Internet Port and PC Port

Introduction

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

Supported Transmission Methods

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

- Auto-negotiate
- Half-duplex (transmit in 10Mbps or 100Mbps)
- Full-duplex (transmit in 10Mbps, 100Mbps or 1000Mbps)

> 1000Mbps is unavailable to CP phones.

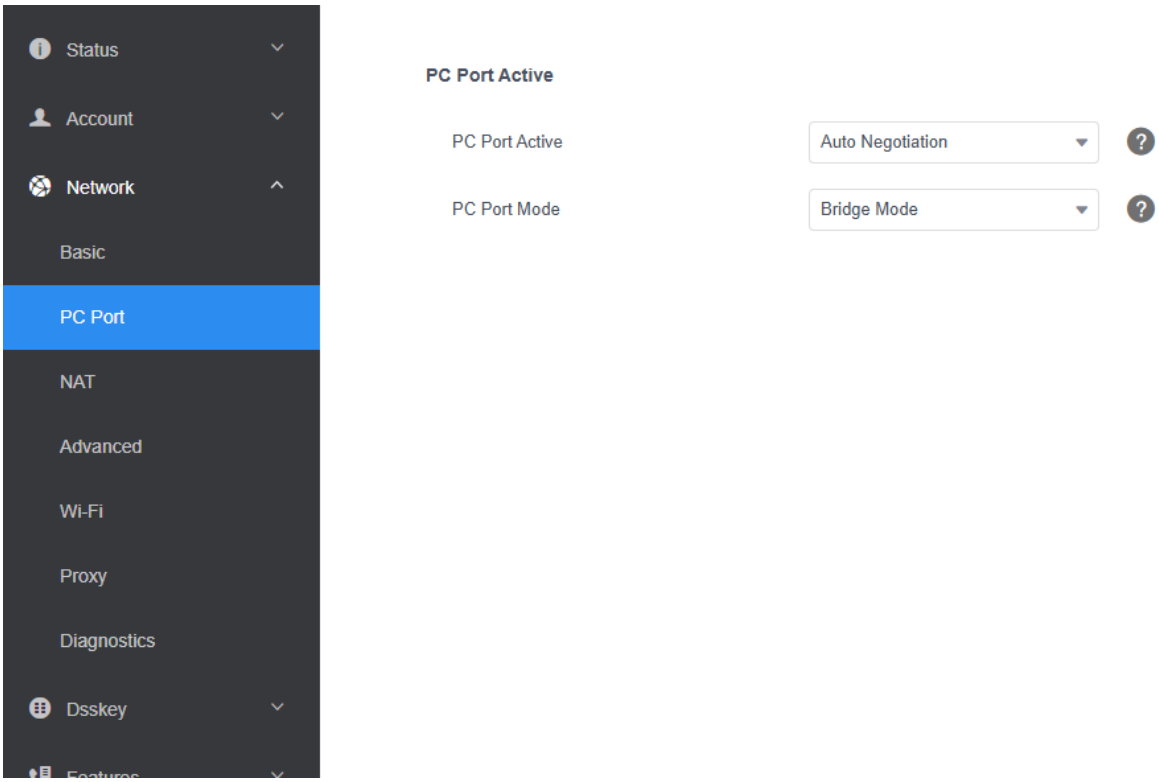
Auto-negotiate is configured for both Internet and PC ports on the IP phone by default.

Internet Port and PC Port Configuration

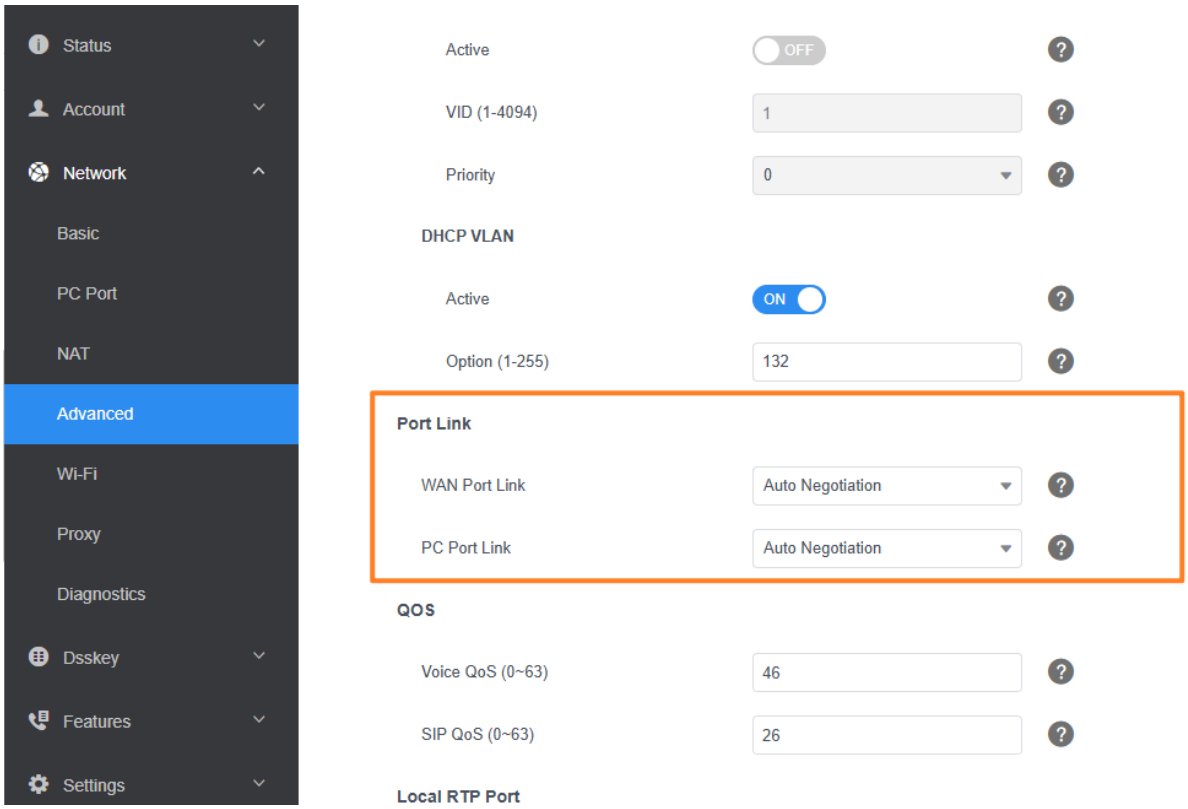
Via Web User Interface

Procedure

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



3. Go to **Network** > **Advanced** > **Port Link** > **WAN Port Link**/**PC Port Link**.



Via Auto Provisioning

static.network.pc_port.enable

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

Parameter	Permitted Values	Default	Description
static.network.pc_port.enable[1]	**0-** Disabled **1**-Auto Negotiation	1	It enables or disables the PC feature.
static.network.internet_port.speed_duplex[1]	**0-** Auto Negotiation **1-** Full Duplex 10Mbps **2**-Full Duplex 100Mbps **3**-Half Duplex 10Mbps **4**-Half Duplex 100Mbps **5**-Full Duplex 1000Mbps	0	It configures the network speed over Ethernet of the Internet port. **Note**: You can set the transmission speed to 1000Mbps/Auto Negotiation to transmit in 1000Mbps if the phone is connected to the switch that supports Gigabit Ethernet. We recommend that you do not change this parameter.
static.network.pc_port.speed_duplex[1]	**0-** Auto Negotiation **1-** Full Duplex 10Mbps **2**-Full Duplex 100Mbps **3**-Half Duplex 10Mbps **4**-Half Duplex 100Mbps **5**-Full Duplex 1000Mbps	0	It configures the network speed over Ethernet of the PC port. **Note**: You can set the transmission speed to 1000Mbps/Auto Negotiation to transmit in 1000Mbps if the phone is connected to the switch that supports Gigabit Ethernet. We recommend that you do not change this parameter.
static.network.vlan.pc_port_mode[1]	**0-** The phone forwards the packets sent from the PC port to the Internet port directly. **1**-If there are no VLAN tags in	1	It configures how the phone processes packets for the PC port when VLAN is enabled on the PC port.

	the packets sent from the PC port to the Internet port, the phone tags the packets and then forwards them; else, the phone forwards the packets directly.		
static.network.pc_port.mode[1]	**0**-The phone can only share the wired network with the connected PC, not the wireless network. **1**-The phone can share both the wired network and wireless network with the connected PC.	0	It configures the PC port mode. **Note**: The parameter is only available to T44W/T5XW/VP59/T7XW/T8X series phones.

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

How to access the web user interface

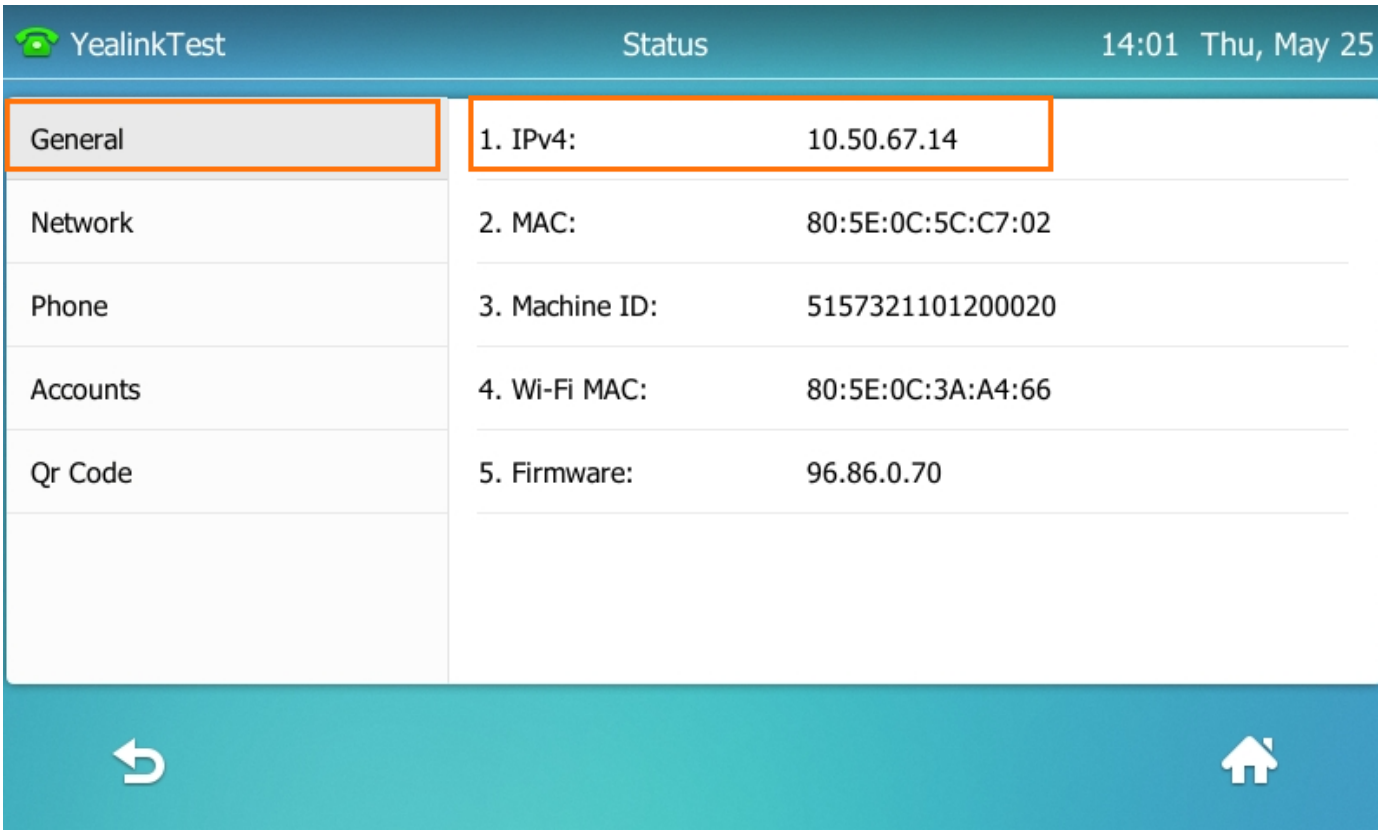
Introduction

You can access the base web user interface by the base IP address.

The switch or gateway distributes the IP address. It doesn't have a factory IP address.

How to get the IP address of DeskPhone?

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



Limiting Concurrent Logins for a Single User

This feature is designed to enhance the security and stability of the phone's web management interface. Restricting the number of users who can log in simultaneously ensures that only one user can perform management operations at any given time.

Configuration parameter

wui.check_remote.mode

Parameter	Permitted Values	Default	Description

		t	
wui.check_remote.mode	**0**-No limit on the number of concurrent logins **1**-Restrict remote login, display message: The user is busy, current login IP: XXXX! **2**-Local login takes precedence and logs out remote users, remote message: Your account has been logged out!	0	It configures the selection for weak session concurrent login mode.

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.

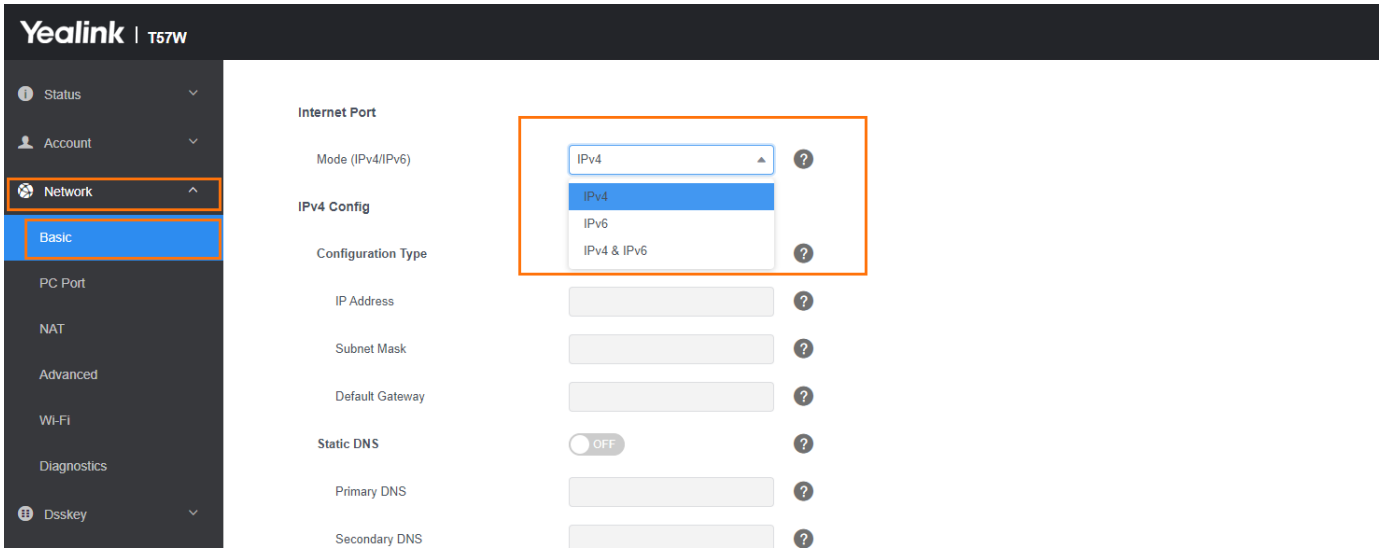
> Yealink devices comply with the DHCPv4 specifications documented in RFC 2131, and DHCPv6 specifications documented in RFC 4443.

IP Addressing Mode Configuration

You can configure IP addressing mode for the wired network.

Set via the Web User Interface

1. On the web user interface, go to **Network** > **Basic** > **Internet Port**.



Configuration parameter

static.network.ip_address_mode
static.network.preference

Parameter	Permitted Values	Default	Description

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

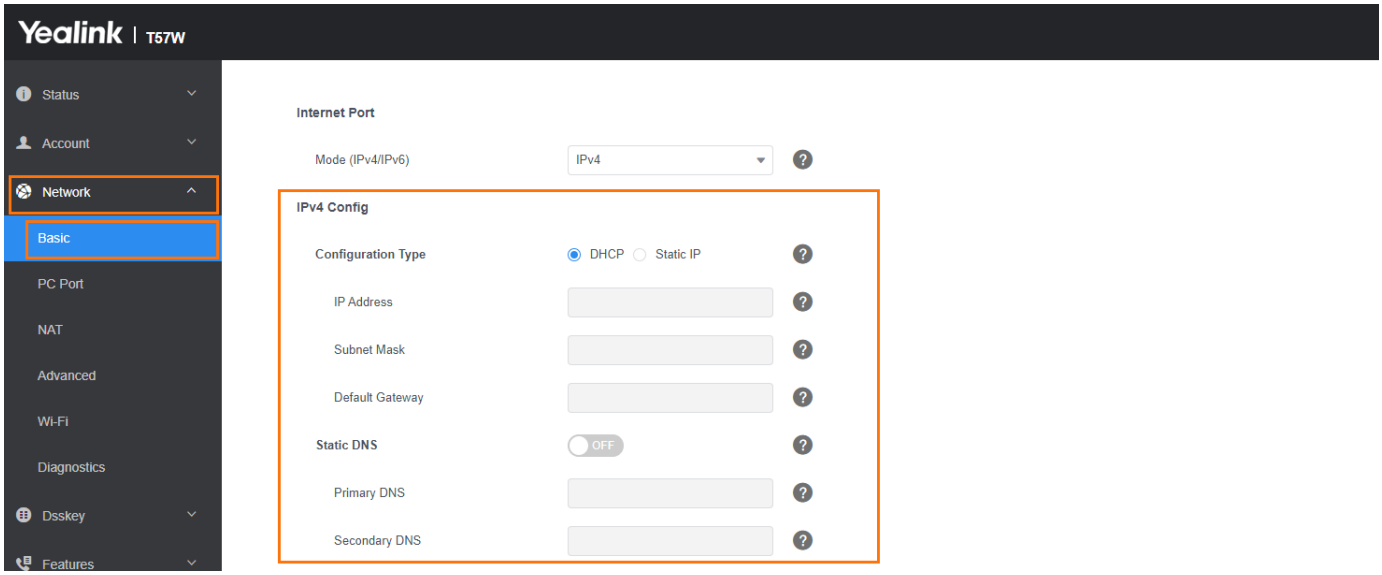
> [1]If you change this parameter, the phone will reboot to make the change take effect.

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** > **Basic** > **IPv4 Config**.



Configuration parameter

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

static.network.primary_dns
static.network.secondary_dns

Parameter	Permitted Values	Default	Description
static.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. It works only if "static.phone_setting.auto_switch_internet_port_type.enable" is set to 1.
static.network.internet_port.type[1]	**0**-DHCP **2**-Static IP	0	It configures the Internet port type for IPv4.
static.network.internet_port.ip[1]	IPv4 Address	Blank	It configures the IPv4 address. It works only if "static.network.internet_port.type" is set to 2 (Static IP).
static.network.internet_port.mask[1]	Subnet Mask	Blank	It configures the IPv4 subnet mask. It works only if "static.network.internet_port.type" is set to 2 (Static IP).
static.network.internet_port.gateway[1]	IPv4 Address	Blank	It configures the IPv4 default gateway. It works only if "static.network.internet_port.type" is set to 2 (Static IP).
static.network.static_dns_enable[1]	**0**-Off, the phone will use the IPv4 DNS	0	It triggers the static DNS feature to turn on or off.

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

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

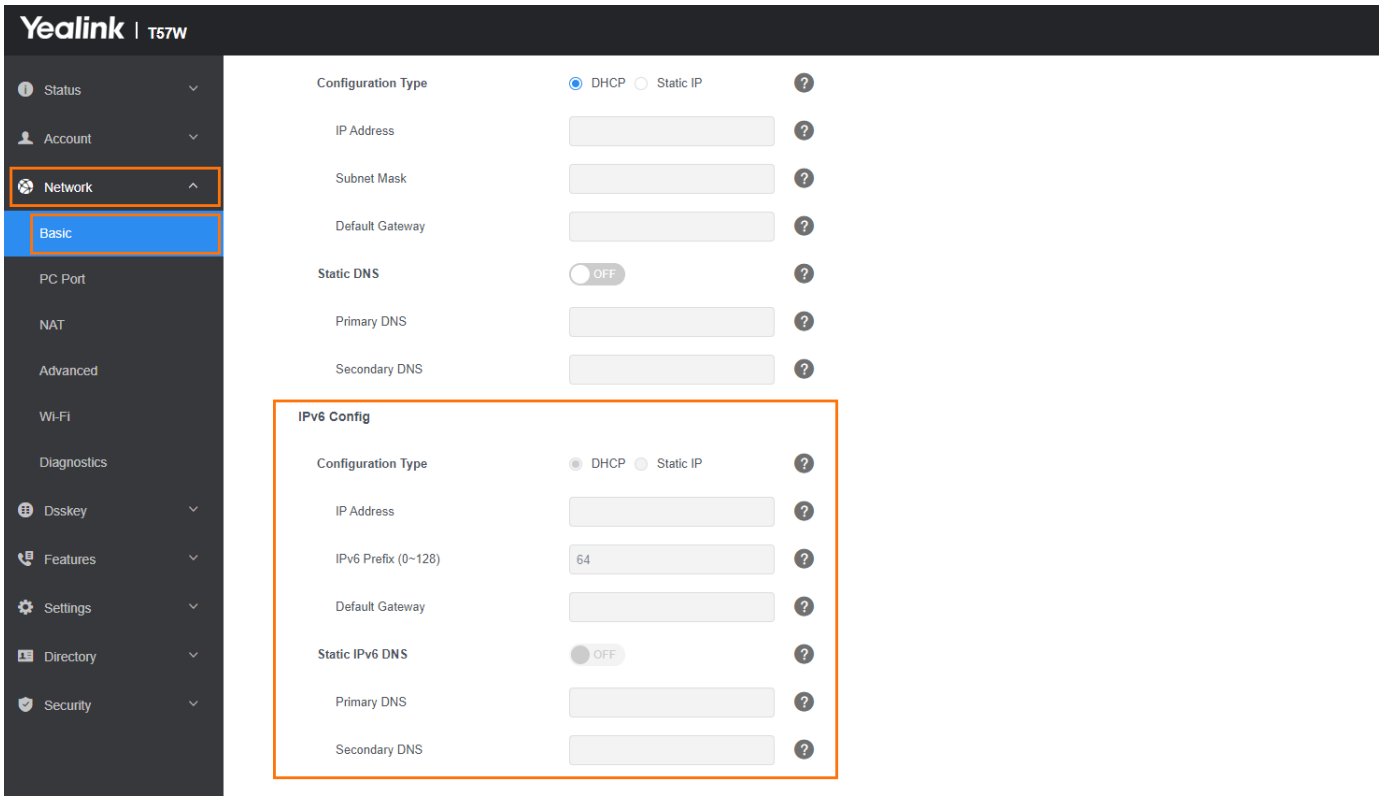
IPv6 Configuration

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** > **Basic** > **IPv6 Config**.



Configuration parameter

static.network.ipv6_internet_port.type
static.network.ipv6_internet_port.ip
static.network.ipv6_prefix
static.network.ipv6_internet_port.gateway
static.network.ipv6_static_dns_enable
static.network.ipv6_primary_dns
static.network.ipv6_secondary_dns
static.network.ipv6_icmp_v6.enable
features.dect_management.ipv6_address
backup.master_dm.ip

Parameter	Permitted Values	Default	Description
static.network.ipv6_internet_port.type[1]	**0**-DHCP (using SLAAC by default) **1**-Static IP	0	It configures the Internet port type for IPv6. It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6).

static.network.ipv6_internet_port.ip[1]	IPv6 Address	Blank	It configures the IPv6 address. It works only if "static.network.ipv6_internet_port.type" is set to 1 (Static IP).
static.network.ipv6_prefix[1]	Integer from 0 to 128	64	It configures the IPv6 prefix. It works only if "static.network.ipv6_internet_port.type" is set to 1 (Static IP).
static.network.ipv6_internet_port.gateway[1]	IPv6 Address	Blank	It configures the IPv6 default gateway. It works only if "static.network.ipv6_internet_port.type" is set to 1 (Static IP).
static.network.ipv6_static_dns_enable[1]	**0**-Off, the phone will use the IPv6 DNS obtained from DHCP. **1**-On, the phone will use manually configured static IPv6 DNS.	0	It triggers the static IPv6 DNS feature to turn on or off. It works only if "static.network.ipv6_internet_port.type" is set to 0 (DHCP).
static.network.ipv6_primary_dns[1]	IPv6 Address	Blank	It configures the primary IPv6 DNS server. It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure "static.network.ipv6_static_dns_enable" is set to 1 (On).
static.network.ipv6_secondary_dns[1]	IPv6 Address	Blank	It configures the secondary IPv6 DNS server. It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In

			DHCP environment, you also need to make sure "static.network.ipv6_static_dns_enable" is set to 1 (On).
static.network.ipv6_icmp_v6.enable[1]	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to obtain IPv6 network settings via SLAAC (Stateless Address Auto-configuration). It works only if "static.network.ipv6_internet_port.type" is set to 0 (DHCP).
features.dect_management.ipv6_address[1]	String within 64 characters	Blank	It configures the IPv6 address of the DM.
backup.master_dm.ip[1]	String within 64 characters	Blank	It configures the master DM IPv6 for the backup DM. It works only if the DM Role is set to DM-Reserve.

[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.

> 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 that connecting to the secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server address. For more information, refer to RFC 3925.

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

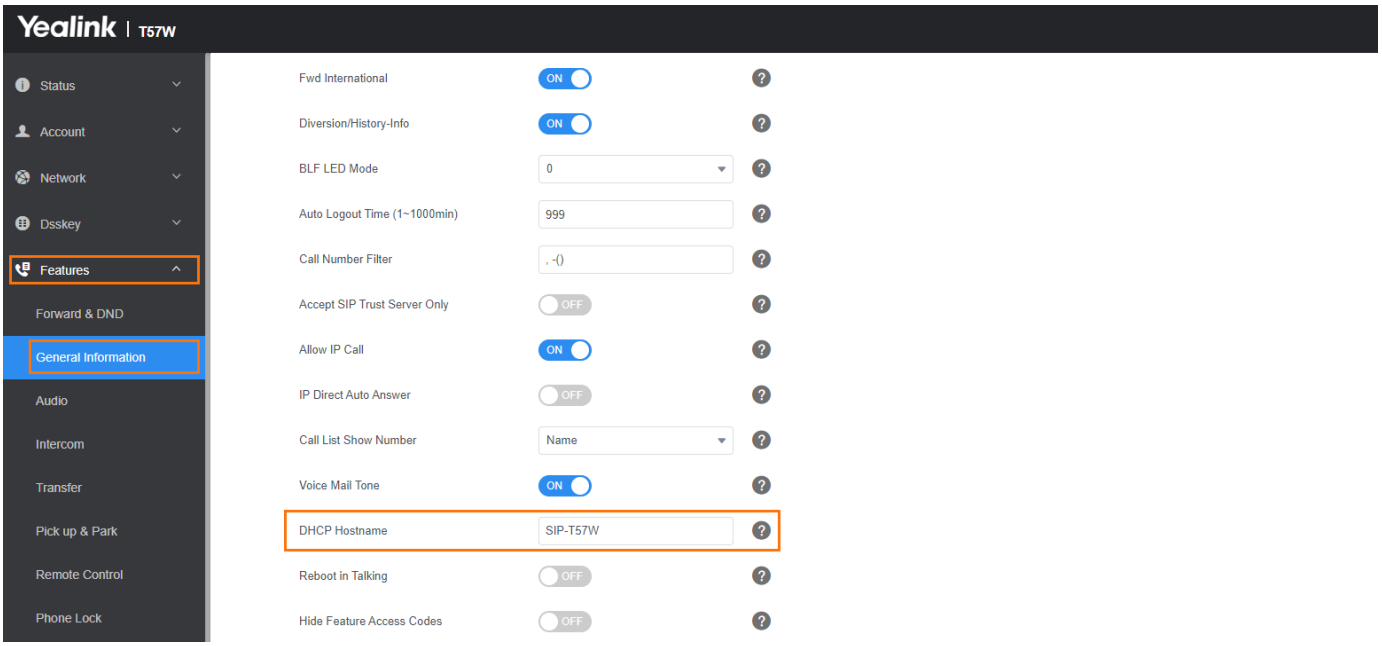
Description

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(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

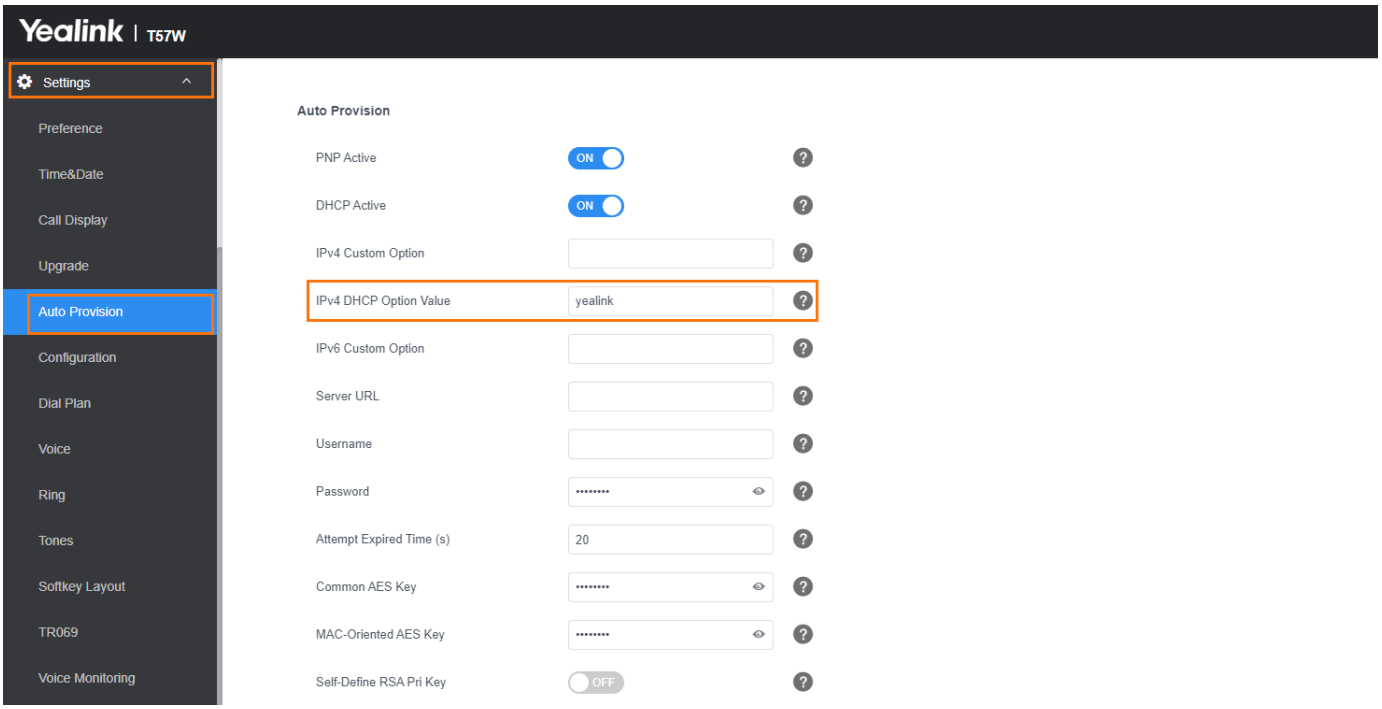
Description

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.

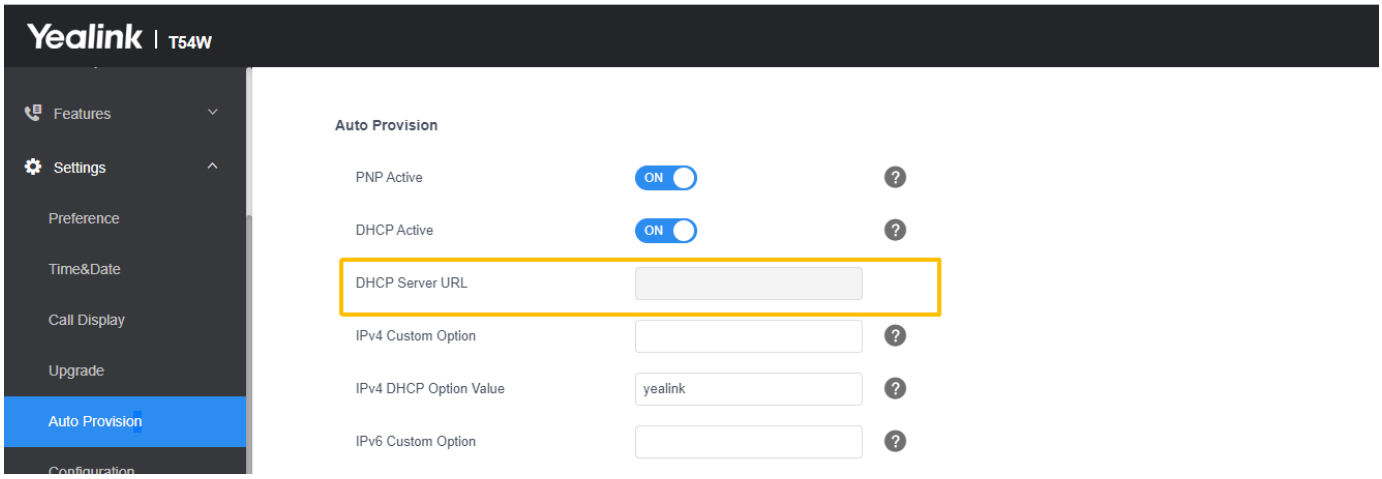
Configuration parameter

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**.



The DHCP Server URL can not be edited.

DHCP Option for IPv6

Introduction

The phone can obtain IPv6-related parameters in an IPv6 network via the 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 for 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

VLAN

About VLAN

VLAN (Virtual Local Area Network) is used to logically divide a physical network into several broadcast domains. VLAN membership can be configured through software instead of physically relocating devices or connections. Grouping devices with a common set of requirements regardless of their physical location can greatly simplify network design. VLANs can address issues such as scalability, security, and network management.

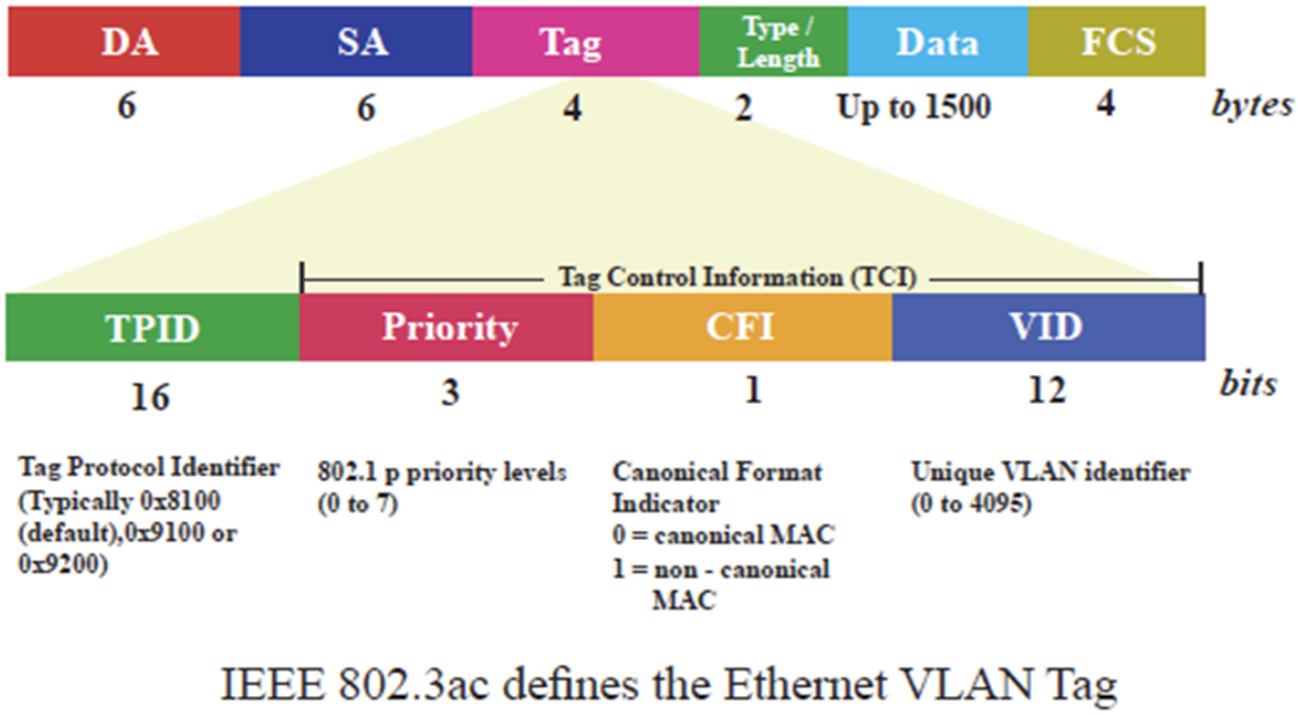
Major Benefits of Using VLANs

VLANs offer many benefits that are not found in typical LANs. Major benefits of segregating IP phones into VLAN(s) are listed below:

- **Performance Enhancements:** VLAN is used to minimize the broadcast domain. Creating a smaller domain for an IP phone can reduce overhead and limit resource utilization. Additionally, less traffic will need to be routed, and the latency added by routers will be reduced.
- **Ease of Administration:** Much of the cost associated with network additions and relocations can be saved through the use of VLANs. An IP phone can be shifted from one workgroup or department to another without installing new network cabling and reconfiguring hubs or routers.
- **Security:** VLANs can be used to create secure user groups and prevent others outside of the broadcast domain from receiving sensitive data of the IP phone. They can also be used to enhance firewall functions and restrict network access for one or more users. By segregating IP phones into VLANs, security filters can be implemented in the network to prevent the IP phones from receiving unnecessary traffic from other devices. This helps prevent disruption due to DoS attacks or attempts to compromise the devices. It also allows locking down access to configuration and signaling servers to only allow access from the IP phones.

IEEE 802.1Q

IEEE 802.1Q is the networking standard that supports VLANs on an Ethernet network. 802.1Q adds a 4-byte tag between the source MAC address and the Ethernet type fields of the Ethernet frame.



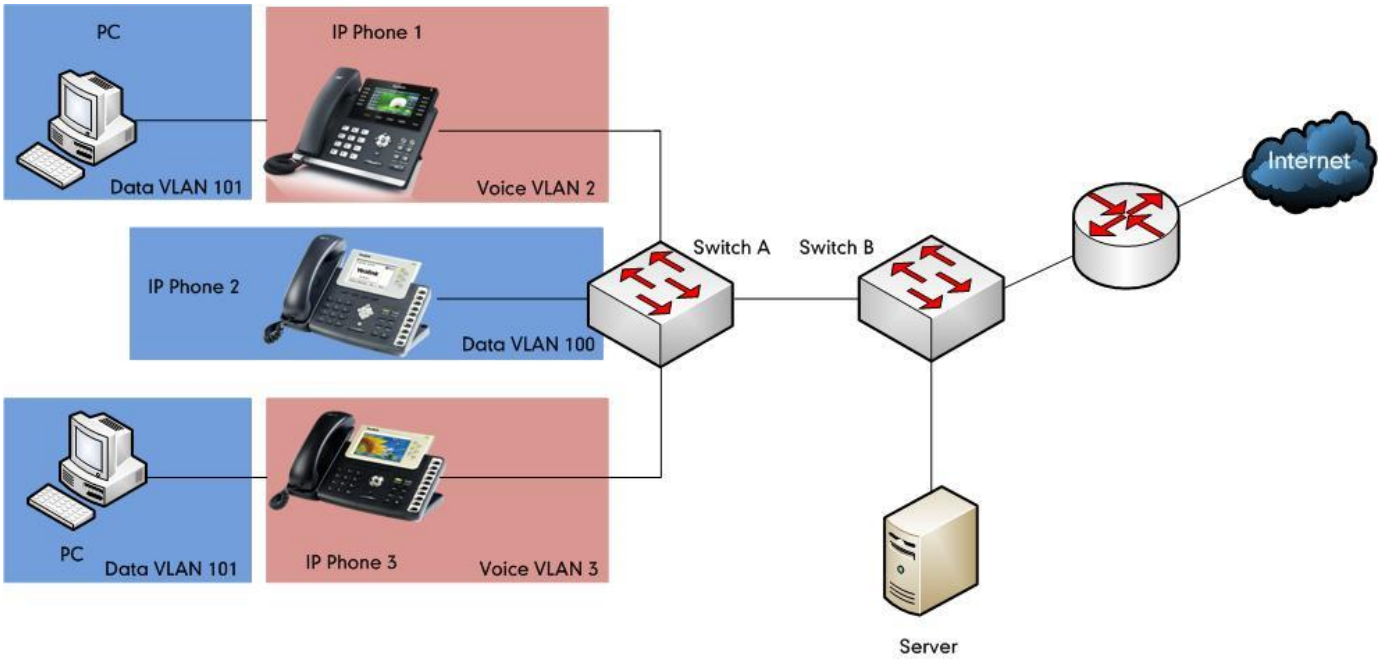
IEEE 802.3ac defines the Ethernet VLAN Tag

Voice VLAN

As voice traffic is delay and jitter-sensitive for the IP phone, it requires higher priority over data traffic to reduce delay and packet loss during transmission. To simplify configuration procedures and better manage voice transmission policies, the connected switch can be configured to provide a voice VLAN function and transmit the voice traffic of the IP phone in a dedicated VLAN.
called voice VLAN.

Voice VLAN is a special access port feature of the switch that allows IP phones to be automatically configured and easily associated with a logically separate VLAN. This feature provides various benefits, but one particular benefit is that when voice VLAN is enabled on a
switch port, this port is also enabled to allow simultaneous access for a PC. This feature allows a PC to be daisy-chained to an IP phone, and the connection for both PC and IP phone to be trunked through the same physical Ethernet cable.

The purpose of VLAN configurations on the phone is to insert a tag with VLAN information into the packets generated by the phone. When VLAN is properly configured for the ports (Internet port and PC port) on the phone, the phone will tag all packets from these ports with the VLAN ID. The switch receives and forwards the tagged packets to the corresponding VLAN according to the VLAN ID in the tag as described in IEEE Std 802.3. In addition to manual configuration, the phone also supports the automatic discovery of VLAN via LLDP, CDP, or DHCP. The assignment takes effect in this order: assignment via LLDP/CDP, manual configuration, then assignment via DHCP.



VLAN Configuration

LLDP

Description

LLDP (Link Layer Discovery Protocol) allows IP phones to receive and/or transmit device-related information to directly connected devices on the network that are also using the protocol, and store the information that is learned about other devices. Information gathered with LLDP is stored in the device as a management information database (MIB) and can be queried with the Simple Network Management Protocol (SNMP) as specified in RFC 2922. LLDP transmits the information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value (TLV) elements, each of which contains a particular type of information about the device or port transmitting it.

Each of the TLV components has the following basic structure:

Type	Length	Value
7 bits	9 bits	0-511 octets

LLDP supports advertising the following TLVs:

TLV Type	TLV Name	Description
Mandatory TLVs	Chassis ID	Specifies the IP address of the IP phone.
	Port	Specifies the MAC address of the IP phone.

	ID	
	Time to Live	Specifies the lifetime of the transmitted information on the IP phone. The default value is 180s.
	End of LLD PDU	Marks the end of the TLV sequence in the LLDPDU. No further processing of TLVs after this is necessary. This is a mandatory TLV and therefore must be present at the end of the data stream.
Optional TLVs	System Name	Specifies the administratively-assigned name for the IP phone (per RFC3418).
	System Description	Specifies the description of the IP phone.
	System Capabilities	Specifies the supported and enabled capabilities of the IP phone. The supported capabilities are Telephone. The enabled capabilities are Telephone by default
	Port Description	Specifies the description of the sending port. The default value is “WAN PORT”.
IEEE Std 802.3 Organizationally Specific TLV	MAC/PHY Configuration/ Status	Specifies duplex and bit rate settings of the IP phone. The Auto-Negotiation is supported and enabled by default. The advertised capabilities of PMD Auto-Negotiation are: • 10BASE-T (half duplex mode) • 10BASE-T (full duplex mode) ☒ • 100BASE-TX (half duplex mode) • 100BASE-TX (full duplex mode) • 1000BASE-T (full duplex mode).

		Note: By default, all phones have the PMD Advertised Capability set for 10BASE-T and 100BASE-TX. Yealink VP59/CP860/SIP VP-T49G/SIP-T58W/T58A/T57W/T54W/T53W/T53/T48U/T48G/T48S/ T46U/T46G/T46S/T43U/T42U/T42G/T42S/T33G/T31G/T29G/T27G/T23G/T7X/T8X phones that have Gigabit Ethernet support PMD Advertise Capability also contain set 1000BASE-T.
LLDPMED TLVs	Media Capabilities	Specifies the MED device type of the IP phone and the supported LLDP-MED TLV type can be encapsulated in LLDPDU. The supported LLDP-MED TLV types are: • LLDP-MED Capabilities • Network Policy • Extended Power via MDI-PD • Inventory
	Network Policy	Specifies the port VLAN ID, application type, L2 priority, and DSCP value.
	Extended Power-via-MDI	Specifies power type, source, priority, and value.
	Inventory–Hardware Revision	Specifies the hardware revision of the IP phone.
	Inventory–Firmware	Specifies the firmware revision of the IP phone.

	Revision	
	Inventory–Software Revision	Specifies the software revision of the IP phone.
	Inventory–Serial Number	Specifies the serial number of the IP phone.
	Inventory–Manufacturer Name	The manufacturer's name of the IP phone. The default value is “Yealink”.
	Inventory–Model Name	Specifies the model name of the IP phone.
	Asset ID	Specifies the asset identifier of the IP phone.

LLDP-MED

LLDP-MED (Media Endpoint Discovery) is published by the Telecommunications Industry Association

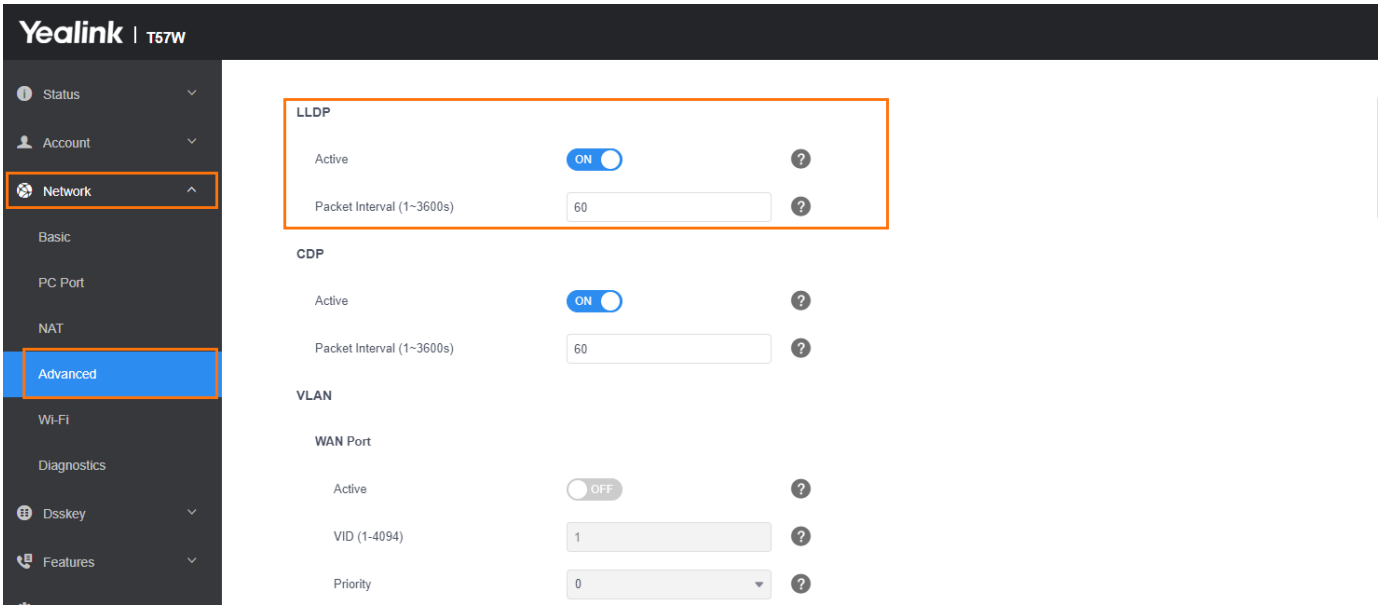
(TIA). It is an extension to LLDP that operates between endpoint devices and network connectivity devices. LLDP-MED specifically provides support for voice over IP (VoIP) applications and provides the following capabilities:

LLDP-MED TLVs	Description
Capabilities Discovery	allows LLDP-MED endpoints to determine the capabilities that the connected device supports and has enabled. It can be used to indicate whether the connected device is a phone, a switch, a repeater, etc.
Voice VLAN Configuration	provides a mechanism for a switch to notify a device which VLAN to use, which enables “plug and play” networking.
Power Management	provides information related to how the device is powered, power priority, and how much power the device needs.
Inventory Management	provides a means to manage the device and the attributes of the device, such as model number, serial number, software revision, etc.
Location Identification Discovery	provides location information from the switch to the device when placing an emergency call.

Configure LLDP Feature on Yealink IP Phones

Set via the Web User Interface

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



Configuration parameter

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

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

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

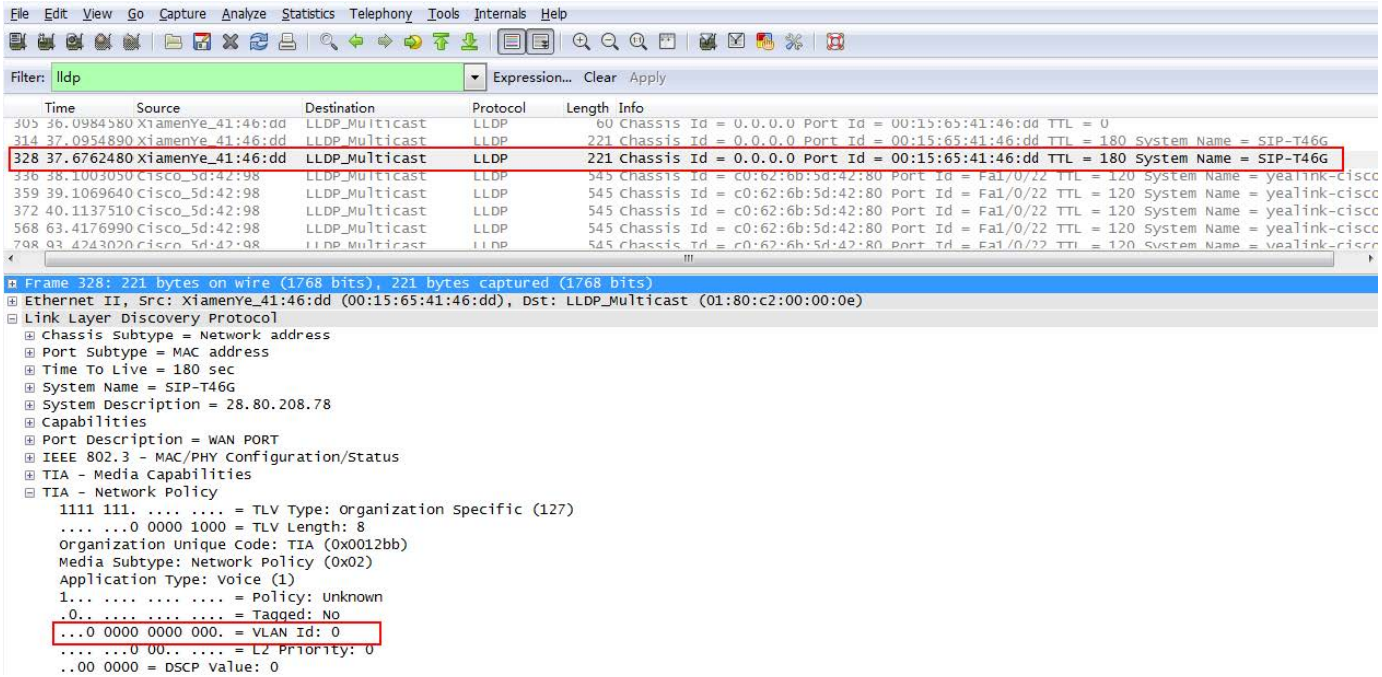
Verify the Configuration

After the LLDP feature is enabled, the IP phone performs the following:

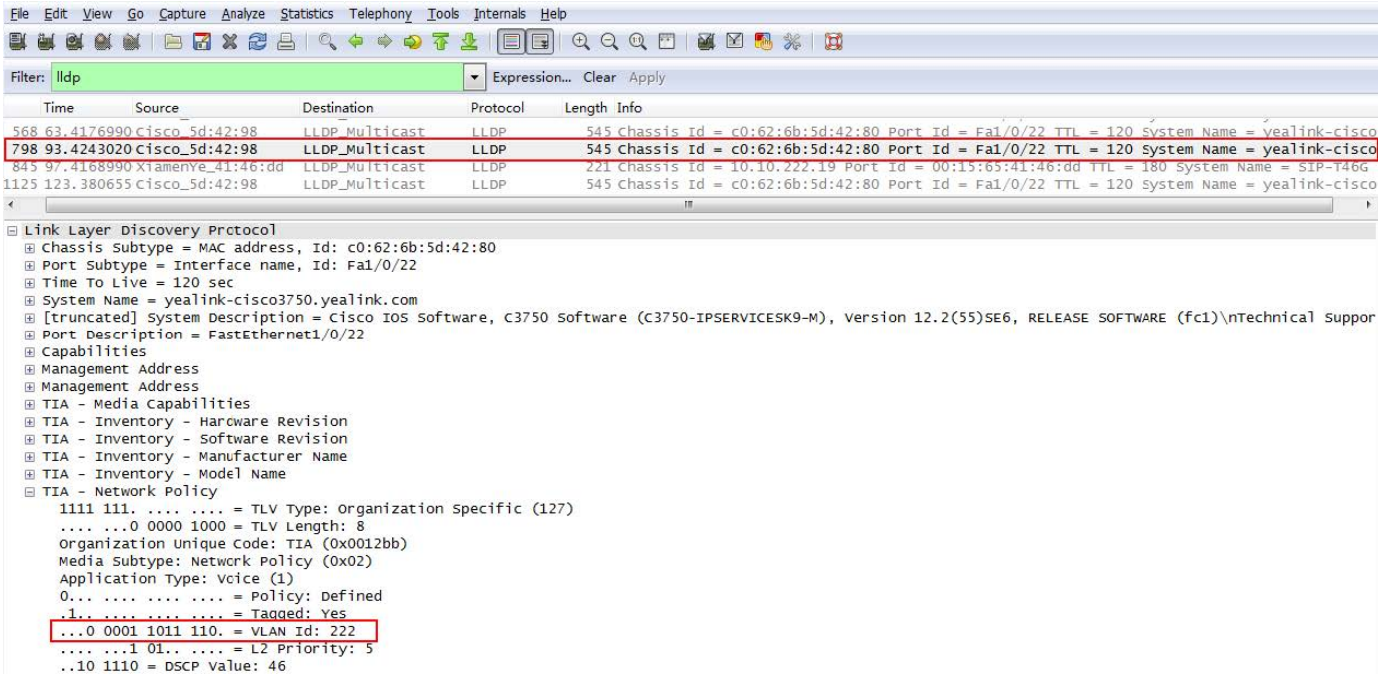
- Periodically advertises information (e.g., hardware revision, firmware revision, serial number) of the IP phone to a multicast address on the network.

- Allows LLDP packets to be received from the Internet (WAN) port or WLAN port.
- Supports the MAC/PHY configuration (e.g., speed rate, duplex mode).
- Obtains VLAN info from the network policy, which takes precedence over manual settings.

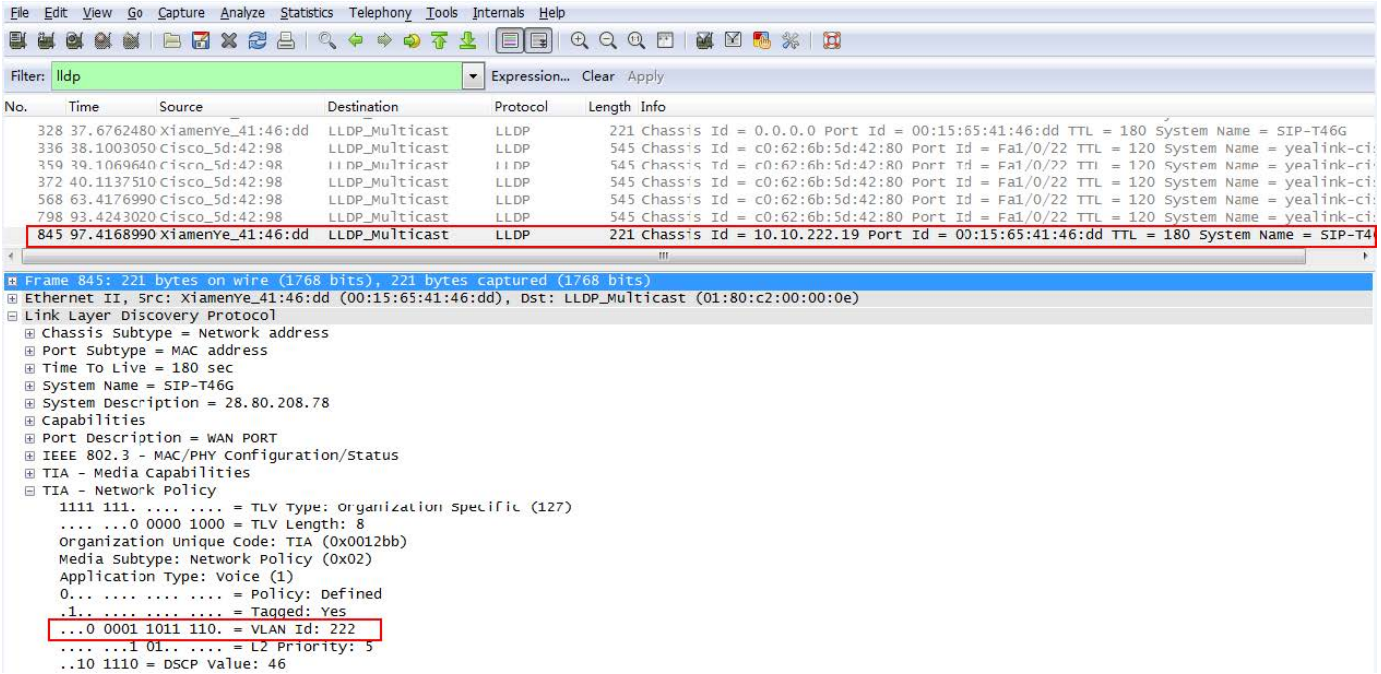
The following figure shows the LLDP packet sent by the IP phone, the packet contains multiple TLVs (before obtaining VLAN ID).



The following figure shows the LLDP packet received by the IP phone, the packet contains multiple TLVs (sent by the switch).



The following figure shows the LLDP packet sent by the IP phone, the packet contains multiple TLVs (after obtaining VLAN ID).



CDP

Description

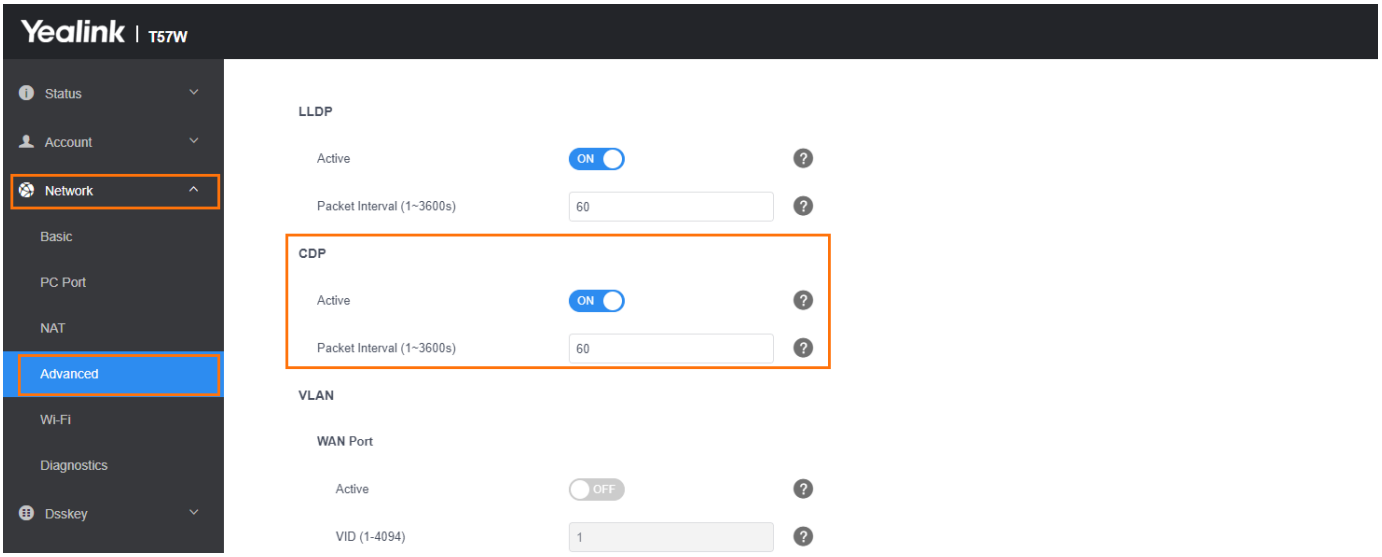
CDP (Cisco Discovery Protocol) allows the phones to receive and/or transmit device-related information from/to directly connected devices on the local network.

When the CDP feature is enabled on the phones, the phones periodically advertise their own information to the directly connected CDP-enabled switch. The phones can also receive CDP packets from the connected switch and obtain their VLAN IDs.

Configure CDP Feature on Yealink IP Phones

Set via the Web User Interface

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



Configuration parameter

static.network.cdp.enable

static.network.cdp.packet_interval

Parameter	Permitted Values	Default	Description
static.network.cdp.enable[1]	**0**-Disabled **1**-Enabled, the phone attempts to determine its VLAN ID through CDP.	1	It enables or disables the CDP feature.
static.network.cdp.packet_interval[1]	Integer from 1 to 3600	60	It configures the interval (in seconds) that determines how often the phone sends the CDP request. It works only if static.network.cdp.enable is set to 1 (Enabled).

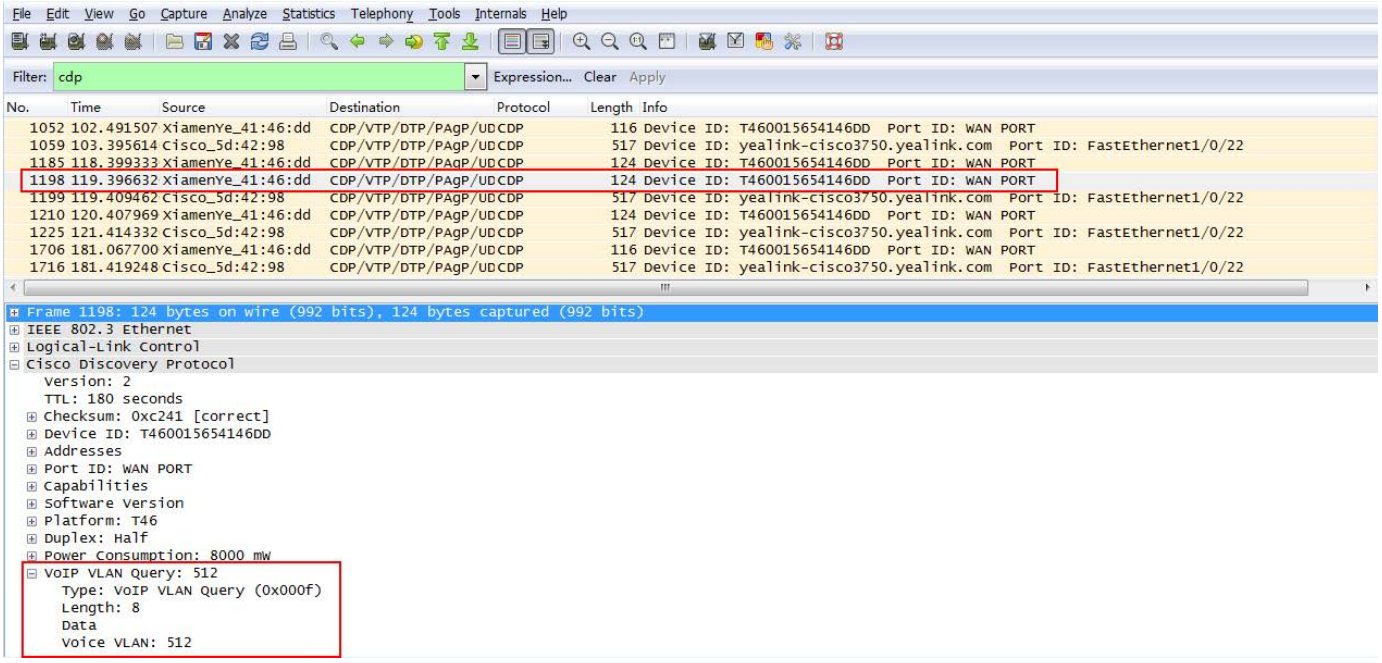
[1]If you change this parameter, the phone will reboot to make the change take effect.

Verify the Configuration

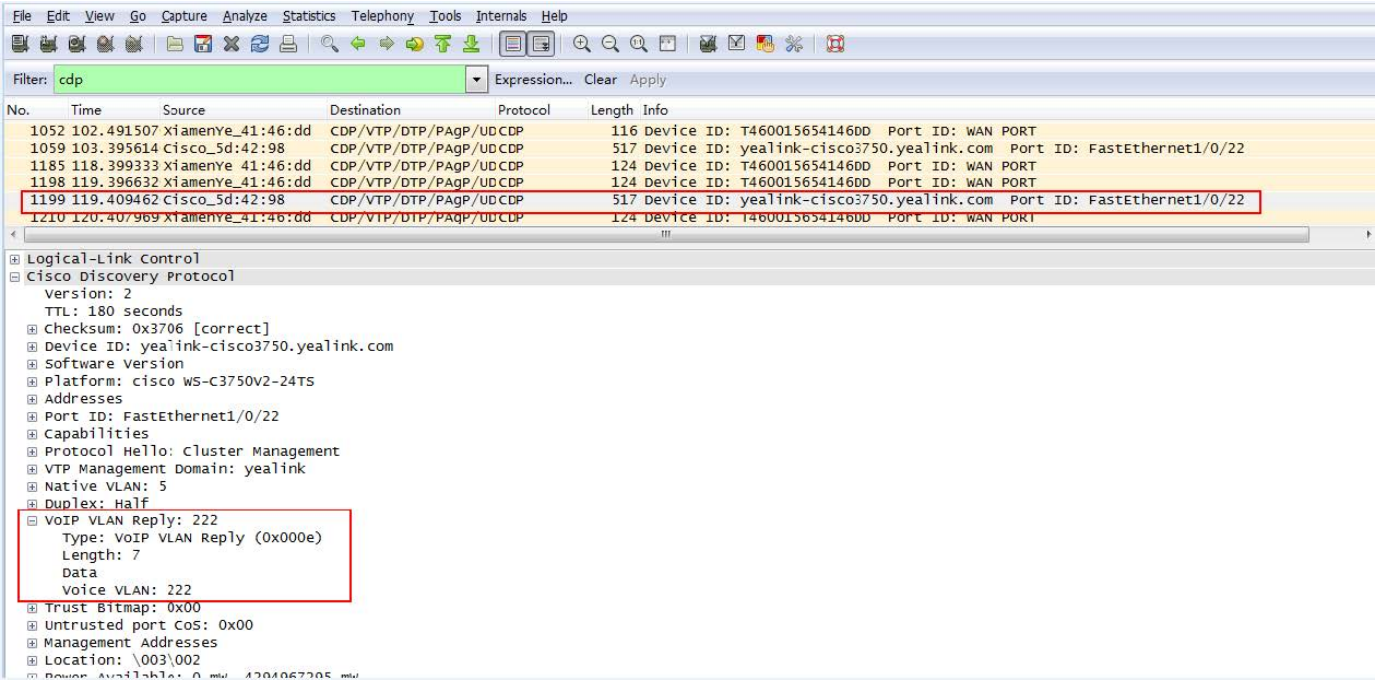
After the CDP feature is enabled, the IP phone performs the following:

- Periodically advertises information (e.g., software revision, device ID, power consumption) of the IP phone to a multicast address on the network.
- Allows CDP packets to be received from the Internet (WAN) port or WLAN port.
- Obtains VLAN ID of connecting ports.

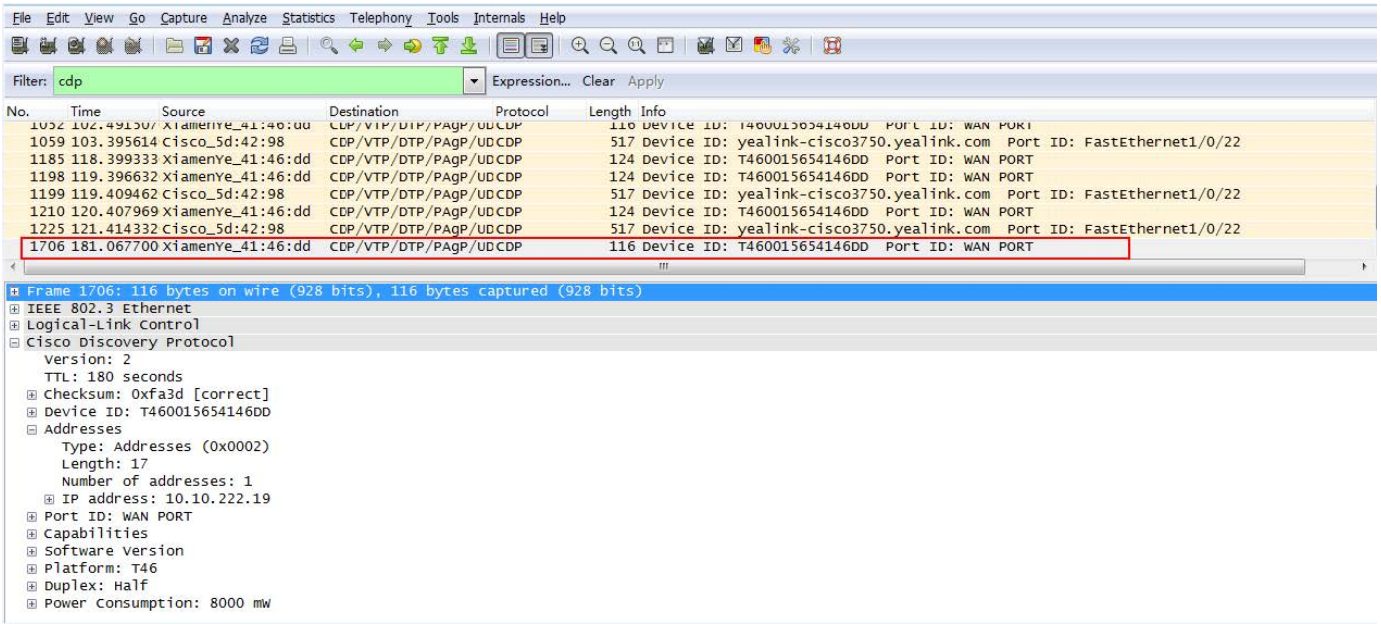
The following figure shows the CDP packet sent by the IP phone (before obtaining VLAN ID-with VLAN Query field).



The following figure shows the CDP packet received by the IP phone (with VLAN Reply field).



The following figure shows the CDP packet sent by the IP phone (after obtaining VLAN ID-without VLAN Query field).



DHCP VLAN

Description

When the VLAN discovery method is set to DHCP, the phone examines the DHCP option for a valid VLAN ID. You can customize the DHCP option used to request the VLAN ID.

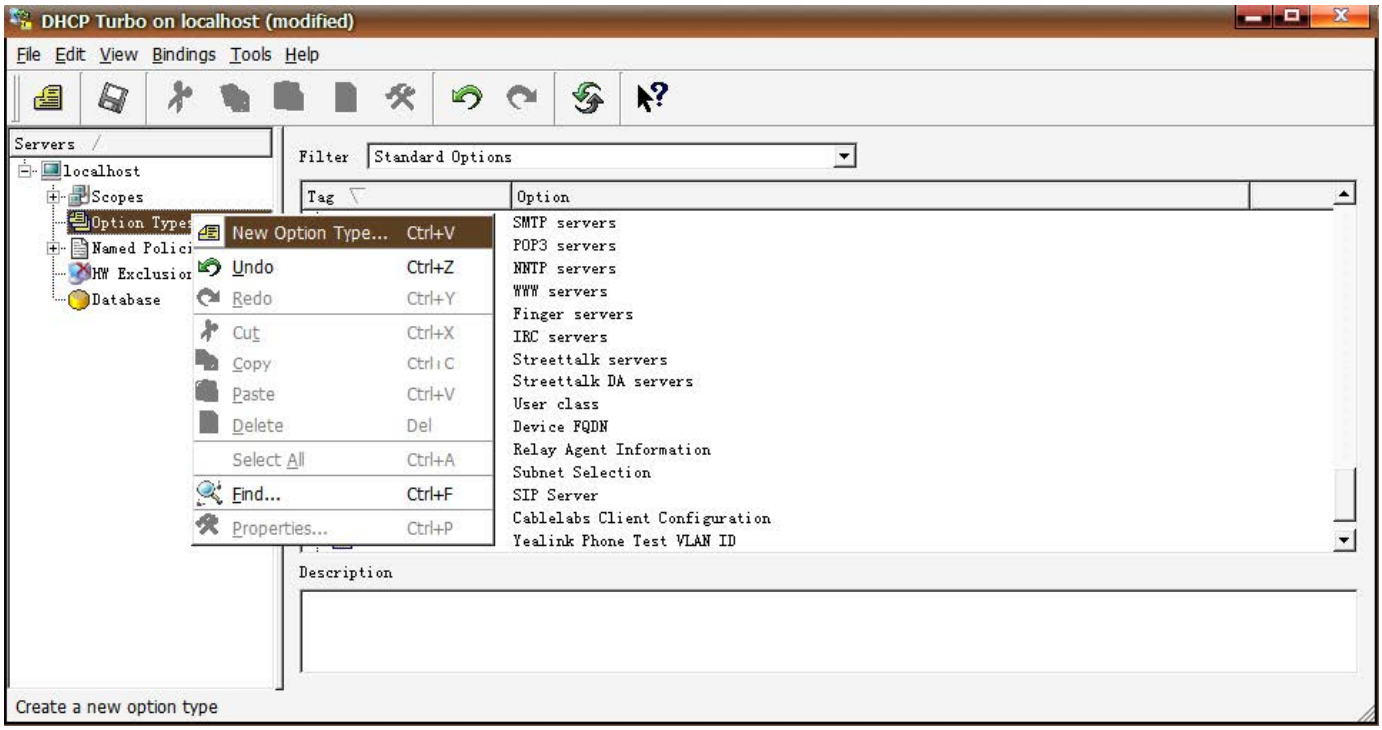
Configure DHCP Option on a DHCP Server

Before using the DHCP VLAN feature on IP phones, you must make sure that the DHCP option on the DHCP server is configured properly. This section provides instructions on how to configure a DHCP option for Windows using DHCP Turbo.

Procedure:

1. Start the DHCP Turbo application.

2. Right-click **Option Types**, and then select **New Option** Type.



3. Enter the desired option in the **Tag** field.

   The custom options range from 128 to 254.

4. Enter the desired name in the **Name** field

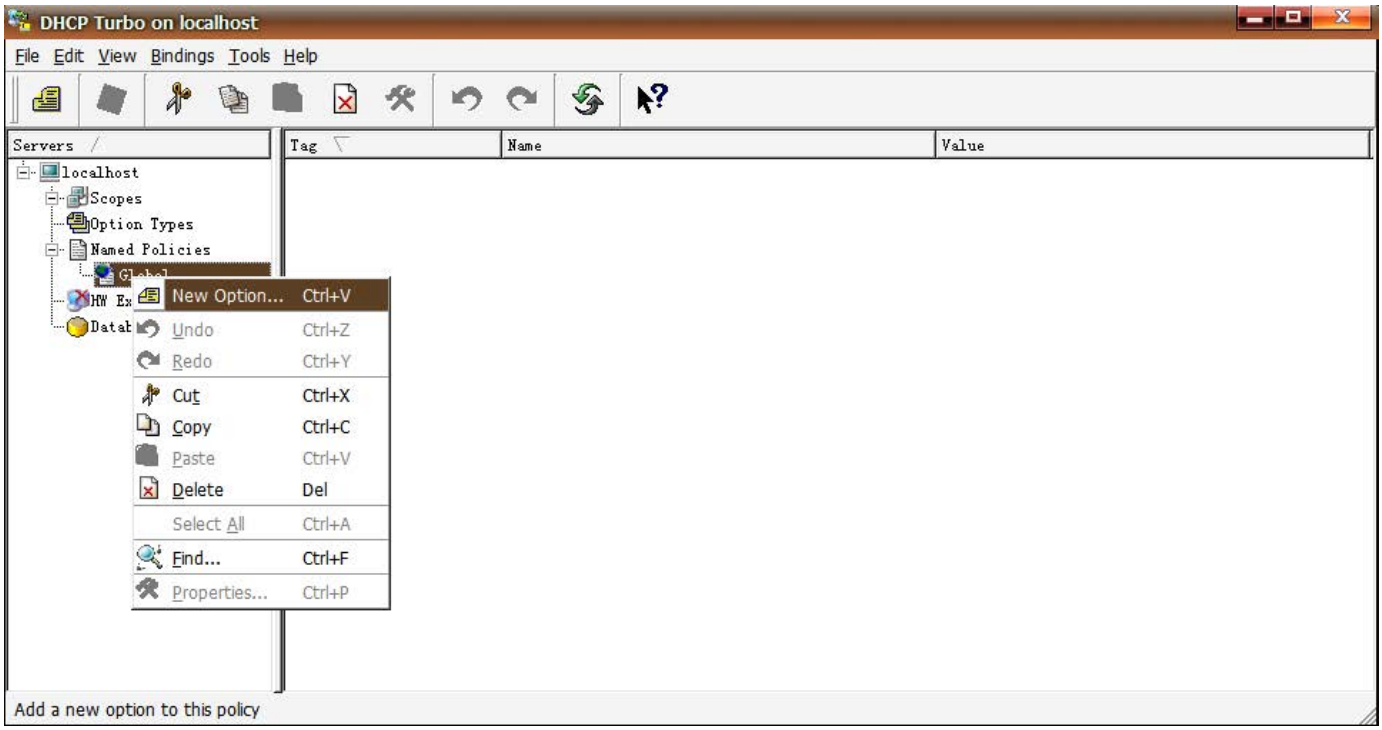
5. Select a **string** from the pull-down list of **Type**.

6. Click **OK** to finish setting the option properties.

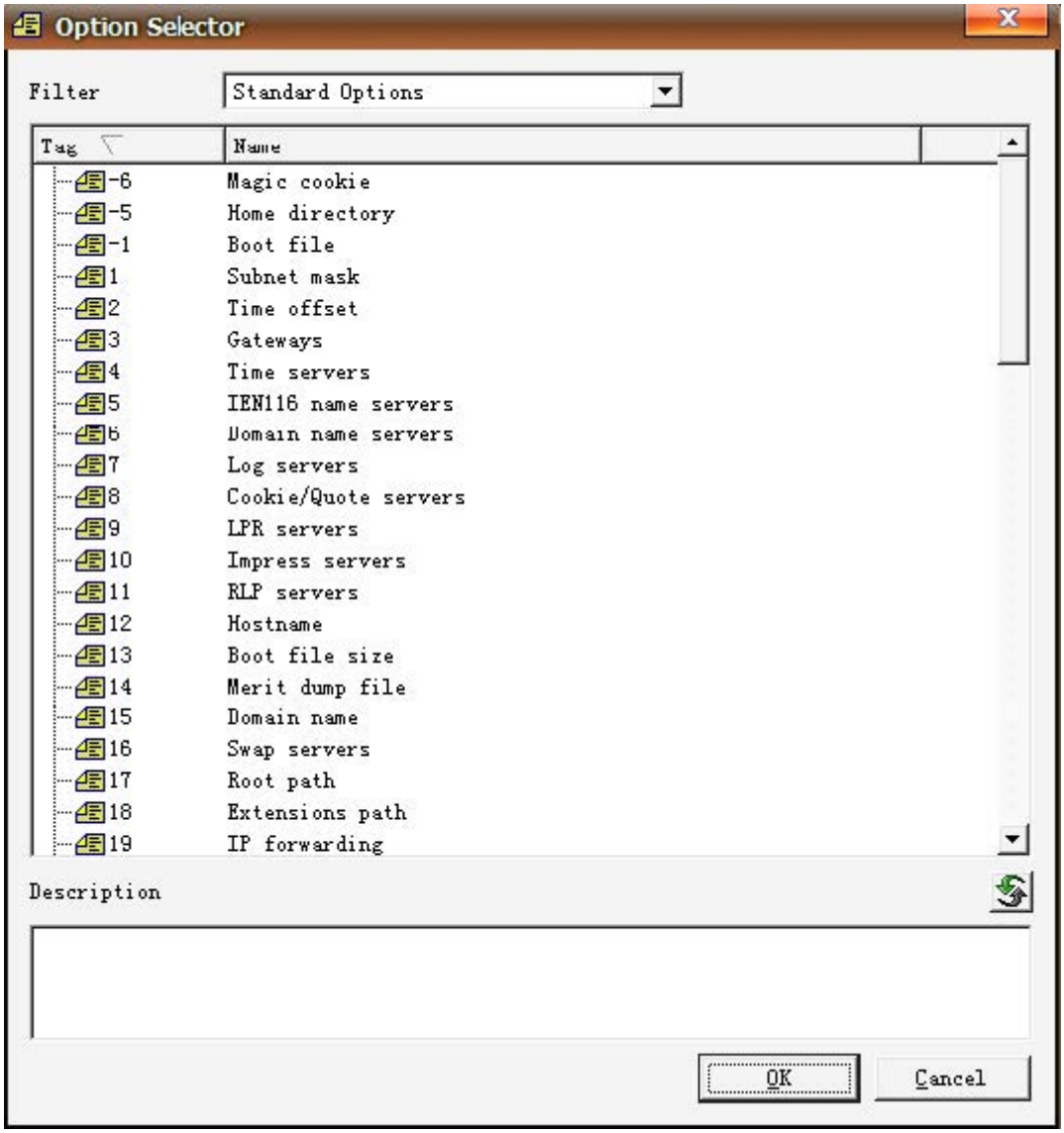
7. Click to accept the change.

8. Double-click **Named Policies**.

9. Right-click **Global**, and then select **New Option**.

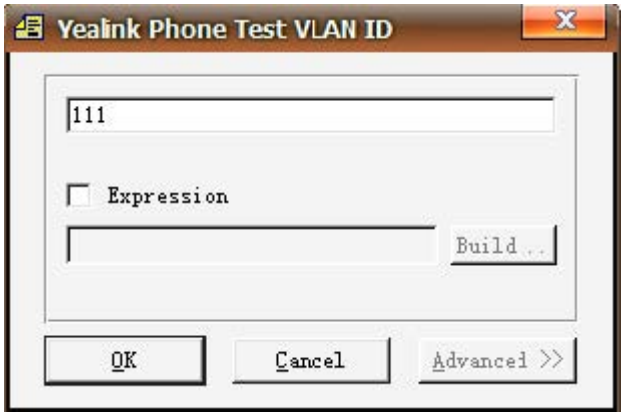


11. The Option Selector screen displays as below:

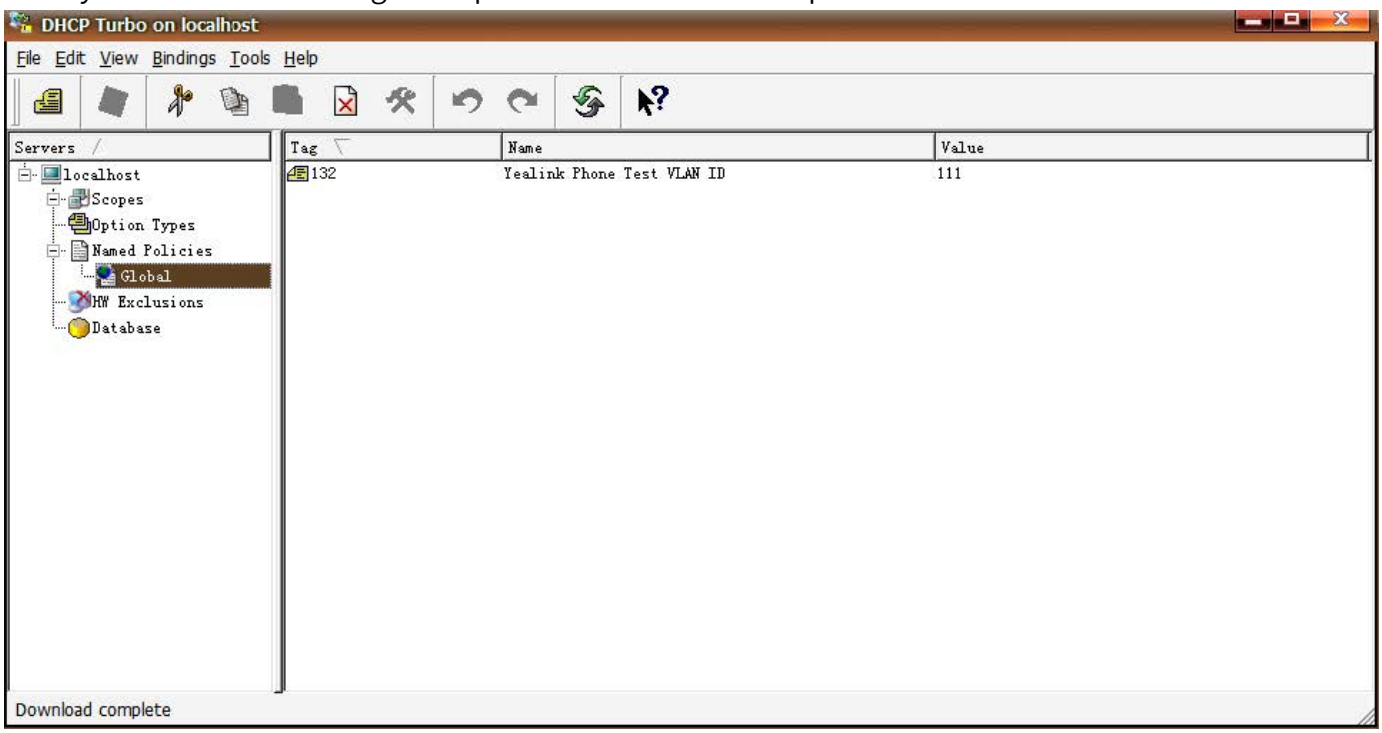


10. Scroll down and double-click the option created above.

11. Fill in the VLAN ID to be assigned in the input field.
12. Three formats of valid values: VLAN-A=*VLANID, VLANID*, and VID=*VLANID*. VLAN ID ranges from 1 to 4094.



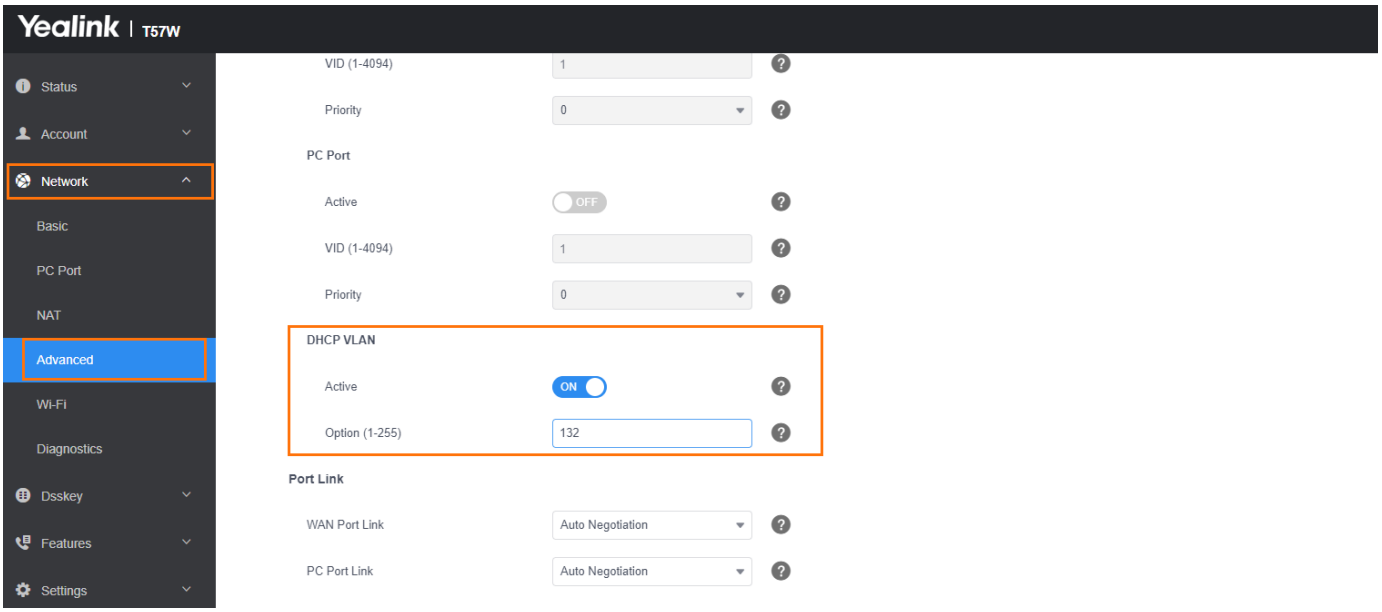
12. Click **OK** to finish setting a custom option.
13. Click to accept the change.
14. Then you can find the configured option under the **Global** option.



Configure DHCP Option on Yealink IP Phones

Set via the Web User Interface

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



Configuration parameter

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

Parameter	Permitted Values	Default	Description
static.network.vlan.dhcp_enable[1]	**0**-Disabled **1**-Enabled	1	It enables or disables the DHCP VLAN discovery feature.
static.network.vlan.dhcp_option[1]	Integer from 1 to 255	132	It configures the DHCP option from which the phone will obtain the VLAN settings. Multiple DHCP options (at most five) are separated by commas.

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

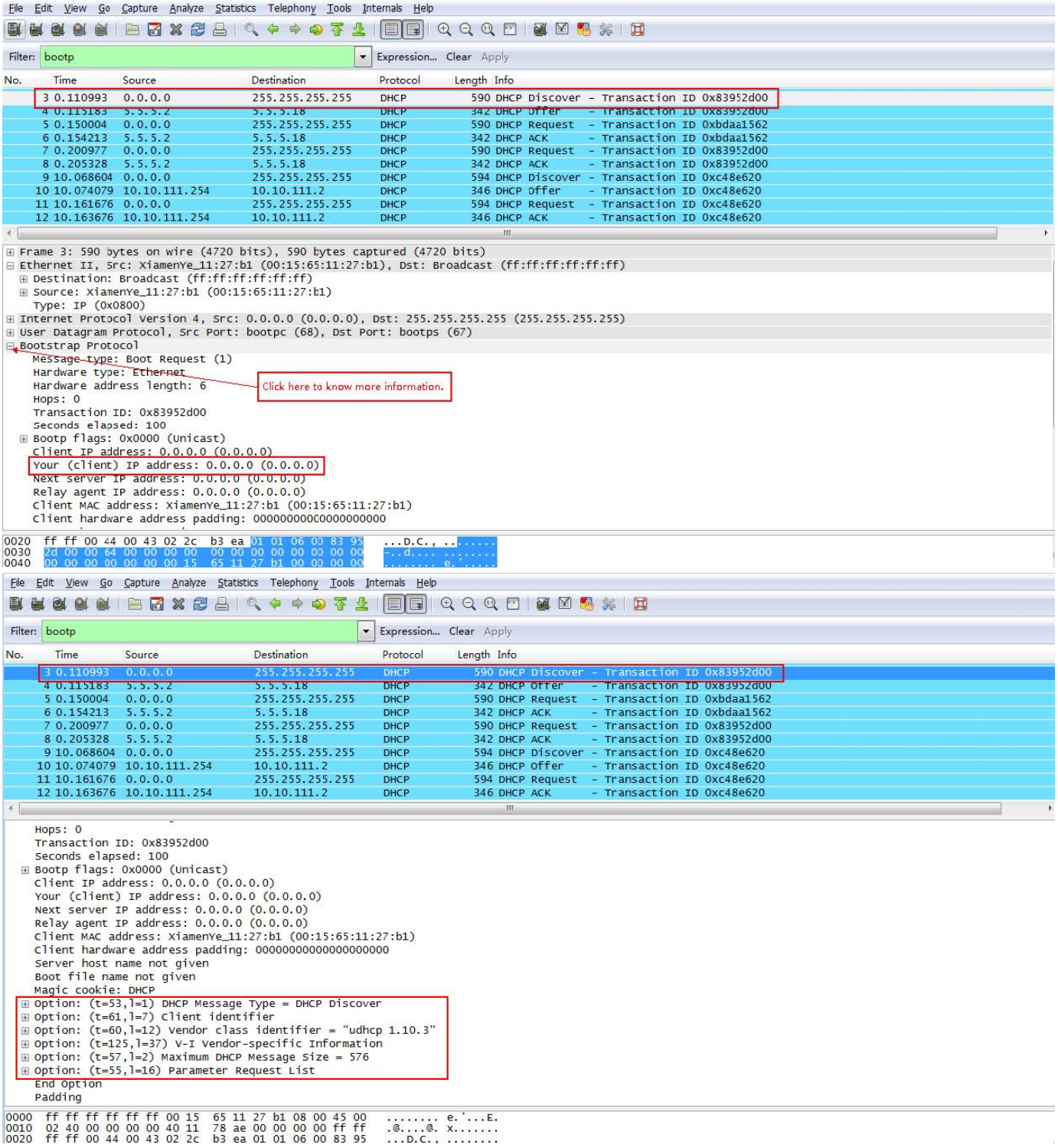
Verify the Configuration

When the IP phone is configured to use DHCP for VLAN discovery, and the DHCP option is set to 132, the following processes occur:

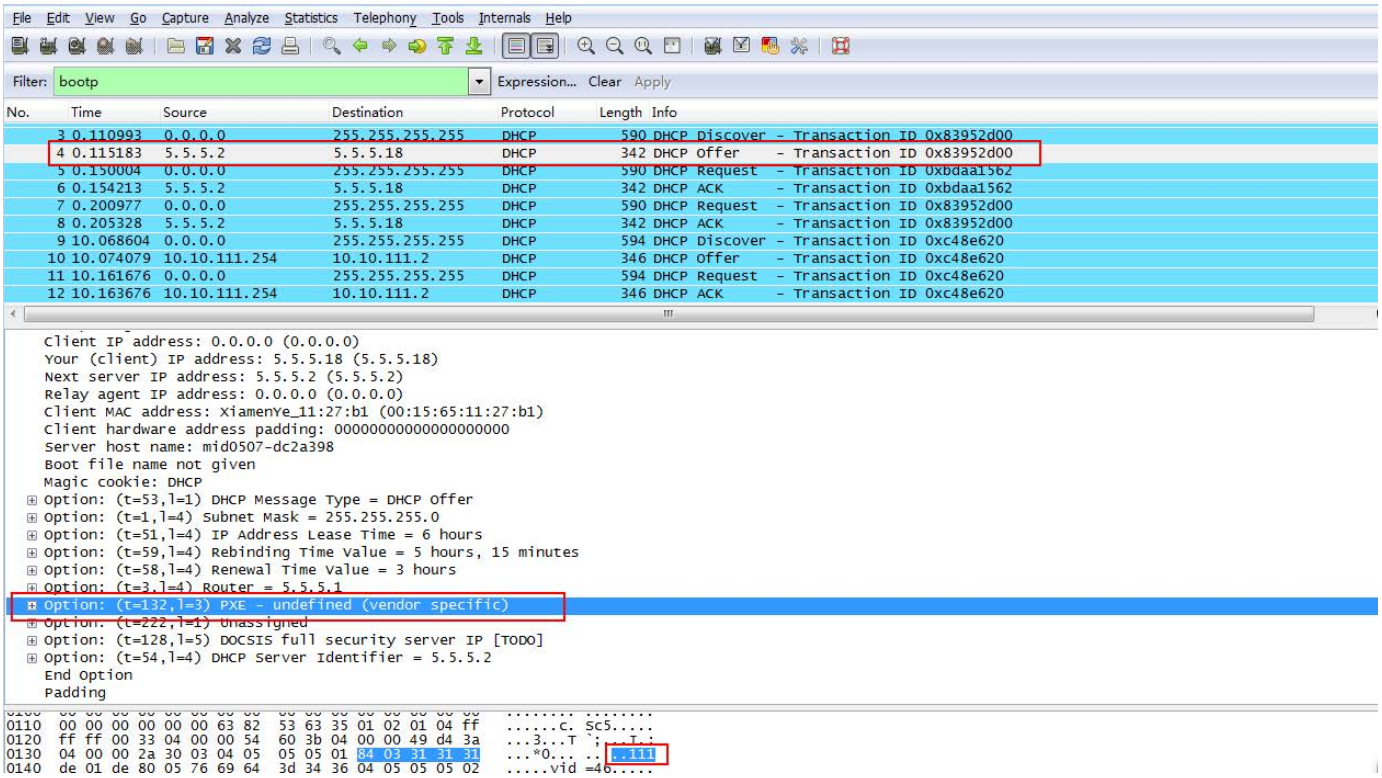
1. The IP phone broadcasts a DHCP Discover message to find out if there is a DHCP server available.
2. If the DHCP server sends a DHCP Offer message with Option 132, the phone will accept the Offer, send a DHCP Request, and save the VLAN ID provided by the DHCP server in the DHCP option 132.
3. After obtaining the VLAN ID from the DHCP server, the phone will release the leased IP address and start a new DHCP Discover cycle with the now known Voice VLAN ID tag.

After this process, the phone will send all packets with the VLAN ID obtained from the DHCP server in the DHCP option 132.

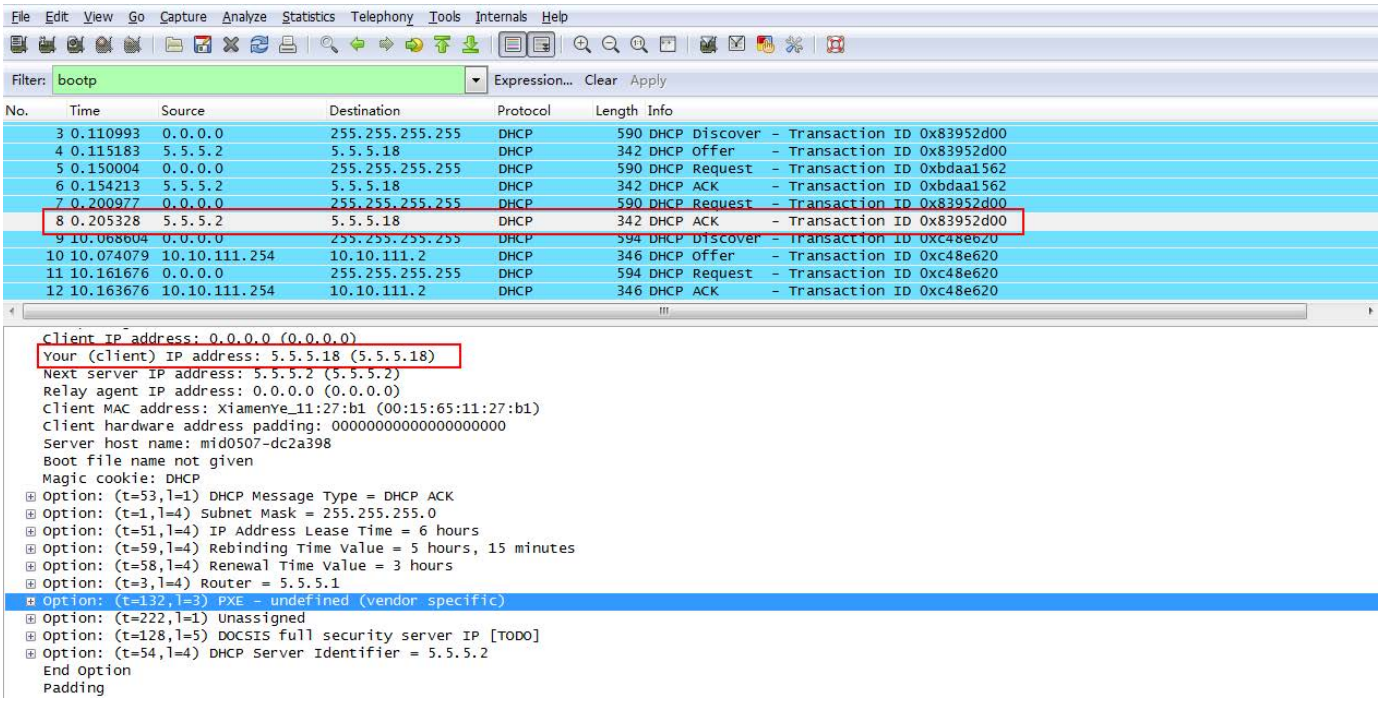
The following figure shows the DHCP Discover message sent by the IP phone (before obtaining the VLAN ID):



The following figure shows the DHCP Offer message received by the IP phone (the DHCP server sends a DHCP Offer message with the Option 132):

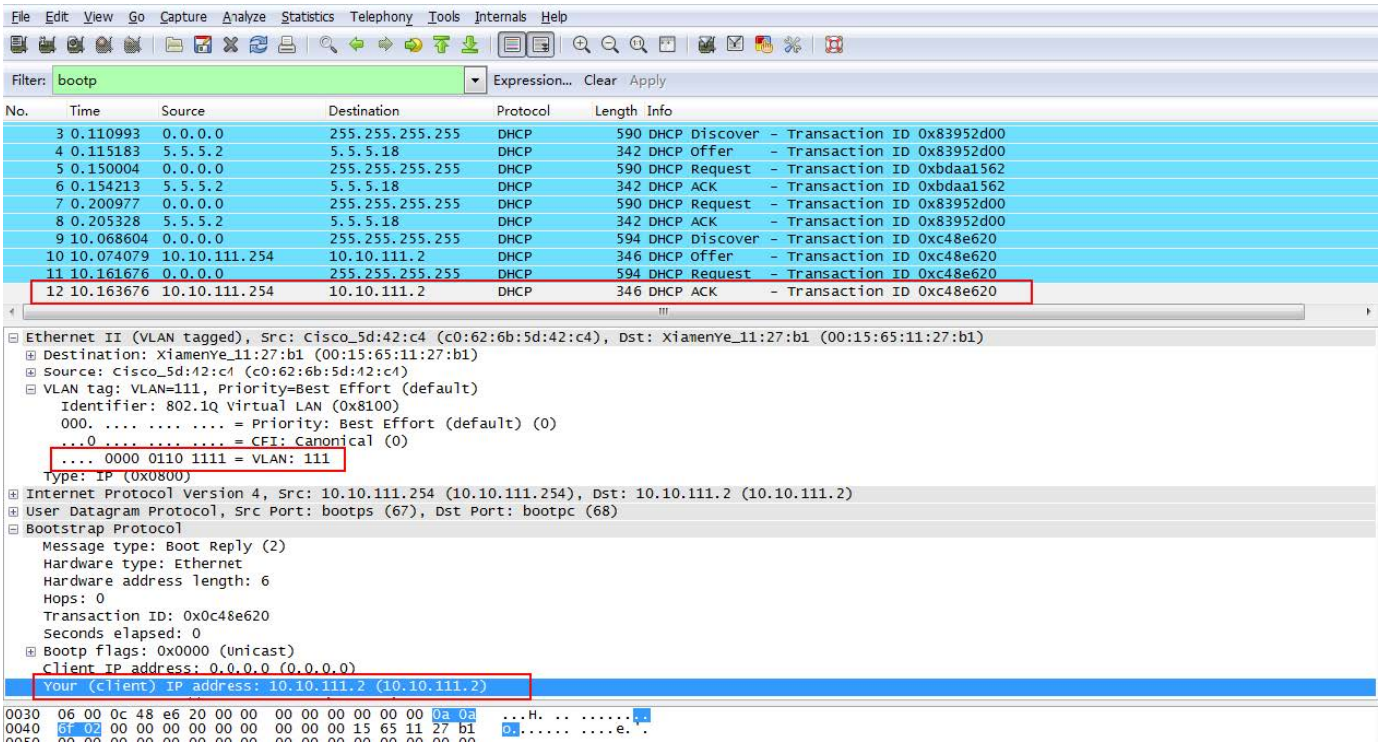


The following figure shows the DHCP message received by the IP phone (the DHCP server sent the ACK message to the phone):



After obtaining the VLAN ID from the DHCP server, the IP phone will release the leased IP address (5.5.5.18) and start a new DHCP Discover message with the VLAN-tag 111.

The following figure shows the DHCP messages received by the IP phone:



After this process, the phone has obtained an IP address (10.10.111.2) from the DHCP server in VLAN 111.

Manual VLAN

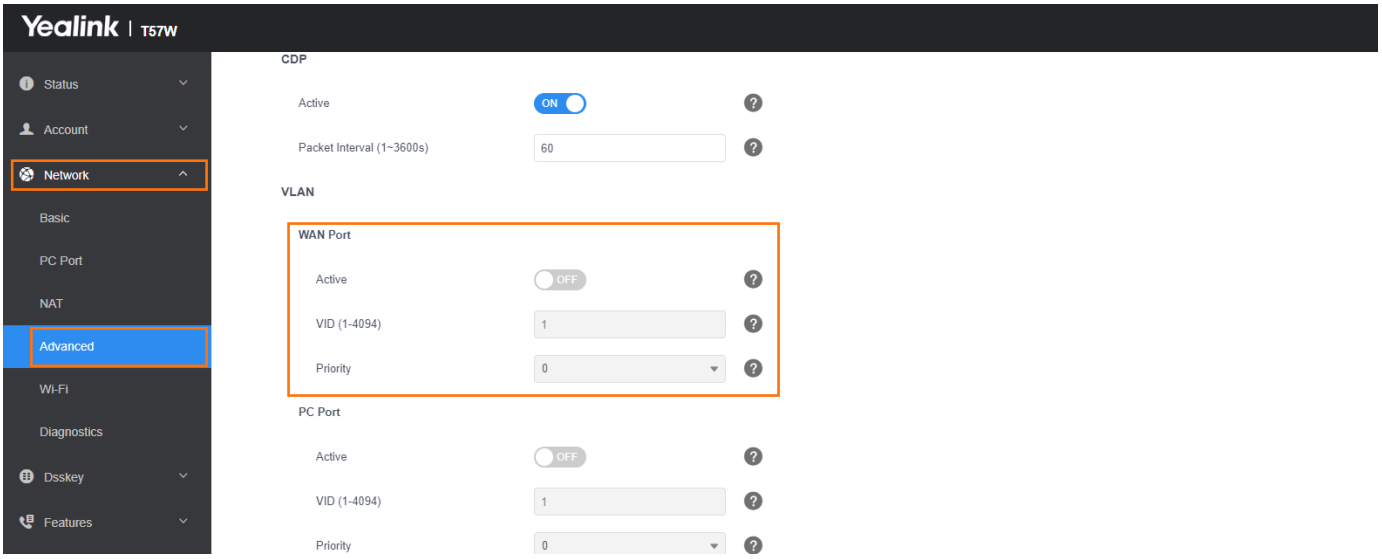
Description

You can configure a VLAN for the Internet port manually. Before configuring VLAN on the phones, you need to obtain the VLAN ID from your network administrator.

Configure VLAN Feature

Set via the Web User Interface

1. On the web user interface, go to **Network** > **Advanced** > **VLAN** > **WAN Port**.



Configuration parameter

```
static.network.vlan.internet_port_enable
static.network.vlan.internet_port_vid
static.network.vlan.internet_port_priority
```

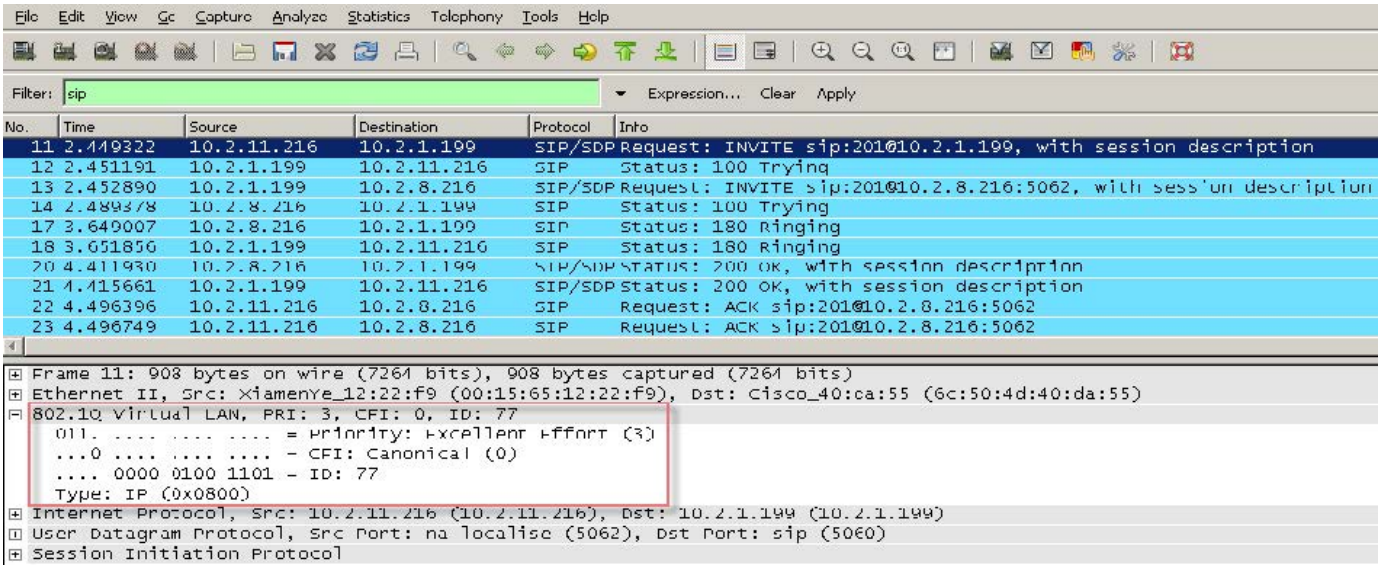
Parameter	Permitted Values	Default	Description
static.network.vlan.internet_port_enable[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the VLAN for the Internet port.
static.network.vlan.internet_port_vid[1]	Integer from 1 to 4094	1	It configures the VLAN ID for the Internet port. It works only if static.network.vlan.internet_port_enable is set to 1 (Enabled).
static.network.vlan.internet_port_priority[1]	Integer from 0 to 7	0	It configures the VLAN priority for the Internet port. 7 is the highest priority, 0 is the lowest priority. It works only if static.network.vlan.internet_port_enable is set to 1 (Enabled).

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

Verify the Configuration

The IP phone reboots after the VLAN feature has been enabled. After starting up, the IP phone will be assigned a subnet address defined for VLAN 77.

The following figure shows the VLAN ID sent and received by the IP phone:



VLAN Change Configuration

Description

You can use the parameter to configure the VLAN change.

Configuration parameter

static.network.vlan.vlan_change.enable

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

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

Real-Time Transport Protocol (RTP) Ports

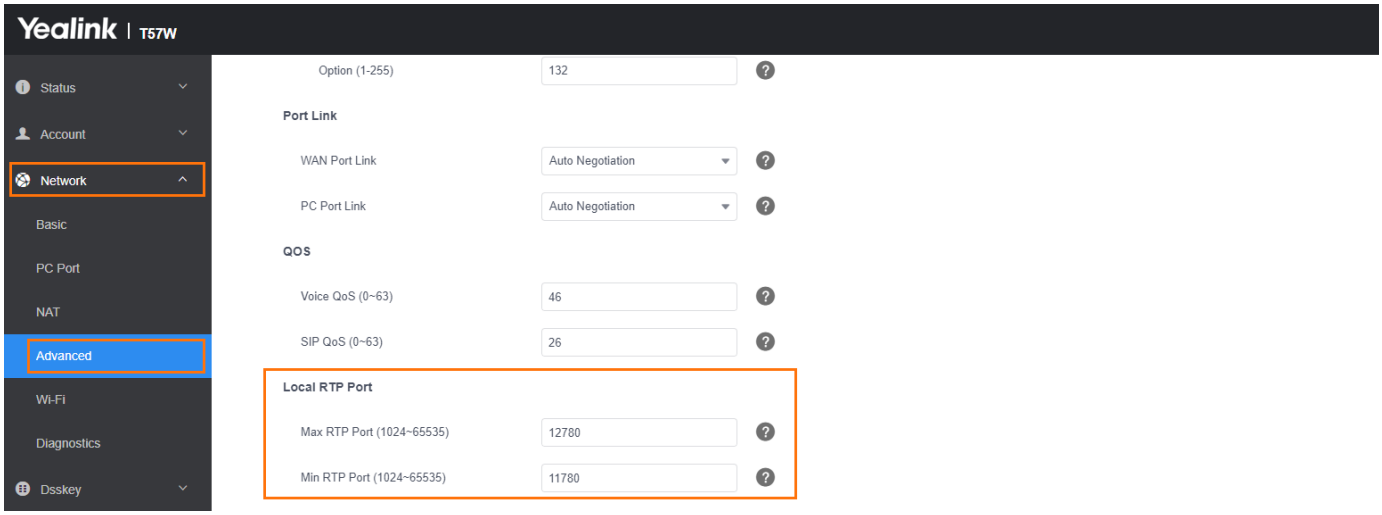
Introduction

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	1178	It configures the minimum local RTP

		0	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

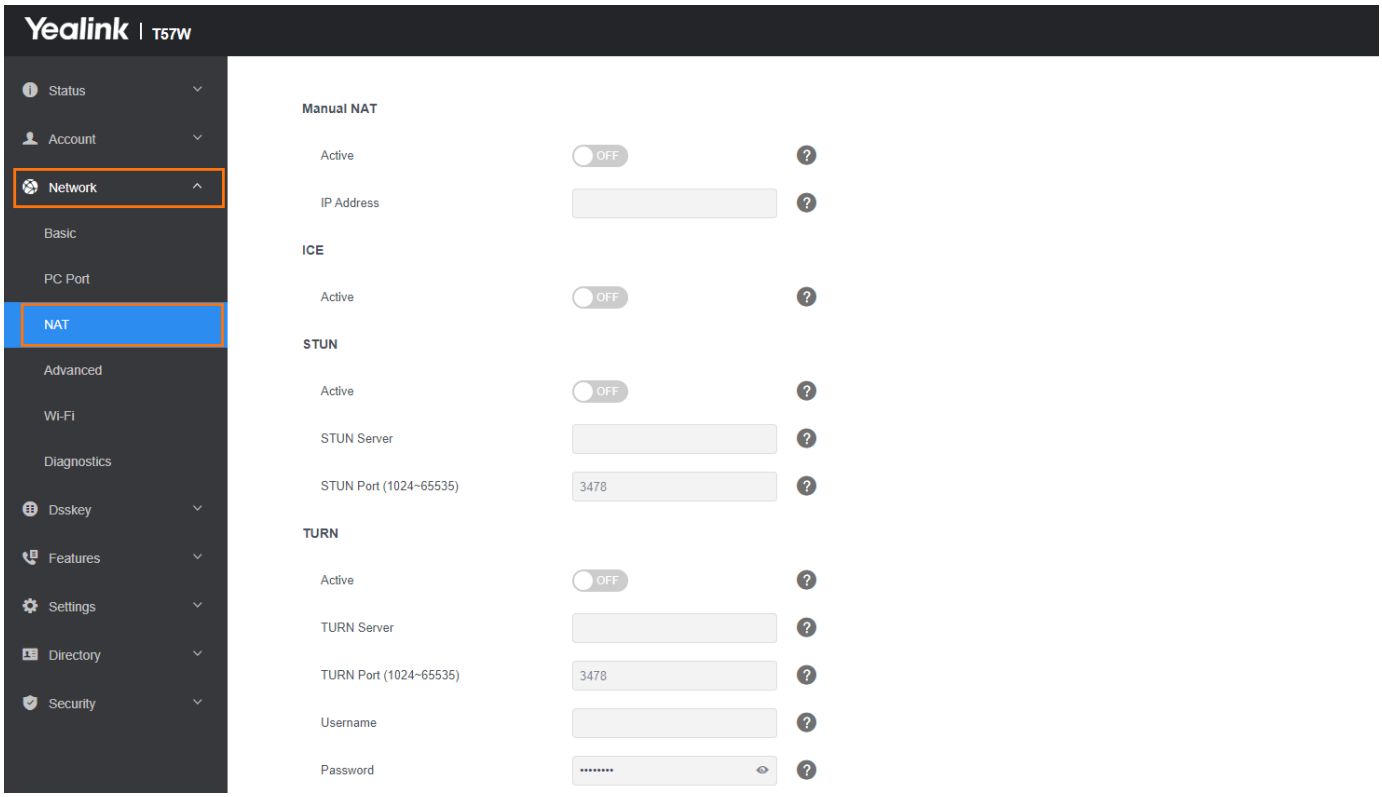
The phones can traverse NAT gateways to establish and maintain connections with external devices.

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. 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. It works only if "static.network.static_nat.enable" is set to 1 (Enabled).
static.sip.nat_	**0**-Disabled	0	It enables or disables the STUN (Simple Traversal of UDP

stun.enable	**1**-Enabled		over NATs) feature.
static.sip.nat_stun.server	String	Blank	It configures the IP address or domain name of the STUN server. 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. 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. 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. 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. 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. 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 forced forward on the DECT manager (DM) during a STUN/ICE call.

			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 forced forward on the DECT manager (DM) during a STUN/ICE call. 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.

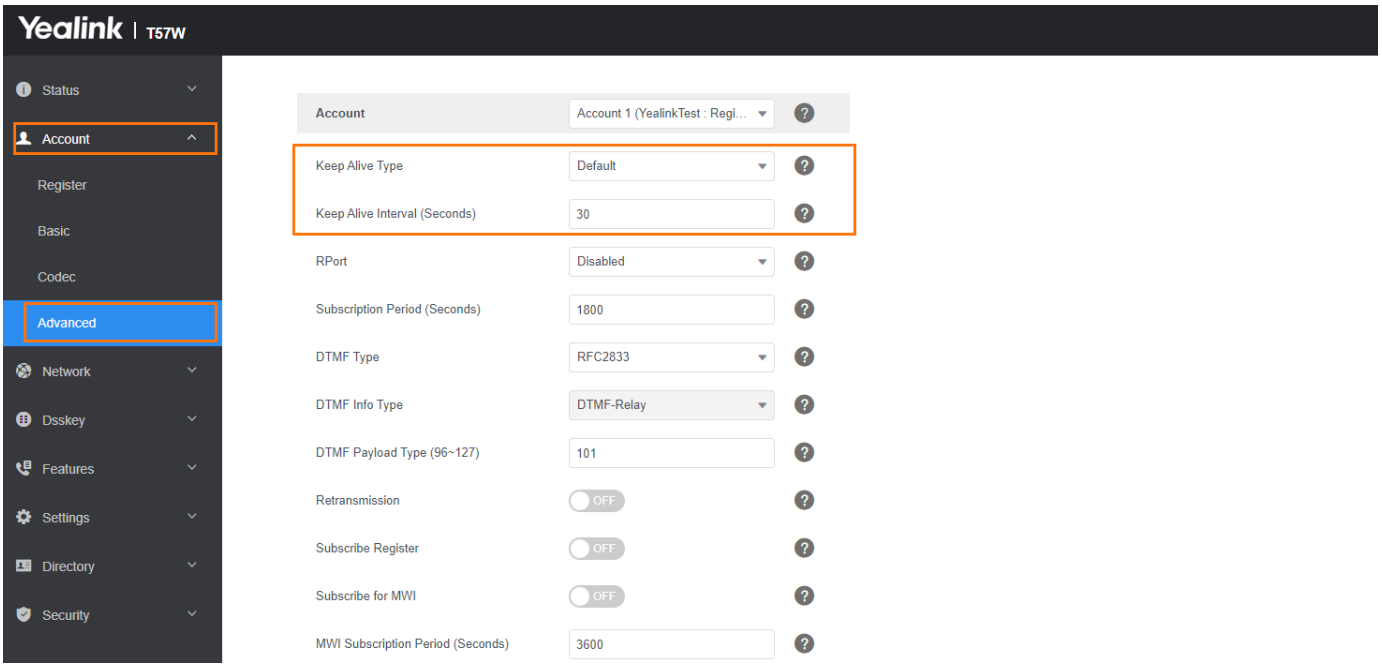
Keep Alive

Yealink phones can send keep-alive packets to the NAT device to keep 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 the 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. 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

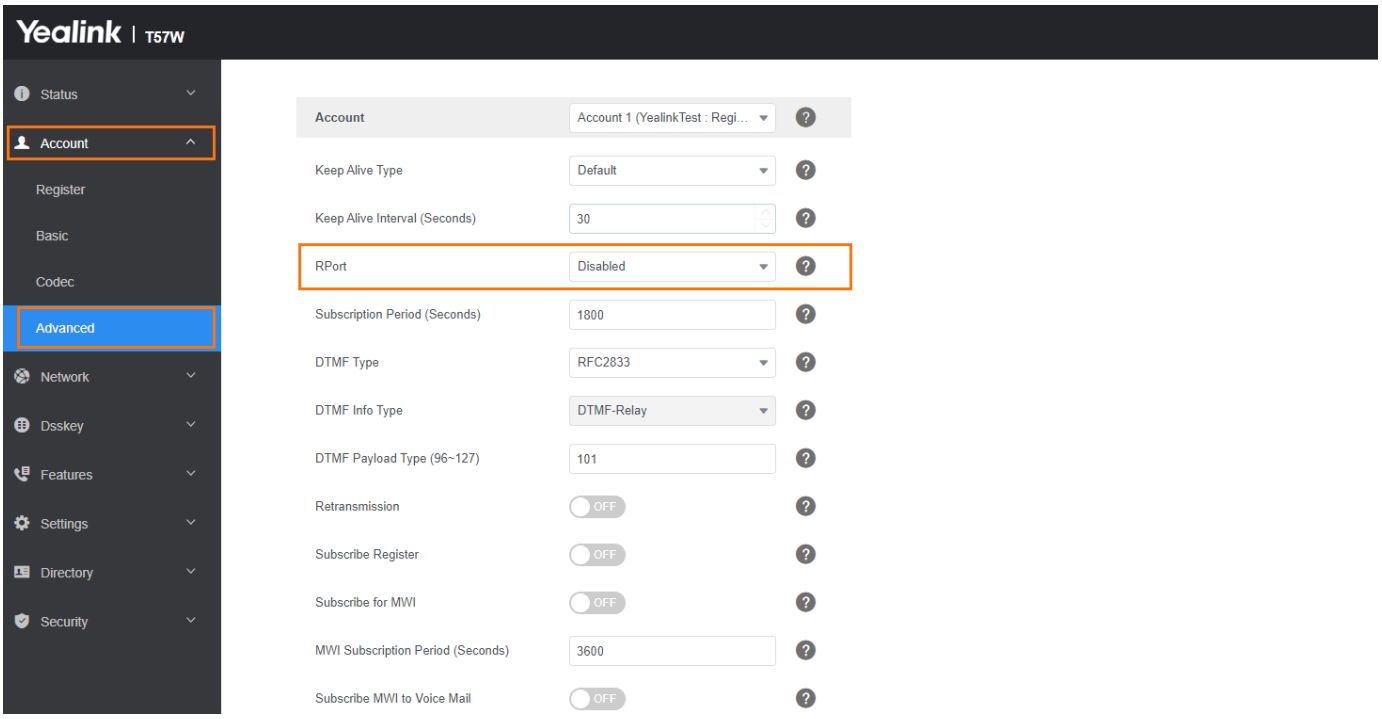
Rport allows a client to request that the server send the response back to the source IP address and port from which the request originated. It helps the phone traverse symmetric NATs.

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 the 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 the 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).

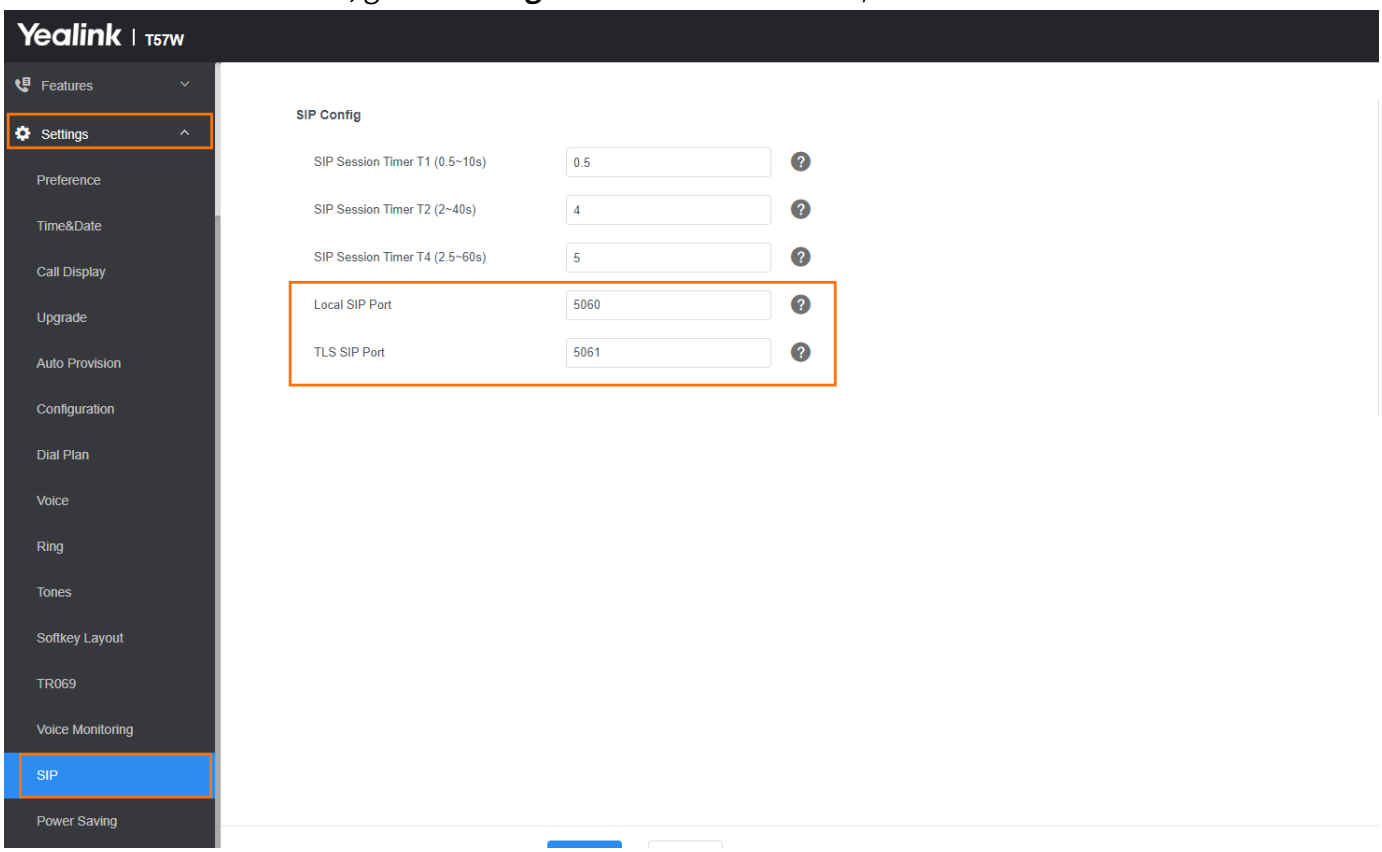
If NAT is disabled, the port number shows in the Via and Contact SIP headers of SIP messages. If NAT is enabled, the phone uses the NAT port number (and NAT IP address) in the Via and Contact SIP

headers of SIP messages, but still uses 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

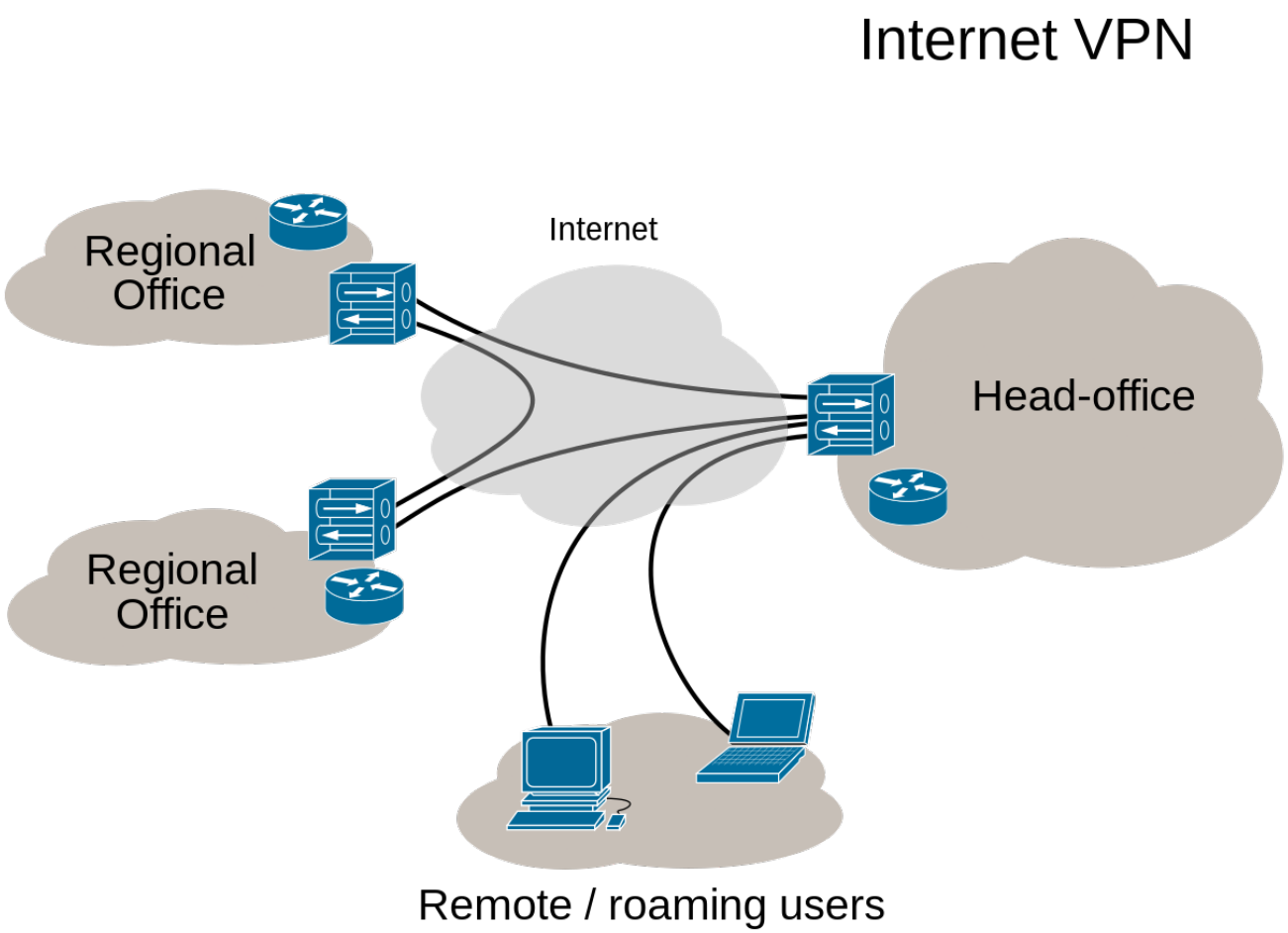
sip.listen_port

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.

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	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.

VPN	
Site to site VPN	Site to site VPN connects entire networks, means that, 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.

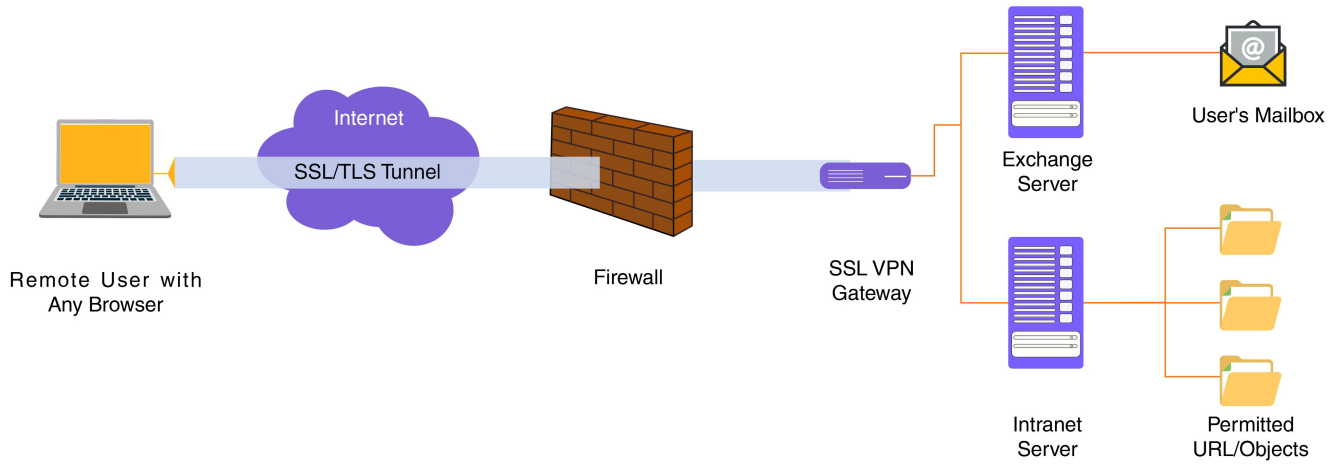
VPN Technology

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 base 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 two most popular VPN tunneling protocols are **SSL** (Secure Socket Layer) and **IPSec** (Internet Protocol Security).

SSL VPN

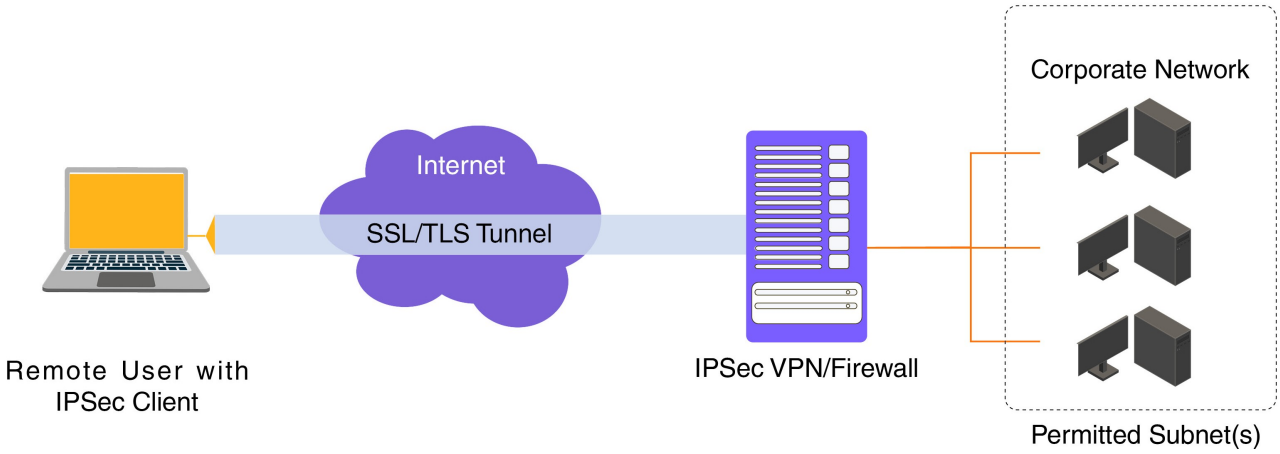
SSL VPN uses the SSL protocol and Transport Layer Security (TLS) protocol to provide a secure connection between remote users and internal network resources. It can be used with a standard web browser and does not require the installation of specialized client software on the end user's device. An SSL 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

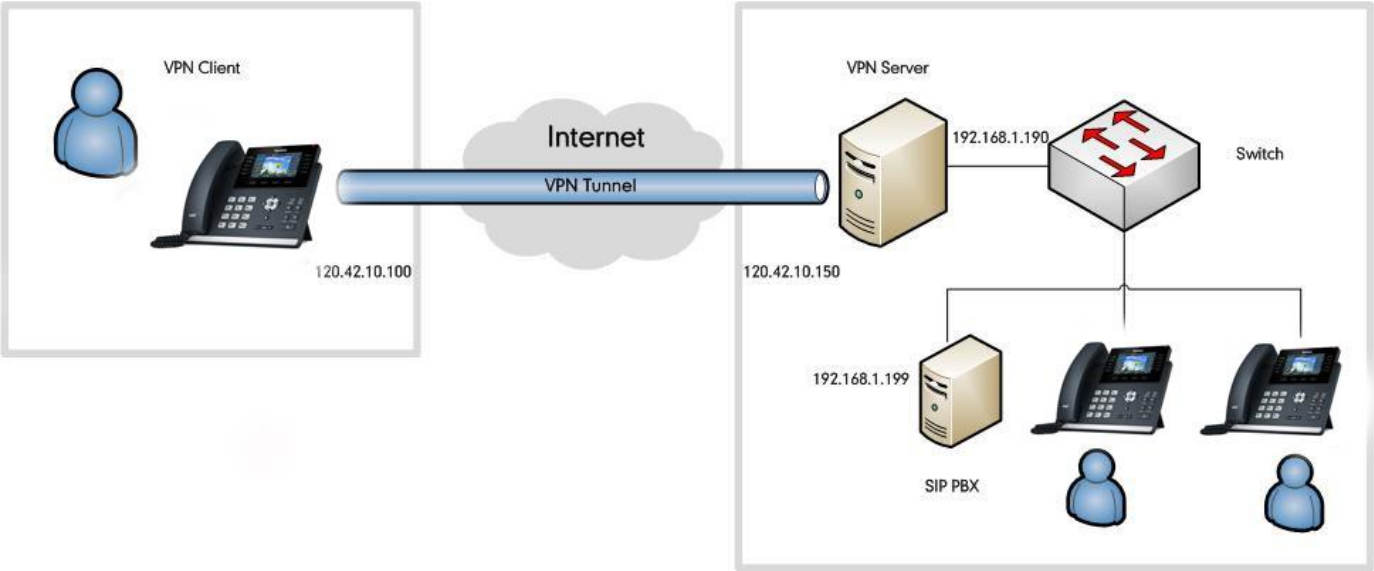
An IPSec VPN uses the standard IPSec mechanism to establish a VPN connection over the public Internet. IPSec is a framework for a set of protocols for security at the network or packet processing

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 an IP 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 IP 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 IP 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 source address 120.42.10.100 and destination address 120.42.10.150.
4. When the packet reaches the VPN server from the Internet, the VPN server de decapsulates 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 atthe 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 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 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 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 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/include/openssl with ssl lib=/usr/local/lib
```

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 IP phones:

1. Enter 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 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]:
```

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.

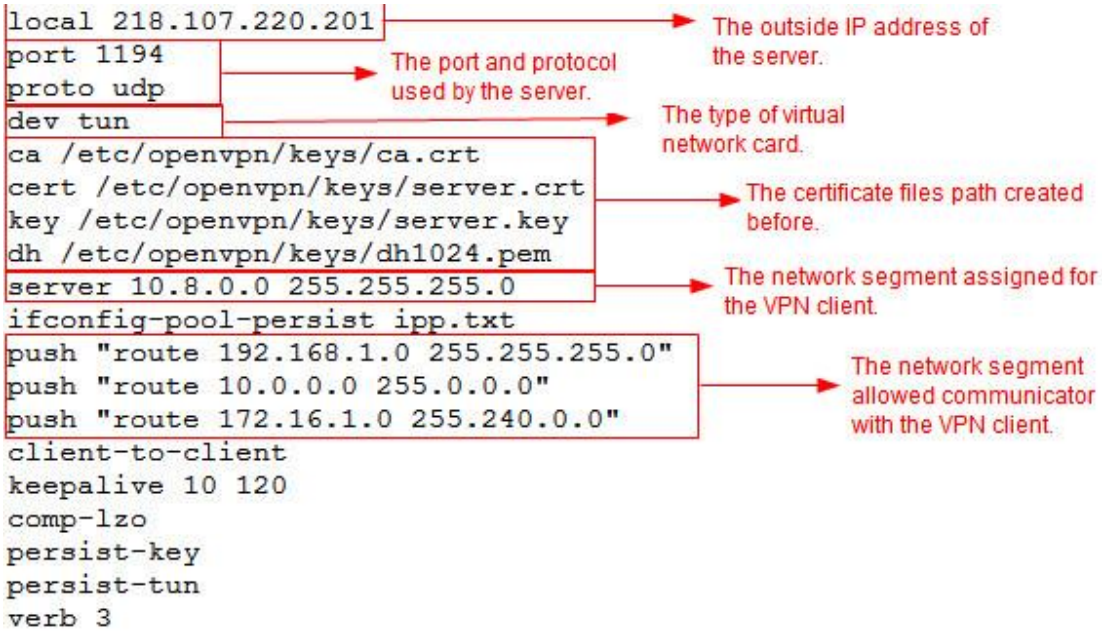
```
[root@localhost openvpn 2.1.4]# cp sample config files/server.conf /etc/openvpn
```

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

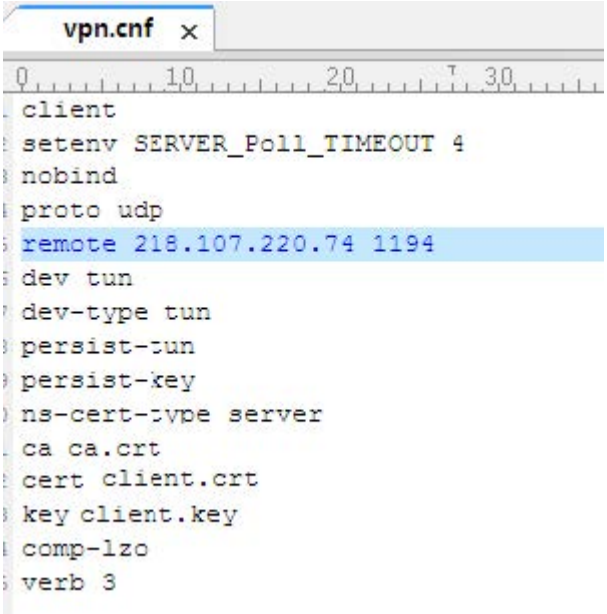
The following parameters should be configured as the same as those of the server.

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

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

1. Enter 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
```

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

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

4. 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
```

5. 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]:
```

6. 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
```

7. 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
```

8. 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.

5. The following shows an example:

```
local 218.107.220.201
port 1194
proto udp
dev tun
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/server.crt
key /etc/openvpn/keys/server.key
dh /etc/openvpn/keys/dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.1.0 255.255.255.0"
push "route 10.0.0.0 255.0.0.0"
push "route 172.16.1.0 255.240.0.0"
client-to-client
keepalive 10 120
comp-lzo
persist-key
persist-tun
verb 3
```

The outside IP address of the server.

The port and protocol used by the server.

The type of virtual network card.

The certificate files path created before.

The network segment assigned for the VPN client.

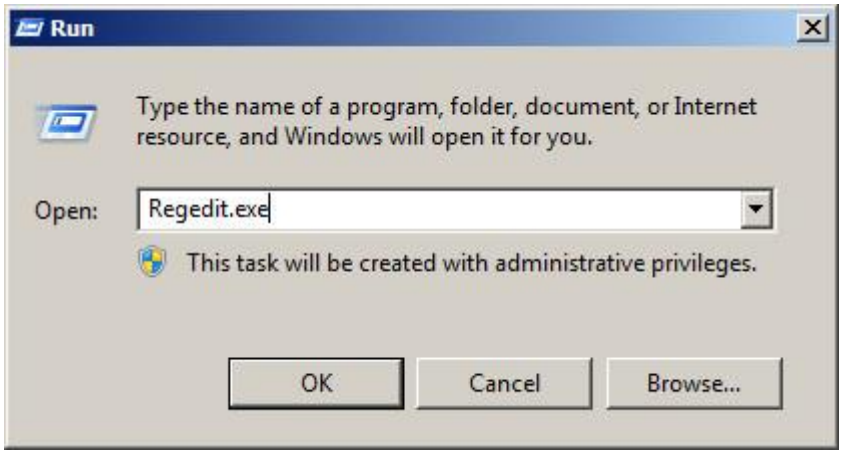
The network segment allowed communicator with the VPN client.

7. 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 TCP/IP forwarding:

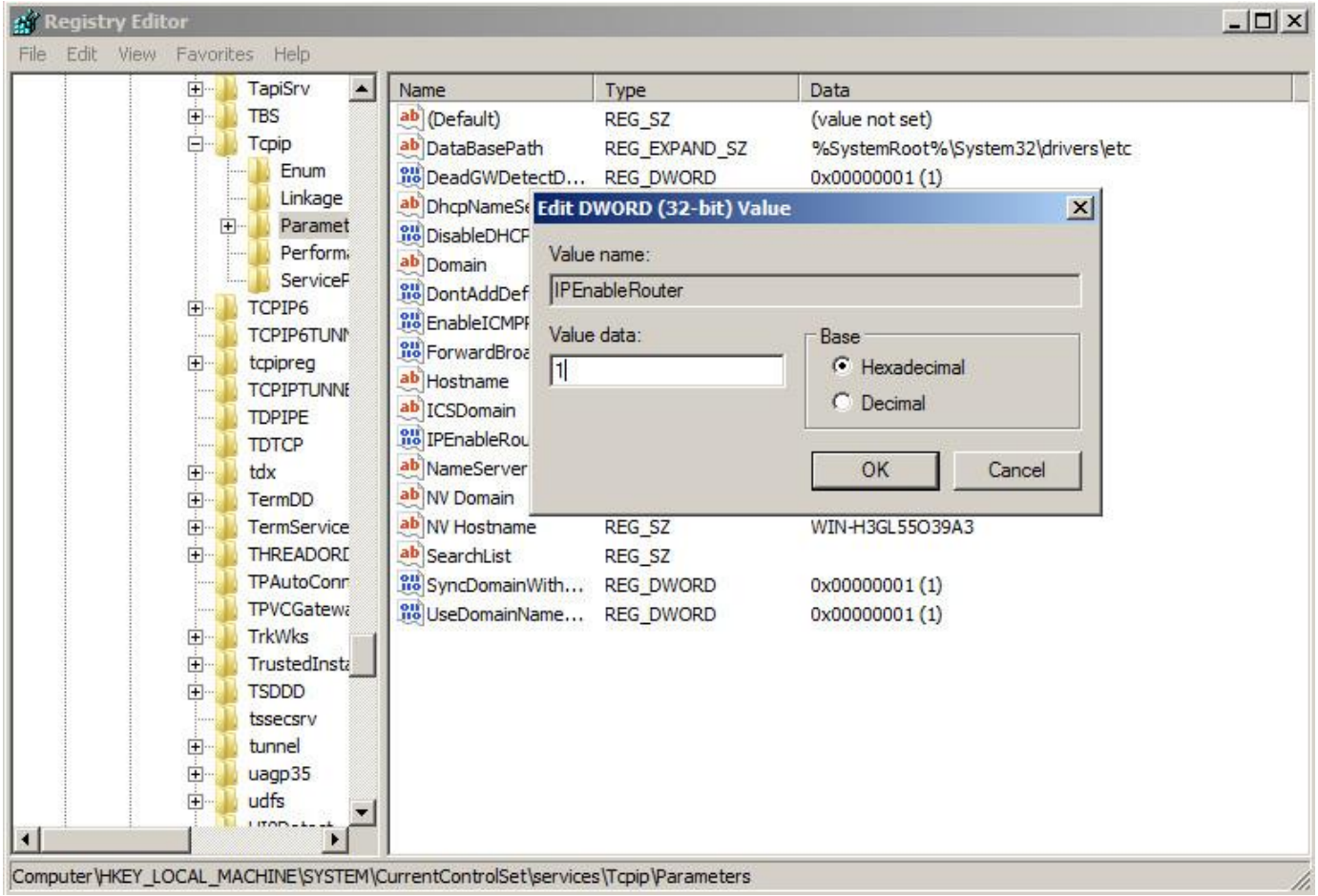
1. Click **Start**–>**Run**.

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 the 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.

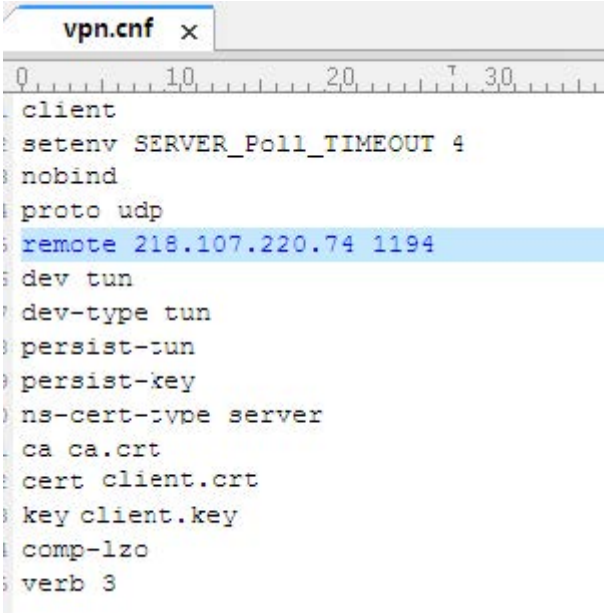
5. Copy ca.crt, client.crt, and client.key files to the keys folder created above.

6. Edit the file vpn.cnf.

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

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

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



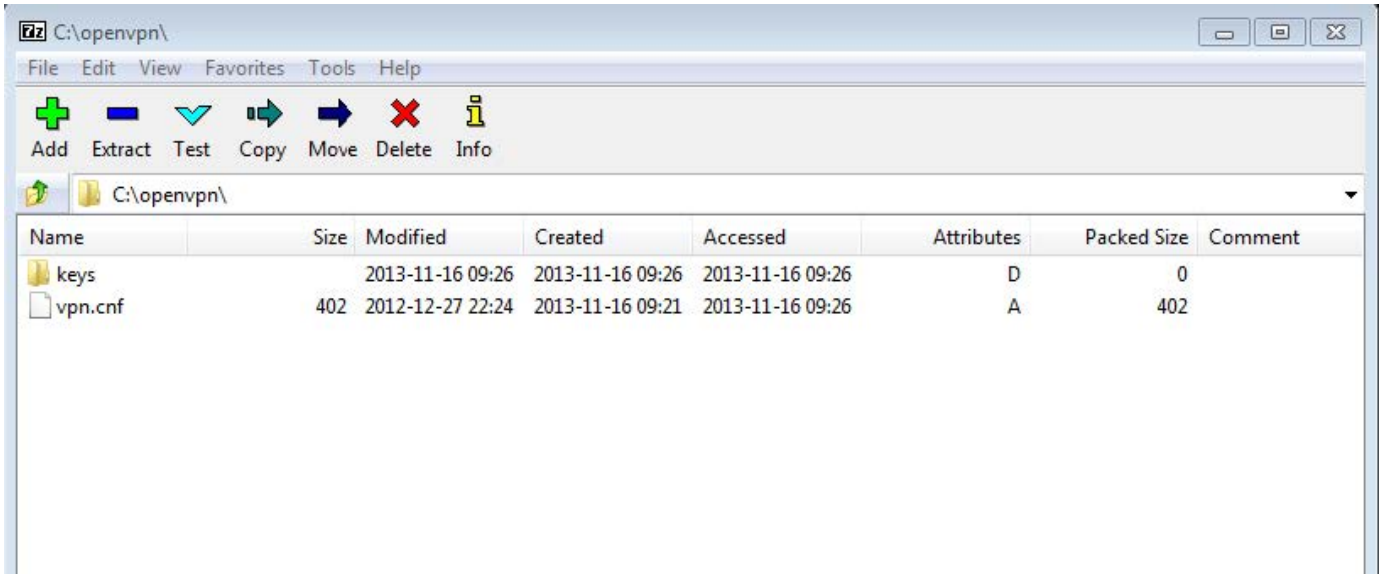
1. Save the change.

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

1. Download and install 7-Zip on the local system.

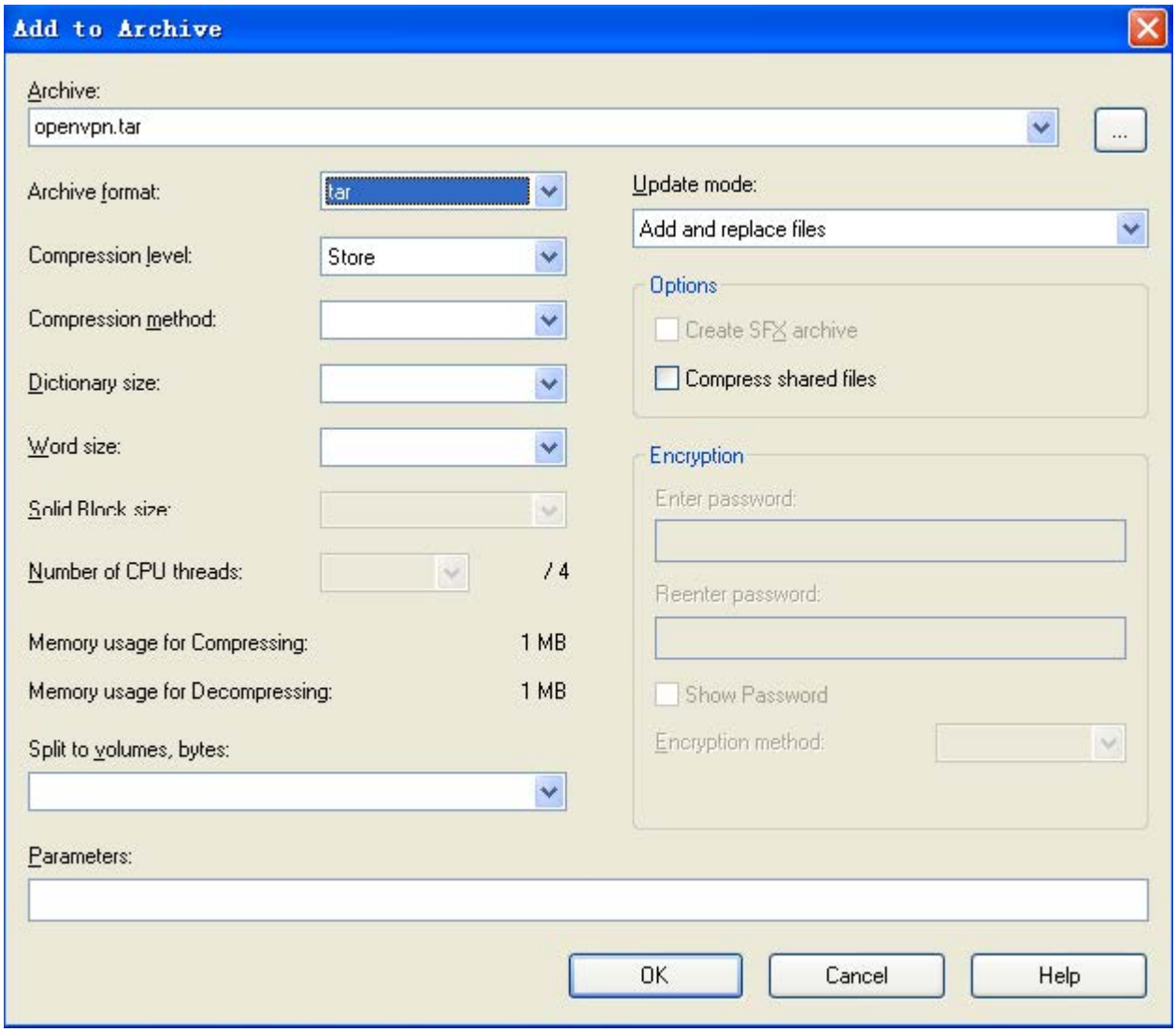
2. Start the 7-Zip file manager application.

3. Locate the OpenVPN folder on 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.

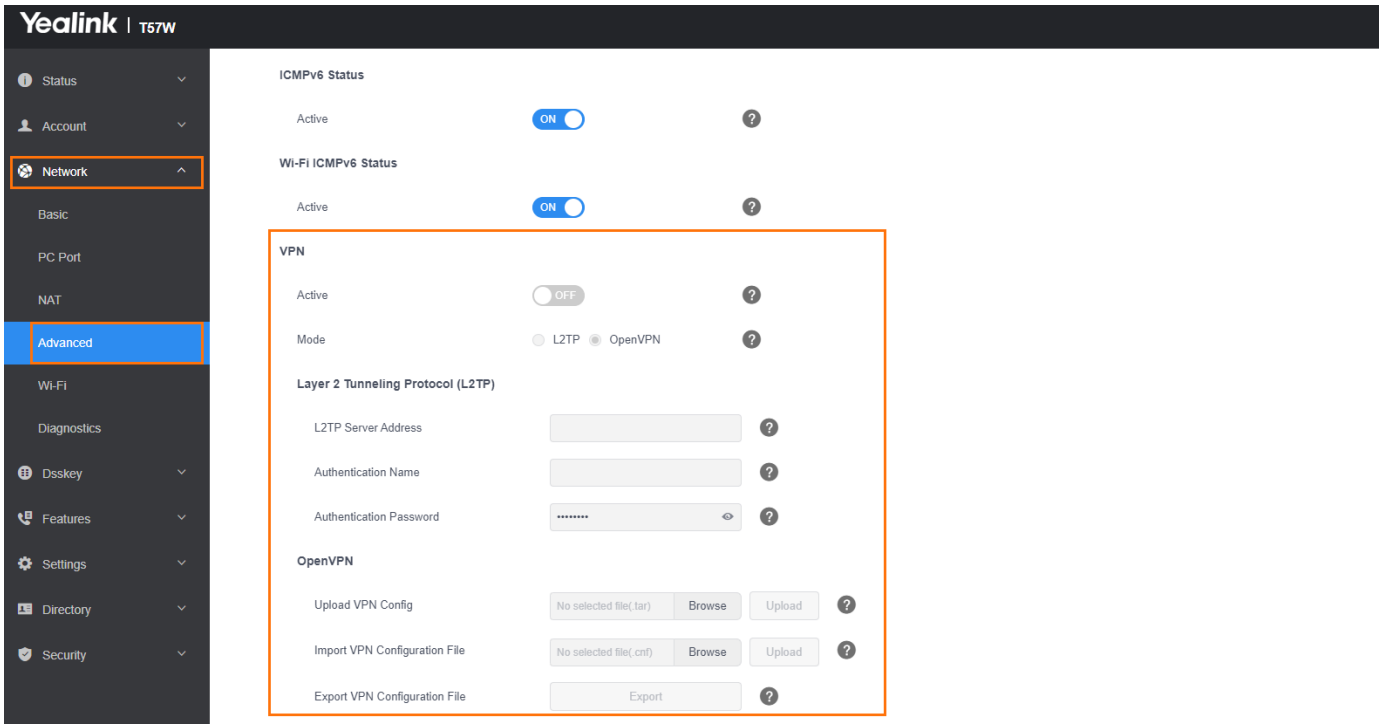
Configure OpenVPN Feature on IP Phones

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

The configurations described in this section apply to the IP phones running firmware version V85 or later.

Set via the Web User Interface

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



To enhance security, the OpenVPN Export feature has been removed in version x.86.0.129 and later for T3X/T4X/T5X devices.

Configuration parameter

static.network.vpn_enable
static.openvpn.url
static.network.openvpn_file.url
static.network.l2tp_server.address
static.network.l2tp_server.username
static.network.l2tp_server.password

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	Blan	It configures the URL for uploading the OpenVPN configuration file (vpn.cnf).

		k	It works only if "static.network.vpn.mode" is set to 1 (OpenVPN).
static.network.l2tp_server.address	String within 512 characters	Blank	It configures the L2TP server address. It works only if "static.network.vpn.mode" is set to 0 (L2TP).
static.network.l2tp_server.username	String within 512 characters	Blank	It configures the user name of the L2TP server. It works only if "static.network.vpn.mode" is set to 0 (L2TP).
static.network.l2tp_server.password	String within 512 characters	Blank	It configures the password of the L2TP server. It works only if "static.network.vpn.mode" is set to 0 (L2TP).

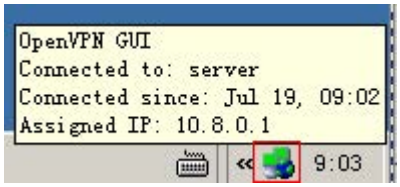
[1]If you change this parameter, the phone will reboot to make the change take effect.

Troubleshooting

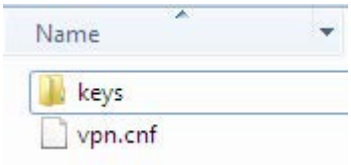
Why does the phone fail to connect to the OpenVPN server?

Do the following in sequence:

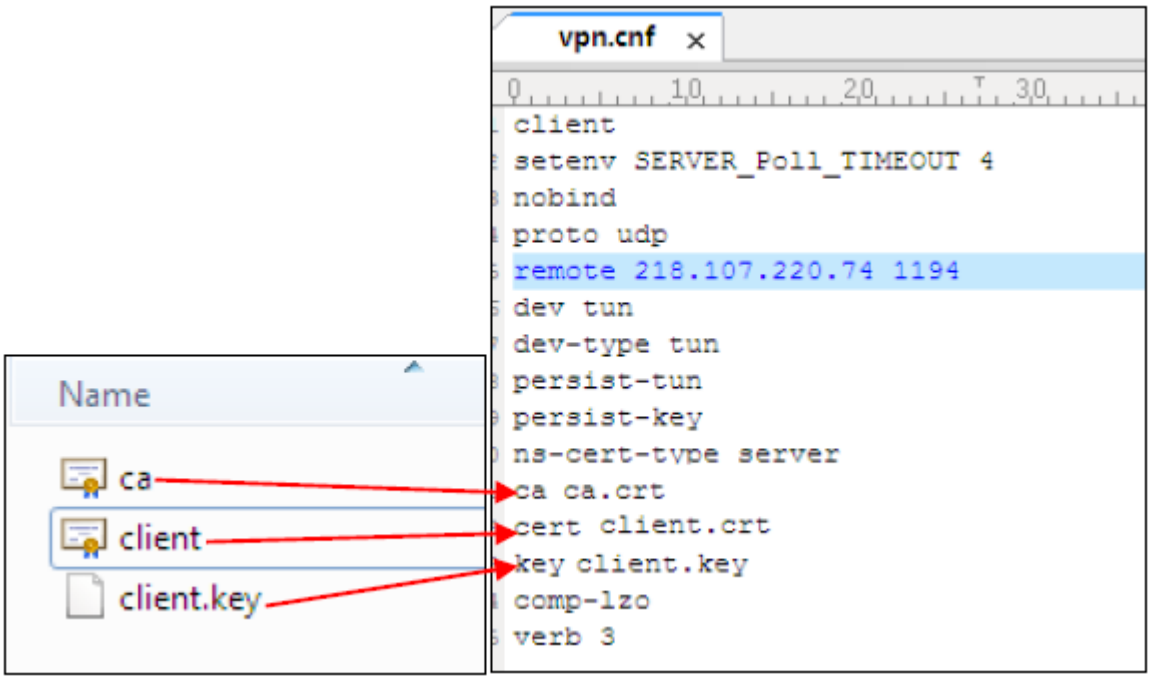
1. Ensure that the OpenVPN server is up and running.
   If the OpenVPN server is running properly, a virtual IP address assigned to the OpenVPN server will appear when you hover your mouse pointer over the VPN icon. The VPN icon in the notification area of the system tray is shown as below:



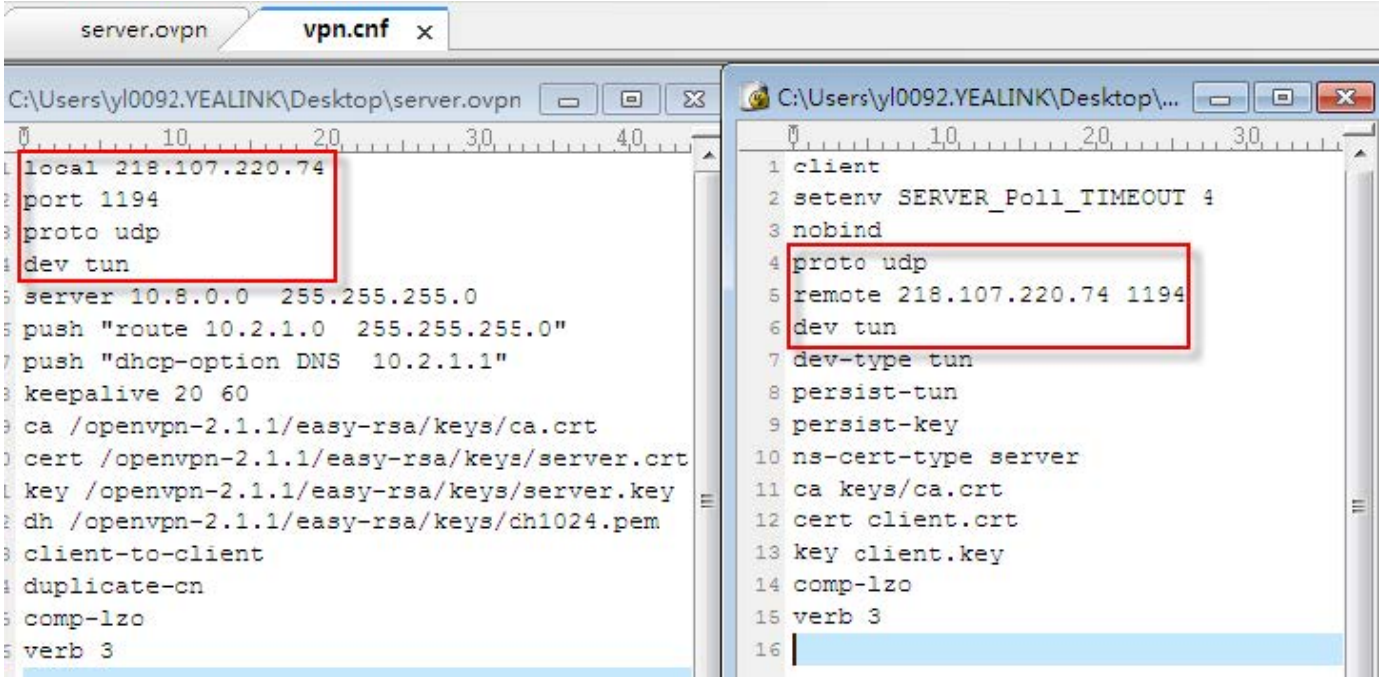
2. Ensure that the OpenVPN TAR file uploaded to the IP phone is correctly created.
3. Extract the TAR file and ensure that the certificate folder is named as “keys” and the client configuration file is named as “vpn.cnf”, as shown below:



3. Ensure that the file names of the client certificates and key defined in the client configuration file are correct.
4. Enter the "keys" directory to check the file names of client certificates and keys.

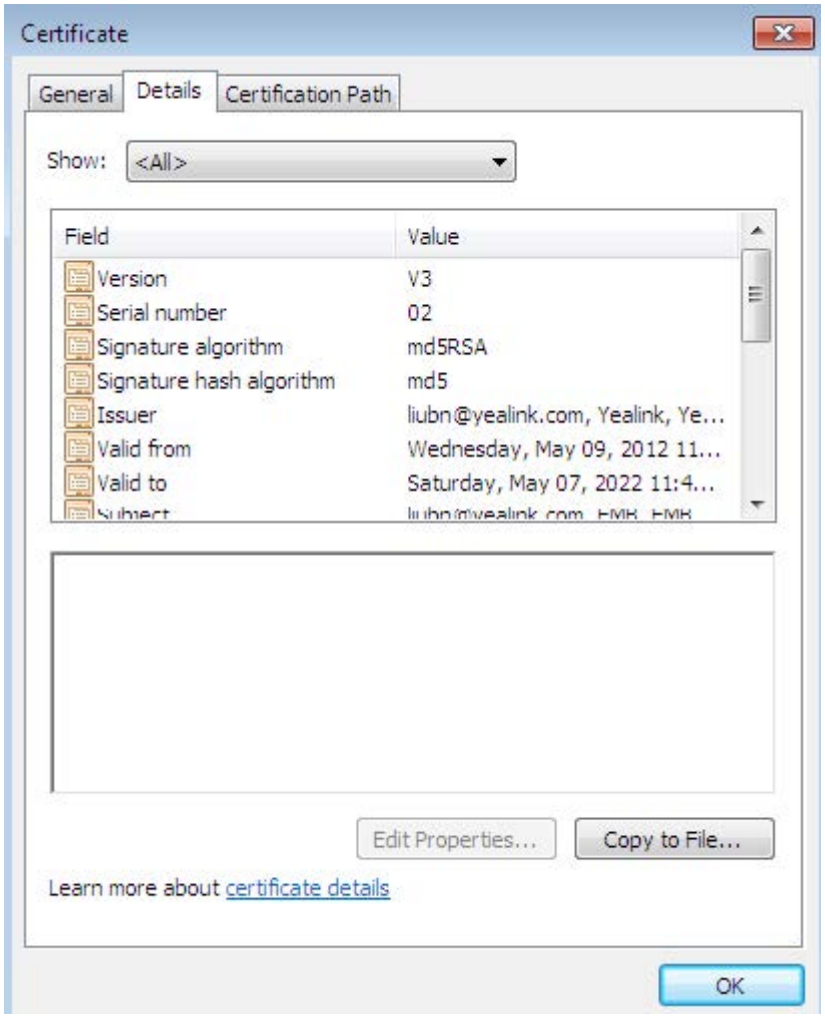


4. Ensure that the following configurations in the server configuration file and client configuration file are exactly matched.



5. Ensure that the time and date on the phone are within the validity time of the certificate.
6. Check if the signature algorithm of the client certificate is supported by the phone.

7. IP 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 IP phones, you need to change the signature algorithm and then re generate the client certificate.

Do the following:

1. Find the openssl.cnf file is 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. Regenerate a client certificate following the steps introduced in the section Installing the OpenVPN Server.

Why does the phone fail to register with 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 using 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 IP 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 is there no sound during a call?

Do the following:

1. Ensure that the client-to-client configuration 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 recommendsthat 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 delays.The DiffServ model can guarantee high-quality voice transmission when the voice packets are configured to a higher DSCP value.

SIP QoS

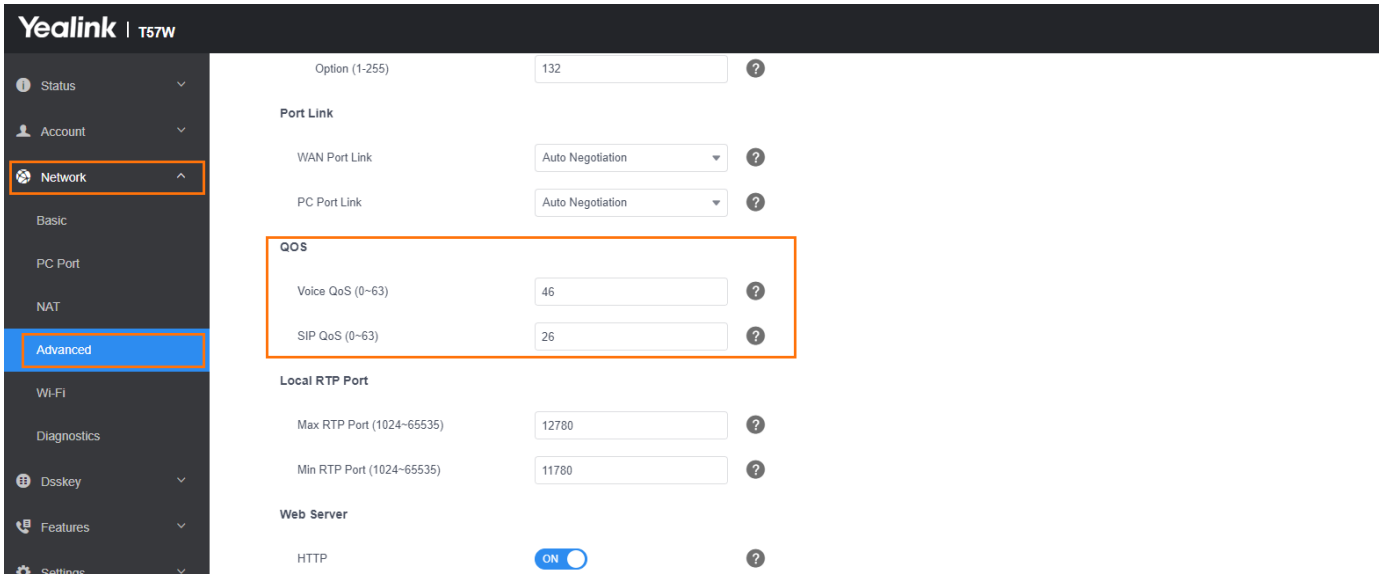
The SIP protocol is used for creating, modifying, and terminating two-party or multi-party sessions. To ensure good voice quality, SIP packets emanated from the phones should be configured with a high transmission priority. DSCPs for voice and SIP packets can be specified respectively.

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.

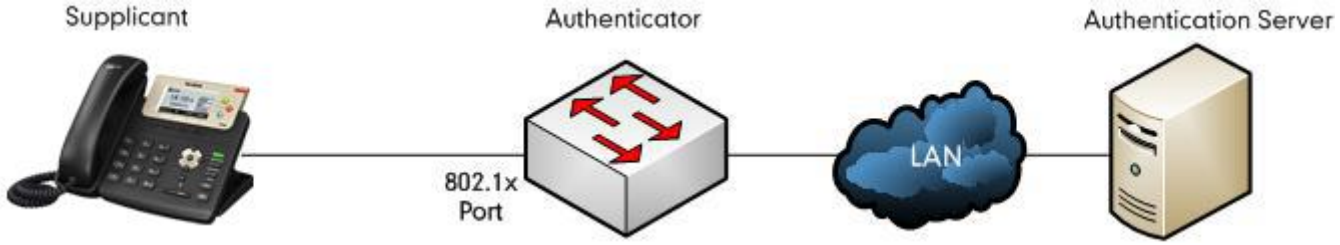
802.1x Authentication

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

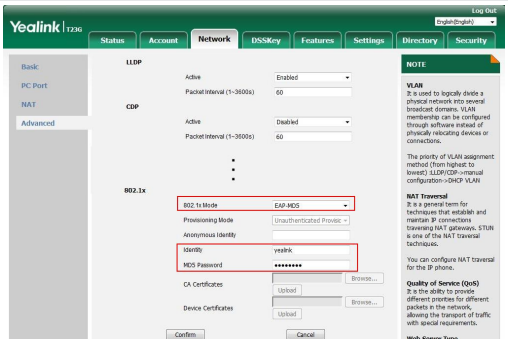
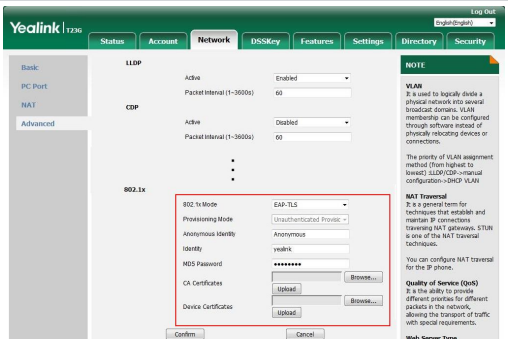
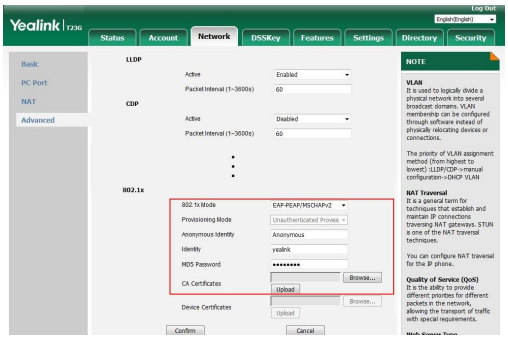
The configuration can be done either using the web or the Configuration parameter.

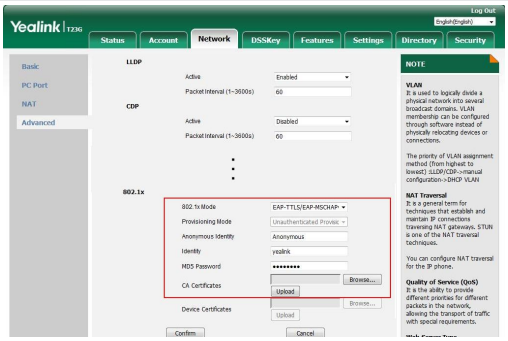
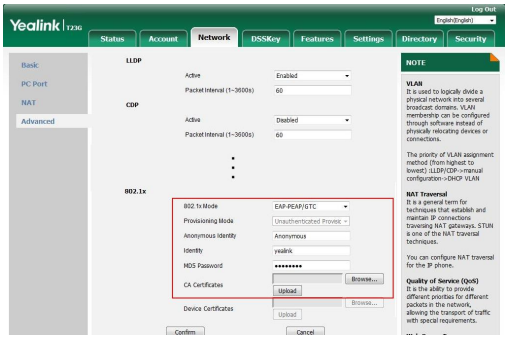
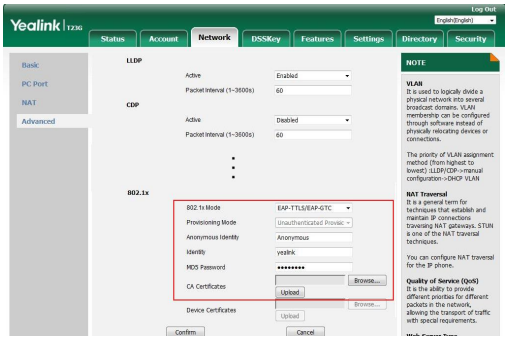
Set via the Web User Interface

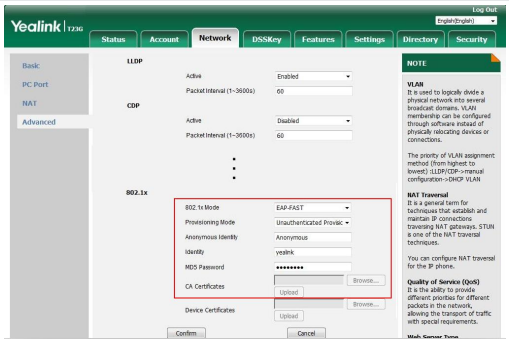
The following takes a SIP-T23G IP phone running firmware version 81 as an example.

1. Connect your phone to a network that is not 802.1X-enabled.
2. Sign in to the web user interface of the phone.
3. Go to **Network** -> **Advanced**.
4. In the **802.1x** block, select the desired protocol from the pull-down list of **802.1x Mode**.

Mode	Parameter	Screenshot
EAP-MD5	1) Enter the user name for authentication in the **Identity** field. 2) Enter the password for authentication	

	in the **MD5 Password** field.	
EAP-TLS	1) (Optional.) Enter the anonymous user name for authentication in the **Anonymous Identity** field. 2) Enter the user name for authentication in the **Identity** field. 3) Leave the **MD5 Password** field blank. 4) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (.pem, .crt, .cer or .der) from your local system. 5) In the **Device Certificates** field, click **Browse** to select the desired client (*.pem or *.cer) certificate from your local system. 6) Click **Upload** to upload the certificates.	
EAP-PEAP/ MSCHAPv2	1) (Optional.) Enter the anonymous user name for authentication in the **Anonymous Identity** field. 2) Enter the user name for authentication in the **Identity** field. 3) Enter the password for authentication in the **MD5 Password** field. 4) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (*.pem, *.crt, *.cer or *.der) from your local system. 5) Click **Upload** to upload the certificates.	
EAP-TTLS/ EAP-	1) (Optional.) Enter the anonymous user name for authentication in the	

MSCHAPv2	**Anonymous Identity** field. 2) Enter the user name for authentication in the **Identity** field. 3) Enter the password for authentication in the **MD5 Password** field. 4) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (*.pem, *.crt, *.cer or *.der) from your local system. 5) Click **Upload** to upload the certificates.	
EAP-PEAP/ GTC	1) (Optional.) Enter the anonymous user name for authentication in the **Anonymous Identity** field. 2) Enter the user name for authentication in the **Identity** field. 3) Enter the password for authentication in the **MD5 Password** field. 4) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (*.pem, *.crt, *.cer or *.der) from your local system. 5) Click **Upload** to upload the certificates.	
EAP-TTLS/ EAP-GTC	1) (Optional.) Enter the anonymous user name for authentication in the **Anonymous Identity** field. 2) Enter the user name for authentication in the **Identity** field. 3) Enter the password for authentication in the **MD5 Password** field. 4) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (*.pem, *.crt, *.cer or *.der) from your local system. 5) Click **Upload** to upload the certificates.	

EAP-FAST	1) Select the desired value from the pull-down list of **Provisioning Mode**. 2) (Optional.) Enter the anonymous user name for authentication in the **Anonymous Identity** field. 3) Enter the user name for authentication in the **Identity** field. 4) Enter the password for authentication in the **MD5 Password** field. 5) (Optional.) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (*.pem, *.crt, *.cer or *.der) from your local system. The CA certificate needs to be uploaded only when **Authenticated Provisioning** mode is selected from the **Provisioning Mode** field. 6) Click **Upload** to upload the certificate.	

5. Click **Confirm** to accept the change.
6. A dialog box pops up to prompt that settings will take effect after a reboot.
6. Click **OK** to reboot the phone.
7. Connect the phone to the 802.1X-enabled network after reboot.

Configuration parameter

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

Parameter	Permitted Values	Def aul	Description

		t	
static.network.802_1x.mode[1]	**0**-EAP-None, no authentication **1**-EAP-MD5 **2**-EAP-TLS **3**-EAP-PEAP/MSCHAPv2 **4**-EAP-TTLS/EAP-MSCHAPv2 **5**-EAP-PEAP/GTC **6**-EAP-TTLS/EAP-GTC **7**-EAP-FAST	0	It configures the 802.1x authentication method.
static.network.802_1x.eap_fast_provision_mode[1]	**0**-Unauthenticated Provisioning, EAP In-Band provisioning is enabled by server unauthenticated PAC (Protected Access Credential) provisioning using the anonymous Diffie-Hellman key exchange. **1**-Authenticated Provisioning, EAP In-Band provisioning is enabled by server authenticated PAC provisioning using certificate-based server authentication.	0	It configures the EAP In-Band provisioning method for EAP-FAST. It works only if "static.network.802_1x.mode" is set to 7 (EAP-FAST).
static.network.802_1x.anonymous_identity[1]	String within 512 characters	Blank	It configures the anonymous identity (user name) for 802.1X authentication. It is used for constructing a secure tunnel for 802.1X authentication. It works only if

			"static.network.802_1x.mode" is set to 2, 3, 4, 5, 6, or 7.
static.network.802_1x.identity[1]	String within 32 characters	Blank	It configures the identity (user name) for 802.1x authentication.
static.network.802_1x.md5_password[1]	String within 32 characters	Blank	It configures the password for 802.1x authentication. It is required for all methods except EAP-TLS.
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. 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. 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

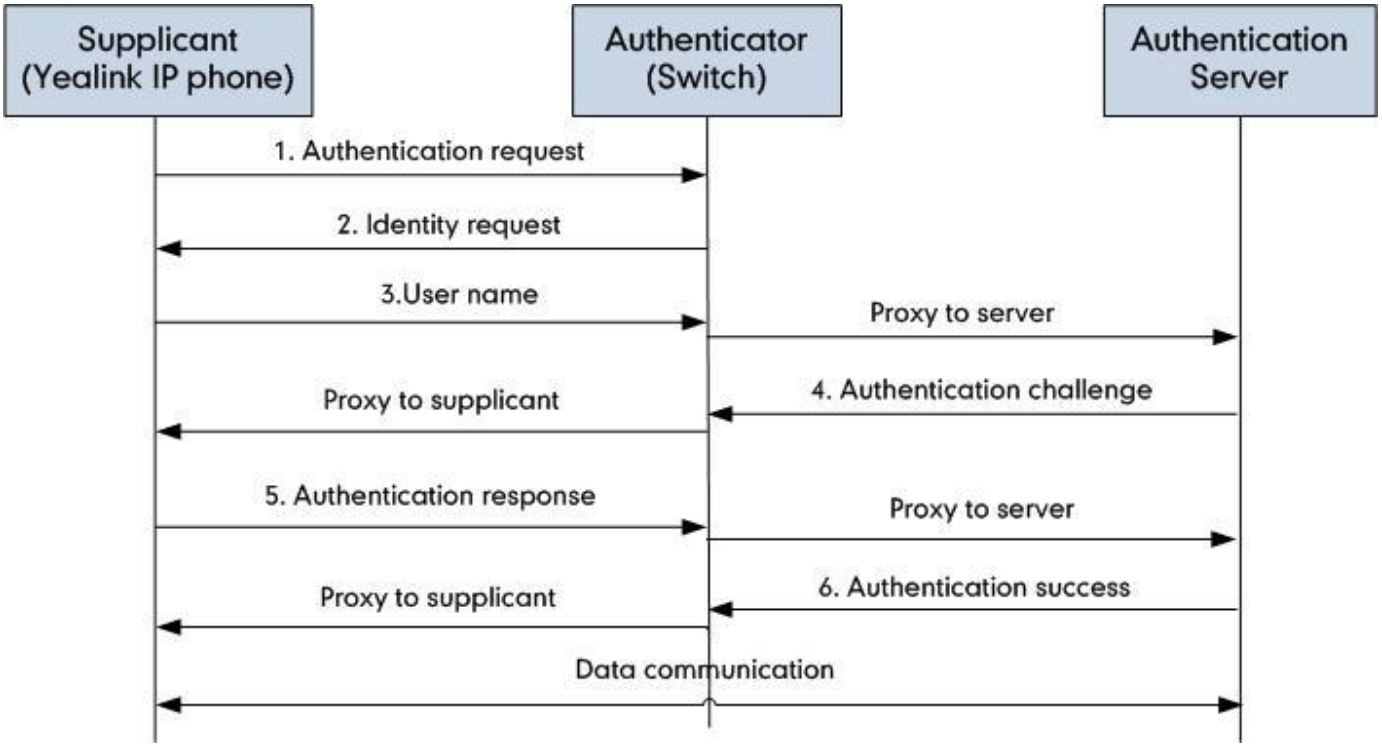
Reboot the phone to activate the 802.1X authentication on the phone. The 802.1X authentication process is divided into two basic stages:

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

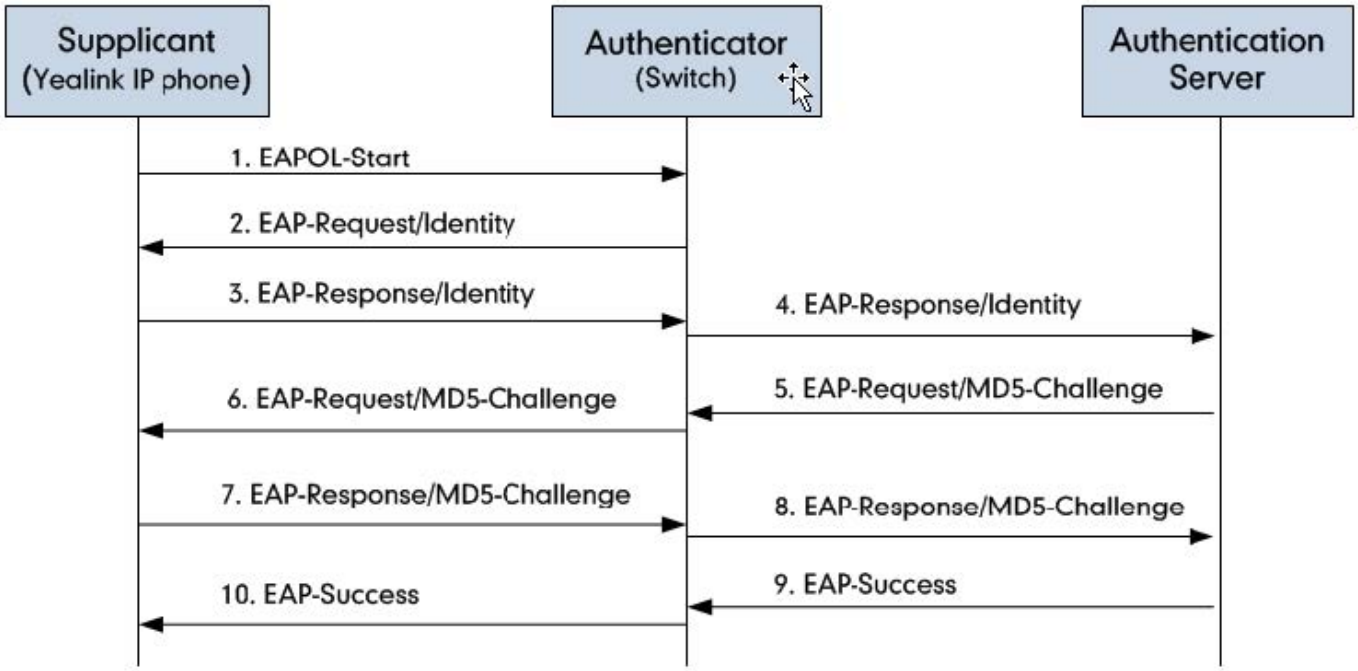
After the authentication server authenticates the IP phone, the authentication server initiates the authentication stage of the process. During this phase, the authenticator facilitates an exchange of keys between the IP phone and the authentication server. After these keys are established, the authenticator 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

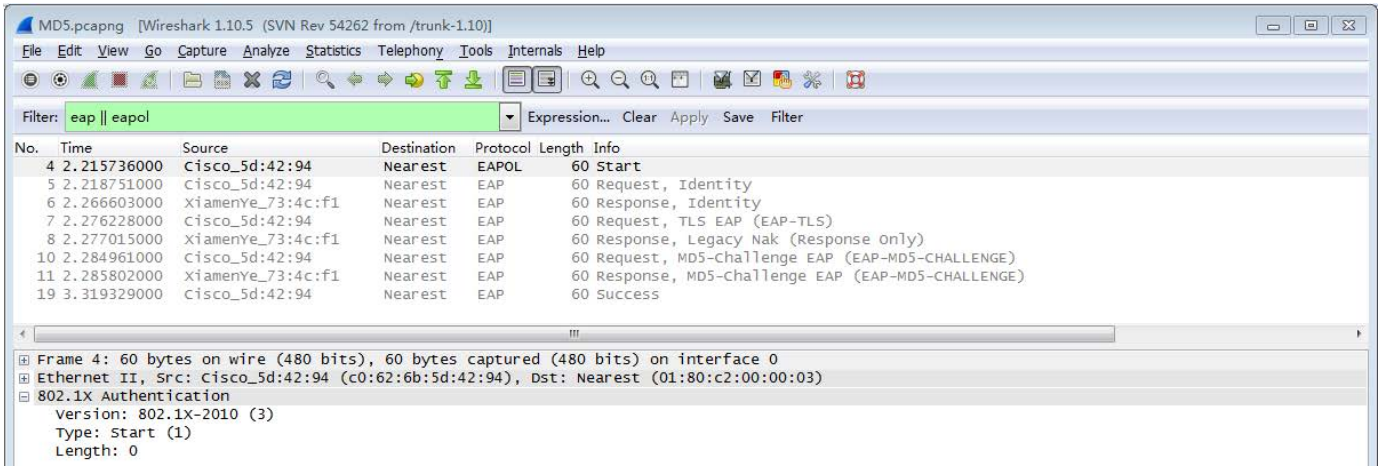
Authentication Process

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 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.

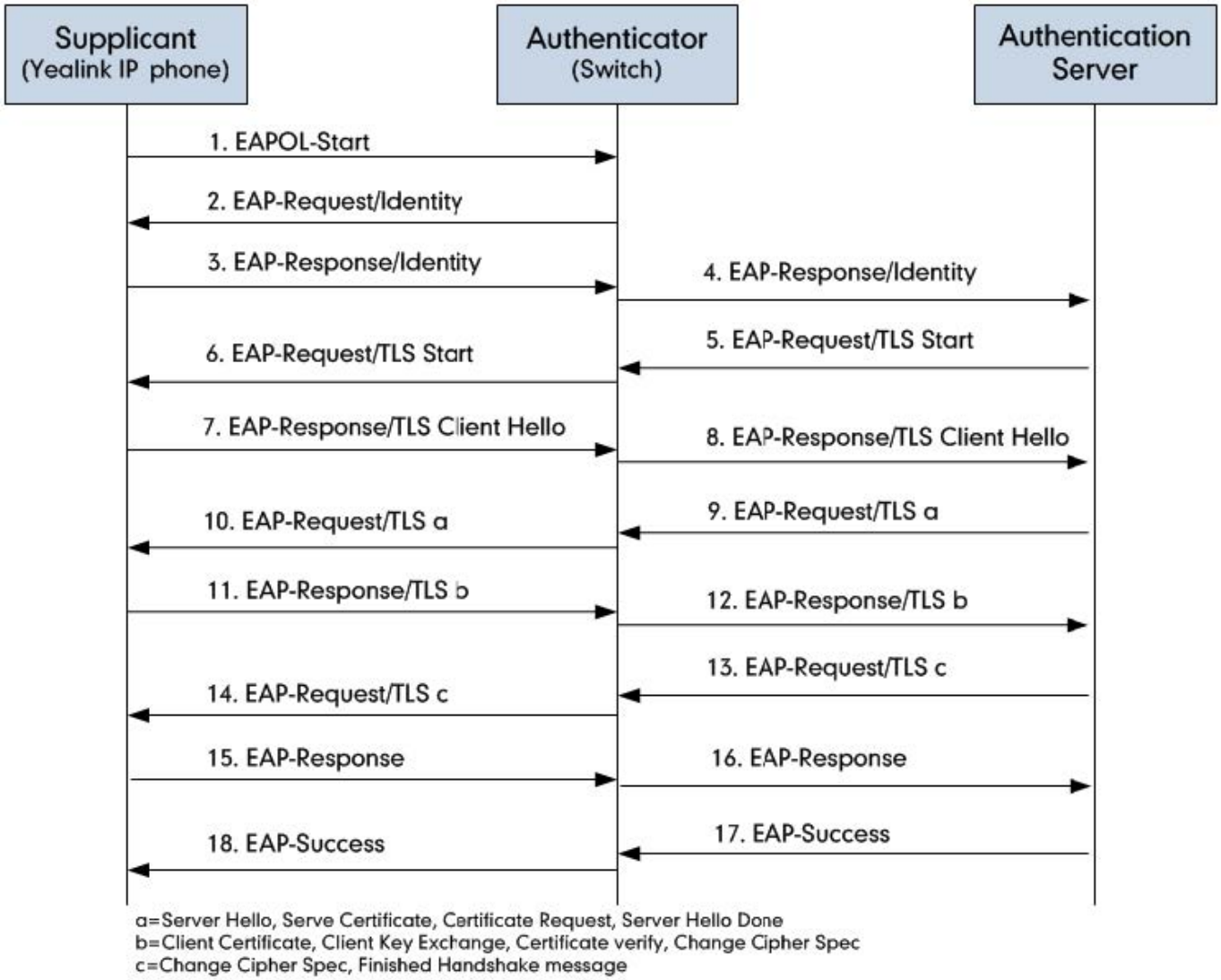
Sample Screenshot



Authentication Process Using EAP-TLS Protocol

Authentication Process

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

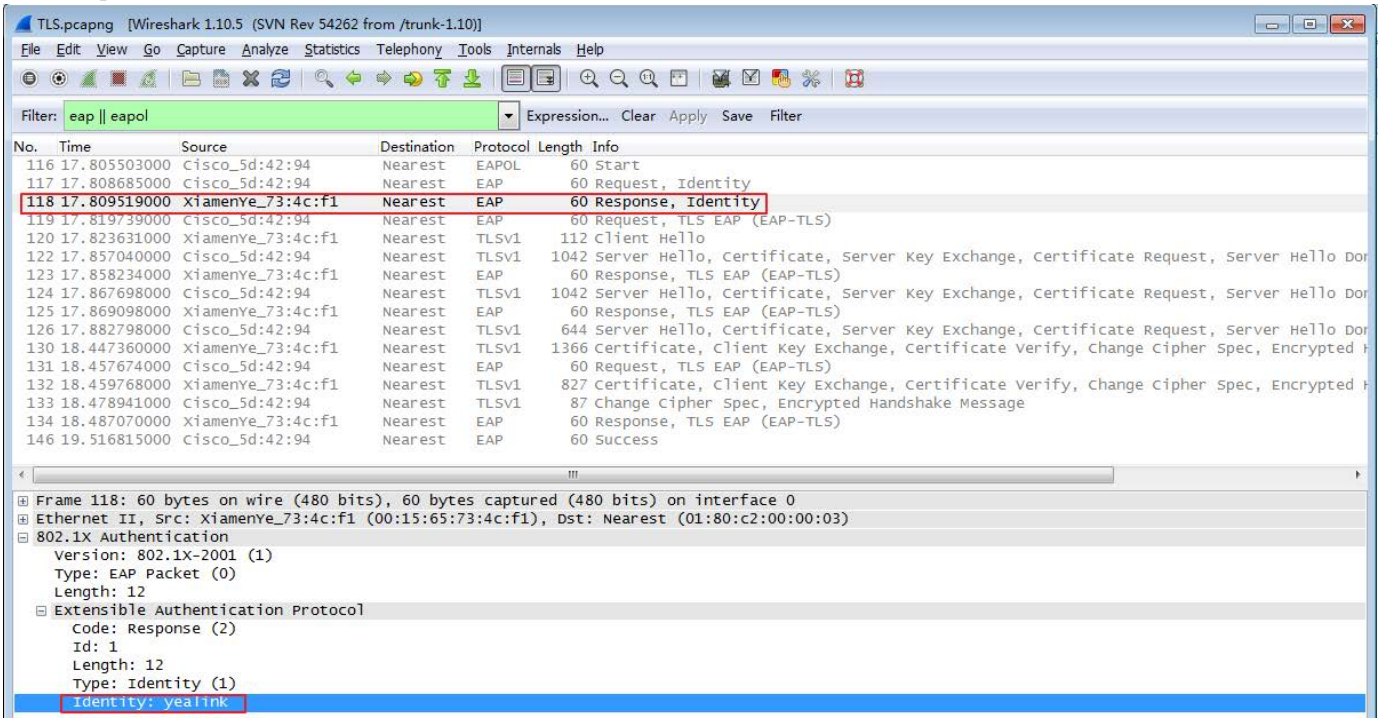


1. The supplicant sends an “EAPOL-Start” packet to the authenticator.

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 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-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 that 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.

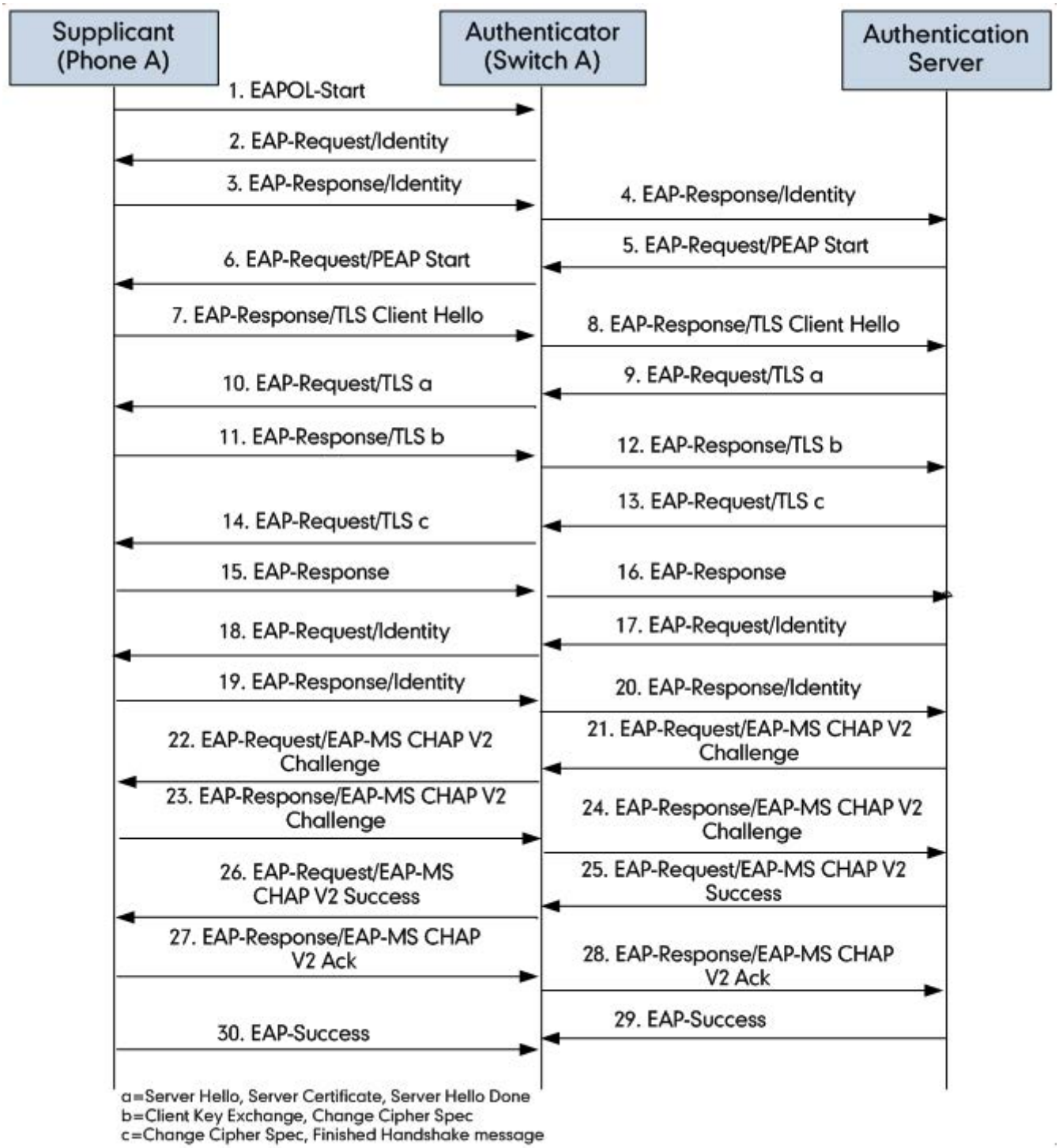
Sample Screenshot



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.



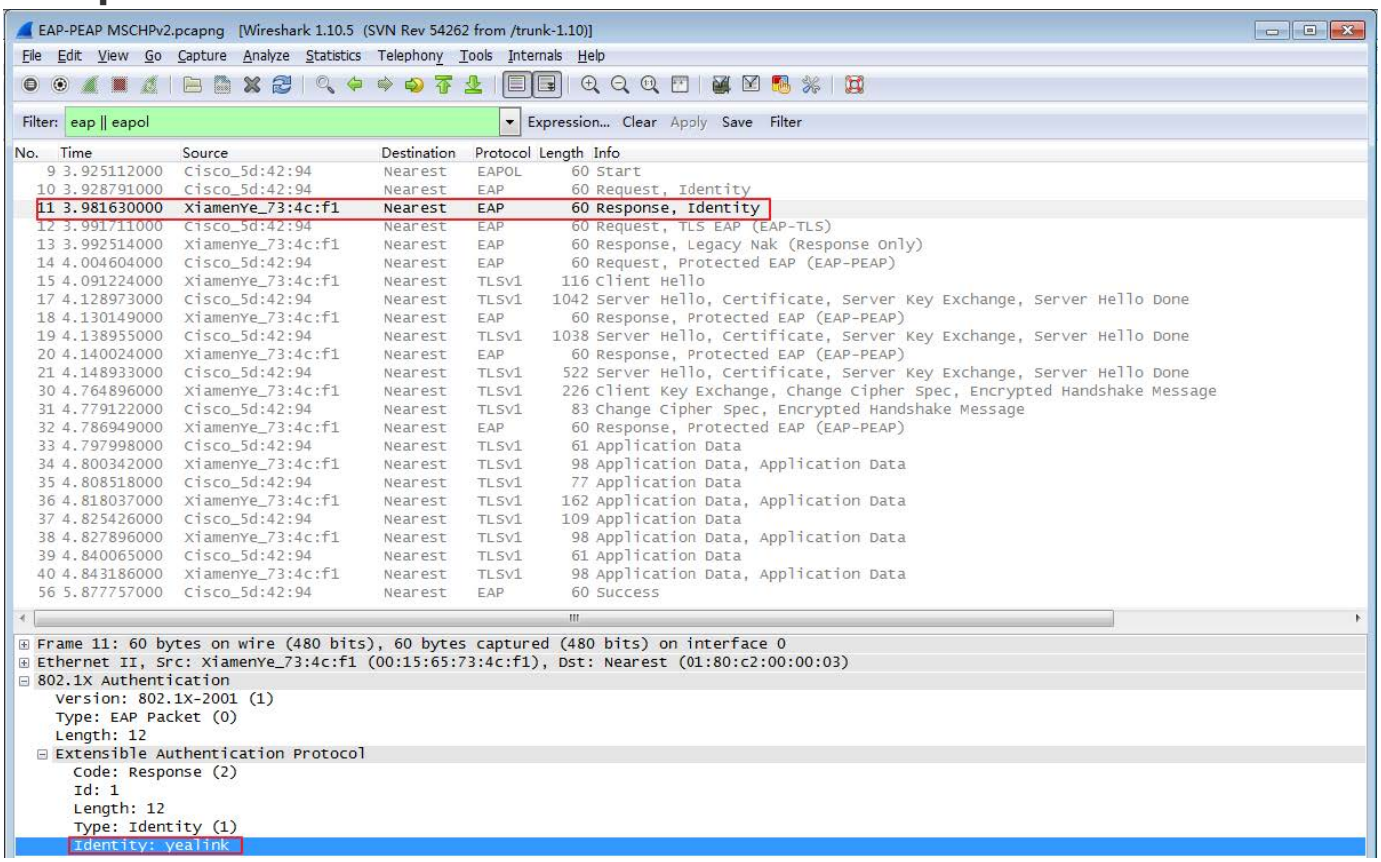
1. The supplicant sends an “EAPOL-Start” packet to the authenticator.
2. The authenticator responds with an “EAP-Request/Identity” packet to the supplicant.
3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
4. The authenticator strips the Ethernet header and encapsulates 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 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, 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 to a challenge message from 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 a 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.
31. 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



Yealink IP Phones Compatible with 802.1X

802.1X is the most widely accepted form of port-based network access control in use and is available on Yealink IP phones. Yealink IP phones support 802.1X authentication based on EAP-MD5, EAP-TLS, EAP-PEAP/MSCHAPv2, EAP-TTLS/EAP-MSCHAPv2, EAP-PEAP/GTC, EAP-TTLS/EAP-GTC, and EAP-FAST protocols.

The table below lists the protocols supported by Yealink SIP IP phones with different versions.

Authentication Protocol	IP Phone Models	Firmware Version
EAP-MD5	All IP phones	All Versions
EAP-TLS	T46G, T42G, T41P, CP860	Firmware version 71

		or later
	T48G	Firmware version 72 or later
	T58A, T49G, T40P, T29G, T23P/G, T21(P) E2, T19(P) E2, CP960, and W56P	Firmware version 80 or later
	T48S, T46S, T42S, T41S, T40G, T27G, W52P	Firmware version 81 or later
	VP59, W53P, and CP930W-Base	Firmware version 83 or later
	T57W, T54W, T53W, T53, T48U, T46U, T43U and T42U	Firmware version 84 or later
	T53C, T33P, T33G, T31P, T31G, T31, T30P and T30	Firmware version 85 or later
	CP965, CP925, T58W	Firmware version 86 or later
	T7X/T8X	Firmware version 87 or later
EAP-TTLS/EAP-MSCHAPv2	T46G, T42G, T41P, CP860	Firmware version 71 or later
	T48G	Firmware version 72 or later
	T58A, T49G, T40P, T29G, T23P/G, T21(P) E2, T19(P) E2, CP960, and W56P	Firmware version 80 or later
	T48S, T46S, T42S, T41S, T40G, T27G, W52P	Firmware version 81 or later
	VP59, W53P, and CP930W-Base	Firmware version 83 or later
	T57W, T54W, T53W, T53, T48U, T46U, T43U and T42U	Firmware version 84 or later
	T53C, T33P, T33G, T31P, T31G, T31, T30P and T30	Firmware version 85 or later
	CP965, CP925, T58W	Firmware version 86 or later

	T7X/T8X	Firmware version 87 or later
EAP-PEAP/GTC	T48G, T46G, T42G, T41P, CP860	Firmware version 73 or later
	T58A, T49G, T40P, T29G, T23P/G, T21(P) E2, T19(P) E2, CP960, and W56P	Firmware version 80 or later
	T48S, T46S, T42S, T41S, T40G, T27G, W52P	Firmware version 81 or later
	VP59, W53P, and CP930W-Base	Firmware version 83 or later
	T57W, T54W, T53W, T53, T48U, T46U, T43U and T42U	Firmware version 84 or later
	T53C, T33P, T33G, T31P, T31G, T31, T30P and T30	Firmware version 85 or later
	CP965, CP925, T58W	Firmware version 86 or later
	T7X/T8X	Firmware version 87 or later
EAP-TTLS/EAP-GTC	T48G, T46G, T42G, T41P, CP860	Firmware version 73 or later
	T58A, T49G, T40P, T29G, T23P/G, T21(P) E2, T19(P) E2, CP960, and W56P	Firmware version 80 or later
	T48S, T46S, T42S, T41S, T40G, T27G, W52P	Firmware version 81 or later
	VP59, W53P, and CP930W-Base	Firmware version 83 or later
	T57W, T54W, T53W, T53, T48U, T46U, T43U and T42U	Firmware version 84 or later
	T53C, T33P, T33G, T31P, T31G, T31, T30P and T30	Firmware version 85 or later
	CP965, CP925, T58W	Firmware version 86 or later
	T7X/T8X	Firmware version 87

		or later
EAP-FAST	T48G, T46G, T42G, T41P, CP860, T58A, T49G, T40P, T29G, T23P/G, T21(P) E2, T19(P) E2, CP960, and W56P	Firmware version 80 or later
	T48S, T46S, T42S, T41S, T40G, T27G, W52P	Firmware version 81 or later
	VP59, W53P, and CP930W-Base	Firmware version 83 or later
	T57W, T54W, T53W, T53, T48U, T46U, T43U and T42U	Firmware version 84 or later
	T53C, T33P, T33G, T31P, T31G, T31, T30P and T30	Firmware version 85 or later
	CP965, CP925, T58W	Firmware version 86 or later
	T7X/T8X	Firmware version 87 or later

Yealink IP phones support 802.1X as a supplicant, both Pass-thru Mode and Pass-thru Mode with Proxy Logoff. When the device is connected to the phone and disconnects from the PC port, the Yealink IP phone can provide additional security by sending an EAPOL Logoff message to the Ethernet switch. This functionality, also known as proxy logoff, prevents another device from using the port without first authenticating via 802.1X.

Troubleshooting

Why doesn’t the IP 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 the authentication server.
2. Ensure that the user name 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.

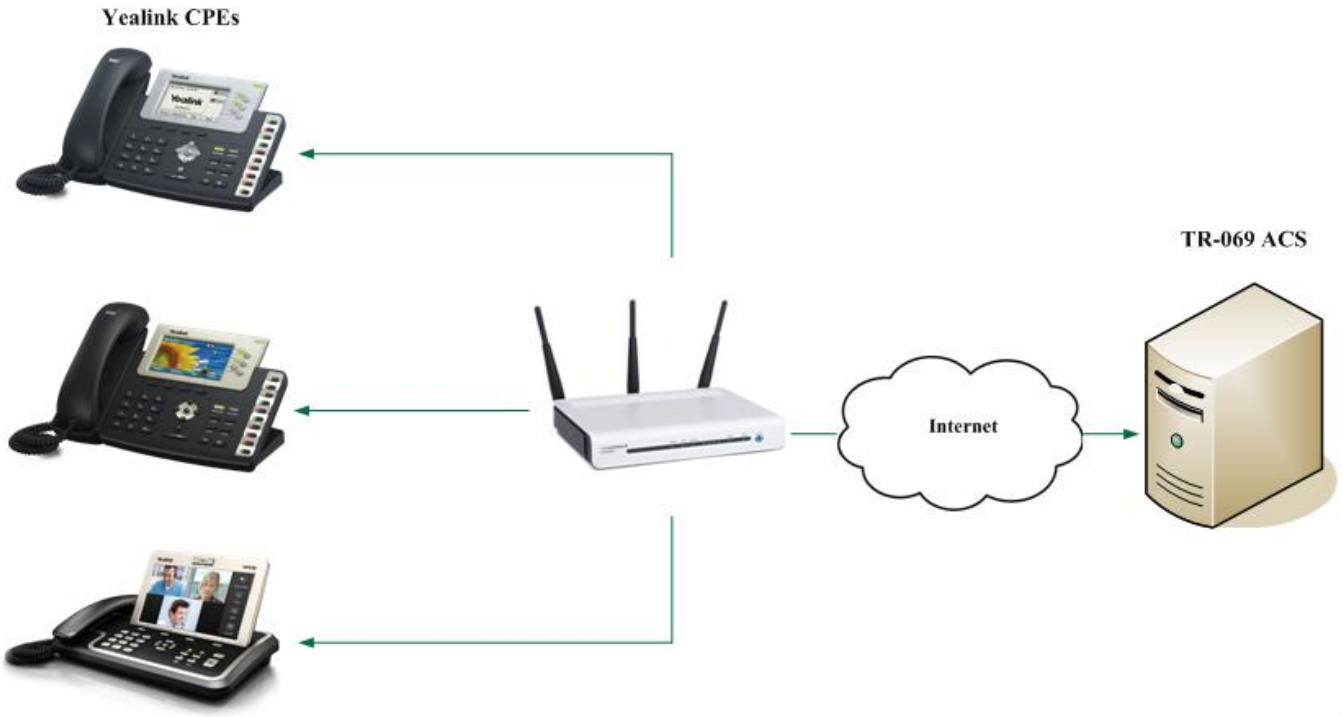
- b) Check if the time and date on the phone are within the validity time of the uploaded certificate. If not, re-generate a certificate and upload it to the phone.

3. Ensure that the failure is not caused by network settings.
   - a) Disable the LLDP feature and manually configure a VLAN ID for the Internet port of the phone to check if the authentication is successful. If the phone is authenticated successfully, contact your network administrator to troubleshoot the LLDP-related problem.
   - b) Disable the 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 that 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 the 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 that has broad applicability and no access restriction. TR-069 standard allows the subscriber to manage all devices on a common platform regardless of their 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 a 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 download.

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 allow the phone to actively notify the ACS of changes to its state.

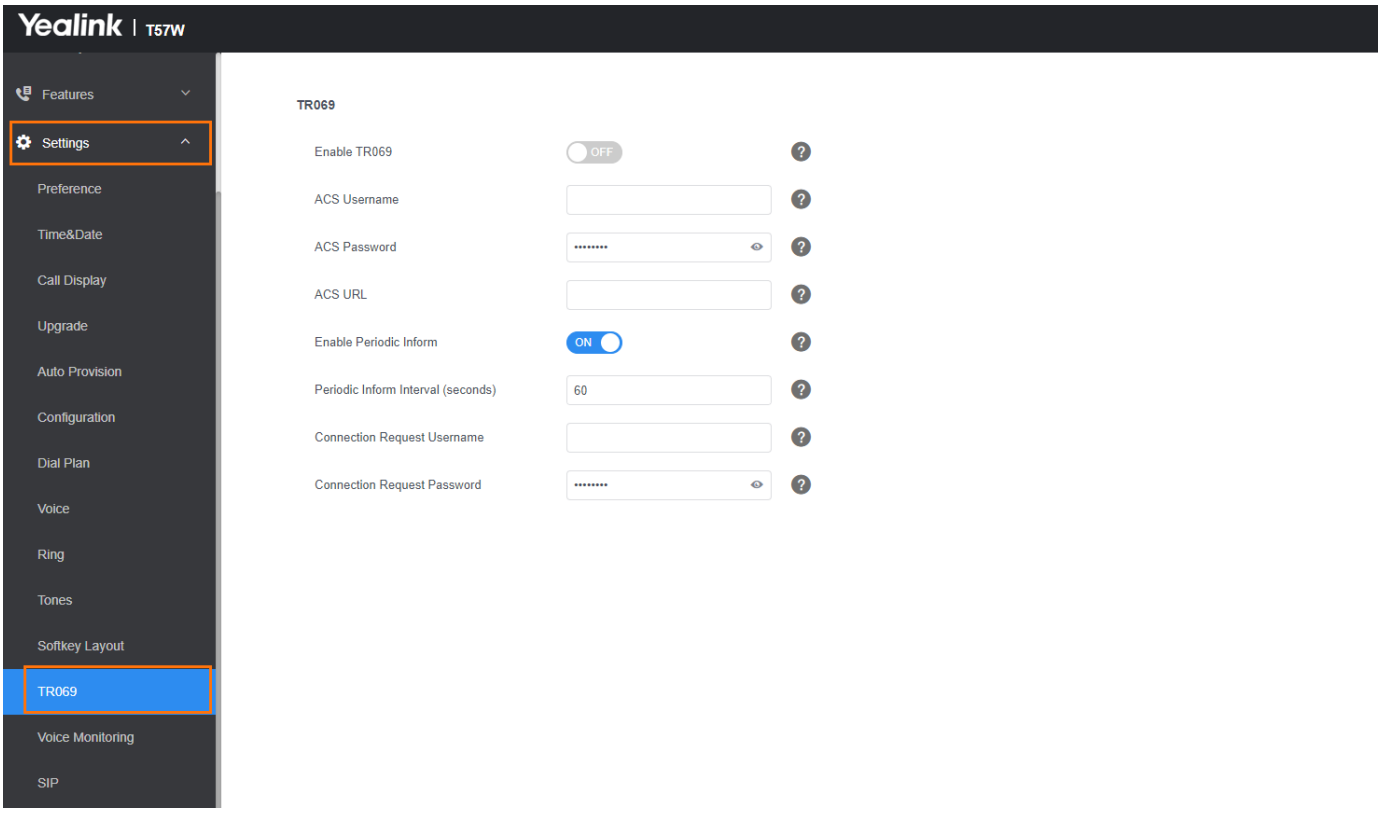
Diagnostics

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 Configuration

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 **60**.
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.

			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 that 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 ACSs. For more information about the supported ACS, contact Yealink technical support.

Data Model

Most of the configuration and diagnostics are performed by 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

Wi-Fi

Wi-Fi

Wi-Fi feature enables you to connect the phones to the organization’s wireless network. Wi-Fi feature is only applicable to T31W/T34W/T57W/T54W/T53W/T53/T53C/T48U/T48S/T48G/T46U/T46S/T46G/T43U/T42U/T42S/T41S/T29G/T27G/CP920/CP925/CP935W/T58W/T58A/VP59/T56A/T58V/CP960/CP965/T7X/T8X phones.

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.

To use the Wi-Fi feature on T53/T53C/T44U/T48U/T48S/T48G/T46U/T46S/T46G/T43U/T42U/T42S/T41S/T29G/T27G/T73U/T74U/T77U phones, make sure the Wi-Fi USB dongle is properly connected to the USB port on the back of the phone.

Wi-Fi Configuration

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

Configuration parameter

static.wifi.function.enable
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 a wireless network preferentially. 2-Use a wired network preferentially.	2
static.network.redundancy.failback.timeout	It configures the time to wait (minutes) for the phone to switch to the preferentially used network. 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 preferred 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. It works only if	0-Disabled 1-Enabled	0

	"static.wifi.function.enable" is set to 1 (Enabled).		
static.wifi.X.ssid[2]	It configures the SSID of a specific wireless network. SSID is a unique identifier for accessing wireless access points. 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. 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. 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. 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. 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. 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. 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. 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 a 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	1

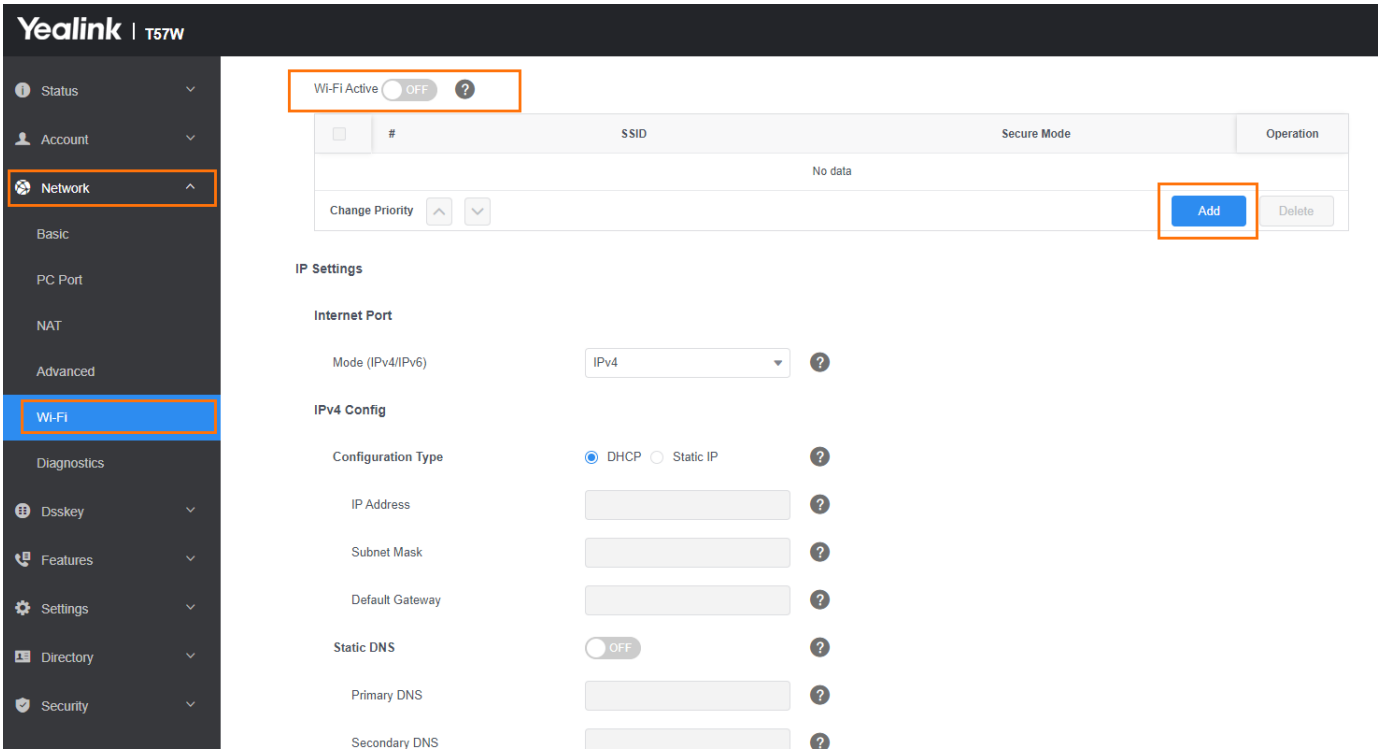
		(according to the priority) automatically. But if the phone fails to connect to any known wireless network, the phone will still display the Wi-Fi scanning prompt when connecting to the phone. 1-Enabled	

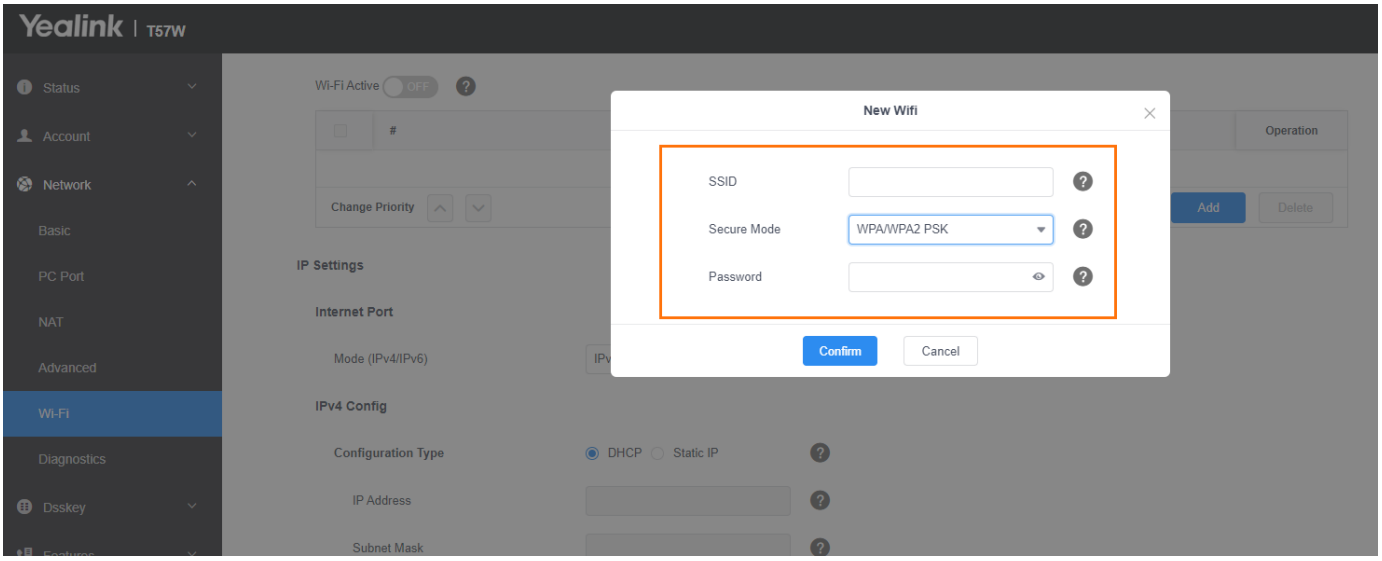
[1]If you change this parameter, the phone will reboot to make the change take effect.

[2]X is the 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.

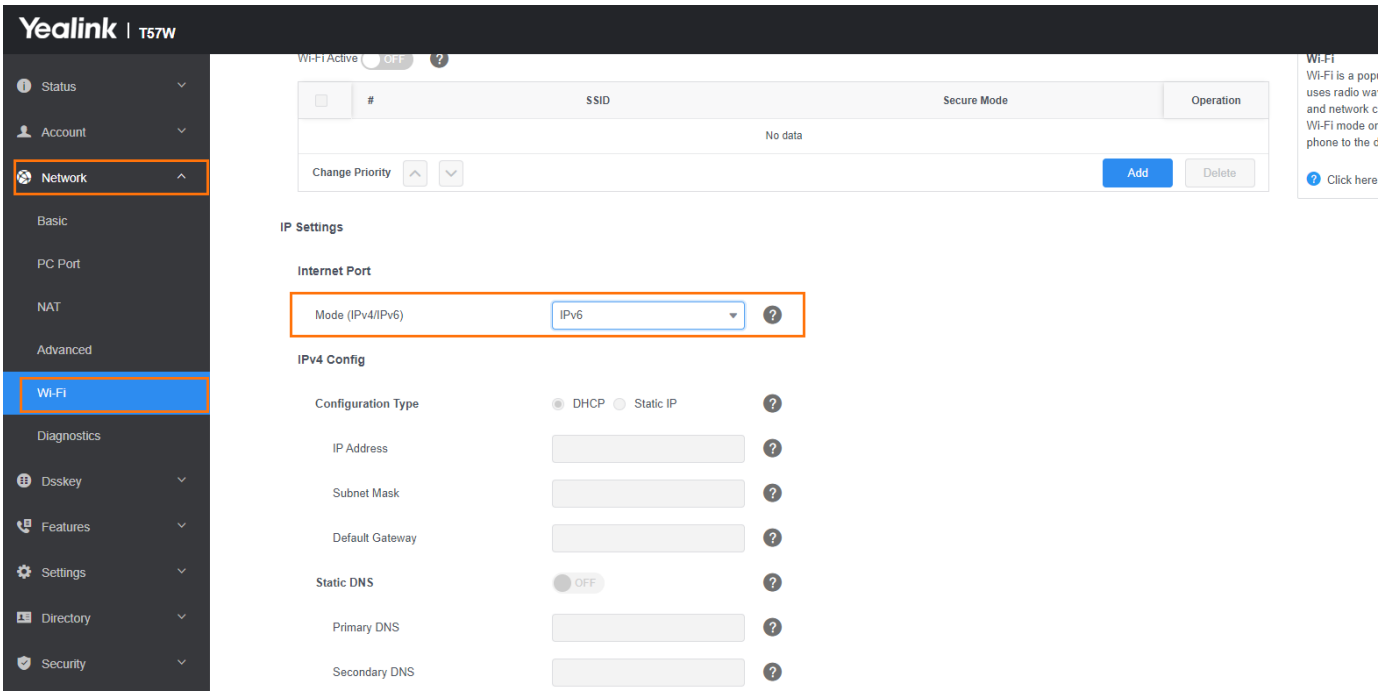
Configuration parameter

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. 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

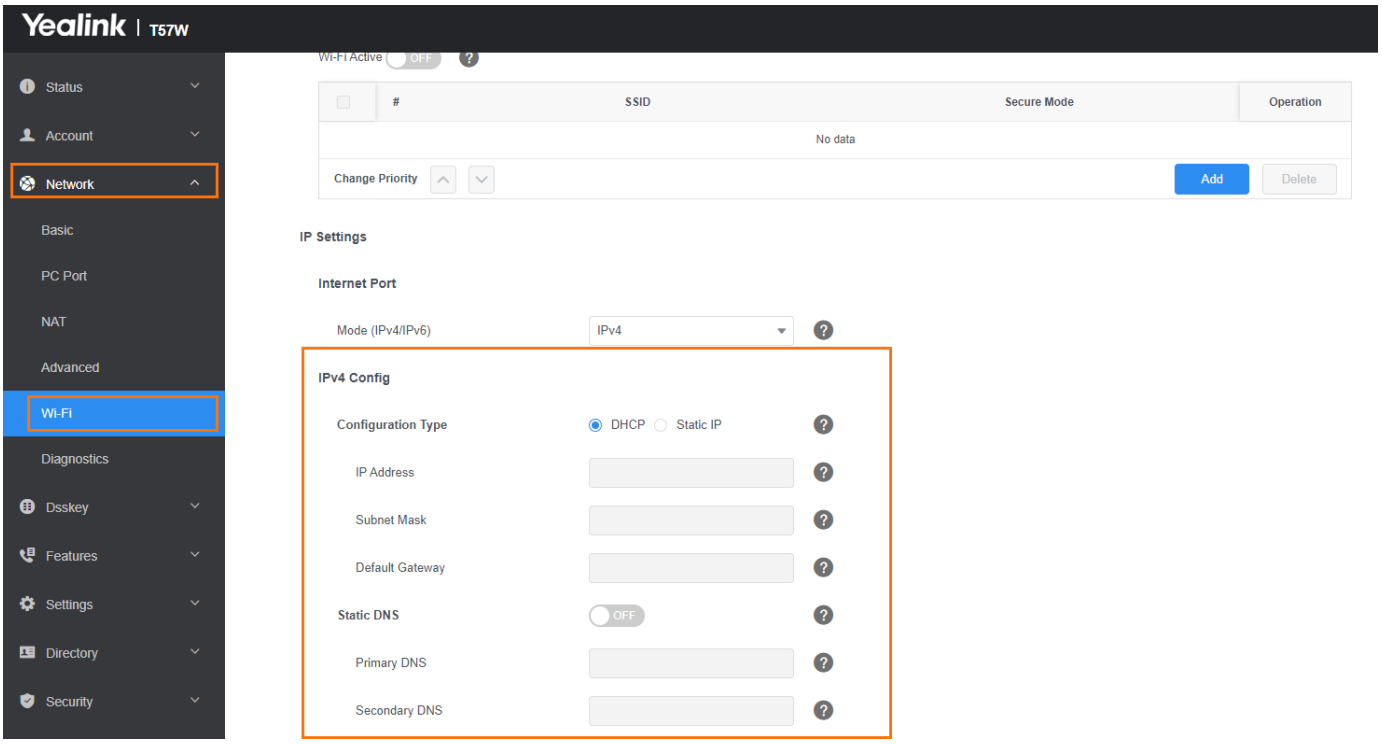
Parameter	Description	Permitted Values	Default
static.network.wifi.internet_port.type	It configures the Internet port type for IPv4 wireless network. It works only if "static.network.wifi.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6).	0-DHCP 2-Static IP	0
static.network.wif	It configures the IPv4 address for the wireless network.	IPv4 Address	Bla

i.internet_port.ip	It works only if "static.network.wifi.internet_port.type" is set to 2 (Static IP).		nk
static.network.wifi.internet_port.mask	It configures the IPv4 subnet mask for the wireless network. 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. 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 turn on or off for the wireless network. 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 a manually configured static IPv4 DNS.	0
static.network.wifi.primary_dns	It configures the primary IPv4 DNS server for the wireless network. 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_dn	It configures the secondary IPv4 DNS server for the wireless network.	IPv4 Address	Blank

s	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).		

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 an IPv6 wireless network.

Configuration parameter

static.network.wifi.ipv6_internet_port.type static.network.wifi.ipv6_internet_port.ip static.network.wifi.ipv6_prefix

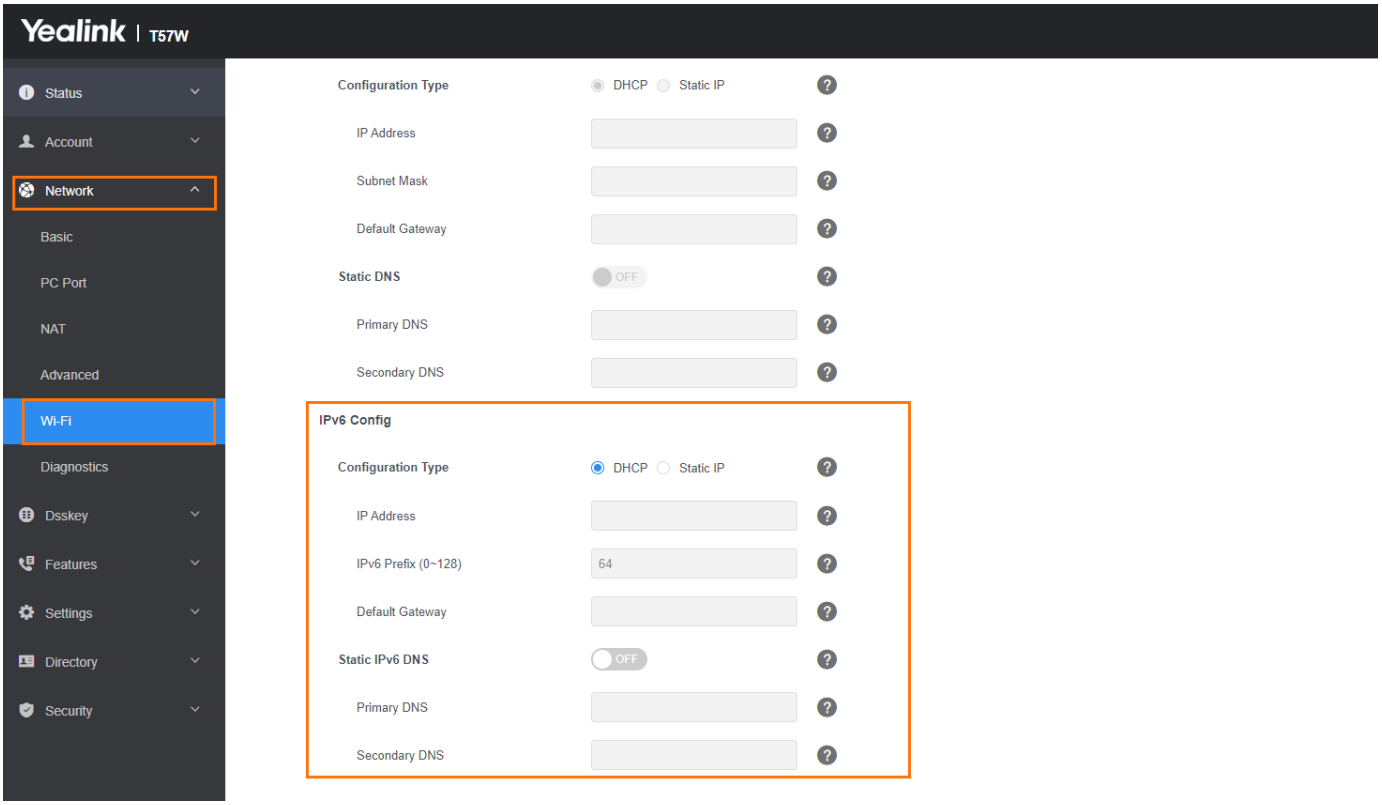
static.network.wifi.ipv6_internet_port.gateway
static.network.wifi.ipv6_static_dns_enable
static.network.wifi.ipv6_primary_dns
static.network.wifi.ipv6_secondary_dns
static.network.wifi.ipv6_icmp_v6.enable

Parameter	Description	Permitted Values	Default
static.network.wifi.ipv6_internet_port.type	It configures the Internet port type for an IPv6 wireless network. 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. 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. 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. It works only if "static.network.wifi.ipv6_internet_port.type" is set to 1 (Static IP).	IPv6 Address	Blank
static.network.wifi	It triggers the static IPv6 DNS feature to turn on	0-Off, the phone will	0

.ipv6_static_dns_enable	or off for the wireless network. It works only if "static.network.wifi.ipv6_internet_port.type" is set to 0 (DHCP).	use the IPv6 DNS obtained from DHCP. 1-On, the phone will use a manually configured static IPv6 DNS.	
static.network.wifi.ipv6_primary_dns	It configures the primary IPv6 DNS server for the wireless network. 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. 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). 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**.



Provision Wi-Fi to Your Phone with a USB Device

Introduction

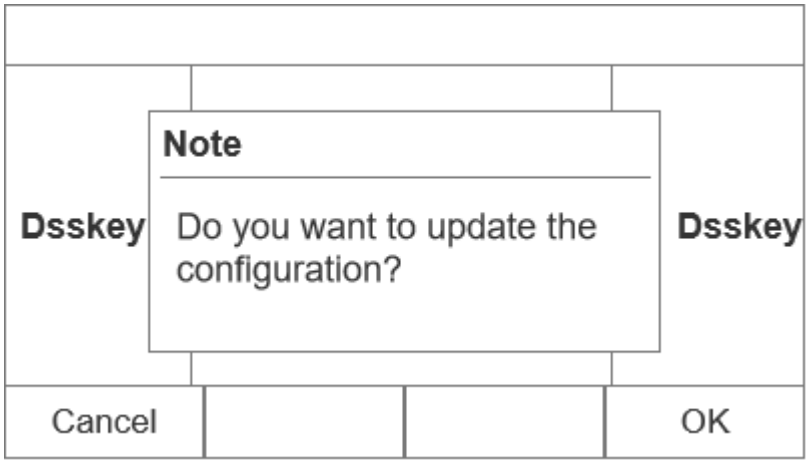
You can provision Wi-Fi to the phones using a USB storage device.

Before You Begin

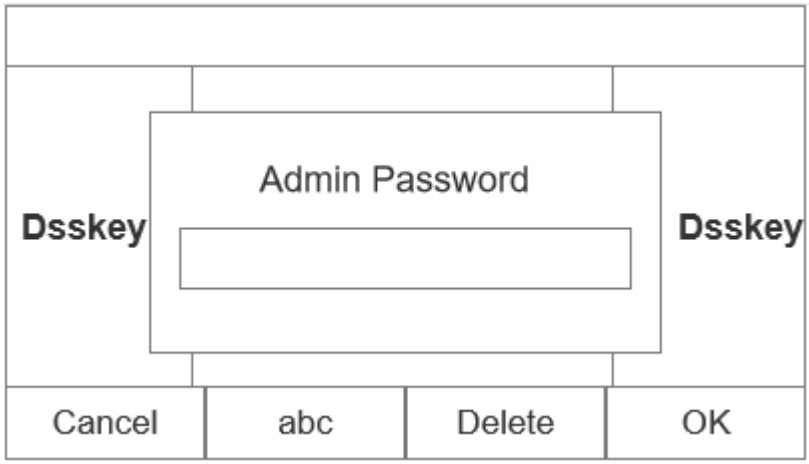
1. The phone supports USB drives formatted in FAT32 and NTFS.
2. Supported deployment files: mac.boot, y000000000000.boot, com.cfg, mac.cfg. The reading priority is: mac.boot > y000000000000.boot > com.cfg, mac.cfg.
3. The actual filename of com.cfg is determined by the configuration value of auto_provision.common_file_name.
4. For NTFS-formatted USB drives, the letters in the deployment file names must be in lowercase.
5. Configuration files only support absolute paths; relative paths are not supported.

Procedure

1. Copy the completed configuration file to the USB drive.
2. When the phone detects a USB drive, it will scan the files on the drive.
3. If it finds boot or cfg files, the phone will prompt the user with a pop-up asking whether to proceed with the configuration update.



4. Upon confirming the update, the user will need to enter a password, and the configuration update will begin.



Proxy Server

Introduction

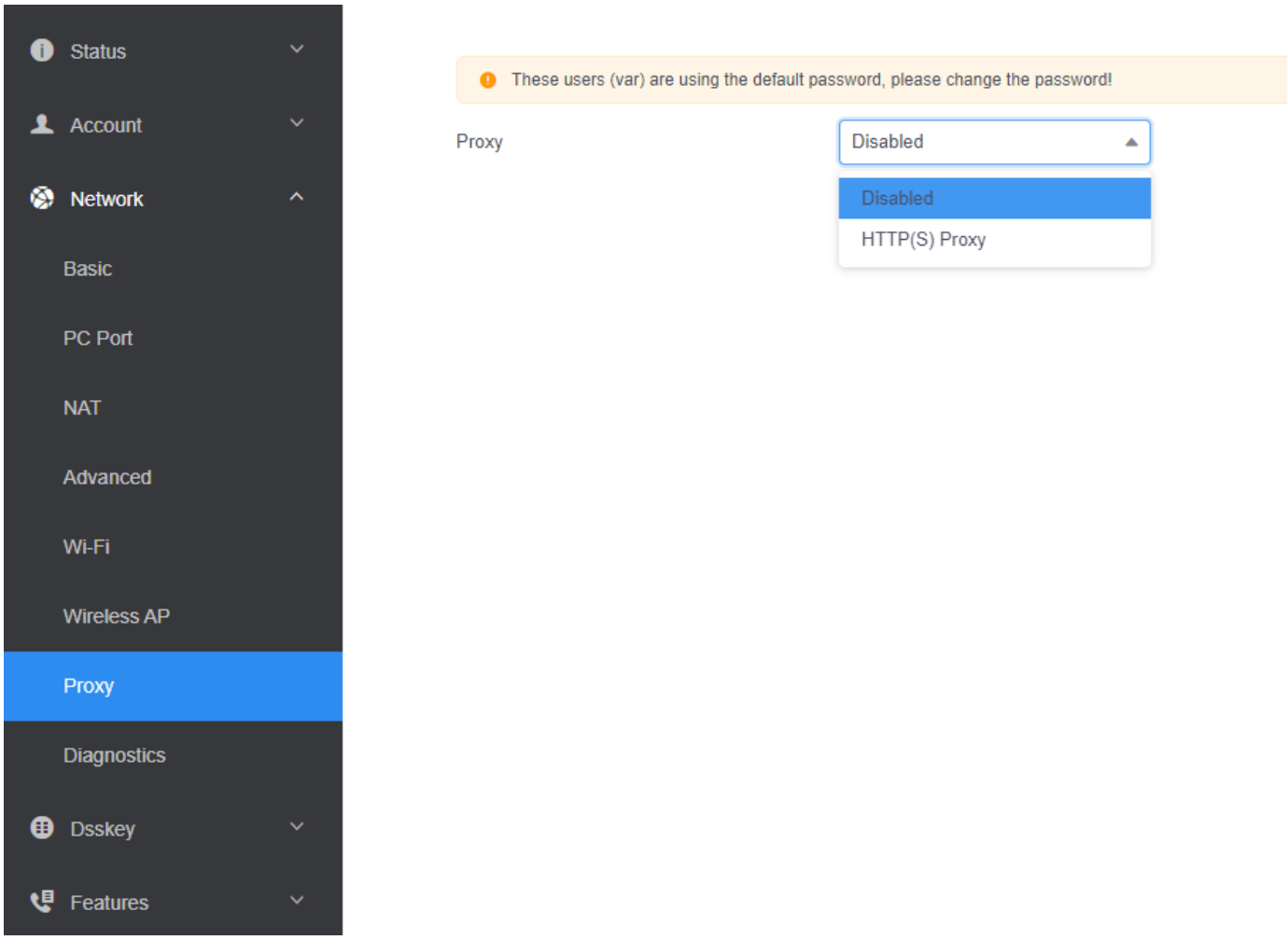
In an environment with high network security requirements, devices cannot directly connect to the public network and must be redirected through a proxy server to complete network access.

HTTP(S) Proxy

You can obtain proxy server information through the PAC file.

Configure via Web User Interface

1. Go to **Network** > **Proxy** on the web user interface.
2. Enable **Proxy**, and select **HTTP(S) Proxy** to do the related configuration.



Parameter	Description
WPAD	Configure the proxy type. - SOCKS5: The proxy server adopts the SOCKS5 protocol, supports TCP/UDP protocol, and supports various authentication mechanisms and other protocols.

	- HTTP Connect: Mainly to proxy browsers to access pages.
Proxy Set From	It configures the proxy mode. - IP: Port - PAC URL: Manually configure the PAC URL - PAC file: Upload PAC file directly
Proxy Hostname	It configures the IP address or domain name of the proxy server.
Proxy Port	It configures the port of the proxy server.
Bypass Proxy For	The configuration does not apply to the proxy's hostname or IP. Multiple host names are supported, and the host names are separated by commas.
PAC URL	Configure the URL where the PAC file is placed, and the device obtains the PAC file through autop. Proxy settings need to be configured when self-configuring as a PAC path.
Import PAC file	Upload the PAC file locally. It needs to be configured when the **Proxy Set From** is set as **PAC File**.

Auto Provisioning

