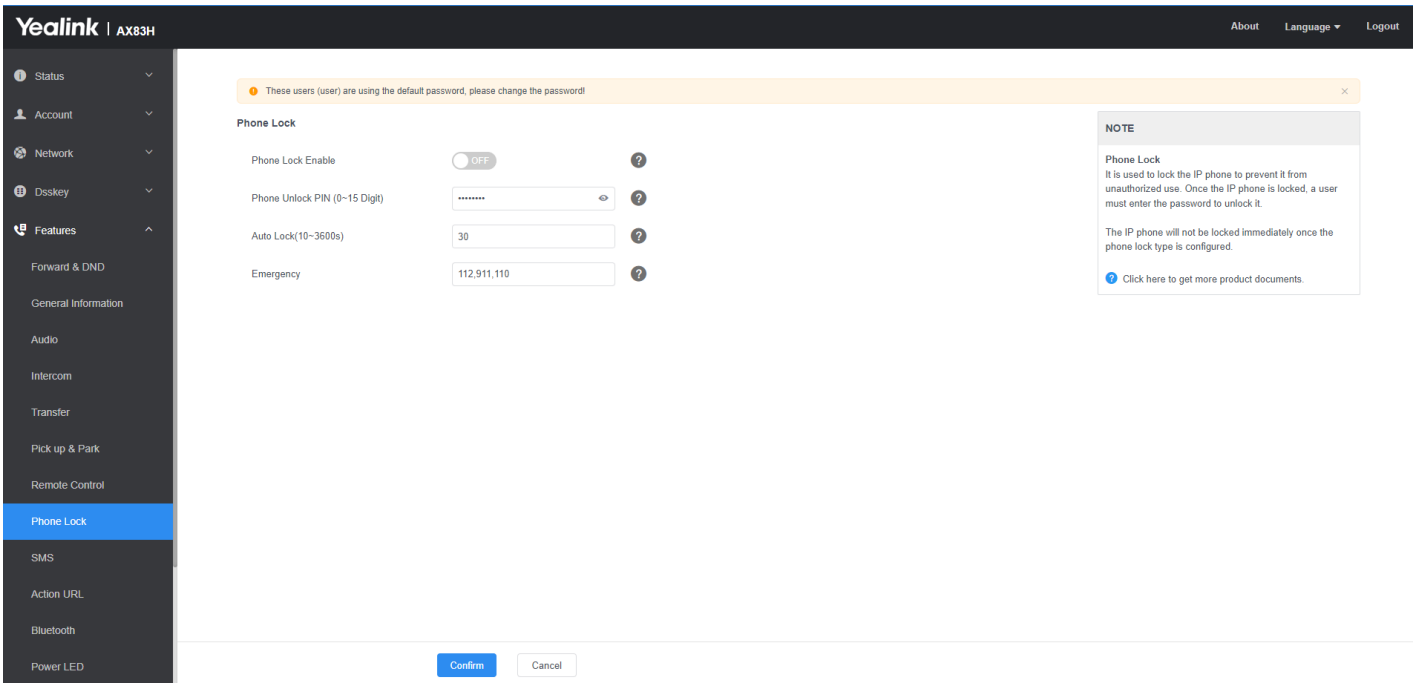
```
phone_setting.phone_lock.enable
phone_setting.phone_lock.unlock_pin
phone_setting.phone_lock.lock_time_out
phone_setting.emergency.number
```

Parameter	Description	Permitted Values	Default
phone_setting.phone_lock.enable	It enables or disables the phone lock feature.	0-Disabled 1-Enabled	0
phone_setting.phone_lock.unlock_pin	It configures the password for unlocking the phone.	Characters within 15 digits	Blank

phone_setting.phone_lock.lock_time_out	It configures the idle time (in seconds) before the phone is automatically locked. The default value is 30 (the phone is locked only by long pressing the # key). **ⓘ NOTE** It works only if "phone_setting.phone_lock.enable" is set to 1 (Enabled).	**0** or Integer from 10 to 3600	30
phone_setting.emergency.number	It configures emergency numbers. Multiple emergency numbers are separated by commas. **ⓘ NOTE** If "phone_setting.phone_lock.enable" is set to 1 (Enabled) and "phone_setting.phone_lock.lock_key_type" is set to 0 (All Keys), you are only allowed to dial the configured emergency numbers.	String within 99 characters	#########

Set via the Web User Interface

On the web user interface, go to **Features** > **Phone Lock**.



Transport Layer Security (TLS)

Introduction

TLS is a commonly used protocol for providing communications privacy and managing the security of message transmission, allowing the phones to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent the data from being eavesdropped and tampered.
Yealink phones support TLS version 1.2. When TLS is enabled for an account, the SIP message of this account will be encrypted, and a lock icon will appear on the LCD screen after the successful TLS negotiation.

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 phones support the following cipher suites:

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

- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC2-CBC-MD5
- EXP-RC4-MD5

Supported Trusted and Server Certificates

The IP phone can serve as a TLS client or a TLS server. In the TLS feature, we use the terms trusted and server certificate. These are also known as CA and device certificates.
The TLS requires the following security certificates to perform the TLS handshake:

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

The IP phone can authenticate the server certificate based on the trusted certificates list. The trusted certificates list and the server certificates list contain the default and custom certificates. You can specify the type of certificates the IP phone accepts: **default certificates**, **custom certificates** or **all certificates**.
The Common Name Validation feature enables the IP phone to mandatorily validate the common name of the certificate sent by the connecting server. The security verification rules are compliant with RFC 2818.

NOTE
Resetting the IP phone to factory defaults will delete custom certificates by default. However, this feature is configurable by the parameter `static.phone_setting.reserve_certs_enable` using the configuration file.

Supported Trusted Certificates

Yealink phones trust the following CAs by default:

- DigiCert High Assurance EV Root CA
- Deutsche Telekom Root CA 2
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure Global eBusiness CA-1
- GeoTrust Global CA
- GeoTrust Global CA2
- GeoTrust Primary Certification Authority
- GeoTrust Primary Certification Authority G2
- GeoTrust Universal CA
- GeoTrust Universal CA2
- Thawte Personal Freemail CA
- Thawte Premium Server CA
- Thawte Primary Root CA
- Thawte Primary Root CA - G2
- Thawte Primary Root CA - G3
- Thawte Server CA
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Universal Root Certification Authority
- ISRG Root X1 (Let’s Encrypt Authority X1 and Let’s Encrypt Authority X2 certificates are signed by the root certificate ISRG Root X1.)
- Baltimore CyberTrust Root
- DST Root CA X3
- Verizon Public SureServer CA G14-SHA2
- AddTrust External CA Root
- Go Daddy Class 2 Certification Authority
- Class 2 Primary CA
- Cybertrust Public SureServer SV CA
- DigiCert Assured ID Root G2
- DigiCert Assured ID Root G3
- DigiCert Assured ID Root CA
- DigiCert Global Root G2

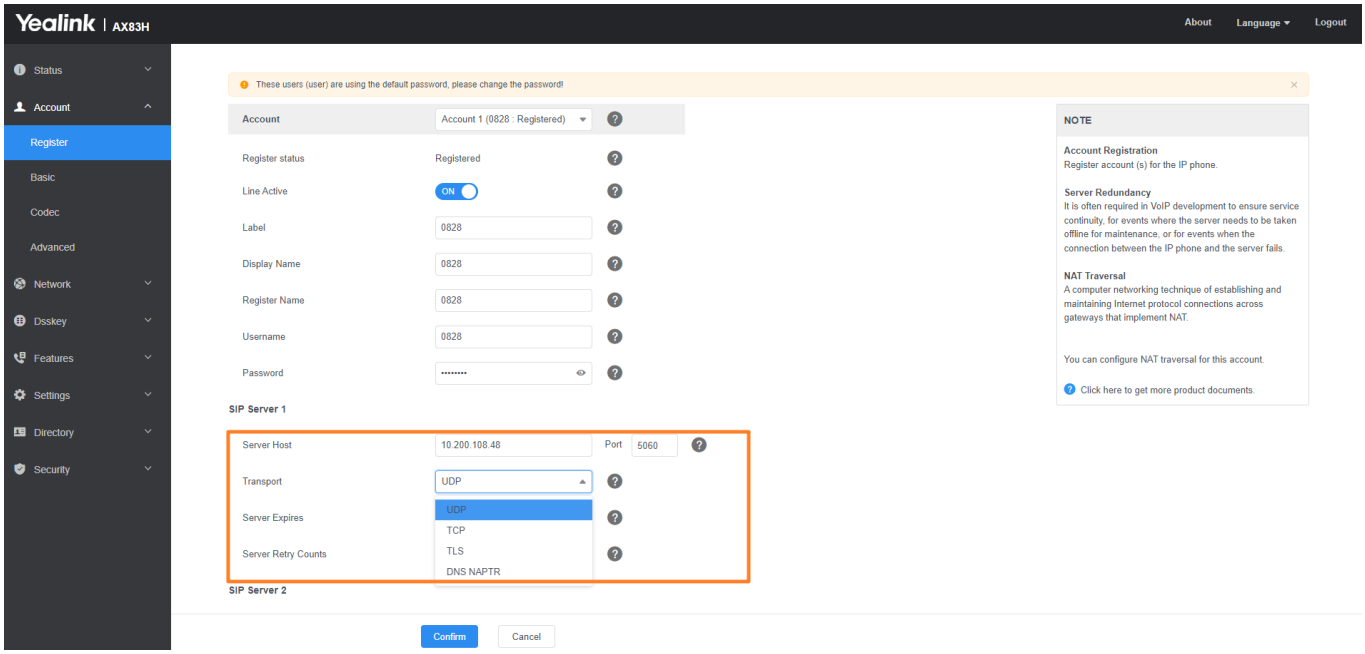
- DigiCert Global Root G3
- DigiCert Global Root CA
- DigiCert Trusted Root G4
- Entrust Root Certification Authority
- Entrust Root Certification Authority - G2
- Entrust.net Certification Authority (2048)
- GeoTrust Primary Certification Authority - G3
- GlobalSign Root CA
- GlobalSign Root CA - R2
- Starfield Root Certificate Authority - G2
- TC TrustCenter Class 2 CA II
- TC TrustCenter Class 3 CA II
- TC TrustCenter Class 4 CA II
- TC TrustCenter Universal CA I
- TC TrustCenter Universal CA III
- Thawte Universal CA Root
- VeriSign Class 3 Secure Server CA - G2
- VeriSign Class 3 Secure Server CA – G3
- Thawte SSL CA
- StartCom Certification Authority
- StartCom Certification Authority G2
- Starfield Services Root Certificate Authority - G2
- RapidSSL CA
- Go Daddy Root Certificate Authority - G2
- Cybertrust Global Root
- COMODOSSLCA
- COMODO RSA Domain Validation Secure Server CA
- COMODO RSA Certification Authority
- AmazonRootCA4
- AmazonRootCA3
- AmazonRootCA2
- AmazonRootCA1
- Yealink Root CA
- Yealink Equipment Issuing CA

NOTE
Yealink endeavors to maintain a built-in list of the 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 not in the list above, you can send a request to your local distributor. You can now upload your particular CA certificate into your phone.

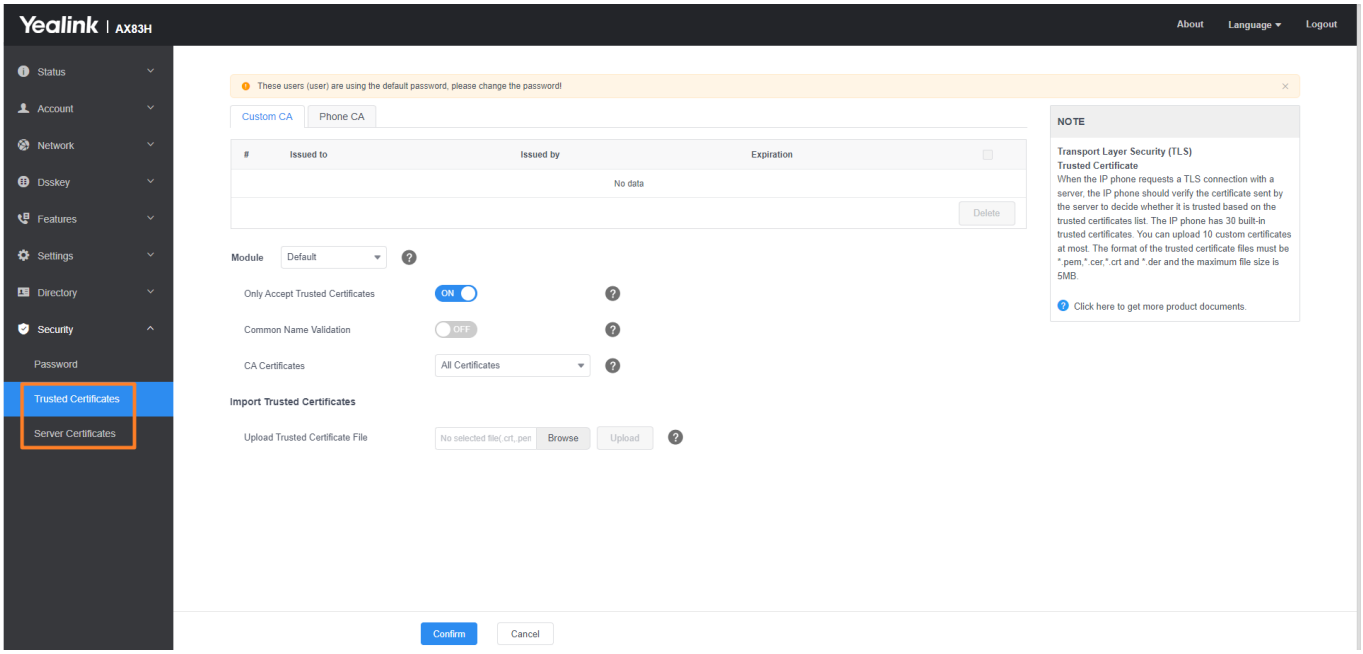
TLS Configuration

Set via the Web User Interface

1. On the web user interface, go to **Account** > **Register** > **SIP Server Y** > **Transport**.



2. On the web user interface, go to **Security** > **Trusted Certificates**/**Server Certificates**.



Configuration Parameter

account.X.sip_server.Y.transport_type
template.X.sip_server.Y.transport_type
static.security.default_ssl_method
static.security.server_ssl_method
static.security.trust_certificates
static.security.ca_cert
static.security.cn_validation
static.security.dev_cert
static.trusted_certificates.url
static.trusted_certificates.delete
static.server_certificates.url
static.server_certificates.delete
static.phone_setting.reserve_certs_enable
security.e911.ca_cert
security.e911.dev_cert
security.e911.cn_validation
security.e911.trust_certificates

Parameter	Permitted Values	Default	Description
account.X.sip_server.Y.transport_type[1] [2] template.X.sip_server.Y.transport_type[1] [2]	**0**-UDP **1**-TCP **2**-TLS **3**-DNS NAPTR, if no server port is given, the phone performs the DNS NAPTR and SRV queries for the service type and port.	0	It configures the type of transport protocol.
static.security.default_ssl_method[3]	**0**-TLS 1.0 **3**-SSL V23 (automatic negotiation with the server. The phone starts with TLS 1.2 for negotiation.) **4**-TLS 1.1 **5**-TLS 1.2 **6**-TLS 1.3	3	It configures the TLS version the phone uses to authenticate with the server.
static.security.server_ssl_method	**0**-TLS 1.0, TLS 1.1 and TLS 1.2 **1**-TLS 1.1 and TLS 1.2 **2**-TLS 1.2 **3**-TLS1.1, TLS1.2 and TLS1.3	1	It configures the supported TLS version to use for handshake negotiation between the phone and web browser.
static.security.trust_certificates[3]	**0**-Disabled **1**-Enabled, the phone will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, will the phone trust the server.	1	It enables or disables the phone to only trust the server certificates in the Trusted Certificates list.
static.security.ca_cert[3]	**0**-Default Certificates **1**-Custom Certificates **2**-All Certificates	2	It configures the type of certificates in the Trusted Certificates list for the phone to authenticate for TLS connection.

static.security.cn_validation[3]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server.
static.security.dev_cert[3]	**0**-Default Certificates **1**-Custom Certificates	0	It configures the type of device certificates for the phone to send for TLS authentication.
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. **NOTE** The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format.
static.trusted_certificates.delete	http://localhost/all: It deletes all uploaded trusted certificates.	Blank	It configures to delete all uploaded trusted certificates.
static.server_certificates.url	URL within 511 characters	Blank	It configures the access URL of the certificate the phone sends for authentication. **NOTE** The certificate you want to upload must be in *.pem or *.cer format.
static.server_certificates.delete	http://localhost/all	Blank	It deletes all uploaded server certificates.

static.phone_setting.reserve_certs_enable	**0**-Disabled **1**-Enabled	Blank	It enables or disables the phone to reserve custom certificates after it is reset to factory defaults.
security.e911.ca_cert	**0**-Default Certificates **1**-Custom Certificates **2**-All Certificates	Blank	It configures the type of certificates in the Trusted Certificates list for the desired module to authenticate for TLS connection.
security.e911.dev_cert	**0**-Default Certificates **1-5**-Custom Certificates	0	It configures the type of device certificates for the desired module to send for TLS authentication.
security.e911.cn_validation	**0**-Disabled **1**-Enabled	Blank	It enables or disables the desired module to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server.
security.e911.trust_certificates	**0**-Disabled **1**-Enabled, the desired module will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds will the desired module trust the server.	Blank	It enables or disables the desired module to only trust the server certificates in the Trusted Certificates list.

[1]X is the account ID.
[2]Y is the server ID. Y=1-2.

Secure Real-Time Transport Protocol (SRTP)

Introduction

Secure Real-Time Transport Protocol (SRTP) encrypts the audio streams during VoIP phone calls to avoid interception and eavesdropping. The parties participating in the call must enable the SRTP feature simultaneously. When this feature is enabled on both phones, the type of encryption to use for the session is negotiated between the phones. This negotiation process is compliant with RFC 4568.
When you place a call on the enabled SRTP phone, the phone sends an INVITE message with the RTP/RTCP encryption algorithm to the destination phone. As described in RFC 3711, RTP/RTCP streams may be encrypted using an AES (Advanced Encryption Standard) algorithm.
Example of the RTP encryption algorithm carried in the SDP of the INVITE message:

```
m=audio 11780 RTP/SAVP 0 8 18 9 101
a=crypto:1 AES_CM_128_HMAC_SHA1_80 > inline:NzFlNTUwZDk2OGVlOTc3YzNkYTkwZWVkMTM1YWFj
a=crypto:2 AES_CM_128_HMAC_SHA1_32 > inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWFm
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDliMWIzZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:9 G722/8000
a=fmtp:101 0-15
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

The callee receives the INVITE message with the RTP encryption algorithm and then answers the call by responding with a 200 OK message which carries the negotiated RTP encryption algorithm.
Example of the RTP encryption algorithm carried in the SDP of the 200 OK message:

```
m=audio 11780 RTP/SAVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NGY4OGViMDYzZjQzYTNiOTNkOWRiYzRlMjM0Yzcz
a=sendrecv
a=ptime:20
a=fmtp:101 0-15
```

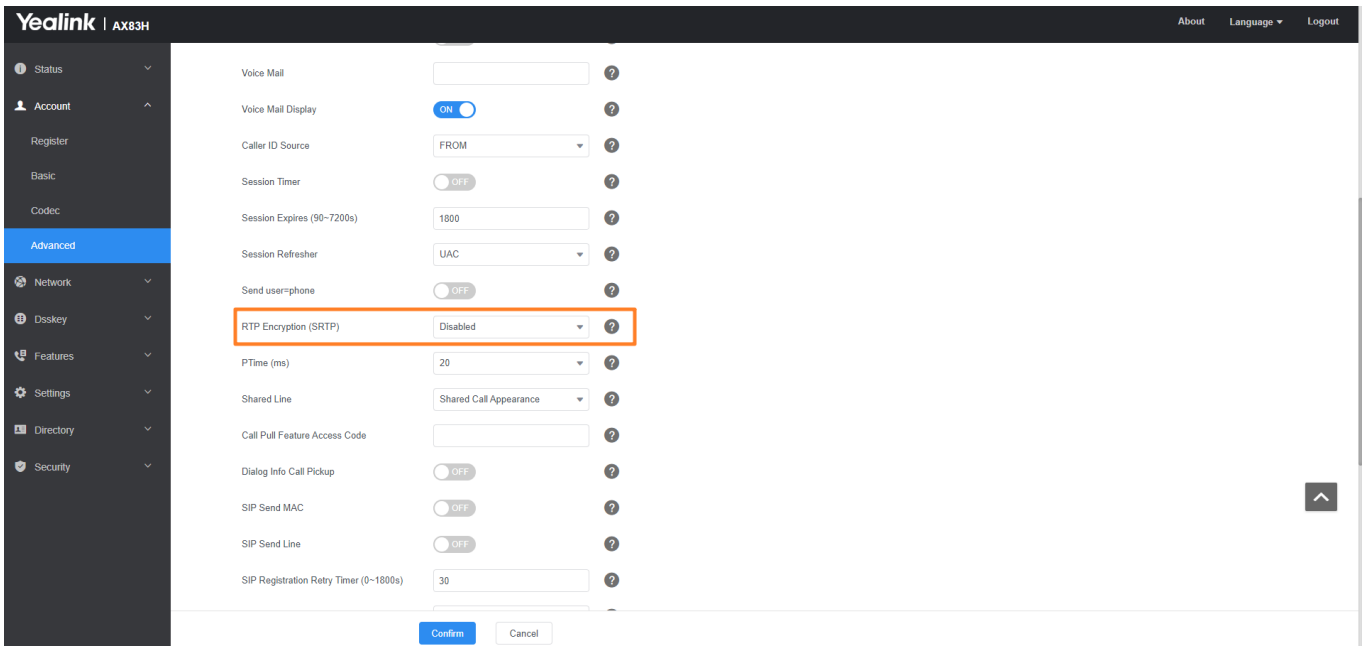
When SRTP is enabled on both phones, RTP streams will be encrypted, and a lock icon will appear on the LCD screen of each IP phone after a successful negotiation.

ⓘ NOTE
If you enable SRTP, then you should also enable TLS. This ensures the security of SRTP encryption. For more information on TLS, refer to Transport Layer Security (TLS) .

SRTP Configuration

Set via the Web User Interface

1. On the web user interface, go to **Account** > **Advanced** > **RTP Encryption (SRTP)**.



Configuration Parameter

account.X.srtp_encryption

Parameter	Permitted Values	Default	Description
account.X.srtp_encryption[1]	**0**-Disabled **1**-Optional, the phone will negotiate with the other phone about what type of encryption to use for the session. **2**-Compulsory, the phone must use SRTP during a call.	0	It configures whether to use an audio encryption service.
account.X.srtp.cipher_list[1]	SM4_CM_128_HMAC_SM3_80, SM4_CM_128_HMAC_SM3_32, AES_256_CM_HMAC_SHA1_80, AES_256_CM_HMAC_SHA1_32, AES_CM_128_HMAC_SHA1_80, AES_CM_128_HMAC_SHA1_32	Blank	It is used to configure the SRTP algorithm list. If multiple values are configured simultaneously, they need to be separated by commas.

Encrypting and Decrypting Files

Introduction

Yealink phones support downloading encrypted files from the server and encrypting files before/when uploading them to the server.

You can encrypt the following files:

- **Configuration Files**: MAC-Oriented CFG file (`<MAC>.cfg`), Common CFG file (y0000000000xx.cfg), MAC-local CFG file (`<MAC>-local.cfg`) or other custom CFG files (for example, sip.cfg, account.cfg)
- **Contact Files**: `<MAC>-contact.xml`

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

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

Configuration Files Encryption Tools

Yealink provides three configuration file encryption tools:

- 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 IP phone, and generate new files named as <xx_Security>.enc (xx is the name of the configuration file, for example, y000000000130_Security.enc for y000000000130.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.

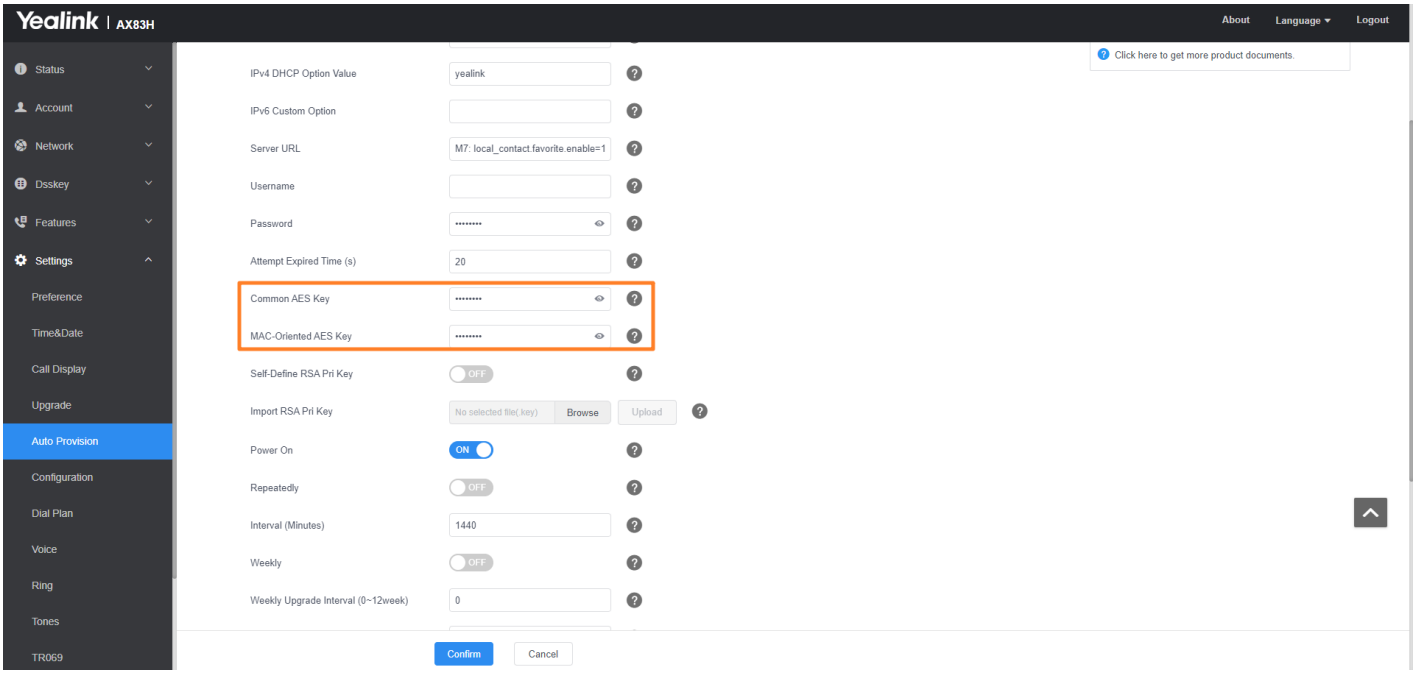
Configuration Files Encryption and Decryption

Encrypted configuration files can be downloaded from the provisioning server to protect against unauthorized access and tampering of sensitive information (for example, login passwords, and registration information).
You can encrypt the configuration files using encryption tools. You can also configure the `<MAC>-local.cfg` files to be automatically encrypted using 16-character symmetric keys when uploading to the server (by setting `static.auto_provision.encryption.config` to 1).
For security reasons, you should upload encrypted configuration files, <xx_Security>.enc files to the root directory of the provisioning server. During auto-provisioning, the phone requests to download the boot file first and then download the referenced configuration files. For example, the phone downloads an encrypted account.cfg file. The phone will request to download <account_Security>.enc file (if enabled) and decrypt it into the plaintext key (for example, key2) using the built-in key (for example, key1). Then the phone decrypts the account.cfg file using key2. After decryption, the phone resolves configuration files and updates configuration settings onto the phone system.

Encryption and Decryption Configuration

Set via the Web User Interface

On the web user interface, go to **Settings** > **Auto Provision** > **Common AES Key**/**MAC-Oriented AES Key**.



Configuration Parameter

static.auto_provision.update_file_mode
static.auto_provision.aes_key_in_file
static.auto_provision.aes_key.com
static.auto_provision.aes_key.mac
static.autoprovision.X.com_aes
static.autoprovision.X.mac_aes
static.auto_provision.encryption.config
static.auto_provision.rsa_pri_key.url
static.auto_provision.rsa_pri_key.enable[2]

Parameter	Permitted Values	Default	Description

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

static.auto_provision.aes_key.com	16 characters	Blank	It configures the plaintext AES key for encrypting/decrypting the Common CFG/Custom CFG file. The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ _ { } ~. **Example**: static.auto_provision.aes_key.com = 0123456789abcdef **NOTE** For decrypting, it works only if `static.auto_provision.aes_key_in_file` is set to 0. If the downloaded MAC-Oriented file is encrypted and the parameter `static.auto_provision.aes_key.mac` is left blank, the phone will try to encrypt/decrypt the MAC-Oriented file using the AES key configured by the parameter `static.auto_provision.aes_key.com`.

static.auto_provision.aes_key.mac	16 characters	Blank	It configures the plaintext AES key for encrypting/decrypting the MAC-Oriented files (<MAC>.cfg, <MAC>-local.cfg and <MAC>-contact.xml). The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ _ { } ~. **Example:** static.auto_provision.aes_key.mac = 0123456789abmins **NOTE** For decrypting, it works only if static.auto_provision.aes_key_in_file is set to 0. If the downloaded MAC-Oriented file is encrypted and the parameter static.auto_provision.aes_key.mac is left blank, the phone will try to encrypt/decrypt the MAC-Oriented file using the AES key configured by the parameter static.auto_provision.aes_key.com.

static.autoprovision.X.com_aes[1][2]	16 characters	Blank	It configures the plaintext AES key for decrypting the Common CFG file. If it is configured, it has a higher priority than the value configured by the parameter `static.auto_provision.aes_key.com`.
static.autoprovision.X.mac_aes[1][2]	16 characters	Blank	It configures the plaintext AES key for decrypting the MAC-Oriented CFG file. If it is configured, it has a higher priority than the value configured by the parameter `static.auto_provision.aes_key_16.mac`.
static.auto_provision.encryption.config	**0**-Disabled, the MAC-local CFG file will be uploaded unencrypted and will replace the one (encrypted or unencrypted) stored on the server if you have configured to back up the MAC-local CFG file to the server by the parameter `static.auto_provision.custom.sync`. **1**-Enabled, the MAC-local CFG file will be uploaded encrypted and will replace the one (encrypted or unencrypted) stored on the server if you have configured to back up the MAC-local CFG file to the server by the parameter `static.auto_provision.custom.sync`. The plaintext AES key is configured by the parameter `static.auto_provision.aes_key.mac`.	0	It enables or disables the phone to encrypt `<MAC>-local.cfg` file using the plaintext AES key.
static.auto_provision.rsa_pri_key.url	URL within 511 characters	Blank	It configures the URL to import the self-define RSA private key file. **NOTE** The key file must be in *.key format. It works only if `static.auto_provision.rsa_pri_key.enable` is set to 1 (Enabled).

static.auto_provision.rsa_pri_key.enable[2]	**0**-Disabled, the phone decrypts the encrypted configuration files using phone built-in RSA keys. **1**-Enabled, the phone decrypts the encrypted configuration files using self-define RSA private key.	0	It enables or disables the self-define RSA private key.

[1]X is an activation code ID. X=1-50.
[2]If you change this parameter, the phone will reboot to make the change take effect.

Example: Encrypting Configuration Files

The following example describes how to use "Config_Encrypt_Tool.exe" to encrypt the account.cfg file. For more information on the other two encryption tools, refer to Yealink Configuration Encryption Tool User Guide .
The way the phone processes other configuration files is the same as that of the account.cfg file.

Procedure

1. Double click **Config_Encrypt_Tool.exe** to start the application tool.

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

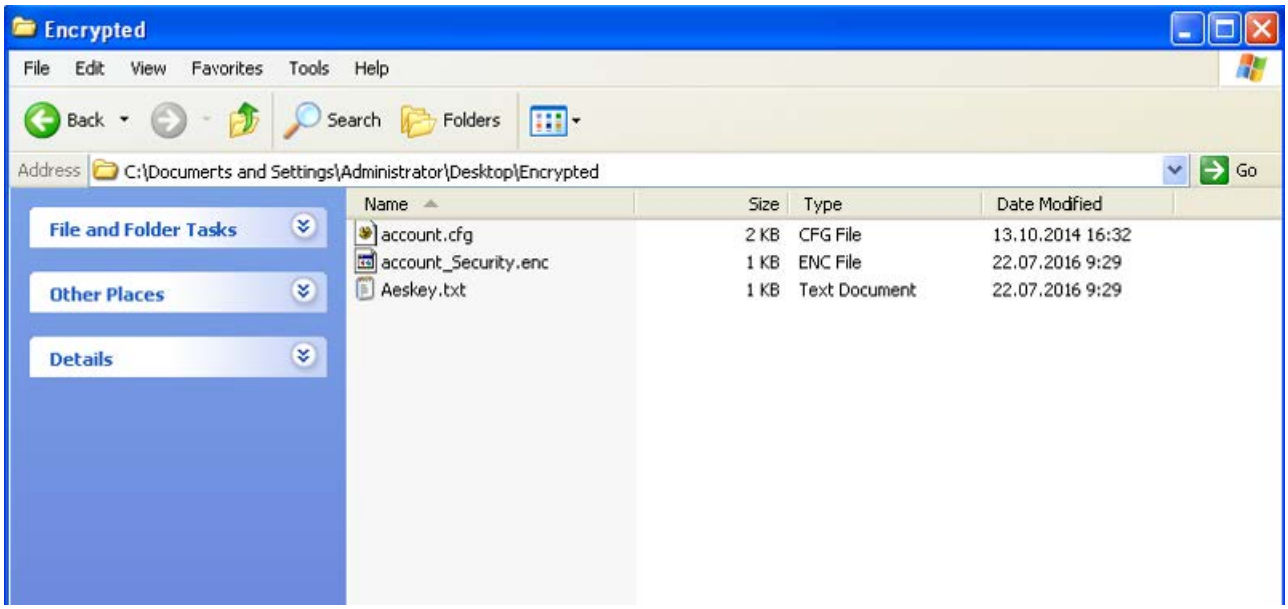
   To select multiple configuration files, you can select the first file and then press and hold the Ctrl key and select other files.
4. (Optional.) Click **Browse** to locate the target directory from your local system in the **Target Directory** field.

   The tool uses the file folder "Encrypted" as the target directory by default.
5. (Optional.) Select the desired radio box in the **AES Model** field.
   If you select the **Manual** radio box, you can enter an AES key in the **AES KEY** field or click **Re-Generate** to generate
   an AES key in the **AES KEY** field. The configuration file(s) will be encrypted using the AES key in the **AES KEY** field.
   If you select the **Auto Generate** radio box, the configuration file(s) will be encrypted using a random AES key. The AES keys of configuration files are different.

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

7. Click **OK**.

   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).



Incoming Network Signaling Validation

Introduction

Yealink phones support the following three optional levels of security for validating incoming network signaling:

- **Source IP address validation**: ensure the request is received from an IP address of a server belonging to the set of target SIP servers.
- **Digest authentication**: challenge requests with digest authentication using the local credentials for the associated registered account.
- **Source IP address validation and digest authentication**: apply both of the above methods.

Incoming Network Signaling Validation Configuration

Configuration Parameter

```
sip.request_validation.source.list
sip.request_validation.digest.list
sip.request_validation.digest.realm
sip.request_validation.event
```

Parameter	Permitted Values	Default	Description
sip.request_validation.source.list	INVITE, ACK, BYE, REGISTER, CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, REFER, PRACK, UPDATE	Blank	It configures the name of the request method for which source IP address validation will be applied. **Example:** sip.request_validation.source.list = INVITE, NOTIFY
sip.request_validation.digest.list	INVITE, ACK, BYE, REGISTER, CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, REFER, PRACK, UPDATE	Blank	It configures the name of the request method for which digest authentication will be applied. **Example:** sip.request_validation.digest.list = INVITE, SUBSCRIBE
sip.request_validation.digest.realm	A valid string	YealinkSPIP	It configures the string used for the authentication parameter Realm when performing the digest authentication.
sip.request_validation.event	A valid string	YealinkSPIP	It configures which events specified within the Event header of SUBSCRIBE or NOTIFY request should be validated. If it is left blank, all events will be validated.

General Features

Line Identification Presentation

Introduction

Yealink phones can derive calling and connected line identification from SIP headers and display the name associated with the telephone number on the LCD screen.

- **Calling Line Identification Presentation (CLIP)**: It allows the phones to display the caller identity, derived from a SIP header contained in the INVITE message when receiving an incoming call. Yealink phones can derive caller identity from three types of SIP header: **From**, **P-Asserted-Identity (PAI)** and **Remote-Party-ID (RPID)**. Identity presentation is based on the identity in the relevant SIP header.
- **Connected Line Identification Presentation (COLP)**: It allows the phones to display the identity of the connected party specified for outgoing calls. The phones can display the Dialed Digits, or the identity in a SIP header (Remote- Party-ID, P-Asserted-Identity or contact) received, or the identity in the From header carried in the UPDATE message sent by the callee as described in RFC 4916. Connected line identification presentation is also known as Called line identification presentation. In some cases, the remote party will be different from the called line identification presentation due to call diversion.

NOTE

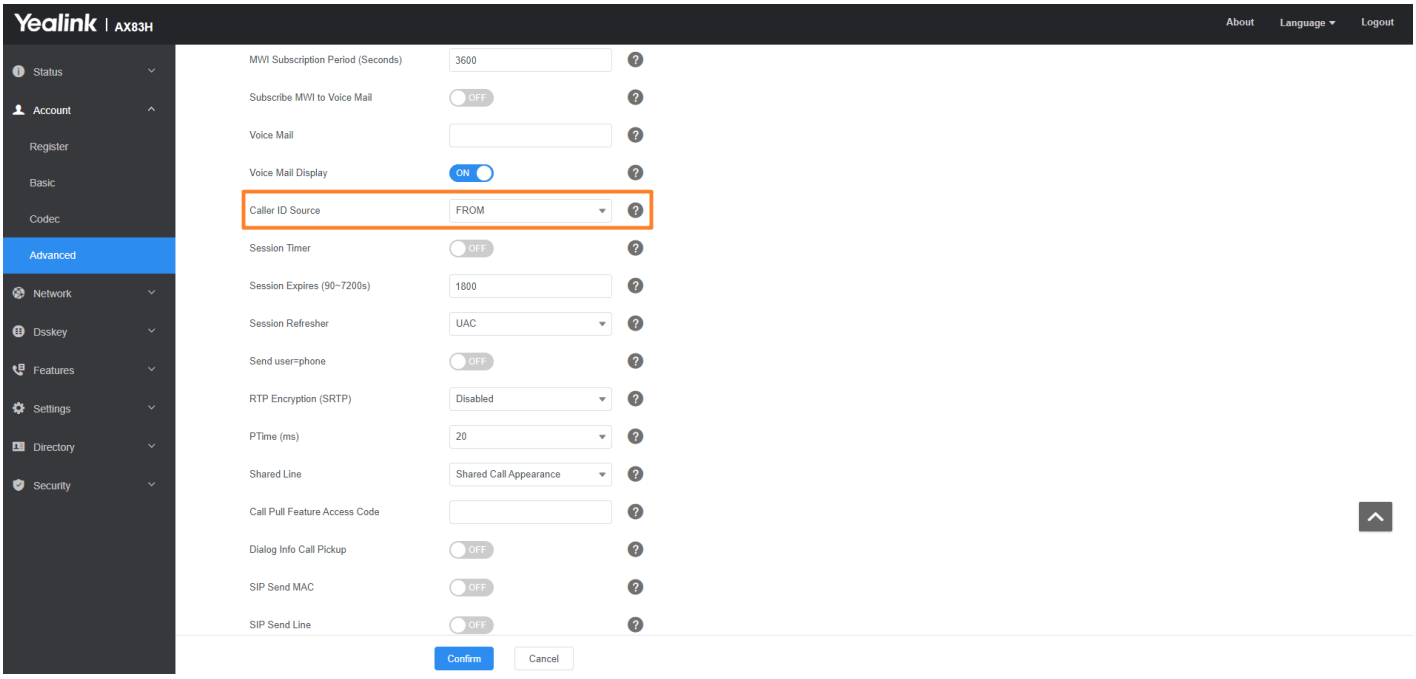
If the caller/callee already exists in the local directory, the local contact name assigned to the caller will be preferentially displayed and stored in the call log.

For more information on calling line identification presentation, refer to Calling and Connected Line Identification Presentation on Yealink IP Phones.

CLIP and COLP Configuration

Set via the Web User Interface

On the web user interface, go to **Account** > **Advanced** > **Caller ID Source**.



Configuration parameter

```
account.X.cid_source
account.X.cid_source_privacy
account.X.cid_source_ppi
sip.cid_source.preference
account.X.cp_source
```

Parameter	Permitted Values	Default	Description
account.X.cid_source[1]	**0**-FROM **1**-PAI **2**-PAI-FROM **3**-RPID-PAI-FROM **4**-PAI-RPID-FROM **5**-RPID-FROM **6**-PREFERENCE, the phone uses the custom priority order for the sources of caller identity (configured by the parameter `sip.cid_source.preference`).	0	It configures the identity of the caller.
account.X.cid_source_privacy[1]	**0**-Disabled, the phone does not process the Privacy header. **1**-Enabled, the phone screen presents anonymity instead if there is a Privacy: id in the INVITE request.	1	It enables or disables the phone to process the Privacy header field in the SIP message. **NOTE** The priority order: PPI > Privacy > PRID/PAI/From.
account.X.cid_source_ppi[1]	**0**-Disabled, the phone does not process the PPI header. **1**-Enabled, the phone presents the caller identity from the PPI header.	0	It enables or disables the phone to process the P-Preferred-Identity (PPI) header in the request message for caller identity presentation.

sip.cid_source.preference	String	P-Preferred-Identity, P-Asserted-Identity, Remote-Party-ID, From	It configures the priority order for the sources of caller identity information. **NOTE** Yealink phones can derive caller identity from the following SIP headers: From, P-Asserted-Identity (PAI), P-Preferred-Identity and Remote-Party-ID (RPID). It works only if `account.X.cid_source` is set to 6 (PREFERENCE).
account.X.cp_source[1]	**0**-PAI-RPID **1**-Dialed Digits **2**-RFC4916, the caller sends the SIP request message which contains the from-change tag in the Supported header. The caller then receives an UPDATE message from the server and displays the identity in the "From" header. **3**-Contact	0	It configures the identity of the callee according to the response message.

[1] X is the account ID.

Return Code for Refused & Unanswered Call

Introduction

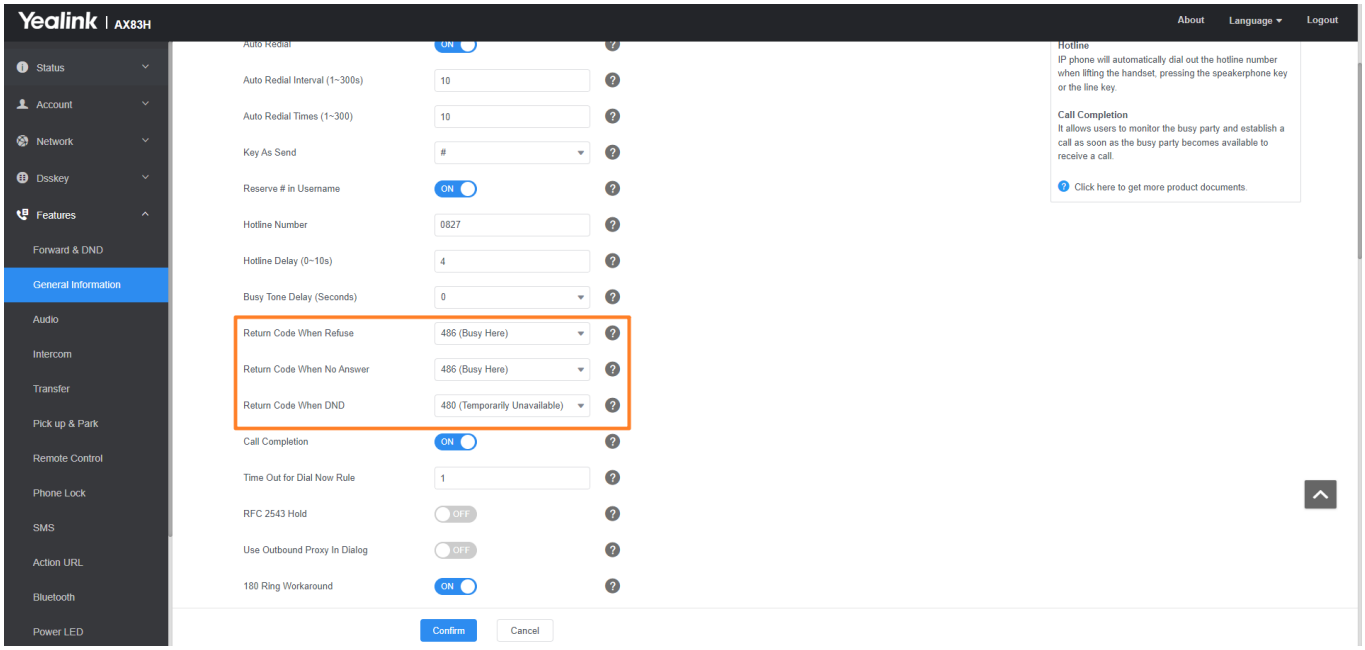
You can define the return code and reason of the SIP response message for the refused call. The caller's phone LCD screen displays the reason according to the received return code. Available return codes and reasons are:

Return Code	Reason
404	Not Found
480	Temporarily Unavailable
486	Busy Here
600	Busy Everywhere
603	Decline

Return Code for Refused Call and not answer Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information**.



Configuration parameter

features.normal_refuse_code
features.unusual_refuse_code
features.no_answer_code

Parameter	Permitted Values	Default	Description
features.normal_refuse_code	**404**-Not Found **480**-Temporarily Unavailable **486**-Busy Here **603**-Decline	486	It configures a return code and reason for SIP response messages when the phone rejects an incoming call. A specific reason is displayed on the caller’ s phone screen.

features.unusual_refuse_code	**404**-Not Found **480**-Temporarily Unavailable **486**-Busy Here **603**-Decline	404	It configures a return code and reason for SIP response messages when the phone rejects an incoming call unusually. A specific reason is displayed on the caller's phone screen.
features.no_answer_code	**404**-Not Found **480**-Temporarily Unavailable **486**-Busy Here **603**-Decline	486	It configures a return code and reason of response messages when the handset does not answer an incoming call. A specific reason is displayed on the caller's phone screen.

Accept SIP Trust Server Only

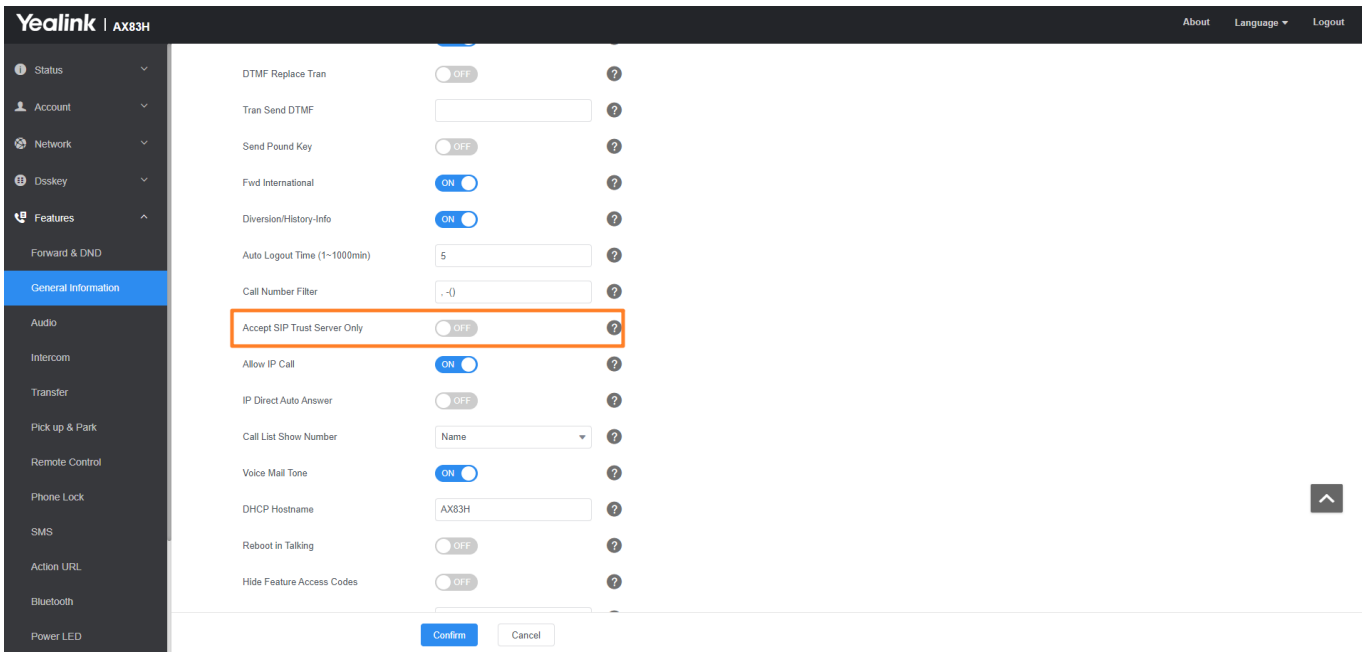
Introduction

Accept SIP trust server only enables the phones to accept the SIP message from your SIP server and outbound proxy server. It can prevent the phone from receiving ghost calls whose phone numbers maybe 100, 1000, and so on. If you enable this feature, the phone cannot accept an IP address call.

Accept SIP Trust Server Only Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Accept SIP Trust Server Only**.



Configuration parameter

```
sip.trust_ctrl
```

Parameter	Permitted Values	Default	Description
sip.trust_ctrl	**0**-Disabled **1**-Enabled, users cannot accept the IP call	0	It enables or disables the phone to only accept the SIP message from the SIP and outbound proxy server.

100 Reliable Retransmission

Introduction

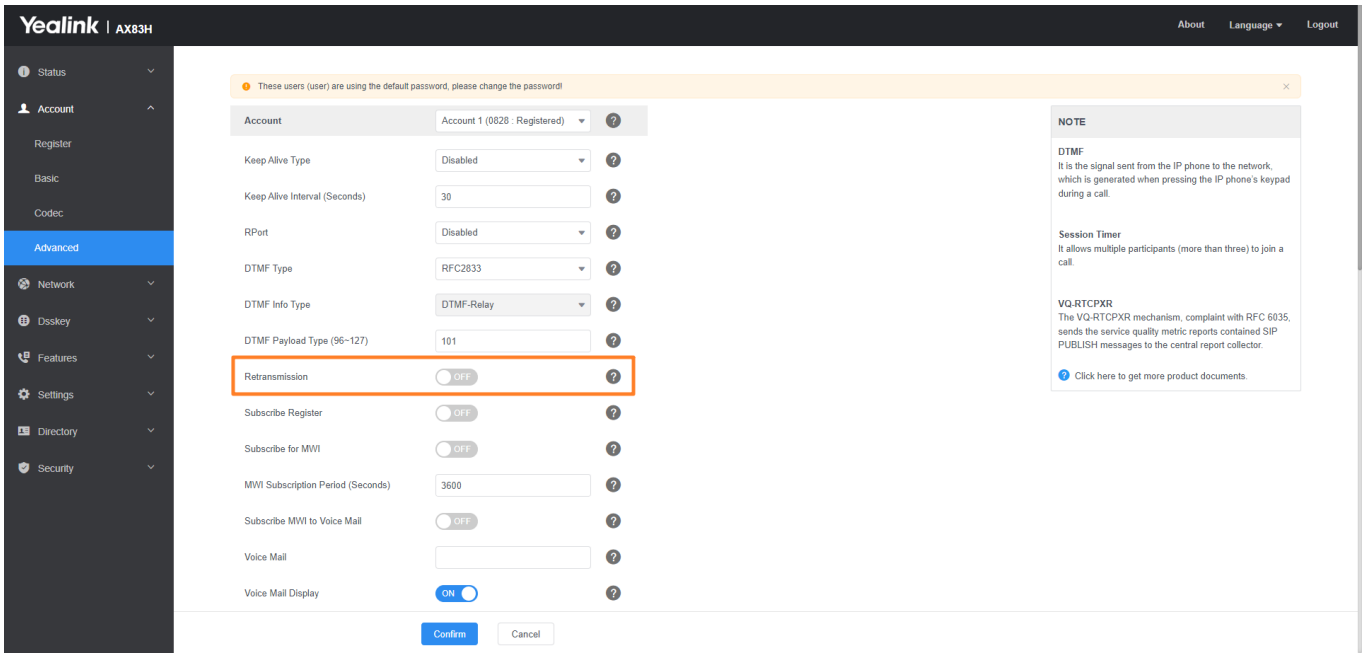
As described in RFC 3262, the 100rel tag is for the reliability of provisional responses. When presented in a Supported header, it indicates that the phone can send or receive reliable provisional responses. When presented in a Require header in a reliable provisional response, it indicates that the response is to be sent reliably.
Example of a SIP INVITE message (take T57W as an example):

```
INVITE sip:1024@pbx.test.com:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.6.197:5060;branch=z9hG4bK1708689023
From: "1025" <sip:1025@pbx.test.com:5060 > ;tag=1622206783
To: <sip:1024@pbx.test.com:5060 >
Call-ID: 0_537569052@10.3.6.197
CSeq: 2 INVITE
Contact: <sip:1025@10.3.6.197:5060 >
Authorization: Digest username="1025", realm="pbx.test.com", nonce="BroadWorksXi5stub71Ts2nb05BW", urii="
sip:1024@pbx.test.com:5060", response="f7e9d35c55af45b3f89beae95e913171", algorithm=MD5, cnonce="
0a4f113b", qop=auth, nc=00000001
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER,
PUBLISH, UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink T57W 96.86.0.70
Supported: 100rel
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length: 302
```

100 Reliable Retransmission Configuration

Set via the Web User Interface

1. On the web user interface, go to **Account** > **Advanced** > **Retransmission**.



Configuration parameter

account.X.100rel_enable

Parameter	Permitted Values	Default	Description

account.X.100rel_enable[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the 100 reliable retransmission feature.

[1] X is the account ID.

SIP Session Timer

Introduction

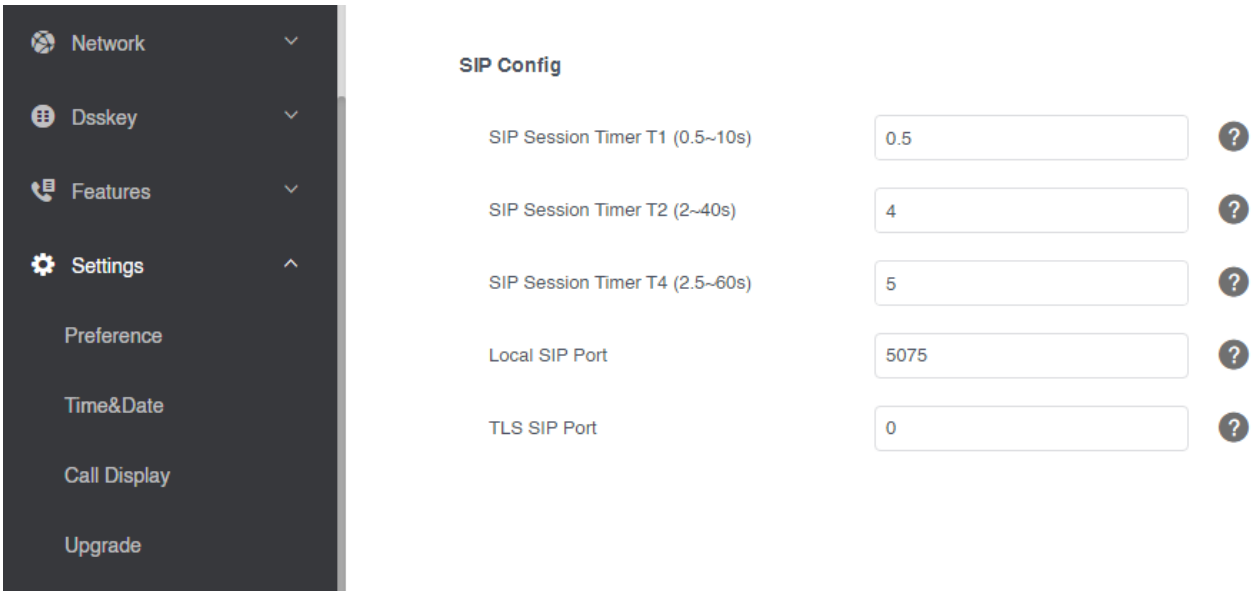
SIP session timers T1, T2 and T4 are SIP transaction layer timers defined in RFC 3261. These session timers are configurable on the phones.

Timer	Description
Timer T1	Timer T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server.
Timer T2	Timer T2 represents the maximum retransmitting time of any SIP request message. The re-transmitting and doubling of T1 will continue until the retransmitting time reaches the T2 value. **Example**: The user registers a SIP account for the IP phone and then set the value of Timer T1, Timer T2 respectively (Timer T1: 0.5, Timer T2: 4). The SIP registration request message will be re-transmitted between the IP phone and SIP server. The re-transmitting and doubling of Timer T1 (0.5) will continue until the retransmitting time reaches the Timer T2 (4). The total registration request retry time will be less than 64 times of T1 (64 * 0.5 = 32). The re-transmitting interval in sequence is 0.5s, 1s, 2s, 4s, 4s, 4s, 4s, 4s, 4s and 4s.
Timer T4	Timer T4 represents that the network will take to clear messages between the SIP client and server.

SIP Session Timer Configuration

Set via the Web User Interface

On the web user interface, go to **Settings** > **SIP** > **SIP Session Timer**.



Configuration parameter

```
sip.timer_t1
sip.timer_t2
sip.timer_t4
```

Parameter	Permitted Values	Default	Description
sip.timer_t1	Float from 0.5 to 10	0.5	It configures the SIP session timer T1 (in seconds).
sip.timer_t2	Float from 2 to 40	4	It configures the SIP session timer T2 (in seconds).
sip.timer_t4	Float from 2.5 to 60	5	It configures the SIP session timer T4 (in seconds).

Session Timer

Introduction

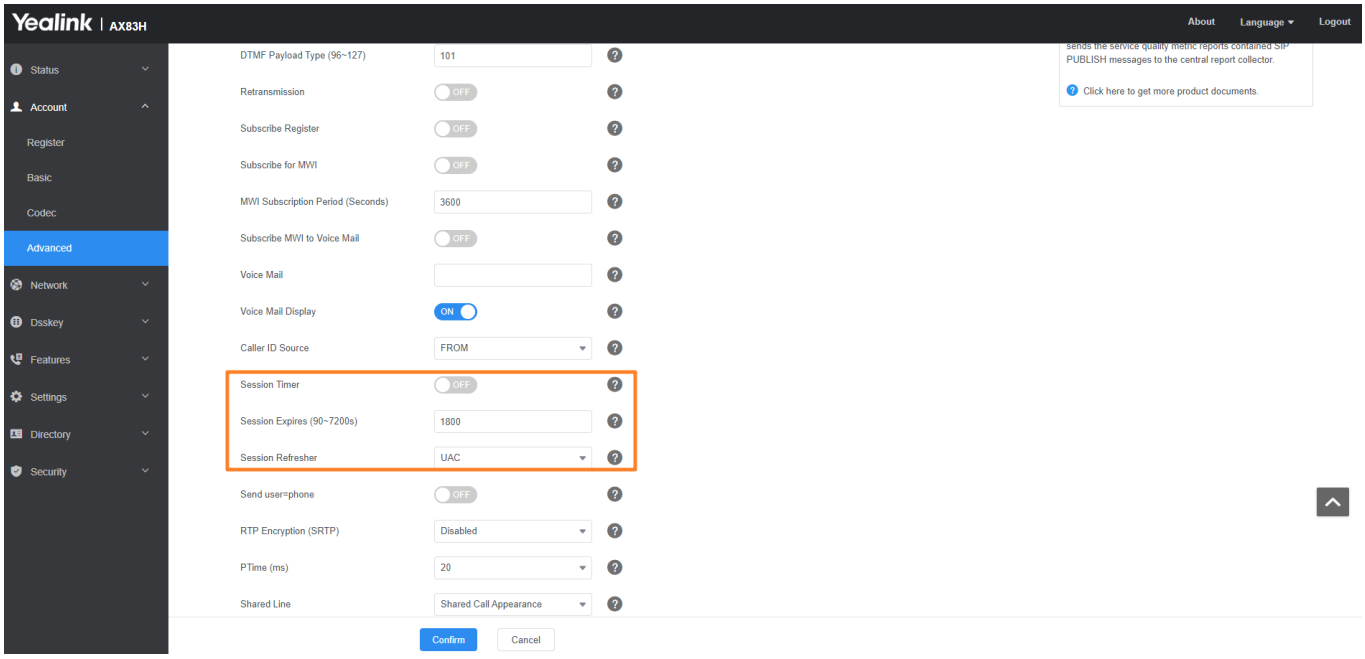
Session timer allows a periodic refresh of SIP sessions through an UPDATE request, to determine whether a SIP session is still active. The session timer is specified in RFC 4028. The phones support two refresher modes: UAC and UAS. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiates the SIP request. If the initiator is configured as UAC, the other client or the SIP server will function as a UAS. If the initiator is configured as UAS, the other client or the SIP server will function as a UAC. The session expiration is negotiated via the Session-Expires header in the INVITE message. The negotiated refresher is always the UAC, which will send an UPDATE request at the expiration of the negotiated session. The value “refresher=uac” included in the UPDATE message means that the UAC performs the refresh.
Example of UPDATE message (UAC mode)

```
UPDATE sip:1058@10.10.20.34:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.20.32:5060;branch=z9hG4bK2104991394
From: "10111" <sip:10111@10.2.1.48:5060 > ;tag=2170397024
To: <sip:1058@10.2.1.48:5060 > ;tag=200382096
Call-ID: 4_1556494084@10.10.20.32
CSeq: 2 UPDATE
Contact: <sip:10111@10.10.20.32:5060 >
Max-Forwards: 70
User-Agent: Yealink AX83H 96.86.0.70
Session-Expires: 90;refresher=uac
Supported: timer
Content-Length: 0
```

Session Timer Configuration

Set via the Web User Interface

1. On the web user interface, go to **Account** > **Advanced** > **Session Timer**/**Session Expires (90~7200s)**/**Session Refresher**.



Configuration parameter

```
account.X.session_timer.enable
account.X.session_timer.expires
account.X.session_timer.refresher
```

Parameter	Permitted Values	Default	Description

account.X.session_timer.enable[1]	**0**-Disabled **1**-Enabled, the phone will send periodic UPDATE requests to refresh the session during a call.	0	It enables or disables the session timer.
account.X.session_timer.expires[1]	Integer from 90 to 7200	1800	It configures the interval (in seconds) for refreshing the SIP session during a call. An UPDATE will be sent after 50% of its value has elapsed. For example, if it is set to 1800 (1800s), the phone will refresh the session during a call every 900 seconds. **NOTE** It works only if `account.X.session_timer.enable` is set to 1 (Enabled).
account.X.session_timer.refresher[1]	**0**-UAC **1**-UAS	0	It configures who refreshes the SIP session during a call. **NOTE** It works only if `account.X.session_timer.enable` is set to 1 (Enabled).

[1] X is the account ID.

Reboot in Talking

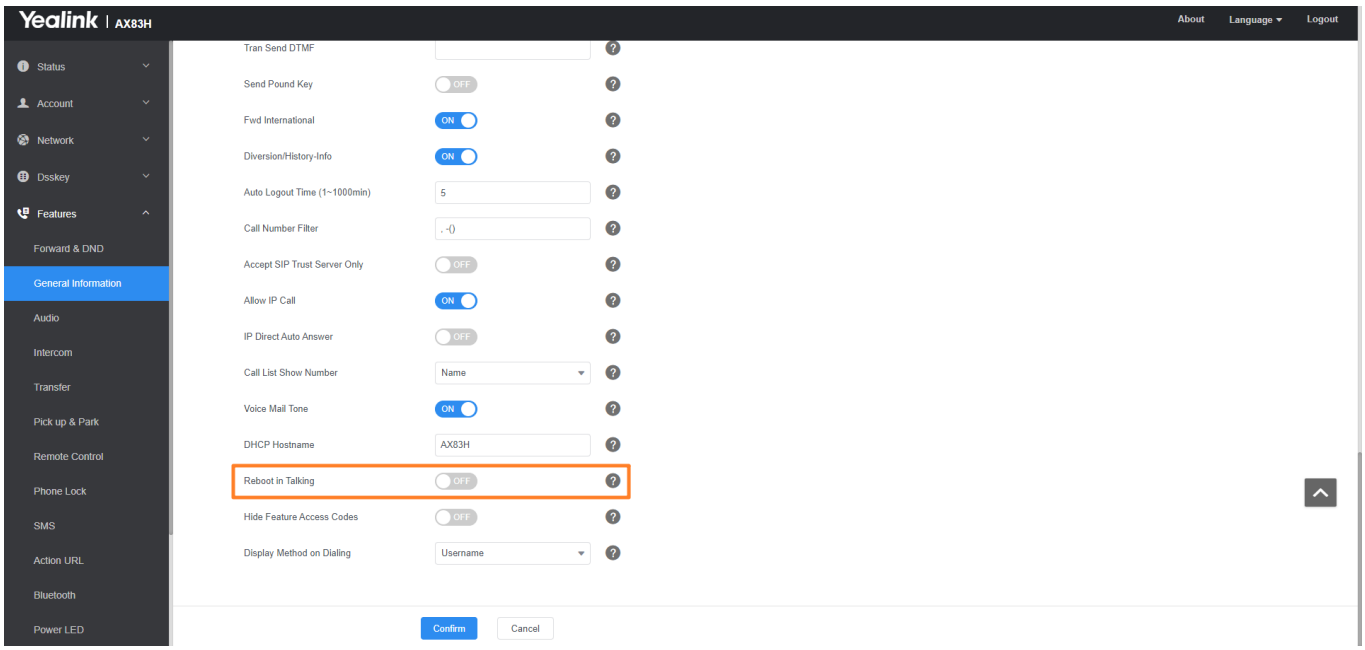
Introduction

Reboot in talking feature allows the phones to reboot during an active call when it receives a reboot Notify message.

Reboot in Talking Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Reboot in Talking**.



Configuration parameter

features.reboot_in_talk_enable

Parameter	Permitted Values	Default	Description
features.reboot_in_talk_enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to reboot during a call when it receives a reboot Notify message.

Reserve # in User Name

Introduction

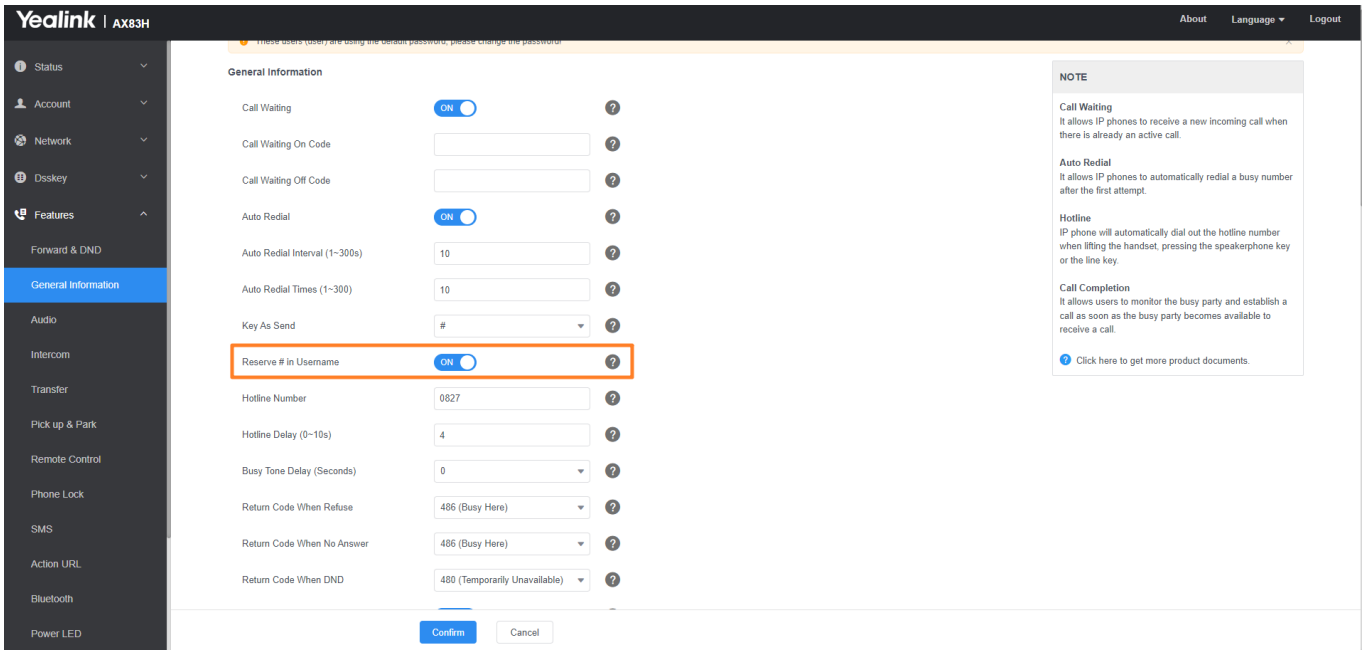
Reserve # in User Name feature allows the phones to reserve “#” in the user name. When Reserve # in User Name feature is disabled, “#” will be converted into “%23”. For example, the user registers an account (user name: 1010#) on the phone, the phone will send 1010%23 instead of 1010# in the REGISTER message or INVITE message to the SIP server.
Example of a SIP REGISTER message:

```
INVITE sip:2@10.2.1.48:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.6:5060;branch=z9hG4bK1867789050
From: "1010" <sip:1010%23@10.2.1.48:5060>;tag=1945988802
To: <sip:2@10.2.1.48:5060>
Call-ID: 0_2336101648@10.3.20.6
CSeq: 1 INVITE

Contact: <sip:1010%23@10.3.20.6:5060>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER,
PUBLISH, UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink AX83H 96.86.0.70
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length: 300
```

Reserve # in User Name Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Reserve # in User Name**.



Configuration parameter

