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 the base/DM/VIM?

- Get W70B IP address
- Get W75/W80/W90 IP address

IPv4 and IPv6 Network Settings

Introduction

You can configure the devices to operate in IPv4, IPv6, or dual-stack (IPv4/IPv6) mode.

After establishing wired network connectivity, the devices obtain the IPv4 or IPv6 network settings from a Dynamic Host Configuration Protocol (DHCPv4 or DHCPv6) server. We recommend using DHCP where possible to eliminate repetitive manual data entry.

You can also configure IPv4 or IPv6 network settings manually.

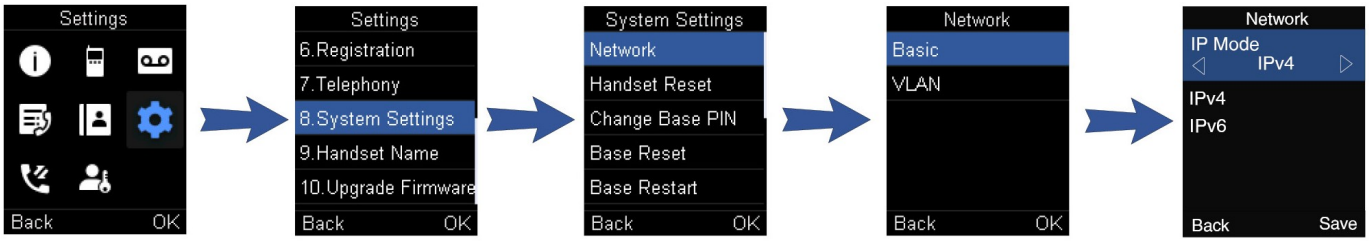
> Yealink devices comply with the DHCPv4 specifications documented in RFC 2131, and DHCPv6 specifications documented in RFC 4443 (For W75DM/W80DM/W90DM), RFC3315 (For W70B).

IP Addressing Mode Configuration

You can configure IP addressing mode for the wired network.

Set via the Device Interface (W70B)

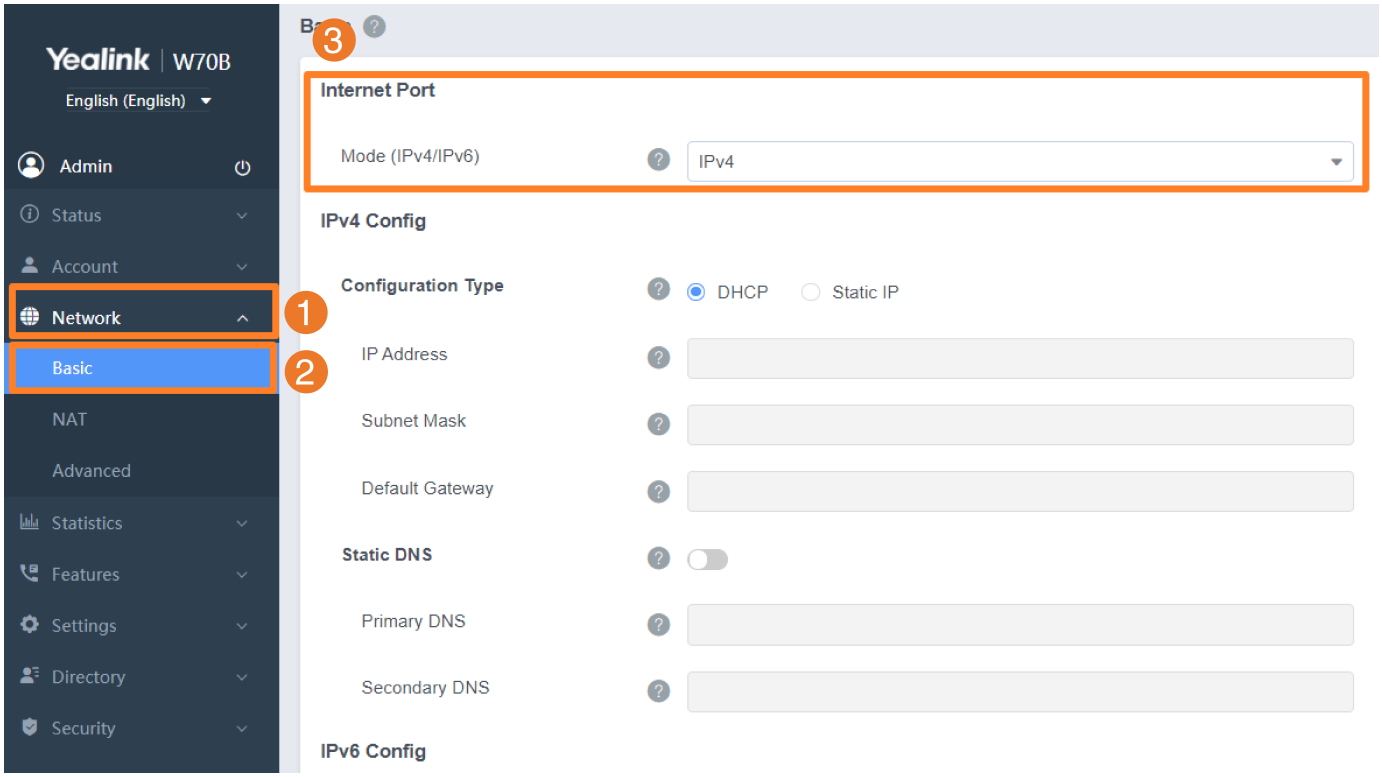
- W53H/W56H/W57R/W59R/W59R Pro/W71H/W73H/W74H/W78H:
- **OK** > **Settings** > **System Settings** > **Network (default PIN: 0000)** > **Basic** > **IP Mode**.



- DD Phone:
- **Menu** > **Advanced Settings (default password: 0000)** > **Network** > **WAN Port** > **IP Mode**.
- CP930W:
- **Menu** > **Settings** > **Advanced Settings (default PIN: 0000)** > **Network** > **Basic** > **IP Mode**.
- CP935W:
- **More** > **Advanced (default PIN: 0000)** > **Network** > **WAN Port** > **IP Address Mode**.

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] [2]	**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).

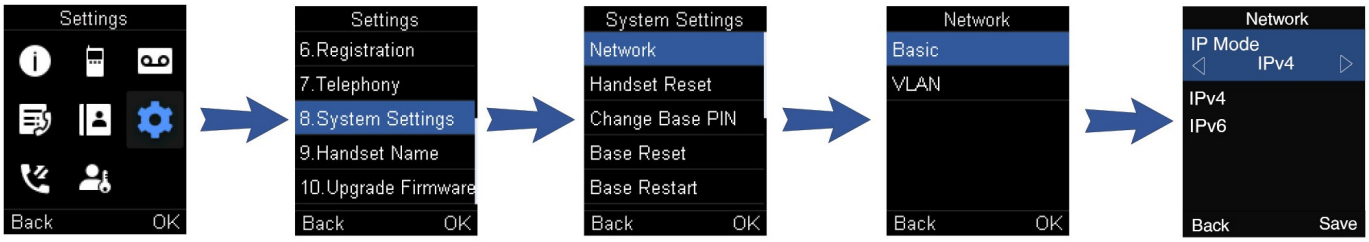
[1]If you change this parameter, the phone will reboot to make the change take effect.
[2]The parameter is only applicable to W75/W80/W90 Multi-Cell System.

IPv4 Configuration

You can configure the devices to operate in IPv4 mode.

Set via the Device Interface (W70B)

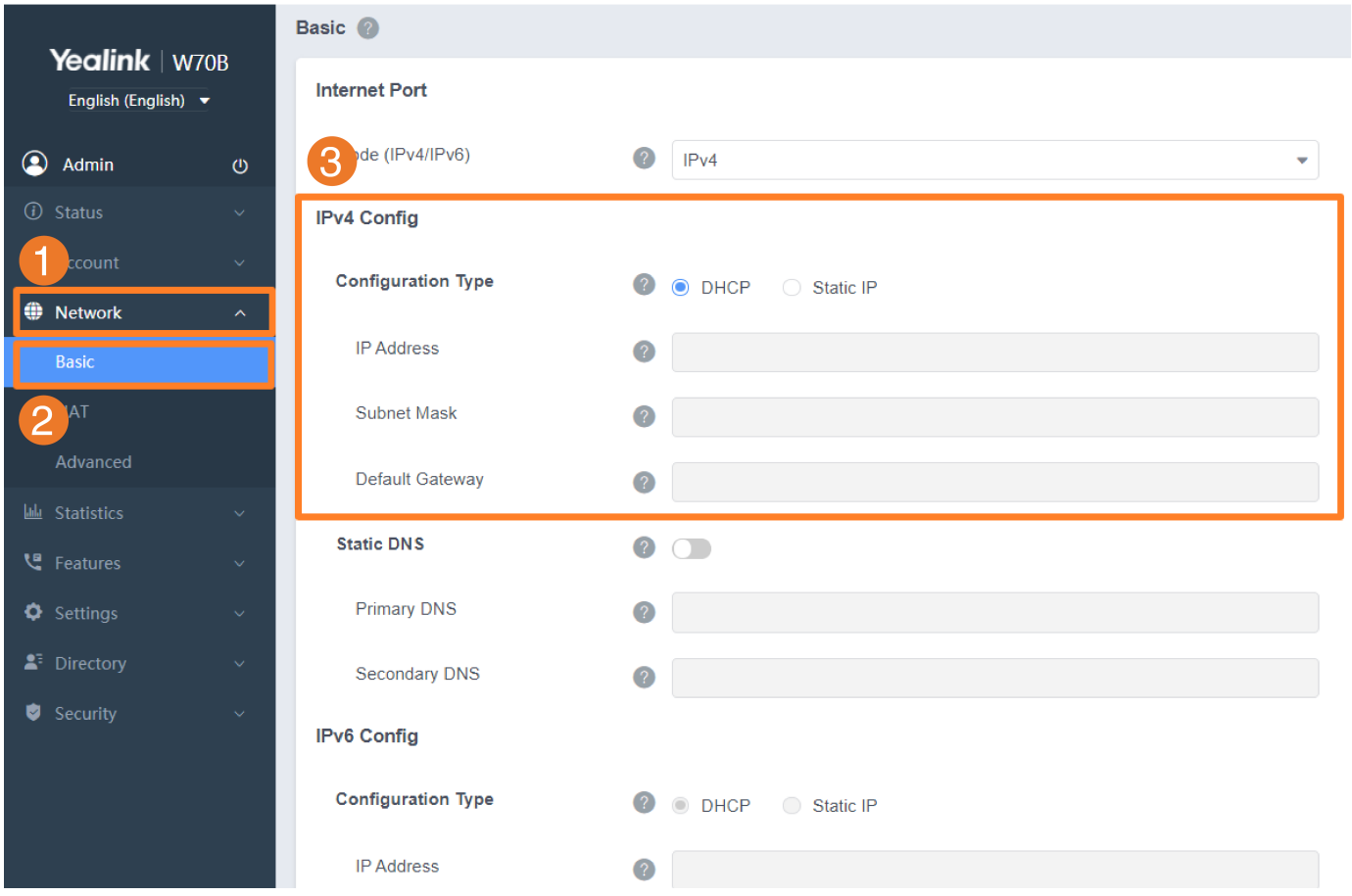
- W53H/W56H/W57R/W59R/W59R Pro/W71H/W73H/W74H/W78H:
- **OK** > **Settings** > **System Settings** > **Network (default PIN: 0000)** > **Basic** > **IPv4**.



- DD Phone:
- **Menu** > **Advanced Settings (default password: 0000)** > **Network** > **WAN Port** > **IPv4**.
- CP930W:
- **Menu** > **Settings** > **Advanced Settings (default PIN: 0000)** > **Network** > **Basic** > **IPv4**.
- CP935W:
- **More** > **Advanced (default PIN: 0000)** > **Network** > **WAN Port** > **IPv4**.

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] [2]	**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] [2]	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.t

			ype" 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 obtained from DHCP. **1**-On, the phone will use manually configured static IPv4 DNS.	0	It triggers the static DNS feature to turn on or off. 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.
[2]The parameter is only applicable to W75/W80/W90 Multi-Cell System.

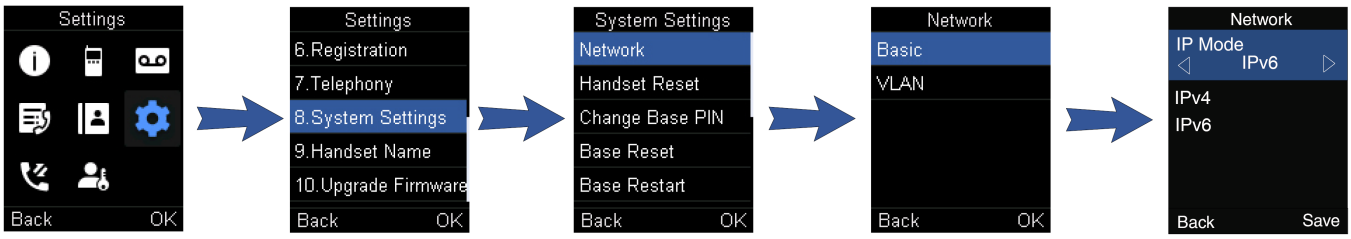
IPv6 Configuration

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 Device Interface (W70B)

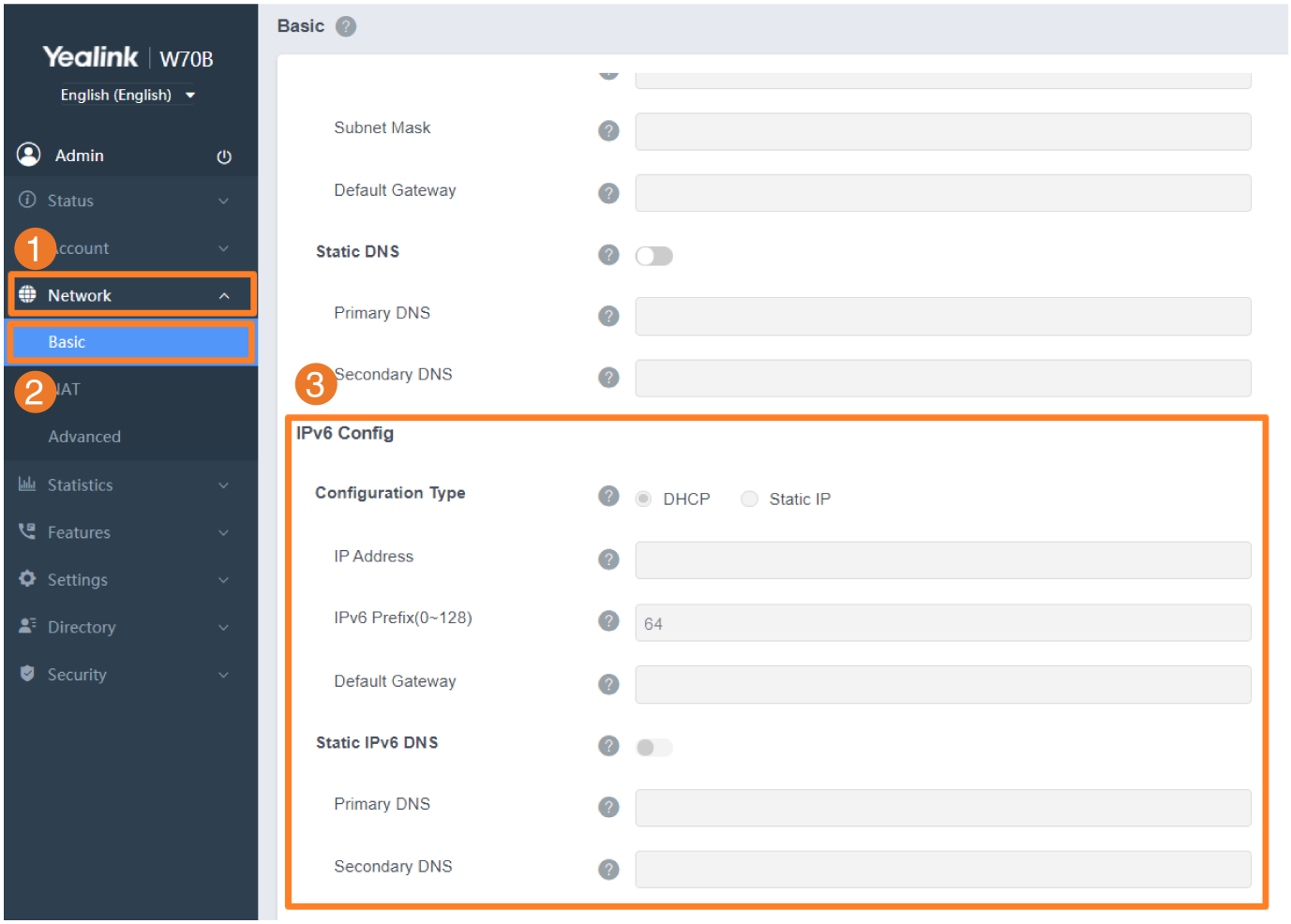
- W53H/W56H/W57R/W59R/W59R Pro/W71H/W73H/W74H/W78H:
- **OK** > **Settings** > **System Settings** > **Network (default PIN: 0000)** > **Basic** > **IPv6**.



- DD Phone:
- **Menu** > **Advanced Settings (default password: 0000)** > **Network** > **WAN Port** > **IPv6**.
- CP930W:
- **Menu** > **Settings** > **Advanced Settings (default PIN: 0000)** > **Network** > **Basic** > **IPv6**.
- CP935W:
- **More** > **Advanced (default PIN: 0000)** > **Network** > **WAN Port** > **IPv6**.

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.ip	**0**-DHCP (using	0	It configures the Internet port type for IPv6.

v6_internet_port.type[1]	SLAAC by default) **1**-Static IP		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 a 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 a 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] [2]	String within 64 characters	Blank	It configures the IPv6 address of the DM.
backup.master_dm.ip[1] [2]	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.
[2]The parameter is only applicable to W75/W80/W90 Multi-Cell System.

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 Mask	Specify the client's subnet mask.
2	Time Offset	Specify the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).
3	Router	Specify a list of IP addresses for routers on the client's subnet.
4	Time Server	Specify a list of time servers available to the client.
6	Domain Name Server	Specify a list of domain name servers available to the client.
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 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

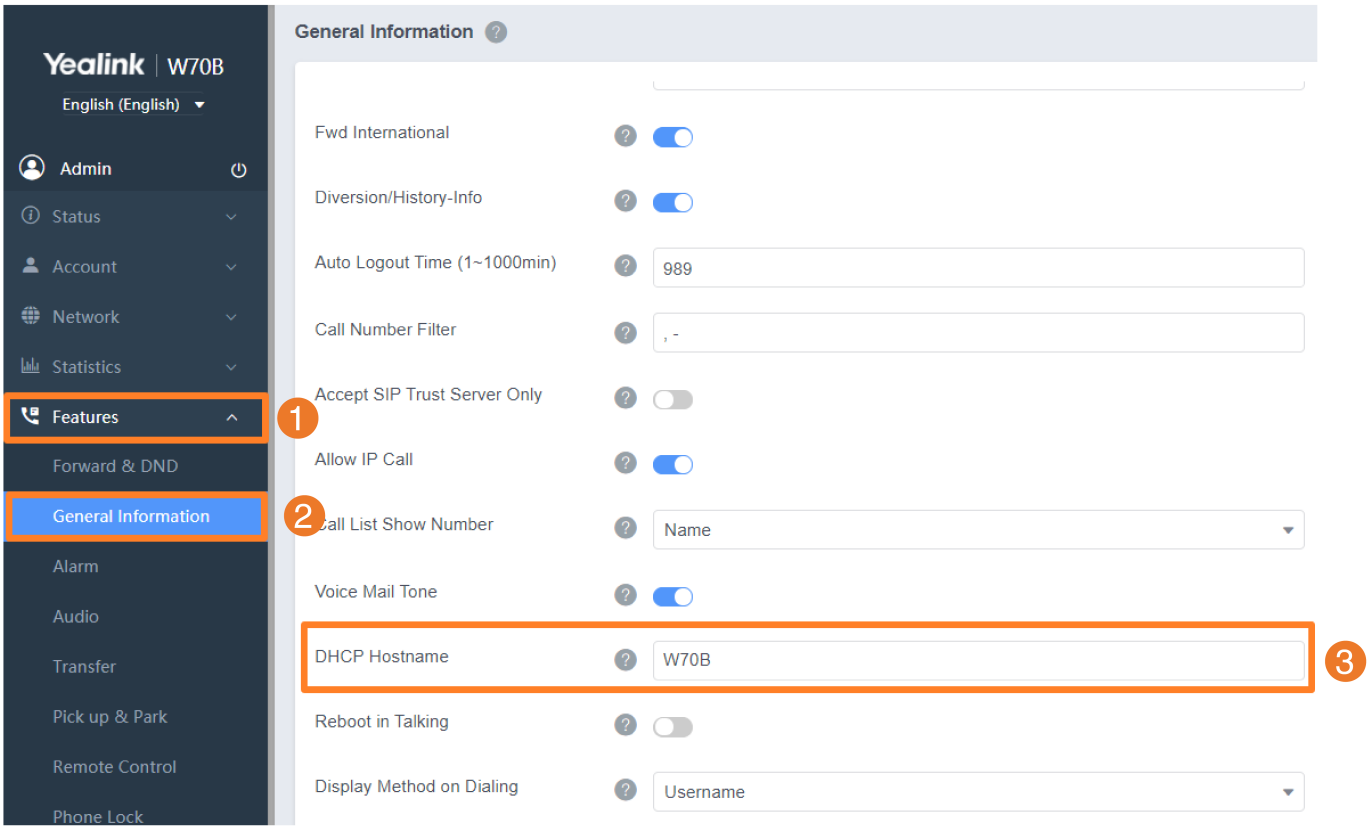
Description

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	For DM: SIP-W90DM For VIM: VIM For W80B: W80B For W70B: W70B For W75B: W75B	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

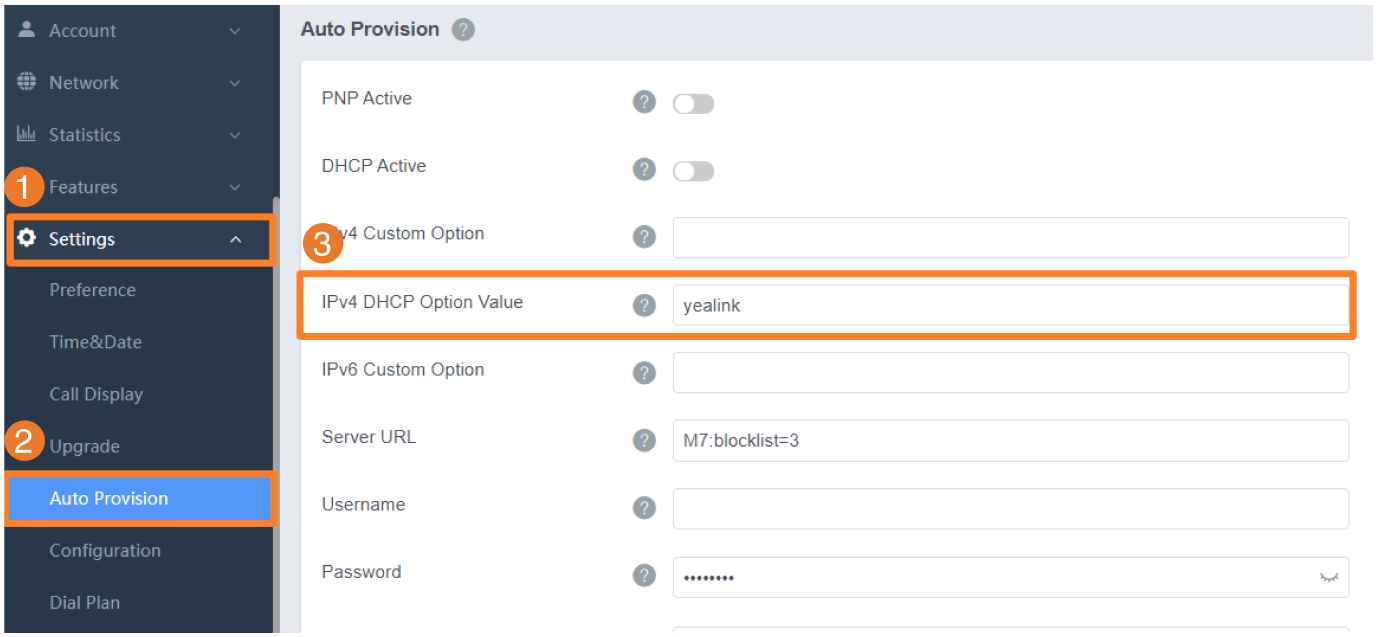
Description

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.

DHCP Option for IPv6

Introduction

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

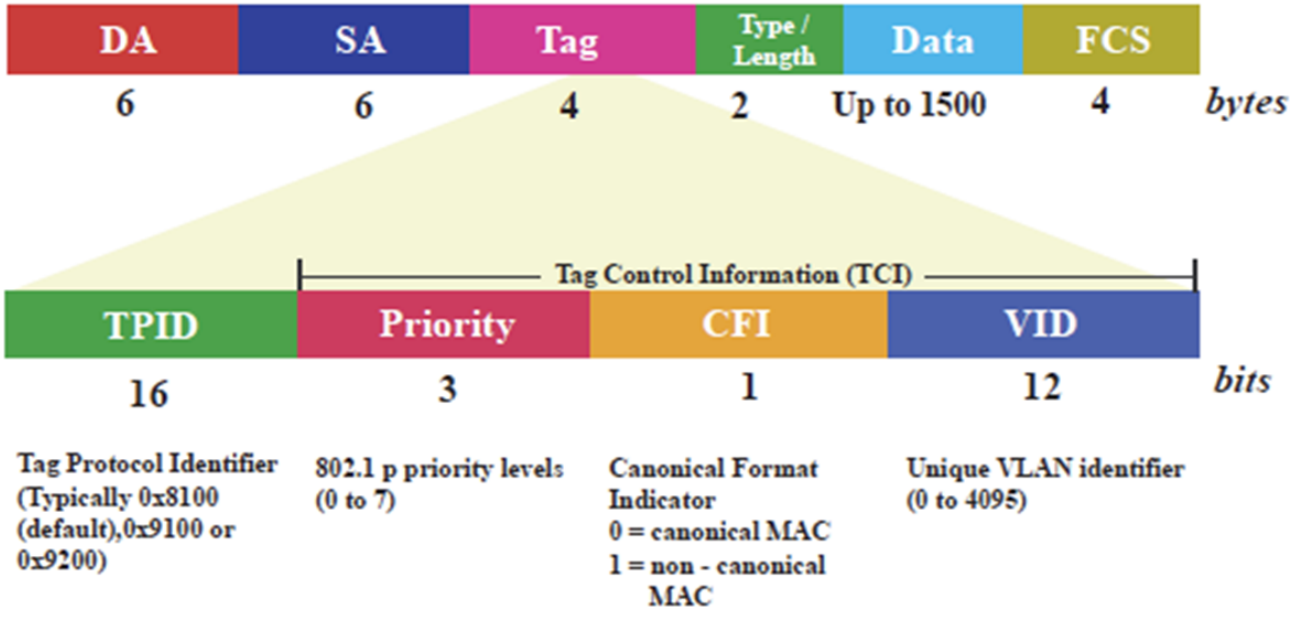
Major Benefits of Using VLANs

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 the 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. 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 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.



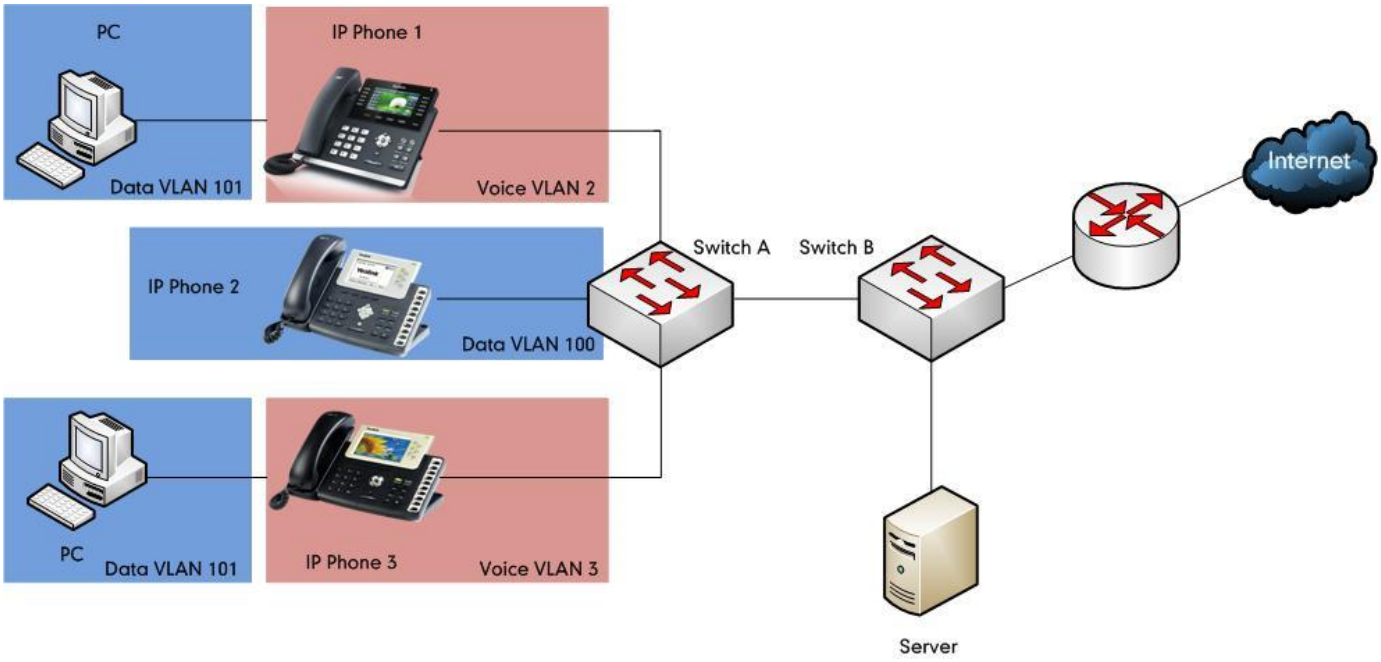
IEEE 802.3ac defines the Ethernet VLAN Tag

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 VLANs 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 ID	Specifies the MAC address of the IP phone.
	Time to Live	Specifies the lifetime of the transmitted information on the IP phone. The default value is 180s.

	End of LLDPDU	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) By default, all phones have the PMD Advertised Capability set for 10BASE-T and 100BASE-TX. Yealink W70B/W75/ W80/W90 Multi-Call systems that have Gigabit Ethernet support PMD Advertise Capability also contain set 1000BASE-T.
LLDP-MED 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 Revision	Specifies the firmware revision of the IP phone.
	Inventory – Software Revision	Specifies the software revision of the IP phone.
	Inventory – Serial Number	Specifies the serial number of the IP phone.
	Inventory – Manufacturer User 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

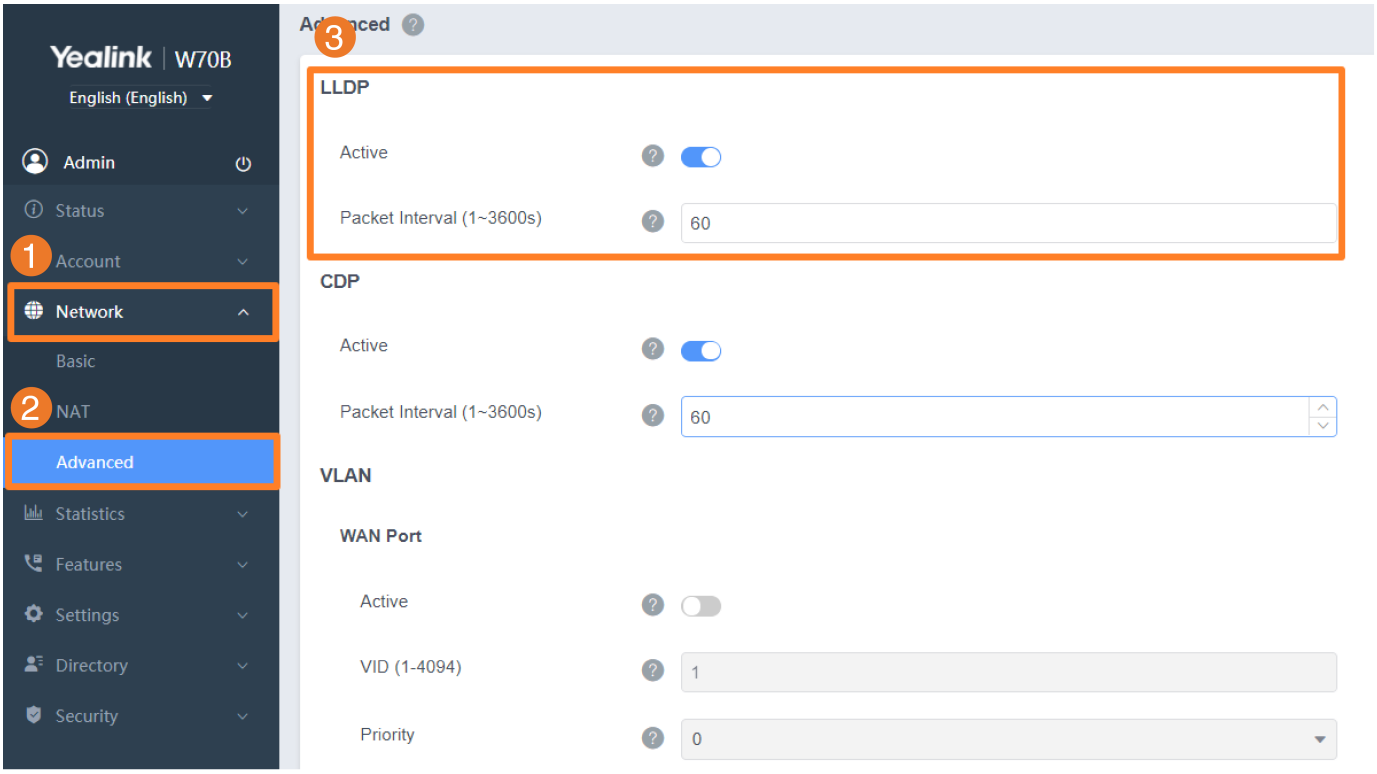
following capabilities:

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) that determines how often the phone sends the LLDP request. It works only if "static.network.lldp.enable" is set to 1 (Enabled).

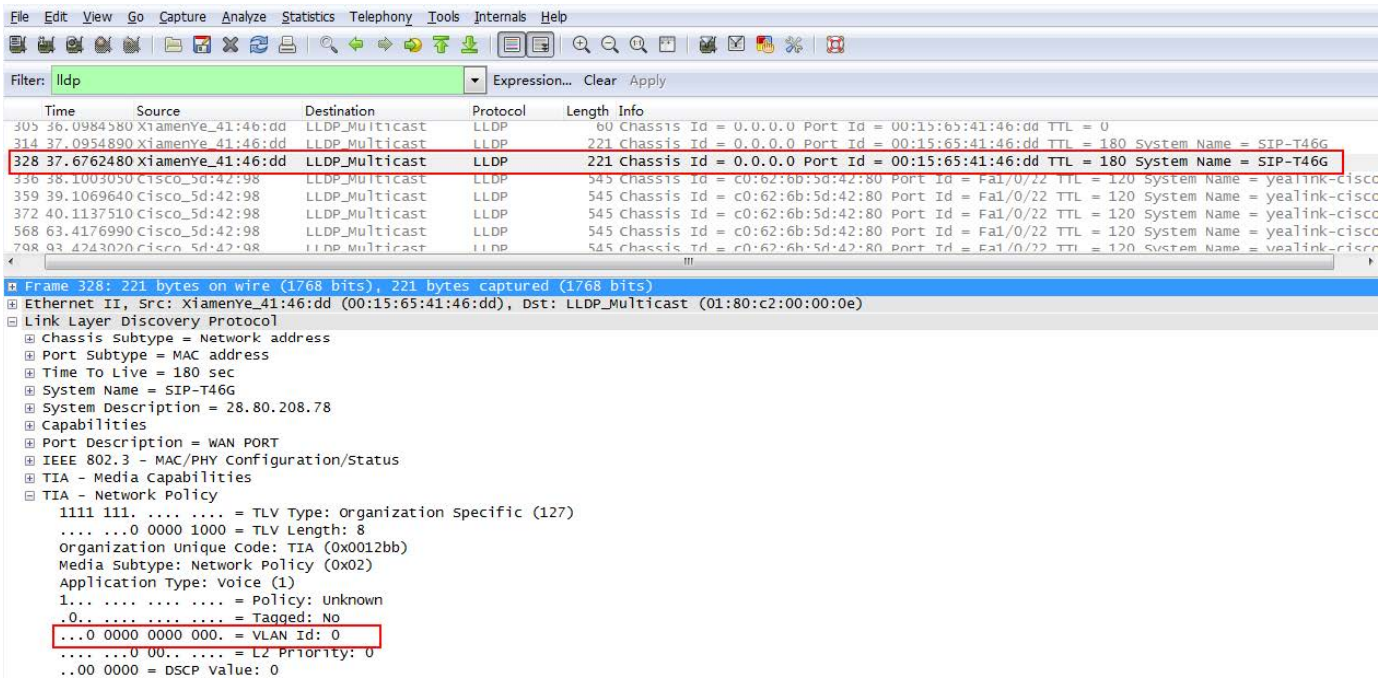
[1]If you change this parameter, the phone will reboot to make the change take effect.

Verify the Configuration

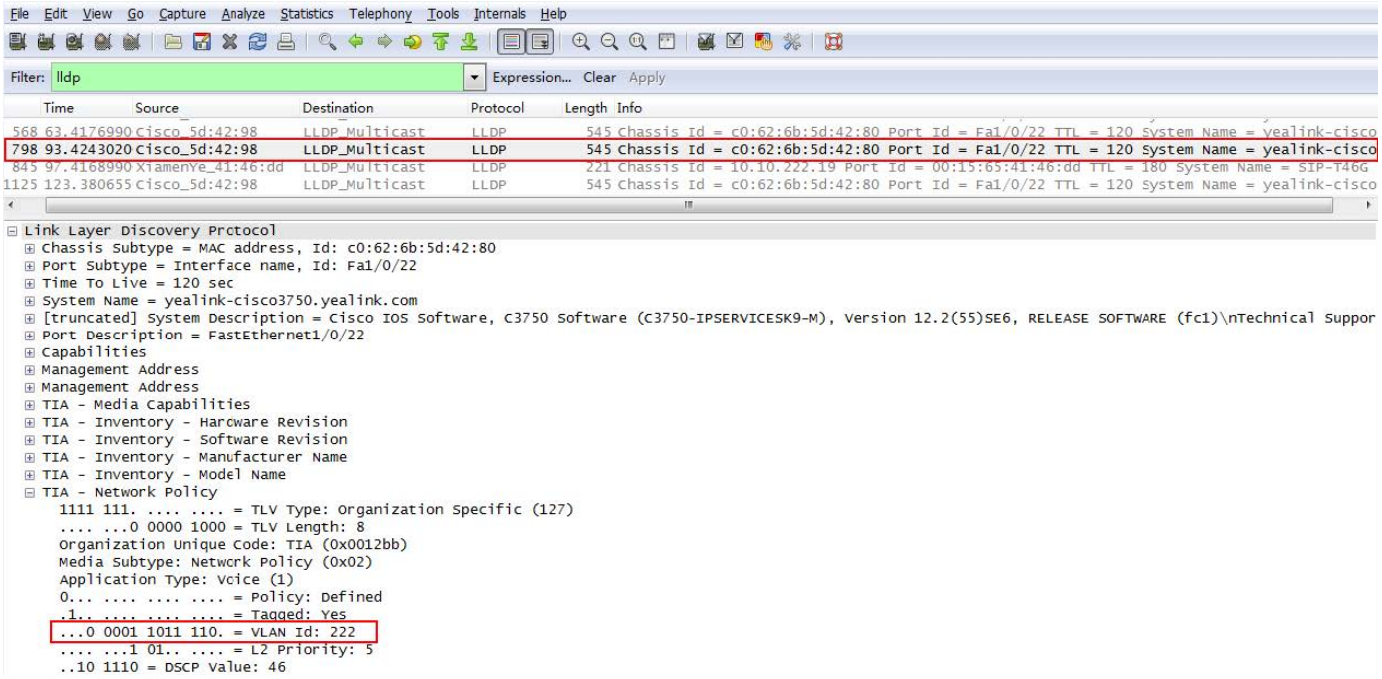
After the LLDP feature is enabled, the IP phone performs the following:

- 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.

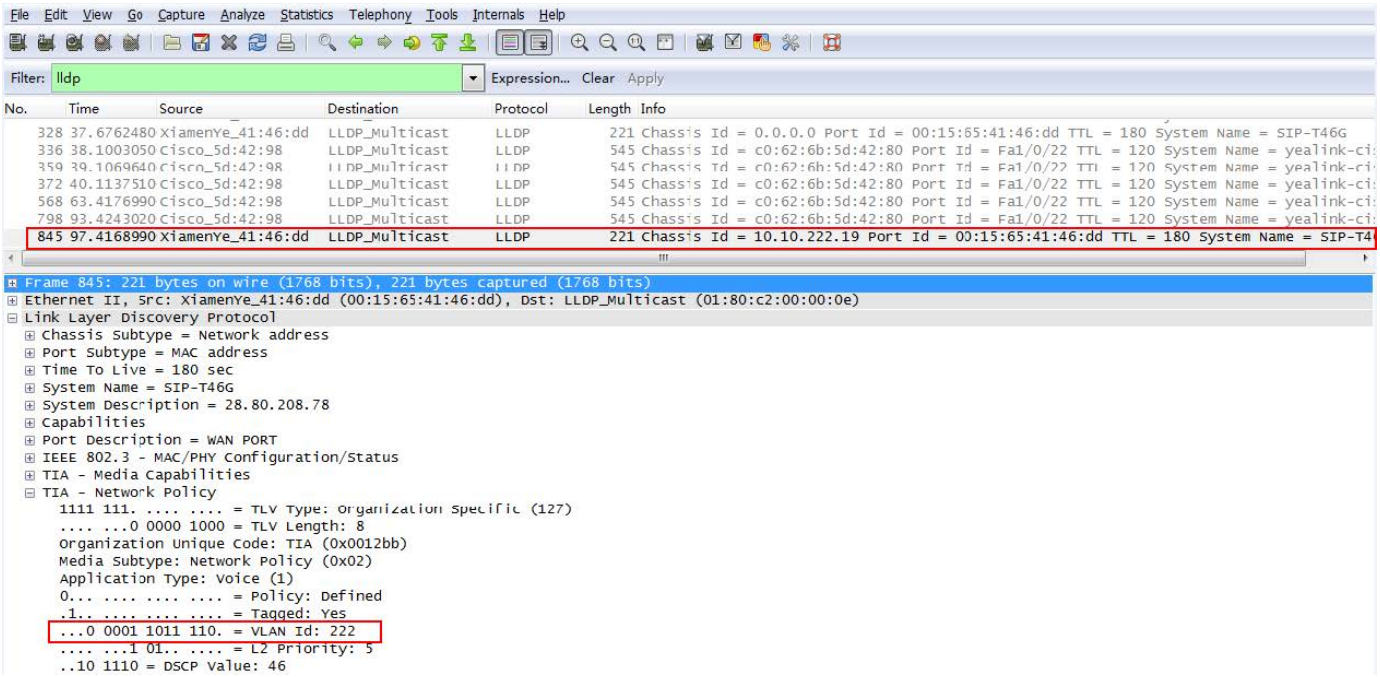
The following figure shows the LLDP packet sent by the IP phone; the packet contains multiple TLVs (before obtaining the VLAN ID).



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 the VLAN ID).



CDP

Description

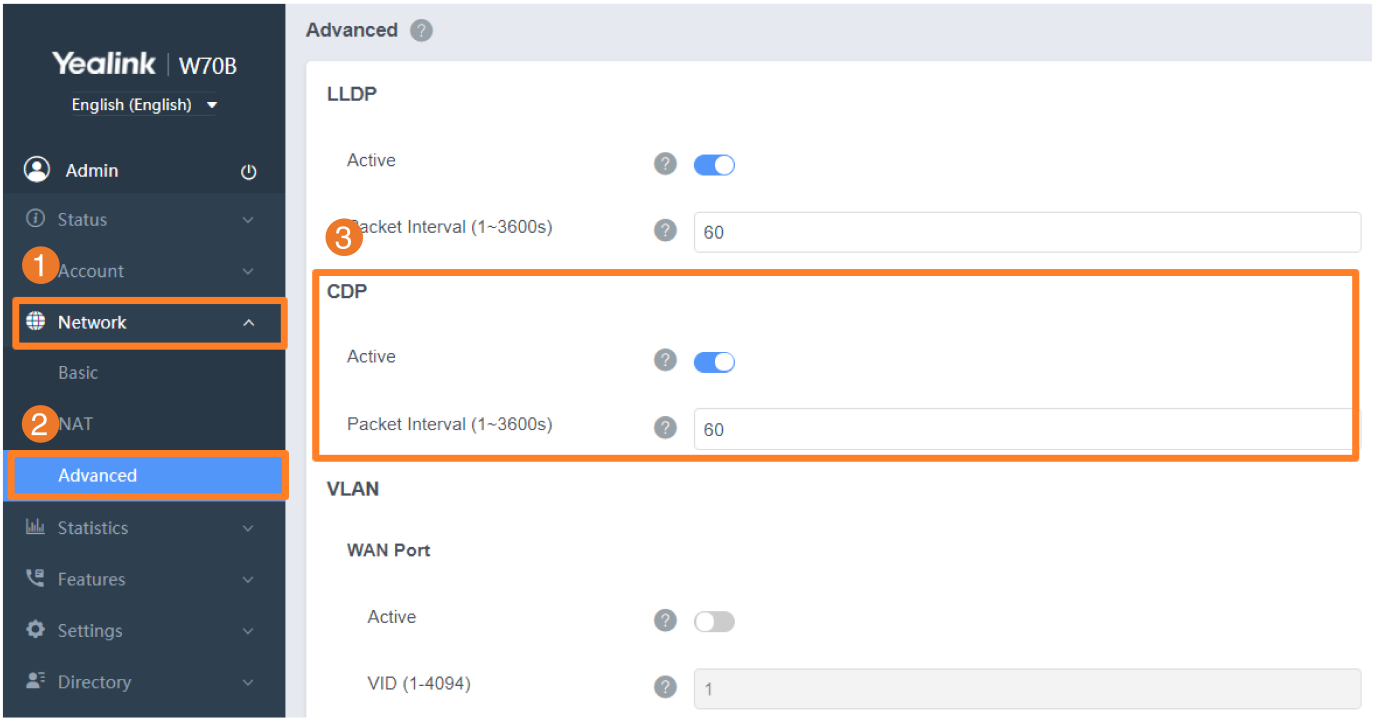
CDP (Cisco Discovery Protocol) allows the phones to receive and/or transmit device-related information from/to directly connected devices on the local network.

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).

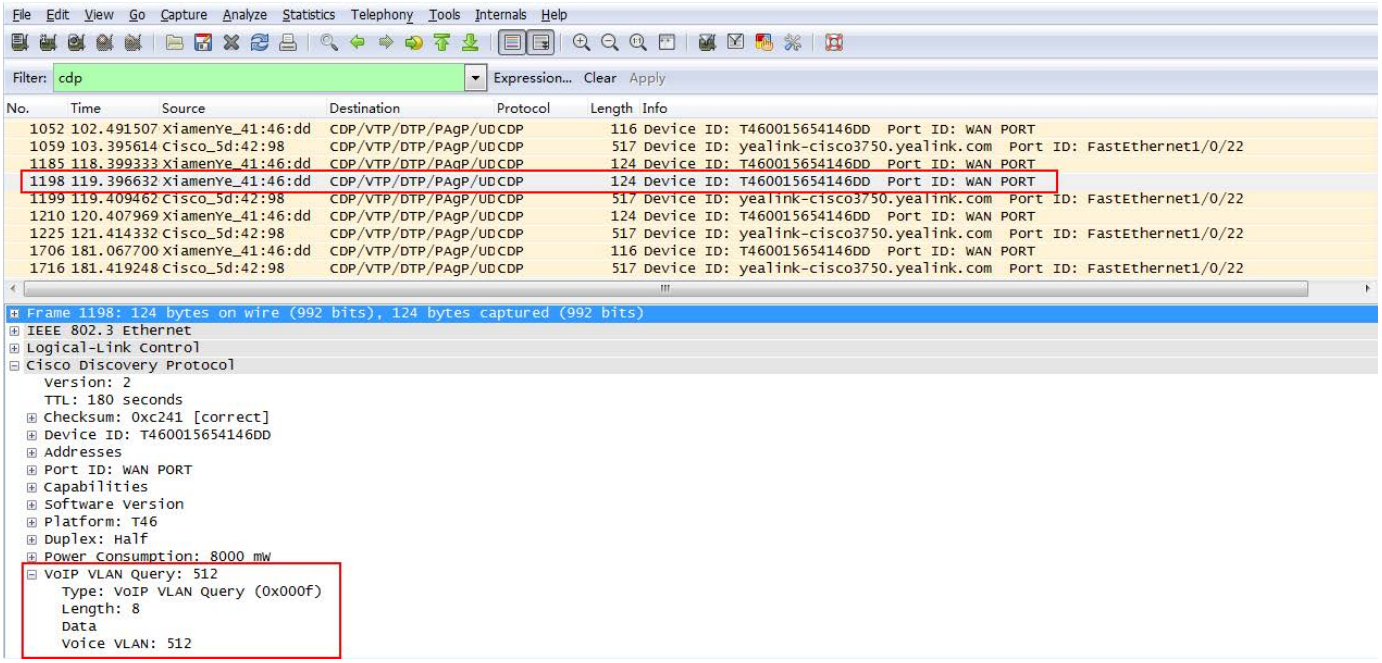
[1]If you change this parameter, the phone will reboot to make the change take effect.

Verify the Configuration

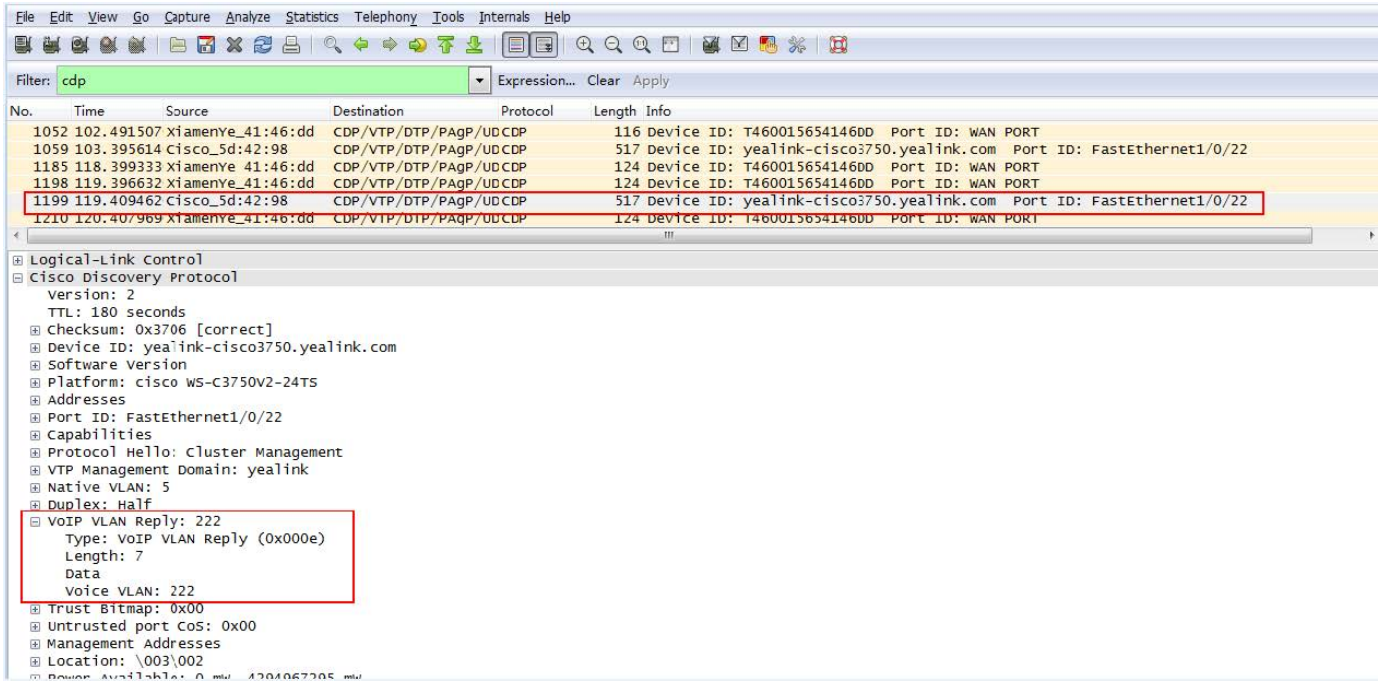
After the CDP feature is enabled, the IP phone performs the following:

- 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.

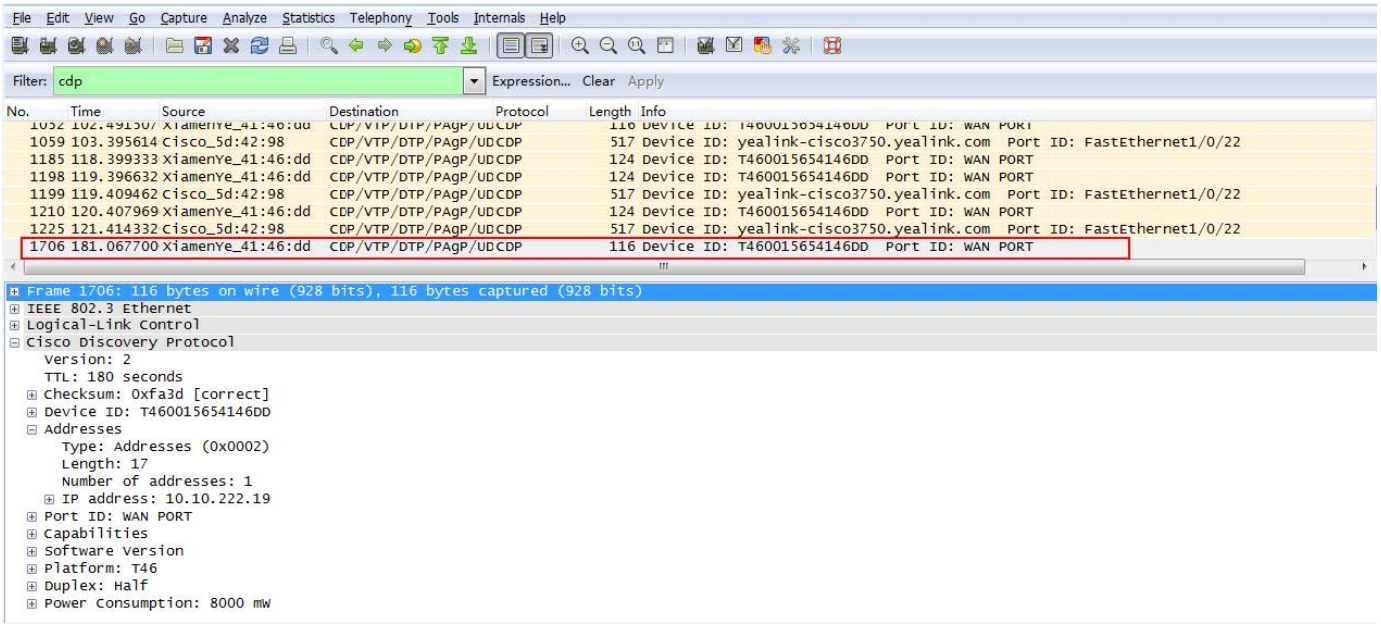
The following figure shows the CDP packet sent by the IP phone (before obtaining the VLAN ID with the VLAN Query field).



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



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



DHCP VLAN

Description

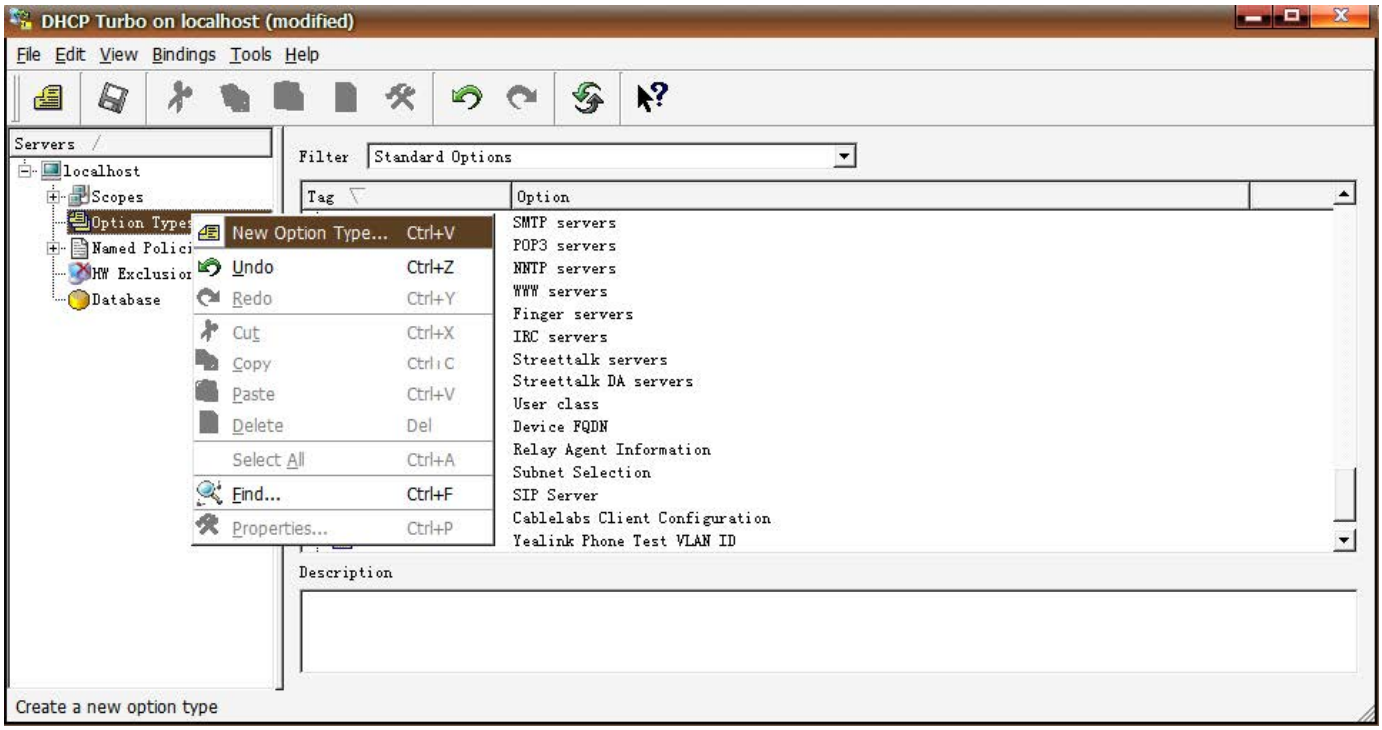
When the VLAN discovery method is set to DHCP, the phone examines the DHCP option for a valid VLAN ID. You can customize the DHCP option used to request the VLAN ID.

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.

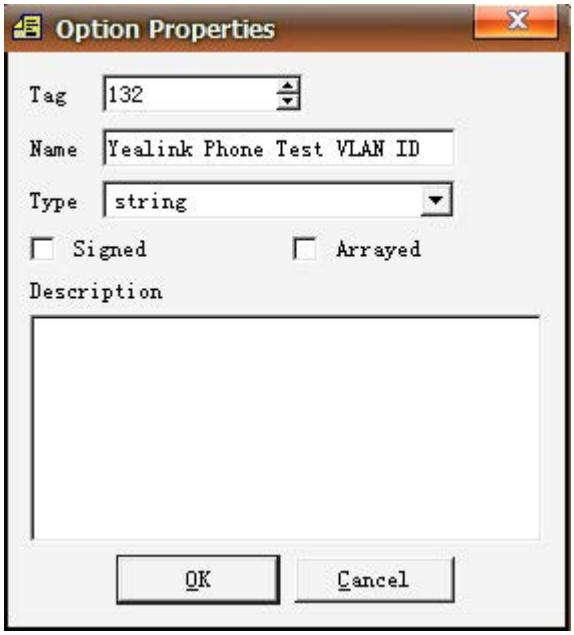


3. Enter the desired option in the **Tag** field.

   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**.

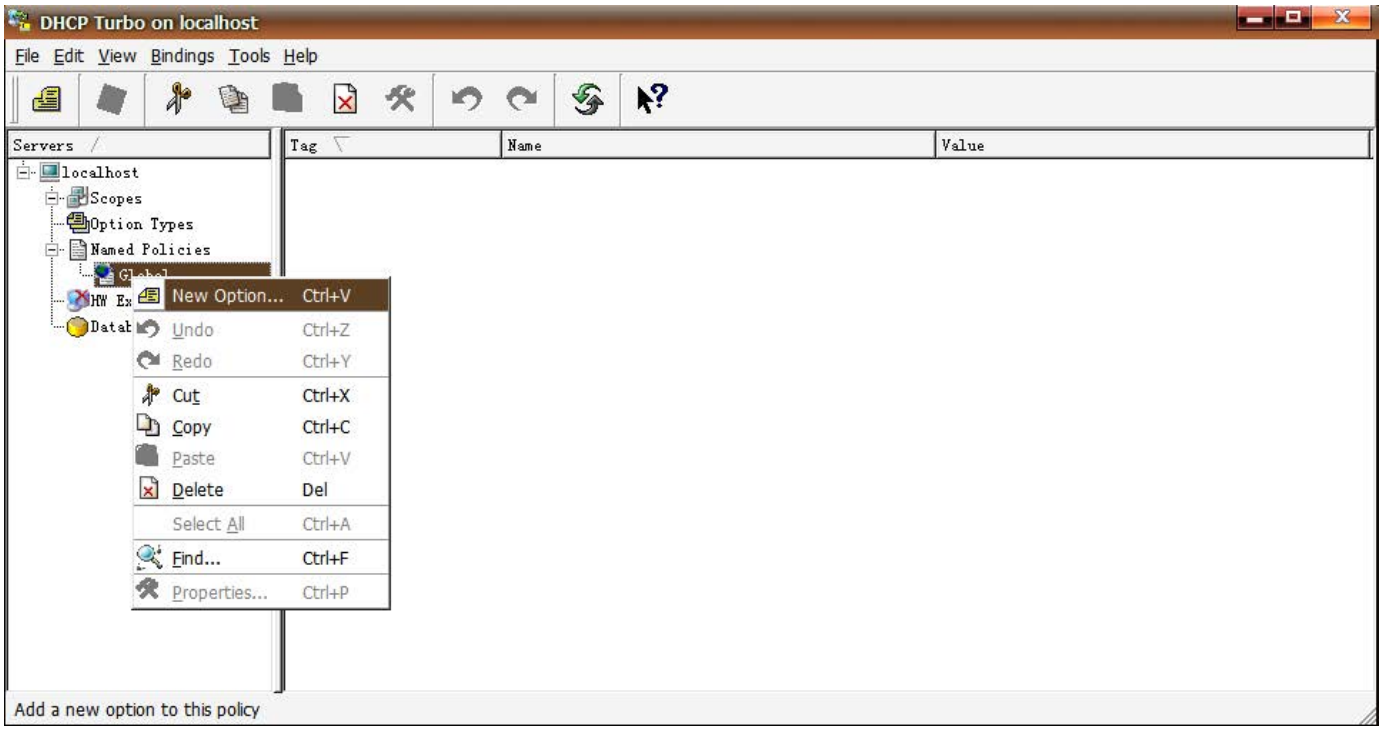


6. Click **OK** to finish setting the option properties.

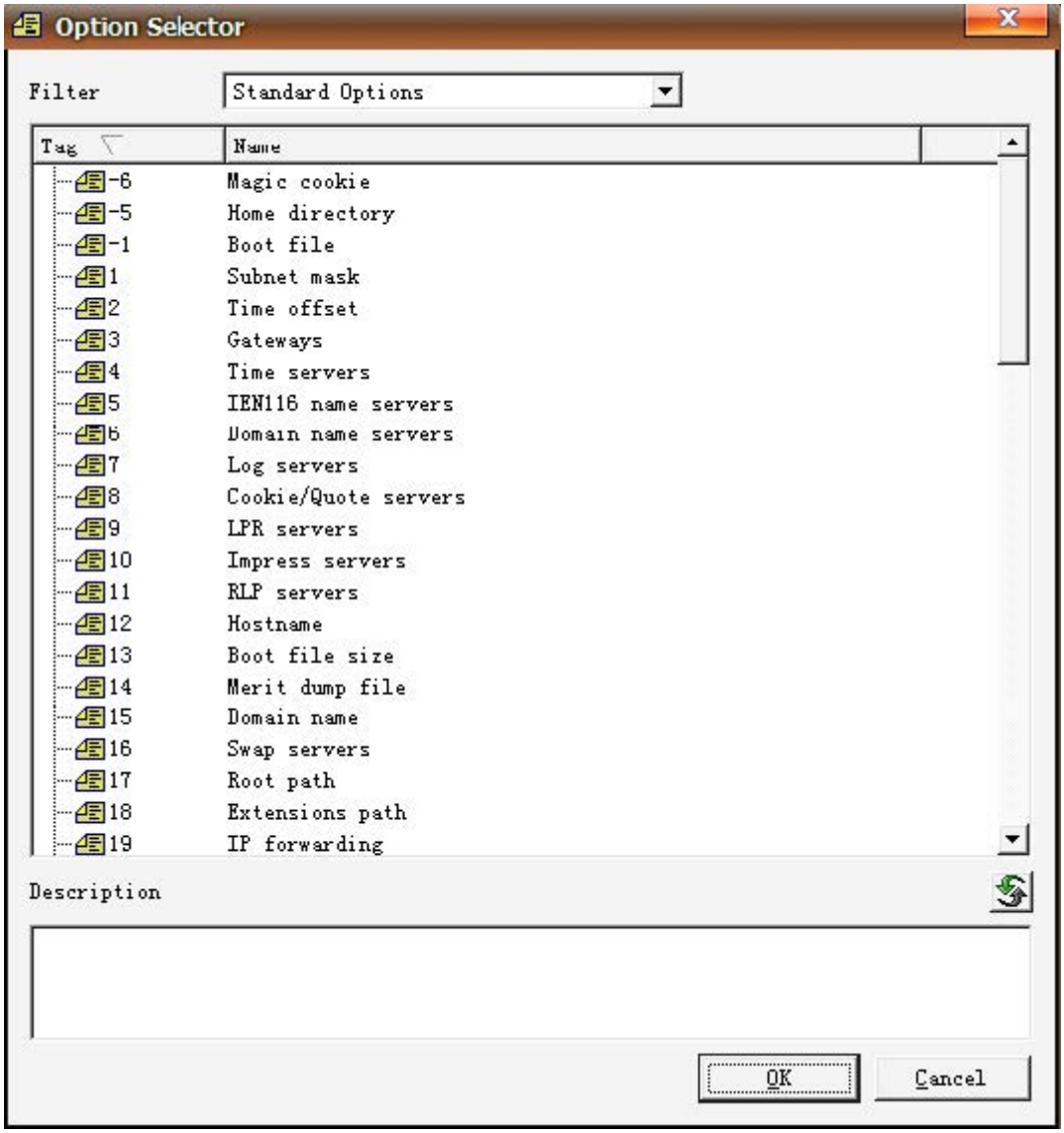
7. Click to accept the change.

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

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

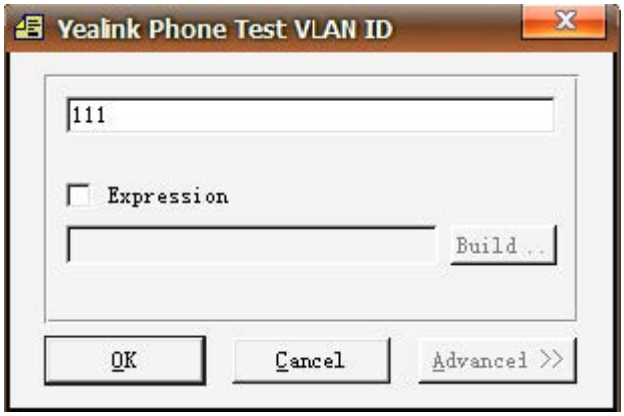


11. The Option Selector screen displays as below:

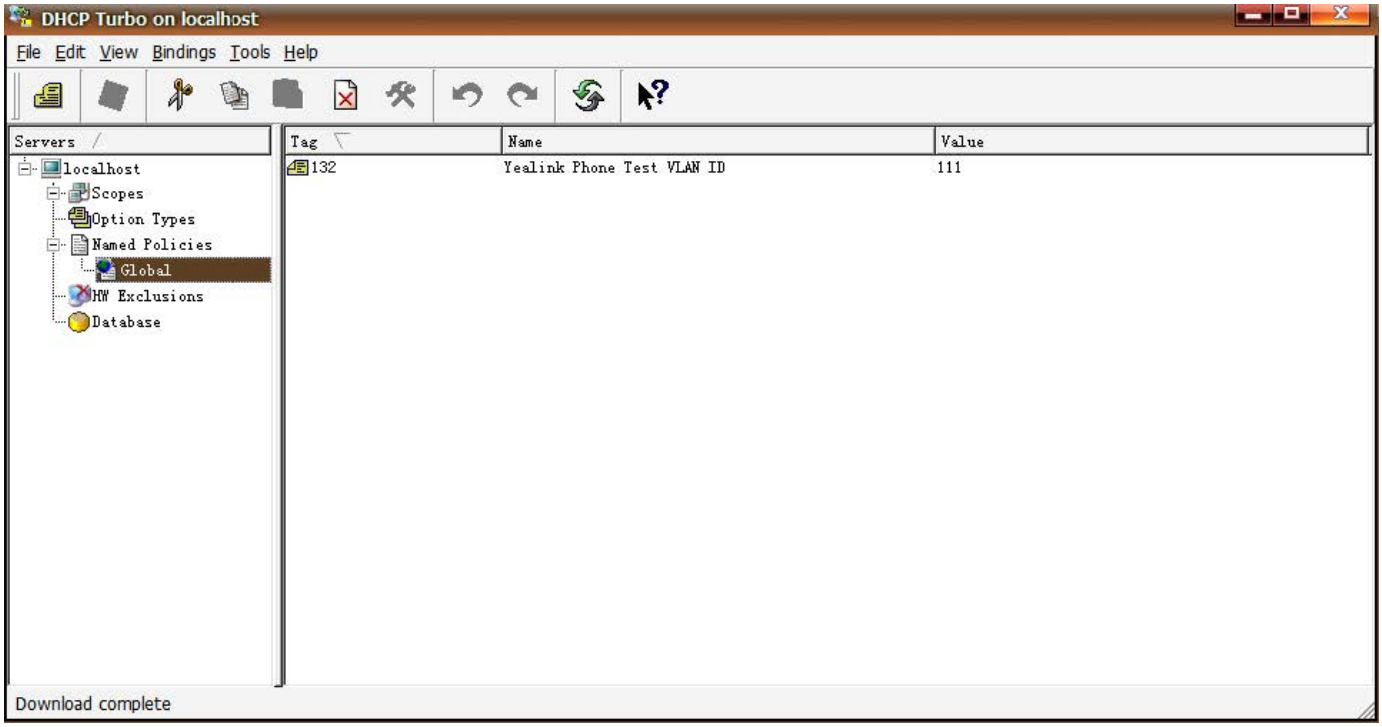


10. Scroll down and double-click the option created above.

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.



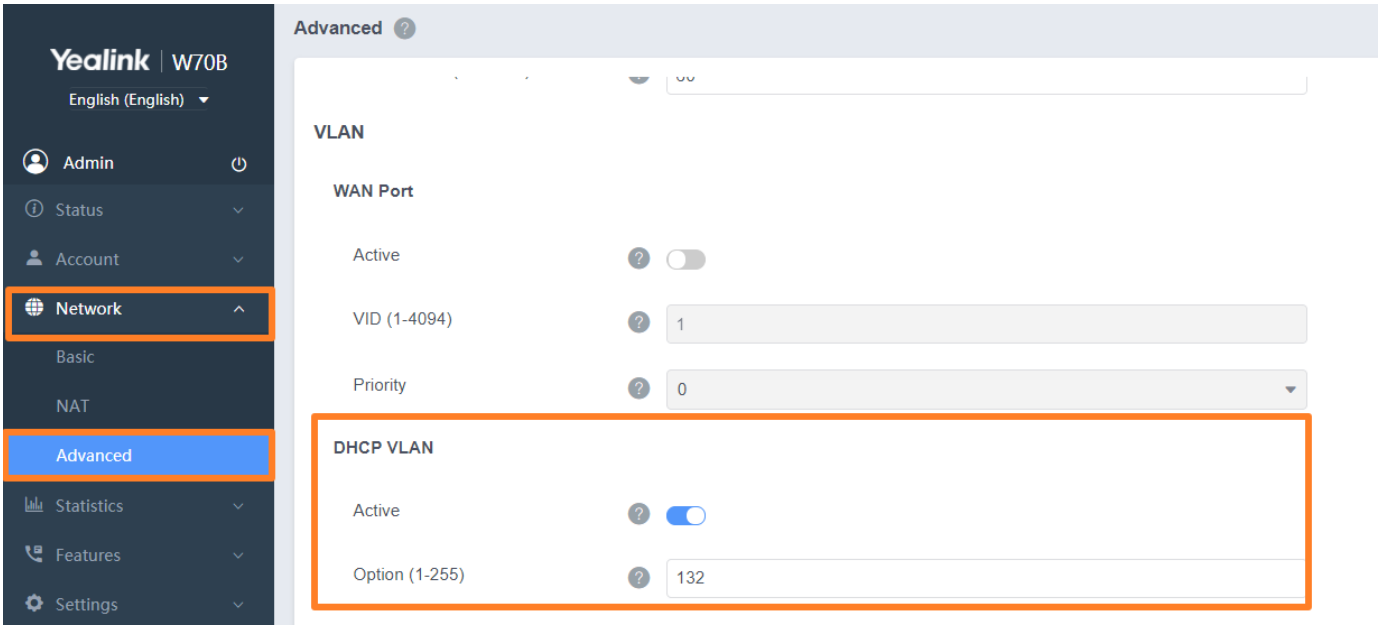
12. Click **OK** to finish setting a custom option.
13. Click to accept the change.
14. Then you can find the configured option under the **Global** option.



Configure DHCP Option on Yealink IP Phones

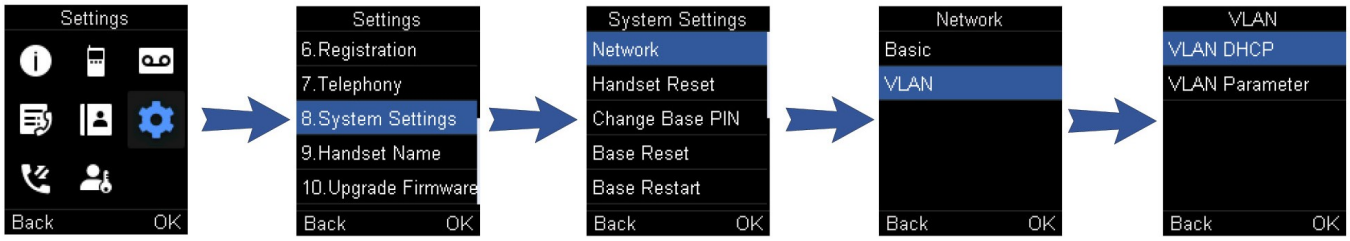
Set via the Web User Interface

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



Set via the Device Interface (W70B)

- W53H/W56H/W57R/W59R/W59R Pro/W71H/W73H/W74H/W78H:
- **OK** > **Settings** > **System Settings** > **Network (default PIN: 0000)** > **VLAN** > **VLAN DHCP**.



- DD Phone:
- **Menu** > **Advanced Settings (default password: 0000)** > **Network** > **VLAN** > **DHCP VLAN**.
- CP930W:
- **Menu** > **Settings** > **Advanced Settings (default PIN: 0000)** > **Network** > **VLAN** > **VLAN DHCP**.
- CP935W:
- **More** > **Advanced (default PIN: 0000)** > **Network** > **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.

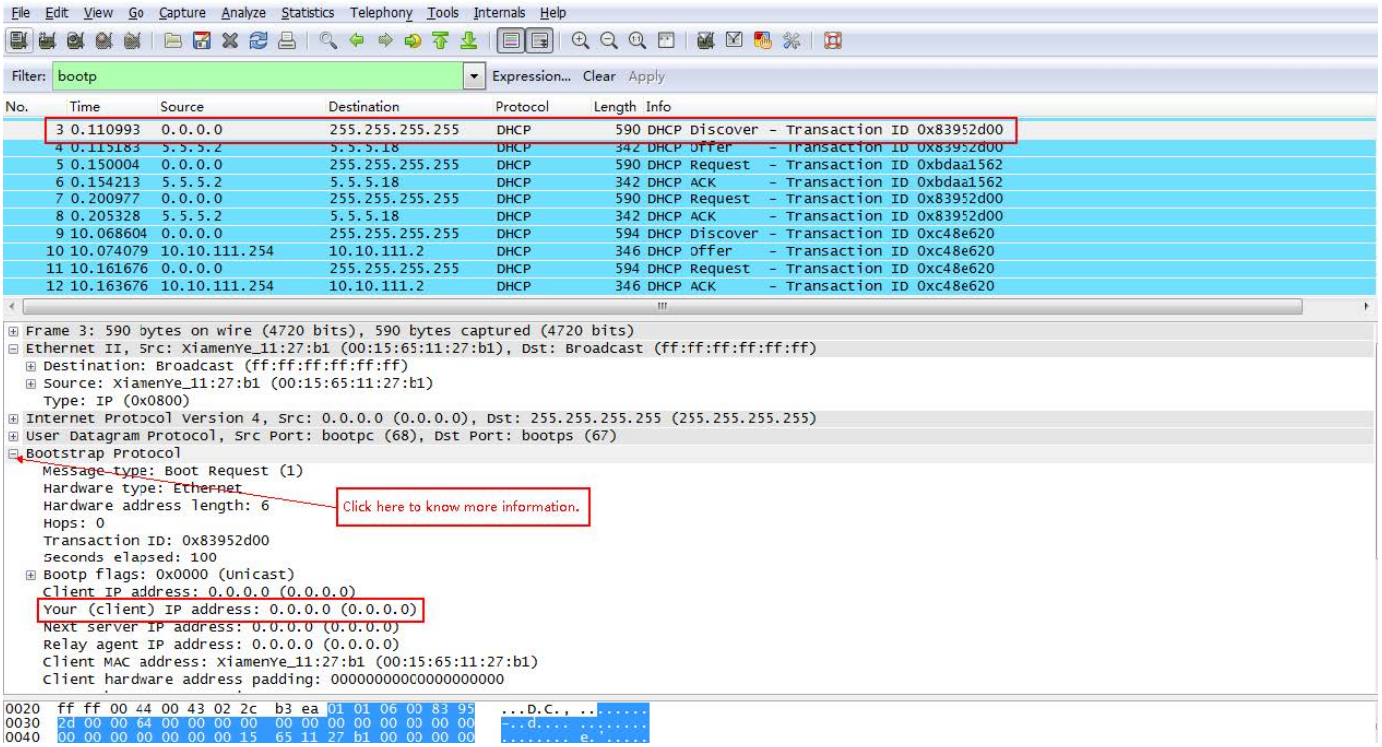
Verify the Configuration

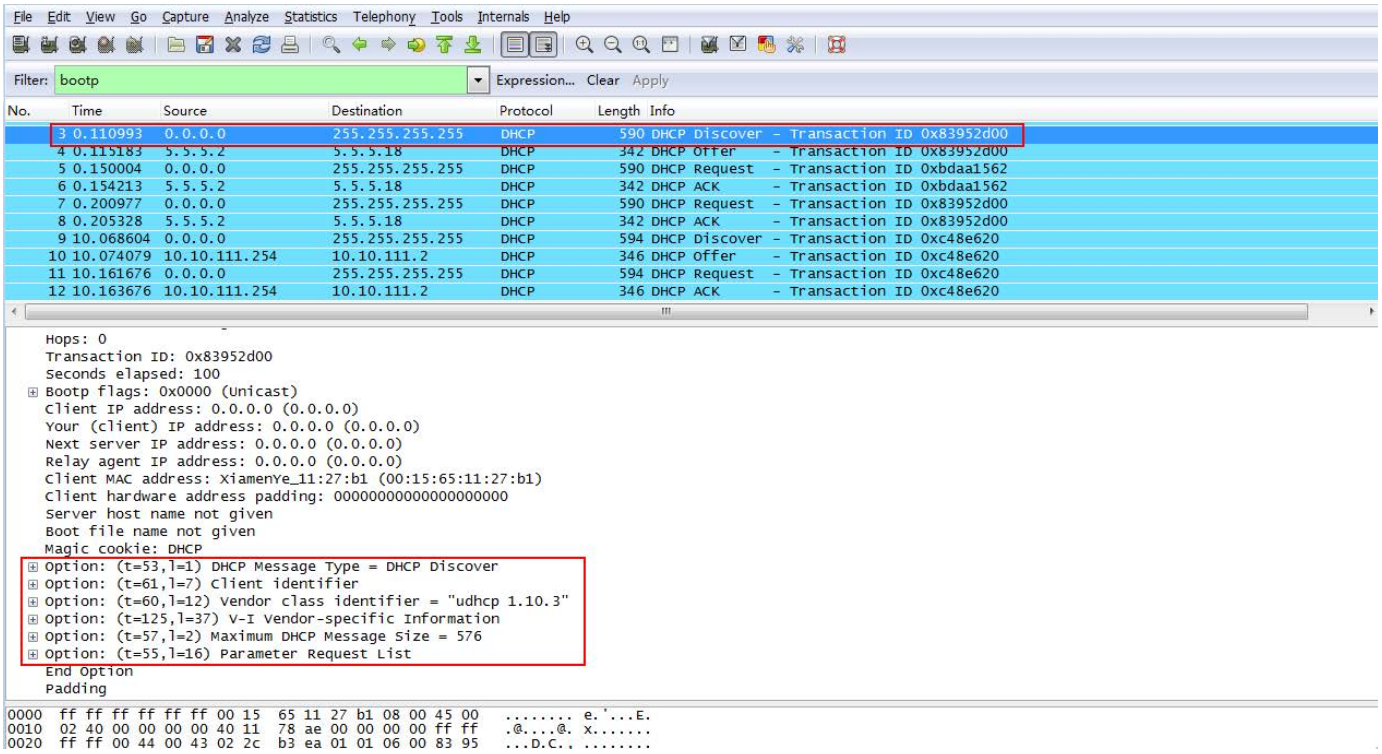
When the IP phone is configured to use DHCP for VLAN discovery, and the DHCP option is set to 132, the following processes occur:

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 the 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.

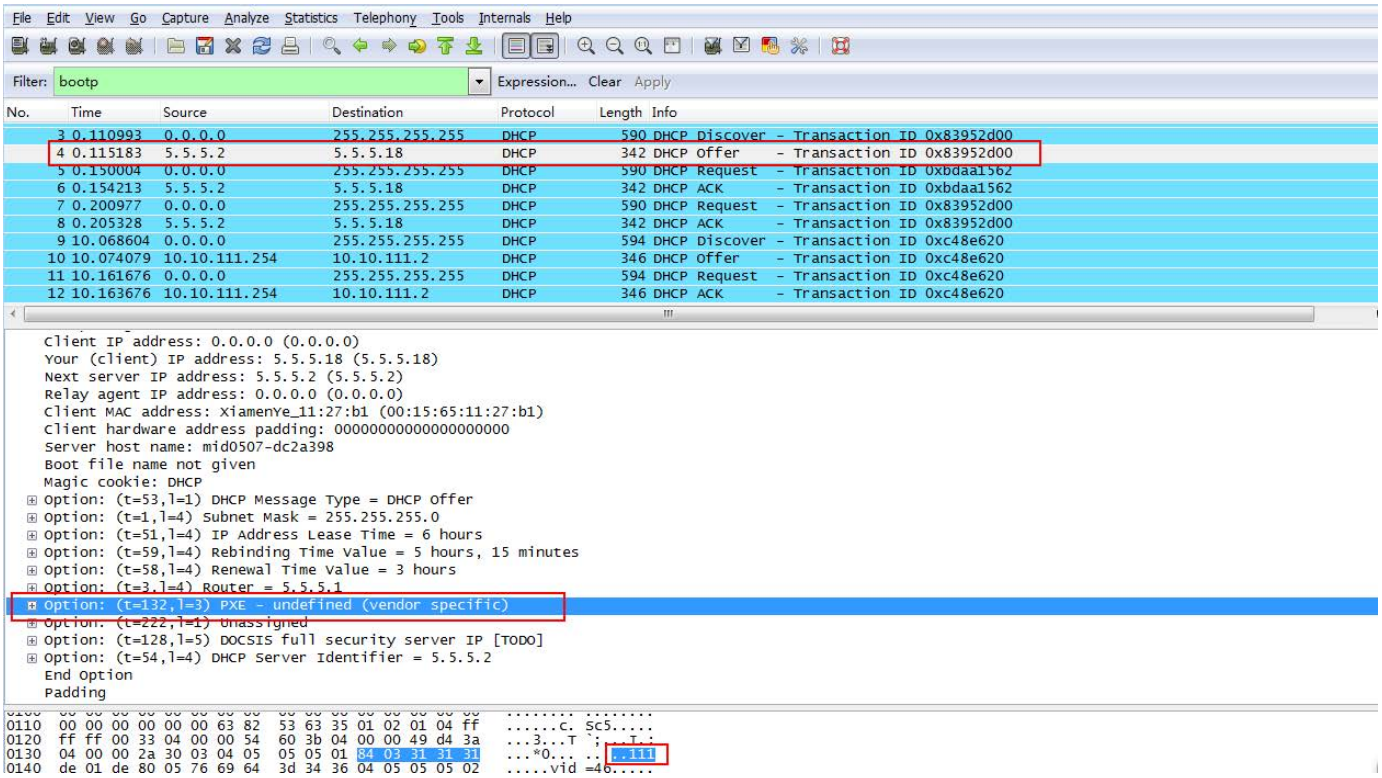
After this process, the phone will send all packets with the VLAN ID obtained from the DHCP server in the DHCP option 132.

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

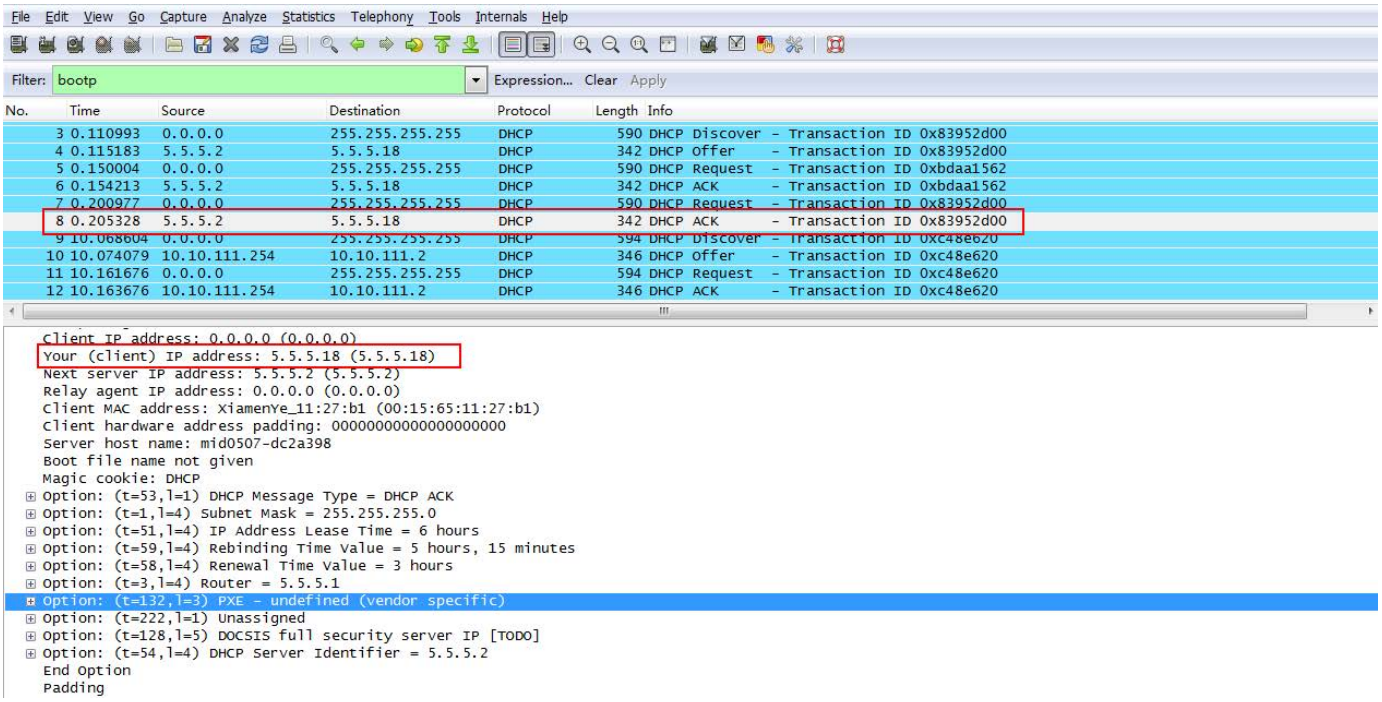




The following figure shows the DHCP Offer message received by the IP phone (the DHCP server sends a DHCP Offer message with the Option 132):

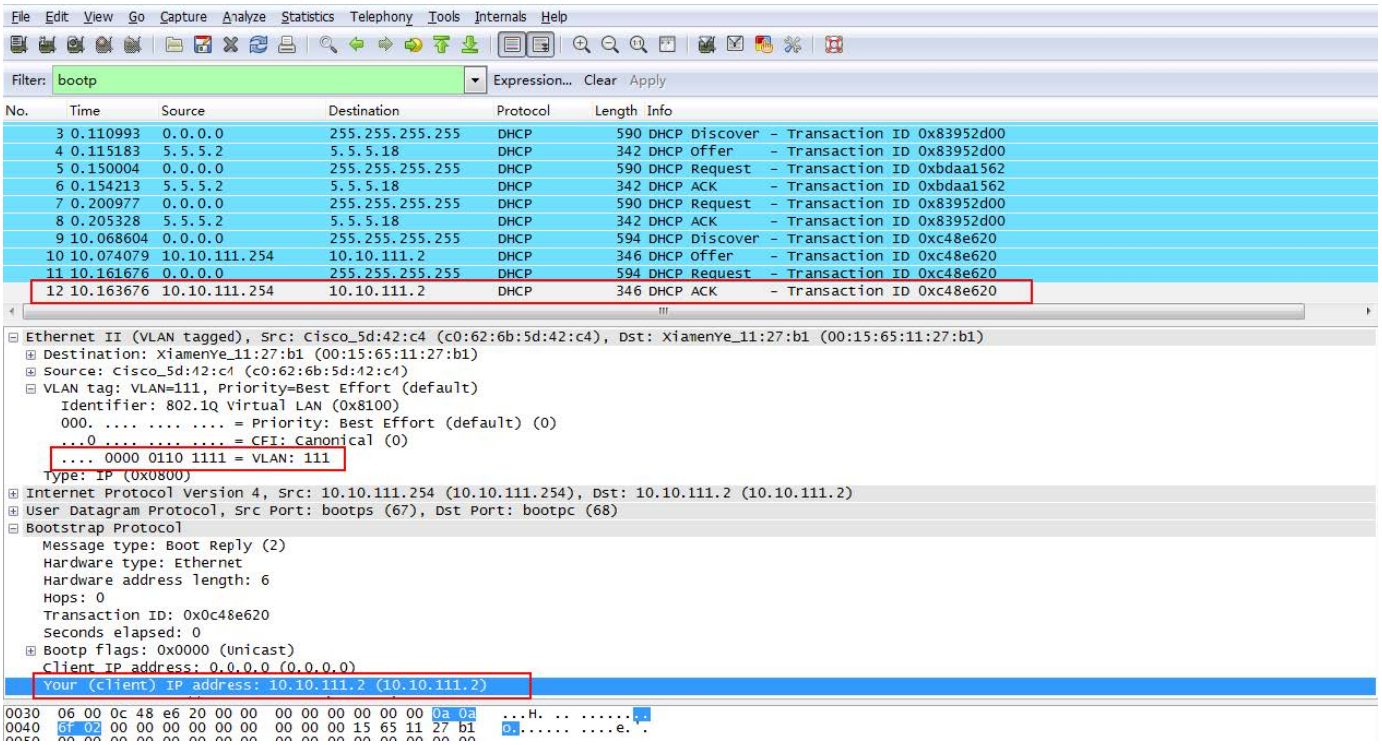


The following figure shows the DHCP message received by the IP phone (the DHCP server sent the ACK message to the phone):



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

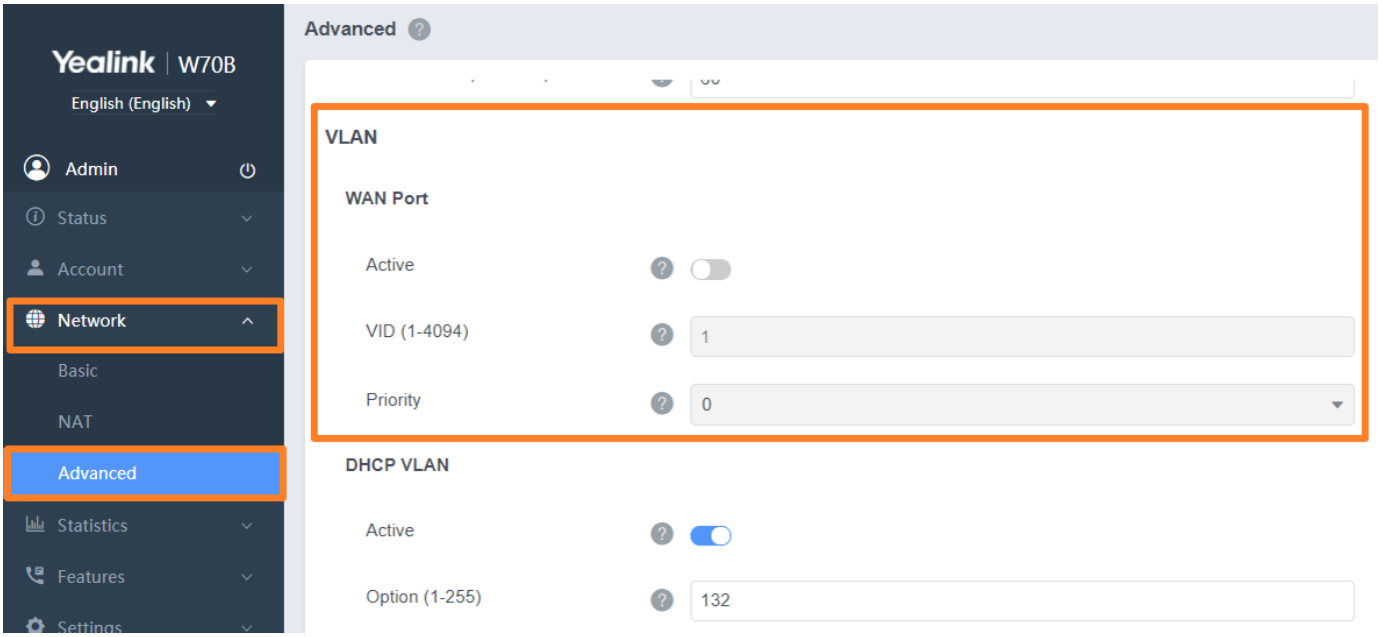
Description

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

Configure VLAN Feature

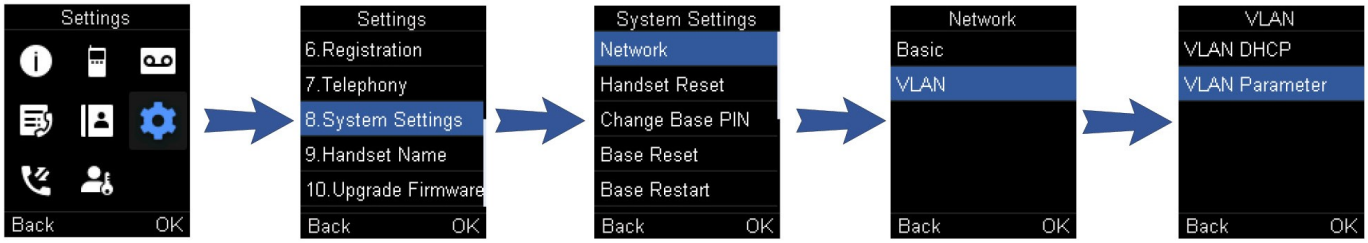
Set via the Web User Interface

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



Set via the Device Interface (W70B)

- W53H/W56H/W57R/W59R/W59R Pro/W71H/W73H/W74H/W78H:
- **OK** > **Settings** > **System Settings** > **Network (default PIN: 0000)** > **VLAN** > **VLAN Parameter**.



- DD Phone:
- **Menu** > **Advanced Settings (default password: 0000)** > **Network** > **VLAN** > **WAN Port**.
- CP930W:
- **Menu** > **Settings** > **Advanced Settings (default PIN: 0000)** > **Network** > **VLAN** > **VLAN Parameter**.
- CP935W:
- **More** > **Advanced (default PIN: 0000)** > **Network** > **VLAN** > **WAN Port** > **VLAN Status**.

Configuration Parameter

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

Parameter	Permitted	Def	Description

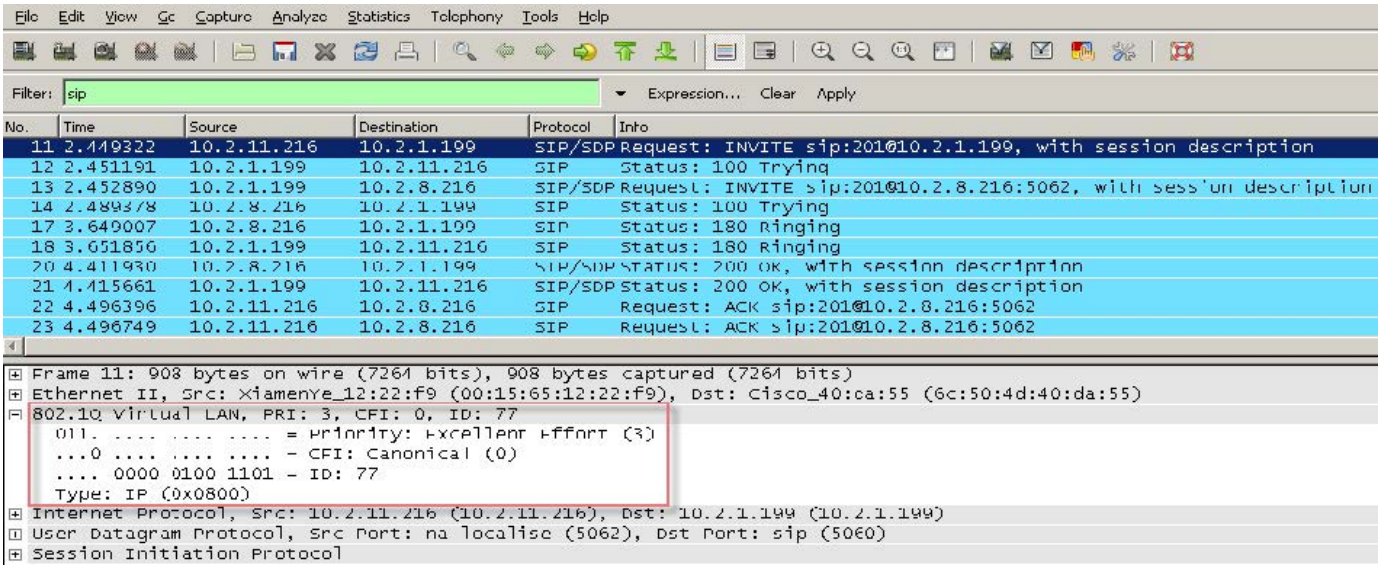
	Values	aul t	
static.network.vlan.internet_port_enable[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the VLAN for the Internet port.
static.network.vlan.internet_port_vid[1]	Integer from 1 to 4094	1	It configures the VLAN ID for the Internet port. It works only if "static.network.vlan.internet_port_enable" 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 the 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

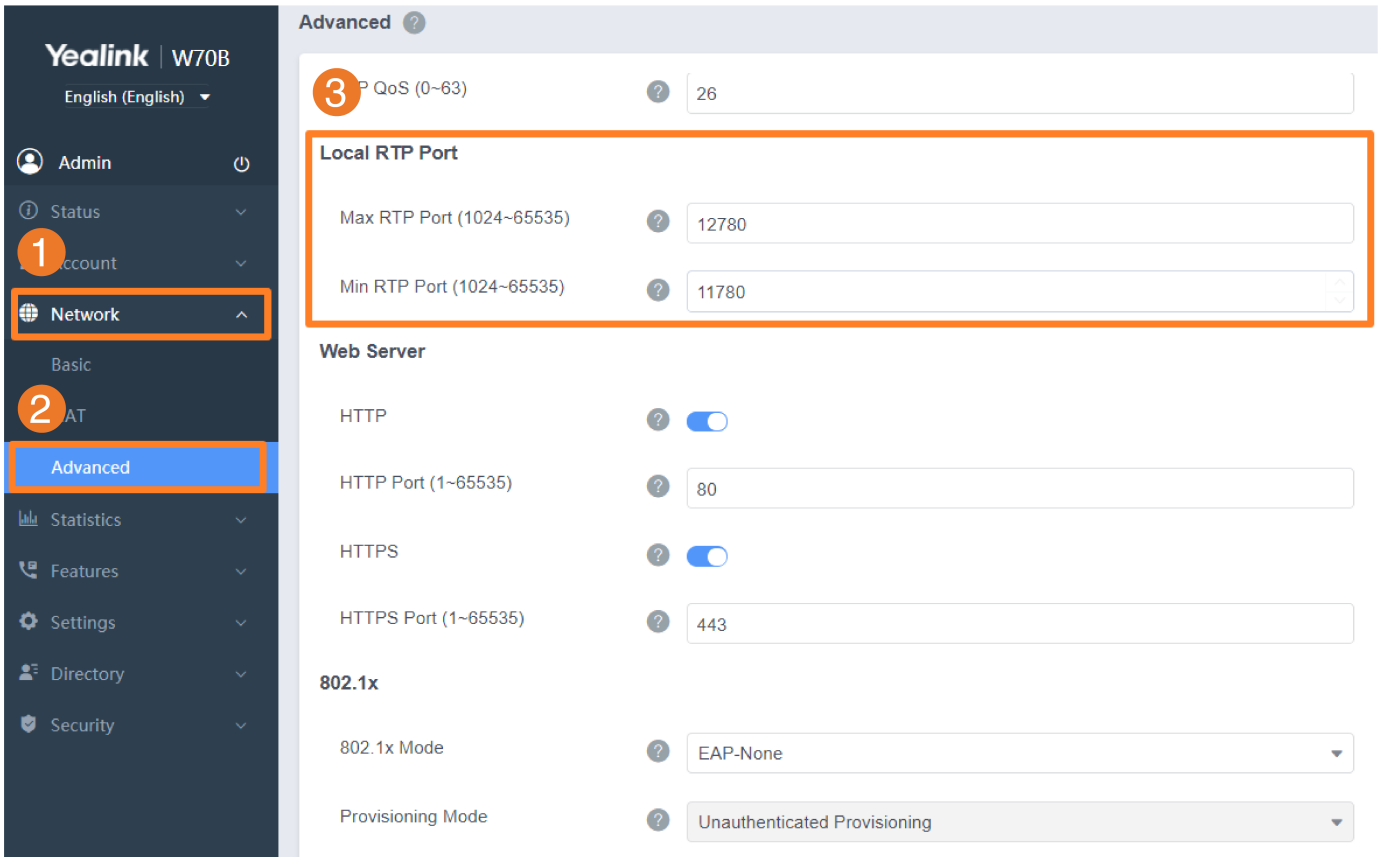
Introduction

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	11780	It configures the minimum local RTP port.
static.network.port.max_rtpport[1]	Integer from 1024 to 65535	12780	It configures the maximum local RTP port.
static.dm.X.network.port.min_rtpport[1] [2]	Integer from 1024 to 65535	11780	It configures the minimum local RTP port of the DM.
static.dm.X.network.port.max_rtpport[1] [2]	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.
[2]The parameter is only applicable to W90 Multi-Cell System. X is the DM ID. X=1-10.

Network Address Translation (NAT)

Introduction

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

NAT Traversal

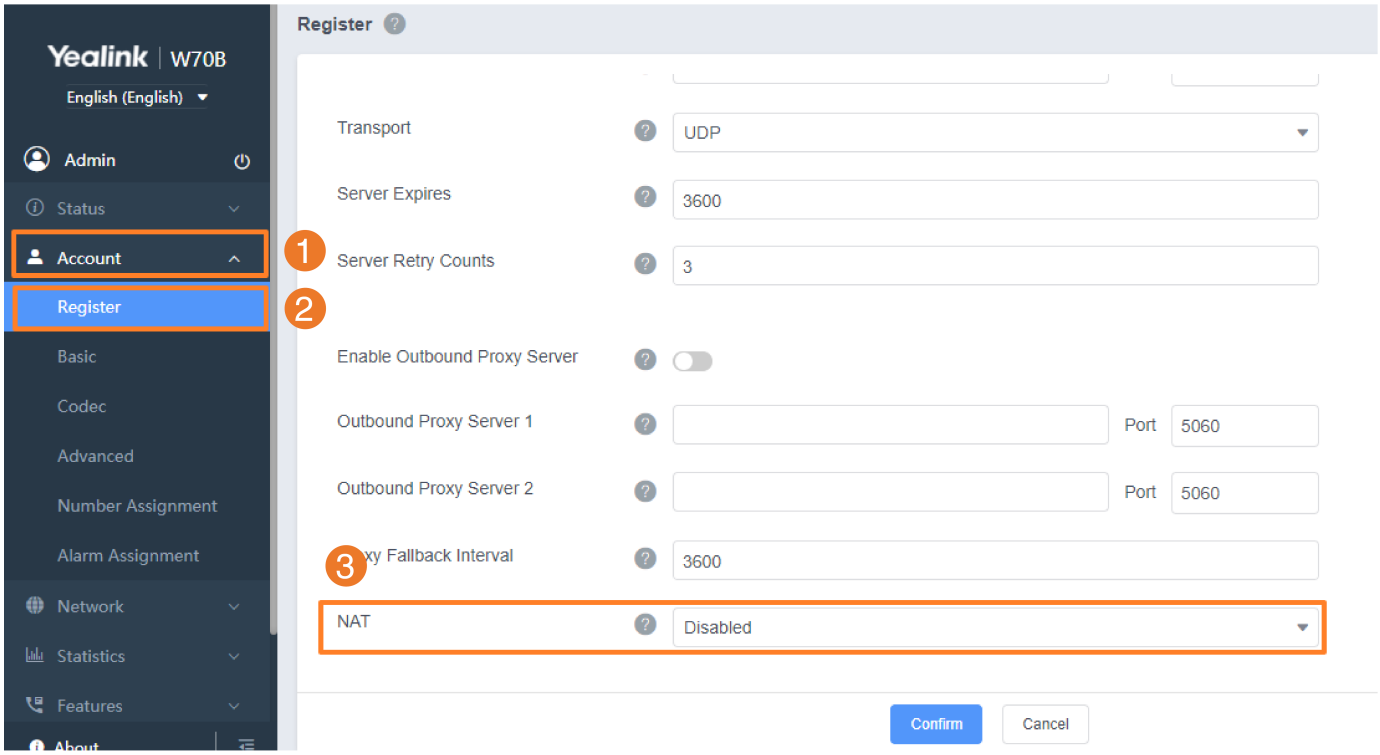
The phones can traverse NAT gateways to establish and maintain connections with external devices.

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.

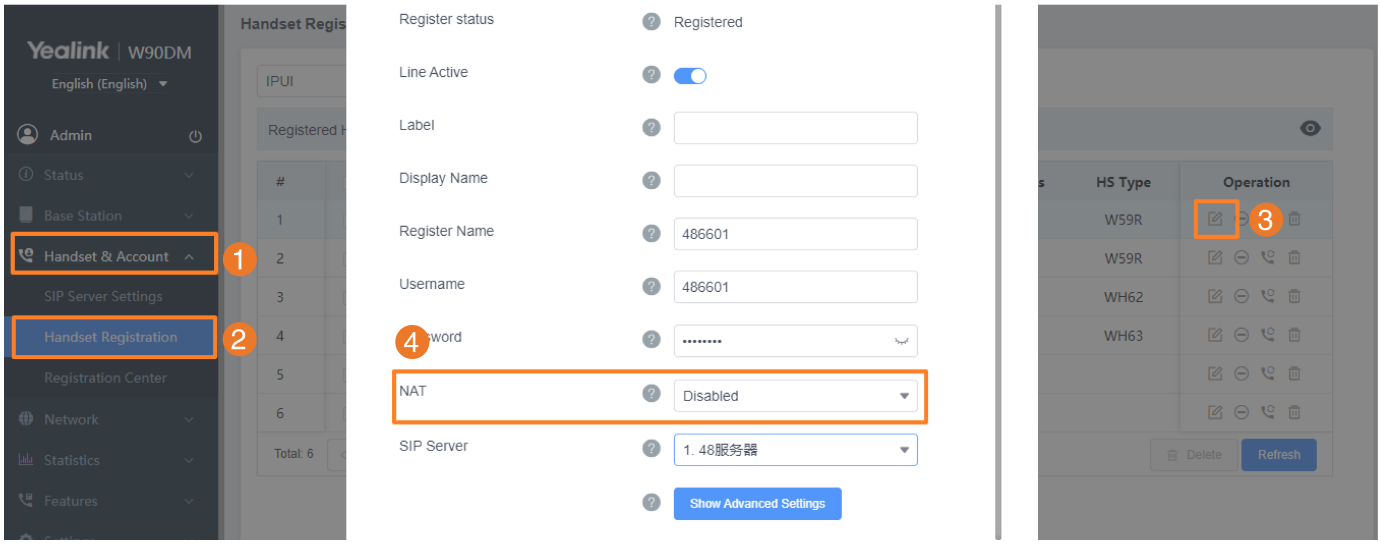
NAT Traversal Configuration

Set via the Web User Interface

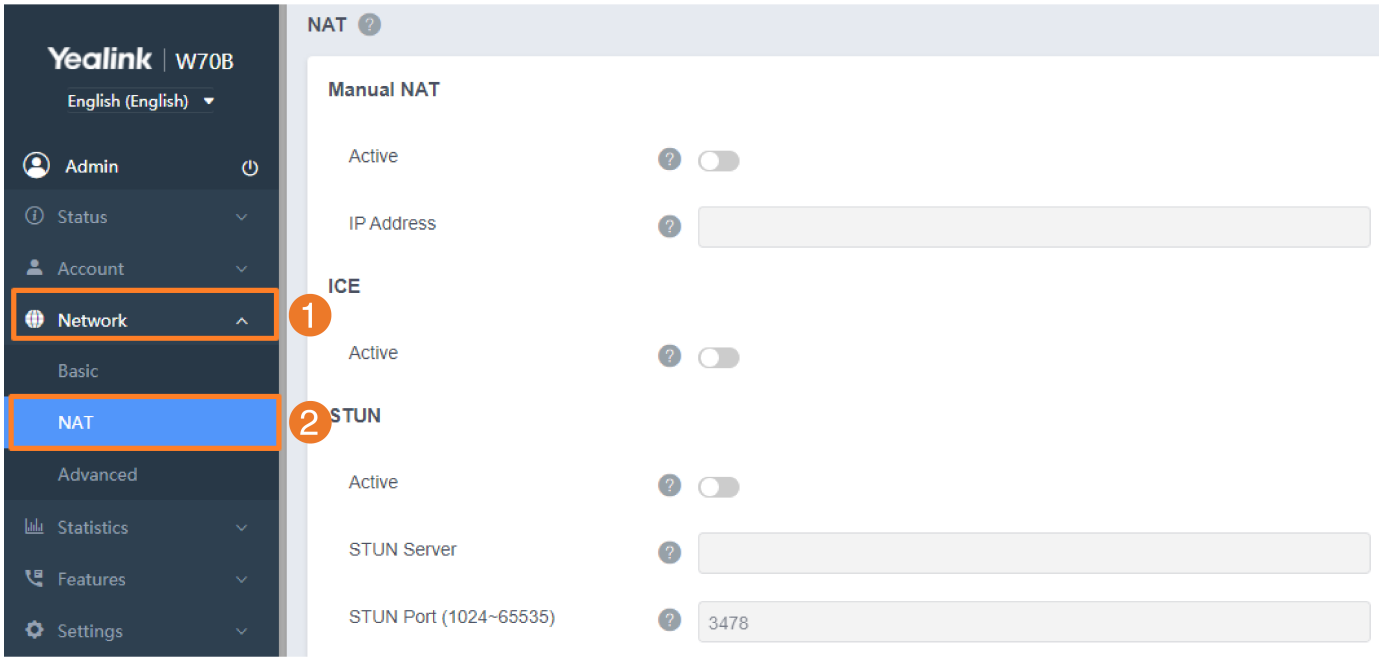
1. For W70B: On the web user interface, go to **Account** > **Register** > **NAT.**



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **NAT**.



3. 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_stun.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the STUN (Simple Traversal of UDP over NATs) feature.
static.sip.nat_stun.server	String	Blank	It configures the IP address or domain name of the STUN server. It works only if "static.sip.nat_stun.enable" is set to 1 (Enabled).
static.sip.nat_stun.port	Integer from 1024	3478	It configures the port of the STUN server. It works only if "static.sip.nat_stun.enable" is

	to 65535		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[3]	**0**-Disabled **1**-Enabled	0	It enables or disables the media stream to be forwarded forcibly 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] [3]	**0**-Disabled **1**-Enabled	Blank	It enables or disables the media stream to be forwarded forcibly 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.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

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

[3]The parameter is only applicable to W75/W80/W90 multi-cell system.

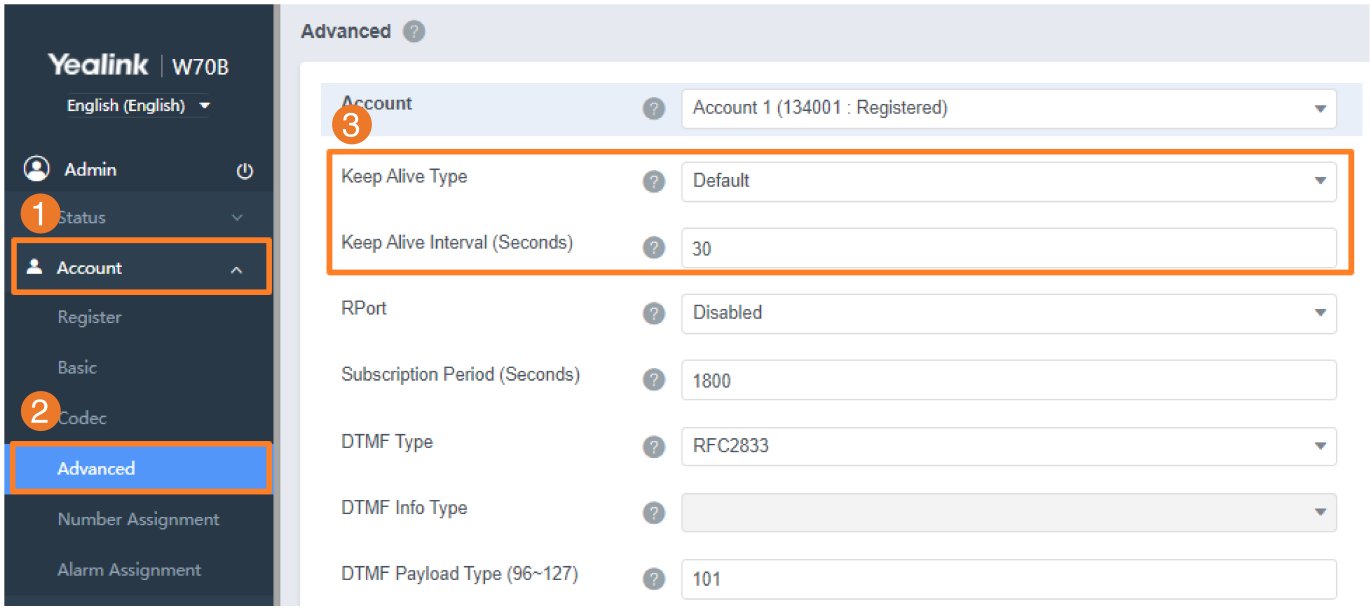
Keep Alive

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

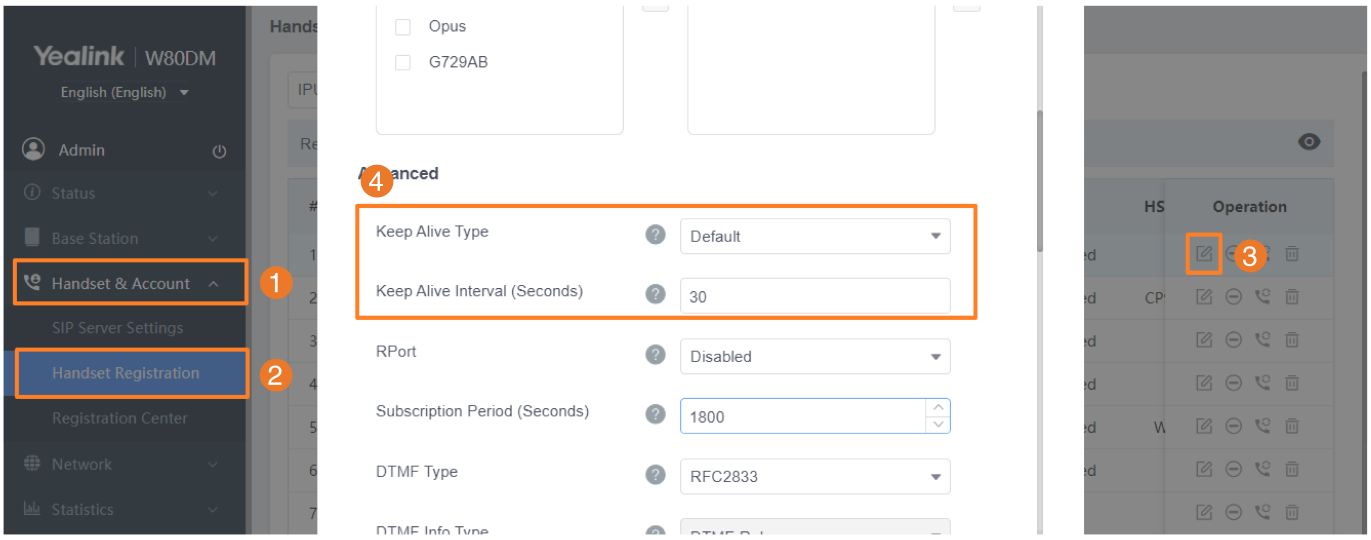
Keep Alive Configuration

Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Advanced** > **Keep Alive Type**/**Keep Alive Interval(Seconds)**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **Keep Alive Type**/**Keep Alive Interval (Seconds)**.



Configuration Parameter

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

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

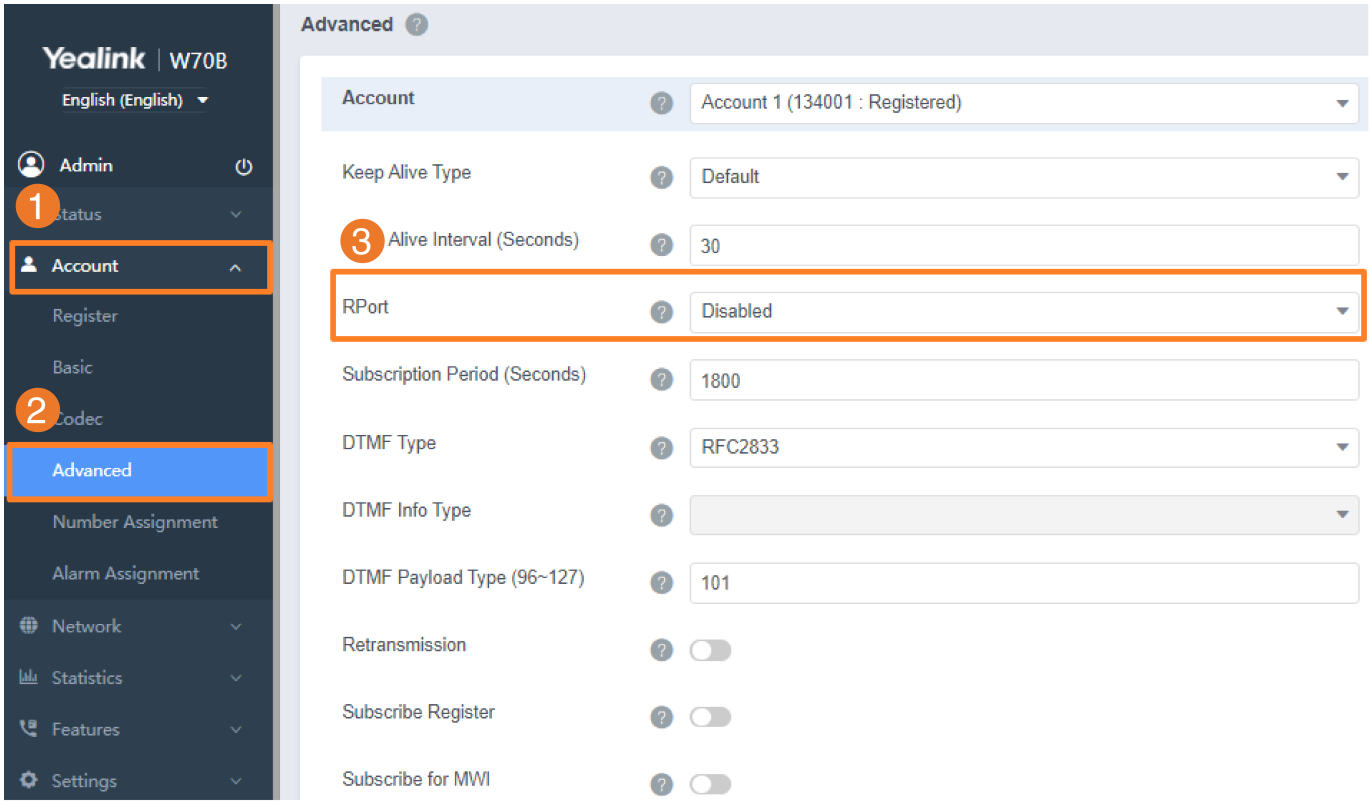
Rport allows a client to request that the server send the response back to the source IP address and port from which the request originated. It helps the phone traverse symmetric NATs.

Rport feature depends on support from a SIP server. For more information, refer to RFC 3581.

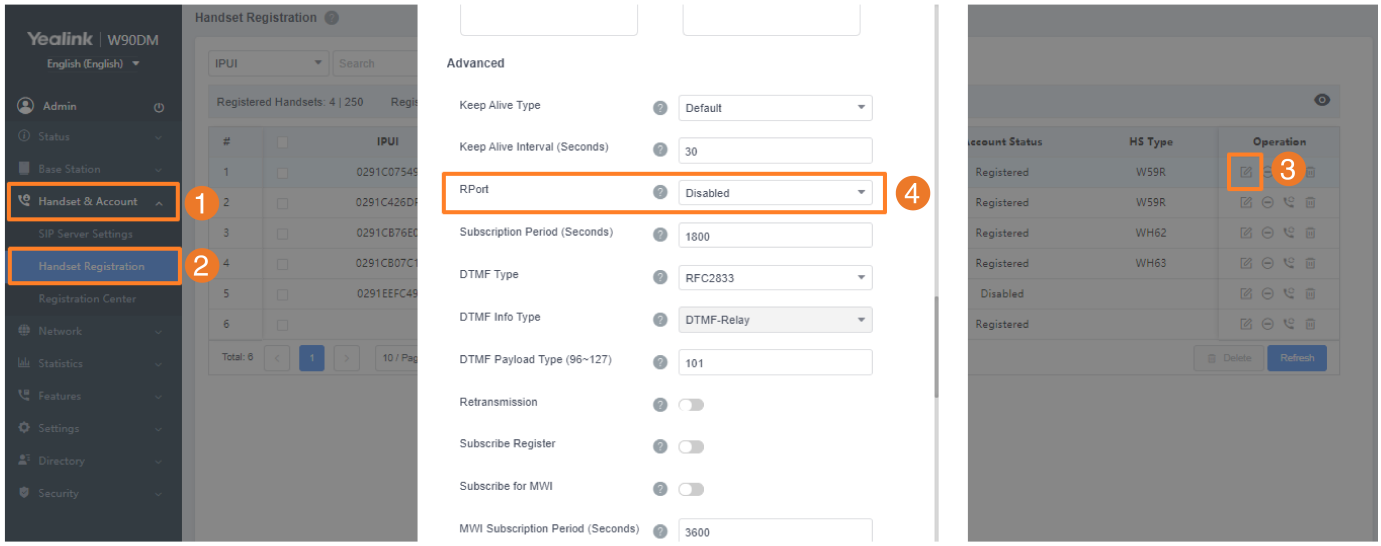
Rport Configuration

Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Advanced** > **RPort**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **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.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

SIP Port and TLS Port

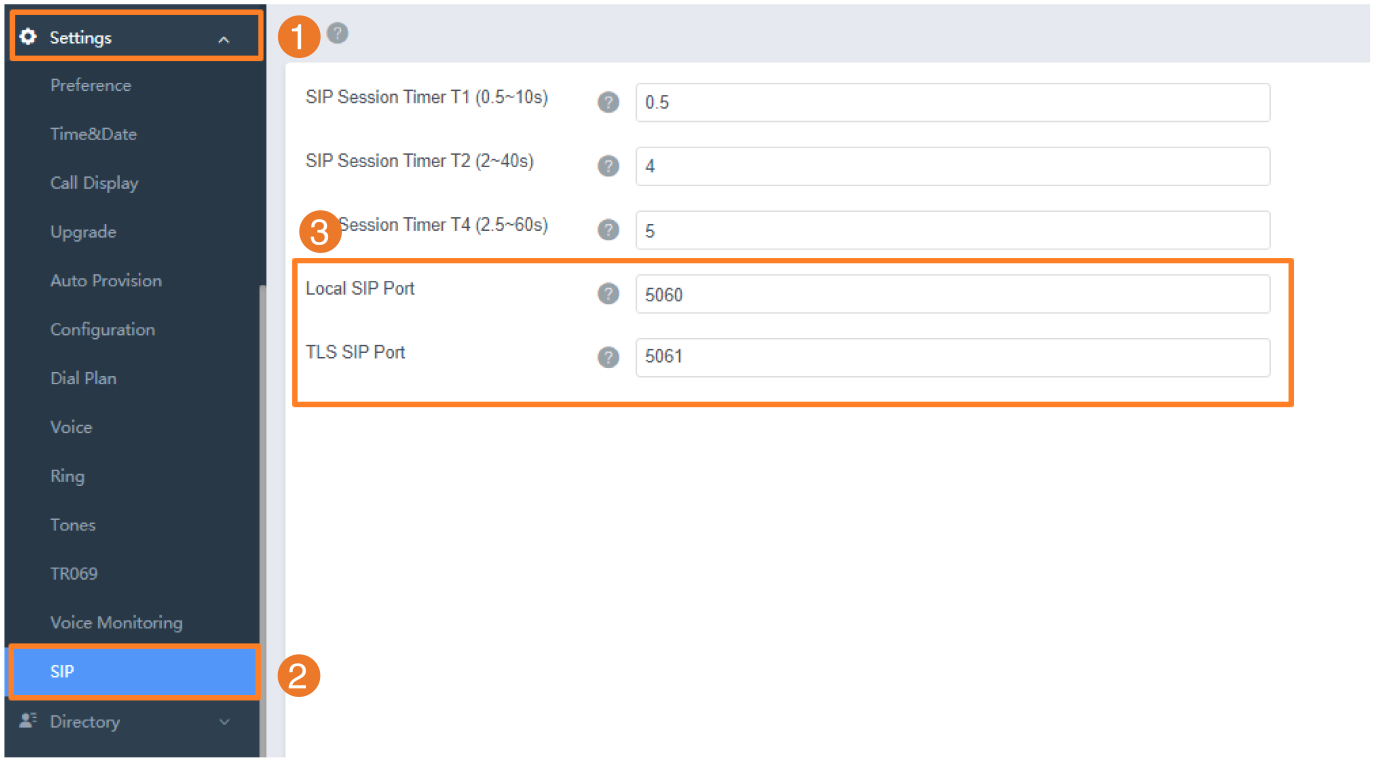
You can configure the SIP and TLS source ports on the phone. Otherwise, the phone uses default values (5060 for UDP/TCP and 5061 for TLS).

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

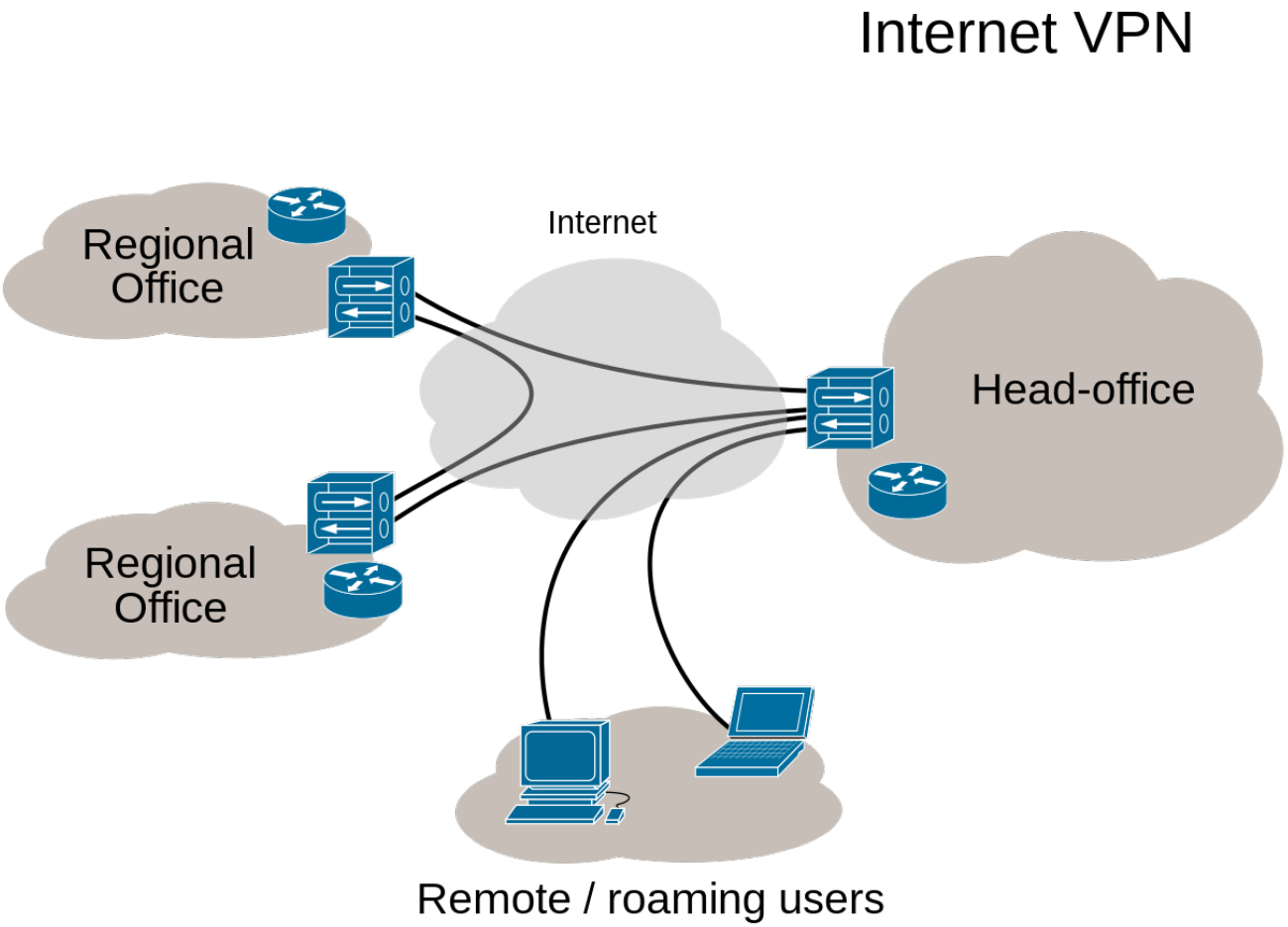
sip.listen_port
sip.tls_listen_port

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

VPN

About VPN

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



Types of VPN Access

Type	Description
Remote access	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, which means site-to-site VPN can be used to connect a branch or remote office network to a company headquarters network. Each site is equipped with a VPN gateway, such as a router, firewall, VPN concentrator, or security appliance.

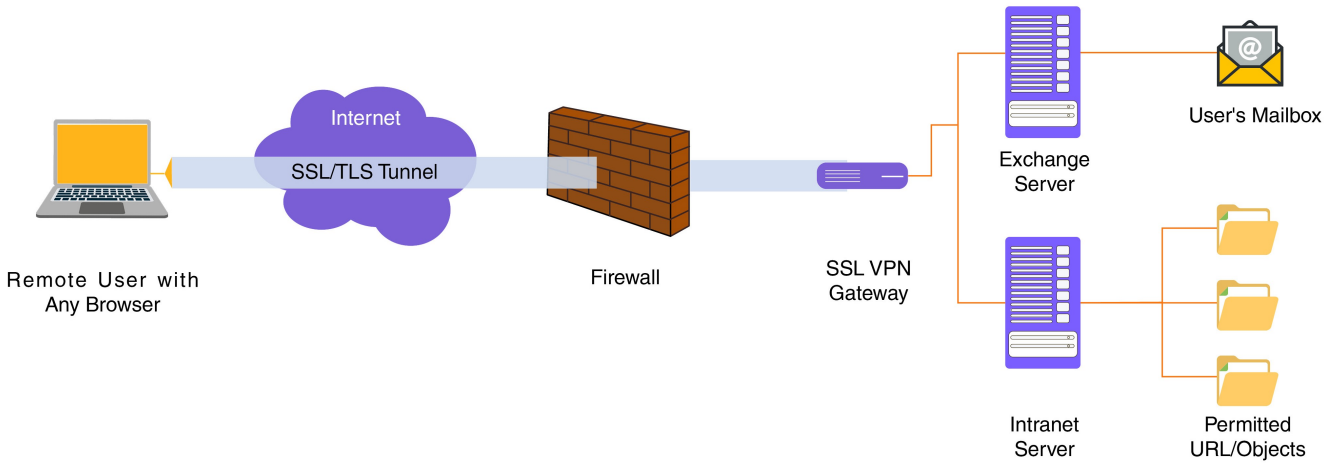
VPN Technology

VPN technology is based on the idea of tunneling. VPN tunneling involves establishing and maintaining a logical network connection (that may contain intermediate hops). In 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 Sockets Layer) and **IPSec** (Internet Protocol Security).

SSL VPN

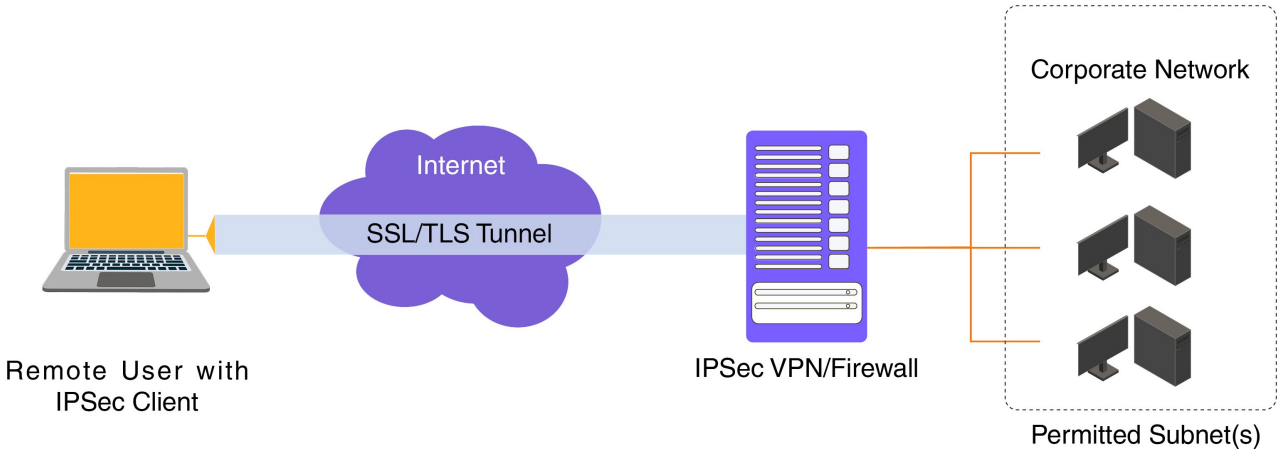
SSL VPN uses the SSL protocol and Transport Layer Security (TLS) protocol to provide a secure connection between remote users and internal network resources. It can be used with a standard web browser and does not require the installation of specialized client software on the end user's device. An SSL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

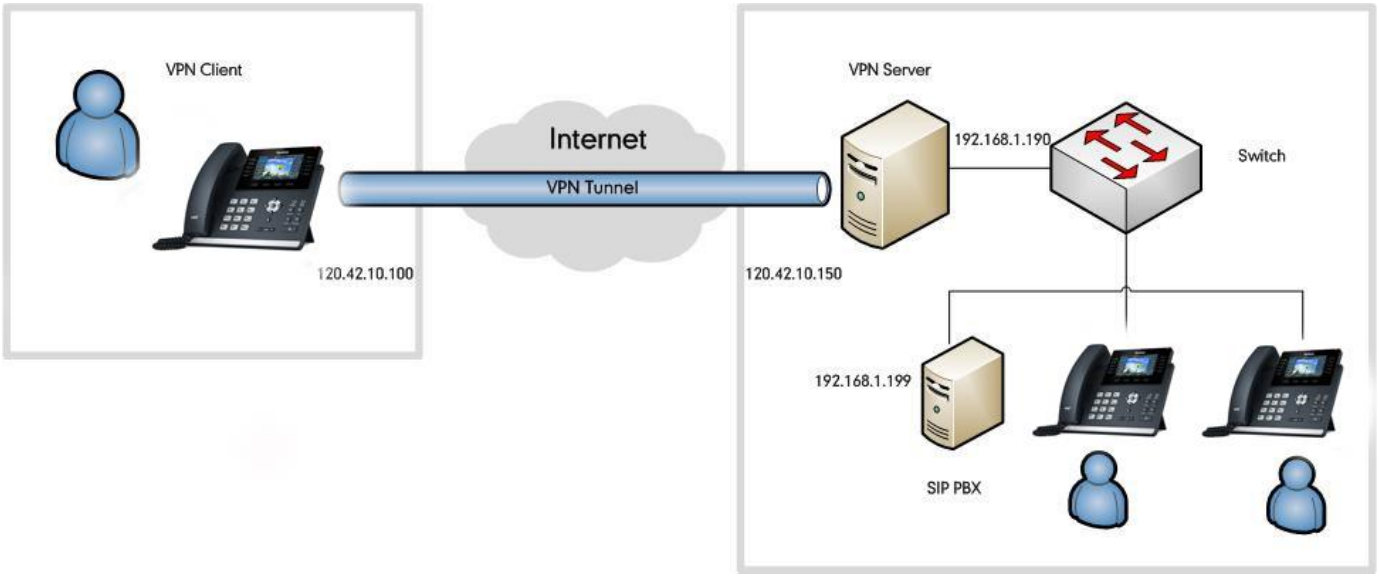
An IPSec VPN uses the standard IPSec mechanism to establish a VPN connection over the public Internet. IPSec is a framework for a set of protocols for security at the network or packet processing

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 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 at 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 and 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 etc]# cd openvpn 2.1.4
```

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 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.

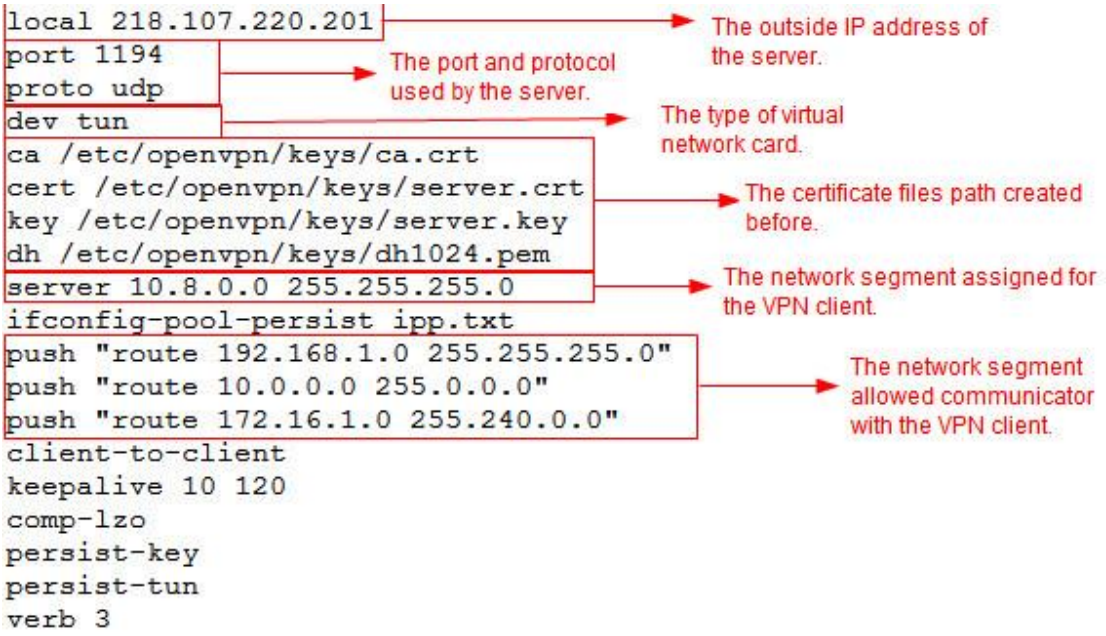
```
[root@localhost openvpn 2.1.4]# cp sample config files/server.conf /etc/openvpn
```

6. Edit the file "server.conf" according to your actual network environment and save the changes.

```
[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.
3. [root@localhost ~]# vi /etc/sysctl.conf
4. 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 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 in 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!".

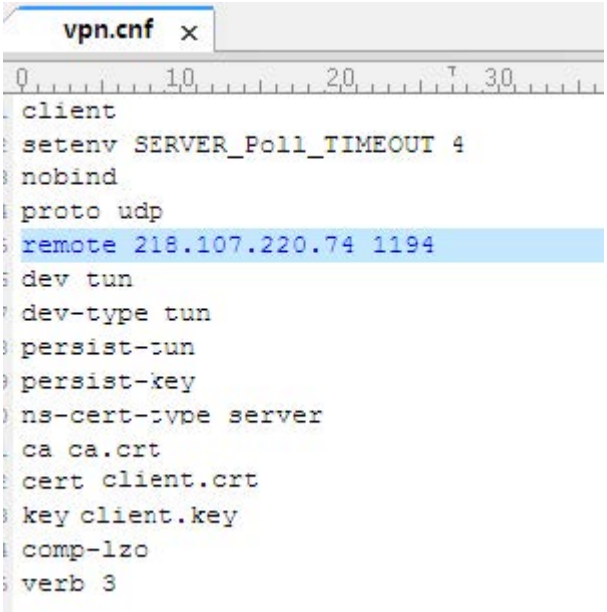
The following parameters should be configured as the same as those of the server.

```
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
```

3. Click **Start** > **Run**.
4. Enter **cmd** in the pop-up dialogue box and click **OK** to open a command prompt screen.