```
network.proxy.mode
network.proxy.wpad
network.proxy.http.set_from
network.proxy.hostname
network.proxy.port
network.proxy.bypass_address
network.proxy_pac.url
network.proxy.address
network.proxy_pac.delete
network.proxy_pac.manual_url
```

Parameter	Description	Optional Value
network.pr	It enables or disables the proxy server.	**0**: Disabled

oxy.mode		**1**: Global proxy. You can configure the proxy server address manually. 2-HTTP(S) Proxy: You can obtain proxy server information through the PAC file.
network.proxy.wpad	Enable or disable WPAD to obtain PAC files dynamically.	**0**: Disabled **1**: Enabled
network.proxy.http.set_from	It configures proxy mode.	0-IP: Port, enter the IP address and port manually. 1-PAC URL, enter the PAC URL manually. 2-PAC File, upload PAC file directly.
network.proxy.hostname	It configures the domain name or the IP address of the proxy server.	String within 99 characters.
network.proxy.port	It configures the port of the proxy server.	Integer from 1 to 65535
network.proxy.bypass_address	It configures the host name or IP address that does not apply to the proxy server to access.	URL within 511 characters. Multiple host names or IP addresses are separated by commas.
network.proxy_pac.url	Configure the URL where the PAC file is placed, and the device obtains the PAC file through autop.	URL String within 511 characters.
network.proxy.address	It configures a proxy address.	IP address or URL.
network.proxy_pac.delete	Delete the PAC file from the phone.	FIxed: http://local_host/all
network.proxy_pac.manual_url	Manually configure the PAC URL.	String within 512 characters

Outbound Proxy in Dialog

Introduction

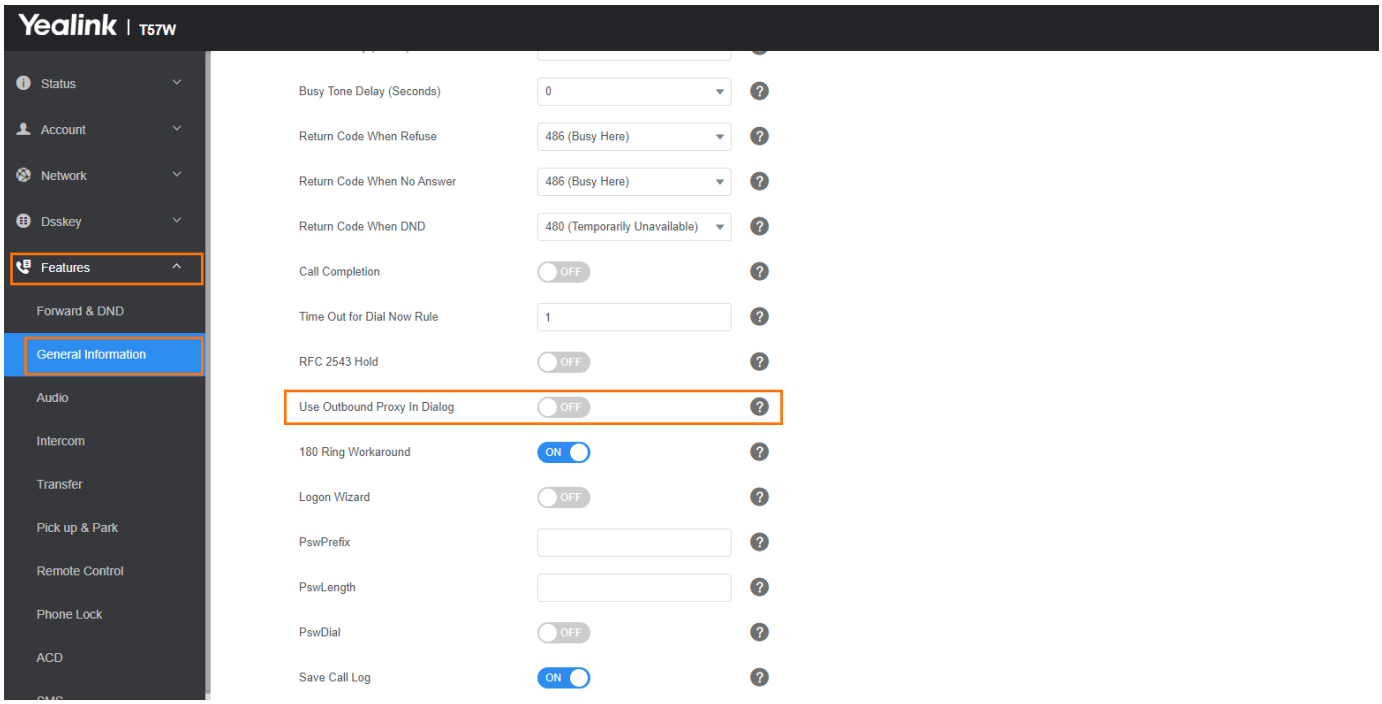
An outbound proxy server can receive all initiating request messages and route them to the designated destination. If the device is configured to use an outbound proxy server within a dialog, all SIP request messages from the device will be sent to the outbound proxy server as a mandatory requirement.

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. It works only if "account.X.outbound_proxy_enable" is set to 1 (Enabled).

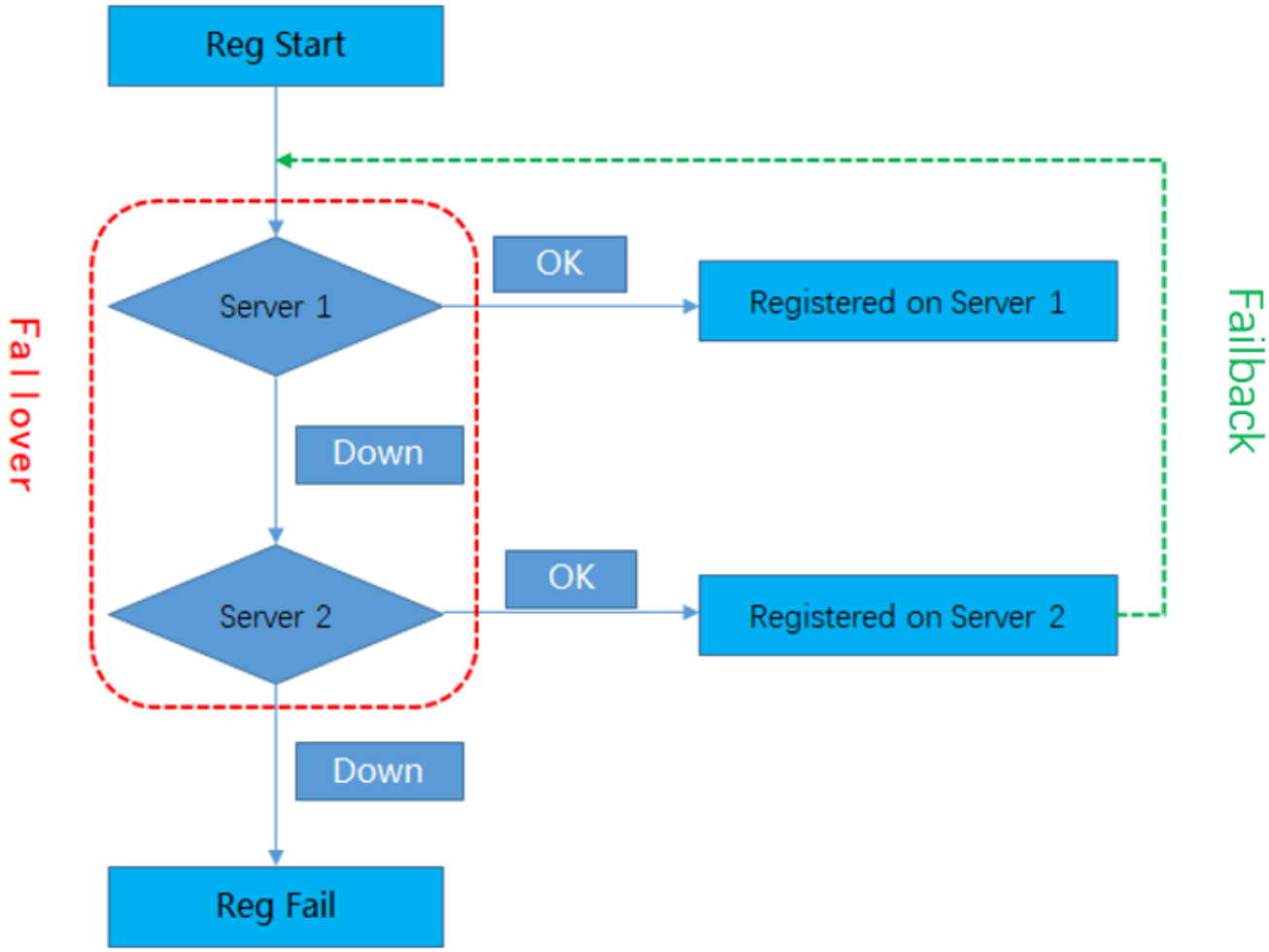
Server Redundancy

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:

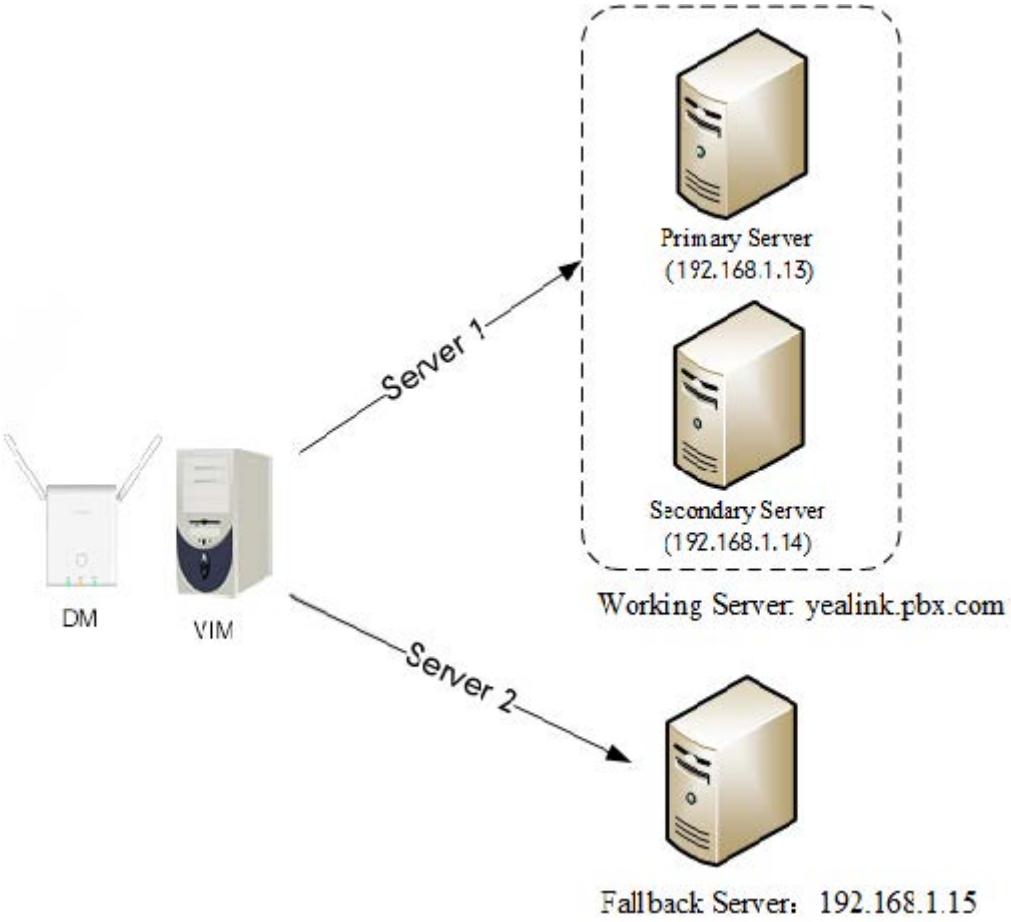
- **Failover**: In this mode, the full phone system functionality is preserved by having a second equivalent capability call server take over from the one that has gone down/offline. This mode of operation should be done using the DNS mechanism from the primary to the secondary server. Therefore, if 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.



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 interrupt 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 an IP 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. 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) is 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 the 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 the 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. Sends 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 a 503 message or the request for responding with a 100 Trying message times out (64*T1 seconds, defined in RFC 3261), then it 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 IP 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 IP 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 IP phone only registers to one server at a time. The IP phone first registers to the working server. In a failure situation, the IP phone registers with the fallback server.

SIP Server Name Resolution

If a domain name is configured for a server, the IP address(s) 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 IP phone to adapt to various deployment environments. The IP phone performs 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 IP phone. The IP phone will attempt to resolve the domain name of the server with the static DNS cache. For more information on static DNS cache, refer to Appendix B: Static DNS Cache.

Configure Yealink IP Phones

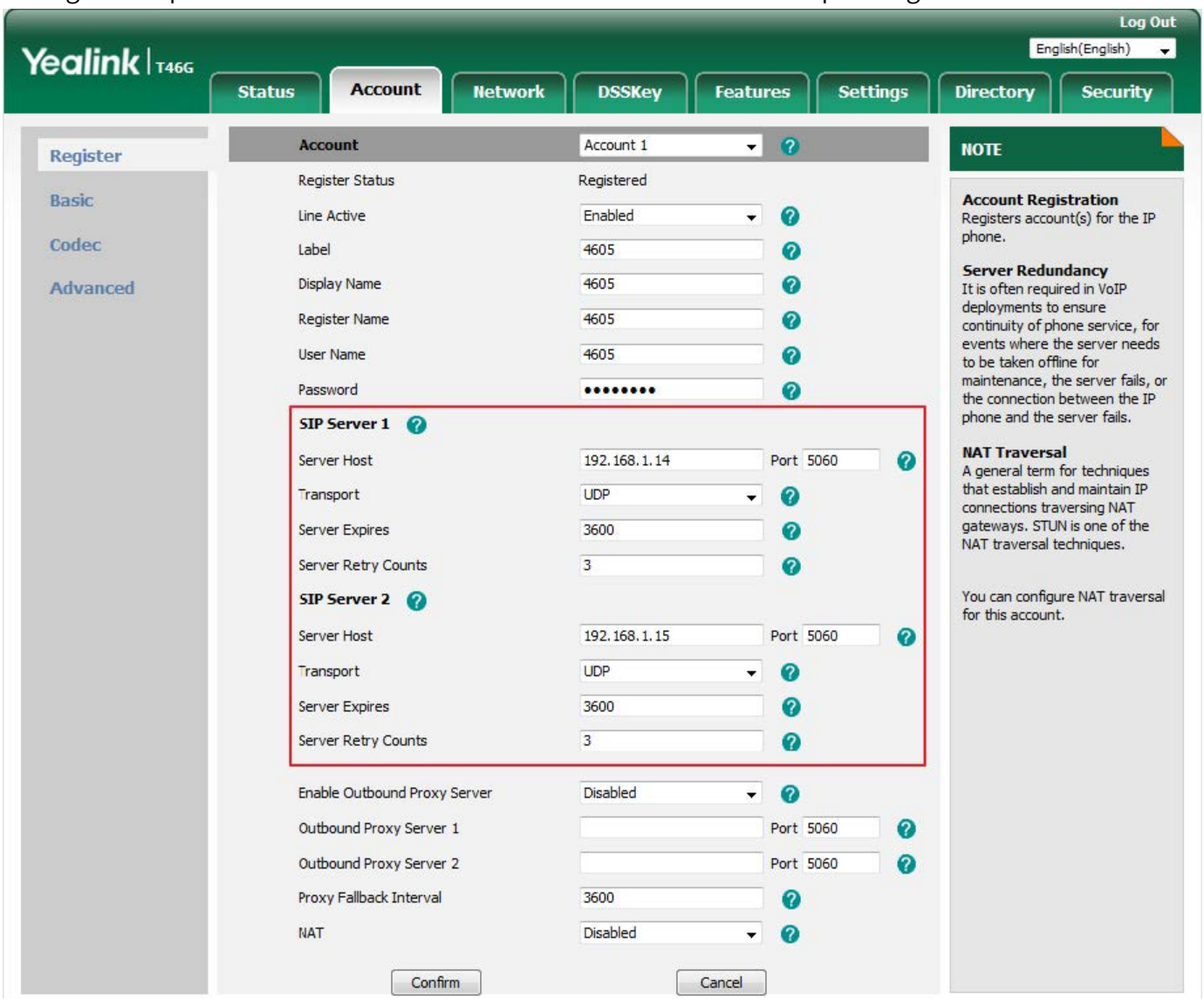
Set via the Web User Interface

The following takes configurations of a SIP-T46G IP phone running firmware 82 as examples.

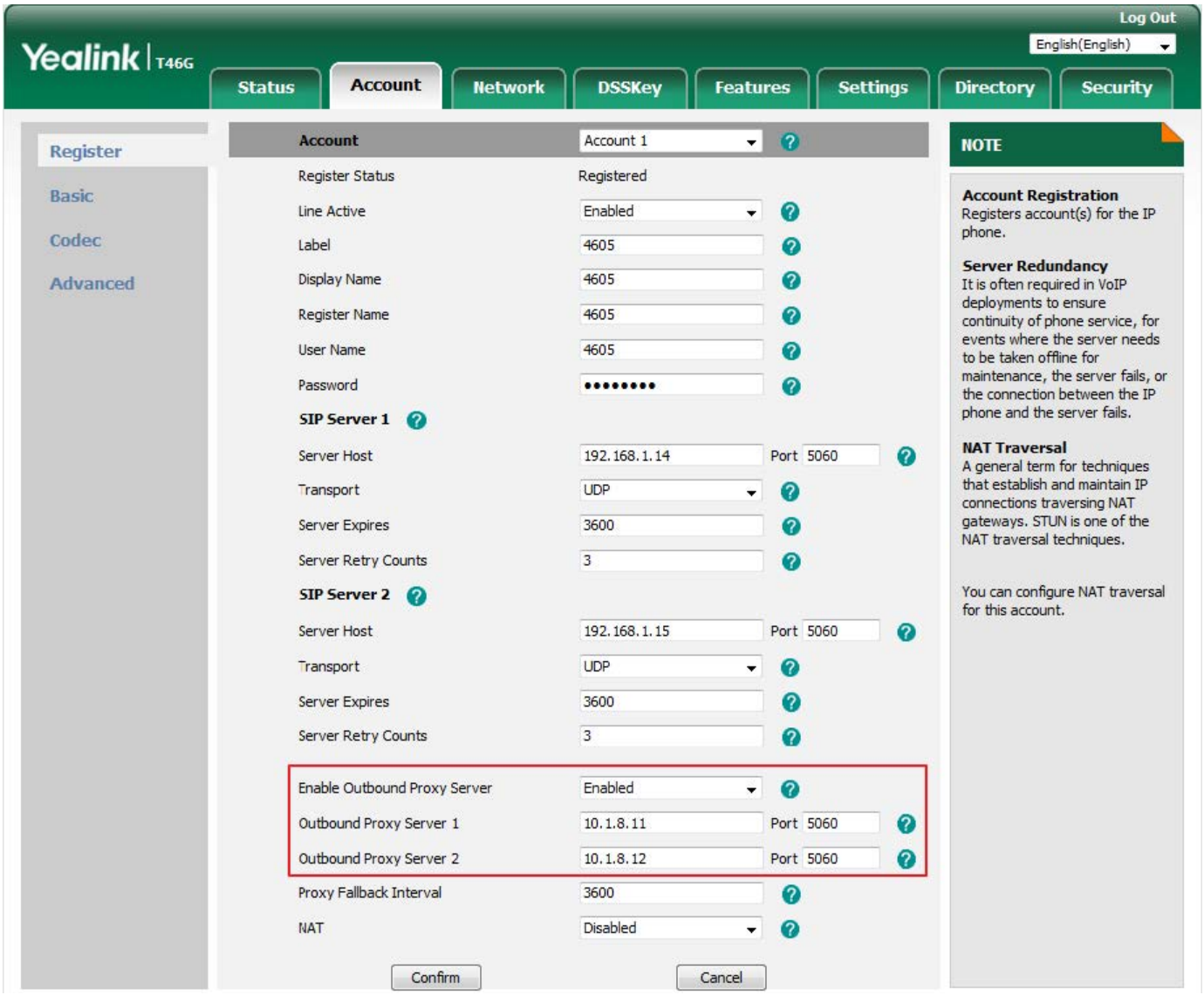
To configure server redundancy for a fallback purpose

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:
6. 1)Select **Enabled** from the **Enable Outbound Proxy Server** drop-down menu.
7. 2)Configure parameters of the outbound proxy server 1 and the outbound proxy server 2 in the corresponding fields.

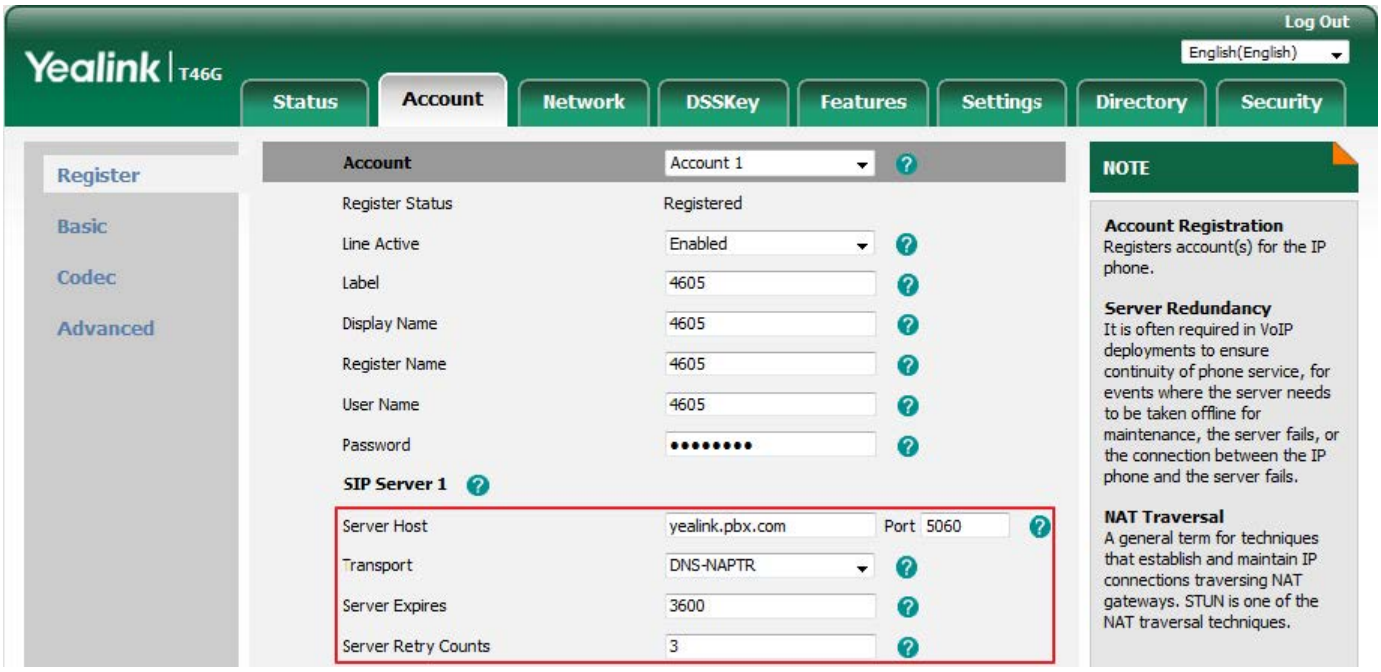


6. Click **Confirm** to accept the change.

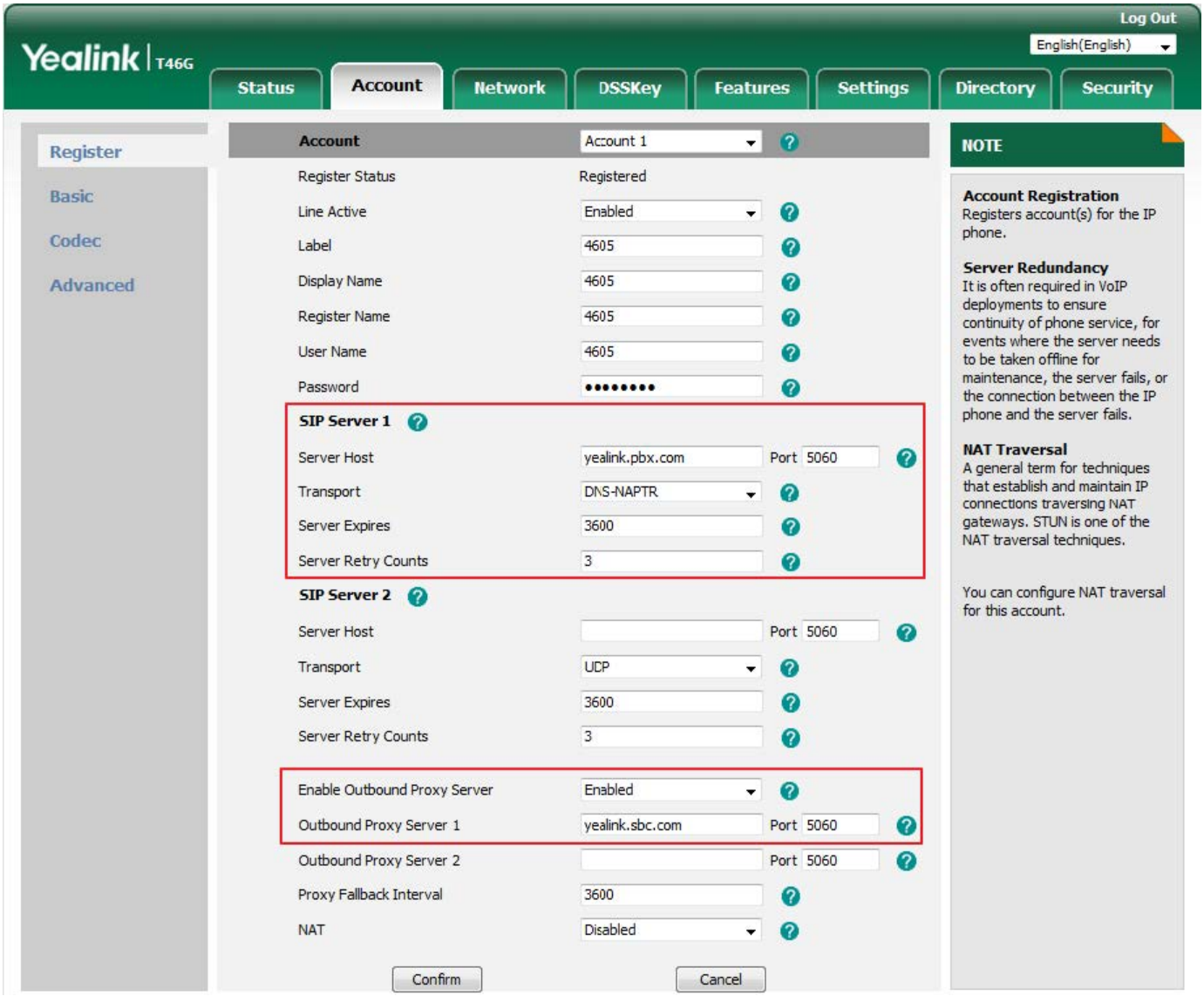
To configure server redundancy for failover purposes

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 parameters of the SIP server 1 or the 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:
7. 1)Select **Enabled** from the **Enable Outbound Proxy Server** drop-down menu.
8. 2)Configure parameters of the outbound proxy server 1 and the outbound proxy server 2 in the corresponding fields.
9. 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 registra	0	It configures the registration mode in fallback mode. It is not applicable to outbound proxy servers.

	tion **1**-Successive registration		
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. 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	0	It enables or disables the phone to send registration requests to the secondary server when encountering a failover.

	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 with the secondary server first, and then send the requests to it.		
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 send requests only to the registered server when encountering a failover. 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_serv	Integer from	3	It configures the number of retries attempted before

er.Y.invite_retry_counts[1] [2]	1 to 10		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	0	It configures the mode for the phone to retry the primary server in failover. It works only if "template.X.sip_server.Y.address" is set to the domain name of the SIP server.

	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.		
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.

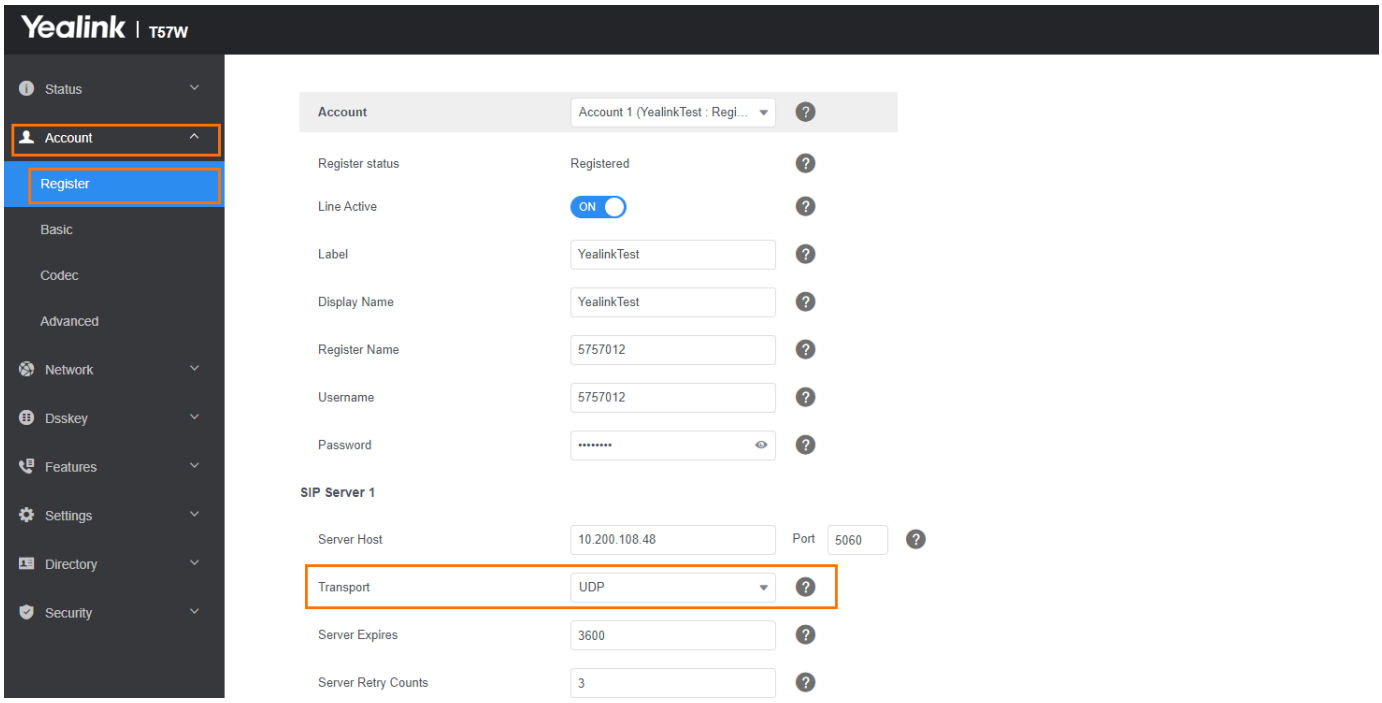
			If you set the parameter between 1 and 59, the timeout will be 60 seconds. It works only if "account.X.sip_server.Y.failback_mode" is set to 3 (duration).
account.X.sip_server.Y.failback_subscribe.enable[1][2]	**0**-Disabled **1**-Enabled, the phone will immediately re-subscribe to the secondary server, for ensuring 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. 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_transp	**0**-UDP	0	It configures the transport protocol the phone

ort_type	**1**-TCP		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 IP 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 IP 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 have not elapsed.
   - If the configured time interval has 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	1	It configures whether the phone uses the DNS cache for domain name resolution of the SIP server and caches the additional DNS records.

	additional DNS records.		
account.X.static_cache_pri[1]	**0**-Use domain name resolution from the server preferentially **1**-Use static DNS cache preferentially	0	It configures whether to preferentially 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 the NAPTR record X refers.
dns_cache_naptr.X.order[2]	Integer from 0 to 65535	0	It configures the order of the NAPTR record X. NAPTR record with the lower order is preferred.
dns_cache_naptr.X.preference[2]	Integer from 0 to 65535	0	It configures the preference of the NAPTR record X. NAPTR record with a 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 the NAPTR record X.
dns_cache_naptr.X.ttl[2]	Integer from 30 to 2147483647	300	It configures the time interval (in seconds) that the 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 the SRV record X.

dns_cache_srv.X.port[2]	Integer from 0 to 65535	0	It configures the port to be used in the SRV record X.
dns_cache_srv.X.priority[2]	Integer from 0 to 65535	0	It configures the priority for the target host in the SRV record X. Lower priority is preferred.
dns_cache_srv.X.target[2]	Domain name	Blank	It configures the domain name of the target host for an A query in the SRV record X.
dns_cache_srv.X.weight[2]	Integer from 0 to 65535	0	It configures the weight of the target host in the SRV record X. When priorities are equal, weight is used to differentiate the preference. Higher weight is preferred.
dns_cache_srv.X.ttl[2]	Integer from 30 to 2147483647	300	It configures the time interval (in seconds) that the 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 the A record X.
dns_cache_a.X.ip[2]	IP address	Blank	It configures the IP address that the domain name in the 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 the 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	3600	It configures the validity period of the expired DNS cache. It works only if "static.network.dns.last_cache_expired.enable" is set to 1 (Enabled).

	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.		
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
```

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

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.

> It is not applicable to CP920 phones.

Logon Wizard Configuration

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

Configuration parameter

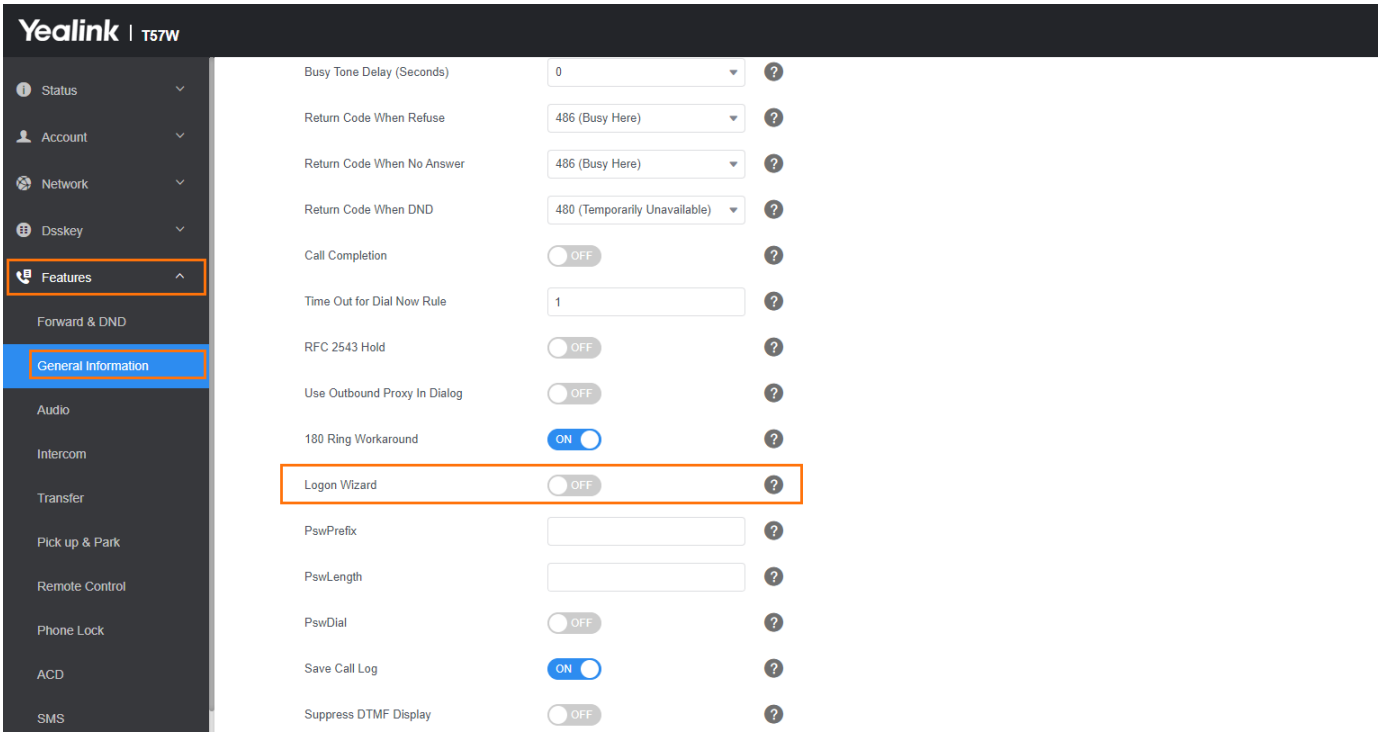
```
phone_setting.logon_wizard
hotdesking.startup_register_name_enable
hotdesking.startup_username_enable
hotdesking.startup_password_enable
hotdesking.startup_sip_server_enable
hotdesking.startup_outbound_enable
phone_setting.logon_wizard_forever_wait
```

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

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

Set via the Web User Interface

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


Yealink | T57W
Status
Account
Network
Dsskey
Features
Forward & DND
General Information
Audio
Intercom
Transfer
Pick up & Park
Remote Control
Phone Lock
ACD
SMS
Busy Tone Delay (Seconds)
0
Return Code When Refuse
486 (Busy Here)
Return Code When No Answer
486 (Busy Here)
Return Code When DND
480 (Temporarily Unavailable)
Call Completion
OFF
Time Out for Dial Now Rule
1
RFC 2543 Hold
OFF
Use Outbound Proxy In Dialog
OFF
180 Ring Workaround
ON
Logon Wizard
OFF
PswPrefix
PswLength
PswDial
OFF
Save Call Log
ON
Suppress DTMF Display
OFF

Multiple Line Keys per Account

Multiple Line Keys per Account

You can assign multiple line keys to associate with a specific account. The line keys are automatically assigned with the Line type from the first unused one (unused one means the line key is configured as N/A or the associated account is not registered). All calls on this account will be distributed evenly among these line keys. It is useful for managing a high volume of calls to an account.

When you assign multiple line keys to be associated with an account, you can configure the IP phone to transfer a call or set up a conference call on the current line key or a new distribution line key.

It is not applicable to T30P/T30/T19 § E2/CP920 phones.

Multiple Line Keys per Account Configuration

The following table lists the parameters you can use to configure multiple line keys per account.

Configuration parameter

features.auto_linekeys.enable
account.X.number_of_linekey
phone_setting.call_appearance.transfer_via_new_linekey
account.X.phone_setting.call_appearance.transfer_via_new_linekey
phone_setting.call_appearance.conference_via_new_linekey
account.X.phone_setting.call_appearance.conference_via_new_linekey

Parameter	Permitted Values	Default	Description
features.auto_linekeys.enable	0-Disabled 1-Enabled	0	It enables or disables to assignment of multiple line keys to associate with a specific account. The number of the line keys is determined by "account.X.number_of_linekey".
account.X.number_of_linekey[1]	Integer from 1 to 999	1	It configures the number of line keys to be assigned to a specific account from the first

	The number of the line keys varies by phone models. For the supported line keys, refer to Supported DSS Keys.		unused one. If a line key is in use, the phone will skip to the next unused DSS key.
phone_setting.call_appearance.transfer_via_new_linekey	0-Disabled, the phone will transfer a call on the current line key. 1-Enabled	1	It enables or disables to distribute a transferring call to a new line key (the new line key is not seized). If all line keys are seized, the current line key will be used. The number of the line keys is determined by "account.X.number_of_linekey". The value configured by the parameter "account.X.phone_setting.call_appearance.transfer_via_new_linekey" takes precedence over that configured by this parameter.
account.X.phone_setting.call_appearance.transfer_via_new_linekey[1]	0-Disabled, the phone will transfer a call on the current line key. 1-Enabled	Blank	It enables or disables to distribute a transferring call to a new line key (the new line key is not seized) for account X. If all line keys are seized, the current line key will be used. The number of the line keys is determined by "account.X.number_of_linekey". The value configured by this parameter takes precedence over that configured by the parameter "phone_setting.call_appearance.transfer_via_new_linekey".

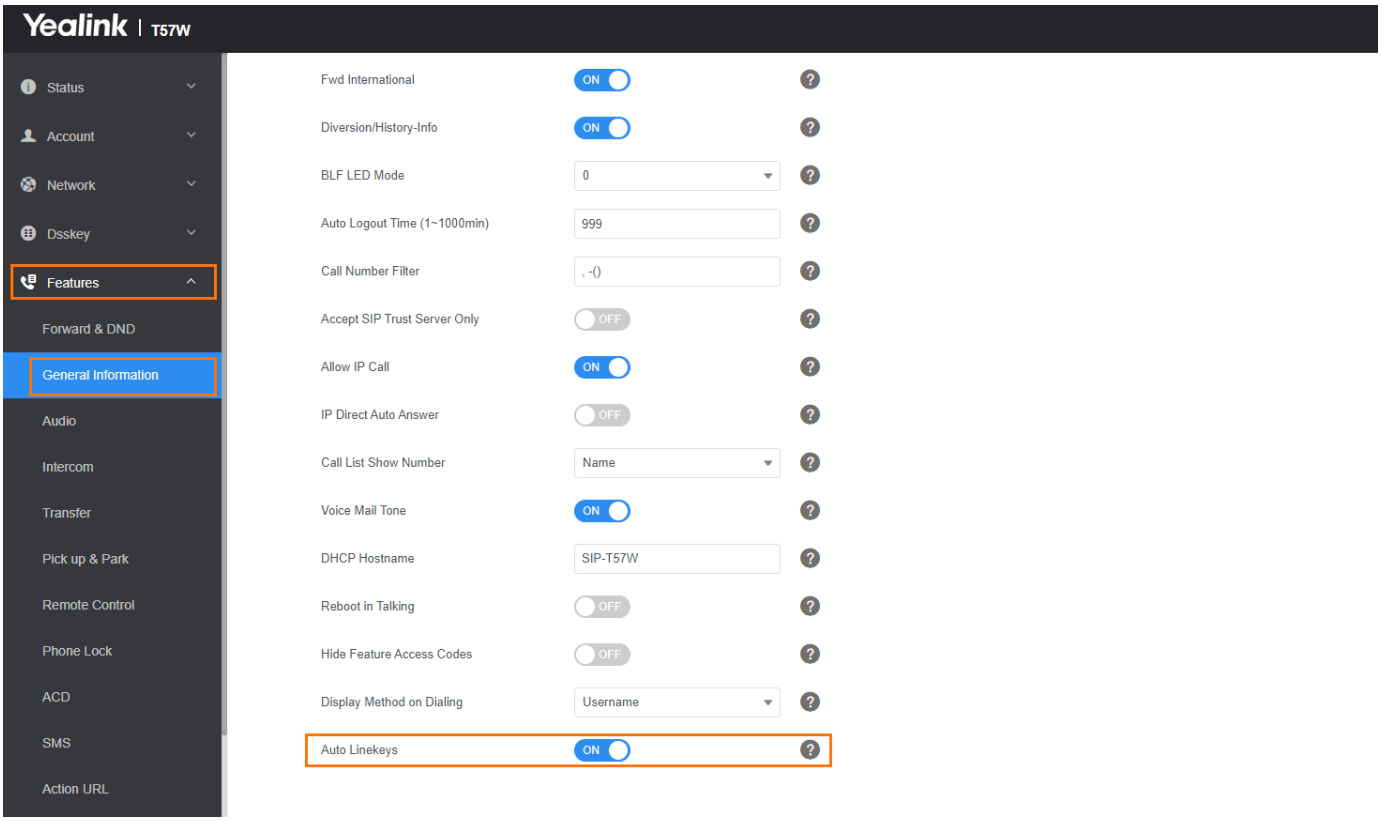
phone_setting.call_appearance.conference_via_new_linekey	0-Disabled, the phone will place a new call using the current line key when pressing the Conf/ Conference soft key. 1-Enabled, the phone will place a new call by automatically selecting a new line key (the corresponding line key is not seized) when pressing the Conf/ Conference soft key. If all line keys are seized, the current line key will be used.	1	It enables or disables to distribute a conference call to a new line key (the new line key is not seized). If all line keys are seized, the current line key will be used. The number of the line keys is determined by "account.X.number_of_linekey". The value configured by the parameter "account.X.phone_setting.call_appearance.conference_via_new_linekey" takes precedence over that configured by this parameter.
account.X.phone_setting.call_appearance.conference_via_new_linekey[1]	0-Disabled, the phone will place a new call using the current line key when	Blank	It enables or disables to distribute a conference call to a new line key (the new line key is not seized) for account X. If all line keys are seized, the current line key will be used. The number of the line keys is

	pressing the Conf/ Conference soft key. 1-Enabled, the phone will place a new call by automatically selecting a new line key (the corresponding line key is not seized) when pressing the Conf/ Conference soft key. If all line keys are seized, the current line key will be used.		determined by "account.X.number_of_linekey". The value configured by this parameter takes precedence over that configured by the parameter "phone_setting.call_appearance.conference_via_new_linekey".

[1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T58W/T58A/VP59/T56A/T58V/T74U/T74W/T77U/T85W/T87W/T88W (Pro)/T88V (Pro), X=1-16; for T53W/T53/T53C/T43U/T42U/T42G/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 § E2, X=1-2; for CP925/CP935W/CP960/CP965, X=1.

Set via the Web User Interface

On the web user interface, go to: **Features** > **General Information** > **Auto Linekeys.**



Auto Line Labels Rule Configuration

When assigning multiple line keys per account, these automatically assigned line keys use their Account Label (set by "account.X.label") as the default label to display on the screen. In order to distinguish these automatically assigned line keys, you can customize the line key labels one by one or configure the auto line labels rule for these line keys.

The following table lists the parameters you can use to configure the auto line labels rule.

Configuration parameter

account.X.auto_label.enable
account.X.auto_label.rule

Parameter	Permitted Values	Default	Description
account.X.auto_label.enable[1]	0-Disabled, the line keys labels are determined by “account.X.label”.	0	It enables or disables the Auto Label feature. It is only applicable to the automatically assigned line DSS keys. It works only if "features.auto_linekeys.enable" is set to 1 (Enabled).

	1-Enabled, the line keys labels are determined by the custom label rule (configure by the parameter “accout.X.auto_label.rule”).		
account.X.auto_label.rule[1]	String	{L}_{1}	It configures the Auto Label rule. You need to know the following basic regular expression syntax: {L}: The value is configured by the parameter “account.X.label”. {N}: An increasing number from N. For example, abc{1}{5} represents the following labels: abc15, abc26, abc37, and so on. Multiple labels are separated by “|”. For example, Yea|Yea|Yea|Tom_{2} means to display “Yea” for the first three line keys, and from the fourth one, display label Tom_2, Tom_3, and so on in turn. Other Characters: for example, ABC, will display ABC the same as what you have configured. It works only if "features.auto_linekeys.enable" and "account.X.auto_label.enable" are set to 1 (Enabled). The number of valid labels is configured by the parameter "account.X.number_of_linekey".

[1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T58W/T58A/VP59/T56A/T58V/T74U/T74W/T77U/T85W/T87W/T88W (Pro)/T88V (Pro), X=1-16; for T53W/T53/T53C/T43U/T42U/T42G/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 § E2, X=1-2; for CP925/CP935W/

> CP960/CP965, X=1.

Default Account

If there are multiple accounts registered on the phone, the phone will use the default account to dial out by default.

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

Configuration parameter

```
static.features.default_account
features.show_default_account
features.linekey_call_with_default_account
```

Parameter	Permitted Values	Default	Description
static.features.default_account	Integer from 1 to 16, 101, 102	1	It configures the default account. 1-Account 1 2-Account 2 3-Account 3 … 16-Account 16 101-PSTN 1 102-PSTN 2 For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T58W/T58A/VP59/T56A/T58V/T74U/T74W/T77U/T85W/T87W/T88W (Pro)/T88V (Pro), accounts 1-16, PSTN 1 and PSTN 2. (PSTN 1 and PSTN 2 are only applicable to T57W/T54W phones) For T53W/T53/T53C/T43U/T42U/T42S/T42G/T73U/T73W, accounts 1-12, PSTN 1, and PSTN 2. (PSTN 1 and PSTN 2 are only applicable to T53W/T53/T53C phones) For T41P/T41S/T27G, accounts 1-6. For T33P/T33G, accounts 1-4. For T40P/T40G/T23P/T23G, accounts 1-3. For T31P/T31G/T31/T21 § E2, accounts 1-2. For CP920/CP925/CP960/CP965: account 1, PSTN 1, and PSTN 2.

features.show_default_account	0-Disabled 1-Enabled	1	It enables or disables the phone to display the label of the default account on the left of the status bar on the idle screen. For T43U/T42G/T42S/T42U/T41P/T41S/T27G phones, the label of the default account is displayed in the bottom middle of the idle screen. It works only if "features.station_name.value" is left blank.
features.linekey_call_with_default_account	0-Disabled 1-Enabled	0	It enables or disables the phone to switch the default account when pressing the line key to dial. For example, the account on line 2 is not the default account. If this feature is enabled, when pressing the line key 2 to dial, the default account will switch to the account on line 2.

Account Registration

Introduction

Any handset must be 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.

Supported Accounts

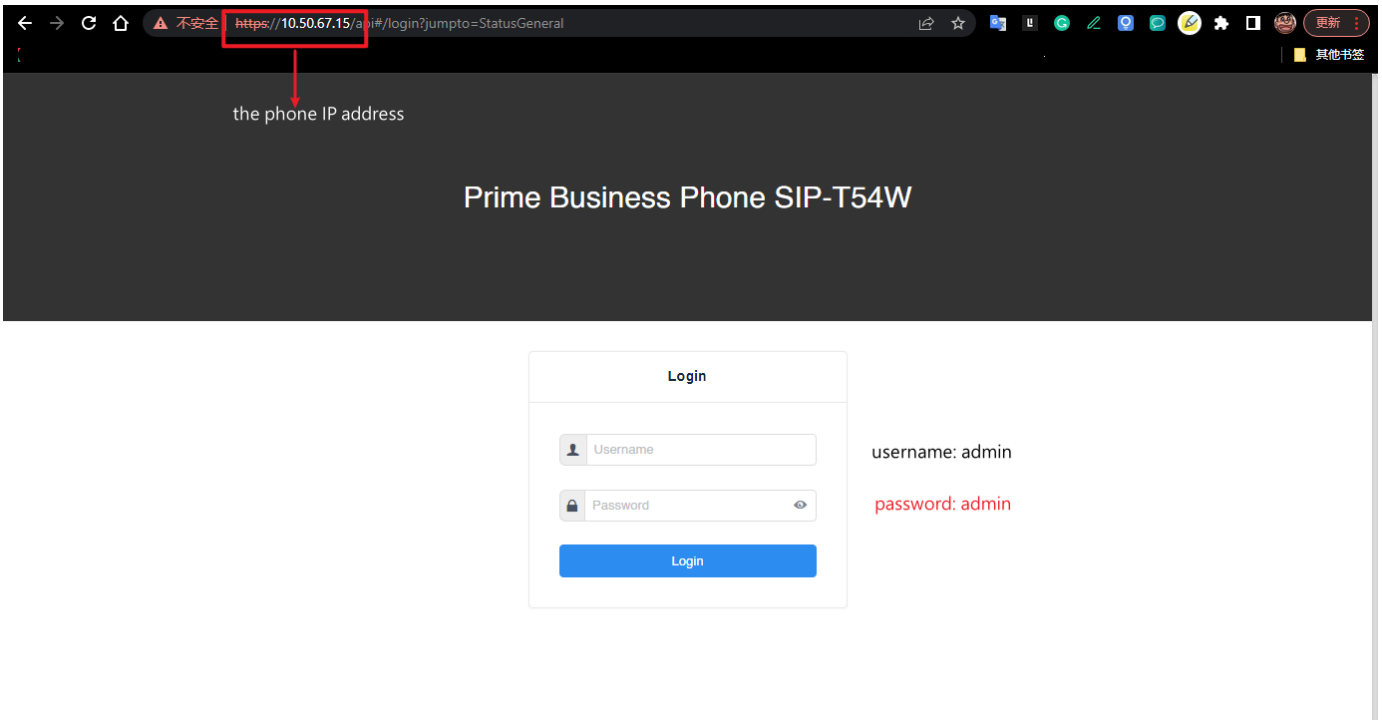
The number of registered accounts must meet the following:

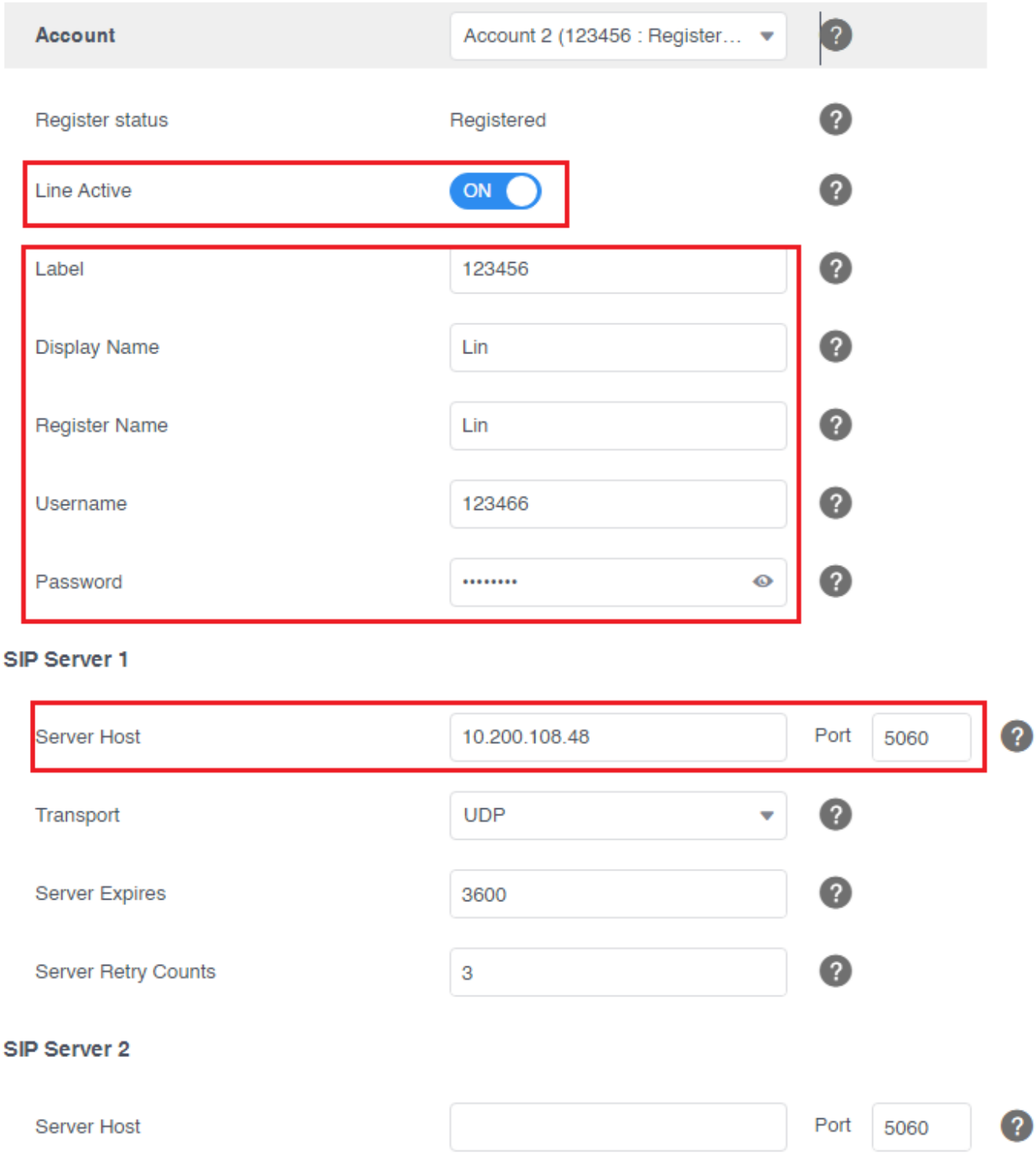
Phone Model	Accounts
T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T58V/VP59/T58W/T74U/T74W/T77U/T85W/T87W/T88W (Pro)/T88V Pro	<=16 <=2 (PSTN account)
T53W/T53/T53C/T43U/T42U/T42S/T42G/T73U/T73W	<=12 <=2 (PSTN account)
T41P/T41S/T27G	<=6
T33P/T33G	<=4
T40P/T40G/T23P/T23G	<=3
T31P/T31G/T31/T21 § E2	<=2
T30P/T30/T19 § E2	1
CP920	1 (SIP/Cloud account) <=2 (PSTN account)
CP925/CP960/CP965	1 (SIP account) <=2 (PSTN account)

Accounts Registration Configuration

Set via the Web User Interface

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


https://10.50.67.15/a#/login?jumpto=StatusGeneral
the phone IP address
Prime Business Phone SIP-T54W
Login
Username
Password
Login
username: admin
password: admin



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.

Starting from version x.86.0.112 and later, 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 the 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. 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. 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	60	It configures the maximum time to wait (in seconds) for the phone to retry to re-register after the account registration fails.

	equal to 0		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_ph	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to add “user=phone” to the SIP header of the INVITE

one[1]			message.
account.X.register_mac[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to add a 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 stands 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 the 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.

PSTN Account Configuration

The following table lists the parameters you can use to register the PSTN account.

> It is not applicable to CP935W phones.

Configuration parameter

pstn.account.X.enable
pstn.account.X.label

Parameter	Description	Permitted Values	Default	Supported Devices
pstn.account.X.enable[1]	It enables or disables the PSTN account X.	0-Disabled 1-Enabled	1	CP925, CP920, T57W, T54W, T53W, T53, T53C
pstn.account.X.label[1]	(Optional.) It configures the label to be displayed on the LCD screen for PSTN account X.	String within 99 characters	Blank	CP925, CP920, T57W, T54W, T53W, T53, T53C

> [1]X is the PSTN account ID. X= 1 to 2

FAQ

1. How to Configure Registration Subscribe?
2. SIP Account Register Failed?
3. How to erase SIP account on Yealink phone?

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 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="" group_id_name="All Contacts" default_photo=""
auto_divert="" />
<contact display_name="Test2" office_number="3510" mobile_number="3511"
other_number="3620" line="2" ring="" group_id_name="Blacklist" default_photo=""
auto_divert="" />
</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
Contac	display_na	Specify the contact name.

t	me	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" 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

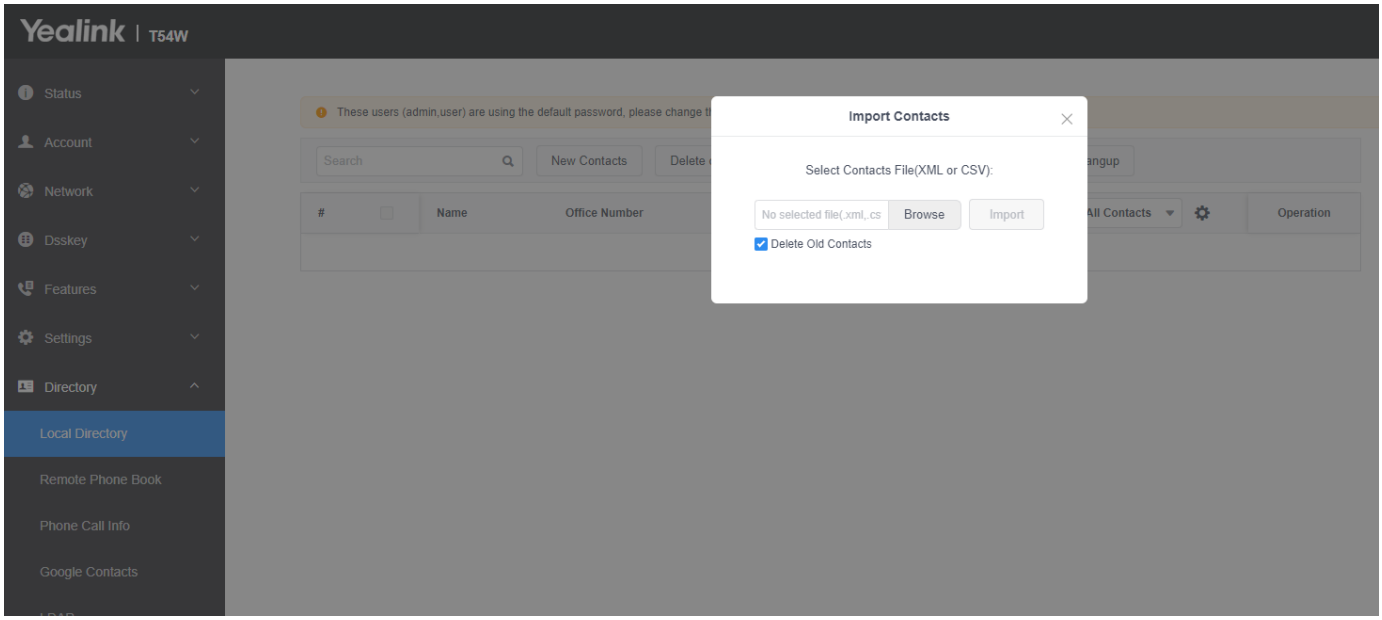
1. Open the local contact file.
2. To add a contact, add <contact display_name="" office_number="" mobile_number="" other_number=""/ > to the file. Each starts on a new line.
3. Specify the values within double quotes.
   For example:
   <contact display_name="Lily"office_number="1020" mobile_number="1021"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

local_contact.data.url
features.local_directory_number.type
features.local_directory.overwrite

Parameter	Permitted Values	Default	Description
local_contact.data.url	URL within 511 characters	Blank	It configures the access URL of the local contact file (*.xml).
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. It only works if your phone model is T3x/T4xU/T5xW and version is

			x.86.0.100 or later.

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).

MAC address, a unique 12-digit serial number, is assigned to each phone. You can obtain it from the barcode 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	Permitted Values	Default	Description
static.auto_provision.local_contact.backup.enable	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	0	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. It does not affect the downloading of the contact avatar/icon files.

	“<MAC>-contact.xml” to the specific path configured by the parameter “static.auto_provision.local_contact.backup.path” each time the contacts update; and downloads the contacts in the “<MAC>-contact.xml” according to its MAC address from the specific path during auto provisioning.		
static.auto_provision.local_contact.backup.path	String	Blank	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”. It works only if "static.auto_provision.local_contact.backup.enable" is set to 1 (Enabled).
static.auto_	0-PUT	0	It configures the way the phone

provision.custom.upload_method	1-POST		uploads the <MAC>-local.cfg file, <MAC>-calllog.xml file, or <MAC>-contact.xml file to the provisioning server (for HTTP/HTTPS server only).

Favorite Contacts

Favorite Contacts

You can enable the user to mark local contacts as favorites. The favorite contacts are stored in the Favorites directory, and the phone will automatically assign Speed Dial keys for these favorite contacts.

Configuration parameter

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

local_contact.favorite.enable
local.dsskey_type_config.mode
phone_setting.favorite_sequence_type

Parameter	Permitted Values	Default	Description
local_contact.favorite.enable	0-Disabled 1-Enabled, the phone automatically assigns Speed Dial keys for favorite contacts.	0 (1 for CP920)	It enables or disables the Favorites feature.
local.dsskey_type_config.mode	0-Enter the line key/ext key configuration screen 1-Enter the Add Contact screen	0	It configures which screen to enter by long pressing the line key or ext key. It works only if "local_contact.favorite.enable" is set to 1 (Enabled).
phone_setting.favorite_sequence_type	0 - linekey > exp1 key > ⋯ > expN key 1 - exp1 key > ⋯ > expN key > linekey 2 - linekey page1 > page1 from exp1 to expN > page2 from exp1 to expN > ⋯ > linekey from page2 to page3 3-page1 from exp1 to expN > page2	0	It configures the order of Speed Dial (Favorite) keys to be assigned automatically. It works only if your firmware version is x.86.0.112 or later.

	from exp1 to expN > ··· > linekey N is the number of your connected expansion modules.		It works only if "local_contact.favorite.enable" is set to 1 (Enabled). To assign Ext key, make sure the expansion module has been connected to the phone in advance.

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 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 T42 T42S T41S T46 T46S T54S T52 T48 T48S T49 T61 T66 T69
T69S CP860 CP920 T54W T53W T53 T57W"/>
<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 T49 T69 T69S T54W T53W T53 T57W"/>
<item id_name="mobilecontant" display_name="Mobile Contacts" priority="13"
enable="1" dev="T29 T46 T46S T54S T52 T48 T48S T42S T41S T27G CP920 T54W T53W
T53 T57W"/>
<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 T57W" />
<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	The existing directory list (For example, “localdirectory” for the local directory list). Do not edit this field.

	uc_buddies mobilecontant blocklist googledirectory sharedirectory (only applicable to T57W/T87W/T54W/T85W/T53W/T53/T53C phones) dectintercom (only applicable to T57W/T87W/T54W/T85W/T53W/T53/T53C phones) presencelist	
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 Shared Directory (only applicable to T57W/T87W/T54W/T85W/T53W/T53/T53C phones) Dect Intercom (only applicable to T57WT54W/T53W/T53/T53C phones) Presence List	The display name of the directory list. 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.

		This attribute is not applicable for T57W/T87W/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 T19 T21 T23 T40 T40G T27 T27G T29 T41 T42 T42S T41S T46 T46S T48 T48S CP920 T54W T53W T53 T53C T57W T48U T46U T43U T42U T29 T46 T46S T48 T48S T54W T53W T53 T53C T57W T48U T46U T43U T42U T29 T46 T46S T48 T48S T42S T41S T27G CP920 T54W T53W T53 T53C T57W T48U T46U T43U T42U T54W T53W T53 T53C T57W T48U T46U T43U T42U T73U T73W T74U T74W T77U T85W T87W T88W T88W Pro T88V Pro	The applicable phone models of the directory list. Common represents that the desired directory list is applicable to all IP phone models. 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 on 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	Permitted Values	Default	Description
static.directory_setting.url	URL within 511 characters	Blank	It configures the access URL of the custom directory file (favorite_setting.xml).
directory_setting.local_directory.enable	0-Disabled 1-Enabled	1	It enables or disables the users to access the local directory by pressing the Directory/Dir soft key.
directory_setting.local_directory.priority	Integer greater than or equal to 0	1	It configures the display priority of the local directory.
directory_setting.history.enable	0-Disabled 1-Enabled	0	It enables or disables the users to access the history by pressing the Directory/Dir soft key.
directory_setting.history.priority	Integer greater than or equal to 0	2	It configures the display priority of the call log list.
directory_setting.remote_phone_book.enable	0-Disabled 1-Enabled	0	It enables or disables the users to access the remote phone book by pressing the Directory/Dir soft key.
directory_setting.remote_phone_book.priority	Integer greater than or equal to 0	4	It configures the display priority of the remote phone book.
directory_setting.ldap.enable	0-Disabled 1-Enabled	0	It enables or disables the users to access the LDAP by pressing the Directory/Dir soft key.
directory_setting.ldap.priority	Integer greater than	5	It configures the display priority of the LDAP.

	or equal to 0		

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 on 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.

Supported devices: T57W, T54W, T53W, T53, T53C, T48U, T46U, T43U, T42U, T33P, T33G, T31P, T31G, T31, T30P, T30, T31W.

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	Permitted Values	Default	Description
features.enterprise_directory.enable	0-Disabled 1-Enabled	0	It enables or disables the Huawei enterprise directory feature.
features.enterprise_directory.host	String	Blank	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/services:443. It works only if "features.enterprise_directory.enable" is set to 1 (Enabled).
features.enterprise_directory_photo.host	String	Blank	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. It works only if "features.enterprise_directory.enable" is set to 1 (Enabled).

features.enterprise_directory.authentication_type	0-SIP authentication, use account 1 information to authenticate by default 1-Authentication information can be configured separately	0	It configures the authentication type of the enterprise contact. It works only if "features.enterprise_directory.enable" is set to 1 (Enabled).
features.enterprise_directory.user	String	Blank	It configures the user name used for authentication of the enterprise directory. It works only if "features.enterprise_directory.authentication_type" is set to 1.
features.enterprise_directory.password	String	Blank	It configures the password used for authentication of the enterprise directory. It works only if "features.enterprise_directory.authentication_type" is set to 1.

Lightweight Directory Access Protocol (LDAP)

Introduction

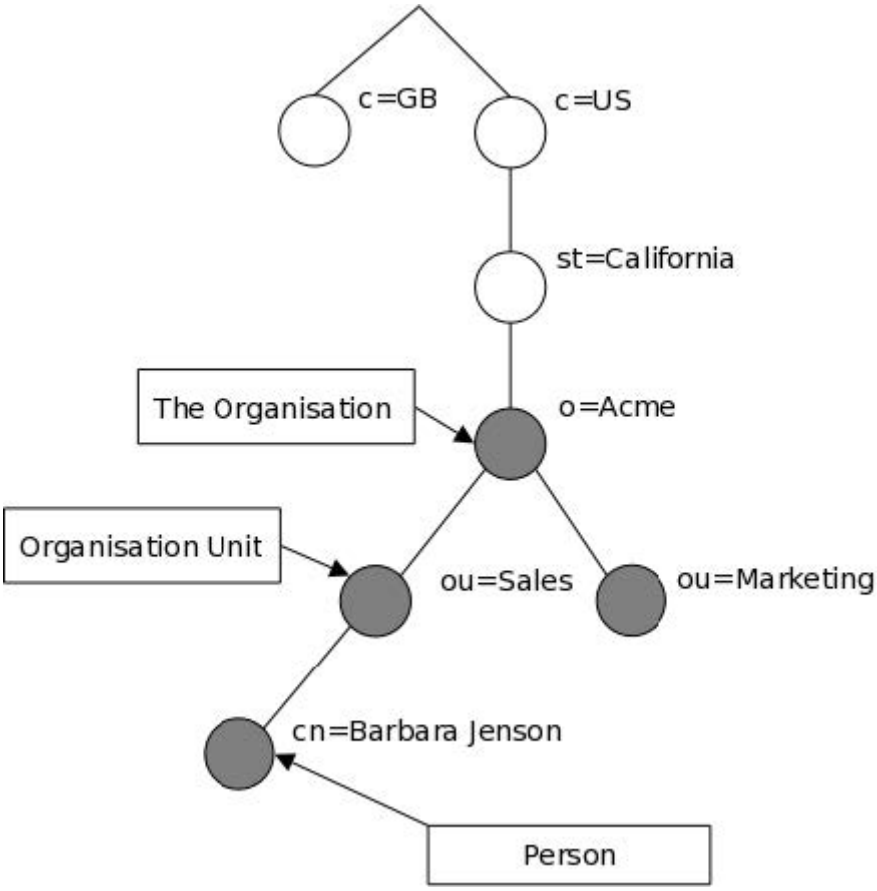
LDAP (Lightweight Directory Access Protocol) is a client/server protocol for accessing a directory service. LDAP is a directory service protocol that runs over TCP/IP.

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.



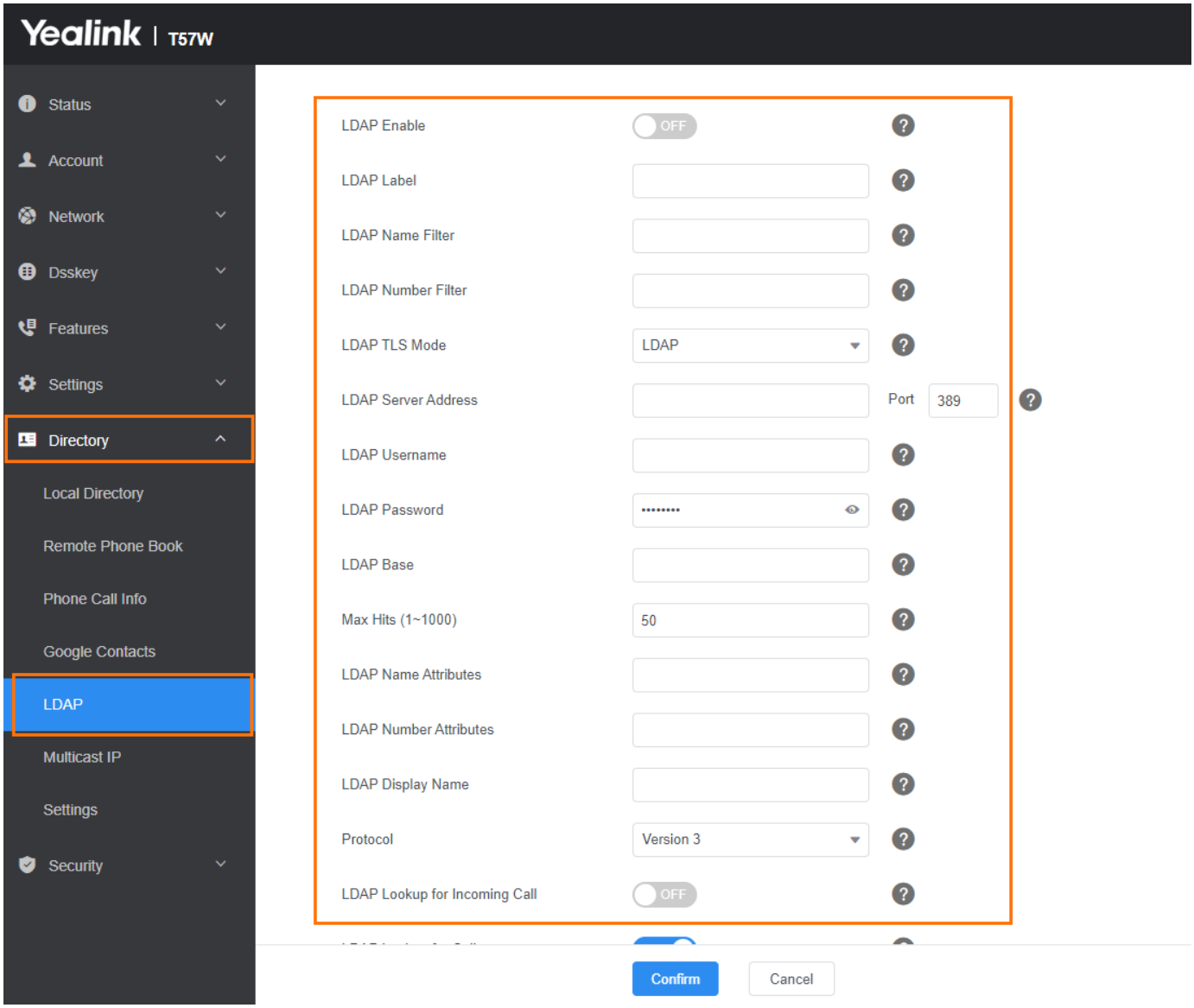
Supported Devices

Model	Firmware
T31/T33/T31P/T33P/T33G/T41U/T42U/T43U/T46U/T48U/T57W/T54W/T53W/T53/VP59/T58W/T58V/T58A/T56A/T27G, CP920, CP925, CP935W/CP960/CP965	version 83 or later
T7X/T8X	version 87 or later

Configure Yealink IP 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_t9.enable

ldap.search_timeout

ldap.search_mode

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 the 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	0	It configures the connection mode between the LDAP server and the phone.

	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).		
ldap.host	IP address or domain name	Blank	It configures the IP address or domain name of the LDAP server.
ldap	Intege	389	It configures the port of the LDAP server.

.port	r from 1 to 65535	(LDAPS: 636)	
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 in. 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 to be set for each contact record on the LDAP server.
lda	String	Bl	It configures the number of attributes of each record to be returned by the

p.numb_attr	within 512 characters	ank	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_sor	**0**-Disabled **1**-	0	It enables or disables the phone to sort the search results in alphabetical order or numerical order.

t	Enabled		
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. 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. It works only if ldap.enable is set to 1 (Enabled).
ldap.search_scope	sub-Arecursive search of all levels below the base domain name is	sub	It controls the search scope when searching for LDAP contact.

	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.		
ldap.search_t9.enable	**0**-Disabled **1**-Enabled	0	It is used to configure whether to enable LDAP T9 search.
lda	int	15	It is used to configure the timeout duration for LDAP request server search

p.search_timeout			results. It works only if you version is x.86.0.111 or later.
ldap.search_mode	**0**-Automatic search **1**-Manual search	0	It configures the search mode of the LDAP.

Handset LDAP Configuration

Prerequisite for using Handset LDAP: Your phone is in CCPhone mode and successfully connected to Handset.

```
handset.X.ldap.enable
handset.X.ldap.name_filter
handset.X.ldap.number_filter
handset.X.ldap.tls_mode
handset.X.ldap.host
handset.X.ldap.port
handset.X.ldap.base
handset.X.ldap.user
handset.X.ldap.password
handset.X.ldap.max_hits
handset.X.ldap.name_attr
handset.X.ldap.numb_attr
handset.X.ldap.display_name
handset.X.ldap.version
```

handset.X.ldap.call_in_lookup
handset.X.ldap.call_out_lookup
handset.X.ldap.ldap_sort
handset.X.ldap.incoming_call_special_search.enable
handset.x.ldap.customize_label

Parameter	Permitted Values	Default	Description
handset.X.ldap.enable[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the LDAP feature.
handset.X.ldap.name_filter[1]	String within 512 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.
handset.X.ldap.number_filter[1]	String within 512 characters	Blank	It configures the search criteria for the 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.
handset.X.ldap.tls_mode[1]	**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	0	It configures the connection mode between the LDAP server and the phone.

	connection between the LDAP server and the IP phone (port 636 is used by default).		
handset.X.ldap.host[1]	IP address or domain name	Blank	It configures the IP address or domain name of the LDAP server.
handset.X.ldap.port[1]	Integer from 1 to 65535	389 (LDAPS: 636)	It configures the port of the LDAP server.
handset.X.ldap.base[1]	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
handset.X.ldap.user[1]	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 in. Otherwise, you will need to provide the user name to log into the LDAP server. **Example:** ldap.user = cn=manager,dc=yealink,dc=cn
handset.X.ldap.password[1]	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.
handset.X.ldap.max_hits[1]	Integer from 1 to 1000	50	It configures the maximum number of search results to be returned by the LDAP server.
handset.X.ldap.name_attr[1]	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.
handset.X.ldap.numb_attr[1]	String within 512 characters	Blank	It configures the number of 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.
handset.X.ldap.display_name[1]	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.
handset.X.ldap.version[1]	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.
handset.X.ldap.call_in_lookup[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to perform an LDAP search when receiving an incoming call.
handset.X.ldap.call_out_lookup[1]	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to perform an LDAP search when placing a call.
handset.X.ldap.ldap_sort[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to sort the search results in alphabetical order or numerical order.
handset.X.ldap.i	**0**-Disabled	0	It enables or disables the phone to search

ncoming_call_special_search.enable[1]	**1**-Enabled		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. 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.
handset.x.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. It works only if ldap.enable is set to 1 (Enabled).

[1] X is the account ID.

Errors and Solutions

Error	Description	Solution
0x0003000000060001 Operations error	Server error. The error code returned by	Check the server.

	the LDAP server is unknown.	
0x0003000000060002 Protocol error	Phone compatibility error. The protocol version between the phone and the LDAP server does not match.	1. Push 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.
0x0003000000060003 Time limit exceeded	Server error. Server processing timeout.	Check the server.
0x0003000000060004 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.
0x0003000000060005 Compare False	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060006 Compare True	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060007 Authentication method not	Phone error. The server does not support the	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,

supported	authentication method of the phone LDAP request.	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.
0x0003000000060008 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.
0x0003000000060000a Referral	Server error. The server is temporarily unavailable to handle this request.	Check the server.
0x0003000000060000b Administrative limit exceeded	Server error. The time token used 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.
0x0003000000060000c Critical extension is unavailable	Phone compatibility error. The server does not support	Please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.

	some attribute items requested by the phone.	
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/.
0x0003000000060024 Alias dereferencing problem	Server error.	Check the server.
0x0003000000060030 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's 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.
0x0003000000060031 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.
0x0003000000060	Server error.	Check whether the server has enabled the access

032 Insufficient access	The server refuses phone access.	permission for the phone.
0x0003000000060033 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.
0x0003000000060034 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.
0x0003000000060035 Server is unwilling to perform	Server error. The server is unwilling to perform the action.	Check the server.
0x0003000000060036 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.
0x0003000000060050 Other (e.g., implementation specific) error	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060 0c7 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.

0x0003000000060 0c6 Local error	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060 0c5 Encoding error	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060 0c4 Decoding error	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060 0c3 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 5s). 2. If the phone stays in the time-out status for a long time, check whether the server works normally.
0x0003000000060 0c2 Unknown authentication method	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060 0c1 Bad search filter	Phone configuratio n 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/.
0x0003000000060 0c0 User cancelled operation	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060 0bf Bad parameter to	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.

an ldap routine		
0x00030000000600be Out of memory	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600bd Connect error	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600bc Not Supported	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600ba 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.
0x00030000000600b9 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).
0x00030000000600b8 Client Loop	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600b7 Referral Limit Exceeded	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600 12c filter attributes invalid	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/. The % symbol in the Yealink phone filter configuration equals *. Therefore, you need to configure the % symbol rather than *.
0x0003000000060	Certificate error. The	Keep the CN value in the phone LDAP server consistent with the one in the CA certificate.

12d CN Validation error	certificate CN fails to be authenticated. The CN value in the server CA certificate is not consistent with the one in the LDAP server.	
0x0003000000060 12e Certificates error	Certificate error. The phone does not detect the correct CA certificate.	Upload the correct server CA certificate to the phone.
0x00030000000601 2f Domain name resolution failed	Phone configuration or network error. The LDAP Server cannot be resolved.	1. If other devices can access the LDAP server, you can put the faulty phone on the same network as the 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.
0x0003000000060 130	Phone compatibility error. The phone and the server fail to negotiate a TLS algorithm	1. Adjust the server algorithm. 2. Yealink FAE will also do further analysis to give you a solution ASAP.

	when using LDAPS.	
0x0003000000060131	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

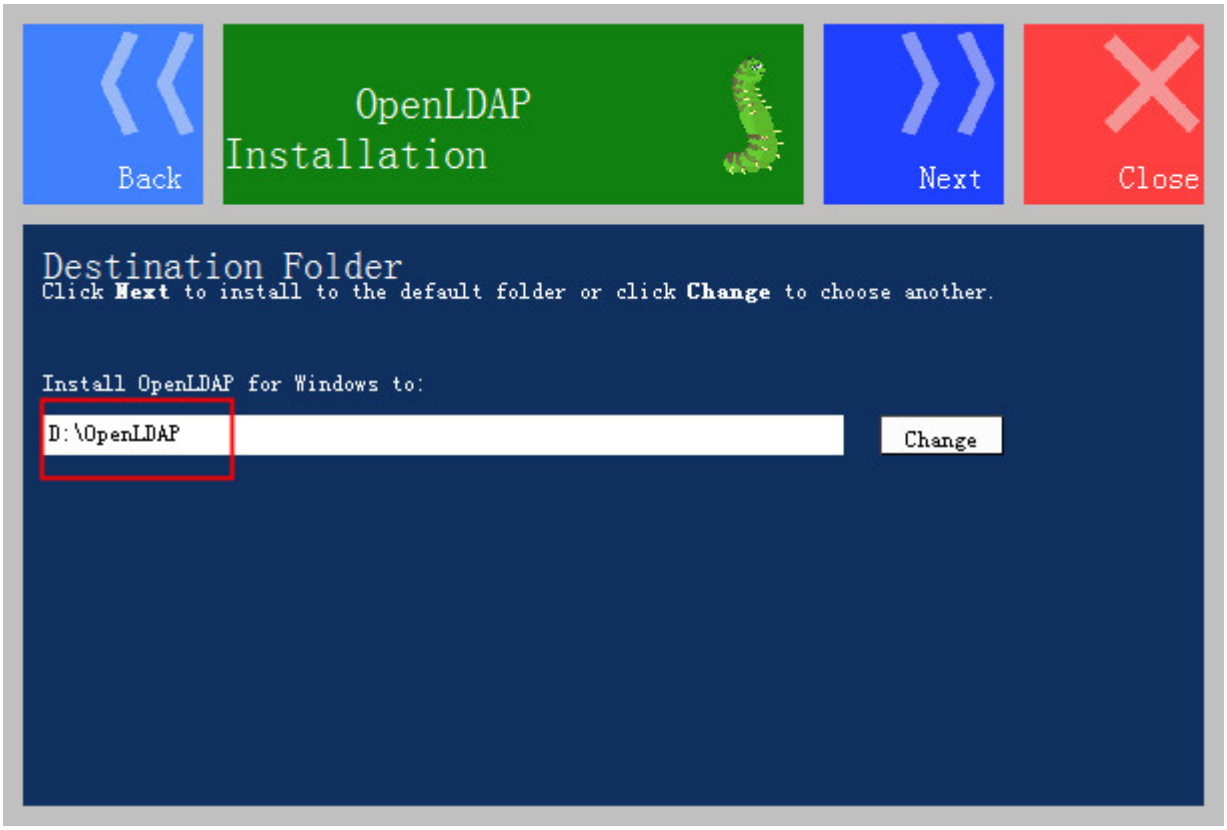
This section shows you how to install an OpenLDAP server on a Microsoft Windows 2007 system. The OpenLDAP server software is available for free.

You can download it from http://www.userbooster.de/en/download/openldap-for-windows.aspx?l=en.

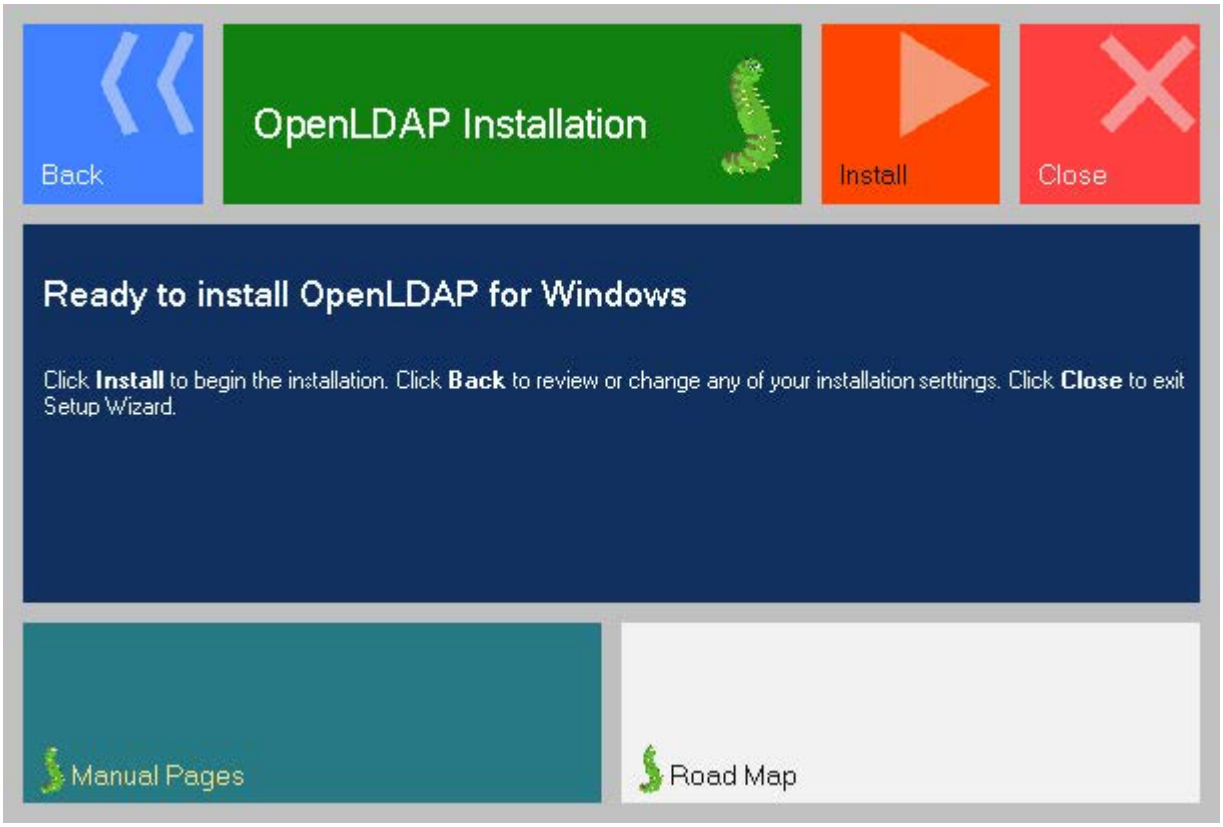
To install the OpenLDAP server:

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.
8. 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.

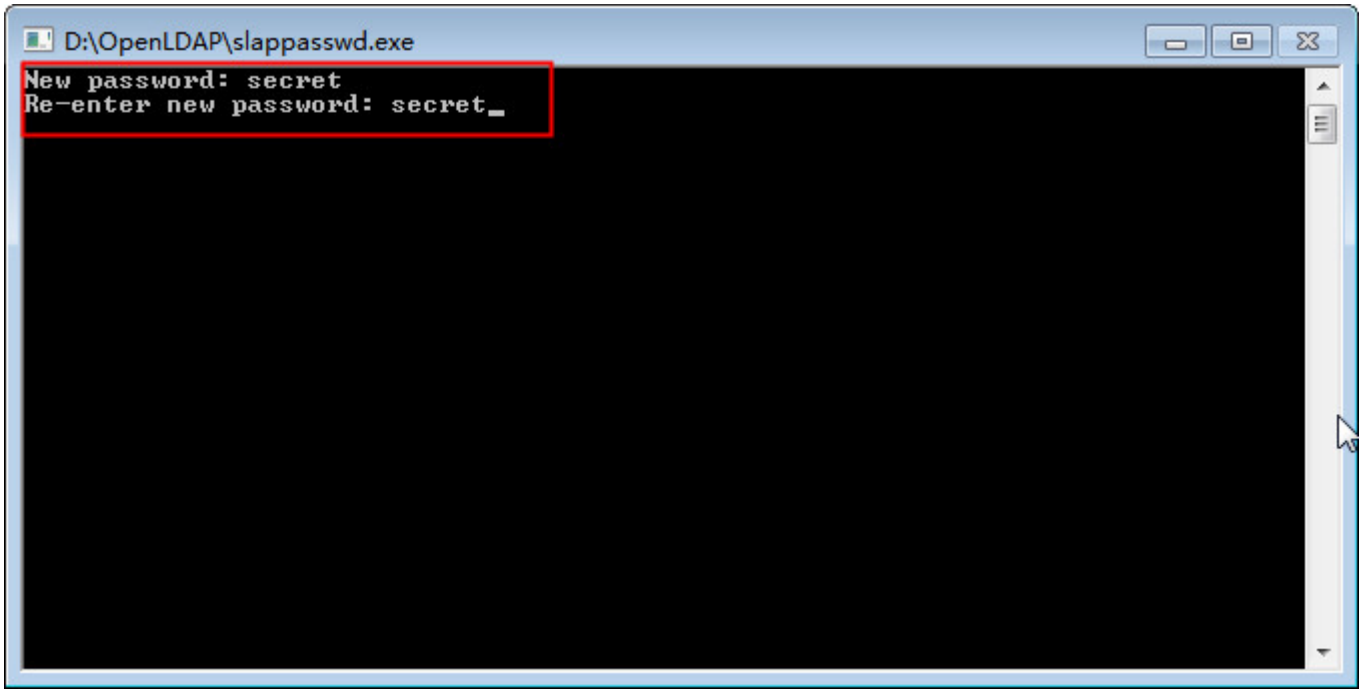
Configure the OpenLDAP Server

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.
2. Find the commands
3. Suffix "dc=maxcrc, dc=com" Rootdn "cn=Manager,dc=maxcrc,dc=com"
4. Suffix defines the components of the domain name.
5. Rootdn defines the manager as a management user for accessing the LDAP server.
6. For example:
7. Suffix "dc=yealink,dc=com" Rootdn "cn=Manager,dc=yealink,dc=com "
8. 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.
9. If the domain name contains additional components, for example, yealink.com.cn, the suffix line will be edited as below:
10. 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.



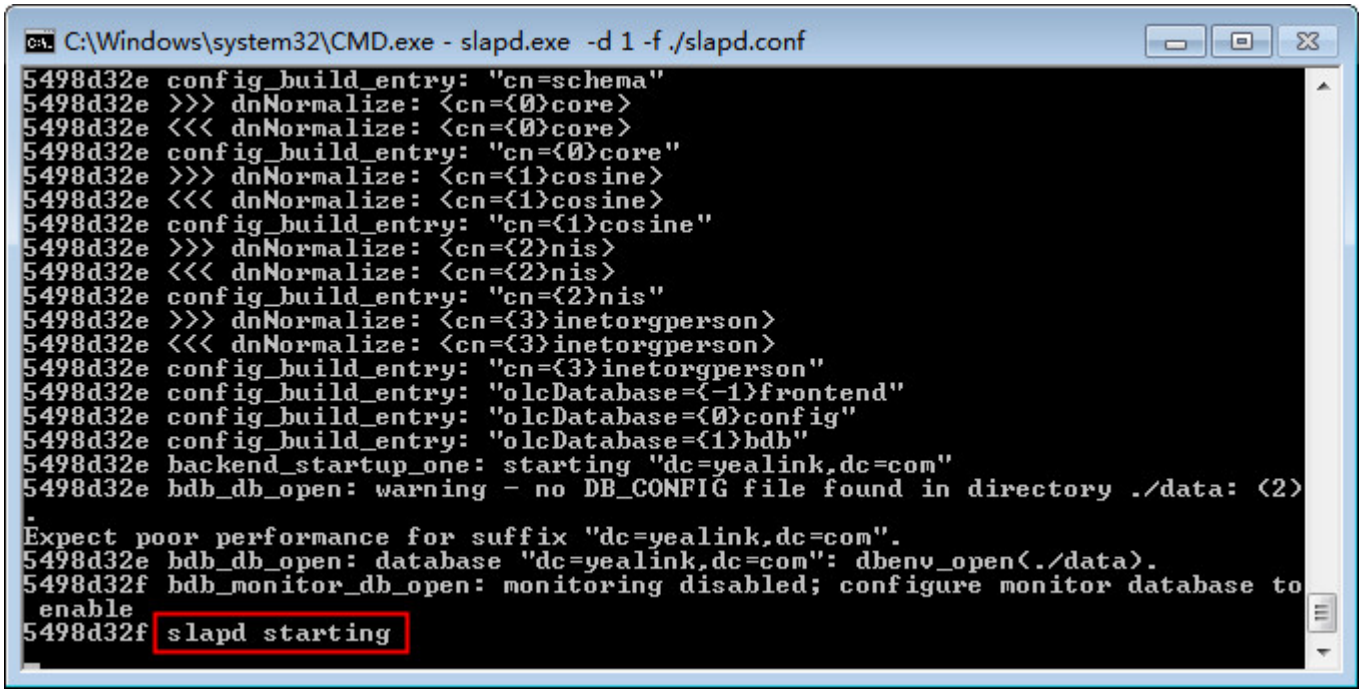
Start the Slapd Service

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.

6. If the service runs successfully, you can find the prompt “**slapd starting**”.
7. The screenshot for reference is shown as below:



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 in the OpenLDAP installation path. For example, create a text document named test.txt, right-click the test.txt document and then select to rename it, modify the filename extension to 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:

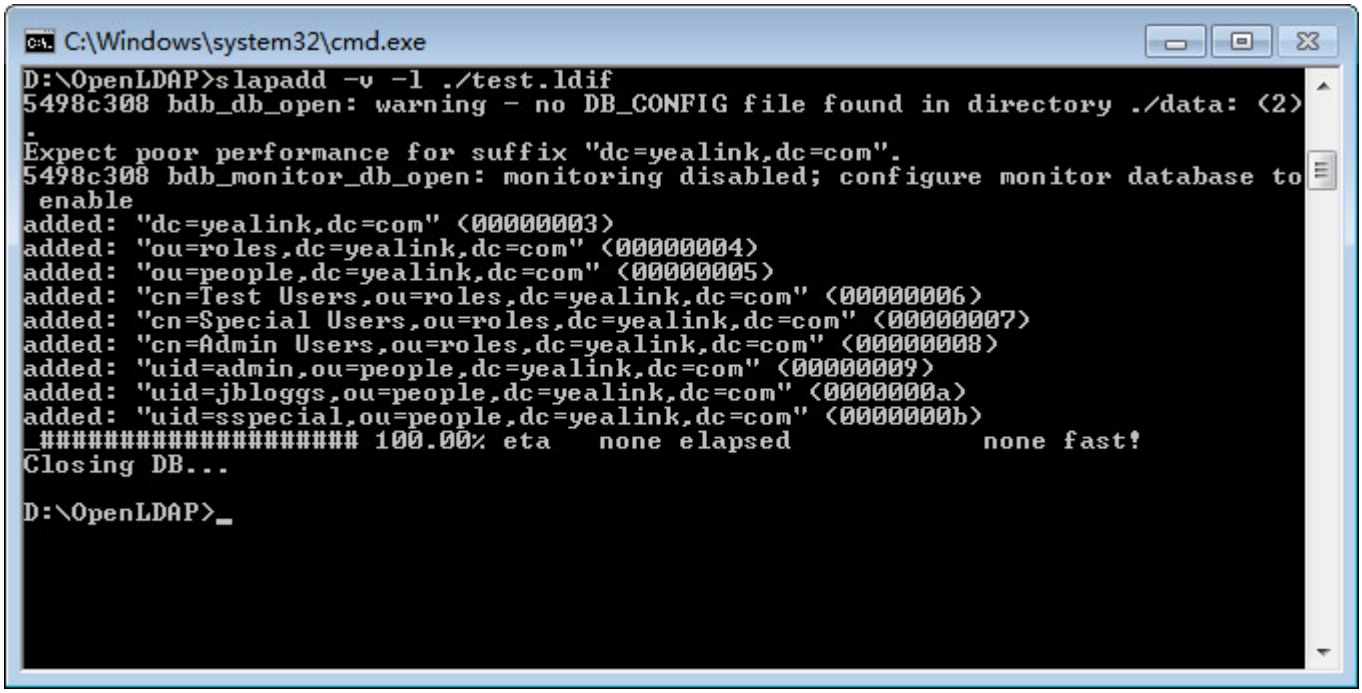
```
dn: dc=yealink,dc=com
objectClass: top
objectClass: dcObject
objectClass: domain
dc: yealink

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 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.

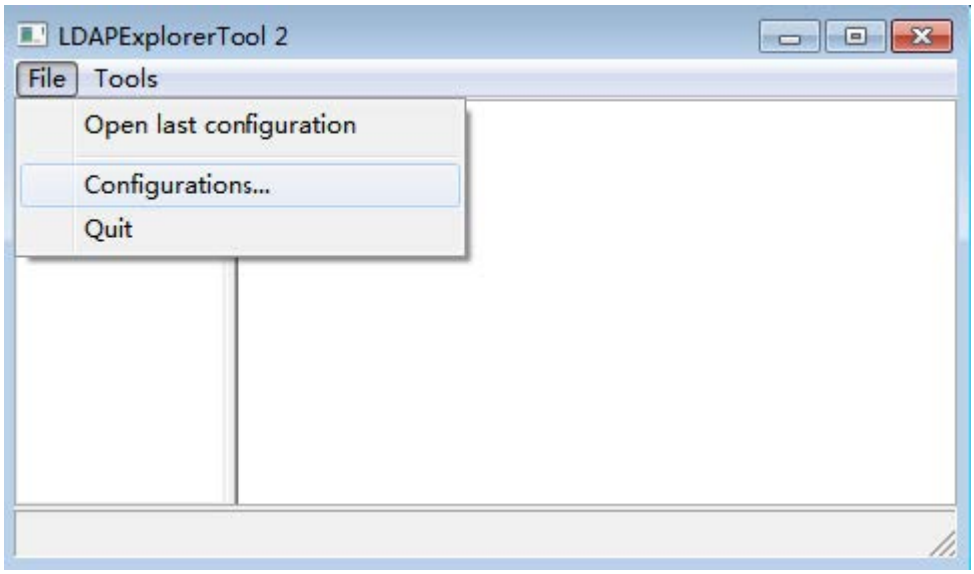
If you have an LDAPExploreTool2 application installed on your computer, open it now; otherwise, download the application from http://ldaptool.sourceforge.net/. And then complete the installation following the wizard.

Create a Configuration

To create a configuration:

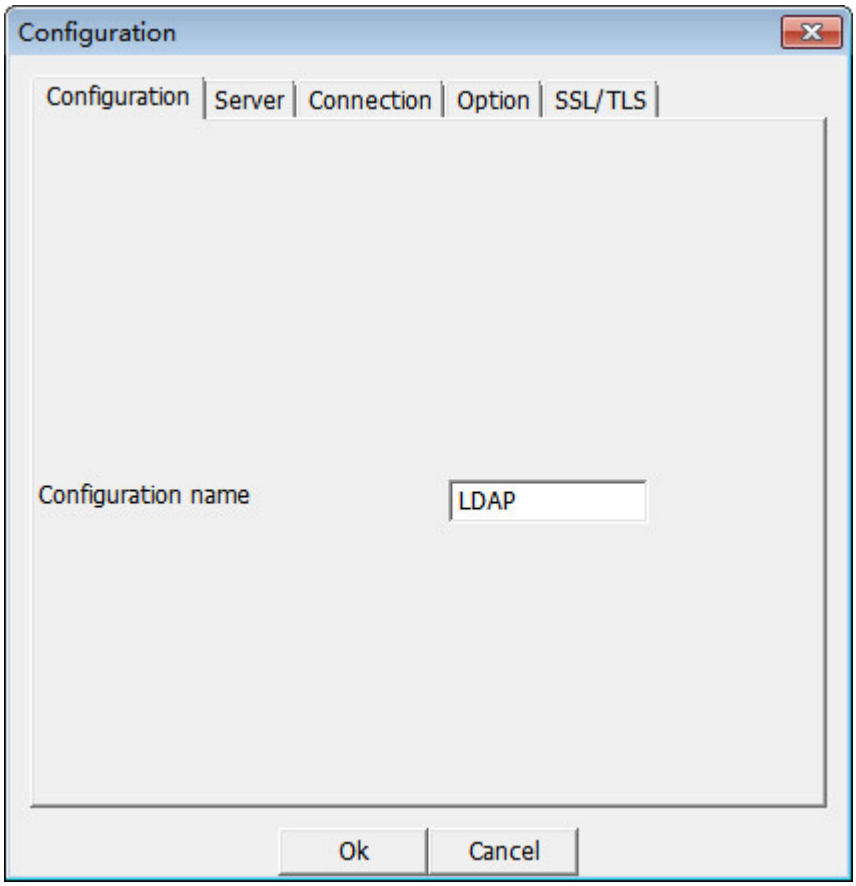
1. Double-click the LDAPExploreTool2.exe to run the application.

2. Click **File** > **Configurations**.

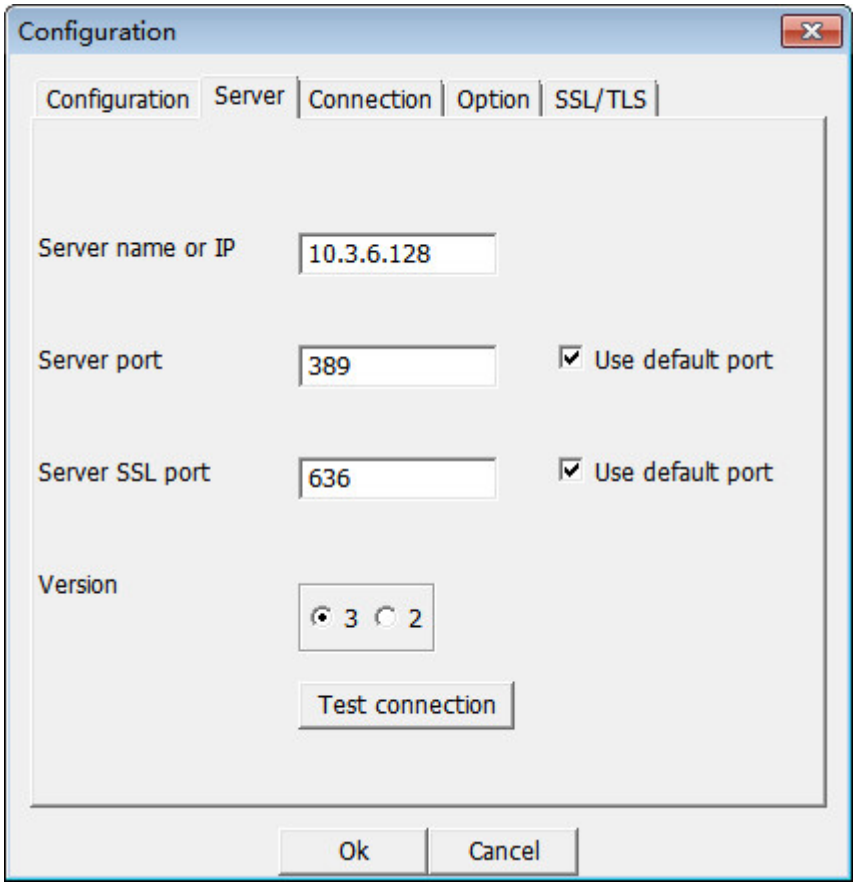


3. Click **New** to create a new configuration.

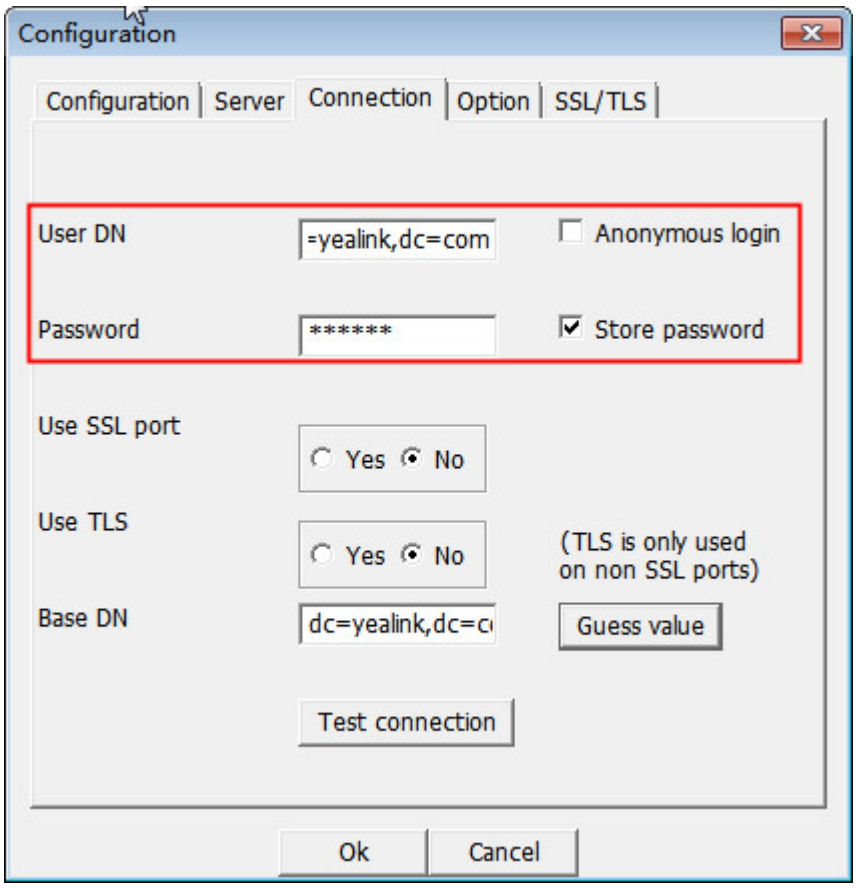
4. Enter a name in the **Configuration name** field under the **Configuration** tab.



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.
7. The user DN and password correspond with the Rootdn and Rootpw defined in the slapd.conf file.
8. For example, according to the manager information defined in the slapd.conf file:
9. Rootdn "cn=Manager,dc=yealink,dc=com" Rootpw secret
10. Enter **cn=Manager,dc=yealink,dc=com** in the **User DN** field and **secret** in the **Password** field under the **Connection** tab.



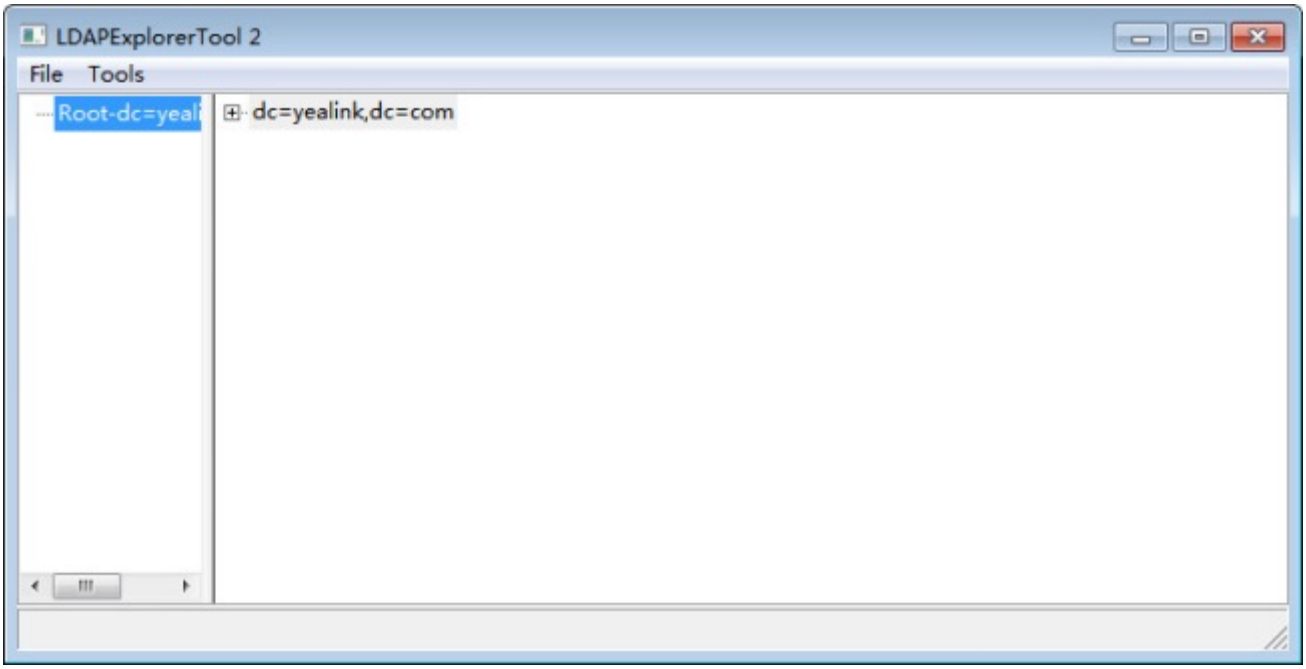
7. Click **Guess value** to fill the **Base DN** automatically.
8. Click **Test connection** to test the connection to the LDAP server. If you encounter an error or warning during the test, you need to resolve the error or warning first according to the prompt, and then retry to test the connection.
9. Click **OK** to accept the change.

Add Entries

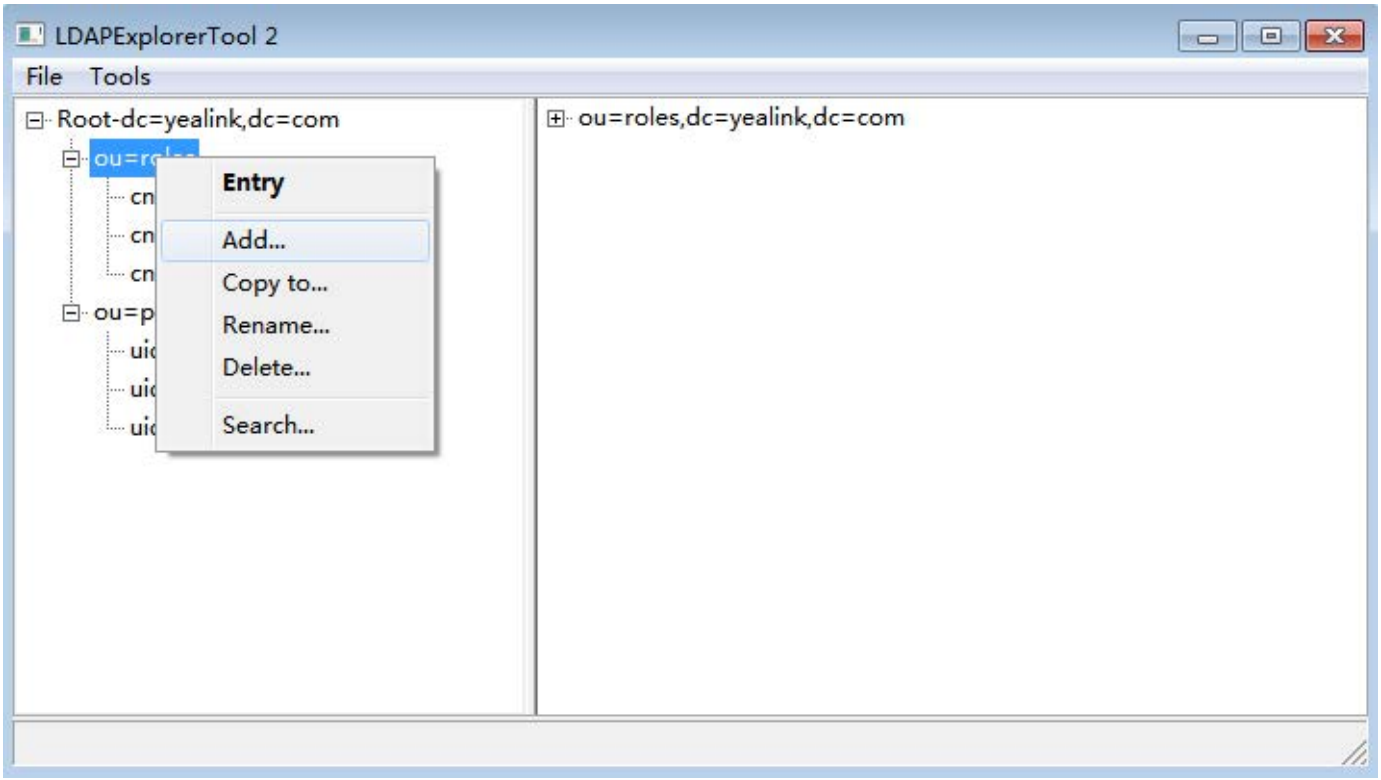
To add entries:

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.

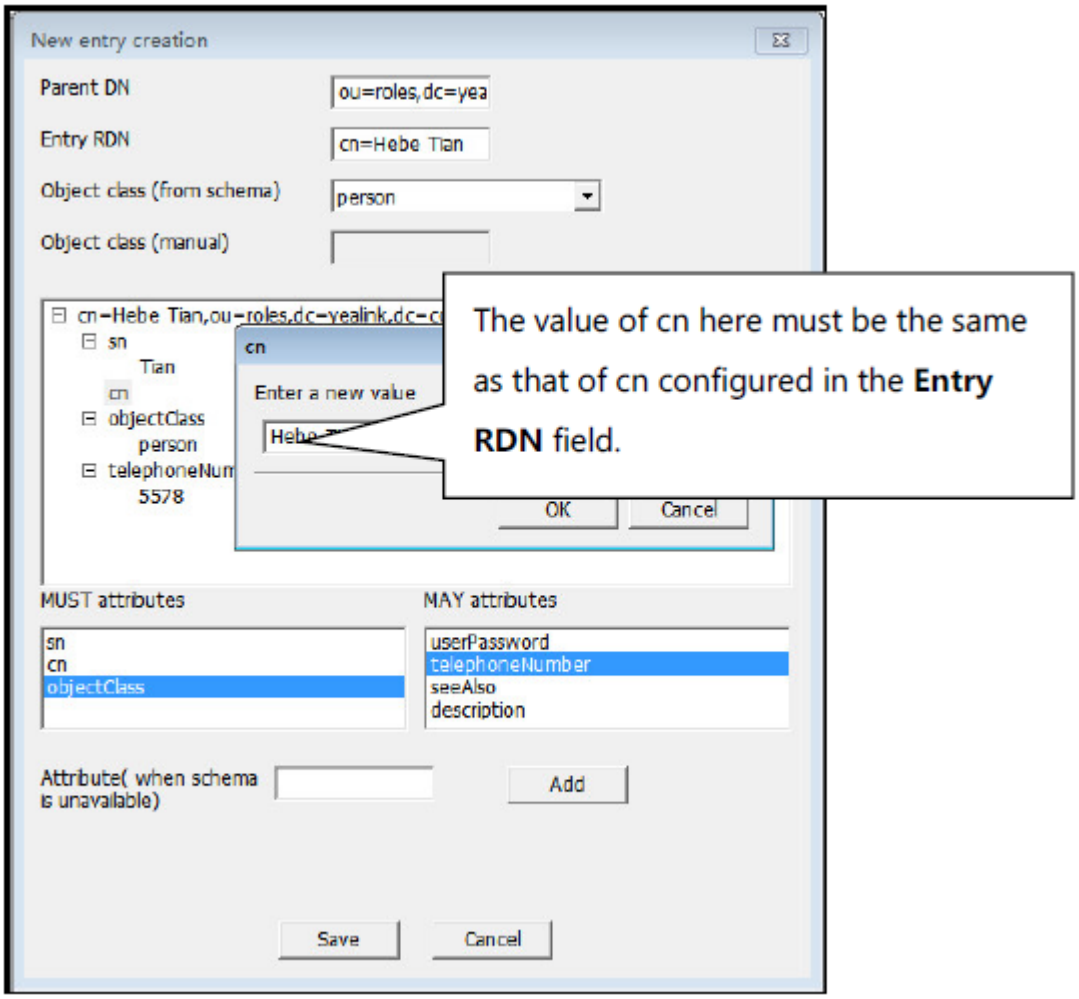


3. Enter the desired values in the corresponding fields.
   - **Parent DN**: It will be automatically generated according to the server configuration.
   - **Entry RDN**: The format is cn=XXX. This is a unique identifier for each entry.
   - **Object Class (from schema)**: Select the structure class to which the entry belongs. Each structure class has its must-have attributes and may have attributes. For example, we select a **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 is also called the 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	A usual department or any sub-entitiy of a larger entity.

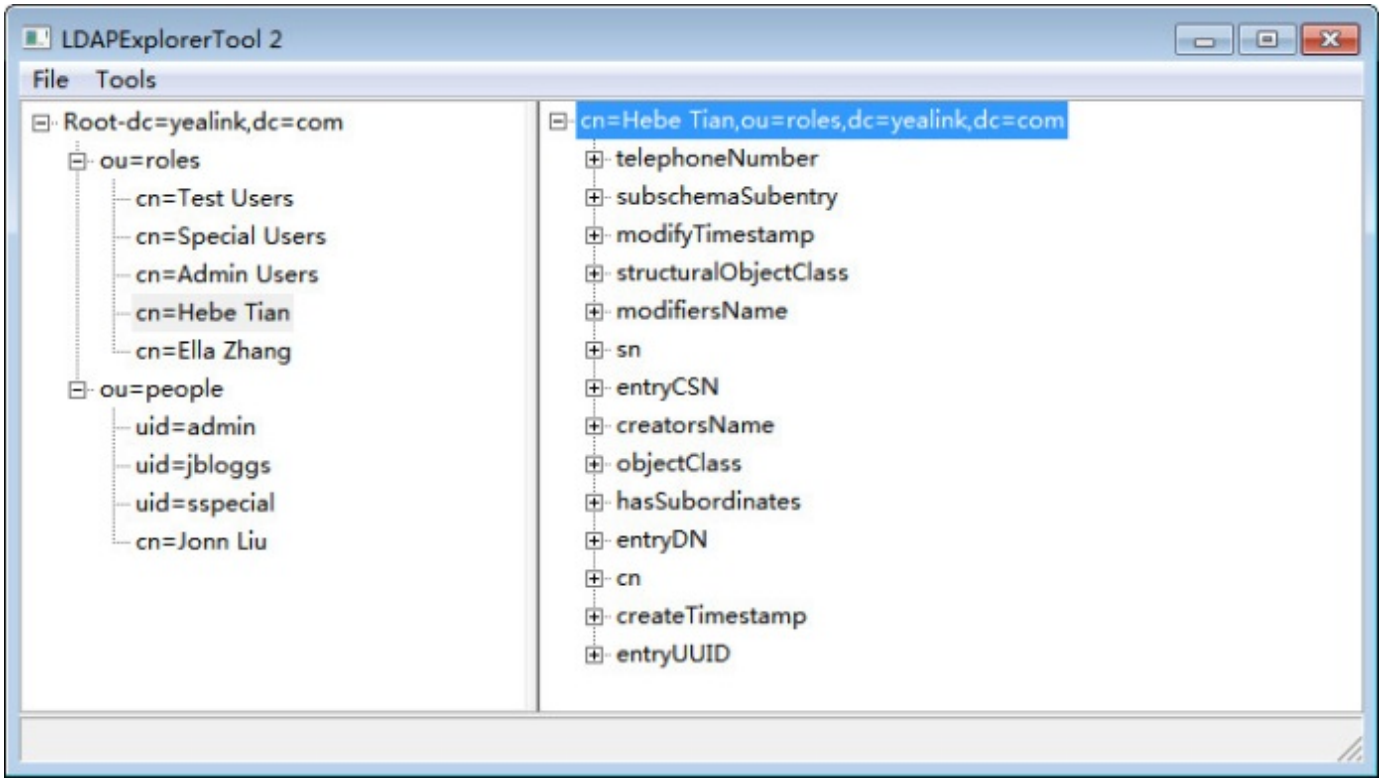
5. Right-click the selected attribute and then select **Add value**.
6. The screenshot of adding a new entry is shown as below:



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

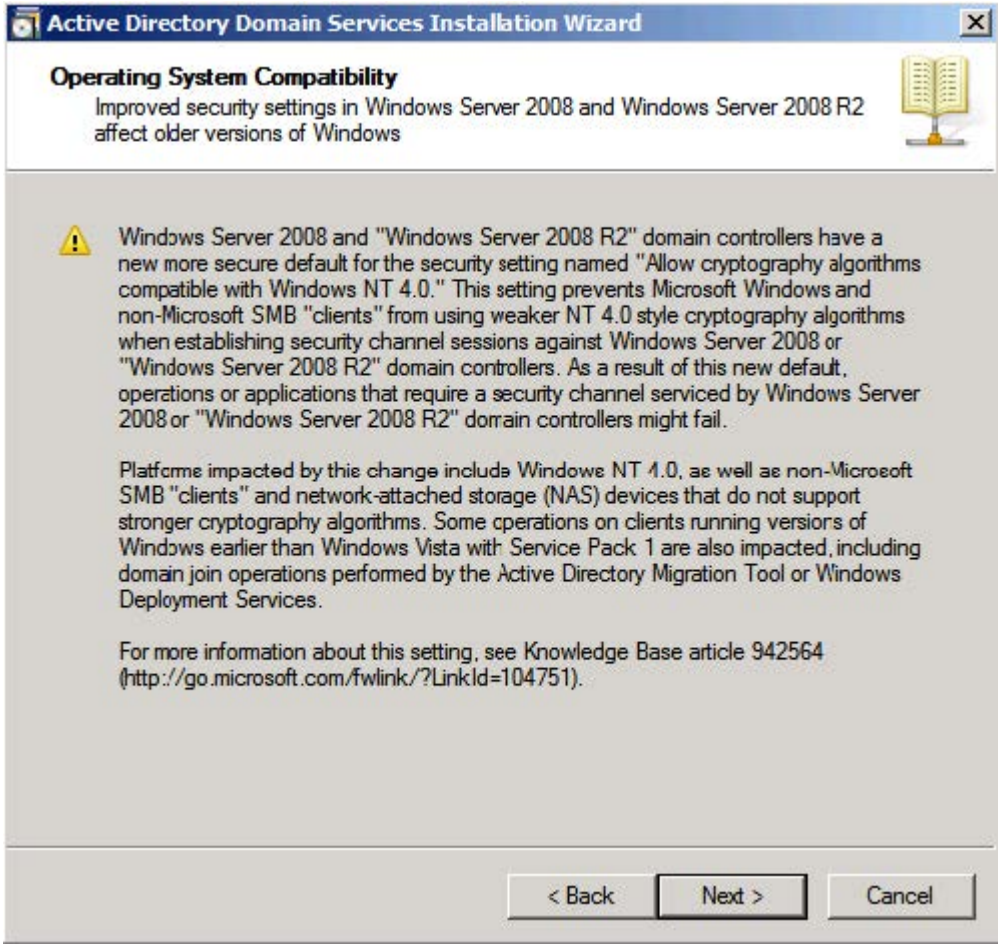
Install the Microsoft Active Directory Domain Services

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

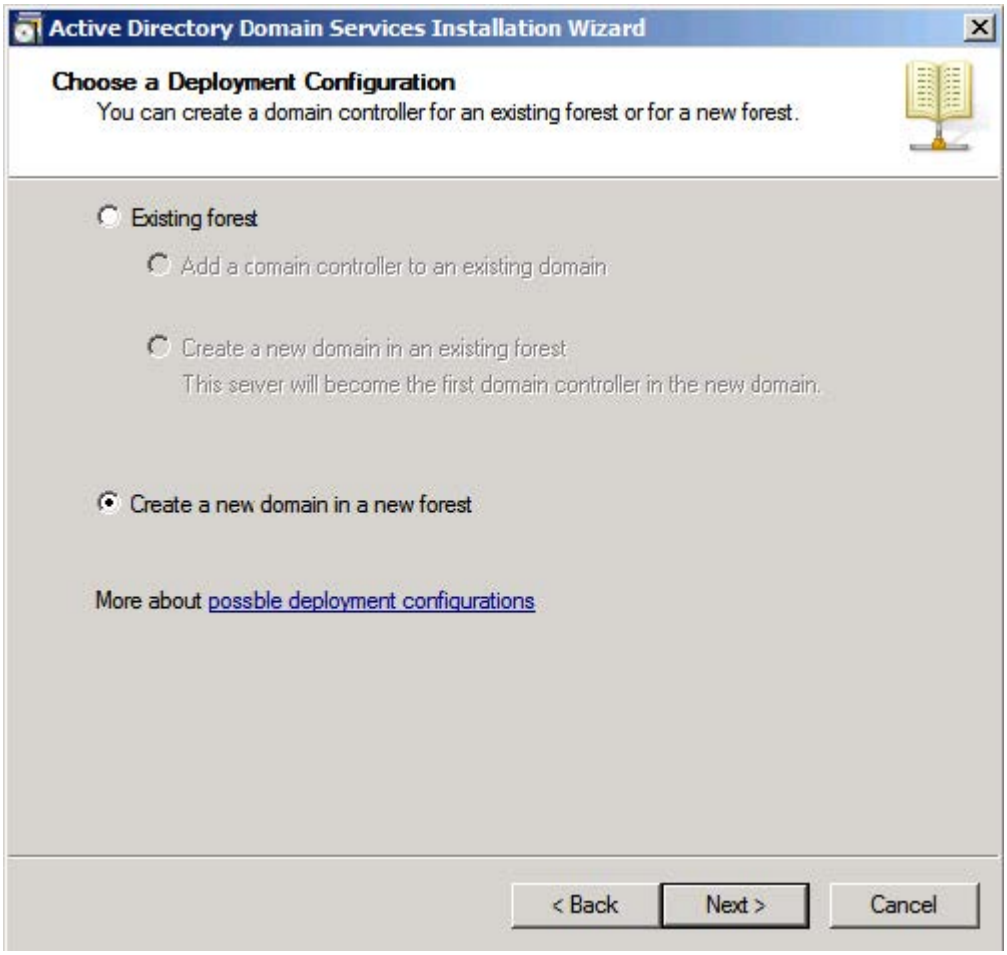
To install the Microsoft Active Directory Domain Services:

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**.

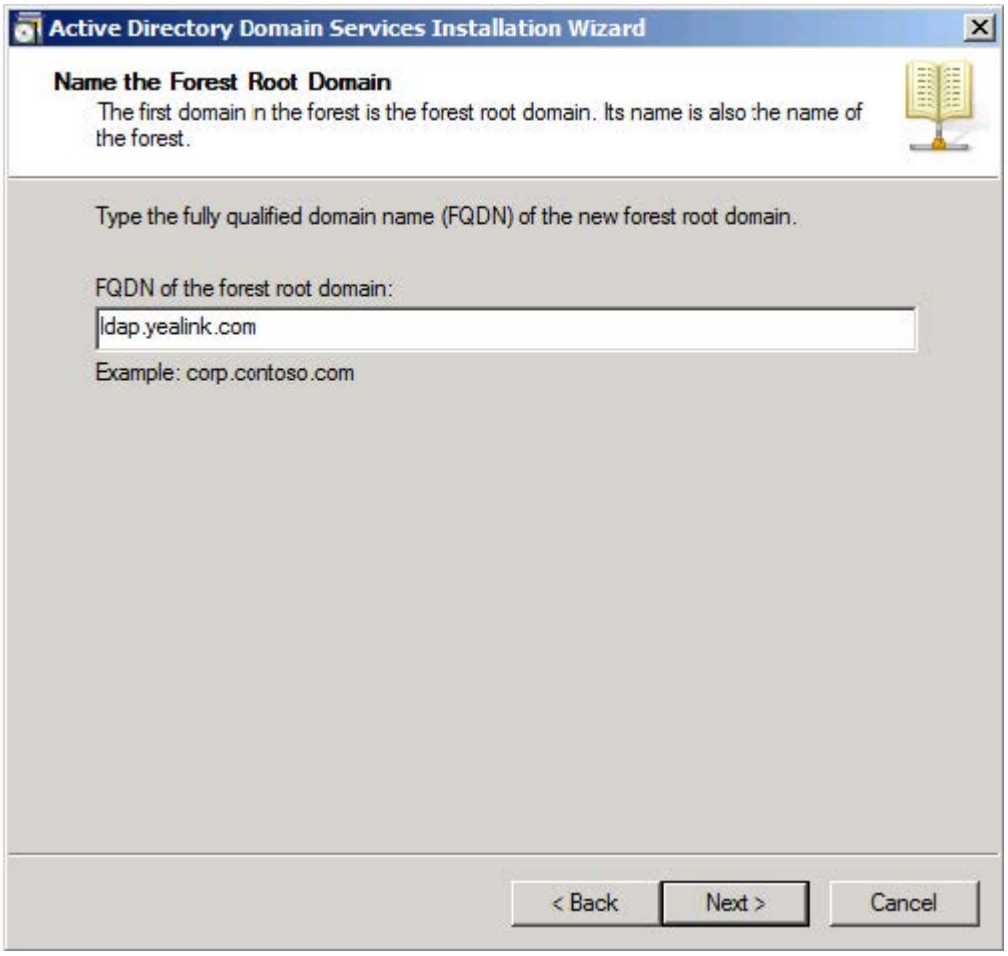
4. Read the provided information and click **Next**.



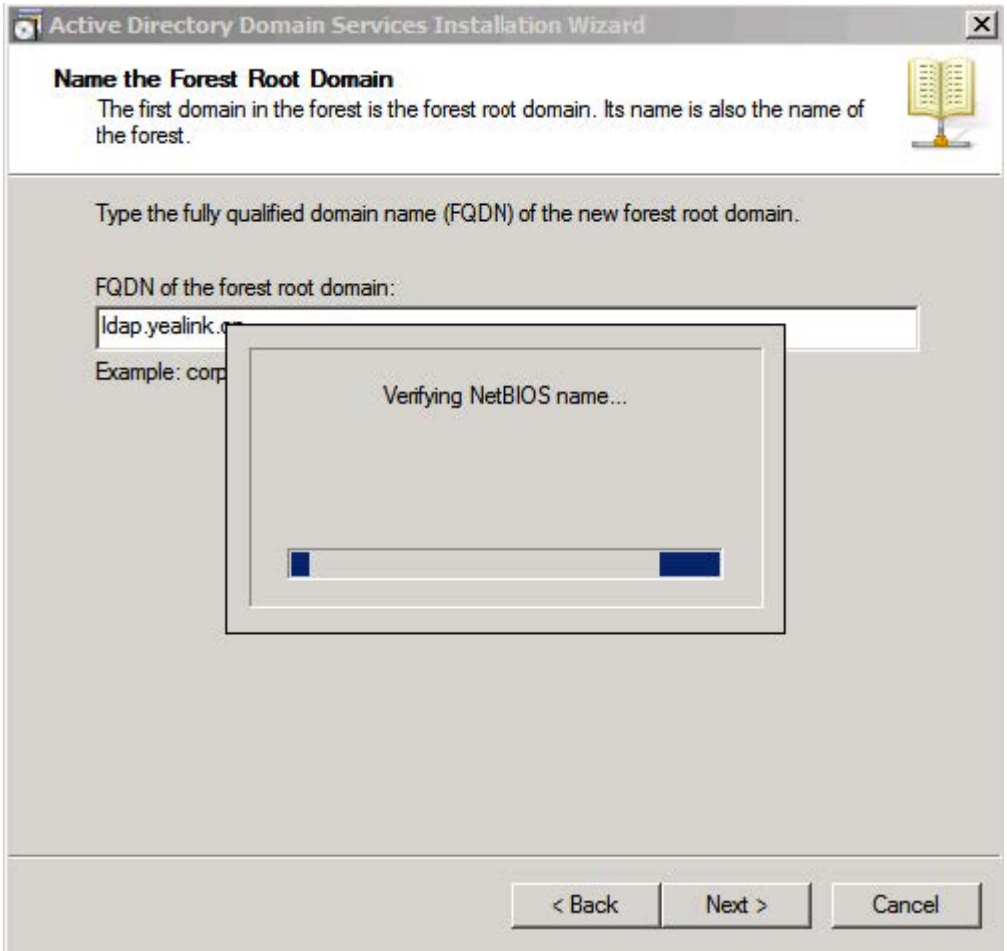
5. Select the **Create a new domain in a new forest** check box and click **Next**.



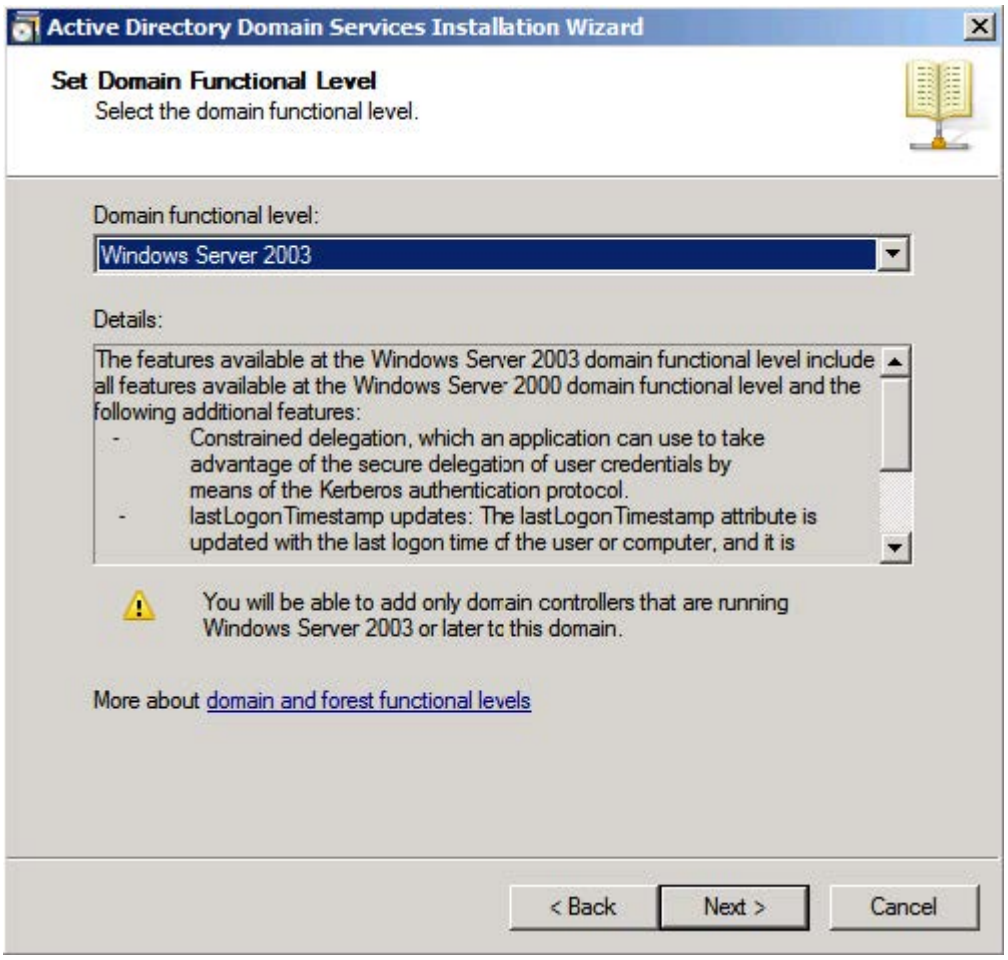
6. Enter an appropriate domain name for the forest root domain and click **Next**.



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

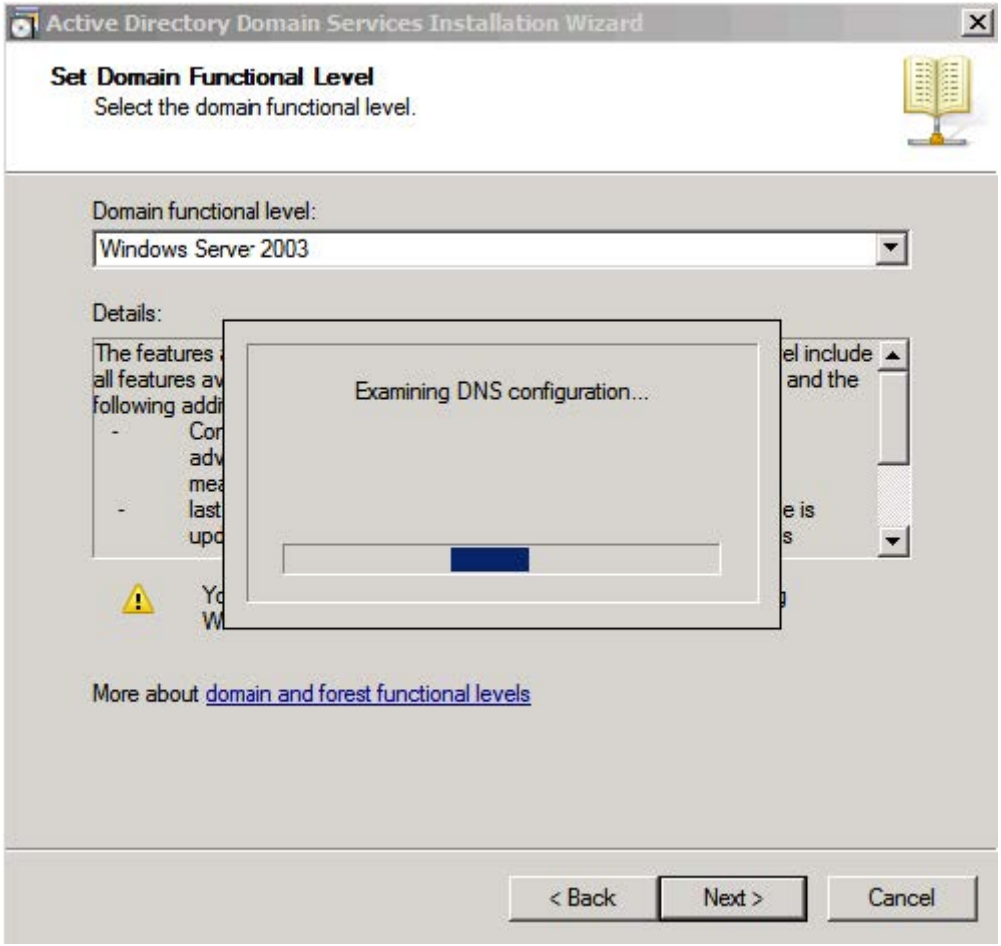


7. Select the desired forest functional level from the **Forest functional level** drop-down menu, and click **Next**.
   For more information, click **domain and forest functional levels**.
8. Select the desired domain functional level from the **Domain functional level** drop-down menu, and click **Next**.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

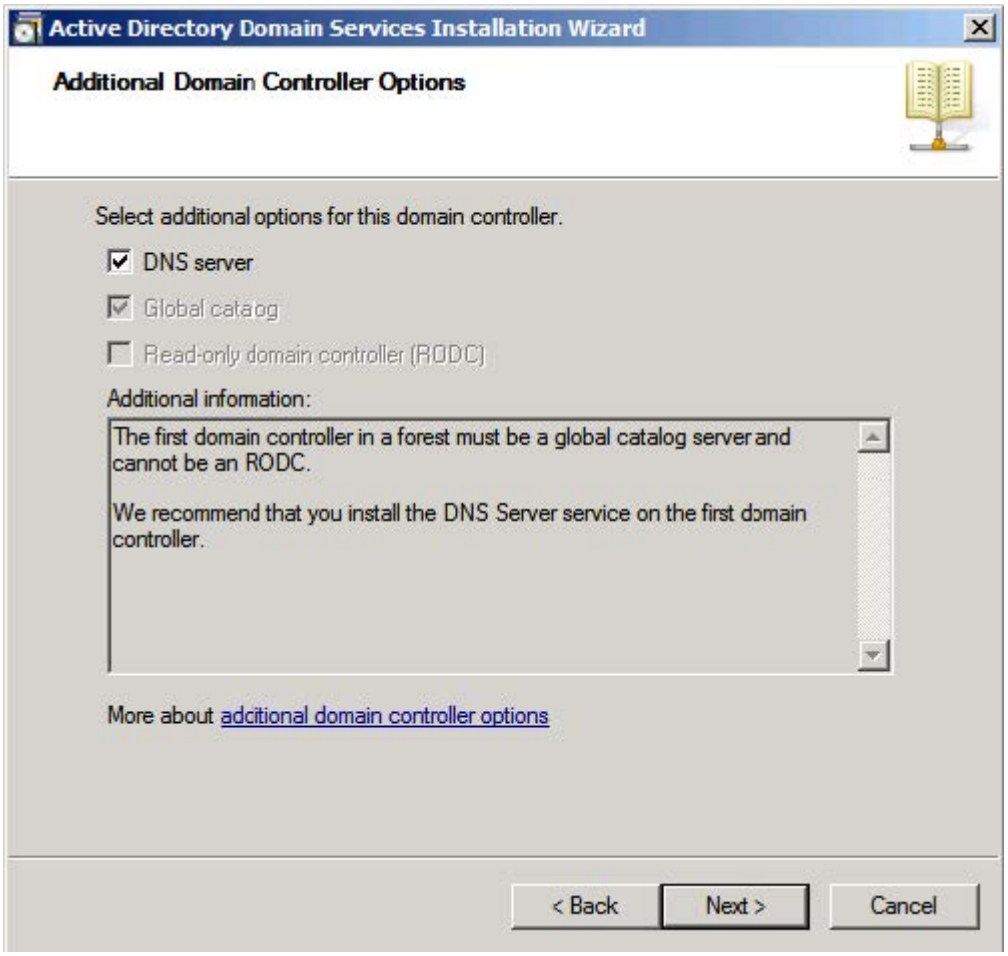


> If you select **Windows Server 2008 R2** for the forest functional level, you will not be prompted to select a domain functional level.

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

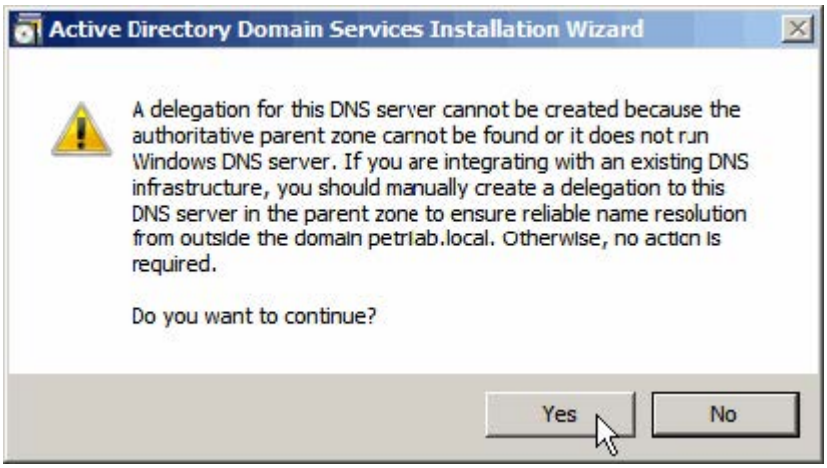


9. Select additional options for this domain controller if required, and click **Next**.

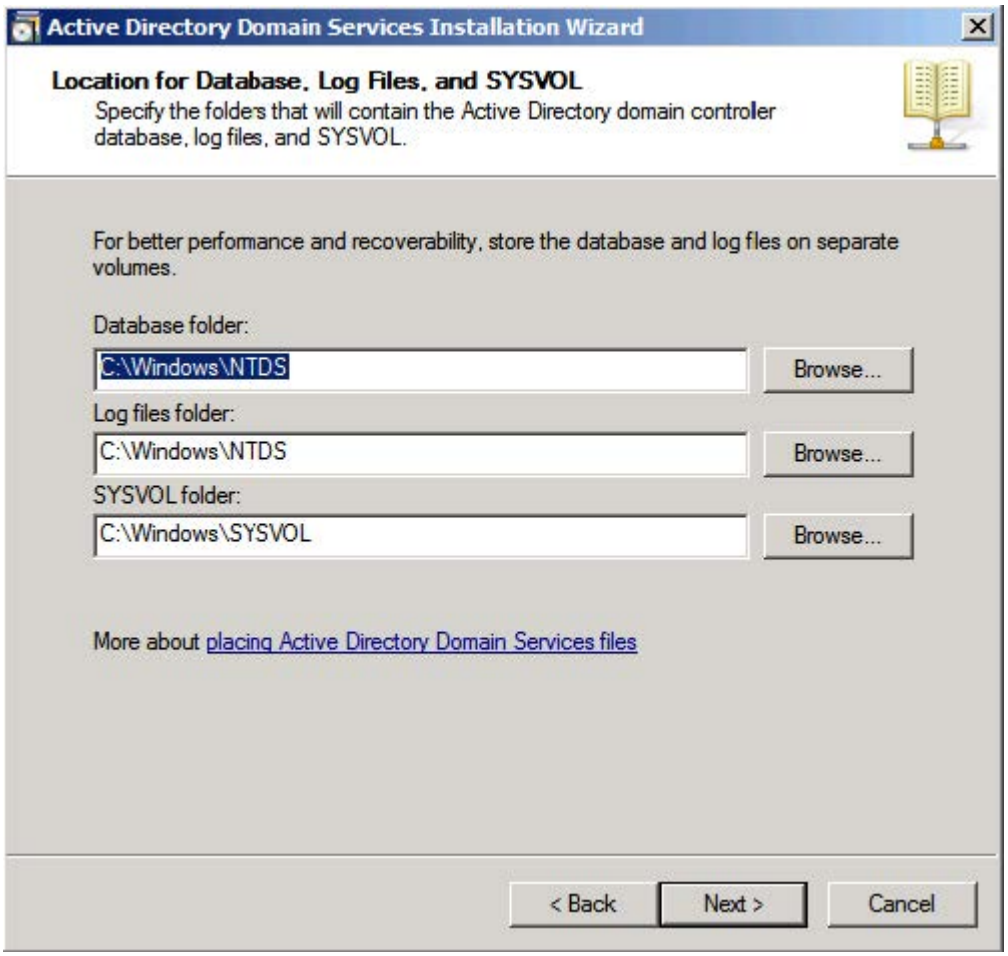


> You may get a warning telling you that the server has one or more dynamic IP addresses. We recommend assigning a static IP address to the server.

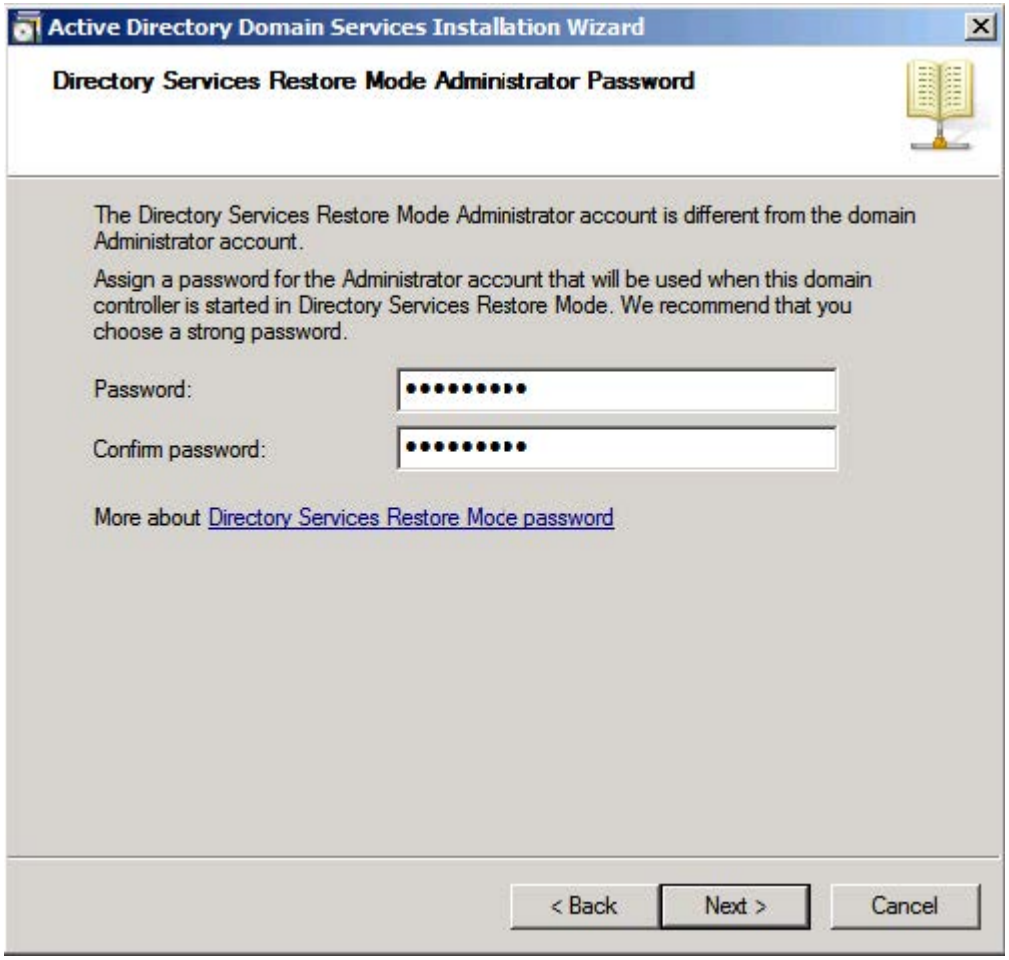
10. The wizard will prompt a warning about DNS delegation. Since no DNS has been configured yet, you can ignore the message and click **Yes**.



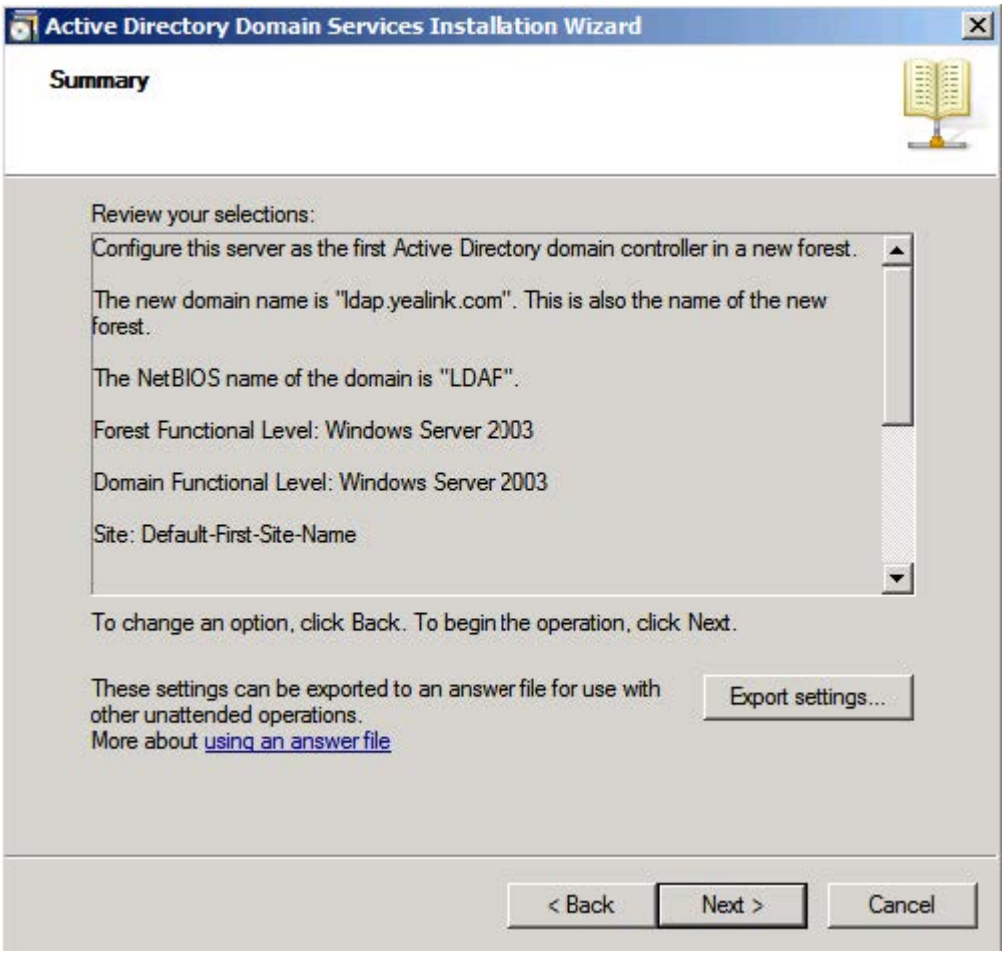
11. Specify the desired paths for the database, log files, and SYSVOL folders, and click **Next**.
12. For more information, click **placing Active Directory Domain Services files**.



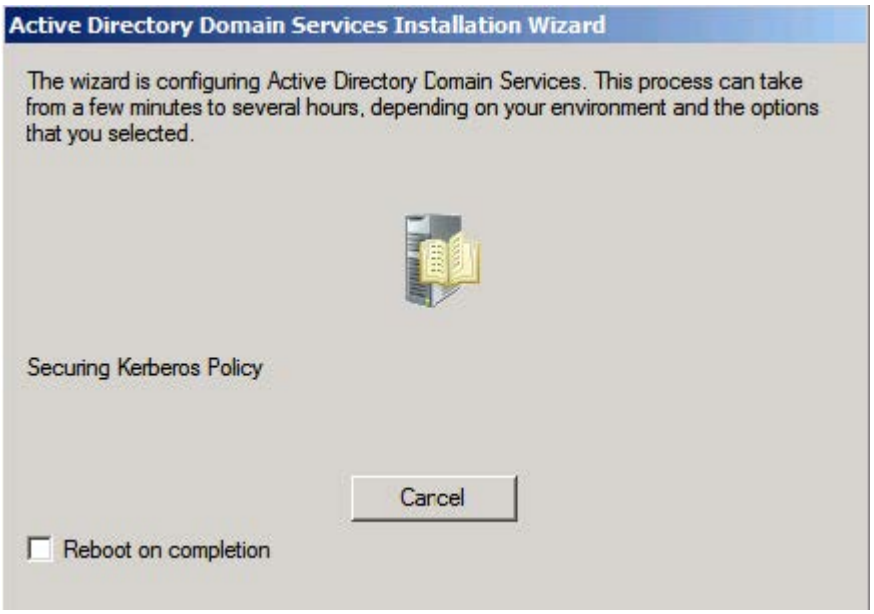
12. Configure the password for the Active Directory recovery mode, and click **Next**.
    For more information, click **Directory Services Restore Mode password**.
    The password should be complex and at least 7 characters long.



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



15. 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

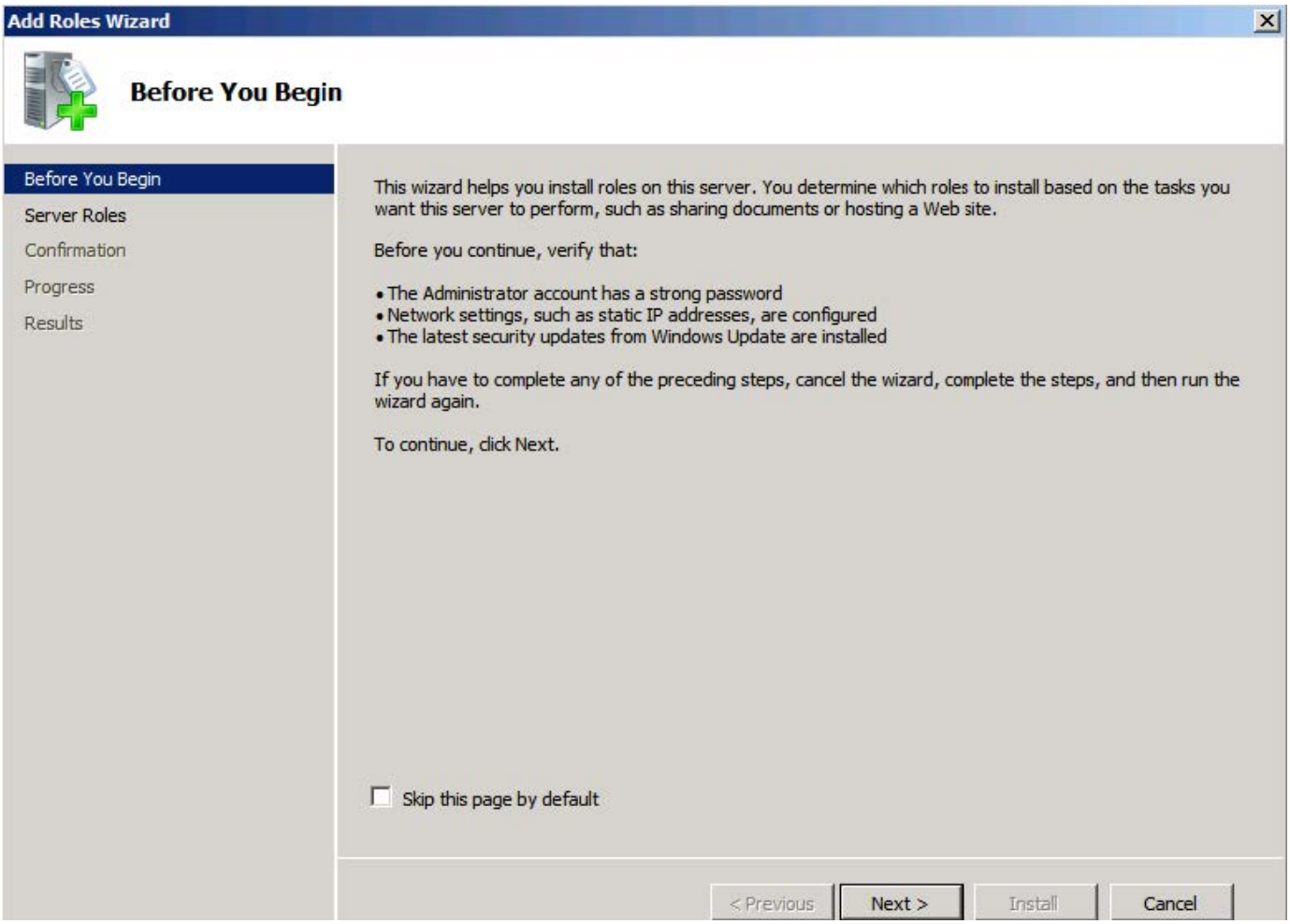
You should also install the Active Directory Lightweight Directory Services role on the Windows Server 2008 system.

To install the Active Directory Lightweight Directory Services role:

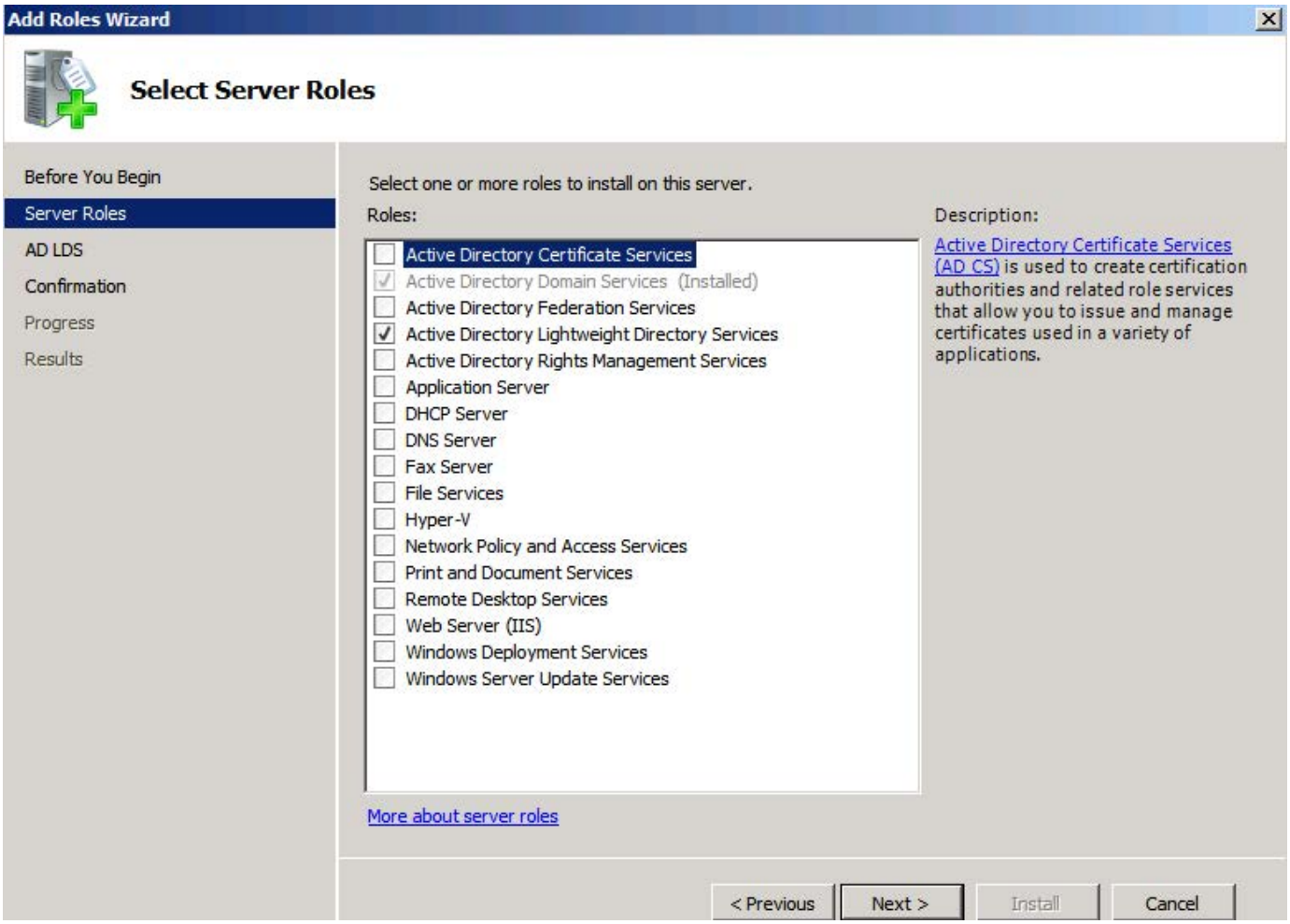
1. Click **Start** > **Administrative Tools** > **Server Manager**.

2. Right-click **Roles**, and then select **Add Roles**.

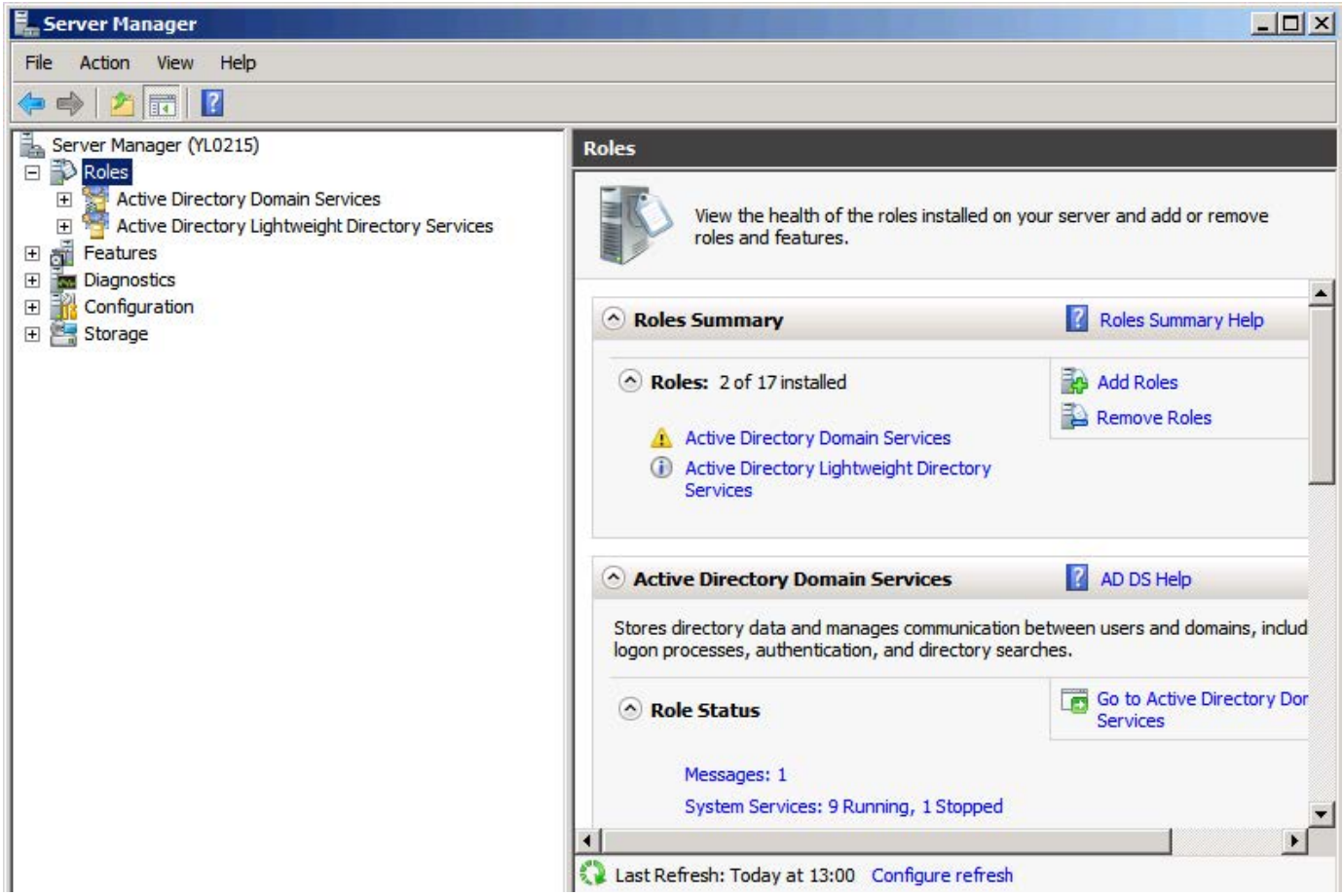
3. The Add Roles Wizard will pop up, click **Next**.



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



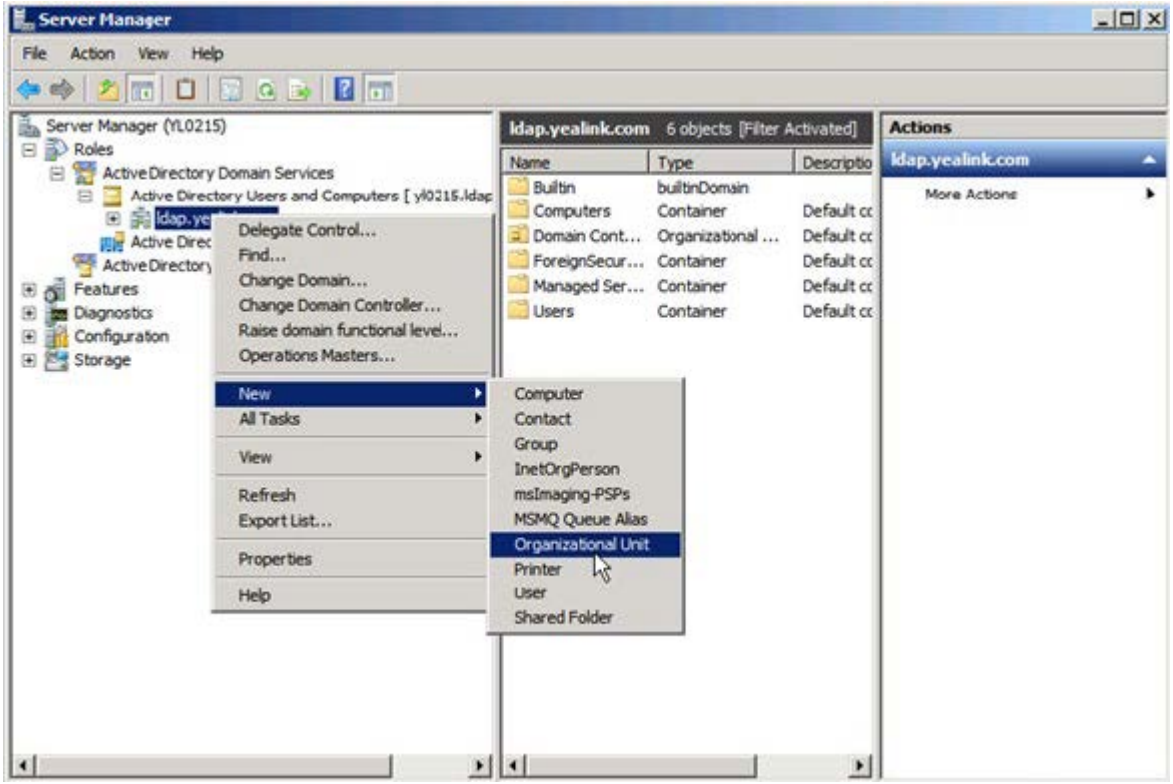
Configure the Microsoft Active Directory Server

Add an Entry to the Active Directory

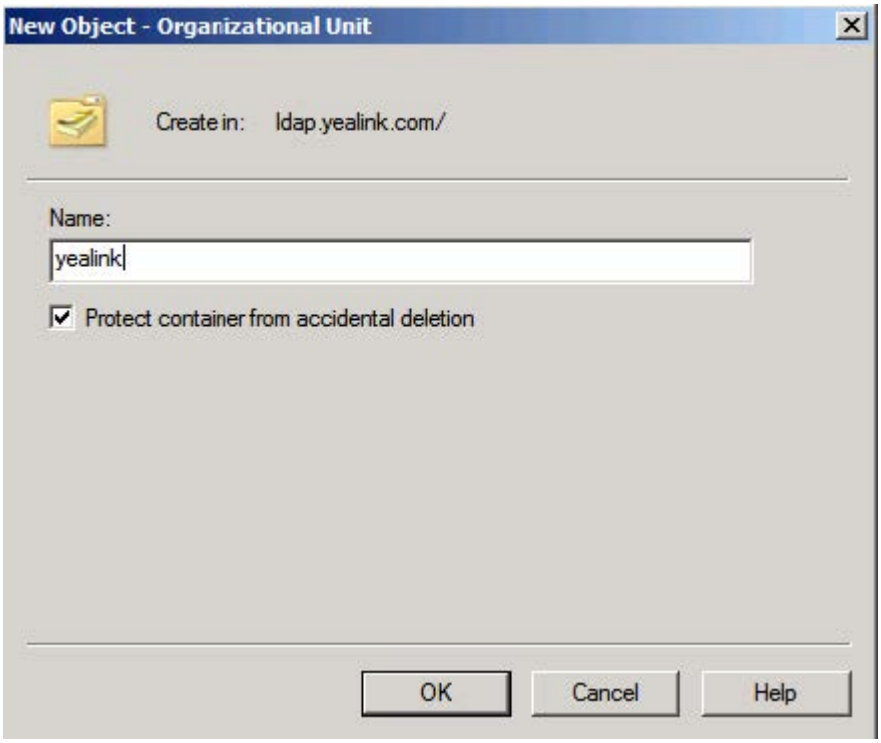
You can add entries to the active directory one by one in this way.

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**.

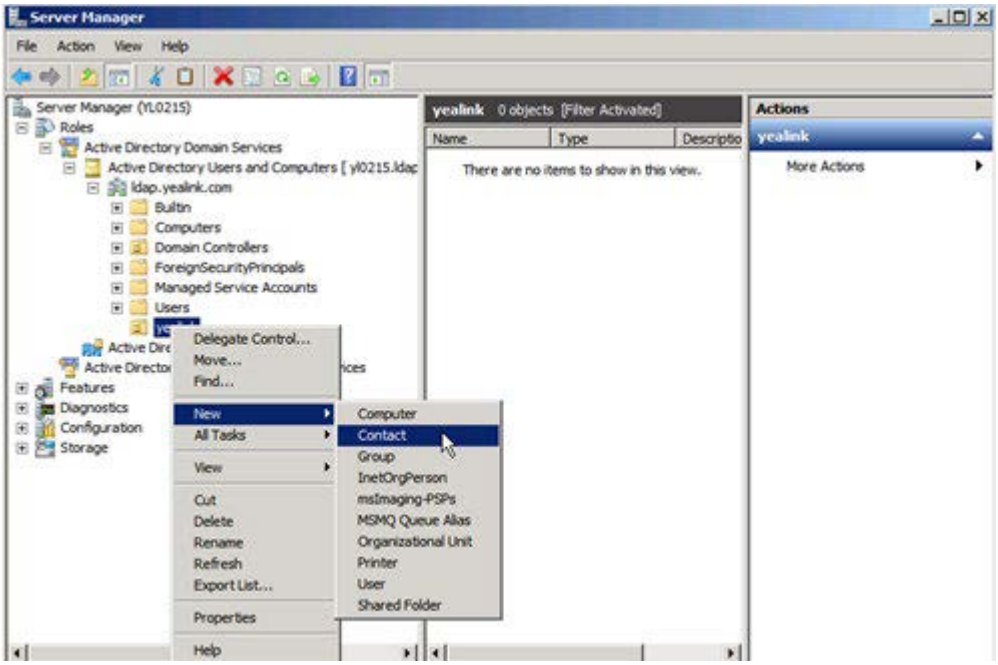


4. Enter the desired name of the organizational unit.

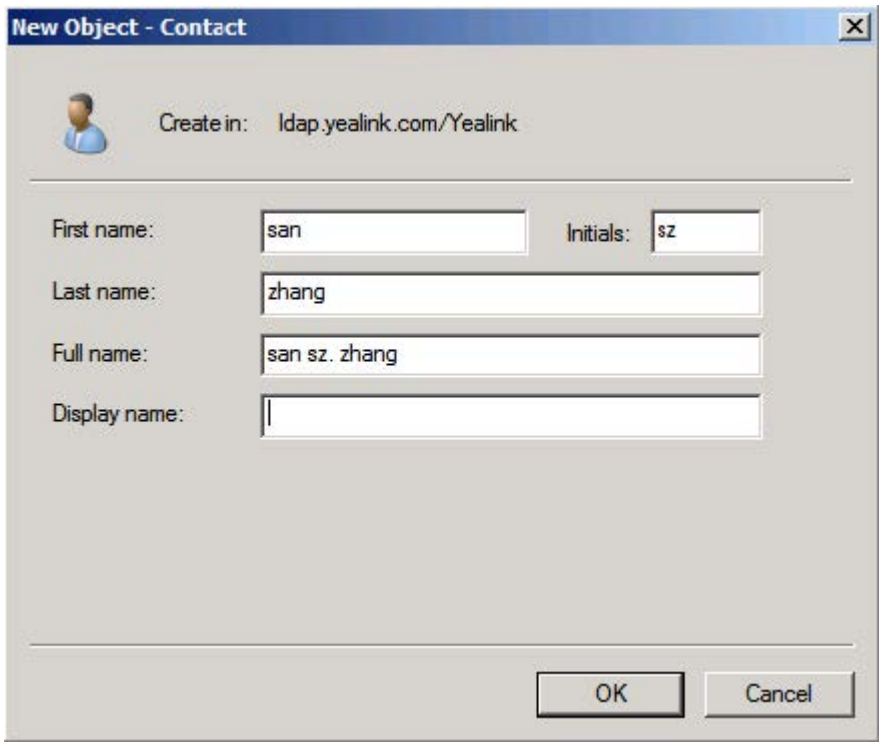


5. Click **OK** to accept the change.

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



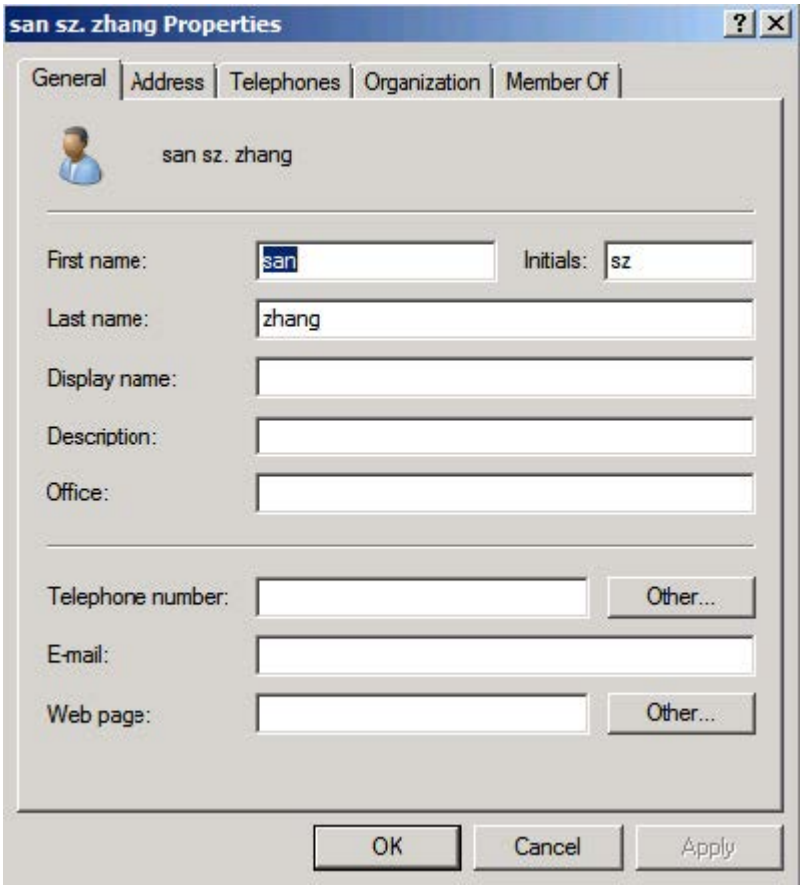
7. Enter the desired values in the corresponding fields.



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:

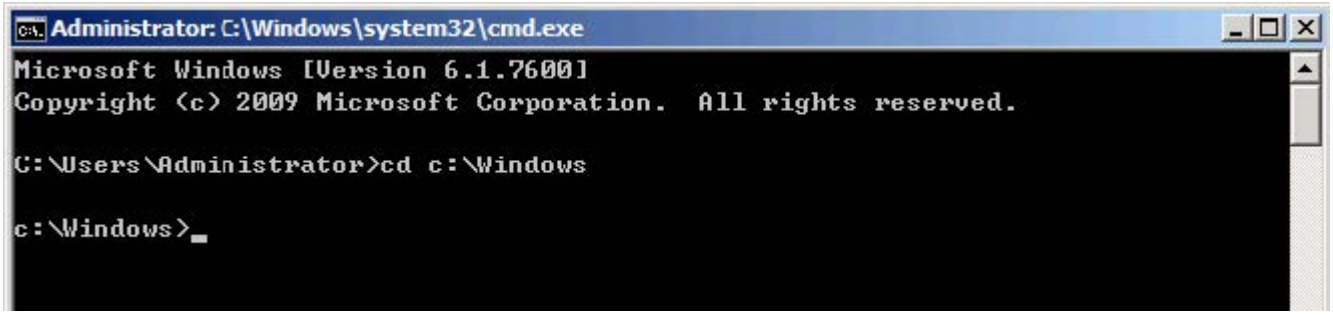
Create a new text document and then modify the filename extension to ldif. For example, create a text document named test.txt, right-click the test.txt document and then select to rename it, modify the filename extension to ldif. Open the LDIF file with your favorite text editor and input the corresponding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

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>cd c:\Windows

c:\Windows>ldifde  -i  -f  test.ldif
Connecting to "yl0215.ldap.yealink.com"
Logging in as current user using SSPI
Importing directory from file "test.ldif"
Loading entries...
2 entries modified successfully.

The command has completed successfully

c:\Windows>
```

6. 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 *

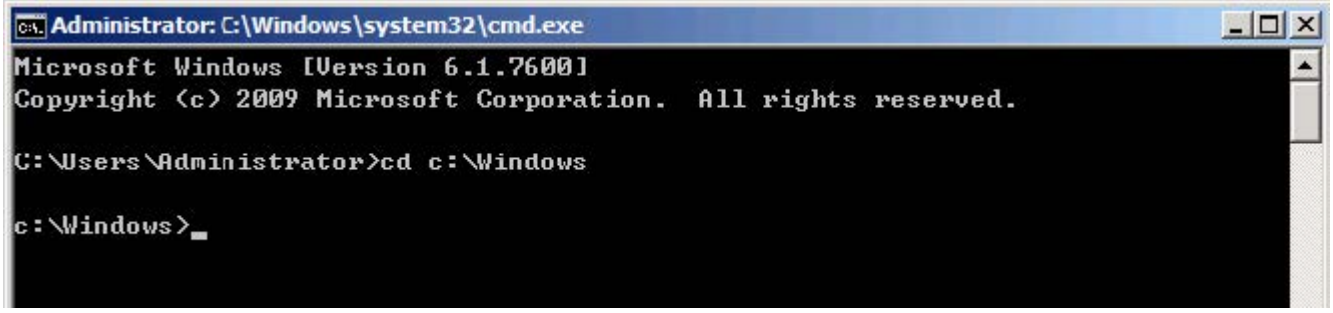
	A	B	C	D	E	F	G	H	I	J
1	DN	objectClass	ou	name	cn	sn	givenName	initials	ipPhone	mobile
2	OU=yealink,DC=ldap,DC=yealink,DC=com	organizationalUnit	yealink	yealink						
3	CN=san zhang,OU=yealink,DC=ldap,DC=yealink,DC=com	contact		san zhang	san zhang	san	zhang	sz	1111	123456789001
4	CN=si li,OU=yealink,DC=ldap,DC=yealink,DC=co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

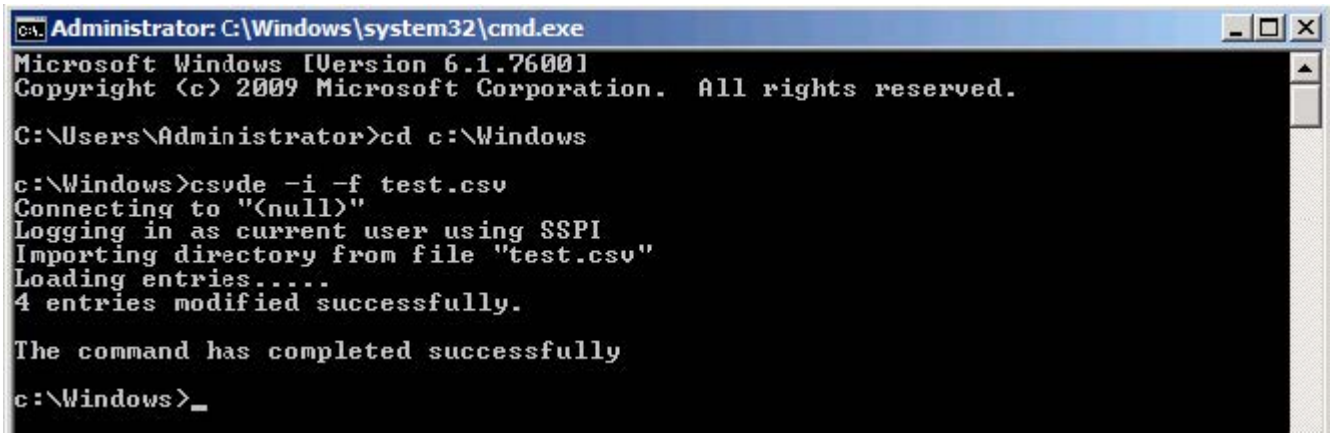
3. Execute the command cd to access the path of the test.csv file. For example, execute **cd c:\Windows** to access the path of the test.csv file at **c:\Windows**.



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:



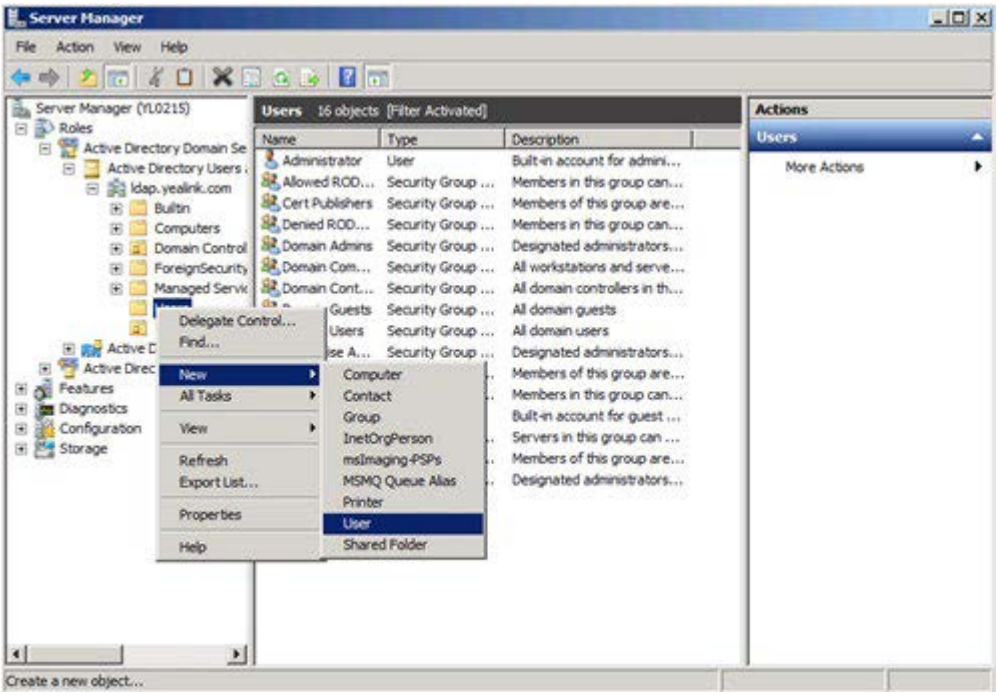
- The csvde tool cannot edit or delete the existing entries on the active directory.
- You can also export the existing entries on the active directory into a *.csv file first, modify the file, and then import the modified file into the active directory. For more information, refer to the network resource.

Create User Accounts

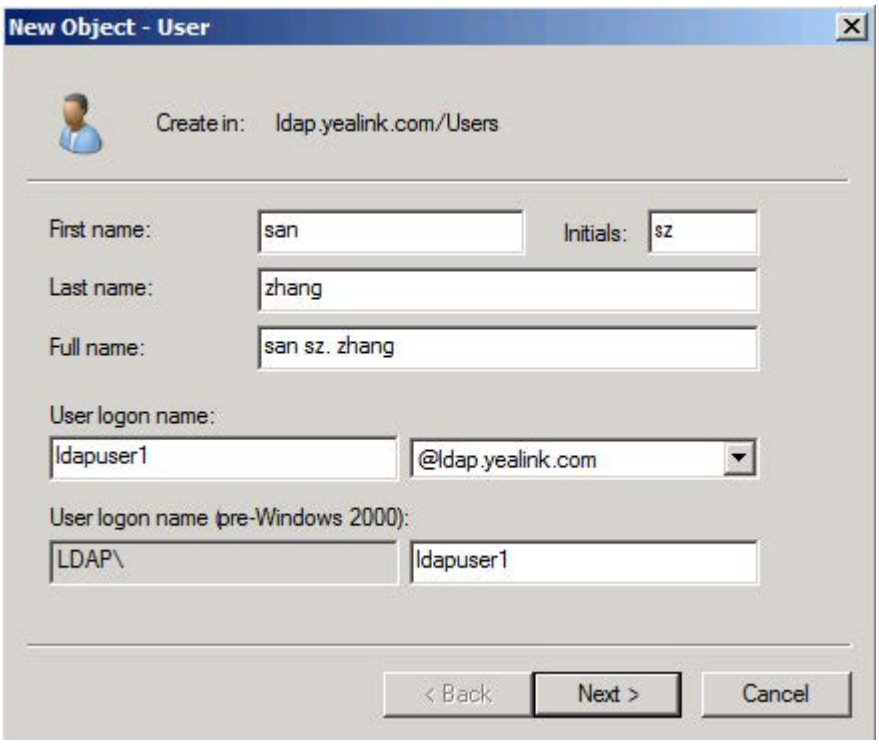
You can create user accounts to allow access to resources on the active directory. User accounts are very important and useful.

To create a user account:

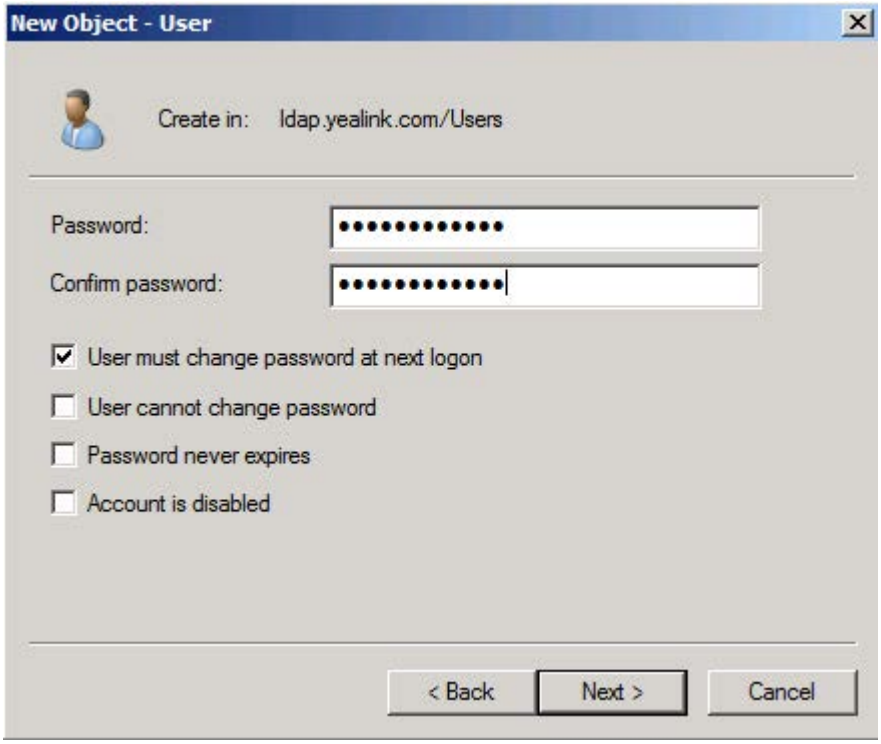
1. Click **Start** > **Administrative Tools** > **Server Manager**.
2. Double click **Server Manager** > **Roles** > **Active Directory Domain Services** > **Active Directory Users and Computers**.
3. Select the domain name created above (e.g., ldap.yealink.com).
4. Right-click **Users**, and then select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



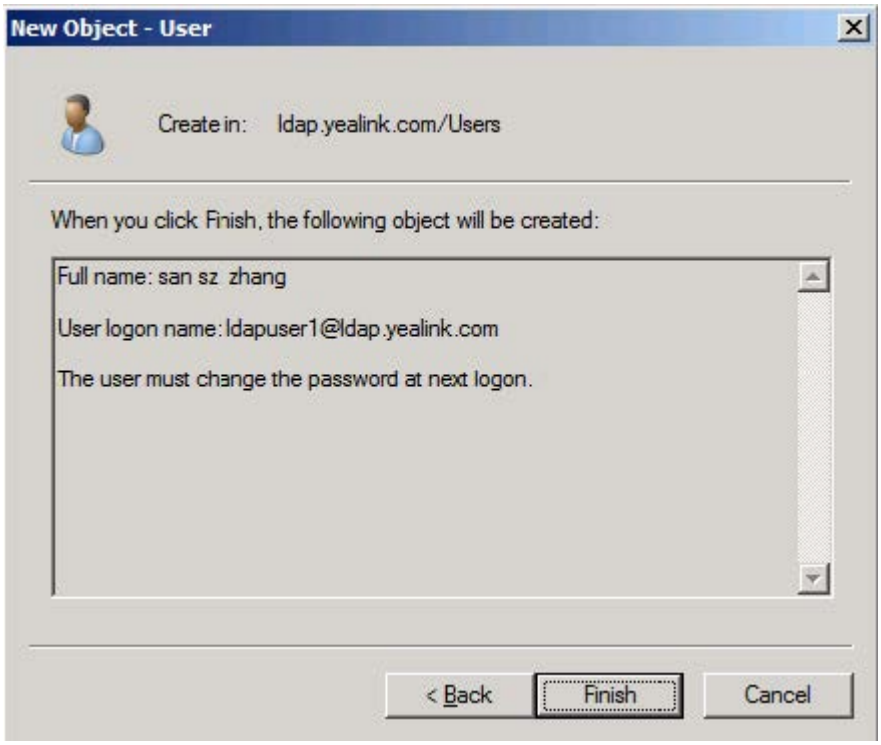
5. Enter desired values in the corresponding fields and click **Next**.



6. Enter the password for the user, select the appropriate options, and click **Next**.
7. 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 a Microsoft Windows Server 2003 SP2 Enterprise 32-bit system. You can download Active Directory Application Mode

(ADAM) online:

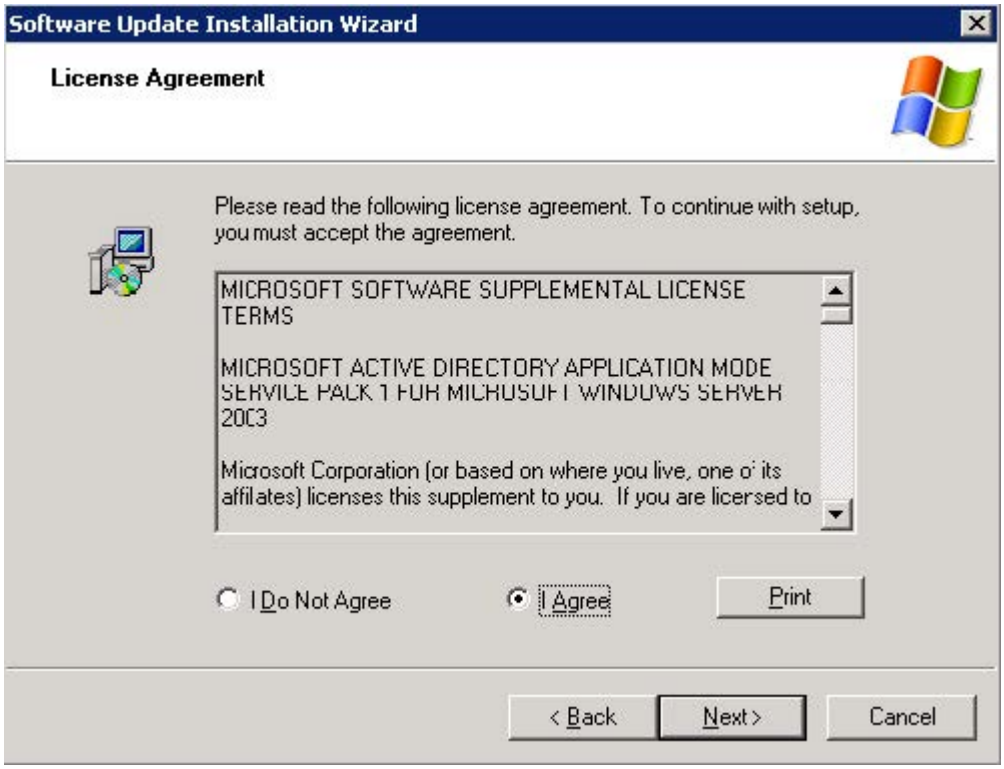
http://www.microsoft.com/en-us/download/confirmation.aspx?id=4201.

Install the Active Directory Application Mode

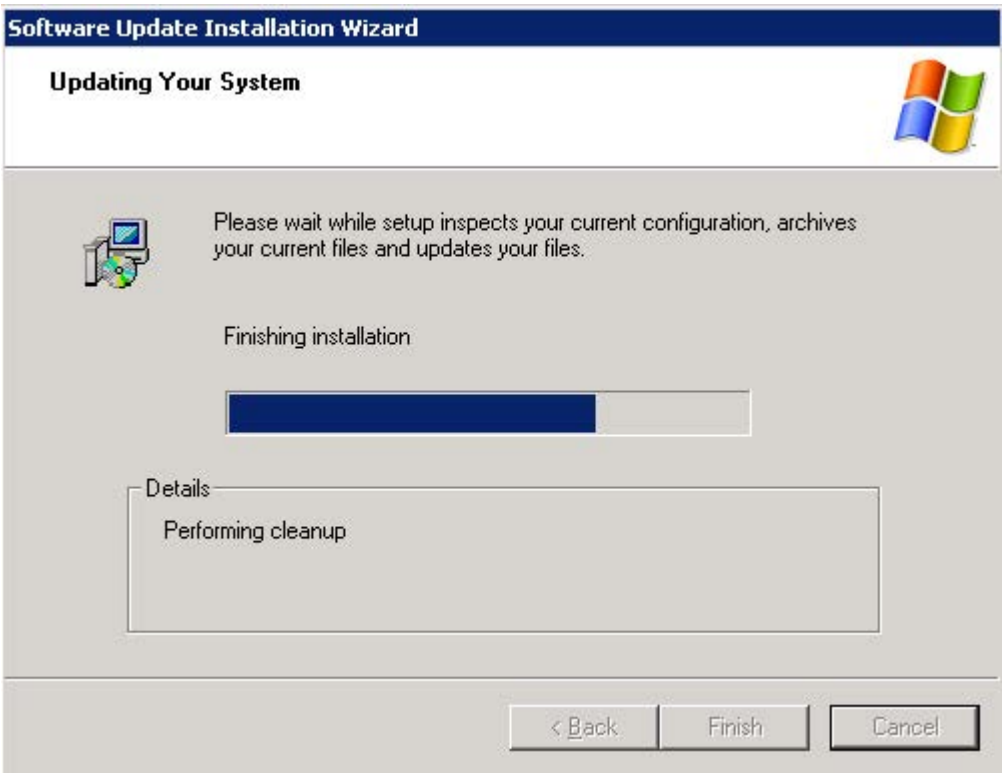
To install the Active Directory Application Mode:

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 the **I Agree** check box. And then click **Next**.



5. The installation progress screen will be shown as below:



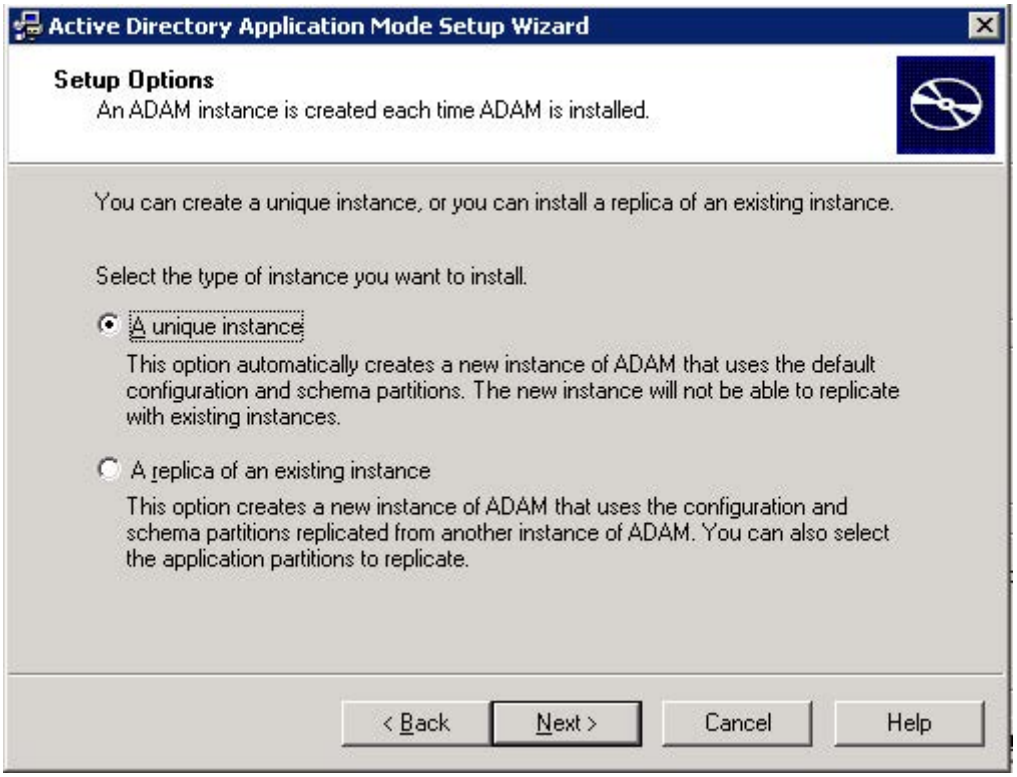
4. Click **Finish** to complete the installation and exit the wizard.

To create an ADAM instance:

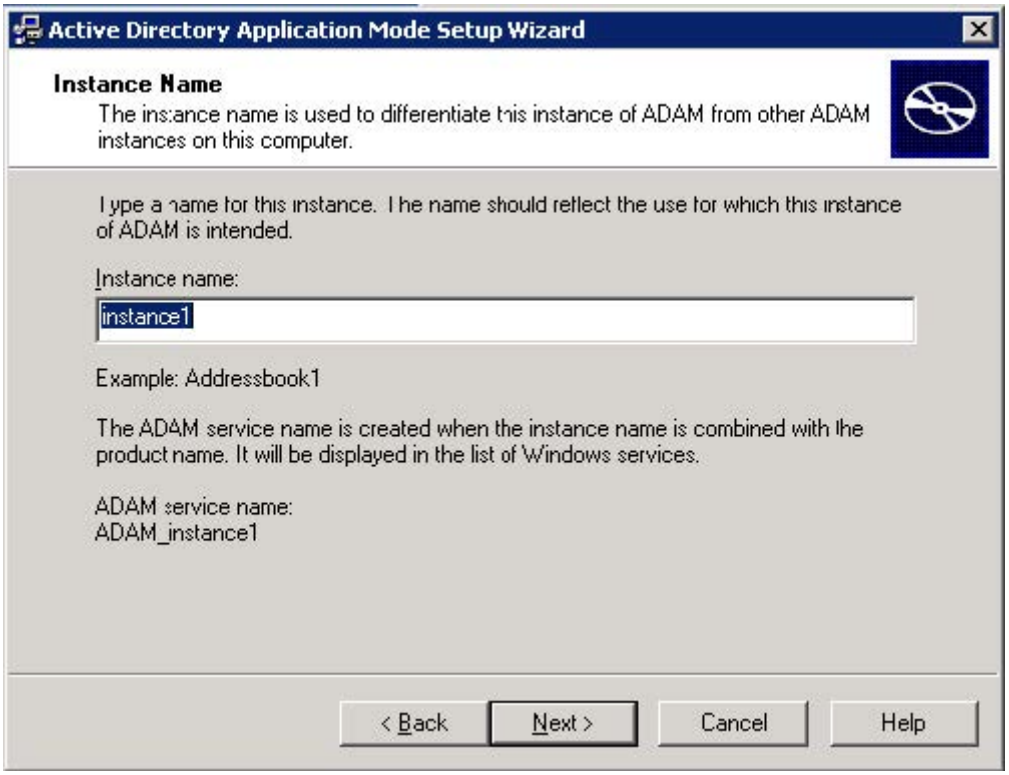
1. Click **Start** > **Programs** > **ADAM** > **Create an ADAM instance**.

   It will prompt the following interface, and click **Next**.

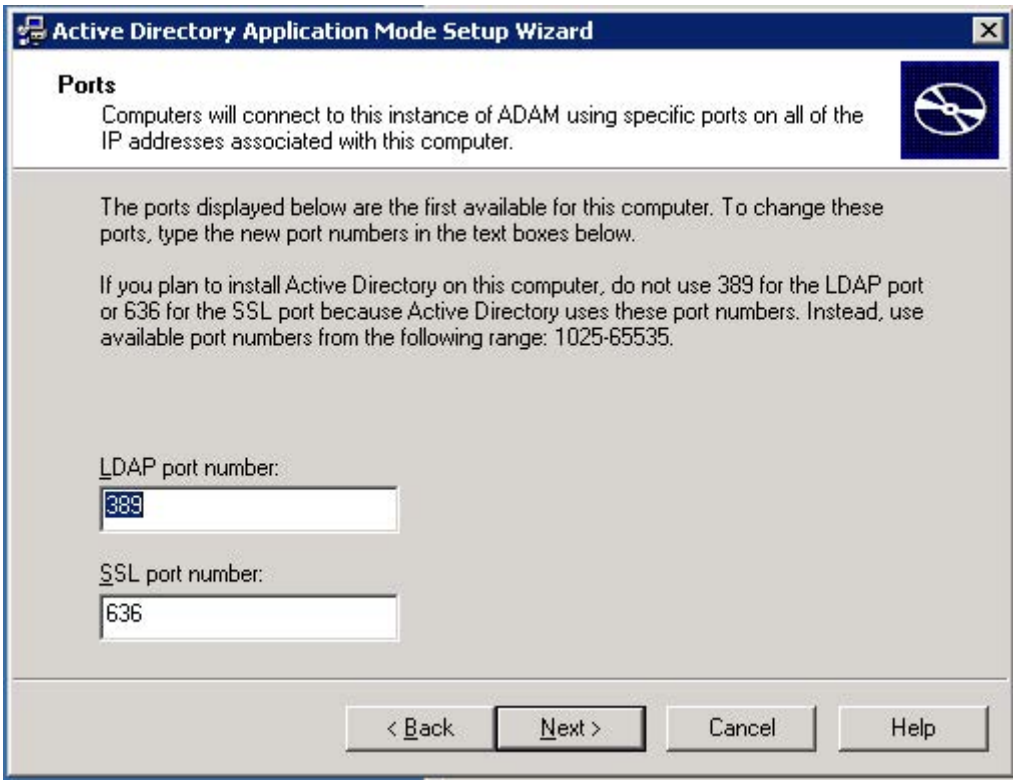
2. Mark the **A unique instance** check box and click **Next**.