```
sip.use_23_as_pound
```

Parameter	Permitted Values	Default	Description
sip.use_23_as_pound	**0**-Disabled (convert the pound sign into “%23”) **1**-Enabled	1	It enables or disables the phone to reserve the pound sign (#) in the user name.

Busy Tone Delay

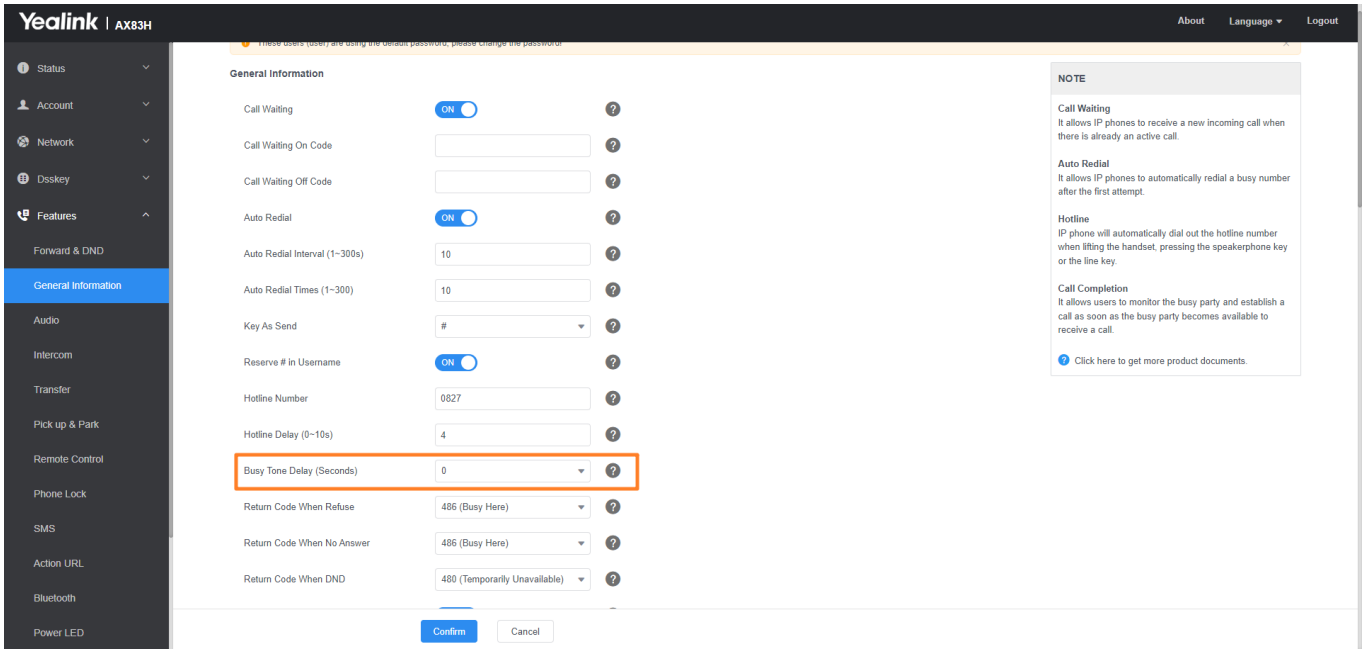
Introduction

The busy tone is an audible signal to indicate that the call is released by the other party. You can define the amount of time that the busy tone lasts.

Busy Tone Delay Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Busy Tone Delay (Seconds)**.



Configuration parameter

features.busy_tone_delay

Parameter	Permitted Values	Default	Description

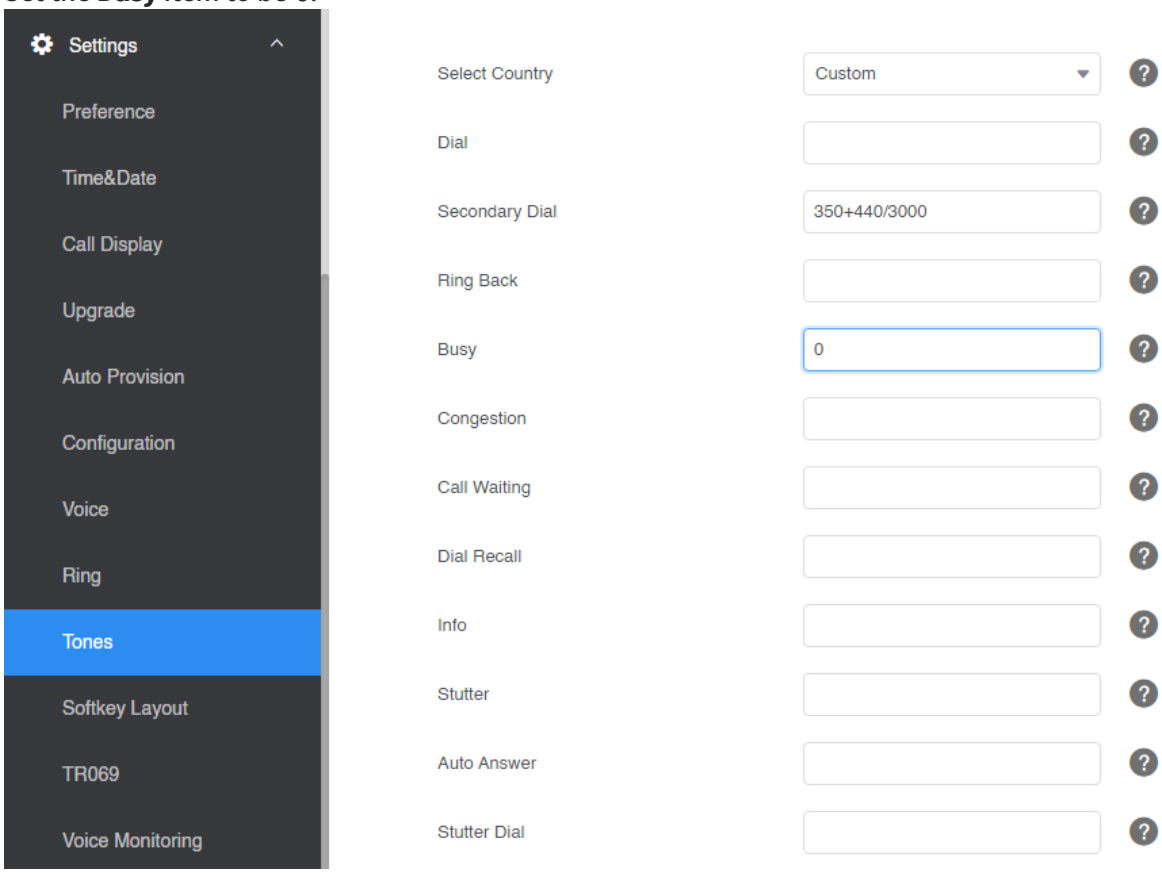
features.busy_tone_delay	**0**-the phone will not play a busy tone. **1**-1s, a busy tone lasts for 1 second on the phone. **3**-3s, a busy tone lasts for 3 seconds on the phone. **5**-5s, a busy tone lasts for 5 seconds on the pho	0	It configures the duration (in seconds) that the busy tone lasts when the call is released by the remote party.

FAQ

How to close the busy tone?

There are two configuration methods:

- **Set via the Web User Interface**
  1. Go to **Settings** > **Tone.**
  2. Set the country tone for the phone to be custom.
  3. Set the B**usy** item to be **0**.



- **Set via the Auto Provision**

```
voice.tone.country = Custom
voice.tone.busy =0
```

Advanced Features

Call Pickup

Call Pickup

You can use call pickup to answer someone else’ s incoming call on your phone.
The Yealink phones support Directed Call Pickup and Group Call Pickup:

- Directed Call Pickup: allows you to pick up incoming calls to a specific phone.
- Group Call Pickup: allows you to pick up incoming calls to any phone within a predefined group of phones.

Directed Call Pickup

Directed call pickup is used for picking up an incoming call on a specific extension. You can answer a call that rings on a specific phone. If there are multiple incoming calls on the phone at the same time, you can only pick up the first incoming call.
You can choose to implement directed call pickup using a directed call pick code or using SIP signaling.

Directed Call Pickup Configuration

You can enable directed call pickup, the LCD screen will display a DPickup soft key when picking up the handset, and pressing the Speakerphone key.
You can configure a directed call pickup code and pick up the incoming call using the DPickup soft key.
The following table lists the parameters you can use to configure directed call pickup.

Configuration parameter

```
features.pickup.direct_pickup_enable
features.pickup.direct_pickup_code
account.X.direct_pickup_code
```

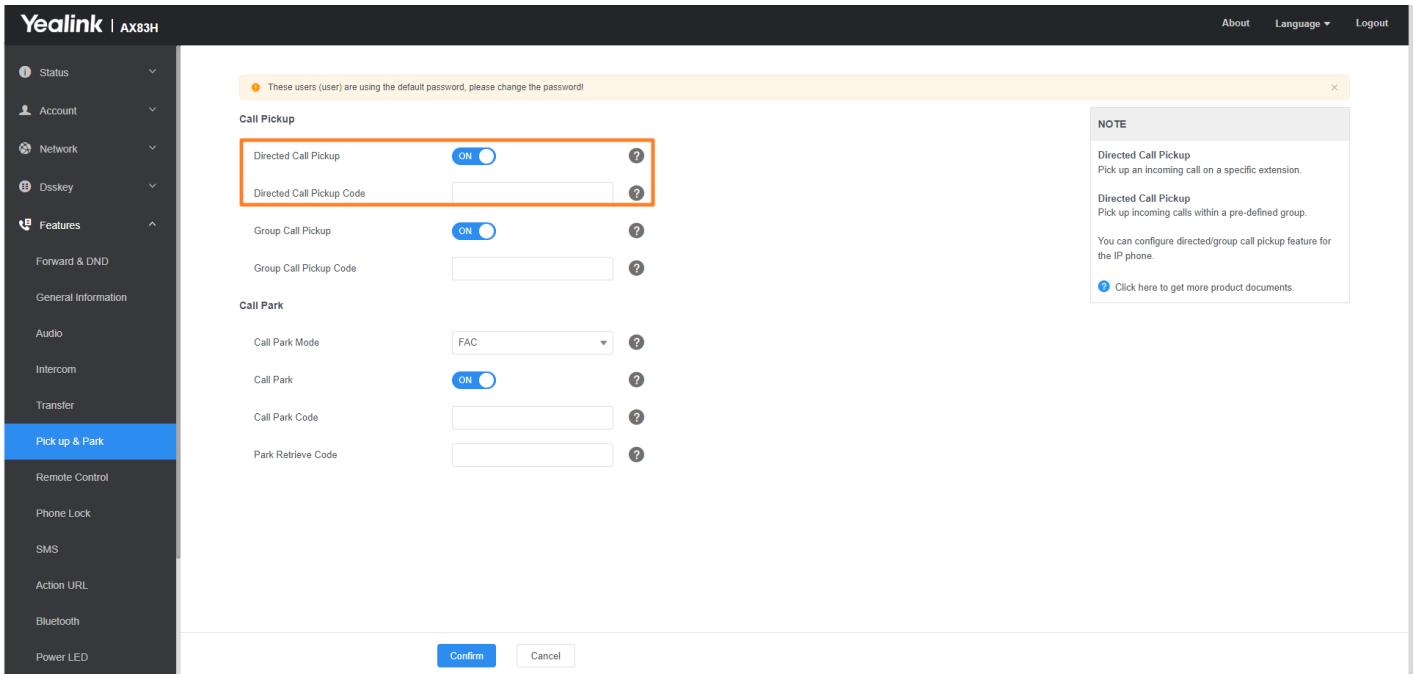
Parameter	Description	Permitted Values	Default	Web UI
features.pickup.direct_pickup_enable	It enables or disables the user to use DPickup soft key when performing the directed call pickup feature.	0-Disabled 1-Enabled, the phone will display the DPickup soft key on the Dialing screen.	0	Features > Pick up & Park > Directed Call Pickup

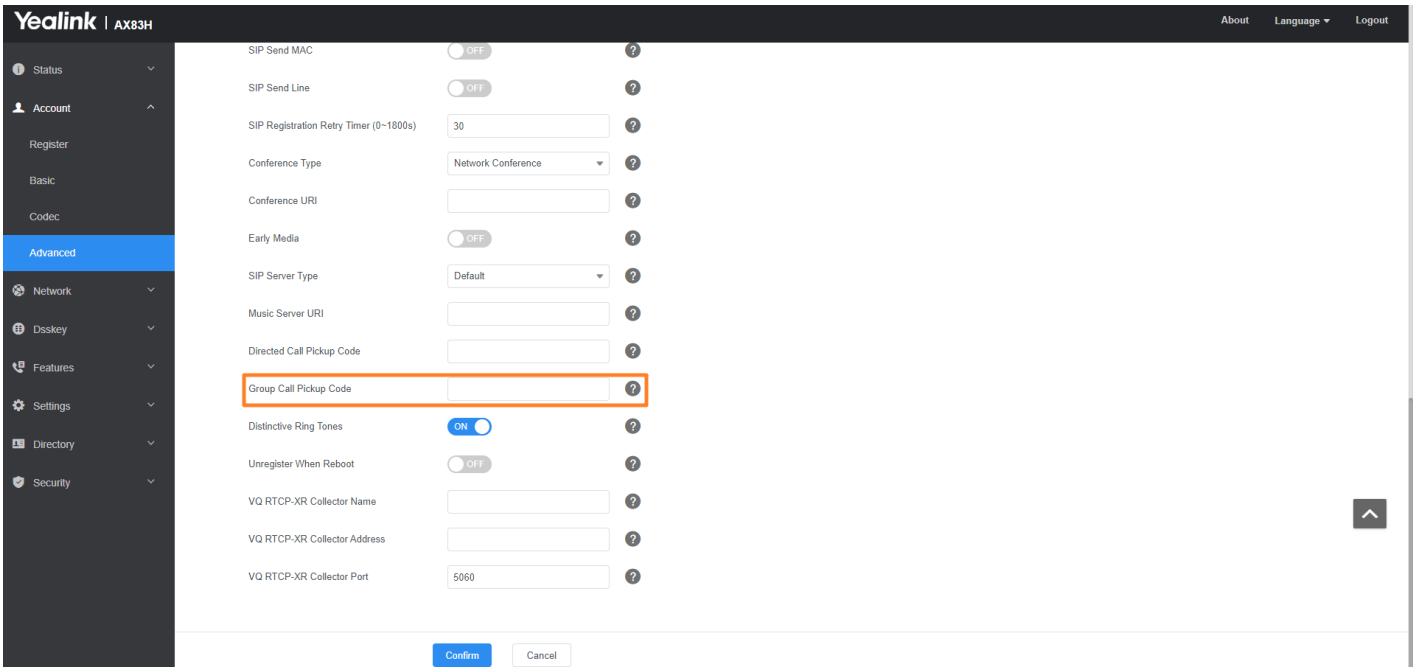
features.pickup.direct_pickup_code	It configures the directed call pickup code on a phone basis. **NOTE** The code configured by "account.X.direct_pickup_code" takes precedence over that configured by this parameter.	String within 32 characters	Blank	Features > Pick up & Park > Directed Call Pickup Code
account.X.direct_pickup_code[1]	It configures the directed call pickup code. **NOTE** The code configured by this parameter takes precedence over that configured by "features.pickup.direct_pickup_code".	String within 32 characters	Blank	Account > Advanced > Directed Call Pickup Code

[1]X is the account ID.

Set via the Web User Interface

On the web user interface, go to: **Features** > **Pick up & Park** > **Directed Call Pickup** / **Account** > **Advanced** > **Directed Call Pickup Code**





Group Call Pickup

Group call pickup is used for picking up incoming calls within a predefined group. When any phone within a predefined group of phones receives an incoming call, you can pick up that call easily on the phone.
If you enable group call pickup, the phone screen will display a GPickup soft key when picking up the handset, and pressing the Speakerphone key.
You can pick up the group incoming call using the GPickup soft key.

TIP
You can set a Softkey Label as a Group Pickup key to pick up a group call.

Group Call Pickup Configuration

The following table lists the parameters you can use to configure the group call pickup.

Configuration parameter

```
features.pickup.group_pickup_enable
features.pickup.group_pickup_code
account.X.group_pickup_code
```

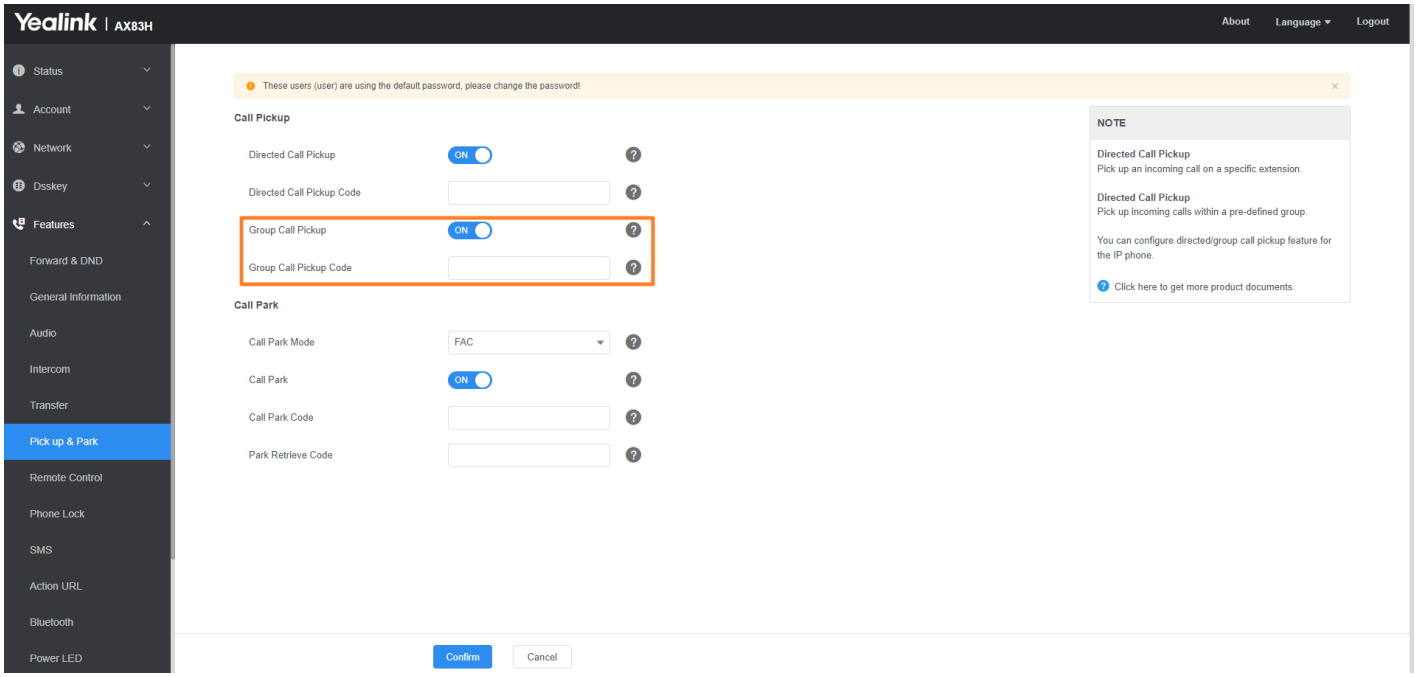
Parameter	Description	Permitted Values	Default	Web UI
features.pickup.group_pickup_enable	It enables or disables the user to use GPickup soft key when performing group call pickup feature.	0-Disabled 1-Enabled, the phone will display the GPickup soft key on the Dialing screen.	0	Features > Pick up & Park > Group Call Pickup

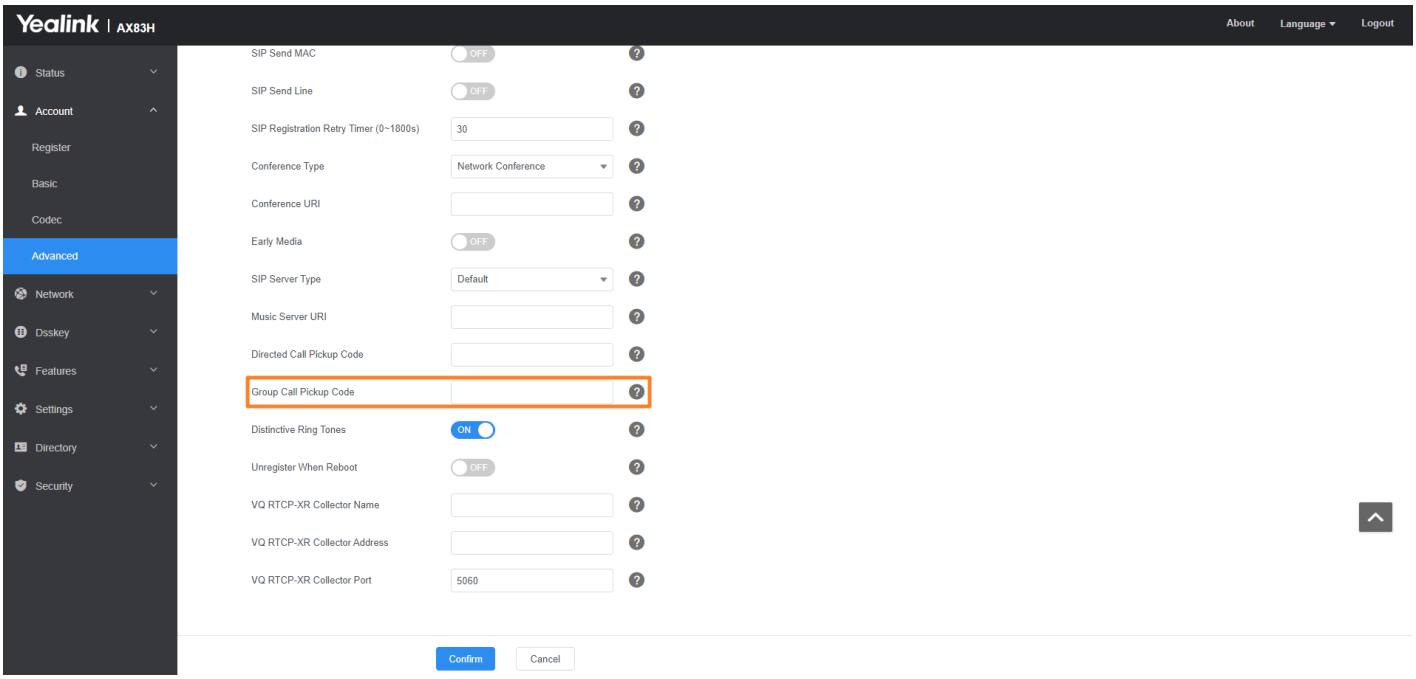
features.pickup.group_pickup_code	It configures the group call pickup code on a phone basis. **ⓘ NOTE** The code configured by "account.X.group_pickup_code" takes precedence over that configured by this parameter.	String within 32 characters	Blank	Features > Pick up & Park > Group Call Pickup Code
account.X.group_pickup_code[1]	It configures the group pickup code. **ⓘ NOTE** The code configured by this parameter takes precedence over that configured by "features.pickup.group_pickup_code".	String within 32 characters	Blank	Account > Advanced > Group Call Pickup Code

[1]X is the account ID.

Set via the Web User Interface

On the web user interface, go to: **Features** > **Pick up & Park** > **Group Call Pickup / Group Call Pickup Code** or **Account** > **Advanced** > **Group Call Pickup Code**





Dialog Info Call Pickup

While some SIP servers implement directed call pickup using a directed call pickup code, others also support implementing this feature through SIP signals.

> **NOTE**
> In this way, you do not need to configure the directed call pickup code.

If you enable the phone to implement directed call pickup through SIP signals, the phone picks up an incoming call via an SIP INVITE message with a Replaces header. The value of Replaces is derived from a NOTIFY message with the dialog-info event. This feature applies only to directed call pick-up attempts initiated against monitored BLF resources. It means you can pick up an incoming call by pressing a BLF/BLF List key.

Example of the dialog-info carried in NOTIFY message:

```
<?xml version="1.0"? >
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="6" state="partial" entity="sip:1011@10.2.1.48:5060" >
<dialog id="65603" call-id="0_1756536024@10.10.20.34" local-tag="3408640225" remote-tag="3779921438" direction=
<state > early</state>
<local >
<identity > sip:1011@10.2.1.48:5060</identity>
<target uri="sip:1011@10.2.1.48:5060"/>
</local >
<remote >
<identity > sip:1058@10.2.1.48:5060</identity >
<target uri="sip:1058@10.2.1.48:5060"/ >
</remote>
</dialog>
</dialog-info>
```

Example of the Replaces carried in INVITE message:

```
Via: SIP/2.0/UDP 10.10.20.18:5060;branch=z9hG4bK2026058891
From: "1010" <sip:1010@10.2.1.48:5060>;tag=826048502
To: <sip:1058@10.2.1.48:5060>
Call-ID: 0_572446084@10.10.20.18
CSeq: 1 INVITE
Contact: <sip:1010@10.10.20.18:5060>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH, UPDATE, MESS
Max-Forwards: 70
User-Agent: Yealink SIP-T46G 28.82.0.20


Replaces: 0_1756536024@10.10.20.34;to-tag=3779921438;from-tag=3408640225
Allow-Events: talk,hold,conference,refer,check-sync
Supported: replaces
Content-Length:  304
```

Dialog Info Call Pickup Configuration

The following table lists the parameters you can use to configure dialog Info call pickup.

Configuration parameter

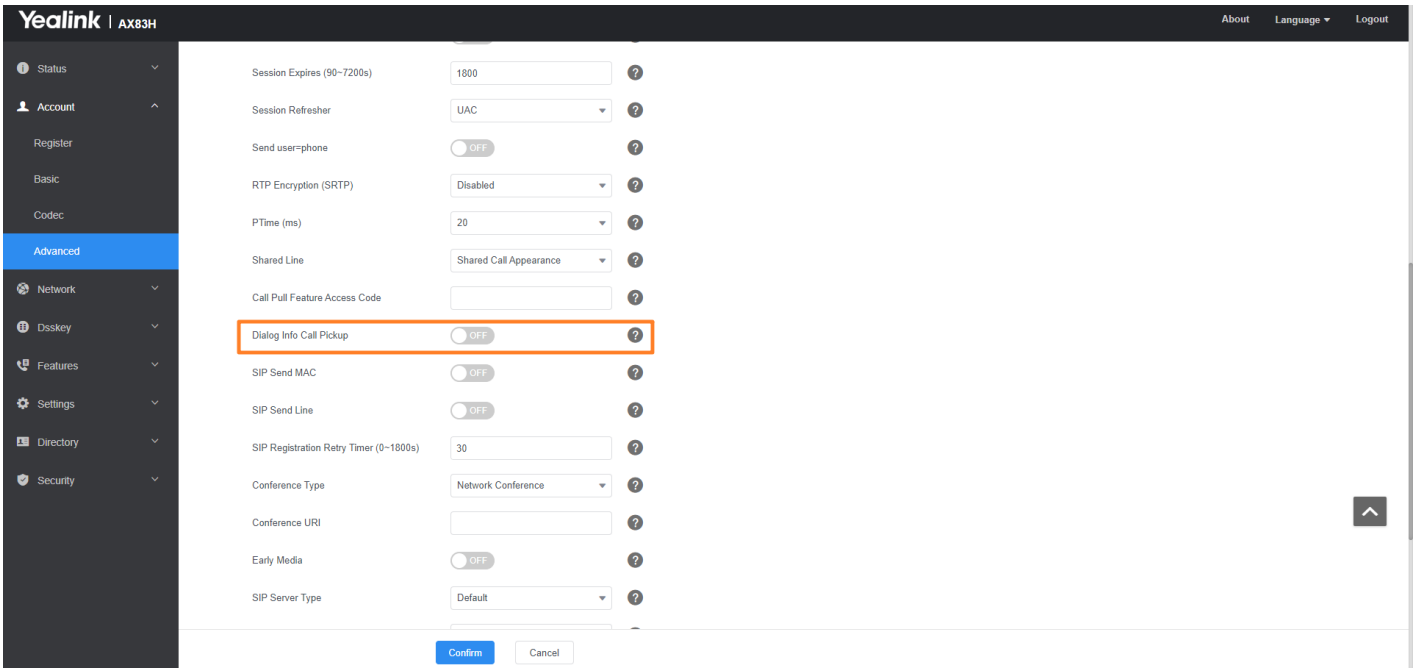
```
account.X.dialoginfo_callpickup
```

Parameter	Description	Permitted Values	Default
account.X.dialoginfo_callpickup[1]	It enables or disables the phone and implements directed call pickup through SIP signals for a specific account. **NOTE** In this way, you do not need to configure the directed call pickup code.	0-Disabled 1-Enabled, the phone picks up a call according to the Replaces header in the INVITE message.	0

[1]X is the account ID.

Set via the Web User Interface

On the web user interface, go to: **Account** > **Advanced** > **Dialog Info Call Pickup**



FAQ

1. Hold the current call and pick up the Intercom automatically

Call Completion

Call Completion

When you place a call and the callee is temporarily unavailable to answer the call, call completion allows your phone to monitor the busy party and establish a call after the busy party becomes available to receive a call.
Two factors commonly prevent a call from connecting successfully:

- Callee does not answer
- Callee actively rejects the incoming call before answering

Yealink phones support call completion using the SUBSCRIBE/NOTIFY method, which is specified in draft-poetzl-sipping-call-completion-00, to subscribe to the busy party and receive notifications of their status changes.
The caller subscribes for update notifications of the dialog event from the busy party.

Example of a SUBSCRIBE message:

```
SUBSCRIBE sip:1000@10.10.20.34:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.20.32:5060;branch=z9hG4bK2880274891
From: "10111" <sip:10111@10.2.1.48:5060>;tag=8643512
To: <sip:1000@10.2.1.48:5060>;tag=4025601441
Call-ID: 4_2103527761@10.10.20.32
CSeq: 2 SUBSCRIBE
Contact: <sip:10111@10.10.20.32:5060>
Accept: application/dialog-info+xml
Max-Forwards: 70
User-Agent: Yealink SIP-T46G 28.82.0.20
Expires: 60


Event: dialog
Content-Length: 0
```

Example of a NOTIFY message

The subscription (SUBSCRIBE message) of the dialog event "Call Completion" is confirmed by the busy party:

```
NOTIFY sip:10111@10.10.20.32:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.20.31:5060;branch=z9hG4bK1830418099
From: <sip:1000@10.2.1.48:5060>;tag=1032948194
To: "10111" <sip:10111@10.2.1.48:5060>;tag=722495580
Call-ID: 0_160090766@10.10.20.32
CSeq: 2 NOTIFY
Contact: <sip:1000@10.10.20.31:5060>
Content-Type: application/dialog-info+xml
Max-Forwards: 70
User-Agent: Yealink SIP-T46G 28.82.0.20
Subscription-State: active;expires=60
Event: dialog
Content-Length:   584

<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="1" state="full" entity="sip:1000@10.2.1.48:5060">
<dialog id="65626" call-id="0_3138198645@10.10.20.31" local-tag="2331766736" remote-tag="1786911541" direction=
<state>confirmed</state>
<local>
<identity>sip:1000@10.2.1.48:5060</identity>
<target uri="sip:1000@10.2.1.48:5060"/>
</local>
<remote>
<identity>sip:1@10.2.1.48:5060</identity>
<target uri="sip:1@10.2.1.48:5060"/>
</remote>
</dialog>
<dialog id="65622">
<state>terminated</state>
</dialog>
</dialog-info>
```

The busy party has finished the call and is available again. A new notification update from the busy party is received by the caller:

```
NOTIFY sip:10111@10.10.20.32:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.20.31:5060;branch=z9hG4bK3431394016
From: <sip:1000@10.2.1.48:5060>;tag=1558968605
To: "10111" <sip:10111@10.2.1.48:5060>;tag=140677866
Call-ID: 0_2584152566@10.10.20.32
CSeq: 5 NOTIFY
Contact: <sip:1000@10.10.20.31:5060>
Content-Type: application/dialog-info+xml
Max-Forwards: 70
User-Agent: Yealink SIP-T46G 28.82.0.20
Subscription-State: active;expires=48
Event: dialog
Content-Length:   217

<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="4" state="partial" entity="sip:1000@10.2.1.48:5060">
<dialog id="65644">
<state>terminated</state>
</dialog>
</dialog-info>
```

Call Completion Configuration

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

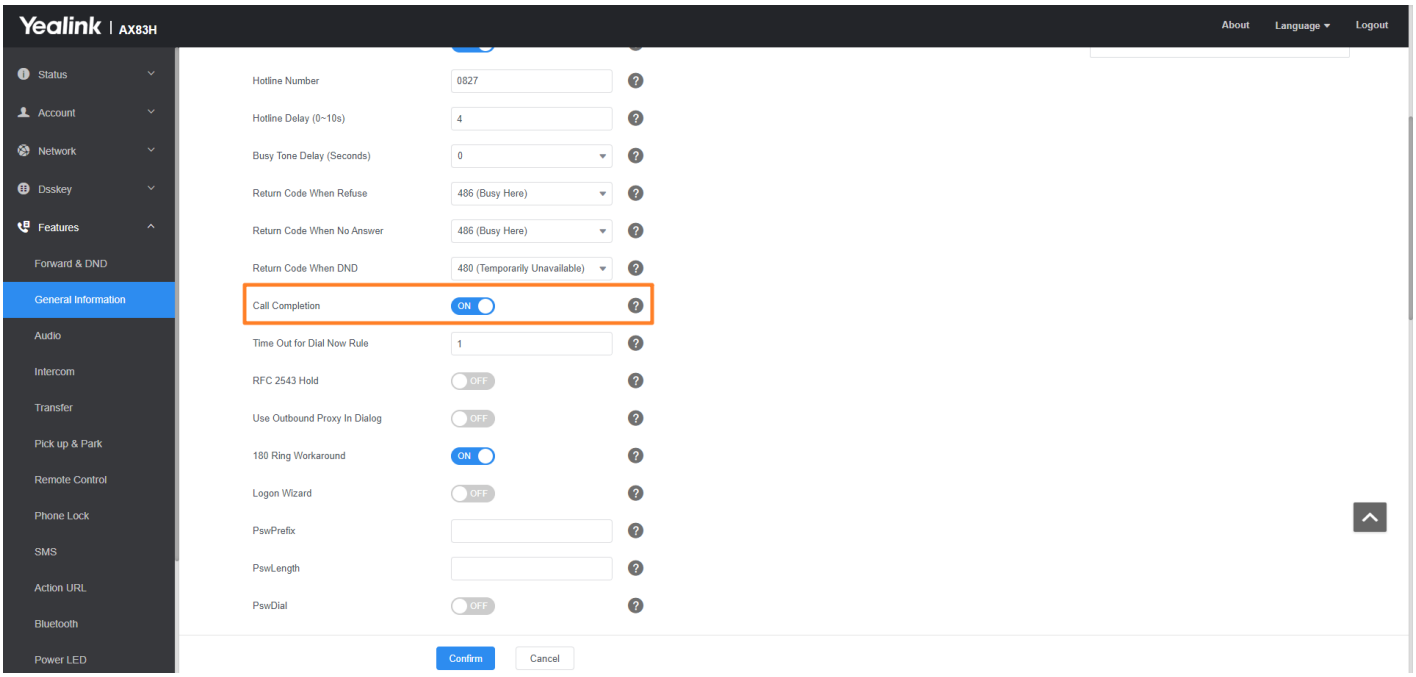
Configuration parameter

```
features.call_completion_enable
```

Parameter	Description	Permitted Values	Default	Web UI
features.call_completion_enable	It enables or disables the call completion feature.	**0**-Disabled **1**-Enabled	0	Features > General Information > Call Completion

Set via the Web User Interface

On the web user interface, go to: **Features** > **General Information** > **Call Completion**



Example: Using Call Completion

The following example shows the configuration for call completion.
Example:

```
features.call_completion_enable = 1
```

After provisioning, when you place a call and the callee is temporarily unavailable to answer the call, the phone screen will prompt whether to wait for the callee party. You can activate the call completion feature. After the called party becomes idle, the phone screen will prompt whether to dial the number.

Call Park and Retrieve

Call Park and Retrieve

Call park allows users to park a call on a special extension and then retrieve it from another phone (for example, a phone in another office or conference room).
The phones support call park feature under the following modes:

- **FAC mode**: parks the call to the local extension or the desired extension through dialing the park code.
- **Transfer mode**: parks the call to the shared parking lot through performing a blind transfer. For some servers, the system will return a specific call park retrieve number (park retrieve code) from which the call can be retrieved after parking successfully.

Call Park and Retrieve Configuration

The following table lists the parameters you can use to configure the call park and retrieve.
Configuration parameter

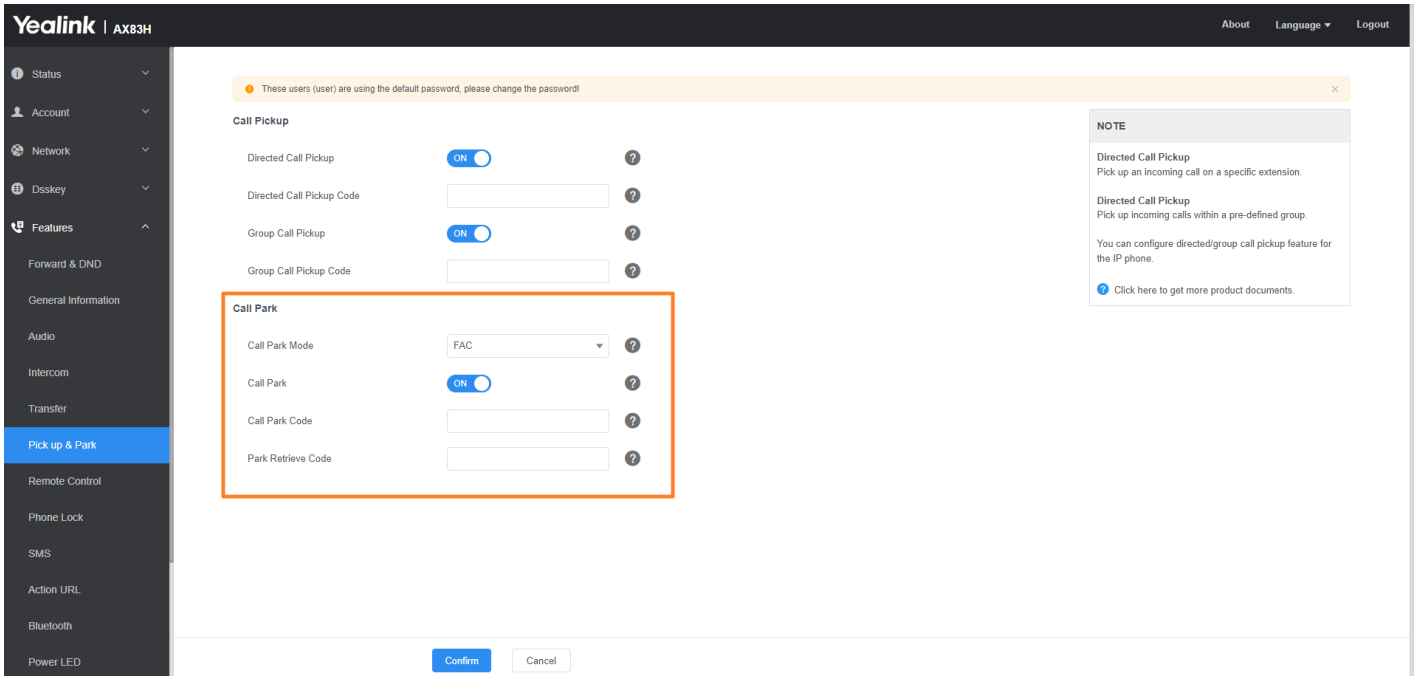
```
features.call_park.park_mode
features.call_park.enable
features.call_park.park_code
features.call_park.park_retrieve_code
features.call_park.direct_send.enable
features.call_park.line_restriction.enable
features.call_park.performby_holdhardkey.enable
```

Parameter	Description	Permitted Values	Default
features.call_park.park_mode	It configures the call park mode.	**1**-FAC, park a call through dialing the call park code. **2**-Transfer, blind transfer the call to a shared parking lot.	2
features.call_park.enable	It enables or disables the call park feature.	**0**-Disabled **1**-Enabled	0
features.call_park.park_code	It configures the call park code for FAC call park mode or configures the shared parking lot for Transfer call park mode.	String within 256 characters	Blank
features.call_park.park_retrieve_code	It configures the park retrieve code for FAC call park mode or configures the retrieve parking lot for Transfer call park mode.	String within 256 characters	Blank
features.call_park.direct_send.enable	It enables or disables the phone to dial out the call park code/park retrieve code directly when pressing the Park/Retrieve soft key. **NOTE** It works only if "features.call_park.park_mode" is set to 1 (FAC) and you have configured the call park code/park retrieve code.	**0**-Disabled, the phone will enter the dialing screen when pressing the Park/Retrieve soft key. The user can dial the specific extension manually or Speed Dial key to park the call to the specific extension or retrieve the call parked from the specific extension. **1**-Enabled	1

features.call_park.line_restriction.enable	It enables or disables the phone to park a call using the specific line of the Call Park key. **NOTE** It works only if "features.call_park.park_mode" is set to 2 (Transfer).	**0**-Disabled, the call is parked by the current line, which is in call state. **1**-Enabled	0
features.call_park.performby_holdhardkey.enable	It enables or disables the phone to park a call using the HOLD hard key.	**0**-Disabled **1**-Enabled	0

Set via the Web User Interface

On the web user interface, go to **Features** > **Pick up & Park**



Example: Setting Call Park and Retrieve in FAC Mode

The following example shows the configuration for the FAC call park mode.

Example:

```
features.call_park.park_mode = 1

features.call_park.enable = 1

features.call_park.park_code = *68

features.call_park.park_retrieve_code = *88
```

After provisioning, the call park mode is set to FAC. A Park soft key will display on the phone during an active call, and a Retrieve soft key will display on the Dialing screen. You can press the Park soft key to park a call or press the Retrieve soft key to retrieve a parked call.

Example: Setting Call Park and Retrieve in Transfer Mode

The following example shows the configuration for Transfer call park mode.
Example:

```
features.call_park.park_mode = 2

features.call_park.enable = 1

features.call_park.park_code = *01

features.call_park.park_retrieve_code = *11
```

After provisioning, the call park mode is set to Transfer. A Park soft key will display on the phone during an active call and a Retrieve soft key will display on the Dialing screen. You can press the Park soft key to park a call to the shared parking lot "`*01`", or press the Retrieve soft key to retrieve the parked call from the shared parking lot "`*01`" using the retrieve code "`*11`".

Shared Line

Shared Line

Yealink phones support Shared Call Appearance (SCA) and Bridged Line Appearance (BLA) to share a line. Shared call appearances and bridged line appearances are similar signaling methods that enable more than one phone to share the same line or registration. The methods you use vary with the SIP server you are using.
The shared line users have the ability to do the following:

- Place and answer calls
- Place a call on hold
- Pull a shared call (only SCA)

Shared Call Appearance (SCA) Configuration

In the SCA scenario, an incoming call can be presented to multiple phones simultaneously. Any IP phone can be used to originate or receive calls on the shared line.

Yealink phones support SCA using a SUBSCRIBE/NOTIFY mechanism as specified in RFC 3265. The events used are:

- "call-info" for call appearance state notification.
- "line-seize" for the phone to ask to seize the line.

You have the option to provide users the ability to do the following:

- Configure a private hold soft key or Private Hold key and provide users the ability to hold a call privately.
- Configure a call pull code, which allows users to retrieve an existing call from another shared phone that is in an active or public hold status.

SCA Configuration

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

Configuration parameter

```
account.X.shared_line
account.X.line_seize.expires
account.X.shared_line_callpull_code
features.barge_in_via_username.enable
phone_setting.call_remote_end_when_hold.busy_tone.enable
account.X.shared_line.idle_details
```

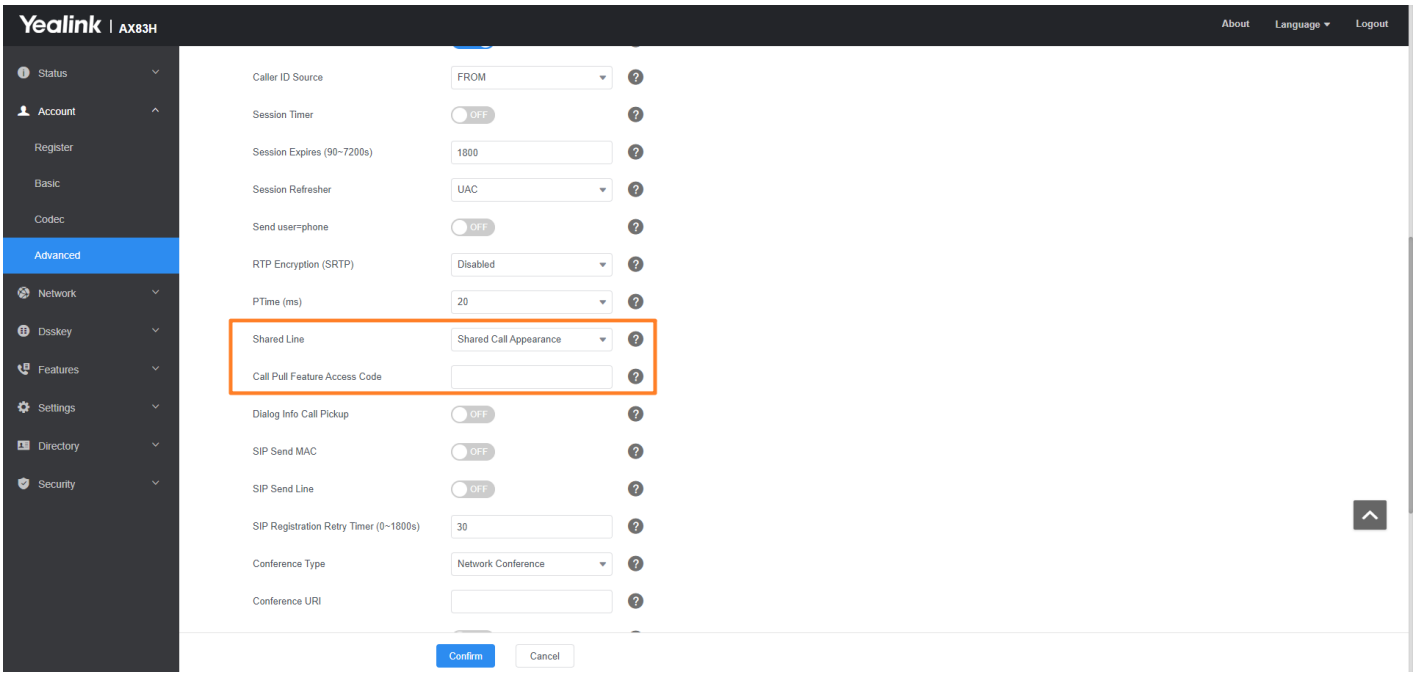
Parameter	Description	Permitted Values	Default
account.X.shared_line[1]	It configures the registration line type.	**0**-Disabled **1**-Shared Call Appearance	0
account.X.line_seize.expires[1]	It configures the line-seize subscription expiration time (in seconds). **NOTE** It works only if "account.X.shared_line" is set to 1 (Shared Call Appearance).	Integer from 0 to 65535	15
account.X.shared_line_callpull_code[1]	It configures the call pull feature access code to retrieve an existing call from another shared phone regardless of the phone's current status. **NOTE** It works only if "account.X.shared_line" is set to 1 (Shared Call Appearance).	String within 99 characters	Blank

features.barge_in_via_username.enable	It enables or disables the phone to use the user name of the account to barge in an active call.	**0**-Disabled, user registers name to barge in, the phone sends INVITE request with the registered name when barging in a call **1**-Enabled, the phone sends INVITE request with the user name when barging in a call	0
phone_setting.call_remote_end_when_hold.busy_tone.enable	It enables or disables the phone to play a busy tone when a public hold call on the shared line is retrieved by the remote party. **NOTE** It works only if "features.busy_tone_delay" is not set to 0.	**0**-Disabled **1**-Enabled	1
account.X.shared_line.idle_details[1]	It enables or disables the phone to display the basic SCA call information on the idle screen. **NOTE** It works only if “account.X.shared_line” is set to 1 (Shared Call Appearance).	**0**-Disabled **1**-Enabled, users can also view the call details by long pressing the SCA line key.	0

[1]X is the account ID.

Set via the Web User Interface

On the web user interface, go to Account > **Advanced** > **Shared Line / Call Pull Feature Access Code** .



Intercom

Intercom

The intercom is a useful feature in an office environment to quickly connect with the operator or the secretary. You can press the intercom key to place a call to a contact that is answered automatically on the contact's phone as long as the contact is not in an active call.

Intercom Key Configuration

You can configure an Intercom key to provide users the ability to initiate intercom calls directly to the specified contact.
The following shows the configuration for an Intercom key.

Programmable Key Configuration
programablekey.X.type = 14 programablekey.X.line = 1 programablekey.X.value = 4603 programablekey.X.label = Bill (Only applicable to SoftKey1 and SoftKey2.)

After provisioning, an Intercom key for Bill (4603) is available on the phone. You can press the Intercom key to place an intercom call to Bill (4603).

Outgoing Intercom Configuration

Yealink phones support two methods for initialing intercom calls.
The following table lists the parameters you can use to configure outgoing intercom.

Configuration parameter

```
features.intercom.mode
features.intercom.feature_access_code
account.X.call_info
```

Parameter	Description	Permitted Values	Default
features.intercom.mode	It configures the intercom mode.	**0**-SIP **1**-FAC, the feature access code is configured by "features.intercom.feature_access_code".	0
features.intercom.feature_access_code	It configures the intercom feature access code. **NOTE** It works only if "features.intercom.mode" is set to 1 (FAC).	String	Blank
account.X.call_info[1]	It configures the value of the Call-Info header for the intercom feature. The value format likes: <sip:XXX (X can be any value)>; answer-after=0. **NOTE** If both Call-Info header and Alert-Info header (defined by the parameter "account.X.alert_info") are configured, the Call-Info header has a higher priority than the Alert-Info header.	String within 256 characters	Blank

[1]X is the account ID.

Incoming Intercom Configuration

The IP phone can process incoming calls differently depending on settings.
The following table lists the parameters you can use to configure incoming intercom.

Configuration parameter

```
features.intercom.allow
features.intercom.mute
features.intercom.tone
features.intercom.barge
features.intercom.barge_in_dialing.enable
features.intercom.headset_prior.enable
account.X.alert_info
```

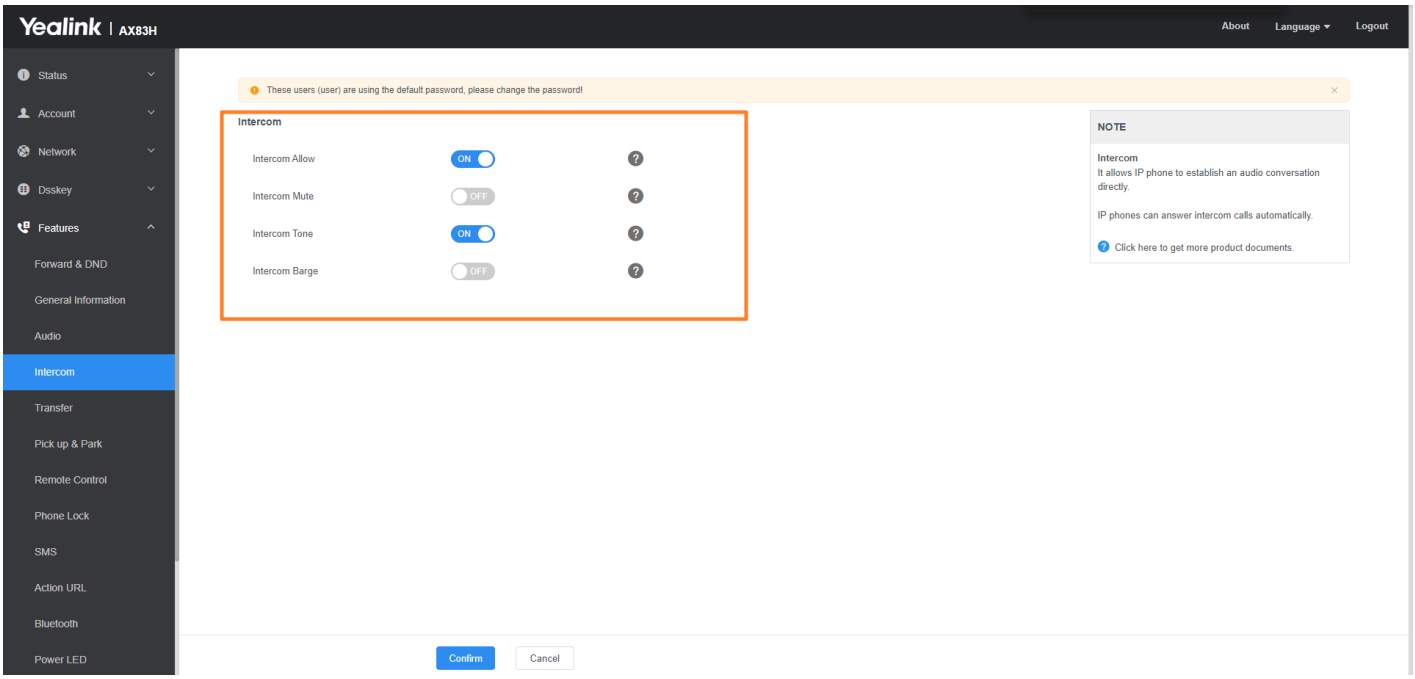
Parameter	Description	Permitted Values	Default
features.intercom.allow	It enables or disables the phone to answer an incoming intercom call.	**0**-Disabled, the phone will handle an incoming intercom call like a normal incoming call. **1**-Enabled, the phone will automatically answer an incoming intercom call.	1
features.intercom.mute	It enables or disables the phone to mute the microphone when answering an intercom call. **NOTE** It works only if "features.intercom.allow" and "features.allow_mute" are set to 1 (Enabled).	**0**-Disabled **1**-Enabled, the microphone is muted for intercom calls, and then the other party cannot hear you.	0
features.intercom.tone	It enables or disables the phone to play a warning tone when answering an intercom call. **NOTE** It works only if "features.intercom.allow" is set to 1 (Enabled).	**0**-Disabled **1**-Enabled	1

features.intercom.barge	It enables or disables the phone to answer an incoming intercom call while there is already an active call on the IP phone. **NOTE** It works only if "features.intercom.allow" and "call_waiting.enable" are set to 1 (Enabled) and "phone_setting.call_appearance.calls_per_linekey" is greater than 1.	**0**-Disabled **1**-Enabled, the phone will automatically answer the intercom call and place the active call on hold.	0
features.intercom.barge_in_dialing.enable	It enables or disables the intercom call to answer an incoming intercom call while dialing. **NOTE** It works only if "features.intercom.barge" is set to 0 (Disabled).	**0**-Disabled **1**-Enabled	0
features.intercom.headset_prior.enable	It configures the channel mode to use when receiving an incoming intercom call.	**0**-Speaker Mode **1**-Headset Mode, it works only if you connect the headset to the IP phone and the headset mode is activated for use.	1
account.X.alert_info[1]	It configures the value of the Alert-Info header for the intercom feature. The value format likes: <sip:XXX (X can be any value)>; answer-after=0. **NOTE** If both Call-Info header (defined by the parameter "account.X.call_info") and Alert-Info header are configured, the Call-Info header has a higher priority than the Alert-Info header.	String within 256 characters	Blank

[1]X is the account ID.

Set via the Web User Interface

On the web user interface, go to **Features** > **Intercom** > **Intercom**



Remote Control

CSTA Control

User Agent Computer Supported Telecommunications Applications (uaCSTA) is explained in detail in Using CSTA for SIP Phone User Agents (uaCSTA) and Services for Computer Supported Telecommunications Applications Phase III.

The uaCSTA feature on the phone may be used for remote control of the phone from computer applications such as PC softphone. You can use the application to control the phone to perform basic call operations. For example, place a call, answer a call, end a call and transfer a call to another party.

CSTA Control Configuration

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

Configuration parameter

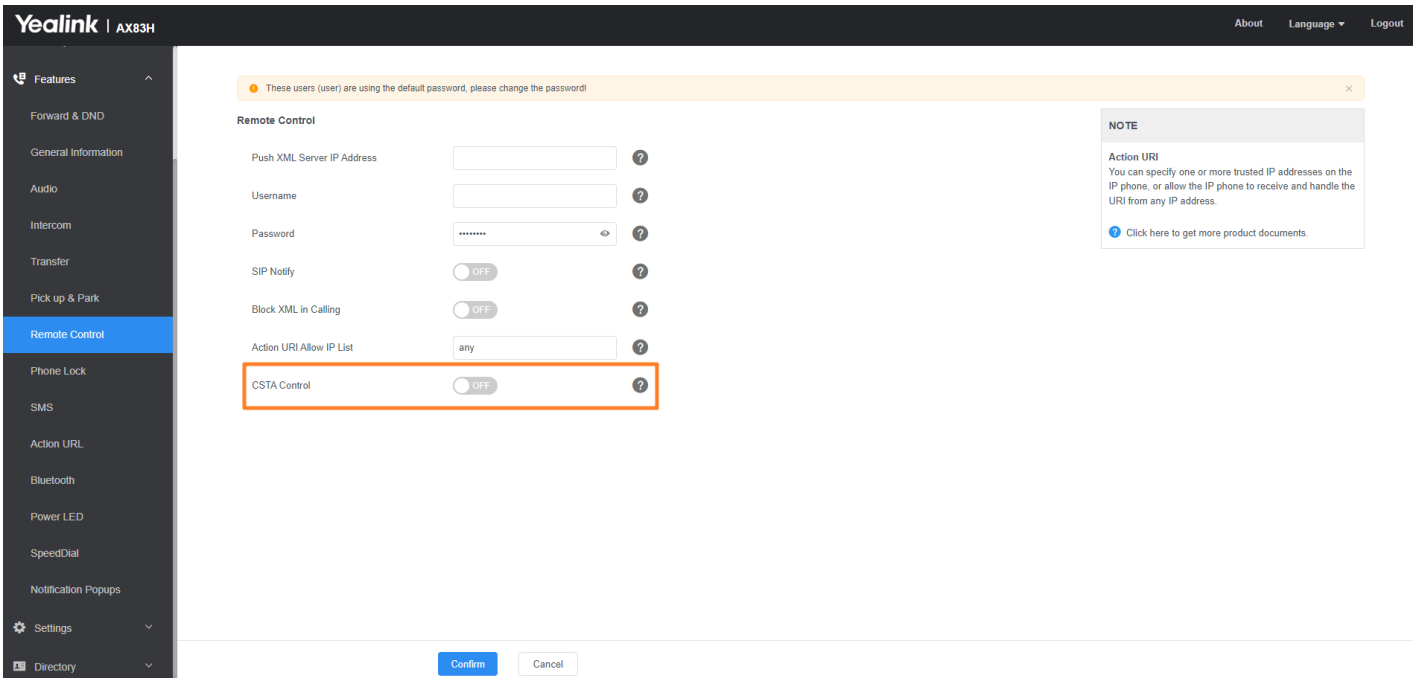
features.csta_control.enable

Parameter	Description	Permitted Values	Default	Supported Devices
features.csta_control.enable[1]	It enables or disables the CSTA feature.	0-Disabled 1-Enabled	0	All phones except T30P, T30, T19 § E2 and CP920

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

Set via the Web User Interface

On the web user interface, go to: **Features** > **Remote Control** > **CSTA Control**



Action URL

Action URL allows the phones to interact with web server applications by sending an HTTP or HTTPS GET request. You can specify a URL that triggers a GET request when a specified event occurs. Action URL can only be triggered by the predefined events (for example, Open DND). The valid URL format is: http(s):// <serverIPAddress> /help.xml?. An HTTP or HTTPS GET request may contain a variable name and a variable value, separated by "=". Each variable value starts with $ in the query part of the URL. The valid URL format is: http(s):// <serverIPAddress> /help.xml?variable name=variablevalue.Thevariablenamecanbecustomizedbyusers,whilethevariablevalueispredefined.Forexample,a URL "http://192.168.1.10/help.xml?mac=variable value. The variable name can be customized by users, while the variable value is predefined. For example, a URL "http://192.168.1.10/help.xml? mac=variablevalue.T hevariablenamecanbecustomizedbyusers, whilethevariablevalueispredefined.F orexample, a URL "http : //192.168.1.10/help.xml?mac =mac" is specified for the event Mute, the $mac will be dynamically replaced with the MAC address of the phone when the phone mutes a call.

Predefined Events List

The following table lists the predefined events for the action URL.

Event	Description
Setup Completed	When the phone completes startup.
Registered	When the phone successfully registers an account.
Unregistered	When the phone logs out of the registered account.
Register Failed	When the phone fails to register an account.

Off Hook	When the phone is off hook.
On Hook	When the phone is on hook.
Incoming Call	When the phone receives an incoming call.
Outgoing Call	When the phone places a call.
Established	When the phone establishes a call.
Terminated	When the phone terminates a call.
Open DND	When the phone enables the DND mode. **ⓘ NOTE** When the DND mode is Phone, the phone sends the action URL for all accounts; when the DND mode is Custom, the phone only sends the action URL for the corresponding account.
Close DND	When the phone disables the DND mode. **ⓘ NOTE** When the DND mode is Phone, the phone sends the action URL for all accounts; when the DND mode is Custom, the phone only sends the action URL for the corresponding account.
Always Forward On	When the phone enables the always forward. **ⓘ NOTE** When the forward mode is Phone, the phone sends the action URL for all accounts; when the forward mode is Custom, the phone only sends the action URL for the corresponding account.
Always Forward Off	When the phone disables the always forward. **ⓘ NOTE** When the forward mode is Phone, the phone sends the action URL for all accounts; when the forward mode is Custom, the phone only sends the action URL for the corresponding account.

Busy Forward On	When the phone enables the busy forward. **NOTE** When the forward mode is Phone, the phone sends the action URL for all accounts; when the forward mode is Custom, the phone only sends the action URL for the corresponding account.
Busy Forward Off	When the phone disables the busy forward. **NOTE** When the forward mode is Phone, the phone sends the action URL for all accounts; when the forward mode is Custom, the phone only sends the action URL for the corresponding account.
No Answer Forward On	When the phone enables the no answer forward. **NOTE** When the forward mode is Phone, the phone sends the action URL for all accounts; when the forward mode is Custom, the phone only sends the action URL for the corresponding account.
No Answer Forward Off	When the phone disables the no answer forward. **NOTE** When the forward mode is Phone, the phone sends the action URL for all accounts; when the forward mode is Custom, the phone only sends the action URL for the corresponding account.
Transfer Call	When the phone transfers a call.
Blind Transfer	When the phone performs the blind transfer.
Attended Transfer	When the phone performs the semi-attended/attended transfer.
Hold	When the phone places a call on hold.
UnHold	When the phone resumes a held call.
Held	When a call on the phone is held.
UnHeld	When a held call is resumed.

Mute	When the phone mutes a call.
UnMute	When the phone un-mutes a call.
Missed Call	When the phone misses a call.
IP Changed	When the IP address of the phone changes.
Idle To Busy	When the state of the phone changes from idle to busy.
Busy To Idle	When the state of the phone changes from busy to idle.
Reject Incoming Call	When the phone rejects an incoming call.
Answer New Incoming Call	When the phone answers a new call.
Transfer Failed	When the phone fails to transfer a call.
Transfer Finished	When the phone completes transferring a call.
Forward Incoming Call	When the phone forwards an incoming call.
Autop Finish	When the phone completes auto provisioning via power on.
Call Waiting On	When the phone enables the call waiting.
Call Waiting Off	When the phone disables the call waiting.
Headset	When the phone presses the HEADSET key (not applicable to CP920/CP925 /CP935W phones).
Handfree	When the phone presses the Speakerphone key (not applicable to CP920/CP925 /CP935W phones).
Cancel Call Out	When the phone cancels an outgoing call in the ring-back state.
Remote Busy	When an outgoing call is rejected.
Call Remote Canceled	When the remote party cancels the outgoing call in the ringing state.
Peripheral Information	When the accessory is unplugged or plugged.
VPN IP	When the phone IP address assigned by the VPN server changes.

Variable Values List

The following table lists predefined variable values.

Variable Value	Description
$mac	The MAC address of the phone.
$ip	The IP address of the phone.
$model	The phone model.
$firmware	The firmware version of the phone.
$active_url	The SIP URI of the current account when the phone places a call, receives an incoming call or establishes a call.
$active_user	The user part of the SIP URI for the current account when the phone places a call, receives an incoming call or establishes a call.
$active_host	The host part of the SIP URI for the current account when the phone places a call, receives an incoming call or establishes a call.
$local	The SIP URI of the caller when the phone places a call. The SIP URI of the callee when the phone receives an incoming call.
$remote	The SIP URI of the callee when the phone places a call. The SIP URI of the caller when the phone receives an incoming call.
$display_local	The display name of the caller when the phone places a call. The display name of the callee when the phone receives an incoming call.
$display_remote	The display name of the callee when the phone places a call. The display name of the caller when the phone receives an incoming call.
$call_id	The call-id of the active call.
$callerID	The display name of the caller when the phone receives an incoming call.
$calledNumber	The phone number of the callee when the phone places a call.
$exp_number	The number of connected expansion modules.
$ehs_number	The number of connected EHS.
$udisk_number	The number of connected USB flash drives.
$usbheadset_number	The number of connected USB headset devices.

$wifi_number	The number of connected Wi-Fi dongles.
$bluetooth_number	The number of connected Bluetooth dongles.
$vpn_ip	The phone IP address assigned by the VPN server.
$cfg_all	The CFG configuration file contains all current configurations of the phone. **NOTE** The valid URI is: http:// <serverIPAddress>/<filename> /?variable name=$variable value.
$cfg_local	The CFG configuration file contains all non-static parameters made via the phone user interface and web user interface. **NOTE** It works only if "static.auto_provision.custom.protect" is set to 1 (Enabled). The valid URI is: http:// <serverIPAddress>/<filename> /?variable name=$variable value

Action URL Configuration

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

Configuration parameter

action_url.setup_completed
action_url.registered
action_url.unregistered
action_url.register_failed
action_url.off_hook
action_url.on_hook
action_url.incoming_call
action_url.outgoing_call
action_url.call_established
action_url.call_terminated
action_url.dnd_on
action_url.dnd_off
action_url.always_fwd_on
action_url.always_fwd_off
action_url.busy_fwd_on
action_url.busy_fwd_off
action_url.no_answer_fwd_on
action_url.no_answer_fwd_off
action_url.transfer_call
action_url.blind_transfer_call
action_url.attended_transfer_call
action_url.hold
action_url.unhold
action_url.held
action_url.unheld
action_url.mute
action_url.unmute
action_url.missed_call
action_url.busy_to_idle
action_url.idle_to_busy
action_url.ip_change
action_url.reject_incoming_call
action_url.answer_new_incoming_call
action_url.forward_incoming_call
action_url.transfer_finished
action_url.transfer_failed
action_url.setup_autop_finish
action_url.call_waiting_on
action_url.call_waiting_off
action_url.headset
action_url.handfree
action_url.cancel_callout
action_url.remote_busy
action_url.call_remote_canceled
action_url.peripheral_information
action_url.vpn_ip
custom.action_url.view_misscall
custom.action_url.view_forward
action_url.call_established
action_url.sip_info_display_update
action_url.idle_to_busy

Parameter	Description	Permitted Values	Default

action_url.setup_completed	It configures the action URL the phone sends after startup. Example: action_url.setup_completed = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.registered	It configures the action URL the phone sends after an account is registered. Example: action_url.registered = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.unregistered	It configures the action URL the phone sends after an account is unregistered. Example: action_url.unregistered = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.register_failed	It configures the action URL the phone sends after a register failed. Example: action_url.register_failed = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.off_hook	It configures the action URL the phone sends when off hook. Example: action_url.off_hook = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.on_hook	It configures the action URL the phone sends when on hook. Example: action_url.on_hook = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.incoming_call	It configures the action URL the phone sends when receiving an incoming call. Example: action_url.incoming_call = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.outgoing_call	It configures the action URL the phone sends when placing a call. Example: action_url.outgoing_call = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank

action_url.call_established	It configures the action URL the phone sends when establishing a call. Example: action_url.call_established = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.call_terminated	It configures the action URL the phone sends when terminating a call. Example: action_url.call_terminated = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.dnd_on	It configures the action URL the phone sends when DND feature is activated. Example: action_url.dnd_on = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.dnd_off	It configures the action URL the phone sends when DND feature is deactivated. Example: action_url.dnd_off = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.always_fwd_on	It configures the action URL the phone sends when the always forward feature is activated. Example: action_url.always_fwd_on = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.always_fwd_off	It configures the action URL the phone sends when the always forward feature is deactivated. Example: action_url.always_fwd_off = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.busy_fwd_on	It configures the action URL the phone sends when the busy forward feature is activated. Example: action_url.busy_fwd_on = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.busy_fwd_off	It configures the action URL the phone sends when the busy forward feature is deactivated. Example: action_url.busy_fwd_off = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank

action_url.no_answer_fwd_on	It configures the action URL the phone sends when the no answer forward feature is activated. Example: action_url.no_answer_fwd_on = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.no_answer_fwd_off	It configures the action URL the phone sends when the no answer forward feature is deactivated. Example: action_url.no_answer_fwd_off = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.transfer_call	It configures the action URL the phone sends when performing a transfer. Example: action_url.transfer_call = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.blind_transfer_call	It configures the action URL the phone sends when performing a blind transfer. Example: action_url.blind_transfer_call = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.attended_transfer_call	It configures the action URL the phone sends when performing an attended/semi-attended transfer. Example: action_url.attended_transfer_call = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.hold	It configures the action URL the phone sends when placing a call on hold. Example: action_url.hold = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.unhold	It configures the action URL the phone sends when resuming a holding call. Example: action_url.unhold = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.held	It configures the action URL the phone sends when a call is held. Example: action_url.held = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.unheld	It configures the action URL the phone sends when a held call is resumed. Example: action_url.unheld = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank

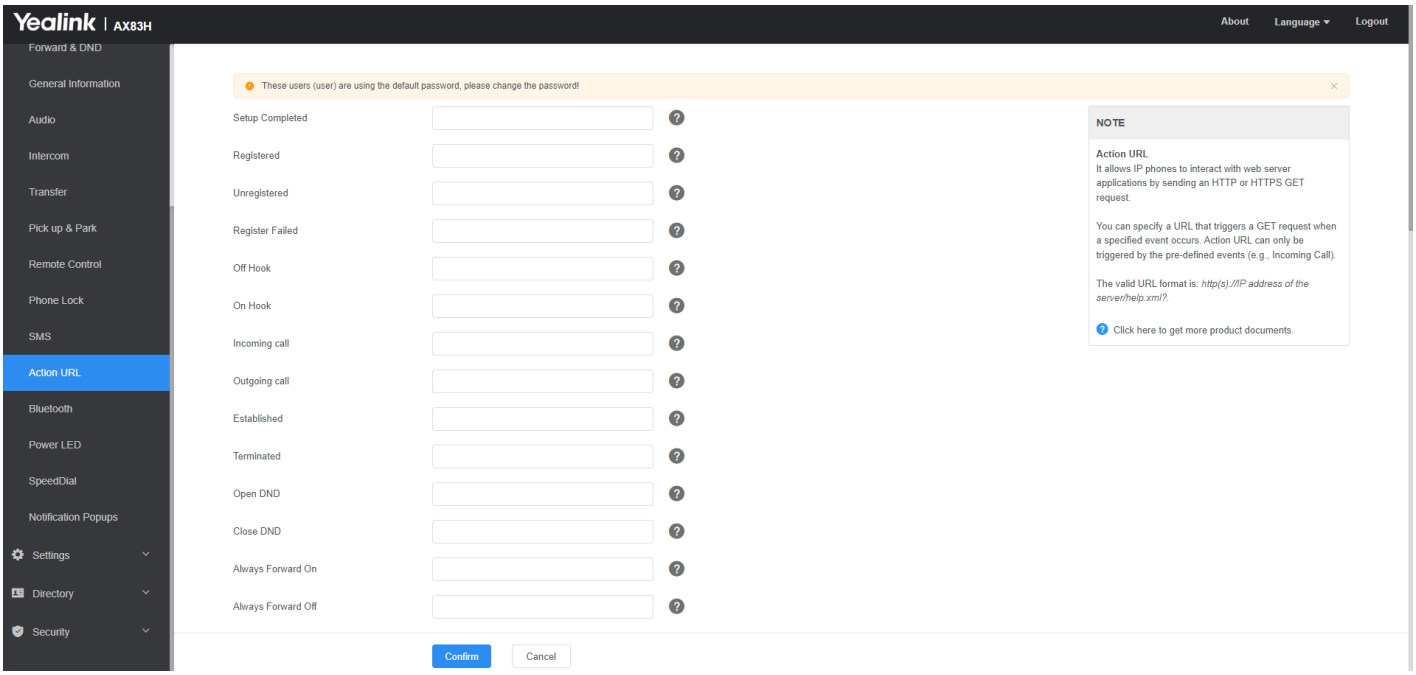
action_url.mute	It configures the action URL the phone sends when muting a call. Example: action_url.mute = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.unmute	It configures the action URL the phone sends when unmuting a call. Example: action_url.unmute = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.missed_call	It configures the action URL the phone sends when missing a call. Example: action_url.missed_call = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.busy_to_idle	It configures the action URL the phone sends when changing the state of the phone from busy to idle. Example: action_url.busy_to_idle = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.idle_to_busy	It configures the action URL the phone sends when changing the state of the phone from idle to busy. Example: action_url.idle_to_busy = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.ip_change	It configures the action URL the phone sends when changing the IP address of the phone. Example: action_url.ip_change = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.reject_incoming_call	It configures the action URL the phone sends when rejecting an incoming call. Example: action_url.reject_incoming_call = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.answer_new_incoming_call	It configures the action URL the phone sends when answering a new incoming call. Example: action_url.answer_new_incoming_call = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.forward_incoming_call	It configures the action URL the phone sends when forwarding an incoming call. Example: action_url.forward_incoming_call = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank

action_url.transfer_finished	It configures the action URL the phone sends when completing a call transfer. Example: action_url.transfer_finished = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.transfer_failed	It configures the action URL the phone sends when failing to transfer a call. Example: action_url.transfer_failed = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.setup_autop_finish	It configures the action URL the phone sends when completing auto provisioning via power on. Example: action_url.setup_autop_finish = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.call_waiting_on	It configures the action URL the phone sends when the call waiting feature is enabled. Example: action_url.call_waiting_on = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.call_waiting_off	It configures the action URL the phone sends when the call waiting feature is disabled. Example: action_url.call_waiting_off = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.headset	It configures the action URL the phone sends when pressing the HEADSET key. Example: action_url.headset = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.handfree	It configures the action URL the phone sends when pressing the Speakerphone key. Example: action_url.handfree = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.cancel_callout	It configures the action URL the phone sends when canceling the outgoing call in the ring-back state. Example: action_url.cancel_callout= http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank

action_url.remote_busy	It configures the action URL the phone sends when the outgoing call is rejected. Example: action_url.remote_busy = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.call_remote_canceled	It configures the action URL the phone sends when the remote party cancels the outgoing call in the ringing state. Example: action_url.call_remote_canceled= http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.peripheral_information	It configures the action URL the phone sends when you unplug or plug the accessory. Example: action_url.peripheral_information = http://192.168.0.20/help.xml?IP=ip&WIFI=wifi_number	URL within 511 characters	Blank
action_url.vpn_ip	It configures the action URL the phone sends when the IP address assigned by the VPN server changes. Example: action_url.vpn_ip= http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
custom.action_url.view_misscall	It is used to configure the URL for viewing missed calls in the ActionURL.	URL within 511 characters	Blank
custom.action_url.view_forward	It is used to configure the URL for viewing forward calls in the ActionURL.	URL within 511 characters	Blank
action_url.call_established	It configures the action URL the phone sends when establishing a call. Example: action_url.call_established = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank
action_url.sip_info_display_update	It is used to configure the action URL triggered by receiving SIP INFO messages during a call.	URL within 511 characters	Blank
action_url.idle_to_busy	It configures the action URL the phone sends when changing the state of the phone from idle to busy. Example: action_url.idle_to_busy = http://192.168.0.20/help.xml?IP=$ip	URL within 511 characters	Blank

Set via the Web User Interface

On the web user interface, go to: **Features** > **Action URL**



Action URI

Yealink phones can perform the specified action by receiving and handling an HTTP or HTTPS GET request or accept a SIP NOTIFY message with the "Event: ACTION-URI" header from a SIP proxy server.

Supported HTTP/HTTPS GET Request

Opposite to action URL, action URI allows the phones to interact with a web server application by receiving and handling an HTTP or HTTPS GET request. When receiving a GET request, the phone will perform the specified action and respond with a 200 OK message.
A GET request may contain a variable named as "key" and a variable value, which are separated by "=". The valid URI format is: http(s):// `<phoneIPAddress>` /servlet?key=variable value.

ⓘ NOTE
Yealink phones are compatible with other two old valid URI formats: http(s):// `<phoneIPAddress>` /cgi-bin/ConfigManApp.com?key=variable value and http(s):// `<phoneIPAddress>` /cgi-bin/cgiServer.exx?key=variable value.

For security reasons, the phones do not handle HTTP/HTTPS GET requests by default. You need to specify the trusted IP address for action URI. You can specify one or more trusted IP addresses on the phone, or configure the phone to receive and handle the URI from any IP address.

Supported SIP Notify Message

In addition, Yealink phones can perform the specified action immediately by accepting a SIP NOTIFY message with the "Event: ACTION-URI" header from a SIP proxy server. The message body of the SIP NOTIFY message may contain a variable named as "key" and a variable value, which are separated by "=".
This method is especially useful for users who always work in the small office/home office where a secure firewall

may prevent the HTTP or HTTPS GET request from the external network.

NOTE
If you want to only accept the SIP NOTIFY message from your SIP server and outbound proxy server, you have to enable the Accept SIP Trust Server Only feature. For more information, refer to Accept SIP Trust Server Only.

If you use SIP NOTIFY message method, you do not need to specify the trusted IP address for action URI. However, you should enable the phone to receive the action URI requests.
Example of a SIP Notify with the variable value (OK):