5. 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
```

6. Enter the following commands.

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

7. Generate a CA certificate.

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

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

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

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

```
Common Name (eg, your name or your server's hostname) []: CA
Email Address [admin@yealink.com]:
```

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

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

The screen prompts the following information:

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

9. Generate a certificate for the OpenVPN server.

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

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

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

```
Organization Name (eg, company) [Yealink]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []: Server
Email Address [admin@yealink.com]:
Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:serverpwd
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state-done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'FJ'
localityName :PRINTABLE:'XM'
organizationName :PRINTABLE:'Yealink'
organizationalUnitName:PRINTABLE:'EMB'
commonName :PRINTABLE:'Server'
emailAddress :IA5STRING:'admin@yealink.com'
Certificate is to be certified until Jan 20 13:10:22 2023 GMT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

10. Generate a certificate for the client.

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

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

```
Loading 'screen' into random state done
Generating a 1024 bit RSA private key
.....++++++
```

.....++++++
writing new private key to 'keys\Client.key'

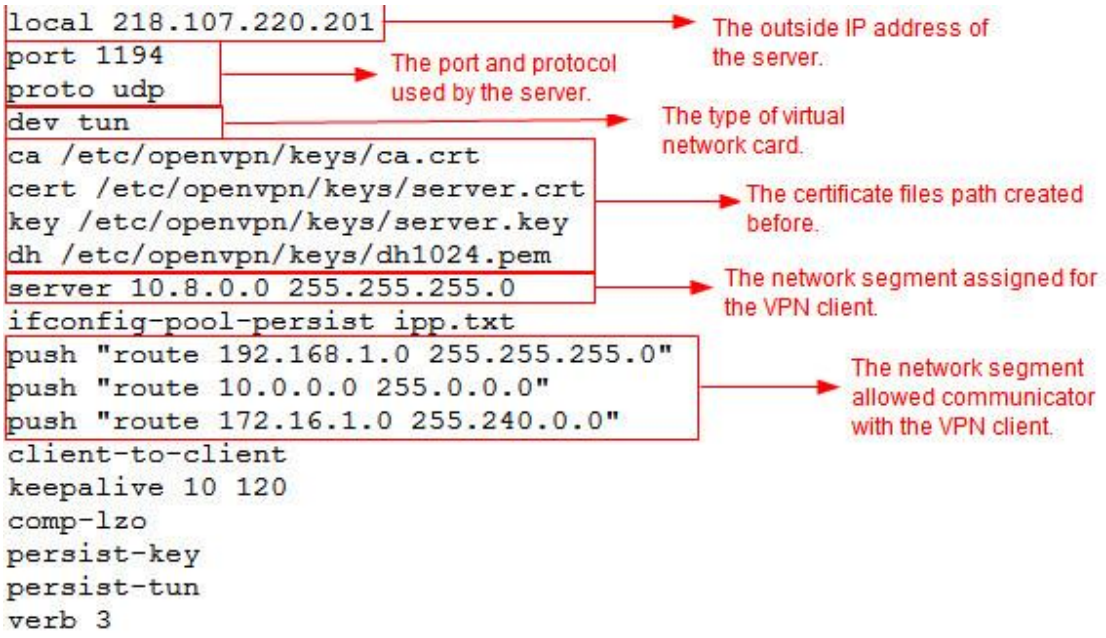
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [CN]:
State or Province Name (full name) [FJ]:
Locality Name (eg, city) [XM]:
Organization Name (eg, company) [Yealink]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []: Client
Email Address [admin@yealink.com]:
Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:clientpwd
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state-done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'FJ'
localityName :PRINTABLE:'XM'
organizationName :PRINTABLE:'Yealink'
organizationalUnitName:PRINTABLE:'EMB'
commonName :PRINTABLE:'Client'
emailAddress :IA5STRING:'admin@yealink.com'
Certificate is to be certified until Jan 20 13:10:22 2023 GMT (3650 days)
Sign the certificate? [y/n]:y

```
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

To configure the server's configuration file:

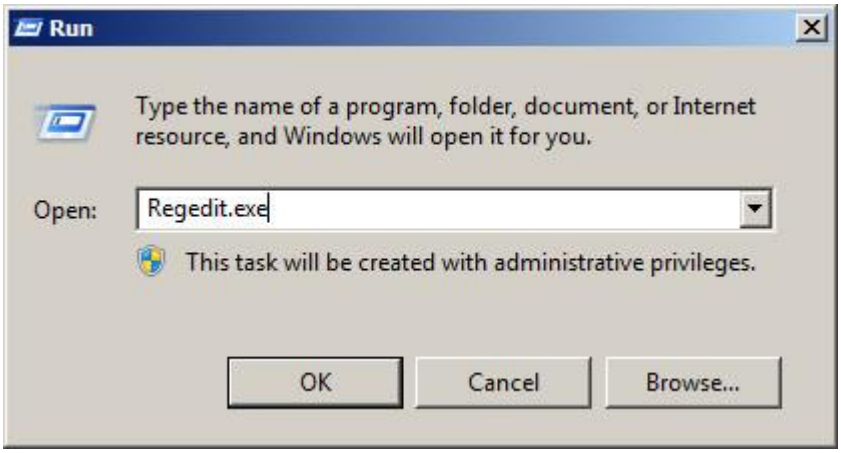
1. Enter the installation directory of the OpenVPN server.
2. Create a new folder "serverconfig" in the directory.
3. Copy the file "server.ovpn" in the sample config folder to the serverconfig folder created above.
4. Edit the file "server.ovpn" according to your actual network environment and save the change.
5. The following shows an example:



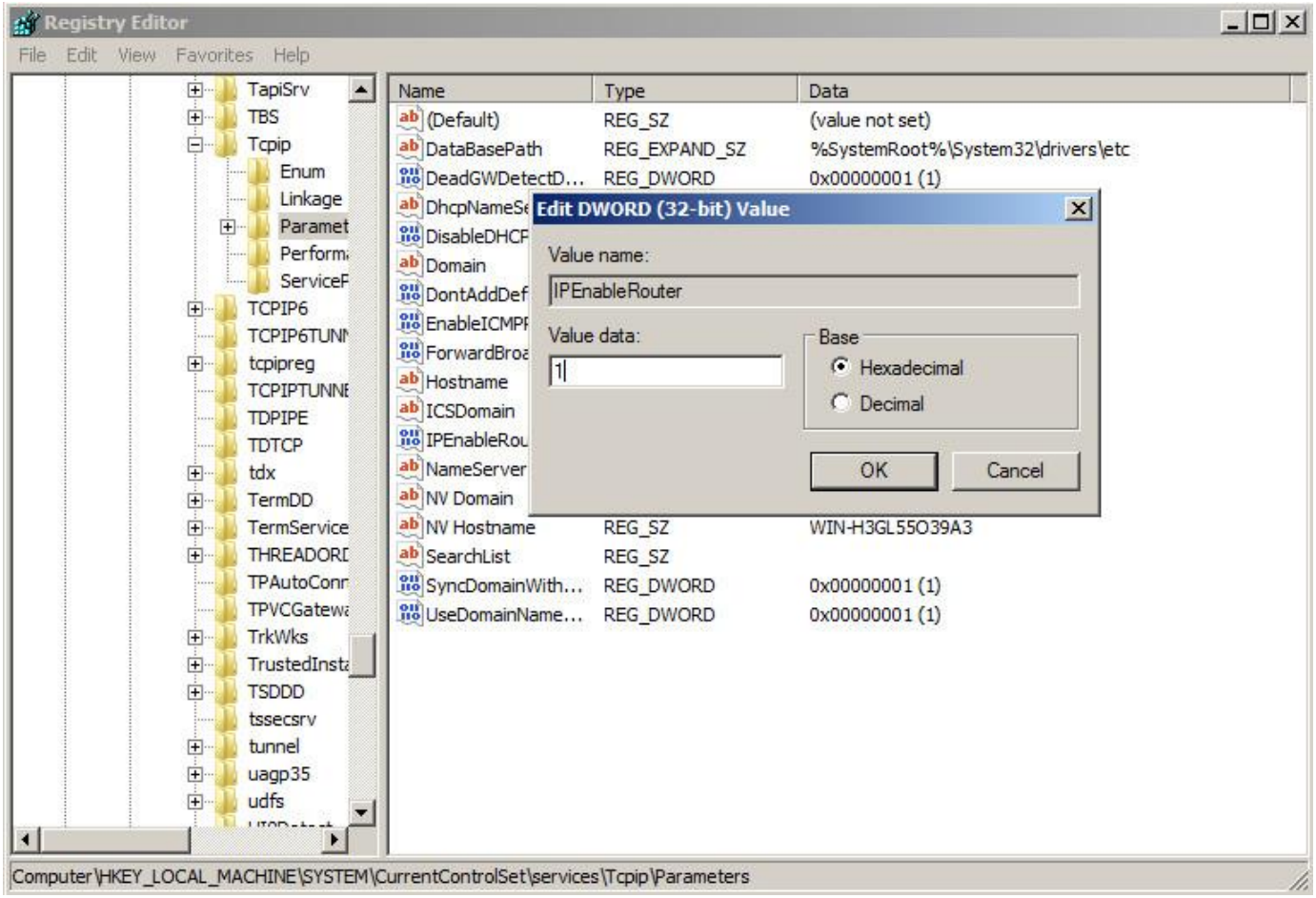
7. According to the actual network environment, configure the network settings of the server, such as the TCP/IP forwarding feature, Internet connection sharing feature and routing entries between the VPN clients and the Intranet. For more information, contact your network administrator.

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.

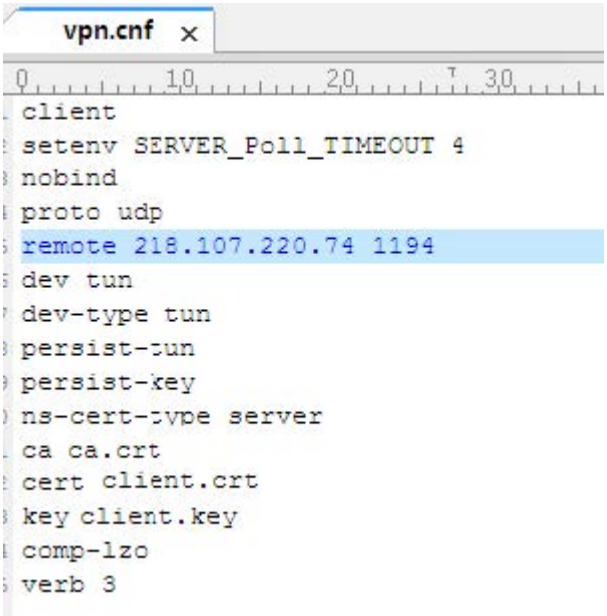
Create the OpenVPN Tar File for the VPN Client

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:

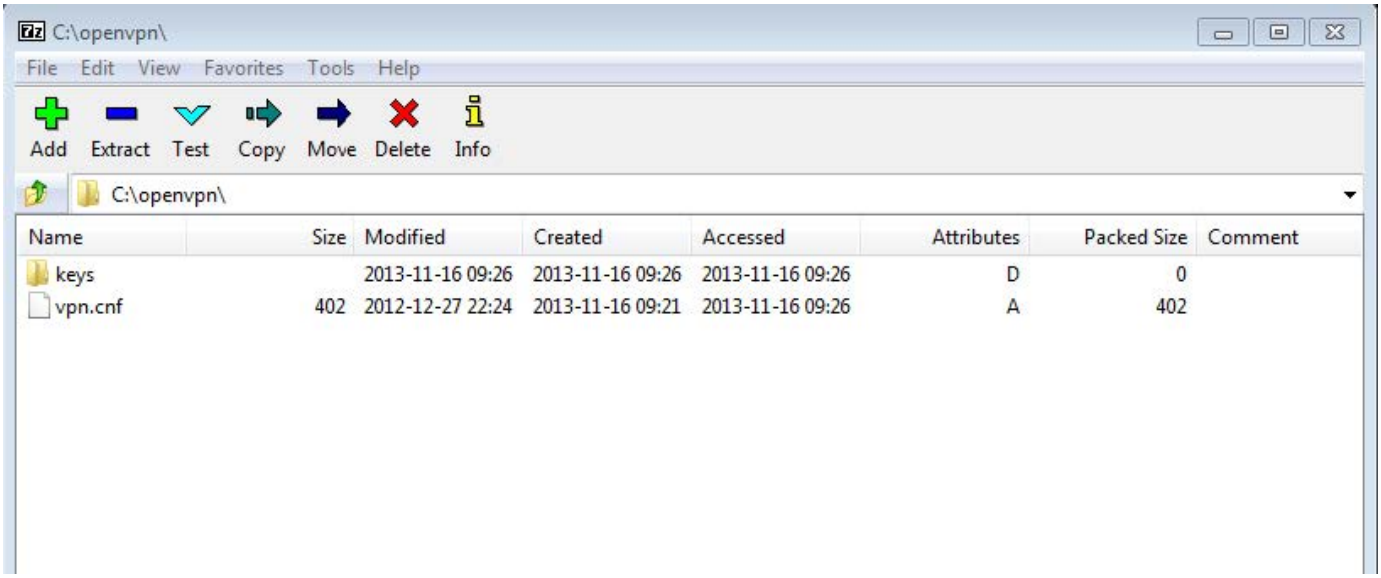
1. Create a new folder "openvpn" in the directory C:/.
2. Copy the file client.ovpn in the sample config folder to the openvpn folder.
3. Rename the file client.ovpn to vpn.cnf.
4. Create a new folder "keys" in the openvpn folder.
5. Copy ca.crt, client.crt, and client.key files to the keys folder created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



7. Save the change.

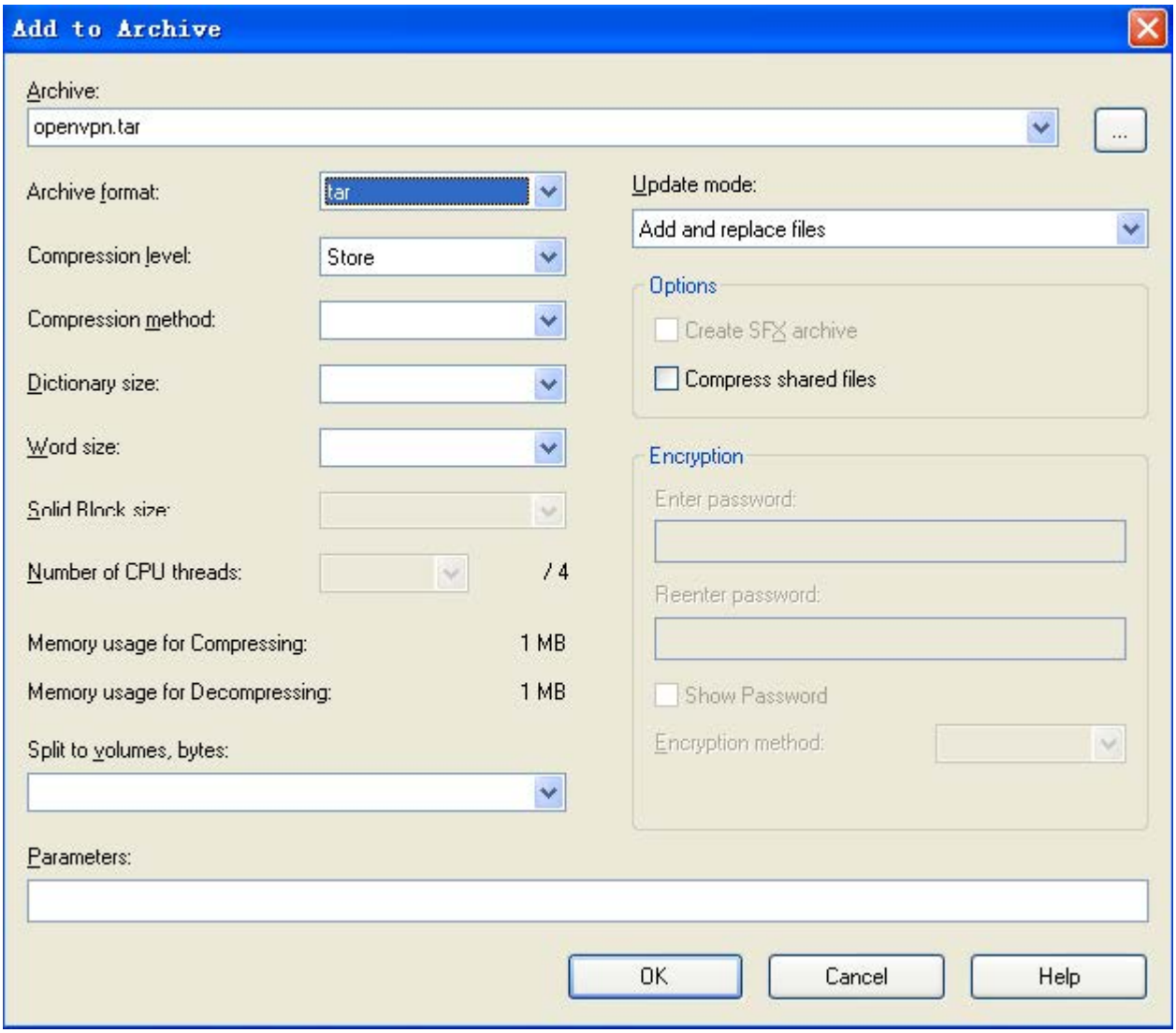
To package a TAR file using the tool 7-Zip on the Windows platform:

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

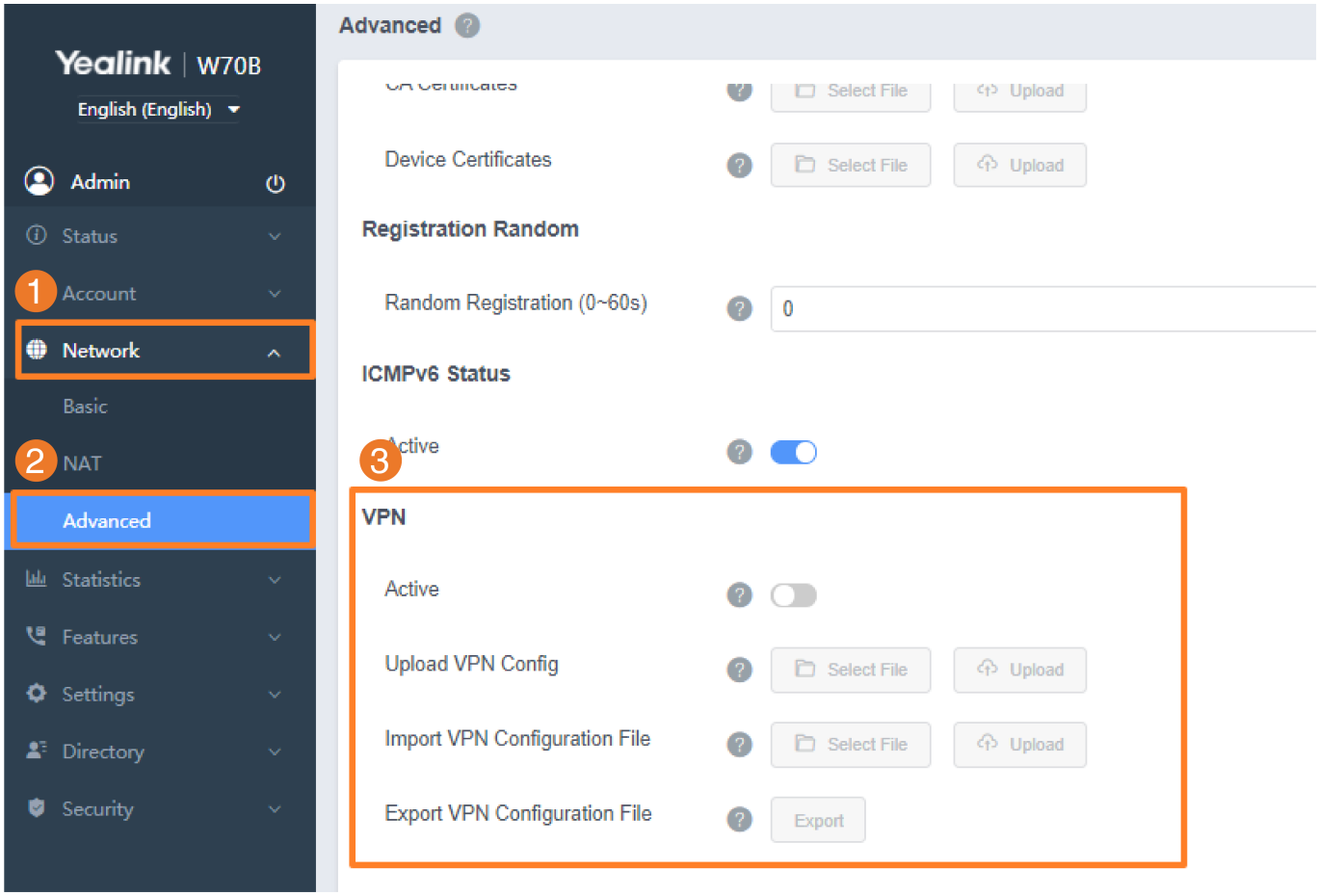
Configure OpenVPN Feature on IP Phones

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**.



Configuration Parameter

static.network.vpn_enable
static.openvpn.url
static.network.openvpn_file.url

Parameter	Permitted Values	Default	Description
static.network.vpn_	**0**-Disabled	0	It enables or disables the OpenVPN feature.

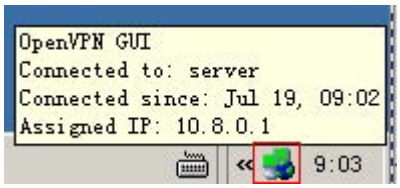
enable[1]	**1**-Enabled		
static.openvpn.url	URL within 511 characters	Blank	It configures the access URL of the *.tar file for OpenVPN.
static.network.openvpn_file.url[2]	String within 512 characters	Blank	It configures the URL for uploading the OpenVPN configuration file (vpn.cnf). It works only if "static.network.vpn.mode" is set to 1 (OpenVPN).

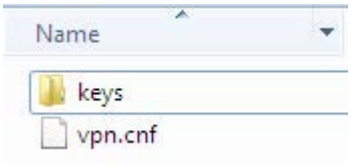
[1]If you change this parameter, the phone will reboot to make the change take effect.
[2]This parameter is only applicable to W70B.

Troubleshooting

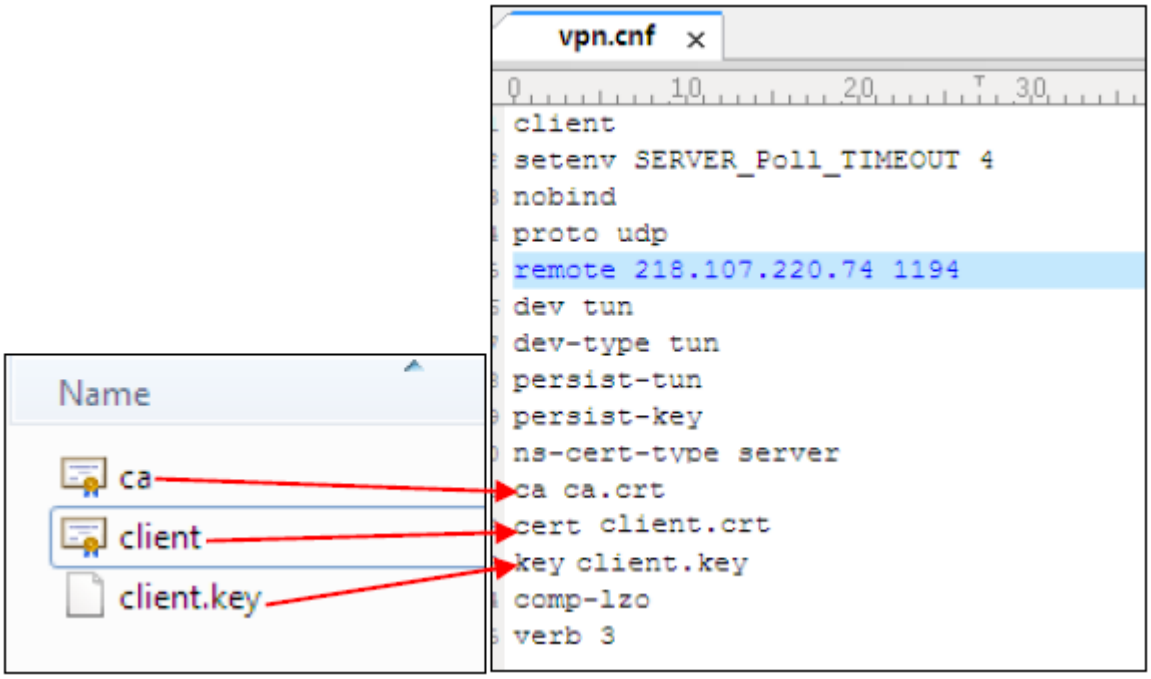
Why does the phone fail to connect to the OpenVPN server?

Do the following in sequence:

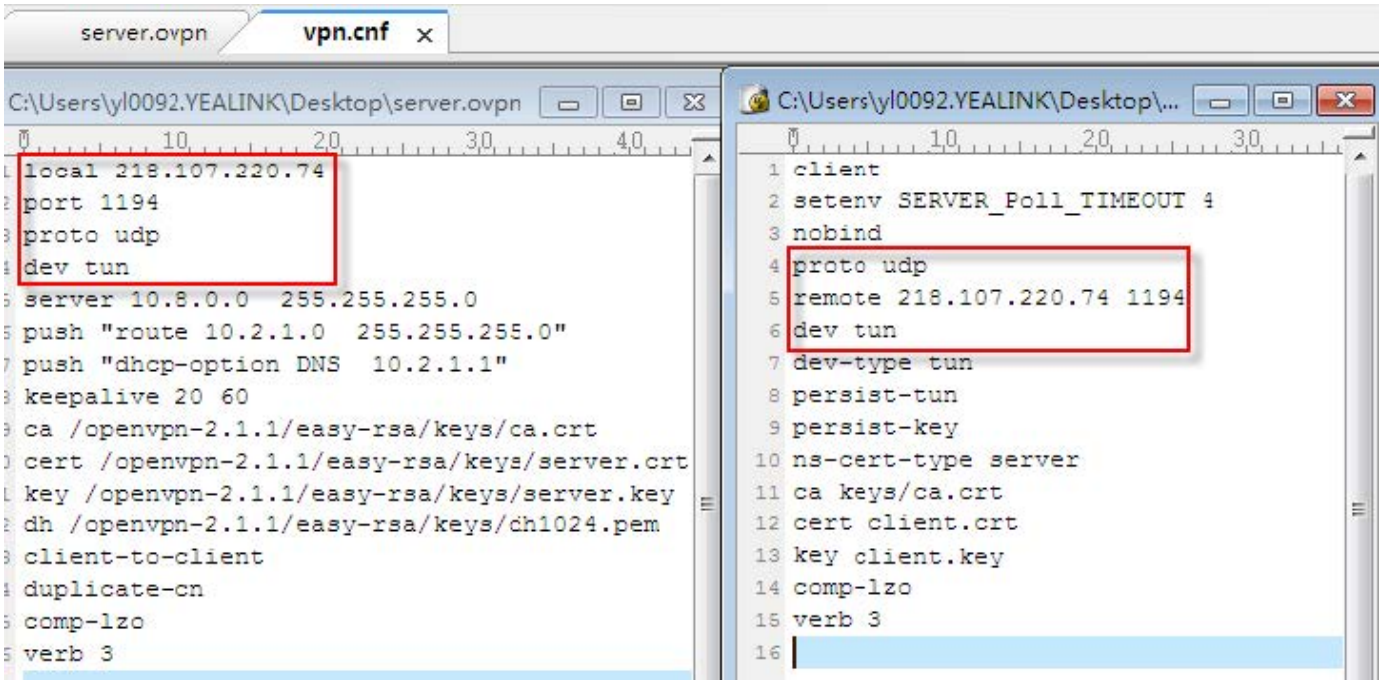
1. Ensure that the OpenVPN server is up and running.
   If the OpenVPN server is running properly, a virtual IP address assigned to the OpenVPN server will appear when you hover your mouse pointer over the VPN icon. The VPN icon in the notification area of the system tray is shown below:
   

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 "keys" and the client configuration file is named as "vpn.cnf", as shown below:
   

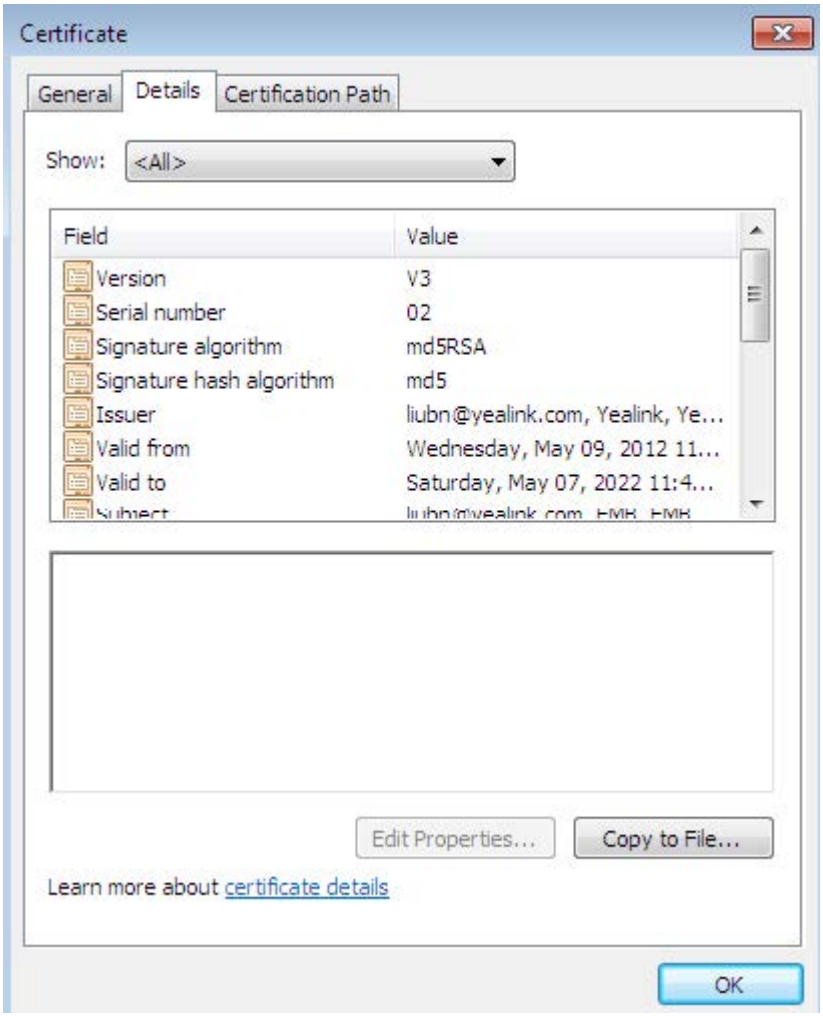
3. Ensure that the file names of the client certificates and key defined in the client configuration file are correct.
4. Enter the "keys" directory to check the file names of client certificates and key.



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



5. Ensure that the time and date on the phone 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 located in the easy-rsa folder 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 the access permission of the SIP server network segment has been assigned to the phone in the server configuration file.
   For example, if 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 192.168.3.10, the server configuration file must contain the configuration **push "dhcp option DNS 192.168.3.10"**.
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 configuration **client-to-client** has been added to the server configuration file.
2. Reboot the OpenVPN server.

Why is the voice quality poor?

Do the following:

1. Network congestion, RTP packet loss, or delay may result in poor call quality. In this case, you need to contact your network administrator.
2. Ensure that an appropriate log level is set in the client configuration file.
   Yealink recommends that you 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

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

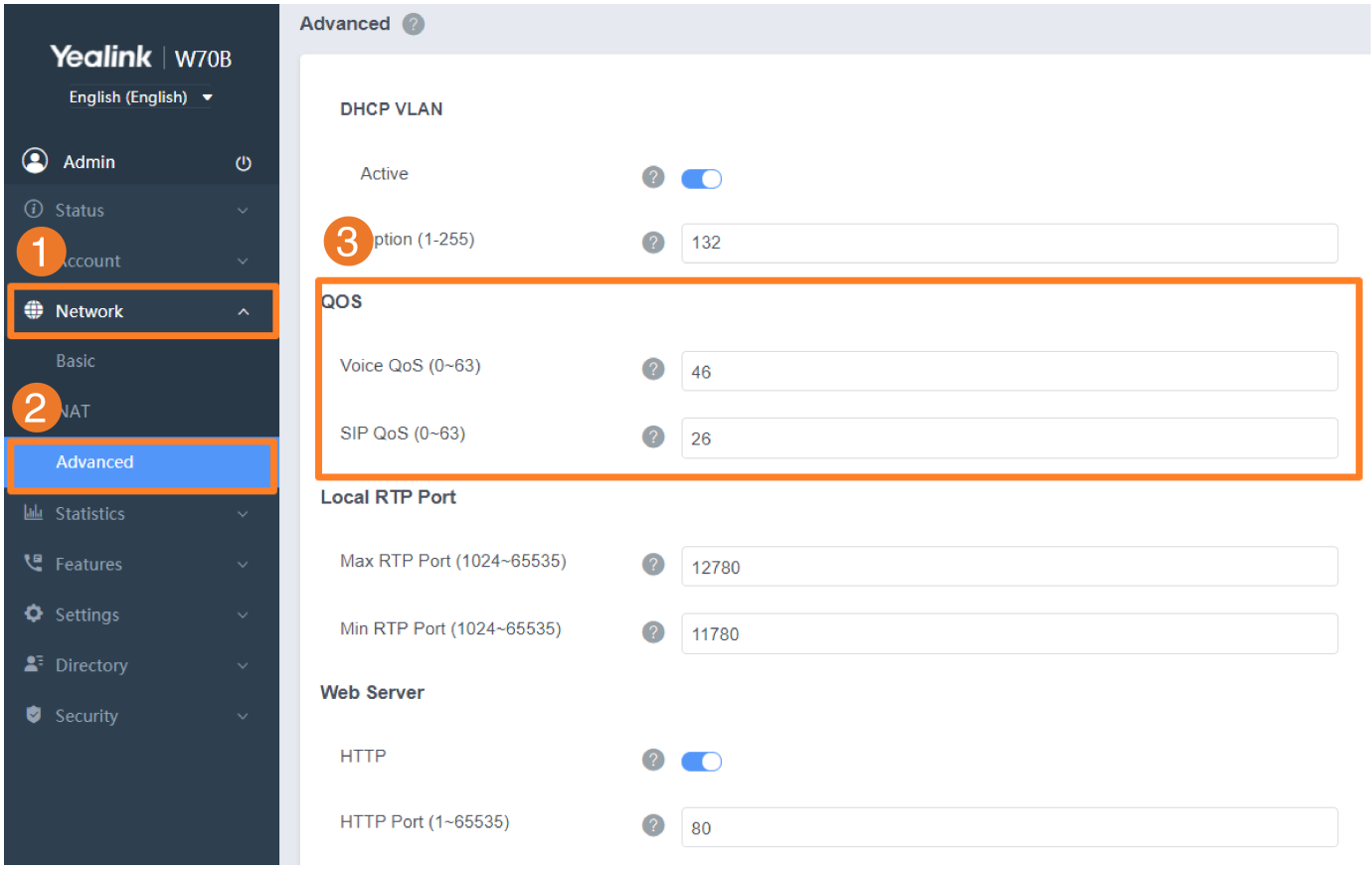
The SIP protocol is used for creating, modifying, and terminating two-party or multi-party sessions. To ensure good voice quality, SIP packets emanating from the phones should be configured with a high transmission priority. DSCPs for voice and SIP packets can be specified, respectively.

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

Voice and SIP QoS Configuration

Set via the Web User Interface

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



Configuration Parameter

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

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

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

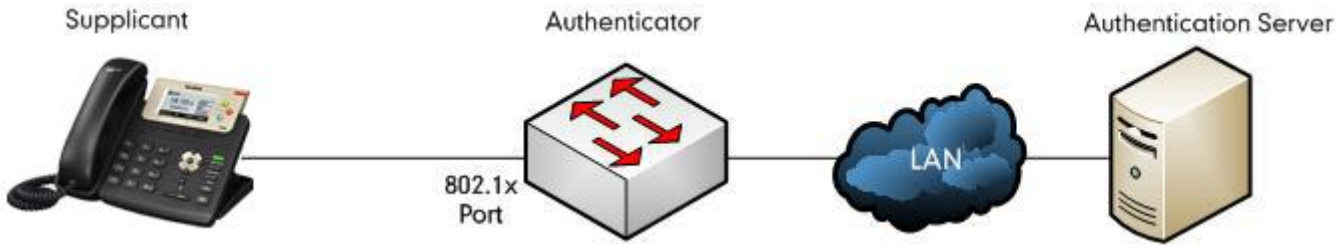
802.1x Authentication

About 802.1X

Introduction

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

802.1x Components



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

802.1X Authentication Configuration

The configuration can be done either using the webGUI or Auto Provisioning.

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
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-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-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 the **Authenticated Provisioning** mode is selected from the **Provisioning Mode** field. 6) Click **Upload** to upload the certificate.

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

A dialog box pops up to prompt that the 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	Default	Description
static.network.802_1x.mode[1]	**0**-EAP-None, no authentication **1**-EAP-MD5 **2**-EAP-TLS **3**-EAP-PEAP/MSCHAPv2	0	It configures the 802.1x authentication method.

	4-EAP-TTLS/EAP-MSCHAPv2 **5**-EAP-PEAP/GTC **6**-EAP-TTLS/EAP-GTC **7**-EAP-FAST		
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 512 characters	Blank	It configures the identity (user name) for 802.1x authentication.
static.network.802_1x.md5_password[1]	String within 512 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:

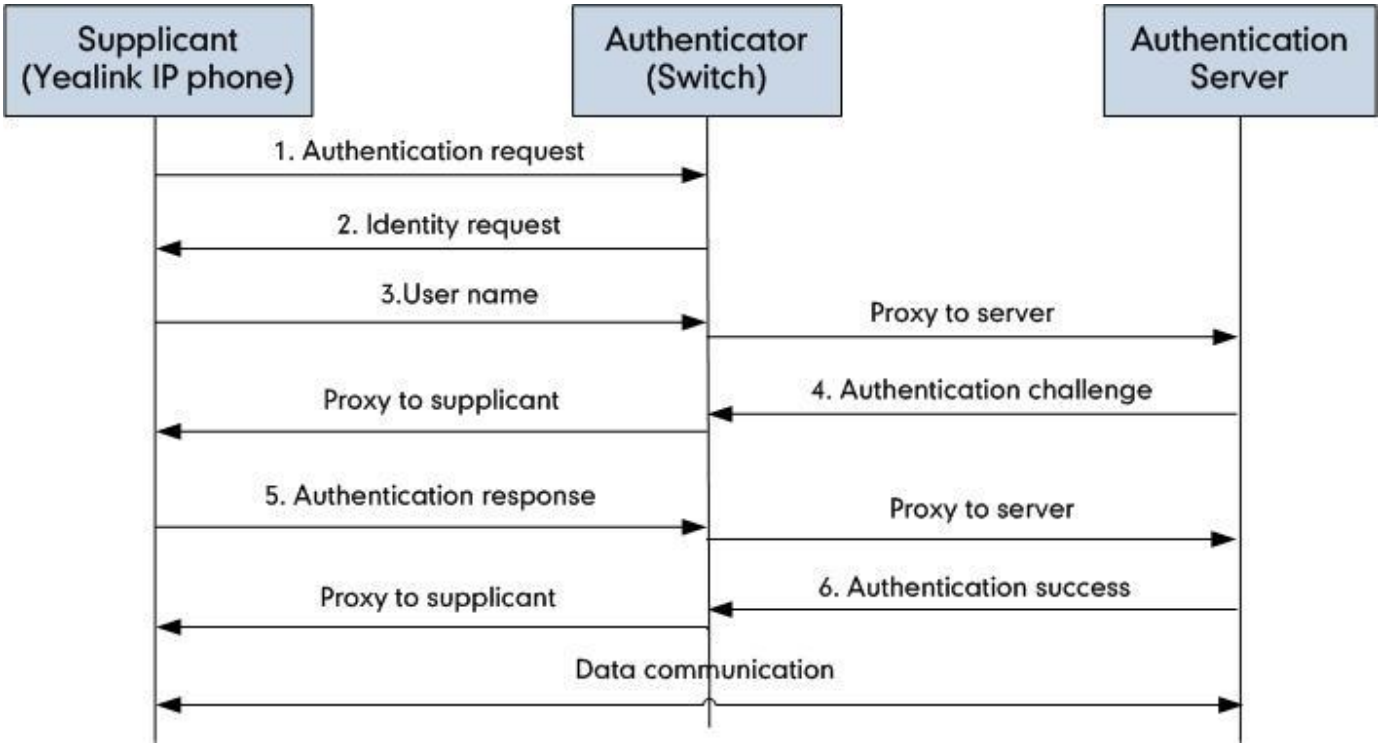
Pre-authentication

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

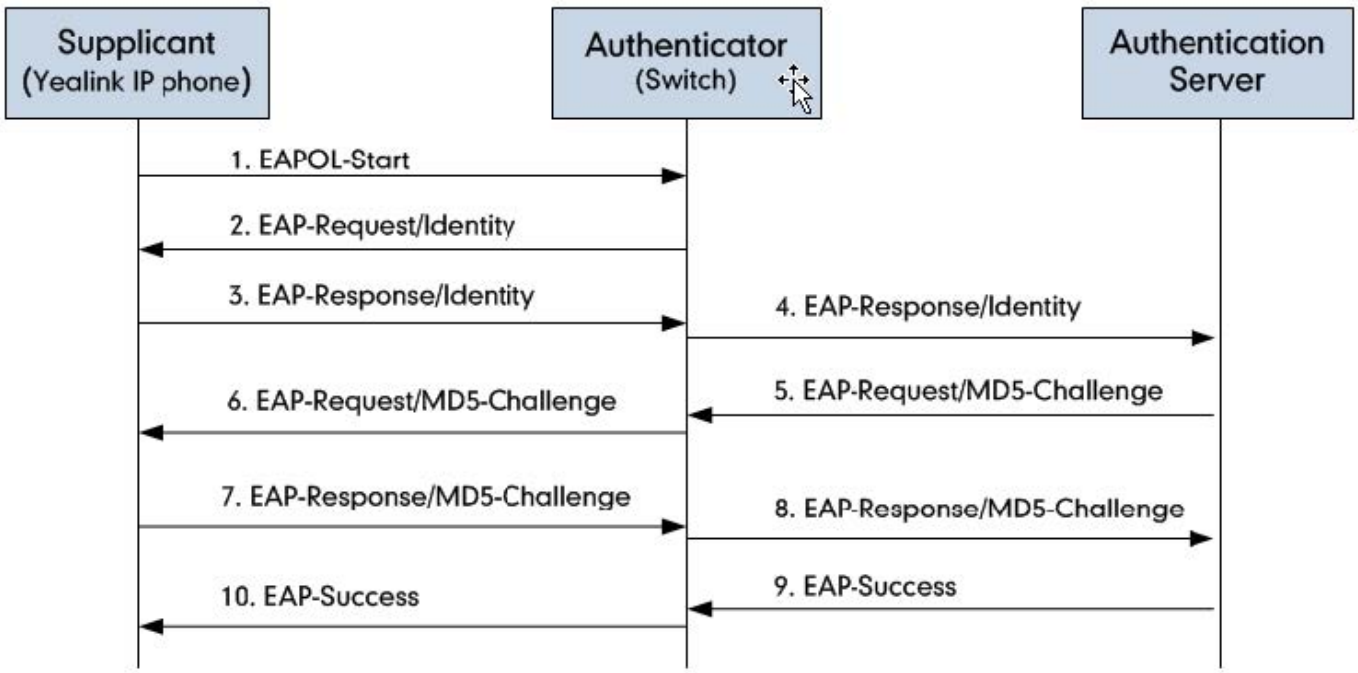
After the authentication server authenticates the IP phone, the authentication server initiates the authentication stage of the process. During this phase, the authenticator facilitates an exchange of keys between the IP phone and the authentication server. After these keys are established, the authenticator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

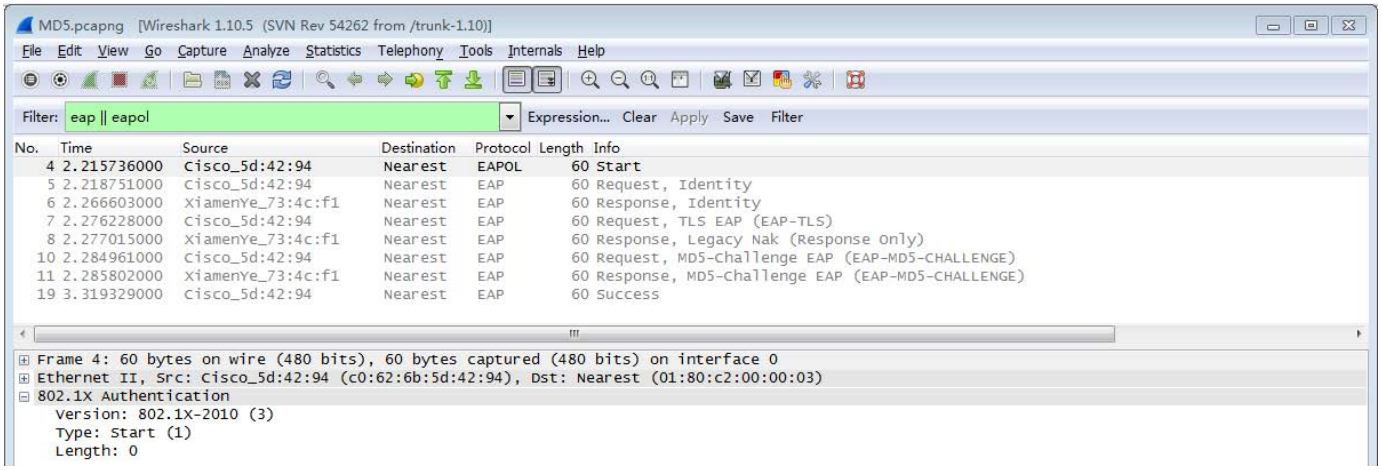
Authentication Process

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

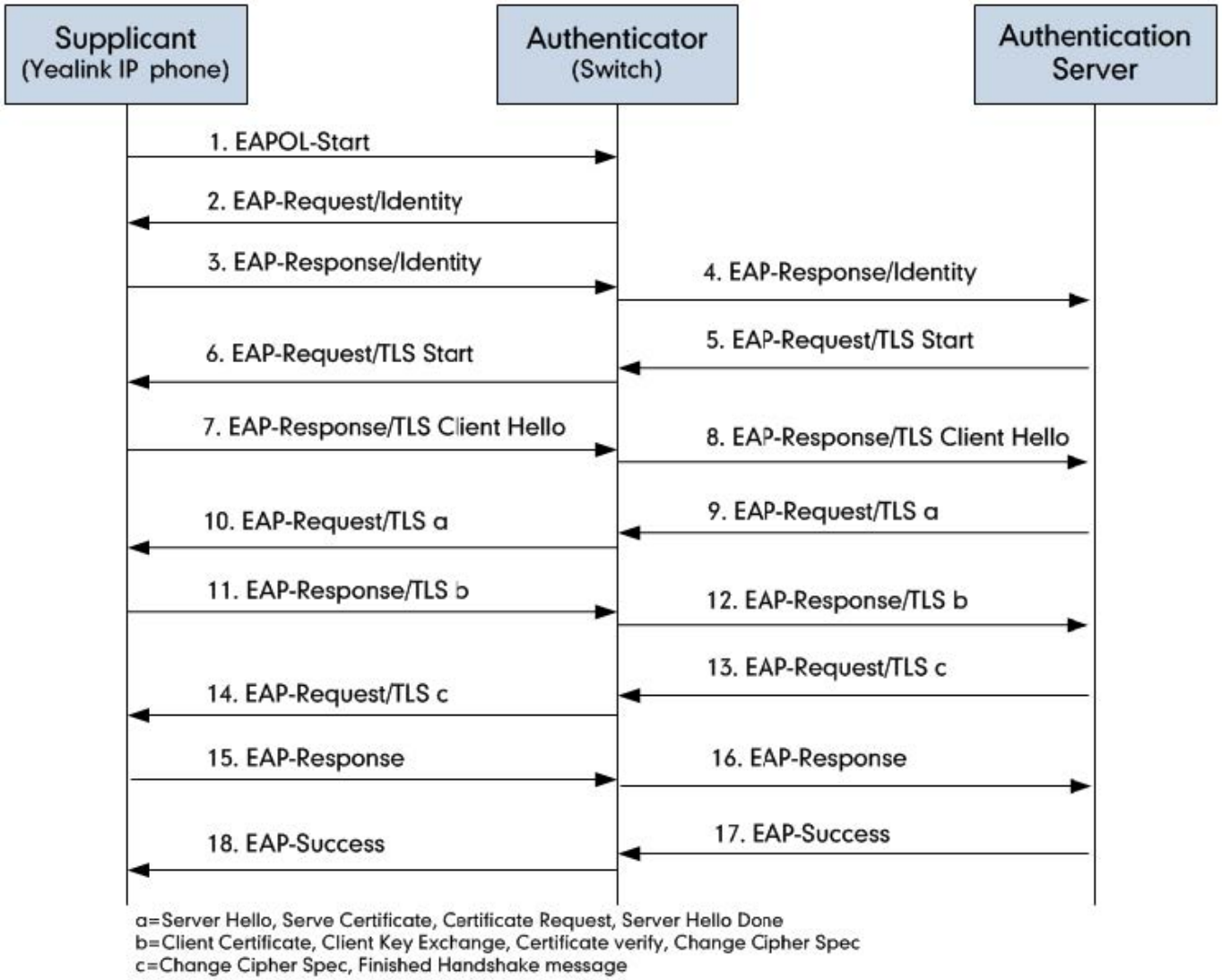
Sample Screenshot



Authentication Process Using EAP-TLS Protocol

Authentication Process

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

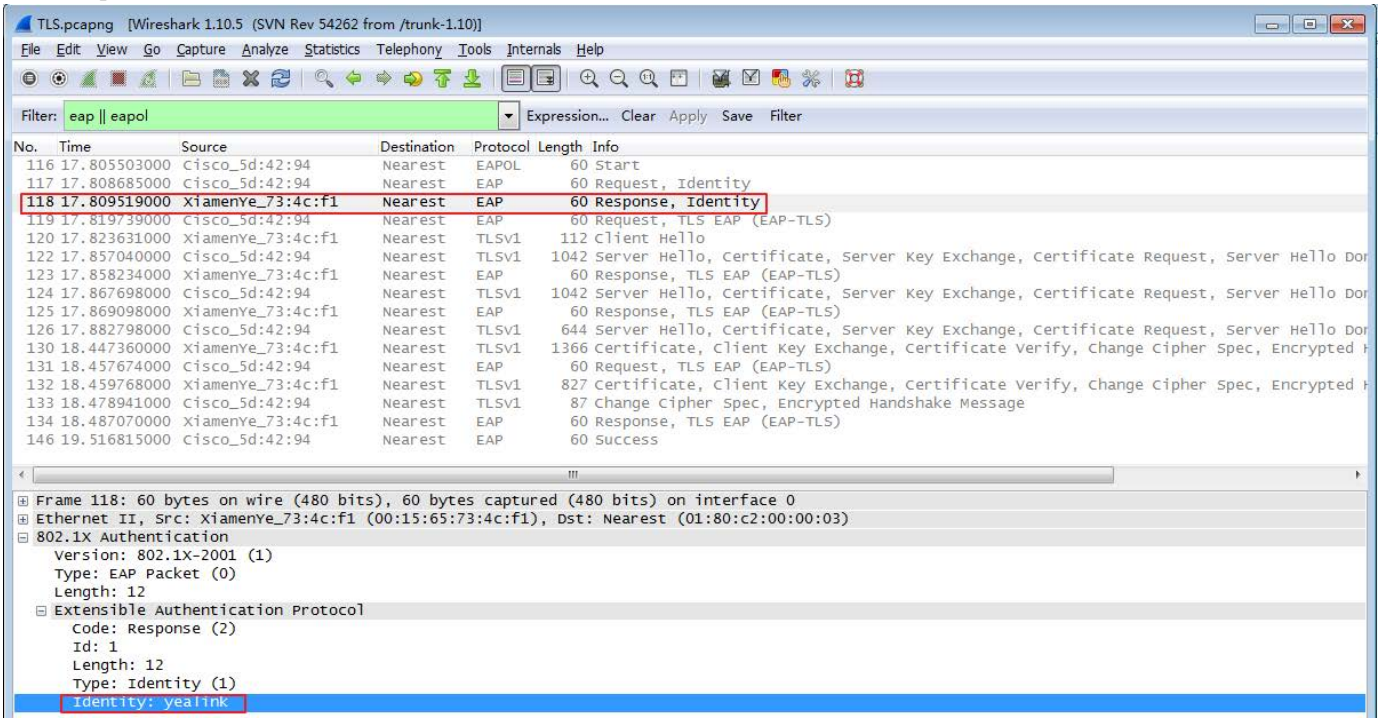


1. The supplicant sends an "EAPOL-Start" packet to the authenticator.

2. The authenticator responds with an "EAP-Request/Identity" packet to the supplicant.

3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
4. The authenticator strips the Ethernet header 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.

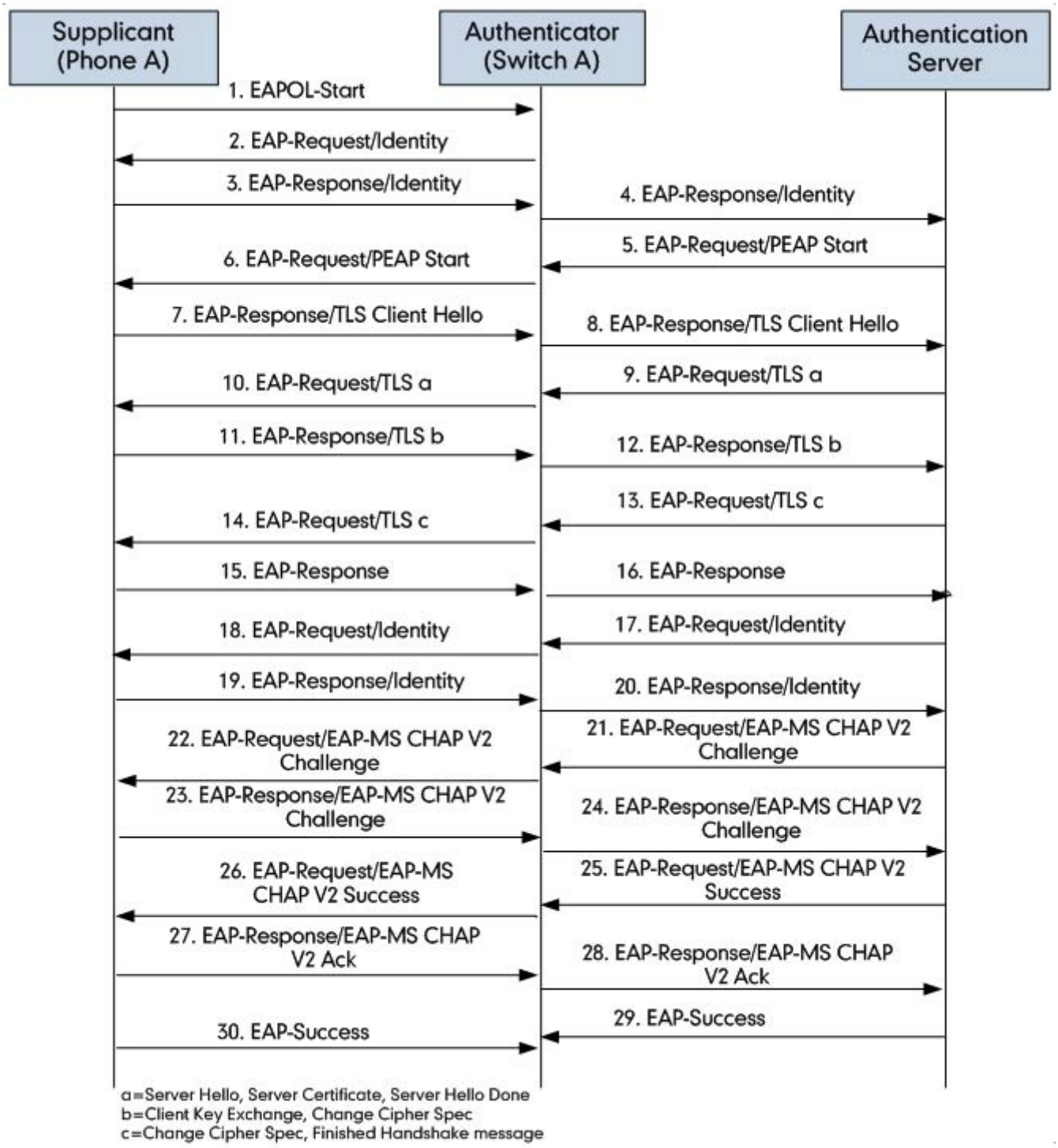
Sample Screenshot



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.



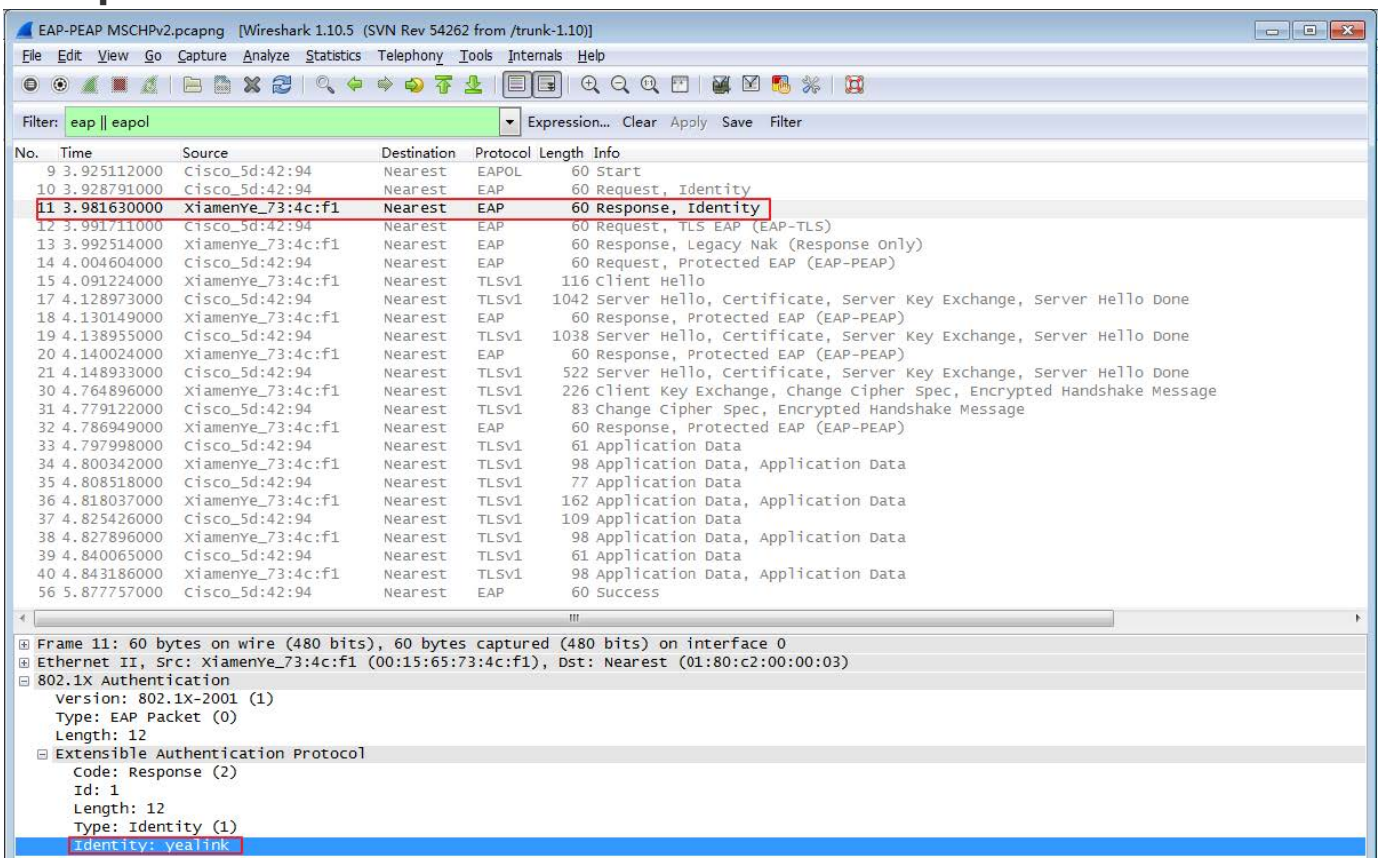
1. The supplicant sends an "EAPOL-Start" packet to the authenticator.
2. The authenticator responds with an "EAP-Request/Identity" packet to the supplicant.
3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
4. The authenticator strips the Ethernet header and encapsulates 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-Respon" 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 to the authenticator.
24. The authenticator passes the message to the authentication server.
25. The authentication server sends a success message indicating that the supplicant provides 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



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.

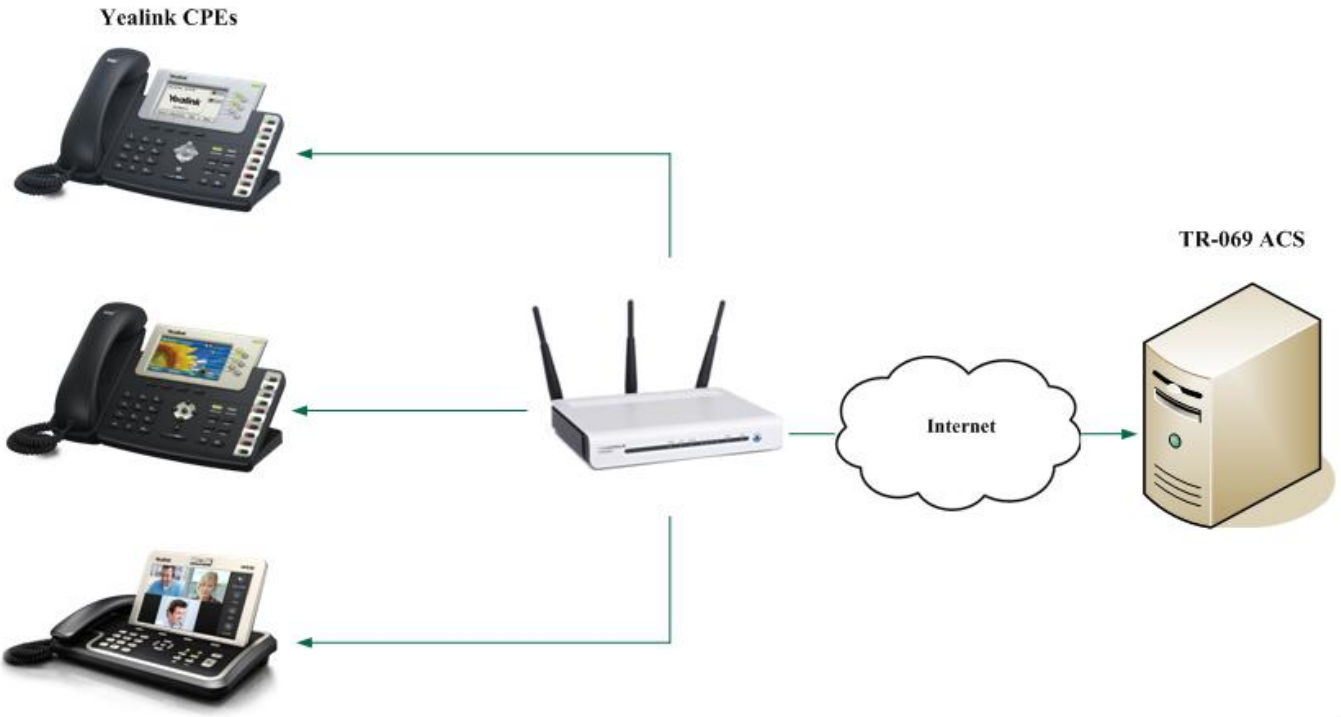
- a) Double-click the certificate to check the validity time.
- b) Check if the time and date on the phone are within the validity time of the uploaded certificate. If not, regenerate a certificate and upload it to the phone.

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 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 restrictions. 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.

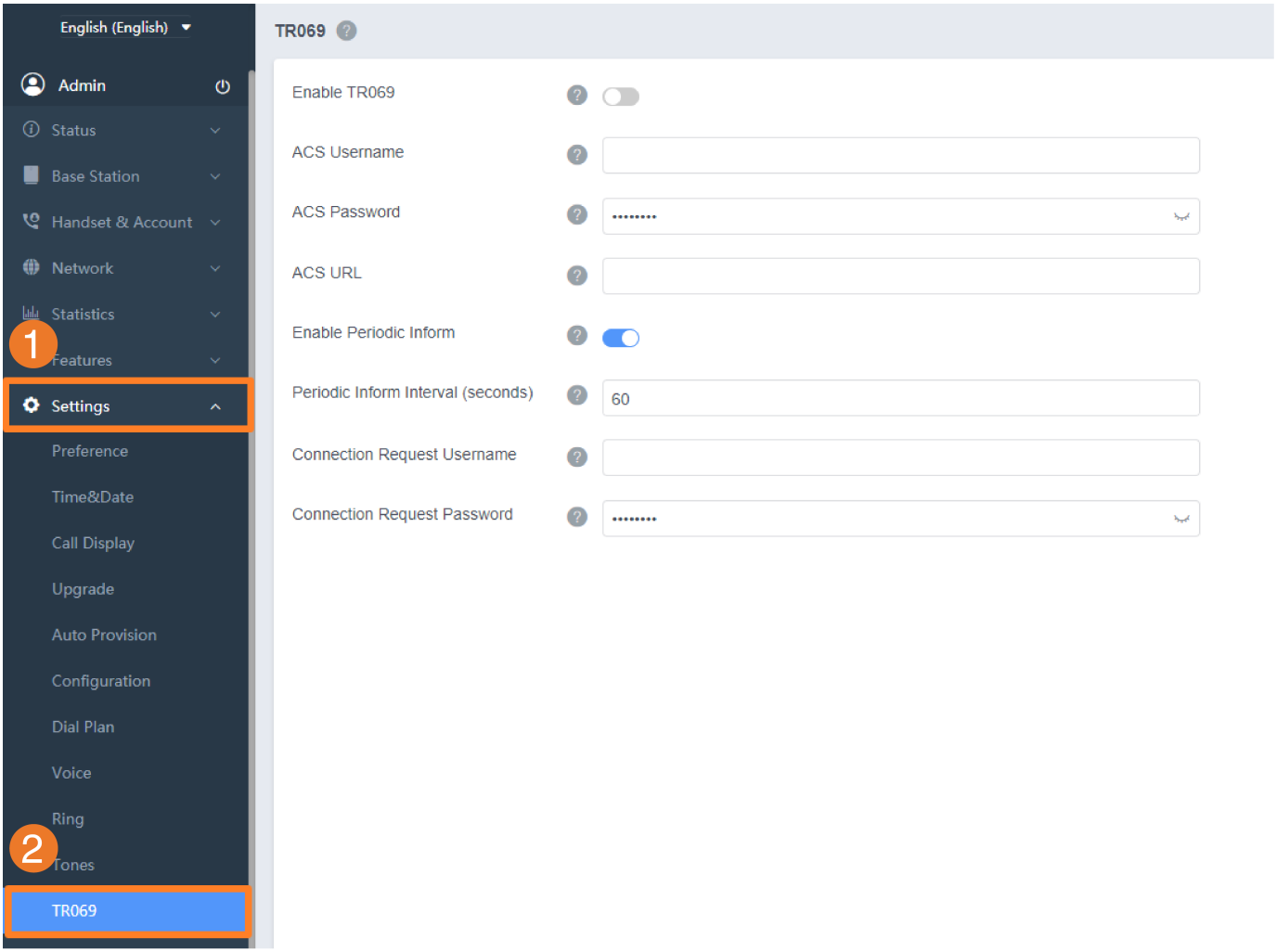
Diagnostics

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 Cconfiguration

Set via the Web User Interface

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



Parameter	Description
Enable TR069	It enables or disables the TR-069 feature.
ACS Username	It configures the TR-069 ACS server user name used to authenticate the phone. Leave it blank if no authentication is required.
ACS Password	It configures the TR-069 ACS server password used to authenticate the phone. Leave it blank if no authentication is required.
ACS URL	It configures the access URL of the TR-069 ACS server.
Enable Periodic Inform	It enables or disables the phone to periodically report its configuration information to the ACS server.
Periodic Inform Interval (seconds)	It configures the interval (in seconds) at which the phone reports its configuration to the ACS server. The default value is **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, which are connected via a LAN through an Internet gateway. The two mechanisms are briefly summarized as follows:

- **Device-Gateway Association**: Allows an ACS to manage a device to identify the associated gateway to which that device is connected.
- **Connection Request via NAT Gateway**: Allows an ACS to initiate a TR-069 Session with a device that is operating behind a NAT gateway.

ACS Specific Information

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

Data Model

Most of the configuration and diagnostics are performed through setting and retrieving the value of the phone parameters. They are organized in a well-defined hierarchical structure that is more or less common to all phone models. For more information about the common and customized phone parameters, refer to the phone-specific document *Yealink_TR-069_DataModel_V4.0.xlsx*.

Contact the Yealink technical support for the data model file. Each of the parameters is marked as writable or non-writable. The phone does not permit the change of any parameter marked as read-only. Values applicable for the parameter, their type, and meaning are also precisely defined in the document.

Normative References

TR-069: http://www.broadband-forum.org/technical/download/TR-069_Amendment-3.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

Proxy Server

Introduction

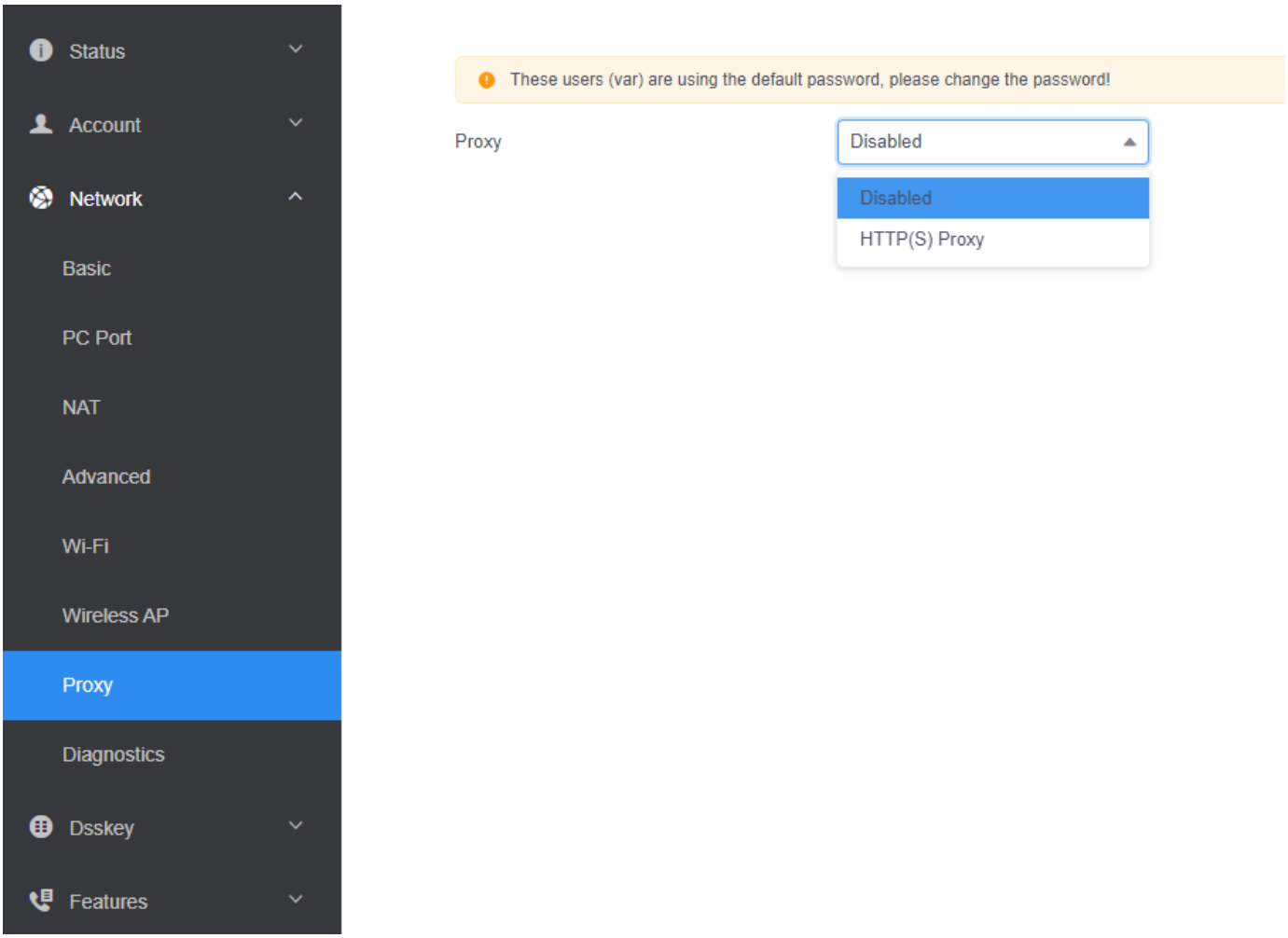
In an environment with high network security requirements, devices cannot directly connect to the public network and must be redirected through a proxy server to complete network access.

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 protocols,

	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**.

Configuration Parameter

```
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	Permitted Value	Default	Description
network.proxy.mode	**0**-Disabled **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.	0	It enables or disables the proxy server.
network.proxy.wpad	**0**-Disabled **1**-Enabled	1	It enables or disables the WPAD to obtain PAC files dynamically.
network.proxy.http.set_from	**0**-IP: Port, enter the IP address and port manually. **1**-PAC URL, enter the PAC URL manually. **2**-PAC File, upload PAC file directly.	0	It configures proxy mode.
network.proxy.hostname	String within 99 characters.	/	It configures the domain name or the IP address of the proxy server.
network.proxy.port	Integer from 1 to 65535	/	It configures the port of the proxy server.
network.proxy.bypass_address	URL within 511 characters. Multiple host names or IP addresses are separated by commas.	/	It configures the host name or IP address that does not apply to the proxy server to access.
network.proxy_pac.url	URL String within 511 characters.	/	It configures the URL where the PAC file is placed, and the device obtains the PAC file through autop.

network.proxy.address	IP address or URL.	/	It configures a proxy address.
network.proxy_pac.delete	Fixed: http://local_host/all	/	Delete the PAC file in the phone.
network.proxy_pac.manual_url	String within 512 characters	/	Manually configure the PAC URL.

Number of Simultaneous Outgoing Calls

Introduction

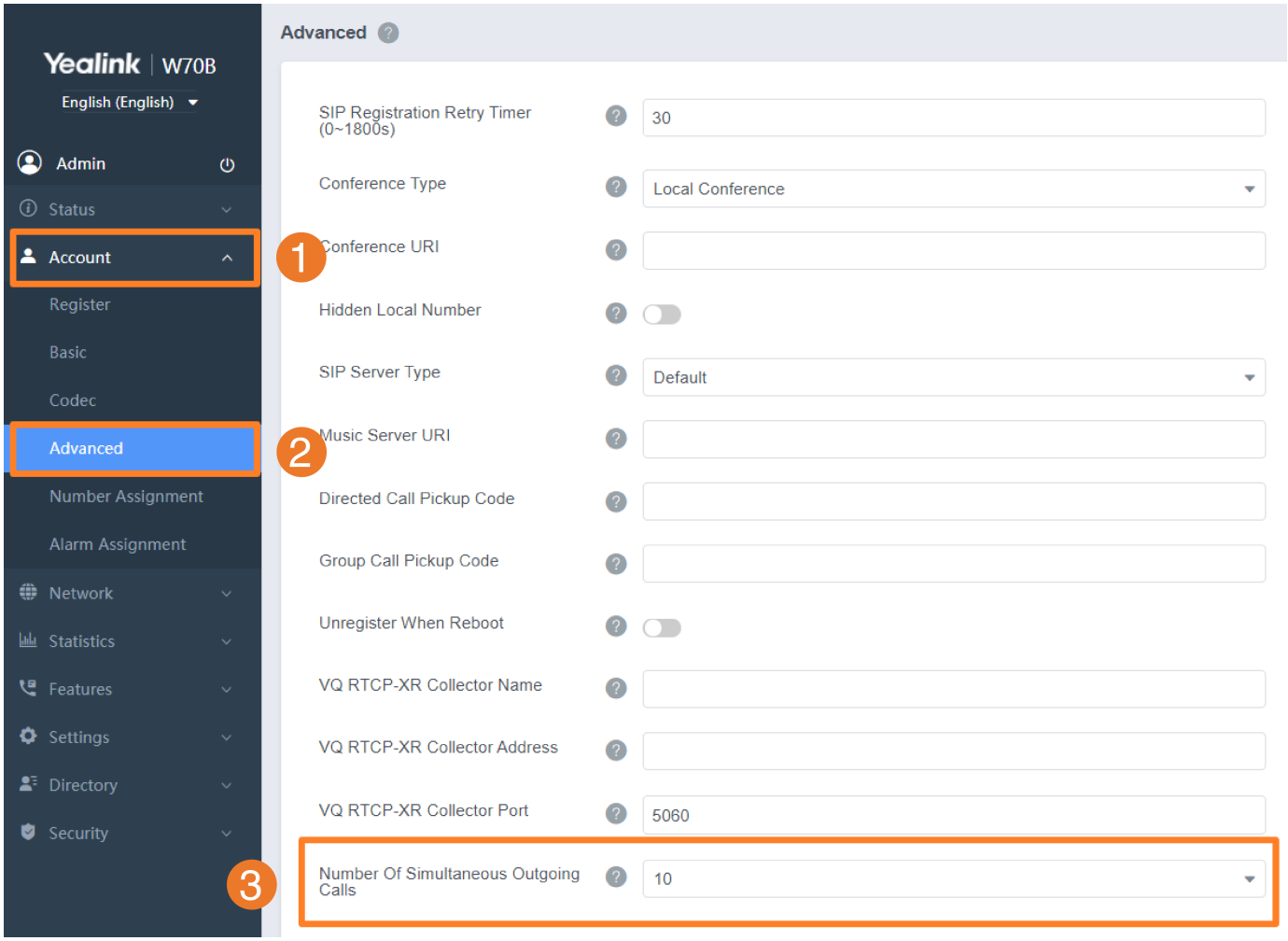
The number of simultaneous outgoing calls allows you to configure the maximum number of simultaneous outgoing calls for a specific account on a base.

The number of active handsets affects this feature.

Number of Simultaneous Outgoing Calls Configuration

Set via the Web User Interface

1. On the web user interface, go to **Account** > **Advanced** > **Number Of Simultaneous Outgoing Calls**.



Auto Provisioning

account.X.simultaneous_outgoing.num

Parameter	Permitted Values	Default	Description
account.X.simultaneous_outgoing.num[1]	Integer from 1 to 10	10	It configures the maximum number of simultaneous outgoing calls for a specific account on a base station. You should set the value of this parameter lower than or equal to "base.active_handset.number".

[1]X is the account ID. X=1-10.

Number of Active Handsets

Introduction

The W70B base station supports up to 10 handsets, and you can limit the maximum number of active handsets. The active handsets are free to communicate, access menu, configure features, and so on. Operation is restricted on the inactive handsets, and the idle screen of the handset prompts "Path Busy".

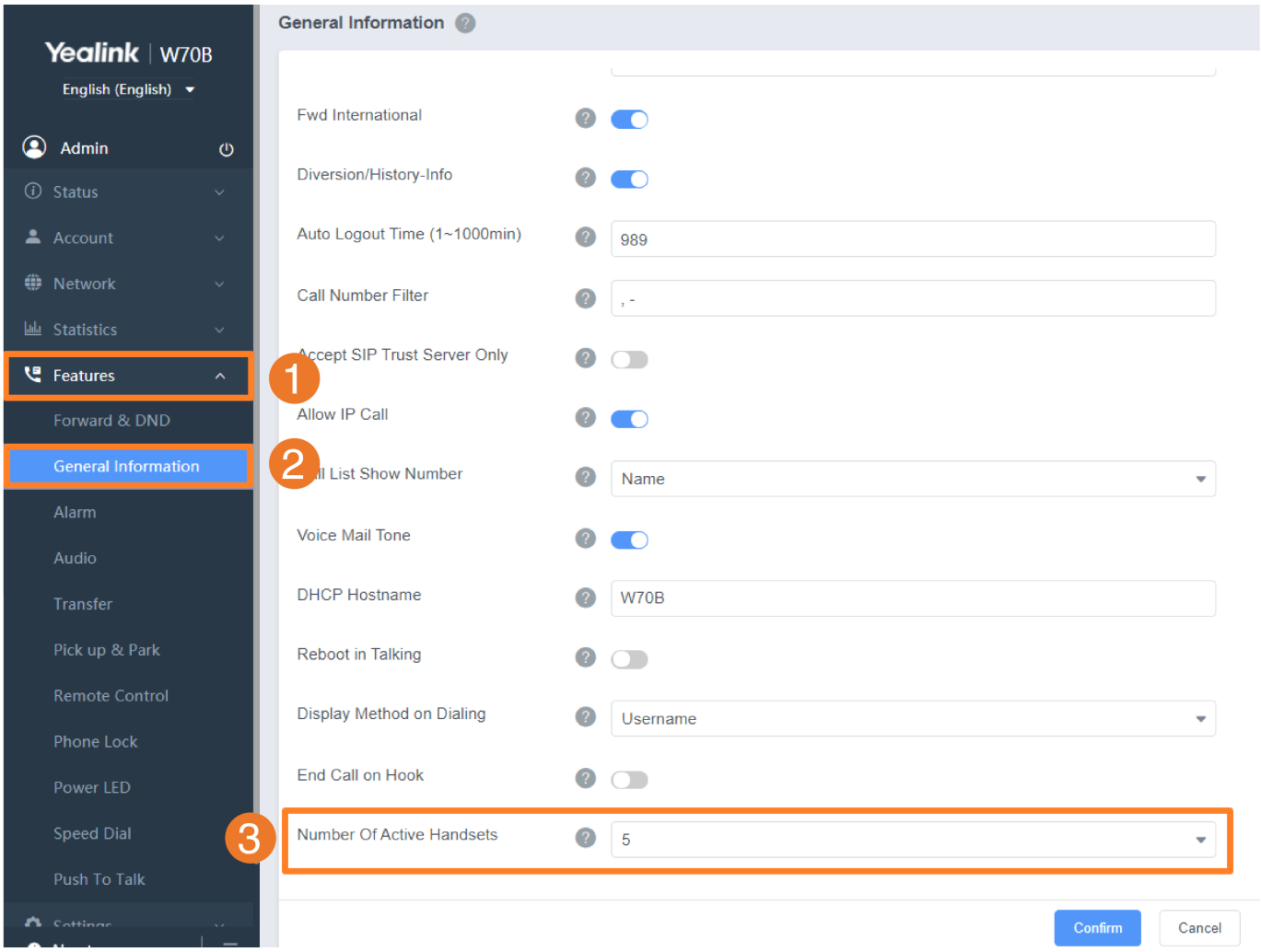
The number of active handsets will also affect the number of simultaneous active calls on the base station.

Call Supported	Number of Active Handsets	Maximum Number of Simultaneous Active Calls	Maximum Number of Simultaneous Calls
Wide-band Calls	5	10	20 (for other codecs)
Narrow-band Calls	10	20 (for other codecs)	20 (for other codecs)

Number of Active Handsets Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Number Of Active Handsets**.



Auto Provisioning

base.active_handset.number

Parameter	Permitted Values	Default	Description
base.active_handset.number[1]	5, 10	5	It configures the maximum number of active handsets.

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

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 connections.

Supported Accounts

The number of registered accounts must meet the following:

1. W70B

Assigned Account(s)		Registered Accounts on W70B
W71P/W73P/W74P/W76P/W77P/W78P/W79P/W79P Pro/W53H/DDPhone/CP935W Base	CP930W Base	
10	1	10

2. W75 Mini Multi-Cell System

Registered Accounts on W75DM	Assigned Account per Handset
20	Only one

3. W80 Multi-Cell System

Registered Accounts on W80DM	Assigned Account per Handset
100	Only one

4. W90 Multi-Cell System

Registered Accounts in W90 Multi-Cell System	Registered Accounts in VIM System	Assigned Account per Handset
250	2500	Only one

SIP Server Template Configuration

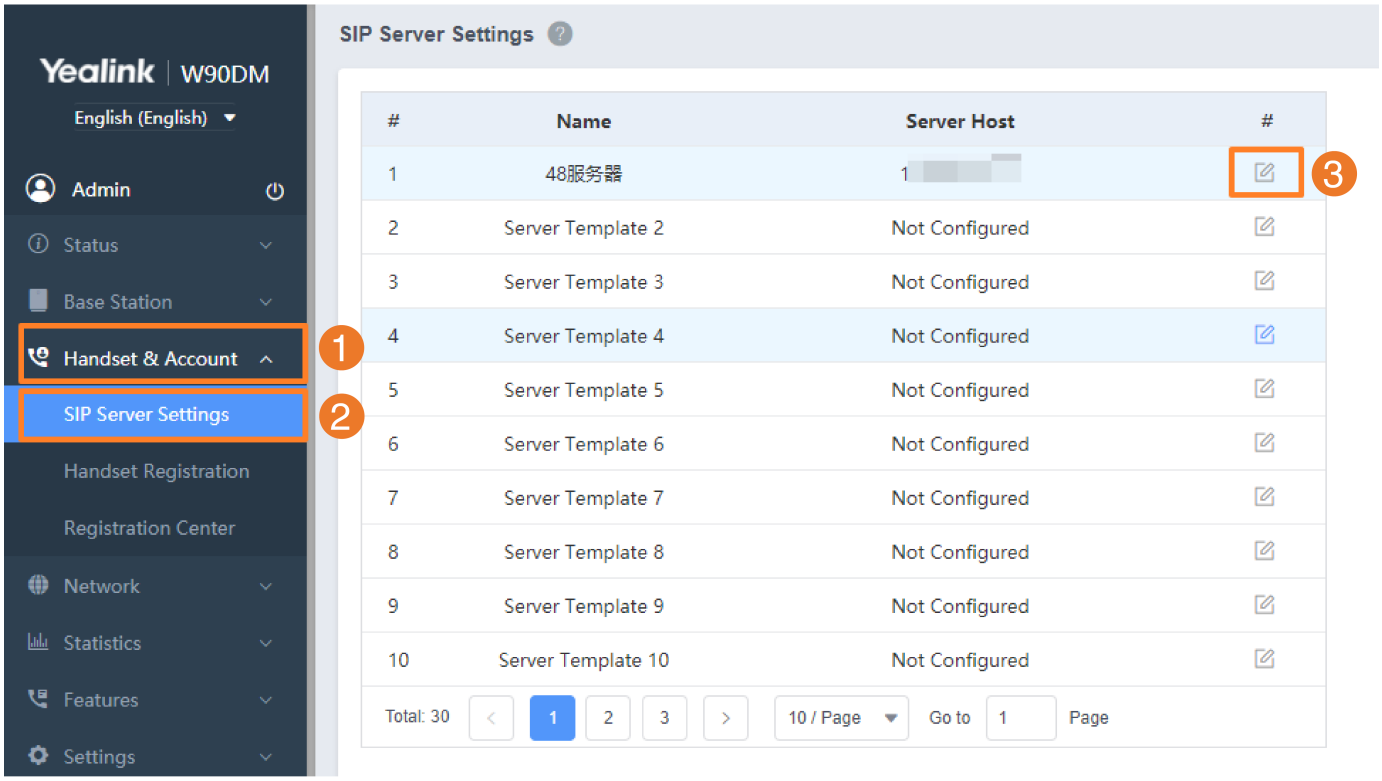
Description

You can use up to ten different SIP servers in the system. You can pre-configure up to 10 SIP server templates for choosing when registering SIP accounts.

Configuration

Set via the Web User Interface

1. On the web user interface, go to **Handset & Account** > **SIP Server Settings** > **Edit**.



Parameter	Description
Template Name	It sets the name of the SIP server template.
Server Host	It configures the IP address or domain name of the SIP server in which the account is registered.
Port	It configures the port of the SIP server in which the account is registered.
Transport	It configures the type of transport protocol.
Server Expires	It configures the registration expiration time (in seconds) of SIP server x.
Server Retry Counts	It configures the retry times for the device to resend requests when the SIP server x is unavailable or there is no response from the SIP server x. The handset moves to the next available server after three failed attempts.
Enable Outbound Proxy Server	It enables or disables the device from sending requests to the outbound proxy server.

Outbound Proxy Server 1	It configures the IP address or domain name and the port of the outbound proxy server x. It works only if "template.X.outbound.enable" is set to 1 (Enabled).
Outbound Proxy Server 2	It configures the IP address or domain name and the port of the outbound proxy server x. It works only if "template.X.outbound.enable" is set to 1 (Enabled).
Proxy Fallback Interval	It configures the time interval (in seconds) for the device to detect whether the working outbound proxy server is available by sending the registration request after the fallback server takes over call control.

Configuration Parameter

```
template.X.name
template.X.sip_server.Y.address
template.X.sip_server.Y.port
template.X.sip_server.Y.transport_type
template.X.sip_server.Y.expires
template.X.sip_server.Y.retry_counts
template.X.nat.traversal
template.X.outbound.enable
template.X.outbound.Y.address
template.X.outbound.Y.port
template.X.outbound.fallback_interval
```

Parameter	Permitted Values	Default	Description
template.X.name[1]	String within 64 characters	Blank	It sets the name of the SIP server template.
template.X.sip_server.Y.addres	String within 64 characters	Blank	It configures the IP address or domain name of the SIP server Y in which the account is registered.

s[1] [2]			
template.X.sip_server.Y.port[1] [2]	Integer from 0 to 65535	5060	It configures the port of the SIP server Y.
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 device performs the DNS NAPTR and SRV queries for the service type and port.	0	It configures the type of transport protocol.
template.X.sip_server.Y.expires[1] [2]	Integer from 30 to 2147483647	3600	It configures the registration expiration time (in seconds) of SIP server Y.
template.X.sip_server.Y.retry_counts[1] [2]	Integer from 0 to 20	3	It configures the retry times for the device to resend requests when the SIP server Y is unavailable or there is no response from the SIP server Y. The handset moves to the next available server after three failed attempts.
template.X.nat.traversal[1] [2]	Integer from 0 to 20	3	It configures the retry times for the device to resend requests when the SIP server Y is unavailable or there is no response from the SIP server Y.
template.X.outbound.enable[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the device to send requests to the outbound proxy server.
templat	String within 64 characters	Bl	It configures the IP address or domain name of

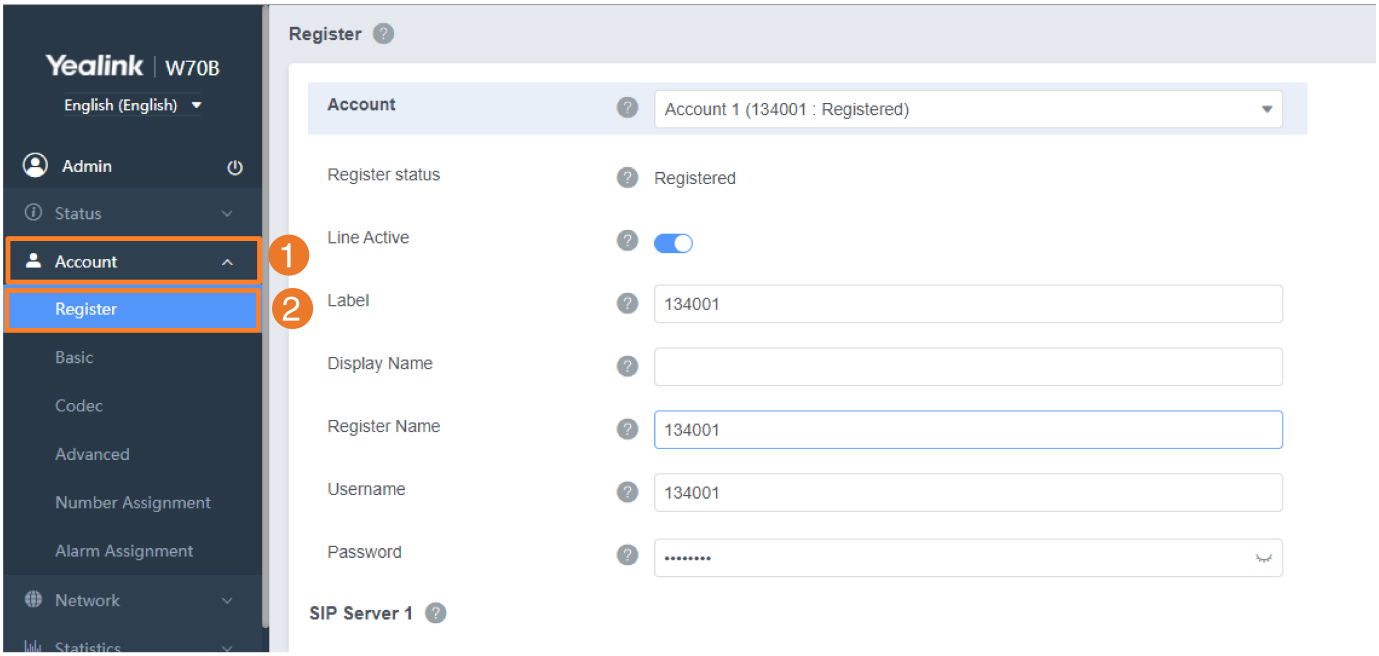
e.X.outbound.Y.address[1] [2]		ank	the outbound proxy server Y. It works only if "template.X.outbound.enable" is set to 1 (Enabled).
template.X.outbound.Y.port[1] [2]	Integer from 0 to 65535	5060	It configures the port of the outbound proxy server Y. It works only if "template.X.outbound.enable" is set to 1 (Enabled).
template.X.outbound.fallback_interval[1]	Integer from 30 to 2147483647	3600	It configures the time interval (in seconds) for the device to detect whether the working outbound proxy server is available by sending the registration request after the fallback server takes over call control.

[1]X is the template ID. X=1-30.
[2]Y is the server ID. Y=1-2.

Accounts Registration Configuration

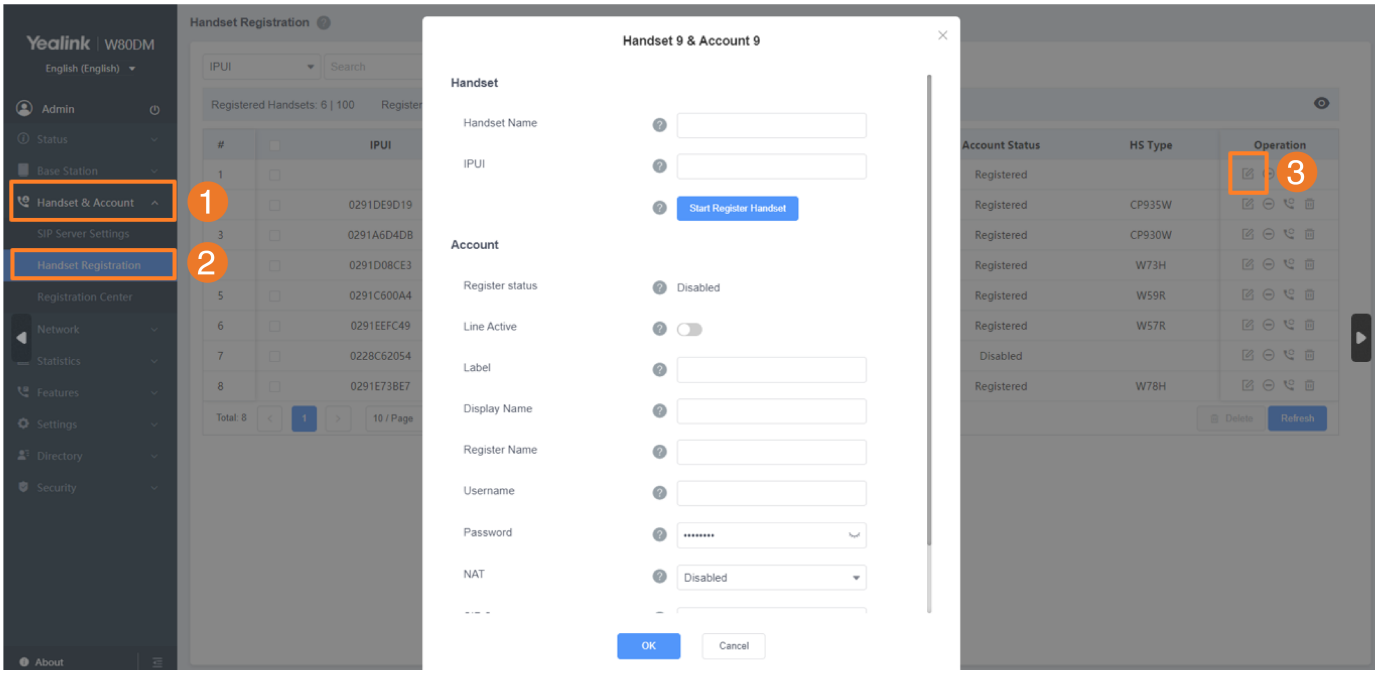
Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Register**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** >

Handset Registration > **Add Handset/Edit**.



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.template
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.template[1]	Integer from 1 to 10	1	It configures which SIP server template 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 equal to 0	60	It configures the maximum time to wait (in seconds) for the phone to retry to re-register after the account registration fails. 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.

[1]X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

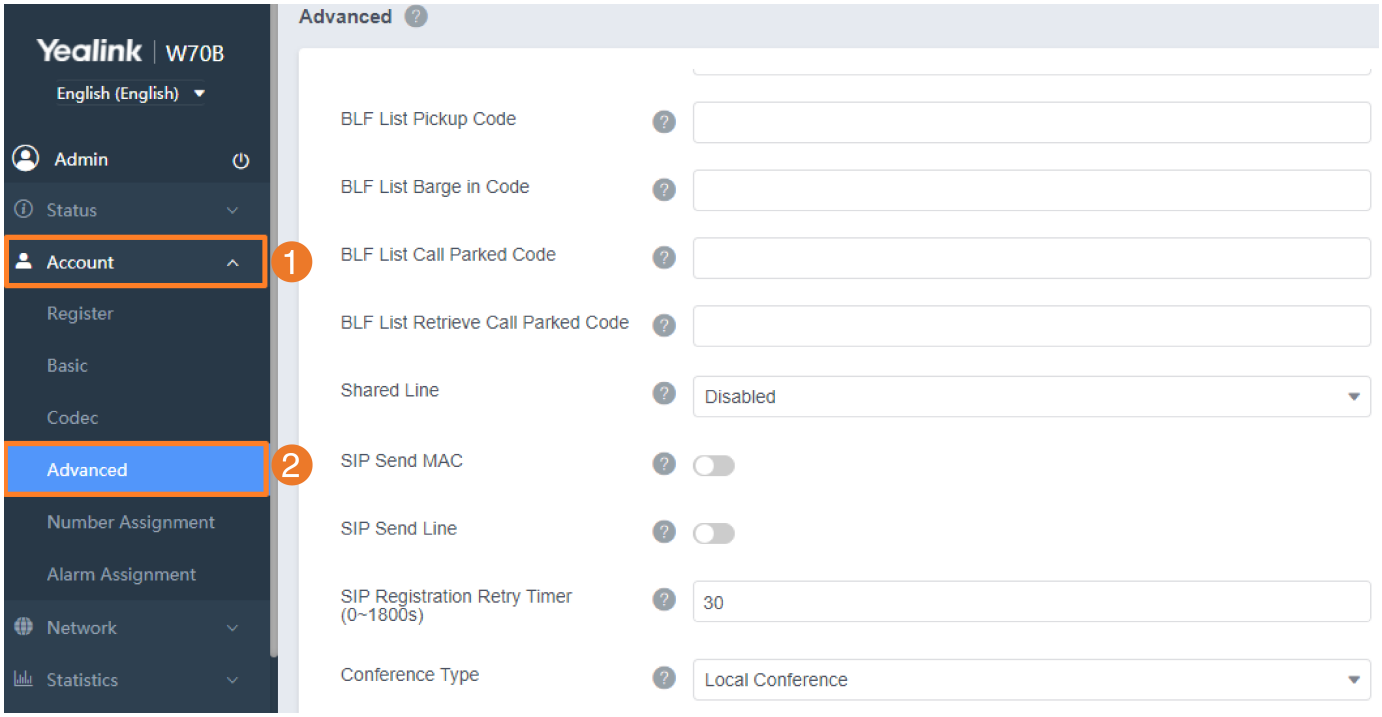
[2]Y is the server ID. Y=1-2.

Registration Settings Configuration

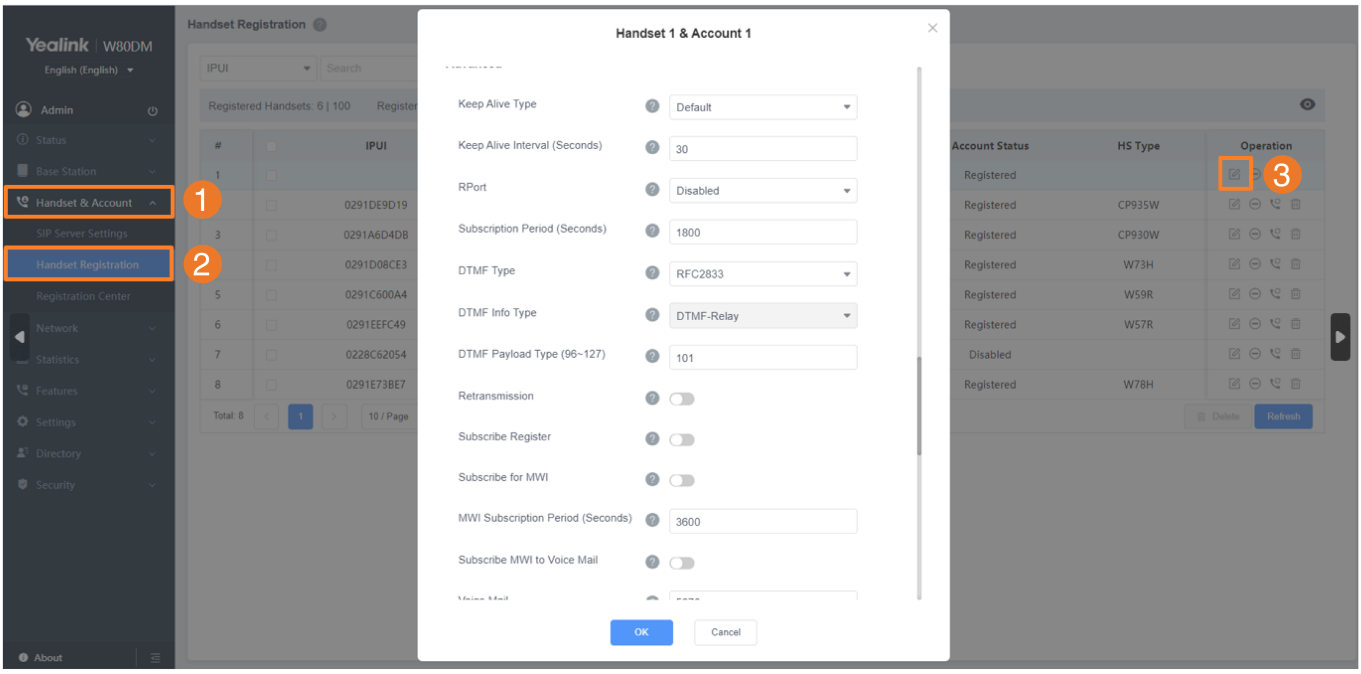
The following table lists the parameters you can use to change the registration settings.

Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Advanced**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit**.



Configuration Parameter

```
account.X.enable_user_equal_phone
account.X.register_mac
account.X.register_line
account.X.unregister_on_reboot
account.X.sip_server_type
```

sip.reg_surge_prevention
account.X.subscribe_register
phone_setting.disable_account_without_username.enable
account.X.register_expires_overlap
account.X.subscribe_expires_overlap

Parameter	Permitted Values	Default	Description
account.X.enable_user_equal_phone[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to add "user=phone" to the SIP header of the INVITE message.
account.X.register_mac[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to add 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.
> - For W70B, X=1-10.
> - For W75DM, X=1-20.
> - For W80 multi-cell system, X=1-100.
> - For W90 multi-cell system, X=1-250.
> - For VIM system, X=1-2500.
>
> [2]If you change this parameter, the phone will reboot to make the change take effect.

Account Registration File Customization

You can ask the distributor or Yealink FAE for the account registration template (Account_configuration.csv).

Before You Begin

This feature is only applicable to the W75/W80/W90 Multi-Cell System.

Account Registration File Elements

The following table lists the elements and attributes you can use to assign accounts for handsets in the account registration file. We recommend that you do not edit these attributes.

Attributes	Description
account	Specify the account ID (1-100). This is required. If not filled, the line will not take effect.
ipui	Specify the IPUI of the handset to which you want to assign the account.
reg.enable	Enable or disable the registration status for the handset.
auth_name	Specify the register name of the account.

user_name	Specify the user name of the account.
password	Specify the password of the account.
display_name	Specify the display name of the account.
label	Specify the label of the account.
enable	Specify the activation status of the account.
sip_server.template	Specify the SIP server template.

Customize Account Registration File

1. Open the account registration file.
2. Specify the account information.
3. For example:

	A	B	C	D	E	F	G	H	I	J
1	account	ipui	reg.enable	auth_name	user_name	password	display_name	label	enable	sip_server.template
2	1	0291c075dd	1	21111	1111		1111	1111	1	1
3	2	0291c075c8	1	222223245	222223245		222223245	222223245	1	1
4	3	0291B11D58	1	1323133245	1323133245		1323133245	1323133245	1	1

3. Save the changes.

Account Registration File Upload

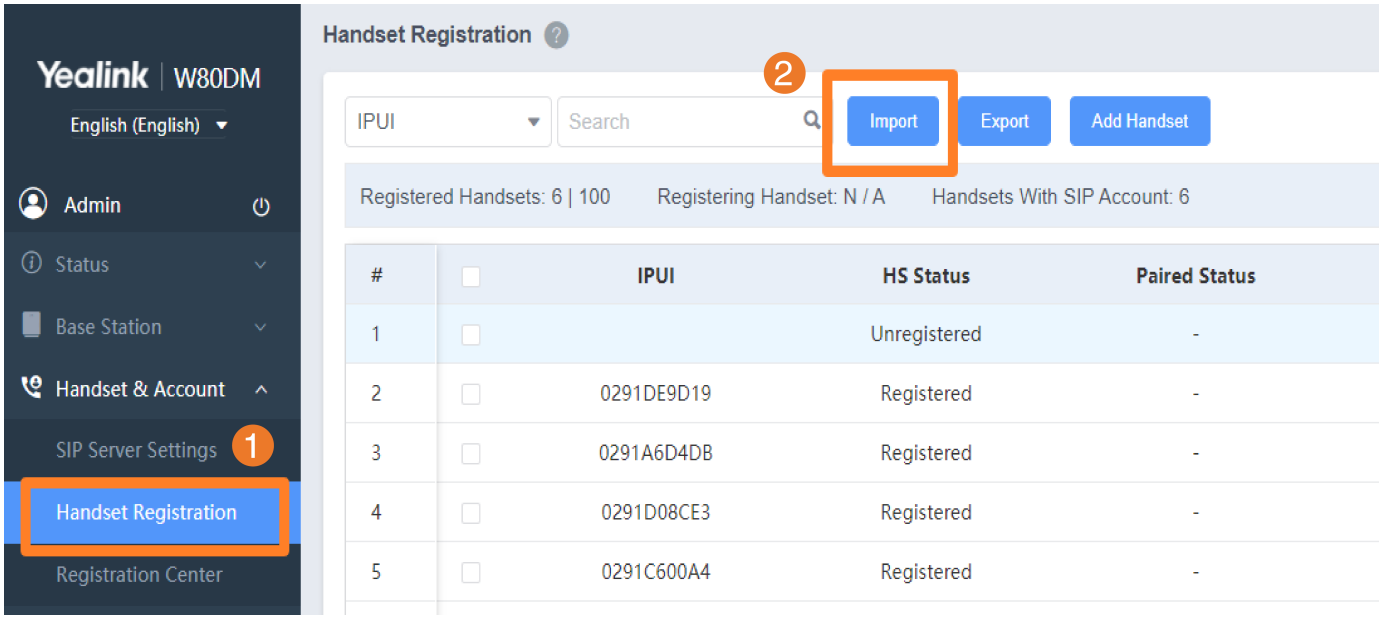
You can upload an account registration file to register accounts in batches and associate the account with the handset IPUI.

Before You Begin

This feature is only applicable to the W75/W80/W90 Multi-Cell System.

Set via the Web User Interface

1. On the web user interface, go to **Handset & Account** > **Handset Registration** > **Import**.



Configuration Parameter

ipui_account.data.url

Parameter	Permitted Values	Default	Description
ipui_account.data.url	String within 512 characters	Blank	It configures the access URL of the custom account registration file (*.csv).

Outbound Proxy in Dialog

Introduction

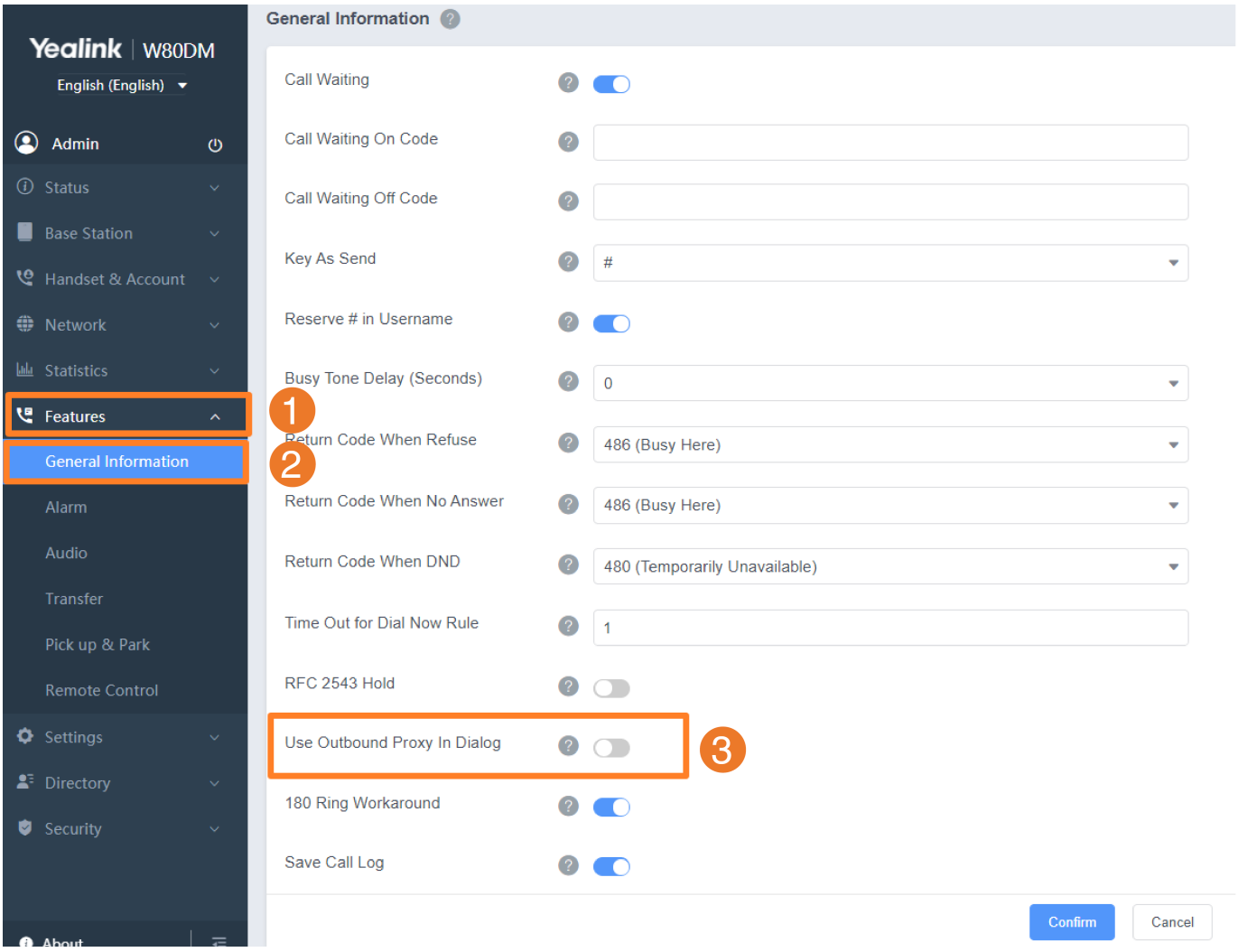
An outbound proxy server can receive all initiating request messages and route them to the designated destination. If the device is configured to use an outbound proxy server within a dialog, all SIP request messages from the device will be sent to the outbound proxy server as a mandatory requirement.

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).

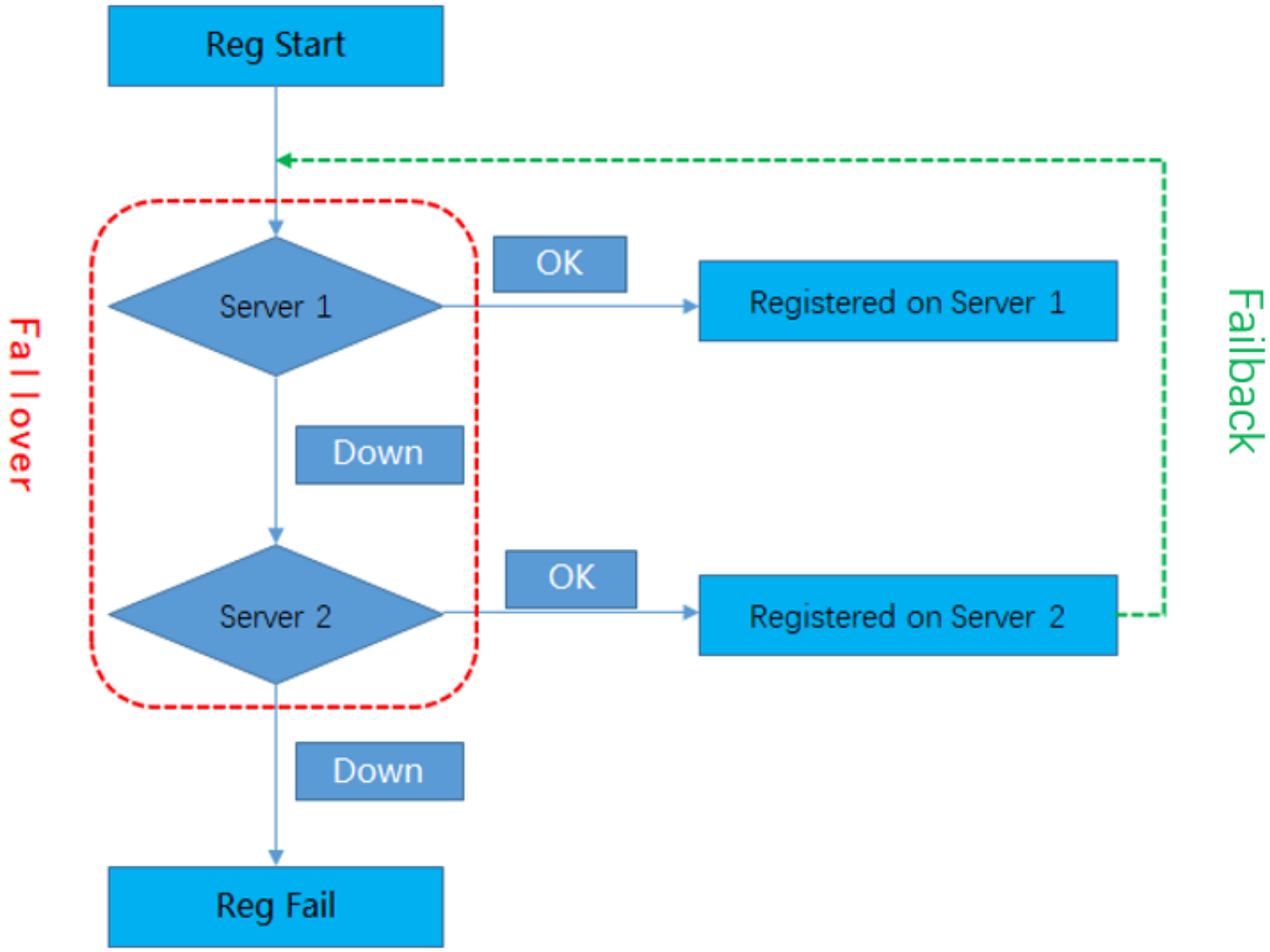
Server Redundancy

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:

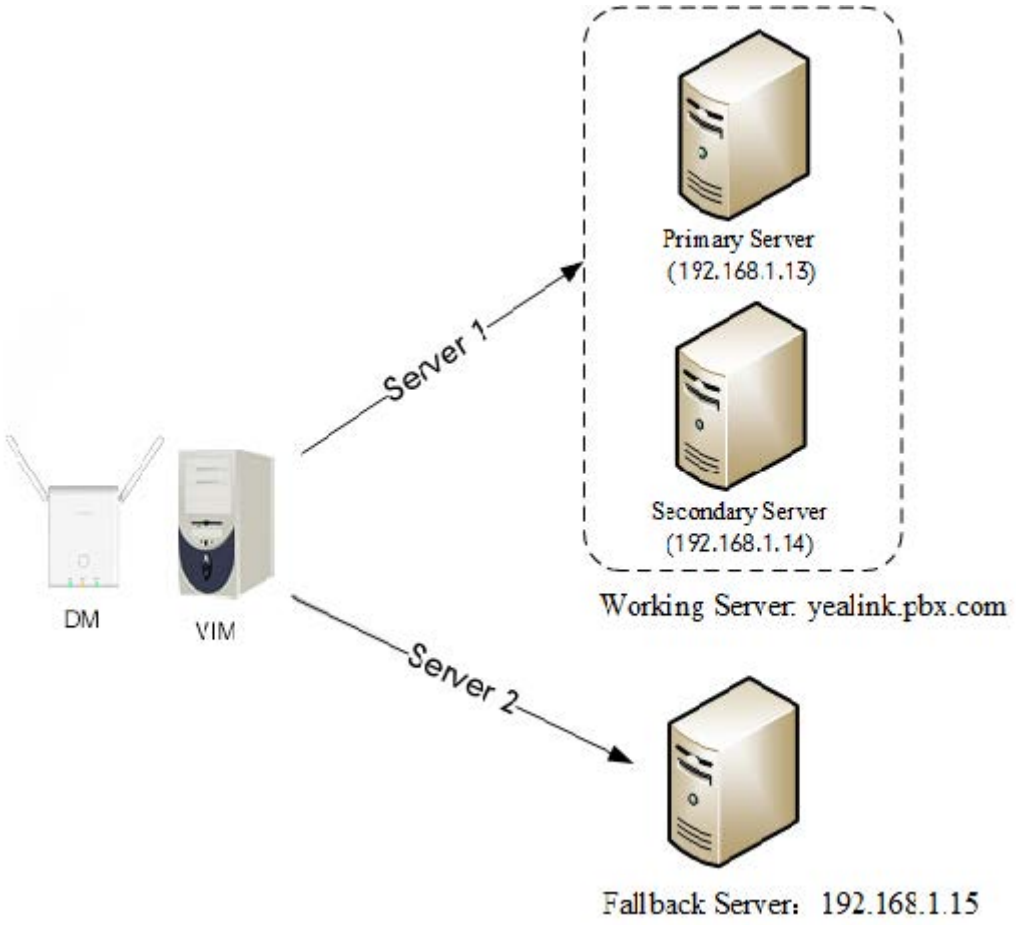
- **Failover**: In this mode, the full phone system functionality is preserved by having a second equivalent capability call server take over from the one that has gone down/offline. This mode of operation should be done using the DNS mechanism from the primary to the secondary server. Therefore, if 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. The DNS mechanism is used such that the working server is resolved to multiple servers with different IP addresses for failover purposes. The working server is deployed in redundant pairs, designated as primary and secondary servers. The primary server (for example, 192.168.1.13) has the highest priority server in a cluster of servers resolved by the DNS server. The secondary server (for example, 192.168.1.14) backs up 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 with 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(es) associated with that domain name will be resolved through DNS as specified by RFC 3263. The DNS query involves NAPTR, SRV and A queries, which allows the 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 an 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 Phones

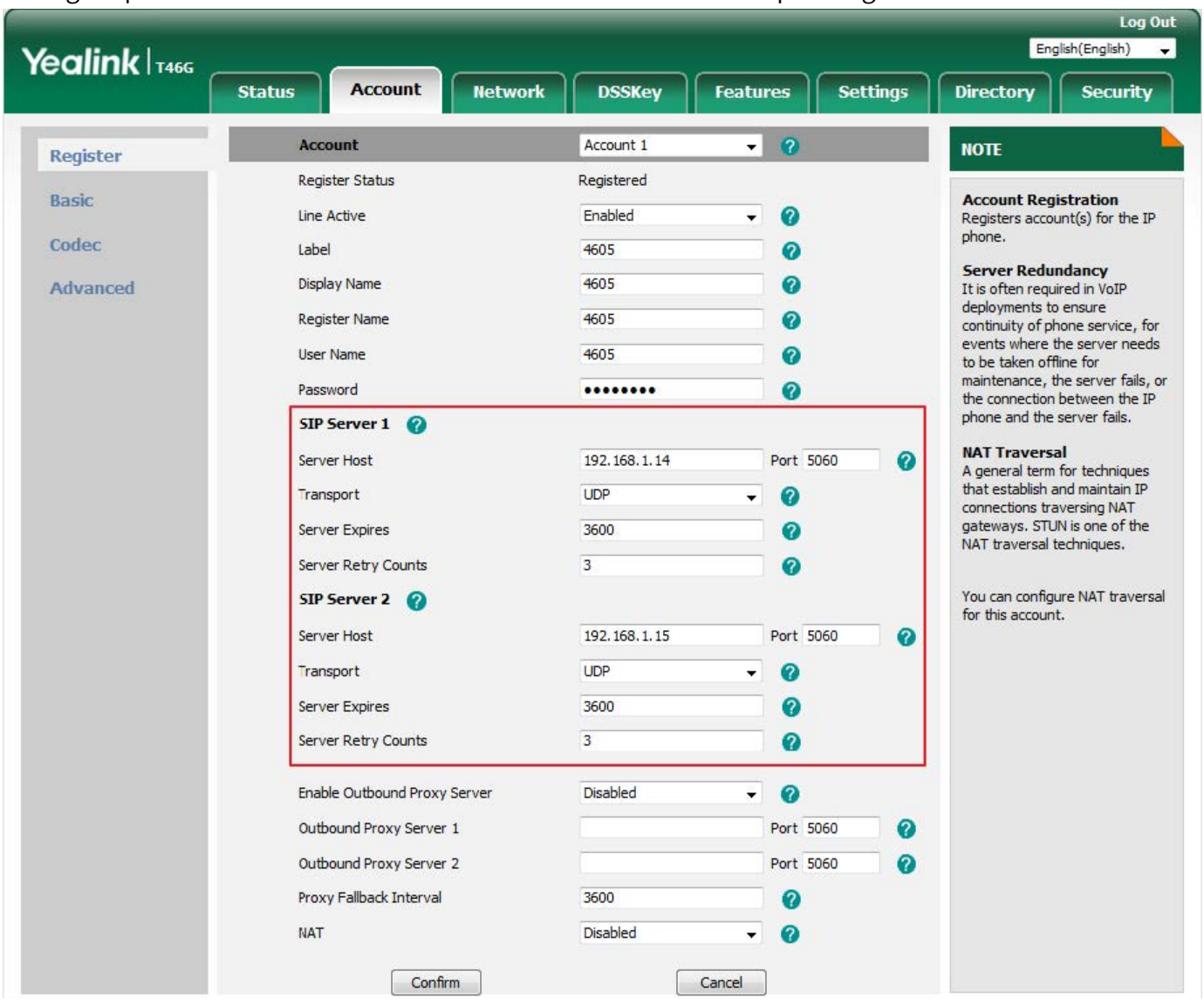
Set via the Web User Interface

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

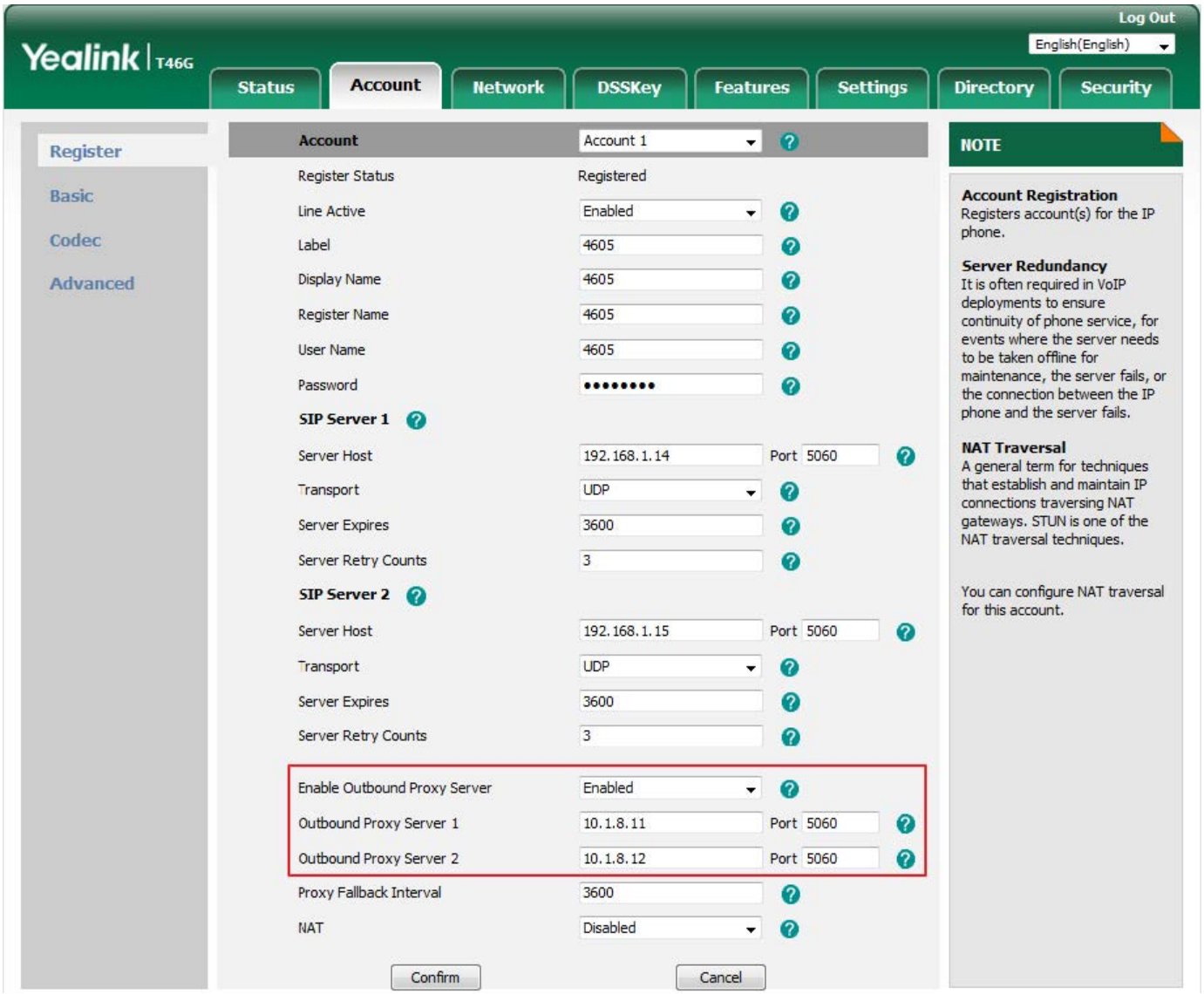
To configure server redundancy for fallback purposes

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 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 outbound proxy server 2 in the corresponding fields.

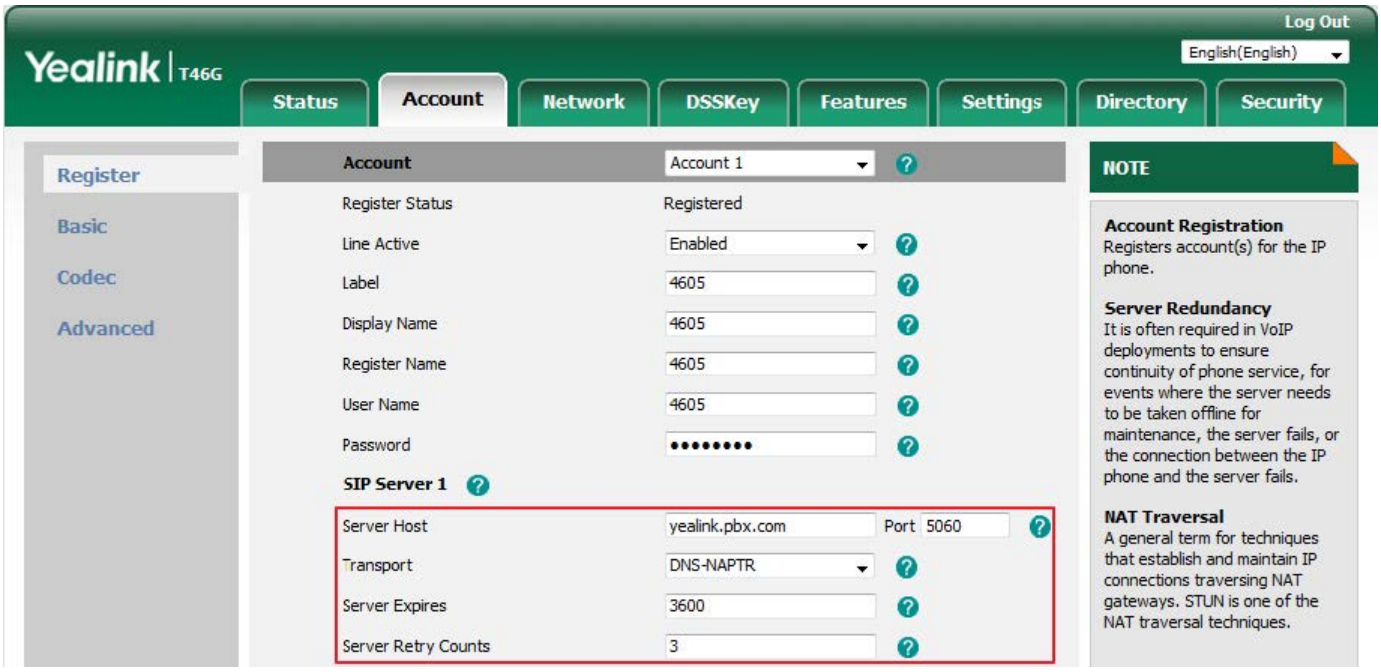


6. Click **Confirm** to accept the change.

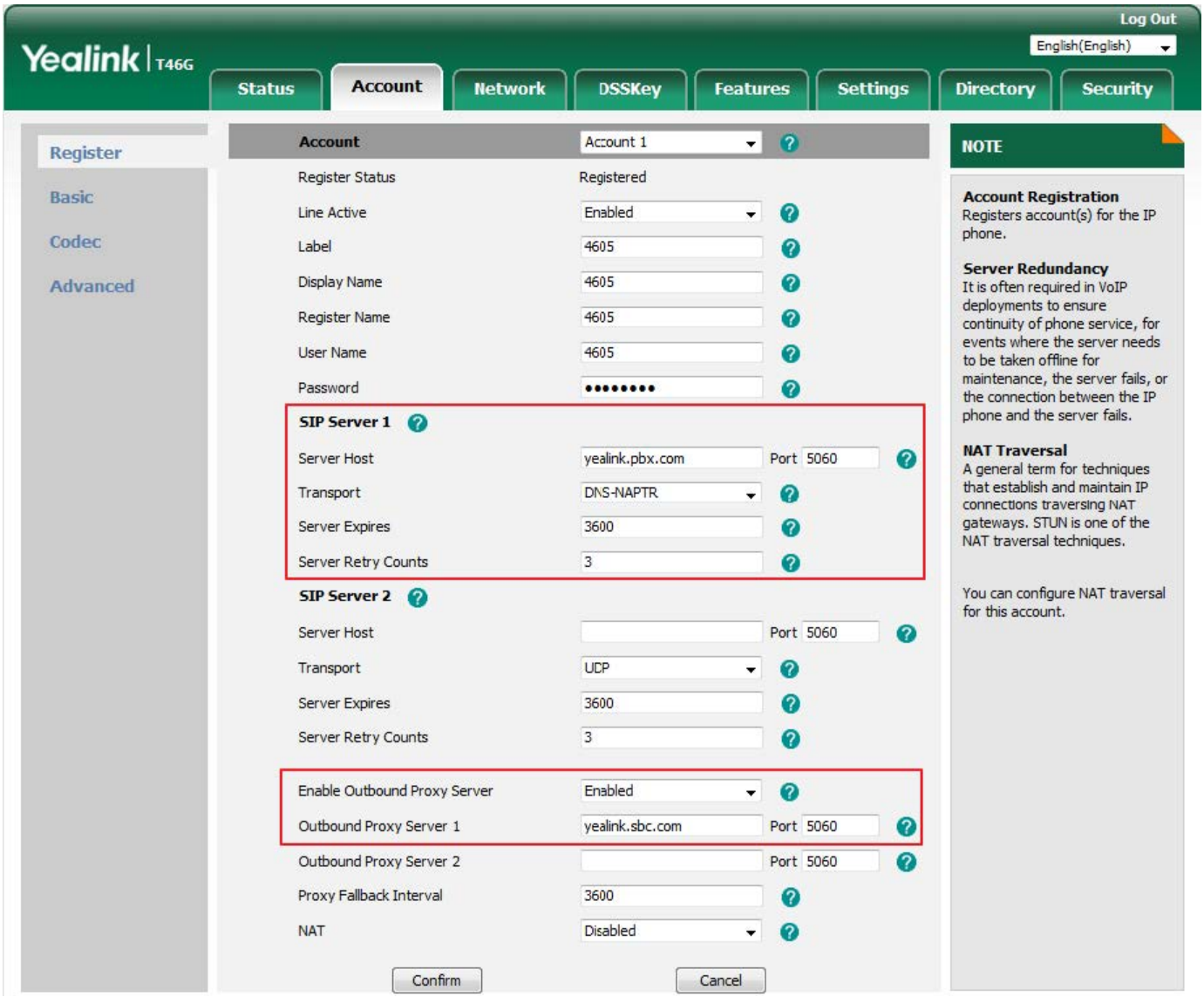
To configure server redundancy for failover purposes

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 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 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.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

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.reg	**0**-Disabled, the phone will not attempt to register to the secondary server, since the phone assumes that the primary and	0	It enables or disables the phone to send registration requests to the secondary

ister_on_enable[1] [2]	secondary servers share registration information. So the phone will directly send the requests to the secondary server. **1**-Enabled, the phone will register to the secondary server first, and then send the requests to it.		server when encountering a failover.
sip.skip_redundant_failover_addr	**0**-Disabled **1**-Enabled	1	It enables or disables the phone only to send requests to the servers with different IP addresses when encountering a failover.
account.X.sip_server.Y.only_signal_with_registered[1] [2]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to only send requests to the registered server when encountering a failover. It works only if "account.X.sip_server.Y.register_on_enable" is set to 1 (Enabled) and "account.X.sip_server.Y.failback_mode" is set to 1, 2, or 3.
account.X.sip_server.Y.invite_retry_counts[1] [2]	Integer from 1 to 10	3	It configures the number of retries attempted before sending requests to the next available server when encountering a failover.
account.X.sip_server.Y.failback_mode[1]	**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	0	It configures the mode for the phone to retry the primary server in failover. It works only if

[2]	by DNSTTL on the registered server expires, the phone will retry to send requests to the primary server. **2**-Registration: the phone will send requests to the last registered server first. If the registration expires, the phone will retry to send requests to the primary server. **3**-duration: the phone will send requests to the last registered server first. If the time defined by the account.X.sip_server.Y.failback_timeout parameter expires, the phone will retry to send requests to the primary server.		"template.X.sip_server.Y.address" is set to the domain name of the SIP server.
account.X.sip_server.Y.failback_timeout[1] [2]	0, Integer from 60 to 65535	3600	It configures the timeout (in seconds) for the phone to retry to send requests to the primary server after failing over to the current working server. If you set the parameter to 0, the phone will not send requests to the primary server until a failover event occurs with the current working server. If you set the parameter between 1 and 59, the timeout will be 60 seconds. It works only if "account.X.sip_server.Y.failback_mode" is set to 3 (duration).
account.X.sip_server.Y.fai	**0**-Disabled **1**-Enabled, the phone will immediately re-subscribe to the secondary server, ensuring	0	It enables or disables the phone to retry to re-subscribe after registering to

lback_subscribe.enable[1] [2]	the normal use of the features associated with the subscription (for example, BLF, SCA).		the secondary server with a different IP address 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.
- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

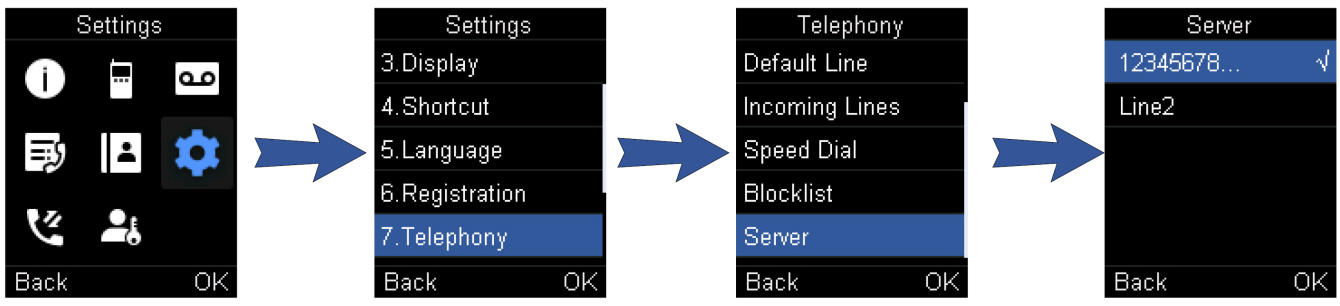
[2] Y is the server ID. Y=1-2.

Appendix

Appendix A: SIP Server Name Resolution Configuration

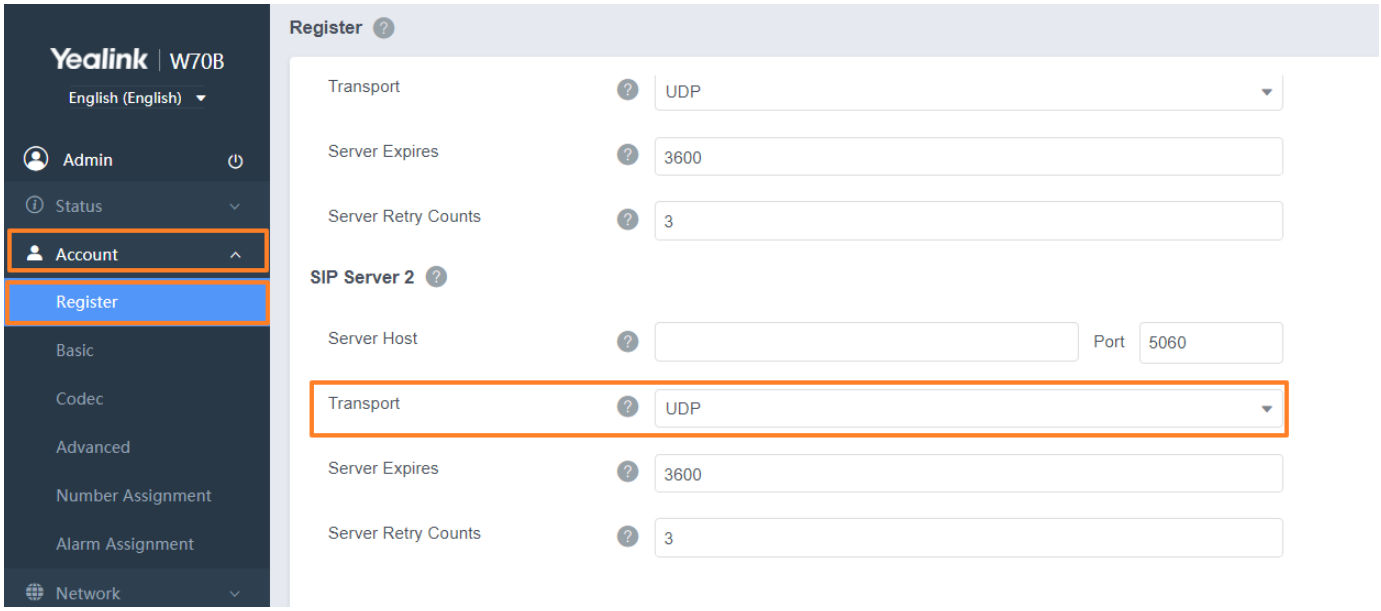
- **Set via the Device Interface (W70B)**
- W53H/W56H/W57R/W59R/W71H/W73H/W74H/W78H:

  OK > **Settings** > **Telephony** > **Server (default PIN: 0000)** > **Server Y** > **Transport**.

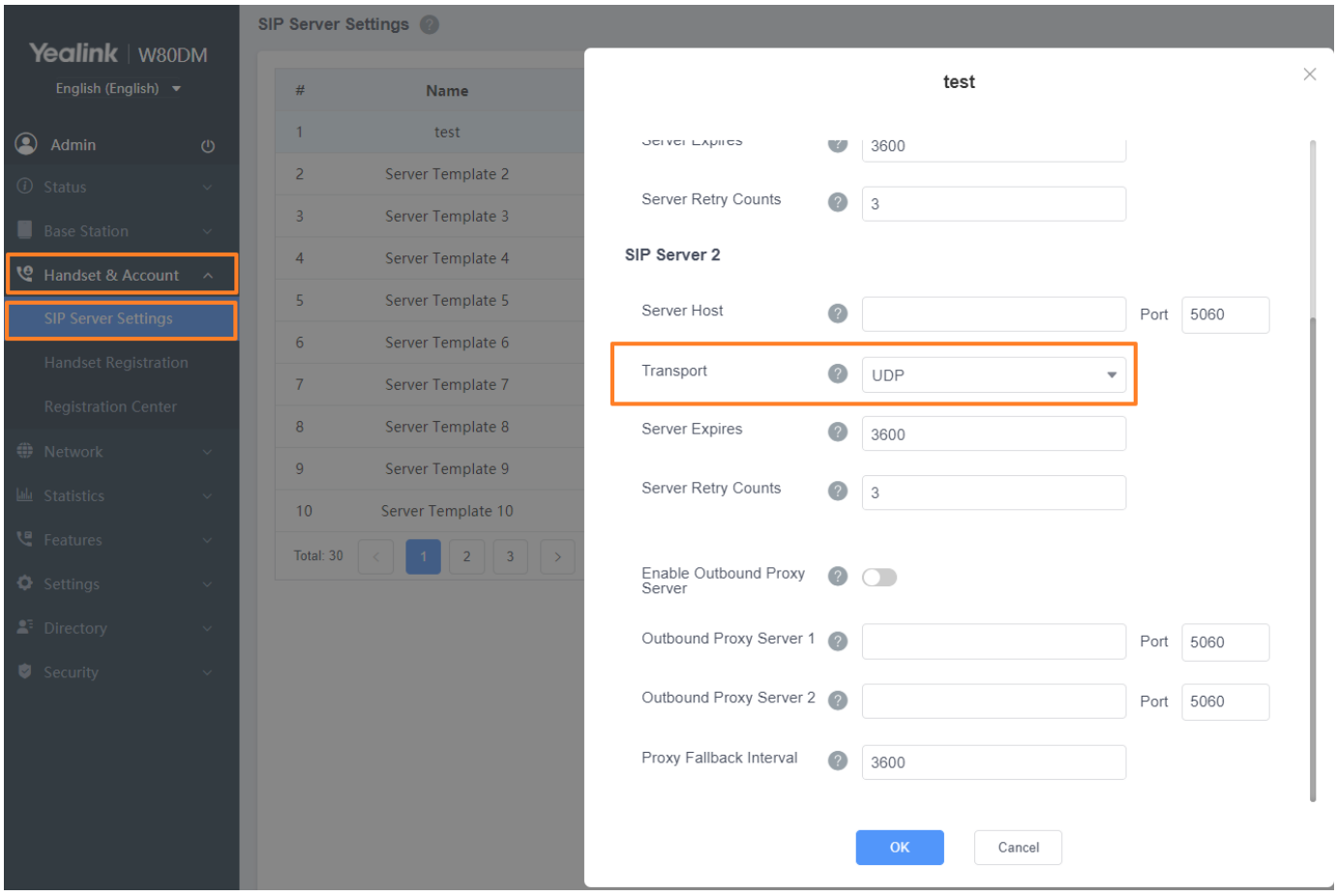


- **Set via the Web User Interface**

  a. On the W70B web user interface, go to **Account** > **Register** > **SIP Server Y** > **Transport**.



b. On the W75/W80/W90 Multi-Cell System web user interface, go to **Handset & Account** > **SIP Server Settings** > **Edit** > **SIP Server Y[2]** > **Transport**.



- **Configuration Parameter**

account.X.sip_server.Y.transport_type
template.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] [4]	**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.
template.X.sip_server.Y.transport_type[2] [5]	**0**-UDP **1**-TCP **2**-TLS **3**-DNS NAPTR, if no server port is given, the device performs the DNS NAPTR and SRV queries for the service type and port.	0	It configures the type of transport protocol.
account.X.naptr_build[1]	**0**-SRV query using UDP only **1**-SRV query using UDP, TCP, and TLS.	0	It configures the way of SRV query for the phone to be performed when no result is returned from the NAPTR query.
sip.dns_transport_type	**0**-UDP **1**-TCP	0	It configures the transport protocol the phone uses to perform a DNS query.
static.network.dns.query_timeout[3]	Integer from 0 to 65535	3	It configures the interval (in seconds) at which the phone retries to resolve a domain name when the DNS server does not respond.
static.network.dns.retry_times[3]	Integer from 0 to 65535	2	It configures the retry times when the DNS server does not respond.

> [1]X is the account ID.
> - For W70B, X=1-10.
> - For W75DM, X=1-20.
> - For W80 multi-cell system, X=1-100.
> - For W90 multi-cell system, X=1-250.
> - For VIM system, X=1-2500.
>
> [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.
> [4]This parameter is only applicable to W70B.
> [5]This parameter is only applicable to W75/W80/W90 Multi-Cell System. X is the template ID. X=1-10.

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 static DNS cache. Support for negative caching of DNS queries as described in RFC 2308 is also provided to allow faster failover when prior DNS queries have returned no results from the DNS server.

Behave with a Configured DNS Server

1. When the phone **is configured with a DNS server**, it will behave as follows to resolve the domain name of the server:
   - The phone performs a DNS query to resolve the domain name from the DNS server.
   - If the DNS query returns no results for the domain name, or the returned record cannot be contacted, the values in the static DNS cache (if configured) are used when their configured time intervals are not elapsed.
   - If the configured time interval 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[2]
account.X.static_cache_pri[1]
account.X.dns_cache_type[1]
dns_cache_naptr.X.name[2]
dns_cache_naptr.X.order[2]
dns_cache_naptr.X.preference[2]
dns_cache_naptr.X.replace[2]
dns_cache_naptr.X.ttl
dns_cache_srv.X.name
dns_cache_srv.X.port
dns_cache_srv.X.priority
dns_cache_srv.X.target
dns_cache_srv.X.weight
dns_cache_srv.X.ttl
dns_cache_a.X.name
dns_cache_a.X.ip
dns_cache_a.X.ttl
static.network.dns.ttl_enable
static.network.dns.last_cache_expired
static.network.dns.last_cache_expired.enable

Parameter	Permitted Values	Default	Description
account.X.dns_cache_type[1]	**0**-Perform real-time DNS query rather than using DNS cache. **1**-Use DNS cache, but do not record the additional records. **2**-Use DNS cache and cache the additional DNS records.	1	It configures whether the phone uses the DNS cache for domain name resolution of the SIP server and caches the additional DNS records.
account.X.static_cache_pri[1]	**0**-Use domain name resolution from 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 more preferred.
dns_cache_naptr.X.preference[2]	Integer from 0 to 65535	0	It configures the preference of NAPTR record X. NAPTR record with lower preference is more preferred.
dns_cache_naptr.X.replace[2]	Domain name	Blank	It configures a domain name to be used for the next SRV query in NAPTR record X.
dns_cache_naptr.X.service[2]	**SIP+D2U**-SIP over UDP **SIP+D2T**-SIP over TCP **SIPS+D2T**-SIPS over TLS	Blank	It configures the transport protocol available for the SIP server in NAPTR record X.
dns_cache_naptr.X.ttl[2]	Integer from 30 to 2147483647	300	It configures the time interval (in seconds) that 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 SRV record X.
dns_cache_srv.X.port[2]	Integer from 0 to 65535	0	It configures the port to be used in SRV record X.
dns_cache_srv.X.priority[2]	Integer from 0 to 65535	0	It configures the priority for the target host in SRV record X. Lower priority is more preferred.
dns_cache_srv.X.target[2]	Domain name	Blank	It configures the domain name of the target host for an A query in SRV record X.
dns_cache	Integer from 0 to 65535	0	It configures the weight of the target

_srv.X.weight[2]			host in SRV record X. When priorities are equal, weight is used to differentiate the preference. Higher weight is more preferred.
dns_cache_srv.X.ttl[2]	Integer from 30 to 2147483647	300	It configures the time interval (in seconds) that 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 A record X.
dns_cache_a.X.ip[2]	IP address	Blank	It configures the IP address that the domain name in A record X maps to.
dns_cache_a.X.ttl[2]	Integer from 30 to 2147483647	300	It configures the time interval (in seconds) that A record X may be cached before the record should be consulted again.
static.network.dns.ttl_enable[3]	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to use TTL (Time To Live) in the A record.
static.network.dns.last_cache_expired	Integer from 0 to 65535 **0**-the expired DNS cache can only be used once. After using, the phone will perform a DNS query again. **1 to 65535**-the phone will use the expired DNS cache during the specified period. After that, the phone will perform a DNS query again.	3600	It configures the validity period of the expired DNS cache. It works only if "static.network.dns.last_cache_expired.enable" is set to 1 (Enabled).
static.network.dns.last_cache_expire	**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.

d.enable			

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

[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 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 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 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.