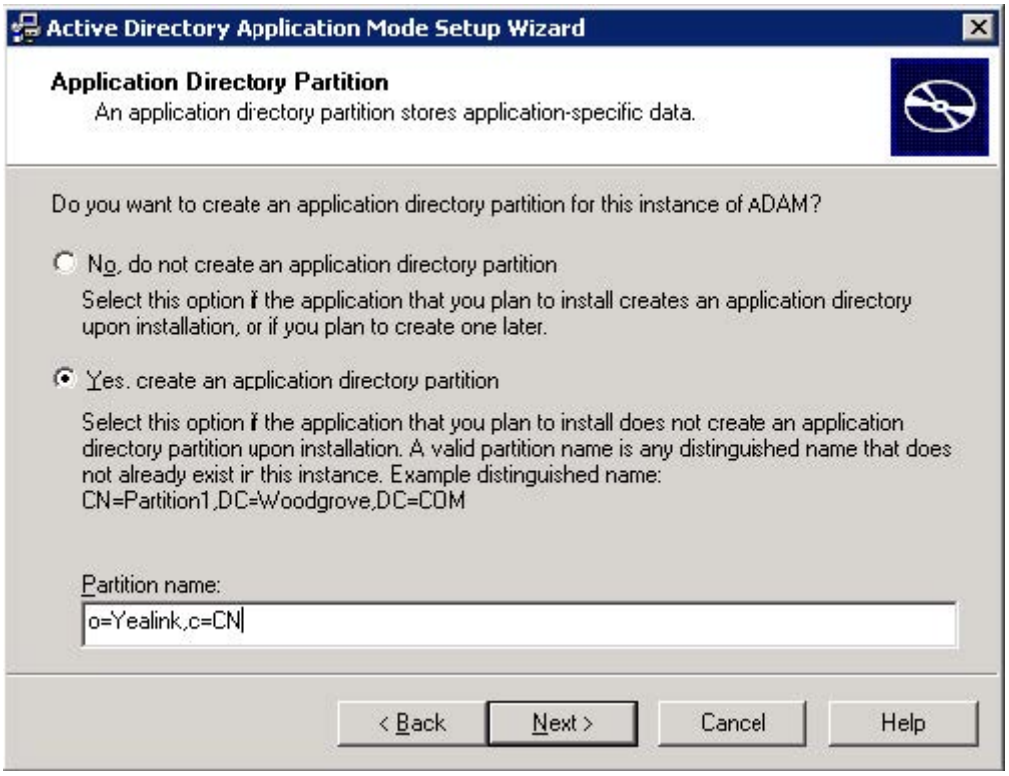
3. Enter the desired name in the **Instance name** field and click **Next**.



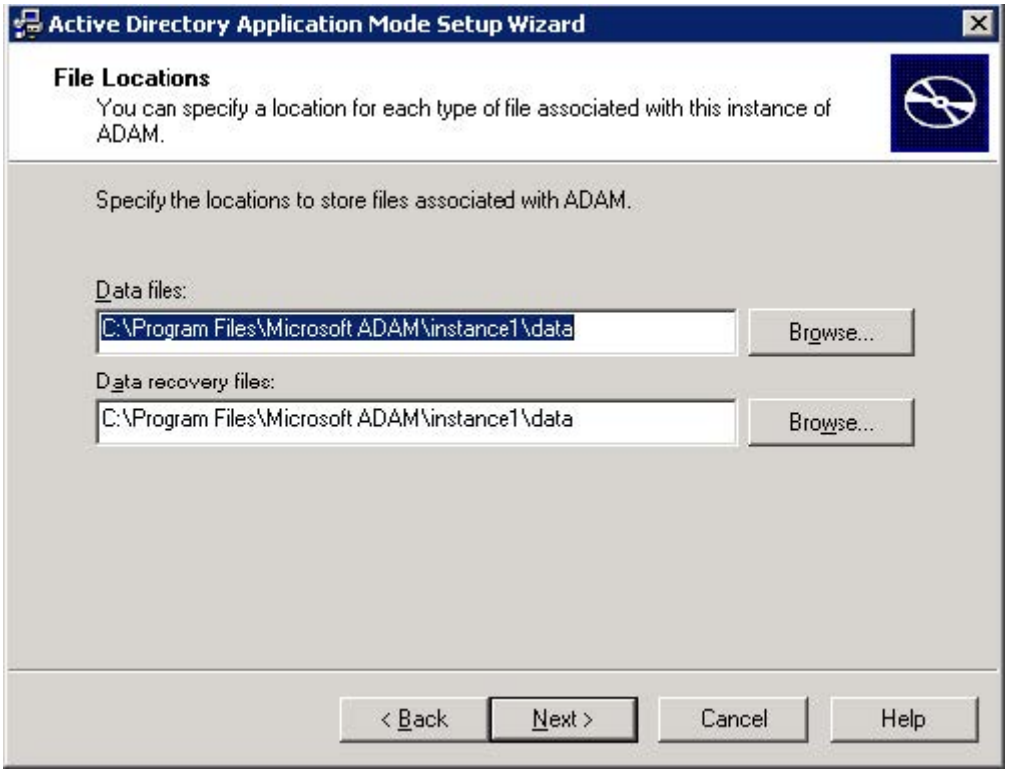
4. Keep the default ports and click **Next**.



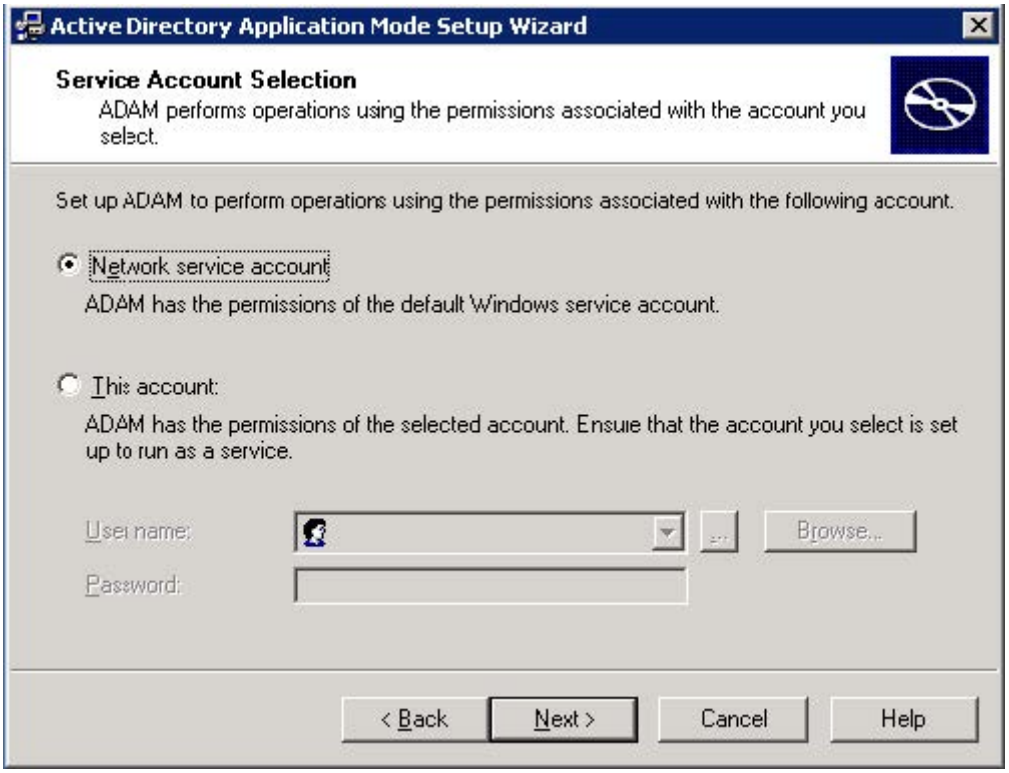
5. Select the **Yes, create an application directory partition** check box and enter the desired name (e.g., o=Yealink,c=CN) in the **Partition name** field, and then click **Next**.



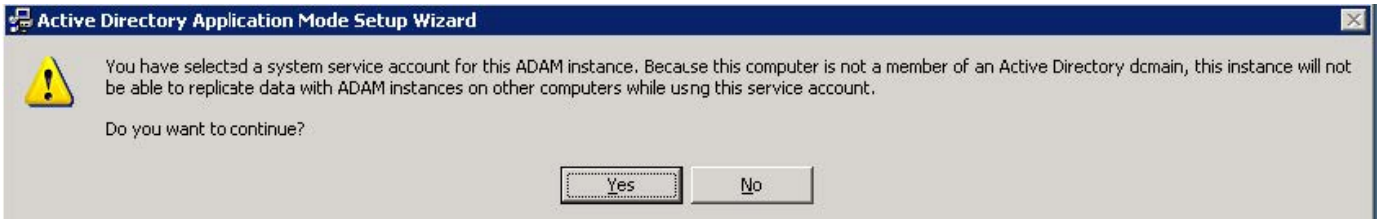
6. Specify the desired paths for the data and data recovery files, and click **Next**.



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

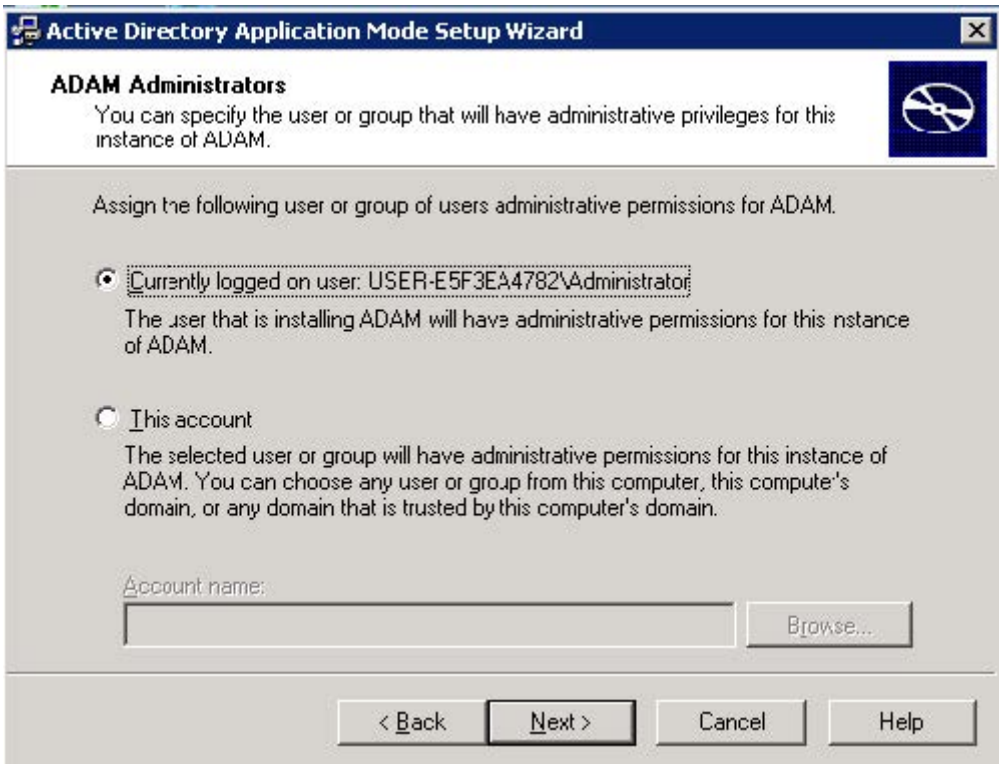


It will pop up the following prompt box. Read the provided information and click **Yes**.



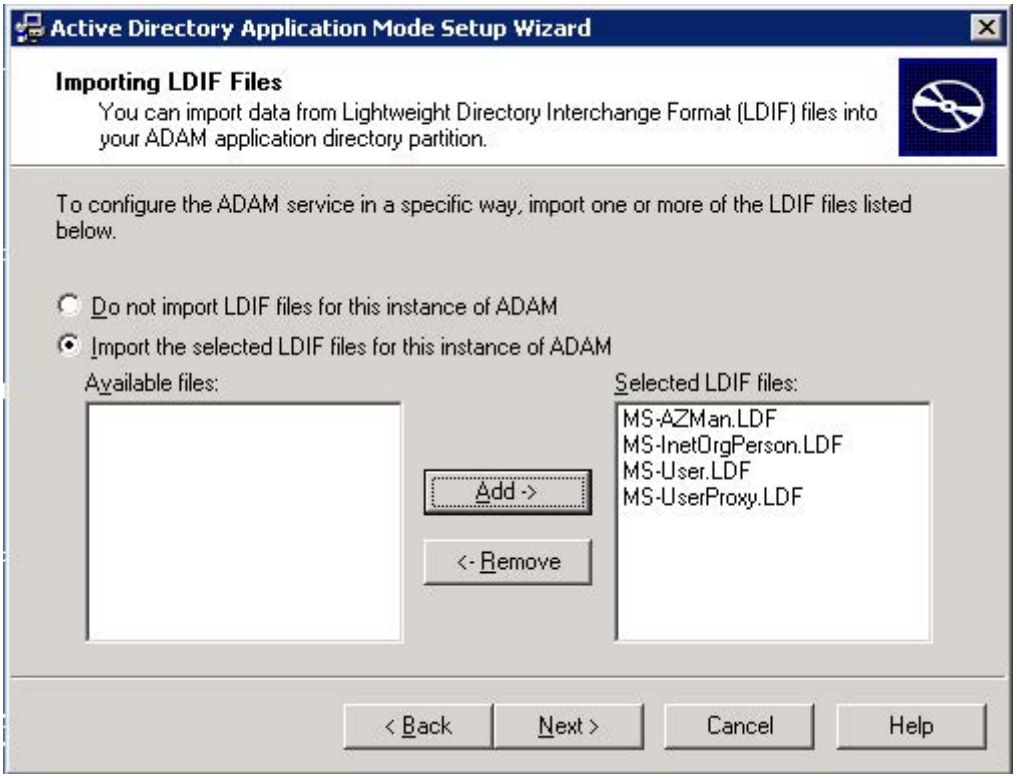
8. Select the first check box to assign the administrative permissions for ADAM to the currently logged

on user (e.g., USER-E5F3EA4782) and click **Next**.

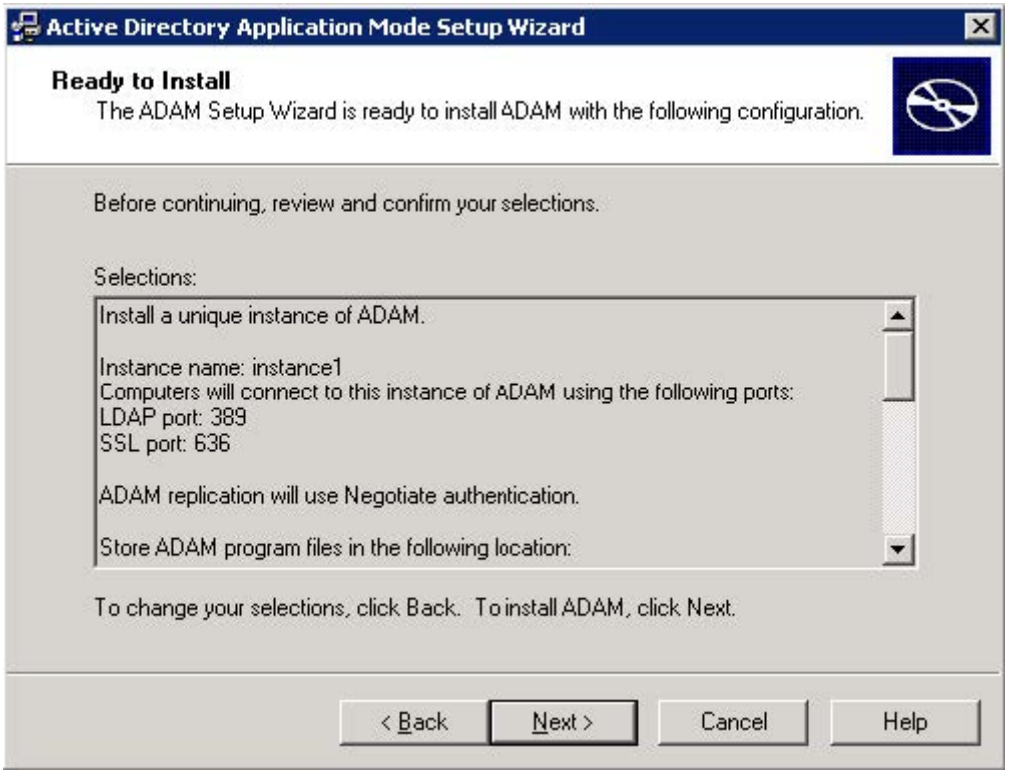


9. Select the **Import the selected LDIF files for this instance of ADAM** check box.

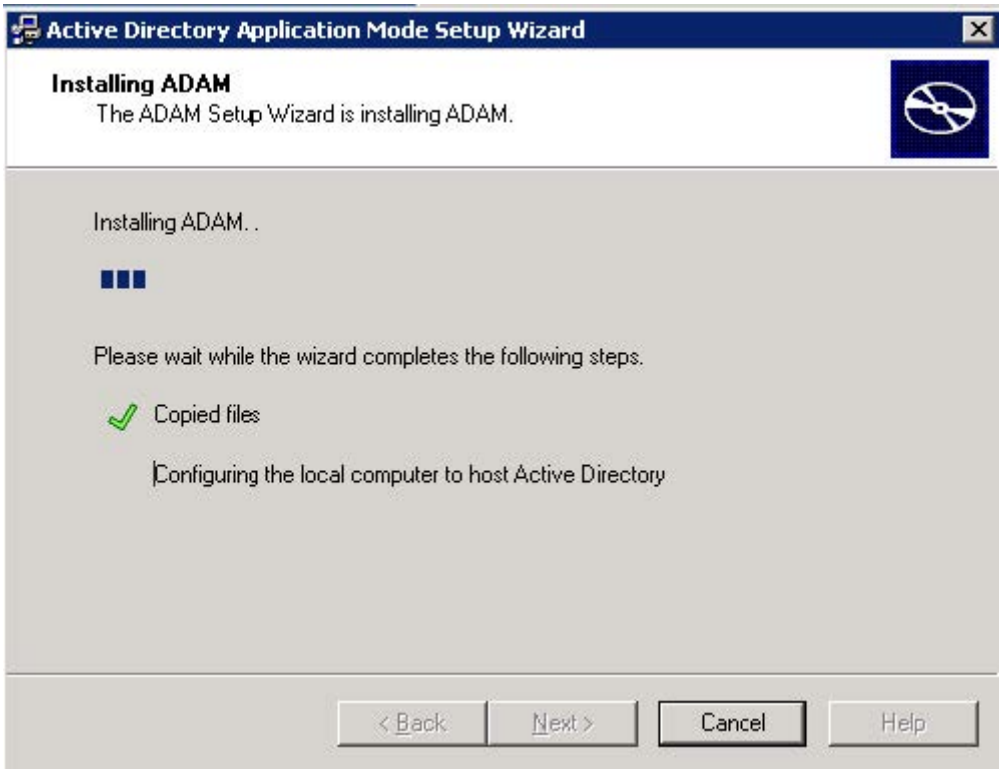
10. In the **Available** files box, select the desired LDF files and then click **Add->**, and then click **Next**.



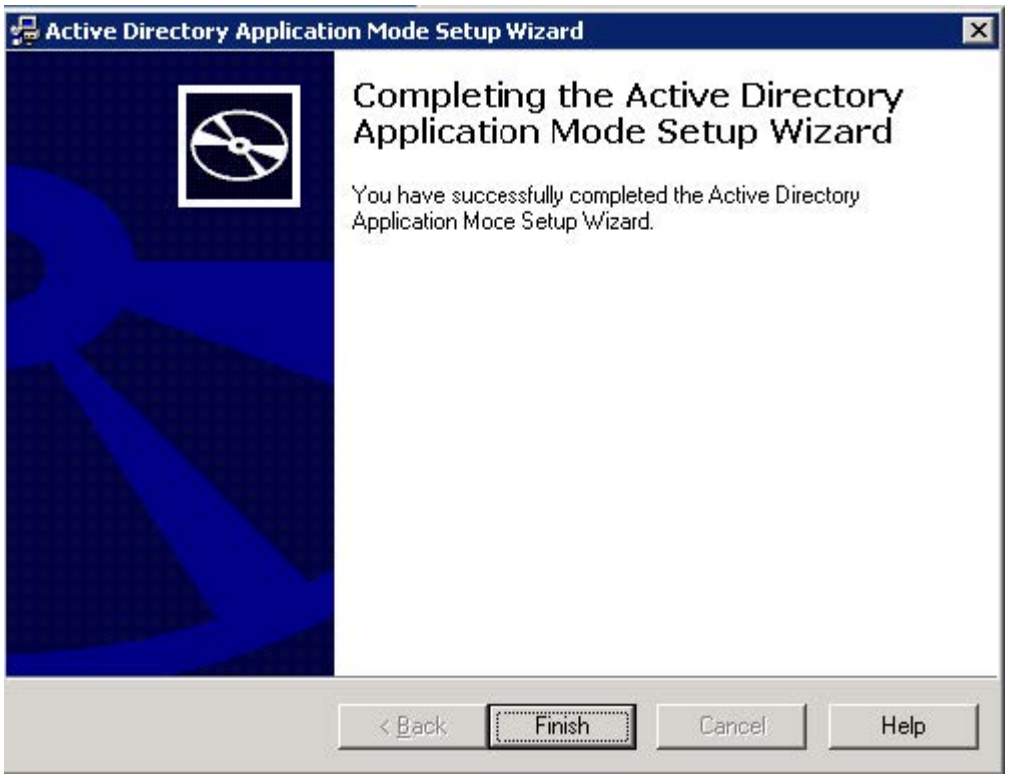
11. Review your selection and click **Next**.



The installation progress is shown as below:



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

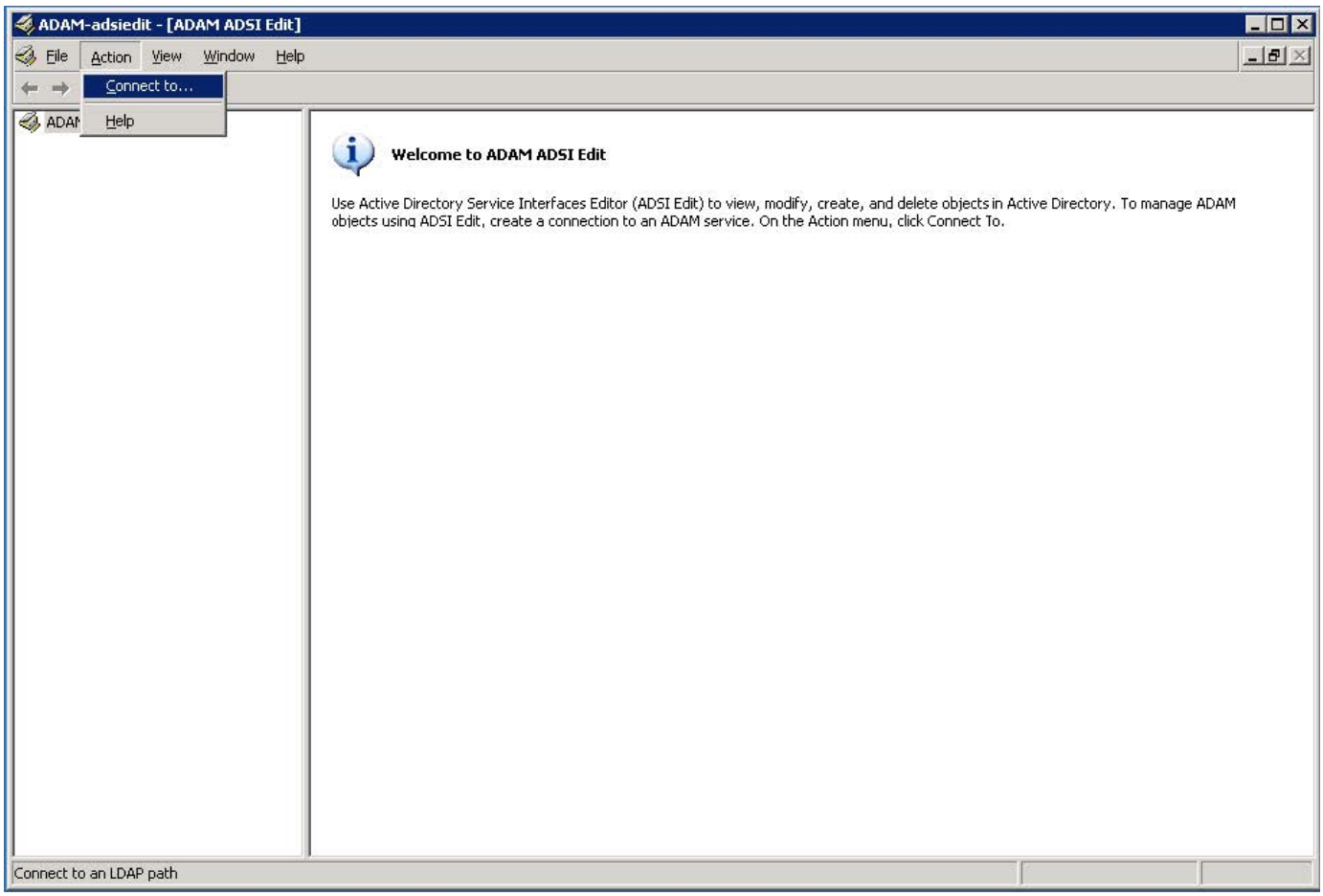


Configure the ADAM ADSI Edit

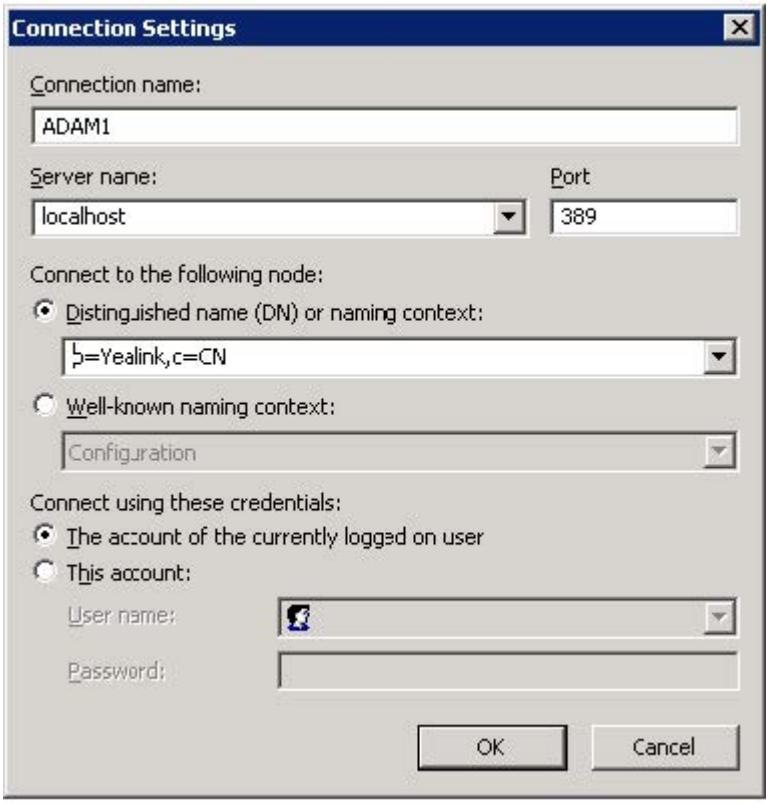
To configure the ADAM ADSI Edit:

1. Click **Start** > **Programs** > **ADAM** > **ADAM ADSI Edit**.

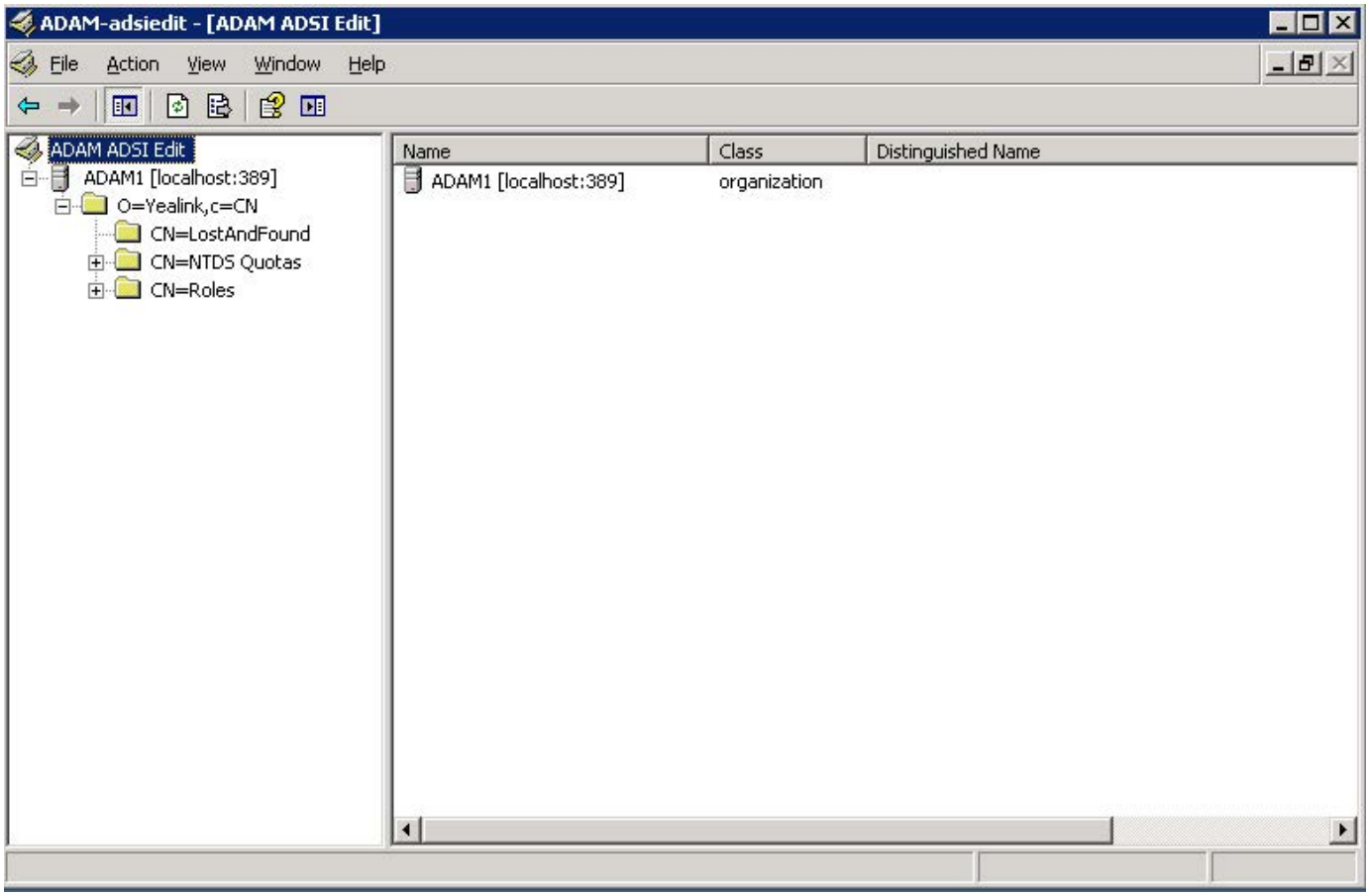
2. Click **Action** > **Connect to**.



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**.

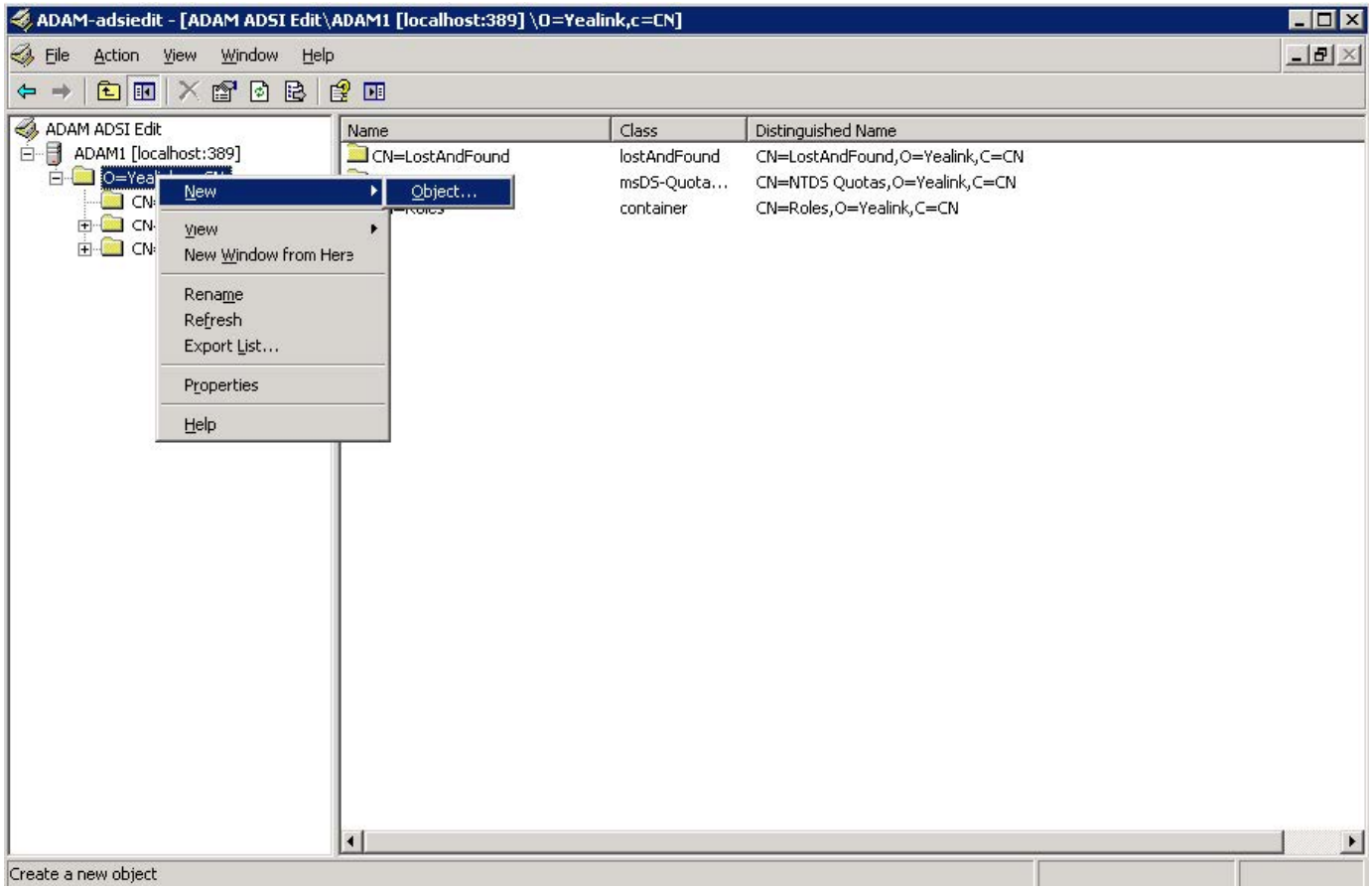


7. When the ADAM ADSI Edit connects an application directory partition (e.g., o=Yealink,c=CN) successfully, it will show as below:

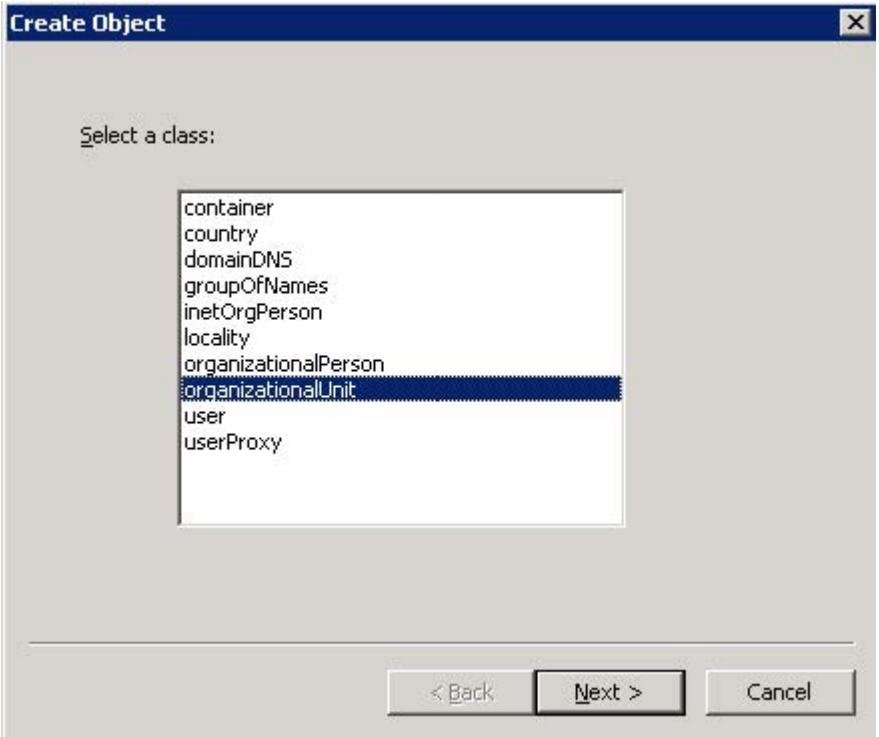


To create the object for ADAM:

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

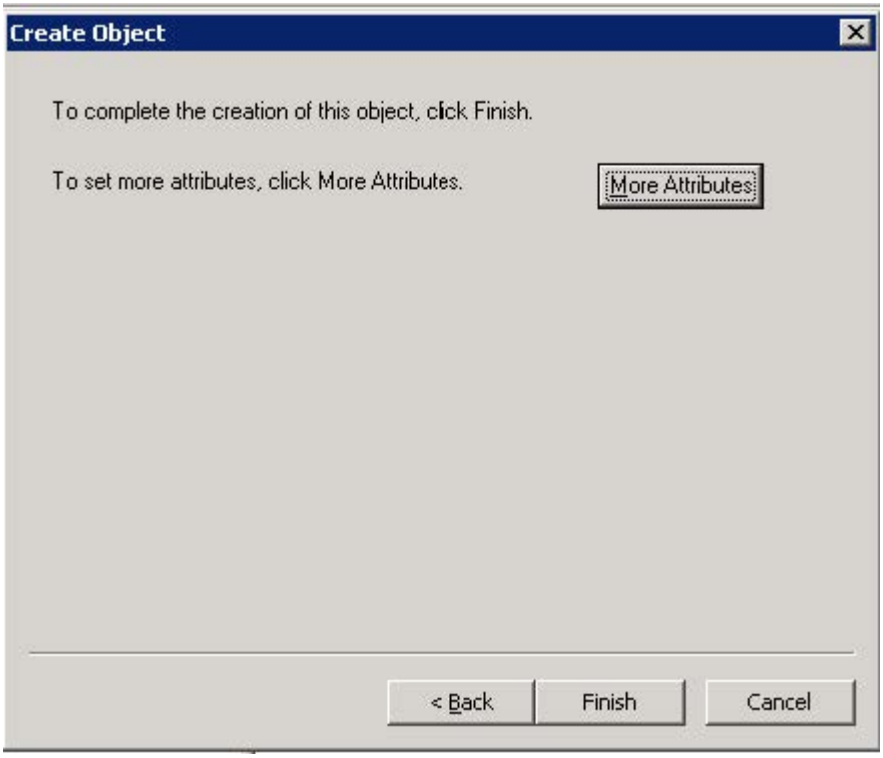


2. Select **organizationalUnit** and click **Next**.

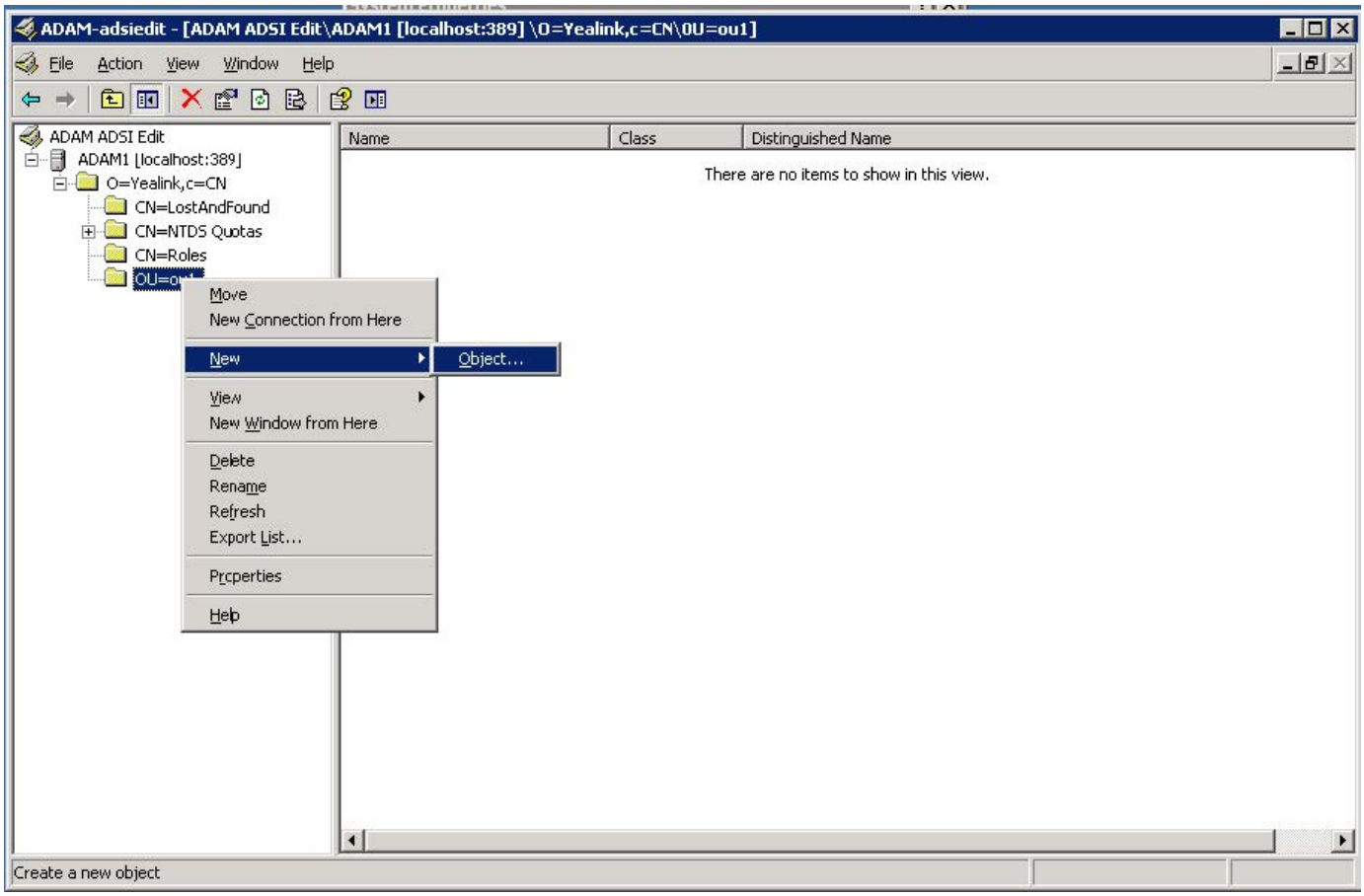


3. Enter the desired value (e.g., ou1) in the **Value** field and click **Next**.
4. Click **Finish** to complete the creation of this object.

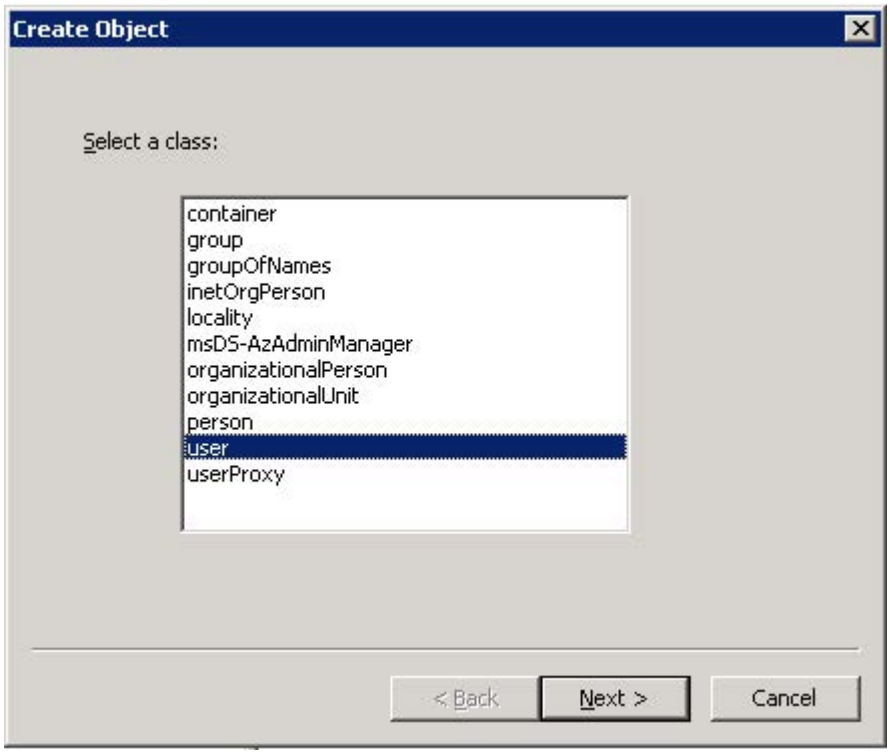
   You can also click **More Attributes** to set more attributes for this object.



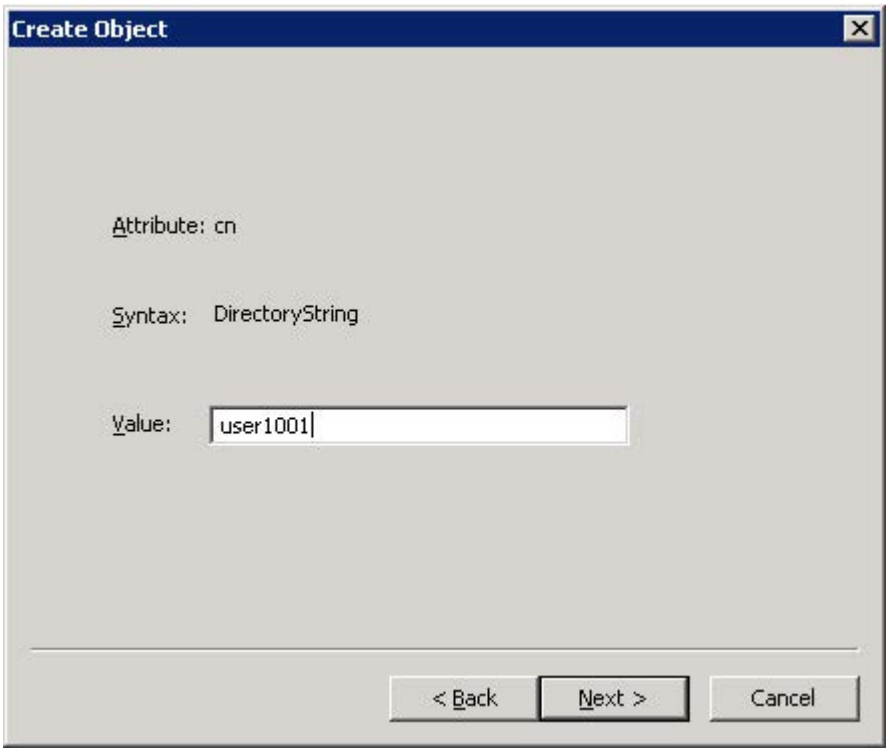
5. Select and right-click **OU=ou1**, and then select **New** > **Object**.



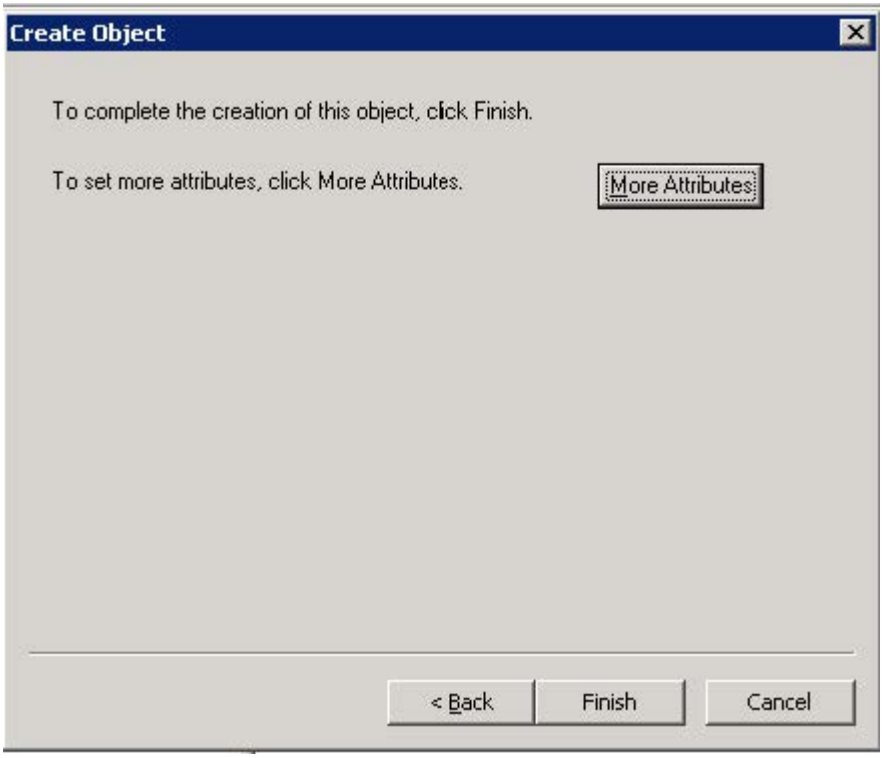
6. Select **user** and click **Next**.



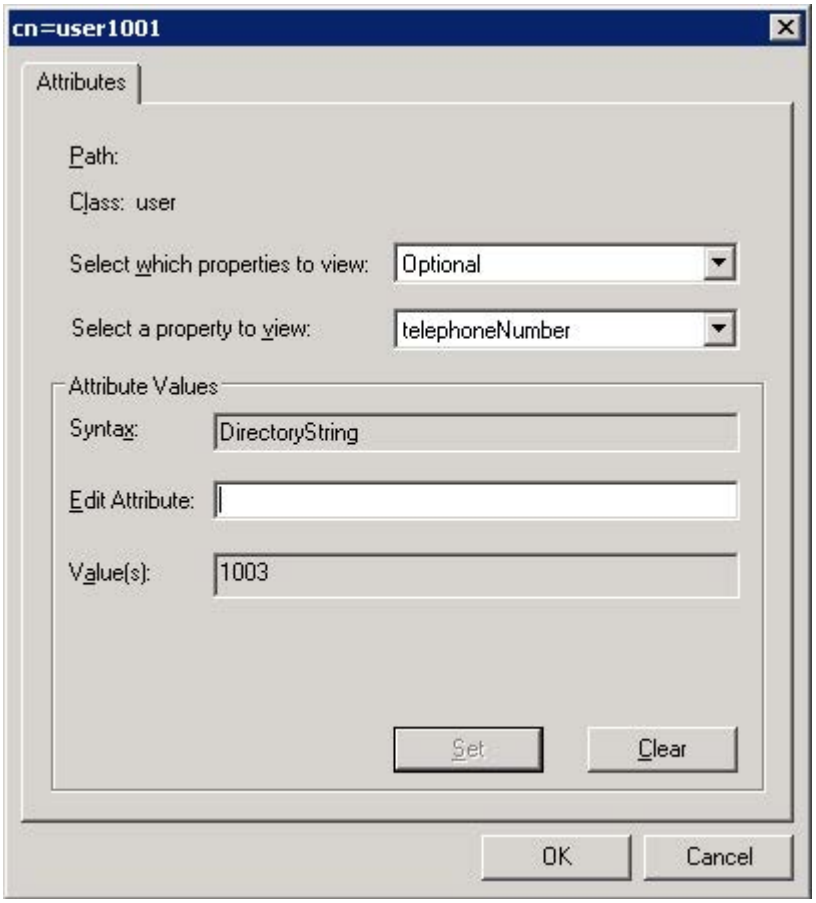
7. Enter the desired value (e.g., user1001) in the **Value** field and click **Next**.



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.



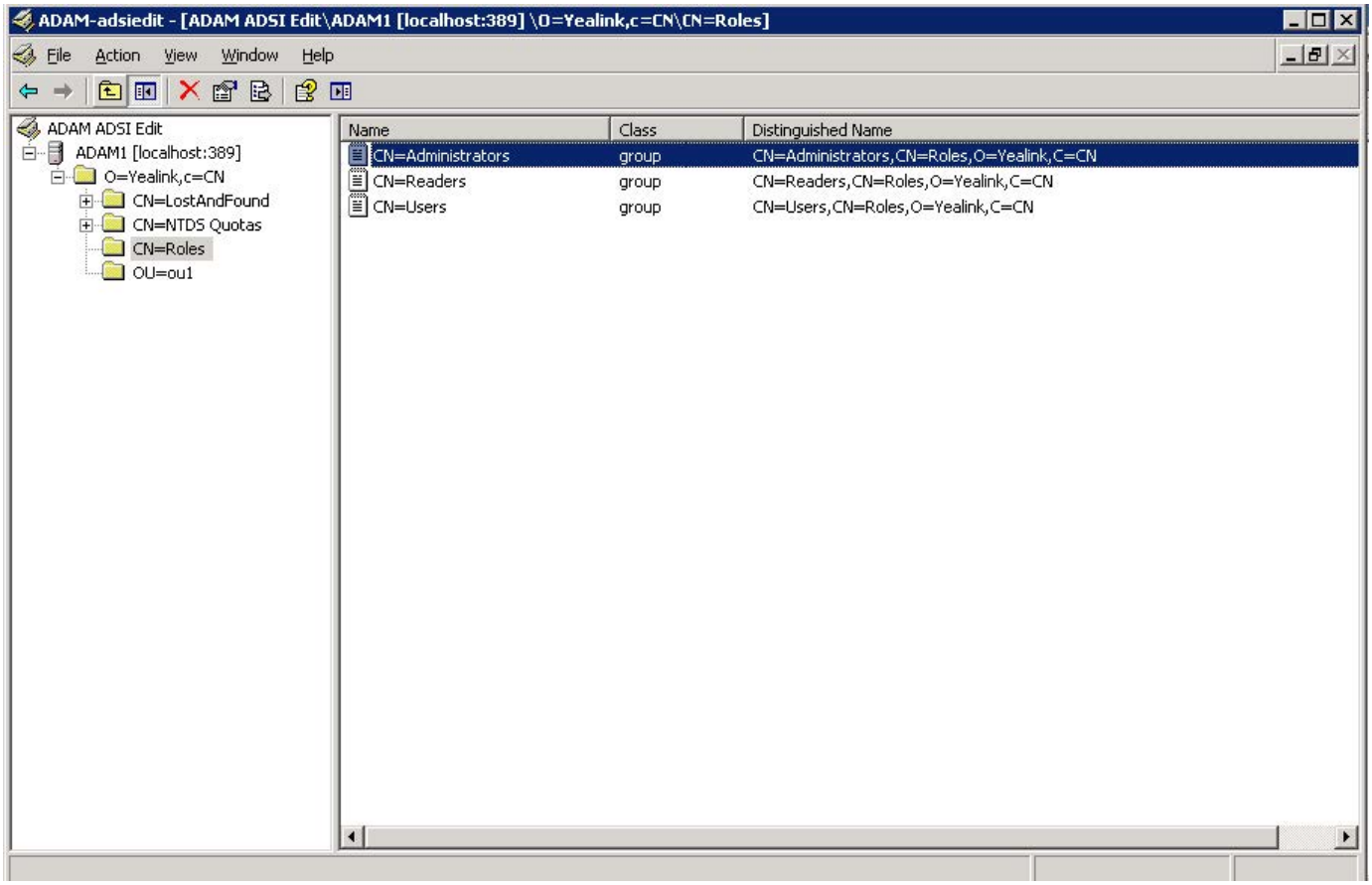
10. Click **OK** to close the Attributes dialog, and click **Finish** to complete the creation of this user.
11. Select and right-click the user created above, and then select **Reset Password**.
12. Enter the password for the user created above in the **New password** field and the **Confirm password** field, respectively.

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

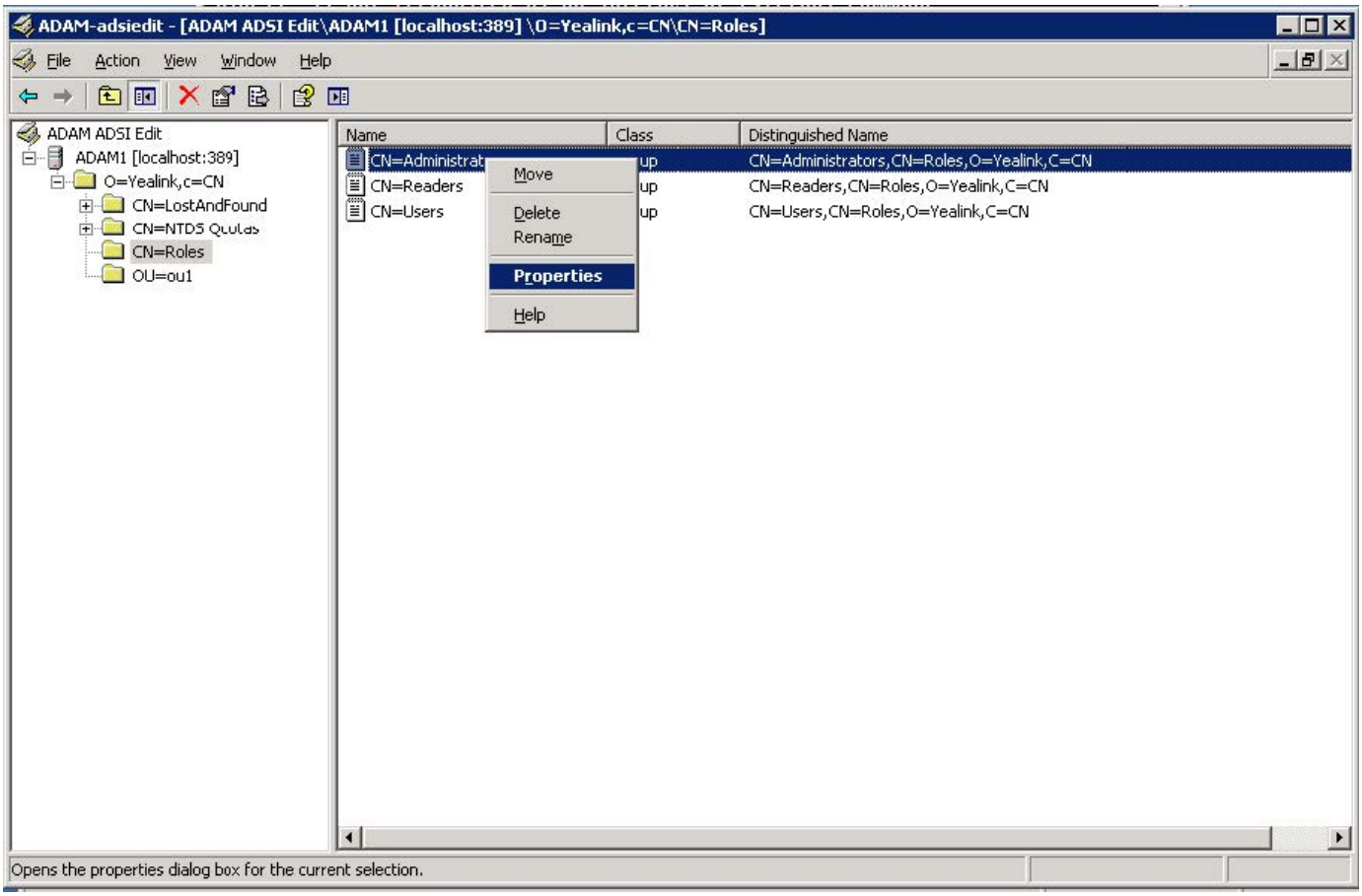
If you want to use the user created above to manage and search for information of LDAP, you need to add the user to the administrator group in advance.

To add the user to the administrator group:

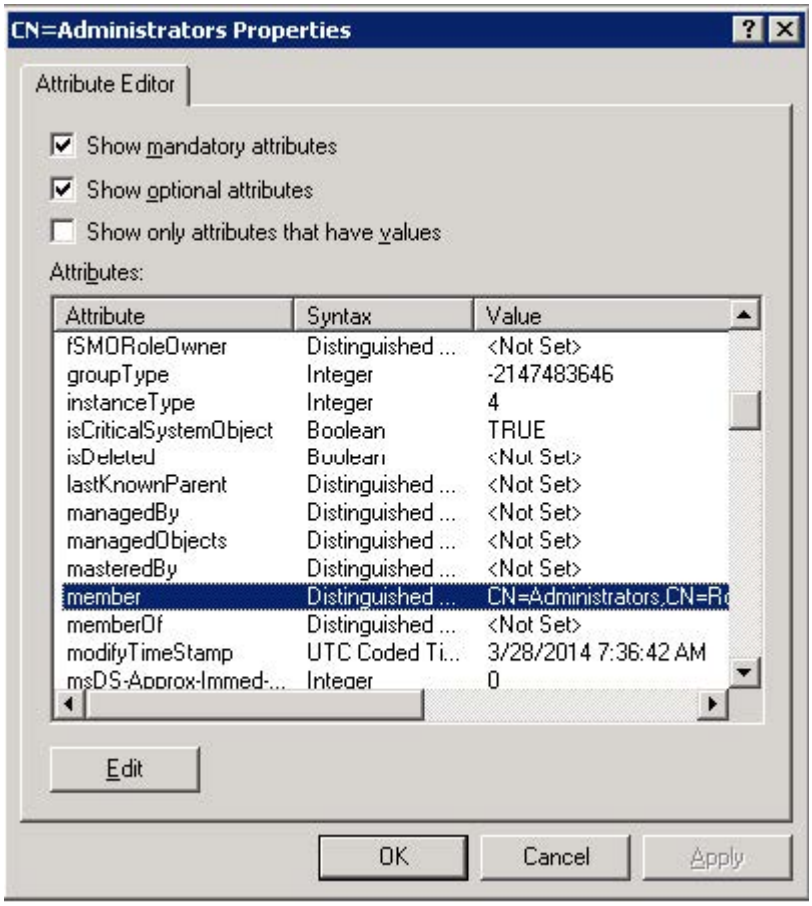
1. Click **ADAM1** > **O=Yealink, c=CN** > **CN=Roles**.



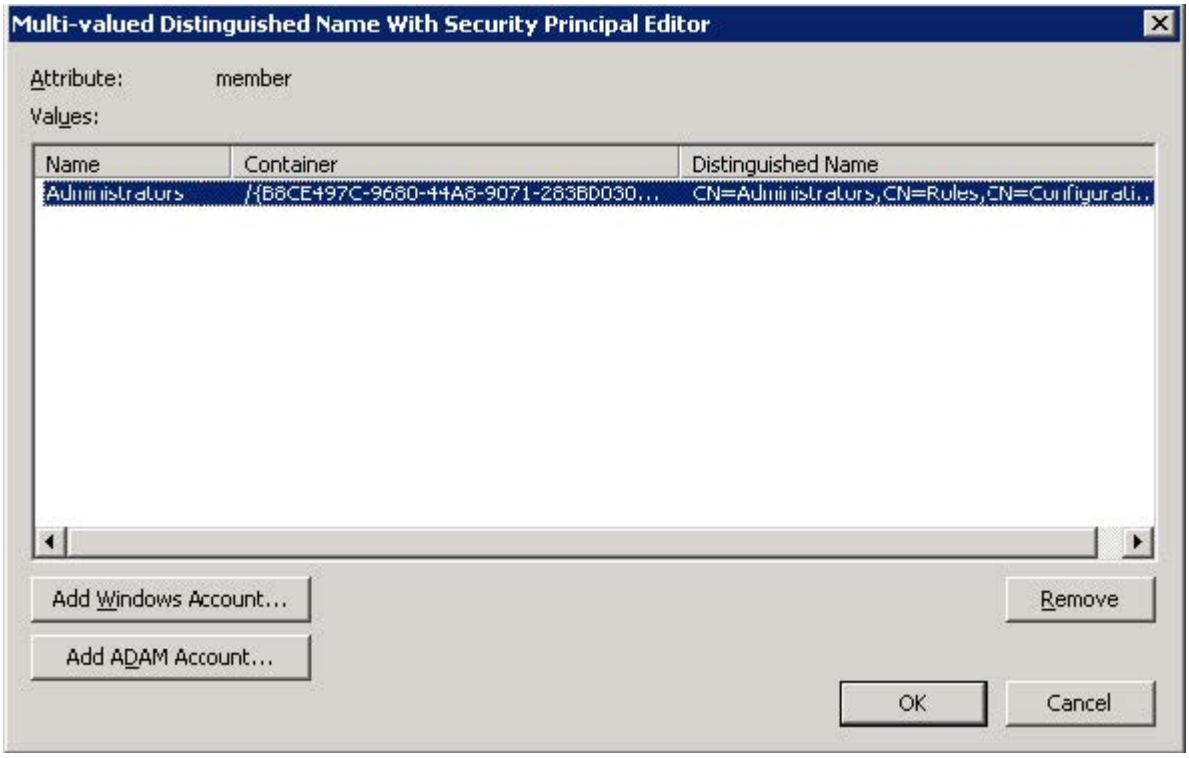
2. Select and right-click **CN=Administrators**, and then select **Properties**.



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 for 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 for adding the ADAM account.

7. Click **OK** to accept the change and close the dialog for the member attribute.

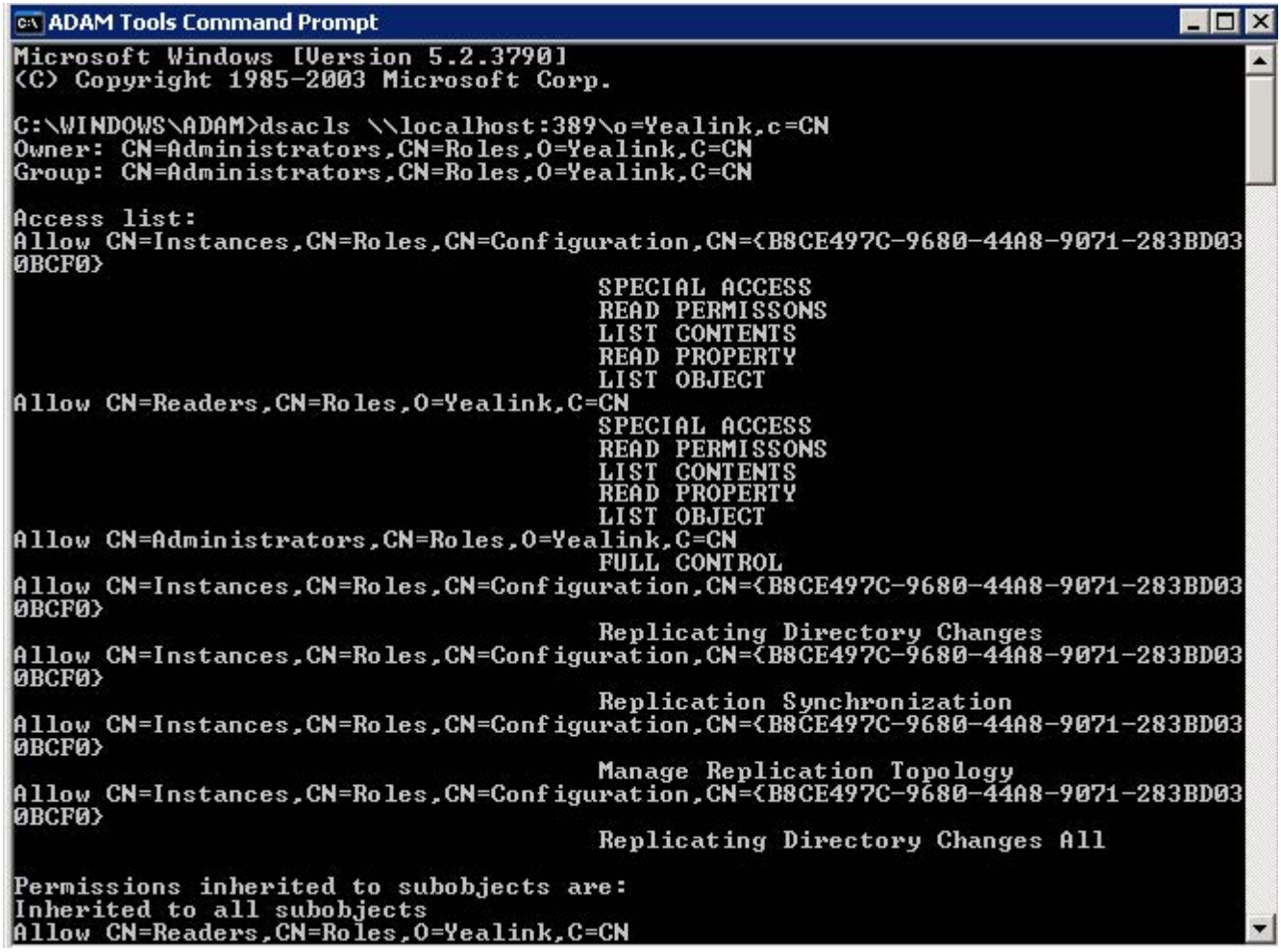
8. Click **OK** to accept the change and close the Administrator's Properties interface.

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
```

1. Save the hosts file.

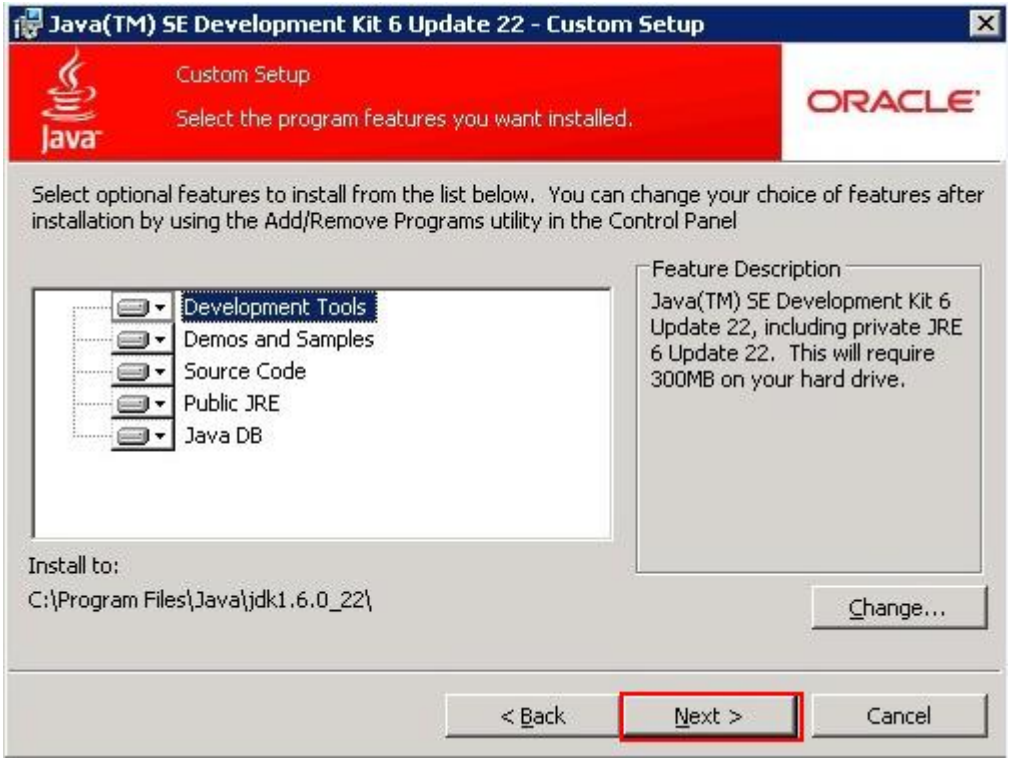
The following shows you how to install the Java Development Kit (JDK) 6 on your computer. You can download it online: http://www.oracle.com/technetwork/java/javase/downloads/index.html.

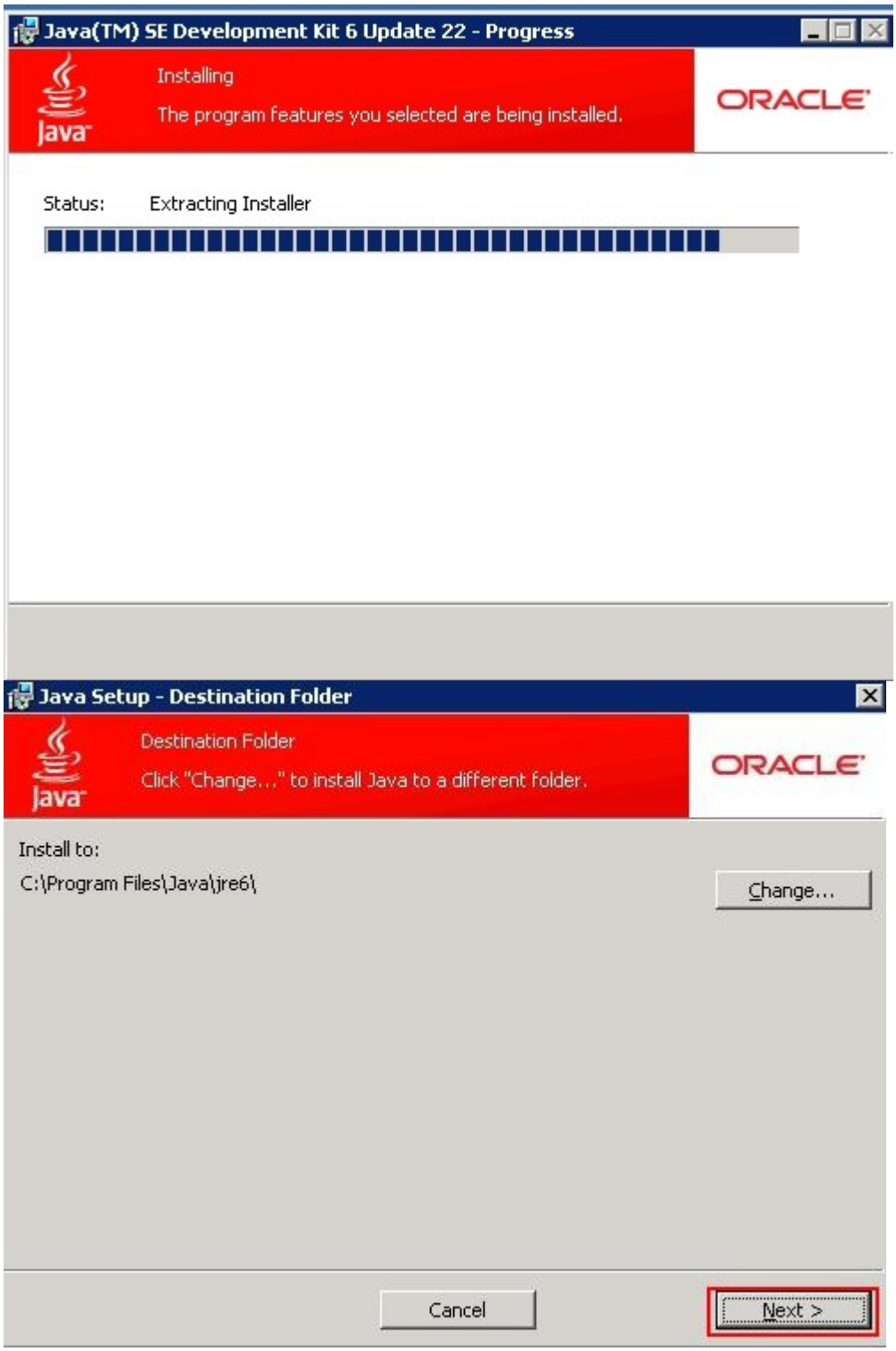
To install the Java Development Kit (JDK) 6:

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**.
4. 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 - 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 >

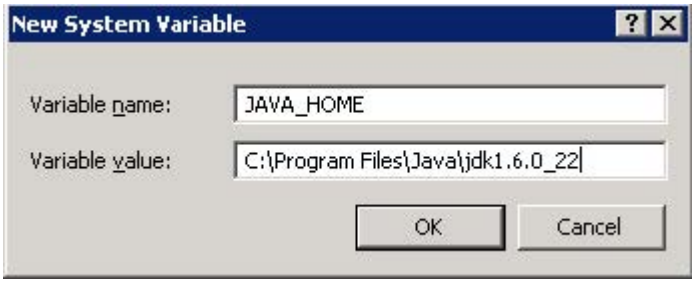
4. Click **Finish** to finish the installation.

   After the installation, you need to configure environment variables.

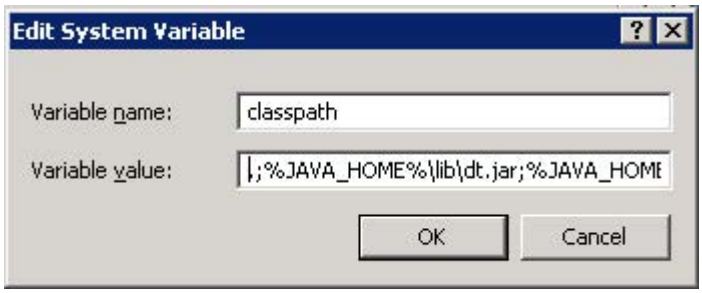
To configure environment variables:

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, and click **New** under **System Variables**.

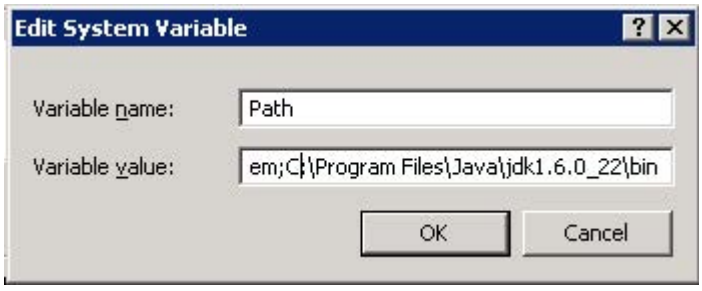
5. Enter the variable name as JAVA_HOME.
6. Enter the variable value as the installation path (e.g., C:\Program Files\Java\jdk1.6.0_22) for the Java Development Kit.



7. Click **OK**.
8. Repeat steps 4-7 to create a new system variable.
9. 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.
10. %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.

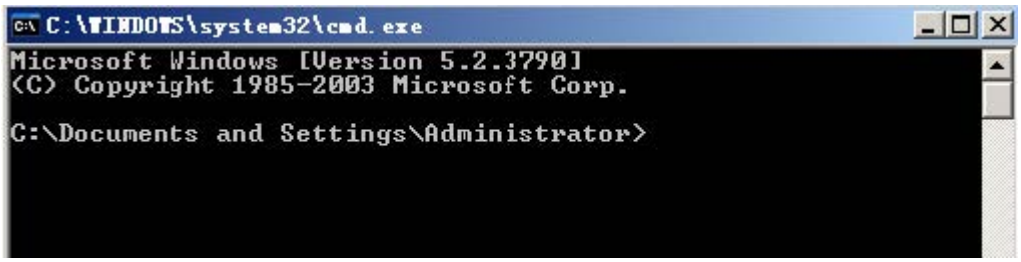


11. Click **OK**.
12. Click **Apply Changes**.

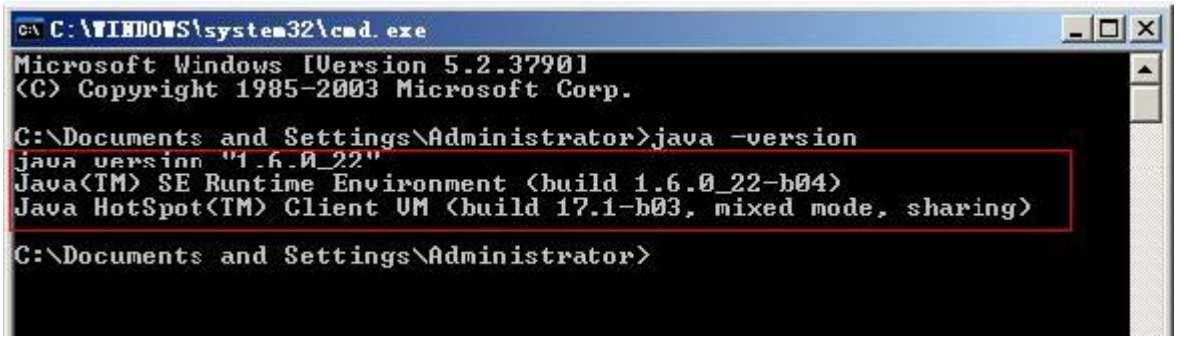
To verify the configuration of environment variables:

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

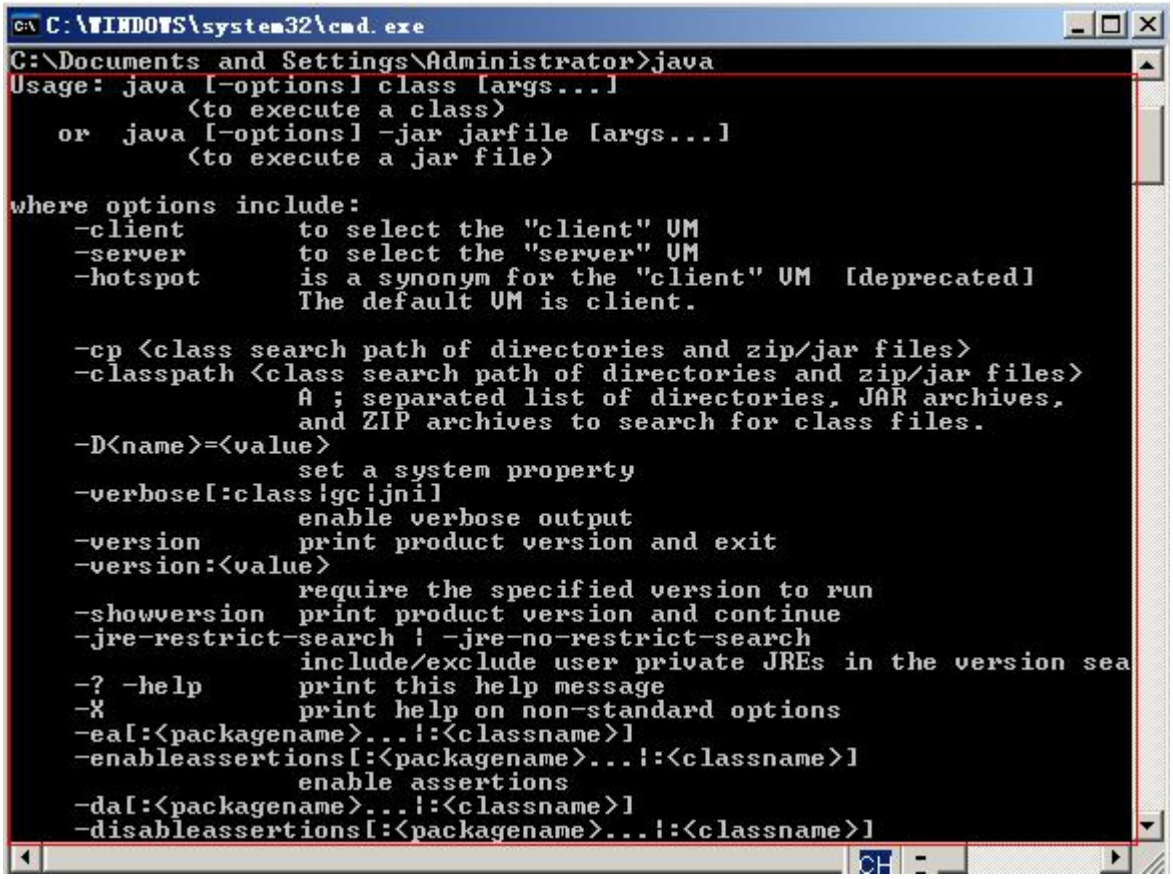
2. Enter **cmd** in the dialog and click **OK** to enter the command line interface.



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



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



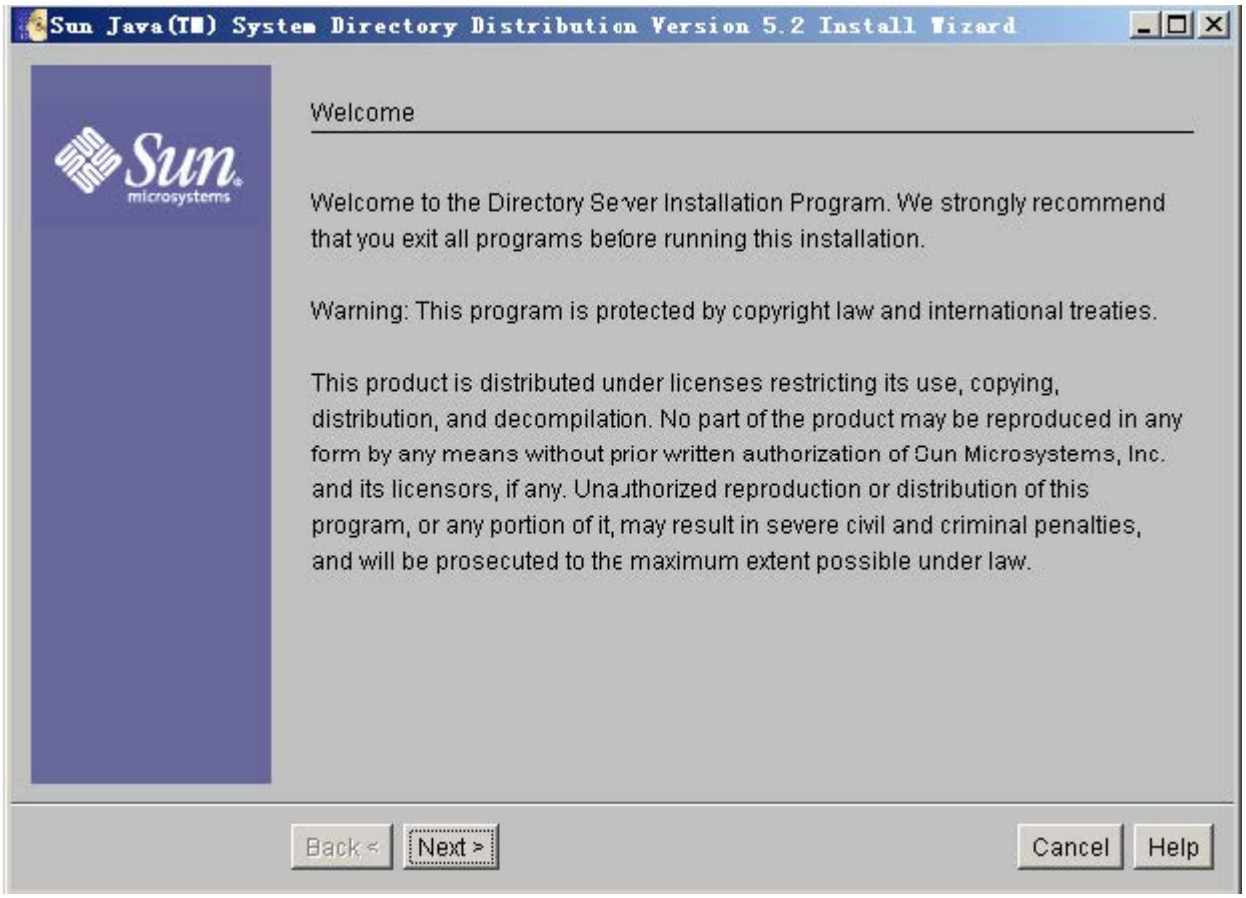
5. Execute the command **javac** to compile java files into class files.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>javac
Usage: javac <options> <source files>
where possible options include:
  -g                         Generate all debugging info
  -g:none                    Generate no debugging info
  -g:{lines,vars,source}     Generate only some debugging info
  -nowarn                    Generate no warnings
  -verbose                   Output messages about what the compiler is doing
  -deprecation               Output source locations where deprecated APIs are
sed
  -classpath <path>          Specify where to find user class files and annota
on processors
  -cp <path>                 Specify where to find user class files and annota
on processors
  -sourcepath <path>         Specify where to find input source files
  -bootclasspath <path>      Override location of bootstrap class files
  -extdirs <dirs>            Override location of installed extensions
  -endorseddirs <dirs>       Override location of endorsed standards path
  -proc:{none,only}          Control whether annotation processing and/or comp
ation is done.
  -processor <class1>[,<class2>,<class3>...]Names of the annotation processors
o run; bypasses default discovery process
  -processorpath <path>      Specify where to find annotation processors
  -d <directory>             Specify where to place generated class files
  -s <directory>             Specify where to place generated source files
  -implicit:{none,class}     Specify whether or not to generate class files fo
implicitly referenced files
  -encoding <encoding>       Specify character encoding used by source files
  -source <release>          Provide source compatibility with specified relea

  -target <release>          Generate class files for specific VM version
  -version                   Version information
  -help                      Print a synopsis of standard options
  -Akey[=value]              Options to pass to annotation processors
  -X                         Print a synopsis of nonstandard options
  -J<flag>                   Pass <flag> directly to the runtime system

C:\Documents and Settings\Administrator>_
```

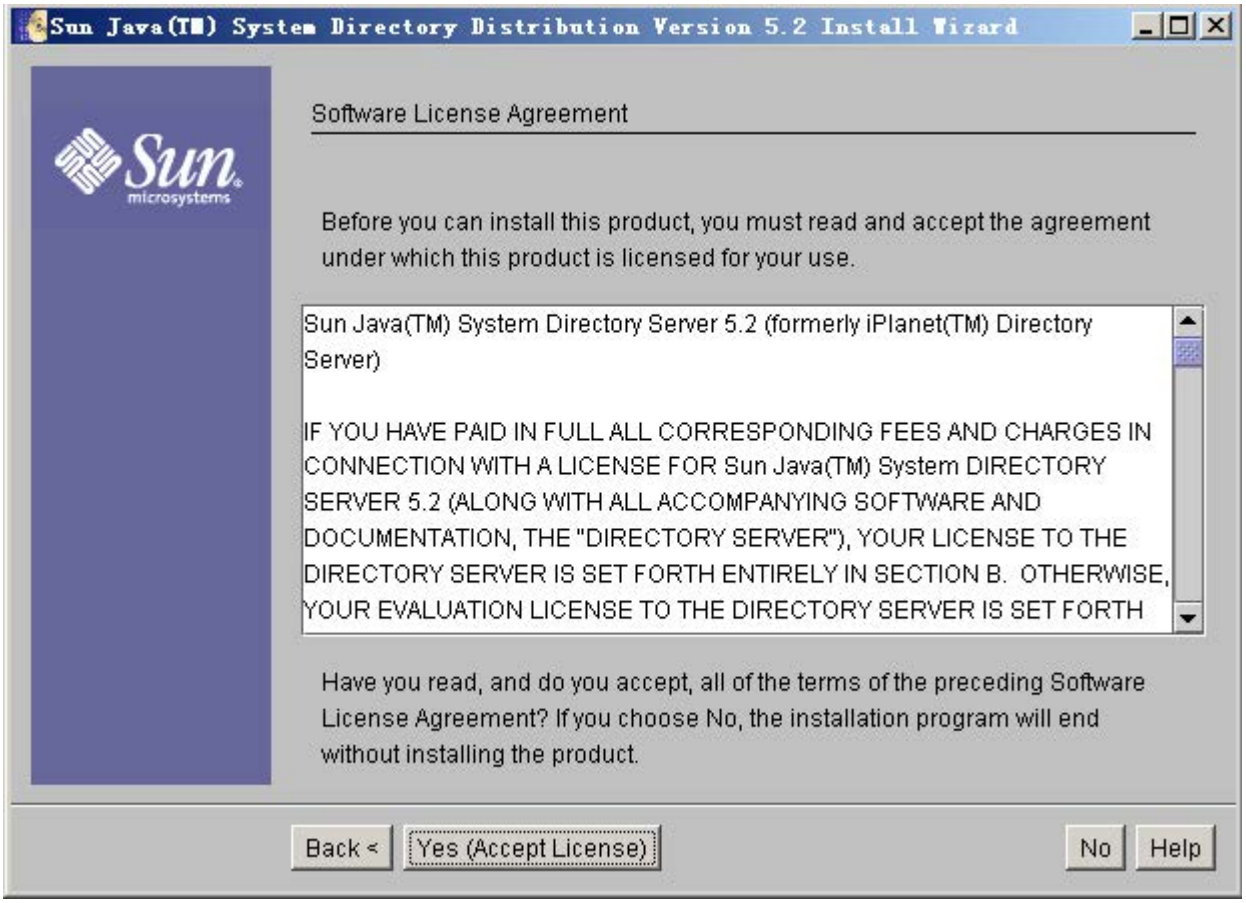
Install the Sun One Directory

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**.

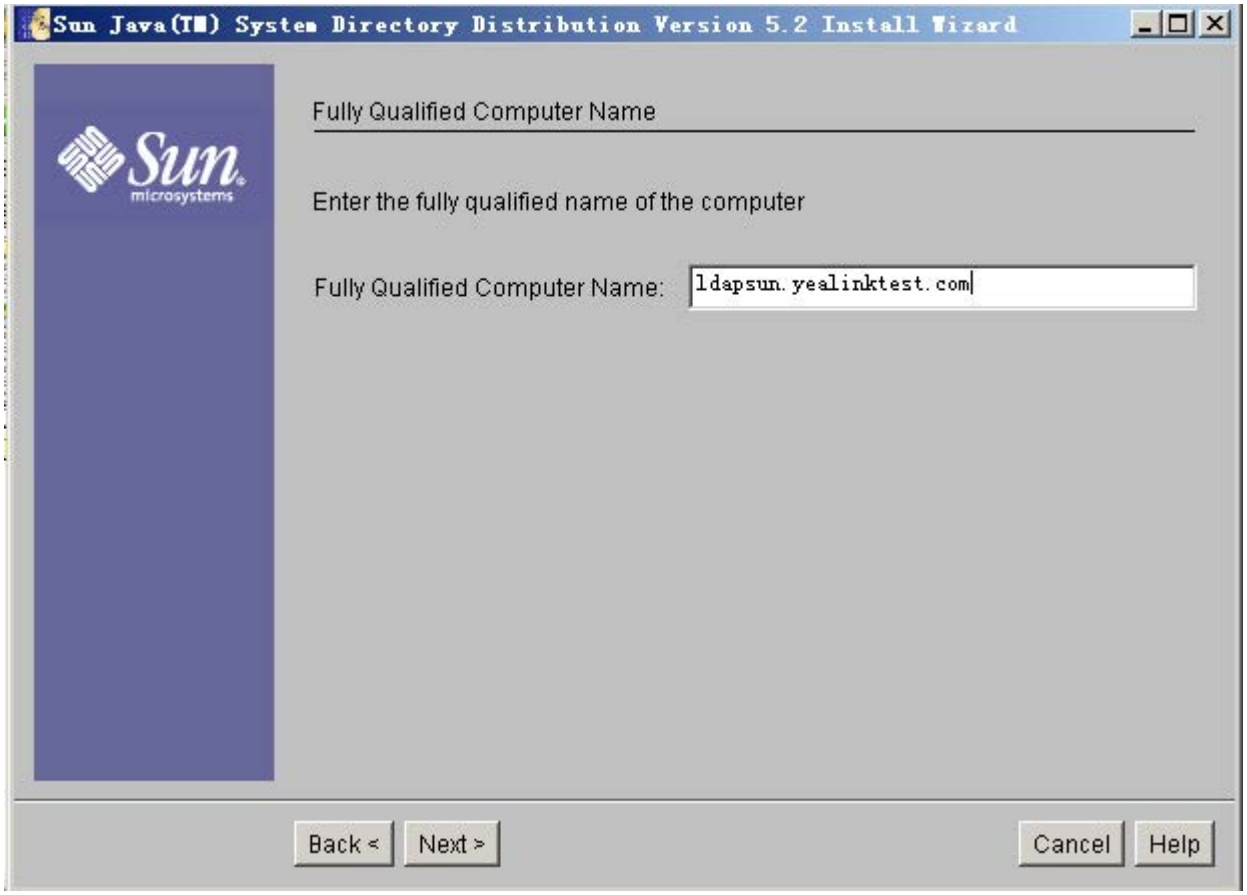


4. Read the software license agreement and click **Yes (Accept License)**.

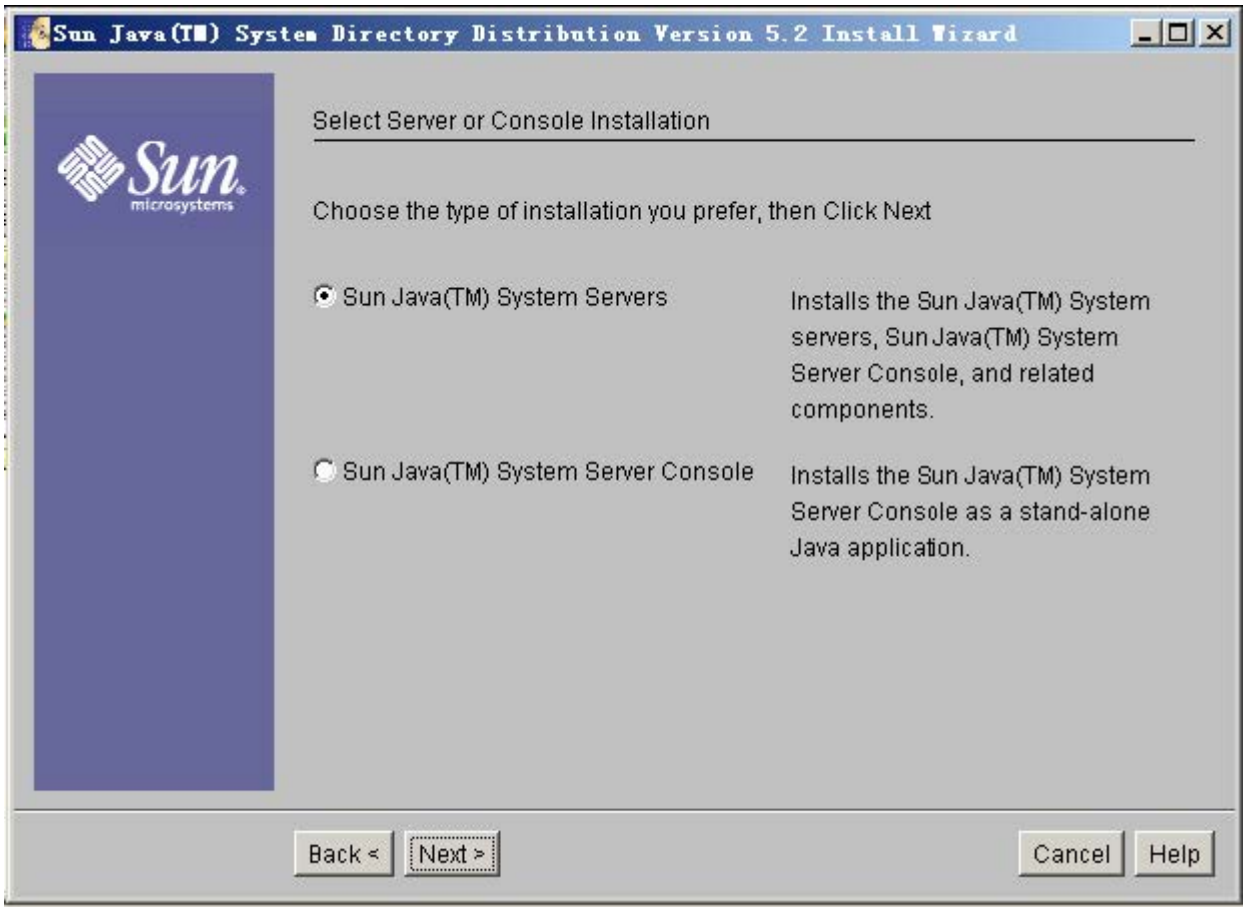


5. Enter the fully qualified name of the computer (e.g., ldapsun.yealinktest.com) in the **Fully Qualified Computer Name** field and click **Next**.

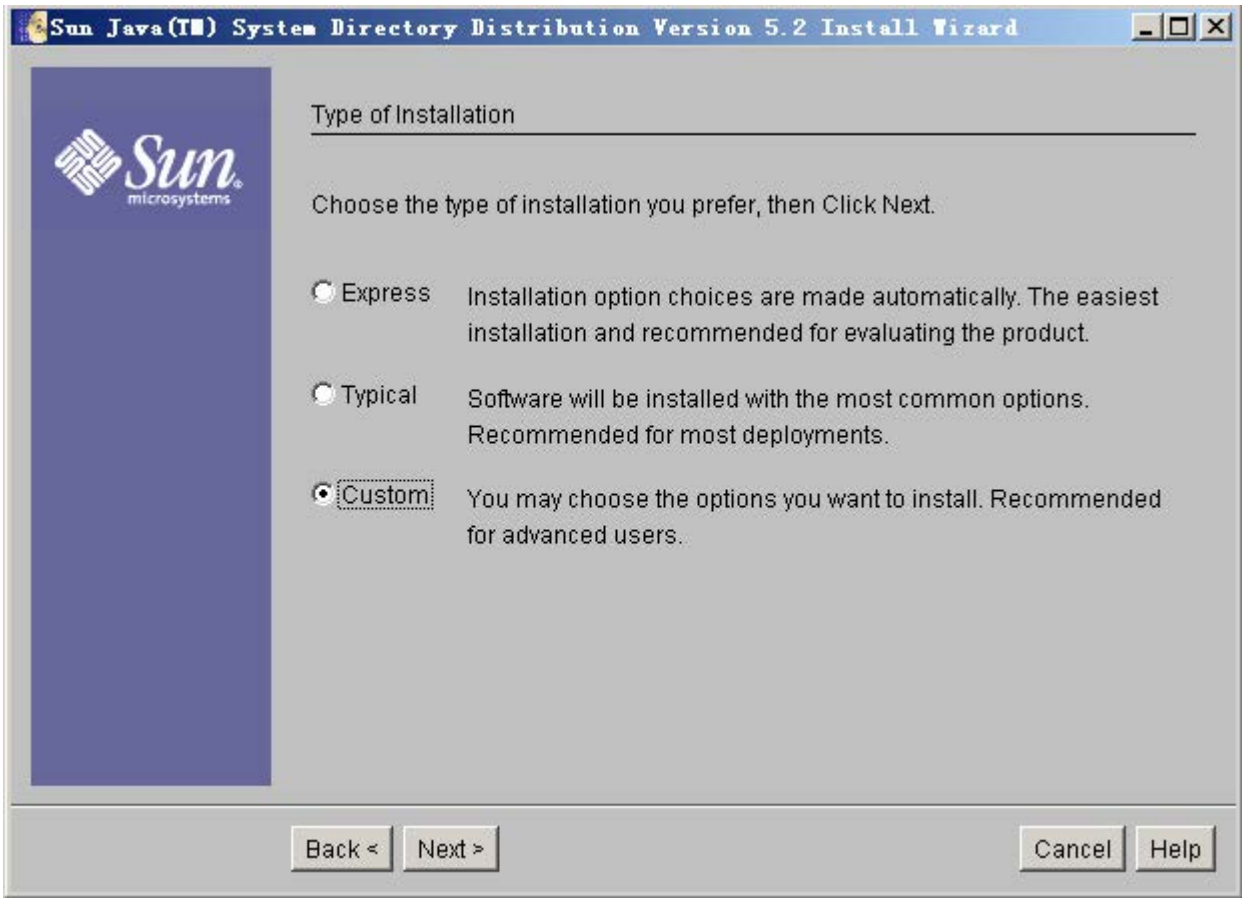
6. The fully qualified name of the computer was planned before. For more information, refer to modify the hosts file of your computer.



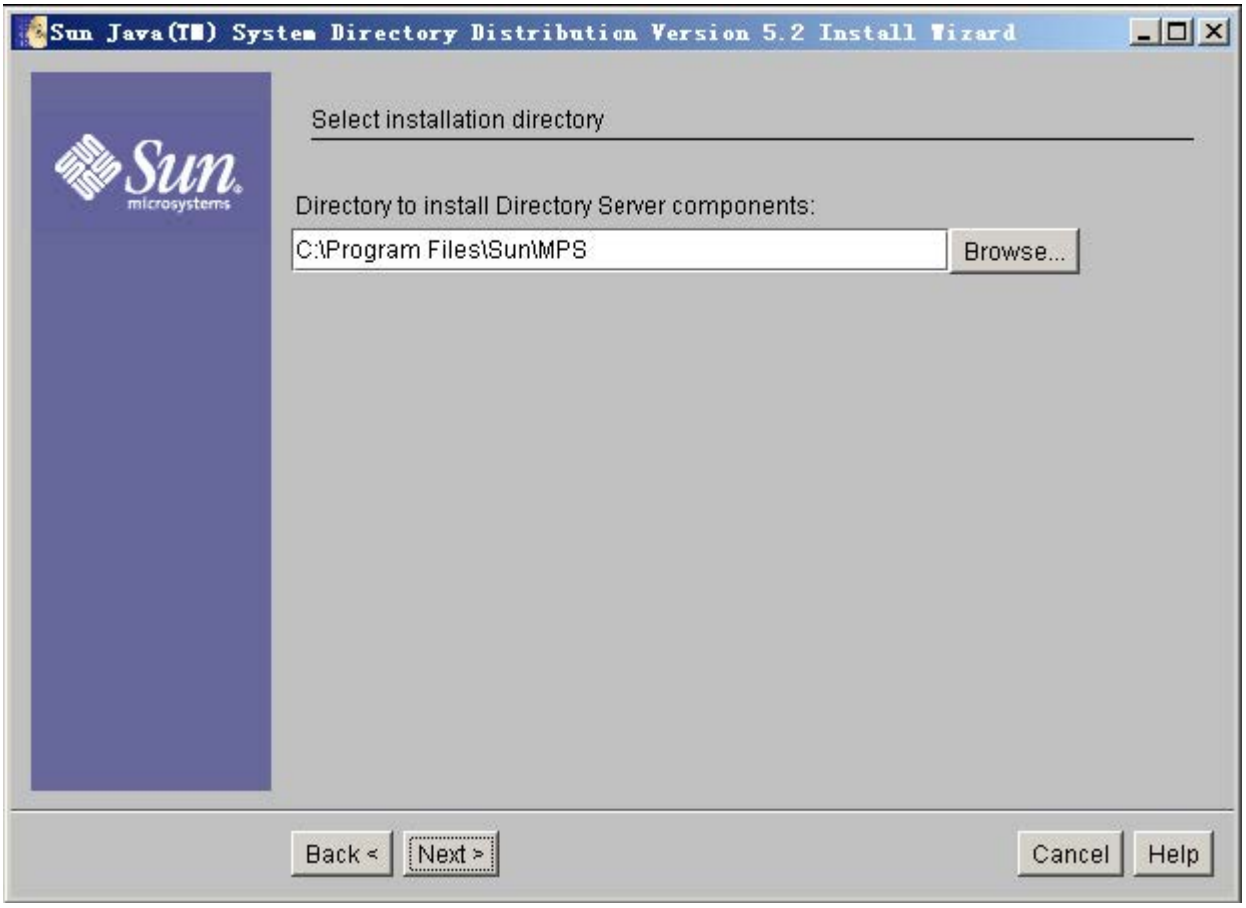
6. Select the **Sun Java ™ System Servers** check box and click **Next**.



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



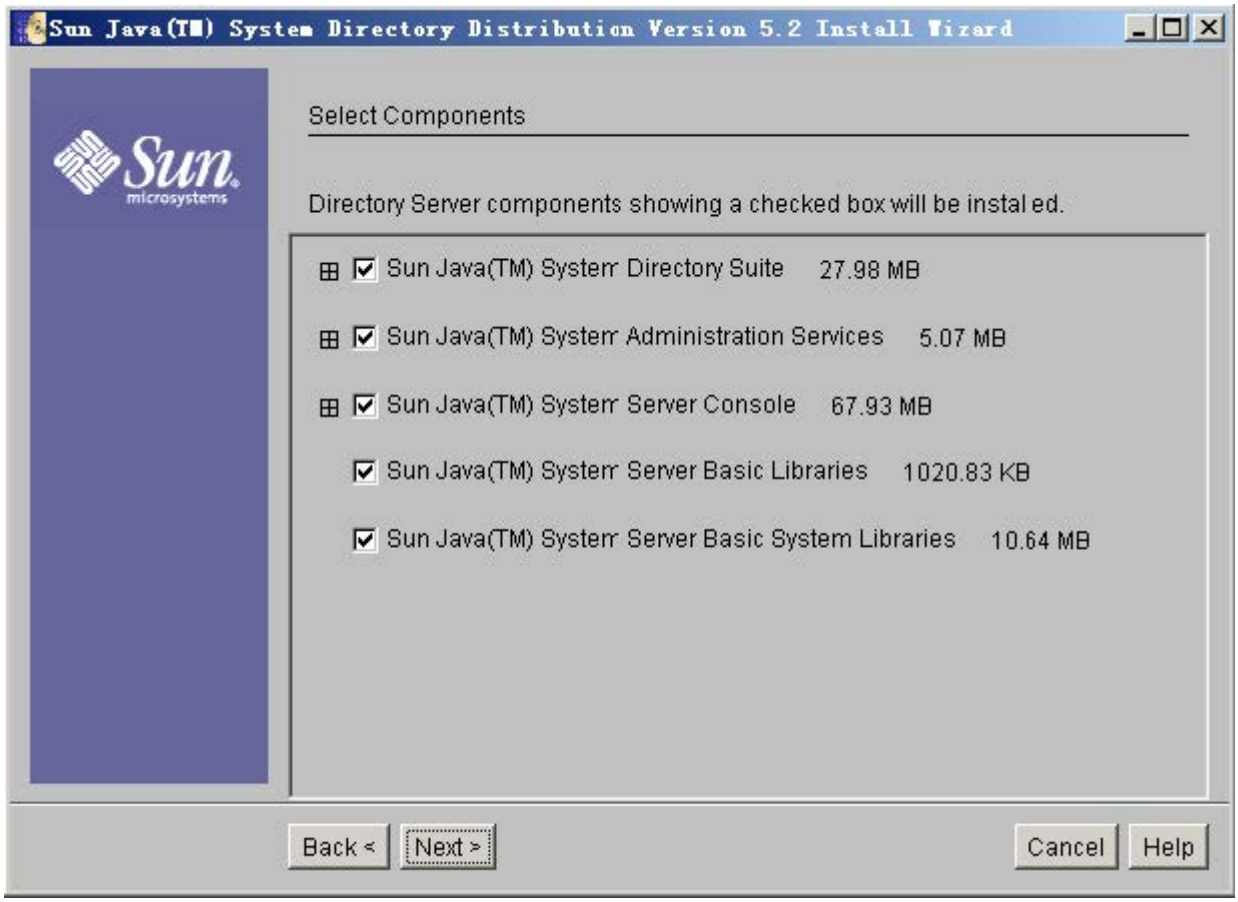
8. Specify the desired installation directory and click **Next**.



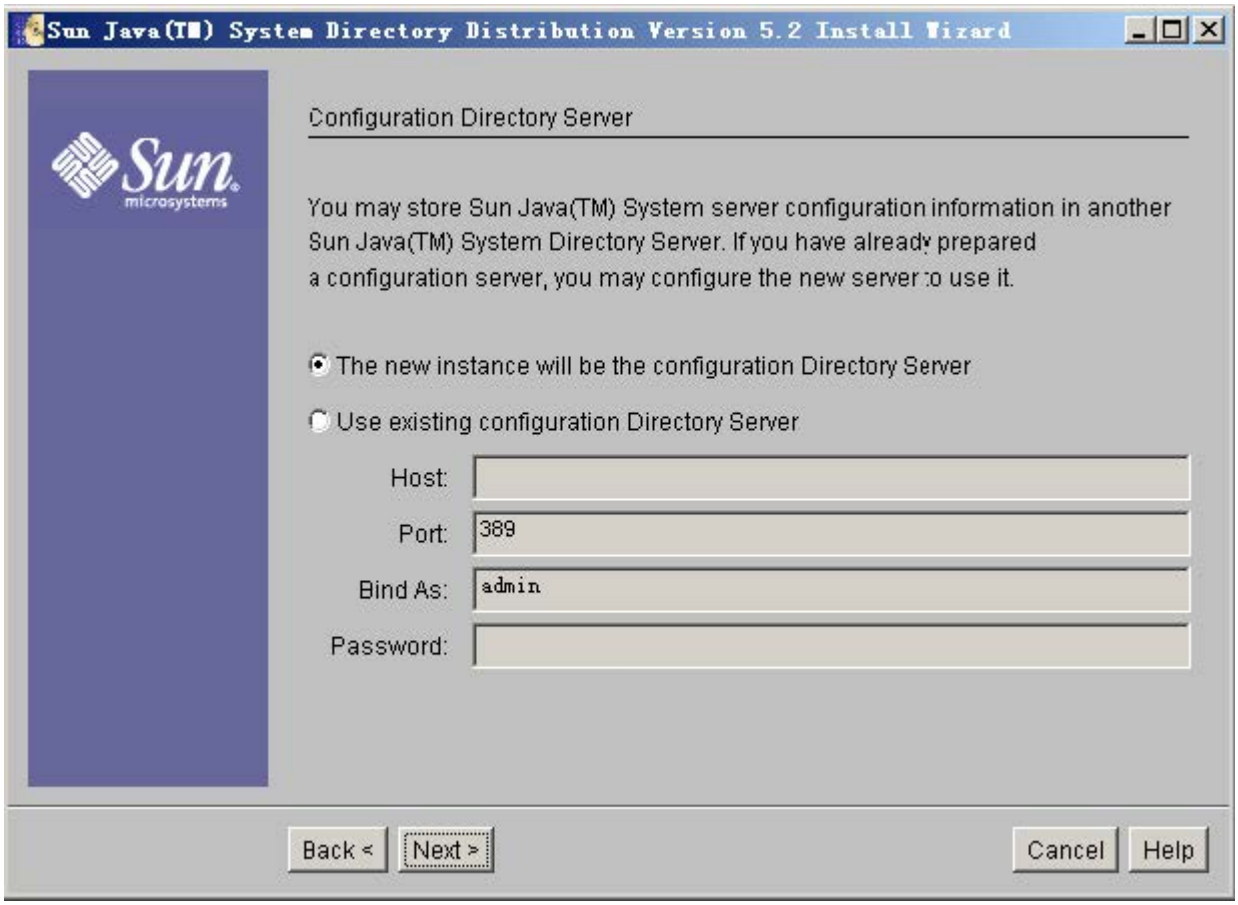
10. It prompts the following window. And you can click **Create Directory** to create the directory or

click **Choose New** to select another path.

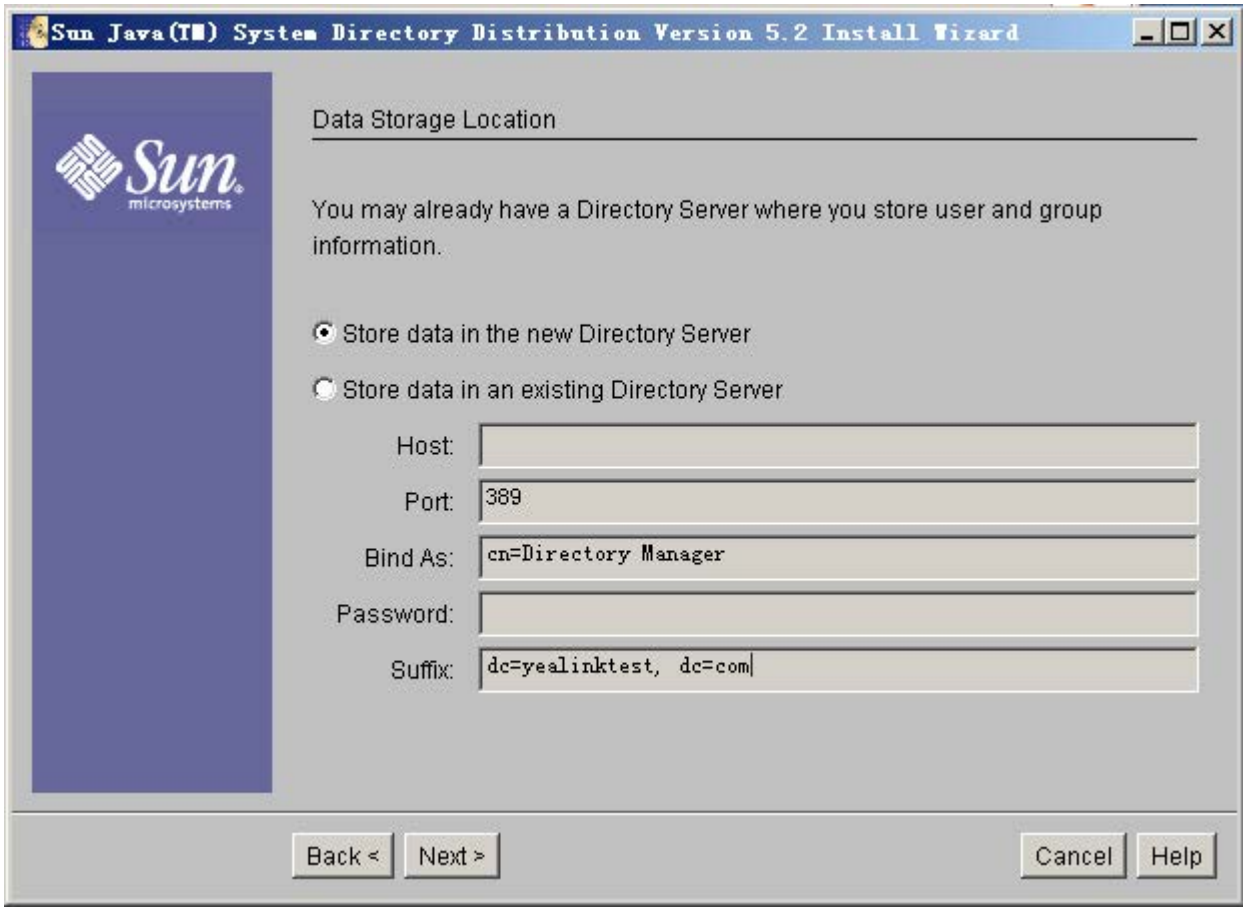
9. Select the desired installation components and click **Next**.



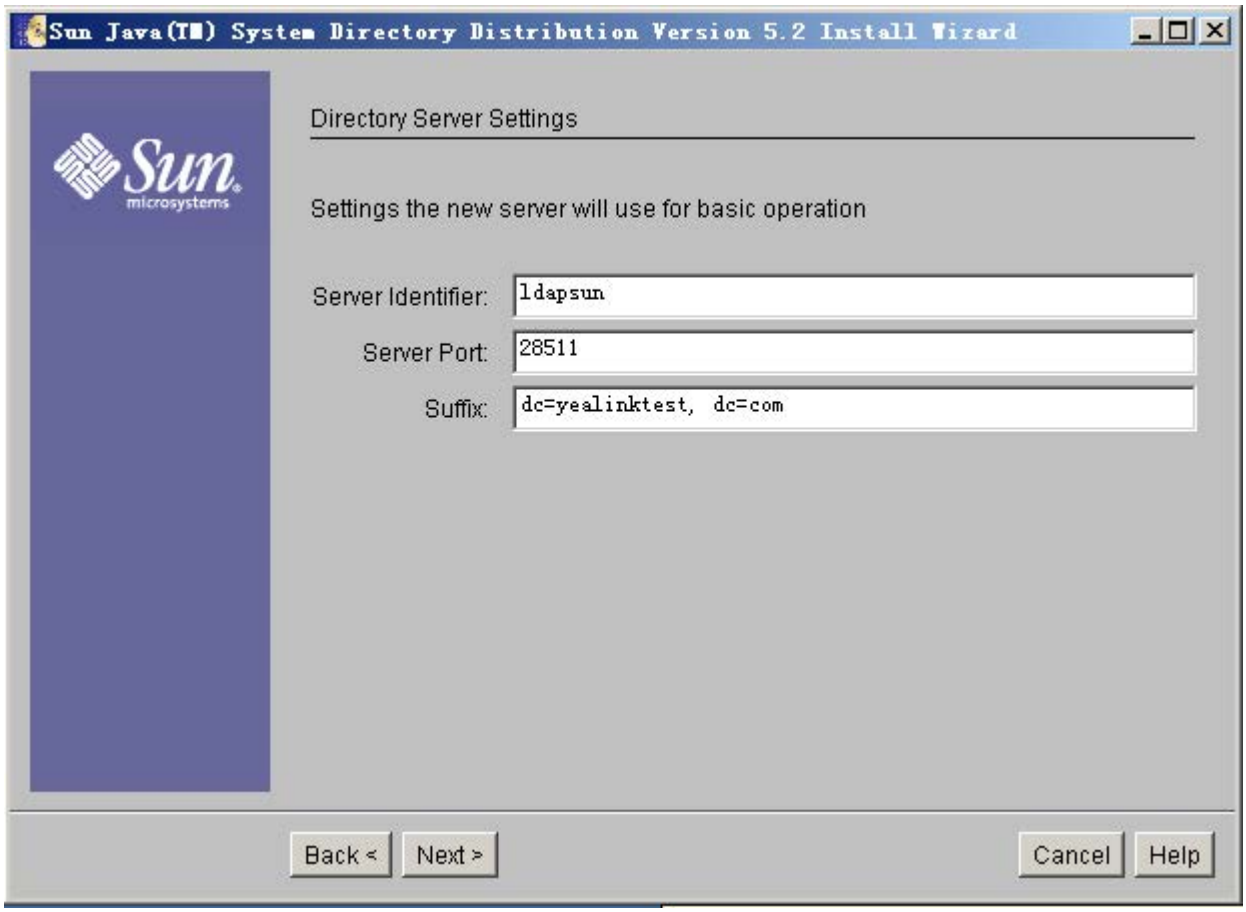
10. Select **The new instance will be the configuration Directory Server** check box, and click **Next**.



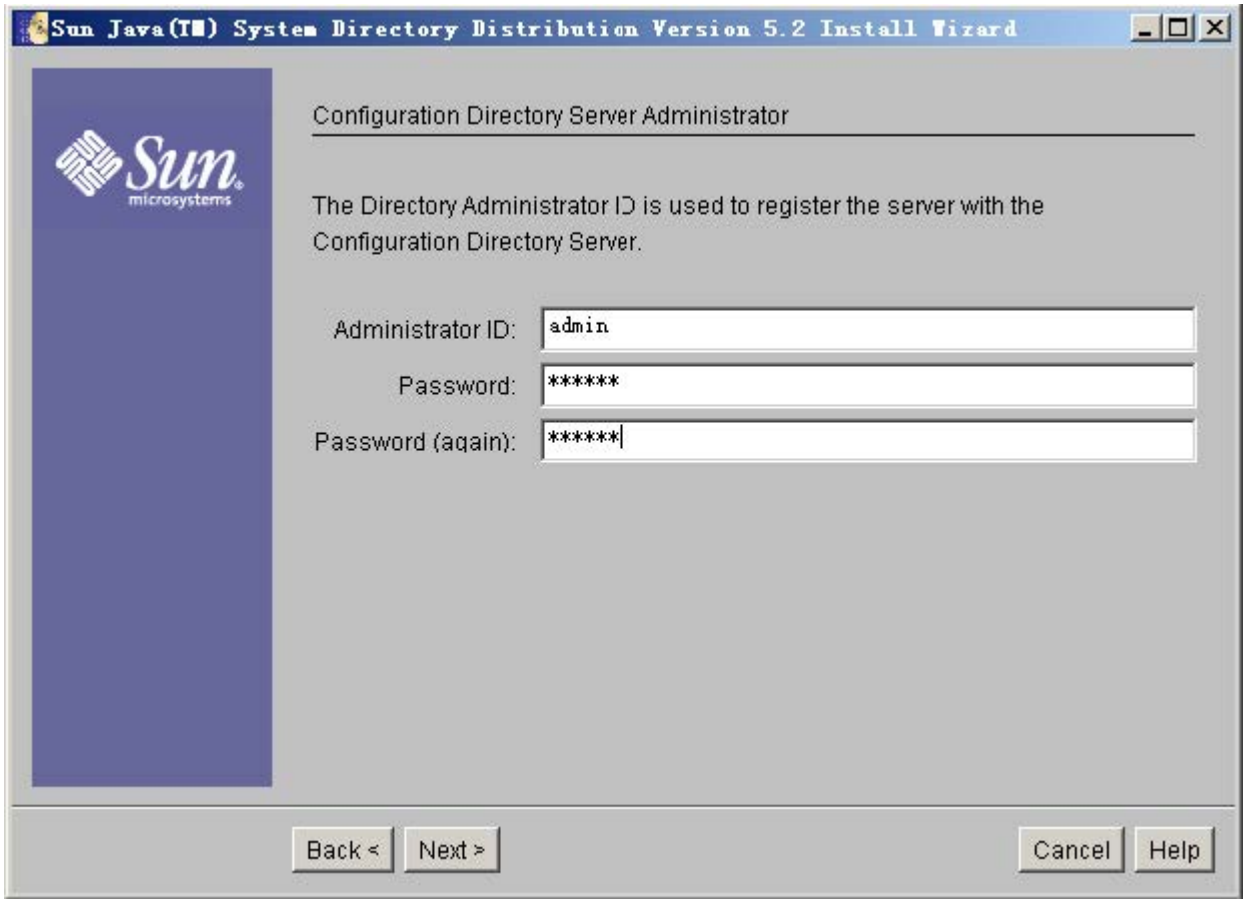
11. Select the **Store data in the new Directory Server** check box and click **Next**.



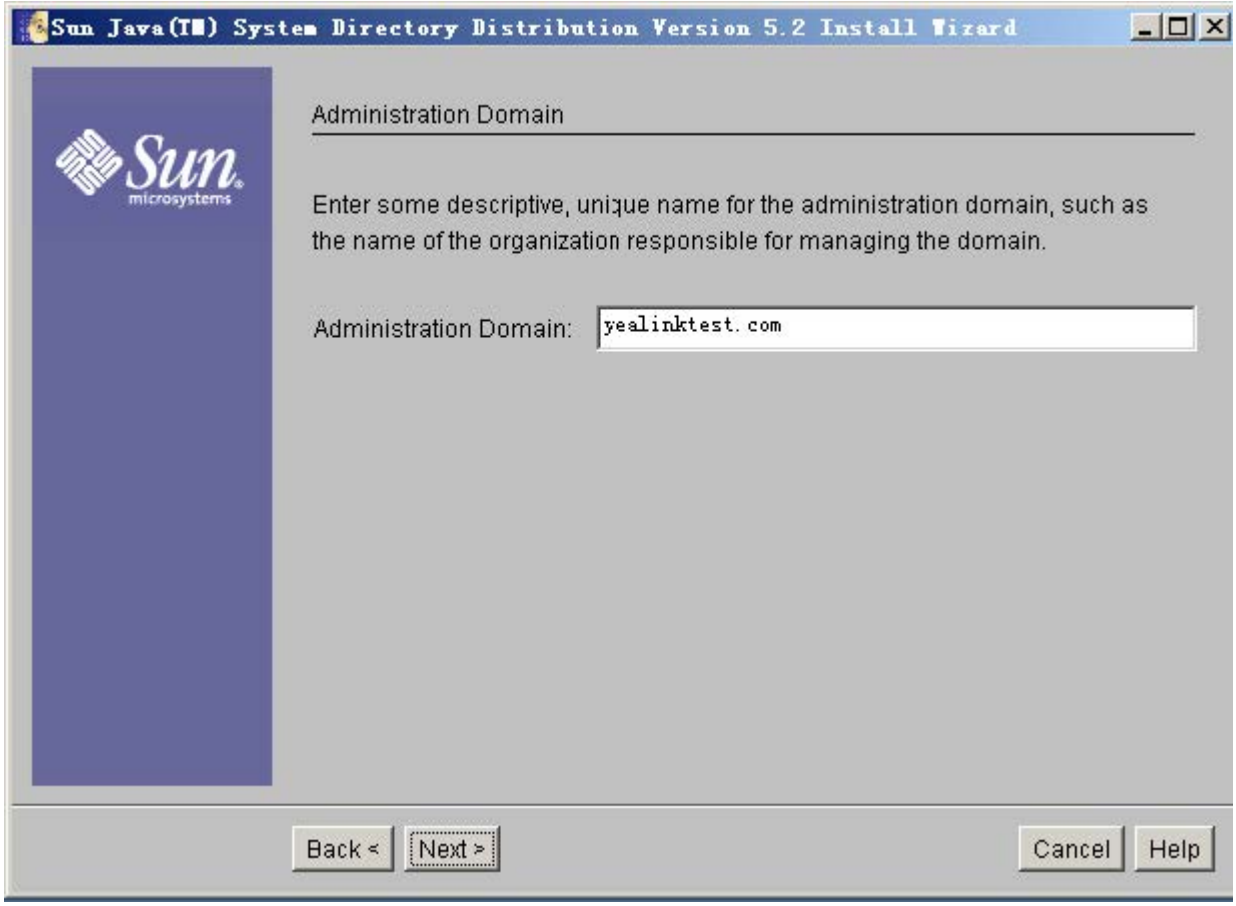
12. Enter the value "ldapsun" in the **Server Identifier** field and keep the default values in the other two fields. And then click **Next**.



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

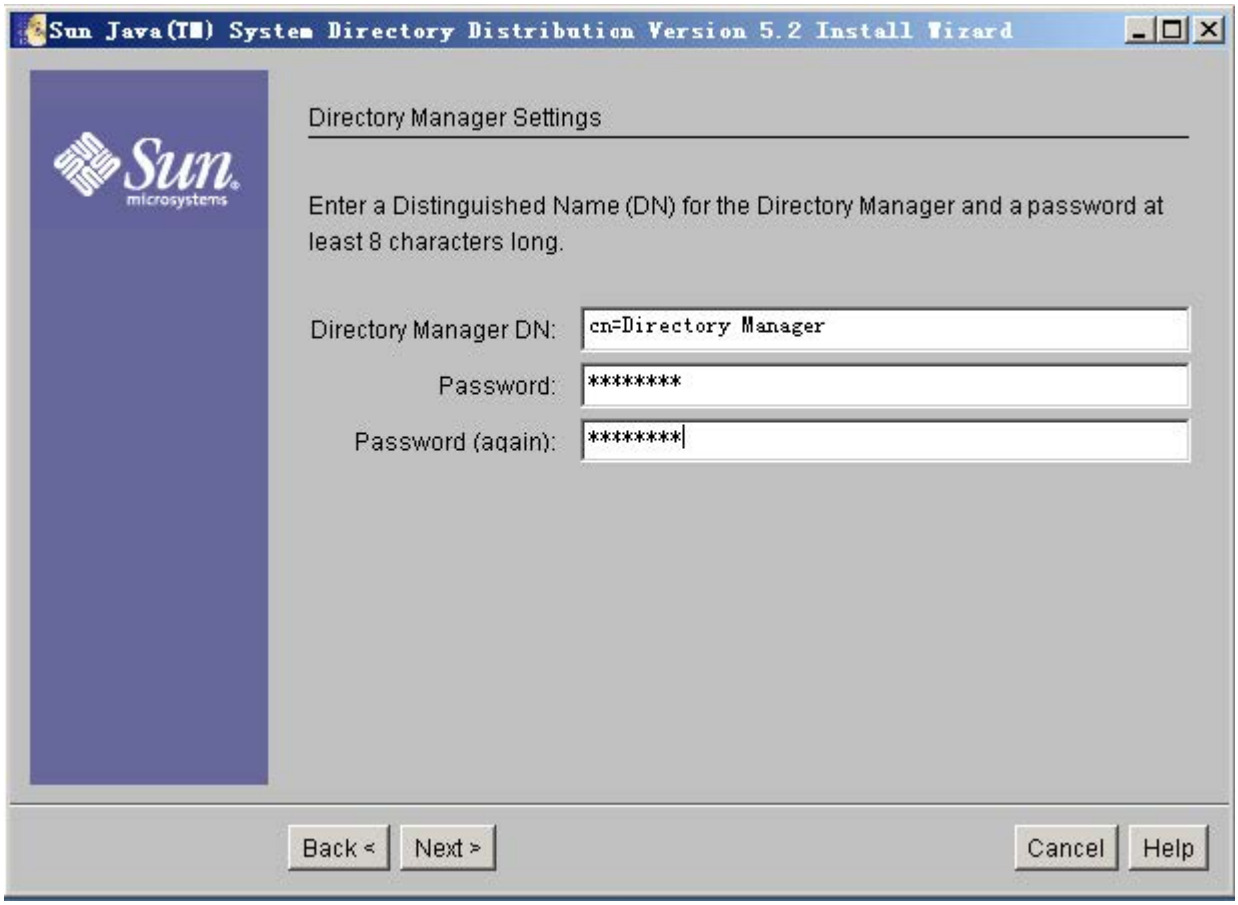


14. Follow the default setting and click **Next**.

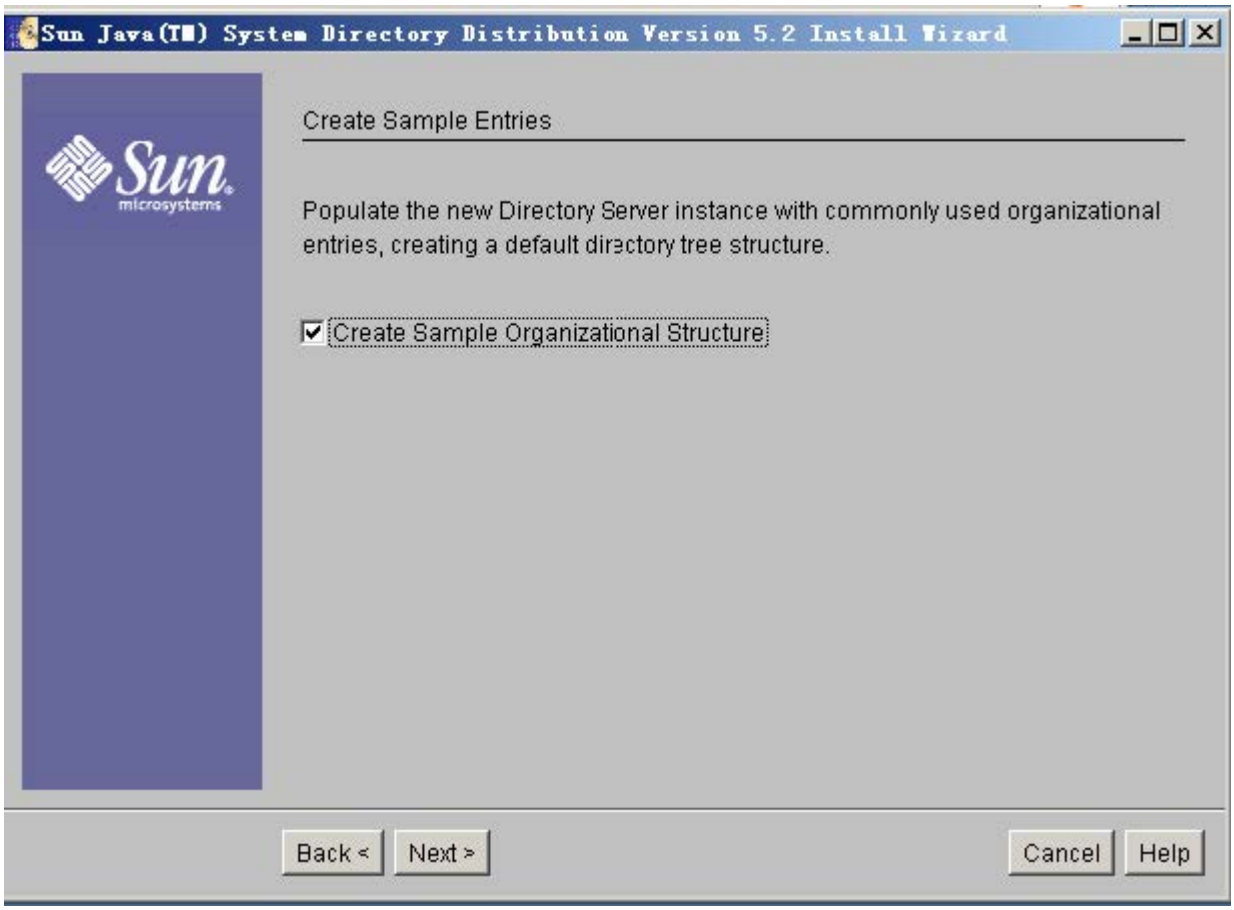


15. Configure the password for the Directory Manager and click **Next**.

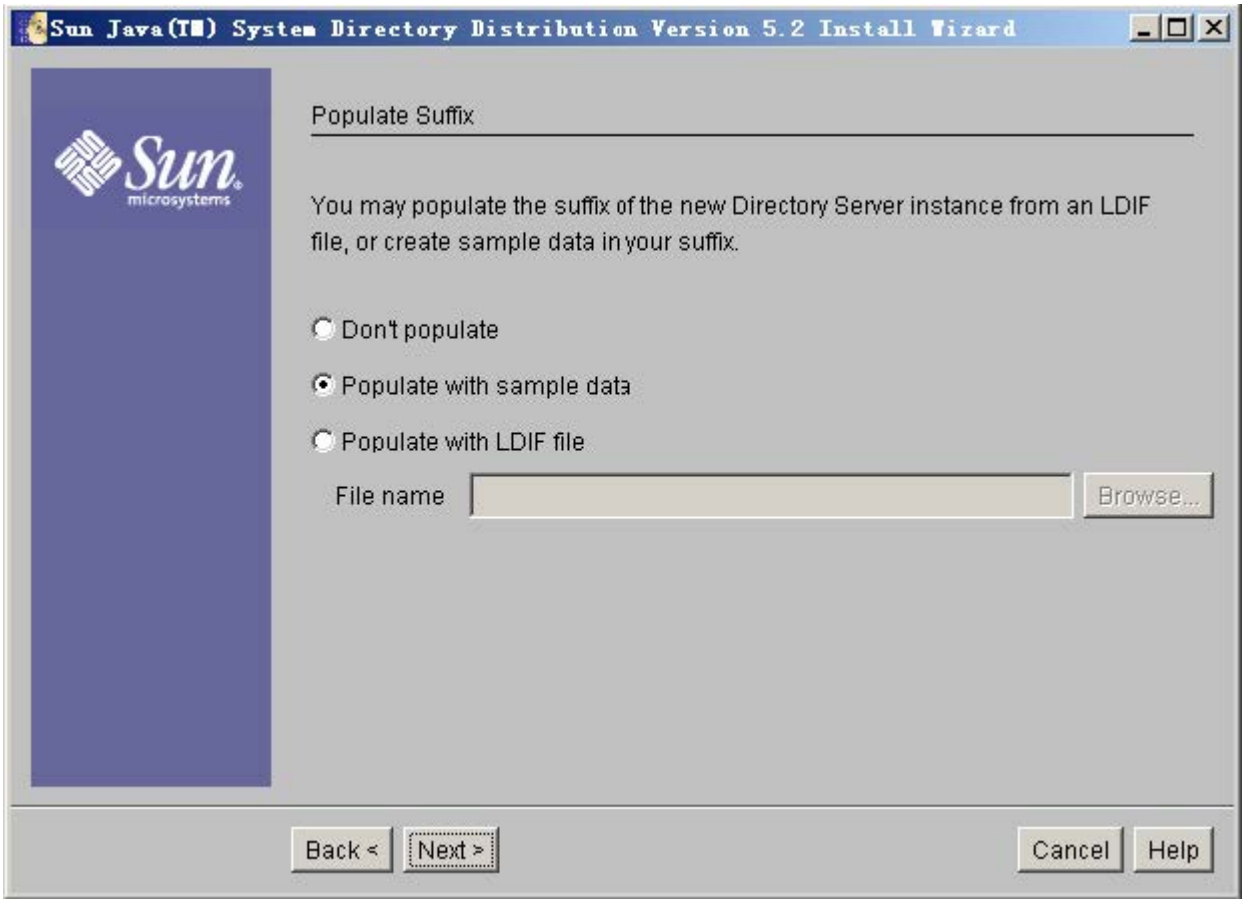
    The password must be at least 8 characters long.



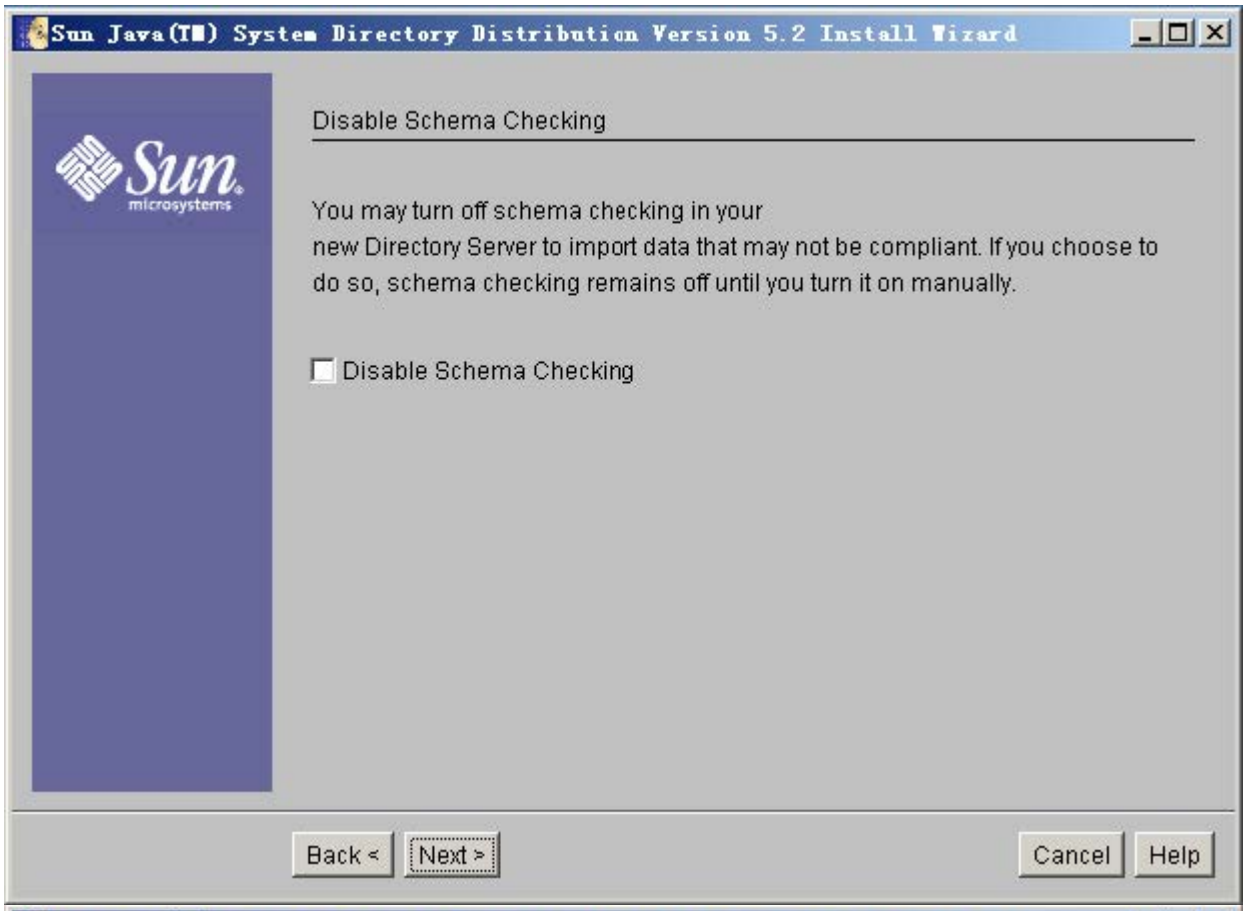
16. Select the **Create Sample Organizational Structure** check box and click **Next**.

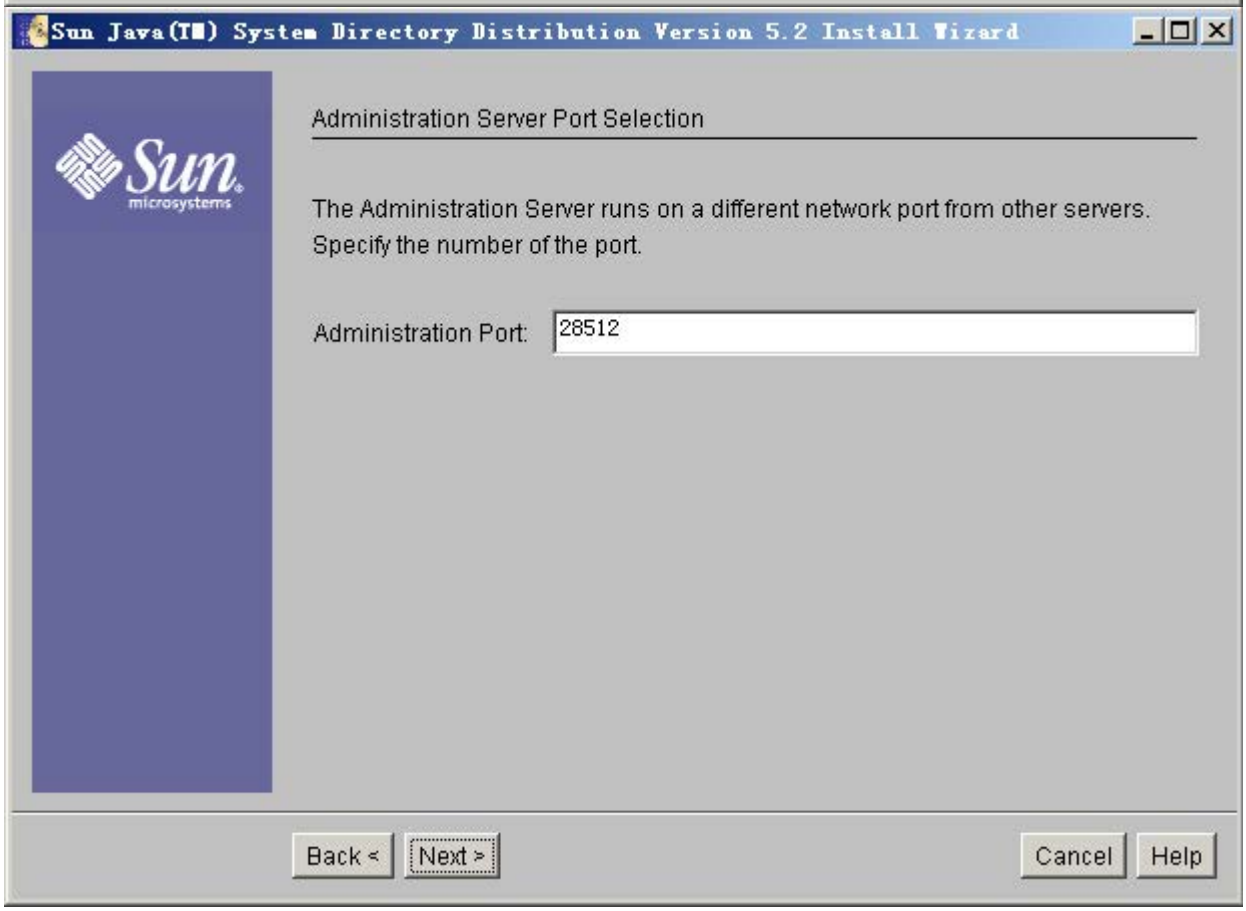


17. Select the **Populate with sample date** check box and click **Next**.

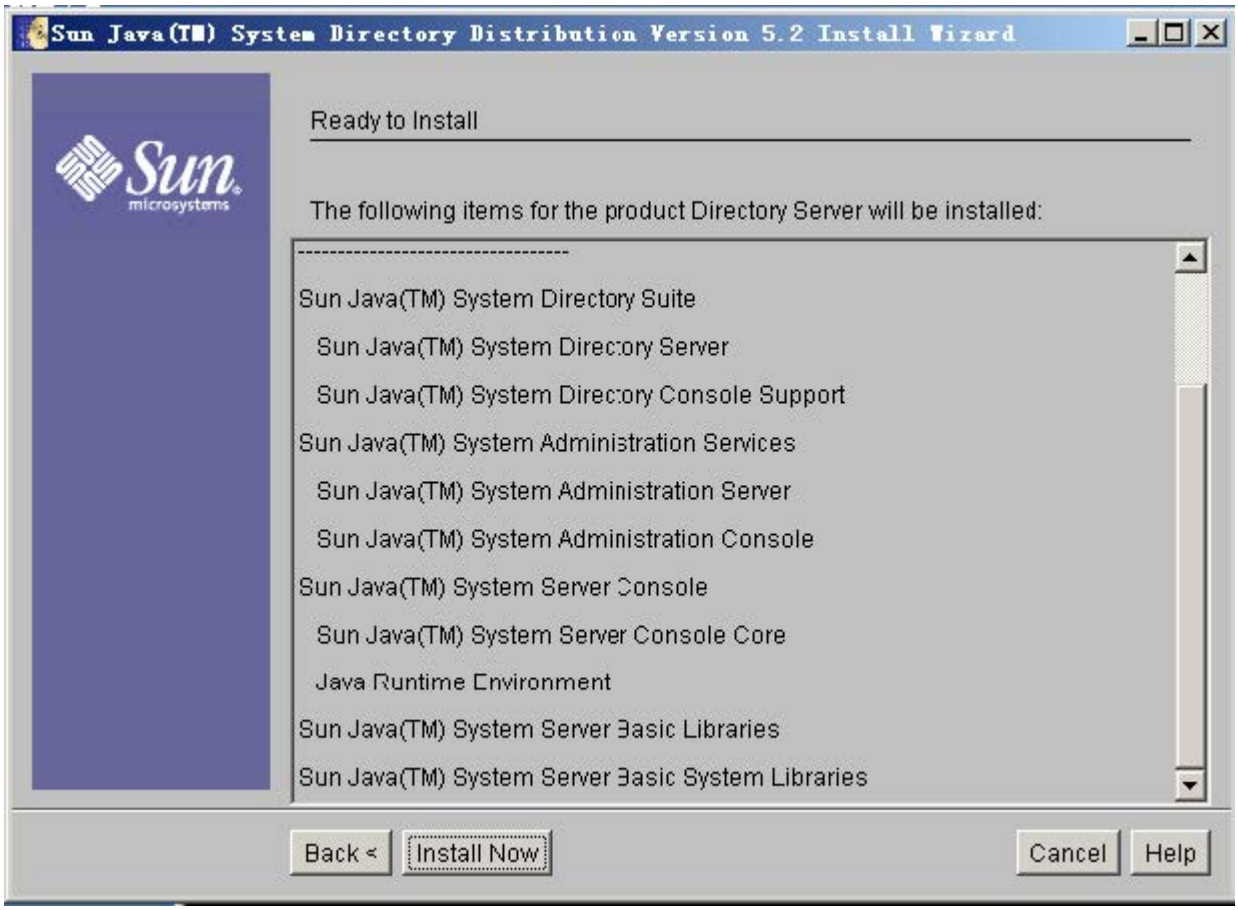


18. Follow the default settings and click **Next** for the following two steps.

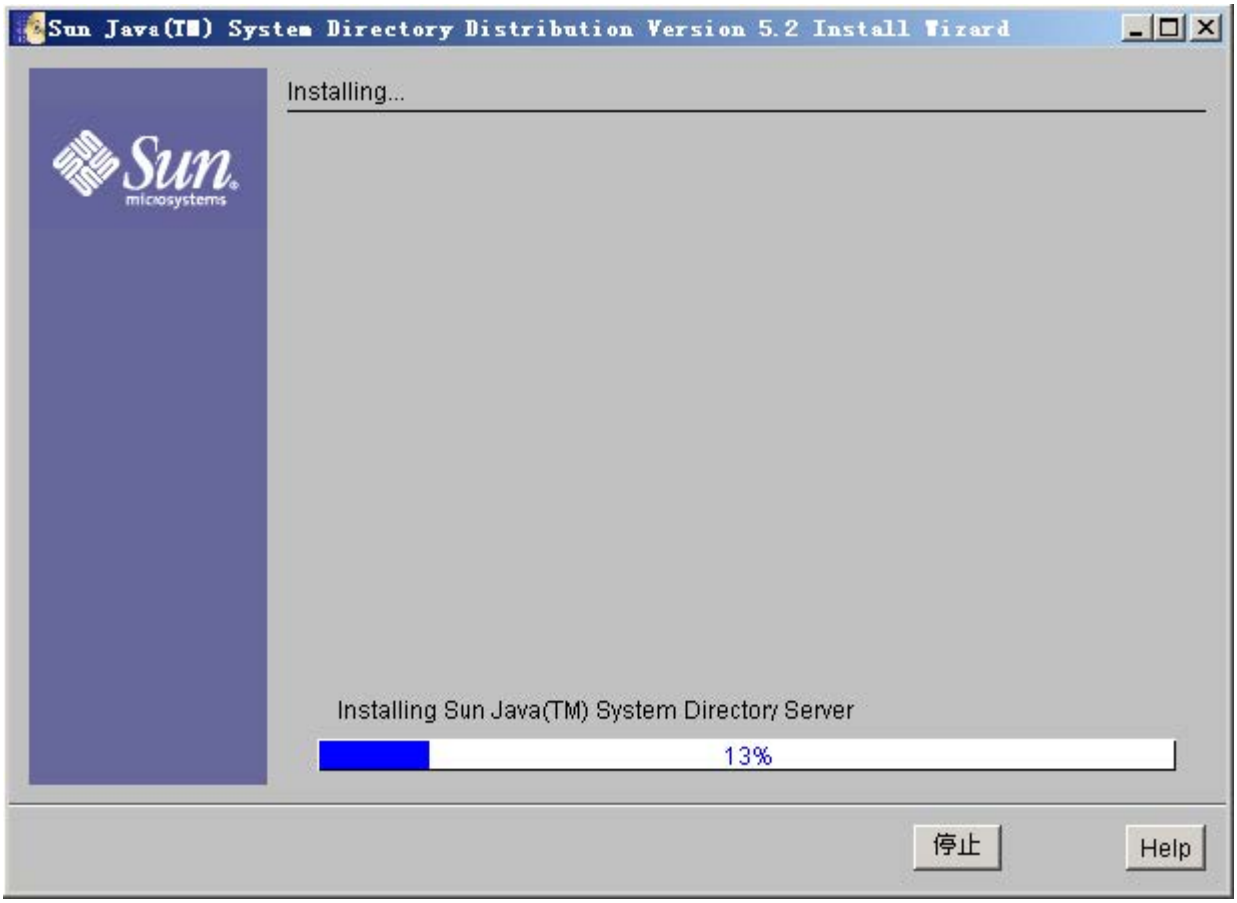




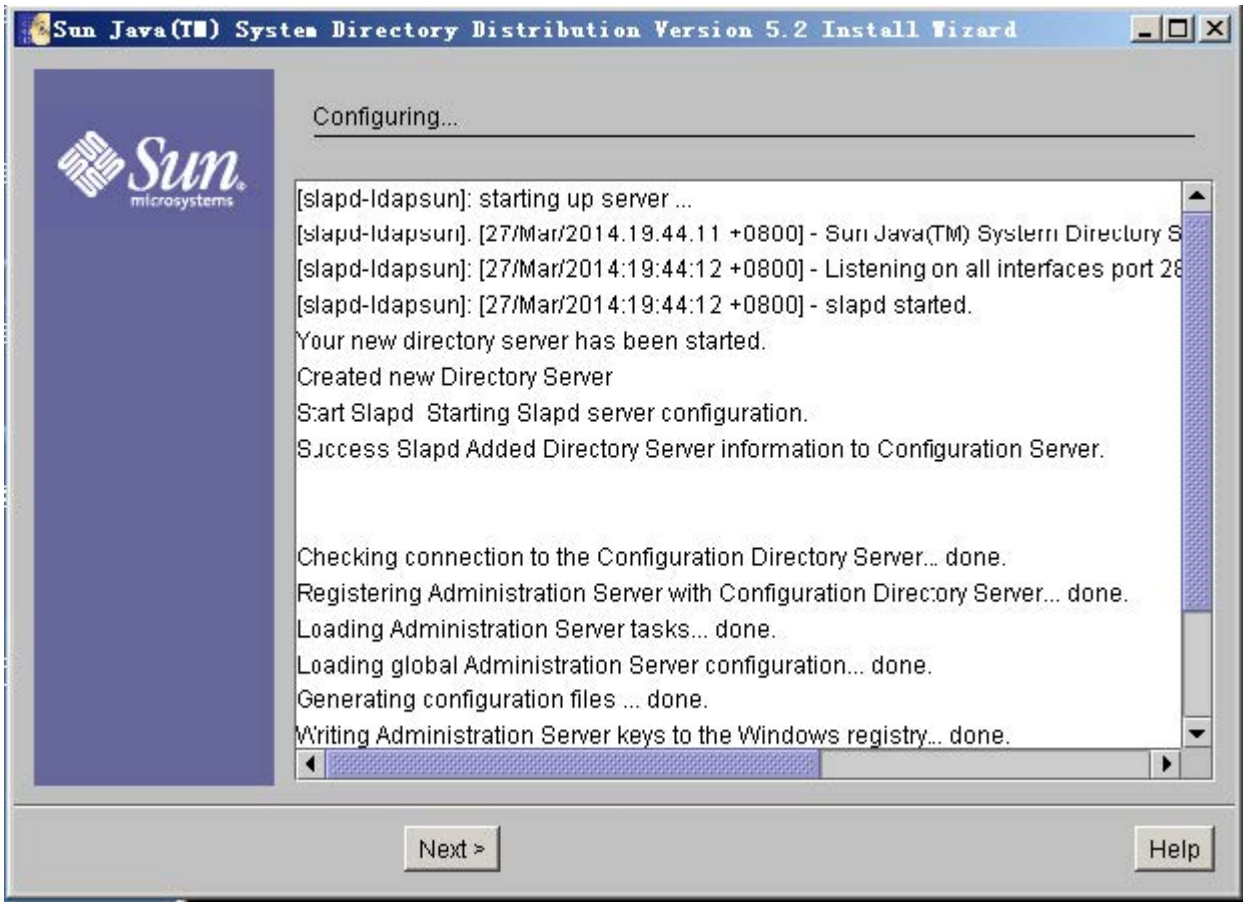
19. View the items to be installed and click **Install Now**.



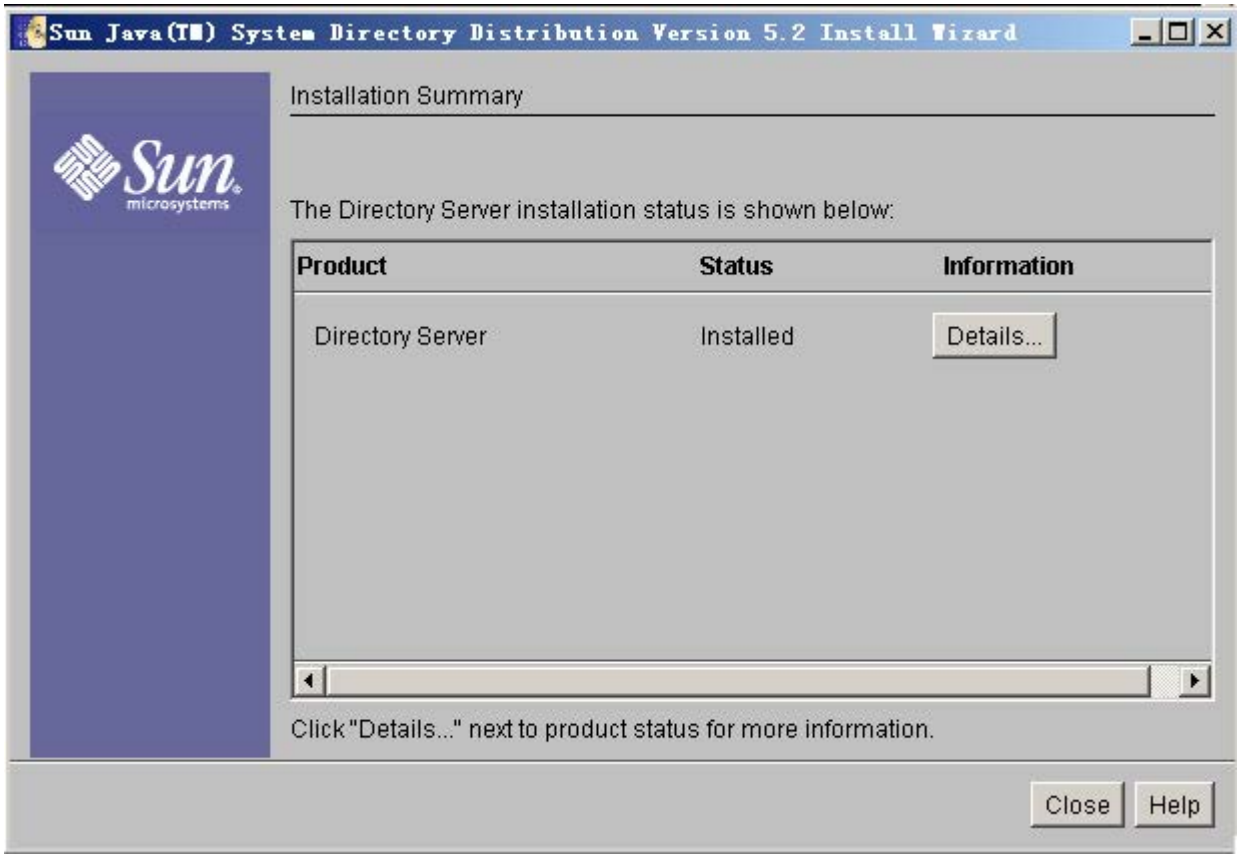
21. The installation progress is shown as below:



23. After the installation, it will enter the configuration 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

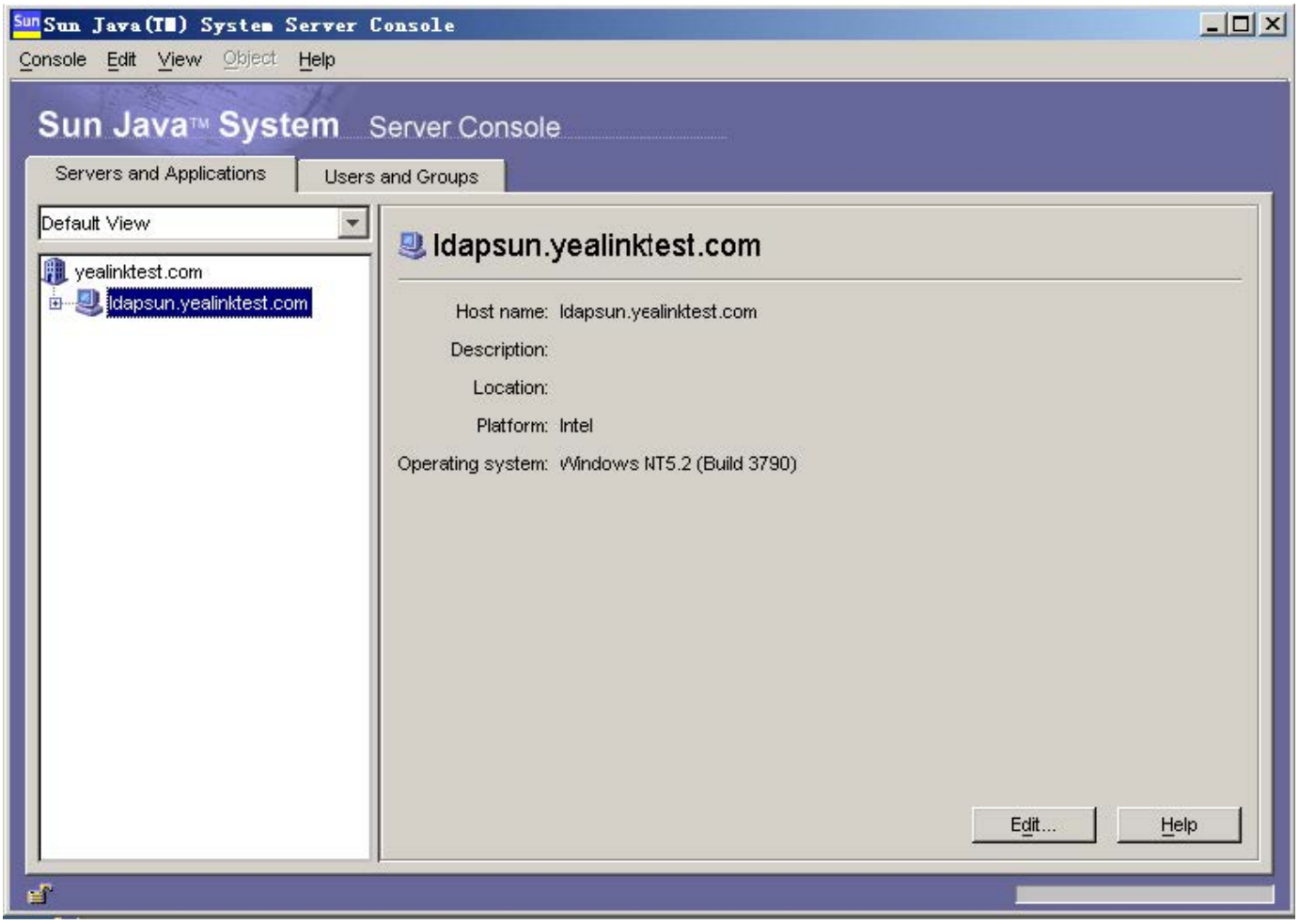
You can add entries to the Directory Server one by one in this way.

To add an entry to the Directory Server:

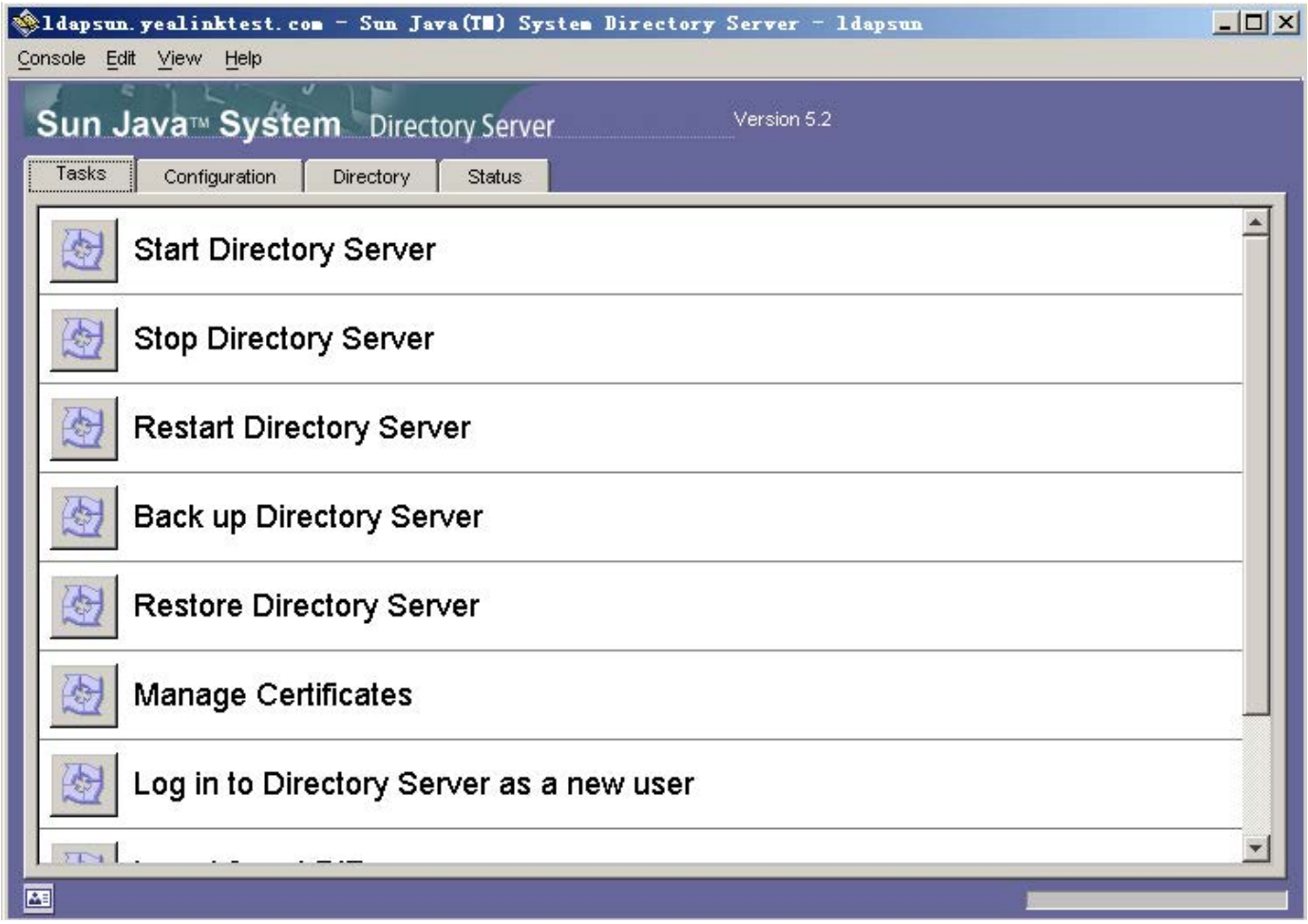
1. Click **Start** > **Program** > **Sun Java™ System Server Products** > **Sun Java™ System Server Console 5.2.**
2. It will enter the login screen. You should enter the administrator user name and its password in the **User ID** field and **Password** field respectively.

> 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.

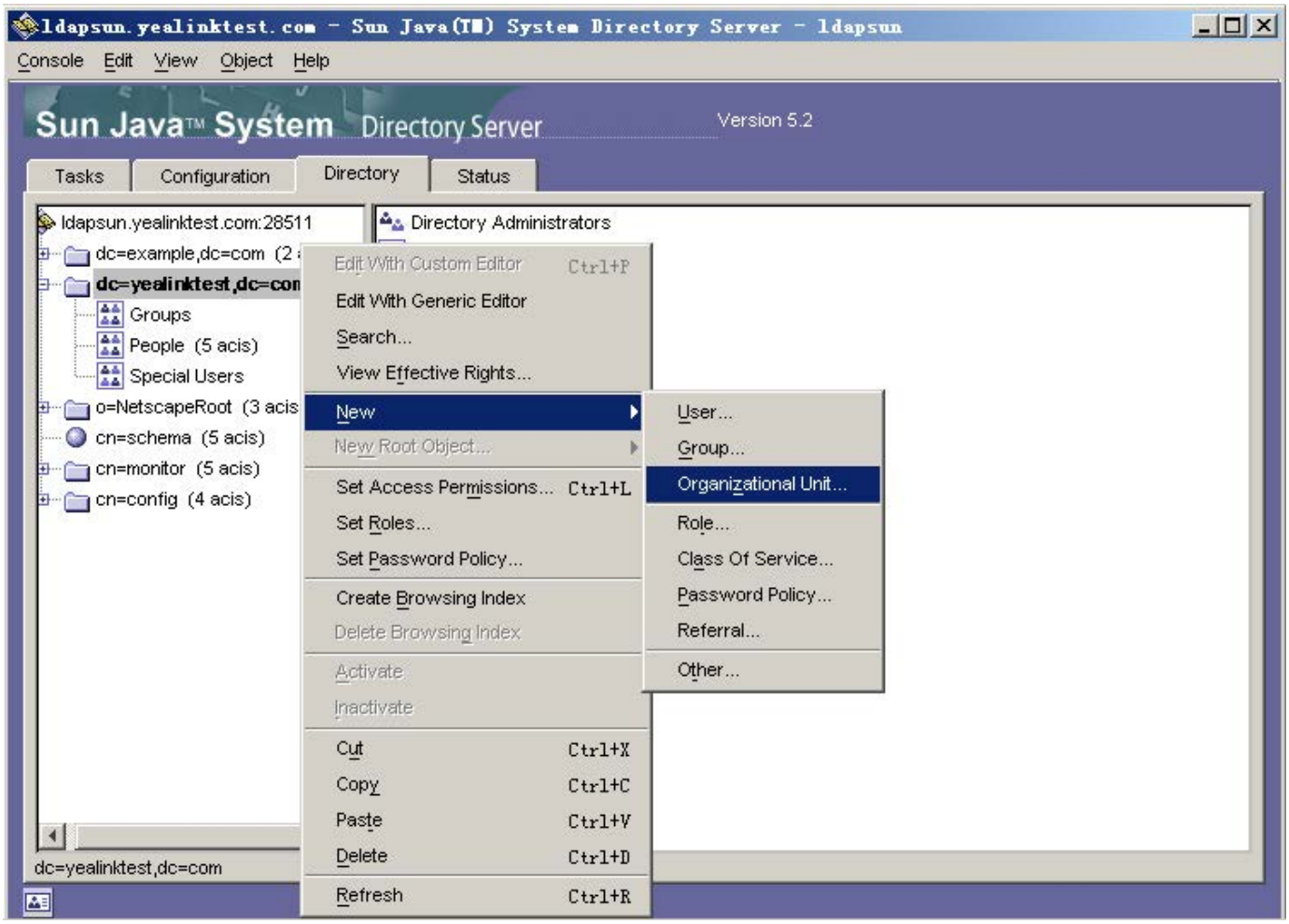
Then click **OK** to enter the home page.



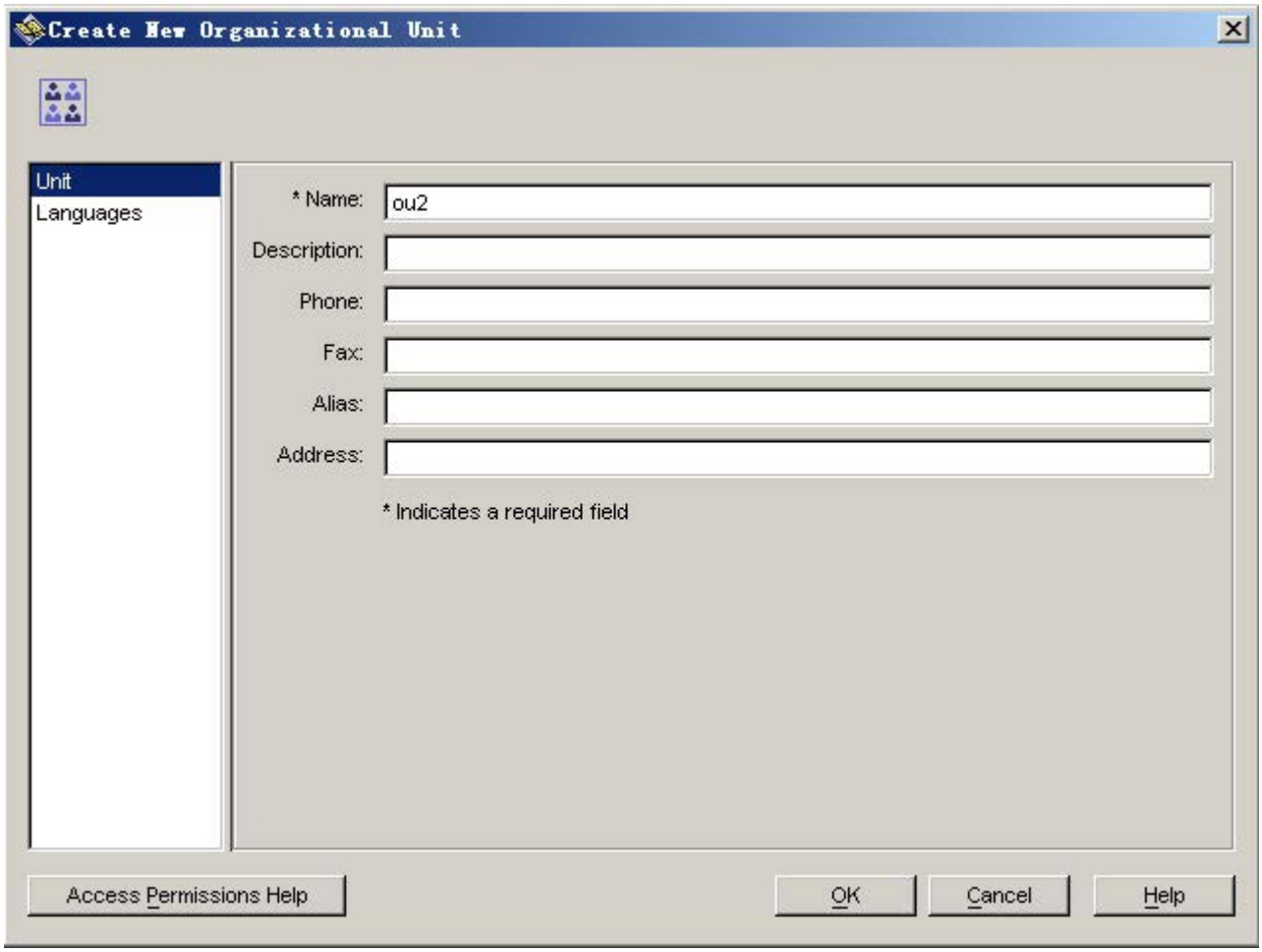
2. Double click **ldapsun.yealinktest.com** > **Server Group** > **Directory Server(ldapsun)**. It will enter the Directory Tasks interface.



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

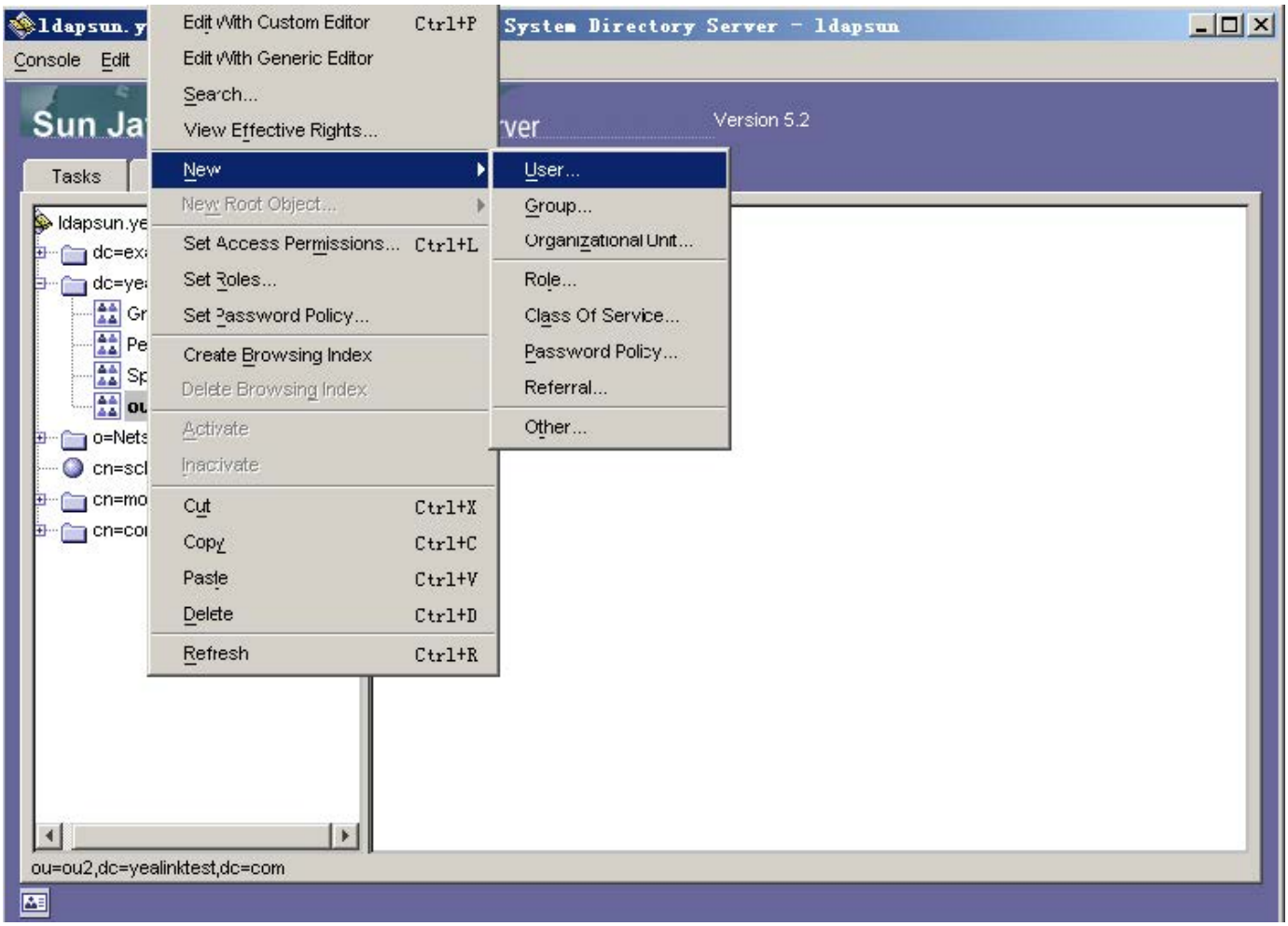


5. Enter the desired name of the organizational unit.

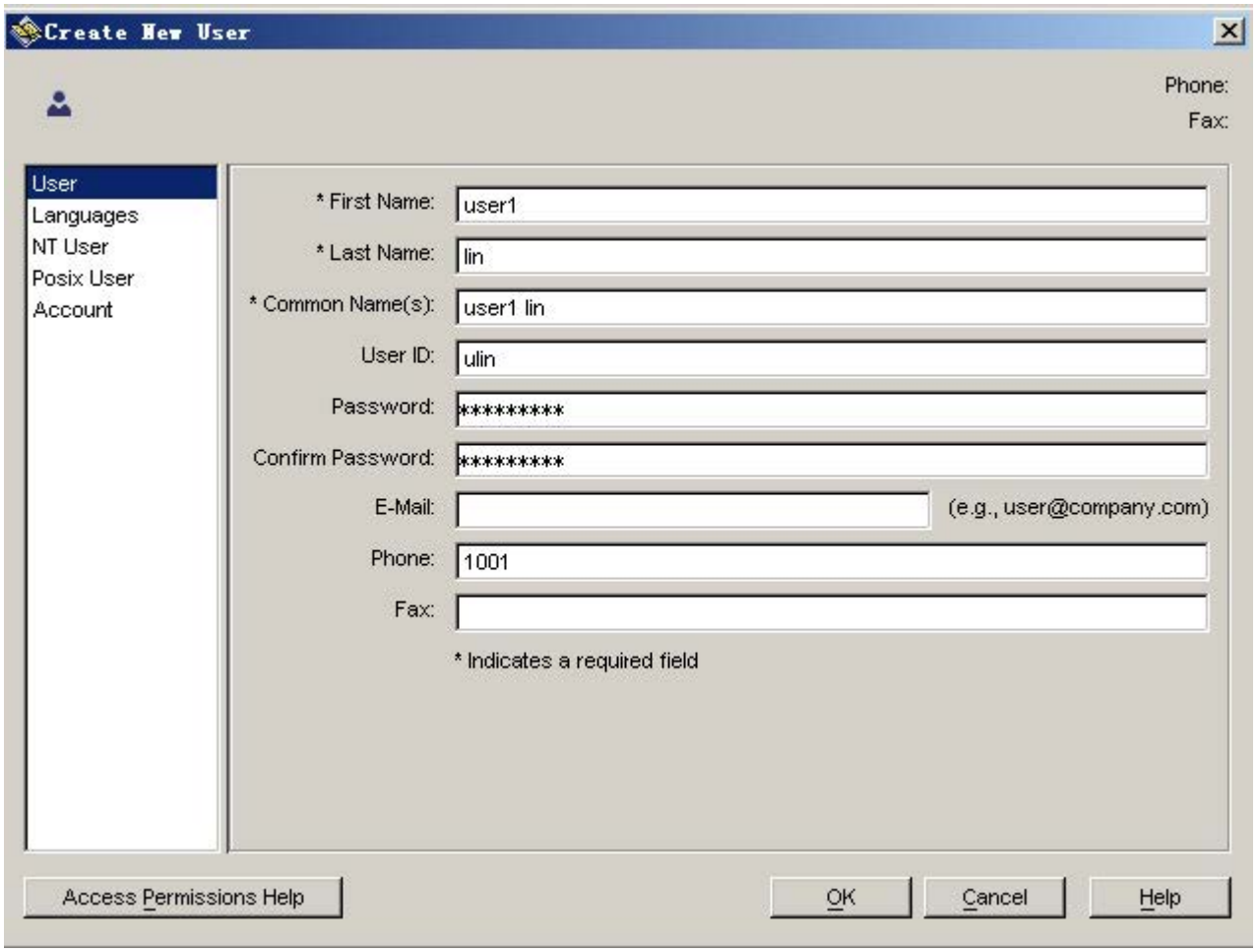


6. Click **OK** to accept the change.

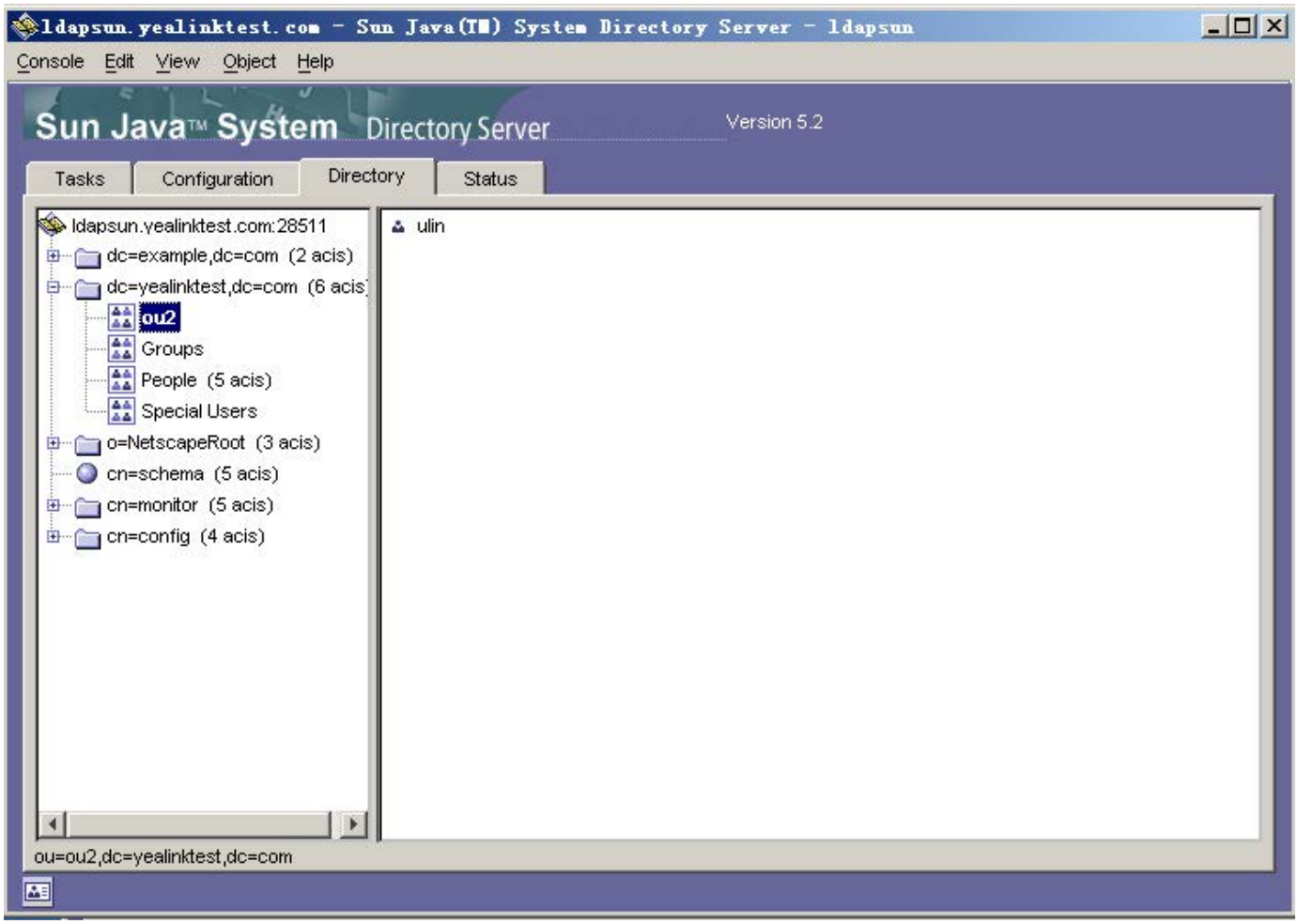
7. Select and right-click the organizational unit created above, and then select **New** > **User**.



8. Enter the desired values in the corresponding fields.



9. Click **OK** to accept the change.
10. 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. The following shows an example of the content of the LDIF file for the Directory Server:

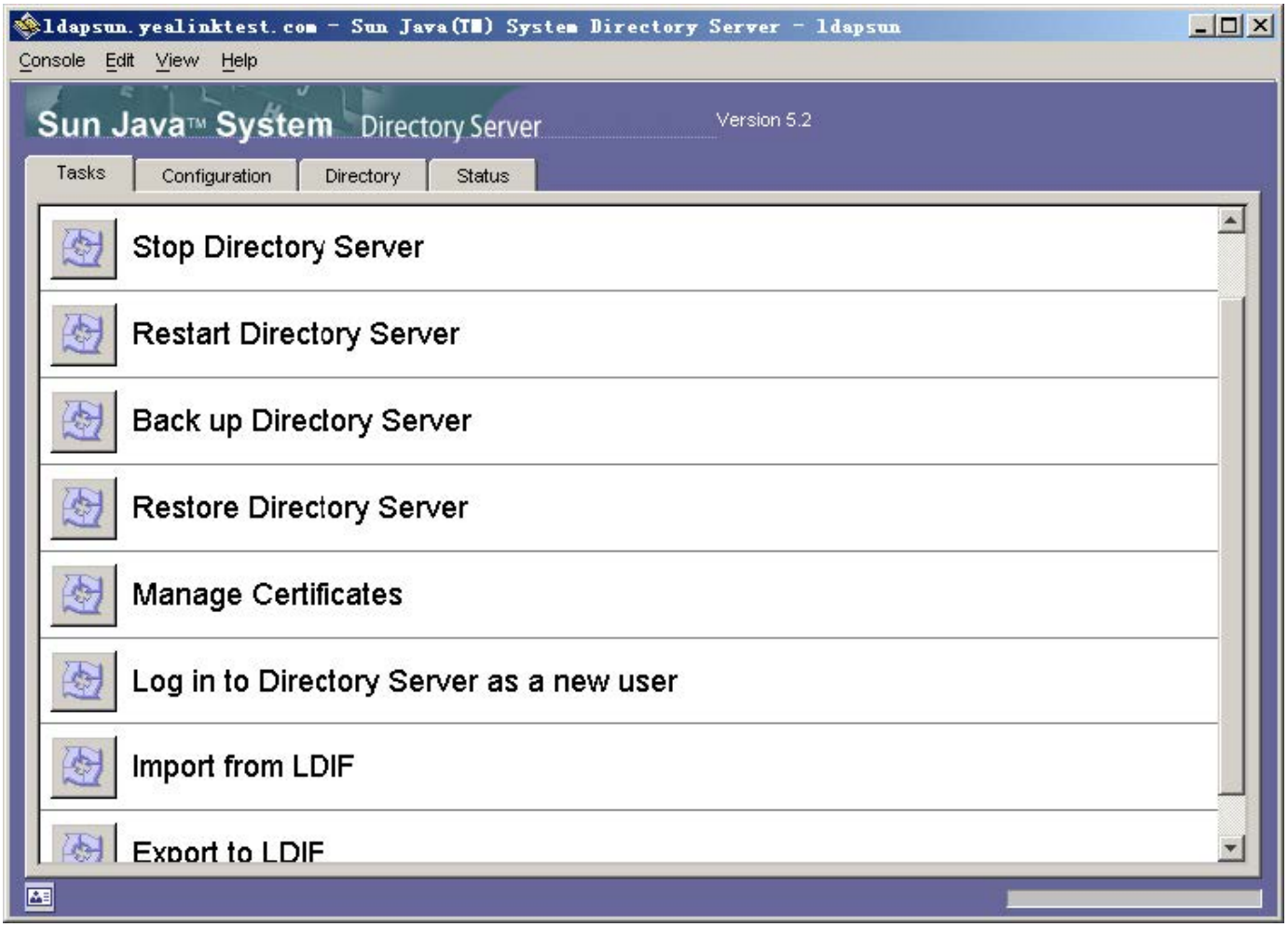
```
##Create a new organizational unit##
dn: ou=ou3,dc=yealinktest,dc=com
ou: ou3
objectClass: top
objectClass: organizationalunit
creatorsname: cn=directory manager
modifiersname: cn=directory manager
parentid: 1
entryid: 15
entrydn: ou=ou3,dc=yealinktest,dc=com

##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
```

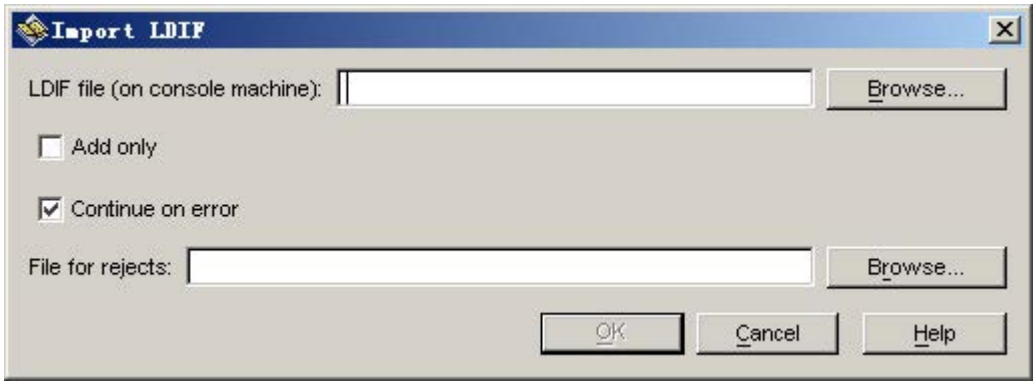
To import the test.ldif file:

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

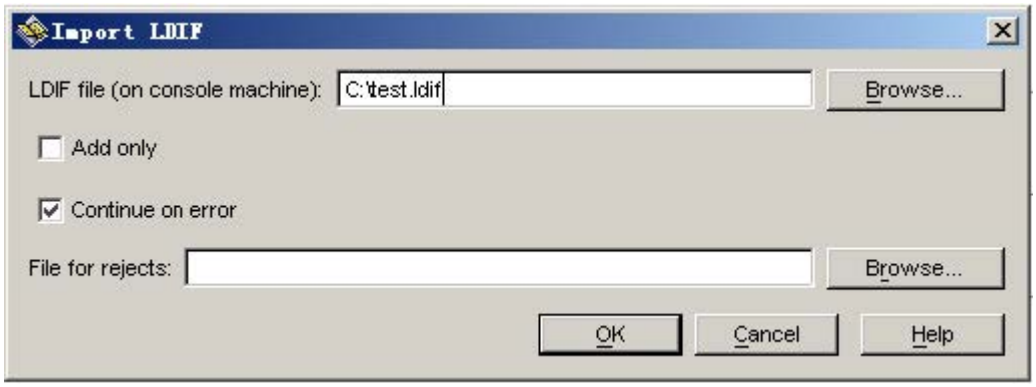
It will enter the Directory **Tasks** interface.



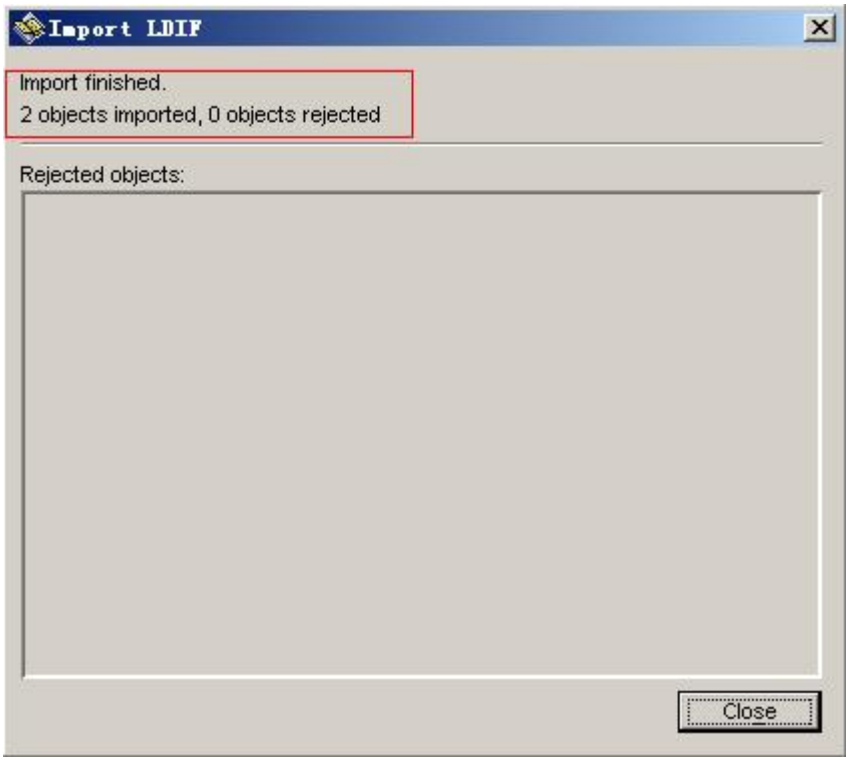
1. Click **Import from LDIF**.



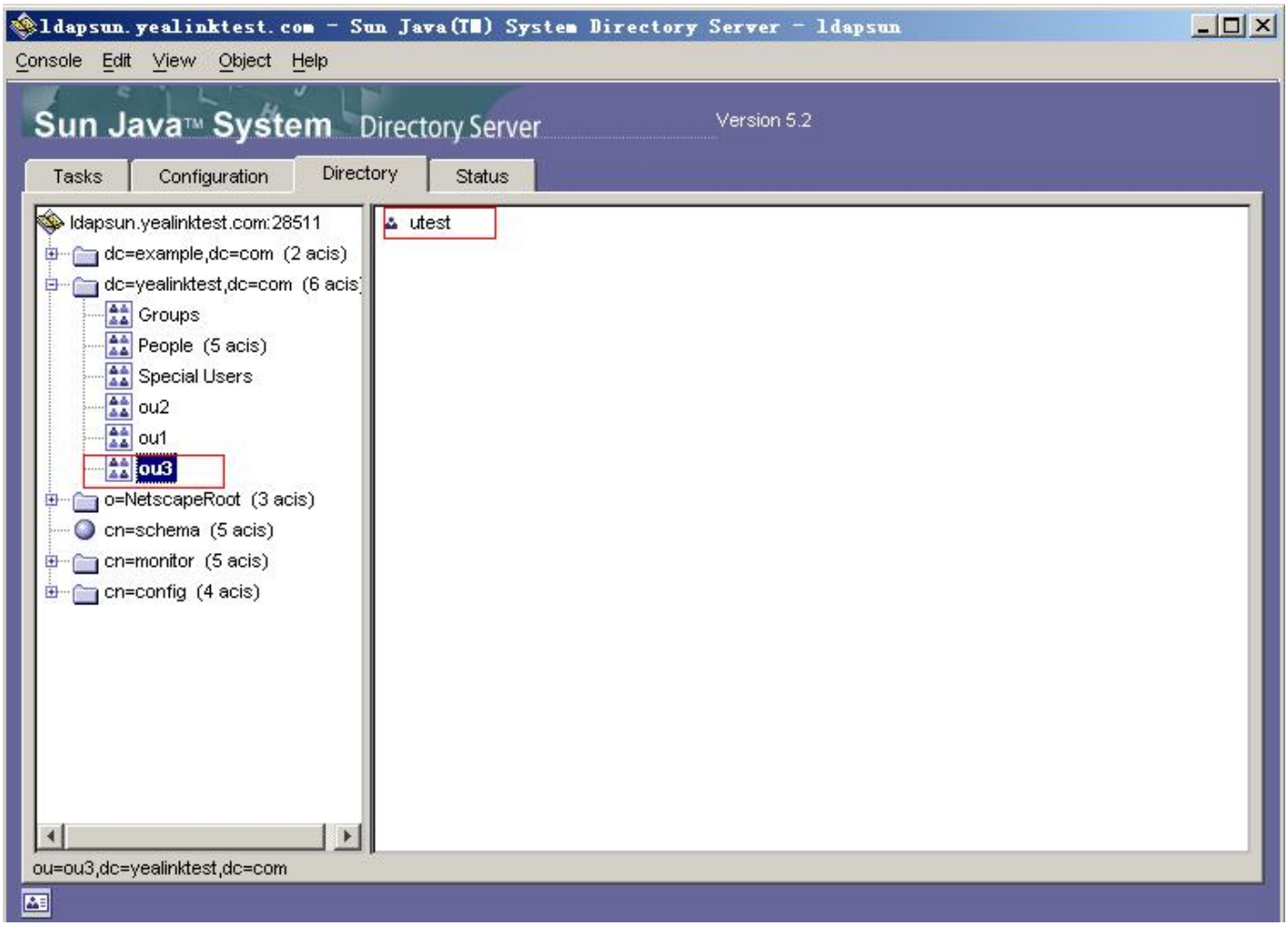
2. Click **Browse** to locate the test.ldif file from your local system, and then click **OK**.



4. 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.



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


ldapsun.yealinktest.com - Sun Java(TM) System Directory Server - ldapsun
Console Edit View Object Help
Sun Java™ System Directory Server
Version 5.2
Tasks
Configuration
Directory
Status
ldapsun.yealinktest.com:28511
dc=example,dc=com (2 acis)
dc=yealinktest,dc=com (6 acis)
Groups
People (5 acis)
Special Users
ou2
ou1
ou3
o=NetscapeRoot (3 acis)
cn=schema (5 acis)
cn=monitor (5 acis)
cn=config (4 acis)
utest
ou=ou3,dc=yealinktest,dc=com

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 IP phone can establish a connection with the remote server and 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.