```
Message Header
NOTIFY sip:3583@10.2.40.10:5062 SIP/2.0
Via: SIP/2.0/UDP 10.2.40.27:5063;branch=z9hG4bK4163876675
From: <sip:3586@10.2.1.48 > ;tag=2900480538
To: "3583" <sip:3583@10.2.1.48 > ;tag=490600926
Call-ID: 2923387519@10.2.40.10
CSeq: 4 NOTIFY
Contact: <sip:3586@10.2.40.27:5063 >
Max-Forwards: 70


User-Agent: Yealink SIP-T46G
Event: ACTION-URI
Content-Type: message/sipfrag
Content-Length: 6

Message Body
key=OK
```

Variable Values List

Yealink phones also support a combination of the variable values in the URI, but the order of the variable value is determined by the operation of the phone. The valid URI format is: http(s):// `<phoneIPAddress>` /servlet?key=variable value[;variable value]. Variable values are separated by a semicolon from each other. Th
The following shows an example for deleting all entries from the call history list when the phone is idle: http://10.3.20.10/servlet?key=F1;F3;DOWN;DOWN;DOWN;OK;OK.

NOTE
The variable value is not applicable to all events. For example, the variable value “MUTE” is only applicable when the IP phone is during a call. When authentication is required, you can use the following URI format: http(s)://username:password@/servlet?key=variable value. If you are using a browser, we recommend that you use Firefox.

The following table lists predefined variable values:

Variable Value	Phone Action

OK	Press the OK/√ / key.
ENTER	Press the Enter soft key.
SPEAKER	Press the Speakerphone key.
F_TRANSFER	Transfer a call to another party.
VOLUME_UP	Increase the volume.
VOLUME_DOWN	Decrease volume.
MUTE	Mute a call.
F_HOLD/HOLD	Place an active call on hold.
F_CONFERENCE	Press the Conf/Conference soft key.
Cancel/CANCEL	Cancel actions, reject incoming calls or end a call.
X	Cancel actions, reject incoming calls or mute or un-mute calls.
0-9/*/POUND	Press the keypad (0-9, * or #).
L1-LX	Press the line keys.
LX_LONGPRESS[1]	Perform a corresponding action when long pressing line key X.
BACK_IDLE	Return idle screen directly.
F1-F4	Press the soft keys.
MSG	Press the MESSAGE key.
HEADSET	Press the HEADSET key.
RD	Press the RD/Redial key.
UP/DOWN/LEFT/RIGHT	Press the navigation keys.
Reboot	Reboot the phone.
AutoP	Perform auto provisioning.
DNDOn	Activate the DND feature. **NOTE** It works only if "features.dnd.allow" is set to 1 (Enabled).

DNDOff	Deactivate the DND feature. **NOTE** It works only if "features.dnd.allow" is set to 1 (Enabled).
number=xxx&outgoing_uri=y	Place a call to xxx from SIP URI y. Example: http://10.3.20.10/servlet?key=number=1234&outgoing_uri=1006@10.2.1.48 (1234 means the number you dial out; 1006@10.2.1.48 means the SIP URL you dial from.)
OFFHOOK	Pick up the handset. (not applicable to CP920/CP925/CP935W phones) Press the off-hook key. (only applicable to CP920 phones)
ONHOOK	Hang up the handset (not applicable to CP920/CP925/CP935W phones). Press the on-hook key. (only applicable to CP920 phones)
ANSWER/ASW/Asw	Answer a call.
Reset	Reset a phone.
ATrans=xxx	Perform a semi-attended/attended transfer to xxx.
ATrans=callid_A@callid_B	Join any two call parties together on the phone using the call-id. After the call is set up, the two parties disconnect with the phone. Scene: A and D are in a call, the call is active; B and D are in a call, the call is placed on hold; C and D are in a call, the call is placed on hold; callid_A: 32775 callid_B: 32776 Example: http://10.10.20.10/servlet?key=ATrans=32775@32776%3Cbr />It means A and B join together and then disconnect with D. But the call between C and D is still in a hold state. **NOTE** To get the call-id of the active call, configure the action URL: http(s):// /help.xml?CallId=$call_id. For more information, refer to Action URL.
BTrans=xxx	Perform a blind transfer to xxx.

phonecfg=get[&accounts=x][&dnd=x][&fw=x]	Get firmware version, registration, DND or forward configuration information. The valid value of "x" is 0 or 1, 0 means you do not need to get configuration information. 1 means you want to get configuration information. **ⓘ NOTE** The valid URI is: http(s):// /servlet?phonecfg=get[&accounts=x][&dnd=x][&fw=x]. Example: http://10.3.20.10/servlet?phonecfg=get[&accounts=1][&dnd=0][&fw=1]
phonecfg=set[&configuration parameter=value]	Set the valid value for the specified configuration parameter. **ⓘ NOTE** The valid URI is: http(s):///servlet?phonecfg=set[&configuration parameter=value]…[&configuration parameter=value]. It can contain up to 10 configuration parameters. Example: http://10.3.20.10/servlet?phone cfg=set[&account.1.enable=1][&features.dnd.enable=1]
phonecfg=get[&configuration parameter]	Get the specified configuration information. Note: The valid URI is: http(s):///servlet?phonecfg=get[&configuration parameter]…[&configuration parameter]. It can contain up to 10 configuration parameters. Example: http://10.3.20.10/servlet?phonecfg= get[&account.1.enable][&features.dnd.enable]
CallWaitingOn	Activate the call waiting feature.
CallWaitingOff	Deactivate the call waiting feature.
AlwaysFwdOn/BusyFwdOn/NoAnswFwdOn=xxx=n	Activate an always/busy/no answer forward feature to xxx for the phone ("xxx" means the destination number) The valid value of "n" means the duration time (seconds) before forwarding incoming calls (n is the times of 6, for example, 24). It is only applicable to no answer forward feature. **ⓘ NOTE** For Yealink phones, it works only if "features.fwd.allow" is set to 1 (Enabled) and call forward mode is Phone, the always/busy/no answer forward feature will apply to all the accounts on the phone. Example: http://10.10.20.10/servlet?key=NoAnswFwdOn=1001=24

AlwaysFwdOff/ BusyFwdOff/N oAnswFwdOff	Deactivate the always/busy/no answer forward feature for the phone. **NOTE** For Yealink phones, it works only if "features.fwd.allow" is set to 1 (Enabled) and call forward mode is Phone, the always/busy/no answer forward feature will apply to all the accounts on the phone. Example: http://10.10.20.10/servlet?key=NoAnswFwdOff
CALLEND/CallE nd	End a call.
ASW/CANCEL/ HOLD/UNHOL D:xxx	Answer/end/hold/unhold a call (xxx refers to the call-id of the active call). Example: http://10.10.20.10/servlet?key=ASW:33093%3Cbr /> **NOTE** To get the call-id of the active call, configure the action URL: http(s):// <serverIPAddress> /help.xml?CallId=$call_id. For more information, refer to Action URL.
ACDlogin	Log into the ACD system. **NOTE** When ACD authentication information is required, the valid URI is: http(s):// <phoneIPAddress> /servlet?key=ACDlogin&agentID=xxx&password=xxx. When ACD authentication information is not required, the valid URI is: http(s):// <phoneIPAddress> /servlet?key=ACDlogin.
ACDlogout	Log out of the ACD system.
SWAP	Swap to the held call when there is an active call and a held call on the phone.
SPLIT	Split the local conference call into individual calls. After the split, the conference call ends, and other parties are held. **NOTE** It is not available for network conference.

[1]X is the line key ID.

Action URI Configuration

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

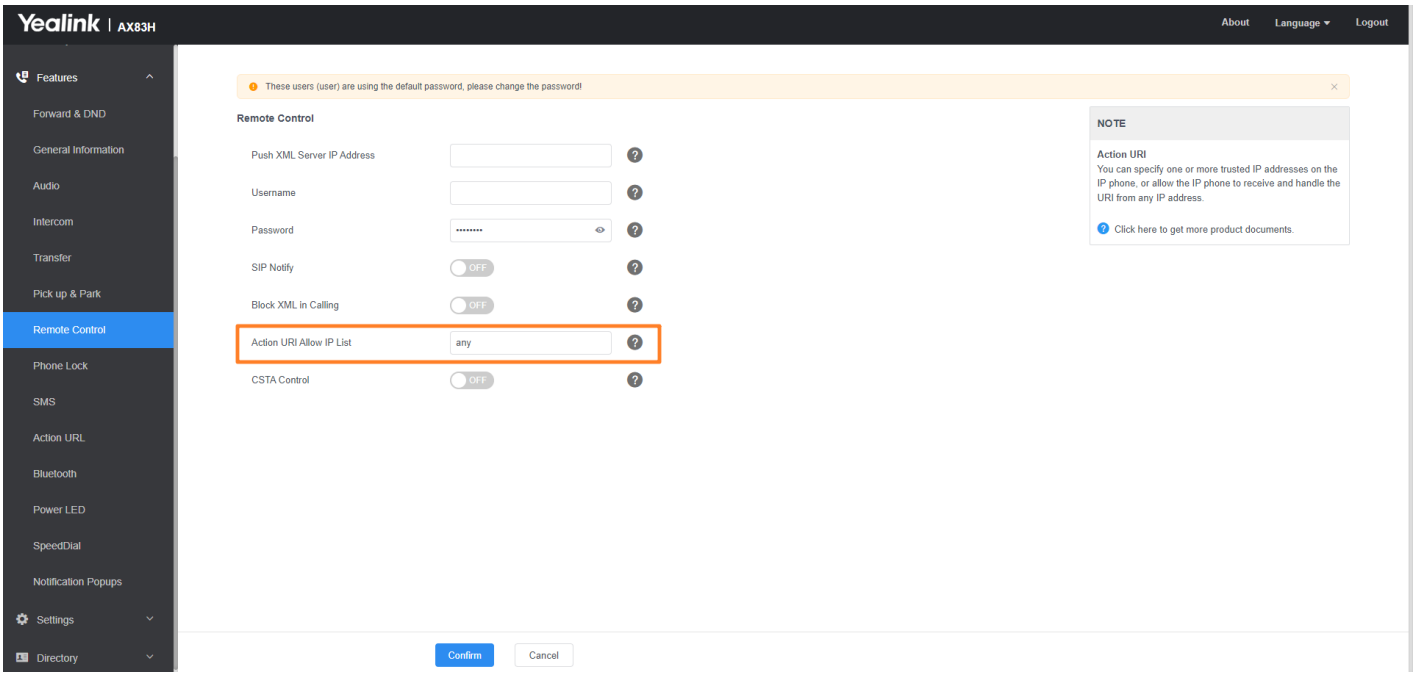
Configuration parameter

```
features.action_uri.enable
features.show_action_uri_option
features.action_uri_limit_ip
```

Parameter	Description	Permitted Values	Default
features.action_uri.enable	It enables or disables the phone to receive the action URI requests.	0-Disabled 1-Enabled	1
features.show_action_uri_option	It enables or disables the phone to pop up the Allow Remote Control prompt when receiving action URI requests. **NOTE** It works only if "features.action_uri.enable" is set to 1 (Enabled).	0-Disabled 1-Enabled	1
features.action_uri_limit_ip	It configures server address from which the phone receives the action URI requests. Multiple addresses are separated by commas. (for example, 10.1.4.3,10.1.4.23); Support asterisk wildcard, each asterisk represents a field of the IP address (10.10.. represents 10.10.0.0 to 10.10.255.255). **NOTE** It works only if "features.action_uri.enable" is set to 1 (Enabled).	IP address Blank-the phone will reject any HTTP GET request. any-the phone will accept and handle HTTP GET requests from any IP address.	Blank

Set via the Web User Interface

On the web user interface, go to **Features** > **Remote Control** > **Action URI Allow IP List**



Example: Capturing the Current Screen of the Phone

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

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

ⓘ NOTE

Yealink phones also support capturing the screen display using the old URI "http:// <phoneIPAddress> /servlet?command=screenshot".

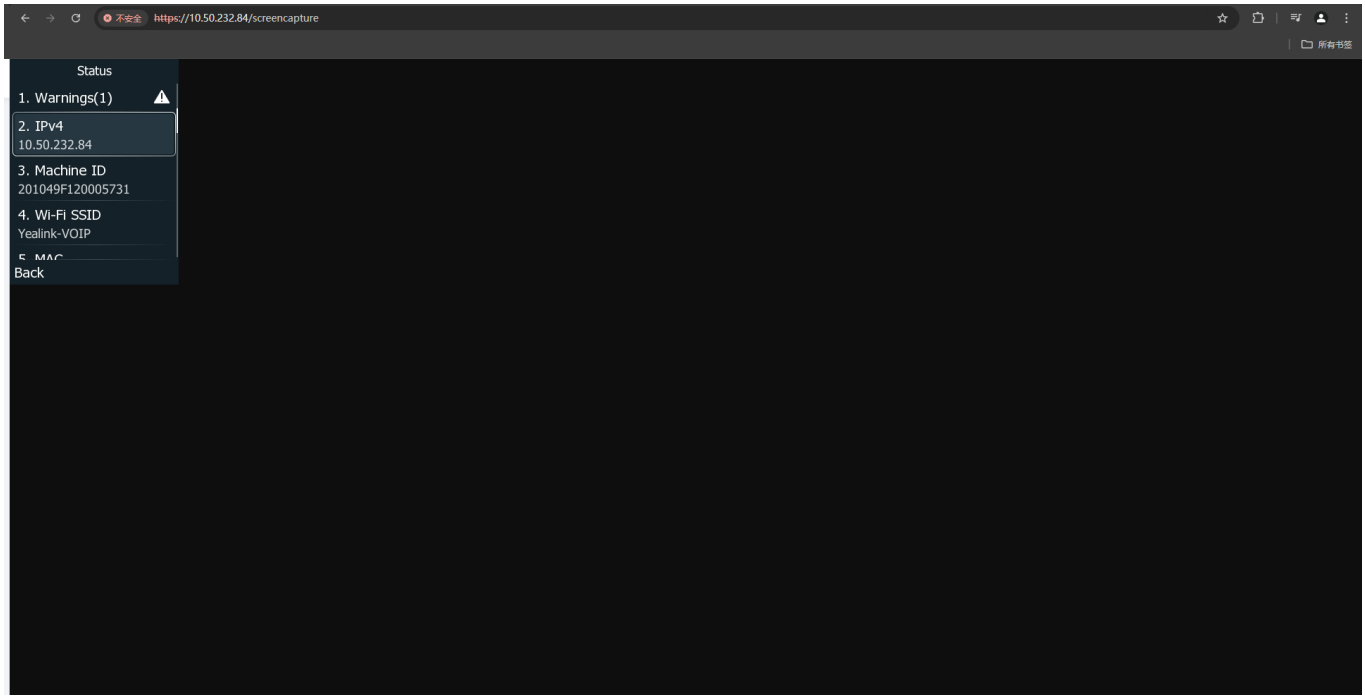
Before capturing the phone's current screen, ensure that the IP address of the computer is included in the trusted IP address for Action URI on the phone. When you capture the screen display, the phone may prompt you to enter the user name and password of the administrator if the web browser does not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

Procedure

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. Do one of the following:

- If it is the first time you capture the phone's current screen using the computer, the browser will display "Remote control forbidden", and the phone screen will prompt the message "Allow remote control?".
- Press OK on the phone to allow remote control. The phone will return to the previous screen.

- Refresh the web page.
- The browser will display an image of the phone’s current screen. You can save the image to your local system.



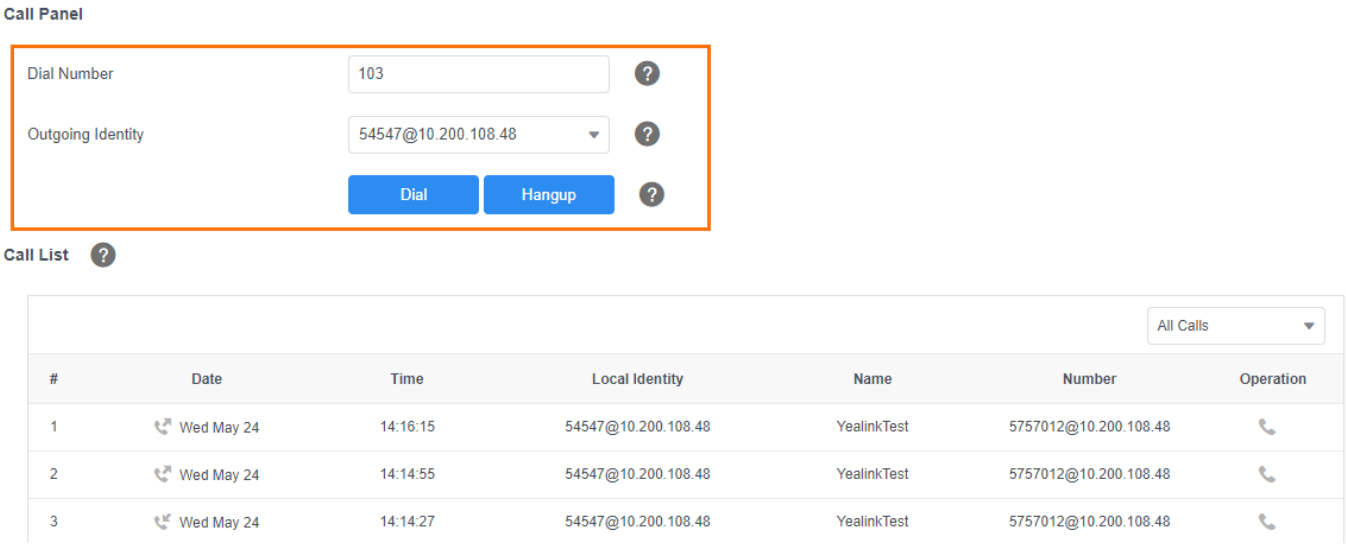
- Else, the browser will display an image of the phone’s current screen directly. You can save the image to your local system.

NOTE
Frequent capture may affect phone performance. Yealink recommends you to capture the phone screen display within a minimum interval of 4 seconds.

Example: Placing a Call via Web User Interface

Procedure

1. Go to **Directory** > **Phone Call Info**.
2. Select the desired account from the Outgoing Identity drop-down menu.
3. Enter the callee’s number in the Dial Number field.



4. Click Dial to dial out the number.

The web user interface prompts "Call Success" and the phone will automatically dial out the number.
You can click Hang Up to end the call.
If it is the first time you place a call via the web user interface, the LCD screen will prompt the message "Allow remote control?". Press OK on the phone to allow remote control and then the phone will automatically dial out the number.

NOTE
You can also place an IP direct call via the web user interface. The phone supports either IPv4 or IPv6 address.

Voice Mail & SMS

Voice Mail

Yealink phones support voice mail.
You can configure a message waiting indicator (MWI) to inform users how many messages are waiting in their mailbox without calling the mailbox. Yealink phones support both audio and visual MWI alert when receiving new voice messages.

MWI for Voice Mail Configuration

Yealink phones support both solicited and unsolicited MWI.
Unsolicited MWI: The IP phone sends a SUBSCRIBE message to the server for message-summary updates. The server sends a message-summary NOTIFY within the subscription dialog each time the MWI status changes. Unsolicited MWI is a server related feature.
Solicited MWI: The phone can subscribe to the MWI messages to the account or the voice mail number. For solicited MWI, you must enable MWI subscription feature on the phones.
Server Voicemail: Play server voicemail content on the IP Phone with a maximum playback duration of two

minutes.

The following table lists the parameters you can use to configure MWI for voice mail.

Configuration parameter

```
account.X.subscribe_mwi
account.X.subscribe_mwi_expires
account.X.mwi_parse_terminated
account.X.sub_fail_retry_interval
account.X.subscribe_mwi_to_vm
voice_mail.number.X
account.X.display_mwi.enable
features.voice_mail_alert.enable
features.voice_mail_key_lamp_field.enable
features.hide_unread_vm_number.enable
```

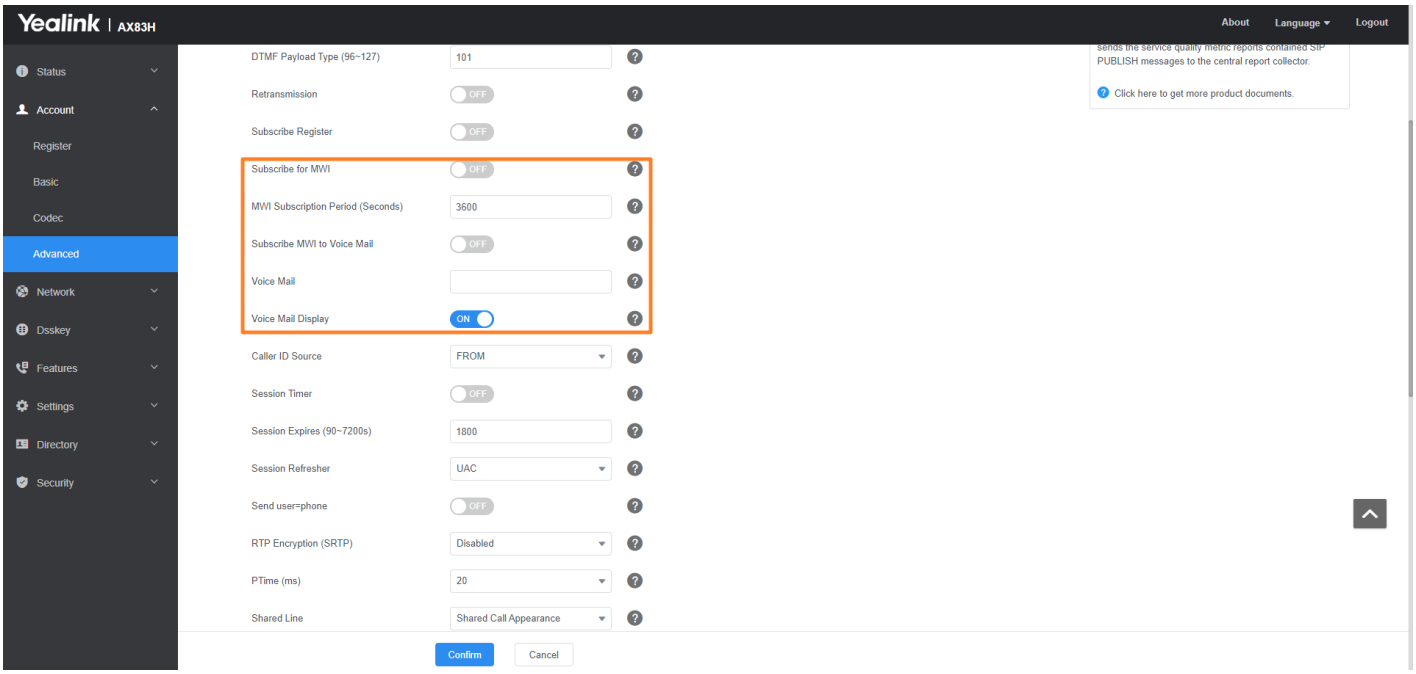
Parameter	Description	Permitted Values	Default
account.X.subscribe_mwi[1]	It enables or disables the phone to subscribe to the message waiting indicator.	**0**-Disabled, the server automatically sends a message-summary NOTIFY in a new dialog each time the MWI status changes (This requires server support). **1**-Enabled, the phone will send a SUBSCRIBE message to the server for message-summary updates.	0
account.X.subscribe_mwi_expires[1]	It configures MWI subscribe expiry time (in seconds). **NOTE** It works only if "account.X.subscribe_mwi" is set to 1 (Enabled).	Integer from 0 to 84600	3600
account.X.mwi_parse_terminated[1]	It enables or disables the phone to parse the Terminated attribute in the received MWI NOTIFY message.	**0**-Disabled **1**-Enabled	0
account.X.sub_fail_retry_interval[1]	It configures the interval (in seconds) for the phone to re-subscribe when the subscription fails.	Integer from 0 to 3600	30

account.X.subscribe_mwi_to_vm[1]	It enables or disables the phone to subscribe to the message waiting indicator for the voicemail number. **NOTE** It works only if "account.X.subscribe_mwi" is set to 1 (Enabled) and "voice_mail.number.X" is configured.	**0**-Disabled, the phone will subscribe to the message waiting indicator to a specific account. **1**-Enabled	0
voice_mail.number.X[1]	It configures the voice mail number.	String within 99 characters	Blank
account.X.display_mwi.enable[1]	It enables or disables the MWI alert to indicate that you have an unread voice mail message.	**0**-Disabled **1**-Enabled	1
features.voice_mail_alert.enable	It enables or disables the phone to pop up the message when receiving the same amount of new voicemails.	**0**-Disabled **1**-Enabled	0
features.voice_mail_key_lamp_field.enable	It enables or disables the phone to subscribe to the message waiting indicator for the voice mail number when configuring a Voice Mail dsskey.	**0**-Disabled **1**-Enabled, the phone will subscribe to the value of the Voice Mail dsskey from the server. When there are unread voice messages, the dsskey LED indicator flashes or the dsskey icon indicates the number of unread messages.	0
features.hide_unread_vm_number.enable	It enables or disables the phone to hide the number of unread voice mails in the pop-up message box.	**0**-Disabled **1**-Enabled	0

[1]X is the account ID.

Set via the Web User Interface

On the web user interface, go to: **Account** > **Advanced** > **Subscribe for MWI / MWI Subscription Period(Seconds) / Subscribe MWI to Voice Mail / Voice Mail Display**



Short Message Service (SMS)

Yealink phones support short message service (SMS). It allows users to send and receive a text message on the support server.

By default, SMS is enabled. You can use SMS at the path: **Menu** > **Message** > **Text Message**. You can also disable SMS.

SMS Configuration

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

Configuration parameter

```
features.text_message.enable
```

Parameter	Description	Permitted Values	Default
features.text_message.enable	It enables or disables the phone to send and receive a text message.	**0**-Disabled **1**-Enabled	1

XML Browser

XML Browser

XML browser simply means that the phone screen display can be managed by external applications. The XML browser feature allows users to develop and deploy custom services that meet the user’ s functional requirements on the server. Users can customize practical applications, such as weather reports, stock information, Google

search, news service, and so on.

To use the XML browser feature, you must configure an XML browser key in advance.

For more information on XML browser, refer to Yealink IP Phones XML Browser Developer's Guide .

XML Browser Configuration

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

Configuration parameter

```
push_xml.server
push_xml.block_in_calling
push_xml.sip_notify
push_xml.phonebook.search.delay
features.xml_browser.loading_tip.delay
features.xml_browser.user_name
features.xml_browser.pwd
push_xml.username
push_xml.password
features.upload_server
xmlbrowser_icon_upload.url
xmlbrowser_icon.delete
```

Parameter	Description	Permitted Values	Default	Web UI
push_xml.server	It configures the address of the push XML server.	Blank-The phone will reject HTTP POST messages from any server. any-The phone will accept HTTP POST messages from any server. IP address or domain name-Multiple addresses are separated by commas. (for example, 10.1.4.3,10.1.4.23); Support asterisk wildcard, each asterisk represents a field of the IP address (10.10.. represents 10.10.0.0 to 10.10.255.255).	Blank	Features > Remote Control > Push XML Server IP Address
push_xml.block_in_calling	It enables or disables the phone to block XML applications during a call.	0-Disabled 1-Enabled	0	Features > Remote Control > Block XML in Calling
push_xml.sip_notify	It enables or disables the phone to process the push XML via SIP NOTIFY message.	0-Disabled 1-Enabled	0	Features > Remote Control > SIP Notify

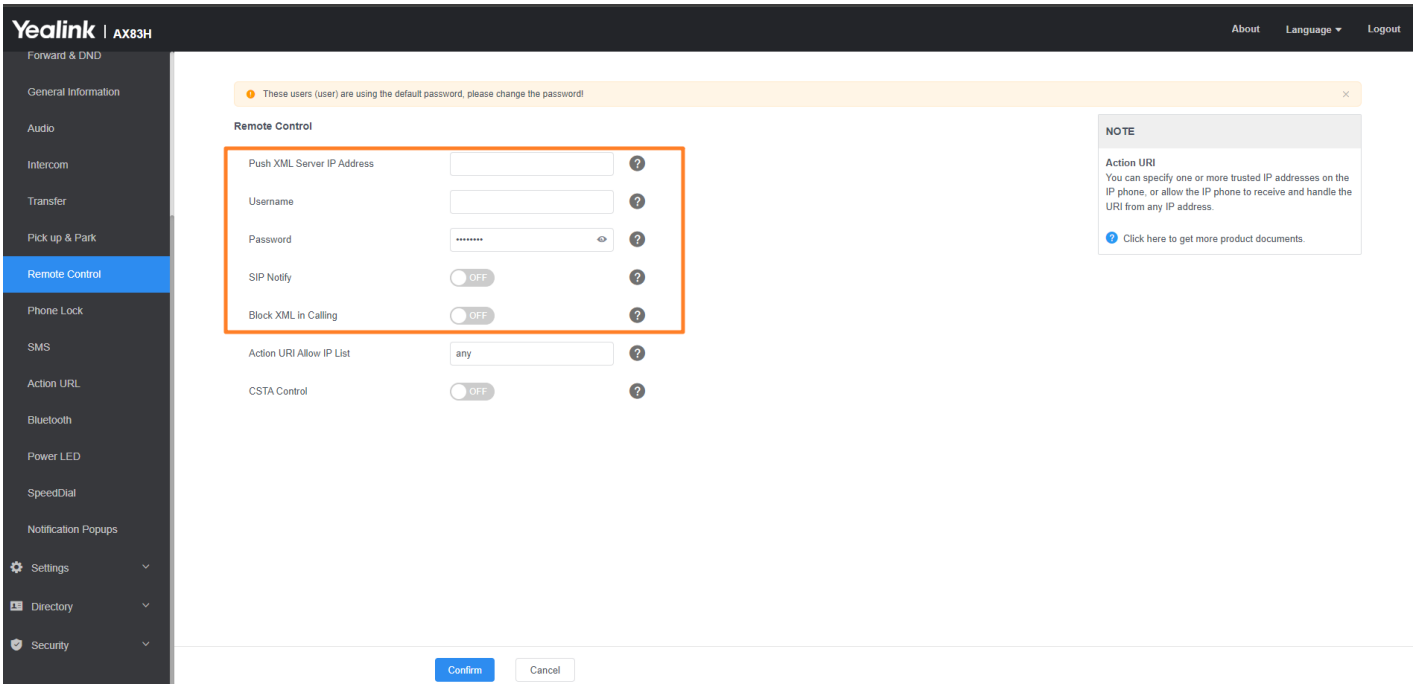
push_xml.phonebook.search.delay	It configures the time (in milliseconds) to wait for the phone to send the entered keywords to XML phonebook server if the user does not press OK to confirm. If it is set to 0, the phone immediately sends the entered keywords to the server.	Integer from 0 to 10000	1000	
features.xml_browser.loading_tip.delay	It configures the time (in milliseconds) to wait for the phone to display the loading tip. If the phone doesn't finish loading an XML page within the specified time, the tip, "Loading, please wait" appears on the LCD screen. If it is set to 0, the loading tip feature is disabled. **ⓘ NOTE** It is not applicable to ImageScreen Object and ImageMenu Object.	Integer from 0 to 50000	100	
features.xml_browser.user_name	It configures the authentication user name for the XML request.	String within 15 characters	Blank	
features.xml_browser.pwd	It configures the authentication password for the XML request.	String within 15 characters	Blank	

push_xml.username	It configures the user name for the phone to authenticate with the push XML server. Leave it blank if no authentication is required.	String	Blank	Features > Remote Control > User Name
push_xml.password	It configures the password for the phone to authenticate with the push XML server. Leave it blank if no authentication is required.	String within 15 characters	Blank	Features > Remote Control > Password
features.upload_server	It configures the server address to which the DssKey.cfg file is uploaded when the phone receives an XML command (Command:UploadSystemInfo).	URL within 1024 characters	Blank	
xmlbrowser_icon_upload.url	It configures the access URL of the *.tar file for custom icons displayed by XML browser. **NOTE** The phone supports icons in `*.jpg/*.png/*.bmp/*.jpeg` format.	URL within 511 characters	Blank	

xmlbrowser_icon.delete	It deletes the specified or all custom icons for XML browser. Example: Delete all custom icons for XML browser: xmlbrowser_icon.delete = http://localhost/all Delete a custom icon for XML browser (for example, customicon.jpg): xmlbrowser_icon.delete = http://localhost/customicon.jpg	http://localhost/all or http://localhost/name.(jpg/png/bmp/jpeg/dob)	Blank	

Set via the Web User Interface

On the web user interface, go to **Features** > **Remote Control** > **Push XML Server IP Address / Block XML in Calling / SIP Notify / User Name / Password**.



Hot Desking

Hot Desking

A primary motivation for hot desking is cost reduction. Hot desking is regularly used in places where not all employees are in the office at the same time, or not in the office for a long time, which means actual personal offices would often be vacant, consuming valuable space and resources.

Hot desking allows the user to clear pre-registration configurations of all accounts on the phone.
To use this feature, you need to assign a Hot Desking key. You can also specify which registration configurations are available to users.

Hot Desking Key Configuration

The following shows the configuration for a Hot Desking key.

Programmable Key Configuration
programablekey.X.type = 34 programablekey.X.label = Bill (Only applicable to SoftKey1 and SoftKey2.)

After provisioning, a Hot Desking key is available on the phone. You can press the Hot Desking key to clear the pre-registration configurations of all accounts and register your own account on line 1.

Hot Desking Configuration

You can specify available configurations for registration when using hot desking.
The following table lists the parameters you can use to configure hot desking.

Configuration parameter

```
hotdesking.dsskey_register_name_enable
hotdesking.dsskey_username_enable
hotdesking.dsskey_password_enable
hotdesking.dsskey_sip_server_enable
hotdesking.dsskey_outbound_enable
features.hotdesking_clear_calllog.enable
hotdesking.log_out_prompt.time
hotdesking.log_out_prompt.duration
```

Parameter	Description	Permitted Values	Default
hotdesking.dsskey_register_name_enable	It enables or disables the phone to provide an input field of register name on the hot desking login wizard when pressing the Hot Desking DSS key.	**0**-Disabled **1**-Enabled	0
hotdesking.dsskey_username_enable	It enables or disables the phone to provide an input field of user name on the hot desking login wizard when pressing the Hot Desking DSS key.	**0**-Disabled **1**-Enabled	1
hotdesking.dsskey_password_enable	It enables or disables the phone to provide an input field of password on the hot desking login wizard when pressing the Hot Desking DSS key.	**0**-Disabled **1**-Enabled	1

hotdesking.dsskey_sip_server_enable	It enables or disables the phone to provide an input field of SIP server on the hot desking login wizard when pressing the Hot Desking DSS key.	**0**-Disabled **1**-Enabled	0
hotdesking.dsskey_outbound_enable	It enables or disables the phone to provide an input field of the outbound server on the hot desking login wizard when pressing the Hot Desking DSS key.	**0**-Disabled **1**-Enabled	0
features.hotdesking_clear_calllog.enable	It enables or disables the phone to clear call records of the last guest after using hot desking to log into a new account.	**0**-Disabled **1**-Enabled	0
hotdesking.log_out_prompt.time	It is used to configure the time interval for prompting to clear account information: After registering an account, if there is no activity for a certain period of time, the phone will display a pop-up window to prompt clearing the account information (in minutes).	**0**: Do not clear **1-1440**: Display a pop-up window to prompt clearing the account information after the specified period of inactivity.	0
hotdesking.log_out_prompt.duration	It is used to control the duration in seconds before executing the exit action after displaying the pop-up window.	**-1**: No pop-up, exit directly **0**: No automatic exit **1-86400**: Auto exit after the corresponding time	0

Device Management

Device Management

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 view device information, manage devices, and diagnose devices.

NOTE
Ensure that you have enabled the feature of Connect DM Service (on the phone screen, go to **Menu > Security > Connect DM Service**). Otherwise, you cannot connect phones to the YDMP/YMCS. After you enable this feature, you also need the following parameters to connect phones to the YDMP/YMCS.

Device Management Configuration

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

Configuration parameter

```
static.dm.enable
static.dm.server.address
static.dm.server.port
phone_setting.qoe.enable
static.remote_control.X.allow
```

Parameter	Description	Permitted Values	Default
static.dm.enable	It enables or disables the device management feature.	**0**-Disabled **1**-Enabled	0
static.dm.server.address	It configures the server address of the YDMP/YMCS.	String within 512 characters	Blank
static.dm.server.port	It configures the server port of the YDMP/YMCS.	Integer from 0 to 65535	443
phone_setting.qoe.enable	It configures whether to report the call statistics to YDMP/YMCS.	**0**-Disabled **1**-Enabled	1
static.remote_control.X.allow[1]	It configures whether to allow the YDMP/YMCS to take phone's screenshots or capture packets.	**0**-Unauthorized, when the YDMP/YMCS wants to take phone's screenshots or capture packets, the phone will pop up a dialog, prompting users to allow or reject the request. When users allow the request, the value will change to Allowed, and the window will not pop up again. If users reject the request, the value will not change, and the window will pop up again when YDMP/YMCS makes a request next time. **1**-Allowed, you allow the YDMP/YMCS to take phone's screenshots or capture packets. **2**-Blocked, you reject the YDMP/YMCS to take phone's screenshots or capture packets.	0

Deploy Phone in Bulk via RPS

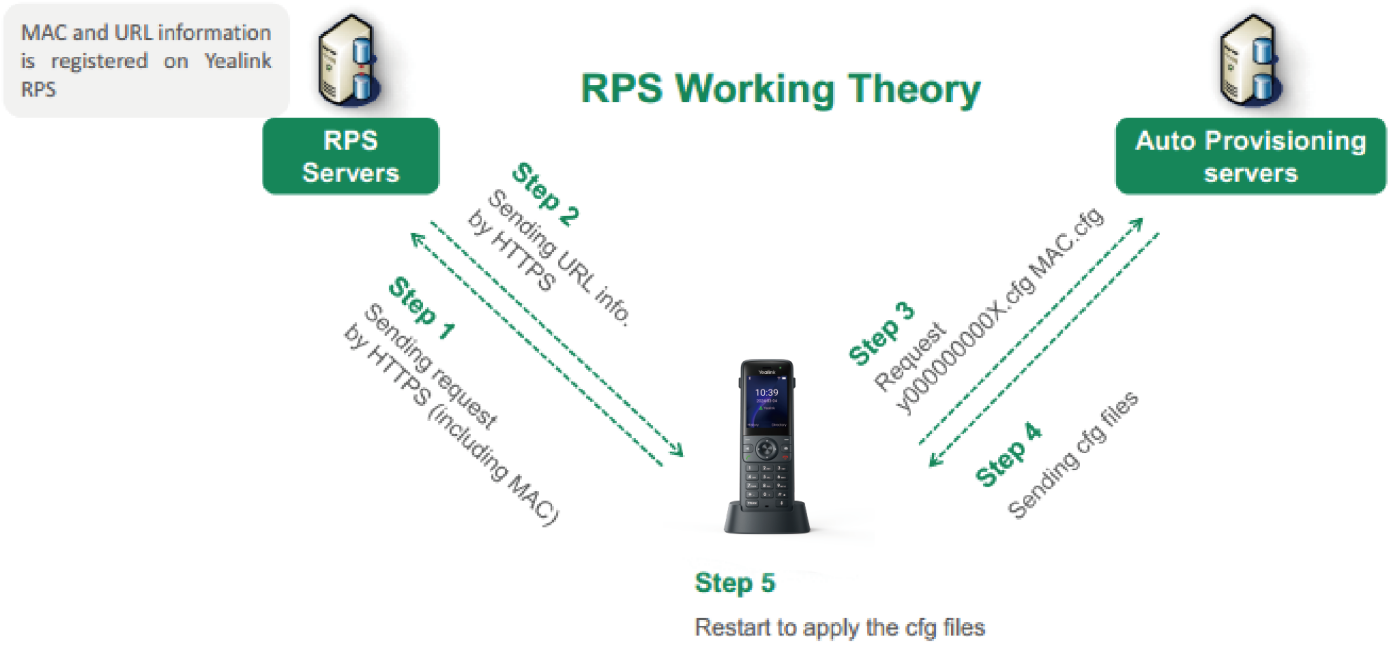
The administrator can enter the phone's MAC address and the URL of the provisioning server in the RPS server. During the initialization process after the phone is powered on/restored to factory settings, the phone will be redirected to the pre-set provisioning server to request Wi-Fi and account configuration updates.

Prerequisites

1. Set the Access Point to transmit Yealink AX83H preset SSID so that the phone can connect to the network automatically after reboot.
   *The default Hotspot SSID is **Axseies_deploy** , and the Hotspot Password is **AXseries@8!***
2. Place the configuration files on the deployment server according to different MAC addresses.
3. Redirect to the deployment server through RPS on YMCS.

> **TIP**
> For detailed information about RPS server Management, refer to RPS Management.

Procedure



1. When the phone is powered on for the first time or restored to factory settings, it will send a request to the RPS server.
2. The RPS server will push the URL of the deployment server to the phone.
3. The phone obtains the configuration file through the URL of the deployment server.
4. The deployment server pushes the configuration file to the phone.
5. The phone completes the deployment based on the downloaded configuration file

Phone Provisioning

Introduction

Phone Provisioning Introduction

You can provision multiple phones with the same settings for large-scale deployments.
For more information, refer to Yealink SIP IP Phones Auto Provisioning Guide .

Boot Files, Configuration Files, and Resource Files

Introduction

Introduction

You can use boot files, configuration files, and resource files to configure phone features and apply feature settings to phones. You can create or edit these files using a text editor such as Notepad++.
You can ask the distributor or Yealink FAE for template files. You can also obtain the template files online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage.

Boot Files

Introduction

Yealink phones support boot files. The boot files maximize the flexibility to allow you to customize features and settings for multiple phones.
With the boot file, you can specify which configuration files should be downloaded. It is effective for you to provision the phones in different deployment scenarios:

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

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

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

Common Boot File

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

MAC-Oriented Boot File

MAC-Oriented boot file, named `<MAC>.boot`. It will only be effective for a specific IP phone. In this way, you have high permission to control each phone by making changes on a per-phone basis.
You can create a MAC-Oriented boot file for each phone by making a copy and renaming the boot template file (y000000000000.boot). For example, if your phone MAC address is 00156574B150, rename the template file as 00156574b150.boot (lowercase).

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

Boot File Attributes

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

Attributes	Description
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
include:config <xxx.cfg> include:config "xxx.cfg"	Each "include" statement can specify a location of a configuration file. The configuration file format must be *.cfg. The locations in the angle brackets or double quotation marks support two forms: · Relative path (relative to the boot file): For example, sip.cfg, HTTP Directory/sip.cfg · Absolute path (or URL): For example, http://10.2.5.258/HTTP Directory/sip.cfg The location must point to a specific CFG file.
overwrite_mode	Enable or disable the overwrite mode. **1-(Enabled)** - If the value of a parameter in configuration files is left blank, or if a non-static parameter in configuration files is deleted or commented out, the factory default value takes effect. **0-(Disabled)** - If the value of a parameter in configuration files is left blank, deleted or commented out, the pre-configured value is kept. **ⓘ NOTE** Overwrite mode can only be used in boot files. If a boot file is used but `overwrite_mode` is not configured, the overwrite mode is enabled by default.

NOTE
The line beginning with “#” is considered to be a comment. You can use “#” to make any comment on 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.
   For example:
   include:config <configure/sip.cfg >
   include:config “http://10.2.5.206/configure/account.cfg”
   include:config “http://10.2.5.206/configure/dialplan.cfg”
4. Specify the overwrite mode.
   For example:
   `overwrite_mode = 1`
5. Save the boot file and place it on the provisioning server.

Configuration Files

Introduction

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

- Static: The parameters start with a prefix “static.”, for example, static.auto_provision.custom.protect.
- Non-static: The parameters do not start with a prefix “static.”, for example, local_time.date_format.

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

NOTE
For protecting against unauthorized access, you can encrypt configuration files. For more information on encrypting configuration files, refer to Encrypting and Decrypting Files .

Common CFG File

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

MAC-Oriented CFG File

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

MAC-local CFG File

MAC-local CFG file, which is named after the MAC address of the IP phone. For example, if the MAC address of an IP phone is 00156574B150, the name of the MAC-local CFG file is 00156574b150-local.cfg (lowercase). It contains changes associated with a non-static parameter that you make via the web user interface or handset user interface (for example, changes for time and date formats).
This file generates only if you enable the provisioning priority mechanism. It is stored locally on the IP phone and you can upload it to the provisioning server each time the file updates. This file enables the users to keep their personalized configuration settings, even though the IP phone performs auto provisioning.

NOTE
The non-static changes that you made before enabling the provisioning priority mechanism are not saved in the generated MAC-local file, but the previous settings still take effect on the phone. The static changes are never be saved to the `<MAC>-local.cfg` file.
The provisioning priority mechanism is enabled by the parameter `static.auto_provision.custom.protect`.

Configuration File Customization

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

Customize a Configuration File

1. Copy and rename a configuration template file. For example, sip.cfg.
2. Rearrange the parameters in the sip.cfg, and set the valid values for them.
   For example:
   `account.1.anonymous_call = 1`
3. Save the configuration file and place it on the provisioning server.

Configuration File Attributes

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

Attributes	Description
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
Configuration Parameter=Valid Value (for example, account. 1.dnd.enable = 1)	Specify the parameters and values to apply specific settings to the phones. · Separate each configuration parameter and value with an equal sign · Set only one configuration parameter per line · Put the configuration parameter and value on the same line and do not break the line

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

Resource Files

Introduction

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

NOTE
If you want to specify the desired phone 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 phones will request the resource files and configuration files.

Supported Resource 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 time zone and DST settings.	Time and Date

Language Packs	For example, 1.English.js	Customize the translation of the existing language On the web user interface.	Language
Replace Rule Template	DialPlan.xml	Customize replace rules for the dial plan.	Dial Plan
Dial Now Template	DialNow.xml	Customize dial now rules for the dial plan.	Dial Plan
Super Search Template	super_search.xml	Customize the search source list.	Dialing Display
Local Contact File	contact.xml	Add or modify multiple local contacts.	Local Directory
Remote Phone Book Template	Department.xml Menu.xml	Add or modify multiple remote contacts.	Remote Phone Book
User Access Level Template	webitemslevel.cfg	Customize the access permission for configurations on the web user interface and phone user interface.	User Access Level

Provisioning Methods

Introduction

Introduction

Yealink provides two ways to provision your phones:

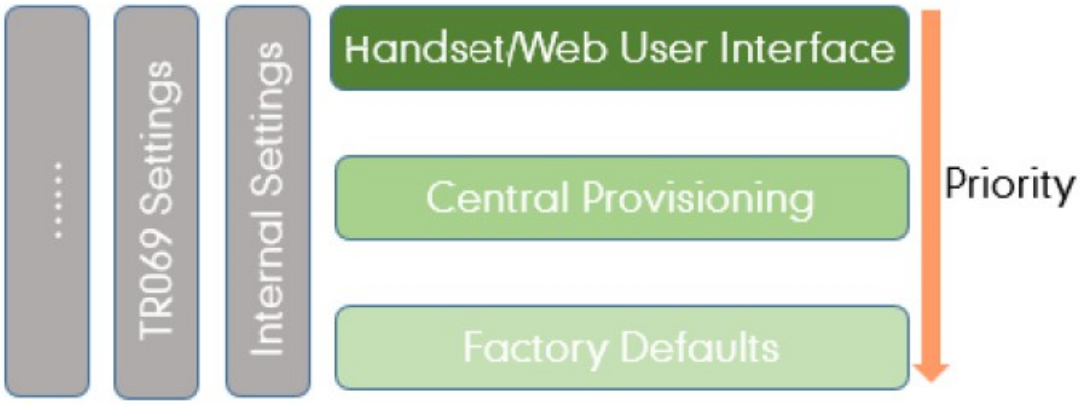
- **Manual Provisioning**: provisioning via the handset user interface or web user interface.
- **Central Provisioning**: provisioning through configuration files stored in a central provisioning server.

The method you use depends on how many phones need to be deployed and what features and settings to be configured. Manual provisioning on the web or handset user interface does not contain all of the phone settings available with the centralized method. You can use the web user interface method in conjunction with a central provisioning method and handset user interface method. We recommend using centralized provisioning as your primary provisioning method when provisioning multiple phones.

Provisioning Methods Priority

Introduction

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 Keep User's Personalized Settings after Auto Provisioning .
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).

Web User Interface

Introduction

You can configure the phones via the web user interface, a web-based interface that is especially useful for remote configuration.
Because features and configurations vary by phone models and firmware versions, options available on each page of the web user interface can vary as well. Note that the features configured via the web user interface are limited. Therefore, you can use the web user interface in conjunction with a central provisioning method and phone user interface.

NOTE
When you manually configure a phone via the web user interface or handset user interface, the changes associated with non-static parameters you make will be stored in the MAC-local CFG file. For more information on the MAC-local CFG file, refer to Configuration Files.

Quick Login Configuration

You can access the web user interface quickly using the request URI. It will locate you in the Status web page after accessing the web user interface. It is helpful to quickly log into the web user interface without entering the username and password on the login page.

ⓘ NOTE
Accessing the web user interface by request URI may be restricted by the web explorer (for example, Internet Explorer).
For security purposes, we recommend that you use this feature in a secure network environment.

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

```
wui.quick_login
wui.secure_domain_list
```

Parameter	Permitted Values	Default	Description
wui.quick_login	**0**-Disabled **1**-Enabled, you can quickly log into the web user interface using a request URI (for example, https://IP/api/auth/login?@admin:admin).	0	It enables or disables the quick login feature. **ⓘ NOTE** It works only if `static.wui.https_enable` is set to 1 (Enabled).

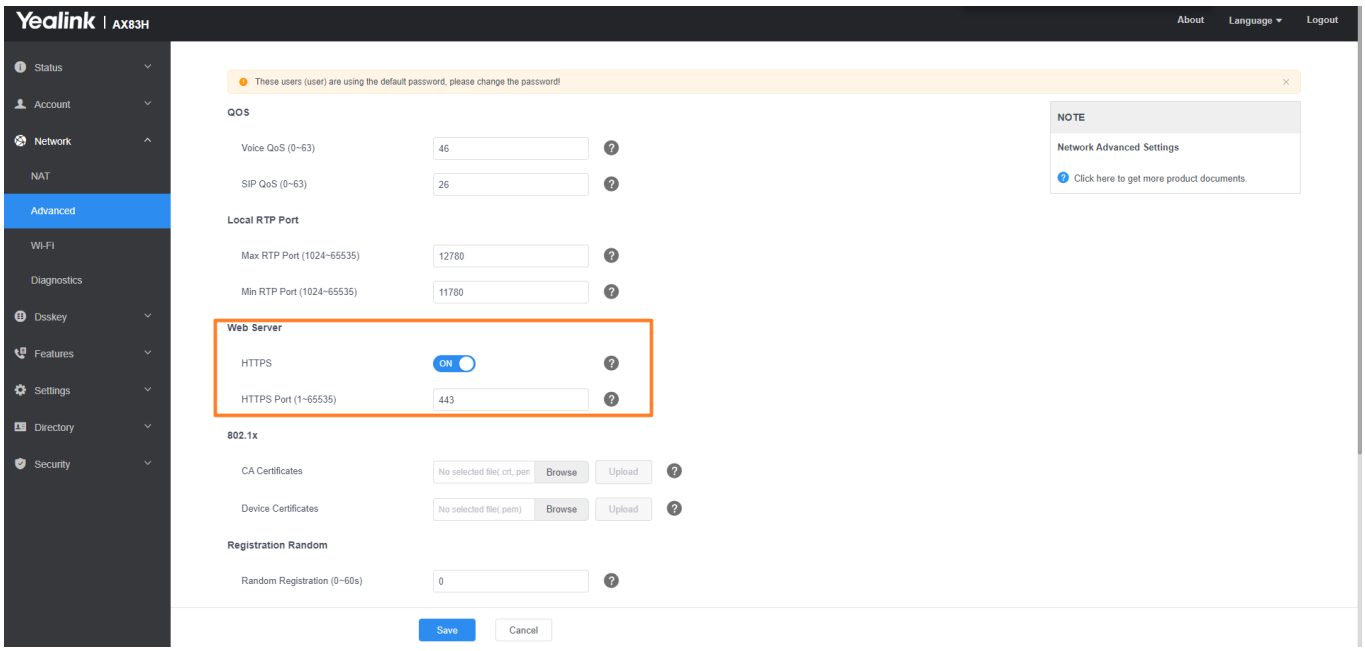
wui.secure_domain_list	String If it is left blank, you are only allowed to use the IP address to access the web user interface of the phone. If it is set to "**any**", you can use IP address or any domain name to access the web user interface of the phone.	any	It configures the valid domain name to access the web user interface of the phone. Multiple domain names are separated by semicolons. **Example:** `wui.secure_domain_list = test.abc.com` You are only allowed to use test.abc.com or IP address to access the web user interface of the phone. **NOTE** To use a domain name to access the web user interface of the phone, make sure your DNS server can resolve the domain name to the IP address of the phone.

Web Server Type Configuration

Yealink phones support HTTP and HTTPS protocols for accessing the web user interface. You can configure the web server type. The 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.

Set via the Web User Interface

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



Auto Provisioning

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

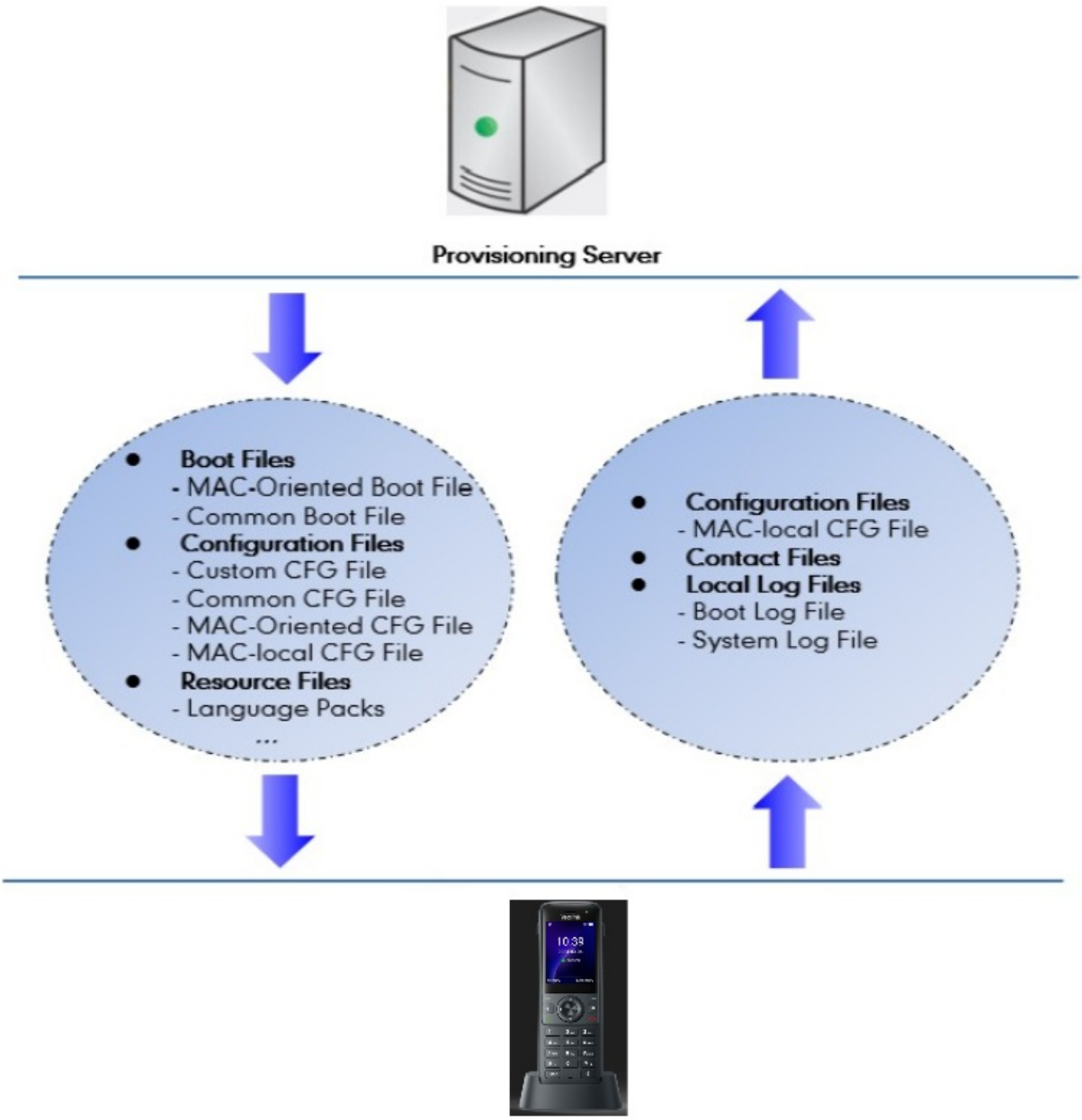
Parameter	Permitted Values	Default	Description
static.wui.https_enable[1]	**0**-Disabled **1**-Enabled	1	It enables or disables to access the web user interface of the phone over a secure tunnel (HTTPS).
static.network.port.https[1]	Integer from 1 to 65535	443	It configures the port used to access the 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.

Central Provisioning

Introduction

Central provisioning enables you to provision multiple phones from a provisioning server that you set up, and maintain a set of boot files, configuration files and resource files for all phones in the central provisioning server. The following figure shows how the phone interoperates with provisioning server when you use the centralized provisioning method:



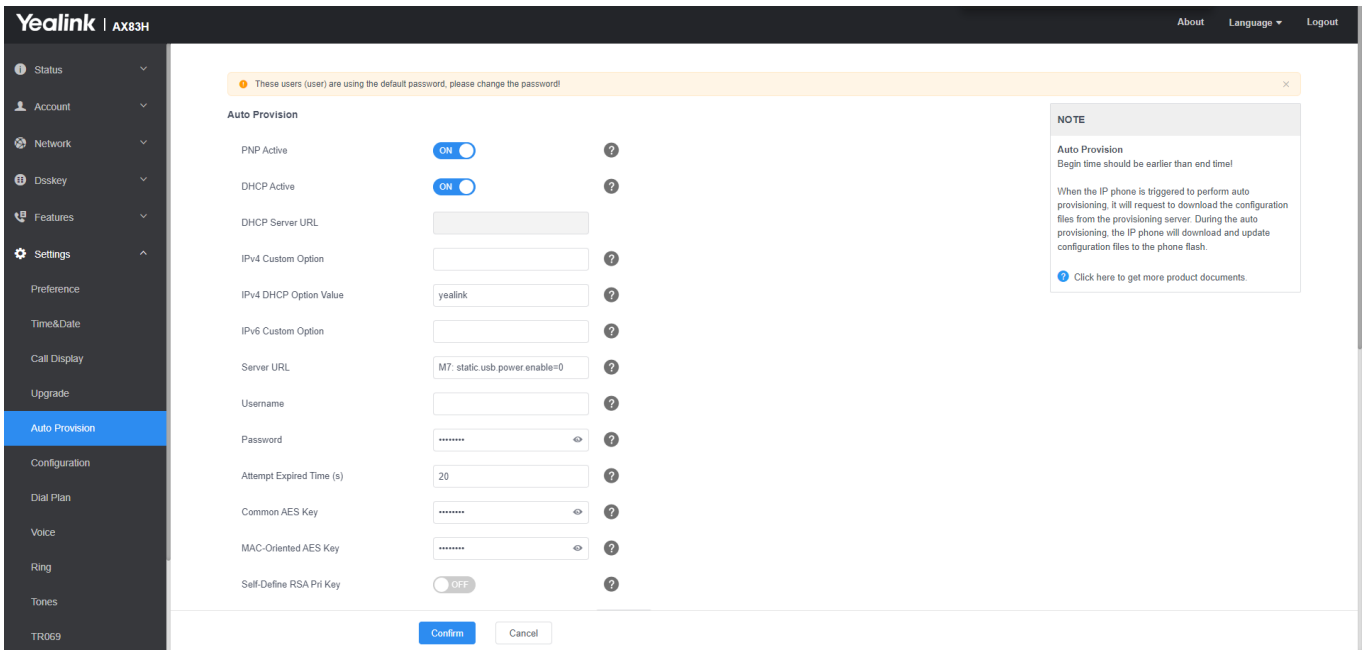
Yealink phones can obtain the provisioning server address during startup. Then the phones first download boot files and configuration files from the provisioning server and then resolve and update the configurations written in configuration files. This entire process is called auto provisioning. For more information on auto provisioning, refer to Auto Provisioning Guide.

The phones can be configured to upload log files (log files provide a history of phone events), call log files, and contact files to the provisioning server. You can also configure a directory for each of these three files respectively.

Auto Provisioning Settings Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Auto Provision**.



Auto Provisioning

static.auto_provision.attempt_expired_time
static.network.attempt_expired_time
static.auto_provision.attempt_before_failed
static.auto_provision.retry_delay_after_file_transfer_failed
static.auto_provision.reboot_force.enable
static.auto_provision.power_on
static.auto_provision.repeat.enable
static.auto_provision.repeat.minutes
static.auto_provision.weekly.enable
static.auto_provision.weekly_upgrade_interval
static.auto_provision.inactivity_time_expire
static.auto_provision.weekly.dayofweek
static.auto_provision.weekly.begin_time
static.auto_provision.weekly.end_time
static.auto_provision.flexible.enable
static.auto_provision.flexible.interval
static.auto_provision.flexible.begin_time
static.auto_provision.flexible.end_time
static.auto_provision.dns_resolv_nretry
static.auto_provision.dns_resolv_timeout

Parameter	Permitted Values	Default	Description

static.auto_provision.attempt_expired_time	Integer from 1 to 300	20	It configures the timeout (in seconds) to transfer a file via auto provisioning. **NOTE** It has a higher priority than the value defined by the parameter static.network.attempt_expired_time.
static.network.attempt_expired_time[1]	Integer from 1 to 20	10	It configures the timeout (in seconds) to transfer a file for HTTP/HTTPS connection. **NOTE** It has a lower priority than the value defined by the parameter static.auto_provision.attempt_expired_time.
static.auto_provision.attempt_before_failed	Integer from 1 to 10	3	It configures the maximum number of attempts to transfer a file before the transfer fails during auto provisioning.
static.auto_provision.retry_delay_after_file_transfer_failed	Integer from 0 to 300	5	It configures the time (in seconds) to wait after a file transfer fails before retrying the transfer via auto provisioning.

static.auto_provision.reboot_force.enable[1]	**0**-Disabled **1**-Enabled	Blank	It enables or disables the phone to reboot after auto provisioning, even if there is no specific configuration requiring a reboot. **NOTE** It works only for the current auto provisioning process. If you want the phone to reboot after every auto provisioning process, the parameter must be always contained in the configuration file and set to 1. If the phone reboots repeatedly after it is set to 1, you can try to set `static.auto_provision.power_on` to 0 (Off).
static.auto_provision.power_on	**0**-Off **1**-On, the phone performs auto provisioning when powered on.	1	It triggers the power-on feature to on or off.
static.auto_provision.repeat.enable	**0**-Off **1**-On	0	It triggers the repeatedly feature to on or off.
static.auto_provision.repeat.minutes	Integer from 1 to 43200	1440	It configures the interval (in minutes) for the phone to perform auto provisioning repeatedly. **NOTE** It works only if `static.auto_provision.repeat.enable` is set to 1 (On).
static.auto_provision.weekly.enable	**0**-Off **1**-On, the phone performs an auto provisioning process weekly.	0	It triggers the weekly feature to on or off.

static.auto_provision.weekly_upgrade_interval	Integer from 0 to 12	0	It configures the time interval (in weeks) for the phone to perform auto provisioning. If it is set to 0, the phone performs auto provisioning at the specific day(s) configured by the parameter `static.auto_provision.weekly.dayofweek` every week. If it is set to other values (for example, 3), the phone performs auto provisioning at a random day between the specific day(s) configured by the parameter `static.auto_provision.weekly.dayofweek` every three weeks. **NOTE** It works only if `static.auto_provision.weekly.enable` is set to 1 (On).
			It configures the delay time (in minutes) to perform auto provisioning when the phone is inactive at regular week. If it is set to 0, the phone performs auto provisioning at random between a starting time configured by the parameter `static.auto_provision.weekly.begin_time` and an ending time configured by the parameter `static.auto_provision.weekly.end_time`. If it is set to other values (for example, 60), the phone performs auto provisioning only when it has been inactivated for 60 minutes (1 hour) between the starting

			time and ending time. **NOTE** The phone may perform auto provisioning when you are using the phone during office hour. It works only if `static.auto_provision.weekly.enable` is set to 1 (On). The operations on the handset will not change the inactive status; only the functional operations related base station, such as calling, will change the inactive status.
static.auto_provision.inactivity_time_expire	Integer from 0 to 120	0	

static.auto_provision.weekly.dayofweek	0,1,2,3,4,5,6 or a combination of these digits **0**-Sunday **1**-Monday **2**-Tuesday **3**-Wednesday **4**-Thursday **5**-Friday **6**-Saturday	0123456	It configures the days of the week for the phone to perform auto provisioning weekly. Example: `static.auto_provision.weekly.dayofweek = 01` If `static.auto_provision.weekly_upgrade_interval` is set to 0, it means the phone performs auto provisioning every Sunday and Monday. If `static.auto_provision.weekly_upgrade_interval` is set to other value (for example, 3), it means the phone performs auto provisioning by randomly selecting a day from Sunday and Monday every three weeks. **NOTE** It works only if `static.auto_provision.weekly.enable` is set to 1 (On).
static.auto_provision.weekly.begin_time static.auto_provision.weekly.end_time	Time from 00:00 to 23:59	00:00	It configures the starting/ending time of the day for the phone to perform auto provisioning weekly. **NOTE** It works only if `static.auto_provision.weekly.enable` is set to 1 (On).

static.auto_provision.flexible.enable	**0**-Off **1**-On, the phone performs auto provisioning at random between a starting time configured by the parameter `static.auto_provision.flexible.begin_time` and an ending time configured by the parameter `static.auto_provision.flexible.end_time` on a random day within the period configured by the parameter `static.auto_provision.flexible.interval`.	0	It triggers the flexible feature to on or off. **NOTE** The day within the period is based upon the phone's MAC address and does not change with a reboot, whereas the time within the start and end is calculated again with every reboot. The timer starts again after each auto provisioning.
static.auto_provision.flexible.interval	Integer from 1 to 1000	30	It configures the interval (in days) for the phone to perform auto provisioning. The auto provisioning occurs on a random day within this period based on the phone's MAC address. The phone performs auto provisioning on a random day (for example, 18) based on the phone's MAC address. **NOTE** It works only if `static.auto_provision.flexible.enable` is set to 1 (On).
static.auto_provision.flexible.begin_time	Time from 00:00 to 23:59	02:00	It configures the starting time of the day for the phone to perform auto provisioning at random. **NOTE** It works only if `static.auto_provision.flexible.enable` is set to 1 (On).

static.auto_provision.flexible.end_time	Time from 00:00 to 23:59	Blank	It configures the ending time of the day for the phone to perform auto provisioning at random. If it is left blank or set to a specific value equal to starting time configured by the parameter `static.auto_provision.weekly.begin_time`, the phone performs auto provisioning at the starting time. If it is set to a specific value greater than starting time configured by the parameter `static.auto_provision.weekly.begin_time`, the phone performs auto provisioning at random between the starting time and ending time. If it is set to a specific value less than starting time configured by the parameter `static.auto_provision.weekly.begin_time`, the phone performs auto provisioning at random between the starting time on that day and ending time in the next day. **NOTE** It works only if `static.auto_provision.flexible.enable` is set to 1 (On).

static.auto_provision.dns_resolv_nretry	Integer from 1 to 10	2	It configures the retry times when the phone fails to resolve the access URL of the provisioning server. **NOTE** For each different DNS server, it works only if `static.auto_provision.dns_resolv_nosys` is set to 1 (Enabled).
static.auto_provision.dns_resolv_timeout	Integer from 1 to 60	5	It configures the timeout (in seconds) for the phone to retry to resolve the access URL of the provisioning server. **NOTE** For each different DNS server, it works only if `static.auto_provision.dns_resolv_nosys` is set to 1 (Enabled).

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

FAQ

1. Let phone automatically reboot after auto provisioning

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)

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

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

Provisioning Protocols Configuration

```
static.auto_provision.server.type
static.auto_provision.user_agent_mac.enable
```

Parameter	Permitted Values	Default	Description
static.auto_provision.server.type	**1**-http **2**-https **3**-ftp **Other values**-tftp	tftp	It configures the protocol the phone uses to connect to the provisioning server. **ⓘ NOTE** It works only if the protocol type is not defined in the access URL of the provisioning server configured by the parameter `static.auto_provision.server.url`.
static.auto_provision.user_agent_mac.enable[1]	**0**-Disabled **1**-Enabled	1	It enables or disables the phone's MAC address to be included in the User-Agent header of HTTP/HTTPS request via auto provisioning.

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

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:

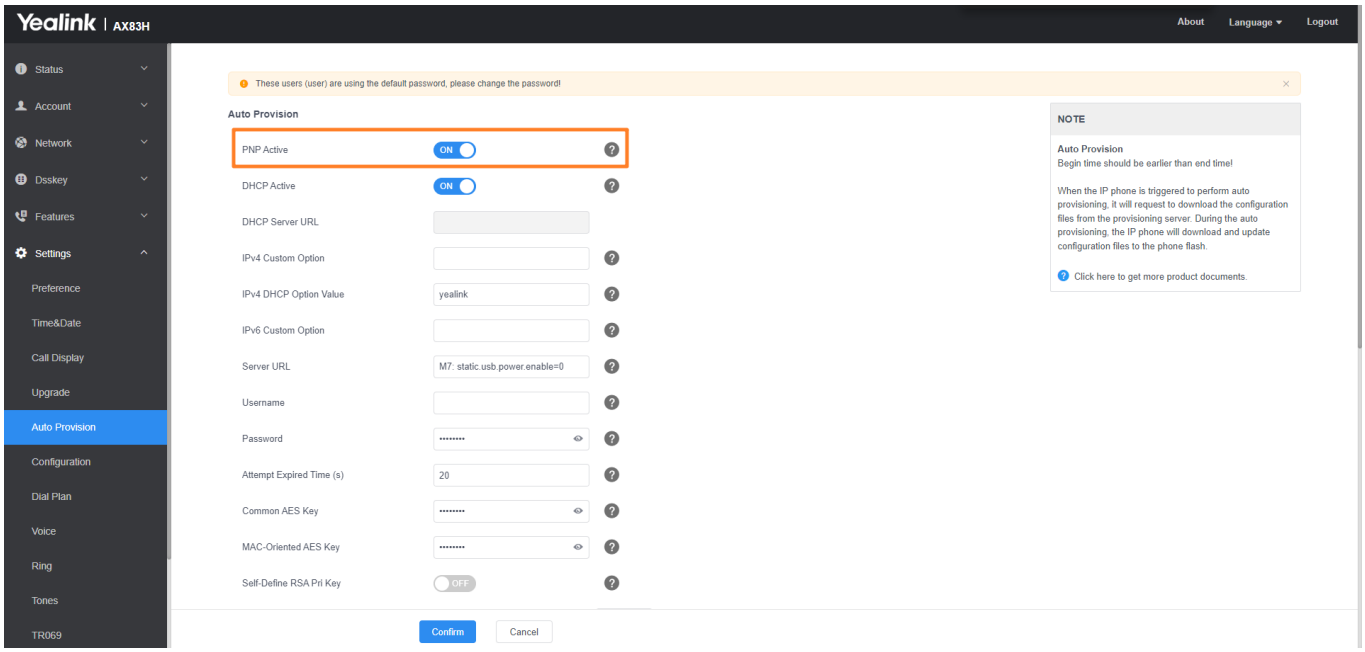
- **PnP**: PnP feature allows the phones to discover the provisioning server address by broadcasting the PnP SUBSCRIBE message during startup.
- **DHCP**: DHCP option can be used to provide the address or URL of the provisioning server to phones. When the IP phone requests an IP address using the DHCP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

PnP Provision Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Auto Provision** > **PNP Active**.



Auto Provisioning

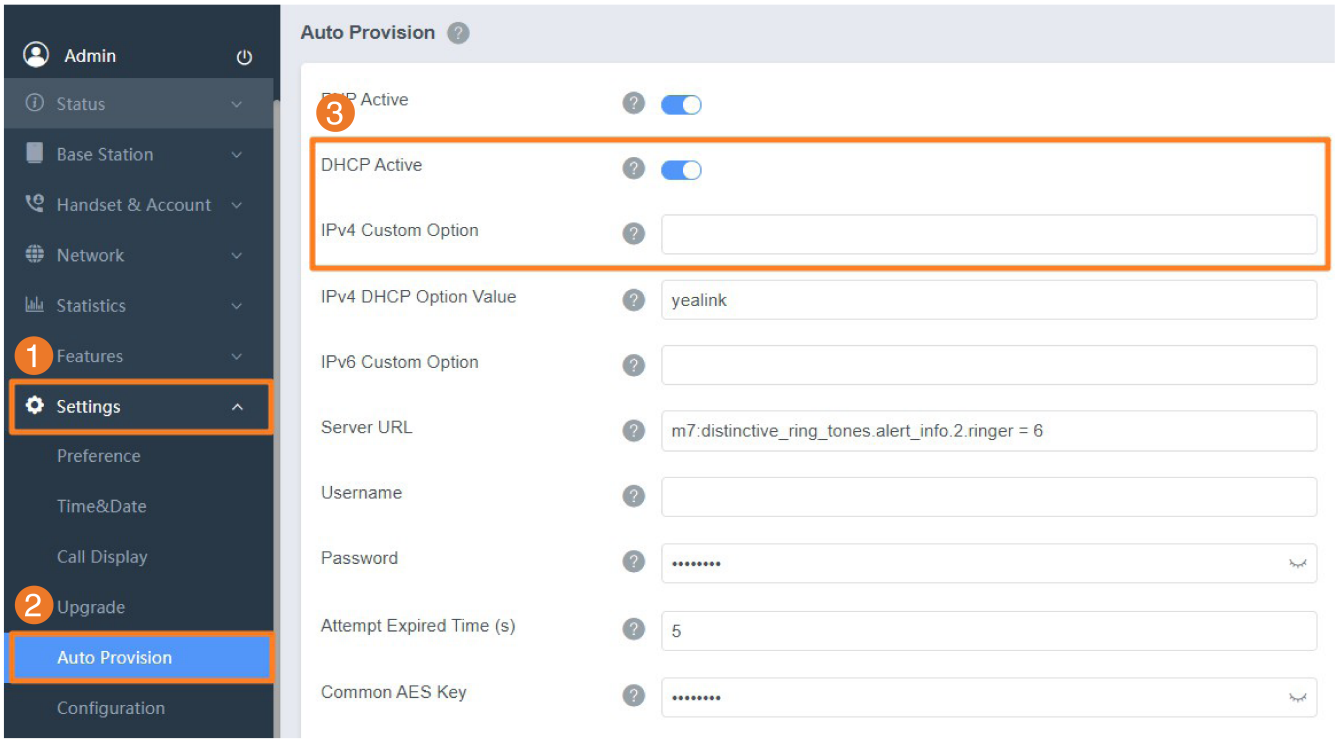
```
static.auto_provision.pnp_enable
```

Parameter	Permitted Values	Default	Description
static.auto_provision.pnp_enable	**0**-Off **1**-On, the phone broadcasts SIP SUBSCRIBE messages to obtain a provisioning server URL where the phone can request the configuration from during startup.	1	It triggers the Plug and Play (PnP) feature to turn on or off.

DHCP Provision Configuration

Set via the Web User Interface

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



Auto Provisioning

```
static.auto_provision.dhcp_option.enable
static.auto_provision.dhcp_option.list_user_options
static.auto_provision.url_wildcard.pn
```

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

static.auto_provision.url_wildcard.pn	String within 32 characters	Blank	It configures the characters to replace the wildcard $PN in the received URL of the provisioning server. **NOTE** The configured characters must be in accordance with the actual directory name of the provisioning server.

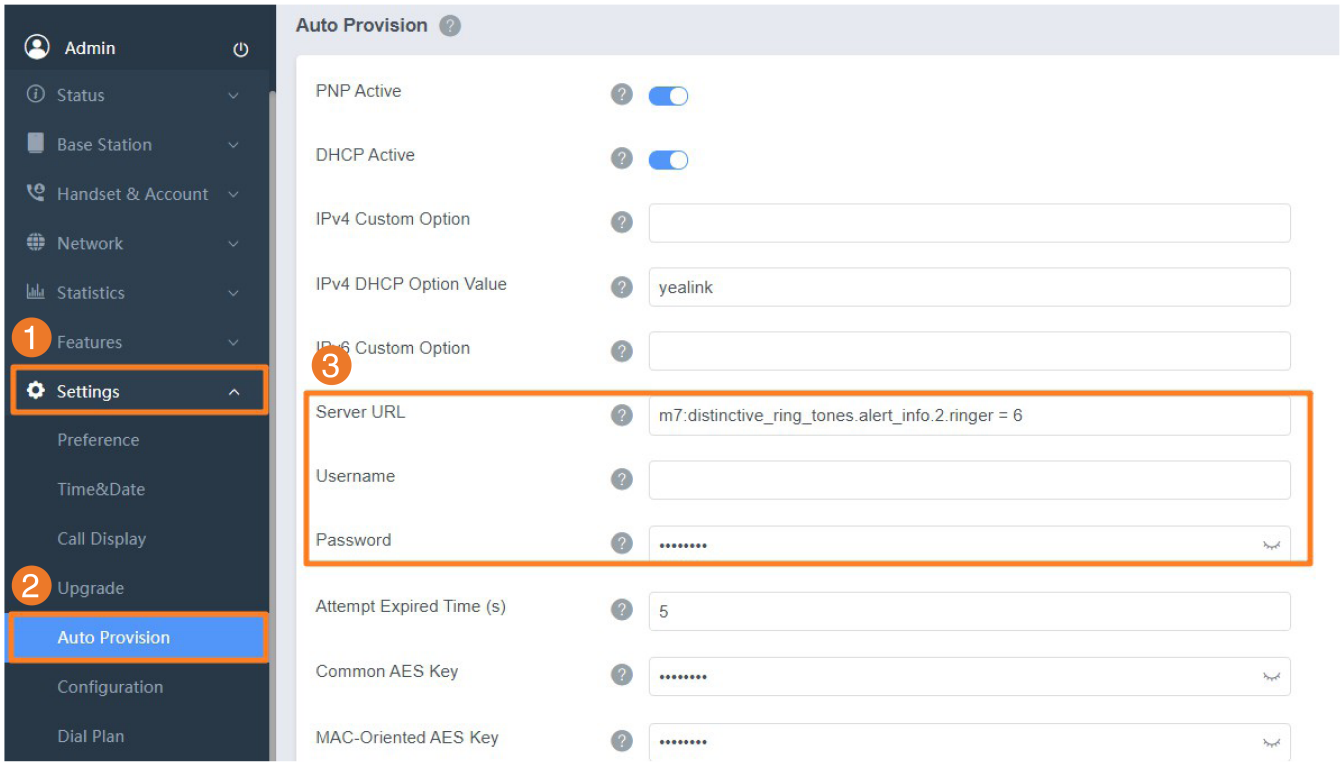
Static Provision Configuration

To use the static provision method, you need to obtain the provisioning server address first when configuring a provisioning server.
The provisioning server address can be an IP address, domain name or URL. If a username and password are specified as part of the provisioning server address, for example, http://user:pwd@server/dir, they will be used only if the server supports them.

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

Set via the Web User Interface

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



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.

To set up the provisioning server:

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.

ⓘ NOTE
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.

Keep User’ s Personalized Settings after Auto Provisioning

Introduction

Generally, you deploy phones in batch and timely maintain company phones via auto provisioning, yet some users would like to keep the personalized settings after auto provisioning.

Keep User’ s Personalized Settings Configuration

The following table lists the parameters you can use to keep the user's personalized settings.