Number Assignment

Introduction

After the handset is registered to the base station, you can assign one or more outgoing lines or incoming lines to 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 base station.

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.

Number Assignment Configuration

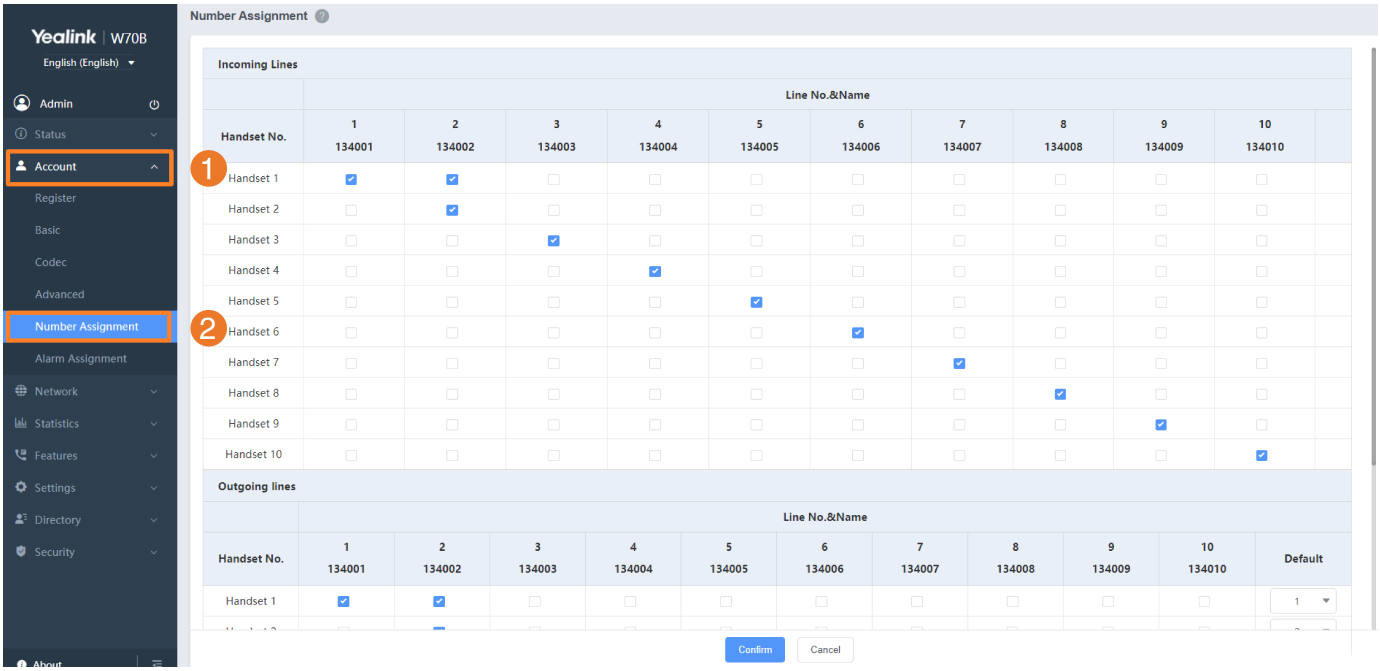
Set via the Device Interface

- W53H/W56H/W57R/W59R/W59R Pro/W71H/W73H/W74H/W78H:
- Go to **OK** > **Settings** > **Telephony.**



Set via the Web User Interface

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



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 5-Line 5 6-Line 6 7-Line 7 8-Line 8 9-Line 9 10-Line 10 Multiple line IDs are separated by commas.	The incoming line for the DECT phone is line 1- line 10. The incoming line for 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. The incoming line for handset 6 is line 6.	It configures the lines to receive incoming calls for a specific handset.

		The incoming line for handset 7 is line 7. The incoming line for handset 8 is line 8. The incoming line for handset 9 is line 9. The incoming line for handset 10 is line 10.	
handset.X.dial_out_lines[1]	1-Line 1 2-Line 2 3-Line 3 4-Line 4 5-Line 5 6-Line 6 7-Line 7 8-Line 8 9-Line 9 10-Line 10	The outgoing line for the DECT phone is line 1-line 10. 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. The outgoing line for handset 6 is line 6. The outgoing line for handset 7 is line 7. The outgoing line for handset 8 is line 8. The outgoing line for handset 9 is line 9. The outgoing line for handset 10 is line 10.	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 10	X	It configures the default line to place outgoing calls for a specific handset. It is applicable to all handsets except the CP930W.

> [1]X is the handset ID. X=1-10.

Local Directory

Introduction

Yealink phones maintain a local directory that you can use to store contacts. You can store up to 100 contacts per handset, each with a name, a mobile number, and an office number.

Contacts and groups can be added either one by one or in batches using a local contact file. Yealink phones support both .xml and .csv format contact files, but you can only customize the *.xml format contact file.

Local Contact File Customization

You can ask the distributor or Yealink FAE for the local contact template.

Local Contact File Elements and Attributes

The following table lists the elements and attributes you can use to add groups or contacts in the local contact file.

We recommend that you do not edit these elements and attributes.

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

	ber	
	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"/>

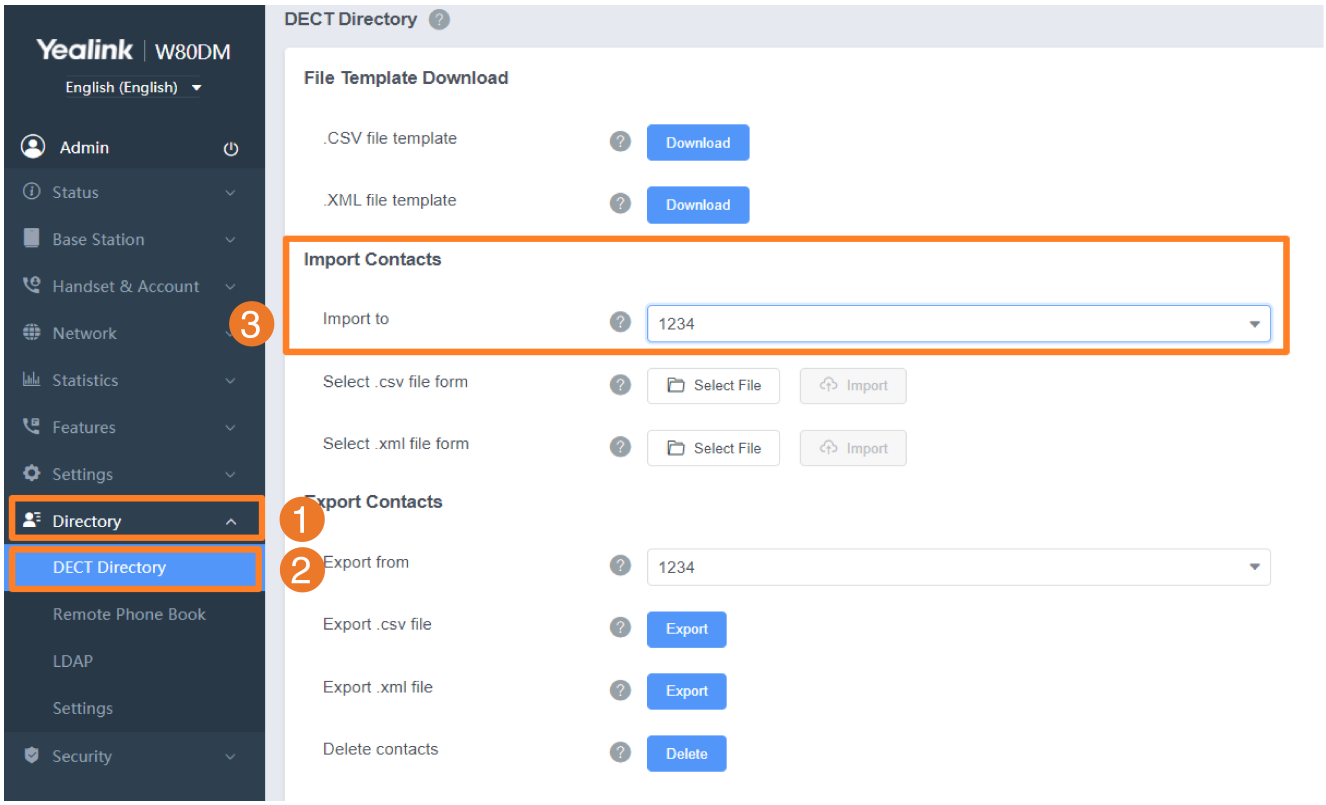
   <contact display_name="Tom" office_number="2020" mobile_number="2021" other_number="2112"/>
4. Save the changes and place this file on the provisioning server.

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** > **DECT Directory** > **Import Contacts** > **Import to (Handset X)**.



Configuration Parameter

handset.X.contact_list.url

Parameter	Permitted Values	Default	Description
handset.X.contact_list.url[1]	URL within 511 characters	Blank	It configures the access URL of the contact file of a specific handset.

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

Lightweight Directory Access Protocol (LDAP)

Introduction

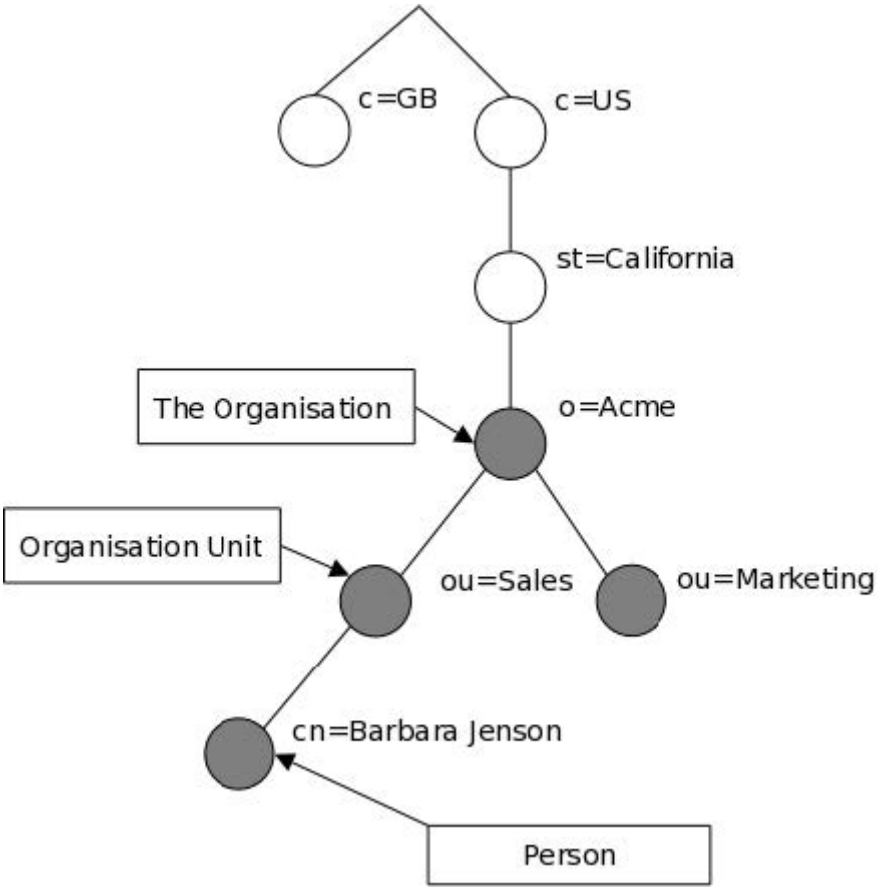
LDAP (Lightweight Directory Access Protocol) is a client/server protocol for accessing a directory service. LDAP is a directory service protocol that runs over TCP/IP.

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
W53P	version 83 or later
CP930W-Base, CP935W-Base, W56P and W60P	version 85 or later

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

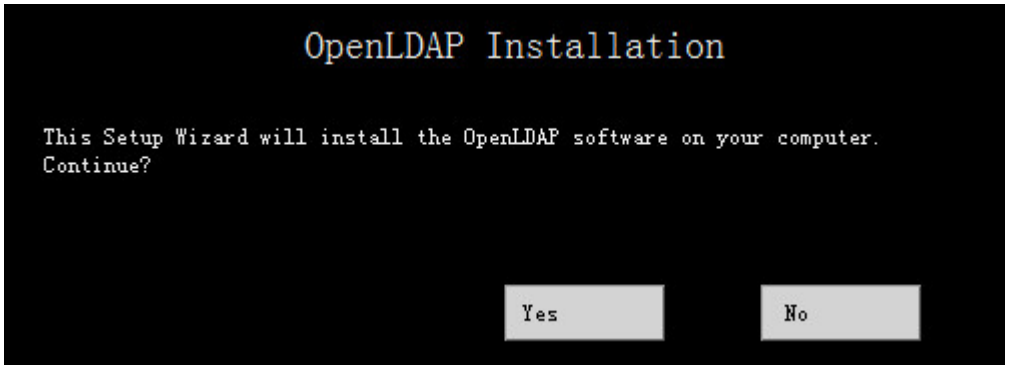
Install the OpenLDAP Server

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

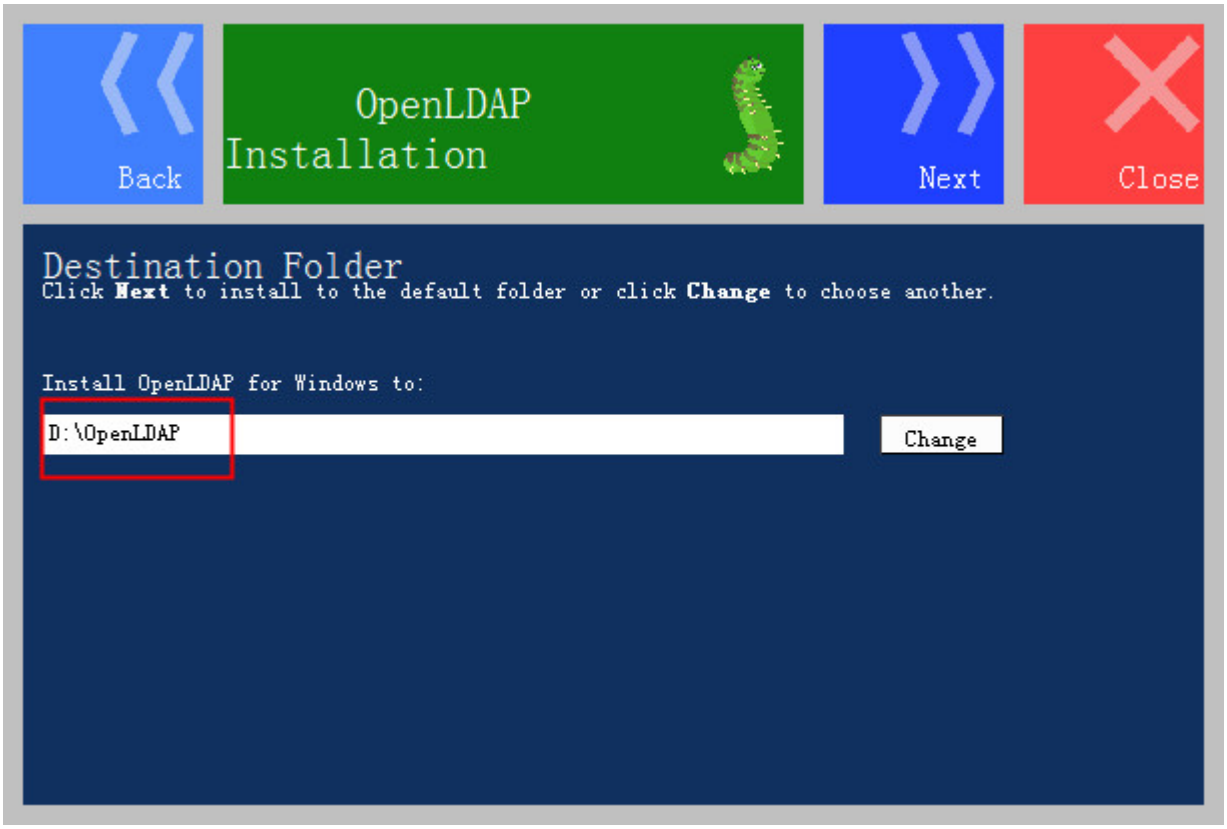
You can download it from http://www.userbooster.de/en/download/openldap-for-windows.aspx?l=en.

To install the OpenLDAP server:

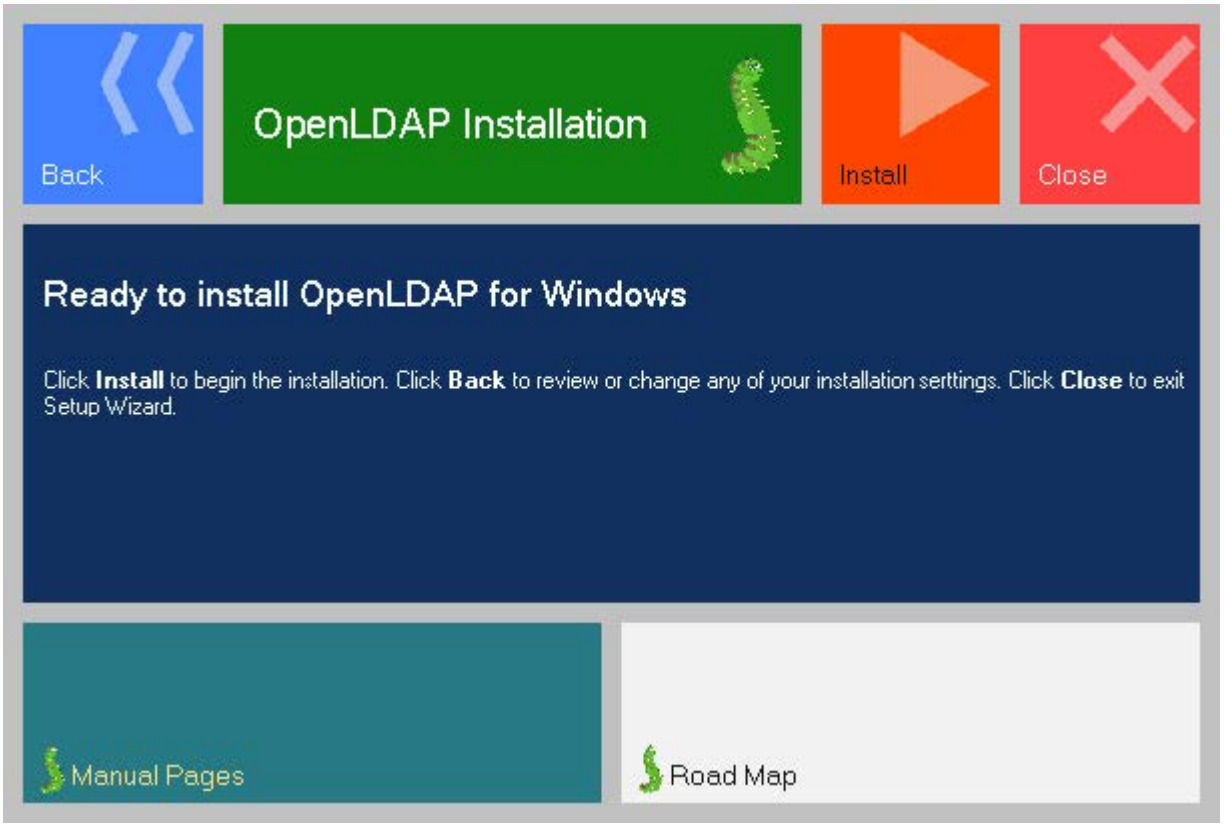
1. Double-click the OpenLDAP application to start the installation. You will be prompted for the installation.



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

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

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

For example:

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

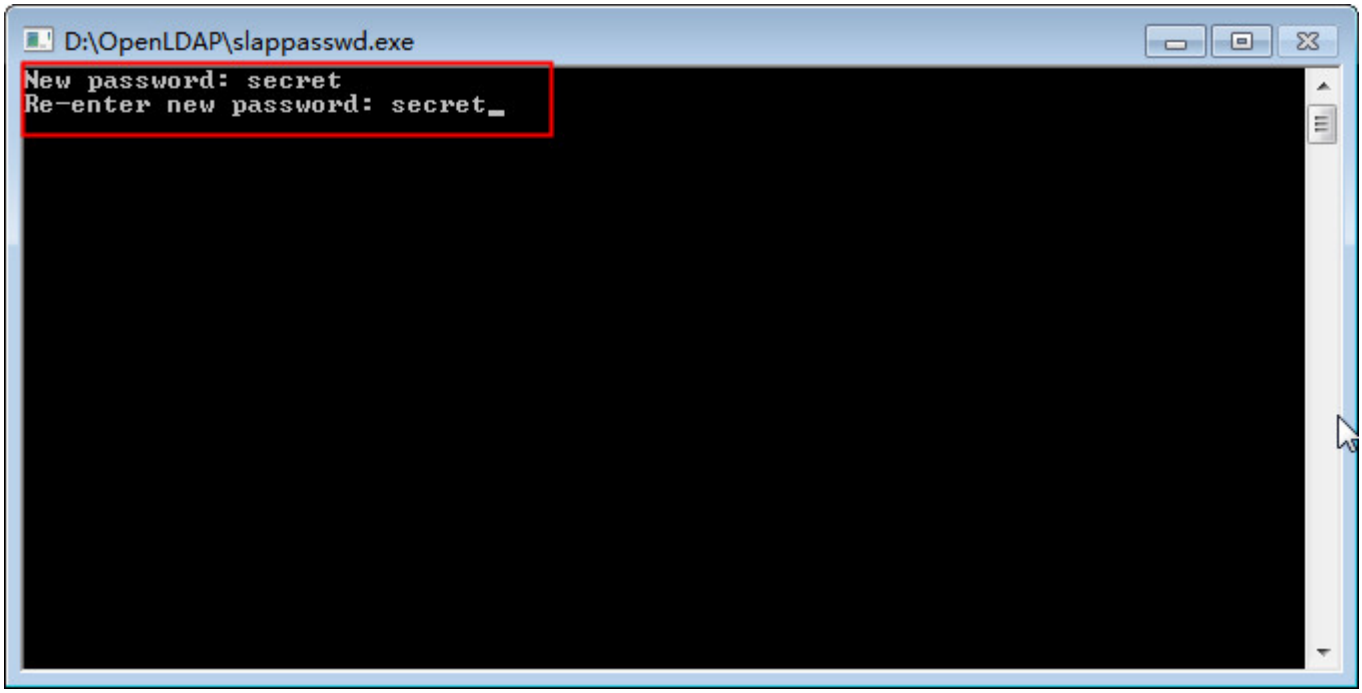
The suffix line means that the domain name of the LDAP directory is yealink.com. The Rootdn line

defines a management user named Manager.

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

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

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



Start the Slapd Service

To start the slapd service:

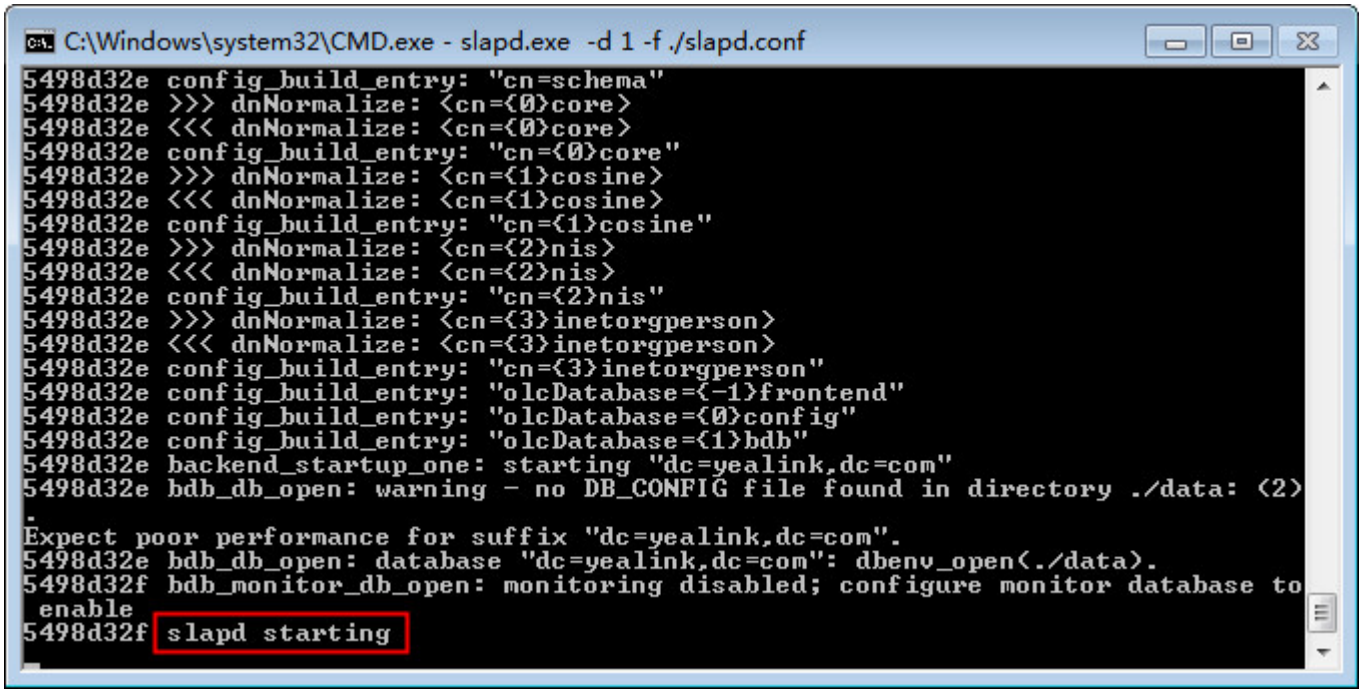
1. Click **Start** > **Run**.
2. Enter **cmd** in the dialog and click **OK** to enter the command line interface.
3. Access the server installation path. For example, execute the following commands to access the server installation path at **D:\OpenLDAP**.



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

```
C:\Users\yl0215>d:

D:\>cd OpenLDAP

D:\OpenLDAP>slapd.exe -d 1 -f ./slapd.conf
```

6. If the service runs successfully, you can find the prompt "**slapd starting**".
7. The screenshot for reference is shown 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 to 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 as ldif. Open the LDIF file with your favorite text editor and input the corresponding content.

The following shows an example of the content of the LDIF file:

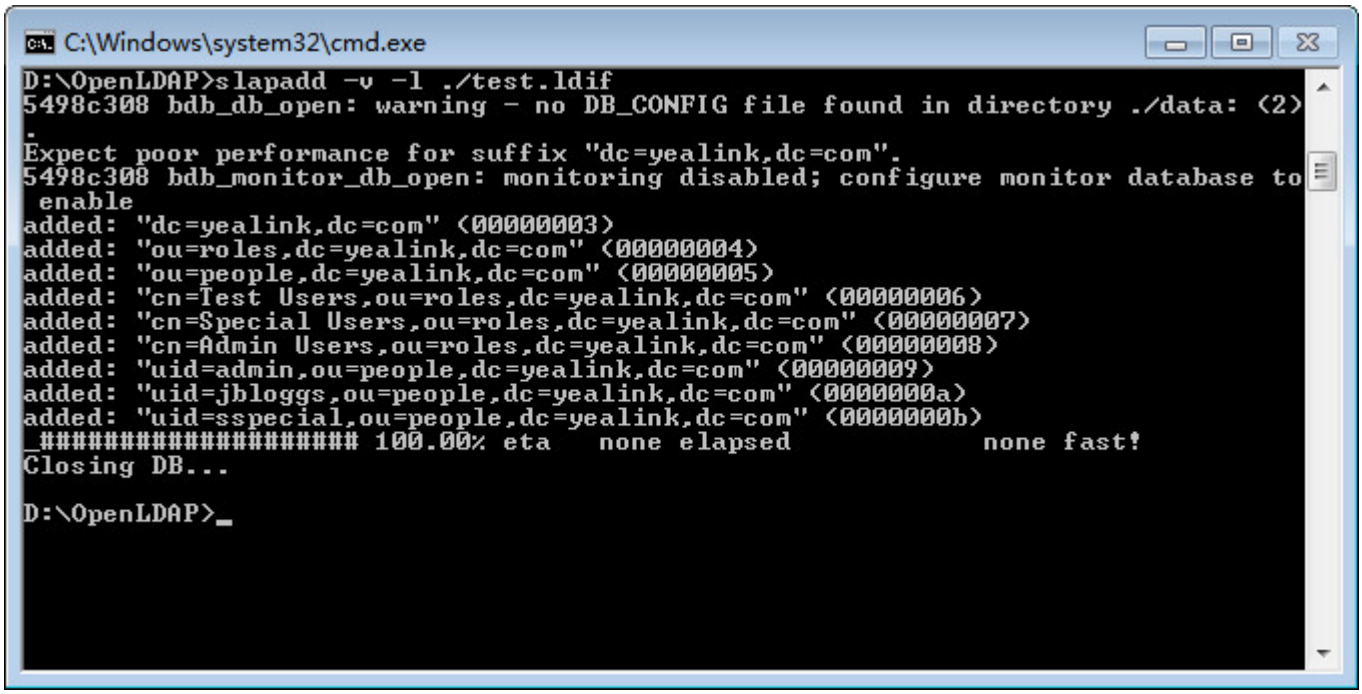
```
dn: dc=yealink,dc=com
objectClass: top
objectClass: dcObject
objectClass: domain
dc: yealink

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

```
objectClass: organizationalUnit
ou: roles

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

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

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

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

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

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

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

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

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

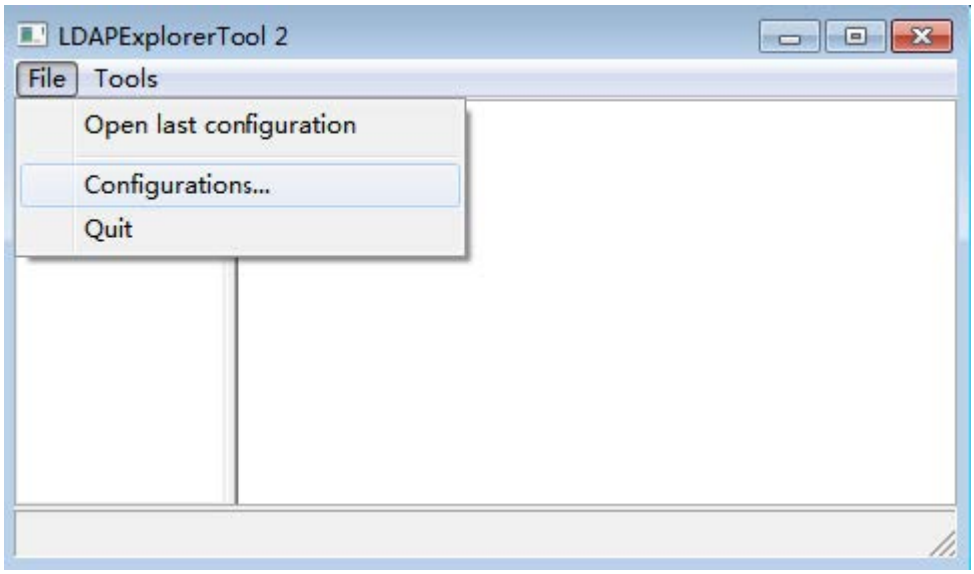
If you have an LDAPExploreTool2 application installed on your computer, open it now; otherwise, download the application from http://ldaptool.sourceforge.net/. And then complete the installation following the wizard.

Create a Configuration

To create a configuration:

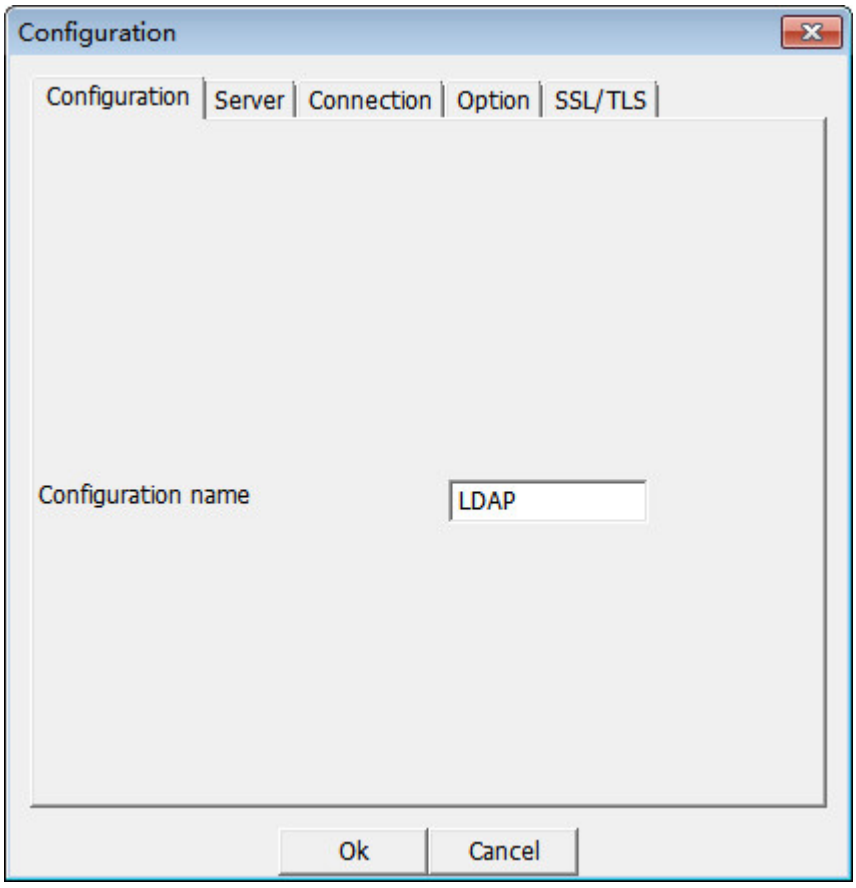
1. Double-click the LDAPExploreTool2.exe to run the application.

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

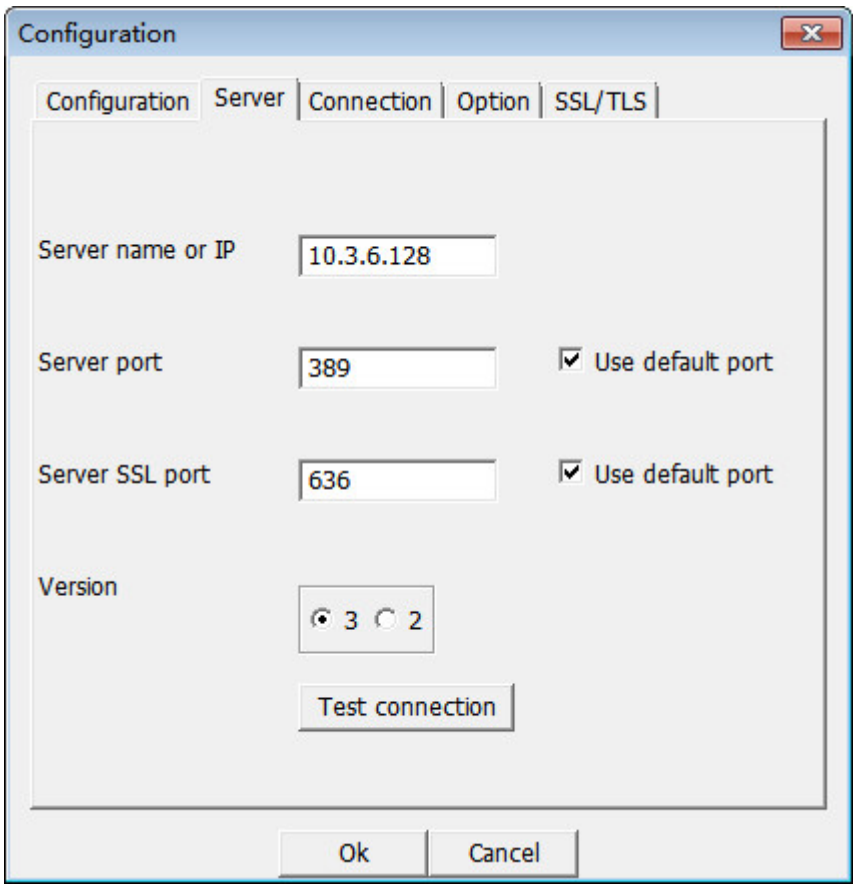


3. Click **New** to create a new configuration.

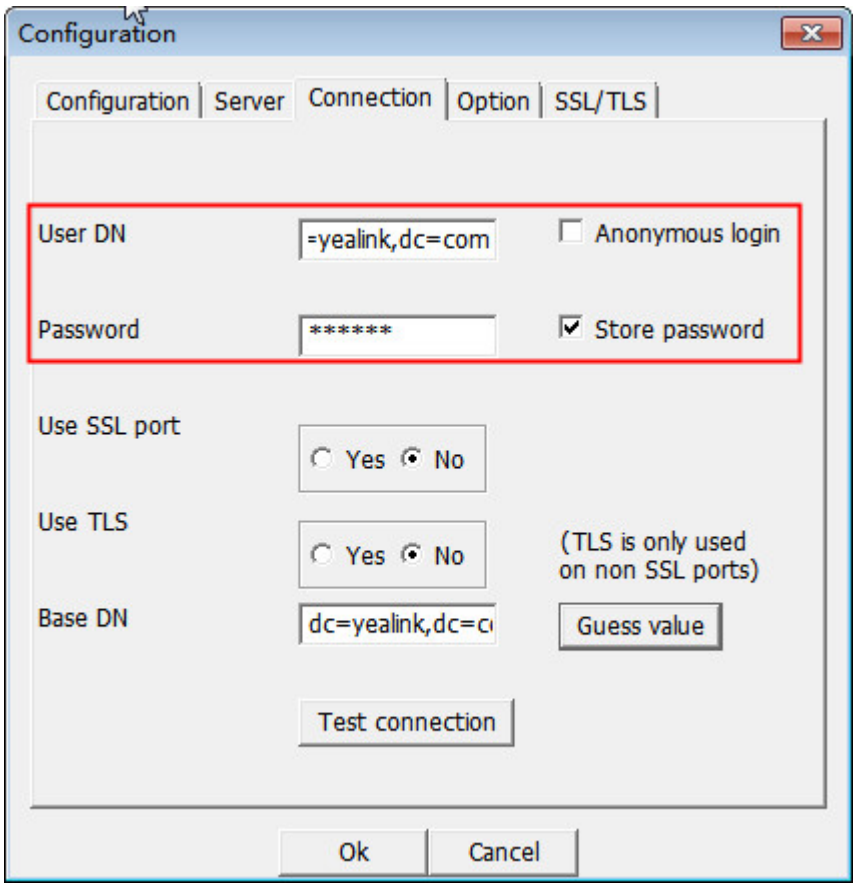
4. Enter a name in the **Configuration name** field under the **Configuration** tab.



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.



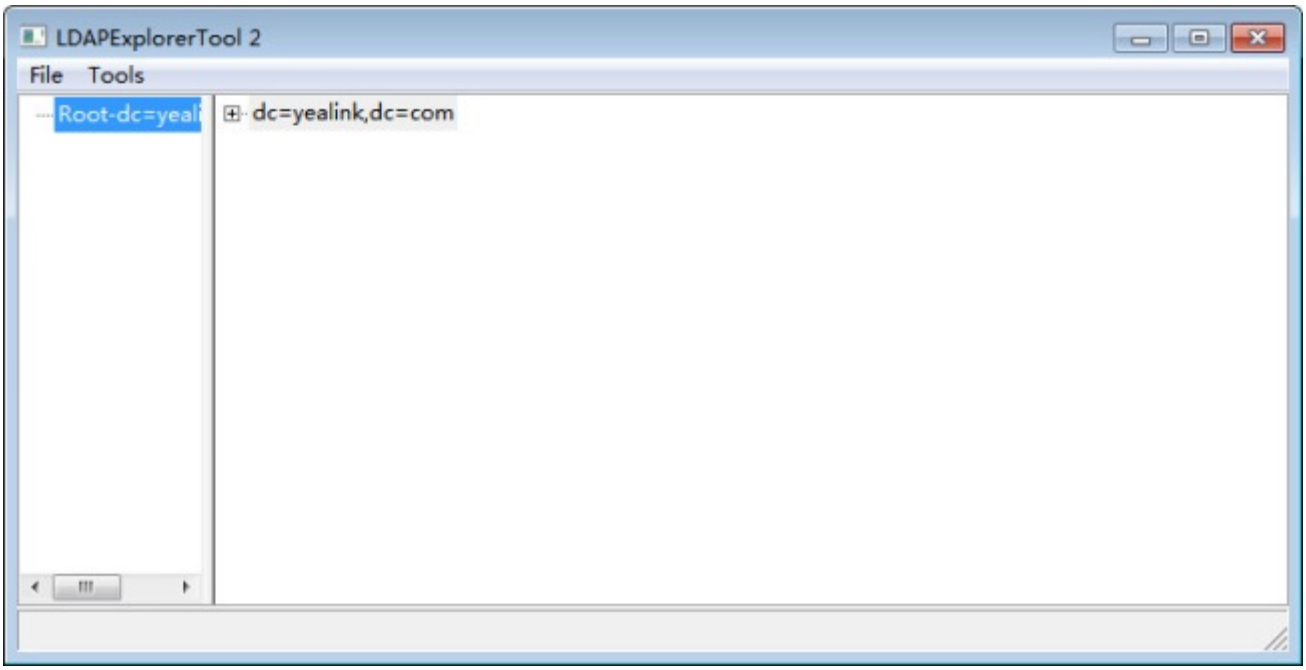
7. Click the **Guess value** to fill the **Base DN** automatically.
8. Click **Test connection** to test the connection to the LDAP server. If you encounter an error or warning during the test, you need to resolve the error or warning first according to the prompt, and then retry to test the connection.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

Add Entries

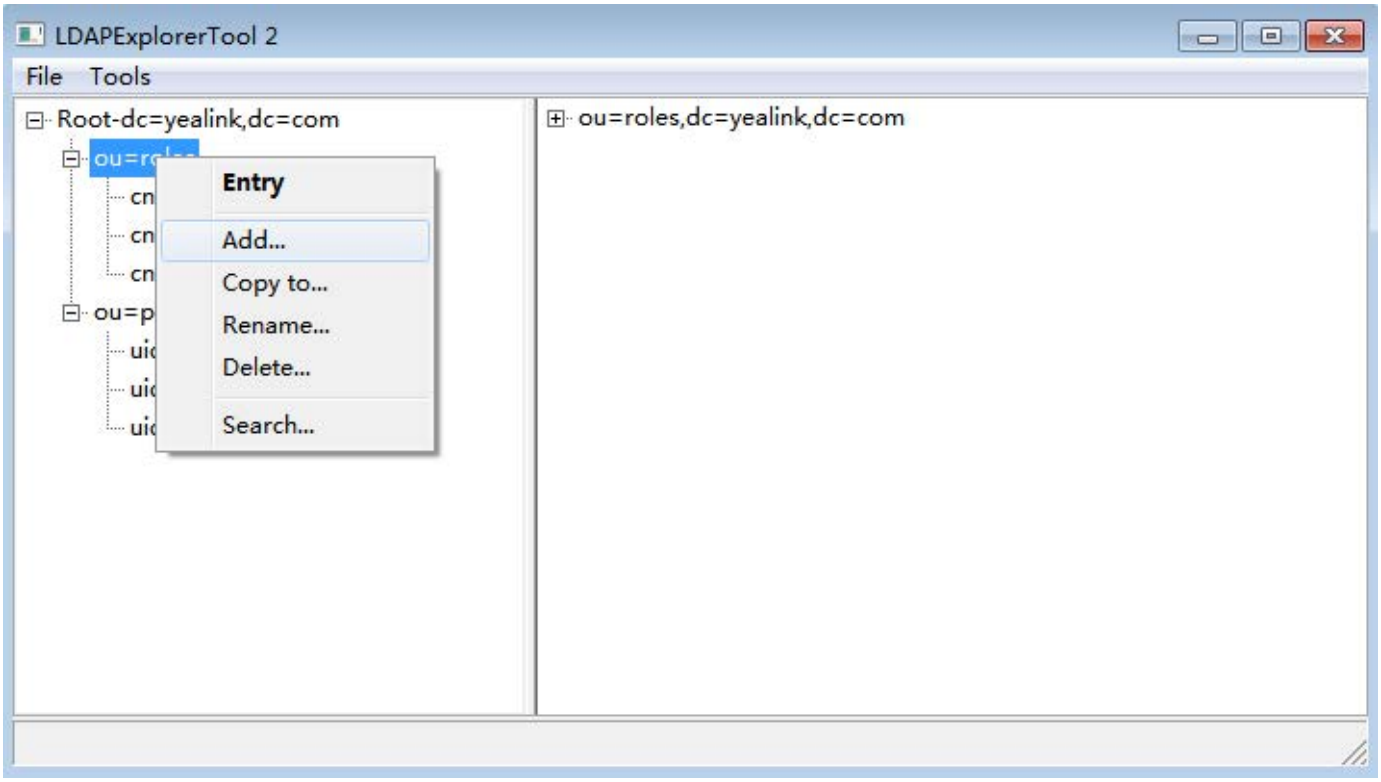
To add entries:

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.

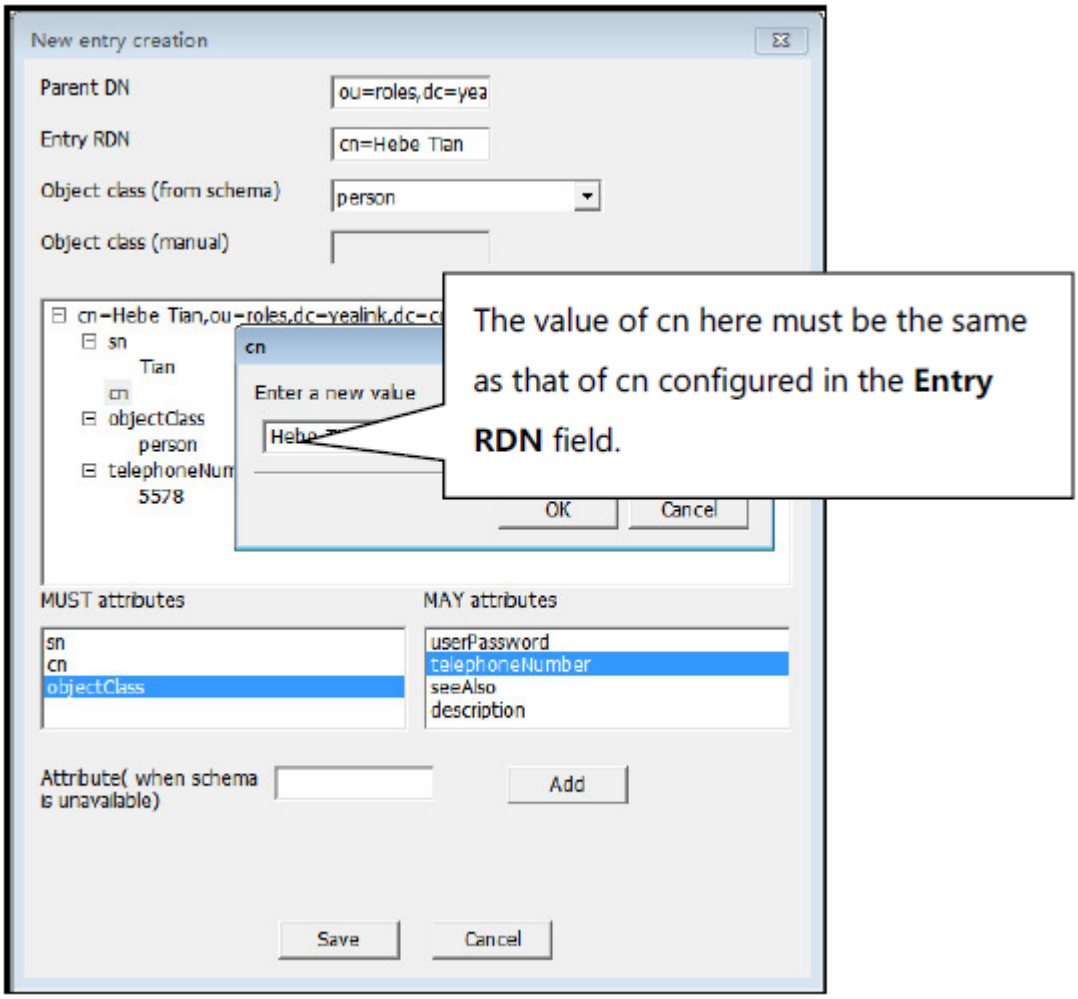
- **Parent DN**: It will be automatically generated according to the server configuration.
- **Entry RDN**: The format is cn=XXX. This is a unique identifier for each entry.
- **Object Class (from schema)**: Select the structure class to which the entry belongs. Each structure class has its must-have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

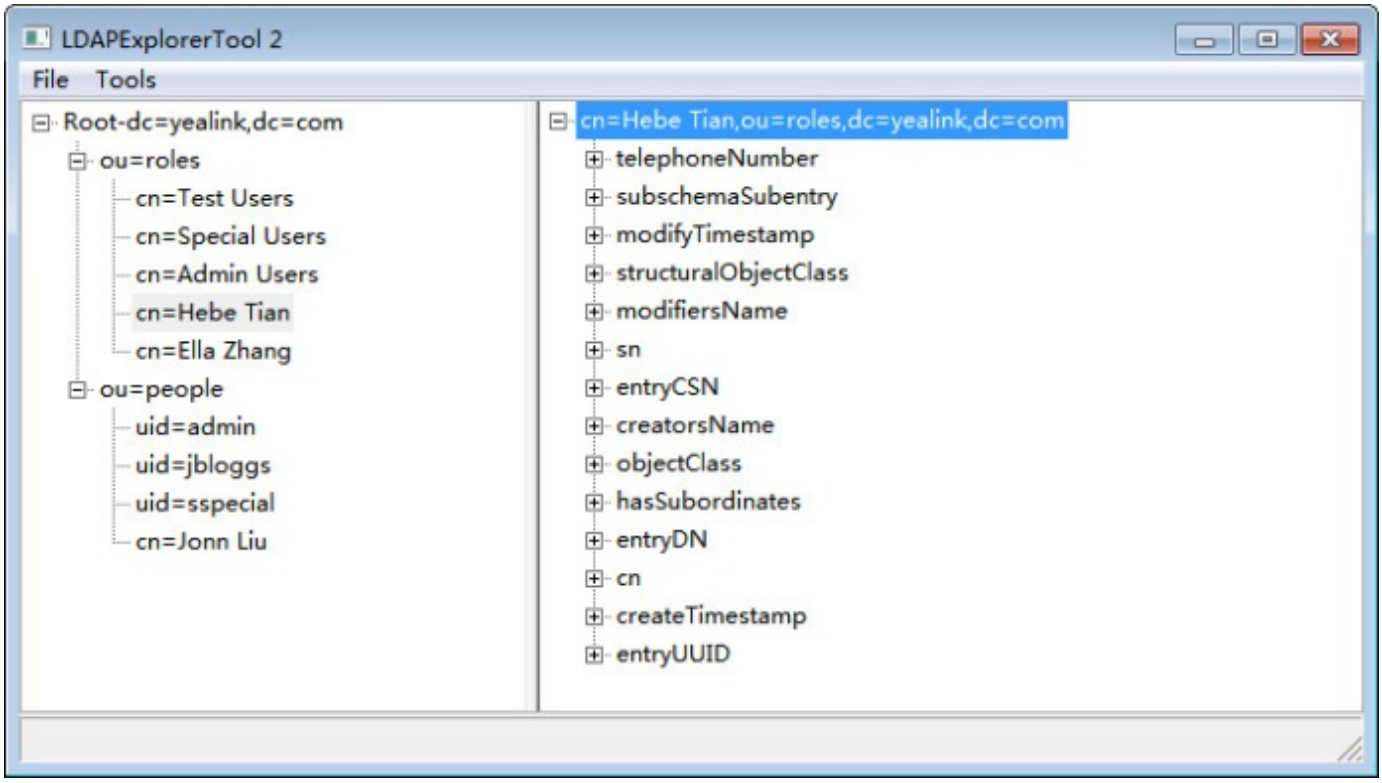
Attribute	Name	Description
cn	commonName	Full name of the entry.
gn	givenName	The first name is also called the Christian name.
sn	surname	Surname, last name, or family name.
telephoneNumber	telephoneNumber	Office phone number.
homePhone	homeTelephoneNumber	Home phone number.
mobile	mobileTelephoneNumber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



Microsoft Active Directory

Install the Microsoft Active Directory Domain Services

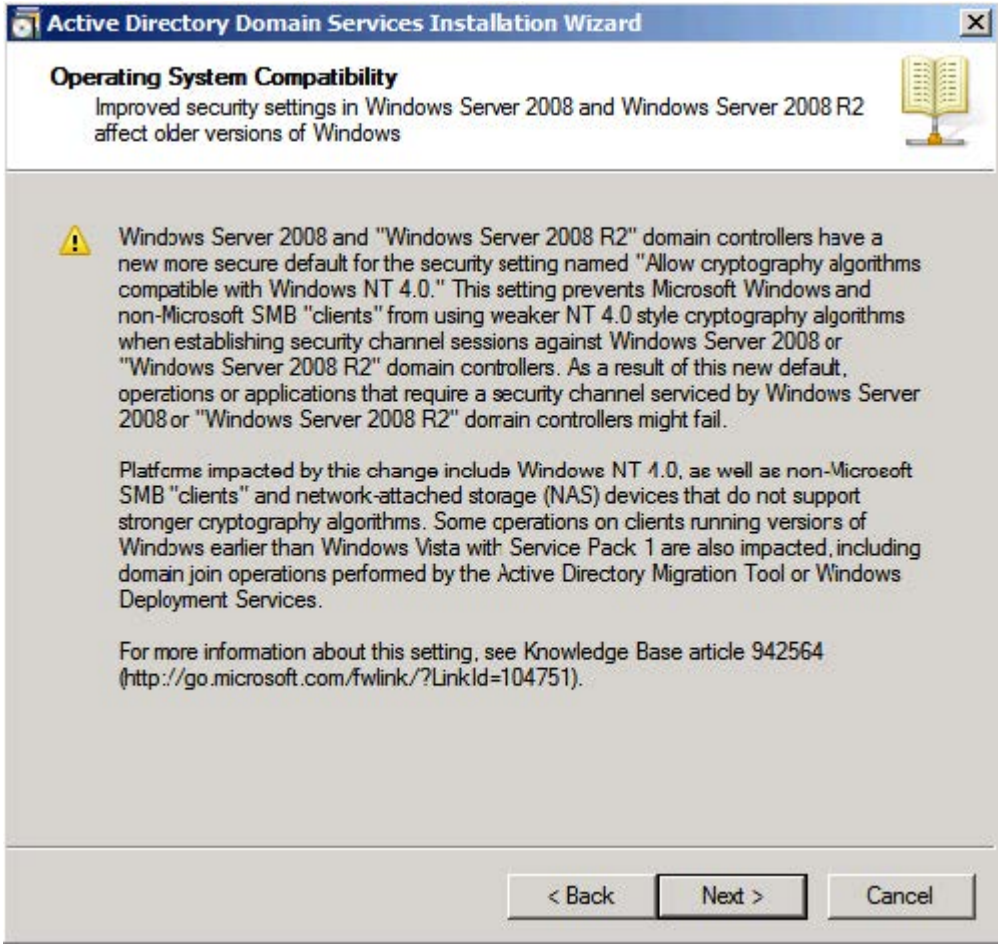
This section shows you how to install an Active Directory on a Microsoft Windows Server 2008 R2 Enterprise 64-bit system.

To install the Microsoft Active Directory Domain Services:

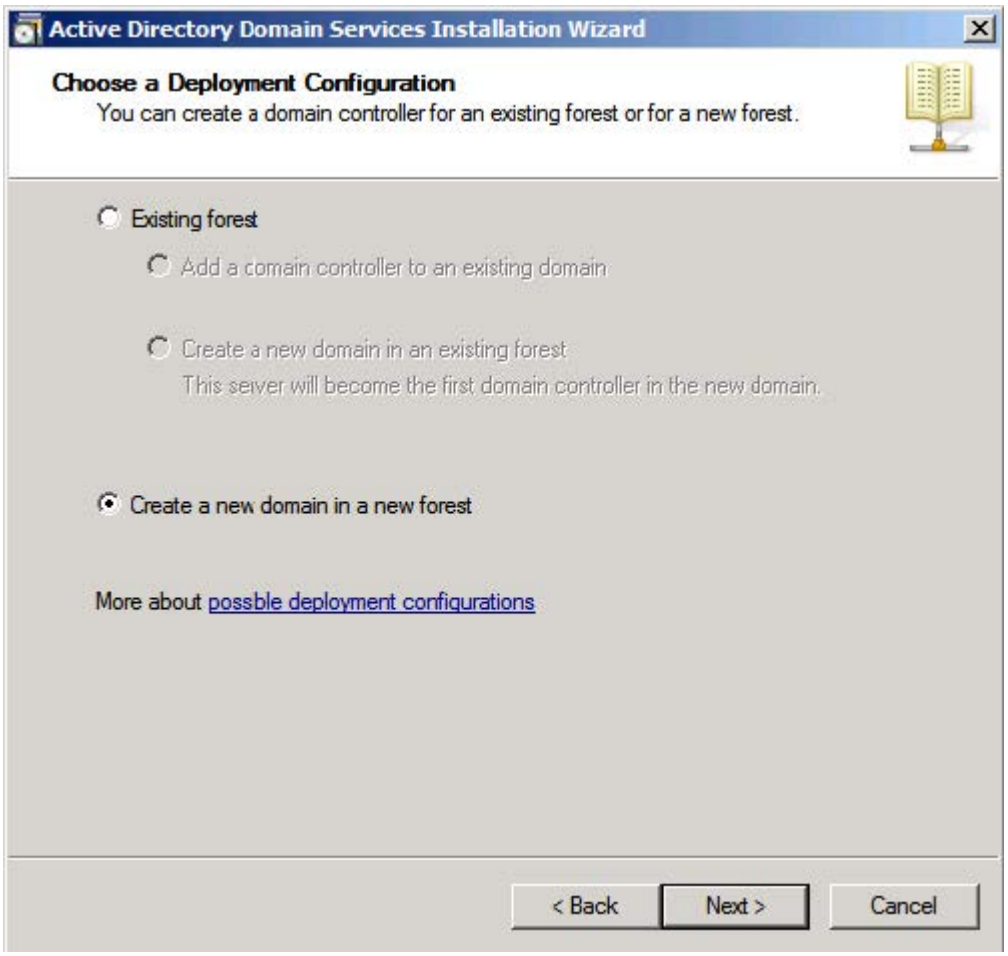
1. Click **Start** > **Run**.
2. Enter **dcpromo** in the dialog and click **OK**.
3. The Active Directory Domain Services Installation Wizard will appear after a short while. Click **Next**.



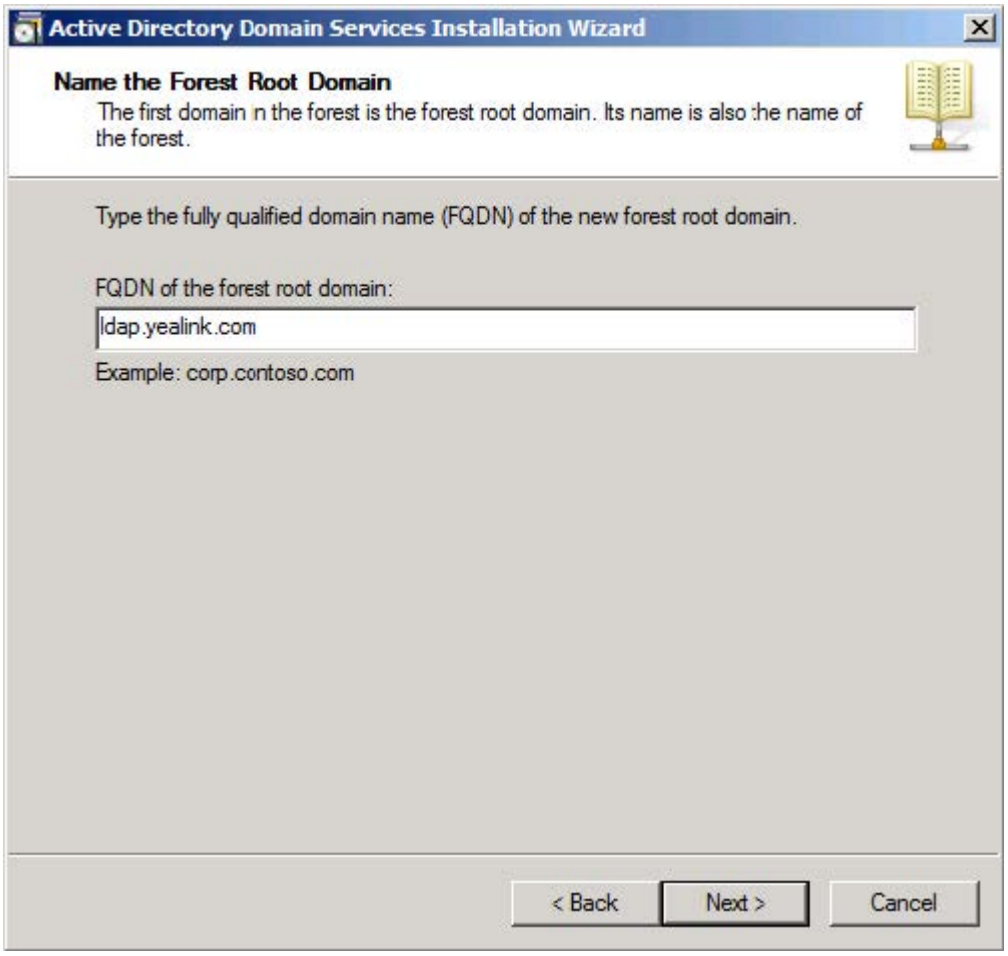
4. Read the provided information and click **Next**.



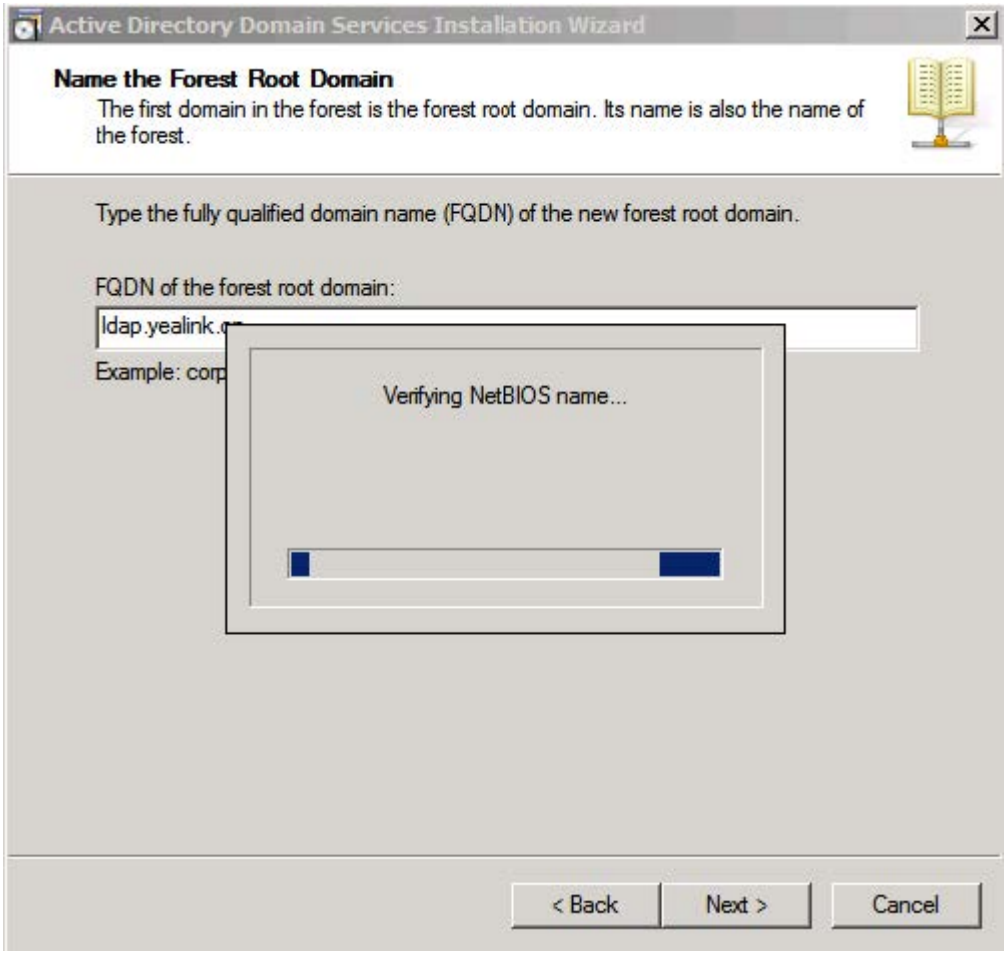
5. Select the **Create a new domain in a new forest** check box and click **Next**.



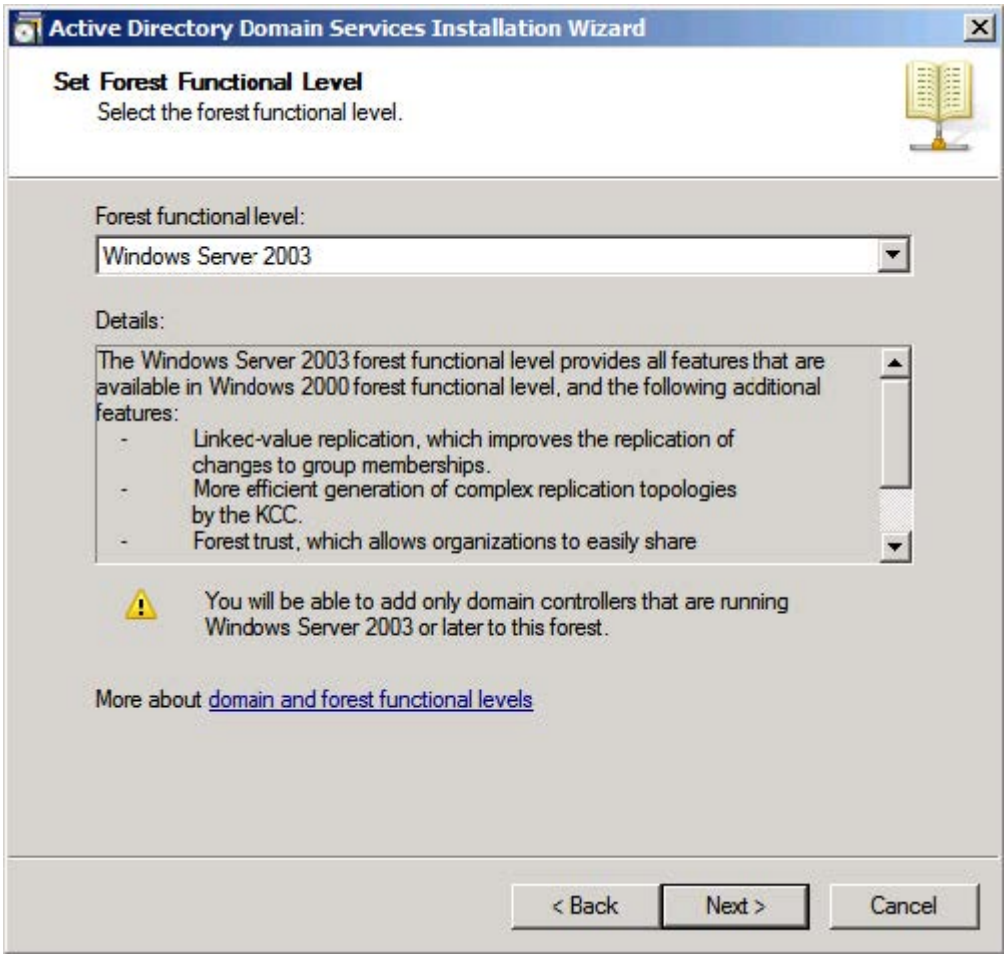
6. Enter an appropriate domain name for the forest root domain and click **Next**.



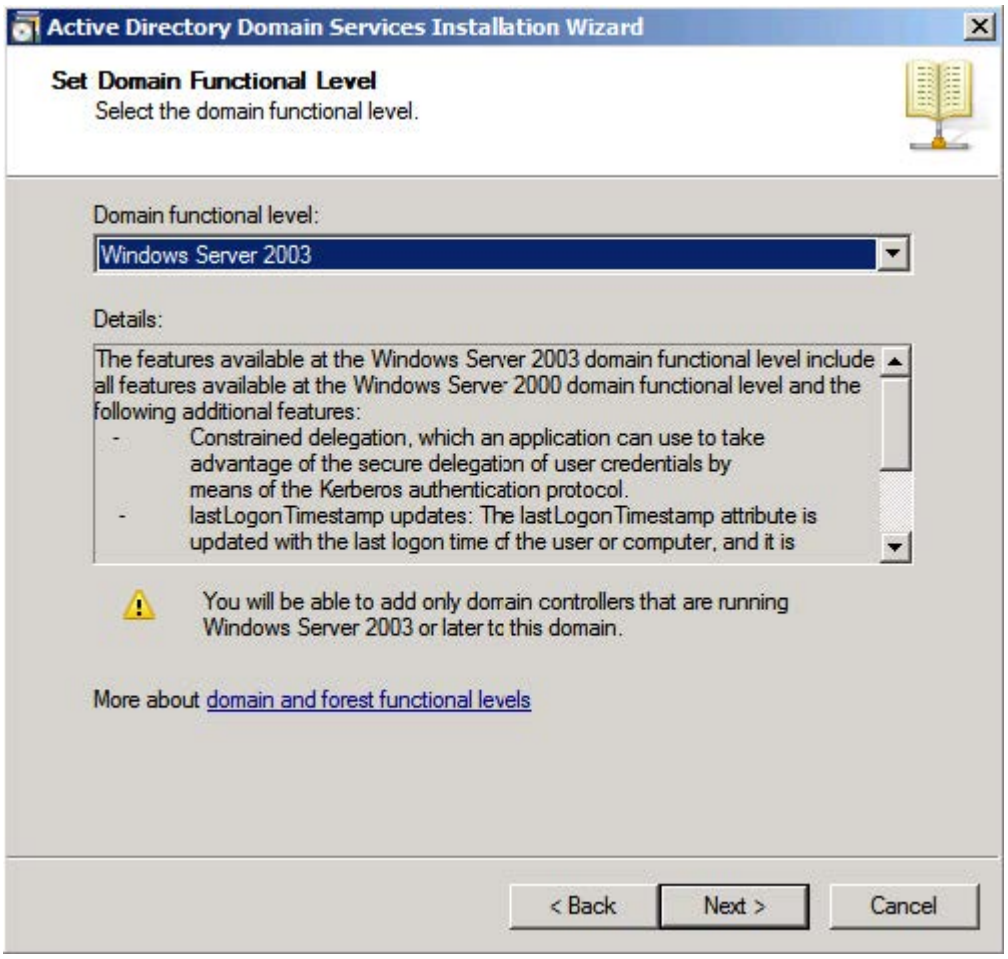
8. The wizard will check if the domain name is in use on the local network.



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

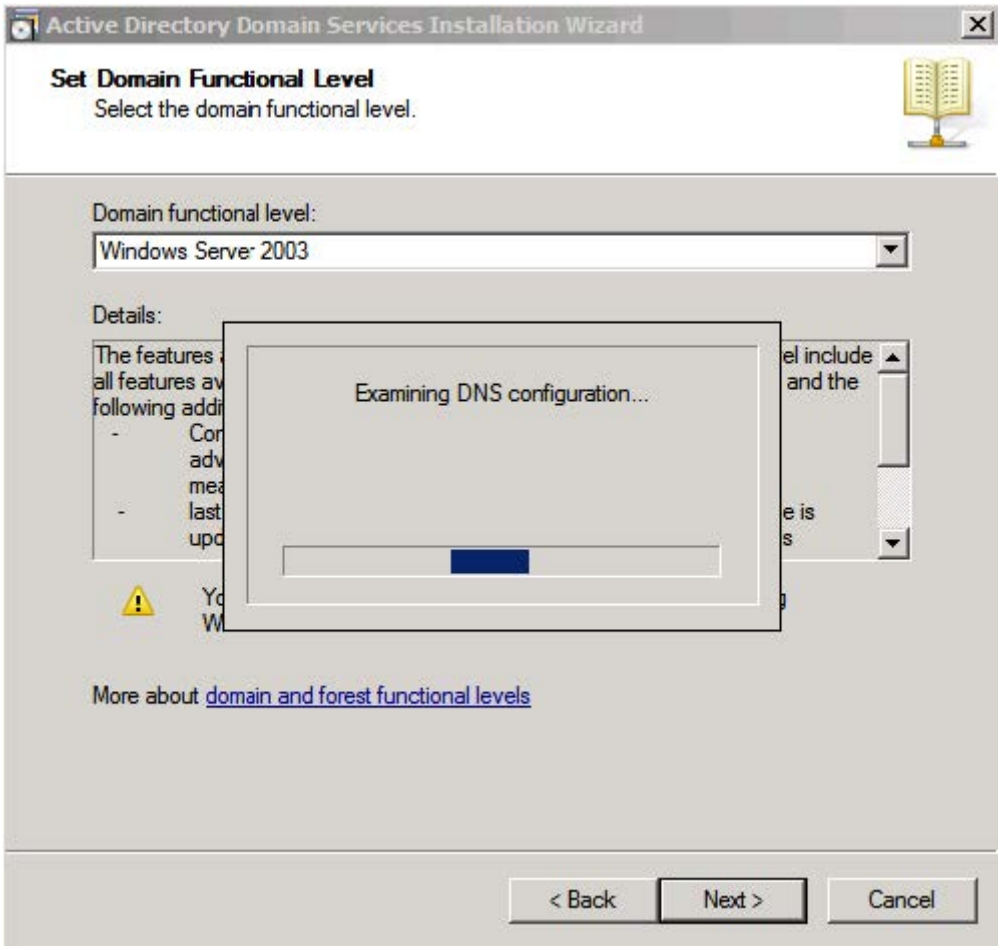


8. Select the desired domain functional level from the **Domain functional level** drop-down menu, and click **Next**.
9. For more information, click the **domain and forest functional levels**.

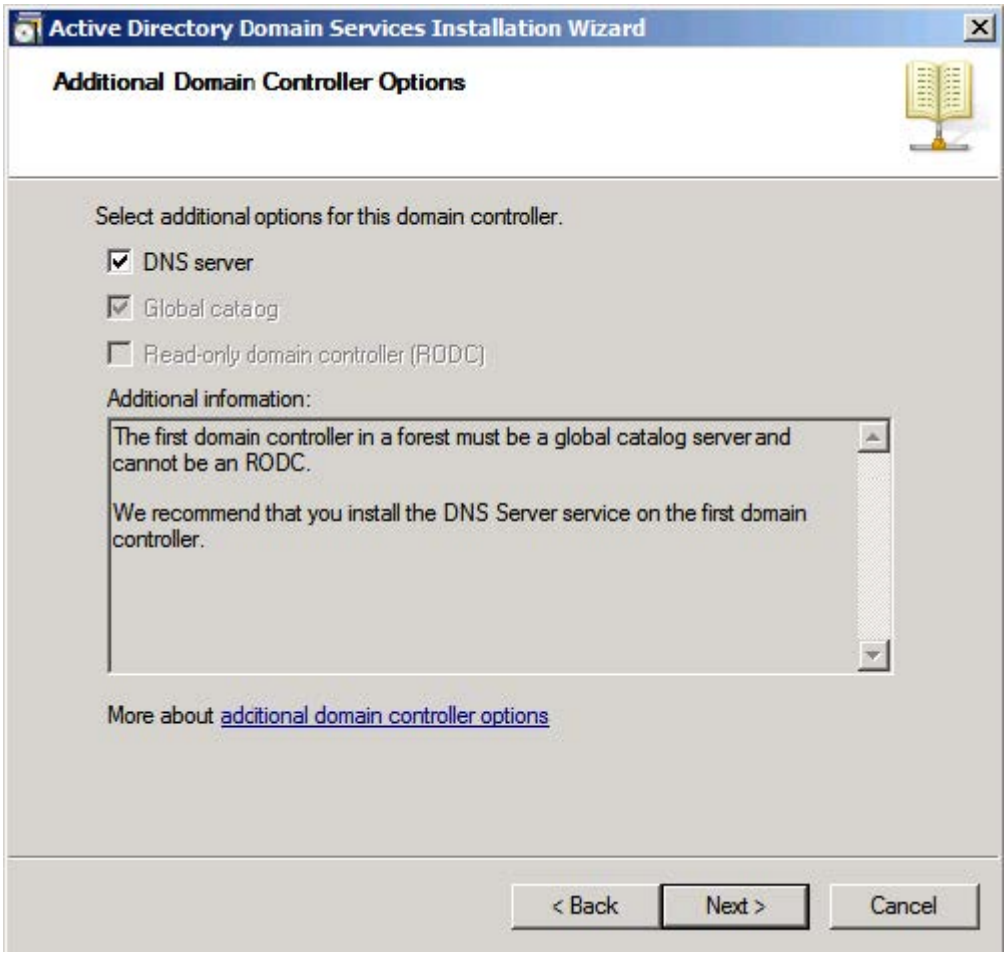


If you select **Windows Server 2008 R2** for the forest functional level, you will not be prompted to select a domain functional level.

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

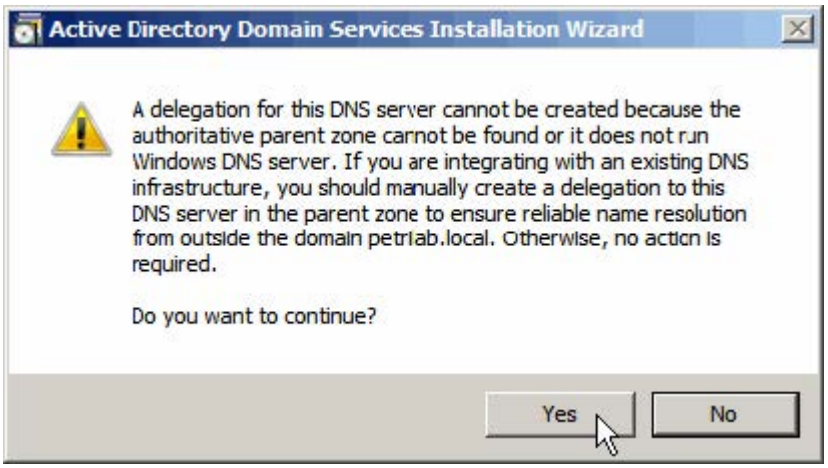


9. Select additional options for this domain controller if required, and click **Next**.

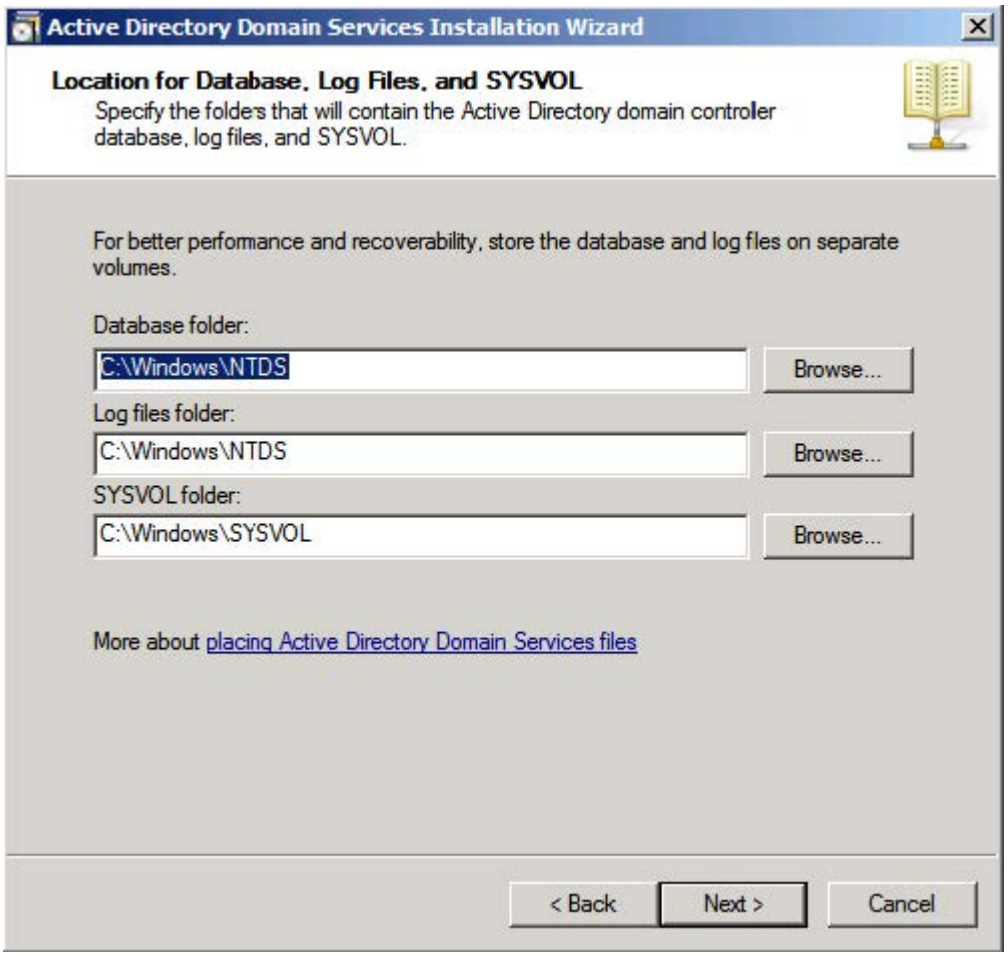


You may get a warning telling you that the server has one or more dynamic IP addresses. We recommend assigning a static IP address to the server.

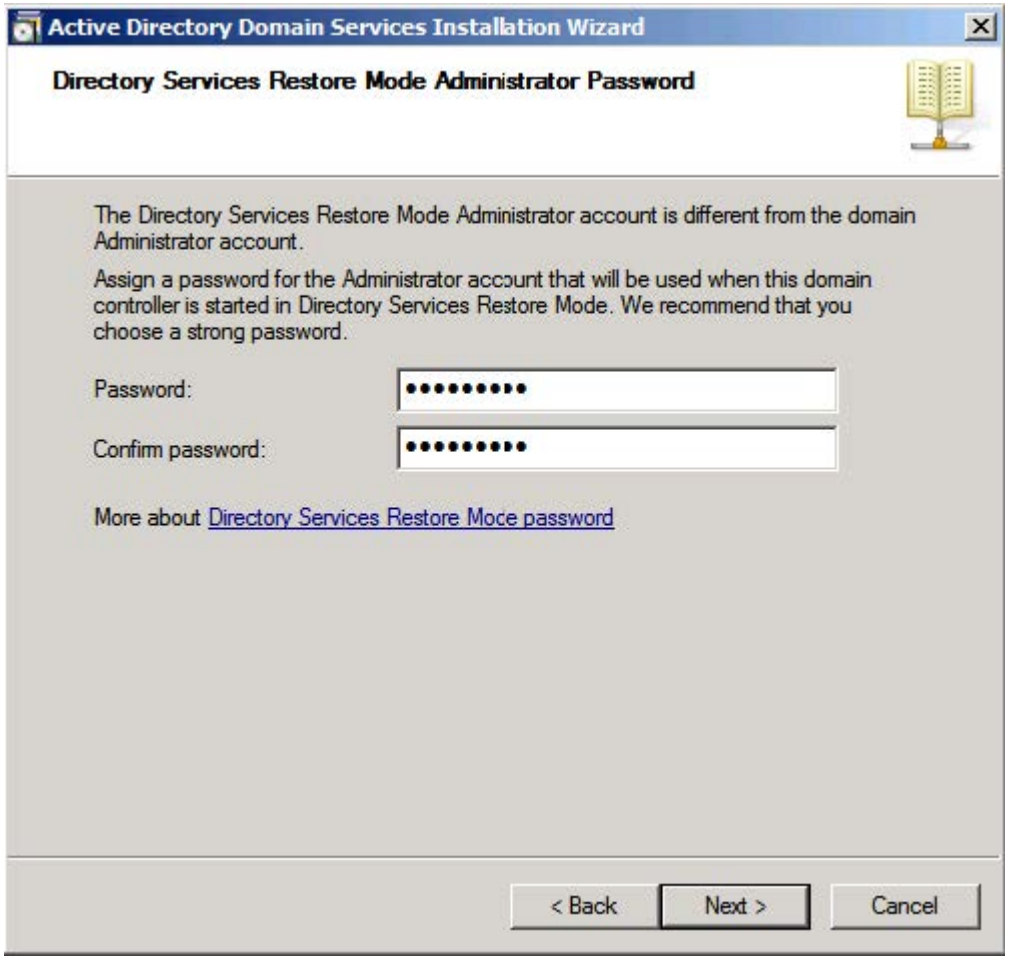
10. The wizard will prompt a warning about DNS delegation. Since no DNS has been configured yet, you can ignore the message and click **Yes**.



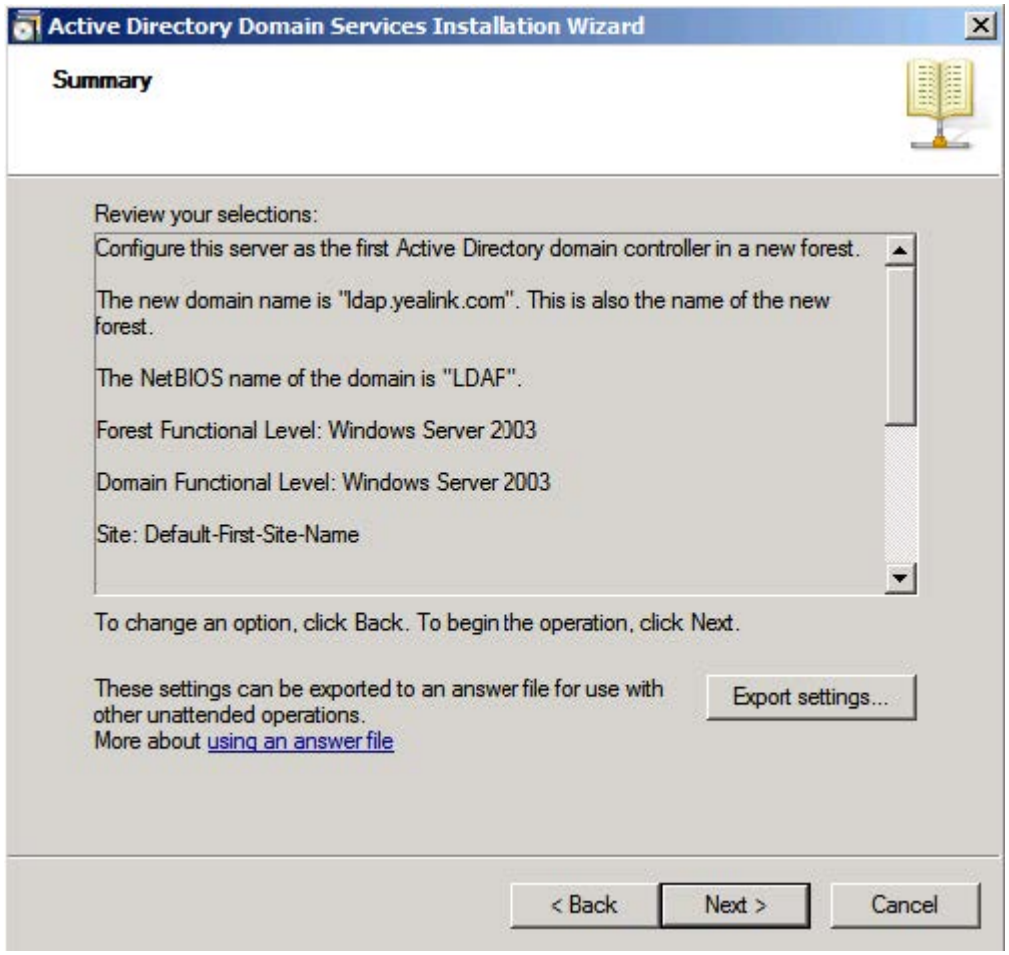
11. Specify the desired paths for the database, log files, and SYSVOL folders, and click **Next**.
12. For more information, click **placing Active Directory Domain Services files**.



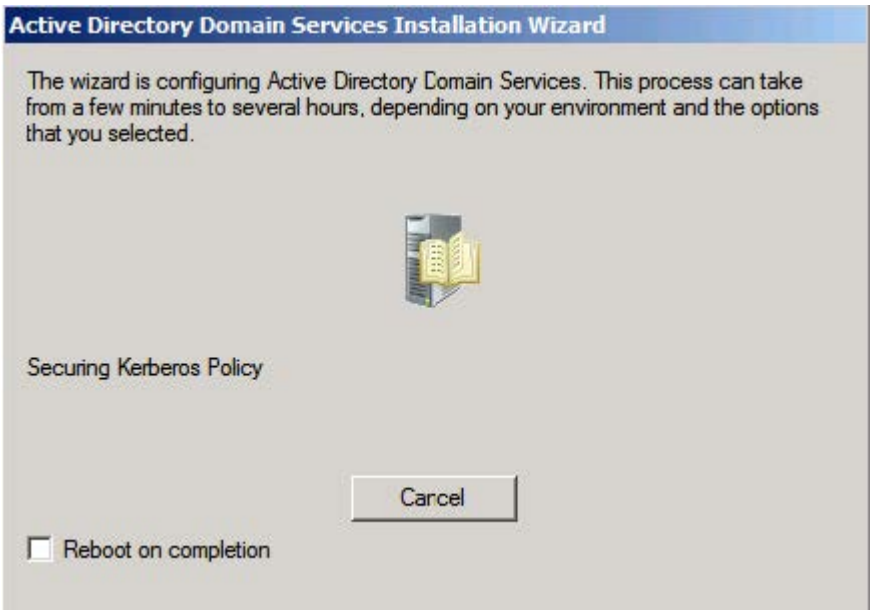
12. Configure the password for the Active Directory recovery mode, and click **Next**.
    For more information, click **Directory Services Restore Mode password**.
    The password should be complex and at least 7 characters long.



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

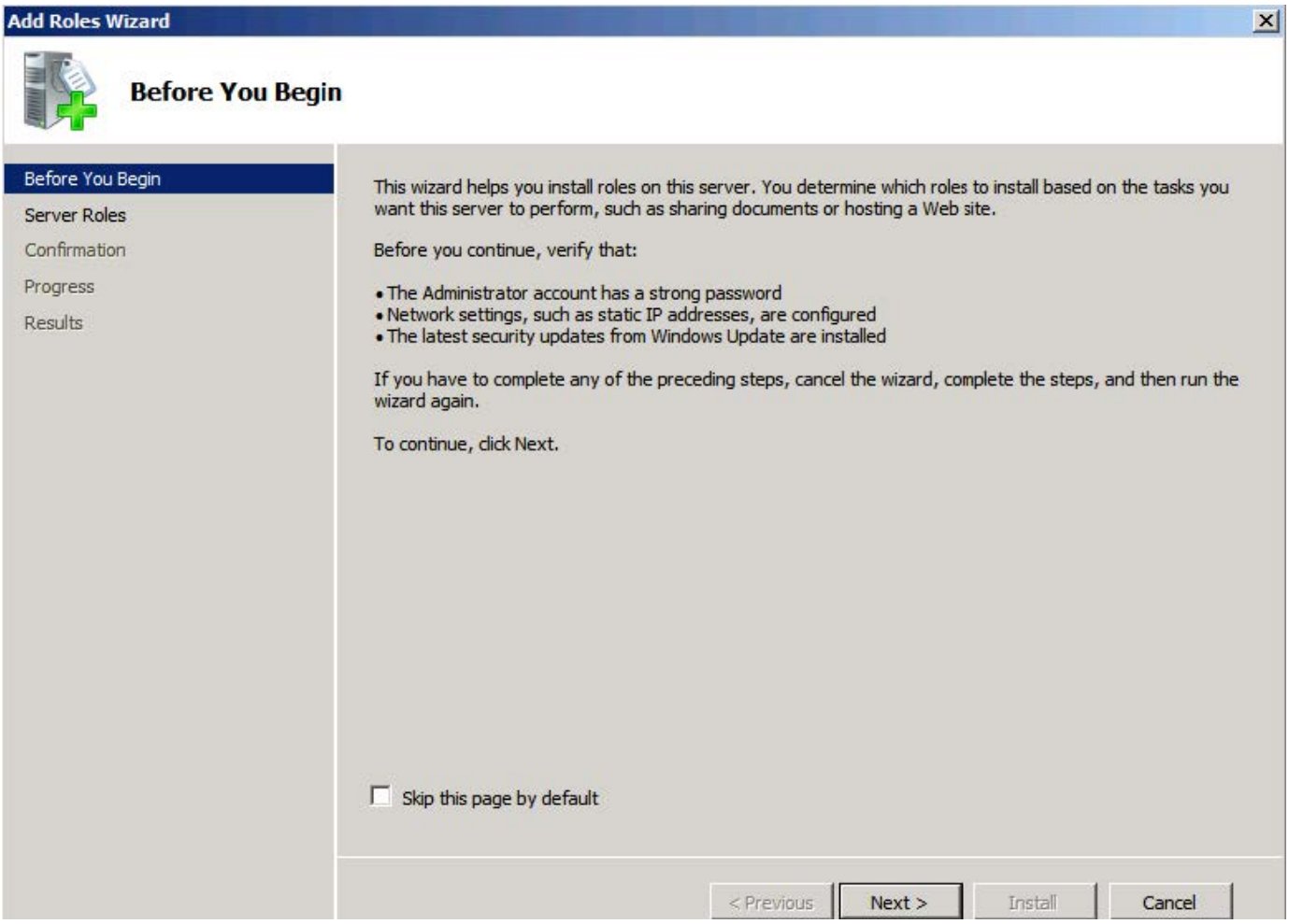
You should also install the Active Directory Lightweight Directory Services role on the Windows Server 2008 system.

To install the Active Directory Lightweight Directory Services role:

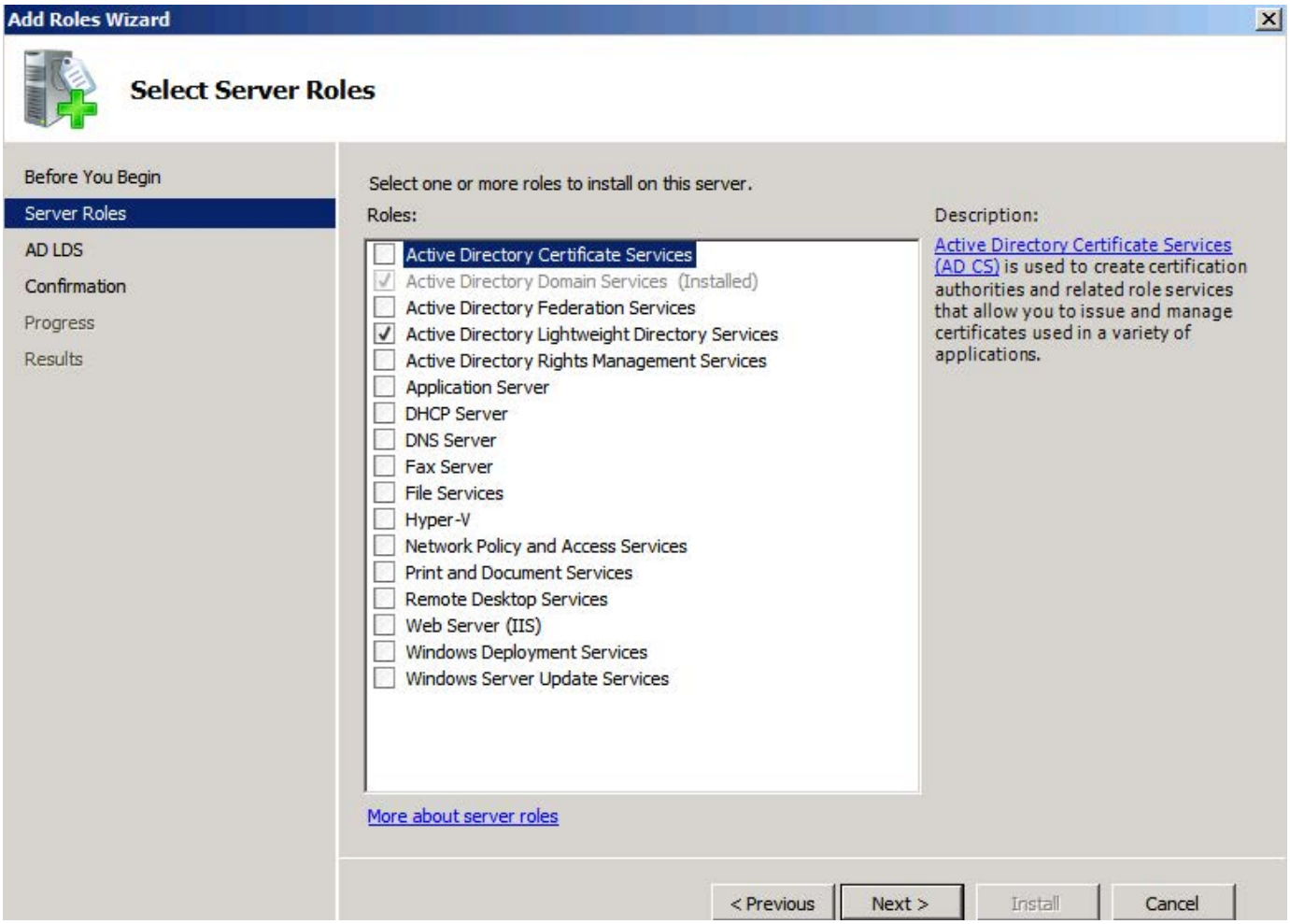
1. Click **Start** > **Administrative Tools** > **Server Manager**.

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

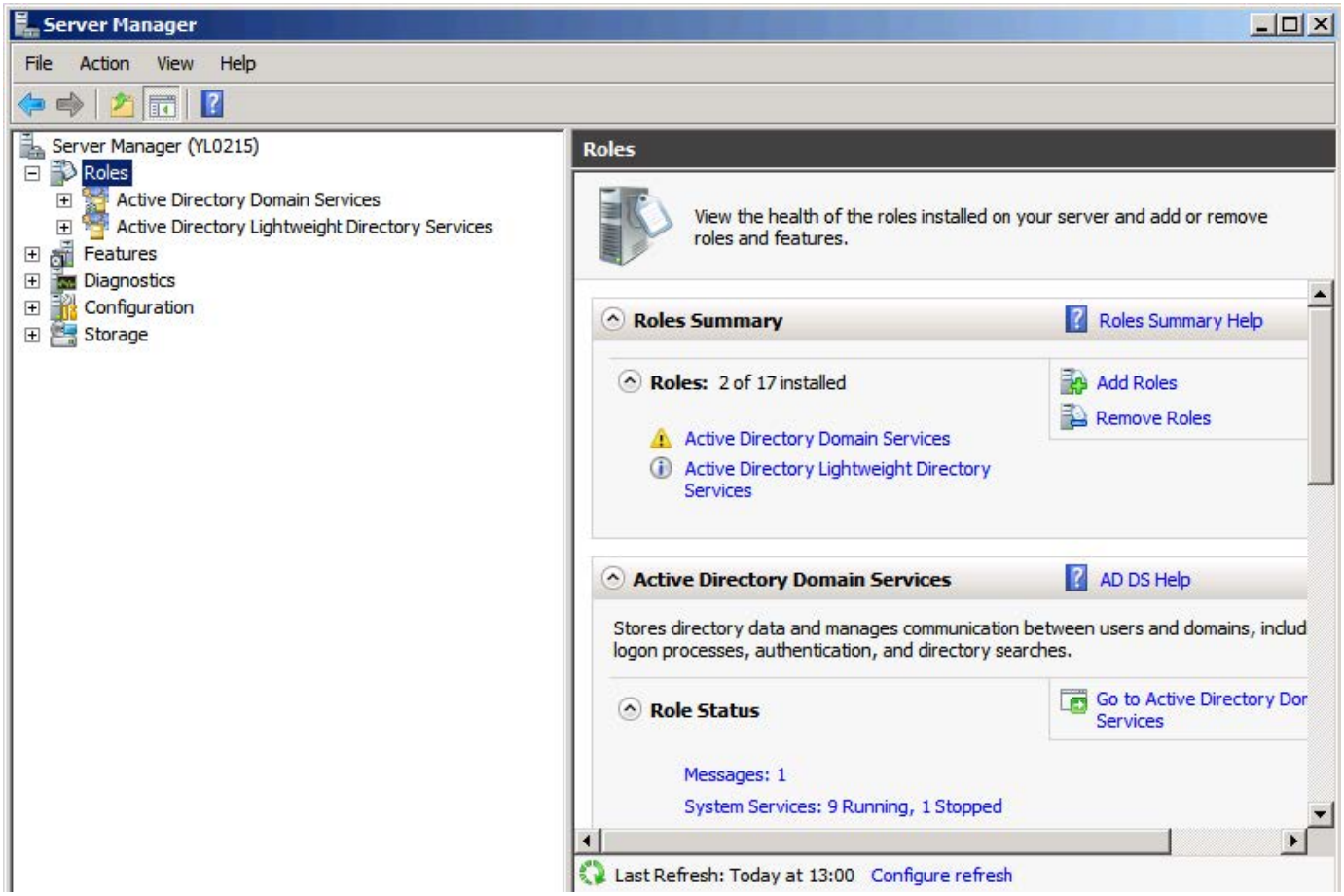
3. The Add Roles Wizard will pop up, click **Next**.



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.



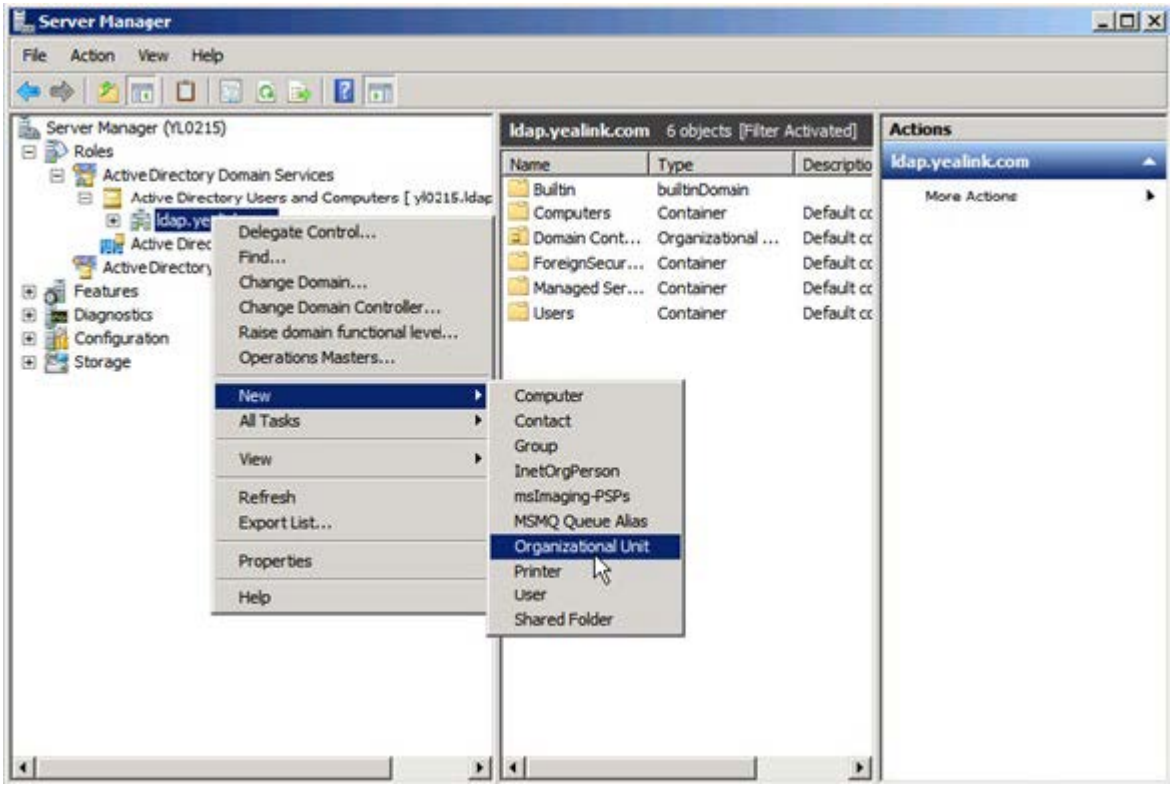
Configure the Microsoft Active Directory Server

Add an Entry to the Active Directory

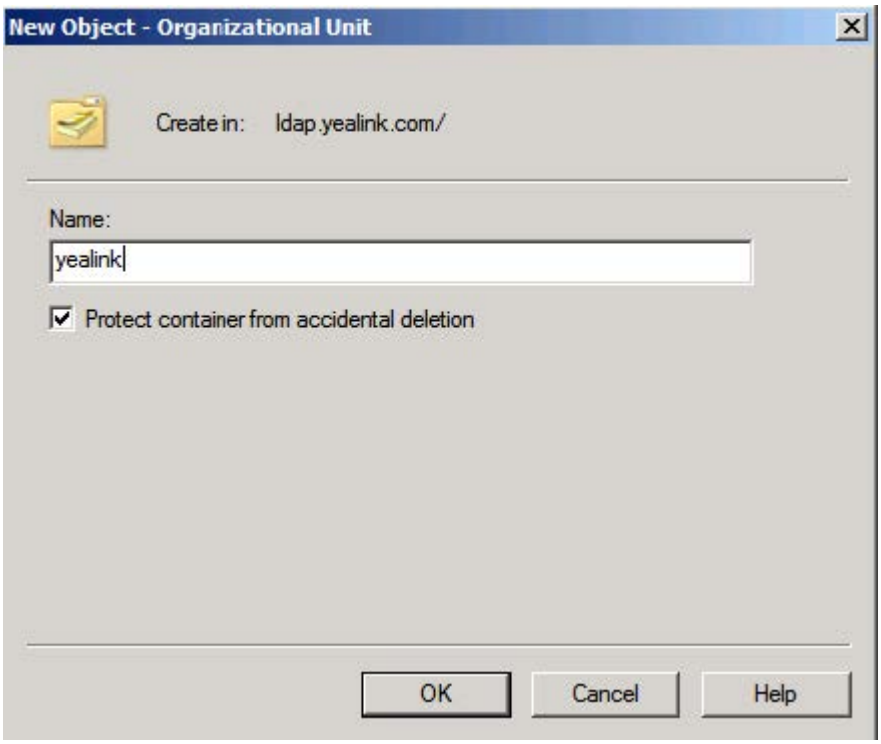
You can add entries to the active directory one by one in this way.

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**.

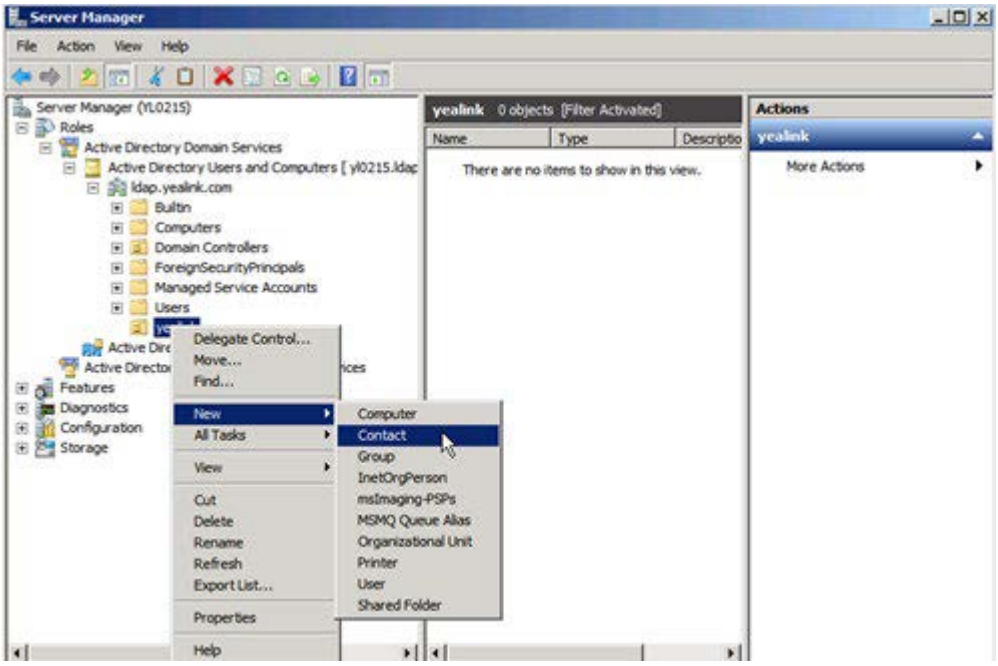


4. Enter the desired name of the organizational unit.

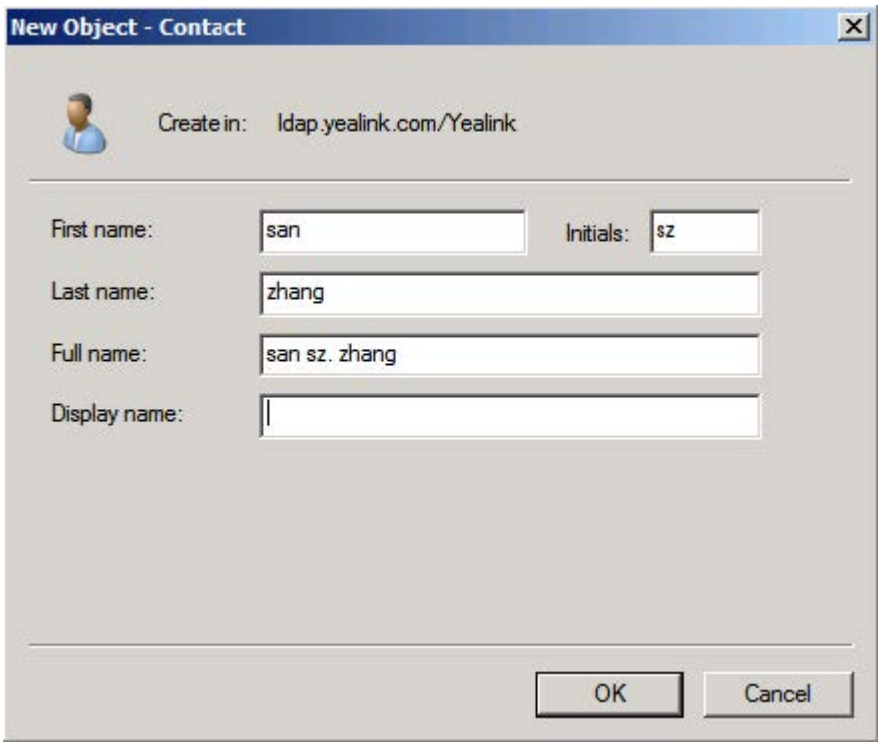


5. Click **OK** to accept the change.

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



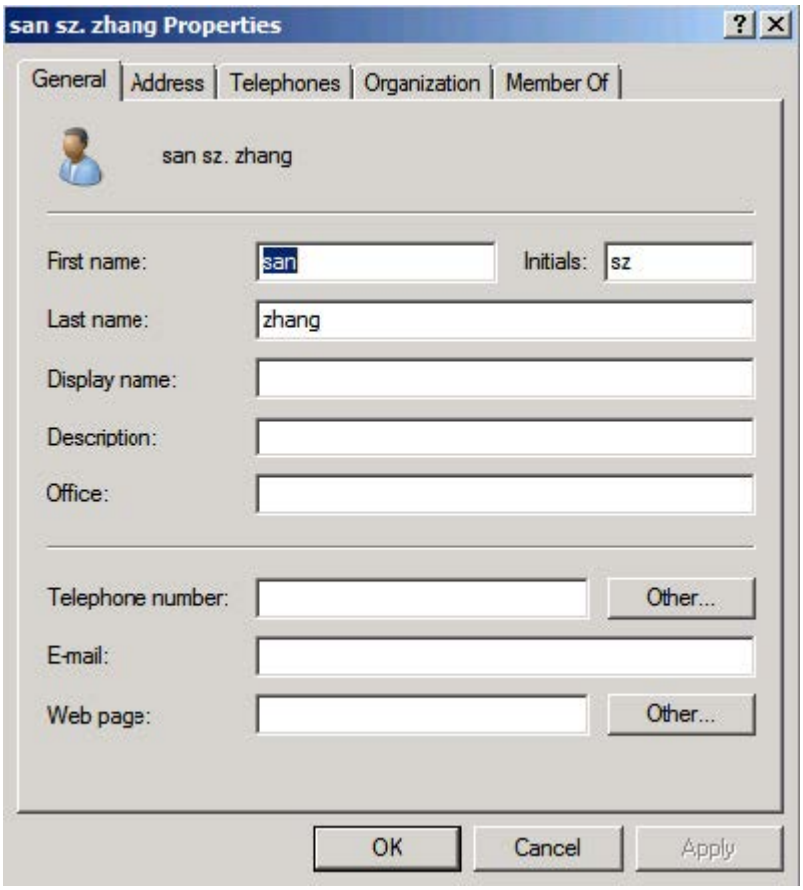
7. Enter the desired values in the corresponding fields.



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:

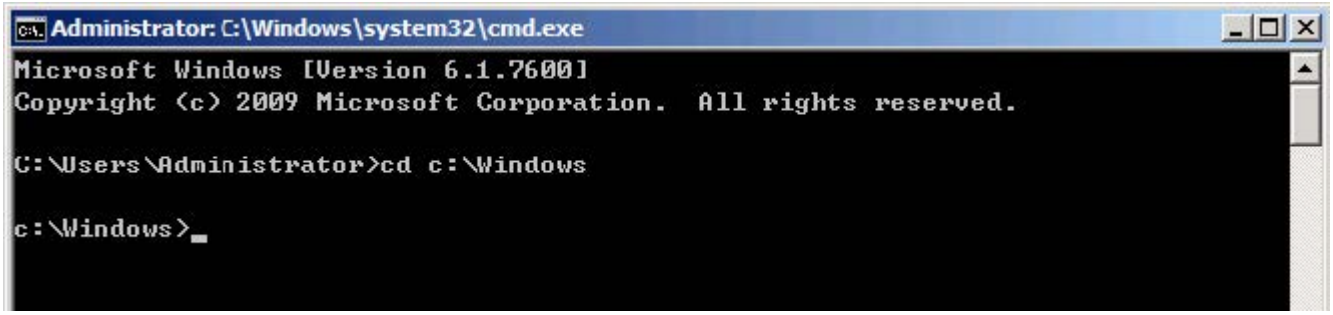
Create a new text document and then modify the filename extension to ldif. For example, create a text document named as test.txt, right-click the test.txt document and then select to rename it, modify the filename extension as ldif. Open the LDIF file with your favorite text editor and input the corresponding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