> 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 the remote phone book template. You can also refer to the following template:

```
html<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.

Templat	Element	Valid Values

e		
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>.

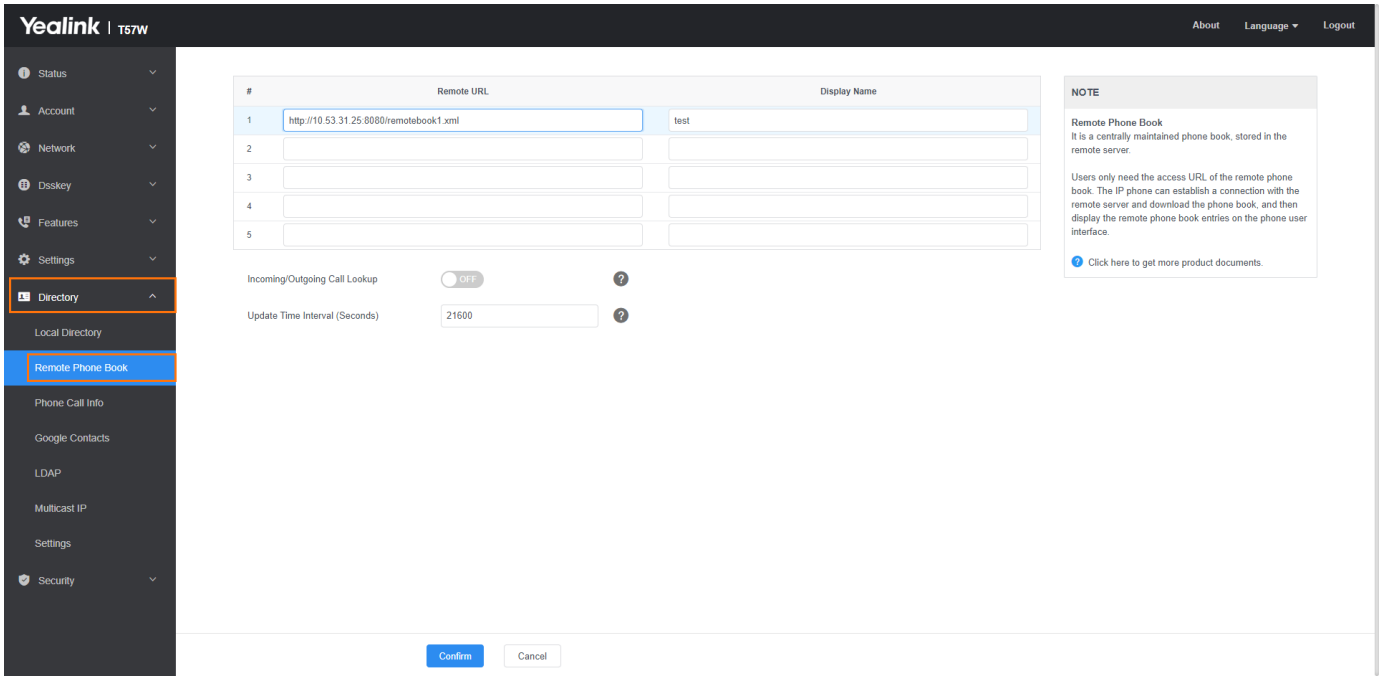
Customize Remote Phone Book File

1. Add contacts in a Department.xml file. Each starts on a new line.
2. For example,
3. <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.
5. For example,
6. <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 on 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. The size of a remote phone book file should be less than 1.5 M.
remote_phonebook.data	String within 99	Blan	It configures the display name of the remote phone book item.

.X.name[1]	characters	k	
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 the handset can access. Multiple values are separated by commas. 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
0x00090000106 0000 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 can do further analysis.
0x00090000106 0001 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.
0x00090000106 0002 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 displays allow file downloading up to 768 KB. Therefore, you need to control the size of the file to be downloaded, for example, the resource file uploaded by users.
0x00090000106	Phone configuration	1. Choose one of the following methods to configure the correct authentication information for the phone:

0003 Auth Error	error. XML file authentication failed.	- 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 can do further analysis.
0x00090 0000106 0004 network unavaila ble	Network error, causing downloading failure.	Check whether the network between the phone and the server is available by using the phone's Ping feature.
0x00090 0000106 0005 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. 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.

			Contacts with multiple numbers are counted as only one contact.

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

Handset XML Phonebook Configuration

Configuration parameter

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

handset.X.xml_phonebook.data.url
handset.X.xml_phonebook.data.name
handset.X.xml_phonebook.data.username
handset.X.xml_phonebook.data.password

Parameter	Permitted Values	Default	Description
handset.X.xml_phonebook.data.url[1]	String within 512 characters	Blank	It configures the requested URL of the XML phonebook. The contacts in the XML phonebook are all in the first level, and any nesting is not allowed.
handset.X.xml_phonebook.data.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.
handset.X.xml_phonebook.data.username[1]	String within 64 characters	Blank	It configures the authentication user name to request the XML phonebook.
handset.X.xml_phonebook.data.password[1]	String within 64 characters	Blank	It configures the authentication password to request the XML phonebook.

[1]X is the handset ID.

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 that contain the entered character(s). **1**-Prefix matching, the phone will search the contact numbers or names that start with the entered character(s).	0	It configures the search type when searching the contact in 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. 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 as +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 a certain matched one of the contact number.
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 a certain matched one of the caller's phone number.

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. It works only if your firmware version is x.86.0.112 or later.
phone_setting.call_number_display.replace.with	String within 512 characters	Blank	It configures the string used to replace a certain matched one of the caller's phone display number. It works only if your firmware version is x.86.0.112 or later.

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.

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 in 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.

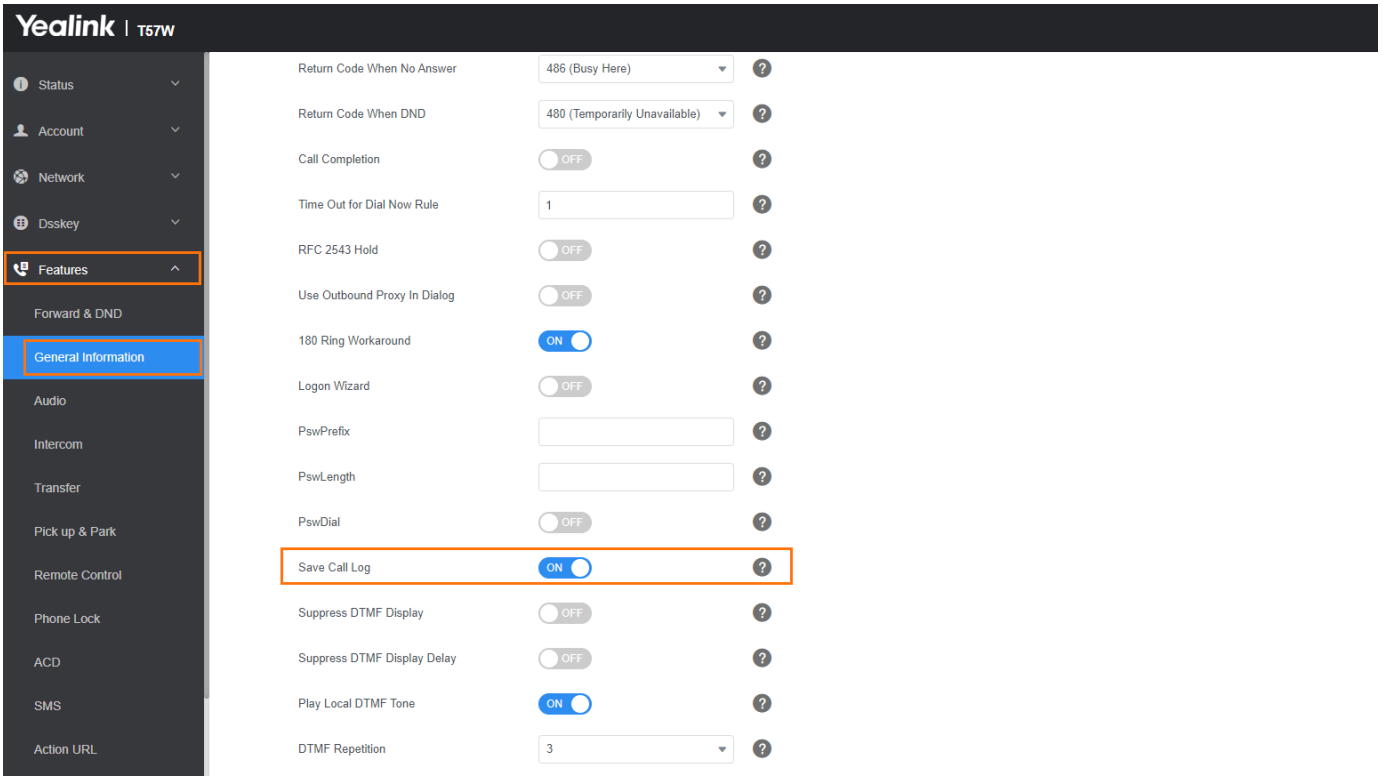
Display Field	Description
Name	Shows the name of the remote party.
Number	Shows the number of the remote party.
Time	Shows the call initiation time.
Duration	Shows the duration of the call.
Relation	Shows what happened to the call. The valid display contents are: • **Rejected**: Reject an incoming call. • **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	Permitted Values	Default	Description

features.save_call_history	0-Disabled, the phone cannot log the placed calls, received calls, missed calls, and forwarded calls in the call lists. 1-Enabled	1	It enables or disables the phone to log the call history (missed calls, placed calls, received calls, and forwarded calls) in the call lists. To log the missed calls, "account.X.missed_calllog" should be set to 1 (Enabled).
account.X.missed_calllog[1]	0-Disabled 1-Enabled	1	It enables or disables the phone to record missed calls for account X. It works only if "features.save_call_history" is set to 1 (Enabled).
pstn.account.X.missed_calllog[2]	0-Disabled, the phone does not display 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-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	It enables or disables the phone to indicate and record missed calls for the PSTN account X. 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).
features.call_log_show_num	0-Name, the name is displayed preferentially; if there is no name, the	0	It configures the display type of the other parties' information in the call log lists. It works only if "features.save_call_history" is set

	number is displayed 1-Number 2-Name & Number, the name and number are displayed; if there is no name, the number is displayed		to 1 (Enabled).
features.calllog_detailed_information	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	It enables or disables the phone to indicate what happened to the call in the call log list. 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. It works only if "features.save_call_history" is set to 1 (Enabled).
features.save_init_num_to_history.enable	0-Disabled, the phone will log the transfer-to party's phone number in the call history list. 1-Enabled	1	It enables or disables the phone from logging the transfer party's phone number in the call history list.
features.call_out_history_by_off_hook.enable	0-Disabled 1-Enabled	0	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.
features.call_log_merge.enable	0-Disabled, each call is logged individually in the calls list. 1-Enabled,	0	It enables or disables the phone from merging the same history records. The merged entry only displays the initiation time of the last call.

	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.		
features.local_calllog.received.replace_rule	String	Blank	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. The records in the Placed Calls are not matched.

[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 IP phone. For example, if the MAC address of an

IP phone is 00156574B150, the name of the call log file is 00156574B150-calllog.xml (uppercase).

> MAC address, a unique 12-digit serial number, is assigned to each phone. You can obtain it from the barcode on the back of the IP 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	Permitted Values	Default	Description
static.auto_provision.local_calllog.backup.enable	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	0	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.

	auto provisioning.		
static.auto_provision.local_calllog.backup.path	String	Blank	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". It works only if "static.auto_provision.local_calllog.backup.enable" is set to 1 (Enabled).
static.auto_provision.local_calllog.write_delay.terminated	Integer from 10 to 600	60	It configures the delay time (in seconds) for the phone to upload the <MAC>-calllog.xml file each time the call logs update. It works only if "static.auto_provision.local_calllog.backup.enable" 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).

Google Contacts

Google Contacts

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

Google Contacts Configuration for Desk Phone

The following table lists the parameters that the phone can use to connect to the Google Contact Server. It is not applicable to T48G/T46G/T42G/T41P/T29G phones.

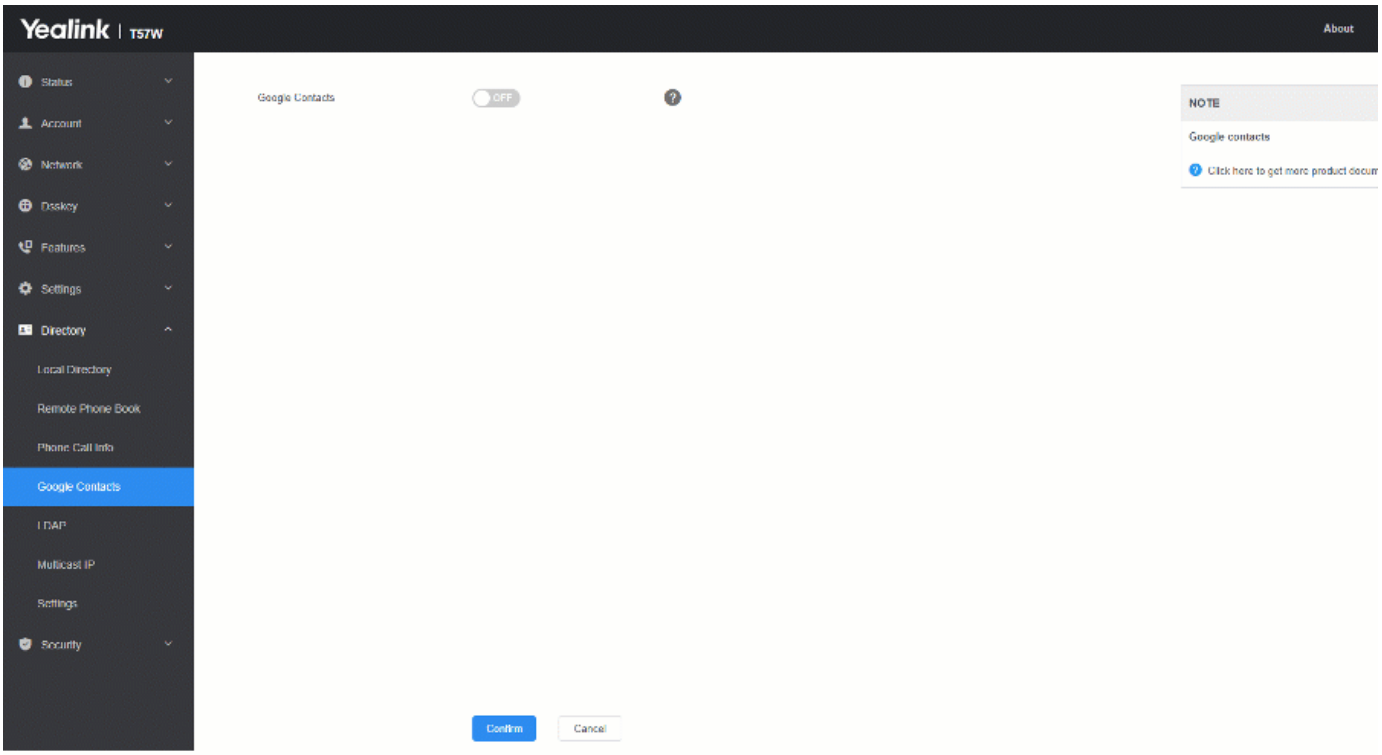
Configuration parameter

google_contact_server.enable
google_contact_server.display_mode

Parameter	Permitted Values	Default	Description
google_contact_server.enable	0-Disabled 1-Enabled	0	It enables or disables the phone to connect to the Google Contact Server.
google_contact_server.display_mode	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	It configures the display mode of the Google contacts. It works only if "google_contact_server.enable" is set to 1 (Enabled).

Set via the Web User Interface

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



Signing in to the Google Contacts 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.

3. Enter the code generated on the web user interface into the pop-up window.
4. Enter your email address and password.
5. Allow the contact test to access your Google account.

Google Contacts Configuration for Android Phone

Yealink IP phone supports the Google contacts feature. After enabling Google contacts on the phone, users can get Google contacts from their Google accounts.

To use this feature, you need to install the GMS core package, and then the user should add Google accounts to the phone. Please ask the distributor or Yealink FAE for the specific version of the GMS core package.

1. It is only applicable to T58A/VP59/T58W/T88W (Pro)/T88V Pro phones. (T58W is no longer supported after V87 due to security issues.)

2. The GMS core package should be a specific version:T58A Android 5.1: open_gapps-arm-5.1-pico-20170713.zipVP59 Android 5.1: open_gapps-arm-5.1-pico-20160619.zipVP59 Android 7.0: open_gapps-arm64-7.1-pico-20190529.zipVP59 Android 9.0: open_gapps-arm64-9.0-pico-20200616.zip

Registering Android ID on VP59 Phones

You need to register the Android ID to use the GMS service on VP59 phones.

Procedure

1. Ask the distributor or Yealink FAE for the GMS core package (open_gapps-arm64-7.1-pico-20190529.zip for Android 7.1; open_gapps-arm64-9.0-pico-20200616.zip for Android 9.0).
2. Place the GMS core package on the provisioning server “192.168.10.25”.
3. Install the GMS core on the phone.

Example

pm.gms_install_url = http://192.168.10.25/open_gapps-arm64-9.0-pico-20200616.zip

Once provisioning, the Play Store application is added on the second idle screen after the phone reboot.

1. Access the web user interface of the phone, navigate to **Settings** > **GMS**.
2. Click Register to jump to the page of Google Android device registration: https://www.google.com/android/uncertified/.
3. Copy the Android ID into the input box and complete the registration.
4. Reboot the phone.

Google Contacts Configuration

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

Configuration parameter

pm.gms_install_url
pm.gms_uninstall
google_contact_server.enable
google_contact_server.display_mode

Parameter	Permitted Values	Default	Description
pm.gms_install_url	String	Bl	It configures the URL of the GMS core package.

[1]		an k	The GMS core package should be a specific version: T58A Android 5.1: open_gapps-arm-5.1-pico-20170713.zip VP59 Android 5.1: open_gapps-arm-5.1-pico-20160619.zip VP59 Android 7.0: open_gapps-arm64-7.1-pico-20190529.zip VP59 Android 9.0: open_gapps-arm64-9.0-pico-20200616.zip Please ask the distributor or Yealink FAE for the specific version of GMS core package. Example: pm.gms_install_url = http://192.168.10.25/open_gapps-arm64-9.0-pico-20200616.zip If you upgrade VP59 from Android 7 to 9, you need to uninstall GMS first, "pm.gms_uninstall=gms".
pm.gms_uninstall[1]	Software package name or APK file name, or Application name	Bl an k	It uninstalls the GMS service.
google_contact_server.enable	0-Disabled 1-Enabled	0	It enables or disables the Google contacts. It works only if the GMS core package is installed (configured by "pm.gms_install_url") successfully and a Google account is added to the phone.
google_contact_server.display_mode	0-All downloaded Google contacts will be displayed on the phone.	1	It configures the display mode of the Google contacts. It works only if "google_contact_server.enable" is set to 1 (Enabled).

	1-Only the Google contacts whose number fields are not empty will be displayed on the phone.		

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

GMS Services List

You can disable some GMS services on the phone.

The following lists all the GMS services you can disable on the phone:

APK Filename/Software Package Name	Description
com.google.android.onetimeinitializer	One-time initialization on first startup.
com.google.android.configupdater	Allows updating the unexecutable system components in the wireless network.
com.google.android.setupwizard	Out-of-the-box user experience.
com.google.android.partnersetup	The initialization service for partner-dedicated equipment.
com.google.android.feedback	Allows users to send error reports and give feedback about GoogleLoginService to Google.
com.google.android.syncadapters.calendar	Syncs calendar data to the user's Google account.
com.google.android.backuptransport	Backs up data to the user's Google account.
com.android.vending	Playstore

Disabling GMS services listed above will not affect the use of Google Contacts. It can reduce CPU consumption and have a positive performance impact for the phone.

Example: Configuring the Google Contacts Feature

This section shows an example for you about how to configure the Google Contacts feature for users.

Procedure

1. Ask the distributor or Yealink FAE for the GMS core package (open_gapps-arm-5.1-pico-20170709.zip).
2. Place the GMS core package on the provisioning server “192.168.10.25”.
3. Install the GMS core on the phone.

T58A Example

pm.gms_install_url = http://192.168.10.25/open_gapps-arm-5.1-pico-20170709.zip

VP59 Example

pm.gms_install_url = http://192.168.10.25/open_gapps-arm64-7.1-pico-20190529.zip

After provisioning, there are two applications (Google Settings and Play Store) added on the second idle screen after phone reboot.

1. Disable some GMS services on the phone.

Example

####Multiple GMS servicess are separated by slashs.####

app.unavailable = com.google.android.onetimeinitializer/com.google.android.configupdater

1. Add a Google account via the phone user interface: Settings > APP Accounts > Add account > Google.
2. Enable the Google Contacts feature on the phone.

google_contact_server.enable = 1

After provisioning, the Google Contacts directory appears on the phone. Users can add, edit, delete or search for a Google contact on the phone.

Enterprise Directory Configuration

Enterprise Directory Configuration

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

> Supported devices:T88V Pro, T88W(Pro), T87W, T85W, T77U, T74W, T74U, T73W, T73U, T57W, T54W, T53W, T53, T53C, T48U, T46U, T43U, T42U, T33P, T33G, T31P, T31G, T31, T30P, T30, T31W.

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	Permitted Values	Default	Description
features.enterprise_directory.enable	0-Disabled 1-Enabled	0	It enables or disables the Huawei enterprise directory feature.
features.enterprise_directory.host	String	Blank	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/services:443. It works only if "features.enterprise_directory.enable" is set to 1 (Enabled).
features.	String	Bl	It configures the IP address of the contact

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

Directory Source Priority

Introduction

You can configure the order of the directory sources for ID lookup in incoming/outgoing calls.

Supported Directory

Number	Directory Type
1	Bluetooth Contact
2	Local Contact
3	Google Contact
4	CLOUD Contact
5	MTSW
6	Remote Phone Book
7	Broadsoft Contact
8	UC Contact
9	PLCM Contact
10	GB
11	LDAP
12	CarDAV
13	DisplayName sent by Sip
14	Enterprise Directory

Configuration Parameter

directory_setting.lookup_call_in.priority
directory_setting.lookup_call_out.priority

Parameter	Description	Permitted Values	Default

directory_setting.lookup_call_in.priority	It configures the priority of incoming call matching for phone contacts.	Integer from 1 to 14	Blank
directory_setting.lookup_call_out.priority	It configures the priority of outgoing call matching for phone contacts.	Integer from 1 to 14	Blank

1. You need to reorder the directory each time you modify the priority.
2. You need to enable the directory first; otherwise, the configuration is invalid, and the directory is skipped directly. For example, if there are LDAP directory in your matching list, you need to enable the LDAP directory function first.
3. If a directory is not configured in the configuration item, the directory will be skipped during matching.

Example

1. Contact information
   - There is a contact in the local directory with the number 11223344 and the name Tom.
   - There is a contact in the Bluetooth directory with the number 11223344 and the name Jimmy.
2. Priority configuration
   At this time, you set the parameter as follows:

```
directory_setting.lookup_call_in.priority=2,1,3,4,5,6,7,8,9,10,11,12,13,14
```

3. Caller ID effect
   In this case, when the phone receives an incoming call with the number 11223344, the phone interface will display the call as coming from Tom based on the matching priority.

CardDAV Directory

Introduction

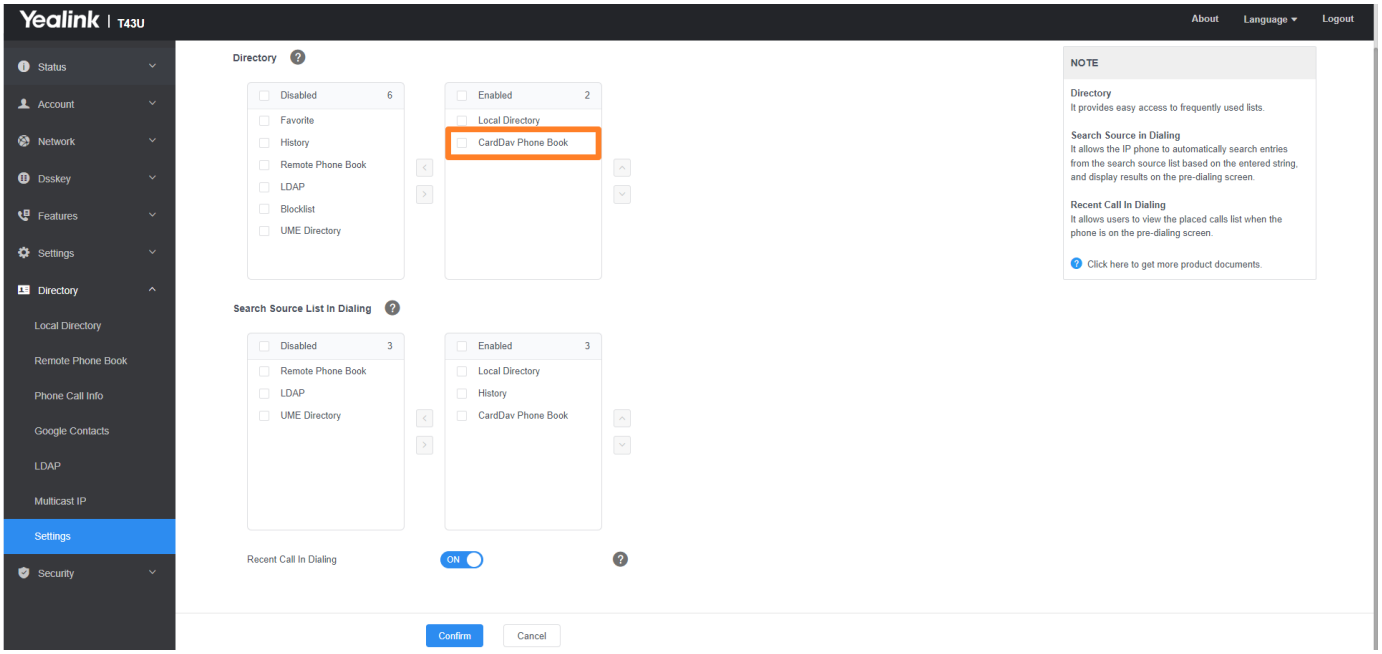
CardDAV is an open standard protocol for synchronizing contact data between devices and applications.

You can get the address book via CardDAV, get its contacts with their vCard fields, and synchronize new contacts/contact fields back to the CardDAV server.

CardDAV Directory Configuration

Set via the Web User Interface

When the "carddav.enable" is set to 1 (Enabled), you can go to **Directory** -> **Settings** to configure the CardDAV directory.



Auto Provisioning

```
carddav.enable
carddav.x.url
carddav.x.username
carddav.x.password
carddav.x.sync_interval
carddav.x.sync_mode
```

carddav.x.label
carddav.call_lookup_enable
directory_setting.carddav.enable
directory_setting.carddav.priority
search_in_dialing.carddav.enable
search_in_dialing.carddav.priority

Parameter	Permitted Values	Default	Description
carddav.enable	0-Disabled 1-Enabled	0	Disable or enable the CardDAV feature.
carddav.x.url	String	Blank	It configures the CardDAV server address. It works only if "carddav.enable" is set to 1 (Enabled).
carddav.x.username	String	Blank	It configures the authentication name for accessing the CardDAV service. It works only if "carddav.enable" is set to 1 (Enabled).
carddav.x.password	String	Blank	It configures the authentication password for accessing the CardDAV service. It works only if "carddav.enable" is set to 1 (Enabled).
carddav.x.sync_interval	300-1296000	1800 s	It configures the periodic time to synchronize contacts from the server. It works only if "carddav.enable" is set to 1 (Enabled).
carddav.x.sync_mode	CSR SCR	SCR	It configures the synchronization mode between the phone and the server.

			It works only if "carddav.enable" is set to 1 (Enabled).
carddav.x.label	String	CardDAV X	It configures the name of the CardDAV contact to be displayed on the phone. It works only if "carddav.enable" is set to 1 (Enabled).
carddav.call_lookup_enable	0-Disabled 1-Enabled	1	It configures whether the phone enables matching CardDAV contacts for incoming and outgoing calls. If enabled, CardDAV contacts will be matched for outgoing calls. It works only if "carddav.enable" is set to 1 (Enabled).
directory_setting.carddav.enable	0-Disabled 1-Enabled	1	It configures whether to display the contact in the contacts entered in the idle state. It works only if "carddav.enable" is set to 1 (Enabled).
directory_setting.carddav.priority	0-14	Blank	It configures the phone to display the priority of the contact in the contacts list when in the idle state. It works only if "carddav.enable" is set to 1 (Enabled).
search_in_dialing.carddav.enable	0-Disabled 1-Enabled	1	It configures whether to search CardDAV contacts when searching in the dialing interface. It works only if "carddav.enable" is set to 1 (Enabled).
search_in_dialing.carddav.priority	0-14	Blank	It configures the priority of CardDAV contacts when searching on the dialing interface. It works only if "carddav.enable" is set to 1 (Enabled).

Privacy Number

Introduction

The phone supports number privacy. Incomplete phone numbers will be displayed when making and receiving calls, as well as in the history records.

Auto Provisioning

```
features.number_privacy.enable
features.number_privacy.start_length=a,b
```

Parameter	Description	Permitted Values	Default
features. number_privacy .enable	It enables or disables the number privacy feature.	0-Disabled 1-Enabled	0
features. number_privacy .start_length=a,b	It configures the number of digits to hide and the length of the hidden digits	a: 1-32 b: 0-32	a: 1 b: 0

Comparison of Different Contacts

Introduction

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 the 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 a dedicated server
Remote Phone Book	5000(T3X),10000(other phones)	√	Shared, Low cost	Inconvenient updates
XML Phonebook	750KB(Black and white screen),1MB(color screen) [5000(T3X),10000(other phones) since x.86.0.112]	√	Easy deployment; User-friendly	Limited display content
Google Contacts	1000	√	Cloud synchronization, Easy to operate	Not shareable
Netw	Requires complementary	× (Requires	Shared; User-	Requires

ork Directory	development	complementary development)	friendly; Easy deployment;	complementary development, such as Broadsoft, Meta.

In general, avatar display requires your device to have a color screen. Black and white screens do not support avatar display.

Different usage scenarios for the 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 the Directory

Introduction

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)

> 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 5 MB.

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:

```
> From: "77852" <sip:77852@10.200.108.48:5060>;tag=3520407363
```

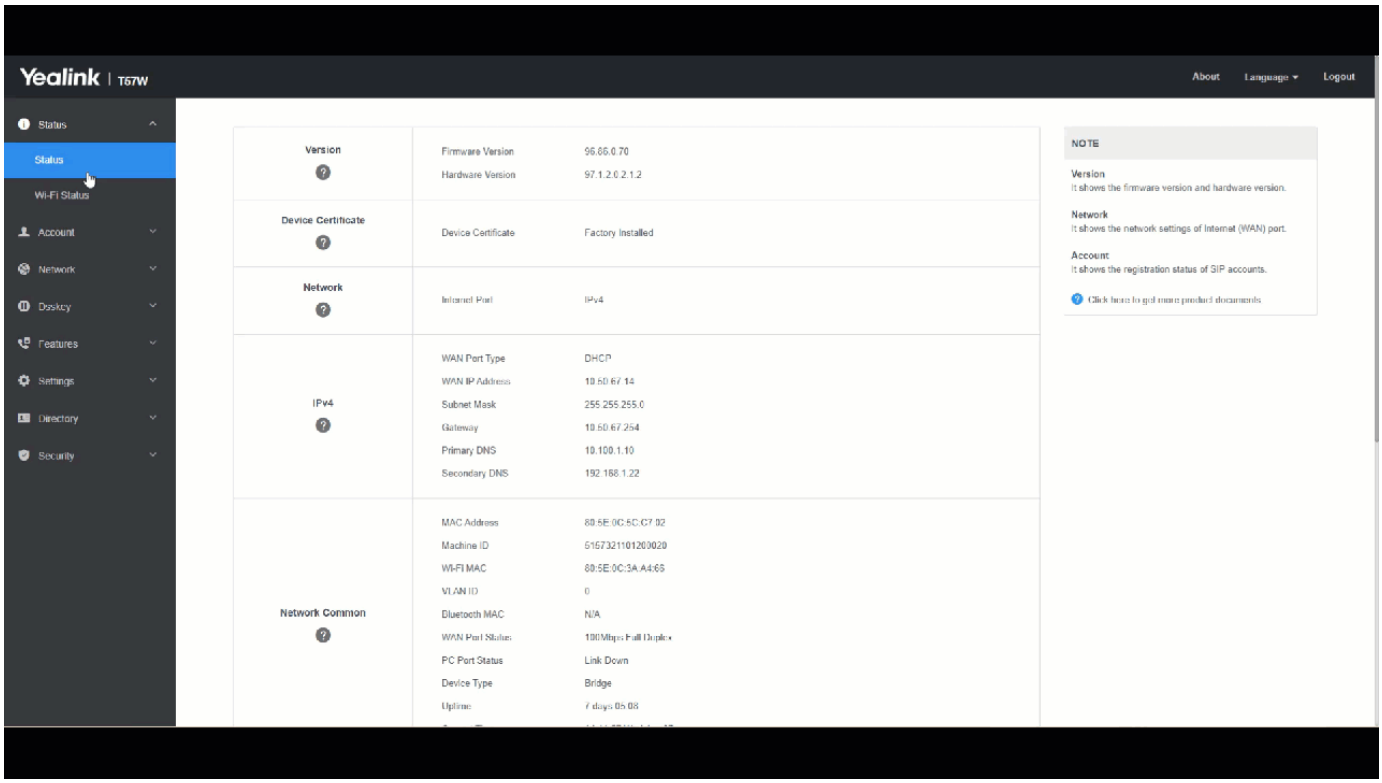
Please confirm if the number carried in the incoming call information is correct.

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 a "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**.



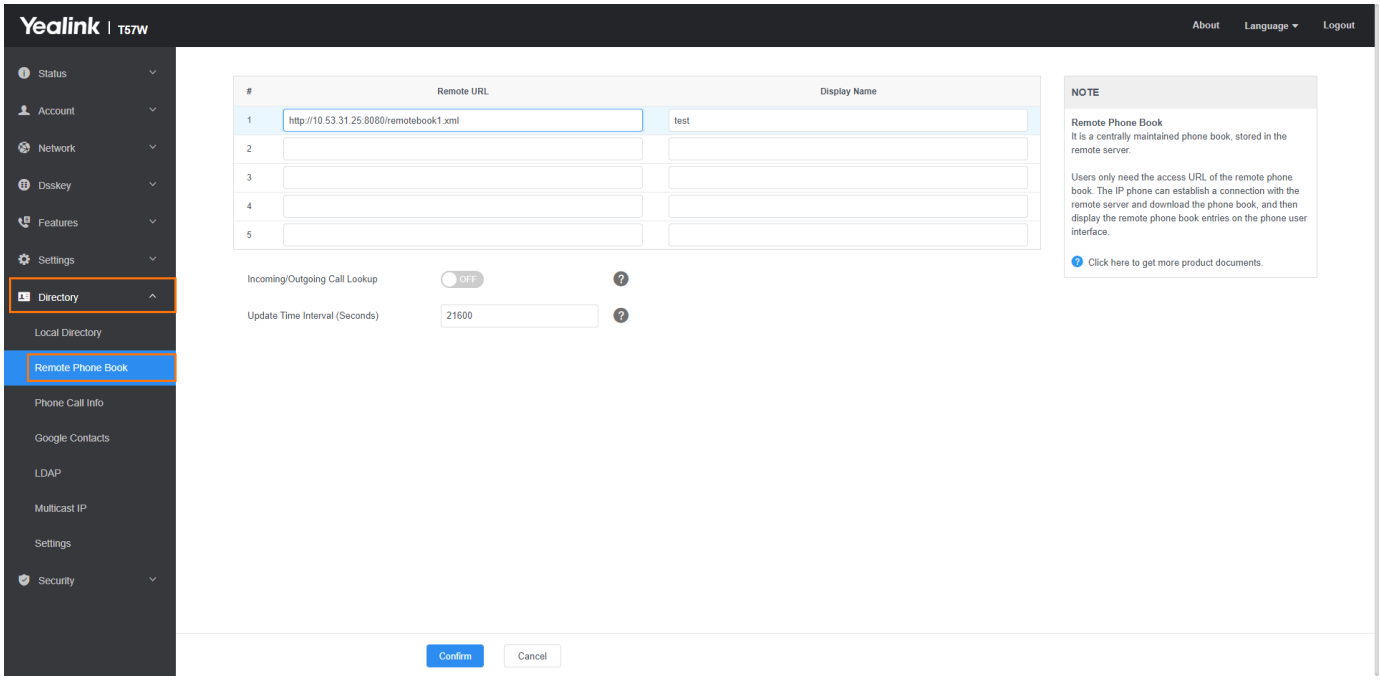
2. Verify certificate settings: Confirm that the device and server have correct certificate settings (HTTPS). Both the server and the phone should have uploaded the appropriate certificates.

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?

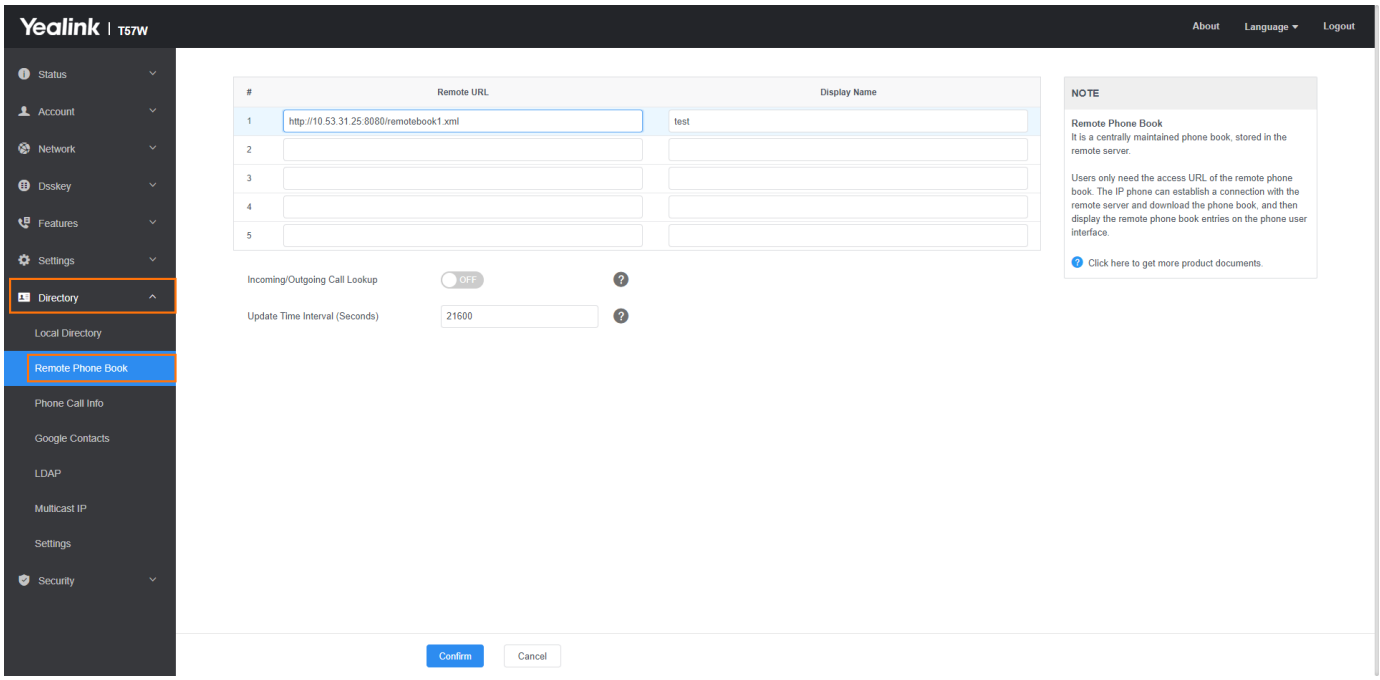
This is normal behavior. The Remote Phone Book is not synchronized with the server in real time. To trigger an update, you can try one of the following methods:

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

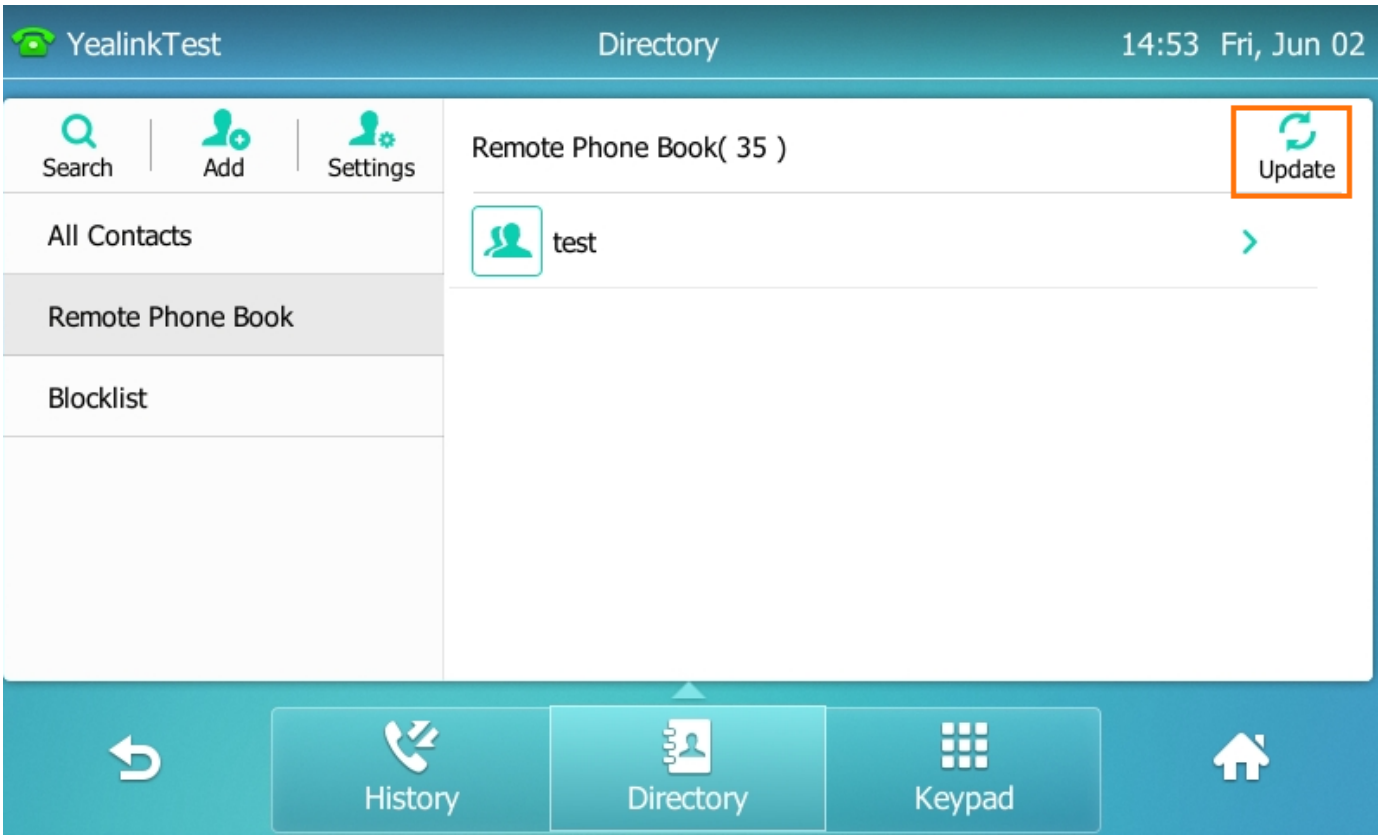


2. Restart the phone to trigger an update.

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 are 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 official Google 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 corresponding 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 situations. Therefore, Yealink provides only three fields on the device to display the numbers in the order they are returned by the server.

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.countr	0	It configures the dial tone for the phone.

	y”） **1**-440/250,0/250 **2**-1000/250,0/250		
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 voice mail. 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 voice mail. 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

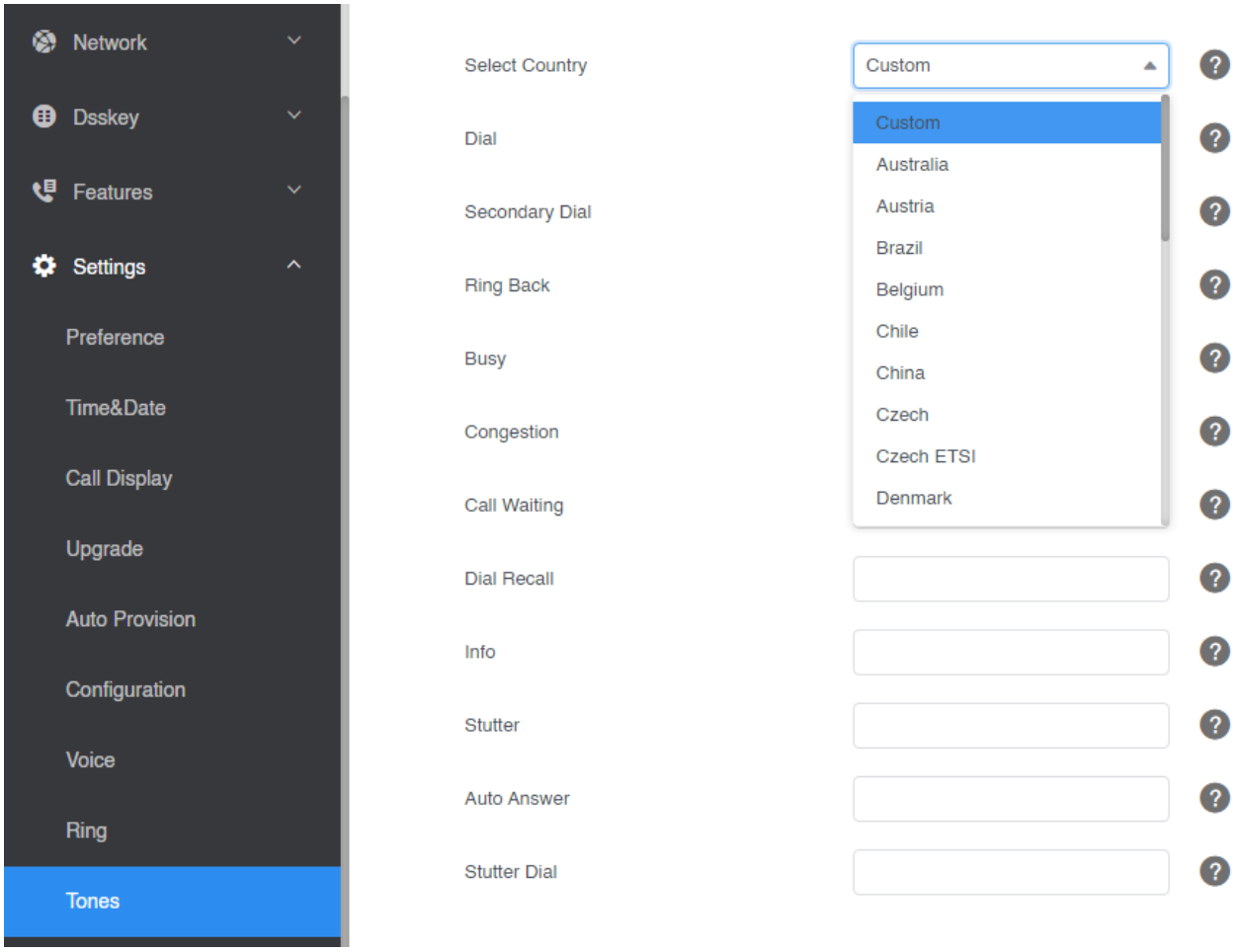
Configured tones can be heard on the phones in the following conditions.

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

			For T40P/T40G/T23P/T23G/T21 § E2/T19 § E2: A tone is comprised of at most two different frequencies. For other phones: A tone is comprised of at most four different frequencies. Duration: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms. You can configure at most eight different tones for one condition, and separate them by commas. (for example, 250/200,0/1000,200+300/500,200+500+800+1500/1000). If you want the IP phone to play tones once, add an exclamation mark "!" before tones (for example, !250/200,0/1000, 200+300/500,200+500+800+1500/1000). It works only if "voice.tone.country" is set to Custom.
features.partition_tone[1]	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	It enables or disables the phone to play the different dial tones when there is no active account. It works only if "voice.tone.dial" is configured.
voice.tone.secondary_dial	String	350+440/3000	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". It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.
voice.tone.ring	String	Blank	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". It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.
voice.tone.busy	String	Blank	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". It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.
voice.tone.congestion	String	Blank	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". It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.
features.congestion_tone.codelist	any code that the server can return	Blank	It configures the return code to play the congestion tone. Multiple codes are separated by commas. **Example**:

			features.congestion_tone.codelist = 403,503,603 The congestion tone can be customized by "voice.tone.congestion".
voice.tone.callwaiting	String	Blank	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". It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.
voice.tone.dialrecall	String	Blank	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". It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.
voice.tone.info	String	Blank	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". It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.
voice.tone.stutter	String	Blank	It customizes the tone when the IP phone receives a voice mail. The value format is Freq/Duration. For more

			information on the value format, refer to the parameter “voice.tone.dial”. It works only if “voice.tone.country” is set to Custom. If you want to disable this warning tone, set it to 0.
voice.tone.message	String	Blank	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”. It works only if “voice.tone.country” is set to Custom. If you want to disable this warning tone, set it to 0.
voice.tone.autoanswer	String	Blank	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”. It works only if “voice.tone.country” is set to Custom. If you want to disable this warning tone, set it to 0.
voice.tone.stutterdial	String within 512 characters	Blank	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”. 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.
voice.tone.stutter_dial_tone.apply_to_dnd.enable	0-Disabled 1-Enabled	0	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". It works only if "voice.tone.country" is set to Custom.
voice.tone.stutter_dial_tone.apply_to_fwd.enable	0-Disabled 1-Enabled	0	It enables or disables the phone to play a specified dial tone when call forwarding is activated on the phone. The dial tone is configured by "voice.tone.stutterdial". It works only if "voice.tone.country" is set to Custom.
voice.tone.stutter_dial_tone.apply_to_vm.enable	0-Disabled 1-Enabled	0	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". It works only if "voice.tone.country" is set to Custom.
features.touch_tone	0-Disabled 1-Enabled	1	It enables or disables the touch tone. It is only applicable to CP920/CP925/CP935W/CP960/CP965 phones.

Ultrasonic Configuration (Only T3 Series)

Introduction

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

Parameter	Permitted Values	Default	Description
voice.ultrasonic.enable	0-Disabled 1-Enabled	1	It enables or disables the ultrasonic. When the user uses a common RJ headset to connect to the phone, the ultrasonic is automatically turned off, and the ultrasonic is automatically turned on after disconnection.

Ringer Device

Introduction

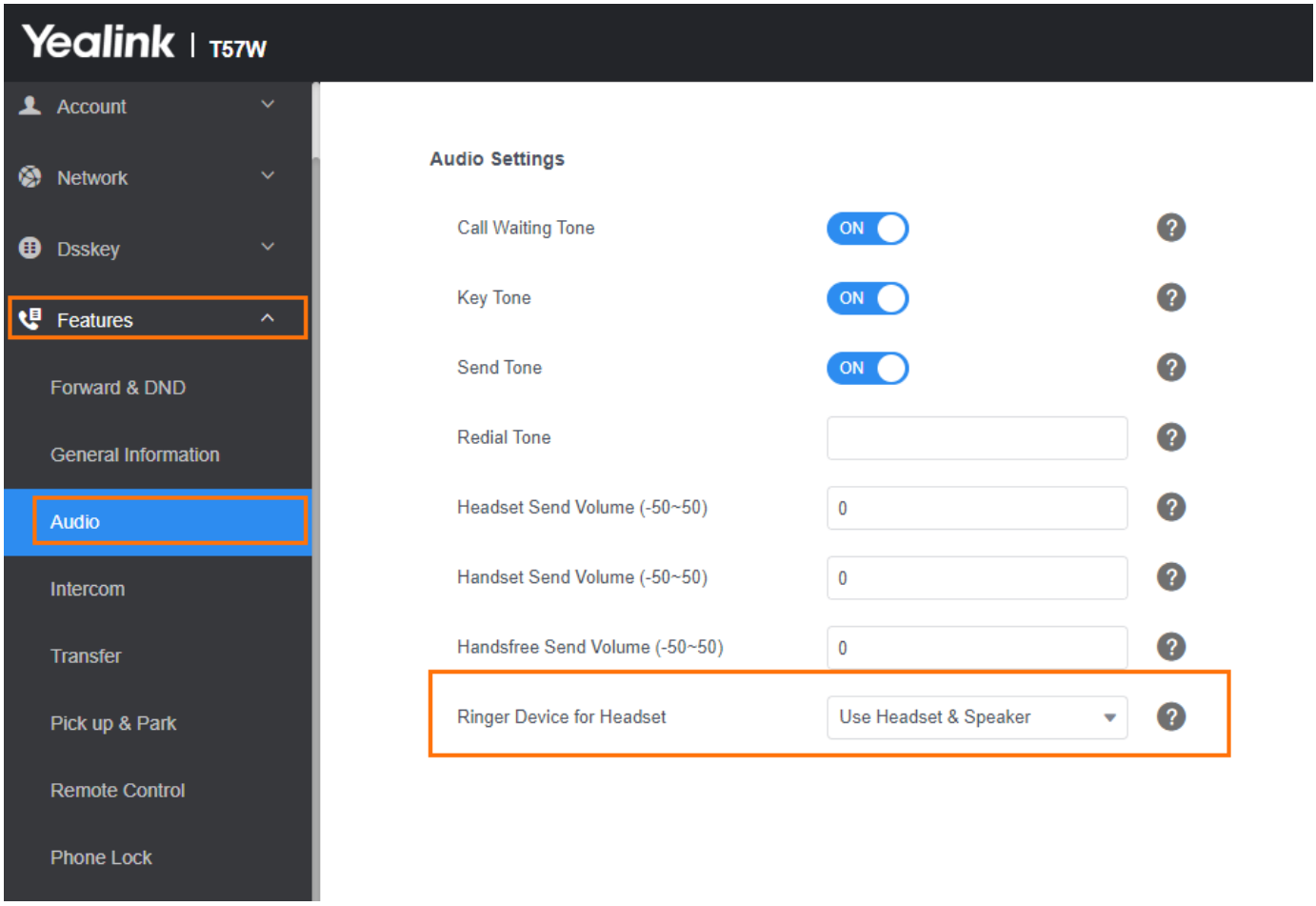
You can use either the speaker or the headset as a ringer device. You can configure which ringer device to use when receiving an incoming call. For example, if the ringer device is set to Headset, the ring tone will be played through your headset.

It is not applicable to CP930W-Base/CP935W-Base phones.

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	Defa	Description

	Values	ult	
features.ringer_device.is_use_headset	**0**-Use Speaker **1**-Use Headset	0	It configures the ringer device for the phone.

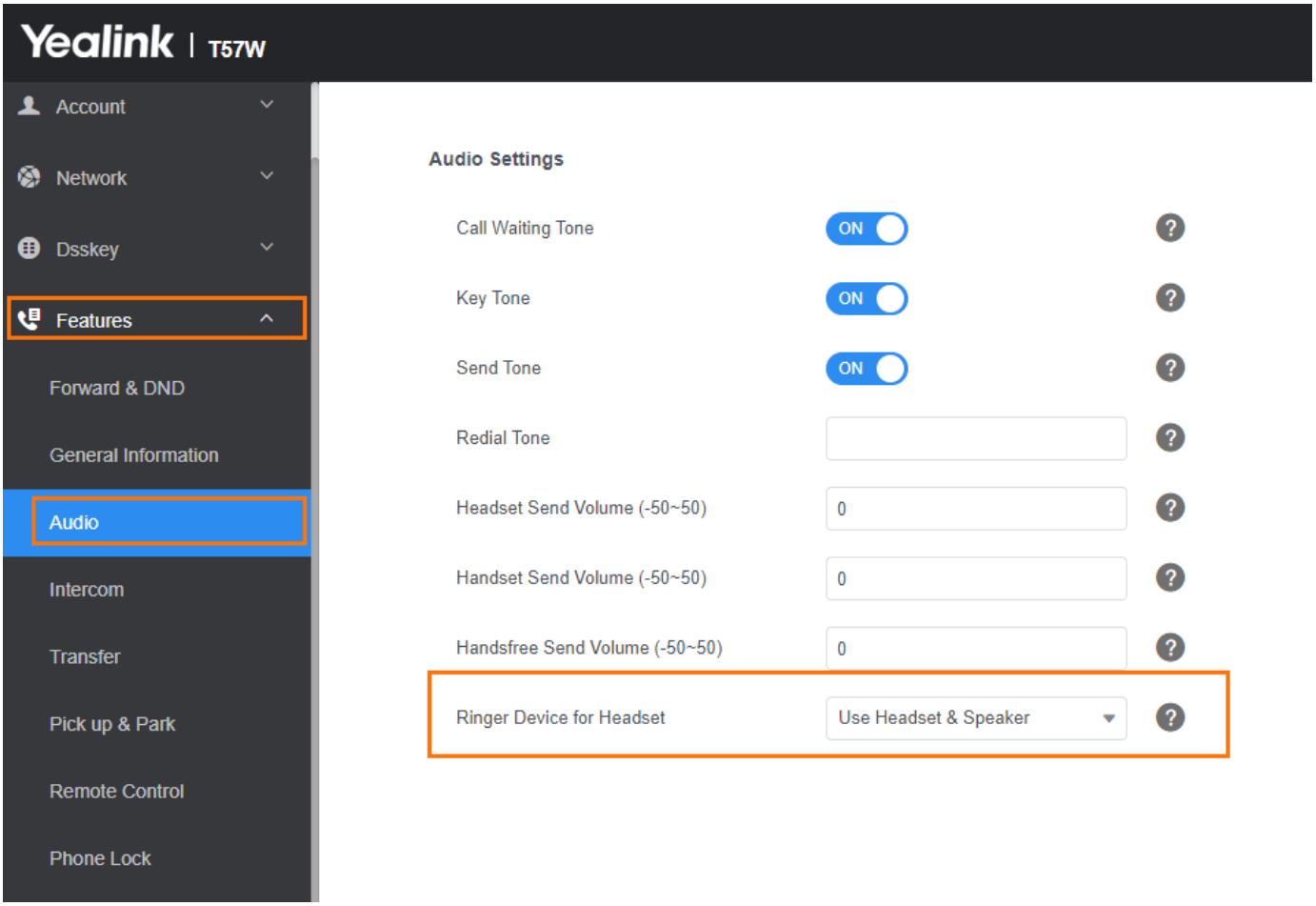
Switch Among the Handset, Speaker, and Headset Modes

During a call, you can switch to Speaker mode by pressing the Speakerphone key , headset mode by pressing the HEADSET key , and handset mode by picking up the handset.

FAQ

How to make it ring through the headset?

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



Audio Volume

Introduction

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

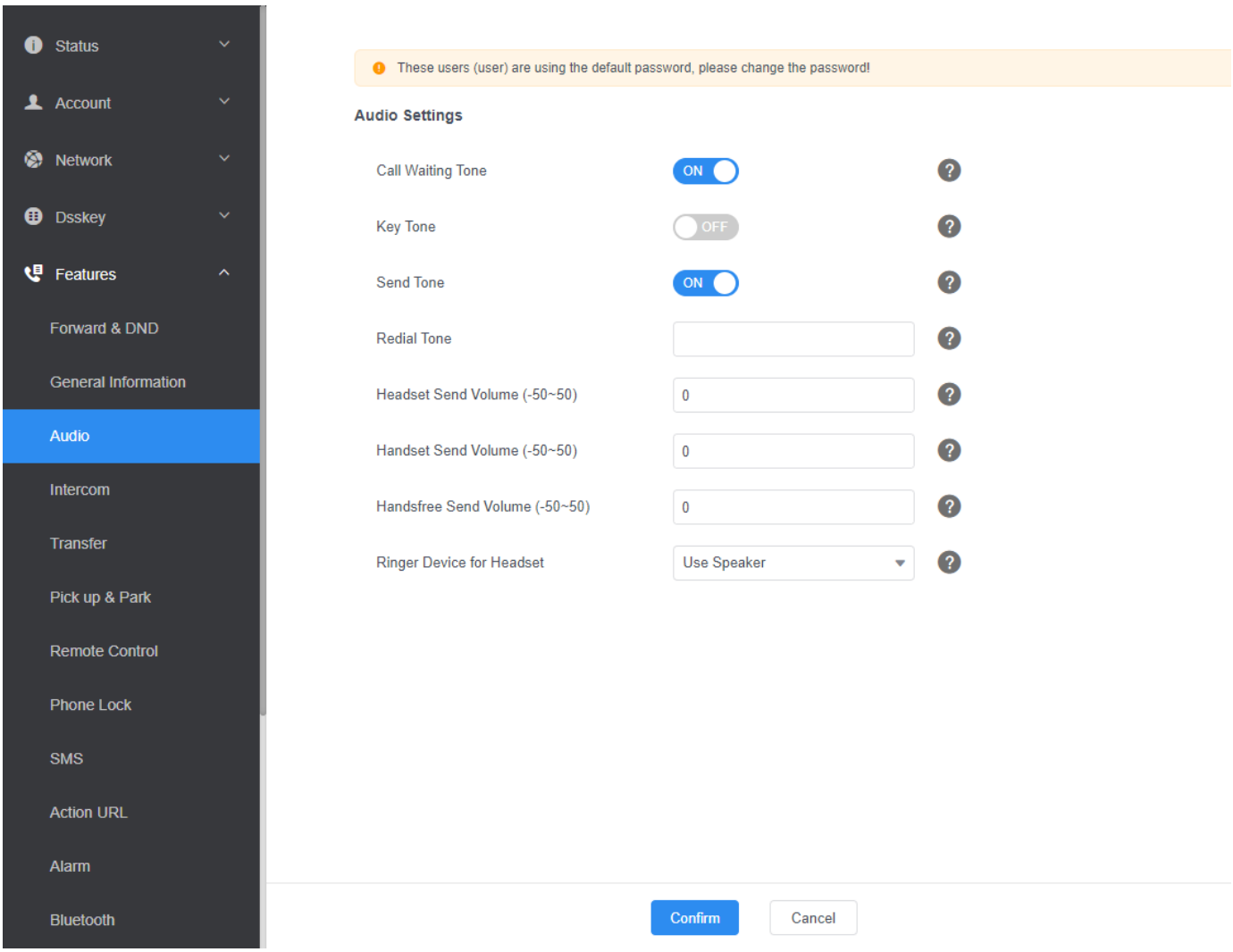
Ringer Volume Configuration

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.

Set via the Web User Interface

On the web user interface, go to **Features** > **Audio**.



Configuration Parameter

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 is used to avoid missing calls when the user turns down the ringer volume.

```
force.voice.ring_vol
phone_setting.voice.ring_vol_min
```

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. You can set the "force.voice.ring_vol">0 only if "custom.handset.silent_charging" is set to 1.
phone_setting.voice.ring_vol_min	Integer from 0 to 15	0	It configures the adjustable minimum ringer volume on the phone. It only takes effect on the ringer volume of the speaker on the phone. After the headset is connected, the ringer volume can only be controlled by the headset itself.

Sending Volume Configuration

You can configure the sending volume of currently engaged audio devices (handset, speakerphone or headset)

when the phone is in use.

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

```
voice.handfree_send
voice.handfree.autoreset_spk_vol
voice.handset_send
voice.handset.autoreset_spk_vol
voice.headset_send
voice.headset.autoreset_spk_vol
voice.handset.tia4965.enable
voice.rx_agc_type.mode
```

Parameter	Permitted Values	Default	Description
voice.handfree_send[1]	Integer from **-50** to **50**	0	It configures the sending volume of the speaker. We recommend that you modify this parameter cautiously. An unsuitable value may render the voice quality bad.
voice.handfree.autoreset_spk_vol	**0** -The speakerphone volume at the end of a call persists between calls. **1** to **15**-The speakerphone volume does not persist between calls and resets to this specified level with each new call.	0	It configures the speaker's volume level during a call.
voice.handset_send[1]	Integer from **-50** to **50**	0	It configures the sending volume of the handset.

			We recommend that you modify this parameter cautiously. An unsuitable value may render the voice quality bad.
voice.handset.autoreset_spk_vol	**0** -The handset volume at the end of a call persists between calls. **1** to **15**-The handset volume does not persist between calls, and resets to this specified level with each new call.	0	It configures the handset's volume level during a call.
voice.headset_send[1]	Integer from **-50** to **50**	0	It configures the sending volume of the headset. We recommend that you modify this parameter cautiously. An unsuitable value may render the voice quality bad.
voice.headset.autoreset_spk_vol	**0** -The headset volume at the end of a call persists between calls. **1** to **15**-The headset volume does not persist between calls, and resets to this specified level each new call.	0	It configures the headset's volume level during a call.
voice.handset.tia4965.enable	**0** -Disabled **1** -Enabled, if the handset's volume level for the current call is adjusted to level 12/13/14/15, the volume level automatically resets to 11 after the call. That is, the initial volume level is 11 for the next call.	1	It enables or disables the handset's volume level to be reset to level 11 after the call if the volume level for the current call exceeds the standard.
voice.rx_ag	**0** -Disabled	0	It configures whether to enable high-

c_type.mode	**2** -High volume mode		volume mode in noisy environments.

Distinctive Ring Tones

Introduction

The feature of distinctive ring tones allows certain incoming calls to trigger the phone to play distinctive ring tones.

The IP 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.

> If the caller already exists in the local directory, the ring tone assigned to the caller should be played preferentially.
> The distinctive ring tones 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), <URL> and info=info text;x-line-id=0.

> 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	Ringin		450	500	550

		g				

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 locaring tone (RingN.wav), or play the first locaring 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 IP 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 wilmap the text with the InternaRinger Text preconfigured (or distinctive_ring_tones.alert_info.X.text is configured) on the IP 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:

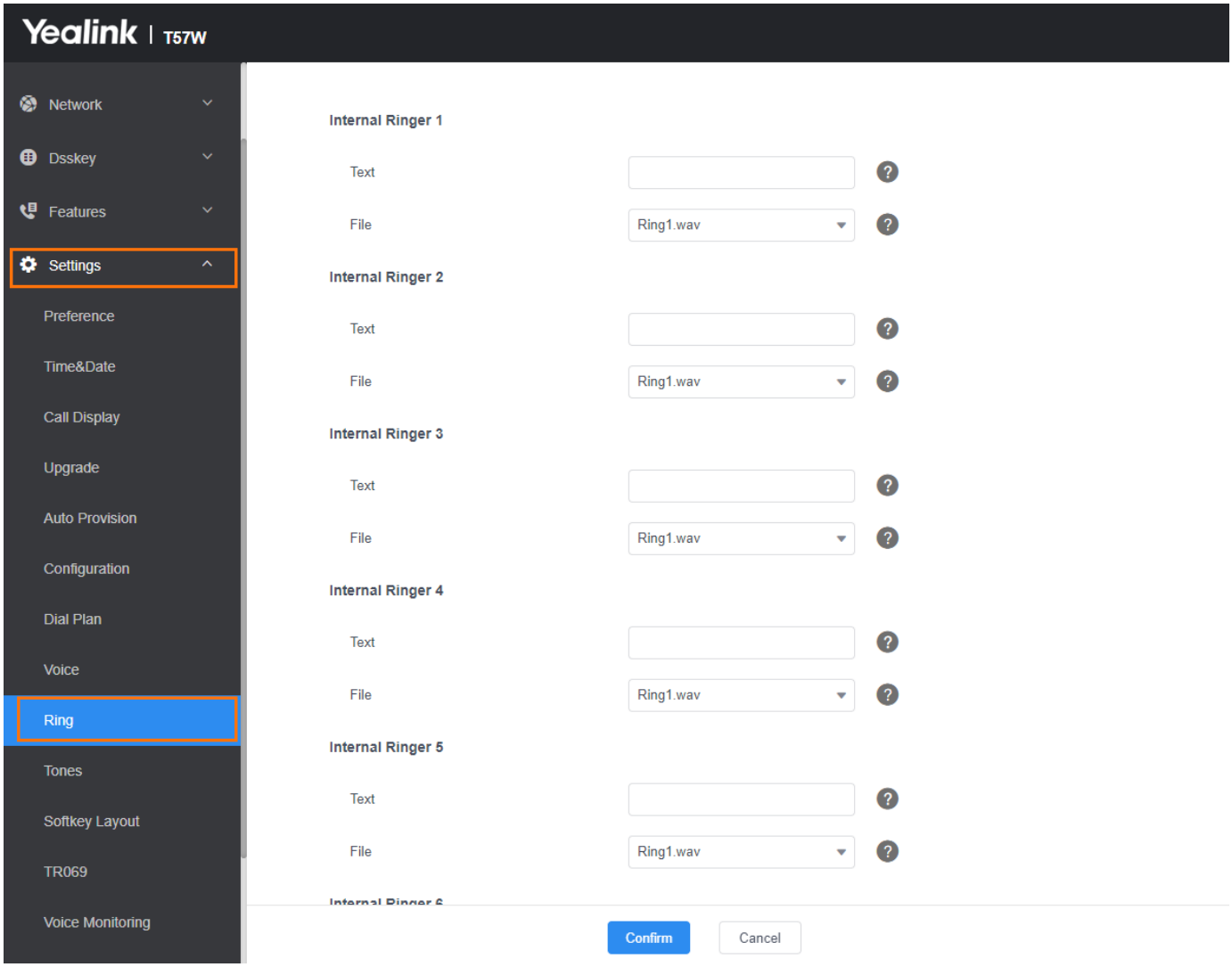
- Alert-Info: Auto Answer
- Alert-Info: info = alert-autoanswer
- Alert-Info: answer-after = 0 (or Alert-Info: Answer-After = 0)
- Alert-Info: Intercom

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 ring tone 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 algorithm's objective 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

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

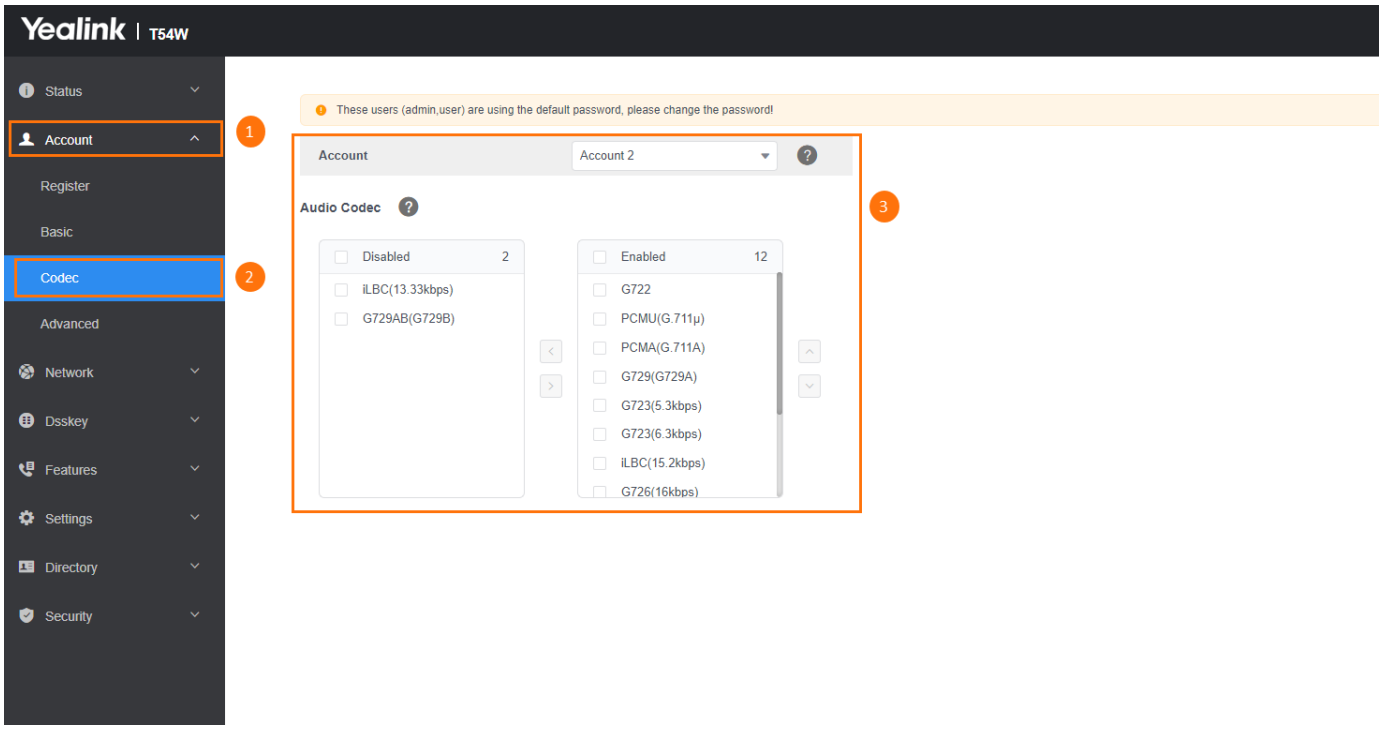
The following table lists the audio codecs supported by each phone model:

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
account.X.codec.<payload_type>.enable[1]	**0**-Disabled **1**-Enabled	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 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;	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) **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 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.
account.X.codec.<payload	Integer from 0 to 10	When the audio codec is G722, the	It configures the priority of the enabled audio codec.

_type>.priority[1]		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 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;	The name of the audio codec: **g722**-G722 **pcmu**-PCMU(G.711μ) **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 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. It works only if your firmware version is x.86.0.112 or later.

> [1] X is the account ID.

Packetization Time (PTime)

Introduction

PTime is a measurement of the duration (in milliseconds) that 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

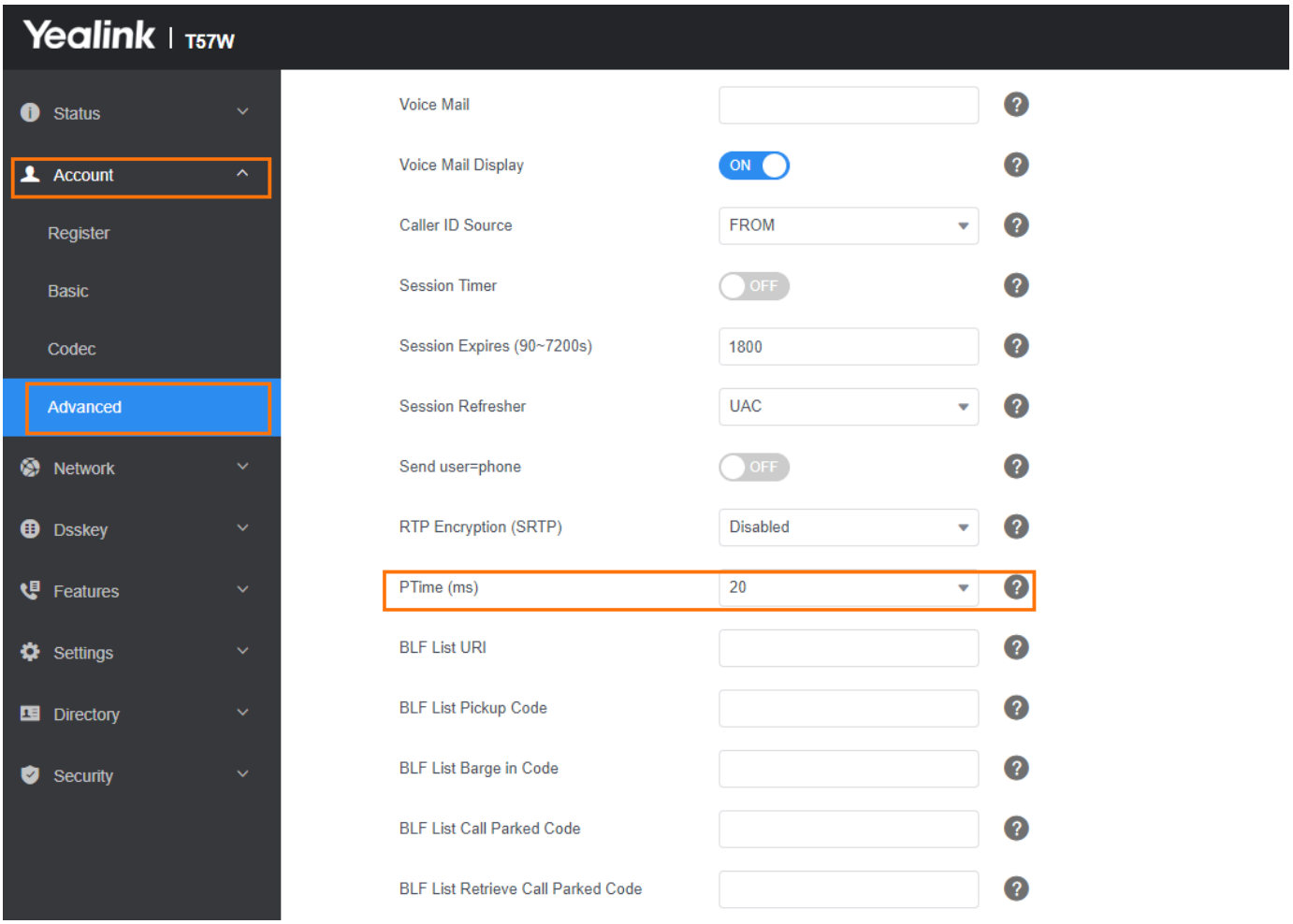
The following table summarizes the valid values of ptime for each audio codec:

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.

[1] X is account ID.

Early Media

Introduction

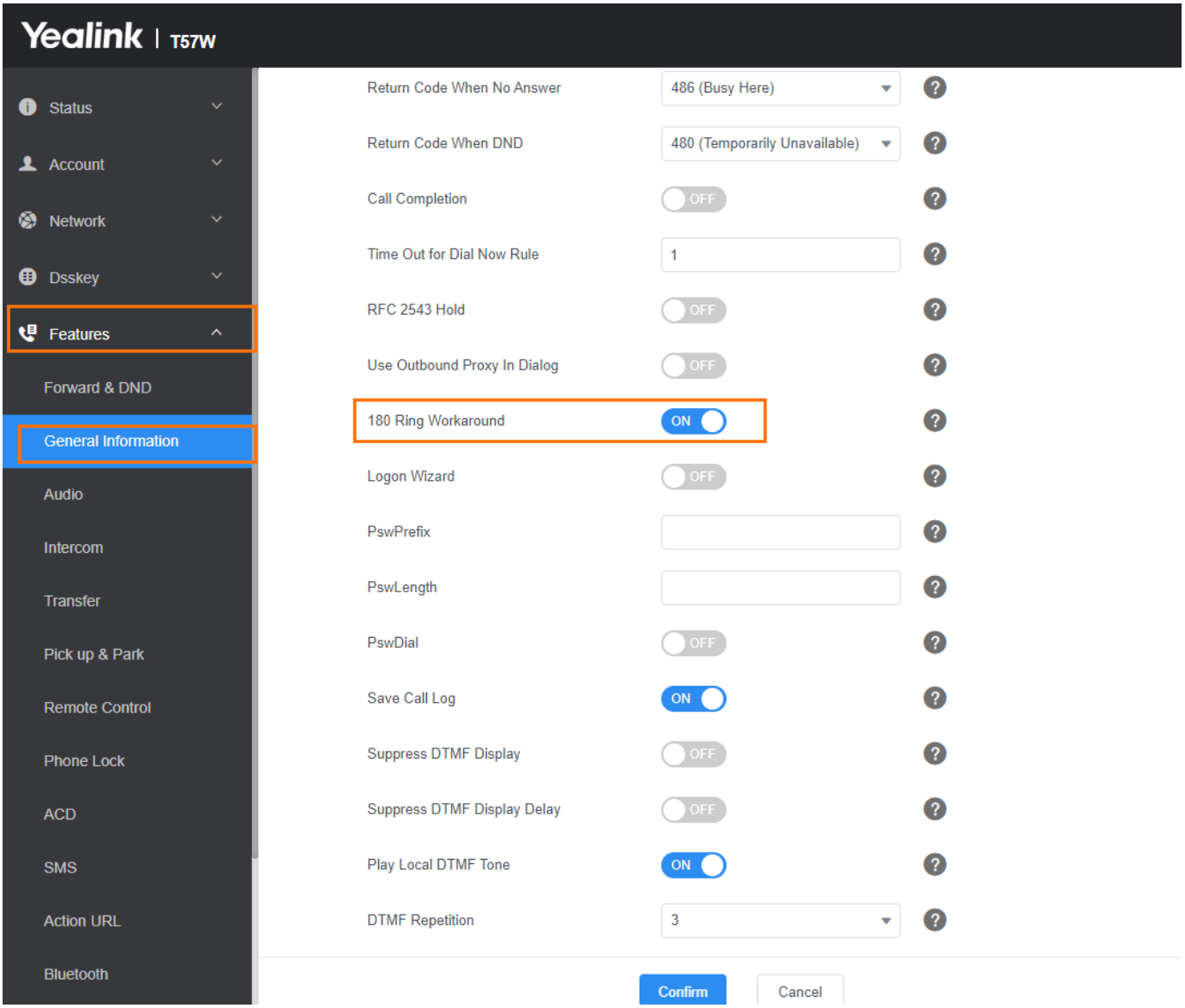
The early media refers to the media (for example, audio and video) played to the caller before a SIP call is actually established.

You can also configure 180 ring workaround which defines whether to deal with the 180 message received after the 183 message. 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 message received after the 183 SIP message.

Acoustic Clarity Technology

Introduction

To optimize the audio quality in your network, Yealink phones support the 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.

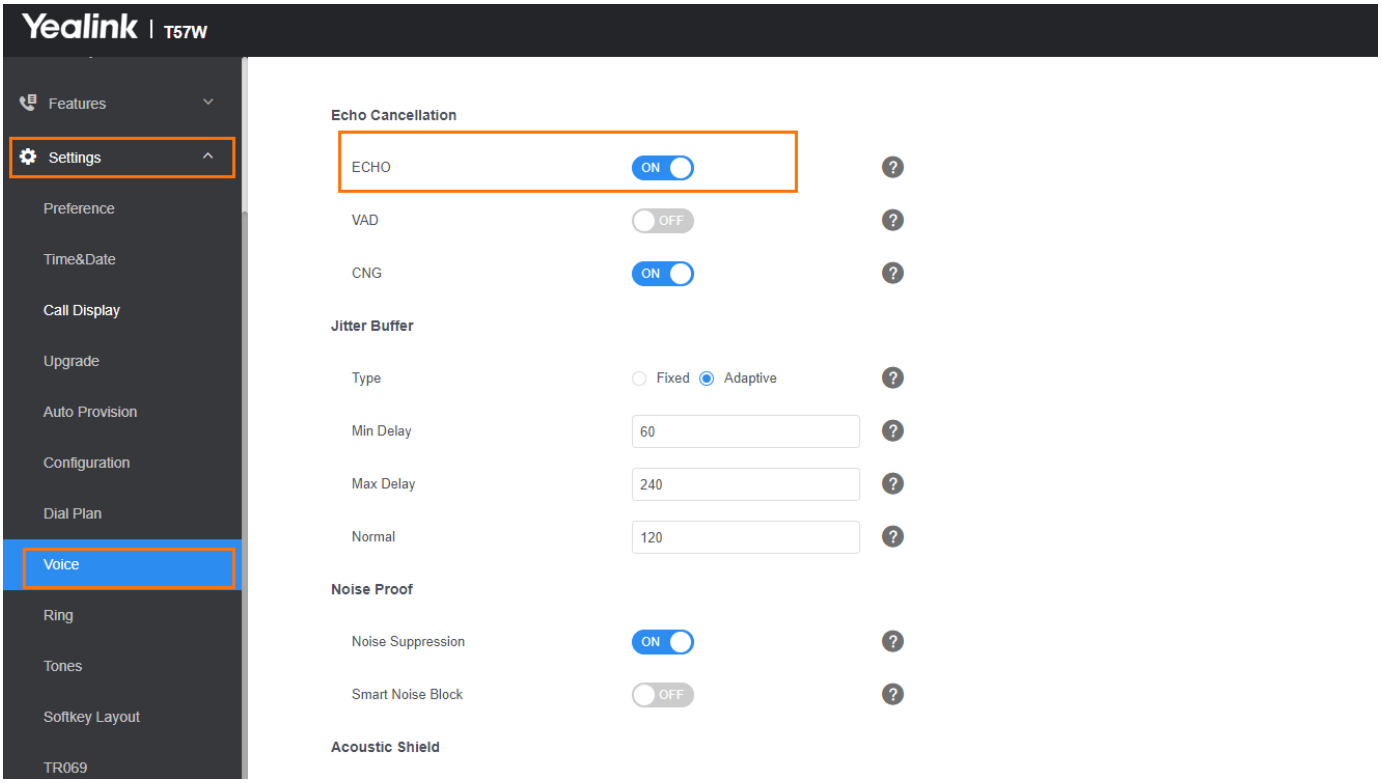
Acoustic Echo Canceller（AEC）

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.echo_cancellation	**0**-Disabled **1**-Enabled	1	It enables or disables the AEC (Acoustic Echo Canceller) feature.

Automatic Gain Control (AGC)

Automatic Gain Control (AGC) is applicable 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.

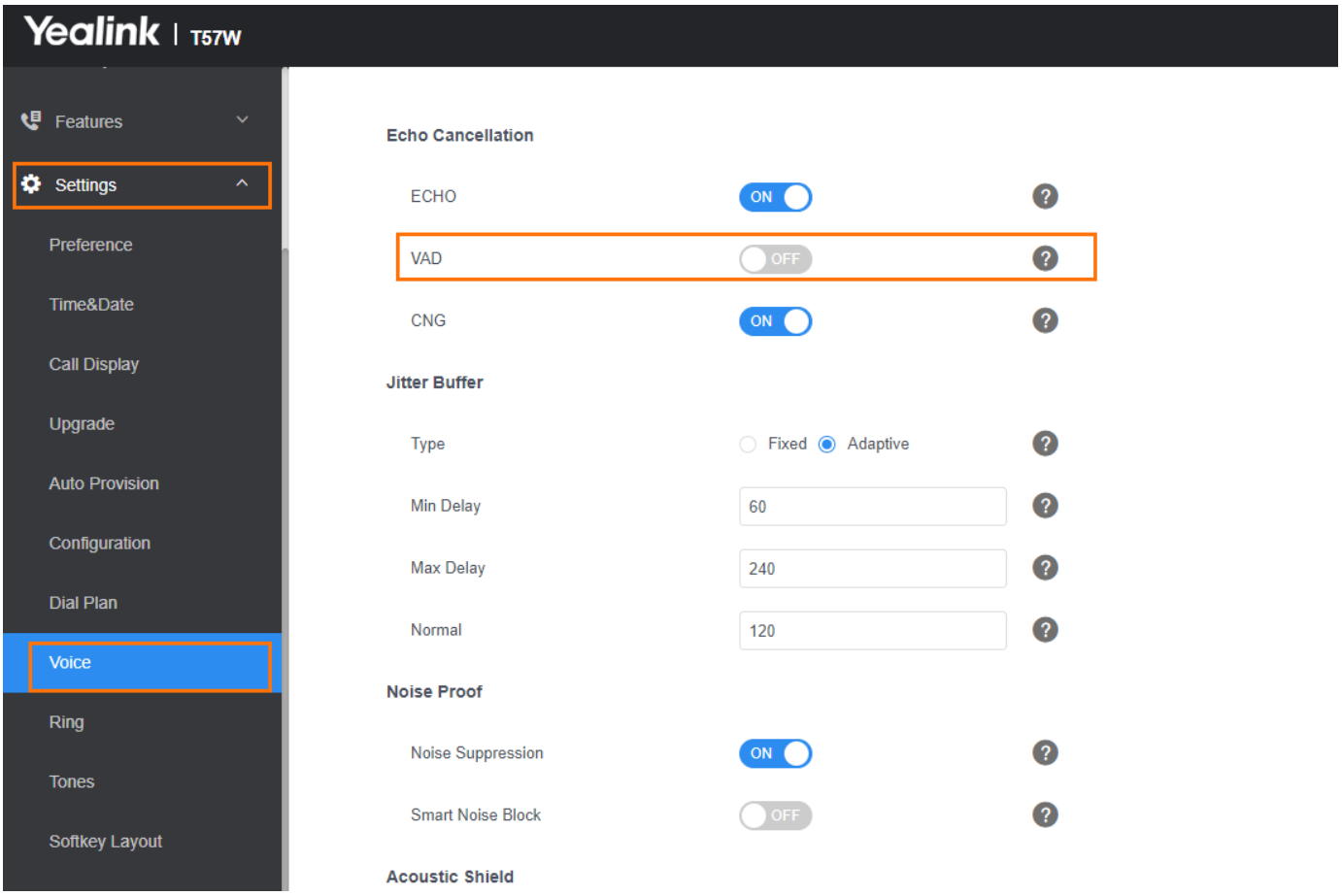
Voice Activity Detection (VAD)

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)

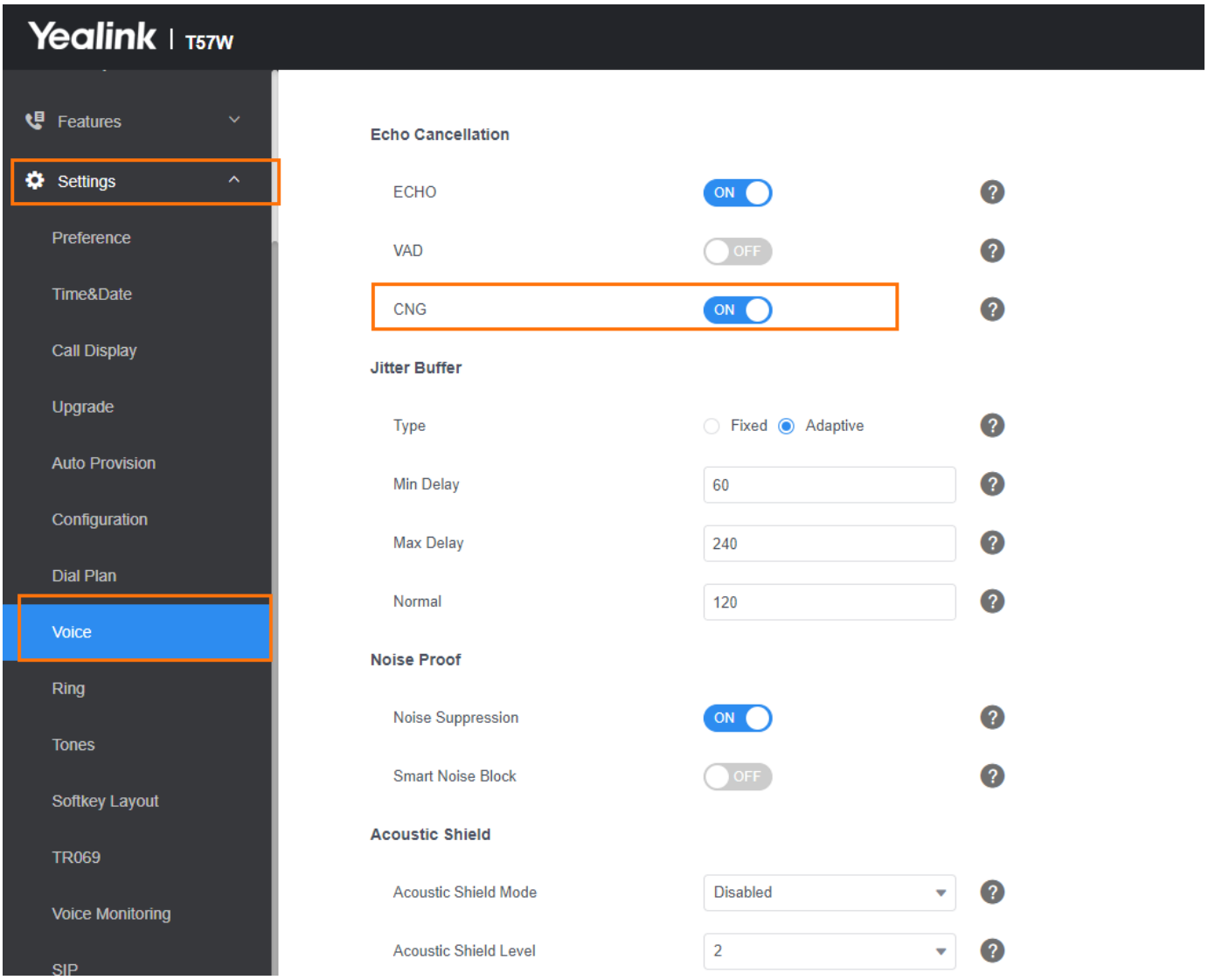
Comfort Noise Generation (CNG) is used to generate background noise for voice communications during periods of silence in a conversation.

> 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.

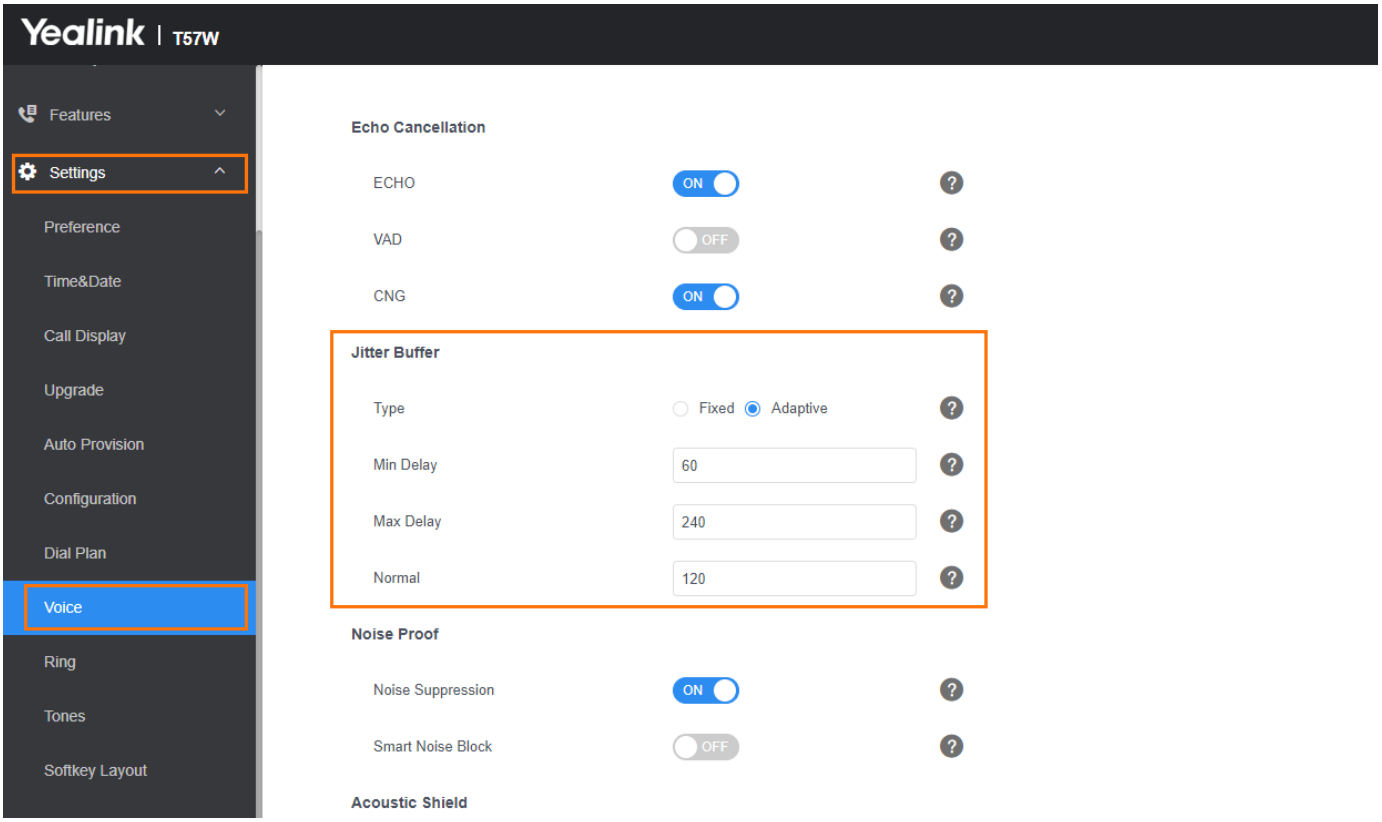
Jitter Buffer

Yealink phones support two types of jitter buffers: **fixed** and **adaptive**. A fixed jitter buffer adds a 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 the changes in the network's delay. The range of the delay time for the dynamic jitter buffer added to packets can also be 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. 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. 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. 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 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

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:

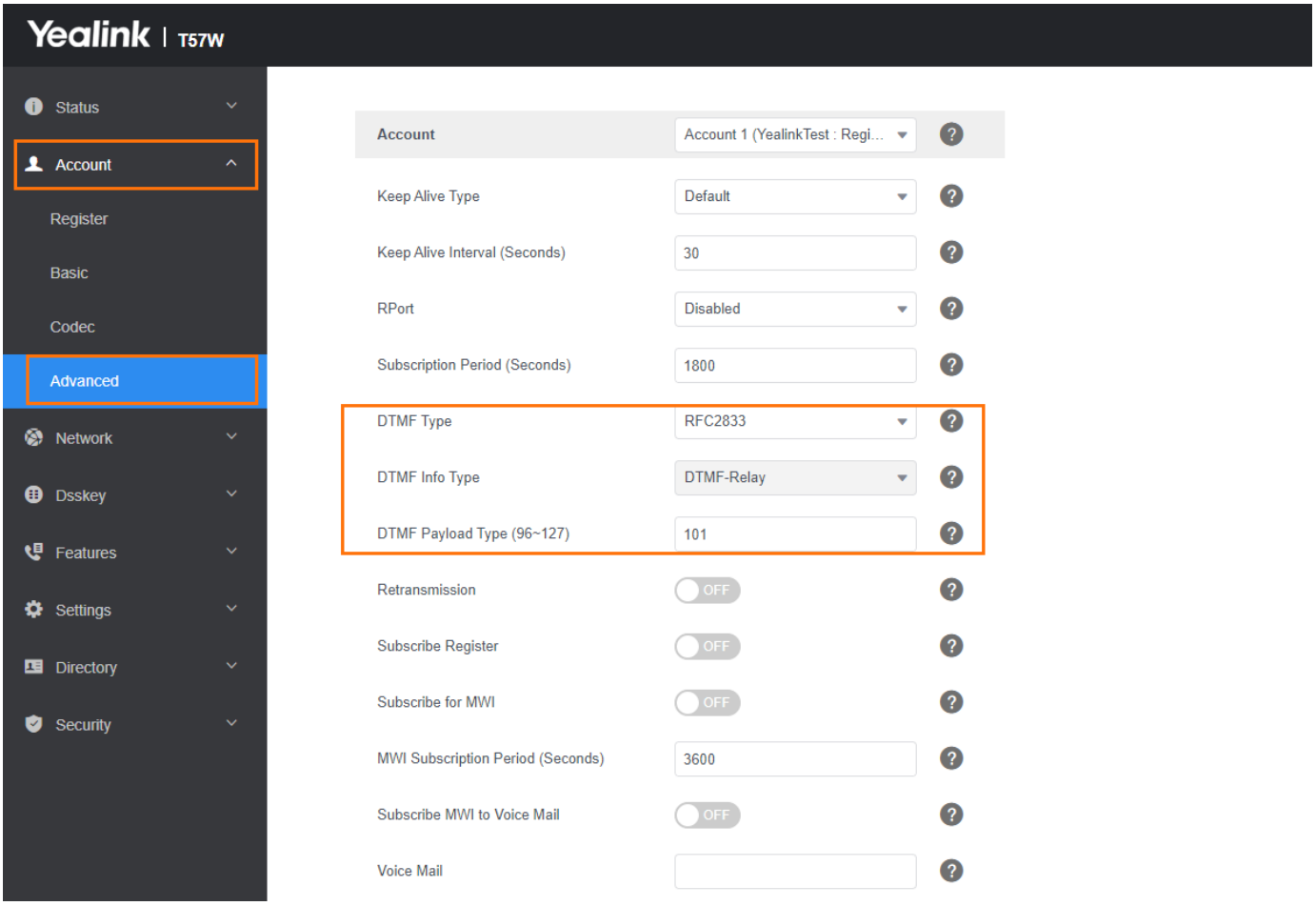
- **RFC 2833** – DTMF digits are transmitted by RTP Events compliant with RFC 2833. You can configure the payload type and sending times of the end RTP Event packet. The RTP Event packet contains 4 bytes. The 4 bytes are distributed over several fields denoted as Event, End bit, R-bit, Volume, and Duration. 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	**0**-INBAND, DTMF digits are	1	It configures the DTMF type.

.dtmf.type[1]	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.		
account.X.dtmf.dtmf_payload[1]	Integer from 96 to 127	101	It configures the value of DTMF payload. 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. 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. 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.

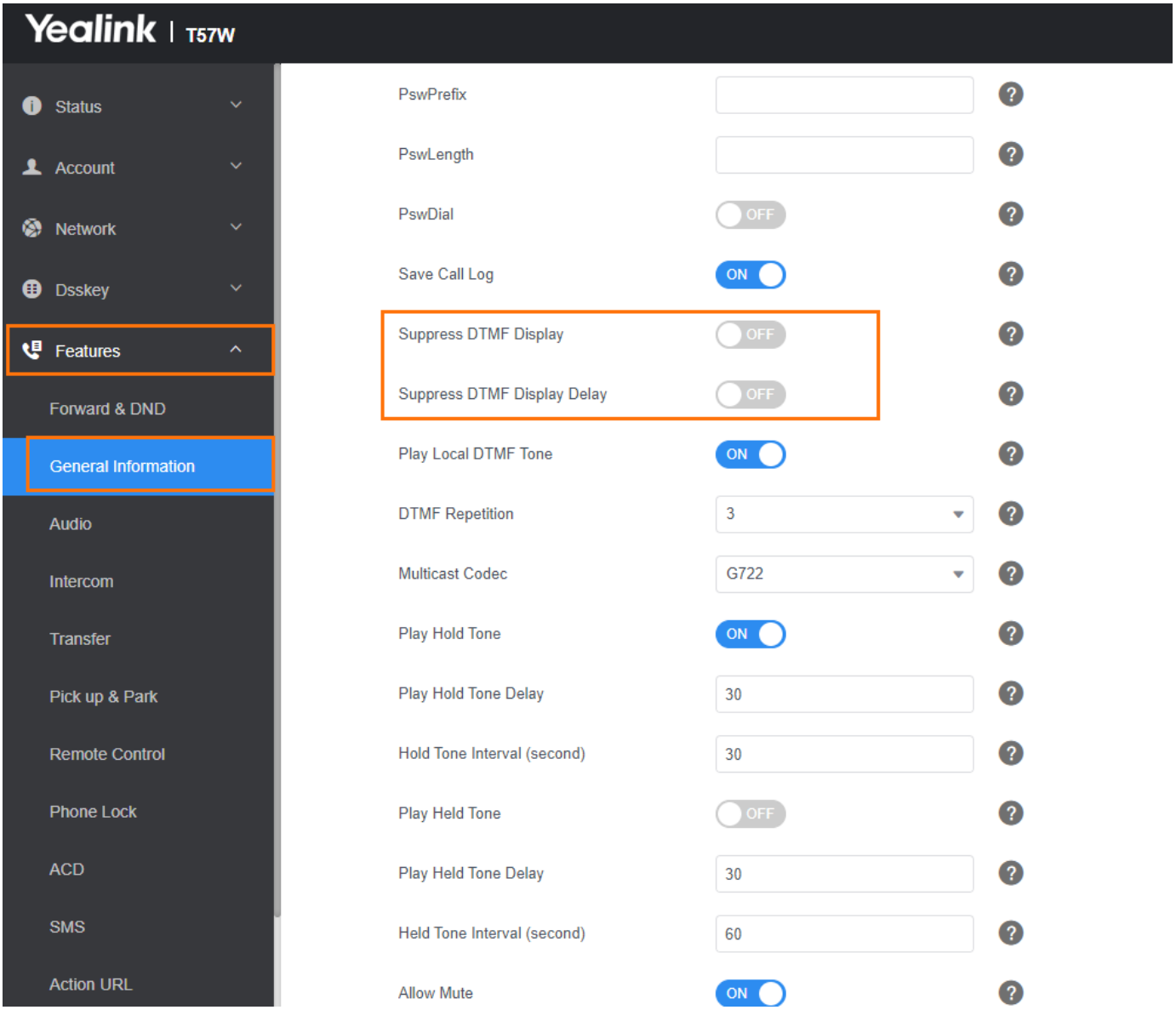
Suppress DTMF Display

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	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to display the DTMF digits for a short period before displaying asterisks

_delay			during an active call. 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**.

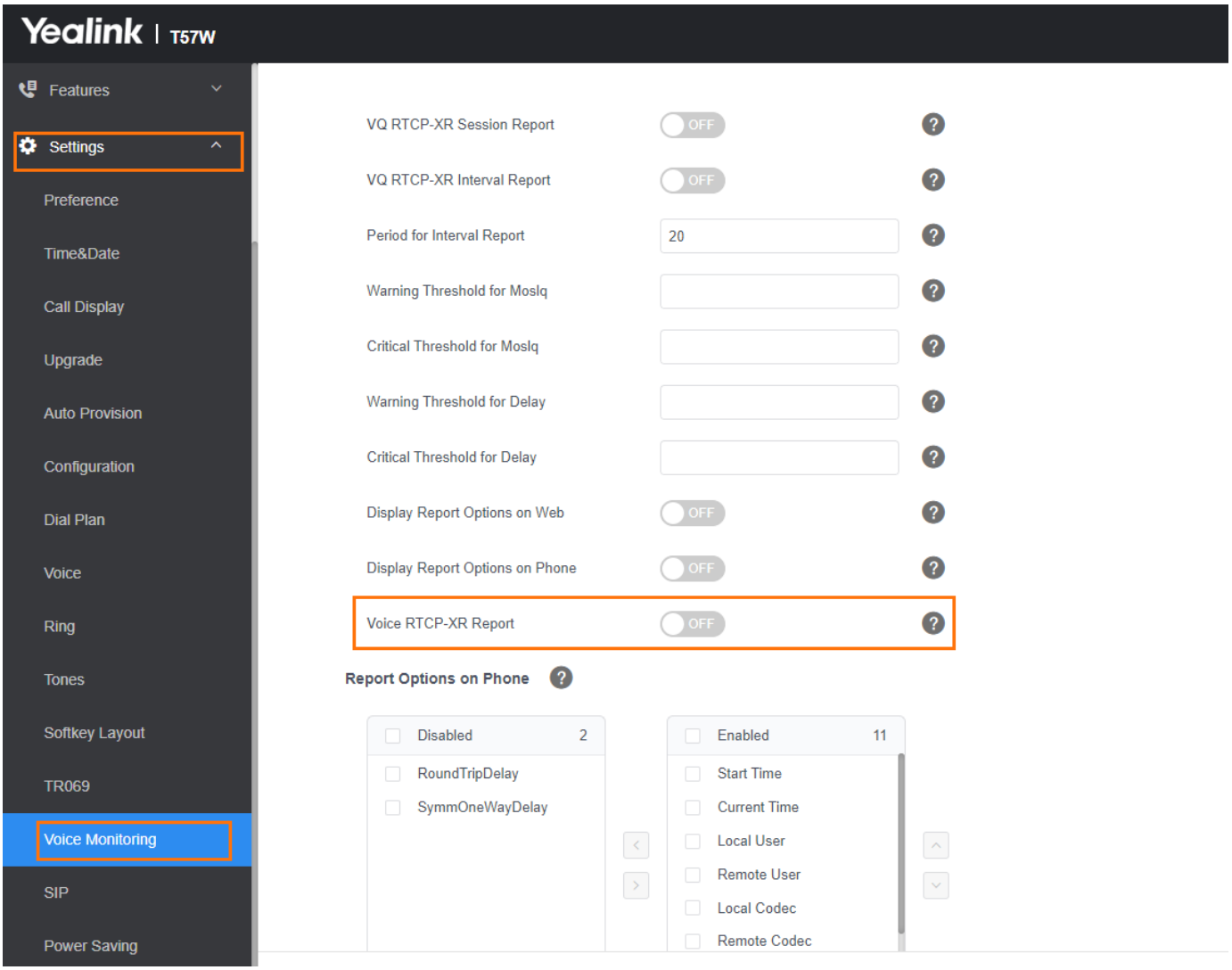
RTCP-XR

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 wilreboot 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 is 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 caluntithe 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

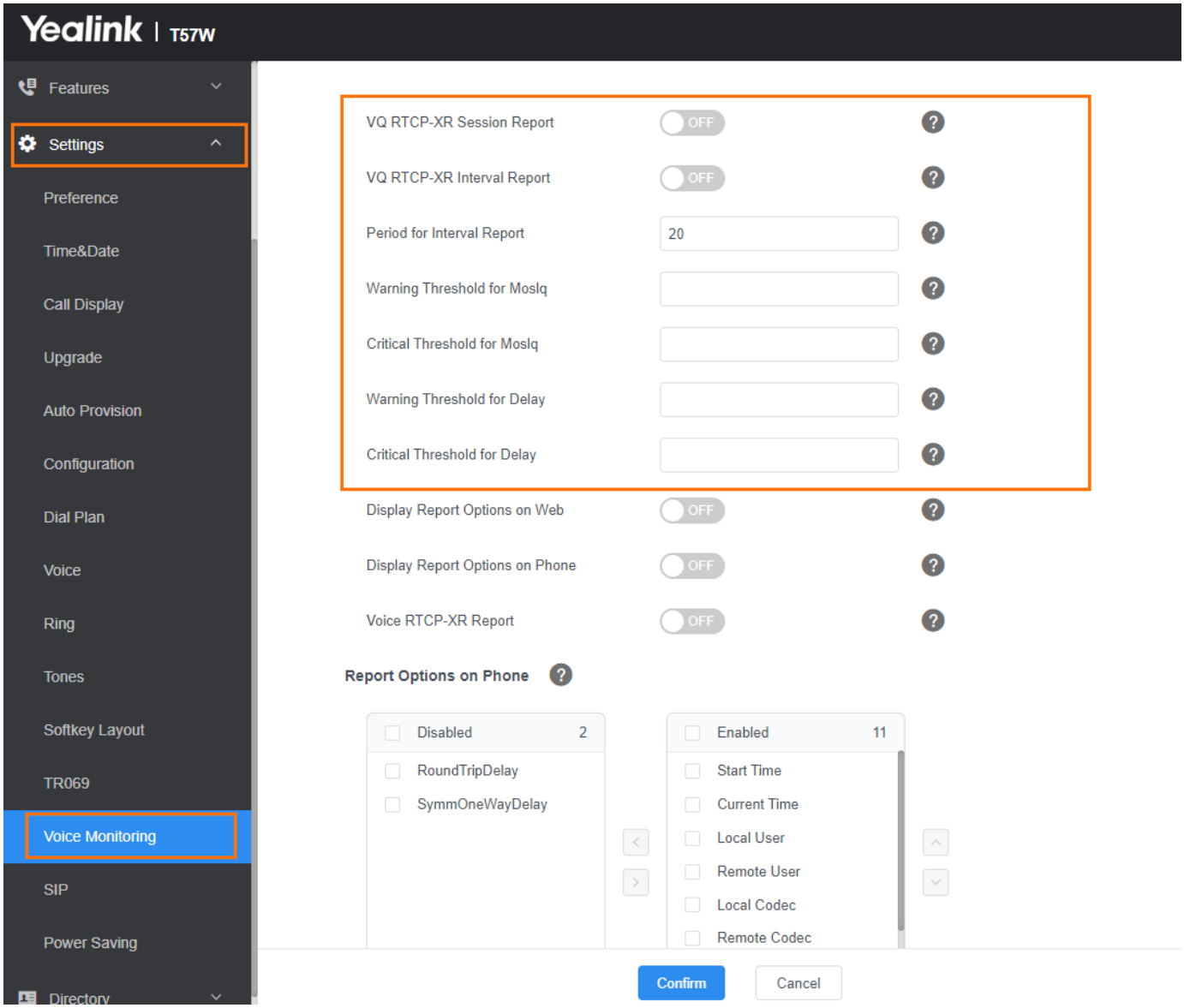
Three types of quality reports can be enabled:

- **Session**: Generated at the end of a call.
- **Interval**: Generated during a calat a configurable period.
- **Alert**: Generated when the calquality 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. 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_	Integer	Blank	It configures the threshold value of the listening MOS

rtcpxr_moslq_threshold_critical	from 15 to 40		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 a 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 a one-way delay. The one-way delay includes both network delay and end system delay.

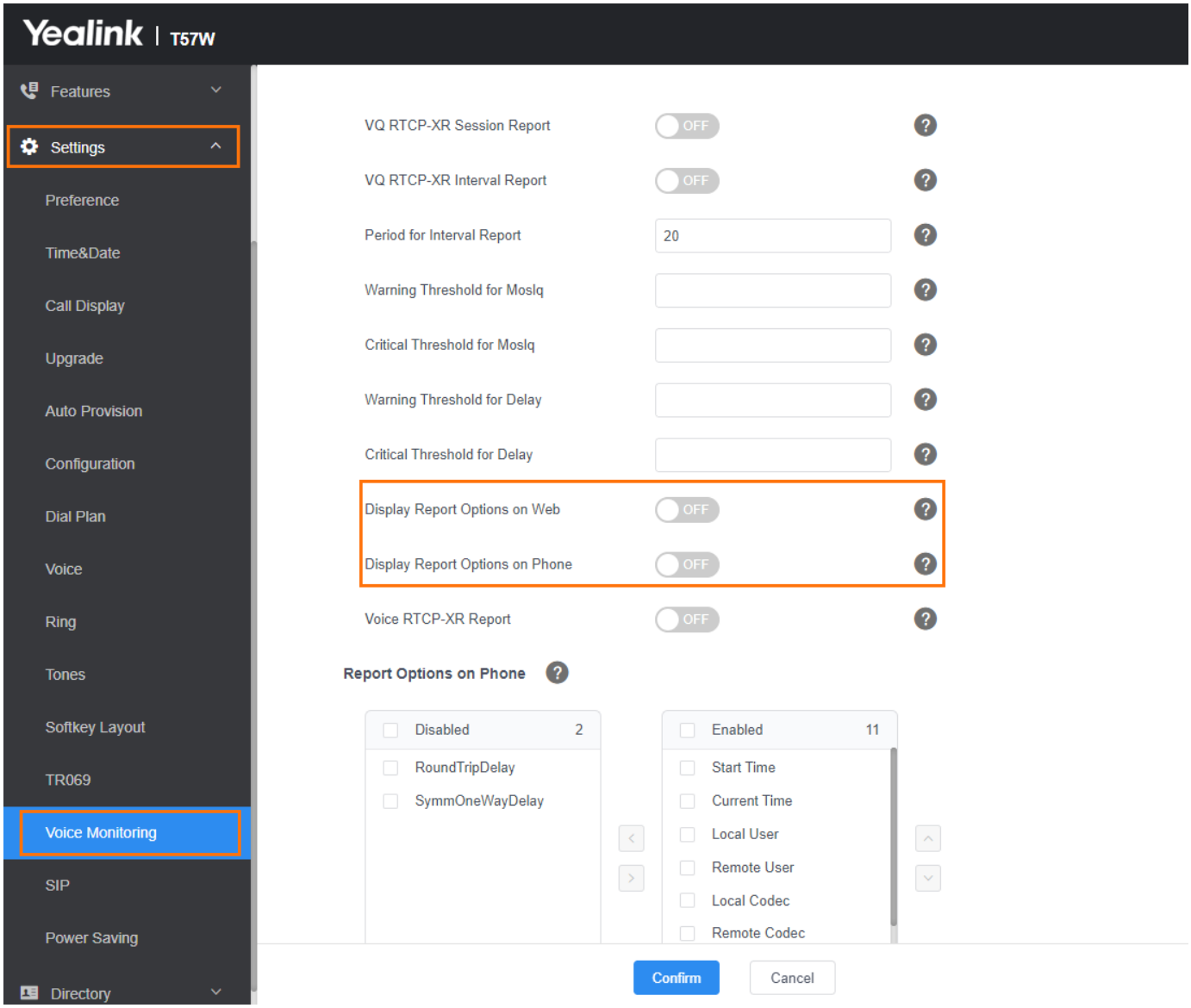
VQ-RTCPXR Display

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	**0**-Dis	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**.

.vq_rtcpxr.states_show_on_web.enable	ab led **1**- En ab led		
phone_setting.vq_rtcpxr.states_show_on_gui.enable	**0**- Dis ab led **1**- En ab led	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.

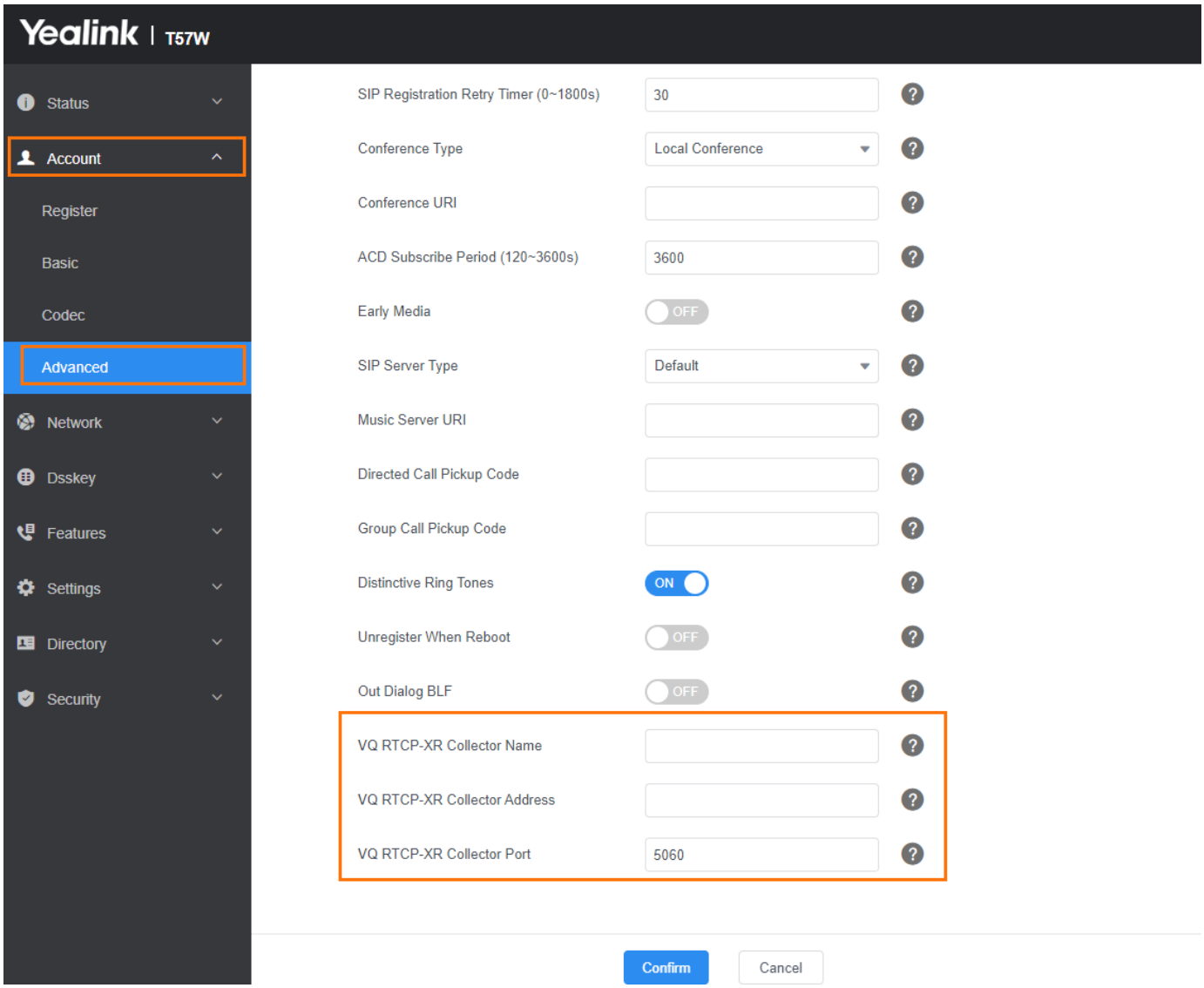
Central Report Collector

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_serv	IPv4 Address/	Blan	It configures the IP address of the central report collector that accepts voice quality reports contained in SIP

er_host[1]	FQDN	k	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

Touch Tone

Touch Tone

If you enable touch tone and tap the keys (except the off-hook key), the phone will produce a sound when it is not on the dialing/pre-dialing screen and not in a call.

For CP925/CP935W, the phone will produce a sound when you tap an option on the phone screen.

> It is only applicable to touchscreen phones.

Touch Tone Configuration

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

Parameter	Description	Permitted Values	Defau lt
features.touch_tone	It enables or disables the touch tone.	0-Disabled 1-Enabled	1

Ring Tones

Ring Tones

Ring tones are used to play for incoming calls. You can select a built-in ring tone or a custom ring tone 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 of time after which the phone will stop ringing if the call is not answered.

Custom Ringtone Limit

The ring tone format must meet the following:

Phone Model	Format	Single File Size
Color Screen Phones	.wav	<=8MB
Black-and-white Screen Phones	.wav	<=100KB

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	Permitted Values	Default	Description
phone_settin	Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav,	Ring	It configures a ring tone for the phone.

g.ring_type	Silent.wav, Splash.wav or custom ring tone name (for example, Customring.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)	1.wav	
account.X.ringtone.ring_type[1]	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) 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	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".
pstn.account.X.ring_type[2]	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	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".
ringtone.url	URL within 511 characters	Blank	It configures the access URL of the custom ring tone file.

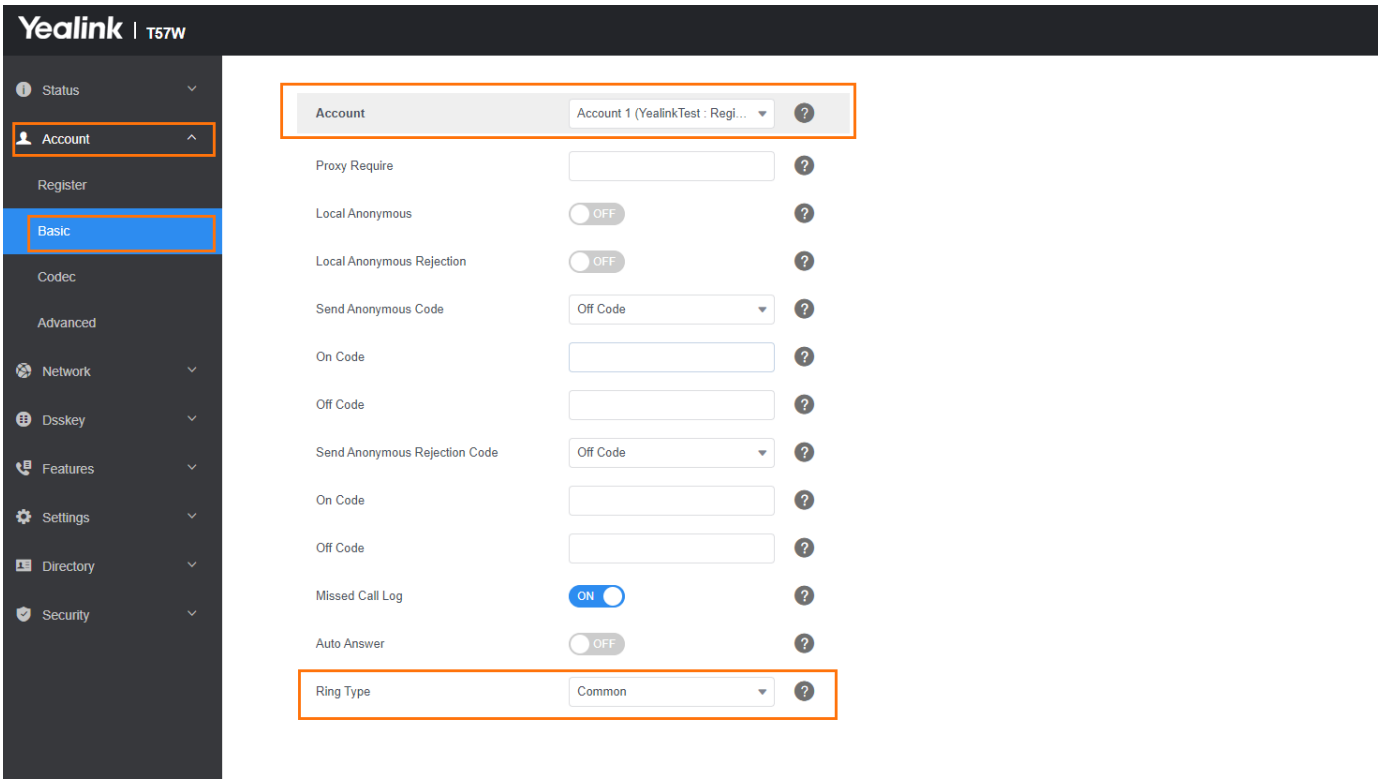
ringtone.delete	http://localhost/all	Blank	It deletes all custom ring tone files.
phone_setting.ringing_timeout	Integer from 1 to 3600	120	It configures the duration time (in seconds) in the ringing state. If it is set to 180, the phone will stop ringing if the call is not answered within 180 seconds.
phone_setting.ring_for_tranfailed	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	It configures the ring tone when the phone fails to transfer a call and displays "Transfer failed" on the screen.

> [1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T58W/T58A/VP59/T56A/T58V, X=1-16; for T53W/T53/T53C/T43U/T42G/T42U/T42S, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 § E2, X=1-2; for T30P/T30/T19 § E2/CP920/CP925/CP935W, X=1.

> [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

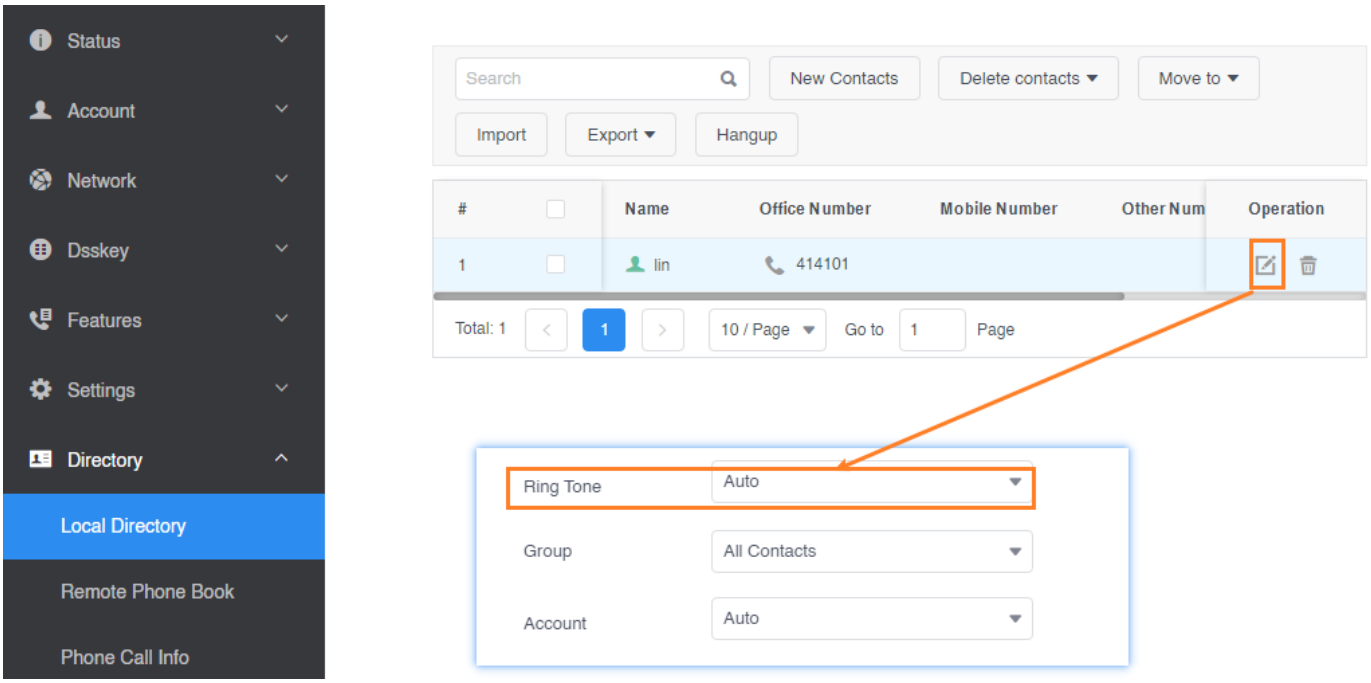
The priority of the ringtone.

There are several ringtone settings in the phone, the priority from high to low is shown below.

You can change the ringtone according to the priority.

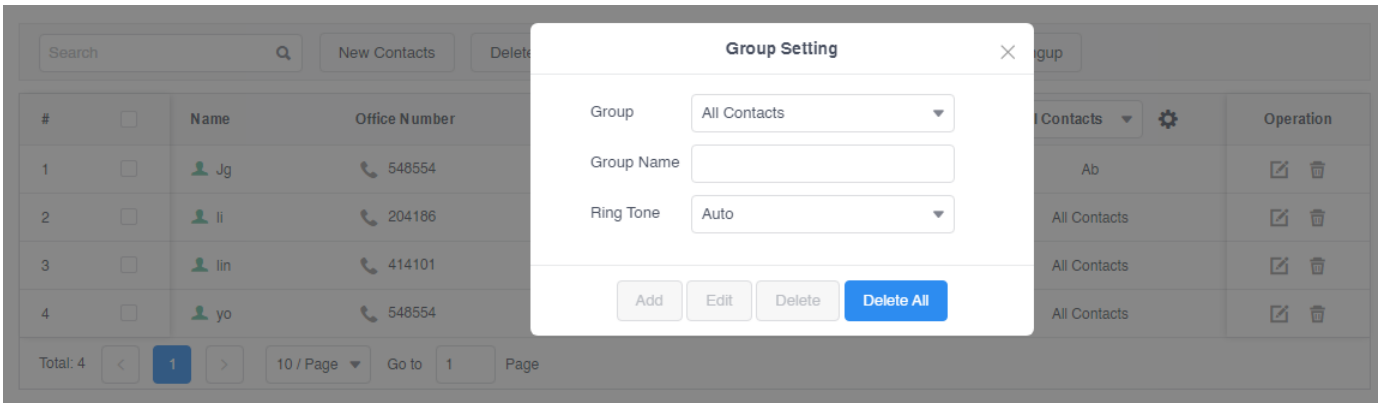
1. Contact Ringtone

On the web user interface, go to **Directory** > **Local Directory** > > Ring Tone.



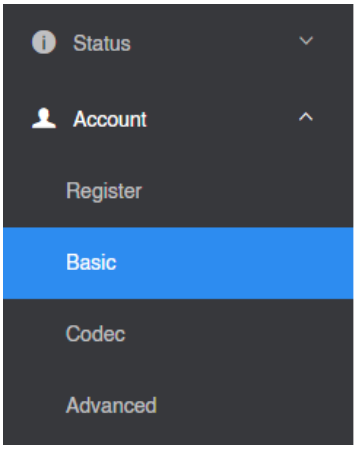
2. Group Ringtone

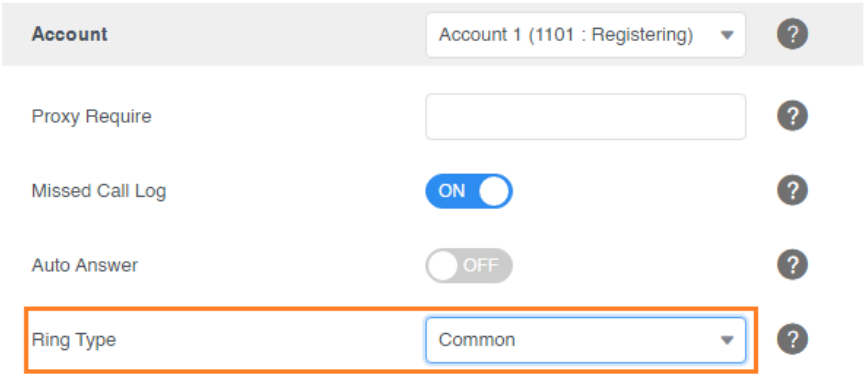
On the web user interface, go to **Directory** > **Local Directory** > > Group Setting.



3. Account Ringtone

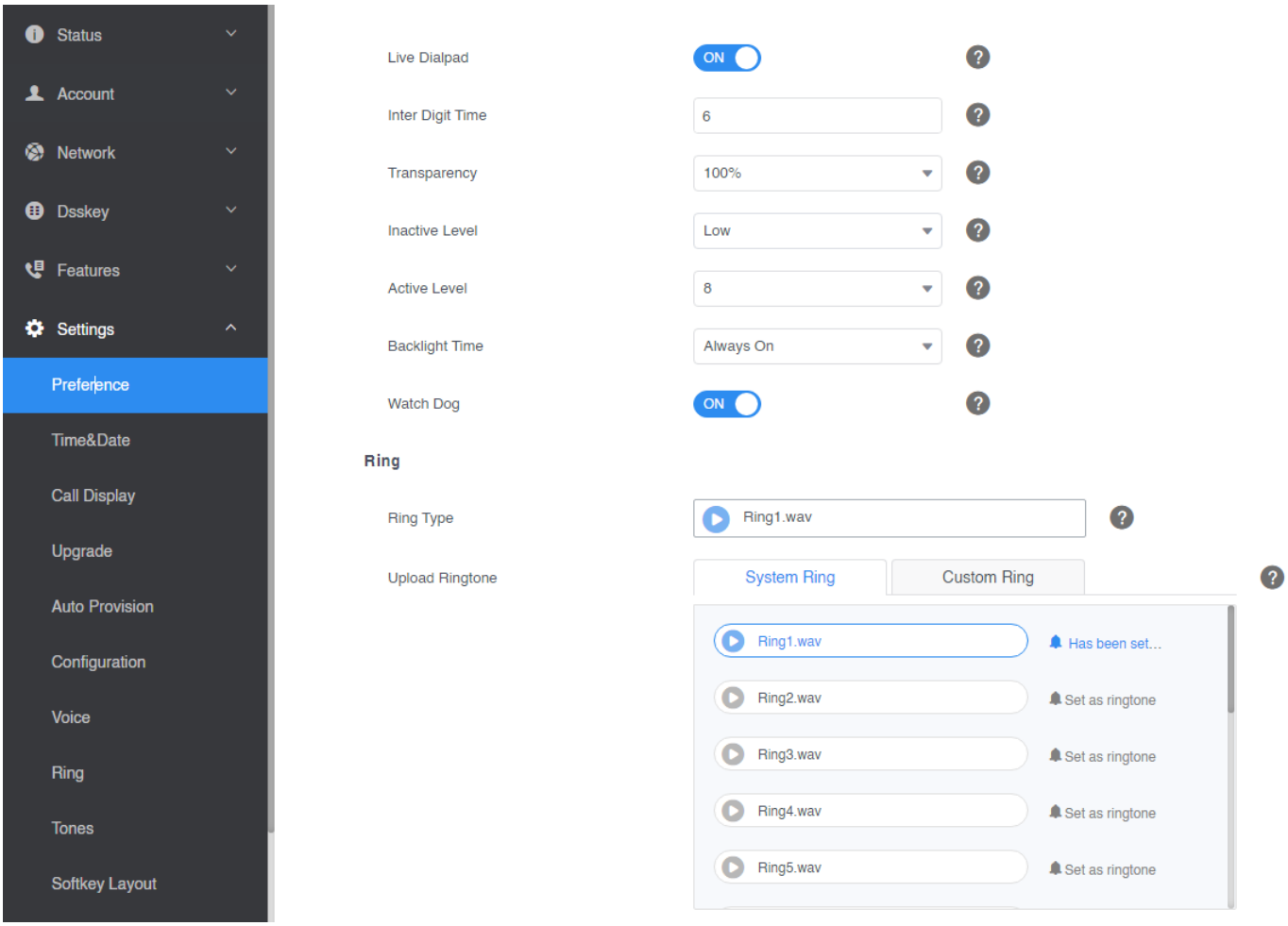
On the web user interface, go to **Account** > **Basic** > **Ring Type**.





4. Default Ringtone

On the web user interface, go to **Settings** > **Preference** > **Ring Type**.


Status
Account
Network
Dsskey
Features
Settings
Preference
Time&Date
Call Display
Upgrade
Auto Provision
Configuration
Voice
Ring
Tones
Softkey Layout
Live Dialpad
ON
Inter Digit Time
6
Transparency
100%
Inactive Level
Low
Active Level
8
Backlight Time
Always On
Watch Dog
ON
Ring
Ring Type
Ring1.wav
Upload Ringtone
System Ring
Custom Ring
Ring1.wav
Has been set...
Ring2.wav
Set as ringtone
Ring3.wav
Set as ringtone
Ring4.wav
Set as ringtone
Ring5.wav
Set as ringtone

Headset Prior & Dual Headset

Headset Prior

The headset prior allows users to use the headset preferentially if a headset is physically connected to the IP phone. This feature is especially useful for permanent or full-time headset users.

1. It is not applicable to the Bluetooth headset and USB headset.
2. It is not applicable to CP920/CP925/CP935W/CP960/CP965 phones.

Headset Prior Configuration

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

Configuration parameter

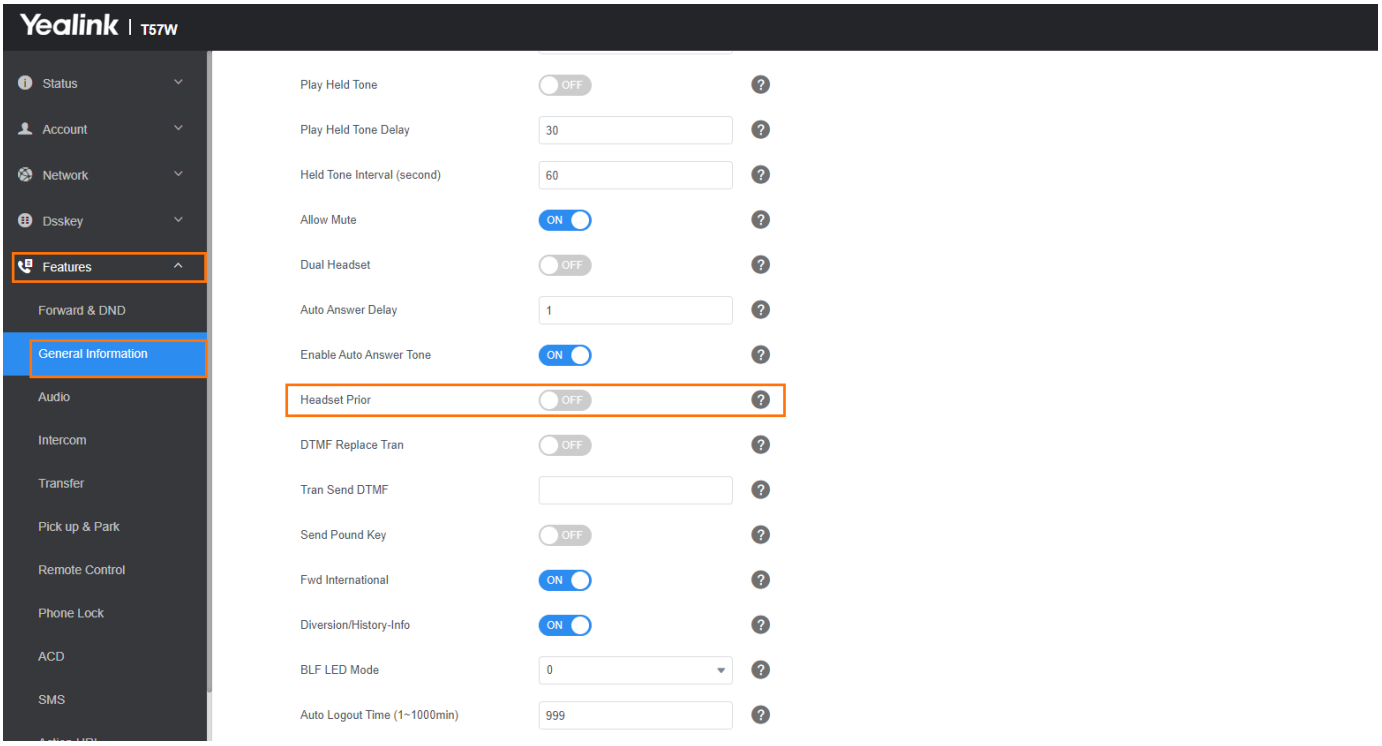
features.headset_prior
features.headset.ctrl_call.enable

Parameter	Permitted Values	Default	Description
features.headset_prior	0-Disabled, the headset mode will be deactivated after the call, if you switch the headset mode to speakerphone/handset mode. 1-Enabled, the headset mode will not be deactivated after the call, even if you switch the headset mode to speakerphone/handset mode.	0	It enables or disables to use of the headset mode for all incoming and outgoing calls. It works only if "features.headset_mode.enable" is set to 1 (Enabled).
features.headset.ctrl_call.enable	0-Disabled 1-Enabled	0	It enables or disables the user to initiate or end a call by pressing the HEADSET key. It works only if "features.headset_mode.enable" is

			set to 1 (Enabled).

Set via the Web User Interface

On the web user interface, go to **Features** > **General Information** > **Headset Prior.**



Dual Headset

The dual headset allows you to use two headsets on one IP phone. To use this feature, you need to physically connect two headsets to the headset and handset jacks, respectively. Once the IP phone connects to a call, the headset connected to the headset jack has full-duplex capability, while the headset connected to the handset jack is only used for listening.

> The dual headset is not applicable to the Bluetooth headset or the USB headset. It is not applicable to CP920/CP925/CP935W phones.

Dual Headset Configuration

The following table lists the parameters you can use to configure a dual headset.

Configuration parameter

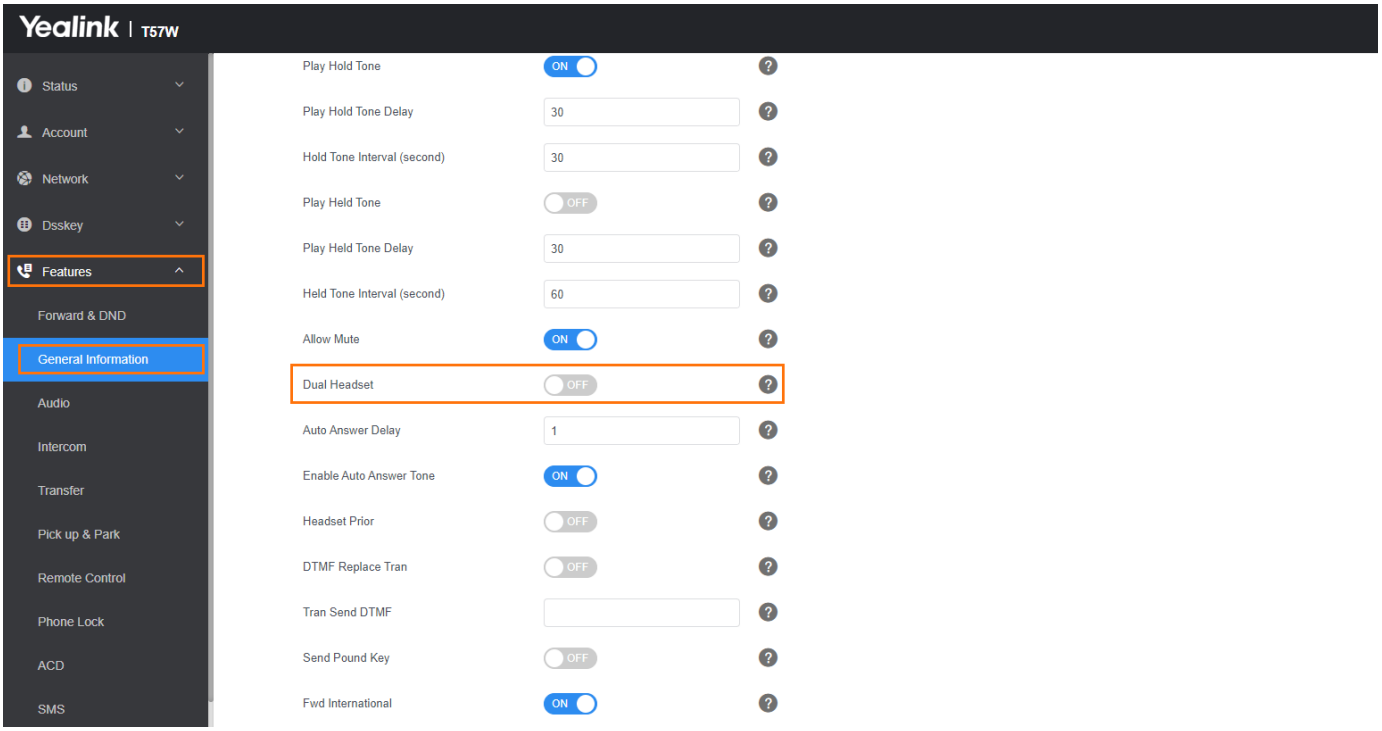
features.headset_training

Parameter	Permitted Values	Default	Description

features.headset_training	0-Disabled 1-Enabled, users can use two headsets on one phone. When the IP phone joins a call, the headset connected to the headset jack has full-duplex capability, while the headset connected to the handset jack is only used for listening.	0	It enables or disables the dual headset feature. It works only if "features.headset_mode.enable" is set to 1 (Enabled).

Set via the Web User Interface

On the web user interface, go to **Features** > **General Information** > **Dual Headset.**


Yealink | T57W
Status
Account
Network
Dsskey
Features
Forward & DND
General Information
Audio
Intercom
Transfer
Pick up & Park
Remote Control
Phone Lock
ACD
SMS
Play Hold Tone
ON
Play Hold Tone Delay
30
Hold Tone Interval (second)
30
Play Held Tone
OFF
Play Held Tone Delay
30
Held Tone Interval (second)
60
Allow Mute
ON
Dual Headset
OFF
Auto Answer Delay
1
Enable Auto Answer Tone
ON
Headset Prior
OFF
DTMF Replace Tran
OFF
Tran Send DTMF
Send Pound Key
OFF
Fwd International
ON

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
account.X.noise_filter.mode

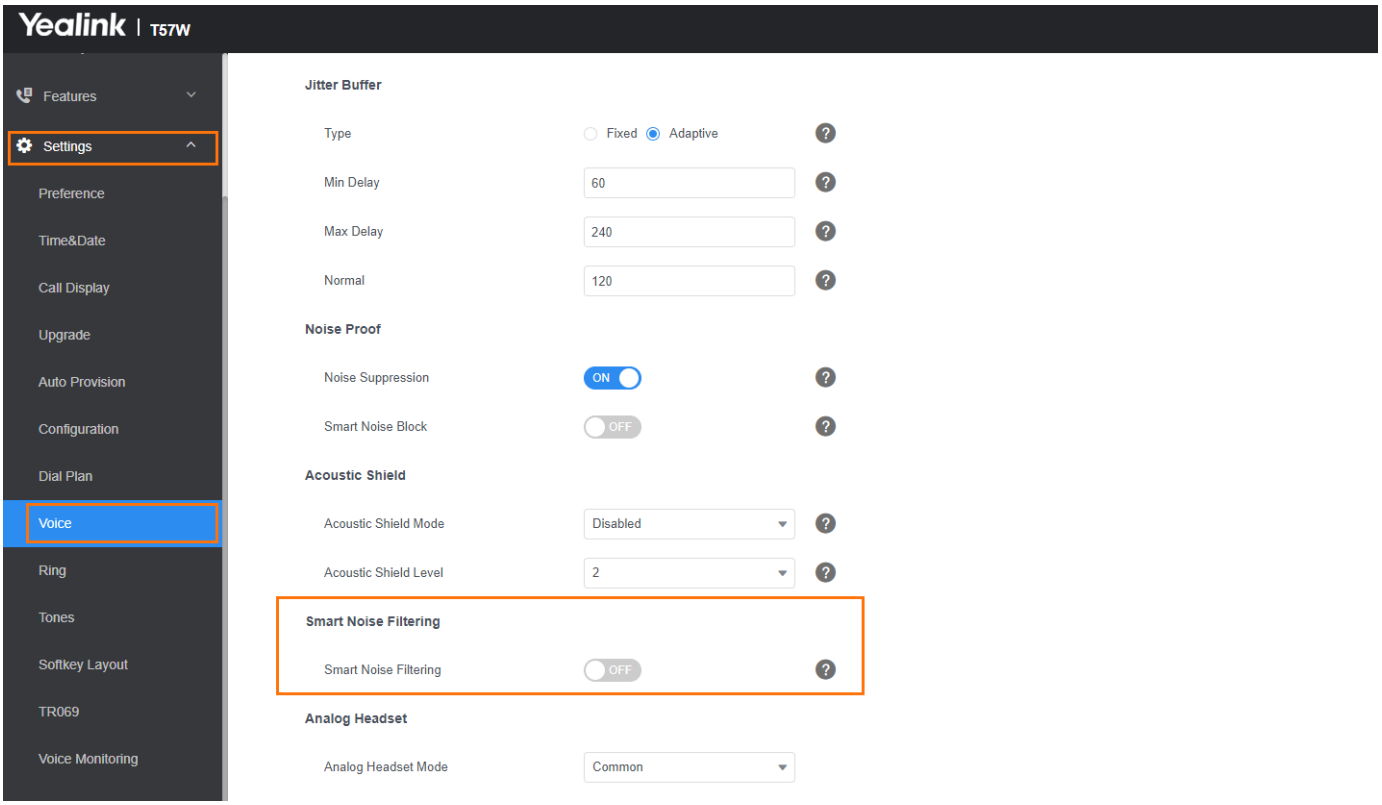
Parameter	Permitted Values	Default	Description
features.noise_filtering_rev.enable	0-Disabled 1-Enabled	0	It enables or disables the phone to block out the slight noise from the far end when there is no speech in a call. After smart noise filtering is enabled, if the far end is playing music or calling a voice service, the background music will also be eliminated when there is no speech in a call.
account.X.noise_filter.mode[1]	0-Enabled, you can hear the slight noise when on hold. 1-Disabled	0	It enables or disables the phone to block out the slight noise from the far end when there is no speech and is on hold in a call. It works only if "features.noise_filtering_rev.enable" is set to 1 (Enabled).

[1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T58W/T58A/VP59/T56A/T58V, X=1-16; for T53W/T53/T53C/T43U/T42G/T42U/T42S, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 § E2, X=1-2;

> for T30P/T30/T19 § E2/CP920/CP925/CP935W/CP960/CP965, X=1.

Set via the Web User Interface

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



Acoustic Shield

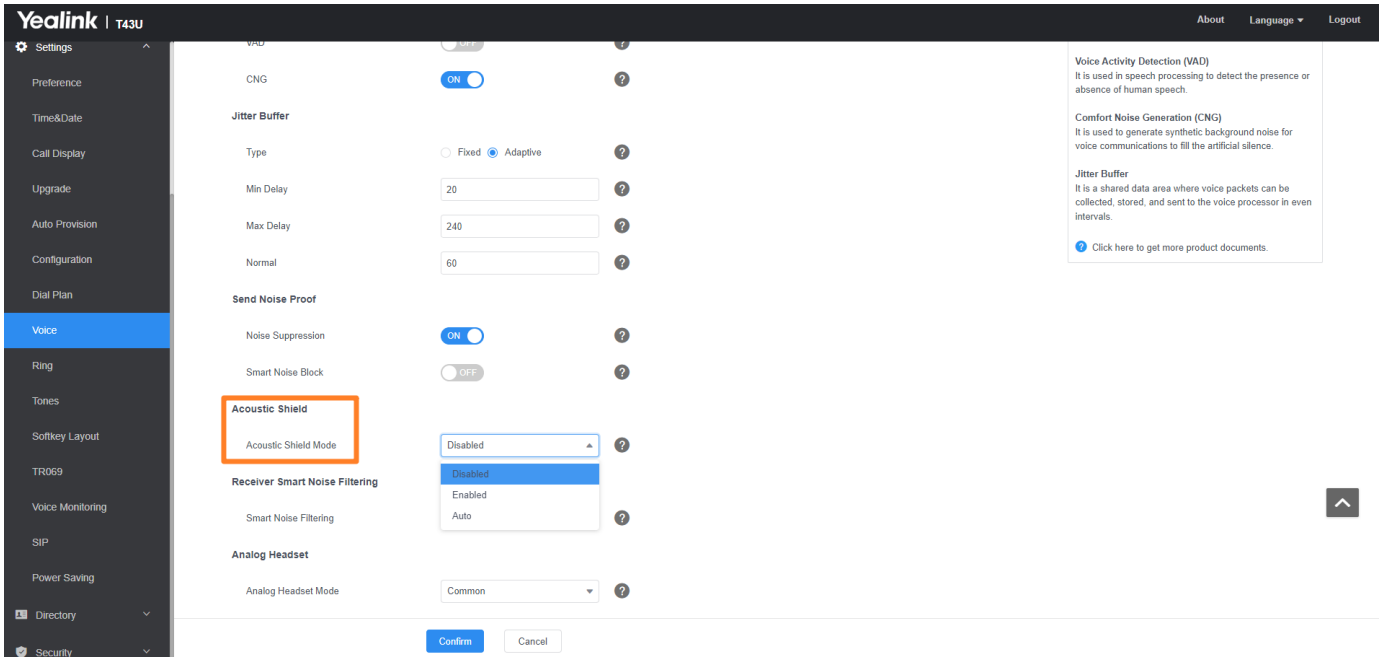
Introduction

The acoustic shield feature is designed to suppress background noise when you are using a phone or a connected headset.

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

Via Web User Interface

1. Go to **Settings** > **Voice** > **Acoustic Shield**.



Via Auto Provisioning

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

features.acoustic_shield.mode
features.acoustic_shield_display.enable

Parameter	Permitted Values	Default	Description
features.acoustic_shield.mode	**0**- Disabled **1**- Enable (The call does not start automatically).	2	It enables or disables the acoustic shield feature during the call.

	2- Auto, the acoustic shield is automatically enabled when the call is set up.		
features.acoustic_shield_display.enable	**0**- Disabled **1**- Enable	0	It controls whether the acoustic shield switch is displayed on the softkey. **Note**: It works only if "features.acoustic_shield.mode" is set to 1 (Enabled).

Noise Proof

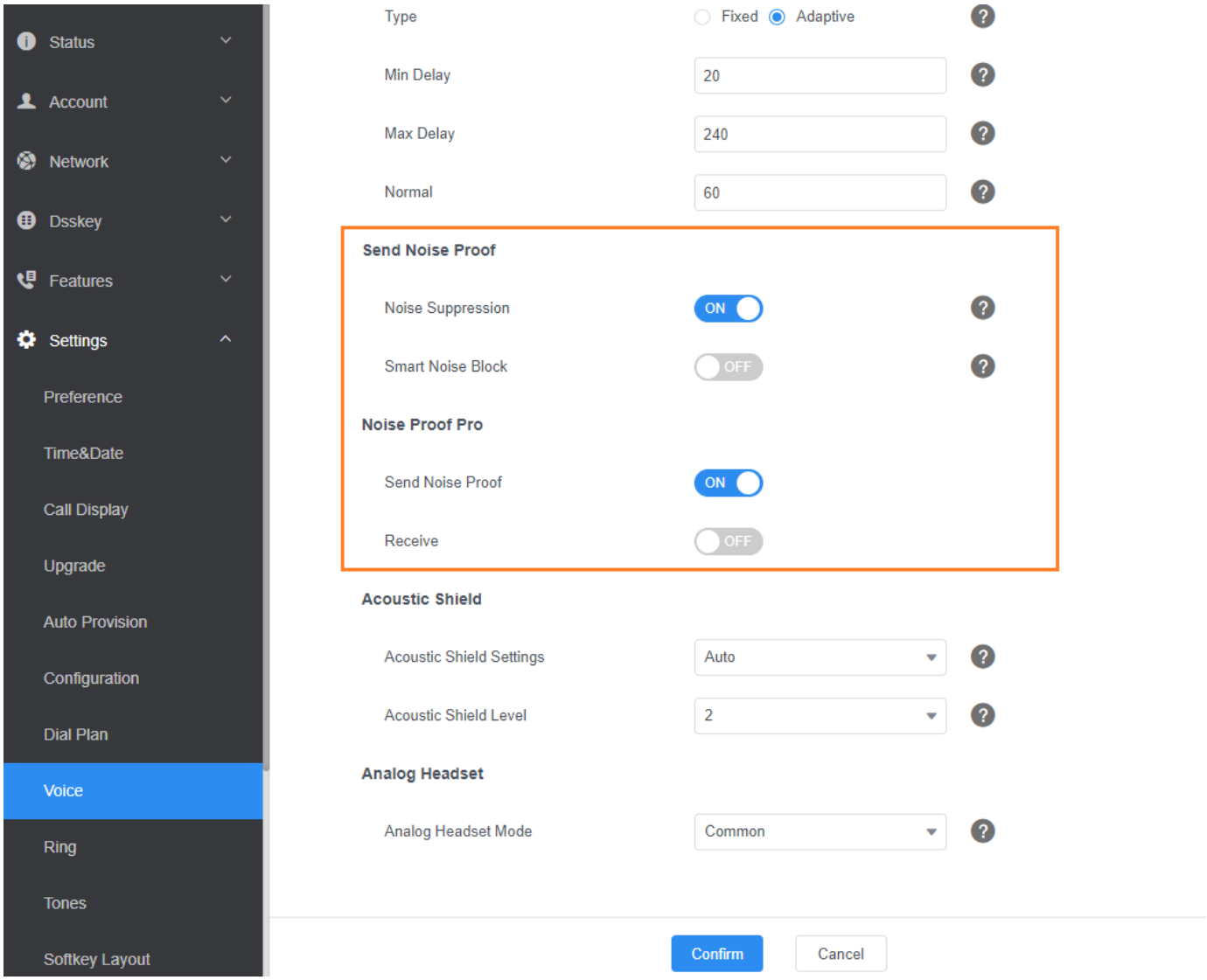
Introduction

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

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

Via Web User Interface

1. Go to **Settings** > **Voice** > **Send Noise Proof**.



Via Auto Provisioning

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

voice.tns.enable
voice.ans_nb.enable

Parameter	Permitted Values	Default	Description
voice.tns.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the **Noise Suppression** feature.
voice.ans_nb.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the **Smart Noise Block** feature. It works only if "voice.tns.enable" is set to 1 (Enabled).

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 a 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 replacement 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 rules now.
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 the 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.

You can configure these four patterns via the web user interface or auto-provisioning. To replace the 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 parentheses "( )" 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 or 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

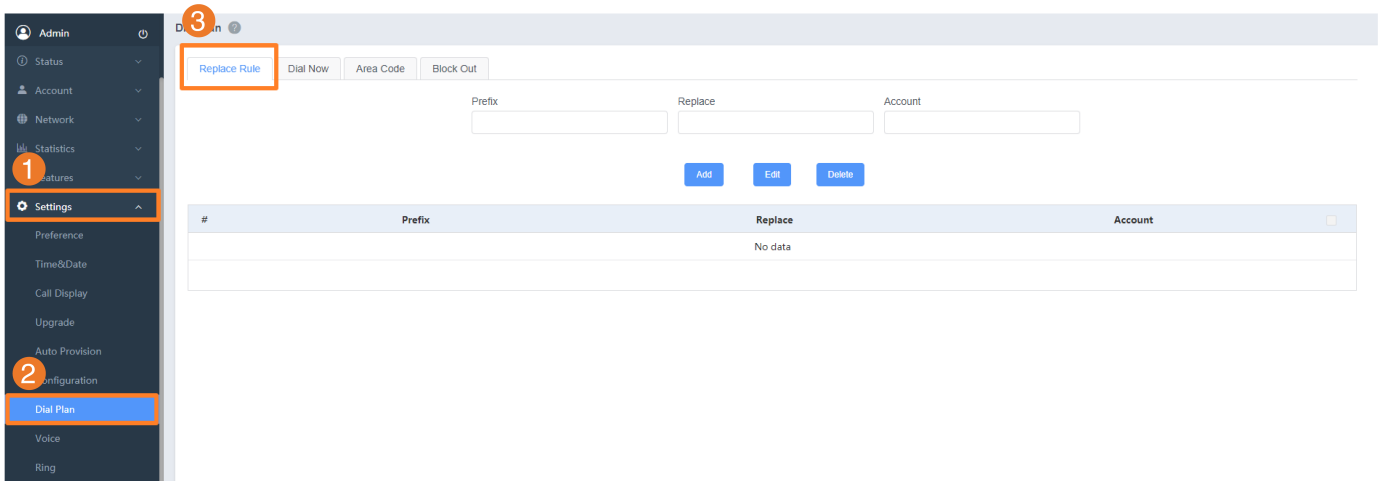
1. Open the dial now file.
2. To add a dial-now rule, add <Data DialNowRule="" LineID="" /> to the file. Each starts on a new line.
3. Specify the values within double quotes.
   For example,
   <Data DialNowRule="1001" LineID="0" />
4. Save the changes and place this file on the provisioning server.

Replace Rule Configuration

You can configure replace rules either one by one or in batches 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. 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 the replace rule template file, refer to Replace Rule File Customization.

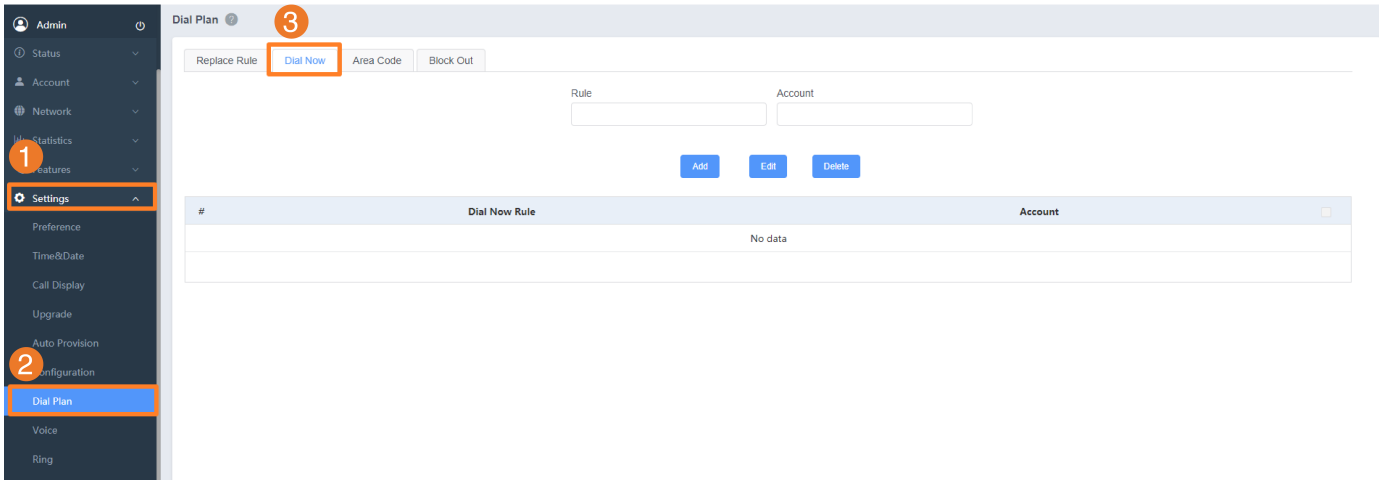
> [1] X is from 1 to 100.

Dial Now Configuration

You can configure dial now rules either one by one or in batch 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. 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.

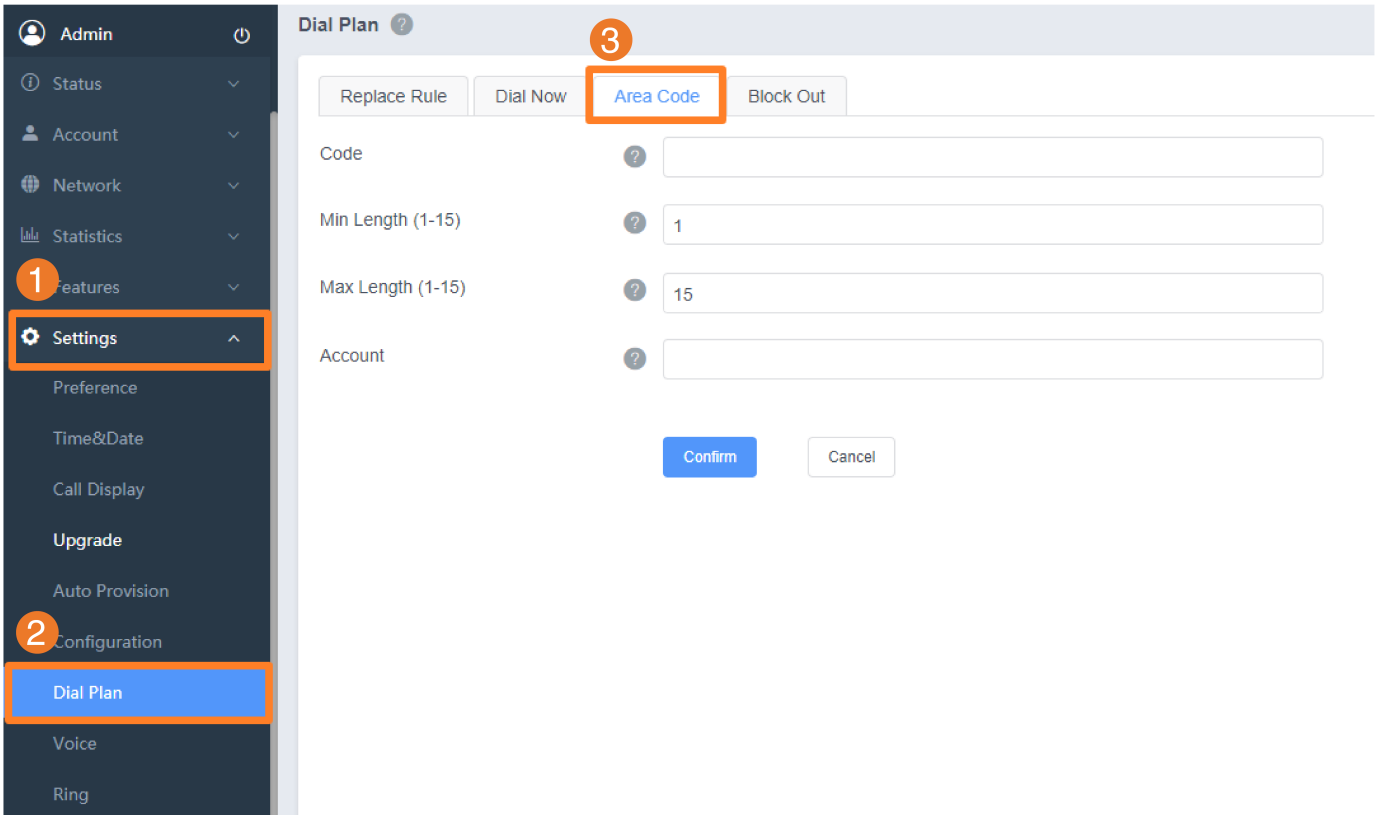
			If it is set to 0, the phone will automatically dial the entered number immediately.
dialplan_dialnow.url	String within 511 characters	Blank	It configures the access URL of the dial now template file. For customizing the dial now template file, refer to Dial Now File Customization.

> [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

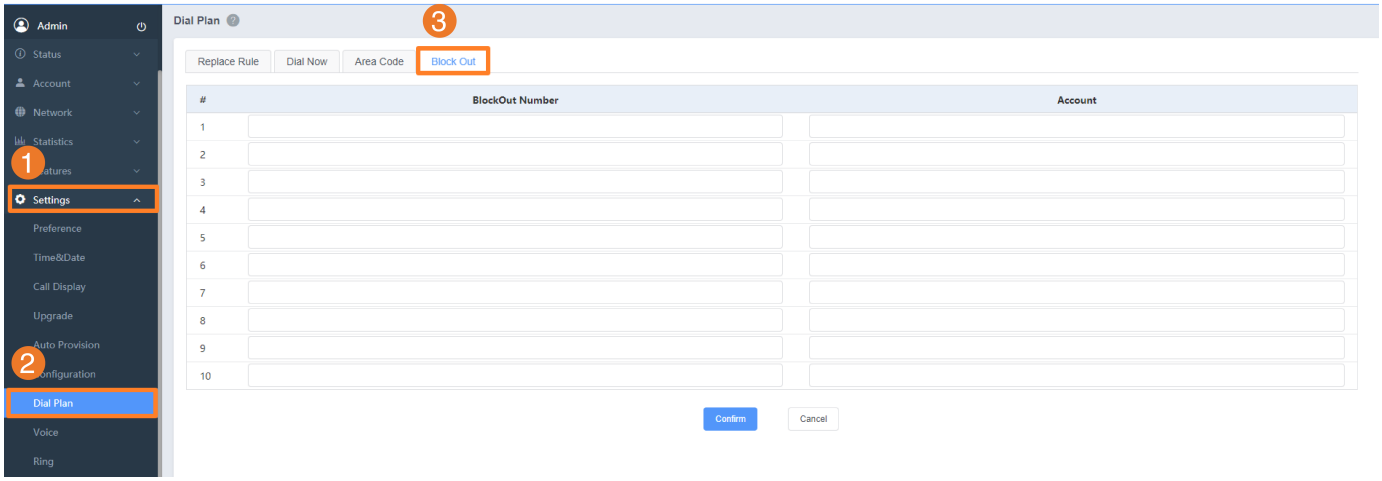
Parame	Permitt	Def	Description

ter	ed Values	aul t	
dialpla n.area_ code.co de	String within 16 characte rs	Bl an k	It configures the area code to be added before the entered numbers when dialing out. 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.
dialpla n.area_ code.mi n_len	Integer from 1 to 15	1	It configures the minimum length of the entered number.
dialpla n.area_ code.m ax_len	Integer from 1 to 15	15	It configures the maximum length of the entered number. The value must be larger than the minimum length.
dialpla n.area_ code.li ne_id	0 to 250	Bl an k	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. 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. Multiple line IDs are separated by commas.

> [1]X is from 1 to 10.
> [2]X is 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 on 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.

Emergency Dialplan and Enhanced 911

Introduction

You can dial the emergency telephone number (emergency services number) at any time when the IP 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 dial plan and enhanced 911.

Emergency Dial Plan

You can configure the emergency dial plan for the phone (for example, emergency number, 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, avoiding that emergency calls could not get through, because of a 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	Defaul	Description

		t	
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	It configures the precedence of the source of emergency outbound identities when placing an emergency call. 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).

	ELIN value will be used.		
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	Blank	It configures the custom outbound identity when placing an emergency call. It works only if "dialplan.emergency.enable" is set to 1 (Enabled).

	example, tel: +16045558000. The full URI is included in the P-Asserted-Identity (PAI) header (for example, <tel: +16045558000 >).		
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. 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 the emergency server X to be used for routing calls. 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. It works only if "dialplan.emergency.enable" is set to 1 (Enabled).
dialplan.emergency.X.value[2	Number or SIP URI	When X = 1,	It configures the emergency number to use on your phones so a caller can contact emergency

]		the default value is 911; When X = 2-255, the default value is Blank.	services in the local area when required. 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. 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. 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	SIMPLE	It configures the type of location request message. It works only if "dialplan.emergency.enable" is set to 1 (Enabled) and "dialplan.emergency.asserted_id_source" is set to **HELD**.

	send the location request message defined by REDSKY.		
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 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 It works only if "dialplan.emergency.enable" is set to 1 (Enabled) and "dialplan.emergency.asserted_id_source" is set to **HELD**.
dialplan.emergency.hel	String	Blank	It configures the user name authentication when the phone sends location information to the E911

d.username			Location Information Server. 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. 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. 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. 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. 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	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.

	the E911 Location Information Server again when it fails 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.		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. 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"	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. It works only if "dialplan.emergency.held.request_type" is set to **YEALINK** or **REDSKY**.

	, "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.		
sip.emgr.header	**priority: emergency**-The E911 INVITE header field contains priority: emergency. **String**-The IVITE header field can be customized.	priority: emergency	It configures the content of the 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.	0	It configures the contents of held requests when the phone cannot connect to the LDAP switch.

	1-The phone sends the ChassisID and PortID fields to the server; the ChassisID field is the MAC of the gateway, and the PortID field is the MAC of the phone.		
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 hold 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 line 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.

> 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

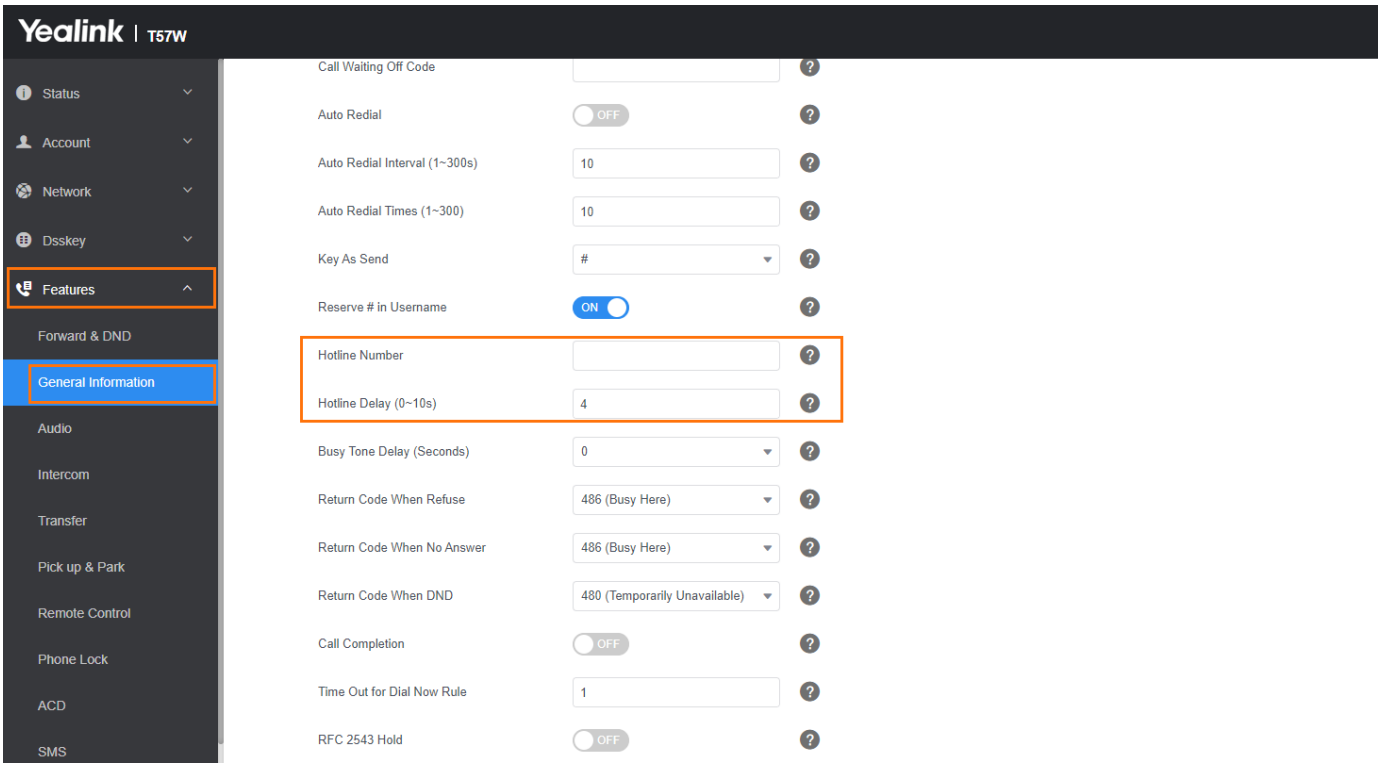
features.hotline_number
features.hotline_delay

Parameter	Description	Permitted Values	Defaul t
features.hot line_number	It configures the hotline number that the phone automatically dials out when you lift the handset, press the **Speakerphone**/**off-hook** key, or the line key. Leaving it blank disables the hotline feature. > Line key is not applicable to T30P/T30/T19 E2/CP920 phones; **handset** and **Speakerphone** keys are not applicable to CP920/CP925/CP935W phones; the **off-hook** key is only applicable to CP920 phones.	String within 32 characters	Blank
features.hotl ine_delay	It configures the waiting time (in seconds) for the phone to automatically dial out the preset	Integer from 0 to 10	4

	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. Line key is not applicable to T30P/T30/T19 E2/CP920 phones; **handset** and **Speakerphone** key are not applicable to CP920/CP925/CP935W phones; the **off-hook** key is only applicable to CP920 phones.		

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 hot line 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 use this account to dial out a call successfully.

Off-hook hot line dialing feature is configurable on a per-line basis and depends on the support from a SIP server. The server actions may vary from different servers.

It is also applicable to the IP call and intercom call.

> Off-hook hot line 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 when a user calls any number. 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 dedicated DSS keys.

Speed Dial Key Configuration

There are two ways to configure a Speed Dial key:

- Manually, configure a line key or programmable key as a Speed Dial key.
- Automatically assign a favorite contact, and the phone automatically links the contact to a line key.

The following shows manual configuration for a Speed Dial key.

Scenario Conditions	Related Topic
local_contact.favorite.enable = 0	Favorite Contacts

Line Key Configuration	Programmable Key Configuration
linekey.X.type = 13 linekey.X.line = 1 linekey.X.value = 4603 linekey.X.label = Bill	programablekey.X.type = 13 programablekey.X.line = 1 programablekey.X.value = 4603

After provisioning, a Speed Dial key for Bill (4603) is available on the phone, and you can press the Speed Dial key to call Bill (4603) quickly.

You can configure multiple Speed Dial keys for different contacts, which are used frequently or are hard to remember. Alternatively, you can use the favorite contact feature and automatically assign Speed Dial keys for favorite contacts.

FAQ

1. How to Set Number Keys as Speed Dial Keys

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 conceal the identity information shown to the callee. The callee’s phone LCD screen prompts an incoming call from an anonymous caller.

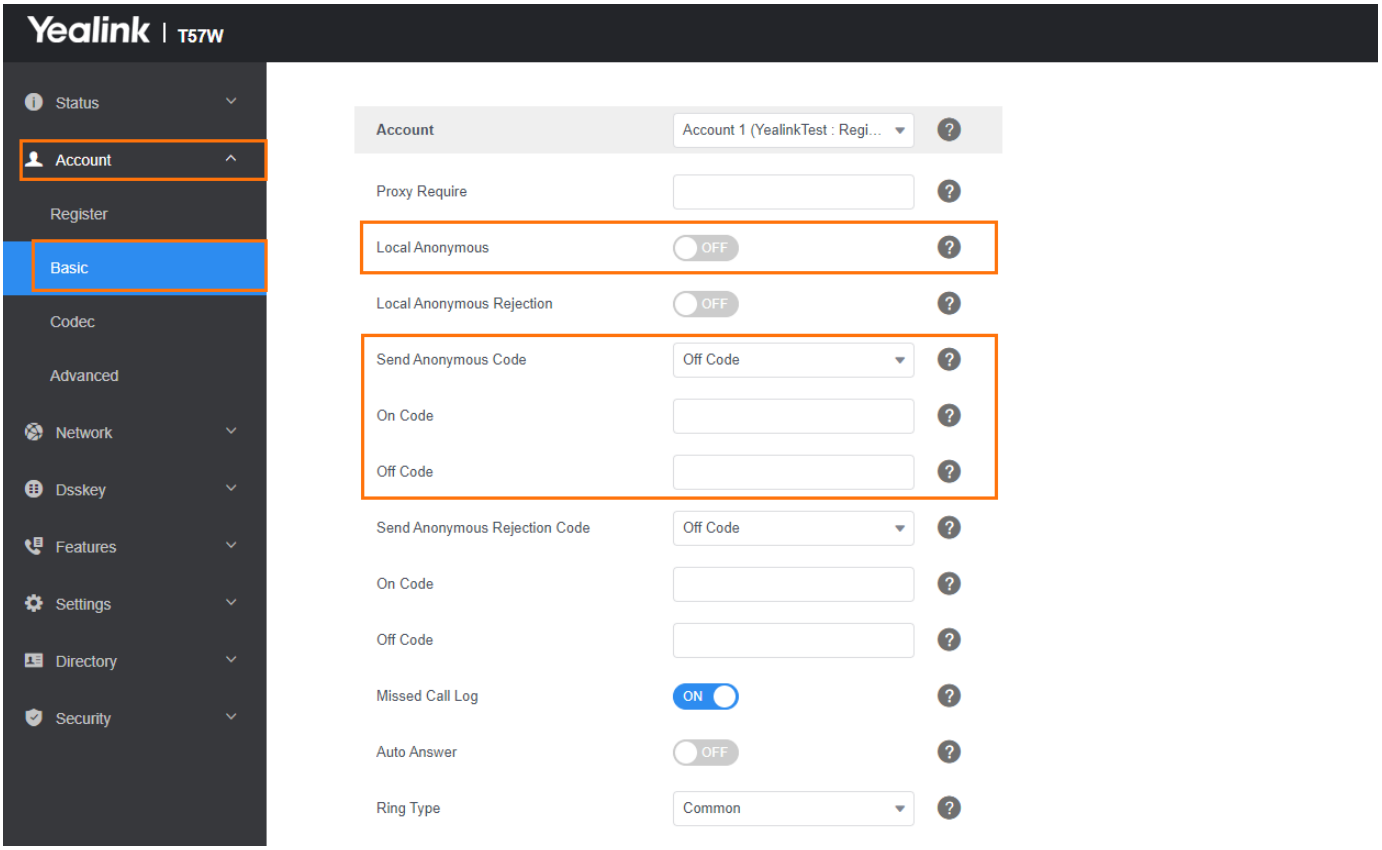
Anonymous calls can be performed locally or on the server. When performing an anonymous call on local, the phone sends an INVITE request with a call source "From: "Anonymous" sip:anonymous@anonymous.invalid”. If performing an Anonymous call on a specific server, you may need to configure anonymous call on code and off code to activate and deactivate the server-side anonymous call feature.

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 turn on or off.
account.X.send_anonymous_code[1]	**0**-Off Code, the phone will send an anonymous off code to the server when you deactivate the anonymous call feature. **1**-On Code, the phone will send an anonymous on code to the server when you activate the anonymous call feature.	0	It configures the phone to send an 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[	String within 32 characters	Blank	It configures the anonymous call off code. The phone will send the code to deactivate the

1]			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 synchronization of the anonymous call status between the IP phone and the server.

> [1] X is the account ID.

Call Number Filter

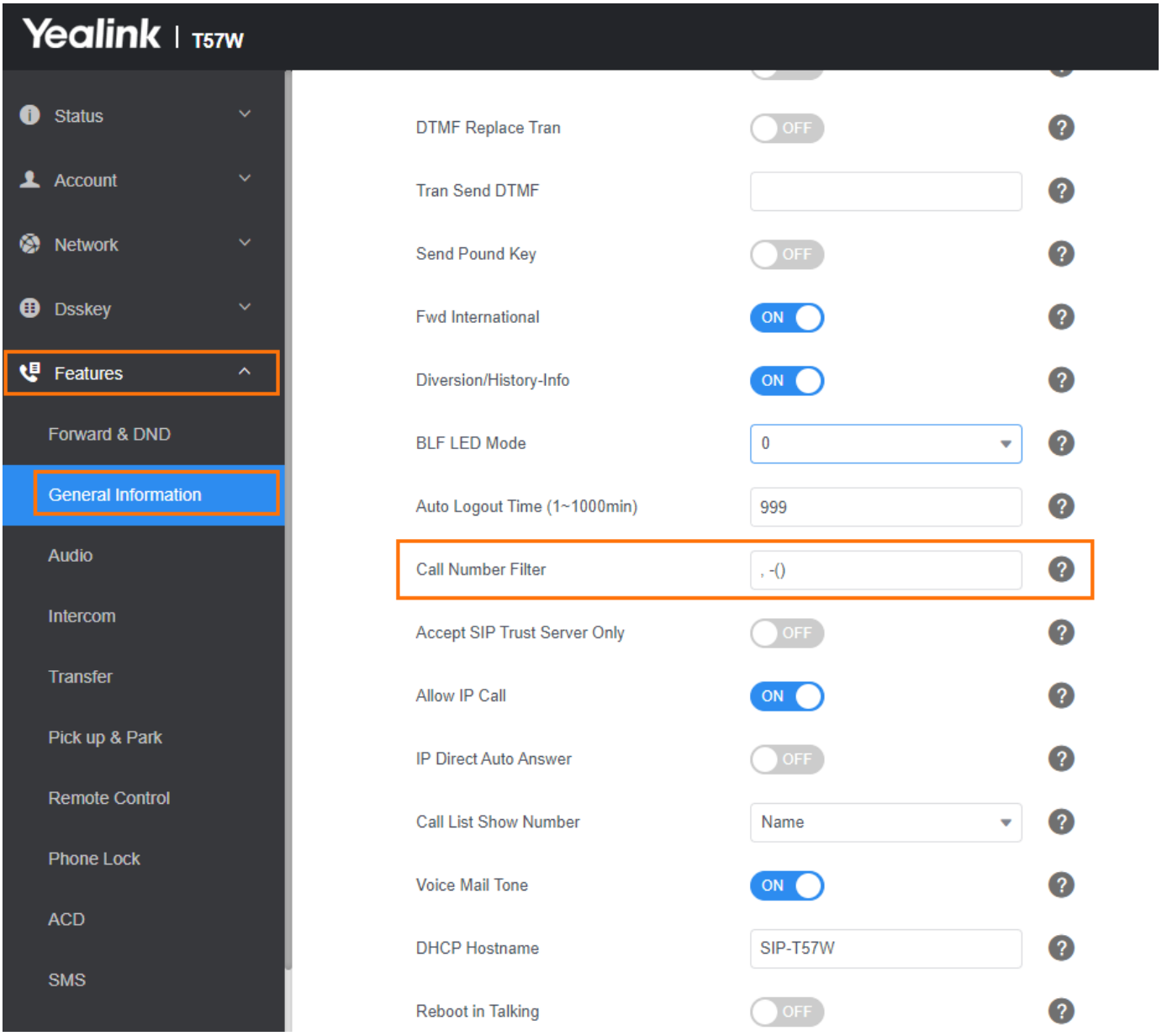
Introduction

Call number filter feature allows IP phone 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. If it is left blank, the phone will not automatically filter any characters when dialing.

IP Address Call

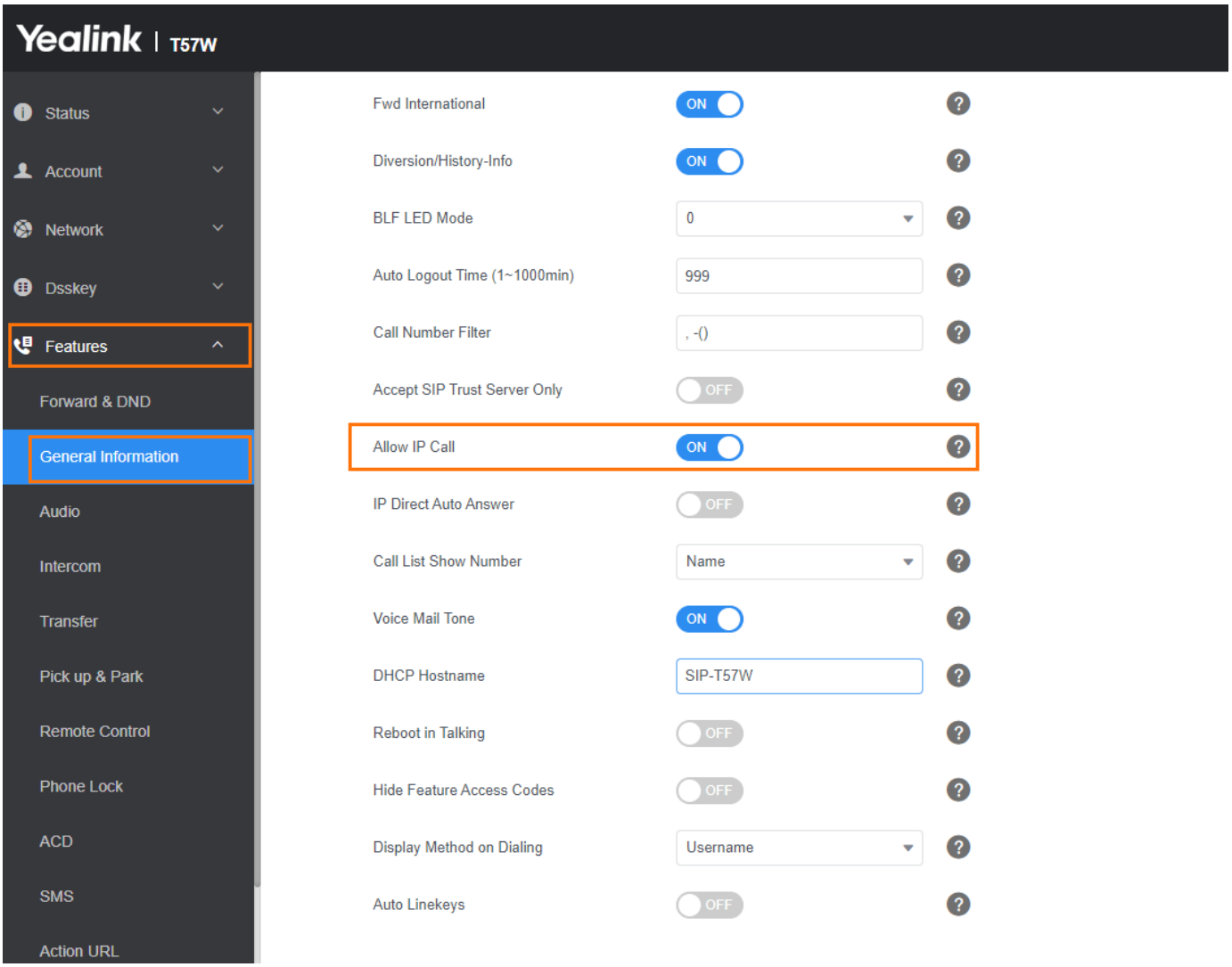
Introduction

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	Defa	Description

	Values	ult	
features.direct_ip_call_enable	**0**-Disabled **1**-Enabled	1	It enables or disables to allow an IP address call. If you want to receive an IP address call, make sure "sip.trust_ctrl" is set to 0 (Disabled).

Auto Answer

Introduction

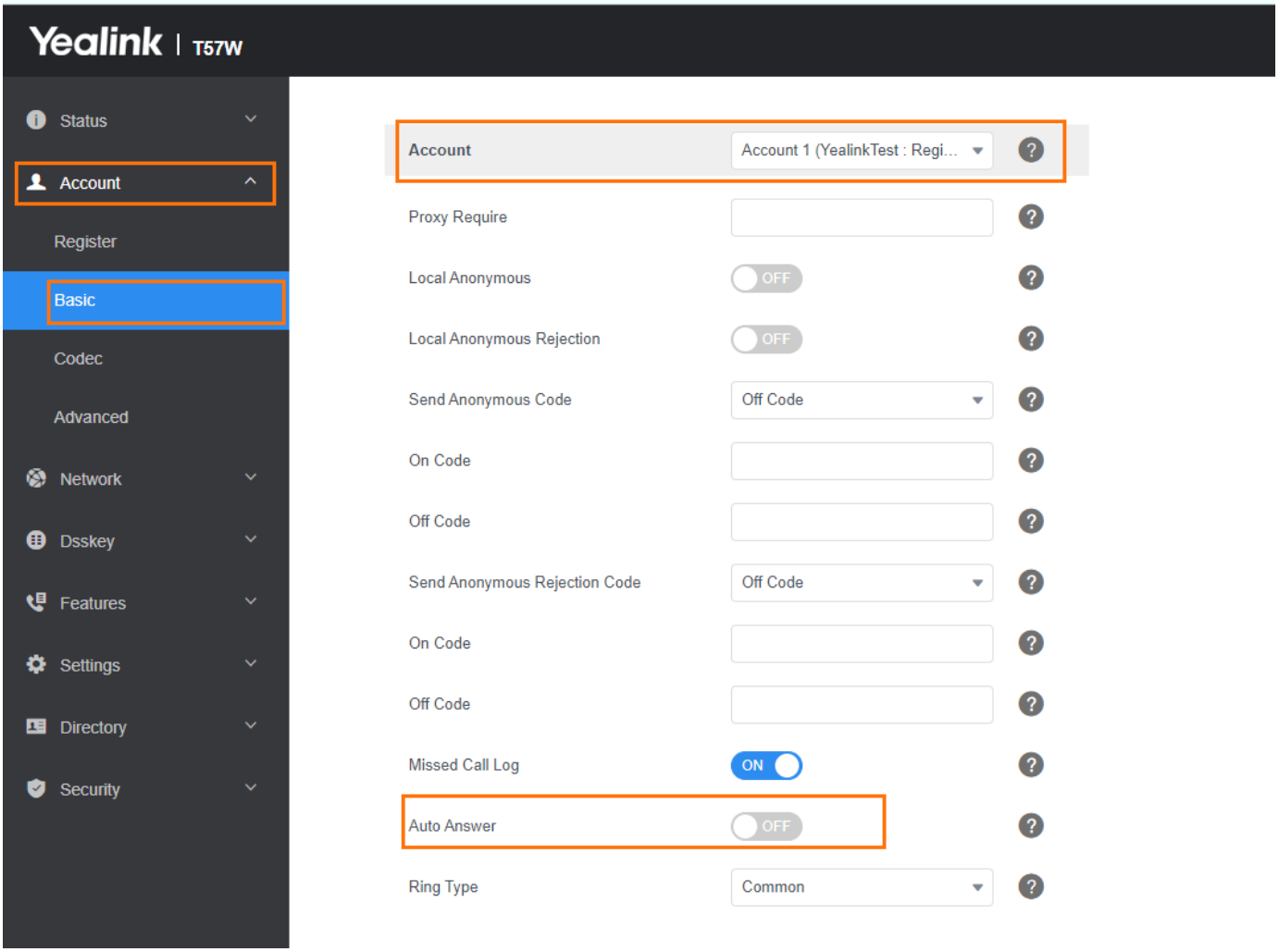
Auto answer allows the handset to automatically answer an incoming call by picking up from the charger cradle without having to press the off-hook key. The handset will not automatically answer the incoming call during a call, even if the auto-answer is enabled.

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 for a SIP call. The phone cannot automatically answer the incoming call during a call or while dialing, even if auto answer is enabled.
features.intercom.allow_string	Numbers. Multiple numbers separated by commas.	Blank	It is used to configure whether incoming calls from specified numbers are treated as intercom calls. Only support x.86.0.112 or later

> X is account ID.

Anonymous Call Rejection

Introduction

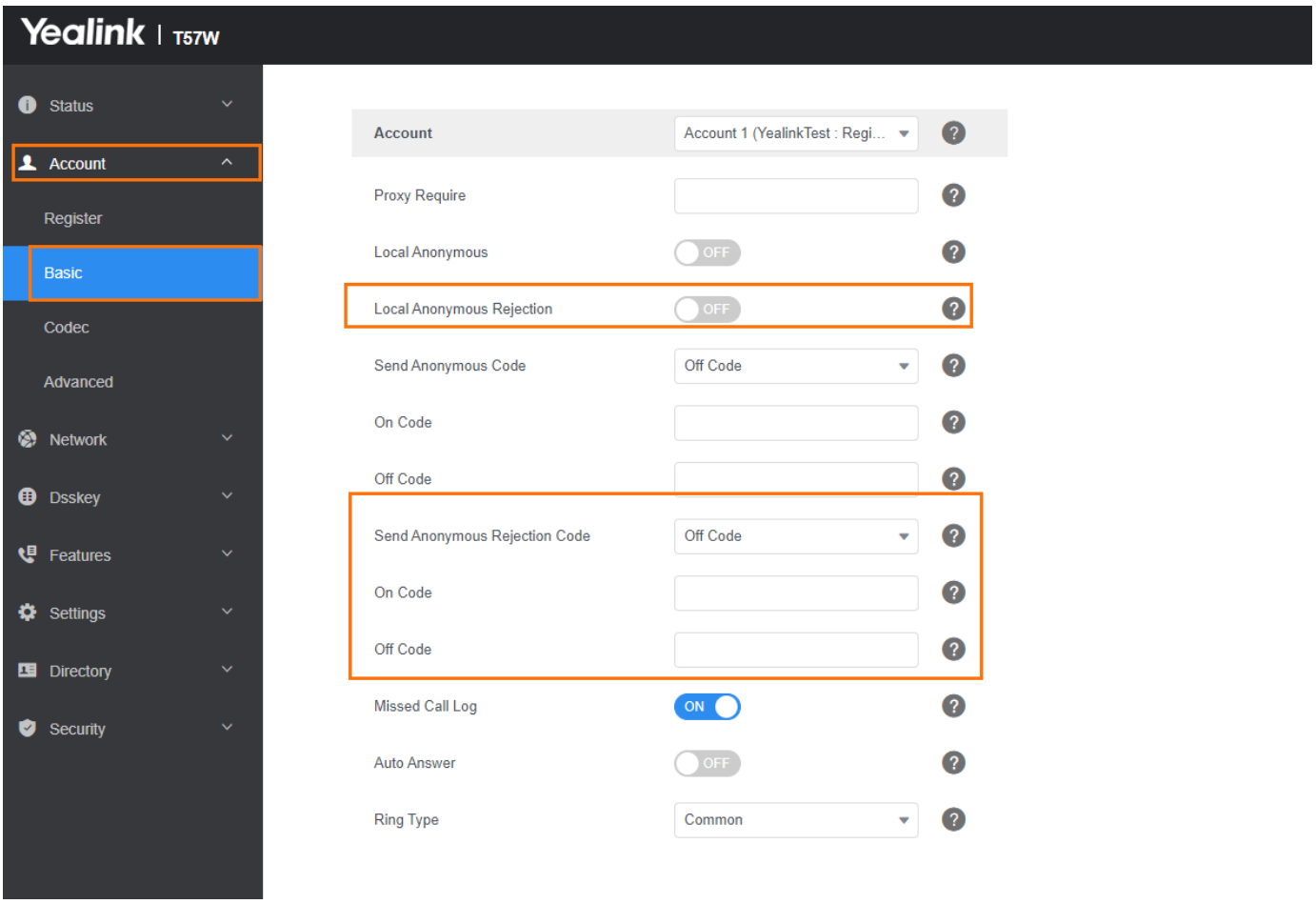
Anonymous call rejection allows the IP phone to automatically reject incoming calls from callers whose identity has been deliberately concealed.

Anonymous call rejection can be performed locally or on the server. When performing anonymous call rejection on local, 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 the 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 the anonymous call feature. The anonymous user’s phone screen presents “**Forbidden**”.	0	It triggers the anonymous call rejection feature to turn on or off.
account.X.anonymous_reject_oncode[1]	String within 32 characters	Blank	It configures the anonymous call rejection on the code. The phone will send the code to activate the anonymous call rejection feature on the 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 an anonymous rejection on code to the server when you activate the anonymous call rejection feature.	0	It configures the IP phone to send the anonymous call rejection on/off code to activate/deactivate the server-side anonymous call rejection feature for account X.
account.X.anonymous_reject_offco	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

de[1]			feature on server side when you deactivate it on the phone.

[1] X is the account ID.

Call Waiting

Introduction

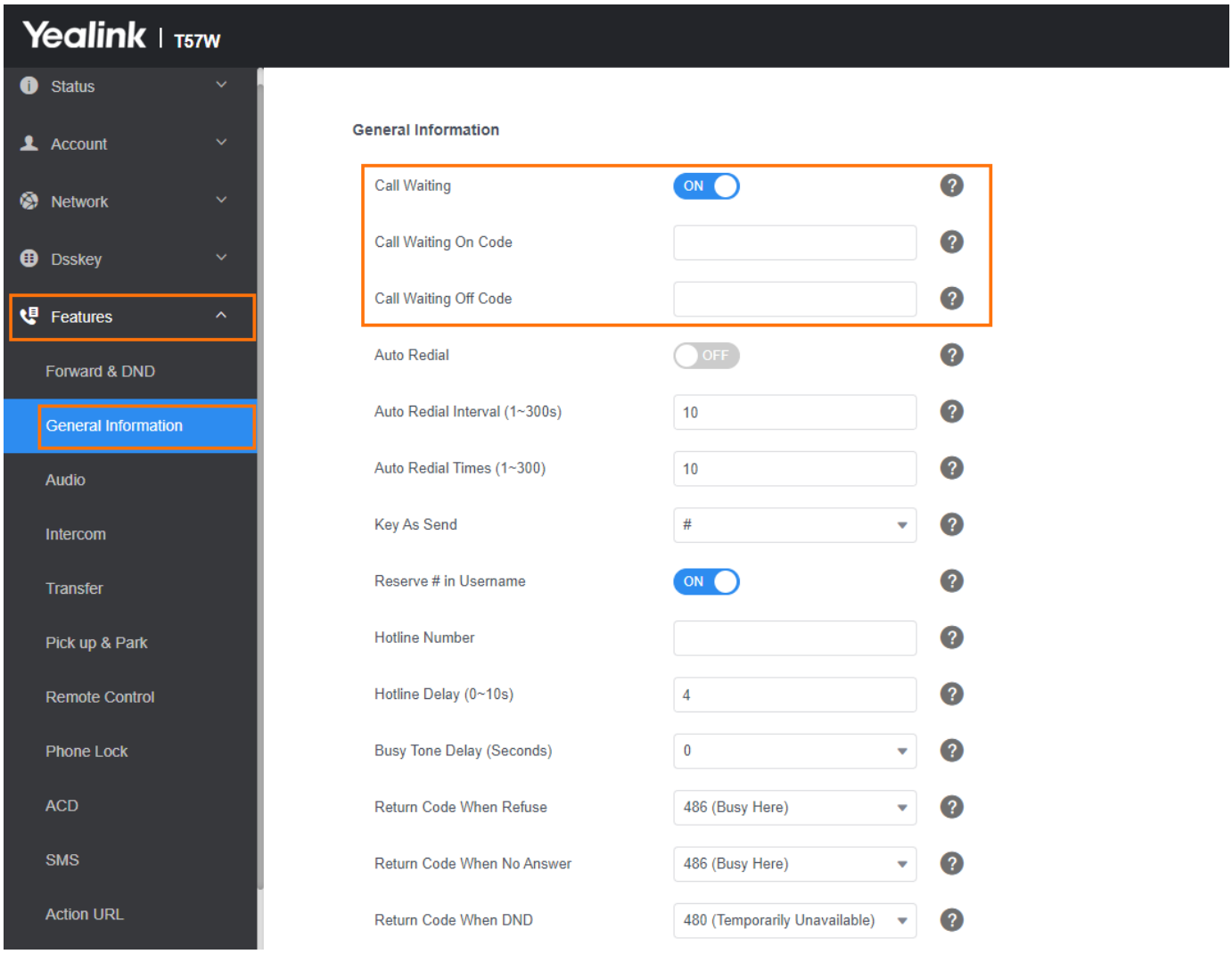
Call waiting enables you to receive another call when there is already an active call on your phone. If it is disabled, the new incoming call will be rejected automatically. You can enable the call waiting feature and set the phone to play a warning tone to avoid missing important calls during a call.

Yealink phones also support call waiting on code and off code to activate and deactivate the server-side call waiting feature. They may vary on different servers.

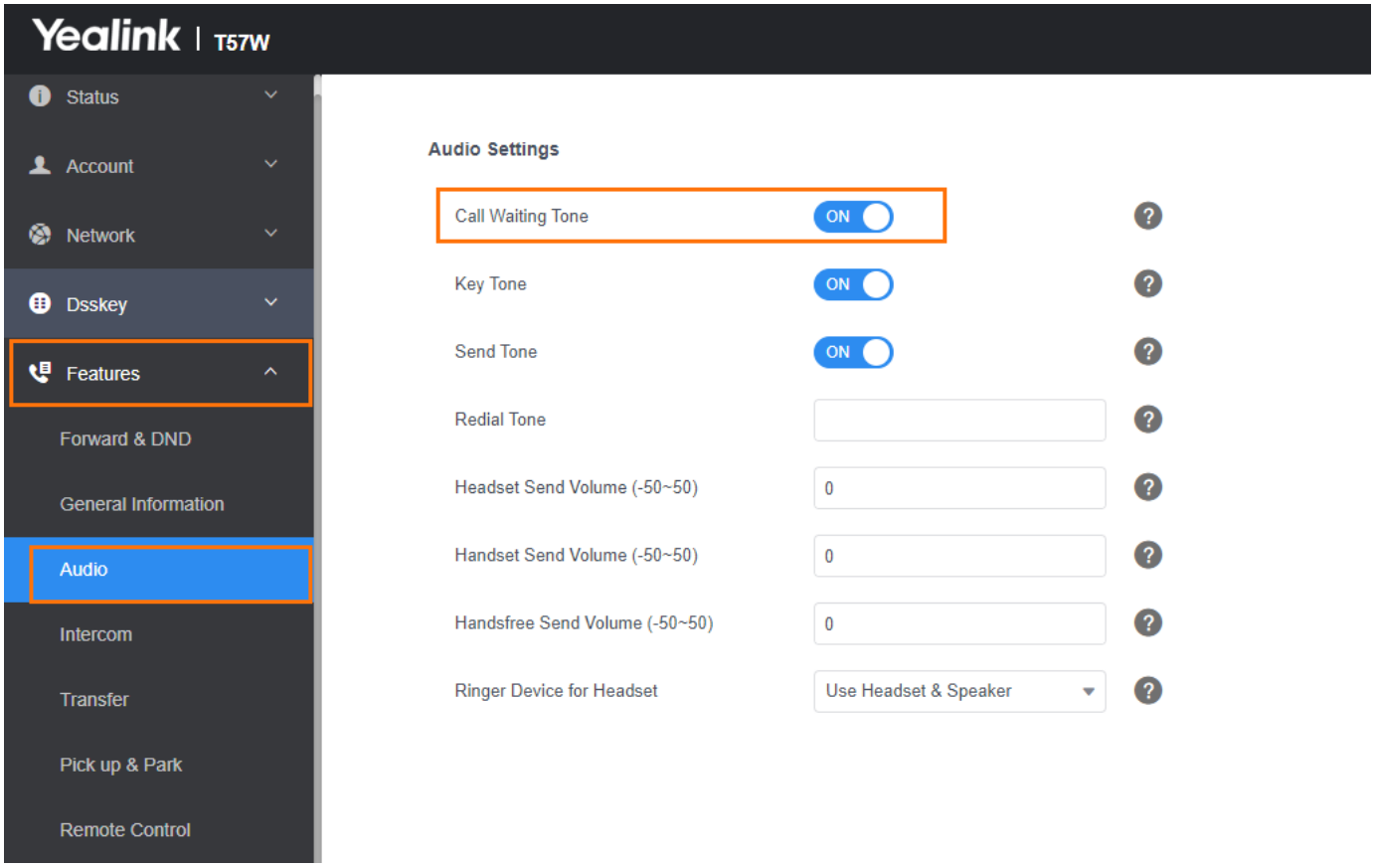
Call Waiting Configuration

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.

			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 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 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.

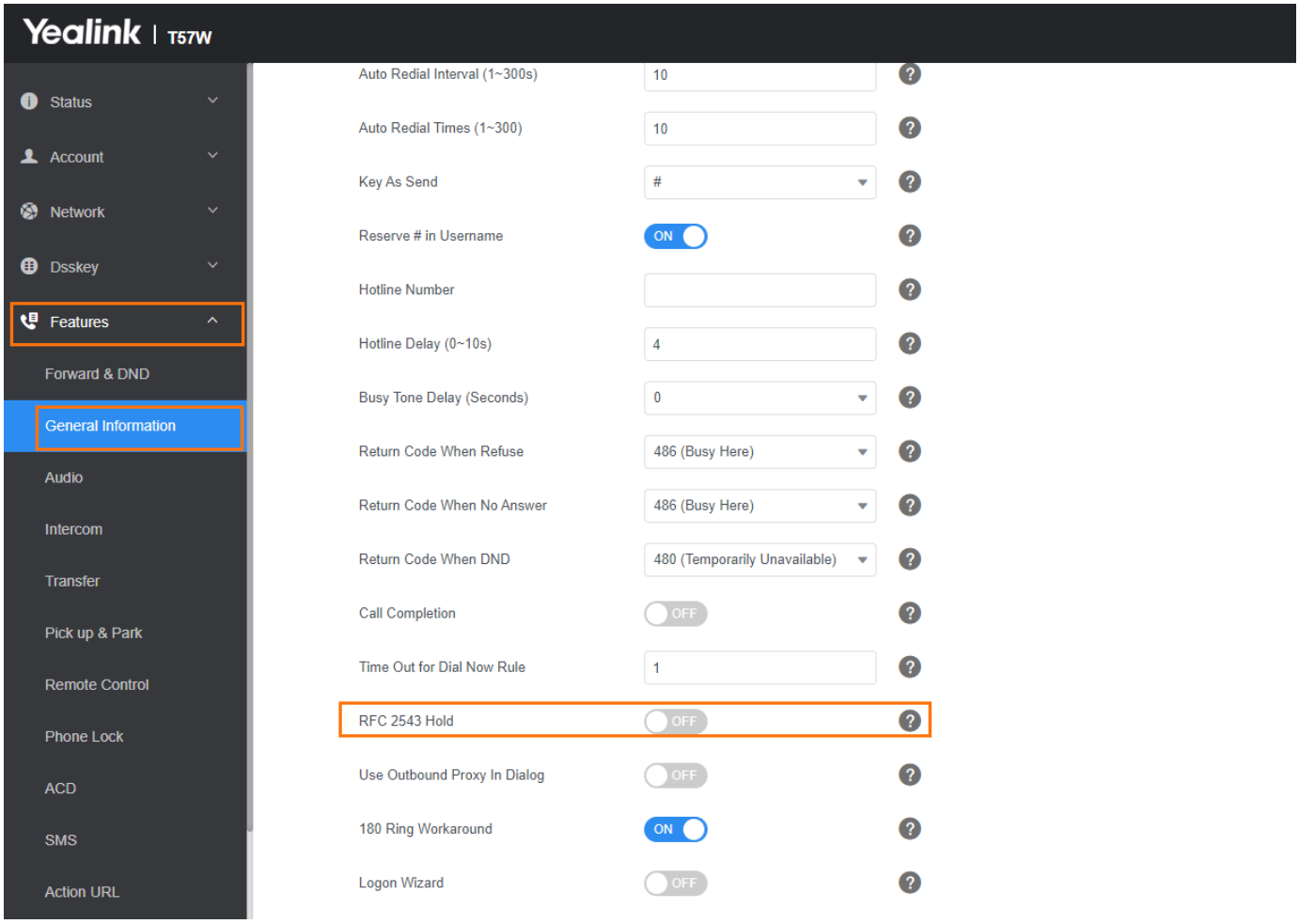
The phones support two call hold methods:

- 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 are 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	0	It enables or disables the phone to use RFC 2543 (c=0.0.0.0) outgoing hold signaling.

	call on hold.		
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. 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. It works only if "features.play_hold_tone.enable" is set to 1 (Enabled).
features.pla	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

y_hold_tone.interval			on hold for 30 seconds and repeat the call hold tone every 3 seconds. 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 hold 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. 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. 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. It works only if the Music on Hold feature is disabled and "features.play_held_tone.enable" is set to 1 (Enabled).

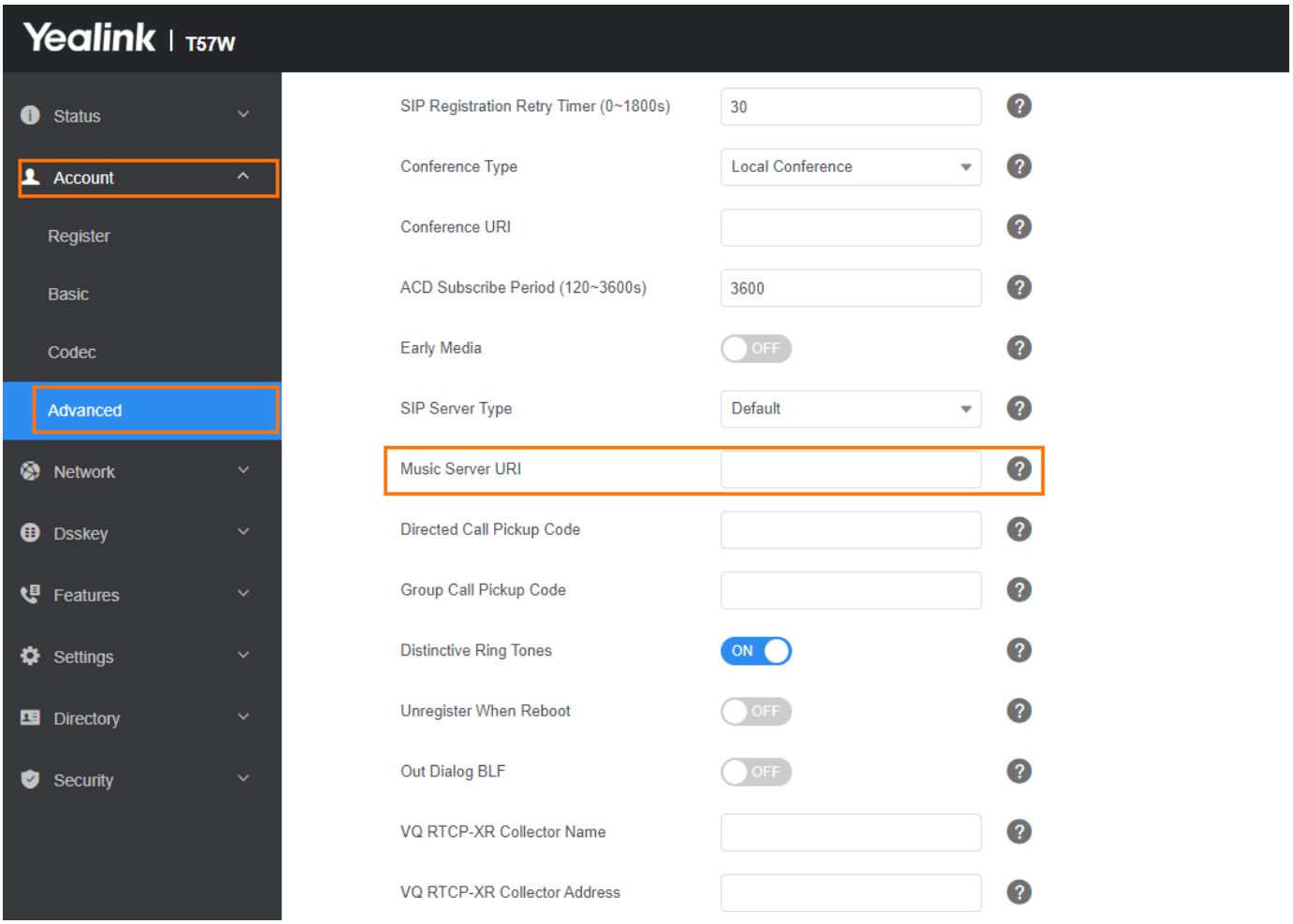
[1] X is the account ID.

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. The DNS query in this parameter only supports A query.
account.X.music_on_h	**0**-Calling the Music On Hold server before	0	It configures the way to process Music On Hold when placing an active call on hold.

old_type[1]	holding the call **1**-Calling the Music On Hold server after holding the call		

[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

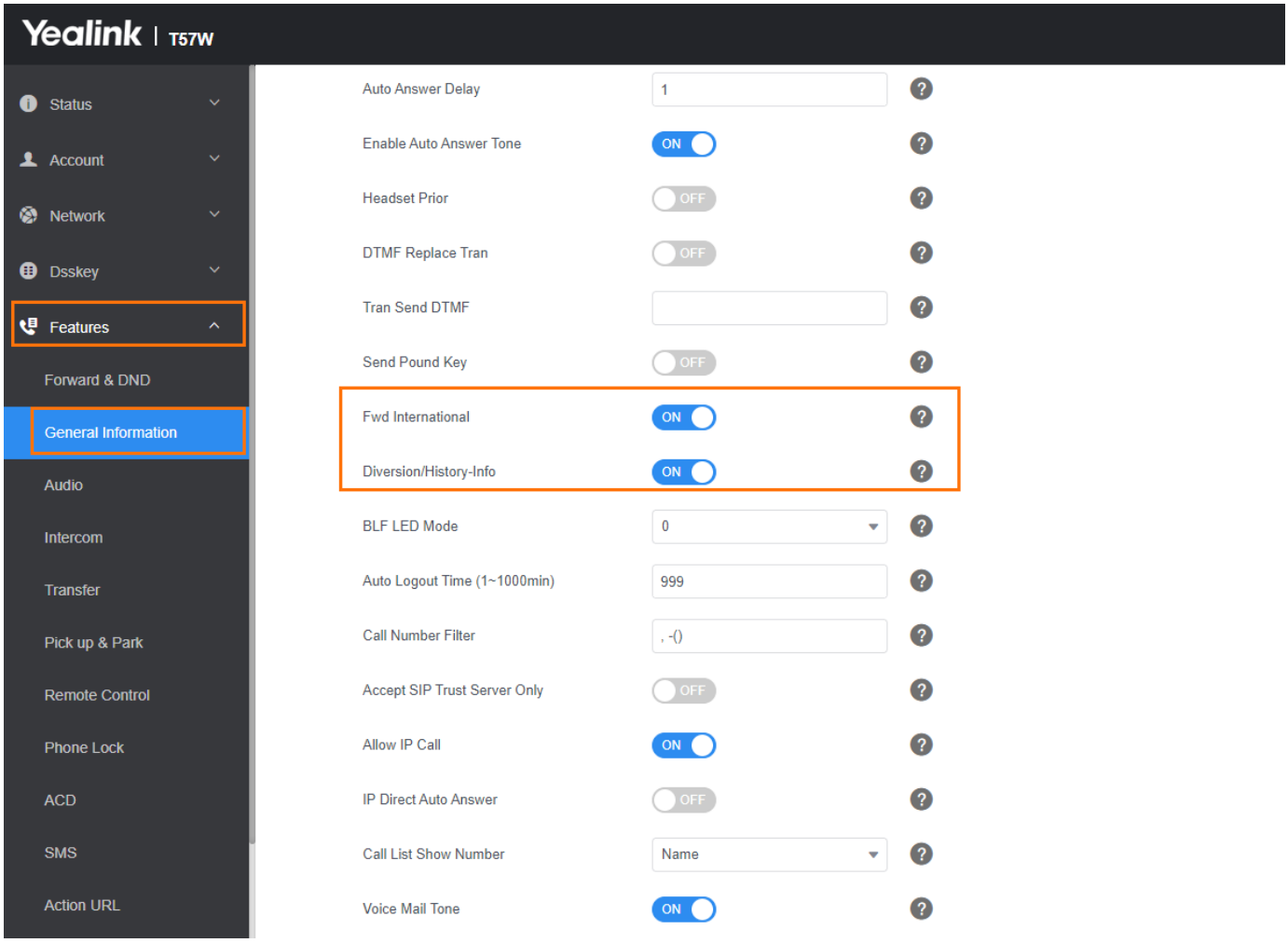
You can change the following call-forward settings:

- Enable or disable the call forward feature. If disabled, the users cannot configure call forwarding 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 a 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 a message when you forward an incoming call to another party.

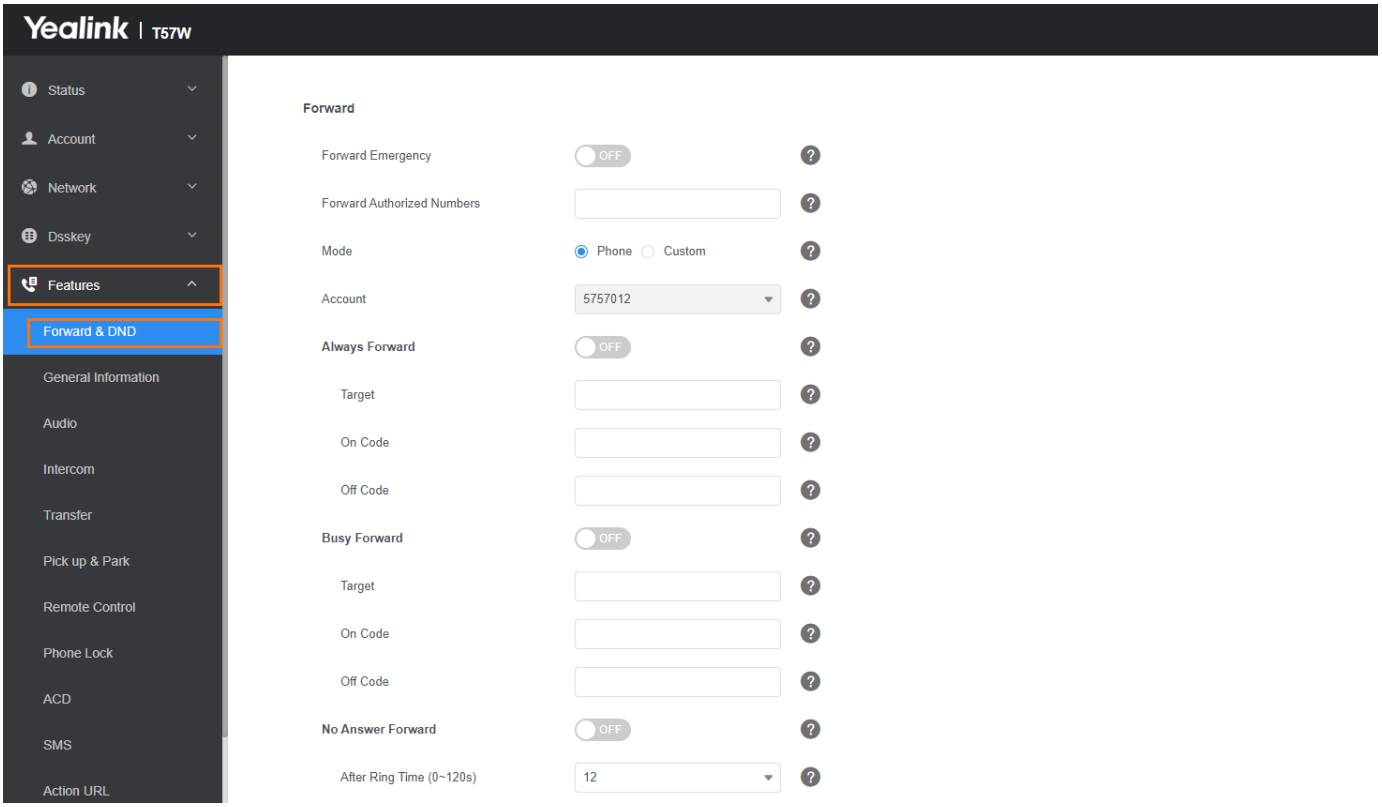
Call Forward Feature Configuration

Yealink phones support call forward on code and off code to activate and deactivate the 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 the always-forward feature to turn on or off. 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 for the always-forward. It works only if "features.fwd.allow" is set to 1 (Enabled) and "features.fwd_mode" is set to 1 (Custom).
account.	String within 32 characters	Blan	It configures the always forward on code to activate the server-side always forward

X.always_fwd.on_code[1]		k	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 the always forward feature on the phone. 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 the always-forward feature on the phone. 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 turn on or off.
account.X.busy_fwd.target	String within 32 characters	Blank	It configures the destination number of the busy forward. It works only if "features.fwd.allow" is set to 1 (Enabled) and "features.fwd_mode" is set to 1 (Custom).

t[1]			
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. 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. 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 the no-answer-forward feature to on or off. It works only if "features.fwd.allow" is set to 1 (Enabled) and "features.fwd_mode" is set to 1 (Custom).
account.X.ti	String within 32 characters	Blank	It configures the destination number for the no-answer forward. It works only if "features.fwd.allow" is

meout_fwd.target[1]			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. 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. 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 code to the server when you deactivate the no-answer-forward feature. 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. It works only if your 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 synchronization of the feature status between the IP phone and the server.
account.X.forward.feature_	**0**-Disabled **1**-Enabled, server-based call	Blan	It enables or disables the forward feature synchronization for

key_sync.enable[1]	forward is enabled. Server and local phone call forward are synchronized.	k	account X. 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.

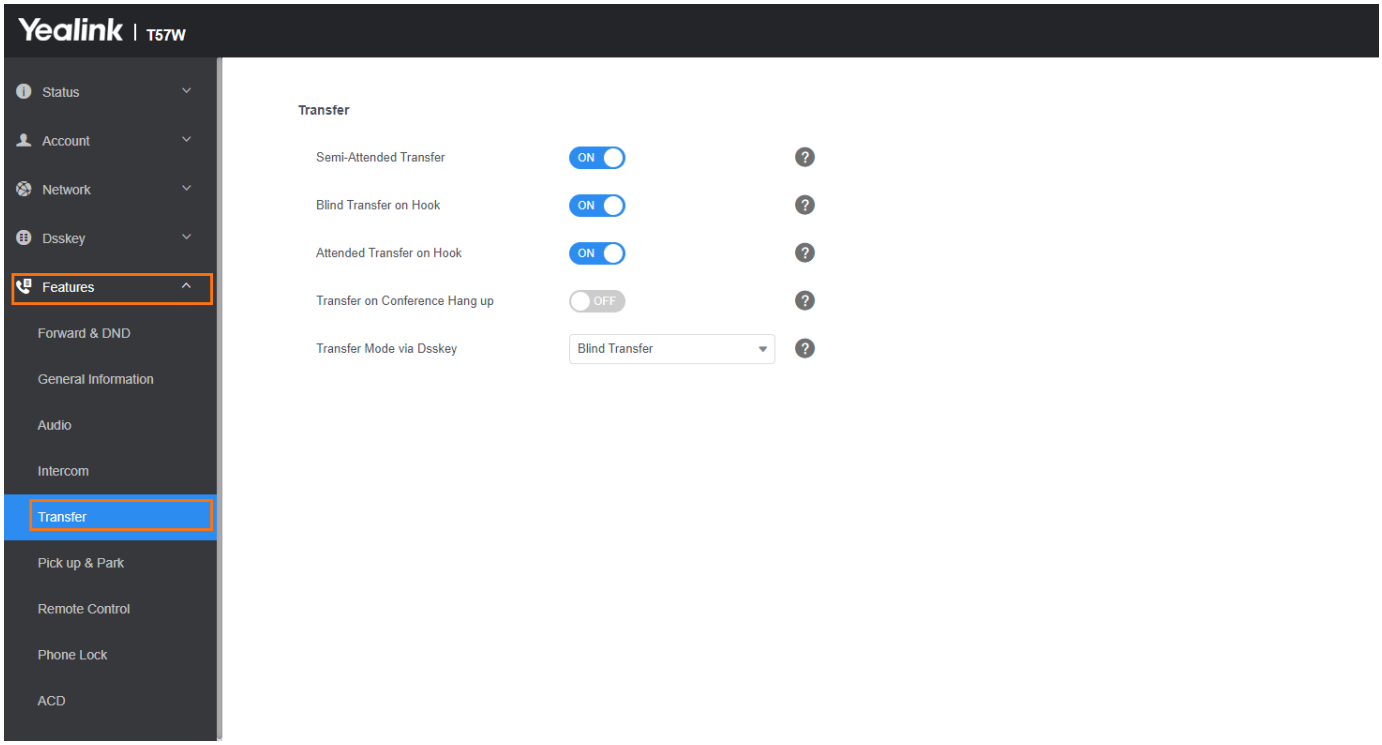
Yealink phones support call transfer using the REFER method specified in RFC 3515 and offer three types of transfer:

Type	Description
Blind Transfer	Transfer a call directly to another party without consulting. Blind transfer is implemented by a simple REFER method without Replaces in 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 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 consultation. Attended transfer is implemented by a REFER method with Replace 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

Parameter	Permitted Values	Default	Description
features.transfer.allow	**0**-Disabled, the 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,	1	It enables or disables the semi-attended transfer.

	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.		
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 an 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 the on-hook, besides pressing the TRAN key. 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. Semi-attended transfer means transferring a call after hearing the ringback tone; Attended transfer means transferring a call with prior

			consulting.

[1] X is the account ID.

Do Not Disturb (DND)

Introduction

DND feature enables the phone to reject all 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

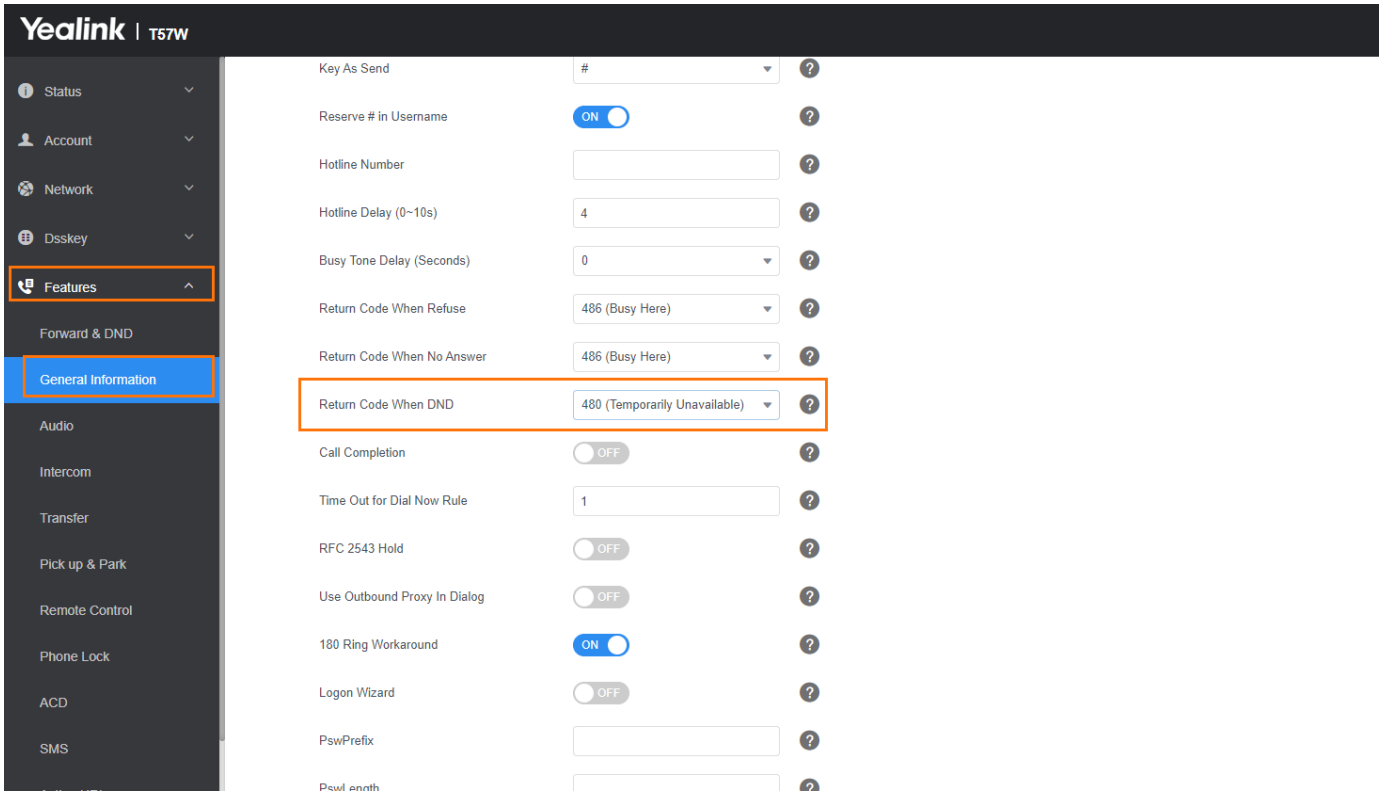
You can change the following DND settings:

- You can enable or disable the DND feature. If disabled, users do not have permission to configure DND on their phones.
- Define the return code and the reason for the SIP response message for a rejected incoming call when 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 the DND feature. **603**-Decline	480	It configures a return code and reason for SIP response messages when rejecting an incoming call by DND. A specific reason is displayed on the caller's phone screen. It works only if "features.dnd.allow" is set to 1 (Enabled).

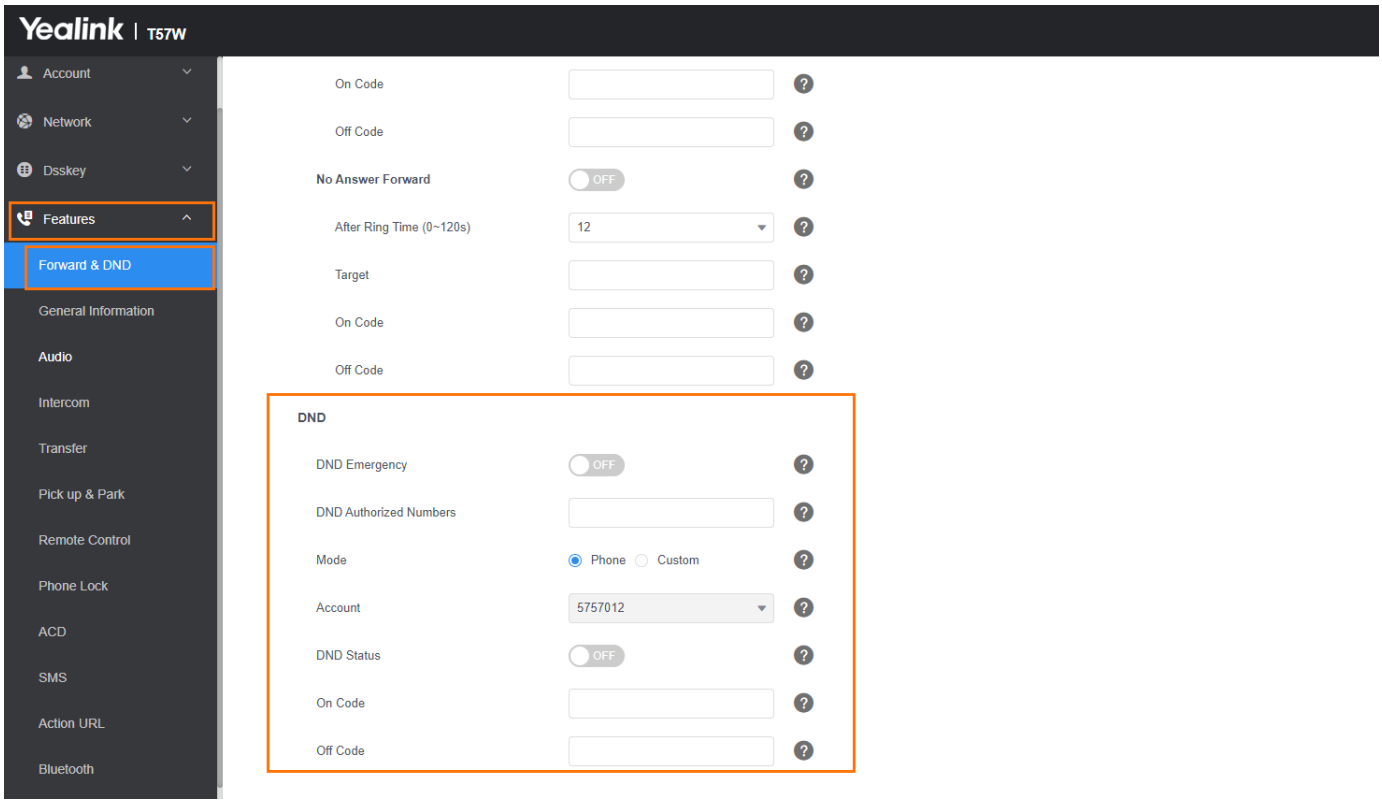
DND Feature Configuration

Yealink phones support DND on code and off code to activate and deactivate the server-side DND feature. 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 turn on or off. 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. 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. 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 change 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 synchronization of the feature status between the IP phone and the server.
account.X.dnd.feature_key_sync.enabl	**0**-Disabled **1**-Enabled, server-	Blank	It enables or disables the DND feature synchronization for account X.

e[1]	based DND is enabled. Server and local phone DND are synchronized.		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).

No Answer

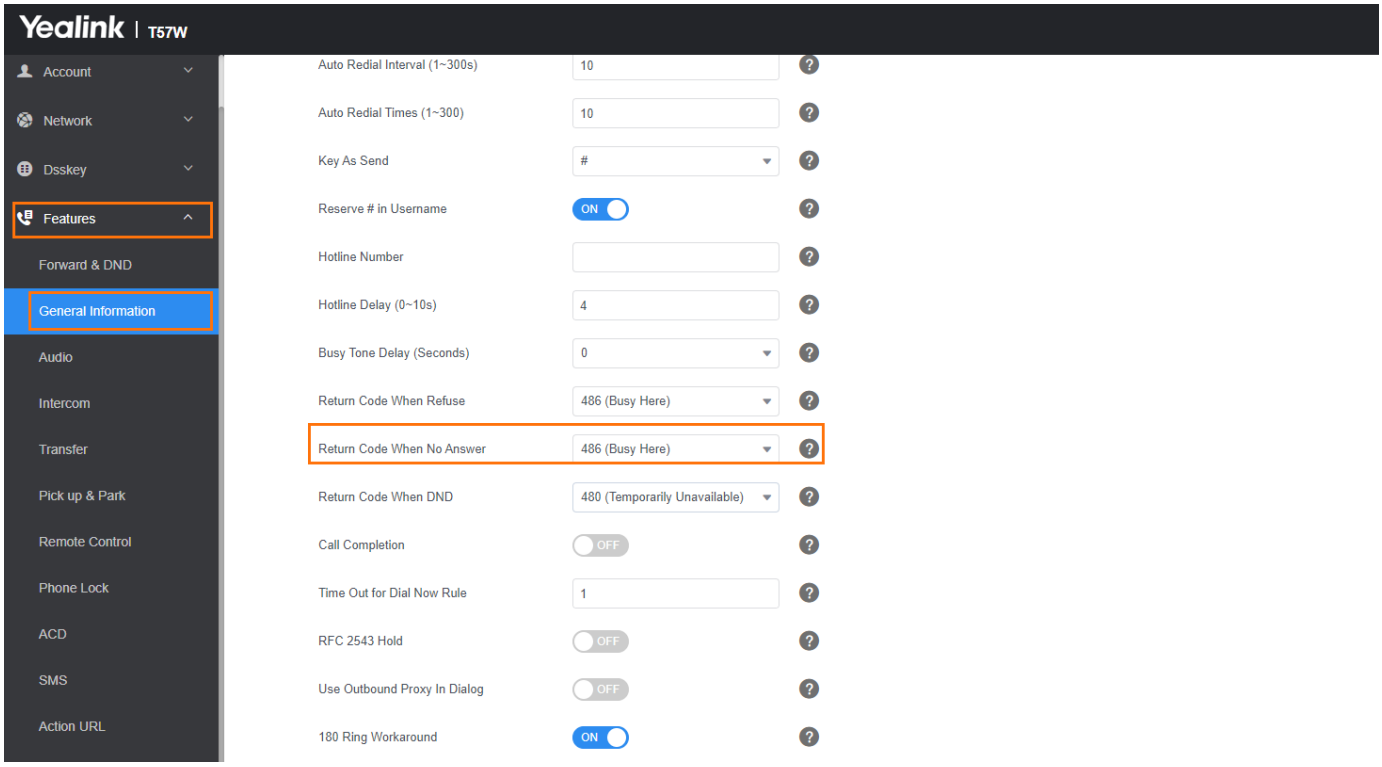
Introduction

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	486	It configures a return code and reason for response messages when the handset does not answer an incoming call.

Everywhere **603**-Decline		

Conference

Introduction

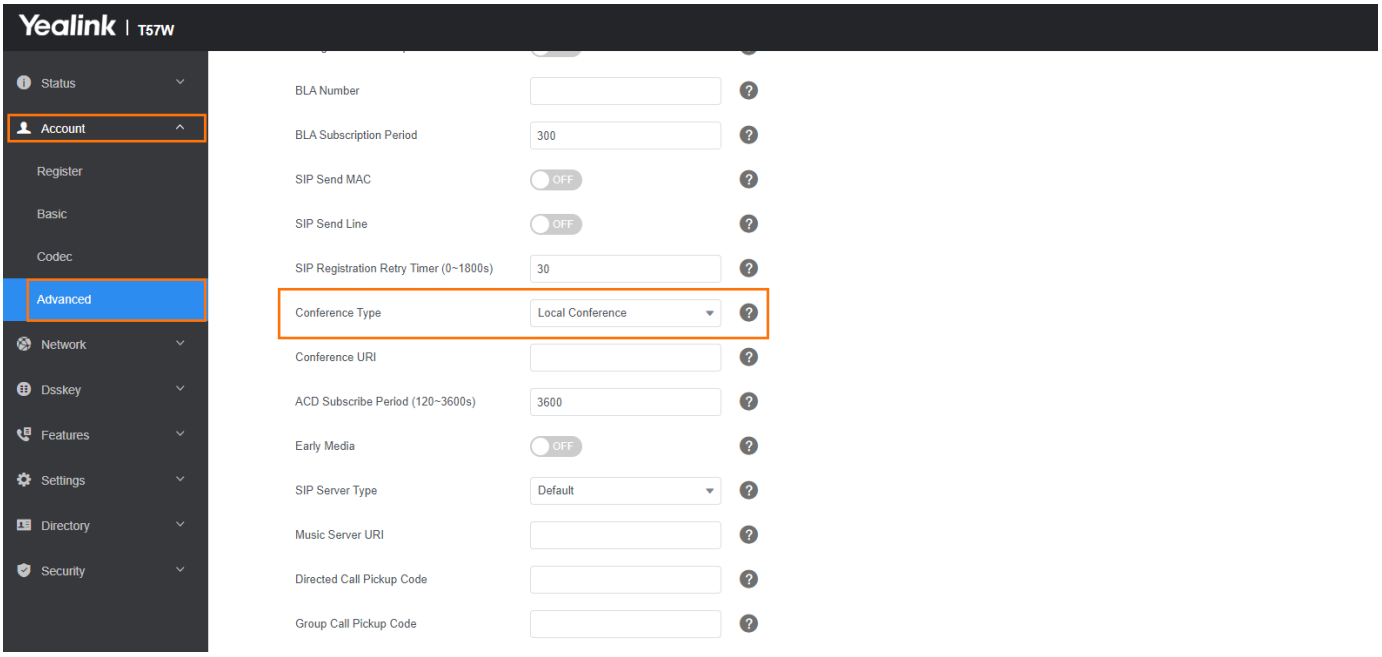
The Yealink phones support local conference and network conference.

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 Conferen	0	It configures the conference type for a specific account.

	ce		
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. It works only if your firmware version is x.86.0.112 or later.

[1] X is the account ID.

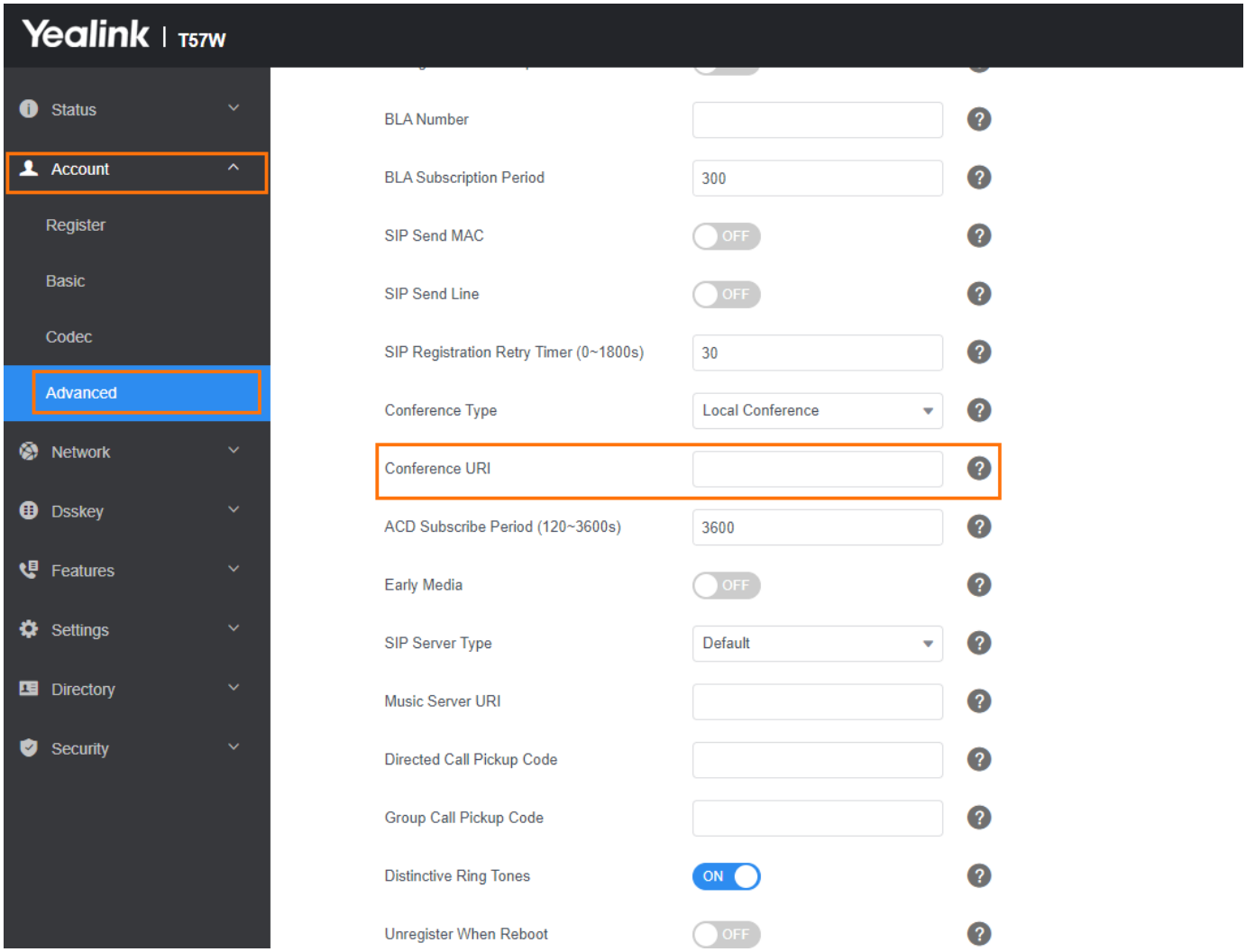
Network Conference Configuration

Network conference, also known as a centralized conference, provides you with the flexibility of calling multiple participants (more than three). The phones implement network conference using the REFER method specified in RFC 4579. This feature depends on the support from a SIP server.

For a network conference, 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. 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. 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. It is the default channel.
- **1 to 30**: Broadcasts are sent to channels 1 to 30. We recommend that you specify these channels when broadcasting with Yealink IP phones.

The phones can only send and receive broadcasts to/from the listened channels. Other channels' broadcasts will be ignored automatically by the IP phone.

Before You Begin

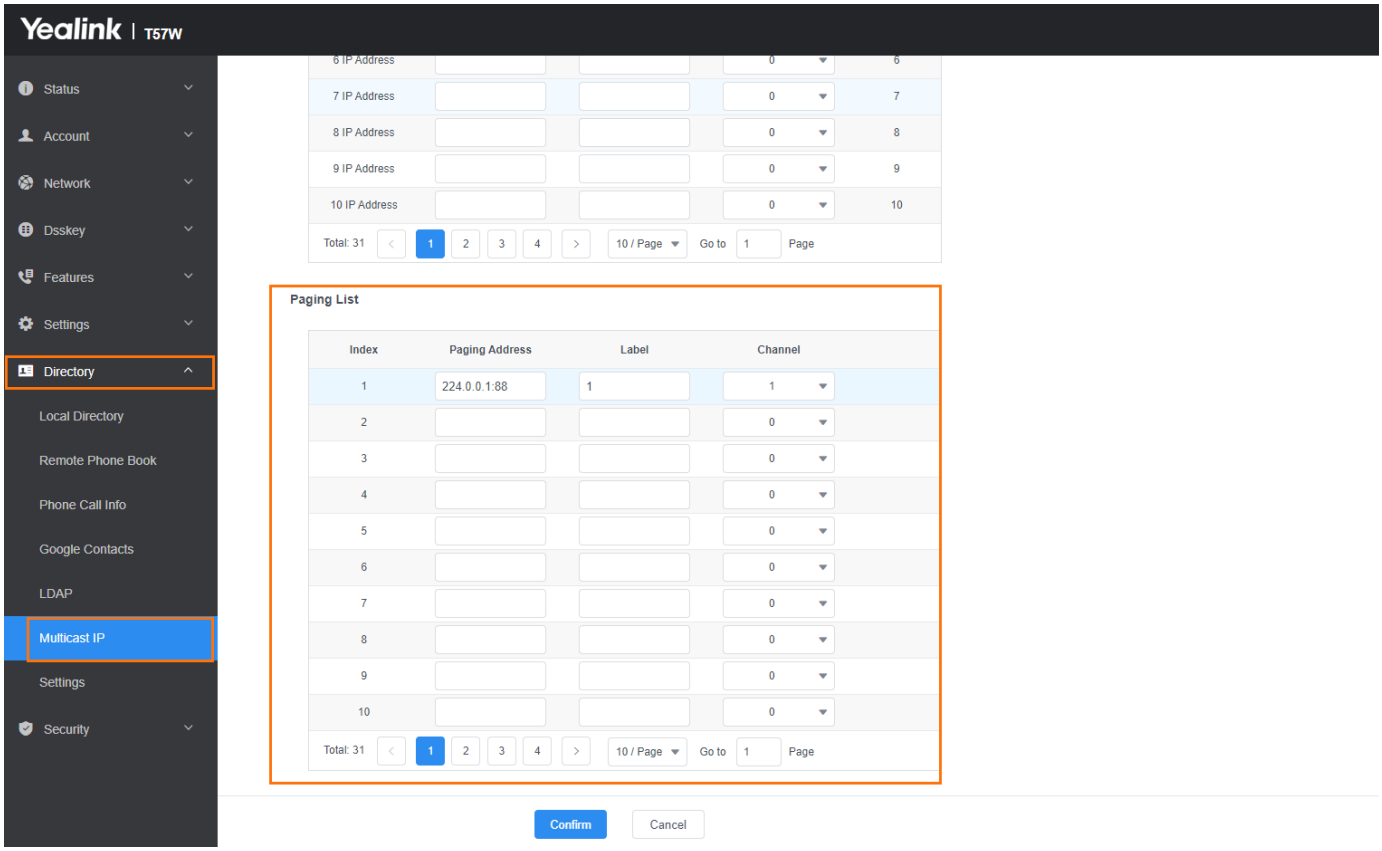
This feature is applicable to all desk IP Phones.

Multicast Paging Group Configuration

Yealink phones support up to 31 groups for paging. You can assign 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	Defau lt	Description
features.send_paging.enable	**0**-Disable **1**-Enable	1	Configure whether to enable Paging and Paging List features. 1. It only works if your phone is T3x/T4xU/T5xW and the version is x.86.0.100 or later. 2. If set to 0, it will synchronize the hiding of functionality entrances on both the LCD interface and the web interface.
multicast.paging_ad	IP address: port	Blank	It configures the IP address and port

dress.X.ip_address[1]	(224.0.0.1-239.255.255.255 port: 0-65535)		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 listening 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	0	It configures the channel of the multicast paging group in the paging list.

	receive the RTP stream.		

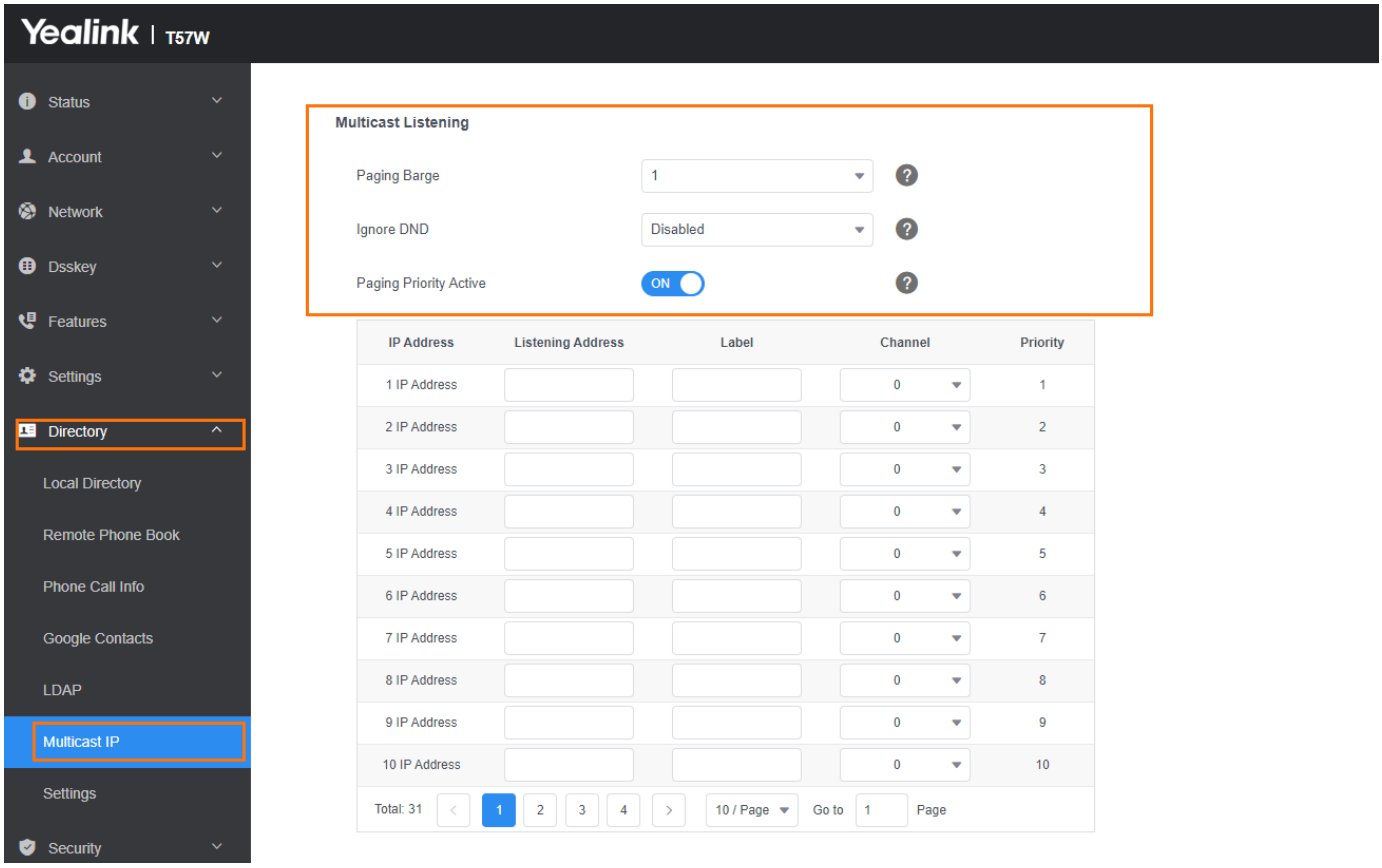
> [1]X ranges from 1 to 31.

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 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** > **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	Defaul t	Description

features.accept_paging.enable	**0**-Disabled **1**-Enabled	1	It configures whether to enable the Multicast Listening feature. 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 versions, from the phones listening to 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 channel 1 to 25, respectively, from Yealink phones. **26 to 30**-the phone can receive the RTP stream of the pre-configured	0	It configures the channel that the phone listens to.

	multicast address on channels 26 to 30, respectively, from Yealink phones.		

> [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 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 that the incoming paging calls with a 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 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

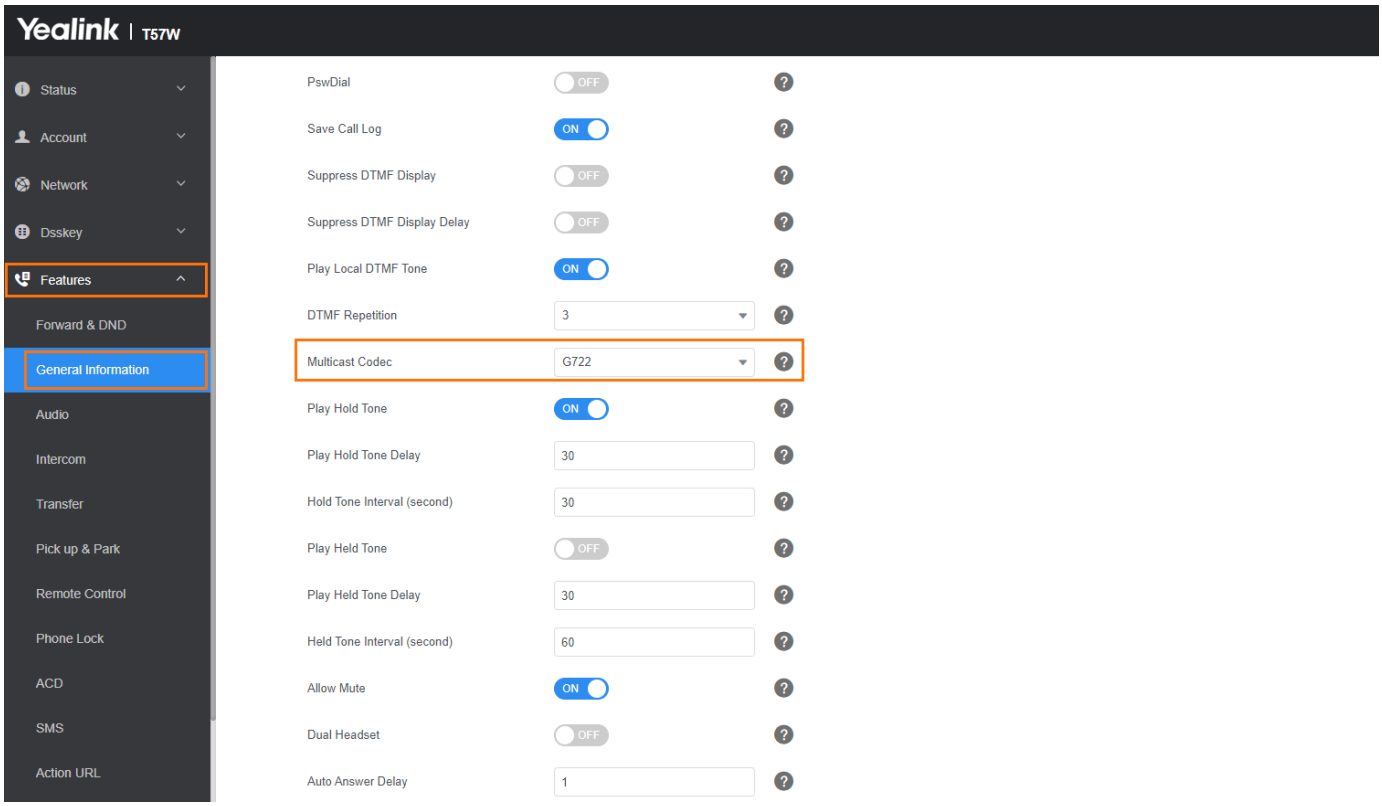
If you do not want to miss some urgent paging calls when DND is activated. You can use the Ignore DND feature to define the lowest priority of the paging group from which the phone can receive an urgent paging call when DND is activated. You can specify a priority so that the incoming paging calls with a 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	Defaul t	Description
multicast.cod ec	PCMU, PCMA, G729, G722	G722	It configures the codec for multicast paging.
multicast.rece ive_priority.e	**0**-Disabled, the phone will ignore the incoming	1	**Directory** > **Multicast IP** > **Paging Priority Active**.

nable	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.		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	**Directory** > **Multicast IP** > **Paging Barge**. 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	0	**Directory** > **Multicast IP** > **Ignore DND**. 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, 31 is the lowest priority.

	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.		
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 in 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.	0	It enables or disables the phone to always use the speaker as the audio device when receiving the multicast paging calls.

	1-Enabled		
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. It works only if your firmware version is x.86.0.138 or later.
multicast.auto_end.popup_timeout	**0-3600:** In second (s) 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. It works only if your firmware version is x.86.0.138 or later.

> [1]X ranges from 1 to 31.

Auto End Multicast Paging

You can set the phone to automatically end paging

Auto Provisioning