```
static.auto_provision.custom.protect
static.auto_provision.custom.sync
static.auto_provision.custom.sync.path
static.auto_provision.custom.upload_method
static.auto_provision.handset_configured.enable
static.auto_provision.custom.handset.protect
```

Parameter	Permitted Values	Default	Description

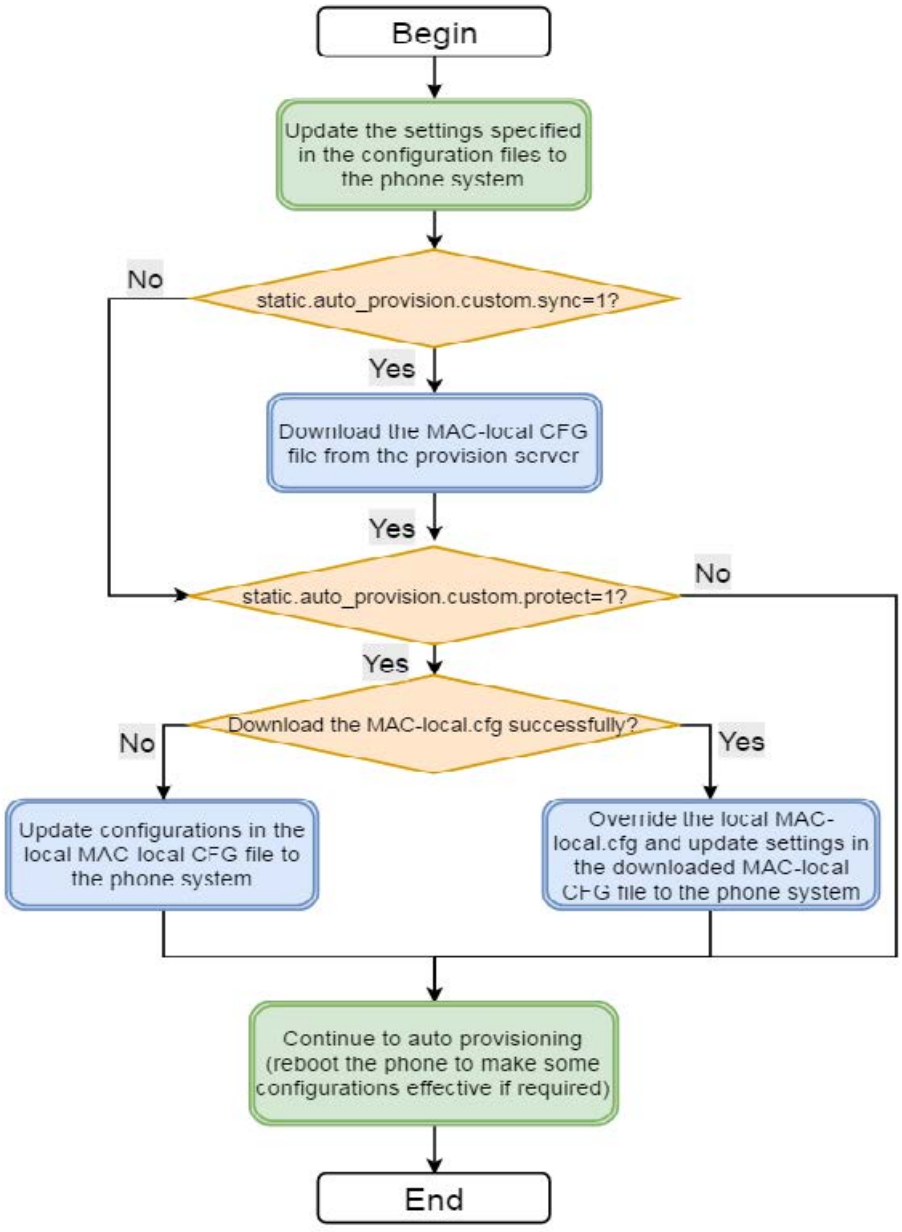
static.auto_provision.custom.protect	**0**-Disabled **1**-Enabled, `<MAC>-local.cfg` file generates and personalized non-static settings configured via the web or handset user interface will be kept after auto provisioning.	0	It enables or disables the phone to keep the user’ s personalized settings after auto provisioning. **NOTE** The provisioning priority mechanism (**handset/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). It is not applicable to the custom handset related configurations.

static.auto_provision.custom.sync	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to upload the <MAC>-local.cfg file to the server each time the file updates, and to download the <MAC>-local.cfg file from the server during auto provisioning. **NOTE** It works only if static.auto_provision.custom.protect is set to 1 (Enabled). The upload/download path is configured by the parameter static.auto_provision.custom.sync.path.
static.auto_provision.custom.sync.path	URL	Blank	It configures the URL for uploading/downloading the <MAC>-local.cfg file. If it is left blank, the phone will try to upload/download the <MAC>-local.cfg file to/from the provisioning server. **NOTE** It works only if static.auto_provision.custom.sync is set to 1 (Enabled).
static.auto_provision.custom.upload_method	**0**-PUT **1**-POST	0	It configures the way the phone uploads the <MAC>-local.cfg file, <MAC>-calllog.xml file or <MAC>-contact.xml file to the provisioning server (for HTTP/HTTPS server only).

static.auto_provision.handset_configured.enable	**0**-Disabled, the custom handset settings can be only changed via the handset user interface. **1**-Enabled, when the parameter `static.auto_provision.custom.handset.protect` is set to 0 (Disabled), the personalized handset settings will be overridden; if the parameter `static.auto_provision.custom.handset.protect` is set to 1 (Enabled), the personalized handset settings will not be overridden.	1	It enables or disables the base station to deliver custom handset configurations to the handset via auto provisioning/handset reboot/handset registration. **NOTE** It is only applicable to the custom handset related configurations.
static.auto_provision.custom.handset.protect	**0**-Disabled **1**-Enabled	1	It enables or disables the handsets to keep user personalized settings after auto provisioning/handset reboot/handset registration. **NOTE** It works only if `static.auto_provision.handset_configured.enable` is set to 0 (Disabled). It is only applicable to the custom handset related configurations.

Auto Provisioning Flowchart for Keep User’s Personalized Configuration Settings

The following shows an auto provisioning flowchart for Yealink phones when a user wishes to keep the user’s personalized configuration settings.



Example: Keep User’ s Personalized Settings

This section shows you how to keep the personalized settings.

Parameters Settings:

`static.auto_provision.custom.protect =1`

After provisioning, if the users make changes via the phone or web user interface, the MAC-local.cfg file with non-static personal settings generates locally.

Scenario: Keep user’ s personalized settings when upgrading the firmware

If you set `static.auto_provision.custom.sync =1`, then the phones attempt to upload the `MAC-local.cfg` file to the provisioning server each time the file updates. When performing auto provisioning, they download their own `MAC-local. cfg` file from the provisioning server, then update MAC-local.cfg file settings to the IP phone system. The

personalized settings locally are overridden by the MAC-local.cfg file from the provisioning server.
If you set static.auto_provision.custom.sync =0, the MAC-local.cfg file will be kept locally. The personalized settings will not be overridden after auto-provisioning.

Scenario: Keep personalized user settings after factory reset

The IP phone requires a factory reset when it has a breakdown, but the user wishes to keep customized settings of the phone after a factory reset. Before factory reset, make sure that you have set static.auto_provision. custom.sync =1, and the MAC-local.cfg file has been kept on the provisioning server.
After resetting all configurations to factory defaults, both the parameters settings static.auto_provision. custom.protect and static.auto_provision.custom.sync are reset to 0. Although the MAC-local.cfg files are cleared locally, they are still kept on the provisioning server.
You can set static.auto_provision.custom.protect =1 and static.auto_provision.custom.sync =1, and then trigger the phone to perform auto-provisioning. The phones download their own MAC-local.cfg file from the provisioning server, then update settings in MAC-local.cfg file to the IP phone system.
As a result, the personalized configuration settings of the phone are retrieved after the factory reset.

Clear User's Personalized Configuration Settings

When the IP phone is given to a new user but many personalized configurations settings of the last user are saved on the phone, or when the end-user encounters some problems because of the wrong configurations, you can clear the user’ s personalized configuration settings via the web user interface at the path: **Settings** > **Upgrade** > **Reset Local Settings**.

NOTE
The Reset local settings option on the web user interface appears only if you set static.auto_provision.custom.protect = 1.
If you set static.auto_provision.custom.sync = 1, the MAC-local.cfg file on the provisioning server will be cleared too. If not, the MAC-local.cfg file is kept on the provisioning server, and the phone could download it and update the configurations to the phone after the following auto-provisioning.

Custom Handset Related Configurations

If you have a CCPhone this section shows you the custom handset-related configurations.

Configuration parameter

custom.handset.date_format
custom.handset.time_format
custom.handset.auto_answer.enable
custom.handset.low_battery_tone.enable
custom.handset.confirmation_tone.enable
custom.handset.keypad_tone.enable
custom.handset.keypad_light.enable
custom.handset.backlight_in_charger.enable
custom.handset.backlight_out_of_charger.enable
custom.handset.screen_saver.enable
custom.handset.language

Parameter	Permitted Values	Default	Description
custom.handset.time_format	**0**-Hour 12, the time will be displayed in 12-hour format with AM or PM specified. **1**-Hour 24, the time will be displayed in 24-hour format (for example, 2:00 PM displays as 14:00).	1	It configures the time format for all registered handsets. **NOTE** It works only if `static.auto_provision.handset_configured.enable` is set to 1 (Enabled).
custom.handset.date_format	**0**-WWW MMM DD **1**-DD-MMM-YY **2**-YYYY-MM-DD **3**-DD/MM/YYYY **4**-MM/DD/YY **5**-DD MMM YYYY **6**-WWW DD MMM Use the following mapping: "WWW" represents the abbreviation of the week; "DD" represents a two-digit day; "MMM" represents the first three letters of the month; "YYYY" represents a four-digit year, and "YY" represents a two-digit year.	0	It configures the date format for all registered handsets. **NOTE** The value configured by the parameter `lcl.datetime.date.format` takes precedence over that configured by this parameter.

custom.handset.auto_answer.enable	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled **1**-Enabled	-1	It enables or disables a user to answer incoming calls by lifting the handset from the charger cradle without having to press the off-hook key. **NOTE** It works if the handset is placed in the charger cradle and the parameter `static.auto_provision.handset_configured.enable` is set to 1 (Enabled).
custom.handset.keypad_tone.enable	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled **1**-Enabled	-1	It enables or disables the handset to play a tone when any key is pressed. For CP930W, it plays a tone only when the touch keypad is tapped. **NOTE** It will take effect on all handsets that are registered on the same base station. It works only if `static.auto_provision.handset_configured.enable` is set to 1 (Enabled) and the silent mode is off.

custom.handset.confirmation_tone.enable	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled **1**-Enabled	-1	It enables or disables the handset to play a tone when a user saves settings or places the handset in the charger cradle. **NOTE** It will take effect on all handsets that are registered on the same base station. It works only if `static.auto_provision.handset_configured.enable` is set to 1 (Enabled) and the silent mode is off.
custom.handset.low_battery_tone.enable	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled **1**-Enabled	-1	It enables or disables the handset to play a tone when battery capacity is low. **NOTE** It will take effect on all handsets that are registered on the same base station. It works only if `static.auto_provision.handset_configured.enable` is set to 1 (Enabled) and the silent mode is off.

custom.handset.keypad_light.enable	**-1**-Do not modify the configuration. **0**-Disabled **1**-Enabled	-1	It enables or disables the handset to turn on the keypad light (digital key, # key, * key, TRAN key, and Mute key) when any key is pressed. **NOTE** It will take effect on all handsets that are registered to the same base station. It works only if `static.auto_provision.handset_configured.enable` is set to 1 (Enabled).
custom.handset.backlight_in_charger.enable[1]	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled, the backlight will be turned off after the handset is idle for about 10 seconds. **1**-Enabled, the backlight will be turned off after the handset is idle for about 30 minutes	-1	It enables or disables the handset backlight to be on for about 30 minutes when it is charged. **NOTE** It will take effect on all handsets that are registered on the same base station. It works only if `static.auto_provision.handset_configured.enable` is set to 1 (Enabled).

custom.handset.backlight_out_of_charger.enable[1]	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled, the backlight will be turned off after the handset is idle for about 10 seconds. **1**-Enabled, the backlight will be turned off after the handset is idle for about 30 minutes.	-1	It enables or disables the handset backlight to be on for about 30 minutes when it is not charged. **NOTE** It will take effect on all handsets that are registered on the same base station. It works only if `static.auto_provision.handset_configured.enable` is set to 1 (Enabled).
custom.handset.screen_saver.enable[1]	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled **1**-Enabled, an analog clock will be activated and appear on the LCD screen if no user activity is sensed for approximately 10 seconds.	-1	It enables or disables screen saver feature. **NOTE** It will take effect on all handsets that are registered on the same base station. It works only if `static.auto_provision.handset_configured.enable` is set to 1 (Enabled).

custom.handset.language	**0**-English **1**-French **2**-German **3**-Italian **4**-Polish **5**-Portuguese **6**-Spanish **7**-Turkish **8**- Russian **9**-Czech (only for CP935W) **10**-Swedish **11**-Slovak (only for CP935W)	0	It configures the language used on the handset user interface. **NOTE** It will take effect on all handsets that are registered on the same system. It works only if `static.auto_provision.handset_configured.enable` is set to 1 (Enabled).

[1] This parameter is only applicable to W53H/W56H/W57R/W59R/W73H/W78H.

Auto Provisioning Guide

Introduction

Yealink phones are full-featured telephones that can be plugged directly into an IP network and can be used easily without manual configuration.
This guide provides instructions on how to provision Yealink phones with the minimum settings required. Yealink IP phones support FTP, TFTP, HTTP, and HTTPS protocols for auto provisioning and are configured by default to use the TFTP protocol.

Get Started

This section provides instructions on how to get ready for auto provisioning. To begin the auto provisioning, the following steps are required:

Obtain Boot, Configuration and Resource Files

Boot Files

The IP phone tries to download the boot file first, and then download the configuration files referenced in the boot file during auto provisioning. You can select whether to use the boot file or not according to your deployment

scenario. If required, you need to obtain the template boot file named as "y000000000000.boot" before auto provisioning.
You can use a boot file to specify which configuration files to be downloaded for specific phone groups by phone model identity, and customize the download sequence of configuration files. It is efficient for you to provision IP phones in different deployment scenarios, including all IP phones, specific phone groups, or a single phone.
The configuration files referenced in the boot file are flexible: you can rearrange the configuration parameters within the Yealink-supplied template configuration files or create your own configuration files from the configuration parameters you want. You can create and name as many configuration files as you want and your own configuration files can contain any combination of configuration parameters.

Configuration Files

Before provisioning, you also need to obtain template configuration files. There are two configuration files both of which are CFG formatted. We call these two files Common CFG file and MAC-Oriented CFG file.
The configuration files contain parameters that affect the features of the phone. You can use the configuration files to deploy and maintain a mass of Yealink IP phones automatically.
You can create and name as many configuration files as you want (for example, account.cfg, sip.cfg, features.cfg) by using the template configuration files. The custom configuration files can contain the configuration parameters of the same feature modules for all phones.

Resource Files

When configuring some particular features, you may need to upload resource files to IP phones, such as personalized AutoDST file, language package file, and local contact file. Resource files are optional, but if the particular feature is being employed, these files are required.
Yealink supplies the following resource file templates:

Feature	Template File Name
DST	AutoDST.xml
Language Packs	For example, 000.GUI.English.lang 1.English_note.xml 1.English.js
Replace Rule	dialplan.xml
Dial-now	dialnow.xml
Softkey Layout	CallFailed.xml CallIn.xml Connecting.xml Dialing.xml RingBack.xml Talking.xml
Directory	favorite_setting.xml

Super Search in dialing	super_search.xml
Local Contact File	contact.xml
Remote XML Phone Book	Department.xml Menu.xml
Screen Saver	CustomScreenSaver.xml
Firmware	X.83.0.XX.rom For example, 44.83.0.10.rom

Obtain Template Files

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

To download template boot, configuration and resource files:

1. Go to Boot Files page and select the desired phone model.
2. Download and extract the combined template files to your local system.
3. Open the folder you extracted and identify the files you want to edit.

Obtain Phone Information

Before provisioning, you also need the phone information. For example, MAC address and the SIP account information of the phone.

MAC Address: The unique 12-digit serial number of the phone. You can obtain it from the bar code on the back of the IP phone.

SIP Account Information: This may include SIP credentials such as user name, password, and IP address of the SIP server. Ask your system administrator for SIP account information.

Provision Yealink Phones

This section provides instructions on how phones interoperate with the provisioning server for auto provisioning, and shows you the auto provisioning process and the four major tasks to provision the phones. It will help users who are not familiar with auto provisioning to understand this process more easily and quickly.

Interoperate with Provisioning Server

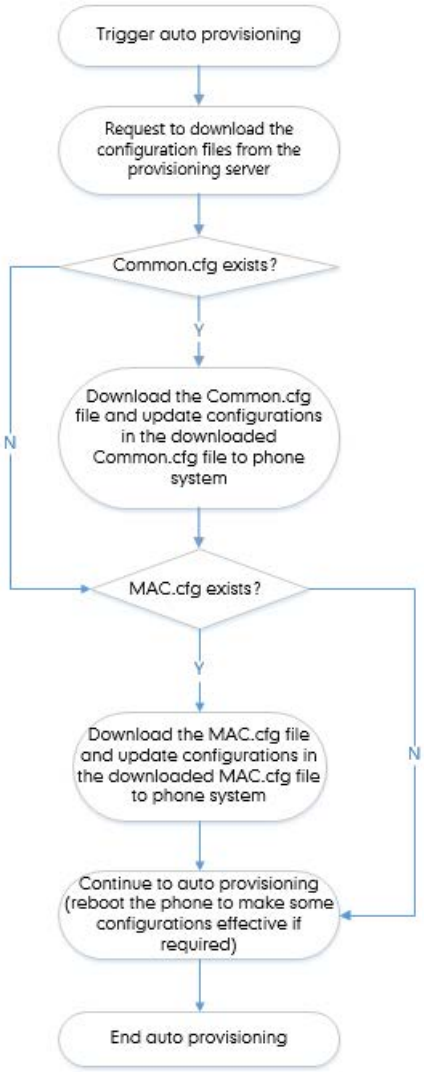
When phones are triggered to perform auto provisioning, they will request to download the boot files and configuration files from the provisioning server. During the auto provisioning, the phone will download and update configuration files to the phone flash.

The following figure shows how the phone interoperates with the provisioning server:

Auto Provisioning Process

Old Mechanism – Without Boot Files

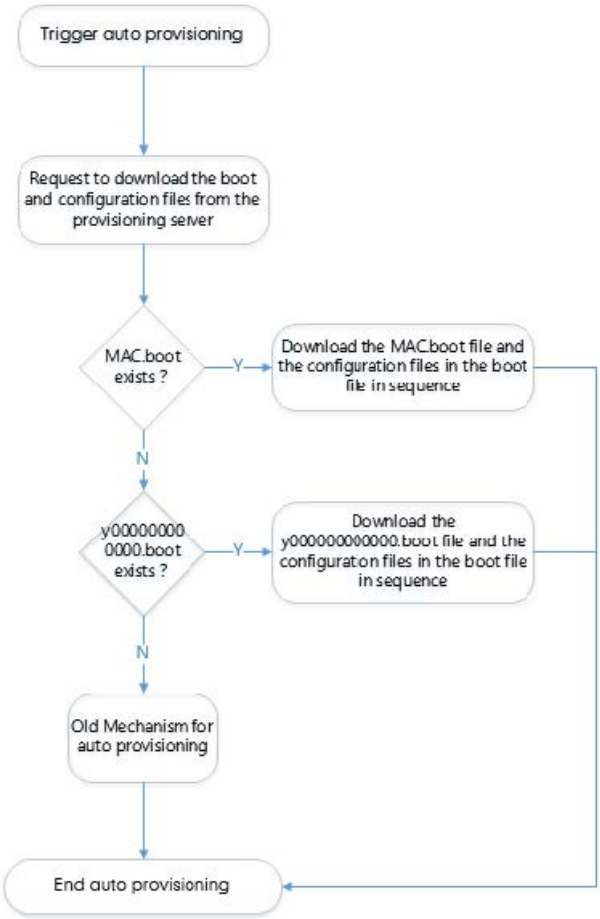
The following flowchart shows how Yealink phones perform auto provisioning when using configuration files only:



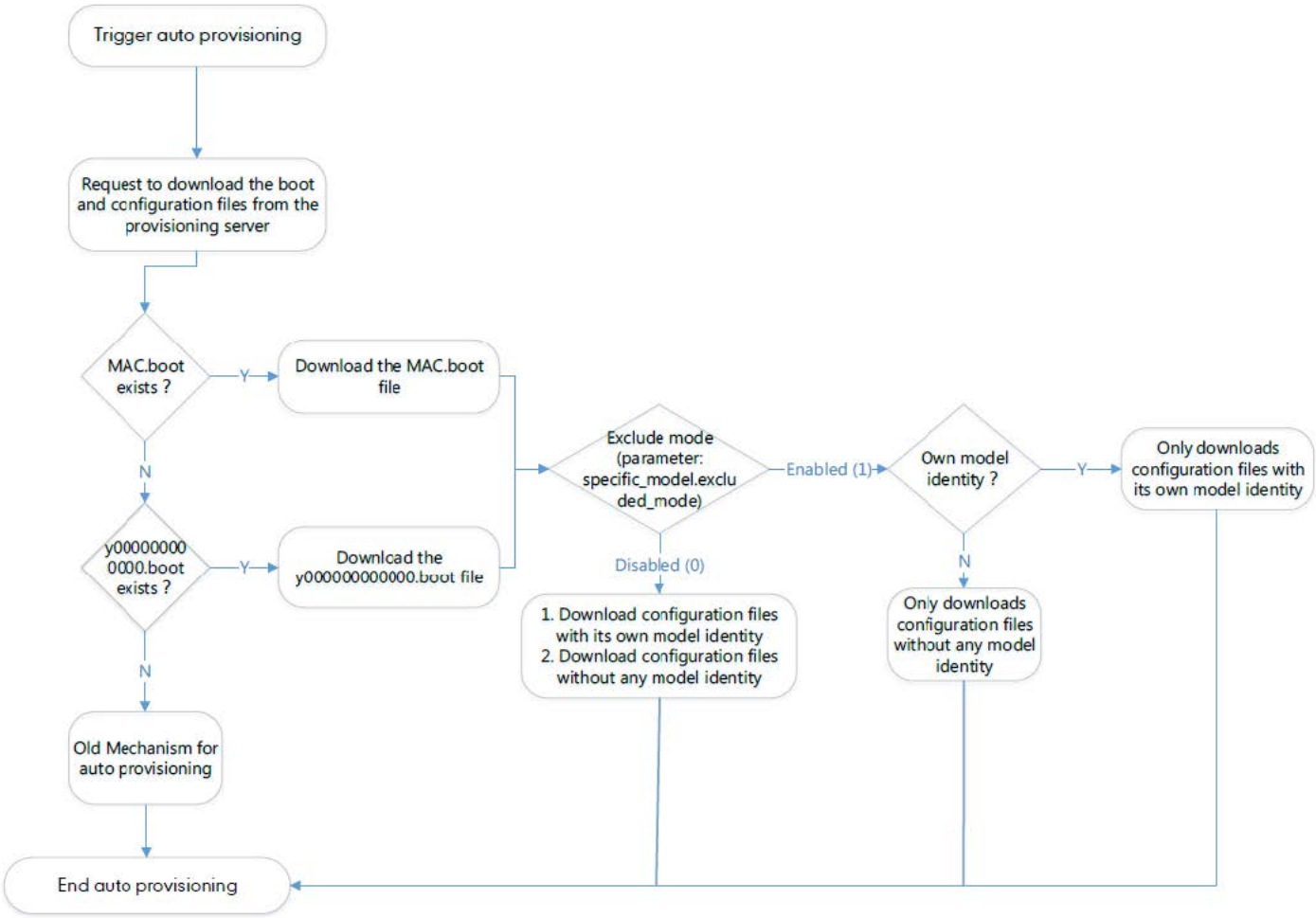
New Mechanism – With Boot Files

The following figure shows auto provisioning flowcharts for Yealink phones when using boot files:

Scenario A – Do Not Support Exclude Mode



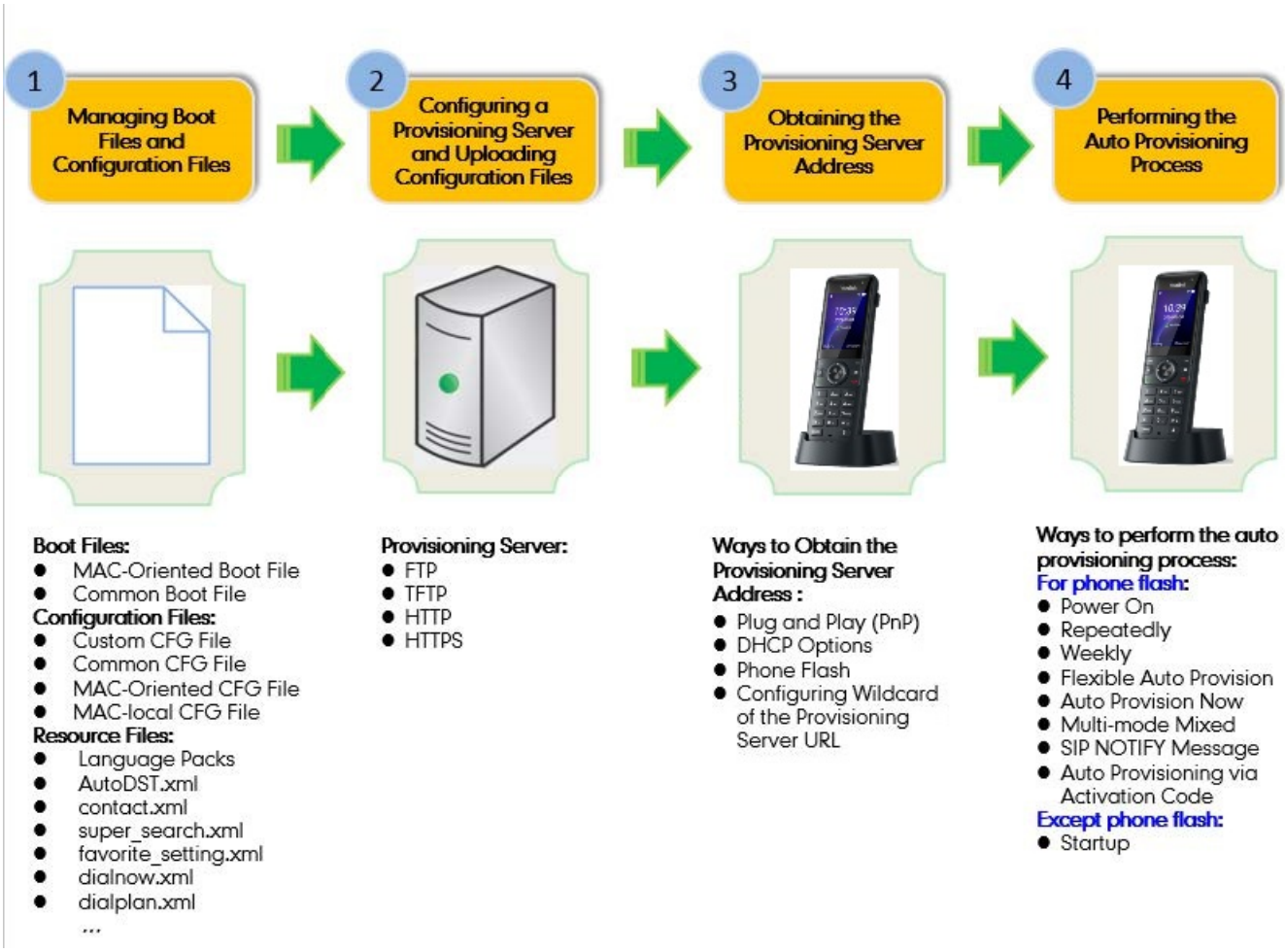
Scenario B – Support Exclude Mode



Major Tasks for Auto Provisioning

You need to complete four major tasks to provision Yealink phones.

The following figure shows an overview of four major provisioning tasks:



For more information on how to manage boot files, refer to Manage Boot Files .

For more information on how to manage configuration files, refer to Manage Configuration Files .

For more information on how to manage resource files, refer to Manage Resource Files .

For more information on how to configure a provisioning server, refer to Configure a Provisioning Server .

For more information on how to obtain the provisioning server address, refer to Obtain the Provisioning Server Address .

For more information on how to perform auto provisioning, refer to Trigger the Phone to Perform Auto Provisioning .

An Instance of Auto Provision Configuration

This section shows an instance of auto-provision configuration.

1. Manage boot files.

Specify the desired URL (for example, tftp://10.2.5.193/network.cfg) of the configuration files in the boot file (for example, y000000000000.boot).

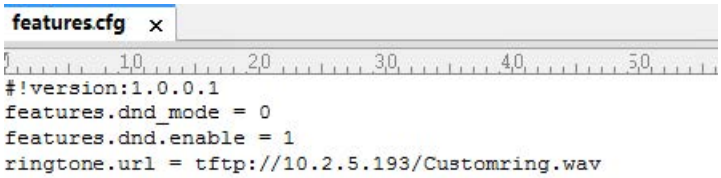
For more information on how to manage boot files, refer to Manage Boot Files .

```
#!version:1.0.0.1
## The header above must appear as-is in the first line

##[$MODEL]include:config <xxx.cfg>
##[$MODEL,$MODEL]include:config "xxx.cfg"

[AX83H]include:config <tftp://10.2.5.193/network.cfg>
[AX83H]include:config <../sip.cfg>
include:config "features.cfg"

overwrite_mode = 1
specific_model.excluded_mode=0
```

2. Manage configuration files.

   Add/Edit the desired configuration parameters in the CFG file (for example, features.cfg) you want the phone to download.

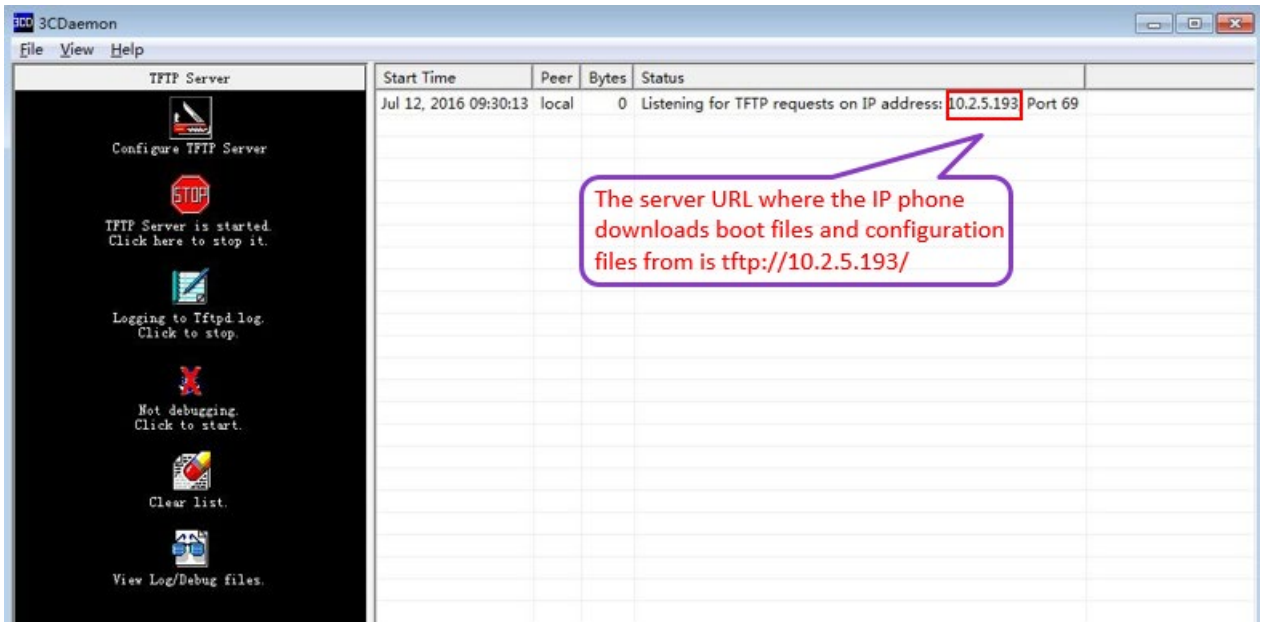
   For more information on how to manage configuration files, refer to Manage Configuration Files .



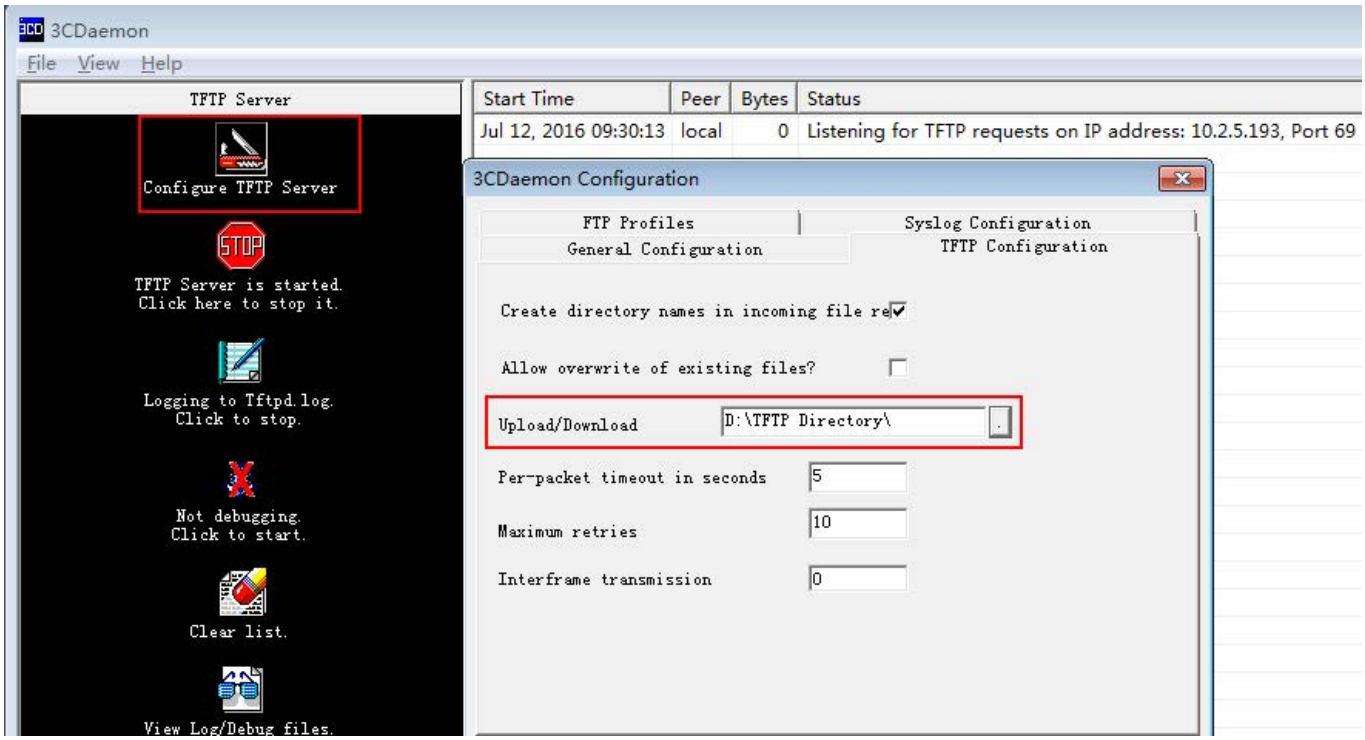
3. Configure the TFTP server.

   ① Place boot files, configuration files, and resource files in TFTP root directory (for example, D:\TFTP Directory).

   ② Start the TFTP server. The IP address of the TFTP server is shown as below:

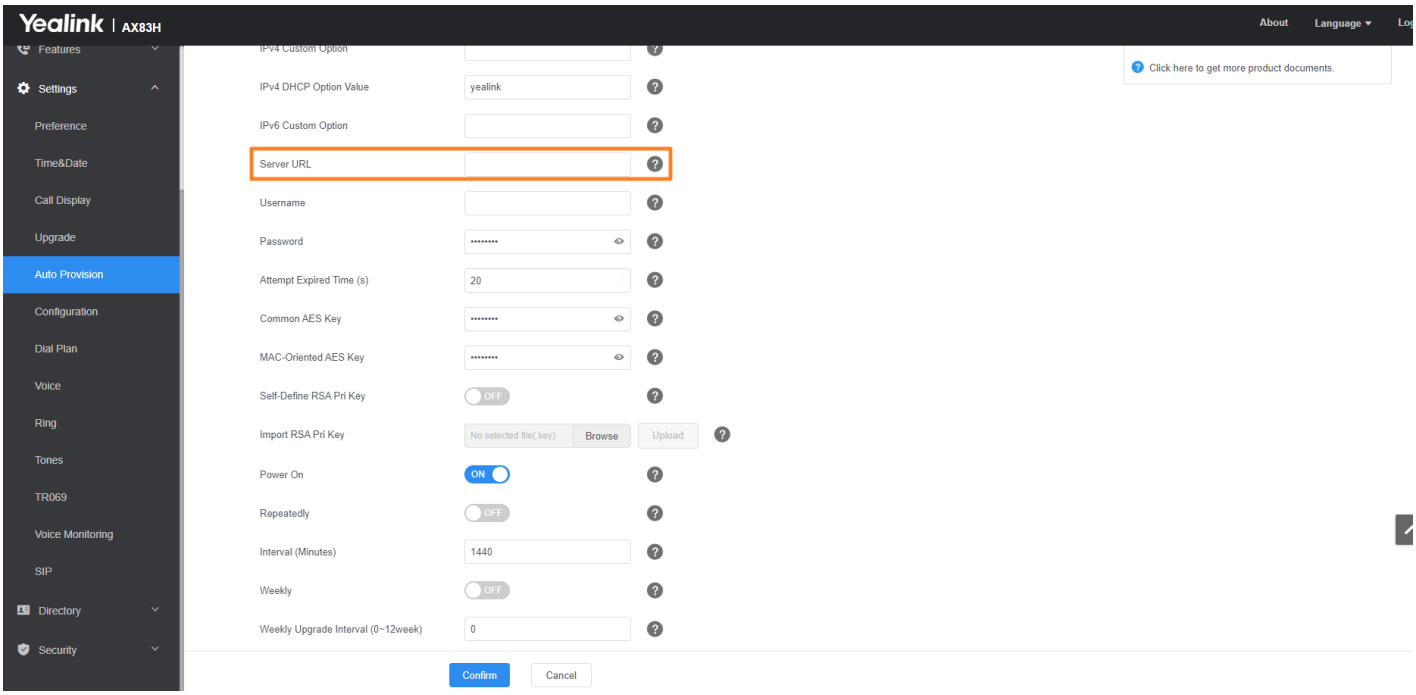


③ Select Configure TFTP Server. Click the ... button to locate the TFTP root directory in your local system.



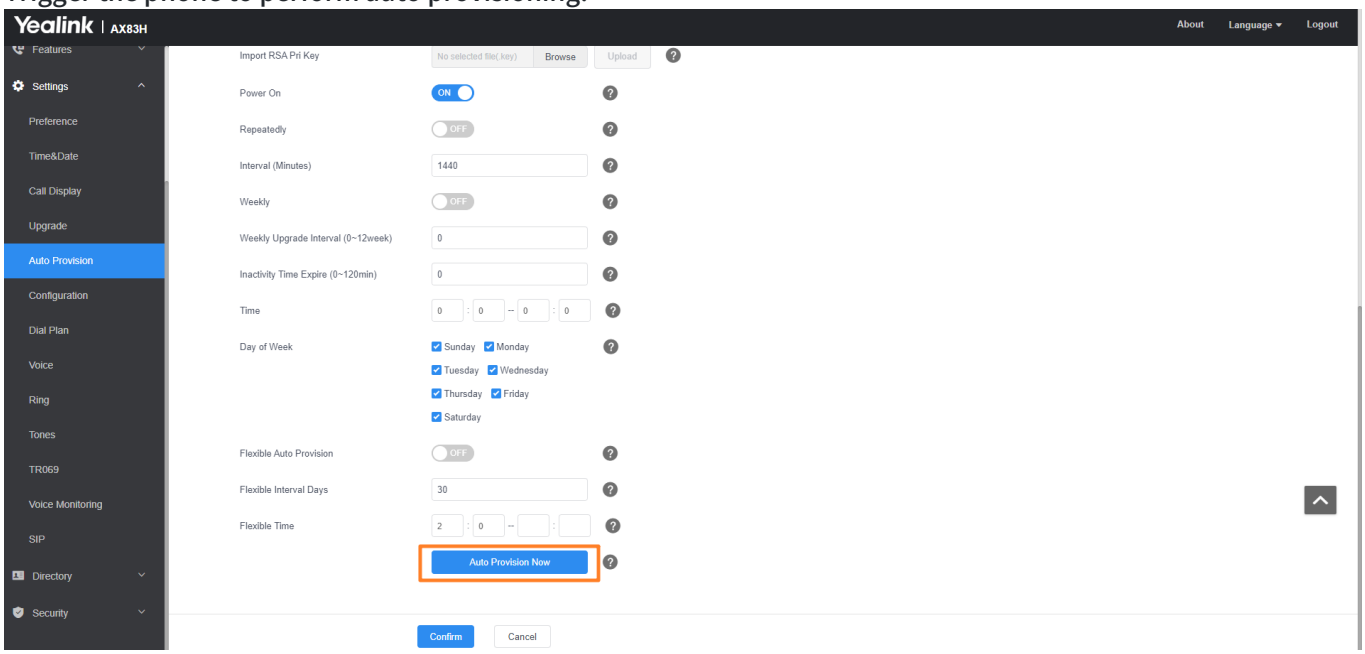
For more information on how to configure a provisioning server, refer to Configure a Provisioning Server .

4. Configure the provisioning server address on the phone.



For more information on how to obtain the provisioning server address, refer to Obtain the Provisioning Server Address .

5. Trigger the phone to perform auto provisioning.



For more information on how to perform auto provisioning, refer to Trigger the Phone to Perform Auto Provisioning .

FAQ

1. How to use the Zero Touch method to change the password
2. Phone Cannot Get Provisioned with Certificate Error
3. How to clear the value of the configuration parameter
4. RPS Can't Work

Manage Boot Files

Yealink phones can download CFG files referenced in the boot files. Before provisioning, you may need to edit and customize your boot files.

Yealink supports the following two types of boot files:

- MAC-Oriented boot file (for example, 00156574b150.boot)
- Common boot file (y000000000000.boot)

You can edit the template boot file directly or create a new boot file as required. Open each boot file with a text editor such as Notepad++.

Edit Common Boot File

The common boot file is effective for all phones. It uses a fixed name "y000000000000.boot" as the file name.

The following figure shows the contents of the common boot file:

```
#!version:1.0.0.1
## The header above must appear as-is in the first line

include:config <xxx.cfg>
include:config "xxx.cfg"

overwrite_mode = 1
```

The following table lists guidelines you need to know when editing the boot file:

Item	Guidelines
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
## The header above must appear as-is in the first line	The line beginning with "#" is considered to be a comment. You can use "#" to make any comment in the boot file.
include:config <xxx.cfg> include:config "xxx.cfg"	1) Each "include" statement can specify a URL where a configuration file is stored. The configuration file format must be *.cfg. 2) The URL in <> or "" supports the following two forms: · Relative URL (relative to the boot file): For example, sip.cfg, HTTP Directory/sip.cfg · Absolute URL: For example, http://10.2.5.258/HTTP Directory/sip.cfg The URL must point to a specific CFG file. The CFG files are downloaded in the order listed (top to bottom). The parameters in the newly downloaded configuration files will override the duplicate parameters in files downloaded earlier. 3) The "include" statement can be repeated as many times as needed. 4) The [$MODEL] can be added to specify settings for specific phone models. $MODEL represents the phone model name.

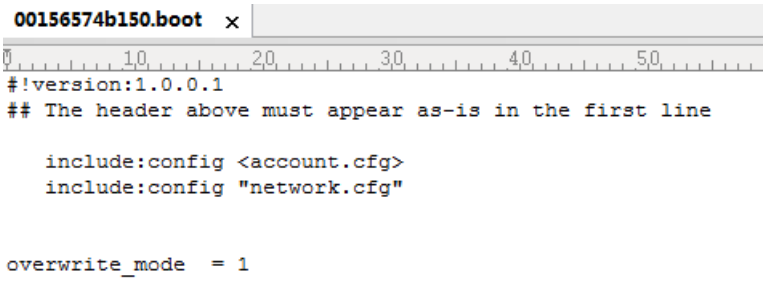
overwrite_mode	Enable or disable the overwrite mode. **1**-(Enabled) - If the value of a parameter in configuration files is left blank, or if a non-static parameter in configuration files is deleted or commented out, the factory default value takes effect. **0**-(Disabled) - If the value of a parameter in configuration files is left blank, deleted or commented out, the pre-configured value is kept. **NOTE** This parameter can only be used in boot files. If a boot file is used but the value of the parameter `overwrite_mode` is not configured, the overwrite mode is enabled by default.
specific_model.excluded_mode	Enable or disable the exclude mode. The exclude mode applies to the configuration files specified in the boot file. **0**-Disabled (Append Mode), the phone downloads its own model-specific configuration files and downloads other model-unspecified configuration files. **1**-Enabled (Exclude Mode), the phone attempts to download its own model-specific configuration files; if there are no own model-specific configuration files found on the server, it downloads model-unspecified configuration files. **NOTE** Exclude mode can only be used in boot files. If a boot file is used but the value of the parameter `specific_model.excluded_mode` is not configured, the exclude mode is disabled by default.

Create MAC-Oriented Boot File

The MAC-Oriented boot file is only effective for the specific phone. It uses the 12-digit MAC address of the IP phone as the file name.
For example, if the MAC address of the IP phone is 00156574B150, the MAC-Oriented boot file has to be named as 00156574b150.boot (case-sensitive) respectively.
If you want to create a MAC-Oriented boot file for your phone, follow these steps:
To create a MAC-Oriented boot file:

1. Create a boot file for your phone. Ensure the file complies with the guidelines that are listed in the Editing Common Boot File.
2. Copy the contents from the common boot file and specify the configuration files to be downloaded.

One or more configuration files can be referenced in the boot file. The following takes two configuration files for example:



3. Save the changes and close the MAC-Oriented boot file.

You can also make a copy of the common boot file, rename it and then edit it.

Manage Configuration Files

Auto provisioning enables Yealink phones to update themselves automatically via downloading Common CFG, MAC-Oriented CFG, custom CFG, and MAC-local CFG files. Before provisioning, you may need to edit and customize your configuration files.

You can edit the template configuration files directly or create a new CFG file as required. Open each configuration file with a text editor such as Notepad++.

For more information on the description of all configuration parameters in configuration files, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

Edit Common CFG File

The Common CFG file is effective for all phones of the same model. It uses a fixed name “y0000000000XX.cfg” as the file name, where "XX" equals to the first two digits of the hardware version of the phone model.

The names of the common CFG file requirements for the phone are:

Product Name	Common CFG File
AX83H	y000000000180.cfg

Common CFG file contains configuration parameters that apply to phones with the same model, such as language and volume.

The following figure shows a portion of the common CFG file:

```
#!version:1.0.0.1

##File header "#!version:1.0.0.1" can not be edited or deleted, and must be placed in the first line.##
##This template file is applicable to IP phones running firmware version 81 or later.##
##For more information on configuration parameters, refer to Description of Configuration Parameters in CFG Files.xlsx.##

############################################################################################
##                                      Hostname                                          ##
############################################################################################
static.network.dhcp_host_name =


############################################################################################
##                                   Network Advanced                                     ##
############################################################################################
##It enables or disables the PC port.0-Disabled,1-Auto Negotiation.
##The default value is 1.It takes effect after a reboot.
static.network.pc_port.enable =

##It configures the transmission mode and speed of the Internet (WAN) port.
##0-Auto Negotiate
##1-Full Duplex 10Mbps
##2-Full Duplex 100Mbps
##3-Half Duplex 10Mbps
##4-Half Duplex 100Mbps
##5-Full Duplex 1000Mbps (only applicable to SIP-T48G/T46G/T46S/T42G/T29G/T23G/CP860 IP phones)
##The default value is 0.It takes effect after a reboot.
static.network.internet_port.speed_duplex =

##It configures the transmission mode and speed of the PC (LAN) port.
##0-Auto Negotiate
##1-Full Duplex 10Mbps
##2-Full Duplex 100Mbps
```

The following table lists guidelines you need to know when editing the common CFG file:

Item	Guidelines
#	The line beginning with "#" is considered to be a comment.
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
Filename	The filename complies with the requirements that are listed in the above table.
Line formats and Rules	Each line must use the following format and adhere to the following rules: Configuration Parameter=Valid Value · Separate each configuration parameter and value with an equal sign. · Set only one configuration parameter per line. · Put the configuration parameter and value on the same line, and do not break the line. · The [$MODEL] can be added to the front of the configuration parameter to specify the value for specific phone groups. $MODEL represents the phone model. Multiple phone models are separated by commas.

Edit MAC-Oriented CFG File

The MAC-Oriented CFG file is only effective for the specific phone. It uses the 12-digit MAC address of the phone as the file name.

For example, if the MAC address of the phone is 00156574B150, the MAC-Oriented CFG file has to be named as 00156574b150.cfg (case-sensitive) respectively.

MAC-Oriented CFG file contains configuration parameters that are expected to be updated per phone, such as the registration information.

The following figure shows a portion of the MAC-Oriented CFG file:

```
1#!version:1.0.0.1

##File header "#!version:1.0.0.1" can not be edited or deleted, and must be placed in the first line.##
##This template file is applicable to IP phones running firmware version 81 or later.##
##For more information on configuration parameters, refer to Description of Configuration Parameters in CFG Files.xslx##

############################################################################################
##                            Account1 Basic Settings                                     ##
############################################################################################
account.1.enable =
account.1.label =
account.1.display_name =
account.1.auth_name =
account.1.user_name =
account.1.password =
account.1.outbound_proxy_enable =
account.1.outbound_host =
account.1.outbound_port =
account.1.dial_tone =


##It configures the transport type for account 1. 0-UDP,1-TCP,2-TLS,3-DNS-NAPTR
##The default value is 0.
account.1.sip_server.1.transport_type =
account.1.sip_server.2.transport_type =

############################################################################################
##                            Failback                                                    ##
############################################################################################

account.1.naptr_build =
account.1.fallback.redundancy_type =
account.1.fallback.timeout =
account.1.sip_server.1.address =
```

The following table lists guidelines you need to know when editing the MAC-Oriented CFG file:

Item	Guidelines
#	The line beginning with “#” is considered to be a comment.
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
Filename	The filename matches the MAC address of your phone.
Line formats and Rules	Each line must use the following format and adhere to the following rules: Configuration Parameter=Valid Value · Separate each configuration parameter and value with an equal sign. · Set only one configuration parameter per line. · Put the configuration parameter and value on the same line, and do not break the line. · The [$MODEL] can be added to the front of the configuration parameter to specify the value for specific phone groups. $MODEL represents the phone model.

ⓘ NOTE

· AX83H phone supports 16 accounts

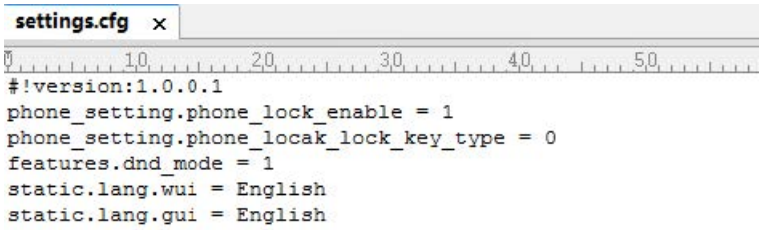
Create a New CFG File

If you want to create a new CFG file for your phone, follow these steps:

To create a new CFG file:

1. Create a CFG file for your phone. Ensure the file complies with the guidelines that are listed in Editing Common CFG File or Editing MAC-Oriented CFG File.

2. Copy configuration parameters from the template configuration files and set valid values for them.



3. (Optional.) Specify different parameter values for specific phone groups.
   For example:

```
[T46S] features.dnd_mode = 1
[T48G, T23G] features.dnd_mode = 0
```

4. Save the changes and close the CFG file.
   You can also make a copy of the template configuration file, rename it and then edit it.

Manage MAC-local CFG File

By default, MAC-local CFG file automatically stores non-static settings modified via web user interface or phone user interface. This file is stored locally on the IP phone, but a copy can also be uploaded to the provisioning server (or a specified URL configured by `static.auto_provision.custom.sync.path`). This file enables the phone to keep the user's personalization settings, even after auto provisioning. As with the MAC-Oriented CFG files, MAC-local CFG files are only effective for the specific phone. They use the 12-digit MAC address of the IP phone as the file name. For example, if the MAC address of the IP phone is 00156574B150, MAC-local CFG file has to be named as 00156574b150-local.cfg (case-sensitive).
If your phone with the current firmware version cannot generate a `<MAC>-local.cfg` file, the IP phone will automatically generate a MAC-local CFG file after it is upgraded to the latest firmware.
For more information on how to keep user's personalization settings, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

ⓘ NOTE
We recommend you do not edit the MAC-local CFG file. If you really want to edit MAC-local CFG file, you can export and then edit it.

Encrypt Configuration Files

To protect against unauthorized access and tampering with sensitive information (for example, login password, registration information), you can encrypt configuration files using Yealink Configuration Encryption Tool. AES keys must be 16 characters and the supported characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # $ % * + , - . : = ? @ [ ] ^ _ { } ~. For more information on how to encrypt configuration files, refer to Yealink Configuration Encryption Tool User Guide .

Manage Resource Files

Before provisioning, you may need to edit and customize your resource files.
You can edit the template resource files directly or create a new resource file as required. Open each resource file with a text editor such as Notepad++.

Customize Resource Files

The resource files are effective for all phones of the same model or the specific phone. If the resource file is to be used for all IP phones of the same model, the access URL of resource file had better be specified in the common CFG file. However, if you want to specify the desired phone to use the resource file, the access URL of the resource file should be specified in the MAC-Oriented CFG file.
Refer to Resource Files to get support resource files:
For more information on how to customize these template resource files and an explanation of the configuration parameters that related to these features, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

Configure a Provisioning Server

Yealink phones support using FTP, TFTP, HTTP, and HTTPS protocols to download boot files and configuration files. You can use one of these protocols for provisioning. The TFTP protocol is used by default. The following section provides instructions on how to configure a TFTP server.
We recommend that you use 3CDaemon or TFTPD32 as a TFTP server. 3CDaemo and TFTPD32 are free applications for Windows. You can download 3CDaemon online and TFTPD32 online.
For more information on how to configure FTP and HTTP servers, refer to Configure FTP Server and Configure HTTP Server .

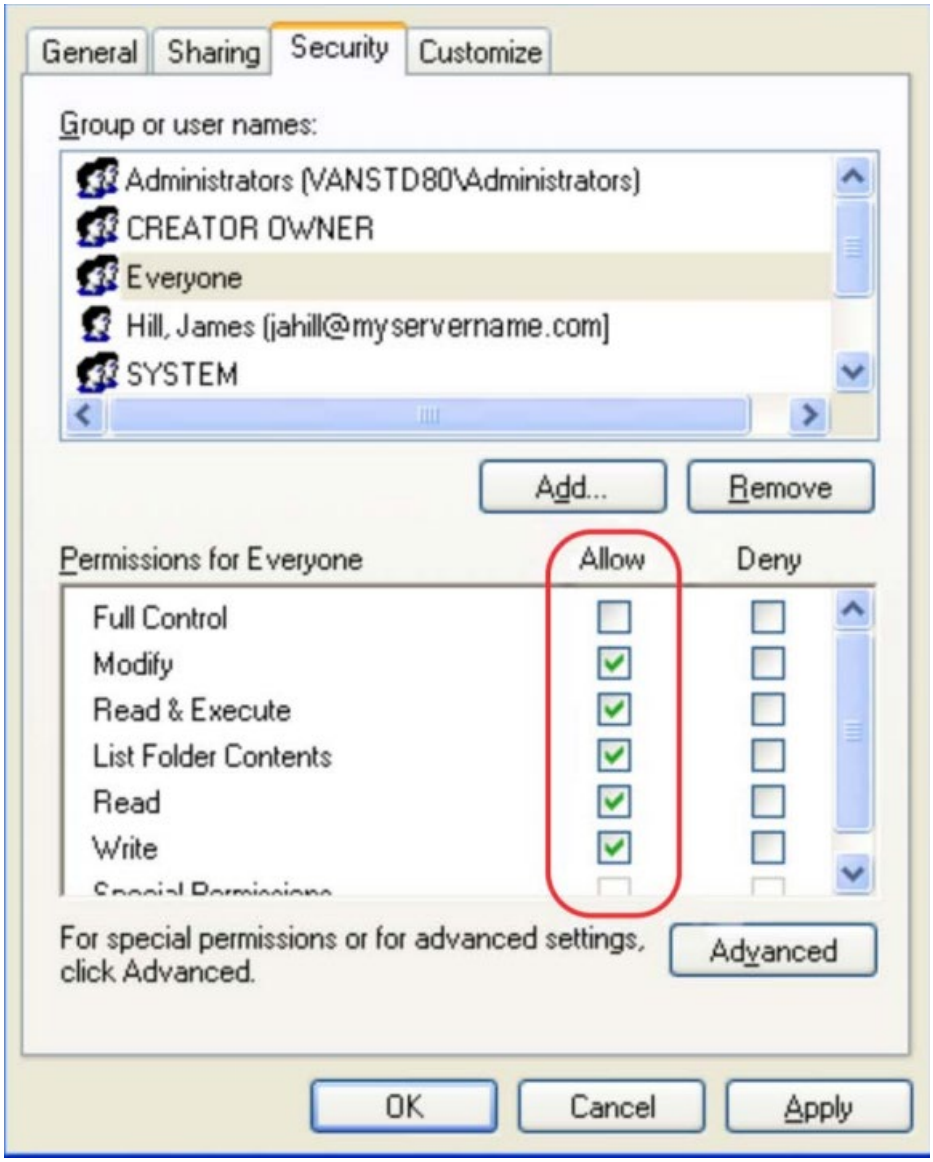
Prepare a Root Directory

To prepare a root directory:

1. Create a TFTP root directory on the local system (for example, D:\TFTP Directory).
2. Place the boot files, configuration files and resource files to this root directory.

3. (Optional.) Set security permissions for the TFTP directory folder.
   You need to define a user or a group name, and set the permissions: read, write or modify. Security permissions vary by organizations.

   An example of configuration on the Windows platform is shown as below:

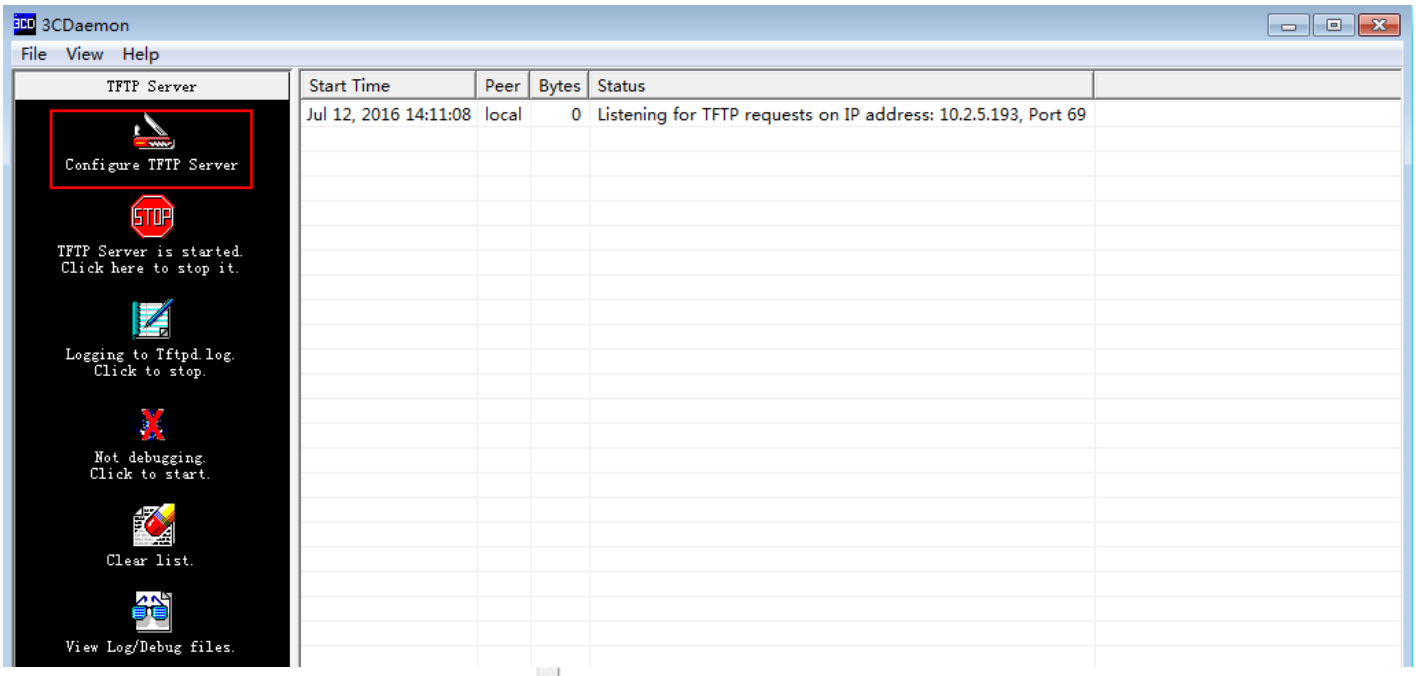


Configure a TFTP Server

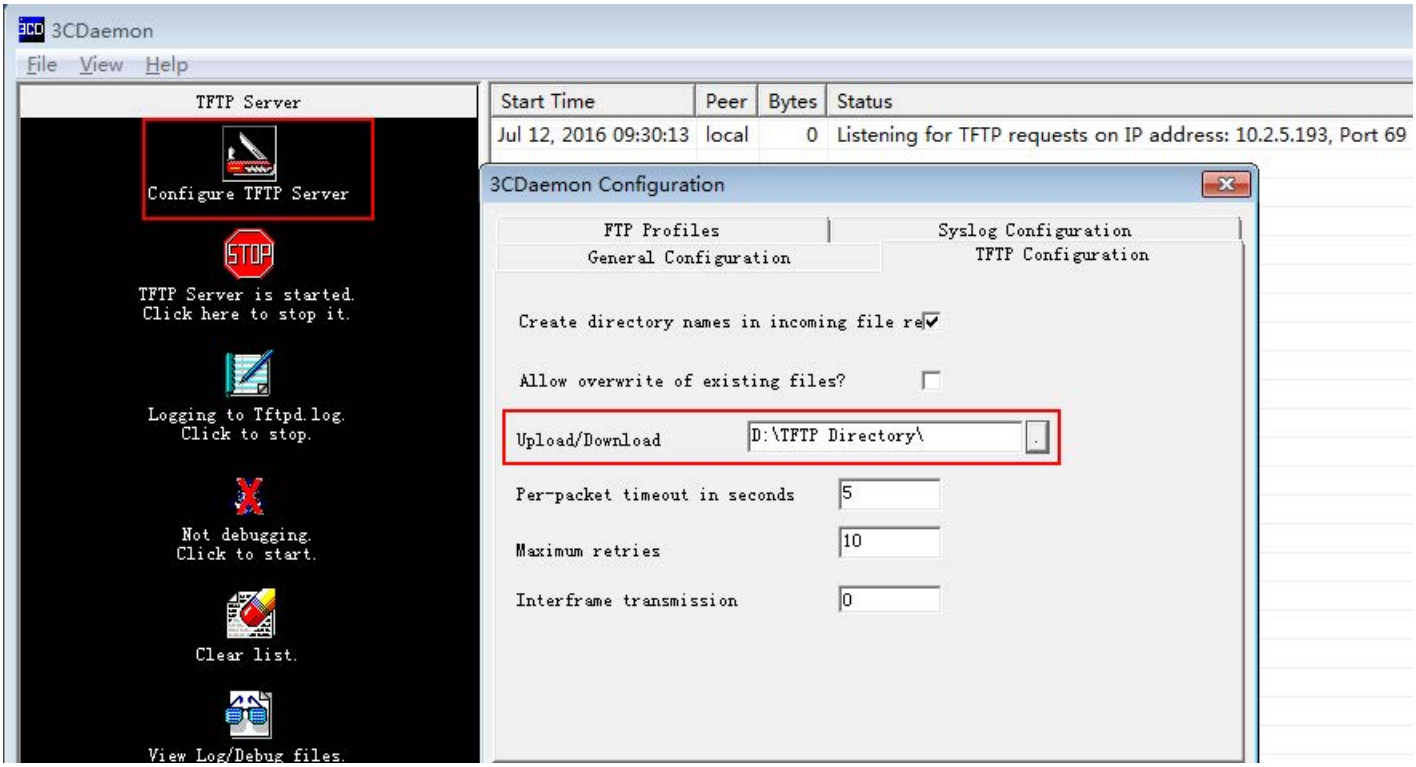
If you have a 3CDaemon application installed on your local system, use it directly. Otherwise, download and install it.

To configure a TFTP server:

1. Double click 3CDaemon.exe to start the application.
   A configuration page is shown as below:



2. Select Configure TFTP Server. Click the ... button to locate the TFTP root directory from your local system:



3. Click the **Confirm** button to finish configuring the TFTP server.

The server URL "tftp://IP/" (Here "IP" means the IP address of the provisioning server, for example, " tftp://10.2.5.193/") is where the IP phone downloads configuration files from.

Obtain the Provisioning Server Address

Yealink phones can obtain the provisioning server address in the following ways:

- Plug and Play (PnP) Server
- DHCP Options

- Phone Flash
- Configuring Wildcard of the Provisioning Server URL

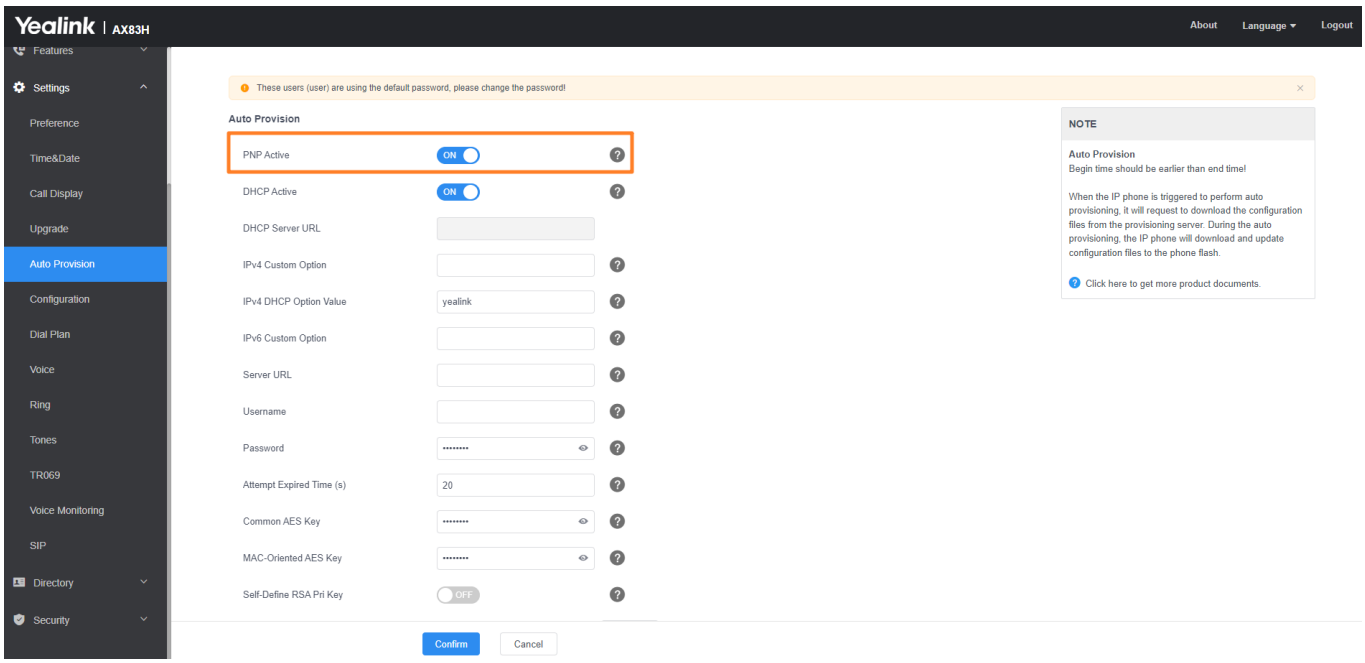
The priority of obtaining the provisioning server address is as follows: PnP Server>DHCP Options (for IPv4: IPv4 Custom option>option 66>option 43; for IPv6: IPv6 Custom option>option 59) >Phone Flash. The following sections detail the process of each way (take the SIP-T23G IP phone as an example).

Plug and Play Server

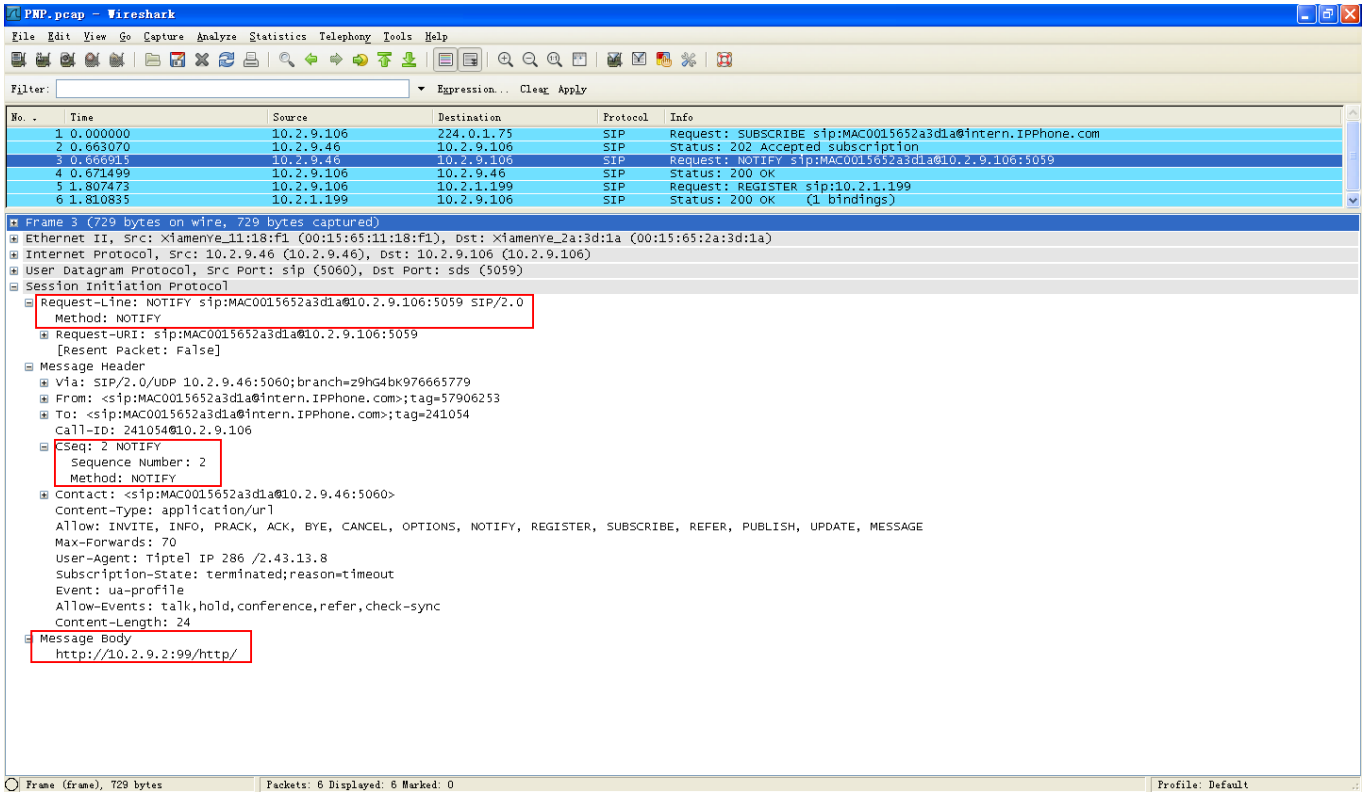
Yealink phones support obtaining the provisioning server address from the PnP server. The IP phone broadcasts the PnP SUBSCRIBE message to obtain the provisioning server address during startup. To use Plug and Play, make sure this feature is enabled.

To configure PnP via web user interface:

1. Click **Settings** > **Auto Provision**.
2. Mark the **On** check box in the **PNP Active** field.



3. Click **Confirm** to accept the change.
   Any PnP server activated in the network responds with a **SIP NOTIFY** message, and the address of the provisioning server is contained in the message body.



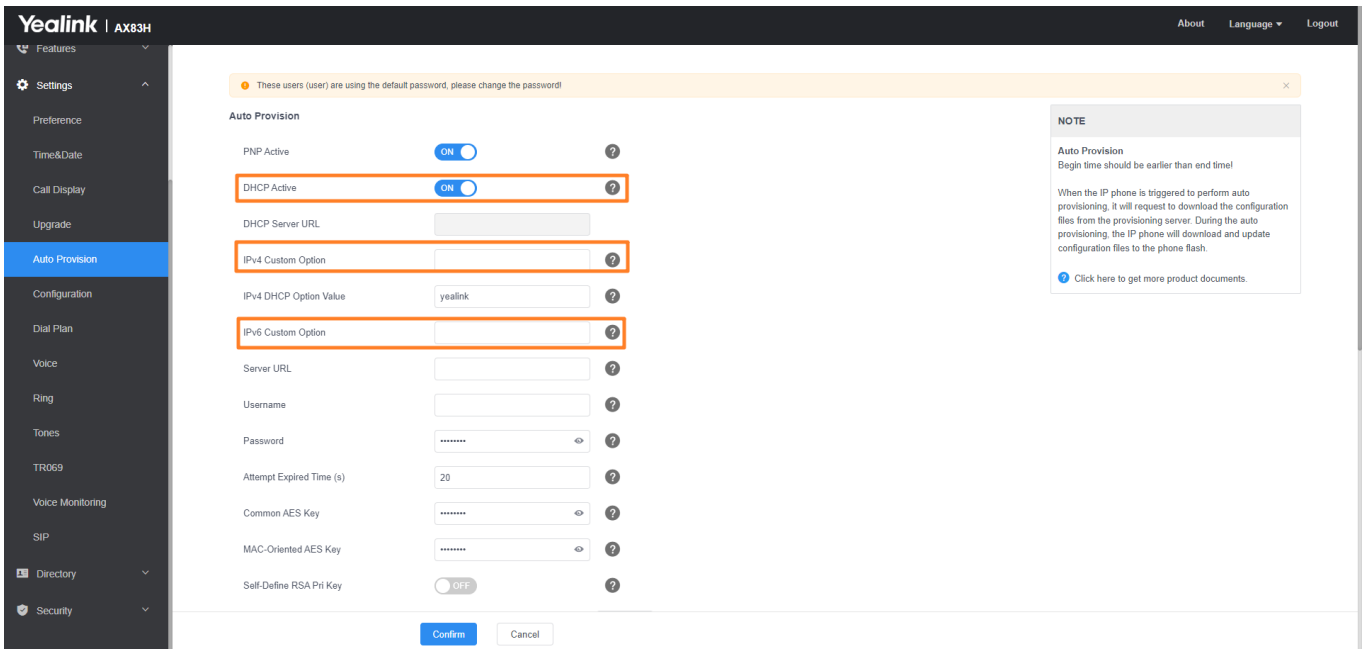
   After the IP phone obtains the provisioning server address from the PNP server, it will connect to the provisioning server and perform auto provisioning during startup.

DHCP Options

Yealink phones can obtain the provisioning server address by detecting DHCP options during startup.
If you are using the IPv4 network, the phone will automatically detect the option 66 and option 43 for obtaining the provisioning server address. DHCP option 66 is used to identify the TFTP server. DHCP option 43 is a vendor-specific option, which is used to transfer the vendor-specific information.
If you are using IPv6 network, the phone will automatically detect the option 59 for obtaining the provisioning server address. DHCP option 59 is used to specify a URL for the boot file to be downloaded by the client.
You can configure the phone to obtain the provisioning server address via a custom DHCP option. You can select to use IPv4 or IPv6 custom DHCP option according to your network environment. To obtain the provisioning server address via an IPv4 or IPv6 custom DHCP option, make sure the DHCP option is properly configured on the phone. The IPv4 or IPv6 custom DHCP option must be in accordance with the one defined in the DHCP server.
To configure the DHCP option via the web user interface:

1. Click **Settings** > **Auto Provision**.
2. Mark the **On** check box in the **DHCP Active** field.
3. If you are using IPv4 network, enter the desired value in the **IPv4 Custom Option** field.

4. If you are using IPv6 network, enter the desired value in the **IPv6 Custom Option** field.



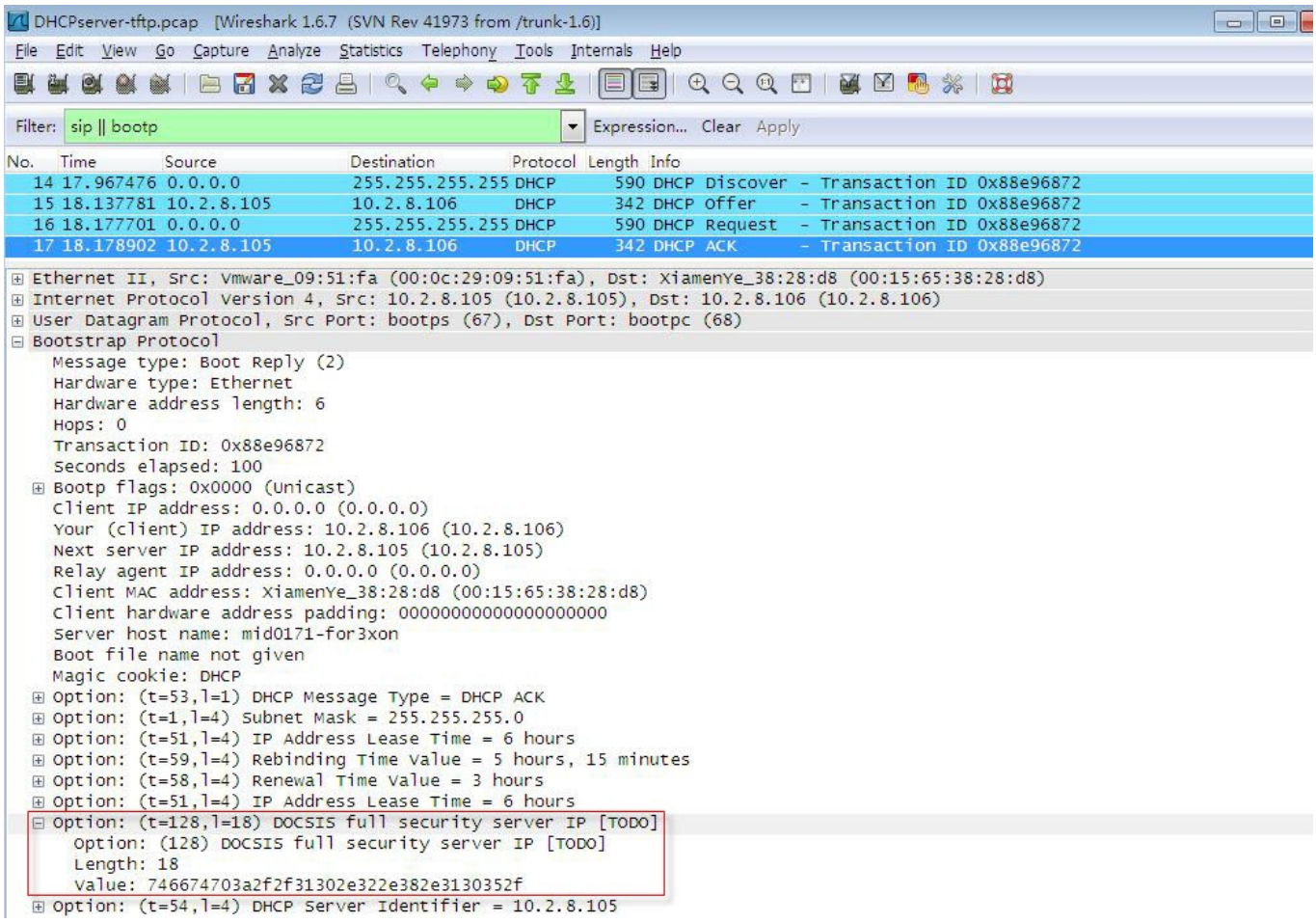
5. Click **Confirm** to accept the change.

   During startup, the phone will broadcast DHCP request with DHCP options for obtaining the provisioning server address. The provisioning server address will be found in the received DHCP response message.

   After the IP phone obtains the provisioning server address from the DHCP server, it will connect to the provisioning server and perform auto provisioning during startup.

   For more information on the DHCP options, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

   The following figure shows the example messages of obtaining the TFTP server address from an IPv4 custom DHCP option:



Right-click the root node of the custom option (for example, option 128) shown on the above figure, and select **Copy** > **Bytes** > **Printable Text Only**. Paste the copied text in your favorite text editor to check the address, for example, tftp://192.168.1.100/.

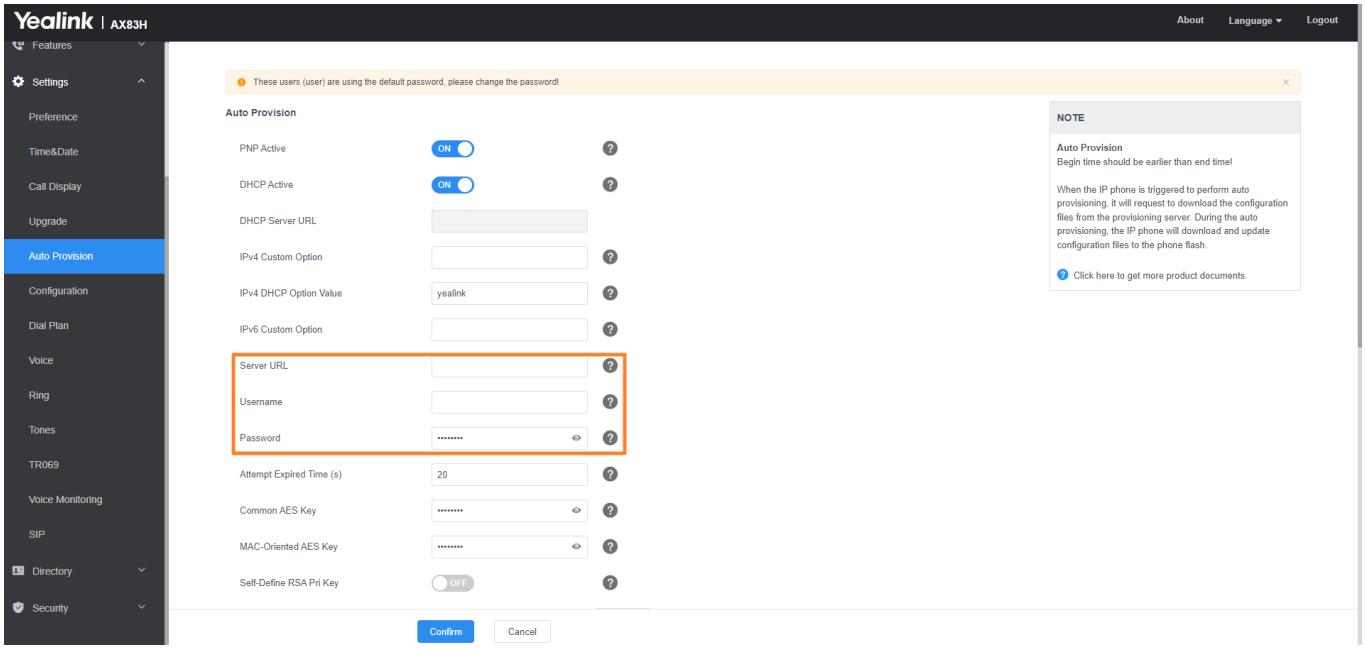
Phone Flash

Yealink IP phones can obtain the provisioning server address from the IP phone flash. To obtain the provisioning server address by reading the IP phone flash, make sure the configuration is set properly.

To configure the IP phone flash via web user interface:

1. Click **Settings** > **Auto Provision**.

2. Enter the URL, user name and password of the provisioning server in the **Server URL**, **User Name** and **Password** field respectively (the user name and password are optional).



3. Click **Confirm** to accept the change.

After the above configuration is completed, the IP phone will connect to the configured provisioning server and perform auto provisioning by one of the following methods: Power On, Repeatedly, Weekly, Flexible Auto Provision, Auto Provision Now, SIP NOTIFY Message and Multi-mode Mixed. For more information on these methods, refer to Trigger the Phone to Perform Auto Provisioning.

Configure Wildcard of the Provisioning Server URL

Normally, many phone models may be deployed in your environment. To deploy many phone models using a unified provisioning server, it is convenient for the administrator to configure a unified provisioning server URL for different phone models. On the provisioning server, many directories need to be configured for different phone models, each with a unique directory name. Yealink IP phones support the following wildcards in the provisioning server URL:

- $PN: it is used to identify the directory name of the provisioning server directory where the corresponding boot files and configuration files are located.
- $MAC: it is used to identify the MAC address of the IP phone.

The parameter `static.auto_provision.url_wildcard.pn` is used to configure the directory name where the boot files and configuration files located.

For more information on the parameter, refer to the latest IP Phones Description of Configuration Parameters in CFG Files or Administrator Guide for your phone on Yealink Technical Support.

When the IP phone obtains a provisioning server URL containing the wildcard $PN, it automatically replaces the character $PN with the value of the parameter "static.auto_provision.url_wildcard.pn" configured on the IP phone. When the IP phone is triggered to perform auto provisioning, it will request to download the boot files and configuration files from the identified directory on the provisioning server.

NOTE
The value of the parameter "static.auto_provision.url_wildcard.pn" must be configured in accordance with the directory name of the provisioning server directory where the boot files and configuration files of the IP phones are located.

The following example assists in explaining the wildcard feature:
You want to deploy SIP-T42G and AX83H phones simultaneously in your environment. IP phones are configured to obtain the provisioning server URL via DHCP option 66. The following details how to deploy the SIP-T42G and AX83H phones using the wildcard feature.

1. Create two directories on the root directory of the provisioning server.
2. Configure the directory names of these two directories to be "T42G" and "AX83H".
3. Place the associated boot files and configuration files in the directory created above.
4. Configure the value of DHCP option 66 on the DHCP server as tftp://192.168.1.100/$PN.
5. Configure the value of the parameter `static.auto_provision.url_wildcard.pn`.
   The default value of the parameter `static.auto_provision.url_wildcard.pn` is "T42G" for the SIP-T42G IP phones and "AX83H" for the AX83H phones. If the default value is different from the directory name, you need to configure the value of this parameter to be the directory name on the IP phones in advance.

During startup, IP phones obtain the provisioning server URL "tftp://192.168.1.100/PN" via DHCP option 66 and then replace the character "PN" via DHCP option 66 and then replace the character "PN" via DHCP option 66 and then replace the character "PN" in the URL with "T42G" for the SIP-T42G IP phones and "AX83H" for the AX83H phones. When performing auto provisioning, the SIP-T42G IP phones, and the AX83H phones first request to download the MAC-Oriented boot files and configuration files referenced in MAC-Oriented boot files from the provisioning server address "tftp://192.168.1.100/T42G" and "tftp://192.168.1.100/AX83H" respectively. If no matched MAC-Oriented boot files are found on the server, the SIP-T42G IP phones and the AX83H phones request to download the common boot files and configuration files referenced in common boot files from the provisioning server address "tftp://192.168.1.100/T42G" and "tftp://192.168.1.100/AX83H" respectively.
If the URL is configured as "tftp://192.168.1.100/PN/PN/PN/MAC.boot" on the DHCP server, the SIP-T42G IP phones, and the AX83H phones will replace the characters "PN" with "T42G" and "AX83H" respectively,and replace the characters "PN" with "T42G" and "AX83H" respectively, and replace the characters "PN" with "T42G" and "AX83H" respectively, and replace the characters "MAC" with their MAC addresses. For example, the MAC address of one SIP-T42G IP phone is 00156543EC97. When performing auto provisioning, the IP phone will only request to download the 00156543ec97.boot file and configuration files referenced in the 00156543ec97.boot file from the provisioning server address "tftp://192.168.1.100/T42G".
For more information on boot files, refer to Manage Boot Files.

Trigger the Phone to Perform Auto Provisioning

This chapter introduces the following methods to trigger the phone to perform auto provisioning:

- Power On

- Repeatedly
- Weekly
- Flexible Auto Provision
- Auto Provision Now
- Multi-Mode Mixed
- SIP NOTIFY Message
- Auto Provisioning via Activation Code

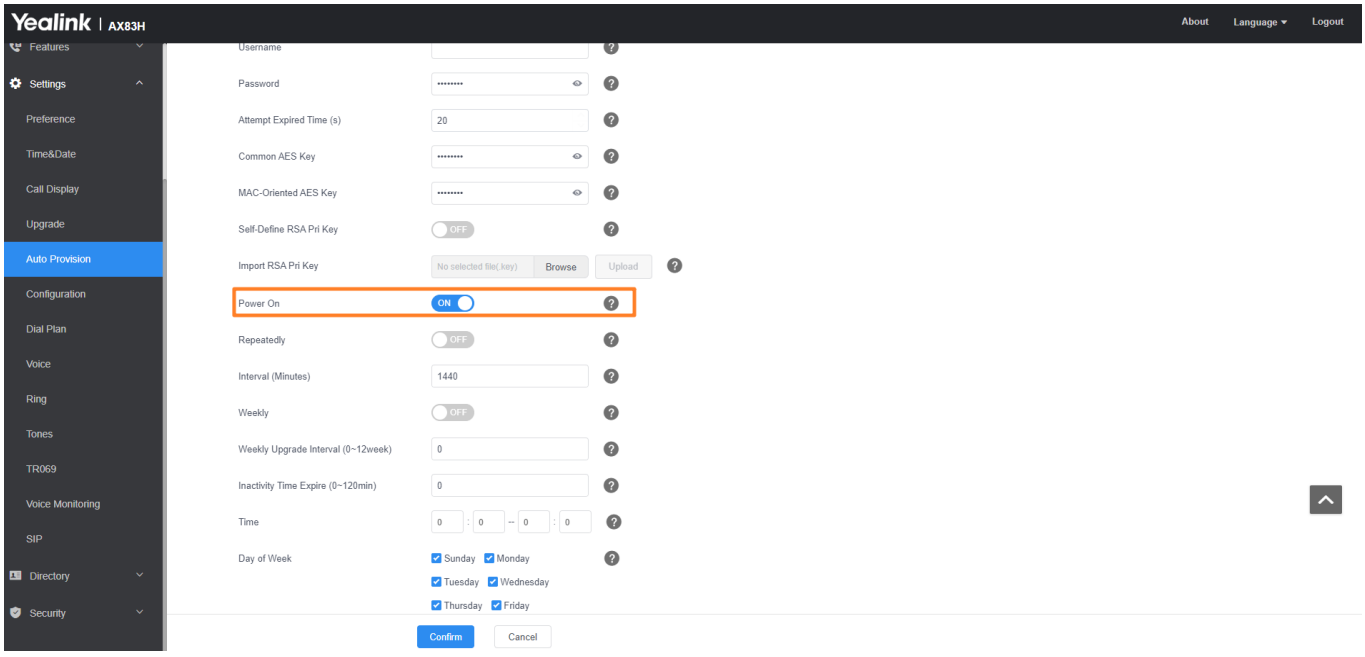
When there is an active call on the phone during auto provisioning, the IP phone will detect the call status every 30 seconds. If the call is released within 2 hours, the auto provisioning will be performed as usual. Otherwise, the process will be ended due to timeout.

Power On

The phone performs the auto provisioning when the IP phone is powered on.

To activate the power on mode via a web user interface:

1. Click **Settings** > **Auto Provision**.
2. Select the **On** check box in the **Power On** field.



3. Click **Confirm** to accept the change.

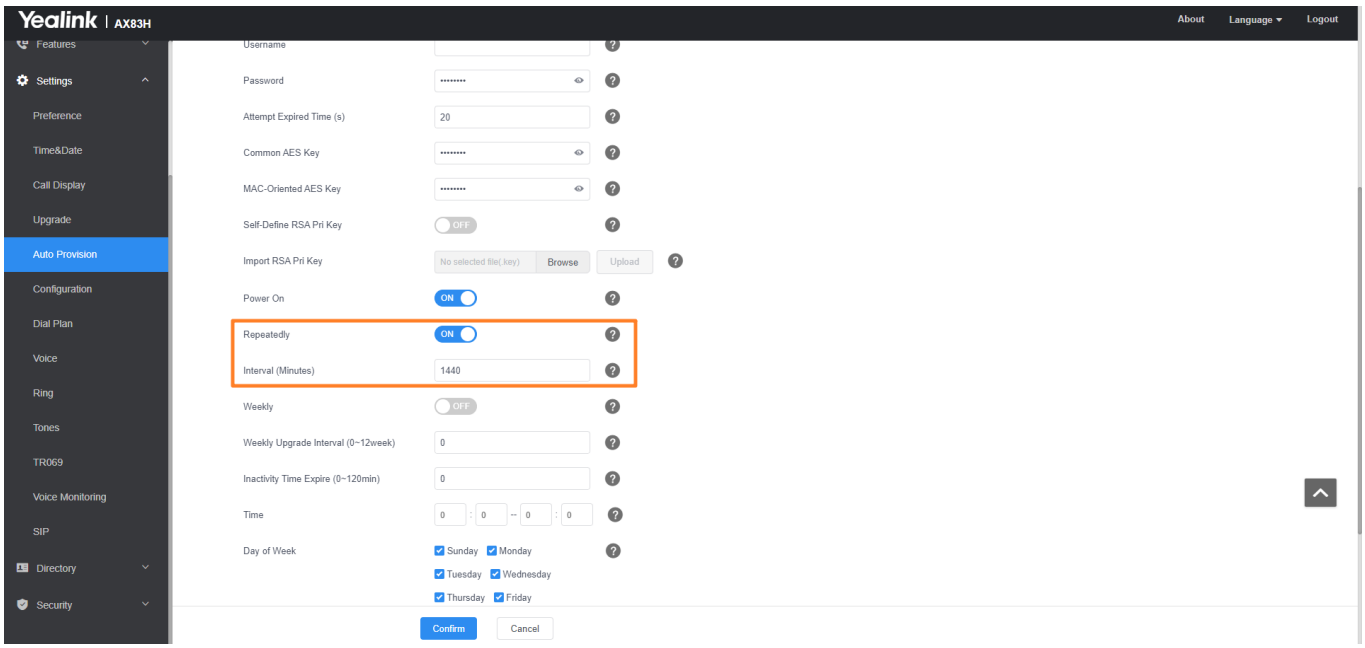
Repeatedly

The IP phone performs the auto provisioning at regular intervals. You can configure the interval for the repeatedly mode. The default interval is 1440 minutes.

To activate the repeatedly mode via web user interface:

1. Click **Settings** > **Auto Provision**.
2. Select the **On** check box in the **Repeatedly** field.

3. Enter the desired interval time (in minutes) in the **Interval(Minutes)** field.



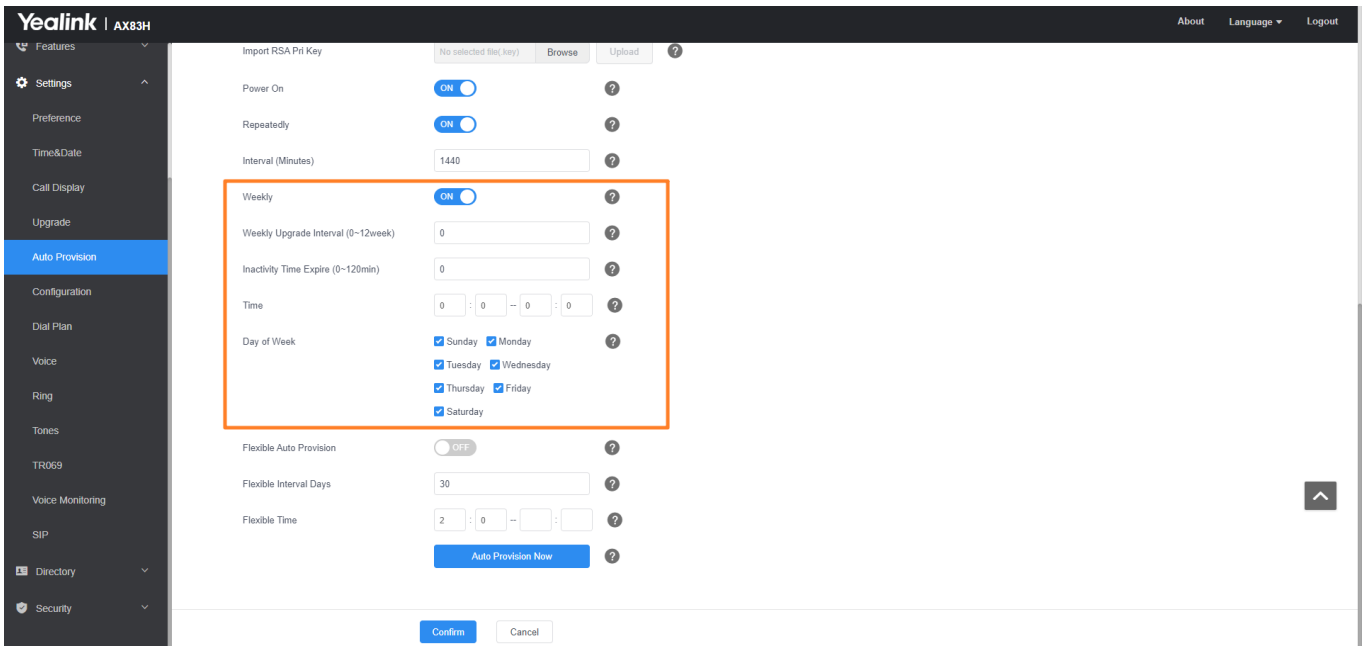
4. Click **Confirm** to accept the change.

Weekly

The IP phone performs auto provisioning at a random time every week/month/quarter. You can configure what time of the day and which day of the week to trigger the IP phone to perform auto provisioning. You can also configure a regular weekly interval to trigger the IP phone to perform auto provisioning. You can specify the delay time to perform auto provisioning when the IP phone is inactive at regular week. For example, you can configure the IP phone to check and update new configuration only when the IP phone has been inactivated for 10 minutes between 2 to 3 o’ clock in the morning every Monday at a 4-week interval.
If you configure two or more days in a week, the auto provisioning only occurs on a random day.
To activate the weekly mode via the web user interface:

1. Click **Settings** > **Auto Provision**.
2. Select the **On** check box in the **Weekly** field.
3. Enter the desired upgrade interval in the **Weekly Upgrade Interval(0~12week)** field.
4. Enter the desired value in the **Inactivity Time Expire(0~120min)** field.
5. Enter the desired time in the **Time** field.

6. Check one or more checkboxes in the **Day of Week** field.



7. Click **Confirm** to accept the change.

Flexible Auto Provision

The IP phone performs auto provisioning at a random time on a random day within a specific period of time. The random day is calculated on the basis of the phone's MAC address. You can specify an interval and configure what time of the day to trigger the IP phone to perform auto provisioning.

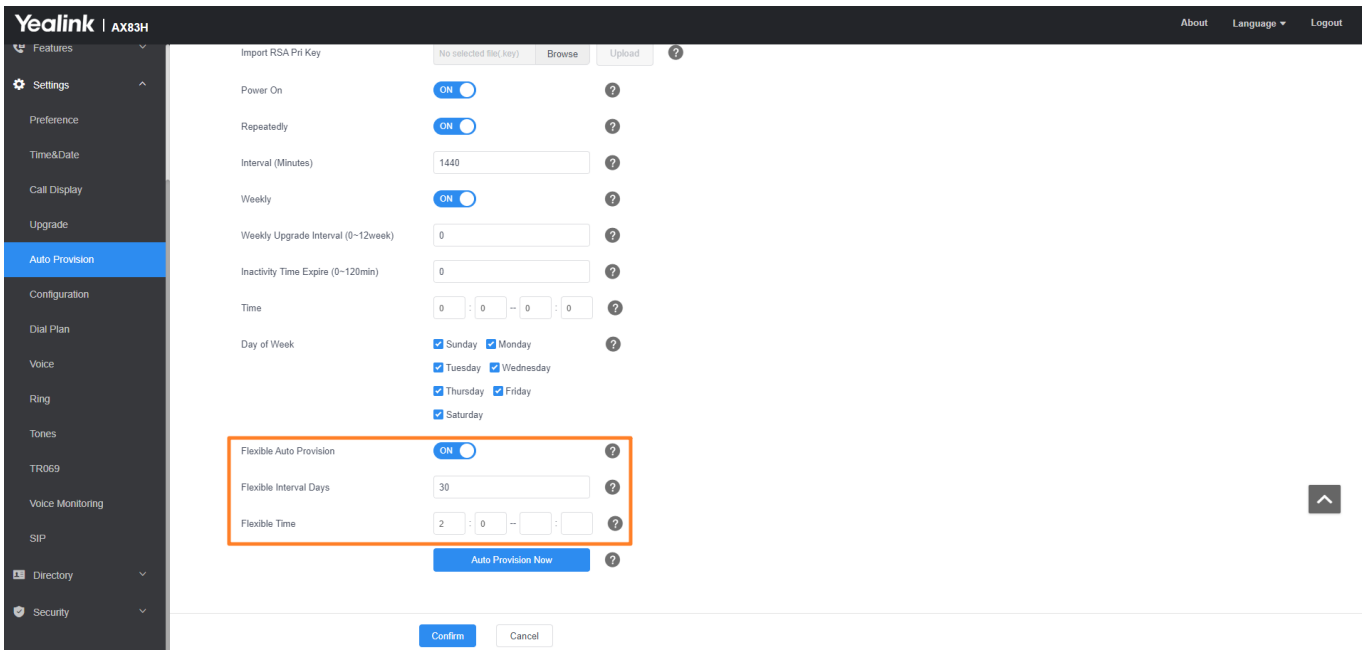
For example, you can configure the IP phone to check and update new configurations between 1 and 6 o’ clock in the morning at a 30-day interval. The IP phone will perform auto provisioning at a random time (for example, 03:47) on a random day (for example, 18) based on the phone's MAC address.

Note that the update time will be recalculated if auto provisioning occurs (for example, Auto Provision Now) during this specific period of time.

To activate the flexible auto provision mode via the web user interface:

1. Click **Settings** > **Auto Provision**.
2. Select the **On** check box in the **Flexible Auto Provision** field.
3. Enter the desired value in the **Flexible Interval Days** field.

4. Enter the desired start time and end time in the **Flexible Time** field.



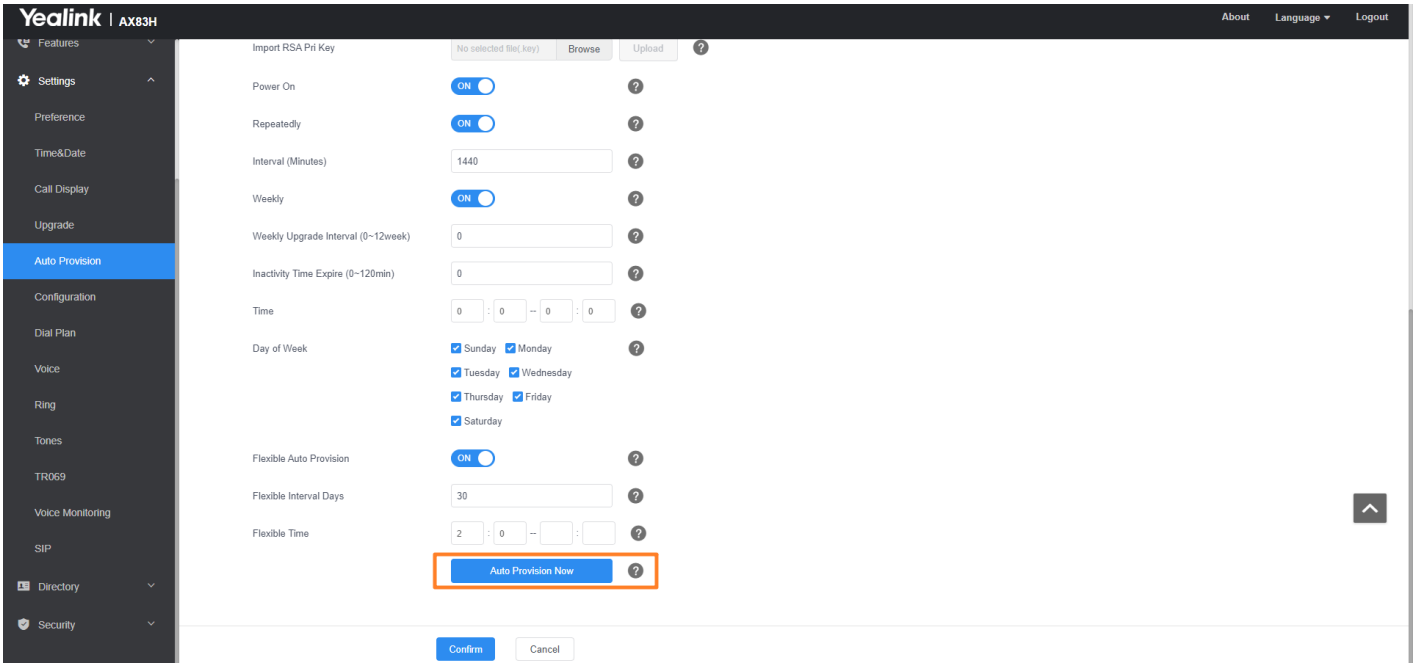
5. Click **Confirm** to accept the change.

Auto Provision Now

You can use auto provision now mode to manually trigger the IP phone to perform auto provisioning immediately.

To use the auto provision now mode via web user interface:

1. Click **Settings** > **Auto Provision**.
2. Click **Auto Provision Now**.



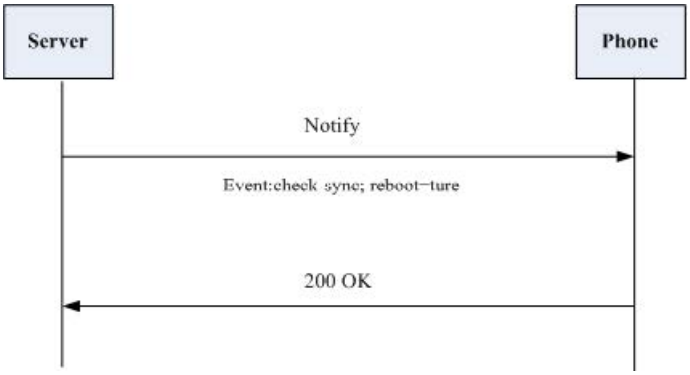
The IP phone will perform auto provisioning immediately.

Multi-Mode Mixed

You can activate more than one method for auto provisioning. For example, you can activate the "Power On" and "Repeatedly" modes simultaneously. The IP phone will perform auto provisioning when it is powered on and at a specified interval.

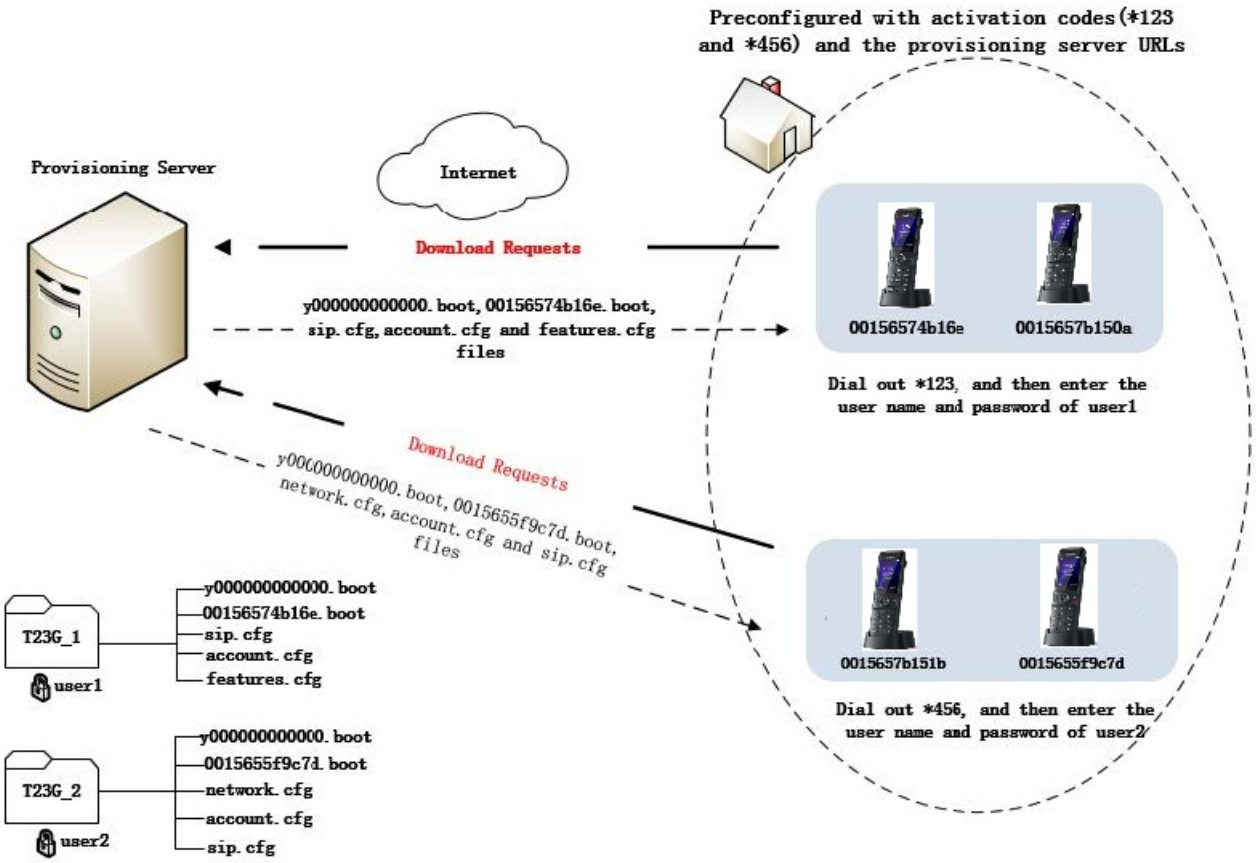
SIP NOTIFY Message

The IP phone will perform auto provisioning when receiving a SIP NOTIFY message which contains the header "Event: check-sync". Whether the IP phone reboots or not depends on the value of the parameter `sip.notify_reboot_enable`. If the value is set to 1, or the value is set to 0 and the header of the SIP NOTIFY message contains an additional string "reboot=true", the IP phone will reboot immediately.
For more information on the parameter `sip.notify_reboot_enable`, refer to the latest IP Phones Description of Configuration Parameters in CFG Files or Administrator Guide for your phone on Yealink Technical Support. This method requires server support.
The following figure shows the message flow:



Auto Provisioning via Activation Code

In addition to the updating modes introduced above, users can trigger IP phones to perform auto provisioning by dialing an activation code. To use this method, the activation code and the provisioning server URL need to be pre-configured on the IP phones. This method works only if there is no registered account on the IP phone. It is usually used for IP phones distributed by retail sales. It has the advantage that the IP phones do not need to be handled (for example, registering an account) before sending them to end-users.



The following lists the processes for triggering auto provisioning via activation code:

1. Create multiple directories on the provisioning server.
2. Store boot files and configuration files to each directory on the provisioning server.
3. Configure a username and password for each directory on the provisioning server.

   The user name and password provide a means of conveniently partitioning the boot files and configuration files for different IP phones. To access the specified directory, you need to provide the correct username and password configured for the directory.
4. Configure unique activation codes and the provisioning server URLs on IP phones.
   The activation code can be numeric characters, special characters "#", "*" or a combination of them within 32 characters.
   The following are example configurations in the configuration file for IP phones:

   ```
   static.autoprovision.1.code = *123
   static.autoprovision.1.url = http://192.168.1.30/AX83H_1/
   static.autoprovision.2.code = *456
   static.autoprovision.2.url = http://192.168.1.30/AX83H_2/
   ```
5. Send the specified activation code, associated user name, and password to each end-user.
6. The user can set up the phone, and then input the activation code (for example, *123) after the phone startup.
7. Press the **OK** soft key to trigger the IP phone to perform auto provisioning.
8. Enter the user name and password in the User Name and Password field respectively.

9. The entered user name and password must correspond to the directory where the boot files and configuration files of the IP phone are located. If you enter an invalid username or password, the LCD screen will prompt the message "Wrong username or password!".

   The prompt message will disappear in two seconds, and the LCD screen will return to the idle screen. You need to input the activation code again to trigger auto provisioning.

   The IP phone downloads the specified configuration files in sequence in boot files from the provisioning server to complete phone configurations. For more information on boot files and configuration files, refer to Manage Boot Files and Manage Configuration Files .

   The entered user name and password will be saved to the IP phone for the next auto provisioning.

The LCD screen will not prompt for user name and password if the provisioning server does not require authentication or the user name and password are already saved on the IP phone.
The following parameters are used to configure the auto provisioning via the activation code method (X ranges from 1 to 50):

```
#(Optional.) Configure the code name for triggering auto provisioning.
```

static.autoprovision.X.name

```
#Configure the activation code.
```

static.autoprovision.X.code

```
#Configure the URL of the provisioning server.
```

static.autoprovision.X.url