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

##create a new contact##
dn: CN=san zhang,OU=yealink,DC=ldap,DC=yealink,DC=com
```

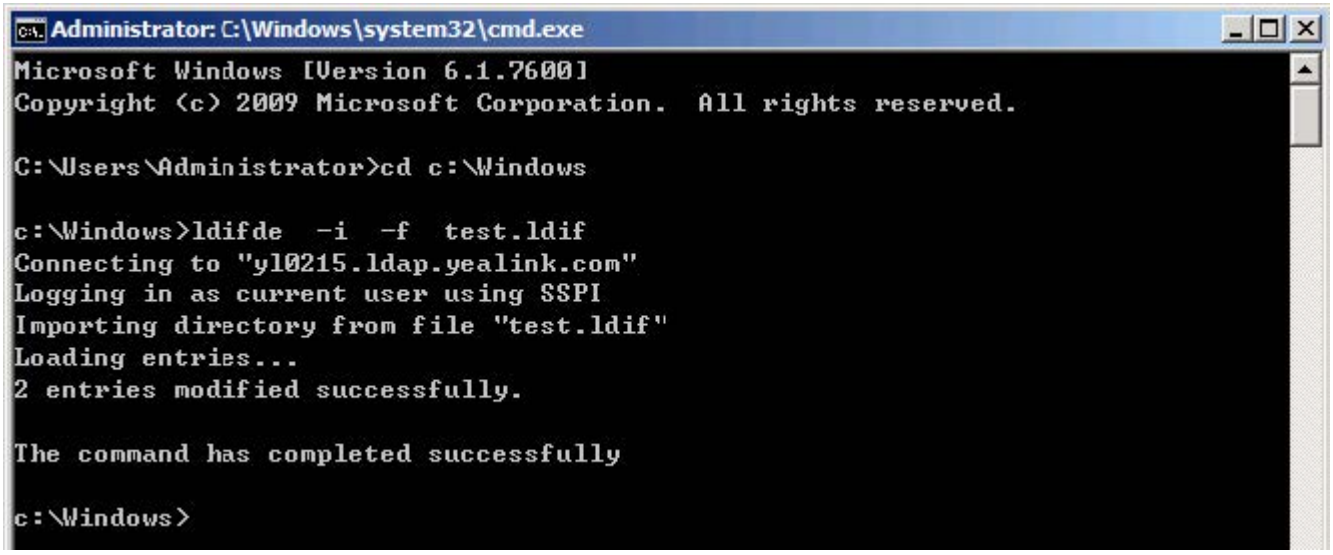
```
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: contact
cn: san zhang
sn: zhang
givenName: san
initials: zs
name: san zhang
ipPhone: 2336
mobile: 15557107369
```

To import the test.ldif file:

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



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



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 *

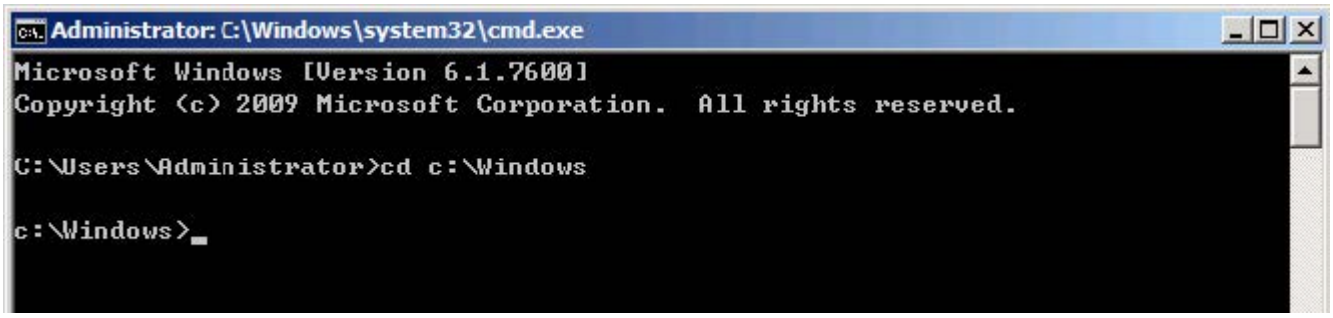
	A	B	C	D	E	F	G	H	I	J
1	DN	objectClass	ou	name	cn	sn	givenName	initials	ipPhone	mobile
2	OU=yealink,DC=ldap,DC=yealink,DC=com	organizationalUnit	yealink	yealink						
3	CN=san zhang,OU=yealink,DC=ldap,DC=yealink,DC=com	contact		san zhang	san zhang	san	zhang	sz	1111	123456789001
4	CN=si li,OU=yealink,DC=ldap,DC=yealink,DC=co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

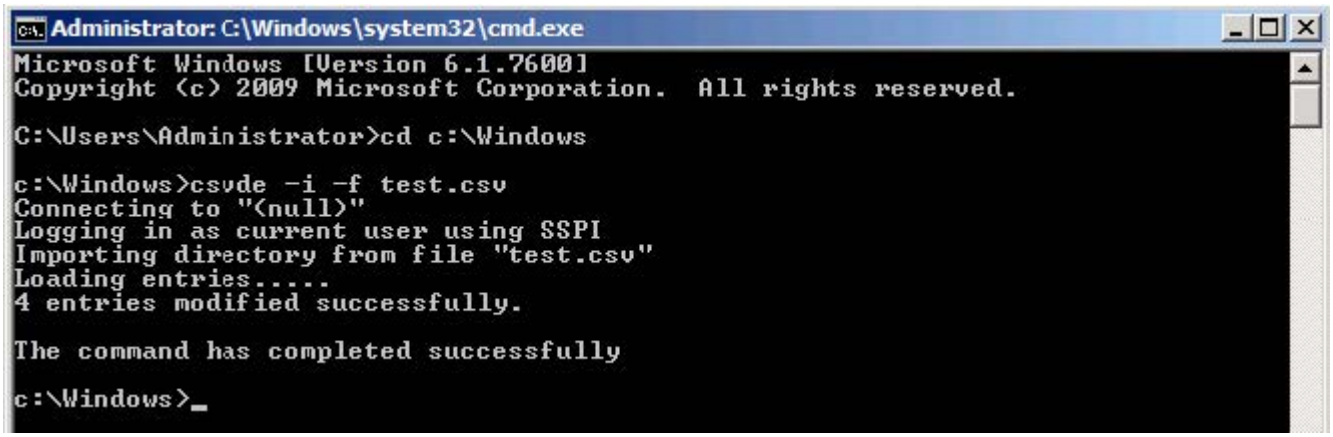
To import the test.csv file:

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 below:



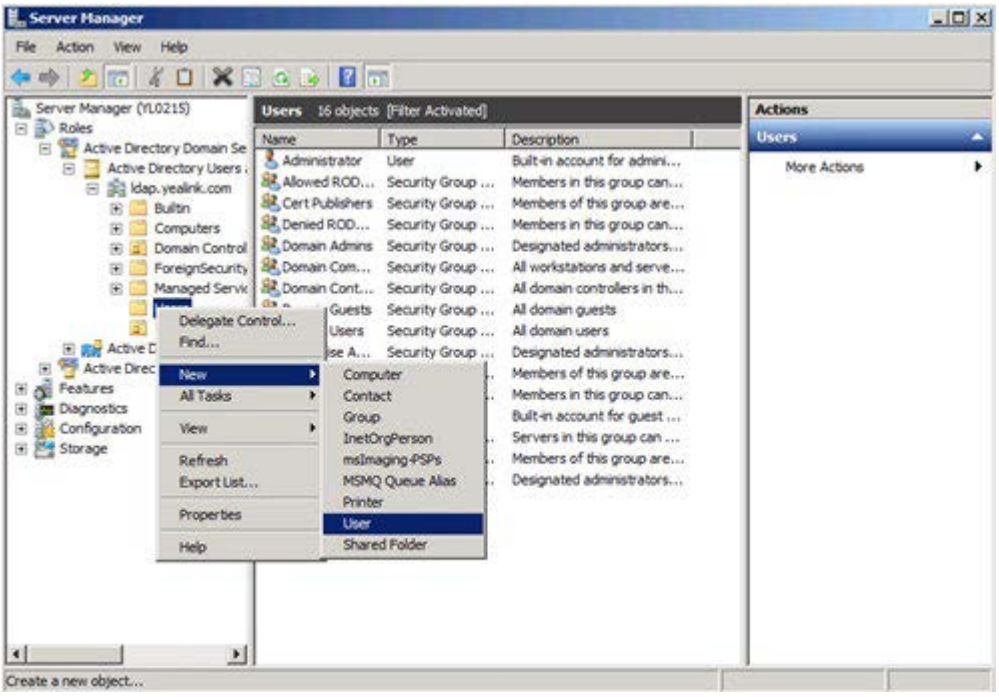
- The csvde tool cannot edit or delete the existing entries on the Active Directory.
- You can also export the existing entries on the active directory into a *.csv file first, modify the file, and then import the modified file into the active directory. For more information, refer to the network resource.

Create User Accounts

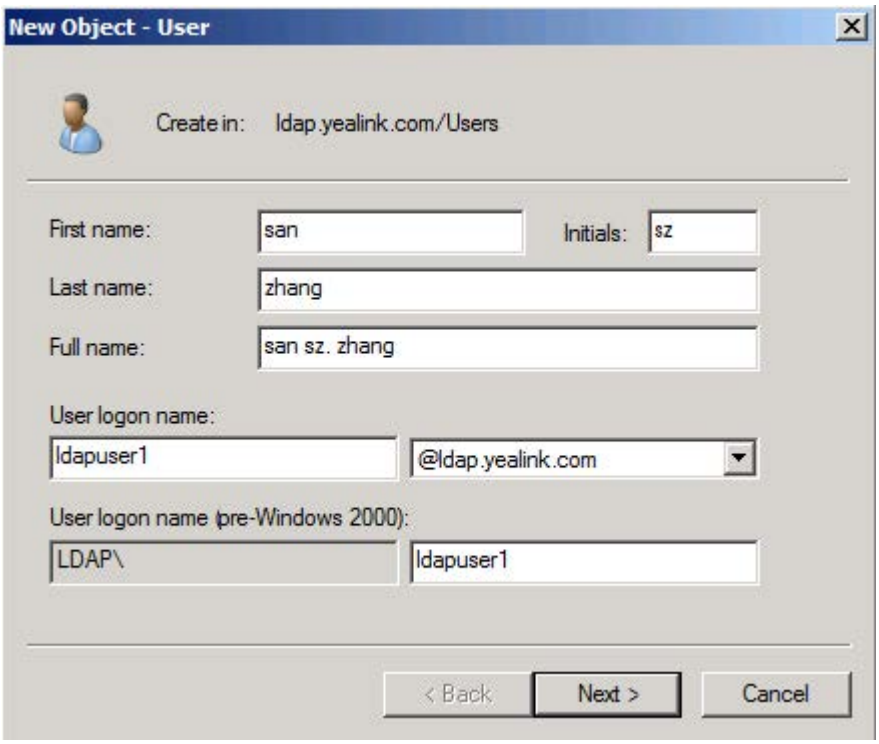
You can create user accounts to allow access to resources on the Active Directory. User accounts are very important and useful.

To create a user account:

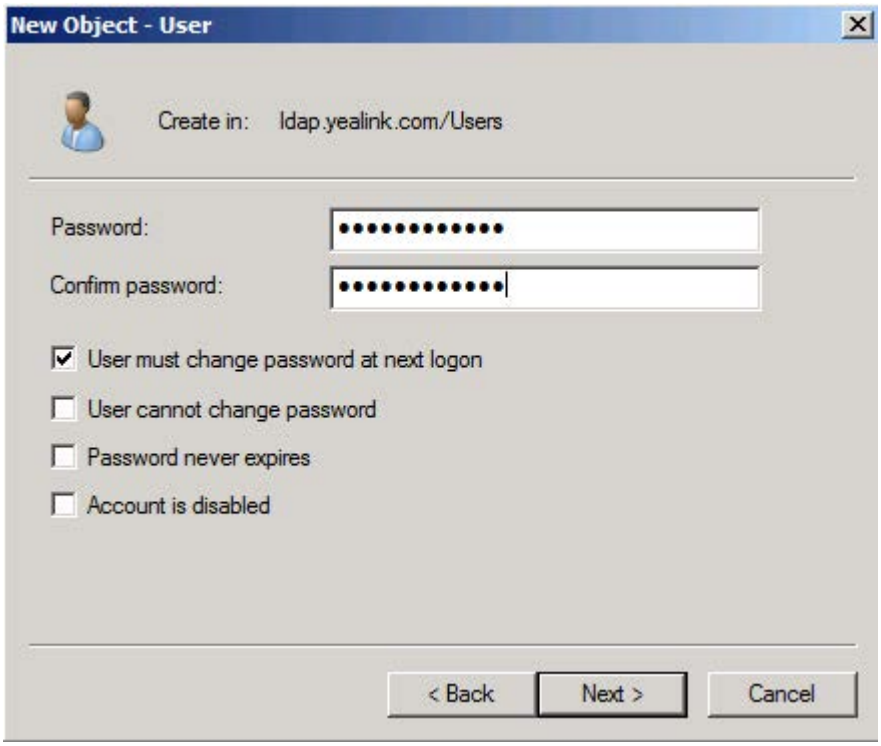
1. Click **Start** > **Administrative Tools** > **Server Manager**.
2. Double-click **Server Manager** > **Roles** > **Active Directory Domain Services** > **Active Directory Users and Computers**.
3. Select the domain name created above (e.g., ldap.yealink.com).
4. Right-click **Users**, and then select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



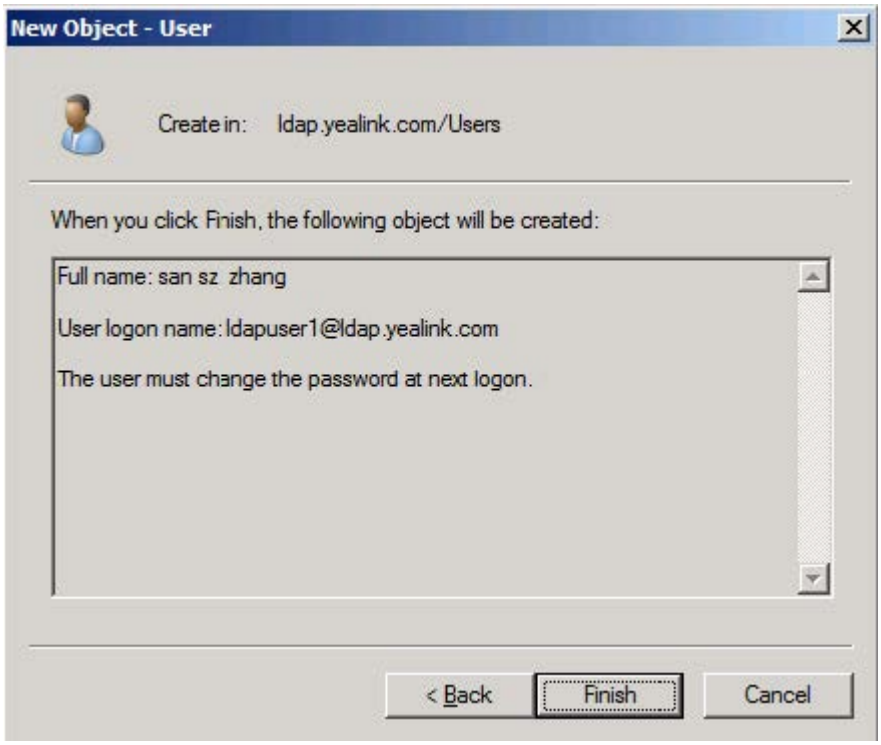
5. Enter desired values in the corresponding fields and click **Next**.



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.

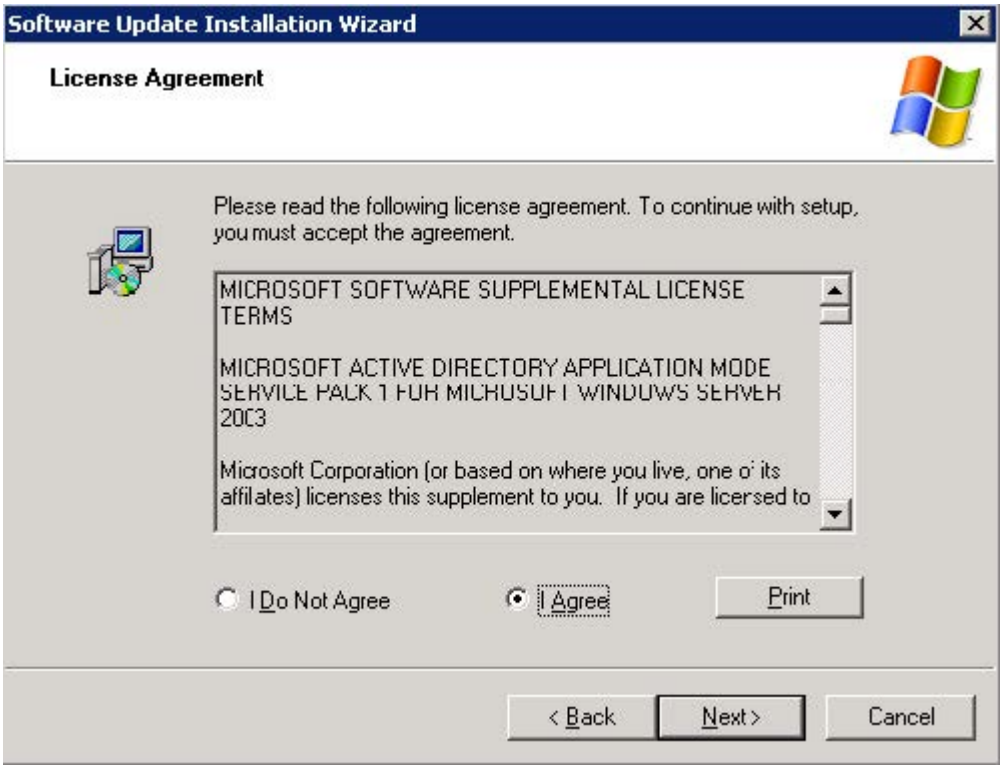
Install the Active Directory Application Mode

To install the Active Directory Application Mode:

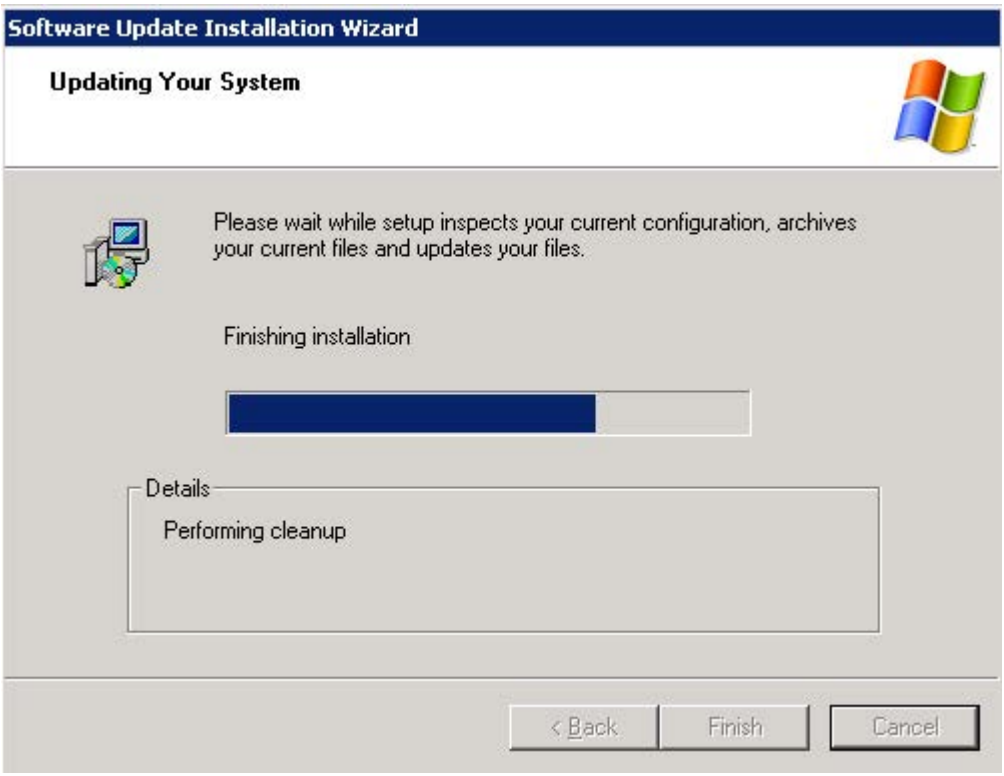
1. Double-click ADAMSP1_x86_English.exe to run the application.
2. The Active Directory Application Mode Service Park 1 Installation Wizard will appear after a short while. Click **Next**.



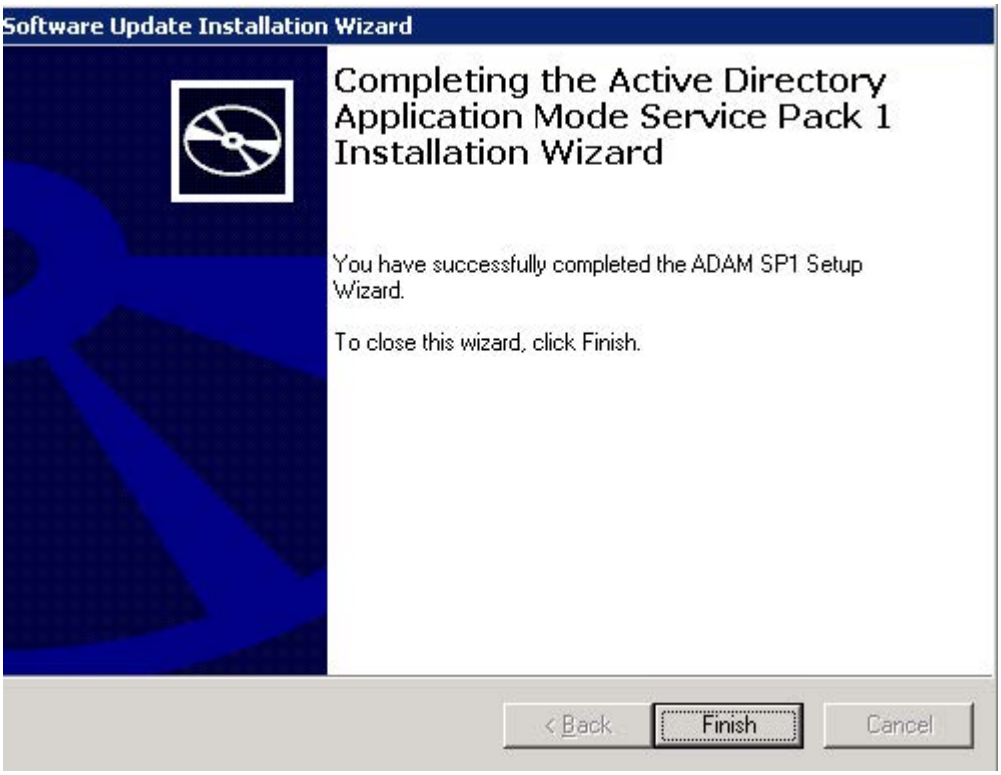
3. Read the software license agreement and select **I Agree** check box. And then click **Next**.



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



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



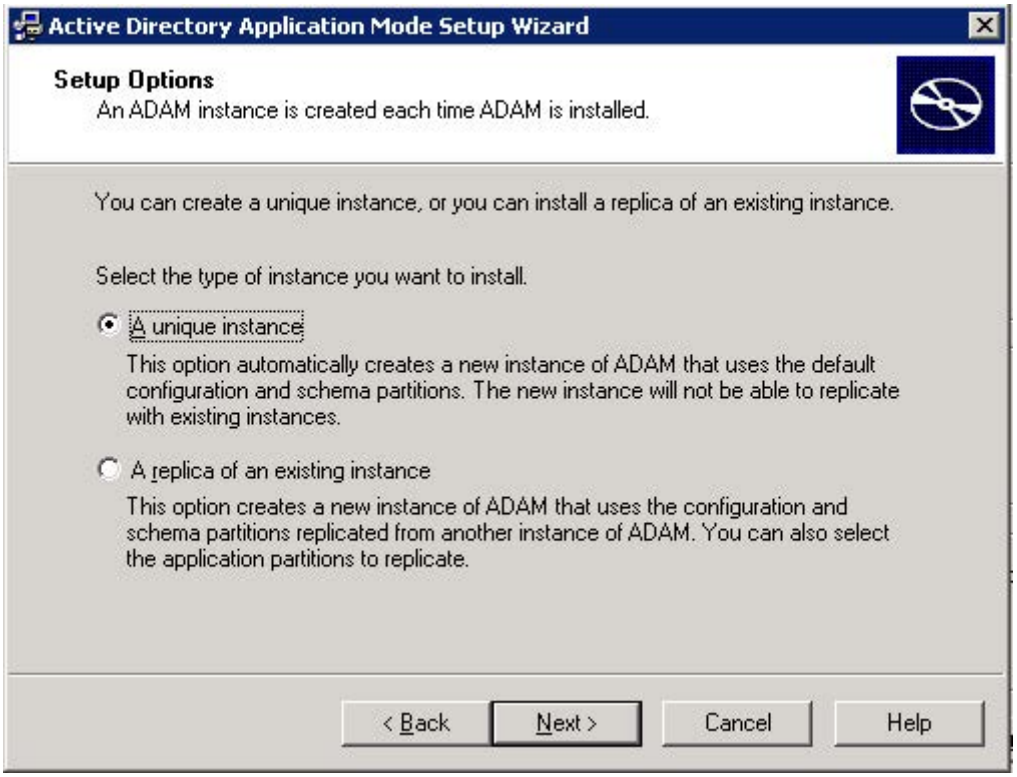
To create an ADAM instance:

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

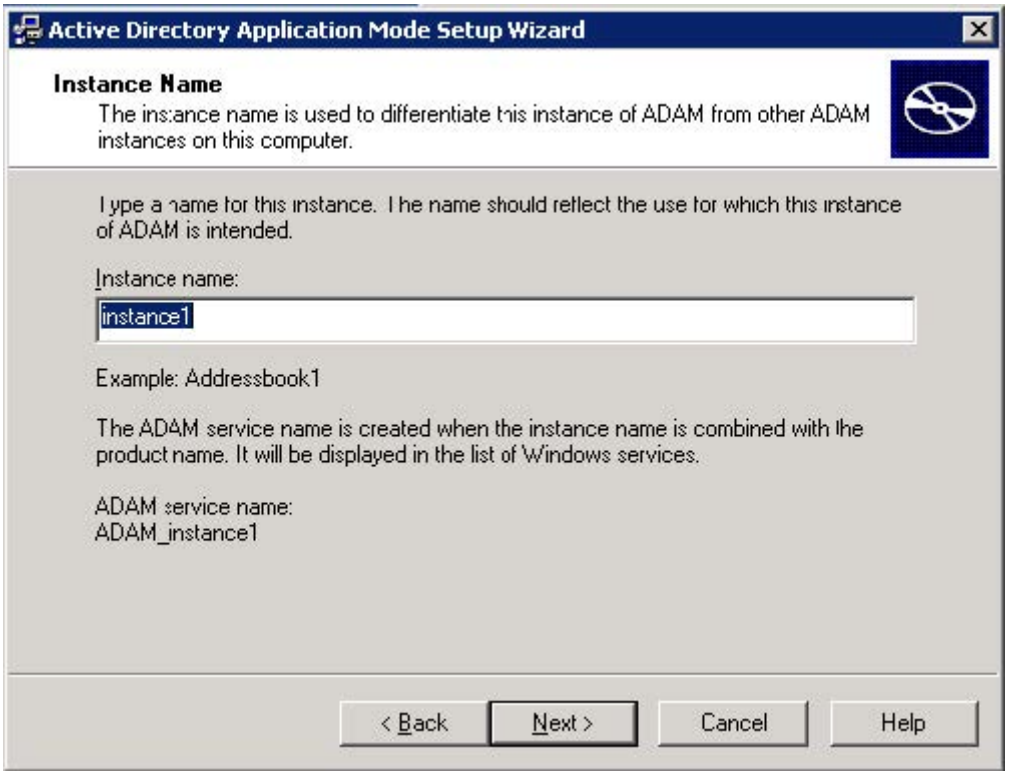
   It will prompt the following interface, and click **Next**.



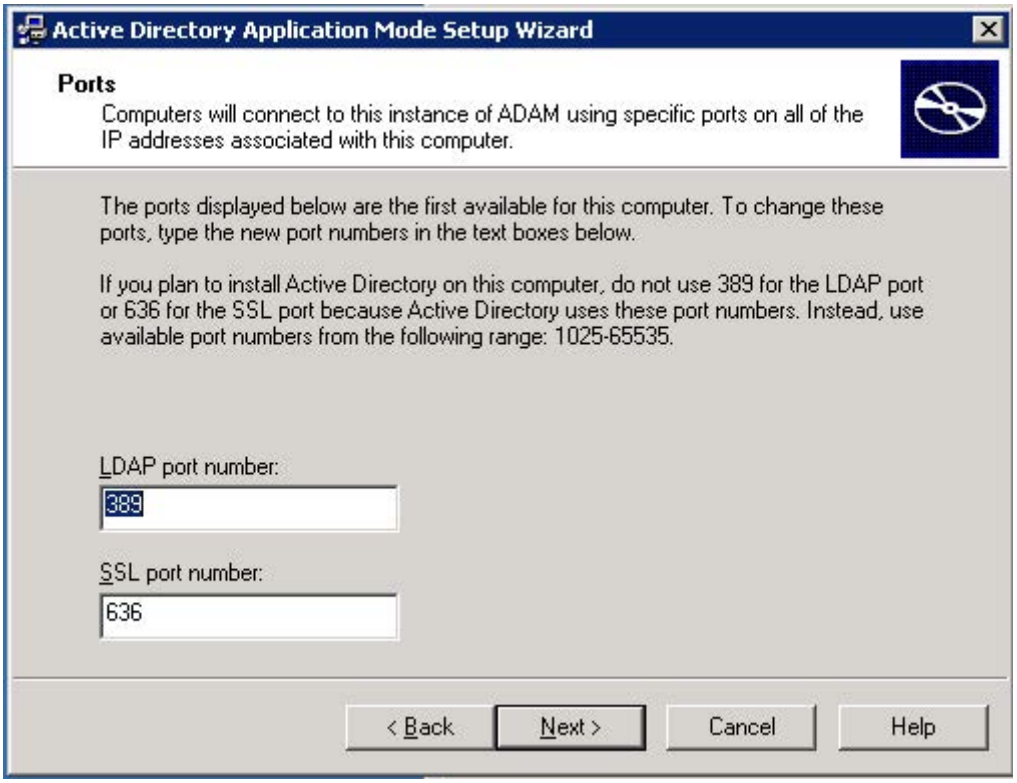
2. Mark the **A unique instance** check box and click **Next**.



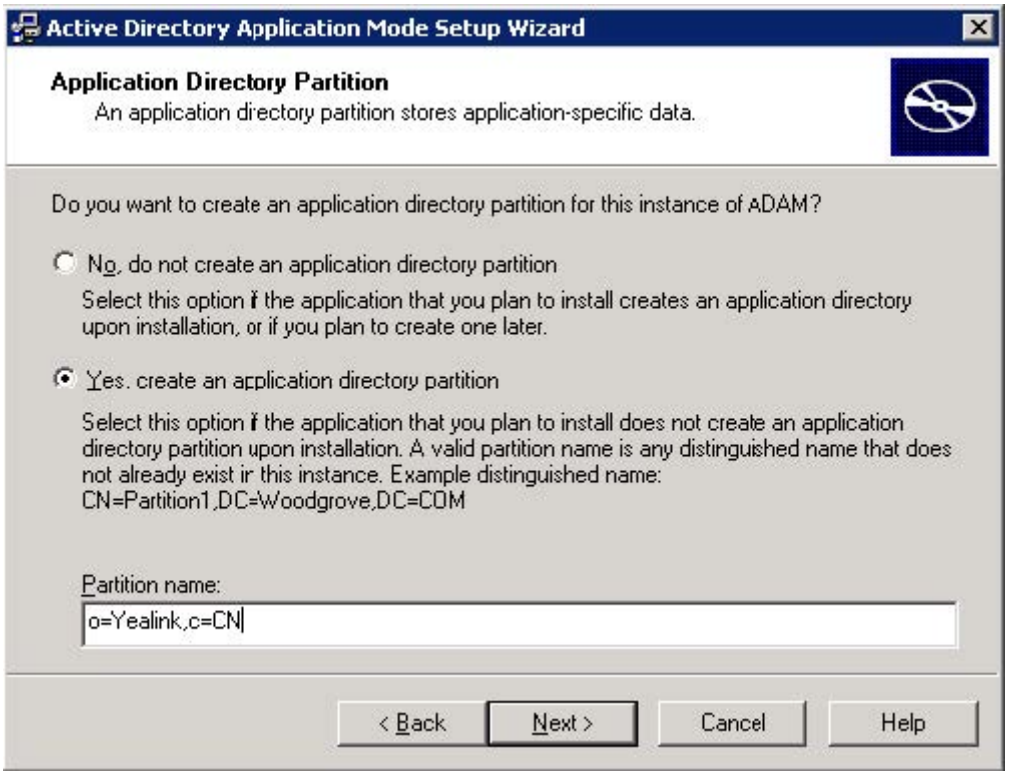
3. Enter the desired name in the **Instance name** field and click **Next**.



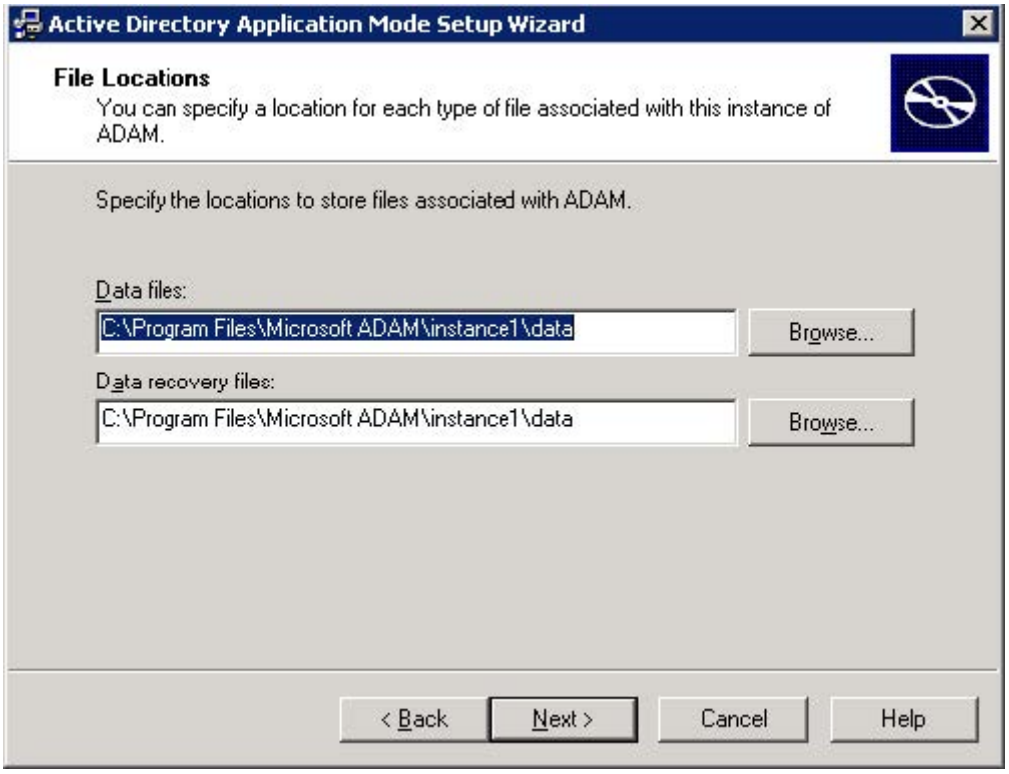
4. Keep the default ports and click **Next**.



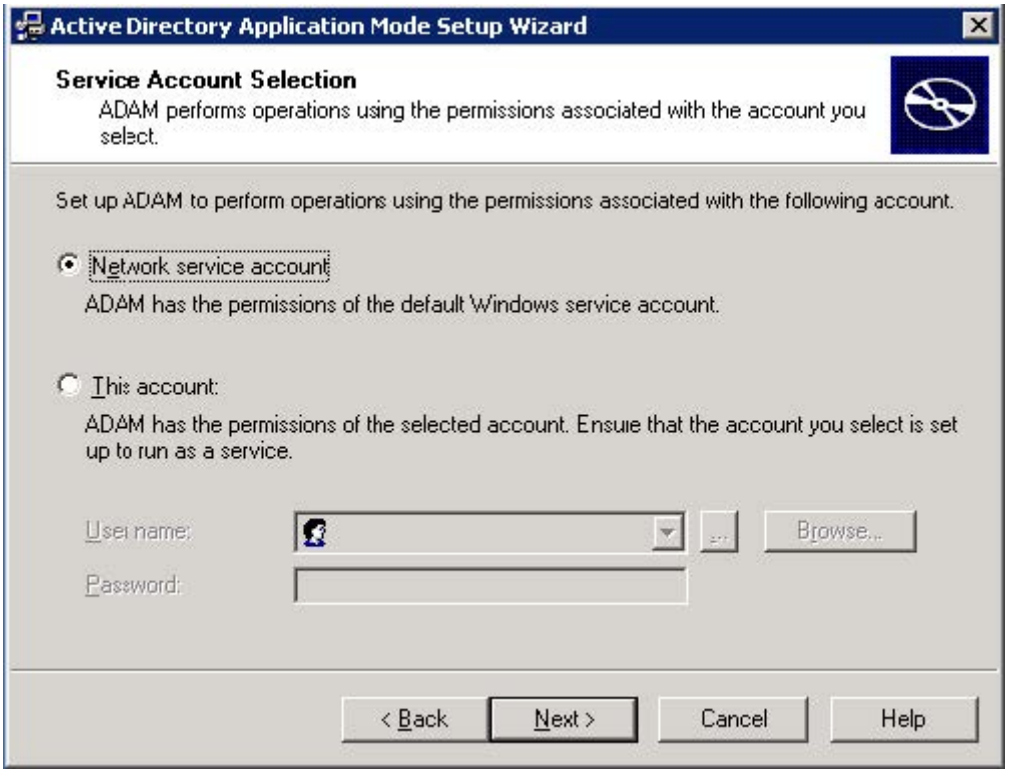
5. Select the **Yes, create an application directory partition** check box and enter the desired name (e.g., o=Yealink,c=CN) in the **Partition name** field, and then click **Next**.



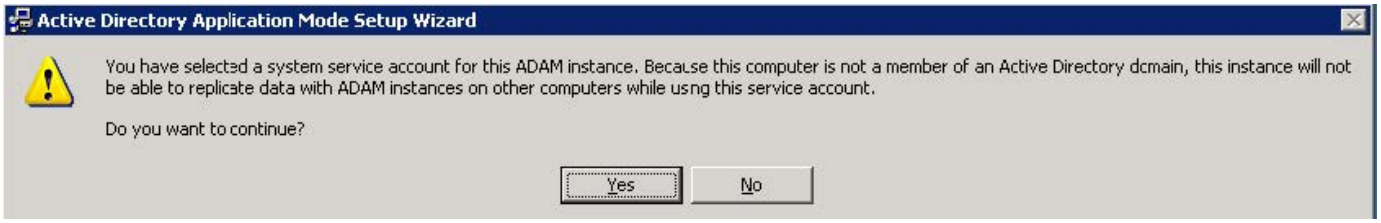
6. Specify the desired paths for the data and data recovery files, and click **Next**.



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

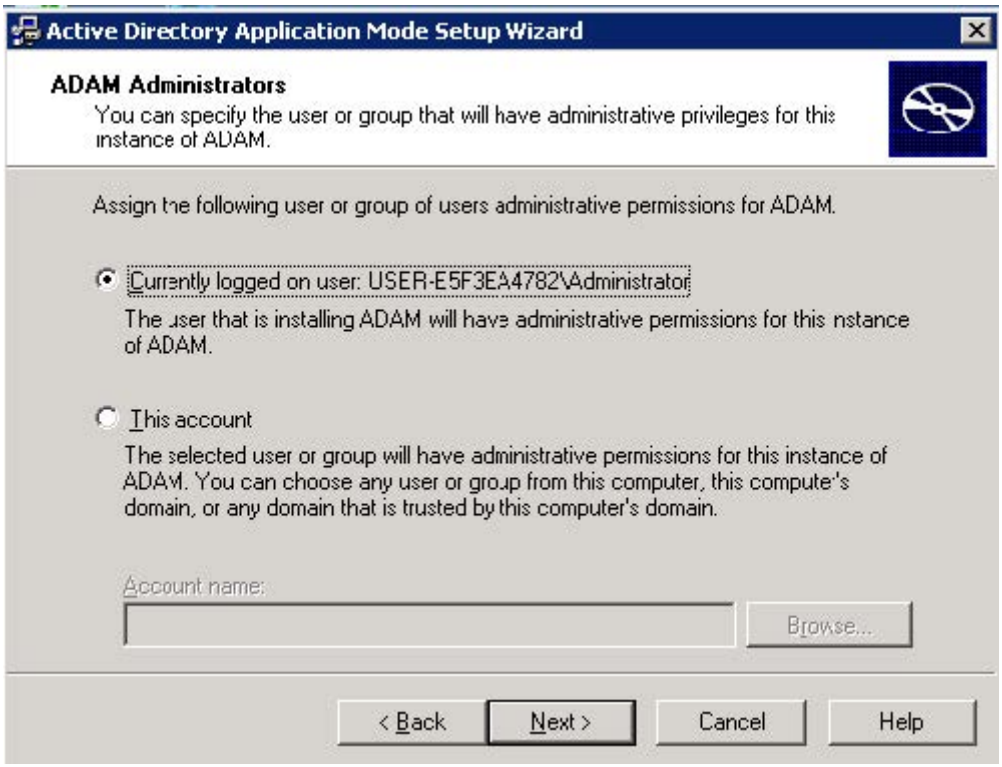


It will pop up the following prompt box. Read the provided information and click **Yes**.



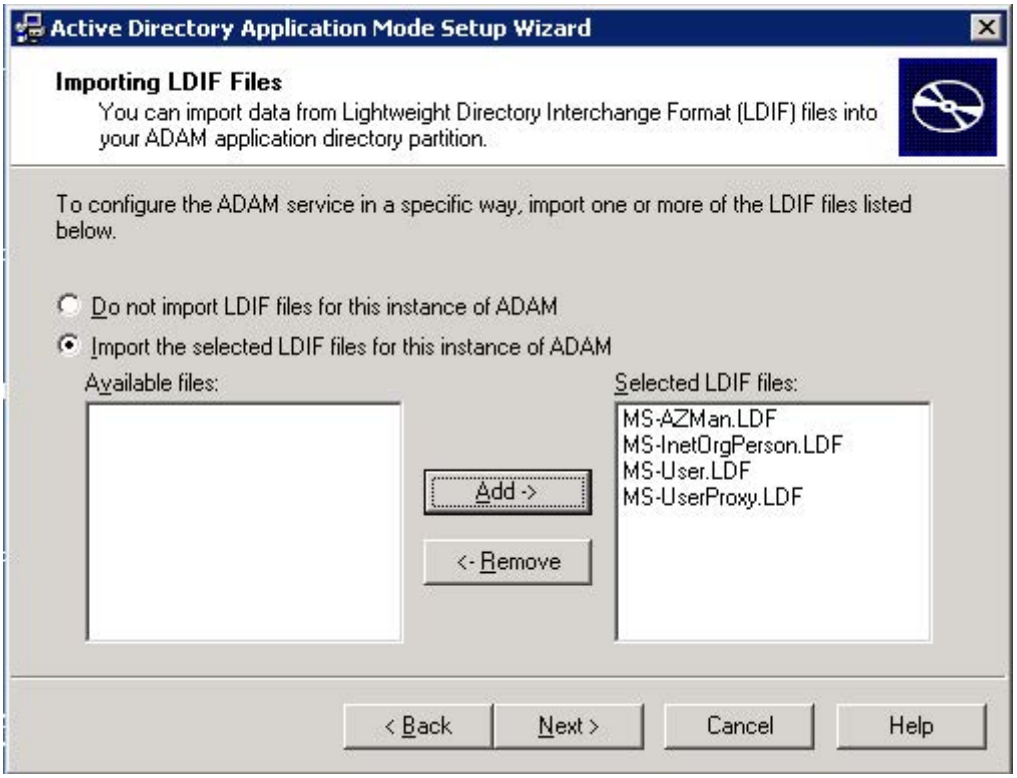
8. Select the first check box to assign the administrative permissions for ADAM to the currently logged-

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

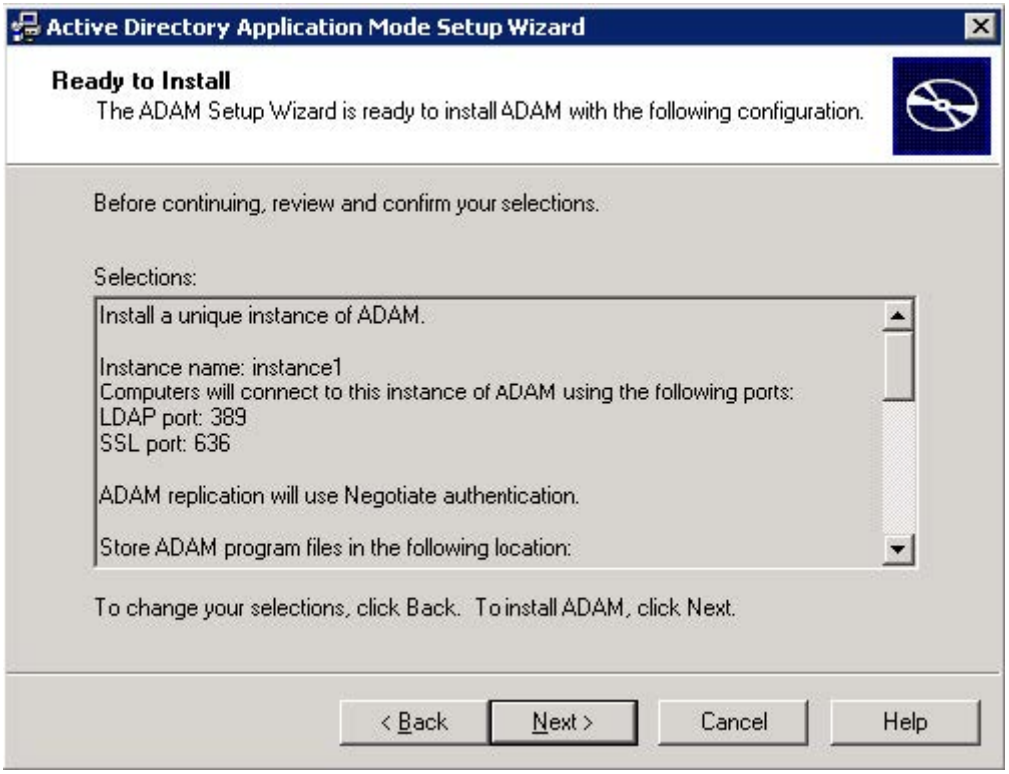


9. Select the **Import the selected LDIF files for this instance of ADAM** check box.

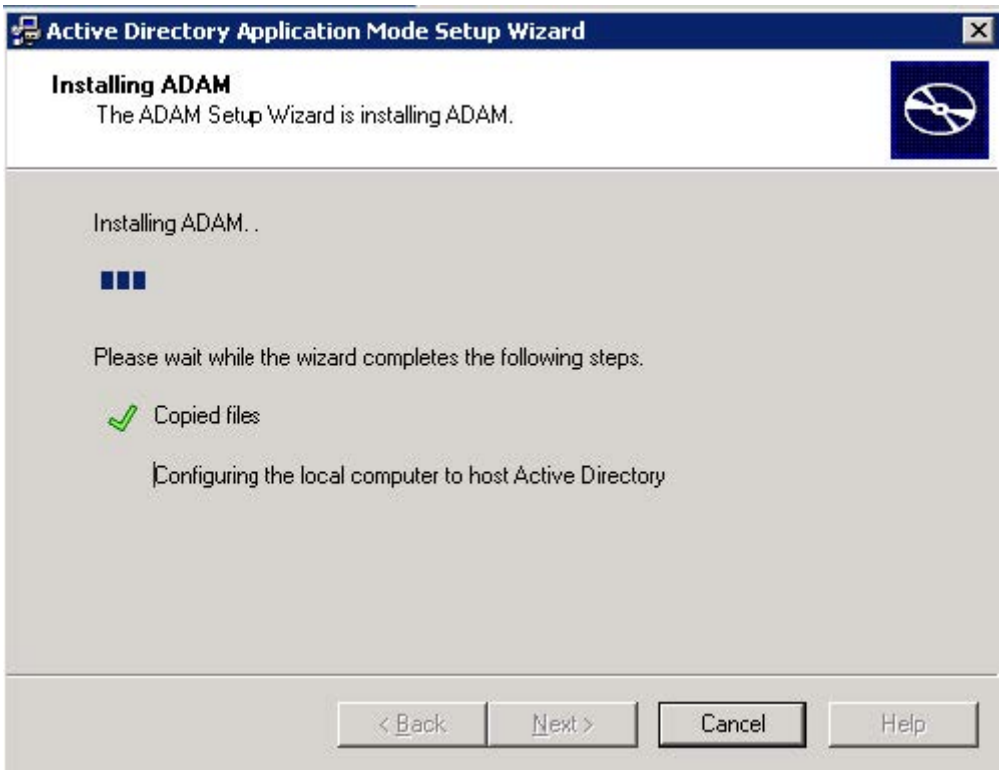
10. In the **Available** files box, select the desired LDF files and then click **Add->**, and then click **Next**.



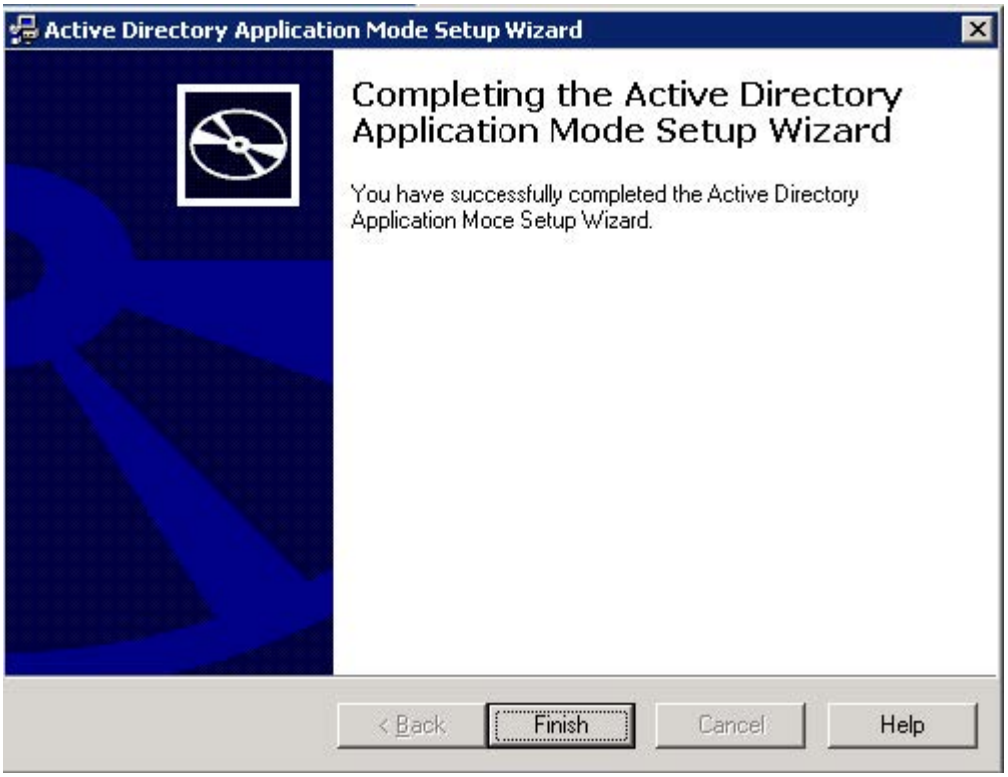
11. Review your selection and click **Next**.



The installation progress is shown below:



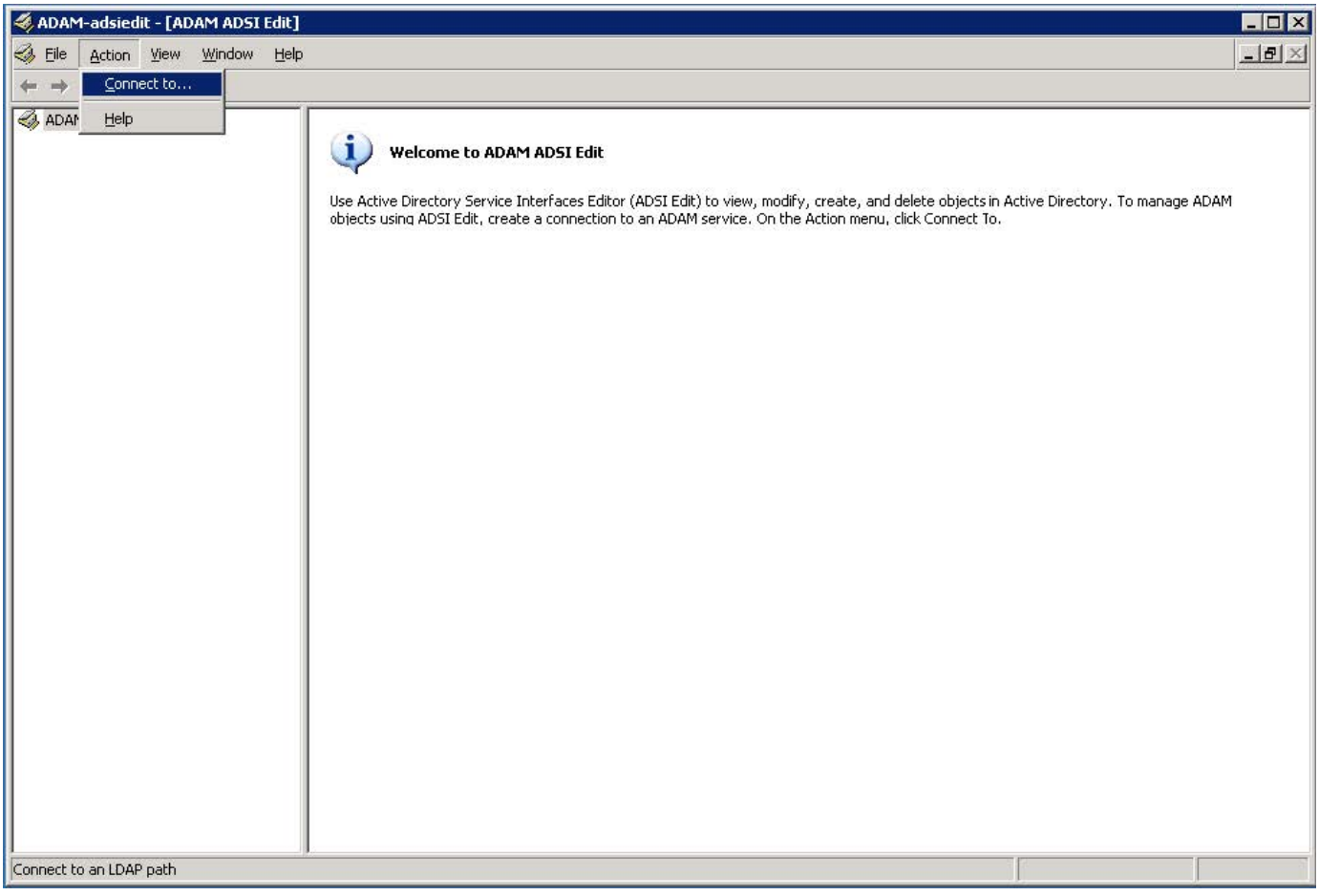
12. Click **Finish** to complete the installation and exit the wizard.



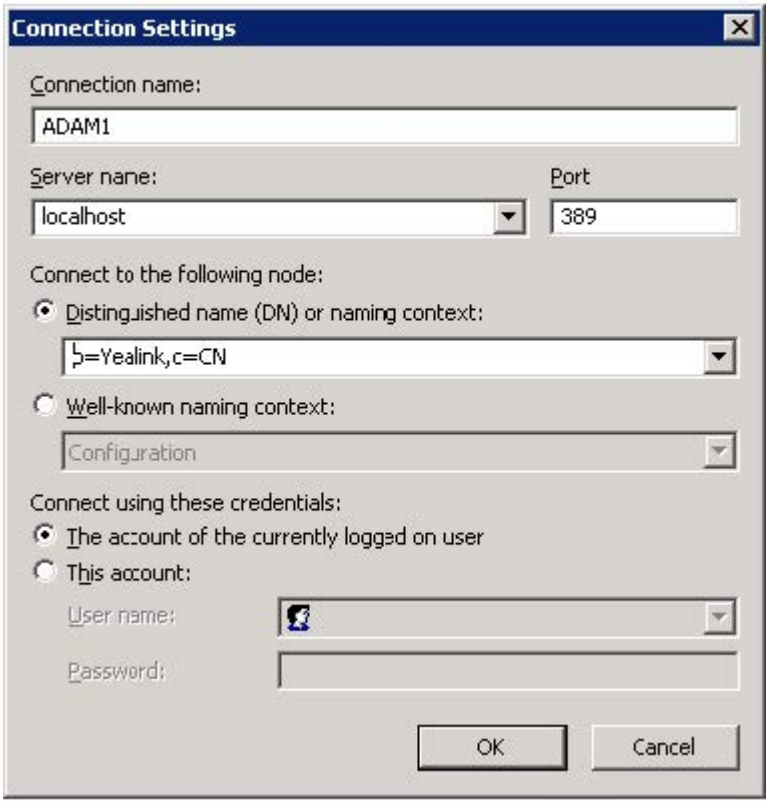
Configure the ADAM ADSI Edit

To configure the ADAM ADSI Edit:

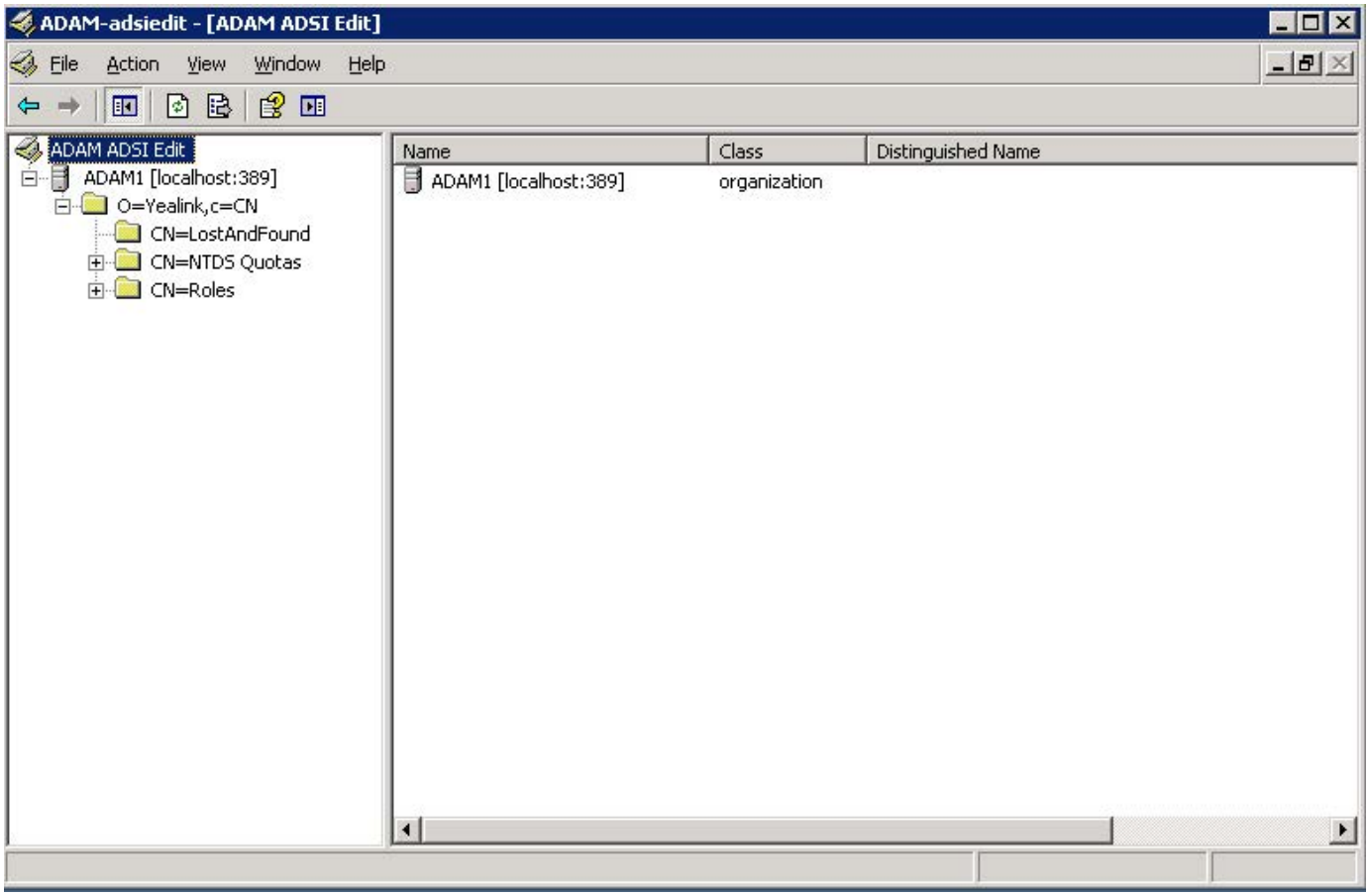
1. Click **Start** > **Programs** > **ADAM** > **ADAM ADSI Edit**.
2. Click **Action** > **Connect to**.



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**.

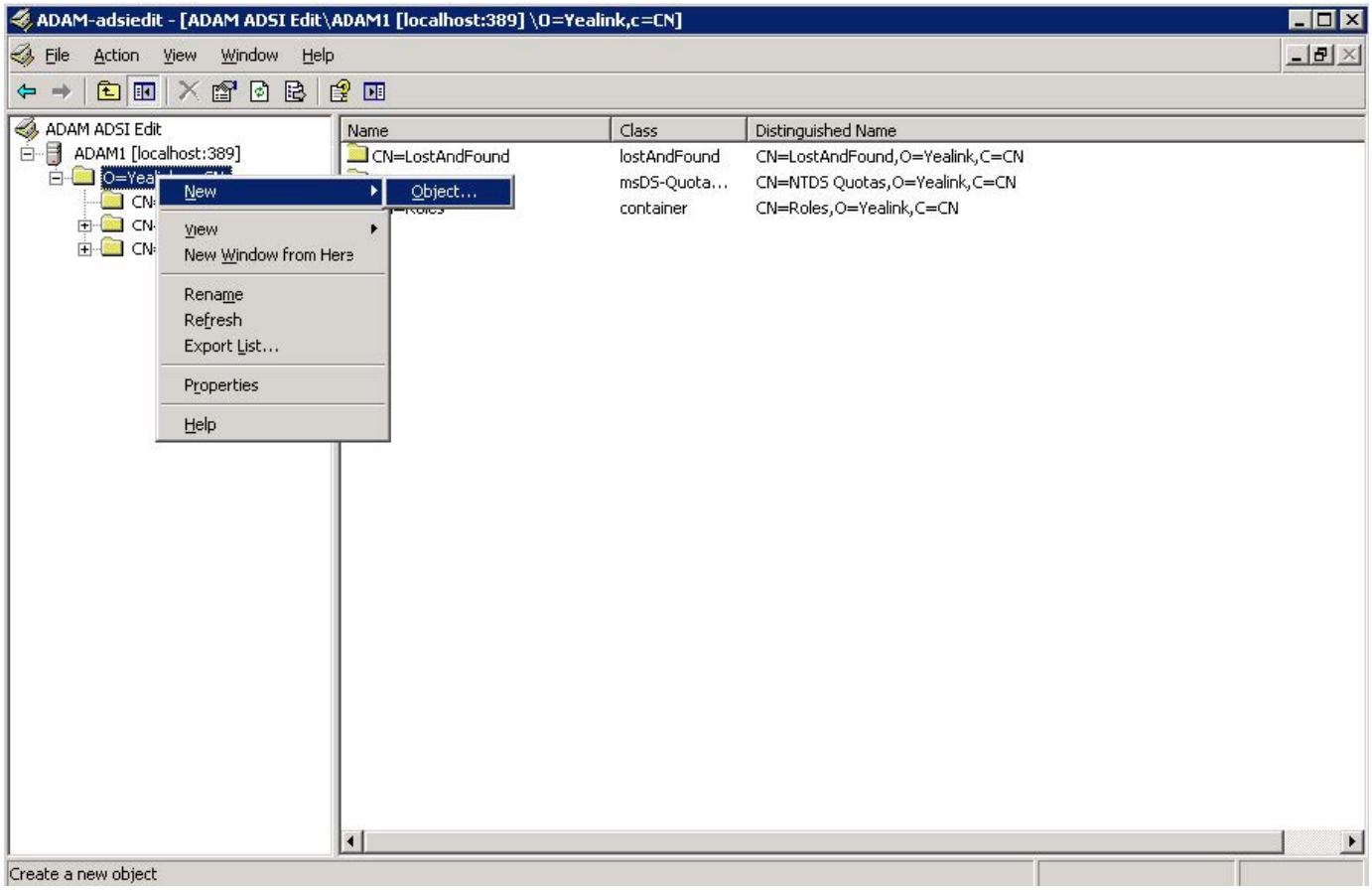


7. When the ADAM ADSI Edit connects an application directory partition (e.g., o=Yealink,c=CN) successfully, it will show as below:

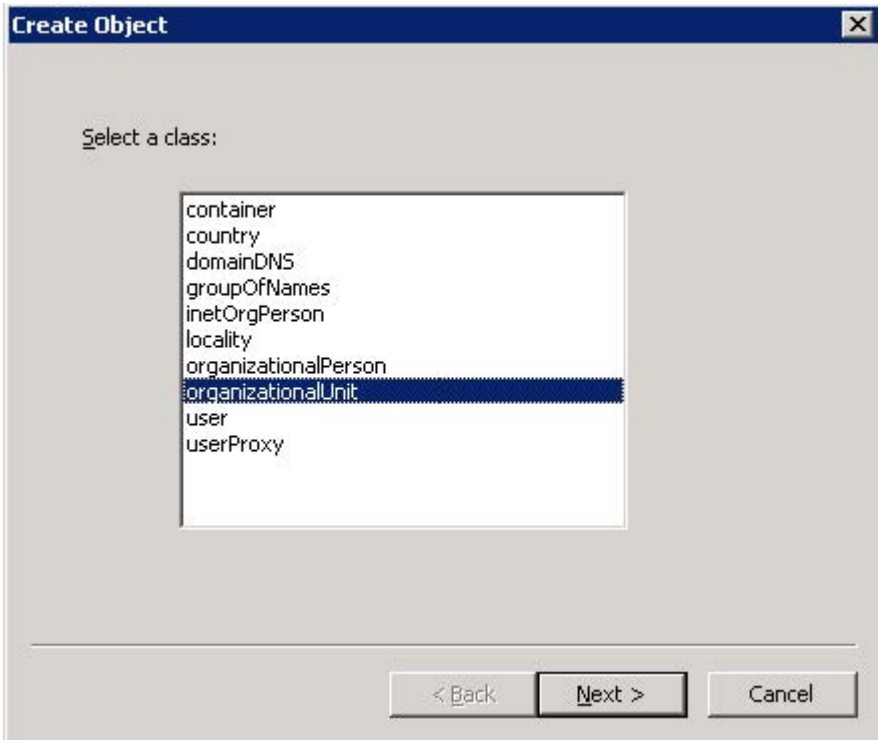


To create the object for ADAM:

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

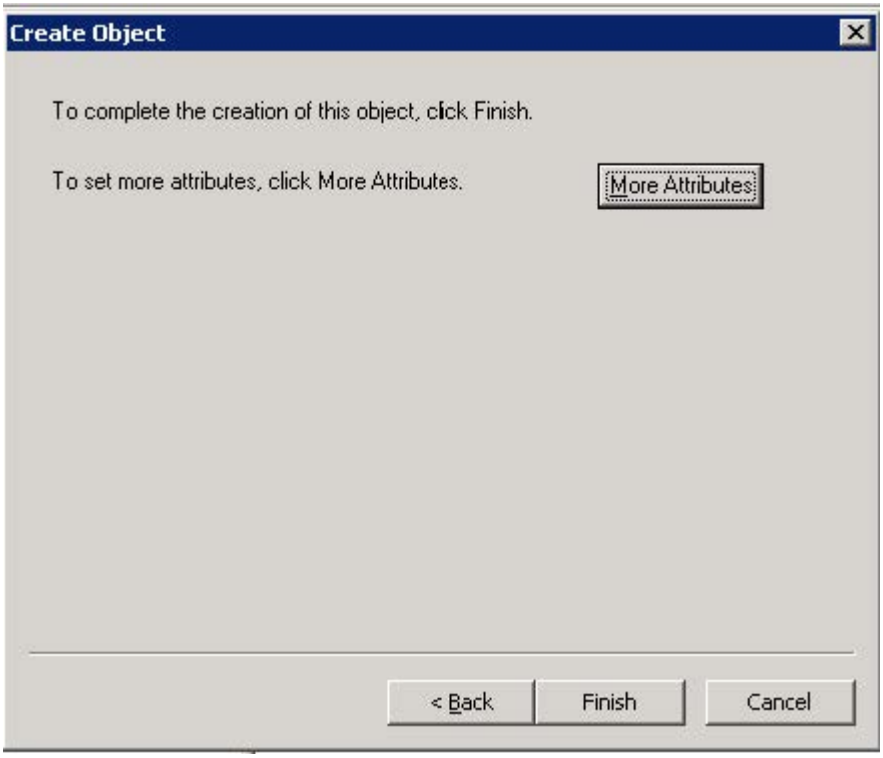


2. Select **organizationalUnit** and click **Next**.

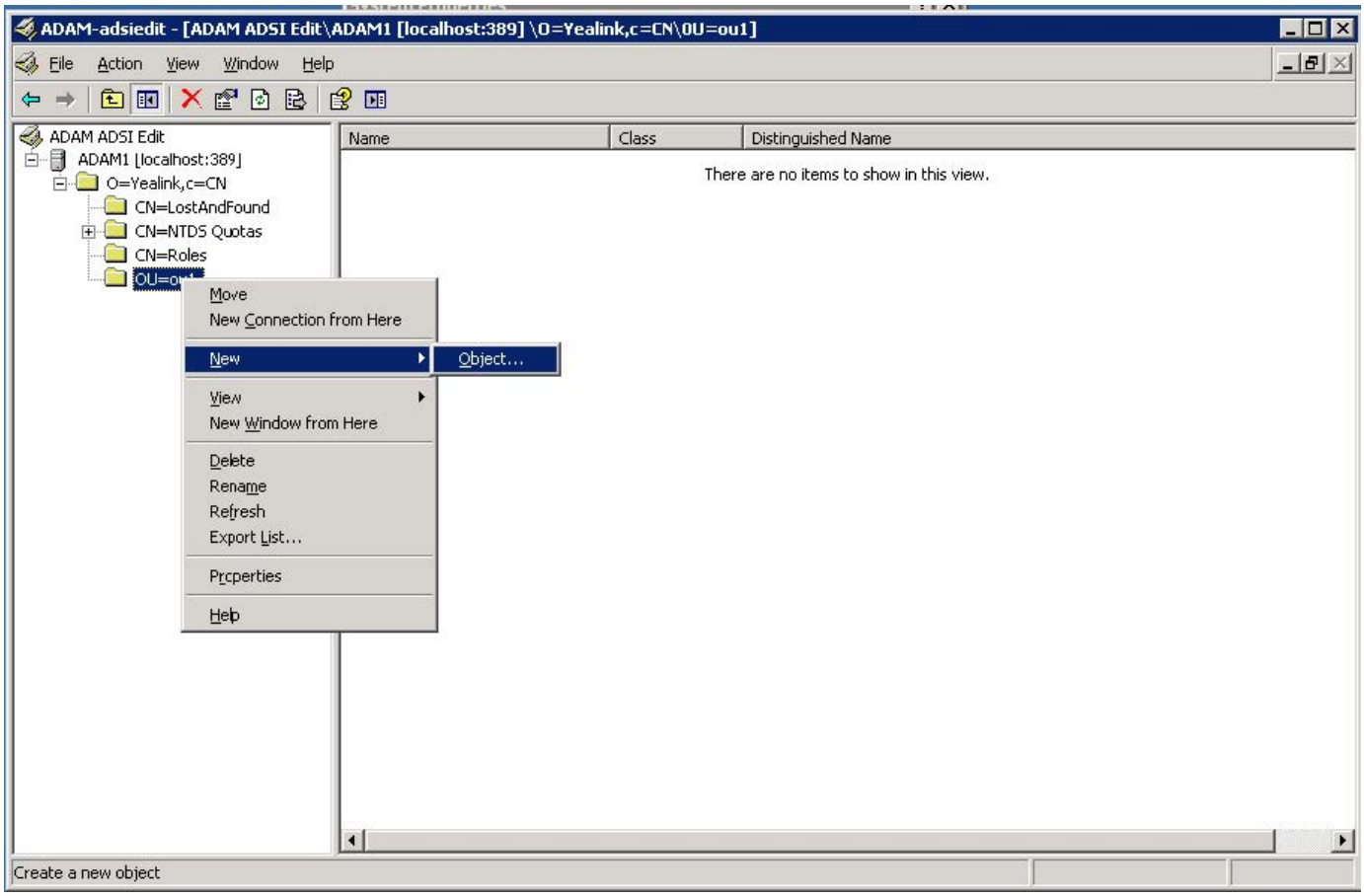


3. Enter the desired value (e.g., ou1) in the **Value** field and click **Next**.
4. Click **Finish** to complete the creation of this object.

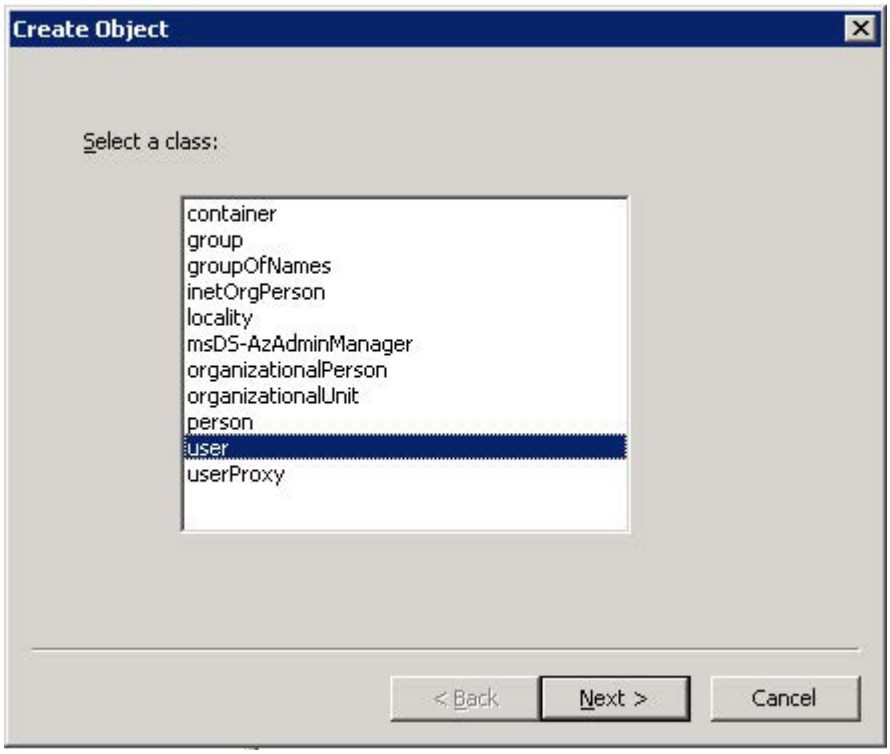
   You can also click **More Attributes** to set more attributes for this object.



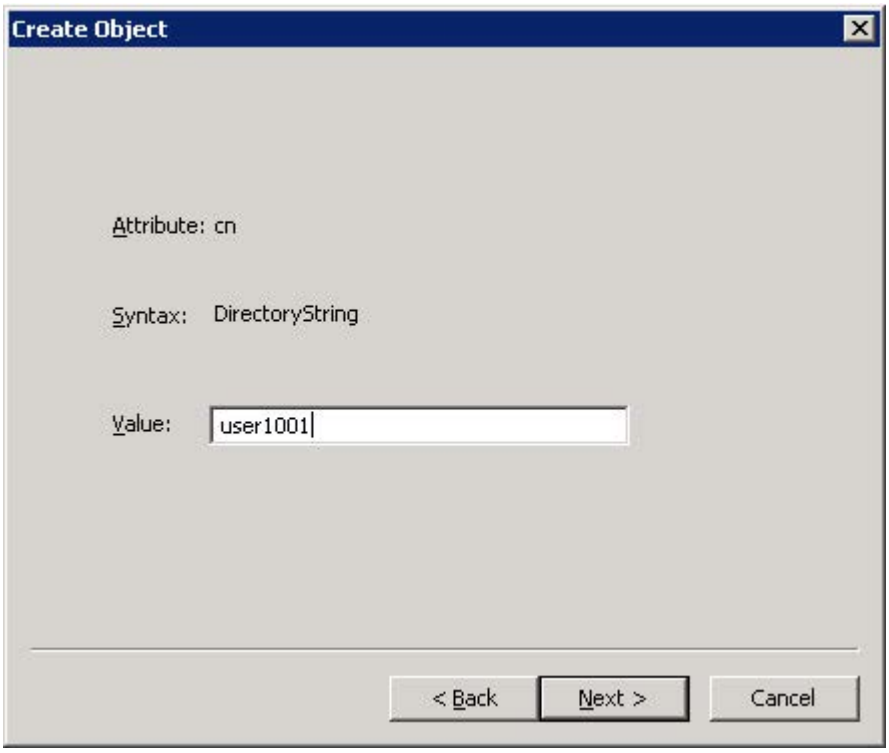
5. Select and right-click **OU=ou1**, and then select **New** > **Object**.



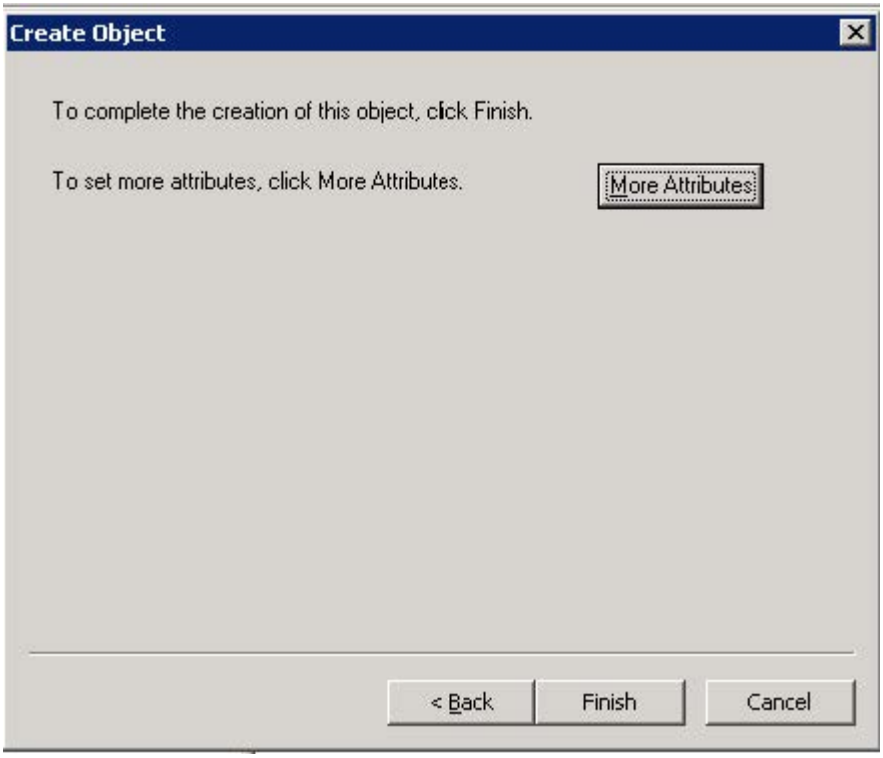
6. Select the **user** and click **Next**.



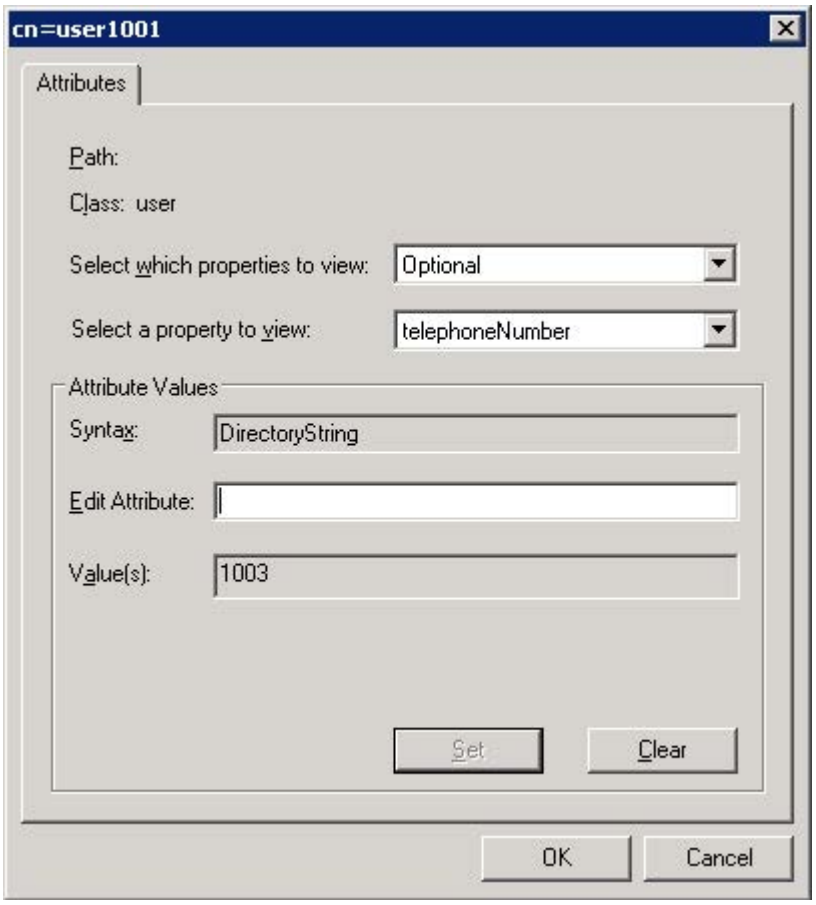
7. Enter the desired value (e.g., user1001) in the **Value** field and click **Next**.



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



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



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

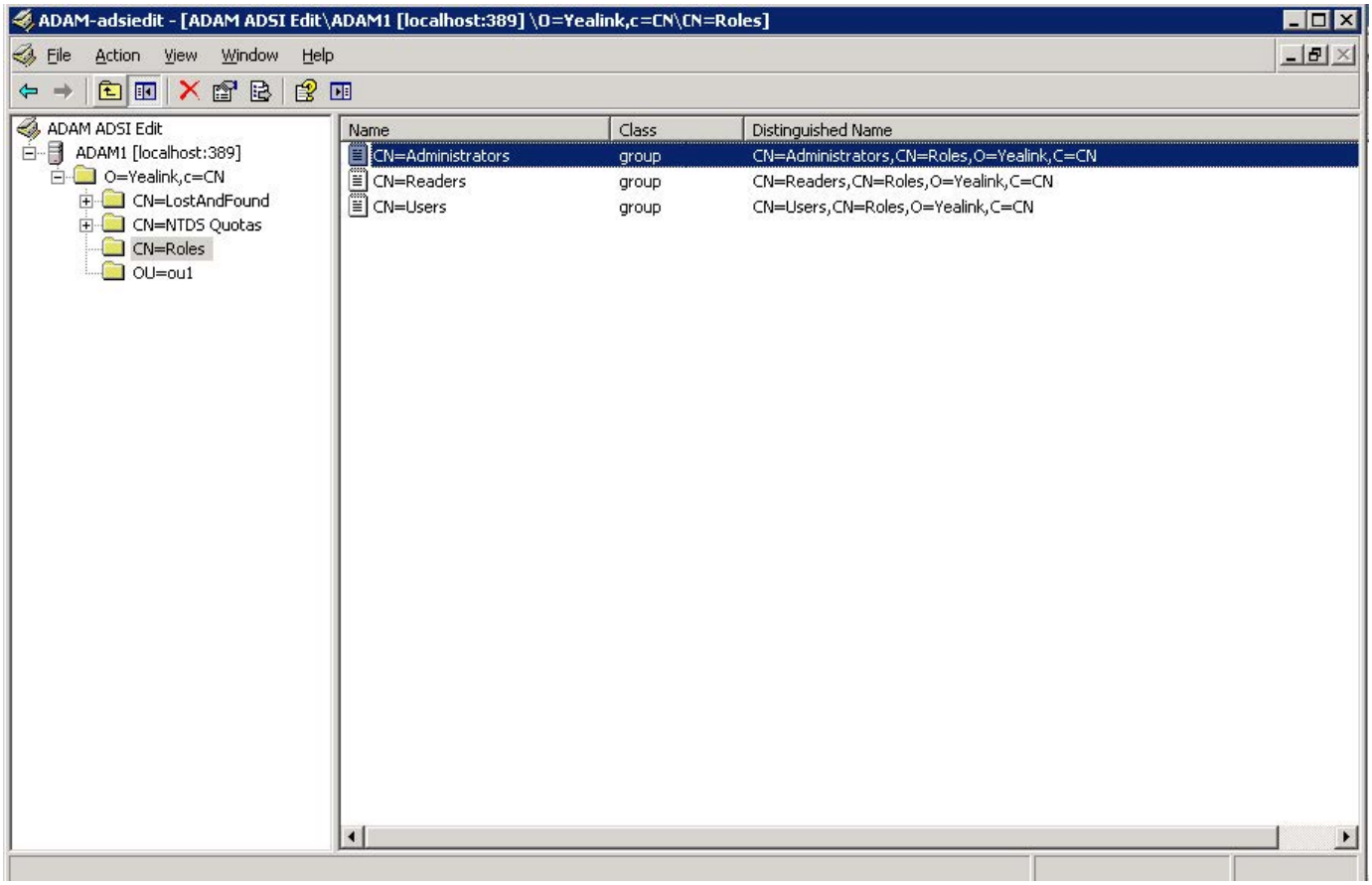


13. Click **OK** to accept the change.

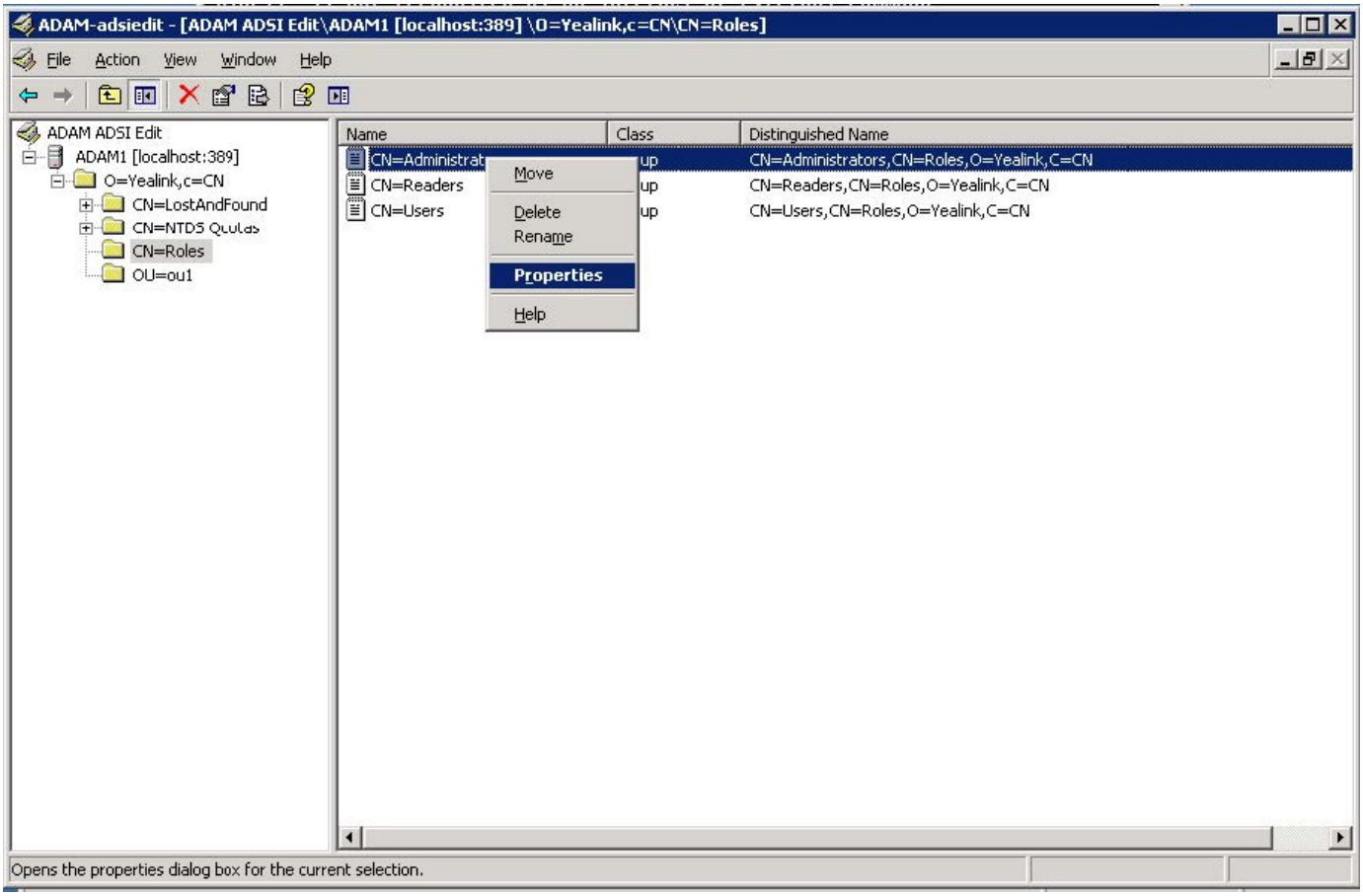
If you want to use the user created above to manage and search for information in LDAP, you need to add the user to the administrator group in advance.

To add the user to the administrator group:

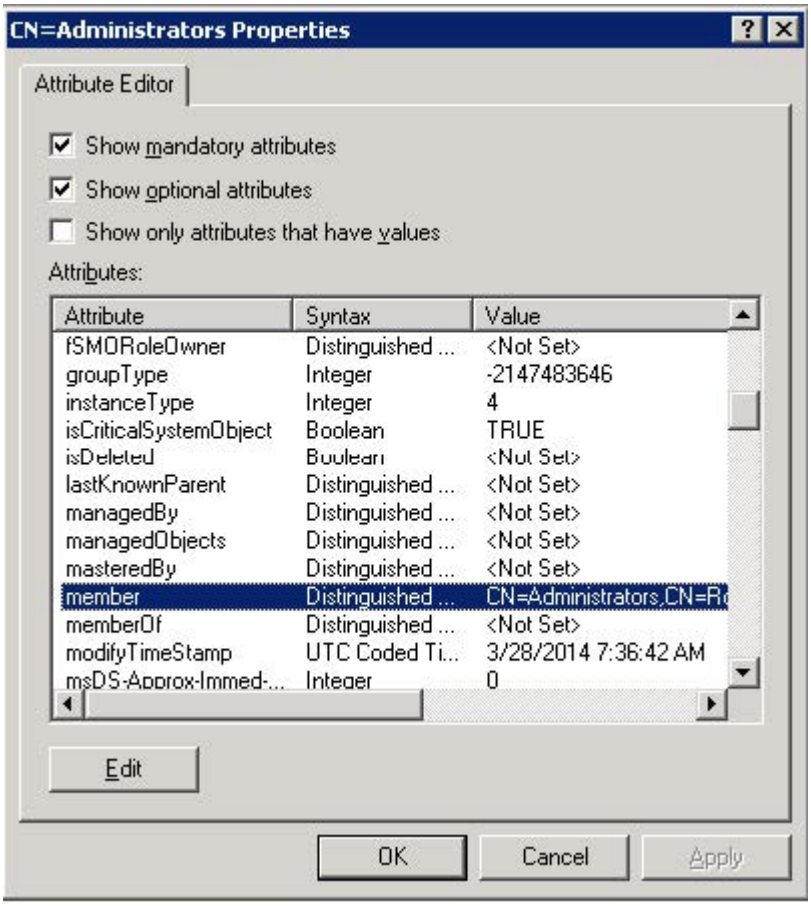
1. Click **ADAM1** > **O=Yealink, c=CN** > **CN=Roles**.



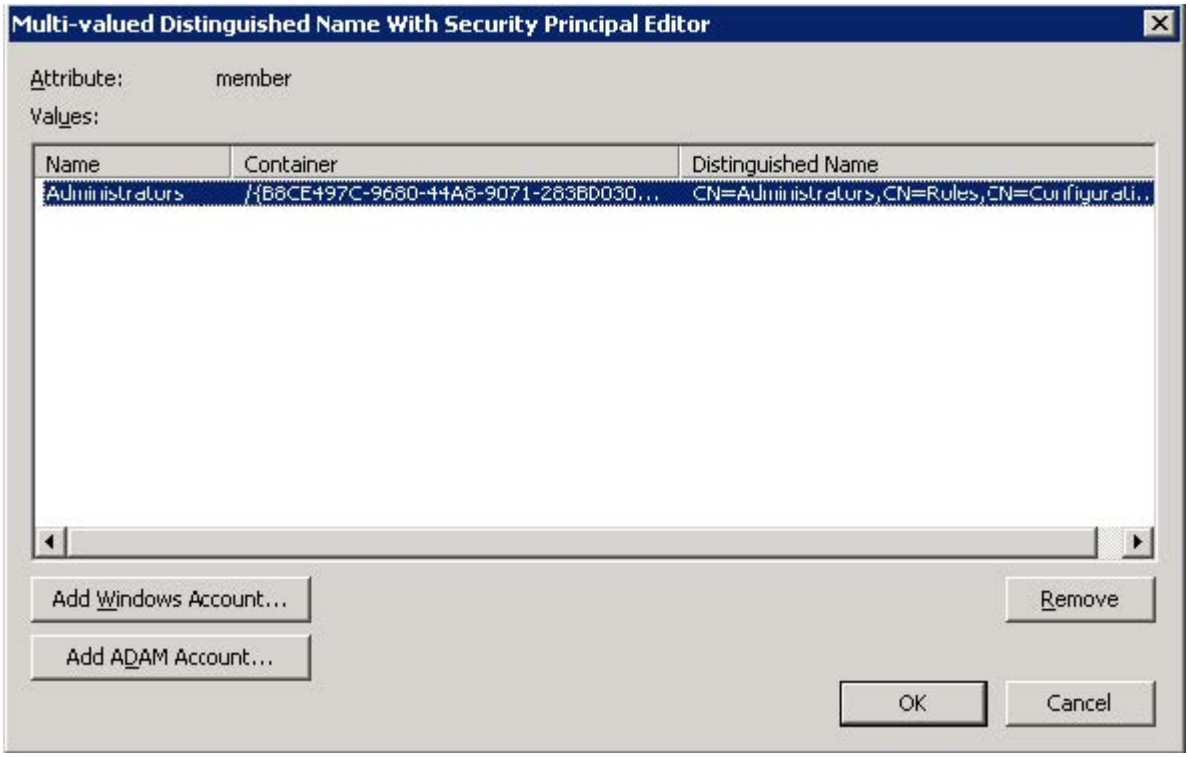
2. Select and right-click **CN=Administrators**, and then select **Properties**.



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



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



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

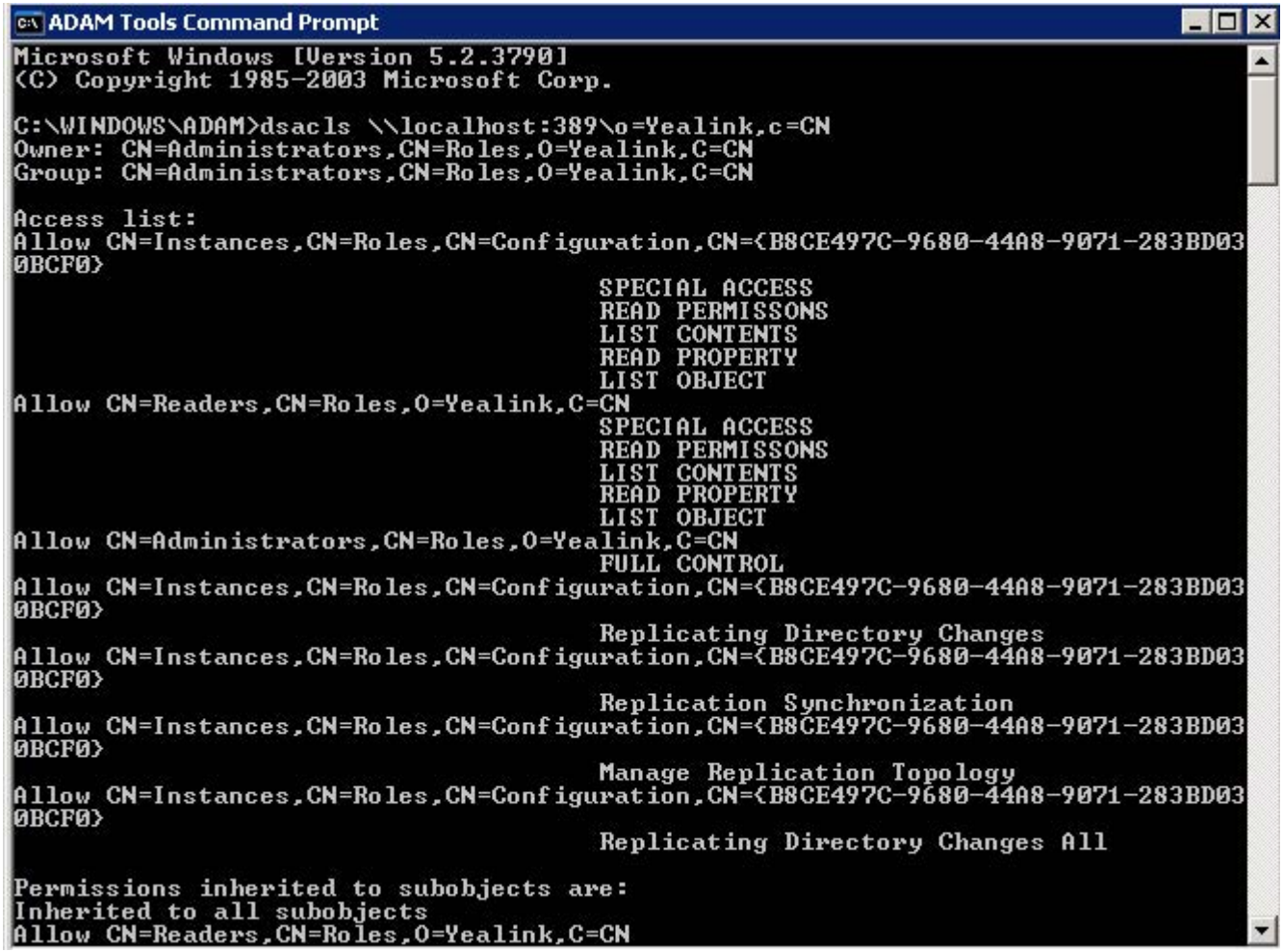
8. Click **OK** to accept the change and close the Administrators Properties interface.

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

To view permissions using the command:

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

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



Sun One Directory Server

Sun One Directory Server, also known as Sun Java System Directory Server, is a component of the Java Enterprise System. Sun One Directory Server can be installed on multiple platforms, such as Windows, Linux, Solaris, and so on. This section shows you how to install Sun One Directory Server version 5.2 on a 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 the FQCN (Fully Qualified Computer Name) of your computer to the file. For example, the FQCN of your computer is ldapsun.yealinktest.com. Add the following mapping:

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

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

127.0.0.1       localhost
127.0.0.1       ldapsun.yealinktest.com
```

4. Save the hosts file.

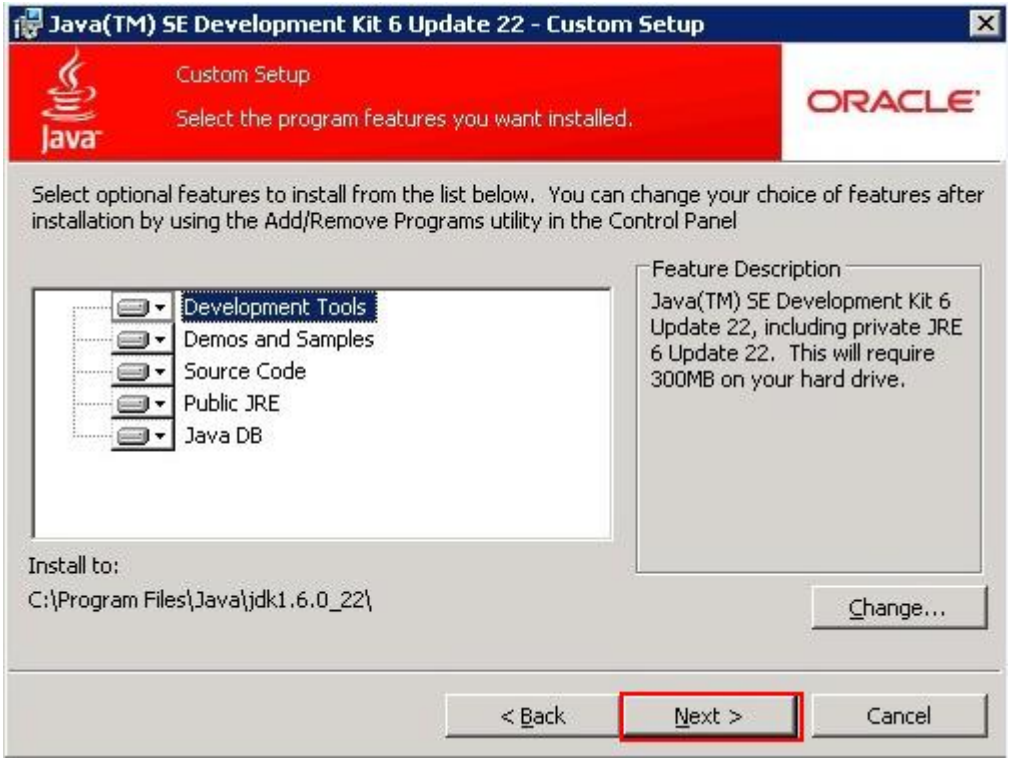
The following shows you how to install the Java Development Kit (JDK) 6 on your computer. You can download it online: http://www.oracle.com/technetwork/java/javase/downloads/index.html.

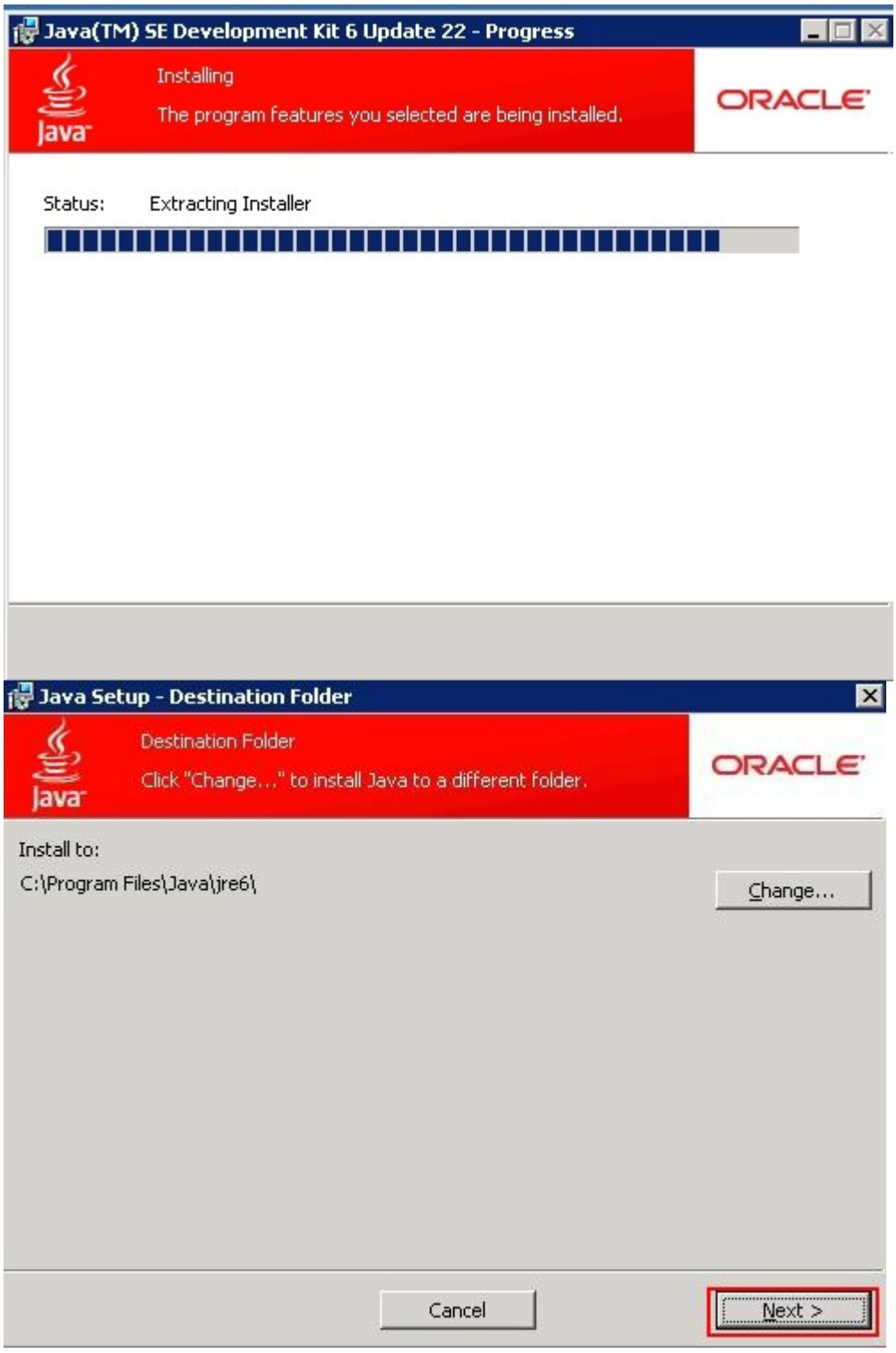
To install the Java Development Kit (JDK) 6:

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



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



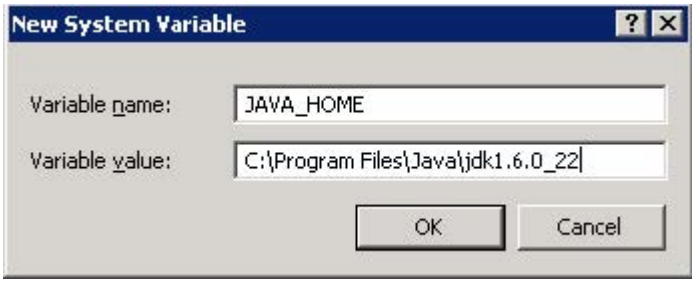
4. Click **Finish** to finish the installation.

   After the installation, you need to configure environment variables.

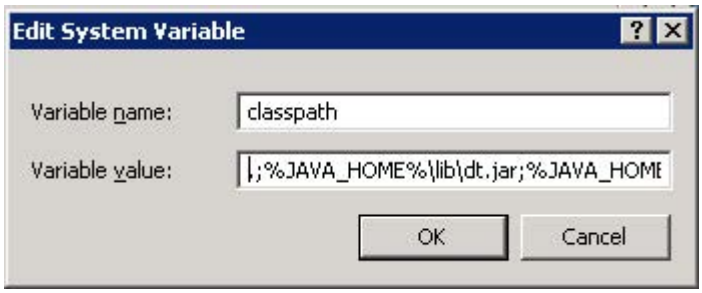
To configure environment variables:

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**.

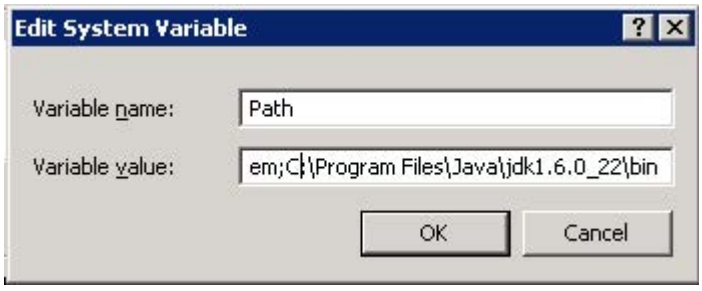
5. Enter the variable name as JAVA_HOME.
6. Enter the variable value as the installation path (e.g., C:\Program Files\Java\jdk1.6.0_22) for the Java Development Kit.



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.

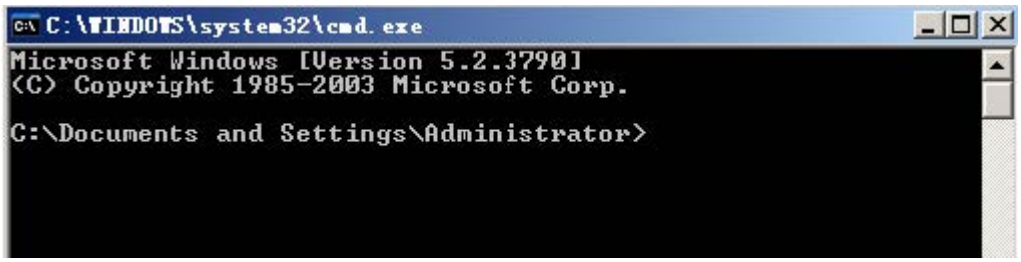


11. Click **OK**.
12. Click **Apply Changes**.

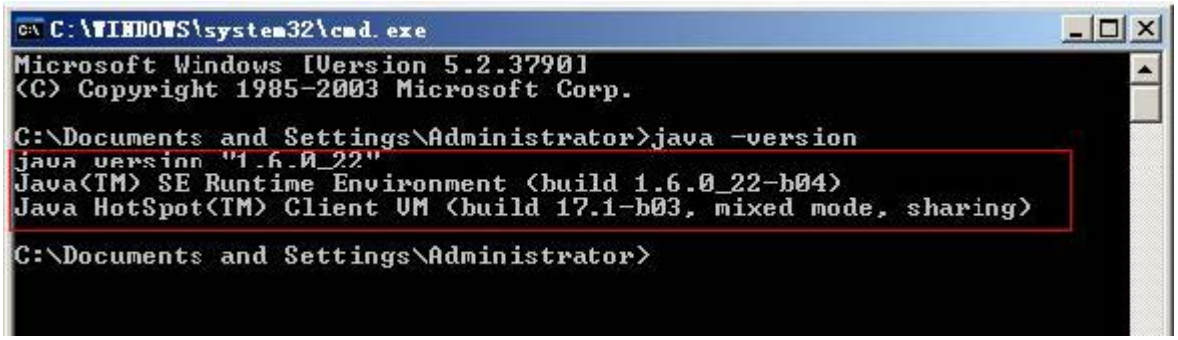
To verify the configuration of environment variables:

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

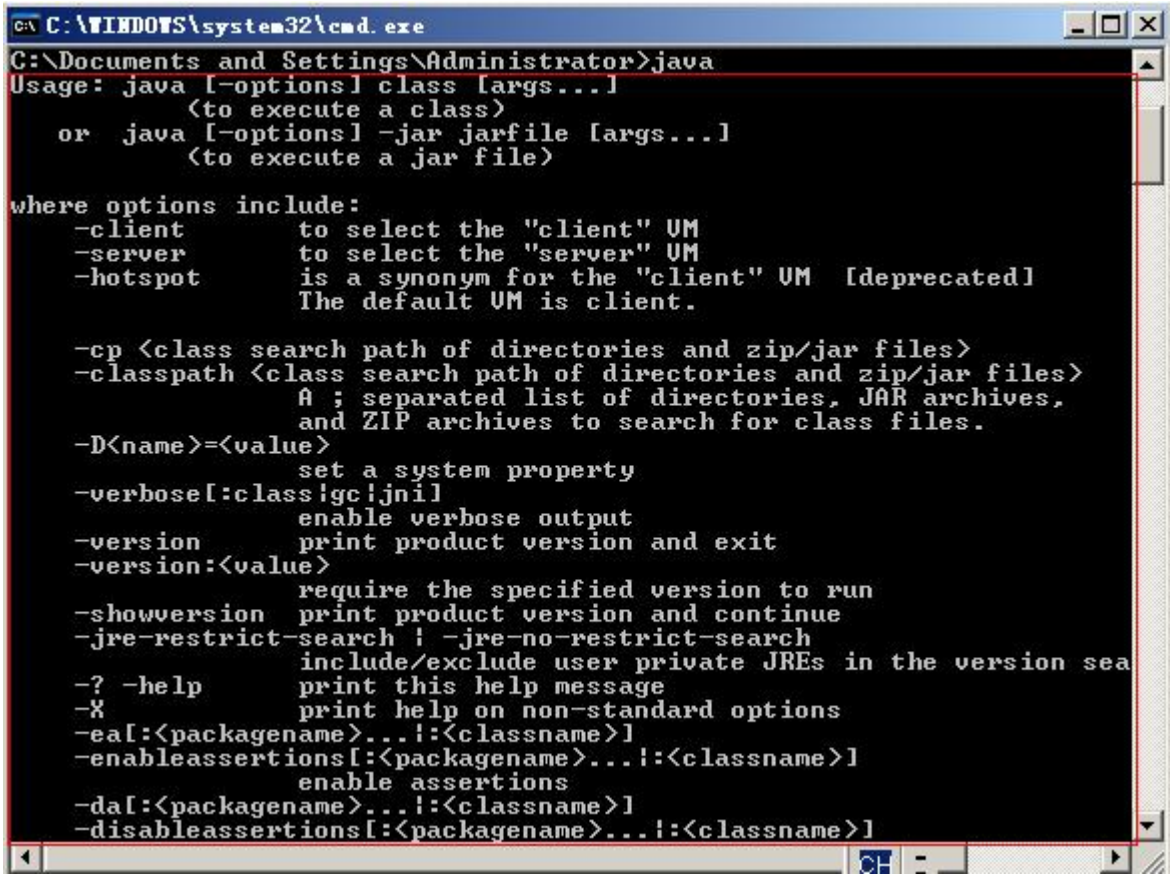
2. Enter **cmd** in the dialog and click **OK** to enter the command line interface.



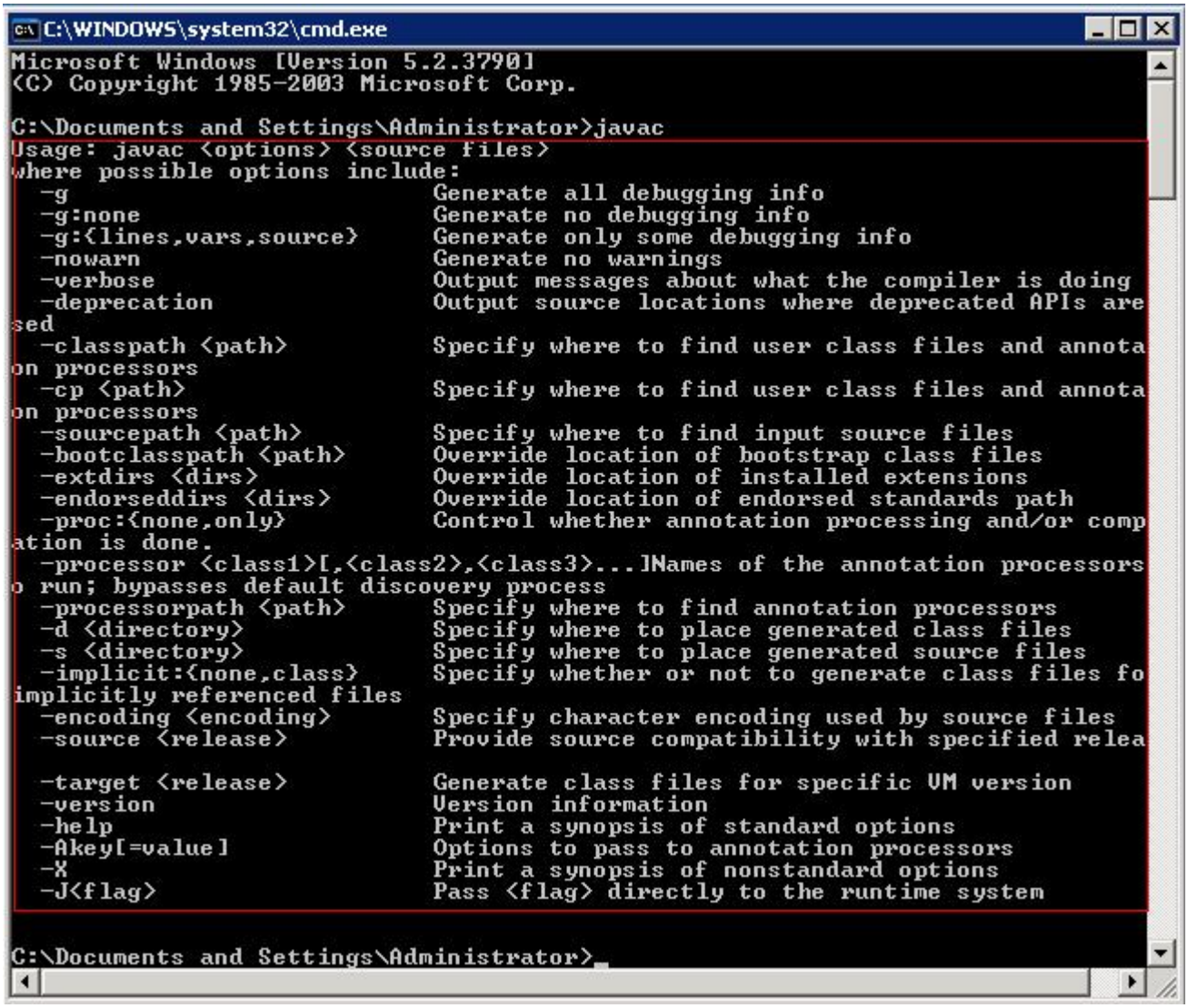
3. Execute the command **java -version** to check the Java version.



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



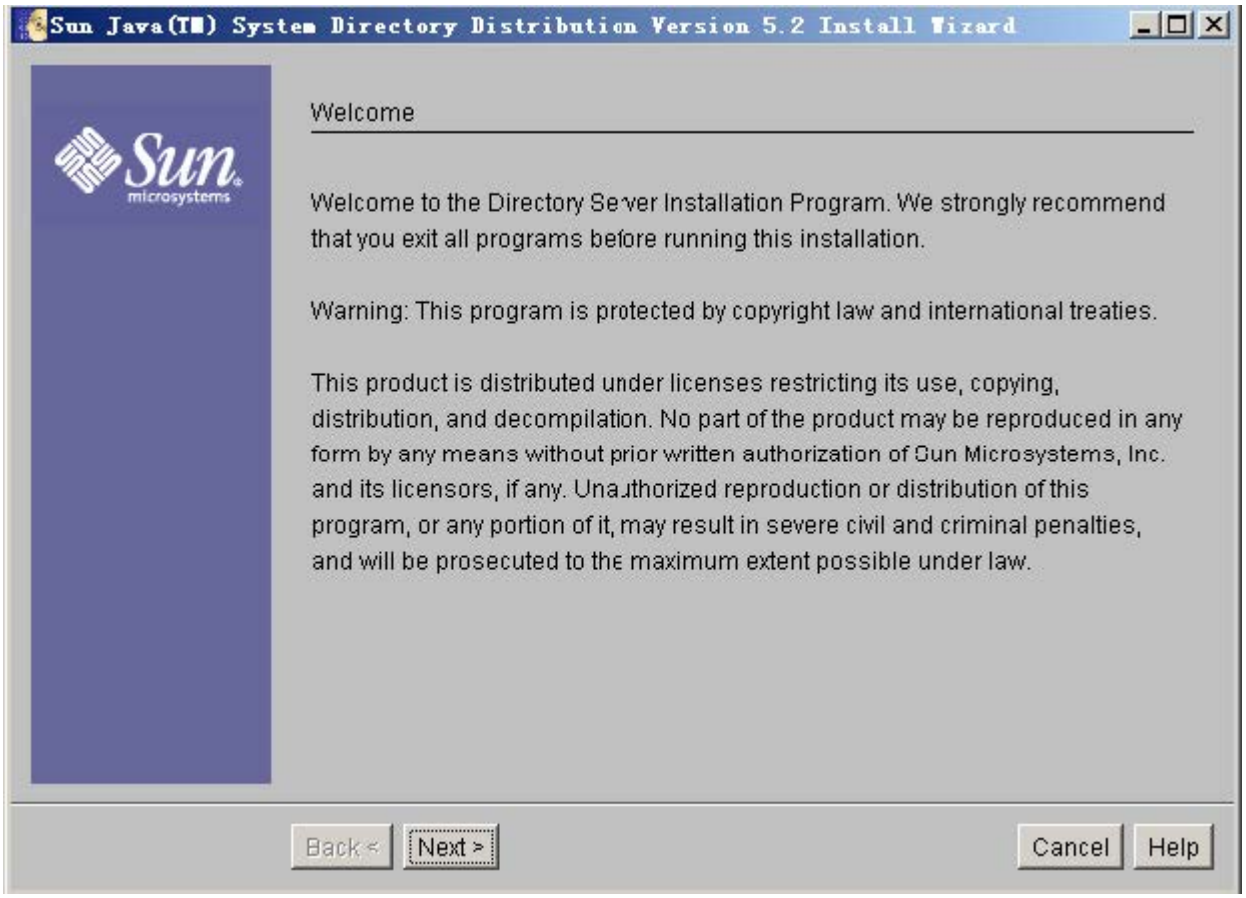
5. Execute the command **javac** to compile java files into class files.



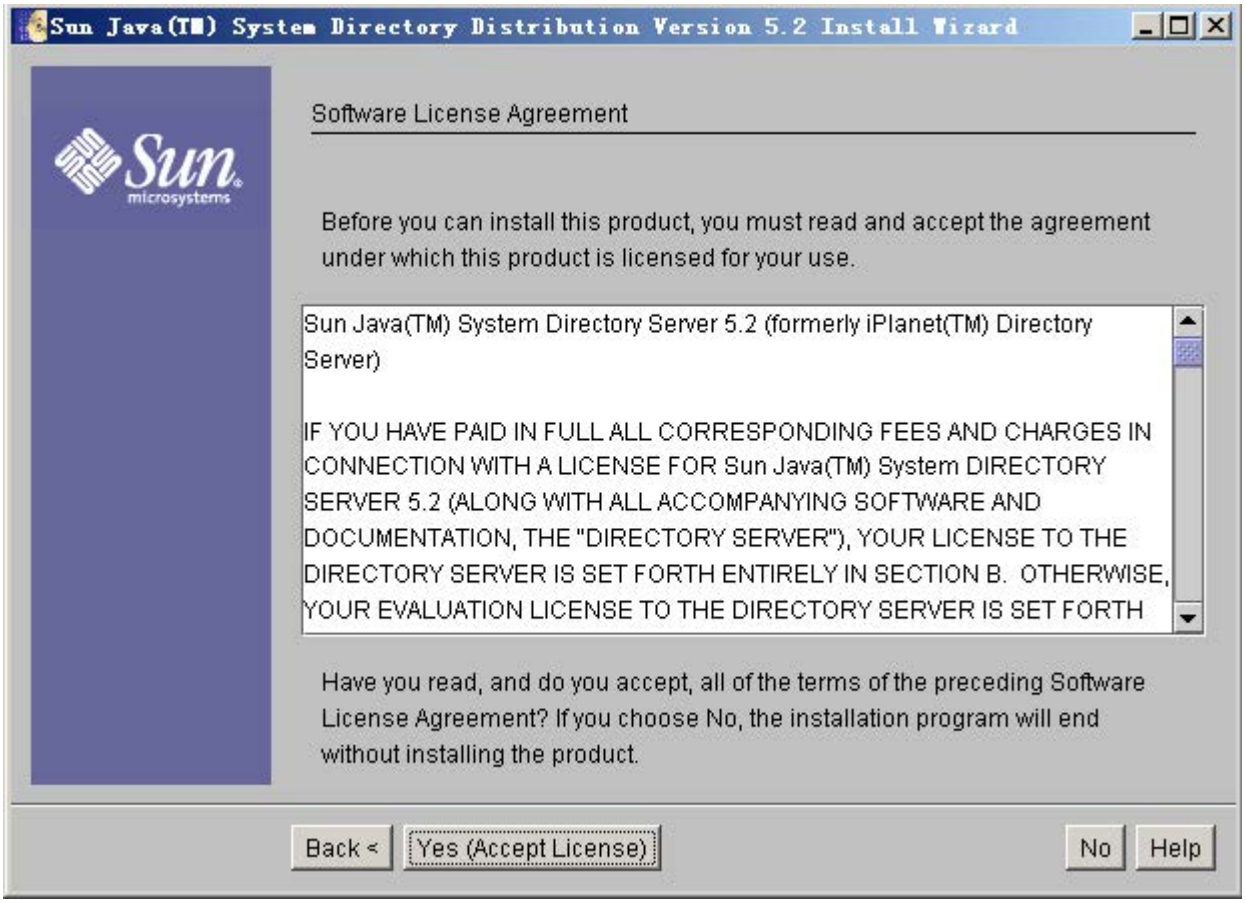
Install the Sun One Directory

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**.

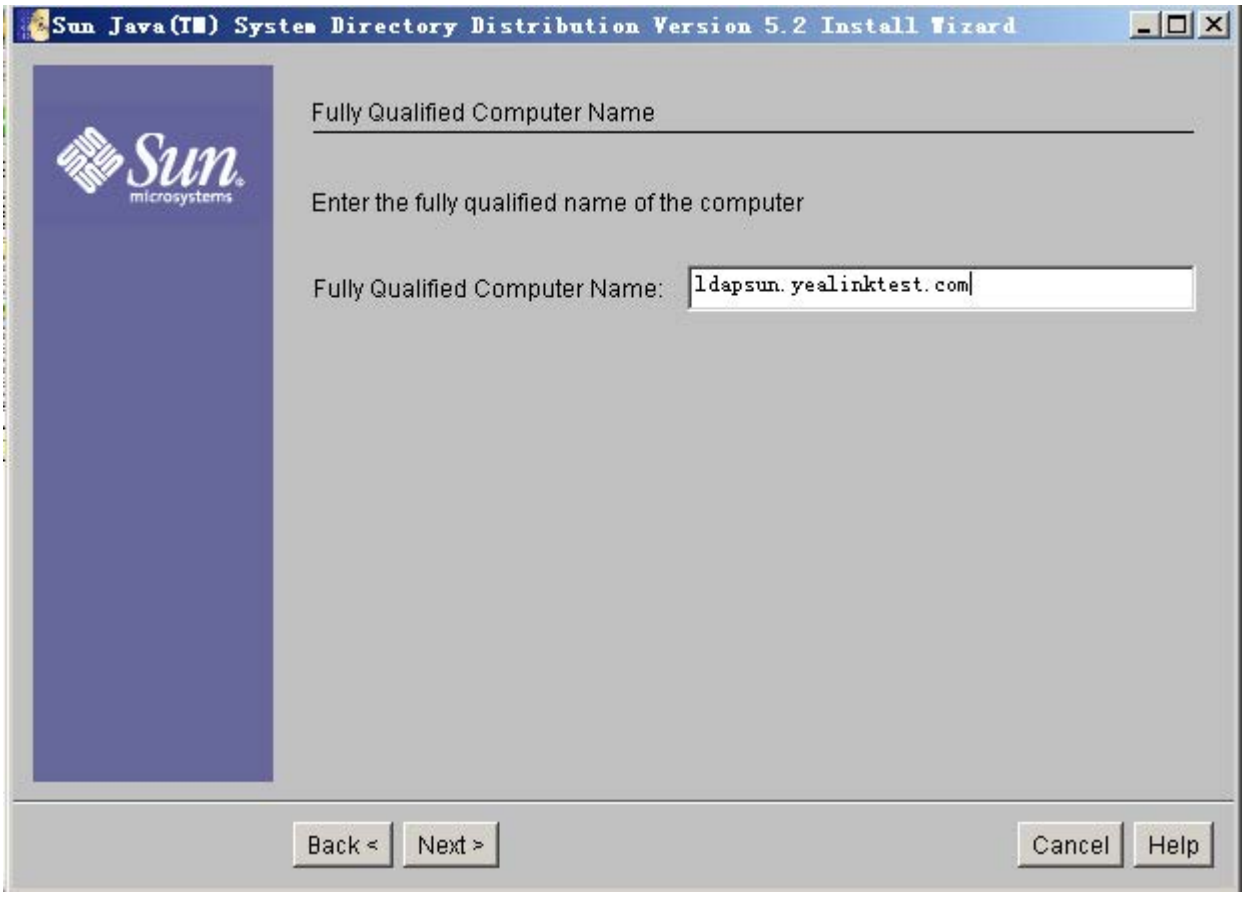


4. Read the software license agreement and click **Yes (Accept License)**.

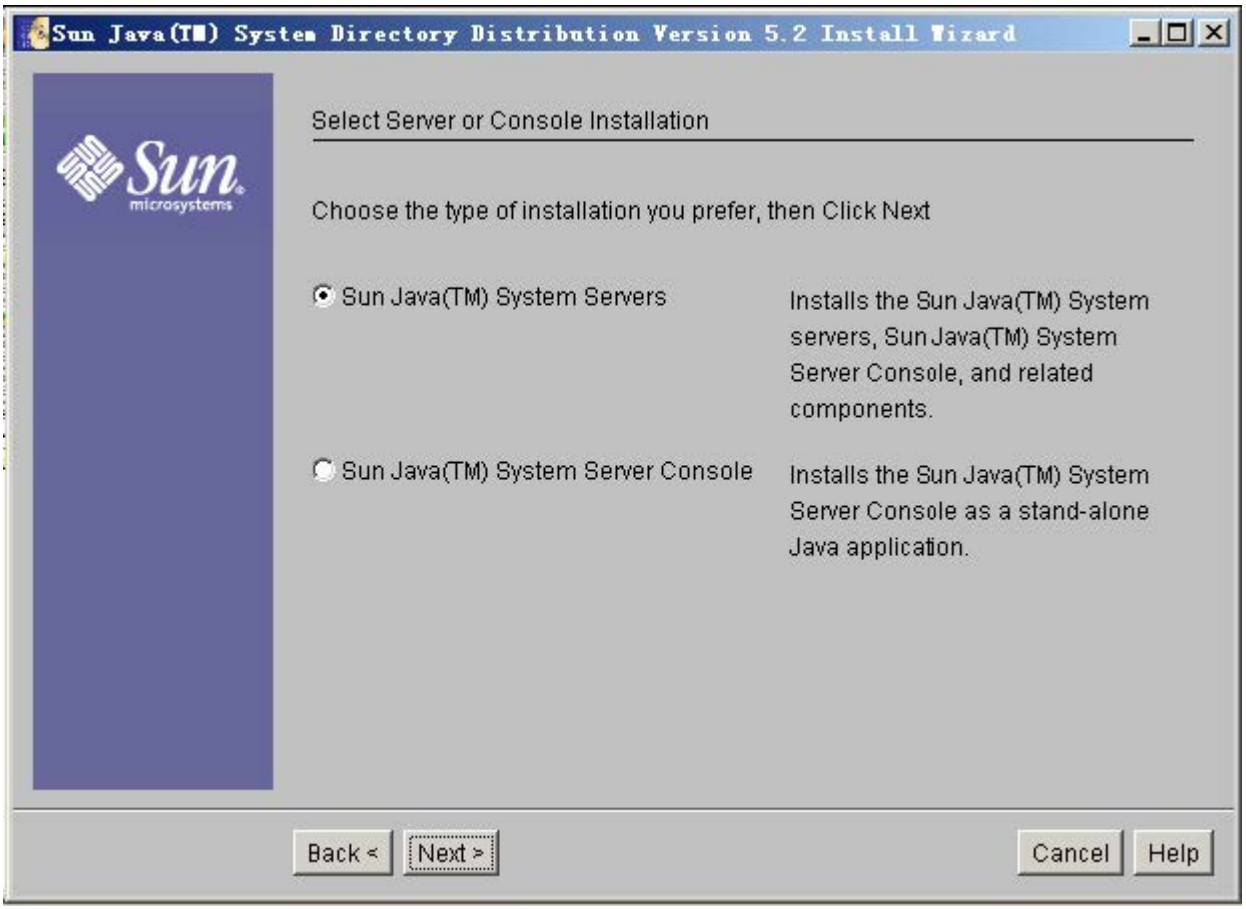


5. Enter the fully qualified name of the computer (e.g., ldapsun.yealinktest.com) in the **Fully Qualified Computer Name** field and click **Next**.

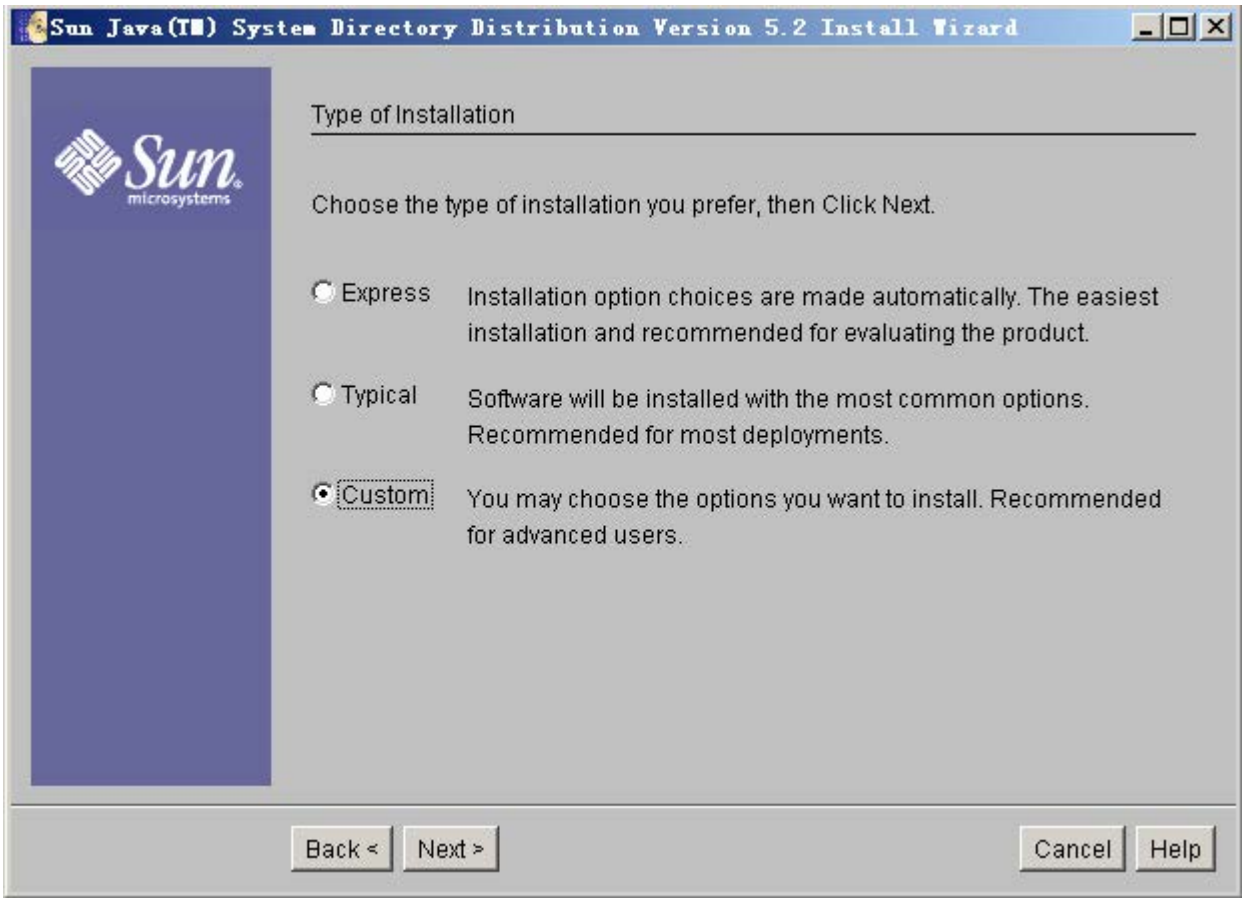
6. The fully qualified name of the computer was planned before.



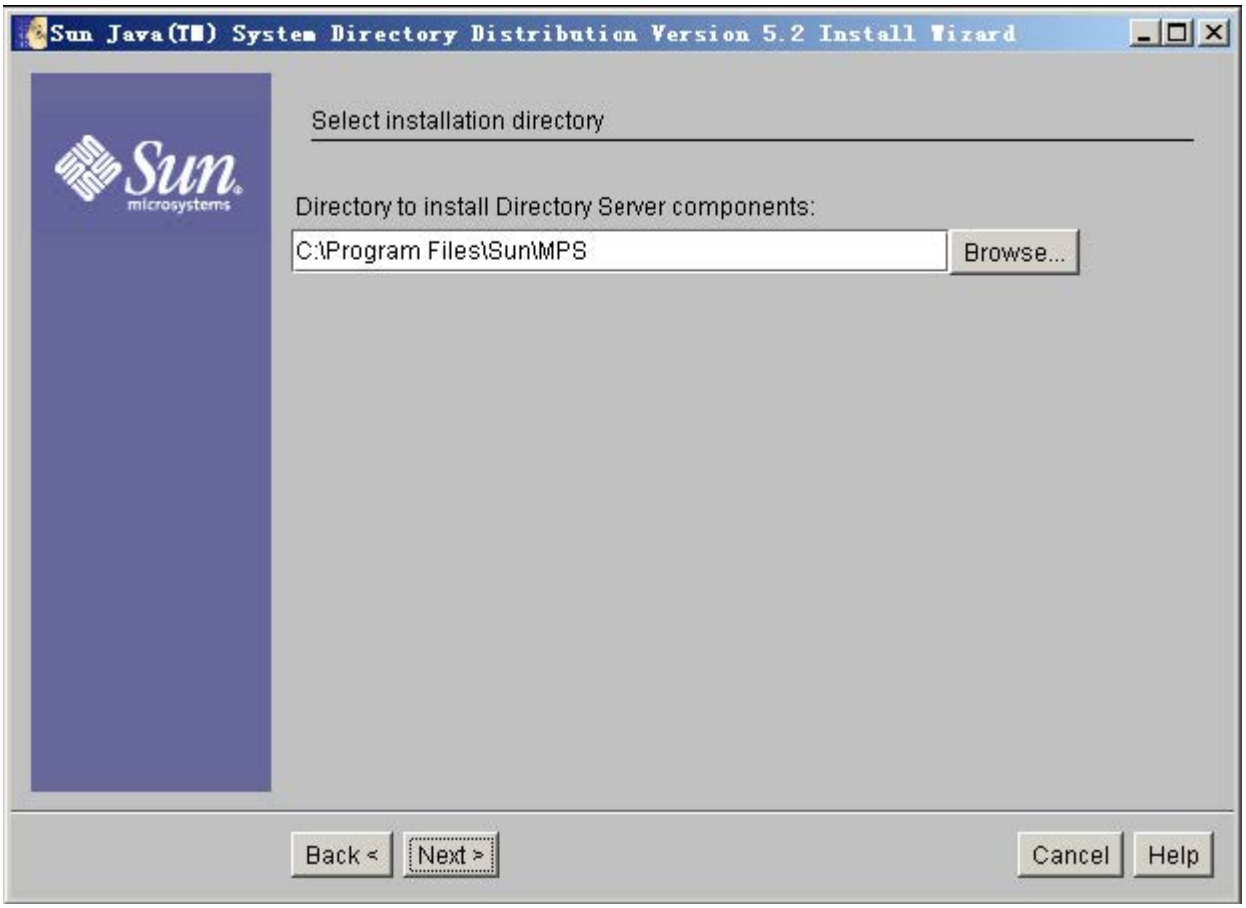
6. Select the **Sun Java ™ System Servers** check box and click **Next**.



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



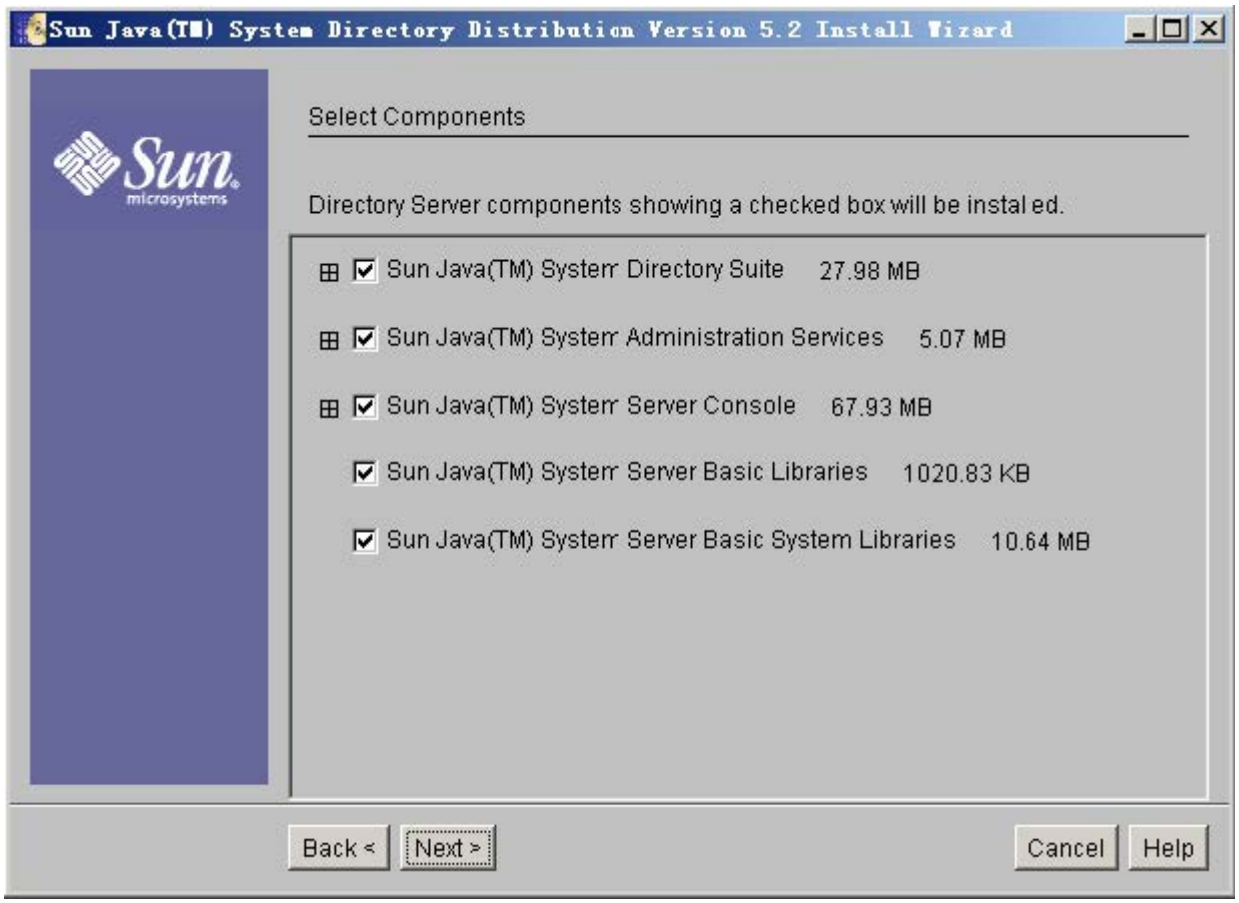
8. Specify the desired installation directory and click **Next**.



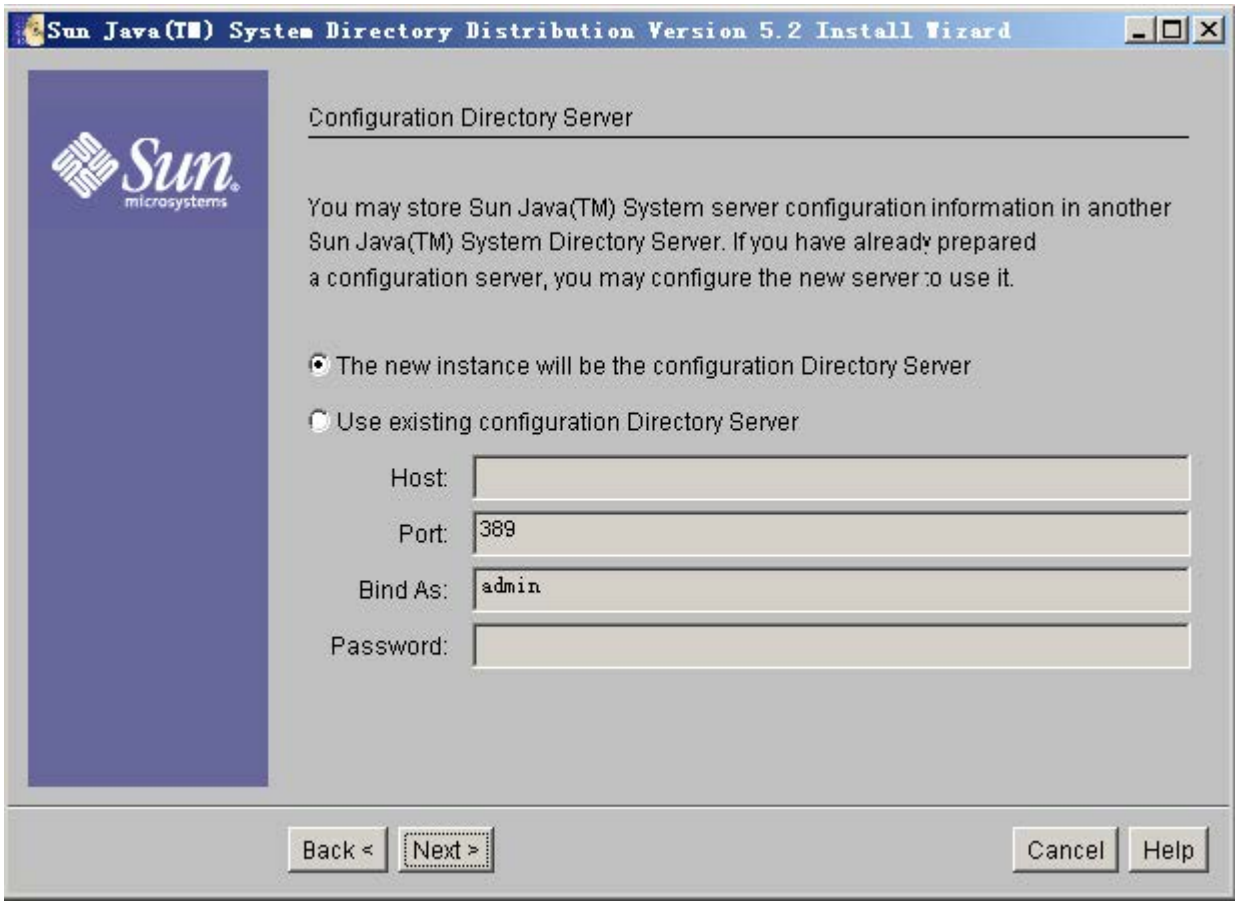
10. It prompts the following window. And you can click **Create Directory** to create the directory or click **Choose New** to select another path.



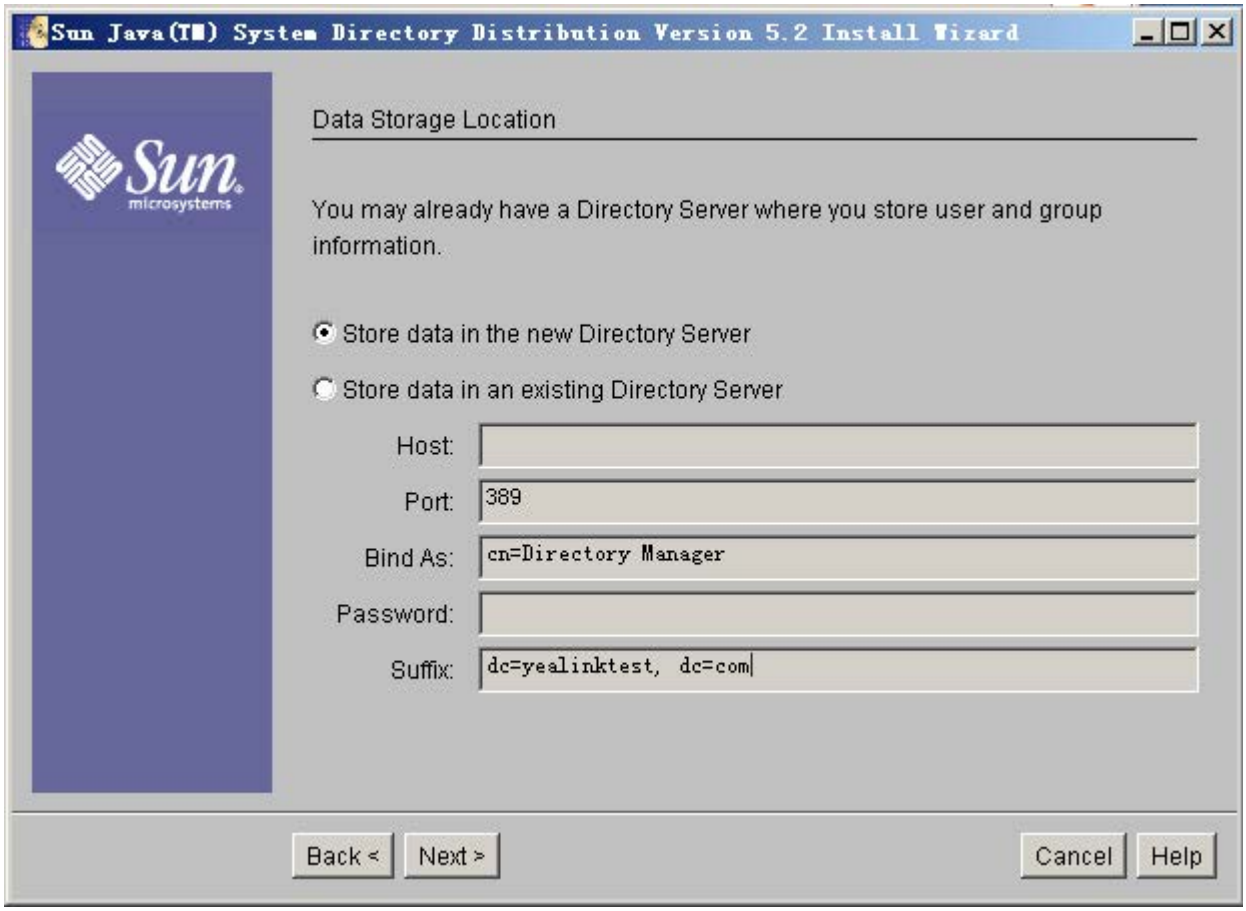
9. Select the desired installation components and click **Next**.



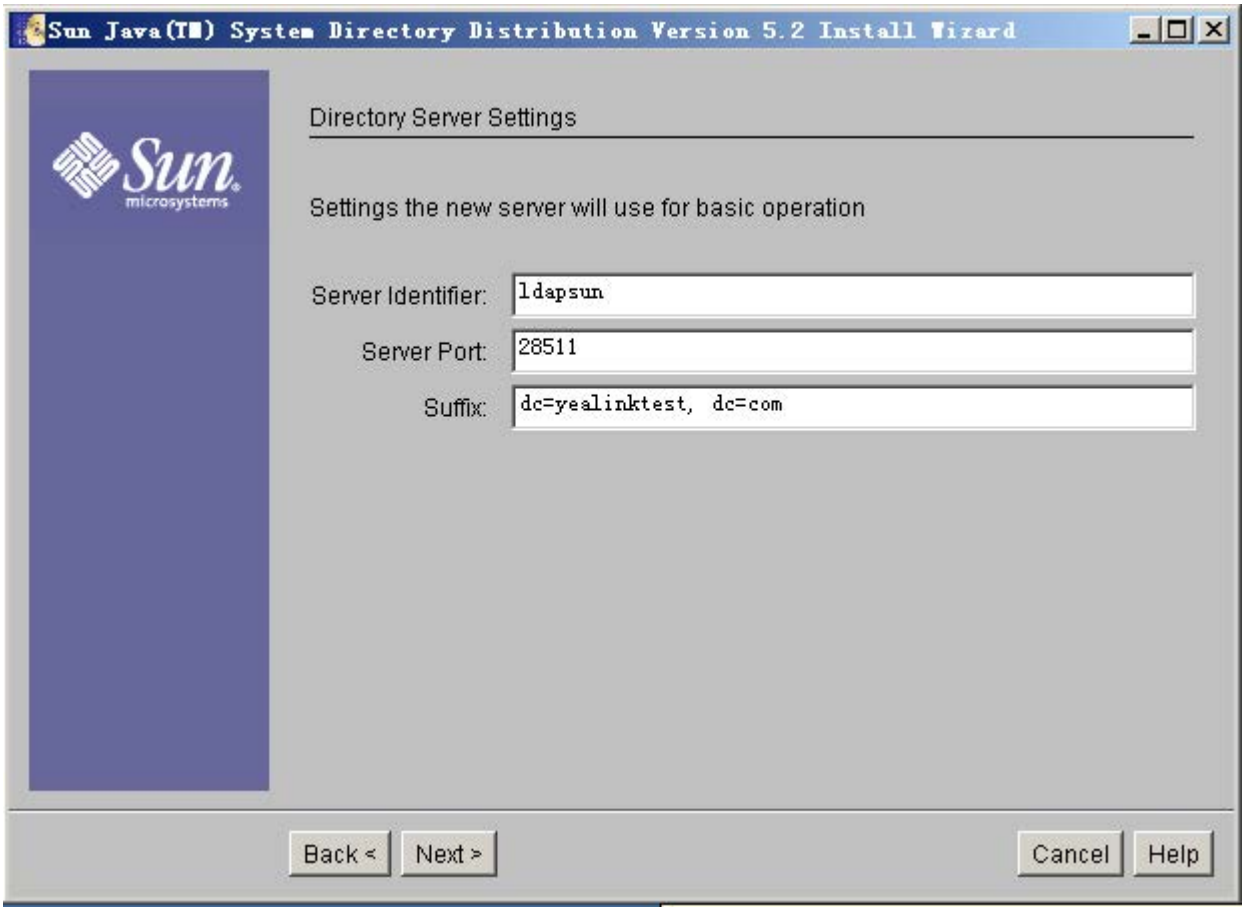
10. Select **The new instance will be the configuration Directory Server** check box and click **Next**.



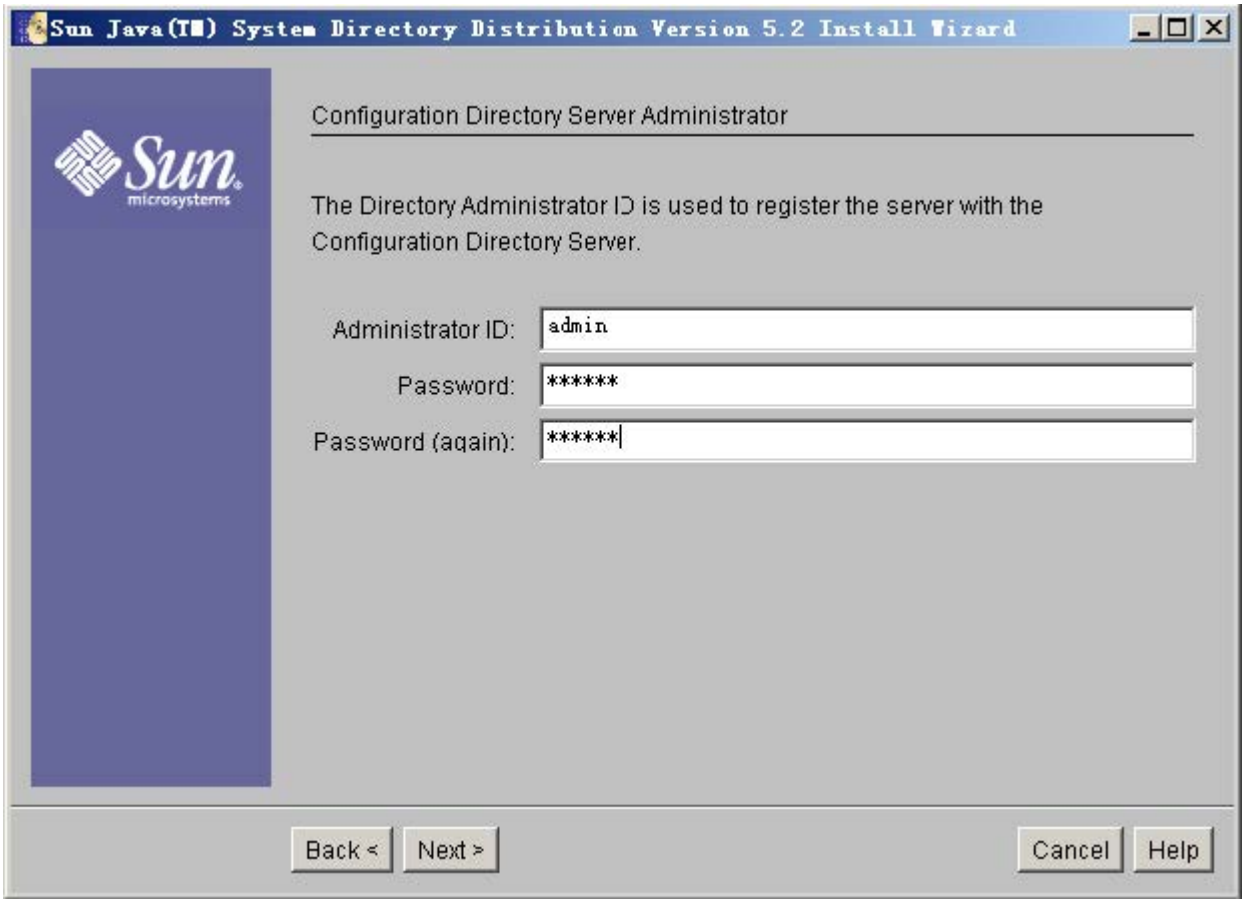
11. Select the **Store data in the new Directory Server** check box and click **Next**.



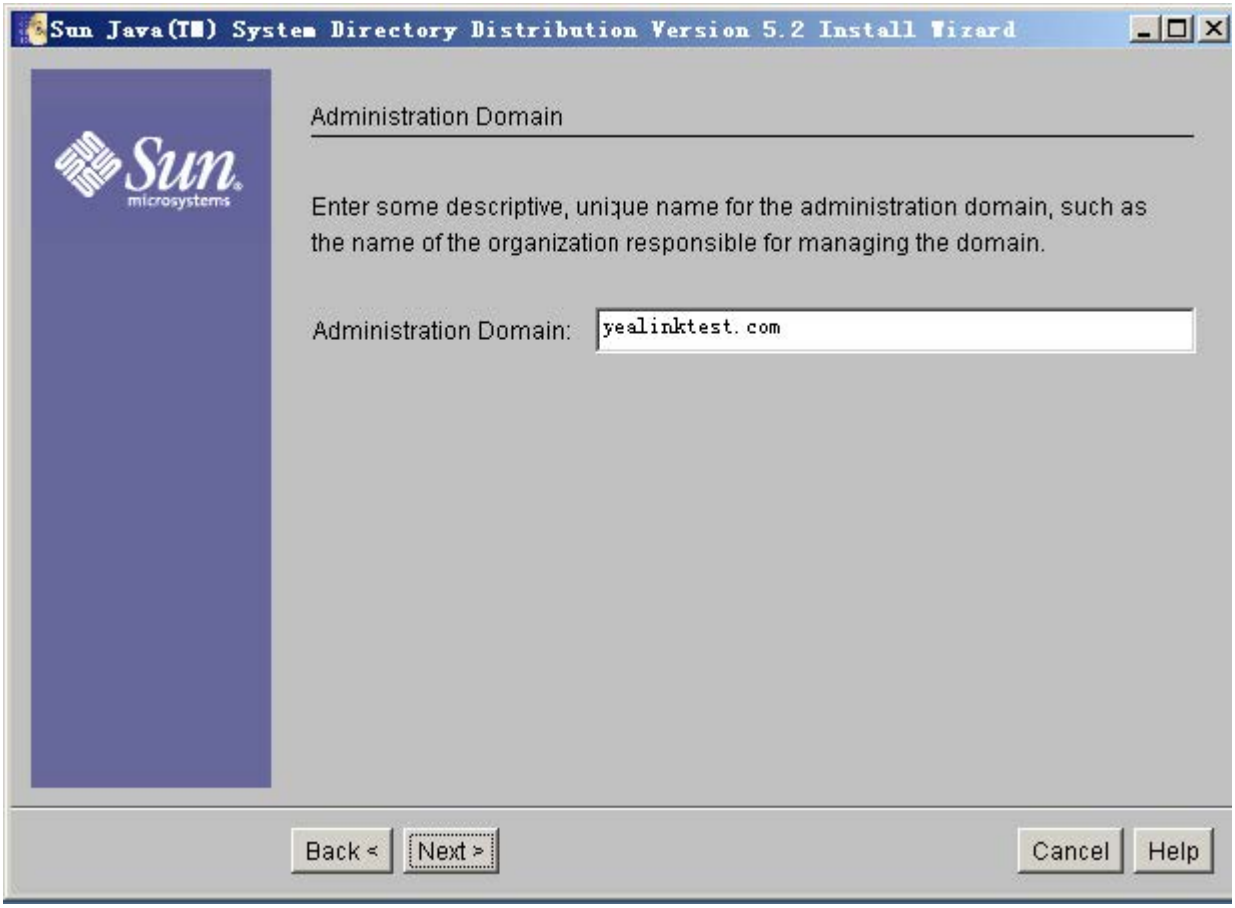
12. Enter the value "ldapsun" in the **Server Identifier** field and keep the default values in the other two fields. And then click **Next**.



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

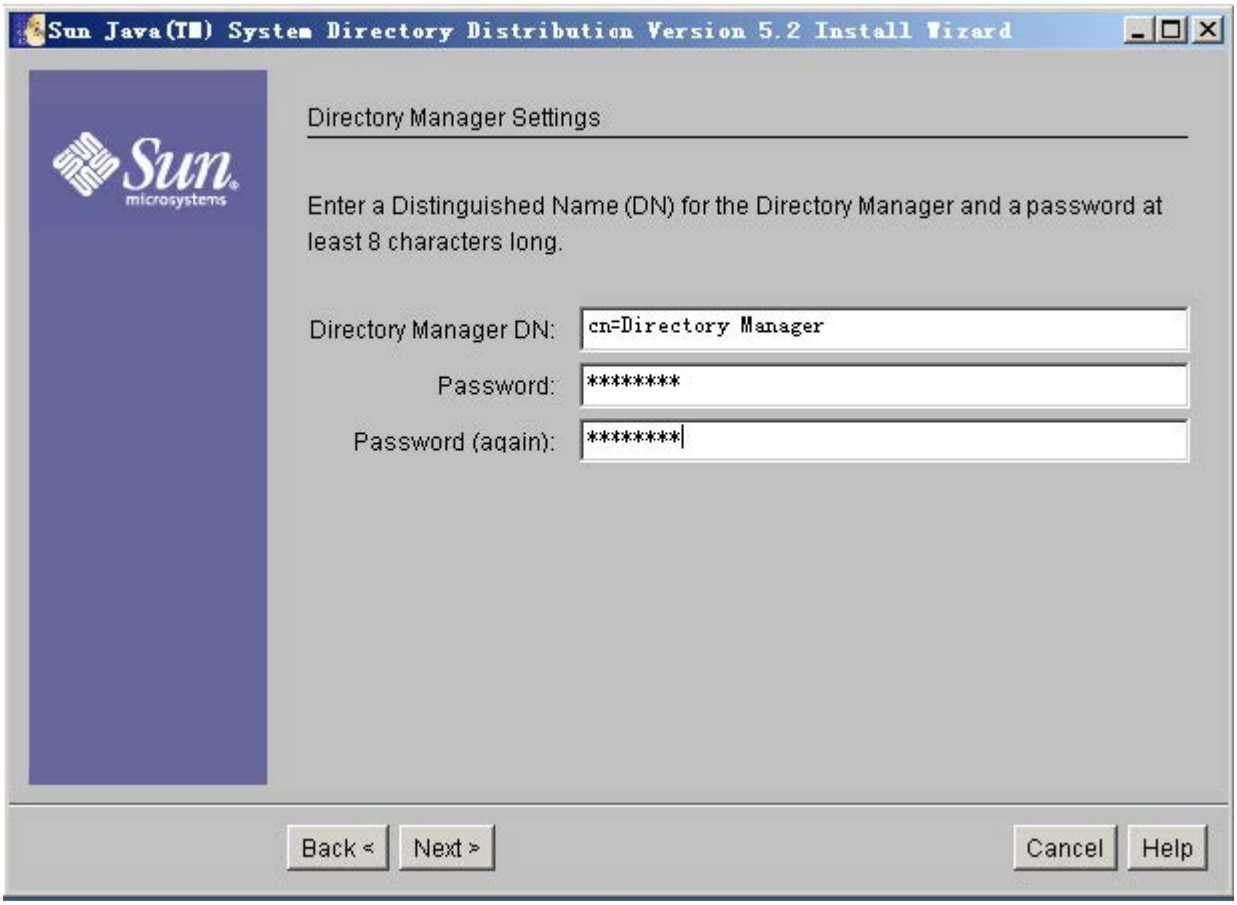


14. Follow the default setting and click **Next**.

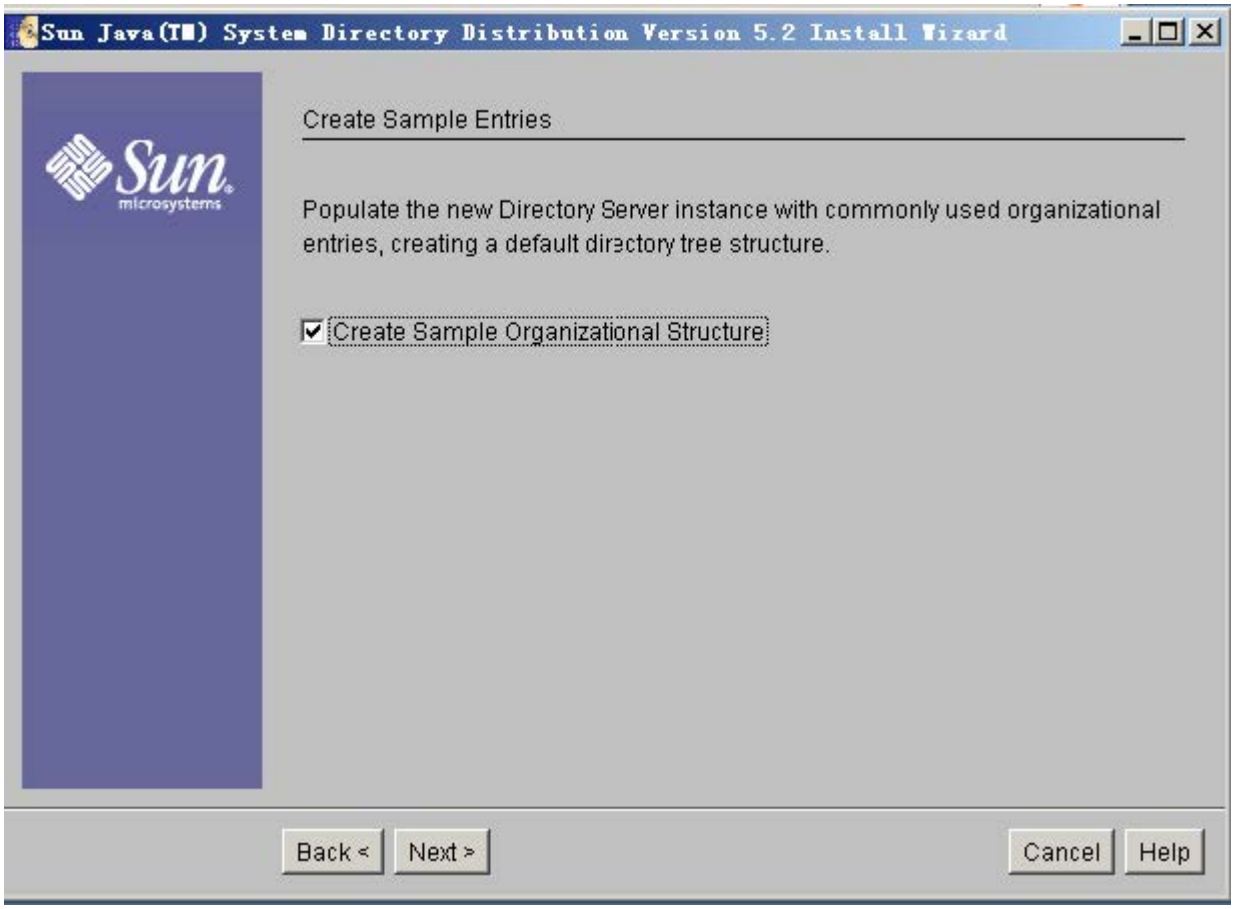


15. Configure the password for the Directory Manager and click **Next**.

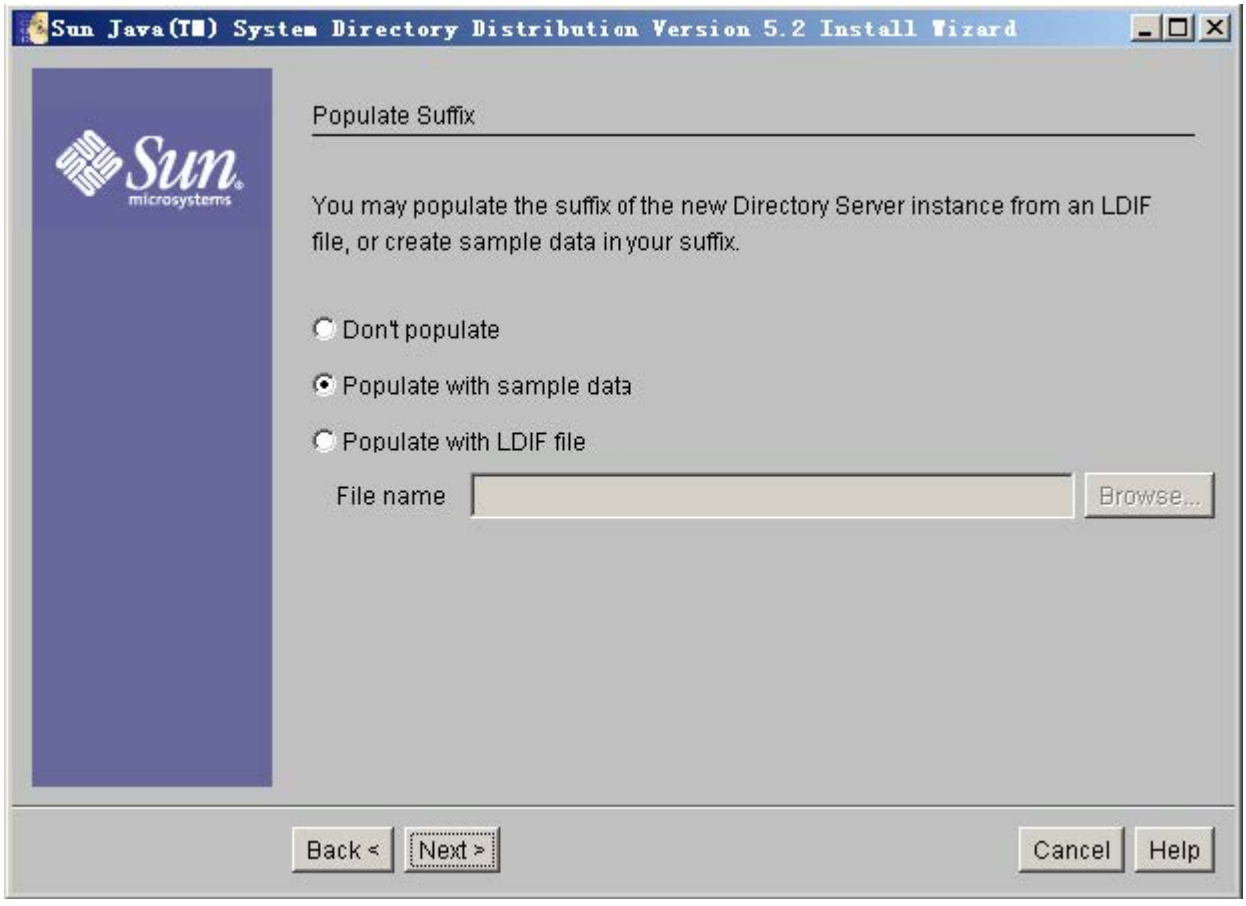
    The password must be at least 8 characters long.



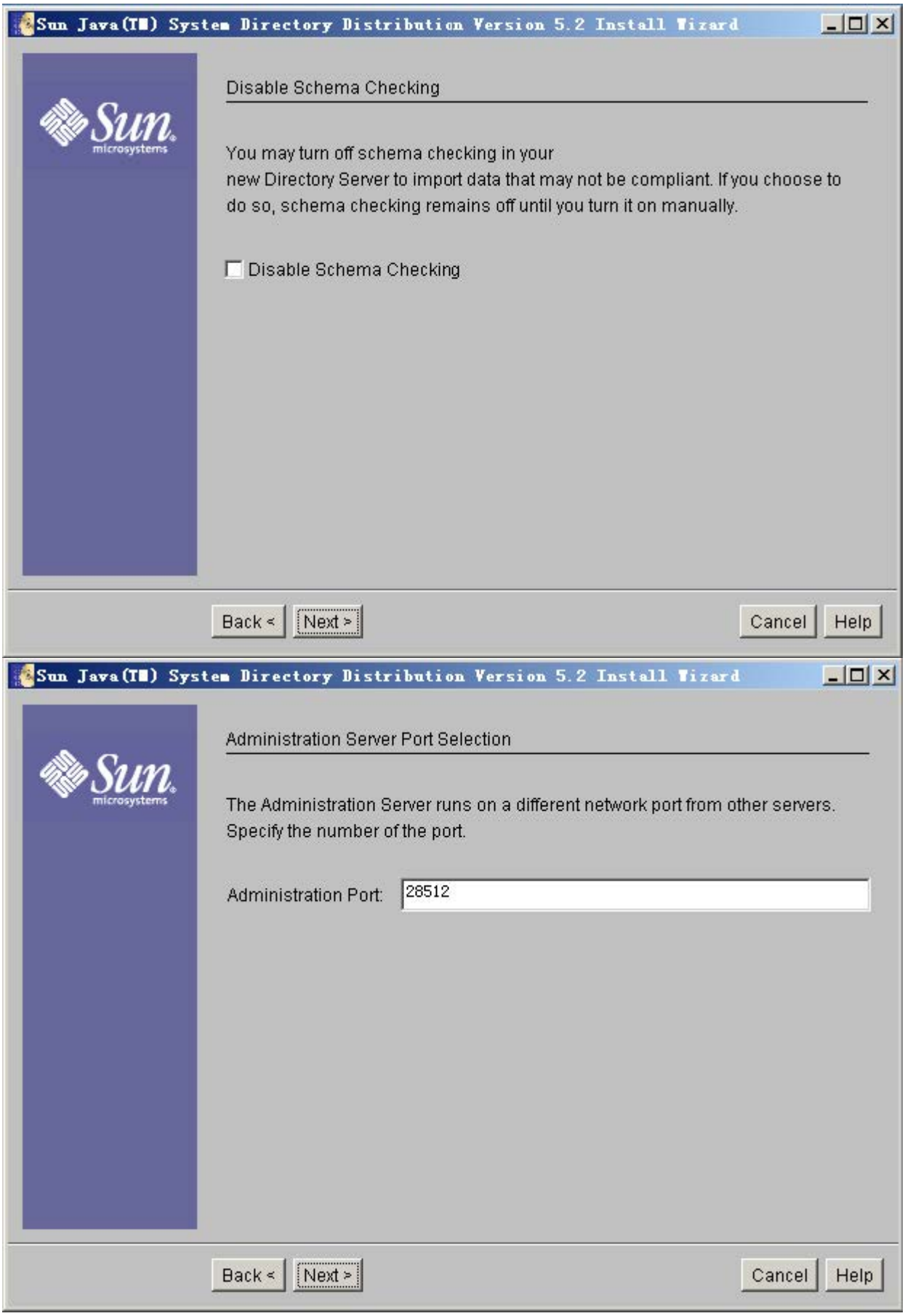
16. Select the **Create Sample Organizational Structure** check box and click **Next**.



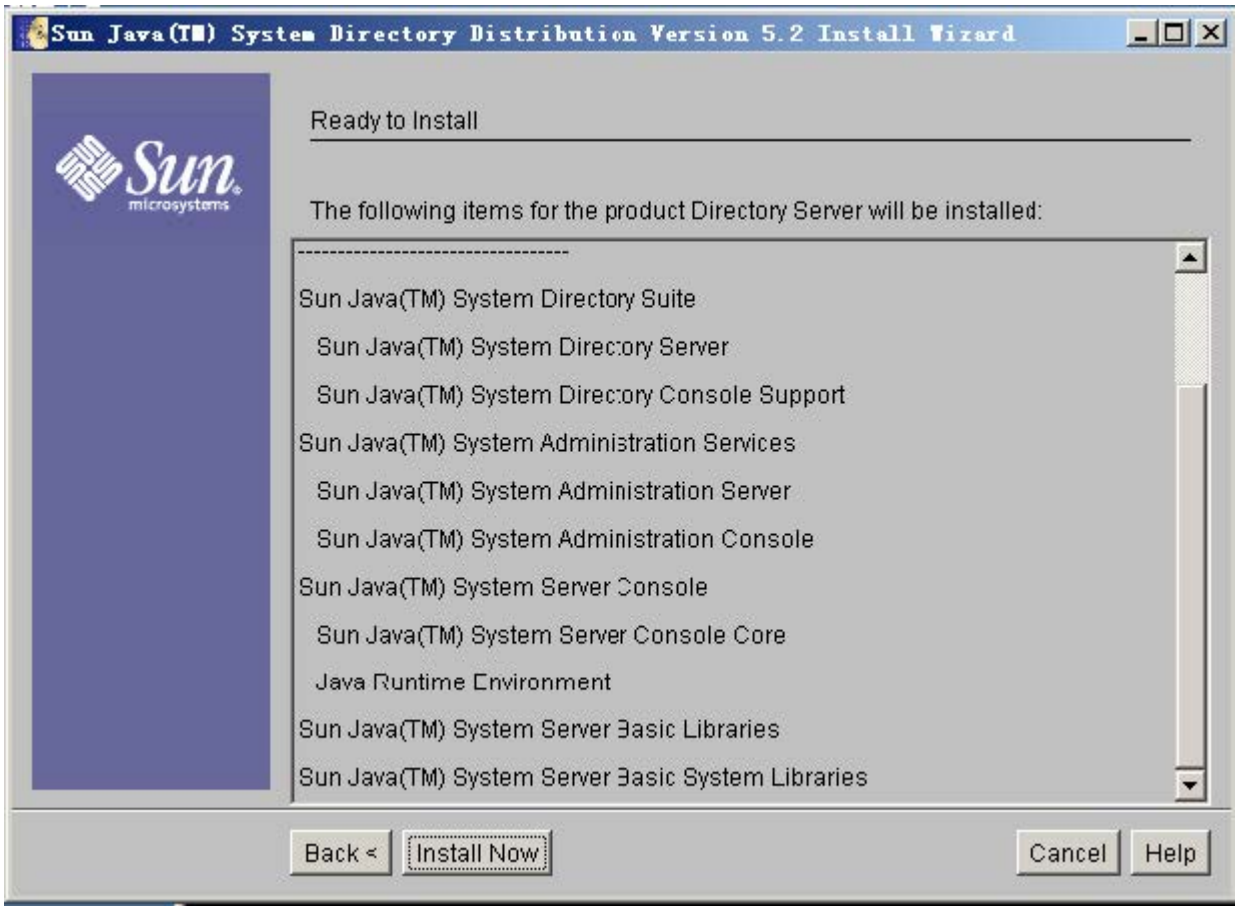
17. Select the **Populate with sample date** check box and click **Next**.