```
multicast.paging.timeout
multicast.auto_end.popup_timeout
```

Parameter	Permitted Values	Default	Description
multicast.paging.timeout	0-1440	0	It configures the timeout period of the multicast paging function. When the timeout period is reached, a pop-up window will appear to remind the user whether to turn off multicast paging.
multicast.auto_end.popup_timeout	0-3600	60	It configures the duration of the multicast paging timeout pop-up window. If the time

			exceeds this limit and the user does not choose to continue the multicast paging, the multicast paging will be directly closed.

Call Mute

Introduction

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 calls.

> Muting the microphone on the pre-dialing/dialing/calling/ringing screen is not available on T23P/T23G/T21 E2 phones when the keep mute feature is disabled.

Microphone Mute Configuration

The following table lists the parameter you can use to configure the microphone mute feature.

Configuration parameter

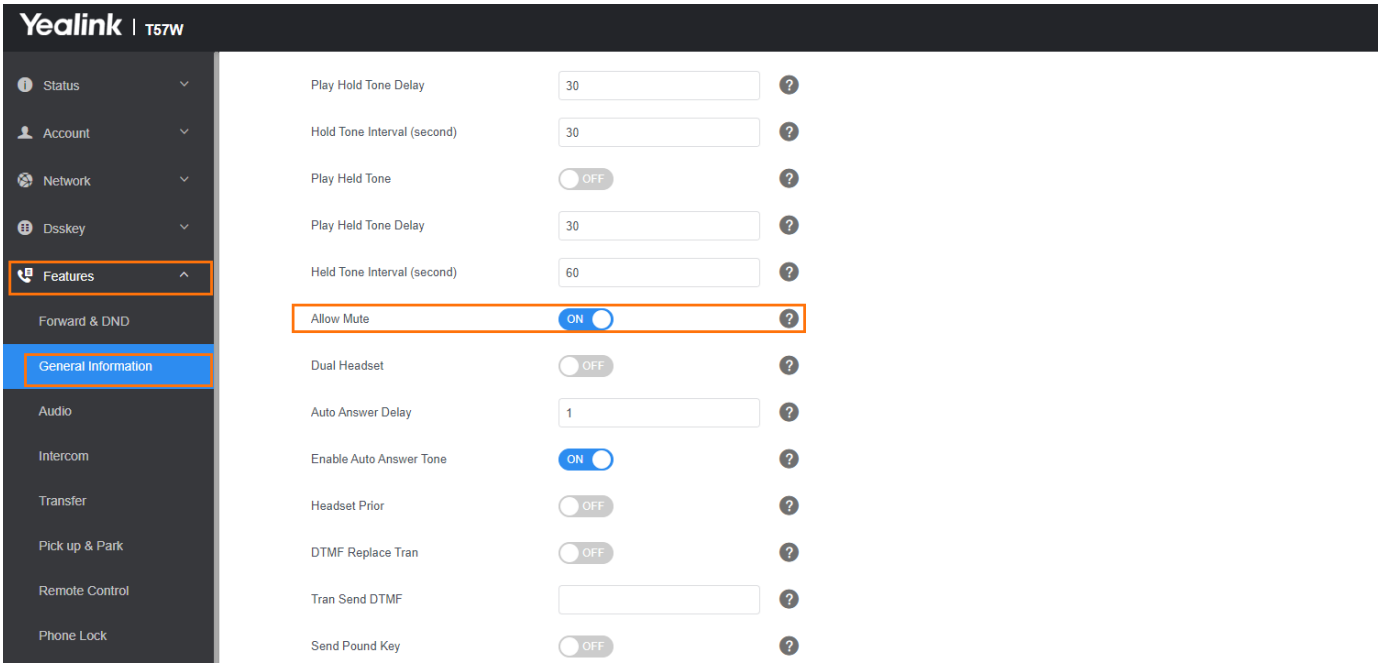
features.allow_mute

Parameter	Permitted Values	Defau lt	Description
features.allow_mute	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. (Mute the microphone on the calling screen is only applicable to the T57W/T54W/T53W/T53/T53C/T48U/T48S/T48G/T46U/T46S/T46G/T33P/	1	It enables or disables the allow mute feature for the IP phone. For T23P/T23G/T21 E2 phones, you are allowed to activate the mute feature on the pre-dialing/dialing/calling/ringing screen only if "features.keep_mute.enable" is set to 1 (Enabled).

	T33G/T29G/T58W/T58A/ VP59/T56A/T58V/T7X/ T8X phones).		

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 the 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 idle/pre-dialing/dialing/ringing/ calling/talking state.

> For T23P/T23G/T21 E2 phones, the Cancel key (X key) can be used to cancel actions, reject incoming calls, mute/unmute calls, or activate the mute feature. If the keep mute feature is enabled, the Cancel key can only be used as a mute key.

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	Permitted Values	Default	Description
features.keep_mute.enable	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 (for other phones) 1 (for CP920/ CP925/ CP935W/ CP960/ CP965)	It configures the keep mute feature. It works only if "features.allow_mute" is set to 1 (Enabled).
features.keep_mute.mode	0: Represents exiting continuous mute mode. 1: Represents entering 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 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 unmutes the call. Pressing the Mute key again will return to mute mode. After the call ends, it returns to continuous mute mode.	0	It configures the keep mute mode. It works only if your Version is V86 or later

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 unmute state. In addition, you can set a periodic reminder that plays the audible tone periodically when the phone is in the mute state. The time interval must not be less than 3 seconds.

It is only applicable to CP920/CP925/CP935W/CP960/CP965 phones.

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	Permitted Values	Default	Description
features.play_mute_tone.enable	0-Disabled 1-Enabled	0	It enables or disables the phone to play an audible tone when the mute status is changed.
features.play_mute_tone.interval	Integer from 3 to 3600	5	It configures the time interval (in seconds) for playing an audible tone when the phone is in the mute state during the call.

Enable and configure STIR & SHAKEN caller ID validation

Introduction

Set up STIR/SHAKEN standard protocol values for caller ID verification on a registered line.

When STIR/SHAKEN is enabled, the phone authenticates incoming calls using SIP headers to help prevent fraudulent activities like caller ID spoofing. The call server and service provider provide the caller ID verification values. If an incoming call fails verification, the phone will show an icon on the caller ID screen indicating a suspicious call. The user can then decide whether to accept or reject the call.

Auto Provisioning

account.x.verstat.enable
verstat.parameter.name
verstat.passed.criteria
verstat.failed.criteria

Parameter	Optional Value	Default	Description
account.X.verstat.enable	**0**: Disabled **1**: Enabled	0	It configures whether to enable the security level verification feature.
verstat.parameter.name	String within 511 characters	verstat	It configures the name of verstat. It works only if "account.x.verstat.enable" is set to 1 (Enabled).
verstat.passed.criteria	String within 511 characters	Blank	It configures the value of the verstat field to determine whether the incoming call number is safe. It works only if "account.x.verstat.enable" is set to 1 (Enabled).
verstat.failed.criteria	String within 511	Blank	It configures the value of the verstat field to determine whether the incoming call number is not verified.

	characters		It works only if "account.x.verstat.enable" is set to 1 (Enabled).

[1] X is the account ID.

Hide Dialpad

Introduction

You can hide the dialpad and input field during video calls.

Only applicable to T58W/T88W/T88T88V Pro.

Auto Provisioning

features.hide_dialpad_in_videocall.enable

Parameter	Permitted Values	Default	Description
features.hide_dialpad_in_videocall.enable	**0**-Not hide **1**-Hide	0	It configures whether pressing the hardware key during a video call hides the on-screen dial pad display.

User and Administrator Identification

Introduction

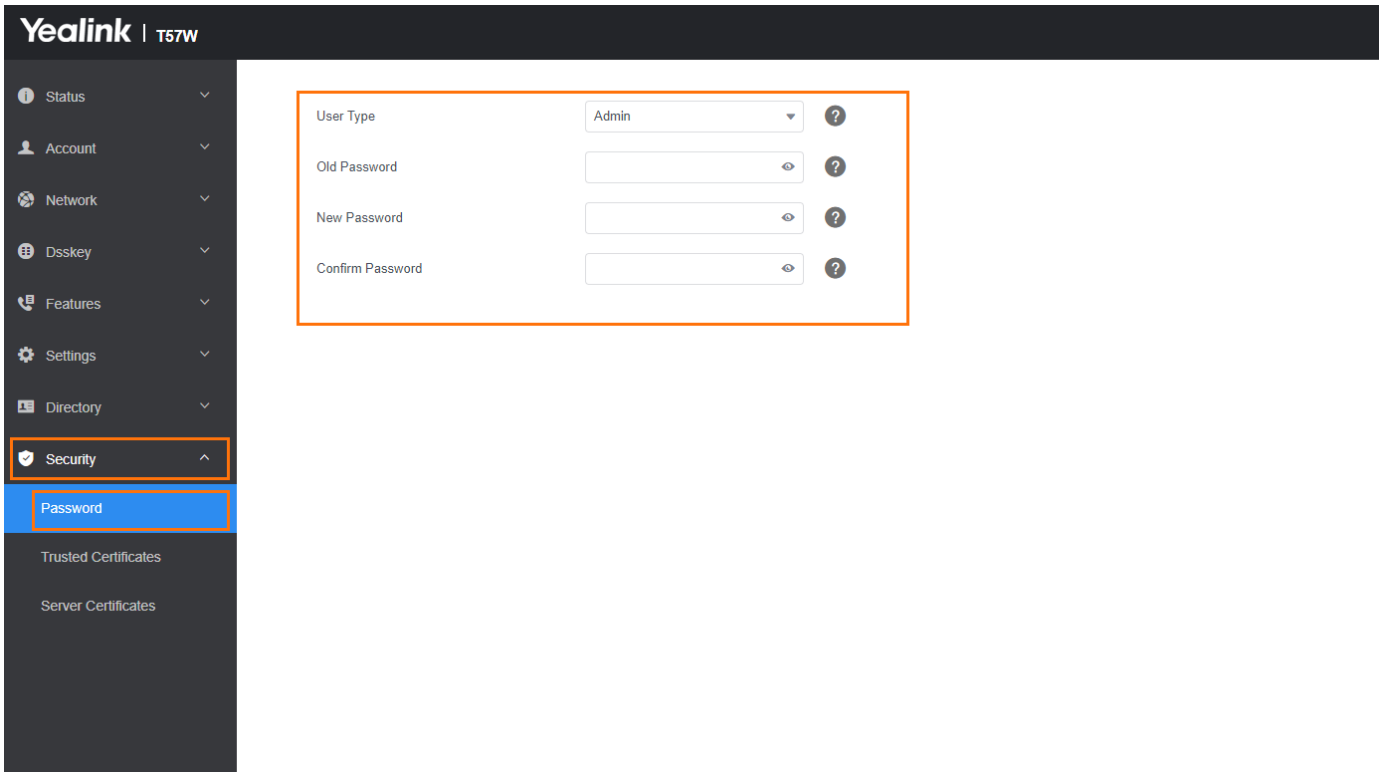
By default, some menu options are protected by privilege levels: user and administrator, each with its own password. You can also customize the access permission for the configurations on the web user interface and phone/handset user interface. Yealink phones support the access levels of admin, var,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

When logging into the web user interface or access 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. 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 <username>:<new password>. **Example**: static.security.user_password = user:123 means setting the password of user to 123. static.security.user_password = admin:456 means setting the password ofthe administrator to 456. static.security.user_password = var:789

			means setting the password of var to 789. 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. And 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 default password when logging in via the web interface; the LCD interface can be	0	Used to configure whether administrators and users can utilize default passwords.

	used without changing the password. **3**-Semi-force mode, requires users to change default password when logging in via the web interface; the LCD interface enforces password change only upon entering advanced settings.		

> [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.defaul	**0**-user	0	It configures the default access level to access

t_access_level[1]	**1**-var **2**-admin		the handset user interface. 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

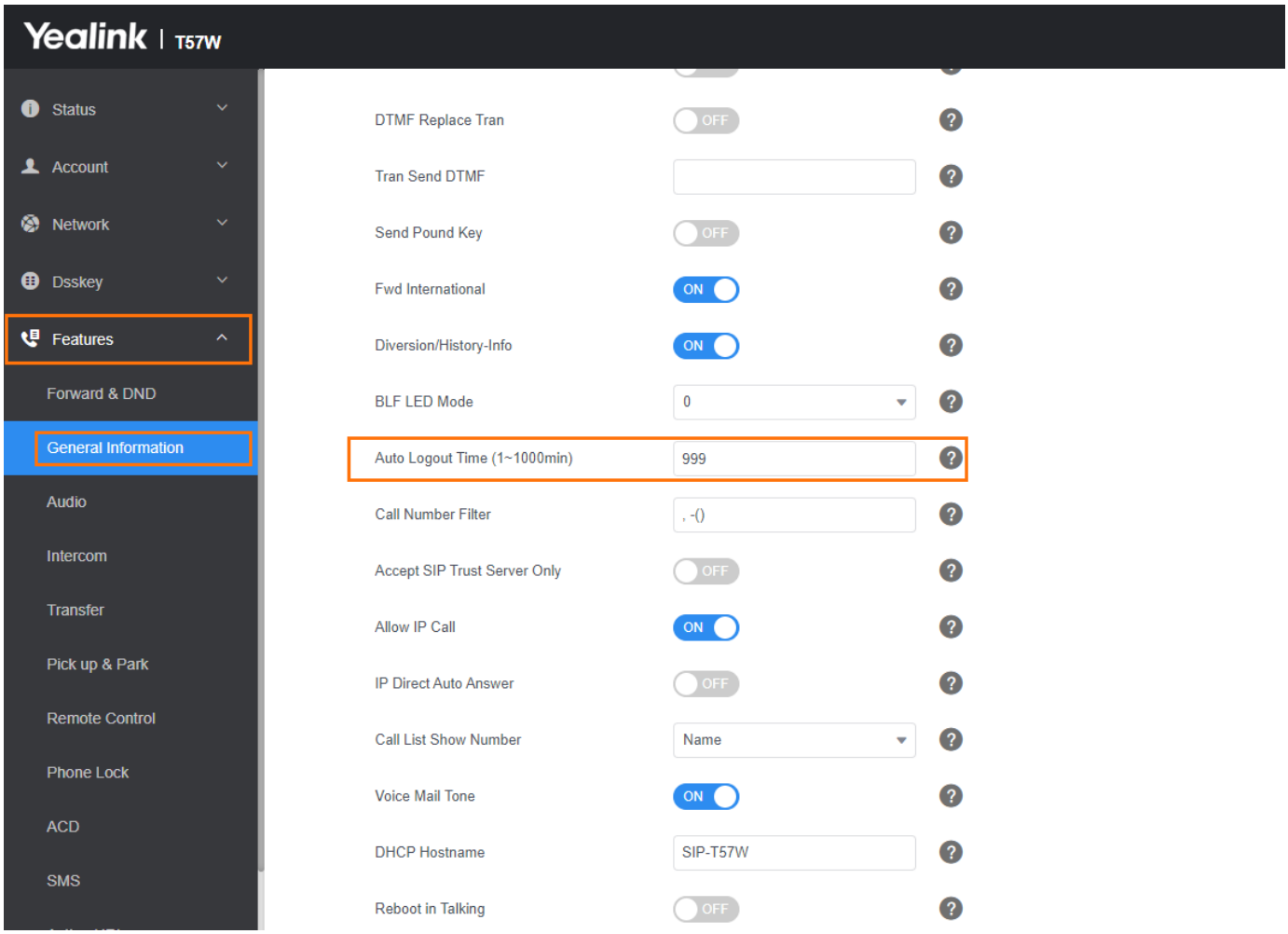
Introduction

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 rea-enter 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
wui.login_wait_time
wui.stay_active_wait_time

wui.operate_wait_time

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. It works only if your firmware version is x.86.0.112 or later.
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). It works only if your firmware version is x.86.0.112 or later.
wui.operate_wait_time	Integer from 1 to 120	15	It is used to configure the maximum allowed duration for operations after logging into the Web GUI configuration interface. It works only if your firmware version is x.86.0.112 or later.

Phone Lock

Phone Lock

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

Yealink phones offer three types of phone lock:

- Lock the Menu soft key: it prevents unauthorized users from accessing the menu and changing the personal settings for your phone.
- Lock the Function keys: it only allows unauthorized users to use the keypad for placing, answering, rejecting, or ending calls.
- Lock all keys: it only allows authorized users to use the keypad for dialing emergency numbers or authorized numbers that are set up by your administrator, answering, rejecting, and ending a call. The T57W/T48U/T48S/T48G phones only support the All Keys type of phone lock.

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.

> The Volume key, HEADSET key, and Speakerphone key are always available even when you lock the phone.

Operation Behaviors on Lock Phone

The following table lists the operation behavior when configuring the type of phone lock:

	All Keys	Function Keys	Menu key
Idle screen	Allowable Behavior: You are allowed to press the desired Line Key (key type is Line) or the Speakerphone/off-hook key to enter the dialing screen. Keys not Locked: Line keys (key type is Line), digit keys, HEADSET key, Volume key, Speakerphone key, off-hook key, and on-hook key. > Line key is not applicable to T30P/T30/T19 E2/T19 Pro E2/CP920 phones; Speakerphone key is not applicable to CP920/CP925/CP935W phones. Off-hook key and the on-hook key are only applicable	The same as All Keys.	The Menu key (key type is Menu) is locked.

	to CP920 phones.		
Incoming call	Allowable Behavior: You are allowed to answer or reject incoming calls. Keys not Locked: Answer and Reject soft key; OK/√ / , X, HEADSET key, Speakerphone key, off-hook key, and on-hook key. Pressing X key to reject the call is not applicable to T31P/T31G/T31/T30P/T30/T23P/T23G/T21 E2/T19 E2/T19 Pro E2/CP920/CP925/CP935W phones; HEADSET key and Speakerphone key are not applicable to CP920/CP925/CP935W phones. Off-hook key and the on-hook key are only applicable to CP920 phones.	The same as All Keys.	The Menu key (key type is Menu) is locked.
Pre-dialing/ Dialing screen	Allowable Behavior: You are allowed to press the Line Key (key type is Line), input or modify numbers, dial emergency numbers and return to the idle screen. Keys not Locked: IME, More, Cancel, Send, Delete and Line soft key; line key (key type is Line), X, OK/√ / , Volume key, Speakerphone key, digit keys, HEADSET key, “*” /” #” (key as send), off-hook key and on-hook key. Line key is not applicable to T30P/T30/T19 E2/T19 Pro E2/CP920 phones; Speakerphone key is not applicable to CP920/CP925/CP935W phones. Off-hook key and on-hook key are only applicable to CP920 phones.	The same as All Keys, but you can dial any number .	The Menu key (key type is Menu) is locked.
Talking	Allowable Behavior: You are allowed to end the call, initiate a new call to the emergency number, and resume a call. Keys not Locked: End Call, Cancel, Resume, NewCall soft key; line key (key type is Line), digit keys, X, Volume key, HEADSET key, Speakerphone key, off-hook key, and on-hook key. Pressing X key to end the call is not applicable to	The same as All Keys, but you can dial any number	The Menu key (key type is Menu) is locked.

	T31P/T31G/T31/T30P/T30/T23P/T23G/T21 E2/T19 E2/T19 Pro E2/CP920/CP925/CP935W phones; Line key is not applicable to T30P/T30/T19 E2/T19 Pro E2/CP920 phones. The headset and Speakerphone key is not applicable to CP920/CP925/CP935W phones. Off-hook key and the on-hook key are only applicable to CP920 phones.	·	

For T57W/T48U/T48S/T48G, all keys and screen are locked except the HEADSET key, Volume key, digit keys, # key, * key, and Speakerphone key.

Phone Lock Configuration

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

Configuration parameter

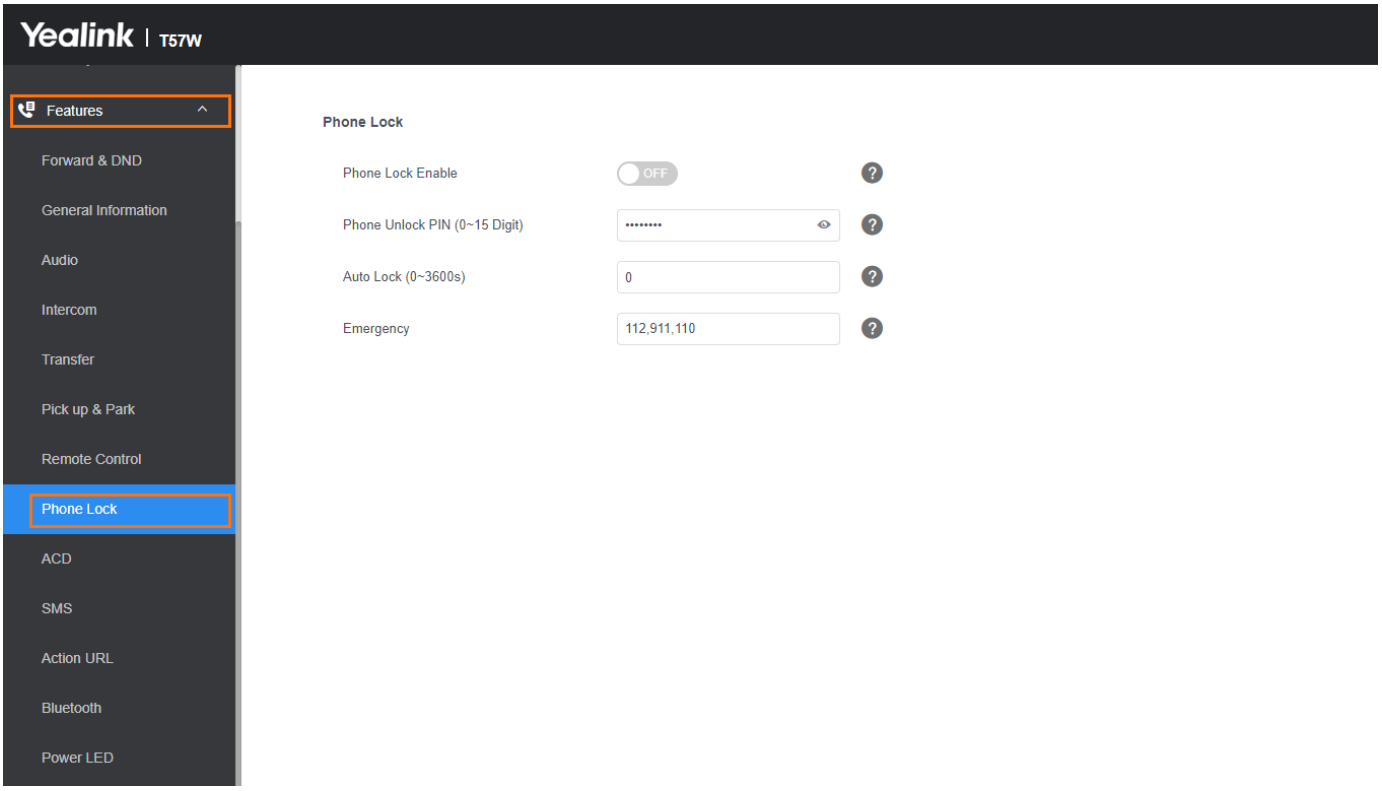
phone_setting.phone_lock.enable
phone_setting.phone_lock.unlock_pin
phone_setting.phone_lock.lock_time_out
phone_setting.emergency.number

Parameter	Permitted Values	Default	Description
phone_setting.phone_lock.enable	0-Disabled 1-Enabled	0	It enables or disables the phone lock feature.
phone_setting.phone_lock.unlock_pin	Characters within 15 digits	123	It configures the password for unlocking the phone.
phone_setting.phone_lock.lock_time_out	Integer from 0 to 3600	0	It configures the idle time (in seconds) before the phone is automatically locked. The default value is 0 (the phone is locked only by long pressing the pound key or pressing the phone lock DSS key). It works only if "phone_setting.phone_lock.enable" is set to 1 (Enabled).

phone_setting.emergency.number	String within 99 characters	Blank	It configures emergency numbers. Multiple emergency numbers are separated by commas. **For T57W/T48U/T48S/T48G**: If "phone_setting.phone_lock.enable" is set to 1 (Enabled), you are only allowed to dial the configured emergency numbers. **For other phones**: 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.

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-SHAA
- 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 *.de,r and the maximum file size is 5 MB.
Ser	When clients request a TLS connection with the IP phone, the phone sends the server

ver Certificate	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* .ce,r and the maximum file size is 5 MB.
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 may 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**.

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.

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

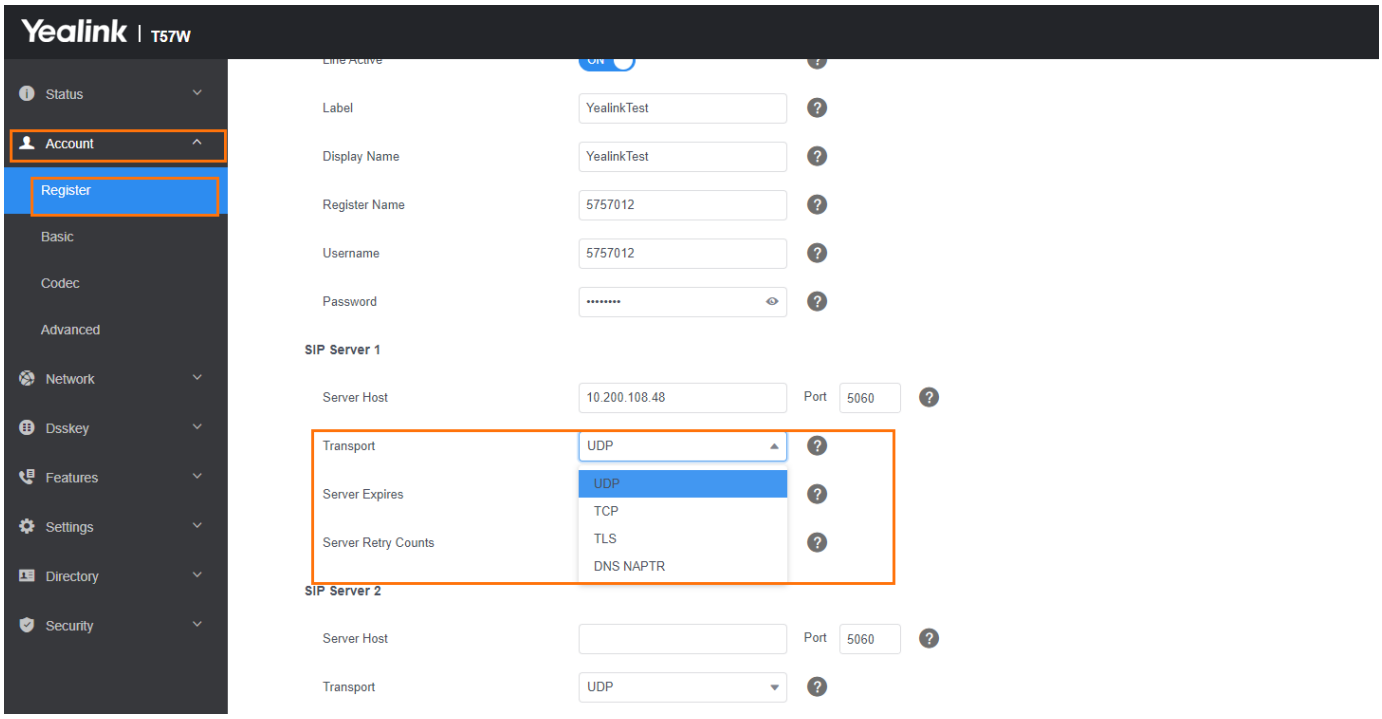
- VeriSign Class 3 Secure Server CA – G3
- Thawte SSL CA
- StartCom Certification Authority
- StartCom Certification Authority G2
- Starfield Services Root Certificate Authority - G2
- RapidSSL CA
- Go Daddy Root Certificate Authority - G2
- Cybertrust Global Root
- COMODOSSLCA
- COMODO RSA Domain Validation Secure Server CA
- COMODO RSA Certification Authority
- AmazonRootCA4
- AmazonRootCA3
- AmazonRootCA2
- AmazonRootCA1
- Yealink Root CA
- Yealink Equipment Issuing CA

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 to your phone.

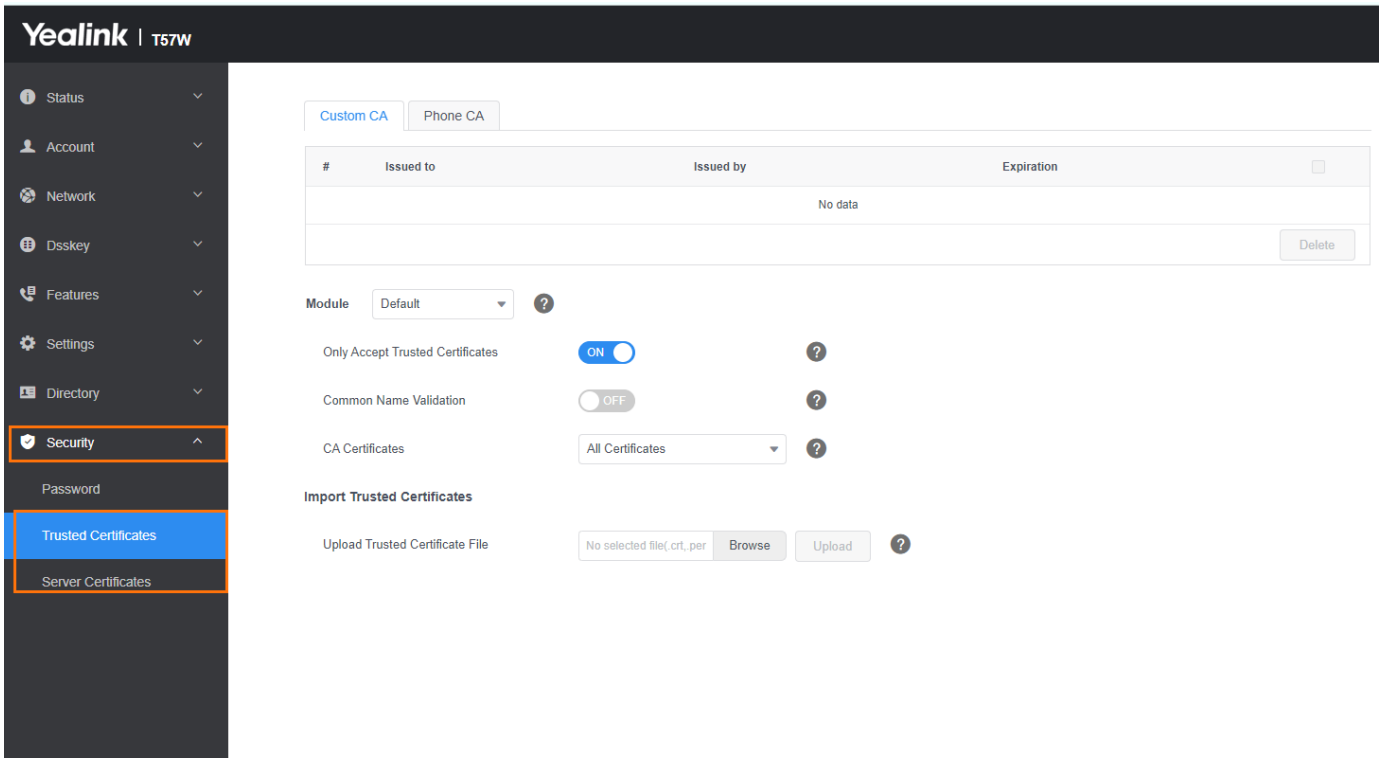
TLS Configuration

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

security.default_ssl_method

security.sip.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
security.sip.cn_validation

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	**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	2	It configures the supported TLS version to use for handshake negotiation between the phone and the web browser.
static.security.trust_certificates	**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.
security.default_ssl_method	**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	5	It configures the TLS version to use for handshake negotiation between the phone and server (for example, SIP registration server, provisioning server).
security.sip.ssl_method	**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	It configures the TLS version forthe SIP module.

	5-TLS 1.2 **6**-TLS 1.3		
static.security.ca_cert	**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 a TLS connection.
static.security.cn_validation	**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	**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. 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 that the phone sends for authentication. 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 a 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.
security	**0**-Disabled	0	It configures the SIP module to

y.sip.cn_validation	**1**-Enabled and verified all **2**-Enabled but do not verify SRV		enable CN verification.

> [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
```

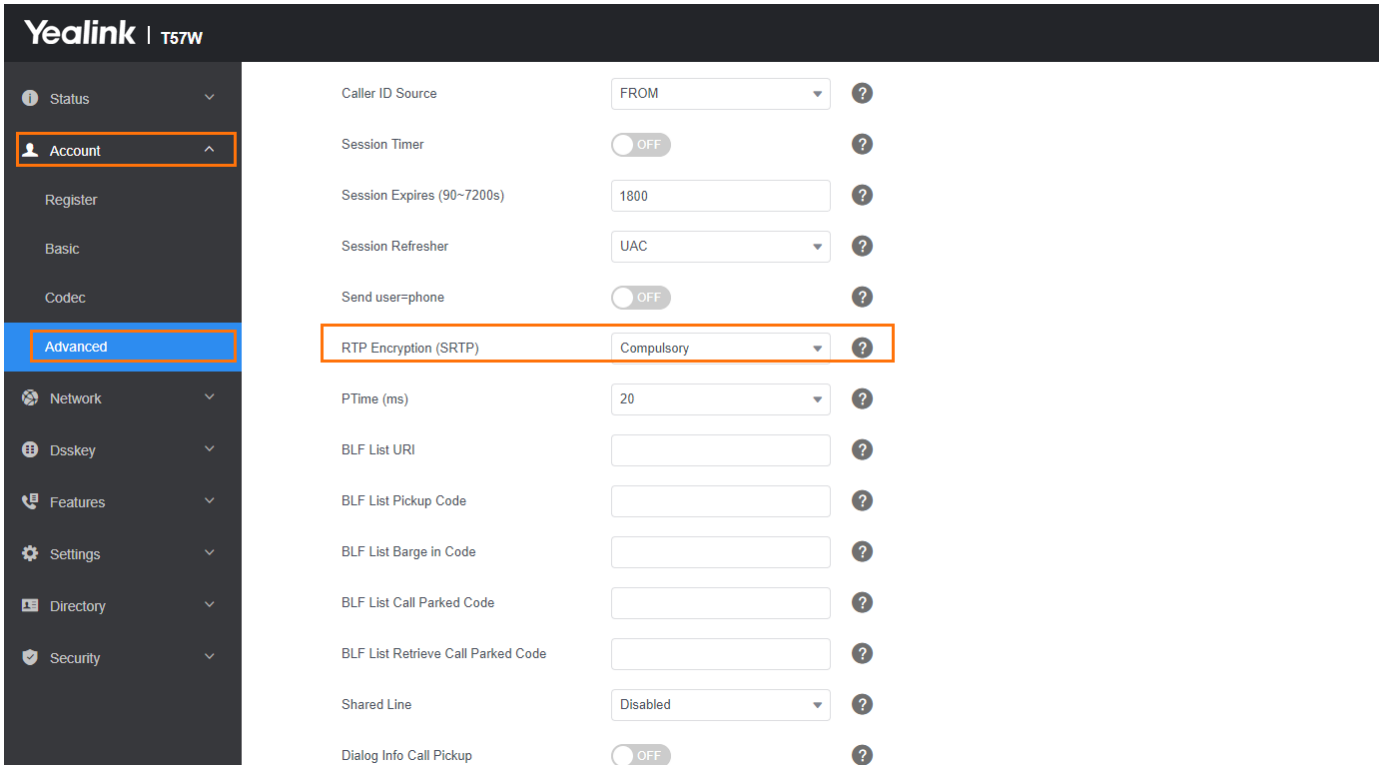
When SRTP is enabled on both phones, RTP streams will be encrypted, and a lock icon appears on the LCD screen of each IP phone after a successful negotiation.

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
account.X.srtp.cipher_list
```

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 the audio encryption service.
account.X.srtp.cipher_list[1]	String within 512 characters	Blank	It is used to configure the SRTP algorithm list. If multiple values are configured simultaneously, they need to be separated by commas. For example: 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,AEAD_AES_256_GCM, AEAD_AES_128_GCM It only works if the firmware version is V87 or later.

[1]X is the account ID.

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 configuration files:

- **MAC-Oriented CFG file** (e.g., <MAC>.cfg)
- **Common CFG file** (e.g., y0000000000xx.cfg)
- **MAC-Local CFG file** (e.g., <MAC>-local.cfg)
- **Other custom CFG files** (e.g., sip.cfg, account.cfg)

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

> 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 files 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 a new file named Aeskey.txt to store the plaintext 16-character symmetric keys for each configuration file.

Configuration Files Encryption and Decryption

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

registration information).

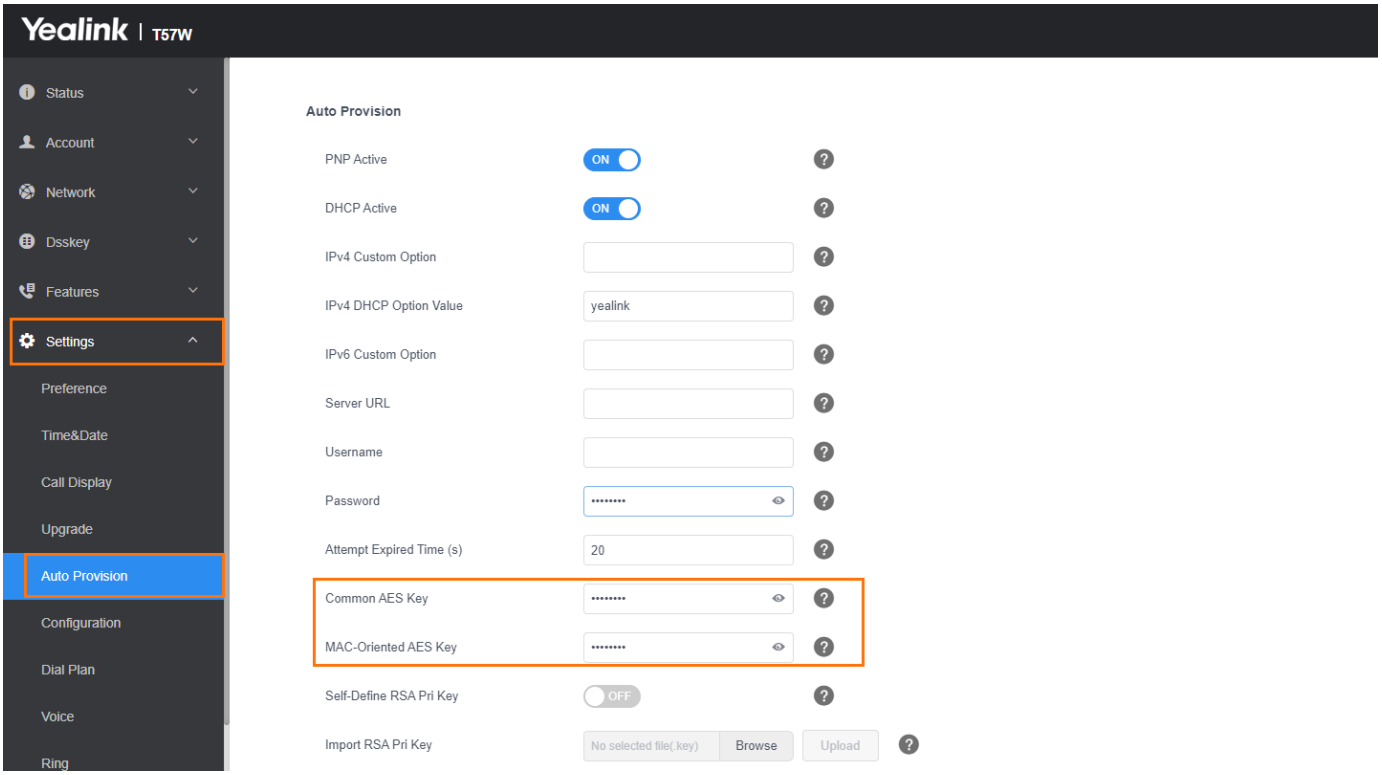
You can encrypt the configuration files using encryption tools. You can also configure the "<MAC>-local.cfg" files to be automatically encrypted using 16-character symmetric keys when uploading to the server (by setting "static. auto_provision.encryption.config" to 1).

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 IP phone decrypts account.cfg file using key2. After decryption, the phone resolves configuration files and updates configuration settings onto the IP 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 the settings on 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_	**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's built-in key (for example, key1). The phone then decrypts the encrypted configuration files using the	0	It enables or disables the phone to decrypt configuration files using the encrypted AES keys.

in_file	corresponding key (for example, key2, key3).		
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 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 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_pro	**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".	0	It enables or disables the phone to encrypt <MAC>-local.cfg file using the plaintext AES

vision.encryption.config	**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".		key.
static.auto_provision.rsa_pri_key.url	URL within 511 characters	Blank	It configures the URL to import the self-defined RSA private key file. 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	**0**-Disabled, the phone decrypts the encrypted configuration files using the phone's built-in RSA keys. **1**-Enabled, the phone decrypts the encrypted configuration files using a self-defined RSA private key.	0	It enables or disables the self-defined RSA private key.

.enable[2]			

> [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 IP 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.
4. To select multiple configuration files, you can select the first file and then press and hold the Ctrl key and select other files.
4. (Optional.) Click **Browse** to locate the target directory from your local system in the **Target Directory** field.
5. The tool uses the file folder "Encrypted" as the target directory by default.
5. (Optional.) 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

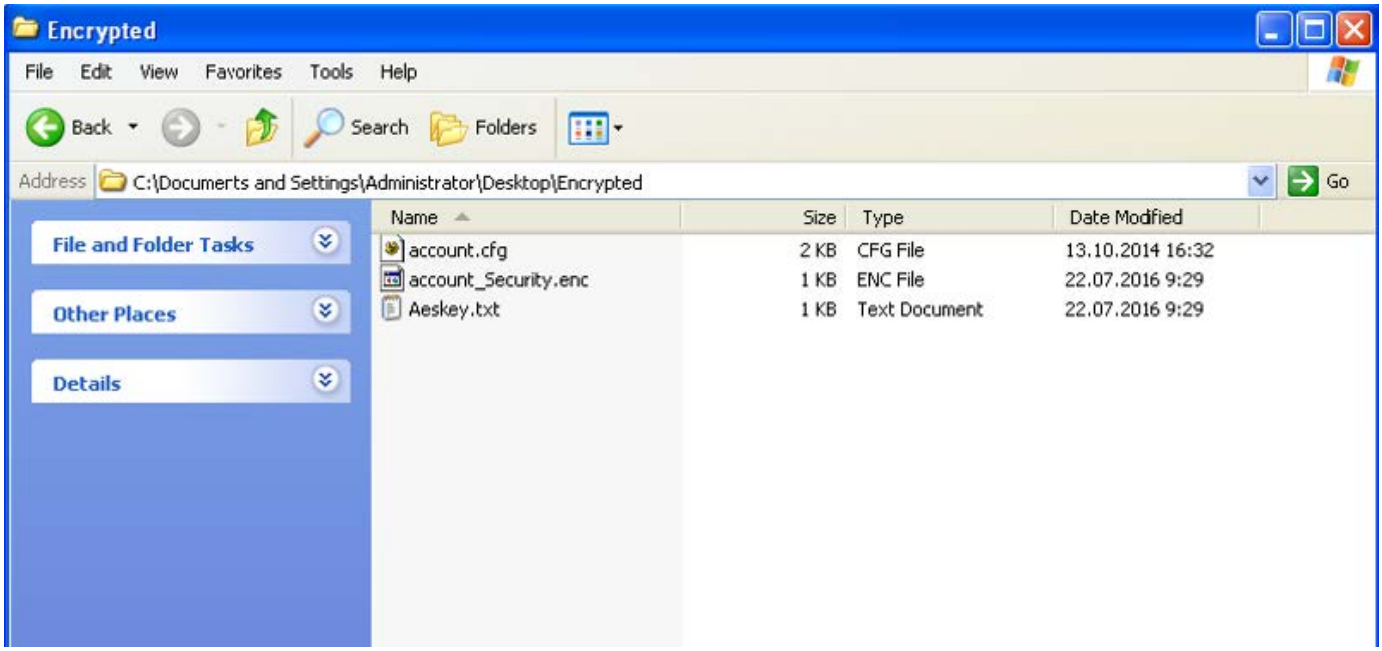
AES KEY field.

If you select the **Auto Generate** radio box, the configuration file(s) will be encrypted using a random AES key.

The AES keys of the configuration files are different.

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

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



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	YealinkSIP	It configures the string used for the authentication parameter Realm when performing the digest authentication.
sip.request_validation.event	A valid string	YealinkSIP	It configures which events specified within the Event header of the SUBSCRIBE or NOTIFY request should be validated. If it is left blank, all events will be validated.

USB Port Lock

Introduction

You can lock the USB port on phones which has a USB port.

The following features are not available when you disable the USB port:

- Adding a Wallpaper from a USB Flash Drive
- Adding a Screensaver Picture from a USB Flash Drive
- Wi-Fi (except T57W/T54W/T53W/CP920/CP925/CP935W)
- Bluetooth (except T57W/T54W/T53W/CP920/CP925/CP935W)
- USB Recording

USB Port Lock Configuration

Configuration parameter

static.usb.power.enable
static.usbdisk.function.enable

Parameter	Permitted Values	Default	Description
static.usb.power.enable[1]	0-Disabled, the phone does not provide power to the USB port and not detect USB devices attached to the USB port. All the USB devices are disabled on the phone. 1-Enabled	1	It enables or disables the USB port.
static.usbdisk.function.enable[1]	0-Disabled, the phone cannot detect the USB flash drive attached to the USB port. The USB item will not appear on the menu screen, and there is no USB icon on the status bar. Only the USB flash drive is disabled; other USB devices, such as a Bluetooth dongle, are still available on the phone. 1-Enabled	1	It enables or disables the USB flash drive feature. It works only if "static.usb.power.enable" is set to 1 (Enabled).

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

Simple Certificate Enrollment Protocol

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

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

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

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

static.scep.password	String within 256 characters	Blank	It configures the password of the SCEP server.
static.scep.enroll.retry_count	Integer from 1 to 12	3	It configures the retry count of the phone registration to the SCEP server error/waiting, and certificate acquisition failure.
static.scep.enroll.retry_interval	Integer from 300 to 3600	300	It configures the seconds between retry attempts for phone registration to the SCEP server, error/wait and certificate acquisition failure.
static.scep.renewal.threshold	Integer from 50 to 100	80	It configures the percentage of the certificate validity period when the phone initiates an update from the SCEP server.
static.scep.renewal.time	The first two digits represent the clock: 00-23; The last two digits represent the minute: 00-59;	100	It configures the start time when the phone initiates the certificate update to the SCEP server.
static.scep.challenge_password	String within 256 characters	Blank	It configures the verification password when the phone requests a certificate from the SCEP server.
static.scep.csr.common_name	String within 64 characters	Blank	It configures the common name used to generate the CSR (Certificate Signing Request).
static.scep.csr.organization	String within 64 characters	Blank	It configures the legal name used to generate the CSR organization.
static.scep.csr.email	String within 64 characters	Blank	It configures the email address used to generate the CSR.
static.scep.csr.state	String within 64 characters	Blank	It configures the state/province name used to generate the CSR.

			It can not be abbreviated and should include suffixes such as Inc, Corp, or LLC.
static.scep.csr.country	String within 2 characters	Blank	It configures the country name used to generate the CSR. The ISO code of the country/region where the organization is located.

Panic Button

Introduction

You can enable the panic button function by connecting a special USB cable to the phone. After connecting, you can set the emergency number and then press the button, the phone will call the emergency number you set before.

- Silence Speed Dial Mode: When making an outgoing emergency call, the screen saver interface is activated and remains on this interface. The keypad is locked, preventing calls to other numbers.
- Speed Dial Mode: When making an emergency call, once the other party answers the call, both parties can continue the conversation normally.

Only applicable to T5XW & T4XU & T7X & T8X phones.

Auto Provisioning

features.emergency_button.mode

Parameter	Description	Permitted Values	Defaul t
features.emergency_button.mode	It configures the alarm mode of the button alarm.	0-Disabled 1-Silence Speed Dial mode 2-Speed Dial mode	0

Emergency Alarm

Introduction

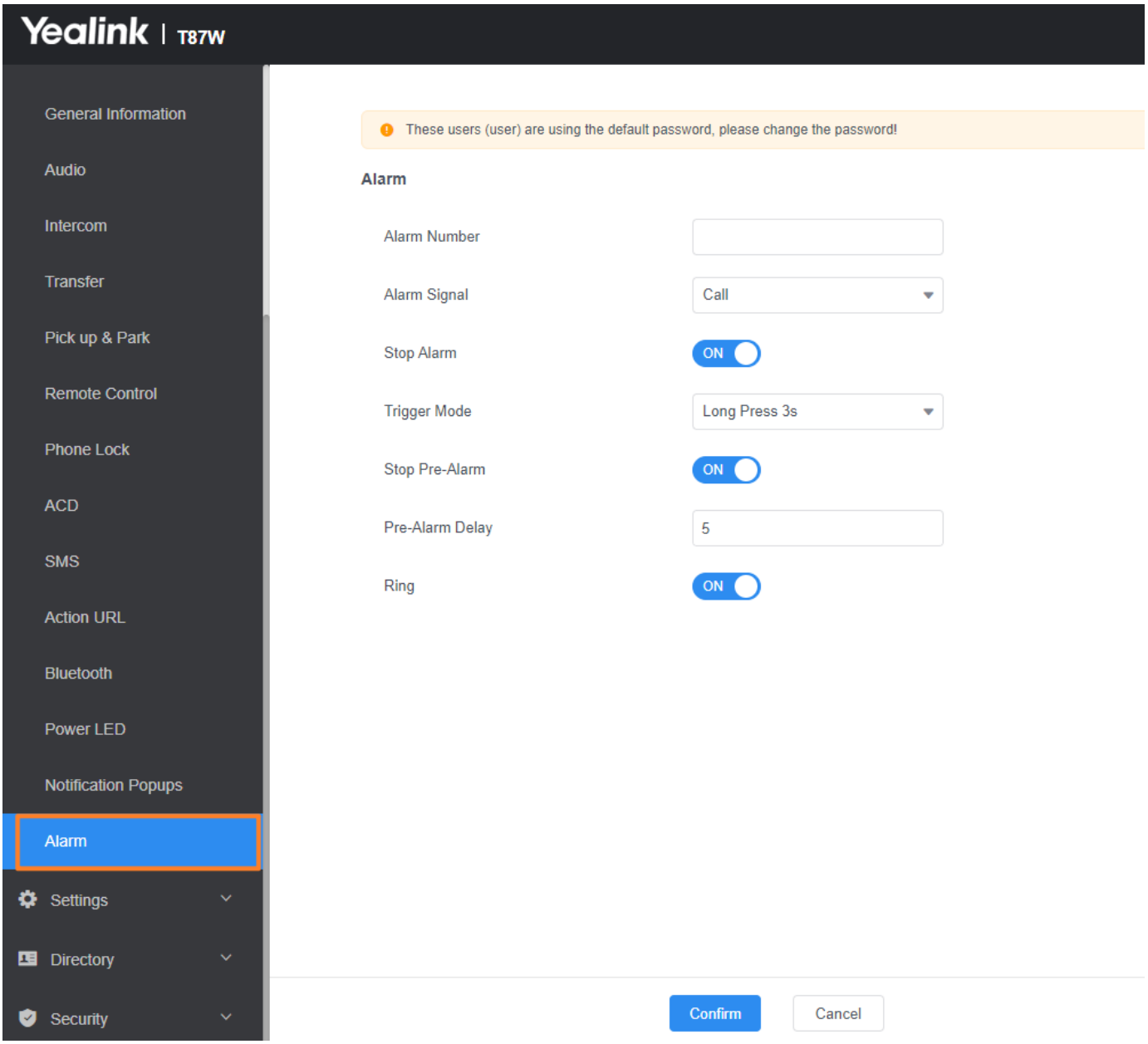
Emergency alarms can provide safety for people who work in dangerous environments.

Only applicable to T85W/T87W/T88W/T88W Pro/T88V Pro phones.

Emergency Alarm Configuration

Set via the Web User Interface

On the web user interface, go to **Features** > **Alarm**.



Auto Provisioning

alarm.button_trigger_mode
features.emergency_button.mode
alarm.button.report.mode
alarm.button.pre_alarm.stop.enable
alarm.button.stop.enable
alarm.button.pre_alarm.delay
alarm.number
action_url.alarm.trigger
alarm.button.ring.enable

Parameter	Optional Values	Default	Description
alarm.button_trigger_mode	**0**-Triggered by long-pressing the alarm key for 3 seconds. **1**-Triggered by double-pressing the alarm key.	0	It configures the triggering method of the alarm for the Button on the phone.
features.emergency_button.mode	**0**-Disable button alarm. **1**-Silent alarm mode. **2**-Normal call mode	2	It configures the alarm mode of the button alarm.
alarm.button.report.mode	**0**-Call, make an outgoing call. **1**-Action URL, report the alarm information to the server only through the Action URL.	0	It configures the way of receiving the alarm signal.
alarm.button.pre_alarm.stop.enable	**0**-Disabled **1**-Enabled	1	It configures whether to enable the function of stopping the pre-alarm on the phone.
alarm.button.stop.enable	**0**-Disabled **1**-Enabled	1	It configures whether to enable the function of stopping the alarm on the phone. It works only if "alarm.button.report.mode" is set to 0.

alarm.button.pre_alarm.delay	Integer from 0 to 7200	5	It configures the pre-alarm time of the Button alarm type, with the unit being seconds.
alarm.number	String within 128 characters	Blank	It configures the alarm call number for the account.
action_url.alarm.trigger	String within 511 characters	Blank	It configures the URL for reporting to the server when the alarm function is triggered.
alarm.button.ring.enable	**0**-Disabled **1**-Enabled	1	It configures whether to enable the ringing prompt when the phone initiates a pre-alarm.

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.

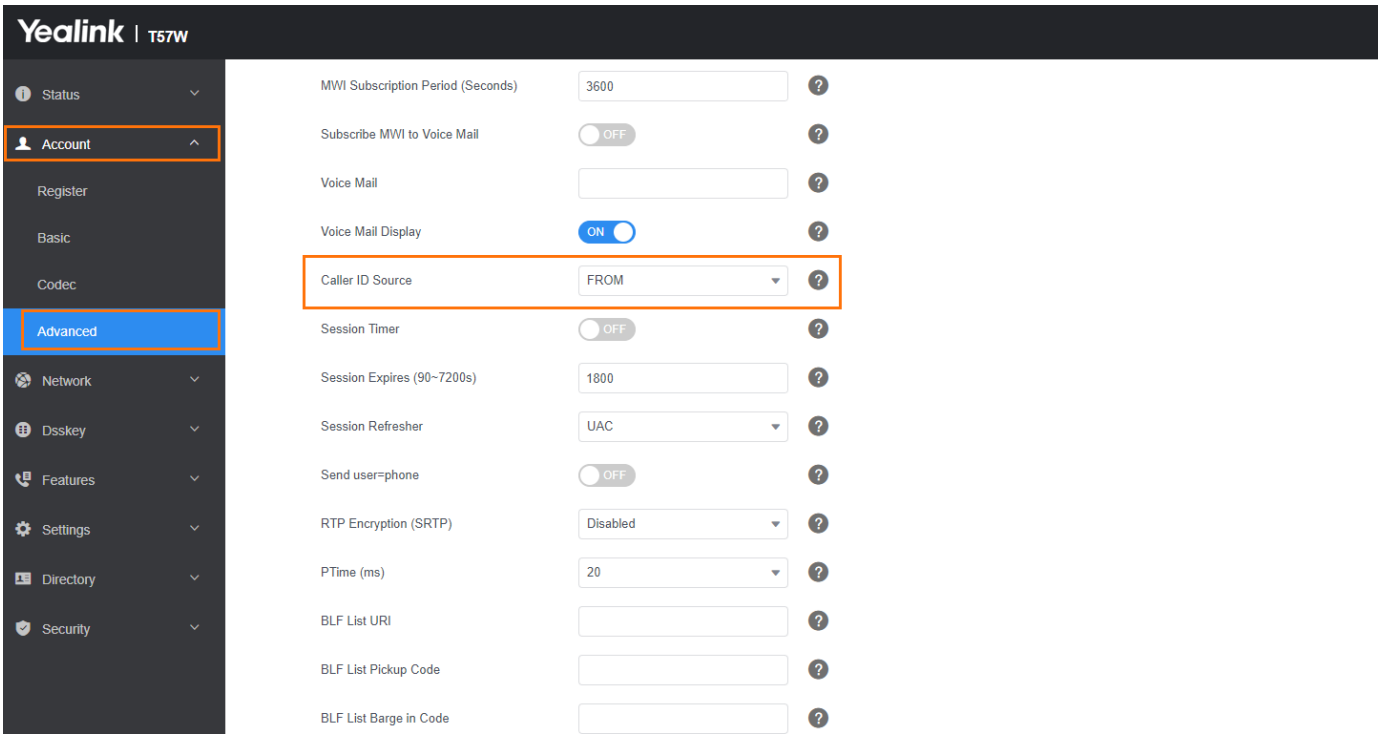
> If the caller/callee already exists in the local directory, the local contact name assigned to the caller will be preferentially displayed and stored in the call log.

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 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. 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. 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.	**0**-PAI-RPID **1**-Dialed Digits	0	It configures the identity of the callee according to the

X.cp_source[1]	**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		response message.

[1] X is the account ID.

Return Code of Refused & Unanswered Call

Introduction

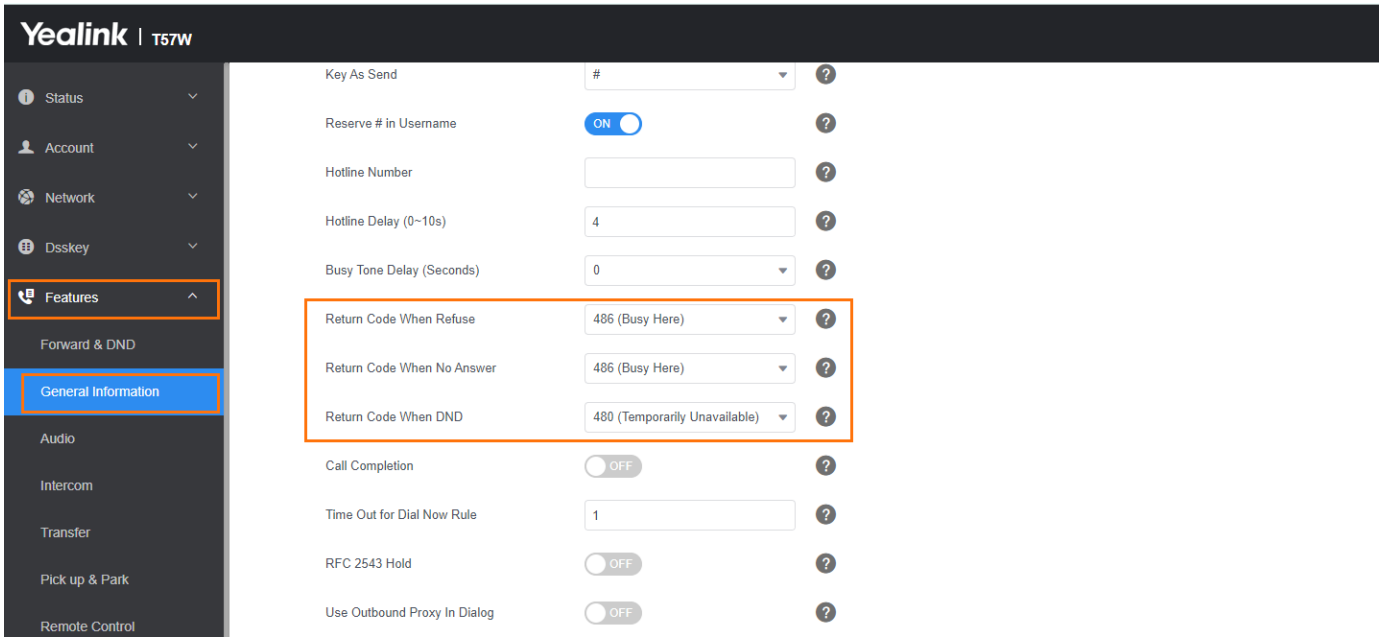
You can define the return code and reason of the SIP response message for the refused call. The caller's phone LCD screen displays the reason according to the received return code. Available return codes and reasons are:

Return Code	Reason
404	Not Found
480	Temporarily Unavailable
486	Busy Here
600	Busy Everywhere
603	Decline

Return Code for Refused Call and Unanswered 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 for response messages when the handset does not answer an incoming call. A specific reason is displayed on the caller’ s phone screen.

Accept the SIP Trust Server Only

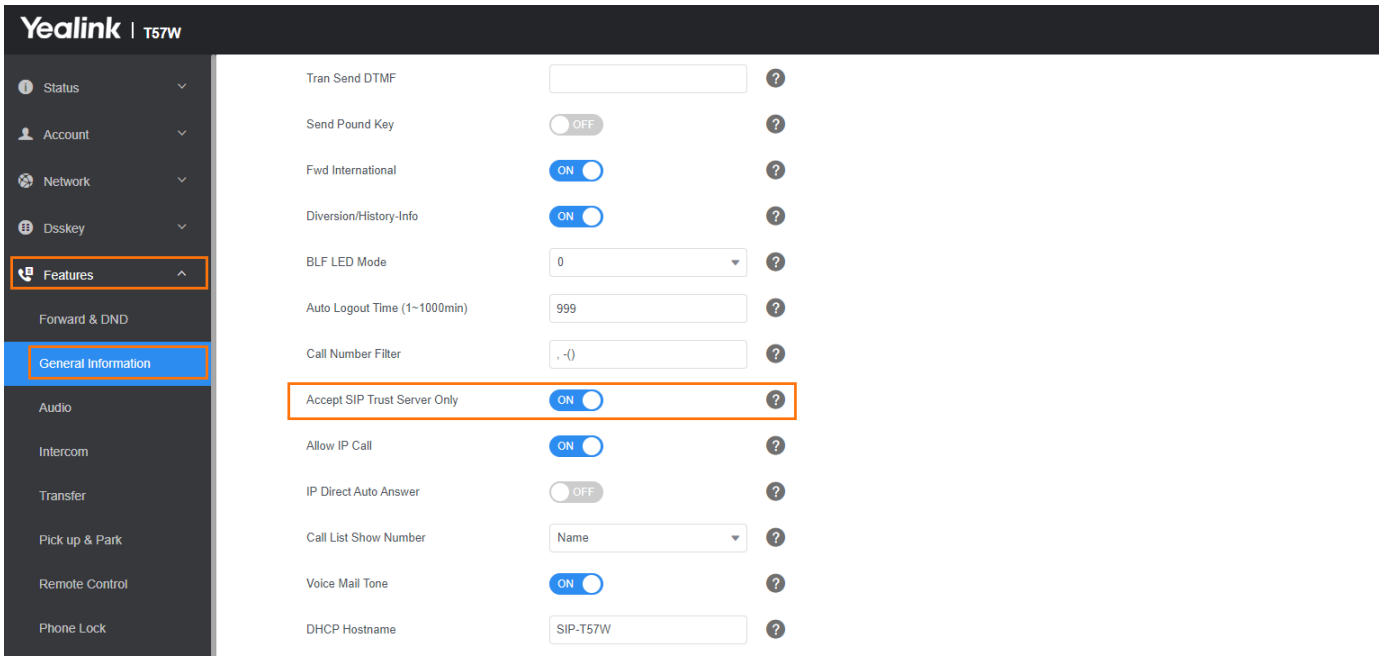
Introduction

Accept SIP trust server only enables the phones to only accept the SIP message from your SIP server and outbound proxy server. It can prevent the phone from receiving the ghost calls whose phone number maybe 100, 1000 and so on. If you enable this feature, the phone cannot accept an IP address call.

Accept the 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.

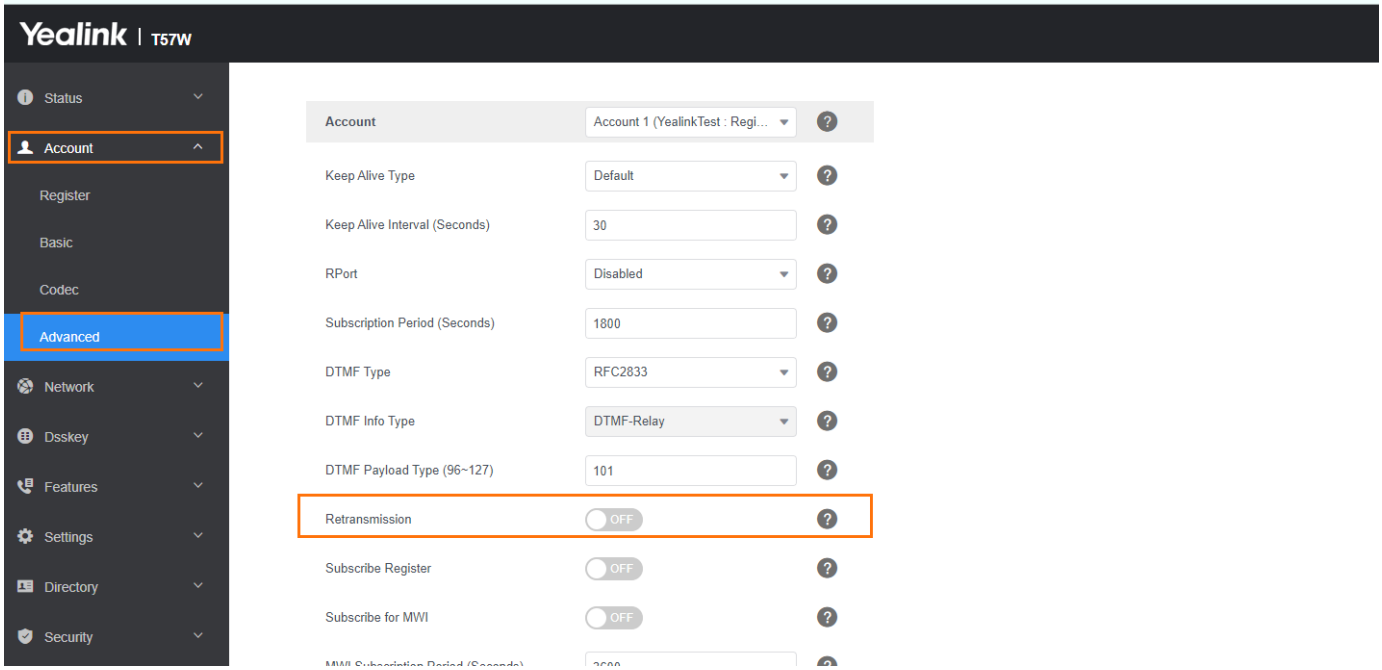
Example of a SIP INVITE message (take T57W as an example):

```
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

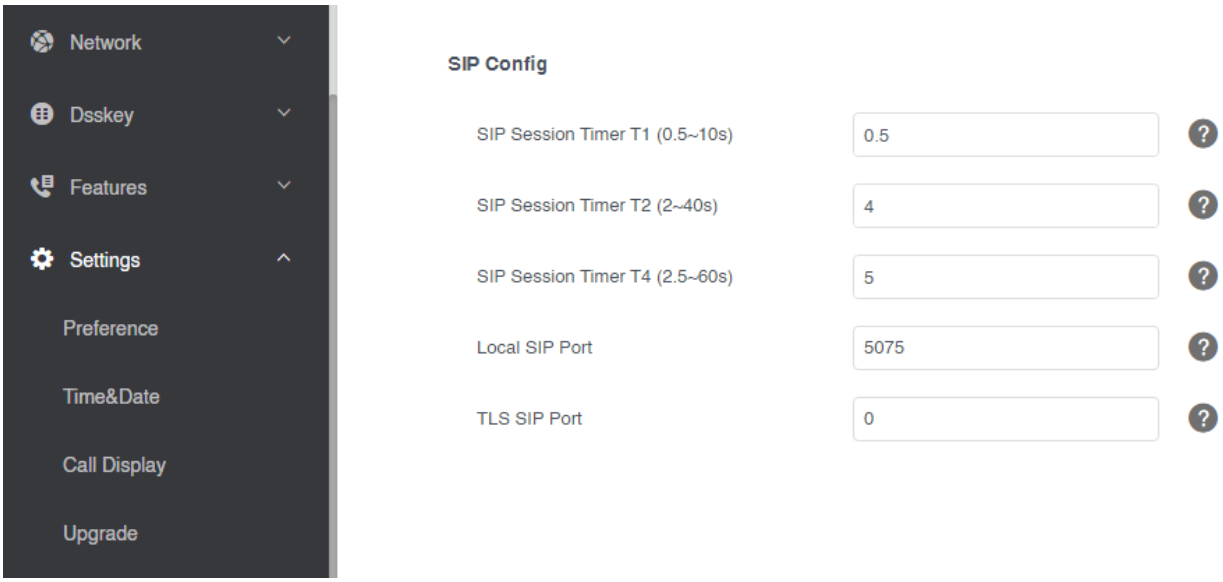
SIP session timers T1, T2 and T4 are SIP transaction layer timers defined in RFC 3261. These session timers are configurable on the phones.

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 sets 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 the SIP server. The re-transmitting and doubling of Timer T1 (0.5) will continue until the retransmitting time reaches 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 a 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.

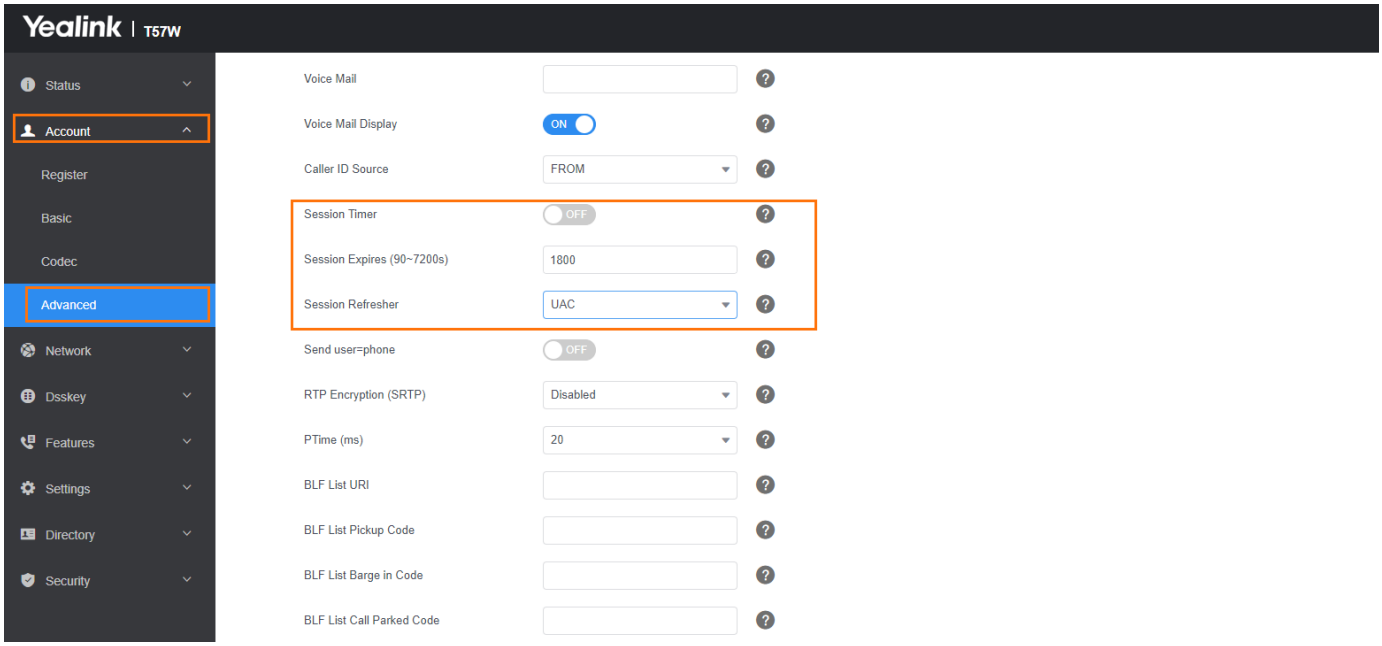
Example of UPDATE message (UAC mode) (take T57W as an example):

```
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 T57W 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. 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. It works only if "account.X.session_timer.enable" is set to 1 (Enabled).

[1] X is the account ID.

Reboot in Talking

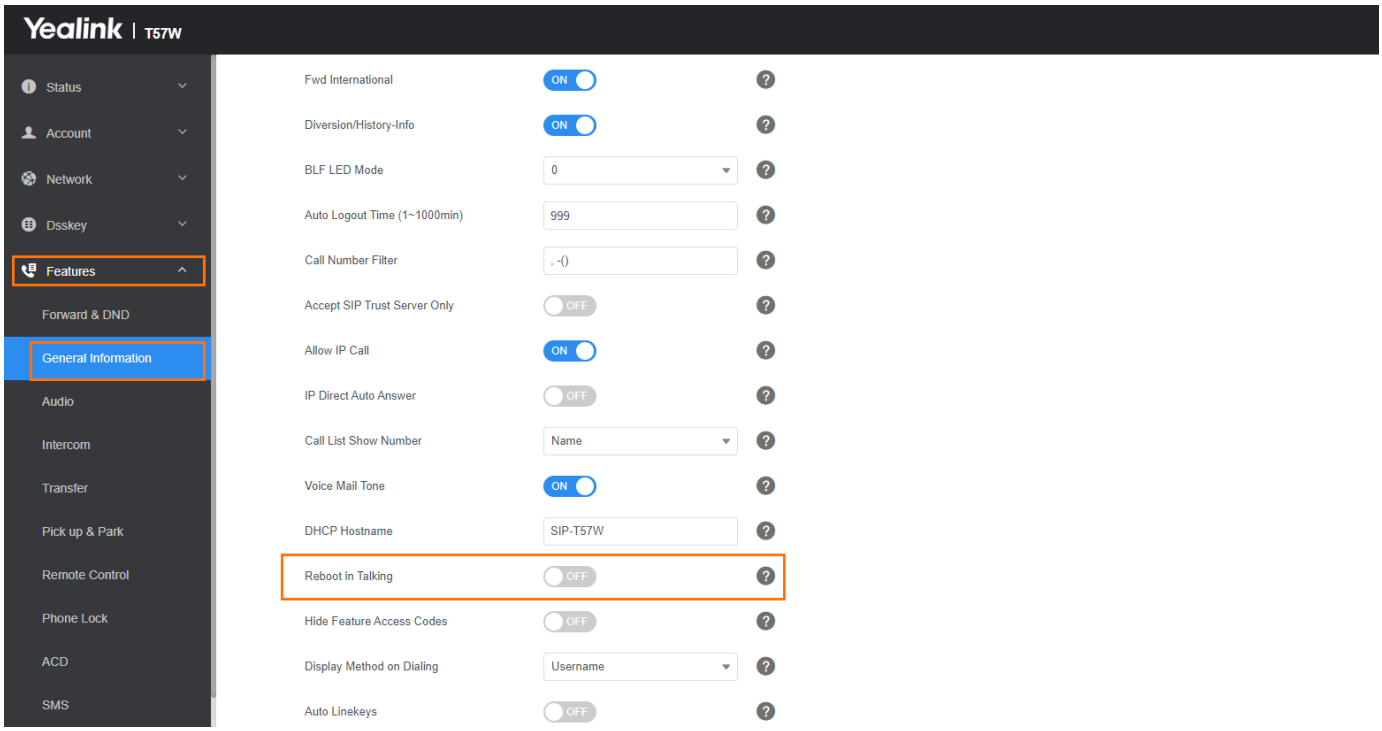
Introduction

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**-Enable	0	It enables or disables the phone to reboot during a call when it receives a reboot Notify message.

	d		

Reserve # in User Name

Introduction

Reserve # in User Name feature allows the phones to reserve “#” in 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.

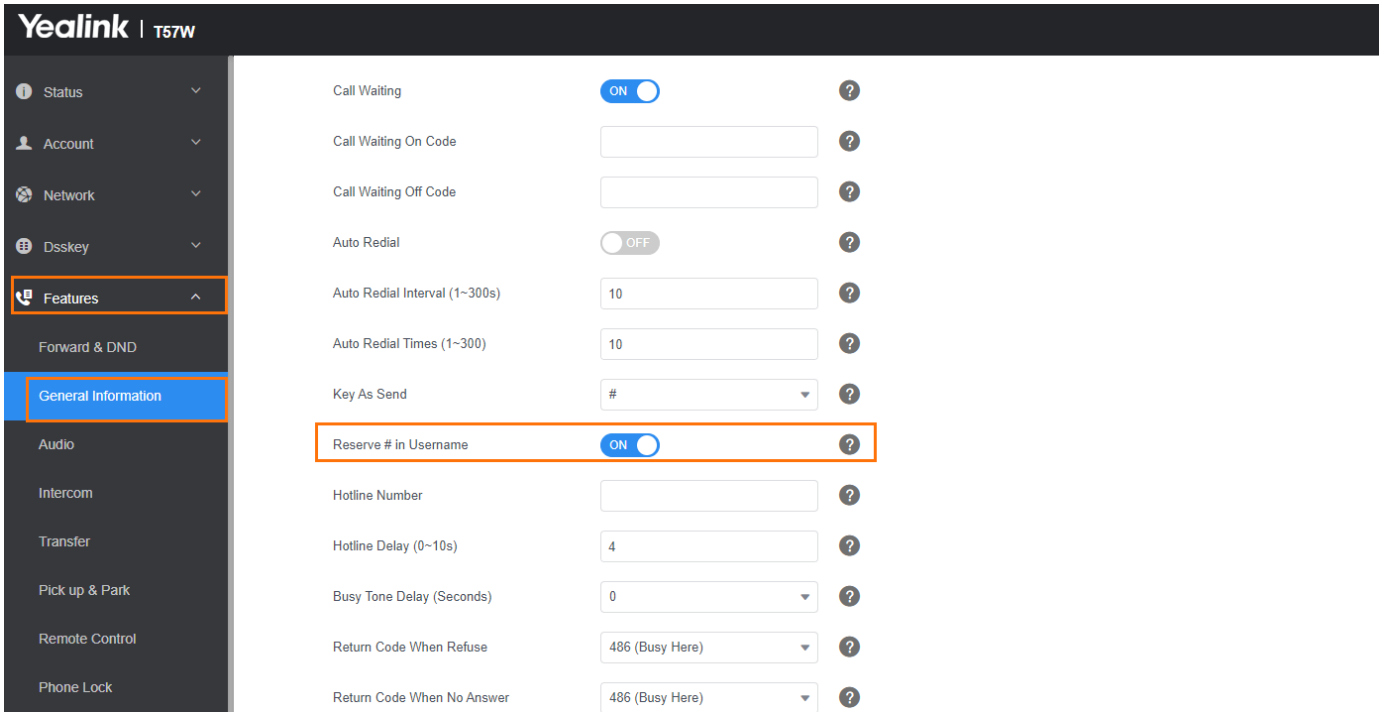
Example of a SIP REGISTER message (take T57W as an example):

```
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 T57W 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

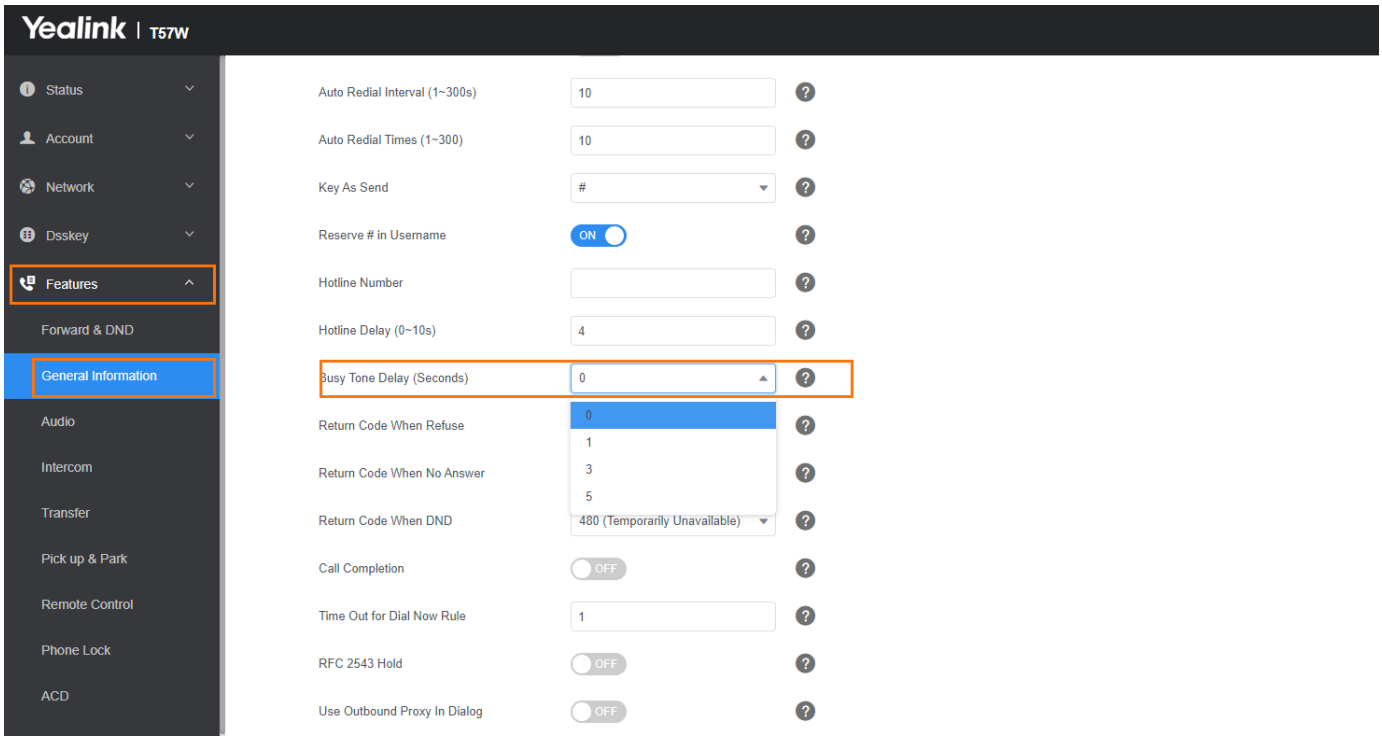
Introduction

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.	0	It configures the duration (in seconds) that the busy tone lasts when the call is released by the remote party.

	3-3s, a busy tone lasts for 3 seconds on the phone. **5**-5s, a busy tone lasts for 5 seconds on the phone		

FAQ

How to close the busy tone?

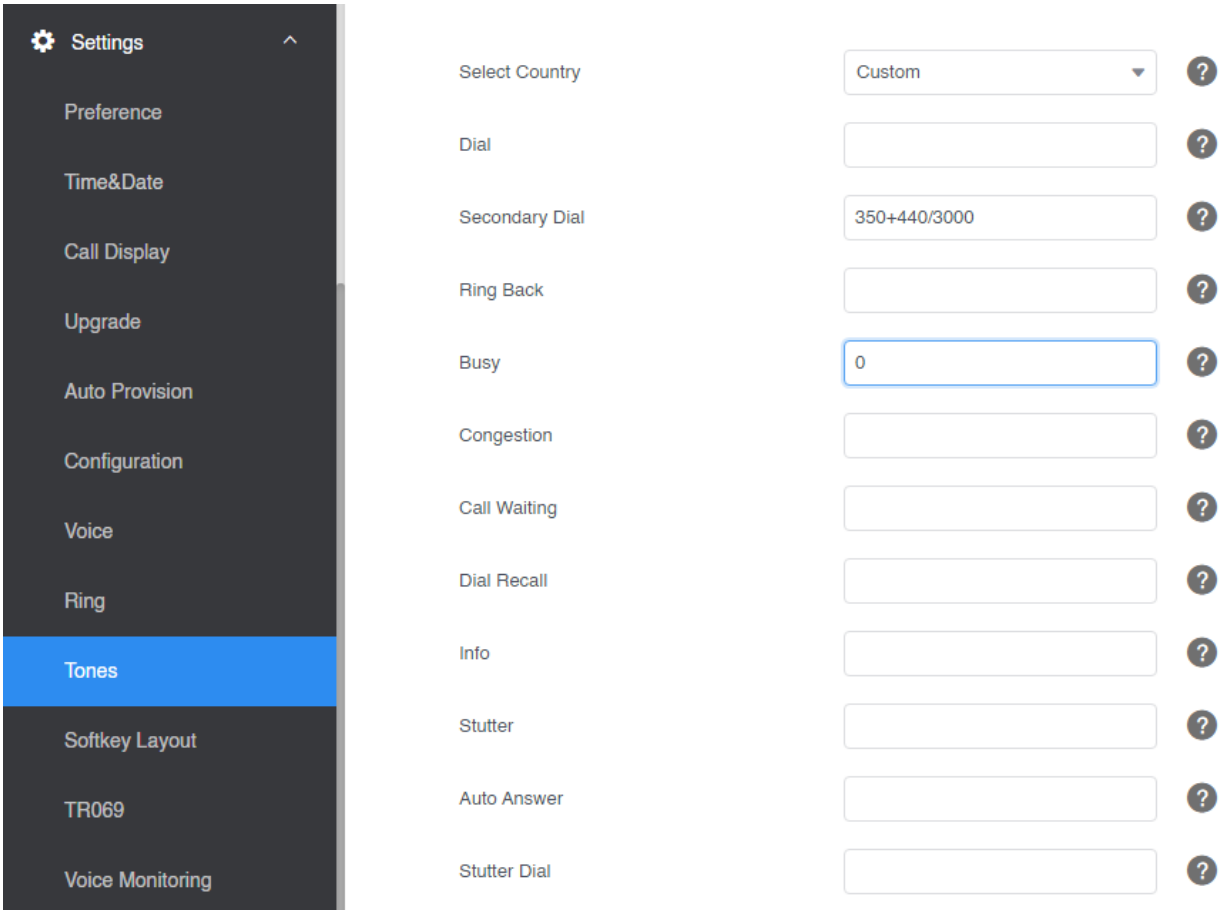
There are two configuration methods:

- **Set via the Web User Interface**

  a. Go to **Settings** > **Tone.**

  b. Set the country tone for the phone to be custom.

  c. Set the B**usy** item to **0**.



- **Set via the Auto Provision**

```
voice.tone.country = Custom
voice.tone.busy =0
```

Call Pickup

Introduction

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.

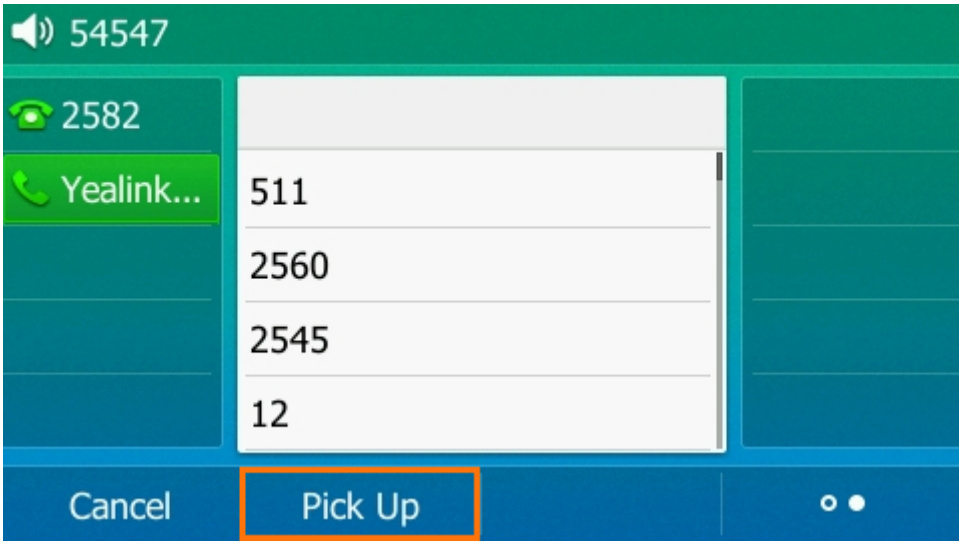
Directed Call Pickup

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, pressing the Speakerphone key, or pressing the line key (You may need to press the More soft key to see the DPickup soft key). As shown below:



You can configure a directed call pickup code and pick up the incoming call using the DPickup soft key.

> You can set a DSS key as a Directed Pickup key, and specify a contact you want to pick up a call from for this key. For more information, refer to DSS Keys.

The following table lists the parameters you can use to configure directed call pickup.

Configuration parameter

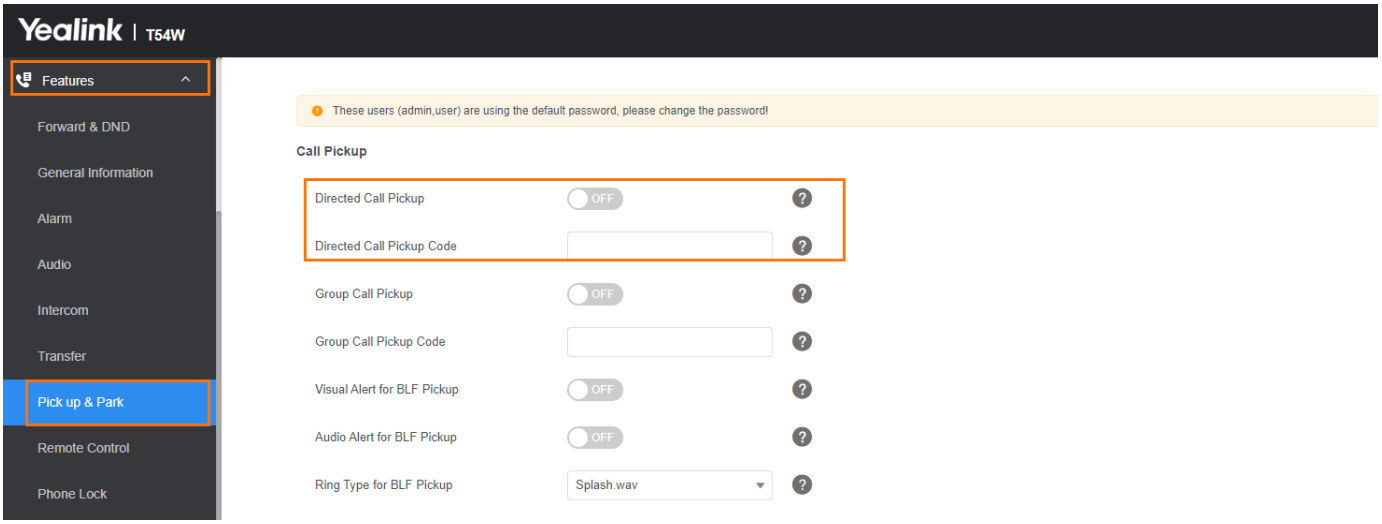
features.pickup.direct_pickup_enable
features.pickup.direct_pickup_code
account.X.direct_pickup_code

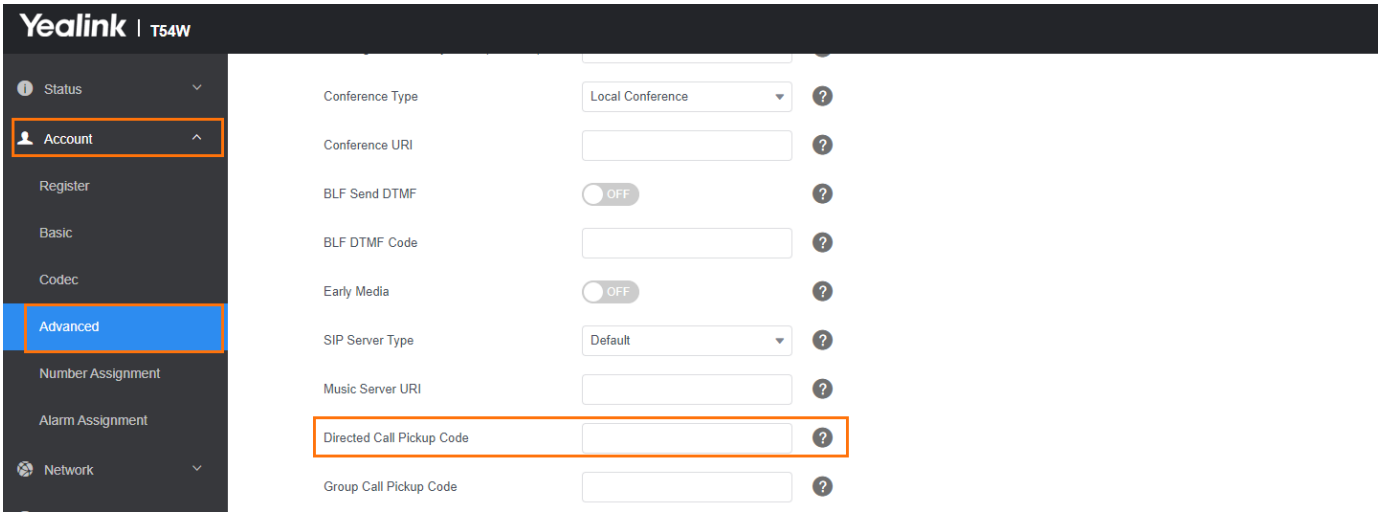
Parameter	Permitted Values	Defaul t	Description
features.pickup.direct_pickup_enable	0-Disabled 1-Enabled, the phone will display the DPickup soft key on the Dialing screen.	0	It enables or disables the user to use DPickup soft key when performing the directed call pickup feature.
features.pickup.direct_pickup_code	String within 32 characters	Blank	It configures the directed call pickup code on a phone basis. The code configured by "account.X.direct_pickup_code" takes precedence over that configured by this parameter.
account.X.direct_pickup_code[1]	String within 32 characters	Blank	It configures the directed call pickup code. The code configured by this parameter takes precedence over that configured by "features.pickup.direct_pickup_code".

[1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/Video Phone/T74U/T74W/T77U/T85W/T87W/T88W (Pro)/T88V Pro, X=1-16; for T53W/T53/T53C/T43U/T42G/T42U/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 E2, X=1-2; for T30P/T30/T19 § E2/CP920/CP925/CP935W, X=1.

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, pressing the Speakerphone key, or pressing the line key. As shown below:

You can pick up the group's incoming call using the GPickup soft key.

> You can set a DSS key as a Group Pickup key to pick up a group call. For more information, refer to DSS Keys.

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	Permitted Values	Default	Description
features.pickup.group_pickup_enable	**0**-Disabled **1**-Enabled, the phone will display the GPickup soft key on the Dialing screen.	0	It enables or disables the user to use GPickup soft key when performing group call pickup feature.
features.pickup.group_pickup_code	String within 32 characters	Blank	It configures the group call pickup code on a phone basis. The code configured by "account.X.group_pickup_code" takes precedence over that configured by this

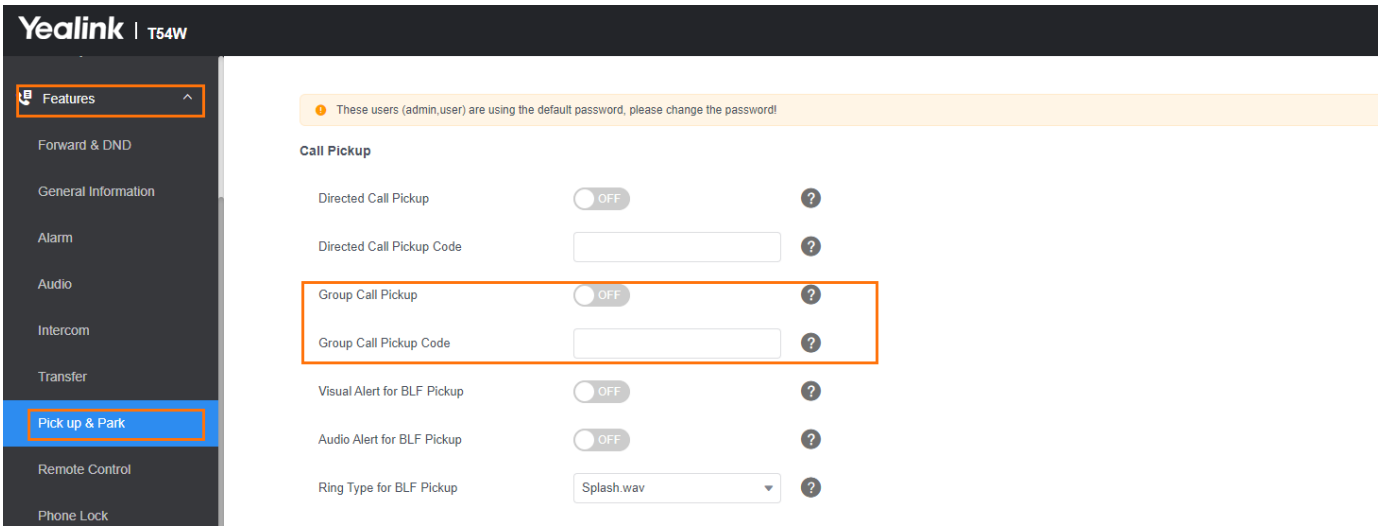
			parameter.
account.X.group_pickup_code[1]	String within 32 characters	Blank	It configures the group pickup code. The code configured by this parameter takes precedence over that configured by "features.pickup.group_pickup_code".

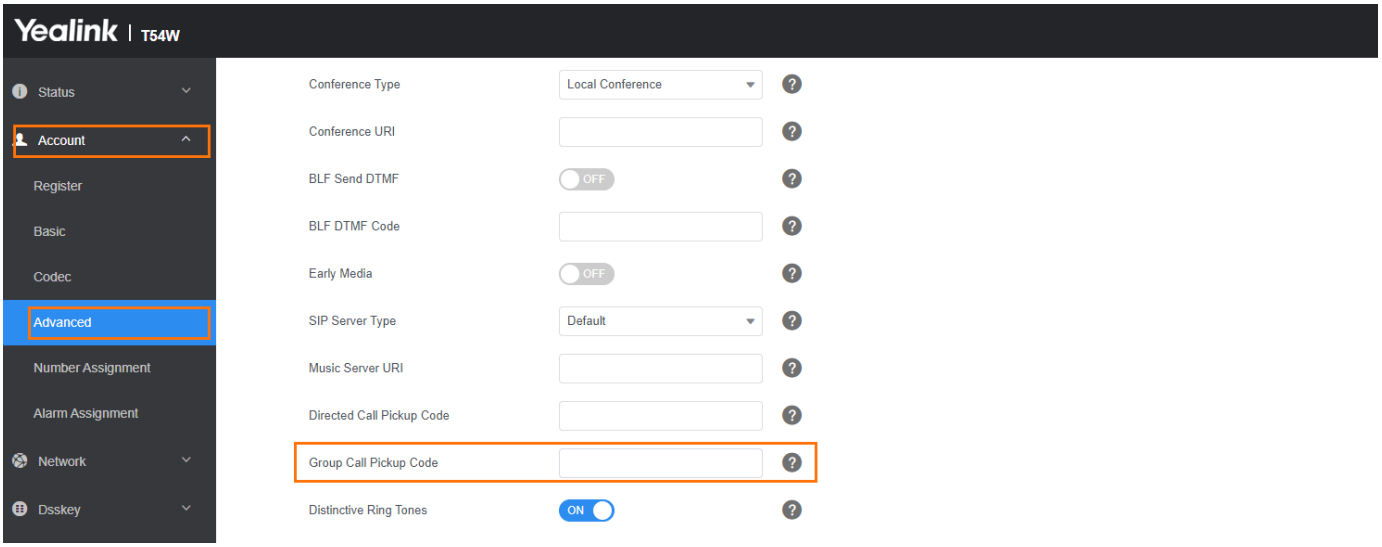
[1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/Video Phone/T74U/T74W/T77U/T85W/T87W/T88W (Pro)/T88V Pro, X=1-16; for T53W/T53/T53C/T43U/T42G/T42U/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 § E2, X=1-2; for T30P/T30/T19 E2/CP920/CP925/CP935W, X=1.

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.

> 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 a 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. It is not applicable to T30P/T30/T19 E2/T19P E2 phones.

Example of the dialog-info carried in the 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="recipient">
<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 the 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, MESSAGE
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 the dialog Info call pickup.

Configuration parameter

```
account.X.dialoginfo_callpickup
```

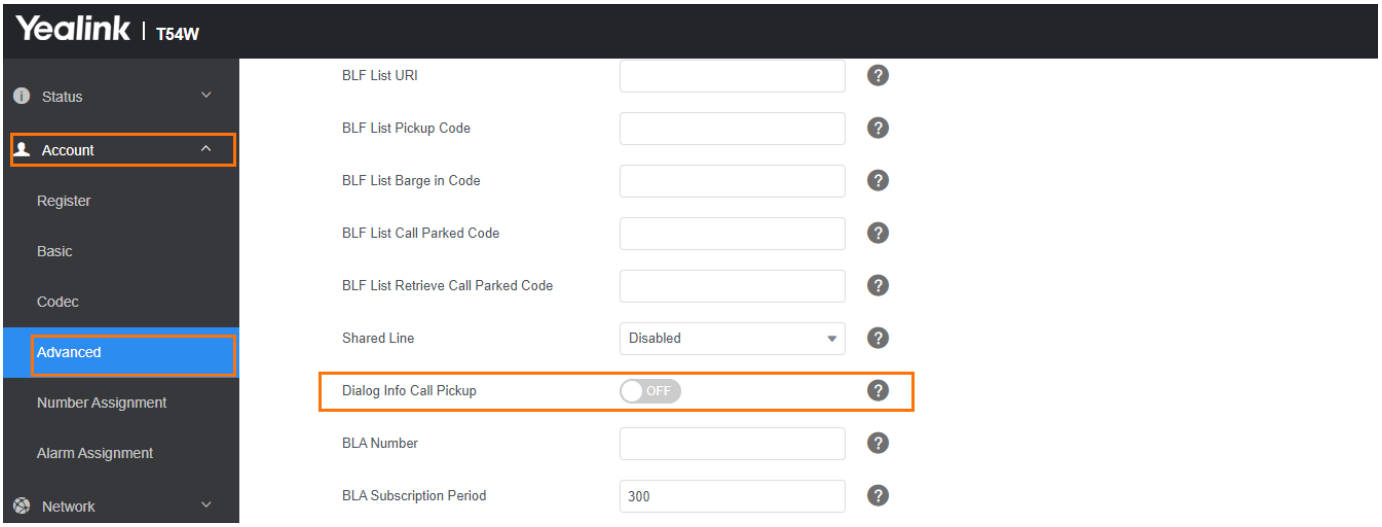
Parameter	Permitted Values	Default	Supported Devices	Description
account.X.dialog	0-Disabled 1-Enabled, the phone picks	0	All phones	It enables or disables the phone implementation's directed call

info_callpickup[1]	up a call according to the Replaces header in the INVITE message.		except T30P/ T30/ T19 § E2	pickup through SIP signals for a specific account. In this way, you do not need to configure the directed call pickup code.

> [1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/Video Phone/ T74U/T74W/T77U/T85W/T87W/T88W (Pro)/T88V Pro, X=1-16; for T53W/T53/T53C/T43U/T42G/ T42U/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/ T23P/T23G, X=1-3; for T31P/T31G/T31/T21 § E2, X=1-2; for T30P/T30/T19 E2/CP920/CP925/ CP935W, X=1.

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 to 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="initiator">
<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

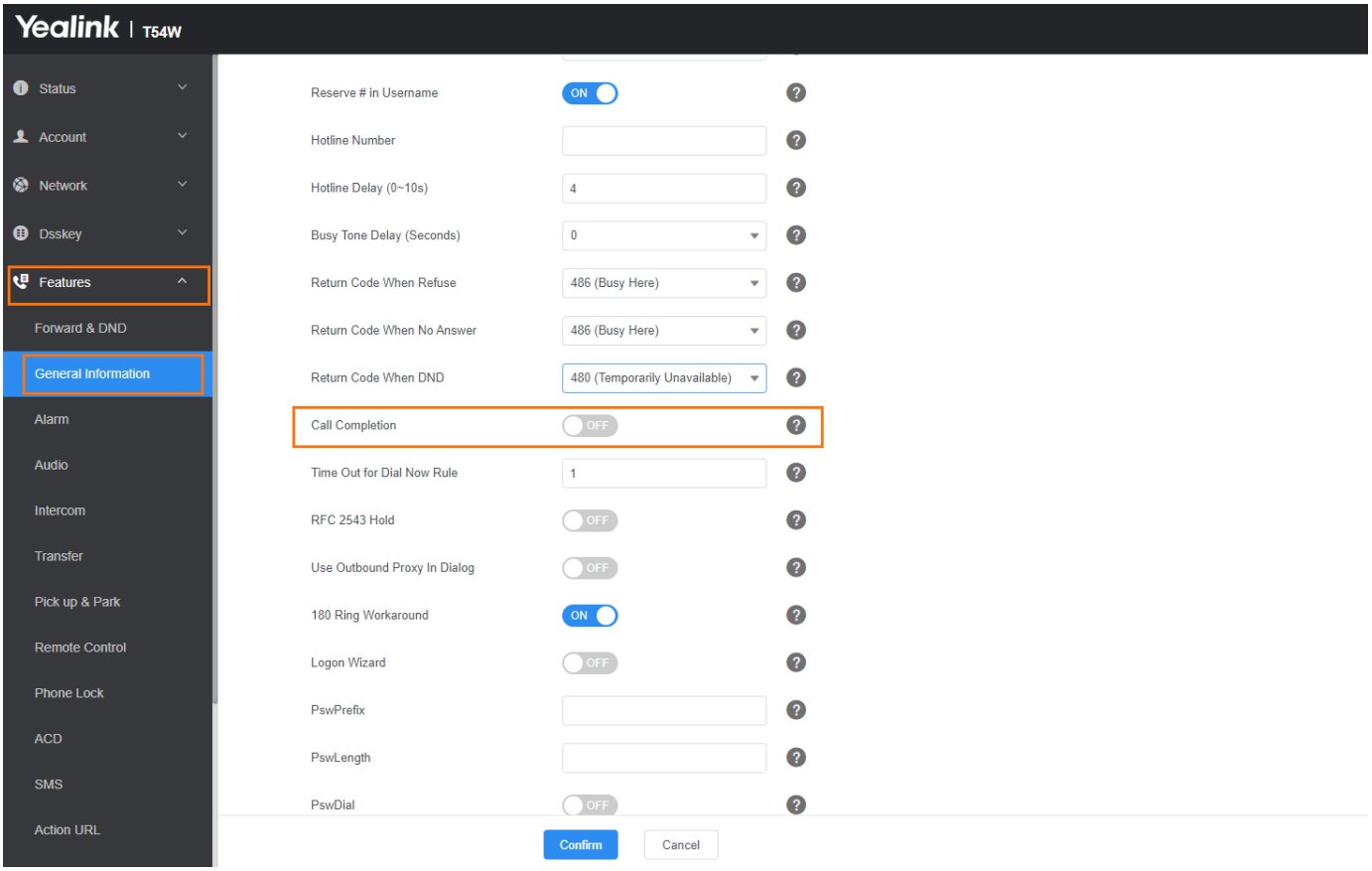
```
features.call_completion_enable
```

Parameter	Permitted Values	Defa ult	Description

features.call_completion_enable	0-Disabled 1-Enabled	0	It enables or disables the call completion feature.

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

Introduction

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 the 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.

Supported devices: All phones except T48G, T46G, T42G, T41P, T30P, T30, T29G, T19 E2, CP920, CP925 and CP935W.

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
sip.call_park_without_blf

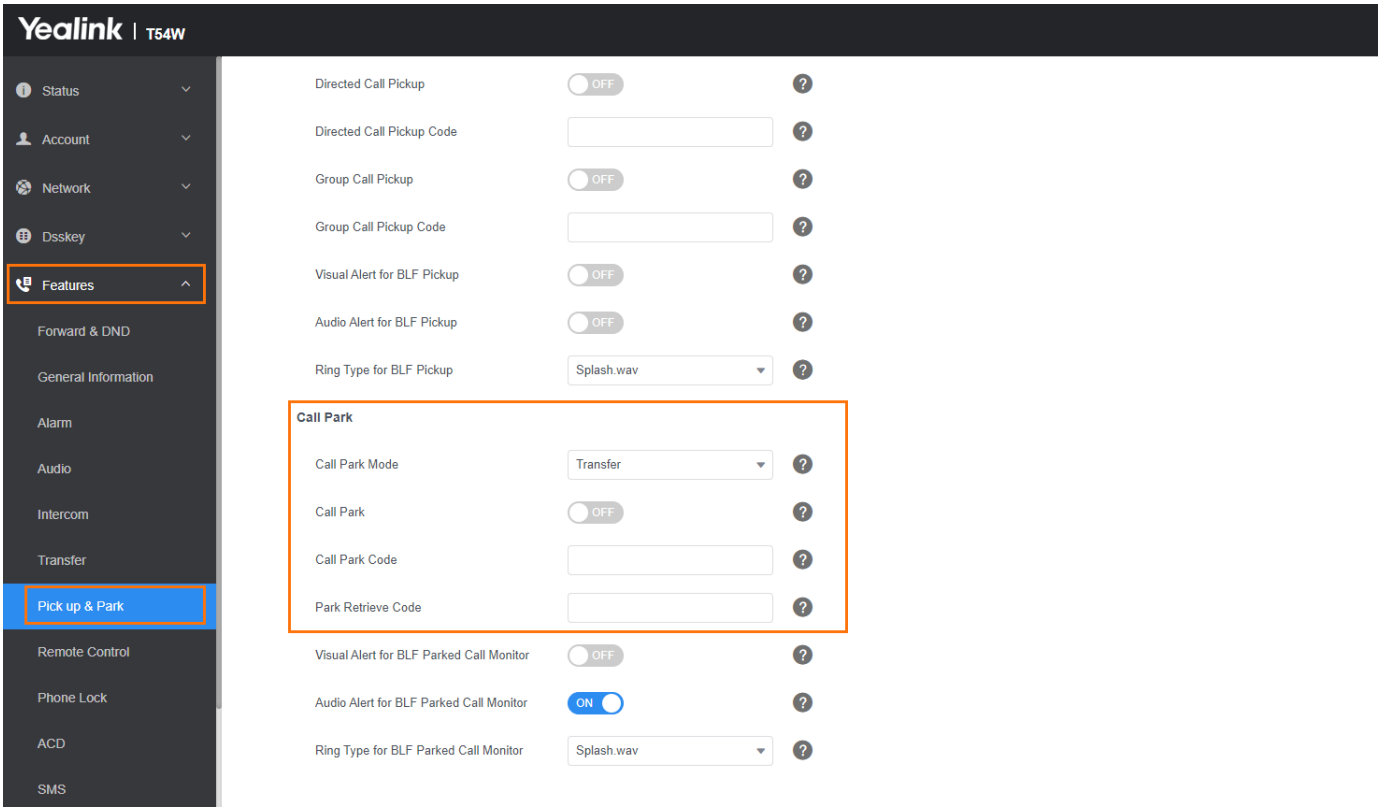
Parameter	Permitted Values	Default	Description
features.call_park.park_mode	**1**-FAC, park a call by dialing the call park code. **2**-Transfer, blind	2	It configures the call park mode.

	transfer the call to a shared parking lot.		
features.call_park.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the call park feature.
features.call_park.park_code	String within 256 characters	Blank	It configures the call park code for FAC call park mode or configures a shared parking lot for Transfer call park mode.
features.call_park.park_retrieve_code	String within 256 characters	Blank	It configures the park retrieve code for FAC call park mode or configures the retrieve parking lot for Transfer call park mode.
features.call_park.direct_send.enable	**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 press the BLF/BLF List or Speed Dial key to park the call to the specific extension or retrieve the call parked from the specific extension. **1**-Enabled	1	It enables or disables the phone to dial out the call park code/park retrieve code directly when pressing the Park/Retrieve soft key. 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.
features.call_park.line_restriction.enable	**0**-Disabled, the call is parked by the current line, which is in call state. **1**-Enabled	0	It enables or disables the phone to park a call using the specific line of the Call Park key. It works only if "features.call_park.park_mode" is set to 2 (Transfer).
features.call_park.performby_hold	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to park a call using the HOLD hard key.

hardkey.enable			
sip.call_park_without_blf	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to close the BLF monitoring feature for the call park DSS key.

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.

> You can set a line key as a Park key or a Retrieve key, specify an extension you want to park a call to for Park key and specify a parked extension you want to retrieve a parked call from for the Retrieve key. For more information, refer to Line Keys.

Example: Setting Call Park and Retrieve in Transfer Mode

The following example shows the configuration for the 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”.

> You can set a line key as a Park key or a Retrieve key, specify a shared parking lot you want to park a call to for Park key and specify a retrieve lot you want to retrieve a parked call from for the Retrieve key. For more information, refer to Line Keys.

FAQ

1. How to disable subscribes for Voice mail & Call park?

Automatic Call Distribution (ACD)

Introduction

ACD enables the use of phones in a call-center role by automatically distributing incoming calls to available users or agents. You can enable users to use their phone in a call center agent/a supervisor role on a supported call server.

The users can sign in and sign out of the ACD state as a call center agent using soft keys. The server distributes calls to the agent when the agent's state is available, and stops distributing calls when the agent changes state to unavailable. The IP phone remains in the unavailable status until the agent manually changes the IP phone status. You can configure how long the IP phone remains unavailable state and changes to available automatically on a supported call server.

It is not applicable to CP920/CP925/CP935W phones.

ACD Key Configuration

You can configure a DSS key as an ACD key to log into the ACD system. The ACD key on the IP phone indicates the ACD state.

The following shows the configuration for an ACD key.

linekey.X.type = 42

linekey.X.label = ACD

After provisioning, an ACD key is available on the phone, and you can press the ACD key to log into the ACD system.

ACD Configuration

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

Configuration parameter

account.X.acd.enable
account.X.acd.available
account.X.subscribe_acd_expires
features.homescreen_softkey.acd.enable
account.X.acd.unavailable_reason_enable
acd.enable
acd.auto_available_timer
phone_setting.idle_text.color

Parameter	Permitted Values	Default	Description
account.X.acd.enable[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the ACD feature.
account.X.acd.available[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to display the Available/Avail or Unavailable/Unavail soft key after the phone logs into the ACD system. It works only if "account.X.acd.enable" is set to 1 (Enabled).
account.X.subscribe_acd_expires[1]	Integer from 120 to 3600	3600	It configures the period (in seconds) of ACD subscription. It works only if "account.X.acd.enable" is set to 1 (Enabled).
features.homescreen_softkey.acd.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to display the ACD softkeys, such as Login or Logout on the idle screen. It works only if "account.X.acd.enable" is set to 1 (Enabled).
account.X.acd.unavailable_reason_enable[1]	**0**-Disabled **1**-Enabled, the unavailable/away reason of the agent state will be displayed on the phone screen (for example, on lunch, in the bathroom, taking a	0	It enables or disables the unavailable/away reason code feature. It works only if "account.X.acd.available" is set to 1 (Enabled).

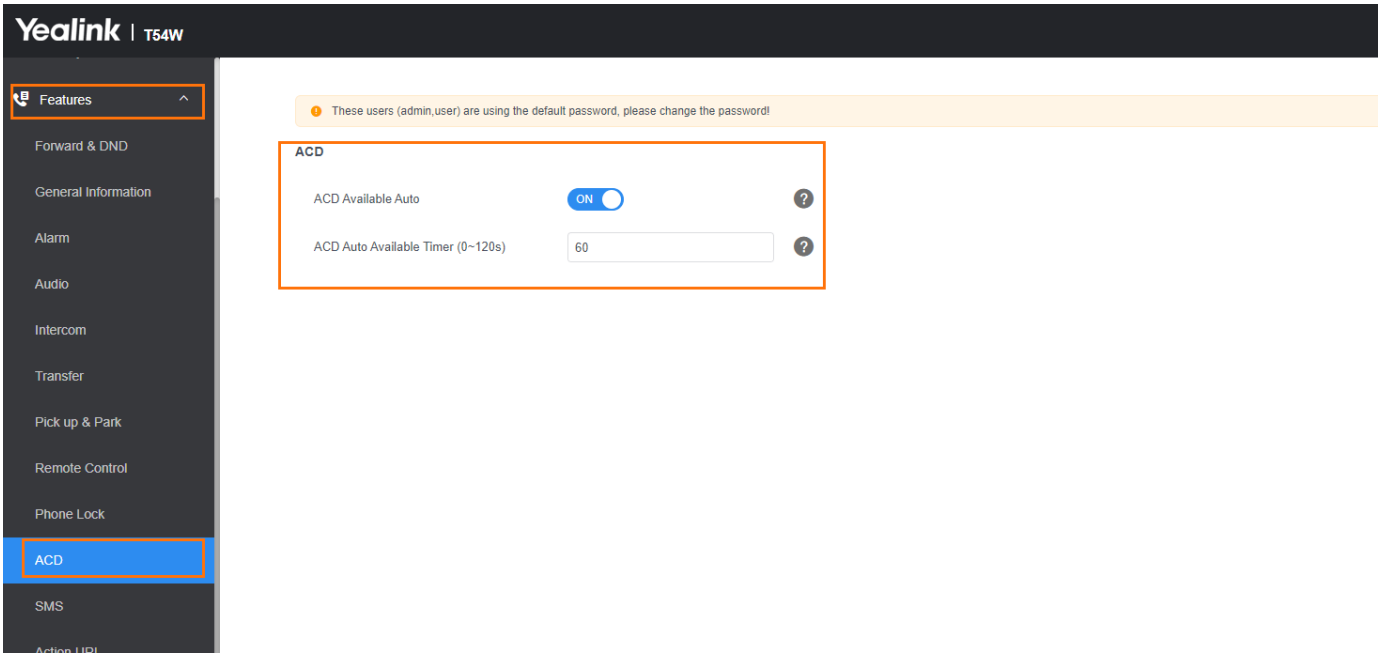
	coffee break, or a personal break).		
acd.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to automatically change the status of the ACD agent to available after the designated time. It works only if "account.X.acd.enable" is set to 1 (Enabled).
acd.auto_available_timer	Integer from 0 to 120	60	It configures the interval (in seconds) for the status of the ACD agent to be automatically changed to available. It works only if "account.X.acd.enable" and "acd.enable" are set to 1 (Enabled).
phone_setting.idle_text.color	**0**-White font color **1**-Black font color **2**-Default color for each model	2	It is used to configure the font color of the idle ACD Label for touch screen models. It works only if your firmware version is x.86.0.112 or later.
acd.available_fixed_display.enable	**0**-Disabled **1**-Enabled, the "Available" and "Unavailable" options will be fixed in the first Softkey position.	0	The "Unavailable" softkey will be consistently displayed as the first softkey. It will be shown as the first softkey when logged in and will be empty when logged out. This feature will only take effect on the Idle screen and requires the condition "account.X.acd.enable " to be enabled.

[1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T74U/T74W/

> T77U/T85W/T87W/T88W (Pro)/T88V Pro, X=1-16; for T53W/T53/T53C/T43U/T42G/T42U/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 E2, X=1-2; for T30P/T30/T19 E2/CP920/CP925/CP935W, X=1.

Set via the Web User Interface

On the web user interface, go to **Features** > **ACD** > **ACD.**



Example: Setting ACD

The following example shows the configuration for ACD.

Example:

```
######Set an ACD for account 1#######
account.1.acd.enable = 1
account.1.acd.available = 1
account.1.subscribe_acd_expires = 3000
acd.enable = 1
acd.auto_available_timer = 60
features.homescreen_softkey.acd.enable = 1
######Set an ACD key#############
linekey.1.type=42
linekey.1.label=ACD
After provisioning, you can press the Login soft key or ACD key to log into the ACD system.
After logging into the ACD system, the Available (Avail)/Unavailable (Unavail) soft key
appears on the phone screen. You can press the Available (Avail)/Unavailable (Unavail)
```

soft key to change the ACD state. The ACD key on the IP phone indicates the ACD state.

Busy Lamp Field

Busy Lamp Field

The Busy Lamp Field (BLF) feature enables the IP phone to monitor specific remote lines for state changes on the phone. It is not available on the T30P/T30/T19 E2/T19P E2/CP920 IP phone.

Yealink phones support two methods of BLF configuration:

- Configure a line key as a BLF key to monitor a specific remote line
- Configure the BLF List to monitor a list of specific remote lines

The BLF feature enables the following functions for the users:

- Monitor the status of the line on their phone
- Display caller ID information
- Answer incoming calls to the monitored line (called directed call pickup)
- Park and retrieve calls to the monitored line
- Initiate an outgoing intercom call to the monitored line
- Barging In an Active Call by BLF List Key
- Park the active call to the monitored users who are in the BLF list

BLF Key Configuration

You can configure a BLF key for a specific line.

The following shows the configuration of a BLF key for Bill.

linekey.X.type=16

linekey.X.line=1

linekey.X.value=1001

linekey.X.label=Bill

Related Topic

Line Keys Configuration

BLF List Configuration

You can configure a BLF List for a monitor phone. It enables the monitor phone to subscribe to a list of lines and receive status notifications of the monitored lines.

> The IP phone subscribes to a BLF list on the server. You must access the server and set up a list of monitored lines.

The following table lists the parameters to configure the BLF List.

Configuration parameter

account.X.blf.blf_list_uri
account.X.blf_list_code
account.X.blf_list_barge_in_code
account.X.blf_list_call_parked_code
account.X.blf_list_call_parked_list
account.X.blf_list_retrieve_call_parked_code
phone_setting.auto_blf_list_enable
phone_setting.blf_list_sequence_type
features.blf_list_version

Parameter	Permitted Values	Default	Description	Supported Devices
account.X.blf.blf_list_uri[1]	SIP URI within 256 characters	Blank	It configures the BLF List URI to monitor a list of users for account X. **Example**: account.1.blf.blf_list_uri = 4609@pbx.test.com	All phones except T30P, T30, T19 E2, T19P E2 and CP920
account.X.blf_list_code[1]	String within 32 characters	Blank	It configures the feature access code that initiates a directed call pickup for account X.	All phones except T30P, T30, T19 E2, T19P E2, and CP920
account.X.blf_list_barge_in_code[1]	String within 32 characters	Blank	It configures the feature access code of directed call pickup with barge-in for account X.	All phones except

				T30P, T30, T19 E2, T19P E2, and CP920
account.X.blf_list_call_parked_code[1]	String within 32 characters	Blank	It configures the feature access code of call park for account X.	All phones except T48G, T46G, T42G, T41P, T30P, T30, T29G, T19 E2, T19P E2, and CP920
account.X.blf_list_call_parked_list[1]	Blank all serial numbers of monitored users in the BLF list	Blank	It configures the serial numbers of the monitored users in the BLF list, where you can park the active call for account X. Multiple serial numbers are separated by commas. **Example**: account.1.blf_list_call_parked_list = When you leave it blank, you cannot park the active call to any monitored user. account.1.blf_list_call_parked_list = all You can park the active call to any monitored user. account.1.blf_list_call_parked_list = 1,3,4	All phones except T48G, T46G, T42G, T41P, T30P, T30, T29G, T19 E2, T19P E2 and CP920

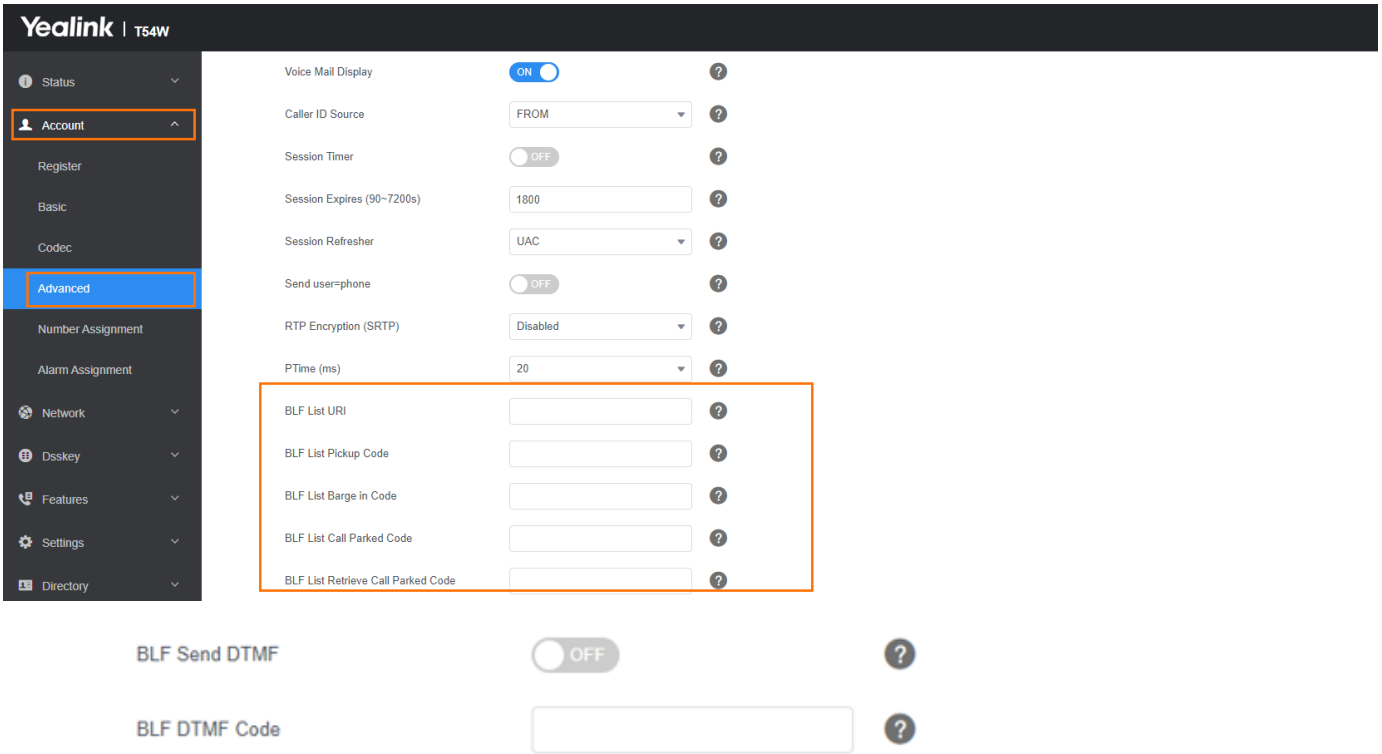
			You can park the active call to the first, third, or fourth monitored user in the BLF list. This parameter has a higher priority than "transfer.dsskey_deal_type", so that when you press the BLF list key during a call, the phone parks a call other than transferring the call. It works only if "account.X.blf_list_call_parked_code" is configured.	
account.X.blf_list_retrieve_call_parked_code[1]	String within 32 characters	Blank	It configures the feature access code that initiates the retrieval of a parked call on the monitored user.	All phones except T30P, T30, T19 E2, T19P E2 and CP920
phone_setting.auto_blf_list_enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to automatically configure the BLF list DSS keys in order.	All phones except T30P, T30, T19 E2, T19P E2 and CP920
phone_setting.blf_list_sequence_type	**0**-linekey > exp1 key > expN key **1**-exp1 key > expN key > linekey **2**-linekey page1 >	0	It configures the order of BLF list DSS keys assigned automatically. It works only if "phone_setting.auto_blf_list_enable" is set to 1	T57W, T54W, T53W, T53, T53C,

	page1 from exp1 key to expN key > page2 from exp1 key to expN key > ··· > linekey from page2 to page3 **3**-page1 from exp1 key to expN key > page2 from exp1 key to expN key > ··· > linekey N is the number of your connected expansion modules.		(Enabled). To assign Ext Key, make sure the expansion module has been connected to the phone in advance.	T48U, T48S, T48G, T46U, T46S, T46G, T43U, T29G, T27G, T58W, T58A, VP59, T56A, T58V, T7X, T8X
features.blf_list_version[2]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to include the Version header in the BLF list NOTIFY message sent by the server.	All phones except T30P, T30, T19 E2, T19P E2 and CP920
account.x.blf_send_dtmf.enable	**0**-Disabled **1**-Enabled	0	It is used to configure whether to enable the function of sending DTMF when pressing the BLF key.	x.86.0.112（x is common number）
account.x.blf_dtmf_code	String	Blank	It is used to configure the DTMF code sent when pressing the BLF key.	x.86.0.112（x is common number）

> [1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T58W/T58A/VP59/T56A/T58V/T74U/T74W/T77U/T8X, X=1-16; for T53W/T53/T53C/T43U/T42U/T42G/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 E2, X=1-2; for CP925/CP935W/CP960/CP965, X=1.
> [2]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 **Account** > **Advanced** > **BLF List URI/BLF List Call Parked Code/BLF List Pickup Code/BLF List Barge in Code/BLF List Retrieve Call Parked Code/BLF Send DTMF/BLF DTMF Code.**



> Starting from version x.86.0.112 of T3X/T4X/T5X, there has been an optimization in the display logic of the BLF list. If the BLF list does not receive any content pushed by the server, it will be displayed as empty instead of showing an icon. For example, if you have set Linekey 1-5 as BLF list type, but your server only has configurations for four BLF accounts, Linekey 5 will not display the BLF list icon, while the first four Linekeys will be displayed normally.

State Indicator of Remote Line

The state indicator of the monitored line on the BLF/BLF List key varies by phone models. For more information, refer to State Indicator of Remote Line by BLF Key.

BLF/BLF List Subscription

Yealink phones support BLF using a SUBSCRIBE/NOTIFY mechanism as specified in RFC 3265.

BLF Subscription

When you configure the IP phone to monitor a specific line, the phone sends a SUBSCRIBE request with Request-URI containing the monitor line URI to the server, and then receives a NOTIFY request. The NOTIFY message contains an XML body with the status of the specific monitored line.

The following example shows a NOTIFY message for a BLF line “012”:

```
<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="1" state="full"
entity="sip:012@10.20.10.42:5060">
<dialog id="0000" > <state > terminated</state > </dialog >
</dialog-info>
```

BLF List Subscription

When you configure the IP phone to monitor a list of specific remote lines, the phone sends a SUBSCRIBE request with Request-URI containing the BLF List URI, and then receives a NOTIFY request. The NOTIFY message contains an XML body with the status of each monitor line.

The following example shows a NOTIFY message for a BLF List, the BLF List contains 4605 and 4607:

```
<?xml version="1.0" <?xml version="1.0"?>
<list xmlns="urn:ietf:params:xml:ns:rlmi" xmlns="urn:ietf:params:xml:ns:rlmi"
version="0" fullState="true">
<resource uri="sip:4605@pbx.yealink.com">
<name > 4605 Yealink</name>
<instance id="JQZxud2qeo" state="active" cid="8y35ri@broadworks"/>
</resource>
<resource uri="sip:4605@pbx.yealink.com">
<name > 4607 Yealink</name>
<instance id="pXHQ97tPyQ" state="active" cid="tYzwJM@broadworks"/>
</resource>
</list>
```

BLF/BLF List Subscription Configuration

The following table lists the parameters you can use to configure the BLF/BLF List subscription.

Configuration parameter

```
account.X.blf.subscribe_period
```

account.X.blf.subscribe_event
account.X.out_dialog_blf_enable
account.X.blf.match_host.enable
sip.terminate_notify_sub_delay_time
sip.sub_refresh_random

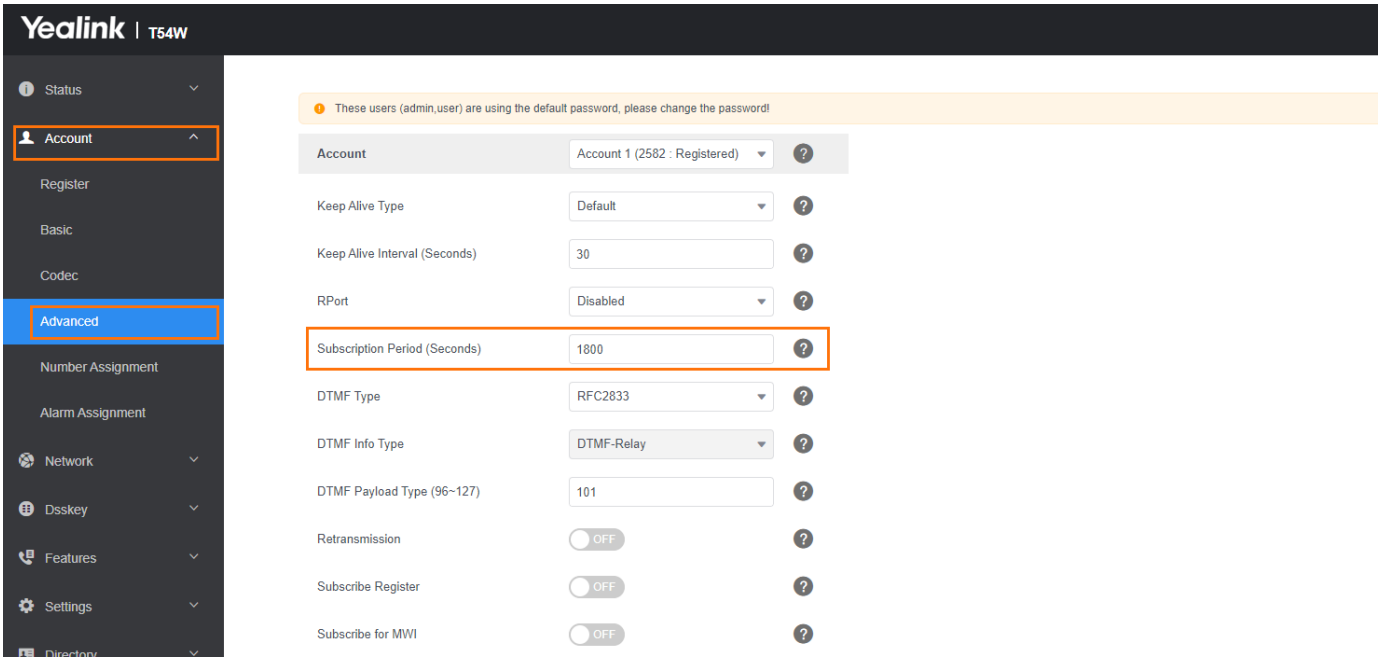
Parameter	Permitted Values	Default	Description	Supported Devices
account.X.blf.subscribe_period[1]	Integer from 30 to 2147483647	1800	It configures the period (in seconds) of the BLF subscription.	All phones except T30P, T30, T19 E2, T19P E2 and CP920
account.X.blf.subscribe_event[1]	0-dialog 1-presence	0	It configures the event of the BLF subscription.	All phones except T30P, T30, T19 E2, T19P E2 and CP920
account.X.out_dialog_blf_enable[1]	0-Disabled 1-Enabled	0	It enables or disables the phone to handle NOTIFY messages out of the BLF dialog.	All phones except T30P, T30, T19 E2, T19P E2 and CP920
account.X.blf.match_host.enable[1]	0-Disabled 1-Enabled, the phone can only recognize the NOTIFY message whose host field is the same as the one in the SUBSCRIBE message.	0	It enables or disables the host match feature for the BLF/BLF list feature.	All phones except T30P, T30, T19 E2, T19P E2 and CP920
sip.terminate_notify_sub_delay_time	Integer greater than 0	0	It configures the interval (in seconds) for the phone to resubscribe when it receives the NOTIFY message with the subscription state of Terminated.	All phones except T30P, T30, T19 E2, T19P E2 and CP920

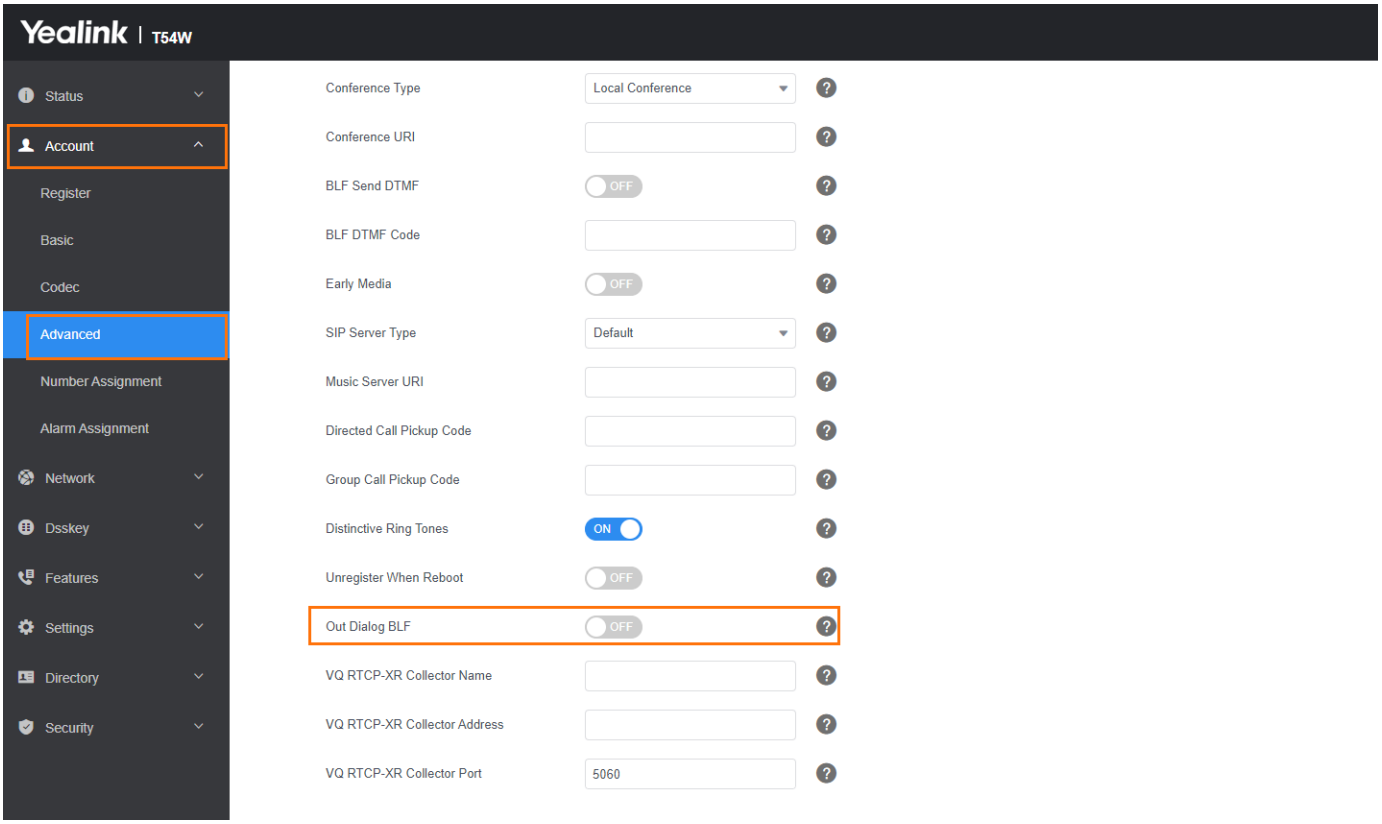
			If it is set to 0, the phone will resubscribe immediately.	
sip.sub_refresh_random	0-Disabled 1-Enabled, the phone will generate a random value. The final renewal time is equal to the original renewal time plus the random value.	0	It enables or disables the phone from using the random renewal mechanism. It works only if "account.X.subscribe_expires_overlap" is set to 0 (Disabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920

> [1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T58W/T58A/VP59/T56A/T58V/T74U/T74W/T77U/T8X, X=1-16; for T53W/T53/T53C/T43U/T42U/T42G/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 E2/T21P E2, X=1-2; for CP925/CP935W/CP960/CP965, X=1.

Set via the Web User Interface

On the web user interface, go to **Account** > **Advanced** > **Subscription Period (Seconds).** Or go to **Account** > **Advanced** > **Out Dialog BLF**





Visual and Audio Alert for Monitor Lines

The Visual and Audio Alert feature allows the phone to display the caller ID and play an audio alert when a BLF line receives an incoming call.

You can configure how the phone displays the caller ID and set a distinctive alert tone for multiple BLF lines.

Visual and Audio Alert for BLF Lines Configuration

The following table lists the parameters you can use to configure a visual and audio alert for BLF lines.

Configuration parameter

features.pickup.blf_visual_enable
features.pickup.blf_visual.list
features.pickup.blf_audio_enable
features.pickup.blf_audio.list
features.blf.ring_type
features.pickup_display.method
features.blf_pickup_only_send_code

Parameter	Permitted Values	Default	Description	Supported Devices

features.pickup.blf_visual_enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to display a visual alert when the monitored user receives an incoming call.	All phones except T30P, T30, T19 E2, T19P E2 and CP920
features.pickup.blf_visual.list	any Monitored phone number ListX[1]	any	It configures the monitored users who want to enable the visual alert for the BLF pickup feature. Multiple monitored users are separated by commas. Example: features.pickup.blf_visual.list = any or leave it blank The phone displays a visual alert when any monitored user receives an incoming call. features.pickup.blf_visual.list = 4604,4605 The phone displays a visual alert when monitored user 4604 or 4605 receives an incoming call. features.pickup.blf_visual.list = List1 The phone displays a visual alert when any user in List 1 receives an incoming call. ListX stands for the BLF list of account X configured by the parameter "account.X.blf.blf_list_uri". It works only if "features.pickup.blf_visual_enable" is set to 1 (Enabled).	All phones except T48G, T46G, T42G, T41P, T30P, T30, T29G, T19 E2, T19P E2 and CP920
features.pickup.blf_audio_e	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to play an audio alert when the monitored user receives an incoming call.	All phones except T30P,

nable				T30, T19 E2, T19P E2 and CP920
features .pickup. blf_audi o.list	any Monitored phone number ListX[1]	any	It configures the monitored users who want to enable the audio alert for the BLF pickup feature. Multiple monitored users are separated by commas. Example: features.pickup.blf_audio.list = any or leave it blank The IP phone plays an audio alert when any monitored user receives an incoming call. features.pickup.blf_audio.list = 4604,4605 The IP phone plays an audio alert when the monitored user 4604 or 4605 receives an incoming call. features.pickup.blf_audio.list = List1 The IP phone plays an audio alert when any user in List 1 receives an incoming call. ListX stands for the BLF list of account X configured by the parameter "account.X.blf.blf_list_uri". It works only if "features.pickup.blf_audio_enable" is set to 1 (Enabled).	All phones except T48G, T46G, T42G, T41P, T30P, T30, T29G, T19 E2, T19P E2 and CP920
features .blf.rin g_type	Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav,	Spl ash .wa v	It configures an alert tone to play when a monitored line rings. It works only if "features.pickup.blf_audio_enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2, CP920,

	Silent.wav, Splash.wav or custom ring tone name (for example, Config:Customring.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)			CP925 and CP935W
features.pickup_display.method	**0**-Name **1**-Number **2**-Name Number **3**-Number Name	0	It configures the display method of the call party information on the visual prompt. It works only if "features.pickup.blf_visual_enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920
features.blf_pickup_only_send_code	**0**-Disabled, the phone dials out the feature access code of the directed pick-up plus monitored number when performing BLF/BLF list pickup. **1**-Enabled	0	It enables or disables the phone to only dial out feature access code of directed pick up when performing BLF/BLF list pickup.	All phones except T30P, T30, T19 E2, T19P E2 and CP920

> [1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T58W/T58A/VP59/T56A/T58V/T74U/T74W/T77U/T8X, X=1-16; for T53W/T53/T53C/T43U/T42U/T42G/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 E2, X=1-2; for CP925/CP935W/CP960/CP965, X=1.

Example: Configuring Visual and Audio Alert for Monitor Lines

The following example shows the configuration for visual and audio for a monitor line.

Scenario Conditions	Related Topic
linekey.1.extension = 97 or account.1.direct_pickup_code = *97 or features.pickup.direct_pickup_code = *97	Line Keys Configuration Directed Call Pickup
linekey.1.type = 16 linekey.1.line = 1 linekey.1.value = 1001 linekey.1.label = Bill	BLF Key Configuration

Example:

features.pickup.blf_visual_enable = 1

features.pickup.blf_audio_enable = 1

When the monitored line receives an incoming call, the phone screen shows an incoming call to the monitored line(for example, “6001<-6002”, 6001 is the monitored extension that receives an incoming call from 6002) (from 1008 to 1001), the following occurs on the phone:

- The phone plays a specific alert tone.
- The BLF key LED flashes red. On the T57W/T48U/T48S/T48G IP phone, the icon/flashes.
- The caller ID appears on the phone screen.

The following shows a visual alert for the monitor line on T46S/G phones:

You can pick up the call to the monitored line, place a call to the monitored line, place a new call, or go back to the idle screen.

BLF Floating Notification

In idle status, the phone can display a BLF floating window at the top, showing BLF functions after Dsskey11.

BLF Floating Notification Configuration

The following table lists the parameters to disable or enable the BLF floating notifications.

features.dsskey_float_notification.enable

Parameter	Permitted Values	Default	Description	Supported Devices
features.dsskey_float_notification.enable	0-Disabled 1-Enabled	1	It configures to disable or enable the BLF floating notifications.	T77U/T87W/T88W/T88W Pro/T88V Pro

LED Mode for BLF/BLF List Key

BLF LED Mode provides five kinds of definitions for the BLF/BLF List key LED status. As there is no hard line key on T57W/T48U/T48S/T48G phones, BLF LED mode configuration is applicable to any phones and expansion module, except T57W/T48U/T48S/T48G/T30P/T30/T19 E2/T19P E2/CP920/CP925/CP935W phones and Video Phones, Conference Phones.

Supported BLF LED Modes

The following table lists the LED statuses of the BLF/BLF list key when BLF LED Mode is set to 0, 1, 2, 3, or 4, respectively. The default value of BLF LED mode is 0.

Line key/Expansion Module Key LED (configured as a BLF key or a BLF List ke,y and BLF LED Mode is set to 0)

LED Status	Description
Solid green	The monitored user is idle.
Fast-flashing red (200ms)	The monitored user receives an incoming call.
Solid red	The monitored user is dialing.The monitored user is talking. The monitored user’ s conversation is placed on hold (This LED status requires server support).
Slowly-flashing red (1s)	The call is parked against the monitored user’ s phone number.
Off	The monitored user does not exist.

Line Key/Expansion Module Key LED (configured as a BLF key or a BLF List key, and BLF LED Mode is set to 1)

LED Status	Description
Fast-flashing red (200ms)	The monitored user receives an incoming call.
Solid red	The monitored user is dialing. The monitored user is talking. The monitored user’ s conversation is placed on hold (This LED status requires server support).
Slowly-flashing red (1s)	The call is parked against the monitored user’ s phone number.
Off	The monitored user is idle. The monitored user does not exist.

Line Key/Expansion Module Key LED (configured as a BLF key or a BLF List key and BLF LED Mode is set to 2)

LED Status	Description
Fast-flashing red (200ms)	The monitored user receives an incoming call.

Solid red	The monitored user is dialing. The monitored user is talking. The monitored user’ s conversation is placed on hold (This LED status requires server support).
Slowly-flashing red (1s)	The call is parked against the monitored user’ s phone number.
Off	The monitored user is idle. The monitored user does not exist.

Line Key/Expansion Module Key LED (configured as a BLF key or a BLF List key, and BLF LED Mode is set to 3)

LED Status	Description
Fast-flashing green (200ms)	The monitored user receives an incoming call
Solid red	The monitored user is dialing. The monitored user is talking. The monitored user’ s conversation is placed on hold (This LED status requires server support).
Slowly-flashing red (1s)	The call is parked against the monitored user’ s phone number.
Off	The monitored user is idle. The monitored user does not exist.

Line Key/Expansion Module Key LED (configured as a BLF key or a BLF List key, and BLF LED Mode is set to 4. This mode is specifically designed for the Ribbon server.)

LED Status	Description
Solid green	The monitored user is talking.
Slowly-flashing green (1s)	The monitored user does not exist.
Off	The monitored user is idle.

BLF LED Mode Configuration

The following table lists the parameters you can use to configure BLF LED Mode.

Configuration parameter

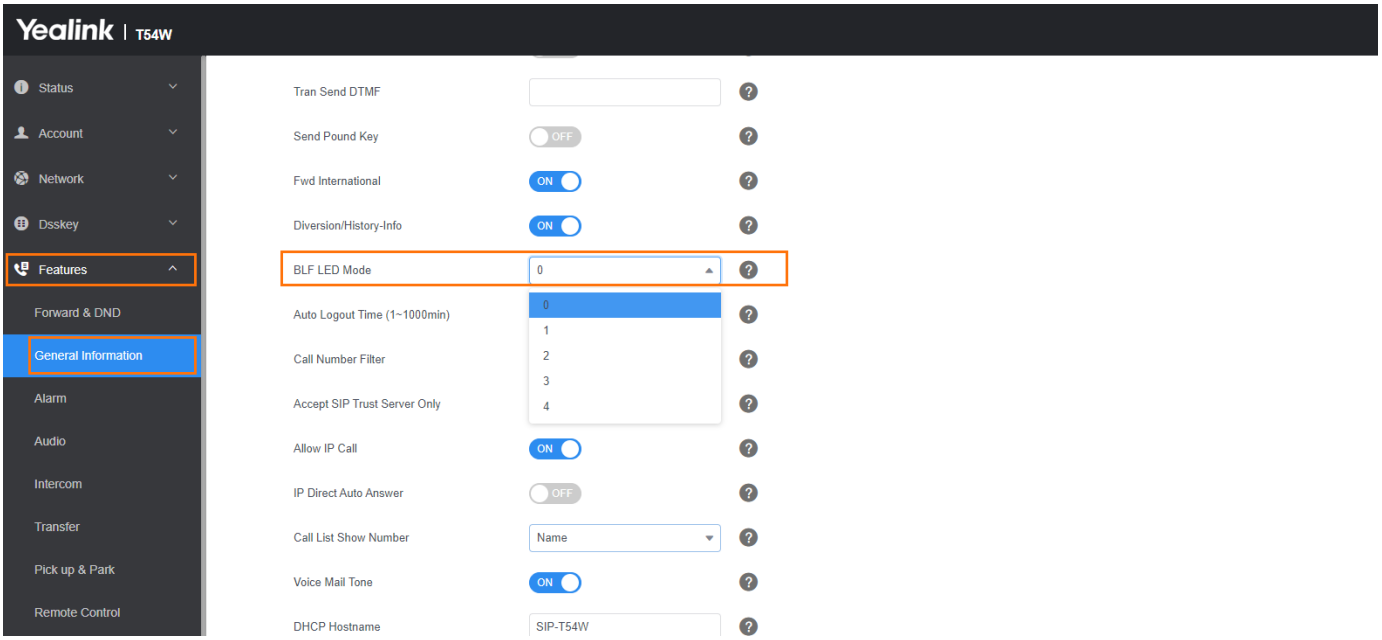
features.blf_led_mode

Parame	Permitted Values	Def	Description	Supported Devices

ter		aul t		
features.blf_led_mode	0,1,2,3,4 (4 is specifically designed for the Ribbon server)	0	It configures the BLF LED mode.	All phones except T30P, T30, T19 E2, T19P E2, CP920, CP925, CP935W, CP960, CP965

Set via the Web User Interface

On the web user interface, go to **Features** > **General Information** > **BLF LED Mode.**



BLF/BLF List Key LED Status and Behavior Configuration

You can customize the BLF LED status (or the color of BLF icon for T57W/T48U/T48S/T48G phones) and BLF/BLF List key behavior using the EDK macros if required.

This feature depends on support from a SIP server.

> For more information on EDK macros, refer to Macro Action Strings.

Supported BLF/BLF List Key Behaviors

The following behaviors are supported when pressing the BLF/BLF List keys:

- newcall - dial the phone number
- btransfer - transfer the active call to the monitored user without consulting
- ctransfer - transfer the active call to the monitored user with prior consultation
- pickup - pick up the call directly
- bargein - barge in and set up a conference call

- custom EDK macros (for example, 1234$Tinvite$) - execute a series of macro action strings
- intercom - place an intercom call to the monitored number
- park - park the call to the monitored user, it works only when configuring "blf.enhanced.idle.talking.action"
- retrieve - retrieve a call from the monitored user, it works only when configuring "blf.enhanced.parked.callin.action", “blf.enhanced.parked.talking.action”, and "blf.enhanced.parked.idle.action"

BLF Key LED/Icon and Behavior for Idle State Configuration

The following table lists the parameters you can use to configure the BLF key LED/icon and Behavior for the idle state (the monitored user is idle).

Configuration parameter

```
blf.enhanced.idle.enable
blf.enhanced.idle.led
blf.enhanced.idle.callin.action
blf.enhanced.idle.talking.action
blf.enhanced.idle.idle.action
```

Parameter	Permitted Values	Defaul t	Description	Support ed Devices
blf.enhance d.idle.enab le	0-Disabled 1-Enabled, the phone will display the custom BLF/ BLF List DSS key LED status/icon colors and perform the custom behavior when pressing the BLF/ BLF List DSS key.	0	It enables or disables the custom configuration when the monitored user is idle.	All phones except T30P, T30, T19 E2, T19P E2 and CP920
blf.enhance d.idle.led	String	Blank	It configures the custom BLF/BLF List DSS key LED status/icon colors when	All phones

			the monitored user is idle. This value uses the same macro action string syntax as an Enhanced DSS key. Example: blf.enhanced.idle.led =$LEDg1000o$ For T57W/T48U/T48S/T48G phones, the BLF/BLF List DSS key field displays a green icon for 1000ms and then turns to white. For other phones, the BLF/BLF list DSS key LED glows green for 1000ms and then goes out. It works only if "blf.enhanced.idle.enable" is set to 1 (Enabled).	except T30P, T30, T19 E2, T19P E2 and CP920
blf.enhanced.idle.callin.action	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor is ringing and monitored user is idle. It works only if "blf.enhanced.idle.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920
blf.enhanced.idle.talking.action	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor is talking and the monitored user is idle. It works only if "blf.enhanced.idle.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920
blf.enhanced.idle.idle.action	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor and monitored user are	All phones except

			idle. It works only if "blf.enhanced.idle.enable" is set to 1 (Enabled).	T30P, T30, T19 E2, T19P E2 and CP920

BLF Key LED/Icon and Behavior for Call-in State Configuration

The following table lists the parameters you can use to configure the BLF key LED/icon and Behavior for the call-in state (the monitored user is ringing).

Configuration parameter

```
blf.enhanced.callin.enable
blf.enhanced.callin.led
blf.enhanced.callin.callin.action
blf.enhanced.callin.talking.action
blf.enhanced.callin.idle.action
```

Parameter	Permitted Values	Default	Description	Supported Devices
blf.enhanced.callin.enable	0-Disabled 1-Enabled, the phone will display the custom BLF/BLF List DSS key LED status/ icon colors and	0	It enables or disables the custom configuration when the monitored user is ringing.	All phones except T30P, T30, T19 E2, T19P E2 and CP920

	perform the custom behavior when pressing the BLF/ BLF List DSS key.			
blf.enhanced.callin.led	String	Blank	It configures the custom BLF/BLF List DSS key LED status/icon colors when the monitored user is ringing. This value uses the same macro action string syntax as an Enhanced DSS key. Example: blf.enhanced.callin.led =$LEDg1000o$ For T57W/T48U/T48S/T48G phones, the BLF/BLF List DSS key field displays a green icon for 1000ms and then turns to white. For other phones, the BLF/BLF list DSS key LED glows green for 1000ms and then goes out. It works only if "blf.enhanced.callin.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920
blf.enhanced.callin.callin.action	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor and monitored user are ringing. It works only if "blf.enhanced.callin.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920
blf.enhanced.callin.talkin	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor is	All phones except T30P,

g.action			talking and monitored user is ringing. It works only if "blf.enhanced.callin.enable" is set to 1 (Enabled).	T30, T19 E2, T19P E2 and CP920
blf.enhanced.callin.idle.action	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor is idle and the monitored user is ringing. It works only if "blf.enhanced.callin.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920

BLF Key LED/Icon and Behavior for Call-out State Configuration

The following table lists the parameters you can use to configure the BLF key LED/icon and Behavior for the call-out state (the monitored user is calling out).

Configuration parameter

```
blf.enhanced.callout.enable
blf.enhanced.callout.led
blf.enhanced.callout.callin.action
blf.enhanced.callout.talking.action
blf.enhanced.callout.idle.action
```

Parameter	Permitted Values	Default	Description	Supported Devices
blf.enhanced.callout.enable	0-Disabled 1-Enabled, the phone will display the custom BLF/BLF List DSS key LED status/icon colors and perform the	0	It enables or disables the custom configuration when the monitored user is calling out.	All phones except T30P, T30, T19 E2, T19P E2 and

	custom behavior when pressing the BLF/BLF List DSS key.			CP920
blf.enhanced.callout.led	String	Blank	It configures the custom BLF/BLF List DSS key LED status/icon colors when the monitored user is calling out. This value uses the same macro action string syntax as an Enhanced DSS key. Example: blf.enhanced.callout.led = $LEDg1000o$ For T57W/T48U/T48S/T48G phones, the BLF/BLF List DSS key field displays a green icon for 1000ms and then turns to white. For other phones, the BLF/BLF list DSS key LED glows green for 1000ms and then goes out. It works only if "blf.enhanced.callout.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920
blf.enhanced.callout.callin.action	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor is ringing and the monitored user is calling out. It works only if "blf.enhanced.callout.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920
blf.enhanced.callout.talking.action	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor is talking and the monitored user is calling out.	All phones except T30P, T30,

			It works only if "blf.enhanced.callout.enable" is set to 1 (Enabled).	T19 E2, T19P E2 and CP920
blf.enhanced.callout.idle.action	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor is idle and the monitored user is calling out. It works only if "blf.enhanced.callout.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920

BLF Key LED/Icon and Behavior for Talking State Configuration

The following table lists the parameters you can use to configure the BLF key LED/icon and Behavior for the talking state (the monitored user is talking).

Configuration parameter

```
blf.enhanced.talking.enable
blf.enhanced.talking.led
blf.enhanced.talking.callin.action
blf.enhanced.talking.talking.action
blf.enhanced.talking.idle.action
```

Parameter	Permitted Values	Default	Description	Supported Devices
blf.enhanced.talking.enable	0-Disabled 1-Enabled, the phone will display the custom BLF/BLF List DSS key LED status/icon colors and perform the custom behavior when pressing the BLF/BLF List DSS key.	0	It enables or disables the custom configuration when the monitored user is talking.	All phones except T30P, T30, T19 E2, T19P E2 and CP920

blf.enhanced.talking.led	String	Blank	It configures the custom BLF/BLF List DSS key LED status/icon colors when the monitored user is talking. This value uses the same macro action string syntax as an Enhanced DSS key. Example: blf.enhanced.talking.led = $LEDg1000o$ For T57W/T48U/T48S/T48G phones, the BLF/BLF List DSS key field displays a green icon for 1000ms and then turns to white. For other phones, the BLF/BLF list DSS key LED glows green for 1000ms and then goes out. It works only if "blf.enhanced.talking.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920
blf.enhanced.talking.callin.action	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor is ringing and the monitored user is talking. It works only if "blf.enhanced.talking.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920
blf.enhanced.talking.talking.ac	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor and	All phones except T30P, T30, T19 E2,

tion			monitored user are talking. It works only if "blf.enhanced.talking.enable" is set to 1 (Enabled).	T19P E2 and CP920
blf.enhanced.talking.idle.action	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor is idle and the monitored user is talking. It works only if "blf.enhanced.talking.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920

BLF Key LED/Icon and Behavior for Parked-Against State Configuration

The following table lists the parameters you can use to configure the BLF key LED/icon and Behavior for the parked-against state (a call is being parked against the monitored phone).

Configuration parameter

```
blf.enhanced.parked.enable
blf.enhanced.parked.led
blf.enhanced.parked.callin.action
blf.enhanced.parked.talking.action
blf.enhanced.parked.idle.action
```

Parameter	Permitted Values	Default	Description	Supported Devices
blf.enhanced.parked.enable	0-Disabled 1-Enabled, the phone will display the	0	It enables or disables the custom configuration when a call is parked against the monitored phone.	All phones except T30P,

	custom BLF/BLF List DSS key LED status/icon colors and perform the custom behavior when pressing the BLF/BLF List DSS key.			T30, T19 E2, T19P E2 and CP920
blf.enhanced.parked.led	String	Blank	It configures the custom BLF/BLF List DSS key LED status/icon colors when a call is parked against the monitored phone. This value uses the same macro action string syntax as an Enhanced DSS key. Example: blf.enhanced.parked.led =$LEDg1000o$ For T57W/T48U/T48S/T48G phones, the BLF/BLF List DSS key field displays a green icon for 1000ms and then turns to white. For other phones, the BLF/BLF list DSS key LED glows green for 1000ms and then goes out. It works only if "blf.enhanced.parked.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920
blf.enhanced.parked.callin.action	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor is ringing and a call is parked against the monitored phone.	All phones except T30P, T30, T19

			It works only if "blf.enhanced.parked.enable" is set to 1 (Enabled).	E2, T19P E2 and CP920
blf.enhanced.parked.talking.action	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor is talking and a call is parked against the monitored phone. This value uses the same macro action string syntax as an Enhanced DSS key. **Example**: blf.enhanced.parked.talking.action = newcall It works only if "blf.enhanced.parked.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920
blf.enhanced.parked.idle.action	String	Blank	It configures the behavior when pressing the BLF/BLF list DSS key if the monitor is idle and a call is parked against the monitored phone. This value uses the same macro action string syntax as an Enhanced DSS key. **Example**: blf.enhanced.parked.idle.action = newcall It works only if "blf.enhanced.parked.enable" is set to 1 (Enabled).	All phones except T30P, T30, T19 E2, T19P E2 and CP920

BLF Key LED/Icon and Behavior for Hold State Configuration

The following table lists the parameters you can use to configure the BLF key LED/icon and Behavior for the hold state (the call on the monitored phone is placed on hold).

Configuration parameter

```
blf.enhanced.hold.enable
blf.enhanced.hold.led
```

Parameter	Permitted Values	Default	Description	Supported Devices
blf.enhanced.hold.enable	0-Disabled 1-Enabled, the phone will display the custom BLF/BLF List DSS key LED status/icon colors.	0	It enables or disables the custom configuration when the call on the monitored phone is placed on hold.	All phones except T48G, T46G, T42G, T41P, T30P, T30, T29G, T19 E2, T19P E2 and CP920
blf.enhanced.hold.led	String	Blank	It configures the custom BLF/BLF List DSS key LED status/icon colors when the call on the monitored phone is placed on hold. This value uses the same macro action string syntax as an Enhanced DSS key. **Example**: blf.enhanced.hold.led =$LEDg1000o$ For T57W/T48U/T48S phones, the BLF/BLF List DSS key field displays a green icon for 1000ms and then turns to white. For other phones, the BLF/BLF list DSS key LED glows green for 1000ms and then goes out.	All phones except T48G, T46G, T42G, T41P, T30P, T30, T29G, T19 E2, T19P E2 and CP920

			It works only if "blf.enhanced.hold.enable" is set to 1 (Enabled).	

BLF Key LED/Icon and Behavior for DND State Configuration

The following table lists the parameters you can use to configure the BLF key LED/icon and Behavior for the DND state (DND is activated on the monitored phone).

Configuration parameter

```
blf.enhanced.dnd.enable
blf.enhanced.dnd.led
```

Parameter	Permitted Values	Default	Description	Supported Devices
blf.enhanced.dnd.enable	0-Disabled 1-Enabled, the phone will display the custom BLF/ BLF List DSS key LED status/ icon colors.	0	It enables or disables the custom configuration when DND is activated on the monitored phone.	All phones except T48G, T46G, T42G, T41P, T30P, T30, T29G, T19 E2, T19P E2 and CP920
blf.enhanced.dnd.led	String	Blank	It configures the custom BLF/BLF List DSS key LED status/icon colors when DND is activated on the monitored phone. This value uses the same macro action string syntax as an Enhanced DSS key. Example: blf.enhanced.dnd.led =$LEDrd1000o100yd300$ For T57W/T48U/T48S phones, an	All phones except T48G, T46G, T42G, T41P, T30P, T30, T29G, T19 E2, T19P E2 and CP920

			infinite loop for the BLF/BLF List DSS key field: displays a red icon for 1000ms, turns to white for 100ms and then displays a yellow icon for 300ms. For other phones, an infinite loop for the BLF/BLF list DSS key LED status: glows red for 1000ms, be in the off state for 100ms and then glows yellow for 300ms. It works only if "blf.enhanced.dnd.enable" is set to 1 (Enabled).	

BLF Key for Intercom Configuration

The BLF key (not including the BLF List key) can also be used to initiate an intercom call.

The following table lists the parameters you can use to configure the BLF key for Intercom.

Configuration parameter

features.blf.intercom_mode.enable

Parameter	Permitted Values	Default	Description	Supported Devices
features.blf.intercom_mode.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to initiate an outgoing intercom call with a monitored user when pressing the BLF key. To use this feature, you also need to configure the intercom mode (configured by the parameter "features.intercom.mode").	All phones except T30P, T30, T19 E2, T19P E2 and CP920

Call Information Display Configuration

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

Configuration parameter

features.blf.show_callinfo.enable

Parameter	Permitted Values	Default	Description	Supported Devices
features.blf.show_callinfo.enable	0-Disabled 1-Enabled, when the monitored line is ringing, during a call, or has a parked call, users can long-press the BLF/BLF List key to view the call information, and then select to pick up the incoming call (only for BLF/BLF List key), barge in a conference (only for BLF/BLF List key), or retrieve the parked call.	0	It enables or disables the phone to display the call information by long pressing the BLF/BLF List key.	All phones except T48G, T46G, T42G, T41P, T30P, T30, T29G, T19 E2, T19P E2 and CP920

Shared Line

Introduction

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
- Retrieve a held call remotely
- Barge in an active call (only SCA)
- Pull a shared call (only SCA)

> Supported devices: All phones except T30P, T30, T19 E2, T19P E2.

State Indicator of Shared Line

The shared line is indicated by a different line key icon. Line key icon is not available on the T30P/T30/T19 § E2 phones.

For more detailed information, refer to State Indicator of Shared Line.

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

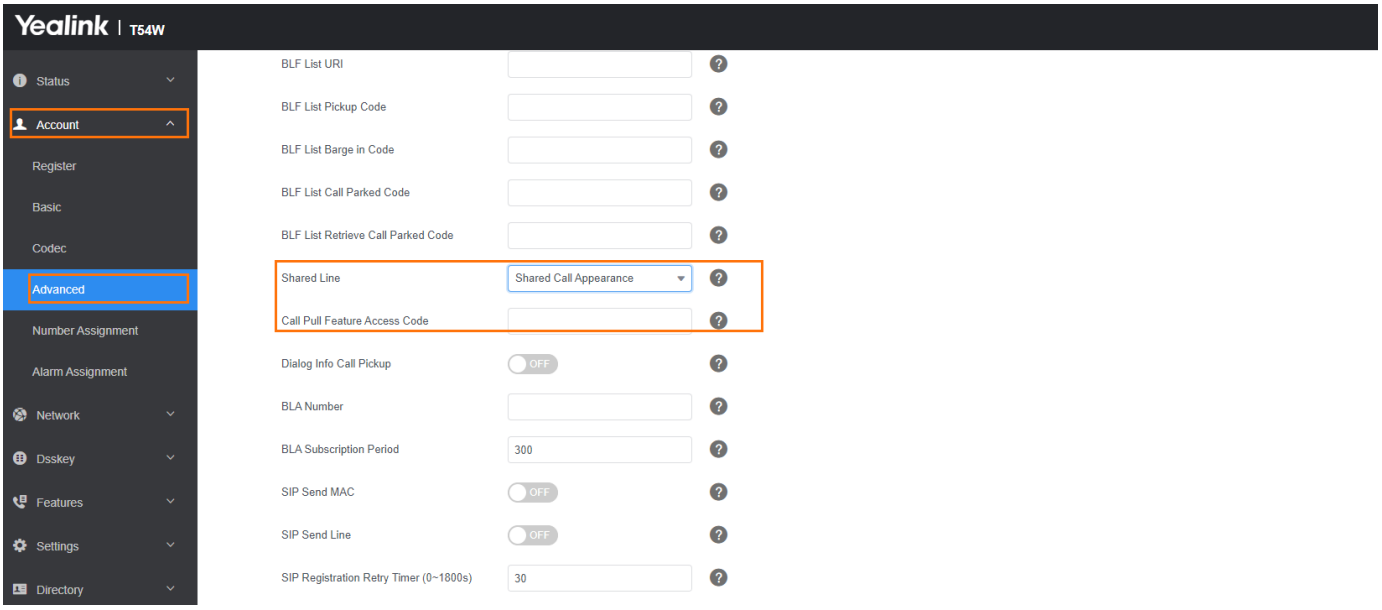
Parameter	Permitted Values	Default	Description
account.X.shared_line[1]	**0**-Disabled **1**-Shared Call Appearance	0	It configures the registration line type.
account.X.line_seize.expires[1]	Integer from 0 to 65535	15	It configures the line-seize subscription expiration time (in seconds). It works only if "account.X.shared_line" is set to 1 (Shared Call Appearance).
account.X.shared_line_callpull_code[1]	String within 99 characters	Blank	It configures the call pull feature access code to retrieve an existing call from another shared phone, regardless of the phone's current status. It works only if "account.X.shared_line" is set to 1 (Shared Call Appearance).
features.barge_in_via_username.enable	**0**-Disabled, user register name to barge in, the phone sends an INVITE request with the register name when	0	It enables or disables the phone to use the user name of the account to barge in an active call.

	barging into a call **1**-Enabled, the phone sends an INVITE request with the user name when barging into a call		
phone_setting.call_remote_end_when_hold.busy_tone.enable	**0**-Disabled **1**-Enabled	1	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. It works only if "features.busy_tone_delay" is not set to 0.
account.X.shared_line.idle_details[1]	**0**-Disabled **1**-Enabled, users can also view the call details by long pressing the SCA line key.	0	It enables or disables the phone to display the basic SCA call information on the idle screen. It works only if "account.X.shared_line" is set to 1 (Shared Call Appearance).

> [1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T74U/T74W/T77U/T85W/T87W/T88W (Pro)/T88V Pro, X=1-16; for T53W/T53/T53C/T43U/T42G/T42U/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 E2, X=1-2; for T30P/T30/T19 E2/CP920/CP925/CP935W, X=1.

Set via the Web User Interface

On the web user interface, go to **Account** > **Advanced** > **Shared Line / Call Pull Feature Access Code.**



Bridge Lines Appearance (BLA)

BLA allows users to share a SIP line on two or more phones. Users can monitor the specific extension (BLA number) for status changes on each IP phone. To use this feature, a BLA group should be pre-configured on the server and one of them is specified as a BLA number.

Yealink phones support BLA using a SUBSCRIBE/NOTIFY mechanism as specified in RFC 3265. The event used is: “dialog” for bridged line appearance subscribe, and notify.

BLA Configuration

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

Configuration parameter

account.X.shared_line
account.X.bla_number
account.X.bla.notify_with_expire.enable
account.X.bla.subscribe_uri_build_type
account.X.bla_subscribe_period
phone_setting.call_remote_end_when_hold.busy_tone.enable

Parameter	Permitted Values	Default	Description
account.X.shared_line[1]	**0**-Disabled **3**-Draft BLA	0	It configures the registration line type.
account.X.bla_number[1]	String within 99 characters	Blan	It configures the BLA number.

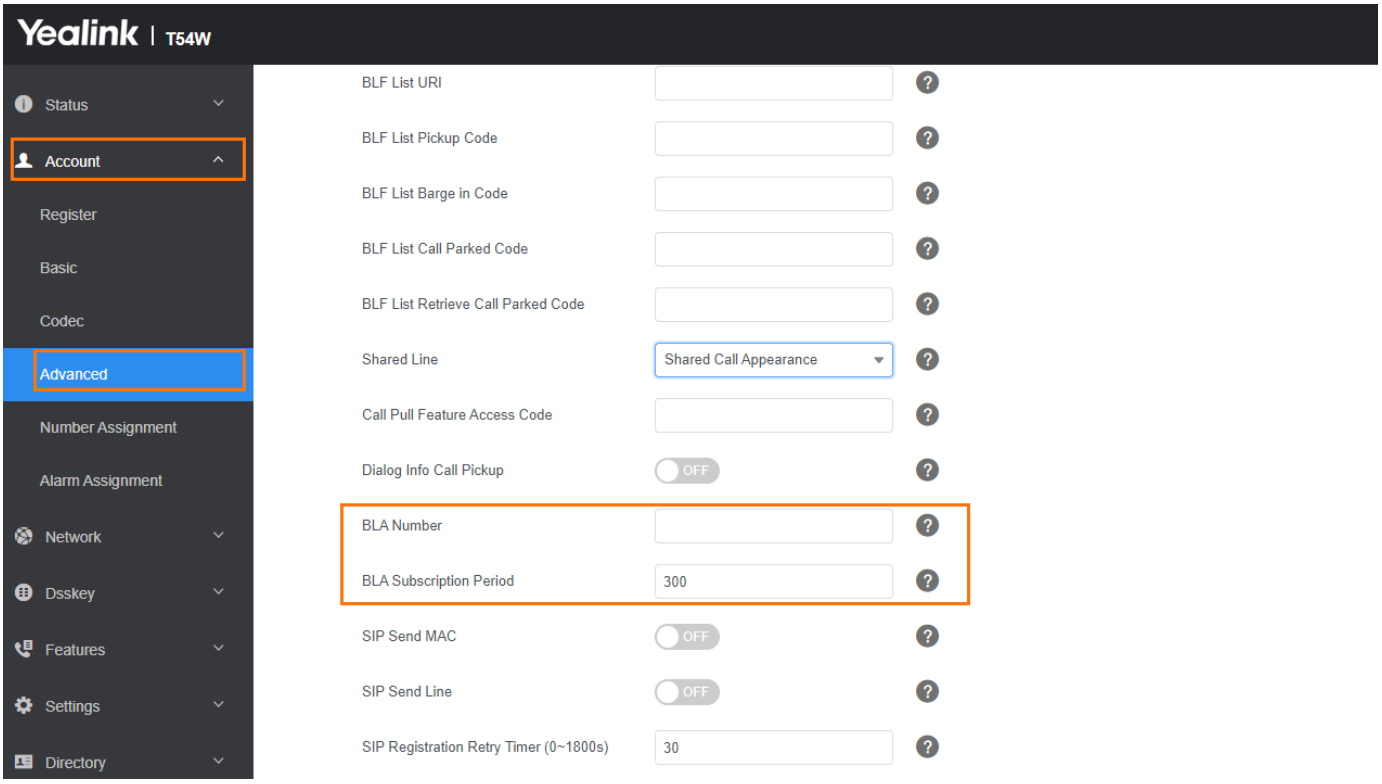
		k	It works only if "account.X.shared_line" is set to 3 (Draft BLA).
account.X.bla.notify_with_expire.enable[1]	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to add the Expires attribute to the Subscription-State header of the BLA NOTIFY message. It works only if "account.X.shared_line" is set to 3 (Draft BLA). For teltronnic BLA, you need to set the value of this parameter to 0 (Disabled).
account.X.bla.subscribe_uri_build_type[1]	**0**-From Contact header in the SUBSCRIBE message sent by the server **1**-According to the BLA number (configured by the parameter "account.X.bla_number")	0	It configures the constitution of the URI for BLA subscription. It works only if "account.X.shared_line" is set to 3 (Draft BLA). For teltronic BLA, you need to set the value of this parameter to 1 (Enabled).
account.X.bla_subscribe_period[1]	Integer from 60 to 7200	300	It configures the period (in seconds) of the BLA subscription. It works only if "account.X.shared_line" is set to 3 (Draft BLA).
phone_setting.call_remote_end_when_hold.busy_tone.enable	**0**-Disabled **1**-Enabled	1	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. It works only if "features.busy_tone_delay" is not set to 0.

[1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T74U/T74W/T77U/T85W/T87W/T88W (Pro)/T88V Pro, X=1-16; for T53W/T53/T53C/T43U/T42G/T42U/T42S/

> T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 E2, X=1-2; for T30P/T30/T19 E2/CP920/CP925/CP935W, X=1.

Set via the Web User Interface

On the web user interface, go to **Account** > **Advanced** > **BLA Number / BLA Subscription Period.**



> [1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T74U/T74W/T77U/T85W/T87W/T88W (Pro)/T88V Pro, X=1-16; for T53W/T53/T53C/T43U/T42G/T42U/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 E2, X=1-2; for T30P/T30/T19 E2/CP920/CP925/CP935W, X=1.

Bridged Call Appearance (BCA)

Introduction

Call delegation allows you to efficiently manage multiple incoming calls from your desktop. Delegated lines or bridged call appearance (BCA) is a standalone extension shared among multiple users. This feature allows your primary number to appear on different phones.

With the delegated lines feature, you can:

- Call on behalf of.
- Hold and pick up within the group.
- Share lines.
- Join calls or barge in.

> Supported device：T33G/T4XU/T5XW.

BCA Configuration

In a BCA scenario where the boss is very busy, you can control the delayed ringing time through the configuration parameter.

```
account.x.share_line.delay_time
```

Parameter	Permitted Values	Default	Description
account.x.share_line.delay_time	**0**: rings immediately upon receiving an INVITE **1-80**: rings 1-80 seconds after receiving an INVITE	0	It configures the delayed ringing time for the BCA account, in seconds.

Intercom

Intercom

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. In addition, the intercom key can be used for monitoring the status changes of a specific line on the phone.

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.

Line Key Configuration	Programmable Key Configuration
linekey.X.type = 14 linekey.X.line = 1 linekey.X.value = 4603 linekey.X.label = Bill	programablekey.X.type = 14 programablekey.X.line = 1 programablekey.X.value = 4603

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).

If you want to use the Intercom key to pick up a call, you need to enable the Intercom key to monitor state changes, and configure the pickup code for the Intercom key, for example, set "linekey.X.extension = *97*" *or* "*programablekey.X.extension* = 97 ". When the monitored user Bill (4603) receives an incoming call, you can press the Intercom key to pick up the call to Bill (4603) directly.

> You cannot use a programmable key to monitor an intercom contact for state changes, but press it to pick up a call.

State Monitor for Intercom Contact

You can make the phone to monitor a specific intercom user for state changes (busy or idle). When the monitored user receives an incoming call, the supervisor can press the intercom key to pick up the call directly. The phones support this feature using a SUBSCRIBE/NOTIFY mechanism as specified in RFC 3265.

> If you want to use the Intercom key to pick up a call, you need to configure the pickup code for

the Intercom key, for example, “linekey.X.extension = *97”.

State Indicator of Intercom Contact

The following table shows the LED indicator associated with the Intercom key:

LED Status	Description
Solid green	The monitored user is idle.
Fast-flashing red (200ms)	The monitored user receives an incoming call.
Solid red	The monitored user is dialing. The monitored user is talking.
Off	The monitored user does not exist.

State Monitor for Intercom Contact Configuration

The following table lists the parameters you can use to configure the state monitor for intercom contact.

Configuration parameter

features.intercom.led.enable
features.intercom.subscribe.enable

Parameter	Permitted Values	Supported Devices	Default	Description
features.intercom.led.enable	0-Disabled 1-Enabled	All phones except T30P, T30, T19 E2, T19 Pro E2 and CP920	0	It enables or disables the phone to display different intercom DSS key LED status/icons when the status of monitored user changes. It works only if “features.intercom.subscribe.enable” is set to 1 (Enabled).
features.intercom.subscribe.enable	0-Disabl	All phones except T30P, T30, T19 E2, T19 Pro E2 and	0	It enables or disables intercom subscription for the phones.

	ed 1-Enabled	CP920		
account.x.external_intercom.ignore_dnd.mode	0-Disabled 1-Enabled	It works only if you firmware version is x.86.0.112 or later.	0	It is used to configure whether a specific account is allowed to ignore DND during Intercom.

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	Permitted Values	Default	Description
features.intercom.mode	0-SIP 1-FAC, the feature access code is configured by "features.intercom.feature_access_code".	0	It configures the intercom mode.
features.intercom.feature_access_code	String	Blank	It configures the intercom feature access code. It works only if "features.intercom.

			mode" is set to 1 (FAC).
account.X.call_info[1]	String within 256 characters	Blank	It configures the value of the Call-Info header for intercom feature. The value format likes: <sip:XXX (X can be any value)>; answer-after=0. 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.

[1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T74U/T74W/T77U/T85W/T87W/T88W (Pro)/T88V Pro, X=1-16; for T53W/T53/T53C/T43U/T42G/T42U/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 E2, X=1-2; for T30P/T30/T19 E2, T19 Pro E2/CP920/CP925/CP935W, X=1.

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 the 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

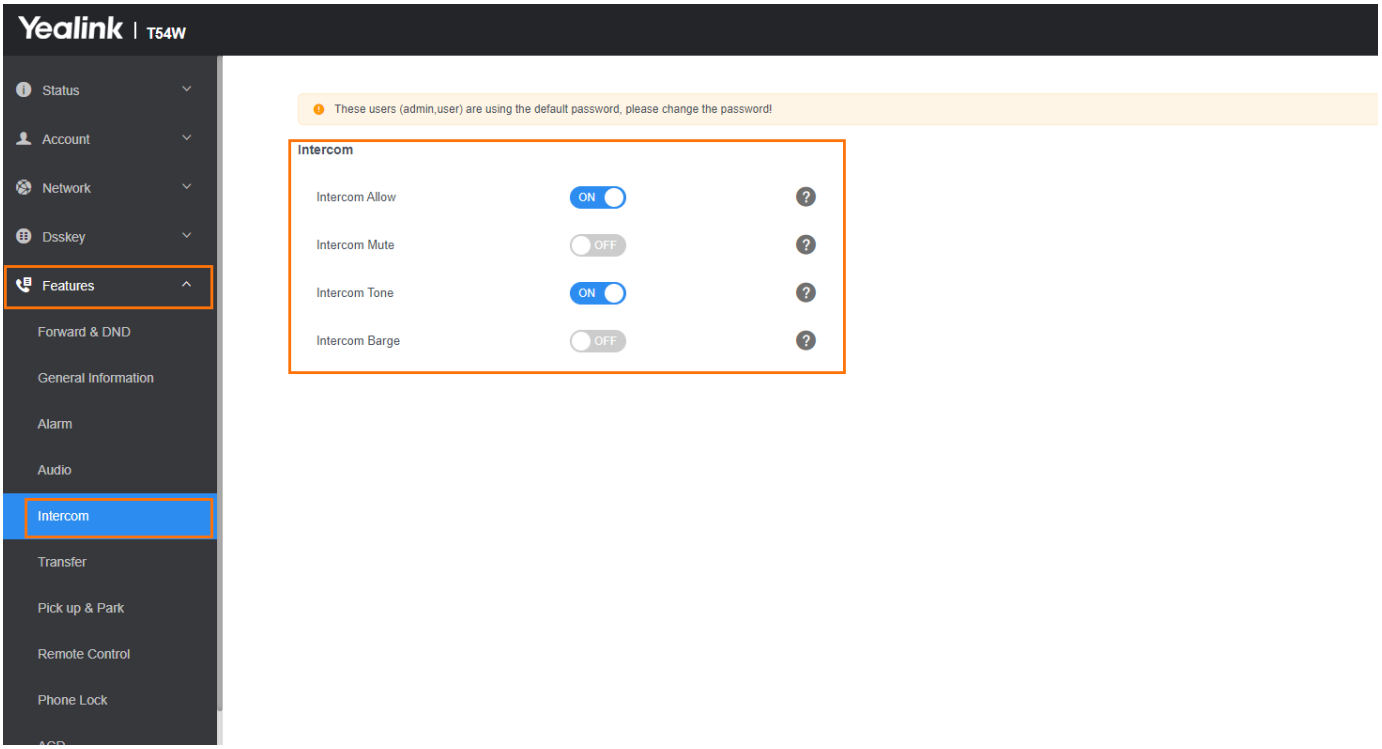
Parameter	Permitted Values	Default	Description
features.intercom.allow	0-Disabled, the phone will handle an incoming intercom call like a normal incoming call. 1-Enabled, the phone will automatically answer an incoming intercom call.	1	It enables or disables the phone to answer an incoming intercom call.
features.intercom.mute	0-Disabled 1-Enabled, the microphone is muted for intercom calls, and then the other party cannot hear you.	0	It enables or disables the phone to mute the microphone when answering an intercom call. It works only if "features.intercom.allow" and "features.allow_mute" are set to 1 (Enabled).
features.intercom.tone	0-Disabled 1-Enabled	1	It enables or disables the phone to play a warning tone when answering an intercom call. It works only if "features.intercom.allow" is set to 1 (Enabled).
features.intercom.barge	0-Disabled 1-Enabled, the phone will automatically answer the intercom call and place the active call on hold.	0	It enables or disables the phone to answer an incoming intercom call while there is already an active call on the IP phone. It works only if "features.intercom.allow" and "call_waiting.enable" are set to 1 (Enabled) and "phone_setting.call_appeara

			nce.calls_per_linekey" is greater than 1.
features.intercom.barge_in_dialing.enable	0-Disabled 1-Enabled	0	It enables or disables the intercom call to answer an incoming intercom call while dialing. It works only if "features.intercom.barge" is set to 0 (Disabled).
features.intercom.headset_prior.enable	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	It configures the channel mode to use when receiving an incoming intercom call.
account.X.alert_info[1]	String within 256 characters	Blank	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. 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.

> [1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T74U/T74W/T77U/T85W/T87W/T88W (Pro)/T88V Pro, X=1-16; for T53W/T53/T53C/T43U/T42G/T42U/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 E2, X=1-2; for T30P/T30/T19 E2, T19 Pro E2/CP920/CP925/CP935W, X=1.

Set via the Web User Interface

On the web user interface, go to **Features** > **Intercom** > **Intercom.**


Yealink | T54W
Status
Account
Network
Dsskey
Features
Forward & DND
General Information
Alarm
Audio
Intercom
Transfer
Pick up & Park
Remote Control
Phone Lock
These users (admin,user) are using the default password, please change the password!
Intercom
Intercom Allow
ON
Intercom Mute
OFF
Intercom Tone
ON
Intercom Barge
OFF

Remote Control

Before You Begin

When your phone connects to YMCS, the **Remote Control** module will be removed from the web user interface.

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.

Auto Provisioning

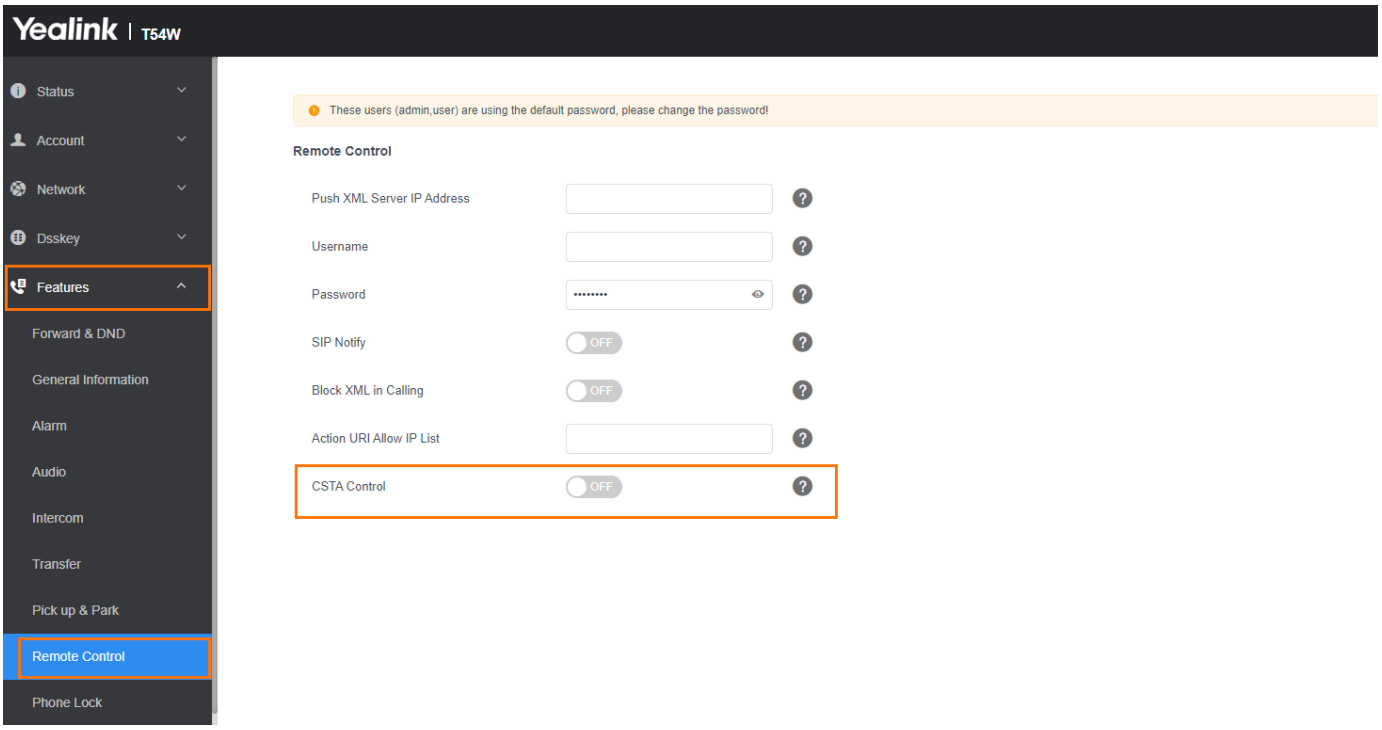
features.csta_control.enable

Parameter	Permitted Values	Default	Description	Supported Devices
features.csta_control.enable[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the CSTA feature.	All phones except T30P, T30, T19(P) 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)://<server-IPAddress>/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)://<server-IPAddress>/help.xml?variable name=$variable value. The variable name can be customized by users, while the variable value is predefined. For example, a URL “http://192.168.1.10/help.xml?mac=$mac” is specified for the event Mute, the $mac will be dynamically replaced with the MAC address of the IP phone when the IP phone mutes a call.

Predefined Events List

The following table lists the predefined events for the action URL.

Event	Description
Setup Completed	When the IP phone completes startup.
Registered	When the IP phone successfully registers an account.
Unregistered	When the IP phone logs out of the registered account.
Register Failed	When the IP phone fails to register for an account.

Off Hook	When the IP phone is off hook.
On Hook	When the IP phone is on hook.
Incoming Call	When the IP phone receives an incoming call.
Outgoing Call	When the IP phone places a call.
Established	When the IP phone establishes a call.
Terminated	When the IP phone terminates a call.
Open DND	When the IP phone enables the DND mode. 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 IP phone disables the DND mode. 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 IP phone enables the always forward. 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 IP phone disables the always forward. 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 IP phone enables the busy forward. 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 IP phone disables the busy forward. 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 IP phone enables the no-answer forward. 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 IP phone disables the no-answer forward. 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 IP phone transfers a call.
Blind Transfer	When the IP phone performs the blind transfer.
Attended Transfer	When the IP phone performs a semi-attended/attended transfer.
Hold	When the IP phone places a call on hold.
UnHold	When the IP phone resumes a held call.
Held	When a call on the IP phone is held.
UnHeld	When a held call is resumed.
Mute	When the IP phone mutes a call.
UnMute	When the IP phone un-mutes a call.
Missed Call	When the IP phone misses a call.
IP Changed	When the IP address of the IP phone changes.
Idle To Busy	When the state of the IP 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 IP phone rejects an incoming call.
Answer New Incoming Call	When the IP phone answers a new call.
Transfer Failed	When the IP phone fails to transfer a call.
Transfer Finished	When the IP phone completes transferring a call.
Forward Incoming Call	When the IP phone forwards an incoming call.
Autop Finish	When the IP phone completes auto provisioning via power-on.
Call Waiting On	When the IP phone enables call waiting.

Call Waiting Off	When the IP phone disables call waiting.
Headset	When the IP phone presses the HEADSET key (not applicable to CP920/ CP925 /CP935W phones).
Handfree	When the IP 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's IP address is assigned by the VPN server changes.
SIP INFO Display Update	It configures the SIP INFO message to trigger the action URL event during the call.
Conference	When the IP phone sets up a conference.
Alarm Trigger	When the IP phone triggers the alarm (Only applicable to T85W/T87W/T88W phones).

Variable Values List

The following table lists predefined variable values.

Variable Value	Description
$mac	The MAC address of the IP phone.
$ip	The IP address of the IP phone.
$model	The IP phone model.
$firmware	The firmware version of the IP phone.
$active_url	The SIP URI of the current account is used when the IP 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 is used when the IP phone places a call, receives an incoming cal,l or establishes a call.
$active_host	The host part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call.

$local	The SIP URI of the caller is used when the IP phone places a call. The SIP URI of the callee is used when the IP phone receives an incoming call.
$remote	The SIP URI of the callee is used when the IP phone places a call. The SIP URI of the caller is used when the IP phone receives an incoming call.
$display_local	The display name of the caller is shown when the IP phone places a call. The display name of the callee is shown when the IP phone receives an incoming call.
$display_remote	The display name of the callee is shown when the IP phone places a call. The display name of the caller is shown when the IP phone receives an incoming call.
$call_id	The call ID of the active call.
$callerID	The display name of the caller is shown when the IP phone receives an incoming call.
$calledNumber	The phone number of the callee when the IP 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's IP address is assigned by the VPN server.
$cfg_all	The CFG configuration file contains all current configurations of the IP phone. **Example**: http://10.82.21.10/Upload/?Cfg=$cfg_all 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. **Example**: http://10.82.21.10/Upload/?Cfg=$cfg_local It works only if "static.auto_provision.custom.protect" is set to 1 (Enabled). The valid URI is: http://<serverIPAddress>/<filename>/?variable name=$variable value.