```
#Configure the username and password for downloading boot files and configuration files. If configured, the LCD screen wi
```

static.autoprovision.X.user
static.autoprovision.X.password

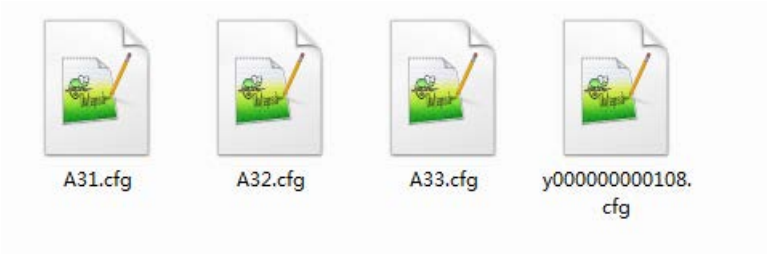
Auto Provisioning via PIN Code

After the phone is powered on and connected to the network, users can trigger it to perform an auto provisioning by entering the PIN code. The phone will download the corresponding PIN CFG file according to the PIN code.
The following lists the processes for triggering auto provisioning via PIN code:

1. Prepare the common CFG file and PIN CFG files in your local system.

   Example:

   Common CFG file: y000000000108.cfg
   PIN CFG files: A31.cfg, A32.cfg, and A33.cfg.



2. Place the common CFG file and PIN CFG files on the provisioning server.
3. Set the valid value for the following configuration parameter in the common CFG file.

   `static.custom_mac_cfg.url = http://<serverIPaddress>/$pin.cfg`

   Example:

   `static.custom_mac_cfg.url = http://10.2.11.101/$pin.cfg`

4. Specify the provisioning server URL (for example, http://10.2.11.101/) for the DHCP option or PnP server.
5. After the phone is powered on and connected to the network, users enter the corresponding PIN code (for example, A31).

The phone downloads the specified configuration file (for example, A31.cfg) from the provisioning server to complete phone configurations.

Download and Verify Configurations

Download Boot, Configuration and Resource Files

After obtaining the provisioning server address in one of the ways introduced above, the phone will request to download the boot files and configuration files from the provisioning server when it is triggered to perform auto provisioning.
The phone will try to download the MAC-Oriented boot file firstly and then download the configuration files referenced in the MAC-Oriented boot file from the provisioning server during the auto provisioning. If no MAC-Oriented boot file is found, the phone will try to download the common boot file and then download the configuration files referenced in the common boot file. If no common boot file is found, the IP phone will try to download the Common CFG file firstly, and then try to download the MAC-Oriented CFG file from the provisioning server – that is, the old mechanism for auto provisioning.
For more information about auto provisioning, refer to Provision Yealink Phones .

If the access URLs of the resource files have been specified in the configuration files, the phone will try to download the resource files.xt

Resolve and Update Configurations

After downloading, the phone resolves the configuration files and resource files (if specified in the configuration files), and then updates the configurations and resource files to the phone flash. Generally, updated configurations will automatically take effect after auto provisioning is completed. For the update of some specific configurations which require a reboot before taking effect, for example, network configurations, the IP phone will reboot to make the configurations effective after auto provisioning is completed.
The phone calculates the MD5 values of the downloaded files before updating them. If the MD5 values of the Common and MAC-Oriented configuration files are the same as those of the last downloaded configuration files, this means these two configuration files on the provisioning server are not changed. The IP phone will complete the auto provisioning without a repeated update. This is used to avoid unnecessary restart and the impact of phone use. On the contrary, the phone will update configurations.
The latest values to be applied to the IP phone are the values that take effect.
The phone only reboots when there is at least a specific configuration requiring a reboot after auto provisioning. If you want to force the IP phone to perform a reboot after auto provisioning, you can configure `static.auto_provision.reboot_force.enable = 1` in the configuration file.
For more information on the specific configurations which require a reboot during auto provisioning and the parameter `static.auto_provision.reboot_force.enable`, refer to the latest IP Phones Description of Configuration Parameters in CFG Files for your phone on Yealink Technical Support.
If configuration files have been AES encrypted, the IP phone will use the Common AES key to decrypt the Common CFG file and the MAC-Oriented AES key to decrypt the `<MAC>.cfg` file after downloading the configuration files. For more information on how the IP phone decrypts configuration files, refer to Yealink Configuration Encryption Tool User Guide.

Use MAC-local CFG File

Upload and download the `<MAC>-local.cfg` file
You can configure whether the IP phone uploads the `<MAC>-local.cfg` file to the provisioning server (or a specified URL configured by `static.auto_provision.custom.sync.path`) once the file changes for backing up this file, and downloads the `<MAC>-local.cfg` file from the provisioning server (or a specified URL configured by `static.auto_provision.custom.sync.path`) during auto provisioning to override the one stored on the phone. This process is controlled by the value of the parameter `static.auto_provision.custom.sync`.
Update configurations in the `<MAC>-local.cfg` file
You can configure whether the IP phone updates configurations in the `<MAC>-local.cfg` file during auto provisioning. This process is controlled by the value of the parameter `static.auto_provision.custom.protect`. If the IP phone is configured to keep the user' s personalized settings (by setting the value of the parameter `static.auto_provision.custom.protect` to 1), it will update configurations in the `<MAC>-local.cfg` file. If the value of the parameter `overwrite_mode` is set to 1 in the boot file, the phone updates configurations in the `<MAC>-local.cfg` file downloaded from the server; if the value of the parameter `overwrite_mode` is set to 0, the phone updates configurations in the `<MAC>-local.cfg` file stored on `the` phone.
The IP phone updates configuration files during auto provisioning in sequence: CFG files referenced in the boot

file>MAC-local CFG file (if no boot file is found, Common CFG file>MAC-Oriented CFG file>MAC-local CFG file). The configurations in the <MAC>-local.cfg file take precedence over the ones in other downloaded configuration files. As a result, the personalized settings of the phone configured via the phone or web user interface can be kept after auto provisioning.

ⓘ NOTE

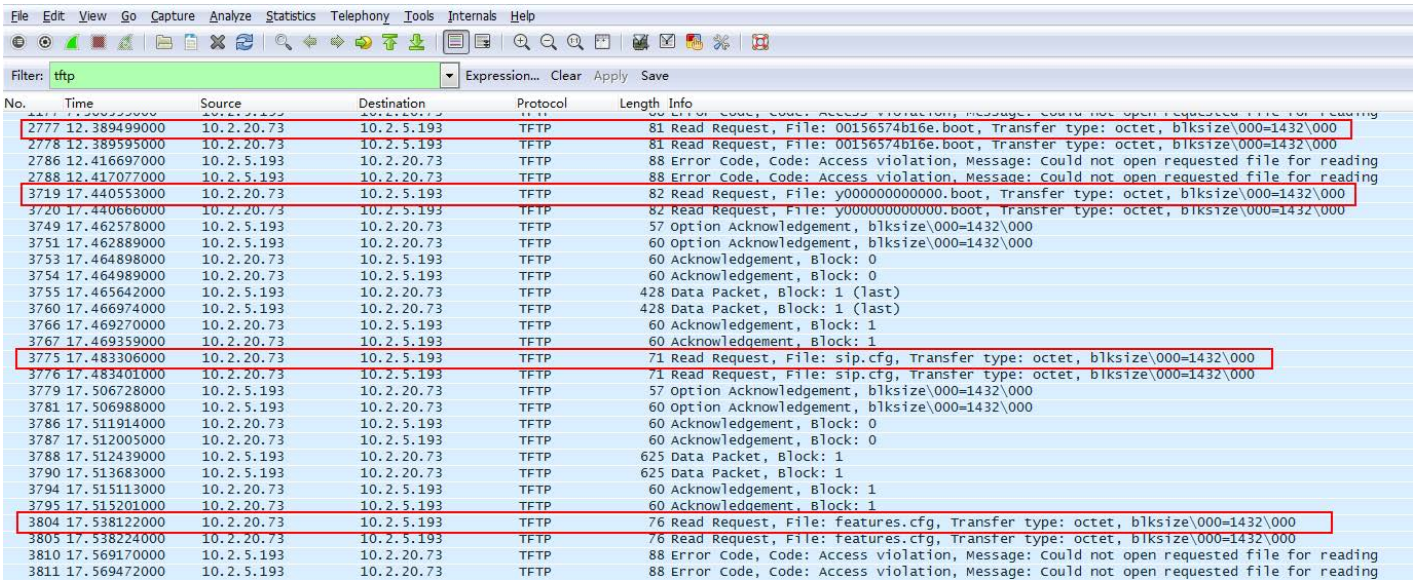
Note that if the personalized settings are static settings, they cannot be kept after auto provisioning because the static settings will never be saved in the <MAC>-local.cfg file.

For more information, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

Verify Configurations

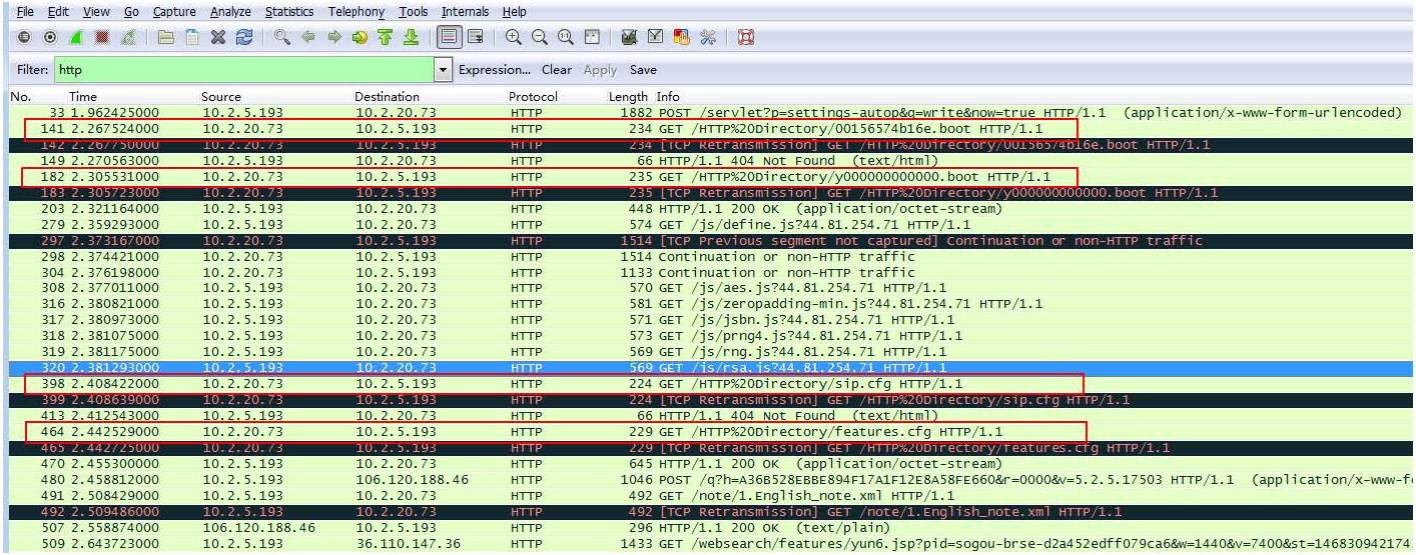
After auto provisioning, you can then verify the update via phone user interface or web user interface of the phone. During auto provisioning, you can monitor the downloading requests and response messages by a WinPcap tool. The following shows some examples.

Example 1: Yealink SIP-T23G IP phone downloads the boot file and configuration files from the TFTP server.



Example 2: Yealink SIP-T23G IP phone downloads the boot file and configuration files from the FTP server.

Example 3: Yealink SIP-T23G IP phone downloads boot file and configuration files from the HTTP server.



Troubleshooting

This chapter provides general troubleshooting information to help you solve problems you might encounter when deploying phones.

If you require additional information or assistance with the deployment, contact your system administrator.

Why does the phone fail to download configuration files?

- Ensure that the auto provisioning feature is configured properly.
- Ensure that the provisioning server and network are reachable.
- Ensure that authentication credentials configured on the phone are correct.
- Ensure that configuration files exist on the provisioning server.

- Ensure that MAC-Oriented boot file and common boot file don't exist simultaneously on the provisioning server. If both exist, the phone only downloads MAC-Oriented boot file and the configuration files referenced in the MAC-Oriented boot file.

Why does the phone fail to authenticate the provisioning server during auto provisioning?

Ensure that the certificate for the provisioning server has been uploaded to the phone's trusted certificates list. If not, do one of the following:

- Import the certificate for the provisioning server to the phone's trusted certificates list (at phone's web path **Security** > **Trusted Certificates** > **Import Trusted Certificates**).
- Disable the phone to only trust the server certificates in the trusted certificates list (at phone's web path **Security** > **Trusted Certificates** > **Only Accept Trusted Certificates**).

Why does the provisioning server return HTTP 404?

- Ensure that the provisioning server is properly set up.
- Ensure that the access URL is correct.
- Ensure that the requested files exist on the provisioning server.

Why does the phone display "Network unavailable"?

- Ensure that the Ethernet cable is plugged into the Internet port on the phone and the Ethernet cable is not loose.
- Ensure that the switch or hub in your network is operational.
- Ensure that the configurations of the network are properly set in the configuration file

Why is the permission denied when uploading files to the root directory of the FTP server?

- Ensure that the complete path to the root directory of the FTP server is authorized.
- Check security permissions on the root directory of the FTP server, if necessary, change the permissions.

Why doesn't the phone obtain the IP address from the DHCP server?

- Ensure that settings are correct on the DHCP server.
- Ensure that the phone is configured to obtain the IP address from the DHCP server

Why doesn't the phone download the ring tone?

- Ensure that the file format of the ring tone is *.wav.
- Ensure that the size of the ring tone file is not larger than that the phone supports.
- Ensure that the properties of the ring tone for the phone are correct.
- Ensure that the network is available and the root directory is right for downloading.
- Ensure that the ring tone file exists on the provisioning server.

Why doesn't the phone update configurations?

- Ensure that the configuration files are different from the last ones.
- Ensure that the phone has downloaded the configuration files.
- Ensure that the parameters are correctly set in the configuration files.
- Ensure that the value of the parameter "static.auto_provision.custom.protect" is set to 0. If it is set to 1, the provisioning priority is shown as follows: phone/web user interface >central provisioning >factory defaults. A setting you make using a lower-priority method does not apply to or override a duplicate setting made using a higher-priority method.

For more information, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

Glossary

MAC Address

A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment.

MD5

The MD5 Message-Digest Algorithm is a widely used as a cryptographic hash function that produces a 128-bit (16-byte) hash value.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network configuration protocol for hosts on Internet Protocol (IP) networks. Computers that are connected to IP networks must be configured before they can communicate with other hosts.

FTP

File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet. It is often used to upload web pages and other documents from a private development machine to a public web-hosting server.

HTTP

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a combination of Hypertext Transfer Protocol (HTTP) with SSL/TLS protocol. It provides encrypted communication and secure identification of a network web server.

TFTP

Trivial File Transfer Protocol (TFTP) is a simple protocol to transfer files. It has been implemented on top of the User Datagram Protocol (UDP) using port number 69.

AES

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data.

URL

A uniform resource locator or universal resource locator (URL) is a specific character string that constitutes a reference to an Internet resource.

XML

Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

Appendix

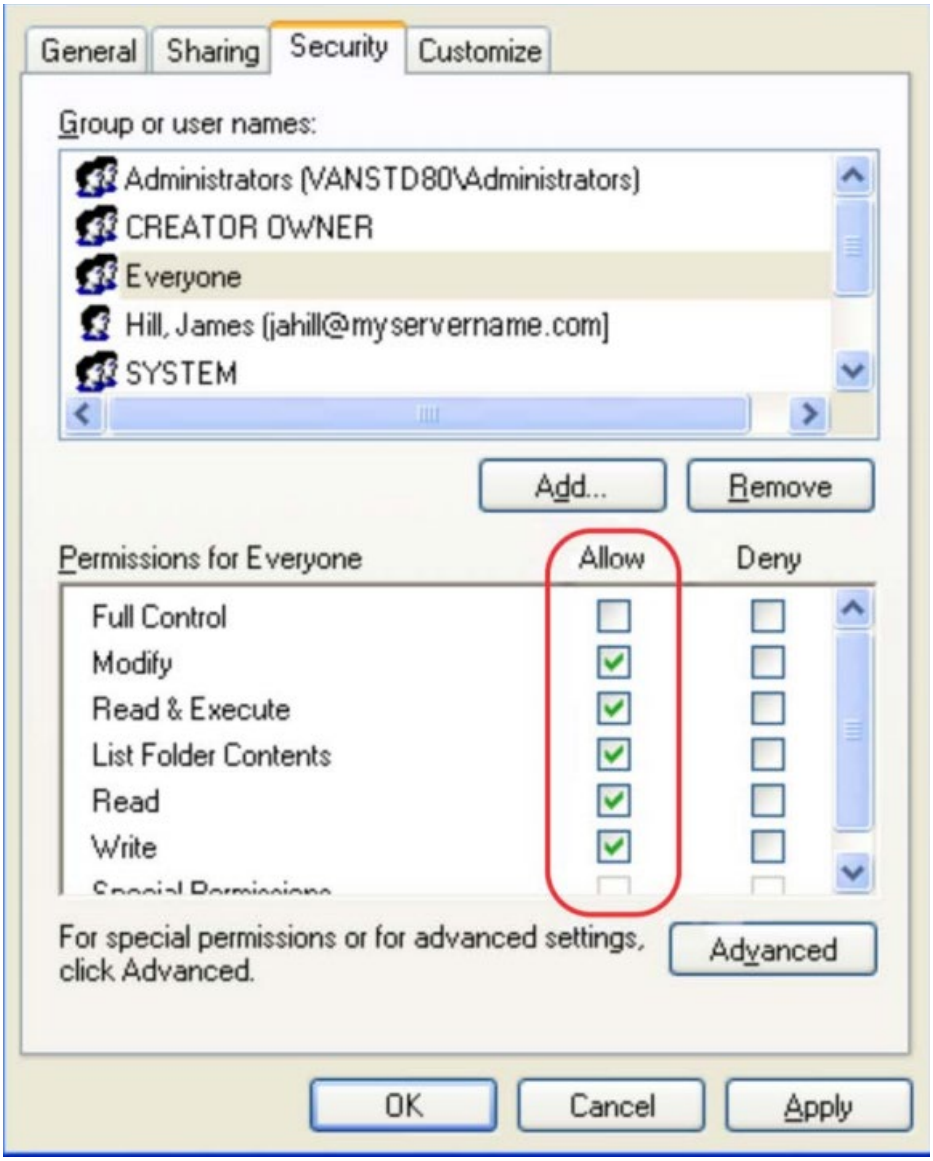
Configure FTP Server

Wftpd and FileZilla are free FTP application software for Windows. This section mainly provides instructions on how to configure an FTP server using wftpd for Windows. You can download wftpd online: http://www.wftpd.com/products/products.html or FileZilla online: https://filezilla-project.org.
We recommend that you use vsftpd as an FTP server for Linux platform if required.

Prepare a Root Directory

To prepare a root directory:

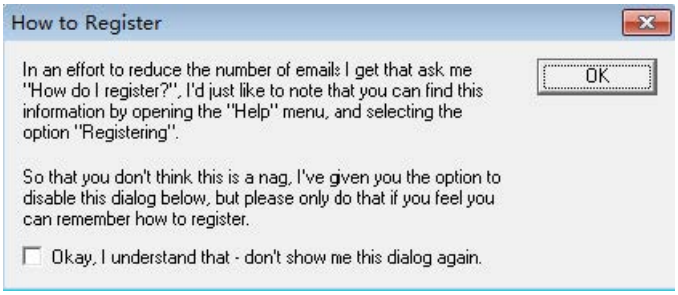
1. Create an FTP root directory on the local system (for example, D:\FTP Directory).
2. Place the boot files and configuration files to this root directory.
3. Set the security permissions for the FTP directory folder.
   You need to define a user or group name, and set the permissions: read, write, and modify. Security permissions vary by organizations.
   An example of configuration on the Windows platform is shown as below:



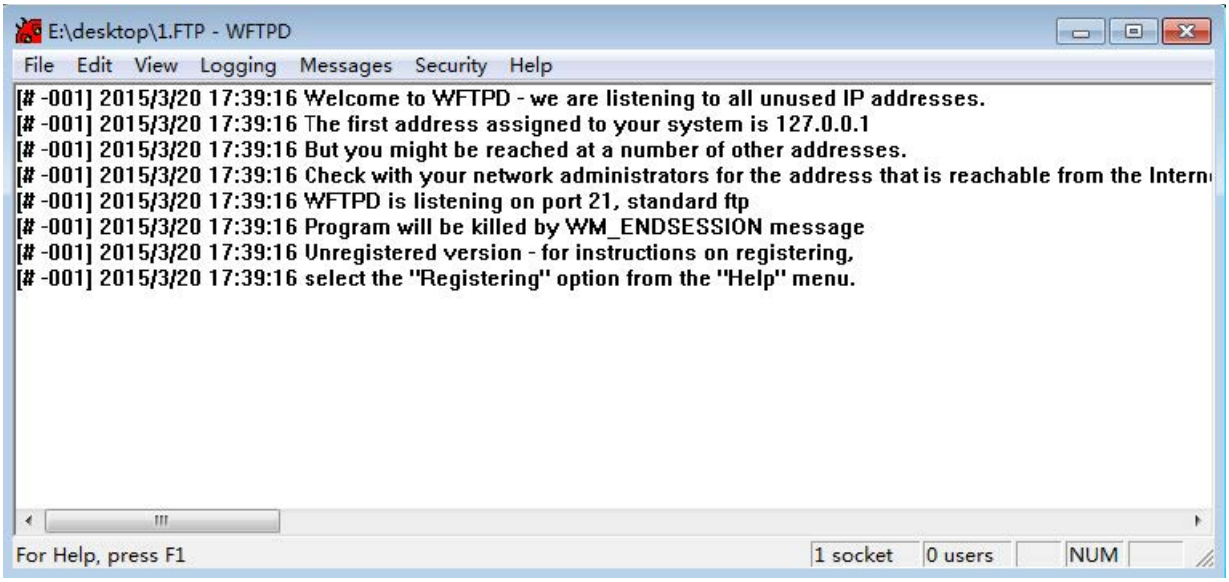
Configure an FTP Server

To configure a wftpd server:

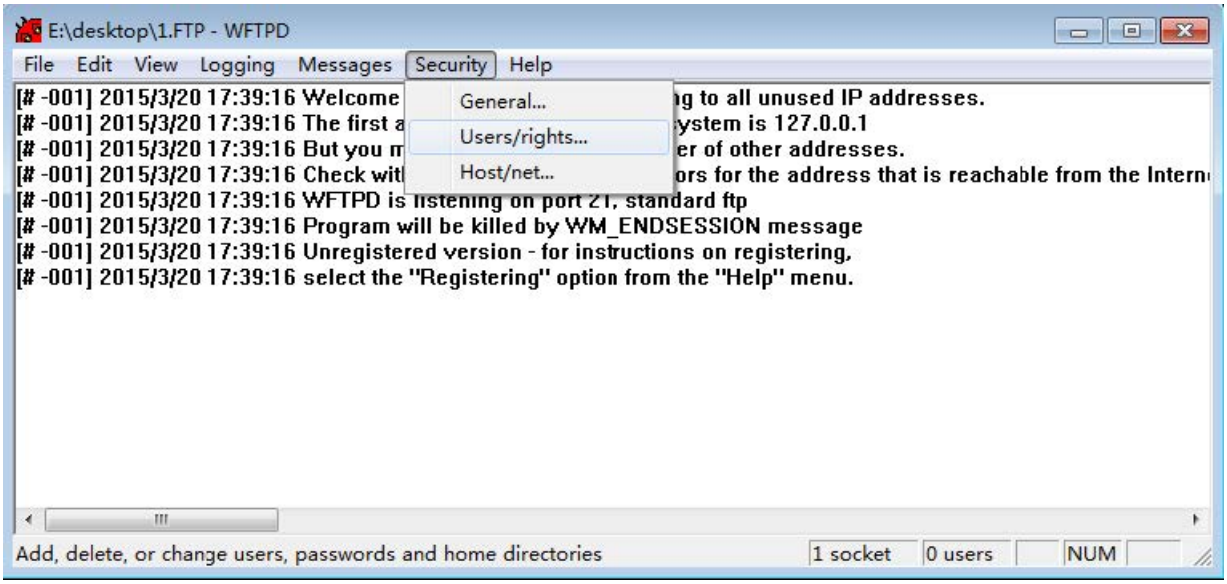
1. Download the compressed file of the wftpd application to your local directory and extract it.
2. Double click the **Wftpd.exe**.
   The dialogue box of how to register is shown as below:



3. Check the check box and click **OK** in the pop-up box.
   The log file of the wftpd application is shown as below:

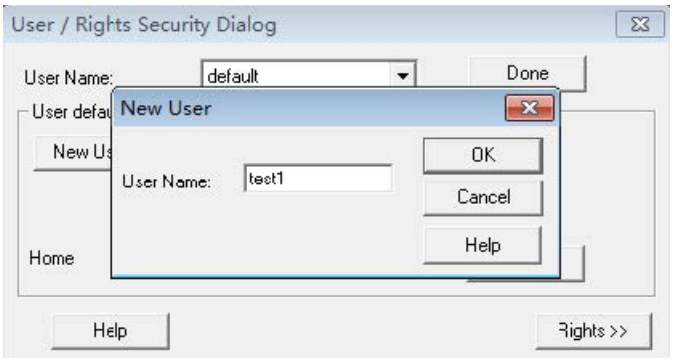


4. Click **Security** > **Users/rights**.



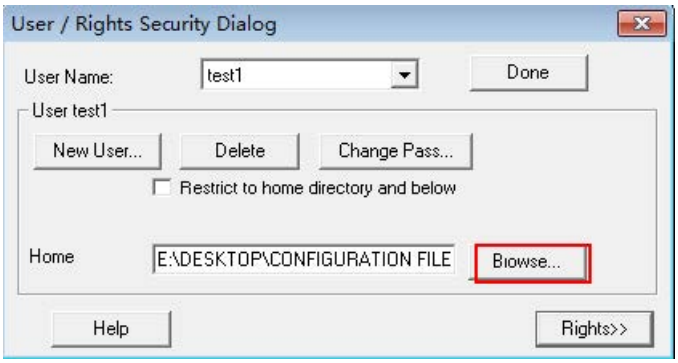
5. Click **New User**.

6. Enter a user name (for example, test1) in the **User Name** field and then click **OK**.



7. Enter the password of the user (for example, test1) created above in the **New Password** and **Verify Password** field respectively, and then click **OK**.

8. Click **Browse** to locate the FTP root directory in your local system.



9. Click **Rights>>** and assign the desired permission for the user (for example, test1) created above.
10. Check the check boxes of **Read, Create Files/Dirs, List Directories** and **Overwrite/Delete** to make sure the FTP user has the read and write permission.

11. Click **Done** to save the settings and finish the configurations.

The server URL "ftp://username:password@IP/" (Here "IP" means the IP address of the provisioning server, "username" and "password" are the authentication for FTP download. For example, "ftp://test1:123456@10.3.6.234/") is where the IP phone downloads boot files and configuration files from.

Before configuring a wftpd server, ensure that no other FTP servers exist in your local system.

Configure HTTP Server

This section provides instructions on how to configure an HTTP server using HFS tool. You can download the HFS software online: http://www.snapfiles.com/get/hfs.html.

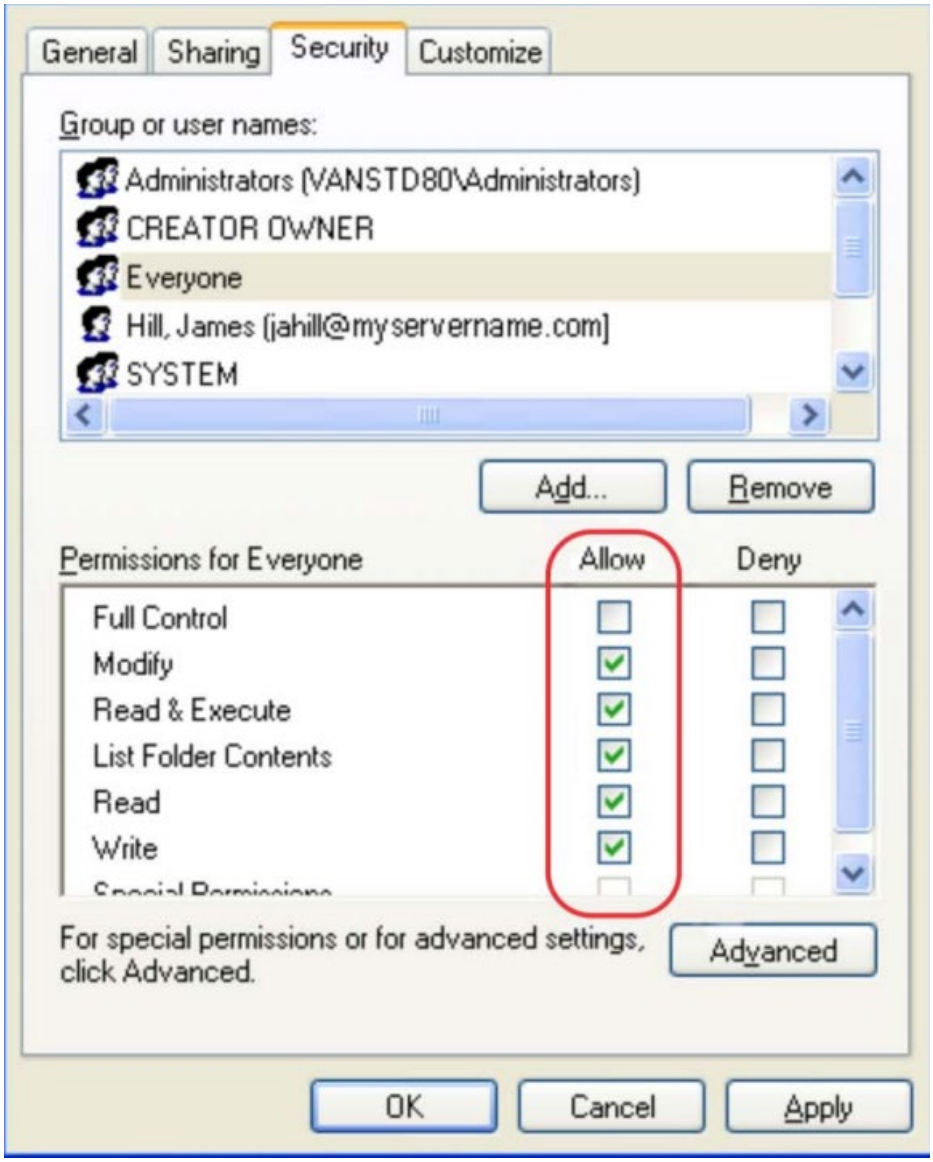
Prepare a Root Directory

To prepare a root directory:

1. Create an HTTP root directory on the local system (for example, D:\HTTP Directory).
2. Place the boot files and configuration files to this root directory.

3. Set the security permissions for the HTTP directory folder.

   You need to define a user or group name and set the permissions: read, write, and modify. Security permissions vary by organizations.
   An example of configuration on the Windows platform is shown as below:



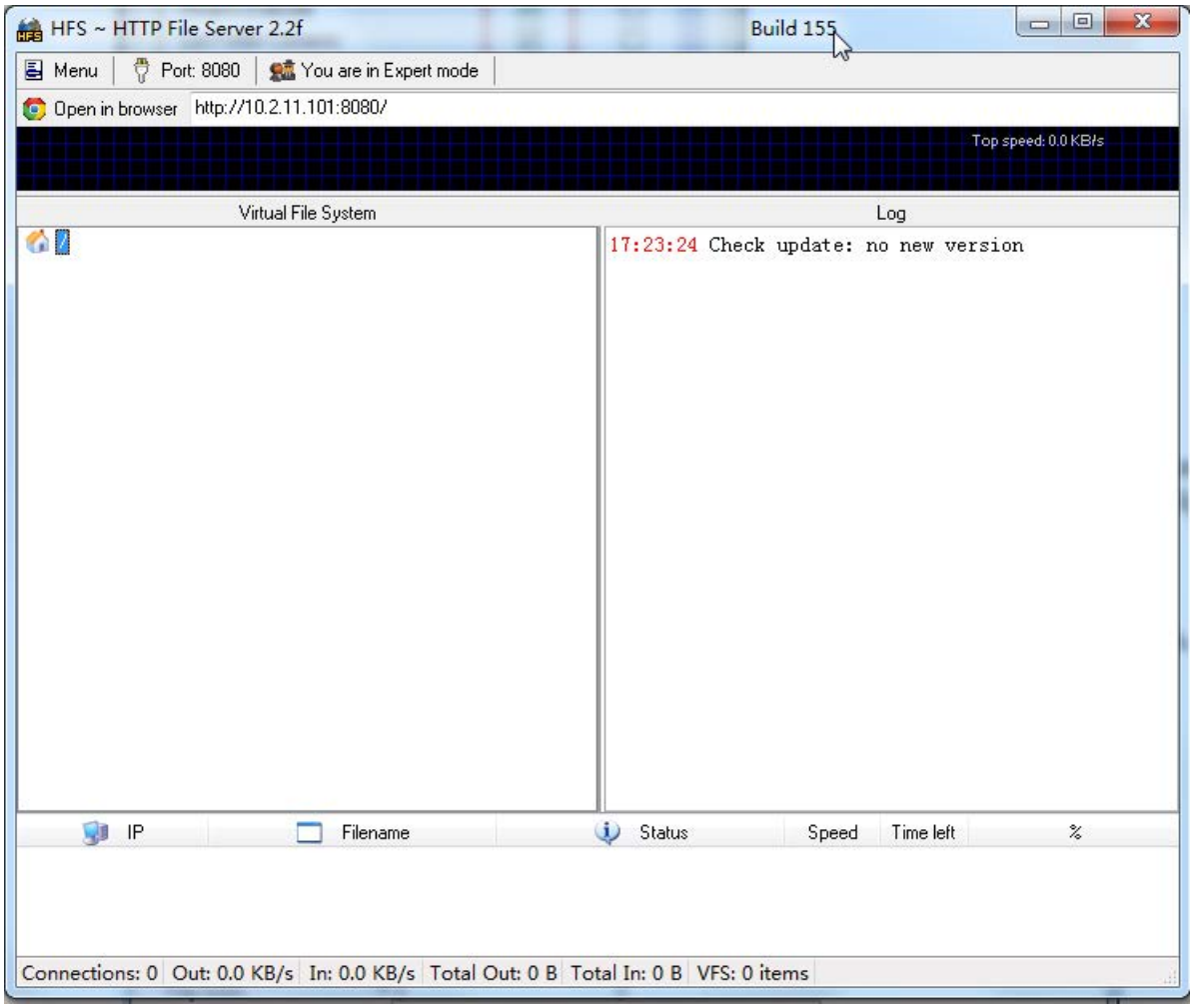
Configure an HTTP Server

HFS tool is an executable application, so you don’ t need to install it.

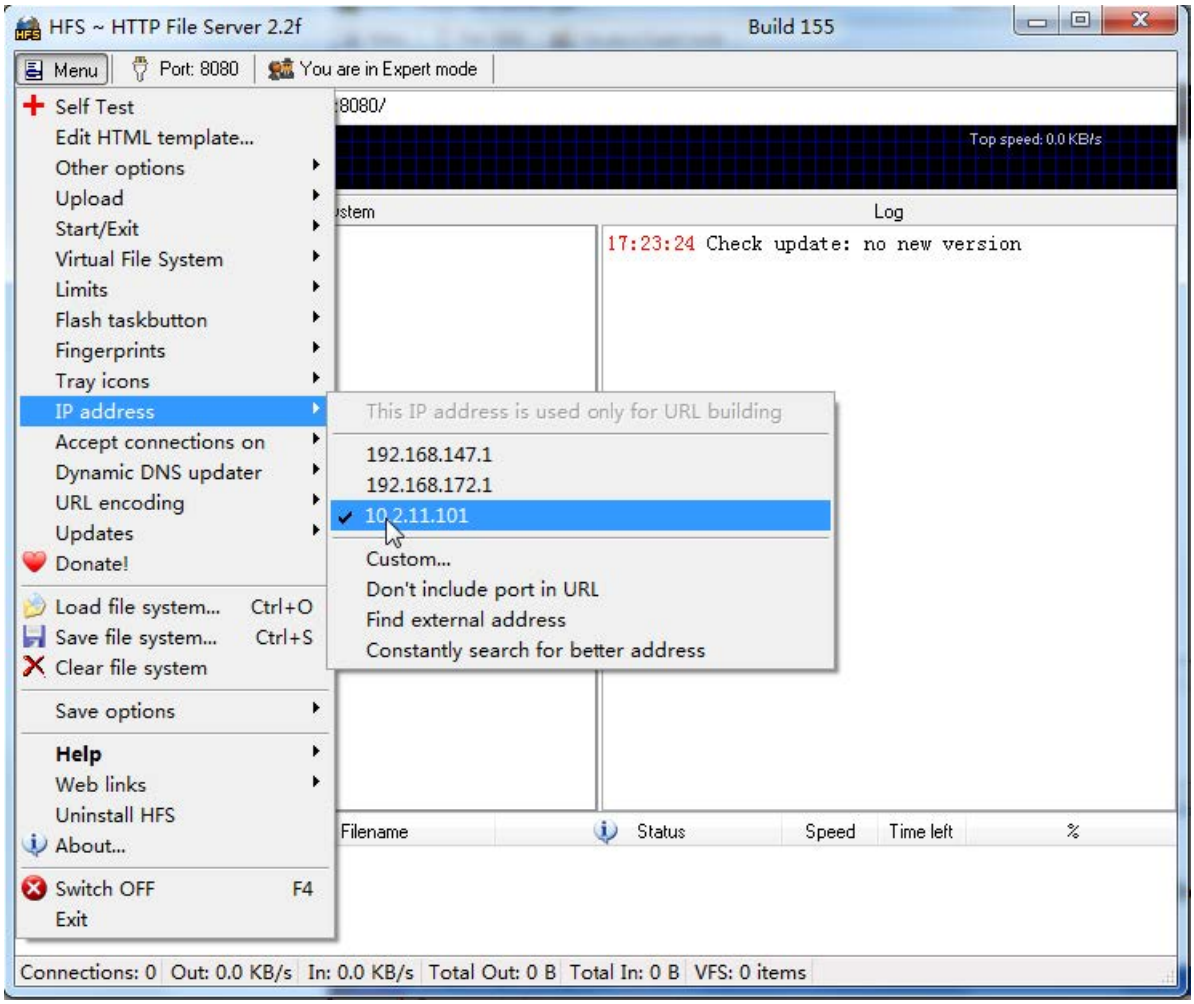
To configure an HTTP server:

1. Download the application file to your local directory, double click the **hfs.exe**.

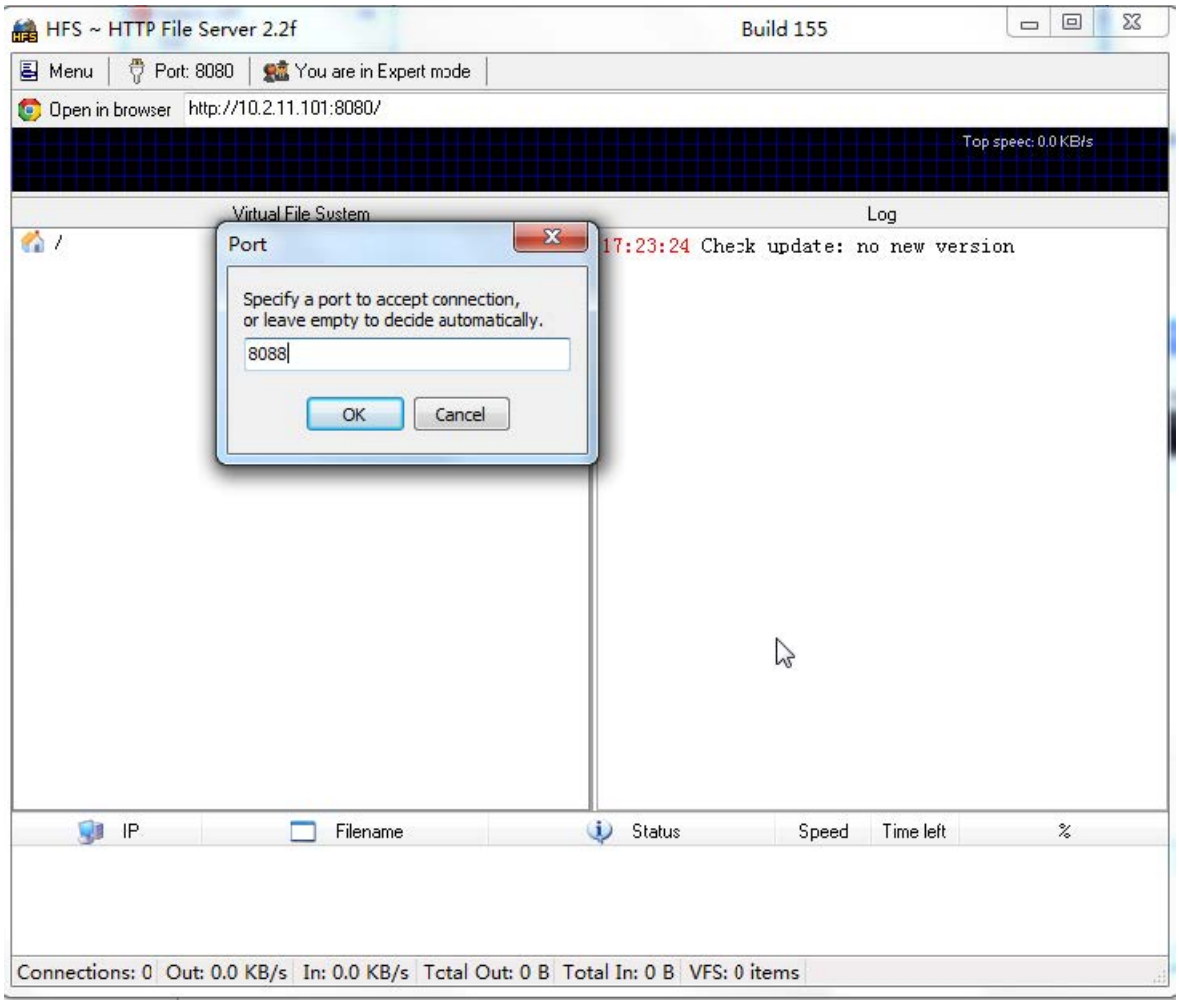
   The main configuration page is shown as below:



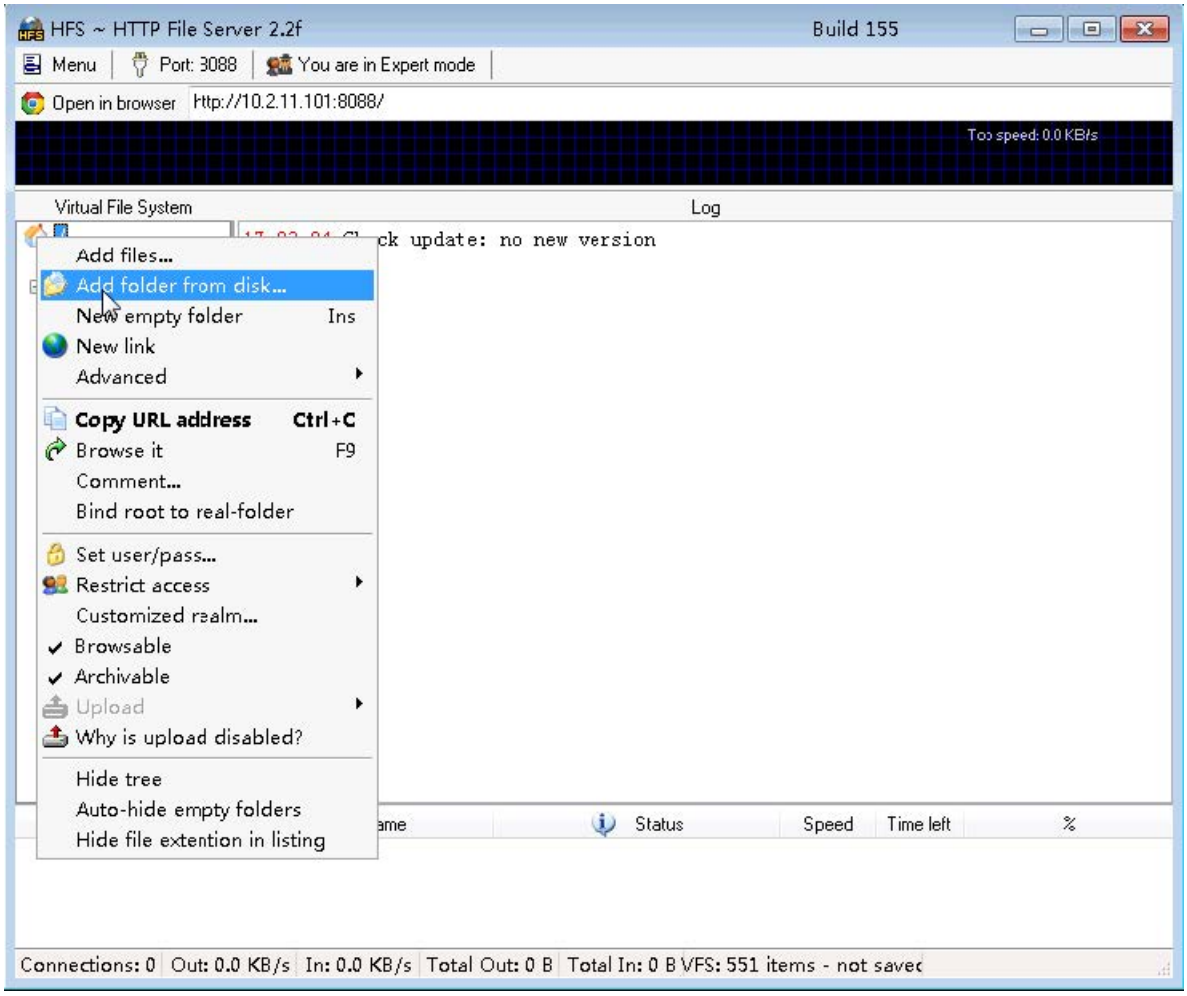
2. Click **Menu** in the main page and select the IP address of the PC from **IP address**.



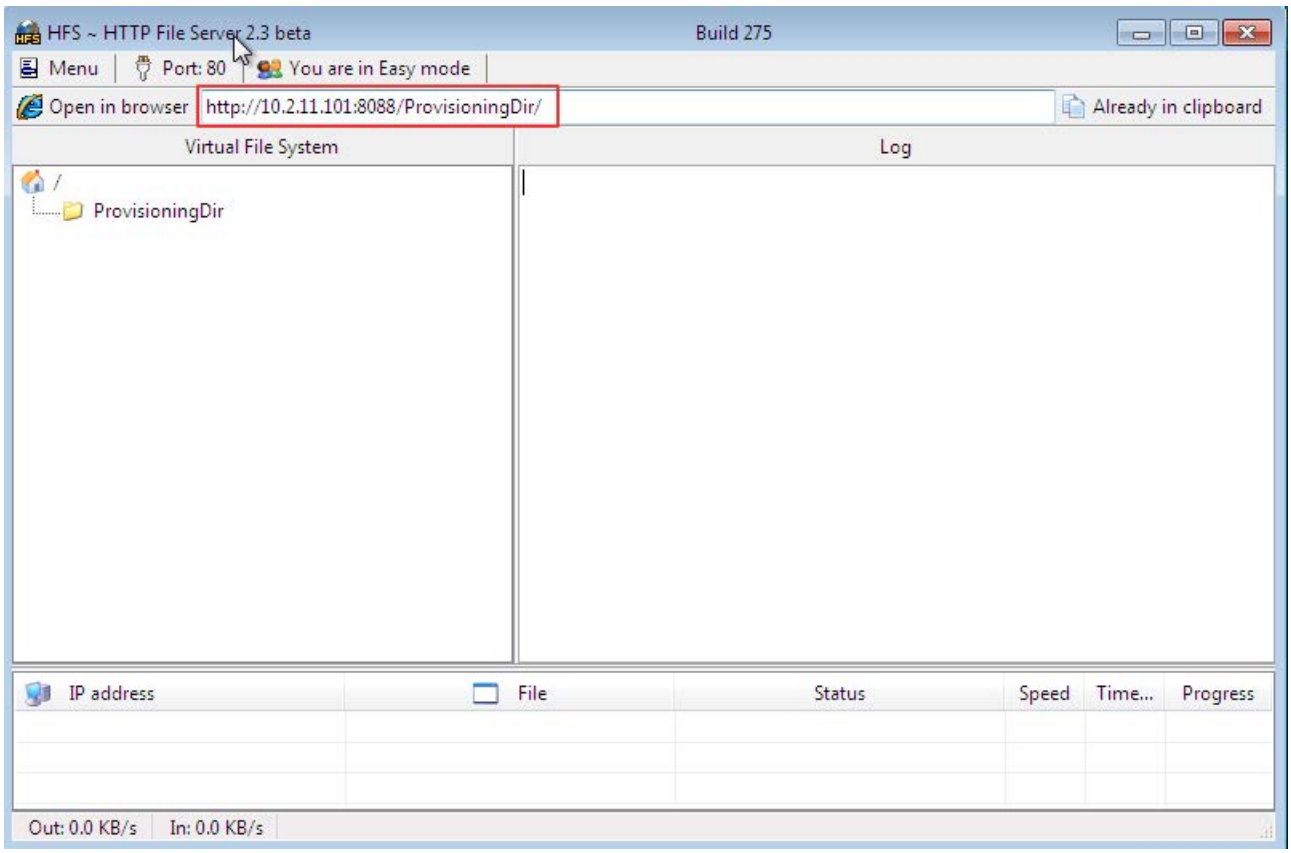
The default HTTP port is **8080**. You can also reset the HTTP port (make sure there is no port conflict).


HFS ~ HTTP File Server 2.2f
Build 155
Menu
Port: 8080
You are in Expert mode
Open in browser
http://10.2.11.101:8080/
Top speed: 0.0 KB/s
Virtual File System
Log
/
17:23:24 Check update: no new version
Port
Specify a port to accept connection,
or leave empty to decide automatically.
8088
OK
Cancel
IP
Filename
Status
Speed
Time left
%
Connections: 0
Out: 0.0 KB/s
In: 0.0 KB/s
Total Out: 0 B
Total In: 0 B
VFS: 0 items

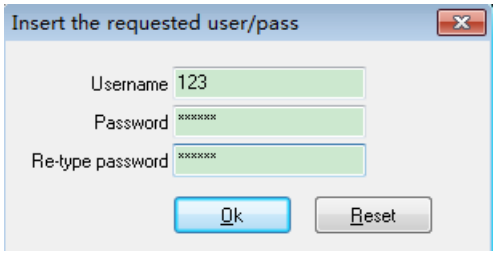
3. Right click the icon on the left of the main page, select Add folder from disk to add the HTTP Server root directory.



4. Locate the root directory from your local system.



5. Check the server URL (for example, http://10.2.11.101:8088/ProvisioningDir) by clicking "**Open in browser**".
6. (Optional.) Right-click the root directory name (for example, ProvisioningDir), and then select **Set user/pass…**.
7. (Optional.) Enter the desired user name and password for the root directory in the corresponding fields and then click **OK**.



Yealink IP phones also support the Hypertext Transfer Protocol with SSL/TLS (HTTPS) protocol for auto provisioning. HTTPS protocol provides encrypted communication and secure identification. For more information on installing and configuring an Apache HTTPS Server, refer to the network resource.

Phone Customization

Language

Supported Languages

Yealink phones support multiple languages. Languages used on the phone user interface and web user interface can be specified respectively as required.
You can ask the distributor or Yealink FAE for language packs. You can also refer to the following template.
User interface template:

```
[ Lang ]

"<New Item>" = "<New Item>"
"1.Confirm that USB device is compliant with USB 2.0." = "1.Confirm that USB device is compliant with USB 2.0."
"10min" = "10min"
"12 Hour" = "12 Hour"
"120s" = "120s"
"15s" = "15s"
"1h" = "1h"
"1min" = "1min"
"2.Try to replug the USB device." = "2.Try to replug the USB device."
"(Empty)" = "(Empty)"
```

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

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

Portuguese (Latin)	009.GUI.Portuguese_LA.lang	Turkish	10.Turkish.js	10.Turkish_note.xml
Spanish (EU)	010.GUI.Spanish.lang	Russian	11.Russian.js	11.Russian_note.xml
Spanish (Latin)	011.GUI.Spanish_LA.lang	Czech	12.Czechlang.js	12.Czechlang_note.xml
Turkish	012.GUI.Turkish.lang	Arabic	13.Arabic.js	13.Arabic_note.xml
Russian	013.GUI.Russian.lang			
Czech	014.GUI.Czechlang.lang			
Hebrew	015.GUI.Hebrew.lang			
Arabic	016.GUI.Arabic.lang			

Language Display Configuration

The default language displayed on the phone user interface is English. If your web browser displays a language not supported by the IP phone, the web user interface will display English by default. You can specify the languages for the phone user interface and web user interface respectively.
The following table lists the parameters you can use to configure the language display.

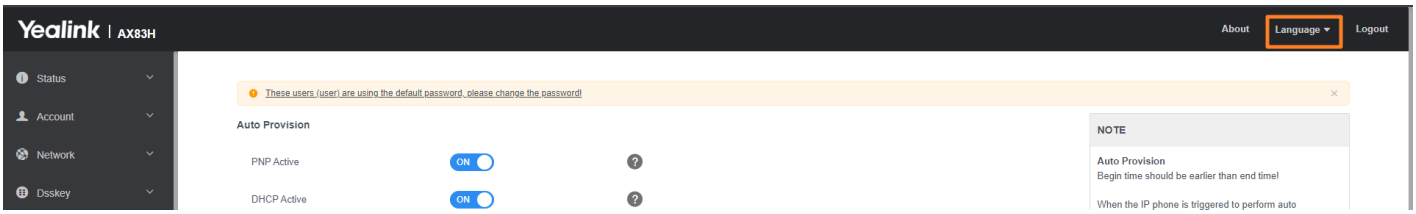
Configuration parameter

```
lang.gui
lang.wui
```

Parameter	Description	Permitted Values	Default	Web UI
lang.gui	It configures the language used on the phone user interface.	English, Chinese_S, Chinese_T, French_CA, French, German, Italian, Polish, Portuguese, Portuguese_LA, Spanish, Spanish_LA, Turkish, Russian, Czech, Arabic, Hebrew, or the custom language name.	English	/
lang.wui	It configures the language used on the web user interface.	English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian, Czech, Arabic, or the custom language name.	English	On the top-right corner of the web user interface

Set via the Web User Interface

On the top-right corner of the web user interface



Language for Phone Display Customization

You can customize the translation of the existing language on the phone user interface. Languages available for selection depend on language packs currently loaded to the IP phone. You can also add new languages (not included in the available language list) available for phone display by loading language packs to the IP phone.

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

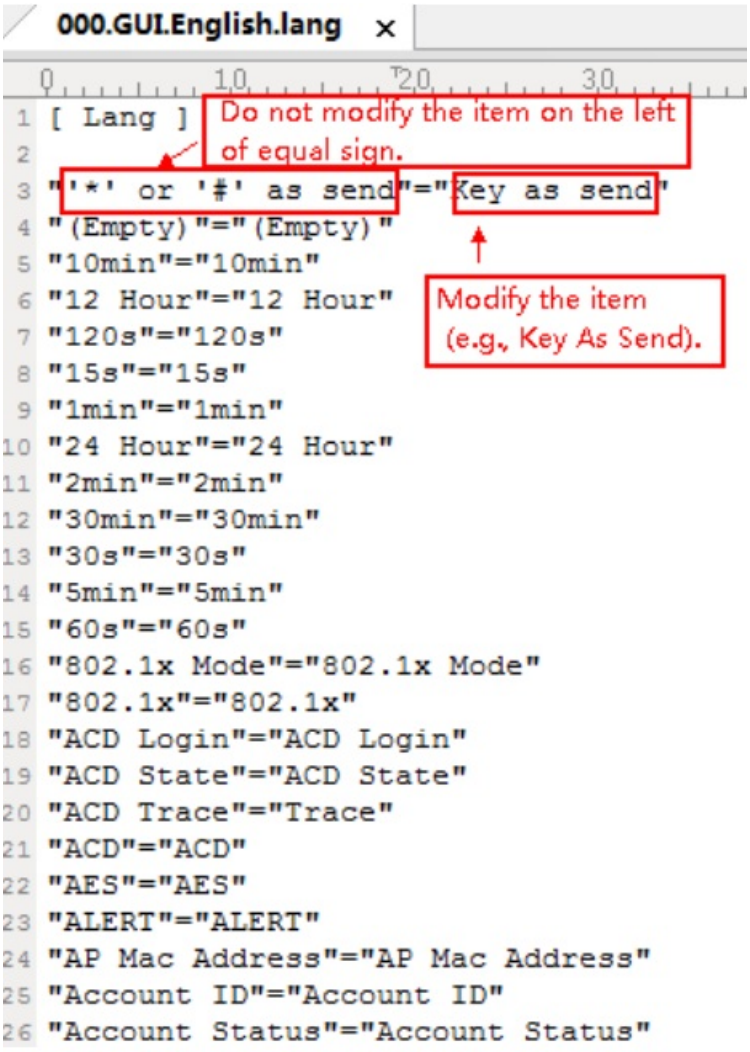
Customizing a Language Pack for Phone Display

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

NOTE
To modify the translation of an existing language, do not rename the language pack.

Procedure

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



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

Custom Language for Phone Display Configuration

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

configuration parameter

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

Parameter	Description	Permitted Values	Default
gui_lang.url	It configures the access URL of the custom LCD language pack for the phone user interface. Note: You can also download multiple language packs to the phone simultaneously.	URL within 511 characters	Blank

gui_lang.delete	It deletes the specified or all custom LCD language packs of the phone user interface.	For example http://localhost/all or http://localhost/X.GUI.name.lang X starts from 017, “name” is replaced with the language name.	Blank

Example: Setting a Custom Language for Phone Display

The following example shows the configuration for uploading custom language files “017.GUI.English_17.lang” and “018.GUI.English_18.lang”, and then specify “017.GUI.English_17.lang” to display on the phone user interface. These language files are customized and placed on the provisioning server “192.168.10.25”.

Example

gui_lang.url= http://192.168.10.25/017.GUI.English_17.lang
gui_lang.url= http://192.168.10.25/018.GUI.English_18.lang
lang.gui=English_17

After provisioning, text displayed on the phone user interface will change to the custom language you defined in “017.GUI.English_17.lang”. You can also find a new language selection “English_17” and “English_18” on the IP phone user interface: **Menu** > **Basic** > **Language or Menu** > **Settings** > **Basic Settings** > **Language**.

Language for Web Display Customization

You can customize the translation of the existing language on the web user interface. You can modify translation of an existing language or add a new language for web display. You can also customize the translation of the note language pack. The note information is displayed in the question mark "?" of the web user interface.

You can ask the distributor or Yealink FAE for language packs. You can also refer to the following template.

Web interface template:

```
var _objTrans =
{
"12-Hour" : "12 Heures",
"180 Ring Workaround" : "Contournement sonnerie 180",
"2 Chars" : "2 Chars",
"24-Hour" : "24 Heures",
"2N" : "2N",
"404 (Not Found)" : "404 (introuvable)",
"480 (Temporarily Unavailable)" : "480 (temporairement indisponible)",
"486 (Busy Here)" : "486 (occupé)",
"600 (Busy Everywhere)" : "600 (occupé partout)",
"603 (Decline)" : "603 (refus)",
"6s" : "6 s",

_END_TRANS:null
}
```

Customizing a Language Pack for Web Display

When you add a new language pack for the web user interface, the language pack must be formatted as

"X.name.js" (X starts from 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 file name of the new language pack should not be the same as the existing one.

NOTE
To modify the translation of an existing language, do not rename the language pack.

Procedure

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

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

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

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

Customizing a Language Pack for Note Display

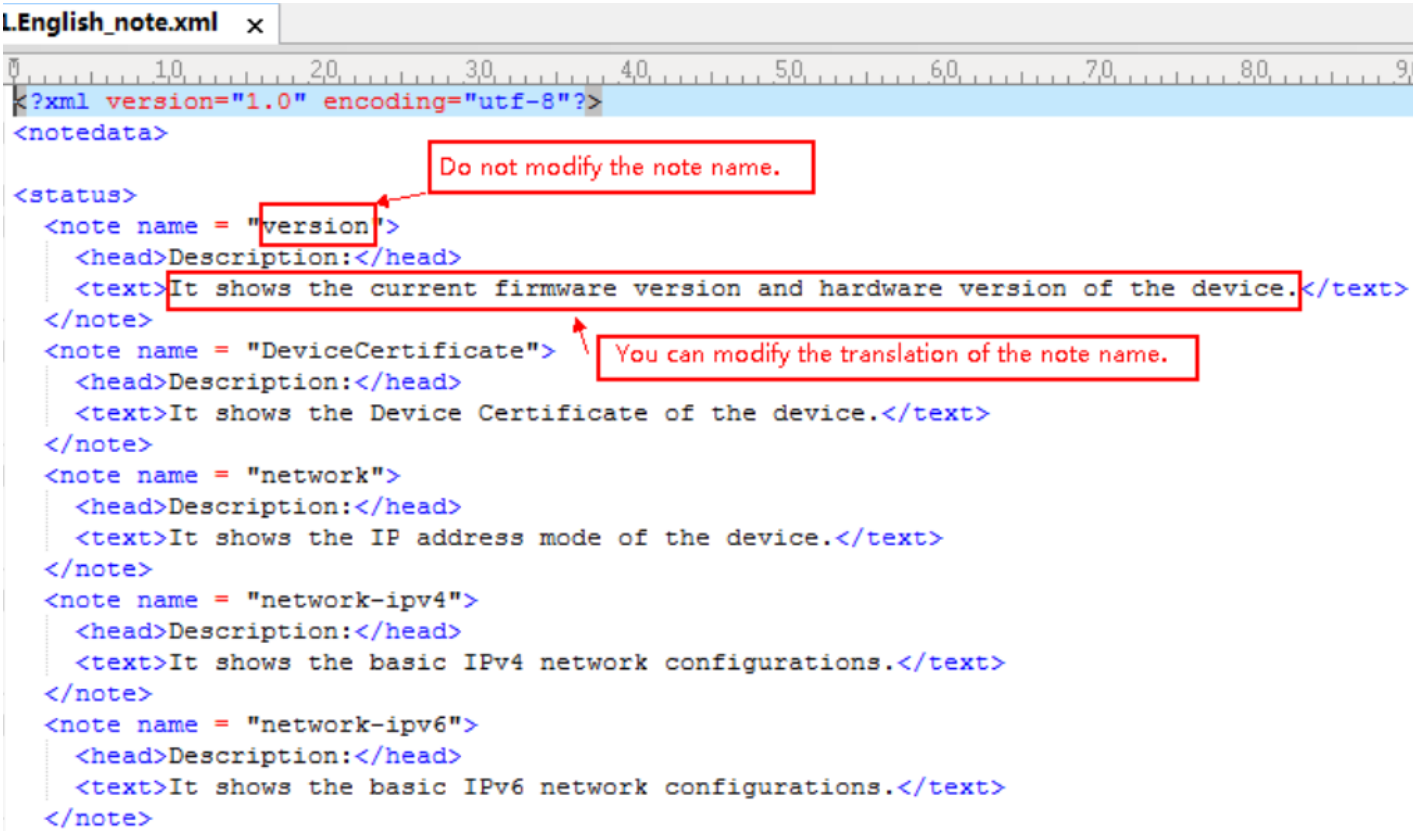
When you add a new language pack for the note, the note language pack must be formatted as "X.name_note.xml" (X starts from 14, "name" is replaced with the language name). If the note language name is the same as the existing one, the new uploaded note language pack will override the existing one. We recommend that the filename of the new note language pack should not be the same as the existing one.

Procedure

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

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:




```
<?xml version="1.0" encoding="utf-8"?>
<notedata>

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

Save the note 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 phones, prepare the language file named as "14.Wuilan.js" and "14.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 the new language is selected.

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

Configuration parameter

```
wui_lang.url
wui_lang_note.url
wui_lang.delete
```

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 For example http://localhost/X.GUI.name.lang X starts from 014, "name" is replaced with the language name	Blank
wui_lang_note.url	It configures the access URL of the custom note language pack for the web user interface.	URL within 511 characters For example http://localhost/X.name_note.xml X starts from 14, "name" is replaced with the language name	Blank
wui_lang.delete	It deletes the specified or all custom web language packs and note language packs of the web user interface.	http://localhost/all or http://localhost/Y.name.js Y starts from 014, "name" is replaced with the language name	Blank

Display

Backlight Setting

You can change the backlight brightness of the phone screen during phone activity and inactivity. The backlight brightness automatically changes when the phone is idle for a specified time.
You can change the screen backlight brightness and time in the following settings:
Active Level: The brightness level of the LCD screen when the phone is active. Digits (1-10) represent different brightness levels. 10 is the brightest level.
Inactive Level: The brightness of the LCD screen when the phone is inactive. You can select a low brightness or turn off the backlight.
Backlight Time: The delay time to change the brightness of the LCD screen when the phone is inactive. Backlight time includes the following settings you can choose from:

- Always On: Backlight is on permanently.
- Always Off: Backlight is off permanently. It is not available for the
- 15s, 30s, 1min, 2min, 5min, 10min, 30min, 1h, 2h, 4h, 6h, 8h, 12h, Backlight is changed when the phone is inactive after the designated time (in seconds).

Backlight and Time Configuration

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

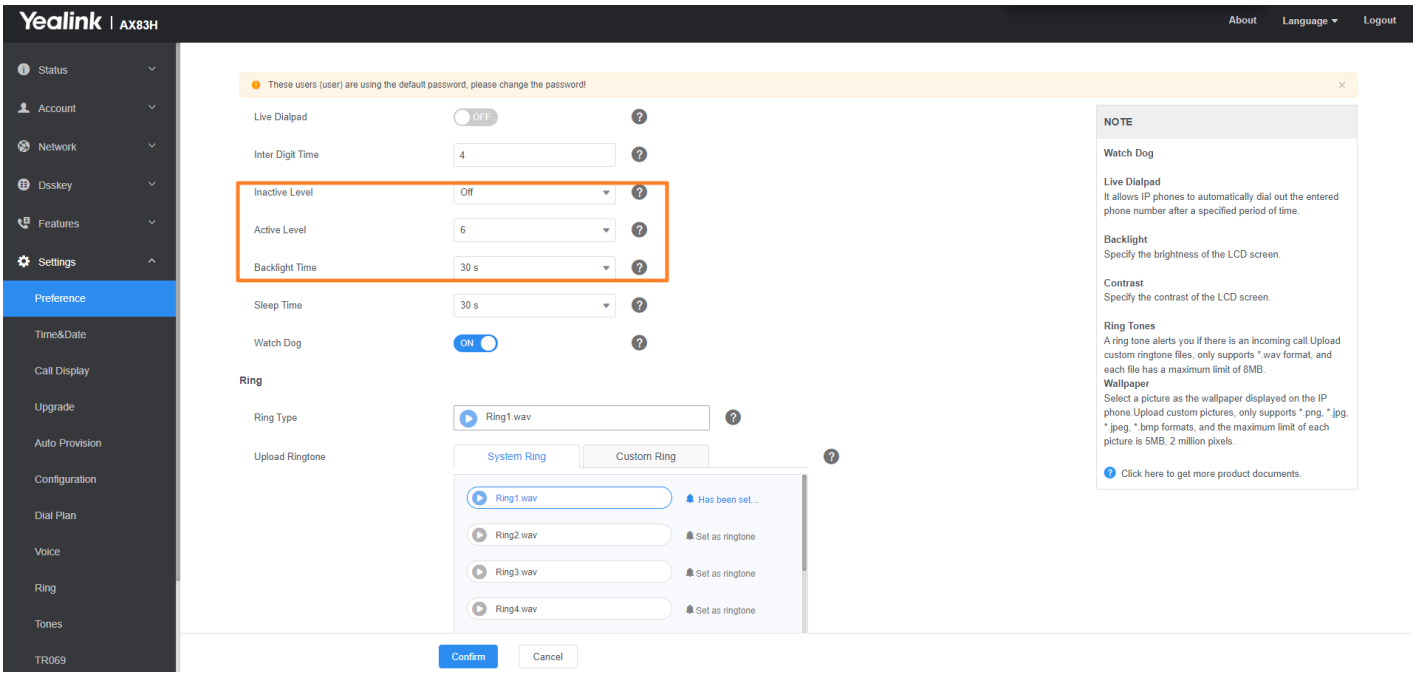
Configuration parameter

```
phone_setting.active_backlight_level
phone_setting.inactive_backlight_level
phone_setting.backlight_time
```

Parameter	Description	Permitted Values	Default
phone_setting.active_backlight_level	It configures the intensity of the LCD screen when the phone is active.	Integer from 1 to 10	8
phone_setting.inactive_backlight_level	It configures the intensity of the LCD screen when the phone is inactive.	0-Off, it works only if "phone_setting.backlight_time" is not set to 1 (Always On). 1-Low	1
phone_setting.backlight_time	It configures the delay time (in seconds) to change the intensity of the LCD screen when the phone is inactive.	0-Always On 15-15s 30-30s 60-1min 120-2min 300-5min 600-10min 1800-30min 3600-1h 7200-2h 14400-4h 21600-6h 28800-8h 43200-12h	

Set via the Web User Interface

On the web user interface, go to **Settings** > **Preference**



Time and Date

Time and Date

Yealink phones 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 Name	Time Zone	Time Zone Name
-12	Eniwetok,Kwajalein	+2	Estonia(Tallinn)
-11	Midway Island	+2	Finland(Helsinki)
-10	United States-Hawaii-Aleutian	+2	Gaza Strip(Gaza)
-10	United States-Alaska-Aleutian	+2	Greece(Athens)
-9:30	French Polynesia	+2	Harare
-9	United States-Alaska Time	+2	Israel(Tel Aviv)
-8	Canada(Vancouver,Whitehorse)	+2	Jordan(Amman)
-8	Mexico(Tijuana,Mexicali)	+2	Latvia(Riga)
-8	United States-Pacific Time	+2	Lebanon(Beirut)

-8	Baja California	+2	Moldova(Kishinev)
-7	Canada(Edmonton,Calgary)	+2	Pretoria
-7	Mexico(Mazatlan,Chihuahua)	+2	Jerusalem
-7	United States-Mountain Time	+2	Russia(Kaliningrad)
-7	United States-MST no DST	+2	Bulgaria(Sofia)
-7	Chihuahua,La Paz	+2	Lithuania(Vilnius)
-7	Arizona	+2	Cairo
-6	Guatemala	+2	Istanbul
-6	El Salvador	+2	E.Europe
-6	Honduras	+2	Tripoli
-6	Nicaragua	+2	Romania(Bucharest)
-6	Costa Rica	+2	Syria(Damascus)
-6	Belize	+2	Turkey(Ankara)
-6	Canada-Manitoba(Winnipeg)	+2	Ukraine(Kyiv, Odessa)
-6	Chile(Easter Islands)	+3	East Africa Time
-6	Guadalajara	+3	Iraq(Baghdad)
-6	Monterrey	+3	Russia(Moscow)
-6	Mexico(Mexico City,Acapulco)	+3	St.Petersburg
-6	Saskatchewan	+3	Kuwait,Riyadh
-6	United States-Central Time	+3	Nairobi
-5	Bahamas(Nassau)	+3	Minsk
-5	Bogota,Lima	+3	Volgograd (RTZ 2)
-5	Canada(Montreal,Ottawa,Quebec)	+3:30	Iran(Teheran)
-5	Cuba(Havana)	+4	Armenia(Yerevan)
-5	Indiana (East)	+4	Azerbaijan(Baku)
-5	Peru	+4	Georgia(Tbilisi)
-5	Quito	+4	Russia(Samara)
-5	United States-Eastern Time	+4	Abu Dhabi,Muscat
-4:30	Venezuela(Caracas)	+4	Izhevsk,Samara (RTZ 3)
-4	Canada(Halifax,Saint John)	+4	Port Louis
-4	Atlantic Time (Canada)	+4:30	Afghanistan(Kabul)
-4	San Juan	+5	Kazakhstan(Aktau)

-4	Manaus,Cuiaba	+5	Kazakhstan(Aqtobe)
-4	Georgetown	+5	Ekaterinburg (RTZ 4)
-4	Chile(Santiago)	+5	Karachi
-4	Paraguay(Asuncion)	+5	Tashkent
-4	United Kingdom-Bermuda(Bermuda)	+5	Pakistan(Islamabad)
-4	United Kingdom(Falkland Islands)	+5	Russia(Chelyabinsk)
-4	Trinidad&Tobago	+5:30	India(Calcutta)
-3:30	Canada-New Foundland(St.Johns)	+5:30	Mumbai,Chennai
-3	Greenland(Nuuk)	+5:30	Kolkata,New Delhi
-3	Argentina(Buenos Aires)	+5:30	Sri Jayawardenepura
-3	Brazil(no DST)	+5:45	Nepal(Katmandu)
-3	Brasilia	+6	Kyrgyzstan(Bishkek)
-3	Cayenne,Fortaleza	+6	Kazakhstan(Astana, Almaty)
-3	Montevideo	+6	Russia(Novosibirsk,Omsk)
-3	Salvador	+6	Bangladesh(Dhaka)
-3	Brazil(DST)	+6:30	Myanmar(Naypyitaw)
-2:30	Newfoundland and Labrador	+6:30	Yangon (Rangoon)
-2	Brazil(no DST)	+7	Russia(Krasnoyarsk)
-2	Mid-Atlantic	+7	Thailand(Bangkok)
-1	Portugal(Azores)	+7	Vietnam(Hanoi)
-1	Cape Verde Islands	+7	Jakarta
0	GMT	+8	China(Beijing)
0	Greenland	+8	Singapore(Singapore)
0	Western Europe Time	+8	Hong Kong,Urumqi
0	Monrovia	+8	Taipei
0	Reykjavik	+8	Kuala Lumpur
0	Casablanca	+8	Australia(Perth)
0	Denmark-Faroe Islands(Torshavn)	+8	Russia(Irkutsk, Ulan-Ude)
0	Ireland(Dublin)	+8	Ulaanbaatar
0	Edinburgh	+8:45	Eucla
0	Portugal(Lisboa,Porto,Funchal)	+9	Korea(Seoul)

0	Spain-Canary Islands(Las Palmas)	+9	Japan(Tokyo)
0	United Kingdom(London)	+9	Russia(Yakutsk,Chita)
0	Lisbon	+9:30	Australia(Adelaide)
0	Morocco	+9:30	Australia(Darwin)
+1	Albania(Tirane)	+10	Australia(Sydney,Melbourne,Canberra)
+1	Austria(Vienna)	+10	Australia(Brisbane)
+1	Belgium(Brussels)	+10	Australia(Hobart)
+1	Caicos	+10	Russia(Vladivostok)
+1	Belgrade	+10	Magadan (RTZ 9)
+1	Bratislava	+10	Guam,Port Moresby
+1	Ljubljana	+10	Solomon Islands
+1	Chad	+10:30	Australia(Lord Howe Islands)
+1	Copenhagen	+11	New Caledonia(Noumea)
+1	West Central Africa	+11	Chokurdakh (RTZ 10)
+1	Poland(Warsaw)	+11	Russia(Srednekolymsk Time)
+1	Spain(Madrid)	+11:30	Norfolk Island
+1	Croatia(Zagreb)	+12	New Zealand(Wellington,Auckland)
+1	Czech Republic(Prague)	+12	Fiji Islands
+1	Denmark(Kopenhagen)	+12	Russia(Kamchatka Time)
+1	France(Paris)	+12	Anadyr
+1	Germany(Berlin)	+12	Petropavlovsk-Kamchatsky (RTZ 11)
+1	Hungary(Budapest)	+12	Marshall Islands
+1	Italy(Rome)	+12:45	New Zealand(Chatham Islands)
+1	Switzerland(Bern)	+13	Nuku'alofa
+1	Sweden(Stockholm)	+13	Tonga(Nukualofa)
+1	Luxembourg(Luxembourg)	+13	Samoa
+1	Macedonia(Skopje)	+13:30	Chatham Islands
+1	Netherlands(Amsterdam)	+14	Kiribati
+1	Namibia(Windhoek)		

NTP Settings

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

DHCP server or configured manually.

NTP Configuration

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

Configuration parameter

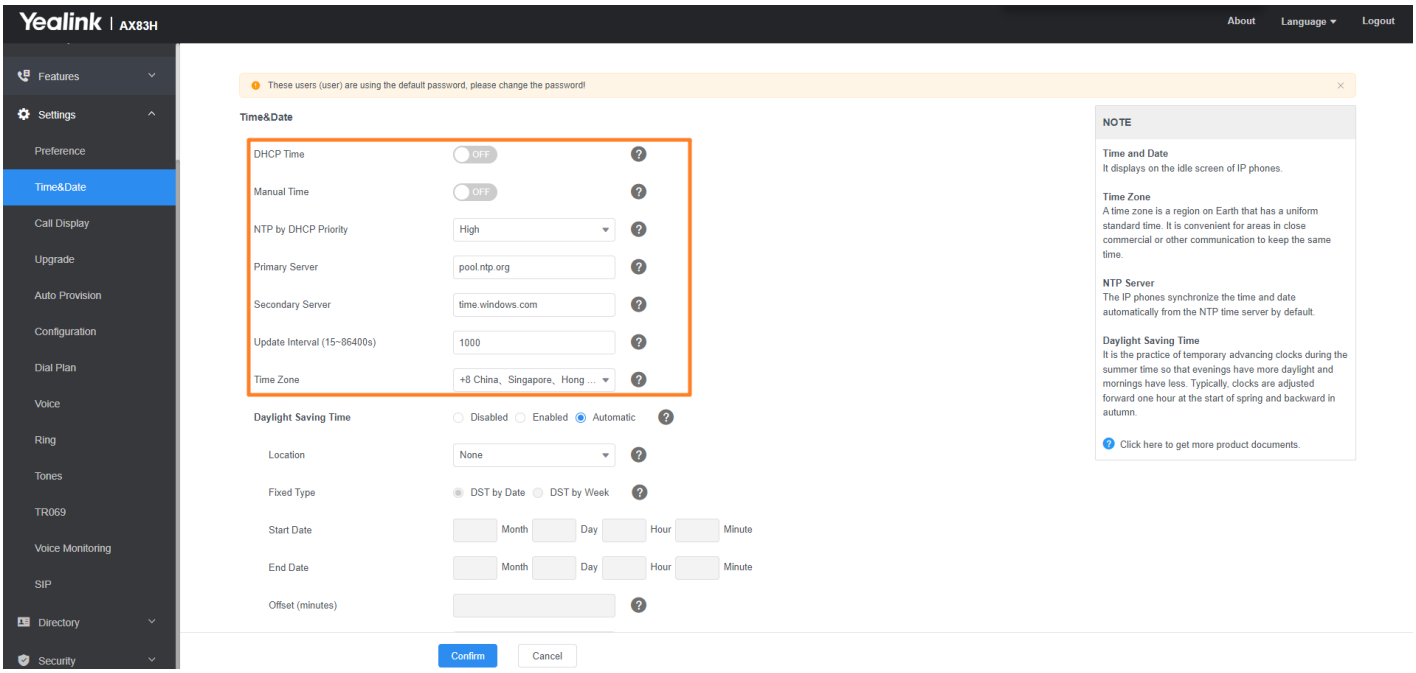
```
local_time.manual_ntp_srv_prior
local_time.dhcp_time
local_time.ntp_server1
local_time.ntp_server2
local_time.interval
local_time.time_zone
local_time.time_zone_name
```

Parameter	Description	Permitted Values	Default Value
local_time.manual_ntp_srv_prior	It configures the priority for the phone to use the NTP server address offered by the DHCP server.	0- High (use the NTP server address offered by the DHCP server preferentially) 1- Low (use the NTP server address configured manually preferentially)	0
local_time.dhcp_time	It enables or disables the phone to update time with the offset time offered by the DHCP server. **NOTE** It is only available to offset from Greenwich Mean Time GMT 0.	0-Disabled 1-Enabled	0
local_time.ntp_server1	It configures the IP address or the domain name of the primary NTP server.	String within 99 characters	cn.pool.ntp.org
local_time.ntp_server2	It configures the IP address or the domain name of the secondary NTP server. If the primary NTP server is not configured by the parameter “local_time.ntp_server1”, or cannot be accessed, the phone will request the time and date from the secondary NTP server.	String within 99 characters	pool.ntp.org
local_time.interval	It configures the interval (in seconds) at which the phone updates time and date from the NTP server.	Integer from 15 to 86400	1000

local_time.time_zone	It configures the time zone.	-12 to +14 For available time zones, refer to Time Zone.	8
local_time.time_zone_name	It configures the time zone name. **ⓘ NOTE** It works only if "local_time.summer_time" is set to 2 (Automatic) and the parameter "local_time.time_zone" should be configured in advance.	String within 32 characters The available time zone names depend on the time zone configured by the parameter "local_time.time_zone". For available time zone names, refer to Time Zone.	China(Beijing)

Set via the Web User Interface

On the web user interface, go to **Settings** > **Time & Date**



DST Settings

You can set DST for the desired area as required. By default, the DST is set to Automatic, so it can be adjusted automatically from the current time zone configuration.
The time zone and corresponding DST pre-configurations exist in the AutoDST file. If the DST is set to Automatic, the phone obtains the DST configuration from the AutoDST file.
You can customize the AutoDST file if required. The AutoDST file allows you to add or modify time zone and DST settings for your area each year.

Auto DST File Attributes

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

Attributes	Type	Values	Description
szTime	required	[+/-][X]:[Y], X=0~14, Y=0~59	Time Zone
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/Minute (for iType=0) Month: 1~12 Day: 1~31 Hour: 0 (midnight)~23 Minute: 0~59 Month/Week of Month/Day of Week/Hour of Day/Offset Days (for iType=1) Month: 1~12 Week of Month: 1~5 (the last week) Day of Week: 1~7 Hour of Day: 0:0 (midnight)~23:59 Offset Days: -1~-6	Starting time of the DST
szEnd	optional	Same as szStart	Ending time of the DST
szOffset	optional	Integer from -300 to 300	The offset time (in minutes) of DST

Customizing Auto DST File

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

```
<DSTData>
 <DST szTime="-12"  szZone="Eniwetok,Kwajalein"/>
 <DST szTime="-11"  szZone="Midway Island"/>
 <DST szTime="-10"  szZone="United States-Hawaii-Aleutian"/>
 <DST szTime="-10"  szZone="United States-Alaska-Aleutian"/>
 <DST szTime="-9:30"  szZone="French Polynesia"/>
 <DST szTime="-9"  szZone="United States-Alaska Time"    iType="1" szStart="3/2/7/2"  szEnd="11/1/7/2"  szOffset="60
 <DST szTime="-8"   szZone="Canada(Vancouver,Whitehorse)"  iType="1" szStart="3/2/7/2"   szEnd="11/1/7/2"  szOffset
 <DST szTime="-8"   szZone="Mexico(Tijuana,Mexicali)"    iType="1" szStart="3/2/7/2"   szEnd="11/1/7/2"  szOffset="60
 <DST szTime="-8"   szZone="United States-Pacific Time"   iType="1" szStart="3/2/7/2"   szEnd="11/1/7/2"  szOffset="6
 <DST szTime="-8"   szZone="Baja California"/>
 <DST szTime="-7"   szZone="Canada(Edmonton,Calgary)" iType="1" szStart="3/2/7/2"   szEnd="11/1/7/2"  szOffset="60
 <DST szTime="-7"   szZone="Mexico(Mazatlan,Chihuahua)" iType="1" szStart="4/1/7/2"   szEnd="10/5/7/2"  szOffset="
 <DST szTime="-7"   szZone="United States-Mountain Time" iType="1" szStart="3/2/7/2"   szEnd="11/1/7/2"  szOffset="
 </DSTData>
```

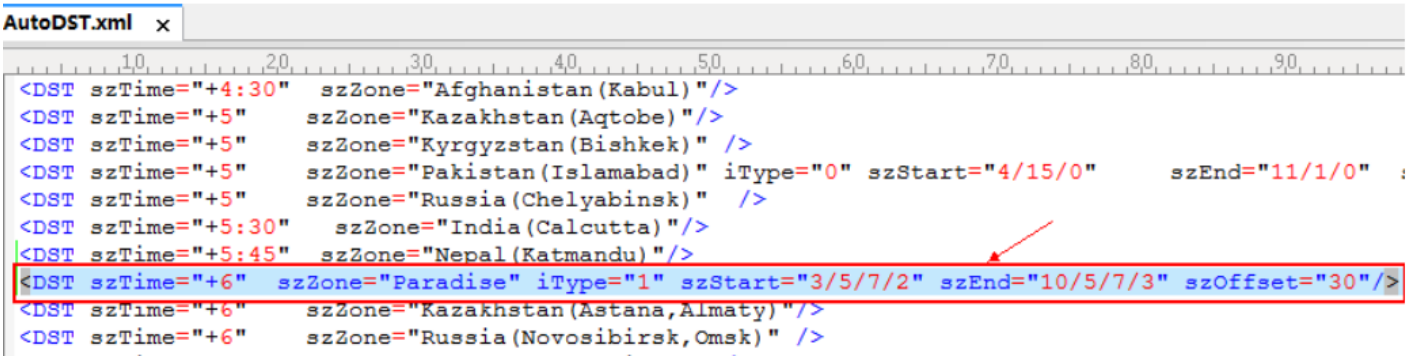
1. Open the AutoDST file.
2. To add a new time zone, add <DST szTime="" szZone="" iType="" szStart="" szEnd="" szOffset=""/> between `<DSTData>` and `</DSTData>`.

3. Specify the DST attribute values within double quotes.

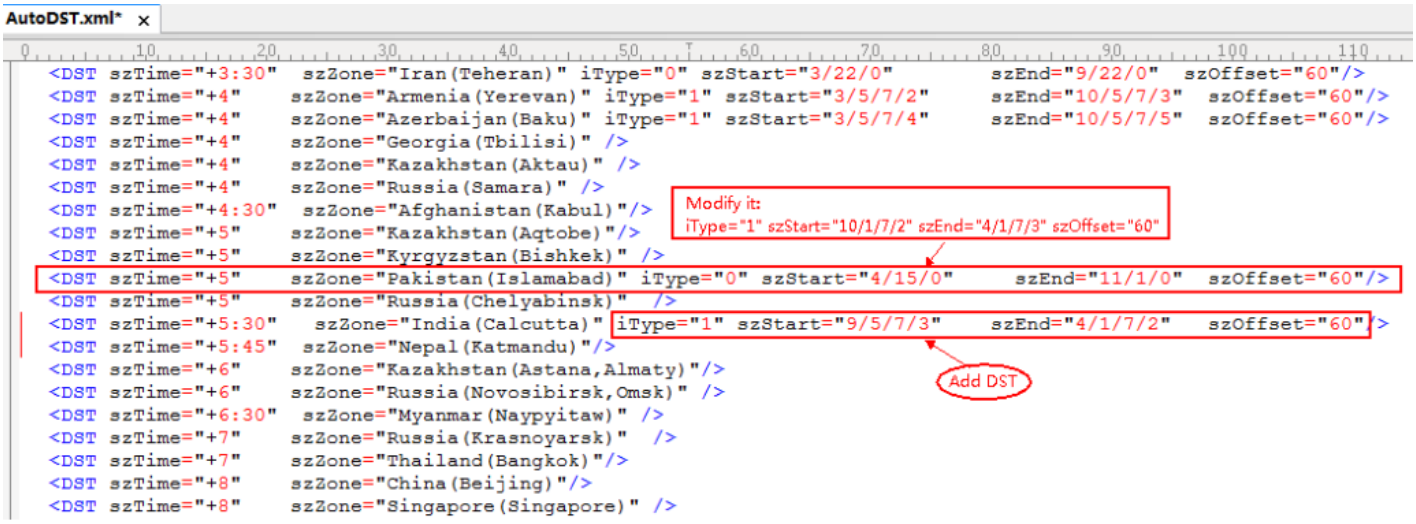
For example:

Add a new time zone (+6 Paradise) with daylight saving time 30 minutes:

<DST szTime="+6" szZone="Paradise" iType="1" szStart="3/5/7/2" szEnd="10/5/7/3" szOffset="30"/ >



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



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

DST Configuration

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

Configuration parameter

local_time.summer_time
local_time.dst_time_type
local_time.start_time
local_time.end_time
local_time.offset_time
auto_dst.url

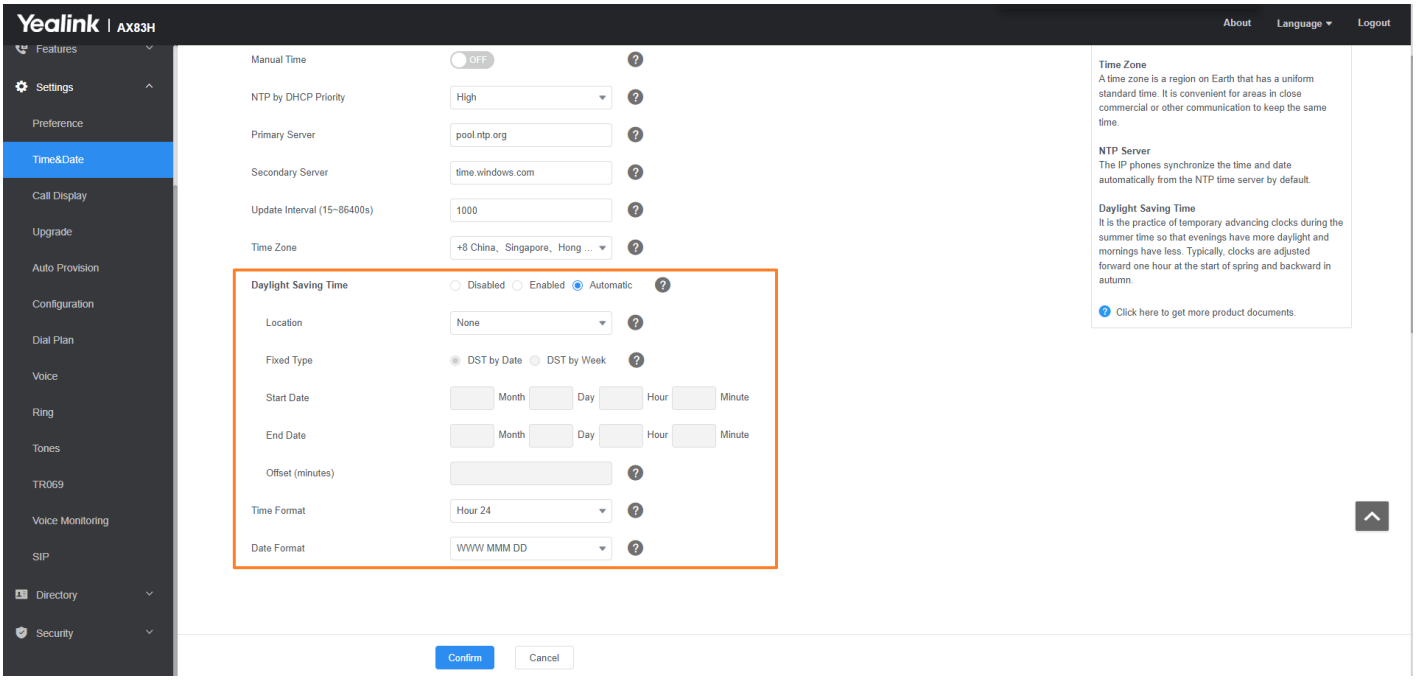
Parameter	Description	Permitted Values	Default
local_time.summer_time	It configures the Daylight Saving Time (DST) feature.	0-Disabled 1-Enabled 2-Automatic	2

local_time.dst_time_type	It configures the Daylight Saving Time (DST) type. **NOTE** It works only if "local_time.summer_time" is set to 1 (Enabled).	0-DST by Date 1-DST by Week	0
local_time.start_time	It configures the start time of the Daylight Saving Time (DST). **NOTE** It works only if "local_time.summer_time" is set to 1 (Enabled).	Month/Day/Hour:Minute-DST by Date, use the following mapping: Month: 1=January, 2=February,…, 12=December Day: 1=the first day in a month,…, 31= the last day in a month Hour:Minute: 0:0=0:0am, 1:45=1:45am,…, 23:59=11:59pm ---------- Month/Week of Month/Day of Week/Hour of Day, Offset Days Forward-DST by Week, use the following mapping: Month: 1=January, 2=February,…, 12=December Week of Month: 1=the first week in a month,…, 5=the last week in a month Day of Week: 1=Monday, 2=Tuesday,…, 7=Sunday Hour of Day: 0:0=0:0am, 1:45=1:45am,…, 23:59=11:59pm Offset Days (Optional.): -1=one day offset forward, -2-two days offset forward,…, -6-six days offset forward	1/1/0

local_time.end_time	It configures the end time of the Daylight Saving Time (DST). **NOTE** It works only if "local_time.summer_time" is set to 1 (Enabled).	Month/Day/Hour:Minute-DST by Date, use the following mapping: Month: 1=January, 2=February,…, 12=December Day: 1=the first day in a month,…, 31= the last day in a month Hour:Minute: 0:0=0:0am, 1:45=1:45am,…, 23:59=11:59pm --- Month/Week of Month/Day of Week/Hour of Day, Offset Days Forward-DST by Week, use the following mapping: Month: 1=January, 2=February,…, 12=December Week of Month: 1=the first week in a month,…, 5=the last week in a month Day of Week: 1=Monday, 2=Tuesday,…, 7=Sunday Hour of Day: 0:0=0:0am, 1:45=1:45am,…, 23:59=11:59pm Offset Days (Optional.): -1=one day offset forward, -2-two days offset forward,…, -6-six days offset forward	12/31/23
local_time.offset_time	It configures the offset time (in minutes) of Daylight Saving Time (DST). **NOTE** It works only if "local_time.summer_time" is set to 1 (Enabled).	Integer from -300 to 300	60
auto_dst.url	It configures the access URL of the DST file (AutoDST.xml). **NOTE** It works only if "local_time.summer_time" is set to 2 (Automatic).	URL within 511 characters	Blank

Set via the Web User Interface

On the web user interface，go to **Settings** > **Time & Date** > **Daylight Saving Time**



Time and Date Manually Configuration

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

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

Configuration parameter

```
local_time.manual_time_enable
```

Parameter	Description	Permitted Values	Default
local_time.manual_time_enable	It enables or disables the phone to obtain time and date from manual settings.	0-Disabled, the phone obtains time and date from the NTP server. 1-Enabled	0

ⓘ NOTE

After the device reboots, it will be forcibly switched to obtain the time and date from the NTP server.

Time and Date Format Configuration

You can customize the time and date by choosing between a variety of time and date formats, including options to date format with the day, month, or year, and time format in 12 hours or 24 hours, or you can also custom the date format as required.