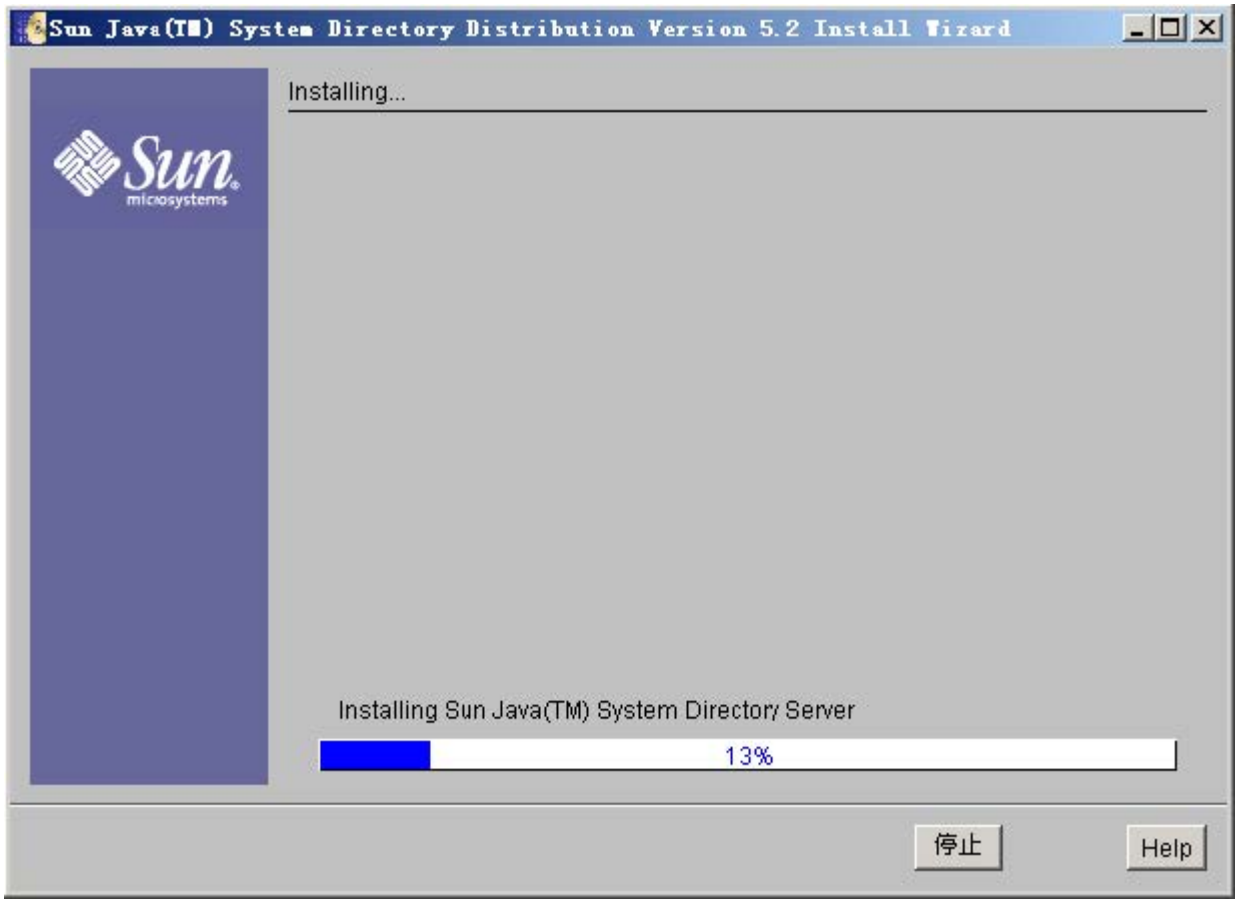
18. Follow the default settings and click **Next** for the following two steps.



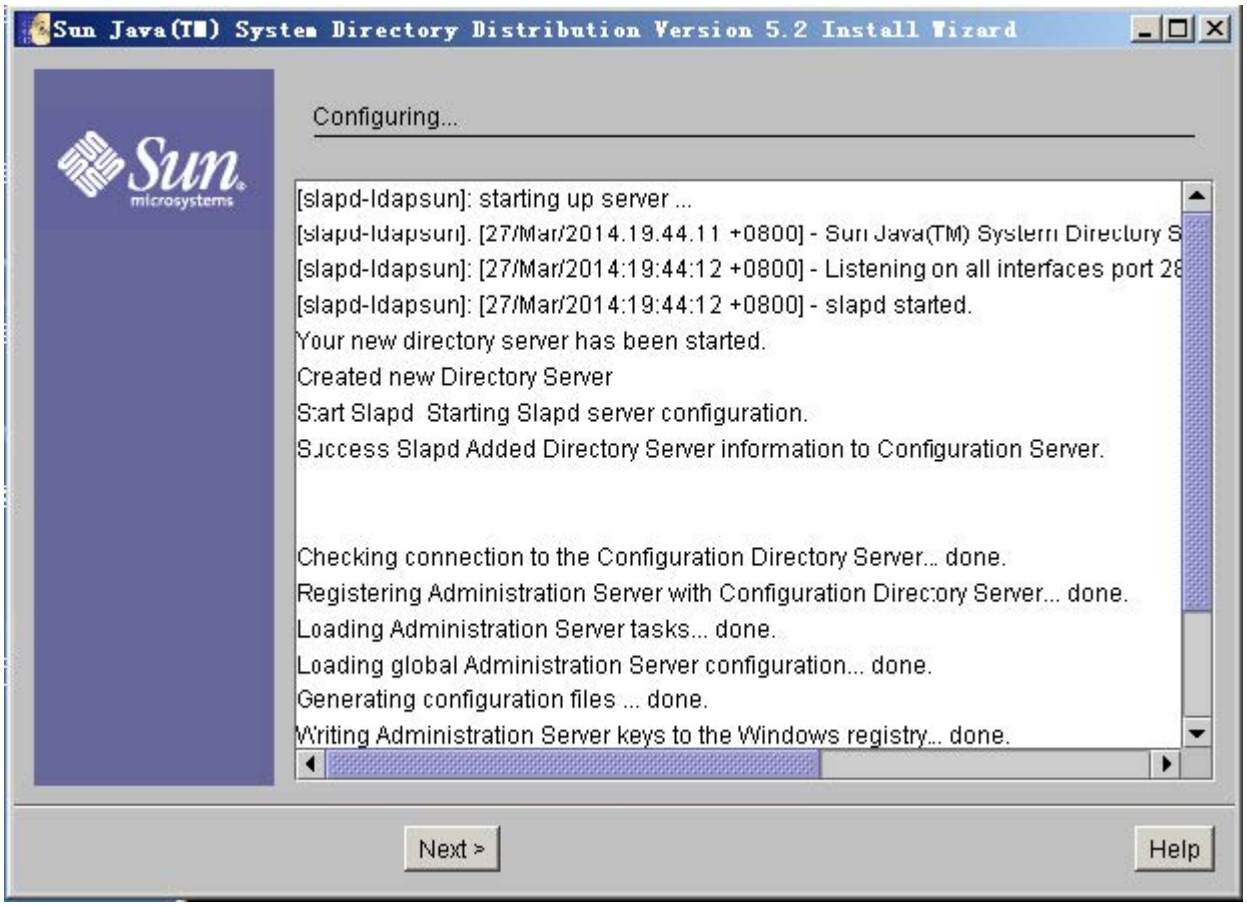
19. View the items to be installed and click **Install Now**.



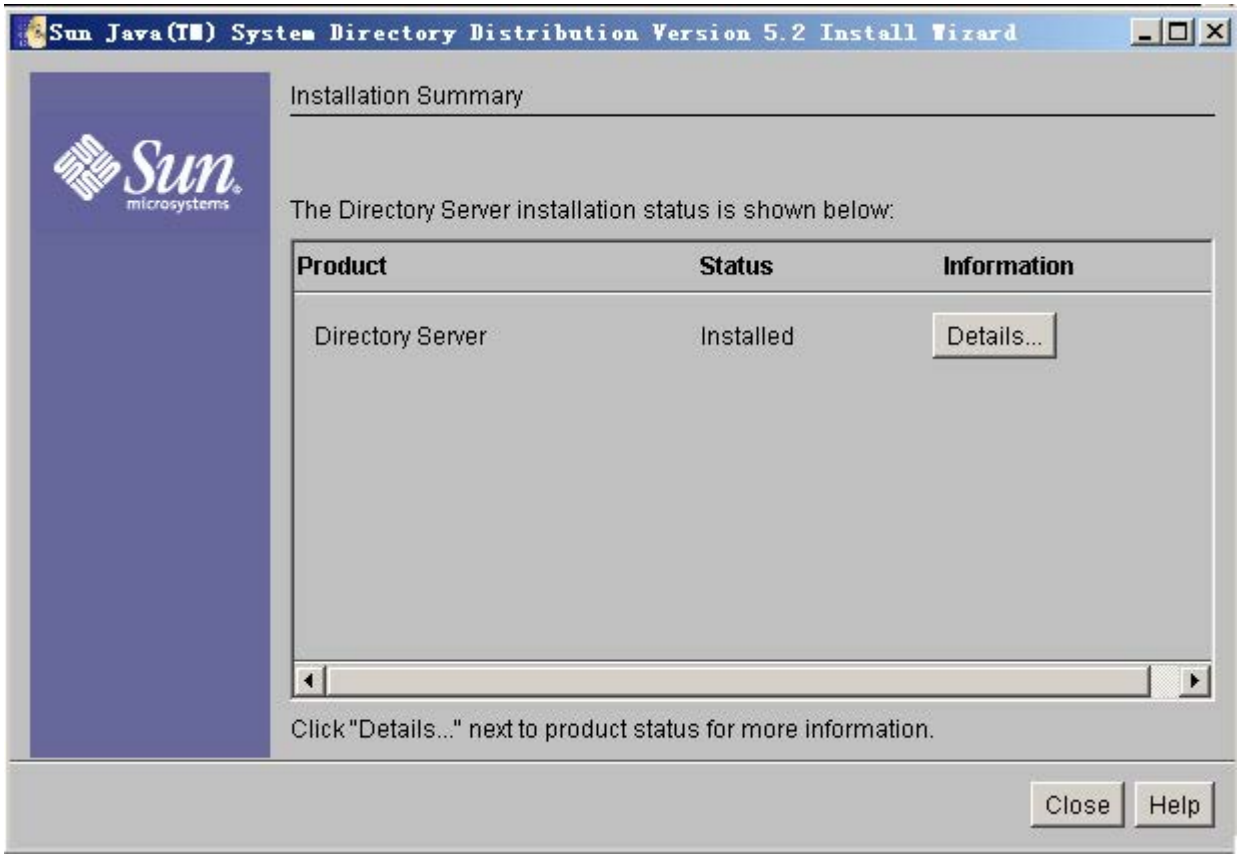
21. The installation progress is shown below:



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.

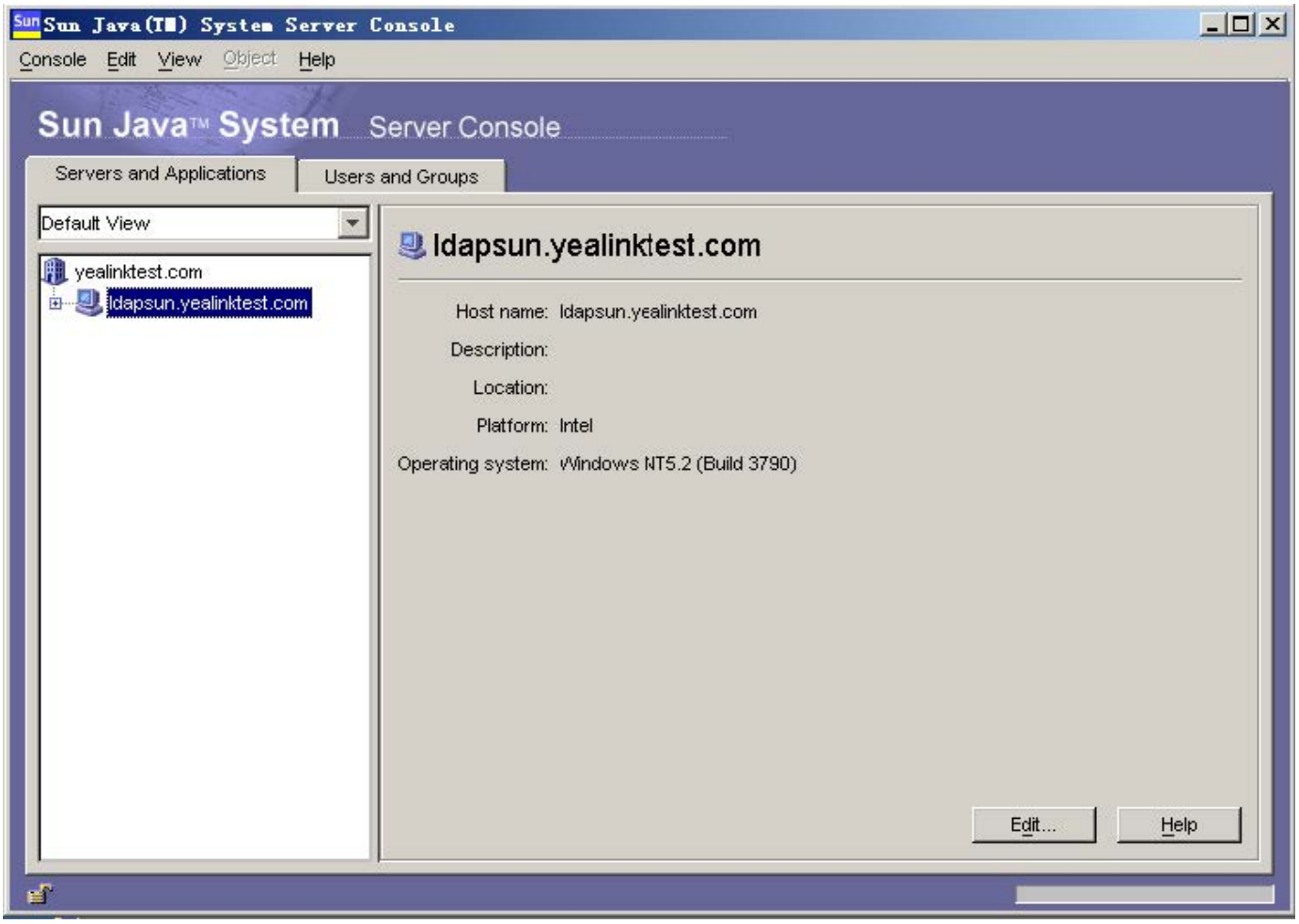
To add an entry to the Directory Server:

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 the **Password** field, respectively.

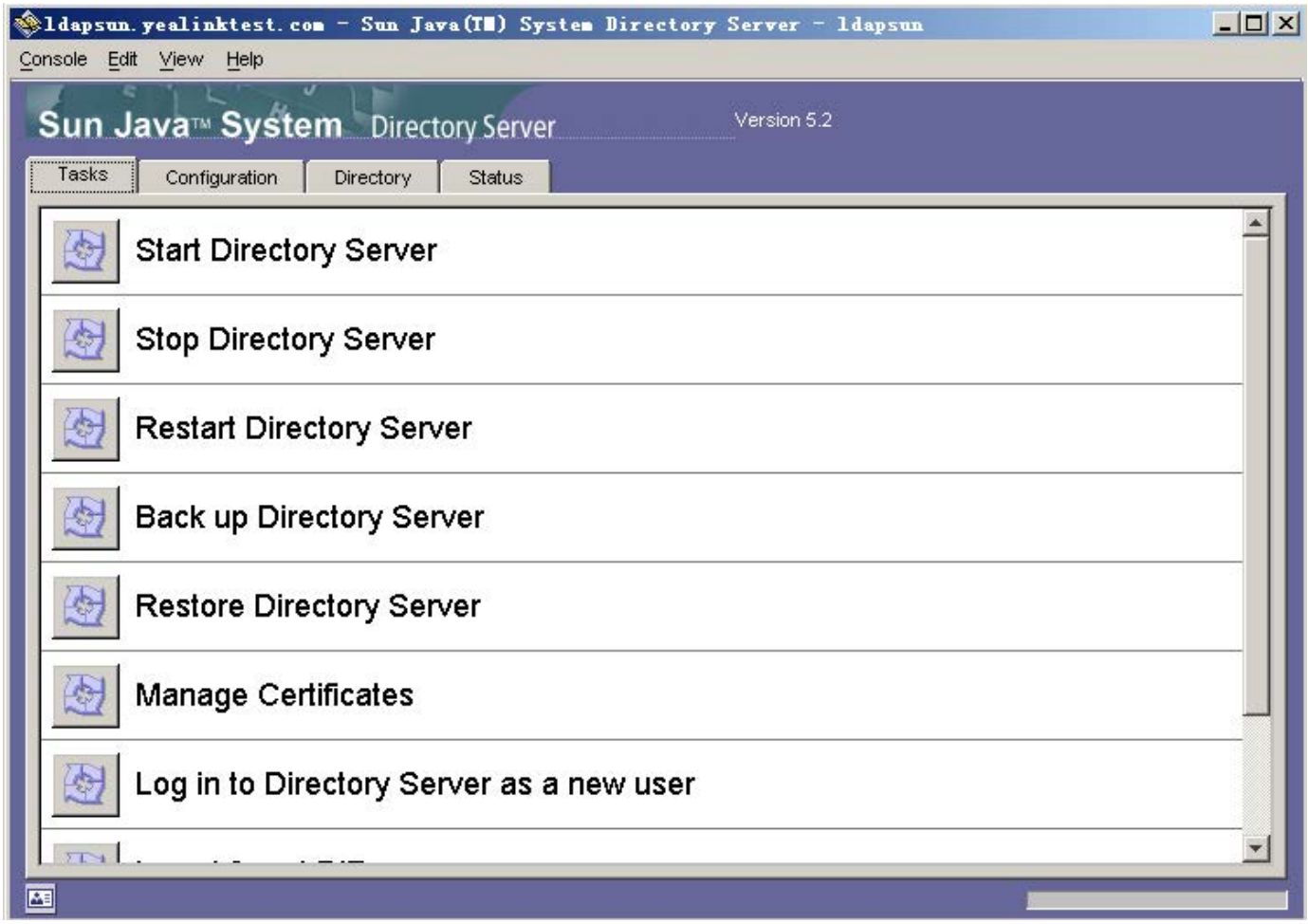


> The system default administrator is **cn=Directory Manager,** and its password, which must be at least 8 characters long, has already been set during the installation process.

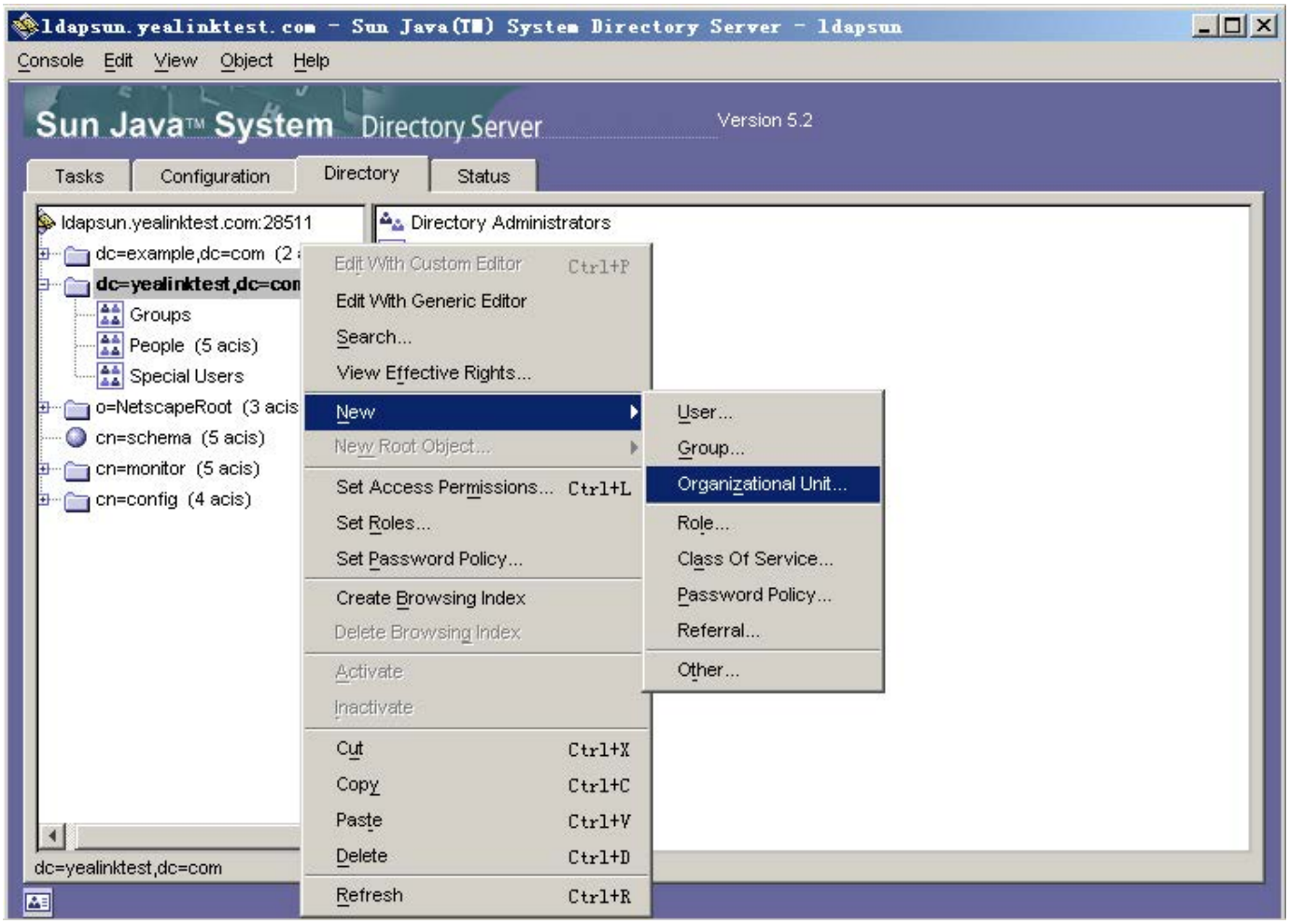
Then click **OK** to enter the home page.



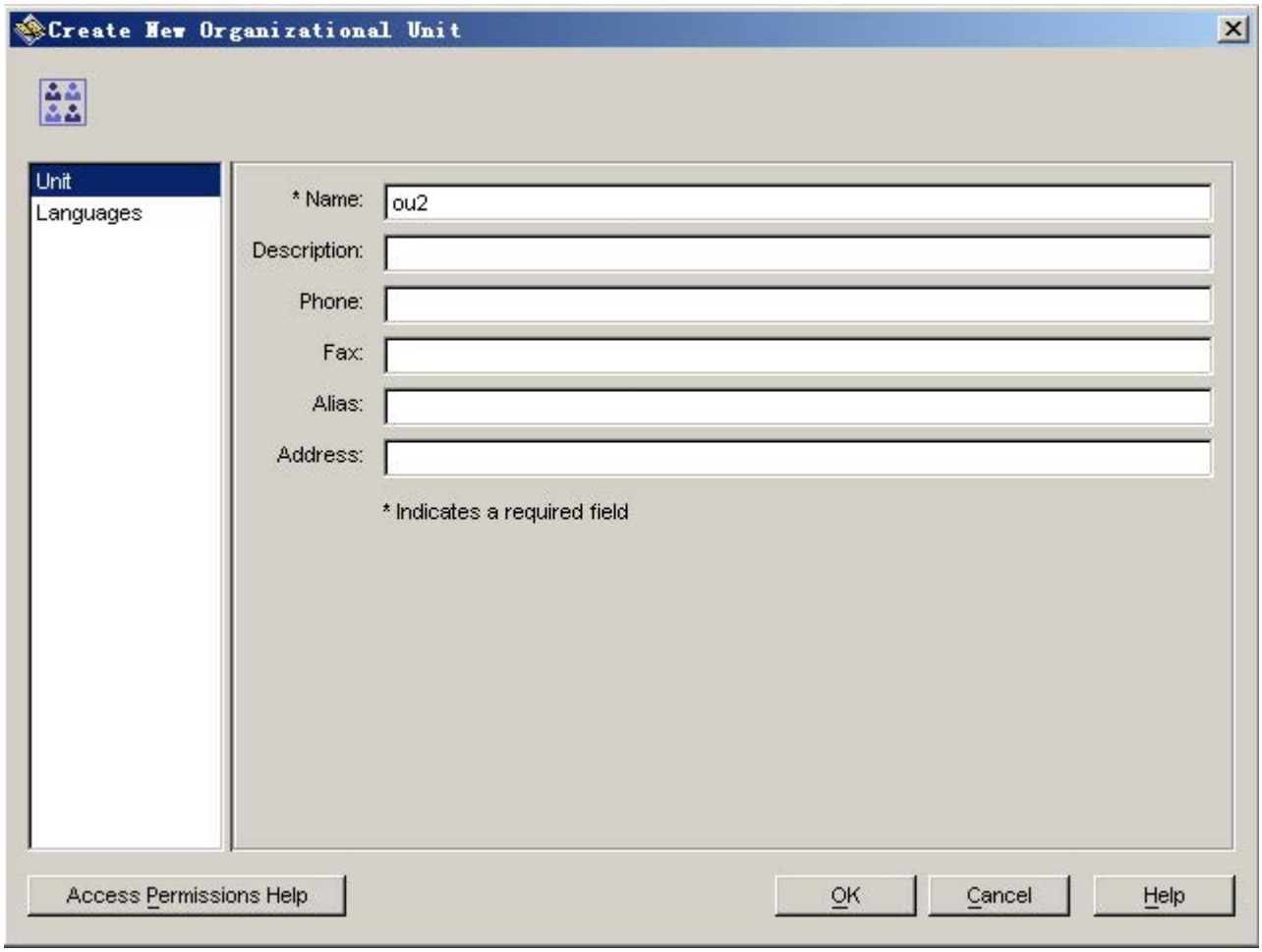
2. Double-click **ldapsun.yealinktest.com** > **Server Group** > **Directory Server(ldapsun)**. It will enter the Directory Tasks interface.



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

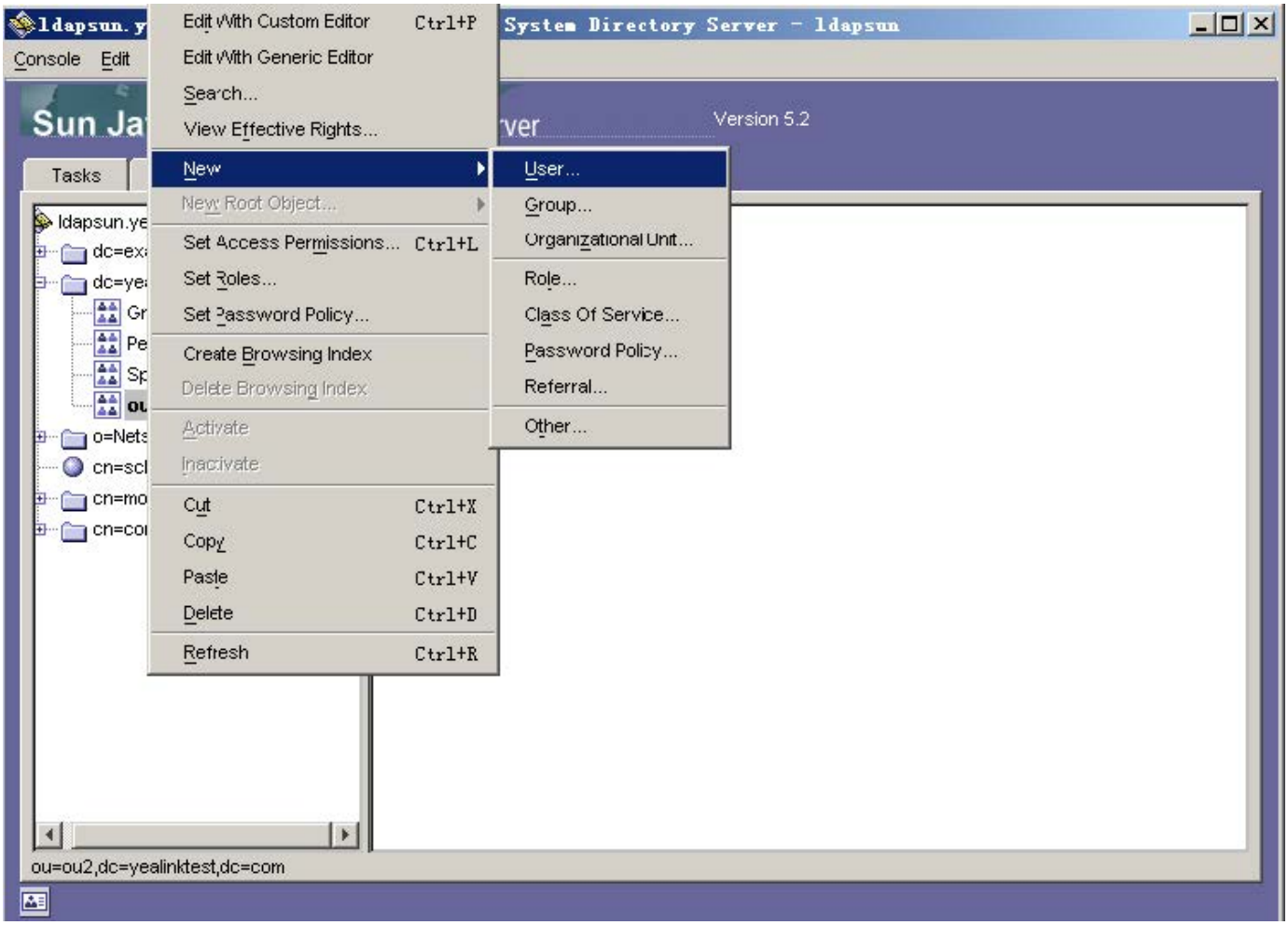


5. Enter the desired name of the organizational unit.

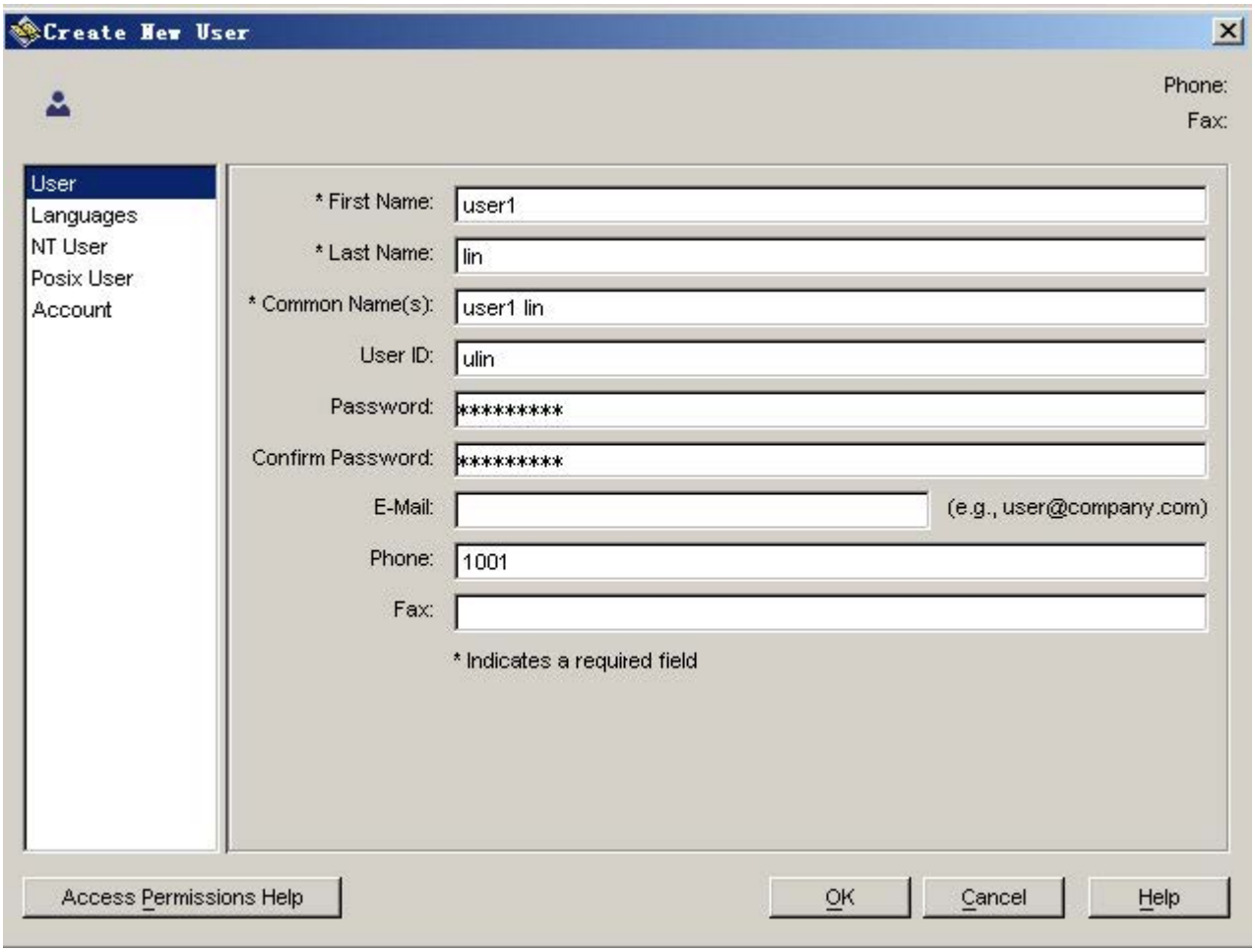


6. Click **OK** to accept the change.

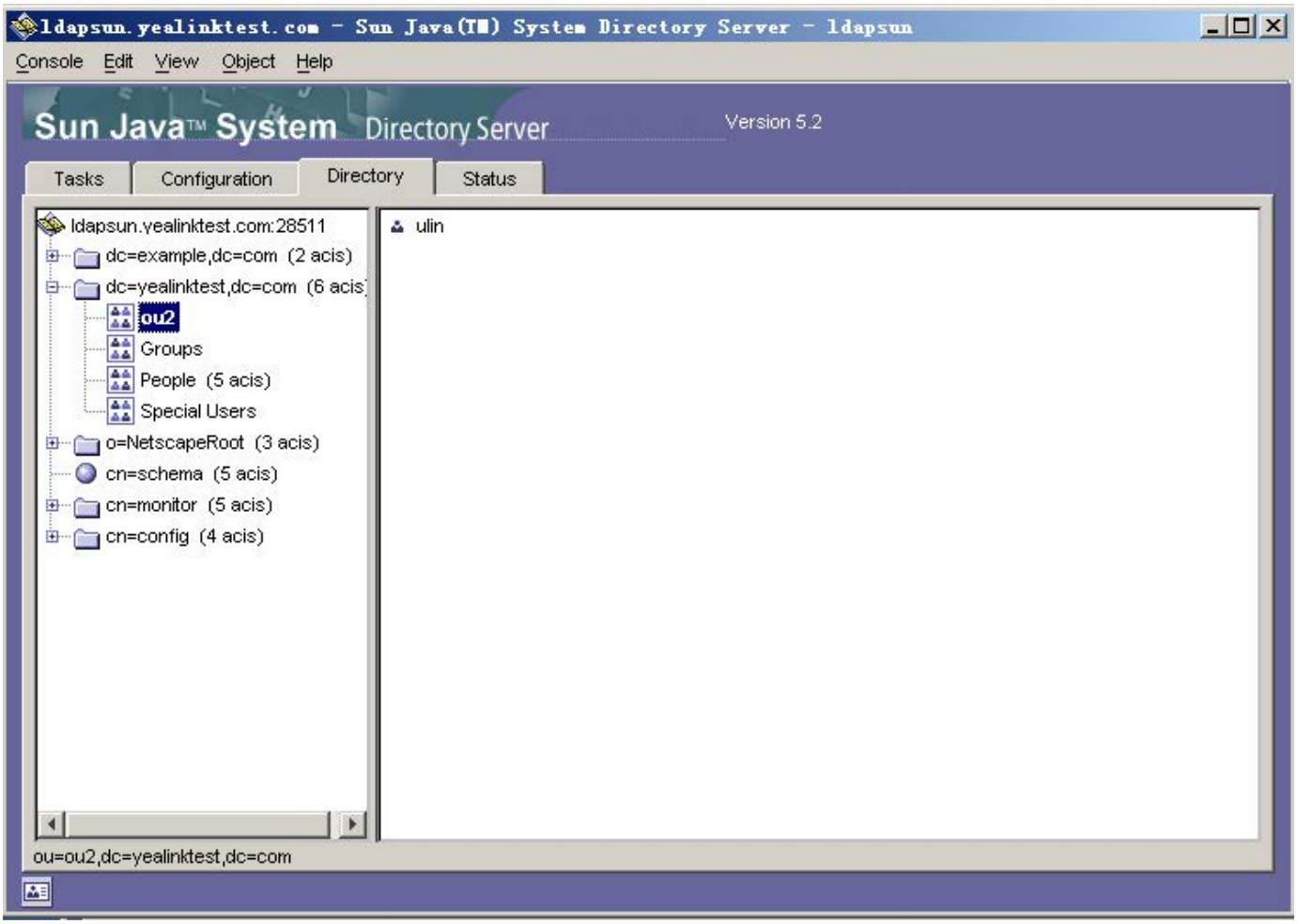
7. Select and right-click the organizational unit created above, and then select **New** > **User**.



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:

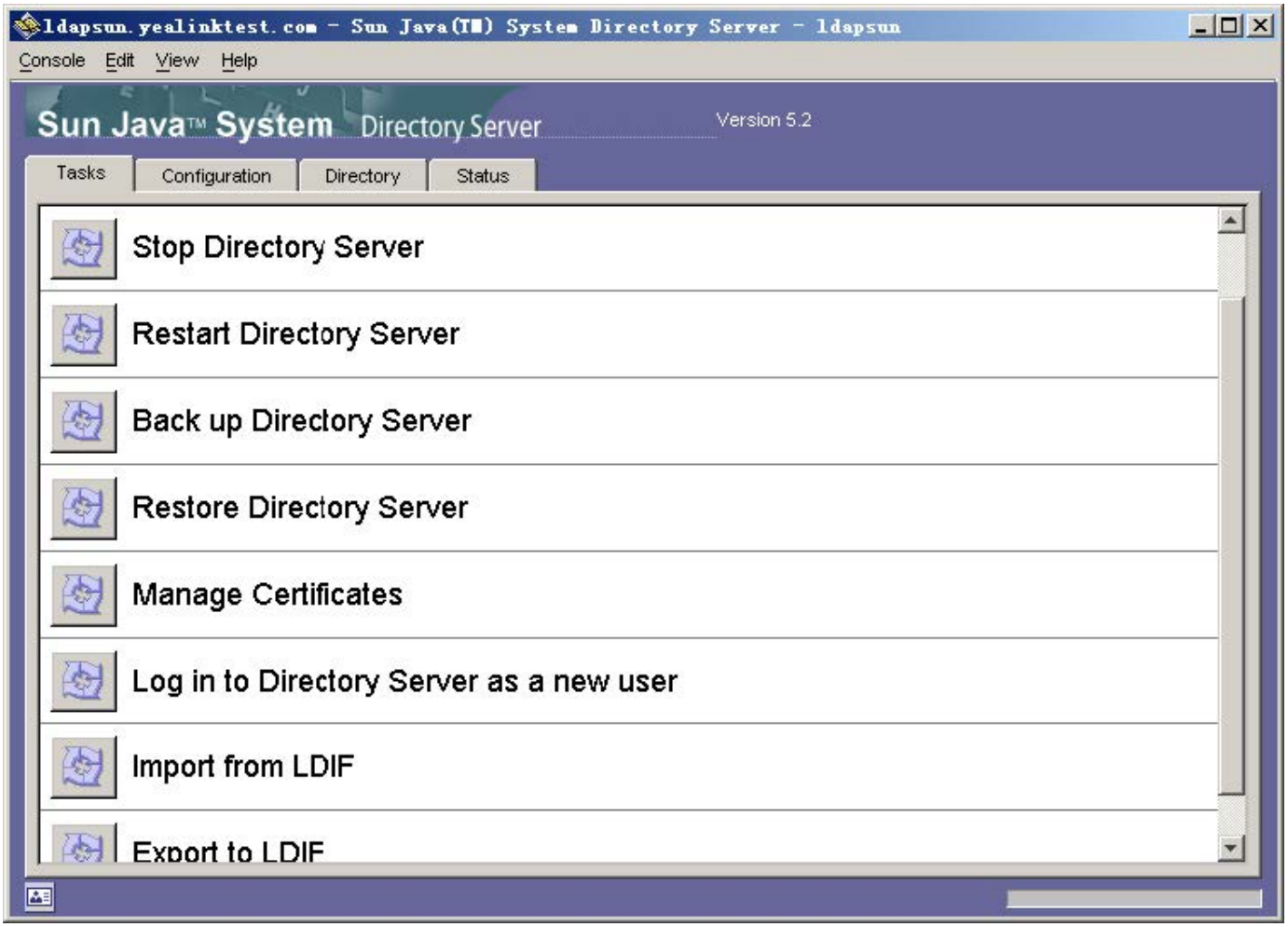
```
##Create a new organizational unit##
dn: ou=ou3,dc=yealinktest,dc=com
ou: ou3
objectClass: top
objectClass: organizationalunit
creatorsname: cn=directory manager
modifiersname: cn=directory manager
parentid: 1
entryid: 15
entrydn: ou=ou3,dc=yealinktest,dc=com

##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
```

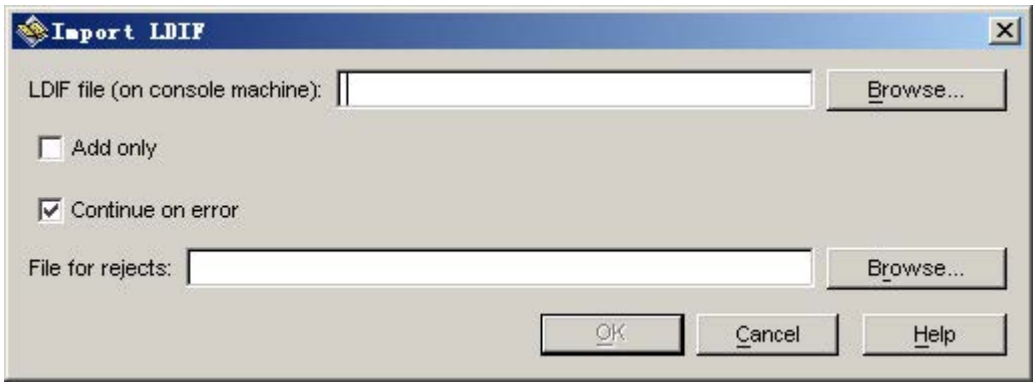
To import the test.ldif file:

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

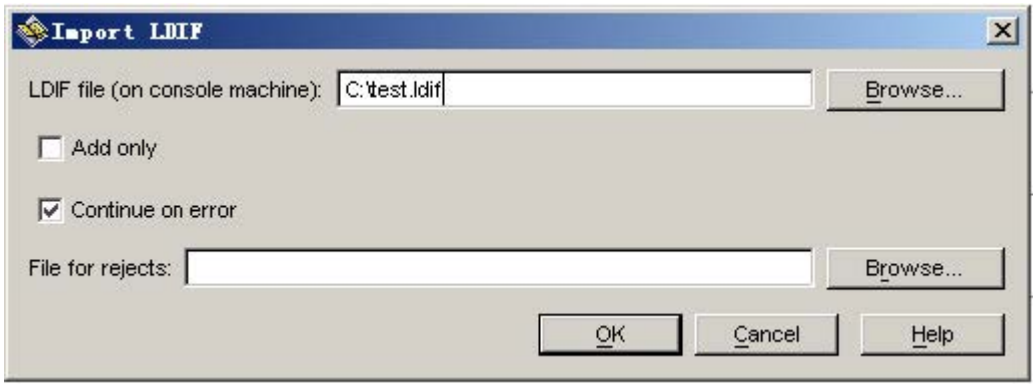
It will enter the Directory **Tasks** interface.



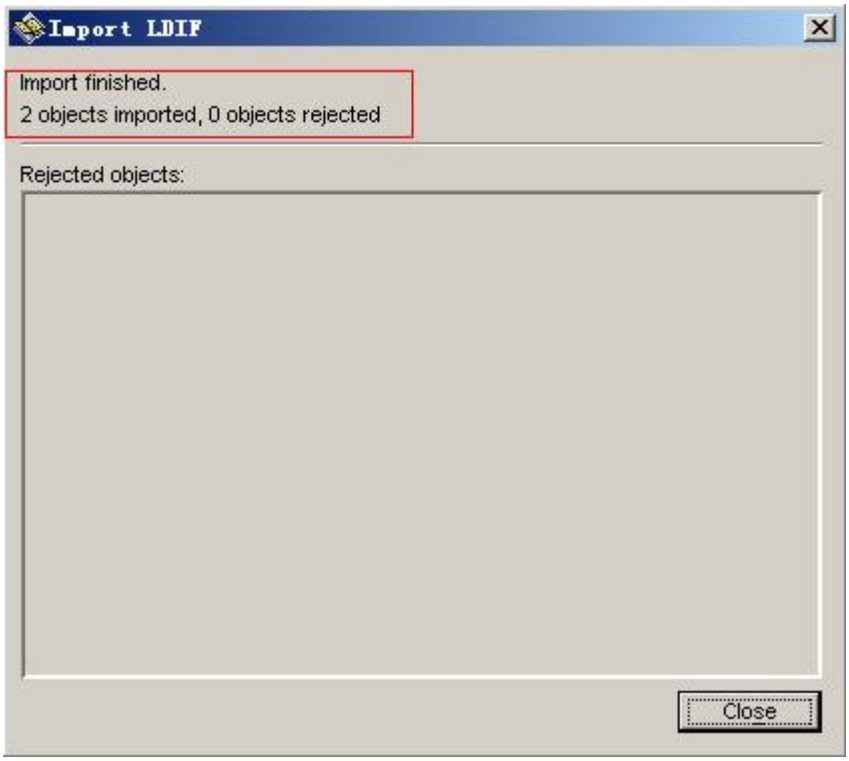
2. Click **Import from LDIF**.



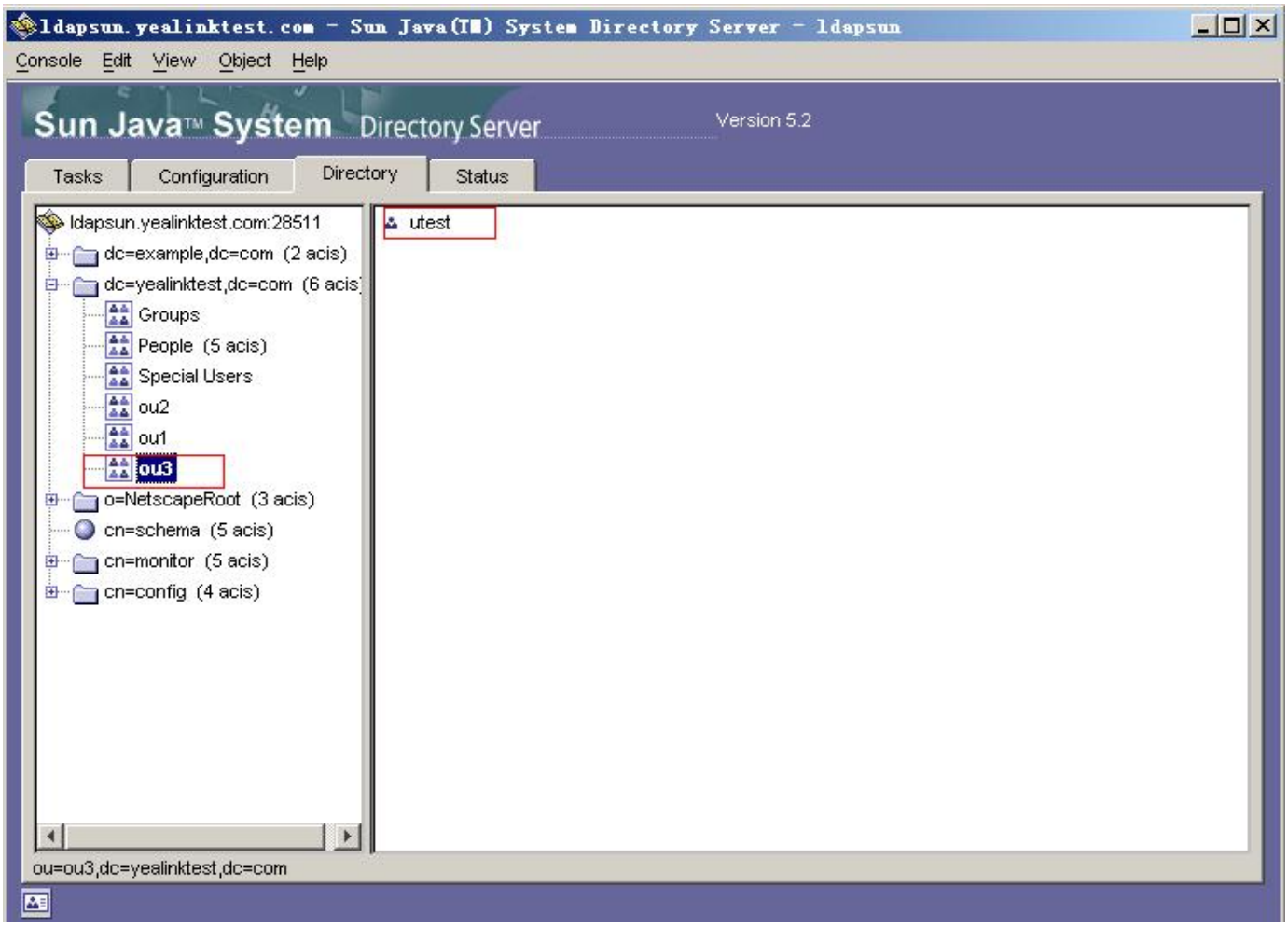
3. Click **Browse** to locate the test.ldif file from your local system, and then click **OK**.



5. 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.



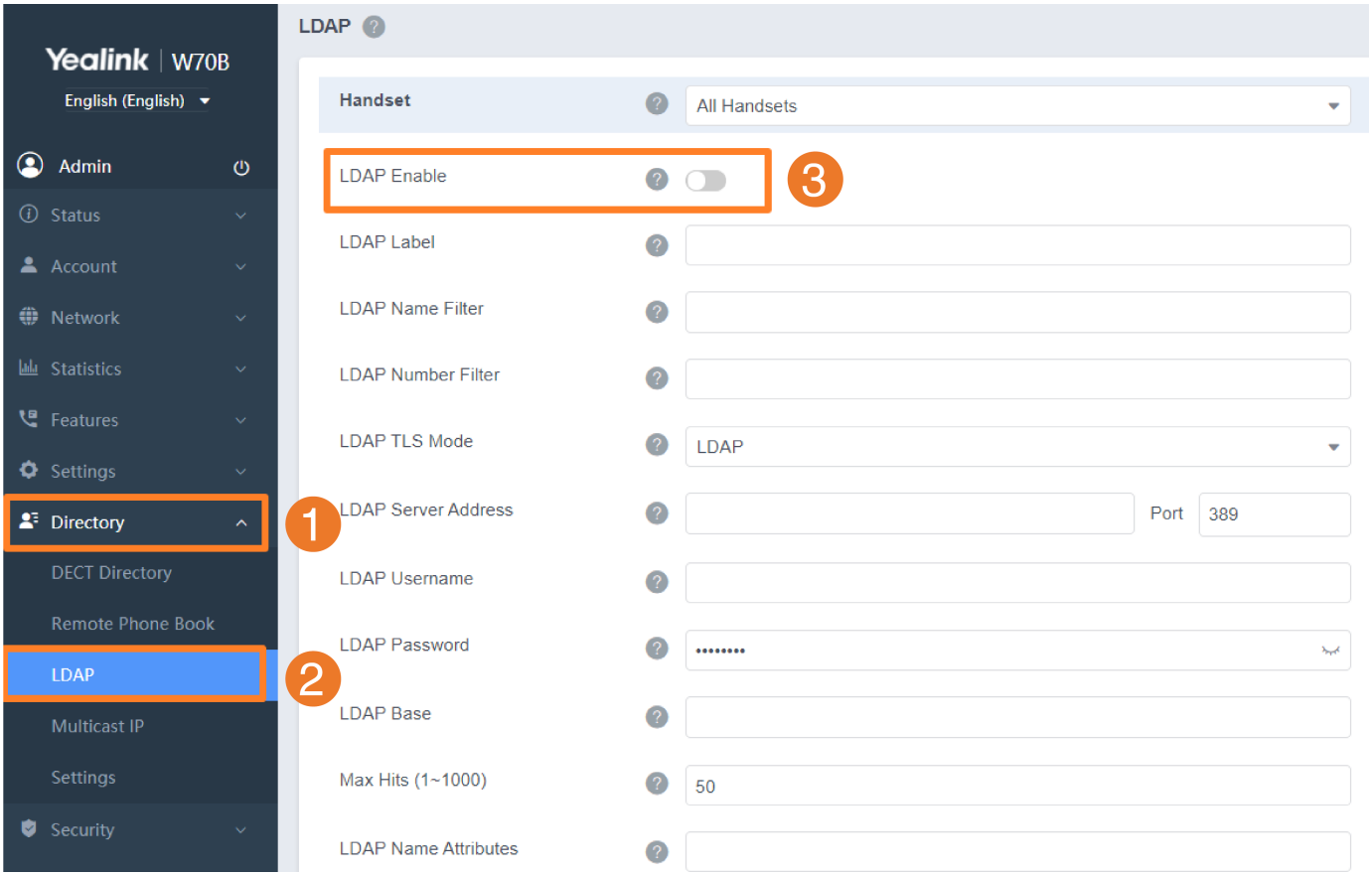
7. You can view the imported organizational unit (e.g., ou3) and user (e.g., uid=utest) under the path: **Directory** > **dc=yealinktest,dc=com (6 acis)**.



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

Parameter	Permitted Values	Default	Description
ldap.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the LDAP feature.
ldap.name_filter	String within 99 characters	Blank	It configures the search criteria for LDAP contact names lookup. The "*" symbol in the filter stands for any character.

			The "%" symbol in the filter stands for the name entered by the user. **Example:** 1. ldap.name_filter = (|(cn=%)(sn=%)) When the cn or sn of the LDAP contact matches the entered name, the record will be displayed on the phone screen. 2. ldap.name_filter = (&(cn=*)(sn=%)) When the cn of the LDAP contact is set and the sn of the LDAP contact matches the entered name, the records will be displayed on the phone screen. 3. ldap.name_filter = (!(cn=%)) When the cn of the LDAP contact does not match the entered name, the records will be displayed on the phone screen.
ldap.number_filter	String within 512 characters	Blank	It configures the search criteria for LDAP contact numbers lookup. The "*" symbol in the filter stands for any number. The "%" symbol in the filter stands for the number entered by the user. **Example:** 1. ldap.number_filter = (|(telephoneNumber=%)(mobile=%)(ipPhone=%)) When the number of the telephoneNumber, mobile or ipPhone of the contact record matches the search criteria, the record will be displayed on the phone screen. 2. ldap.number_filter = (&(telephoneNumber=*)(mobile=%)) When the telephoneNumber of the LDAP contact is set and the mobile of the LDAP contact matches the entered number, the record will be displayed on the phone screen.
ldap.tls_mo	**0**-LDAP—The unencrypted	0	It configures the connection mode between the LDAP server and the phone.

de	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).		
ldap.host	IP address or domain name	Blank	It configures the IP address or domain name of the LDAP server.
ldap.port	Integer from 1 to 65535	389 (LDAPS: 636)	It configures the port of the LDAP server.
ldap.base	String within 512 characters	Blank	It configures the LDAP search base, which corresponds to the location of the LDAP phonebook from which the LDAP search request begins. The search base narrows the search scope and decreases directory search time. **Example:** ldap.base = dc=yealink,dc=cn
ldap.u	String within 512	Bl	It configures the user name used to log into the LDAP

ser	characters	ank	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
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 in. Otherwise, you will need to provide the password to log into the LDAP server.
ldap.max_hits	Integer from 1 to 1000	50	It configures the maximum number of search results to be returned by the LDAP server.
ldap.name_attr	String within 512 characters	Blank	It configures the name attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple name attributes separated by spaces. **Example:** ldap.name_attr = cn sn This requires the "cn" and "sn" attributes set for each contact record on the LDAP server.
ldap.numb_attr	String within 512 characters	Blank	It configures the number attributes of each record to be returned by the LDAP server. Multiple number attributes are separated by spaces. **Example:** ldap.numb_attr = mobile ipPhone This requires the "mobile" and "ipPhone" attributes set for each contact record on the LDAP server.
ldap.display_name	String within 512 characters	Blank	It configures the display name of the contact record displayed on the phone screen. The value must start with a "%" symbol. **Example:** ldap.display_name = %cn The cn of the contact record is displayed on the phone

			screen.
ldap.version	2 or 3	3	It configures the LDAP protocol version supported by the IP phone. The version must be the same as the version assigned on the LDAP server.
ldap.call_in_lookup	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to perform an LDAP search when receiving an incoming call.
ldap.call_out_lookup	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to perform an LDAP search when placing a call.
ldap.ldap_sort	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to sort the search results in alphabetical order or numerical order.
ldap.incoming_call_special_search.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to search the telephone numbers starting with "+" symbol and "00" from the LDAP server if the incoming phone number starts with"+" or "00". When completing the LDAP search, all the search results will be displayed on the phone screen. **Example:** If the phone receives an incoming call from the phone number 0044123456789, it will search 0044123456789 from the LDAP server first, if no result found, it will search +44123456789 from the server again. The phone will display all the search results. 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.c	String within 512	Bl	It configures the display name of the LDAP phone book.

ustomize_label	characters	ank	If it is left blank, LDAP is displayed. It works only if "ldap.enable" is set to 1 (Enabled).
ldap.search_scope	**sub**-A recursive search of all levels below the base domain name is performed. **one**-A search of one level below the base domain name is performed. **base**-A search at the base domain name level is performed.	sub	It controls the search scope when searching for an LDAP contact.

Handset LDAP Configuration

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

	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 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 to 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_a	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

ttr[1]			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. 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.incomi	**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"+"

ng_call_special_search.enable[1]			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 is 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.

- For W70B, X=1-10.
- For W75DM， X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

Use LDAP Directory on Yealink Phones

You can access the LDAP directory and enter the desired numbers to match the search criteria for searching a contact, add local contacts from the LDAP directory, and dial a contact from the LDAP directory. You can also enable the DECT phone to perform an LDAP search when receiving an incoming call or dialing an outgoing call.

The following takes the W53P running firmware version 83 as an example.

To search for a contact from the LDAP directory:

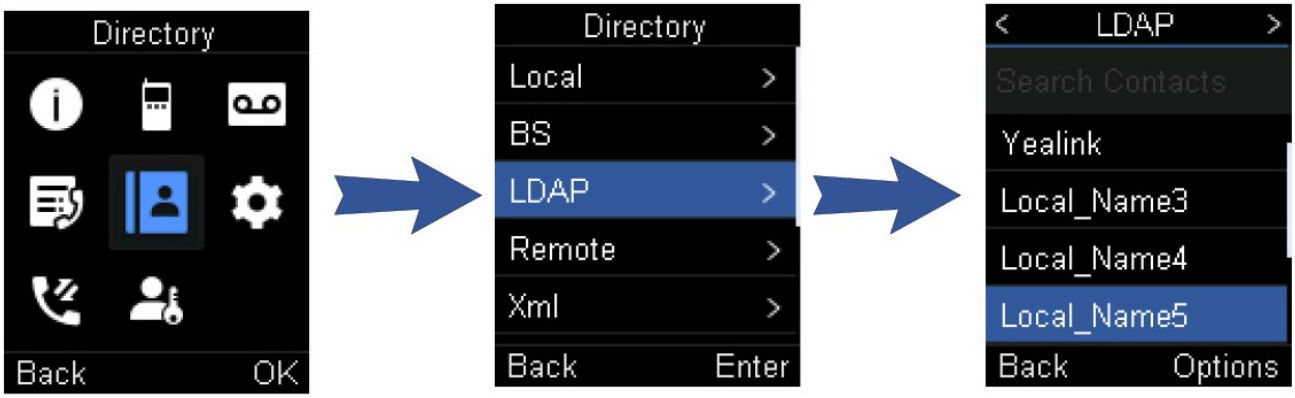
1. Press **OK** > **Directory** > **LDAP**.
   The LCD screen of the handset displays the contact list.

2. Enter a few continuous characters of the contact name or continuous digits of the contact phone number using the keypad.

The contacts that match the search criteria will display on the LCD screen.

3. Press or to select the desired contact.
4. Do one of the following:

- Press the **Options** soft key and then select **Detail** to view the detailed information of the contact.
- Press the **Options** soft key and then select **Add** to Local to add the contact to local.
- Press or to dial out.



- If the **LDAP Lookup For Incoming Call** parameter is enabled on the DECT phone, the DECT phone will perform an LDAP search when receiving an incoming call. If there is a contact record that matches the caller ID, the contact name will be displayed on the handset LCD screen as the calling line identification.
- The **Search Source List In Dialing** feature enables the phone to perform an LDAP search when you enter the digits using the keypad in the dialing interface. For more information on the configuration of the Search Source List In Dialing feature, refer to the Yealink phone-specific user guide.
- If contact records match the search criteria, the contact records will be listed on the handset LCD screen. You can select the desired contact record to dial out. The contact name will be displayed on the handset LCD screen during the call.
- If the **LDAP Lookup For Callout** parameter is enabled on the DECT phone, the DECT phone will perform an LDAP search when dialing an outgoing call. If there is a contact record that matches the called ID, the contact name will be displayed on the handset LCD screen as the called line identification.

Errors and Solutions

Error	Description	Solution
0x0003000000060001 Operations error	Server error. The error code returned by the LDAP server is unknown.	Check the server.
0x0003000000060002 Protocol error	Phone compatibility error. The protocol version between the phone and the LDAP server does not match.	1. Punch the configuration line ***ldap.version=2*** into 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	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

method not supported		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.
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.
0x0003000000060 00a Referral	Server error. The server is temporarily unavailable to handle this request.	Check the server.
0x0003000000060 00b Administrative limit exceeded	Server error. The time token used by the LDAP search 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.
0x0003000000060 00c Critical extension is unavailable	Phone compatibility error. The server does not support some attribute items requested by the phone.	Please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x0003000000060 010 No such attribute	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060 011 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.
0x0003000000060 012 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.
0x0003000000060 013 Constraint violation	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060 014 Type or value	Phone error.	Yealink FAE will do further analysis to give you a

exists		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 the password of LDAP is correct. 2. If you use LDAPs, please upload the CA of the server to the phone.
0x0003000000060032 Insufficient access	Server error. The server refuses phone access.	Check whether the server has enabled the 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.
0x0003000000060	Phone error.	Yealink FAE will do further

050 Other (e.g., implementation specific) error		analysis to give you a solution ASAP.
0x00030000000600c7 Can't contact LDAP server	Phone configuration or compatibility error. The phone cannot connect to the LDAP server.	1. Check whether the server address, port number, and authentication password of the phone's LDAP are correct. 2. When you use the LDAPS connection, you need to upload the server CA certificate from the phone end, and the CA's Common Name should be consistent with the LDAP server. 3. If the above methods do not solve the problem, please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x00030000000600c6 Local error	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600c5 Encoding error	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600c4 Decoding error	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060	Server or network error. The phone exceeds the	1. Push the configuration

0c3 Timed out	time limit when waiting for a response.	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.
0x00030000000600c2 Unknown authentication method	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600c1 Bad search filter	Phone configuration error. The format of the phone LDAP Filter is incorrect.	Check the configuration format of the LDAP Filter. For more information on the standards, see https://ldap.com/ldap-filters/.
0x00030000000600c0 User cancelled operation	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x00030000000600bf Bad parameter to an ldap routine	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
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.

0x000300000006 00ba 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.
0x0003000000060 0b9 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).
0x0003000000060 0b8 Client Loop	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060 0b7 Referral Limit Exceeded	Phone error.	Yealink FAE will do further analysis to give you a solution ASAP.
0x0003000000060 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 *.
0x000300000006 012d	Certificate error. The certificate CN fails to be authenticated. The CN value in the server CA	Keep the CN value in the phone LDAP server

CN Validation error	certificate is not consistent with the one in the LDAP server.	consistent with the one in the CA certificate.
0x0003000000060 12e Certificates error	Certificate error. The phone does not detect the correct CA certificate.	Upload the correct server CA certificate to the phone.
0x0003000000060 12f 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 under 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.
0x000300000006 0130	Phone compatibility error. The phone and the server fail to negotiate a TLS algorithm when using LDAPS.	1. Adjust the server algorithm. 2. Yealink FAE will also do further analysis to give you a solution ASAP.
0x000300000006 0131	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.

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 fewer 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.

Remote Phone Book File Elements

Yealink phones support two template files: Menu.xml and Department.xml.

The Menu.xml file defines the group/department of a remote phone book. The Department.xml file defines contact lists for a department/group, which is nested in Menu.xml file.

The following table lists the elements you can use to add groups or contacts in the remote phone book file. We recommend that you do not edit these elements.

Template	Element	Valid Values
Department.xml	<DirectoryEntry> <Name>Contact Name</Name> <Telephone>Contact Number</Telephone> </DirectoryEntry>	Add a contact in a department/group: Specify the contact name between <Name> and </Name>; Specify the contact number between <Telephone> and </Telephone>.
Menu.xml	<MenuItem> <Name>Department</Name> <URL>Department URI</URL> </MenuItem>	Add a contact department/group file: Specify the department/group name between <Name> and </Name>; Specify the department/group access URL between <URL>and </URL>.
Menu.xml	<SoftKeyItem> <Name>#</Name> <URL>http://10.2.9.1:99/	Specify a department/group file for a key: Specify *key, # key or digit key between <Name> and </Name>;

	Department.xml</URL > </SoftKeyItem>	Specify the department/group access URL between <URL> and </URL>.

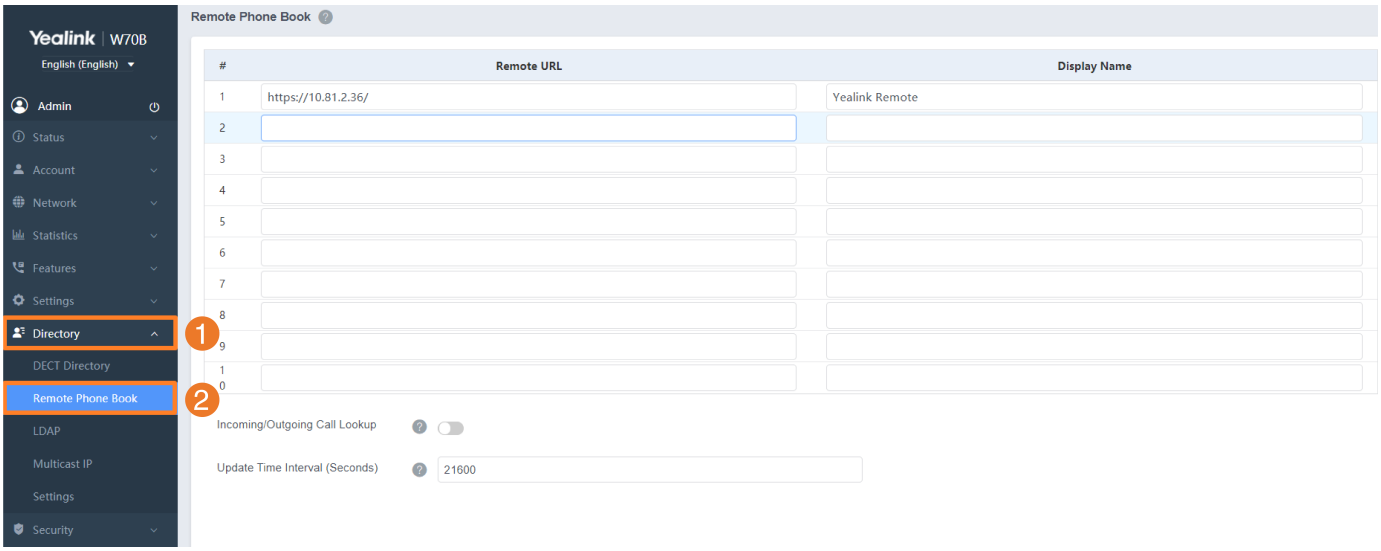
Customize Remote Phone Book File

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 the Menu.xml file and place it in 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 MB.
remote_phonebook.data.X.name[1]	String within 99 characters	Blank	It configures the display name of the remote phone book item.
remote_phonebook.data.X.username[1] [3]	String	Blank	It configures the user name used to access the remote phone book X.
remote_phonebook.data.X.password[1] [3]	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_phone	**0**-	0	It configures whether the remote phone book can be allocated.

book.assignment.enable	Disabled **1**-Enabled		
handset.X.remote_phonebook_access[2][3]	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.
- For W70B, X=1-10.
- For W75DM/W80DM/W90DM, X=1-5.

[2]X is the handset ID. X=1-10.
[3]This parameter is only applicable to W70B.

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
```

After provision, you can access the corporate directory.

- W71P/W73P/W74P/W76P/W77P/W78P/W79P/W53H:
- **OK** > **Directory** > **Remote Phone Book**
- CP930W-Base/DD phones:
- **Menu** > **Directory** > **Remote Phone Book**
- CP935W-Base:
- **Directory** > **Remote Phone Book**

Errors and Solutions

Error	Description	Solution
0x00090000106	Remote Phone Book	1. Refer to the corresponding error code to find out the solution. 2. If the above method does not solve the problem, please provide

0000 Remote dir download failed	downloading failure.	the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x00090000010600001 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.
0x00090000010600002 Download limit exceeded	Phone performance limits. The contact files you download exceed the maximum limit.	Generally, the color screen phones allow file downloading up to 1.5 M. However, the phones with black and white LCD display allow file downloading up to 768KB. Therefore, you need to control the size of the file to be downloaded, for example, the resource file uploaded by users.
0x00090000010600003 Auth Error	Phone configuration error. XML file authentication failed.	1. Choose one of the following methods to configure the correct authentication information for the phone: - Set the user name and password: remote_phonebook.data.x.username= and remote_phonebook.data.x.password= - Bring the authentication information in the URL. For example, http://user:password@IP/RemotePhonebook.xml 2. If the above method does not solve the problem, please provide the diagnostic file in the working scenario for comparison so that Yealink FAE can do further analysis.
0x00090000010600004 network	Network error, causing downloading failure.	Check whether the network between the phone and the server is available by using the phone's Ping feature.

unavailable		
0x00090000001060005 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.

Shared Directory

Introduction

Users can manage contacts and use them in all handsets that are registered on the same base station.

- For W70B: The shared directory can store up to 100 contacts.
- For W75/W80/W90 Multi-Cell System: The shared directory can store up to 1000 contacts.

Before You Begin

This feature is not applicable to DD Phones registered on W70B.

Shared Contact File Customization

You can customize the shared contacts using a local contact template.

You can ask the distributor or Yealink FAE for the local contact template.

Shared Contact File Elements and Attributes

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.

Elements	Attributes	Description
Contact	display_name	Specify the contact name. 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.

Customize Shared Contact File

1. Open the shared 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"

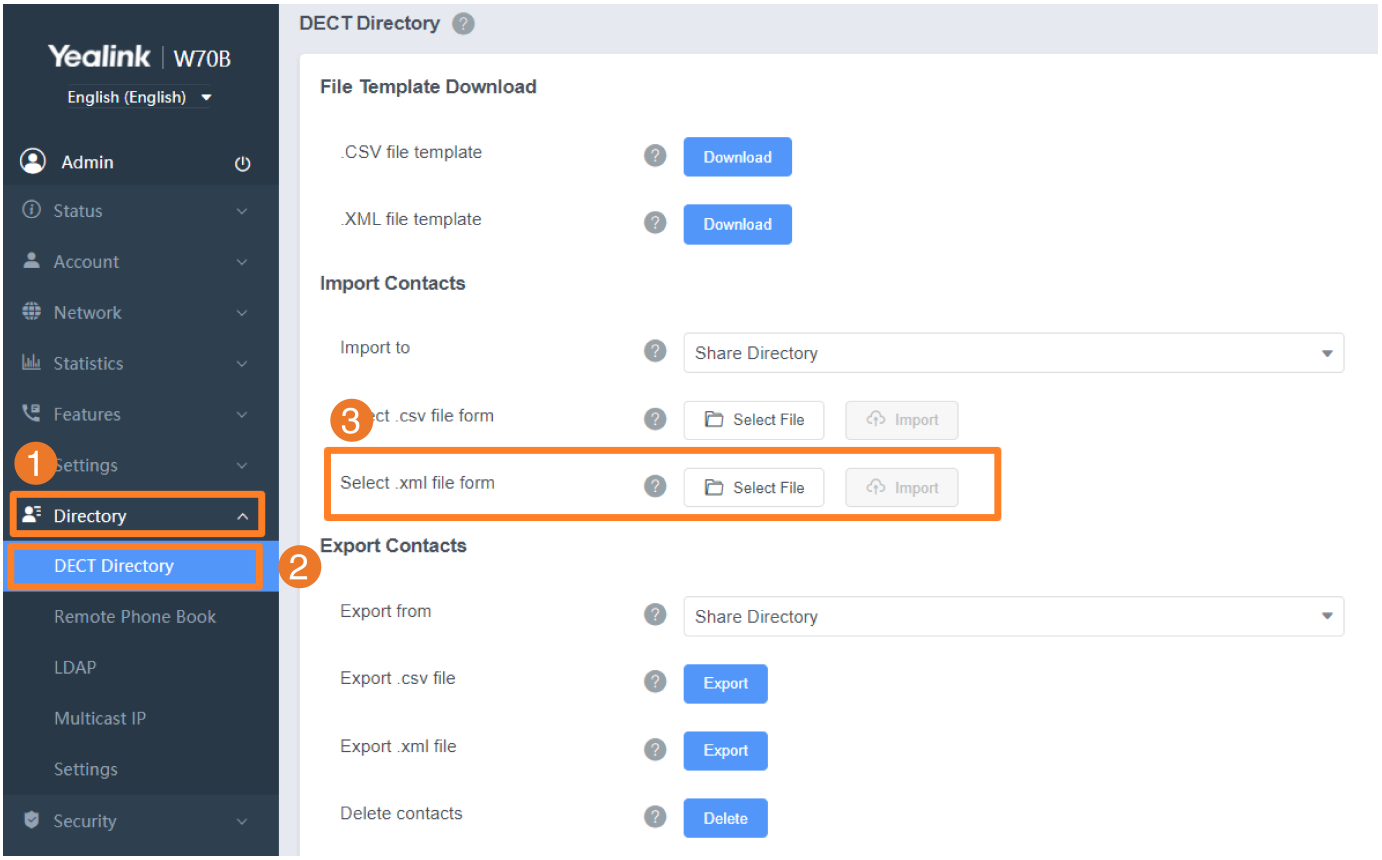
other_number="2112"/>

4. Save the changes and place this file on the provisioning server.

Shared Directory Configuration

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**.



Configuration Parameter

static.directory_setting.shared_contact.enable
shared_contact_list.url

Parameter	Permitted Values	Default	Description
static.directory_setting.shared_contact.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the Shared Directory feature.
shared_contact_list.url	URL within 511 characters	Blank	It configures the access URL of the shared contact file (*.xml) of the handsets. **Example**:

			shared_contact_list.url = http://192.168.10.25/contact.xml It works only if static.directory_setting.shared_contact.enable is set to 1 (Enabled).

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 handset.

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.

- For W70B, X=1-10.

- For W75DM, X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

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 [1]	**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).

[1] This parameter is only applicable to W70B.

Number Matching Settings

Introduction

You can configure the pattern to match the contact numbers with the caller's phone number.

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

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.

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

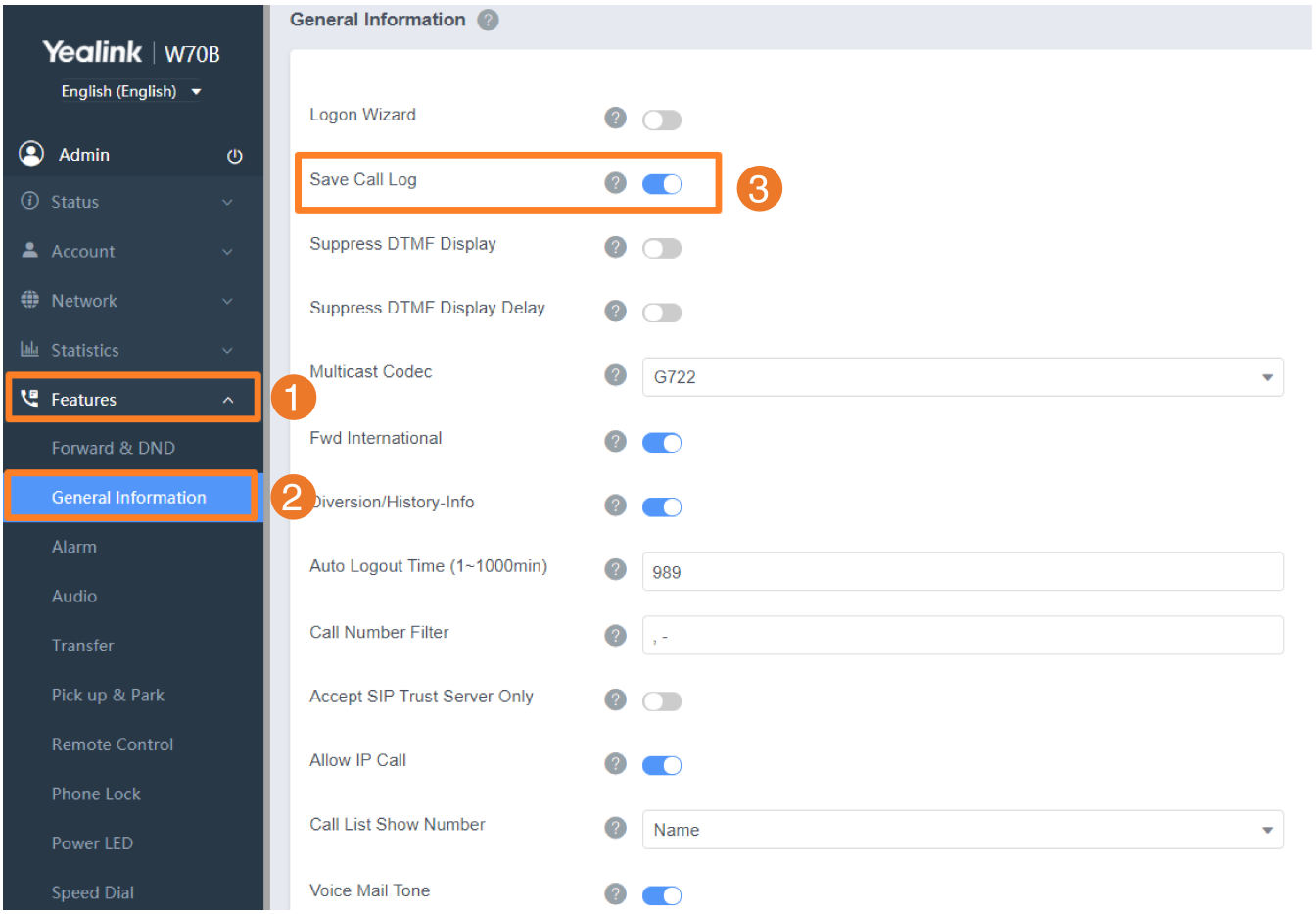
The following table describes the detailed call log information:

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". This display field is only applicable to W70B.

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.hide_local_number.enable
features.call_log_show_num
features.calllog_detailed_information

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.

account.X.hide_local_number.enable[1] [2]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to hide the account's local number in the call history.
features.call_log_show_num[2]	**0**-Name, the name is displayed preferentially; if there is no name, the number is displayed **1**-Number **2**-Name & Number, the name and number are displayed; if there is no name, the number is displayed	0	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 to 1 (Enabled).
features.calllog_detailed_information[2]	**0**-Disabled **1**-Enabled, you can get the detailed call-disposition information via the phone user interface: **History** > **Options** > **Detail** > **Relation**.	1	It enables or disables the phone to indicate what happened to the call in the call log lists. It is applicable to the following scenarios: • Reject an incoming call • Forward an incoming call • The outgoing call is rejected • Transfer a call • Answer a transferred/forwarded call from the remote party; your call is transferred/forwarded to another party. It works only if "features.save_call_history" is set to 1 (Enabled).

[1]X is the account ID. X=1-10.

[2]This parameter is only applicable to W70B.

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	Permitted Values	Default	Description

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

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 is an 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.

Power LED Indicator of Handset

Introduction

The handset power LED indicator indicates power status and phone status.

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

- The handset is idle
- The handset receives an incoming call
- The handset receives a voice mail

Before You Begin

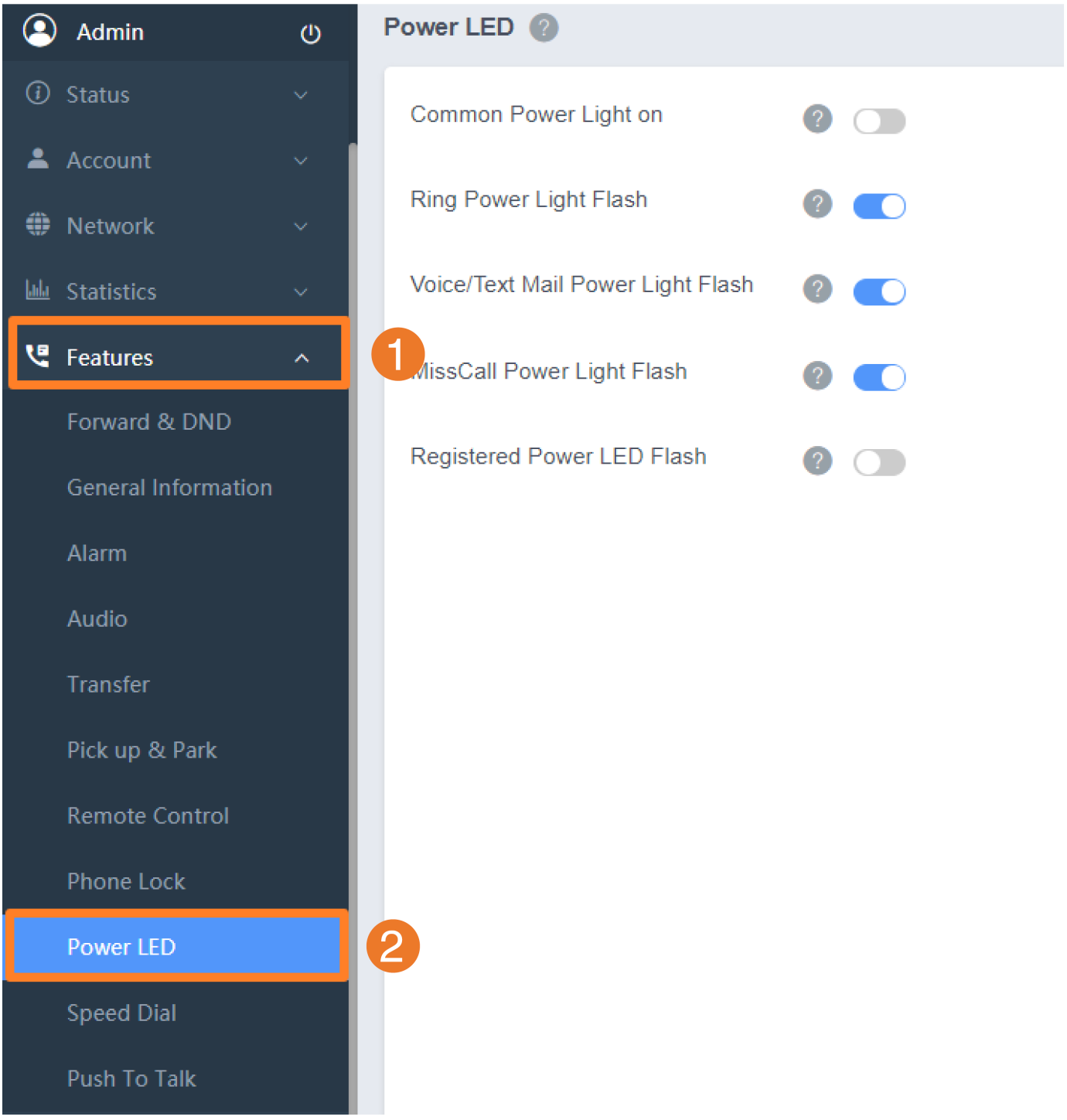
It is not applicable to CP930W/CP935W.

Power LED Indicator of Handset Configuration

Set via the Web User Interface

> Only W70B can configure it via Web User Interface.

1. On the web user interface, go to **Features** > **Power LED**.



Configuration Parameter

```
phone_setting.common_power_led_enable
phone_setting.ring_power_led_flash_enable
phone_setting.mail_power_led_flash_enable
phone_setting.missed_call_power_led_flash.enable
features.registered_power_led_flash.enable[1]
```

Parameter	Permitted Values	Def	Description

		aul t	
phone_setting.common_power_led_enable	**0**-Disabled (handset power LED indicator is off) **1**-Enabled (handset power LED indicator is solid red)	0	It enables or disables the handset power LED indicator to be turned on when the handset is idle.
phone_setting.ring_power_led_flash_enable	**0**-Disabled (handset power LED indicator is off) **1**-Enabled (handset power LED indicator fast flashes (300ms) red)	1	It enables or disables the handset power LED indicator to flash when the handset receives an incoming call.
phone_setting.mail_power_led_flash_enable	**0**-Disabled (handset power LED indicator does not flash) **1**-Enabled (handset power LED indicator slowly flashes (1000ms) red)	1	It enables or disables the handset power LED indicator to flash when the handset receives a voice mail.
phone_setting.missed_call_power_led_flash.enable	**0**-Disabled (handset power LED indicator does not flash) **1**-Enabled (handset power LED indicator slowly flashes (1000ms) red)	1	It enables or disables the handset power LED indicator to flash when the handset receives an incoming call.
features.registered_power_led_flash.enable[1]	**0**-Disabled power LED indicator does not flash **1**-Enabled (handset power LED indicator slow flashes (1000ms) red)	0	It enables or disables the power LED indicator to flash when the account registration is successful.

[1] This parameter is only applicable to W70B.

Handset Keypad Light

Introduction

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.

Before You Begin

It is only applicable to W71H, W73H, W74H, W78H, W53H, W56H, W57R, W59R and W59R Pro.

Handset Keypad Light Configuration

Set via the Device Interface

See Set the Keypad Light.

Configuration Parameter

custom.handset.keypad_light.enable

Parameter	Permitted Values	Default	Description
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 base station. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).

Handset Backlight

Introduction

The handset supports different backlight statuses, and you can configure it.

- For W53H/W56H/W71H/W73H/W74H/W78H/W57R/W59R/W59R Pro, the backlight in the charger or out of the charger can be configured independently.
- For CP930W, the backlight automatically turns off when the phone is charging and inactive for a specified time. You can only change the specified time.
- For CP935W, you can adjust the active level, inactive level, and choose the backlight time.

Handset Backlight Configuration

Set via the Device Interface

See Change the Brightness.

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
custom.handset.backlight_in_charger.enable[1]	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled, the backlight will be turned off after the handset is idle for about 10 seconds. **1**-Enabled, the backlight will be turned off after the handset is idle for about 30 minutes	-1	It enables or disables the handset backlight to be on for about 30 minutes when it is charged. It will take effect on all handsets that are registered on the same base station. It works only if

			"static.auto_provision.handset_configured.enable" is set to 1 (Enabled).
custom.handset.backlight_out_of_charger.enable[1]	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled, the backlight will be turned off after the handset is idle for about 10 seconds. **1**-Enabled, the backlight will be turned off after the handset is idle for about 30 minutes.	-1	It enables or disables the handset backlight to be on for about 30 minutes when it is not charged. 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).
phone_setting.on_call.backlight_mode[2]	**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.

[1] This parameter is only applicable to W53H/W56H/W57R/W59R/W59R Pro/W71H/W73H/W74H/W78H.
[2]This parameter is only applicable to CP935W.

Handset Wallpaper

Introduction

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.

Before You Begin

It is only applicable to W71H, W73H, W74H, W78H, W53H, W56H, W57R, W59R, W59R Pro and CP935W.

Handset Wallpaper Configuration

Set via the Device Interface

See Change the Wallpaper.

Configuration Parameter

custom.handset.wallpaper

Parameter	Permitted Values	Default	Description
custom.handset.wallpaper	**1**-Wallpaper1 **2**-Wallpaper2 **3**-Wallpaper3 **4**-Wallpaper4 **5**-Wallpap	-1, do not change the wallpaper set on each handset.	It configures the wallpaper displayed on the handset LCD screen. 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).

	er5		

Handset Screen Saver

Introduction

The screen saver of the handset is designed to protect your LCD screen. You can enable the screen saver to protect the LCD screen, and an analog clock will be activated and appear on the LCD screen after the handset is idle for approximately 10 seconds.

Before You Begin

It is only applicable to W71H, W73H, W74H, W78H, W53H, W56H, W57R, W59R, and W59R Pro.

Handset Screen Saver Configuration

Set via the Device Interface

See Set the Screen Saver.

Configuration Parameter

custom.handset.screen_saver.enable

Parameter	Permitted Values	Default	Description
custom.handset.screen_saver.enable[1]	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled **1**-Enabled, an analog clock will be activated and appear on the LCD screen if no user activity is sensed for approximately 10 seconds.	-1	It enables or disables 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).

Handset Name

Introduction

The handset will be assigned a name by default if successfully registered to the base station. You can personalize the handset name.

Handset Name Configuration

Set via the Device Interface

See Rename the Handset.

Configuration Parameter

handset.X.name
features.reset_headset_name_after_de_reg_handset.enable

Parameter	Permitted Values	Default	Description
handset.X.name[1]	String within 24 characters	The handset name for handset 1 is Handset 1. 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. The handset name for handset	It configures the name of the handset. If it is set to blank, it will display the corresponding default handset name.

		6 is Handset 6. The handset name for handset 7 is Handset 7. The handset name for handset 8 is Handset 8. The handset name for handset 9 is Handset 9. The handset name for handset 10 is Handset 10.	
features.reset_headset_name_after_de_reg_handset.enable	**0**-Yes **1**-No	1	It configures whether the handset name is maintained after the handset is deregistered.

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

Language

Introduction

Yealink phones support multiple languages. Languages used on the handset user interface and web user interface can be specified, respectively, as required.

Supported Languages

You can ask the distributor or Yealink FAE for language packs. You can also obtain the language packs online.

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

> Czech and Slovak are only applicable to W71H/W73H/W74H/W78H/W57R/W59R/CP935W.

Phone User Interface		Web User Interface		
Language	Language Pack	Language	Language Pack	Note Language Pack
English	/	English	1.English.js	1.English_note.xml
French	/	French	4.French.js	4.French_note.xml
German	/	German	5.German.js	5.German_note.xml
Italian	/	Italian	6.Italian.js	6.Italian_note.xml
Polish	/	Polish	7.Polish.js	7.Polish_note.xml
Portuguese	/	Portuguese	8.Portuguese.js	8.Portuguese_note.xml
Spanish	/	Spanish	9.Spanish.js	9.Spanish_note.xml
Turkish	/	Turkish	10.Turkish.js	10.Turkish_note.xml
Russian	/	Russian	11.Russian.js	11.Russian_note.xml
Czech	/	Czech	12.Czech.js	12.Czech_note.xml
Slovak	/	Slovak	13.Slovak.js	13.Slovak_note.xml

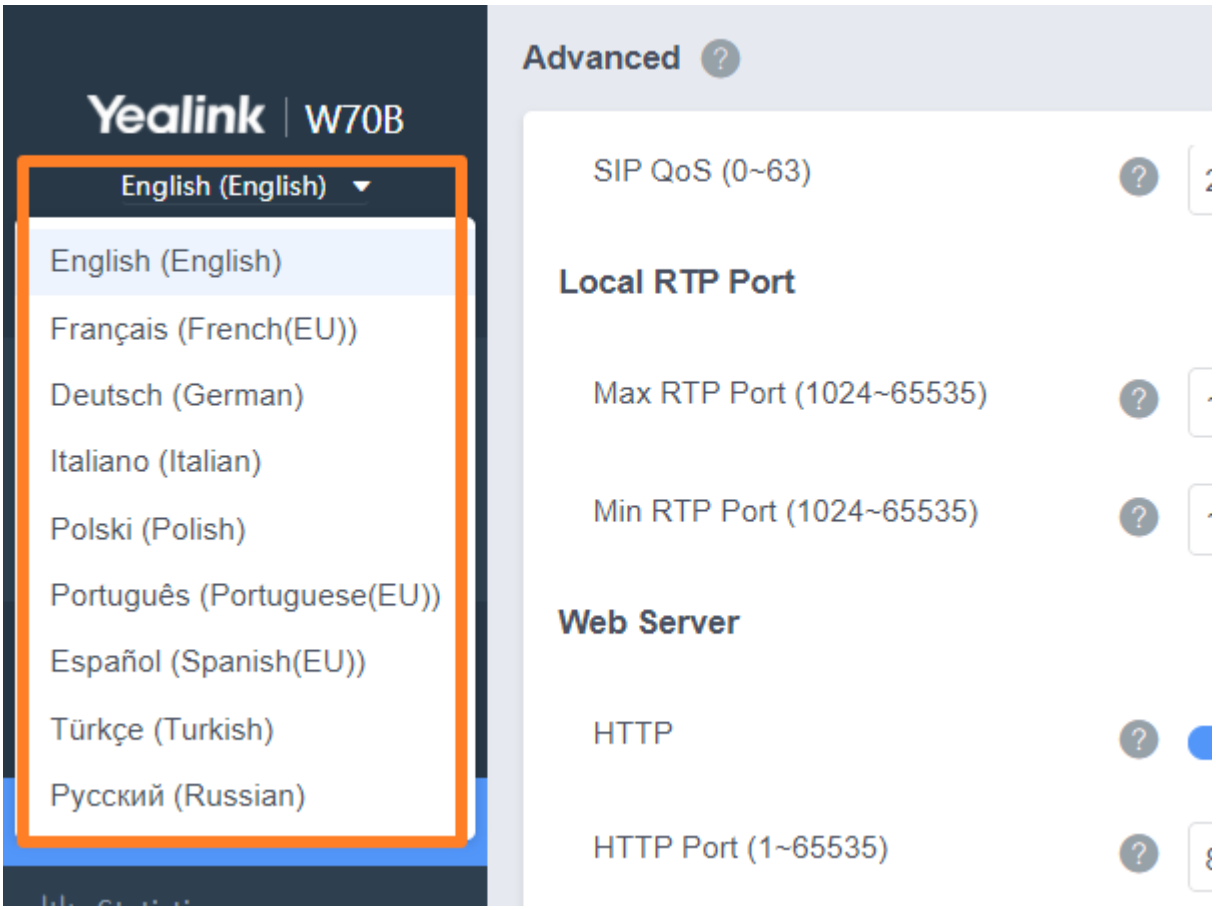
Language Display Configuration

The default language displayed on the phone/user interface is English. If your web browser displays a language not supported by the IP phone, the web user interface will display English by default. You

can specify the languages for the phone/user interface and web user interface.

Set via the Web User Interface

1. On the top-right corner of the web user interface



Set via the Device Interface

See Change the Language.

Configuration Parameter

lang.wui
custom.handset.language

Parameter	Permitted Values	Default	Description
lang.wui	English, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian, or a custom language name.	English	It configures the language used on the web user interface.
custom.h	**0**-English	0	It configures the language

andset.language	**1**-French **2**-German **3**-Italian **4**-Polish **5**-Portuguese **6**-Spanish **7**-Turkish **8**- Russian **9**-Czech (only for CP935W) **10**-Swedish **11**-Slovak (only for CP935W)		used on the handset user interface. It will take effect on all handsets that are registered on the same system. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).

Language for Web Display Customization

You can customize the translation of the existing language on the web user interface. You can modify the translation of an existing language or add a new language for web display.

You can ask the distributor or Yealink FAE for language packs. You can also obtain the language packs online.

Customize a Language Pack for Web Display

When you add a new language pack for the web user interface, the language pack must be formatted as "X.name.js" (X starts from 14, "name" is replaced with the language name). If the language name is the same as the existing one, the newly uploaded language file will override the existing one. We recommend that the 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.

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

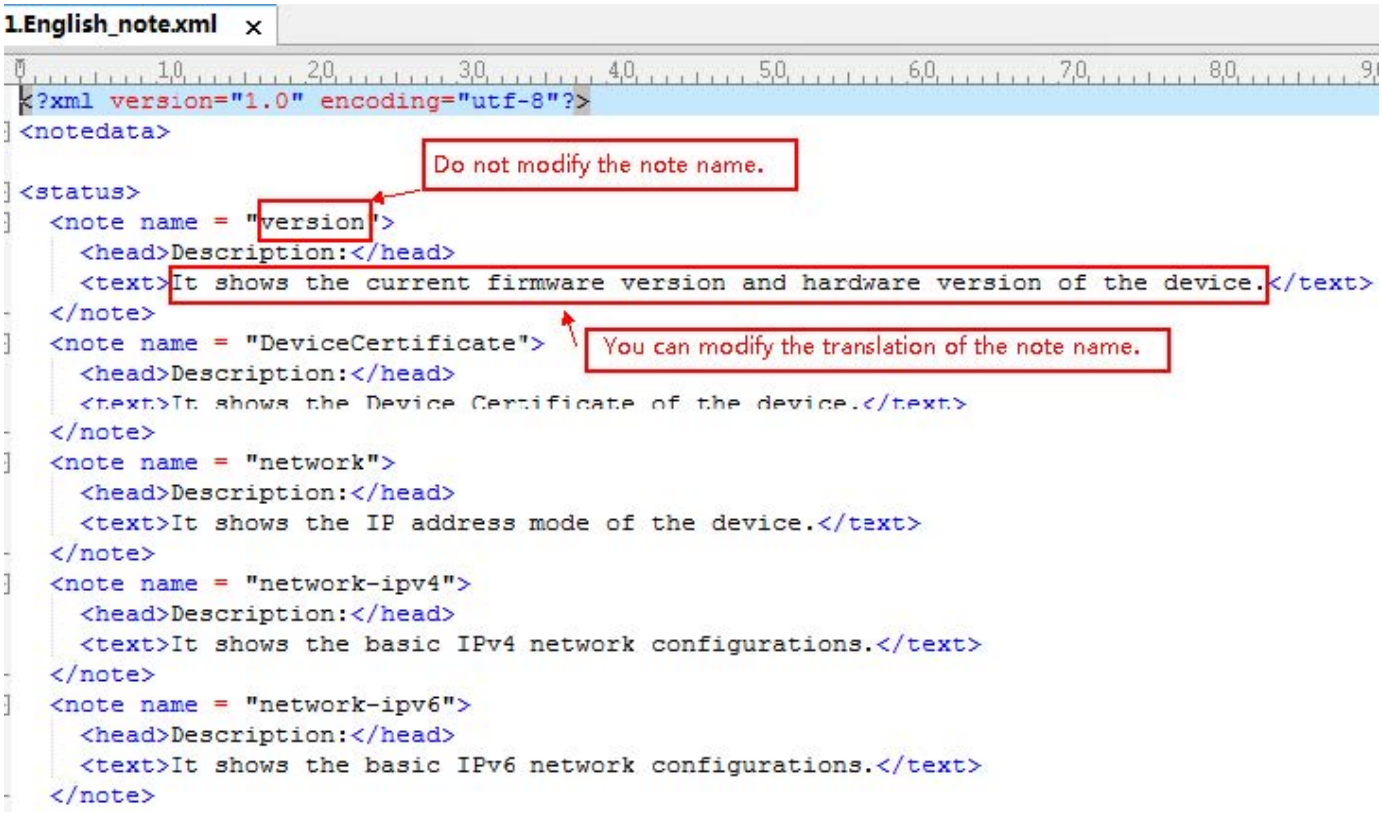


3. Save the language pack and place it on the provisioning server.

Customize a Language Pack for Note Display

When you add a new language pack for the note, the note language pack must be formatted as "X.name_note.xml" (X starts from 14, "name" is replaced with the language name). If the note language name is the same as the existing one, the newly uploaded note language pack will override the existing one. We recommend that the filename of the new note language pack should not be the same as the existing one.

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



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

Custom Language for Web Display Configuration

If you want to add a new language (for example, Wuilan) to phones, prepare the language file named "14.Wuilan.js" for downloading. After the update, you will find a new language selection "Wuilan" at the top-right corner of the web user interface.

Configuration Parameter

wui_lang.url
wui_lang.delete

Parameter	Permitted Values	Default	Description
wui_lang.url	URL within 511 characters For example http://localhost/X.GUI.name.lang X starts from 014, "name" is replaced with the language name	Blank	It configures the access URL of the custom language pack for the web user interface.
wui_l	http://localhost/all or	Bl	It deletes the specified or all custom web language

ang.delete	http://localhost/Y.name.js Y starts from 014, "name" is replaced with the language name	ank	packs and note language packs of the web user interface.

Time and Date

Introduction

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

Time Zone

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

Time Zone	Time Zone Name	Time Zone	Time Zone Name
-12	Eniwetok,Kwajalein	+2	Estonia(Tallinn)
-11	Midway Island	+2	Finland(Helsinki)
-11	Samoa	+2	Gaza Strip(Gaza)
-10	United States-Hawaii-Aleutian	+2	Greece(Athens)
-10	United States-Alaska-Aleutian	+2	Harare
-9:30	French Polynesia	+2	Israel(Tel Aviv)
-9	United States-Alaska Time	+2	Jordan(Amman)
-8	Canada(Vancouver,Whitehorse)	+2	Latvia(Riga)
-8	Mexico(Tijuana,Mexicali)	+2	Lebanon(Beirut)
-8	United States-Pacific Time	+2	Moldova(Kishinev)
-8	Baja California	+2	Pretoria
-7	Canada(Edmonton,Calgary)	+2	Jerusalem
-7	Mexico(Mazatlan,Chihuahua)	+2	Russia(Kaliningrad)
-7	United States-Mountain Time	+2	Bulgaria(Sofia)
-7	United States-MST no DST	+2	Lithuania(Vilnius)
-7	Chihuahua,La Paz	+2	Cairo
-7	Arizona	+2	Istanbul
-6	Guatemala	+2	E.Europe

-6	El Salvador	+2	Tripoli
-6	Honduras	+2	Romania(Bucharest)
-6	Nicaragua	+2	Syria(Damascus)
-6	Costa Rica	+2	Turkey(Ankara)
-6	Belize	+2	Ukraine(Kyiv, Odessa)
-6	Canada-Manitoba(Winnipeg)	+3	East Africa Time
-6	Chile(Easter Islands)	+3	Iraq(Baghdad)
-6	Guadalajara	+3	Russia(Moscow)
-6	Monterrey	+3	St.Petersburg
-6	Mexico(Mexico City,Acapulco)	+3	Kuwait, Riyadh
-6	Saskatchewan	+3	Nairobi
-6	United States-Central Time	+3	Minsk
-5	Bahamas(Nassau)	+3	Volgograd (RTZ 2)
-5	Bogota, Lima	+3:30	Iran(Teheran)
-5	Canada(Montreal,Ottawa,Quebec)	+4	Armenia(Yerevan)
-5	Cuba(Havana)	+4	Azerbaijan(Baku)
-5	Indiana (East)	+4	Georgia(Tbilisi)
-5	Peru	+4	Kazakhstan(Aktau)
-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(Aqtobe)
-4	Manaus, Cuiaba	+5	Kyrgyzstan(Bishkek)
-4	Georgetown	+5	Ekaterinburg (RTZ 4)
-4	Chile(Santiago)	+5	Karachi
-4	Paraguay(Asuncion)	+5	Tashkent
-4	United Kingdom-	+5	Pakistan(Islamabad)

	Bermuda(Bermuda)		
-4	United Kingdom(Falkland Islands)	+5	Russia(Chelyabinsk)
-4	Trinidad&Tobago	+5:30	India(Calcutta)
-3	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	Kazakhstan(Astana, Almaty)
-3	Cayenne,Fortaleza	+6	Russia(Novosibirsk,Omsk)
-3	Montevideo	+6	Bangladesh(Dhaka)
-3	Salvador	+6:30	Myanmar(Naypyitaw)
-3	Brazil(DST)	+6:30	Yangon (Rangoon)
-2:30	Newfoundland and Labrador	+7	Russia(Krasnoyarsk)
-2	Brazil(no DST)	+7	Thailand(Bangkok)
-2	Mid-Atlantic	+7	Vietnam(Hanoi)
-1	Portugal(Azores)	+7	Jakarta
-1	Cape Verde Islands	+8	China(Beijing)
0	GMT	+8	Singapore(Singapore)
0	Greenland	+8	Hong Kong, Urumqi
0	Western European Time	+8	Taipei
0	Monrovia	+8	Kuala Lumpur
0	Reykjavik	+8	Australia(Perth)
0	Casablanca	+8	Russia(Irkutsk, Ulan-Ude)
0	Denmark-Faroe Islands(Torshavn)	+8	Ulaanbaatar
0	Ireland(Dublin)	+8:45	Eucla
0	Edinburgh	+9	Korea(Seoul)
0	Portugal(Lisboa,Porto,Funchal)	+9	Japan(Tokyo)
0	Spain-Canary Islands(Las	+9	Russia(Yakutsk,Chita)

	Palmas)		
0	United Kingdom(London)	+9:30	Australia(Adelaide)
0	Lisbon	+9:30	Australia(Darwin)
0	Morocco	+10	Australia(Sydney,Melbourne,Canberra)
+1	Albania(Tirane)	+10	Australia(Brisbane)
+1	Austria(Vienna)	+10	Australia(Hobart)
+1	Belgium(Brussels)	+10	Russia(Vladivostok)
+1	Caicos	+10	Magadan (RTZ 9)
+1	Belgrade	+10	Guam, Port Moresby
+1	Bratislava	+10	Solomon Islands
+1	Ljubljana	+10:30	Australia(Lord Howe Islands)
+1	Chad	+11	New Caledonia(Noumea)
+1	Copenhagen	+11	Chokurdakh (RTZ 10)
+1	West Central Africa	+11	Russia(Srednekolymsk Time)
+1	Poland(Warsaw)	+11:30	Norfolk Island
+1	Spain(Madrid)	+12	New Zealand(Wellington,Auckland)
+1	Croatia(Zagreb)	+12	Fiji Islands
+1	Czech Republic(Prague)	+12	Russia(Kamchatka Time)
+1	Denmark(Kopenhagen)	+12	Anadyr
+1	France(Paris)	+12	Petropavlovsk-Kamchatsky (RTZ 11)
+1	Germany(Berlin)	+12	Marshall Islands
+1	Hungary(Budapest)	+12:45	New Zealand(Chatham Islands)
+1	Italy(Rome)	+13	Nuku'alofa
+1	Switzerland(Bern)	+13	Tonga(Nukualofa)
+1	Sweden(Stockholm)	+13:30	Chatham Islands
+1	Luxembourg(Luxembourg)	+14	Kiribati
+1	Macedonia(Skopje)		
+1	Netherlands(Amsterdam)		
+1	Namibia(Windhoek)		

+1	Spain(Madrid)		

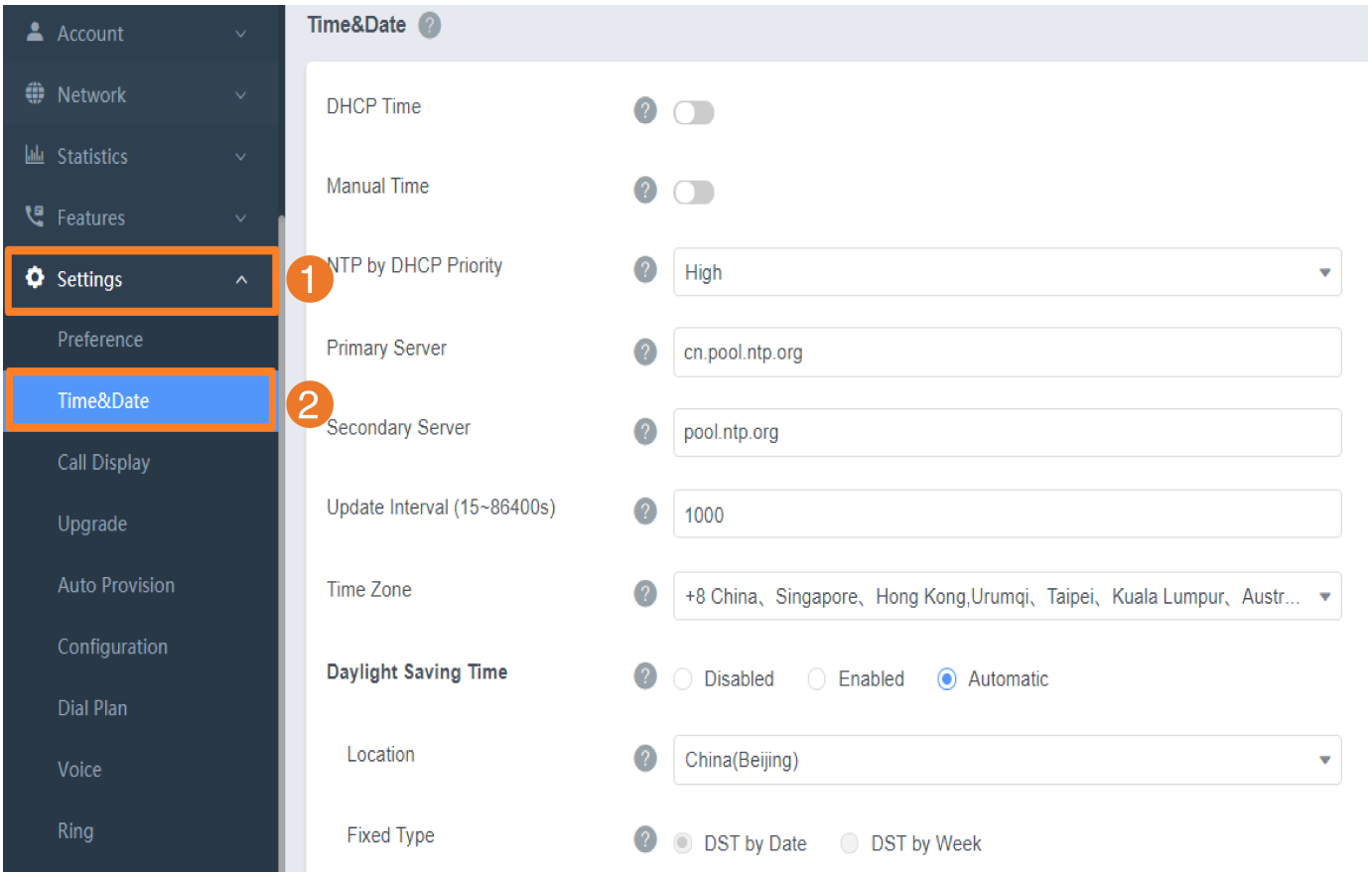
NTP Settings

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

Set via the Web User Interface

On the web user interface, go to **Settings** > **Time&Date**.



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
```

Param	Permitted Values	Def	Description

eter		aul t	
local_ time.m anual_ ntp_sr v_prio r	**0**- High (use the NTP server address offered by the DHCP server preferentially) **1**- Low (use the NTP server address configured manually preferentially)	0	It configures the priority for the phone to use the NTP server address offered by the DHCP server.
local_ time.d hcp_t ime	**0**-Disabled **1**-Enabled	0	It enables or disables the phone from updating its time with the offset time offered by the DHCP server. It is only available to offset from Greenwich Mean Time GMT 0.
local_ time.n tp_ser ver1	String within 99 characters	cn. poo l.n tp. org	It configures the IP address or the domain name of the primary NTP server.
local_ time.n tp_ser ver2	String within 99 characters	poo l.n tp. org	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.
local_ time.in terval	Integer from 15 to 86400	10 00	It configures the interval (in seconds) at which the phone updates time and date from the NTP server.
local_ time.t ime_z one	-12 to +14	+8	It configures the time zone.
local_ time. time_	String within 32 characters The available time zone names depend on the time	Chi na(Bei	It configures the time zone name. It works only if "local_time.summer_time" is set to 2

zone_name	zone configured by the parameter local_time.-time_zone.	jing)	(Automatic) and the parameter "local_time.-time_zone" should be configured in advance.

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:

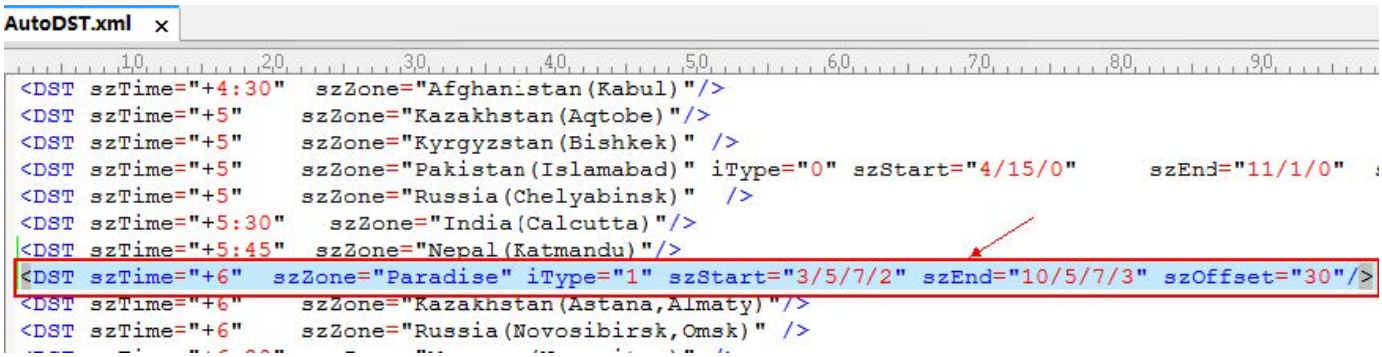
Attributes	Type	Values	Description
szTime	required	[+/-][X]:[Y], X=0~14, Y=0-59	Time Zone
szZone	required	String (if the content is more than one city, it is best to keep their daylight saving time the same)	Time Zone name
iType	optional	0/1 **0**-DST by Date **1**-DST by Week	DST time type (This item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

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

Customize Auto DST File

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

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.
4. For example:
5. 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"/ >



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

AutoDST.xml*

```
<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"

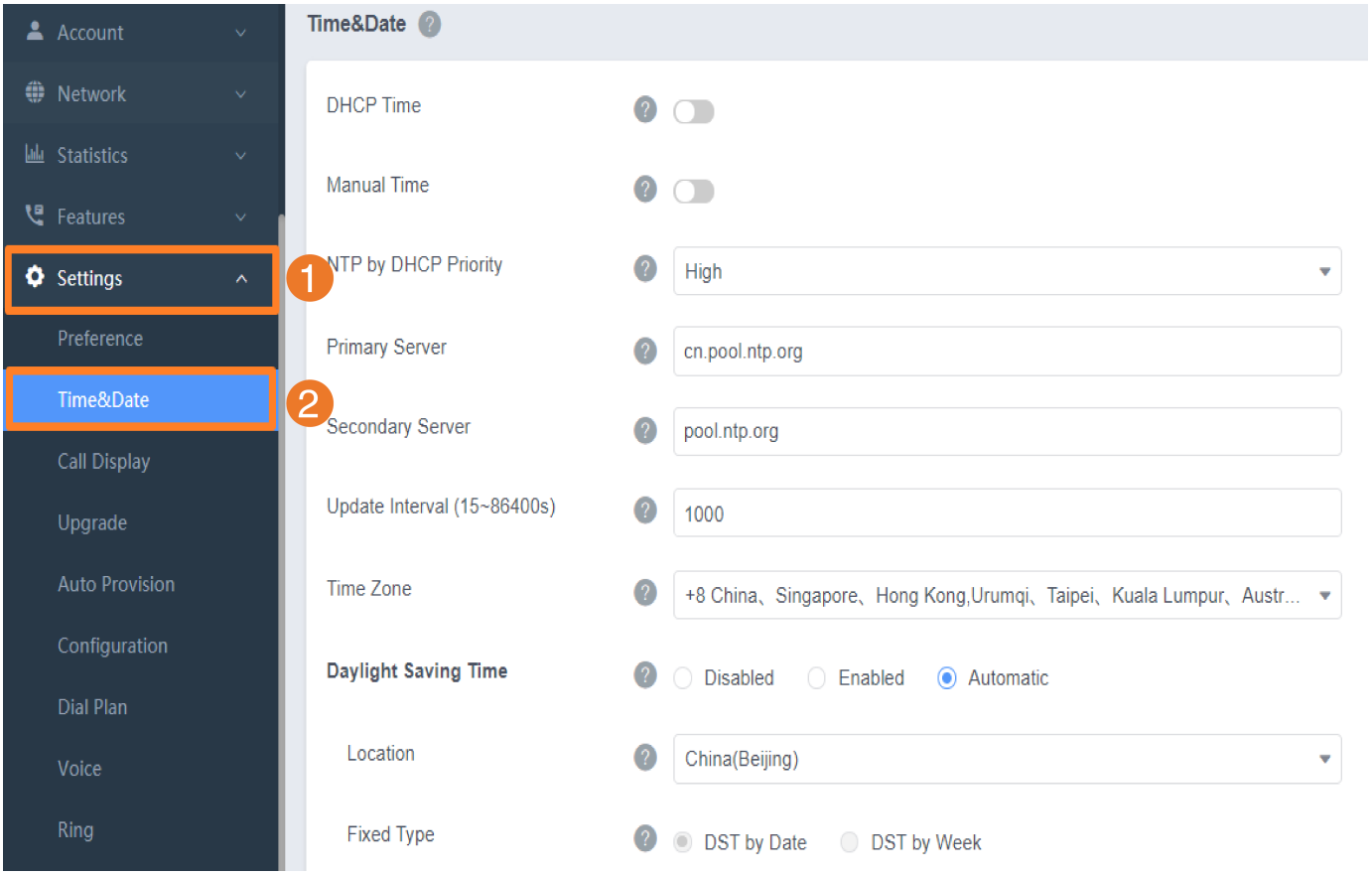
Add DST

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

DST Configuration

Set via the Web User Interface

On the web user interface, go to **Settings** > **Time&Date**.



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

local_time.end_time	Month/Day/Hour-DST by Date, use the following mapping: **Month**: 1=January, 2=February,…, 12=December **Day**: 1=the first day in a month,…, 31=the last day in a month **Hour**: 0=0am, 1=1am,…, 23=11pm Month/Week of Month/Day of Week/Hour of Day-DST by Week, use the following mapping: **Month**: 1=January, 2=February,…, 12=December **Week of Month**: 1=the first week in a month,…, 5=the last week in a month **Day of Week**: 1=Monday, 2=Tuesday,…, 7=Sunday **Hour of Day**: 0=0am, 1=1am,…, 23=11pm	12/31/23	It configures the end time of the Daylight Saving Time (DST). It works only if "local_time.summer_time" is set to 1 (Enabled).
local_time.offset_time	Integer from -300 to 300	60	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).
auto_dst.url	URL within 511 characters	Blank	It configures the access URL of the DST file (AutoDST.xml). It works only if "local_time.summer_time" is set to 2 (Automatic).

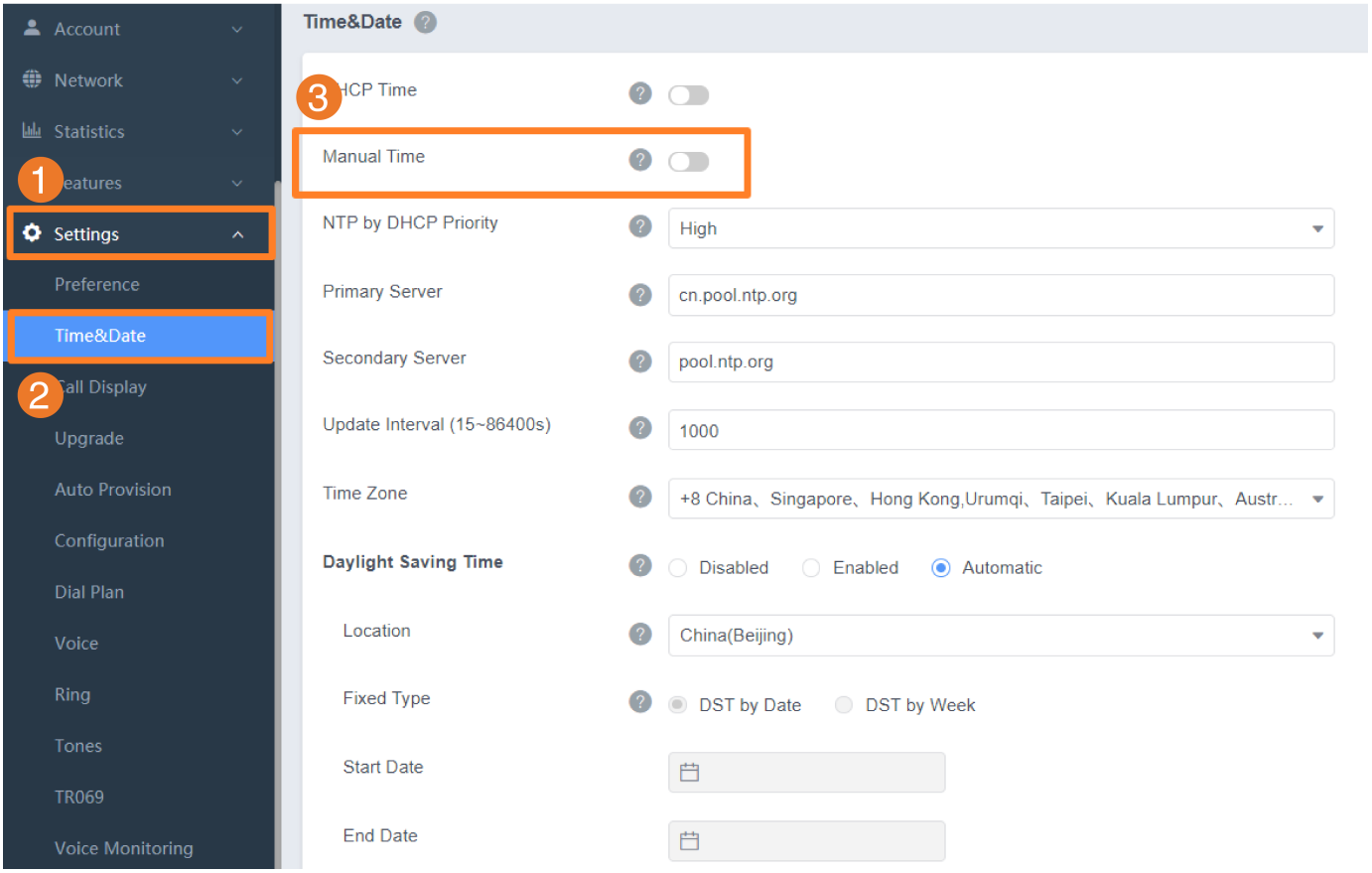
Time and Date Manual Configuration

You can manually set the time and date when the phones cannot obtain the time and date from the

NTP time server.

Set via the Web User Interface

On the web user interface, go to **Settings** > **Time&Date** > **Manual Time**.



Configuration Parameter

local_time.manual_time_enable

Parameter	Permitted Values	Default	Description
local_time.manual_time_enable	**0**-Disabled, the phone obtains time and date from the NTP server. **1**-Enabled	0	It enables or disables the phone from obtaining time and date from manual settings.

After the device reboots, it will be forcibly switched to obtain the time and date from the NTP server.

Time and Date Format Configuration

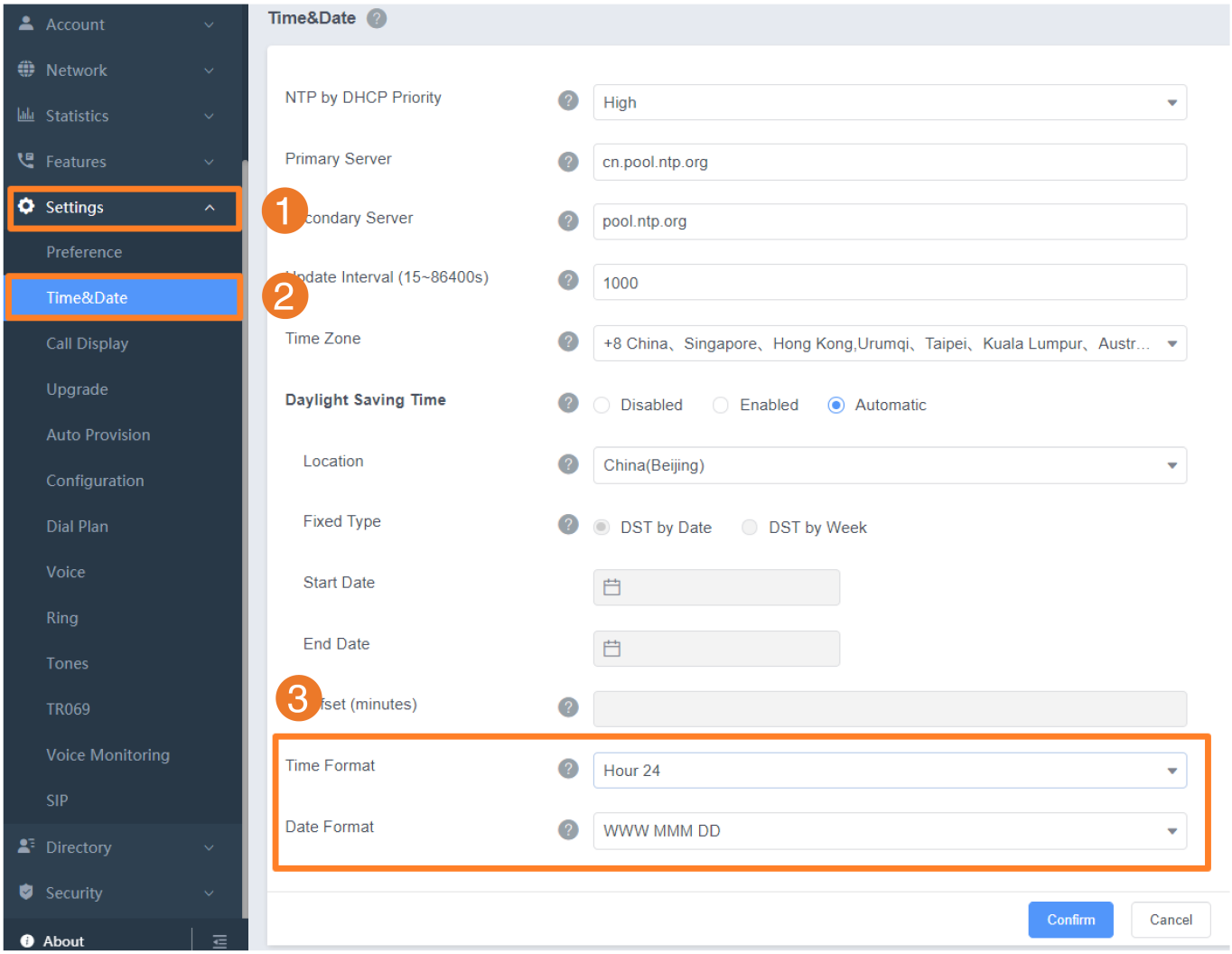
You can customize the time and date by choosing between a variety of time and date formats,

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.

Set via the Device Interface

See Time & Date.

Set via the Web User Interface



Configuration Parameter

custom.handset.time_format
custom.handset.date_format
local_time.time_format
local_time.date_format
lcl.datetime.date.format

Parameter	Permitted Values	Default	Description

custom.handset.time_format	**0**-Hour 12, the time will be displayed in 12-hour format with AM or PM specified. **1**-Hour 24, the time will be displayed in 24-hour format (for example, 2:00 PM displays as 14:00).	1	It configures the time format for all registered handsets. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).
custom.handset.date_format	**0**-WWW MMM DD **1**-DD-MMM-YY **2**-YYYY-MM-DD **3**-DD/MM/YYYY **4**-MM/DD/YY **5**-DD MMM YYYY **6**-WWW DD MMM Use the following mapping: "WWW" represents the abbreviation of the week; "DD" represents a two-digit day; "MMM" represents the first three letters of the month; "YYYY" represents a four-digit year, and "YY" represents a two-digit year.	0	It configures the date format for all registered handsets. The value configured by the parameter lcl.datetime.date.format takes precedence over that configured by this

			parameter.
local_time.time_format	**0**-Hour 12, the time will be displayed in 12-hour format with AM or PM specified. **1**-Hour 24, the time will be displayed in 24-hour format (for example, 2:00 PM displays as 14:00).	1	It configures the time format.
local_time.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. The value configured by the parameter "lcl.datetime.date.format" takes precedence over that configured by this parameter.
lcl.datetime.date.format	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"	Blank	It configures the display format of the date.

	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 "W" letters (for example, WWW) represent the long format of the day of the week. It will take effect on all handsets that are registered on the same base station. If configured, users can only change the date format via the handset.		

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
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 (not applicable to CP930W/CP935W/DD Phones). For example, Mon., Tues., Wed., Thur., Fri., Sat., Sun.
W is used more than twice (for example, WWW, WWWW)	It represents the long format of the day of the week (only applicable to CP930W/CP935W/DD Phones). For example, Monday, Tuesday,…, Sunday

Input Method

Introduction

The handset provides you with 12 input modes, and different input modes provide different characters. The default input modes are Abc, 123, ABC, and abc. You can specify the default input method for the handset when searching for contacts.

Before You Begin

It is not applicable to DD phones.

Input Method Configuration

Set via the Device Interface

1. Go to **OK** > **Settings** > **Display** > **Input Method**.

- For CP930W, go to **Menu** > **Settings** > **Basic Settings** > **Display** > **Input Method**.

2. Select the desired input mode and then select **Change**.

Configuration Parameter

directory.search_default_input_method

Parameter	Permitted Values	Default	Description
directory.search_default_input_method	**1**-Abc **2**-123 **3**-ABC **4**-abc **5**-АВГ	1	It configures the default input method when the user searches for contacts in the Local Directory, LDAP, Remote Phone Book, Blocklist, or Network Directory.

	6- AÄÅ **7**- aää **8**- S□ □ **9**- s□ □ **10**- абв **11**- АБВ **12**- □□ □		

Search Source List in Dialing

Introduction

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.

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 the super search template.

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	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	The display name of the directory list. We recommend that you do not edit this field.
priority	1 to 5 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.

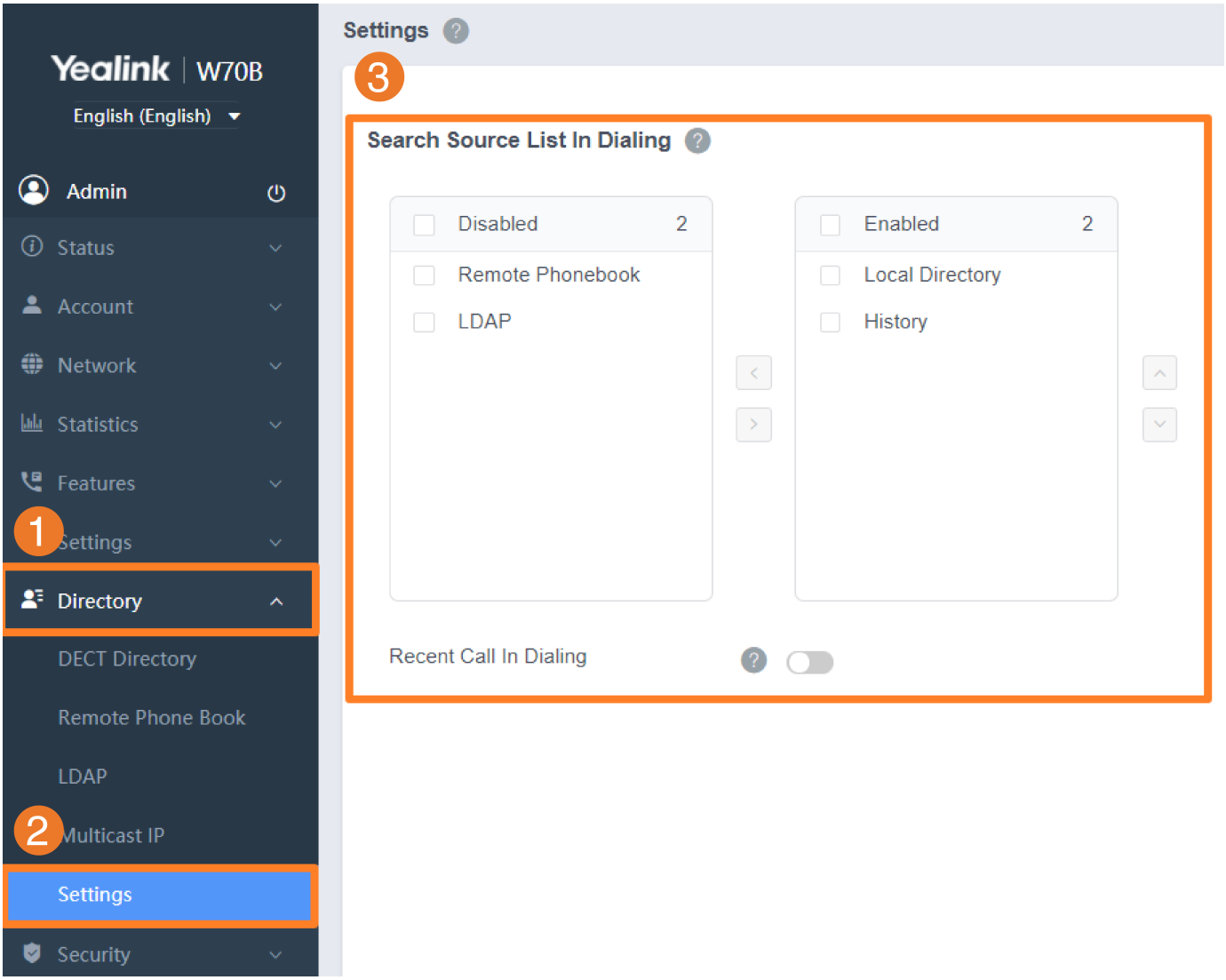
Customize Search Source File

1. Open the search source file.
2. To configure each directory list, edit the values within double quotes in the corresponding field.
   For example, enable the local directory search, disable the call log search, and specify a priority.
   <item id_name="local_directory_search" display_name="Local Contacts" priority="1" enable="1" />
   <item id_name="calllog_search" display_name="History" priority="2" enable="0" />
3. Save the change and place this file to the provisioning server.

Search Source List Configuration

Set via the Web User Interface

1. On the web user interface, go to **Directory** > **Settings** > **Search Source List In Dialing**.



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
bw.plcm_phone_services.enable
bw.plcm_phone_services_update_interval
directory_setting.plcm_directory.enable
directory_setting.plcm_directory.priority
search_in_dialing.plcm_directory.enable
search_in_dialing.plcm_directory.priority

Parameter	Permitted Values	Default	Description
super_search.url	URL within 511 characters	Blank	It configures the access URL of the custom super search file.
search_in_dialing.local_directory.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to automatically search entries from the local directory and display results on the pre-dialing/dialing screen.
search_in_dialing.local_directory.priority	Integer greater than or equal to 0	1	It configures the search priority of the local directory.
search_in_dialing.history.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to automatically search entries from the call history list and display results on the pre-dialing/dialing screen.

search_in_dialing.history.priority	Integer greater than or equal to 0	2	It configures the search priority of the call history list.
search_in_dialing.remote_phone_book.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to automatically search entries from the remote phone book and display results on the pre-dialing/dialing screen.
search_in_dialing.remote_phone_book.priority	Integer greater than or equal to 0	3	It configures the search priority of the remote phone book.
search_in_dialing.ldap.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to automatically search entries from the LDAP and display results on the pre-dialing/dialing screen.
search_in_dialing.ldap.priority	Integer greater than or equal to 0	4	It configures the search priority of the LDAP.
bw.plcm_phone_services.enable[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to open the PLCM phonebook service.
bw.plcm_phone_services_update_interval[1]	Integer from 60 to 86400	1440	It configures the automatic update interval of the PLCM phonebook service.
directory_setting.plcm_directory.enable[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the directory list to display to the PLCM phone book.
directory_setting.plcm_directory.priority[1]	Integer greater than or equal to 0	11	It configures the priority of the PLCM phone book on the directory list.
search_in_dialing.plcm_directory.enable[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to automatically search entries from the PLCM phone book and display results on the pre-dialing/dialing screen.

search_in_dialing.plcm_directory.priority[1]	Integer greater than or equal to 0	11	It configures the search priority of the PLCM phone book.

[1]This parameter is only applicable to W70B.

Call Display

Introduction

By default, the phones present the contact information when receiving an incoming call and engaging in a call.

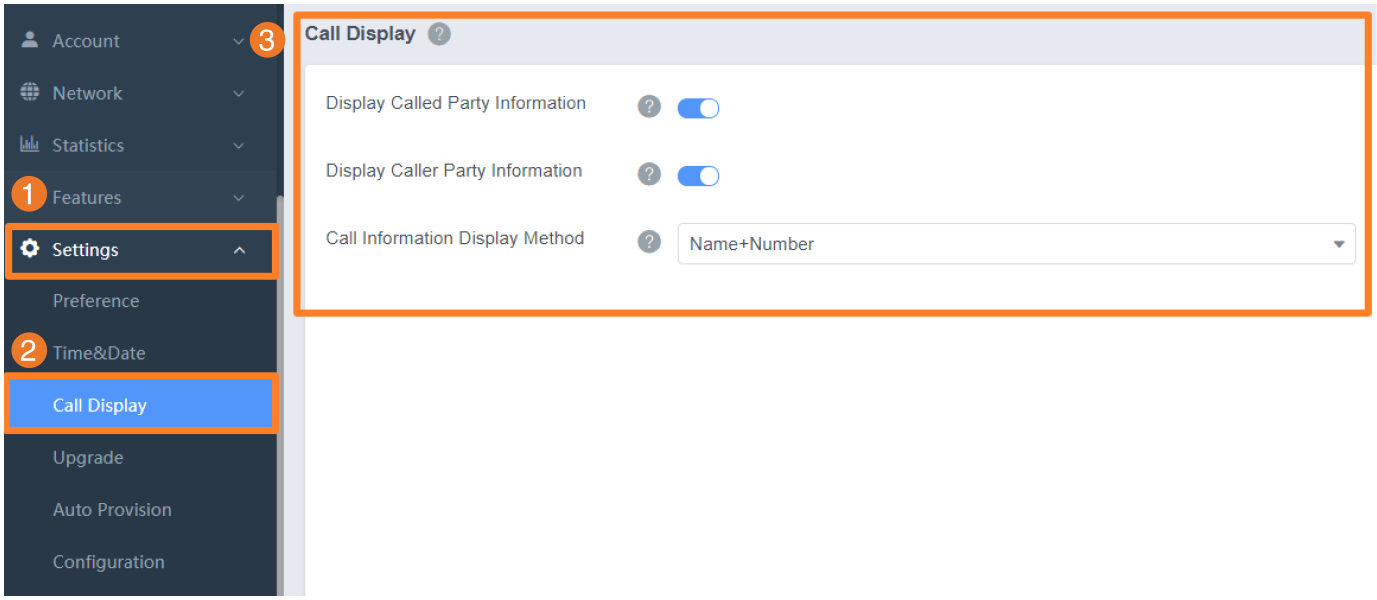
If you enable the configuration: "features.caller_name_type_on_dialing", when you dial an outgoing call, the contact information shown in the Call Display will be the same as the Line Status and only show the caller name. It will show the IP address if the account has not been registered.

You can configure what contact information is presented 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

Set via the Web User Interface

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



Configuration Parameter

phone_setting.called_party_info_display.enable
phone_setting.call_info_display_method
phone_setting.caller_party_info_display.enable
account.X.update_ack_while_dialing
sip.disp_incall_to_info

phone_setting.line_status_display.mode
handset.X.line_status_display_mode
bw.xsi.directory.alphabetized_by_lastname.enable

Parameter	Permitted Values	Default	Description
phone_setting.called_party_info_display.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone from displaying the local identity when it receives an incoming call. The information display method is configured by the parameter "phone_setting.call_info_display_ method".
phone_setting.call_info_display_method	**0**-Name+Number **1**-Number+Name **2**-Name **3**-Number **4**-Full Contact Info (display name sip:xxx@domain.com) Name refers to the Label; Number refers to the User Name.	0	It configures the call information display method when the phone receives an incoming call, dials an outgoing call, or is in a call.
phone_setting.caller_party_info_display.enable	**0**-Disabled **1**-Enabled	1	It enables or disables to display of the corresponding line account when outgoing. If the handset is only assigned the incoming and outcoming permissions of one account, the line account will not be displayed even if the configuration item is enabled.

account.X.update_ack_while_dialing[1]	**0**-Disabled **1**-Enabled	0	It enables or disables the phone from updating the display of the call ID according to the ACK message.
sip.disp_incall_to_info[2]	**0**-Disabled **1**-Enabled	0	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.
phone_setting.line_status_display.mode	**0**-Disabled, you can check the status of all registered Lines. **1**-Enabled	0	It configures that the handset only displays the outgoing line in Line status.
handset.X.line_status_display_mode[1]	**0**-Disabled, you can check the status of all registered Lines, including available or unavailable, whether DND, FWD, etc. **1**-Enabled, only displays the status of the available lines of the current handset, and hides the accounts that are not assigned call rights.	Blank	It controls the mode displayed after entering Line Status on the handset.
bw.xsi.directory.alphabetized_by_lastname.enable[1]	**0**-First name, Last name **1**-Last name, First name	0	It configures the call ID (first name and last name) display method when the phone receives an incoming call, places an outgoing call, or is in an active call.

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

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

Display Method on Dialing

Introduction

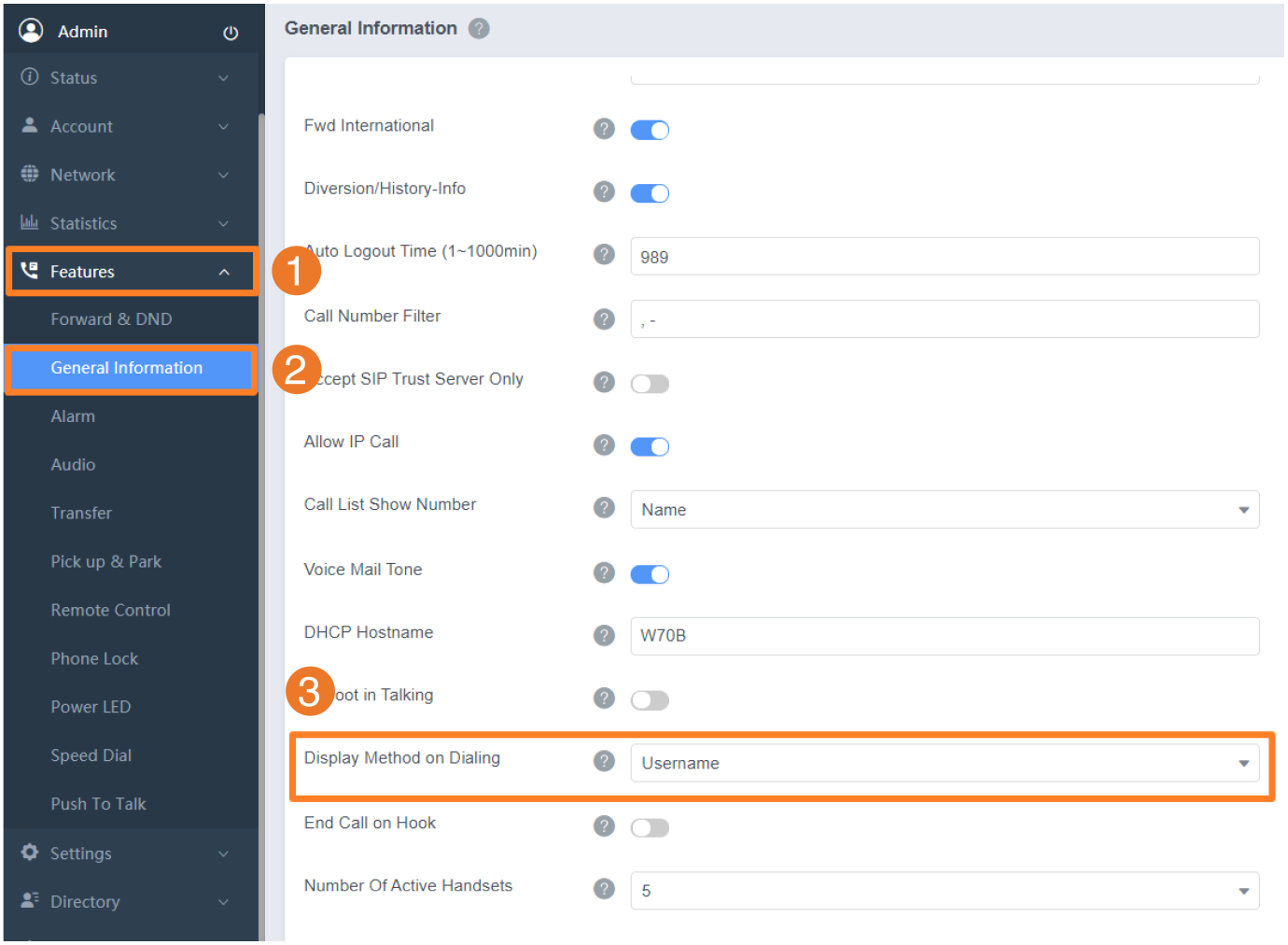
When the phone is on the pre-dialing or dialing screen, the account information will be displayed on the phone screen.

Yealink phones support three display methods: **Label**, **Display Name**, and **User Name**. You can customize the account information to be displayed on the IP phone as required.

Display Method on Dialing Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Display Method on Dialing**.



Configuration Parameter

features.caller_name_type_on_dialing

Parameter	Permitted Values	Default	Description
features.caller_name_type_on_dialing	**1**-Label, configured by the parameter account.X.label. **2**-Display Name, configured by the parameter account.X.display_name. **3**-User Name, configured by the parameter account.X.user_name.	3	It configures the selected account information displayed on the pre-dialing or dialing screen.

Key As Send

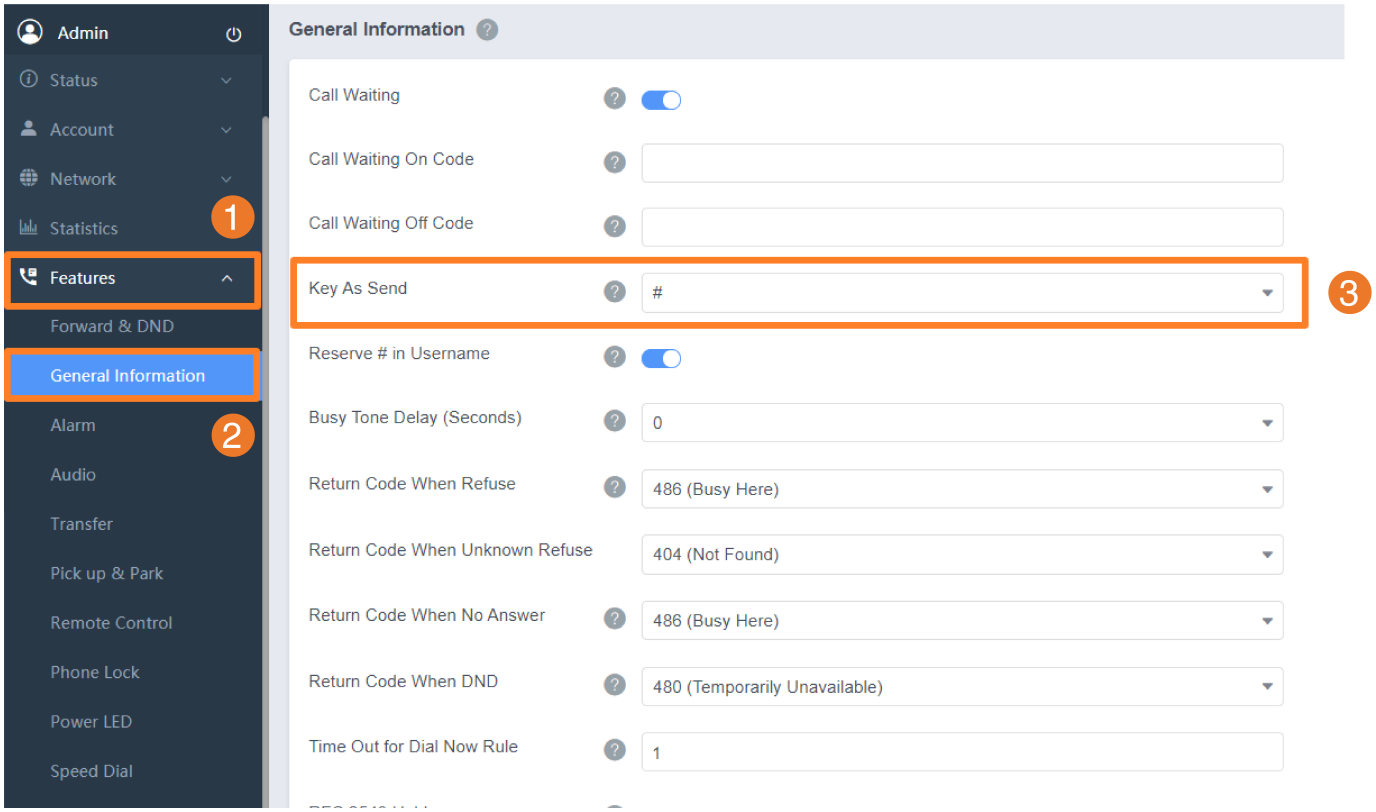
Introduction

Key as send allows you to assign the pound key ("#") or asterisk key ("*") as the send key.

Key As Send Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Key As Send**.



Configuration Parameter

features.key_as_send

Parameter	Permitted Values	Default	Description
features.key_as_send	**0**-Disabled **1**-# key **2**-* key	0	It configures the "#" or "*" key as the send key.

Recent Call Display in Dialing

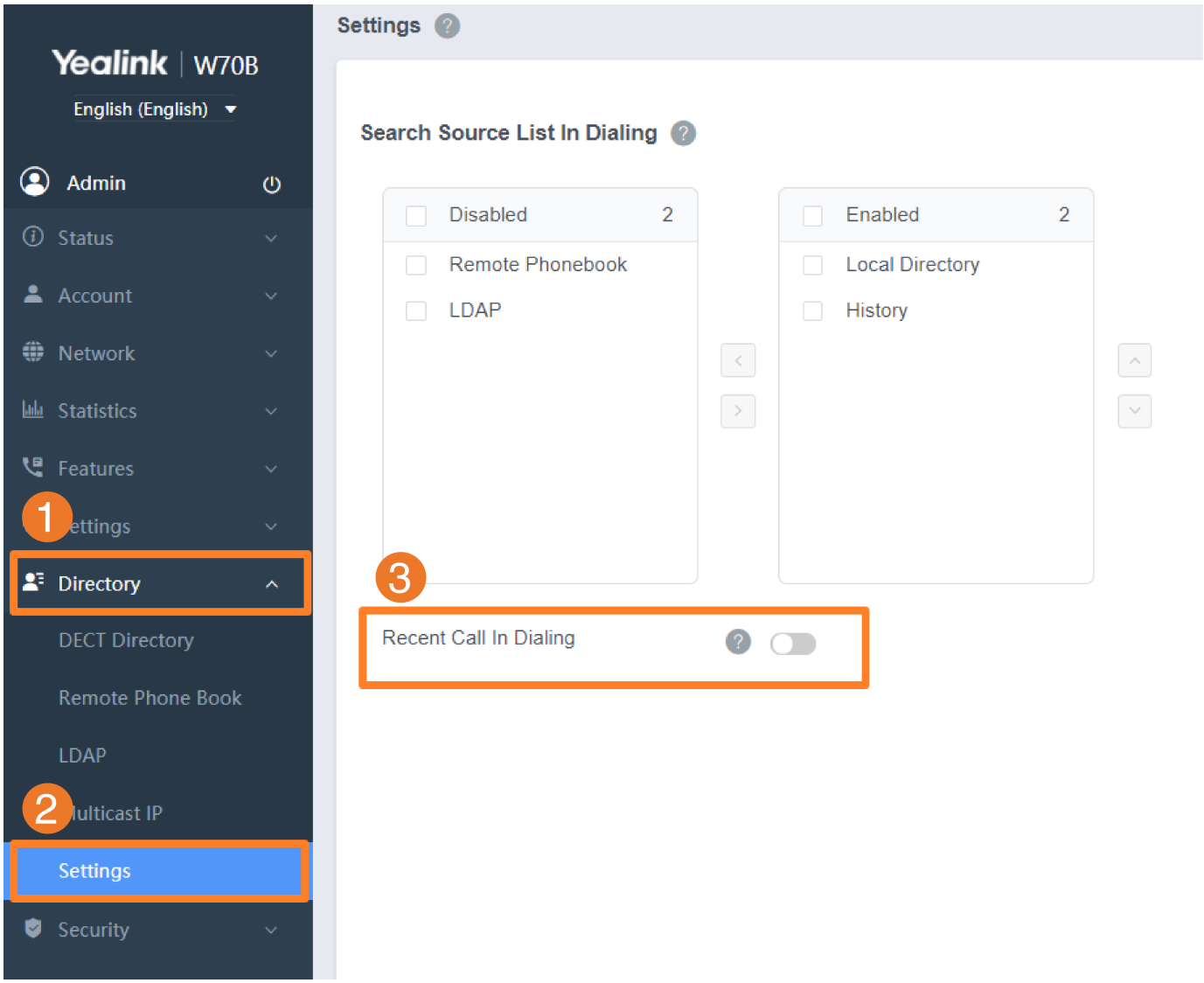
Introduction

Recent call display allows you to view the placed calls list when the phone is on the dialing screen. You can select to place a call from the placed calls list.

Recent Call in Dialing Configuration

Set via the Web User Interface

1. On the web user interface, go to **Directory** > **Settings** > **Recent Call In Dialing**.



Configuration Parameter

super_search.recent_call

Paramete	Permitted Values	Def	Description

r		aul t	
super_search.recent_call	**0**-Disabled **1**-Enabled, users can view the placed calls list when the phone is on the dialing screen.	1	It enables or disables the **Recent Call in Dialing** feature.

Warnings Display

Introduction

Yealink phones support displaying the warning details about the issue in the **Status** screen when the default password is used.

Warnings Display Configuration

Configuration Parameter

phone_setting.warnings_display.mode

Parameter	Permitted Values	Default	Description
phone_setting.warnings_display.mode	**0**-Disabled **1**-Enabled	1	It enables or disables the phone to display warnings.

Advisory Tone

Introduction

Advisory tones are the acoustic signals of your handset, which inform you of different actions and states.

You can configure the following advisory tones independently of each other:

Advisory Tones	Description	Supported Device
Keypad Tone	Plays when you press any key on the keypad.	W53H/W56H/W57R/W59R/W59R Pro/ W71H/W73H/W74H/W78H/CP930W
Key Tone	Plays when you tap the dial pad.	CP935W
Touch Tone	Plays when you tap the keys (except the off-hook key and the touch keypad).	CP930W/CP935W
Confirmation	Plays when you save settings or place the handset in the charger cradle.	W53H/W56H/W57R/W59R/W59R Pro/ W71H/W73H/W74H/W78H/CP930W
Low Battery	Plays when the battery capacity is low and the handset requires charging.	W53H/W56H/W57R/W59R/W59R Pro/ W71H/W73H/W74H/W78H/CP930W/ CP935W

Before You Begin

This feature is not applicable to DD phones.

Advisory Tones Configuration

Configuration Parameter