Action URL Configuration

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

Auto Provisioning

```
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
action_url.conference

Parameter	Permitted Values	Default	Description

action_url.setup_completed	URL within 511 characters	Blank	It configures the action URL that the phone sends after startup. **Example**: action_url.setup_completed = http://192.168.0.20/help.xml?IP=$ip
action_url.registered	URL within 511 characters	Blank	It configures the action URL that the phone sends after an account is registered. **Example**: action_url.registered = http://192.168.0.20/help.xml?IP=$ip
action_url.unregistered	URL within 511 characters	Blank	It configures the action URL that the phone sends after an account is unregistered. **Example**: action_url.unregistered = http://192.168.0.20/help.xml?IP=$ip
action_url.register_failed	URL within 511 characters	Blank	It configures the action URL that the phone sends after a registration failure. **Example**: action_url.register_failed = http://192.168.0.20/help.xml?IP=$ip
action_url.off_hook	URL within 511 characters	Blank	It configures the action URL the phone sends when off-hook. **Example**: action_url.off_hook = http://192.168.0.20/help.xml?IP=$ip
action_url.on_hook	URL within 511 characters	Blank	It configures the action URL the phone sends when on hook. **Example**: action_url.on_hook = http://192.168.0.20/help.xml?IP=$ip
action_url.incoming_call	URL within 511 characters	Blank	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=$ip
action_url.outgoing_call	URL within 511 characters	Blank	It configures the action URL the phone sends when placing a call. **Example**: action_url.outgoing_call = http://192.168.0.20/help.xml?IP=$ip
action_url.call_established	URL within 511 characters	Blank	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=$ip
action_url.call_terminated	URL within 511 characters	Blank	It configures the action URL the phone sends when terminating a call. **Example**: action_url.call_terminated = http://192.168.0.20/help.xml?IP=$ip
action_url.dnd_on	URL within 511 characters	Blank	It configures the action URL that the phone sends when the DND feature is activated. **Example**: action_url.dnd_on = http://192.168.0.20/help.xml?IP=$ip
action_url.dnd_off	URL within 511 characters	Blank	It configures the action URL the phone sends when the DND feature is deactivated. **Example**: action_url.dnd_off = http://192.168.0.20/help.xml?IP=$ip
action_url.always_fwd_on	URL within 511 characters	Blank	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=$ip
action_url.always_fwd_off	URL within 511 characters	Blank	It configures the action URL the phone sends when the always forward feature is deactivated. **Example**: action_url.always_fwd_off = http://192.168.0.20/help.xml?IP=$ip

action_url.busy_fwd_on	URL within 511 characters	Blank	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=$ip
action_url.busy_fwd_off	URL within 511 characters	Blank	It configures the action URL the phone sends when the busy forward feature is deactivated. **Example**: action_url.busy_fwd_off = http://192.168.0.20/help.xml?IP=$ip
action_url.no_answer_fwd_on	URL within 511 characters	Blank	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=$ip
action_url.no_answer_fwd_off	URL within 511 characters	Blank	It configures the action URL the phone sends when the no-answer forward feature is deactivated. **Example**: action_url.no_answer_fwd_off = http://192.168.0.20/help.xml?IP=$ip
action_url.transfer_call	URL within 511 characters	Blank	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=$ip
action_url.blind_transfer_call	URL within 511 characters	Blank	It configures the action URL the phone sends when performing a blind transfer. **Example**: action_url.blind_transfer_call = http://192.168.0.20/help.xml?IP=$ip
action_url.attended_transfer_call	URL within 511 characters	Blank	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=$ip
action_url.hold	URL within 511 characters	Blank	It configures the action URL the phone sends when placing a call on hold. **Example**: action_url.hold = http://192.168.0.20/help.xml?IP=$ip
action_url.unhold	URL within 511 characters	Blank	It configures the action URL the phone sends when resuming a hold call. **Example**: action_url.unhold = http://192.168.0.20/help.xml?IP=$ip
action_url.held	URL within 511 characters	Blank	It configures the action URL the phone sends when a call is held. **Example**: action_url.held = http://192.168.0.20/help.xml?IP=$ip
action_url.unheld	URL within 511 characters	Blank	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=$ip
action_url.mute	URL within 511 characters	Blank	It configures the action URL the phone sends when muting a call. **Example**: action_url.mute = http://192.168.0.20/help.xml?IP=$ip
action_url.unmute	URL within 511 characters	Blank	It configures the action URL the phone sends when unmuting a call. **Example**: action_url.unmute = http://192.168.0.20/help.xml?IP=$ip
action_url.missed_call	URL within 511 characters	Blank	It configures the action URL the phone sends when missing a call. **Example**: action_url.missed_call = http://192.168.0.20/help.xml?IP=$ip
action_url.busy_to_idle	URL within 511 characters	Blank	It configures the action URL the phone sends when changing the state of the IP phone from busy to idle. **Example**:

			action_url.busy_to_idle = http://192.168.0.20/help.xml?IP=$ip
action_url.idle_to_busy	URL within 511 characters	Blank	It configures the action URL the phone sends when changing the state of the phone from idle to busy. **Example**: action_url.idle_to_busy = http://192.168.0.20/help.xml?IP=$ip
action_url.ip_change	URL within 511 characters	Blank	It configures the action URL that the phone sends when changing the IP address of the phone. **Example**: action_url.ip_change = http://192.168.0.20/help.xml?IP=$ip
action_url.reject_incoming_call	URL within 511 characters	Blank	It configures the action URL the phone sends when rejecting an incoming call. **Example**: action_url.reject_incoming_call = http://192.168.0.20/help.xml?IP=$ip
action_url.answer_new_incoming_call	URL within 511 characters	Blank	It configures the action URL that the phone sends when answering a new incoming call. **Example**: action_url.answer_new_incoming_call = http://192.168.0.20/help.xml?IP=$ip
action_url.forward_incoming_call	URL within 511 characters	Blank	It configures the action URL the phone sends when forwarding an incoming call. **Example**: action_url.forward_incoming_call = http://192.168.0.20/help.xml?IP=$ip
action_url.transfer_finished	URL within 511 characters	Blank	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
action_url.transfer_failed	URL within 511	Blan	It configures the action URL the phone sends when failing to transfer a call.

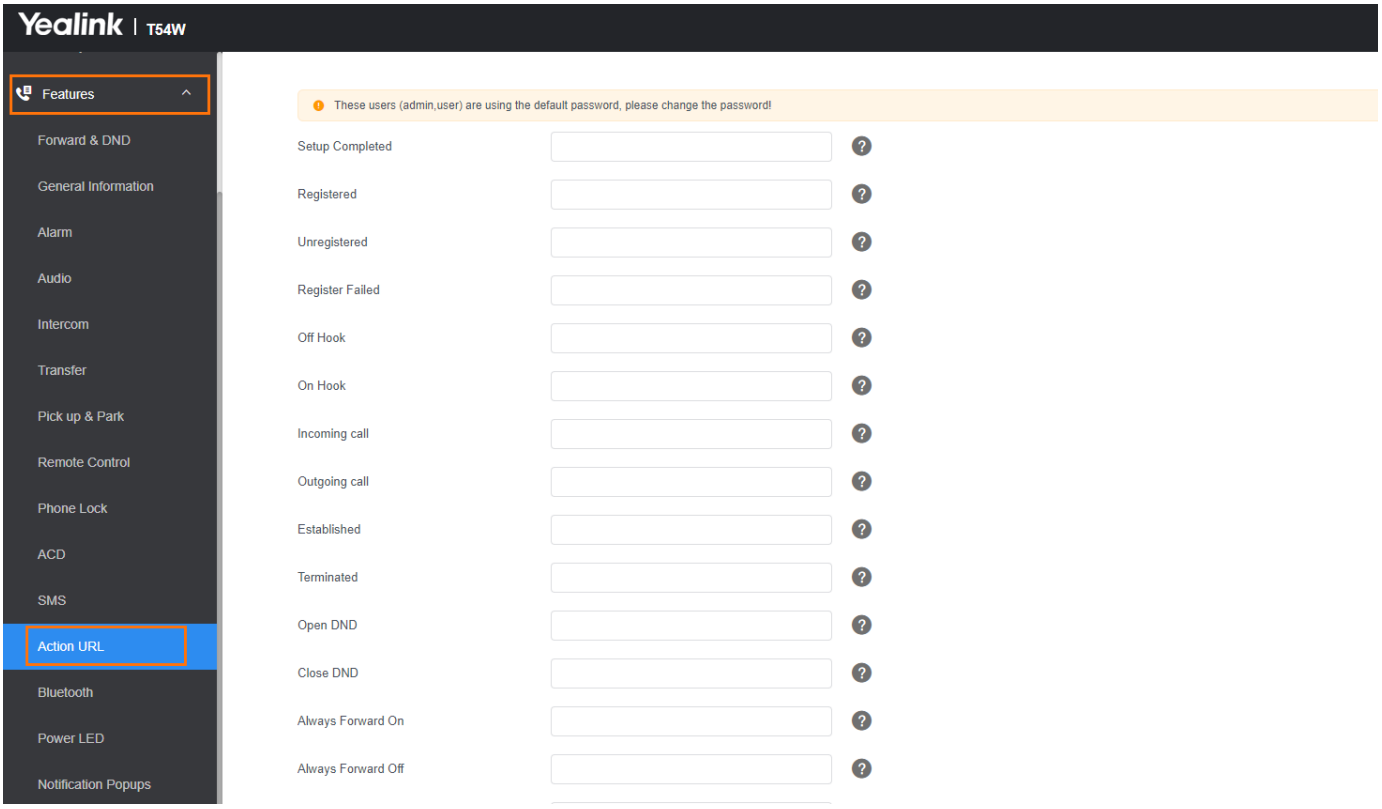
	characters	k	**Example**: action_url.transfer_failed = http://192.168.0.20/help.xml?IP=$ip
action_url.setup_autop_finish	URL within 511 characters	Blank	It configures the action URL the phone sends when completing auto provisioning via power on. **Example**: action_url.setup_autop_finish = http://192.168.0.20/help.xml?IP=$ip
action_url.call_waiting_on	URL within 511 characters	Blank	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=$ip
action_url.call_waiting_off	URL within 511 characters	Blank	It configures the action URL the phone sends when the call waiting feature is disabled. **Example**: action_url.call_waiting_off = http://192.168.0.20/help.xml?IP=$ip
action_url.headset	URL within 511 characters	Blank	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=$ip
action_url.handfree	URL within 511 characters	Blank	It configures the action URL the phone sends when pressing the Speakerphone key. **Example**: action_url.handfree = http://192.168.0.20/help.xml?IP=$ip
action_url.cancel_callout	URL within 511 characters	Blank	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
action_url.remote_busy	URL within 511	Blan	It configures the action URL the phone sends when the outgoing call is rejected.

	characters	k	**Example**: action_url.remote_busy = http://192.168.0.20/help.xml?IP=$ip
action_url.call_remote_canceled	URL within 511 characters	Blank	It configures the action URL the phone sends when the remote party cancels the outgoing call in the ringing state. **Example**: action_url.call_remote_canceled= http://192.168.0.20/help.xml?IP=$ip
action_url.peripheral_information	URL within 511 characters	Blank	It configures the action URL that 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
action_url.vpn_ip	URL within 511 characters	Blank	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=$ip
custom.action_url.view_misscall	URL within 511 characters	Blank	It is used to configure the URL for viewing missed calls in the ActionURL.
custom.action_url.view_forward	URL within 511 characters	Blank	It is used to configure the URL for viewing forward calls in the ActionURL.
action_url.call_established	URL within 511 characters	Blank	It configures the action URL that the IP phone sends when establishing a call. **Example**: action_url.call_established = http://192.168.0.20/help.xml?IP=$ip
action_url.sip_info_display_update	URL within 511 characters	Blank	It is used to configure the action URL triggered by receiving SIP INFO messages during a call.
action_url.idle_to_busy	URL within 511	Blan	It configures the action URL that the IP phone sends when changing the state of the IP phone from idle to

	characters	k	busy. **Example**: action_url.idle_to_busy = http://192.168.0.20/help.xml?IP=$ip
action_url.conference	URL within 511 characters	Blank	It configures the action URL for the phone to set up a conference. **Example**: action_url.conference = http://192.168.0.20/help.xml?IP=$ip

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 accepting 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.

> Yealink phones are compatible with the 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 the action URI. You can specify one or more trusted IP addresses on the IP phone, or configure the IP 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 a small office/home office where a secure firewall may prevent the HTTP or HTTPS GET request from the external network.

> If you want to only accept the SIP NOTIFY message from your SIP server and the 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 the SIP NOTIFY message method, you do not need to specify the trusted IP address for the action URI. However, you should enable the IP 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 values 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. This method does not apply to T57W/T48U/T48S/T48G phones.

The following shows an example for deleting all entries from the call history list when the phone is idle:

For CP920 phones:

http://10.3.20.10/servlet?key=F1;OK;F3;DOWN;DOWN;DOWN;OK;OK.

For other phones:

http://10.3.20.10/servlet?key=F1;F3;DOWN;DOWN;DOWN;OK;OK.

> 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@<phoneIPAddress>/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. (not applicable to T57W/CP925/CP935W/T58/VP59/CP960/CP965 phones)
ENTER	Press the Enter soft key. (not applicable to T57W/T48U/T48S/T48G/T58/VP59/CP960/CP965 phones)
SPEAKER	Press the Speakerphone key. (not applicable to CP920/CP925/CP935W/CP960/CP965 phones)
F_TRANSF	Transfer a call to another party.

ER	
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 unmute calls. (not applicable to T57W phones)
0-9/*/POUND	Press the keypad (0-9, * ,or #)(not applicable to CP925/CP935W phones).
L1-LX	Press the line keys (for T57W/T48U/T48S/T48G, X=29; for T54W/T46U/T46S/T46G/T29G/VP59/T58/CP960/CP965, X=27; for T42U/T42G/T42S/T41P/T41S, X=15; for T53W/T53/T53C/T43U/T27G, X=21; for T33P/T33G, X=12; for T40P/T40G/T23P/T23G, X=3; for T31P/T31G/T31/T21 § E2, X=2; for CP925/CP935W, X=30).
LX_LONGPRESS[1]	Perform a corresponding action when long-pressing the line key X.
BACK_IDLE	Return idle screen directly.
F1-F4	Press the soft keys.
MSG	Press the MESSAGE key. (not applicable to CP920/CP925/CP935W/CP960/CP965 phones)
HEADSET	Press the HEADSET key. (not applicable to CP920/CP925/CP935W/CP960/CP965 phones)
RD	Press the RD/Redial key (not applicable to CP920/CP925/CP935W/CP960/CP965 phones).
UP/DOWN/LEFT/RIGHT	Press the navigation keys. (not applicable to T57W/T58/VP59/CP960/CP965 phones)

Reboot	Reboot the phone.
AutoP	Perform auto provisioning.
DNDOn	Activate the DND feature. It works only if "features.dnd.allow" is set to 1 (Enabled).
DNDOff	Deactivate the DND feature. 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 from 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. 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.
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. **Example**: http://10.3.20.10/servlet?phonecfg=get[&accounts=1][&dnd=0][&fw=1] The valid URI is: http(s)://<phoneIPAddress > /servlet?phonecfg=get[&accounts=x][&dnd=x][&fw=x].
phonecfg=set[&configuration parameter=value]	Set the valid value for the specified configuration parameter. The valid URI is: http(s)://<phoneIPAddress>/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. **Example**: http://10.3.20.10/servlet?phonecfg= get[&account.1.enable][&features.dnd.enable] The valid URI is: http(s)://<phoneIPAddress>/servlet?phonecfg=get[&configuration parameter]…[&configuration parameter]. It can contain up to 10 configuration parameters.
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 IP 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. **Example**:

	http://10.10.20.10/servlet?key=NoAnswFwdOn=1001=24 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.
AlwaysFwdOff/ BusyFwdOff/ NoAnswFwdOff	Deactivate the always/busy/no answer forward feature for the IP phone. **Example**: http://10.10.20.10/servlet?key=NoAnswFwdOff 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.
CALLEND/ CallEnd	End a call.
ASW/ CANCEL/ HOLD/ UNHOLD: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 /> 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 in to the ACD system. 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	Switch 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. It is not available for a network conference.

[1]X is the line key ID. For T57W/T48U/T48S/T48G, X=1-29; for T54W/T46U/T46S/T46G/T29G, X=1-27; for T53W/T53/T53C/T43U/T27G, X=1-21; for T42U/T42G/T42S/T41P/T41S, X=1-15; for T33P/

> T33G, X=1-12; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 § E2, X=1-2; for CP925/CP935W, X=1-30.

Action URI Configuration

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

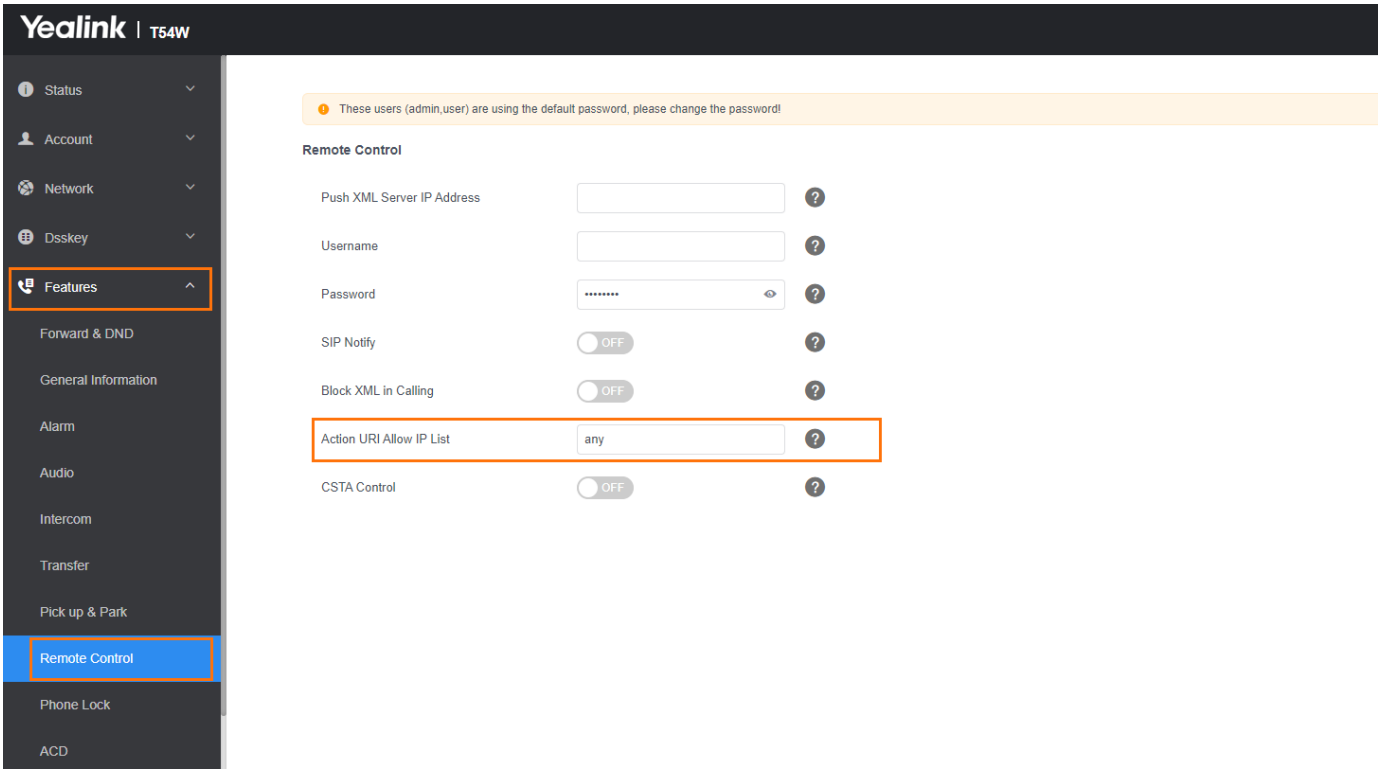
Auto Provisioning

```
features.action_uri.enable
features.show_action_uri_option
features.action_uri_limit_ip
```

Parameter	Permitted Values	Default	Description
features.action_uri.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to receive the action URI requests.
features.show_action_uri_option	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to pop up the Allow Remote Control prompt when receiving action URI requests. It works only if "features.action_uri.enable" is set to 1 (Enabled).
features.action_uri_limit_ip	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	It configures the 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). It works only if "features.action_uri.enable" is set to 1 (Enabled).

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 IP 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.

> 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 the web user interface login.

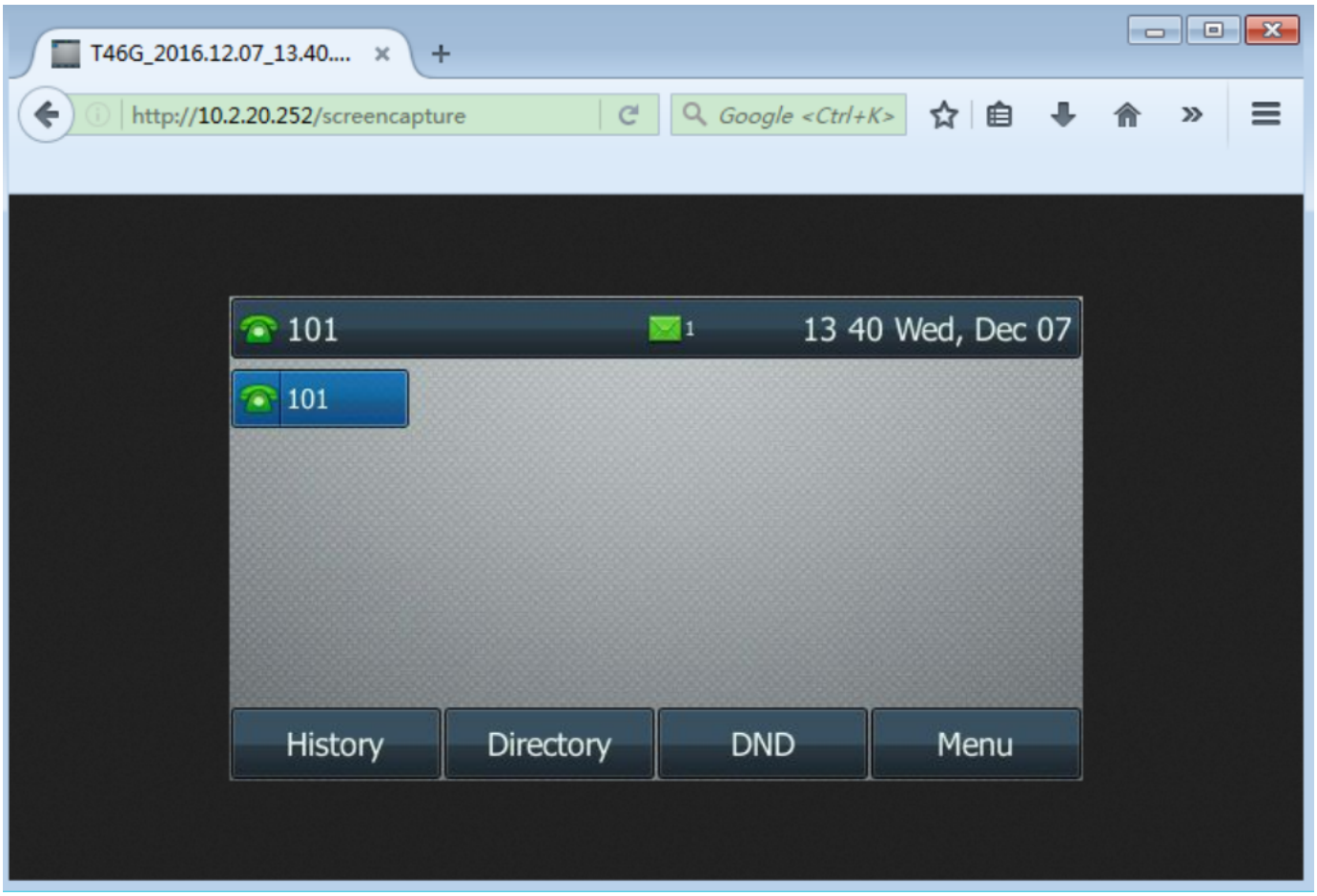
Procedure

1. Enter the 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.



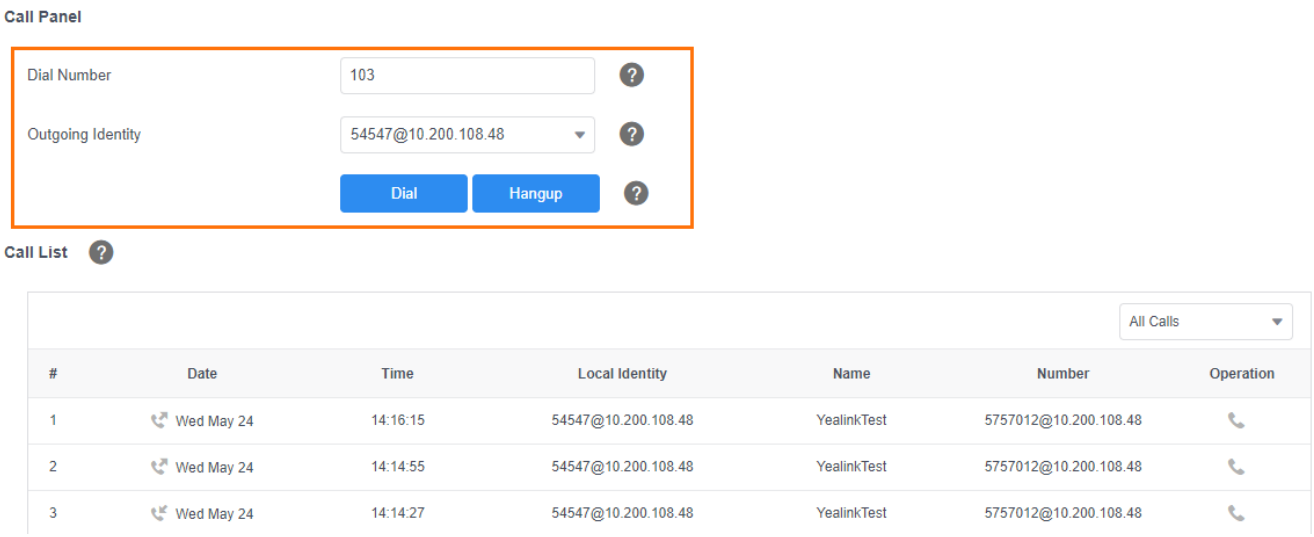
- Otherwise, the browser will display an image of the phone’s current screen directly. You can save the image to your local system.

> Frequent capture may affect phone performance. Yealink recommends that 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 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 the number.

> You can also place an IP direct call via the web user interface. The IP phone supports either IPv4 or IPv6 addresses.

Short Message Service (SMS)

Introduction

Yealink phones (except CP920/CP925/CP935W phones) support short message service (SMS). It allows users to send and receive text messages 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 parameters you can use to configure SMS.

Auto Provisioning

```
features.text_message.enable
```

Parameter	Permitted Values	Default	Description
features.text_message.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to send and receive a text messages.

Voice Mail

Introduction

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.

Before You Begin

Your version needs to be V86 or later to enable this feature.

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 IP phone can subscribe to the MWI messages for 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

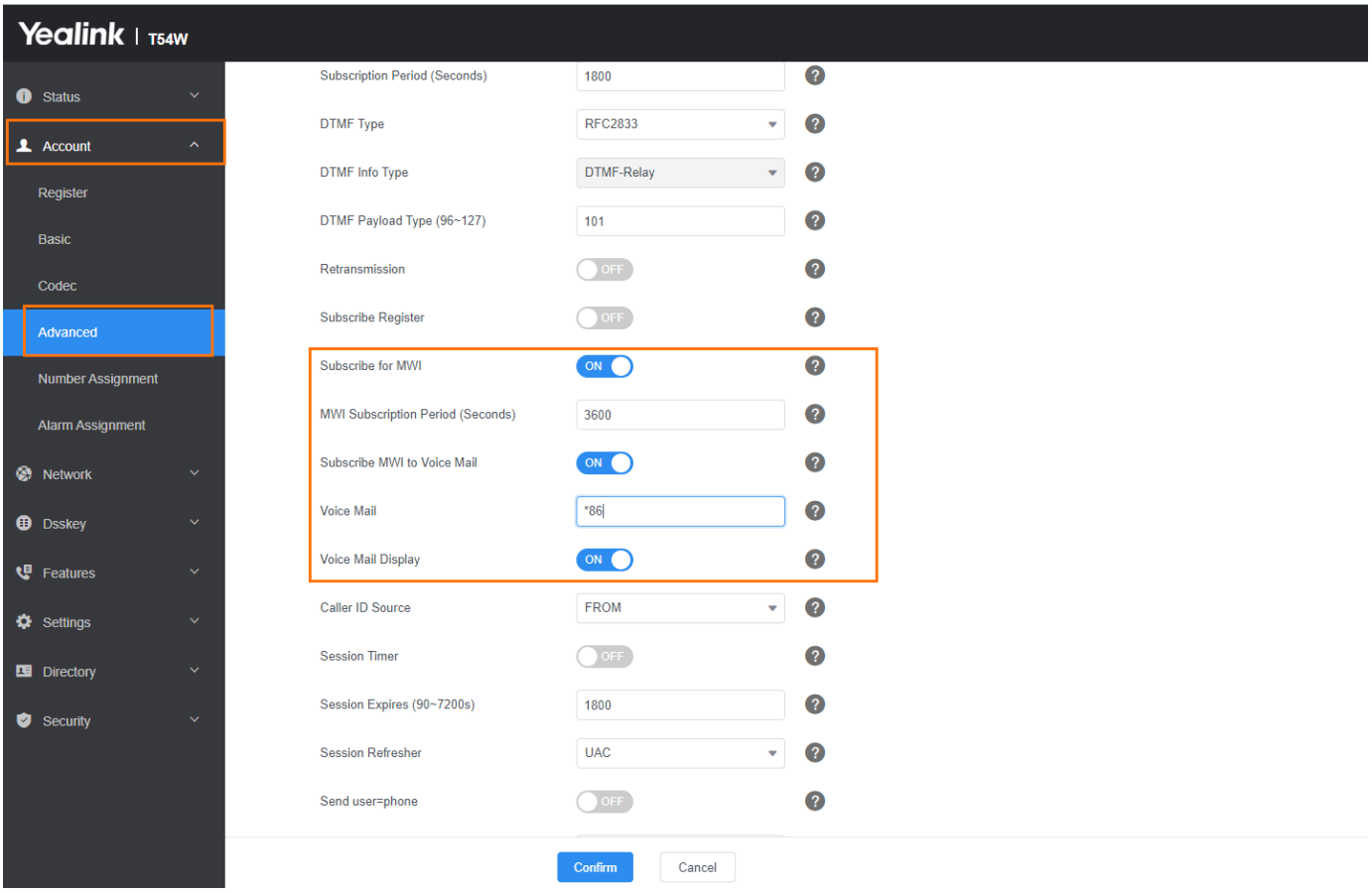
Parameter	Permitted Values	Default	Description
account.X.subscribe_mwi[1]	**0**-Disabled, the server automatically sends a message-summary NOTIFY in a new dialog each time the MWI status changes (This requires server support). **1**-Enabled, the phone will send a SUBSCRIBE message to the server for message-summary updates.	0	It enables or disables the phone from subscribing to the message waiting indicator.
account.X.subscribe_mwi_expires[1]	Integer from 0 to 84600	3600	It configures MWI subscribe expiry time (in seconds). It works only if **account.X.subscribe_mwi** is set to 1 (Enabled).
account.X.mwi_parse_terminated[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to parse the Terminated attribute in the received MWI NOTIFY message.
account.X.sub_fail_retry_interval[1]	Integer from 0 to 3600	30	It configures the interval (in seconds) for the phone to resubscribe when subscription fails.
account.X.subscribe_mwi_to_vm[1]	**0**-Disabled, the phone will subscribe to the message waiting indicator for a specific account. **1**-Enabled	0	It enables or disables the phone to subscribe to the message waiting indicator for the voice mail number. It works only if **account.X.subscribe_mwi** is set to 1 (Enabled) and **voice_mail.number.X** is configured.
voice_mail.number.X[1]	String within 99 characters	Blank	It configures the voice mail number.

account.X.display_mwi.enable [1]	**0**-Disabled **1**-Enabled	1	It enables or disables the MWI alert to indicate that you have an unread voice mail message.
features.voice_mail_alert.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to pop up the message when receiving the same number of new voicemails.
features.voice_mail_key_lamp_field.enable	**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	It enables or disables the phone to subscribe to the message waiting indicator for the voice mail number when configuring a Voice Mail dsskey.
features.hide_unread_vm_number.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to hide the number of unread voice mails in the pop-up message box.

> [1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T74U/T74W/T77U/T85W/T87W/T88W (Pro)/T88V Pro, X=1-16; for T53W/T53/T53C/T43U/T42G/T42U/T42S/T73U/T73W, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 E2, X=1-2; for T30P/T30/T19 E2/CP920/CP925/CP935W, X=1.

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.**


Yealink | T54W
Status
Account
Register
Basic
Codec
Advanced
Number Assignment
Alarm Assignment
Network
Dsskey
Features
Settings
Directory
Security
Subscription Period (Seconds)
1800
DTMF Type
RFC2833
DTMF Info Type
DTMF-Relay
DTMF Payload Type (96~127)
101
Retransmission
OFF
Subscribe Register
OFF
Subscribe for MWI
ON
MWI Subscription Period (Seconds)
3600
Subscribe MWI to Voice Mail
ON
Voice Mail
*86
Voice Mail Display
ON
Caller ID Source
FROM
Session Timer
OFF
Session Expires (90~7200s)
1800
Session Refresher
UAC
Send user=phone
OFF
Confirm
Cancel

XML Browser

Introduction

The 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 users' 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 the 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	Permitted Values	Default	Description
push_xml.server	**Blank**-The phone will reject HTTP POST messages from any server. **any**-The phone will accept HTTP POST messages from any	Blank	It configures the address of the push XML server.

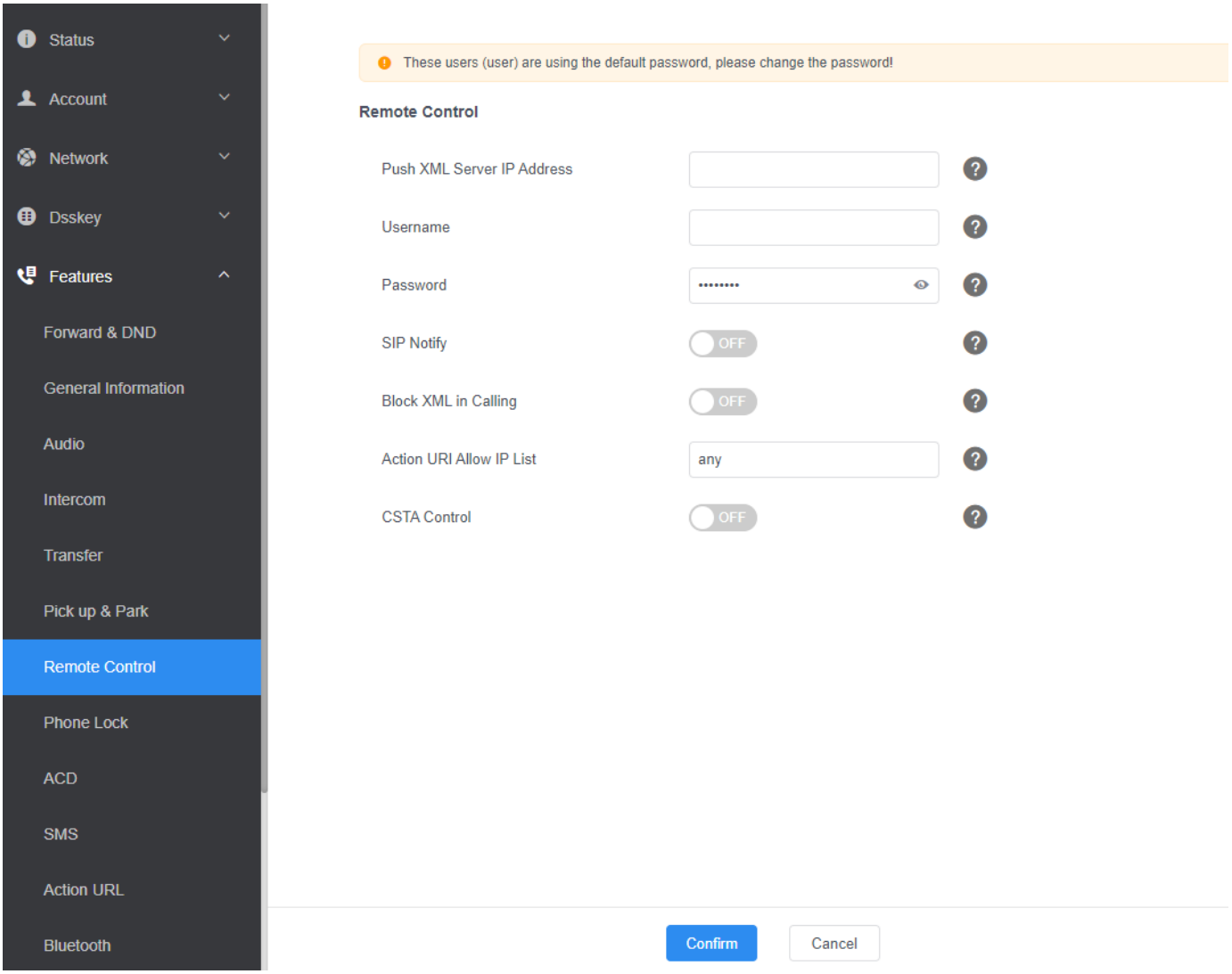
	server. IP address or domain name-Multiple addresses are separated by commas. (for example, 10.1.4.3,10.1.4.23); Support asterisk wildcard, each asterisk represents a field of the IP address (10.10.. represents 10.10.0.0 to 10.10.255.255).		
push_xml.block_in_calling	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to block XML applications during a call.
push_xml.sip_notify	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to process the push XML via the SIP NOTIFY message.
push_xml.phonebook.search.delay	Integer from 0 to 10000	1000	It configures the time (in milliseconds) to wait for the phone to send the entered keywords to the 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. For T23P/T23G/T40P/T40G phones, we recommend that you not download a large number of contacts from the server.
features.xml_browser.loading_tip.delay	Integer from 0 to 50000	100	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. It does not apply to the ImageScreen Object and the ImageMenu Object.
features.xml_browser.user_name	String within 15 characters	Blank	It configures the authentication user name for the XML request.
features.xml_browser.pwd	String within 15 characters	Blank	It configures the authentication password for the XML request.
push_xml.username	String	Blank	It configures the user name for the phone to authenticate with the push XML server. Leave it blank if no authentication is required.
push_xml.password	String within 15 characters	Blank	It configures the password for the phone to authenticate with the push XML server. Leave it blank if no authentication is required.
features.upload_server	URL within 1024 characters	Blank	It configures the server address to which the DssKey.cfg file is uploaded when the phone receives an XML command (Command: UploadSystemInfo).
xmlbrowser_icon_upload.url	URL within 511 characters	Blank	It configures the access URL of the *.tar file for custom icons displayed by the XML browser. The black-and-white screen phones support icons in DOB format, while the color-screen phones support icons in .jpg/.png/*.bmp/*.jpeg

			format.
xmlbrowser_icon.delete	http://localhost/all or http://localhost/name.(jpg/png/bmp/jpeg/dob)	Blank	It deletes the specified or all custom icons for the 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

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.**


Status
Account
Network
Dsskey
Features
Forward & DND
General Information
Audio
Intercom
Transfer
Pick up & Park
Remote Control
Phone Lock
ACD
SMS
Action URL
Bluetooth
These users (user) are using the default password, please change the password!
Remote Control
Push XML Server IP Address
Username
Password
SIP Notify
OFF
Block XML in Calling
OFF
Action URI Allow IP List
any
CSTA Control
OFF
Confirm
Cancel

Hot Desking

Introduction

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 for the users.

> It is not applicable to CP920 phones.

Hot Desking Key Configuration

The following shows the configuration for a Hot Desking key.

Line Key Configuration	Programmable Key Configuration
linekey.X.type = 34 linekey.X.label = Hot Desking	programablekey.X.type = 34

After provisioning, a Hot Desking key is available on the phone. You can press the Hot Desking key to clear pre-registration configurations of all accounts and register their 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	Permitted Values	Default	Description
hotdesking.dsskey_register_name_enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to provide an input field for the register name on the hot desking login wizard when pressing the Hot Desking DSS key.
hotdesking.dsskey_username_enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to provide an input field for the user name on the hot desking login wizard when pressing the Hot Desking DSS key.
hotdesking.dsskey_password_enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to provide an input field for the password on the hot desking login wizard when pressing the Hot Desking DSS key.
hotdesking.dsskey_sip_server_enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to provide an input field for the SIP server on the hot desking login wizard when pressing the Hot Desking DSS key.
hotdesking.dsskey_outbound_enable	**0**-Disabled **1**-Enabled	0	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.
features.hotdesking_clear_calllog.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to clear call records of the last guest after using hot desking to log into a new account.
hotdesking.log_out_prompt.time	**0**-Do not clear **1-1440**-Display a pop-up window to prompt clearing the account information after the specified period of inactivity.	0	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, the phone will display a pop-up window to prompt clearing the account information (in minutes). It works only if your firmware version is x.86.0.112 or later.

hotdesking.log_out_prompt.duration	**-1**-No pop-up, exit directly **0**-No automatic exit **1-86400**-Auto exit after the corresponding time	0	It is used to control the duration in seconds before executing the exit action after displaying the pop-up window. It works only if your firmware version is x.86.0.112 or later.

Device Management

Device Management

You can enable the device management feature to connect the 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.

For the T4XU series, make sure 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
static.remote_control.X.allow
dm.qoe_report.enable
dm.qoe_report.periodic.enable

Parameter	Permitted Values	Defau lt	Description
static.dm.ena ble	**0**-Disabled **1**-Enabled	0	It enables or disables the device management feature. For T4XU/T5XW, you do not need to set this parameter. On the contrary, you need to enable this feature on the phone (see phone UI below).
static.dm.ser ver.address	String within 512 characters	Blank	It configures the server address of the YDMP/YMCS.

static.dm.server.port	Integer from 0 to 65535	443	It configures the server port of the YDMP/YMCS.
dm.qoe_report.enable	**0**-Disabled **1**-Enabled	1	It configures whether to report the call statistics to YDMP/YMCS.
static.remote_control.X.allow[1]	**0**-Unauthorized, when the YDMP/YMCS wants to take the 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 screenshots or capture packets. **2**-Blocked, you reject the YDMP/YMCS to take phone screenshots or capture packets.	0	It configures whether to allow the YDMP/YMCS to take the phone's screenshots or capture packets.
dm.qoe_report.periodic.enable	**0**-Disabled **1**-Enabled	1	It configures whether to periodically report QoE parameters.

Introduction

Yealink IP 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 IP 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.

Supported Phones

The purpose of this guide is to serve as a basic guide for provisioning Yealink IP phones.

The following table lists product names and available firmware versions for IP phones that use the auto provisioning process outlined in this guide.

Product Name	Boot File (Available Firmware Version)	Exclude Mode (Available Firmware Version)
VP59	Yes (83 or later)	Yes (83 or later)
SIP-T58W	Yes (86 or later)	Yes (86 or later)
SIP-T58A	Yes (80 or later)	Yes (83 or later)
SIP-T33P/T33G/T31P/T31G/T31/T30P/T30	Yes (85 or later)	Yes (85 or later)
SIP-T57W/T54W/T53W/T53/T53C	Yes (84 or later)	Yes (84 or later)
SIP-T48U/T46U/T43U/T42U	Yes (84 or later)	Yes (84 or later)
SIP-T7X/T8X	Yes (87 or later)	Yes (87 or later)
SIP-T48G/S	Yes (81 or later)	Yes (83 or later)
SIP-T46G/S	Yes (81 or later)	Yes (83 or later)
SIP-T42G/S	Yes (81 or later)	Yes (83 or later)
SIP-T41P/S	Yes (81 or later)	Yes (83 or later)
SIP-T40P/G	Yes (81 or later)	Yes (83 or later)
SIP-T29G	Yes (81 or later)	Yes (83 or later)
SIP-T27G	Yes (81 or later)	Yes (83 or later)
SIP-T23P/G	Yes (81 or later)	Yes (83 or later)

SIP-T21(P) E2	Yes (81 or later)	Yes (83 or later)
SIP-T19(P) E2	Yes (81 or later)	Yes (83 or later)
CP860	Yes (81 or later)	No
CP960	Yes (80 or later)	Yes (83 or later)
CP965	Yes (86 or later)	Yes (86 or later)
CP920	Yes (81 or later)	Yes
CP925	Yes (86 or later)	Yes (86 or later)

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

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 downloads 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 "y000000000000.boot" before auto provisioning.

You can use a boot file to specify which configuration files to download 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 the Common CFG file and the 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 a personalized AutoDST file, a language package file, and a 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 (not applicable to VP59/T58A/T58W/T57W/T48U/T48G/T48S phones) 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 (not applicable to VP59/T58A/T58W/CP960)	CustomScreenSaver.xml
Firmware	X.83.0.XX.rom For example, 44.83.0.10.rom

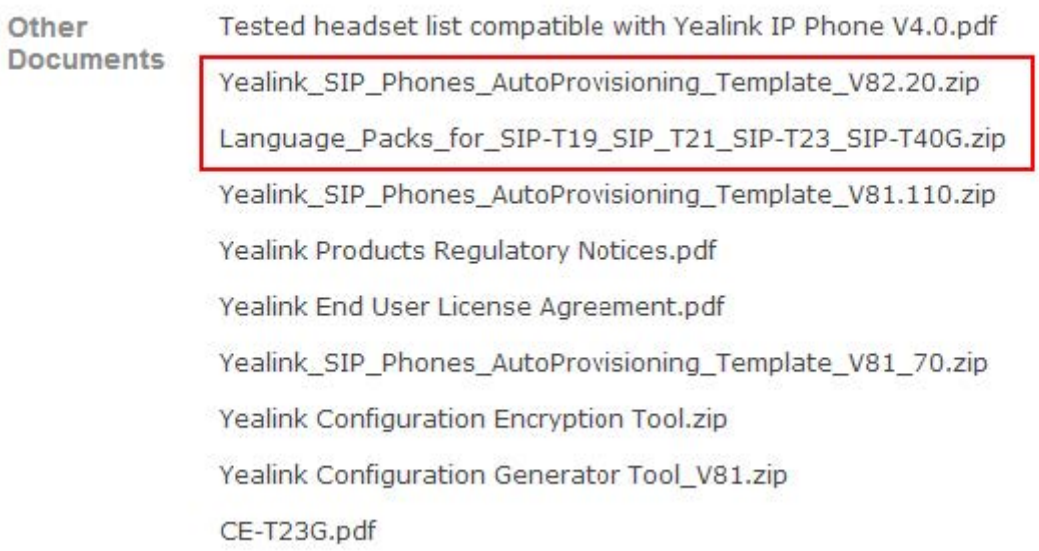
Obtain Template Files

You can ask the distributor or Yealink FAE for template files. You can also obtain them online:Yealink Support.

To download the 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.

For example, the following illustration shows the template files available for SIP-T23G IP phones running firmware version 82.



3. Open the folder you extracted and identify the files you want to edit.

Obtain Phone Information

Before provisioning, you also need the IP phone information. For example, the MAC address and the SIP account information of the IP phone.

MAC Address: The unique 12-digit serial number of the IP phone. You can obtain it from the barcode 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.

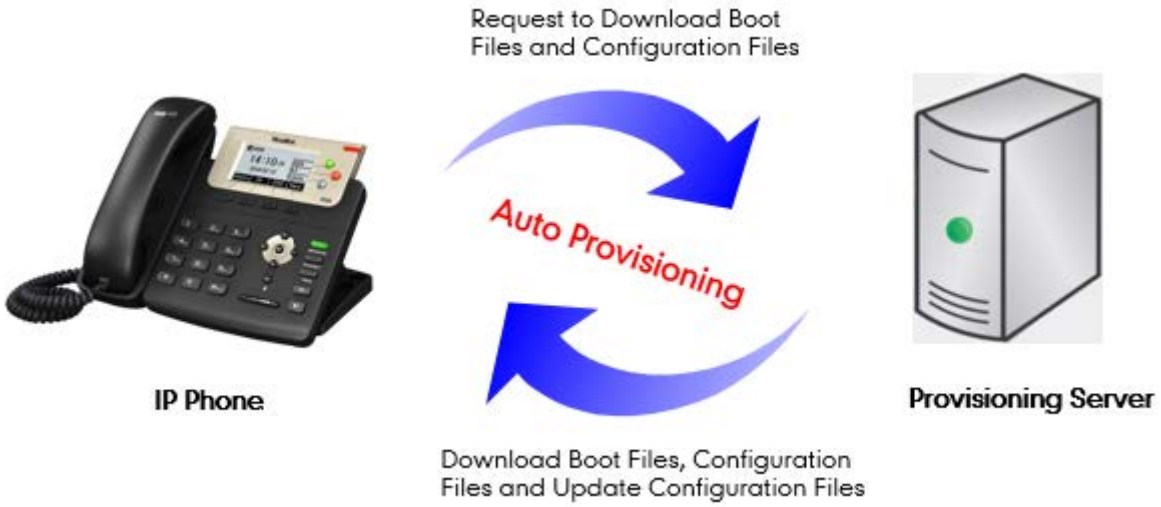
Provision Yealink IP Phones

This section provides instructions on how IP 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 IP 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 IP phone will download and update configuration files to the phone's flash.

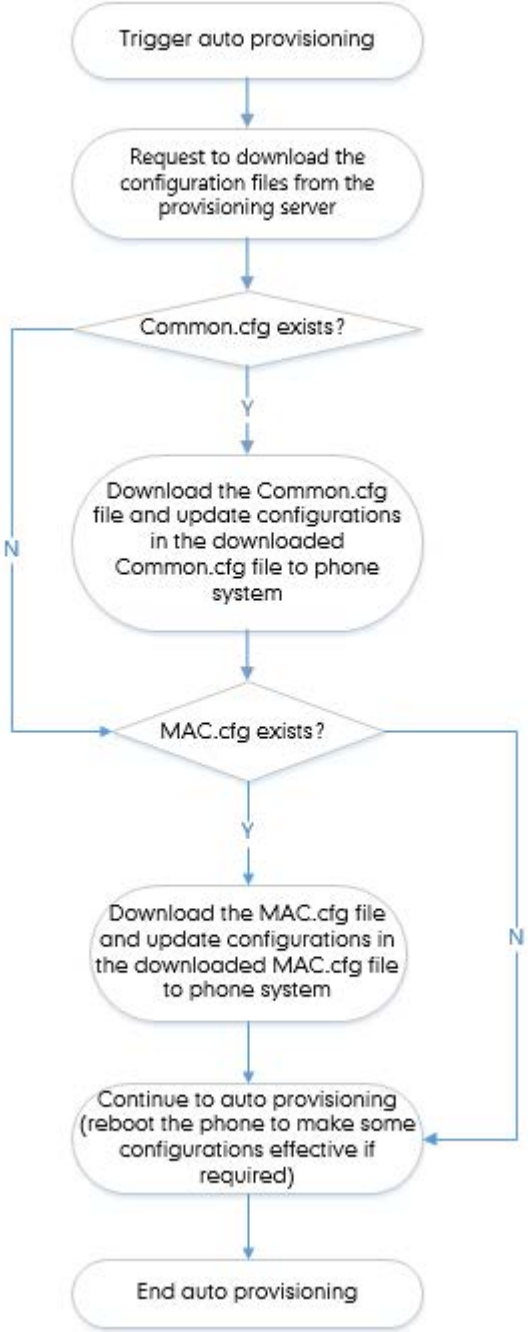
The following figure shows how the IP phone interoperates with the provisioning server:



Auto Provisioning Process

Old Mechanism – Without Boot Files

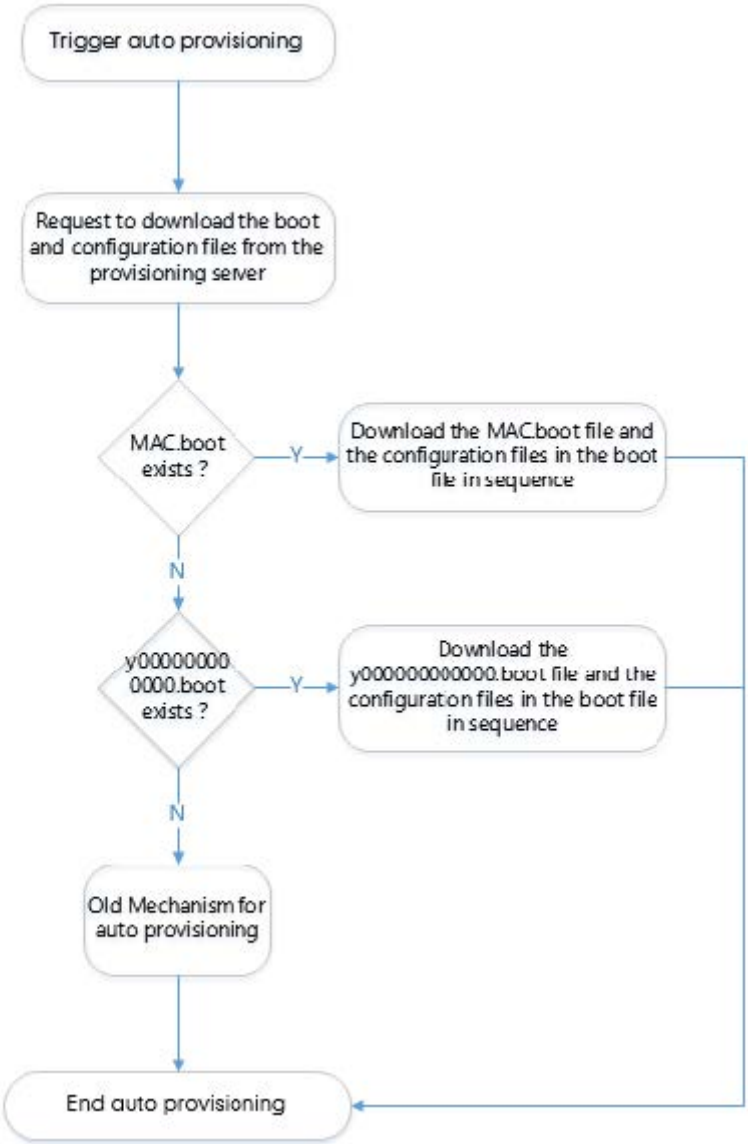
The following flowchart shows how Yealink IP phones perform auto provisioning when using configuration files only:



New Mechanism – With Boot Files

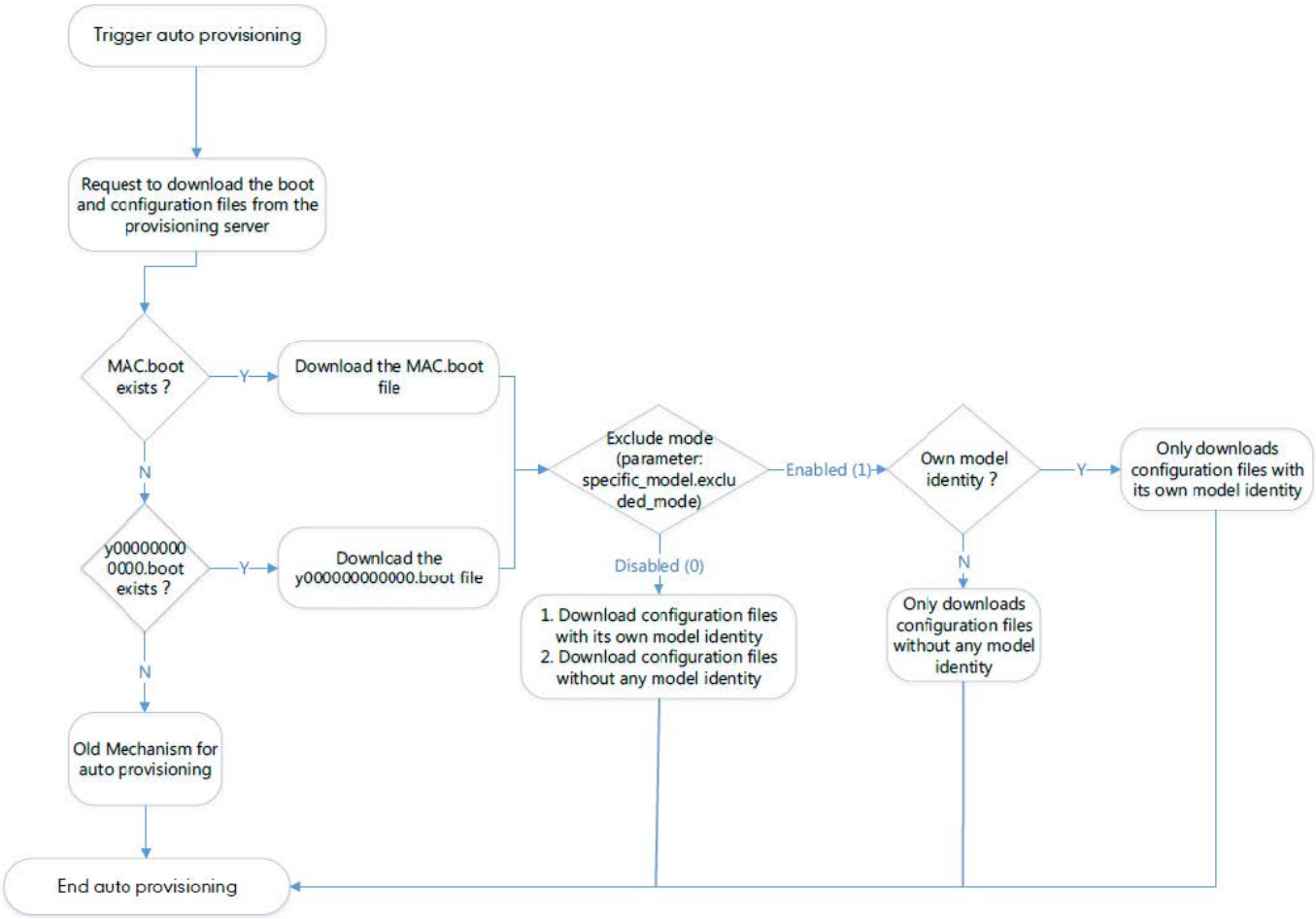
The following figure shows auto-provisioning flowcharts for Yealink IP phones when using boot files:

Scenario A – Do Not Support Exclude Mode



Scenario B – Support Exclude Mode

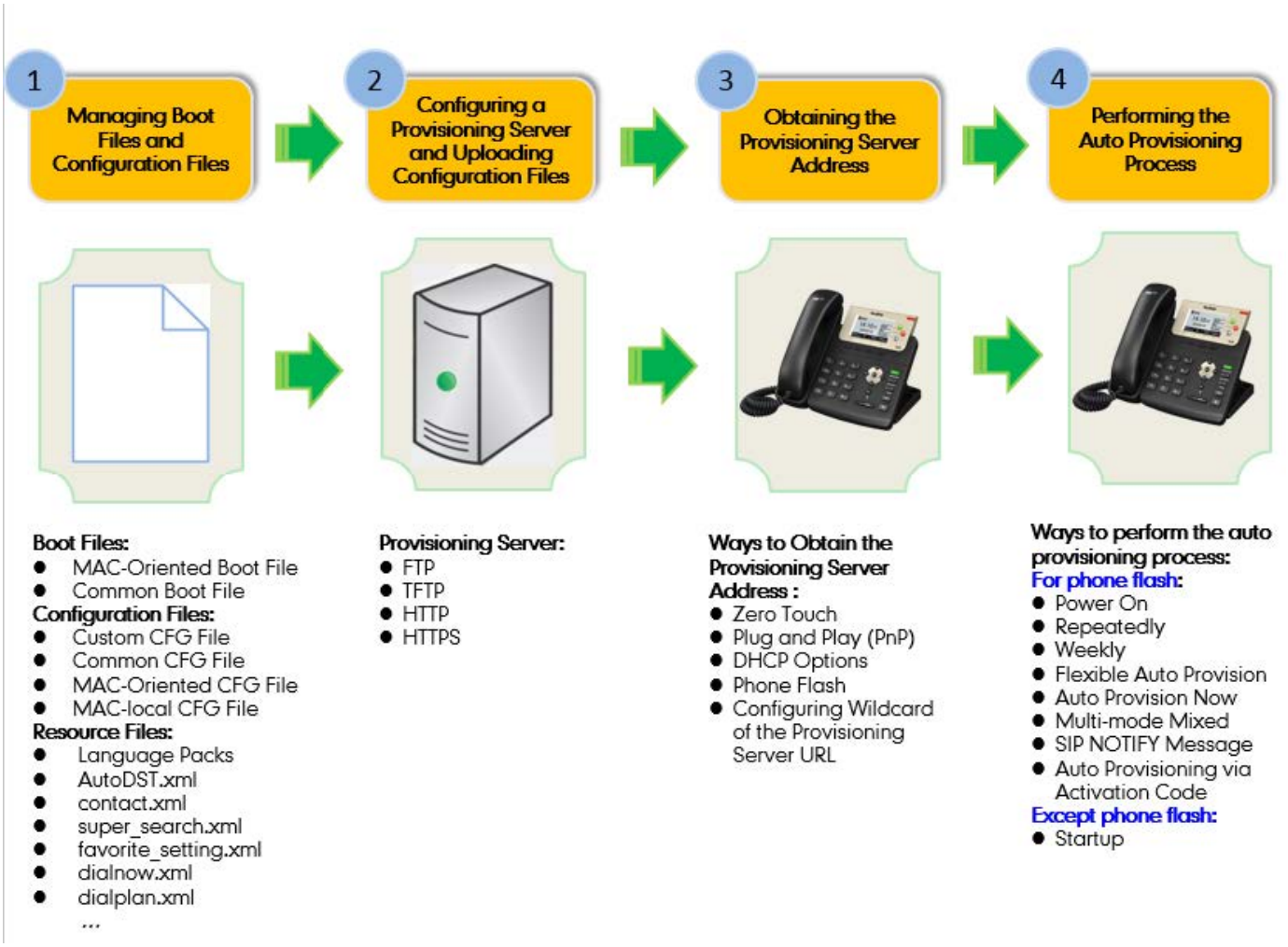
This scenario is only applicable to IP phones (except W52P/W56P IP phones) running firmware version 83 or later.



Major Tasks for Auto Provisioning

You need to complete four major tasks to provision Yealink IP 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 IP 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"

[T46S]include:config <tftp://10.2.5.193/network.cfg>
[T48S,T46G]include:config <../sip.cfg>
include:config "features.cfg"

overwrite_mode = 1
specific_model.excluded_mode=0
```

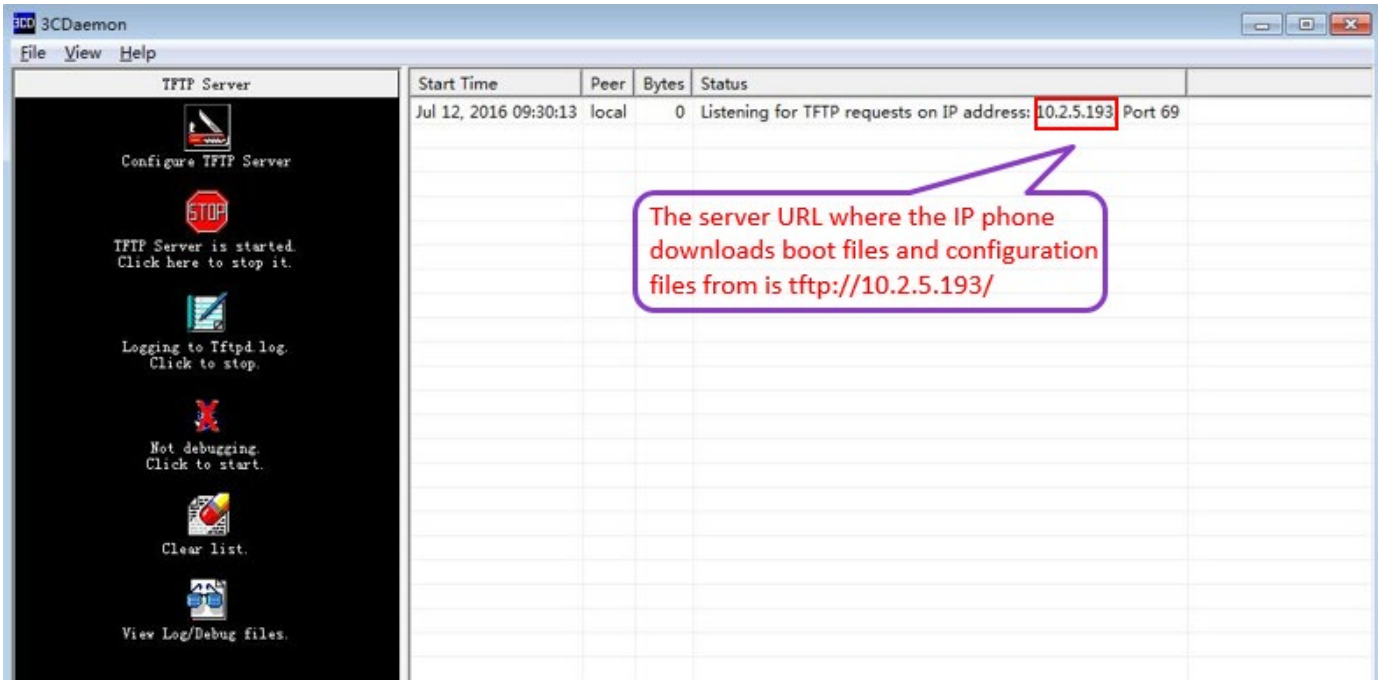
2. Manage configuration files.
3. Add/Edit the desired configuration parameters in the CFG file (for example, features.cfg) you want the IP phone to download.
4. For more information on how to manage configuration files, refer to Manage Configuration Files .

features.cfg

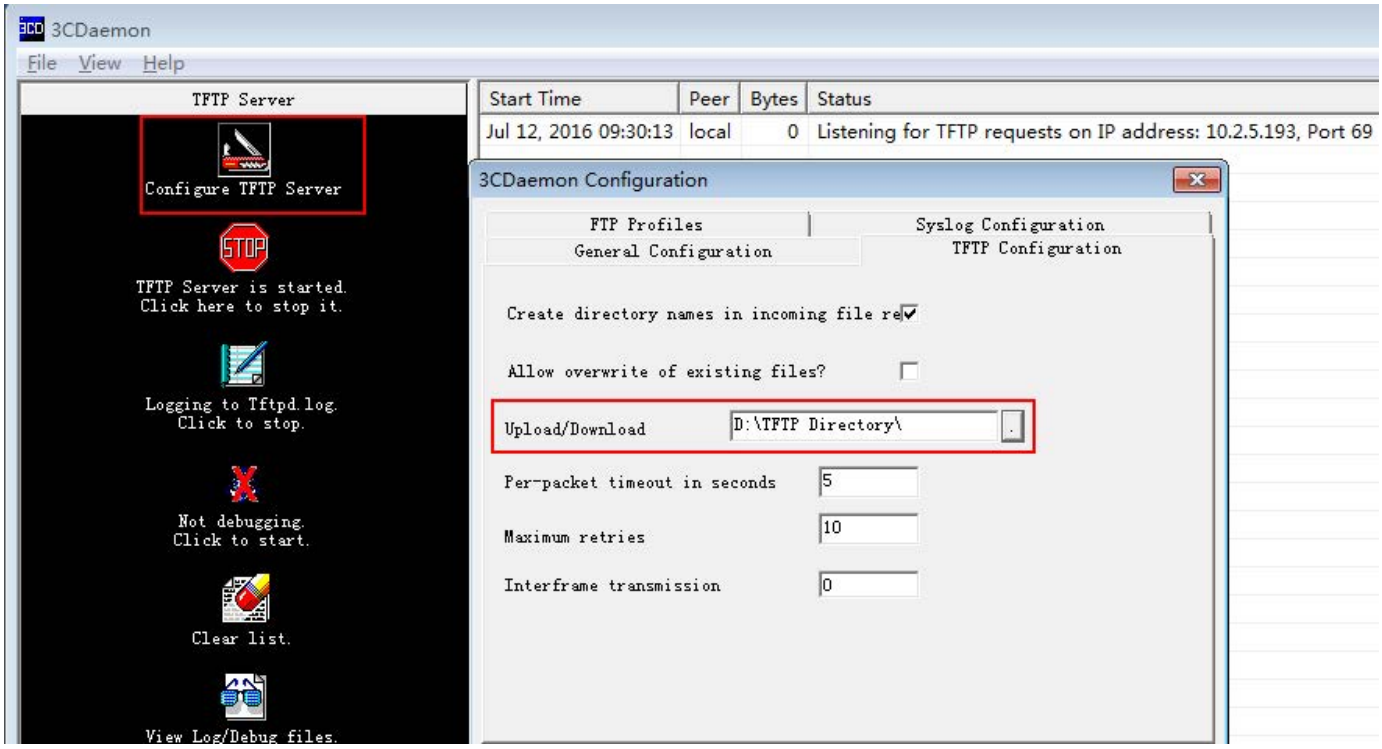
```
#!version:1.0.0.1
features.dnd_mode = 0
features.dnd.enable = 1
ringtone.url = tftp://10.2.5.193/Customring.wav
```

3. Configure the TFTP server.
4. ① Place boot files, configuration files, and resource files in the TFTP root directory (for example, D:\TFTP Directory).

6. ② Start the TFTP server. The IP address of the TFTP server is shown below:

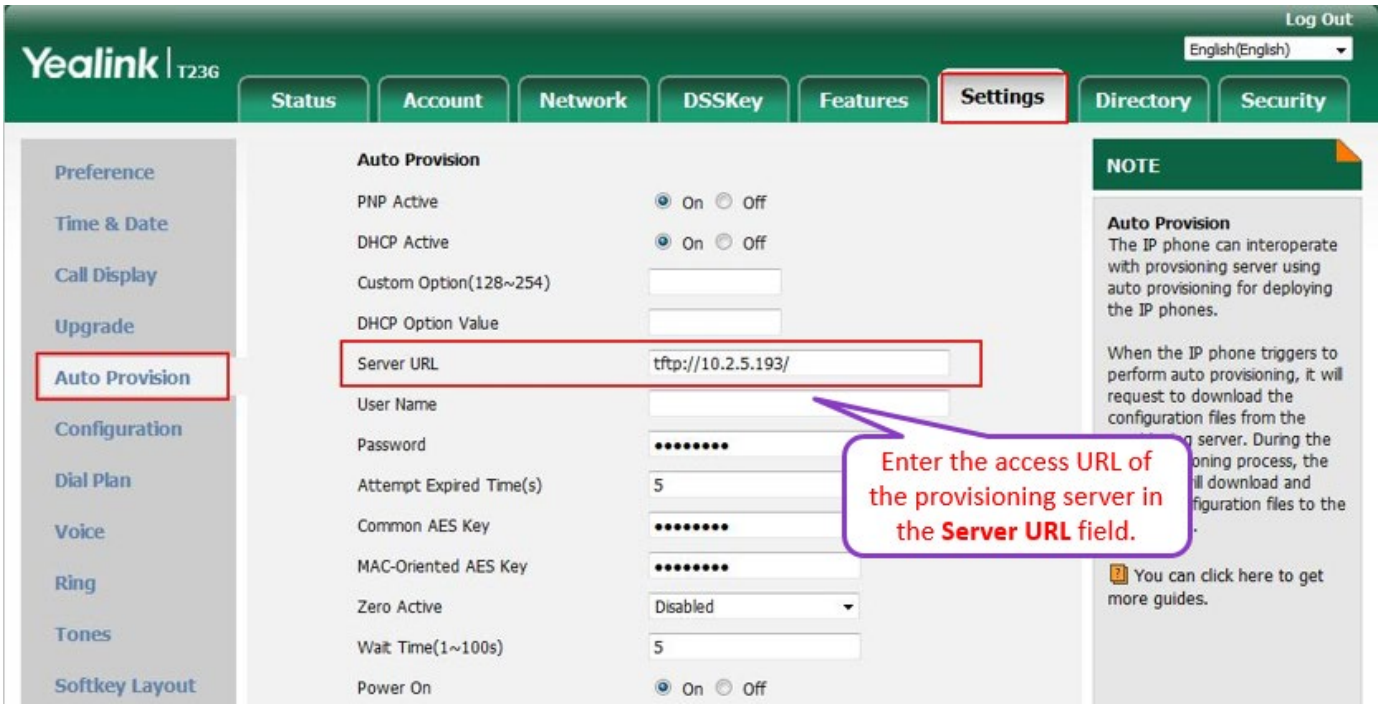


8. ③ Select Configure TFTP Server. Click the button to locate the TFTP root directory in your local system.



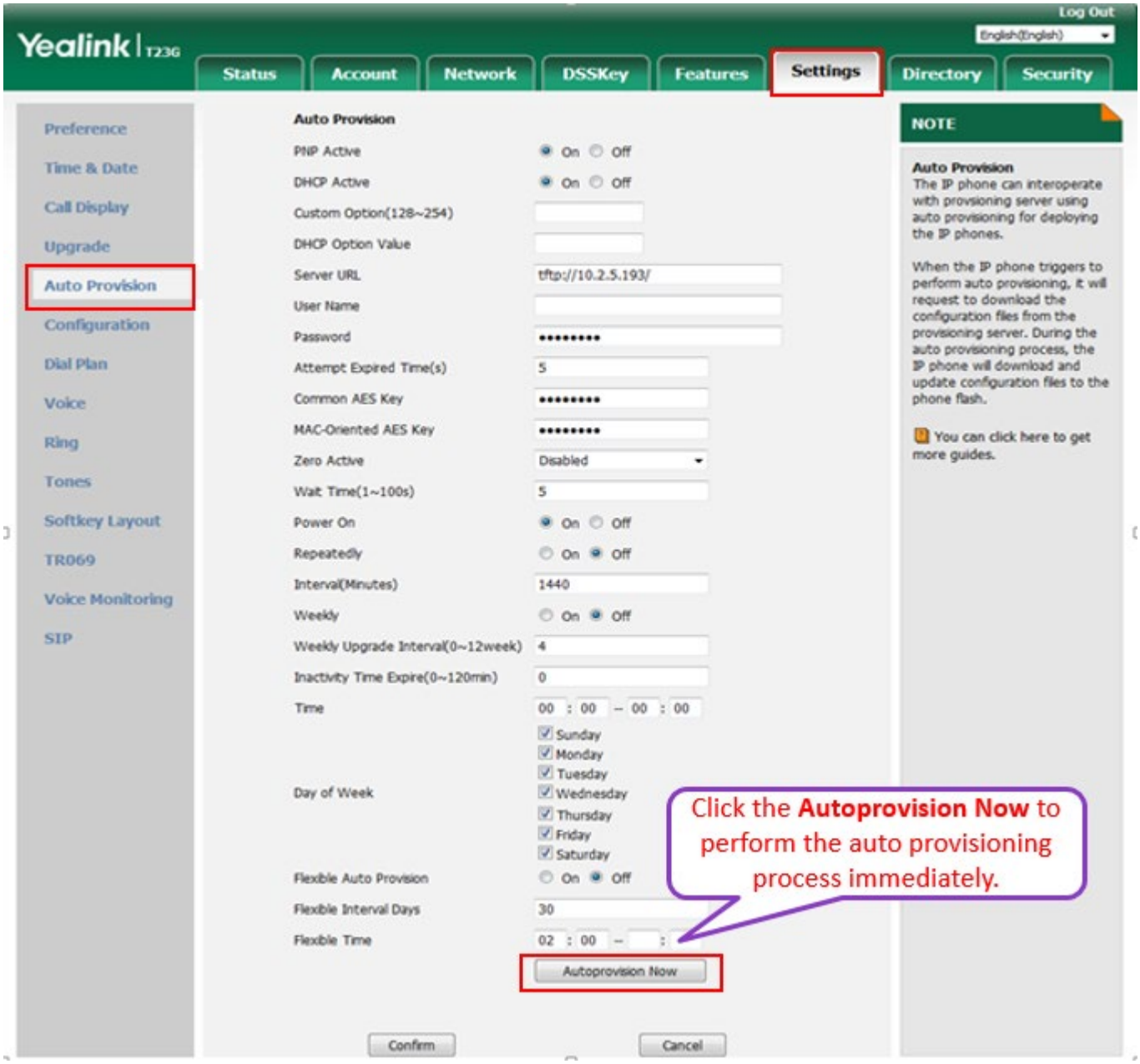
For more information on how to configure a provisioning server, refer to [Configure a Provisioning Server](#) .

4. Configure the provisioning server address on the IP phone.



For more information on how to obtain the provisioning server address, refer to [Obtain the Provisioning Server Address](#) .

5. Trigger the IP phone to perform auto provisioning.



For more information on how to perform auto provisioning, refer to [Trigger the IP Phone to Perform Auto Provisioning](#).

Manage Boot Files

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

must appear as-is in the first line	
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. The valid phone model names are: VP59, T58, T58W, CP960, CP965, T57W, T54W, T53W, T53, T53C, T48U, T48S, T48G, T46U, T46S, T46G, T43U, T42U, T42S, T42G, T41P, T41S, T40P, T40G, T33P, T33G, T31P, T31G, T31, T30P, T30, T29G, T27G, T23P, T23G, T21P_E2, T19P_E2, CP920, CP925, CP935W, T73U, T73W, T74U, T74W, T77U, T85W, T87W, T88W, T88V. Multiple phone models are separated by commas. For example, [T46S, T23G]. It is only applicable to IP phones running firmware version 83 or later.
overwrite_	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.

mode	• **0**-(Disabled) - If the value of a parameter in configuration files is left blank, deleted or commented out, the pre-configured value is kept. 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 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 model-specific configuration files are found on the server, it downloads model-unspecified configuration files. The 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. The exclude mode feature is only applicable to IP phones running firmware version 83 or later.

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:

00156574b150.boot

```
#!version:1.0.0.1
## The header above must appear as-is in the first line

   include:config <account.cfg>
   include:config "network.cfg"


overwrite_mode  = 1
```

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 IP 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 the first two digits of the hardware version of the IP phone model.

The names of the common CFG file requirements for the phone are:

Product Name	Common CFG File
VP59	y000000000091.cfg
SIP-T58W	y000000000150.cfg
SIP-T58A	y000000000058.cfg
SIP-T57W	y000000000097.cfg
SIP-T54W	y000000000096.cfg
SIP-T53W/T53/T53C	y000000000095.cfg
SIP-T48U	y000000000109.cfg
SIP-T46U	y000000000108.cfg
SIP-T43U	y000000000107.cfg
SIP-T42U	y000000000116.cfg
SIP-T48S	y000000000065.cfg
SIP-T46S	y000000000066.cfg
SIP-T42S	y000000000067.cfg
SIP-T41S	y000000000068.cfg
SIP-T48G	y000000000035.cfg

SIP-T46G	y000000000028.cfg
SIP-T42G	y000000000029.cfg
SIP-T41P	y000000000036.cfg
SIP-T40P	y000000000054.cfg
SIP-T40G	y000000000076.cfg
SIP-T33P/T33G	y000000000124.cfg
SIP-T31P/T31G/T31	y000000000123.cfg
SIP-T30P/T30	y000000000127.cfg
SIP-T31W	y000000000172.cfg
SIP-T34W	y000000000171.cfg
SIP-T44U	y000000000173.cfg
SIP-T44W	y000000000174.cfg
SIP-T29G	y000000000046.cfg
SIP-T27G	y000000000069.cfg
SIP-T23P/G	y000000000044.cfg
SIP-T21 E2/T21P E2	y000000000052.cfg
SIP-T19 E2/T19P E2	y000000000053.cfg
CP960	y000000000073.cfg
CP965	y000000000143.cfg
CP860	y000000000037.cfg
CP920	y000000000078.cfg
CP925	y000000000148.cfg
CP935W	y000000000149.cfg
T73U	y0000000000186.cfg
T73W	y0000000000183.cfg
T74U	y0000000000187.cfg
T74W	y0000000000184.cfg
T77U	y0000000000188.cfg
T85W	y0000000000196.cfg
T87W	y0000000000197.cfg

T88W(Pro)	y0000000000192.cfg
T88V Pro	y0000000000192.cfg

A 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. The valid phone models are: VP59, T58, T58W, CP960, CP965, T57W, T54W, T53W, T53, T53C, T48U, T48S, T48G, T46U, T46S, T46G, T43U, T42U, T42S, T42G, T41P, T41S, T40P, T40G, T33P, T33G, T31P, T31G, T31, T30P, T30, T29G, T27G, T23P, T23G, T21P_E2, T19P_E2, CP920, CP925, CP935W, T73U, T73W, T74U, T74W, T77U, T85W, T87W, T88W(Pro), T88V Pro. Multiple phone models are separated by commas. For example, [T46S, T23G]. It is only applicable to IP phones running firmware version 83 or later. The phone updates model-specific configurations and model-unspecified configurations. The phone model name T21P_E2 is applicable to T21P E2 and T21 E2 phones.

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 IP phone as the file name.

For example, if the MAC address of the IP 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. The valid phone models are: VP59, T58, T58W, CP960, CP965, T57W, T54W, T53W, T53, T53C, T48U, T48S, T48G, T46U, T46S, T46G, T43U, T42U, T42S, T42G, T41P, T41S, T40P, T40G, T33P, T33G, T31P, T31G, T31, T30P, T30, T29G, T27G, T23P, T23G, T21P_E2, T19P_E2, CP920, CP925, CP935W, T73U, T73W, T74U, T74W, T77U, T85W, T87W, T88W, T88V. Multiple phone models are separated by commas. For example, [T46S, T23G]. It is only applicable to IP phones running firmware version 83 or later. The phone updates model-specific configurations and model-unspecified configurations. The phone model name T21P_E2 is applicable to T21P E2 and T21 E2 phones.

• VP59/SIP-T58A/T58W/T57W/T54W/T48U/T48G/T48S/T46U/T46G/T46S/T29G/T7X/T8X IP phones support 16 accounts

• SIP-T53W/T53/T53C/T43U/T42G/T42S IP phones support 12 accounts

• CP930W-Base phones support only one assigned account

• SIP-T42U/T41P/T41S/T27G IP phones support 6 accounts

• SIP-T33P/T33G/T33 IP phones support 4 accounts

• SIP-T40P/T40G/T23P/T23G IP phones support 3 accounts

• SIP-T31P/T31G/T31/T21 E2/T21P E2 IP phones support 2 accounts

• CP960/CP965/CP920/CP925/CP935W/CP860/SIP-T19 E2/T19P E2/T30P/T30 IP phones support only one account

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.

```
settings.cfg
#!version:1.0.0.1
phone_setting.phone_lock_enable = 1
phone_setting.phone_locak_lock_key_type = 0
features.dnd_mode = 1
static.lang.wui = English
static.lang.gui = English
```

3. (Optional.) Specify different parameter values for specific phone groups.
   For example:
4. [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, the MAC-local CFG file automatically stores non-static settings modified via the web user interface or the 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 IP 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.

> 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 of sensitive information (for example, login password and registration information), you can encrypt configuration files using the 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 the 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 IP 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. 3CDaemon and TFTPD32 are free applications for Windows. You can download 3CDaemon online and TFTPD32 online.

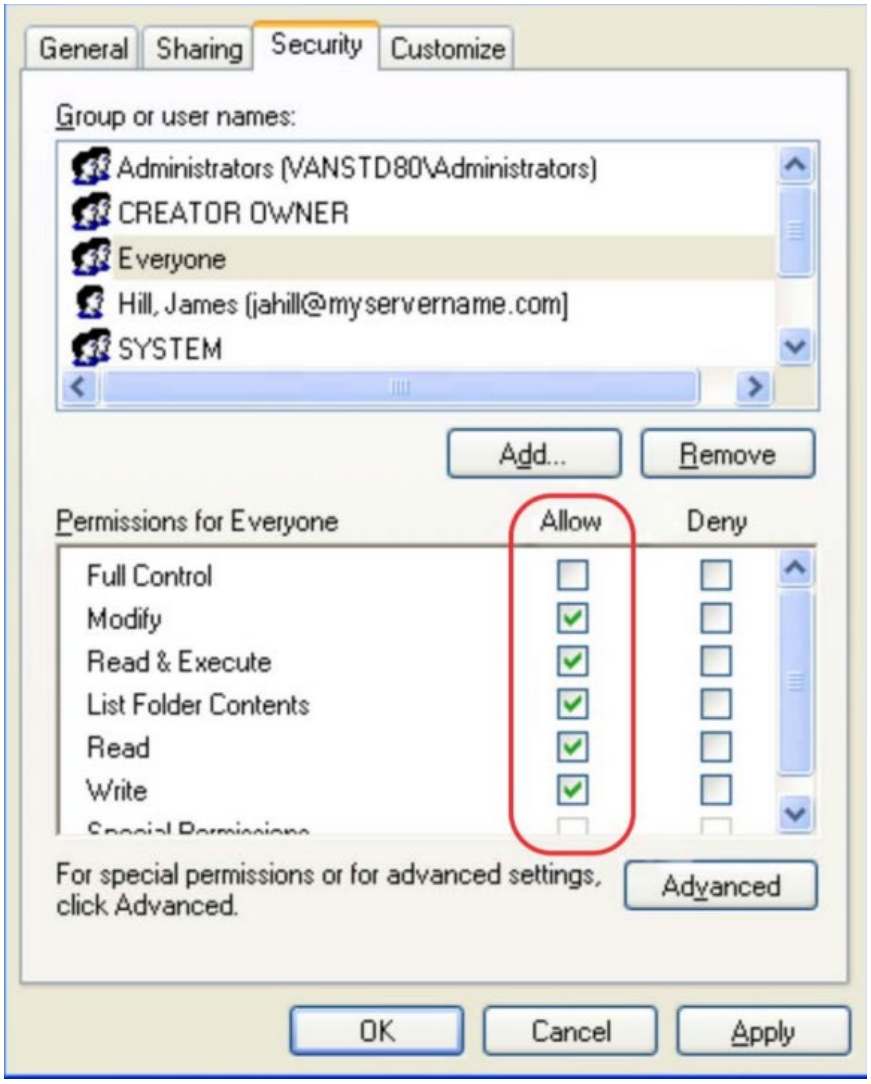
For more information on how to configure FTP and HTTPS servers, refer to Configure FTP Server and Configure HTTPS Server.

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 organization.
4. An example of configuration on the Windows platform is shown below:



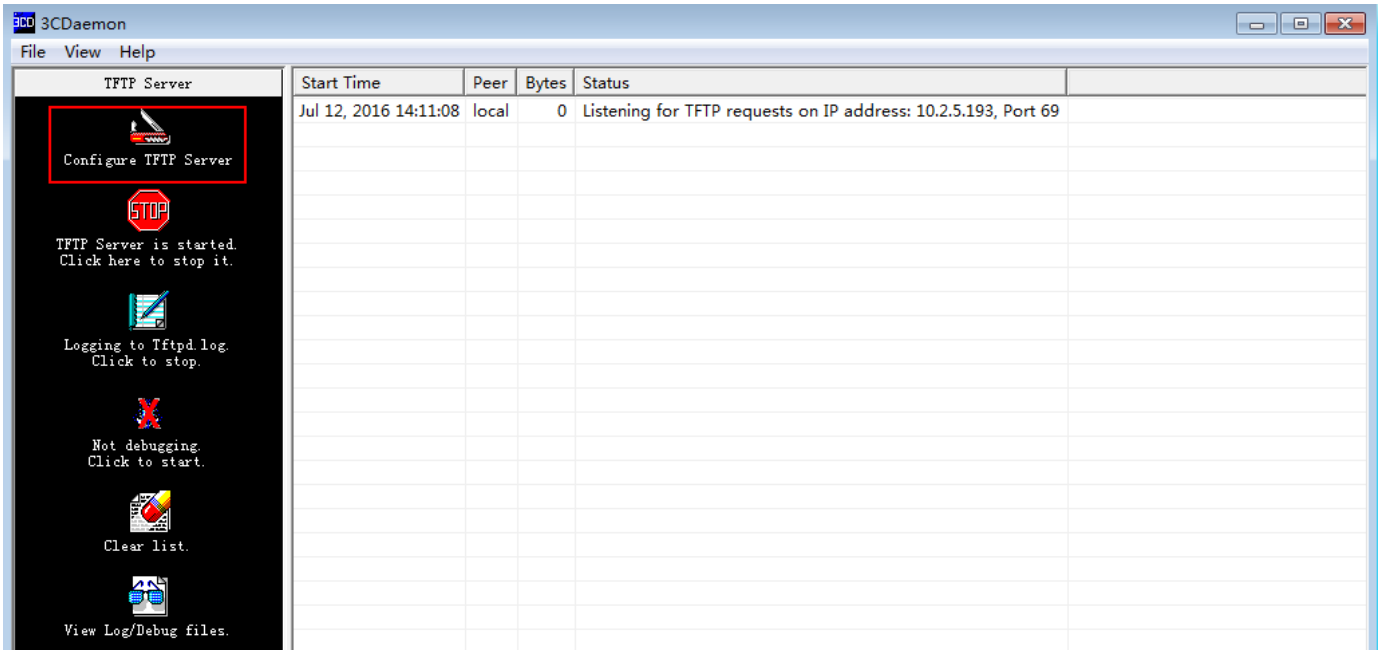
Configure a TFTP Server

If you have a 3CDaemon application installed on your local system, use it directly. Otherwise, download and install it.

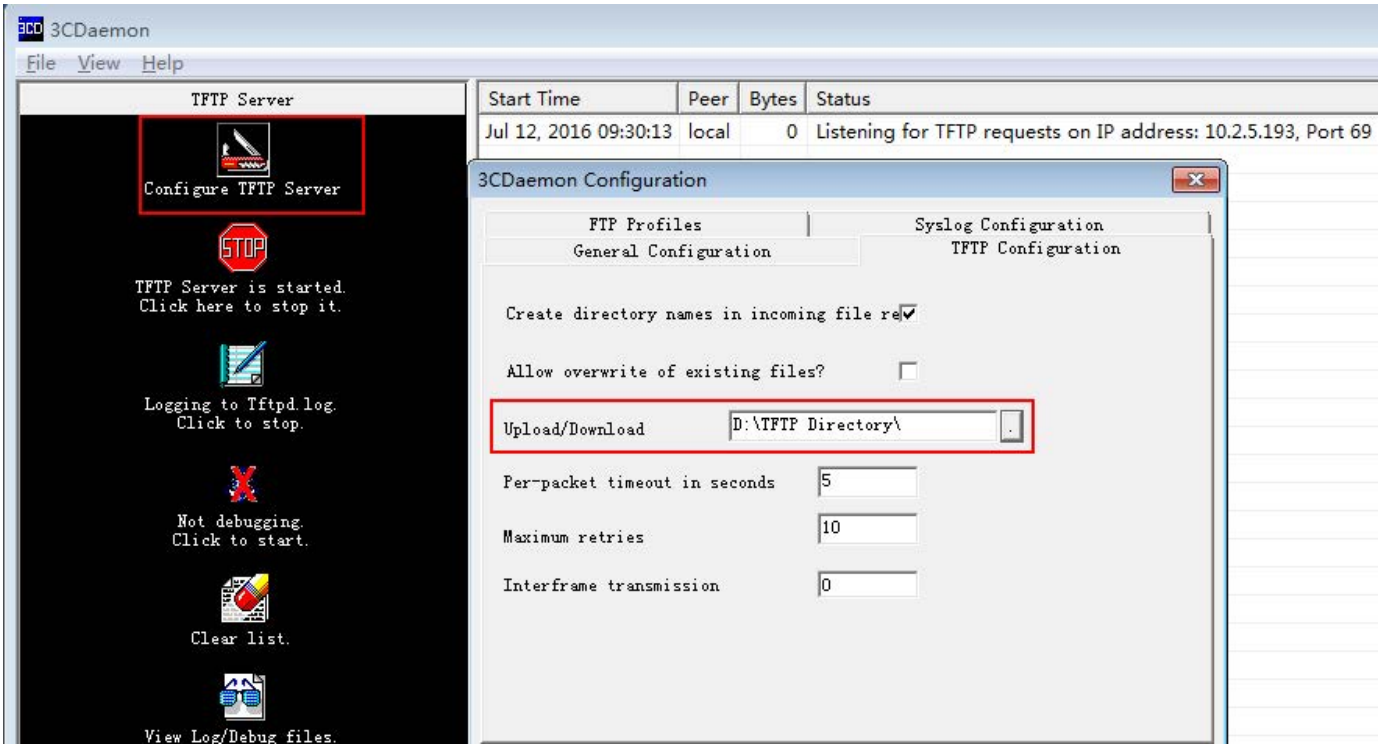
To configure a TFTP server:

1. Double-click 3CDaemon.exe to start the application.

   A configuration page is shown 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 IP phones can obtain the provisioning server address in the following ways:

- Zero Touch
- Plug and Play (PnP) Server
- DHCP Options
- Phone Flash
- Configuring Wildcard of the Provisioning Server URL

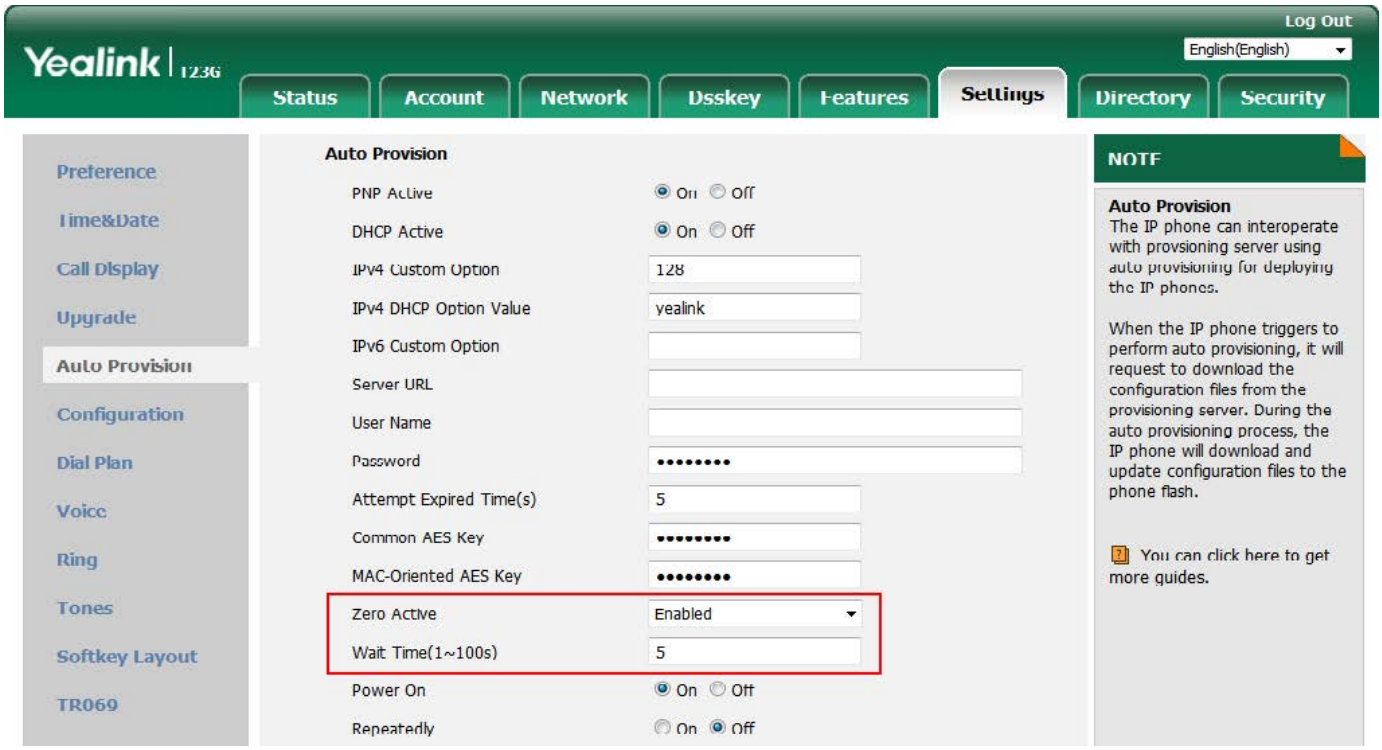
The priority of obtaining the provisioning server address is as follows: Zero Touch>PnP Server>DHCP Options (for IPv4: IPv4 Custom option>option 66>option 43; for IPv6: IPv6 Custom option>option 59) >Phone Flash. The following sections detail the process of each way (take the SIP-T23G IP phone as an example).

Zero Touch

Zero Touch allows you to configure the network parameters and provisioning server address via phone user interface during startup. This feature is helpful when there is a system failure on the IP phone. To use Zero Touch, make sure this feature is enabled.

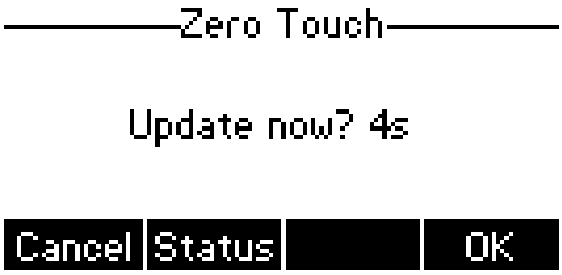
To configure zero touch via the web user interface:

1. Click **Settings** > **Auto Provision**.
2. Select **Enabled** from the pull-down list of **Zero Active**.
3. Enter the desired waiting time in the **Wait Time(1~100s)** field. The default value is **5**.



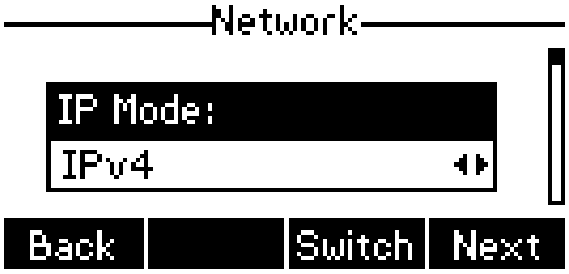
4. Click **Confirm** to accept the change.

   When Zero Touch is enabled, there will be a configuration wizard during startup:



6. Press the **OK** soft key.

   The network parameters are configurable via the phone user interface:



8. Press the **Next** soft key after finishing the network settings.

   Configure the provisioning server address, authentication user name (optional), and password (optional) in the **Auto Provision** screen.

   An example of the screenshot is shown below:

10. Press the **OK** soft key.

    After the above configuration is completed, the IP phone will connect to the configured provisioning server and perform auto-provisioning during startup.

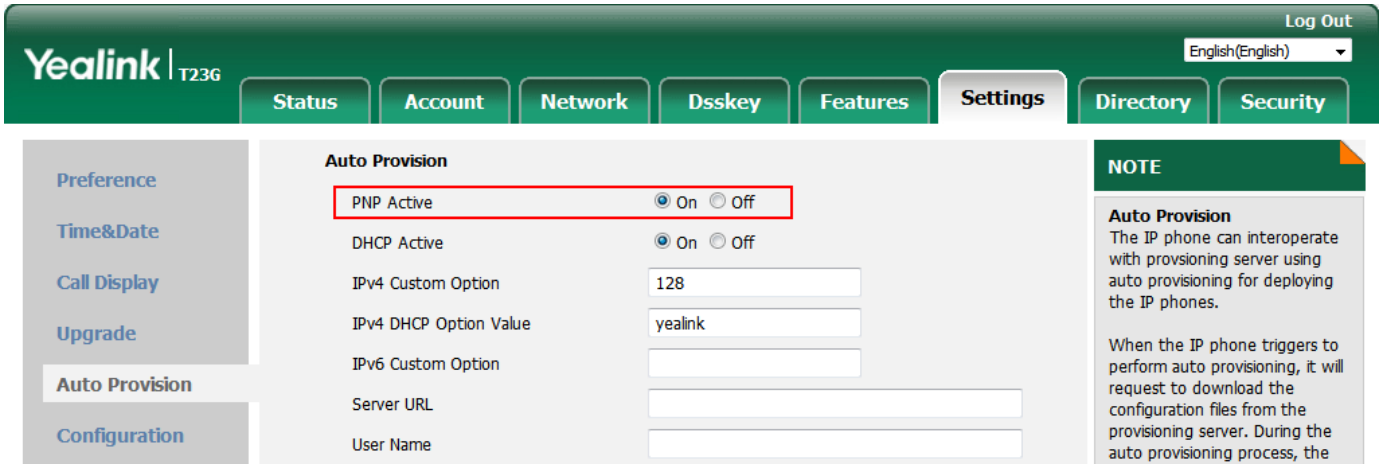
Plug and Play Server

Yealink IP 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 the web user interface:

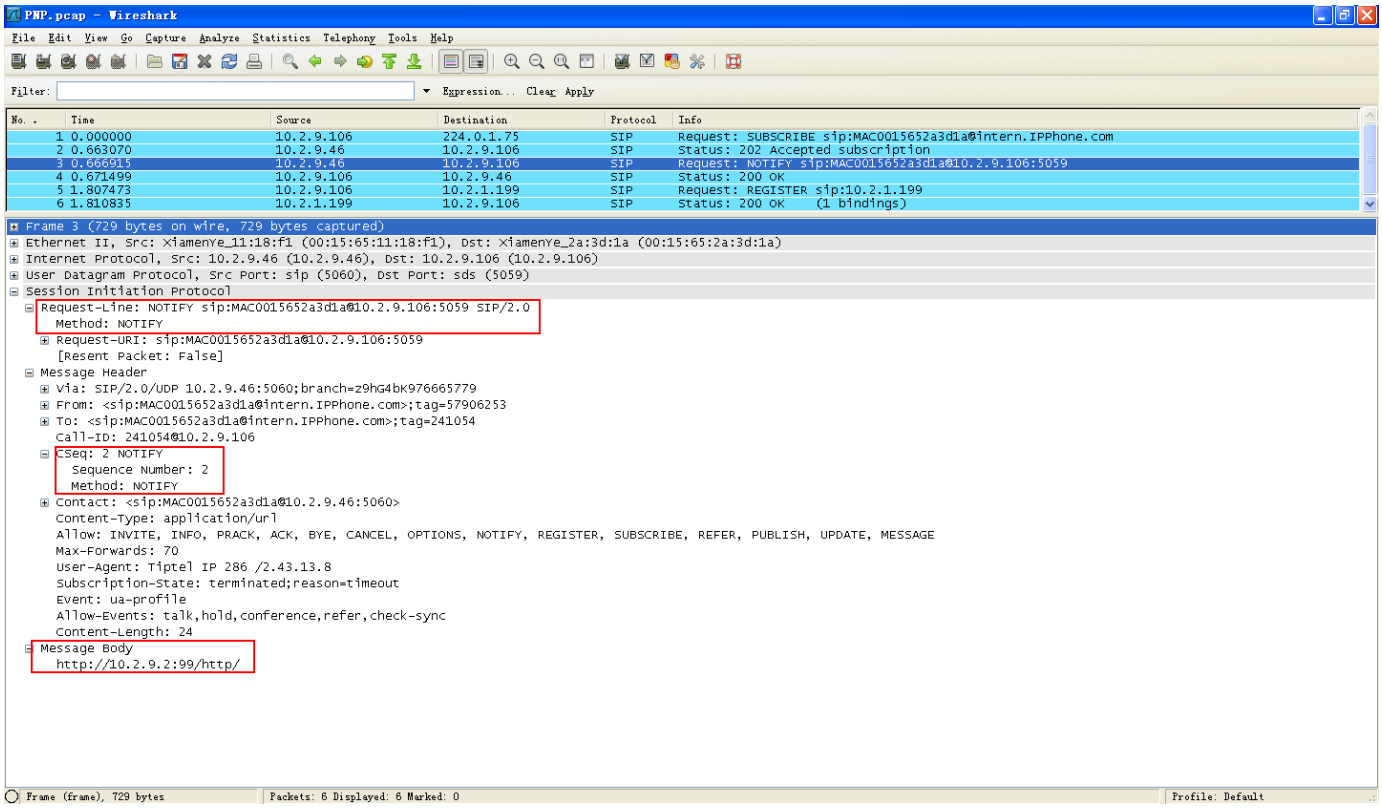
1. Click **Settings** > **Auto Provision**.

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.



5. 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 IP 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 that is used to transfer vendor-specific information.

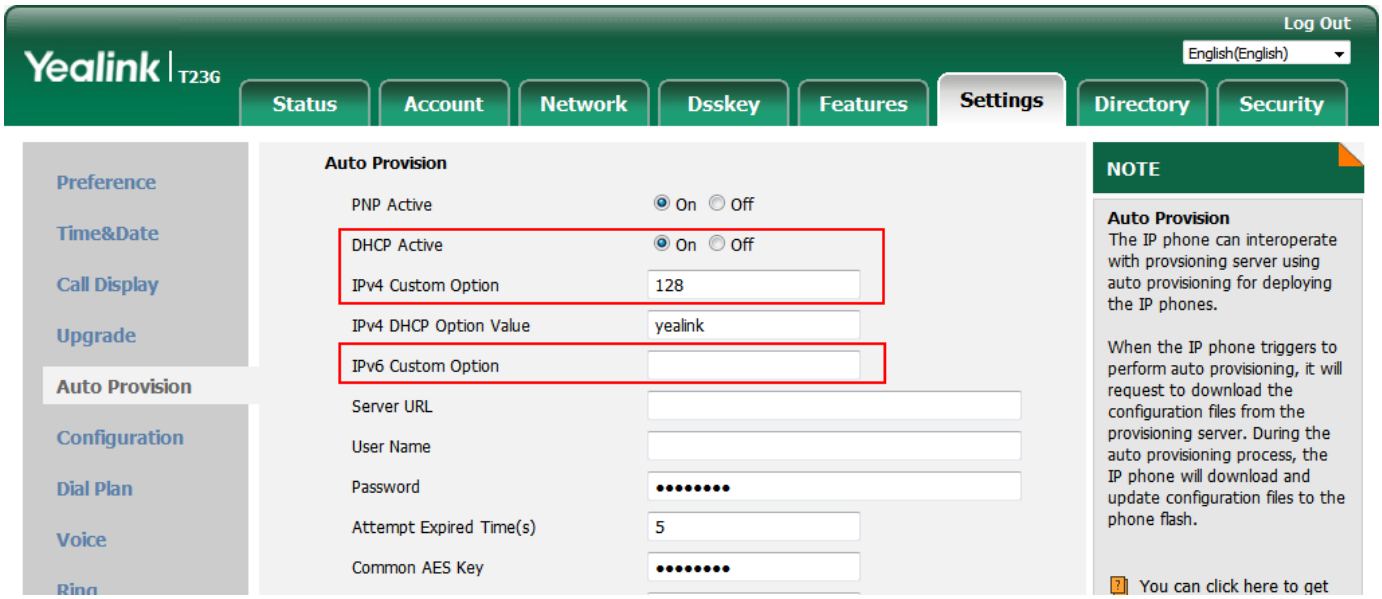
If you are using an IPv6 network, the phone will automatically detect option 59 for obtaining the provisioning server address. DHCP option 59 is used to specify a URL for the boot file to be downloaded by the client.

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.

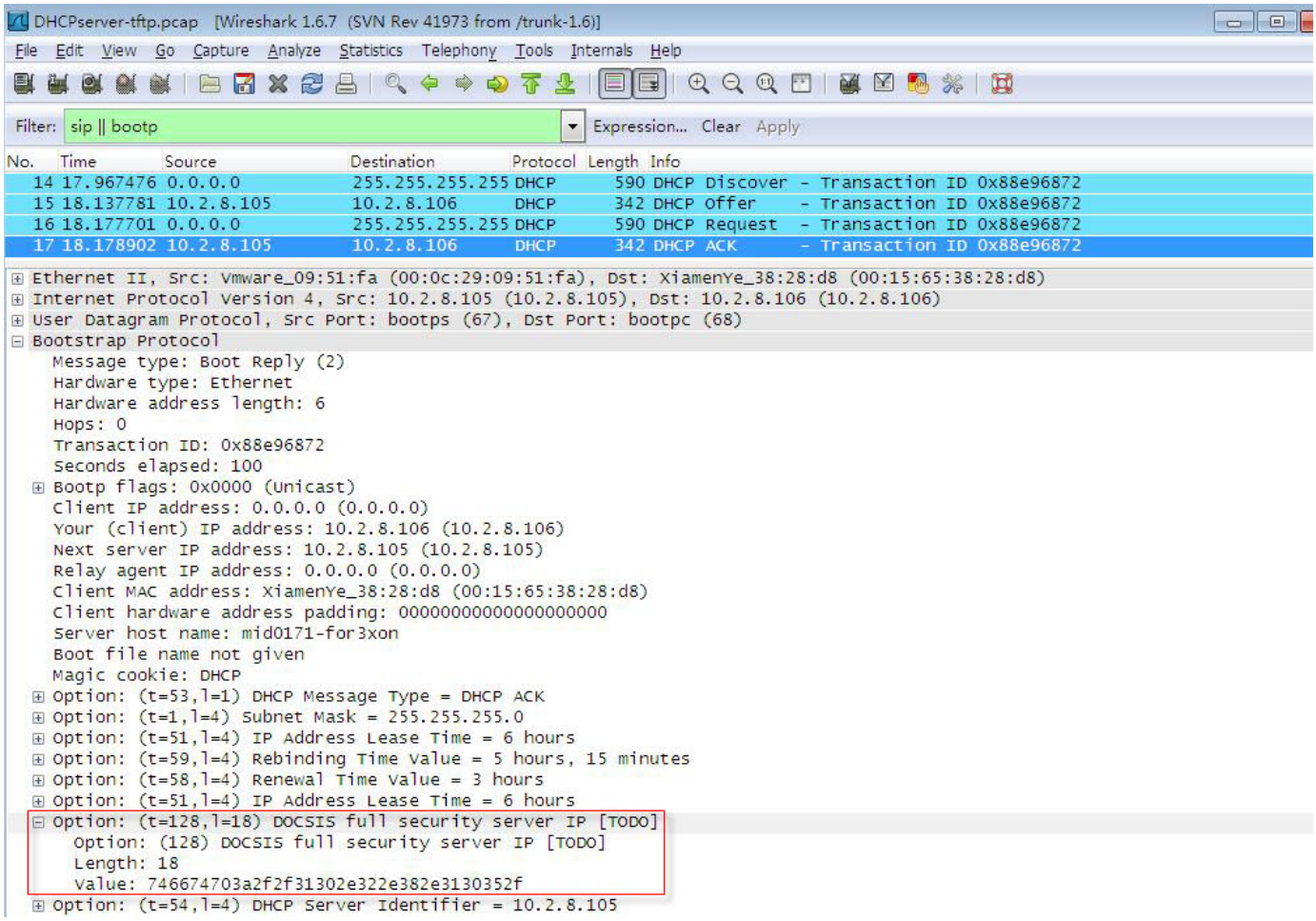
To configure the DHCP option via the web user interface:

1. Click **Settings** > **Auto Provision**.
2. Mark the **On** check box in the **DHCP Active** field.
3. If you are using an IPv4 network, enter the desired value in the **IPv4 Custom Option** field.

4. If you are using an IPv6 network, enter the desired value in the **IPv6 Custom Option** field.



5. Click **Confirm** to accept the change.
6. During startup, the phone will broadcast a DHCP request with DHCP options for obtaining the provisioning server address. The provisioning server address will be found in the received DHCP response message.
7. 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.
8. For more information on the DHCP options, refer to the latest Administrator Guide for your phone on Yealink Technical Support.
9. The following figure shows the example messages of obtaining the TFTP server address from an IPv4 custom DHCP option:



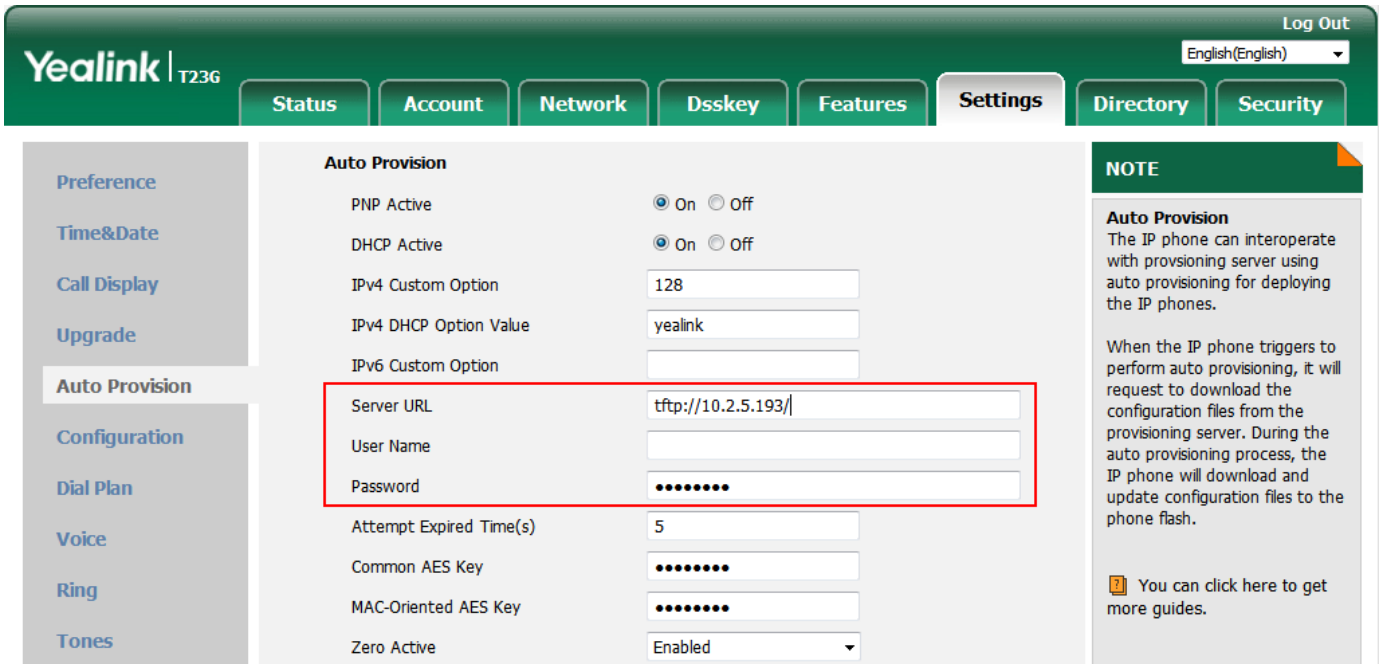
Right-click the root node of the custom option (for example, option 128) shown in the above figure, and select **Copy** > **Bytes** > **Printable Text Only**. Paste the copied text in your favorite text editor to check the address, for example, tftp://192.168.1.100/.

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 the web user interface:

1. Click on **Settings** > **Auto Provision**.
2. Enter the URL, user name, and password of the provisioning server in the **Server URL**, **User Name,** and **Password** fields, 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 IP Phone to Perform Auto Provisioning.

Configure the 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 are located.

For more information on the parameter, refer to the latest IP Phones Description of Configuration Parameters in CFG Files or the 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.

> 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 SIP-T46G IP 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 SIP-T46G IP phones using the wildcard feature.

1. Create two directories in the root directory of the provisioning server.
2. Configure the directory names of these two directories to be "T42G" and "T46G".
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 "T46G" for the SIP-T46G IP 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” in the URL with “T42G” for the SIP-T42G IP phones and “T46G” for the SIP-T46G IP phones. When performing auto provisioning, the SIP-T42G IP phones, and the SIP-T46G IP 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/T46G” respectively. If no matched MAC-Oriented boot files are found on the server, the SIP-T42G IP phones and the SIP-T46G IP 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/T46G” respectively.

If the URL is configured as “tftp://192.168.1.100/$PN/$MAC.boot” on the DHCP server, the SIP-T42G IP phones, and the SIP-T46G IP phones will replace the characters “$PN” with “T42G” and “T46G” respectively, and replace the characters “$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 IP Phone to Perform Auto Provisioning

This chapter introduces the following methods to trigger the IP 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
- Auto Provisioning via PIN Code

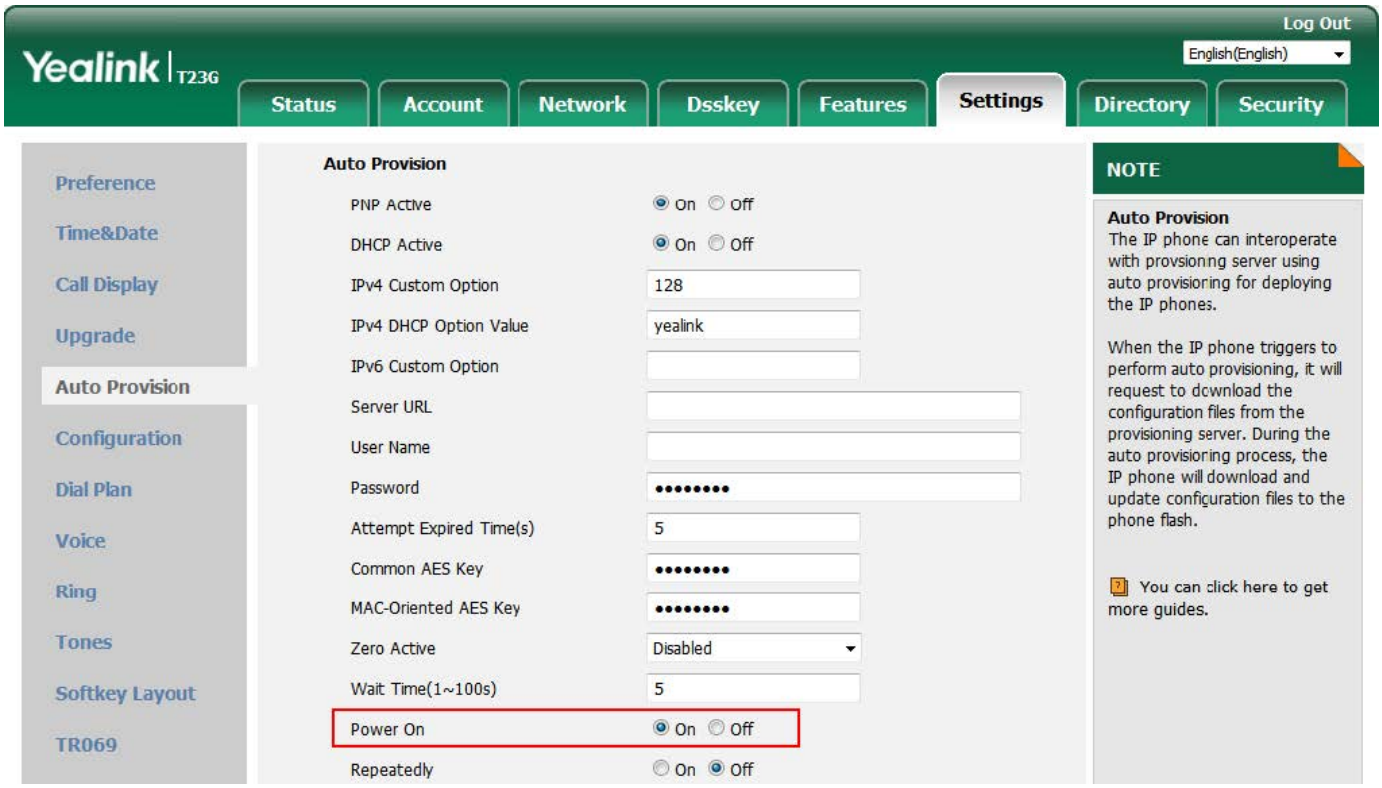
When there is an active call on the IP phone during auto provisioning, the IP phone will detect the call status every 30 seconds. If the call is released within 2 hours, the auto-provisioning will be performed as usual. Otherwise, the process will end due to a timeout.

Power On

The IP phone performs 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.



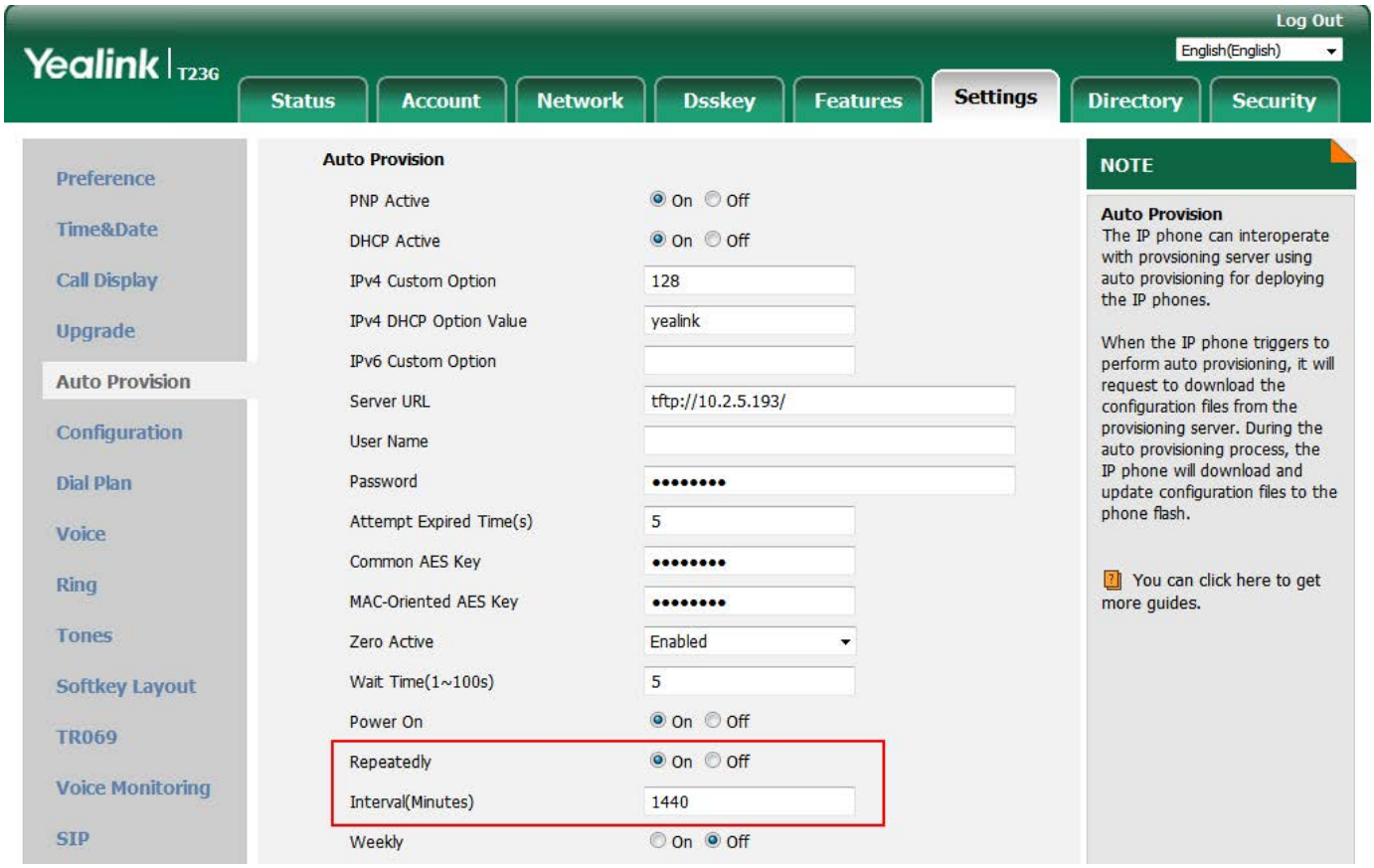
3. Click **Confirm** to accept the change.

Repeatedly

The IP phone performs the auto provisioning at regular intervals. You can configure the interval for the repeated mode. The default interval is 1440 minutes.

To activate the repeat mode via the 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.

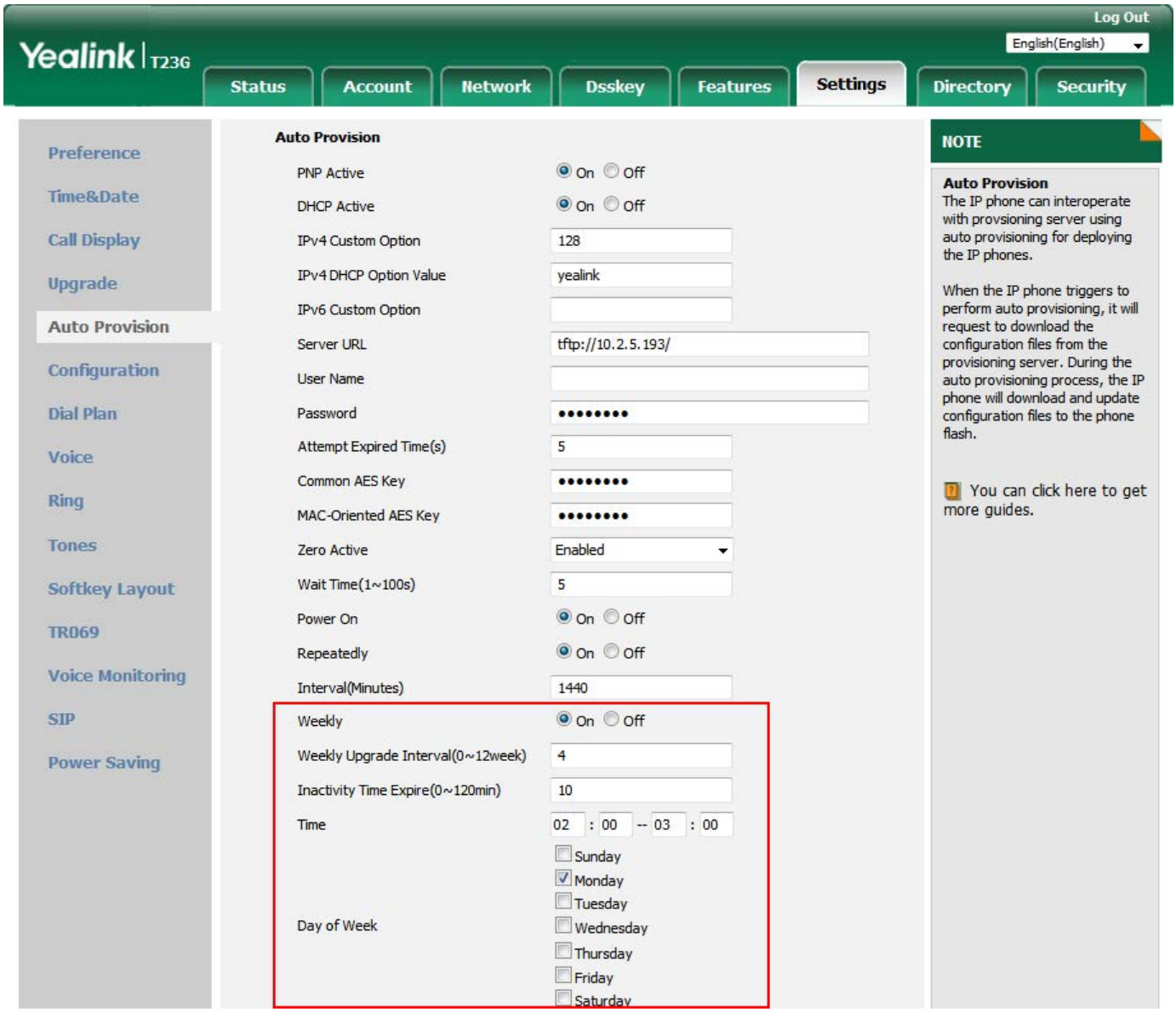
Weekly

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 a regular week. For example, you can configure the IP phone to check and update the 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. 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.

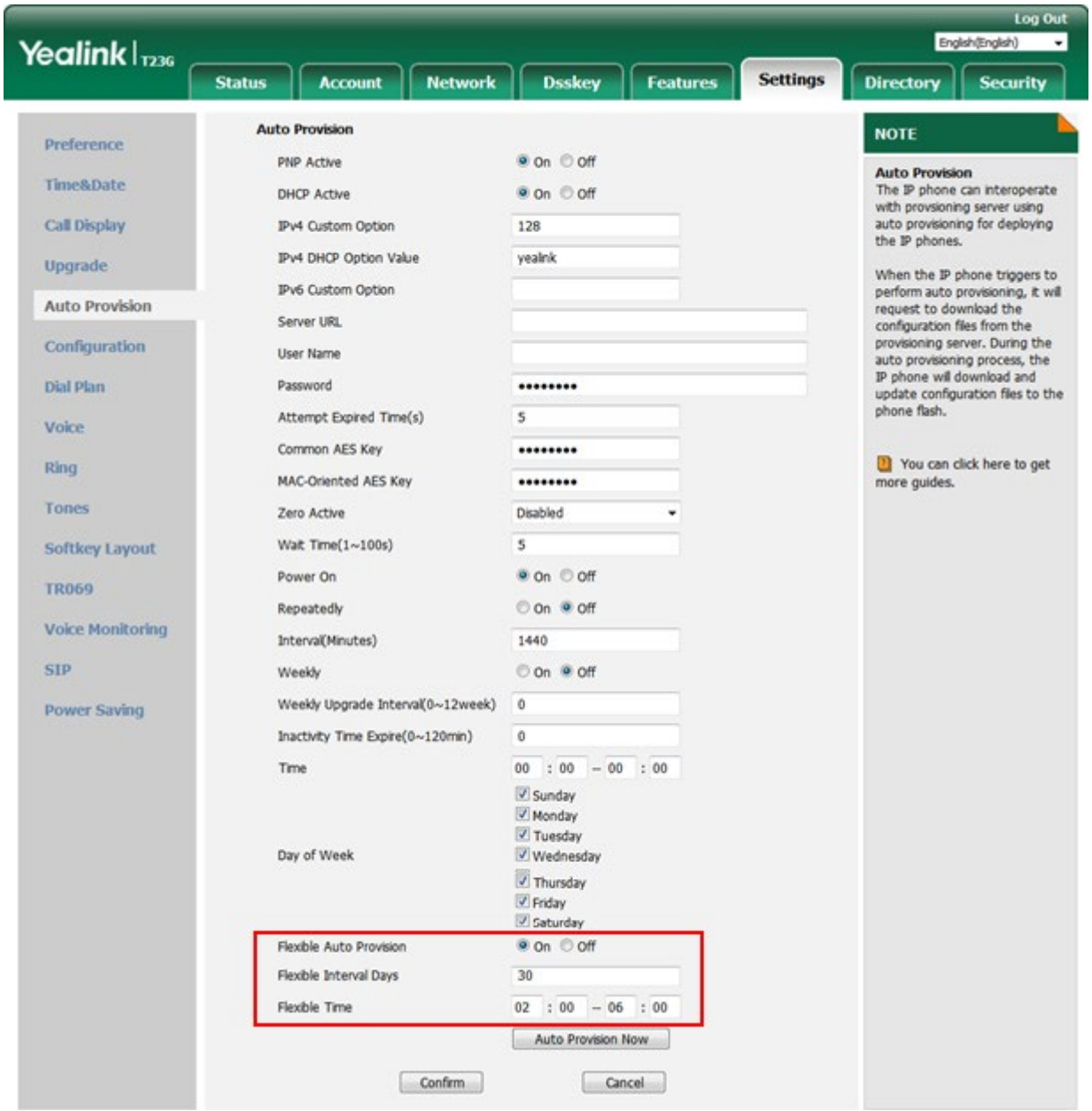
To activate the flexible auto-provision mode via the web user interface:

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.

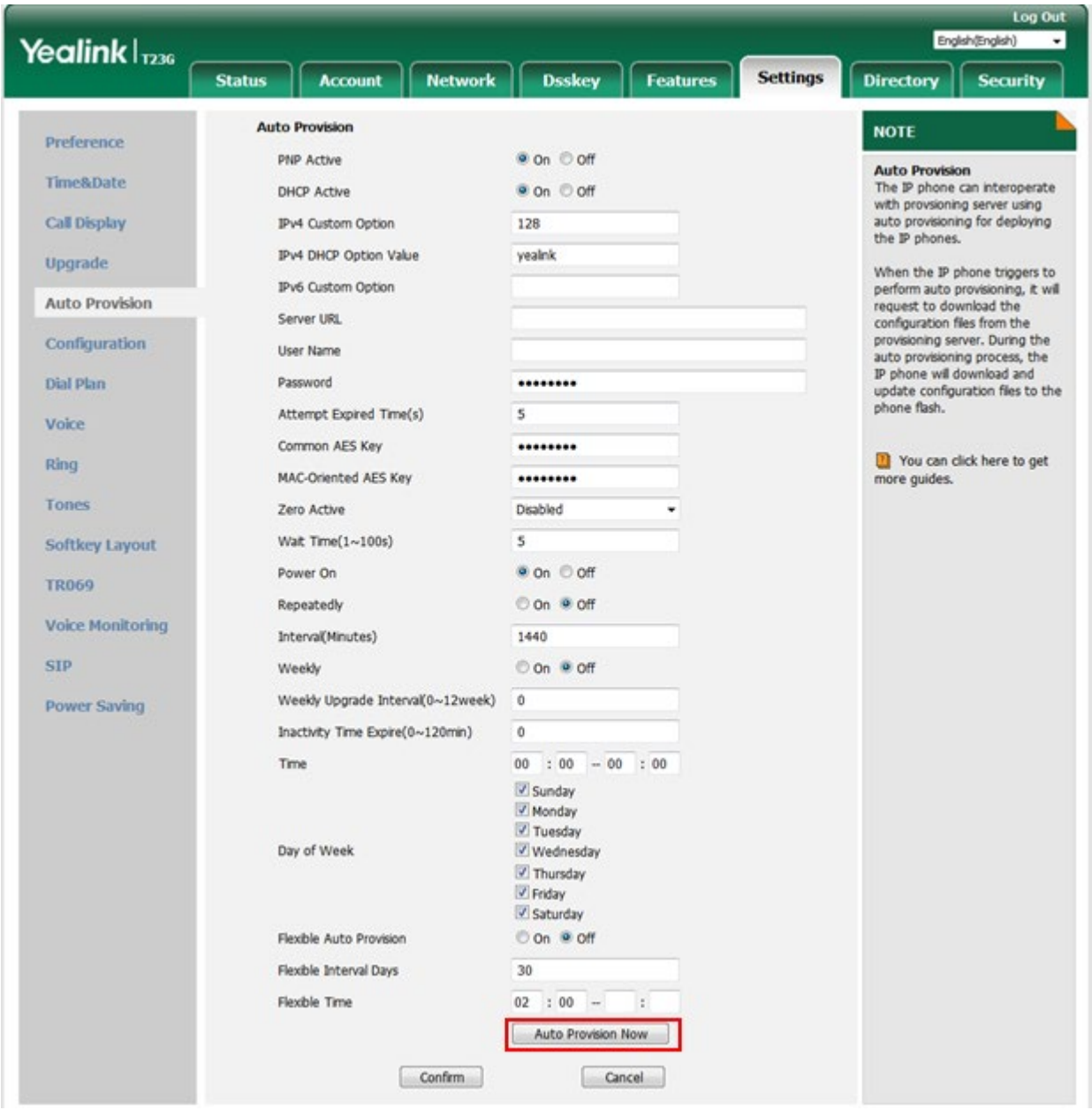
Auto Provision Now

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 the 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.

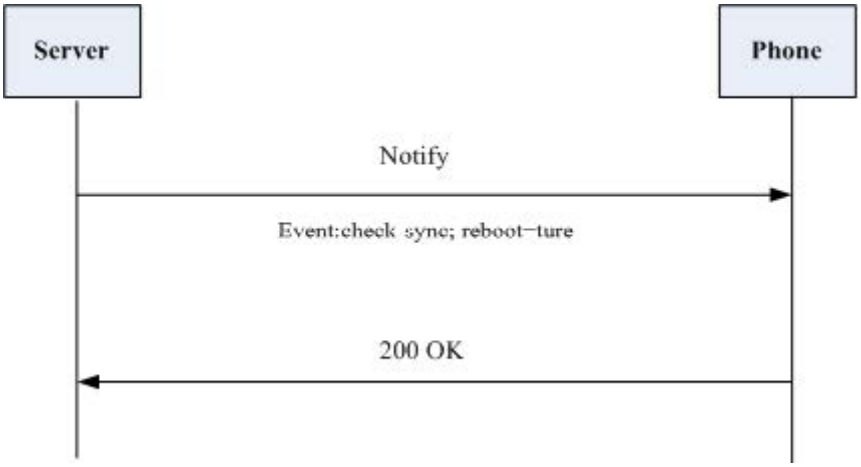
SIP NOTIFY Message

The IP phone will perform auto provisioning when receiving a SIP NOTIFY message that contains the header "Event: check-sync". Whether the IP phone reboots or not depends on the value of the parameter [redacted]. 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 [redacted], refer to the latest IP Phones

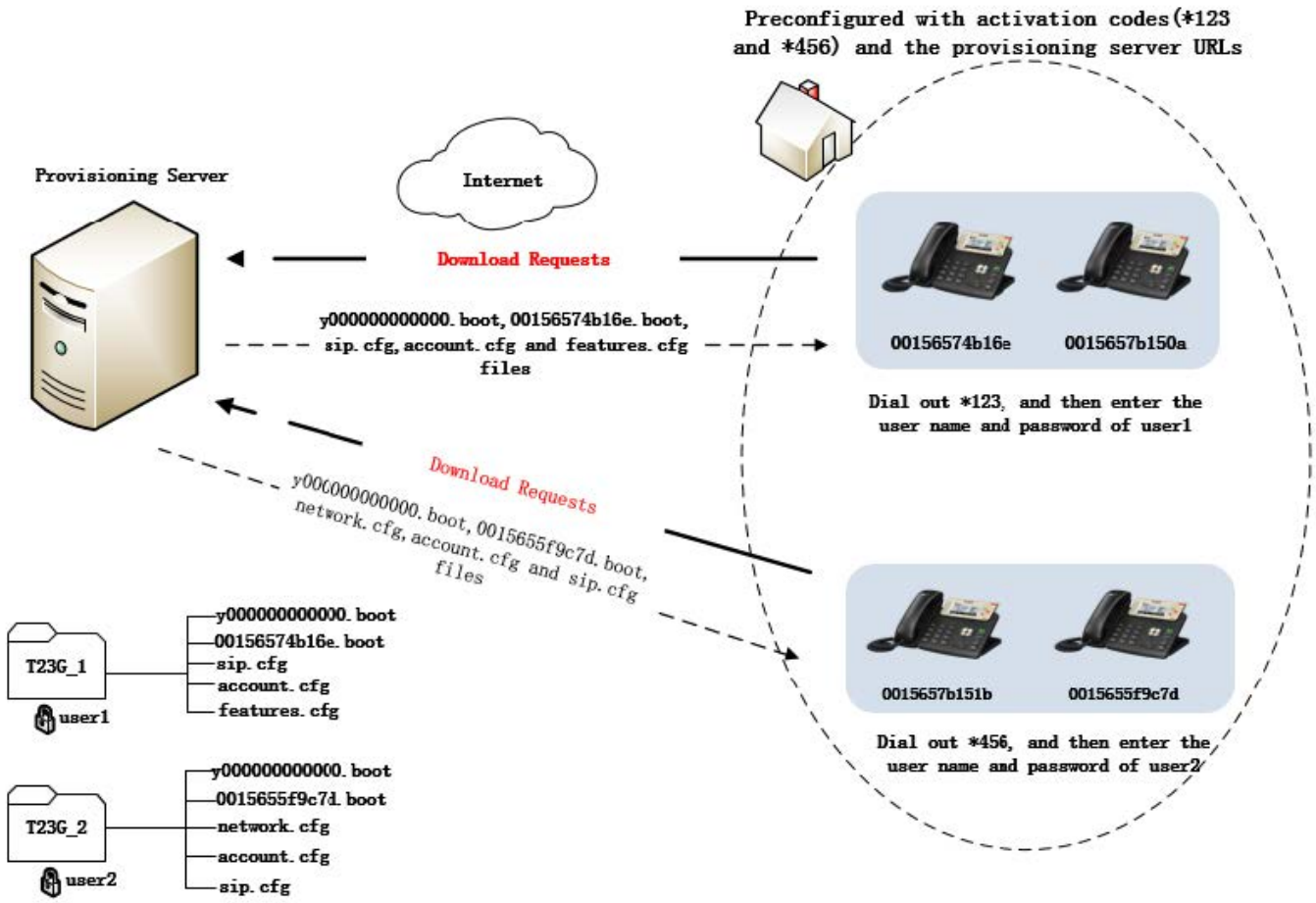
Description of Configuration Parameters in CFG Files or Administrator Guide for your phone on Yealink Technical Support. This method requires server support.

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 (for example, T23G_1 and T23G_2) on the provisioning server.
2. Store boot files and configuration files in each directory on the provisioning server.
3. Configure a username and password for each directory on the provisioning server.
4. The username 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/T23G_1/
static.autoprovision.2.code = *456
static.autoprovision.2.url = http://192.168.1.30/T23G_2/
```

5. Send the specified activation code, associated user name, and password to each end-user.
6. The user can set up the IP phone, and then input the activation code (for example, *123) after the phone startup.
7. The LCD screen will prompt the following dialog box:

7. Press the **OK** soft key to trigger the IP phone to perform auto provisioning.
   The LCD screen will prompt the following input box:

8. Enter the user name and password in the **User Name** and **Password** fields, 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!".
10. 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.
11. 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.
12. 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):

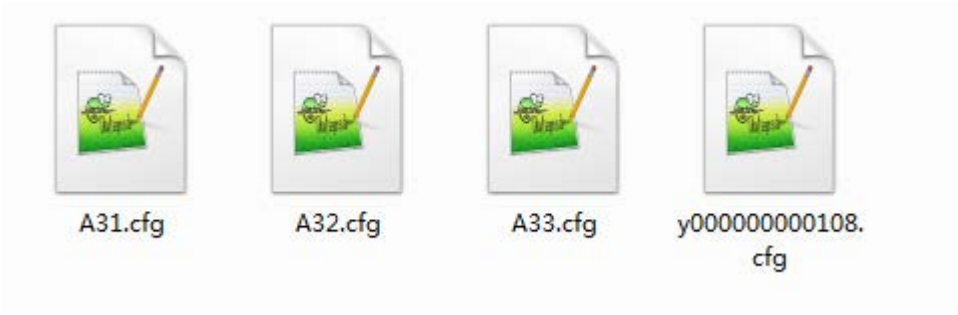
```
#(Optional.) Configure the code name for triggering auto provisioning.
static.autoprovision.X.name
#Configure the activation code.
static.autoprovision.X.code
#Configure the URL of the provisioning server.
static.autoprovision.X.url
#Configure the username and password for downloading boot files and configuration files. If configured, the LCD screen will not prompt for user name and password.
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.

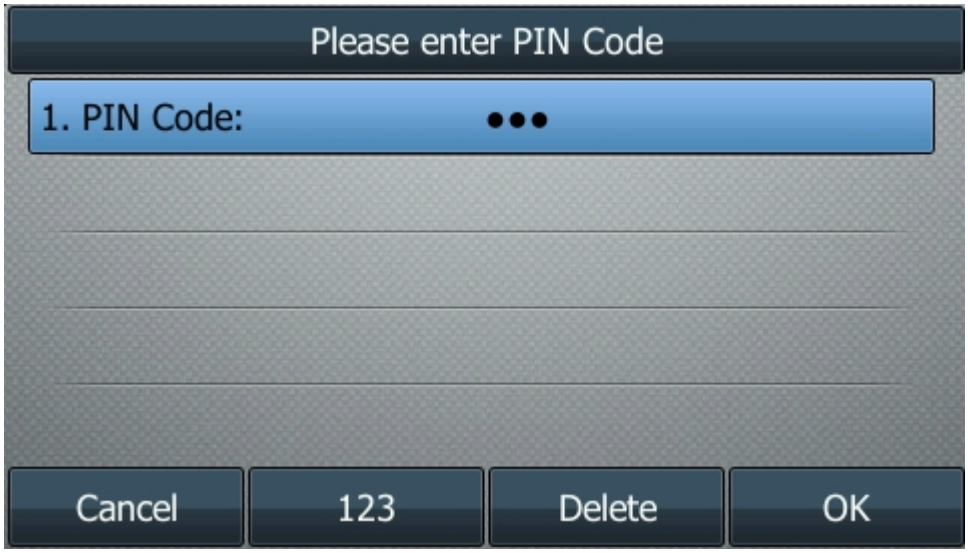
The following lists the processes for triggering auto provisioning via PIN code:

1. Prepare the common CFG file and PIN CFG files in your local system.
2. **Example**:
3. 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.
4. static.custom_mac_cfg.url = http://<serverIPaddress>/$pin.cfg
5. **Example:**
6. static.custom_mac_cfg.url = http://10.2.11.101/$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 IP 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 IP phone will try to download the MAC-Oriented boot file first 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 IP 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 first, 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 IP 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.

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's flash. Generally, updated configurations will automatically take effect after auto-provisioning is completed. For the update of some specific configurations that 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 IP 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 have not been changed. The IP phone will complete the auto-provisioning without a repeated update. This is used to avoid unnecessary restarts and the impact of phone use. On the contrary, the IP 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 that 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 the Yealink Configuration Encryption Tool User Guide.

Use the 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.

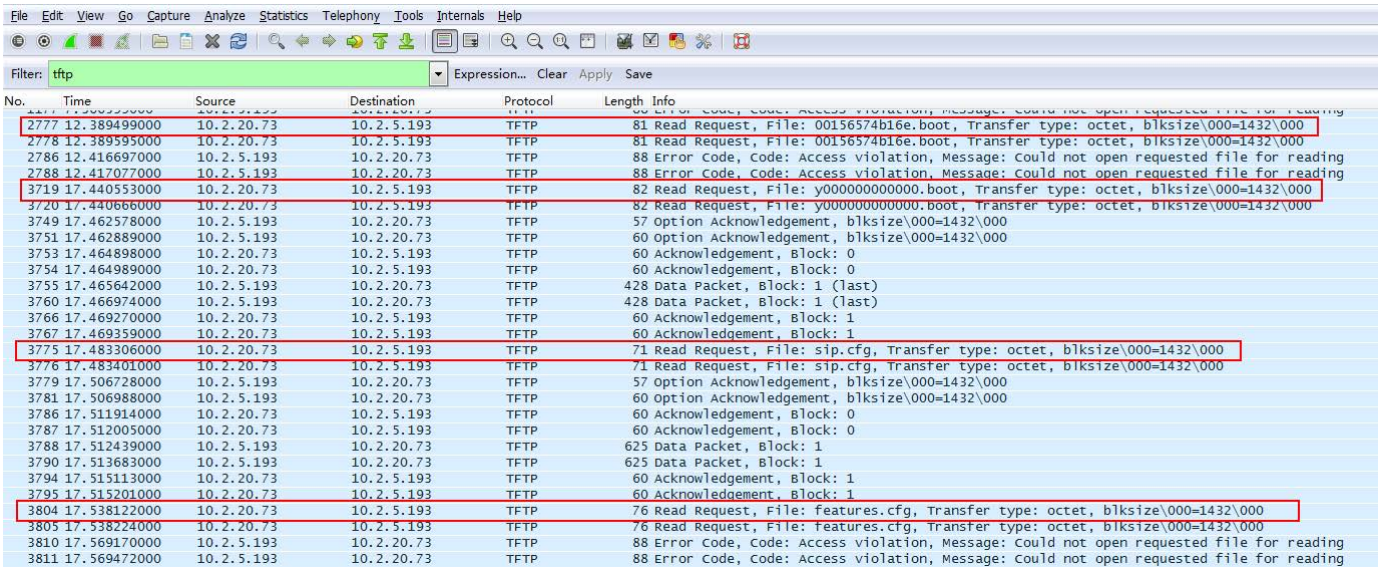
> Note that if the personalized settings are static settings, they cannot be kept after auto-provisioning because the static settings will never be saved in the <MAC>-local.cfg file. For more information, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

Verify Configurations

After auto-provisioning, you can then verify the update via the phone user interface or the web user interface of the phone.

During auto provisioning, you can monitor the download requests and response messages using a packet capture tool such as Wireshark (with WinPcap/Npcap). The following shows some examples.

Example 1: Yealink SIP-T23G IP phone downloads the boot file and configuration files from the TFTP server.

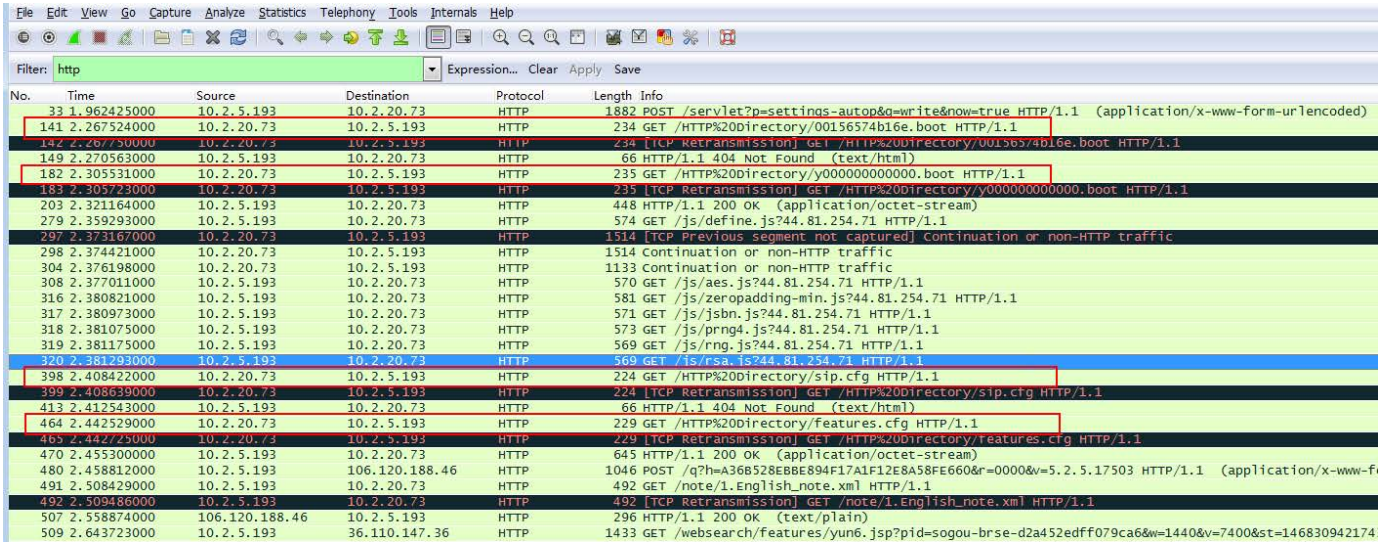


No.	Time	Source	Destination	Protocol	Length	Info
2777	12.389499000	10.2.20.73	10.2.5.193	TFTP	81	Read Request, File: 00156574b16e.boot, Transfer type: octet, blksize\000=1432\000
2778	12.389595000	10.2.20.73	10.2.5.193	TFTP	81	Read Request, File: 00156574b16e.boot, Transfer type: octet, blksize\000=1432\000
2786	12.416697000	10.2.5.193	10.2.20.73	TFTP	88	Error Code, Code: Access violation, Message: Could not open requested file for reading
2788	12.417077000	10.2.5.193	10.2.20.73	TFTP	88	Error Code, Code: Access violation, Message: Could not open requested file for reading
3719	17.440553000	10.2.20.73	10.2.5.193	TFTP	82	Read Request, File: y000000000000.boot, Transfer type: octet, blksize\000=1432\000
3720	17.440666000	10.2.20.73	10.2.5.193	TFTP	82	Read Request, File: y000000000000.boot, Transfer type: octet, blksize\000=1432\000
3749	17.462578000	10.2.5.193	10.2.20.73	TFTP	57	Option Acknowledgement, blksize\000=1432\000
3751	17.462889000	10.2.5.193	10.2.20.73	TFTP	60	Option Acknowledgement, blksize\000=1432\000
3753	17.464898000	10.2.20.73	10.2.5.193	TFTP	60	Acknowledgement, Block: 0
3754	17.464989000	10.2.20.73	10.2.5.193	TFTP	60	Acknowledgement, Block: 0
3755	17.465642000	10.2.5.193	10.2.20.73	TFTP	428	Data Packet, Block: 1 (last)
3760	17.466974000	10.2.5.193	10.2.20.73	TFTP	428	Data Packet, Block: 1 (last)
3766	17.469270000	10.2.20.73	10.2.5.193	TFTP	60	Acknowledgement, Block: 1
3767	17.469359000	10.2.20.73	10.2.5.193	TFTP	60	Acknowledgement, Block: 1
3775	17.483306000	10.2.20.73	10.2.5.193	TFTP	71	Read Request, File: sip.cfg, Transfer type: octet, blksize\000=1432\000
3776	17.483401000	10.2.20.73	10.2.5.193	TFTP	71	Read Request, File: sip.cfg, Transfer type: octet, blksize\000=1432\000
3779	17.506728000	10.2.5.193	10.2.20.73	TFTP	57	Option Acknowledgement, blksize\000=1432\000
3781	17.506988000	10.2.5.193	10.2.20.73	TFTP	60	Option Acknowledgement, blksize\000=1432\000
3786	17.511914000	10.2.20.73	10.2.5.193	TFTP	60	Acknowledgement, Block: 0
3787	17.512005000	10.2.20.73	10.2.5.193	TFTP	60	Acknowledgement, Block: 0
3788	17.512439000	10.2.5.193	10.2.20.73	TFTP	625	Data Packet, Block: 1
3790	17.513683000	10.2.5.193	10.2.20.73	TFTP	625	Data Packet, Block: 1
3794	17.515113000	10.2.20.73	10.2.5.193	TFTP	60	Acknowledgement, Block: 1
3795	17.515201000	10.2.20.73	10.2.5.193	TFTP	60	Acknowledgement, Block: 1
3804	17.538122000	10.2.20.73	10.2.5.193	TFTP	76	Read Request, File: features.cfg, Transfer type: octet, blksize\000=1432\000
3805	17.538224000	10.2.20.73	10.2.5.193	TFTP	76	Read Request, File: features.cfg, Transfer type: octet, blksize\000=1432\000
3810	17.569170000	10.2.5.193	10.2.20.73	TFTP	88	Error Code, Code: Access violation, Message: Could not open requested file for reading
3811	17.569472000	10.2.5.193	10.2.20.73	TFTP	88	Error Code, Code: Access violation, Message: Could not open requested file for reading

Example 2: Yealink SIP-T23G IP phone downloads the boot file and configuration files from the FTP server.

No.	Time	Source	Destination	Protocol	Length	Info
3173	28.950484000	10.2.5.193	10.2.20.73	FTP	75	[TCP Retransmission] Response: 213 382
3175	28.952342000	10.2.20.73	10.2.5.193	FTP	91	Request: RETR y000000000000.boot
3176	28.952453000	10.2.20.73	10.2.5.193	FTP	91	[TCP Retransmission] Request: RETR y000000000000.boot
3179	28.958927000	10.2.5.193	10.2.20.73	FTP	102	Response: 125 Using existing data connection
3180	28.959253000	10.2.5.193	10.2.20.73	FTP	102	[TCP Retransmission] Response: 125 Using existing data connection
3190	28.963510000	10.2.5.193	10.2.20.73	FTP	122	Response: 226 Closing data connection; File transfer successful.
3193	28.963862000	10.2.5.193	10.2.20.73	FTP	122	[TCP Retransmission] Response: 226 Closing data connection; File transfer successful.
3222	28.991053000	10.2.5.193	10.2.20.73	FTP	108	Response: 220 3Com 3CDaemon FTP Server Version 2.0
3225	28.992201000	10.2.20.73	10.2.5.193	FTP	76	Request: USER 123
3226	28.992302000	10.2.20.73	10.2.5.193	FTP	76	[TCP Retransmission] Request: USER 123
3229	28.993908000	10.2.5.193	10.2.20.73	FTP	99	Response: 331 User name ok, need password
3230	28.994220000	10.2.5.193	10.2.20.73	FTP	99	[TCP Retransmission] Response: 331 User name ok, need password
3231	28.994857000	10.2.20.73	10.2.5.193	FTP	78	Request: PASS admin
3232	28.994966000	10.2.20.73	10.2.5.193	FTP	78	[TCP Retransmission] Request: PASS admin
3235	28.995764000	10.2.5.193	10.2.20.73	FTP	91	Response: 530 Login access denied
3236	28.996077000	10.2.5.193	10.2.20.73	FTP	91	[TCP Retransmission] Response: 530 Login access denied
3237	28.996878000	10.2.20.73	10.2.5.193	FTP	82	Request: USER anonymous
3238	28.996979000	10.2.20.73	10.2.5.193	FTP	82	[TCP Retransmission] Request: USER anonymous
3241	28.997855000	10.2.5.193	10.2.20.73	FTP	99	Response: 331 User name ok, need password
3242	28.998113000	10.2.5.193	10.2.20.73	FTP	99	[TCP Retransmission] Response: 331 User name ok, need password
3244	28.998745000	10.2.20.73	10.2.5.193	FTP	73	Request: PASS
3248	29.000393000	10.2.5.193	10.2.20.73	FTP	101	Response: 230-The response '' is not valid.
3249	29.000715000	10.2.5.193	10.2.20.73	FTP	101	[TCP Retransmission] Response: 230-The response '' is not valid.
3253	29.035465000	10.2.5.193	10.2.20.73	FTP	145	Response: 230-Next time, please use your email address as password.
3255	29.035867000	10.2.5.193	10.2.20.73	FTP	145	[TCP Retransmission] Response: 230-Next time, please use your email address as password.
3258	29.037118000	10.2.20.73	10.2.5.193	FTP	74	Request: TYPE I
3259	29.037213000	10.2.20.73	10.2.5.193	FTP	74	[TCP Retransmission] Request: TYPE I
3262	29.038460000	10.2.5.193	10.2.20.73	FTP	86	Response: 200 Type set to I.
3263	29.038702000	10.2.5.193	10.2.20.73	FTP	86	[TCP Retransmission] Response: 200 Type set to I.
3264	29.039357000	10.2.20.73	10.2.5.193	FTP	72	Request: PASV
3268	29.040715000	10.2.5.193	10.2.20.73	FTP	114	Response: 227 Entering passive mode (10,2,5,193,211,172)
3269	29.041000000	10.2.5.193	10.2.20.73	FTP	114	[TCP Retransmission] Response: 227 Entering passive mode (10,2,5,193,211,172)
3279	29.054116000	10.2.20.73	10.2.5.193	FTP	80	Request: SIZE sip.cfg
3280	29.054212000	10.2.20.73	10.2.5.193	FTP	80	[TCP Retransmission] Request: SIZE sip.cfg
3283	29.055169000	10.2.5.193	10.2.20.73	FTP	75	Response: 213 579

Example 3: Yealink SIP-T23G IP phone downloads the boot file and configuration files from the HTTP server.



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
33	1.962425000	10.2.5.193	10.2.20.73	HTTP	1882	POST /servlet?p=settings-autop&g=write&now=true HTTP/1.1 (application/x-www-form-urlencoded)
141	2.267524000	10.2.20.73	10.2.5.193	HTTP	234	GET /HTTP%20Directory/00156574b16e.boot HTTP/1.1
142	2.267750000	10.2.20.73	10.2.5.193	HTTP	234	[TCP Retransmission] GET /HTTP%20Directory/00156574b16e.boot HTTP/1.1
149	2.270563000	10.2.5.193	10.2.20.73	HTTP	66	HTTP/1.1 404 Not Found (text/html)
182	2.305531000	10.2.20.73	10.2.5.193	HTTP	235	GET /HTTP%20Directory/y000000000000.boot HTTP/1.1
183	2.305723000	10.2.20.73	10.2.5.193	HTTP	235	[TCP Retransmission] GET /HTTP%20Directory/y000000000000.boot HTTP/1.1
203	2.321164000	10.2.5.193	10.2.20.73	HTTP	448	HTTP/1.1 200 OK (application/octet-stream)
279	2.359293000	10.2.5.193	10.2.20.73	HTTP	574	GET /js/define.js?44.81.254.71 HTTP/1.1
297	2.373167000	10.2.20.73	10.2.5.193	HTTP	1514	[TCP Previous segment not captured] Continuation or non-HTTP traffic
298	2.374421000	10.2.20.73	10.2.5.193	HTTP	1514	Continuation or non-HTTP traffic
304	2.376198000	10.2.20.73	10.2.5.193	HTTP	1133	Continuation or non-HTTP traffic
308	2.377011000	10.2.5.193	10.2.20.73	HTTP	570	GET /js/aes.js?44.81.254.71 HTTP/1.1
316	2.380821000	10.2.5.193	10.2.20.73	HTTP	581	GET /js/zeropadding-min.js?44.81.254.71 HTTP/1.1
317	2.380973000	10.2.5.193	10.2.20.73	HTTP	571	GET /js/jsbn.js?44.81.254.71 HTTP/1.1
318	2.381075000	10.2.5.193	10.2.20.73	HTTP	573	GET /js/prng4.js?44.81.254.71 HTTP/1.1
319	2.381175000	10.2.5.193	10.2.20.73	HTTP	569	GET /js/rng.js?44.81.254.71 HTTP/1.1
320	2.381293000	10.2.5.193	10.2.20.73	HTTP	569	GET /js/rsa.js?44.81.254.71 HTTP/1.1
398	2.408422000	10.2.20.73	10.2.5.193	HTTP	224	GET /HTTP%20Directory/sip.cfg HTTP/1.1
399	2.408639000	10.2.20.73	10.2.5.193	HTTP	224	[TCP Retransmission] GET /HTTP%20Directory/sip.cfg HTTP/1.1
413	2.412543000	10.2.5.193	10.2.20.73	HTTP	66	HTTP/1.1 404 Not Found (text/html)
464	2.442529000	10.2.20.73	10.2.5.193	HTTP	229	GET /HTTP%20Directory/features.cfg HTTP/1.1
465	2.442725000	10.2.20.73	10.2.5.193	HTTP	229	[TCP Retransmission] GET /HTTP%20Directory/features.cfg HTTP/1.1
470	2.455300000	10.2.5.193	10.2.20.73	HTTP	645	HTTP/1.1 200 OK (application/octet-stream)
480	2.458812000	10.2.5.193	106.120.188.46	HTTP	1046	POST /q?h=A36B528EBBE894F17A1F12E8A58FE660&r=0000&v=5.2.5.17503 HTTP/1.1 (application/x-www-f
491	2.508429000	10.2.5.193	10.2.20.73	HTTP	492	GET /note/1.English_note.xml HTTP/1.1
492	2.509486000	10.2.5.193	10.2.20.73	HTTP	492	[TCP Retransmission] GET /note/1.English_note.xml HTTP/1.1
507	2.558874000	106.120.188.46	10.2.5.193	HTTP	296	HTTP/1.1 200 OK (text/plain)
509	2.643723000	10.2.5.193	36.110.147.36	HTTP	1433	GET /websearch/features/yun6.jsp?pid=sogou-brse-d2a452edff079ca6&w=1440&v=7400&st=146830942174

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 IP 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 IP 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 IP phone only downloads MAC-Oriented boot file and the configuration files referenced in the MAC-Oriented boot file.

Why does the IP 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 IP 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 IP phone display "Network unavailable"?

- Ensure that the Ethernet cable is plugged into the Internet port on the IP 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 IP phone obtain the IP address from the DHCP server?

- Ensure that settings are correct on the DHCP server.
- Ensure that the IP phone is configured to obtain the IP address from the DHCP server

Why doesn't the IP 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 IP phone supports.
- Ensure that the properties of the ring tone for the IP 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 IP phone update configurations?

- Ensure that the configuration files are different from the last ones.
- Ensure that the IP 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 HTTPS Server

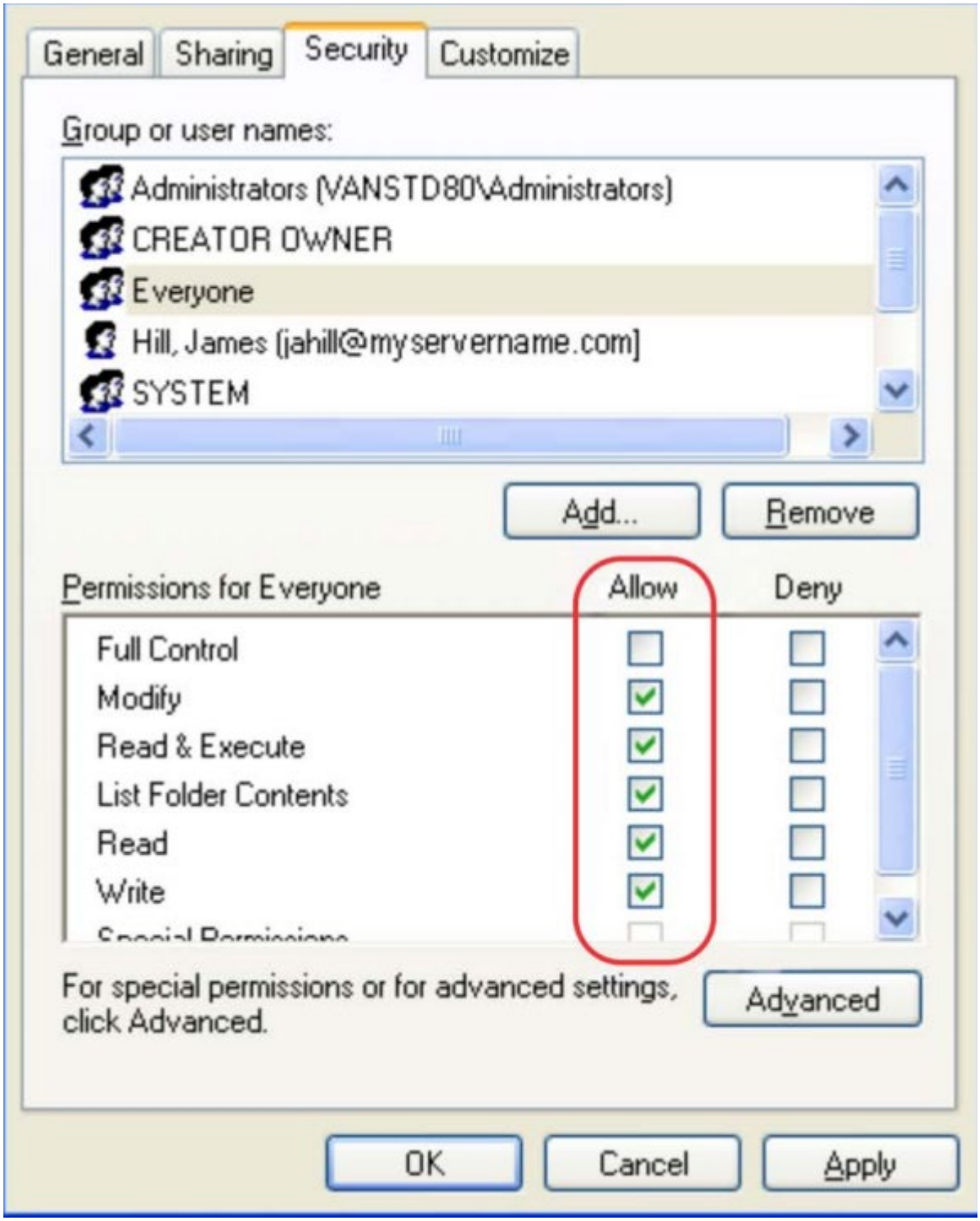
Introduction

This section provides instructions on how to configure an HTTPS server using the 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 HTTPS root directory on the local system (for example, D:\HTTP Directory).
2. Place the boot files and configuration files in this root directory.
3. Set the security permissions for the HTTPS directory folder.
4. You need to define a user or group name and set the permissions: read, write, and modify. Security permissions vary by organization.
   An example of configuration on the Windows platform is shown as below:

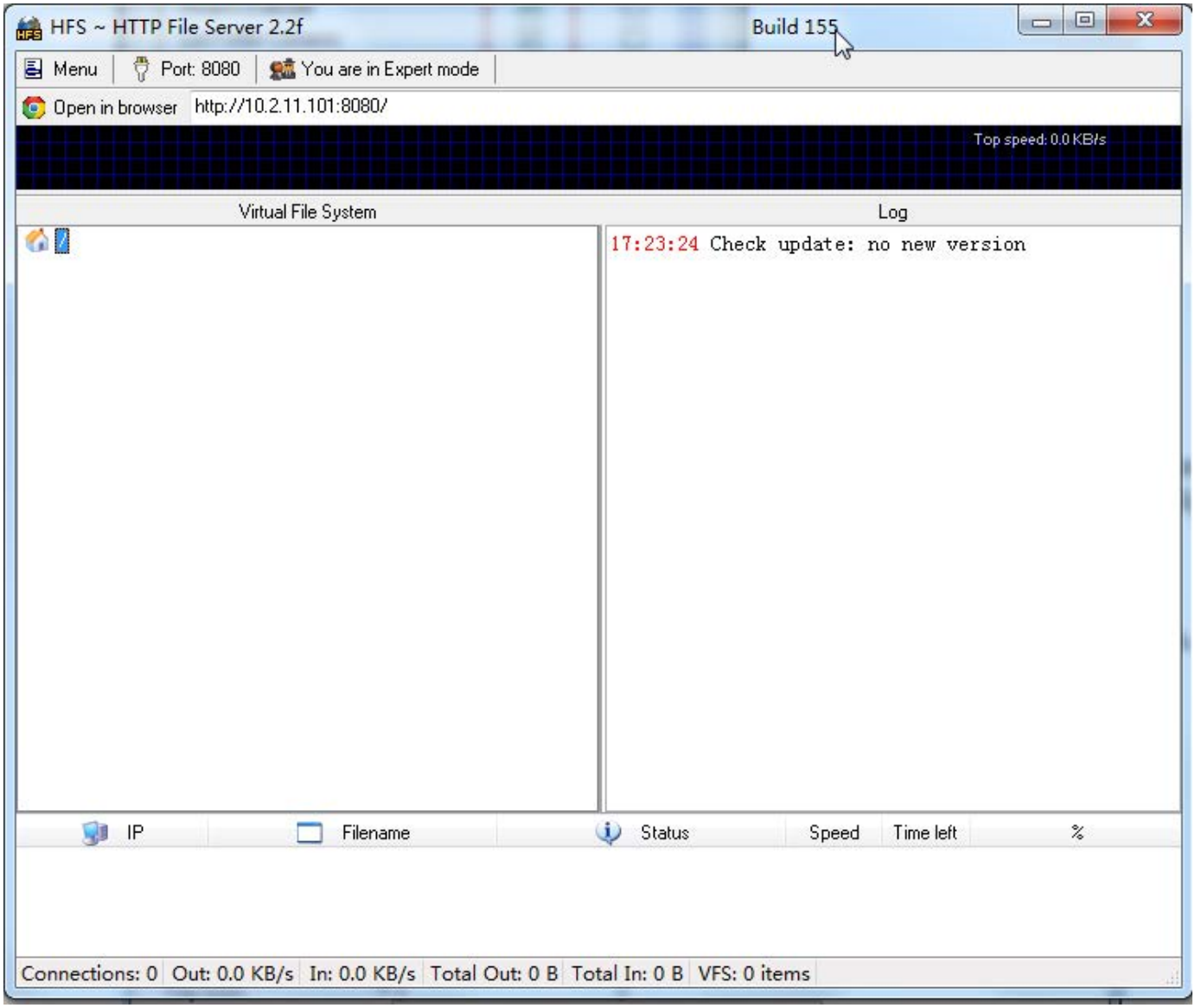


Configure an HTTPS Server

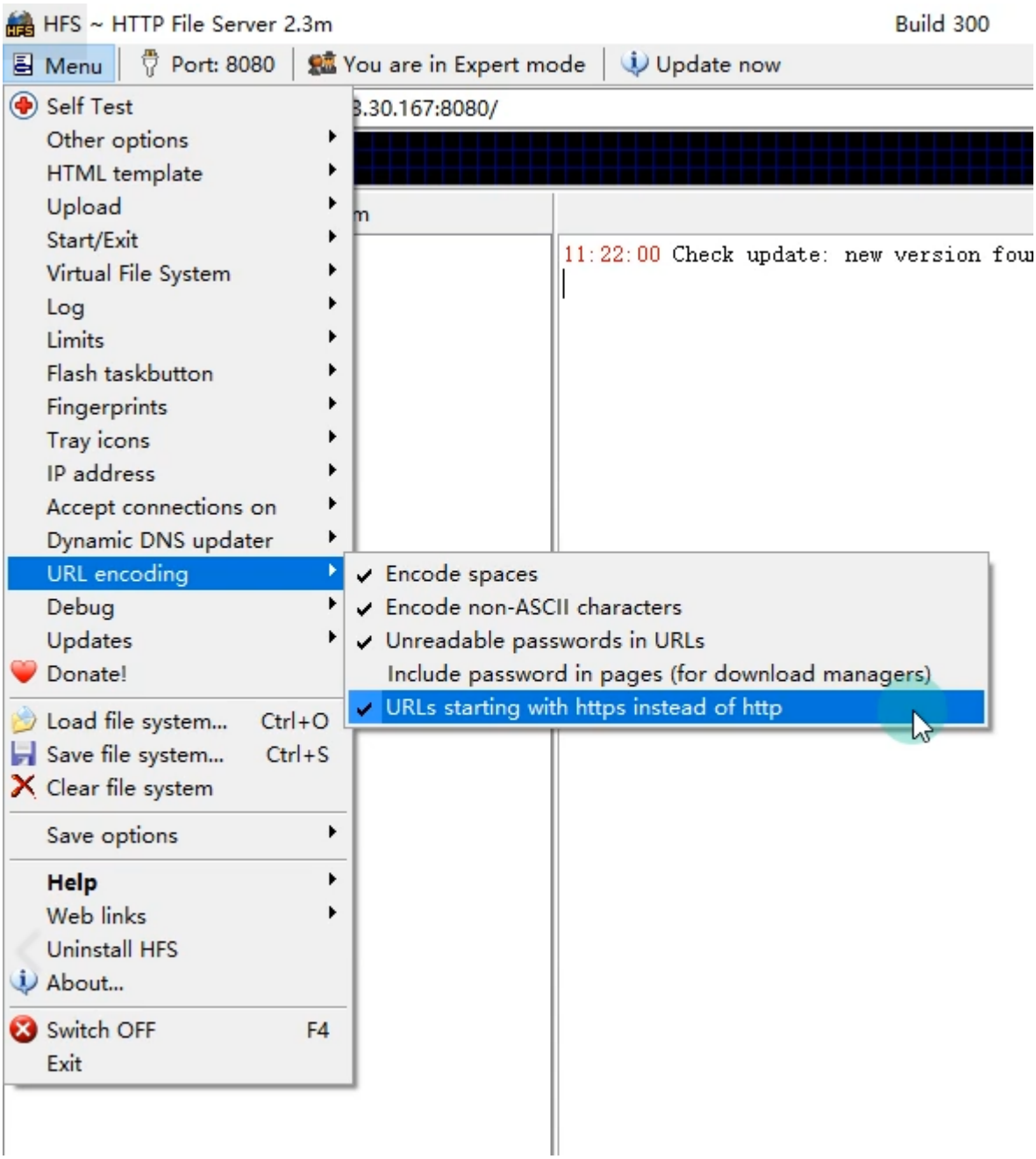
HFS tool is an executable application, so you don't need to install it.

To configure an HTTPS server:

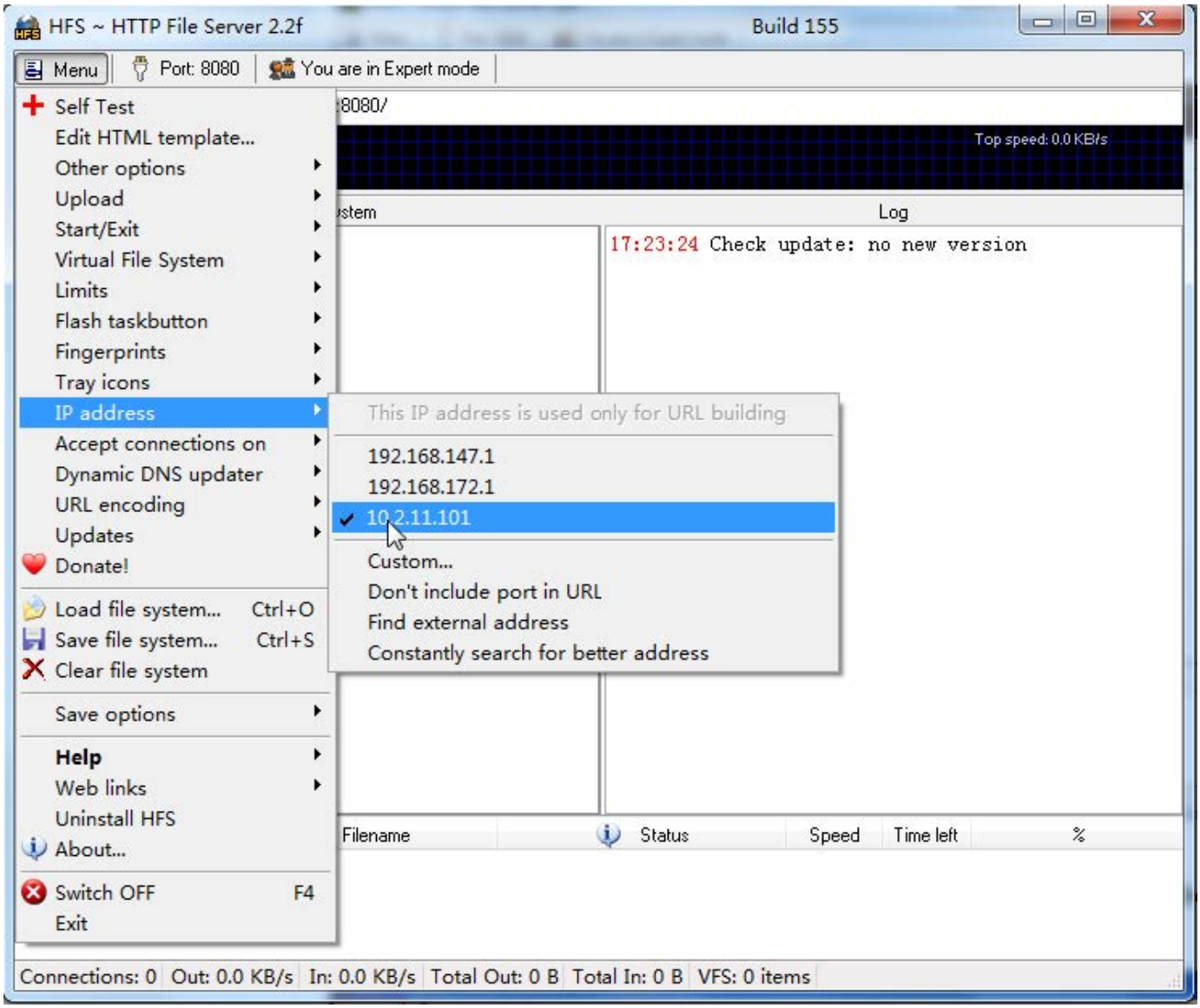
1. Download the application file to your local directory, and double-click the **hfs.exe**.
2. The main configuration page is shown below:



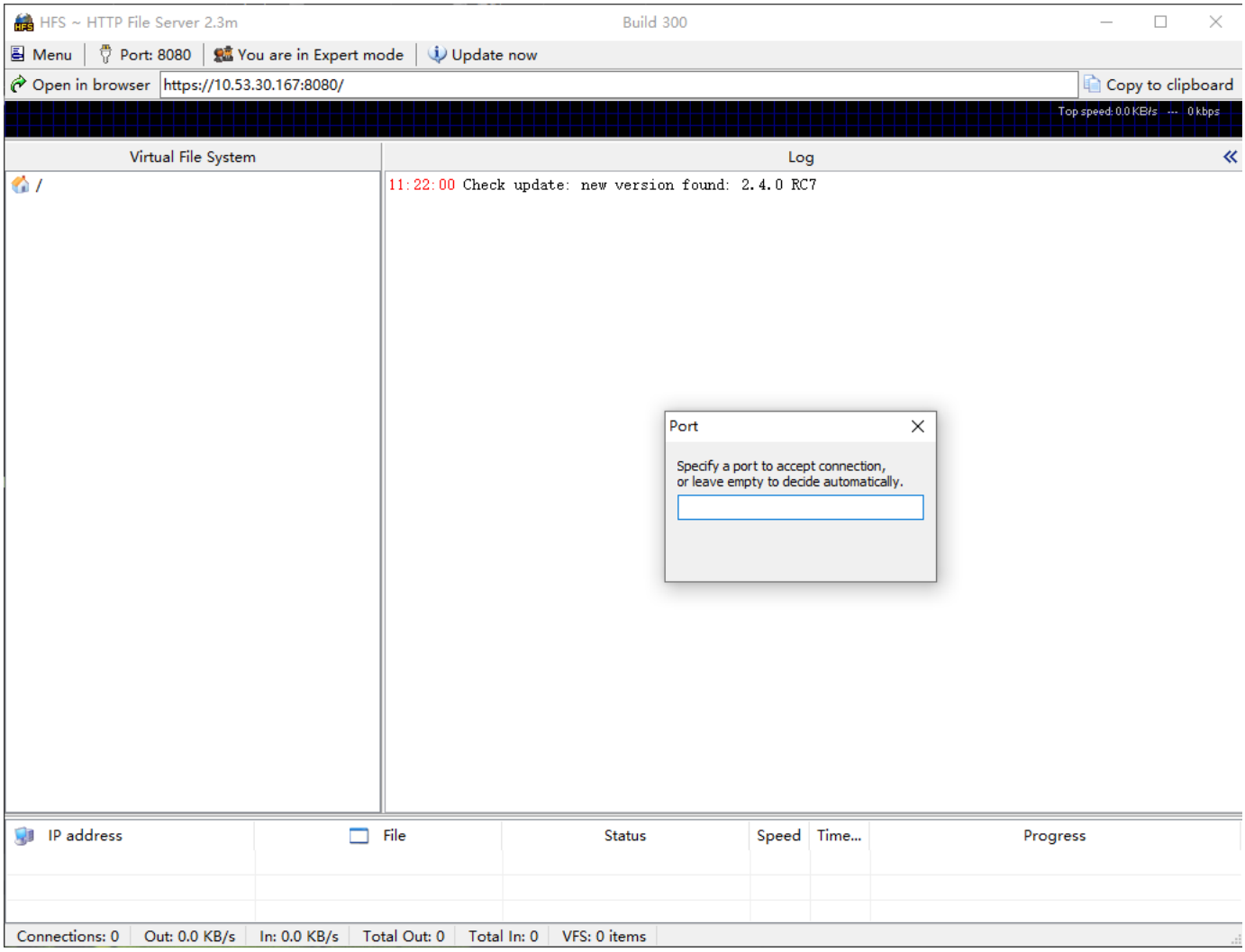
2. Click **Menu** –> **URL encoding** –> **URLs starting with https instead of http**.



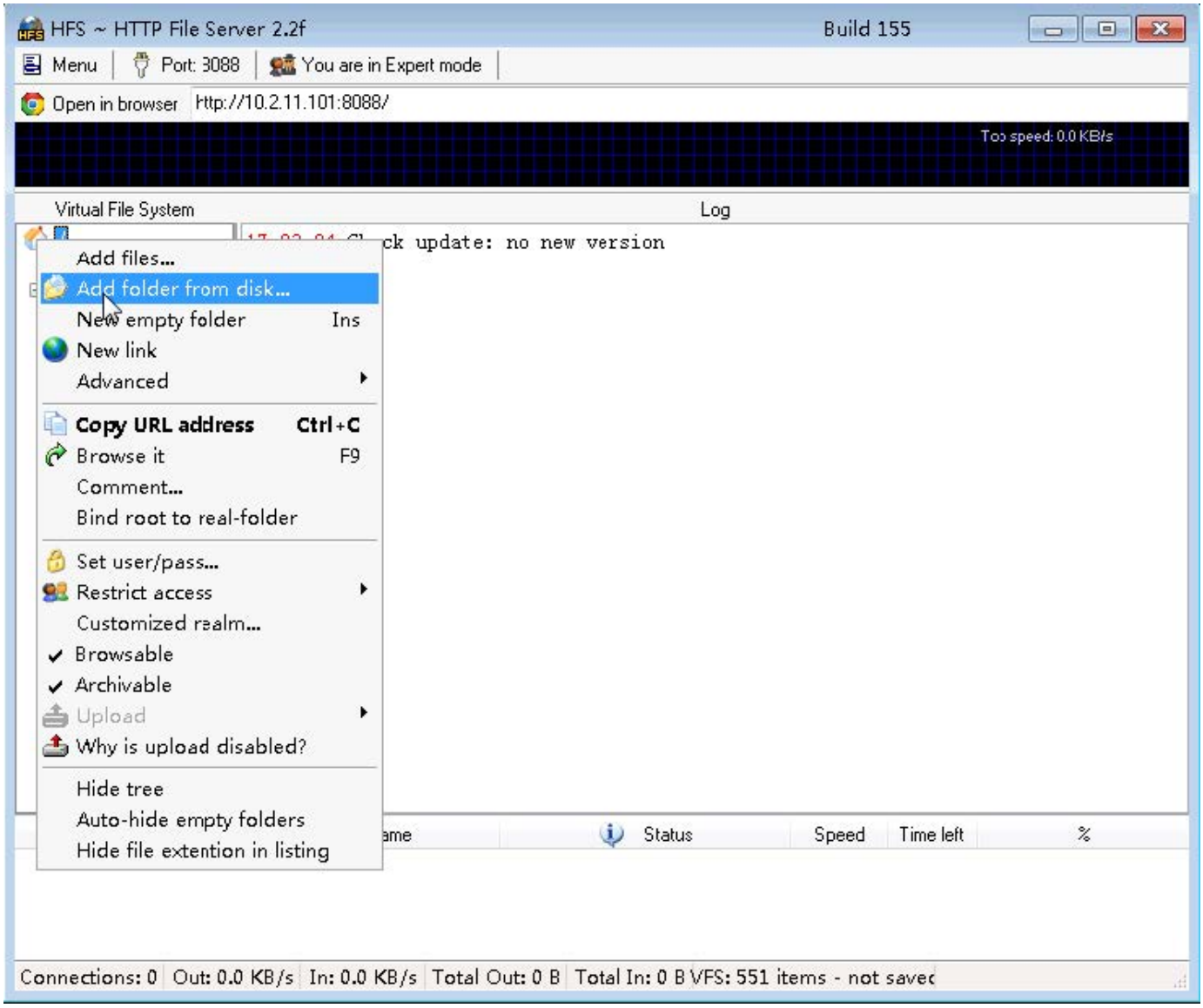
3. Click **Menu** on the main page and select the IP address of the PC from **IP address**.



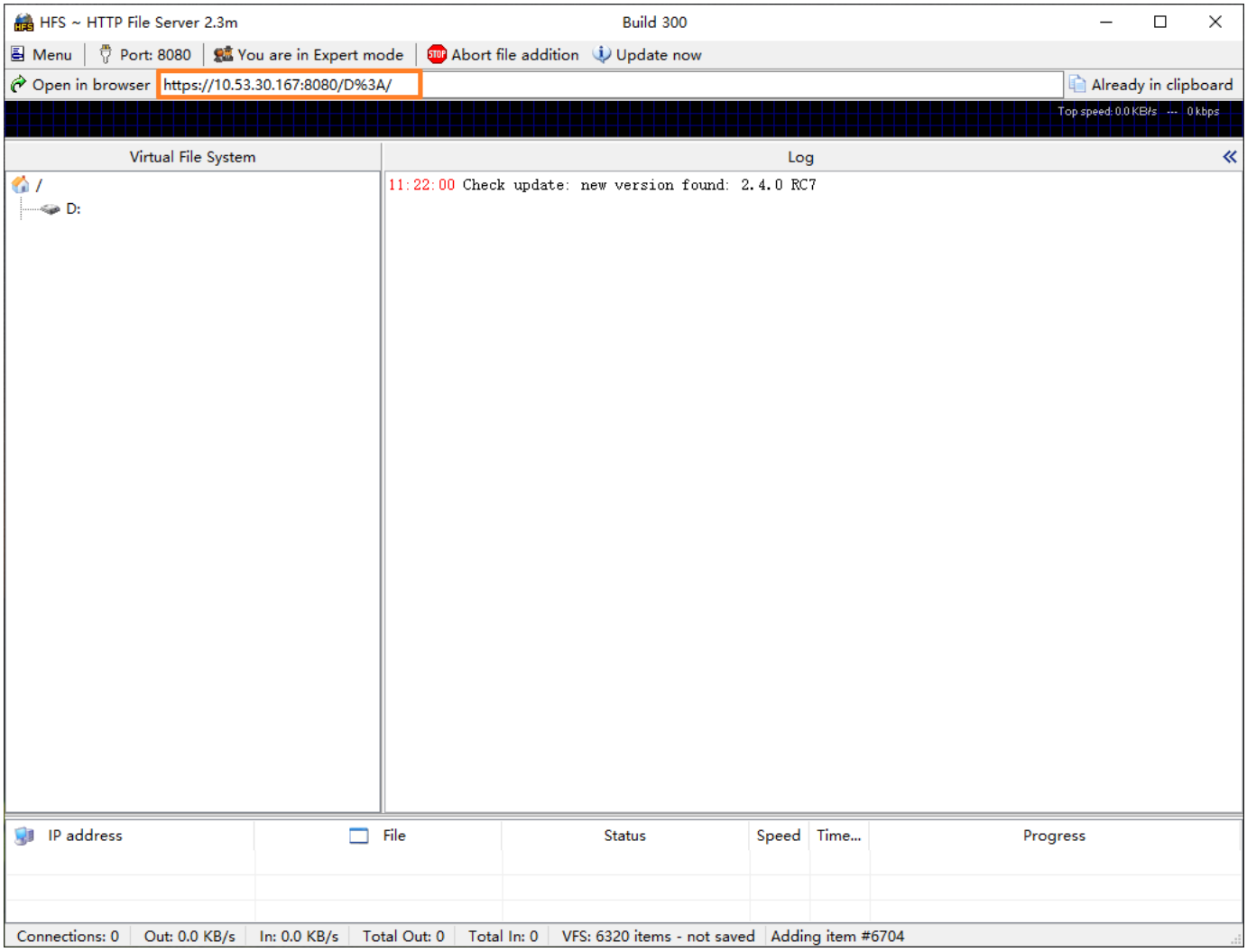
5. The default HTTP port is **8080**. You can also reset the HTTP port (make sure there is no port conflict).



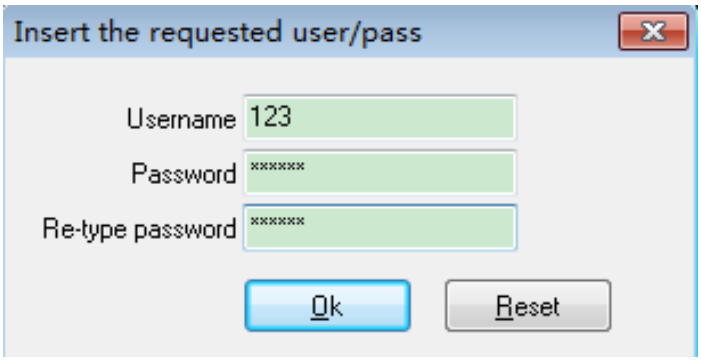
4. Right-click the icon on the left of the main page, select Add folder from disk to add the HTTPS Server root directory.



5. Locate the root directory on your local system.



6. Check the server URL (for example, https://10.2.11.101:8088/ProvisioningDir) by clicking "**Open in browser**".
7. (Optional.) Right-click the root directory name (for example, ProvisioningDir), and then select **Set user/pass…**.
8. (Optional.) Enter the desired user name and password for the root directory in the corresponding fields and then click **OK**.



Configure FTP Server

Introduction

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.

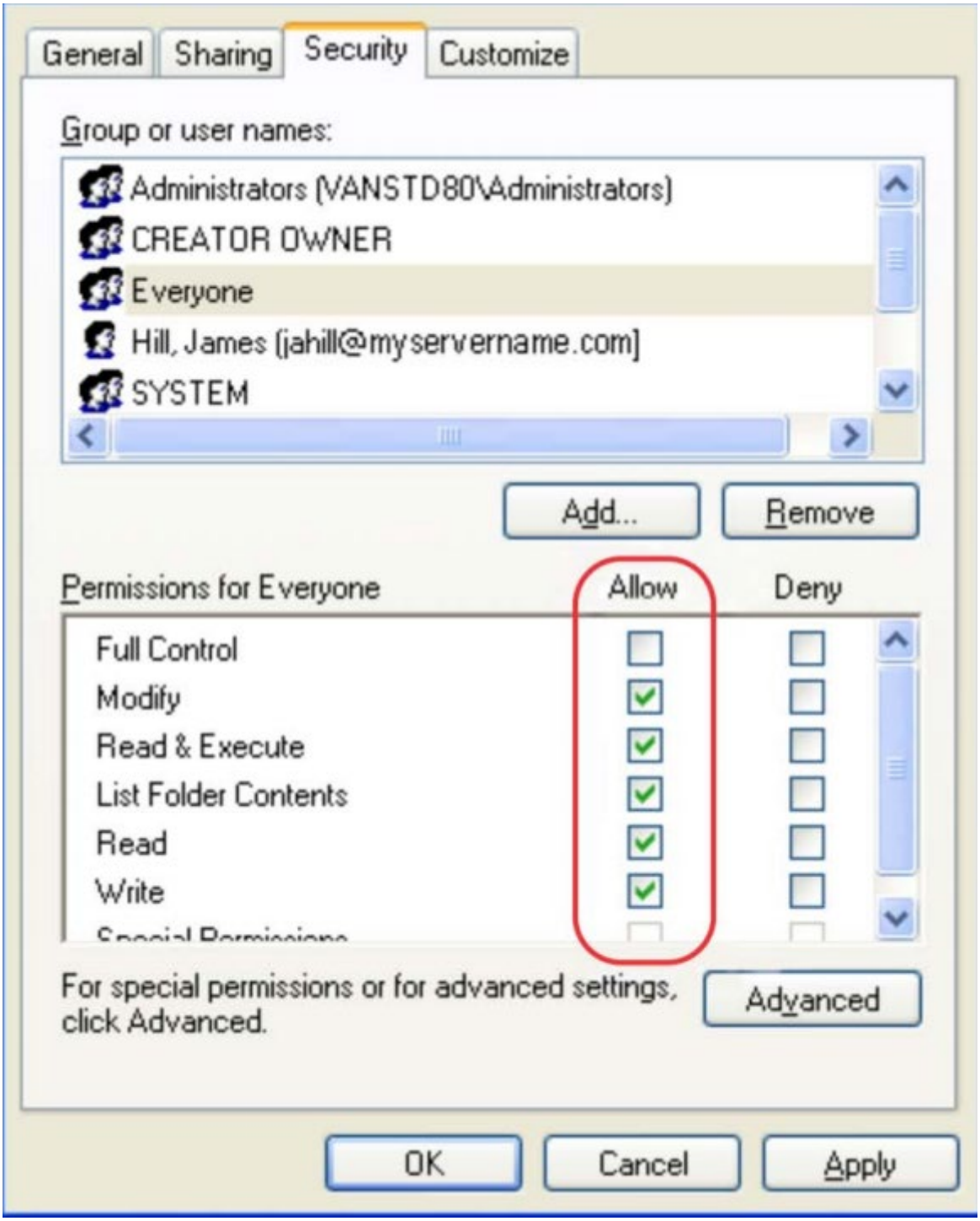
We recommend that you use vsftpd as an FTP server for the Linux platform if required.

Before configuring a wftpd server, ensure that no other FTP servers exist in your local system.

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 in 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 to read, write, and modify.
   Security permissions vary by organization.
   An example of configuration on the Windows platform is shown below:

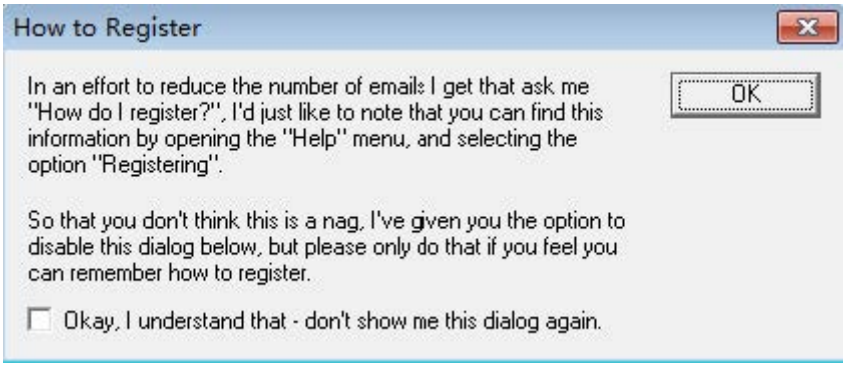


Configure an FTP Server

To configure a wftpd server:

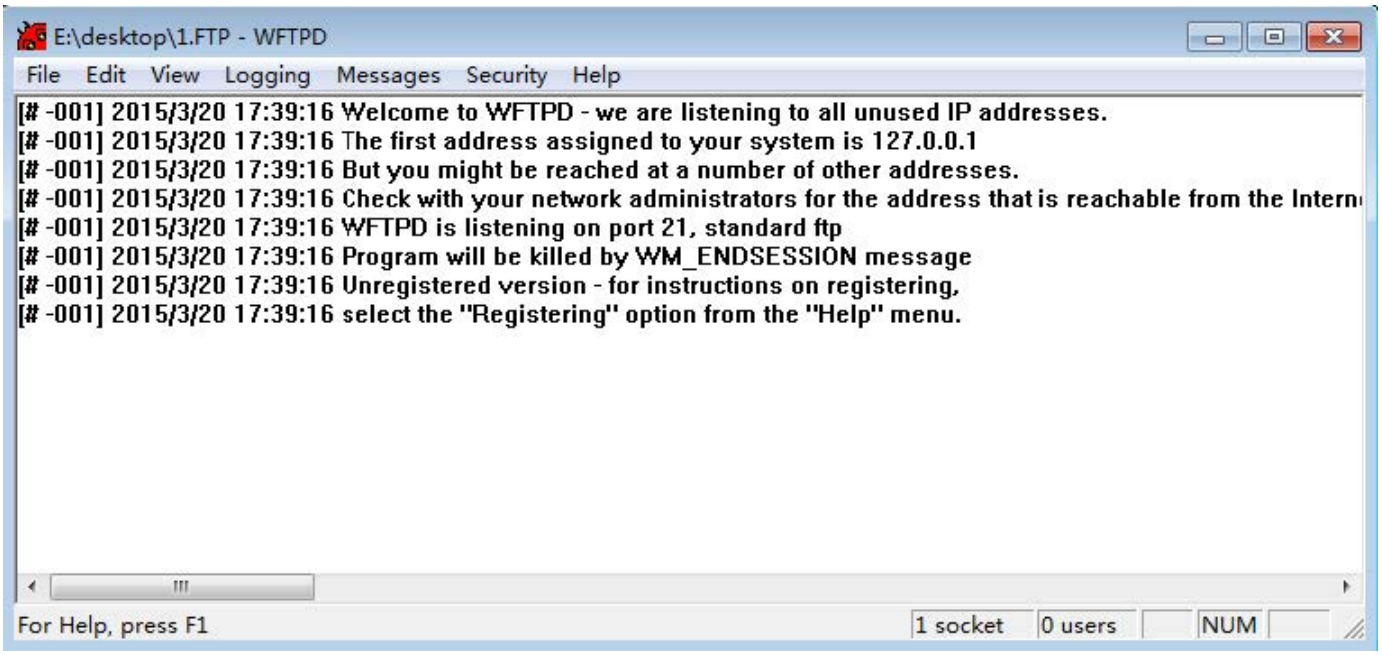
1. Download the compressed file of the wftpd application to your local directory and extract it.
2. Double-click the **Wftpd.exe**.

   The dialogue box for registering is shown below:

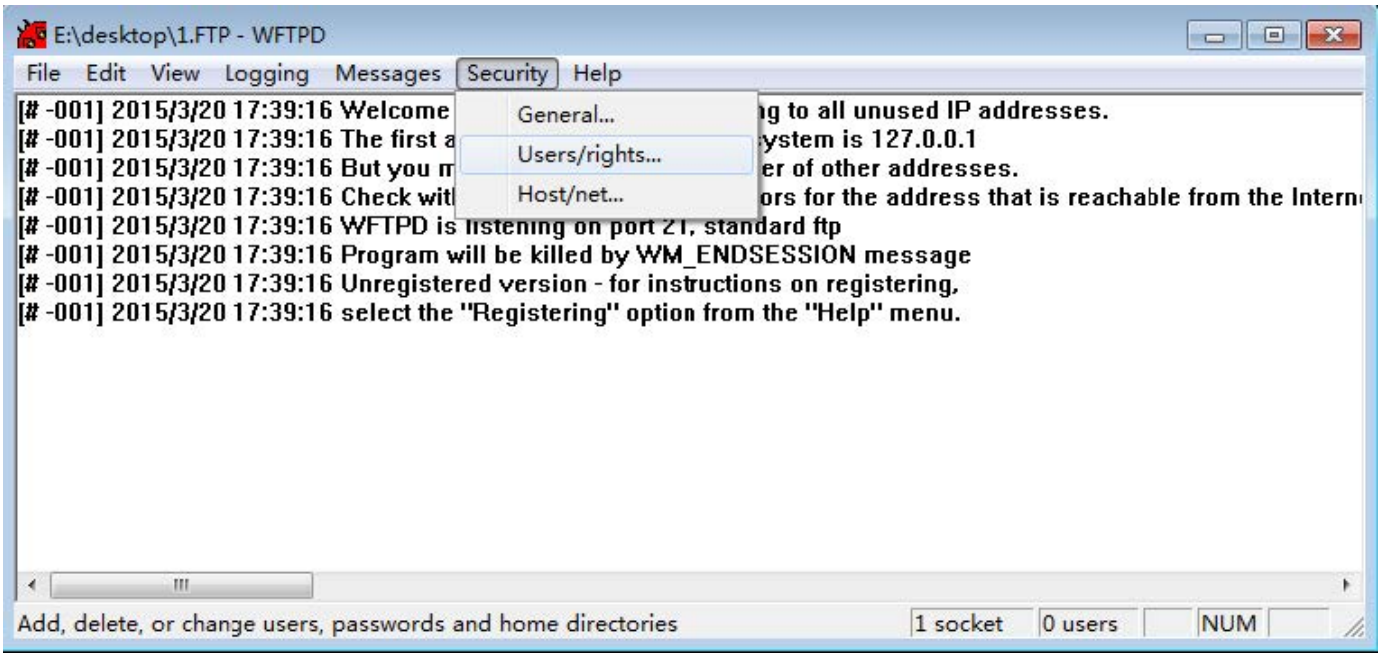


3. Check the check box and click **OK** in the pop-up box.

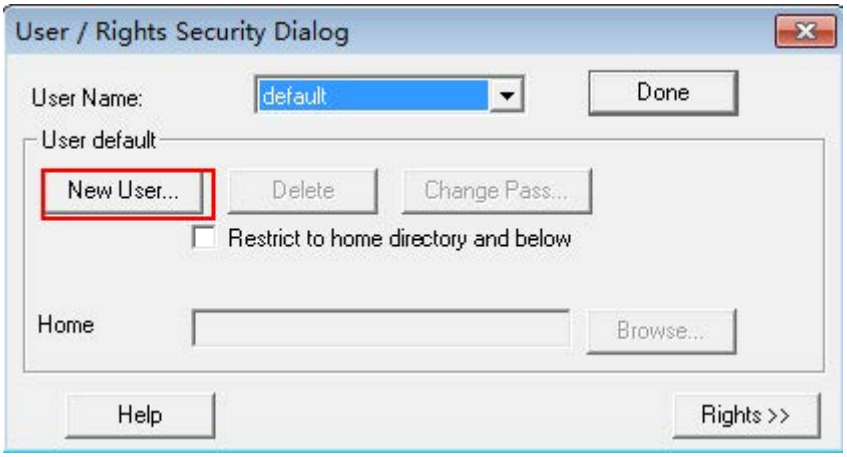
The log file of the wftpd application is shown as below:



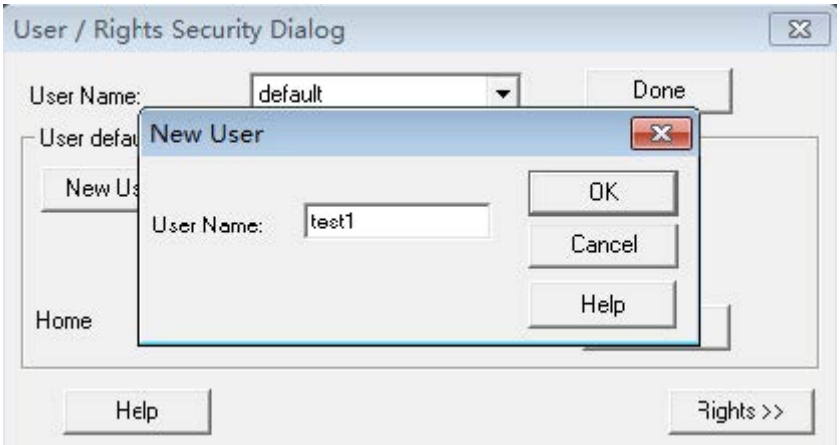
4. Click **Security** > **Users/rights**.



5. Click **New User**.

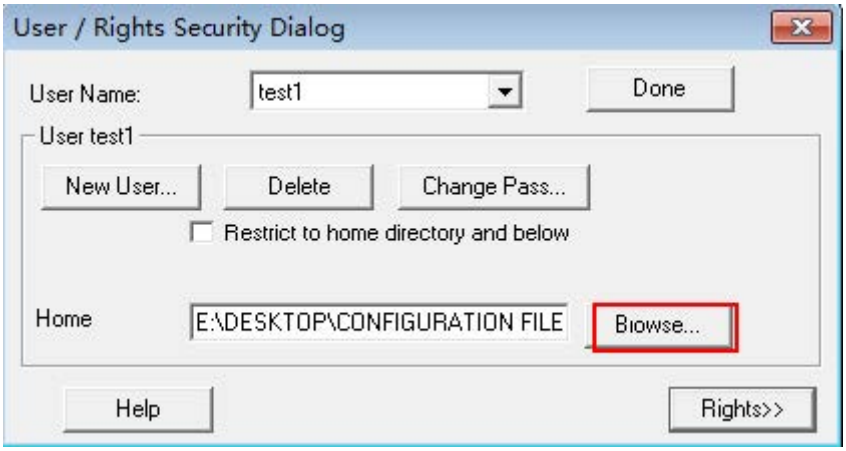


6. Enter a user name (for example, test1) in the **User Name** field and then click **OK**.



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.

Phone Provisioning Parameter

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

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: Yealink Support.

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.

> 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's MAC address is 00156574B150, rename the template file as 00156574b150.boot (lowercase).

> 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.

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

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.

> To protect against unauthorized access, you can encrypt configuration files.
> For more information on encrypting configuration files, refer to Encrypting and Decrypting Files.

Common CFG File

The 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 the 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 is generated 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.

1. 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.
2. The static changes are never be saved to the <MAC>-local.cfg file.
3. 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

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.

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	DialPla	Customize the replace rules for the dial plan.	Dial Plan

Template	n.xml		
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

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.

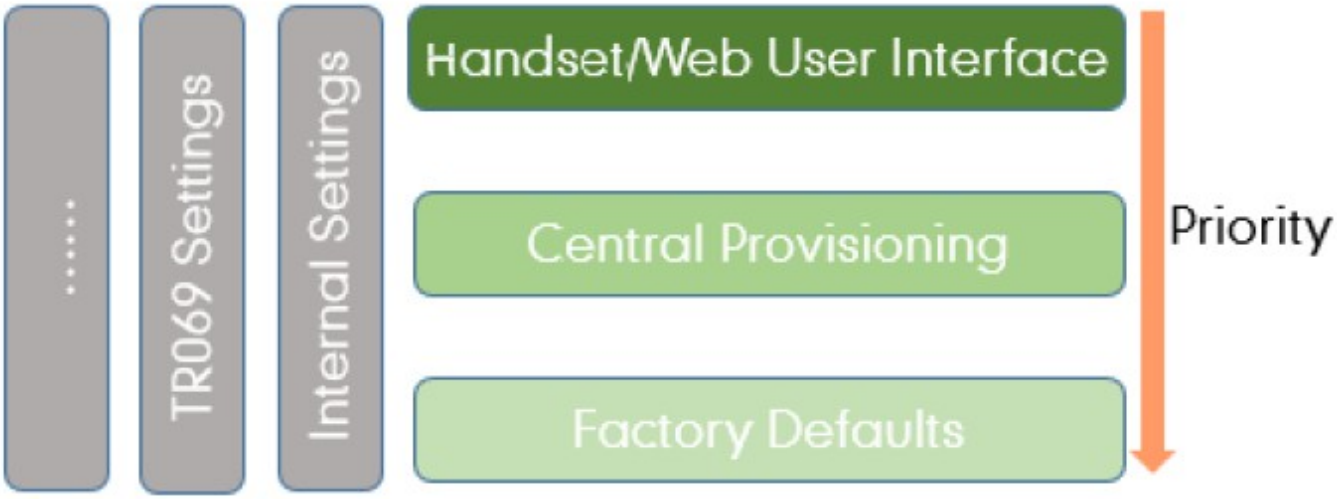
Provisioning Methods Priority

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):



1. 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.
2. 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.
3. 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.

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.

> Accessing the web user interface by request URI may be restricted by the web browser (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	Description	Permitted Values	Default
wui.quick_login	It enables or disables the quick login feature. > It works only if "static.wui.https_enable" is set to 1 (Enabled).	**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
wui.secure_domain_list	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.	• 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

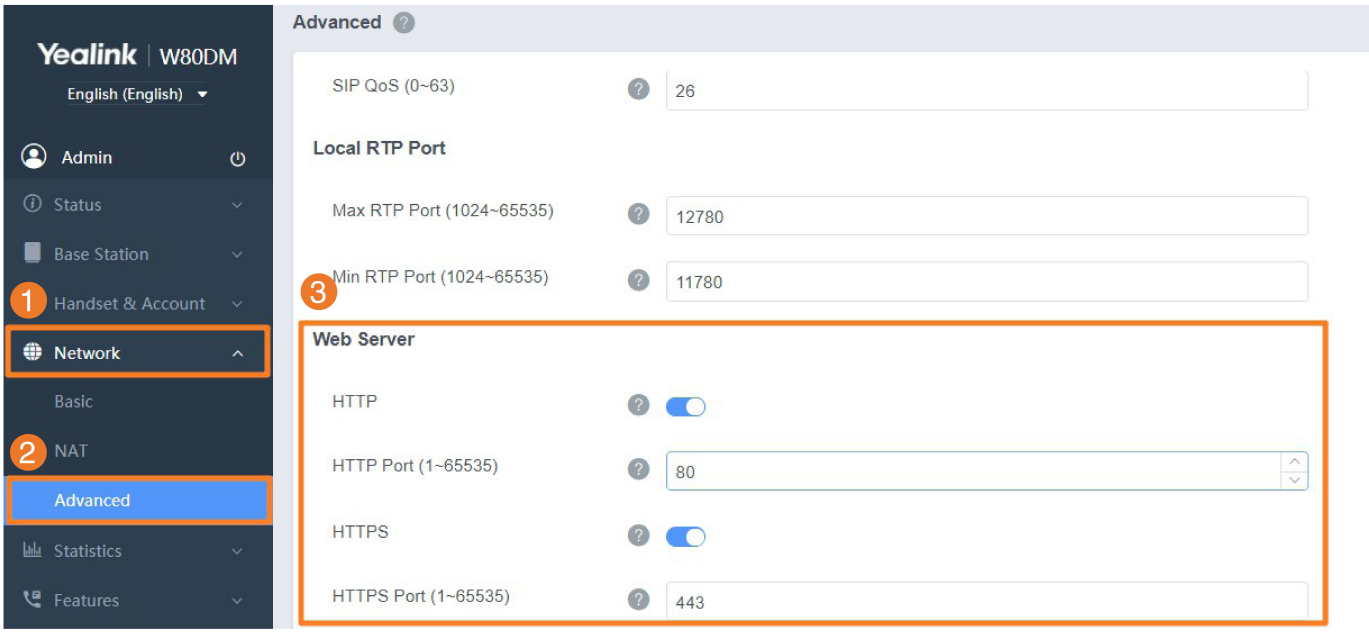
	To use a domain name to access the web user interface of the phone, make sure your DNS server can resolve the domain name to the IP address of the phone.		

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 access to the web user interface using the HTTP/HTTPS protocol, neither you nor the user can 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.http_enable
static.wui.https_enable
static.network.port.https

Parameter	Description	Permitted Values	Default

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

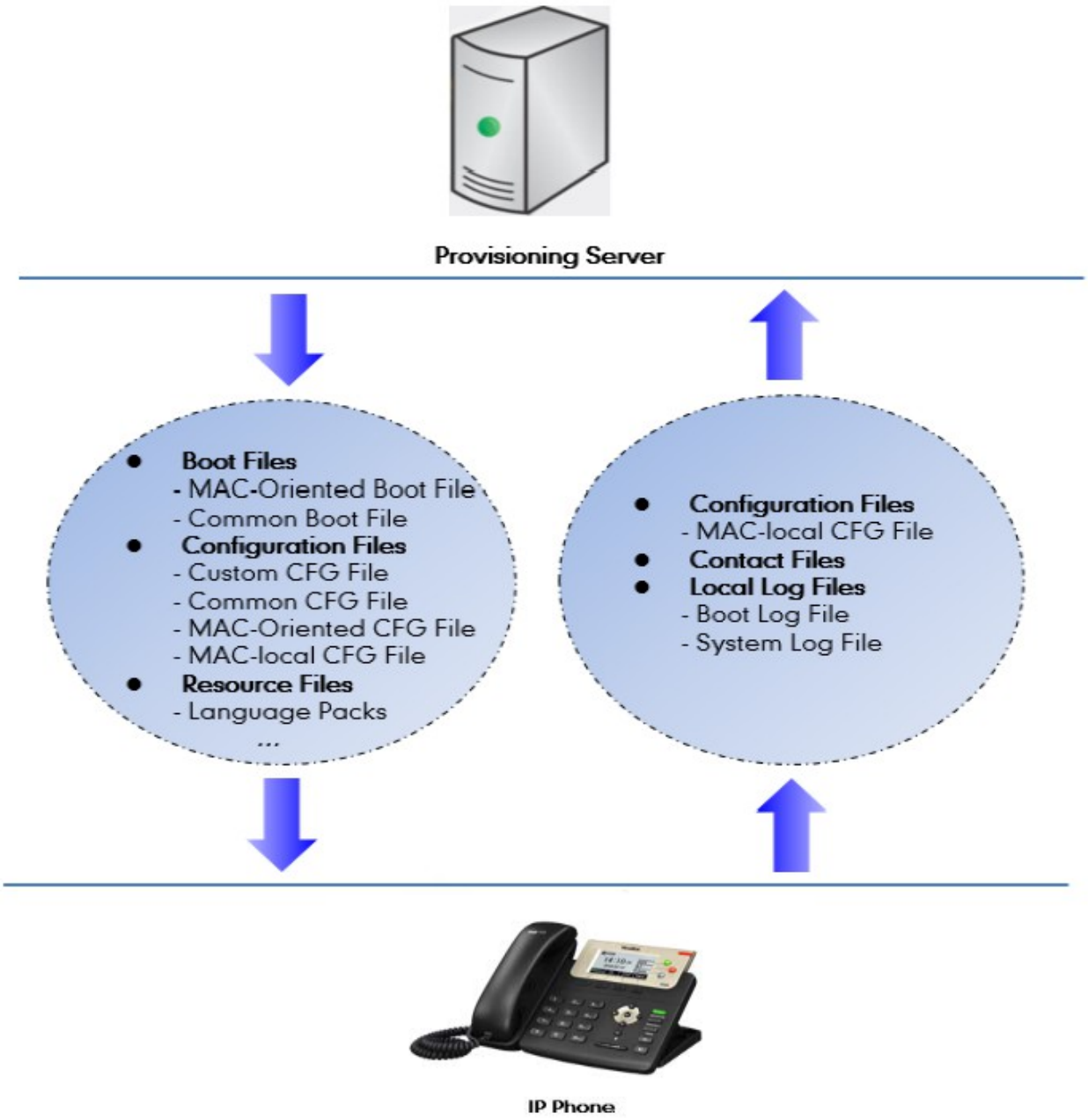
> [1]If you change this parameter, the phone will reboot to make the change take effect.

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 the provisioning server when you use the centralized provisioning method:



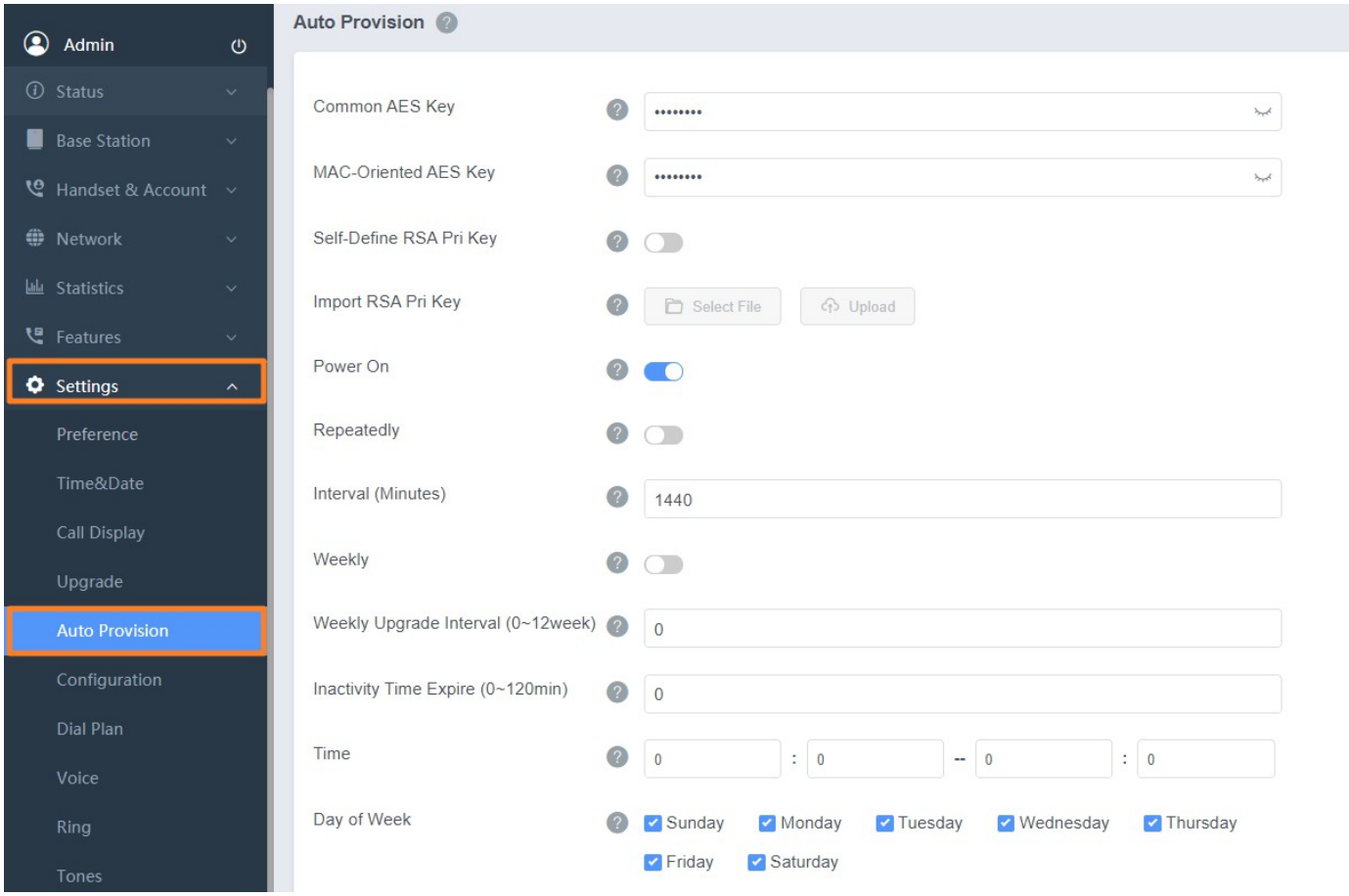
Yealink phones can obtain the provisioning server address during startup. Then the phones first download boot files and configuration files from the provisioning server, and then resolve and update the configurations written in configuration files. This entire process is called auto-provisioning. For 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.

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	Description	Permitted Values	Default
static.auto_provision.attempt_expired_time	It configures the timeout (in seconds) to transfer a file via auto provisioning. It has a higher priority than the value defined by the parameter "static.network.attempt_expired_time".	Integer from 1 to 300	20
static.network.attempt_expired_time[1]	It configures the timeout (in seconds) to transfer a file for HTTP/HTTPS connection. It has a lower priority than the value defined by the parameter "static.auto_provision.attempt_expired_time".	Integer from 1 to 20	10
static.auto_provision.attempt_before_failed	It configures the maximum number of attempts to transfer a file before the transfer fails during auto provisioning.	Integer from 1 to 10	3

static.auto_provision.retry_delay_after_file_transfer_failed	It configures the time (in seconds) to wait after a file transfer fails before retrying the transfer via auto provisioning.	Integer from 0 to 300	5
static.auto_provision.reboot_force.enable[1]	It enables or disables the phone to reboot after auto provisioning, even if there is no specific configuration requiring a reboot. It works only for the current auto-provisioning process. If you want the phone to reboot after every auto-provisioning process, the parameter must always be 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).	**0**-Disabled **1**-Enabled	Blank
static.auto_provision.power_on	It triggers the power on feature to turn on or off.	**0**-Off **1**-On, the phone performs auto provisioning when powered on.	1

static.auto_provision.repeat.enable	It triggers the repeat feature to turn on or off.	**0**-Off **1**-On	0
static.auto_provision.repeat.minutes	It configures the interval (in minutes) for the phone to perform auto provisioning repeatedly. It works only if "static.auto_provision.repeat.enable" is set to 1 (On).	Integer from 1 to 43200	1440
static.auto_provision.weekly.enable	It triggers the weekly feature to turn on or off.	**0**-Off **1**-On, the phone performs an auto-provisioning process weekly.	0
static.auto_provision.weekly_upgrade_interval	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 on a random day between the specific day(s) configured by the parameter	Integer from 0 to 12	0

	"static.auto_provision.weekly.dayofweek" every three weeks. It works only if "static.auto_provision.weekly.enable" is set to 1 (On).		
static.auto_provision.inactivity_time_expire	It configures the delay time (in minutes) to perform auto provisioning when the phone is inactive during a 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. The phone may perform auto	Integer from 0 to 120	0

	provisioning when you are using the phone during office hours. 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.weekly.dayofweek	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"	0,1,2,3,4,5,6 or a combination of these digits **0**-Sunday **1**-Monday **2**-Tuesday **3**-Wednesday **4**-Thursday **5**-Friday **6**-Saturday	01 23 45 6

	is set to a value other (for example, 3), it means the phone performs auto provisioning by randomly selecting a day from Sunday and Monday every three weeks. 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	It configures the starting/ ending time of the day for the phone to perform auto provisioning weekly. It works only if "static.auto_provision.weekly.enable" is set to 1 (On).	Time from 00:00 to 23:59	00:00
static.auto_provision.flexible.enable	It triggers the flexible feature to turn on or off. 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	**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

	again after each auto-provisioning.		
static.auto_provision.flexible.interval	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. It works only if "static.auto_provision.flexible.enable" is set to 1 (On).	Integer from 1 to 1000	30
static.auto_provision.flexible.begin_time	It configures the starting time of the day for the phone to perform auto provisioning at random. It works only if "static.auto_provision.flexible.enable" is set to 1 (On).	Time from 00:00 to 23:59	02:00
static.auto_provision.flexible.end_time	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 the starting time configured by the	Time from 00:00 to 23:59	Blank

	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 the 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 the 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 the ending time on the next day. It works only if "static.auto_provision.flexible.enable" is set to 1 (On).		
static.auto_provision.dns_resolv_nretry	It configures the retry times when the phone fails to resolve the access URL	Integer from 1 to 10	2

	of the provisioning server. 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	It configures the timeout (in seconds) for the phone to retry to resolve the access URL of the provisioning server. For each different DNS server, it works only if "static.auto_provision.dns_resolv_nosys" is set to 1 (Enabled).	Integer from 1 to 60	5

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

Set Up a Provisioning Server

Introduction

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

Supported Provisioning Protocols

Yealink phones support several transport protocols for provisioning:

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

> 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	Description	Permitted Values	Default
static.auto_provision.server.type	It configures the protocol the phone uses to connect to the provisioning server. 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".	**1**-http **2**-https **3**-ftp **Other values**-tftp	tftp
static.auto_provision.user_agent_mac.enable[1]	It enables or disables the phone's MAC address to be included in the User-Agent header of HTTP/HTTPS requests via auto provisioning.	**0**-Disabled **1**-Enabled	1

> [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.

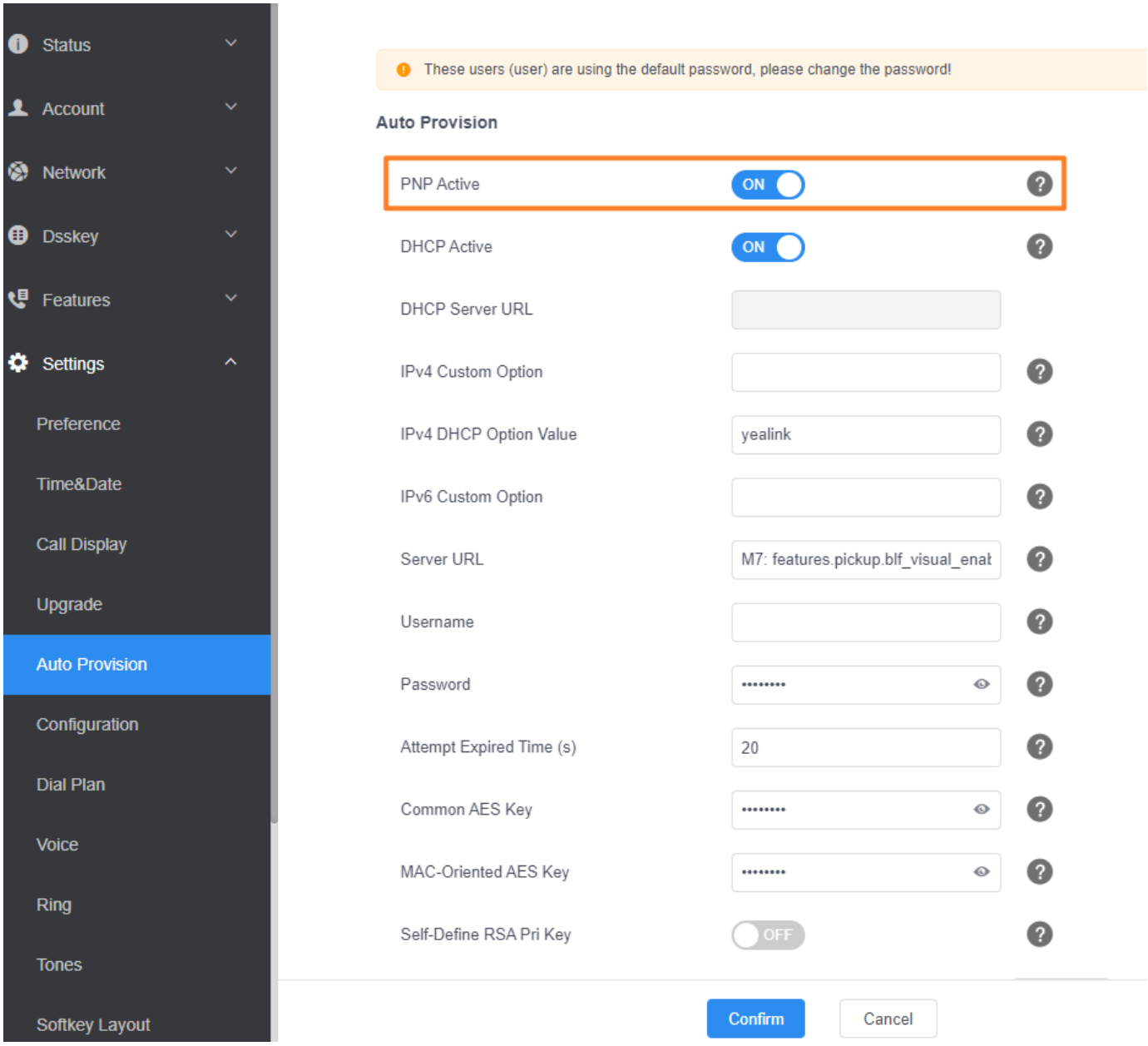
The IP phone supports the following methods to discover the provisioning server address:

- **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

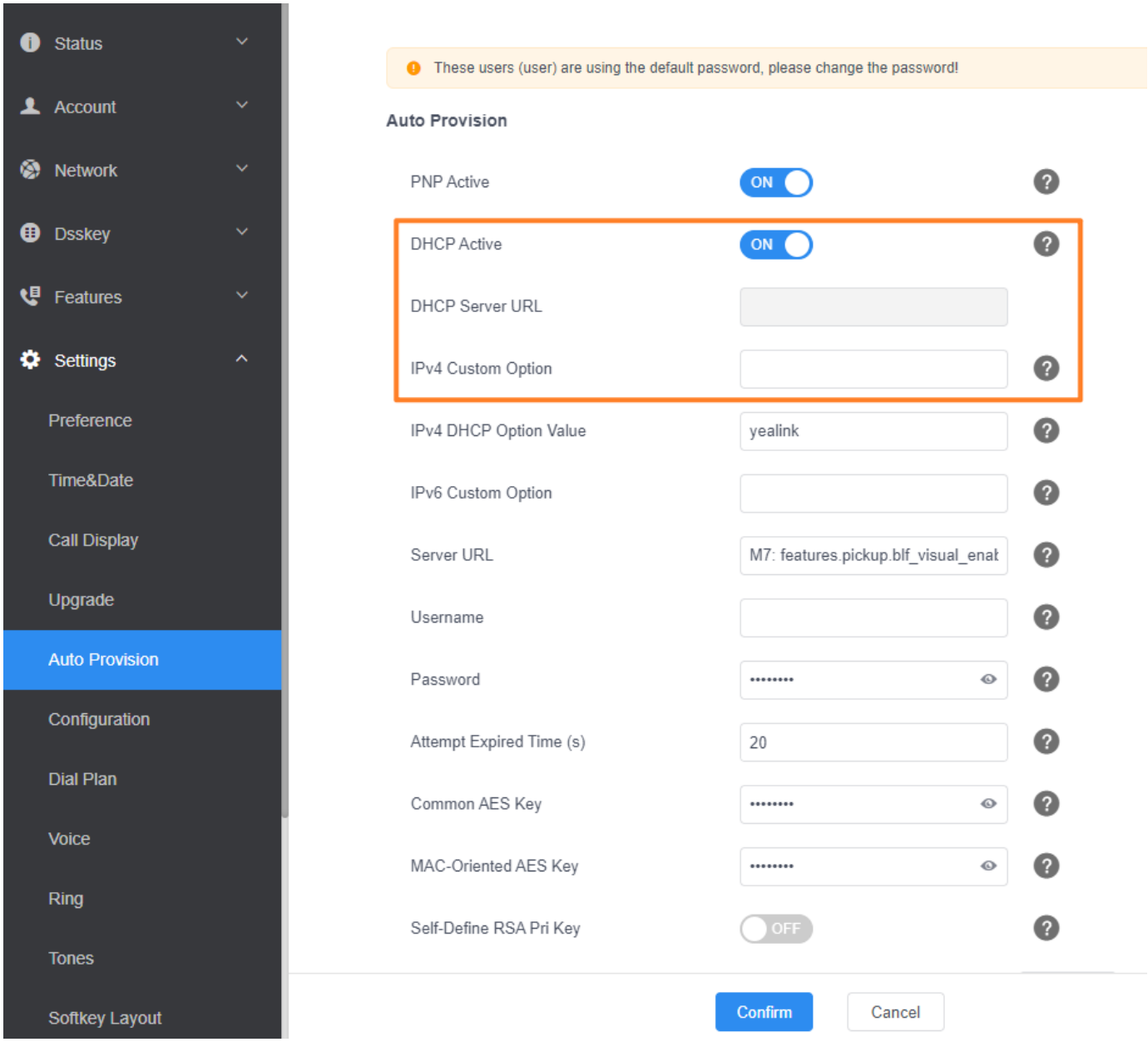
static.auto_provision.pnp_enable

Parameter	Description	Permitted Values	Default
static.auto_provision.pnp_enable	It triggers the Plug and Play (PnP) feature to turn on or off.	**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

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	Description	Permitted Values	Default
static.auto_provision.dhcp_o	It triggers the DHCP Active feature to turn on or off.	**0**-Off	1

ption.enable		**1**-On, the phone obtains the provisioning server address by detecting DHCP options.	
static.auto_provision.dhcp_option.list_user_options	It configures the IPv4 custom DHCP option for requesting provisioning server address. Multiple options are separated by commas. It works only if "static.auto_provision.dhcp_option.enable" is set to 1 (On).	Integer from 128 to 254	Blank
static.auto_provision.url_wildcard.pn	It configures the characters to replace the wildcard $PN in the received URL of the provisioning server. The configured characters must be in accordance with the actual directory name of the provisioning server.	String within 32 characters	Blank

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, a domain name, ora 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.

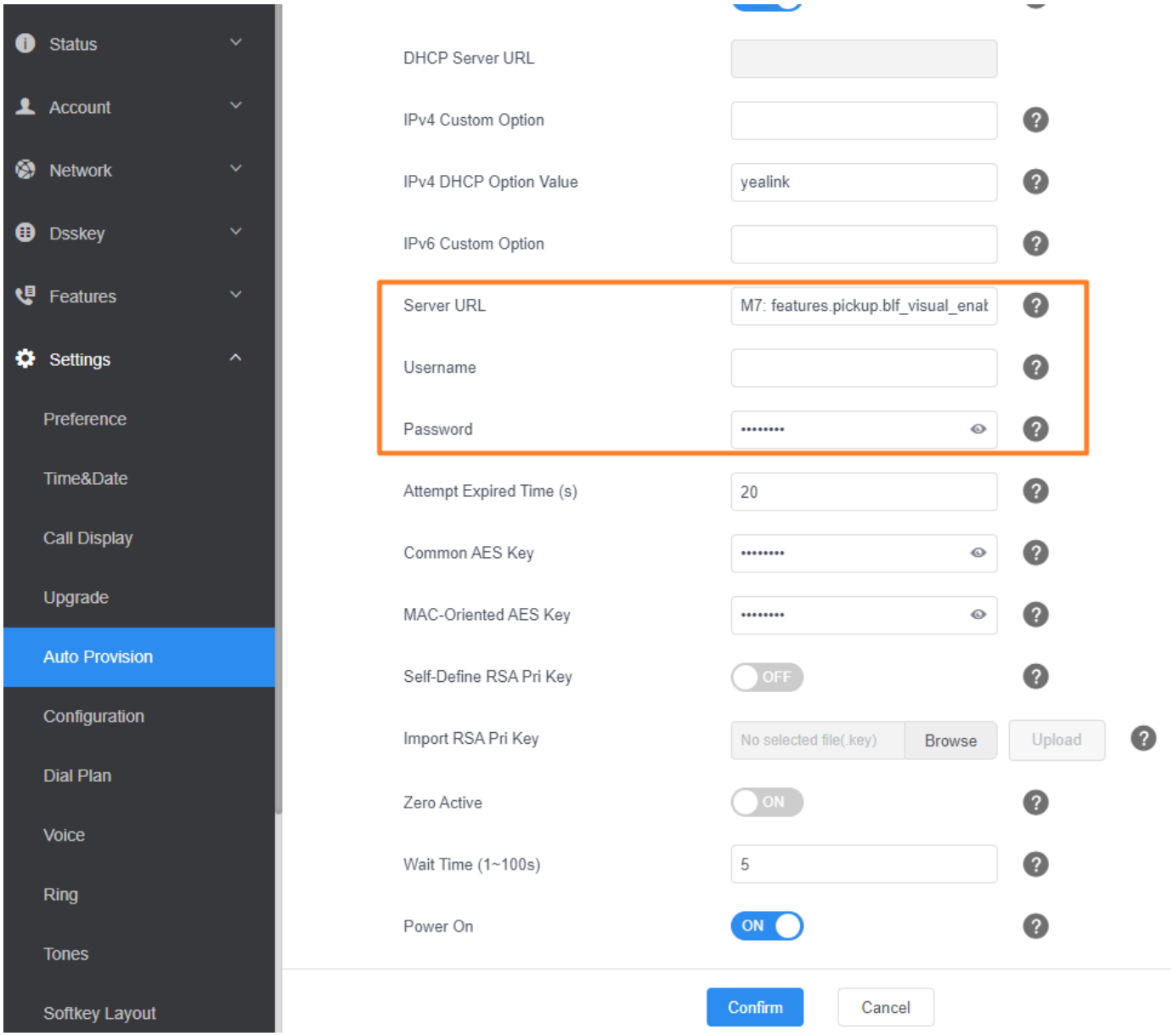
NOTE

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

rver.username	provisioning server access.	characters	an k
static.auto_provision.se rver.password	It configures the password for provisioning server access.	String within 32 characters	Bl an k

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.

> 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 Users' Personalized Settings after Auto Provisioning

Introduction

Generally, you deploy phones in batches and maintain company phones via auto provisioning, yet some users would like to keep the personalized settings after auto provisioning.

Keep Users' 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

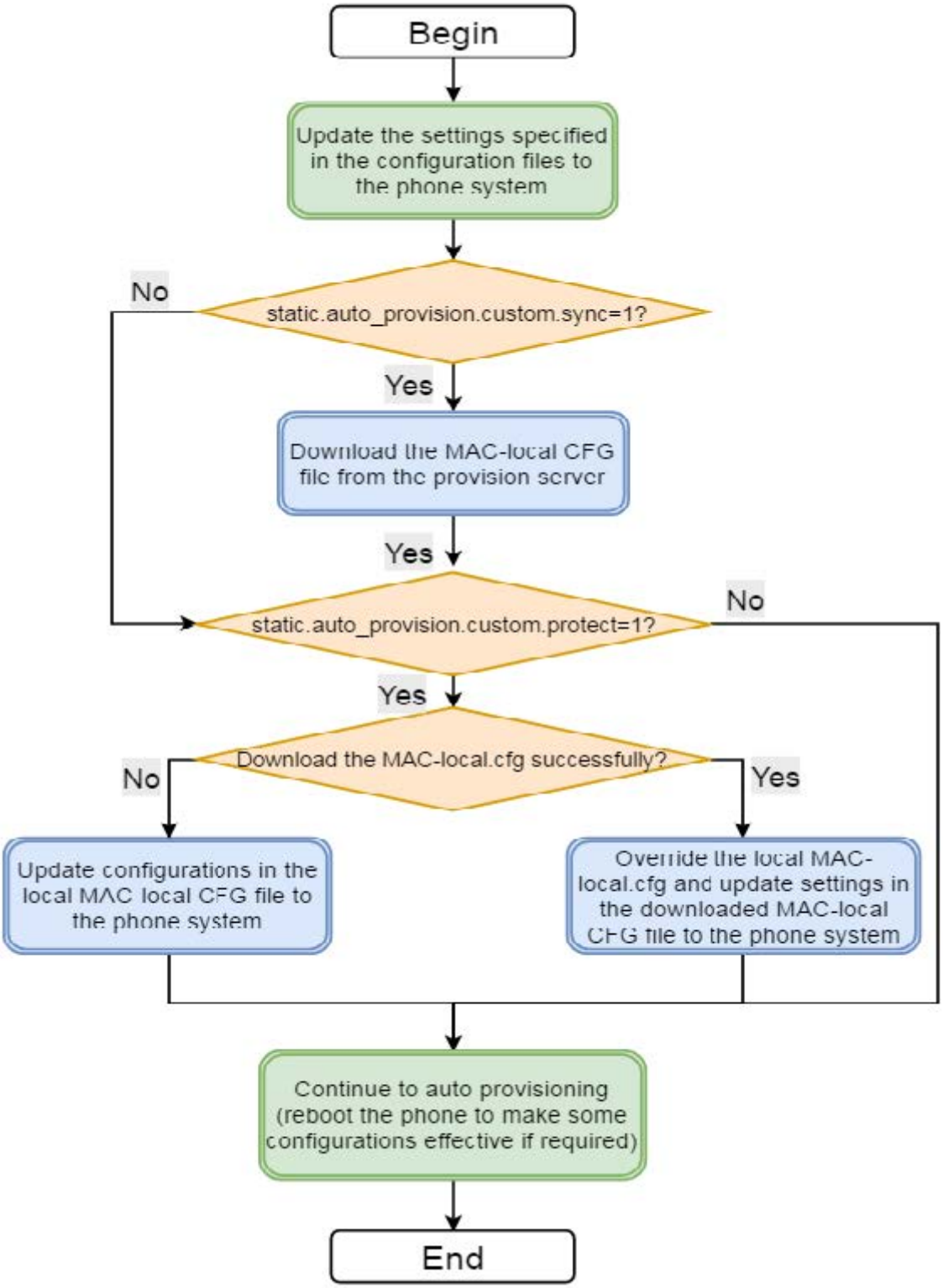
Parameter	Description	Permitted Values	Default
static.auto_provision.custom.protect	It enables or disables the phone to keep the User's personalized settings after auto provisioning. The provisioning priority mechanism (**handset/web user interface** > **central provisioning** > **factory defaults**) 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.	**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
static.auto_provision.custom.sync	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. 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.sy	**0**-Disabled **1**-Enabled	0

	nc.path".		
static.auto_provision.custom.sync.path	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. It works only if "static.auto_provision.custom.sync" is set to 1 (Enabled).	URL	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
static.auto_provision.handset_configured.enable	It enables or disables the base station to deliver custom handset configurations to the handset via auto provisioning/handset reboot/handset registration. It is only applicable to the custom handset related configurations.	**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
static.auto_provision.custom	It enables or disables the handsets to keep user personalized settings after auto provisioning/handset reboot/handset registration.	**0**-Disabled **1**-Enabled	1

.handset.protect	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 Users' 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 Users 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 is generated locally.

Scenario: Keep the 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 breaks down, but the user wishes to keep the 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 parameter 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**.

> 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 CC Phone, 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	Description	Permitted Values	Default
custom.handset.time_format	It configures the time format for all registered handsets. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	**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
custom.handset.date_format	It configures the date format for all registered	**0**-WWW MMM DD **1**-DD-MMM-YY	0

	handsets. The value configured by the parameter "lcl.datetime.date.format" takes precedence over that configured by this parameter.	**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.	
custom.handset.auto_answer.enable	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. It works if the handset is placed in the charger cradle and the parameter "static.au	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled **1**-Enabled	-1

	to_provision.handset_configured.enable" is set to 1 (Enabled).		
custom.handset.keypad_tone.enable	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. 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	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled **1**-Enabled	-1

	(Enabled) and the silent mode is off.		
custom.handset.confirmation_tone.enable	It enables or disables the handset to play a tone when a user saves settings or places the handset in the charger cradle. 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	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled **1**-Enabled	-1

	mode is off.		
custom.handset.low_battery_tone.enable	It enables or disables the handset to play a tone when the battery capacity is low. 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.	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled **1**-Enabled	-1
custom.handset.keypad_light.enable	It enables or disables the handset to turn on	**-1**-Do not modify the configuration. **0**-Disabled **1**-Enabled	-1

	the keypad light (digital key, # key, * key, TRAN key, and Mute key) when any key is pressed. 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]	It enables or disables the handset backlight to be on for about 30 minutes when it is charged. It will take effect on all	**-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

	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]	It enables or disables the handset backlight to be on for about 30 minutes when it is not charged. It will take effect on all handsets that are registered on the same base station. It works only if	**-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

	"static.auto_provision.handset_configured.enable" is set to 1 (Enabled).		
custom.handset.screen_saver.enable[1]	It enables or disables the screen saver feature. 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).	**-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
custom.handset.language	It configures the language used on the handset's user	**0**-English **1**-French **2**-German	0

	interface. 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).	**3**-Italian **4**-Polish **5**-Portuguese **6**-Spanish **7**-Turkish **8**- Russian **9**-Czech (only for CP935W) **10**-Swedish **11**-Slovak (only for CP935W)	

[1] This parameter is only applicable to W53H/W56H/W57R/W59R/W73H/W78H.

PC Mode(Only CP960,CP965)

PC Mode

When the CP960/CP965 is connected to a PC via USB, users can switch between the hybrid UC conference and the idle screen, and can synchronize the volume with the PC.

PC Mode Configuration

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

Configuration parameter

phone_setting.usb.pc_mode
phone_setting.usb.pc_mode.audio_union
phone_setting.usb.pc_mode.default_conference

Parameter	Description	Permitted Values	Default
phone_setting.usb.pc_mode	It specifies the display screen when the phone is connected to the PC via USB.	0-The phone enters the hybrid UC conference screen directly and you cannot return to the idle screen. 1-USB mode is enabled. The phone stays in the screen before connected to the PC and you can return to the idle screen. 2-When the phone is not in a call, the mute LEDs are off; during a call, the mute LEDs glow green. The screen experience is the same as when "phone_setting.usb.pc_mode=1".	1
phone_setting.usb.pc_mode.audio_union	It configures whether the volume is adjusted synchronously on both PC and CP in PC mode.	0-Tap the Volume key on the hybrid UC conference screen (PC-mode screen) or dialing screen to adjust the hybrid UC conference volume;	0

	NOTE It works only if "phone_setting.usb.pc_mode" is set to 1 (Enabled). It works only for the audio volume on CP, not media volume. The CP volume is kept synchronized with the PC volume (only available when "phone_setting.usb.pc_mode = 1 & phone_setting.usb.pc_mode.audio_union = 1" or "phone_setting.usb.pc_mode = 2 & phone_setting.usb.pc_mode.audio_union = 1").	tap the Volume key on the idle screen or other settings screen is used to adjust the ringer volume. 1-Tap the Volume key on any screen to adjust the call volume (media volume or hybrid UC conference volume) and the ringer volume.	
phone_setting.usb.pc_mode.default_conference	It configures whether to invite a new party to the hybrid UC conference after you tap Dial on the idle screen in PC mode. NOTE It works only if "phone_setting.usb.pc_mode" is set to 1 (Enabled).	0-Tap Dial on the idle screen to create a new call. The original call will be held. 1-Tap Dial on the idle screen to invite a new party to the hybrid UC conference directly. When the phone receives an incoming SIP call, tap Answer/Join conf to join the hybrid UC conference directly; tap Reject to return to the previous screen.	0

Door Phone

Introduction

The IP phone is compatible with the 2N and Baudisch IP intercoms. You can pair up to 99 IP intercoms on the IP phone.

When a visitor rings your doorbell, the phone will also ring. You can answer the incoming call and then open the door.

The phones also support the following:

- Preview: get a preview of who’s there when receiving a visitor’s incoming call.
- One-button Open: open the door at any time.
- Monitoring: check the camera video at any time.

In addition to the IP phone, the IP intercom should be configured. For more information on how to configure the IP intercom, refer to the documentation from the manufacturer.

> Door phone feature is only applicable to T56A/T58V/T58W/VP59/T88W/T88W Pro/T88V Pro Phones.