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

Configuration parameter

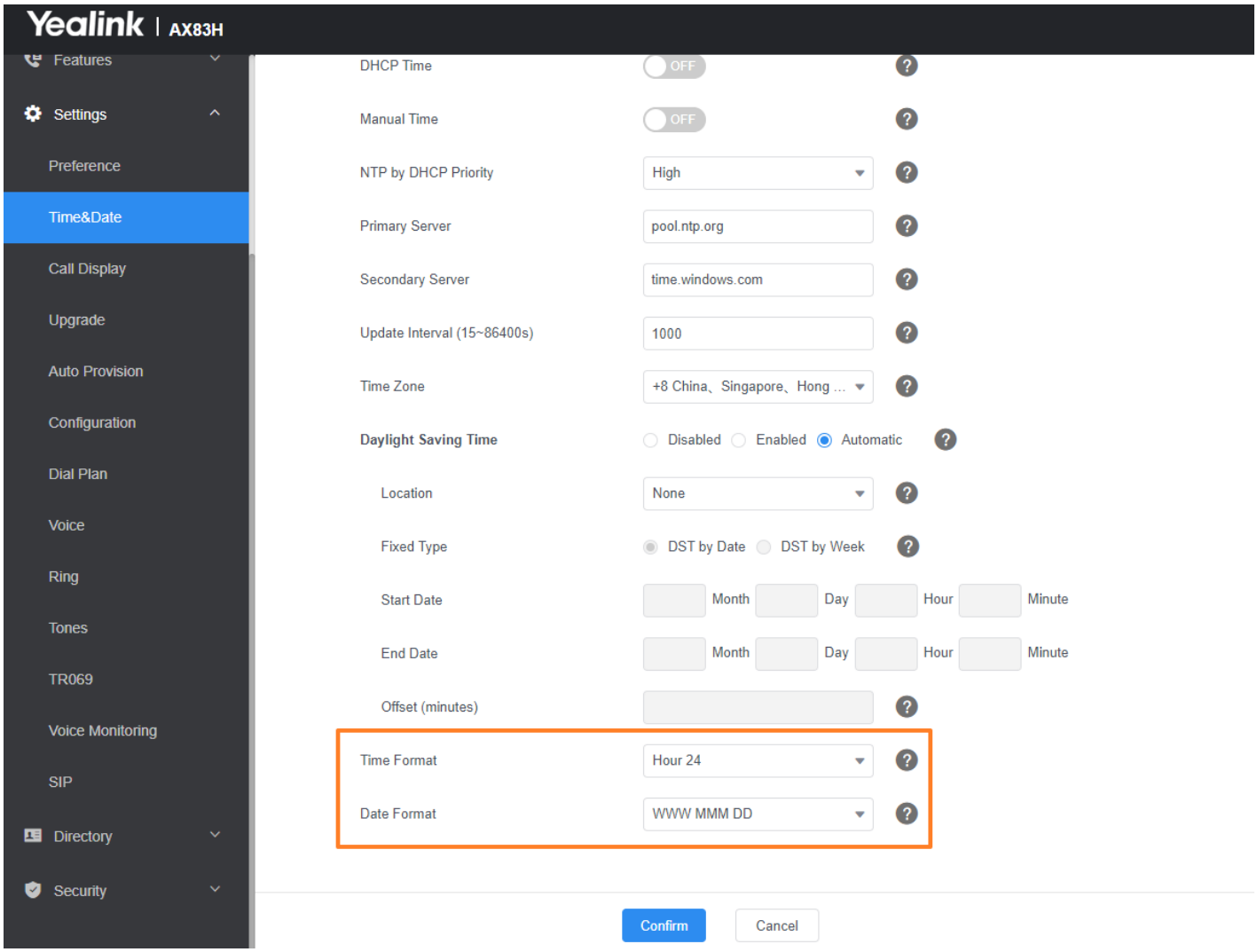
```
local_time.time_format
local_time.date_format
lcl.datetime.date.format
```

Parameter	Description	Permitted Values	Default
local_time.time_format	It configures the time format.	0-Hour 12, the time will be displayed in 12-hour format with AM or PM specified. 1-Hour 24, the time will be displayed in 24-hour format (for example, 2:00 PM displays as 14:00).	1
local_time.date_format	It configures the date format. **NOTE** The value configured by the parameter "lcl.datetime.date.format" takes precedence over that configured by this parameter.	0-WWW MMM DD (for Chinese display: MM DD WWW) 1-DD-MMM-YY (for Chinese display: YY-MMM-DD) 2-YYYY-MM-DD 3-DD/MM/YYYY (for Chinese display: YYYY/MM/DD) 4-MM/DD/YY (for Chinese display: YY/MM/DD) 5-DD MMM YYYY (for Chinese display: YYYY MMM DD) 6-WWW DD MMM (for Chinese display: MM DD WWW) 20-Custom format configured by "lcl.datetime.date.format", for example, DD.MM.YYYY Use the following mapping: "WWW" represents the abbreviation of the week; "DD" represents a two-digit day; "MMM" represents the first three letters of the month; "YYYY" represents a four-digit year, and "YY" represents a two-digit year.	0

lcl.datetime.date.format	It configures the display format of the date.	Any combination of Y, M, D, W, and the separator (for example, space, dash, slash). Use the following mapping: Y = year, M = month, D = day, W = day of week "Y" /" YY" represents a two-digit year, more than two "Y" letters (for example, YYYY) represent a four-digit year; "M" / "MM" represents a two-digit month, "MMM" represents the abbreviation of the month, three or more than three "M" letters (for example, MMM) represent the long format of the month; One or more than one "D" (for example, DDD) represents a two-digit day; "W" / "WW" represents the abbreviation of the day of the week, three or more three "W" letters (for example, WWW) represent the long format of the day of the week. For more rules, refer to Date Customization Rule.	Blank

Set via the Web User Interface

On the web user interface，go to **Settings** > **Time & Date** > **Time Format（Date Format)**



Date Customization Rule

You need to know the following rules when customizing date formats:

Format	Description
Y/YY	It represents a two-digit year. For example, 16, 17, 18…
Y is used more than twice (for example, YYY, YYYY)	It represents a four-digit year. For example, 2016, 2017, 2018…
M/MM	It represents a two-digit month. For example, 01, 02,…, 12
MMM	It represents the abbreviation of the month. For example, Jan, Feb, …, Dec
M is used more than three times (for example, MMMM)	It represents the long format of the month. For example, January, February,…, December
D is used once or more than once (for example, DD)	It represents a two-digit day. For example, 01, 02,…, 31
W/WW	It represents the abbreviation of the day of the week. For example, Mon, Tue,…, Sun

W is used more than twice (for example, WWW, WWWW)	It represents the long format of the day of the week. For example, Monday, Tuesday,⋯, Sunday
W is used more than twice (for example, WWW, WWWW)	It represents the long format of the day of the week. For example, Monday, Tuesday,⋯, Sunday

Call Display

Call Display

By default, the phones present the contact information (including avatar and identity) when receiving an incoming call, dialing an outgoing call or engaging in a call.
You can configure what contact information presents and how to display the contact information. If the contact exists in the phone directory, the phone displays the saved contact name and number. If not, it will use the Calling Line Identification Presentation (CLIP) or Connected Line Identification Presentation (COLP) to display the contact’ s identity.

Call Display Configuration

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

Configuration parameter

```
phone_setting.contact_photo_display.enable
phone_setting.little_contact_photo_display.enable
account.X.picture_info_enable[1]
phone_setting.called_party_info_display.enable
phone_setting.call_info_display_method
phone_setting.called_party_info_display_method
phone_setting.call_display_name.mode
phone_setting.incoming_call.horizontal_roll_interval
account.X.update_ack_while_dialing
account.X.refresh_remote_id.enable
sip.disp_incall_to_info
```

Parameter	Description	Permitted Values	Default
phone_setting.contact_photo_display.enable	It configures whether to display contact avatar when it receives an incoming call, dials an outgoing call or engages in a call.	0-Never, do not display contact avatar no matter whether the contact avatar exists or not 1-Always, display the customized contact avatar if it exists; display the built-in avatar if the customized contact avatar does not exist 2-Adaptive, display the customized contact avatar if it exists; otherwise, do not display	1

phone_setting.little_contact_photo_display.enable	It enables or disables the phone to display the little contact photo when it receives an incoming call, dials a call or is in a call. Note: It works only if "phone_setting.contact_photo_display.enable" is set to 1 (Always) or 2 (Adaptive).	0-Disabled 1-Enabled, the phone can display the full 16-digit number.	1
account.X.picture_info_enable[1]	It enables or disables the phone to download the picture from the URL contained in the Call-Info header of the INVITE message. Format of call info: Call-Info: ;purpose=wallpaper Call-Info: ;purpose=icon **ⓘ NOTE** If the phone receives both the call info information of "purpose = wallpaper" (wallpaper) and "purpose = icon" (avatar) at the same time, only the wallpaper is displayed, the avatar is not displayed.	0-Disabled 1-Enabled	0
phone_setting.called_party_info_display.enable	It enables or disables the phone to display the local identity when it receives an incoming call or during a call. **ⓘ NOTE** The information display method is configured by the parameter “phone_setting.call_info_display_method”.	0-Disabled 1-Enabled	0

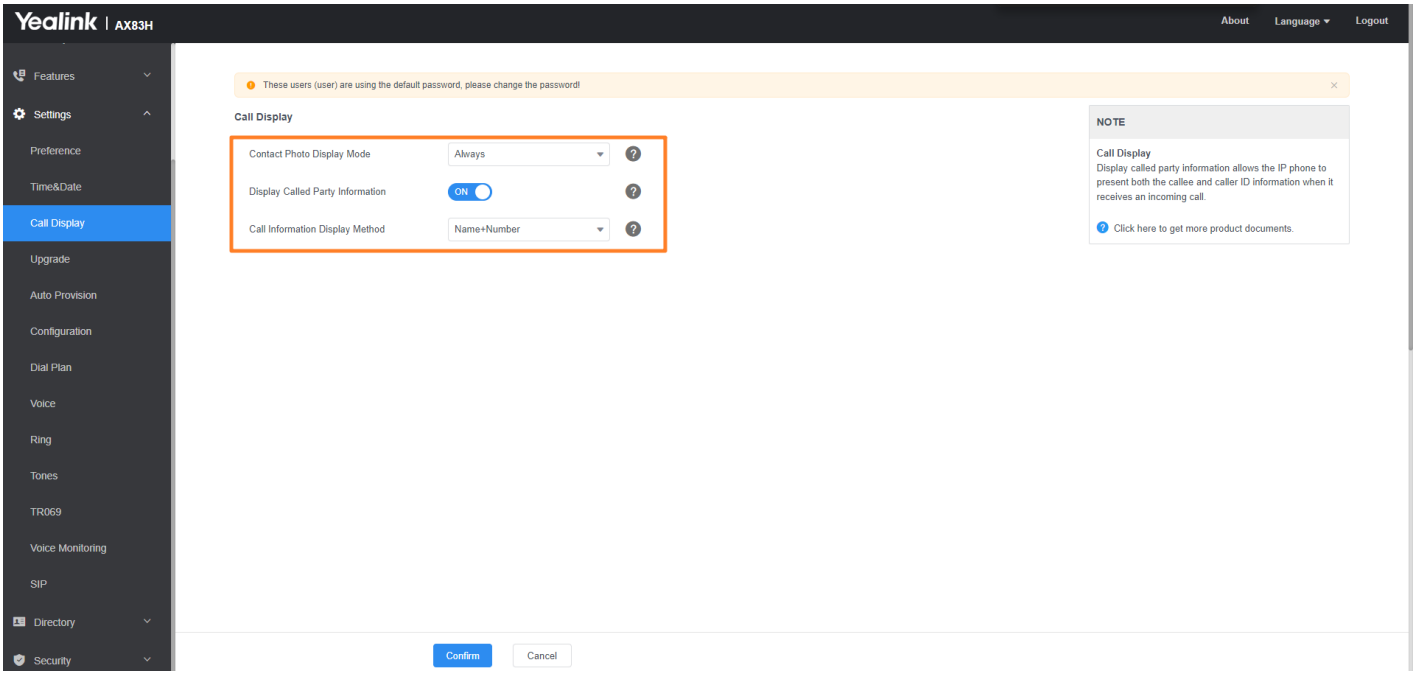
phone_setting.call_info_display_method	It configures the remote information display method when the phone receives an incoming call, dials an outgoing call or is during a call.	0-Name+Number 1-Number+Name 2-Name 3-Number 4-Full Contact Info (display namesip:xxx@domain.com) 5-Null Note: Name refers to the Label; Number refers to the User Name.	0
phone_setting.called_party_info_display_method	It configures the local party information display method when the phone receives an incoming call or is during a call. **ⓘ NOTE** It works only if "phone_setting.called_party_info_display.enable" is set to 1 (Enabled).	0-Name+Number 1-Number+Name 2-Name 3-Number 4-Full Contact Info (display namesip:xxx@domain.com) Note: Name refers to the Label, Display Name (Label > Display Name > User Name); Number refers to the User Name.	0
phone_setting.call_display_name.mode	It specifies which display names to be used as the caller ID/callee ID for calls from/to contacts in the phone directory. **ⓘ NOTE** This parameter also affects the history records display.	0-Names matched to the entries in the following phone directories are displayed preferentially, the priority is as follows: Local Directory > Remote Phone Book > Broadsoft Network Directory > BroadCloud Buddies > LDAP Directory > Network signaling. 1-Names provided through network signaling are displayed preferentially.	0
phone_setting.incoming_call.horizontal_roll_interval	It configures the interval (in milliseconds) for the phone to horizontally scroll the caller information when the phone is ringing.	Integer from 100 to 2000	500
account.X.update_ack_while_dialing[1]	It enables or disables the phone to update the display of call ID according to the ACK message.	0-Disabled 1-Enabled	0
account.X.refresh_remote_id.enable[1]	It enables or disables the phone to update the identity of the caller according to the request message from the remote party.	0-Disabled 1-Enabled	1

sip.disp_incall_to_info	It enables or disables the phone to display the identity contained in the To field of the INVITE message when it receives an incoming call.	0-Disabled 1-Enabled	0
features.number_privacy.enable	It is used to configure whether to enable the number privacy feature.	0-Disabled 1-Enabled	0
features.number_privacy.start_length	It is used to configure the number of digits at which the number starts to be hidden and the length of the hidden portion.	a, b: "a" represents the starting position, and "b" represents the hidden length. **For example:** 3, 4 means hiding four digits starting from the third position.	Blank

> [1]X is the account ID.

Set via the Web User Interface

On the web user interface, go to **Settings** > **Call Display**



Dialing Display

Display Method on Dialing Configuration

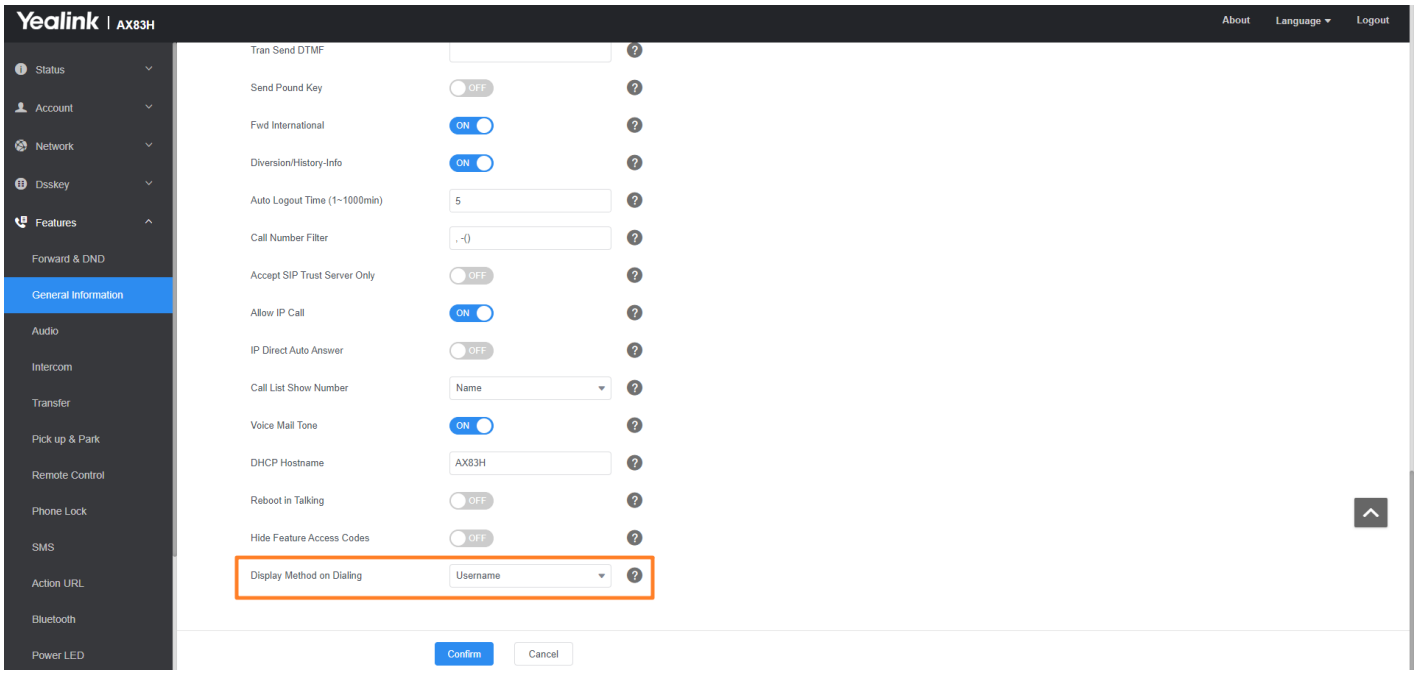
Configuration parameter

features.caller_name_type_on_dialing

Parameter	Description	Permitted Values	Default
features.caller_name_type_on_dialing	It configures the selected account information displayed on the pre-dialing or dialing screen. Note: It works only if "features.station_name.value" is left blank.	1-Label, configured by the parameter "account.X.label". 2-Display Name, configured by the parameter "account.X.display_name". 3-User Name, configured by the parameter "account.X.user_name".	3
features.password_dial.enable	It enables or disables the phone to partly display the callee number when placing a call.	0-Disabled 1-Enabled	0
features.password_dial.prefix	It configures the prefix that the number starts with this prefix will be partly displayed. Example: features.password_dial.prefix = 12 **NOTE** It works only if "features.password_dial.enable" is set to 1 (Enabled).	String within 32 characters	Blank
features.password_dial.length	It configures how many digits to be displayed as asterisks. Example: features.password_dial.length = 3 If you set the prefix to 12 and the length to 3, when you want to dial the number 123456, the entered number is displayed as 12***6 on the phone screen. **NOTE** It works only if "features.password_dial.enable" is set to 1 (Enabled).	Integer from 0 to 32	Blank

Set via the Web User Interface

On the web user interface，go to: **Features** > **General Information** > **Display Method on Dialing**



Search Source List in Dialing

The search source list in dialing allows you to search entries from the source list when the phone is on the pre-dialing/dialing screen. You can select the desired entry to dial out quickly.

When you haven't entered a number in the dialing interface, the softkey will display the "History" option and disappear once you start entering a number.

The search source list can be configured using a supplied super search template file (super_search.xml).

Search Source File Customization

You can ask the distributor or Yealink FAE for a supper search template. You can also refer to the following template:

```
<?xml version="1.0"?>
<root_super_search>
 <item id_name="local_directory_search" display_name="Local Directory" priority="1" enable="1" />
 <item id_name="calllog_search" display_name="History" priority="2" enable="1" />
 <item id_name="remote_directory_search" display_name="Remote Phone Book" priority="3" enable="0" />
  <item id_name="ldap_search" display_name="LDAP" priority="4" enable="0" dev="T19 T21 T23 T40 T40G T27 T27G T2
 <item id_name="BroadSoft_directory_search" display_name="Network Directory" priority="5" enable="0" />
  <item id_name="BroadSoft_UC_search" display_name="Buddies" priority="6" enable="0" dev="T29 T46 T46S T54S T52
 <item id_name="plcm_directory_search" display_name="Phonebook" priority="7" enable="0" />
 <item id_name="genband_directory_search" display_name="Personal Address Book" priority="8" enable="1" />
 <item id_name="MetaSwitch_directory_search" display_name="Network Contacts" priority="9" enable="0" />
 <item id_name="MetaSwitch_calllog_search" display_name="Network Call List" priority="10" enable="0" />
  <item id_name="mobile_directory_search" display_name="Mobile Contacts" priority="11" enable="1" dev="T29 T46 T4
  <item id_name="google_directory_search" display_name="Google Contacts" priority="12" enable="0" />
</root_super_search>
```

Search Source File Attributes

The following table lists the attributes you can use to add source lists to the super search file:

Attributes	Valid Values	Description
id_name	local_directory_search calllog_search remote_directory_search ldap_search BroadSoft_directory_search BroadSoft_UC_search plcm_directory_search genband_directory_search MetaSwitch_directory_search MetaSwitch_calllog_search mobile_directory_search google_directory_search	The directory list (For example, "local_directory_search" for the local directory list). **NOTE** Do not edit this field.
display_name	Local Contacts History Remote Phonebook LDAP Network Directories BroadSoft Buddies PhoneBook Personal Address Book Network Contacts Network Call List Mobile Contacts Google Contacts	The display name of the directory list. **NOTE** We recommend that you do not edit this field.
priority	1 to 12 1 is the highest priority.	The priority of the search results.
enable	0/1 0: Disabled 1: Enabled.	Enable or disable the phone to search the desired directory list.
dev	AX83H	The applicable phone models of the directory list. **NOTE** Do not edit this field.

Customizing Search Source File

1. Open the search source file.
2. To configure each directory list, edit the values within double quotes in the corresponding field.

For example, enable the local directory search, disable the call log search, and specify a priority.

```
<item id_name="local_directory_search" display_name="Local Contacts" priority="1" enable="1" />
<item id_name="calllog_search" display_name="History" priority="2" enable="0" />
```

3. Save the change and place this file to the provisioning server.

Search Source List Configuration

The following table lists the parameters you can use to configure the search source list.

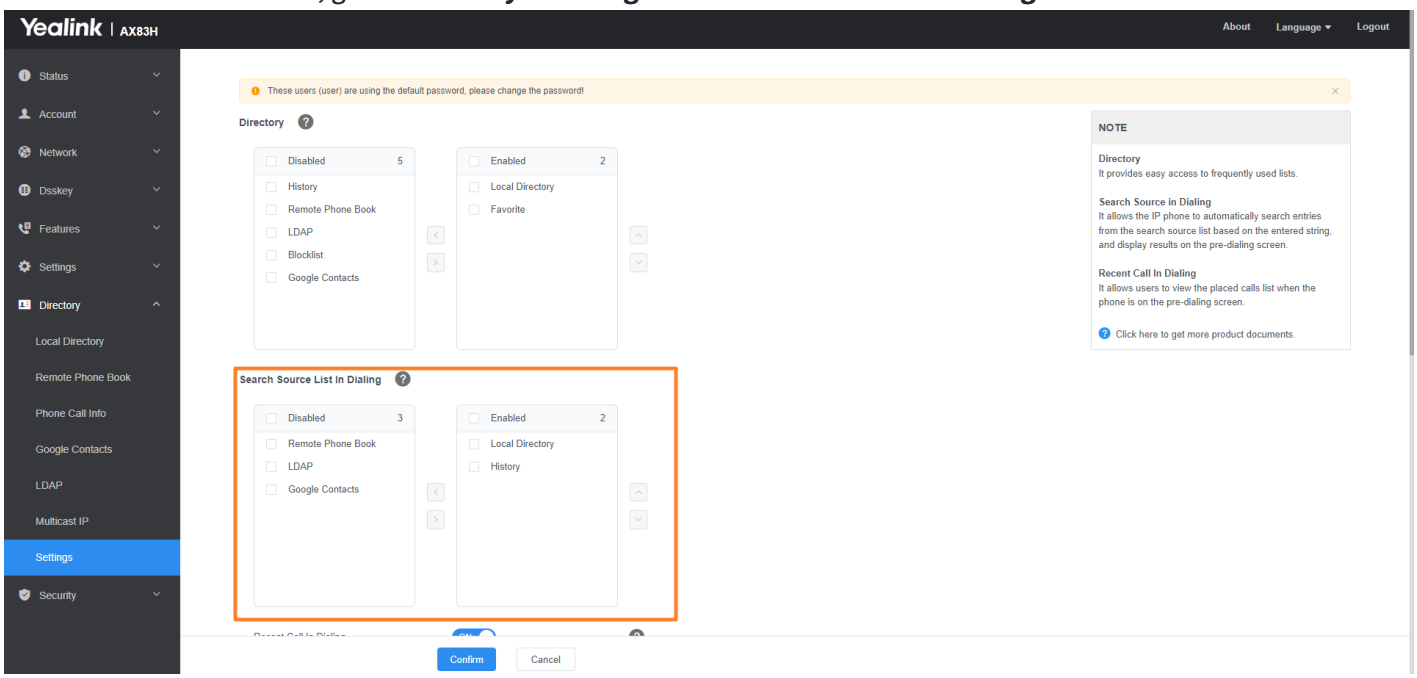
Configuration parameter

```
super_search.url
search_in_dialing.local_directory.enable
search_in_dialing.local_directory.priority
search_in_dialing.history.enable
search_in_dialing.history.priority
search_in_dialing.remote_phone_book.enable
search_in_dialing.remote_phone_book.priority
search_in_dialing.ldap.enable
search_in_dialing.ldap.priority
```

Parameter	Description	Permitted Values	Default
super_search.url	It configures the access URL of the custom super search file.	URL within 511 characters	Blank
search_in_dialing.local_directory.enable	It enables or disables the phone to automatically search entries from the local directory, and display results on the pre-dialing/dialing screen.	0-Disabled 1-Enabled	1
search_in_dialing.local_directory.priority	It configures the search priority of the local directory.	Integer greater than or equal to 0	1
search_in_dialing.history.enable	It enables or disables the phone to automatically search entries from the call history list, and display results on the pre-dialing/dialing screen.	0-Disabled 1-Enabled	1
search_in_dialing.history.priority	It configures the search priority of the call history list.	Integer greater than or equal to 0	2
search_in_dialing.remote_phone_book.enable	It enables or disables the phone to automatically search entries from the remote phone book, and display results on the pre-dialing/dialing screen.	0-Disabled 1-Enabled	0
search_in_dialing.remote_phone_book.priority	It configures the search priority of the remote phone book.	Integer greater than or equal to 0	3
search_in_dialing.ldap.enable	It enables or disables the phone to automatically search entries from the LDAP, and display results on the pre-dialing/dialing screen.	0-Disabled 1-Enabled	0
search_in_dialing.ldap.priority	It configures the search priority of the LDAP.	Integer greater than or equal to 0	4

Set via the Web User Interface

On the web user interface, go to **Directory** > **Settings** > **Search Source List In Dialing**.



Recent Call Display in Dialing

Recent call display allows you to view the placed calls list when the phone is on the dialing screen (lifts the handset, presses the Speakerphone key or desired line key). You can select to place a call from the placed calls list.

Recent Call in Dialing Configuration

The following table lists the parameter you can use to configure the recent call display in dialing.

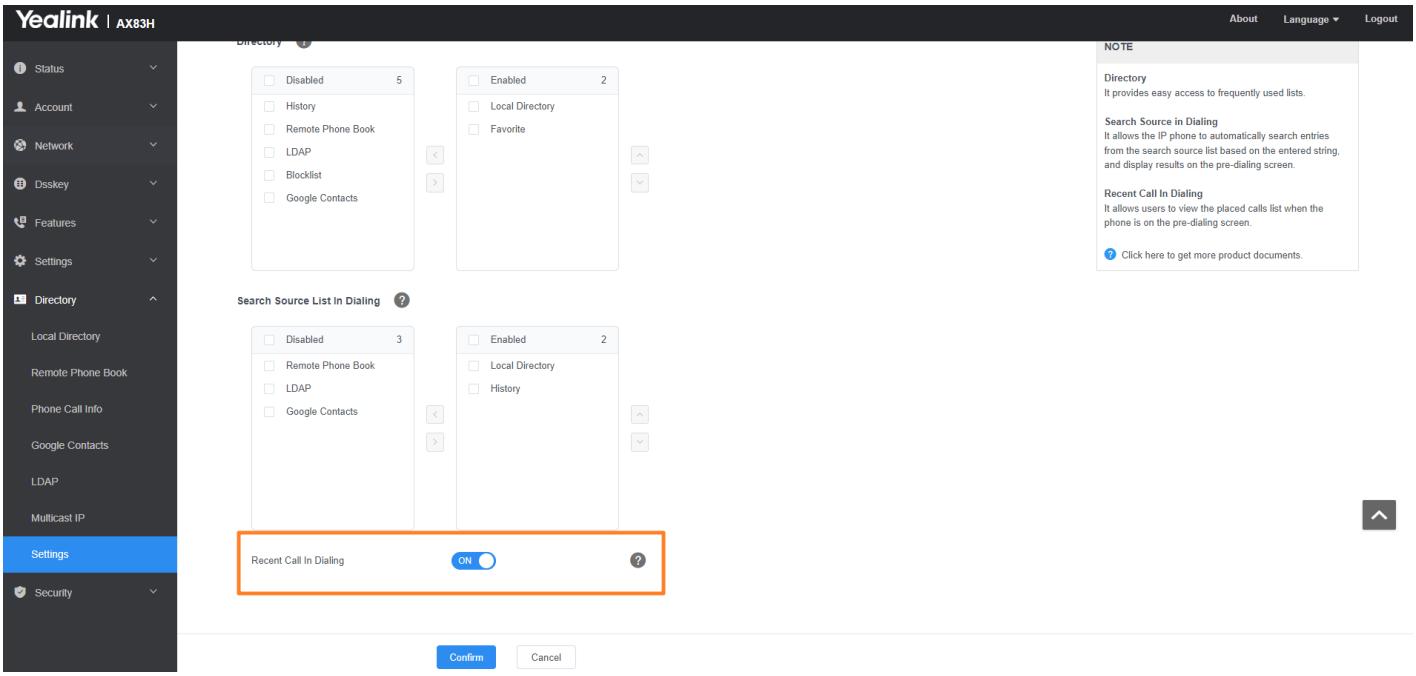
Configuration parameter

```
super_search.recent_call
```

Parameter	Description	Permitted Values	Default
super_search.recent_call	It enables or disables the Recent Call in Dialing feature.	0-Disabled 1-Enabled, users can view the placed calls list when the phone is on the dialing screen.	1

Set via the Web User Interface

On the web user interface, go to **Directory** > **Settings** > **Recent Call In Dialing**.



Screen Saver

Screen Saver

The screen saver will automatically start when the IP phone is idle for the preset waiting time. You can stop the screen saver at any time by pressing any key or touching the screen. When your phone is idle again for a preset waiting time, the screen saver starts again.

By default, the phone screen displays a built-in picture when the screen saver starts.

You can set custom pictures as the screen saver. You can also add personal pictures on your phone using a USB flash drive.

The time & date, certain status icons (for example, auto answer, DND, a new text message), or custom information (for example, notifications or company logo) is also configurable to display on the screen saver.

Screensaver Display Customization

You can customize the screen saver file to configure the phone whether to display custom information (for example, notifications or company logo) on the screen saver.

Screensaver File Elements and Attributes

The following table lists the elements and attributes you can use to add custom information in the screensaver file. We recommend that you do not edit these elements and attributes.

Elements	Attributes	Description

YealinkIPPhoneCustomScreenSaver	LineSpacing	The vertical distance between different lines.
	InsertImageLineNum	Specify which line to insert the image (configured by the Image element).
SystemTime	Size horizontalAlign verticalAlign Color	Specify "show" or "hide" between <SystemTime> and </SystemTime> to decide whether to display the time and date. Edit the attributes to decide how to display the time and date, including the size, position, and color.
StatusIcons	horizontalAlign verticalAlign	Specify "show" or "hide" between <StatusIcons> and </StatusIcons> to decide whether to display the status icons. Edit the attributes to decide the icons displayed position.
Line	Size Align Color	Specify the display text between <Line> and </Line>. Edit the attributes to decide how to display the text, including text size, position, and color.
Image	horizontalAlign verticalAlign height width	Specify the display image source between <Image> and </Image>. Edit the attributes to decide how to display the image, including position and size. **ⓘ NOTE** VerticalAlign works only if you do not configure InsertImageLineNum or set the InsertImageLineNum to 0.

Customizing the Screen Saver File

1. Open the screen saver file.
2. Modify settings as you want.

CustomScreenSaver.xml

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<YealinkIPPhoneCustomScreenSaver  LineSpacing = "9"     InsertImageLineNum = "1"  >

<SystemTime Size="Large" horizontalAlign="right" verticalAlign="top" Color="black">show</SystemTime>

<StatusIcons horizontalAlign="middle" verticalAlign="top">show</StatusIcons>

<Line Size="large" Align="center" Color="blue">Yealink</Line>
<Line Size="large" Align="center" Color="RGB" >SIP Phone</Line>
<Line Size="large" Align="center" Color="RGB">Test</Line>

<Image horizontalAlign="middle"  verticalAlign="bottom"  height="30" width="30">http://192.168.1.1/Yealink.jpeg</Image>

</YealinkIPPhoneCustomScreenSaver>
```

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

4. Specify the access URL of the screen saver file in the configuration file.

Custom Screensaver Picture Limit

Either the smaller or the larger picture will be scaled proportionally to fit the screen. The screensaver picture format must meet the following:

Phone Model	Format	Resolution	Single File Size	Note
AX83H	*.jpg/*.png/*.bmp/*.jpeg	<=4.2 megapixels	<=5MB	2MB of space should be reserved for the phone

Screensaver Configuration

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

Configuration parameter

```
screensaver.wait_time
screensaver.display_clock.enable
screensaver.type
screensaver.upload_url
screensaver.delete
screensaver.clock_move_interval
screensaver.picture_change_interval
```

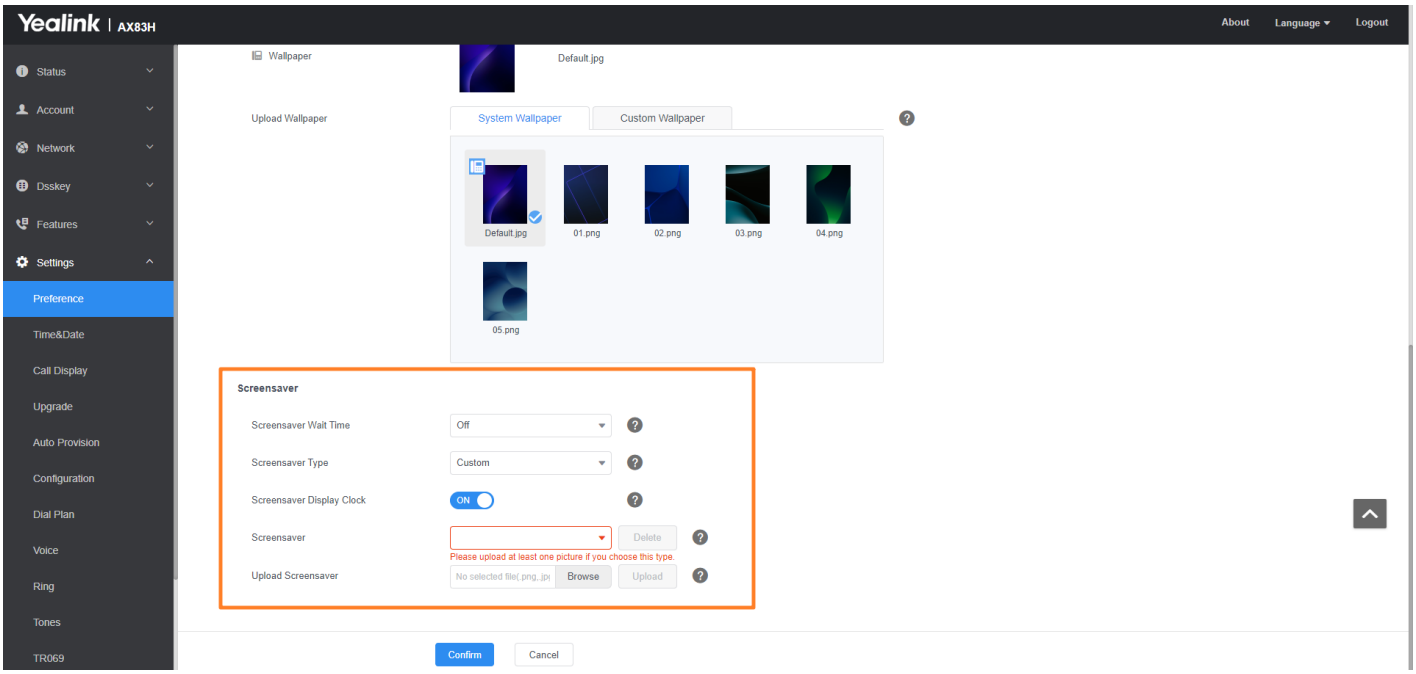
Parameter	Description	Permitted Values	Default
screensaver.wait_time	It configures the time (in seconds) to wait in the idle state before the screen saver starts.	Off 15-15s 30-30s 60-1min 120-2min 300-5min 600-10min 1800-30min 3600-1h 7200-2h 10800-3h 14400-4h 21600-6h 28800-8h 43200-12h	Off

screensaver.display_clock.enable	It enables or disables the phone to display the clock and icons when the screen saver starts. **NOTE** It works only if "screensaver.type" is set to 0 (System) or 1 (Custom).	0-Disabled 1-Enabled	1
screensaver.type	It configures the type of screen saver to display.	0-System, the LCD screen will display the built-in picture. 1-Custom, the LCD screen will display the custom screen saver images (configured by the parameter "screensaver.upload_url"). If multiple images are uploaded, the phone will display all images alternately. The time interval is configured by the parameter "screensaver.picture_change_interval".	0
screensaver.upload_url	It configures the access URL of the custom screen saver image. Example: screensaver.upload_url = http://192.168.10.25/Screencapture.jpg During auto provisioning, the phone connects to the HTTP provisioning server "192.168.10.25", and downloads the screen saver image "Screencapture.jpg". If you want to upload multiple screen saver images to the phone simultaneously, you can configure as follows: screensaver.upload_url = http://192.168.10.25/Screencapture.jpg screensaver.upload_url = http://192.168.10.25/Screensaver.jpg	URL within 511 characters	Blank

screensaver.delete	It deletes the specified or all custom screen saver images. Example: Delete all custom screen saver images: screensaver.delete = http://localhost/all Delete a custom screen saver image (for example, Screencapture.jpg): screensaver.delete = http://localhost/Screencapture.jpg	http://localhost/all or http://localhost/name.(jpg/png/bmp/jpeg)	Blank
screensaver.clock_move_interval	It configures the interval (in seconds) for the phone to move the clock and icons when the screen saver starts. **NOTE** It works only if "screensaver.display_clock.enable" is set to 1 (Enabled).	Integer from 5 to 1200	600
screensaver.picture_change_interval	It configures the interval (in seconds) for the phone to change the picture when the screen saver starts. **NOTE** It works only if "screensaver.type" is set to 1 (Custom) and the parameter "screensaver.upload_url" should be configured in advance.	Integer from 5 to 1200	60

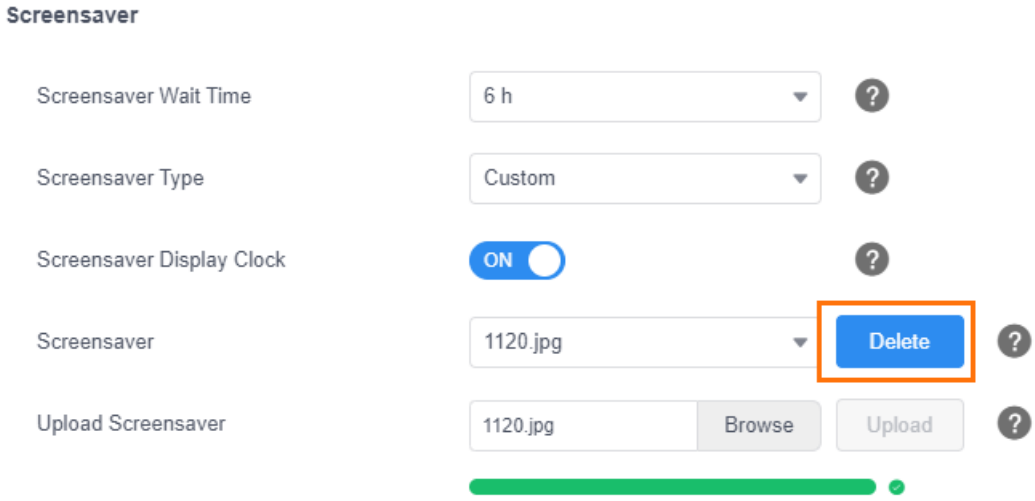
Set via the Web User Interface

On the web user interface, go to **Settings** > **Preference** > **Screensaver Display Clock.



Deleting a Screensaver Picture

You can delete the uploaded custom pictures for a specific IP phone via the web user interface at the path: **Settings** > **Preference**, select Custom from the Screensaver Type field, and then select a desired custom picture from the Screensaver field, click Del (Delete). You can only delete the custom pictures.



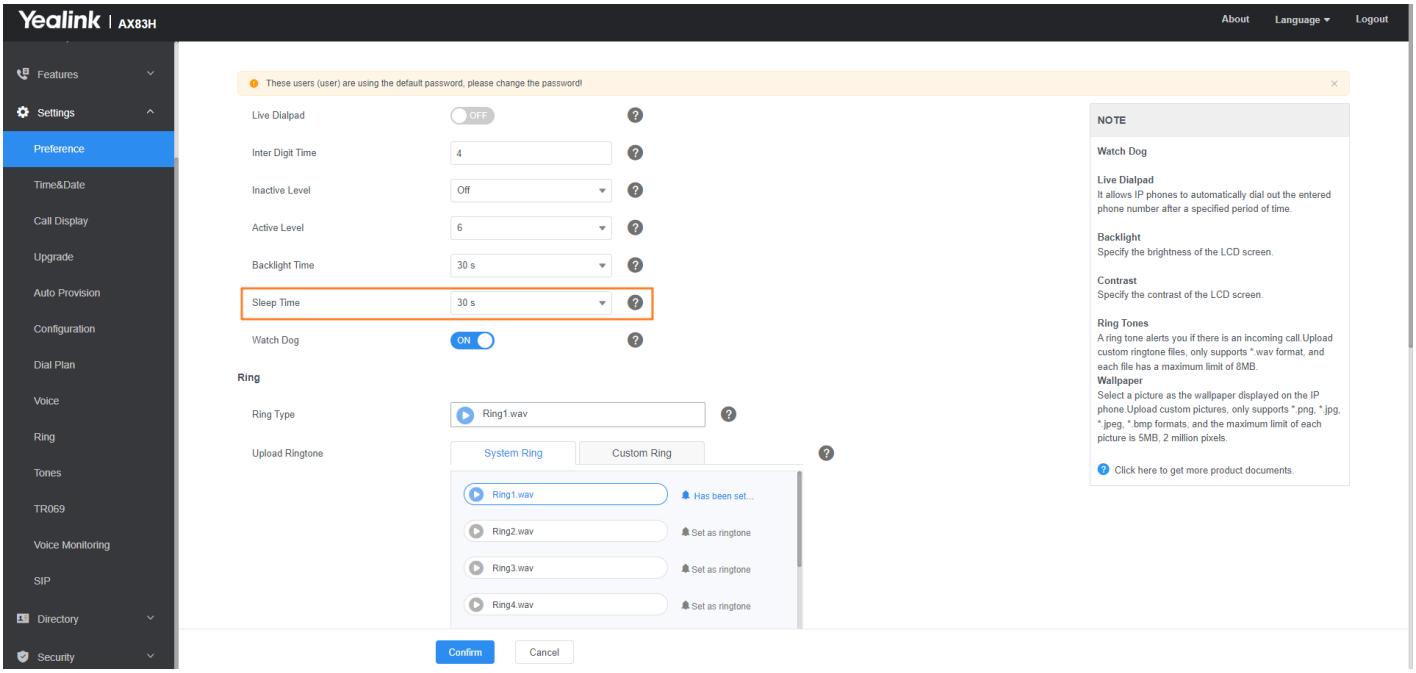
Sleep Time

Introduction

When the phone is in no operation state, it enters the sleep state by default for 30 S. You can adjust the time according to your needs.

Set via the Web User Interface

On the web user interface, go to **Settings** > **Preference** > **Sleep Time**.



Configuration Parameter

phone_setting.sleep_time

Parameter	Description	Permitted Values	Default
phone_setting.sleep_time	It configures the sleep time when the phone is inactive.	-Off - 15S - 30S - 1min - 2min - 5min - 10min - 30min	30S

Wallpaper Settings

Wallpaper

Wallpaper is a picture used as the background of the phone. The phone comes with a default picture. You can change it to a built-in picture or custom wallpaper from personal pictures.

Wallpaper Configuration

You can change the wallpaper to any built-in picture or custom picture.
The following table lists the parameters you can use to change the wallpaper.

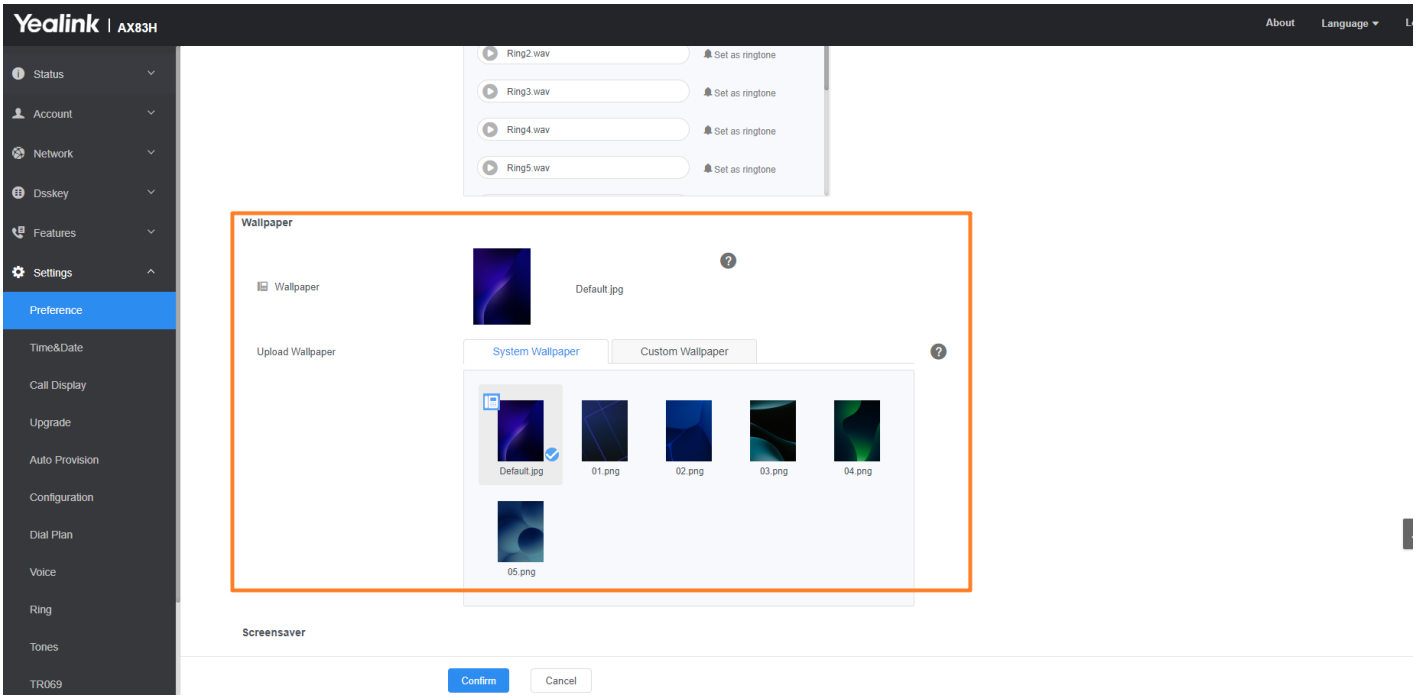
Configuration parameter

```
phone_setting.backgrounds
```

Parameter	Description	Permitted Values	Default
phone_setting.backgrounds	It configures the wallpaper displayed on the phone idle screen.	Default.jpg, 01.png, 02.png, 03.png, 04.png, 05.png or uploaded custom wallpaper name (for example, wallpaper.jpg)	Default.jpg

Set via the Web User Interface

On the web user interface，go to **Settings** > **Preference** > **Wallpaper**.



Wallpaper Customization

You can configure a custom picture, such as the company logo, and then upload the custom picture to the IP phone that users can choose from when changing the wallpaper for the phone idle screen, expansion module or Dsskey screen.

Custom Wallpaper Picture Limit

Either the smaller or the larger picture will be scaled proportionally to fit the screen. The wallpaper picture format must meet the following:

Phone Model	Format	Resolution	Single File Size	Note

AX83H	*.jpg/*.png/*.bmp/*.jpeg	<=2 megapixels	<=5MB	2MB of space should be reserved for the phone

Custom Wallpaper Configuration

The following table lists the parameter you can use to upload a custom picture.

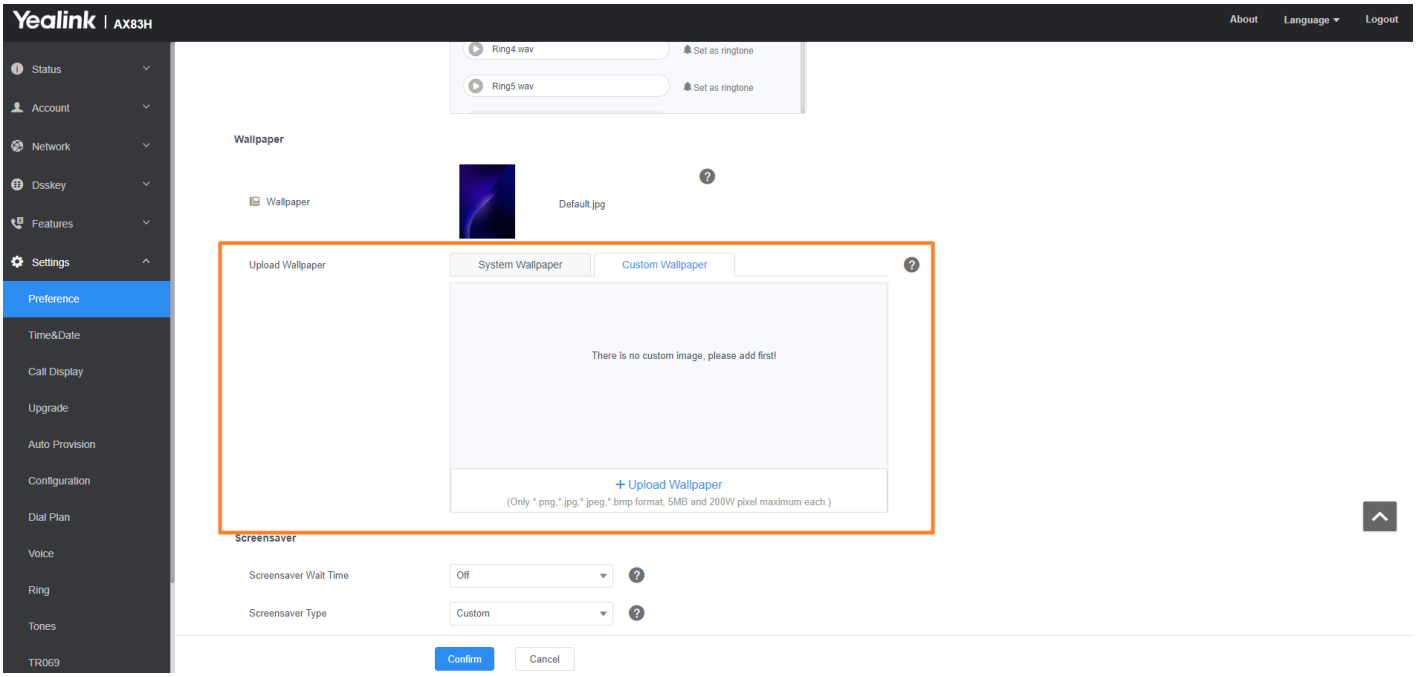
Configuration parameter

wallpaper_upload.url

Parameter	Description	Permitted Values	Default
wallpaper_upload.url	It configures the access URL of the custom wallpaper picture.	URL within 511 characters	Blank

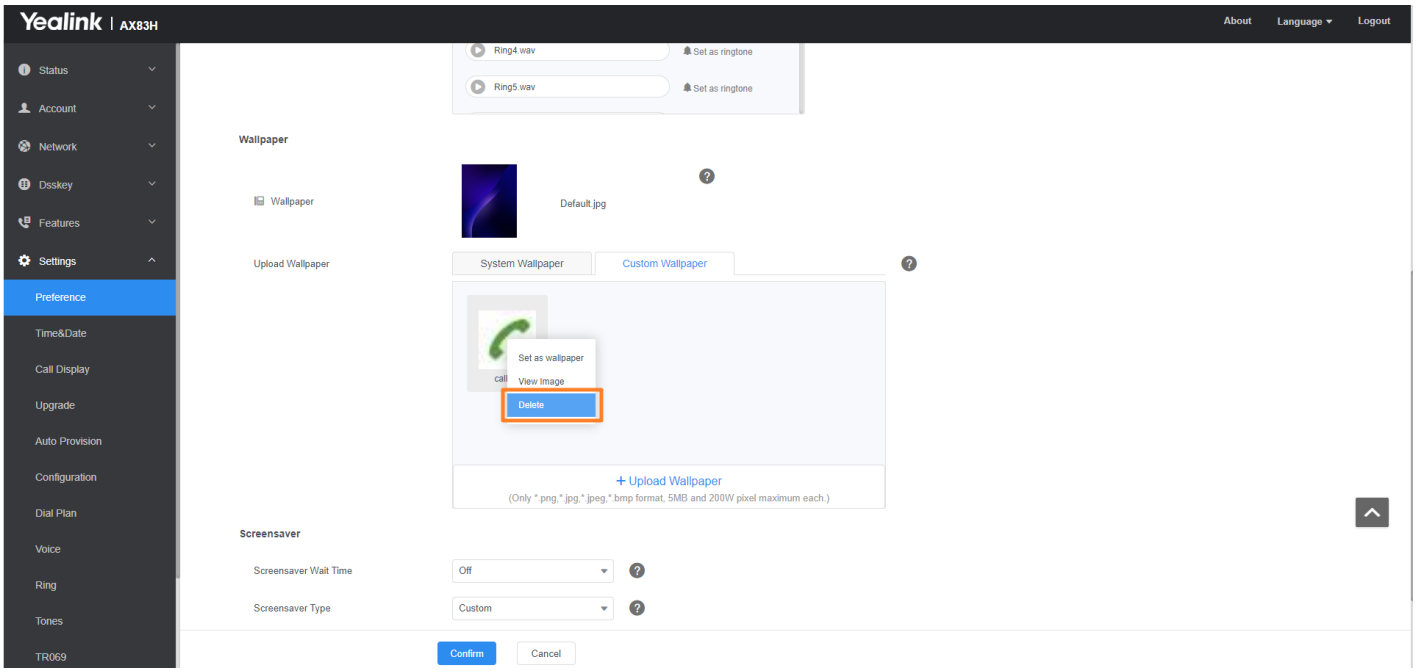
Set via the Web User Interface

On the web user interface, go to **Settings** > **Preference** > **Upload Wallpaper** > **Custom Wallpaper** > **Upload Wallpaper**.



Deleting a Custom Picture

You can delete the uploaded custom pictures for a specific IP phone via the web user interface at the path: **Settings** > **Preference** > **Wallpaper (Settings** > **Preference** > **Wallpaper** > **Upload Wallpaper** > **Custom Wallpaper)**, select the desired custom picture and click Del (Delete).



Example: Setting a Custom Picture as Wallpaper

The following example shows the configuration for uploading a custom picture named "wallpaper.jpg" and setting it as idle screen wallpaper. The custom picture is placed on the provisioning server "192.168.10.25".

Example

```
wallpaper_upload.url = http://192.168.10.25/wallpaper.jpg

phone_setting.backgrounds = wallpaper.jpg
```

After provisioning, the phone idle screen wallpaper changes to a custom picture "wallpaper.jpg".

Example

```
wallpaper_upload.url = http://192.168.10.25/wallpaper.jpg

phone_setting.backgrounds = wallpaper.jpg
```

After provisioning, the phone idle screen wallpaper changes to a custom picture "wallpaper.jpg".

Customization of Com Version and MAC Version

Customization of "Com Version" and "MAC Version"

In version V86, Yealink IP Phone devices have added the customization feature for "Com Version" and "MAC Version". This feature is solely used for modifying the display and serves no other purpose.

Configuration parameter

```
phone_setting.config_version.com
phone_setting.config_version.mac
```

Parameter	Description	Default
phone_setting.config_version.com	Used to modify the Com version displayed on the Status > Phone interface.	Blank
phone_setting.config_version.mac	Used to modify the Mac version displayed on the Status > Phone interface.	Blank

Input Method

Input Method

You can customize the existing keypad input method for the phones

Keypad Input Method File Customization

You can first customize the Yealink-supplied keypad input method file “ime.txt”, “Russian_ime.txt” or “Hebrew_ime.txt”, and then download it to the IP phone. The changes in the “Russian_ime.txt” file becomes effective when the language is set to Russian. If you want to customize the input method for all languages, the input method file must be named as "custom_ime.txt" (case-sensitive).
Yealink phones support 6 input methods: 2aB, abc, Abc, 123, ABC, and Hebrew.

ⓘ NOTE
By default, the Hebrew input method is hidden, the phone will automatically use the Hebrew input method when the language is set to Hebrew. The changes in the “Hebrew_ime.txt” file becomes effective when the language is set to Hebrew.

You can ask the distributor or Yealink FAE for keypad input method file. You can also refer to the following template:

```
[2aB]
1 = "1"
2 = "2abcABC"
3 = "3defDEF"
4 = "4ghiGHI"
5 = "5jklJKL"
6 = "6mnoMNO"
7 = "7pqrsPQRS"
8 = "8tuvTUV"
9 = "9wxyzWXYZ"
0 = "0"
* = "*.,'?!\-()@/:_;+&%=<>£$¥¤[]{}~^¡¿§#"|"
# = "#"
```

```
[abc]
1 = ""
2 = "abc2äæåàáâãç"
3 = "def3èéêëð"
4 = "ghi4ìíîï"
5 = "jkl5£"
6 = "mno6öøòóôõñ"
7 = "pqrs7ßS"
8 = "tuv8ùúûü"
9 = "wxyz9ýÞ"
0 = " "
* = "*.,'?!\-()@/:_;+&%=<>£$¥¤[]{}~^¡¿§#"|"
# = "#"

[Abc]
1 = ""
2 = "abc2äæåàáâãç"
3 = "def3èéêëð"
4 = "ghi4ìíîï"
5 = "jkl5£"
6 = "mno6öøòóôõñ"
7 = "pqrs7ßS"
8 = "tuv8ùúûü"
9 = "wxyz9ýÞ"
0 = " "
* = "*.,'?!\-()@/:_;+&%=<>£$¥¤[]{}~^¡¿§#"|"
# = "#"

[ABC]
1 = ""
2 = "ABC2ÄÆÅÀÁÂÃÇ"
3 = "DEF3ÈÉÊËÐ"
4 = "GHI4ÌÍÎÏ"
5 = "JKL5£"
6 = "MNO6ÖØÒÓÔÕÑ"
7 = "PQRS7S"
8 = "TUV8ÙÚÛÜ"
9 = "WXYZ9ÝÞ"
0 = " "
* = "*.,'?!\-()@/:_;+&%=<>£$¥¤[]{}~^¡¿§#"|"
# = "#"

[123]
1 = "1"
2 = "2"
3 = "3"
4 = "4"
5 = "5"
6 = "6"
7 = "7"
8 = "8"
9 = "9"
0 = "0"
* = ".*:/@[]"
# = "#"

[123_Dial]
1 = "1"
2 = "2"
3 = "3"
```

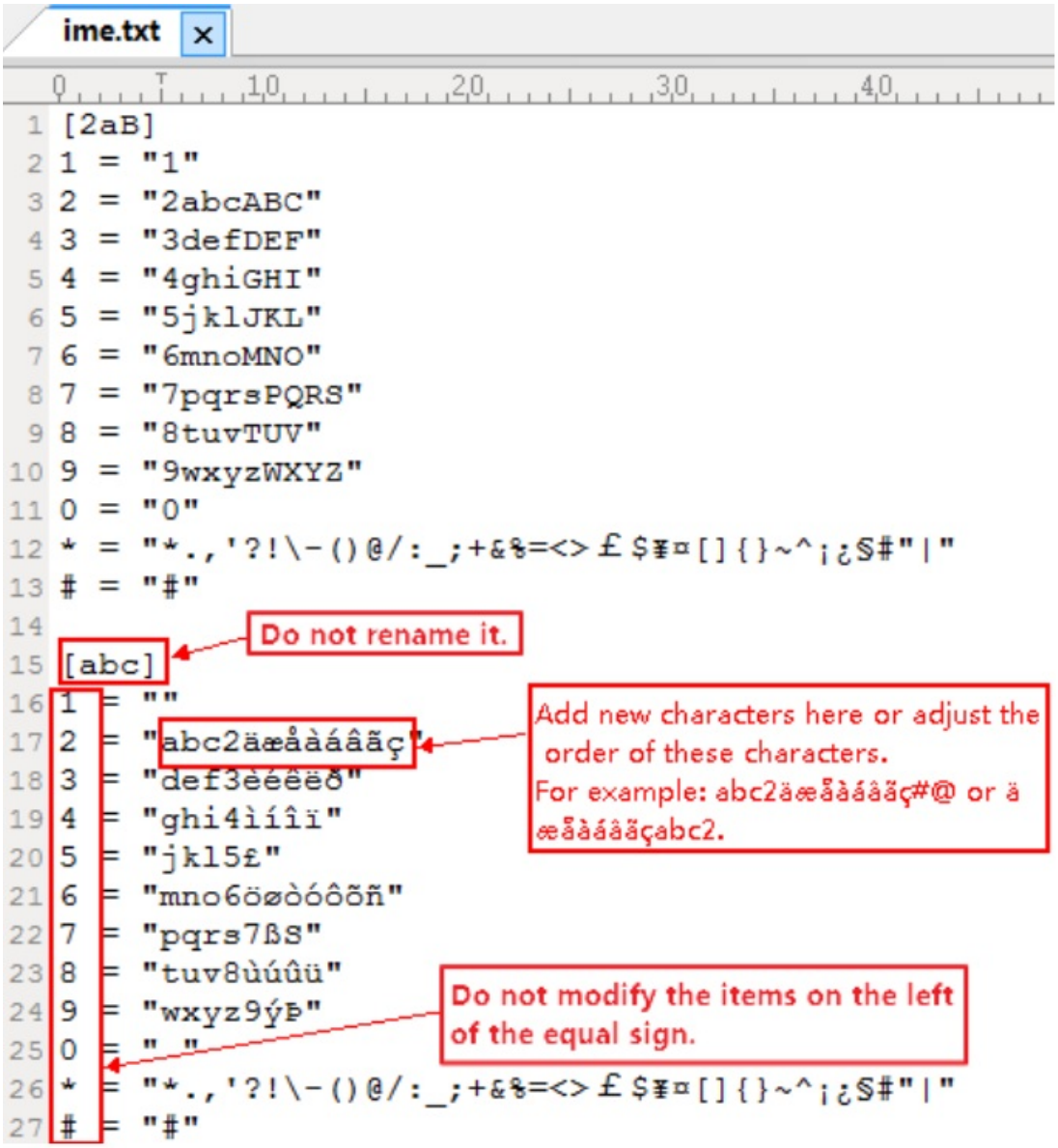
```
4 = "4"
5 = "5"
6 = "6"
7 = "7"
8 = "8"
9 = "9"
0 = "0"
* = "*"
# = "#"


[2aB_PWD]
1 = "1"
2 = "2abcABC"
3 = "3defDEF"
4 = "4ghiGHI"
5 = "5jklJKL"
6 = "6mnoMNO"
7 = "7pqrsPQRS"
8 = "8tuvTUV"
9 = "9wxyzWXYZ"
0 = "0"
* = "*.,'?!\-()@/:_;+&%=<>£$¥¤[]{}~^¡¿§#"|"
# = "#"

[abc_PWD]
1 = ""
2 = "abc2äæåàáâãç"
3 = "def3èéêëð"
4 = "ghi4ìíîï"
5 = "jkl5£"
6 = "mno6öøòóôõñ"
7 = "pqrs7ßS"
8 = "tuv8ùúûü"
9 = "wxyz9ýÞ"
0 = " "
* = "*.,'?!\-()@/:_;+&%=<>£$¥¤[]{}~^¡¿§#"|"
# = "#"

[ABC_PWD]
1 = ""
2 = "ABC2ÄÆÅÀÁÂÃÇ"
3 = "DEF3ÈÉÊËÐ"
4 = "GHI4ÌÍÎÏ"
5 = "JKL5£"
6 = "MNO6ÖØÒÓÔÕÑ"
7 = "PQRS7S"
8 = "TUV8ÙÚÛÜ"
9 = "WXYZ9ÝÞ"
0 = " "
* = "*.,'?!\-()@/:_;+&%=<>£$¥¤[]{}~^¡¿§#"|"
# = "#"

[123_PWD]
1 = "1"
2 = "2"
3 = "3"
4 = "4"
5 = "5"
6 = "6"
7 = "7"
```

```
8 = "8"
9 = "9"
0 = "0"
* = ".*:/@[]"
# = "#"
```

Customizing the Keypad Input Method File

When adding new characters for the existing input method, ensure that the added characters are supported by the phones. The IP phone can only recognize the keypad input method files uploaded using Unicode encoding.

1. Open the desired keypad input method file (for example, ime.txt).
2. Under the input method field (for example, [abc]), add new characters or adjust the order of the characters within the double quotation marks on the right of the equal sign.



3. Save the keypad input method file.
4. Rename the input method file (for example, custom_ime.txt), and place it to the provisioning server.

NOTE
If you just want to customize the input method for a certain language, the file name must be "language name_ime.txt" (for example, German_ime.txt). The valid language names are: English, Chinese_S, Chinese_T, French_CA, French, German, Italian, Polish, Portuguese, Portuguese_LA, Spanish, Spanish_LA, Turkish and Russian

Input Method Configuration

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

Configuration parameter

```
gui_input_method.url
gui_input_method.delete
default_input_method.dialing
directory.edit_default_input_method
directory.search_default_input_method
```

Parameter	Description	Permitted Values	Default
gui_input_method.url	It configures the access URL of the custom keypad input method file for the phone user interface. Example: gui_input_method.url = http://192.168.10.25/custom_ime.txt During the auto provisioning process, the phone connects to the provisioning server "192.168.1.25", and downloads the custom keypad input method file "custom_ime.txt". gui_input_method.url = http://192.168.10.25/Russian_ime.txt During auto provisioning, the phone connects to the provisioning server "192.168.1.25", and downloads the custom keypad input method file "Russian_ime.txt" for the Russian language. **NOTE** If you want to upload a custom keypad input method file for the desired language, you can name the file "language name_ime.txt". The valid language names are: English, Chinese_S, Chinese_T, French_CA, French, German, Italian, Polish, Portuguese, Portuguese_LA, Spanish, Spanish_LA, Turkish and Russian.	URL within 511 characters	Blank

gui_input_method.delete	It deletes the specified or all custom keypad input method files of the phone user interface. Delete all custom keypad input method files: gui_input_method.delete = http://localhost/all Delete a custom keypad input method file (for example, custom_ime.txt) for the phone: gui_input_method.delete = http://localhost/custom_ime.txt	http://localhost/all or http://localhost/Name.txt	Blank
default_input_method.dialing	It configures the default input method in the dialing screen.	0-2aB 1-123 2-abc 3-ABC	1
directory.edit_default_input_method	It configures the default input method when the user edits contacts in the Local Directory, LDAP, Remote Phone Book, Blocklist or Network Directory.	Abc, 2aB, 123, abc, ABC or Hebrew Note: By default, the Hebrew input method is hidden, the phone will automatically use the Hebrew input method when the language is set to Hebrew.	Abc
directory.search_default_input_method	It configures the default input method when the user searches for contacts in the Local Directory, LDAP, Remote Phone Book, Blocklist or Network Directory.	Abc, 2aB, 123, abc or ABC	Abc
default_input_method.xml_browser_input_screen	It configures the default input method when the type for the input box is set to “string” in the InputScreen object.	Abc, 2aB, 123, abc or ABC	2aB

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

Example: Configuring the French Onscreen Keyboard Input Method

The following example shows the configuration for configuring the French onscreen keyboard input method. Customize the onscreen keyboard input method files “keyboard_lang.xml”, "keyboard_ime_francais.xml", "keyboard_ime_num.xml", "keyboard_layout_francais.xml", "keyboard_layout_2.xml" and place these files to the provisioning server “http://192.168.10.25”.

Example

phone_setting.virtual_keyboard.enable = 1

gui_onscreen_keyboard.url = http://192.168.10.25/keyboard_lang.xml

gui_onscreen_keyboard.url = http://192.168.10.25/keyboard_ime_francais.xml

gui_onscreen_keyboard.url = http://192.168.10.25/keyboard_ime_num.xml

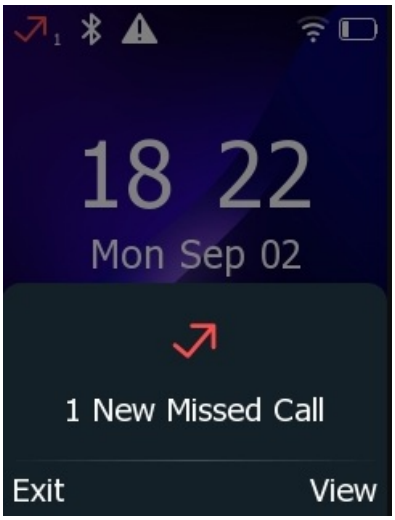
gui_onscreen_keyboard.url = http://192.168.10.25/keyboard_layout_francais.xml

gui_onscreen_keyboard.url = http://192.168.10.25/keyboard_layout_2.xml
After provisioning, you can use the French onscreen keyboard for entering information.

Notification

Notification Popups

The notification popups feature allows the IP phone to pop up the message when it misses a call, forwards an incoming call to another party, or receives a new voice mail or a new text message.
The following shows an example of receiving a new missed call:



Notification Popups Configuration

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

Configuration parameter

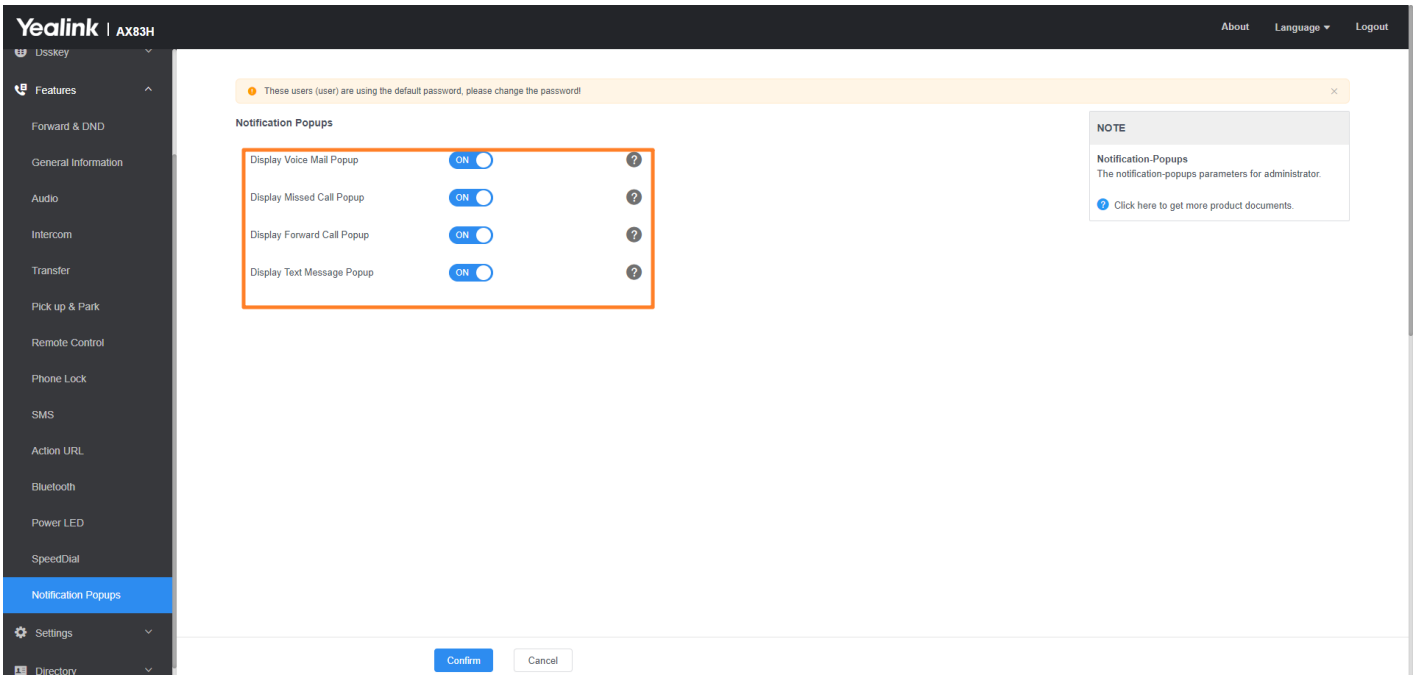
```
features.voice_mail_popup.enable
features.missed_call_popup.enable
features.forward_call_popup.enable
features.text_message_popup.enable
```

Parameter	Description	Permitted Values	Default

features.voice_mail_popup.enable	It enables or disables the phone to pop up the message when it receives a new voice mail. If the message disappears, it will not pop up again unless the phone receives a new voice mail or the user re-registers the account that has unread voice mail(s). **NOTE** It works only if "account.X.display_mwi.enable" is set to 1 (Enabled).	0-Disabled 1-Enabled	1
features.missed_call_popup.enable	It enables or disables the phone to pop up the message when it misses a call. **NOTE** It works only if "account.X.missed_calllog" is set to 1 (Enabled).	0-Disabled 1-Enabled	1
features.forward_call_popup.enable	It enables or disables the phone to pop up the message when it forwards an incoming call to another party.	0-Disabled 1-Enabled	1
features.text_message_popup.enable	It enables or disables the phone to pop up the message when it receives a new text message. **NOTE** It works only if "features.text_message.enable" is set to 1.	0-Disabled 1-Enabled	1

Set via the Web User Interface

On the web user interface, go to **Features** > **Notification Popups**



Power LED Indicator

Power LED indicator indicates the power status and phone status.

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

- The IP phone receives an incoming call
- The IP phone receives a voice mail or a text message
- A call is muted
- A call is placed on hold or is held
- The IP phone is busy
- The IP phone misses a call

Power LED Indicator Configuration

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

Configuration parameter

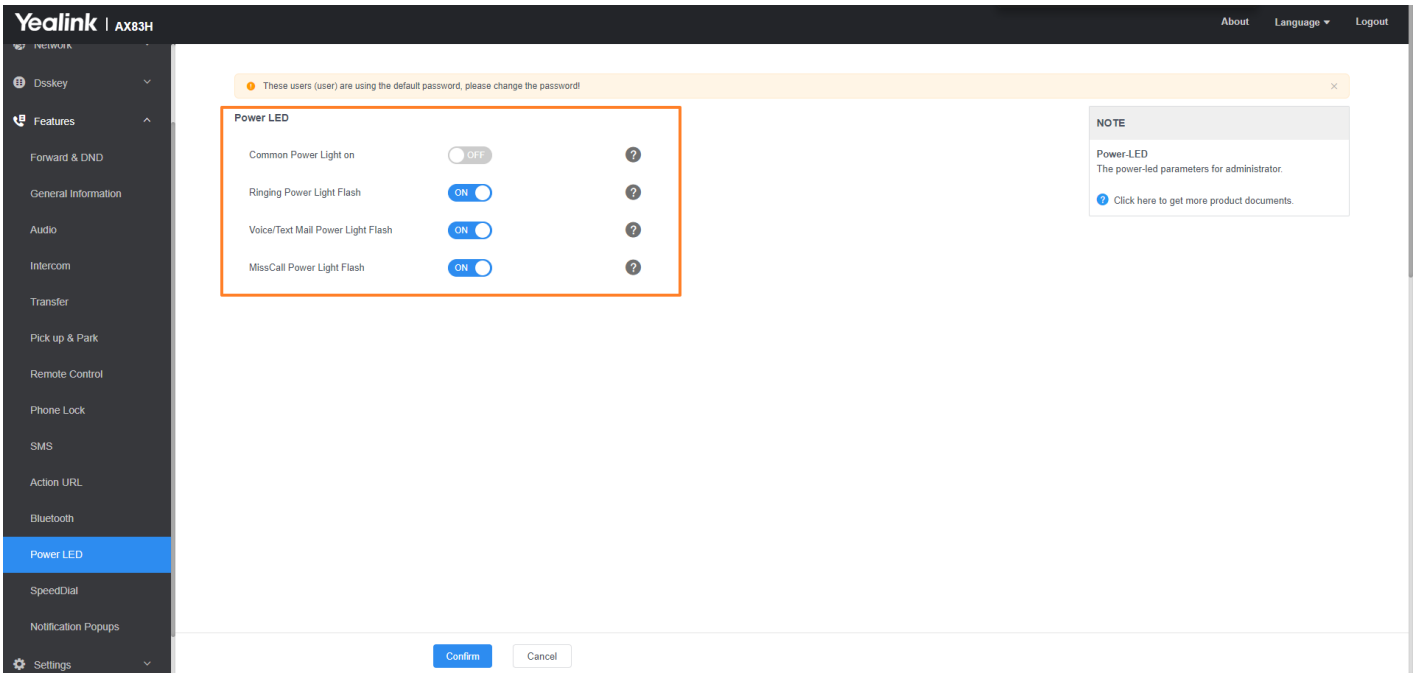
```
phone_setting.common_power_led_enable
phone_setting.ring_power_led_flash_enable
phone_setting.mail_power_led_flash_enable
phone_setting.missed_call_power_led_flash.enable
phone_setting.autop_led_flash_enable
```

Parameter	Description	Permitted Values	Default
phone_setting.common_power_led_enable	It enables or disables the power LED indicator to be turned on.	0-Disabled (power LED indicator is off) 1-Enabled (power LED indicator glows red) For T19 § E2 phones: 0-Disabled (power LED indicator is off) 1-Enabled (power LED indicator glows yellow)	0

phone_setting.ring_power_led_flash_enable	It enables or disables the power LED indicator to flash when the phone receives an incoming call.	0-Disabled (power LED indicator does not flash) 1-Enabled (power LED indicator fast flashes (0.3s) red) For T19 § E2 phones: 0-Disabled (power LED indicator does not flash) 1-Enabled (power LED indicator fast flashes (0.3s) yellow)	1
phone_setting.mail_power_led_flash_enable	It enables or disables the power LED indicator to flash when the phone receives a voice mail or a text message. Note: It works only if "account.X.display_mwi.enable" is set to 1 (Enabled).	0-Disabled (power LED indicator does not flash) 1-Enabled (power LED indicator slowly flashes (1s) red) 2-Enabled (if there are unread voice mails or text messages, the power LED indicator slowly flashes (1s) red) even when the phone is busy, but value set by "phone_setting.talk_and_dial_power_led_enable" has a higher priority.) For T19 § E2 phones: 0-Disabled (power LED indicator does not flash) 1-Enabled (power LED indicator slowly flashes (1s) yellow) 2-Enabled (if there are unread voice mails or text messages, the power LED indicator slowly flashes (1s) yellow even when the phone is busy, but value set by "phone_setting.talk_and_dial_power_led_enable" has a higher priority.)	1
phone_setting.missed_call_power_led_flash.enable	It enables or disables the power LED indicator to flash when the phone misses a call.	0-Disabled (power LED indicator does not flash) 1-Enabled (power LED indicator slowly flashes (1s) red) For T19 § E2 phones: 0-Disabled (power LED indicator does not flash) 1-Enabled (power LED indicator slowly flashes (1s) yellow)	1
phone_setting.autop_led_flash_enable	It enables or disables the power LED indicator to flash when the phone performs an auto provisioning.	0-Disabled, auto provisioning does not change the LED status (that is, the original LED status will be kept). 1-Enabled, during auto provisioning, the power LED indicator flashes at a fixed frequency.	1

Set via the Web User Interface

On the web user interface, go to **Features** > **Power LED**.



Bluetooth

Bluetooth

You can pair and connect a Bluetooth headset with the phone.

Bluetooth Configuration

You can activate or deactivate the Bluetooth mode and personalize the Bluetooth device name for the IP phone. The pre-configured Bluetooth device name will be displayed in a scanning list of other devices. It is helpful for the other Bluetooth devices to identify and pair with your phone.
The following table lists the parameters you can use to configure Bluetooth.

Configuration parameter