```
custom.handset.keypad_tone.enable
custom.handset.confirmation_tone.enable
custom.handset.low_battery_tone.enable
```

Parameter	Permitted Values	Default	Description
custom.handset.keypad_tone.enable	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled **1**-Enabled	-1	It enables or disables the handset to play a tone when any key is pressed. For CP930W, it plays a tone only when the touch keypad is tapped. It will take effect on all handsets that are registered on the same base station. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled) and the silent mode is off.
custom.handset.confirmation_tone.enable	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled **1**-Enabled	-1	It enables or disables the handset to play a tone when a user saves settings or places the handset in the charger cradle. It will take effect on all handsets that are registered on the same base station. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled) and the silent mode is off.
custom.handset.low_battery_tone.enable	**-1**-Do not modify the handset configuration (Keep the original configuration of the handset). **0**-Disabled **1**-Enabled	-1	It enables or disables the handset to play a tone when 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.

Shortcut Customization

Introduction

Shortcuts allow you to quickly and directly access the feature without scrolling through the menu when the phone is idle. You can customize six shortcuts on the handset in total.

Before You Begin

It is only applicable to W71H, W73H, W74H, W78H, W53H, W56H, W57R, W59R, and W59R Pro.

Shortcut Customization Configuration

Configuration Parameter

```
custom.handset.defined_left_key.type
custom.handset.defined_right_key.type
custom.handset.defined_direction_left_key.type
custom.handset.defined_direction_right_key.type
custom.handset.defined_direction_up_key.type
custom.handset.defined_direction_down_key.type
custom.handset.defined_left_key.xml_url
custom.handset.defined_right_key.xml_url
custom.handset.defined_direction_left_key.xml_url
custom.handset.defined_direction_right_key.xml_url
custom.handset.defined_direction_up_key.xml_url
custom.handset.defined_direction_down_key.xml_url
custom.handset.X.defined_left_key.xml_url
custom.handset.X.defined_right_key.xml_url
custom.handset.X.defined_direction_left_key.xml_url
custom.handset.X.defined_direction_right_key.xml_url
custom.handset.X.defined_direction_up_key.xml_url
custom.handset.X.defined_direction_down_key.xml_url
```

Parameter	Permitted Values	Def aul	Description

		t	
custom.handset.defined_left_key.type custom.handset.defined_right_key.type	0: current experience 1: History 2: missed calls 3: accepted calls 4: Redial 5: SpeedDial 6: Menu 7: Line Status 8: Outgoing Line 9: Call Forward 10: DND 11: Intercom 12: Directory 13: Local Directory 14: Network Directory 15: LDAP 16: Remote phonebook 17: Volume+ 18: Volume- 19: Balance 20: Retrieve 21: History 23: Shared Directory 24: Status 25: XML Browser	0	It configures the role of the Left Softkey/Right Softkey on the idle screen.

	26: XML Dir (XML Phone Book) 29: Signin 30: Login 31: Empty		
custom.handset.defined_direction_left_key.type custom.handset.defined_direction_right_key.type custom.handset.defined_direction_up_key.type custom.handset.defined_direction_down_key.type	0: current experience 1: History 2: missed calls 3: accepted calls 4: Redial 5: SpeedDial 6: Menu 7: Line Status 8: Outgoing Line 9: Call Forward 10: DND 11: Intercom 12: Directory 13: Local Directory 14: Network Directory 15: LDAP 16: Remote phonebook 17: Volume+ 18: Volume- 19: Balance 20: Retrieve 21: History	0	It configures the role of the left/right/up/down navigation key on the idle screen.

	23: Shared Directory 24: Status 25: XML Browser 26: XML Dir (XML Phone Book) 29: Signin 30: Login 31: Empty		
custom.handset.defined_left_key.xml_url custom.handset.defined_right_key.xml_url custom.handset.defined_direction_left_key.xml_url custom.handset.defined_direction_right_key.xml_url custom.handset.defined_direction_up_key.xml_url custom.handset.defined_direction_down_key.xml_url	String within 512 characters	Blank	It configures the available access URL to browse the XML object. It works only if "custom.handset.defined_left_key.type"/"custom.handset.defined_right_key.-type"/"custom.handset.defined_direction_left_key.type"/'custom.handset.defined_direction_right_key.type"/"custom.handset.defined_direction_up_key.type"/"custom.handset.defined_direction_down_key.type" is set to 25 (XML Browser).
custom.handset.X.defined_left_key.xml_url[1] custom.handset.X.defined_right_key.xml_url[1] custom.handset.X.defined_direction_left_key.xml_url[1] custom.handset.X.defined_direction_right_key.xml_url[1]	String within 512 characters	Blank	It configures the available access URL to browse the XML object. It works only if "custom.handset.defined_left_key.type"/"custom.handset.defined_right_key.-type"/"custom.handset.def

custom.handset.X.defined_direction_up_key.xml_url[1] custom.handset.X.defined_direction_down_key.xml_url[1]			ined_direction_left_key.type"/'custom.handset.defined_direction_right_key.type"/"custom.handset.defined_direction_up_key.type"/"custom.handset.defined_direction_down_key.type" is set to 25 (XML Browser).

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

Bluetooth

Introduction

CP930W-Base/CP935W-Base phones support Bluetooth. You can pair and connect the Bluetooth-enabled mobile phone with your phone, and make and receive mobile calls on the phone. After connecting the Bluetooth-enabled mobile phone, you can also use your phone as a Bluetooth speaker for your mobile phone and PC. You can set up a conference among the calls on your IP phone, PC, and connected mobile phone. CP935W-Base also supports Bluetooth name editing; you can edit the Bluetooth name that you want.

Supported Devices

CP935W-Base



CP930W-Base



Bluetooth Configuration

You can activate or deactivate the Bluetooth mode and personalize the Bluetooth device name for the IP phone. It is helpful for the other Bluetooth devices to identify and pair with your IP phone.

Configuration Parameter

static.bluetooth.function.enable
bluetooth.connect_confirm.enable

Parameter	Permitted Values	Default	Description
static.bluetooth.function.	**0**-Disabled, you are not allowed to trigger	1	It enables or disables the Bluetooth feature.

enable[1]	Bluetooth mode on. **1**-Enabled		
bluetooth.connect_confirm.enable[1]	**0**-Disabled **1**-Enabled, the prompt will not appear during the call.	0	It enables or disables the phone to prompt users to confirm the connection request from the Bluetooth device.

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

DSS Keys

Introduction

You can assign various functions to DSS keys. This section explains how to set these keys.

Line Keys

Line keys provide a 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).

Supported Devices

CP935W-Base



T54W



Line Keys Configuration

Set via the Device Interface

- DD Phone:
- **Menu** > **Features** > **Dsskey**
- CP935W:
- **More** > **Features** > **Dsskey**

Configuration Parameter

ddp.X.linekey.Y.type
ddp.X.linekey.Y.line
ddp.X.linekey.Y.value
ddp.X.linekey.Y.label
ddp.X.linekey.Y.extension
handset.x.blf_base_handset.enable

Parameter	Permitted Values	Default	Description
ddp.X.linekey.Y.type[1] [2]	**0**-N/A **13**-SpeedDial (Speed Dial) **15**-Line **16**-BLF **310**-DECT Intercom **39**-BLF List **56**-Retrieve Park **114**-Push-to-Talk	0	It configures the key feature.
ddp.X.linekey.Y.line[1] [2]	0, 1-10	Blank	It configures the desired line to apply the line key feature.
ddp.X.linekey.Y.value[1] [2]	String within 99 characters	Blank	It configures the value for 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.
ddp.X.linekey.Y.label[1] [2]	String within 99 characters	Blank	It configures the label displayed on the phone screen. This is an optional configuration.
ddp.X.linekey.Y.extension[1] [2]	String within 99 characters	Blank	For the BLF/BLF list feature: It configures the pickup code.
handset.x.blf_base_handset.enable	**0**-Disabled **1**-Enabled	0	It configures whether the handset X can subscribe to other handsets via the base.

> [1]X is the DD phone ID. X=1-10.
> [2]Y is the line key ID. Y=1-16 (for T54W DD phone)/Y=1-30 (for CP935W-Base).

Other Handset Settings Parameter

Handset Settings Parameters

custom.handset.eco_mode.enable
handset.X.hac.enable

Parameter	Permitted Values	Default	Description
custom.handset.eco_mode.enable	**0**-Disabled **1**-Enabled	0	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.
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.

[1]X is the handset ID. X=1 to 10.

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**.

Before You Begin

This feature is only applicable to W70B.

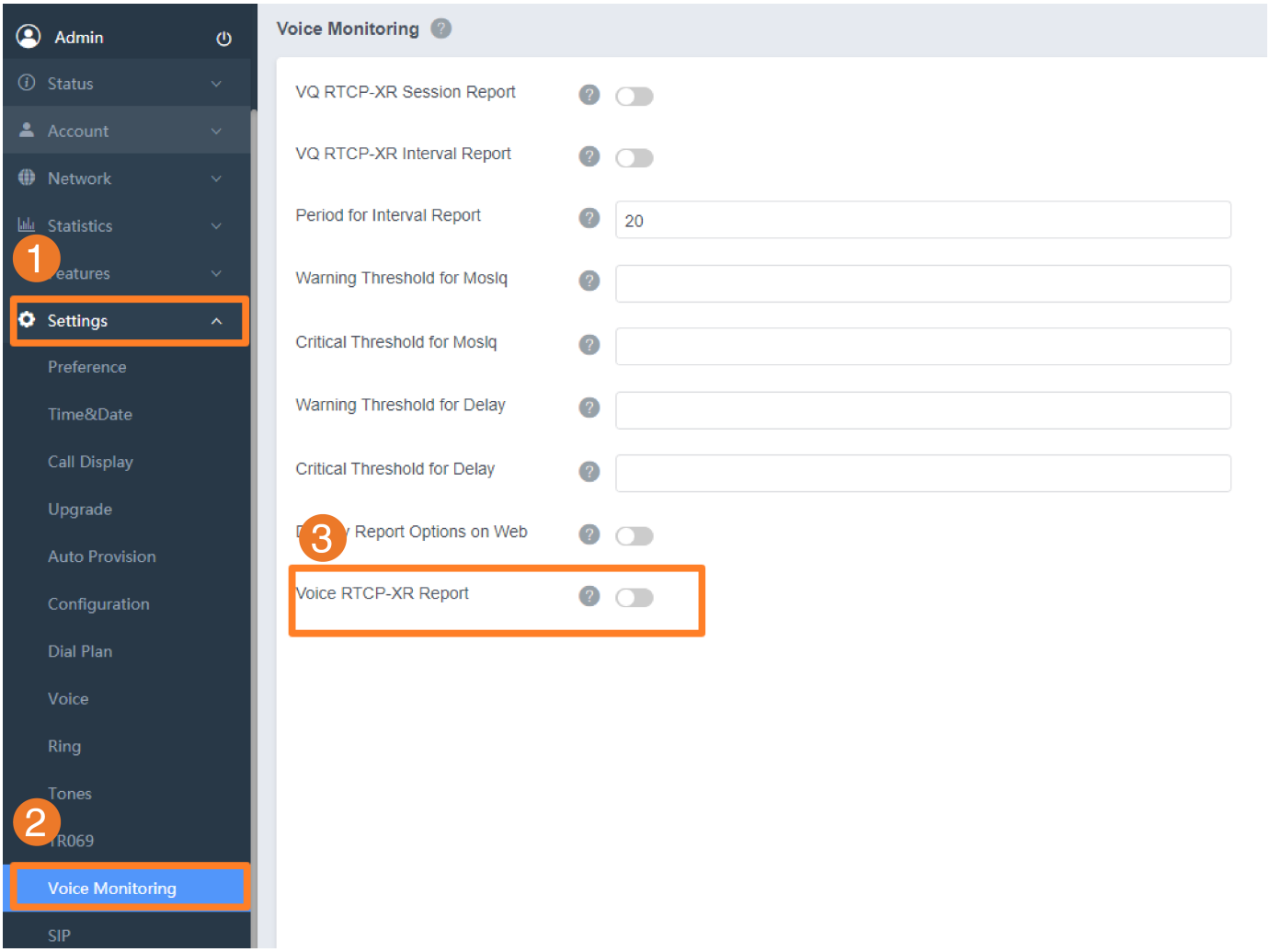
RTCP-XR

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

1. 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 are generated in the following three ways:

- Based on current values, such as jitter, jitter buffer max, and round trip delay.
- Covers the time period from the beginning of the caluntithe 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

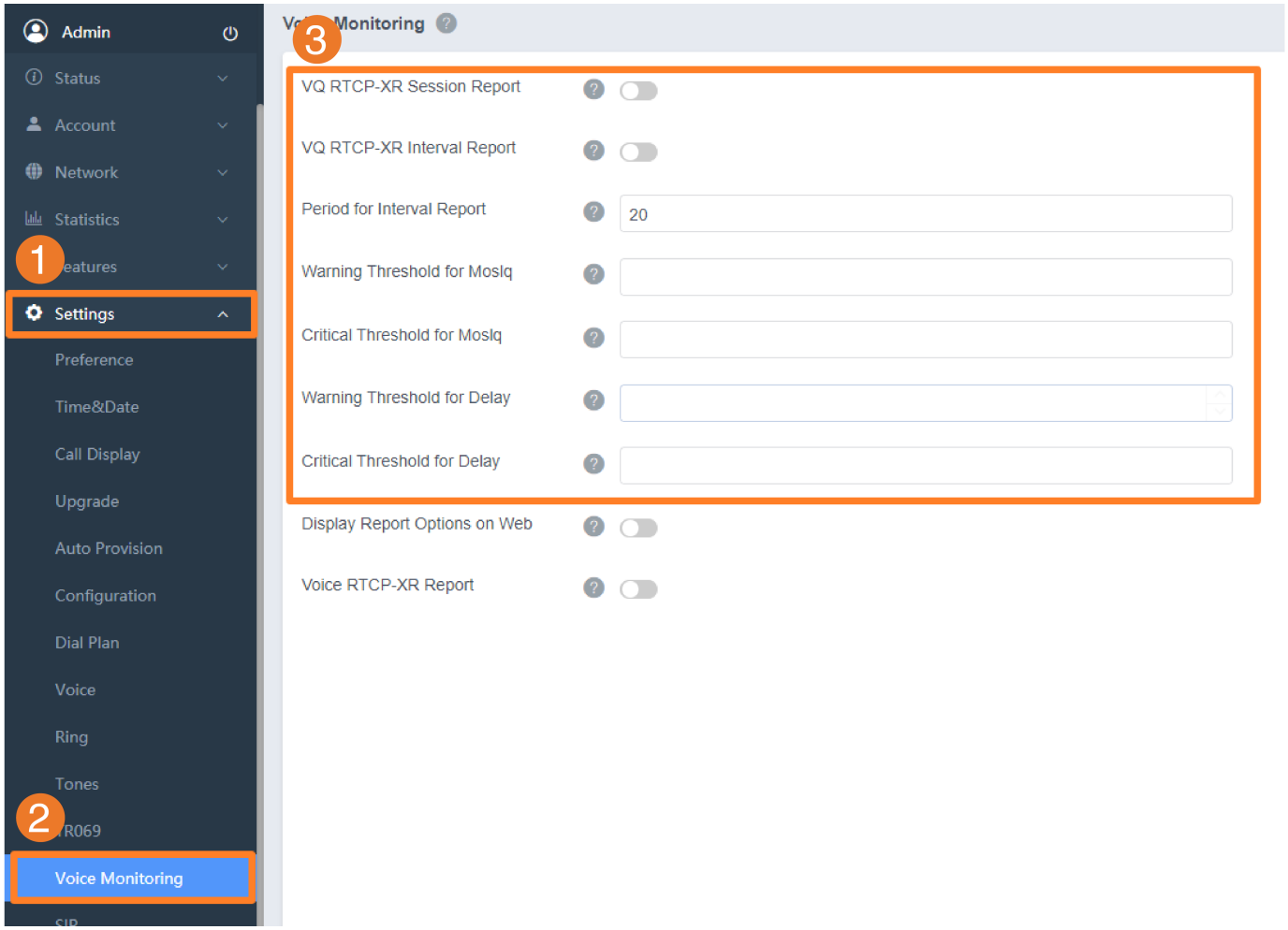
Three types of quality reports can be enabled:

- **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_rtcpxr_moslq_threshold_critical	Integer from 15 to 40	Blank	It configures the threshold value of listening MOS score (MOS-LQ) multiplied by 10. The threshold value of MOS-LQ causes the phone to send a critical alert quality report to the central report collector. For example, a configured value of 28 corresponds to the MOS score 2.8. When the MOS-LQ value computed by the phone is less than or equal to 2.8, the phone will send a critical alert quality report to the central report collector. When the MOS-LQ value computed by the phone is greater than 2.8, the phone will not send a critical alert quality report to the central report collector. If it is set to blank, critical alerts are not generated due to MOS-LQ.
phone_setting.vq_rtcpxr_delay_threshold_warning	10 to 2000	Blank	It configures the threshold value of one-way delay (in milliseconds) that causes the phone to send a warning alert quality report to the central report collector. For example, if it is set to 500, when the value of one way delay computed by the phone is greater than or equal to 500, the phone will send a warning alert quality report to the central report collector; when the value of one way delay computed by the phone is less than 500, the phone will not send a warning alert quality report to the central report collector. If it is set to blank, warning alerts are not generated due to one-way delay. The one-way delay includes both network delay and end system delay.
phone_setting.vq_rtcpxr_delay_threshold_critical	10 to 2000	Blank	It configures the threshold value of one-way delay (in milliseconds) that causes the phone to send a critical alert quality report to the central report collector. For example, if it is set to 500, when the value of one-way delay computed by the phone is greater than or equal to 500, the phone will send a critical alert quality report to the central report collector; when the value of one way delay computed by the phone is less than 500, the phone will not send a critical alert quality report to the central report collector.

			If it is set to blank, critical alerts are not generated due to one-way delay. The one-way delay includes both network delay and end system delay.

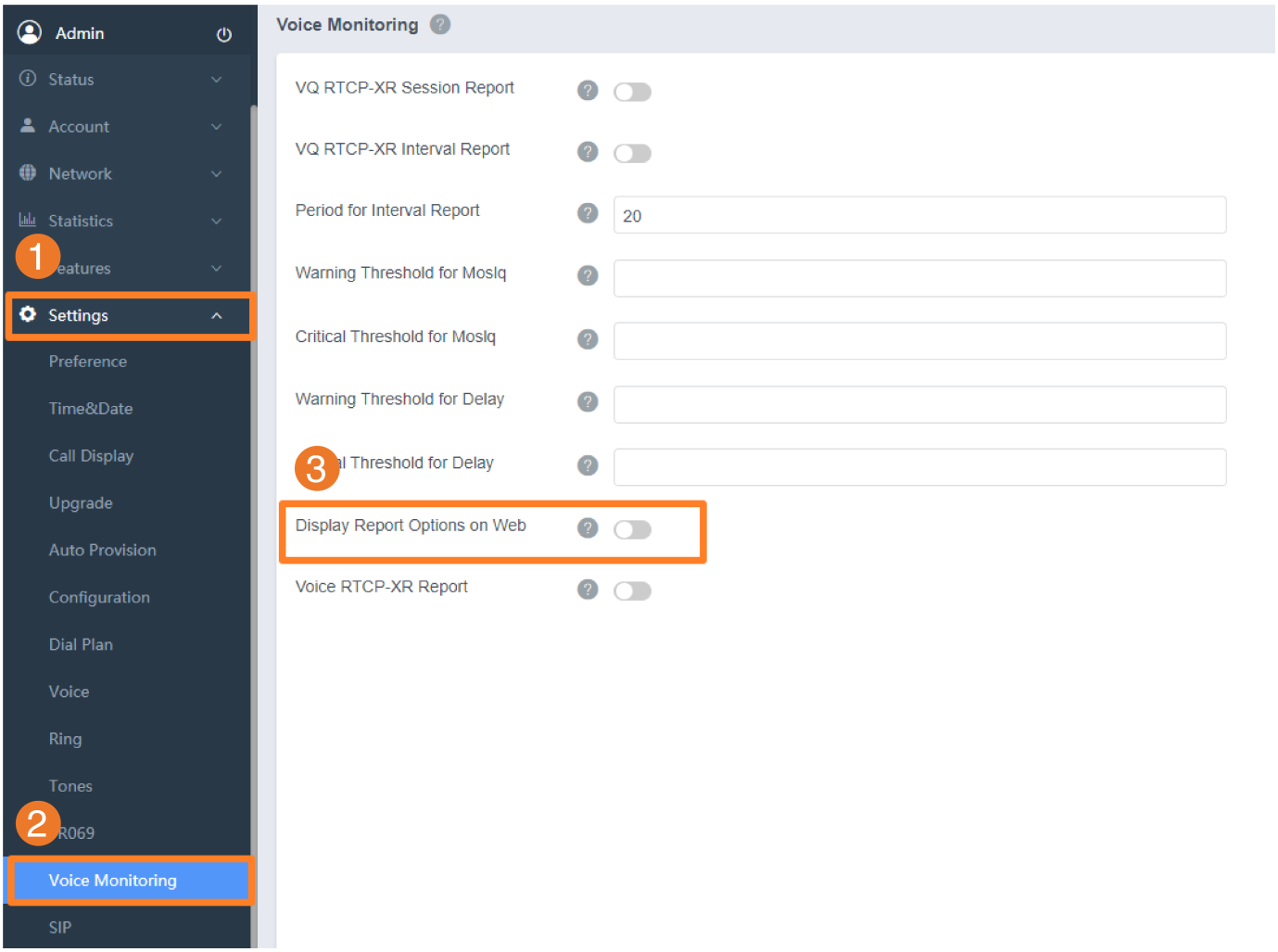
VQ-RTCPXR Display

You can check the voice quality data of the last call via the web user interface.

VQ-RTCPXR Display Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Voice Monitoring** > **Display Report Options on Web**.



Configuration Parameter

```
phone_setting.vq_rtcpxr.states_show_on_web.enable
```

Parameter	Permitted Values	Default	Description

phone_setting.vq_rtcpxr.states_show_on_web.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the voice quality data of the last call to be displayed on the web interface at the path **Status** > **RTP Status**.

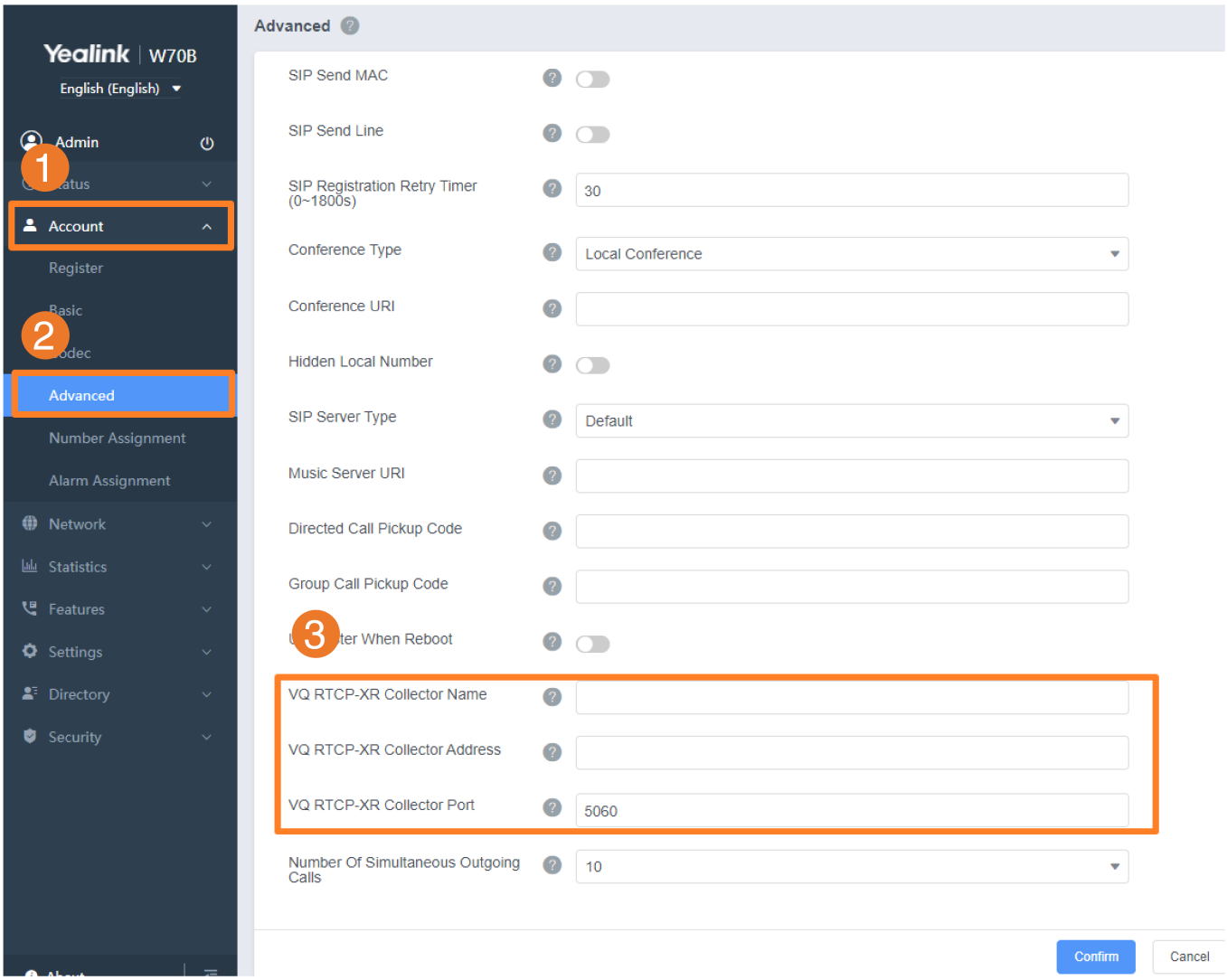
Central Report Collector

To operate with the central report collector, the phones must be configured to forward their voice quality reports to the specified report collector. You can specify the report collector on a per-line basis.

Central Report Collector Configuration

Set via the Web User Interface

1. On the web user interface, go to **Account** > **Advanced** > **VQ RTCP-XR Collector Name/VQ RTCP-XR Collector Address/VQ RTCP-XR Collector Port**.



Configuration Parameter

```
account.X.vq_rtcpxr.collector_name
account.X.vq_rtcpxr.collector_server_host
account.X.vq_rtcpxr.collector_server_port
```

Parameter	Permitted Values	Default	Description
account.X.vq_rtcpxr.collector_name[1]	String within 32 characters	Blank	It configures the hostname of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.
account.X.vq_rtcpxr.collector_server_host[1]	IPv4 Address/ FQDN	Blank	It configures the IP address of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.
account.X.vq_rtcpxr.collector_server_port[1]	Integer from 0 to 65535	5060	It configures the port of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

Alert Tone

Introduction

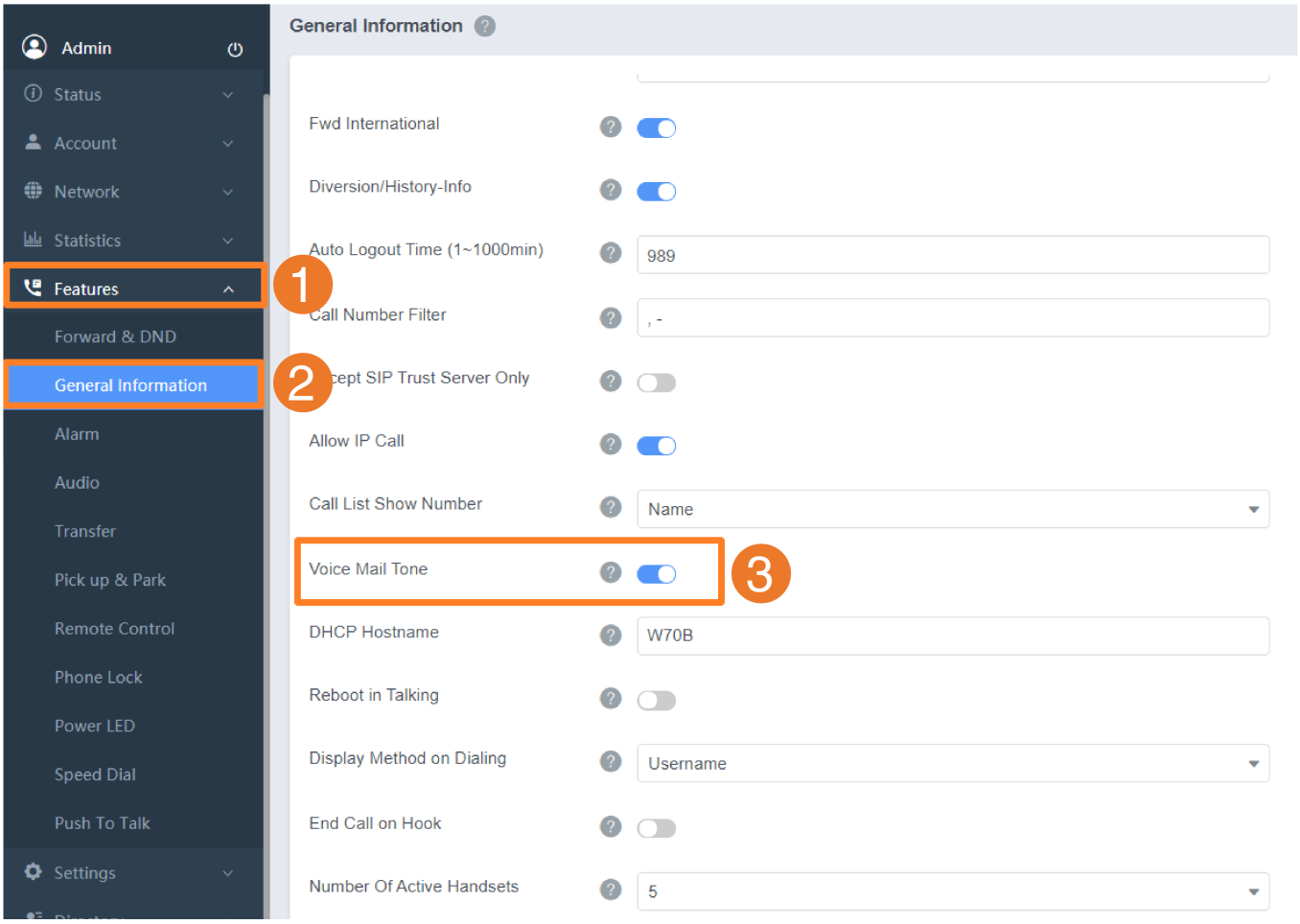
You can configure the following audio alert for the phone:

- **Voice mail tone**: allow the IP phone to play a warning tone when receiving a new voice mail. You can customize the warning tone or select specialized tone sets (which 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.

Alert Tone Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Voice Mail 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.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 from playing a warning tone when it receives a new voice mail. It works only if "account.X.display_mwi.enable" is set to 1 (Enabled).

Ringer Device

Introduction

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

The following table describes the headset types supported by different handsets.

Handset	3-segment Headset	4-segment Headset
W53H (3.5 mm)	supports	Only supports international standards (I version)
W56H (3.5 mm)	supports	Only supports international standards (I version)
W73H (3.5 mm)	supports	Only supports international standards (I version)
W74H (3.5 mm)	supports	Only supports international standards (I version)

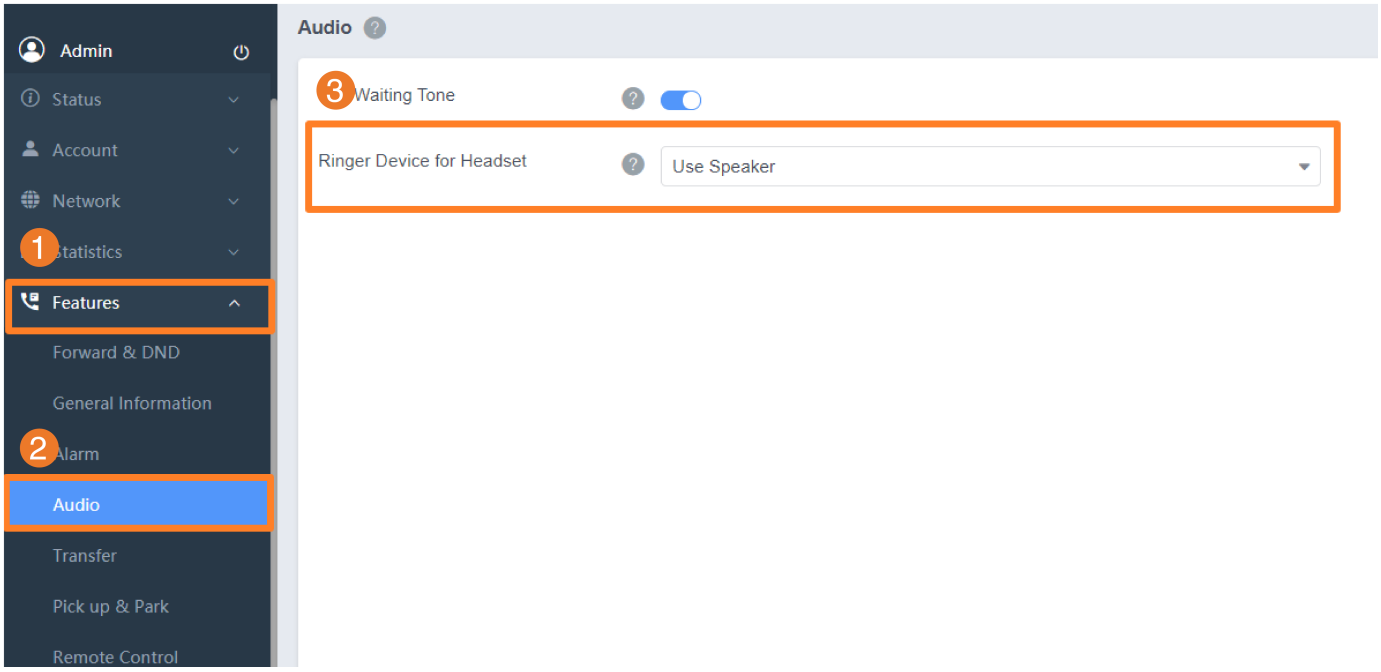
Before You Begin

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 Values	Default	Description
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 among Speaker mode by pressing the Speakerphone key , headset mode by pressing the HEADSET key , and handset mode by picking up the handset.

Audio Volume

Introduction

You can configure the phone's sending volume and ringer volume.

Fixed Ringer Volume

You can configure the ringer volume as a fixed level, so the user cannot adjust the ringer volume on the phone.

This feature avoids missing calls when the user turns down the ringer volume.

force.voice.ring_vol

Parameter	Permitted Values	Default	Description
force.voice.ring_vol	**Blank**-the user can adjust the ringer volume on the phone. **0 to 5**-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.

High Volume Mode

When using it in a noisy environment, you can adjust the volume of your device to a level higher than the normal range.

voice.device_volume.mode

Parameter	Permitted Values	Default	Description
voice.device_volume.mode	**0**-Disabled **1**-Enable	0	It configures whether to enable the handset's hands-free volume boost mode. Only applicable to W78H.

Tones

Introduction

When receiving a message, the phone will play a warning tone. You can customize tones or select specialized tone sets (which 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

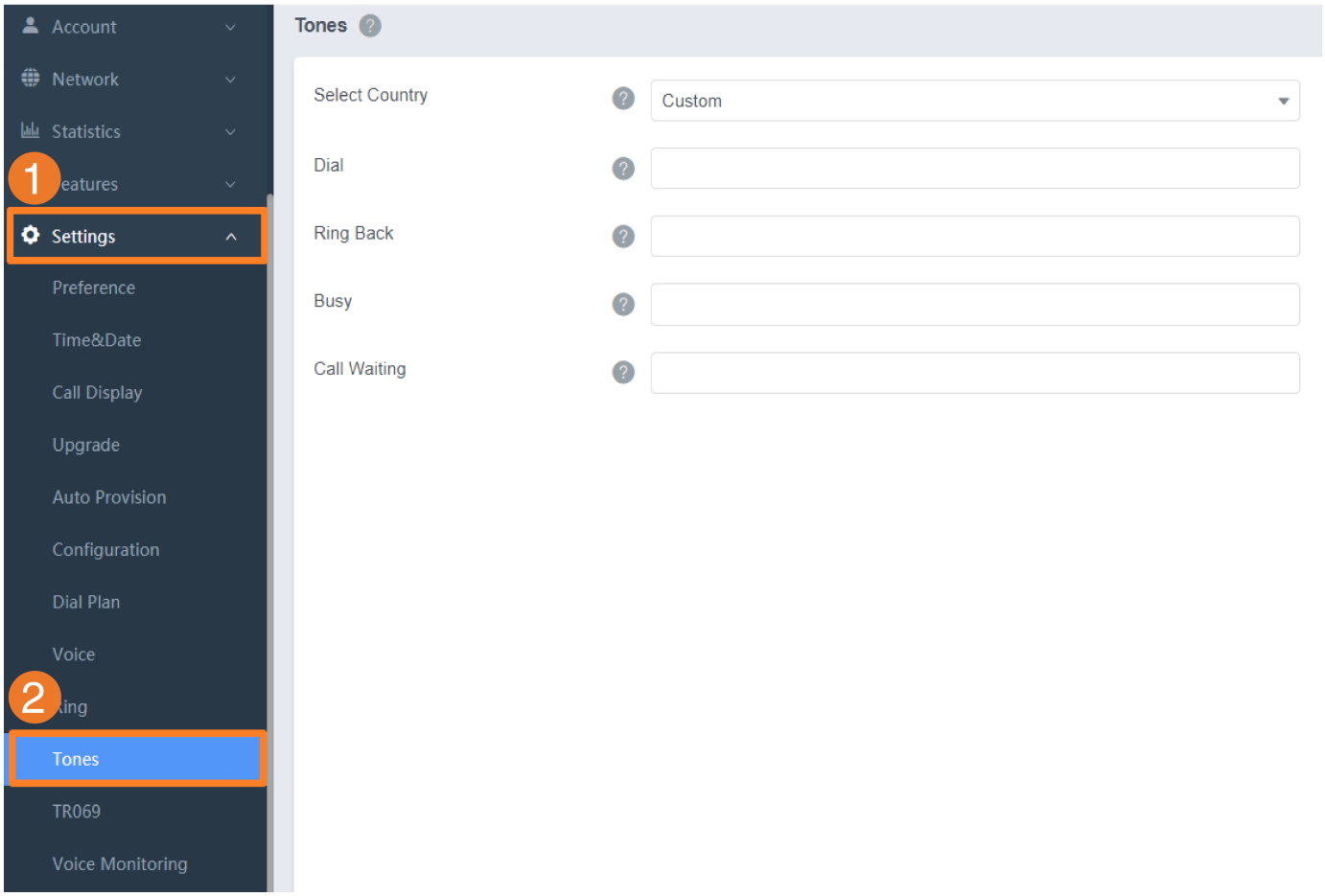
Configured tones can be heard on the phones in the following conditions.

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

```
voice.tone.country
voice.tone.dial
voice.tone.ring
voice.tone.busy
voice.tone.callwaiting
```

Parameter	Permitted Values	Default	Description
voice.tone.country	Custom, Australia, Austria, Brazil, Belgium, Chile, China, Czech, Czech ETSI, Denmark, Finland, France, Germany, Great	Custom	It configures the country tone for the phones.

	Britain, Greece, Hungary, Lithuania, India, Italy, Japan, Mexico, New Zealand, Netherlands, Norway, Portugal, Spain, Switzerland, Sweden, Russia, United States		
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. **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.
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	String	Bl	It customizes the tone when the callee is busy.

.tone.busy		Blank	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.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.

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 URL or keyword parameter and maps it to the appropriate ring tone.

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

Firmware Requirement

Supported Devices	Firmware Requirements
W70B	130.85.0.20 or later
W75B/W75DM	175.85.0.5 or later
W80B/W80DM	130.85.0.20 or later
W90B/W90DM	130.85.0.20 or later

Supported Alert-Info Headers Format

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

- 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 Alert-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	Ring Tone

	(features.alert_info_tone = 1)	(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	
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
Bellcore-dr2	2	Ringing	Long	630	800	1025
		Ringin	Long	630	800	1025

		g				
Bellcore-dr3	3	Ringing	Short	315	400	525
		Ringing	Short	315	400	525
		Ringing	Long	630	800	1025
Bellcore-dr4	4	Ringing	Short	200	300	525
		Ringing	Long	800	1000	1100
		Ringing	Short	200	300	525
Bellcore-dr5	5	Ringing		450	500	550

If the user is waiting for a call, "Bellcore-dr5" is a splash ring tone reminding the user that the DND or Always Call Forward 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 "MyMelodyN/MyMelodyRingN", the phone will play the corresponding local ring tone (RingN.wav), or play the first local ring tone (Ring1.wav) for about 10 seconds if "N" is greater than 10 or less than 1.

Examples:

```
Alert-Info: ringtone-2
Alert-Info: ringtone-Ring2.wav
```

```
Alert-Info: ringtone-2;x-line-id=1
Alert-Info: <http://10.1.0.31>;info=ringtone-2
Alert-Info: <http://127.0.0.1/ringtone-2>
Alert-Info: MyMelody2
Alert-Info: MyMelodyRing2.wav
Alert-Info: MyMelody2;x-line-id=1
Alert-Info: <http://10.1.0.31>;x-line-id=0;info=MyMelody2
```

The following table identifies the corresponding local ring tones:

Value of N	Ring Tone
1 Ring1.wav	Ring1.wav
2 Ring2.wav	Ring2.wav
3 Ring3.wav	Ring3.wav
4 Ring4.wav	Ring4.wav
5 Ring5.wav	Ring5.wav
6 Ring6.wav	Ring6.wav
7 Ring7.wav	Ring7.wav
8 Ring8.wav	Ring8.wav
N<1 or N>10	Ring1.wav

Alert-Info: info=info text;x-line-id=0

When the Alert-Info header contains an info text, the phone will map the text with the Interna Ringer 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 Interna Ringer 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:

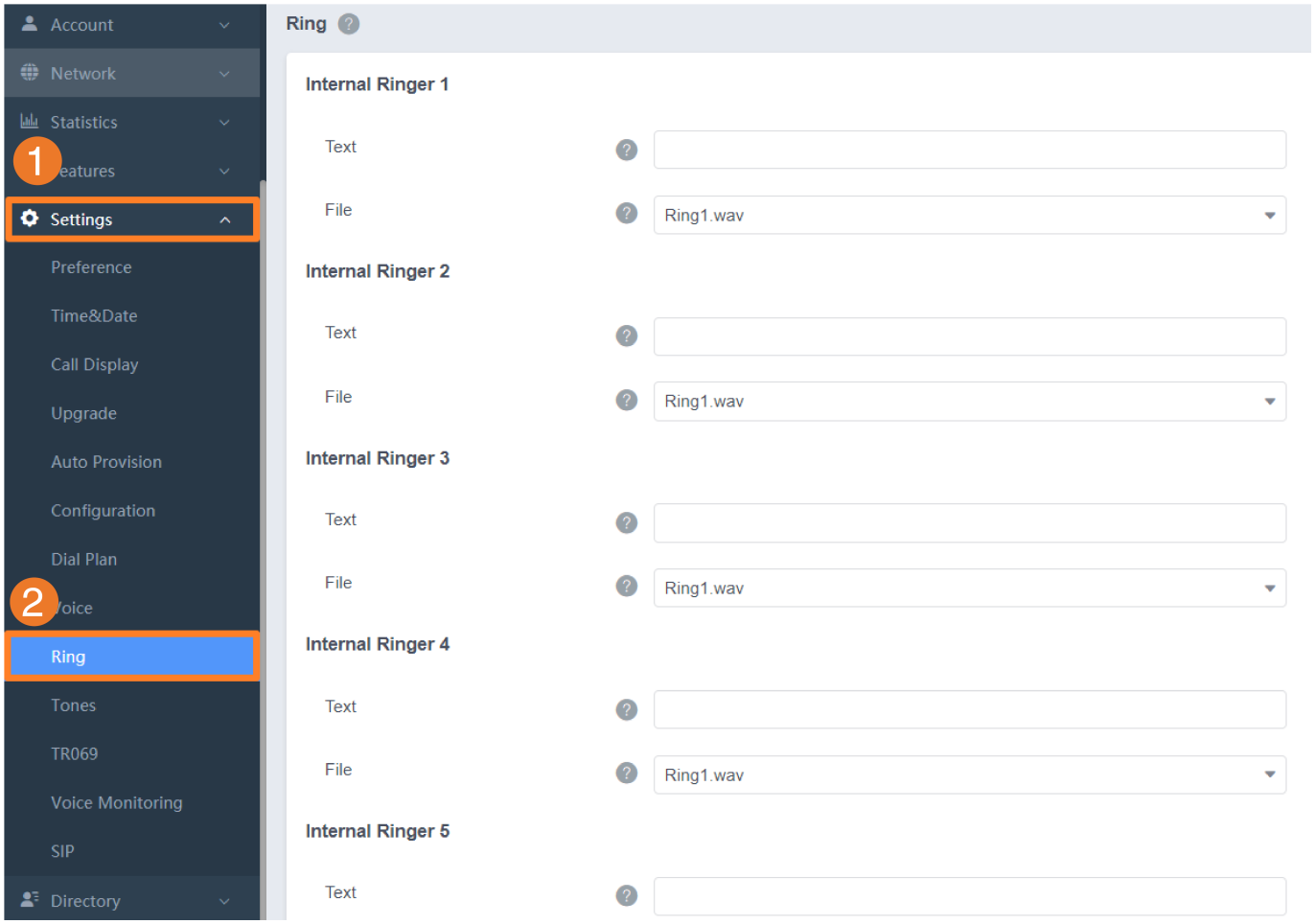
- Alert-Info: Auto Answer
- Alert-Info: info = alert-autoanswer
- Alert-Info: answer-after = 0 (or Alert-Info: Answer-After = 0)
- Alert-Info: Intercom

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[2]**.



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]	**For W70B**: • 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**	1	It configures the desired ring tone for each internal ringer text.

	3 or **Ring3.wav** **4** or **Ring4.wav** **5** or **Ring5.wav** **6** or **Ring6.wav** **7** or **Ring7.wav** **8** or **Ring8.wav** • Custom ring tone name (for example, CustomRing.wav) **For W75/W80/W90 Multi-Cell System:** • 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**		

[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 objective of the algorithm is to represent the high-fidelity audio signal with a minimum number of bits while retaining the quality. This can effectively reduce the frame size and the bandwidth required for audio transmission.

The audio codec that the phone uses to establish a call should be supported by the SIP server. When placing a call, the phone will offer the enabled audio codec list to the server and then use the audio codec negotiated with the called party according to the priority.

Supported Audio Codecs

The following table summarizes the supported audio codecs on the phones:

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
G722	G.722	RFC 3551	64 Kbps	16 Ksps	20 ms
PCMA(G.711A)	G.711 a-law	RFC 3551	64 Kbps	8 Ksps	20 ms
PCMU(G.711μ)	G.711 u-law	RFC 3551	64 Kbps	8 Ksps	20 ms
G729(G729A)	G.729	RFC 3551	8 Kbps	8 Ksps	20 ms
G726-16	G.726	RFC 3551	16 Kbps	8 Ksps	20 ms
G726-24	G.726	RFC 3551	24 Kbps	8 Ksps	20 ms
G726-32	G.726	RFC 3551	32 Kbps	8 Ksps	20 ms
G726-40	G.726	RFC 3551	40 Kbps	8 Ksps	20 ms
iLBC	iLBC	RFC 3952	15.2 Kbps 13.33 Kbps	8 Ksps	20 ms 30 ms

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.

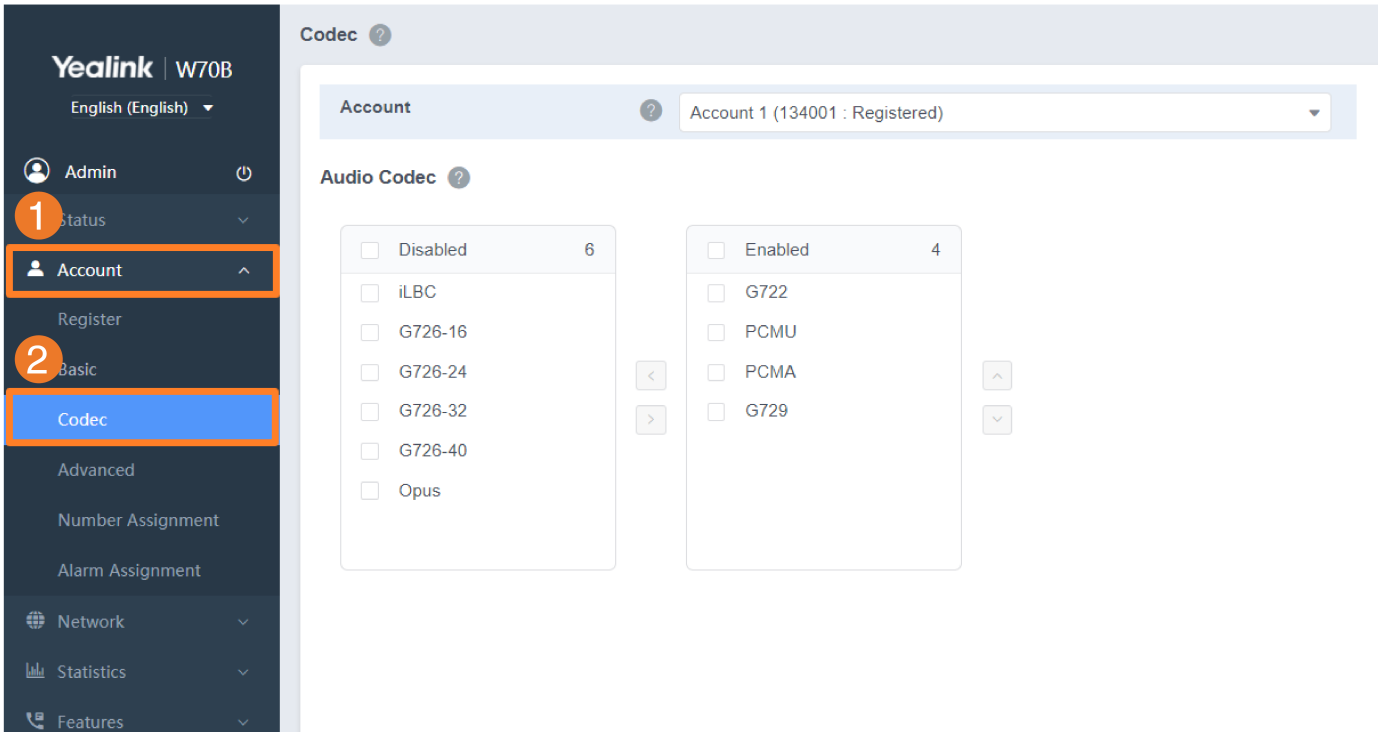
The following table lists the audio codecs supported by each phone model:

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

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	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)

		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;	**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_type>.priority[1]	Integer from 0 to 10	When the audio codec is G722, the default value is 1; When the audio codec is PCMU(G.711μ), the default value is 2; When the audio codec is PCMA(G.711A), the default 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	It configures the priority of the enabled audio codec. 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

		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 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.

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

Packetization Time (PTime)

Introduction

PTime is a measurement of the duration (in milliseconds) of how long the audio data in each RTP packet is sent to the destination, and defines how much the network bandwidth is used for the RTP stream transfer. Before establishing a conversation, codec and ptime are negotiated through SIP signaling. The valid values of ptime range from 10 to 60, in increments of 10 milliseconds. The default ptime is 20 ms. You can also disable the ptime negotiation.

Supported PTime of Audio Codec

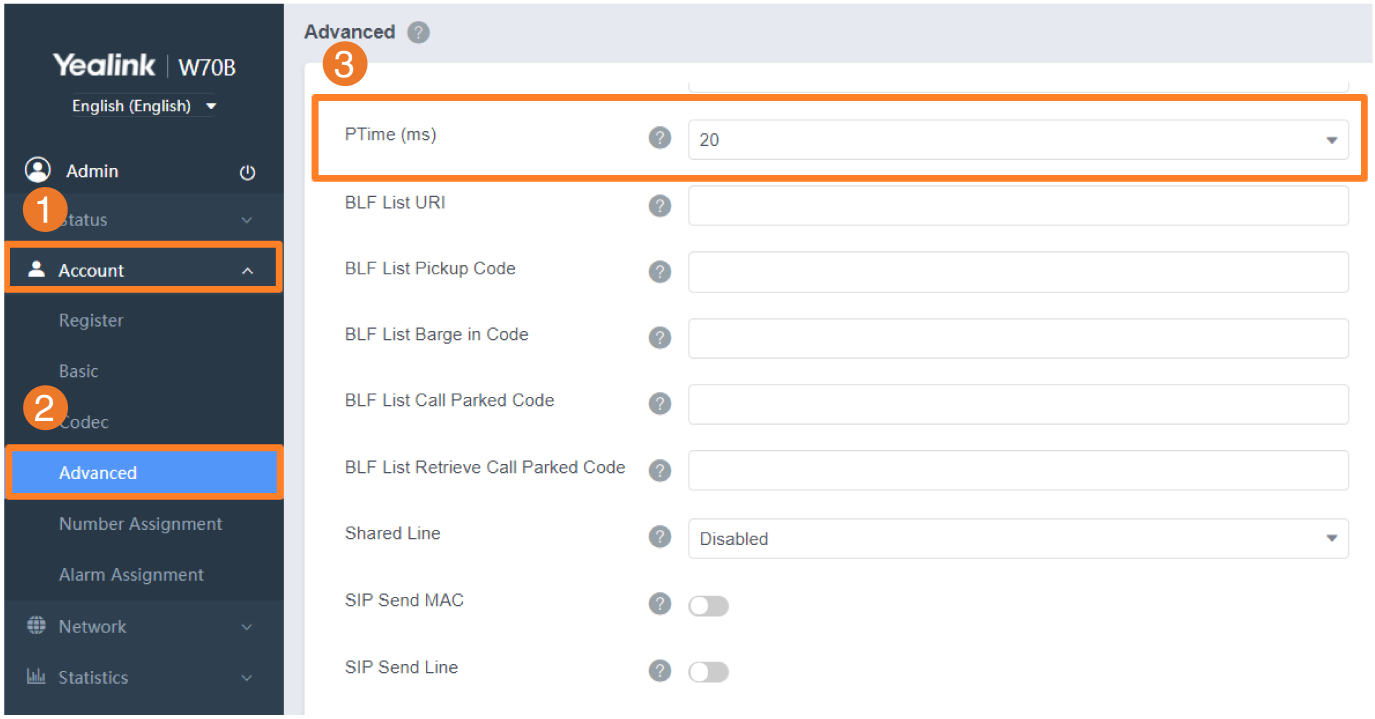
The following table summarizes the valid values of ptime for each audio codec:

Codec	Packetization Time (Minimum)	Packetization Time (Maximum)
G722	10 ms	40 ms
PCMA	10 ms	40 ms
PCMU	10 ms	40 ms
G729	10 ms	80 ms
G726-16	10 ms	30 ms
G726-24	10 ms	30 ms
G726-32	10 ms	30 ms
G726-40	10 ms	30 ms
iLBC	20 ms	30 ms

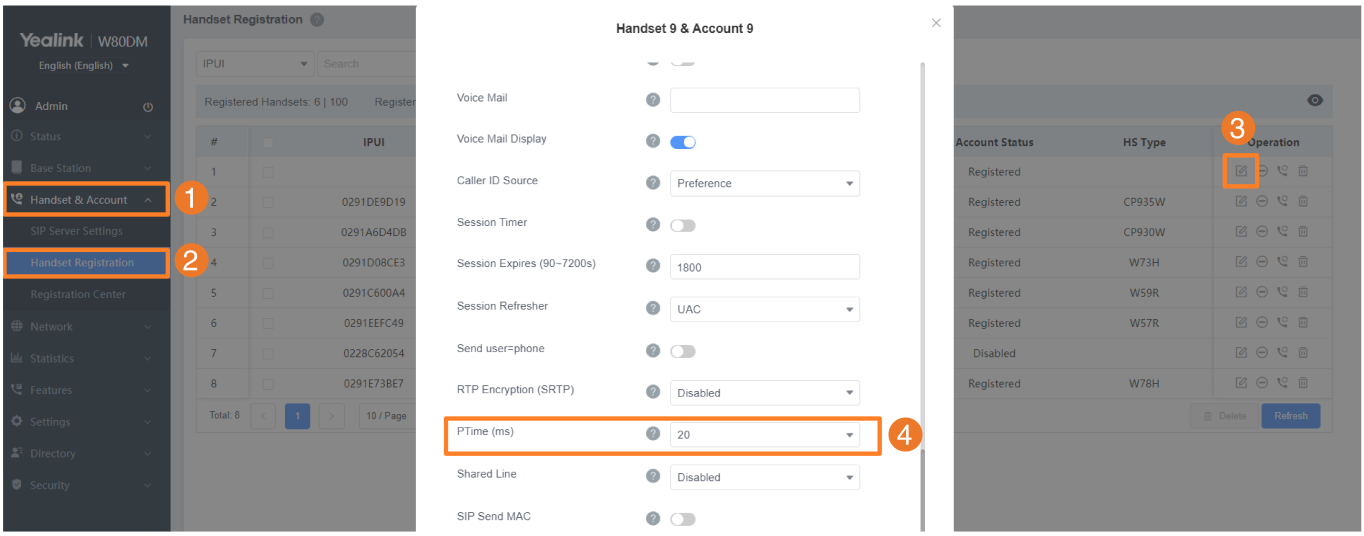
PTime Configuration

Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Advanced** > **PTime (ms)**.



2. For W75/W80/W90 Multi-Cell system: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **PTime (ms)**.



Configuration Parameter

account.X.ptime

Parameter	Permitted Values	Default	Description
account.X.ptime[1]	**0**-Disabled **10**-10 **20**-20 **30**-30	20	It configures the ptime (in milliseconds) for the codec.

	40-40 **50**-50 **60**-60		

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 multi-cell system, X=1-100.
- For W90 multi-cell system, X=1-250.
- For VIM system, X=1-2500.

Early Media

Introduction

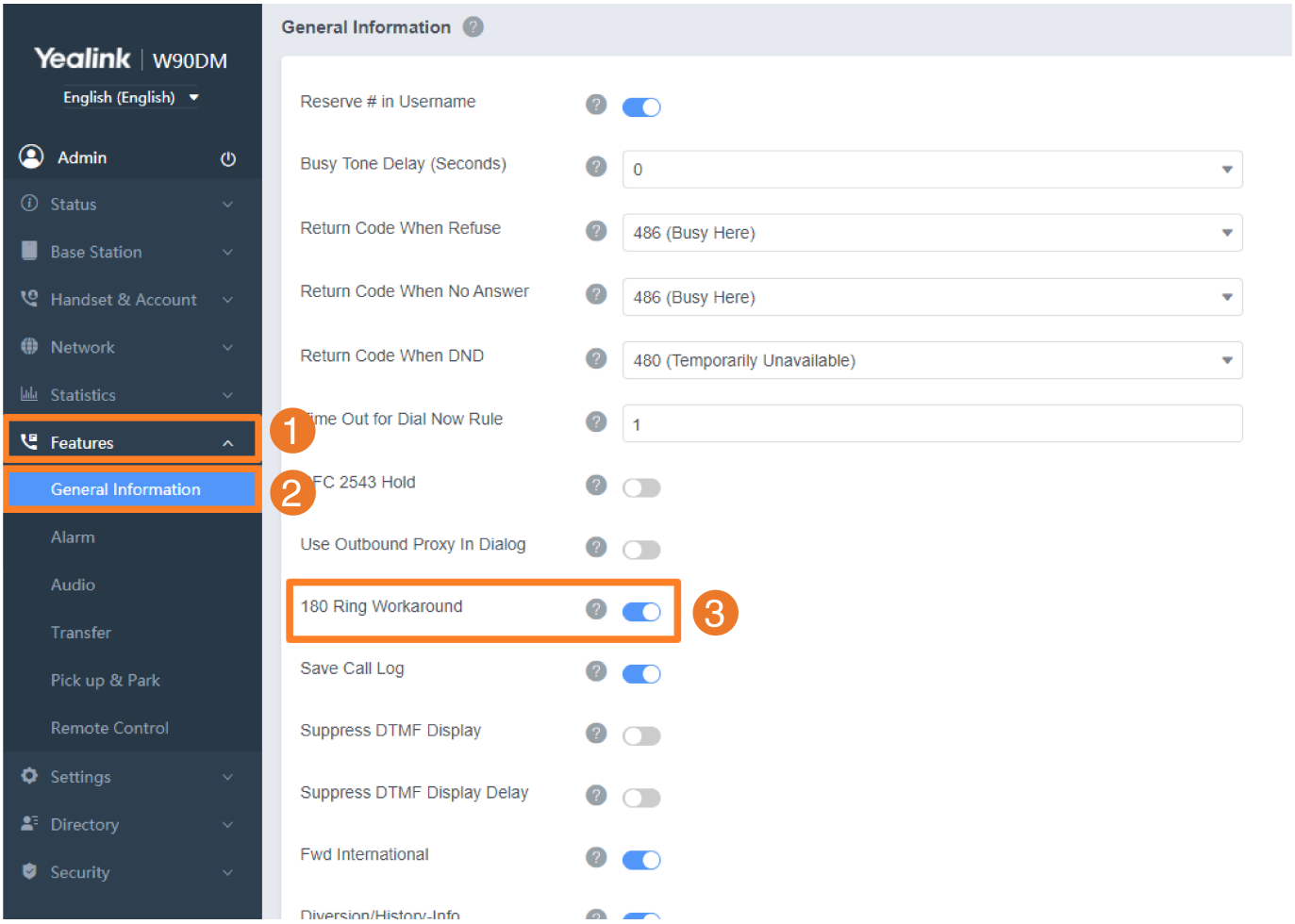
The early media refers to the media (for example, audio and video) played to the caller before a SIP call is actually established.

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

1. 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.

Supported Devices

CP935W-Base



CP930W-Base



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.

Automatic Gain Control (AGC)

Automatic Gain Control (AGC) is applicable to 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.

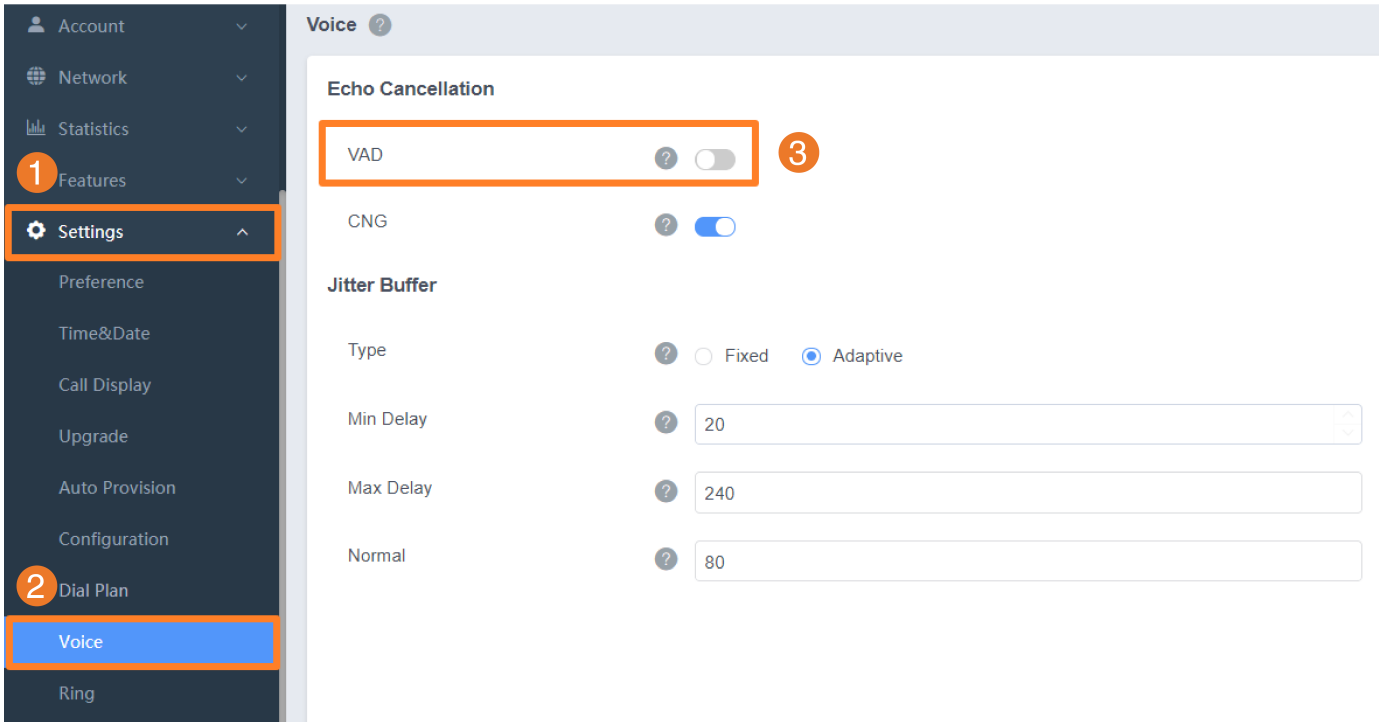
Voice Activity Detection (VAD)

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

1. 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)

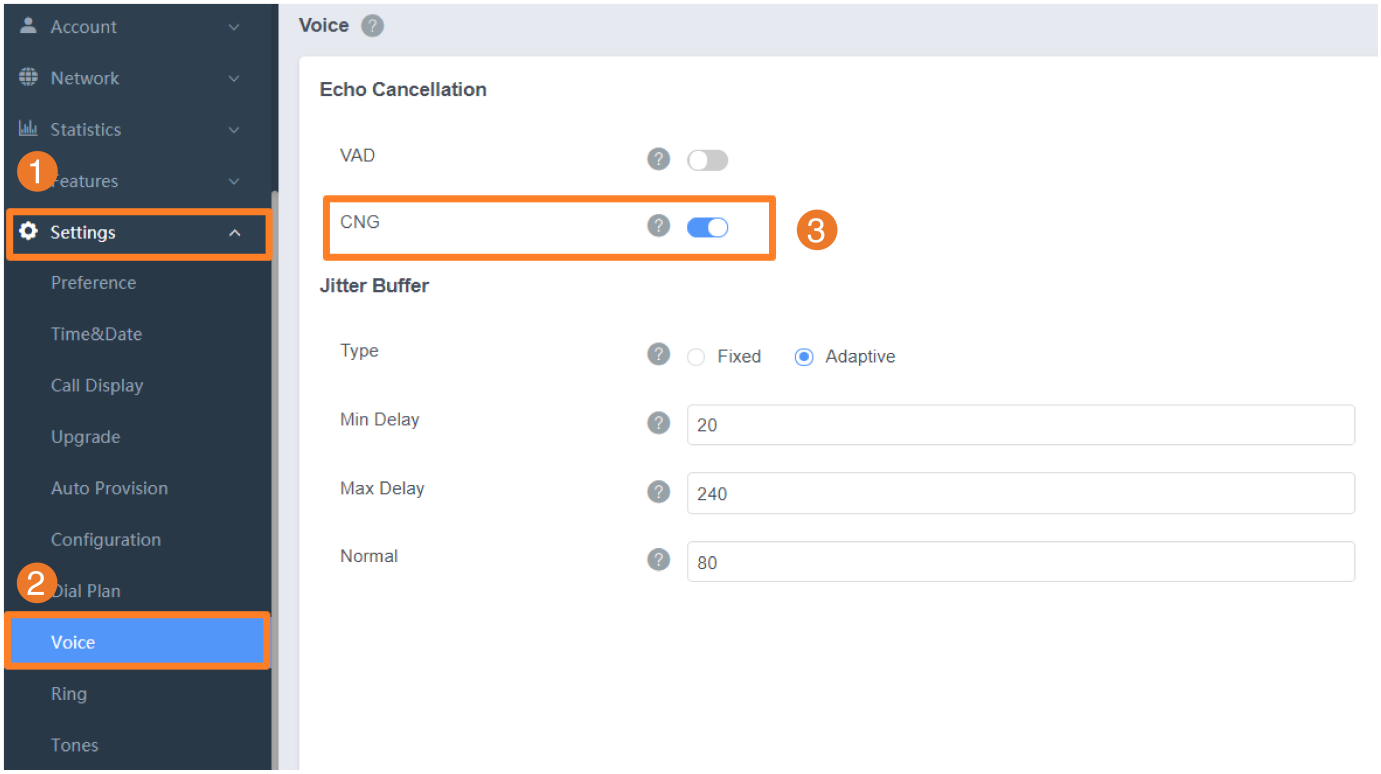
Comfort Noise Generation (CNG) is used to generate background noise for voice communications during periods of silence in a conversation.

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

1. 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.

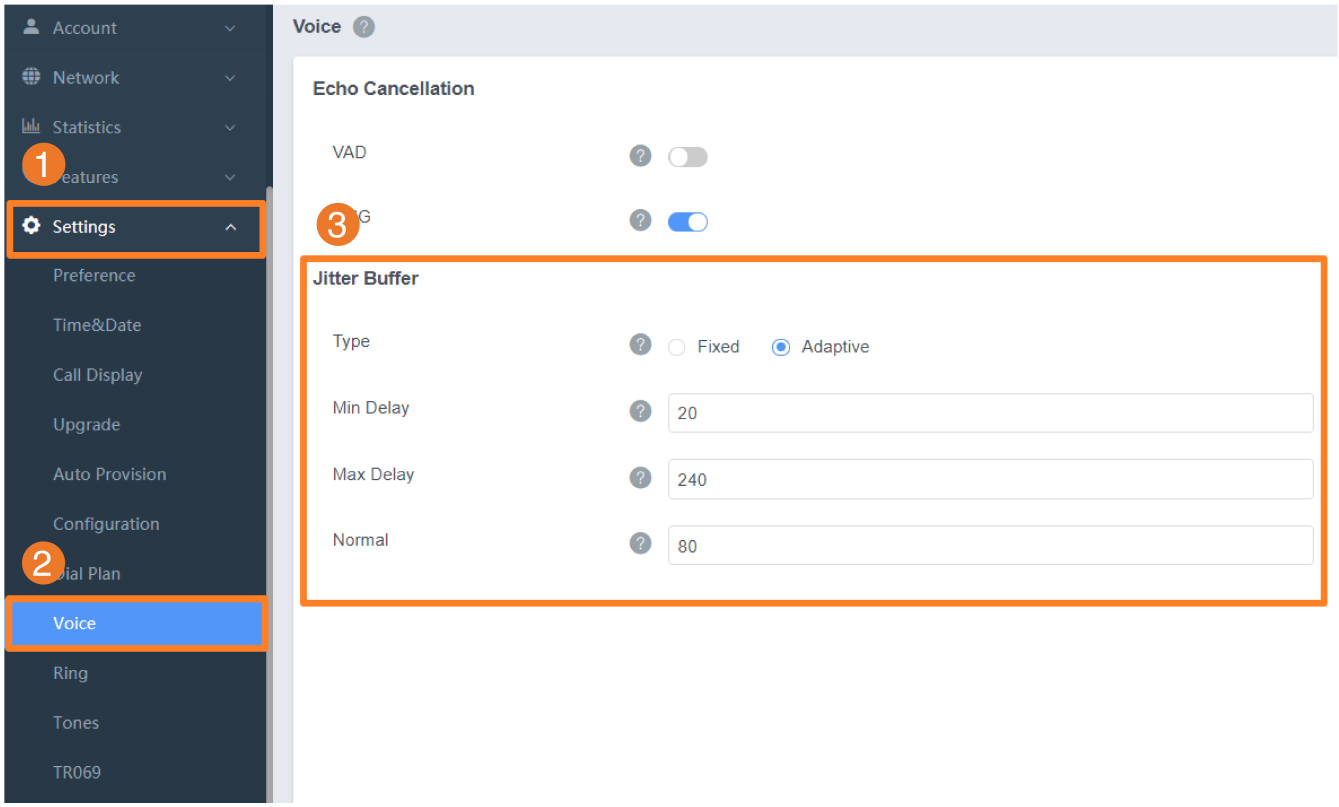
Jitter Buffer

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

1. 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:

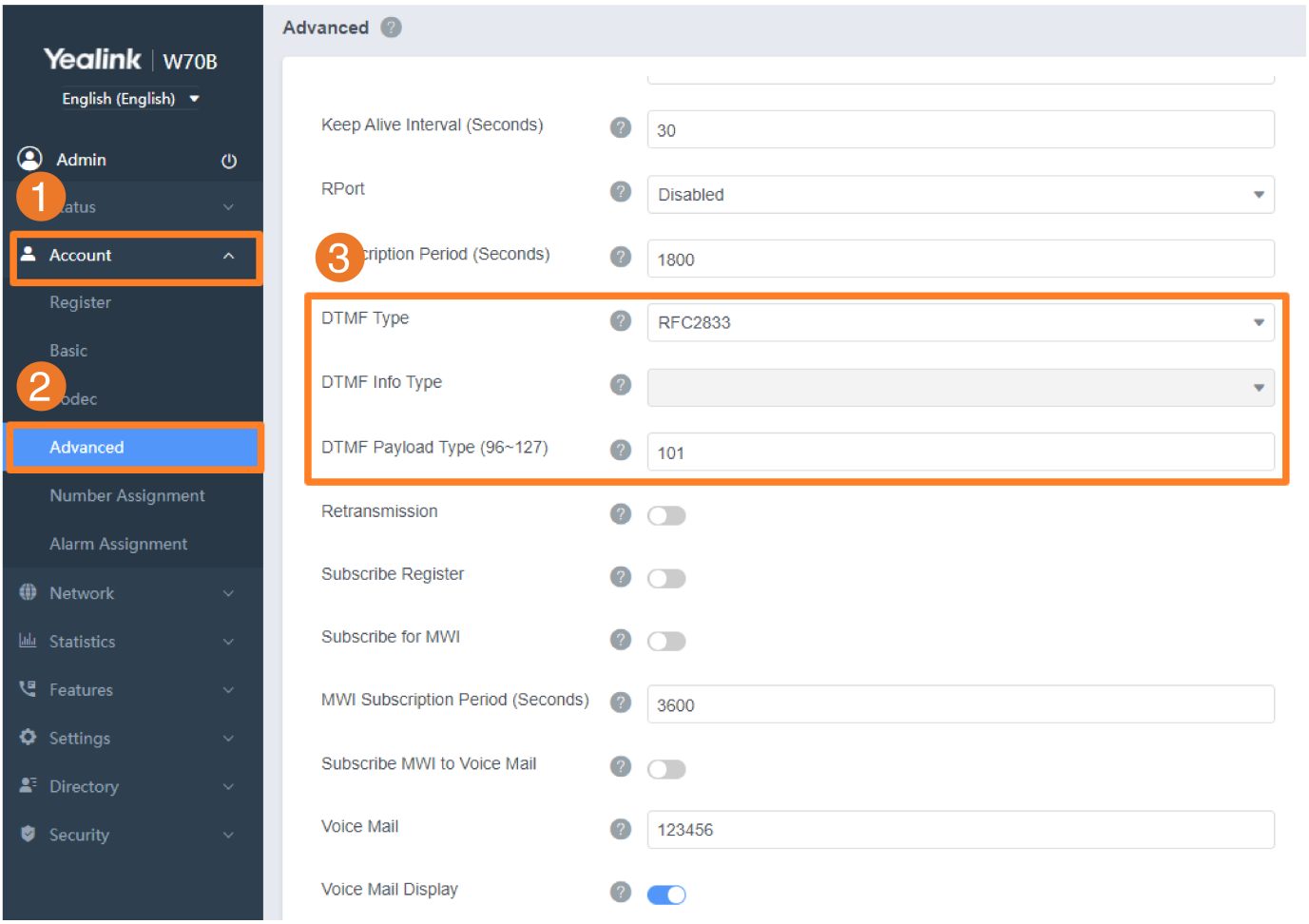
- **RFC 2833** – DTMF digits are transmitted by RTP Events compliant with RFC 2833. You can configure the payload type and sending times of the end RTP Event packet. The RTP Event packet contains 4 bytes. The 4 bytes are distributed over several fields denoted as Event, End bit, R-bit, Volume, and Duration.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

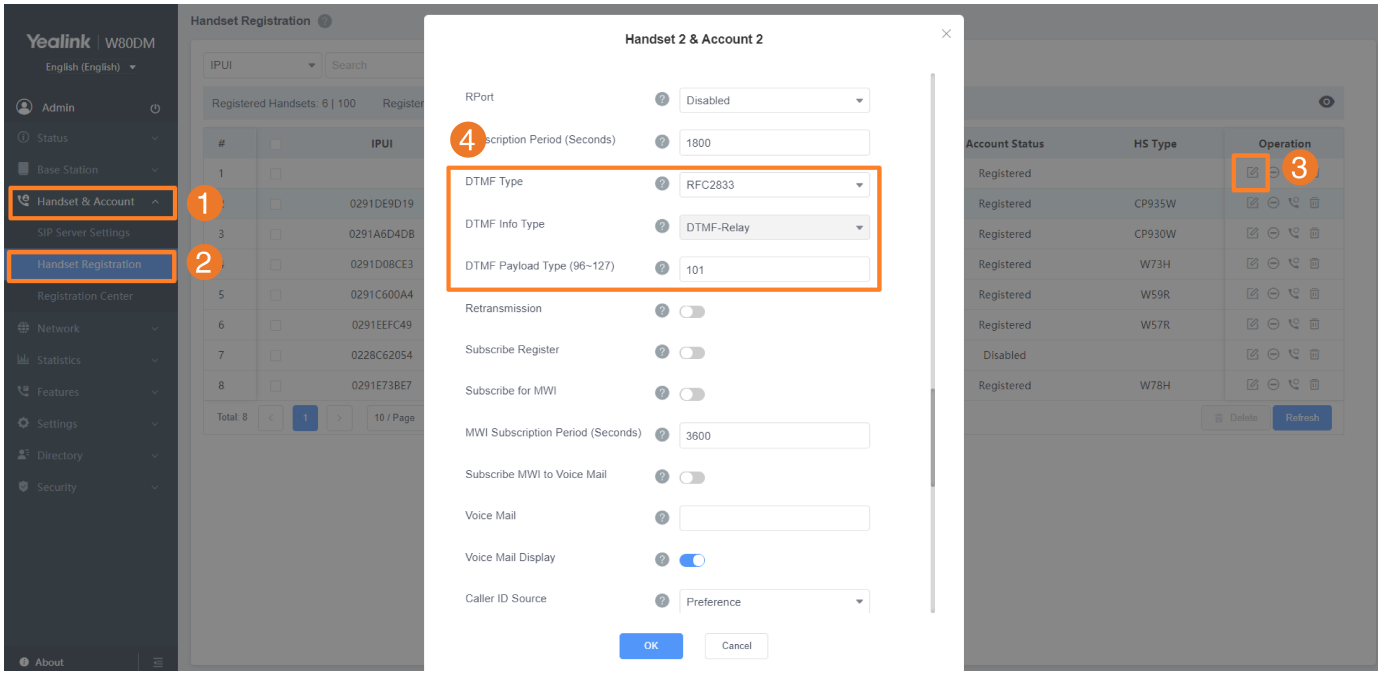
Transmit DTMF Digit Configuration

Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Advanced** > **DTMF Type/DTMF Payload Type(96~127)/DTMF Info Type**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **DTMF Type/DTMF Payload Type(96~127)/DTMF Info Type**.



Configuration Parameter

account.X.dtmf.type
account.X.dtmf.dtmf_payload
account.X.dtmf.info_type
features.dtmf.repetition
features.dtmf.duration
features.dtmf.volume

Parameter	Permitted Values	Default	Description
account.X.dtmf.type[1]	**0**-INBAND, DTMF digits are transmitted in the voice band. **1**-RFC2833, DTMF digits are transmitted by RTP Events compliant to RFC 2833. **2**-SIP INFO, DTMF digits are transmitted by the SIP INFO messages. **3**-RFC2833 + SIP INFO, DTMF digits are transmitted by RTP Events compliant to RFC 2833 and the SIP	1	It configures the DTMF type.

	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.
> - For W70B, X=1-10.
> - For W75DM, X=1-20.
> - For W80 multi-cell system, X=1-100.
> - For W90 multi-cell system, X=1-250.
> - For VIM system, X=1-2500.
>
> [2]If you change this parameter, the phone will reboot to make the change take effect.

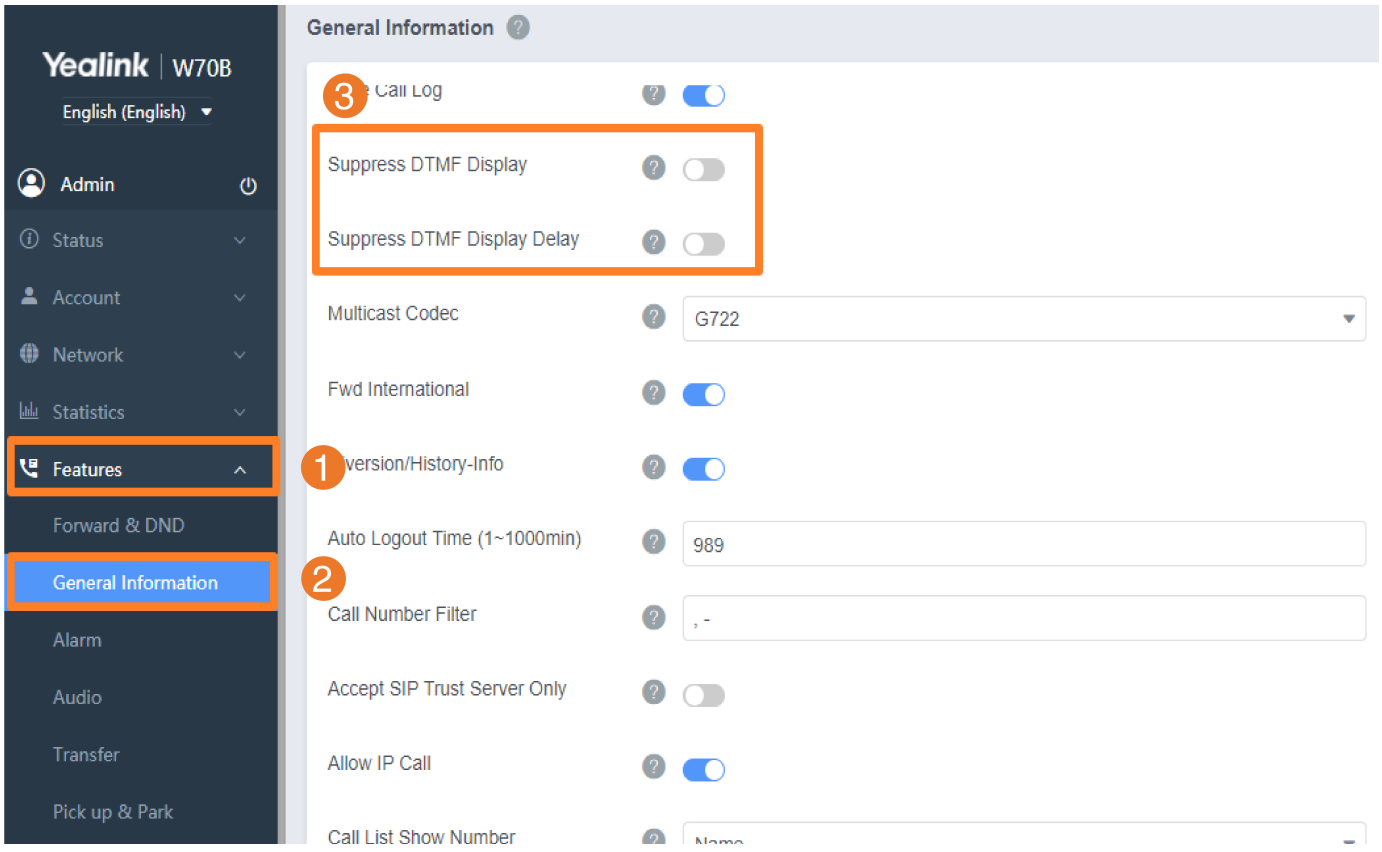
Suppress DTMF Display

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

1. On the web user interface, go to **Features** > **General Information** > **Suppress DTMF Display/ Suppress DTMF Display Delay**.



Configuration Parameter

features.dtmf.hide
features.dtmf.hide_delay

Parameter	Permitted Values	Default	Description
features.dtmf.hide	**0**-Disabled **1**-Enabled, the DTMF digits are displayed as asterisks.	0	It enables or disables the phone to suppress the display of DTMF digits during an active call.
features.dtmf.hide_delay	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to display the DTMF digits for a short period before displaying asterisks during an active call. It works only if "features.dtmf.hide" is set to 1 (Enabled).

Silent Charging

Introduction

You can enter the silent mode when the handset is charging. When you exit charging, the handset restores the previous volume.

Before You Begin

It is only applicable to W71H, W73H, W74H, W78H, W53H, W56H, W57R, W59R, W59R Pro, and CP930W-Base.

Silent Charging Configuration

Set via the Device Interface

See Silent Charging.

Configuration Parameter

```
custom.handset.silent_charging
```

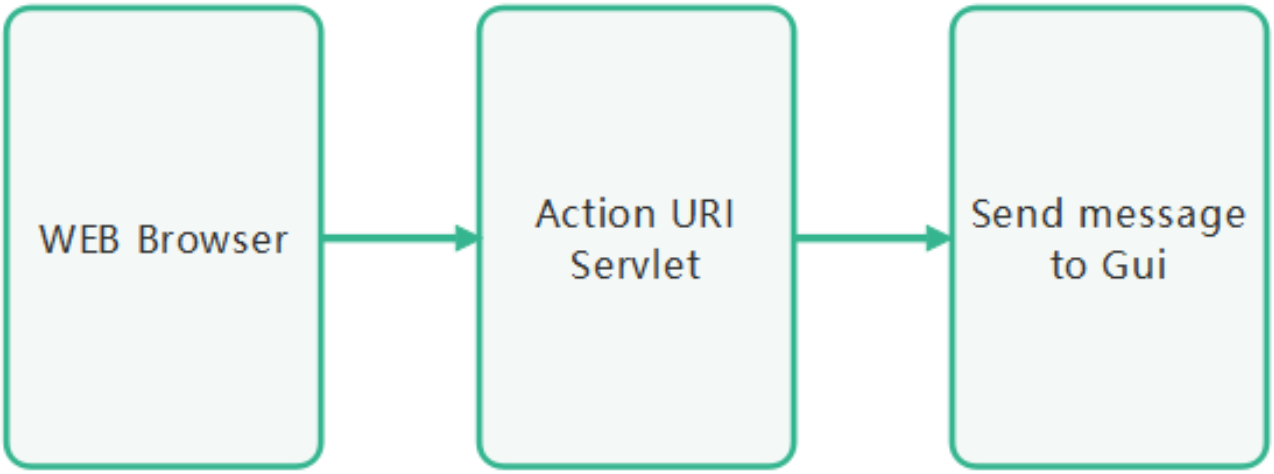
Parameter	Permitted Values	Default	Description
custom.handset.silent_charging	**0**-Disabled **1**-Enabled, the handset in silent mode when charging, even if "force.voice.ring_vol" > 0.	0	It enables or disables the silent mode when the handset is charging.

Action URI

Introduction

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.

Action URI on W70B only supports Reboot, Reset, and AutoP features.



Basic working principle

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 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.

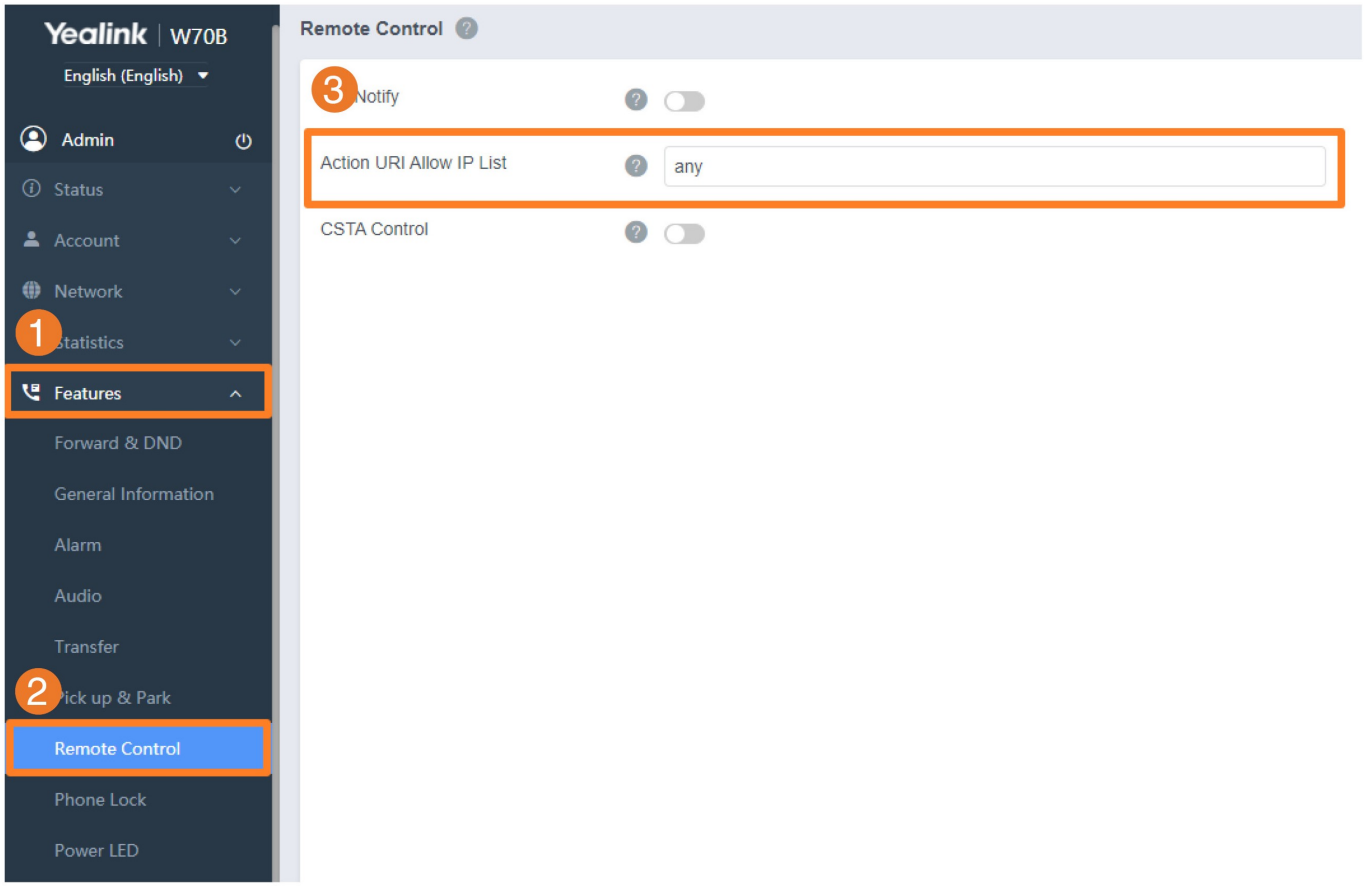
Example of a SIP Notify with the variable value (OK):

```
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
Event: ACTION-URI
Content-Type: message/sipfrag
Content-Length: 6
Message Body

key=OK
```

Action URI Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **Remote Control** > **Action URI Allow IP List**.



Configuration Parameter

features.action_uri.enable
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 from receiving the action URI requests.
features.action_uri_	IP address **Blank**-the phone will reject any HTTP GET request.	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,

limit_ip	**any**-the phone will accept and handle HTTP GET requests from any IP address.		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).

Action URL

Introduction

Action URL allows the phone 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?.

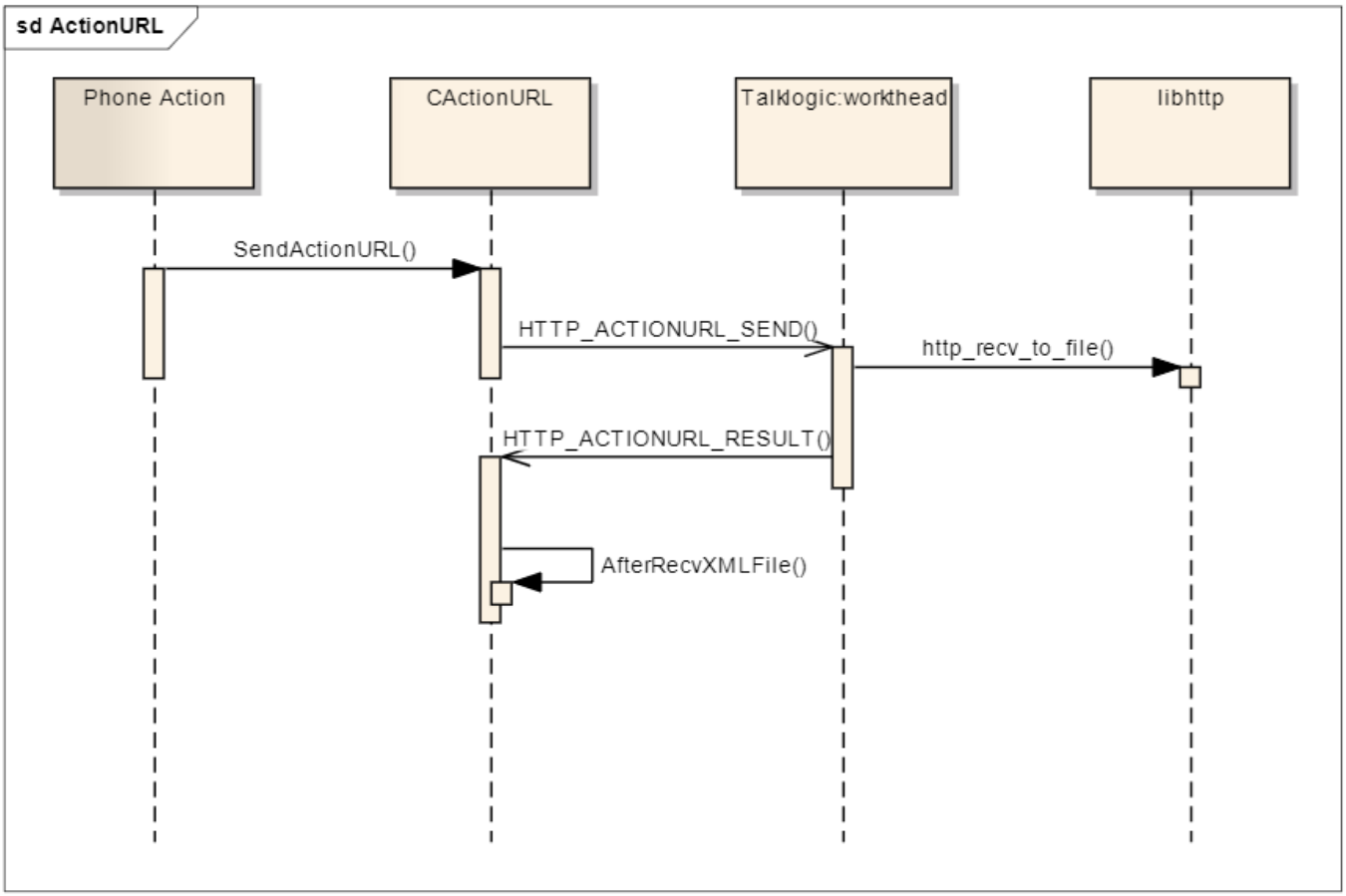
An HTTP or HTTPS GET request may contain a variable name and a variable value, separated by "=". Each variable value starts with $ in the query part of the URL.

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 phone when the phone mutes a call.



Before You Begin

This feature is only applicable to W70B.

Predefined Events List

The following table lists the predefined events for the action URL.

Event	Description
Setup Completed	When the phone completes startup.
Registered	When the phone successfully registers an account.
Unregistered	When the phone logs out of the registered account.
Register Failed	When the phone fails to register an account.
Off Hook	When the phone is off-hook.
On Hook	When the phone is on hook.
Incoming Call	When the phone receives an incoming call.
Outgoing Call	When the phone places a call.
Established	When the phone establishes a call.
Terminated	When the phone terminates a call.
Open DND	When the phone enables the DND mode. When the DND mode is Phone, the phone sends the action URL for all accounts; when the DND mode is Custom, the phone only sends the action URL for the corresponding account.
Close DND	When the phone disables the DND mode. When the DND mode is Phone, the phone sends the action URL for all accounts; when the DND mode is Custom, the phone only sends the action URL for the corresponding account.
Always Forward On	When the phone enables the always forward. When the forward mode is Phone, the phone sends the action URL for all accounts; when the forward mode is Custom, the phone only sends the action URL for the corresponding account.
Always Forward Off	When the phone disables the always forward. When the forward mode is Phone, the phone sends the action

	URL for all accounts; when the forward mode is Custom, the phone only sends the action URL for the corresponding account.
Busy Forward On	When the phone enables the busy forward. When the forward mode is Phone, the phone sends the action URL for all accounts; when the forward mode is Custom, the phone only sends the action URL for the corresponding account.
Busy Forward Off	When the phone disables the busy forward. When the forward mode is Phone, the phone sends the action URL for all accounts; when the forward mode is Custom, the phone only sends the action URL for the corresponding account.
No Answer Forward On	When the phone enables the no answer forward. When the forward mode is Phone, the phone sends the action URL for all accounts; when the forward mode is Custom, the phone only sends the action URL for the corresponding account.
No Answer Forward Off	When the phone disables the no answer forward. When the forward mode is Phone, the phone sends the action URL for all accounts; when the forward mode is Custom, the phone only sends the action URL for the corresponding account.
Transfer Call	When the phone transfers a call.
Blind Transfer	When the phone performs a blind transfer.
Attended Transfer	When the phone performs a semi-attended/attended transfer.
Hold	When the phone places a call on hold.
UnHold	When the phone resumes a held call.
Held	When a call of the phone is held by the other end of the call.
UnHeld	When a held call is resumed by the other end of the call.

Mute	When the phone mutes a call.
UnMute	When the phone unmutes a call.
Missed Call	When the phone misses a call.
IP Changed	When the IP address of the phone changes.
Idle To Busy	When the state of the phone changes from idle to busy.
Busy To Idle	When the state of the phone changes from busy to idle.
Reject Incoming Call	When the phone rejects an incoming call.
Answer New Incoming Call	When the phone answers a new call.
Transfer Failed	When the phone fails to transfer a call.
Transfer Finished	When the phone completes transferring a call.
Forward Incoming Call	When the phone forwards an incoming call.
Autop Finish	When the phone completes auto provisioning by powering on.
Call Waiting On	When the phone enables call waiting.
Call Waiting Off	When the phone disables call waiting.
Headset	When the phone presses the HEADSET key.
Handfree	When the phone presses the Speakerphone key.
Cancel Call Out	When the phone cancels an outgoing call in the ring-back state.
Remote Busy	When an outgoing call is rejected.
Call Remote Canceled	When the remote party cancels the outgoing call in the ringing state.
Peripheral Information	When the accessory is unplugged or plugged.
VPN IP	When the phone IP address is assigned by the VPN server changes.

Variable Values List

The following table lists predefined variable values.

Variable Value	Description
$mac	The MAC address of the phone.
$ip	The IP address of the phone.
$model	The phone model.
$firmwa	The firmware version of the phone.

re	
$active_url	The SIP URI of the current account when the phone places a call, receives an incoming call, or establishes a call.
$active_user	The user part of the SIP URI for the current account when the phone places a call, receives an incoming call, or establishes a call.
$active_host	The host part of the SIP URI for the current account when the phone places a call, receives an incoming call, or establishes a call.
$local	The SIP URI of the caller when the phone places a call. The SIP URI of the callee when the phone receives an incoming call.
$remote	The SIP URI of the callee when the phone places a call. The SIP URI of the caller when the phone receives an incoming call.
$display_local	The display name of the caller when the phone places a call. The display name of the callee when the phone receives an incoming call.
$display_remote	The display name of the callee when the phone places a call. The display name of the caller when the phone receives an incoming call.
$call_id	The call ID of the active call.
$callerID	The display name of the caller when the phone receives an incoming call.
$calledNumber	The phone number of the callee when the phone places a call.
$handset_number	The handset number of the base.

Action URL Configuration

Configuration Parameter

```
action_url.setup_completed
action_url.registered
action_url.unregistered
action_url.register_failed
action_url.off_hook
```

```
action_url.on_hook
action_url.incoming_call
action_url.outgoing_call
action_url.call_established
action_url.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
```

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 that 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 that the phone sends when on hook. **Example**: action_url.on_hook = http://192.168.0.20/help.xml?IP=$ip
action_url.incoming_call	URL within 511 characters	Blank	It configures the action URL that the phone sends when receiving an incoming call. **Example**: action_url.incoming_call = http://192.168.0.20/help.xml?IP=$ip
action_url.outgoing_call	URL within 511 characters	Blank	It configures the action URL that the phone sends when placing a call. **Example**: action_url.outgoing_call = http://192.168.0.20/help.xml?IP=$ip
action_url.call_established	URL within 511 characters	Blank	It configures the action URL that the phone sends when establishing a call. **Example**: action_url.call_established = http://192.168.0.20/help.xml?IP=$ip
action_url.call_terminated	URL within 511 characters	Blank	It configures the action URL that the phone sends when terminating a call. **Example**: action_url.call_terminated = http://192.168.0.20/help.xml?IP=$ip
action_url.dnd_on	URL within 511 characters	Blank	It configures the action URL that the phone sends when DND feature is activated. **Example**: action_url.dnd_on = http://192.168.0.20/help.xml?IP=$ip
action_url.dnd_off	URL within 511 characters	Blank	It configures the action URL that the phone sends when 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	Blan	It configures the action URL that the phone sends when the always forward feature is activated.

	characters	k	**Example**: action_url.always_fwd_on = http://192.168.0.20/help.xml?IP=$ip
action_url.always_fwd_off	URL within 511 characters	Blank	It configures the action URL that the phone sends when the always forward feature is deactivated. **Example**: action_url.always_fwd_off = http://192.168.0.20/help.xml?IP=$ip
action_url.busy_fwd_on	URL within 511 characters	Blank	It configures the action URL that the phone sends when the busy forward feature is activated. **Example**: action_url.busy_fwd_on = http://192.168.0.20/help.xml?IP=$ip
action_url.busy_fwd_off	URL within 511 characters	Blank	It configures the action URL that the phone sends when the busy forward feature is deactivated. **Example**: action_url.busy_fwd_off = http://192.168.0.20/help.xml?IP=$ip
action_url.no_answer_fwd_on	URL within 511 characters	Blank	It configures the action URL that 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=$ip
action_url.no_answer_fwd_off	URL within 511 characters	Blank	It configures the action URL that the phone sends when the no-answer-forward feature is deactivated. **Example**: action_url.no_answer_fwd_off = http://192.168.0.20/help.xml?IP=$ip
action_url.transfer_call	URL within 511 characters	Blank	It configures the action URL that the phone sends when performing a transfer. **Example**: action_url.transfer_call = http://192.168.0.20/help.xml?IP=$ip
action_url.blin	URL	Bl	It configures the action URL that the phone sends when

d_transfer_call	within 511 characters	an k	performing a blind transfer. **Example**: action_url.blind_transfer_call = http://192.168.0.20/help.xml?IP=$ip
action_url.attended_transfer_call	URL within 511 characters	Blank	It configures the action URL that the phone sends when performing an attended/semi-attended transfer. **Example**: action_url.attended_transfer_call = http://192.168.0.20/help.xml?IP=$ip
action_url.hold	URL within 511 characters	Blank	It configures the action URL that the phone sends when placing a call on hold. **Example**: action_url.hold = http://192.168.0.20/help.xml?IP=$ip
action_url.unhold	URL within 511 characters	Blank	It configures the action URL that the phone sends when resuming a hold call. **Example**: action_url.unhold = http://192.168.0.20/help.xml?IP=$ip
action_url.held	URL within 511 characters	Blank	It configures the action URL that the phone sends when a call is held by the other end of the call. **Example**: action_url.held = http://192.168.0.20/help.xml?IP=$ip
action_url.unheld	URL within 511 characters	Blank	It configures the action URL that the phone sends when a held call is resumed by the other end of the call. **Example**: action_url.unheld = http://192.168.0.20/help.xml?IP=$ip
action_url.mute	URL within 511 characters	Blank	It configures the action URL that the phone sends when muting a call. **Example**: action_url.mute = http://192.168.0.20/help.xml?IP=$ip
action_url.unmute	URL within 511 characters	Blank	It configures the action URL that the phone sends when unmuting a call. **Example**: action_url.unmute = http://192.168.0.20/help.xml?IP=$ip

action_url.missed_call	URL within 511 characters	Blank	It configures the action URL that the phone sends when missed a call. **Example**: action_url.missed_call = http://192.168.0.20/help.xml?IP=$ip
action_url.busy_to_idle	URL within 511 characters	Blank	It configures the action URL that the phone sends when the state of the phone changes from busy to idle. **Example**: action_url.busy_to_idle = http://192.168.0.20/help.xml?IP=$ip
action_url.idle_to_busy	URL within 511 characters	Blank	It configures the action URL that the phone sends when the state of the phone changes from idle to busy. **Example**: action_url.idle_to_busy = http://192.168.0.20/help.xml?IP=$ip
action_url.ip_change	URL within 511 characters	Blank	It configures the action URL that the phone sends when changes the IP address of the phone. **Example**: action_url.ip_change = http://192.168.0.20/help.xml?IP=$ip
action_url.reject_incoming_call	URL within 511 characters	Blank	It configures the action URL that the phone sends when rejects an incoming call. **Example**: action_url.reject_incoming_call = http://192.168.0.20/help.xml?IP=$ip
action_url.answer_new_incoming_call	URL within 511 characters	Blank	It configures the action URL that the phone sends when answered a new incoming call. **Example**: action_url.answer_new_incoming_call = http://192.168.0.20/help.xml?IP=$ip
action_url.forward_incoming_call	URL within 511 characters	Blank	It configures the action URL that the phone sends when forwarding an incoming call. **Example**: action_url.forward_incoming_call = http://192.168.0.20/

			help.xml?IP=$ip
action_url.transfer_finished	URL within 511 characters	Blank	It configures the action URL that the phone sends when completed a call transfer. **Example**: action_url.transfer_finished = http://192.168.0.20/help.xml?IP=$ip
action_url.transfer_failed	URL within 511 characters	Blank	It configures the action URL that the phone sends when failed to transfer a call. **Example**: action_url.transfer_failed = http://192.168.0.20/help.xml?IP=$ip
action_url.setup_autop_finish	URL within 511 characters	Blank	It configures the action URL that the phone sends when completed auto provisioning via power on. **Example**: action_url.setup_autop_finish = http://192.168.0.20/help.xml?IP=$ip
action_url.call_waiting_on	URL within 511 characters	Blank	It configures the action URL that the phone sends when the call waiting feature is enabled. **Example**: action_url.call_waiting_on = http://192.168.0.20/help.xml?IP=$ip
action_url.call_waiting_off	URL within 511 characters	Blank	It configures the action URL that the phone sends when the call waiting feature is disabled. **Example**: action_url.call_waiting_off = http://192.168.0.20/help.xml?IP=$ip
action_url.headset	URL within 511 characters	Blank	It configures the action URL that the phone sends when pressed the HEADSET key. **Example**: action_url.headset = http://192.168.0.20/help.xml?IP=$ip
action_url.handfree	URL within 511 characters	Blank	It configures the action URL that the phone sends when pressed the Speakerphone key. **Example**: action_url.handfree = http://192.168.0.20/help.xml?IP=$ip

action_url.cancel_callout	URL within 511 characters	Blank	It configures the action URL that 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=$ip
action_url.remote_busy	URL within 511 characters	Blank	It configures the action URL that the phone sends when the outgoing call is rejected. **Example**: action_url.remote_busy = http://192.168.0.20/help.xml?IP=$ip
action_url.call_remote_canceled	URL within 511 characters	Blank	It configures the action URL that 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=$ip
action_url.peripheral_information	URL within 511 characters	Blank	It configures the action URL that the phone sends when you unplug or plug an accessory. **Example**: action_url.peripheral_information = http://192.168.0.20/help.xml?IP=$ip&WIFI=$wifi_number
action_url.vpn_ip	URL within 511 characters	Blank	It configures the action URL that the phone sends when the IP address assigned by the VPN server changes. **Example**: action_url.vpn_ip= http://192.168.0.20/help.xml?IP=$ip

Intercom

Introduction

Intercom is a useful feature in an office environment to quickly connect with the operator or the secretary. You can make internal intercom calls and external intercom calls on the phone. Internal intercom calls are made between handsets registered to the same base station. External intercom calls can be made by dialing the feature access code followed by the number. External intercom calls depend on support from a SIP server.

The handset can automatically answer an incoming external intercom call and play a warning tone only when there is only one handset subscribed and no call in progress on the handset.

The **CP930W-Base** phones can not automatically answer either the external or internal intercom call; you can only answer it manually.

To automatically answer an incoming internal intercom call, you need to enable the auto intercom feature on the handset. The following configuration types of auto intercom features are available:

Type	Description
On (Beep On)	Auto intercom feature is on. The handset will answer an incoming internal intercom call automatically and play a warning tone.
On (Beep Off)	Auto intercom feature is on. The handset will answer an incoming internal intercom call automatically without a warning tone.
Off	Auto intercom feature is off. You need to answer an incoming internal intercom call manually.

Intercom Configuration

Set via the Device Interface

See Place Internal Calls.

Configuration Parameter

```
features.intercom.headset_prior.enable
custom.handset.auto_intercom
```

account.X.auto_external_intercom
account.X.external_intercom.mute
account.X.external_intercom.barge.enable
account.X.external_intercom.barge_in_dialing.enable
custom.handset.x.auto_intercom

Parameter	Permitted Values	Default	Description
features.intercom.headset_prior.enable	**0**-Speaker Mode **1**-Headset Mode	1	It configures the channel mode when an incoming intercom call is answered through the handset. The headset should be connected in advance. All phones except CP930W-Base/CP935W-Base are applicable to this parameter.
custom.handset.auto_intercom	**0**-Off, users need to answer incoming internal intercom calls manually. **1**-On(Beep Off), the handset will answer an incoming internal intercom call automatically without a warning tone. **2**-On(Beep On), the handset will answer an incoming internal intercom call automatically and play a warning tone. It works when the silent mode is off (silent mode is not applicable to CP930WBase/ CP935W-Base phones).	0	It configures whether the DECT IP phone automatically answers an incoming internal intercom call and plays a warning tone. 1. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled). 2. This parameter is applicable to W53H/ W56H/W57R/W59R/ W73H.
account.X.auto_ext	**0**-Off, users need to answer incoming external intercom calls manually.	0	It configures whether the DECT IP phone automatically answers

ernal_intercom[1]	**1**-On(Beep Off), the handset will answer an incoming external intercom call automatically without a warning tone. **2**-On(Beep On), the handset will answer an incoming external intercom call automatically and play a warning tone. It works when the silent mode is off (silent mode is not applicable to CP930WBase/ CP935W-Base phones).		an incoming external intercom call and plays a warning tone. It works only if there is no active call on the handset.
account.X.external_intercom.mute[1]	**0**-Disabled **1**-Enabled	0	It configures whether the DECT IP phone is mute after automatically answering an incoming external intercom call. It works only if "account.X.auto_external_intercom" is set to 1 or 2 and "features.allow_mute" is set to 1.
account.X.external_intercom.barge.enable[1]	**0**-Disabled, **1**-Enabled, the handset will automatically answer incoming external Intercom and hold on the active call.	0	It enables or disables the Dect IP phone automatically answers an incoming external intercom call while there is already an active call on the phone. It works only if "account.X.auto_external_intercom" is set to 1 or 2 and "call_waiting.enable" is set to 1.
account.X.external_intercom	**0**-Disabled, **1**-Enabled, the handset will automatically answer incoming external Intercom and	0	It configures whether to automatically answer external Intercom when dialing.

.barge_in_dialing.enable[1]	cancel dialing.		It works only if "account.X.external_intercom.barge.enable" is set to 0.
custom.handset.x.auto_intercom	**0**-Disabled, **1**-Enabled and without beep hint. **2**-Enabled and with beep hint.	0	It configures whether the handsets will accept the intercom calling automatically.

Dial Plan

Introduction

Dial plan is a string of characters that governs the way how the phones process the inputs received from the IP phone's keypads. You can use the regular expression to define the dial plan.

Yealink phones support four patterns:

Pattern	Description
Replace rule	An alternative string that replaces the numbers entered by the user. Yealink phones support up to 100 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 now rules.
Area code	Also known as Numbering Plan Areas (NPAs). They usually indicate geographical areas in one country. When entered numbers match the predefined area code rule, the phone will automatically add the area code before the numbers when dialing out them. Yealink phones only support 1 area code rule.
Block out	Prevents users from dialing out specific numbers. When entered numbers match the predefined block-out rule, the phone screen prompts "Forbidden Number". Yealink phones support up to 10 block-out rules.

You can configure these four patterns via the web user interface or auto provisioning. For replace rule and dial now, you can select to add the rule one by one or use the template file to add multiple rules at a time.

Basic Regular Expression Syntax for Four Patterns

You need to know the following basic regular expression syntax when creating a dial plan:

Regular Expression	Description
.	The dot "." can be used as a placeholder or multiple placeholders for any string. **Example**: "12." would match "123", "1234", "12345", "12abc", and so on.
x	The "x" can be used as a placeholder for any character. **Example**: "12x" would match "121", "122", "123", "12a", and so on.
-	The dash "-" can be used to match a range of characters within the brackets. **Example**: "[5-7]" would match the number "5", "6" or "7".
,	The comma "," can be used as a separator within the bracket. **Example**: "[2,5,8]" would match the number "2", "5" or "8".
[]	The square bracket "[]" can be used as a placeholder for a single character that matches any of a set of characters. **Example**: "91[5-7]1234"would match "9151234", "9161234", "9171234".
()	The 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$145$2". 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 replace rule file template.

Replace Rule File Attributes

The following table lists the attributes you can use to add replace rules to the replace rule file:

Attributes	Description
Prefix	Specify the number to be replaced.
Replace	Specify the alternate string instead of what the user enters.
LineID	Specify a registered line to apply the replace rule. Valid Values: **0-10** **0** stands for all lines; **1-10** stand for line1-line10 Multiple line IDs are separated by commas.

Customize the Replace Rule File

1. Open the replace rule file.
2. To add a replace rule, add <Data Prefix="" Replace="" LineID=""/> to the file. Each starts on a new line.
3. Specify the values within double quotes.
   For example,
   <Data Prefix="2512" Replace="05922512" LineID="1"/>
4. Save the changes and place this file on the provisioning server.

Dial Now File Customization

The dial now file helps create multiple dial now rules. At most 20 dial now rules can be added to the IP phone.

You can ask the distributor or Yealink FAE for dial now file template.

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.

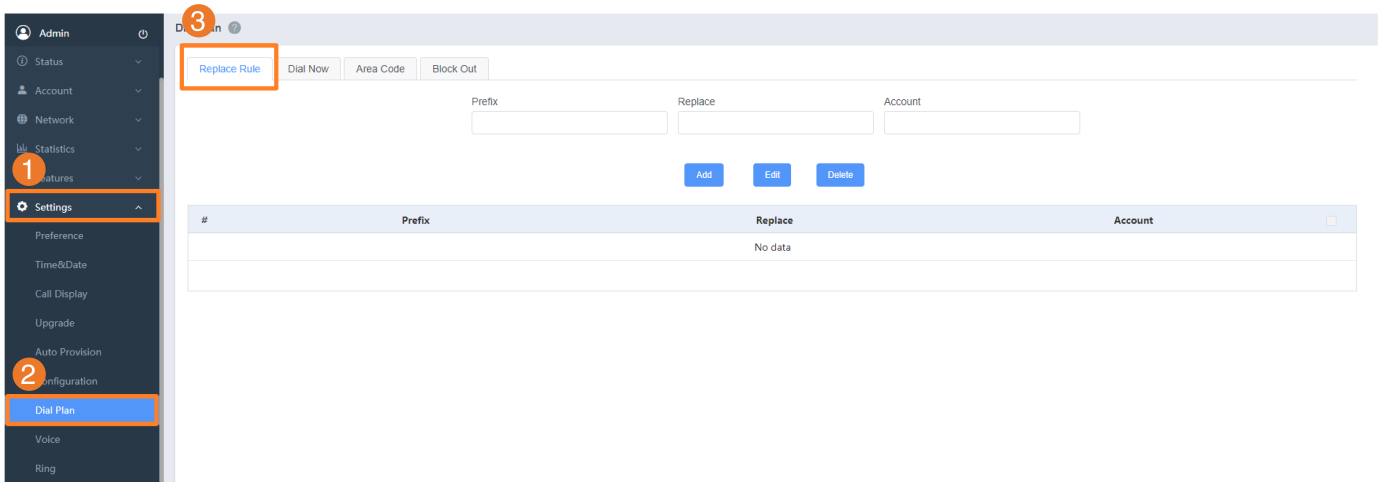
2. To add a dial-now rule, add <Data DialNowRule="" LineID="" /> to the file. Each starts on a new line.
3. Specify the values within double quotes.
   For example,
   <Data DialNowRule="1001" LineID="0" />
4. Save the changes and place this file on the provisioning server.

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.	String	Bl	It configures the alternate number to replace the entered number.

replace.replace.X[1]	within 32 characters	ank	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.

[1]

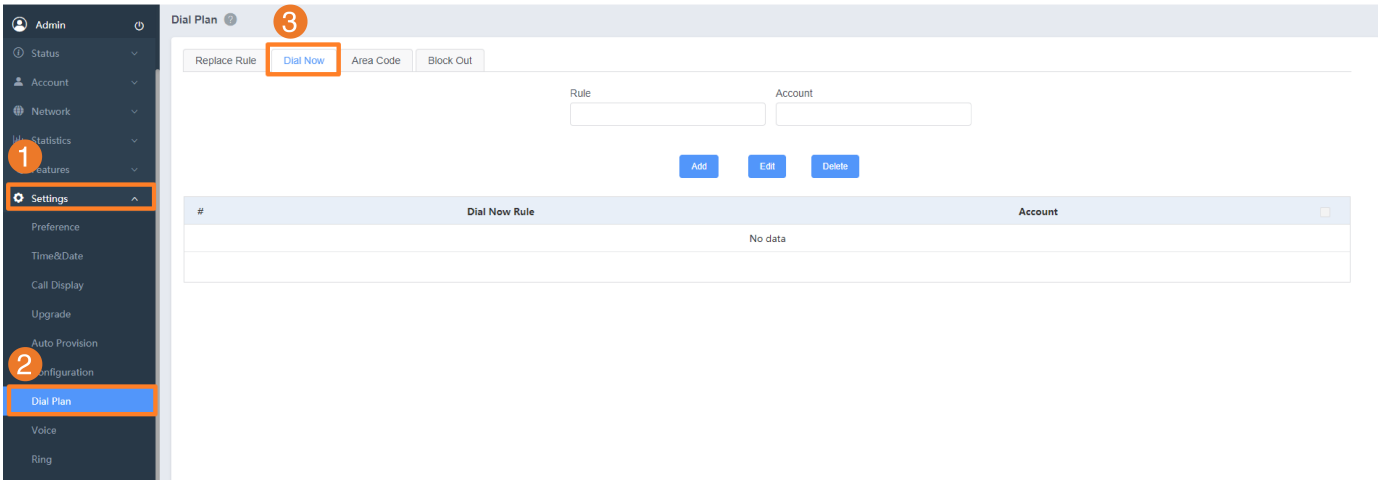
- For W70B, X is from 1 to 10.
- For W75DM, X is from 1 to 20.
- For W80 Multi-Cell System, X is from 1 to 100.
- For W90 Multi-Cell System, X is from 1 to 250.

Dial Now Configuration

You can configure dial now rules either one by one or in batches using a dial now template.

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Dial Plan** > **Dial Now**.



Configuration Parameter

```
dialplan.dialnow.rule.X
dialplan.dialnow.line_id.X
phone_setting.dialnow_delay
dialplan_dialnow.url
```

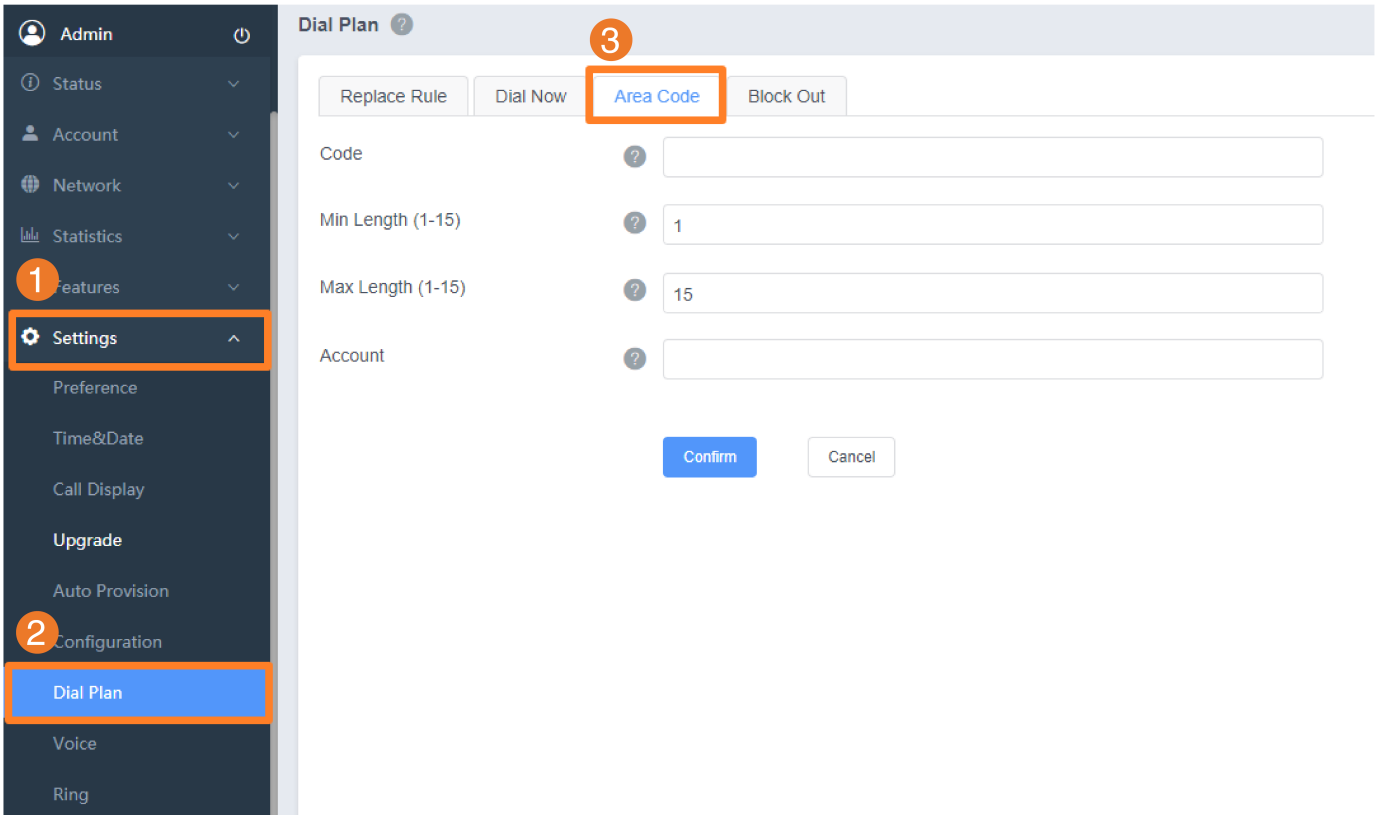
Parameter	Permitted Values	Default	Description
dialplan.dialnow.rule.X[1]	String within 511 characters	Blank	It configures the dial now rule (the string used to match the numbers entered by the user). When entered numbers match the predefined dial now rule, the phone will automatically dial out the numbers without pressing the send key. **Example**: dialplan.dialnow.rule.1 = 123
dialplan.dialnow.line_id.X[1]	0 to 10	Blank	It configures the desired line to apply the dial now rule. The digit 0 stands for all lines. If it is left blank, the dial-now rule will apply to all lines on the phone. Multiple line IDs are separated by commas.
phone_setting.dialnow_delay	Integer from 0 to 14	1	It configures the delay time (in seconds) for the dial now rule. When entered numbers match the predefined dial now rule, the phone will automatically dial out the entered number after the designated delay time. If it is set to 0, the phone will automatically dial out the entered number immediately.
dialplan_dialnow.url	String within 511 characters	Blank	It configures the access URL of the dial now template file.

[1] X is from 1 to 20.

Area Code Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Dial Plan** > **Area Code**.



Configuration Parameter