Door Phone Parameters

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

Configuration parameter

```
features.doorphone.amount
features.doorphone.X.device_model
features.doorphone.X.display_name
features.doorphone.X.phone_number
features.doorphone.X.unlock_pin
features.doorphone.X.full_screen
features.doorphone.X.send_audio
features.doorphone.X.send_video
features.doorphone.X.video.stream.httpurl
features.doorphone.X.videopreview.enable
features.doorphone.X.autopreview.enable
```

features.doorphone.X.autopreview_record.enable
features.doorphone.X.httpapi.username
features.doorphone.X.httpapi.password

Parameter	Description	Permitted Values	Default
features.doorphone.amount	It configures how many IP intercoms are supported by the phone.	Integer from 0 to 99	99
features.doorphone.X.device_model[1]	It configures the device type of the IP intercom.	0-Custom 1-2N 3-Baudisch	0
features.doorphone.X.display_name[1]	It configures the display name of the IP intercom to be displayed on the phone’s screen.	String within 99 characters	Blank
features.doorphone.X.phone_number[1]	It configures the phone number or IP address of the IP intercom.	String within 32 characters	Blank
features.doorphone.X.unlock_pin[1]	It configures the unlock PIN of the IP intercom. Example: features.doorphone.1.unlock_pin=8888* When tapping the Open Door soft key after answering the call, the phone will send the DTMF sequence “8888*” to the IP intercom. And if the DTMF sequence matches the code configured on the IP intercom, the door will be opened.	String within 99 characters	Blank
features.doorphone.X.full_screen[1]	It enables or disables the phone to enter full-screen display automatically after answering the visitor’s call. **NOTE**	0-Disabled 1-Enabled	0

	It works only if "video.enable" is not set to 0 (Disabled).		
features.doorphone.X.send_audio[1]	It enables or disables the phone from transmitting your audio during a visitor's call.	0-Disabled 1-Enabled	1
features.doorphone.X.send_video[1]	It enables or disables the phone from transmitting your video during a visitor's call. **NOTE** It works only if "video.enable" is not set to 0 (Disabled), "static.camera.function.enable" is set to 1 (Enabled), and "features.doorphone.X.device_model" is not set to 3 (Baudisch).	0-Disabled 1-Enabled	1
features.doorphone.X.video.stream.httpurl[1]	It configures the video access URL of the IP intercom camera. The valid URL format is: http(s)://<IP address of the IP intercom>/mjpg/video.mjpg or http(s)://username:password@<IP address of the IP intercom>/mjpg/video.mjpg. Example: features.doorphone.1.video.stream.httpurl= http://192.168.1.1/mjpg/video.mjpg **NOTE** You need to configure this parameter if	URL within 511 characters	Blank

	"features.doorphone.X.device_model" is set to 1 (2N) or 3 (Baudisch). If you use the first URL format and the IP intercom needs HTTP API authentication, you should configure the authentication account (configured by the parameters "features.doorphone.X.httpapi.username" and "features.doorphone.X.httpapi.password").		
features.doorphone.X.videopreview.enable[1]	It enables or disables the video preview when receiving a visitor's incoming call. **NOTE** It works only if "account.X.auto_answer" is set to 0 (Disabled) and "video.enable" is not set to 0 (Disabled).	0-Disabled 1-Enabled, when "features.doorphone.X.autopreview.enable" is set to 0 (Disabled), users can tap Preview to check the visitor's video when receiving a visitor's incoming call. The phone will stop playing the ringtone.	0
features.doorphone.X.autopreview.enable[1]	It enables or disables the phone to preview the visitor's video automatically when receiving a visitor's incoming call. **NOTE** It works only if "features.doorphone.X.videopreview.enable" is set to 1 (Enabled),	0-Disabled 1-Enabled, the phone will display the visitor's video automatically when receiving a visitor's incoming call. And the phone keeps playing the ringtone.	0

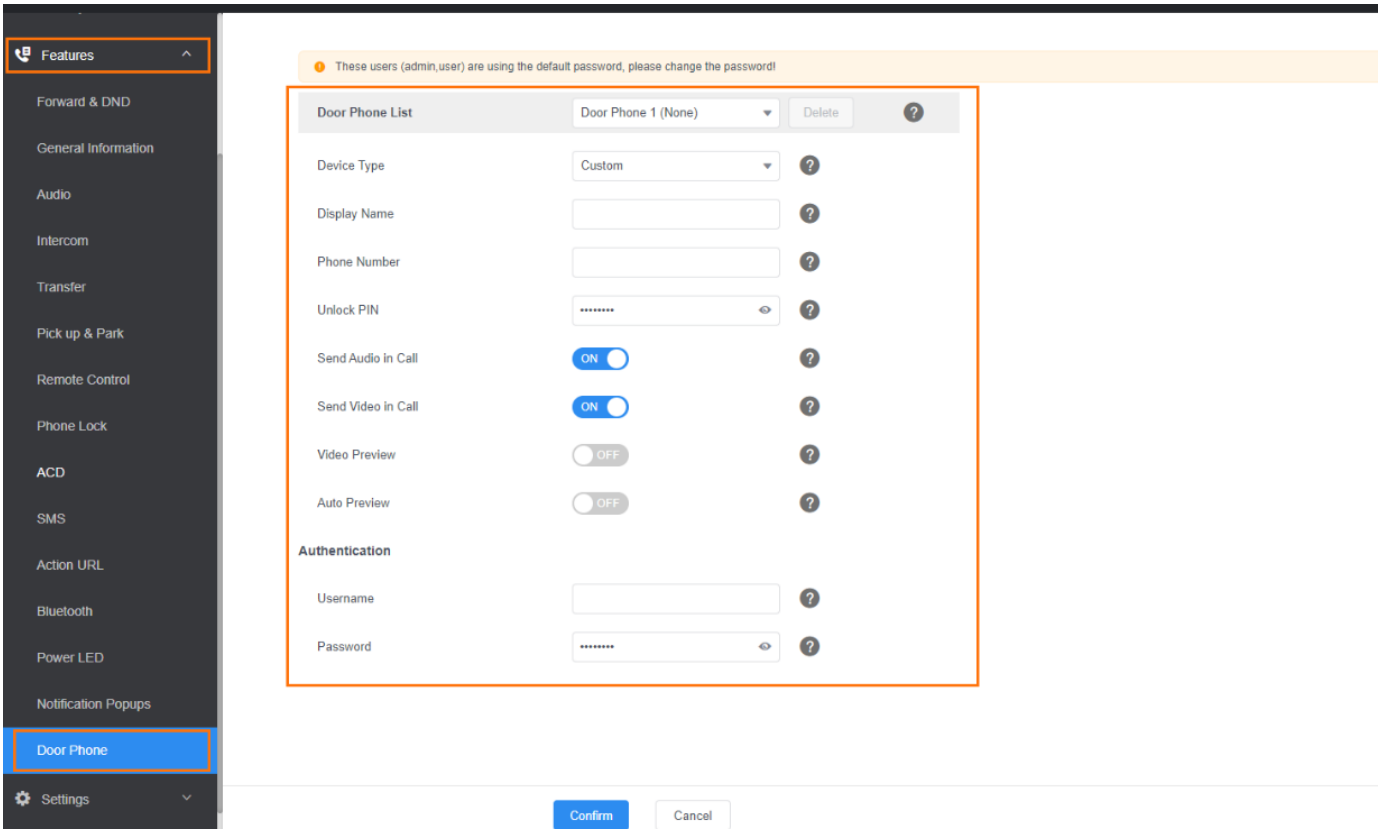
	"account.X.auto_answer" is set to 0 (Disabled), and "video.enable" is not set to 0 (Disabled).		
features.doorphone.X.autopreview_record.enable[1]	It enables or disables the phone to record the preview video automatically when receiving a visitor's incoming call. **NOTE** It works only if "features.doorphone.X.autopreview.enable" is set to 1 (Enabled). It is only applicable to 2N IP intercom.	0-Disabled 1-Enabled, you can check the recorded preview video in the history list or File Manager.	0
features.doorphone.X.httpapi.username[1]	It configures the user name for HTTP API authentication. **NOTE** It is required only when the IP intercom needs HTTP API authentication.	String within 99 characters	Blank
features.doorphone.X.httpapi.password[1]	It configures the password for HTTP API authentication. **NOTE** It is required only when the IP intercom needs HTTP API authentication.	String within 99 characters	Blank
linekey.Y.type[1]	It configures the function of the Xth line key. **NOTE** The corresponding value for "Door Phone" is	For more information, please refer to Dsskeys.	0

	"304". e.g."linekey.2.type=304"		

> [1]X ranges from 1 to 99.
> [2] Y is linekey ID.

Set via the Web User Interface

On the web user interface, go to: **Features** > **Door Phone**



Language

Before You Begin

Only applicable to: T31/T33/T31P/T33P/T33G/T41U/T42U/T43U/T46U/T48U/T57W/T54W/T53W/T53/VP59/T58W/T58V/T58A/T56A/T7X/T8X.

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			

The T48G/T46G/T42G/T41P/T58W/VP59/CP965 phones do not support French (Canada),

Portuguese (Latin) and Spanish (Latin).

Language Display Configuration

The default language displayed on the phone's 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

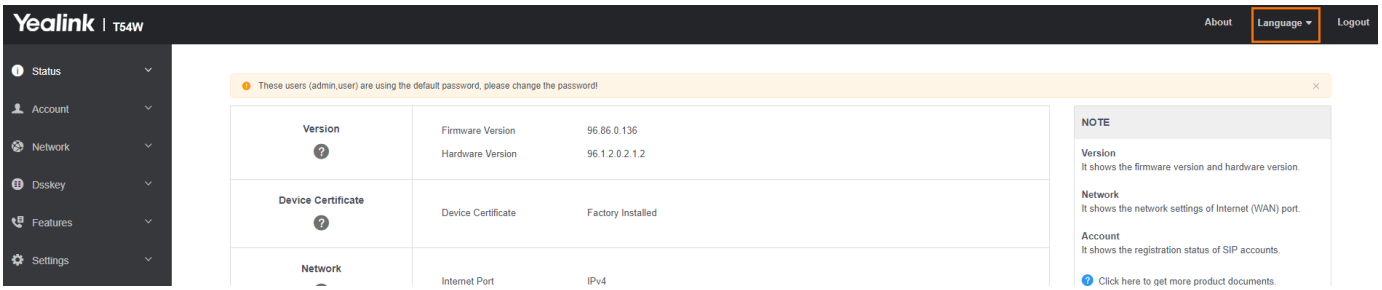
lang.gui
lang.wui

Parameter	Description	Permitted Values	Default	Web UI
lang.gui	It configures the language used on the phone user interface.	T48G/T46G/T42G/T41P: English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian, or the custom language name. T40P/T40G/T29G/T23P/T23G/T21 § E2/T19 § E2: English, Chinese_S, Chinese_T, French_CA, French, German, Italian, Polish, Portuguese, Portuguese_LA, Spanish, Spanish_LA, Turkish, Russian, or the custom language name. CP925/CP935W: English, Chinese_S, Chinese_T, French_EU, German, Italian, Polish, Portuguese_EU, Spanish_EU, Turkish, Russian, Czech, Arabic, Hebrew, Slova,k or the custom language name. Other Phones: 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.

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.

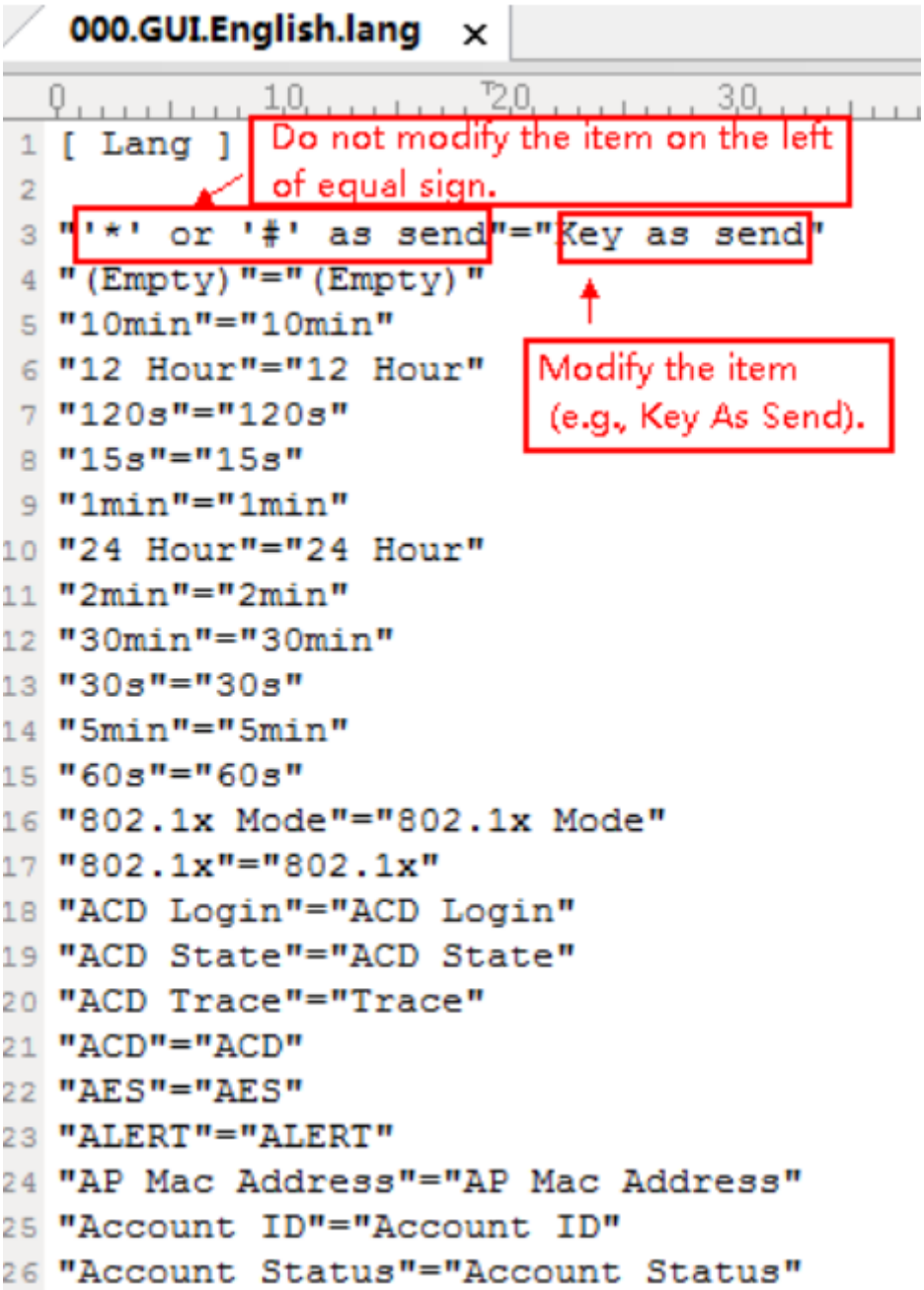
> To modify the translation of an existing language, do not rename the language pack.

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 on 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

r			t
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.

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:

```
L.English_note.xml
<?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>
```

Do not modify the note name.

You can modify the translation of the note name.

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	URL within 511 characters For example http://localhost/	Blank

	for the web user interface.	X.GUI.name.lang X starts from 014, “name” is replaced with the language name	
wui_lang_note.url	It configures the access URL of the custom note language pack for the web user interface.	URL within 511 characters For example http://localhost/X.name_note.xml X starts from 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

Contrast

Introduction

Contrast determines the readability of the texts displayed on the LCD screen. Adjusting the contrast to a comfortable level can optimize the screen viewing experience.

You can adjust the contrast for T53W/T53/T43U/T40P/T40G/T31P/T31G/T31/T30P/T30/T27G/T23P/T23G/T21 E2/T21P E2/T19 E2/T19P E2/CP920 phones, or for expansion module EXP20 (connected to T29G/T27G phones), EXP40 (connected to T48S/T48G/T46S/T46G phones).

The following table lists the parameters you can use to adjust contrast for the phone.

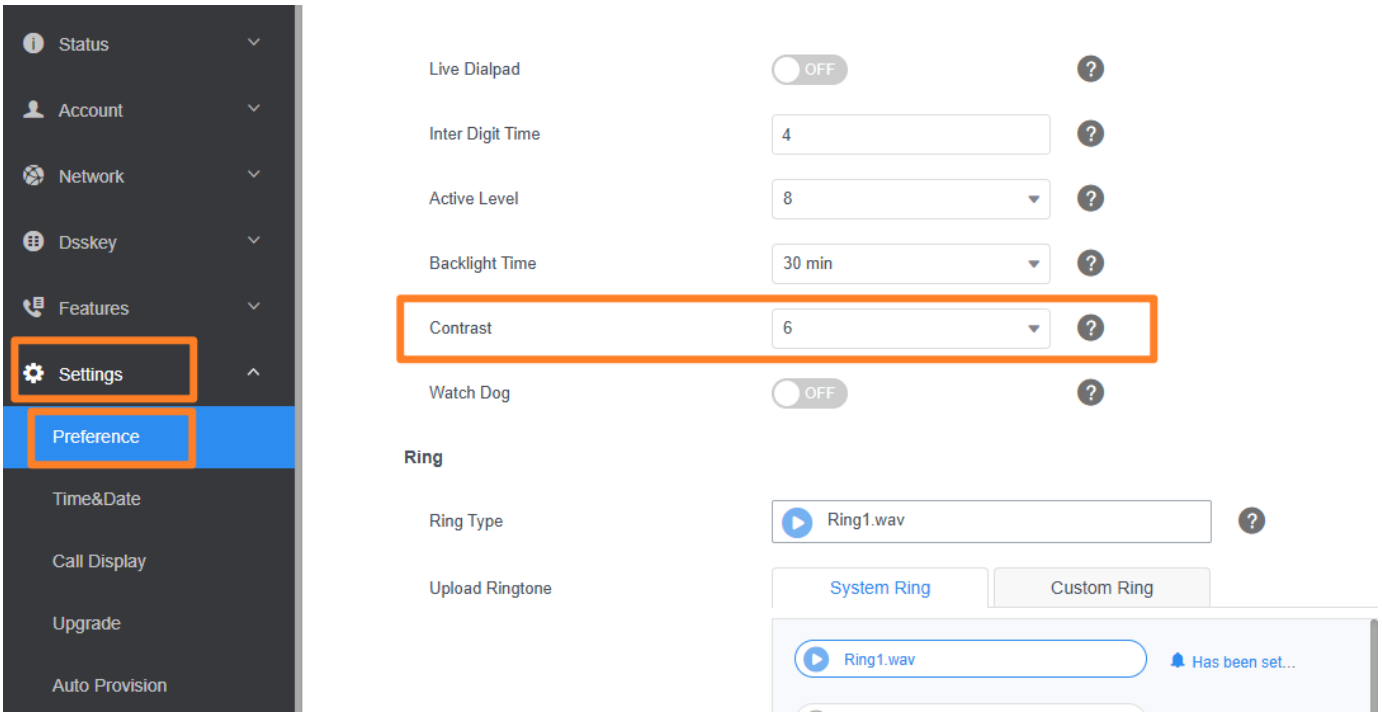
Configuration Parameter

phone_setting.contrast

Parameter	Permitted Values	Default	Description
phone_setting.contrast	Integer from 1 to 10	6	It configures the contrast of the LCD screen. For T53W/T53/T43U/T31P/T31G/T31/T30P/T30/T40P/T40G/T23P/T23G/T21 E2/T21P E2/T19 E2/T19P E2 phones, it configures the LCD's contrast of the IP phone. For T48S/T48G/T46S/T46G phones, it configures the LCD's contrast of the connected EXP40 only. For T29G phones, it configures the LCD’s contrast of the connected EXP20 only. For T27G phones, it configures the LCD’s contrast of the IP phone and the connected EXP20. We recommend that you set the contrast of the LCD screen to 6 as a more comfortable level.

Set via the Web User Interface

On the web user interface, go to: **Settings** > **Preference** > **Contrast**.



Transparency

Introduction

Phones display line keys and status bars transparently, if you use a custom picture with a color or complex background, it may affect the user' s experience. You can choose the appropriate transparency for DSS key labels and the status bar on the idle screen as required.

1. This is only applicable to T57W/T54W/T48U/T48S/T48G/T73U(W)/T74U(W)/T77U/T85W/T87W phones.
2. On T7XT8X, only the transparency of the Dsskey can be adjusted, while the transparency of the tab bar cannot be adjusted.

The transparency is adjusted to **10%** (**left image below**) and **50%** (**right image below**), and the effect on the T73U is as follows:

The transparency is adjusted to **0%** (**left image below**) and **100%** (**right image below**), and the effect

on the T48U is as follows:

The following table lists the parameter you can use to adjust transparency.

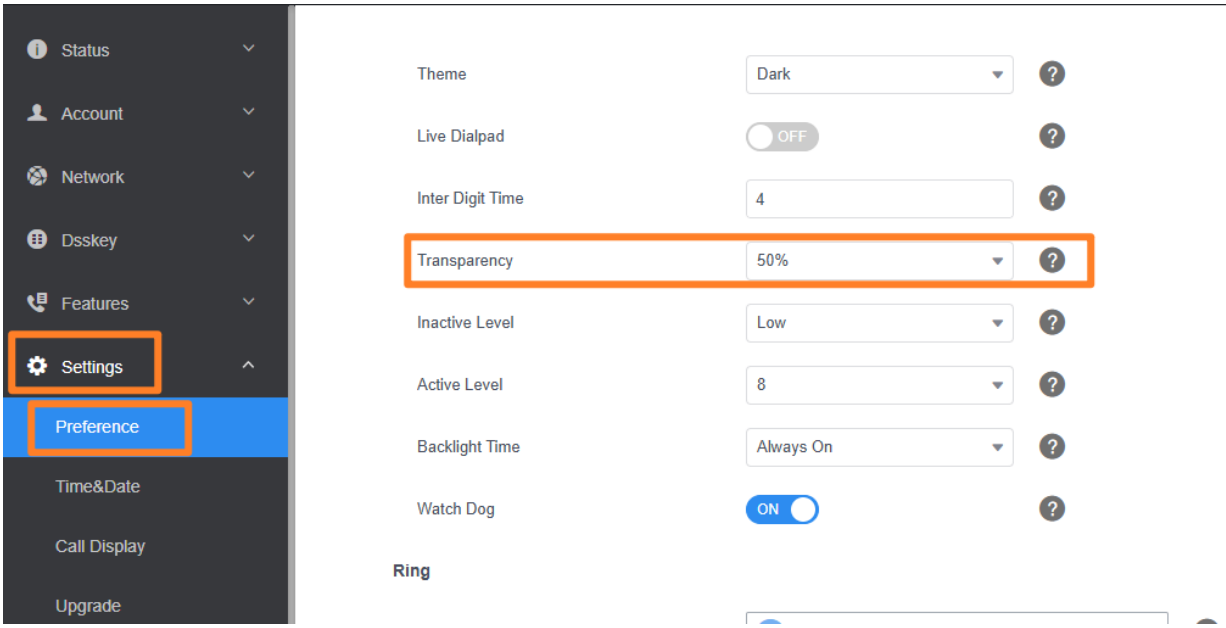
Configuration Parameter

phone_setting.idle_dsskey_and_title.transparency

Parameter	Permitted Values	Default	Description
phone_setting.idle_dsskey_and_title.transparency	For T7XT8X: 10%, 20%, 30%, 40% or 50% For T4XT5X: 0%, the DSS key labels and status bar are non-transparent. 20%, 40%, 60%, 80% or 100%	For T7XT8X: 20% For T4XT5X: 100%	It configures the transparency of the DSS key labels and status bar on the idle screen for the IP phone. It is also applicable when the DSS key list is unfolded on the T57W/T48U/T48S/T48G phones.

Set via the Web User Interface

On the web user interface, go to: **Settings** > **Preference** > **Transparency.**



Backlight Setting

Introduction

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. It is not available on T30P/T30/T19 § E2 phones.

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 T57W/T54W/T53C/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T33P/T33G IP phone and Video phone.
- 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).

Supported Backlight Options

The following table lists available configuration options to configure the backlight of phone models/expansion modules:

Phone Model (and the connected expansion module)	Configuration Options
T57W(EXP50) T54W(EXP50) T53C(EXP50) T48U(EXP43) T48S/G(EXP40) T46U(EXP43) T46S/G(EXP40) T33P/T33G T29G(EXP20) CP925 CP935W VP59 T58W T56A T58V/A CP965 CP960	Inactive Level (not applicable to EXP50/EXP43) Active Level Backlight Time (not applicable to EXP50/EXP43)
T53W/T53(EXP50) T43U(EXP43) T31P/T31G/T31 T27G(EXP20) T42U	Active Level Backlight Time (not applicable to EXP50/EXP43)
T42S/G T41P/S T40P/G T23P/G T21(P) E2/ CP920	Backlight Time

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
phone_setting.on_call.backlight_mode
```

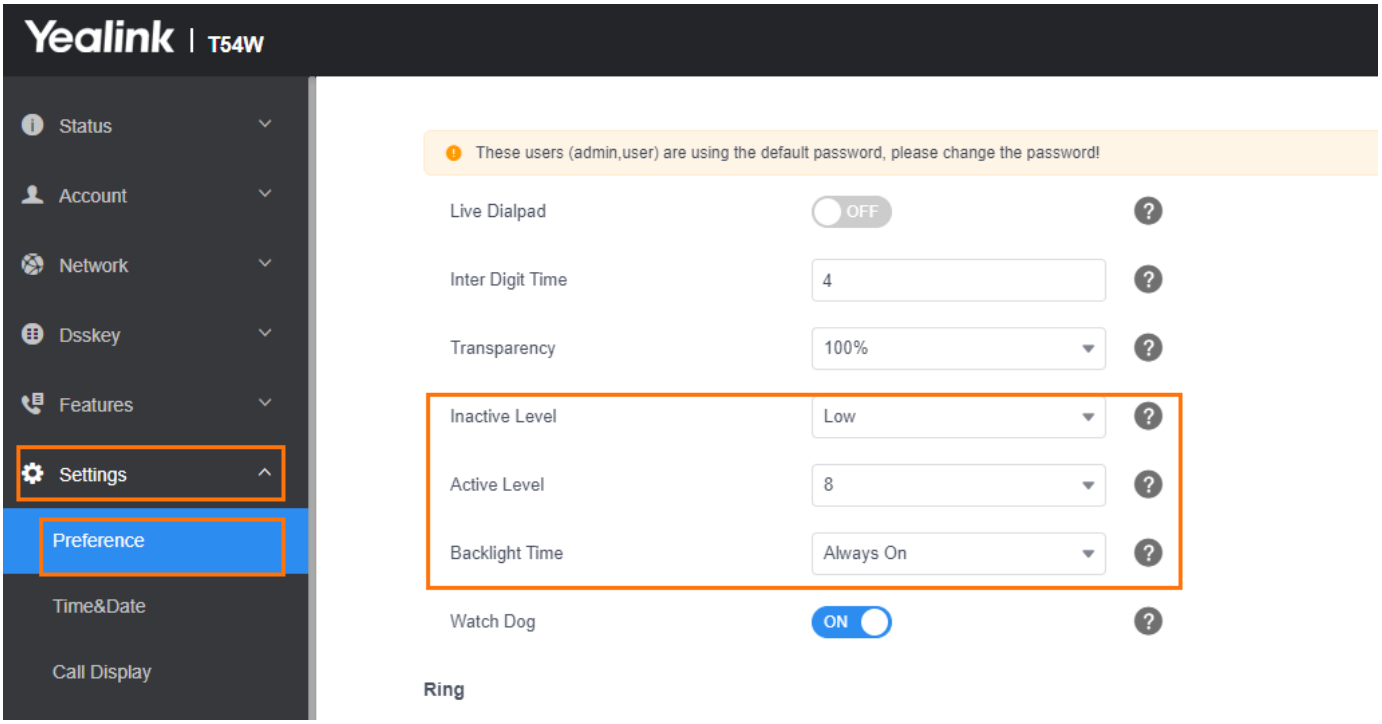
Parameter	Permitted Values	Default	Description
phone_setting.active_backlight_level	Integer from 1 to 10	8	It configures the intensity of the LCD screen when the phone is active. **NOTE** If the expansion module is connected, the backlight on the expansion module automatically changes to match this setting.
phone_setting.inactive_backlight_level	0-Off, it works only if “phone_setting.backlight_time” is not set to 1 (Always On).	1	It configures the intensity of the LCD screen when the phone

	1-Low		is inactive. **NOTE** If expansion module EXP20 or EXP40 is connected, the backlight on the expansion module automatically changes to match this setting.
phone_setting.backlight_time	0-Always On 1-Always Off (not applicable to color screen phones) 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 The permitted values for web/phone UI are Always On (default), 30min, 1h, 2h, 4h, 6h, 8h, 12h.	0	It configures the delay time (in seconds) to change the intensity of the LCD screen when the phone is inactive.
phone_setting.on_call.backlight_mode	0-When talking for about 2 minutes without any operation on the phone, the backlight is reduced to 10% brightness when the "phone_setting.inactive_backlight_level	0	It configures the backlight brightness of the phone during a call.

	" is set to 1. 1-The backlight always maintains the intensity set by " phone_setting.active_backlight_level" during a call.		

Set via the Web User Interface

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



Linekey Setting

Label Length Display Configuration

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

Configuration parameter

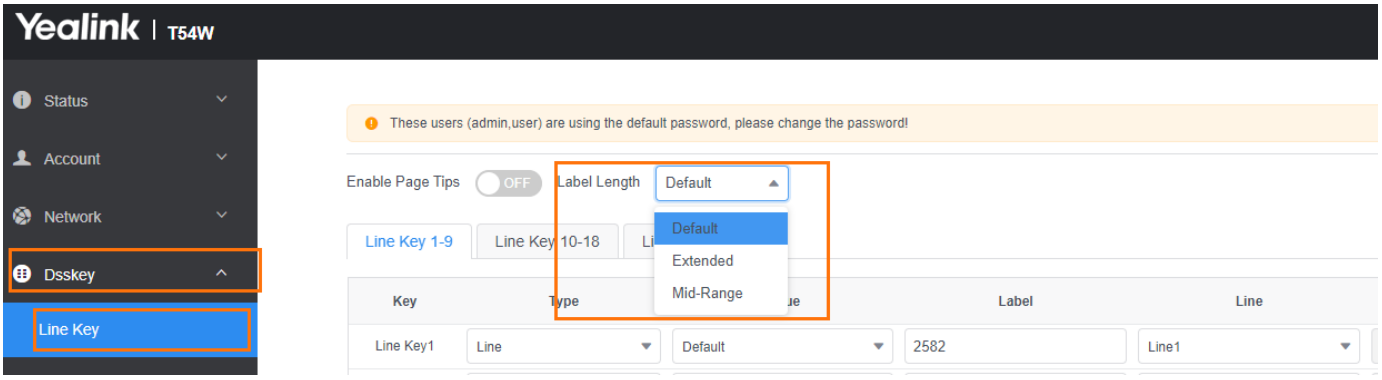
features.config_dsskey_length
features.shorten_linekey_label.enable

Parameter	Description	Permitted Values	Default	Supported Devices

features.config_dsskey_length	It configures the label length displayed on the idle LCD screen for the line key.	0-Default 1-Extended 2-Mid-Range (only applicable to T7X/T8X/T54W/T46U/T46S/T46G/T29G phones)	0	All color screen phones except CP925/CP935W
features.shorten_linekey_label.enable	It enables or disables the phone to display the length of the line key label with 9 digits. It works only if "features.config_dsskey_length" is set to 0 (Default).	0-Disabled, the line key label can display at most 8 digits. 1-Enabled, the line key label can display at least 9 digits.	0	T7X, T8X, T54W, T46U, T46S, T46G, T29G

Set via the Web User Interface

On the web user interface, go to: **Dsskey** > **Line Key** > **Label Length.**



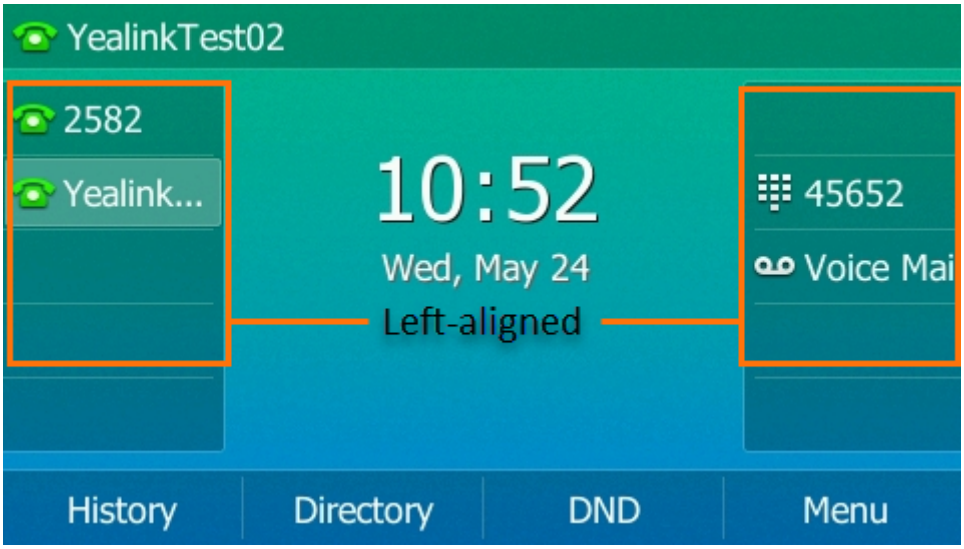
Label Alignment for Line/Ext Key Display

You can customize the line/Ext key label alignment.

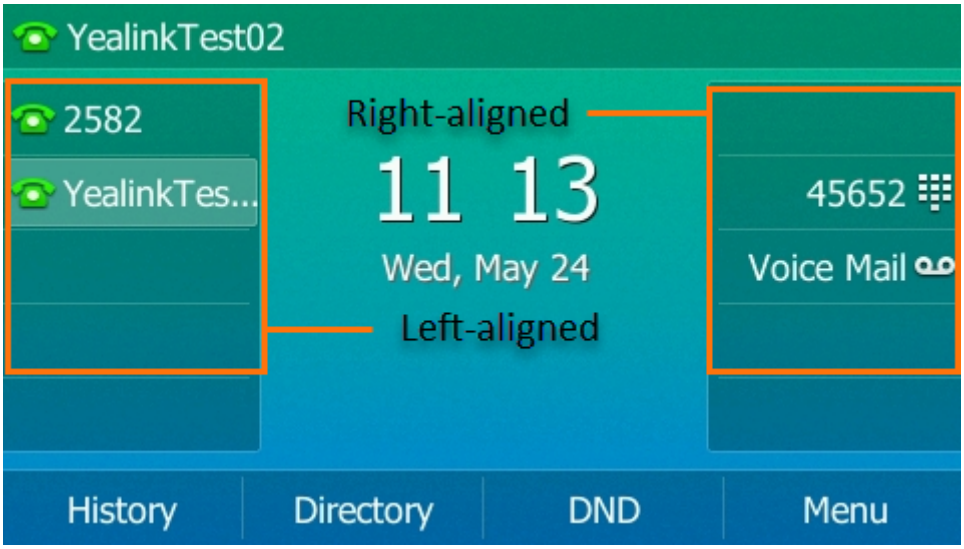
This feature is only applicable to T54W/T53C/T46U/T46S/T46G/T33P/T33G/T29G phones/Video phone and expansion module EXP50 (connected to the T57W/T54W/T53W/T53/T53C phones)/EXP43 (connected to the T48U/T46U/T43U phones).

The following figures show the line key label alignment on T54W phone:

Left aligned:



Right aligned:



Label Alignment Display Configuration

The following table lists the parameter you can use to configure the label alignment display.

Parameter	Description	Permitted Values	Default	Supported Devices
phone_setting.dsskey_label.display_method	• It configures the alignment mode of the line key/Ext key label. • If some Ext keys already exist before configuration, you need to refresh the	0-the label and icon align left 1-when the line key/Ext key is on the left side of the screen, the label and icon align left; when the line	0	T54W, T53C, T46U, T46S, T46G, T33P, T33G, T29G, EXP50 connected to the T57W/T54W/T53W/T53/T53C phones/video phone, and EXP43 connected to the T48U/T46U/T43U phones

	page (press the page keys, or try re-connecting the expansion module) to make the change take effect.	key/Ext key is on the right side of the screen, the label and icon align right		

Page Switch Key

By default, the page switch key is available only if a line key not located on the first page is assigned functionality. If you want to configure line keys on more pages from the idle screen quickly, you can configure the line key in the right bottom to be a page switch key.

> It is only applicable to T54W/T53W/T53/T53C/T46U/T46S/T46G/T43U/T42U/T42S/T42G/T41P/T41S/T33P/T33G/T29G/T27G phones.

Page Switch Key Configuration

The following table lists the parameter you can use to configure the page switch key.

Configuration parameter

```
features.keep_switch_page_key.enable
```

Parameter	Description	Permitted Values	Default
features.keep_switch_page_key.enable	It enables or disables the line key in the bottom right of the phone to be fixed as a page switch key.	0-Disabled, the page icons appear only if a line key not located on the first page is assigned functionality. Then you can use the hard line key in the right bottom to switch pages. 1-Enabled	0

Page Tips

Page tips feature allows the page switch key to indicate different key status on the non-current page. It is mainly used when multi-page line keys are configured.

Yealink T54W/T53W/T53/T53C/T46U/T46S/T46G/T43U/T42U/T42S/T42G/T41P/T41S/T33P/T33G/T29G/

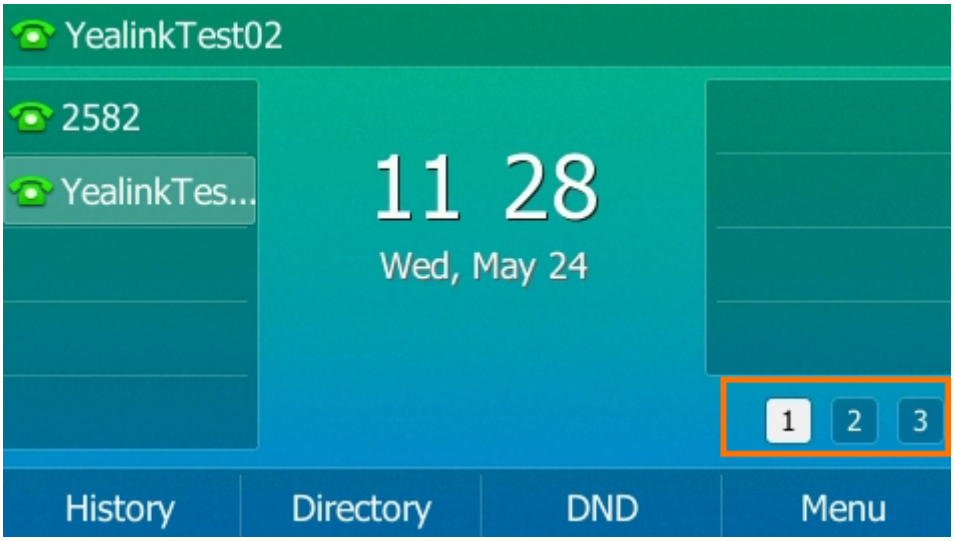
T27G/CP925/CP935W phones and expansion module EXP50/EXP43 support page tips.

Phone Page Tips

On T54W/T53W/T53/T53C/T46U/T46S/T46G/T43U/T42U/T42S/T42G/T41P/T41S/T33P/T33G/T29G/T27G/CP925/CP935W phones, the page tips feature supports the page icon and page switch key LED to indicate different line key status.

Phone Page Tips Indicator

The following shows the page icons on T54W phone:



Phone Page Tips Configuration

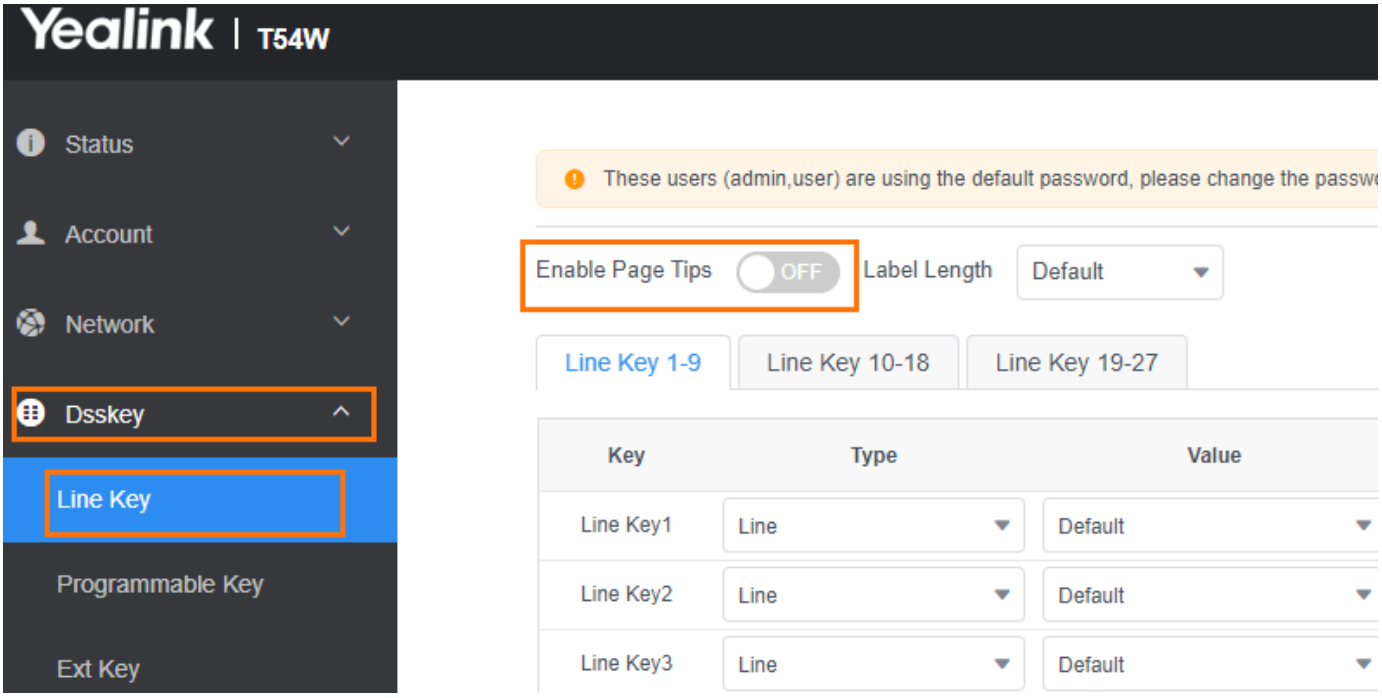
The following table lists the parameter you can use to configure phone page tips.

Configuration parameter

phone_setting.page_tip

Parameter	Description	Permitted Values	Default
phone_setting.page_tip	It enables or disables the page icon and page switch key LED to indicate the different status of line keys on the non-current page.	0-Disabled 1-Enabled	0

Set via the Web User Interface



Expansion Module Page Tips

On the expansion module EXP50/EXP43, the page tips feature allows the page switch key LED to indicate that the BLF monitored user receives an incoming call on the non-current page.

Expansion Module Page Tips Indicator

The following table lists the status of the page switch key LED displayed on the expansion module:

Models	LED Status	Icons	Description
EXP50/ EXP43	Flashing red	/	The BLF monitored user receives an incoming call on the non-current pages.

Expansion Module Page Tips Configuration

The following table lists the parameters you can use to configure expansion module page tips.

Configuration parameter

```
expansion_module.page_tip.blf_call_in.enable
expansion_module.page_tip.blf_call_in.led
```

Parameter	Description	Permitted Values	Default	Supported Devices
expansion_module.page_tip.blf_call_in.enable	It enables or disables the page switch key LED on the EXP50/ EXP43 expansion module to	0-Disabled 1-	1	T57W, T54W, T53W, T53,

	indicate when BLF monitored user receives an incoming call on the non-current pages.	Enabled		T53C, T48U, T46U, T43U, T56A, T58A/V/W, VP59
expansion_module.page_tip.blf_call_in.led	It configures the page switch key LED status on the EXP50/EXP43 expansion module when BLF monitored user receives an incoming call on the non-current pages. This value uses the same macro action string syntax as an Enhanced DSS key. If it is left blank, the default value takes effect. Example: expansion_module.page_tip.blf_call_in.led = $LEDr300o300$ It means an infinite loop for the page switch key LED status: glow red for 300ms and then be in the off state for 300ms. It works only if "expansion_module.page_tip.blf_call_in.enable" is set to 1 (Enabled).	String	$LEDr300o300$	T57W, T54W, T53W, T53, T53C, T48U, T46U, T43U, T56A, T58A/V/W, VP59

Key As Send

Key as send allows you to assign the pound key (“#”) or asterisk key (“*”) as the send key.

Key As Send Configuration

The following table lists the parameters you can use to configure the key as send.

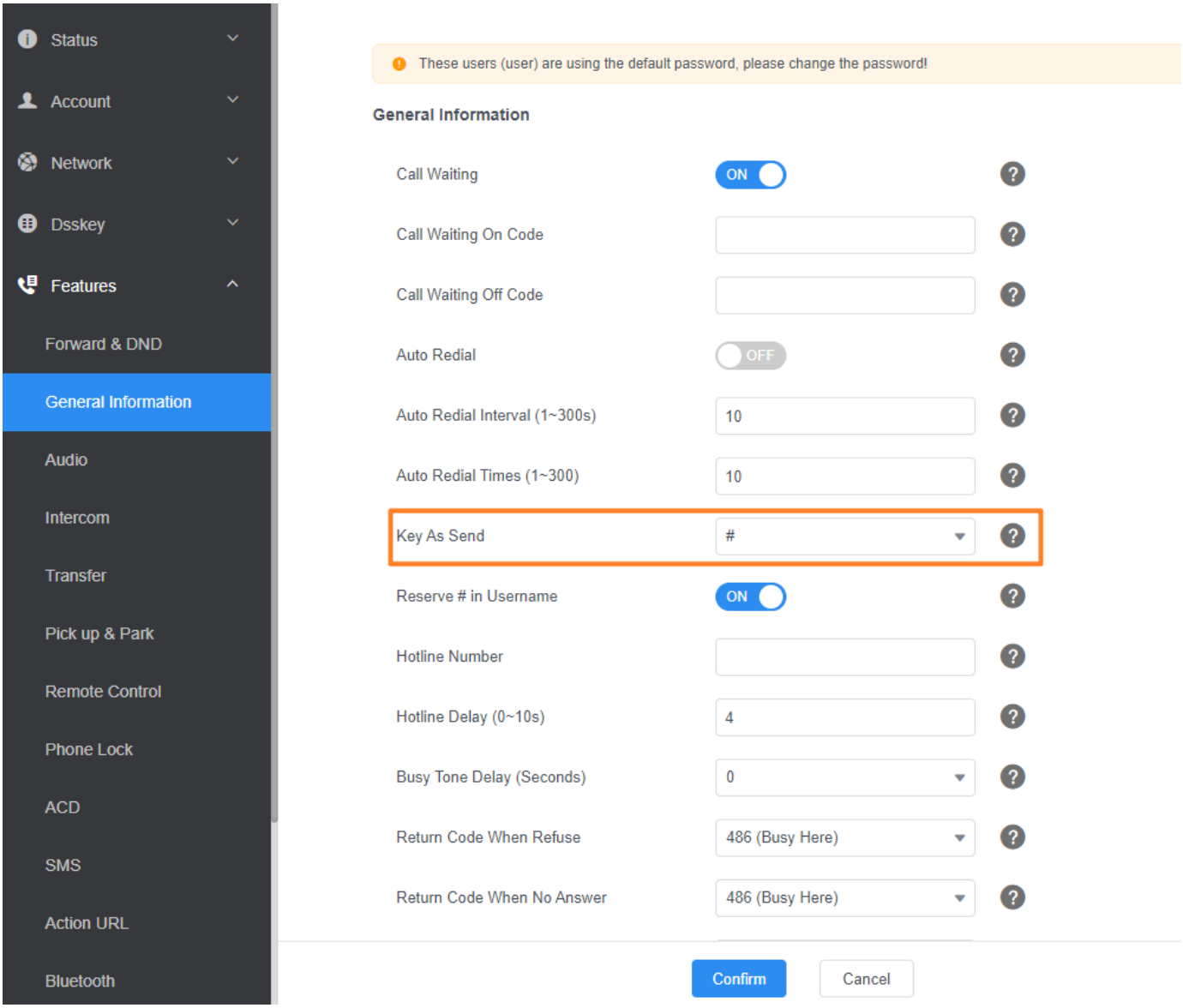
Configuration parameter

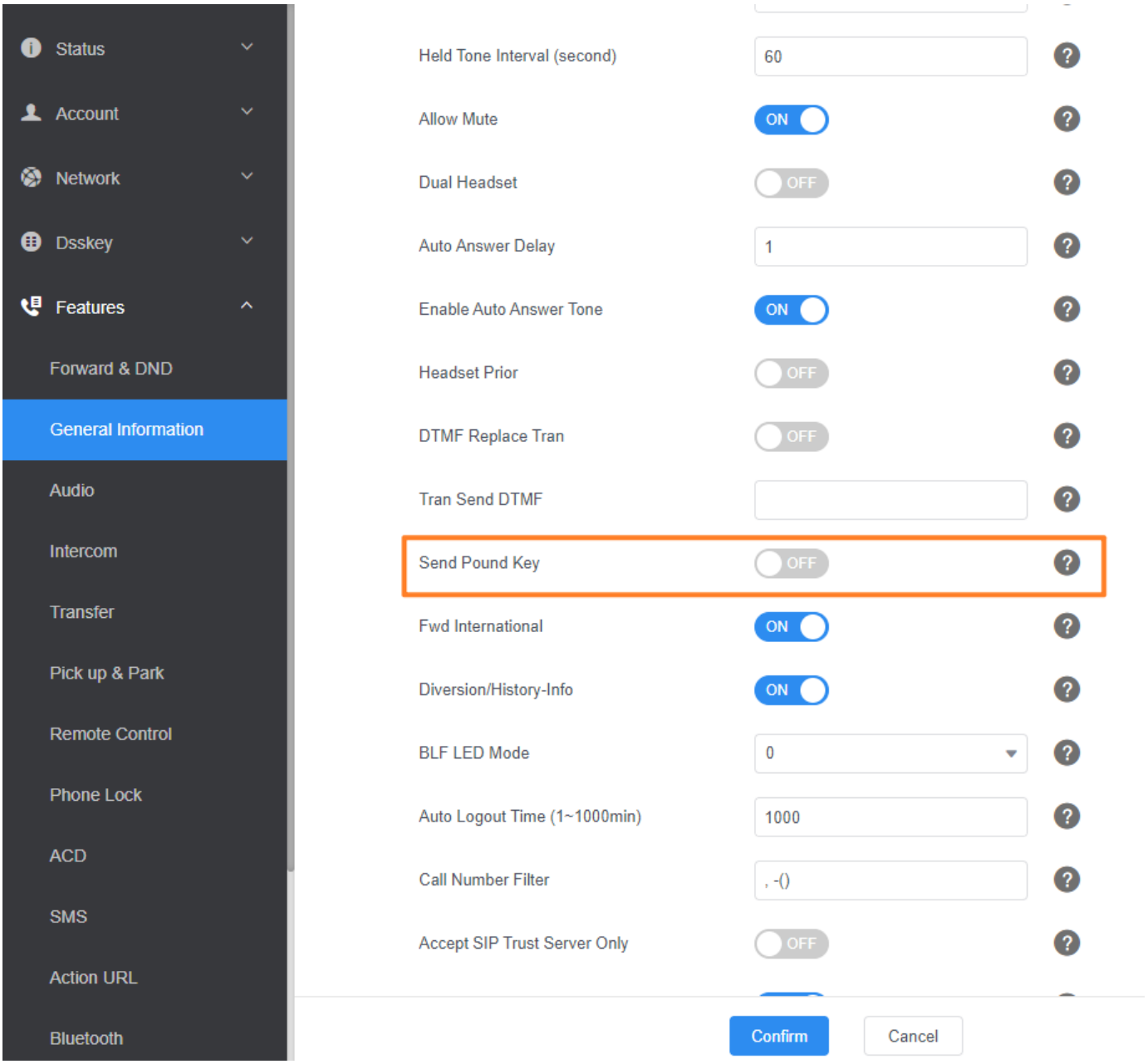
```
features.key_as_send
features.send_pound_key
```

Parameter	Description	Permitted Values	Default	Supported Devices
features.key_as_send	It configures the "#" or "*" key as the send key.	0-Disabled, neither “#” nor “*****” can be used as the send key. 1-# key 2-* key	0	All phones except CP925/CP935W
features.send_pound_key	It configures the behavior when the user presses the # key twice on the dialing screen. It works only if "features.key_as_send" is set to 1 (# key).	0-The phone will dial out “#”. 1-The phone will not dial out “#”. After the user presses the # key again, the phone will dial out “##”.	0	All phones except CP925/CP935W

Set via the Web User Interface

On the web user interface, go to: **Features** > **General Information** > **Key As Send&Send Pound Key.**


Status
Account
Network
Dsskey
Features
Forward & DND
General Information
Audio
Intercom
Transfer
Pick up & Park
Remote Control
Phone Lock
ACD
SMS
Action URL
Bluetooth
These users (user) are using the default password, please change the password!
General Information
Call Waiting
ON
Call Waiting On Code
Call Waiting Off Code
Auto Redial
OFF
Auto Redial Interval (1~300s)
10
Auto Redial Times (1~300)
10
Key As Send
#
Reserve # in Username
ON
Hotline Number
Hotline Delay (0~10s)
4
Busy Tone Delay (Seconds)
0
Return Code When Refuse
486 (Busy Here)
Return Code When No Answer
486 (Busy Here)
Confirm
Cancel



Time and Date

Introduction

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	Time Zone Name	Time	Time Zone Name

Zone		Zone	
-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
local_time.android_time_zone
```

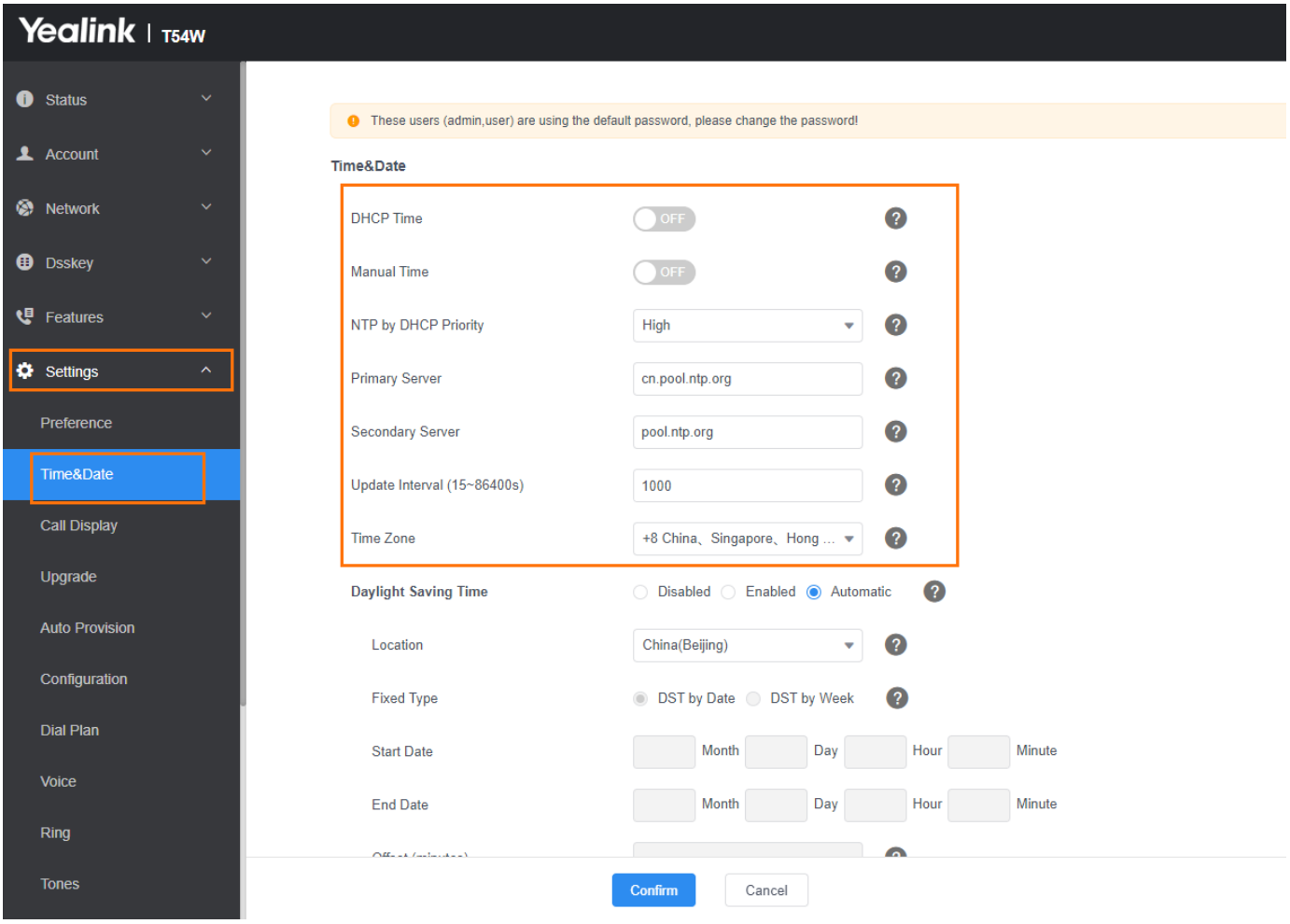
Parameter	Description	Permitted Values	Default

			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. 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. 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)
local_time.android_time_zone	Specify the system time zone using a standard time zone name that must exist in the TZDatabaseName.xml file (e.g., Asia/Beijing). Daylight saving time rules are defined automatically by the time zone database and require no additional configuration.	String within 64 characters	NULL

Set via the Web User Interface

On the web user interface, go to: **Settings** > **Time & Date.**



TIP

- The default NTP server addresses for the T3X, T4XU, and T5XW series of Yealink devices have been changed after version x.86.0.139. The Primary Server default address has been changed to "pool.ntp.org," and the Secondary Server default address has been changed to "time.windows.com."
- The T44U/T44W's time and date display format cannot be changed. The current version only supports the 24-hour clock format and the date format is fixed as MM/DD.

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 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"/>
```

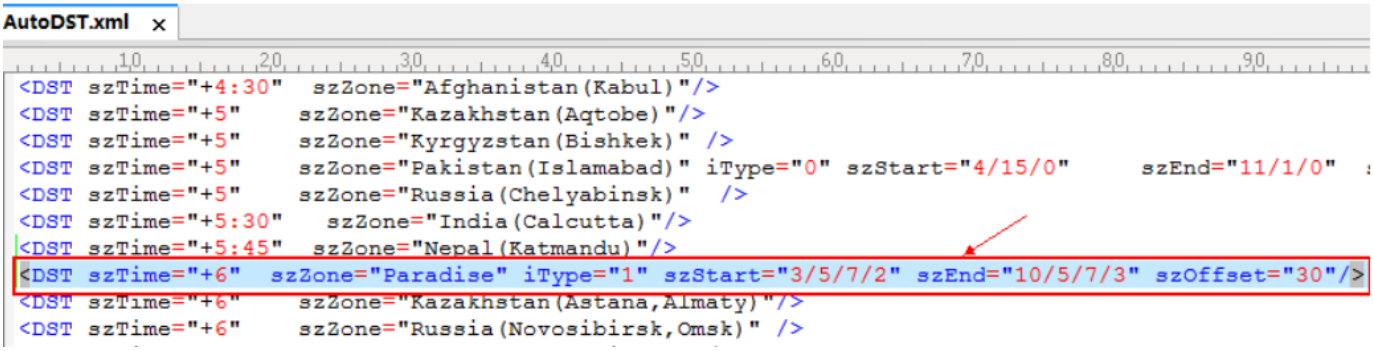
```
<DST szTime="-10"      szZone="United States-Alaska-Aleutian"/>
<DST szTime="-9:30"  szZone="French Polynesia"/>
<DST szTime="-9"      szZone="United States-Alaska Time"      iType="1"
szStart="3/2/7/2"      szEnd="11/1/7/2"    szOffset="60"/>
<DST szTime="-8"       szZone="Canada(Vancouver,Whitehorse)"  iType="1"
szStart="3/2/7/2"       szEnd="11/1/7/2"    szOffset="60"/>
<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="60"/>
<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="60"/>
<DST szTime="-7"     szZone="United States-Mountain Time" iType="1"
szStart="3/2/7/2"       szEnd="11/1/7/2"    szOffset="60"/>
</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)” .

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

Modify it:
iType="1" szStart="10/1/7/2" szEnd="4/1/7/3" szOffset="60"

Add DST
```

4. Save this file and place it to 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	Defau lt
local_time.s ummer_time	It configures the Daylight Saving Time (DST) feature.	0-Disabled 1-Enabled 2-Automatic	2
local_time.ds t_time_type	It configures the Daylight Saving Time (DST) type. It works only if "local_time .summer_ti me" is set to	0-DST by Date 1-DST by Week	0

	1 (Enabled).		

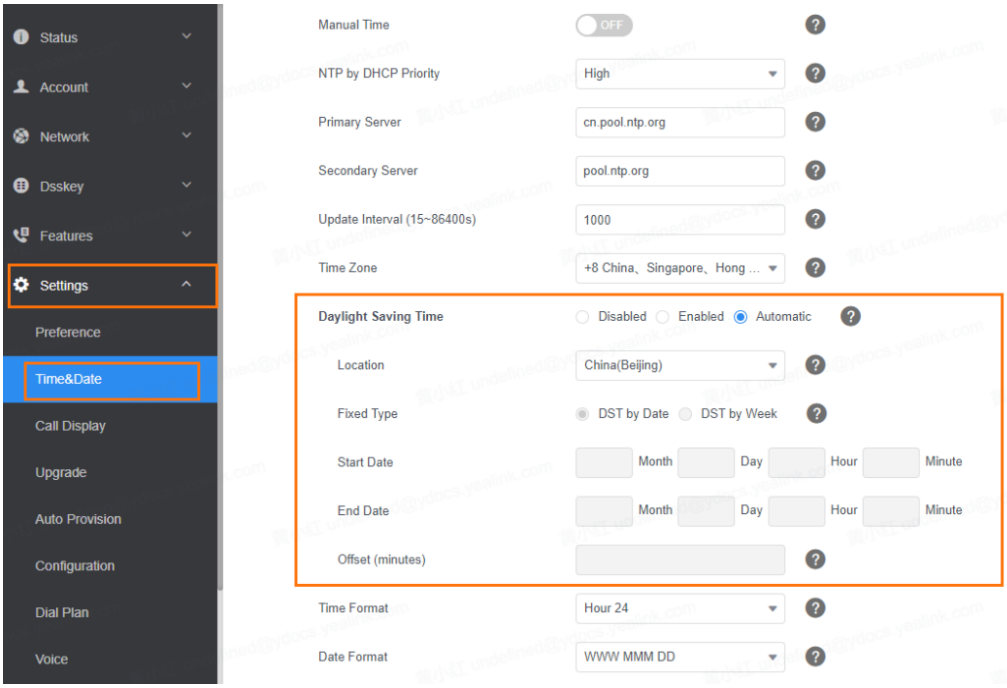
local_time.start_time	It configures the start time of Daylight Saving Time (DST).
	It works only if "local_time.summer_time" is set to 1 (Enabled).
		// Month/Day/Hour:Minute-DST by Date, use the following mapping:
		- Month: 1=January, 2=February,…, 12=December
		- Day: 1=the first day in a month,…, 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).
	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
			12/31/23

		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	
local_time.offset_time	It configures the offset time (in minutes) of Daylight Saving Time (DST). 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). 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 Manual 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 parameters 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

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 customize the date format as required.

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

Configuration parameter

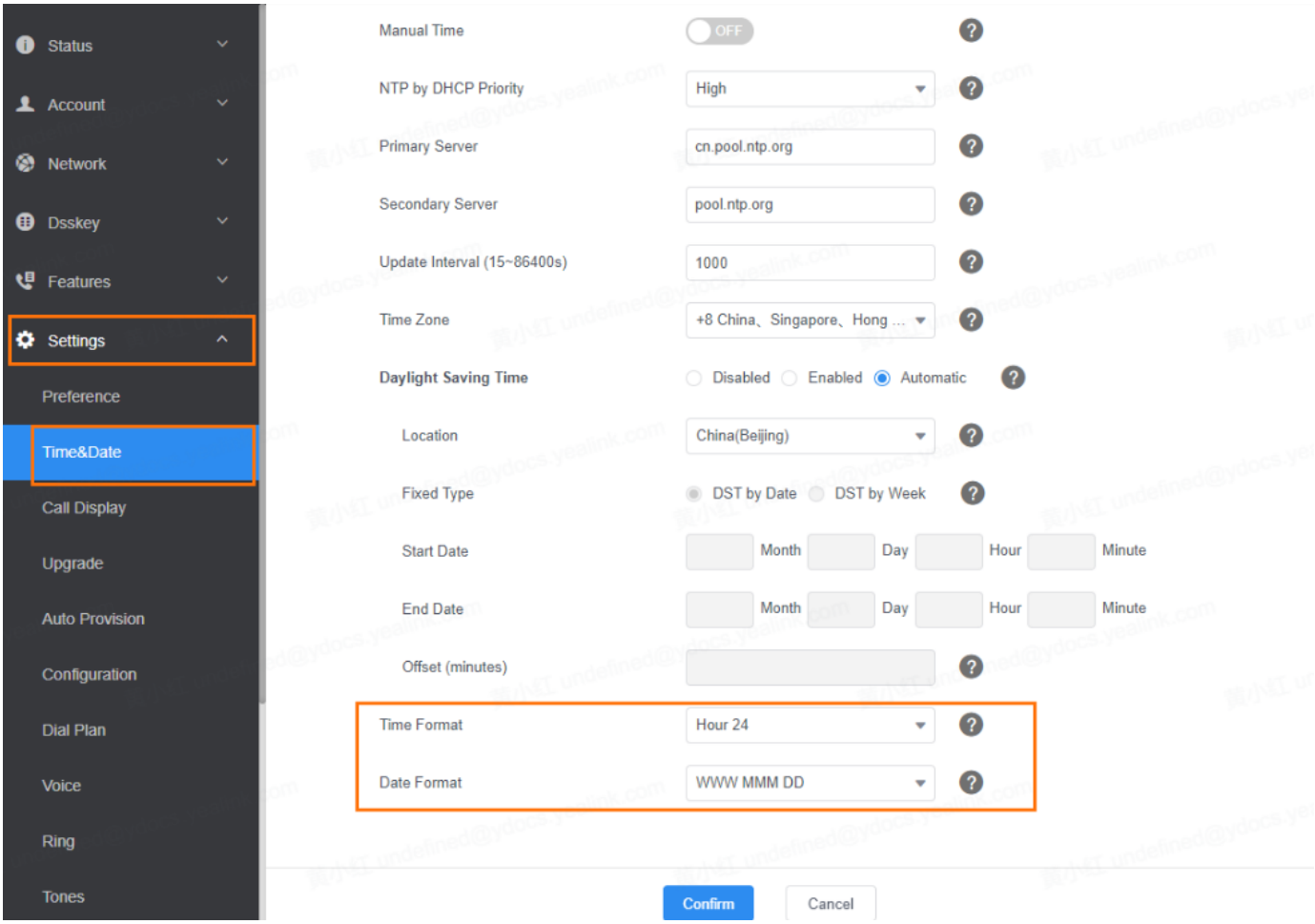
```
local_time.time_format
local_time.date_format
lcl.datetime.date.format
```

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. The value configured by the parameter "lcl.datetime.date.format" takes precedence over that configured by	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;	0

	this parameter.	“MMM” represents the first three letters of the month; “YYYY” represents a four-digit year, and “YY” represents a two-digit year.	
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 the 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（Data Format).**



Date Customization Rule

You need to know the following rules when customizing date formats:

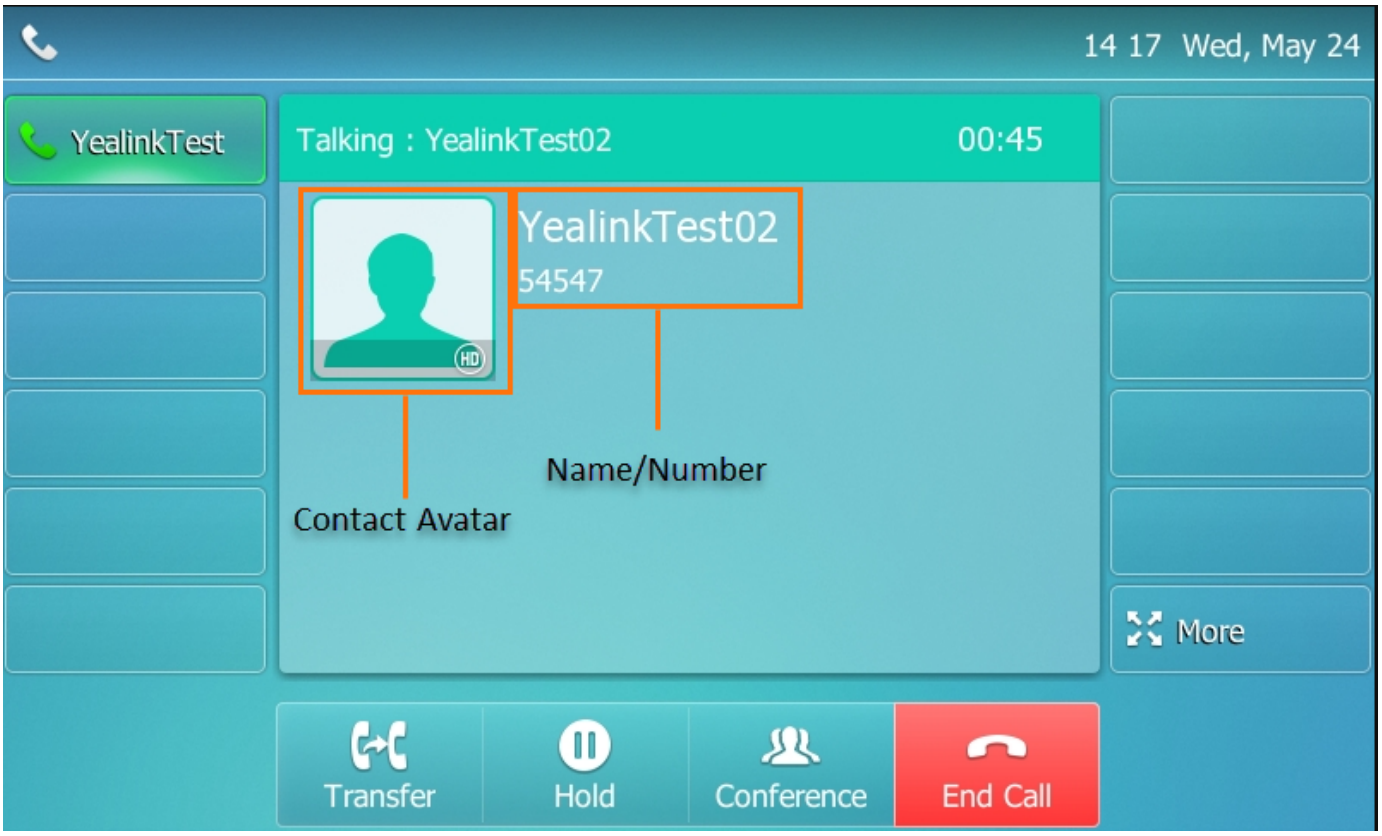
Format	Description
Y/YY	It represents a two-digit year. For example, 16, 17, 18⋯
Y is used more than twice (for example, YYY, YYYY)	It represents a four-digit year. For example, 2016, 2017, 2018⋯
M/MM	It represents a two-digit month. For example, 01, 02,⋯, 12
MMM	It represents the abbreviation of the 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

Call Display

Introduction

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 to present 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
features.number_privacy.enable
features.number_privacy.start_length

Parameter	Description	Permitted Values	Default	Supported Devices
phone_setting.contact_photo_display.enable	It configures whether to display the contact avatar when it receives an incoming call, dials an outgoing call, or engages in a call.	0-Never, do not displaythe 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	All color screen phones
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,	0-Disabled 1-Enabled, the phone can display the full 16-digit number.	1	T46U, T46S

	dials a call, or is in a call. It works only if "phone_setting.contact_photo_display.enable" is set to 1 (Always) or 2 (Adaptive).			
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: <Image URL>;purpose=wallpaper Call-Info: <Image URL>;purpose=icon 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	T46S, T48S, T46U, T48U, T53C, T54W, T57W, T33P, T33G, Video Phone
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. The information	0-Disabled 1-Enabled	0	

	display method is configured by the parameter "phone_setting.call_info_display_method". To display the local identity during a call is not applicable to T48G/T46G/T42G/T41P/T31P/T31G/T31/T30P/T30/T29G/T23P/T23G/T21(P) E2/T19(P) E2 phones.			
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 in 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 in a call. It works only if "phone_setting.called_party_info_display.enable" is set to 1	0-Name+Number 1-Number+Name 2-Name 3-Number 4-Full Contact Info (display namesip:xxx@domain.com)	0	

	(Enabled).	Name refers to the Label, Display Name (Label > Display Name > User Name); Number refers to the User Name.		
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. 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	All phones except T48G, T46G, T42G, T41P and T29G
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	All phones except CP920, CP925, CP935W,

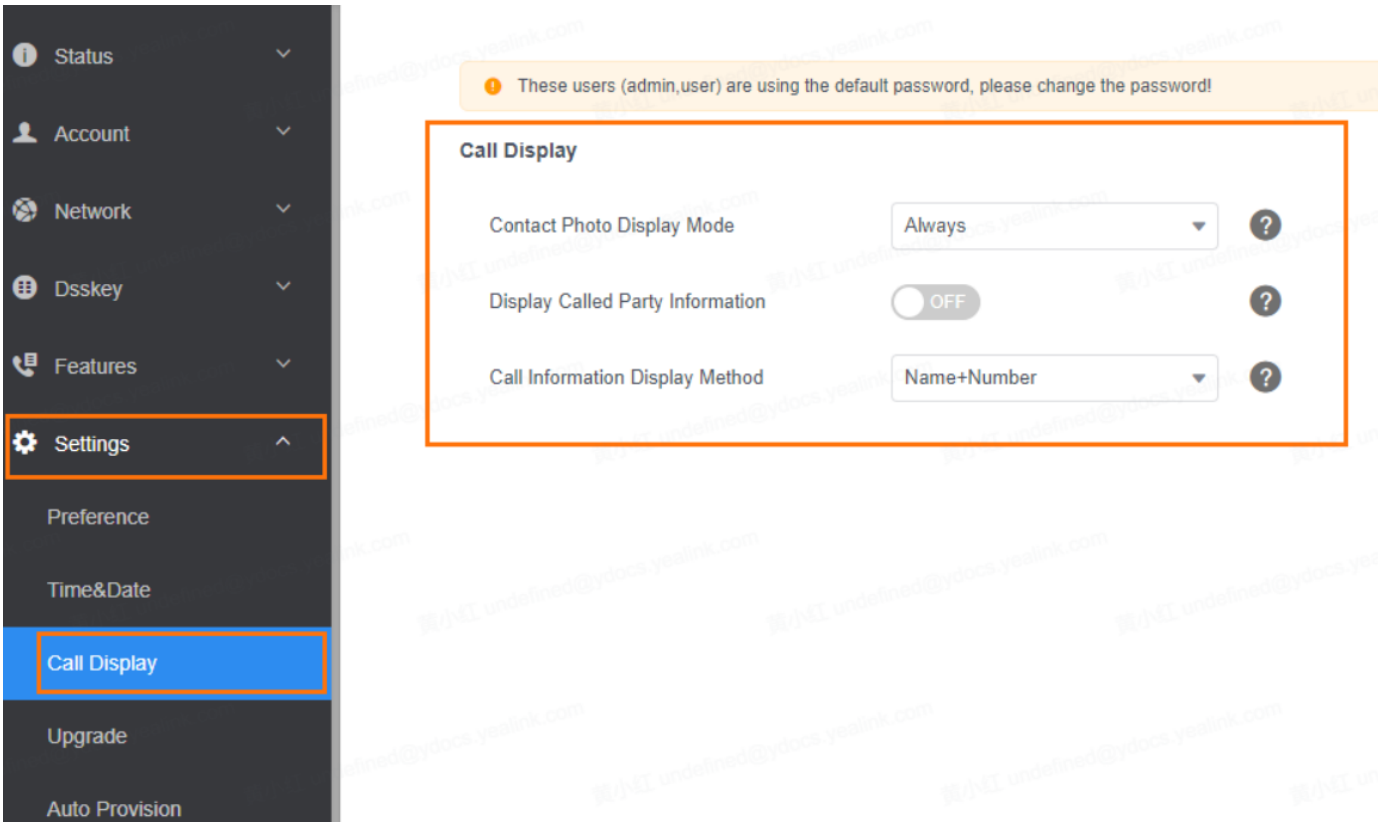
				CP960, CP965
account.X.update_ack_while_dialing[1]	It enables or disables the phone to update the display of call ID according to the ACK message.	0-Disabled 1-Enabled	0	
account.X.refresh_remote_id.enable[1]	It enables or disables the phone to update the identity of the caller according to the request 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	T3xW, T4xU, T5xW
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. It only works if your phone version is x.86.0.141 or later and "features.number_privacy.enable" is set to 1.	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	T3xW, T4xU, T5xW

[1]X is the account ID. For T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G/T56A/T58A/T58V/VP59/T7X/T8X, X=1-16; for T53W/T53/T53C/T43U/T42G/T42U/T42S, X=1-12; for T41P/T41S/T27G, X=1-6; for T33P/T33G, X=1-4; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21(P) E2,

> X=1-2; for T30P/T30/T19(P) E2/CP920/CP925/CP935W/CP960/CP965, X=1.

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

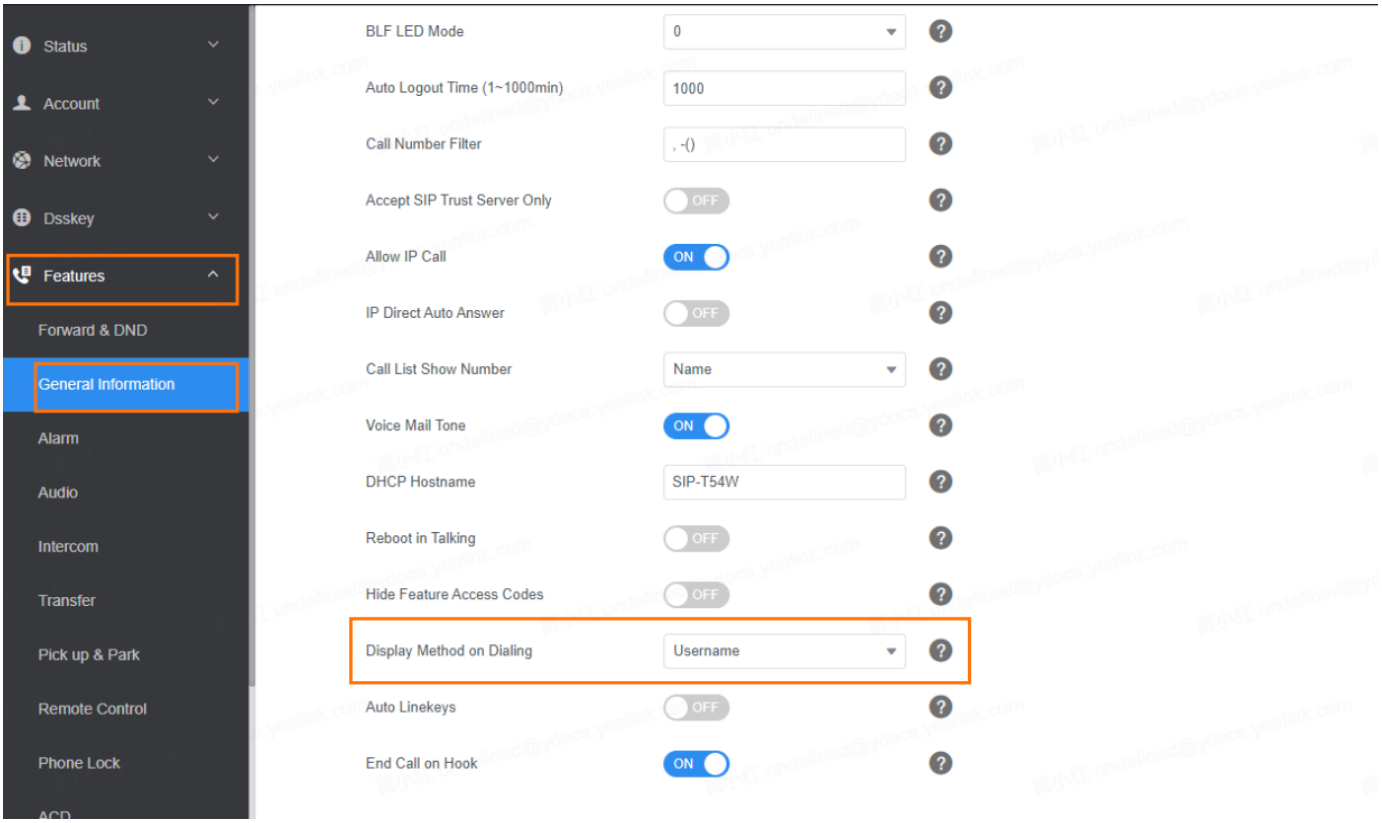
features.caller_name_type_on_dialing
features.password_dial.enable
features.password_dial.prefix
features.password_dial.length

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. It works only if	1-Label, configured by the parameter "account.X.label". 2-Display Name,	3

	"features.station_name.value" is left blank.	configured by the parameter "account.X.display_name". 3-User Name, configured by the parameter "account.X.user_name".	
features.password_dial.enable	It enables or disables the phone to partly display the callee's 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 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. 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 following shows search results displayed on T46S/G phones:

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 super 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 T29 T41 T42 T42S T41S T46 T46S T54S T52 T48 T48S T49 T61
T66 T69 T69S CP860 DECT CP920 T54W T53W T53 T57W"/>
<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 T48 T48S T49 T69 T69S T54W T53W T53 T57W"/
>
<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 T46S T54S T52 T48 T48S T42S T41S T27G CP920
T54W T53W T53 T57W"/>
<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). 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. 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-Disabled 1-Enabled.	Enable or disable the phone to search the desired directory list.
dev	T19 T21 T23 T40 T40G T27 T27G T29 T41 T42 T42S T41S T46 T46S T48 T48S CP920 T54W T53W T53 T53C T57W	The applicable phone models of the directory list. Do not edit this field.

	T48U T46U T43U T42U T29 T46 T46S T48 T48S T54W T53W T53 T53C T57W T48U T46U T43U T42U T29 T46 T46S T48 T48S T42S T41S T27G CP920 T54W T53W T53 T53C T57W T48U T46U T43U T42U T56A T58A T58V VP59 CP960 CP965	

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 on the provisioning server.

Search Source List Configuration

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

Configuration parameter

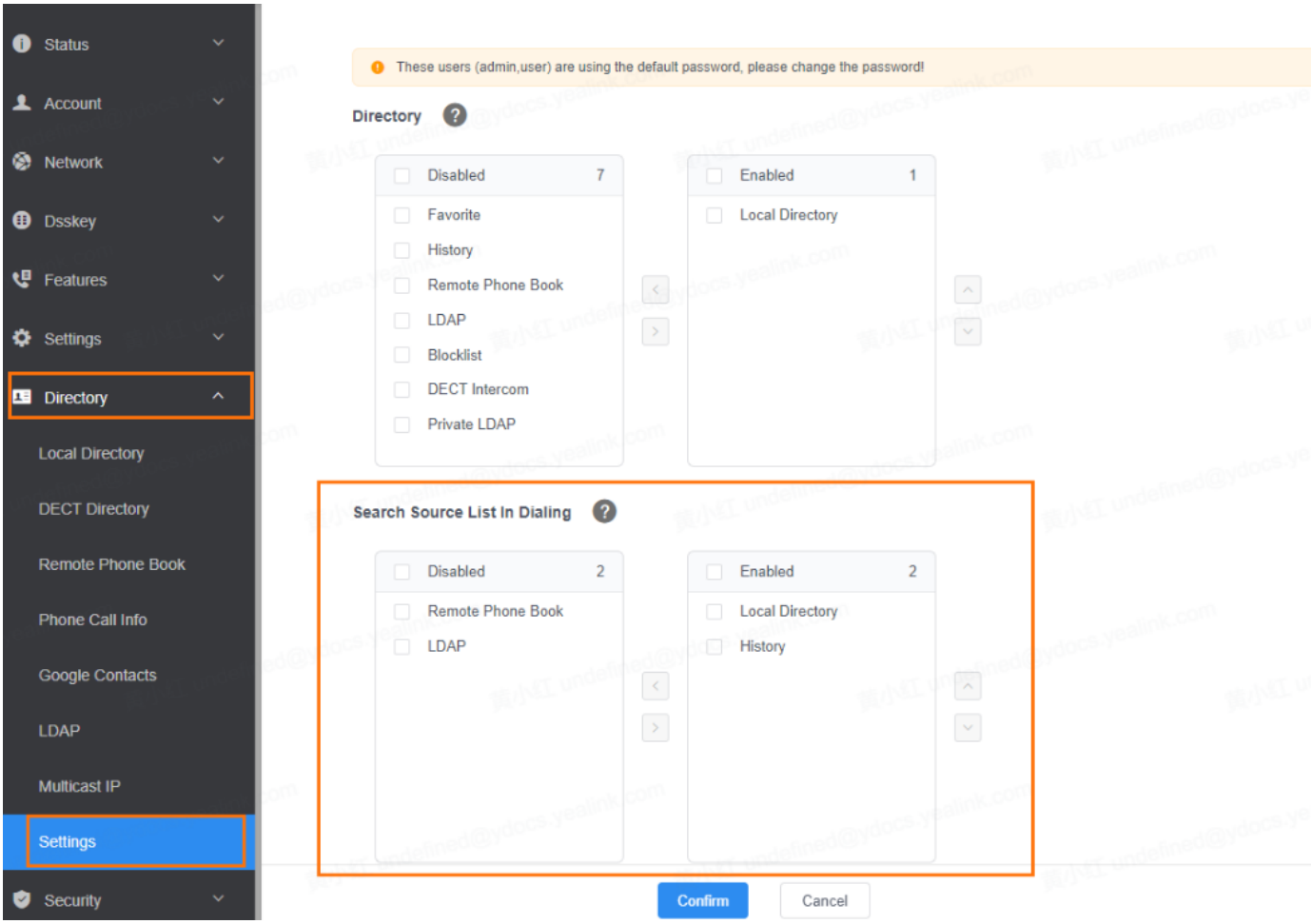
```
super_search.url
search_in_dialing.local_directory.enable
search_in_dialing.local_directory.priority
search_in_dialing.history.enable
search_in_dialing.history.priority
search_in_dialing.remote_phone_book.enable
search_in_dialing.remote_phone_book.priority
search_in_dialing.ldap.enable
search_in_dialing.ldap.priority
```

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

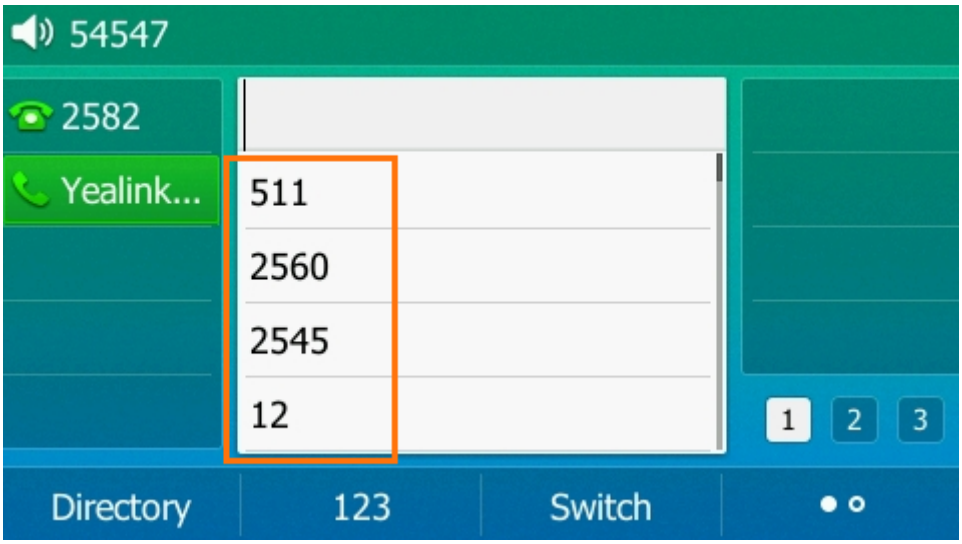
On the web user interface, go to: **Directory** > **Settings** > **Search Source List In Dialing.**



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.

The following shows the recent calls displayed on T46S/G phones:



Recent Call in Dialing Configuration

The following table lists the parameter you can use to configure the recent call display in dialing.

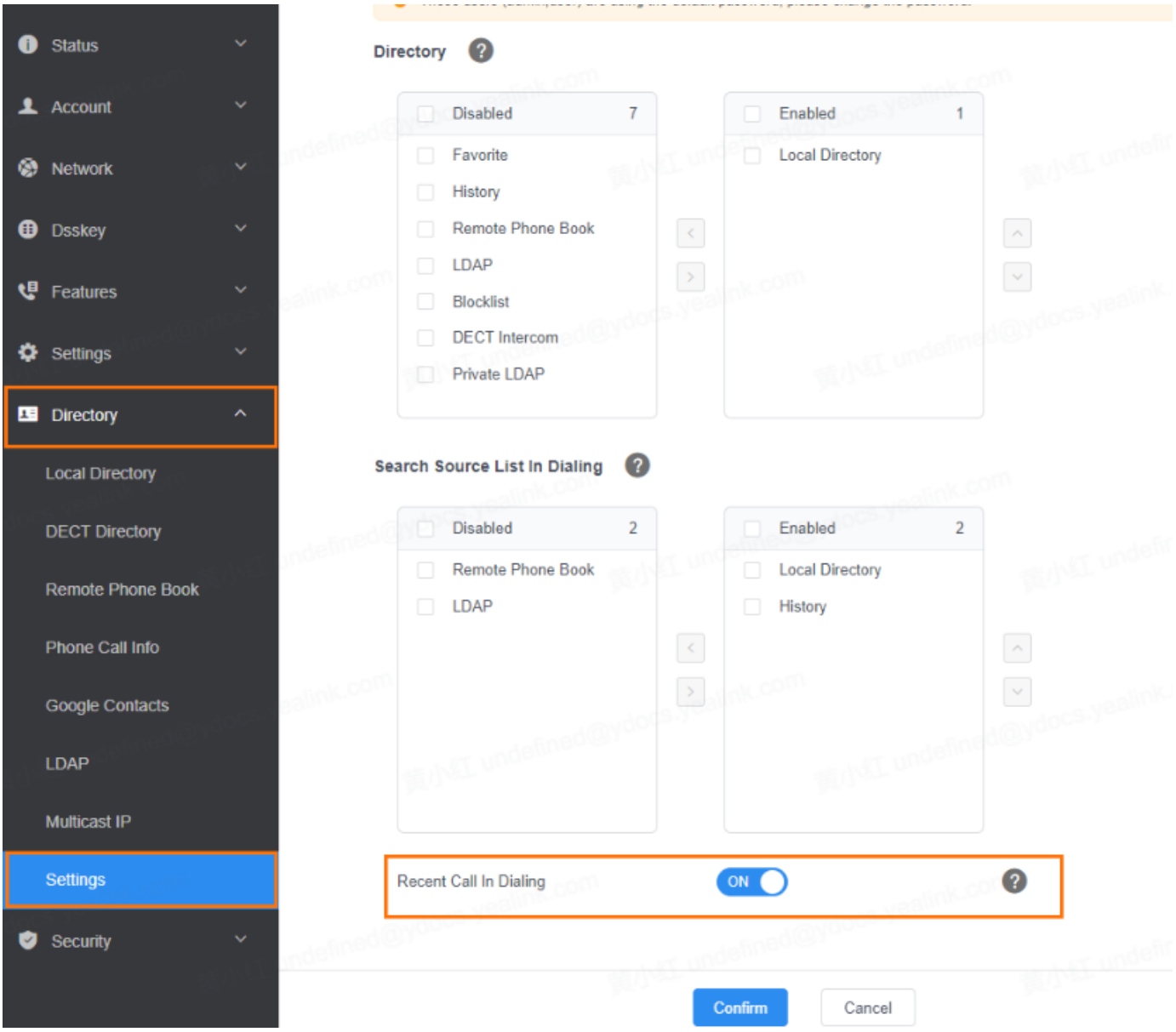
Configuration parameter

```
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.**

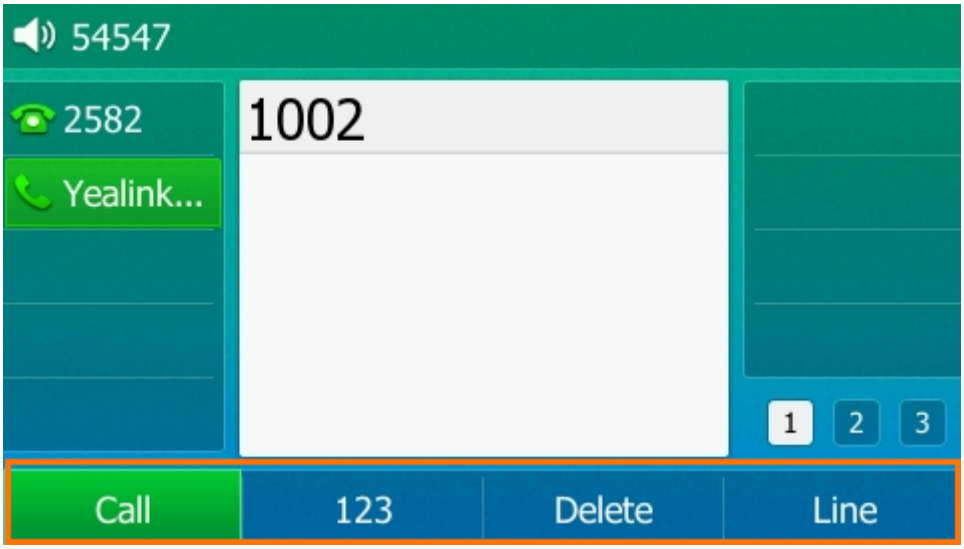


Softkey Layout

Introduction

Softkey layout is used to customize the soft keys at the bottom of the phone screen to best meet users' requirements. In addition to specifying which soft keys to display, you can determine their display order. The configurations for softkey layout are based on call states.

The following shows the soft keys displayed on the phone in the dialing state:



You can configure the EDK soft keys in different call states. Configuring the EDK soft keys may affect the softkey layout in different call states. For more information on EDK soft keys, refer to EDK Soft Keys Configuration.

Softkey Layout File Customization

You can also configure the softkey layout using the softkey layout templates for different call states.

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

```
<?xml version="1.0"?>
<CallIn>
<Disable>
<Key Type="Empty"/>
<Key Type="Switch"/>
<Key Type="Decline"/>
<Key Type="Extend" />
</Disable>
<Enable>
<Key Type="Answer"/>
<Key Type="Forward"/>
<Key Type="Silence"/>
<Key Type="Reject"/>
</Enable>
<Default>
<Key Type="Answer"/>
```

```
<Key Type="Forward"/>
<Key Type="Silence"/>
<Key Type="Reject"/>
</Default>
</CallIn>
```

Softkey Layout File Elements and Attributes

The following table lists the elements and attributes you need to understand in the softkey layout file. We recommend that you do not edit these elements and attributes.

Elements & Attributes	Description
<Disable> </Disable>	Specify the disabled soft key list. The phone screen will not display the disabled soft keys.
<Enable> </Enable>	Specify the enabled soft key list. The phone screen will display the enabled soft keys.
<Default> </Default>	Specify the default soft key list. The phone screen displays these soft keys by default.
<Key Type=" "/>	Specify the soft key type.

Customizing Softkey Layout File

1. Open the template file.
2. For each soft key that you want to enable, move the string from the disabled soft key list to the enabled soft key list in the file, or replace the Empty in the enabled soft key list.

The following shows a portion of the softkey layout file “CallFailed.xml”:

```
CallFailed.xml*
1  <?xml version="1.0"?>
2  <CallFailed>
3    <Disable>
4      <Key Type="Empty" />
5      <Key Type="End Call" />
6    </Disable>
7    <Enable>
8      <Key Type="NewCall" />
9      <Key Type="Empty" />
10     <Key Type="Empty" />
11     <Key Type="Cancel" />
12
13   </Enable>
14   <Default>
15     <Key Type="NewCall" />
16     <Key Type="Empty" />
17     <Key Type="Empty" />
18     <Key Type="Cancel" />
```

If you want to enable the **End Call** soft key in CallFailed state, just move this string.

3. For each soft key that you want to disable, just move the string from the enabled soft key list to the disabled soft key list.

The following shows a portion of the softkey layout file “CallFailed.xml”:

CallFailed.xml*

```
1  <?xml version="1.0"?>
2  <CallFailed>
3    <Disable>
4      <Key Type="Empty" />
5      <Key Type="End Call" />
6
7    </Disable>
8    <Enable>
9      <Key Type="NewCall" />
10     <Key Type="Empty" />
11     <Key Type="Empty" />
12     <Key Type="Cancel" />
13       </Enable>
14   <Default>
15     <Key Type="NewCall" />
16     <Key Type="Empty" />
17     <Key Type="Empty" />
18     <Key Type="Cancel" />
```

If you want to disable the **NewCall** soft key in CallFailed state, just move this string.

4. Save the change and place this file on the provisioning server.

Softkey Layout Configuration

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

Configuration parameter

phone_setting.custom_softkey_enable
phone_setting.custom_softkey.apply_to_states
features.custom_softkey_dynamic.enable
custom_softkey_call_failed.url
custom_softkey_call_in.url
custom_softkey_connecting.url
custom_softkey_dialing.url
custom_softkey_ring_back.url
custom_softkey_talking.url

Parameter	Description	Permitted Values	Default

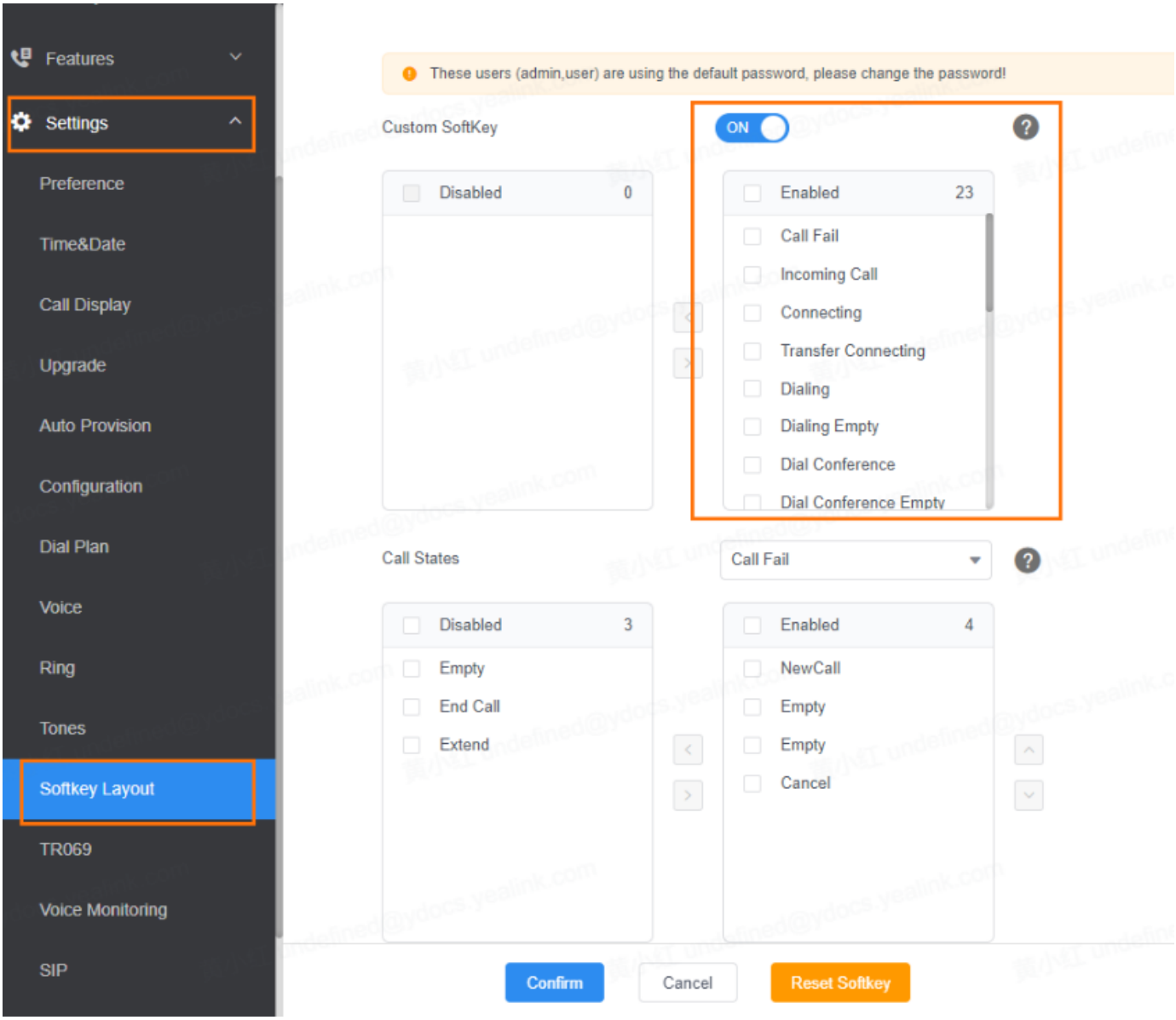
phone_setting.custom_softkey_enable	It enables or disables the custom soft keys layout feature.	0-Disabled 1-Enabled	0
phone_setting.custom_softkey.apply_to_states[1]	It configures the desired call state to apply the custom softkey layout. To configure the call states to apply the custom softkey layout: Example: phone_setting.custom_softkey.apply_to_states = DialingEmpty,DialTransEmpty It means that DialingEmpty and DialTransEmpty call states will use the custom softkey layout. To configure the call states not to apply the custom softkey layout: Example: phone_setting.custom_softkey.apply_to_states = -DialingEmpty,DialTransEmpty It means that DialingEmpty and DialTransEmpty call states will not use the custom softkey layout. Multiple call states are separated by commas.	Blank (all call states will use the custom softkey layout) Dialing, DialingEmpty, DialTrans, DialTransEmpty, DialConference, DialConferenceEmpty, Talk, Hold, Held, CallIn, NewCallIn, BeTransferred, SemiAttendTrans, Conferenced, ConferencedHold, ConferencedNewCallIn, Connecting, CallFailed, Paging, ListeningPaging, RingBack, SemiAttendTransBack	Blank
features.custom_softkey_dynamic.enable[1]	It enables or disables the phone to display the soft keys relevant to the features (call center, centralized call recording, and executive-assistant).	0-Disabled 1-Enabled, the functional soft keys display on the phone screen if the corresponding feature is available.	1
custom_softkey_call_failed.url[1]	It configures the access URL of the custom softkey layout file in	URL within 511 characters	Blank

	the CallFailed state.		
custom_softkey_call_in.url[1]	It configures the access URL of the custom softkey layout file in the CallIn state.	URL within 511 characters	Blank
custom_softkey_connecting.url[1]	It configures the access URL of the custom softkey layout file in the Connecting state.	URL within 511 characters	Blank
custom_softkey_dialing.url[1]	It configures the access URL of the custom softkey layout file in the Dialing state.	URL within 511 characters	Blank
custom_softkey_ring_back.url[1]	It configures the access URL of the custom softkey layout file in the RingBack state.	URL within 511 characters	Blank
custom_softkey_talking.url[1]	It configures the access URL of the custom softkey layout file in the Talking state.	URL within 511 characters	Blank

> [1] NOTE: It works only if "phone_setting.custom_softkey_enable" is set to 1 (Enabled).

Set via the Web User Interface

On the web user interface, go to: **Settings** > **Softkey Layout** > **Custom SoftKey**



Example: Setting the Soft Keys Layout in Talking State

The following example shows the configuration for setting the soft key layout in the talking state.

Customize a softkey layout file "Talking.xml" and place this file to the provisioning server "http://192.168.10.25".

```
phone_setting.custom_softkey_enable = 1
custom_softkey_talking.url = http://192.168.10.25/Talking.xml
```

After provisioning, you can use the enabled soft keys during a call.

Screen Saver

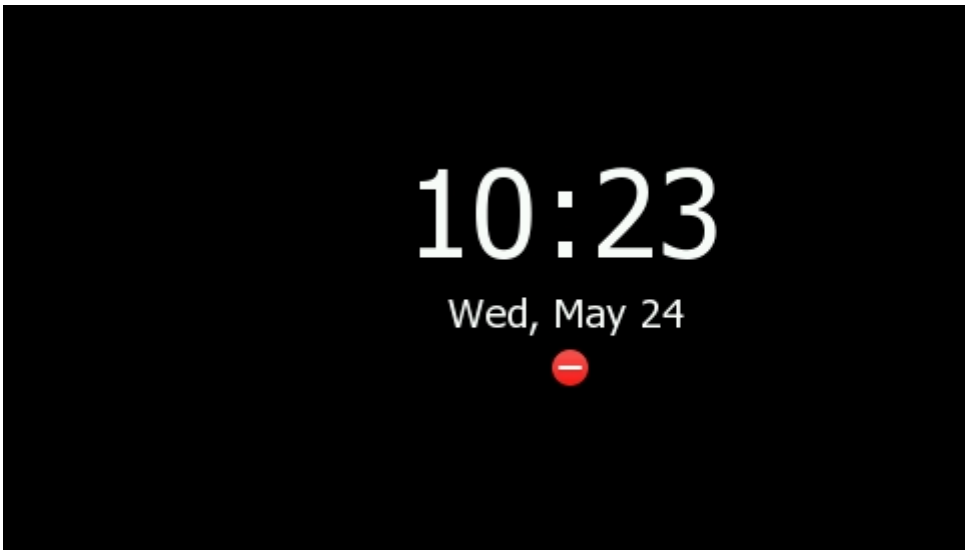
Introduction

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.

The following shows that the built-in screen saver is displayed on T54W phones:



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.

The black-and-white screen IP phone only displays custom information as the screen saver.

Screensaver Display Customization

You can customize the screen saver file to configure the IP phone to display custom information (for example, notifications or company logo) on the screen saver.

For color screen phones, the custom information is displayed on the built-in picture or custom pictures (if uploaded).

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	Specify "show " or "hide" between <SystemTime> and </

	horizontalAlign verticalAlign Color	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.
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. VerticalAlign works only if you do not configure InsertImageLineNum or set the InsertImageLineNum to 0.

> [1] NOTE: It is only applicable to color screen phones.

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 on 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
EXP50/EXP43	.jpg/.png/.bmp/.jpeg	<=4.2 megapixels	<=5MB	2MB of space should be reserved for the phone
T57W/T54W/T53C/T48U/T48S/T48G/CP925/CP935W /Video Phone/Conference Phone/T73U/T73W/T74U/T74W/T77U/T85W/T87W/T88W/T88W Pro/T88V Pro	.jpg/.png/.bmp/.jpeg	<=2.0 megapixels	<=5MB	
T46U/T46S/T46G/T33P/ T33G/T29G	.jpg/.png/.bmp/.jpeg	<=1.8 megapixels	<=5MB	

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.xml_browser.url
screensaver.clock_move_interval
screensaver.picture_change_interval
features.blf_active_backlight.enable
screensaver.mode
```

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.	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 Note: The permitted values for web/phone UI are Off, 30min, 1h, 2h, 4h, 6h (default), 8h, 12h. For CP925/CP935W: 15-15s 30-30s 60-1min 120-2min 300-5min 600-10min 900-15min 1200-20min 1800-30min 2700-45min 3600-1h 7200-2h	21600 (7200 for CP925/CP935W)

		The permitted values for web/phone UI are 5min, 10min, 30min, 1h, 2h (default).	
screensaver.display_clock.enable	It enables or disables the phone to display the clock and icons when the screen saver starts. 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.	**For T88W/T88W Pro/T88V Pro/T58W/T58A/VP59/CP965/CP960:** 0-Clock 1-Colours 2-Photo Frame 3-Photo Table **For other phones:** 0-System, the LCD screen will display the built-in picture. 1-Custom, the	0

		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”. 2-Server XML, the LCD screen will display XML items (configured by the parameter “screensaver.xml_browser.url”) when the screen saver starts.	
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	URL within 511 characters	Blank

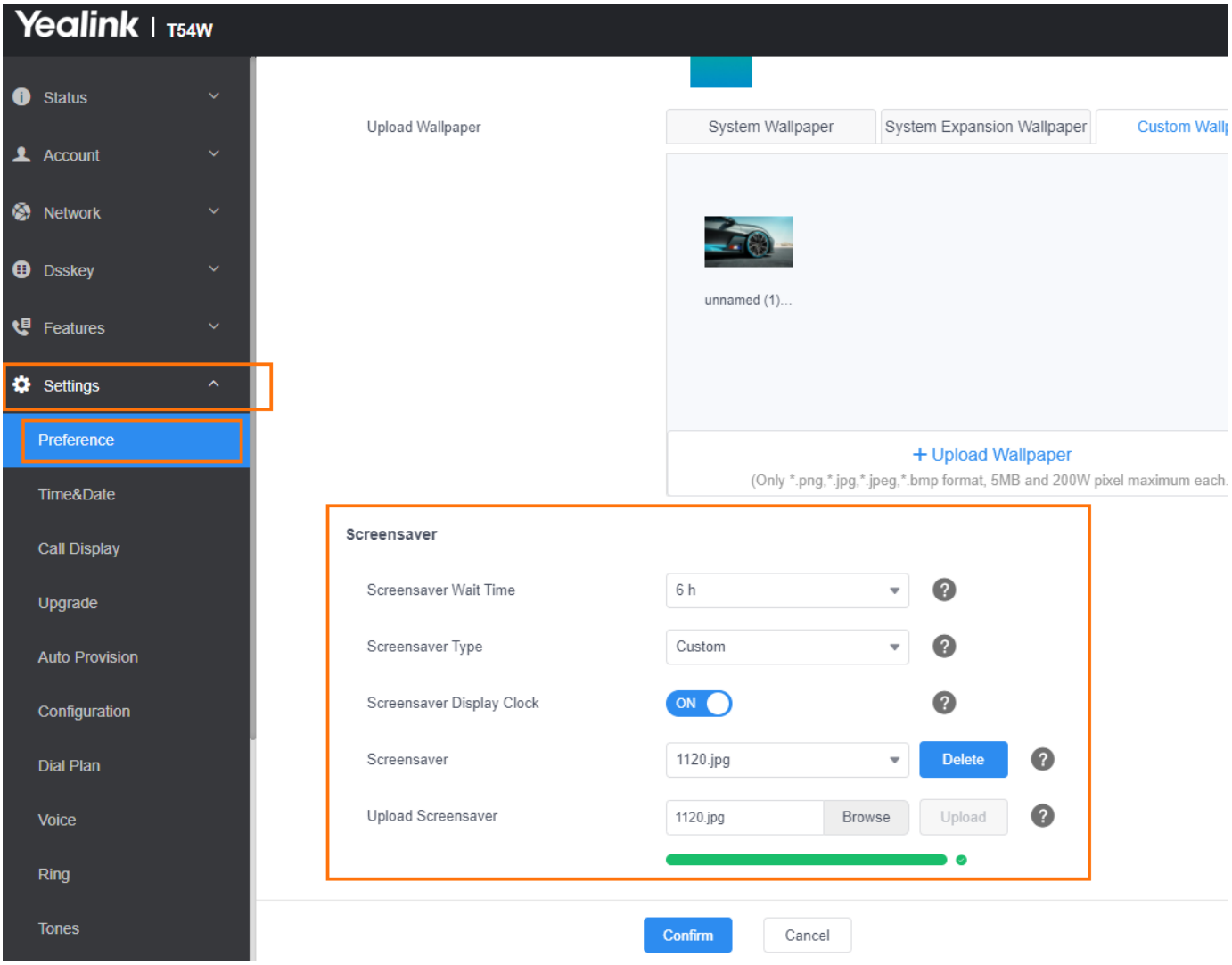
	phone connects to the HTTP provisioning server “192.168.10.25”, and downloads the screen saver image “Screencapture.jpg”. If you want to upload multiple screen saver images to the phone simultaneously, you can configure it as follows: screensaver.upload_url = http://192.168.10.25/Screencapture.jpg screensaver.upload_url = http://192.168.10.25/Screensaver.jpg		
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.xml_browser.url	It configures the access URL of the screen saver XML file. Example: screensaver.xml_browser.url = http://192.168.10.25/ScreenSaver.xml During the auto provisioning, the phone connects to the	URL within 511 characters	Blank

	HTTP provisioning server “192.168.10.25”, and downloads the screen saver XML file “ScreenSaver.xml”. For color screen phones, it works only if "screensaver.type" is set to 2 (Server XML).		
screensaver.clock_move_interval	It configures the interval (in seconds) for the phone to move the clock and icons when the screen saver starts. 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. 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
features.blf_active_backlight.enable	It enables or disables the phone to turn on the backlight or stop the screen saver when the BLF/BLF list status changes.	0-Disabled 1-Enabled	1
screensaver.	It configures the use of the	**For T88W/T88W**	

mode	built-in screensaver or a custom screensaver.	**Pro/T88V Pro/ T58W/T58A/ VP59/CP965/ CP960：** 0-4 0-Clock；1-Colours；2-Photo Frame；3-Photo Table; 4-Server XML **For other phone：** 0-2 0-System; 1-Custom; 2-Server XML	• **For T88W/T88W Pro/ T88V Pro/T58W/ T58A/VP59/CP965/ CP960：** 1 • **For other phone：** 0

Set via the Web User Interface

On the web user interface, go to: **Settings** > **Preference** > **Screensaver Display Clock (not configurable when the Screensaver Type is set to Server XML)**



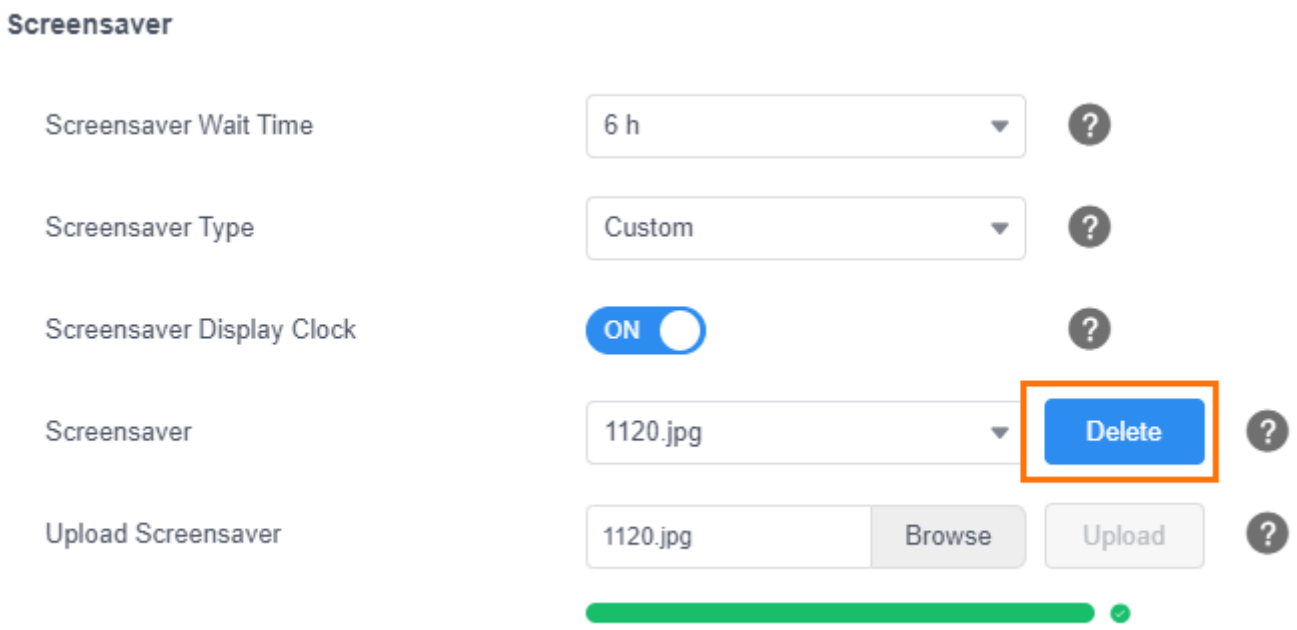
Adding a Screensaver Picture from a USB Flash Drive

The T57W/T54W/T53C/T48U/T48S/T48G/T46U/T46S/T46G/T29G IP phone, Video phone and Conference phone enables you to add a screensaver picture from a USB flash drive on their phones. You can go to **Menu** > **USB** > **Browse Photo**, preview pictures, and then set the desired picture as a screensaver. After you set a picture on USB flash drive as a screensaver, the picture is added to the Screensaver list.

> Yealink phones support USB flash drives in FAT32 or NTFS format.

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.



Wallpaper Settings

Introduction

Wallpaper is a picture used as the background of a phone. The phone comes with a default picture. You can change it to a built-in picture or custom wallpaper from personal pictures.

The wallpaper is only applicable to color screen phones and expansion module EXP50 (connected to the T57W/T54W/T53W/T53/T53C phones)/expansion module EXP43 (connected to the T48U/T46U/T43U phones).

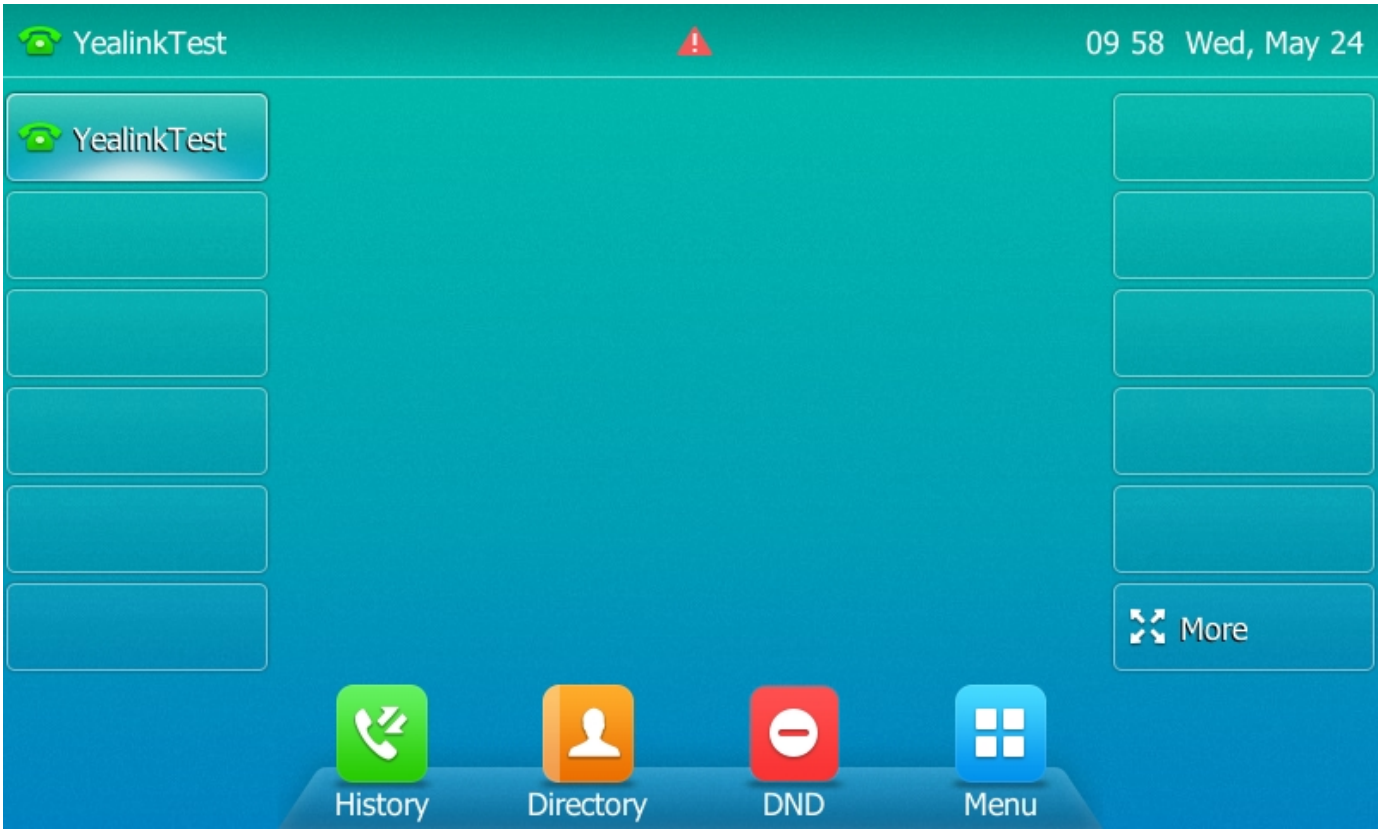
Wallpaper Configuration

You can change the wallpaper to any built-in picture or custom picture.

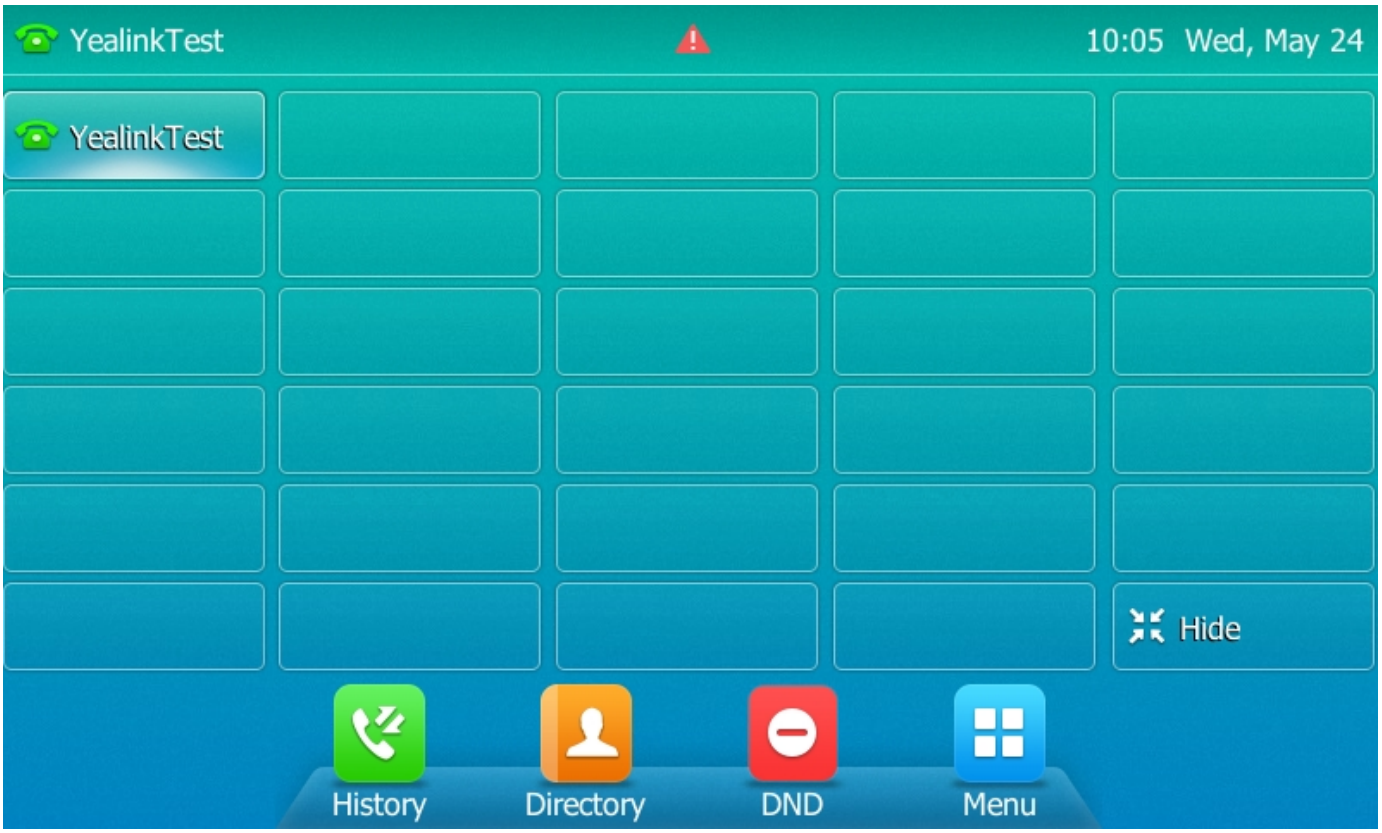
On T57W/T48U/T48S/T48G phones or video phones, you can also separately set the wallpaper when the DSS key list is unfolded, avoiding the display of the line key labels being blocked by the background picture.

The following shows a wallpaper set on T57W phones:

line key list is folded:



line key list is unfolded:



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

Configuration parameter

phone_setting.backgrounds

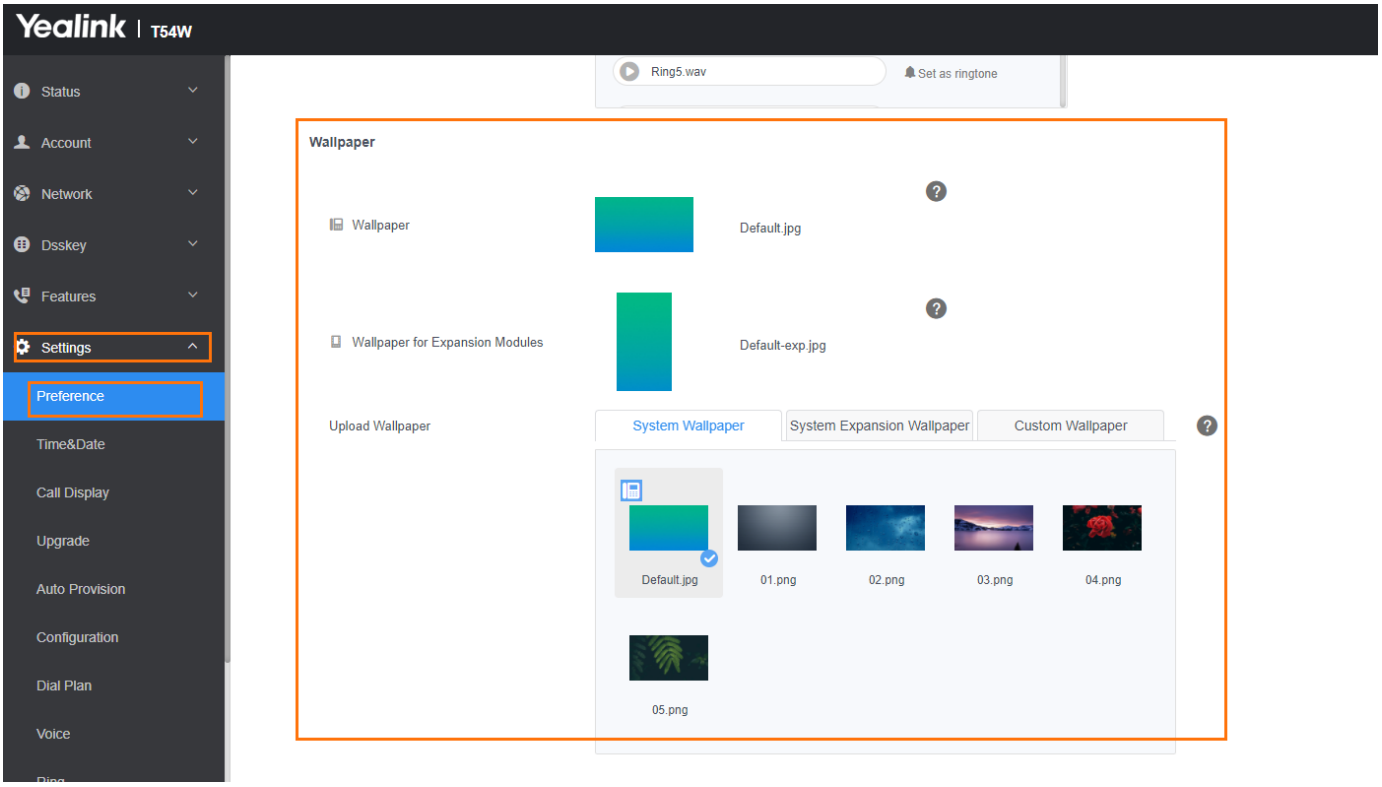
expansion_module.backgrounds
phone_setting.backgrounds_with_dsskey_unfold

Parameter	Description	Permitted Values	Default	Supported Devices
phone_setting.backgrounds	It configures the wallpaper displayed on the phone's idle screen.	T57W/T54W/T53C/T48U: Default.jpg, 01.png, 02.png, 03.png, 04.png, 05.png or uploaded custom wallpaper name (for example, wallpaper.jpg) T46U: Default.png, 01.png, 02.png, 03.png, 04.png, 05.png or uploaded custom wallpaper name (for example, wallpaper.png) T33P/T33G: Default.jpg, 1.jpg, 2.jpg, 3.jpg, 4.jpg, 5.jpg or uploaded custom wallpaper name (for example, wallpaper.jpg) CP925/CP935W: Default.jpg, 1.png, 2.png, 3.png, 4.png or uploaded custom wallpaper name (for example, wallpaper.png) Other Phones: Default.jpg, 01.jpg, 02.jpg, 03.jpg, 04.jpg, 05.jpg, 06.jpg, 07.jpg, 08.jpg, 09.jpg or 10.jpg or uploaded custom	Default.jpg (Default.png for T46U)	All color screen phones

		wallpaper name (for example, wallpaper.jpg)		
expansion_module.backgrounds	It configures the wallpaper displayed on the connected EXP50 expansion module of the phone.	T57W/T54W/T53W/T53/T53C: Default-exp50.jpg, 01-exp50.jpg, 02-exp50.jpg, 03-exp50.jpg, 04-exp50.jpg, 05-exp50.jpg, 06-exp50.jpg, 07-exp50.jpg, 08-exp50.jpg, 09-exp50.jpg or 10-exp50.jpg or custom wallpaper name (for example, wallpaper.jpg) T48U/T46U/T43U: Default-exp.jpg, 01-exp.jpg, 02-exp.jpg, 03-exp.jpg, 04-exp.jpg, 05-exp.jpg or custom wallpaper name (for example, wallpaper.jpg)	T57W/T54W/T53W/T53/T53C: Default-exp50.jpg T48U/T46U/T43U: Default-exp.jpg	All color screen phones
phone_setting.backgrounds_with_dsskey_unfold	It configures the wallpaper displayed on the phone when the DSS key list is unfolded.	T57W/T48S/T48G: Auto, Default.jpg, 01.jpg, 02.jpg, 03.jpg, 04.jpg, 05.jpg, 06.jpg, 07.jpg, 08.jpg, 09.jpg or 10.jpg or uploaded custom wallpaper name (for example, wallpaper.jpg) T48U: Auto, Default.jpg, 01.jpg, 02.jpg, 03.jpg, 04.jpg, 05.jpg or uploaded custom wallpaper name (for example, wallpaper.jpg)	Auto (use the wallpaper configured by the parameter "phone_setting.backgrounds")	T57W, T48U, T48S, T48G, Video phone

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 a company logo, and then upload the custom picture to the IP phone that users can choose from when changing the wallpaper for the phone's idle screen, expansion module, or DSS key 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
EXP50/EXP43	.jpg/.png/.bmp/.jpeg	<=4.2 megapixels	<=5MB	2MB of space should be reserved for the phone
T57W/T54W/T53C/T48U/T48S/T48G/CP925/CP935W/Video Phone/Conference Phone/T7X/T8X		<=2.0 megapixel	<=5MB	

		s		
T46U/T46S/T46G/T33P/ T33G/T29G		<=1.8 mega pixels	<=5MB	

Custom Wallpaper Configuration

The following table lists the parameter you can use to upload a custom picture.

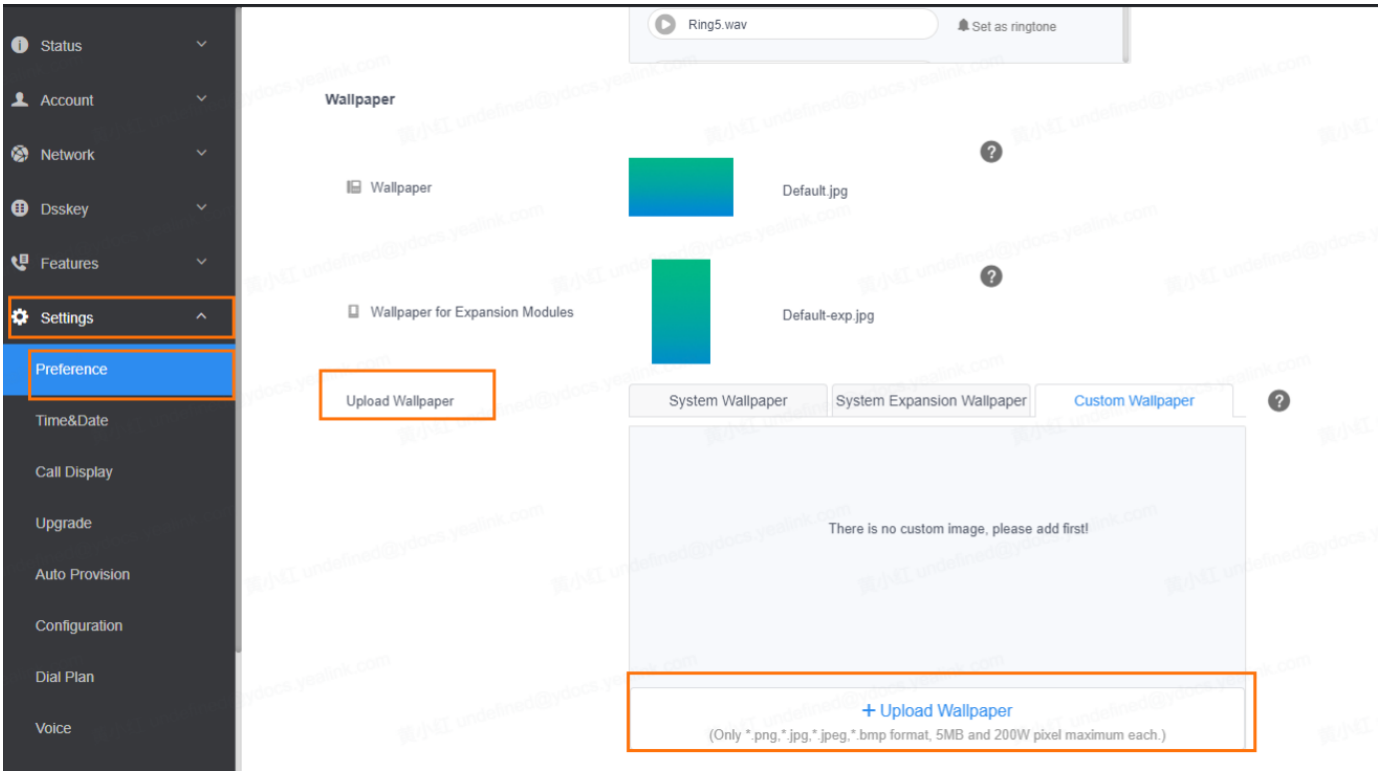
Configuration parameter

```
wallpaper_upload.url
```

Parameter	Description	Permitted Values	Default	Supported Devices
wallpaper_upload.url	It configures the access URL of the custom wallpaper picture.	URL within 511 characters	Blank	T57W, T54W, T53W, T53, T53C, T48U, T48S, T48G, T46U, T46S, T46G, T43U, T33P, T33G, T29G, CP925, CP935W, Video Phone, Conference Phone, T7X, T8X

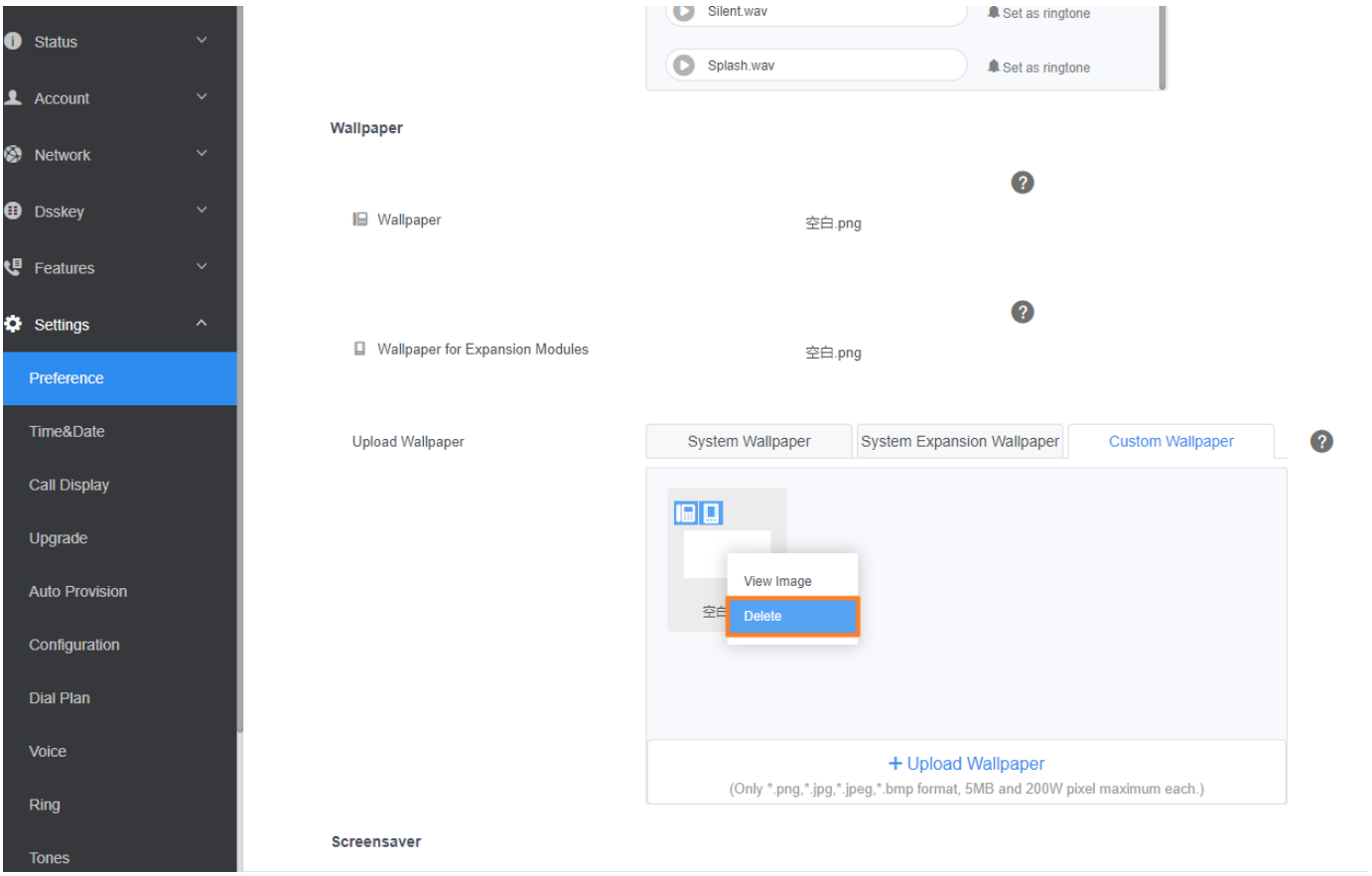
Set via the Web User Interface

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).



Adding a Wallpaper from a USB Flash Drive

The T57W/T54W/T53C/T48U/T48S/T48G/T46U/T46S/T46G/T29G IP phone and Video phone enable you to add wallpaper from a USB flash drive to their phones. You can go to Menu > USB > Browse Photo, preview pictures, and then set the desired picture as the idle screen/Dsskey screen or EXP wallpaper. After you set a picture on a USB flash drive as the idle screen/Dsskey screen or EXP wallpaper, the picture is added to the Wallpaper list.

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 the 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's idle screen wallpaper changes to the custom picture “wallpaper.jpg”.

Example

```
wallpaper_upload.url = http://192.168.10.25/wallpaper.jpg
phone_setting.backgrounds = wallpaper.jpg
```

After provisioning, the phone's idle screen wallpaper changes to the custom picture “wallpaper.jpg”.

Customization of Com Version and MAC Version

Introduction

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.

This feature is only supported in versions x.86.0.50 and later.

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

Introduction

You can customize the existing keypad input method for all phones except CP925/CP935W and the existing onscreen keyboard input method for T57W/T48U/T48S/T48G CP925/CP935W/T56A/T58A/T58V/VP59/CP960/CP965 phones.

The T57W/T48U/T48S/T48G/CP925/CP935W/T56A/T58A/T58V/VP59/CP960/CP965 phones use the onscreen keyboard by default. After you disable it, you can use the phone keypad to enter data except CP925/CP935W.

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 become 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). It is not applicable to CP925/CP935W phones.

Yealink phones support 6 input methods: 2aB, abc, Abc, 123, ABC, and Hebrew.

> 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 become effective when the language is set to Hebrew.

You can ask the distributor or Yealink FAE for the 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 = "pqrs7ß⌧"
8 = "tuv8ùúûü"
9 = "wxyz9ýÞ"
0 = " "
* = "*.,'?!\-()@/:_;+&%=<> £ $¥¤[]{}~^¡¿ § #"|"
# = "#"
```

```
[Abc]
1 = ""
2 = "abc2äæåàáâãç"
3 = "def3èéêëð"
4 = "ghi4ìíîï"
5 = "jkl5£"
6 = "mno6öøòóôõñ"
7 = "pqrs7ß⌧"
8 = "tuv8ùúûü"
9 = "wxyz9ýÞ"
0 = " "
* = "*.,'?!\-()@/:_;+&%=<> £ $¥¤[]{}~^¡¿ § #"|"
# = "#"
```

```
[ABC]
```

```
1 = ""
2 = "ABC2ÄÆÅÀÁÂÃÇ"
3 = "DEF3ÈÉÊËÐ"
4 = "GHI4ÌÍÎÏ"
5 = "JKL5£"
6 = "MNO6ÖØÒÓÔÕÑ"
7 = "PQRS7⊠"
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 = "pqrs7ß⊠"
8 = "tuv8ùúûü"
9 = "wxyz9ýÞ"
0 = " "
```

```
* = "*.,'?!\-()@/:_;+&%=<> £ $¥¤[]{}~^¡¿ § #"|"
# = "#"
```

```
[ABC_PWD]
1 = ""
2 = "ABC2ÄÆÅÀÁÂÃÇ"
3 = "DEF3ÈÉÊËÐ"
4 = "GHI4ÌÍÎÏ"
5 = "JKL5£"
6 = "MNO6ÖØÒÓÔÕÑ"
7 = "PQRS7⊠"
8 = "TUV8ÙÚÛÜ"
9 = "WXYZ9ÝÞ"
0 = " "
* = "*.,'?!\-()@/:_;+&%=<> £ $¥¤[]{}~^¡¿ § #"|"
# = "#"
```

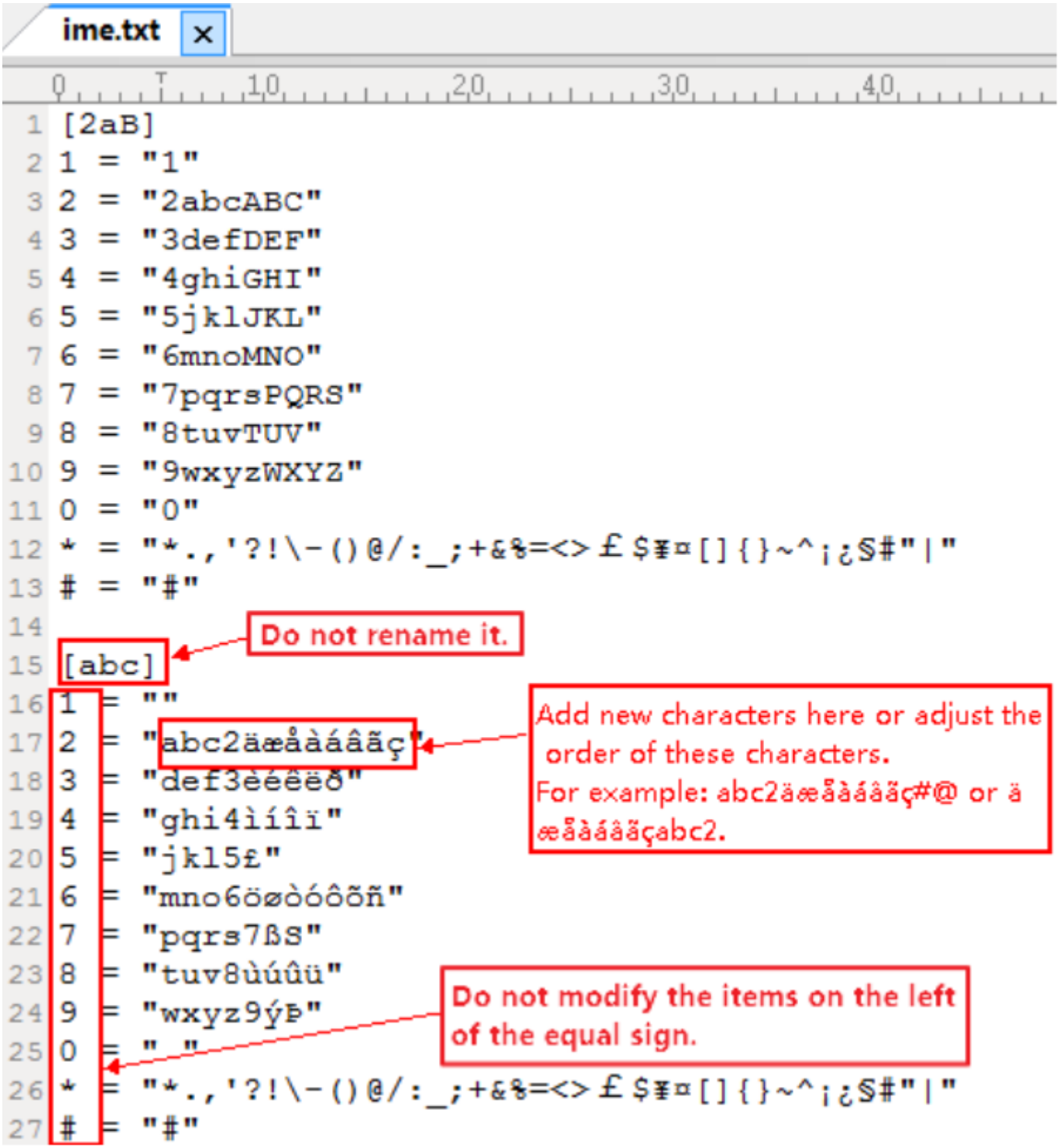
```
[123_PWD]
1 = "1"
2 = "2"
3 = "3"
4 = "4"
5 = "5"
6 = "6"
7 = "7"
8 = "8"
9 = "9"
0 = "0"
* = ".*:/@[]"
# = "#"
```

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.

> 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

Onscreen Keyboard Input Method File Customization

The T57W/T48U/T48S/T48G/T56A/T58A/T58V/VP59/CP960/CP965 phones support using the onscreen keyboard to enter data and provide English onscreen keyboard by default. You can create a new language onscreen keyboard or customize the existing input method files of the onscreen keyboard.

Yealink provides three types of input method files for onscreen keyboard customization. You can configure them as required.

You can ask the distributor or Yealink FAE for onscreen keyboard input method files. You can also refer to the following template:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<KeyboardIme Layout="keyboard_layout_francais.xml" DisplayName="abc"
CapitalName="ABC" ImeType="Char">

<Line>
<Key ImeNormal="aàâæáäãåāª" ImeCapital="AÀÂÆÁÄÃÅĀª"></Key>
<Key ImeNormal="z" ImeCapital="Z"></Key>
<Key ImeNormal="eéèêë⊠⊠ē" ImeCapital="EÉÈÊË⊠⊠Ē"></Key>
<Key ImeNormal="r" ImeCapital="R"></Key>
<Key ImeNormal="t" ImeCapital="T"></Key>
<Key ImeNormal="yÿ" ImeCapital="Y⊠"></Key>
<Key ImeNormal="uūúüùû" ImeCapital="UŪÚÜÙÛ"></Key>
<Key ImeNormal="iī⊠îïíī" ImeCapital="IĪ⊠ÎÏÍĪ"></Key>
<Key ImeNormal="oºōøõóòöœô" ImeCapital="OºŌØÕÓÒÖŒÔ"></Key>
<Key ImeNormal="p" ImeCapital="P"></Key>

<Key Function="backspace"></Key>
</Line>

<Line>
<Key ImeNormal="q" ImeCapital="Q"></Key>
<Key ImeNormal="s" ImeCapital="S"></Key>
```

```
<Key ImeNormal="d" ImeCapital="D"></Key>
<Key ImeNormal="f" ImeCapital="F"></Key>
<Key ImeNormal="g" ImeCapital="G"></Key>
<Key ImeNormal="h" ImeCapital="H"></Key>
<Key ImeNormal="j" ImeCapital="J"></Key>
<Key ImeNormal="k" ImeCapital="K"></Key>
<Key ImeNormal="l" ImeCapital="L"></Key>
<Key ImeNormal="m" ImeCapital="M"></Key>

<Key Function="enter"></Key>
</Line>

<Line>
<Key Function="shift"></Key>

<Key ImeNormal="w" ImeCapital="W"></Key>
<Key ImeNormal="x" ImeCapital="X"></Key>
<Key ImeNormal="cç⊠⊠" ImeCapital="CÇ⊠⊠"></Key>
<Key ImeNormal="v" ImeCapital="V"></Key>
<Key ImeNormal="b" ImeCapital="B"></Key>
<Key ImeNormal="nńñ" ImeCapital="NŃÑ"></Key>
<Key ImeNormal="," ImeCapital="?"></Key>
<Key ImeNormal=";" ImeCapital="."></Key>
<Key ImeNormal=":" ImeCapital="/"></Key>
<Key ImeNormal="!" ImeCapital=" § "></Key>

<Key Function="shift"></Key>

</Line>

<Line>
<Key Function="switch"></Key>
<Key Function="lang"></Key>
```

```
<Key Function="space"></Key>

<Key Function="left"></Key>
<Key Function="right"></Key>

<Key Function="hide"></Key>
</Line>

</KeyboardIme>
```

Description of the Onscreen Keyboard Input Method Files

Before you customize the onscreen keyboard input method files, take a few moments to familiarize yourself with their formats and descriptions.

File Type	File Name (* represents any character)	Template File	Description
Lang	keyboard_lang.xml	keyboard_lang.xml	Configures the language of the keyboard.
Ime	keyboard_ime_*.xml	keyboard_ime_en.xml	Configures the alternative characters for the English keyboard in alphabetic input mode.
Ime	keyboard_ime_*.xml	keyboard_ime_francais.xml	Configures the alternative characters for the French keyboard in alphabetic input mode.
Ime	keyboard_ime_*.xml	keyboard_ime_num.xml	Configures the alternative characters for keyboard in numeric&symbolic input modes
Layout	keyboard_layout_*.xml	keyboard_layout_1.xml	Configures the layout of the English keyboard in alphabetic input mode.
Layout	keyboard_layout_*.xml	keyboard_layout_2.xml	Configures the layout of English or French keyboard in numeric&symbolic input mode.
Layout	keyboard_layout_*.xml	keyboard_layout_francais.xml	Configures the layout of the French keyboard in alphabetic input mode.

If you want to customize the existing input method files of the onscreen keyboard, you just

need to upload the custom files. If you want to create a new language onscreen keyboard, you should upload all three types of input method files at a time. For the example above, you should upload “keyboard_lang.xml", "keyboard_ime_francais.xml", and "keyboard_layout_francais.xml" files at a time.

Lang File Elements and Attributes

The following table lists the elements and attributes you need to understand in the Lang file. We recommend that you do not edit these elements and attributes.

Elements	Attributes	Description
Lang	Name	Specify the display name of the language.
Ime	Name	Specify the IME file(s) that the language will use. One IME file can be used by multiple languages. For example, the keyboard in numeric&symbolic input mode is almost the same for each language, you can use the template file (keyboard_ime_num.xml) as the input method file for multiple languages.

Customizing a Lang File

1. Open the template file.
2. Edit the corresponding string in the file.

keyboard_lang.xml

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<KeyboardLang>

<!--
-->
<!--
  <Lang Name="English">
    <Ime Name="keyboard_ime_en.xml"></Ime>
    <Ime Name="keyboard_ime_num.xml"></Ime>
  </Lang>
  -->

  <Lang Name="Francais">
    <Ime Name="keyboard_ime_francais.xml"></Ime>
    <Ime Name="keyboard_ime_num.xml"></Ime>
  </Lang>

</KeyboardLang>
```

Specify the display name of the language.

Specify the Ime file for the language.

3. Save the change and place this file on the provisioning server.

IME File Elements and Attributes

The following table lists the elements and attributes you need to understand in the Ime file. We recommend that you do not edit these elements and attributes.

Elements	Attributes	Description
KeyboardIme	Layout	Configures the Layout file that the keyboard will use.
KeyboardIm	DisplayNam	Configures the display name of the input mode when the input mode changes to lowercase.

e	e	
KeybOardImE	CapitalName	Configures the display name of the input mode when the input mode changes to uppercase.
KeybOardImE	ImeType	It can be set to Char or Symbol. If it is set to Symbol, the shift key will not take effect.
Line	/	Specifies a line on the keyboard. The first Line element represents the first line of the keyboard.
Key	ImeNormal	Configures the characters the key provides when the input mode is set to lowercase.
Key	ImeCapital	Configures the characters the key provides when the input mode is set to uppercase. It works only if the ImeType is set to Char.
Key	Function	Configures the key's function. There are 11 types of values for function attributes, which you can set to different values to provide different functions. The details are introduced below.

The following table lists the usage of the function keys:

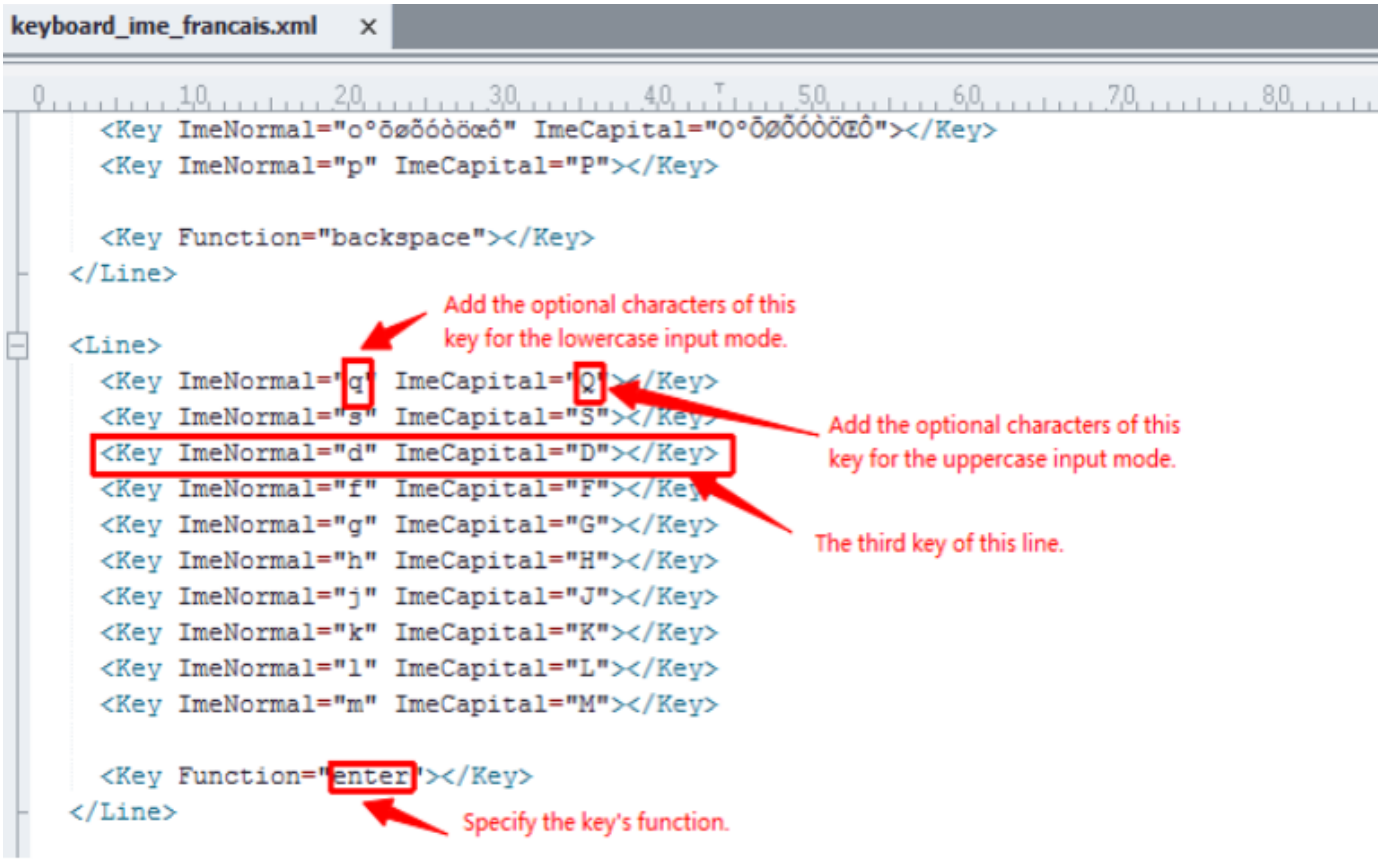
No.	Function Key	Usage
1	backspace	Delete the entered characters.
2	space	Enter spaces.
3	enter	Confirm the settings/Go to the next field.
4	left	Position the cursor.

5	right	Position the cursor.
6	up	Position the cursor.
7	down	Position the cursor.
8	hide	Hide the onscreen keyboard.
9	shift	Switch between the uppercase input mode and the lowercase input mode.
10	lang	Change the language of the keyboard.
11	switch	Change input mode.

Customizing an Ime File

1. Open the template file.

2. Edit the corresponding string in the file.



3. Save the change and place this file on the provisioning server.

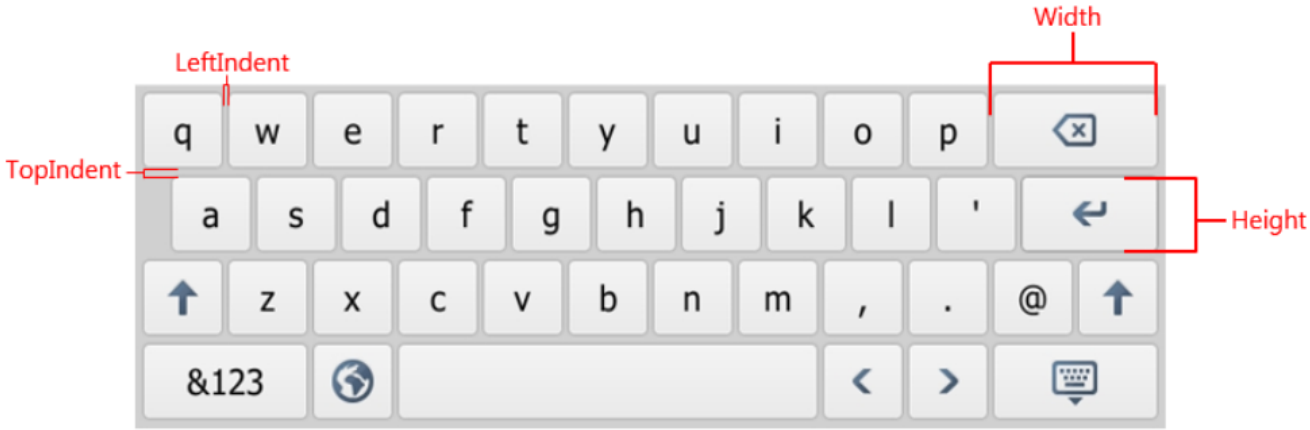
Layout File Elements and Attributes

The following lists the elements and attributes you need to understand in the Layout file. We recommend that you do not edit these elements and attributes.

Elements	Description
<KeyboardLayout > </	Indicate the start and end of a Layout file.

KeyboardLayout >	
<Line > </Line >	Specify a line on the keyboard. The first Line element represents the first line of the keyboard.
<Key > </Key >	Specify a key on the keyboard. The first key element in the Line element represents the first key of this line.

- The Line elements and Key elements both have four attributes: LeftIndent, TopIndent, Width, and Height (all attribute values are in pixels). The following picture shows the meaning of four attributes:



- The value of attributes in a line element is the default value of the corresponding attribute in the key element. For example, if you have not configured the width attribute in the key element, the key will automatically use the value of the width attribute configured in the line element as the width.
- The size of the onscreen keyboard is 800 pixels wide by 256 pixels high. If the area of the keyboard you configured is larger than the size of the keyboard, the part of the area beyond the keyboard will not be shown.

Customizing a Layout File

1. Open the template file.
2. Edit the corresponding string in the file.

```
keyboard_layout_francais.xml
<Line LeftIndent="2" TopIndent="6" Width="64" Height="58" >
  <Key LeftIndent="5"></Key>
  <Key></Key>
  <Key></Key>
  <Key></Key>
  <Key></Key>
  <Key></Key>
  <Key></Key>
  <Key></Key>
  <Key></Key>
  <Key></Key>
  <Key></Key>
  <Key Width="130"></Key>
</Line>
```

The first key of this line.

The first line of the keyboard.

3. Save the change and place this file on the provisioning server.

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
default_input_method.xml_browser_input_screen
phone_setting.virtual_keyboard.enable
gui_onscreen_keyboard.url

Parameter	Description	Permitted Values	Default	Supported Devices
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	URL within 511 characters	Blank	All phones except CP925/CP935W

	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. 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.			
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:	http://localhost/all or http://localhost/Name.txt	Blank	All phones except CP925/CP935W

	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			
default_input_method.dialing	It configures the default input method in the dialing screen.	0-2aB 1-123 2-abc 3-ABC	1	All phones except CP925/CP935W
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	All phones except CP925/CP935W
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	All phones except CP925/CP935W
default_input_method.xml_browser_input_screen	It configures the default input method when the type forthe input box is set to “string” in the InputScreen object. For T57W/T48U/T48S/T48G, it works only if "phone_setting.virtual_ke	Abc, 2aB, 123, abc or ABC	2aB	All phones except CP925/CP935W

	yboard.enable" is set to 0 (Disabled).			
phone_setting.virtual_keyboard.enable[1]	It enables or disables the phone to use the onscreen keyboard.	0-Disabled 1-Enabled	1	T57W, T48U, T48S, T48G, Video Phone, Conference Phone
gui_onscreen_keyboard.url[1]	It configures the access URL of the custom onscreen keyboard input method file.	URL within 511 characters	Blank	T57W, T48U, T48S, T48G, CP925, CP935W, Video Phone, Conference Phone
gui_input_method_hide.list	Used to control the full keyboard input method.	String	Blank	T48U/T57W

> [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 the French onscreen keyboard input method. The onscreen keyboard input method is only applicable to T57W/T48U/T48S/T48G phones and video phone.

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 on 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.

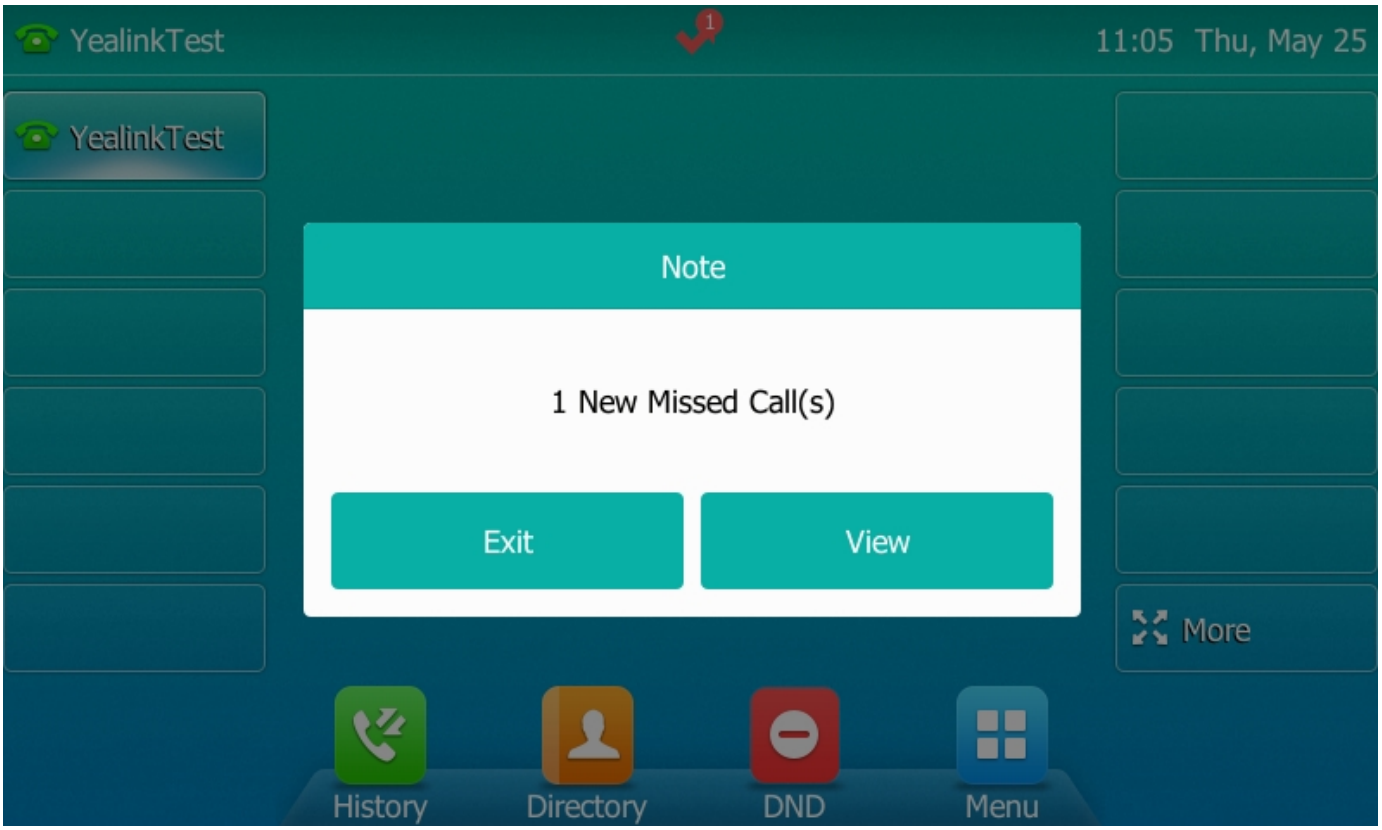
When using multiple keyboards, you can tap to change the language of keyboard for entering information.

Notification

Notification Popups

The notification popups feature allows the IP phone to pop up a message when it misses a call, forwards an incoming call to another party, receives a new voicemail, or areceives 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

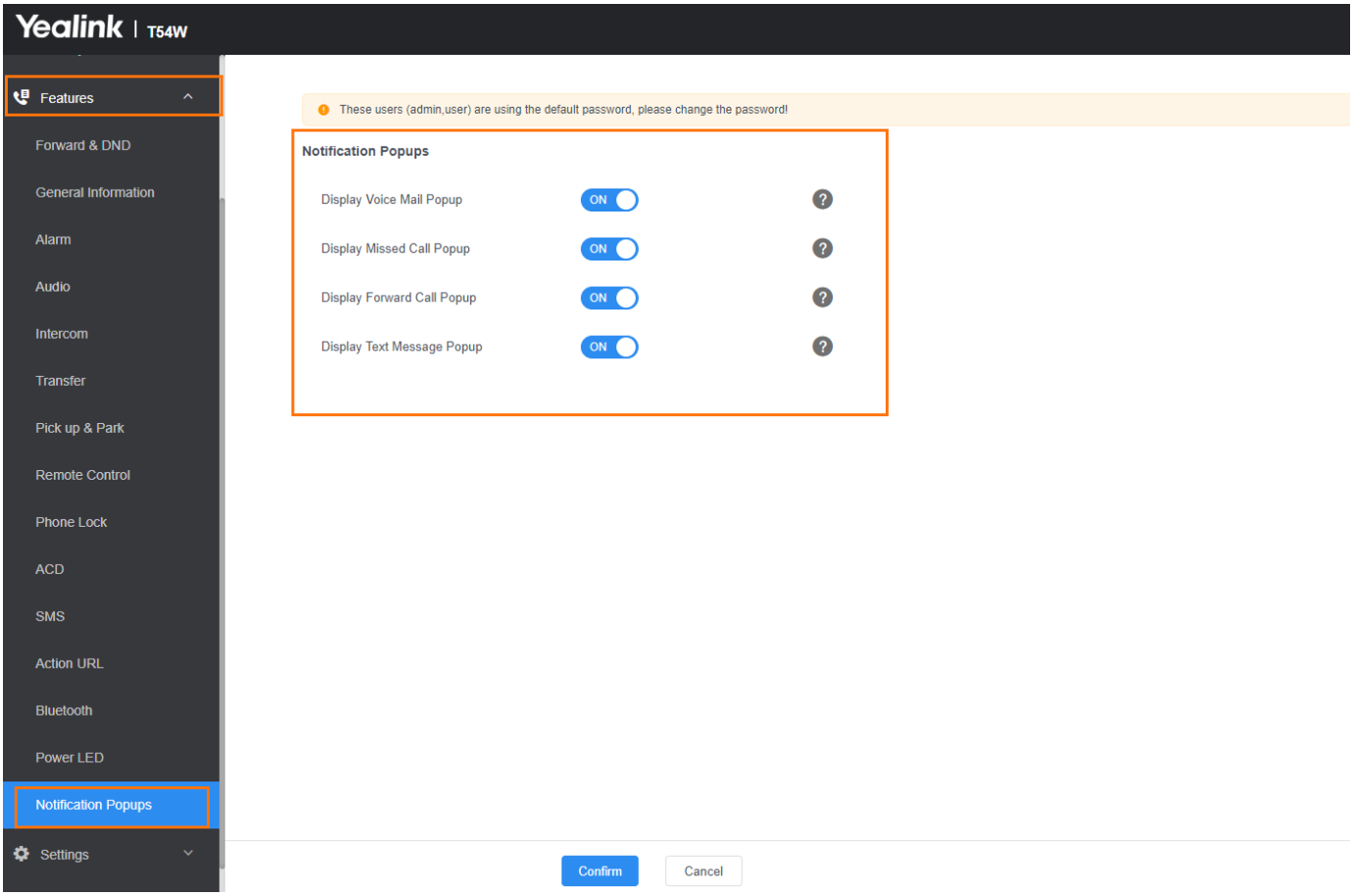
features.voice_mail_popup.enable
features.missed_call_popup.enable
features.forward_call_popup.enable
features.text_message_popup.enable

Parameter	Description	Permitted Values	Default

features.voice_mail_popup.enable	It enables or disables the phone to pop up a message when it receives a new voicemail. If the message disappears, it will not pop up again unless the phone receives a new voicemail or the user re-registers the account that has unread voicemail (s). 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 from popping up the message when it misses a call. 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 from popping up a 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 from popping up a message when it receives a new text message. 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

The power LED indicator indicates power status and phone status. It is not applicable to CP920/CP925/CP935W phones.

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

- The IP phone receives an incoming call
- The IP phone receives a voicemail 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.mute_power_led_flash_enable
phone_setting.hold_and_held_power_led_flash_enable
phone_setting.talk_and_dial_power_led_enable
phone_setting.missed_call_power_led_flash.enable
phone_setting.autop_led_flash_enable

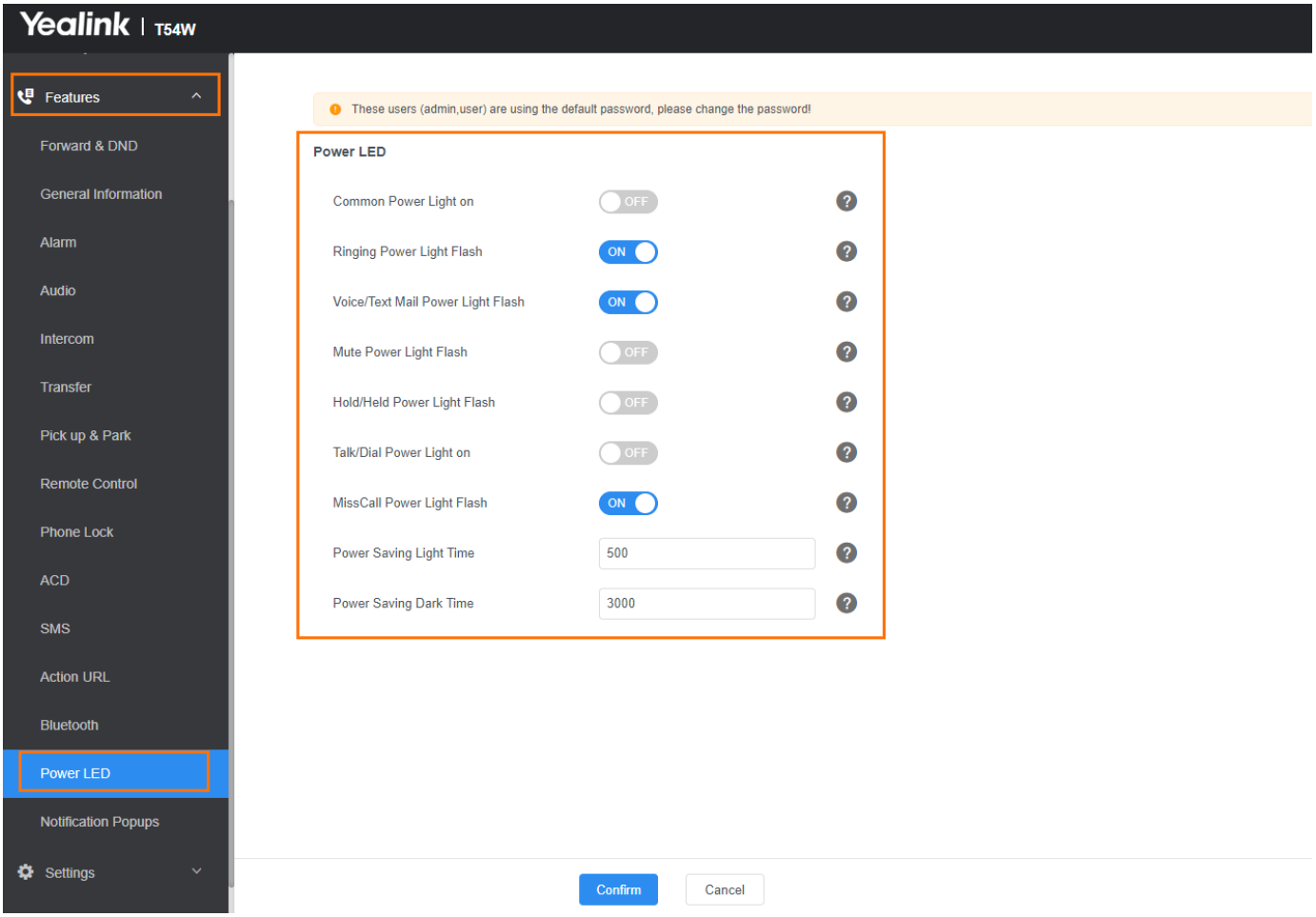
Parameter	Description	Permitted Values	Default	Supported Devices
phone_setting.common_power_led_enable	It enables or disables the power LED indicator to be turned on.	0-Disabled (power LED indicator is off) 1-Enabled (power LED indicator glows red) For T19 § E2 phones: 0-Disabled (power LED indicator is off) 1-Enabled (power LED indicator glows yellow)	0	All phones except CP920, CP925, CP935W, CP960, CP965
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	All phones except CP920, CP925, CP935W, CP960, CP965
phone_setting.mail_power_led_flash_enable	It enables or disables the power LED indicator to flash when the phone receives a voicemail or a text message. It works only if	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_en	1	All phones except CP920, CP925, CP935W, CP960, CP965

	"account.X.display_mwi.enable" is set to 1 (Enabled).	able" 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.)		
phone_setting.mute_power_led_flash_enable	It enables or disables the power LED indicator to flash when a call is muted.	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)	0	All phones except CP920, CP925, CP935W, CP960, CP965
phone_setting.hold_and_held_power_led_flash_enable	It enables or disables the power LED indicator to flash when a call is placed on hold or is held.	0-Disabled (power LED indicator does not flash) 1-Enabled (power LED indicator fast flashes (0.5s) red) For T19 § E2 phones: 0-Disabled (power LED indicator does not flash) 1-Enabled (power LED indicator fast flashes (0.5s) yellow)	0	All phones except CP920, CP925, CP935W, CP960, CP965
phone_setting.talk_and_dial_power	It enables or disables the power LED indicator from turning on when the phone is busy.	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	0	All phones except CP920, CP925,

_led_enable		yellow)		CP935W, CP960, CP965
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	All phones except CP920, CP925, CP935W, CP960, CP965
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	All phones except CP920, CP925, CP935W, CP960, CP965

Set via the Web User Interface

On the web user interface, go to: **Features** > **Power LED.**


Yealink | T54W
Features
Forward & DND
General Information
Alarm
Audio
Intercom
Transfer
Pick up & Park
Remote Control
Phone Lock
ACD
SMS
Action URL
Bluetooth
Power LED
Notification Popups
Settings
These users (admin,user) are using the default password, please change the password!
Power LED
Common Power Light on
OFF
Ringing Power Light Flash
ON
Voice/Text Mail Power Light Flash
ON
Mute Power Light Flash
OFF
Hold/Held Power Light Flash
OFF
Talk/Dial Power Light on
OFF
MissCall Power Light Flash
ON
Power Saving Light Time
500
Power Saving Dark Time
3000
Confirm
Cancel

Bluetooth

Introduction

You can pair and connect a Bluetooth headset or Bluetooth-enabled mobile phone with the IP phone. After connecting the Bluetooth-enabled mobile phone, you can synchronize the mobile contacts to the IP phone.

For VP59/T58W/T58V/T58A/T56A/T57W/T54W/T53W/T53/T53C/T48U/T46U/T43U/T42U phones, they can also make and receive mobile calls on the IP phone. For CP920/CP925/CP935W/CP960/CP965 phones, you can also use your IP phone as a Bluetooth speaker for your mobile phone and PC. You can set up a conference among the calls on your IP phone, the PSTN, and the connected mobile phone (PSTN does not apply to CP935W phones).

> To use the Bluetooth feature on T53/T53C/T48U/T48S/T48G/T46U/T46S/T46G/T43U/T42U/T42S/T41S/T29G/T27G phones, make sure the Bluetooth USB dongle is properly connected to the USB port on the back of the phones. The Bluetooth dongle should be purchased separately.

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 display in a scanning list of other devices. It is helpful for the other Bluetooth devices to identify and pair with your IP 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.a2dp_sink
bluetooth.high_encryption.enable
phone_setting.headset_auto_connect

Parameter	Description	Permitted Values	Def aul	Supported Devices

			t	
static.bluetooth.function.enable[1]	It enables or disables the Bluetooth feature. For T53/T53C/T48U/T48S/T48G/T46U/T46S/T46G/T43U/T42U/T42S/T41S/T29G/T27G phones, it works only if "static.usb.power.enable" is set to 1 (Enabled).	0-Disabled, you are not allowed to trigger Bluetooth mode on. 1-Enabled	1	T57W, T54W, T53W, T53, T53C, T48U, T48S, T48G, T46U, T46S, T46G, T43U, T42U, T42S, T41S, T29G, T27G, CP920, CP925, CP935W
features.bluetooth_enable	It triggers the Bluetooth mode to turn on or off. It works only if "static.bluetooth.function.enable" is set to 1 (Enabled).	0-Off 1-On	0	T57W, T54W, T53W, T53, T53C, T48U, T48S, T48G, T46U, T46S, T46G, T43U, T42U, T42S, T41S, T29G, T27G, CP920, CP925, CP935W
features.bluetooth_adapter_name	It configures the Bluetooth device name. It works only if "features.bluetooth_enable" is set to 1 (On).	String within 64 characters	Yealink-$DEV	T57W, T54W, T53W, T53, T53C, T48U, T48S, T48G, T46U, T46S, T46G, T43U, T42U, T42S, T41S, T29G, T27G, CP920, CP925, CP935W
bluetooth.c	It enables or disables the	0-Disabled	0	CP920, CP925,

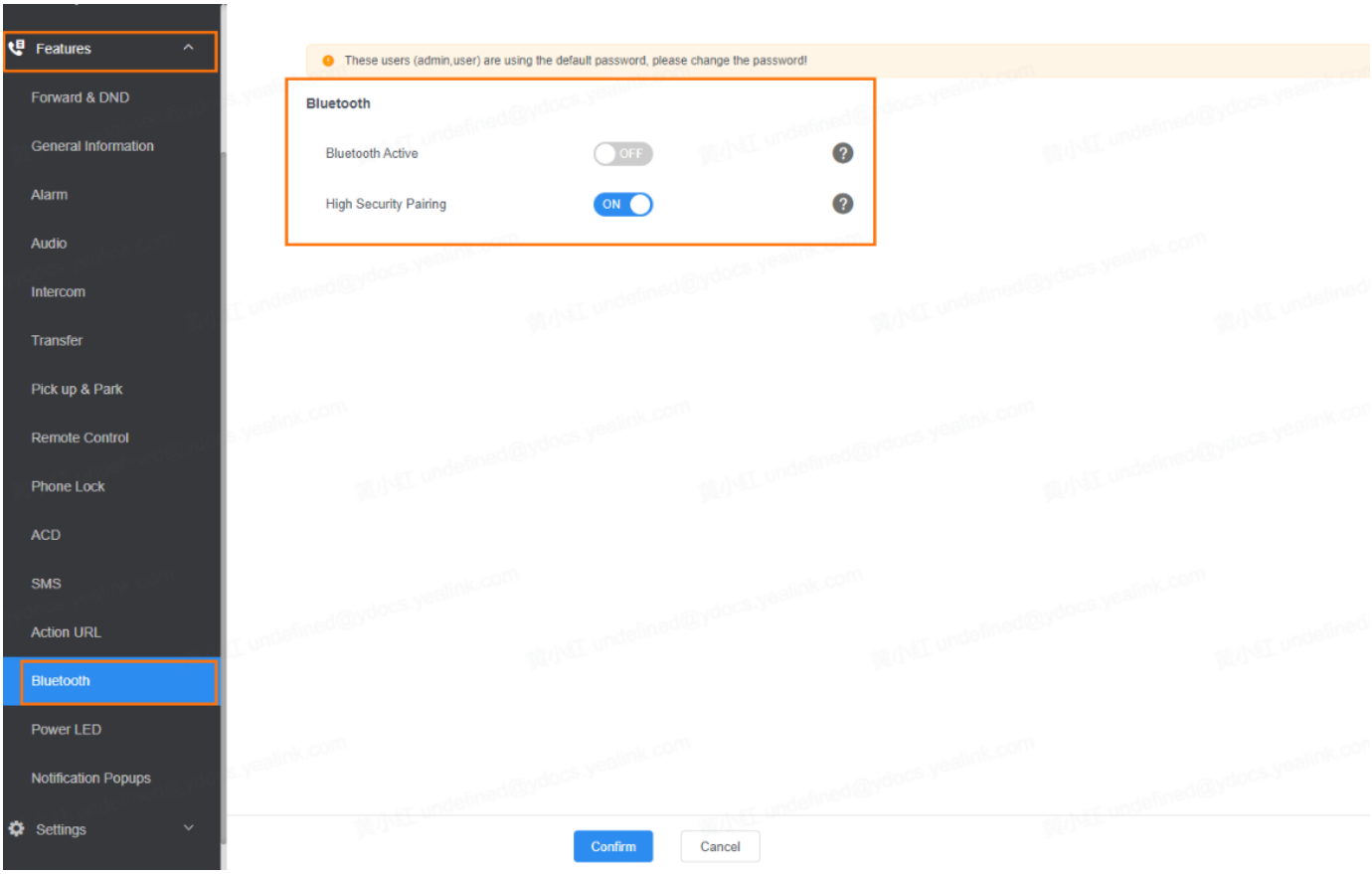
onnect_confirm.enable[1]	phone to prompt users to confirm the connection request from the Bluetooth device.	1-Enabled, the prompt will not appear during the call.		CP935W
bluetooth.connect_confirm.enable[1]	It enables or disables the phone to prompt users to confirm the connection request from the Bluetooth device.	0-Disabled 1-Enabled, the prompt will not appear during the call.	0	CP920, CP925, CP935W
bluetooth.a2dp_sink[1]	It enables or disables the phone to act as a connected Bluetooth-enabled mobile phone player.	0-Disabled, the Media audio item is hidden on the connected Bluetooth-enabled mobile phone. 1-Enabled, you need to enable the Media audio feature manually after the Bluetooth-enabled mobile phone is paired and connected. Enable the Media audio feature via the phone user interface at the path: Menu > Settings > Basic Settings > Bluetooth > Paired Bluetooth Device > Option > Detail > Channel Control > > Media Audio. 2-Enabled, the phone automatically acts as the Bluetooth-enabled mobile phone player after you pair and connect the Bluetooth-enabled mobile phone	1	CP920, CP925, CP935W

		to the phone successfully. Media Audio. For CP925/ CP935W: More > Basic > Bluetooth > Paired Device >		
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 56 bits.	1	T57W, T54W, T53W, T53, T53C, T48U, T48S, T46U, T46S, T43U, T42U, T42S, T41S, T27G, CP920, CP925, CP935W
phone_setting.headset_auto_connect	It configures whether to enable the automatic connection prompt function of the Bluetooth headset.	0-Disabled 1-Enabled	1	T57W, T54W, T53W, BH71,BH72, BH76

> [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.**


Features
Forward & DND
General Information
Alarm
Audio
Intercom
Transfer
Pick up & Park
Remote Control
Phone Lock
ACD
SMS
Action URL
Bluetooth
Power LED
Notification Popups
Settings
These users (admin,user) are using the default password, please change the password!
Bluetooth
Bluetooth Active
OFF
High Security Pairing
ON
Confirm
Cancel

Handset & Headset & Speakerphone Mode

Introduction

Yealink phones support three ways to place/answer a call: using the handset, using the headset or using the speakerphone. You can disable the infrequently used audio device as required.

Handset/Headset/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.group_listen_in_talking_enable
features.headset_mode.enable
features.headset.group_listen_in_talking_enable
phone_setting.headsetkey_mode

Parameter	Description	Permitted Values	Default	Supported Devices
features.speaker_mode.enable	It enables or disables the phone’s speakerphone mode.	0-Disabled 1-Enabled	1	All phones except CP920/CP925/ CP935W
features.handset_mode.enable	It enables or disables the phone’s handset mode.	0-Disabled 1-Enabled	1	All phones except CP920/CP925
features.group_listen_in_talking_enable	It enables or disables the phone to enter the group listening mode by pressing the Speakerphone key when you first answer the call using the handset. The audio is sent only through the handset. So you can	0-Disabled 1-Enabled	1	All phones except CP920/CP925

	speak and listen through the handset, but you can only listen through the speaker.			
features.headset_mode.enable	It enables or disables the phone’ s headset mode.	0-Disabled 1-Enabled	1	All phones except CP920/CP925
features.headset.group_listen_in_talking_enable	It enables or disables the phone to enter the group listening mode by pressing the Speakerphone key when you first answer the call using the headset. The audio is sent only through the headset. So you can speak and listen through the headset, but you can only listen through the speaker. It does not apply to Bluetooth headsets.	0-Disabled 1-Enabled	0	T57W, T54W, T53W, T53, T53C, T48U, T46U, T43U, T42U, T48S, T46S, T42S, T41S, T33P, T33G, T31P, T31G, T31, T30P, T30, T27G
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	All phones except CP920/CP925

DSS Keys

DSS Keys

There are three kinds of DSS keys: Line Keys, Programmable Keys, and Ext Keys. You can assign various functions to DSS keys. This section explains how to set these keys.

Line key does not apply to T30P/T30/T19 E2/T19P E2/CP920 phones. Ext key is only applicable to expansion modules connected to T57W/T54W/T53W/T53/T53C/T48U/T48S/T48G/T46U/T46S/T46G/T43U/T29G/T27G phones.

NOTE

If the phone is downgraded to an earlier firmware from firmware version 83, the DSS key configuration will be reset after downgrading.

Supported DSS Keys

The following table lists the number of DSS keys you can configure for each phone model:

Phone Model	Line Keys	Programmable Keys	Ext Keys
T88V Pro/T88W (Pro)	84	10	78
T87W	84	10	78
T85W	60	16	78
T77U	84	9	78
T74U/T74W	50	15	78
T73U/T73W	40	15	78
T57W	29	9	60
T54W	27	15	60
T53W/T53/T53C/T43U	21	13	60
T48U	29	15	60
T48G/T48S	29	15	40
T46U	27	15	60
T46S/T46G	27	15	40
T42U/T42G/T42S	15	13	/
T41P/T41S	15	13	/

T40P/T40G	3	13	/
T33P/T33G	12	13	/
T31P/T31G/T31	2	13	/
T30P/T30	/	13	/
T29G	27	16	39
T27G	21	16	39
T23P/T23G	3	13	/
T19 E2/T19P E2	/	13	/
CP920	/	8	/
CP925	30	4	/
CP935W	30	4	/
CP960	30	3	/
CP965	30	4	/
T58A	27	9	60
T58W	27	9	60
VP59	27	9	/
T73U/T73W	40	15	78
T74U/T74W	50	15	78
T77U	84	10	78
T85W	60	15	78
T87W	84	10	78
T88W/T88V	84	10	78

NOTE

The programmable key takes effect only if the phone is idle. The ext key takes effect only if the expansion module is connected to the phone.

Supported Dsskey Types

The supported Dsskey function types vary by line keys, programmable keys, and Ext keys.

ID	DSS Key Types	ID	DSS Key Types	ID	DSS Key Types
0	N/A	20	Private Hold	51	Switch Account Up (Programmable key)

1	Conference (Line key/Ext key)	22	XML Group	52	Switch Account Down (Programmable key)
2	Forward	23	Group Pickup	56	Retrieve Park (Line key/Ext key)
3	Transfer (Line key/Ext key)	24	Paging(Multicast Paging) (Line key/ Ext key)	61	Directory
4	Hold (Line key/ Ext key)	25	Record (Line key/ Ext key)	66	Paging List
5	DND	27	XML Browser	73	Custom Key (only appear when “features.enhanced_dss_keys.enable = 1”)
7	Recall	28	History (Programmable key)	77	Mobile Account (only appear when the Bluetooth-enabled mobile phone is connected)
8	SMS	30	Menu (Programmable key)	104	Google Contacts (only appear when “google_contact_server.enable = 1”)
9	Pickup(Pick up/ Direct Pickup)	33	Status (Programmable key)	105	XML Park (Line key/Ext key)
10	Call Park (Line key/Ext key)	34	Hot Desking	150	Extend (Line key/Programmable key)
11	DTMF (Line key/ Ext key)	35	URL Record (Line key/Ext key)	310	Dect Intercom (only appear when the DECT USB dongle is connected)
12	Voice Mail (Line key/Ext key)	38	LDAP(only appear when “ldap.enable=1”)	72	Missed Call (need V86)
13	Speed Dial(SpeedDial)	39	BLF List	62	Emergency Call (Only applicable to T85W/T87W/T88W phones)
14	Intercom	40	Prefix		
15	Line (Line key/	41	Zero Touch		

	Ext key)				
16	BLF (Line key/ Ext key)	42	ACD (Line key/Ext key)		
17	URL (Line key/ Ext key)	45	Local Group		
18	Group Listening (Line key/Ext key)	50	Phone Lock (Line key/Ext key)		

Line Keys

Line keys provide one-touch feature (for example, one-touch park). This allows you to quickly access features and to view the monitored status when the line keys are assigned with particular features (for example, BLF).

Line key is not applicable to T30P/T30/T19 E2/T19P E2/CP920 phones.

Line Keys Configuration

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

Configuration parameter

linekey.type_range.custom
linekey.X.type
linekey.X.line
linekey.X.value
linekey.X.label
linekey.X.extension
linekey.X.xml_phonebook
features.flash_url_dsskey_led.enable
features.block_linekey_in_menu.enable
auto_provision.allsettings.sync.path
auto_provision.allsettings.sync
custom.hide_url_dsskey_icon.enable

Parameter	Description	Permitted Values	Default	Supported Devices

linekey.type_range.custom	It configures the list of available line key types when configuring line keys. To assign function types, specify line key type IDs which start with or without a symbol ”+”. For example, “+2,15,16,7,4” or “2,15,16,7,4” means only “N/A”, “Forward”, “Line”, “BLF”, “Recall”, “Hold” types are available when you configure line keys. To remove a function type, specify line key type IDs which start with the symbol “-”. For example, “-14, 5, 2” means to remove “Intercom”, “DND”, “Forward” types from the line key types list. These line key types are not available when you configure line keys. NOTE Multiple line key type IDs are separated by commas. “N/A” type is always kept.	Blank or 0 (all valid function types are available); line key type IDs. For supported line key types and IDs, refer to Supported Dsskey Types.	Blank	All phones except T30P, T30, T19 E2/ T19P E2 and CP920
linekey.X.ty	It configures the key	0-N/A	15:	All

pe[1]	feature.	1-Conference 2-Forward 3-Transfer 4-Hold 5-DND 7-Recall 8-SMS 9-Pickup(pick up/ Direct Pickup) 10-Call Park 11-DTMF 12-Voice Mail 13-SpeedDial(Speed Dial) 14-Intercom 15-Line16-BLF 17-URL 18-Group Listening 20-Private Hold 22-XML Group 23-Group Pickup 24-Paging(Multicast Paging) 25-Record 27-XML Browser 34-Hot Desking 35-URL Record 38-LDAP (only appear when “ldap.enable=1”) 39-BLF List 40-Prefix 41-Zero Touch	T57W/T54W/ T48U/T48S/T48G/ T46U/T46S/T46G/ T29G: X= 1-16; T53W/T53/T53C/ T43U/T42U/T42S/ T42G: X = 1-12; T41P/T41S/T27G: X = 1-6; T33P/T33G: X = 1-4; T40P/T40G/T31P/ T31G/T31/T23P/ T23G/T21 § E2: all line keys. CP925/CP935W: 1 0: other line keys	phones except T30P, T30, T19 E2/ T19P E2 and CP920

		42-ACD 45-Local Group 50-Phone Lock 56-Retrieve Park 61-Directory 62-Emergency Call (only applicable to T85W/T87W/ T88Wphones) 66-Paging List 73-Custom Key (only available when “features.enhanced_dss_keys.enable =1”) 77-Mobile Account (only applicable to T57W/T54W/T53W/ T53/T53C/T48U/ T46U/T43U/T42U phones when the Bluetooth-enabled mobile phone is connected) 104-Google Contacts (only appear when “google_contact_server.enable = 1”) 105-XML Park (not applicable to CP920 phones) 150-Extend (only applicable to T54W/ T53W/T53/T53C/		

		T46U/T46S/T43U/T42S/T42U/T41S/T27G phones) 310-DECT Intercom (only applicable to T57W/T54W/T53W/T53/T53C phones when the DECT USB dongle is connected) NOTE The permitted values are configurable by "linekey.type_range.custom".		
linekey.X.line[1]	It configures the desired line to apply the line key feature.	T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G: 0, 1-16; T53W/T53/T53C/T43U/T42U/T42S/T42G: 0, 1-12; T41P/T41S/T27G: 0, 1-6; T33P/T33G: 0, 1-4; T40P/T40G/T23P/T23G: 0, 1-3 T31P/T31G/T31/T21 § E2: 0, 1-2 CP925/CP935W: 1	1	All phones except T30P, T30, T19 E2/T19P E2 and CP920

		features.fwd_mode = 1 & linekey.X.type =2 & linekey.X.line =0: it means forward will apply to all lines on the phone; linekey.X.type = 13 & linekey.X.line =0: it means the phone can automatically switch accounts for speed dial; linekey.X.type = 14 & linekey.X.line =0: it means the phone can automatically switch accounts for intercom.		
linekey.X.va	It configures the value for	String within 99	Blank	All

lue[1]	some line key features. For example, when you assign the Speed Dial to the line key, this parameter is used to specify the contact number you want to dial out. It is also used to specify the contact number with the DTMF sequence. The contact number and DTMF sequence are separated by commas.	characters		phones except T30P, T30, T19 E2/ T19P E2 and CP920
linekey.X.label[1]	It configures the label displayed on the phone screen. This is an optional configuration.	String within 99 characters	Blank	All phones except T30P, T30, T19 E2/ T19P E2 and CP920
linekey.X.extension[1]	For multicast paging: It configures the channel of the multicast paging group. For the BLF/BLF list/ intercom feature: It configures the pickup code. It is only applicable when "linekey.X.type" is set to 14, 16, 24	For multicast paging: 0 to 31 For the BLF/BLF list/intercom feature: String within 256 characters	Blank	All phones except T30P, T30, T19 E2/ T19P E2 and CP920

	or 39.			
linekey.X.xml_phonebook[1]	It specifies a specific group/phone book when multiple groups/phone books are configured on the phone. For example, both Remote Phone Book 1 "Sell" and Remote Phone Book 2 "Market" are configured on the phone, you can configure "linekey.X.xml_phonebook = 0" to specify the Remote Phone Book 1 "Sell" for the specific line key. The user can press this line key to access the Remote Phone Book 1 "Sell". It is only applicable when "linekey.X.type" is set to 22 or 45.	Integer from 0 to 48	0	All phones except T30P, T30, T19 E2/ T19P E2 and CP920
features.flash_url_dsskey_led.enable	It enables or disables the LED indicator of the URL DSS key. The LED indicator behavior depends on the response message from the server when you press the URL DSS key on the phone.	0-Disabled 1-Enabled	1	All phones except T30P, T30, T19 E2/ T19P E2, CP920, CP925

				and CP935W
features.block_linekey_in_menu.enable	It enables or disables the phone to prevent the user from using line keys when browsing the menu.	0-Disabled 1-Enabled, it prevents the user from using line keys.	0	All phones except T57W, T48U, T48S, T48G, T30P, T30, T19 E2/ T19P E2, CP920, CP925 and CP935W, Video phone, CP960, CP965
auto_provision.allsettings.sync.path	It specifies the path for uploading the mac-all.cfg file. Example: static.auto_provision.allsettings.sync.path = https://192.168.1.100/hotdesking.cfg The phone uploads the cfg file to 192.168.1.100 and names it hotdesking.cfg;	String	Blank	

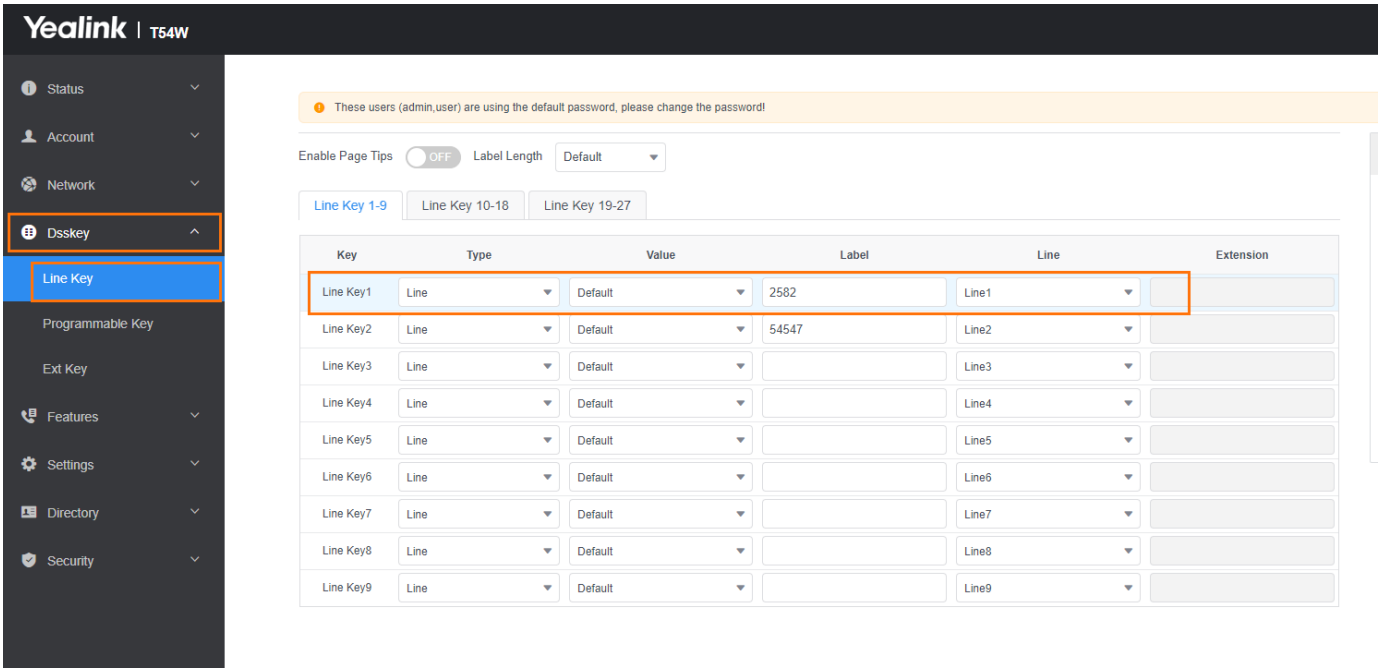
	and it also requests the hotdesking.cfg file when downloading synchronously. It works only if "static.auto_provision.allsettings.sync" is set to 1 (Enabled).			
auto_provision.allsettings.sync	It enables or disables the phone to upload the mac-all.cfg file to the server.	0-Disabled 1-Enabled	0	
custom.hide_url_dsskey_icon.enable	It is used to configure whether to hide the icon of URL-type DSS keys. It works only if your firmware version is x.86.0.112 or later.	0: Do not hide the default icon displayed in front of URL-type DSS keys (default value). 1: Hide the default icon displayed in front of URL-type DSS keys, and use the empty space to display the label, with the label starting from the top left.	0	
features.dsskey_page_reset.switch_time	It is used to configure the time for DSS key page to return to the default page. It works only if your firmware version is x.86.0.112 or later.	0-Disable 5-3600-After the corresponding time (between 5 and 3600 seconds), it will jump back to the default page, which is the first page by default.	0	

features.hide_feature_access_codes.dsskey_type	It is used to configure the Dsskey Type types that hide the code functionality. Multiple values can be set simultaneously, separated by commas. It works only if your firmware version is x.86.0.112 or later.	9(Pickup) 10(Call Park) 12(Voice Mail) 13(SpeedDial) 14(Intercom) 16(BLF) 23(Group Pickup) 56(Retrieve Park)	Blank	

> [1]X is the line key ID. For T57W/T48U/T48S/T48G, X=1-29; for T54W/T46U/T46S/T46G/T29G, X=1-27; for T53W/T53/T53C/T43U/T27G, X=1-21; for T42U/T42G/T42S/T41P/T41S, X=1-15; for T33P/T33G, X=1-12; for T40P/T40G/T23P/T23G, X=1-3; for T31P/T31G/T31/T21 § E2, X=1-2; for CP925/CP935W, X=1-30; for T73U/T73W, X=1-40; for T74U/T74W, X=1-50; for T85W, X=1-60; for T77U/T87W/T88W(Pro)/T88V Pro, X=1-84.

Set via the Web User Interface

On the web user interface, go to: **Dsskey** > **Line Key**



Example: Set a Park/Retrieve Key for FAC Call Park Mode

Scenario Conditions	Related Topic

features.call_park.park_code = *68	Call Park and Retrieve
features.call_park.park_retrieve_code = *88	Call Park and Retrieve
features.call_park.park_mode = 1	Call Park and Retrieve

Example

```
######Set a Park key######
linekey.1.type = 10
linekey.1.value =4603
linekey.1.label =Bill
######Set a Retrieve key####
linekey.3.type = 56
linekey.3.line =1
linekey.3.value =4603
linekey.3.label =Retrieve Bill
```

After provisioning, you can easily press the Park key (line key 1) to park a call to a specific extension (4603) during a call, and press the Retrieve key (line key 3) to retrieve the parked call from the specific extension (4603) when the phone is idle.

If the "linekey.1.value" is set to blank, the park key will perform as the Park soft key.

NOTE

In FAC call park mode, the Park/Retrieve key invokes the call park code/park retrieve code by default. Therefore, the phone dials out *684603 to park a call, and dials out *884603 to retrieve a call. If these codes are not set, you can assign code and extension to "linekey.X.value", for example, "*684603".

Example: Set a Park/Retrieve Key for Transfer Call Park Mode

Scenario Conditions	Related Topic
features.call_park.park_mode = 2	Call Park and Retrieve
features.call_park.line_restriction.enable = 1	Call Park and Retrieve

Example

```
######Set a Park key######
linekey.1.type = 10
linekey.1.value =*01
```

```
linekey.1.line = 1
linekey.1.label =Bill
######Set a Retrieve key####
linekey.3.type = 56
linekey.3.line = 1
linekey.3.value =*11
linekey.3.label =Retrieve Bill
```

After provisioning, you can easily press the Park key (line key 1) to park a call to the specific shared parking lot (*01) during a call, and press the Retrieve key (line key 3) to retrieve the parked call from the shared parking lot (*01) using the retrieve code (*11). You can only perform call park feature on the specific line (line 1).

If the "features.call_park.line_restriction.enable" is set to 0 (Disabled), the phone will park/retrieve the call to the server on the current line in use.

NOTE

In Transfer call park mode, if you press the Park key when the phone is idle, the Park key will invoke the call park code. Therefore, you can use a Park key to park and retrieve a call. In this case, you need to assign the park retrieve code (*****11) to "features.call_park.park_code". When you press the Park key again on the idle screen, the phone will dial out "1101" to retrieve the parked call.

Example: Setting a Line Key as Directed Pickup Key

Scenario Conditions	Related Topic
account.1.direct_pickup_code = *97 or features.pickup.direct_pickup_code = *97	Directed Call Pickup

Example

```
linekey.1.type = 9
linekey.1.line =1
linekey.1.value= 4603
linekey.1.label=Bill
```

After provisioning, you can easily press the Directed Pickup key (line key 1) to pick up an incoming call to a specific phone (4603).

NOTE

The Directed Pickup invokes the directed pickup code by default. Therefore, the phone dials out *974603 to pick up a call. If the directed code is not set, you can assign code and extension to “linekey.X.value”, for example, “*974603”.

Example: Setting a Line Key as Group Pickup Key

The following example shows the configuration for a group pickup key.

Example

```
linekey.1.type = 23
linekey.1.line =1
linekey.1.value =*98
linekey.1.label =Sell
```

After provisioning, you can easily press the Group Pickup key (line key 1) to pick up an incoming call to any phone within a predefined group of phones.

NOTE
If the “linekey.X.value” is not assigned with a group pickup code, the Park key will invoke the group pickup code set by “features.pickup.group_pickup_code” or ”account.X.group_pickup_code”.

Example: Setting a Line Key as Forward Key

When the phone receives an incoming call, you can press a Forward key to forward the incoming call to the preset number.

When the phone is idle, the key behavior depends on the forward modes:

Forward Modes	Key Behavior
Phone Mode	The destination number is configured: Press the Forward key to activate/deactivate the always forward feature or switch the target among Forward keys. The destination number is blank: Press the Forward key to enter the forward setting screen or activate/deactivate the forward feature (if forward has been configured from the Call Forward menu).

Custom Mode	Press the Forward key to enter the forward setting screen.

The following example shows the configuration for Forward keys.

Scenario Conditions	Related Topic
features.fwd.allow = 1	Call Forward
features.fwd_mode = 0	
forward.idle_access_always_fwd.enable = 0	

Example

```
######Set a Forward key for Bill######
linekey.1.type = 2
linekey.1.line =1
linekey.1.value =4603
linekey.1.label =Bill
######Set a Forward key for Tom######
linekey.2.type = 2
linekey.2.line =1
linekey.2.value =4605
linekey.2.label =Tom
```

After provisioning, you can easily press the Forward key (line key 1 or line key 2) to activate/deactivate the always forward feature. For example, after pressing line key 1 to activate always forward and forward all calls to Bill (4603), you can press the line key 1 to deactivate always forward, or press line key 2 to switch the forward target and forward all calls to Tom (4605).

Example: Setting a Line Key as BLF List Key

The following example shows the configuration for a BLF List key.

Scenario Conditions	Related Topic
phone_setting.auto_blf_list_enable = 0	BLF List Configuration

Example

```
linekey.1.type = 39
linekey.1.line =1
```

After provisioning, a BLF List key displays on line key 1. You can easily use this key to monitor a remote line. The monitored line depends on a pre-configured SIP server.

Example: Setting a Line Key as Private Hold Key

The following example shows the configuration for a Private Hold key.

Example

```
linekey.1.type = 20
linekey.1.label =Private Hold
```

After provisioning, you can press the line key 1 to hold calls without notifying other phones registered with the shared line, the shared line displays active to others shared line. It is only applicable to Shared Line Appearance.

Example: Setting a Line Key as Multicast Paging Key

The following example shows the configuration for a Multicast Paging key.

Example

```
linekey.1.type = 24
linekey.1.value = 224.5.6.20:10008
linekey.1.label = Sales
linekey.1.extension = 2
```

After provisioning, you can press the line key 1 to send announcements quickly to the Sales group.

Programmable Keys

You can customize programmable keys on the phone to enable users to access frequently used functions, or, if your phone does not have a particular hard key, you can create a soft key. For example, if the phone does not have a Do Not Disturb hard key, you can create a Do Not Disturb soft key.

The programmable key takes effect only when the IP phone is idle.

Supported Programmable Keys

The following tables list programmable keys for each phone model.

Programs	CP925/	CP920	T31P/T31G/T31/	T23P/	T29G/	T53W/T53/T53C/T43U/T42G/T42S/	T54W/T48U/T48G/ T48S/T46U/T46S/	T57W/	T85W	T87W/

mmable Key IDs	CP935W		T30P/T30/T19E2/T19PE2	T23G/T21§E2	T27G	T42U/ T41P/ T41S /T40P/ T40G/ T33P/ T33G	T46G/T73U/ T73W/T74U/ T74W	T77U		T88W/T88V
1	SoftKey1	SoftKey1	SoftKey1	SoftKey1	SoftKey1	SoftKey1	SoftKey1	SoftKey1	SoftKey1	SoftKey1
2	SoftKey2	SoftKey2	SoftKey2	SoftKey2	SoftKey2	SoftKey2	SoftKey2	SoftKey2	SoftKey2	SoftKey2
3	SoftKey3	SoftKey3	SoftKey3	SoftKey3	SoftKey3	SoftKey3	SoftKey3	SoftKey3	SoftKey3	SoftKey3
4	SoftKey4	SoftKey4	SoftKey4	SoftKey4	SoftKey4	SoftKey4	SoftKey4	SoftKey4	SoftKey4	SoftKey4
5	/	Up	Up	Up	Up	Up	Up	/	Up	/
6	/	Down	Down	Down	Down	Down	Down	/	Down	/
7	/	/	Left	Left	Left	Left	Left	/	Left	/
8	/	/	Right	Right	Right	Right	Right	/	Right	/
9	/	OK	OK	OK	OK	OK	OK	/	OK	/
10	/	/	/	Cancel	Cancel	Cancel	Cancel	/	Cancel	/
11	/	/	/	/	CO	/	/	/	/	/

					NF					
12	/	/	/	/	HOLD	/	HOLD	HOLD	HOLD	HOLD
13	/	MUTE	MUTE	/	MUTE	MUTE	MUTE	MUTE	MUTE	MUTE
14	/	/	TRAN	TRAN	TRAN	/	TRAN	TRAN	TRAN	TRAN
17	/	/	Redial	Redial	Redial	Redial	Redial	Redial	Redial	Redial
18	/	/	Message	Message	Message	Message	Message	Message	Message	Message
19	/	/	/	/	/	/	/	/	Action Button	Action Button

Programmable Keys Configuration

For T23P/T23G/T21 E2 phones, Cancel key can be configured only when "features.keep_mute.enable" is set to 0 (Disabled).

For other phones, Mute key can be configured only when "features.keep_mute.enable" is set to 0 (Disabled).

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

Configuration parameter

```
programablekey.type_range.custom
programablekey.X.type
programablekey.X.history_type
programablekey.X.line
programablekey.X.value
programablekey.X.label
programablekey.X.extension
programablekey.X.xml_phonebook
```

programablekey.19.type

Parameter	Description	Permitted Values	Default
programablekey.type_range.custom	It configures the list for available programmable key types when configuring programmable keys. To assign function types, specify programmable key type IDs which start with or without a symbol ”+”. For example, “+2,15,16,7,4” or “2,15,16,7,4” means only “N/A”, “Forward”, “Line”, “BLF”, “Recall”, “Hold” types are available when you configure programmable keys. To remove a function type, specify programmable key type IDs which start with the symbol “-”. For example, “-14, 5, 2” means to remove “Intercom”, “DND”, “Forward” types from the Dsskey function types list. These programmable key types are not available when you configure programmable keys. Note: Multiple programmable key type IDs are separated by commas. “N/A” type is always	Blank or 0 (all valid function types are available); Dsskey type IDs. For supported Dsskey types and IDs, refer to Supported Dsskey Types.	Blank

	kept.		
programablekey.X.type[1]	It configures a key feature for a specific programmable key.	0-N/A 2-Forward 5-DND 7-Recall 8-SMS 9-Pick up 13-Speed Dial 14-Intercom 22-XML Group 23-Group Pickup 24-Multicast Paging (Paging) 27-XML Browser 28-History 29-Directory (only applicable to CP925/CP935W) 30-Menu 32-New SMS 33-Status 34-Hot Desking 38-LDAP (only appear when “ldap.enable = 1”) 40-Prefix 41-Zero Touch43-Local Directory (Local Phonebook) 45-Local Group 50-Phone Lock 51-Switch Account Up (not applicable to T57W/T30P/T30/T19 E2/T19P E2) 52-Switch Account Down (not applicable to T57W/T30P/T30/T19 § E2) 61-Directory	X=1, default: 28 - History X=2, default: 61 - Directory X=3, default: 5 – DND X=4, default: 30 - Menu X=5, default: 28- History X=6, default: 61- Directory X=7, default: 51- Switch Account Up X=8, default: 52- Switch Account Down X=9, default: 33- Status X=10, default: 0 - NA X=11, default: 0 – NA X=12, default: 0 - NA X=13, default: 0 – NA

		62-Emergency Call (only applicable to T85W/T87W/T88Wphones) 66-Paging List 73-Custom Key (only appear when "features.enhanced_dss_keys.enable = 1") 104-Google Contacts (only appear when "google_contact_server.enable = 1") 150-Extend (only applicable to T54W/T53W/T53/T53C/T46U/T46S/T43U/T42S/T42U/T41S/T27G phones) 308-Dial (only applicable to CP925/CP935W) 309-Bluetooth (only applicable to CP925/CP935W) 310-DECT Intercom (only applicable to T57W/T54W/T53W/T53/T53C phones when the DECT USB dongle is connected) NOTE The permitted values are configurable by "programablekey.type_range.custom". The CP925/CP935W phones only support the following types: N/A (0), XML Browser (27), Dial (308), Bluetooth (309), History (28), Directory (29), Status (33).	X=14, default: 2-Forward X=17, default: 0 – NA X=18, default: 0 – NA X=19, default: 62 – Emergency call

programablekey.X.history_type[1]	It configures the history type of programmable key.	0-Local History 1-Network CallLog (only appear when "bw.enable=1" and "bw.xsi.call_log.enable=1")	0
programablekey.X.line[1]	It configures the desired line to apply the programmable key feature.	T57W/T54W/T48U/T48S/T48G/T46U/T46S/T46G/T29G: 0, 1-16; T53W/T53/T53C/T43U/T42U/T42S/T42G: 0, 1-12; T41P/T41S/T27G: 0, 1-6; T33P/T33G: 0, 1-4; T40P/T40G/T23P/T23G: 0, 1-3; T31P/T31G/T31/T21 § E2: 0, 1-2; CP920: 1, 101, 102. 0-All (it is configurable only when "features.fwd_mode" is set to 1 (Custom) and "programablekey.X.type" is set to 2 (Forward)); Auto (it is configurable only when "linekey.X.type" is set to 13 (SpeedDial) or 14 (Intercom). 1-Line 1 2-Line 2 … 16-Line 16 101-PSTN1 102-PSTN2 NOTE features.fwd_mode = 1 & programablekey.X.type =2 & programablekey.X.line =0: it means forward will	1

		apply to all lines on the phone; programablekey.X.type = 13 & programablekey.X.line =0: it means the phone can automatically switch accounts for speed dial; programablekey.X.type = 14 & programablekey.X.line =0: it means the phone can automatically switch accounts for intercom.	
programablekey.X.value[1]	It configures the value for some programmable key features. For example, when you assign the Speed Dial to the programmable key, this parameter is used to specify the contact number you want to dial out. It is also used to specify the contact number with the DTMF sequence. The contact number and DTMF sequence are separated by commas.	String within 99 characters	Blank
programablekey.X.label[1]	It configures the label displayed on the phone screen for a specific programmable key.	String within 99 characters	Blank

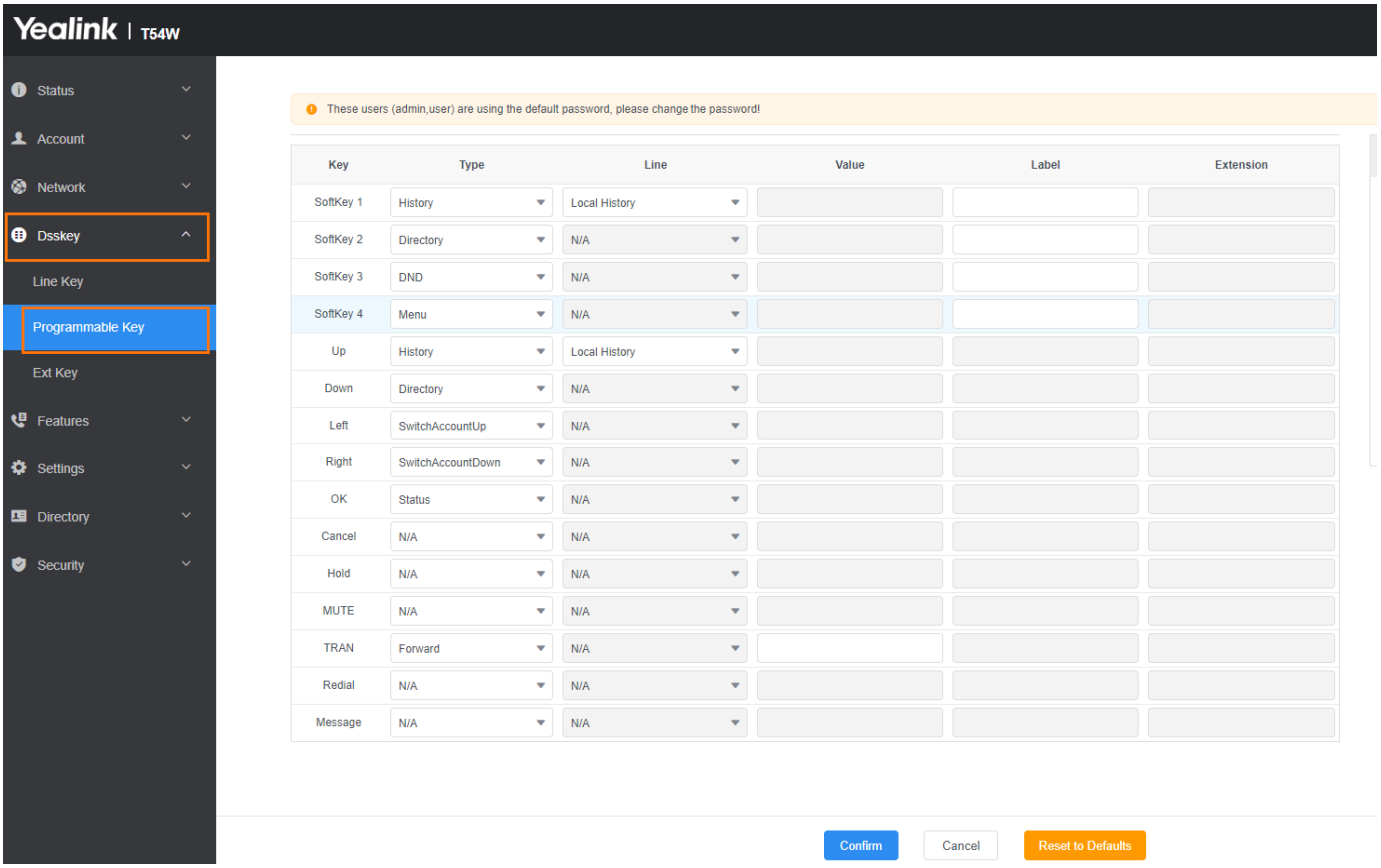
	This is an optional configuration.		
programablekey.X.extension[1]	For multicast paging: It configures the channel of the multicast paging group. For intercom feature: It configures the pickup code. NOTE It is only applicable when "programablekey.X.type" is set to 13, 14 or 24.	For multicast paging: 0 to 31 For intercom feature: String within 256 characters	0
programablekey.X.xml_phonebook[1]	It specifies a specific group/phone book when multiple groups/phone books are configured on the IP phone. For, example, both Remote Phone Book 1 "Sell" and Remote Phone Book 2 "Market" are configured on the phone, you can configure "programablekey.X.xml_phonebook = 0" to sp ecify the Remote Phone Book 1 "Sell" for the specific programmable key. The user can press this line key to access the Remote Phone Book 1 "Sell". NOTE It is only applicable	Integer from 0 to 48	0

	when “programablekey.X.type” is set to 22 or 45.		

> [1]X is the programmable key ID. For T57W/T77U, X=1-4, 12-14, 17-18; For T54W/T48U/T48S/T48G/T46U/T46S/T46G//T73U/T73W/T74U/T74W/T85W, X=1-10, 12-14, 17-18; For T53W/T53/T53C/T43U/T42U/T42G/T42S/T41P/T41S/T40P/T40G/T33P/T33G, X=1-10, 13, 17-18; for T29G/T27G, X=1-14, 17-18; for T23P/T23G/T21 E2, X=1-10, 14, 17-18; for T31P/T31G/T31/T30P/T30/T19 E2/T19P E2, X=1-9, 13, 14, 17-18; for CP920: X=1-6, 9, 13; for CP925/CP935W: X=1-4; For T85W/T87W/T88W, X=1-4, 12-14, 17-19.

Set via the Web User Interface

On the web user interface, go to: **Dsskey** > **Programmable Key**.



Ext Keys

The ext keys take effect only if the expansion module is connected to the IP phone.

It is only applicable to T57W/T54W/T53W/T53/T53C/T48U/T48S/T48G/T46U/T46S/T46G/T43U/T29G/T27G/T56A/T58A/T58V/T58W/VP59/T73U/T73W/T74U/T74W/T77U/T85W/T87W/T88W(Pro)/T88V Pro phones.