```
static.bluetooth.function.enable
features.bluetooth_enable
features.bluetooth_adapter_name
bluetooth.connect_confirm.enable
bluetooth.connect_confirm.enable
bluetooth.high_encryption.enable
```

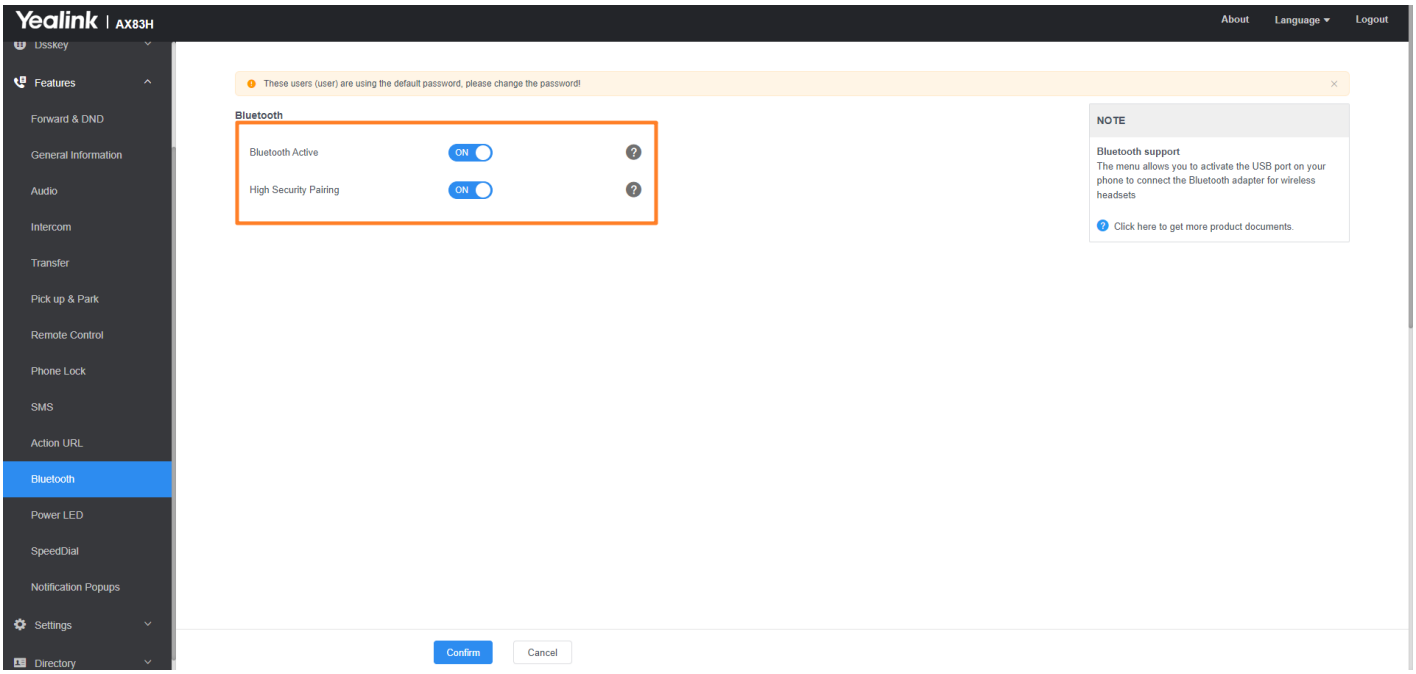
Parameter	Description	Permitted Values	Default
static.bluetooth.function.enable[1]	It enables or disables the Bluetooth feature.	0-Disabled, you are not allowed to trigger Bluetooth mode to on. 1-Enabled	1

features.bluetooth_enable	It triggers the Bluetooth mode to on or off. **NOTE** It works only if "static.bluetooth.function.enable" is set to 1 (Enabled).	0-Off 1-On	0
features.bluetooth_adapter_name	It configures the Bluetooth device name. **NOTE** It works only if "features.bluetooth_enable" is set to 1 (On).	String within 64 characters	Yealink-$DEV
bluetooth.connect_confirm.enable [1]	It enables or disables the phone to prompt users to confirm the connection request from the Bluetooth device.	0-Disabled 1-Enabled, the prompt will not appear during the call.	0
bluetooth.connect_confirm.enable [1]	It enables or disables the phone to prompt users to confirm the connection request from the Bluetooth device.	0-Disabled 1-Enabled, the prompt will not appear during the call.	0
bluetooth.high_encryption.enable	It enables or disables the minimum password strength limit.	0-Disabled 1-Enabled, when the Bluetooth device is paired with the phone, the minimum password strength cannot be lower than 56bits.	1

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

Set via the Web User Interface

On the web user interface, go to **Features** > **Bluetooth**.



Handset/Headset/Speakerphone Mode

Handset/Speakerphone Mode

Yealink phones support three ways to place/answer a call: using the handset, headset, or speakerphone. You can disable the infrequently used audio device as required.

Handset/Speakerphone Mode Configuration

The following table lists the parameters you can use to configure handset/headset/speakerphone mode.

Configuration parameter

```
features.speaker_mode.enable
features.handset_mode.enable
features.headset_mode.enable
phone_setting.headsetkey_mode
```

Parameter	Description	Permitted Values	Default
features.speaker_mode.enable	It enables or disables the phone’s speakerphone mode.	0-Disabled 1-Enabled	1
features.handset_mode.enable	It enables or disables the phone’s handset mode.	0-Disabled 1-Enabled	1

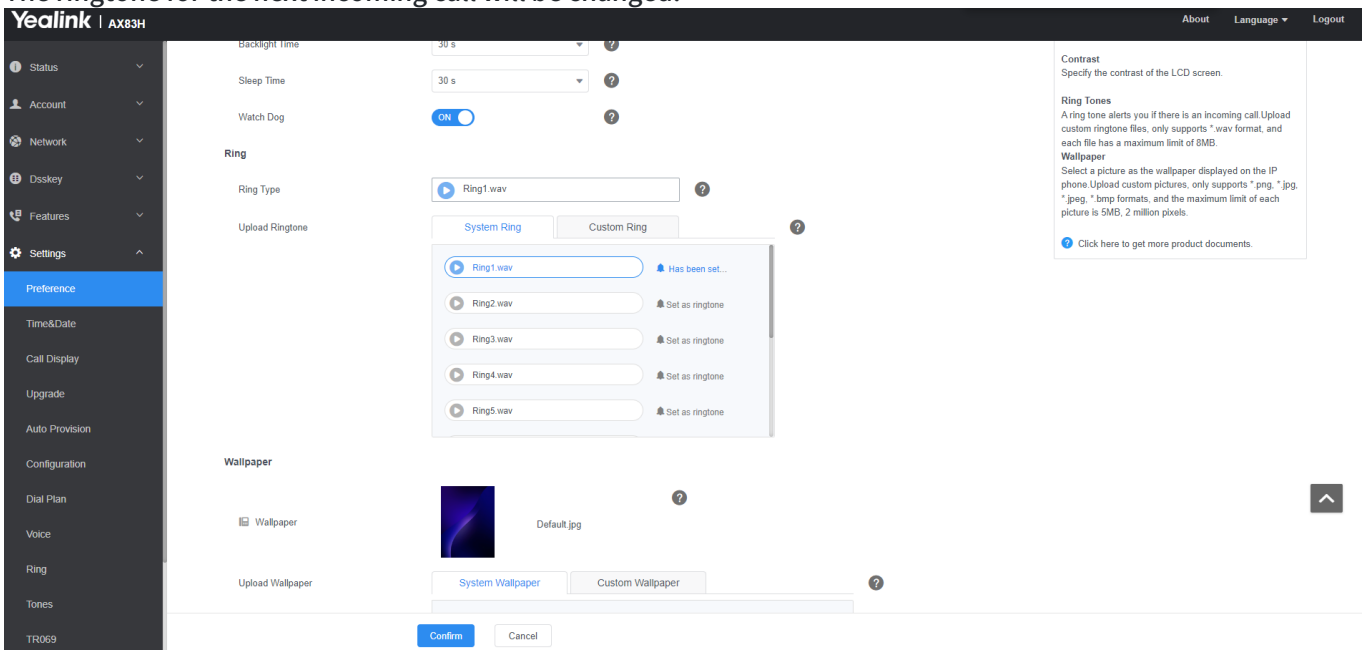
features.headset_mode.enable	It enables or disables the phone’ s headset mode.	0-Disabled 1-Enabled	1
phone_setting.headsetkey_mode	It configures headset mode during a call.	0-Always use (pressing the Speakerphone key and picking up the handset are not effective when the headset mode is activated) 1-Use as normal	1

Ring Tone

Our phone only supports *.wav format. And the ring tone file must be in PCMU/PCMA audio format, mono channel. 8K sample rate and 16-bit resolution.
(Only *.wav format, 8MB maximum each)

ⓘ NOTE
Only *.wav format, 8MB maximum each.

1. On the web user interface, go to **Settings** > **Preference** > **Ring**.
2. Click **Upload Ringtong** to upload your custom ringtone files, and click **Set as ringtone**.
3. Confirm the change.
   The ringtone for the next incoming call will be changed.



No Perception Upgrade

Firmware Upgrade

We support no perception upgrade and you can download the phone firmware on the web user interface or via auto provision.

NOTE

- We recommend that the devices running the latest firmware should not be downgraded to an earlier firmware version. The new firmware is compatible with old configuration parameters and vice versa.
- Downgrading will result in some configurations being cleared, so please restore the factory settings after downgrading before using the device again.

Firmware Downloading

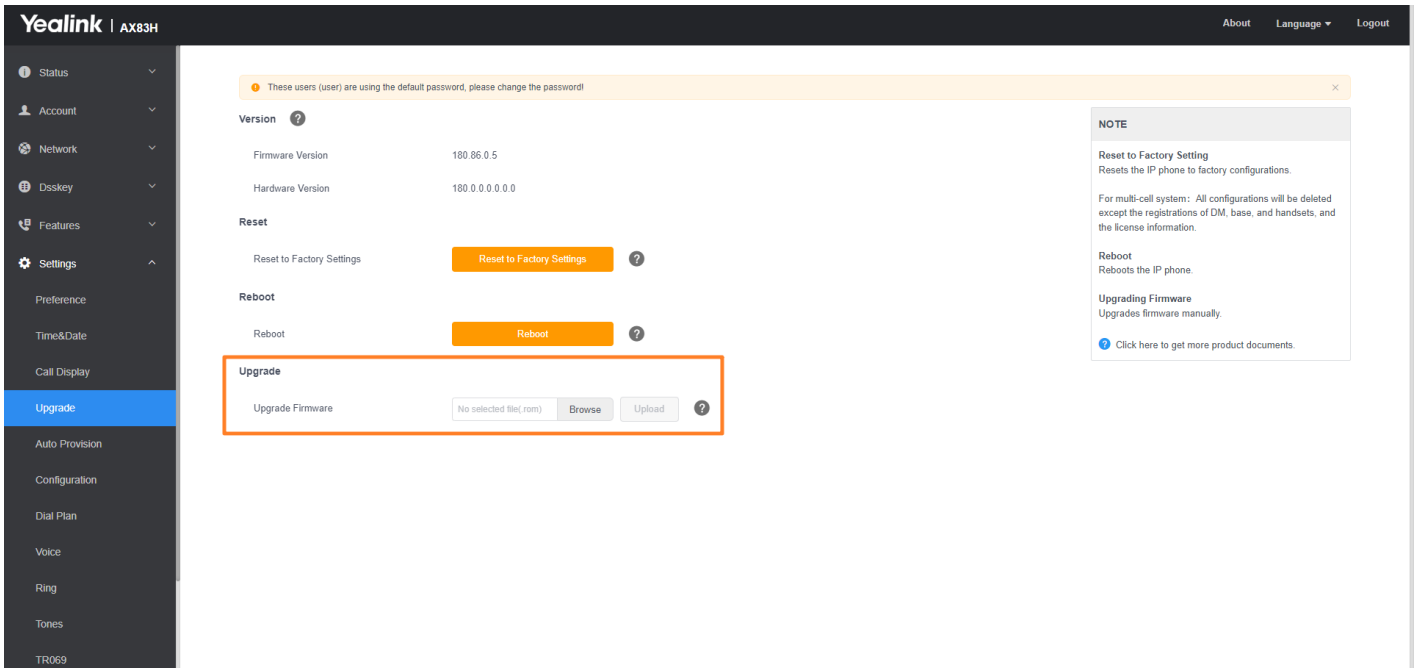
You can download the latest firmware online:
http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage.

Firmware Upgrading

NOTE
Do not close and refresh the browser when the device is upgrading firmware via the web user interface.

1. Do one of the following to download the firmware to the system:
   - Set via the Web User Interface

   On the web user interface, go to **Settings** > **Upgrade** > **Upgrade Firmware**.



- Auto Provisioning

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

```
static.firmware.url
```

Parameter	Description	Permitted Values	Default
static.firmware.url	It configures the access URL of the firmware file.	URL within 511 characters	Blank

2. After the system upgrade is complete, the phone will prompt you to confirm whether to upgrade immediately (if the phone is in a call, it will wait until the call ends). The prompt will count down for 20 seconds. If you do not take any action before the countdown ends, the system will automatically start the upgrade.

   NOTE
   During the countdown, if the phone receives a new call, the countdown in the pop-up window will be interrupted. After the call ends, the pop-up window will reappear and the countdown will restart.

3. If you decline the immediate upgrade, a new warning will appear, indicating that the current version is outdated and needs to be upgraded to the new version.

   TIP
   - Under low battery conditions, the firmware cannot be upgraded. A pop-up message will appear: Low battery, unable to upgrade.

Troubleshooting

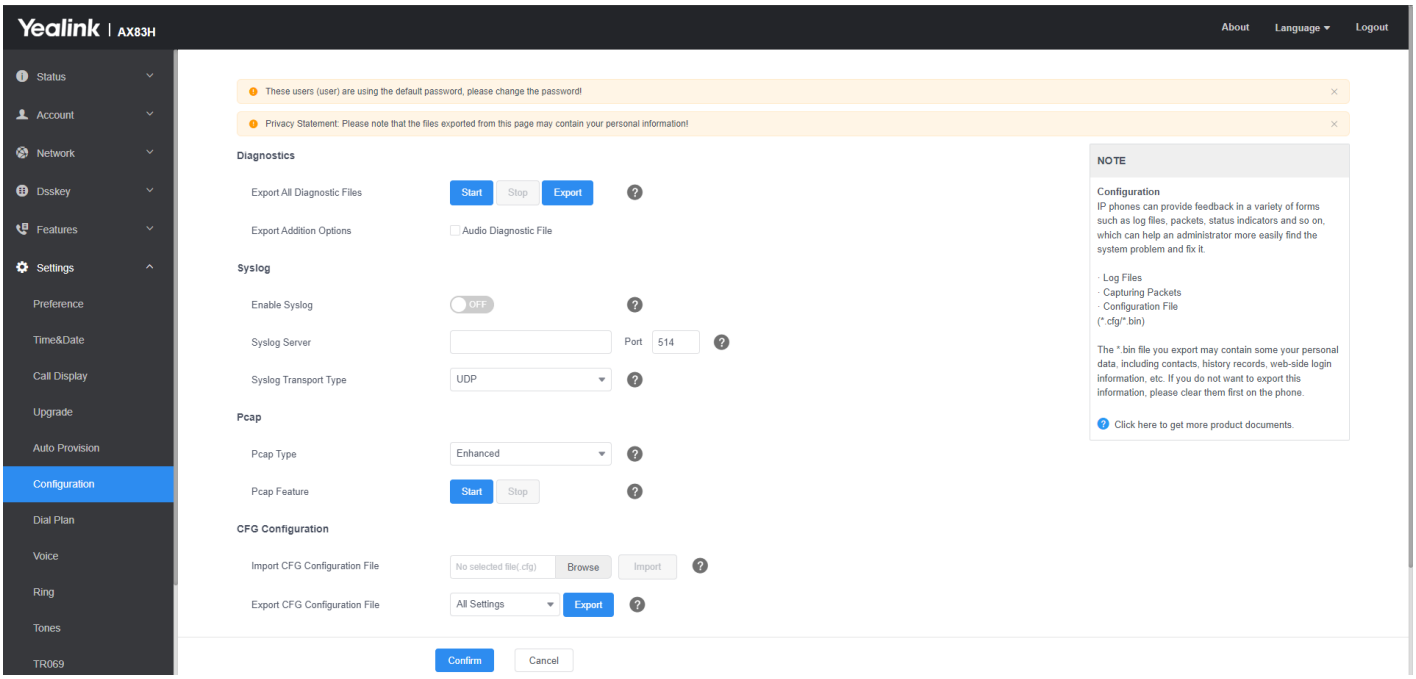
Get Start

Get Start

Before you start troubleshooting, it is important to understand the purpose of each file. This section provides an overview of the various diagnostic files and their use in different scenarios.

NOTE
When retrieving diagnostic information for troubleshooting, it is crucial to record the timestamp when the issue occurred and clearly communicate it to the technical support team.

The web path for diagnostic files is **Settings** > **Configuration**

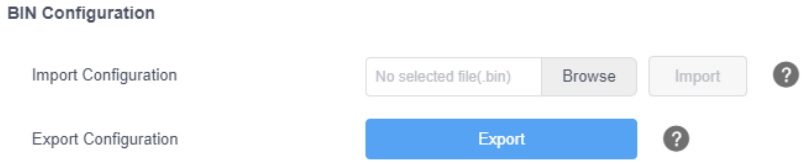


BIN Configuration

The bin file primarily stores the configuration information of the phone, which helps determine if the issue is caused by abnormal configuration parameters.

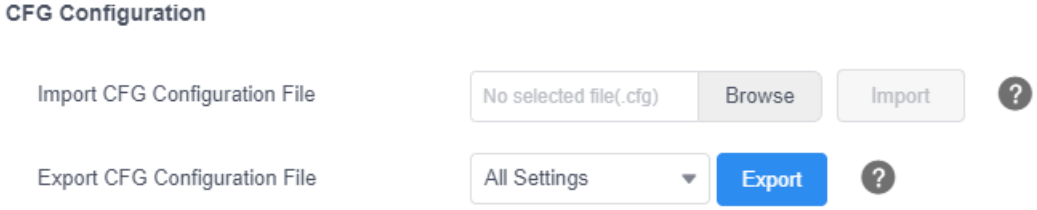
> **NOTE**
> The *.bin file you export may contain some of your personal data, including contacts, history records, web-side login information, etc. If you do not want to export this information, please clear them first on the phone.

You can choose to import or export bin files.



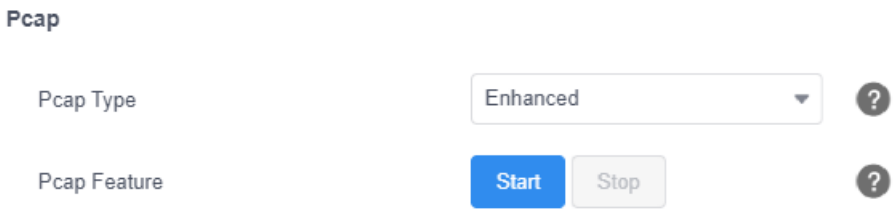
CFG Configuration

The cfg file configuration is mainly used for importing and exporting cfg type configuration files. This function is commonly used to import cfg files. Unlike bin files, this file does not include the default values of configuration parameters.



Pcap

The pcap file is one of the key files for analyzing call-related issues, such as audio quality problems, and no sound during calls. It is essential to provide the pcap file to Yealink for troubleshooting purposes.



Audio Diagnostic

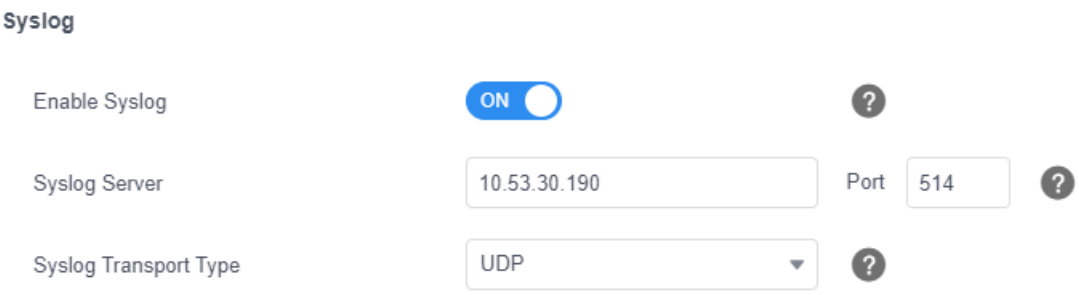
Audio Diagnostic is commonly used in conjunction with pcap files and is primarily used to diagnose the playback of speakers and the pickup of microphones. It helps to accurately pinpoint the root cause of audio issues.

Syslog

Syslog is different from the local log in that it transmits logs to a configured log server instead of storing them in the device's memory. It is primarily used to handle issues that occur over a longer period, upgrade failures, and faults that may cause device restarts.

- Enable Syslog: It enables or disables the phone to upload log messages to the syslog server in real-time.
- Syslog Server and port: It configures the IP address or domain name and port of the syslog server when exporting log to the syslog server.
- Syslog Transport Type: It configures the transport protocol that the IP phone uses when uploading log messages to the syslog server.

> ⓘ **NOTE**
> To capture syslog, please ensure that the Log Level is set to 6.



Export All Diagnostic Files

Export All Diagnostic Files Yealink phones support three types of diagnostic files (including Pcap trace, log files

(boot.log and sys.log), and BIN configuration files) to help analyze your problem. You can export these files at a time and troubleshoot if necessary. The file format of the exported diagnostic file is *.tar.The "Export All Diagnostic Files" feature can meet most of the log data requirements for troubleshooting purposes.
For detailed information, refer to Export All the Diagnostic Files.

Optimizing troubleshooting

Yealink has optimized the method of obtaining log files, starting from **x.86.0.112** (x corresponds to the specific device's common). The Diagnostics feature has been modified as follows:

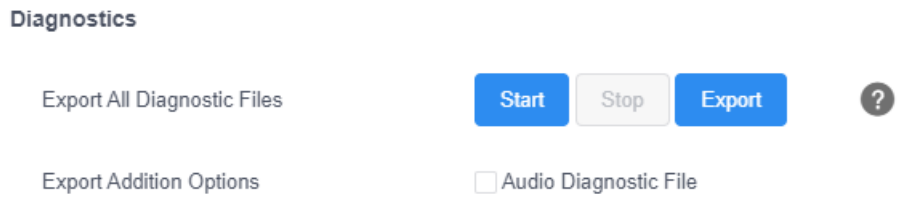
- The settings related to local log have been removed.
- The issue of being unable to obtain the Audio Diagnostic File along with the Export All Diagnostic Files has been resolved.

Here are the steps to use this feature:

1. Check the **Audio Diagnostic File** option.
2. Click **Start.** A file selection dialog box will appear on the web page. Please save it in a folder that is easy to locate.
3. Reproduce the issue.
4. After reproducing the issue, click **Stop** and export the files. Please send the .data file that was saved along with the other files to Yealink's technical support team.

NOTE

1. Please consult the Yealink documentation or contact their technical support for the exact procedure and any specific requirements.



Log Files

Introduction

Yealink phone can log events into two different log files: boot log and system log. You can send the log to a syslog server in real time, and use these log files to generate informational, analytic, and troubleshooting phones.
The following table lists the log files generated by the phone:

Local		Syslog Server	Description
	boot .log	< MAC >-boot.log	It can only log the last reboot events. It is required to report the logs with all severity levels.

< MAC >-all.tgz	sys.log	< MAC >-sys.log	It reports the logs with a configured severity level and the higher. For example, if you have set the severity level to 4, then the logs with a severity level of 0 to 4 will all be reported.

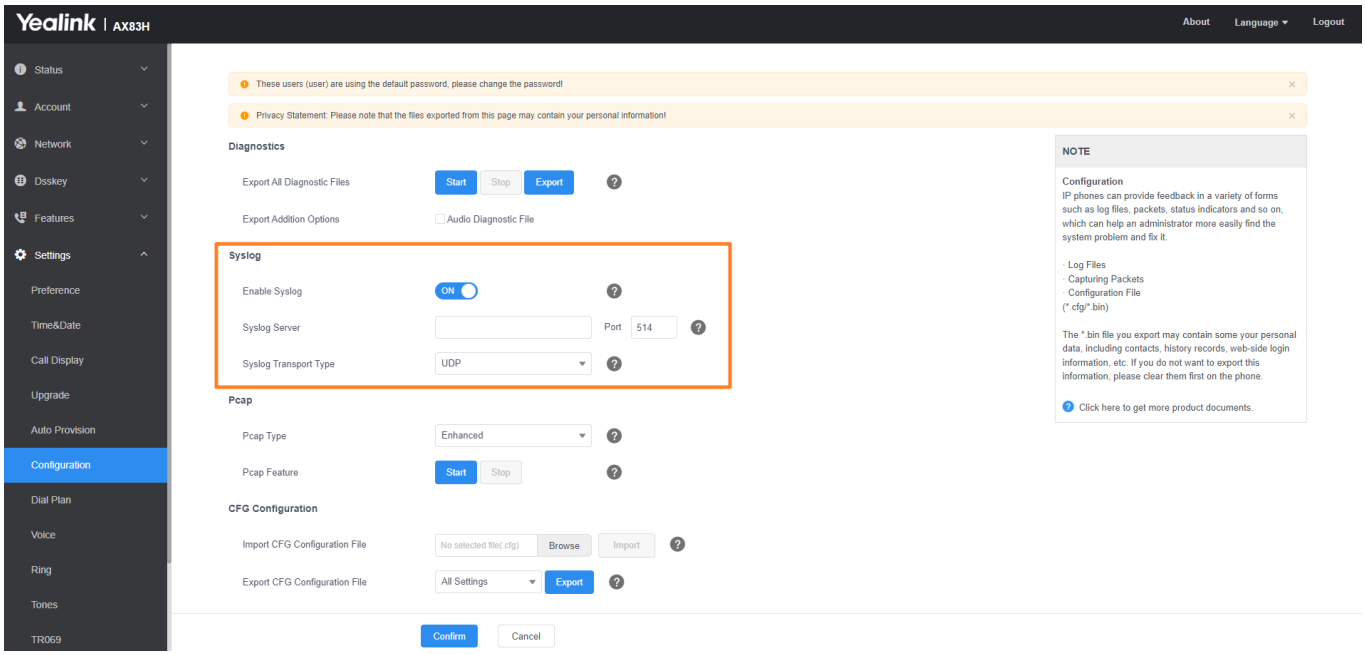
Syslog Logging

You can also configure the to send syslog messages to a syslog server in real time.
You can specify syslog details such as IP address or hostname, server type, facility, and the severity level of events you want to log. You can also choose to prepend the phone's MAC address to log messages.

Syslog Logging Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Configuration** > **Syslog**.



Auto Provisioning

```
static.syslog.enable
static.syslog.server
static.syslog.server_port
static.syslog.transport_type
```

Parameter	Permitted Values	Default	Description
static.syslog.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to upload log messages to the syslog server in real time.
static.syslog.server	String within 99 characters	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.
static.syslog.transport_type	**0**-UDP **1**-TCP **2**-TLS	0	It configures the transport protocol that the IP phone uses when uploading log messages 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， It could also be a txt document:

```
Jun 02 08:42:17 10.2.20.160 local0.notice Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: APP <5+notice> [SIP]    dtmf_payload    :101
Jun 02 08:42:17 10.2.20.160 local0.notice Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: APP <5+notice> [SIP]    version        :0
Jun 02 08:42:17 10.2.20.160 local0.notice Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: APP <5+notice> [SIP] call channels info
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+info > [000] cb_nict_kill_transaction (id=88)
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+info > [000] m=audio 7150 RTP/AVP 9 0 8 18 101
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+info > [000] Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY,
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+info > [000] CSeq: 4 INVITE
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+info > [000] Call-ID: ZWQ3MWM5ZDgwZDMyMmZjY2JkN2YyMzQ1NTJiNWI5Nzg.
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+info > [000] From: <sip:101@10.2.1.43:5060>;tag=4035593836
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+info > [000] To: "102" <sip:102@10.2.1.43:5060>;tag=8d378436
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+info > [000] Contact: <sip:102@10.2.1.43:5060>
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+info > [000] Via: SIP/2.0/UDP 10.2.20.160:5060;branch=z9hG4bK2209216293
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+info > [000] SIP/2.0 200 OK
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+info > [000]
Jun 02 08:42:17 10.2.20.160 local0.notice Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+notice> [000] Message recv: (from src=10.2.1.43:5060 len=808)
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: SIP <5+info > [SIP] match line:name:101 host:10.2.1.43
Jun 02 08:42:17 10.2.20.160 local0.notice Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: NET <5+notice> [255] <<<<=== UDP socket 10.2.1.43:5060: read 808 bytes
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: SUA <5+info > [000] ****eCore event:(0x0010)ECORE_CALL_PROCEEDING ****
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+info > [000]
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:43 [00:15:65:74:b1:50] sua [845]: DLG <5+info > [000]
```

NOTE
Usually, when exporting syslog, it is recommended to also export the Bin file. Along with exporting syslog, please try to provide the local log and Bin file synchronously if possible.

Packets Capture

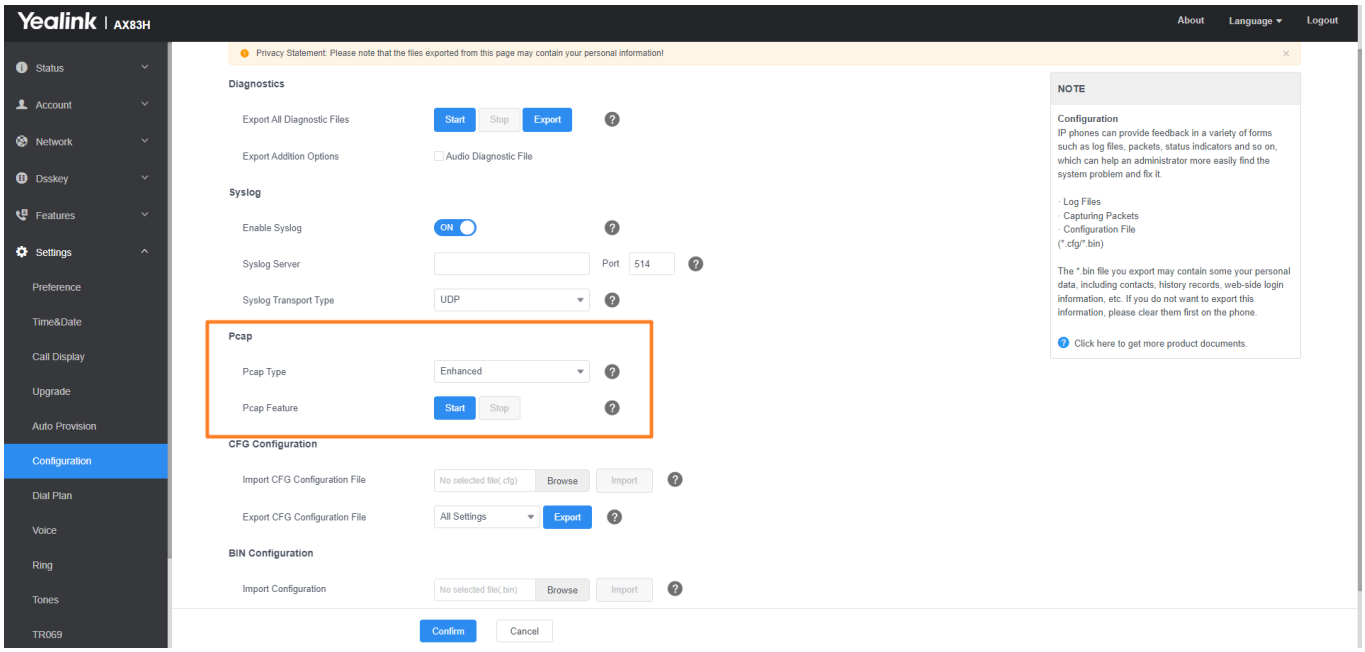
Introduction

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

Capture the Packets via Web User Interface

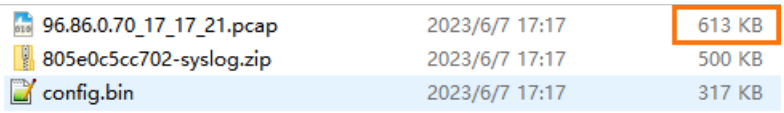
For Yealink phones, you can export the packets file to the local system and analyze it.
Procedure

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



Please Check

Please ensure that the PCAP data is valid. Typically, the PCAP size should not be lower than 100KB. You can make an initial assessment of the file's validity based on its size.



Reset to Factory Settings

Introduction

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

You can reset the phone to default factory configurations. The default factory configurations are the settings that reside on the phone after it has left the factory.

You can also reset the phone to custom factory configurations if required. The custom factory configurations are

the settings defined by the user to keep some custom settings after resetting. You have to import the custom factory configuration files in advance.

NOTE

The **Reset local settings**/**Reset non-static settings**/**Reset static settings**/**Reset userdata & local config** option on the web user interface appears only if `static.auto_provision.custom.protect` is set to 1.

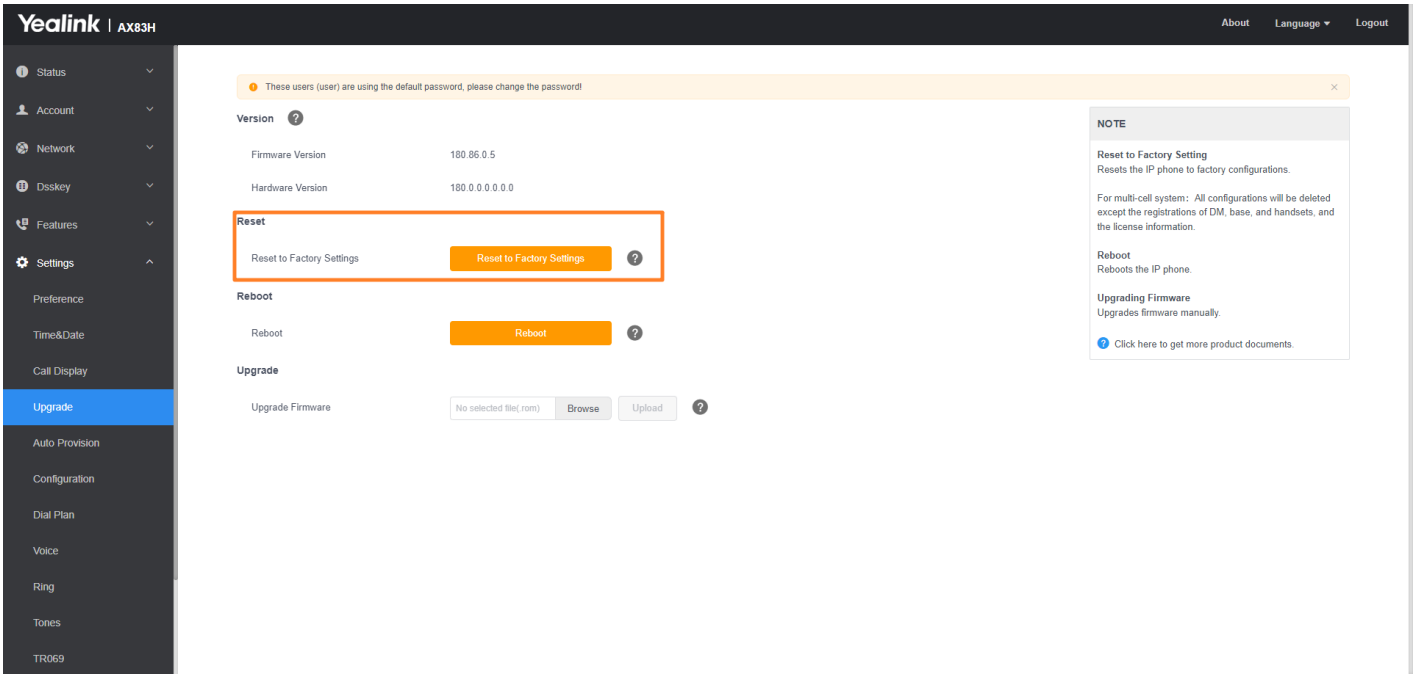
Reset the Phone to Default Factory Settings

Procedure

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

NOTE

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



Analyze Configuration Files

Introduction

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

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

Export CFG Configuration Files from Phone

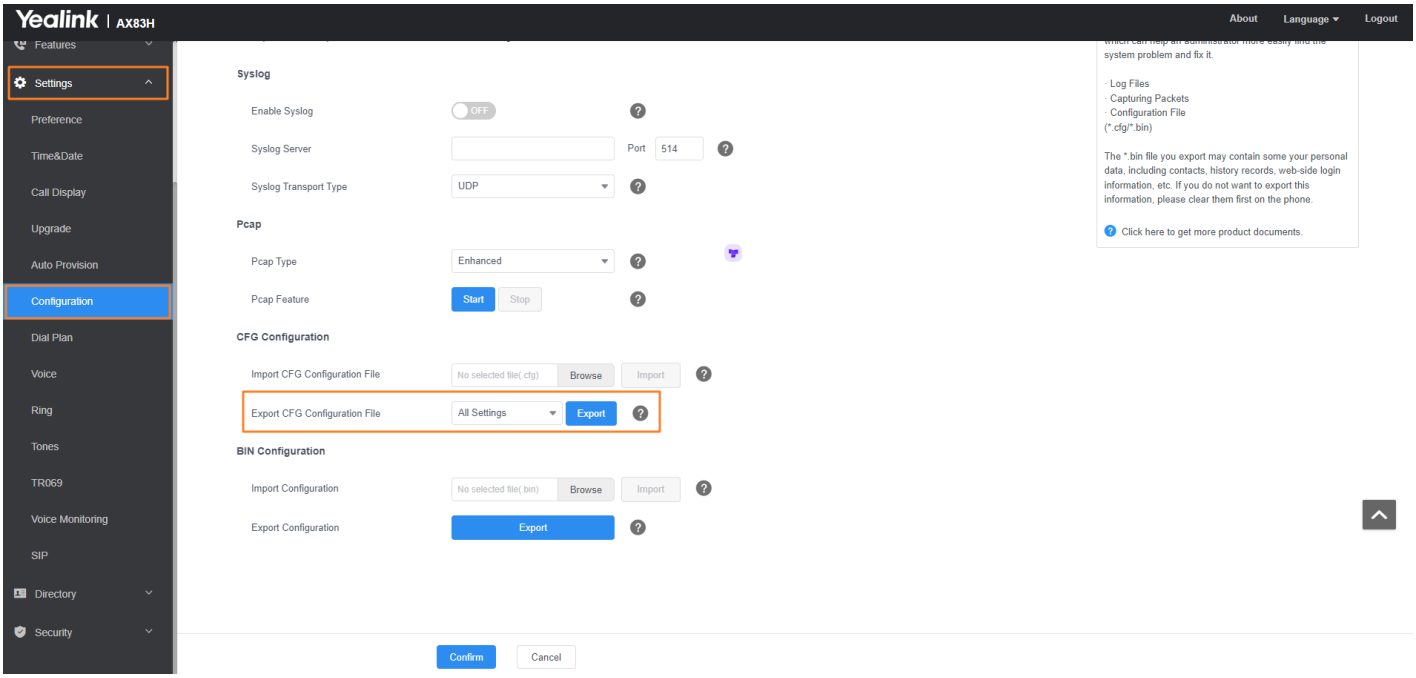
You can export the phone's configuration file to local and make changes to the phone's current feature settings. You can apply these changes to any phone by importing the configuration files via the web user interface.

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

- `<MAC>-local.cfg` : It contains 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 static parameters (for example, network settings) made via the phone user interface, web user interface and using configuration files.
- `<MAC>-non-static.cfg` : It contains all changes associated with non-static parameters made via the phone user interface, web user interface and using configuration files.
- `<MAC>-config.cfg` : It contains changes associated with 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. Go to **Settings** > **Configuration**.
2. In the **Export CFG Configuration File** field, click **Export** to open the file download window, and then save the file to your local system.



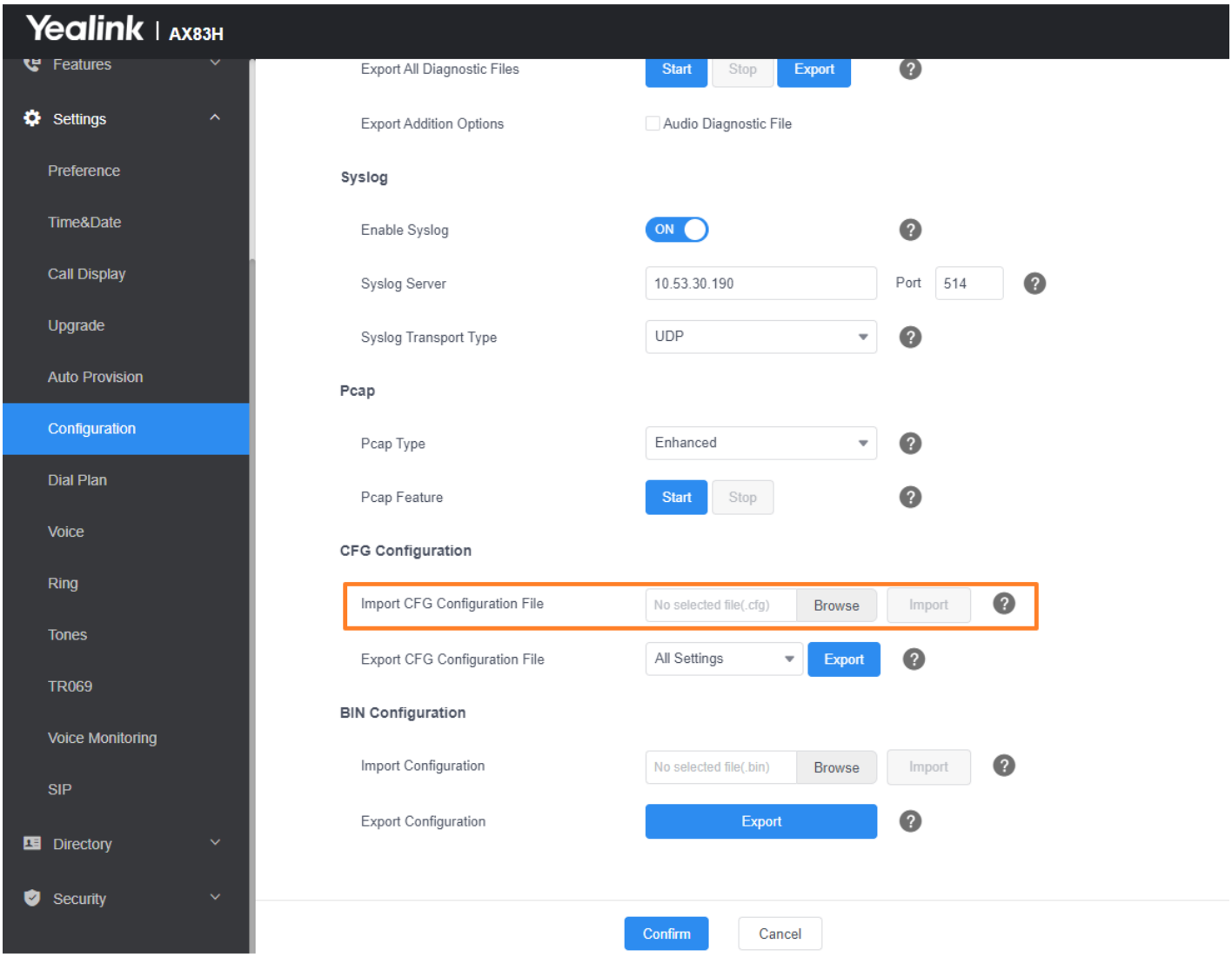
Import CFG Configuration Files to Phone

You can import the configuration files from local to the phones via the web user interface. The configuration files

contain the changes for phone features and these changes will take effect after importing.

Procedure

1. Go to **Settings** > **Configuration**.
2. In the **Import CFG Configuration File** field, click **Browse** to locate a CFG configuration file in your local system.
3. Click **Import** to import the configuration file.



Configuration Files Import URL Configuration

The following table lists the parameters you can use to configure the configuration files import URL.

static.custom_mac_cfg.url

Parameter	Permitted Values	Default	Description
static.custom_mac_cfg.url	URL within 511 characters	Blank	It configures the access URL of the custom MAC-Oriented CFG file.

Export BIN Files from the Phone

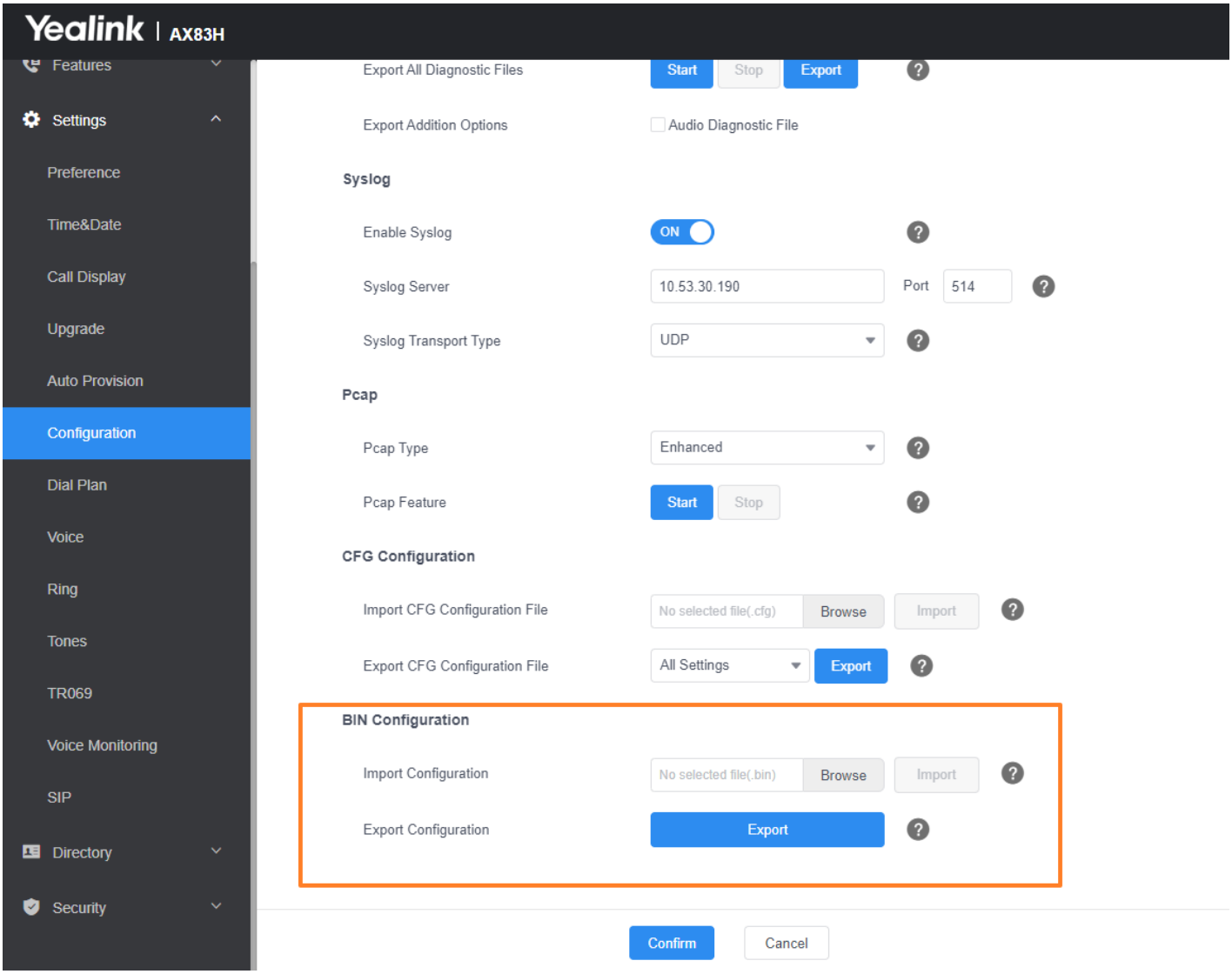
Procedure

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

Import BIN Files from the Phone

Procedure

1. From the web user interface, click **Settings** > **Configuration** > **BIN Configuration**.
2. In the **Import Configuration** field, click **Browse** to locate a BIN configuration file from your local system.
3. Click **Import** to import the configuration file.



BIN Files Import URL Configuration

static.configuration.url

Parameter	Permitted Values	Default	Description

static.configuration.url[1]	URL within 511 characters	Blank	It configures the access URL for the custom configuration files. **ⓘ NOTE** The file format of the custom configuration file must be *.bin.

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

Export All the Diagnostic Files

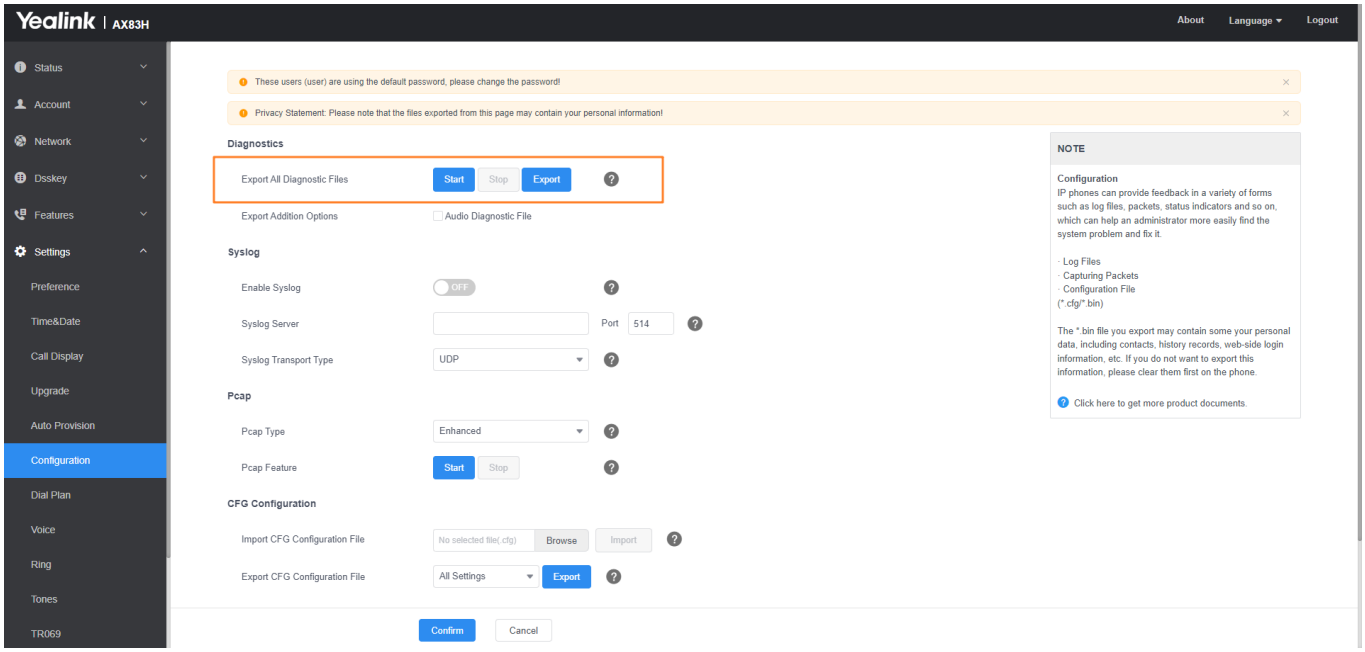
Introduction

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

Procedure

1. From the web user interface, 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.
4. Click **Stop** in the **Export All Diagnostic Files** field to stop the capture.
   The system log level will be reset to 3.

5. 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.



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

> ⓘ **NOTE**
> "Export All Diagnostic Files" is often used for issues that can be easily reproduced in a short period of time. For issues with a longer reproduction cycle or those involving restarts, it is often necessary to provide additional information along with the diagnostic files.

Please Check:

1. Please ensure that your Diagnostic files are complete and not missing any components.

2. Please ensure that the file size is within a normal range. If the size is too small(under 100KB), the data is typically considered invalid. Make sure to start the process before reproducing the issue.
   the process before reproducing the issue.

Watch Dog

Introduction

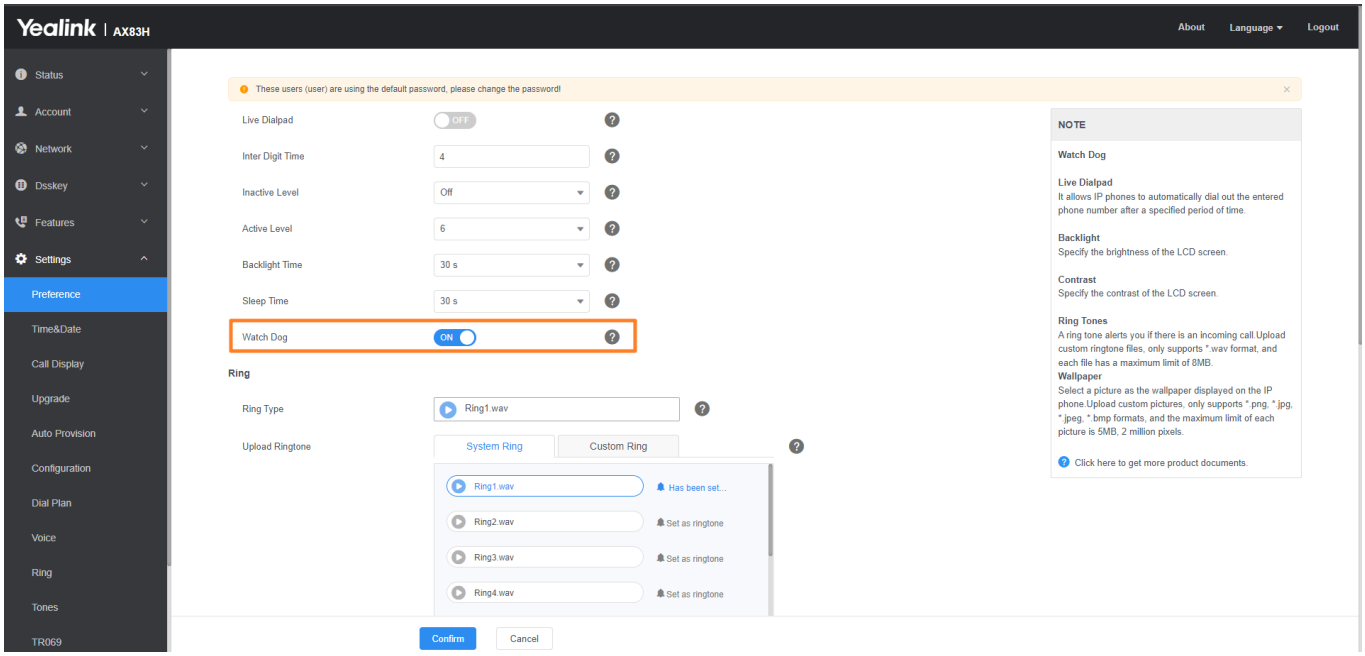
The phone provides a troubleshooting feature called “Watch Dog”, which helps you monitor the phone status

and provides the ability to get stack traces from the last time the phone failed. If the Watch Dog feature is enabled, the phone will automatically reboot when it detects a fatal failure. This feature can be configured using the configuration files or via the web user interface.

Watch Dog Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Preference** > **Watch Dog**.



Auto Provisioning

```
static.watch_dog.enable
```

Parameter	Permitted Values	Default	Description
static.watch_dog.enable	**0**-Disabled **1**-Enabled, the phone will reboot automatically when the system crashed.	1	It enables or disables the Watch Dog feature.

NOTE

Under normal circumstances, you do not need to pay attention to the Watch Dog feature, and please keep it enabled during daily use. Its main function is to restart processes that have crashed due to unknown internal errors, often accompanied by device restarts. If you have contacted Yealink's technical support, you can, if necessary, disable this feature and capture relevant data under the guidance of technical support.

Phone Reboot

Introduction

You can reboot the phone remotely or locally.

Reboot the Phone Remotely

You can reboot the phones remotely using a SIP NOTIFY message with "Event: check-sync" header. Whether the phone reboots or not depends on `sip.notify_reboot_enable`. If the value is set to 1, or the value is set to 0 and the header of the SIP NOTIFY message contains an additional string "reboot=true", the phone will reboot immediately.

The NOTIFY message is formed as shown:

```
NOTIFY sip:<user>@<dsthost> SIP/2.0
To: sip:<user>@<dsthost>
From: sip:sipsak@<srchost>
CSeq: 10 NOTIFY
Call-ID: 1234@<srchost>
Event: check-sync;reboot=true
```

Notify Reboot Configuration

```
sip.notify_reboot_enable
```

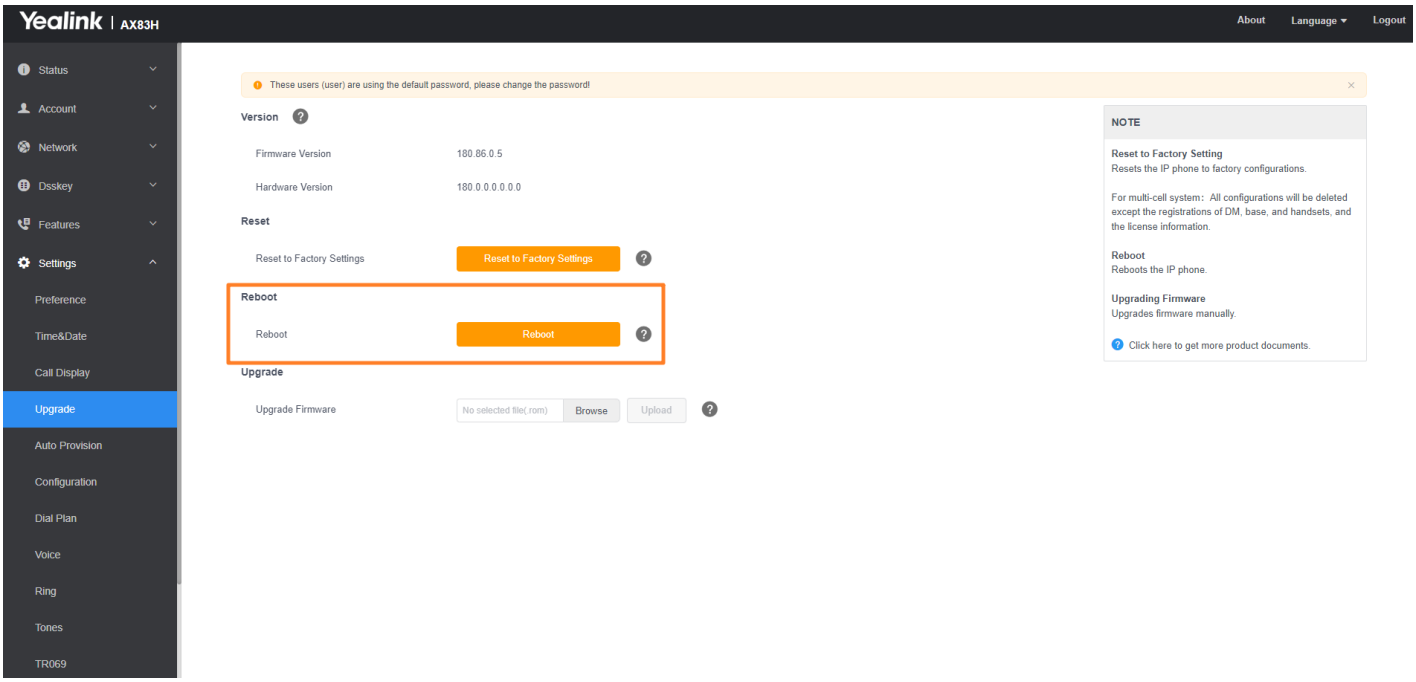
Parameter	Permitted Values	Default	Description
sip.notify_reboot_enable	**0**-The phone will reboot only if the SIP NOTIFY message contains an additional string "reboot=true". **1**-The phone will reboot. **2**-The phone will ignore the SIP NOTIFY message.	1	It configures the phone behavior when receiving a SIP NOTIFY message which contains the header "Event: check-sync".

Reboot the Device via Web User Interface

You can reboot your IP phone via the web user interface.

Procedure

1. Click **Settings** > **Upgrade**.
2. Click **Reboot**.
   The device begins rebooting. Any reboot of the device may take a few minutes.



Example of Troubleshooting

This chapter will demonstrate troubleshooting methods through several common examples.

> **NOTE**
> If the scenario involves device reboot, upgrade, or any other action that may clear the device cache, please make sure to provide both syslog and local log to avoid any loss of data and save your valuable time.

Troubleshooting Sound Issues

The following section provides troubleshooting methods and examples for common audio issues and how to provide feedback on the problems.

Troubleshooting No Audio during Calls

Common scenarios of no sound issues:

1. One-way Audio: The call can be established successfully, but only one party can hear the sound while the other cannot.
2. No Audio on Both Sides: Both parties cannot hear each other during the call.
3. One-way Audio on External Calls: One-way audio issue occurs specifically when making calls to external phone lines.
4. One-way Audio with a Specific Codec: One-way audio problem is encountered when using a particular codec.

To troubleshoot these issues, you can follow these steps:

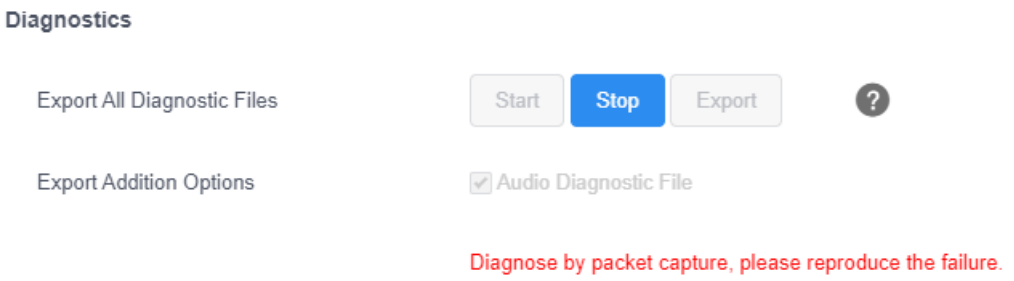
1. Ensure that the volume settings on both devices are not muted or set too low.
2. Check if the microphone and speaker are functioning properly and not obstructed.

3. Verify the network connectivity and quality, as network issues can affect audio transmission.
4. Test the call with different devices or codecs to identify if the issue is specific to certain configurations.

If the above objective reasons do not apply, please follow the steps below to provide the necessary information.

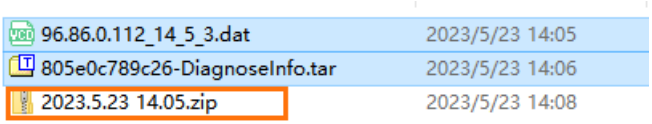
Steps for Obtaining Diagnostic Information:

1. Determine the likelihood of the issue occurring. Identify how many devices are affected and whether the problem is related to specific user accounts. If the issue is related to a specific account, prioritize troubleshooting the account-related issues.
2. Identify the specific symptoms of the issue. For example, in a scenario where A calls B, A is unable to hear B's voice, and the same issue occurs when B calls A, with A still unable to hear B's voice.
3. Click "Start" to begin capturing the data, and make sure both A and B capture the data simultaneously.



4. After reproducing the issue, record the timestamp and export the Diagnostic files.

5.Please compress the .dat and .tar files into a single archive and send them to Yealink technical support(https://ticket.yealink.com/index). You can either name the archive with the timestamp or mention the timestamp in the problem description.



6. If possible, please provide comparative Diagnostic files of a successful call between A and B.

Troubleshooting Audio Quality Issues.

Common scenarios of no sound issues:

1. Intermittent sound during calls.
2. Low volume or significant background noise during calls.

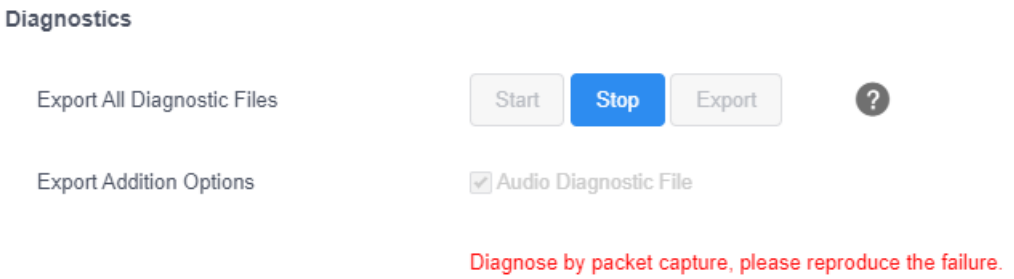
To troubleshoot these issues, you can follow these steps:

1. Determine the number of devices involved and whether the issue is specific to a single or a few devices.
2. Verify if the volume settings are appropriate, avoiding excessively high or low volume levels.
3. Check if both parties are speaking simultaneously. If so, a decrease in volume is a normal occurrence due to duplex suppression.
4. Try IP call to test the audio quality. If the audio quality is normal during IP call, prioritize checking for audio codec issues on the server side.

If the above objective reasons do not apply, please follow the steps below to provide the necessary information.

Steps for Obtaining Diagnostic Information:

1. Check the "Audio Diagnostic File" option and click "Start" to begin capturing the data. Ensure that both parties, A and B, capture the data simultaneously.



2. Please make sure to provide a video of the issue along with the Diagnostic File. The video should clearly capture the problem phenomenon.

Troubleshooting Restart Issues

Common scenarios of no Restart issues:

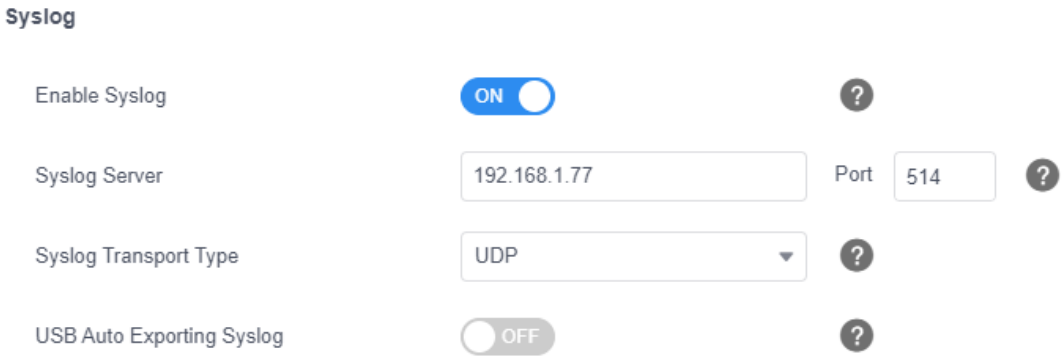
1. Device restarts abruptly without any user intervention.
2. Regular and scheduled restarts at fixed intervals.

To troubleshoot these issues, you can follow these steps:

1. In the case of a sudden device restart without any user intervention, it is recommended to check if the correct power adapter is being used or if the POE power supply is insufficient.
2. For regular and scheduled restarts at fixed intervals, it is advisable to check if the server associated with the device is periodically pushing certain configuration parameters or SIP signals that may cause the device to restart.

Steps for Obtaining Diagnostic Information:

1. Troubleshooting restart issues requires capturing logs using syslog. Please ensure that you correctly fill in the syslog server address and port.



2. After encountering the issue, wait for the device to successfully boot up and then export the local log.
3. Please compress the syslog and .tar files into a single archive and send them to Yealink technical support. You can either name the archive with the timestamp or mention the timestamp in the problem description.

Troubleshooting Network Issues

Symptoms of configuration file download failure.:

After entering the server address in the device, it cannot download the configuration file from the server.

To troubleshoot these issues, you can follow these steps:

1. Check if the server address entered in the device is correct. Incorrect addresses can result in the device sending requests to the wrong address, leading to failure.
2. Verify the network connectivity between the device and the server. You can use the device to ping the server address：
3. Ensure that the file exists on the server. If the file is not found (resulting in a 404 error), the device will fail to download.
4. If your server address is a domain name, check if the DNS configuration is correct. DNS resolution issues can also cause download failures.

Steps for Obtaining Diagnostic Information:

If the connection between your device and the server is normal, and you have ensured that your server settings are correct, please provide the following information:

Preparation:

1. Please set the log level to 6 before reproducing the issue.
2. If the reproduction process involves a restart, you will also need to set up Syslog correctly to upload the logs to the server, or use a USB drive to capture the logs.

Steps:

1. Reproduce the problem.
2. Wait for one minute, then export the diagnostic files and include the syslog.
3. If your device restarts during this process, please provide a video of the phenomenon if possible.