```
dialplan.area_code.code
dialplan.area_code.min_len
dialplan.area_code.max_len
dialplan.area_code.line_id
```

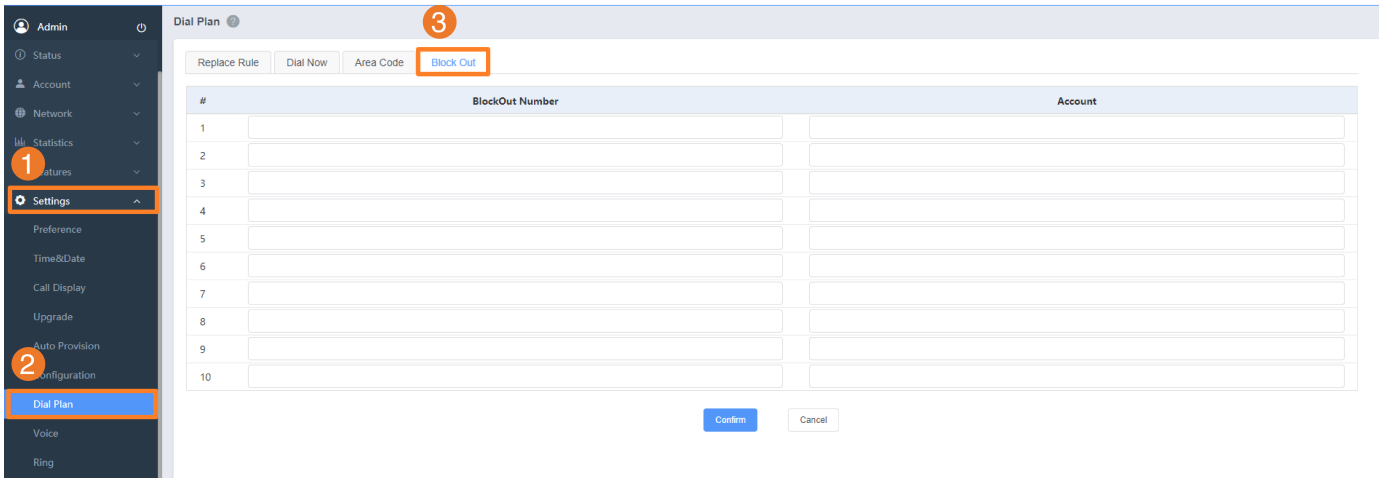
Parameter	Permitted Values	Default	Description
dialplan.area_code.code	String within 16 characters	Blank	It configures the area code to be added before the entered numbers when dialing out. The length of the entered number must be between the minimum length configured by the parameter dialplan.area_code.min_len and the maximum length configured by the parameter dialplan.area_code.max_len.
dialplan.area_code.mi	Integer from 1 to 15	1	It configures the minimum length of the entered number.

n_len			
dialplan.area_code.max_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.
dialplan.area_code.line_id	0 to 250	Blank	It configures the desired line to apply the area code rule. The digit 0 stands for all lines. If it is left blank, the area code rule will apply to all lines on the IP phone. 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]

- For W70B, X is from 1 to 10.
- For W75DM, X is from 1 to 20.
- For W80 Multi-Cell System, X is from 1 to 100.
- For W90 Multi-Cell System, X is from 1 to 250.

Example: Add Replace Rules Using a Replace Rule File

The following example shows the configuration for adding replacement 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 the 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

Para	Permitted Values	Defau	Description

meter		lt	
dialplan.emergency.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the Emergency dialplan feature.
dialplan.emergency.asserted_id_source	**ELIN**-The outbound identity used in the P-Asserted-Identity (PAI) header of the SIP INVITE request is taken from the network using an LLDP-MED Emergency Location Identifier Number (ELIN). The custom outbound identity configured by dialplan.emergency.custom_asserted_id will be used if the phone fails to get the LLDP-MED ELIN value. **CUSTOM**-The custom outbound identity configured by dialplan.emergency.custom_asserted_id will be used; if dialplan.emergency.custom_asserted_id is left blank, the LLDP-MED ELIN value will be used.	ELIN	It configures the precedence of the source of emergency outbound identities when placing an emergency call. If the obtained LLDP-MED ELIN value is blank and no custom outbound identity, the PAI header will not be included in the SIP INVITE request. It works only if "dialplan.emergency.enable" is set to 1 (Enabled).

dialplan.emergency.custom_asserted_id	**A number with 10 to 25 digits** - for example, 1234567890. The SIP URI constructed from the number and SIP server (for example, abc.com) is included in the P-Asserted-Identity (PAI) header (for example, <sip:1234567890@abc.com >). **SIP URI** - for example, sip:1234567890123@abc.com. The full URI is included in the P-Asserted-Identity (PAI) header and the address will be replaced by the emergency server (for example, <sip:1234567890123@emergency.com >). **TEL URI** - for example, tel:+16045558000. The full URI is included in the P-Asserted-Identity (PAI) header (for example, <tel:+16045558000 >).	Blank	It configures the custom outbound identity when placing an emergency call. It works only if "dialplan.emergency.enable" is set to 1 (Enabled).
dialplan.emergency.server.X.address[1]	IP address or domain name	Blank	It configures the IP address or domain name of the emergency server X to be used for routing calls. 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 that the phones use to communicate with the emergency server X. It works only if "dialplan.em

			ergency.enable" is set to 1 (Enabled).
dialplan.emergency.X.value[2]	Number or SIP URI	When X = 1, the default value is 911; When X = 2-255, the default value is Blank.	It configures the emergency number to use on your phones so a caller can contact emergency services in the local area when required. 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 a 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 a 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.	SIMPLE	It configures the type of location request message. It works only if "dialplan.emergency.enable" is set to 1 (Enabled) and

	If it is set to **REDSKY**, the phone will send the location request message defined by REDSKY.		"dialplan.emergency.asserted_id_source" is set to **HELD**.
dialplan.emergency.held.request_element.X.name[2]	String	Blank	It configures the custom element name to be sent in a location request message. **Example**: dialplan.emergency.held.request_element.1.name = mac dialplan.emergency.held.request_element.2.name = companyID dialplan.emergency.held.request_element.3.name = nai 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.held.username	String	Blank	It configures the user name 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.
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 the E911 Location Information Server again when failed to report the location to the server. **60 to 86400**-The phone reports the location to the E911 Location Information Server within the specified time interval.	0	It configures the time interval (seconds) for the phone to report location information to the E911 Location Information Server when the phone fails to report the location to the server. 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", "Supported: geolocation" do not exist. **1**-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.reque

	Routing: yes" exists in the E911 INVITE message, and the information "geolocation", "Supported: geolocation" also exist.		st_type" is set to YEALINK or REDSKY.
sip.emgr.header	**priority:emergency**-The E911 INVITE header field contains priority: emergency. **String**-The INVITE header field can be customized.	priority: emergency	It configures the content of 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. **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.	0	It configures the contents of held requests when the phone cannot connect to the LDAP switch.
dialplan.emergency.held.resync_period	**0**-The phone will not periodically send held requests to the server. **Integer from 1 to 10800**-The phone sends 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.

Off Hook Hot Line Dialing

Introduction

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 the call service. Only if you enter a valid activation code does 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 across 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 out 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.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

Speed Dial

Introduction

Speed dial allows you to speed up dialing contacts on the phone's idle screen using dedicated DSS keys.

Speed Dial Key Configuration

Set via the Device Interface

See the following topic:

1. Speed Dial on the Handset
2. Speed Dial on the DD Phone

Configuration Parameter

handset.x.features.key.y.speeddial

Parameter	Permitted Values	Default	Description
handset.x.features.key.y.speeddial	String within 24 characters	Blank	It configures Handset x Speed Dial Number or Speed Dial Internal Handset x. 1. "X" means Handset 1-10; "y" means Key 2-9. 2. When "Handset x" refers to the handset and DD Phone, "Key 2-9" means the digital key 2-9. 3. When "Handset x" refers to the headset, only digital key 2 is available, and you can configure a speed dial number for digital key 2.

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

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 anonymity.

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.

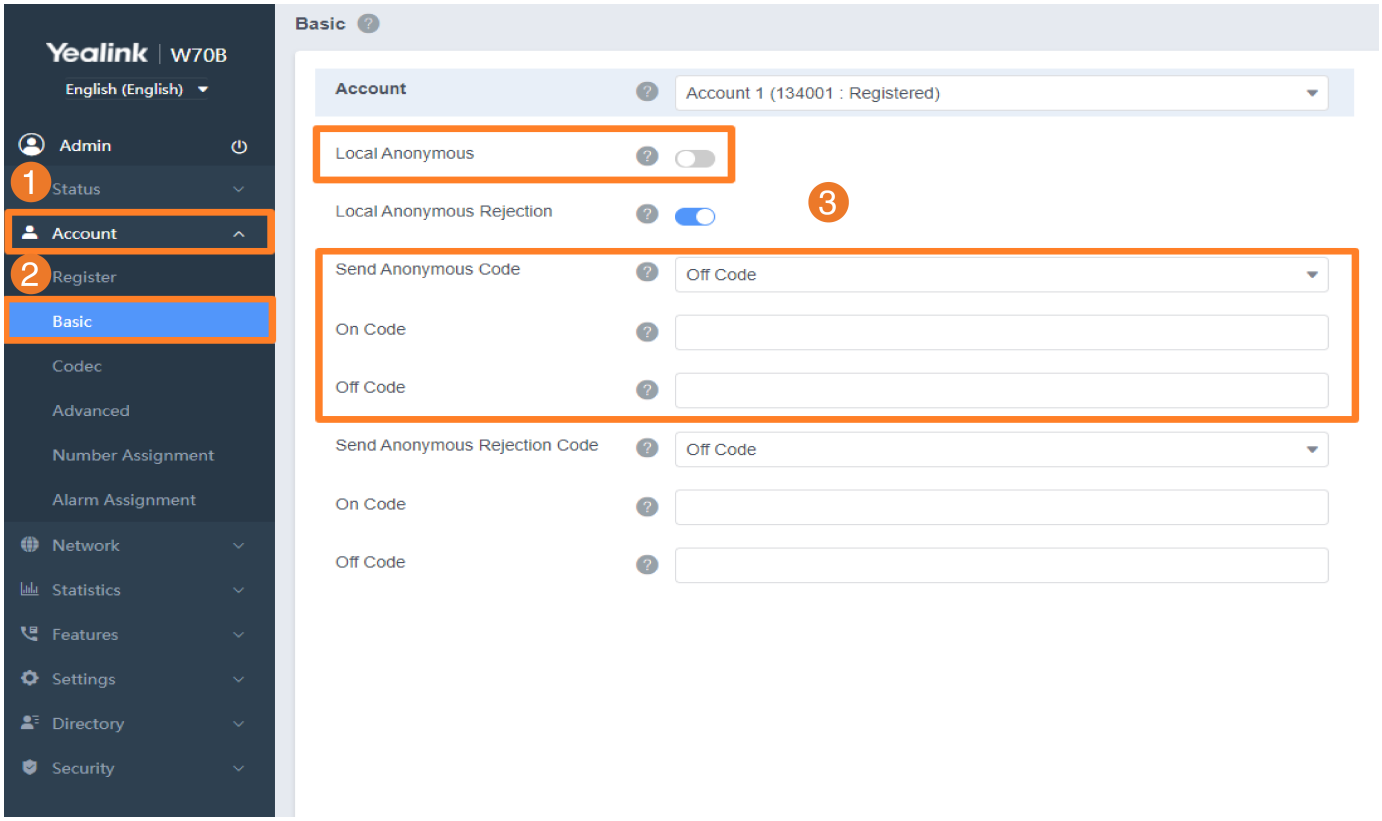
Anonymous Call Configuration

Set via the Device Interface

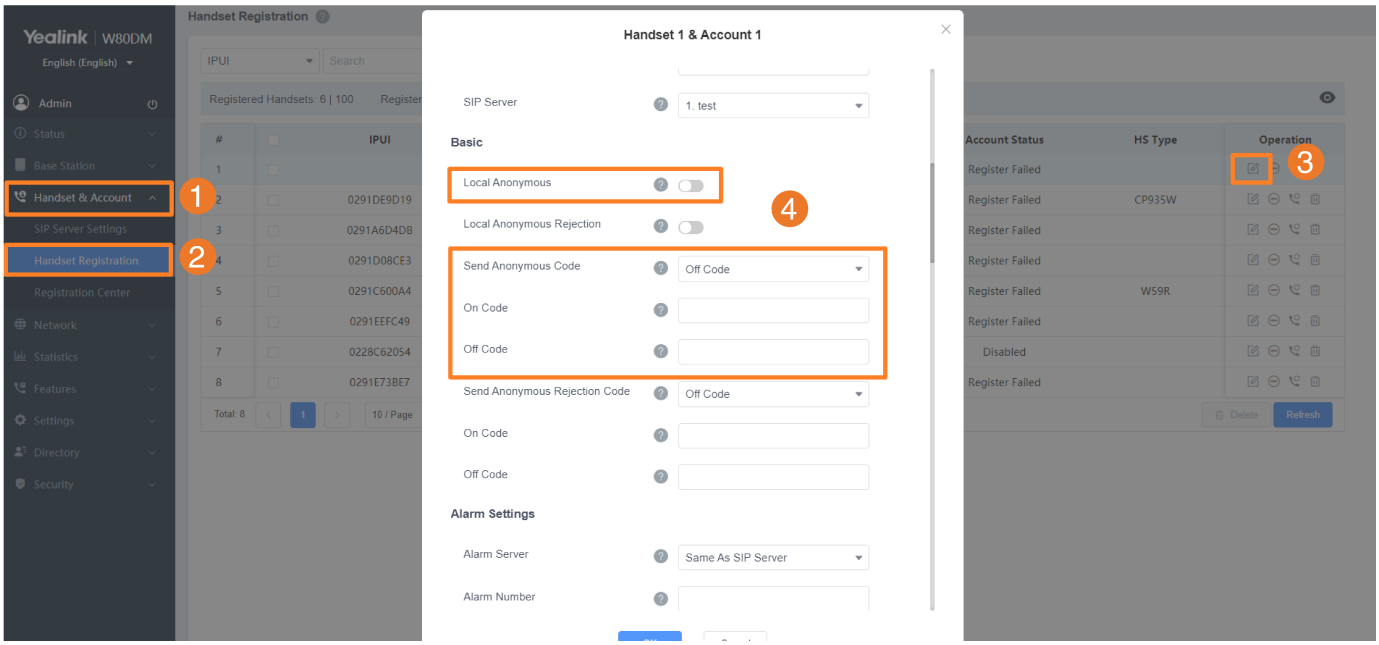
See Place an Anonymous Call.

Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Basic** > **Local Anonymous**/**Send Anonymous Code**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **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 anonymous off code to the server when you deactivate the anonymous call feature. **1**-On Code, the phone will send anonymous on code to the server when	0	It configures the phone to send anonymous on/off code to activate/deactivate the server-side anonymous call feature for a specific account.

	you activate the anonymous call feature.		
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 the server-side when you activate it on the phone.
account.X.anonymous_call_offcode[1]	String within 32 characters	Blank	It configures the anonymous call off code. The phone will send the code to deactivate the anonymous call feature on server side when you deactivate it on the phone.
features.anonymous.feature_key_sync.enable	**0**-Disabled **1**-Enabled	0	It enables or disables to synchronize the anonymous call status between the IP phone and the server.

Call Number Filter

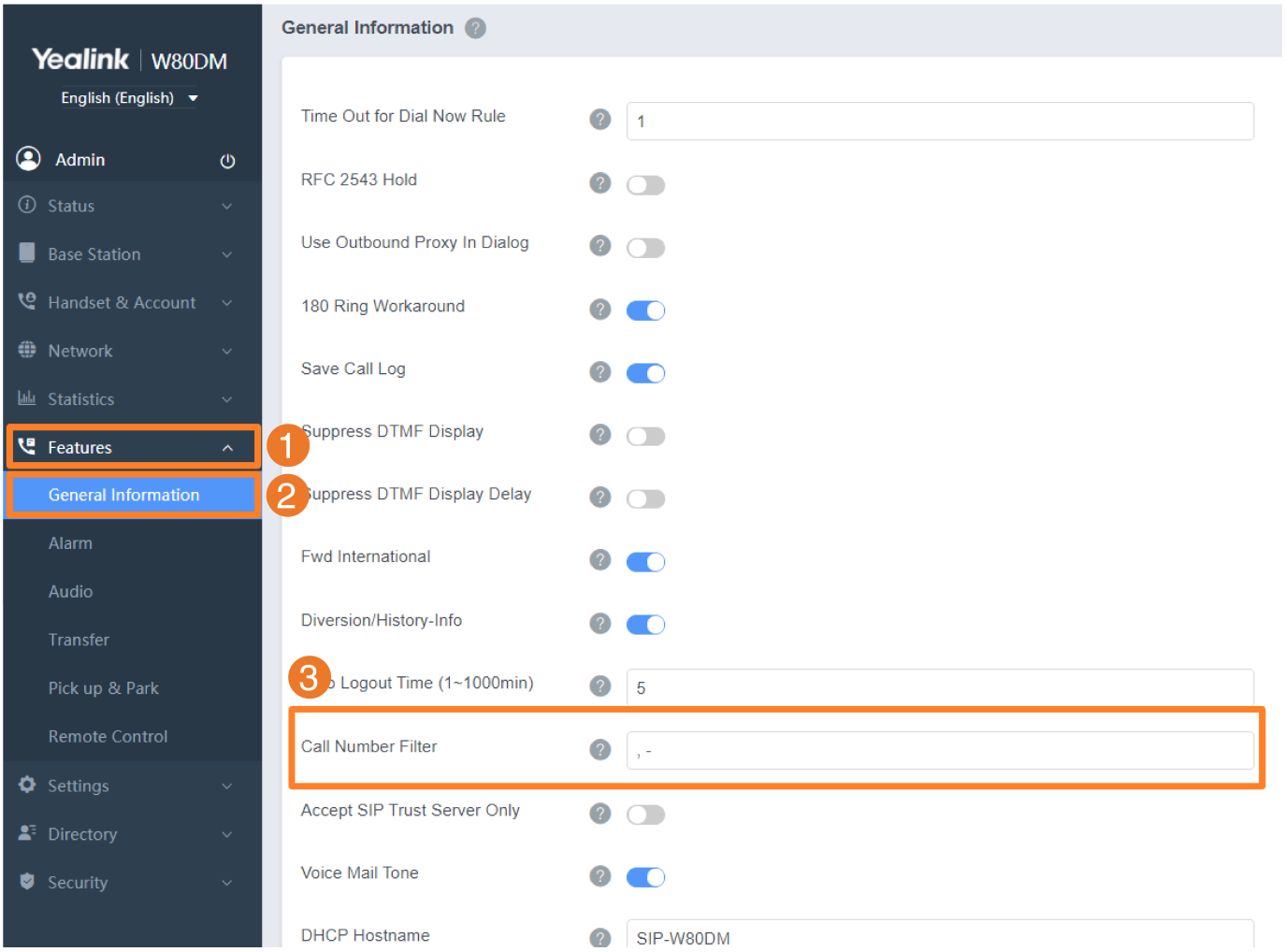
Introduction

The call number filter feature allows a phone to filter designated characters automatically when dialing.

Call Number Filter Configuration

Set via the Web User Interface

1. 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**: fatures.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 whether to receive or place an IP call. You can neither receive nor place an IP call if you disable this feature.

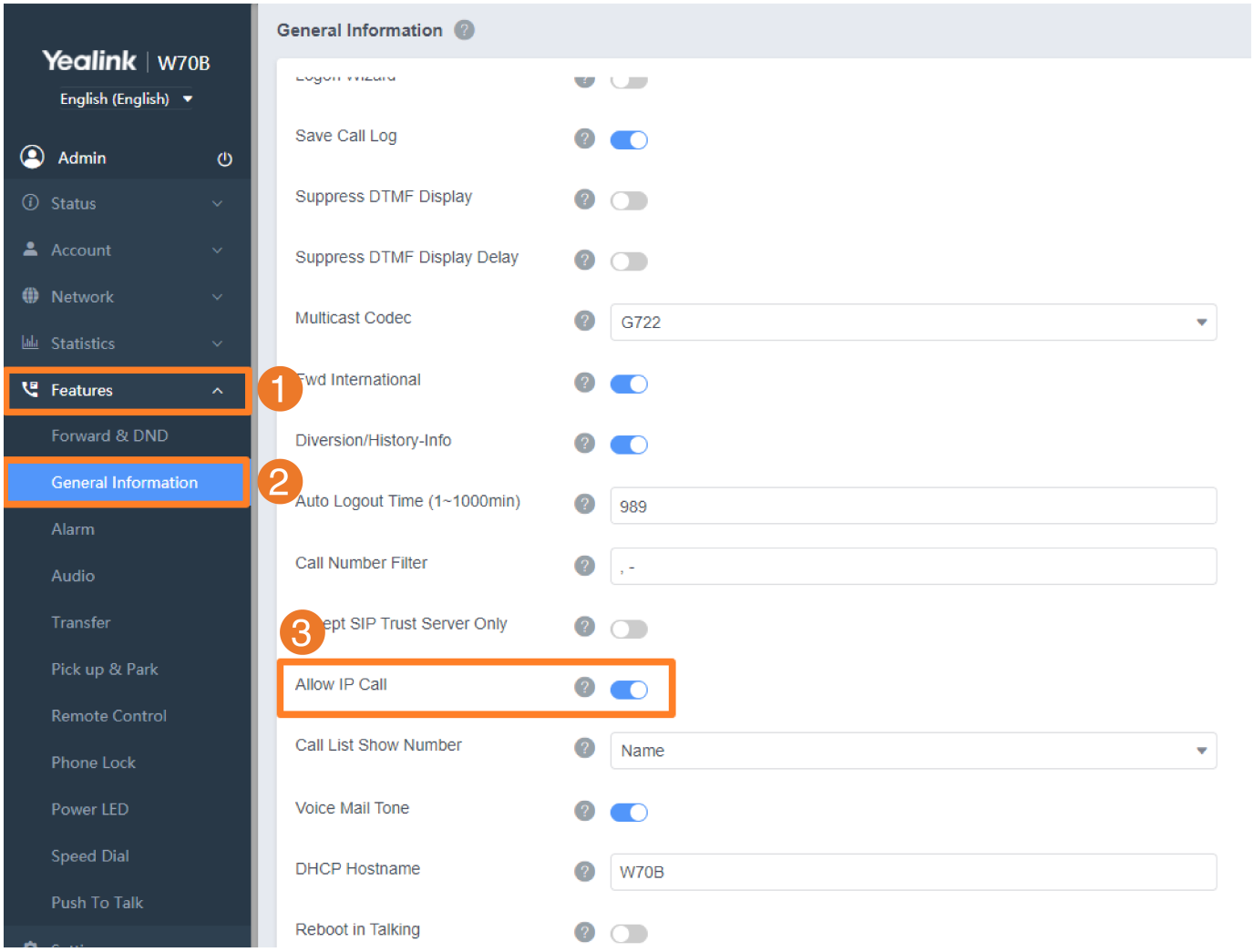
Before You Begin

This feature is only applicable to W70B.

IP Address Call Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Allow IP Call**.



Configuration Parameter

features.direct_ip_call_enable

Parameter	Permitted Values	Default	Description
features.direct_ip_call_enable	**0**-Disabled **1**-Enabled	1	It enables or disables allowing IP address calls. 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 it 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.

Before You Begin

It is only applicable to W71H, W73H, W74H, W78H, W53H, W56H, W57R, W59R, and W59R Pro.

Auto Answer Configuration

Set via the Device Interface

See Answer a Call Automatically.

Configuration Parameter

custom.handset.auto_answer.enable
account.X.auto_answer

Parameter	Permitted Values	Default	Description
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 from answering 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.auto_provision.handset_configured.enable" is set to 1 (Enabled).
account	**0**-Disabled	0	It enables or disables auto-answer for a SIP call.

.X.auto_answer[1]	**1**-Enabled, the phone can automatically answer an incoming call.		The phone cannot automatically answer the incoming call during a call or while dialing, even if the auto answer is enabled.

[1] The parameter is only applicable to W90 Multi-Cell System.

Anonymous Call Rejection

Introduction

Anonymous call rejection allows the 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.

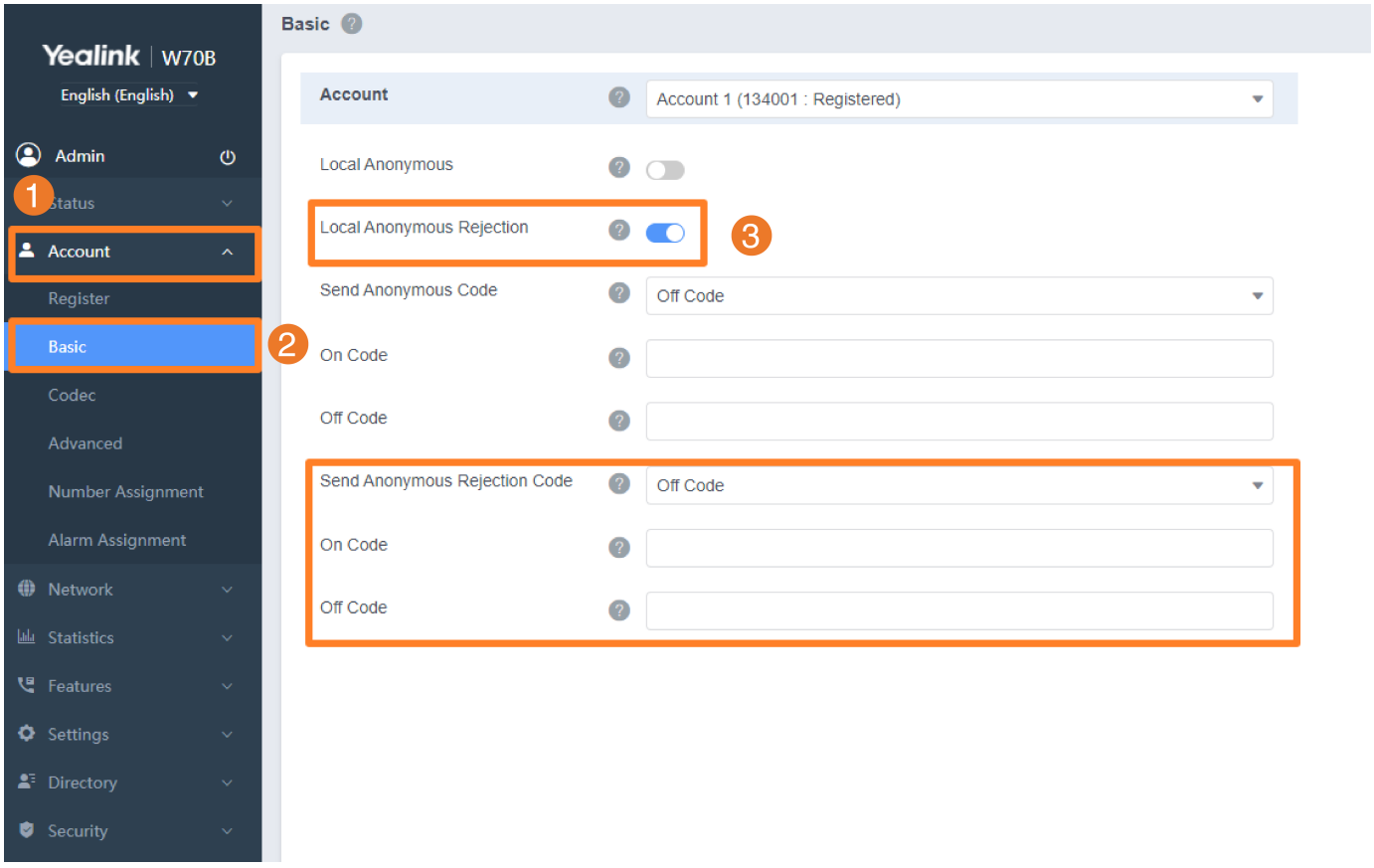
Anonymous Call Rejection Configuration

Set via the Device Interface

See Reject Anonymous Calls.

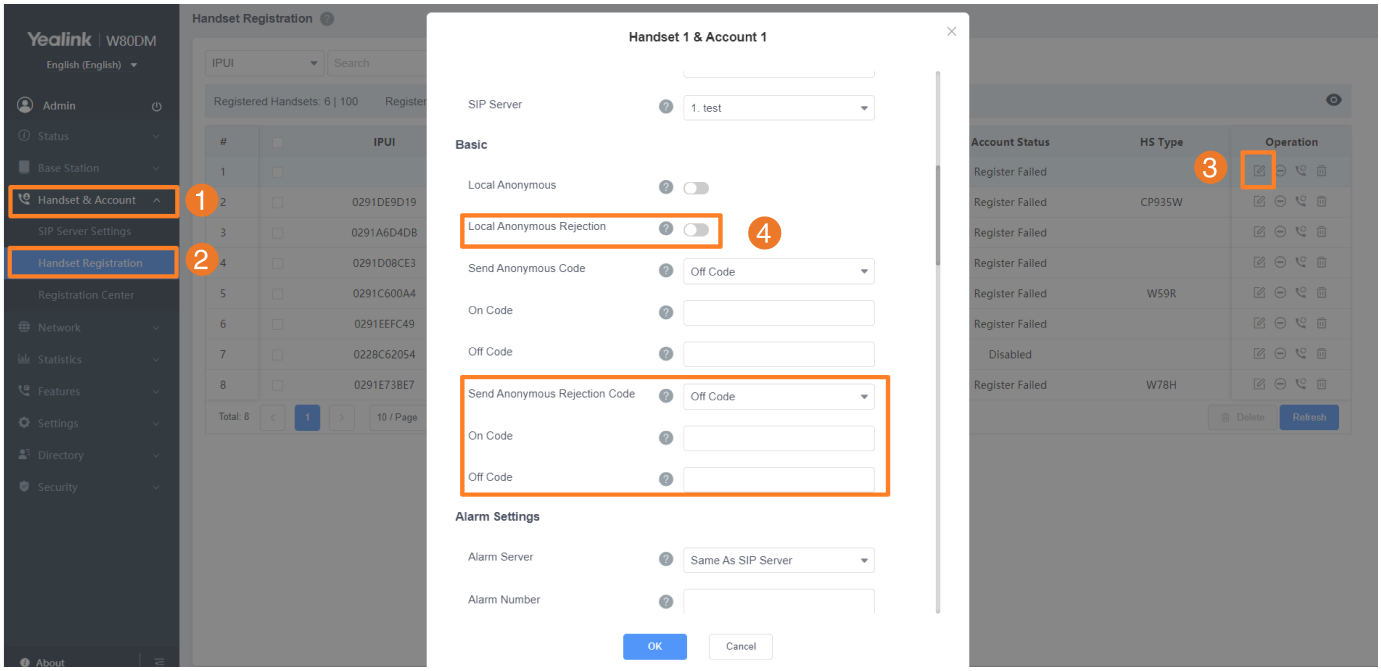
Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Basic** > **Local Anonymous Rejection**/**Send Anonymous Rejection Code**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** >

Handset Registration > **Add Handset/Edit** > **Local Anonymous Rejection**/**Send Anonymous Rejection Code**.



Configuration Parameter

account.X.reject_anonymous_call
account.X.anonymous_reject_oncode
account.X.send_anonymous_rejection_code
account.X.anonymous_reject_offcode

Parameter	Permitted Values	Default	Description
account.X.reject_anonymous_call [1]	**0**-Off **1**-On, the phone will automatically reject incoming calls from users enabled anonymous call feature. The anonymous user's phone screen presents "**Forbidden**".	0	It triggers the anonymous call rejection feature to turn on or off.
account.X.anonymous_reject_on	String within 32 characters	Blank	It configures the anonymous call rejection on code. The phone will send the code to activate the anonymous call rejection feature on

code[1]			the server-side when you activate it on the phone.
account.X.send_anonymous_rejection_code[1]	**0**-Off Code, the phone will send anonymous rejection off code to the server when you deactivate the anonymous call rejection feature. **1**-On Code, the phone will send anonymous rejection on code to the server when you activate the anonymous call rejection feature.	0	It configures the IP phone to send the anonymous call rejection on/off code to activate/deactivate the server-side anonymous call rejection feature for account X.
account.X.anonymous_reject_offcode[1]	String within 32 characters	Blank	It configures the anonymous call rejection off code. The phone will send the code to deactivate the anonymous call rejection feature on the server-side when you deactivate it on the phone.

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

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.

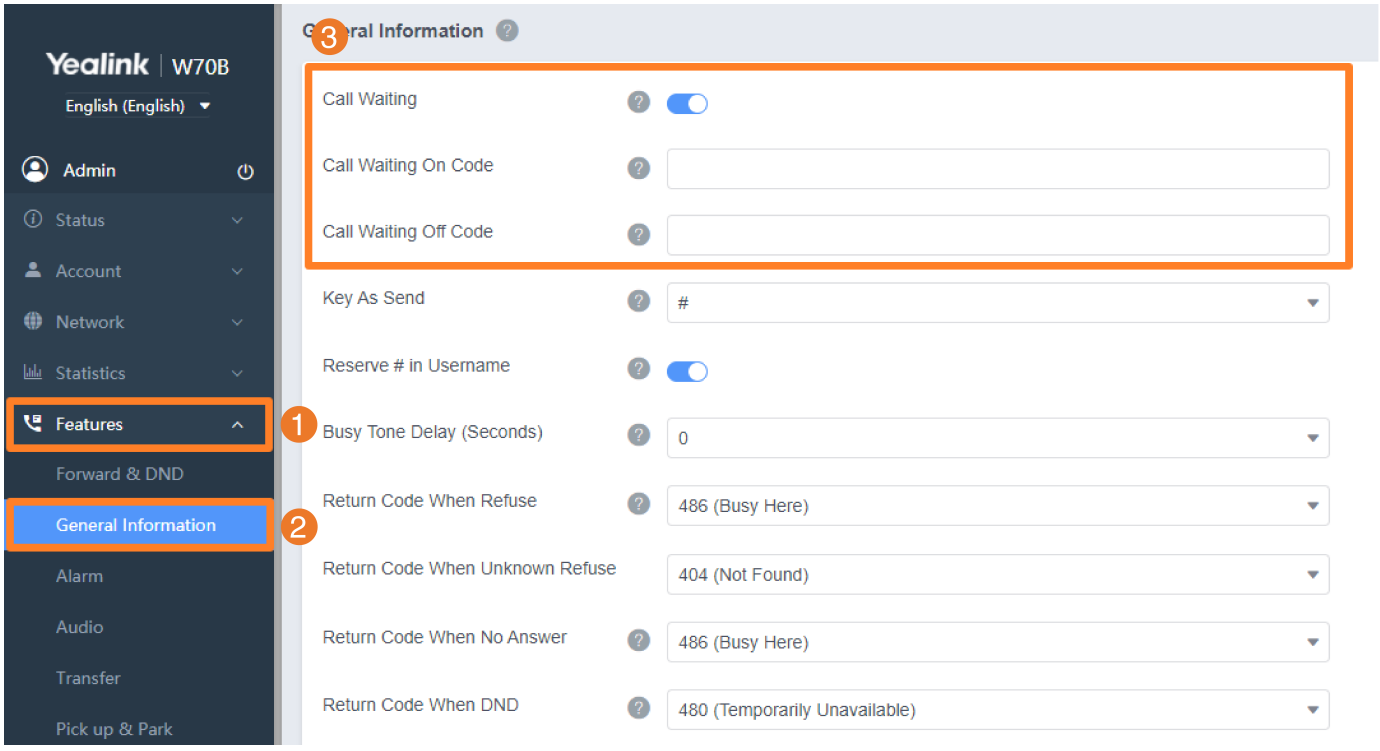
Call Waiting Configuration

Set via the Device Interface

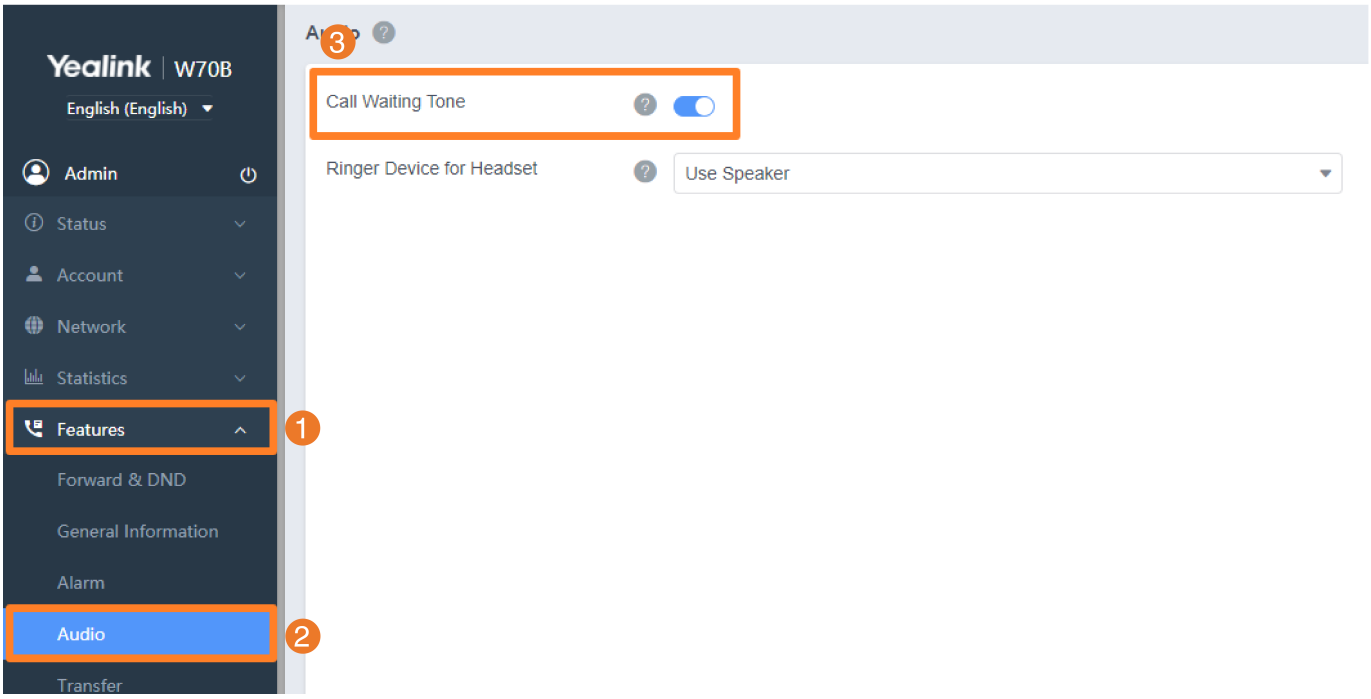
See Call Waiting.

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 from playing 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.

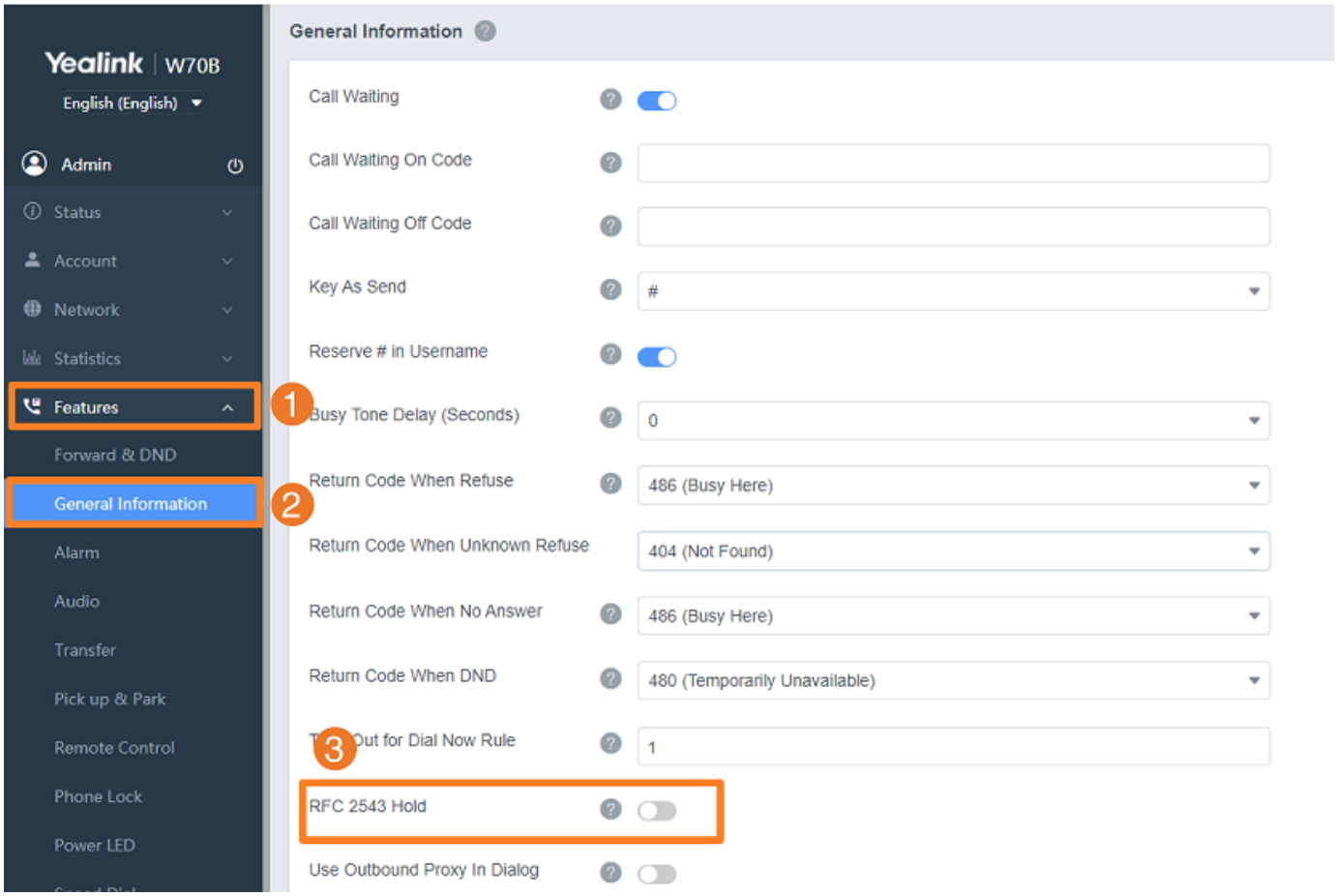
The phones support two call hold methods:

- RFC 3264, which sets the "a" (media attribute) in the SDP to sendonly, recvonly, or inactive (for example, a=sendonly).
- 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**.



Configuration Parameter

sip.rfc2543_hold
account.X.hold_use_inactive[1]

Parameter	Permitted Values	Default	Description
sip.rfc2543_hold	**0**-Disabled, SDP media direction attributes (such as a=sendonly) per RFC 3264 is used when placing a call on hold. **1**-Enabled, SDP media connection address c=0.0.0.0 per RFC 2543 is used when placing a call on hold.	0	It enables or disables the phone to use RFC 2543 (c=0.0.0.0) outgoing hold signaling.
account.X.hold_use_inactive[1]	**0**-Disabled, SDP media direction attribute "a=sendonly" is used when placing a call on hold. **1**-Enabled, SDP media direction attribute "a=inactive" is used when placing a call on hold. RTP packets will not be sent or received.	0	It enables or disables the phone from using inactive outgoing hold signaling. It works only if "sip.rfc2543_hold" is set to 0 (Disabled).

[1] X is the account ID.

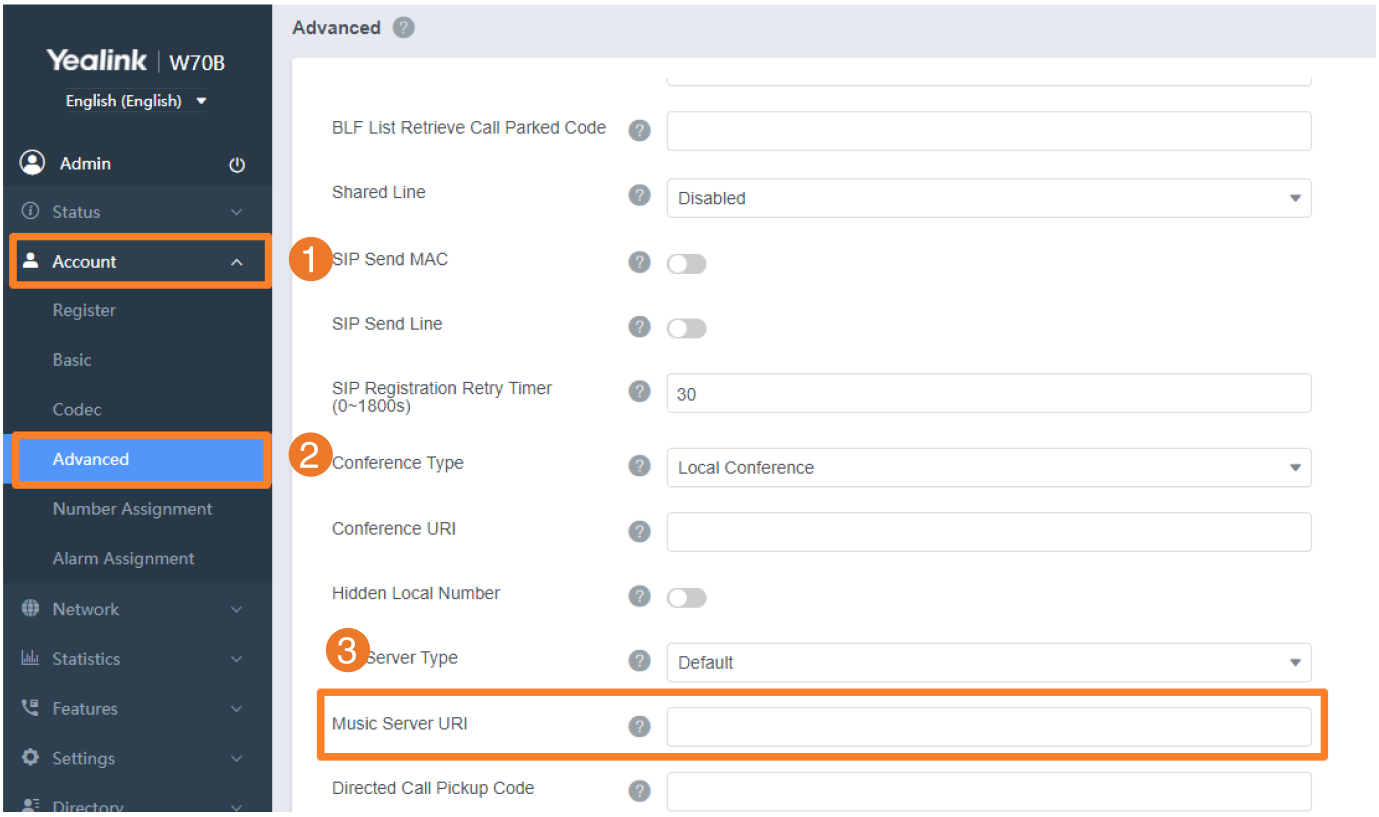
- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

Music on Hold (MoH) Configuration

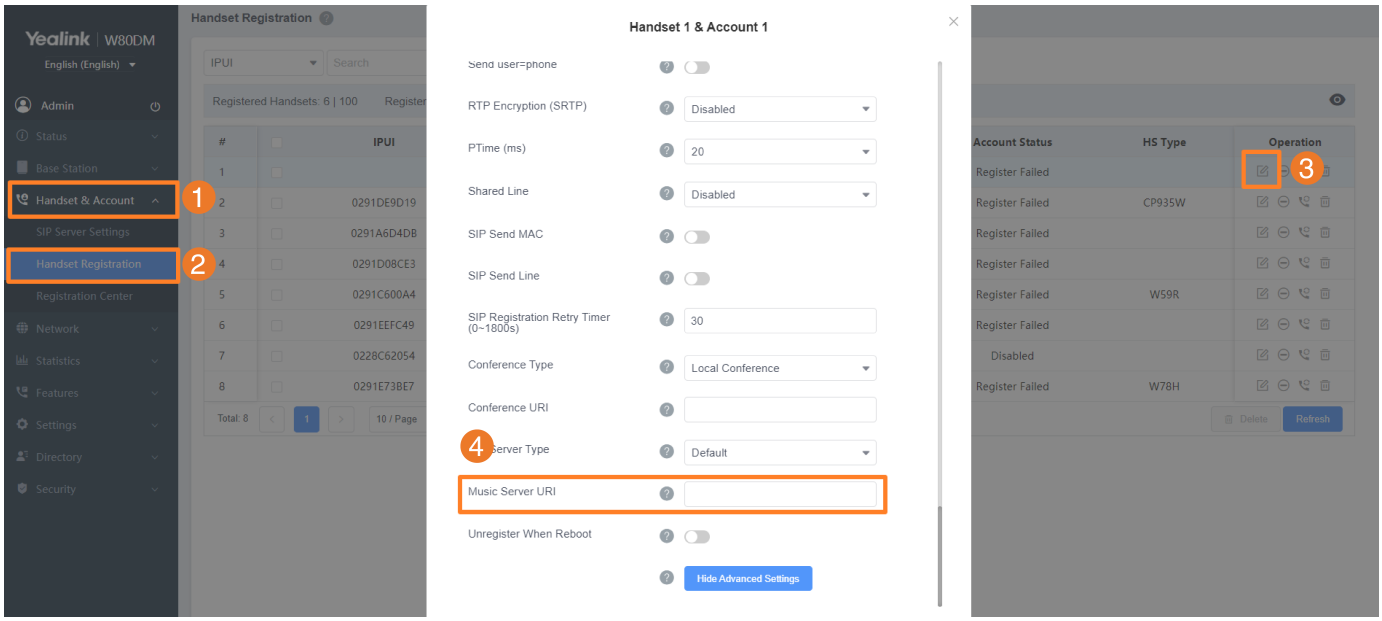
When a call is placed on hold, the phone will send an INVITE message to the specified MoH server account according to the SIP URI. The MoH server account automatically responds to the INVITE message and immediately plays audio from some source located anywhere (LAN, Internet) to the held party. For more information, refer to draft RFC draft-worley-service-example.

Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Advanced** > **Music Server URI**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **Show Advanced Settings** > **Music Server URI**.



Configuration Parameter

account.X.music_server_uri
account.X.music_on_hold_type

Parameter	Permitted Values	Default	Description

		t	
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_hold_type[1]	**0**-Calling the Music On Hold server before holding the call **1**-Calling the Music On Hold server after holding the call	0	It configures the way to process Music On Hold when placing an active call on hold.

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

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

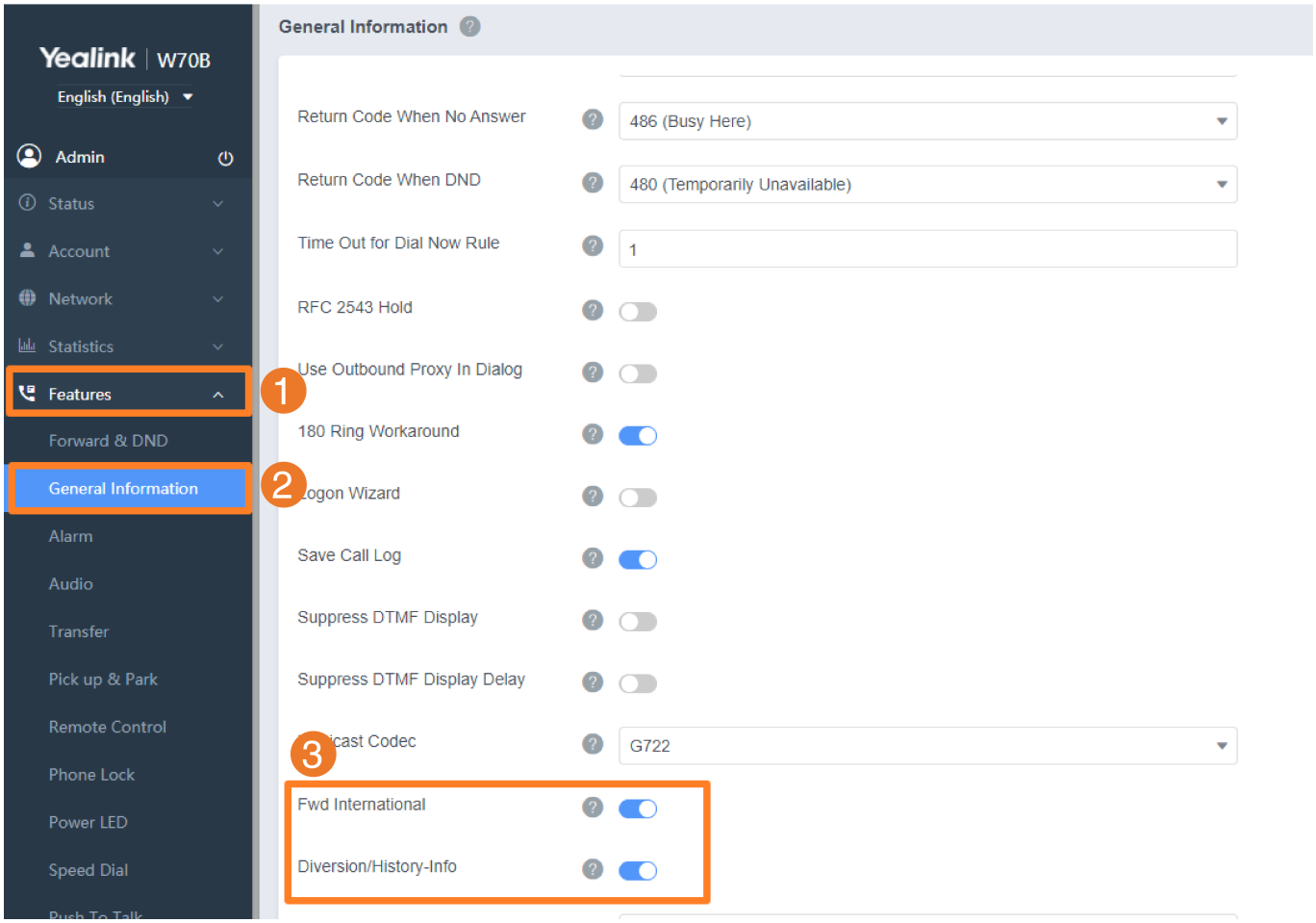
You can change the following call-forward settings:

- Enable or disable the call forward feature. If disabled, 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 the message when you forward an incoming call to another party.

Call Forward Feature Configuration

Yealink phones support call forward on code and off code to activate and deactivate server-side call forward feature.

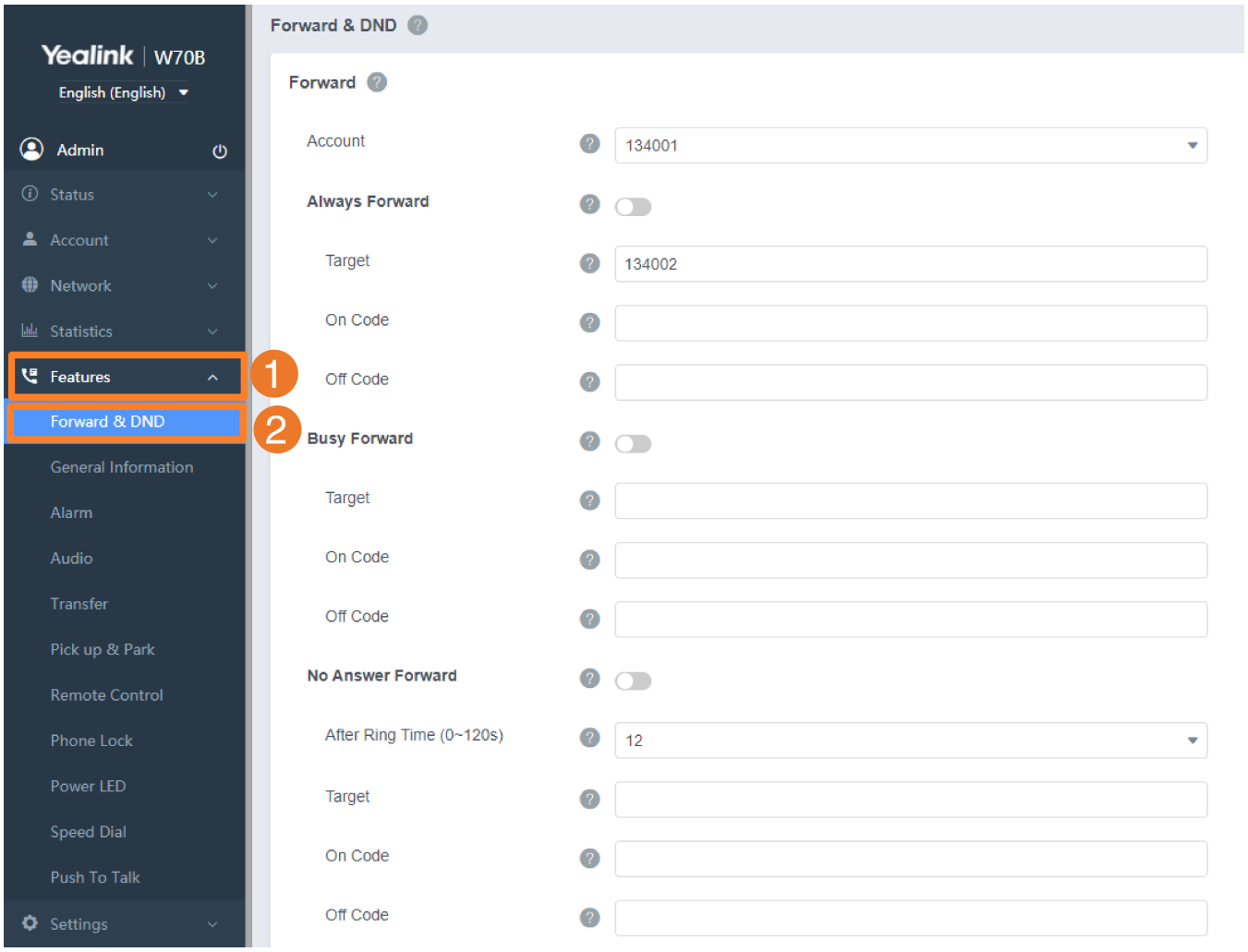
They may vary on different servers.

Set via the Device Interface

See Call Forward.

Set via the Web User Interface

1. On the web user interface, go to **Features** > **Forward&DND** > **Forward**.



Auto Provisioning

```
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
```

Par	Permitted Values	Def	Description

ameter		ault	
account.X.always_fwd.enable[1]	**0**-Off **1**-On, incoming calls to the account X are forwarded to the destination number (configured by the parameter account.X.always_fwd.target) immediately.	0	It triggers always forward feature to on or off. 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.X.always_fwd.on_code[1]	String within 32 characters	Blank	It configures the always forward on code to activate the server-side always forward feature. The phone will send the always forward on code, and the pre-configured destination number (configured by the parameter account.X.always_fwd.target) to the server when you activate always forward feature on the phone. 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	String within 32 characters	Blank	It configures the always forward off code to deactivate the server-side always forward feature. The phone will send the always forward off code to the server when you deactivate always forward feature on the phone.

_code[1]			It works only if "features.fwd.allow" is set to 1 (Enabled) and "features.fwd_mode" is set to 1 (Custom).
account.X.busy_fwd.enable[1]	**0**-Off **1**-On, incoming calls to the account X are forwarded to the destination number (configured by the parameter account.X.busy_fwd.target) when the callee is busy.	0	It triggers the busy forward feature to on or off.
account.X.busy_fwd.target[1]	String within 32 characters	Blank	It configures the destination number of the busy forward. It works only if "features.fwd.allow" is set to 1 (Enabled) and "features.fwd_mode" is set to 1 (Custom).
account.X.busy_fwd.on_code[1]	String within 32 characters	Blank	It configures the busy forward on code to activate the server-side busy forward feature. The phone will send the busy forward on code and the pre-configured destination number (configured by the parameter account.X.busy_fwd.target) to the server when you activate the busy forward feature on the phone. 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.o	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.

ff_code[1]			It works only if "features.fwd.allow" is set to 1 (Enabled) and "features.fwd_mode" is set to 1 (Custom).
account.X.timeout_fwd.enable[1]	**0**-Off **1**-On, incoming calls to the account X are forwarded to the destination number (configured by the parameter account.X.timeout_fwd.target) after a period of ring time.	0	It triggers no answer forward feature to on or off. It works only if "features.fwd.allow" is set to 1 (Enabled) and "features.fwd_mode" is set to 1 (Custom).
account.X.timeout_fwd.target[1]	String within 32 characters	Blank	It configures the destination number for the no answer forward. It works only if "features.fwd.allow" is set to 1 (Enabled) and "features.fwd_mode" is set to 1 (Custom).
account.X.timeout_fwd.timeout[1]	Integer from 0 to 20	2	It configures ring times (N) to wait before forwarding incoming calls. 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[	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

1]			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 off 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).

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

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.

Auto Provisioning

```
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_key_sync.enable[1]	**0**-Disabled **1**-Enabled, server-based call forward is enabled. Server and local phone call forwarding are synchronized.	Blank	It enables or disables the forward feature synchronization for 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.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

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.

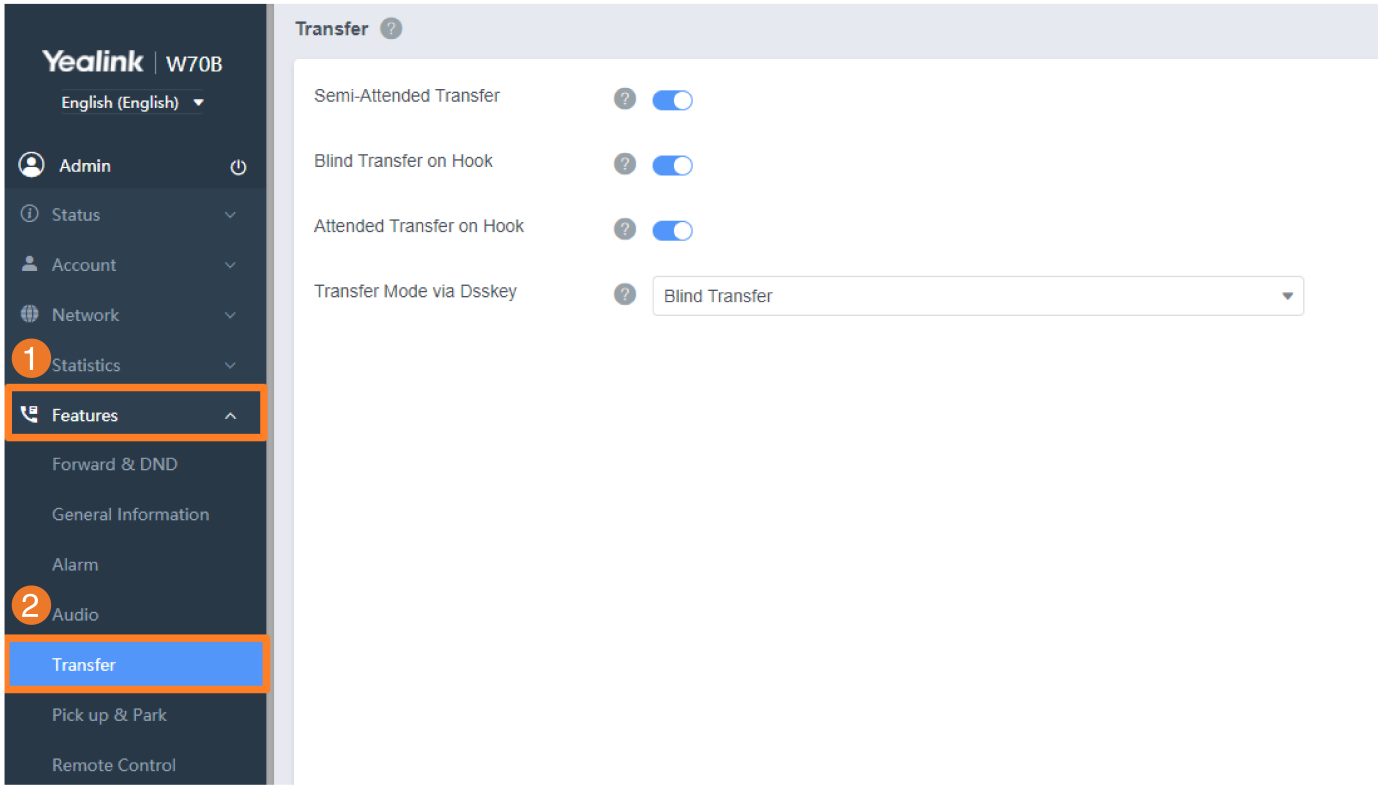
Yealink phones support call transfer using the REFER method specified in RFC 3515 and offer three types of transfer:

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 consulting. Attended transfer is implemented by a REFER method with Replaces in the Refer-To header.

Call Transfer Configuration

Set via the Web User Interface

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



Configuration Parameter

features.transfer.allow
transfer.semi_attend_tran_enable
account.X.transfer_refer_to_contact_header.enable
features.transfer_keep_session2_after_failed.enable
transfer.blind_tran_on_hook_enable
transfer.on_hook_trans_enable

Parameter	Permitted Values	Default	Description
features.transfer.allow	**0**-Disabled, call transfer feature is not available to users. **1**-Enabled	1	It enables or disables the call transfer feature.
transfer.semi_attend_tran_enable	**0**-Disabled, when the user presses the TRAN key after hearing the ringback tone, the phone will blind transfer the call. **1**-Enabled, when the user presses the TRAN key after hearing the ringback	1	It enables or disables the semi-attended transfer.

	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 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.

- For W70B, X=1-10.

- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

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

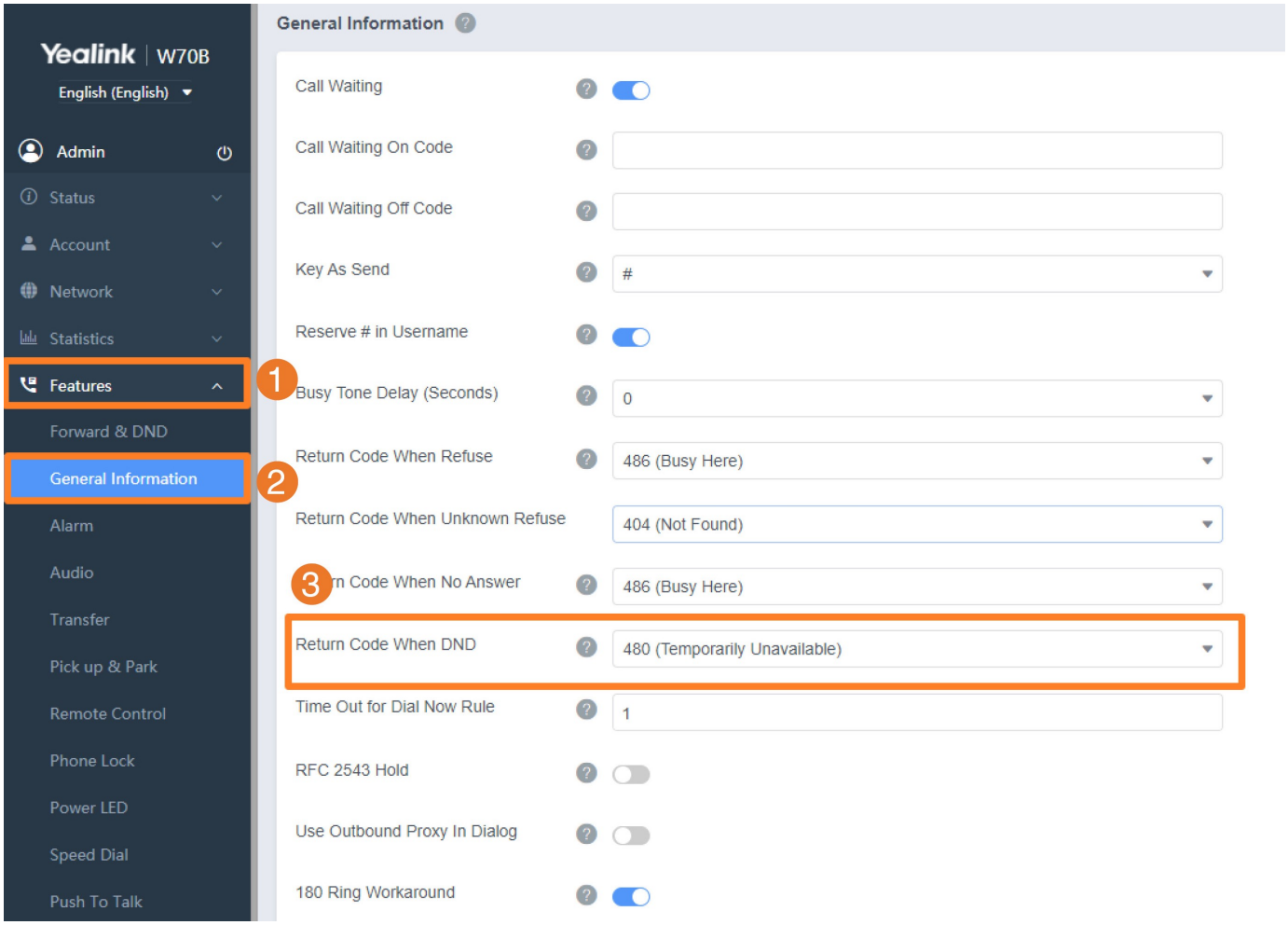
You can change the following DND settings:

- Enable or disable the DND feature. If disabled, the users have no permission to configure DND on their phone.
- 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.

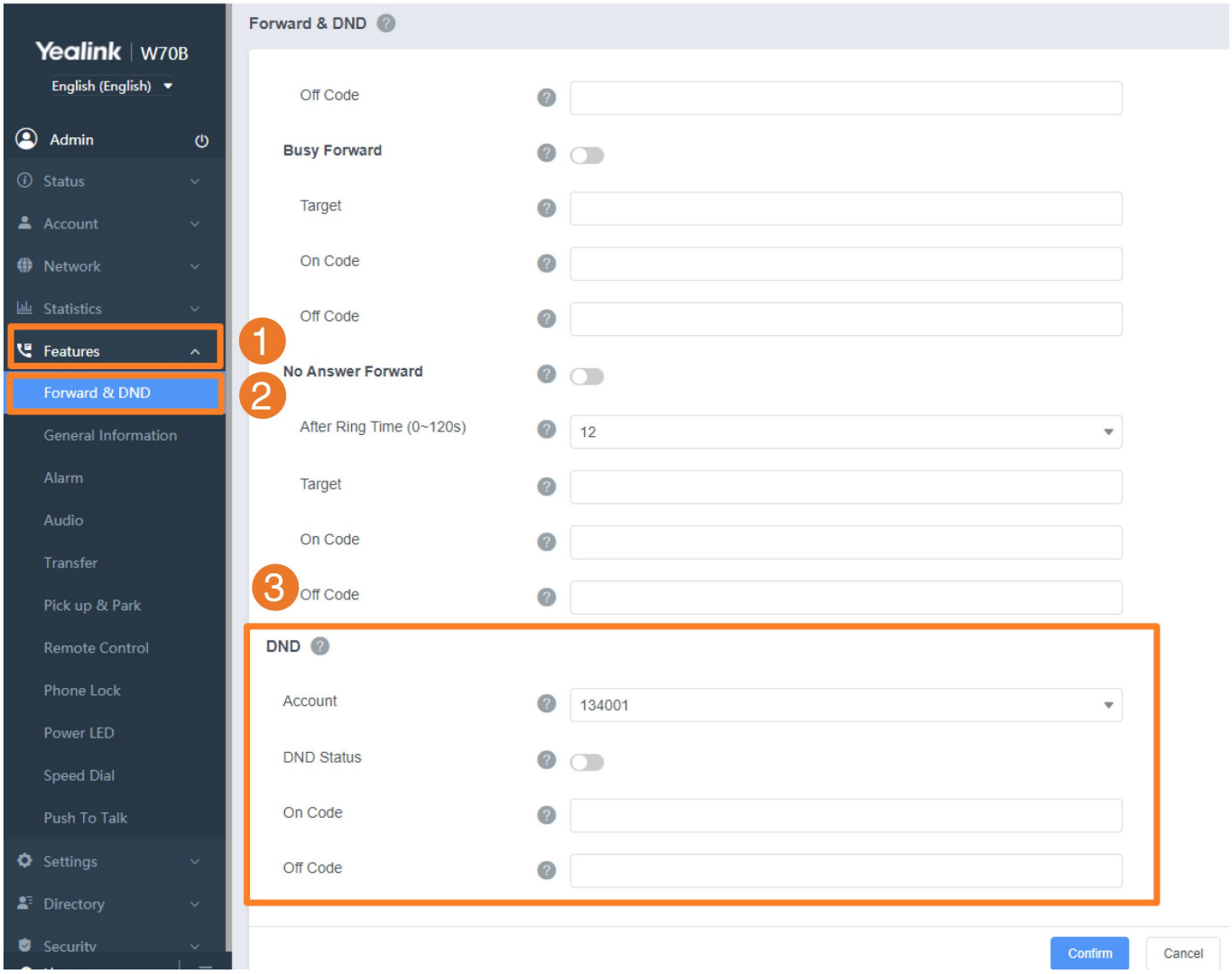
The following table lists the parameters you can use to configure DND.

Set via the Device Interface

See Do Not Disturb.

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	String within 32	Bl	It configures the DND on code to activate the

.dnd.on_code[1]	characters	Blank	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.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

DND Synchronization for Server-side Configuration

DND synchronization feature provides the capability to synchronize the status of the DND features between the IP phone and the server.

If the DND is activated in phone mode, the DND status changing locally will be synchronized to all registered accounts on the server; but if the DND status of a specific account is changed on the server, the DND status locally will be changed.

The following table lists the parameters you can use to configure DND synchronization for server-side.

Configuration Parameter

features.feature_key_sync.enable
account.X.dnd.feature_key_sync.enable

Parameter	Permitted Values	Default	Description
features.feature_key_sync.enable	**0**-Disabled **1**-Enabled, the phone sends a SUBSCRIBE message with event "as-feature-event".	0	It enables or disables synchronization of the feature status between the IP phone and the server.
account.X.dnd.feature_key_sync.enable[1]	**0**-Disabled **1**-Enabled, server-based DND is enabled. Server and local phone DND are synchronized.	Blank	It enables or disables the DND feature synchronization for account X. The value configured by this parameter takes precedence over that configured by the parameter "features.dnd.feature_key_sync.enable". It works only if "account.X.feature_key_sync.enable" is set to 1 (Enabled).

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

No Answer

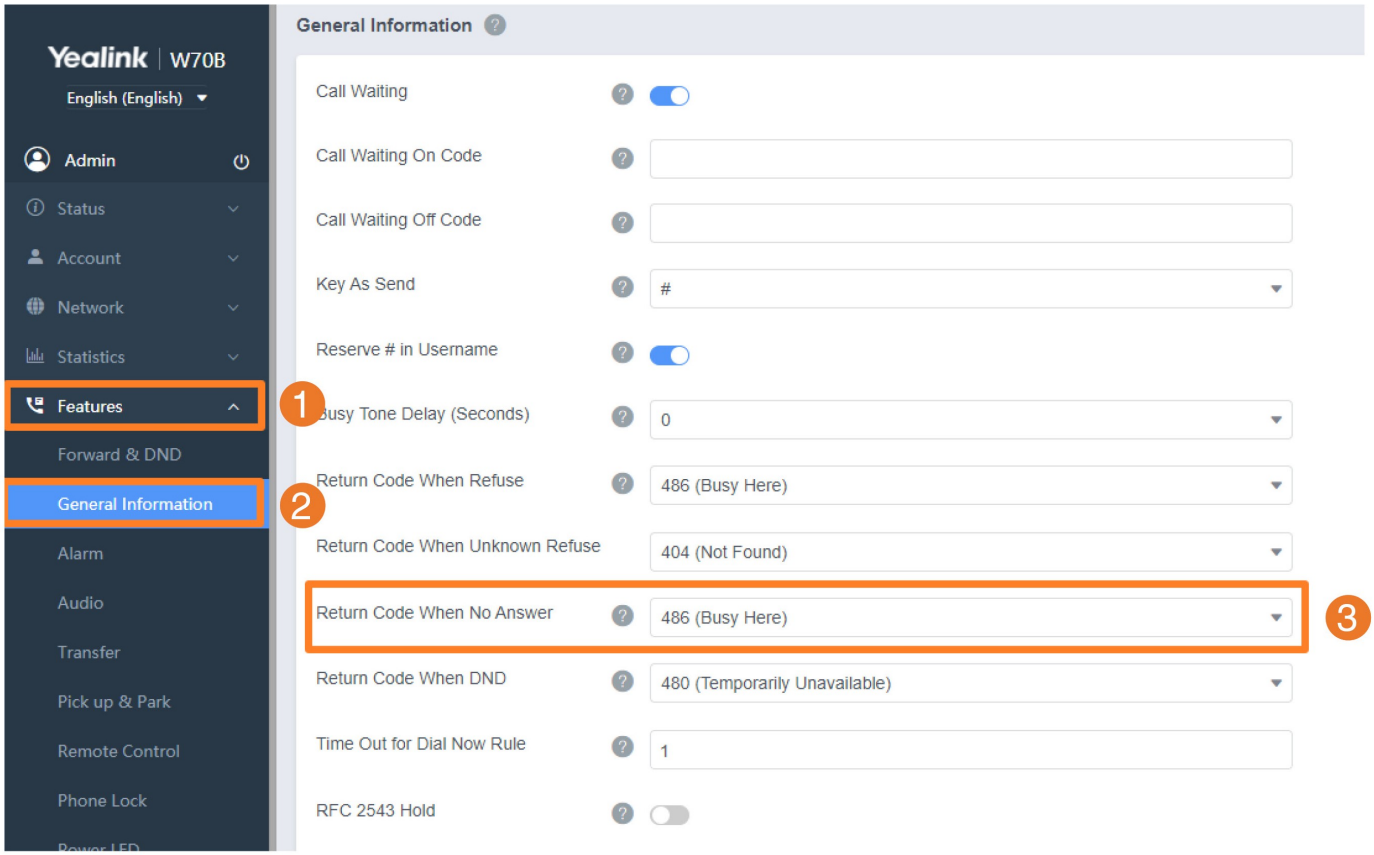
Introduction

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

Parameter	Permitted Values	Default	Description
features.no_answer_code	**404**-Not Found **480**-Temporarily	486	It configures a return code and reason for response messages when the handset does not answer an incoming call.

	Unavailable **486**-Busy Here **600**-Busy Everywhere **603**-Decline		

Push-to-Talk (PTT)

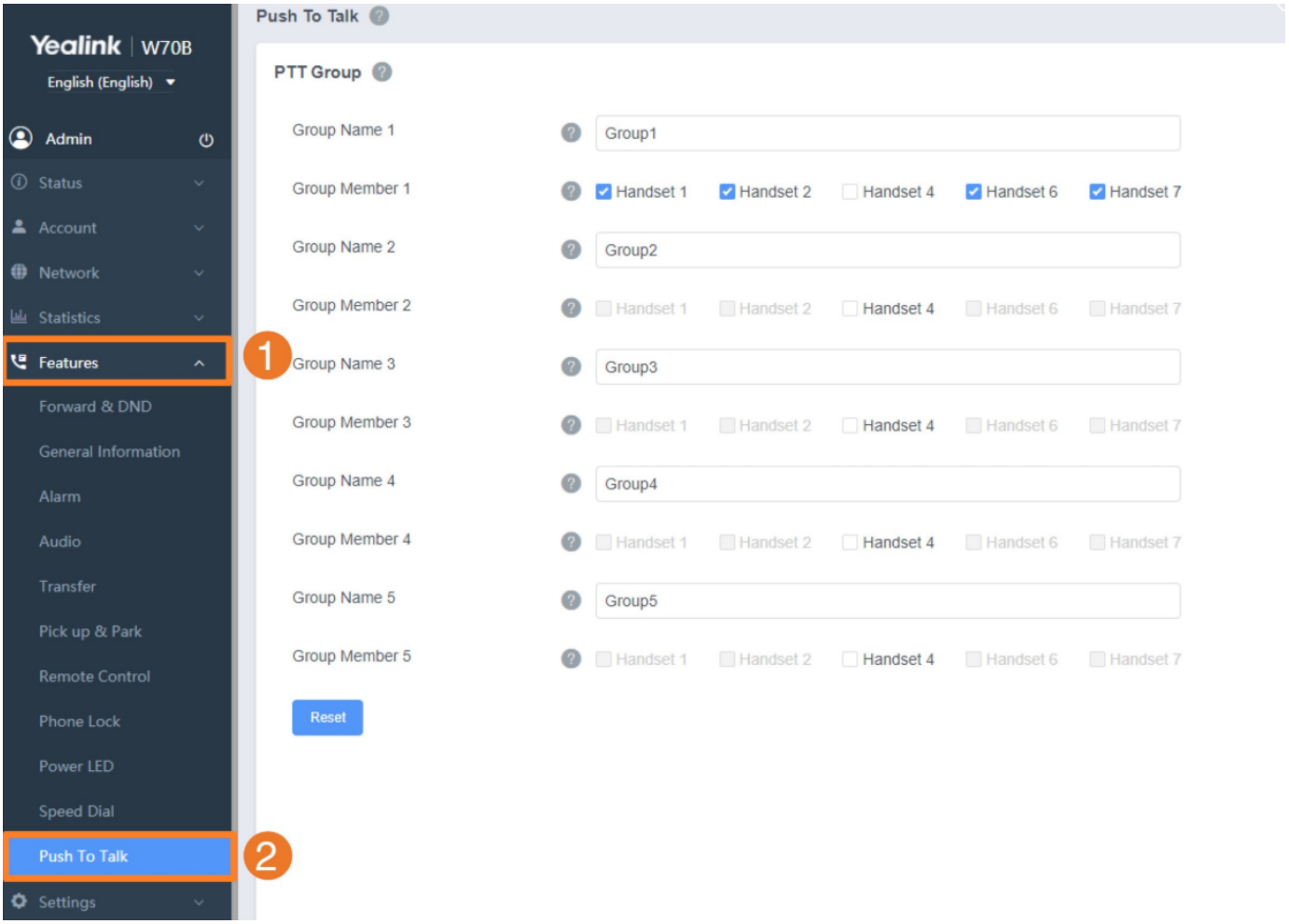
Introduction

Starting with firmware 146.85.0.35, the push-to-talk feature is available on Yealink handsets, headsets, and DD Phone. The handset can be used like a handheld transceiver (walkie-talkie) among handsets, headsets, and DD Phone registered at the same base station.

Push-to-Talk (PTT) Configuration

Set via the Web User Interface

On the web user interface, go to **Features** > **Push-to-Talk**.



Configuration Parameter

features.ptt.group.x.name
features.ptt.group.x.member
features.ptt.handset_accept.enable

features.ptt.time
handset.x.ptt_presskey.idle_play.enable
handset.x.ptt_presskey.idle_play.track

Parameter	Permitted Values	Default	Description
features.ptt.group.x.name	String within 32 characters	GroupX	It configures the PTT group name.
features.ptt.group.x.member	Integer from 1 to 10	Blank	It selects the PTT groupX members. 1. You can only fill in a maximum of 10 members. 2. The number of members is affected by the wide and narrow-band channels. 3. A maximum of 5 calls are allowed simultaneously under the broadband. 4. If there are more than 5 active members, switch to narrowband.
features.ptt.handset_accept.enable	**0**-Disabled **1**-Enabled	0	It configures whether the device receives the PTT meeting prompt. 1. This parameter is only applicable to the handset and the DD Phone. 2. PTT calls prompt will only be received by idle handsets.
features.ptt.time	60, 120, 240, 480, 0 (min) The value **0** means that the meeting continues, and all	3 mins	It configures the duration of the PTT message or PTT meeting. After auto provisioning, when the meeting duration is reached, your device will automatically exit the meeting.

	participants will not exit the meeting until the meeting ends.		
handset.x.ptt_presskey.idle_play.enable	**0**-Disabled **1**-Enabled	0	It configures the device to join and listen to the talk in the same PTT group automatically or manually.
handset.x.ptt_presskey.idle_play.track	**0**-speaker channel **1**-handset channel	0	It configures the channel where the device automatically plays the PTT talk sound.

Conference

Introduction

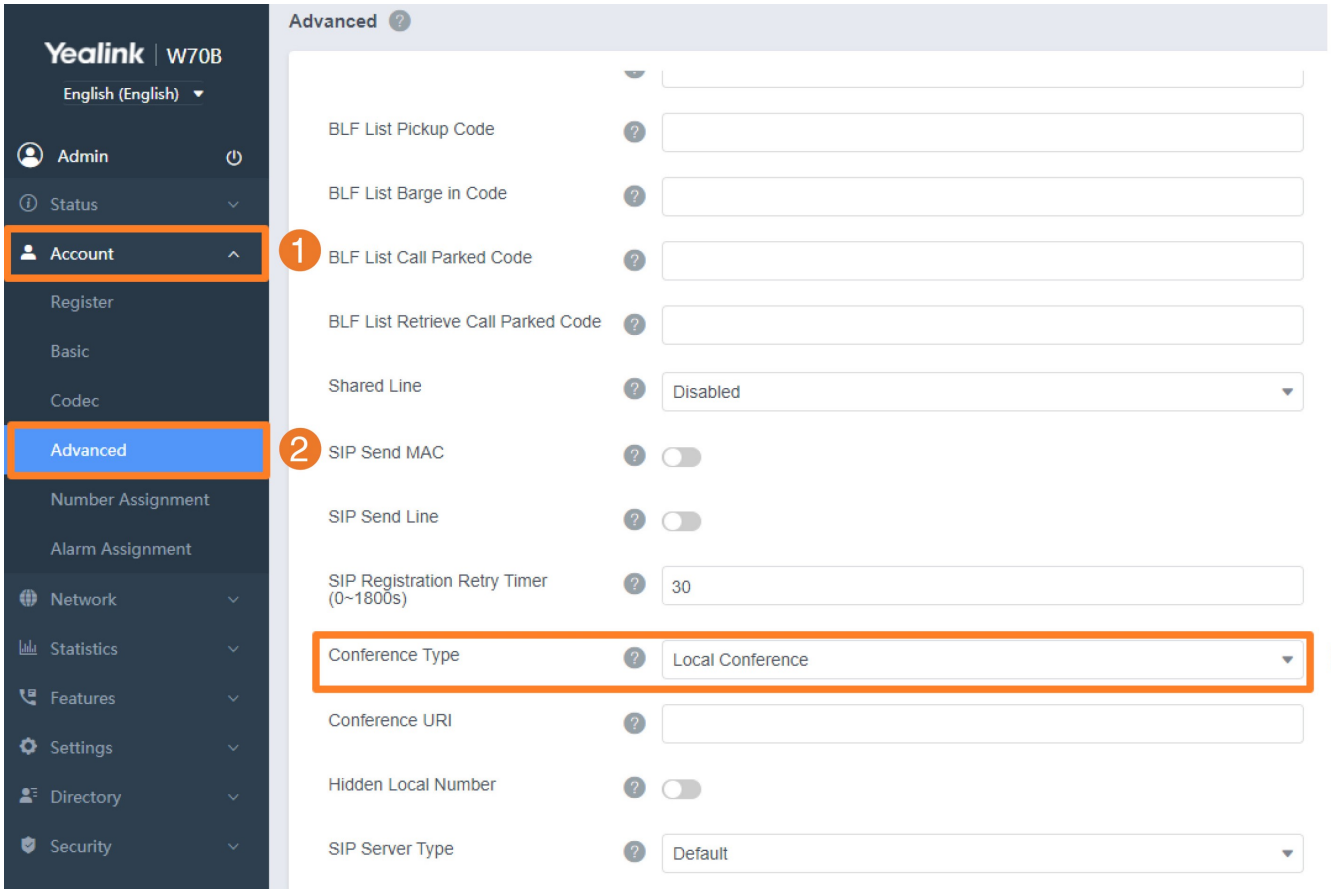
The Yealink phones support local conferences and network conferences.

Conference Type Configuration

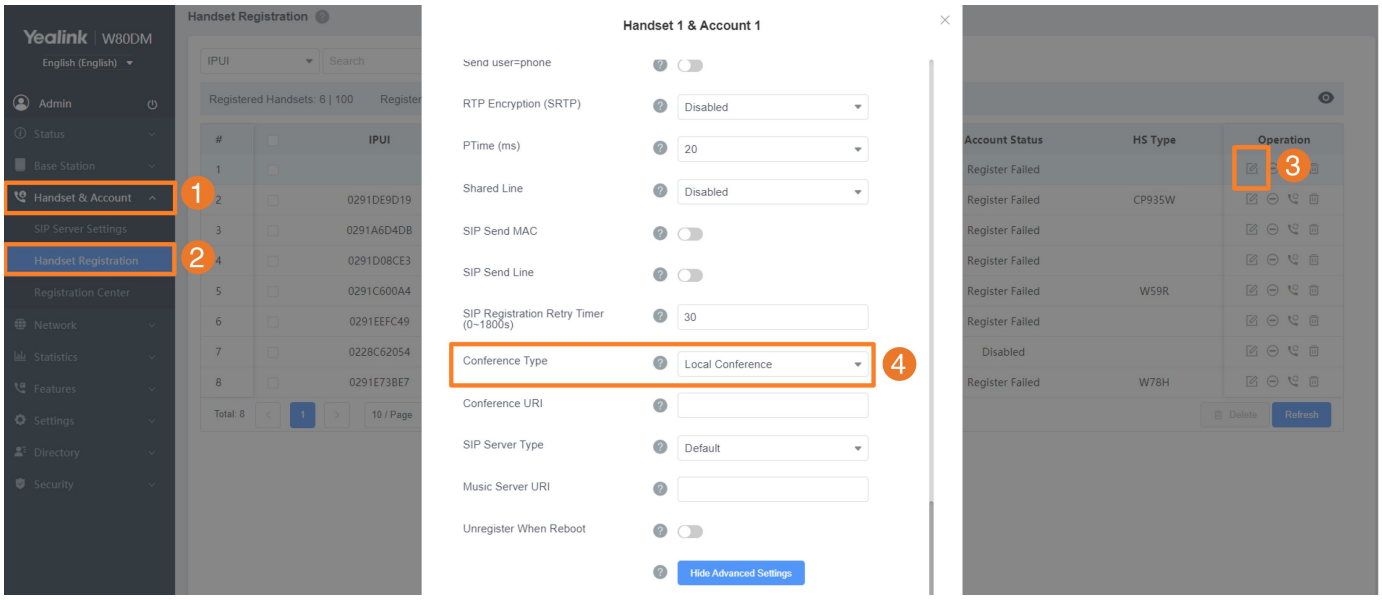
You can specify which type of conference to establish.

Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Advanced** > **Conference Type**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **Conference Type**.



Configuration Parameter

Parameter	Permitted Values	Default	Description
account.X.conf_type[1]	**0**-Local Conference **2**-Network Conference	0	It configures the conference type for a specific account.

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

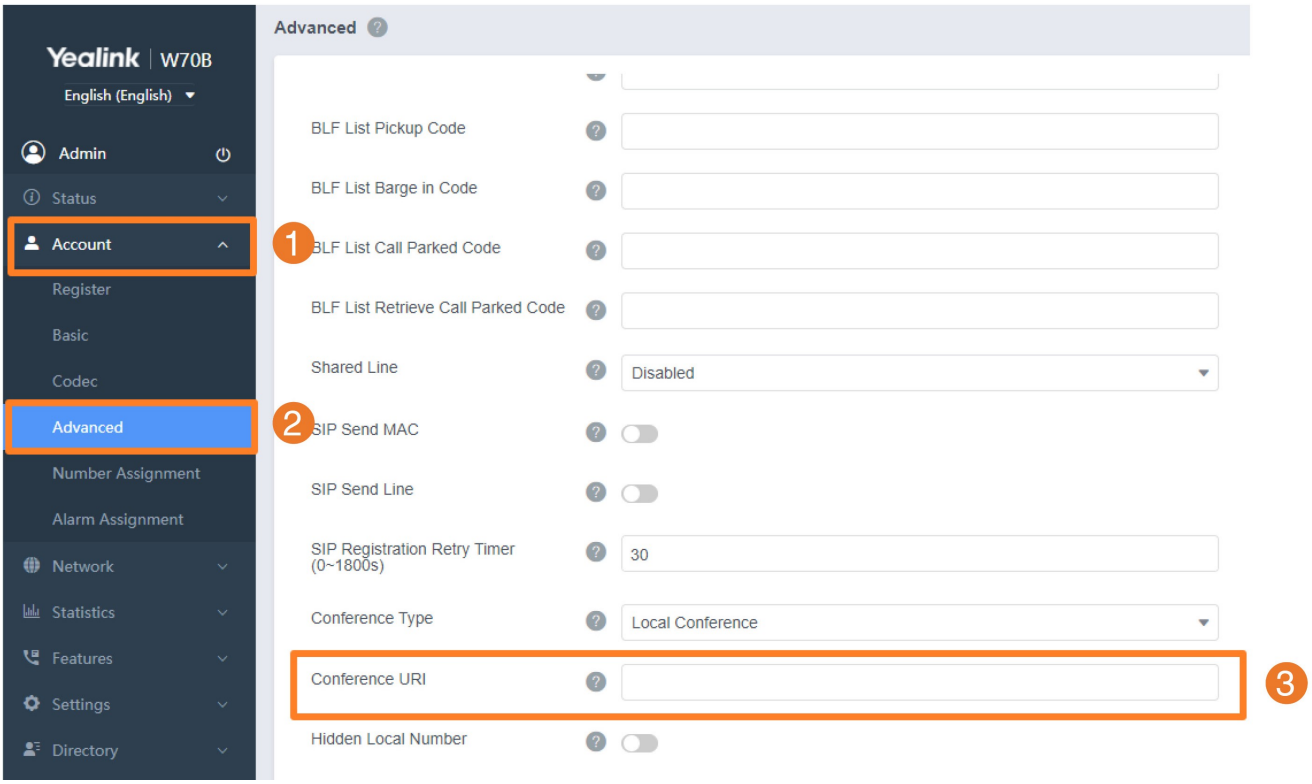
Network Conference Configuration

Network conference, also known as a centralized conference, provides you with the flexibility of call with 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.

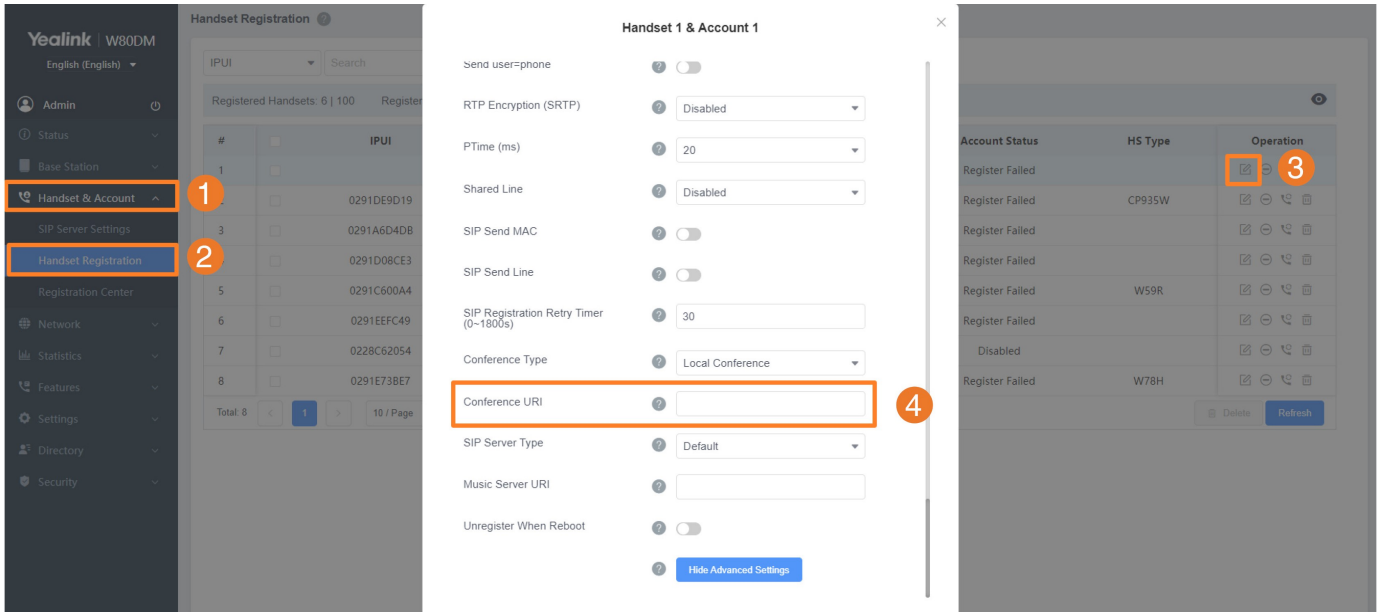
For network conferences, if any party leaves the conference, the remaining parties are still connected.

Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Advanced** > **Conference URI**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **Conference URI**.



Configuration Parameter

account.X.conf_uri

Parameter	Permitted Values	Default	Description
account.X.conf	SIP URI within 511	Bla	It configures the network conference URI for a

_uri[1]	characters	nk	specific account. It works only if "account.X.conf_type" is set to 2 (Network Conference).

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

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).

SD Card Recording

Introduction

CP930W-Base phones support manual recording during a call. Before recording, ensure that the SD card has been connected to the phone.

> Yealink phones support an SD card in FAT32 or NTFS format.

The recorded calls are saved in "*.wav" format and include a date/time stamp, the other party's number/IP address/name (or the first person's number/IP address/name you called), and the recording file size. For example, 20160422-1515-Bob was created on Apr. 22, 2016, at 15:15, and you have a call with Bob. Recorded calls can be played on either the phone itself or on a computer using an application capable of playing *.wav files.

> Before recording any call, especially those involving PSTN, it is necessary to know about the rules and restrictions of any governing call recording in the place where you are. It is also very important to have the consent of the person you are calling before recording the conversation.

USB and SD Card Recording Configuration

The following table lists the parameters you can use to configure SD-card and USB recording.

Configuration Parameter

features.usb_call_recording.enable
features.sd_card_call_recording.enable

Parameter	Permitted Values	Default	Description
features.usb_call_recording.enable	**0**-Disabled **1**-Enabled, the recorded calls will be saved to the USB flash drive.	0	It enables or disables the USB call recording feature. > It works only if "static.usbdisk.function.enable" is set to 1 (Enabled).

features.sd_card_call_recording.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the call recording (using an SD card) feature.

End Call on Hook

Introduction

You can configure whether to end a call when you place the handset into the charging cradle.

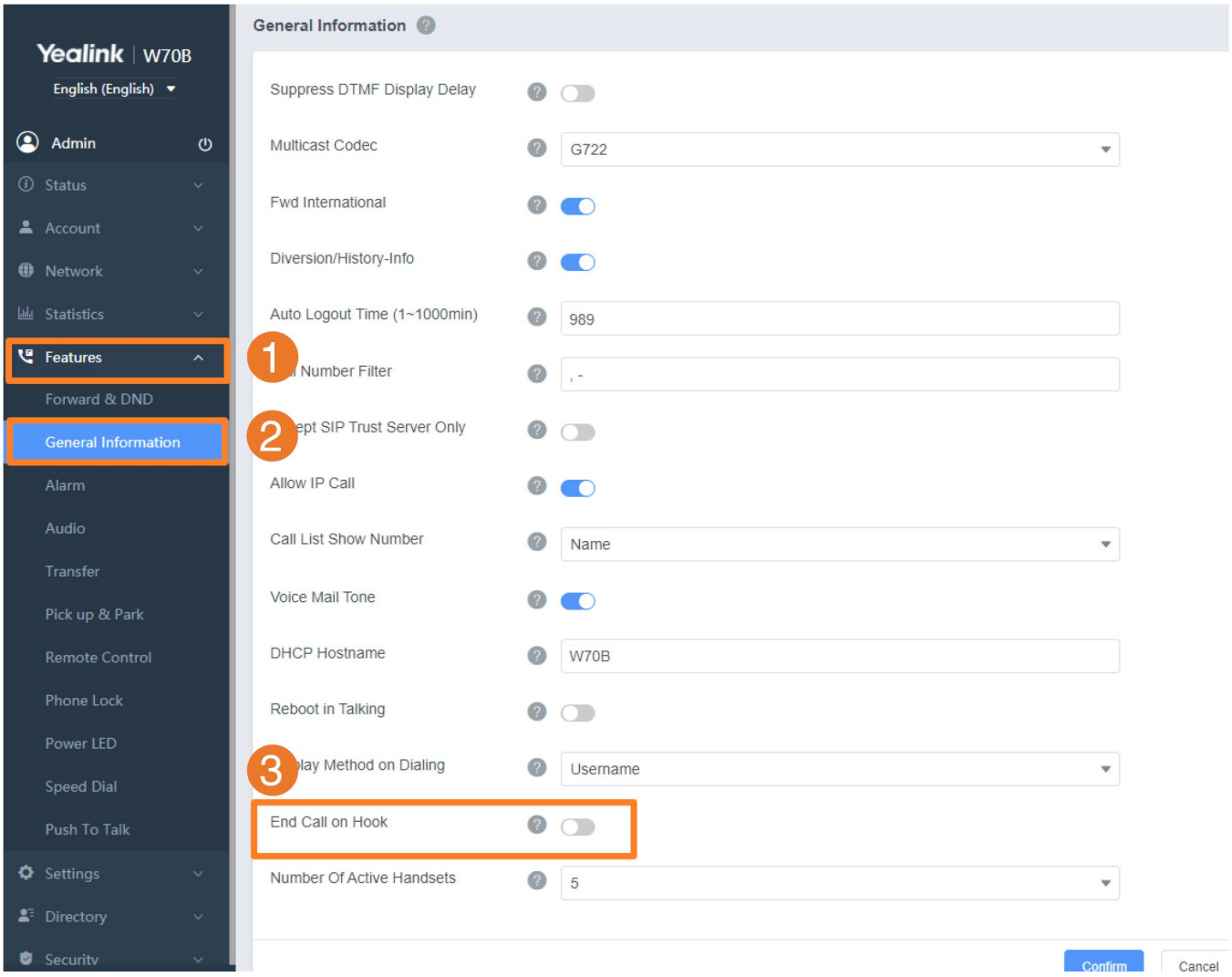
Before You Begin

It is only applicable to W71H, W73H, W74H, W78H, W53H, W56H, W57R, W59R, and W59R Pro.

End Call on Hook Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **End Call On Hook**.



Configuration Parameter

phone_setting.end_call_on_hook.enable

phone_setting.end_call_net_disconnect.enable

Parameter	Permitted Values	Default	Description
phone_setting.end_call_on_hook.enable	**0**-Never **1**-Always	1	It enables or disables ending a call when placing the handset into the charger cradle.
phone_setting.end_call_net_disconnect.enable	**0**-Disabled **1**-Enabled, the phone will end the call and go to the Idle screen after 5 seconds.	0	It enables or disables the phone to end the call if the network is unavailable during the call.

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).

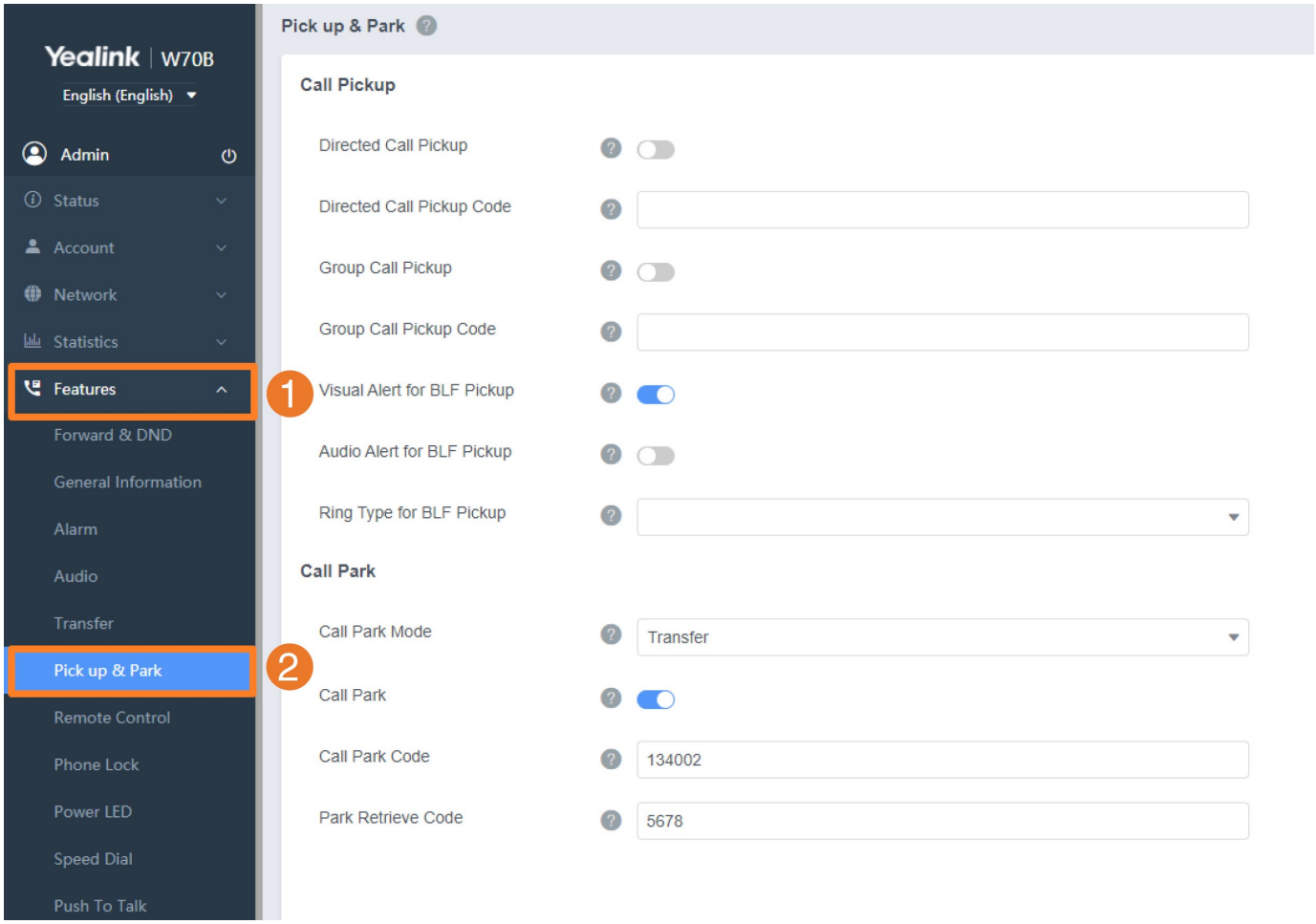
The phones support the call park feature under the following modes:

Mode	Description
FAC Mode	Parks the call to the local extension or the desired extension by dialing the park code.
Transfer Mode	Parks the call to the shared parking lot by 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.

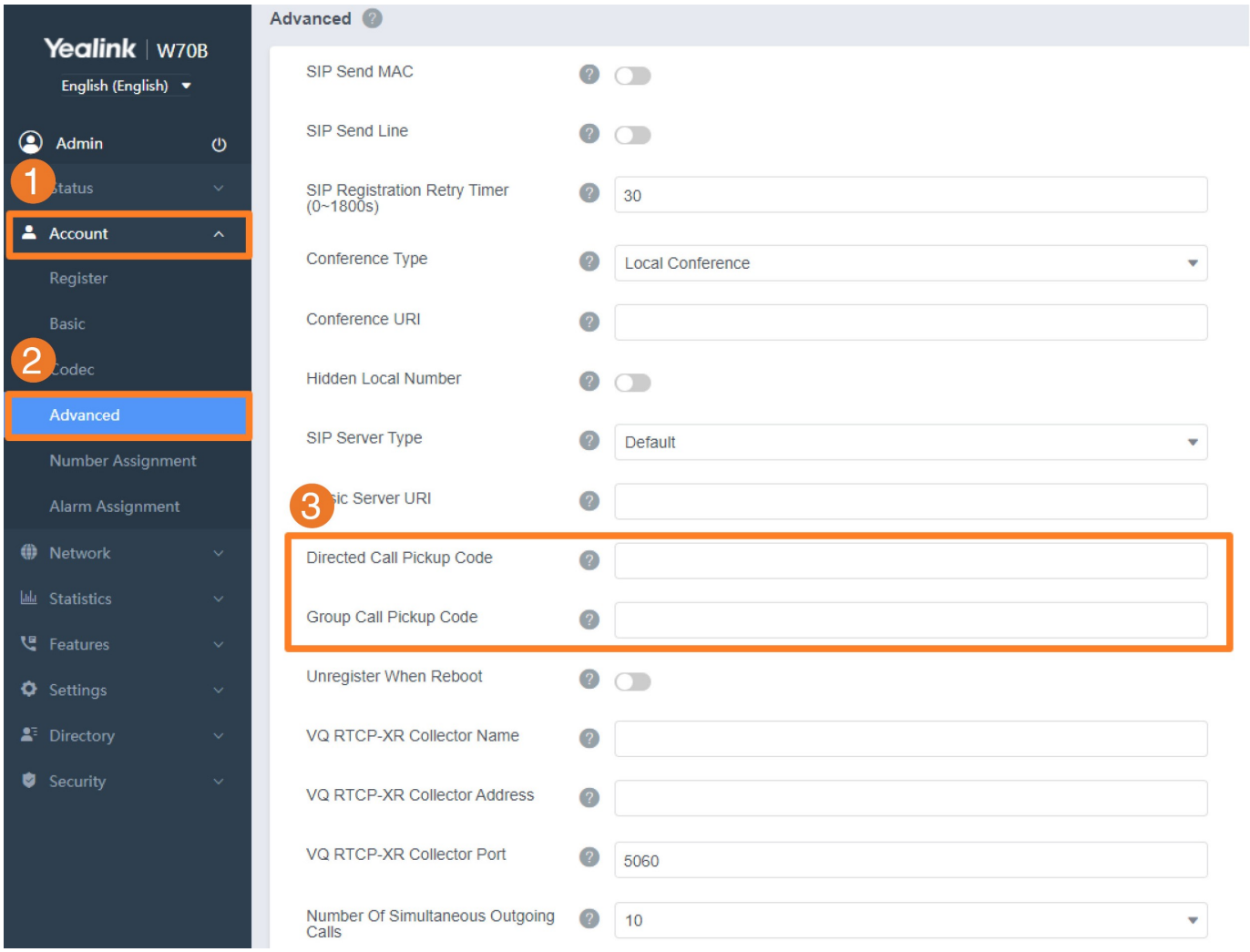
Call Park and Retrieve Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **Pick up & Park**.



2. On the web user interface, go to **Account** > **Advanced** > **Directed Call Pickup Code**/**Group Call Pickup Code**.



Configuration Parameter

features.call_park.park_mode
features.call_park.enable
features.call_park.park_code
features.call_park.park_retrieve_code
features.pickup.direct_pickup_enable
features.pickup.direct_pickup_code
features.pickup.group_pickup_enable
features.pickup.group_pickup_code
account.X.direct_pickup_code
account.X.group_pickup_code

Parameter	Permitted Values	Default	Description

features.call_park.park_mode	**1**-FAC, park a call through dialing the call park code. **2**-Transfer, blind transfer the call to a shared parking	2	It configures the call park mode.
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 retrieve parking lot for Transfer call park mode.
features.pickup.direct_pickup_enable[2]	**0**-Disabled **1**-Enabled, the phone will display the **DPickup** soft key on the Dialing screen.	0	It enables or disables the user from using **DPickup** soft key when performing the directed call pickup feature.
features.pickup.direct_pickup_code[2]	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.
features.pickup.group_pickup_enable[2]	String within 32 characters	Blank	It enables or disables the user from using **GPickup** soft key when performing the group call pickup feature.
features.pickup.group_pickup_code[2]	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".

account.X.direct_pickup_code[1] [2]	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".
account.X.group_pickup_code[1] [2]	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. X=1-10.
[2] This parameter is only applicable to DD Phone (Color Screen) registered on W70B.

Shared Line

Introduction

Yealink phones support Shared Call Appearance (SCA) to share a line. Shared call appearances 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 (not applicable to CP930W-Base phones)
- Barge in an active call (not applicable to CP930W-Base phones)
- Pull a shared call (not applicable to CP930W-Base phones)

Shared Call Appearance (SCA) Configuration

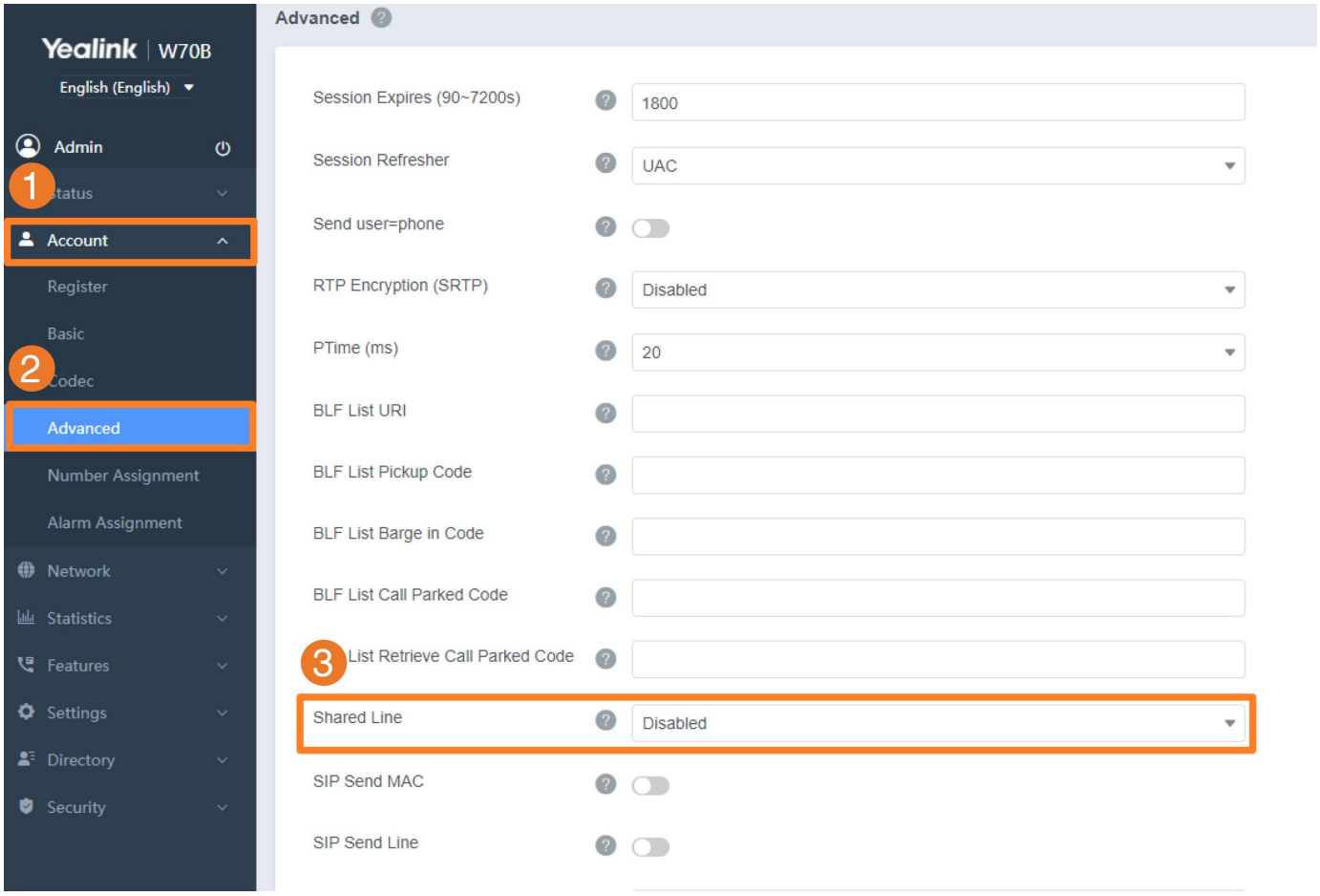
In the SCA scenario, an incoming call can be presented to multiple phones simultaneously. Any IP phone can be used to originate or receive calls on the shared line.

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.

Set via the Web User Interface

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



Configuration Parameter

account.X.shared_line
account.X.line_seize.expires
features.barge_in_via_username.enable

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).
features.barge_in_via_username.enable	**0**-Disabled, user registers name to barge in, the phone sends an INVITE request with the registered name when barging in a call **1**-Enabled, the phone sends an INVITE request with the user name when barging in a call	0	It enables or disables the phone to use the user name of the account to barge in an active call. All phones except CP930W-Base/ CP935W-Base registered on W70B is applicable to this parameter.

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

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 alerts when receiving new voice messages.

MWI for Voice Mail Configuration

Yealink phones support both solicited and unsolicited MWI.

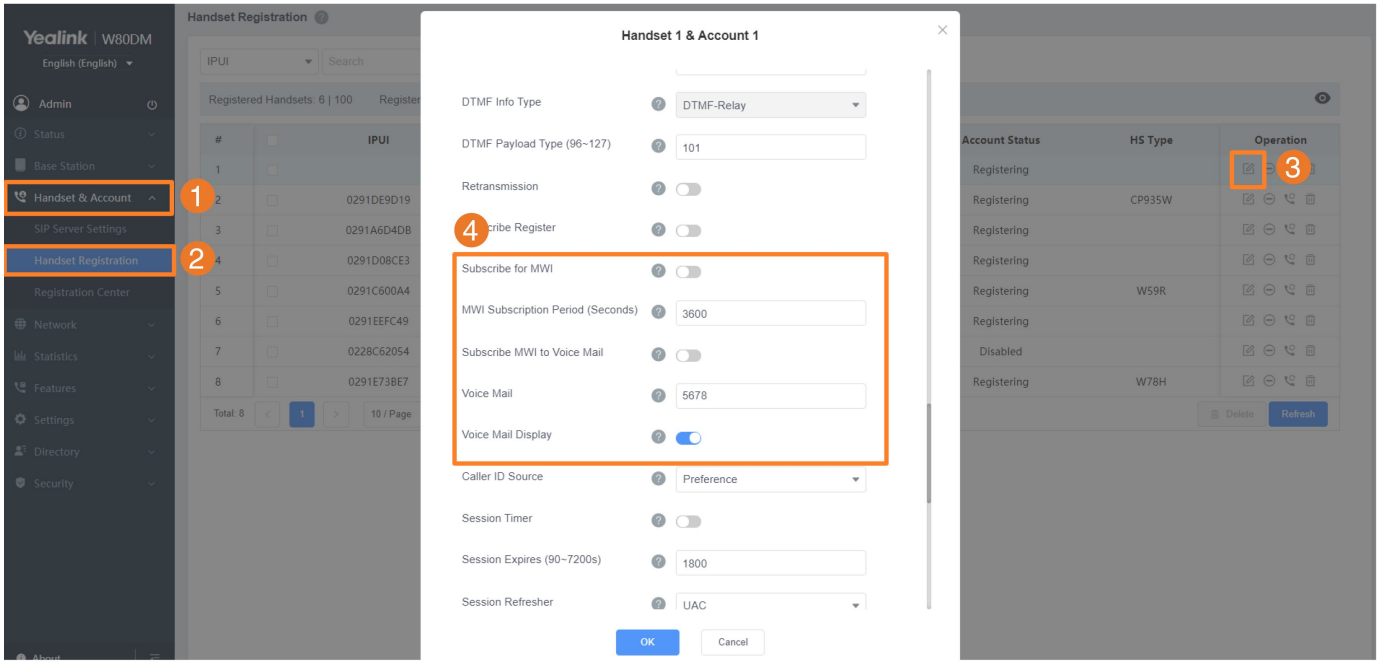
- **Unsolicited MWI**: The IP phone sends a SUBSCRIBE message to the server for message-summary updates. The server sends a message-summary NOTIFY within the subscription dialog each time the MWI status changes. Unsolicited MWI is a server-related feature.
- **Solicited MWI**: The IP phone can subscribe to the MWI messages to the account or the voice mail number. For solicited MWI, you must enable the MWI subscription feature on the phones.

Set via the Device Interface

See Voice Mail.

Set via the Web User Interface

1. On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **Show Advanced Settings**.



Configuration Parameter

account.X.subscribe_mwi
account.X.subscribe_mwi_expires
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

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 to subscribe 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.sub_fail_retry_interval[1]	Integer from 0 to 3600	30	It configures the interval (in seconds) for the phone to resubscribe when the 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 from subscribing 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	1	It enables or disables the phone to pop up the message when receiving the same number of new voicemails.

[1] X is the account ID.

- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

XML Browser

Introduction

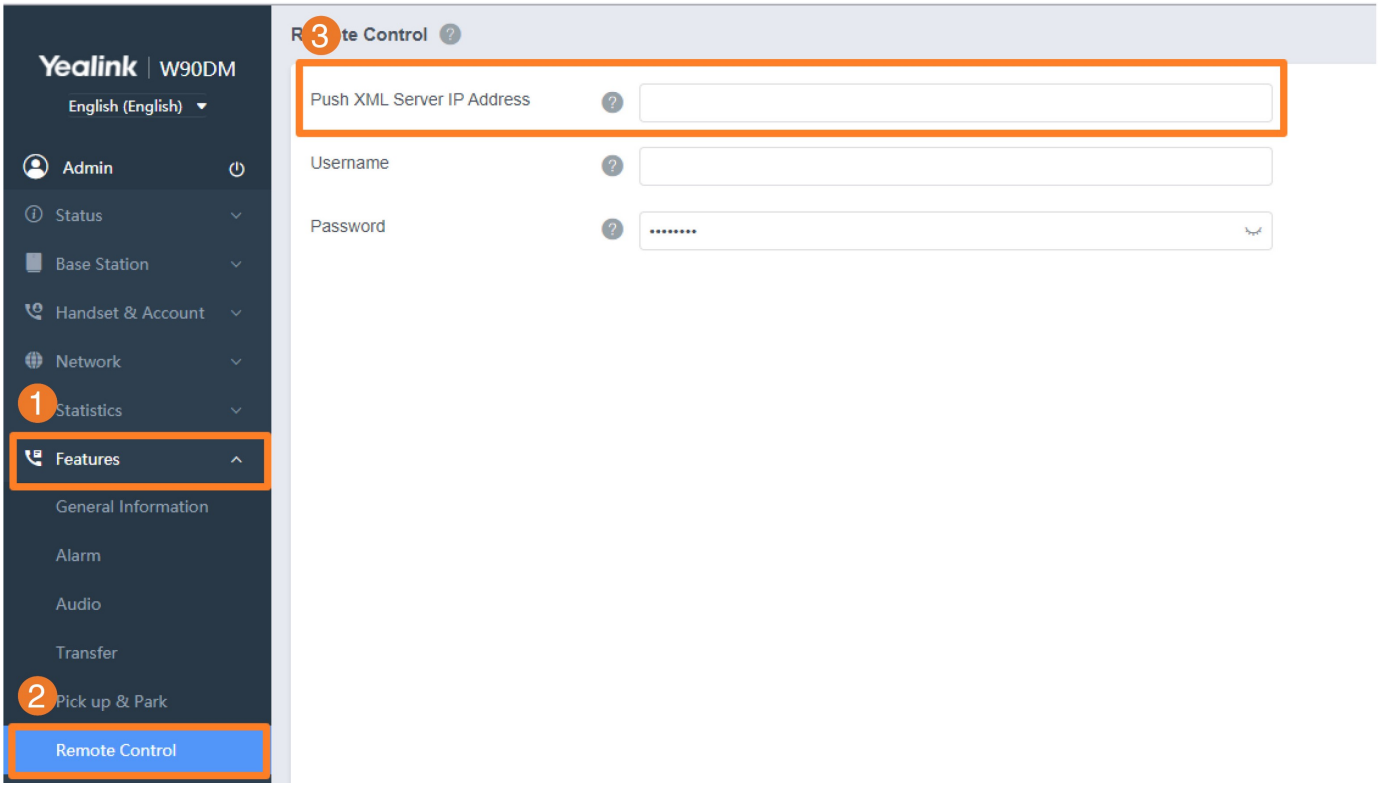
Yealink phones support processing the push XML via SIP NOTIFY message.

The XML browser feature allows users to develop and deploy custom services that meet the user's functional requirements on the server. Users can customize practical applications, such as weather reports, stock information, Google search, news service, etc.

XML Browser Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **Remote Control** > **Push XML Server IP Address**.



Configuration Parameter

```
push_xml.server
push_xml.username
push_xml.password
```

Parame	Permitted Values	Default	Description

ter			
push_xml.server	**Blank**-The phone will reject HTTP POST messages from any server. **any**-The phone will accept HTTP POST messages from any server. **IP address** or **domain name**-Multiple addresses are separated by commas. (for example, 10.1.4.3,10.1.4.23); Support asterisk wildcard, each asterisk represents a field of the IP address (10.10.. represents 10.10.0.0 to 10.10.255.255).	Blank	It configures the address of the push XML server.
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.

Busy Lamp Field

Introduction

The Busy Lamp Field (BLF) feature enables the IP phone to monitor specific remote lines for state changes on the phone.

Yealink phones support two methods of BLF configuration:

- Configure a line key as a BLF key to monitor a specific remote line
- Configure BLF List to monitor a list of specific remote lines

The BLF feature enables the following functions to 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

You can set up to 6 BLF Keys.

Supported Devices

This feature is only applicable to the T54W register on W70B.



State Indicator of Remote Line

LED Status	Icons	Description
Solid green		The monitored line is idle.
Solid red		The monitored line is busy or in a call.
Slowly-flashing red		The monitored line places a call on hold.
Slowly-flashing red		A call is parked to the monitored line.
Off		The monitored line fails to register or does not exist.

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"
entityy="
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.

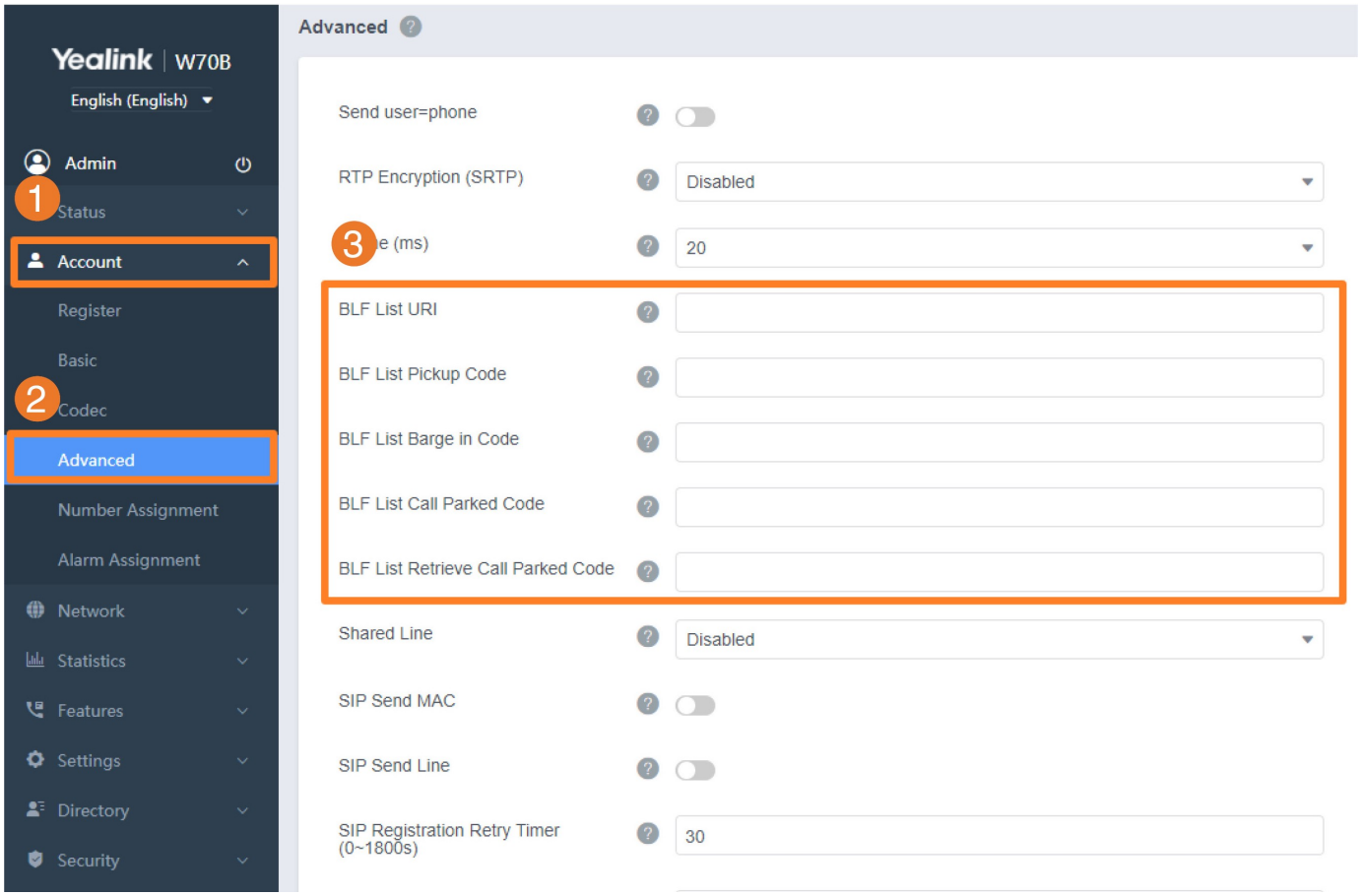
The following example shows a NOTIFY message for a BLF List; the BLF List contains 4605 and 4607:

```
<?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

Set via the Web User Interface

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



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
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_retrieve_call_parked_code

Parameter	Permitted Values	Default	Description
account.X	Integer from 30 to 2147483647	18	It configures the period (in seconds) of the

.blf.subscribe_period[1]		00	BLF subscription.
account.X.blf.subscribe_event[1]	**0**-dialog **1**-presence	0	It configures the event of the BLF subscription.
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.
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 host match feature for BLF/BLF list feature.
sip.terminate_notify_sub_delay_time	Integer greater than 0	0	It configures the interval (in seconds) for the phone to re-subscribe when it receives the NOTIFY message with the subscription state of Terminated. If it is set to 0, the phone will re-subscribe immediately.
sip.sub_refresh_random	**0**-Disabled **1**-Enabled, the phone will generate a random value. The final renewal time equals 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).
account.X.blf.blf_list_uri[1]	String within 256 characters	Blank	It configures the BLF List URI to monitor a list of users for account X.
account.X.blf_list_	String within 32 characters	Blan	It configures the feature access code that initiates a directed call pickup for account

code[1]		k	X.
account.X.blf_list_barge_in_code[1]	String within 32 characters	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.
account.X.blf_list_call_parked_code[1]	String within 32 characters	Blank	It configures the feature access code for the call park for account X. 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 for the monitored user.

[1]X is the account ID. X=1-10.

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.

Visual and Audio Alert for BLF Lines Configuration

Configuration Parameter

```
ddp.X.features.pickup.blf_visual_enable
ddp.X.features.pickup.blf_visual.list
```

ddp.X.features.pickup.blf_audio_enable
ddp.X.features.pickup.blf_audio.list

Parameter	Permitted Values	Default	Description
ddp.X.features.pickup.blf_visual_enable	**0**-Disabled **1**-Enabled	0	It enables or disables the handset to display a visual alert when the monitored user receives an incoming call.
ddp.X.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**: ddp.X.features.pickup.blf_visual.list = any or leave it blank The phone displays a visual alert when any monitored user receives an incoming call. ddp.X.features.pickup.blf_visual.list = 4604,4605 The phone displays a visual alert when the monitored user 4604 or 4605 receives an incoming call. ddp.X.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 "ddp.X.features.pickup.blf_visual_enable" is set to 1 (Enabled).
ddp.X.features.pickup.blf_audio_enable	**0**-Disabled **1**-	0	It enables or disables the handset to play an audio alert when the monitored user receives an incoming call.

	Enabled		
ddp.X.features.pickup.blf_audio.list	• any • Monitored phone number • ListX[1]	any	It configures the monitored users who want to enable the audio alert for BLF pickup feature. Multiple monitored users are separated by commas. **Example**: ddp.X.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. ddp.X.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. ddp.X.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 "ddp.X.features.pickup.blf_visual_enable" is set to 1 (Enabled).

[1]X is the account ID. X=1-10.

Call Information Display Configuration

Configuration Parameter

features.blf.show_callinfo.enable

Parameter	Permitted Values	Default	Description
features.blf.show_callinf	**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, barge in a conference, or	0	It enables or disables the phone to display the call information by long pressing the BLF/BLF List key.

o.enable	retrieve the parked call.		

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.

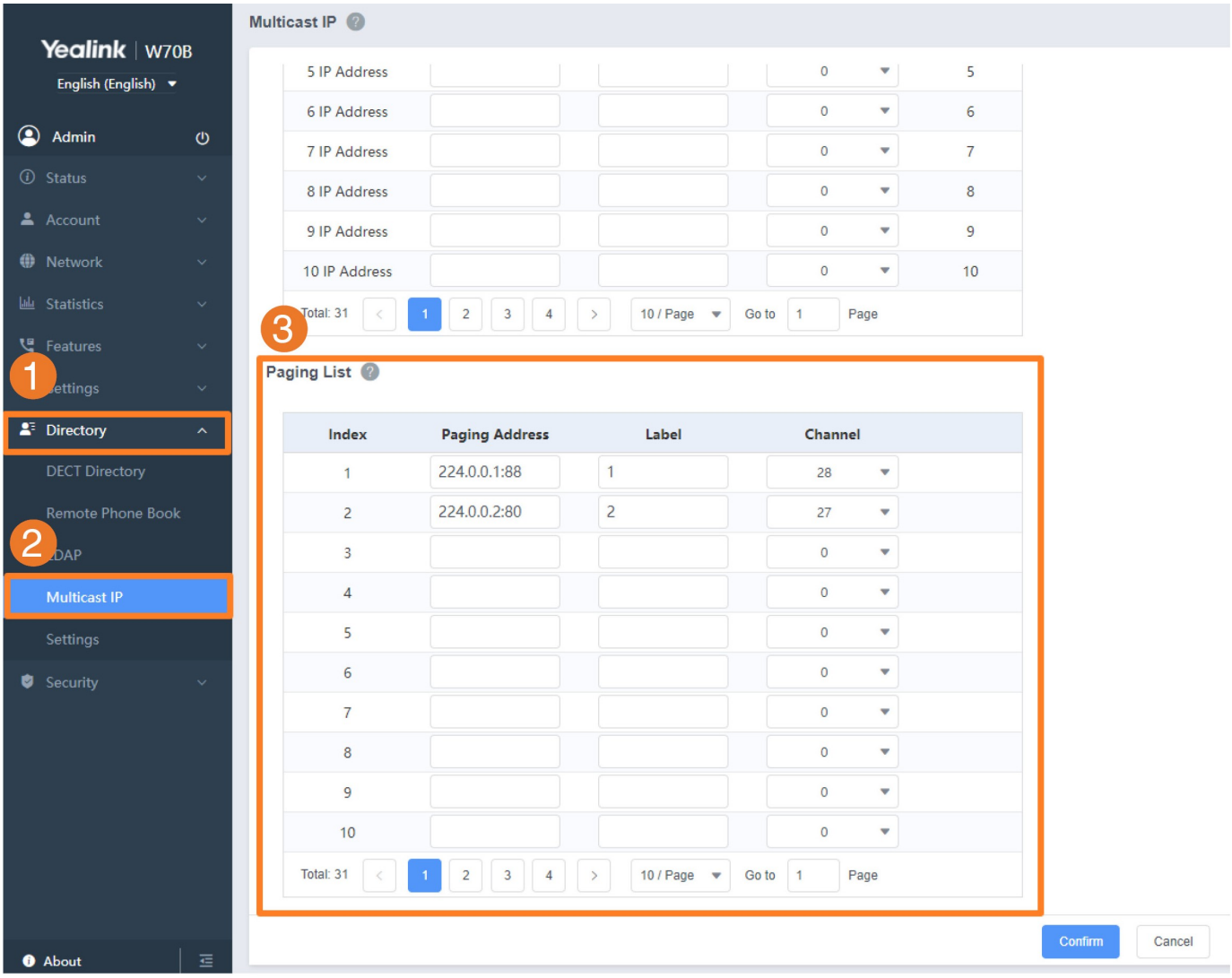
> All phones in the multicast paging group must be deployed in the same subnet since a broadcast is used. The phone can only send/receive broadcasts to/from the listened channels. Other channels' broadcasts will be ignored automatically by the IP phone.

Multicast Paging Group Configuration

Yealink phones support up to 31 groups for paging. You can assign a multicast IP address with a channel for each group, and specify a label to each group to identify the phones in the group, such as All, Sales, or HR.

Set via the Web User Interface

1. On the web user interface, go to **Directory** > **Multicast IP** > **Paging List**.



Configuration Parameter

multicast.paging_address.X.ip_address
multicast.paging_address.X.label
multicast.paging_address.X.channel

Parameter	Permitted Values	Default	Description
multicast.paging_address.X.ip_address[1]	IP address: port (224.0.0.1-239.255.255.255 port: 0-65535)	Blank	It configures the IP address and port number of the multicast paging group in the paging list.
multicast.paging_address	String	Blan	It configures the name of the multicast paging group to be

.X.label[1]		k	displayed in the paging list. It will be displayed on the phone screen when placing the multicast paging calls.
multicast.paging_address.X.channel[1]	**0**-all the Yealink phones running old firmware version or Yealink phones listen to channel 0 or thirdparty available devices in the paging group can receive the RTP stream. **1 to 25**-the Polycom or Yealink phones preconfigured to listen to the channel can receive the RTP stream. **26 to 30**-the Yealink phones preconfigured to listen to the channel can receive the RTP stream.	0	It configures the channel of the multicast paging group in the paging list.

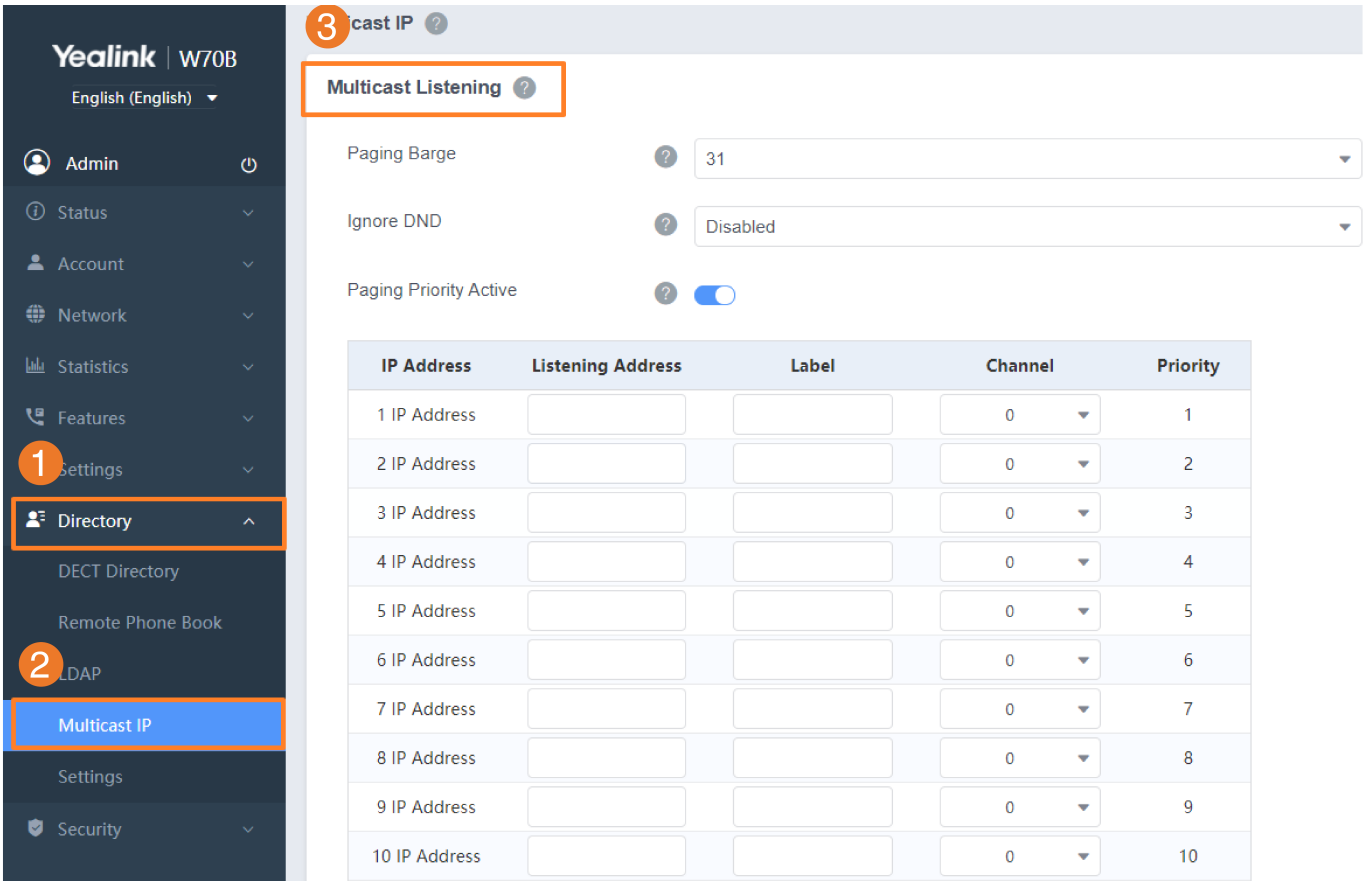
[1]X ranges from 1 to 31.

Multicast Listening Group Configuration

Yealink phones support up to 31 groups for listening. You can assign 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

2. On the web user interface, go to **Directory** > **Multicast IP** > **Multicast Listening**.



Configuration Parameter

```
multicast.listen_address.X.ip_address
multicast.listen_address.X.label
multicast.listen_address.X.channel
```

Parameter	Permitted Values	Default	Description
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	String within 99 characters	Blank	It configures the label to be displayed on the phone screen when receiving the multicast

l[1]			paging calls.
multicast.listen_address.X.channel[1]	**0**-the phone can receive an RTP stream of the pre-configured multicast address from the phones running old firmware version, from the phones listening to the channel 0, or from the available third-party devices. **1 to 25**-the phone can receive an RTP stream of the pre-configured multicast address on the channels 1 to 25 respectively from Yealink or Polycom phones. **26 to 30**-the phone can receive the RTP stream of the pre-configured multicast address on the channels 26 to 30 respectively from Yealink phones.	0	It configures the channel that the phone listens to.

[1]X ranges from 1 to 31.

Multicast Paging Settings

You can configure some general settings for multicast paging, for example, specify a codec, 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 determine 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 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 determine whether a new incoming paging call interrupts a current paging call.

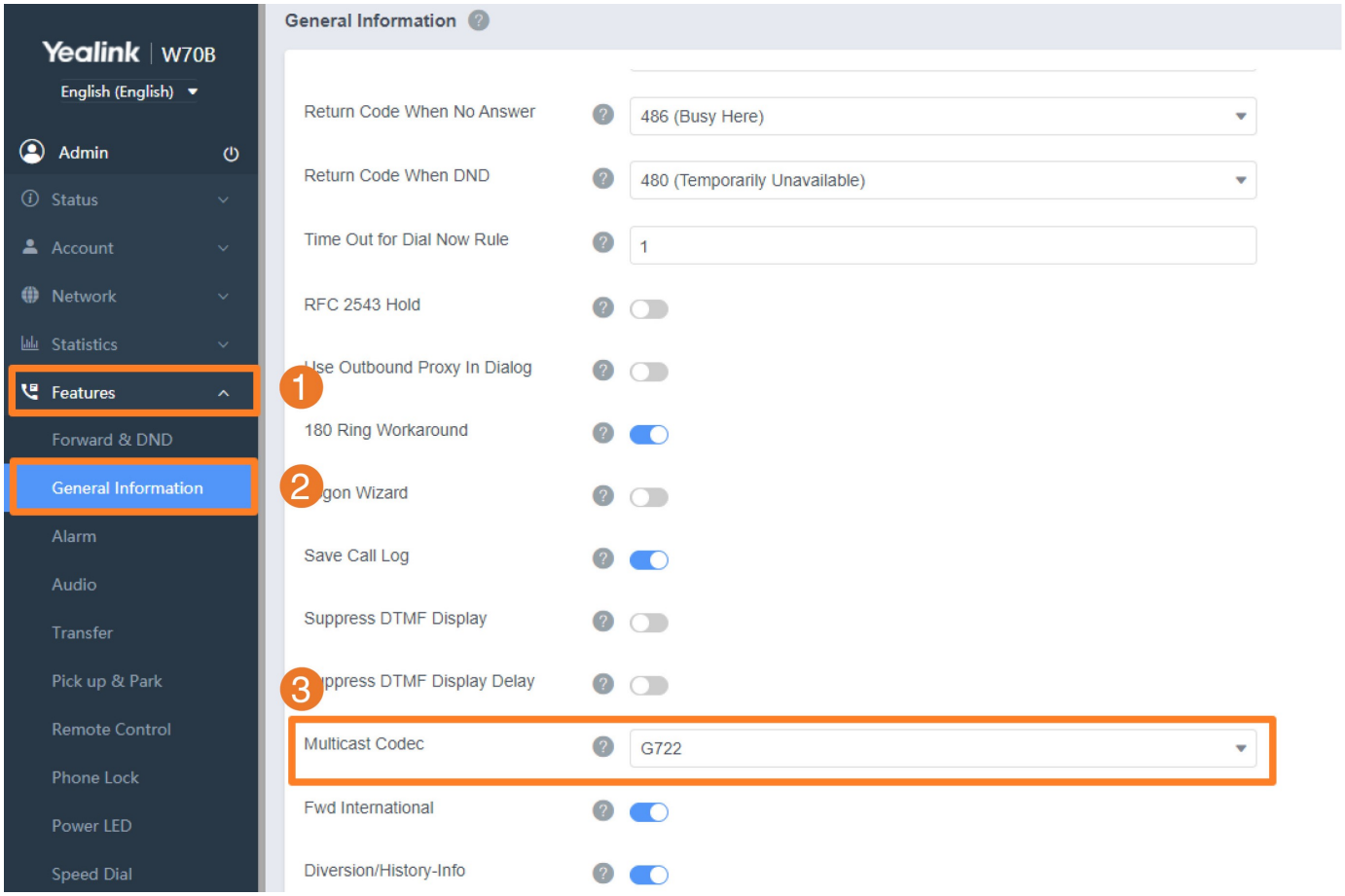
The **Paging Priority** feature decides how the phone handles incoming paging calls when there is

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.

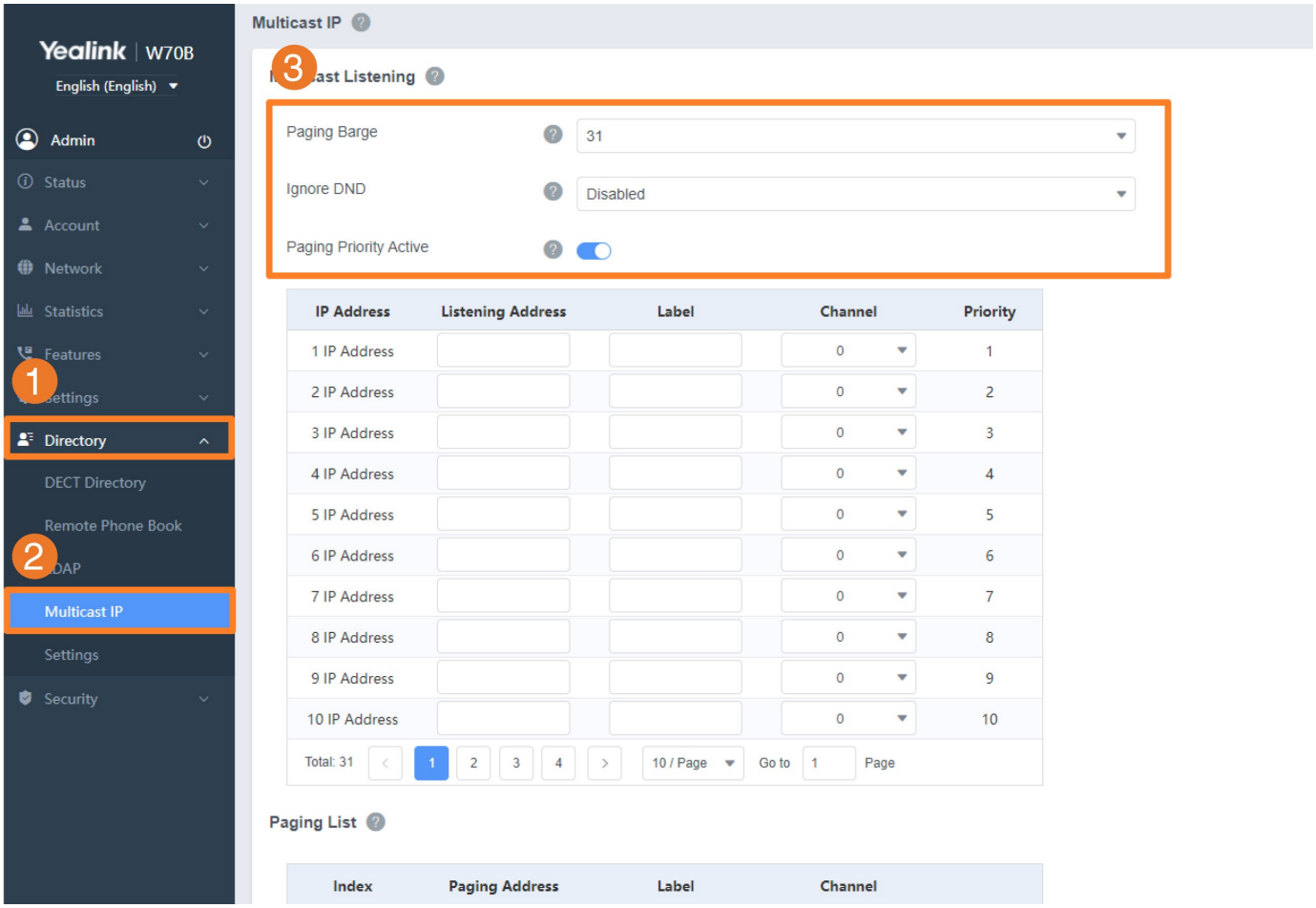
Multicast Paging Settings Configuration

Set via the Web User Interface

3. On the web user interface, go to **Features** > **General Information** > **Multicast Codec**.



4. On the web user interface, go to **Directory** > **Multicast IP**.



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

Parameter	Permitted Values	Default	Description
multicast.codec	PCMU, PCMA, G729, G722	G722	It configures the codec for multicast paging.
mult	**0**-Disabled, the phone will ignore the	1	It enables or disables the phone to handle

icast.receive_priority.enable	incoming multicast paging calls when there is an active multicast paging call on the phone. **1**-Enabled, the phone will receive the incoming multicast paging call with a higher priority and ignore the one with a lower priority.		the incoming multicast paging calls when there is an active multicast paging call on the phone.
multicast.receive_priority.priority	**0**-Disabled, all incoming multicast paging calls will be automatically ignored when a voice call is in progress. **1**-1 **2**-2 **3**-3 … **31**-31 If it is set to other values, the phone will receive the incoming multicast paging call with a higher or equal priority and ignore the one with a lower priority when a voice call is in progress.	31	It configures the priority of the voice call (a normal phone call rather than a multicast paging call) in progress. 1 is the highest priority, 31 is the lowest priority.
multicast.receive.ignore_dnd.priority	**0**-Disabled, all incoming multicast paging calls will be automatically ignored when DND is activated in phone mode. **1**-1 **2**-2 **3**-3 … **31**-31 If it is not set to 0 (Disabled), the phone will receive the incoming multicast paging call with a higher or	0	It configures the lowest priority of the multicast paging call that can be received when DND is activated in phone mode. 1 is the highest priority, 31 is the lowest priority.

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

[1]X ranges from 1 to 31.

IP Address Call

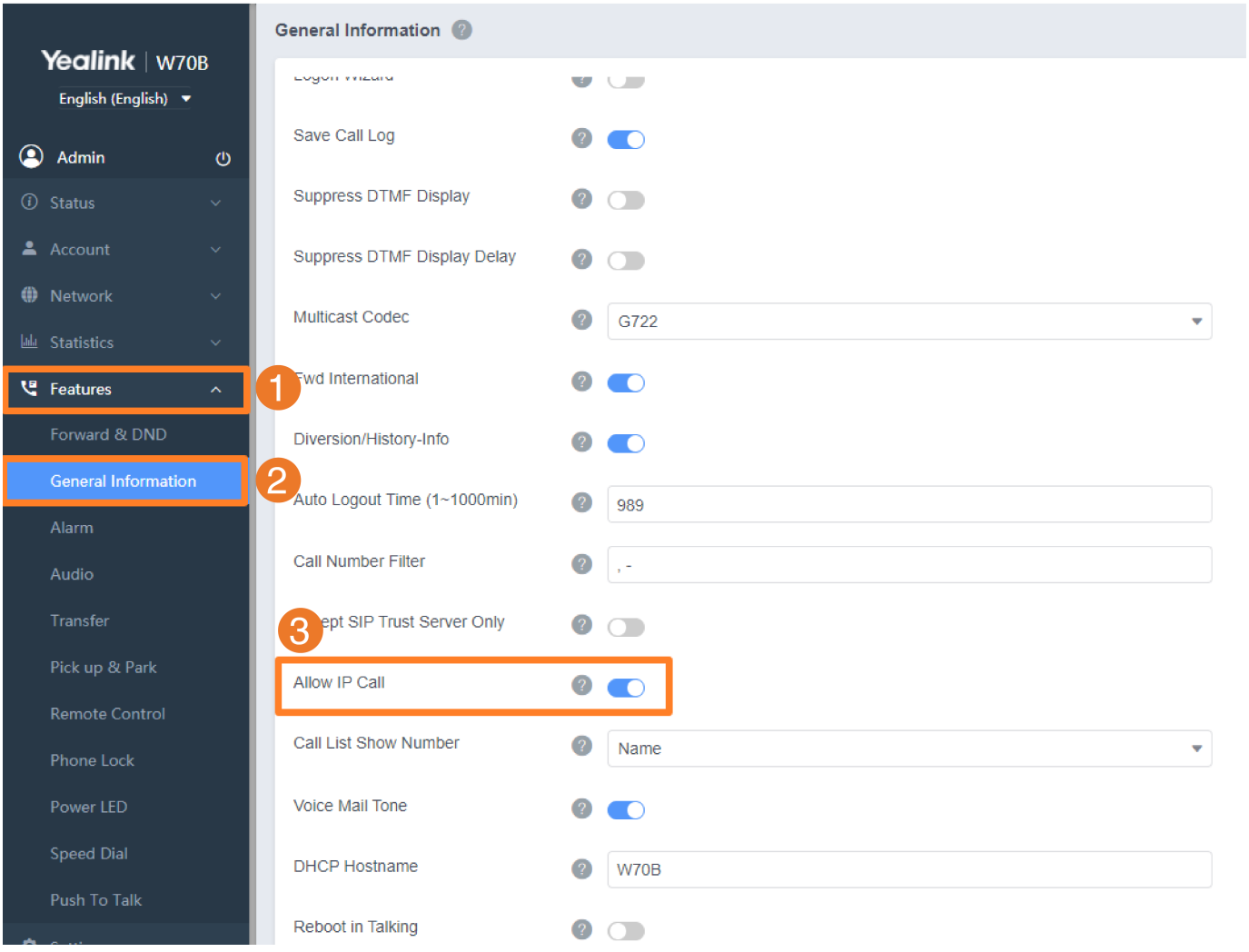
Introduction

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

1. On the web user interface, go to **Features** > **General Information** > **Allow IP Call**.



Configuration Parameter

features.direct_ip_call_enable

Parameter	Permitted Values	Default	Description
features.direct_ip_call_enable	**0**-Disabled **1**-Enabled	1	It enables or disables allowing IP address calls. If you want to receive an IP address call, make sure sip.trust_ctrl is set to 0 (Disabled).

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 SUBSCRIBE or NOTIFY request should be validated. If it is left blank, all events will be validated.

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 a graphical tool for the Windows platform)
- Config_Encrypt.exe (via DOS command line for the 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).

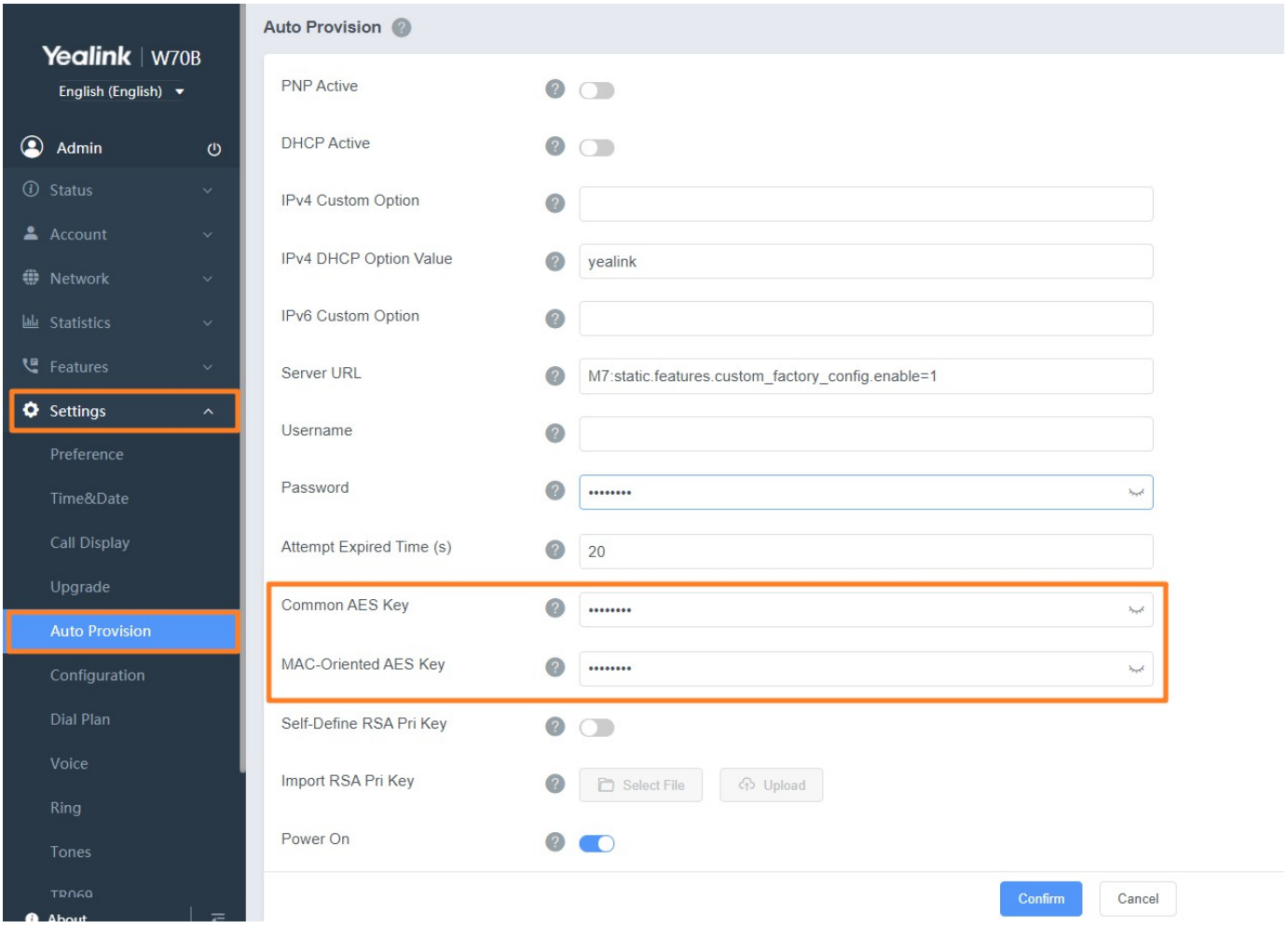
You can encrypt the configuration files using encryption tools. You can also configure the <MAC>-local.cfg files to be automatically encrypted using 16-character symmetric keys when uploading to the server (by setting "static. auto_provision.encryption.config" to 1).

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 the <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 the account.cfg file using key2. After decryption, the phone resolves configuration files and updates configuration settings on 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

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_k	**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.

ey_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][3]	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][3]	16 characters	Blank	It configures the plaintext AES key for decrypting the MAC-Oriented CFG file. If it is configured, it has a higher priority than the value configured by the parameter "static.auto_provision.aes_key_16.mac".

static.auto_provision.encryption.config	**0**-Disabled, the MAC-local CFG file will be uploaded unencrypted and will replace the one (encrypted or unencrypted) stored on the server if you have configured to back up the MAC-local CFG file to the server by the parameter static.auto_provision.custom.sync. **1**-Enabled, the MAC-local CFG file will be uploaded encrypted and will replace the one (encrypted or unencrypted) stored on the server if you have configured to back up the MAC-local CFG file to the server by the parameter static.auto_provision.custom.sync. The plaintext AES key is configured by the parameter static.auto_provision.aes_key.mac.	0	It enables or disables the phone to encrypt <MAC>-local.cfg file using the plaintext AES key.
static.auto_provision.rsa_pri_key.url	URL within 511 characters	Blank	It configures the URL to import the self-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	**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 the self-defined RSA private key.	0	It enables or disables the self-defined RSA private key.

.rs a_p ri_ key .en abl e[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.
[3]This parameter is only applicable to W70B.

Example: Encrypting Configuration Files

The following example describes how to use "Config_Encrypt_Tool.exe" to encrypt the account.cfg file.

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.

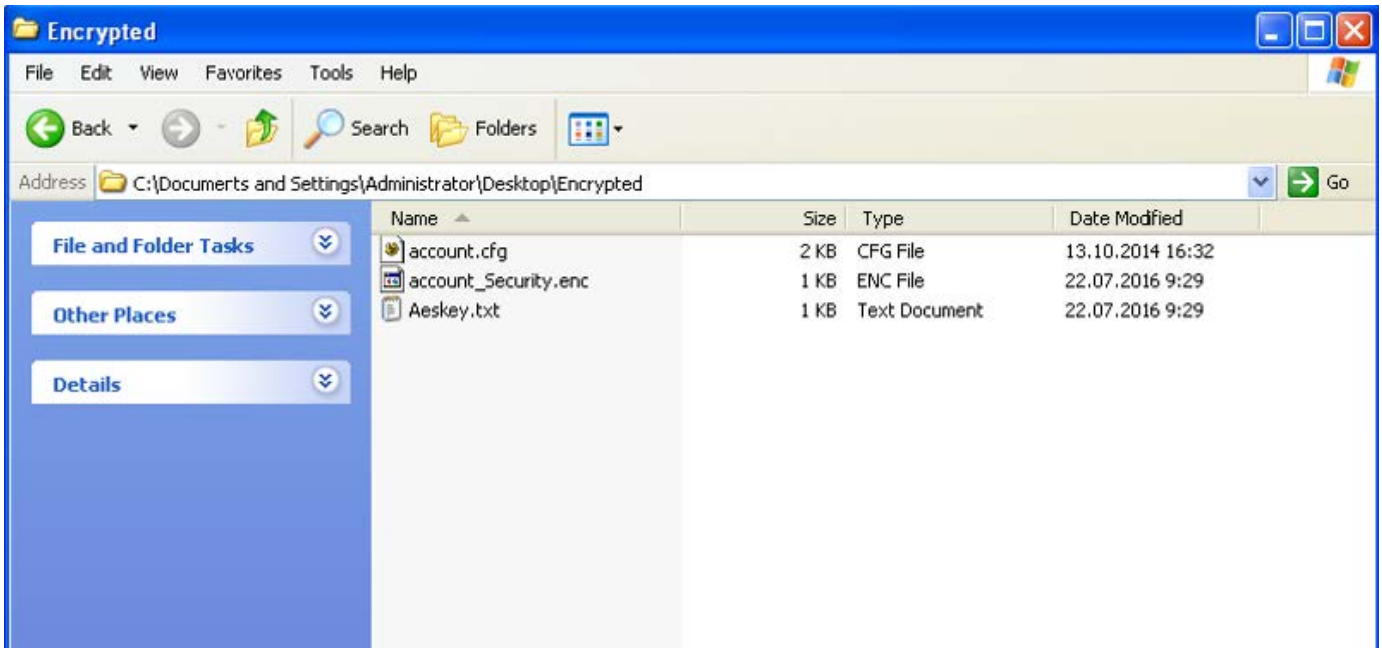
If you select the **Auto Generate** radio box, the configuration file(s) will be encrypted using a random AES key.

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).



Simple Certificate Enrollment Protocol (SCEP)

SCEP is an industry-standard protocol and technology. It mainly issues certificates for devices through the internal CA of the enterprise, which can provide digital certificates for devices 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.stat	String within 64 characters	Blank	It configures the state/province name used to generate the CSR.

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

Secure Real-Time Transport Protocol (SRTP)

Introduction

Secure Real-Time Transport Protocol (SRTP) encrypts the audio streams during VoIP phone calls to avoid interception and eavesdropping. The parties participating in the call must enable the SRTP feature simultaneously. When this feature is enabled on both phones, the type of encryption to use for the session is negotiated between the phones. This negotiation process is compliant with RFC 4568.

When you place a call on the enabled SRTP phone, the phone sends an INVITE message with the RTP/RTCP encryption algorithm to the destination phone. As described in RFC 3711, RTP/RTCP streams may be encrypted using an AES (Advanced Encryption Standard) algorithm.

Example of the RTP encryption algorithm carried in the SDP of the INVITE message:

```
m=audio 11780 RTP/SAVP 0 8 18 9 101
a=crypto:1 AES_CM_128_HMAC_SHA1_80 >
inline:NzFlNTUwZDk2OGVlOTc3YzNkYTkwZWVkMTM1YWFj
a=crypto:2 AES_CM_128_HMAC_SHA1_32 >
inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWFm
a=crypto:3 F8_128_HMAC_SHA1_80
inline:NDliMWIzZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:9 G722/8000
a=fmtp:101 0-15
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

The callee receives the INVITE message with the RTP encryption algorithm and then answers the call by responding with a 200 OK message, which carries the negotiated RTP encryption algorithm.