Ext Keys Configuration

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

Configuration parameter

expkey.type_range.custom
expansion_module.X.key.Y.type
expansion_module.X.key.Y.line
expansion_module.X.key.Y.value
expansion_module.X.key.Y.label
expansion_module.X.key.Y.extension
expansion_module.X.key.Y.xml_phonebook
expansion_module.display_order.type

Parameter	Description	Permitted Values	Default
expkey.type_range.custom	It configures the list for available ext key types list when configuring ext keys. To assign function types, specify ext key type IDs which start with or without a symbol ”+”. For example, “+2,15,16,7,4” or “2,15,16,7,4” means only “N/A”, “Forward”, “Line”, “BLF”, “Recall”, “Hold” types are available when you configure ext keys. To remove a function type, specify ext key type IDs which start with the symbol “-”. For example, “-14, 5, 2” means to remove “Intercom”, “DND”, “Forward” types from the ext key types list. These ext key types are not available when you configure ext keys. NOTE Multiple ext key type IDs are	Blank or 0 (all valid function types are available); Dsskey type IDs. For supported Dsskey types and IDs, refer to Supported Dsskey Types.	Blank

	separated by commas. N/A type is always kept.		
expansion_module.X.key.Y.type[1]	It configures the feature for a specific ext key.	0-N/A 1-Conference 2-Forward 3-Transfer 4-Hold 5-DND 7-Recall 8-SMS 9-Direct Pickup 10-Call Park 11-DTMF 12-Voice Mail 13-Speed Dial 14-Intercom 15-Line 16-BLF 17-URL 18-Group Listening 20-Private Hold 22-XML Group 23-Group Pickup 24-Multicast Paging (Paging) 25-Record 27-XML Browser 34-Hot Desking 35-URL Record 37-Switch (only applicable to ext key 1 for T29G/	Y=1-40 or 1-60, default: 0 – NA Y=1 or 21, default: 37 – Switch, only for T29G/T27G Y=2-20, 22-40, default: 0 – NA, only for T29G/T27G

		T27G phones) 38-LDAP (only appears when "ldap.enable=1") 39-BLF List 40-Prefix 41-Zero Touch 42-ACD 45-Local Group 50-Phone Lock 56-Retrieve Park 61-Directory 66-Paging List 73-Custom Key (only available when "features.enhanced_dss_keys.enable=1") 77-Mobile Account (only available to T57W/T54W/T53W/T53/T53C/T48U/T46U/T43U/Video phones when the Bluetooth-enabled mobile phone is connected) 104-Google Contacts (only appear when "google_contact	

		_server.enable = 1”) 105-XML Park 310-DECT Intercom (only applicable to T57W/T54W/ T53W/T53/T53/ Video phones when the DECT USB dongle is connected) NOTE The permitted values are configurable by “expkey.type_range.custom” .	
expansion_module.X.key.Y.line[1]	It configures the desired line to apply the ext key feature.	T57W/T54W/ T48U/T48S/ T48G/T46U/ T46S/T46G/ T29G: 0, 1-16; T53W/T53/T53C/ T43U: 0, 1-12; T27G: 0, 1-6; NOTE The permitted value	1

		0 is configurable only when "features.fwd_mode" is set to 1 (Custom) and "expansion_module.X.key.Y.type" is set to 2 (Forward).	
expansion_module.X.key.Y.value[1]	It configures the value for some ext key features. For example, when you assign the Speed Dial to the ext key, this parameter is used to specify the contact number you want to dial out. It is also used to specify the contact number with the DTMF sequence. The contact number and DTMF sequence are separated by commas.	String within 99 characters	Blank
expansion_module.X.key.Y.label[1]	It configures the label displayed on the LCD screen for a specific programmable key. This is an optional configuration.	String within 99 characters	Blank
expansion_module.X.key.Y.extension[1	For multicast paging: It configures the channel of the	For multicast paging:	0

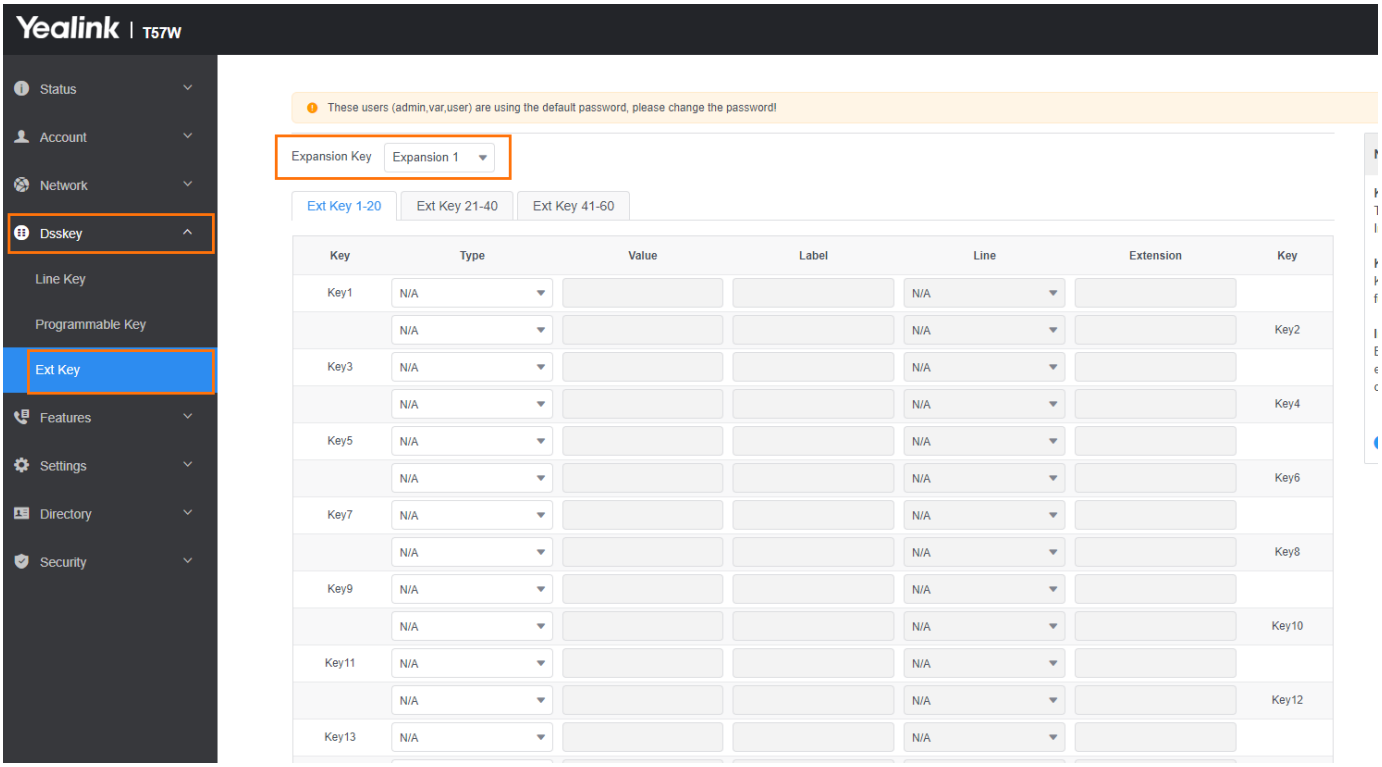
]	multicast paging group. For the BLF/BLF list/intercom feature: It configures the pickup code. NOTE It is only applicable when "expansion_module.X.key.Y.type" is set to 14, 16, 24 or 39.	0 to 31 For the BLF/BLF list/intercom feature: String within 256 characters	
expansion_module.X.key.Y.xml_phonebook[1]	It specifies a specific group/phone book when multiple groups/phone books are configured on the phone. For example, both Remote Phone Book 1 "Sell" and Remote Phone Book 2 "Market" are configured on the phone, you can configure "expansion_module.X.key.Y.xml_phonebook = 0" to specify the Remote Phone Book 1 "Sell" for the specific ext key. The user can press this line key to access the Remote Phone Book 1 "Sell". NOTE It is only applicable when "expansion_module.X.key.Y.type" is set to 22 or 45.	Integer from 0 to 48	0
expansion_module.display_order.type	It configtures the order of ext key. NOTE It is only applicable when "expansion_module.X.key.Y.type" is set to 22 or 45.	0-The first row displays ext key in the order of No.1, No.2 from left to right, the second row displays ext key in the order of No.3, No.4 ext	0

		key from left to right, and so on. 1-The first column displays ext key in the order of No.1, No.2, ··· No.N , and the second column displays the ext key in the order of No.(N+1), No.(N+2), …	

> [1]X is the expansion module ID, Y is the EXT key ID. For T57W/T54W/T53W/T53/T53C/T48U/T46U/T43U, X=1-3, Y=1-60; For T48S/T48G/T46S/T46G, X=1-6, Y=1-40; for T29G/T27G, X=1-6, Y=1-20, 22-40.

Set via the Web User Interface

On the web user interface, go to: **Dsskey** > **Ext Key**



Dsskey Lock Configuration

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

Configuration parameter

custom.features.dsskey_lock_type
custom.features.dsskey_unlock_password

Parameter	Description	Permitted Values	Default	Supported Devices
custom.features.dsskey_lock_type	It configures which types of dsskeys to be locked on the phone. Multiple dsskey type IDs are separated by commas.	Blank (all valid function types are not locked); dsskey type IDs. For supported dsskey types and IDs, refer to Supported Dsskey Types.	Blank	All phones except T48G, T46G, T42G, T41P and T29G
custom.features.dsskey_unlock_password	It configures the password for unlocking the phone's dsskeys. If it is set to a value, the phone prompts users to enter the password when using the corresponding dsskey configured by "custom.features.dsskey_lock_type".	String within 32 characters	Blank (no prompt for entering the unlock password)	All phones except T48G, T46G, T42G, T41P and T29G

Dsskey Page Reset Configuration

The following table lists the parameter you can use to configure reset dsskey page.

Configuration parameter

features.dsskey_page_reset.call_established.enable
features.dsskey_page_reset.call_established.page
features.dsskey_page_reset.enable
features.dsskey_page_reset.page

Parameter	Description	Permitted Values	Defaul	Supported Devices

			t	
features.dsskey_page_reset.call_established.enable	It enables or disables the phone to automatically switch to a specified dsskey page when a call is established.	0-Disabled 1-Enabled	0	T54W, T53W, T53, T53C, T46U, T46S, T43U, T42S, T42U, T41S, T33P, T33G, T27G
features.dsskey_page_reset.call_established.page	It controls which dsskey page the phone automatically switches to when a call is established. Note: It works only if "features.dsskey_page_reset.call_established.enable" is set to 1 (Enabled).	Integer from 1 to 3 (4 for T3 phones)	1	T54W, T53W, T53, T53C, T46U, T46S, T43U, T42S, T42U, T41S, T33P, T33G, T27G
features.dsskey_page_reset.enable	It enables or disables the phone to automatically switch to a specified dsskey page when all calls end.	0-Disabled 1-Enabled	0	T54W, T53W, T53, T53C, T46U, T46S, T43U, T42S, T42U, T41S, T33P, T33G, T27G
features.dsskey_page_reset.page	It controls which dsskey page the phone automatically switches to when all calls end. Note: It works only if "features.dsskey_page_reset.enable" is set to 1 (Enabled).	Integer from 1 to 3 (4 for T3 phones)	1	T54W, T53W, T53, T53C, T46U, T46S, T43U, T42S, T42U, T41S, T33P, T33G, T27G

Enhanced DSS Keys

Enhanced DSS Keys

Enhanced DSS Keys (EDK) enable users to customize the functions of the phone’s DSS keys.

With EDK, you can do the following:

- Assign a frequently-used function to DSS keys.
- Create menu shortcuts for frequently-used phone settings as needed.
- Use EDK macro strings as the contact number.

Application scenarios involve the following:

- Adding new DSS keys to simplify the operation of common telephony tasks that may need more than one keypress with the default configuration.
- Removing certain default DSS keys for the functions that may be redundant or never used.
- One-touch connecting to the contact's extension number without entering DTMF manually.

The rules for configuring EDK for DSS keys are different. Before using EDK, you are advised to become familiar with the macro language.

For more information on Enhanced DSS Keys, refer to Using Enhanced DSS Keys on Yealink IP Phones.

Guidelines for Configuring Enhanced DSS Keys

The following guidelines will help you to configure EDK efficiently:

- Activation of EDK functions requires valid macro construction.
- Character “$” delimits the parts of the macro string (except the digits only), and it must exist in pairs. For more information, refer to Macro Action Strings.
- Macros can be invoked in the format “!<macro name>”, where <macro name > is defined by the parameter “edk.edklist.X.mname”.
- If there are two or more same macros, the soft key or DSS key will invoke the macro with the smallest value of X defined by the parameter “edk.edklist.X.mname”.

Macro Action Strings

Before using EDK, you must be familiar with the macro language shown in this section.

The following table shows the basic macro action string syntax when creating EDK macros:

Macro Action	Description
Digits	The characters to be sent. The following characters are supported: . @ * # +

	0-9 and English letters. The appearance of this parameter depends on the action string. Example: *981135.
$C<command>$	This is the command. It can appear anywhere in the action string. Supported commands (or shortcuts) include: hang up (hu) hold (h) waitconnect (wc) pause <number of seconds> (p <num sec>) where the maximum value is 10 Example: 4411$Cwc$$Cp10$ defines dialing 4411 > > waitconnect > > connected and lasts 10 seconds.
$T<type>$	The embedded action type. Multiple actions can be defined. Supported action types include: invite dtmf refer intercom Example: *338$Tdtmf$ defines sending the *338 by the type of DTMF. We recommend that you always define this field. If not, the supplied digits are dialed using INVITE.
$M<macro>$	The embedded macro. The <macro > string must begin with a letter. If the macro name is not defined, the execution of the action string will be ignored. Example: MAA means invoking the EDK macro AA.
$S<softkey ID>$	It has the same effect as pressing the desired soft key. Each soft key has a unique identifier on the IP phone, you can configure this parameter according to the system-defined softkey ID. If the softkey ID is not defined on the phone or there is no matched soft key on the current screen, the execution of the action string will be ignored. The softkey ID is case-insensitive. Example: $Sanswer$ means pressing the Answer soft key. Yealink phones support customizing soft keys. When the phone invokes a custom soft key, the prefix “#” must be added. Example: If the custom softkey label is IVR1, the custom softkey ID is

	custom_macro, then $S#custom_macro$ means pressing the IVR1 soft key. To view the softkey ID, you can set "features.enhanced_dss_keys.enable" and "edk.id_mode.enable" to 1 (Enabled) and then long-press the Volume Up key when the phone is idle.
$K<key name>$	The functionality of performing this action is the same as that of pressing the desired hard key. Supported key names include: LineKeyX SoftKeyX (X ranges from 1 to 4) ArrowUp (not applicable to T57W) ArrowDown (not applicable to T57W) ArrowLeft (not applicable to T57W) ArrowRight (not applicable to T57W) VolDown VolUp Cancel (not applicable to T57W) OK (not applicable to T57W) DialPadX (X ranges from 0 to 9) DialPadPound DialPadStar Headset Mute Message Hold Redial Transfer Speaker Conference ExtX@Y (X stands for the serial number of the expansion module key, Y stands for the serial number of the expansion module.) Menu (You can enter the menu by executing this command at any interface except the non-executable situations. For example, entering the menu is

	blocked during an active call.) Home (You can return to the idle screen by executing this command on the dialing screen for T57W/T48U/T48S/T48G phones) Example: $KDialPadPound$ means pressing the pound key. If a key (for example, Redial key) is not found but the function is available, the phone will perform the corresponding action. If a key is not found and the function is unavailable, the execution of the action string will be ignored.
$I<menu item ID>$	The action is to position and enter the desired menu item. Each menu item has a unique identifier on the IP phone, and you can configure this parameter according to the system-defined menu item ID. If the menu item ID is not defined on the phone or there is no matched menu item on the current screen, the execution of the action string will be ignored. The menu item ID is case-insensitive. Example: $Istatus_list& means entering the Status menu. To view the menu item ID, you can set "edk.id_mode.enable" to 1 (Enabled) and then long press the Volume Up key when the phone is idle.
$P<label>&T<title>&C<characters number allowed>&N&M$	The string of the user input prompt. "label" means the specified label for the user input prompt. "title" means the specified title for the user input prompt. "characters number allowed" defines the maximum number of input characters. If &N is included, the character type is Number (default input method: 123). If &N is not included, the character type is Text (default input method: abc), you can manually change the input method. (For T57W/T48U/T48S/T48G, if &N is included, the input mode is numeric & symbolic. If &N is not included, the onscreen keyboard is displayed, and you can manually change the input mode.) If &M is included, the inputs are masked by the asterisk characters "*" *(dot for T57W/T48U/T48S/T48G).* *Example: PPassword&C3&N&M means prompting a Password pop-up box, the maximum number of input characters is 3, the input type is Number, and the input is masked by the asterisk characters "*"* (dot for T57W/

	T48U/T48S/T48G). &T<title> is not applicable to T57W/T48U/T48S/T48G/T46G/T42G/T41P/T29G phones.
$P<EDK user input prompt X>N<characters number allowed>$	The user input prompt string. "EDK user input prompt X" means which EDK user input prompt is invoked. It indicates the X defined by "edk.edkprompt.X.enable". "characters number allowed" defines the maximum number of input characters. You need to press the Enter soft key to complete data entry. Example: $P2N5$ means invoking the EDK user input prompt 2 and inputting 5 characters at most. For more information on the EDK user input prompt, refer to EDK User Input Prompt Configuration.
$L<label>$	This is the label for the entire operation. The value can be any string, including the null string (in this case, no label displays). This label is used if no label is configured for a custom DSS key or soft key, otherwise, this one is ignored. Make this the first entry in the action string. Example: $LEDK2$1234$Tinvite$ defines calling out the number 1234 and using the label “EDK2” for a Custom Key.
$LED<color and time>&L<label>$ (not applicable to T30P/T30/T19 § E2/CP920 phones)	The status of the BLF/BLF list DSS key LED. Specify the LED color for the BLF/BLF list DSS key and the duration time (in milliseconds) for the corresponding status of the BLF/BLF list DSS key. The valid value of the duration ranges from 100 to 60000ms. Can be composed of multiple combinations of “color” and “time”. The status will be stuck in an infinite loop until triggered by other macros. Supported colors include (must be lowercase): r (red) ri (red; red with an incoming mark for T57W/T48U/T48S/T48G) ro (red; red with an outgoing mark for T57W/T48U/T48S/T48G) rd (red; red with a DND mark for T57W/T48U/T48S) g (green) gi (green; green with an incoming mark for T57W/T48U/T48S/T48G) go (green; green with an outgoing mark for T57W/T48U/T48S/T48G) y (yellow)

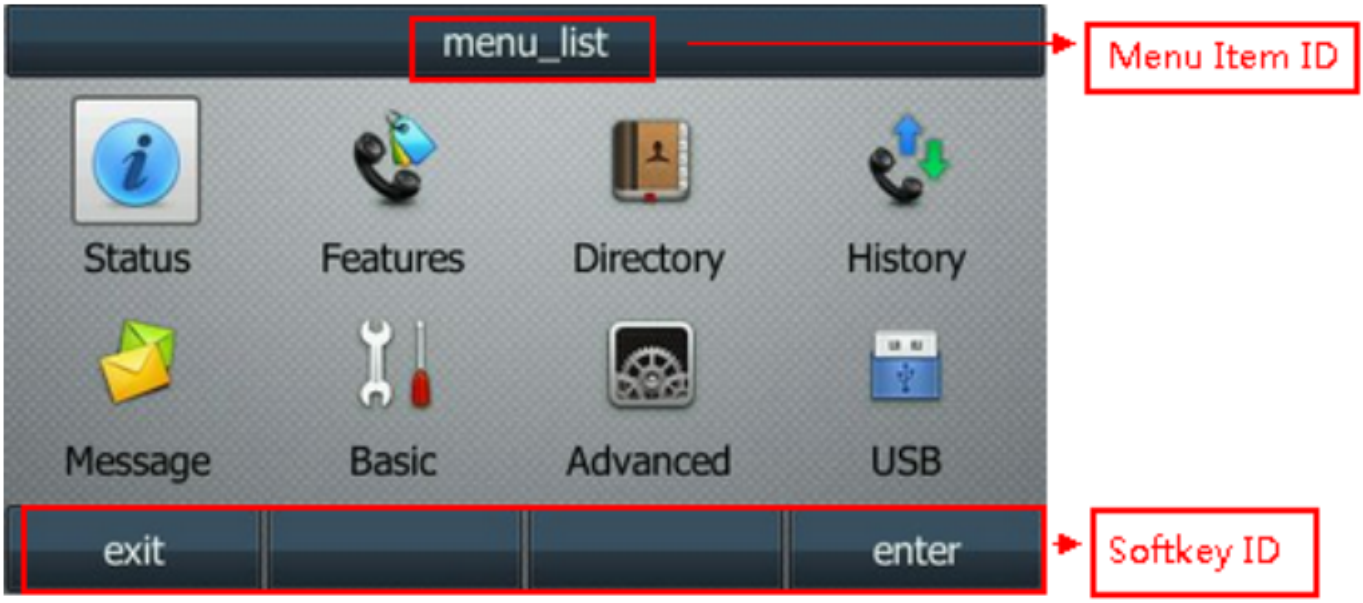
	yi (yellow; yellow with an incoming mark for T57W/T48U/T48S/T48G) yo (yellow; yellow with outgoing mark for T57W/T48U/T48S/T48G) yd (yellow; yellow with a DND mark for T57W/T48U/T48S) o (off) &L<label> (Optional.): You have to put the “&L<label>” last in the command flow. Example: $LEDg1000o100r300&Lidle$ means an infinite loop for BLF/BLF list DSS key LED status: glow green for 1000ms, be in the off state for 100ms, and then glow red for 300ms. At the same time, the label of the BLF/BLF list DSS key is changed to “idle”. The last “color” can be configured without “time”, and it means permanently displaying the last color until triggered by other macros. This macro can only be used for the BLF/BLF list feature. For more information, refer to BLF/BLF List Key LED Status and Behavior Configuration.
$XML<xml browser url>$	The action is to execute the XML browser URL. Example: "$XMLhttp://10.83.3.12/XML/PhoneExecute.xml$" defines executing the XML browser URL "http://10.83.3.12/XML/PhoneExecute.xml". For more information on the XML browser, refer to XML Browser.

EDK Configuration

To configure the EDK list, EDK user input prompt, EDK soft keys, and custom DSS keys, you have to enable EDK feature. By default, the EDK feature is disabled.

Yealink phones can display the softkey ID or menu item ID by long pressing the Volume Up key. It is especially useful for those users who need to view the softkey ID or menu item ID when configuring EDK macros.

The following graphic shows an example of displaying the softkey ID and menu item ID after accessing the menu of T46S/G phones:



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

Configuration parameter

features.enhanced_dss_keys.enable
edk.id_mode.enable

Parameter	Description	Permitted Values	Default
features.enhanced_dss_keys.enable	It enables or disables the Enhanced DSS Keys (EDK) feature.	0-Disabled 1-Enabled	0
edk.id_mode.enable	It enables or disables viewing the softkey or menu item ID by long pressing the Volume Up key for three seconds on any screen. • The menu item ID is displayed on the status bar of the phone. • Long-press the Volume Up key again for three seconds to exit. • It works only if "features.enhanced_dss_keys.enable" is set to 1 (Enabled).	0-Disabled 1-Enabled	0

EDK List Configuration

Using the Enhanced DSS Keys (EDK) List parameters to define a macro is useful when defining more than one soft key or DSS key.

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

Configuration parameter

```
edk.edklist.X.enable
edk.edklist.X.mname
edk.edklist.X.action
```

Parameter	Description	Permitted Values	Default
edk.edklist.X.enable[1]	It enables or disables Enhanced DSS Keys (EDK) macro X. It works only if "features.enhanced_dss_keys.enable" is set to 1 (Enabled).	0-Disabled 1-Enabled	0
edk.edklist.X.mname[1]	It configures the unique identifier used by the soft key or DSS key configuration to reference the enhanced DSS keys entry for macro X. It cannot start with a digit. This parameter must have a value, it cannot be left blank. Example: edk.edklist.2.mname = macro2 • If there are two or more same macros, the soft key or DSS key will invoke the macro with the smallest value of X. • It works only if "features.enhanced_dss_keys.enable" is set to 1 (Enabled).	String	Blank
edk.edklist.X.action[1]	It configures the action string that contains a macro definition of the action that the softkey or DSS key performs.	String	Blank

	Example: edk.edklist.2.action = 1013$Tinvite$ • This parameter must have a value, it cannot be left blank. • It works only if "features.enhanced_dss_keys.enable" is set to 1 (Enabled).		

[1]X is the macro ID. X=1-255.

EDK User Input Prompt Configuration

The EDK user input prompt parameters must be used if interactivity with the user is implemented as part of any macro.

The following table lists the parameters you can use to configure the EDK user input prompt.

Configuration parameter

edk.edkprompt.X.enable
edk.edkprompt.X.label
edk.edkprompt.X.type
edk.edkprompt.X.userfeedback
edk.edkprompt.X.title

Parameter	Description	Permitted Values	Default
edk.edkprompt.X.enable[1]	It enables or disables user input prompt X. • If a macro attempts to use an EDK user input prompt that is disabled, the macro execution fails. • It works only if "features.enhanced_dss_keys.enable" is set to 1 (Enabled).	0-Disabled 1-Enabled	0
edk.edkprompt.X.label[1]	It configures the text string used as a label of the user input prompt X. If it is left blank, the Default is displayed.	String	Default

	Example: edk.edkprompt.1.label = Enter Password It works only if "features.enhanced_dss_keys.enable" and "edk.edkprompt.X.enable" are set to 1 (Enabled).		
edk.edkprompt.X.type[1]	It configures the type of characters entered by the user for user input prompt X. • If it is set to numeric, the default input method is 123, and you can switch among abc/ABC/2aB input methods. • If it is set to text, the default input method is abc, and you can switch among ABC/2aB/123 input methods. It works only if "features.enhanced_dss_keys.enable" and "edk.edkprompt.X.enable" are set to 1 (Enabled).	text or numeric	text
edk.edkprompt.X.userfeedback[1]	It configures the user input feedback method for user input prompt X. It works only if "features.enhanced_dss_keys.enable" and "edk.edkprompt.X.enable" are set to 1 (Enabled).	visible-the entered text is visible. masked-the entered text is displayed as asterisk characters “*” . It can be used to mask password fields.	visible
edk.edkprompt.X.title[1]	It configures the text string used as a title for the user input prompt X. The title appears at the top of the user input prompt screen.	String	EDK Prompt

	If it is left blank, the EDK Prompt is displayed. It works only if "features.enhanced_dss_keys.enable" and "edk.edkprompt.X.enable" are set to 1 (Enabled).		

> [1]X is the prompt ID. X=1-10.

EDK Soft Keys Configuration

You can customize the soft keys as needed. This feature is typically used to access frequently-used functions or to create menu shortcuts to frequently-used phone settings.

- Custom soft keys can be added in the following phone states:
- **Idle** - There are no active calls on the phone.
- **Alerting (or ringing)** – There is an incoming call on the phone.
- **Connecting** – There is an outgoing call on the phone. Moreover, the call is connecting.
- **Transfer connecting** – There is a call being transferred to another phone. Moreover, the call is connecting.
- **Talk** – There is an active call on the phone.
- **Call failed** – The outgoing call encounters a failure.
- **Ring back** - There is an outgoing call on the phone. Moreover, the phone is in the ringback state.
- **Transfer ring back** - There is a call being transferred to another phone. Moreover, the phone is in the ringback state.
- **Hold** – The call is placed on hold on the phone.
- **Held** – The call is held.
- **Conference** – The phone sets up a conference call.
- **Dial tone** –The phone is on the dialing screen without entering the number.
- **Dialing** – The phone is on the dialing screen, with the number, but not dialing.

> Configuring the custom soft keys may affect the softkey layout in different call states. For more information on softkey layout, refer to Softkey Layout.

The following table lists the parameters you can use to configure EDK soft keys.

Configuration parameter

softkey.X.enable

softkey.X.label
softkey.X.position
softkey.X.action
softkey.X.softkey_id
softkey.X.use.idle
softkey.X.use.incoming_call
softkey.X.use.connecting
softkey.X.use.transfer_connecting
softkey.X.use.on_talk
softkey.X.use.call_failed
softkey.X.use.ring_back
softkey.X.use.transfer_ring_back
softkey.X.use.hold
softkey.X.use.held
softkey.X.use.conferenced
softkey.X.use.dialtone
softkey.X.use.dialing

Parameter	Description	Permitted Values	Default
softkey.X.enable[1]	It enables or disables the custom soft key X. It works only if "**features.enhanced_dss_keys.enable"** is set to 1 (Enabled).	0-Disabled 1-Enabled	0
softkey.X.label[1][2]	It configures the text displayed on the soft key label.	String	Blank
softkey.X.position[1][2]	It configures the location on the phone screen for soft key X.	Integer from 0 to 10 If it is set to 0, the soft key X is located in the first available position from the left. If it is set to other values, a	0

		More soft key appears and the soft key X is located in the specified position. The following soft keys are moved by one position to the right. Press the More soft key to view the remaining soft keys.	
softkey.X.action[1][2]	It configures the action or function for custom soft key X. This value uses the same macro action string syntax as an Enhanced DSS key. You can also invoke the EDK macro that was already defined. The macro name follows the character “!”. Example: softkey.1.action = !macro1 In this example, macro1 stands for the macro name configured by the parameter “edk.edklist.X.mname”.	String	Blank
softkey.X.softkey_id[1][2]	It configures the softkey id for custom soft key X. Example: softkey.1.softkey_id = custom_macro1	String	Blank
softkey.X.use.idle[1][2]	It enables or disables the custom soft key X to be displayed in the idle state.	0-Disabled 1-Enabled	0
softkey.X.use.incoming_call[1][2]	It enables or disables the custom soft key X to be displayed in the alerting (ringing) state.	0-Disabled 1-Enabled	0
softkey.X.use.connecting[1][2]	It enables or disables the custom soft key X to be displayed in the connecting state.	0-Disabled 1-Enabled	0
softkey.X.use.transfer_connecting[1][2]	It enables or disables the custom soft key X to be displayed in the transfer connecting state.	0-Disabled 1-Enabled	0

softkey.X.use.on_talk[1][2]	It enables or disables the custom soft key X to be displayed in the talking state.	0-Disabled 1-Enabled	0
softkey.X.use.call_failed[1][2]	It enables or disables the custom soft key X to be displayed in the call failed state.	0-Disabled 1-Enabled	0
softkey.X.use.ring_back[1][2]	It enables or disables the custom soft key X to be displayed in the ringback state.	0-Disabled 1-Enabled	0
softkey.X.use.transfer_ring_back[1][2]	It enables or disables the custom soft key X to be displayed in the transfer ring back state.	0-Disabled 1-Enabled	0
softkey.X.use.hold[1][2]	It enables or disables the custom soft key X to be displayed in the hold state.	0-Disabled 1-Enabled	0
softkey.X.use.held[1][2]	It enables or disables the custom soft key X to be displayed in the held state.	0-Disabled 1-Enabled	0
softkey.X.use.conferenced[1][2]	It enables or disables the custom soft key X to be displayed in the conference state.	0-Disabled 1-Enabled	0
softkey.X.use.dial tone[1][2]	It enables or disables the custom soft key X to be displayed in the dial tone (no numbers entered) state.	0-Disabled 1-Enabled	0
softkey.X.use.dialing[1][2]	It enables or disables the custom soft key X to be displayed in the dialing state.	-Disabled 1-Enabled	0

> [1]X is the soft key ID. X=1-10.
> [2]NOTE：It works only if "features.enhanced_dss_keys.enable" and "softkey.X.enable" are set to 1 (Enabled).

Example: Configuring EDK List for a Line Key

The following takes an example to help you understand how to execute the macro action string.

Example

```
features.enhanced_dss_keys.enable = 1
```

```
edk.edklist.1.enable = 1
edk.edklist.1.mname = IVR1
edk.edklist.1.action = 1013$Tinvite$$Cwc$$Cp10$$Penter number&C4&N$$Tdtmf$
$Cp3$$Chu$
linekey.1.type = 73
linekey.1.value = !IVR1
linekey.1.label = Custom
```

After provisioning, the line key 1 will invoke the macro "IVR1". You can press the line key 1 to execute the action "1013$Tinvite$$Cwc$$Cp10$$Penter number&C4&N$$Tdtmf$$Cp3$$Chu$".

You can also set "linekey.1.value = 1013$Tinvite$$Cwc$$Cp10$$Penter number&C4&N$$Tdtmf$ $Cp3$$Chu$" without configuring an EDK list. You can also manually assign a line key using the macro "IVR1" or action string "1013$Tinvite$$Cwc$$Cp10$$Penter number&C4&N$$Tdtmf$$Cp3$ Chu" manually on their phone.

Example: Using EDK Macro Strings as the Contact Number

When you add a contact number in the local directory, LDAP, Remote phone book, or XML phone book, you can use the EDK macro strings.

Use one of the following formats when adding a contact number:

- Add an exclamation mark (!) prefix to the macro name, and then enclose it in parentheses. For example, (!macro1).
- EDK macro strings are enclosed in parentheses. For example, (8001234567Cwc $Cp2$103$Tdtmf$).

Example: Assume that a contact whose company phone number is 8001234567, and extension number is 103. If you want to call this contact directly, you can configure the contact number according to the following steps:

1. Configure the following parameters:

```
features.enhanced_dss_keys.enable = 1
☒ edk.edklist.1.enable = 1
☒ edk.edklist.1.mname = macro1
☒ edk.edklist.1.action = 8001234567$Cwc$$Cp2$103$Tdtmf$
```

2. Trigger the phone to perform auto provisioning.

3. On your phone, assign (!macro1) to be the contact number.

When you call this contact, the phone will invoke the macro "macro1". So that the phone will

execute the action “8001234567$Cwc$$Cp2$103$Tdtmf$”.

You can also assign (8001234567$Cwc$$Cp2$103$Tdtmf$) to be the contact number directly.

> 8001234567$Cwc$$Cp2$103$Tdtmf$ defines that the phone dials 8001234567 first, and sends DTMF sequence 103 automatically after the call is connected and lasts for 2 seconds.

Power Saving & Office Hours & Idle TimeOut

Power Saving

The power-saving feature turns off the backlight and screen (turning off the screen is only applicable to color screen phones and EXP50 (connected to the T57W/T54W/T53W/T53/T53C/Video phones)/ EXP43 (connected to the T48U/T46U/T43U phones) to conserve energy. The IP phone and EXP50/ EXP43 (if connected) enter power-saving mode after the phone has been idle for a certain period of time. And the IP phone and EXP50/EXP43 (if connected) will exit power-saving mode if a phone/ EXP50/EXP43 event occurs - for example, the phone receives an incoming call or a new message, or you press a key on the phone/EXP50/EXP43 or tap the touch screen (touch screen is only applicable to T57W/T48U/T48S/T48G phones). The power saving does not apply to T30P/T30/T19 E2/T19P E2 phones.

> If the **Screen Saver** is enabled on your phone, the power-saving mode will still occur. For example, suppose a screen saver is configured to display after the phone has been idle for 5 minutes, and the power-saving mode is configured to turn off the backlight and screen after the phone has been idle for 15 minutes. In that case, the backlight and screen will be turned off after the screen saver displays for 10 minutes.

Power Saving Configuration

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

- **Office Hour**: specify the start time and end time of the day’ s office hours. You can change the office hours to avoid affecting your work.
- **Maximum Power Saving Mode**: You can enable or disable the maximum power saving mode.
- **Idle Timeout**: specify the period of time before the IP phone enters the power-saving mode.
- **Intelligent Mode**: During work hours, the screen will automatically light up, unaffected by the phone's AutoP behavior or notifications.
- **Inactive Level**: In power-saving mode, the screen backlight can be set to dim or completely off.

You can specify the following three types of idle timeout:

- **Office Hours Idle TimeOut**: specify the idle timeout for office hours.
- **Off Hours Idle TimeOut**: specify the idle timeout for non-office hours.
- **User Input Extension Idle TimeOut**: specify the idle timeout that applies after you use the IP phone (for example, press a key on the phone or pick up/hang up the handset).

By default, the **Office Hours Idle Timeout** is much longer than the **Off Hours Idle TimeOut**. If you

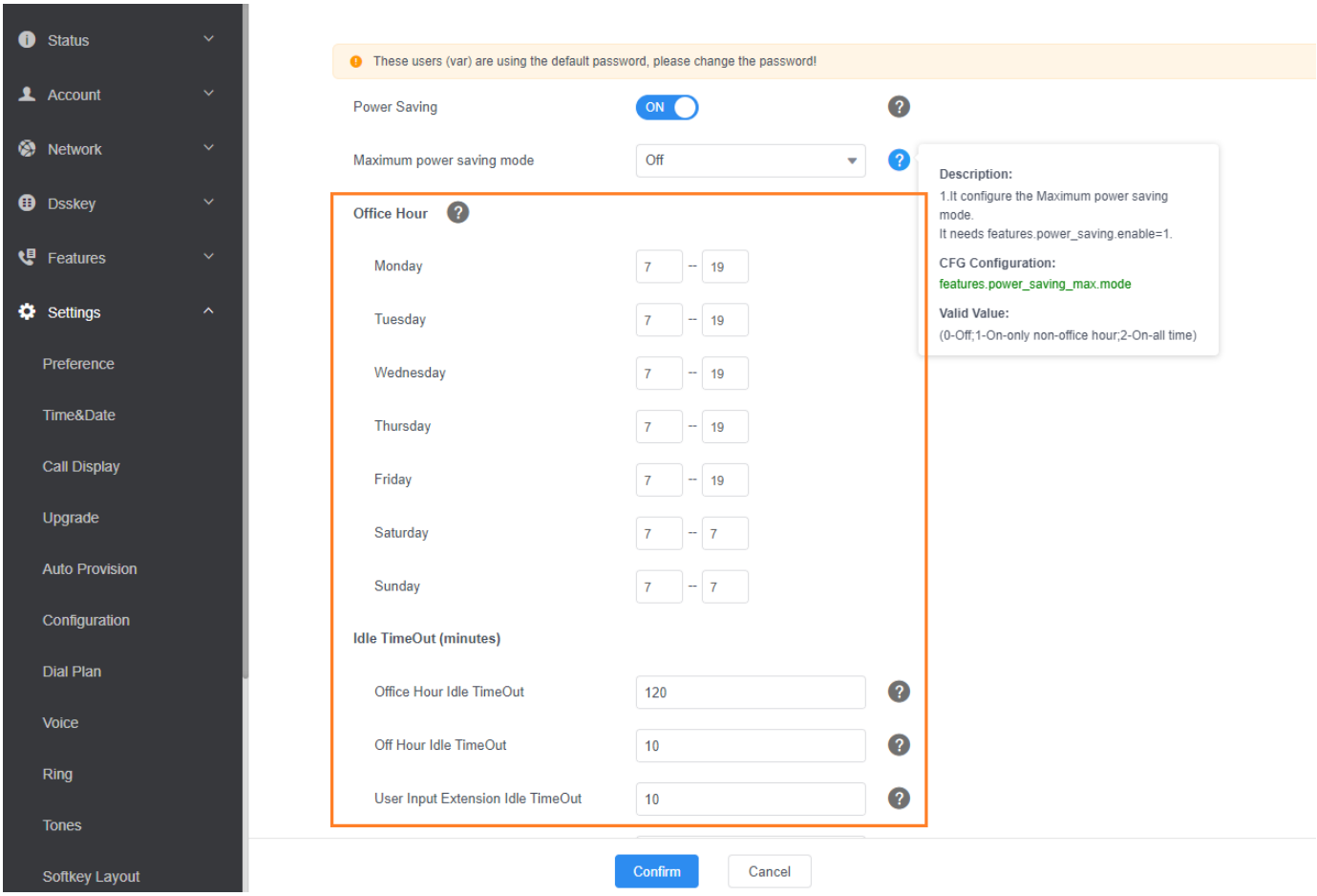
use the IP phone, the idle timeout that applies (**User Input Extension Idle Timeout** or **Office Hours/ Off Hours Idle TimeOut**) is the timeout with the highest value.

If the phone has an incoming call or new message, the User Input Extension Idle TimeOut is ignored.

You can choose to set a higher **User InputExtension Idle TimeOut** than the **Office Hours Idle TimeOut** and **Off Hours IdleTimeOut** so that the phone does not enter the power-saving mode too often after you use the phone.

Set via the Web User Interface

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



Configuration parameter

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

features.power_saving.intelligent_mode
features.power_saving.enable
features.power_saving.office_hour.idle_timeout
features.power_saving.off_hour.idle_timeout
features.power_saving.user_input_ext.idle_timeout
features.power_saving.office_hour.monday
features.power_saving.office_hour.tuesday

features.power_saving.office_hour.wednesday
features.power_saving.office_hour.thursday
features.power_saving.office_hour.friday
features.power_saving.office_hour.saturday
features.power_saving.office_hour.sunday
features.power_saving.power_led_flash.on_time
features.power_saving.power_led_flash.off_time

Parameter	Description	Permitted Values	Default
features.power_saving.intelligent_mode	It enables or disables the power-saving intelligent mode.	0-Disabled, the phone stays in power-saving mode even if the office hour arrives the next day. 1-Enabled, the phone automatically identifies the office hours and lights up the screen once the office hour arrives the next day. 3-In non-intelligent mode, the screen will not automatically light up during work hours and remains unaffected by the phone's AutoP behavior or notifications, such as registration updates, voice mail alerts, subscription updates, BLF/BLF list	1

		synchronization, and hotdesking logins or logouts.	
features.power_saving.enable	It enables or disables the power-saving feature.	0-Disabled, the phone automatically enters the power-saving mode to protect the screen when the phone is inactive for 72 hours. That is, the color-screen phones will turn off the backlight and screen, and the black-and-white screen phones will only turn off the backlight. LCD may cause image persistence. 1-Enabled	1
features.power_saving.office_hour.idle_timeout	It configures the time (in minutes) to wait in the idle state before the phone enters power-saving mode during office hours.	Integer from 1 to 960	30
features.power_saving.off_hour.idle_timeout	It configures the time (in minutes) to wait in the idle state before the phone enters power-saving mode during non-office hours.	Integer from 1 to 10	5
features.power_saving.user_input_ext.idle_timeout	It configures the minimum time (in minutes) to wait in the idle state after using the phone, before the phone enters the power-saving	Integer from 1 to 30	105

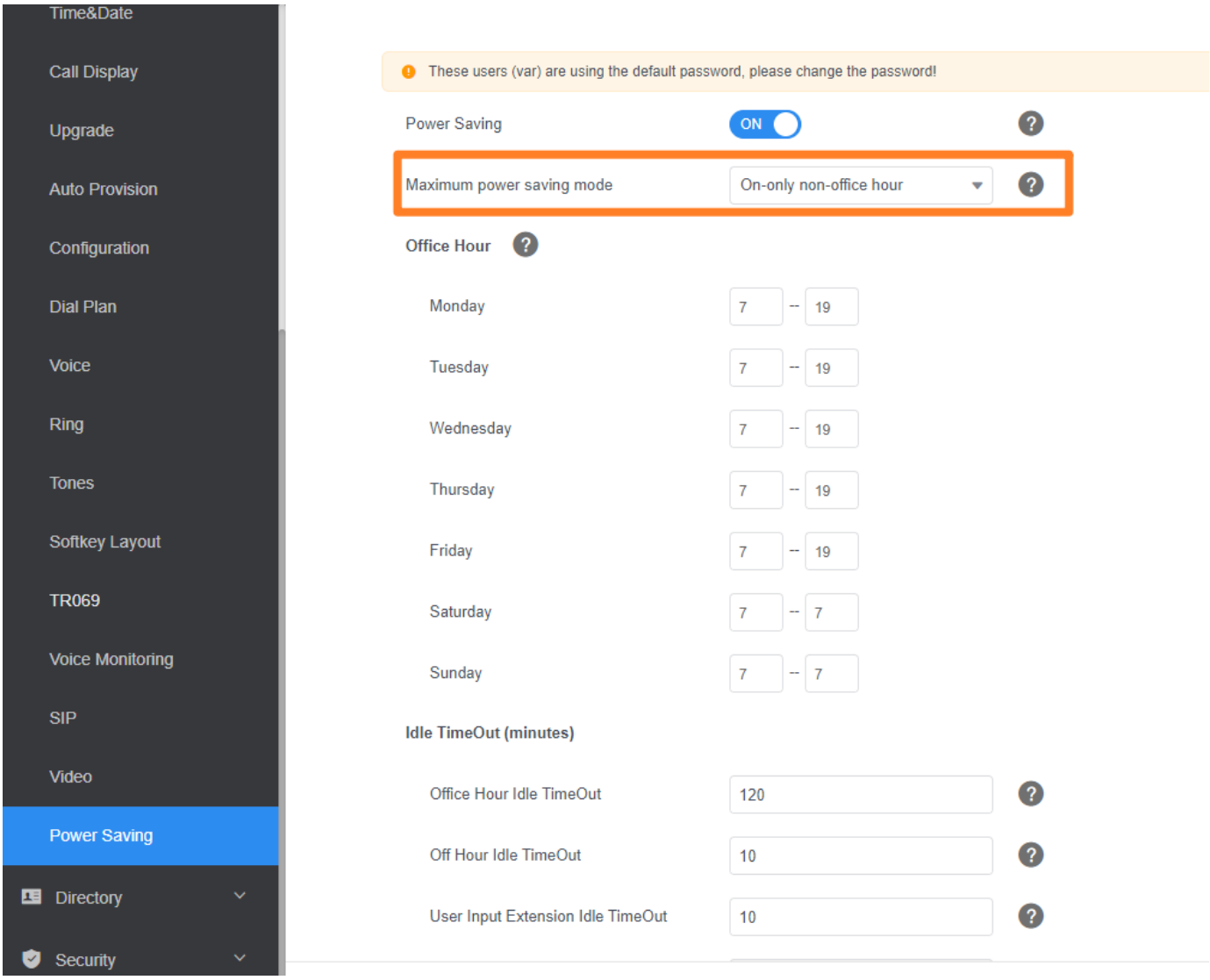
	mode.		
features.power_saving.office_hour.monday features.power_saving.office_hour.tuesday features.power_saving.office_hour.wednesday features.power_saving.office_hour.thursday features.power_saving.office_hour.friday features.power_saving.office_hour.saturday features.power_saving.office_hour.sunday	It configures the start time and end time of the day's office hours. Start time and end time are separated by a comma. Example: features.power_saving.office_hour.monday = 7,19	Integer from 0 to 23, Integer from 0 to 23	7,19 - for Monday, Tuesday, Wednesday, Thursday, Friday. 7,7 - for Saturday, Sunday.
features.power_saving.power_led_flash.on_time	It configures the period of time (in milliseconds) when the power LED indicator is on in the power-saving mode. If it is set to 0 and "features.power_saving.power_led_flash.off_time" is not set to 0, the power LED indicator will be off when the phone enters the power-saving mode.	0, Integer from 100 to 10000	500
features.power_saving.power_led_flash.off_time	It configures the period of time (in milliseconds) when the power LED indicator is off in the power-saving mode. If it is set to 0, the power LED indicator will be on when the phone enters the power-saving mode.	0, Integer from 100 to 10000	3000

Maximum Power Saving Mode

The V87 version has a new feature - **Maximum Power Saving Mode**, reducing the power consumption of the phone. The phone will automatically enter sleep mode after 15 seconds of inactivity, and the screen brightness will be reduced accordingly.

Set via the Web User Interface

On the web user interface, go to: **Settings** > **Power Saving** > **Maximum power saving mode**.



Configuration parameter

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

features.power_saving_max.mode

Parameter	Description	Permitted Values	Default
features.power_saving_max.mode	Enable or disable the maximum power saving mode. Only applicable when	0-Off 1-On-only non-office hour	0

	"features.power_saving.enable"=1.	2-On-all time	

Icon & Warning Setting

Icon Customization

You can upload custom DSS keys icons and menu icons to the phone. Contact Yealink FAE to obtain the Icon Templates Pack. Make sure that the name, size, and format of new icons are the same as the built-in ones.

Custom Icons Configuration

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

Configuration parameter

```
phone_setting.icon.url
phone_setting.icon.delete
```

Parameter	Description	Permitted Values	Default
phone_setting.icon.url[1]	It configures the access URL of the *.tar file for custom icons.	URL within 511 characters	Blank
phone_setting.icon.delete[1]	It deletes all custom icons.	http://localhost/all	Blank

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

Warnings Display

When one of the following situations occurs, a warning icon appears in the status bar.

- The default password is being used
- Account registration failed
- Provisioning credentials are wrong
- Network is unavailable
- Line on redundancy registration

On the T42S/T42U/T41S phones, a warning message appears on the idle screen.

On the other phones, a warning icon appears in the status bar.

Warnings Display Configuration

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

Configuration parameter

phone_setting.warnings_display.mode

Parameter	Description	Permitted Values	Default	Supported Devices
phone_setting.warnings_display.mode	It enables or disables the phone from displaying warnings.	0-Disabled 1-Enabled	1	All phones except T48G, T46G, T42G, T41P and T29G

Out of Service

When the network of the phone is disconnected and the warning message appears on the screen, the phone will play an alert tone.

Out of Service Configuration

The following table lists the parameter you can use to configure out of service.

Configuration parameter

features.out_of_service_alert.enable
features.out_of_service_alert_time

Parameter	Description	Permitted Values	Default
features.out_of_service_alert.enable	It enables or disables the phone to play an alert tone when out of service caused to a network abnormality. You can customize the alert tone by the parameter "voice.tone.congestion".	0-Disabled 1-Enabled	0

features.out_of_service_alert_time	It configures the time (in seconds) to wait before the phone plays an alert tone after the network is abnormal. It works only if "features.out_of_service_alert.enable" is set to 1 (Enabled).	Integer from 0 to 3600	60

Theme

Introduction

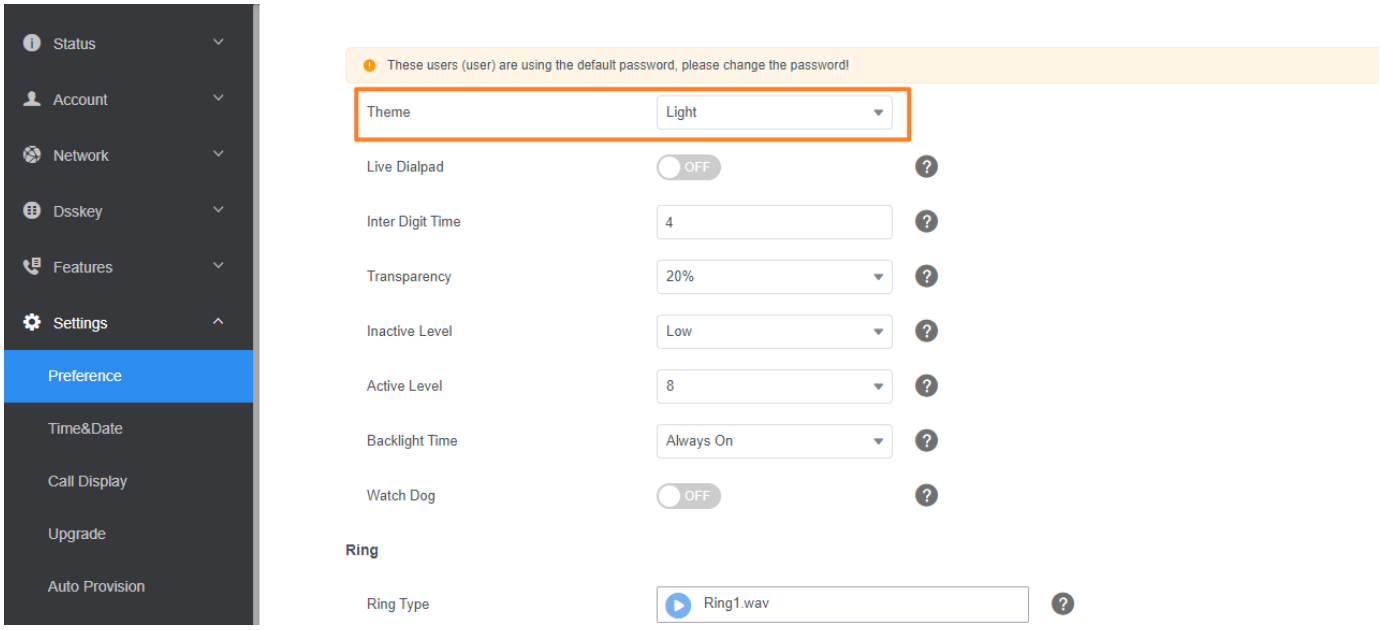
You can switch between the dark and light themes displayed on your phone.

Configure via Device Interface

For more detailed information, refer to Theme.

Set via the Web User Interface

1. Go to **Settings** > **Preference** > **Theme**.



Auto Provisioning

Parameter	Description	Permitted Values	Default
features.theme.mode	It configures the theme color of the phone.	1-Light 2-Dark	2

Ring Tone

Introduction

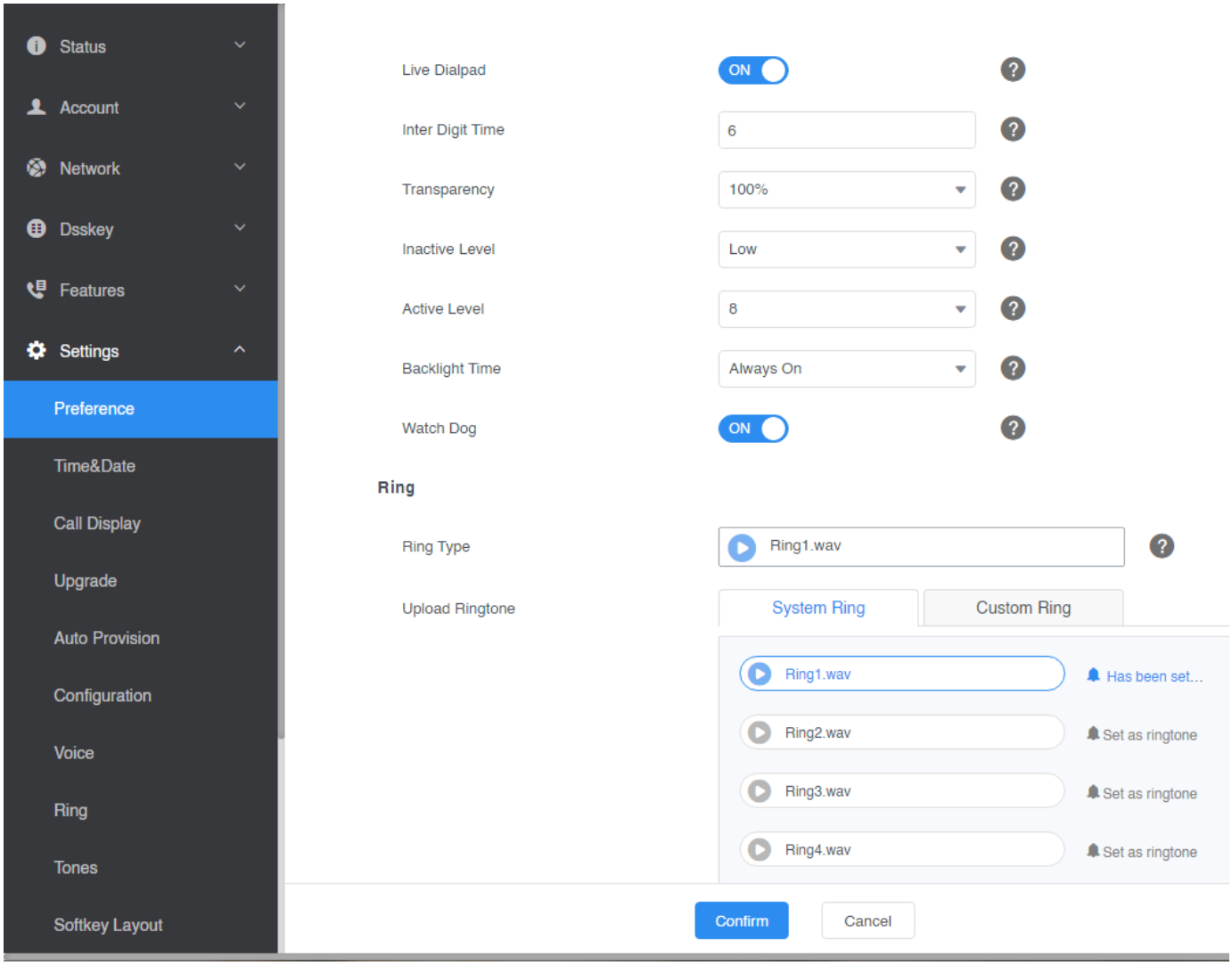
Our phone only supports *.wav format. And the ring tone file must be in PCMU/PCMA audio format, mono channel. 8K sample rate and 16-bit resolution.

Different models have different ringtone file size limits. The specific data can refer in the following table.

Phone Model	Format	Single File Size
VP59/T58A/CP960	WAV	<=8 MB
T57W/T54W/T48U/T48S/T46U/T46S/T7X/T8X	WAV	<=8 MB
T48G/T46G/T29G	WAV	<=8 MB (2.4 MB of space should be reserved for the phone)
T53W/T53/T42U/T42S/T41S/T42G/T41P/T40P/T40G/T27G/T23P/T23G/T21(P)/E2/T19(P)/E2/CP920	WAV	<=100 KB

Set via the Web User Interface

1. 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.


Status
Account
Network
Dsskey
Features
Settings
Preference
Time&Date
Call Display
Upgrade
Auto Provision
Configuration
Voice
Ring
Tones
Softkey Layout
Live Dialpad
ON
Inter Digit Time
6
Transparency
100%
Inactive Level
Low
Active Level
8
Backlight Time
Always On
Watch Dog
ON
Ring
Ring Type
Ring1.wav
Upload Ringtone
System Ring
Custom Ring
Ring1.wav
Has been set...
Ring2.wav
Set as ringtone
Ring3.wav
Set as ringtone
Ring4.wav
Set as ringtone
Confirm
Cancel

Analog Headset

Introduction

When an analog headset is plugged in, you can configure whether the phone recognizes the headset. After disabling the analog headset mode, the phone will not be switched to the headset channel due to accidental pressing of the headset button.

Configuration Parameter

features.analog_headset.enable

Parameter	Description	Permitted Values	Default
features.analog_headset.enable	It enables or disables the phone's analog headset mode.	**0**-Disabled **1**-Enabled	0

Firmware Upgrade

Firmware Upgrade

There are two methods for firmware upgrades:

- Manually, from the local system for a single device via the web user interface.
- Automatically, from the provisioning server for a mass of devices.

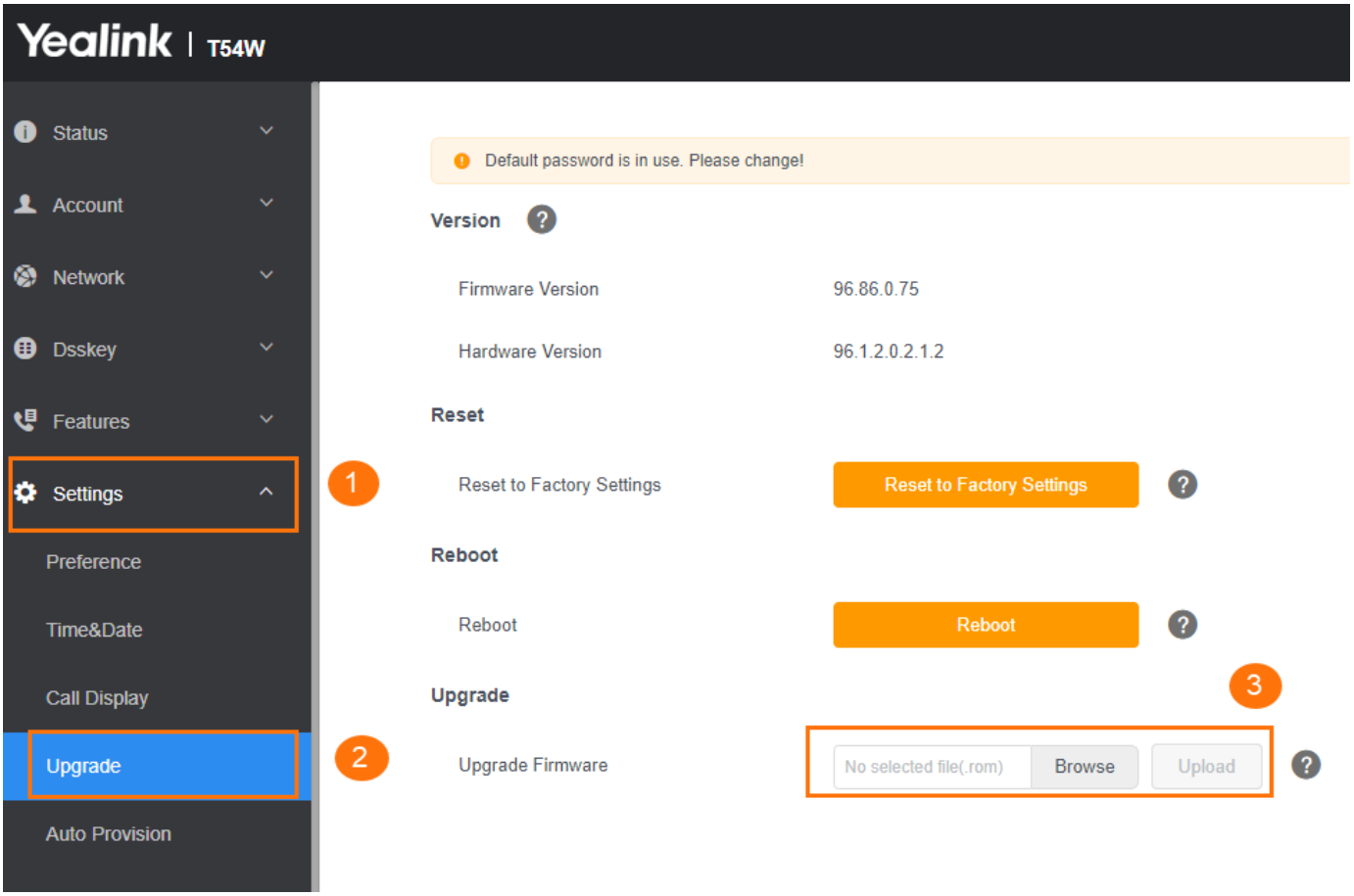
- We recommend that the devices running the latest firmware should not be downgraded to an earlier firmware version. The new firmware is compatible with old configuration parameters and vice versa.
- Downgrading will result in some configurations being cleared, so please restore the factory settings after downgrading before using the device again.

Firmware for Each Phone Model

You can download the latest firmware online: Yealink Support.

Set via the Web User Interface

On the web user interface, go to: **Settings** > **Upgrade** > **Upgrade Firmware.**



Firmware Upgrade Configuration

Before upgrading firmware, you need to know the following:

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

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

Configuration parameter

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

Before You Begin

Supported devices: T57W/T54W/T53W/T53/VP59/T58W/T58V/T58A/T56A/T85W/T87W/T88W (Pro)/T88V Pro.

Handset Screen Setting

Handset Screen Setting

To turn your Yealink phone into a corded-cordless phone, you'll need a T57W/T54W/T53W/T53/VP59/T58W/T58V/T58A/T56A/T85W/T87W/T88W (Pro)/T88V Pro phone, a DECT USB dongle DD10K, and at least one handset.The supported handsets include W59R, W52H, W56H, W53H, CP930W, CP935W, W73H, W78H, W57R and DD phone. The corded-cordless phone acts as a base station and Handset 1. Users can register up to four other handsets to one phone. It allows users to manage calls when they are away from their desk.

To use this feature, you should insert a DD10K into the rear USB port on the phone in advance.

Note that you can still use the phone features as usual on the corded-cordless phone.

> To use this feature, you should set "static.usb.power.enable" to 1 (Enabled). When satellite mode is disabled, Yealink recommends using forward and DND features in custom mode.

Handset Backlight

The handset supports different backlight statuses, and you can configure it.

For W78H/W73H/W59R/W53H/W56H/W57R, the backlight in charger or out of charger can be configured independently. You can enable the backlight to be on for about 30 minutes when the handset is charged, and then you can check the charging state during this period. You can also enable the backlight to be on for about 30 minutes when the handset is not charged. The backlight will be turned off after the handset is idle for a period of time. When an incoming call arrives, a key is pressed, or the status of the handset changes, the backlight is automatically turned on.

Handset Backlight Configuration

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

Configuration parameter

custom.handset.backlight_in_charger.enable
custom.handset.backlight_out_of_charger.enable
phone_setting.on_call.backlight_mode

Parameter	Permitted Values	Default	Description	Supported Devices

custom.handset.backlight_in_charger.enable	**-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. It will take effect on all handsets that are registered on the same phone. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	W78H, W73H, W59R, W53H, W56H, W57R
custom.handset.backlight_out_of_charger.enable	**-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. It will take	W78H, W73H, W59R, W53H, W56H, W57R

			effect on all handsets that are registered on the same phone. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	
phone_setting.on_call.backlight_mode	**0**-When talking for about 2 minutes without any operation on the phone, the backlight is reduced to 10% brightness when the Inactive Level is chosen Low. **1**-The backlight always maintains the intensity set by "phone_setting.active_backlight_level" during a call.	0	It configures the backlight brightness of the CP935W during a call.	CP935W

Handset Keypad Light

You can enable the handset keypad light to light up the keypad when any key is pressed. This helps you distinguish keys from each other in a dark environment.

The following table lists the parameters you can use to configure the handset keypad light.

Configuration parameter

custom.handset.keypad_light.enable

Parameter	Permitted Values	Default	Description	Supported Devices
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. It will take effect on all handsets that are registered to the same phone. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	W78H, W73H, W59R, W53H, W56H, W57R

Handset Wallpaper

Wallpaper is an image used as the background for the handset's idle screen. Users can select an image from the handset's built-in background.

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

Configuration parameter

custom.handset.wallpaper

Parameter	Permitted Values	Default	Description	Supported Devices
custom.handset.wallpaper	**1**-Wallpaper1 **2**-Wallpaper2 **3**-Wallpaper3 **4**-Wallp	-1, do not change the wallpaper set on each handset.	It configures the wallpaper displayed on the handset's LCD screen. It will take effect on all handsets that are registered on the same phone. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	W59R, W52H, W56H, W53H, CP935W, W73H, W78H, W57R

	aper4 **5**- Wallp aper5			

Handset Screen Saver

The screen saver of the handset is designed to protect your LCD screen. You can enable the screen saver to protect the LCD screen, an analog clock will be activated and appear on the LCD screen after the handset is idle for approximately 10 seconds.

It is only applicable to W78H/W73H/W59R/W53H/W56H/W57R handsets.

The following table lists the parameters you can use to configure the handset screen saver.

Configuration parameter

custom.handset.screen_saver.enable

Parameter	Permitted Values	Default	Description	Supported Devices
custom.handset.screen_saver.enable	**-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 the screen saver feature. It will take effect on all handsets that are registered on the same phone. It works	W78H, W73H, W59R, W53H, W56H, W57R

			only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	

Handset Contact Setting

Handset contact setting

Handset LDAP Configuration

The following table lists the parameters you can use to configure LDAP for each handset.

Configuration parameter

handset.X.ldap.enable
handset.X.ldap.name_filter
handset.X.ldap.number_filter
handset.X.ldap.tls_mode
handset.X.ldap.host
handset.X.ldap.port
handset.X.ldap.base
handset.X.ldap.user
handset.X.ldap.password
handset.X.ldap.max_hits
handset.X.ldap.name_attr
handset.X.ldap.numb_attr
handset.X.ldap.display_name
handset.X.ldap.version
handset.X.ldap.call_in_lookup
handset.X.ldap.call_out_lookup
handset.X.ldap.ldap_sort
handset.X.ldap.incoming_call_special_search.enable

Parameter	Permitted Values	Defau lt	Description
handset.X.l dap.enable[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the LDAP feature.
handset.X.ld	String within	Blank	It configures the search criteria for LDAP contact

ap.name_filter[1]	512 characters		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**: 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. 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. 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.
handset.X.ldap.number_filter[1]	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**: 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. 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.

handset.X.ldap.tls_mode[1]	**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.
handset.X.ldap.host[1]	IP address or domain name	Blank	It configures the IP address or domain name of the LDAP server.
handset.X.ldap.port[1]	Integer from 1 to 65535	389 (LDAPS: 636)	It configures the port of the LDAP server.
handset.X.l	String within	Blank	It configures the LDAP search base, which corresponds

dap.base[1]	512 characters		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
handset.X.ldap.user[1]	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 in. Otherwise, you will need to provide the username to log into the LDAP server. **Example**: ldap.user = cn=manager,dc=yealink,dc=cn
handset.X.ldap.password[1]	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 log in. Otherwise, you will need to provide the password to log into the LDAP server.
handset.X.ldap.max_hits[1]	Integer from 1 to 1000	50	It configures the maximum number of search results to be returned by the LDAP server.
handset.X.ldap.name_attr[1]	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.
handset.X.ldap.numb_attr[1]	String within 512 characters	Blank	It configures the number attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple number attributes, 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.
handset.X.ldap.display_name[1]	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.
handset.X.ldap.version[1]	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.
handset.X.ldap.call_in_lookup[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to perform an LDAP search when receiving an incoming call.
handset.X.ldap.call_out_lookup[1]	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to perform an LDAP search when placing a call.
handset.X.ldap.ldap_sort[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to sort the search results in alphabetical order or numerical order.
handset.X.ldap.incoming_call_special_search.enable[1]	**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. 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.

[1]X is the handset ID. X=1-5.

Set via the Web User Interface

On the web user interface, go to **Directory** > **LDAP** >**Handset X.**

Shared Directory

Users can manage and call the contacts in the Shared Directory on the phone and all the registered handsets.

The shared directory can store up to 1000 contacts.

It is not applicable to DD phones.

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

Configuration parameter

shared_contact_list.url
static.directory_setting.shared_contact.enable

Parameter	Description	Permitted Values	Default	Supported Devices
shared_contact_list.url	It configures the access URL of the shared contact file (*.xml) of the phone and registered handsets. Example: shared_contact_list.url = http://192.168.10.25/contact.xml NOTE It works only if "static.directory_setting.shared_contact.enable" is set to 1 (Enabled).	URL within 511 characters	Blank	All handsets except DD phones

static.directory_setting.shared_contact.enable	It enables or disables the Shared Directory feature.	0-Disabled 1-Enabled	0	All handsets except DD phones

Set via the Web User Interface

On the web user interface, go to **Directory** > **DECT Directory** > **Import Contacts** > **Import to (Shared Directory)** > **Select ".xml" file form**.

Shared Contact File Customization

You can customize the shared contacts using the local contact template.

You can ask the distributor or Yealink FAE for the local contact template. You can also obtain the template online: Local Directory

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

Attributes	Description
display_name	Specify the contact name. Note: The contact name cannot be blank or duplicated.
office_number	Specify the office number.
mobile_number	Specify the mobile number.
other_number	Specify the other number.
line	Do not modify this attribute and value.
ring	Do not modify this attribute and value.
default_photo	Do not modify this attribute and value.
selected_photo	Do not modify this attribute and value.
group_id_name	Do not modify this attribute and value.

Customizing Shared Contact File

1. Open the shared contact file.
2. To add a contact, add <contact display_name="" office_number="" mobile_number="" other_number="" line="-1" ring="Auto" default_photo="Default:default_contact_image.png" selected_photo="0" group_id_name="All Contacts"/ > to the file. Each starts on a new line.
3. Specify the values within double quotes.
4. 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 on the provisioning server. Place this file on the provisioning server.

Handset Name & Number Setting

Handset Name

The handset will be assigned a name by default if successfully registered to the phone. You can personalize the handset name.

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

Configuration parameter

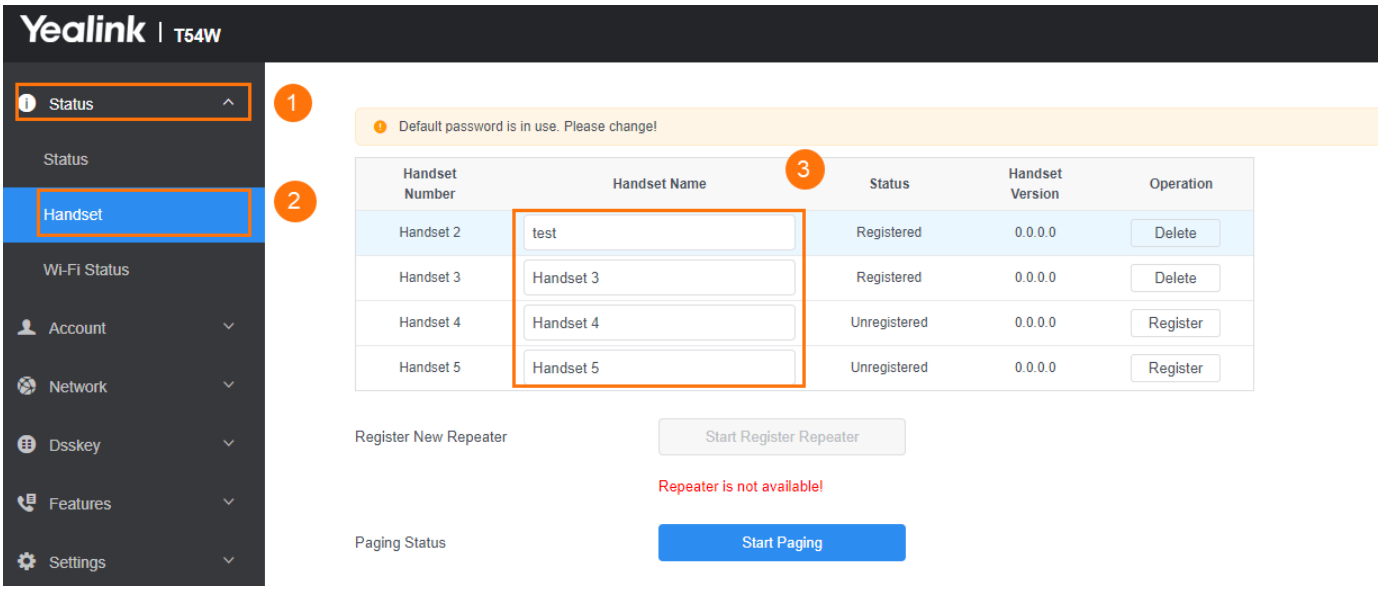
handset.X.name

Parameter	Permitted Values	Default	Description
handset.X.name[1]	String within 24 characters	The handset name for handset 1 is Corded phone. The handset name for handset 2 is Handset 2. The handset name for handset 3 is Handset 3. The handset name for handset 4 is Handset 4. The handset name for handset 5 is Handset 5.	It configures the name of the handset. If it is set to blank, it will display the corresponding default handset name.

> [1]X is the handset ID. X=2-5.

Set via the Web User Interface

On the web user interface, go to **Status** > **Handset** > **Handset Name** > **Handset X.**



Number Assignment

After the handset is registered to the phone, you can assign one or more outgoing lines or incoming lines for the handset. The phone acts as the Handset 1 (Corded phone).

The handset can only use the assigned outgoing line(s) to place calls. When multiple outgoing lines are assigned to the handset, the handset uses the first line as the default outgoing line. You can change the default outgoing line of the handset.

The handset can only receive incoming calls via the assigned incoming line(s). You can assign incoming lines to all handsets that are registered to the same phone.

> You can only assign one outgoing line and one incoming line for the CP930W. And make sure that the outgoing line and the incoming line are the same line.

The following table lists the parameters you can use to assign lines.

Configuration parameter

handset.X.incoming_lines
handset.X.dial_out_lines
handset.X.dial_out_default_line

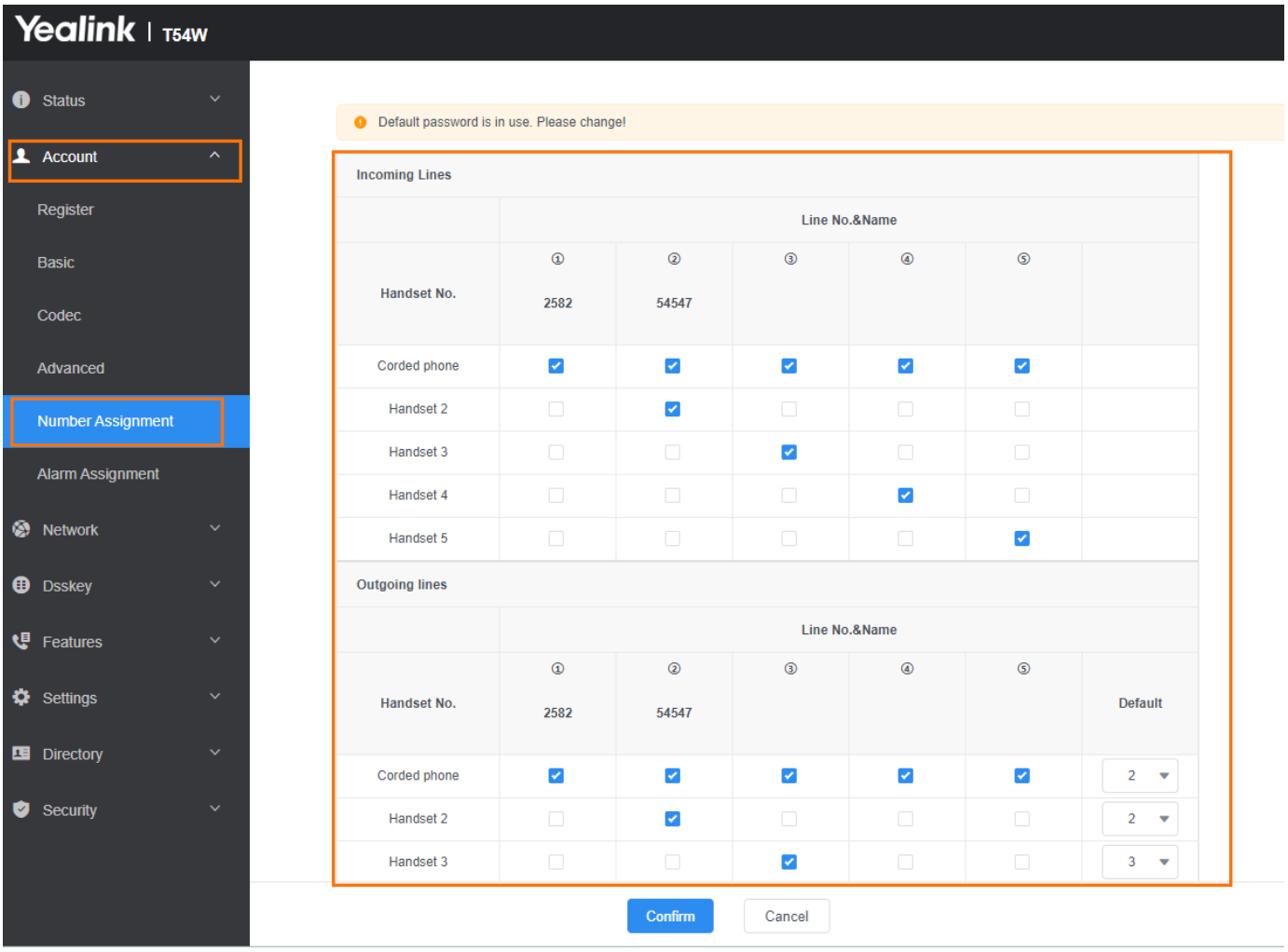
Parameter	Permitted Values	Default	Description
handset.X.incoming_lines[1]	**1**-Line 1 **2**-Line 2 **3**-Line 3 **4**-Line 4	The incoming line for Corded phone is line 1-line5. The incoming line for	It configures the lines to receive incoming calls for a specific handset.

	5-Line 5 Multiple line IDs are separated by commas.	handset 1 is line 1. The incoming line for handset 2 is line 2. The incoming line for handset 3 is line 3. The incoming line for handset 4 is line 4. The incoming line for handset 5 is line 5.	
handset.X.dial_out_lines[1]	**1**-Line 1 **2**-Line 2 **3**-Line 3 **4**-Line 4 **5**-Line 5	The outgoing line for Corded phone is line 1-line5. The outgoing line for handset 2 is line 2. The outgoing line for handset 3 is line 3. The outgoing line for handset 4 is line 4. The outgoing line for handset 5 is line 5.	It configures the lines to place outgoing calls for a specific handset. Multiple line IDs are separated by commas.
handset.X.dial_out_default_line[1]	Integer from 1 to 5	X	It configures the default line to place outgoing calls for a specific handset.

> [1]X is the handset ID. X=1-5.

Set via the Web User Interface

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



End Call on Hook

You can configure whether to end a call when you place the handset into the charging cradle.

The following table lists the parameters you can use to configure the end call on hook.

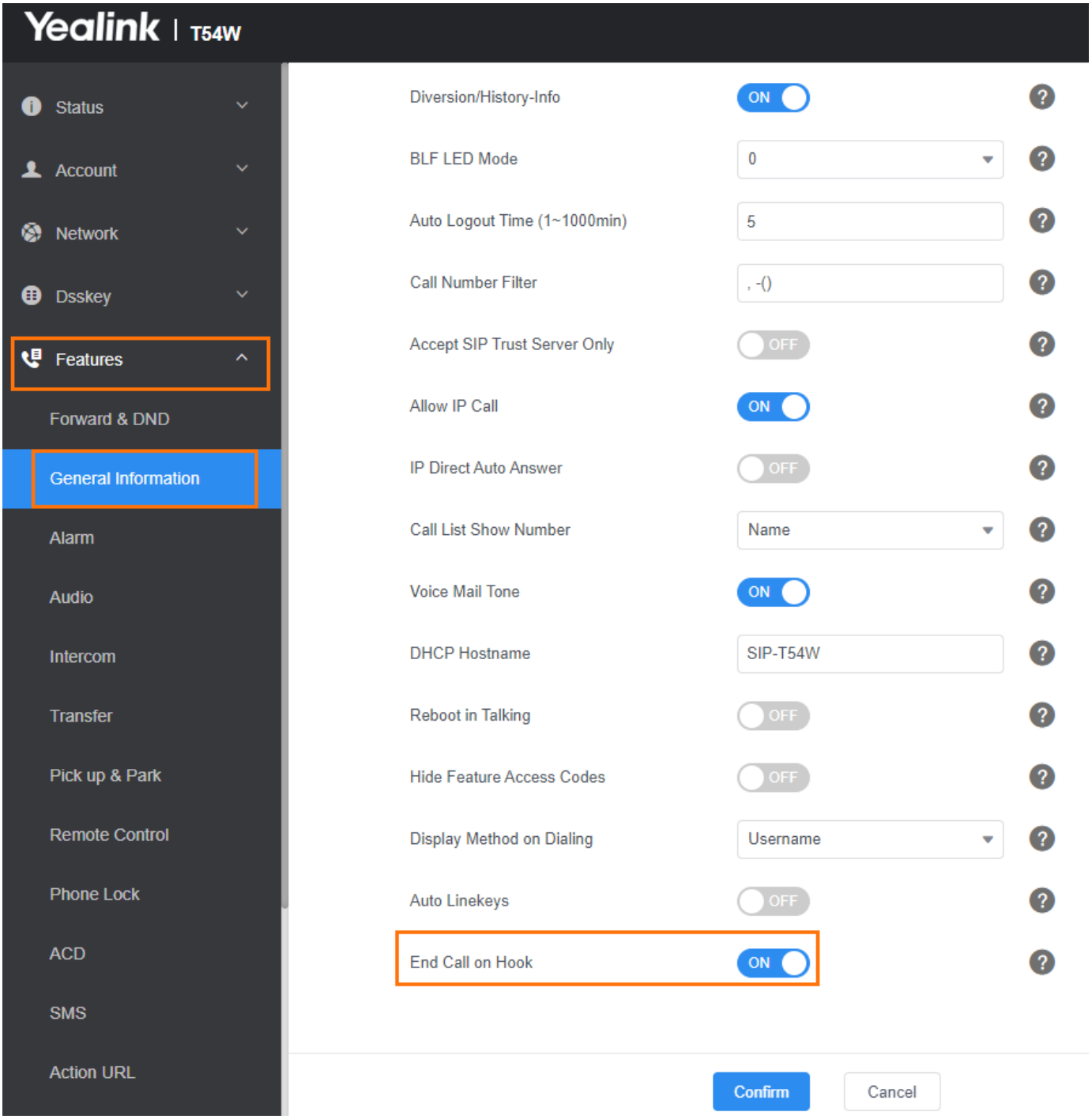
Configuration parameter

phone_setting.end_call_on_hook.enable

Parameter	Permitted Values	Default	Description	Supported Devices
phone_setting.end_call_on_hook.enable	0-Never 1-Always	1	It enables or disables to end of a call when placing the handset into the charger cradle.	W78H, W73H, W59R, W53H, W56H

Set via the Web User Interface

On the web user interface, go to **Features** > **General Information** > **End Call On Hook.**



Base PIN

To avoid unauthorized registration or access to some features on the handset, you should keep the base PIN secret.

You can change the base PIN for security.

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

Configuration parameter

```
base.pin_code
base.double_pin_code.enable
base.pin_code_for_register
```

Parameter	Permitted Values	Default	Description
base.pin_code	Integer from 0000 to 9999	0	It configures the base PIN.
base.double_pin_code.enable	**0**-Disabled, users use the PIN configured by "base.pin_code" to register the handset or access some features. **1**-Enabled, users use the PIN configured by "base.pin_code_for_register" to register the handset, and use the PIN configured by "base.pin_code" to access some features.	0	It enables or disables the double PIN feature.
base.pin_code_for_register	Integer from 0000 to 9999	0	It configures the PIN for registering or deregistering a handset. It works only if "base.double_pin_code.enable" is set to 1 (Enabled).

DECT Intercom

Intercom is a useful feature in an office environment to quickly connect with the operator or the secretary. Users can make internal intercom calls and external intercom calls on the handset. Internal intercom calls are made among handsets registered to the same phone.

The handset can automatically answer an incoming external intercom call and play a warning tone.

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

Configuration parameter

```
custom.handset.auto_intercom
```

features.intercom.headset_prior.enable

Parameter	Permitted Values	Default	Description
custom.handset.auto_intercom	**-1**-Do not modify the configuration. **0**-Off, auto intercom feature is disabled. Users need to answer incoming internal intercom calls manually. **1**-On(Beep Off), the phone/ handset answers an incoming internal intercom call automatically without a warning tone. **2**-On(Beep On), the phone/ handset answers an incoming internal intercom call automatically and plays a warning tone. It works when the silence mode is off.	-1	It enables or disables the auto intercom feature on the handset.
features.intercom.headset_prior.enable	**0**-Speaker Mode **1**-Headset Mode	1	It configures the channel mode when an incoming intercom call is automatically answered.

			It works only if "custom.handset.auto_intercom" is set to 1 or 2. For the phone, the headset mode should be activated for use; for the handset registered to the phone, the headset should be connected in advance.

Satellite Mode Configuration

Satellite Mode Configuration

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

Configuration parameter

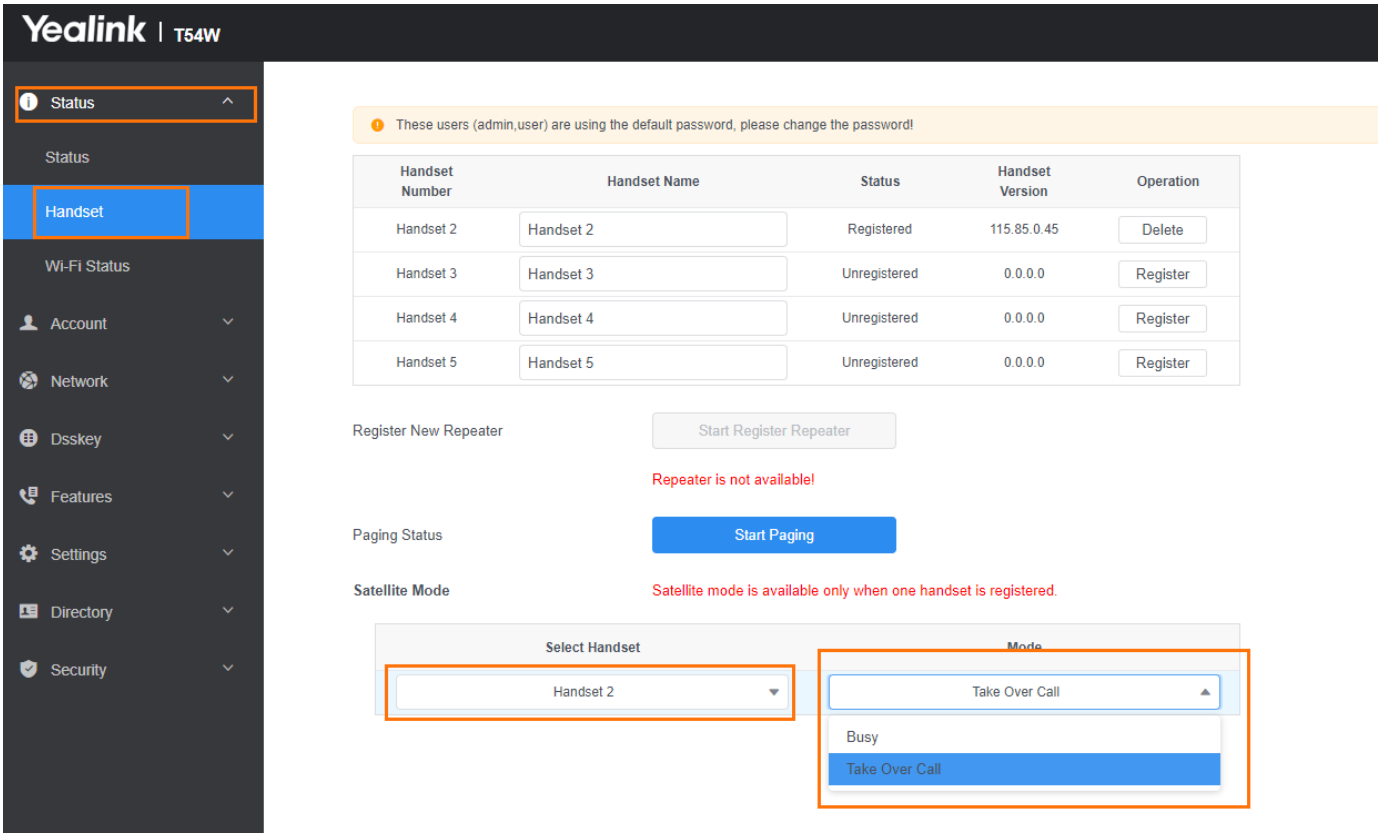
features.ms.X.slave_handset_number
features.ms.X.mode

Parameter	Permitted Values	Default	Description
features.ms.X.slave_handset_number[1]	**0**-None, the satellite mode is disabled. **2**-Handset 2 **3**-Handset 3 **4**-Handset 4 **5**-Handset 5	0	It specifies which handset to use the satellite mode with the phone.
features.ms.X.mode[1]	**0**-Busy, users cannot switch the active call between the phone and handset. Regardless of the phone or the handset, the device that is during a call can initiate a new call. If users are not in a call and try to initiate a call on the phone/handset, the phone/handset will prompt "Path Busy". **1**-Take over call, when the handset is during the call, users can retrieve the call after off-hook on the phone. When the phone is during the call, users can push the call to the handset.	1	It configures the satellite mode for the phone. It works only if "features.ms.X.slave_handset_number" is configured correctly.

[1]X is the handset ID. X is equal to 1.

Set via the Web User Interface

On the web user interface, go to **Status** > **Handset** > **Satellite Mode.**



Repeater Settings Parameters

Parameter	Permitted Values	Default	Description
static.base.repeater_mode.enable[1]	**0**-Off **1**-RT10/RT20 **2**-RT30	0	It configures the repeater mode to extend the radio coverage of the phone.

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

Handset Settings Parameters

Handset Settings Parameters

Configuration parameter

custom.handset.eco_mode.enable
custom.handset.color_scheme
custom.handset.missed_call_notify_light.enable
custom.handset.voice_mail_notify_light.enable
custom.handset.language
custom.handset.auto_answer.enable
custom.handset.time_format
custom.handset.date_format
handset.X.hac.enable
static.auto_provision.handset_configured.enable
static.auto_provision.custom.handset.protect
handset.X.contact_list.url

Parameter	Permitted Values	Default	Description	Supported Devices
custom.handset.eco_mode.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 eco mode to greatly reduce the transmission power and signal output when the phone is in the talk mode.	All handsets except DD phones
custom.handset.color_scheme	**-1**-Do not modify the handset configuration (Keep the original	-1	It configures the color scheme of the handset. It will take effect on all handsets that are	W52H

	configuration of the handset). **0**-Color scheme 1 **1**-Color scheme 2		registered on the same phone. It works only if the value of the parameter "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	
custom.handset.missed_call_notify_light.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 message key LED to flash red when the handset misses a call. It will take effect on all handsets that are registered on the same phone. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	W52H
custom.handset.voice_mail_notify_light.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 message key LED to flash when the handset receives a voice mail. It will take effect on all handsets that are registered on the same phone. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	W52H
custom.handset.language	For W59R/W56H/W53H/CP930W handset: **0**-English **1**-French **2**-German **3**-Italian	0	It configures the language used on the DECT handset user interface. It will take effect on all handsets that are registered on the same phone. It works only if "static.auto_provision.ha	W59R, W52H, W56H, W53H, CP930W, CP935W, W73H, W78H, W57R

	4-Polish **5**-Portuguese **6**-Spanish **7**-Turkish **8**-Swedish **9**-Russian For W52H handset: **0**-English **1**-French **2**-German **3**-Italian **4**-Polish **5**-Portuguese **6**-Spanish **7**-Turkish **8**-Czech **9**-Swedish **10**-Hebrew **11**-Russian		ndset_configured.enable" is set to 1 (Enabled).	
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 pressing the off-hook key. 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).	W78H, W73H, W59R, W53H, W56H
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	1	It configures the time format for all registered handsets. It works only if "static.auto_provision.ha	All handsets except DD phones

	will be displayed in 24-hour format (for example, 2:00 PM displays as 14:00).		ndset_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.	All handsets except DD phones
handset.X.hac.enable [1]	**0**-Disabled **1**-Enabled	0	It enables or disables the HAC (Hearing Aid Compatibility) handset settings.	All handsets except DD phones
static.auto_provision.handset_configured.enable	**0**-Disabled, the phone will not deliver custom handset configurations via auto provisioning/ handset reboot to	1	It enables or disables the handsets to keep user's personalized settings after auto provisioning. It is only applicable to the custom handset related configurations.	All handsets except DD phones

	the handset. The custom handset settings can only be changed via the handset user interface. **1**-Enabled, the phone will deliver the custom handset configurations via auto provisioning to the handset. Handset reboot or registration will also trigger the phone to deliver the stored handset settings to the handset. 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.			
static.auto_provisi	**0**-Disabled **1**-Enabled	1	It enables or disables the handsets to keep user's personalized settings	All handsets except DD

on.custom.handset.protect			after handset reboot or registration. 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.	phones
handset.X.contact_list.url[2]	URL within 511 characters	Blank	It configures the access URL of the contact file (*.xml) for a specific handset. Example: handset.2.contact_list.url= http://192.168.10.25/contact.xml	All handsets except DD phones

> [1]X is the handset ID. X=1 to 5.

> [2]X is the handset ID. X=2 to 5.

Custom Handset Related Configurations

This section shows you the custom handset-related configurations.

Configuration parameter

```
custom.handset.date_format
custom.handset.time_format
custom.handset.eco_mode.enable
custom.handset.auto_answer.enable
custom.handset.missed_call_notify_light.enable
custom.handset.voice_mail_notify_light.enable
custom.handset.color_scheme
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.auto_intercom
custom.handset.language

Parameter	Related Topic
custom.handset.date_format	Handset Settings Parameters
custom.handset.time_format	Handset Settings Parameters
custom.handset.eco_mode.enable	Handset Settings Parameters
custom.handset.auto_answer.enable	Auto Answer Configuration
custom.handset.missed_call_notify_light.enable	Handset Settings Parameters
custom.handset.voice_mail_notify_light.enable	Handset Settings Parameters
custom.handset.color_scheme	Handset Settings Parameters
custom.handset.low_battery_tone.enable	Advisory Tones Configuration
custom.handset.confirmation_tone.enable	Advisory Tones Configuration
custom.handset.keypad_tone.enable	Advisory Tones Configuration
custom.handset.keypad_light.enable	Handset Keypad Light Configuration
custom.handset.backlight_in_charger.enable	Handset Settings Parameters
custom.handset.backlight_out_of_charger.enable	Handset Settings Parameters
custom.handset.screen_saver.enable	Handset Settings Parameters
custom.handset.auto_intercom	DECT Intercom Configuration
custom.handset.language	Handset Settings Parameters

Handset Firmware Upgrade Configuration

Handset Firmware Upgrade Configuration

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

Configuration parameter

over_the_air.url
over_the_air.url.w56h
over_the_air.url.cp930w
over_the_air.handset_tip
over_the_air.handset_trigger
over_the_air.base_trigger
over_the_air.url.w52h
over_the_air.url.w53h
over_the_air.url.w59r
over_the_air.url.t41s_dd10k
over_the_air.url.t54w_dd10k

Parameter	Permitted Values	Default	Description
over_the_air.url	URL within 511 characters	Blank	It configures the access URL of the handset firmware file.
over_the_air.url.w56h	URL within 511 characters	Blank	It configures the access URL of the W56H handset firmware file. The priority of parameter "over_the_air.url.w56h" is higher than "over_the_air.url" .
over_the_air.url.cp930w	URL within 512 characters	Blank	It configures the access URL of the CP930W phone firmware file. The priority of parameter

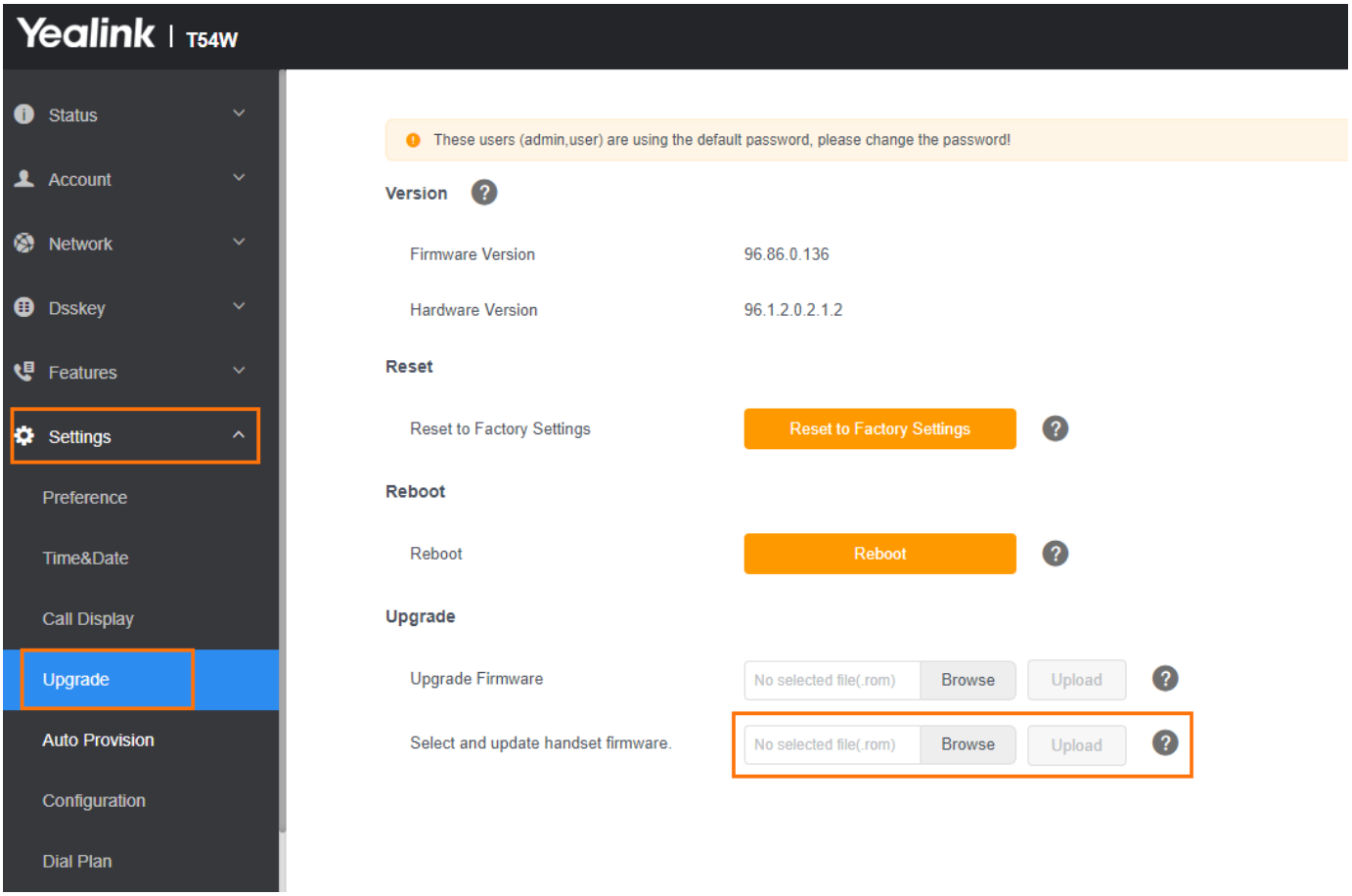
			"over_the_air.url.cp930w" is higher than "over_the_air.url".
over_the_air.handset_tip	0-Disabled 1-Enabled, the handset will pop up the message "Handset has a new firmware, update now?".	1	It enables or disables to pop up a tip when upgrading the handset firmware from the provisioning server. It works only if "over_the_air.base_trigger" and "over_the_air.handset_trigger" are set to 0 (Disabled).
over_the_air.handset_trigger	0-Disabled, if "over_the_air.handset_tip" is set to 1 (Enabled), it will pop up a tip on the handset to notify the user of a firmware upgrade. If "over_the_air.handset_tip" is set to 0, you may go to Settings > Upgrade Firmware on the handset to trigger the upgrade manually. 1-Enabled, it will upgrade the handset firmware compulsively without a pop-up tip on the handset.	1	It enables or disables to upgrade the handset firmware compulsively when the handset is registered to a phone or turned on successfully. It is only applicable when the current handset firmware is different from the one on the provisioning server.
over_the_air.base_trigger	0-Disabled, if "over_the_air.handset_tip" is set to 1 (Enabled), it will pop	1	It enables or disables to upgrade of the handset firmware compulsively when the phone detects a new handset firmware from the provisioning server.

	up a tip on the handset to notify the user to confirm upgrading the firmware or not. If "over_the_air.handset_tip" is set to 0, you may go to Settings > Upgrade Firmware on the handset to trigger the upgrade manually. 1-Enabled, it will upgrade the handset firmware compulsively without a pop-up tip on the handset.		
over_the_air.url.w52h	URL within 511 characters	Blank	It configures the access URL of the W52H handset firmware file. The priority of parameter "over_the_air.url.w52h" is higher than "over_the_air.url".
over_the_air.url.w53h	URL within 512 characters	Blank	It configures the access URL of the W53H handset firmware file. The priority of parameter "over_the_air.url.w53h" is higher than "over_the_air.url".
over_the_air.url.w59r	URL within 512 characters	Blank	It configures the access URL of the W59R handset firmware file. The priority of parameter "over_the_air.url.w59r" is higher than "over_the_air.url".

over_the_air.url.t41s_dd10k	URL within 512 characters	Blank	It configures the access URL of the DD phone firmware file. The priority of parameter "over_the_air.url.t41s_dd10k" is higher than "over_the_air.url".
over_the_air.url.t54w_dd10k	URL within 512 characters	Blank	It configures the access URL of the DD Phone firmware file. The priority of parameter "over_the_air.url.t54w_dd10k" is higher than "over_the_air.url".

Set via the Web User Interface

On the web user interface, go to **Setting->Upgrade->Select and update handset firmware.**



Video Settings

Video Settings

The VP59/T58A/T58W/T88W Pro/T88V Pro phones support using a USB camera for point-to-point video calls. Users can place and answer video calls. You can configure camera flicker to optimize video calling. Indoor lights powered by a 50Hz or 60Hz power source can produce a flicker. You can adjust the camera flicker frequency according to the power source.

During video calls, near-site and far-site video images are displayed on the touch screen. You can change the default video layout.

Video Settings Configuration

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

Configuration parameter

static.camera.function.enable
camera.status_bar_icon.enable
video.enable
account.X.video.mode
camera.flicker
features.default_layout
features.full_screen_in_call_enable
features.video_call_bandwidth
sip.h264.peer_resolution.default

Parameter	Permitted Values	Default	Description
static.camera.function.enable [1]	**0**-Disabled, the top USB port is disabled, and the near-site video image will not be transmitted in outgoing and incoming calls. **1**-Enabled	1	It enables or disables the USB camera feature.
camera.status_ba	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to display an icon in the status

r_icon.enable			bar when the camera is not detected.
video.enable	**0**-Disabled, users are only allowed to establish an audio-only call. **1**-Video first, users can establish a video call with the other party that is video-enabled. **2**-Optional, users can choose to establish an audio-only or video call; and switch between the audio-only call and the video call.	1	It configures the video call feature for the IP phone. If you want to transmit the near-site video image during the video call, you need to set "static.camera.function.enable" to 1 (Enabled).
account.X.video.mode[2]	**0**-Disabled, users are only allowed to establish an audio-only call. **1**-Video first, users can establish a video call with the other party that is video-enabled. **2**-Optional, users can choose to establish an audio-only or video call; and switch between the audio-only call and the video call.	Blank	It configures the video call feature for the IP phone. If you want to transmit the near-site video image during the video call, you need to set "static.camera.function.enable" to 1 (Enabled). The value configured by this parameter takes precedence over that configured by the parameter "video.enable".
camera.flicker	50-50Hz 60-60Hz	50	It configures camera flicker frequency (Hz). Indoor lights powered by a 50Hz or 60Hz power source can produce a flicker. You can adjust the camera flicker frequency according to the power source.

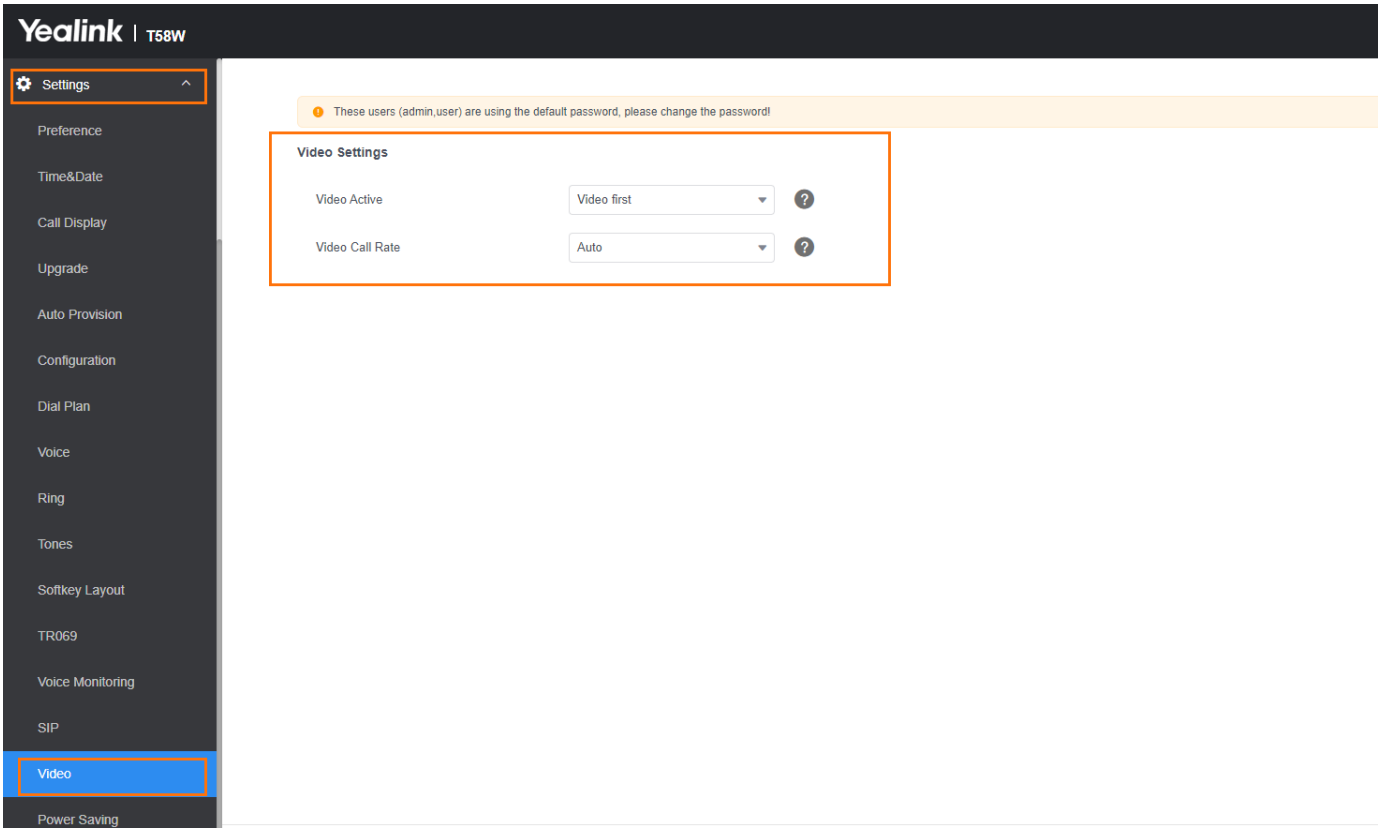
features.default_layout	**1**-Focus Big: One video image displays in a large size, the other video image, along the right side of the screen displays in small size. **2**-Focus Full Screen: One video image displays in full size, the other video images are hidden.	1	It configures the default call layout after a single-way call is set up. It works only if "video.enable" is set to 1 (Video first) or 2 (Optional). There is no near-site video image on the VP59/T58A phones if USB camera is not connected.
features.full_screen_in_call_enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to enter the full screen automatically when a video call is set up. It applies to VP59 only and works only if "video.enable" is set to 1 (Video first) or 2 (Optional).
features.video_call_bandwidth	**0**-Auto, the default transmission bandwidth is 768kb/s. The network environment may affect the performance of the phone. **256**-256kb/s **384**-384kb/s **512**-512kb/s **640**-640kb/s **768**-768kb/s **1024**-1024kb/s **1280**-1280kb/s **1500**-1500kb/s **2000**-2000kb/s	0	It specifies the transmission bandwidth for a video call. It works only if “video.enable” is set to 1 (Video first) or 2 (Optional). We recommend that you reduce transmission bandwidth when the network environment is relatively poor.
sip.h264	**0**-CIF	2	It configures the default video

.peer_resolution .default	**1**-4CIF **2**-720P **3**-1080P		resolution if the other party doesn't specify the resolution in H264 packet.

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

Set via the Web User Interface

On the web user interface, go to **Settings** > **Video** > **Video Active/Video Call Rate.**



Video Codecs

CODEC is an abbreviation of COmTap-DEComTap, 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 video signal with a minimum number of bits while retaining the quality. This can effectively reduce the frame size and the bandwidth required for video transmission.

The video 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 video codec list to the server and then use the video codec negotiated with the called party according to the priority.

RTPmap

Codecs and priorities of these codecs are configurable on a per-line basis. The attribute “rtpmap” is used to define a mapping from RTP payload codes to a codec, clock rate, and other encoding

parameters.

The following table lists the video codecs supported by the VP59/T58A phone model:

Name	MIME Type	Bit Rate	Frame Rate	Frame Size
H.264 BP	H264/90000	90 kbps to2048 kbps	5 fps to30 fps	Tx: CIF, 360P, W448P, 720PRx: Conventional Size Below 720P
H.264 HP	H264/90000	90 kbps to2048 kbps	5 fps to30 fps	Tx: CIF, 360P, W448P, 720PRx: Conventional Size Below 720P
VP8	VP8/90000	128kbps to 2048 kbps	5 fps to30 fps	Tx: CIF, 360P, W448P, 720PRx: Conventional Size Below 720P
H.263	H263	90 kbps to2048 kbps	5 fps to30 fps	Tx: CIF, 4CIFRX: QCIF, CIF, 4CIF

Video Codecs Configuration

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

Configuration parameter

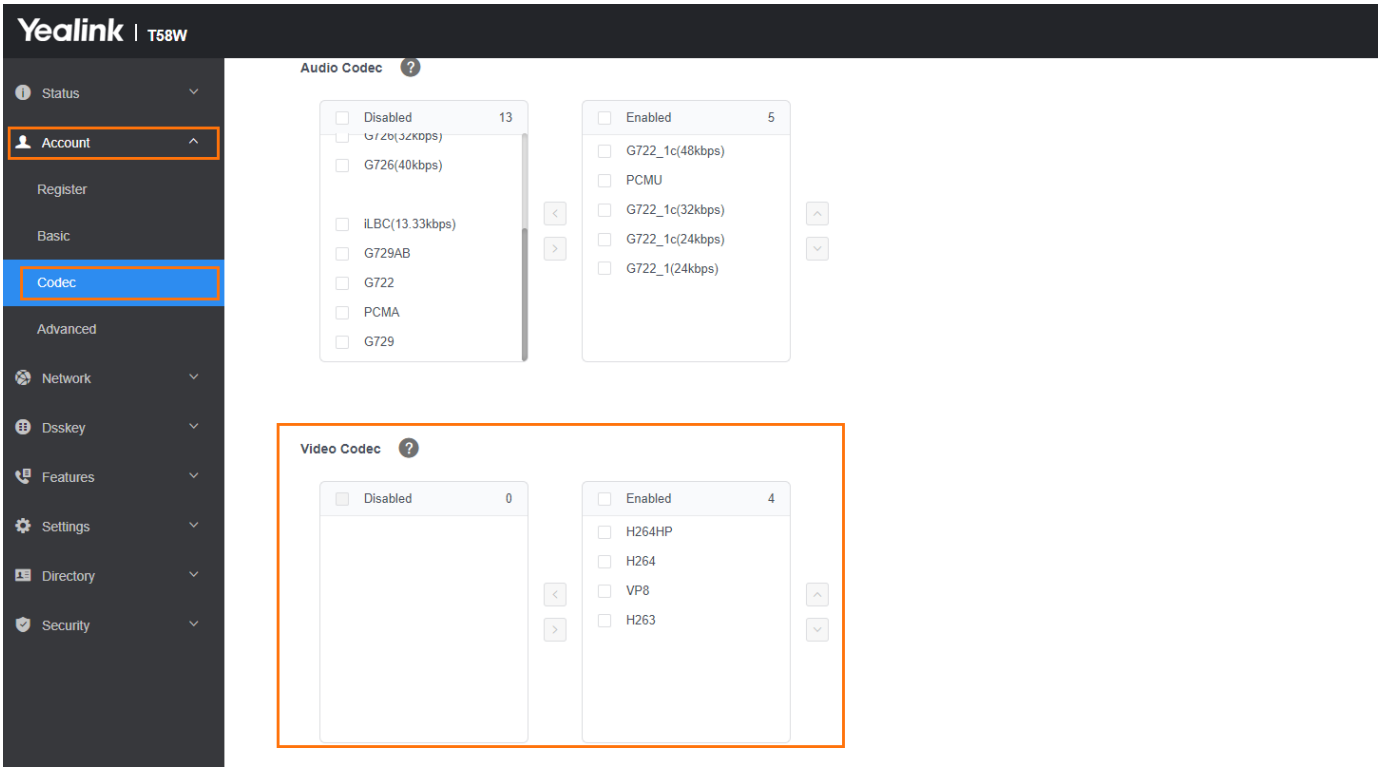
```
account.X.video.<payload_type>.enable
account.X.video.<payload_type>.priority
```

Parameter	Permitted Values	Default	Description
account.X.video.<payload_type>.enable (where <payload_type> should be replaced by the name of video codec)	**0**-Disabled **1**-Enabled	1	It enables or disables the specified video codec for account X. The name of the video codec: h264-H264 h264hp-H264HP vp8-VP8 h263-H263 Example: account.1.video.h264.enable = 1

			The name of video codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect.
account.X.video.<payload_type>.priority (where <payload_type> should be replaced by the name of video codec)	Integer from 0 to 3 (0 to 4 for VP59 phones)	When the audio codec is H264HP, the default value is 1; When the audio codec is H264, the default value is 2; When the audio codec is VP8, the default value is 3; When the audio codec is H263, the default value is 4;	It configures the priority of the enabled video codec for account X. The name of the video codec: h264-H264 h264hp-H264HP vp8-VP8 h263-H263 Example: account.1.video.h264.priority = 2 The name of video codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect.

Set via the Web User Interface

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


Yealink | T58W
Status
Account
Register
Basic
Codec
Advanced
Network
Dsskey
Features
Settings
Directory
Security
Audio Codec
Disabled 13
G726(32kbps)
G726(40kbps)
iLBC(13.33kbps)
G729AB
G722
PCMA
G729
Enabled 5
G722_1c(48kbps)
PCMU
G722_1c(32kbps)
G722_1c(24kbps)
G722_1(24kbps)
Video Codec
Disabled 0
Enabled 4
H264HP
H264
VP8
H263

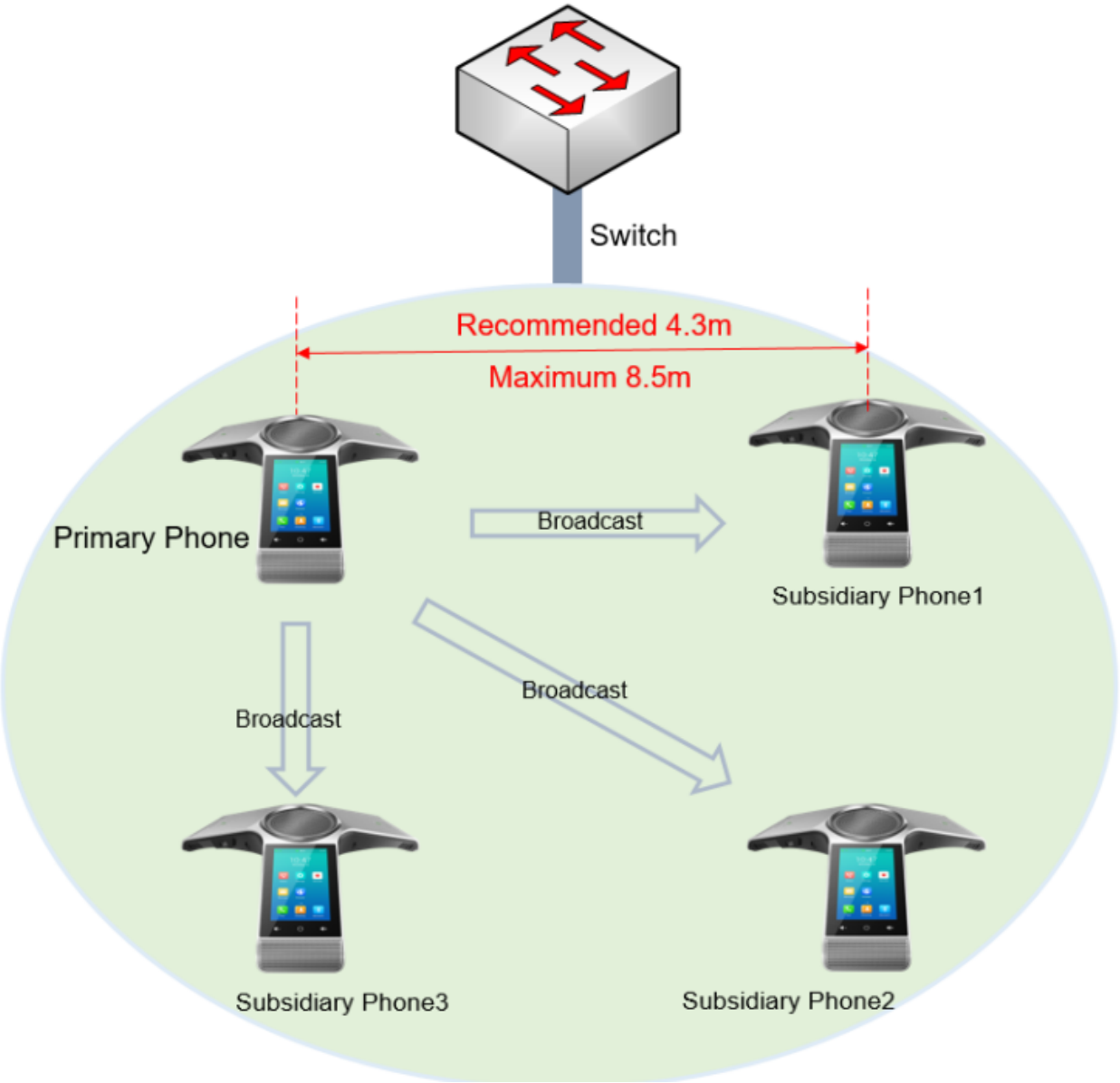
CP960 & CP965 Star Connection

Using CP960/CP965 Star Connection Feature

You can deploy up to four CP960/CP965 conference phones in a star layout in a large meeting room, one as the primary phone and others as the subsidiary phones. The primary phone keeps all features, while the subsidiary phones only sync some key features of the primary phone, such as DND and call mute. After connecting, the subsidiary phones are mainly used to work as speakers or microphones.

This feature allows users to control the calls either on the master phone or on the subsidiary phones; it also helps all participants to hear each other clearly even though they are distance away in the meeting room.

The following shows an example for setting up a star connection group:



Guidelines for Configuring the Star Connection Feature

The following instructions you need to know when configuring the star connection feature for CP960/CP965:

- Ensure all the phones are deployed in the same subnet.
- Ensure all the phones are running the same firmware versions.
- You can only deploy the CP960/CP965 phones in a star layout in the wired network.
- If the primary phone is not in the broadcast status, the subsidiary phones will not reconnect automatically after reboot.
- The subsidiary phones are unable to sync some custom features of primary phone, for example, wallpaper or contact avatar.
- You cannot access the web user interface of the subsidiary phones.
- If you upgrade firmware via the web user interface for the primary phone, only the primary phone will be upgraded. After upgrading, the subsidiary phones are disconnected from the primary phone because of the different firmware version.
- If you upgrade firmware via auto provisioning, both the primary phone and subsidiary phones will be upgraded.

CP960/CP965 Star Connection Feature Configuration

The following table lists the parameters you can use to configure the CP960/CP965 star connection feature.

Configuration parameter

features.cp_star_connection.master.enable
features.cp_star_connection.slave.X.mac
features.cp_star_connection.master.mac

Parameter	Permitted Values	Default	Description
features.cp_star_connection.master.enable	**0**-Not a primary phone **1**-primary phone, the phone automatically generates a four-digit PIN number and sends a broadcast. Users do not need to manually create a star connection group on the phone.	0	It specifies whether or not the phone is to be a primary phone.

features.cp_star_connection.slave.X.mac[1]	MAC Address	Blank	It specifies the MAC address of a subsidiary phone on the primary phone. After being configured, the phone with this MAC address is authorized to connect with the primary phone. Example: features.cp_star_connection.slave.1.mac = 805EC0092F4B Note that the MAC address is case insensitive, and the following format of the MAC address is invalid: 80:5E:C0:09:2F:4B. It works only if "features.cp_star_connection.master.enable" is set to 1 (Enabled).
features.cp_star_connection.master.mac[2]	MAC Address	Blank	It specifies the MAC address of the primary phone on the subsidiary phones. After being configured, the phones can join the star connection group created by the primary phone with this MAC address. Example: features.cp_star_connection.master.mac=805EC0092F33 Note that the MAC address is case insensitive, and the following format of the MAC address is invalid:

			80:5E:C0:09:2F:4B. It works only if "features.cp_star_connection.master.enable" is set to 0 (Disabled), and the phone is authorized by the primary phone to connect with it.

[1]X is the subsidiary phone ID. X = 1-3.

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

Example: Configuring CP960/CP965 Star Connection Feature

Scenario Conditions

- The MAC address of phone A is 805EC0092F33.
- The MAC address of phone B is 805EC0092F4B.
- The MAC address of phone C is 805EC009223B.
- The MAC address of phone D is 805EC0033E2B.
- All the phones are in the same subnet, and are running the same firmware versions.

You want phone A to act as a primary phone, and phone B, phone C and phone D act as the subsidiary phones.

The following example shows the configuration for the phones:

```
######For Phone A (primary phone)######
features.cp_star_connection.master.enable=1
features.cp_star_connection.slave.1.mac=805EC0092F4B
features.cp_star_connection.slave.2.mac=805EC009223B
features.cp_star_connection.slave.3.mac=805EC0033E2B
######For Phones B、C、D (subsidiary phones)######
features.cp_star_connection.master.enable=0
features.cp_star_connection.master.mac=805EC0092F33
After reboot, phone A, B, C, D are in a star connection group.
```

Get Start

Get Started

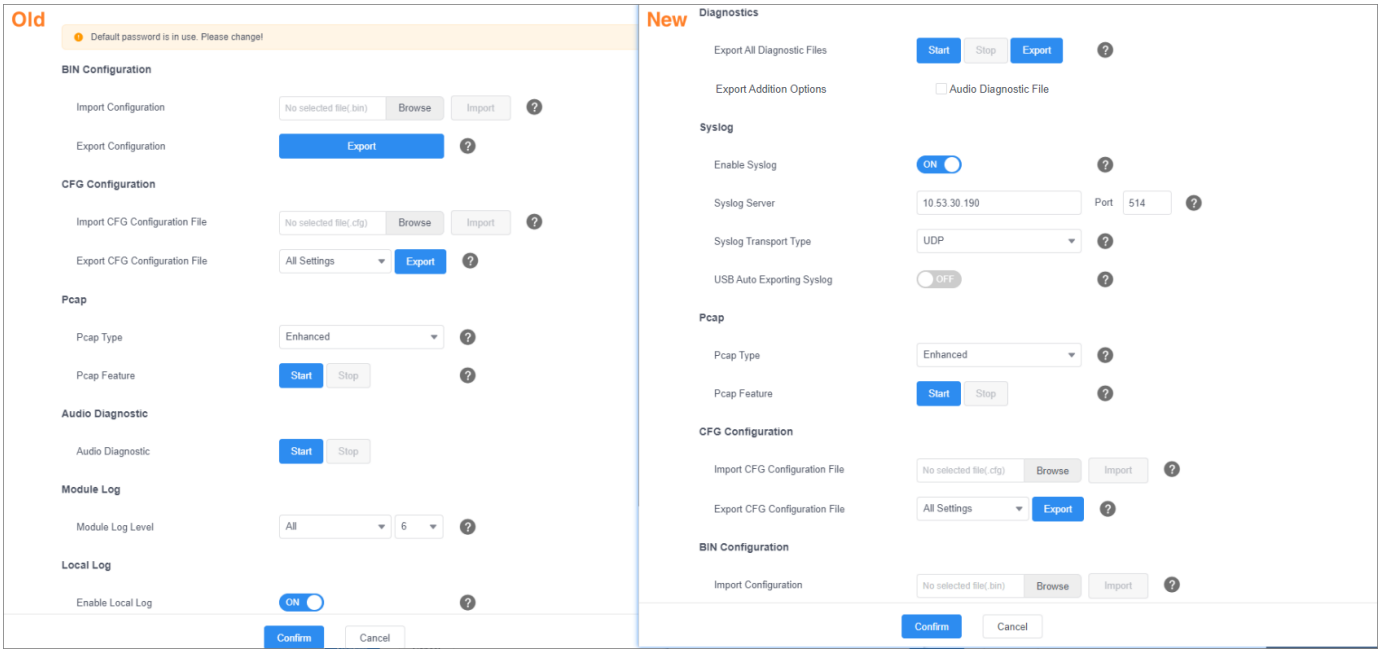
Before you start troubleshooting, it is important to understand the purpose of each file. This section provides an overview of the various diagnostic files and their use in different scenarios. You can go to **Settings** > **Configuration** on the web user interface to check the detailed information.

> When retrieving diagnostic information for troubleshooting, it is crucial to record the timestamp when the issue occurred and communicate it to the technical support team.

Optimize the Configuration Module

Yealink has optimized the Configuration Module on the web user interface. Details are as follows:

- Removed **Module Log Level**, **Local Log**, **Pcap Type**, and **Audio Diagnostic**; all factory defaults are 6.
- Removed **Syslog Level**, **Syslog Facility**, and **Syslog Prepend Mac**.

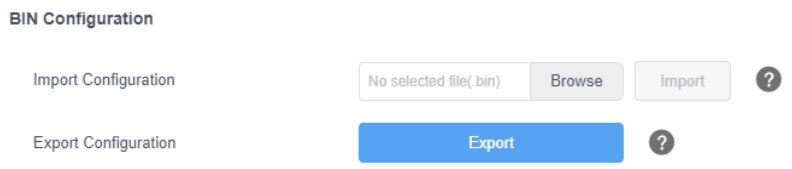


BIN Configuration

The bin file primarily stores the configuration information of the phone, which helps determine if the issue is caused by abnormal configuration parameters.

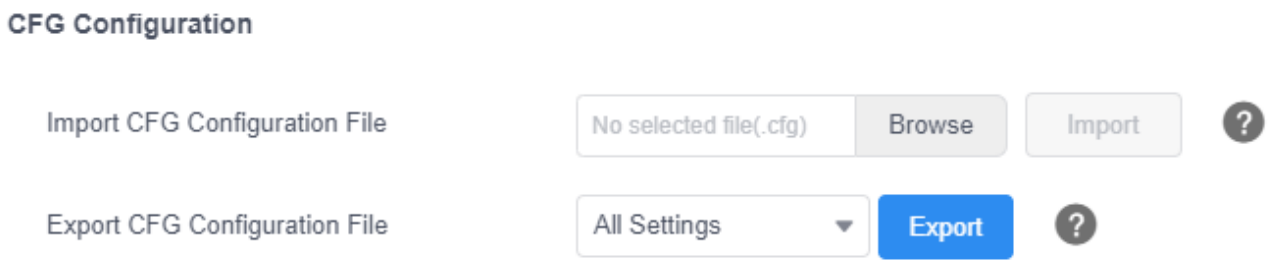
> **Note**
>
> The *.bin file you export may contain some of your personal data, including contacts, history records, web-side login information, etc. If you do not want to export this information, please clear them first on the phone.

You can choose to import or export bin files.



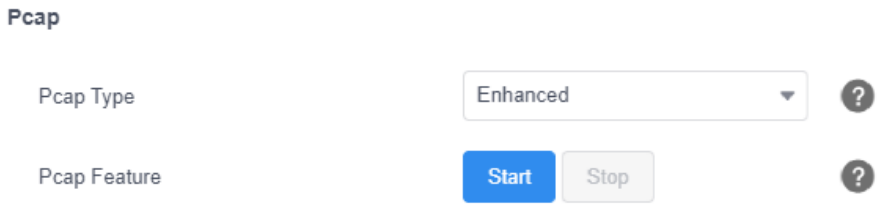
CFG Configuration

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, no sound during calls. It is essential to provide the pcap file to Yealink for troubleshooting purposes.

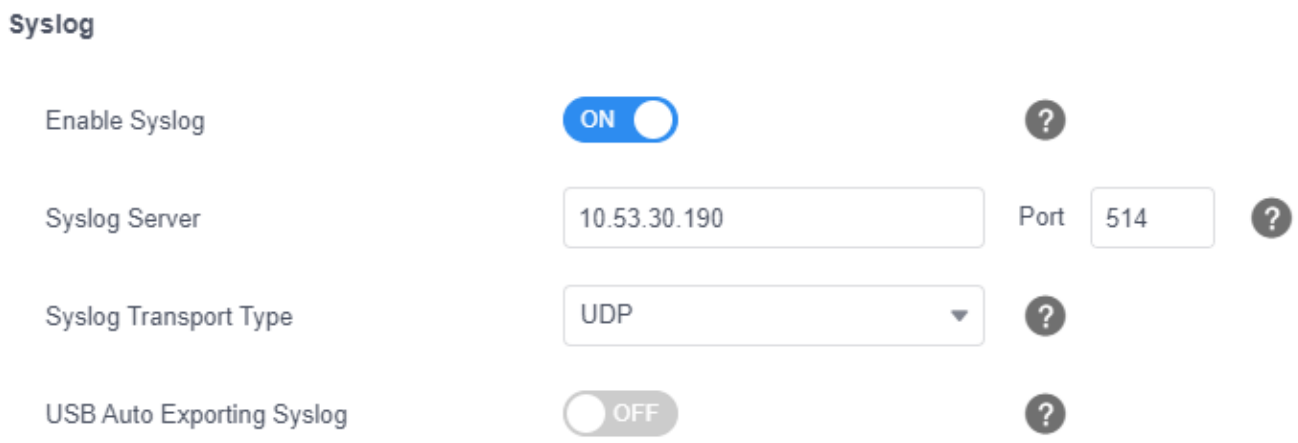


Syslog

Syslog is different from 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 logs 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.

- USB Auto Exporting Syslog: It enables or disables the phone to collect logs using a USB flash drive.



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.

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.

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 issue of being unable to obtain the Audio Diagnostic File along with the Export All Diagnostic Files has been resolved.

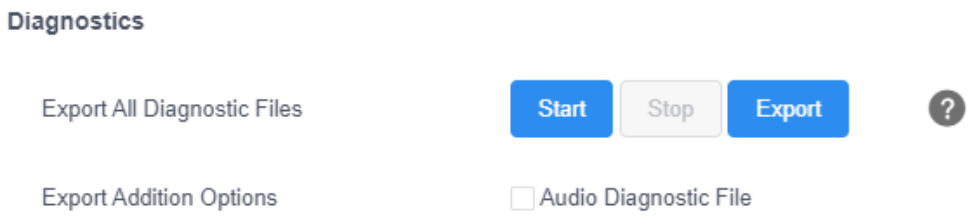
Here are the steps to use this feature:

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.
2. Your Phone version should be x.86.0.112 or later



Log Files

Introduction

You can configure your device to generate the log files locally, upload the log to the USB flash drive connected to the phone, or send the log to a syslog server in real time, and use these log files to generate informational, analytic, and troubleshoot phones.

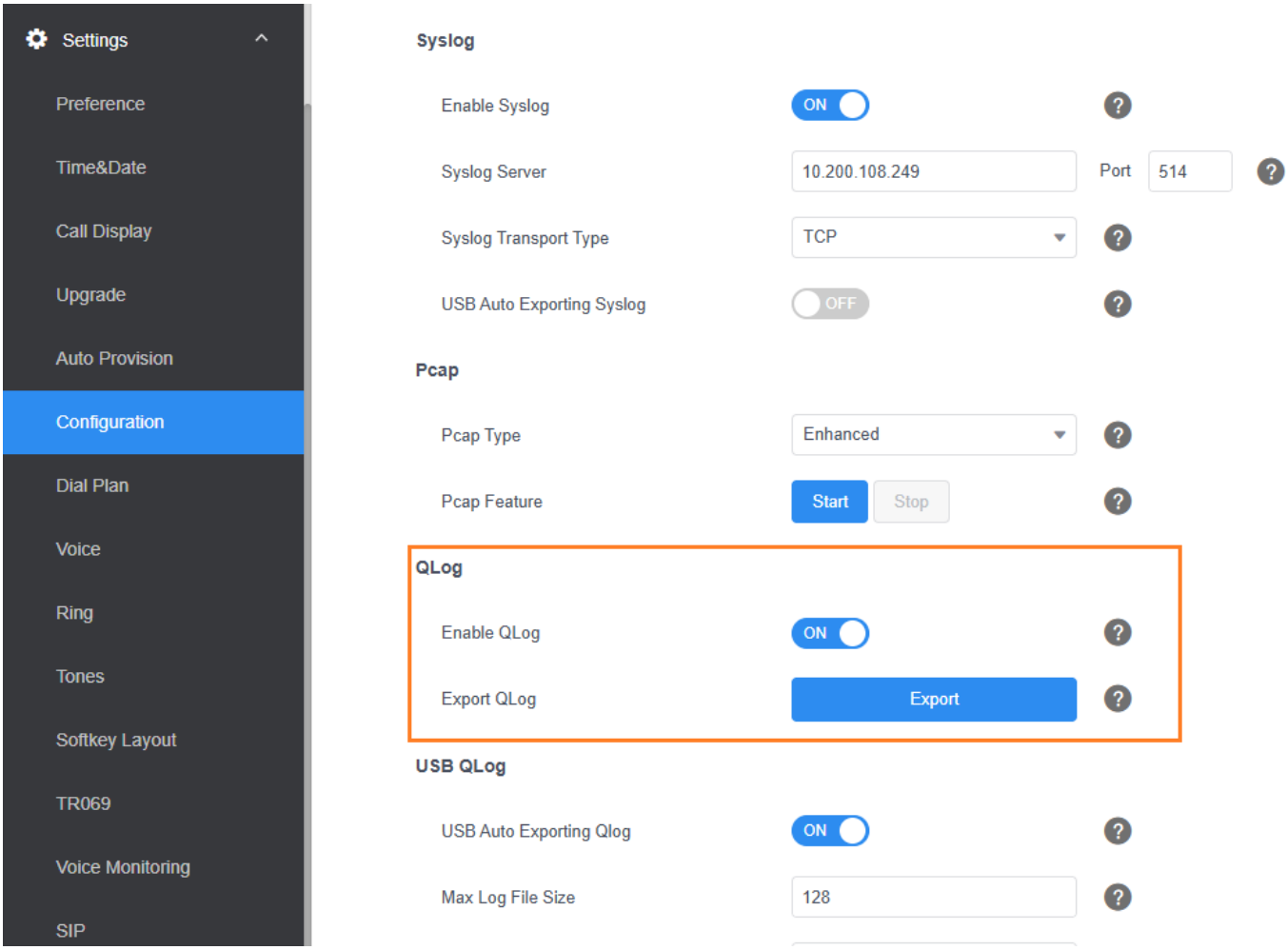
QLog

You can collect the 4G phone module qlog to the local system or a USB flash drive.

QLog Configuration

Set via the Web User Interface

On the web user interface, go to **Settings** > **Configuration** > **QLog** > **Enable QLog**.



Configuration Parameter

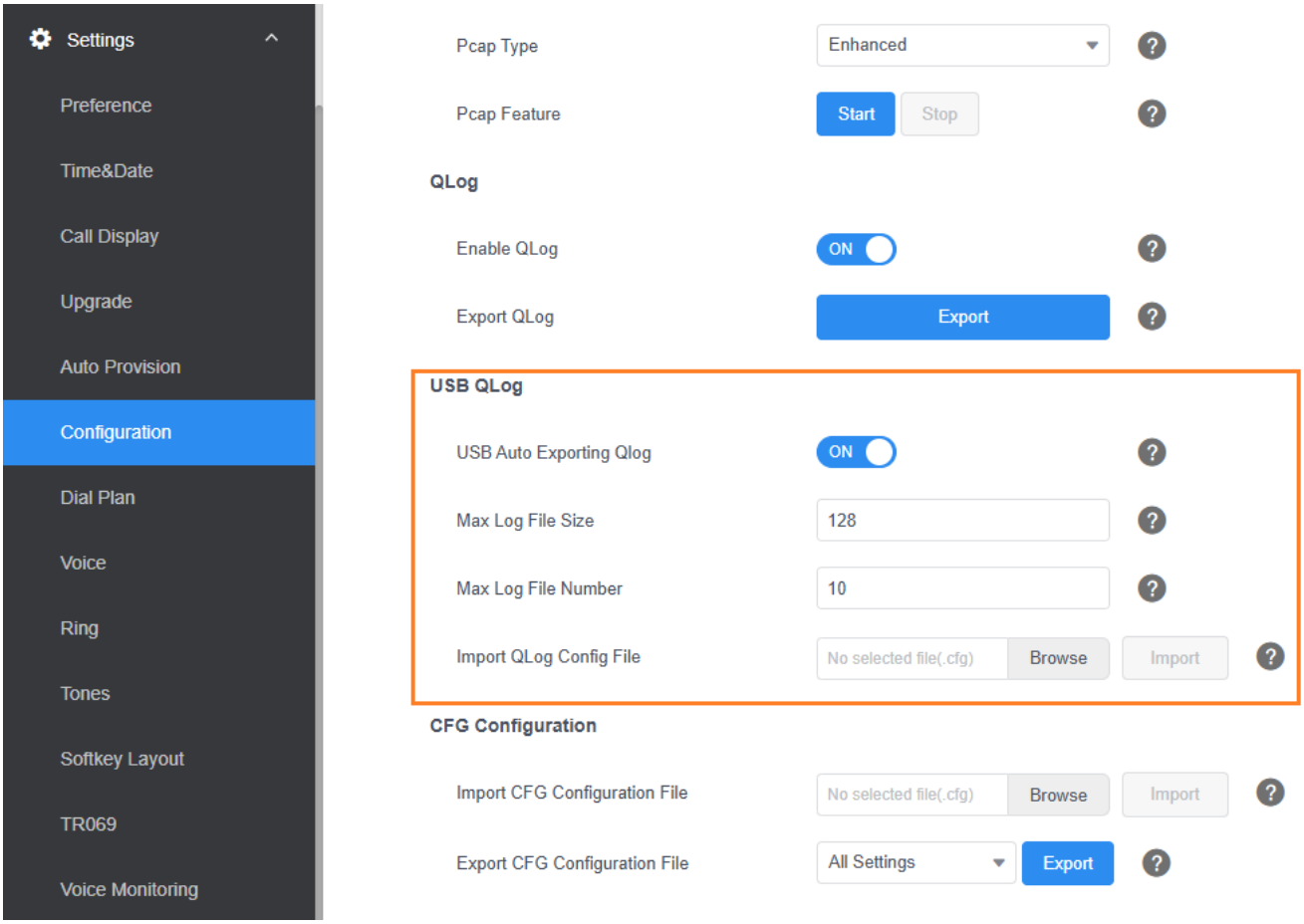
The following table lists the parameters you can use to configure qlog.

Parameter	Permitted Values	Default	Description
qlog.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to record qlog locally.

USB QLog Configuration

Set via the Web User Interface

On the web user interface, go to **Settings** > **Configuration** > **USB QLog**.



Configuration Parameter

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

Parameter	Permitted Values	Default	Description
qlog.usb.enable	**0**-Disabled **1**-Enabled	**0**	It enables or disables the phone to collect qlog using a USB flash drive.
qlog.usb.file_	Integer	**128**	It configures the maximum size (in MB) of the qlog files that

max_size	from **2** to **512**		can be exported to the USB flash drive.
qlog.usb.file_max_num	Integer from **0** to **512**	**0** (unlimited)	It configures the maximum number of qlog files that can be exported to the USB flash drive.
qlog.usb.file_filter_url	String	Blank	It configures the access URL of the qlog filtering configuration file.
qlog.usb.file_filter_delete	http://localhost/all	Blank	It deletes the qlog filtering configuration file.

Export the QLog Files to a Local PC

Procedure

1. From the web user interface, go to **Settings** > **Configuration**.
2. In the **Enable QLog** field, select **ON**.
3. Click **Confirm** to accept the change.
4. Click **Export** to open the file download window, and then save the file to your local system.
5. A diagnostic file named **qlog.tar** is successfully exported to your local system.

Export the QLog Files to the USB Flash Drive

Procedure

1. From the web user interface, go to **Settings** > **Configuration**.
2. In the **USB Auto Exporting QLog** field, select **ON**.
3. Enter the limit size of the qlog files in the **Max Log File Size** field.
4. Enter the limit number of the qlog files in the **Max Log File Number** field.
5. Click **Confirm** to accept the change.
6. From the phone user interface, tap **Qlog Start**.

The phone starts to collect the qlog to the connected USB flash drive and copies the previously collected local qlog files to the USB flash drive under **yealink.qlog** folder.

7. Tap **Qlog Stop** to stop collecting qlog to the USB flash drive.

You can connect the USB flash drive to your PC to export yealink.qlog information.

After using the USB flash drive to collect qlog files, wait for more than ten seconds before unplugging it.

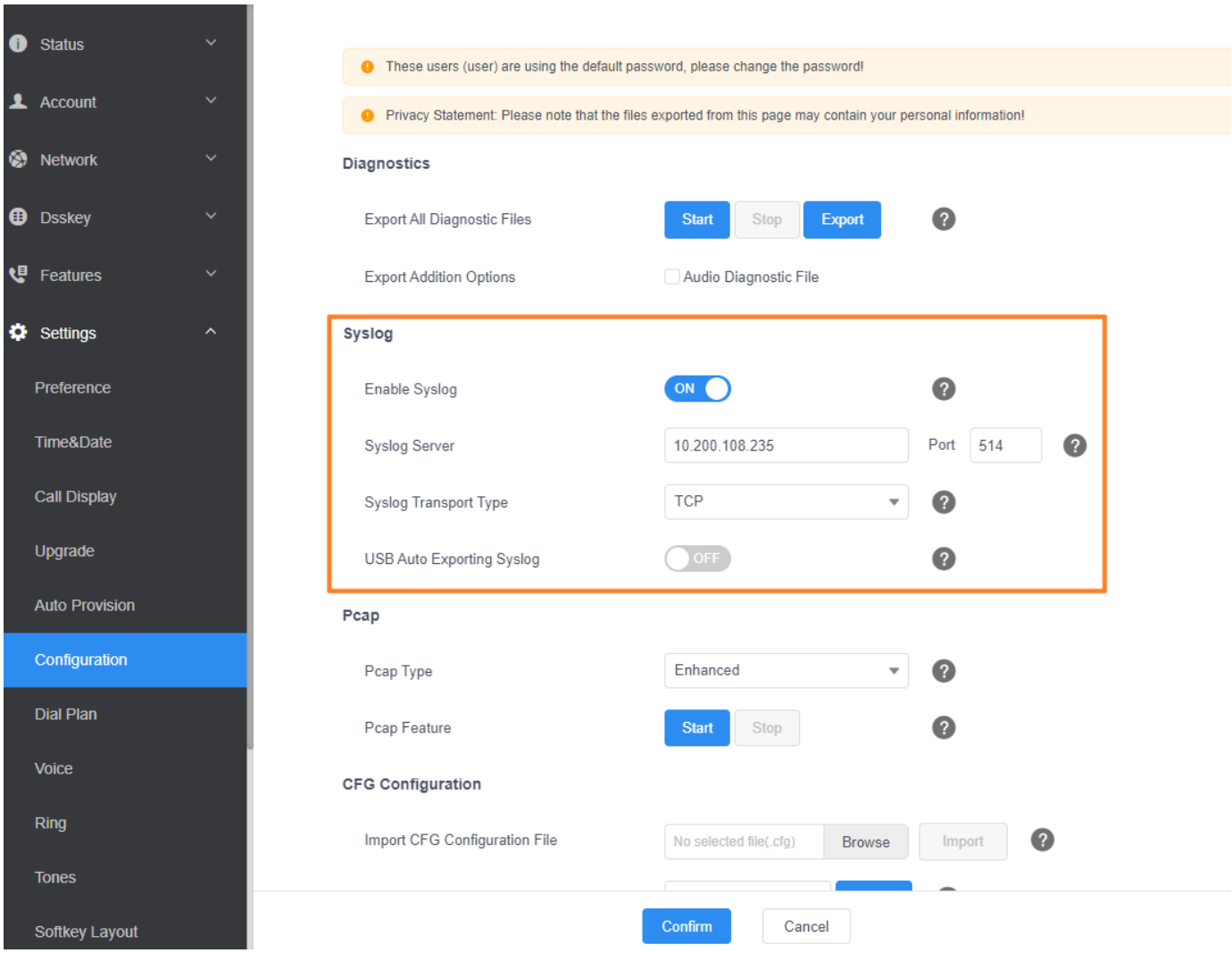
Syslog Logging

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**.



Configuration Parameter

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	Blan k	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_t ype	**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 text 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: ZWQ3MWM5ZDgwZDMyMmZY2JkN2YyMzQ1NTJiNWI5Nzg.
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=4085593836
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=z9hG4bK2209216298
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]
```

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 packets in two ways: by capturing packets via the web user interface or using the Ethernet software.

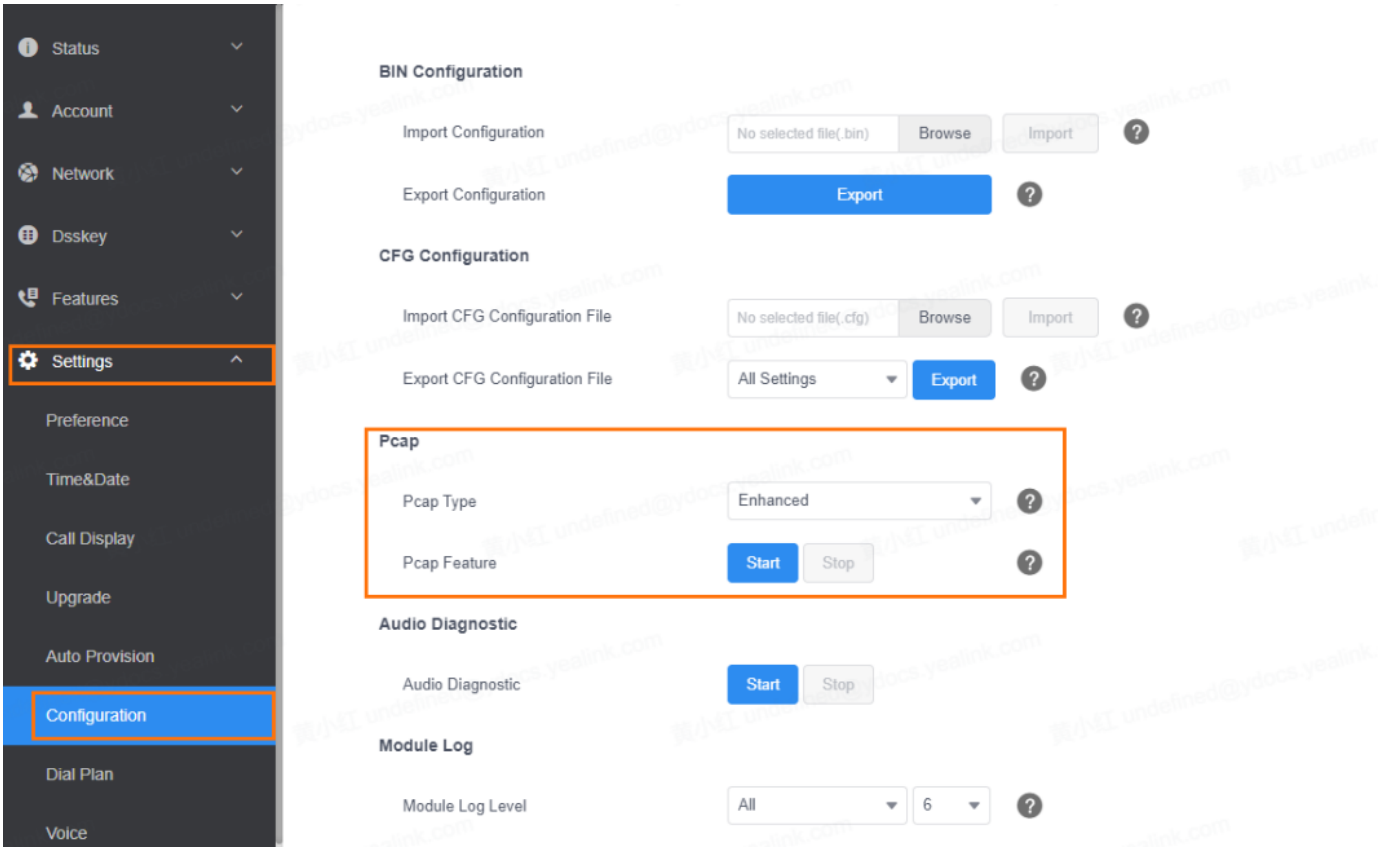
You can analyze the packet captured for troubleshooting purposes.

Capture the Packets via Web User Interface

For Yealink phones, you can export the packet 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 100 KB. You can make an initial assessment of the file's validity based on its size.

96.86.0.70_17_17_21.pcap	2023/6/7 17:17	613 KB
805e0c5cc702-syslog.zip	2023/6/7 17:17	500 KB
config.bin	2023/6/7 17:17	317 KB

FAQ

1. How to Export pcap to Wireshark?

Reset Phone and Configuration

Introduction

Generally, some common issues may occur while using the IP phone. You can reset your phone to factory settings 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.

Five ways to reset the phone:

Options	Description	Note
Reset to Factory	All configurations on the phone will be reset.	/
Reset local settings	All configurations saved in the <MAC>-local.cfg file on the phone will be reset. Changes associated with non-static settings made via the web user interface and phone user interface are saved in the <MAC>-local.cfg file.	The option on the web user interface appears only if "static.auto_provision.custom.protect" is set to 1.
Reset non-static settings	All non-static parameters will be reset. After resetting the non-static settings, the phone will perform auto provisioning immediately.	
Reset static settings	All static parameters will be reset.	
Reset userdata & local config	All the local cache data (for example, user data, history, or directory) will be cleared. And all configurations saved in the <MAC>-local.cfg configuration file on the phone will be reset.	

You can reset the IP phone to its default factory configuration. The default factory configurations are the settings that reside on the IP phone after it has left the factory.

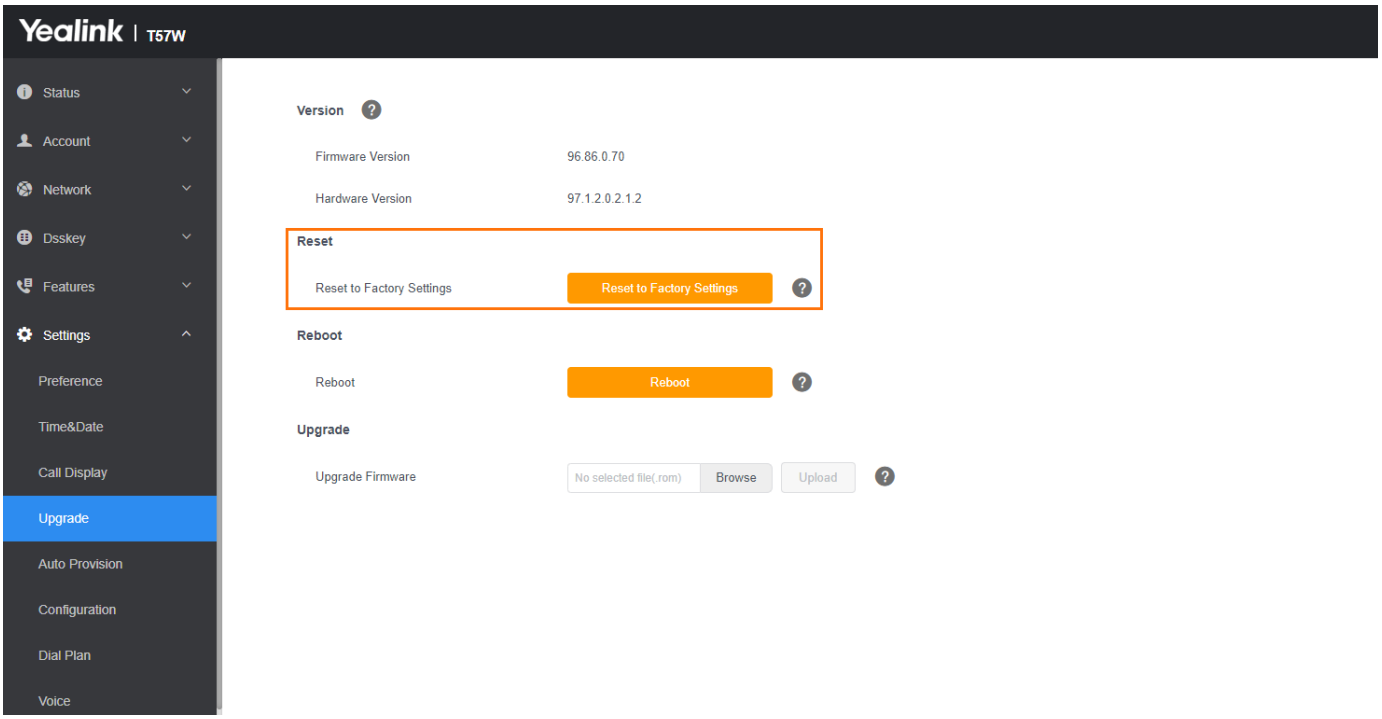
You can also reset the IP phone to custom factory configurations if required. The custom factory configurations are the settings defined by the user to keep some custom settings after resetting. You have to import the custom factory configuration files in advance.

Reset the IP phone to the Default Factory Settings

Procedure

1. Click **Settings** > **Upgrade**.
2. Click **Reset to Factory** 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 reset.
   The phone will be reset to factory settings successfully after startup.

> Resetting your phone may take a few minutes. Do not power off until the phone starts up successfully.

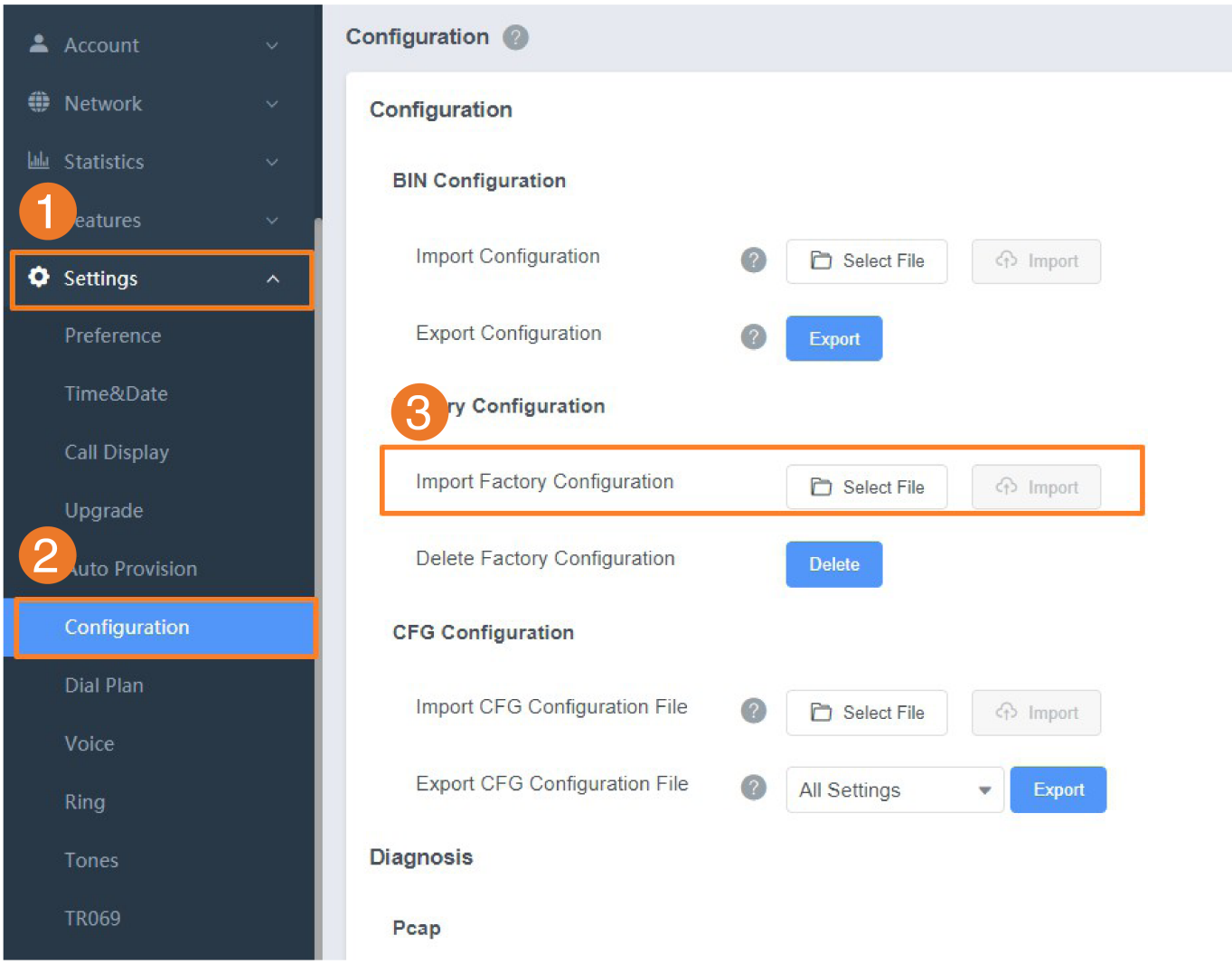


Reset the IP phone to Custom Factory Settings

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

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Configuration** > **Import Factory Configuration**.



Auto Provisioning

static.features.custom_factory_config.enable
static.custom_factory_configuration.url

Parameter	Description	Permitted Values	Default
static.features.custom_factory_config.enable	It enables or disables the Custom Factory Configuration feature.	**0**-Disabled **1**-Enabled, the Import Factory Configuration item will be displayed on the IP phone's web user interface at the path **Settings** > **Configuration**. You can import a custom factory configuration file or delete the user-defined factory configuration via the web user interface.	0

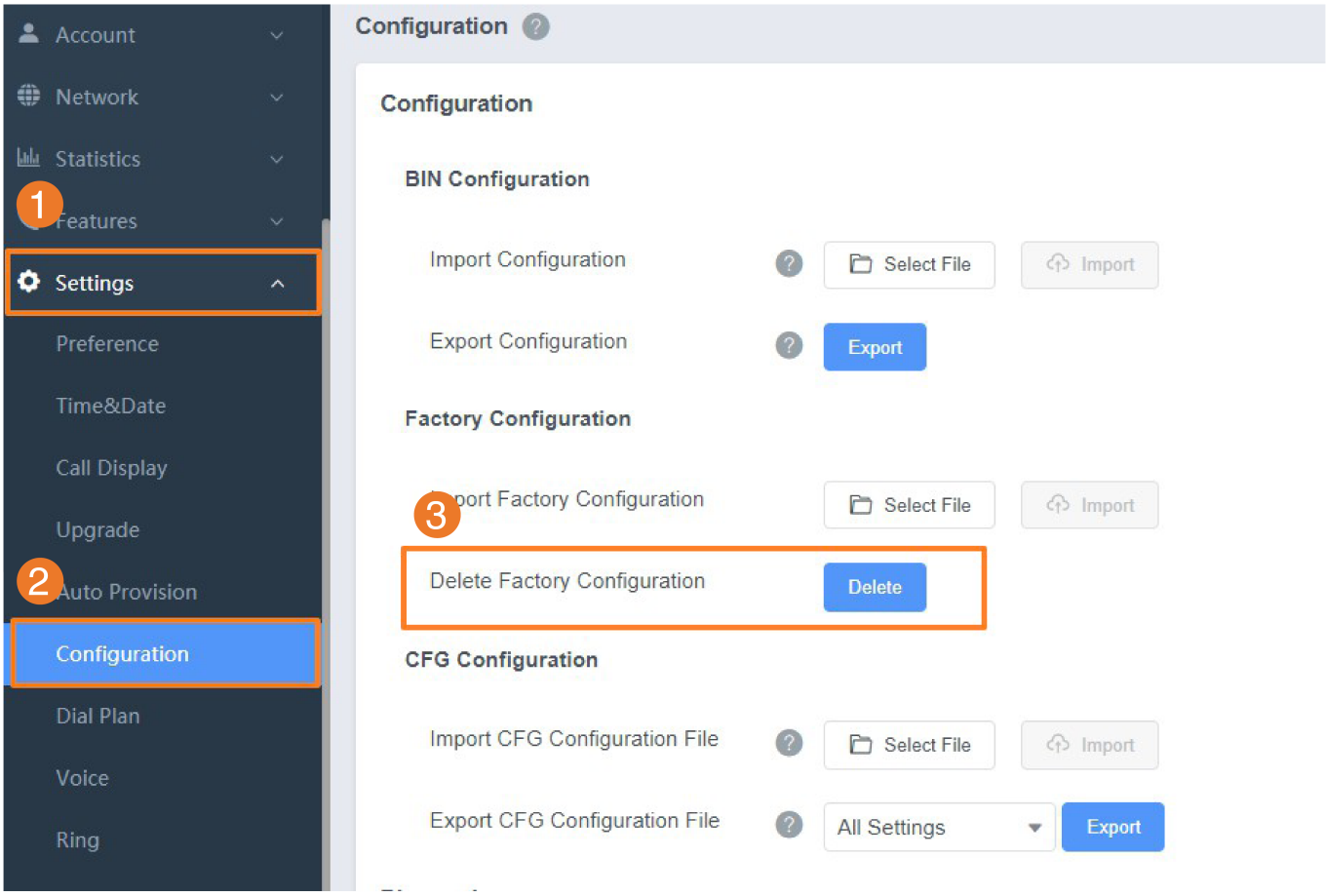
static.custom_factory_configuration.url	It configures the access URL of the custom factory configuration files. It works only if "static.features.custom_factory_config.enable" is set to 1 (Enabled) and the file format of the custom factory configuration file must be *.bin.	URL within 511 characters	Blank

Delete the Custom Factory Settings Files

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

Procedure

1. From the web user interface, click **Settings** > **Configuration**.
2. Click **Del/Delete** in the **Delete Factory Configuration** field.
   The web user interface prompts you whether to delete the user-defined factory configuration.
3. Click **OK** to delete the custom factory configuration files.
   The imported custom factory file will be deleted. The phone will be reset to its default factory settings after resetting.


Account
Network
Statistics
1
Features
Settings
Preference
Time&Date
Call Display
Upgrade
2
Auto Provision
Configuration
Dial Plan
Voice
Ring
Configuration
Configuration
BIN Configuration
Import Configuration
Select File
Import
Export Configuration
Export
Factory Configuration
3
Import Factory Configuration
Select File
Import
Delete Factory Configuration
Delete
CFG Configuration
Import CFG Configuration File
Select File
Import
Export CFG Configuration File
All Settings
Export

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 encrypted. For more information on the config.bin file, contact your Yealink reseller.

Export CFG Configuration Files from Phone

You can export the phone’s configuration file to the local and make changes to the phone’s current feature settings.

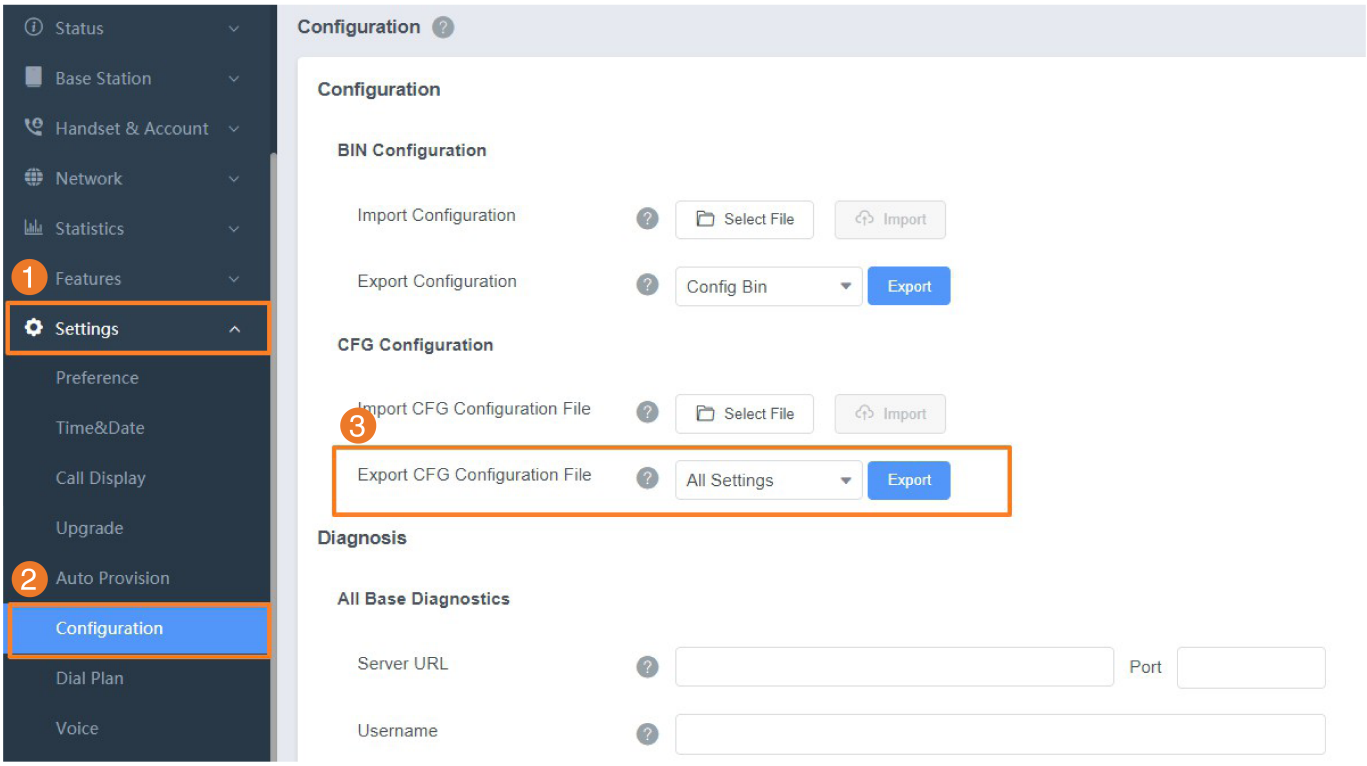
You can apply these changes to any phone by importing the configuration files via the web user interface.

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,e 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.

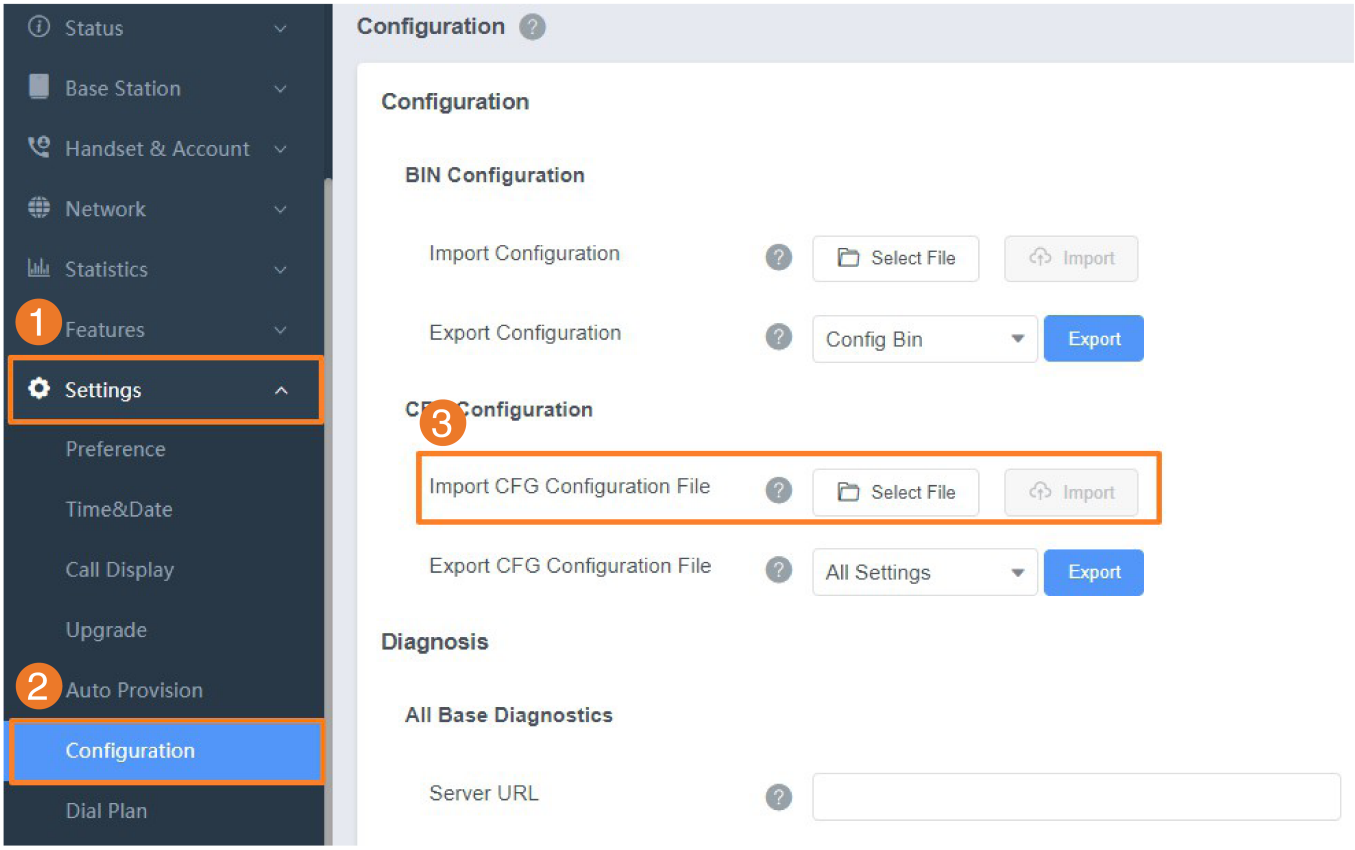


Import CFG Configuration Files to Phone

You can import the configuration files from the 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 import URL.

static.custom_mac_cfg.url

Parameter	Description	Permitted Values	Default
static.custom_mac_cfg.url	It configures the access URL of the custom MAC-oriented CFG file.	URL within 511 characters	Blank

Export BIN Files from the Phone

Procedure

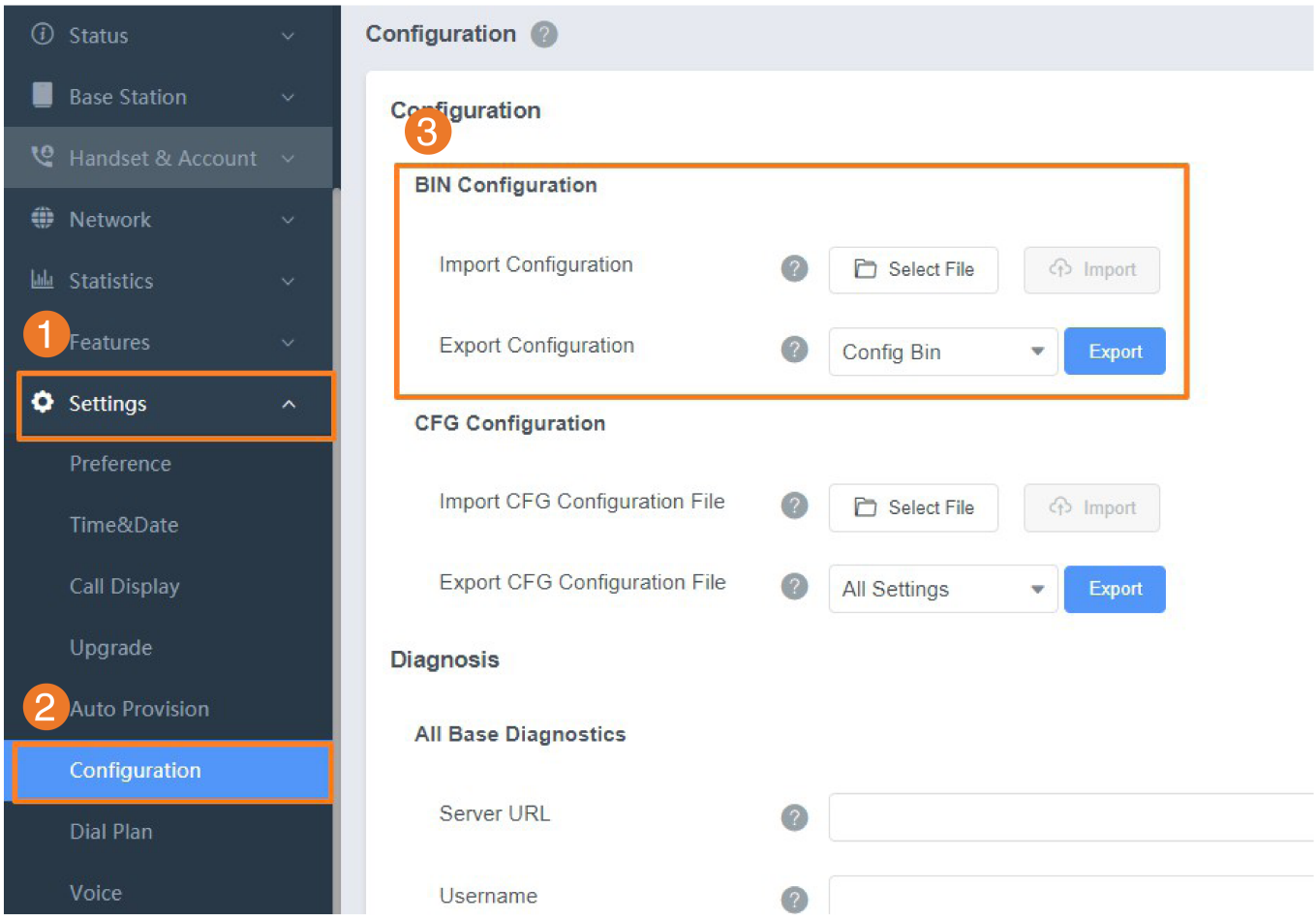
1. From the web user interface, click **Settings** > **Configuration** > **BIN Configuration**.
2. In the **Export Configuration** field, click **Export** to open the file download window, and then save the file to your local system.

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	Description	Permitted Values	Default
static.configuration.url[1]	It configures the access URL for the custom configuration files. The file format of the custom configuration file must be *.bin.	URL within 511 characters	Blank

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

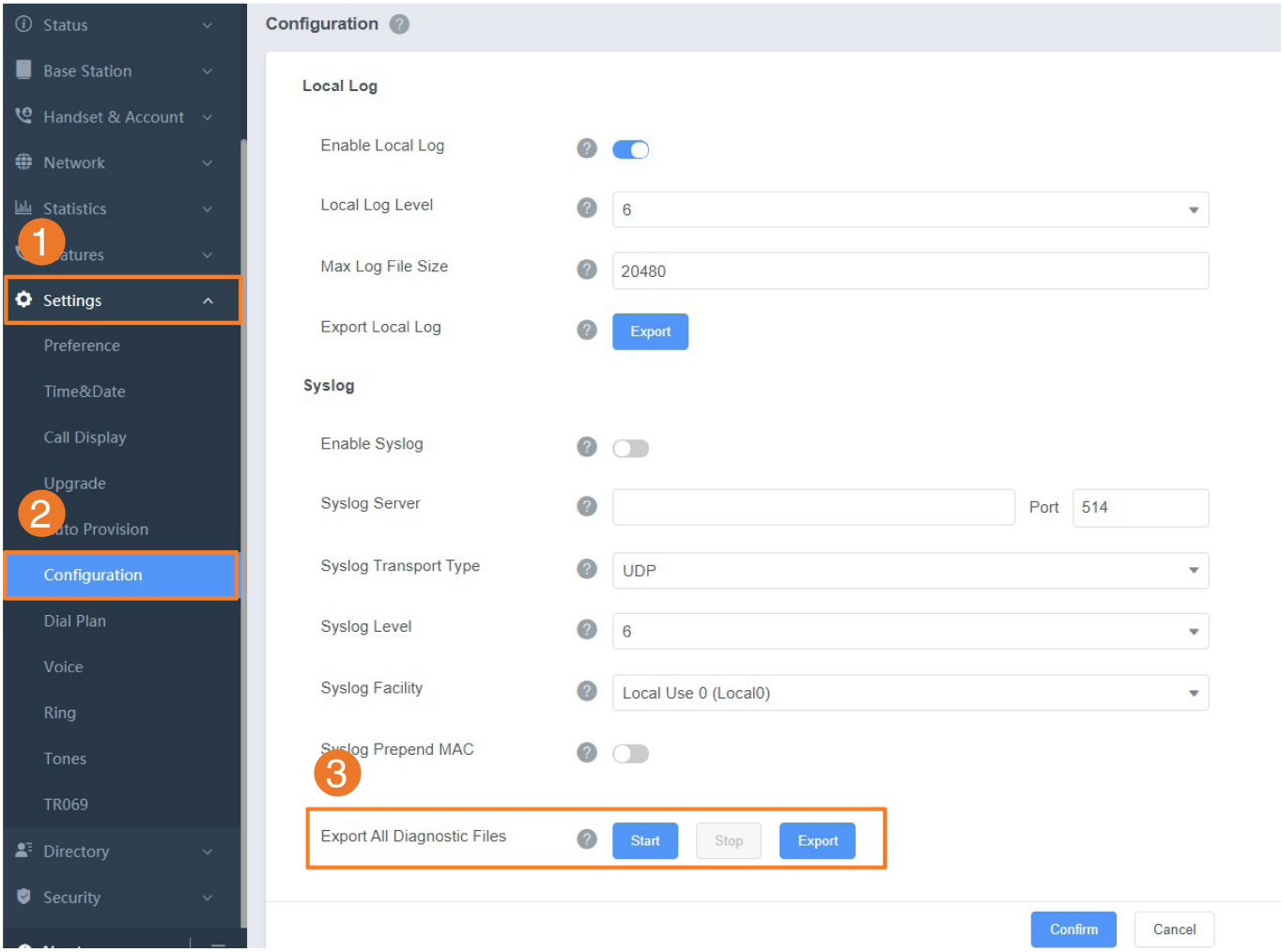
Export All the Diagnostic Files

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.

> "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.

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.

FAQ

1. How to Get Correct Diagnostic Files from Yealink Phones?

Watch Dog

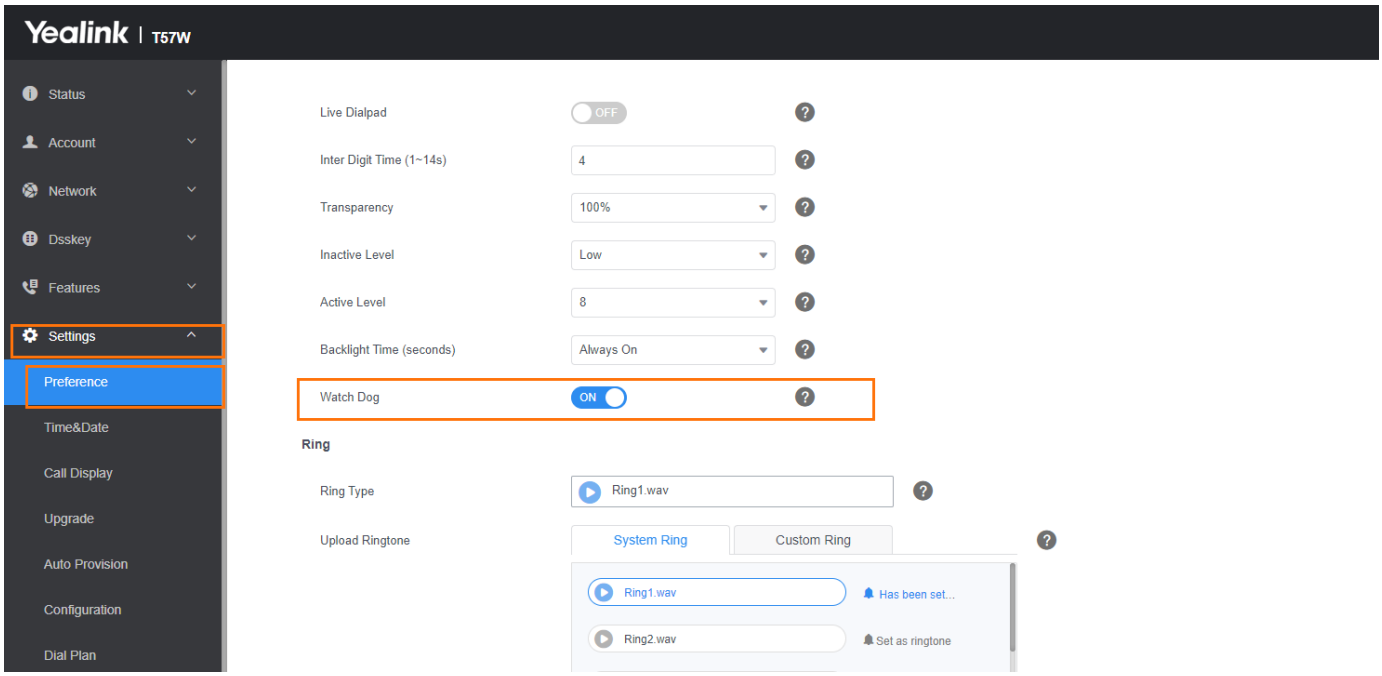
Introduction

The IP phone provides a troubleshooting feature called “Watch Dog”, which helps you monitor the IP phone status and provides the ability to get stack traces from the last time the IP 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	Description	Permitted Values	Default
static.watch_dog.enable	It enables or disables the watchdog feature.	**0**-Disabled **1**-Enabled, the phone will reboot automatically when the system crashes.	1

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 IP phone remotely or locally.

Reboot the IP Phone Remotely

You can reboot the phones remotely using a SIP NOTIFY message with the “Event: check-sync” header. Whether the IP phone reboots or not depends on [redacted]. 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 IP phone's behavior when receiving a SIP NOTIFY message that contains the header “Event: check-sync”.

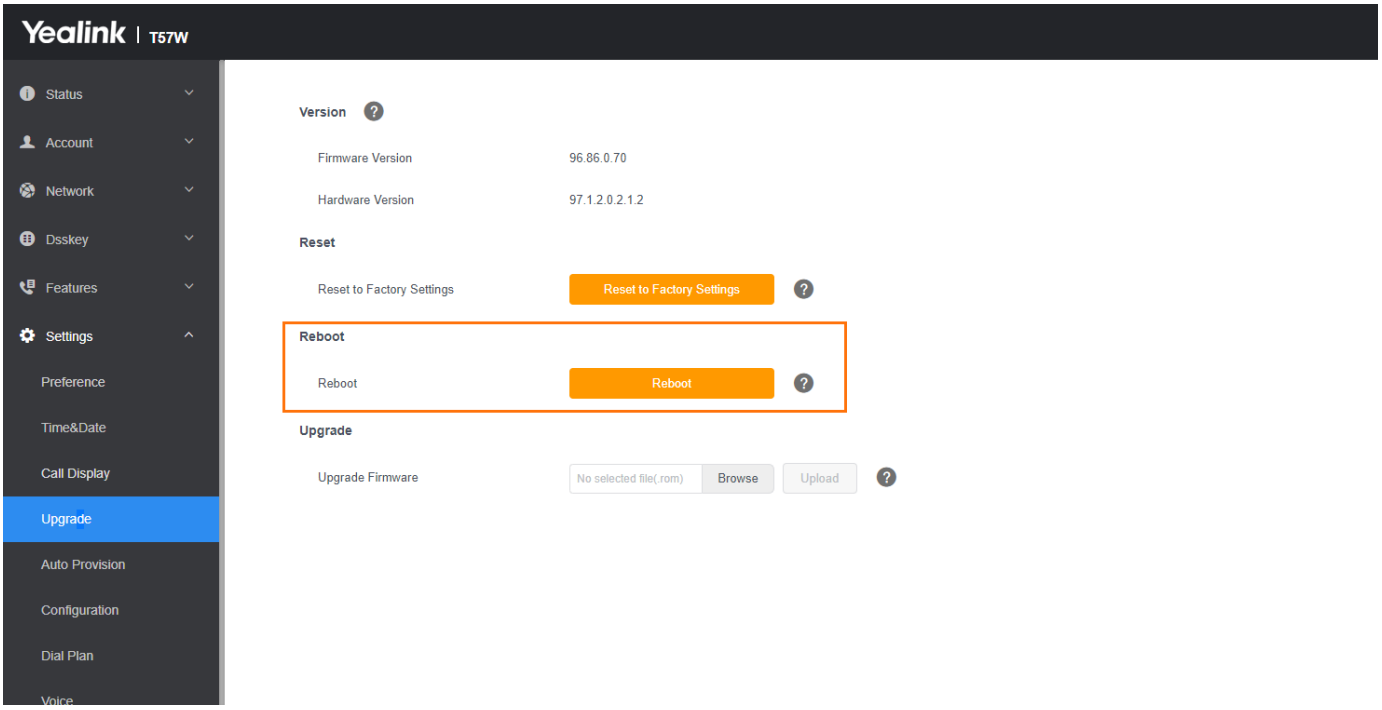
Reboot the Device via Web User Interface

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.



Auto Reboot

The phone supports scheduled reboots in Version 87 and later versions. After configuring **Auto Reboot**, a reboot countdown prompt will pop up on the phone 30S before the set time is reached. If you choose **Reboot** Immediately, the phone will reboot immediately; if you choose **Cancel**, the reboot will be automatically postponed to the next cycle; if no operation is performed, it will reboot after the countdown is over.

> If the phone is on a call or upgrading (including downloading firmware) during the set reboot time, the auto reboot cannot be triggered, and the reboot process will be postponed to the next cycle to take effect.

Auto Provisioning

features.auto_task.x.enable
features.auto_task.x.type
features.auto_task.x.time
features.auto_task.x.weekday

Parameter	Description	Permitted Values	Defaul

			t
features.auto_task.x.enable	Scheduled tasks, indicating whether the xth task is enabled.	0-Disabled 1-Enabled	0
features.auto_task.x.type	Scheduled tasks, indicating the type of the xth task.	reboot	Blank
features.auto_task.x.time	Scheduled tasks, indicating the start time of the xth task.	hh:mm hh:mm-hh:mm (Execute the task at a random time within this time range.)	Blank
features.auto_task.x.weekday	Scheduled tasks, indicating the weekly execution cycle of the xth task.	Integer from 1-7	Blank

Example of Troubleshooting

This chapter will demonstrate troubleshooting methods through several common examples.

> 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.

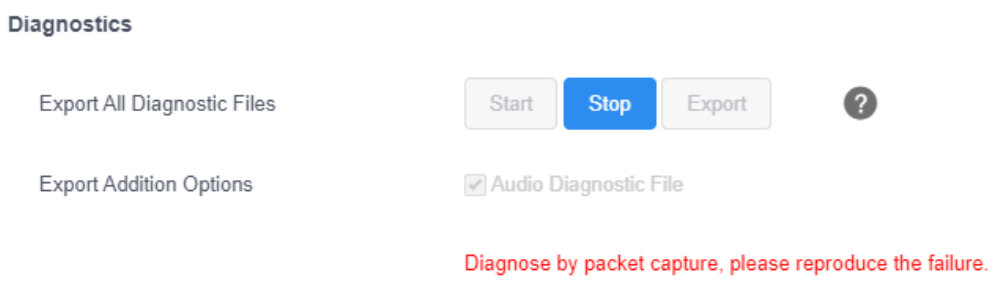
If the above objective reasons do not apply, please follow the steps below to provide the necessary information.

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

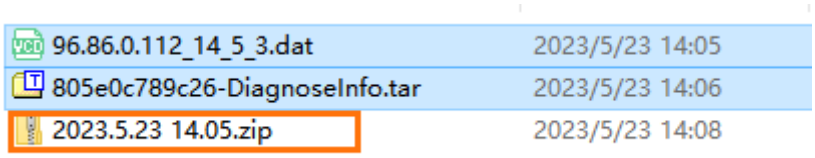
hear B's voice, and the same issue occurs when B calls A, with A still unable to hear B's voice.

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:

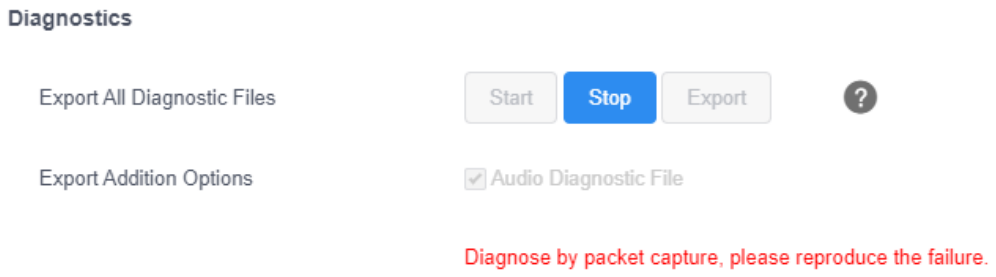
1. Determine the number of devices involved and whether the issue is specific to a single device or a few devices.
2. Verify if the volume settings are appropriate, avoiding excessively high or low volume levels.
3. Check if both parties are speaking simultaneously. If so, a decrease in volume is a normal occurrence due to duplex suppression.
4. Try an IP call to test the audio quality. If the audio quality is normal during an 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:

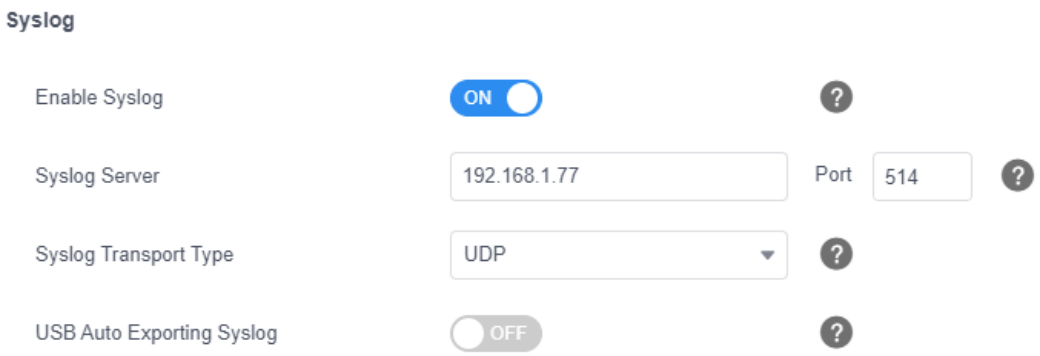
1. The device restarts abruptly without any user intervention.
2. Regular and scheduled restarts at fixed intervals.

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. Similarly, you can also use a USB drive to capture USB logs. Please note that the USB drive should be formatted in FAT32 format. This method is only applicable to devices that have a USB port.
3. After encountering the issue, wait for the device to successfully boot up and then export the local log. If you have a version prior to x.86.0.112, make sure to modify the log level to 6 before starting the first step. Once you have reproduced the issue, click "Export" to export the local log. If you have

a version from x.86.0.112 or later, you can directly click on "Export" of "Export All Diagnostic Files" on the web page.

4. Please compress the syslog 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.

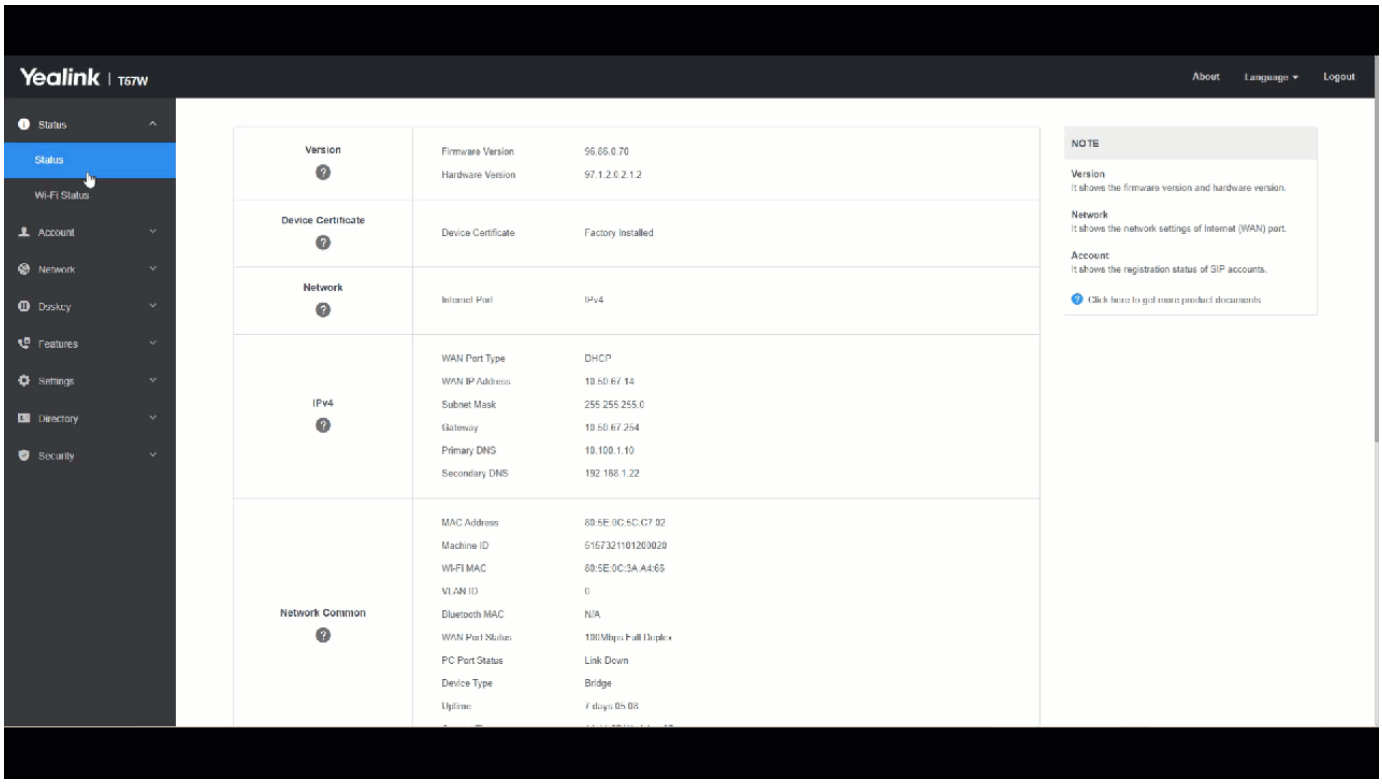
Troubleshooting Network Issues

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. An incorrect address 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. **example：**



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 local log and include the syslog.
3. If your device restarts during this process, please provide a video of the phenomenon if possible.

Device cannot obtain an IP address troubleshooting:

Your device is unable to obtain an IP address for an extended period of time after connecting to the network via Ethernet or Wi-Fi.

To troubleshoot these issues, you can follow these steps:

1. Please check if your DHCP server's address pool is full.
2. Verify if your network environment has any restrictions, such as MAC address filtering, device type restrictions, or firewall limitations.
3. Determine if your environment requires 802.1x authentication and if the device has successfully passed the 802.1x authentication.
4. Verify if the device has sent out a DHCP Discover message by checking your DHCP server.
5. Example of normal DHCP Process：

No.	Time	Source	Destination	Protocol	Length	Info
2884	60.911426	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0xe6f2416d
2885	60.922997	10.81.5.254	10.81.4.119	DHCP	405	DHCP Offer - Transaction ID 0xe6f2416d
2887	60.971766	0.0.0.0	255.255.255.255	DHCP	590	DHCP Request - Transaction ID 0xe6f2416d
2888	60.986424	10.81.5.254	10.81.4.119	DHCP	405	DHCP ACK - Transaction ID 0xe6f2416d
2890	61.049361	10.82.22.30	255.255.255.255	DHCP	450	DHCP Offer - Transaction ID 0xe6f2416d
2891	61.050388	10.82.22.30	255.255.255.255	DHCP	450	DHCP Offer - Transaction ID 0xe6f2416d
3413	65.261205	10.81.4.119	255.255.255.255	DHCP	590	DHCP Inform - Transaction ID 0xe6f2416d
3414	65.270328	10.100.1.21	10.81.4.119	DHCP	394	DHCP ACK - Transaction ID 0xe6f2416d
3416	65.373927	10.82.22.30	10.81.4.119	DHCP	450	DHCP ACK - Transaction ID 0xe6f2416d
3779	68.331210	10.81.4.119	255.255.255.255	DHCP	590	DHCP Inform - Transaction ID 0xe6f2416d
3781	68.342005	10.100.1.21	10.81.4.119	DHCP	394	DHCP ACK - Transaction ID 0xe6f2416d
3785	68.447134	10.82.22.30	10.81.4.119	DHCP	450	DHCP ACK - Transaction ID 0xe6f2416d

5. Please check if your VLAN is configured correctly. You can verify this by manually setting a static VLAN to see if it functions properly. When setting a static VLAN, ensure that all dynamic VLAN configurations are disabled. You can configure the phone as follows:
6. network.lldp.enable=0 network.cdp.enable=0 network.vlan.dhcp_enable=0

Steps for Obtaining Diagnostic Information:

The process for obtaining diagnostic files in this scenario is different since the device is not yet connected to the network and cannot access the web interface. Therefore, the method for retrieving the files is as follows:

Preparation:

1. Access the device's web interface in a normal network environment and set the local log level to 6. It is recommended to enable USB syslog.
2. Connect the device to a power adapter and ensure that the device remains powered on during the troubleshooting process.

Steps:

1. With the device connected to the power adapter, insert the network cable into the device in the problematic network.
2. If the device has a USB port, insert a USB drive (FAT32 formatted) into the device's USB port. (Skip this step if the device does not have a USB port.)
3. Without disconnecting the power adapter, replace the current network cable with a known working network cable that can successfully obtain network connectivity.
4. Log in to the device's web interface and export the local log and Bin files.

Troubleshooting Video Issues

Unable to establish a video call.

Symptoms:

1. Yealink video phones cannot establish video calls with other Yealink video phones. Only audio can be heard, but no video is visible.
2. Yealink video phones cannot establish video calls with video phones from other brands.

Possible causes:

1. One party in the video call negotiation process did not carry a video codec.
2. One party does not support the video codec used by the other party.
3. Video negotiation port is set to 0, causing an abnormality.

Initial solutions:

1. You can check if it is a codec negotiation issue. You can adjust the device's codec through the web interface to ensure that both parties have the same video codec.
2. Verify if the server associated with the account bound to the device supports video calls.
3. Try changing the video negotiation codec on both sides of the call.

Steps for Obtaining Diagnostic Information:

1. Please export diagnostic files for both parties involved in the issue and for the parties who can establish video calls with other devices (Export All Diagnostic Files).

2. For the parties experiencing the video call issue, please ensure that the accounts are the same and the diagnostic files can be matched accordingly.

Video call issues such as screen distortion, black screen, and pixelation:

Common problem symptoms:

1. Video call starts normally but experiences intermittent freezing or screen distortion during the call.
2. When establishing a call with non-Yealink video devices, there are persistent screen distortion and pixelation issues.

Common causes and solutions:

1. If you experience occasional freezing or screen distortion during video calls, it is likely due to packet loss in the network. The most common causes of packet loss are insufficient bandwidth and router issues.
2. When encountering screen distortion and pixelation issues with non-Yealink devices, the most common cause is the PBX's lack of support for Yealink codecs, resulting in transcoding issues or abnormal keyframe requests and transmission. You can try disabling Yealink's proprietary codec capabilities and then reattempting the call:
3. Set "account.1.media.capset=%EMPTY%" in the device's configuration.
4. Enable the option "features.reset_mediacapset_after_reboot.enable=1".

Steps for Obtaining Diagnostic Information:

1. Please export diagnostic files for both parties involved in the issue and for the parties who can establish video calls with other devices (Export All Diagnostic Files).

2. For the parties experiencing the video call issue, please ensure that the accounts are the same and the diagnostic files can be matched accordingly.

Recovery Mode

Introduction

When encountering a phone upgrade failure, the restoration of the upgrade is achieved through a recovery mode.

- The recovery mode upgrade encompasses three methods: TFTP, HTTP, and USB drive.
- For USB drive upgrade: Store the boot file and ROM on a USB drive, and forcefully upgrade the phone while simultaneously restoring it to its factory settings.

Solution:

For single system products such as T4XG, T29G, and W52B (earliest recovery mode solution): Two boot files (.rfs, .bin) and the ROM package need to be placed on the server.

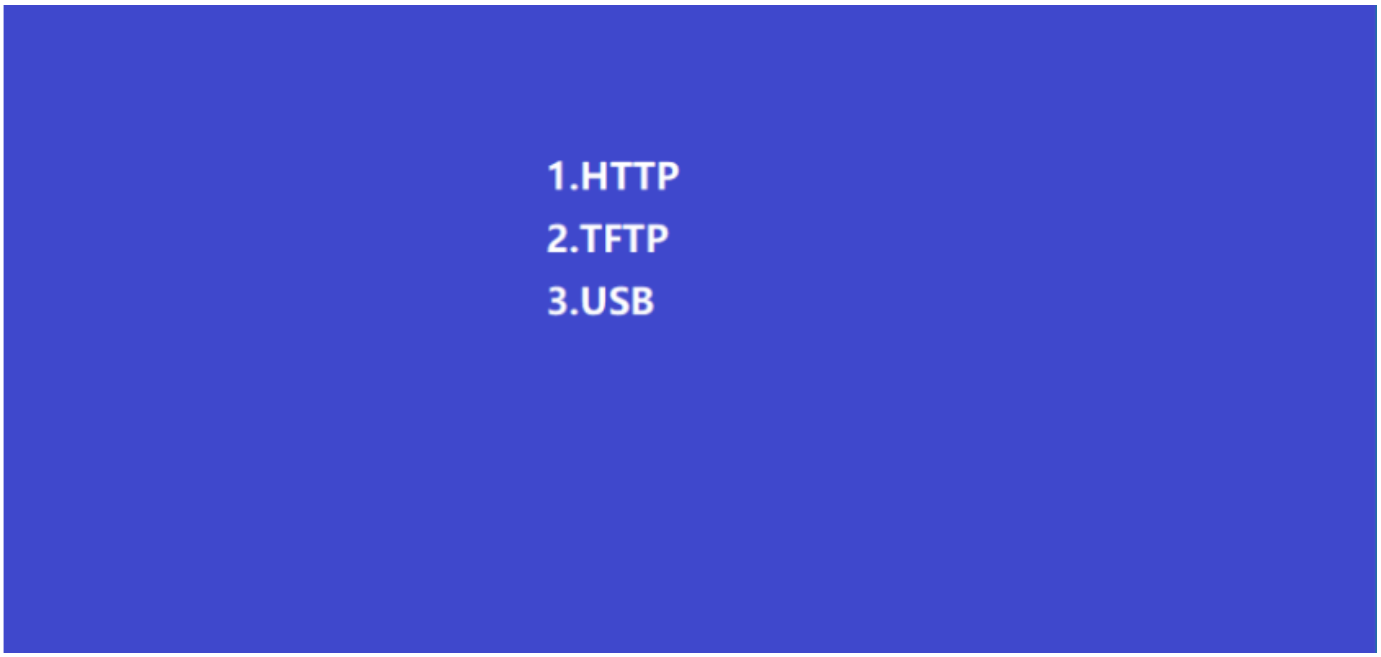
For secure system products like T27G, T3X, T4XS, T58, CP960, and CP920: Similar to the earliest recovery mode solution, the difference lies in the fact that users no longer require two boot files (.rfs, .bin). Instead, they just need to place the ROM package for restoration.

For dual system products such as T4XU, T5XW, VP59, W60B, W80B, and future new models: These products adopt a dual system solution. To enter recovery mode, simply launch the backup system, and selecting "Yes" will initiate the self-restoration process.

Enter Recovery Mode

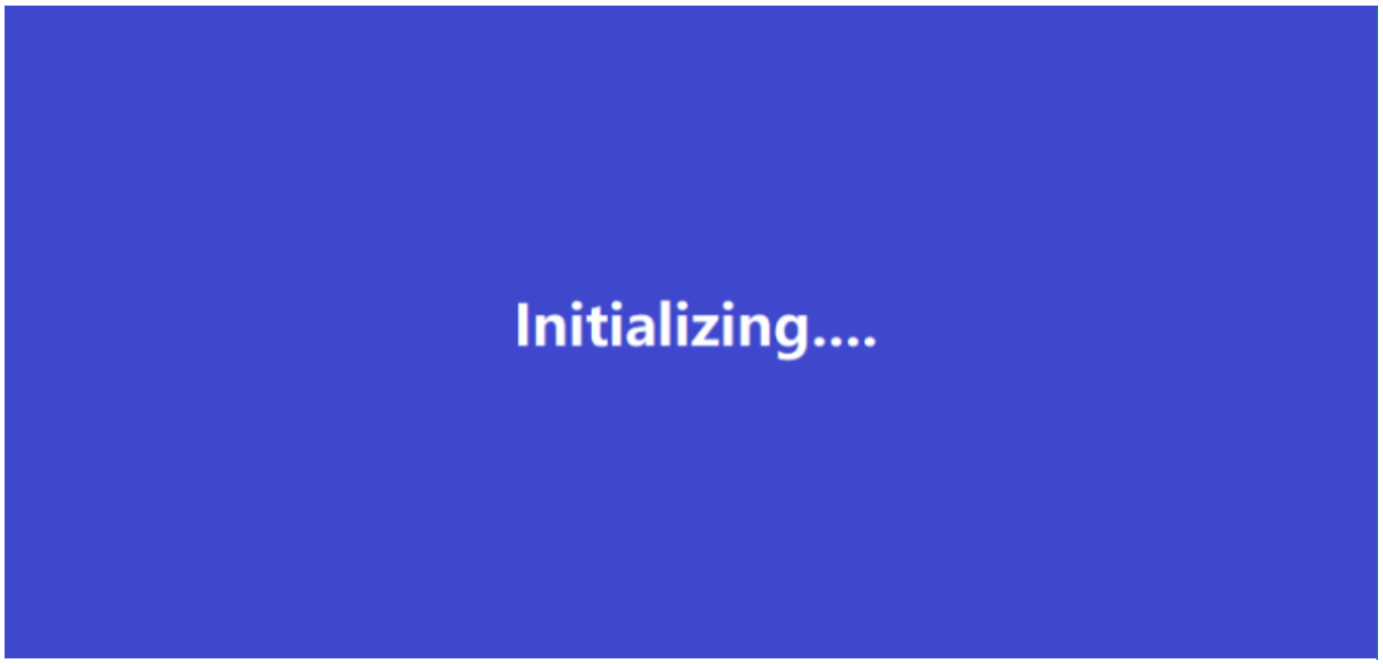
Single System

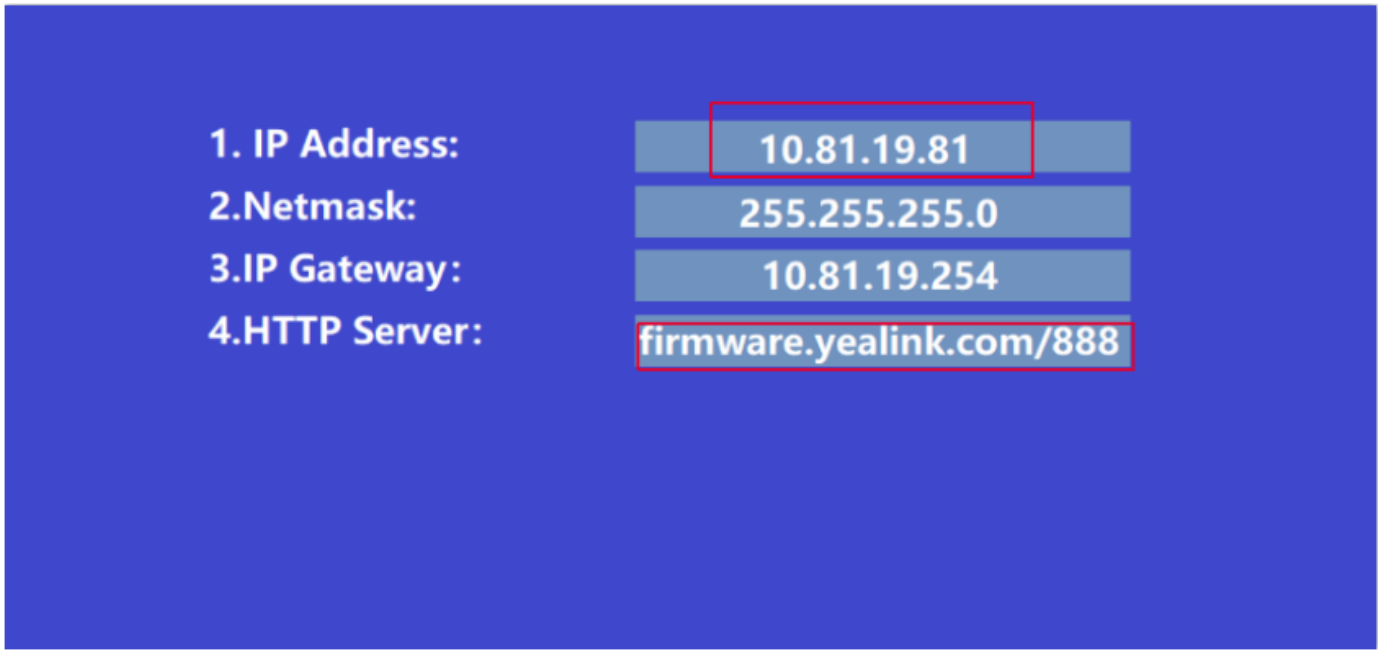
Press and hold the speakerphone button while powering on the device to enter the recovery mode interface, as shown in the below:



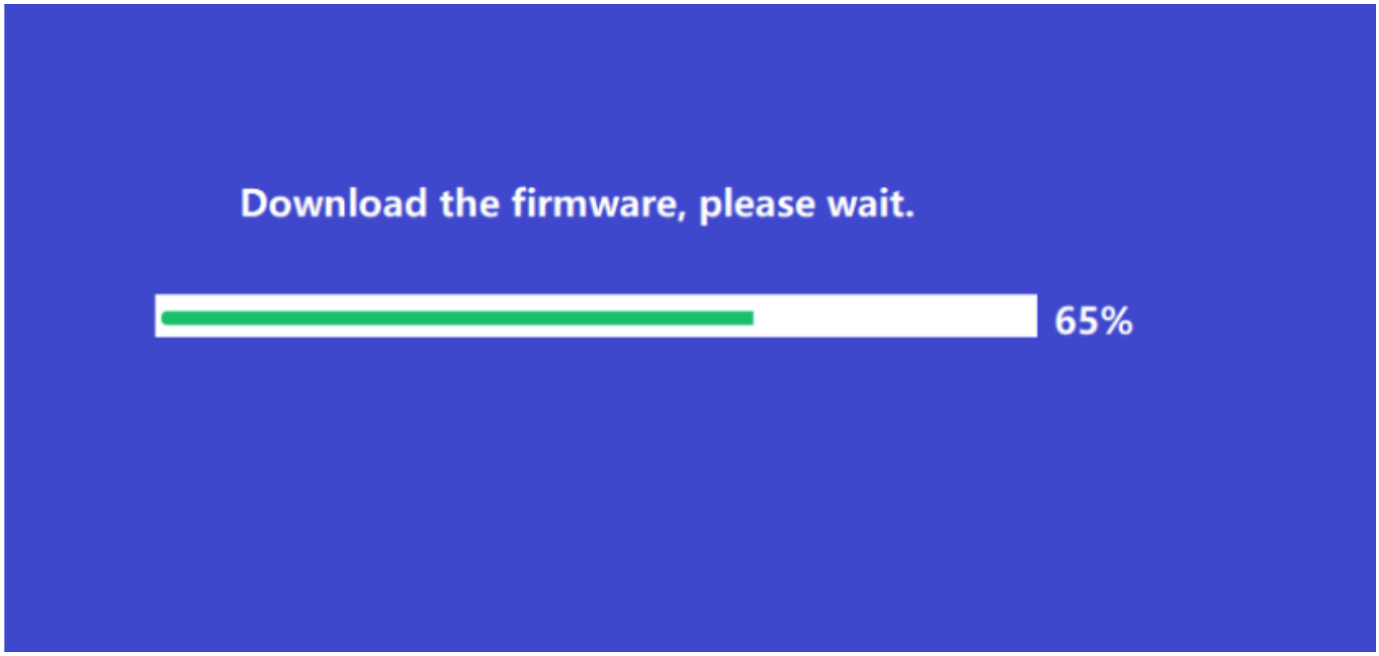
HTTP

1. Place the XX.rom file on the HFS server.
2. Press and hold the speakerphone button while powering on the device to enter the recovery mode interface. Then, press **1** to select the HTTP method. You will first enter the initialization interface and then proceed to the IP configuration interface, as shown in the below:

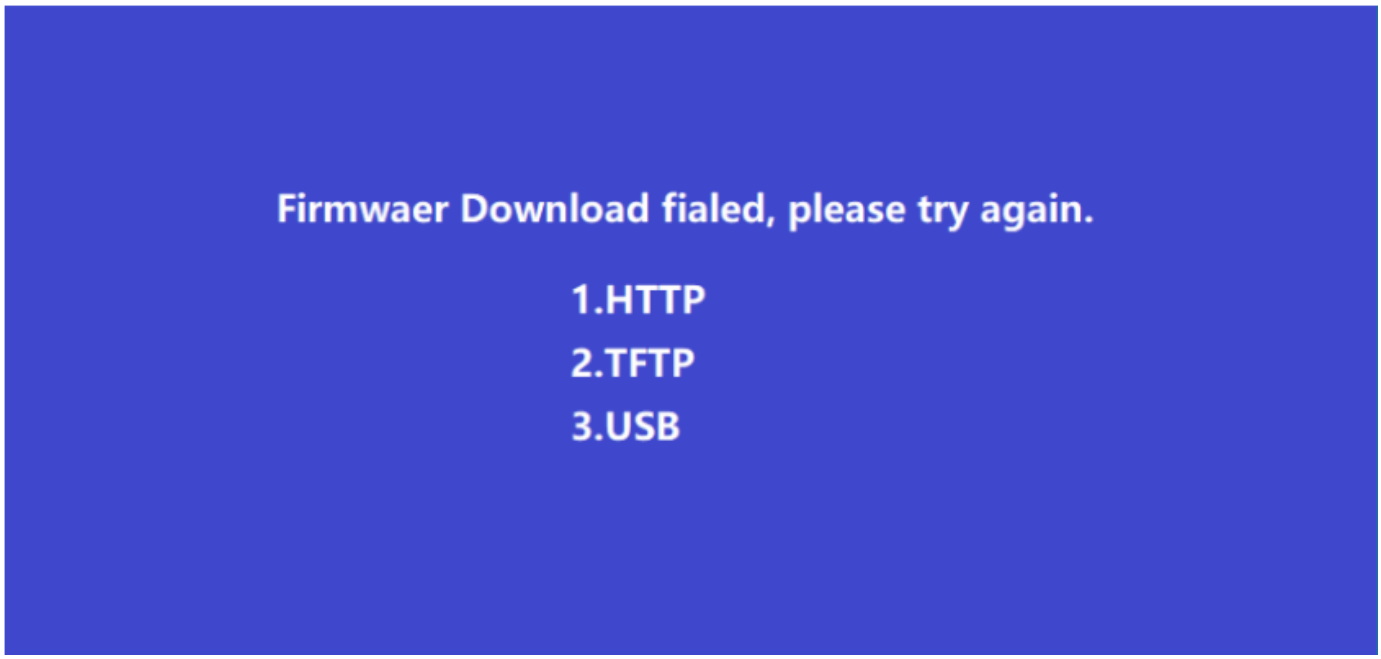




3. Fill in the IP Address field with the phone's IP address, and in the HTTP Server field, enter the URL where the ROM package is stored. The URL can be in the form of a domain name or an IP address. Here are some examples of a local testing environment.
   If the ROM package is placed in the following path on the HFS server: \10.200.108.89\www\upload, then the HTTP Server field should be filled as: user1:1234@xmyealink.com/yealink/upload/
   If the ROM package is hosted on the HFS server: http://10.82.1.101:8080/T58V/, then the HTTP Server field should be filled as: 10.82.1.101:8080/T58V.
4. Press the **OK** key to enter the download interface. During the download process, a progress bar and percentage will be displayed.

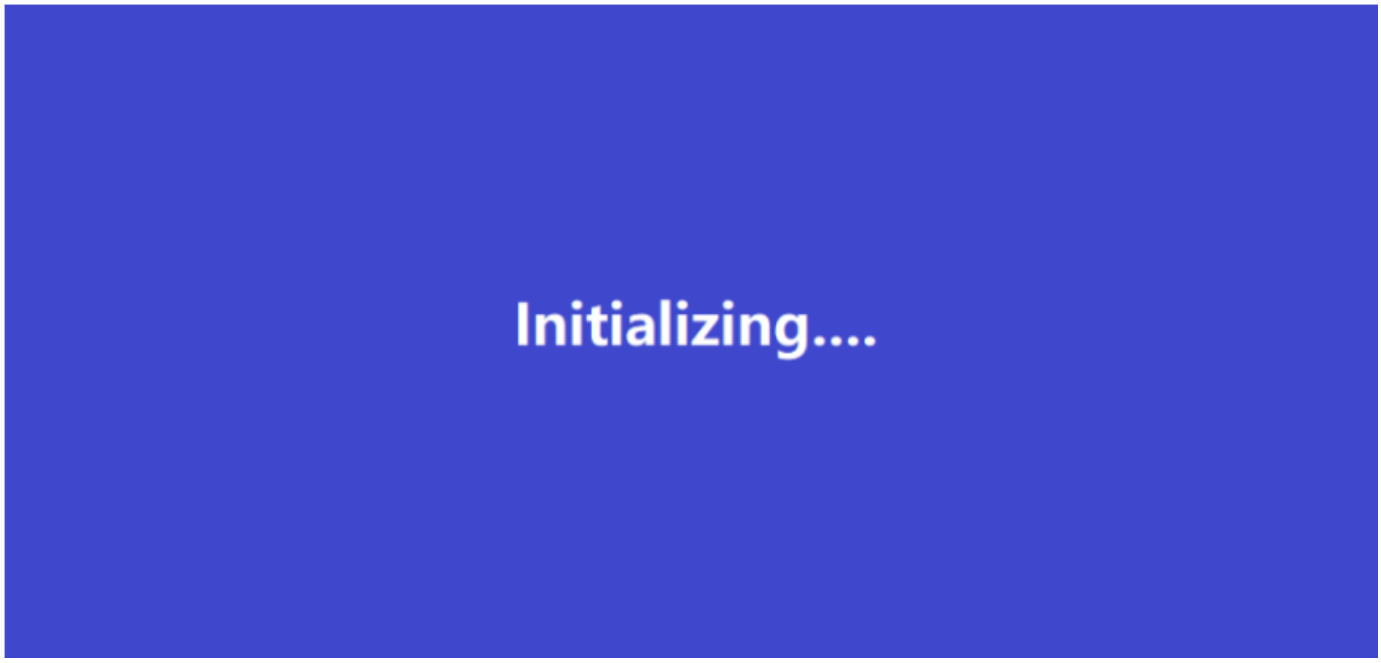


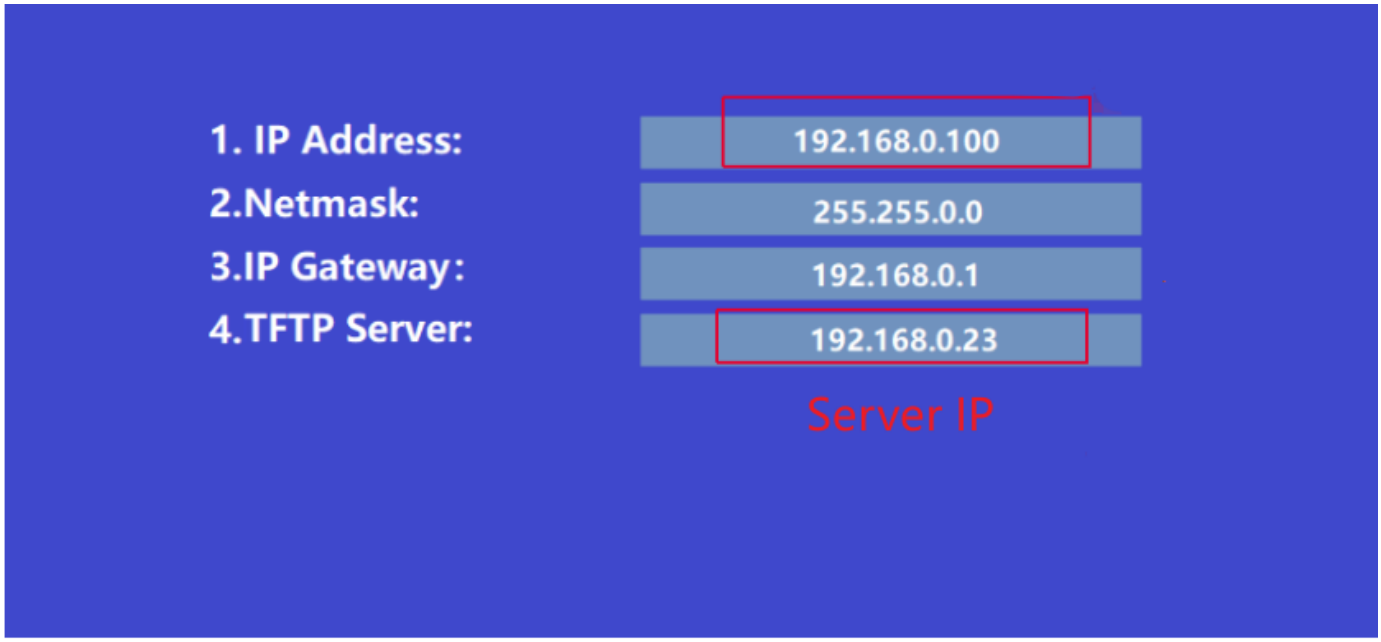
5. If you receive a notification of a download failure, you have the option to select a different mode to initiate a factory reset.



TFTP

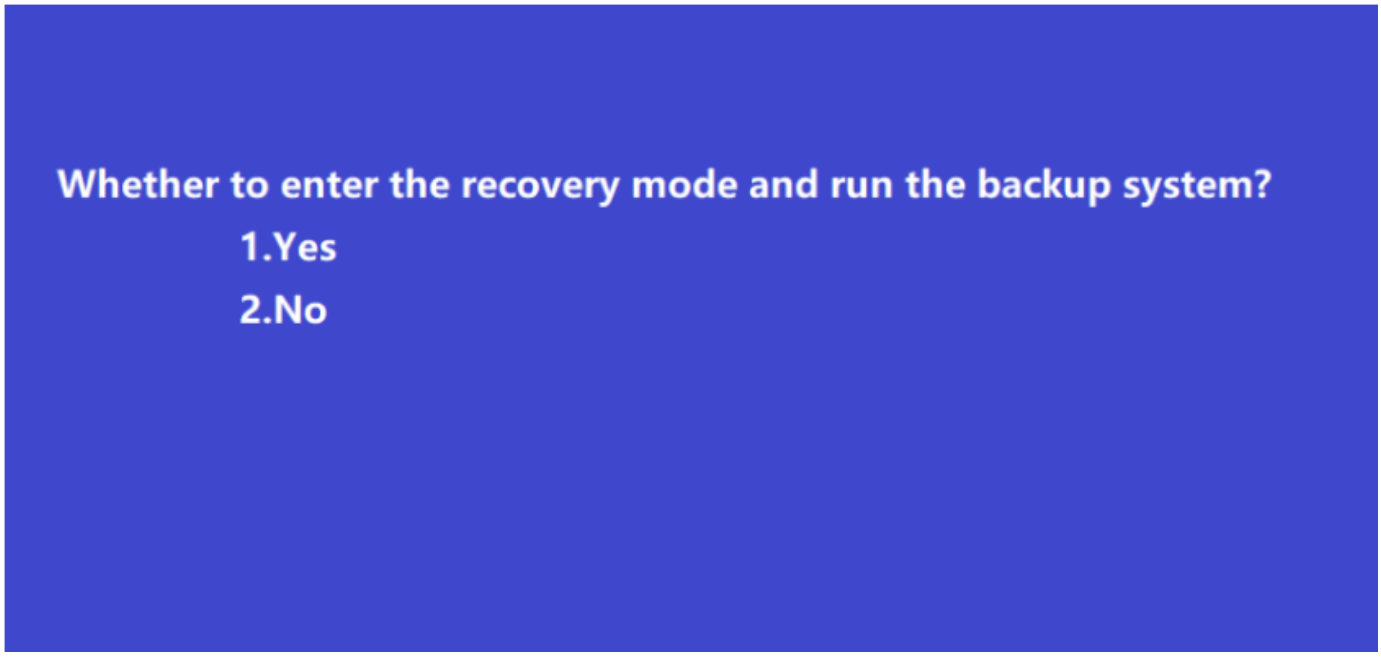
1. Place the ROM on a TFTP server.
2. Power on the device by long pressing the speakerphone button to enter the recovery mode interface. Press **2** to select the TFTP method. You will first enter the initialization interface, and then proceed to the IP configuration interface, as shown below:





USB

1. Ensure that the USB flash drive is formatted with the FAT32 file system, and place the ROM file in the USB.
2. Connect the Device Under Test (DUT) to the USB. Power on the DUT by long-pressing the speakerphone button, then select option 3 for USB.



3. Select **Yes** and follow the recovery mode process to start the backup system within the phone.

4. Select **No** and proceed with the original process to start the phone normally.

Dual System

- Press and hold the speakerphone button while powering on the device to enter the recovery mode interface.
- For CP920: Power on the device by long-pressing Softkey **2**.
- For CP960: Power on the device by long-pressing the Home key.
- For the model that lacks the up, down, left, right, and OK keys:

Model	Key	Action
VP59	Hold key	Left
VP59	Video key	Right
VP59	Headset key	Up
VP59	Transfer key	Down
VP59	Mute key	Start recovering

Model	Key	Action
T57W/T58V	Hold key	Up
T57W/T58V	Video key	Right
T57W/T58V	Voice key	Left
T57W/T58V	Transfer key	Down
T57W/T58V	Mute key	Start recovering
T57W/T58V	Headset key	Cancel recovering