Example of the RTP encryption algorithm carried in the SDP of the 200 OK message:

```
m=audio 11780 RTP/SAVP 0 101
```

```
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:NGY4OGViMDYzZjQzYTNiOTNkOWRiYzRlMjM0Yzcz
a=sendrecv
a=ptime:20
a=fmtp:101 0-15
```

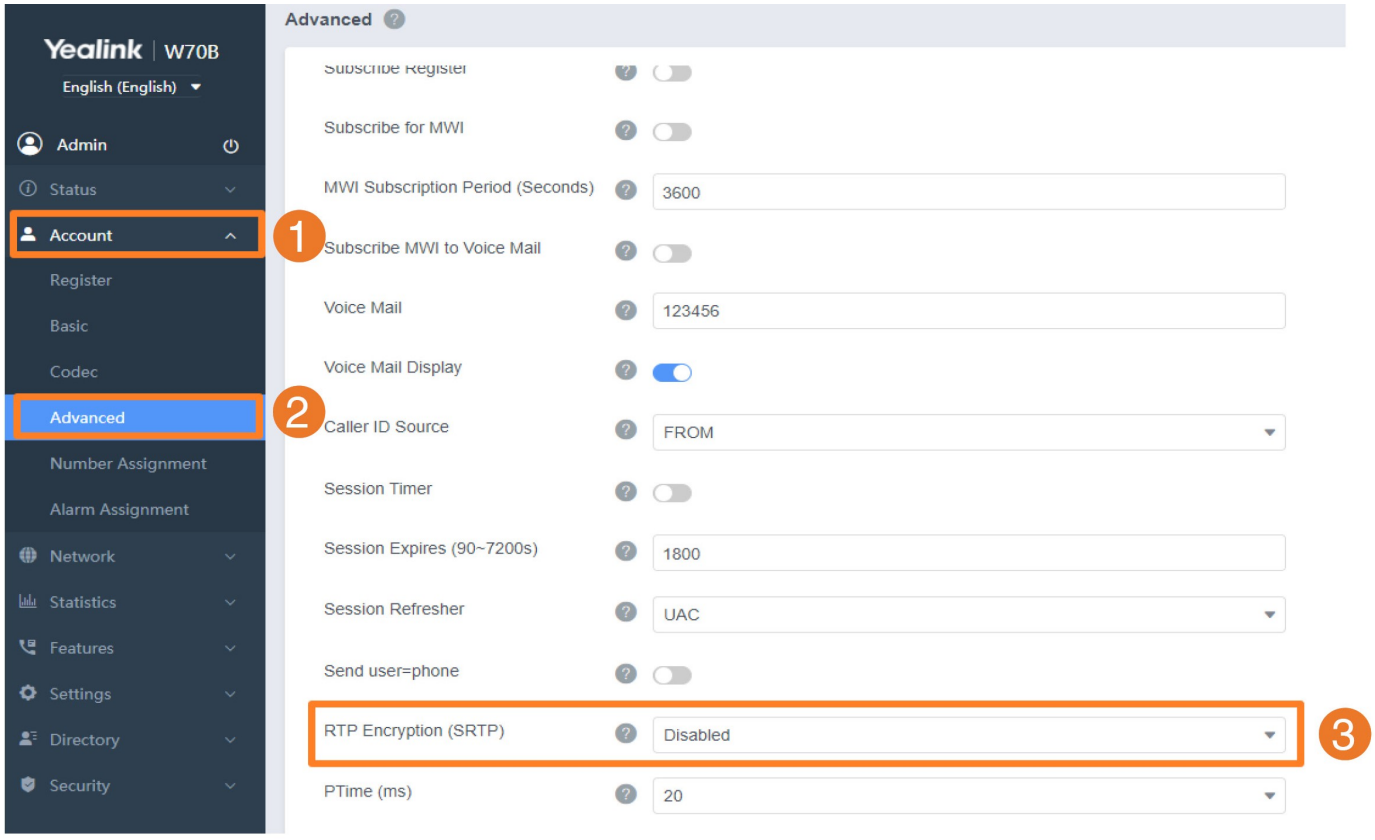
When SRTP is enabled on both phones, RTP streams will be encrypted, and a lock icon will appear on the LCD screen of each IP phone after a successful negotiation.

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).

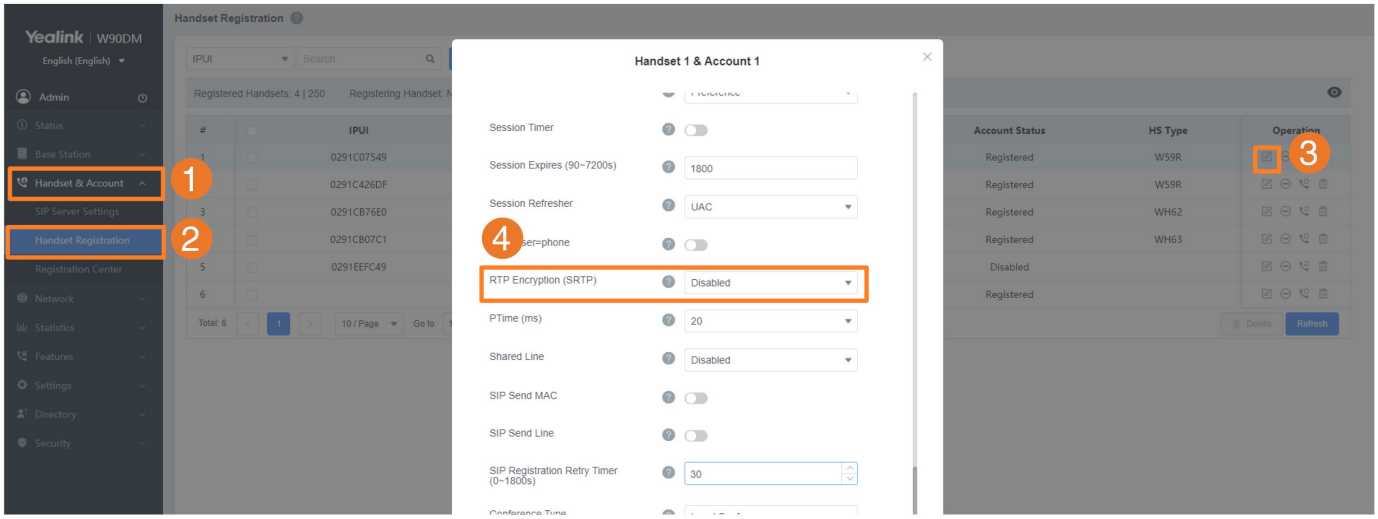
SRTP Configuration

Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Advanced** > **RTP Encryption (SRTP)**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **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 an audio encryption service.
account.X.srtp.cipher_list	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.

Transport Layer Security (TLS)

Introduction

TLS is a commonly used protocol for providing communications privacy and managing the security of message transmission, allowing the phones to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent the data from being eavesdropped and tampered.

Yealink phones support TLS version 1.2. When TLS is enabled for an account, the SIP message of this account will be encrypted, and a lock icon will appear on the LCD screen after the successful TLS negotiation.

Supported Cipher Suites

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

Yealink phones support the following cipher suites:

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

- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- DES-CBC-MD5
- EXP1024-DHE-DSS-RC4-SHA
- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC2-CBC-MD5
- EXP-RC4-MD5

Supported Trusted and Server Certificates

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

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

Security Certificates	Description
Trusted Certificate	When the IP phone requests a TLS connection with a server, the phone should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. You can upload 10 custom certificates at most. The format of the trusted certificate files must be .pem, .cer, *.crt, and *.der, and the maximum file size is 5MB.
Ser	When clients request a TLS connection with the IP phone, the phone sends the server

server 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 .cer, and the maximum file size is 5MB.
A unique server certificate	It is unique to an IP phone (based on the MAC address) and issued by the Yealink Certificate Authority (CA).
A generic server certificate	It is issued by the Yealink Certificate Authority (CA). Only if no unique certificate exists, the phone sends a generic certificate for authentication.

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

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

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

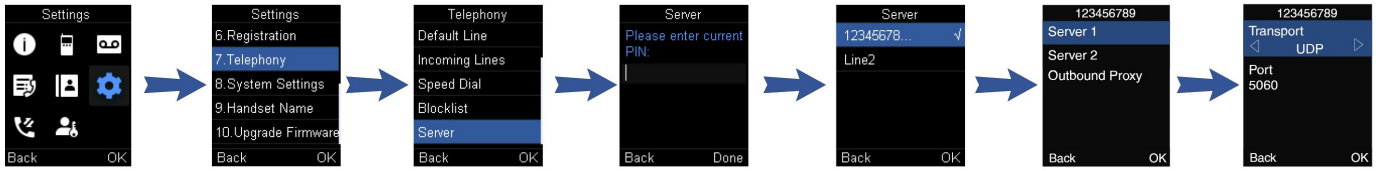
Yealink endeavors to maintain a built-in list of the most commonly used CA Certificates. Due to memory constraints, we cannot ensure a complete set of certificates. If you are using a certificate from a commercial Certificate Authority not in the list above, please take your certificate to create a Yealink ticket for further support. You can now upload your particular CA certificate to your phone.

TLS Configuration

Set via the Device Interface (W70B)

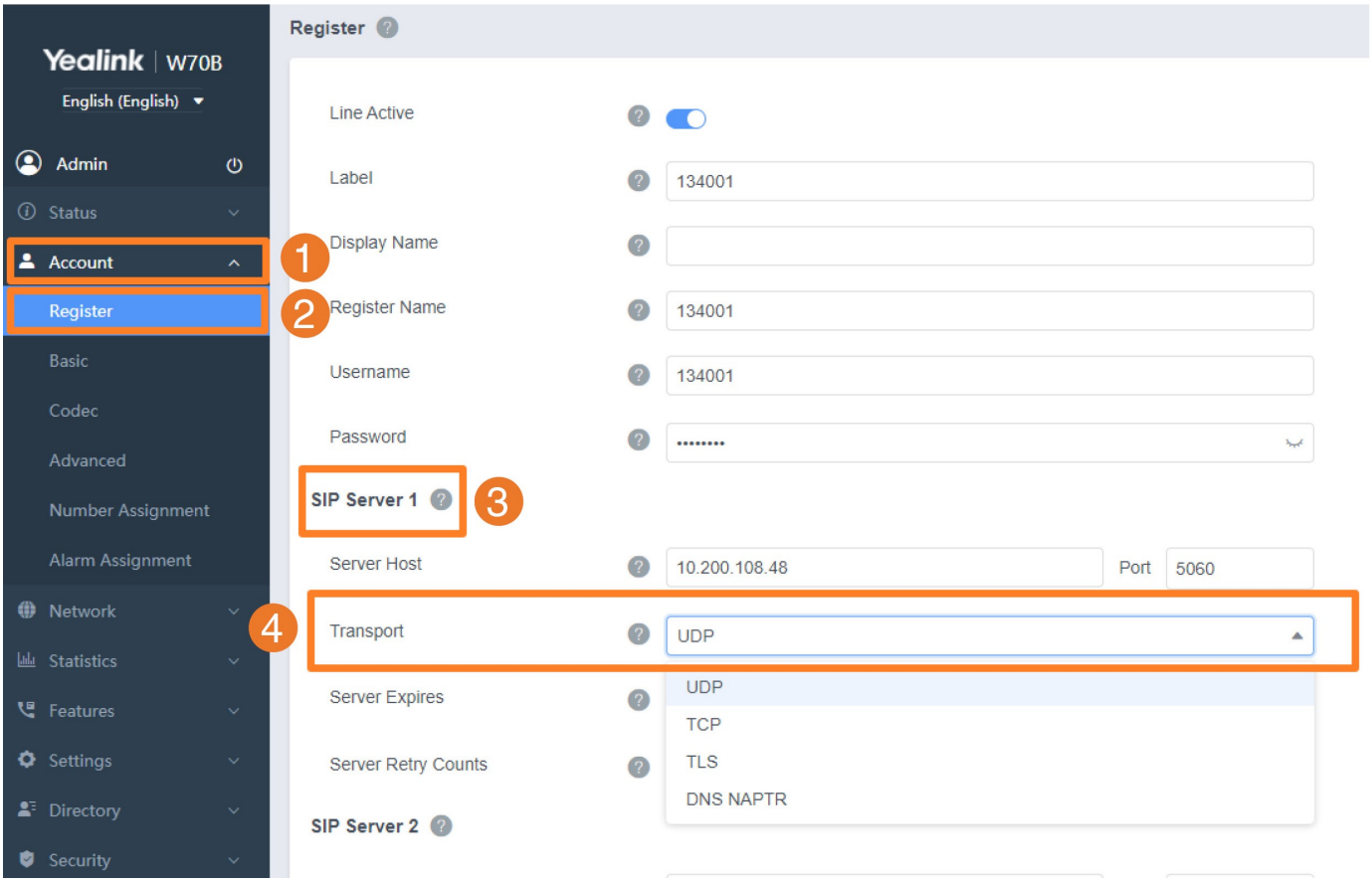
W53H/W56H/W57R/W59R/W59R Pro/W71H/W73H/W74H/W78H:

OK > **Settings** > **Telephony** > **Server** (default PIN: 0000) >**Line X** > **Server Y** > **Transport**

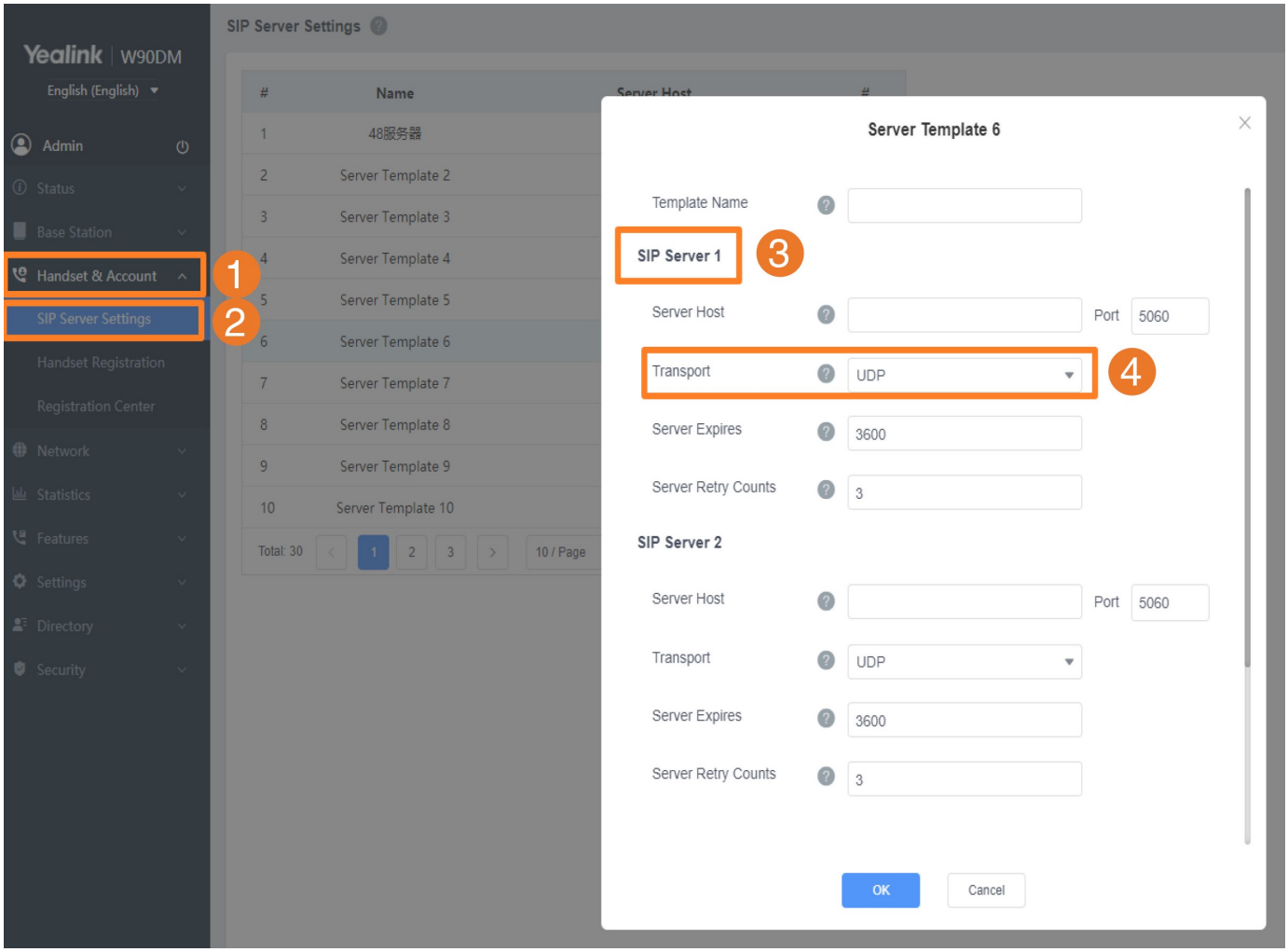


Set via the Web User Interface

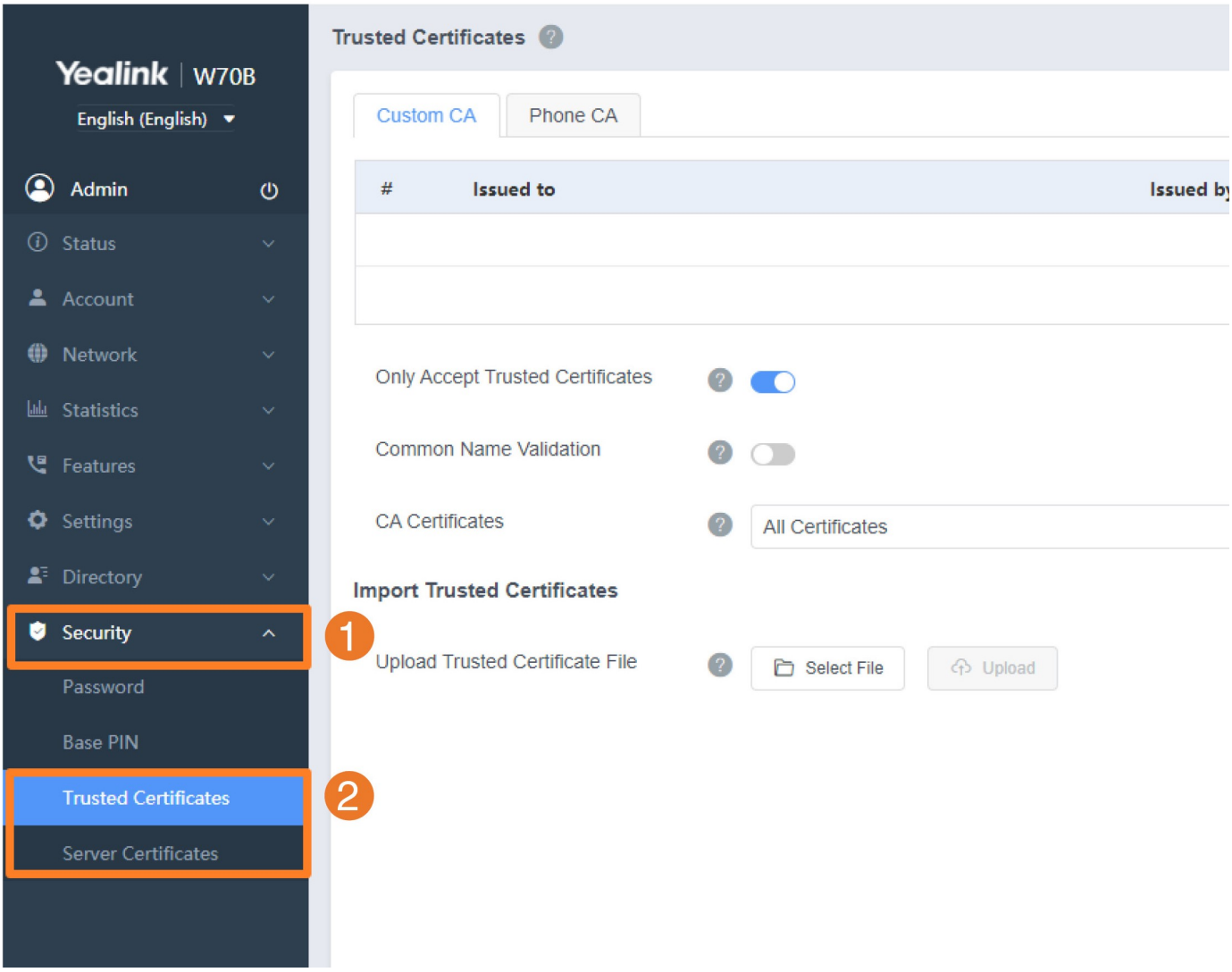
1. For W70B: On the web user interface, go to **Account** > **Register** > **SIP Server Y** > **Transport**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** > **SIP Server Settings** > **Edit** > **SIP Server Y[2]** > **Transport**.



3. On the web user interface, go to **Security** > **Trusted Certificates**/**Server Certificates**.



Configuration Parameter

account.X.sip_server.Y.transport_type
template.X.sip_server.Y.transport_type
static.security.default_ssl_method
static.security.server_ssl_method
static.security.trust_certificates
static.security.sip.ssl_method
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
static.security.e911.ca_cert
static.security.e911.dev_cert
static.security.e911.cn_validation
static.security.e911.trust_certificates

Parameter	Permitted Values	Default	Description
account.X.sip_server.Y.transport_type[1] [2] template.X.sip_server.Y.transport_type[1] [2]	**0**-UDP **1**-TCP **2**-TLS **3**-DNS NAPTR, if no server port is given, the phone performs the DNS NAPTR and SRV queries for the service type and port.	0	It configures the type of transport protocol.
static.security.default_ssl_method	**0**-TLS 1.0 **3**-SSL V23 (automatic negotiation with the server. The phone starts with TLS1.2 for negotiation.) **4**-TLS 1.1 **5**-TLS 1.2 **6**-TLS 1.3	5	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_certi	**0**-Disabled **1**-Enabled, the phone will authenticate the server certificate based on the trusted	1	It enables or disables the phone to only trust the server certificates in the Trusted

ficates	certificates list. Only when the authentication succeeds will the phone trust the server.		Certificates list.
static.security.sip.ssl_method	**0**-TLS 1.0 **3**-SSL V23 (automatic negotiation with the server. The phone starts with TLS1.2 for negotiation.) **4**-TLS 1.1 **5**-TLS 1.2 **6**-TLS 1.3	5	It configures the TLS version for the SIP module.
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	http://localhost/all: It deletes all uploaded trusted certificates.	Blank	It configures to delete all uploaded trusted certificates.

.delete			
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.
static.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.
static.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.
static.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.
static.security.e9	**0**-Disabled **1**-Enabled, the desired module will	Blan	It enables or disables the desired module to only trust

11.trust_certificates	authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds will the desired module trust the server.	k	the server certificates in the Trusted Certificates list.

[1]X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

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

AML-Report to the Server

Report Device Status to the Server

Introduction

From version V87 onwards, DECT devices support two device status reporting modes: status change-triggered reporting and automatic periodic reporting.

Distinction of reporting scenarios:

1. Periodic reporting and status change reporting are only available for data synchronization with the Yealink YMCS platform.
2. For third-party platforms: The device only supports handset status reporting triggered by alarms. Regular periodic reporting and status change reporting are not supported.

Supported Values List

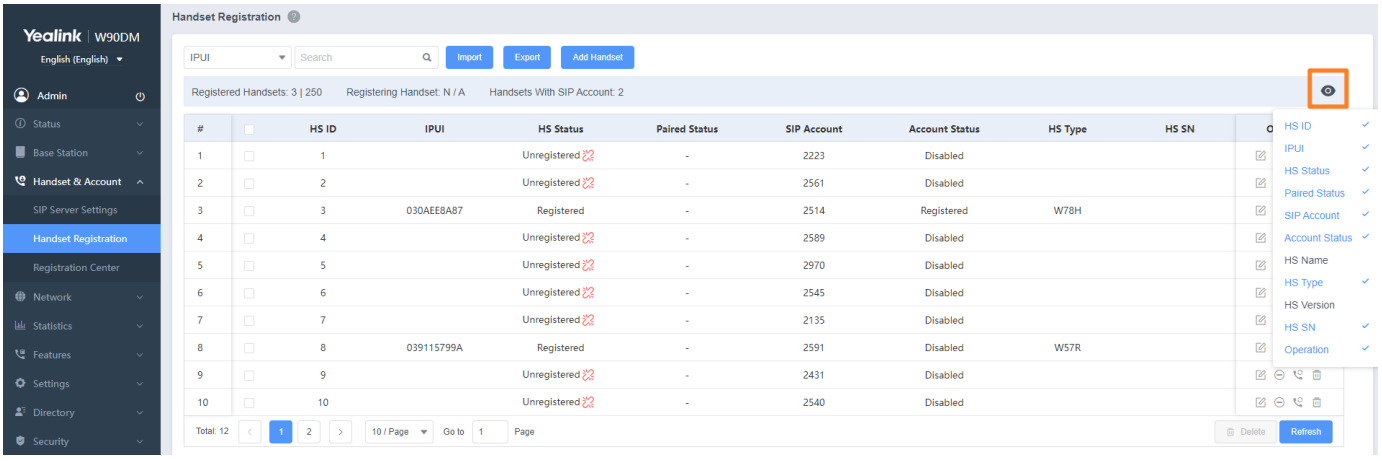
	Value	Description
Base	$bsmac	Base's MAC address
	$bsstatus	Base's synchronization status, optional values are: • active and synced • active • deactive - Base is not active • offline
Handset Basic Information	$ipui	Handset's IPUI
	$sip_id	Handset's default account
	$handset_number	Handset number under the Base
	$hs_model	Handset's model
	$hs_sn	Device's SN Only applicable to the headset.
Handset Status	$hs_online	Handset's online status, optional values are: • **0** - Offline

Information		• **1** - Online
	$signal	Handset's signal status, optional values are: 0, 1, 2, 3, 4, 5
	$battery	Handset's battery status, optional values are: • 0 = 5% • 1 = 20% • 2 = 40% • 3 = 60% • 4 = 80% • 5 = 100%
	$charging	Handset's charging status, optional values are: • **0** - Not charging • **1** - Charging
	$hs_upgrade	Handset's upgrade status, optional values are: • idle - Not upgrading • upgrade - Upgrading

Configuration

Set via the Web User Interface

On the web user interface, go to **Handset & Account** > **Handset Registration** > .



Configuration Parameter

alarm.x.report.mode

phone_setting.base_auto_obtain.enable

features_base.auto_send_ymcs.enable

Parameter	Permitted Values	Default	Description
alarm.x.report.mode	**0**-Outgoing call **1**-Only report alarm information to the server via the Action URL **2**-Only report alarm info to server via "alarm.report_to_server.url"	0	It configures the event alarm reporting method.
phone_setting.base_auto_obtain.enable	**0**-Disabled **1**-Enabled; actively obtain status information from the Handset (HS) every 30 minutes.	0	It configures to enable the base to actively obtain status information from the HS (Handset) to YMCS.
features_base.auto_send_ymcs.enable	**0**-Disabled **1**-Enabled	0	It configures to enable the Base to report handset/base status information to YMCS. The reporting mechanism is triggered by any change in the information.

Report Alarm to the Server

When administrators set "alarm.X.report.mode=2", the device will push handset status data to the configured server independently.

Field	Description
sip-id	The default SIP account of the handset. Default value: None
hs_model	Handset hardware model, e.g., W57R, W73H, W59R
ipui	Unique IPUI identifier of the handset
signal	Current signal strength of the handset

battery_level	Remaining battery capacity of the handset
alarm_type	Triggered alarm event type. Optional values: None / Button / ManDown / NoMovement / Running, consistent with the options of parameter "alarm.x.type"
handset_number	Index number of the handset registered to the base station, used to identify which handset triggers the alarm

```
{
"event":"alarm",
"hs_id":1,
"ipui":"0291C075AA",
"sipid":"127",
"model":"W59R",
"alarm_type":"Button",
"signal":5,
"battery":5
}
```

Report Heartbeat to Server

This heartbeat feature allows third-party monitoring platforms to query the running status of DECT multi-base station clusters.

Mandatory Pre-configuration

Complete the following parameters before using heartbeat reporting:

```
features.action_uri.enable = 1
action_url.show_msgbox = 0
features.action_uri_limit_ip = any
```

Configuration Parameter

```
alarm.report_to_server.url
```

alarm.report_to_server.username
alarm.report_to_server.password

Parameter	Permitted Values	Default	Description
alarm.report_to_server.url	URL within 512 characters	Blank	It configures the server address for reporting alarm information in the alarm function.
alarm.report_to_server.username	String within 512 characters	Blank	It configures the authentication account for the server used to report alarm information in the alarm function.
alarm.report_to_server.password	String within 512 characters	Blank	It configures the authentication password for the server used to report alarm information in the alarm function.

Action URI Request Format

https://<DM_IP>/servlet?bsstatus=get&bsmac=<Base_MAC>

AML-Location

Introduction

The Location Reporting feature is designed to upload the location information of the base station (Base) connected to a handset to the server in real time whenever an alarm event occurs. This helps administrators quickly locate the person who triggered the alarm and improves emergency response efficiency. This feature supports two implementation methods: Handset-Initiated Reporting and Server-Initiated Search.

Before You Begin

It is only applicable to W71H, W73H, W74H, W78H, W53H, W56H, W57R, W59R, and W59R Pro.

Handset-Initiated Reporting

Introduction

When the handset triggers an alarm (such as pressing an emergency button or a fall detection alarm, etc), the handset sends a GET request to the specified Action URL on the server, including the MAC address of the connected base station. The server can then determine the area where the alarm was triggered based on this information.

Configuration Parameter

action_url.alarm_call_established
action_url.alarm_call_outgoing
action_url.alarm.trigger
alarm.X.report.mode
alarm.x.report_location.enable

Parameter	Permitted Values	Default	Description
action_url.alarm_call_established	URL within 511 characters	Blank	It reports the Action URL when the alarm call is successfully established on the handset.
action_url.a	URL within 511 characters	Bl	It reports the Action URL when the alarm

larm_call_outgoing		ank	call is successfully outgoing on the handset.
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.X.report.mode	**0**-Outgoing call **1**-Only report alarm information to the server via the Action URL **2**-Only report alarm info to server via alarm.report_to_server.url	0	It configures the event alarm reporting method.
alarm.x.report_location.enable	**0**-Disabled **1**-Enabled	0	It configures whether to report the current handset position when event alarms are configured.

Scenario Example

Scenario Overview

This scenario illustrates how the handset reports its location to the server after an alarm is triggered.

When the alarm location reporting feature is enabled, and the reporting server is properly configured, the handset will:

1. Report the alarm event to the server
2. Wait for a short interval
3. Report its location information
4. Return to the idle state after user confirmation

Preconditions

Before this scenario can occur, the following conditions must be met:

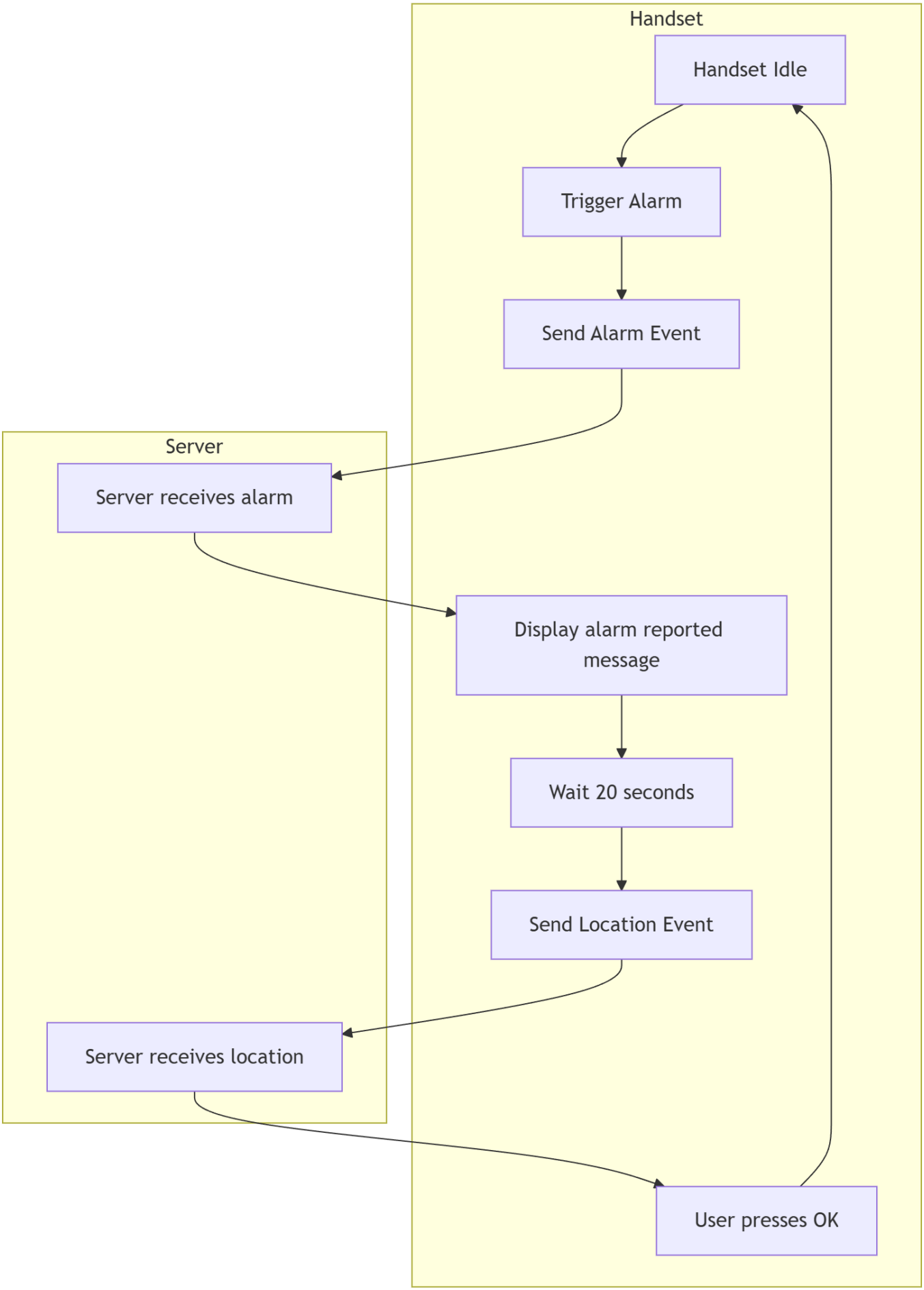
- The handset is successfully registered and synchronized with the Base (DM status: Active & Synced)
- The alarm type (e.g. Button, Man Down, No Movement, Running) is configured and enabled
- Alarm location reporting is enabled: alarm.X.report_location.enable = 1
- The alarm reporting server URL is configured: alarm.report_to_server.url = http://<server-address>

Scenario Flow Description

Step-by-step Behavior

1. The handset is in the **Idle** state.
2. The user triggers an alarm (for example, by pressing the emergency button).
3. The handset sends an **alarm event** to the configured server.
4. The handset displays a confirmation message indicating that the alarm has been reported successfully.
5. After a short delay (approximately 20 seconds), the handset sends a **location event** to the server.
6. The user presses the **OK** button to acknowledge the alarm.
7. The handset returns to the **Idle** state.

Workflow Diagram


Handset
Handset Idle
Trigger Alarm
Send Alarm Event
Server
Server receives alarm
Display alarm reported message
Wait 20 seconds
Send Location Event
Server receives location
User presses OK

Location Event Reported Information

Approximately 10–20 seconds after the alarm event is reported, the handset sends a location event to the server.

Reported data includes:

```
ret: ok
event: location
ipui: 0291EADA2E       (Handset IPUI)
sipid: 1478521         (Registered account / user name)
bs_name: Base Station 1 (Connected Base name)
bs_rpn: 1              (Base RPN)
bs_rssi: -7            (Signal strength to Base)
bs_mac: 80:5e:c0:3e:72:15 (Base MAC address)
```

Server-Initiated Search

Introduction

The server can actively request the DECT system to search for the location of a specific handset via an Action URI command, allowing the user's location to be obtained even before an alarm is triggered. This is suitable for scenarios that require proactive device location.

Prerequisites and Configuration

Enable the Action URI feature

Enables the Action URI feature, allowing the server to control the handset to perform positioning actions via DM.

```
features.action_uri.enable
features.action_uri_limit_ip
action_url.show_msgbox
```

Parameter	Permitted Values	Default	Description
featu	**0**-Disabled	1	It enables or disables the phone from receiving the action

res.action_uri.enable	**1**-Enabled		URI requests.
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).
action_url.show_msgbox	**0**-Not required **1**-Required	0	It configures whether the remote control requires a confirmation pop-up.

Location Report Server Configuration

Used to configure the destination server address and authentication information for reporting location data after positioning is completed.

```
alarm.report_to_server.url
alarm.report_to_server.username
alarm.report_to_server.password
```

Parameter	Permitted Values	Default	Description
alarm.report_to_server.url	URL within 512	Blank	It configures the server address for reporting alarm information in the alarm function.

	characters		
alarm.report_to_server.username	string within 512 characters	Blank	It configures the authentication account for the server used to report alarm information in the alarm function.
alarm.report_to_server.password	string within 512 characters	Blank	It configures the authentication password for the server used to report alarm information in the alarm function.

Location Trigger Method (Action URI)

The server triggers handset positioning by calling the DM interface via an HTTP request:

```
https://DM_IP/servlet?
key=location&ipui=Handset_IPUI&sipid=Handset_Account&timeout=5
```

Parameter Description

Command	Description
ipui	Initiate a search using the designated controller
sip-id	Commence a search from the designated controller associated with the specified account (corresponding to the user name of the SIP account within the DECT system). If both ipui and sip-id are provided, only ipui will be used.
time-out	Establish the time frame for this search, which ranges from 5 to 10. In the case of an invalid configuration value, if the value is less than 5, it shall be set to 5; if it exceeds 10, it shall be set to 10.

AML-Messaging

Introduction

You can view the history of pushed messages on the handset and check their processing status. The information to be displayed in the **Message List** includes priority, time, and message title. The list supports a maximum of 50 messages.

Before You Begin

It is only applicable to W73H, W74H, W78H, W53H, W56H, W57R, W59R, and W59R Pro.

Message Configuration

Set via the Device Interface

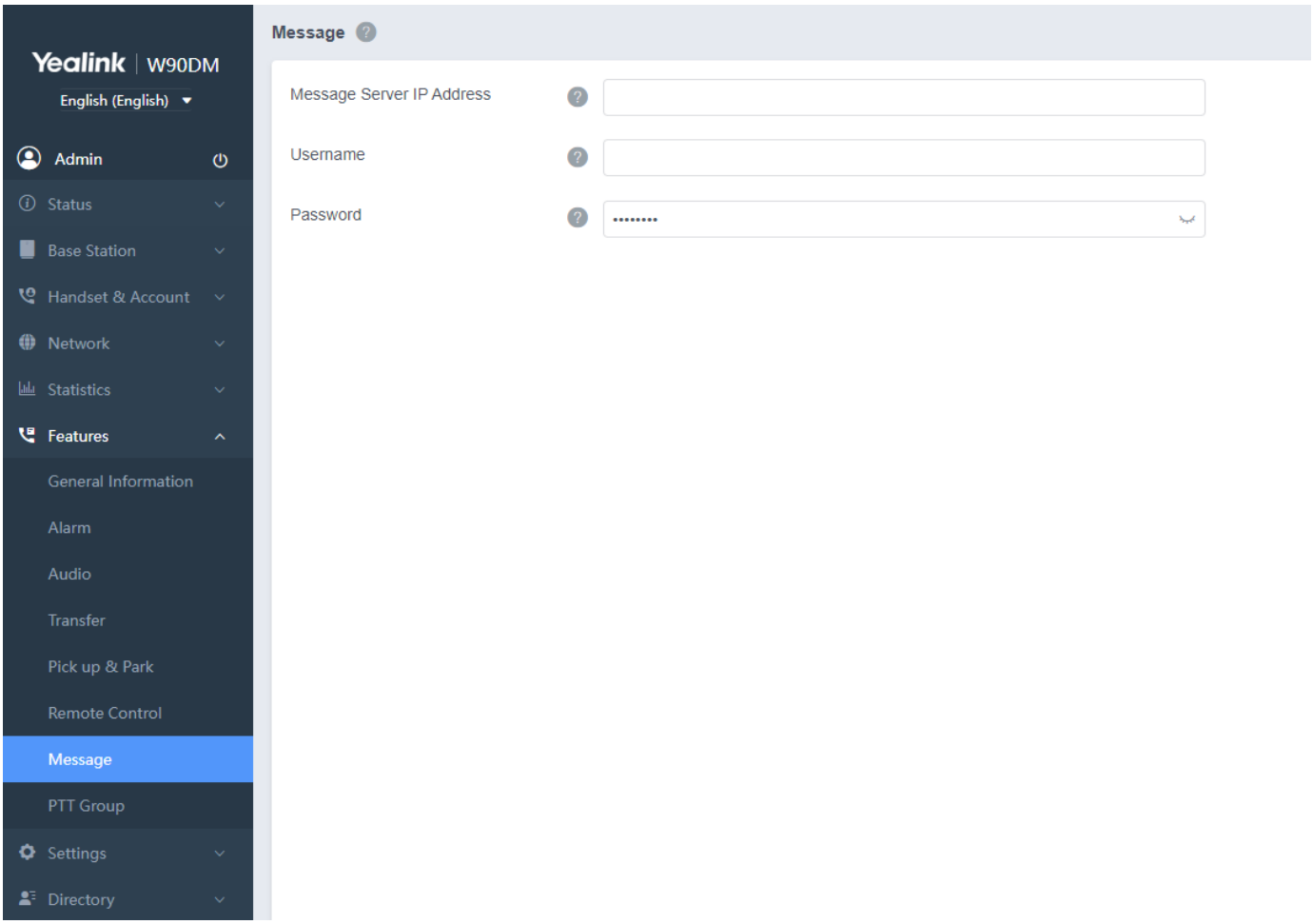


1. The **Message List** icon is displayed only when the handset is connected to a Multi-Cell system, "features.message_server.url" is properly configured, and the **Message Server** service is accessible.
2. If it is not configured or the configuration is invalid, the icon will not be displayed on the handset.

Set via the Web User Interface

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

You can specify one or more trusted IP addresses on the IP phone, or allow it to receive and send messages from any IP address.



Configuration Parameter

features.action_uri.enable
features.action_uri_limit_ip
action_url.show_msgbox
features.message_server.url
features.message_server.username
features.message_server.password

Parameter	Permitted Values	Default	Description
features.action_uri.enable	**0**-Disabled **1**-Enabled	1	It enables or disables the phone from receiving the action URI requests.
features.action_uri_limit_ip	IP address **Blank**-the phone will	Blank	It configures the server address from which the phone receives the action URI requests. Multiple addresses are separated by commas.

	reject any HTTP GET request. **any**-the phone will accept and handle HTTP GET requests from any IP address.		(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).
action_url.show_msgbox	**0**-No confirmation dialog box required **1**-Confirmation dialog box required		It configures whether a confirmation dialog box is required for remote control actions.
features.message_server.url [1]	URL within 511 characters	Blank	It configures the server used for sending messages.
features.message_server.username	URL within 32 characters	Blank	It configures the authentication account for the server used to send messages.
features.message_server.password	URL within 32 characters	Blank	It configures the authentication password for the server used to send messages.

[1] The configuration rules for the value are the same as push_xml.server.

Message Format

Example: The following is an Alarm XML message example.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<YealinkIPPhoneTextScreen
AlarmId="1"
Priority="0"
Beep="yes"
Ring="Ring1.wav"
Timeout="0"
```

```
Vibration="yes"
LockIn="no">
<Title>Yealink Alarm Server</Title>
<Text bgcolor="254,14,14" textcolor="0,0,0">
Room 1 Emergency
</Text>
<SoftKey index="1">
<Label>Reject</Label>
<URI>
https://10.50.1.173/yealink.php?action=decline
</URI>
</SoftKey>
<SoftKey index="2">
<Label>Accept</Label>
<URI>
https://10.50.1.173/yealink.php?action=confirm
</URI>
</SoftKey>
</YealinkIPPhoneTextScreen>
```

Parameter	Position	Type	Value
YealinkIPPhoneTextScreen	Root tag	mandatory	none Original experience.
Beep	Root tag	optional	"yes" "no"
Ring	Root tag	optional	"Ring1.wav" "Ring2.wav" "Ring3.wav" "Ring4.wav" "Ring5.wav" "Ring6.wav" "Ring7.wav" "Ring8.wav" "Ring9.wav" "Ring10.wav" "Ring11.wav" "Ring12.wav" "Ring13.wav" "Silent.wav" "Splash.wav"
Timeout	Root tag	optional	integer, if not configured, the default timeout is 45 seconds; if configured as 0, there will be no timeout.

LockIn	Root tag	optional	"yes" "no"
Vibration	Root tag	optional	"yes" "no"
Extensions	Root tag	optional	string
handsets	Root tag	optional	string
AlarmId	Root tag	mandatory	int The alarm ID must be less than 65535.
Priority	Root tag	optional	int (0-10, default 2)
Title	Body	mandatory	string
wrap	Title tag	optional	"yes" "no"
Text	Body	mandatory	string
bgcolor	Text tag	optional	RGB (0-255, 0-255, 0-255)
textcolor	Text tag	optional	RGB (0-255, 0-255, 0-255)
SoftKey	Body	optional	string
index	SoftKey tag	mandatory	integer
label	SoftKey tag	mandatory	string
URI	SoftKey tag	mandatory	string

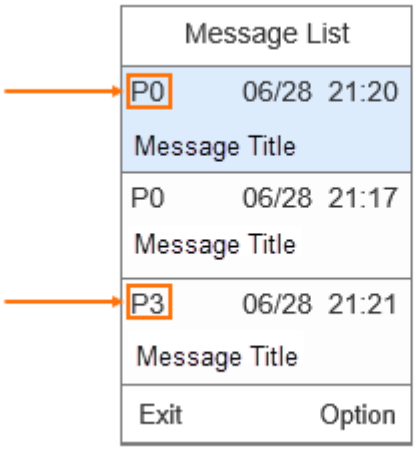
Push XML Request URI

To send message XML content to the device, use the following HTTP request address: https://<ServerIP>/servlet?push=msg

For detailed information, please refer to the XML Customization Guide.

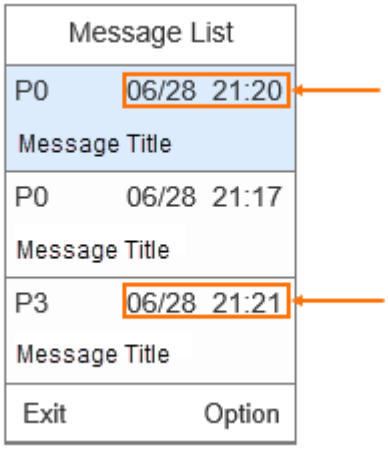
Message Details

Prior



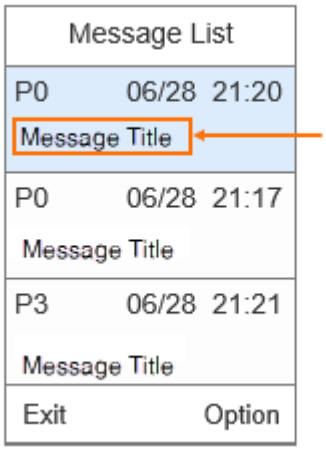
Priority, with values taken from the tag in the message. The display rule on the LCD screen is P + the tag value. For example, if 0, then the LCD screen will display P0 (refer to the diagram below).

Time



Time, indicating the time the message was received. The display rule on the LCD screen is date + time

Message Title



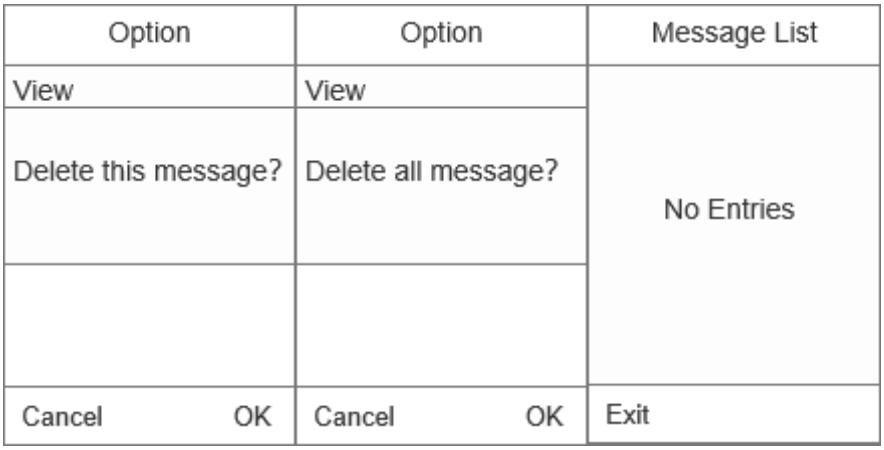
Message Title, with values taken from the Title tag in the message. When the number of characters is too long, if the cursor is not displayed, it will be represented by ellipsis (…). When the cursor is selected, it will scroll for display.

View



This option allows users to enter the details of the message.

Delete



- **Delete**: This option deletes the current message. Clicking it will prompt a pop-up on the current page, asking whether to delete the current message. Clicking "OK" will delete it, and clicking "Cancel" will cancel the operation. After deletion, the page returns to the message list.
- **Delete all**: This option deletes all messages. Clicking it will prompt a confirmation on the operation page, asking whether to delete all messages. After successful deletion, it returns to the list, and the list will be empty (see the diagram above).

User and Administrator Identification

Introduction

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

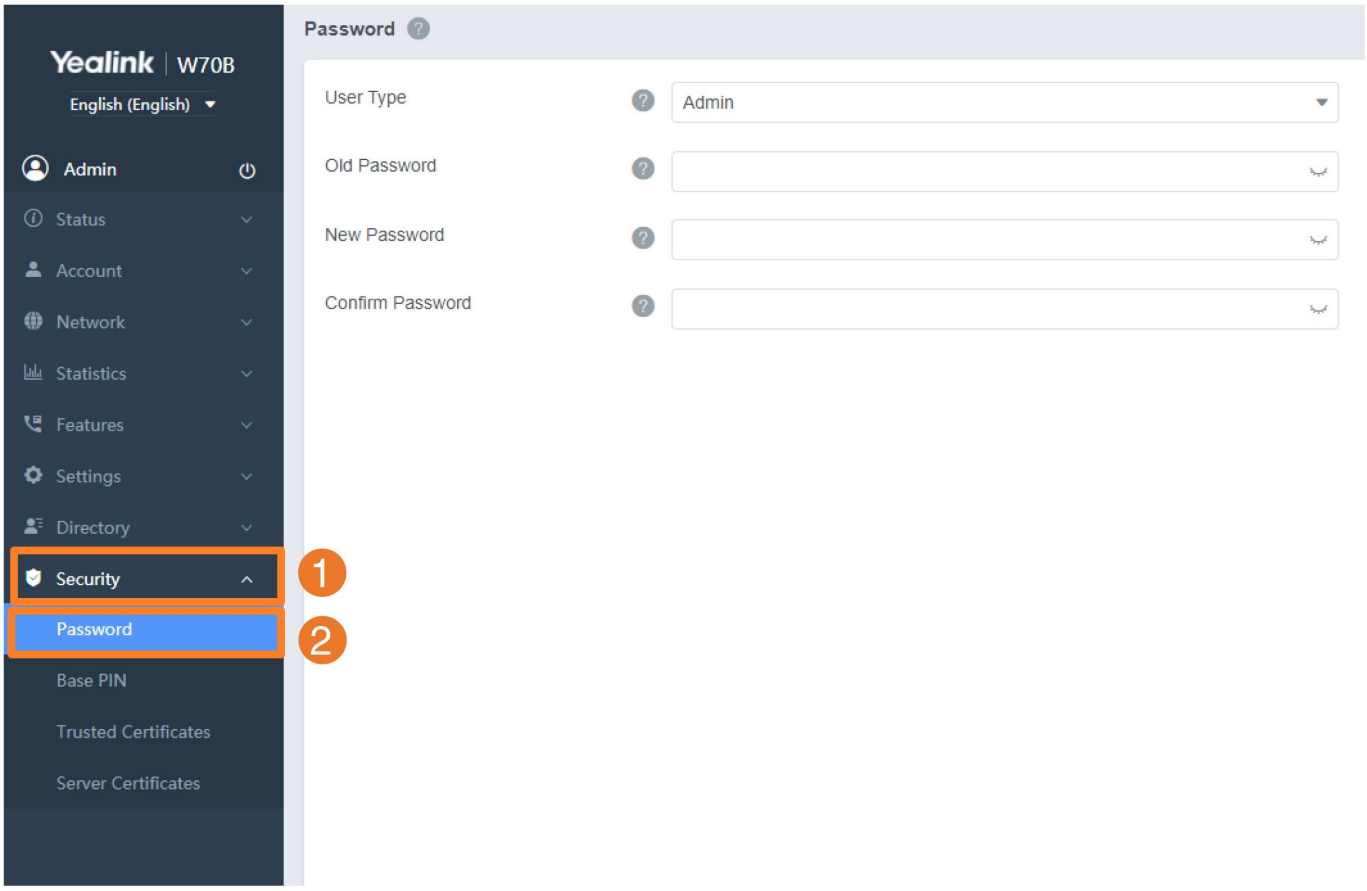
When logging into the web user interface or accessing advanced settings on the phone, as an administrator, you need an administrator password to access various menu options. The default username and password for the administrator are "**admin**". Both you and the user can log into the web user interface,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

For security reasons, you should change the default user or administrator password as soon as possible. Since 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

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 :. **Example**: static.security.user_password = user:123 means setting the password of user to 123. static.security.user_password = admin:456 means setting the password of the 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.

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

User Access Level Configuration

Configuration Parameter

static.security.var_enable
static.web_item_level.url
static.security.default_access_level

Parameter	Permitted Values	Default	Description
static.security.var_en	**0**-Disabled	0	It enables or disables the 3-level access

able[1]	**1**-Enabled		permissions (admin, user, var).
static.web_item_level.url[1]	URL within 511 characters	Blank	It configures the access URL of the file, which defines 3-level access permissions.
static.security.default_access_level[1]	**0**-user **1**-var **2**-admin	0	It configures the default access level to access the handset user interface. 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

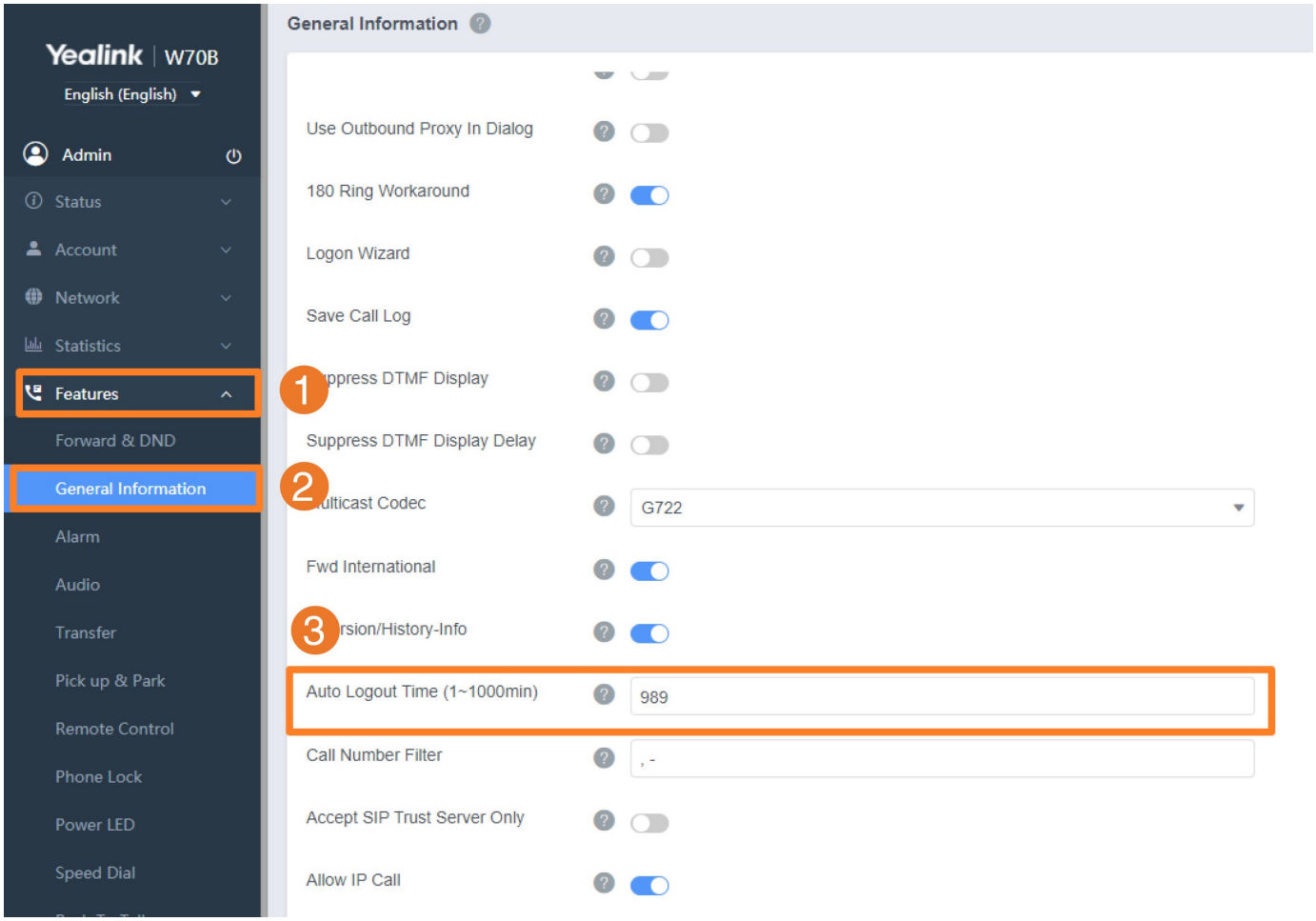
Introduction

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 you log out, you must re-enter your username and password for web access authentication.

Auto Logout Time Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Auto Logout Time(1~1000min)**.



Configuration Parameter

features.relog_offtime

Parameter	Permitted Values	Default	Description

		t	
features.relog_offtime	Integer from 1 to 1000	5	It configures the timeout interval (in minutes) for web access authentication

Phone Lock

Introduction

You can lock the DD phone or handsets to prevent them from unauthorized use.

Yealink phones offer three types of phone lock:

Type	Description
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 unauthorized 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.

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.

For the DD Phone, the Volume key, HEADSET key, and Speakerphone key are always available even when you lock the phone.

Phone Lock Configuration

Configuration Parameter

```
phone_setting.phone_lock.dialing_contorl_type
phone_setting.phone_lock.dialing_contorl_time
```

Parameter	Permitted Values	Default	Description
phone_setting.phone_lock.dialing_contor	**0**-After locking the phone, the keypad tone still exists, and the dial pad will appear when you press the digital key.	0	It configures the dialing control types of phone lock.

l_type	**1**-After locking the phone, there is no keypad tone, and the dial pad will only appear when you input the emergency number.		
phone_setting.phone_lock.dialing_contorl_time	0, 3, 5, 10	3	It configures the time to judge whether the input number is an emergency number. It works only if "phone_setting.phone_lock.dialing_contorl_type" is set to 1 (Enabled).

Base PIN

Introduction

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.

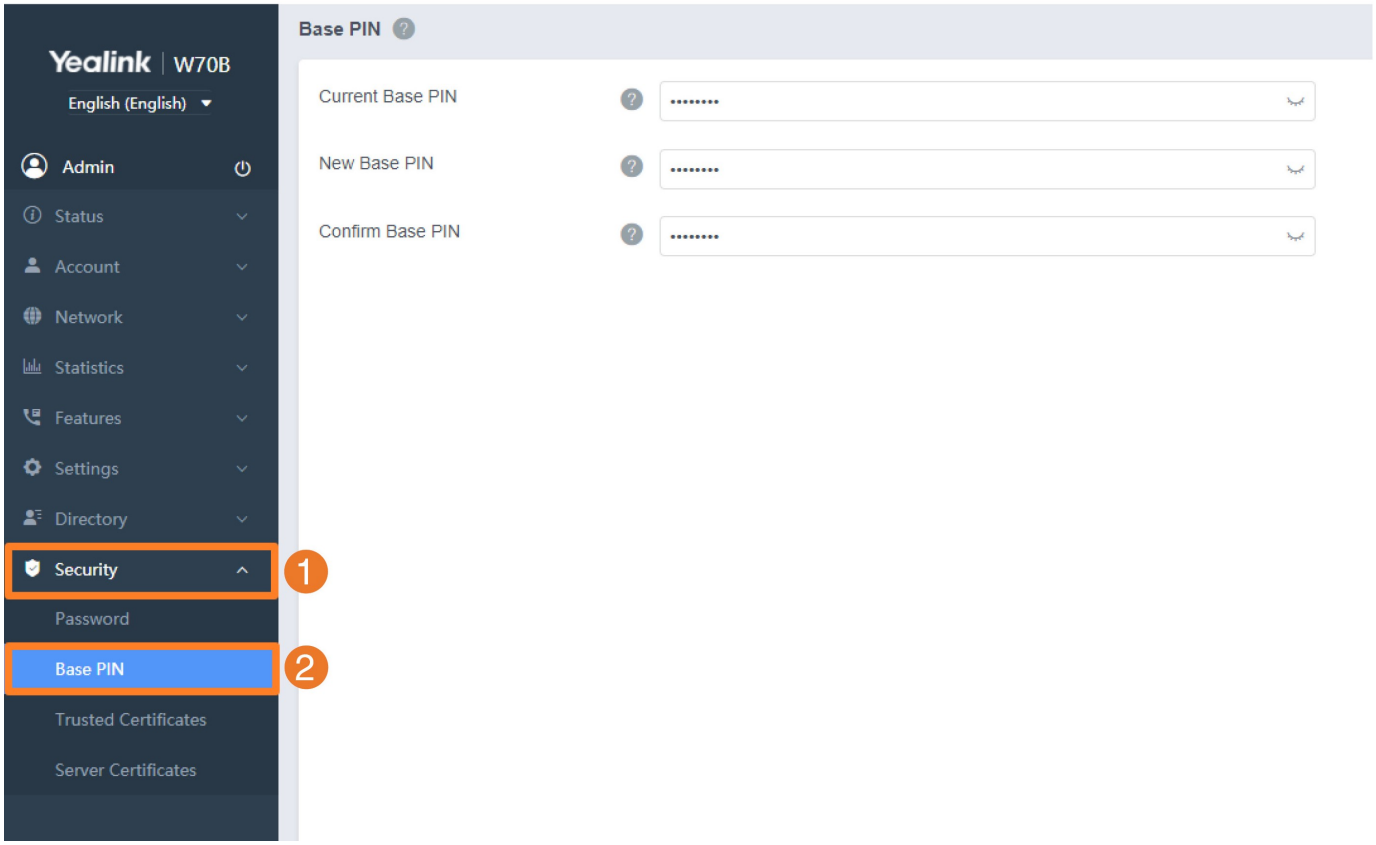
Base PIN Configuration

Set via the Device Interface (For W70B)

See Change the Base PIN.

Set via the Web User Interface

1. On the web user interface, go to **Security** > **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	0000	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	0000	It configures the PIN for registering or deregistering a handset. It works only if "base.double_pin_code.enable" is set to 1 (Enabled).

Emergency Number

Introduction

Public telephone networks in countries around the world have a single emergency telephone number (emergency services number), that allows a caller to contact local emergency services for assistance when necessary.

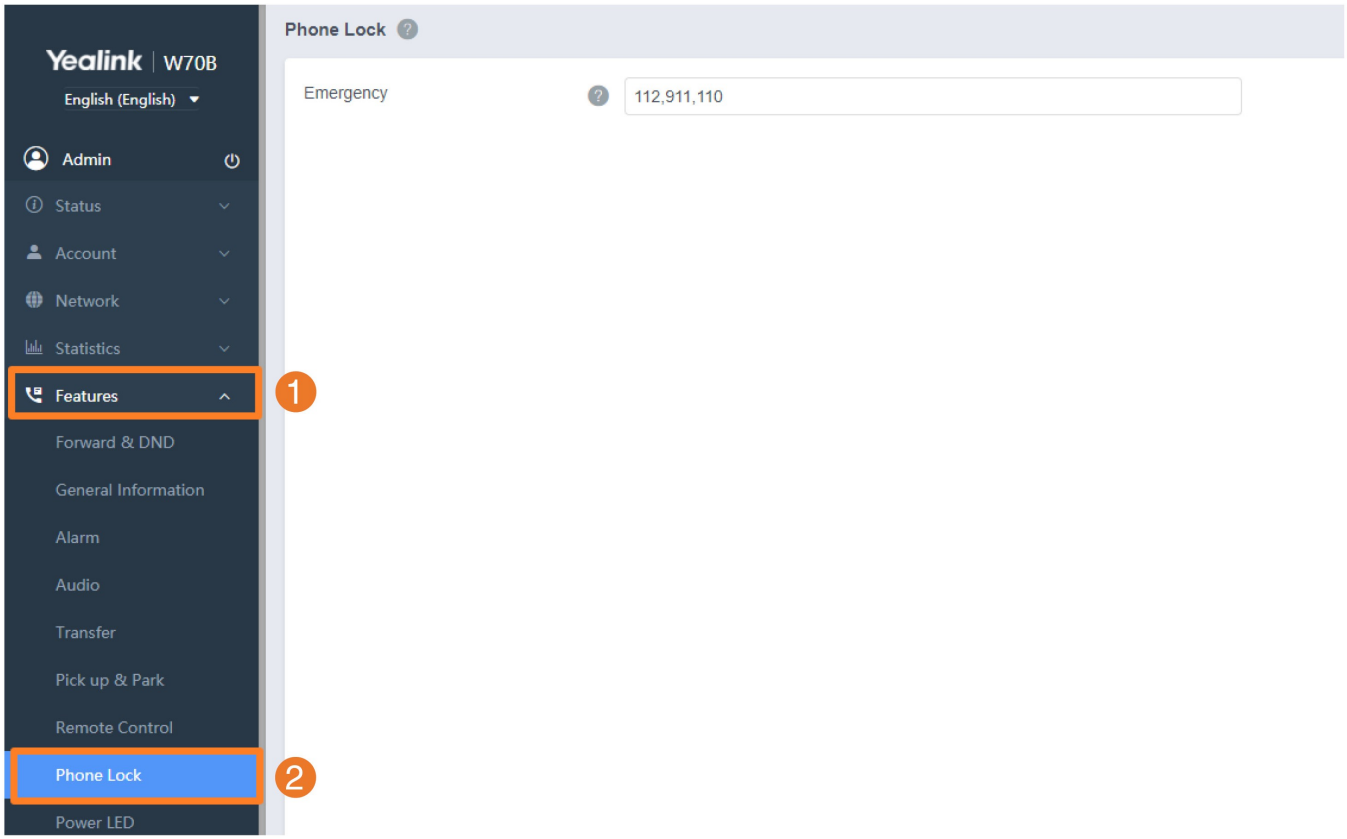
You can specify the emergency numbers for contacting the emergency services in an emergency situation. The emergency telephone number may differ from country to country. It is typically a three-digit number so that it can be easily remembered and dialed quickly.

You can dial these numbers when the phone is locked (CP930W-Base/CP935W-Base phones can not be locked).

Emergency Number Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **Phone Lock** > **Emergency**.



Configuration Parameter

phone_setting.emergency.number

Parameter	Permitted Values	Default	Description
phone_setting.emergency.number	String within 99 characters	112, 911, 110	It configures emergency numbers. Multiple emergency numbers are separated by commas.

Emergency Alarm

Introduction

An emergency alarm can provide safety reliance for people who work in dangerous environments.

Before You Begin

Only W59R/W59R Pro/W57R support this feature.

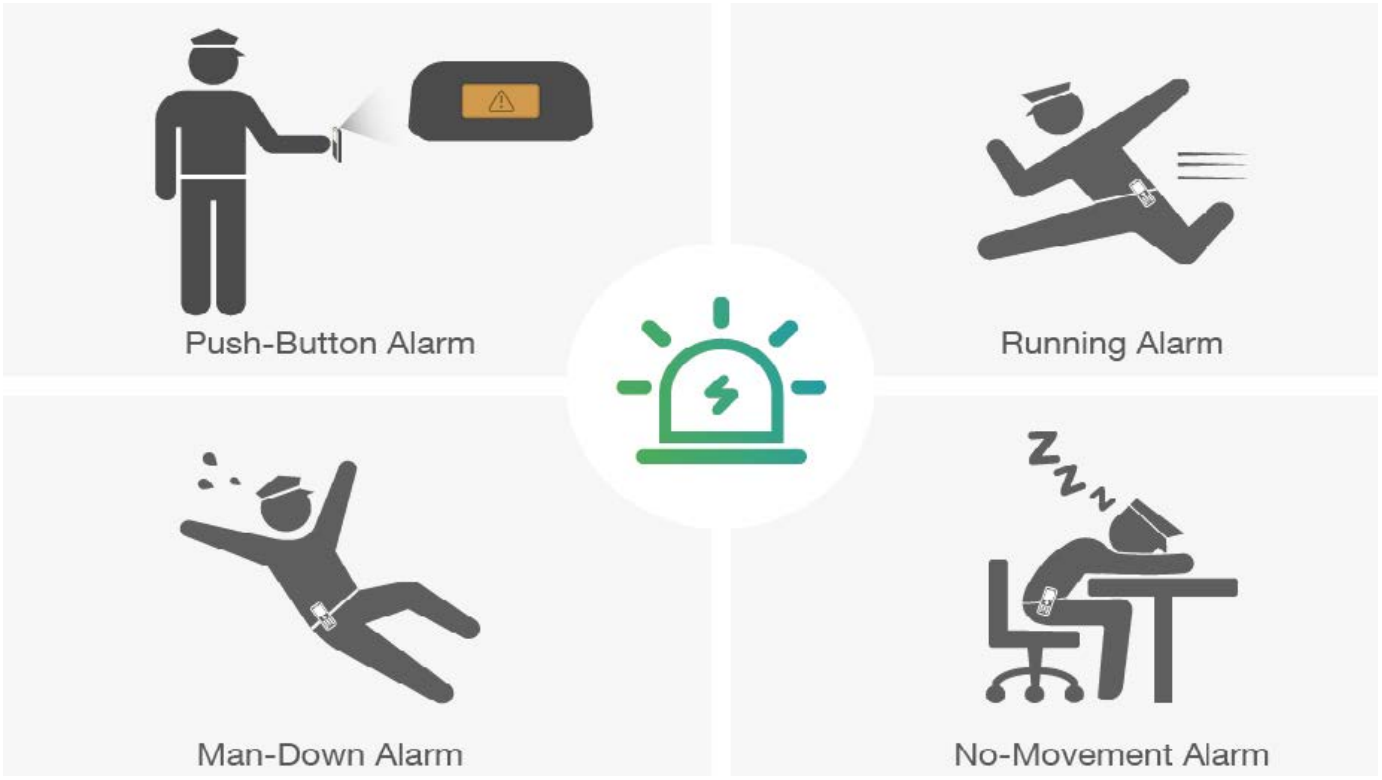
Video Tutorial

For a detailed video, refer to How to Use the Emergency Alarm.

Supported Alarm Types

W59R handset supports the following four alarm types, W57R only supports button:

Type	Description
Button	Long-press the emergency alarm button for 2 seconds to manually set off the emergency alarm.
Man Down	If the handset stays at a tilt angle of less than 30 degrees with the ground for some time, an alarm will be triggered.
No-Movement	If the handset stays in a fixed position without movement for a certain period of time, an alarm will be triggered.
Running	The handset detects the running state and maintains this state for a certain period of time; an alarm will be triggered.

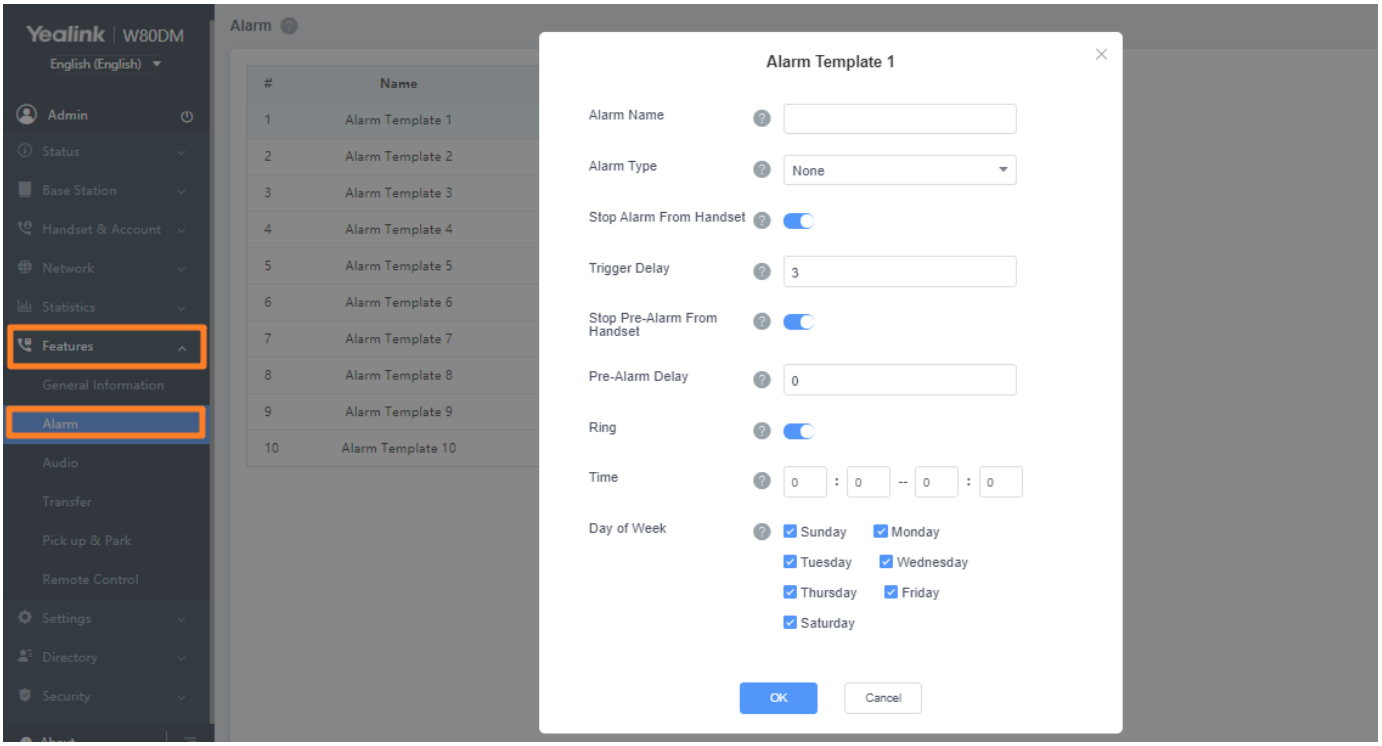


In order to increase the accuracy of the alarm and prevent false alarms, you can also set the corresponding delayed alarm time. The delayed alarm time is actually the time during which the handset maintains the state, and the alarm will be triggered when the time is reached.

Emergency Alarm Configuration

Set via the Web User Interface

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



Configuration Parameter

alarm.X.name
alarm.X.type
alarm.X.handset_stop.enable
alarm.X.trigger_delay
alarm.X.pre_alarm.handset_stop.enable
alarm.X.pre_alarm.delay
alarm.X.ring.enable
alarm.X.weekly.begin_time
alarm.X.weekly.end_time
alarm.X.weekly.dayofweek
account.X.alarm.template
account.X.alarm.server
account.X.alarm.number
account.x.alarm.number.button
account.x.alarm.number.man_down
account.x.alarm.number.no_movement
account.x.alarm.number.running
handset.X.alarm.number
alarm.server.address
alarm.server.port
alarm.server.transport_type
alarm.server.expires
alarm.server.retry_counts

Parameter	Permitted Values	Default	Description
alarm.X.name[1]	String within 64 characters	Blank	It configures the alarm name.
alarm.X.type[1]	**0**-None, do not turn on the alarm. **1**-Button **2**-Man Down	0	It configures the alarm type.

	3-No Movement **4**-Running		
alarm.X.handset_stop.enable[1]	**0**-Disabled **1**-Enabled	1	It enables or disables terminating the alarm from the handset.
alarm.X.trigger_delay[1]	Integer from 1 to 7200	3	It configures the delay time (in seconds) to trigger the alarm from the handset.
alarm.X.pre_alarm.handset_stop.enable[1]	**0**-Disabled **1**-Enabled	1	It enables or disables the handset to stop the pre-alarm (reminder before the alarm).
alarm.X.pre_alarm.delay[1]	Integer from 0 to 7200	0	It configures the pre-alarm time (in seconds) of the handset.
alarm.X.ring.enable[1]	**0**-Disabled **1**-Enabled	1	It enables or disables playing the ringtone when the handset initiates the pre-alarm.
alarm.X.weekly.begin_time[1]	Time from 00:00 to 23:59	00:00	It configures the starting time of the day for the handset to perform an alarm detection. The alarm detection occurs at a random time between the starting time and the ending time. If the configured starting time is greater than the ending time, such as 23:00-06:00, it means that the alarm detection is enabled on the day from 00:00-06:00 and 23:00-00:00.
alarm.X.weekly.end_time[1]	Time from 00:00 to 23:59	00:00	It configures the ending time of the day for the handset to perform an alarm detection. The alarm detection occurs at a random time between the starting time and the ending time. If the configured starting time is

			greater than the ending time, such as 23:00-06:00, it means that the alarm detection is enabled on the day from 00:00-06:00 and 23:00-00:00.
alarm.X.weekly.dayofweek[1]	0123456 or a combination of these digits	0123456	It configures the days of the week for the handset to perform an alarm detection weekly.
account.X.alarm.template[2] [3]	Random combination of numbers 1 to 10	Blank	It configures the alarm template for the specific account. Multiple alarm templates are separated by commas.
account.X.alarm.server[2] [3]	**0**-Same As SIP Server **1-10**-Pre-configured SIP server (server name is configured by template.X.name)	0	It configures the server through which the specific account sends an alarm.
account.X.alarm.number[2] [3]	String within 128 characters	Blank	It configures the emergency alarm number.
account.x.alarm.number.button[2] [3]	String within 128 characters	Blank	It configures the emergency alarm number to call when the alarm type of the specific account is Button.
account.x.alarm.number.man_down[2] [3]	String within 128 characters	Blank	It configures the emergency alarm number to call when the alarm type of the specific account is Man-Down.
account.x.alarm.number.no_movement[2] [[3]	String within 128 characters	Blank	It configures the emergency alarm number to call when the alarm type of the specific account is No-Movement.
account.x.alarm.number.run	String within 128 characters	Blan	It configures the emergency alarm number to call when the alarm type of

ning[2] [3]		k	the specific account is Running.
handset.X.alarm.number[2][4]	String within 128 characters	Blank	It configures the handset X alarm number.
alarm.server.address[4]	String within 256 characters	Blank	It configures the address of the alarm server.
alarm.server.port[4]	Integer from 0 to 65535	5060	It configures the port of the alarm server.
alarm.server.transport_type[4]	0-UDP 1-TCP 2-TLS 3-DNS-NAPTR	0	It configures the type of alarm server transmission protocol.
alarm.server.expires[4]	Integer from 30 to 2147483647	30	It configures the registration expiration time of the alarm server.
alarm.server.retry_counts[4]	Integer from 0 to 20	3	It configures the number of times to retry the request when the alarm server is unavailable or not responding.

[1]X is the alarm ID. X=1-10.
[2]X is the account ID.
- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

[3]This parameter is only applicable to W80/90 Multi-Cell System.
[4]This parameter is only applicable to W70B.

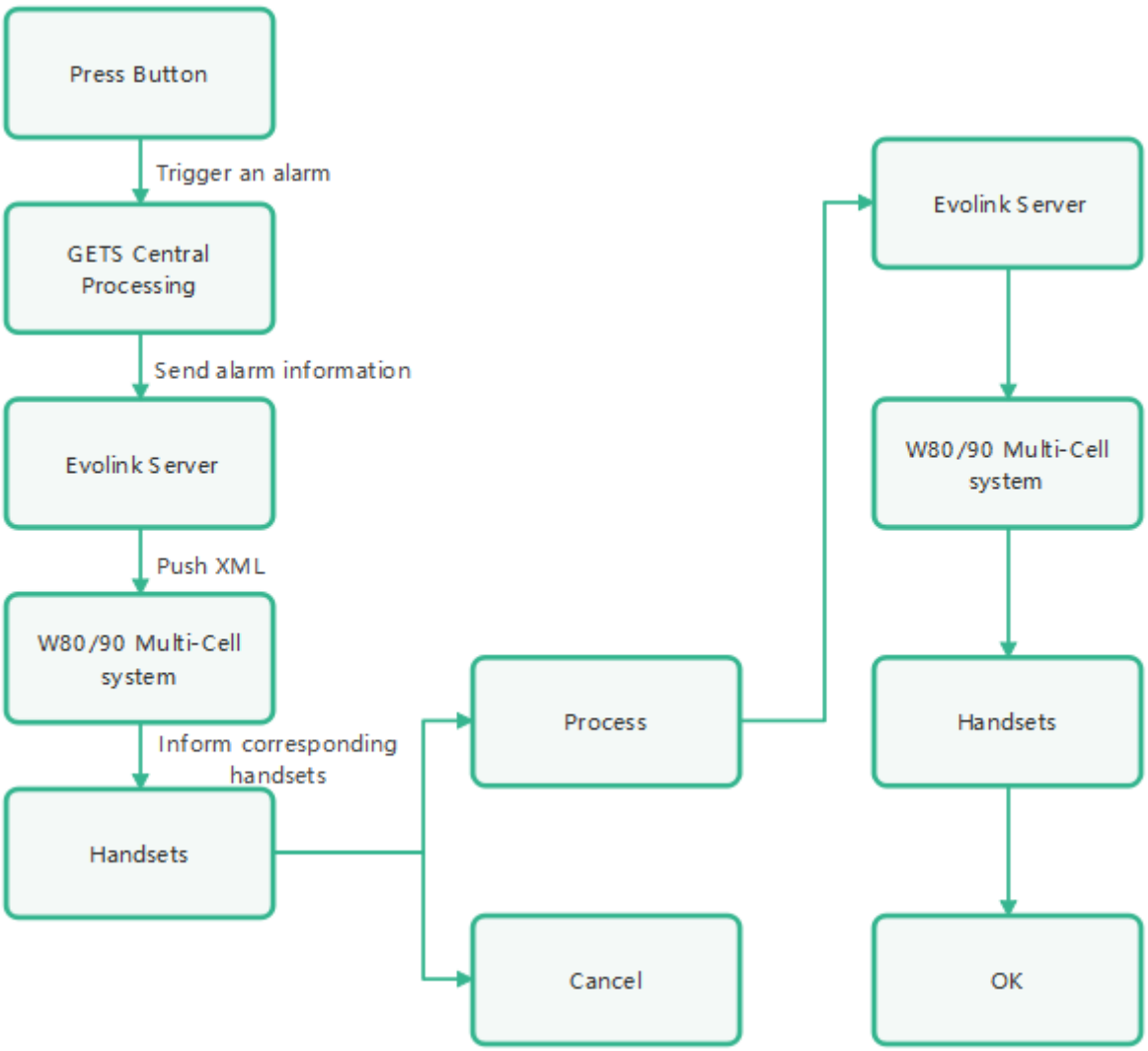
GETS Alarm System

The W80/W90 Multi-Cell System supports the GETS alarm system. In case of emergency, you can press the GETS alarm, which will send the corresponding information to the EvoLink application, and EvoLink will send an XML file to the W80/W90 Multi-Cell System. The W80/W90 Multi-Cell System will parse the file and notify the corresponding handsets to ring and display the corresponding information.

Before You Begin

This feature is only applicable to the W80/90 Multi-Cell system.

Alarm Process



For more information about XML Browser configuration, please refer to XML Browser.

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.

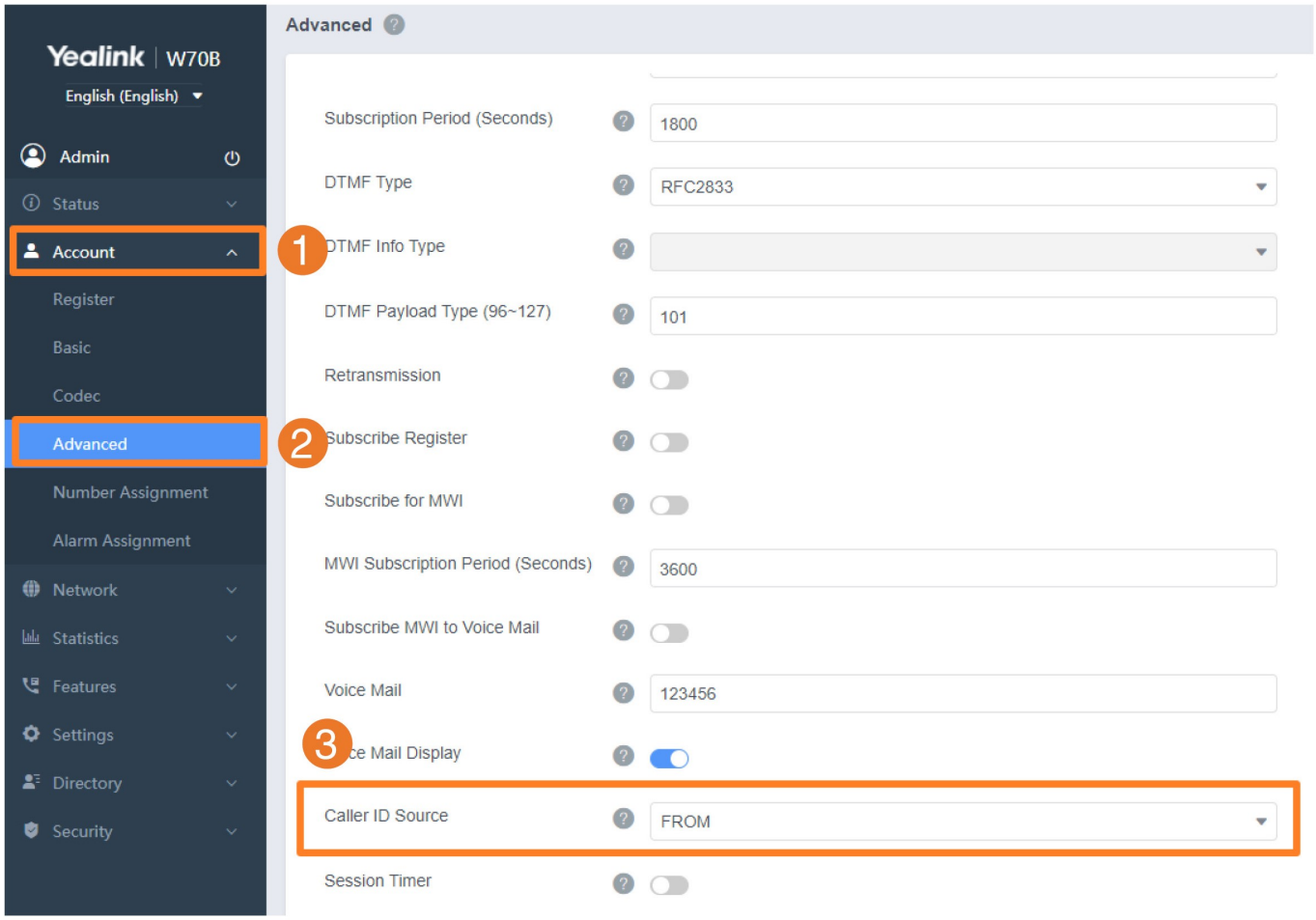
- **Calling Line Identification Presentation (CLIP)**: It allows the phones to display the caller identity, derived from a SIP header contained in the INVITE message when receiving an incoming call. Yealink phones can derive caller identity from three types of SIP headers: **From**, **P-Asserted-Identity (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.

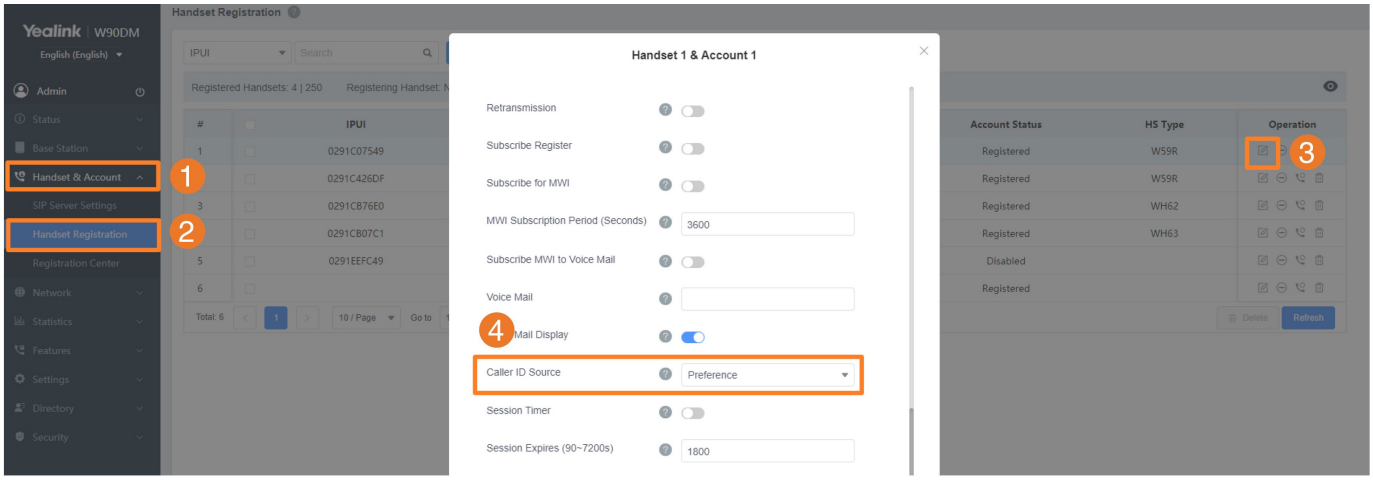
CLIP and COLP Configuration

Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Advanced** > **Caller ID Source**.



2. For W75/W80/W90 Multi-Cell system: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **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**-PRID-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,	It configures the priority order for the sources of caller identity information. Yealink phones can derive caller identity from the following SIP

		From	headers: From, P-Asserted-Identity (PAI), P-Preferred-Identity, and Remote-Party-ID (RPID). It works only if "account.X.cid_source" is set to 6 (PREFERENCE).
account.X.cp_source[1]	**0**-PAI-RPID **1**-Dialed Digits **2**-RFC4916, the caller sends the SIP request message, which contains the from-change tag in the Supported header. The caller then receives an UPDATE message from the server and displays the identity in the "From" header. **3**-Contact	0	It configures the identity of the callee according to the response message.

[1] X is the account ID.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

Return Code for Refused & Unanswered Call

Introduction

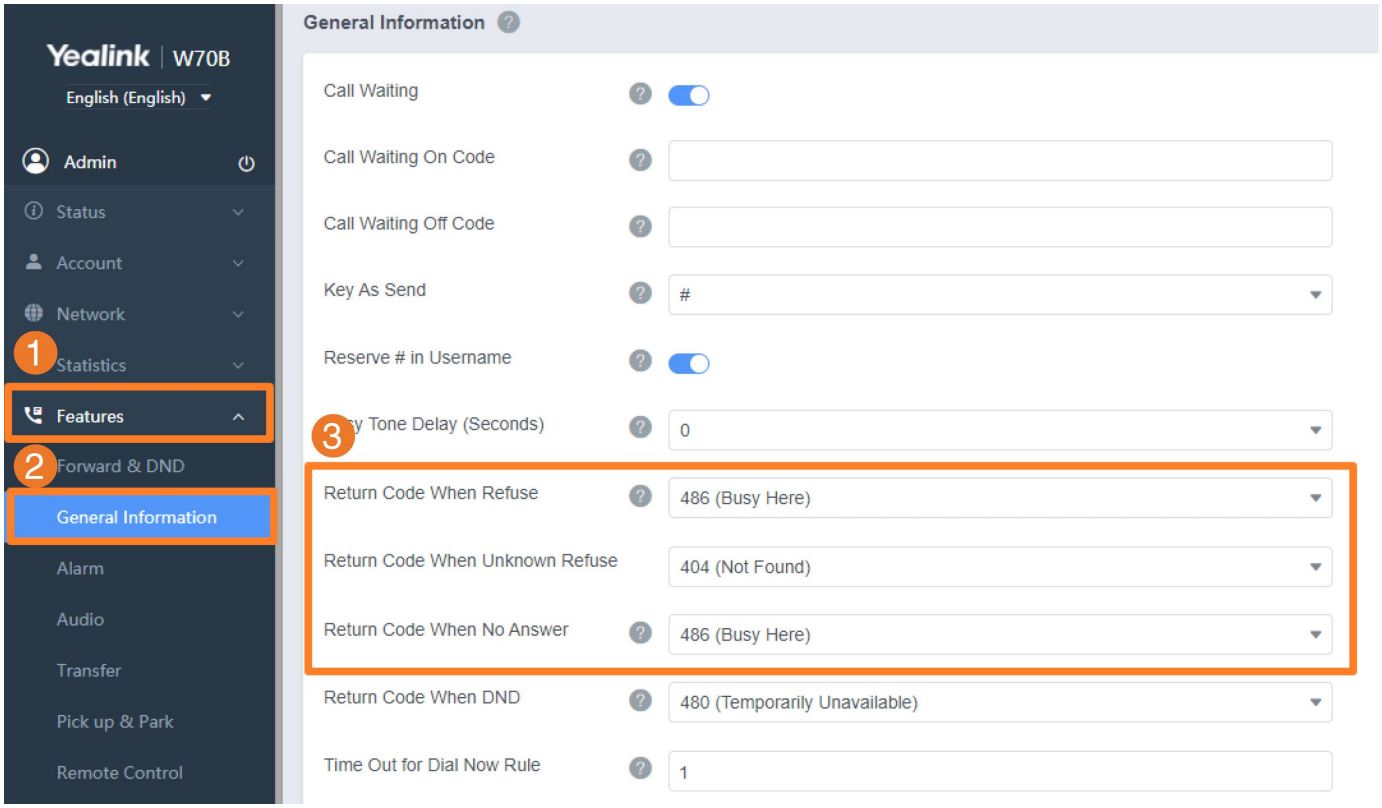
You can define the return code and reason of the SIP response message for the refused call. The caller's phone LCD screen displays the reason according to the received return code. Available return codes and reasons are:

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

Return Code for Refused Call and Unanswered Call 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 SIP Trust Server Only

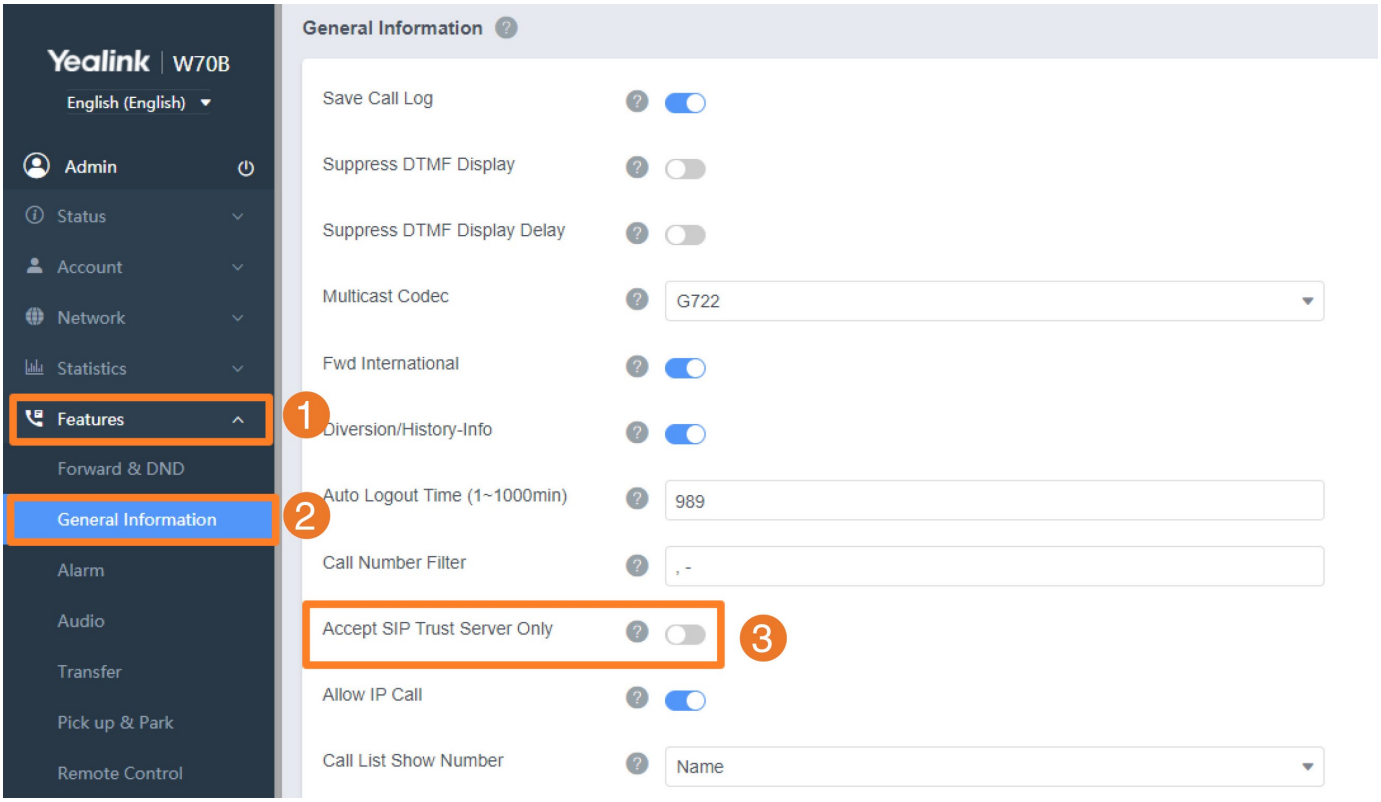
Introduction

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

Accept SIP Trust Server Only Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Accept SIP Trust Server Only**.



Configuration Parameter

sip.trust_ctrl

Parameter	Permitted Values	Default	Description
sip.trust_ct	**0**-Disabled **1**-Enabled, users	0	It enables or disables the phone to only accept the SIP message from the SIP and outbound proxy server.

rl	cannot accept the IP call		

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.

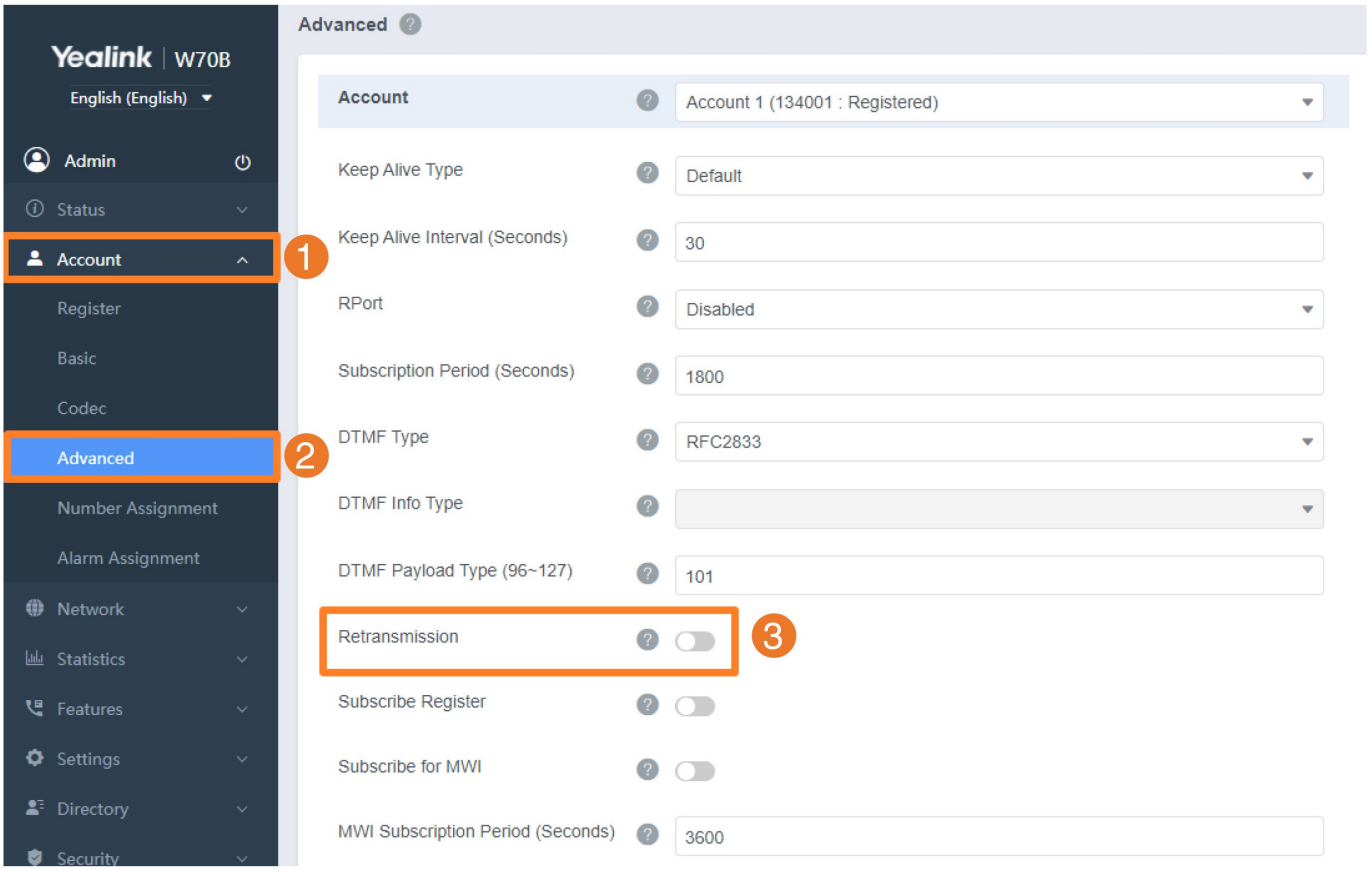
Example of a SIP INVITE message (take W70B as an example):

```
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", uri="
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 W70B 146.85.0.20
Supported: 100rel
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length: 302
```

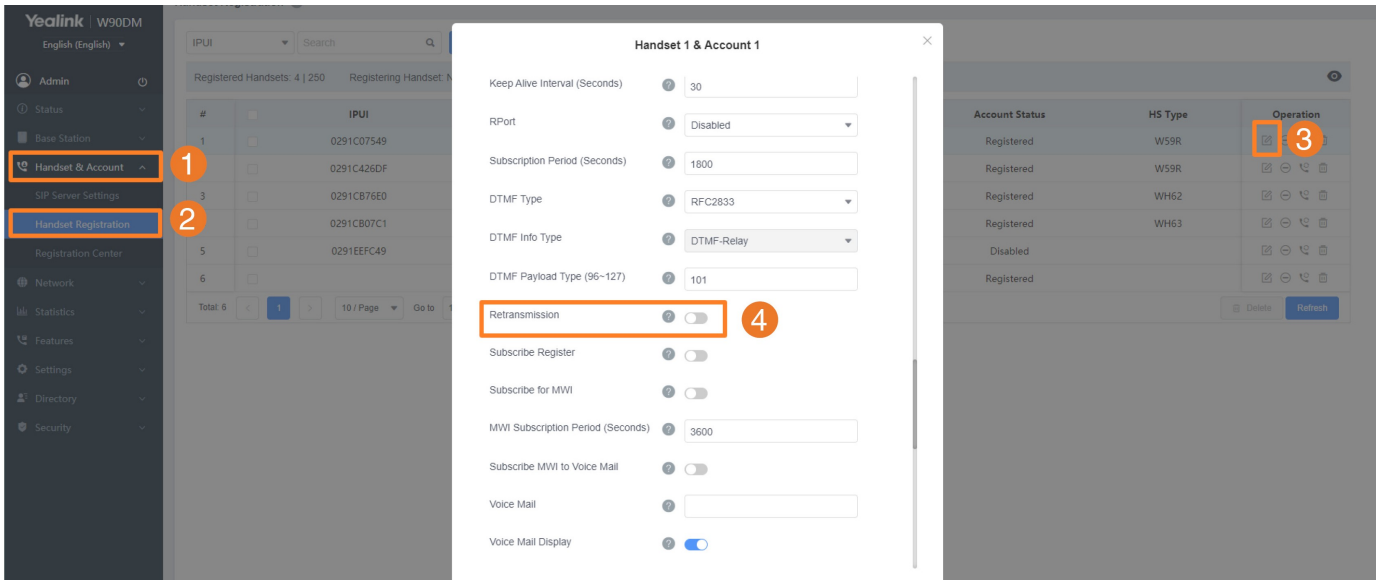
100 Reliable Retransmission Configuration

Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Advanced** > **Retransmission**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **Retransmission**.



Configuration Parameter

account.X.100rel_enable

Parameter	Permitted Values	Default	Description

		t	
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.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

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 a 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 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

Configuration Parameter

```
sip.timer_t1
sip.timer_t2
sip.timer_t4
```

Parameter	Permitted Values	Default	Description
sip.timer_t1	Float from 0.5 to 10	0.5	It configures the SIP session timer T1 (in seconds).
sip.timer_t2	Float from 2 to 40	4	It configures the SIP session timer T2 (in seconds).
sip.timer_t4	Float from 2.5 to 60	5	It configures the SIP session timer T4 (in seconds).

Session Timer

Introduction

Session timer allows a periodic refresh of SIP sessions through an UPDATE request, to determine whether a SIP session is still active. The session timer is specified in RFC 4028. The phones support two refresher modes: UAC and UAS. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiates the SIP request. If the initiator is configured as UAC, the other client or the SIP server will function as a UAS. If the initiator is configured as UAS, the other client or the SIP server will function as a UAC. The session expiration is negotiated via the Session-Expires header in the INVITE message. The negotiated refresher is always the UAC, which will send an UPDATE request at the expiration of the negotiated session. The value “refresher=uac” included in the UPDATE message means that the UAC performs the refresh.

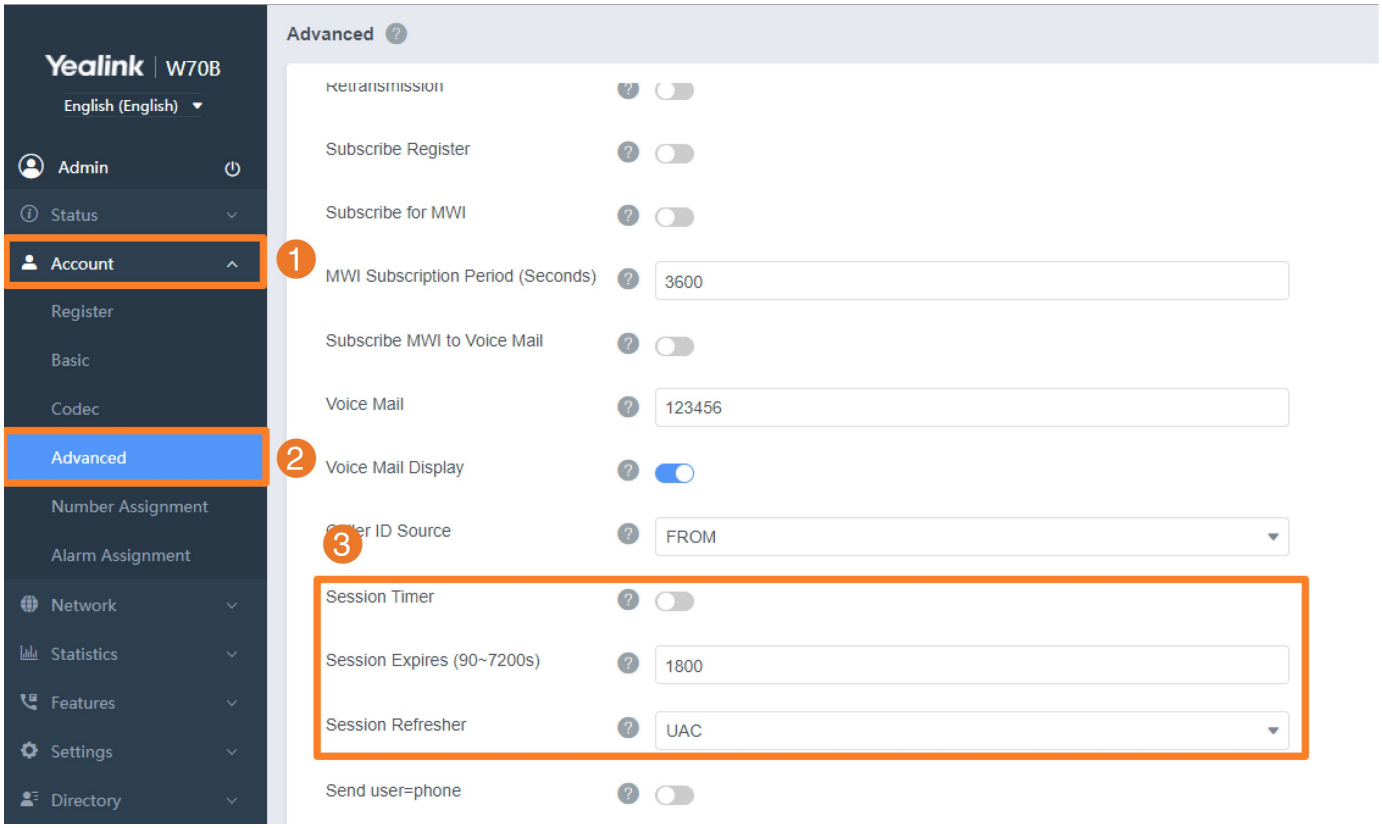
Example of UPDATE message (UAC mode) (take W70B as an example):

```
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 W70B 146.85.0.20
Session-Expires: 90;refresher=uac
Supported: timer
Content-Length: 0
```

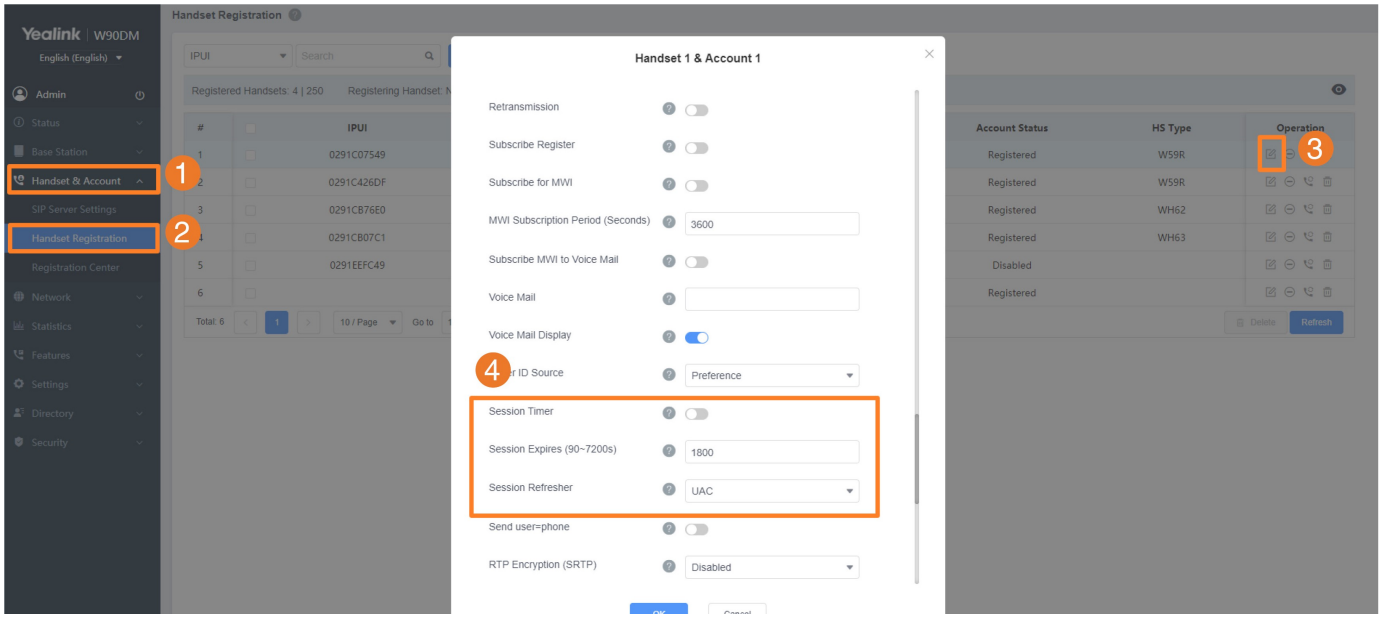
Session Timer Configuration

Set via the Web User Interface

1. For W70B: On the web user interface, go to **Account** > **Advanced** > **Session Timer**/**Session Expires (90~7200s)**/**Session Refresher**.



2. For W75/W80/W90 Multi-Cell System: On the web user interface, go to **Handset & Account** > **Handset Registration** > **Add Handset/Edit** > **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.

- For W70B, X=1-10.
- For W75DM, X=1-20.
- For W80 Multi-Cell System, X=1-100.
- For W90 Multi-Cell System, X=1-250.
- For VIM system, X=1-2500.

Reboot in Talking

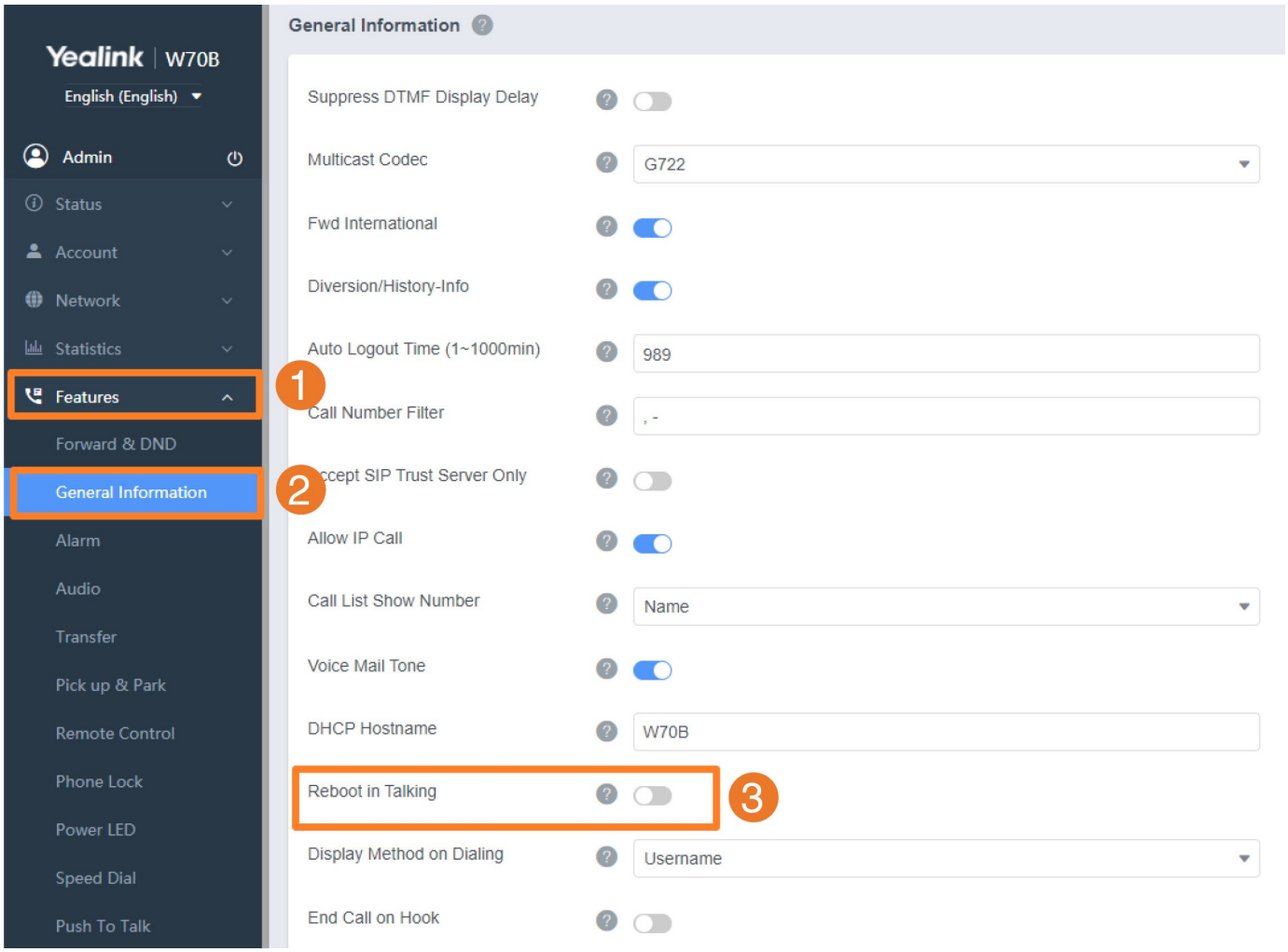
Introduction

Reboot in talking feature allows the phones to reboot during an active call when they receive a reboot notification message.

Reboot in Talking Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Reboot in Talking**.



Configuration Parameter

features.reboot_in_talk_enable

Parameter	Permitted Values	Default	Description

features.reboot_in_talk_enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to reboot during a call when it receives a reboot notification message.

Reserve # in User Name

Introduction

Reserve # in User Name feature allows the phones to reserve "#" in the user name. When the 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.

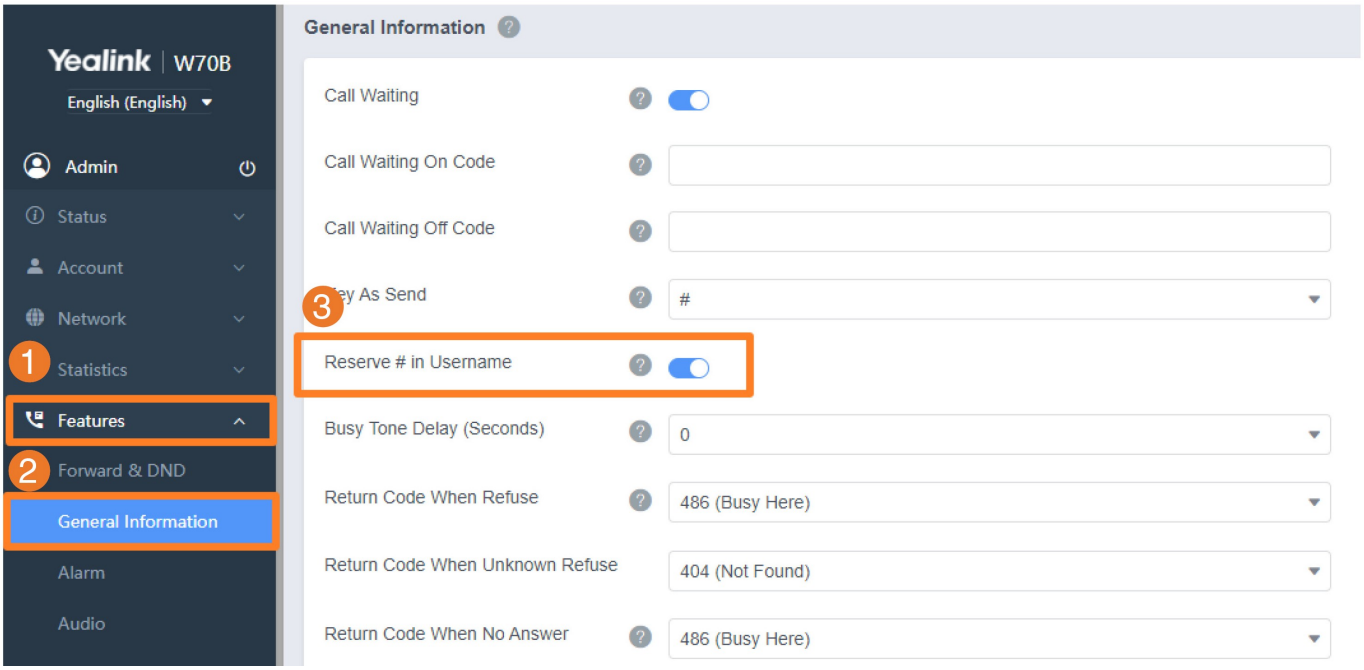
Example of a SIP REGISTER message (take W70B as an example):

```
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 W70B 146.85.0.20
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

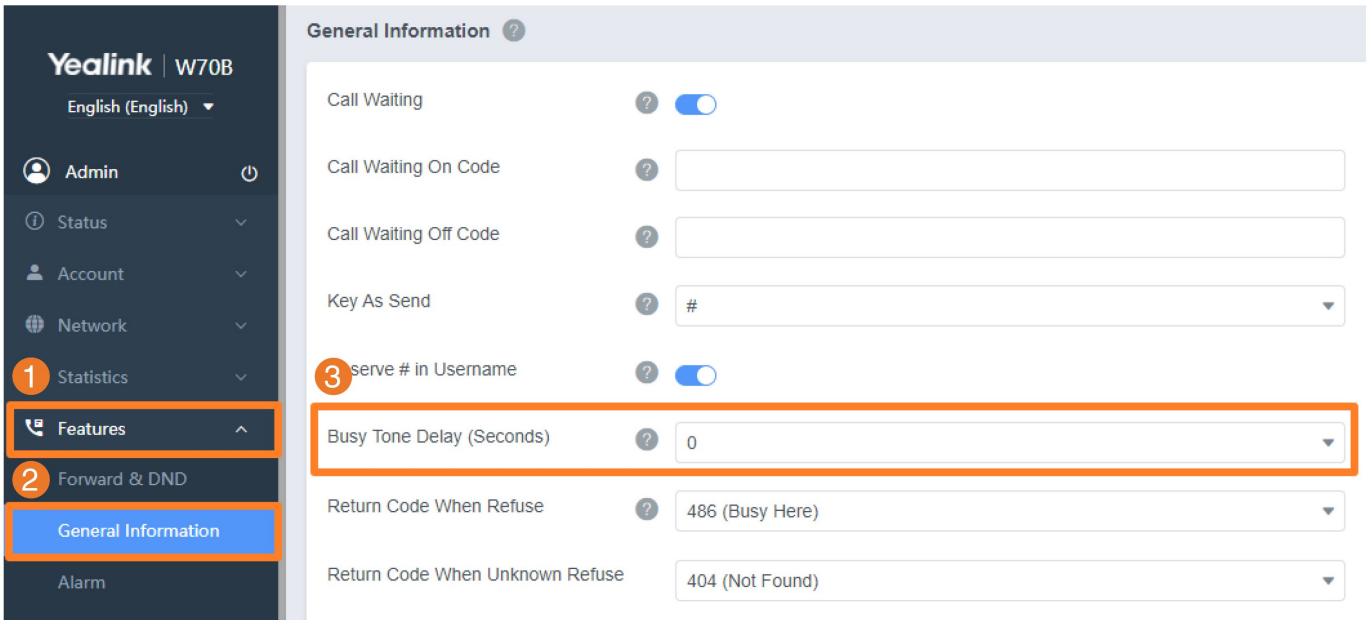
Introduction

The busy tone is an audible signal to indicate that the call has been released by the other party. You can define the amount of time that the busy tone lasts.

Busy Tone Delay Configuration

Set via the Web User Interface

1. On the web user interface, go to **Features** > **General Information** > **Busy Tone Delay (Seconds)**.



Configuration Parameter

features.busy_tone_delay

Parameter	Permitted Values	Default	Description
features.busy_tone_delay	**0**-the phone will not play a busy tone. **1**-1s, a busy tone lasts for 1 second on the phone. **3**-3s, a busy tone lasts for 3 seconds on the	0	It configures the duration (in seconds) that the busy tone lasts when the call is released by the remote party.

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

Web Page Display

Introduction

You can customize the web page display, such as the model name.

Before You Begin

This feature is only applicable to the W90 Multi-Cell System.

Web Page Display Configuration

Configuration Parameter

```
web_setting.dm.title
web_setting.dm.model_name
phone_setting.dm.login_note_text
web_setting.base.title
web_setting.base.model_name
phone_setting.dm.login_note_text
```

Parameter	Permitted Values	Default	Description
web_setting.dm.title	String within 32 characters	Yealink $DEV (Yealink W90DM)	It configures the title bar name of the web page for W90DM.
web_setting.dm.model_name	String within 32 characters	$DEV (W90DM)	It configures the model name of the web page for W90DM.
phone_setting.dm.login_note_text	String within 128 characters	$DEVNAME (DECT IP Multi-Cell DECT Manager)	It configures the product name of the web login page for W90DM.
web_setting.base.title	String within 32 characters	Yealink $DEV (Yealink W90B)	It configures the title bar name of the web page for W90
web_setting.base.model_name	String within 32 characters	$DEV (W90B)	It configures the model name of the web page for W90B.
phone_setting.dm.login_note_text	String within 128 characters	$DEVNAME (DECT IP Multi-Cell Base Station)	It configures the product name of the web login page for W90B.

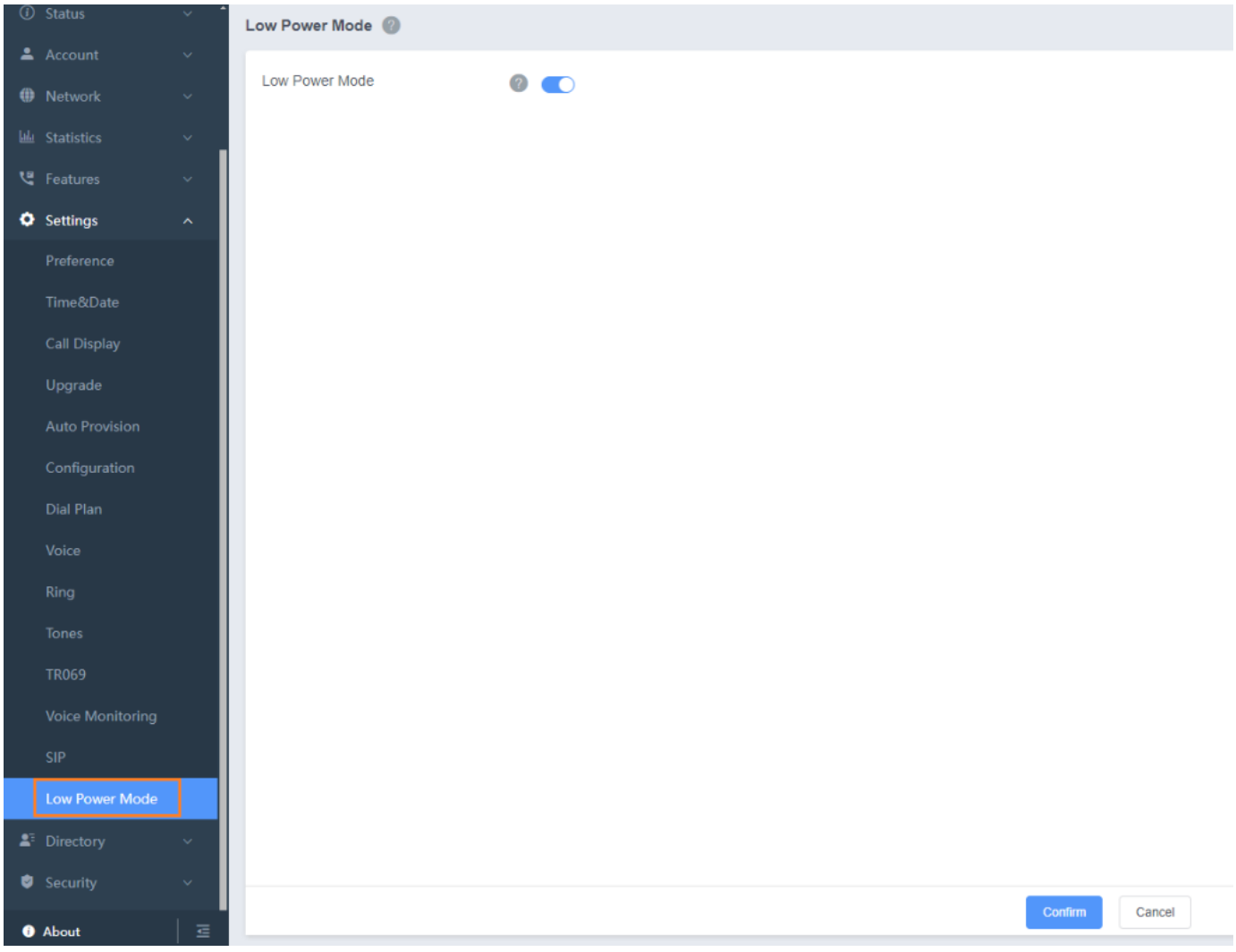
Low Power Mode

Introduction

You can enable the **Low Power Mode** to reduce power consumption during Base standby.

Set via the Device Interface

1. On the web user interface, go to **Settings** > **Low Power Mode**.



Configuration Parameter

features.low_power.mode

Parameter	Permitted Values	Default	Description

features.low_power.mode	**0**-Disabled **1**-Enabled	0	It enables or disables the Low Power Mode to reduce power consumption during BASE standby. Only the European version of the ba

			s e i s e n a b l e d b y d e f a u l t .

Introduction

Phone Provisioning Introduction

You can provision multiple phones with the same settings for large-scale deployments.

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.

Boot Files

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: a common boot file and a MAC-oriented boot file. You can use the default boot template file "y000000000000.boot" to create a 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

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

MAC-oriented Boot File

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

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

> 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 base.

Boot File Attributes

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

Attributes	Description
#! version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
include: config <xxx.cfg> include: config "xxx.cfg"	Each "include" statement can specify a location of a configuration file. The configuration file format must be *.cfg. The locations in the angle brackets or double quotation marks support two forms: • Relative path (relative to the boot file): For example, sip.cfg, HTTP Directory/sip.cfg • Absolute path (or URL): For example, http://10.2.5.258/HTTP Directory/sip.cfg The location must point to a specific CFG file.
overwrite_mode	Enable or disable the overwrite mode. **1-(Enabled)** - If the value of a parameter in configuration files is left blank, or if a non-static parameter in configuration files is deleted or commented out, the factory default value takes effect. **0-(Disabled)** - If the value of a parameter in configuration files is left blank, deleted, or commented out, the pre-configured value is kept. 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.

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

Customize a Boot File

Procedure

1. Open a boot template file.

2. To add a configuration file, add include: config < > or include: config "" to the file. Each starts on a

separate line.

3. Specify a configuration file for downloading.
   For example:
   include:config <configure/sip.cfg >
   include:config "http://10.2.5.206/configure/account.cfg"
   include:config "http://10.2.5.206/configure/dialplan.cfg"
4. Specify the overwrite mode.
   For example:
   overwrite_mode = 1
5. Save the boot file and place it on the provisioning server.

Configuration Files

Yealink supports two configuration template files: the Common CFG file and the 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 of the same model. The common CFG file has a fixed name for each phone model.

The name of the common CFG file for the VIM is y000000001000.cfg.

The name of the common CFG file for the W90DM device is y000000000130.cfg.

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 users to keep their personalized configuration settings, even though the IP phone performs auto provisioning.

The non-static changes that you made before enabling the provisioning priority mechanism are not saved in the generated MAC-local file, but the previous settings still take effect on the phone. The static changes are never saved to the <MAC>-local.cfg file.
The provisioning priority mechanism is enabled by the parameter static.auto_provision.custom.protect.

Configuration File Customization

You can create some new CFG files by making a copy and renaming the configuration template file (for example, sip.cfg, account.cfg). You can rearrange the parameters in the configuration template file and create your own configuration files with the 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.	Specify the parameters and values to apply specific settings to the phones. • Separate each configuration parameter and value with an equal

1.dnd.enable = 1)	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

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

Supported Resource Files

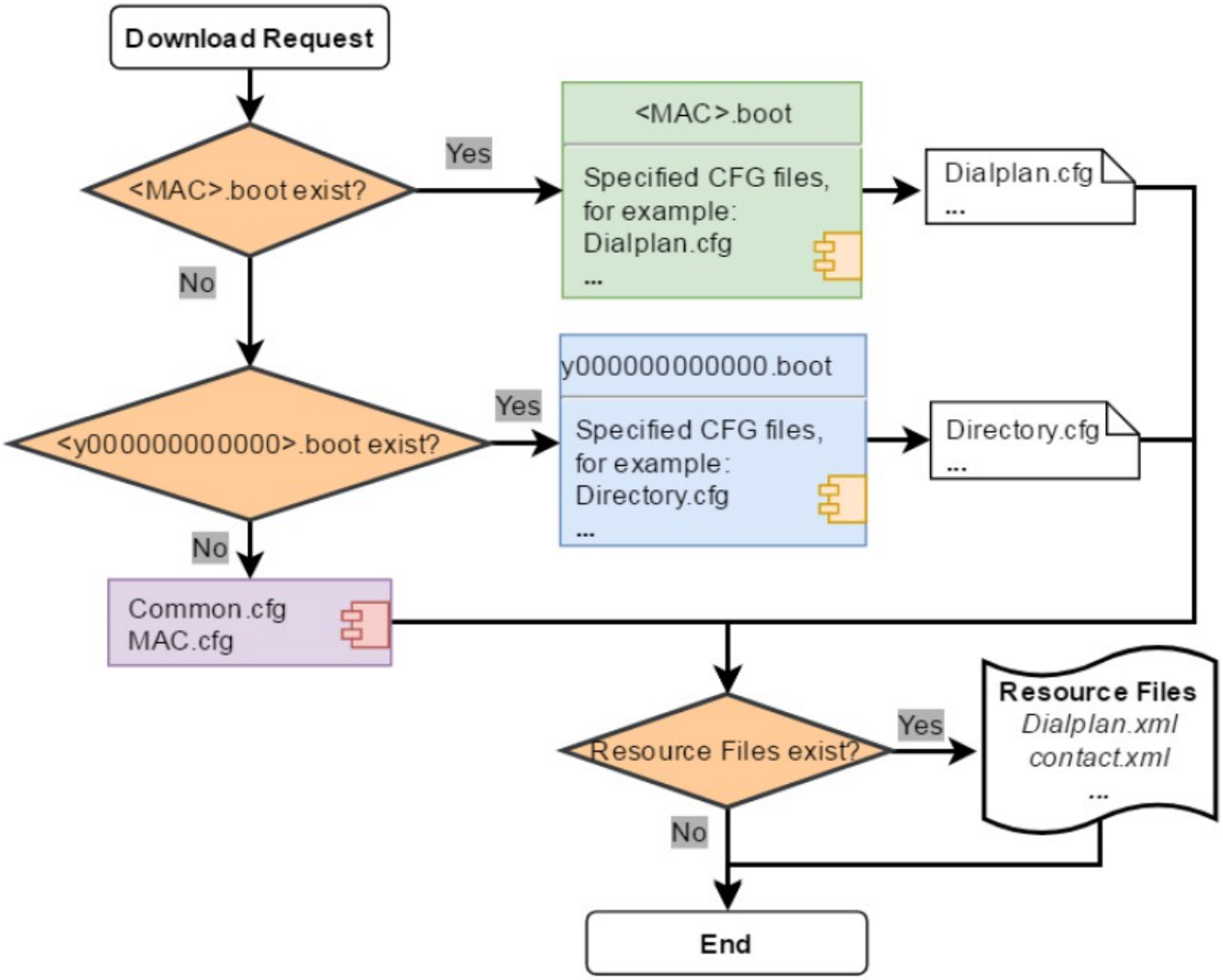
Yealink supplies some templates of resource files for you, so you can directly edit the files as required. The following table lists the resource files Yealink supplies:

Template File	File Name	Description	Reference in Section
AutoDST Template	AutoDST.xml	Add or modify time zone and DST settings.	DST Settings
Language Packs	For example, 1.English.js	Customize the translation of the existing language on the web user interface.	Language for Web Display Customization
Replace Rule Template	DialPlan.xml	Customize replace rules for the dial plan.	Replace Rule File Customization
Dial Now Template	DialNow.xml	Customize dial now rules for the dial plan.	Dial Now File Customization
Super Search Template	super_search.xml	Customize the search source list.	Search Source File Customization
Local Contact	contact.x	Add or modify multiple local	Local Contact File

File	ml	contacts.	Customization
Remote Phone Book Template	Department.xml Menu.xml	Add or modify multiple remote contacts.	Remote Phone Book File Customization

Files Download Process

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



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

Provisioning Methods

Introduction

Yealink provides two ways to provision your phones:

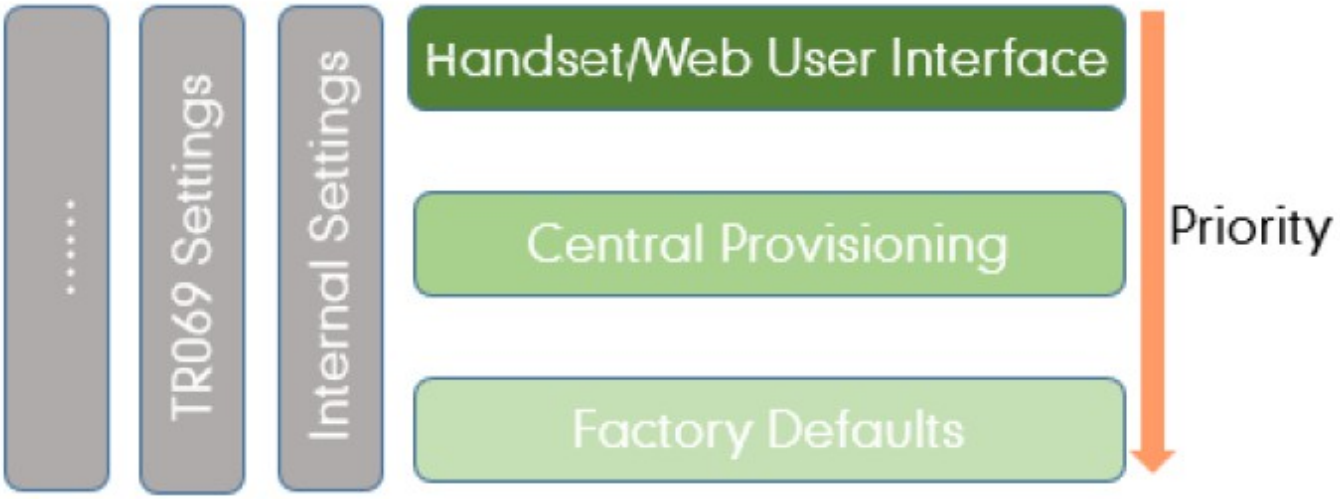
- **Manual Provisioning**: provisioning via the handset user interface or web user interface.
- **Central Provisioning**: provisioning through configuration files stored in a central provisioning server.

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

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):



The provisioning priority mechanism takes effect only if "static.auto_provision.custom.protect" is set to 1. For more information on this parameter, refer to Keep User's Personalized Settings after Auto Provisioning.

Static parameters have no priority. They take effect no matter what method (web user interface or phone user interface, or configuration files) you are using for provisioning.

Static parameters are the parameters that start with a prefix "static.". For example, the parameters associated with auto provisioning/network/syslog, TR069 settings, and internal settings (the temporary configurations to be used for program running).

Web User Interface

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.

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 explorer (for example, Internet Explorer).
  For security purposes, we recommend that you use this feature in a secure network environment.

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

```
wui.quick_login
wui.secure_domain_list
```

Parameter	Permitted Values	Default	Description
wui.quick_login	**0**-Disabled **1**-Enabled, you can quickly log into the web user interface using a request URI (for	0	It enables or disables the quick login feature. It works only if

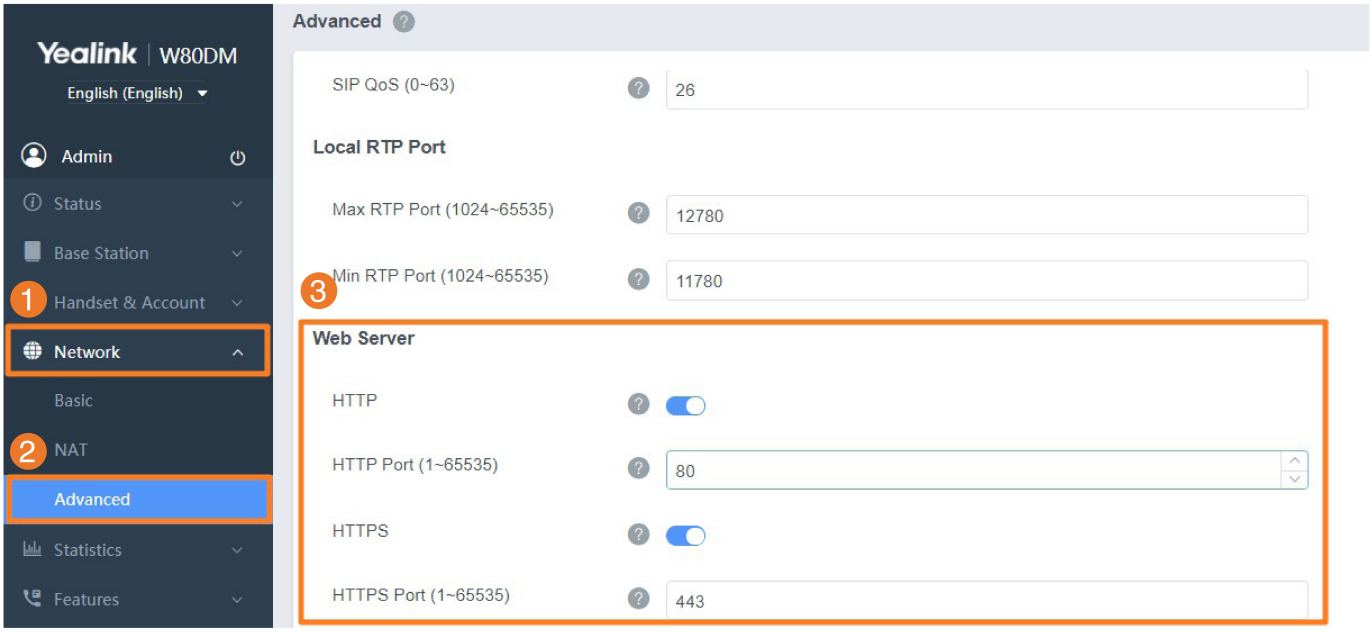
	example, https://IP/api/auth/login?@admin:admin).		"static.wui.https_enable" is set to 1 (Enabled).
wui.secure_domain_list	String If it is left blank, you are only allowed to use the IP address to access the web user interface of the phone. If it is set to "**any**", you can use IP address or any domain name to access the web user interface of the phone.	any	It configures the valid domain name to access the web user interface of the phone. Multiple domain names are separated by semicolons. **Example**: wui.secure_domain_list = test.abc.com You are only allowed to use test.abc.com or IP address to access the web user interface of the phone. 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 both HTTP and HTTPS protocols for accessing the web user interface. You can configure the web server type. Web server type determines the access protocol of the web user interface. If you are unable to access 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**.



Configuration Parameter

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

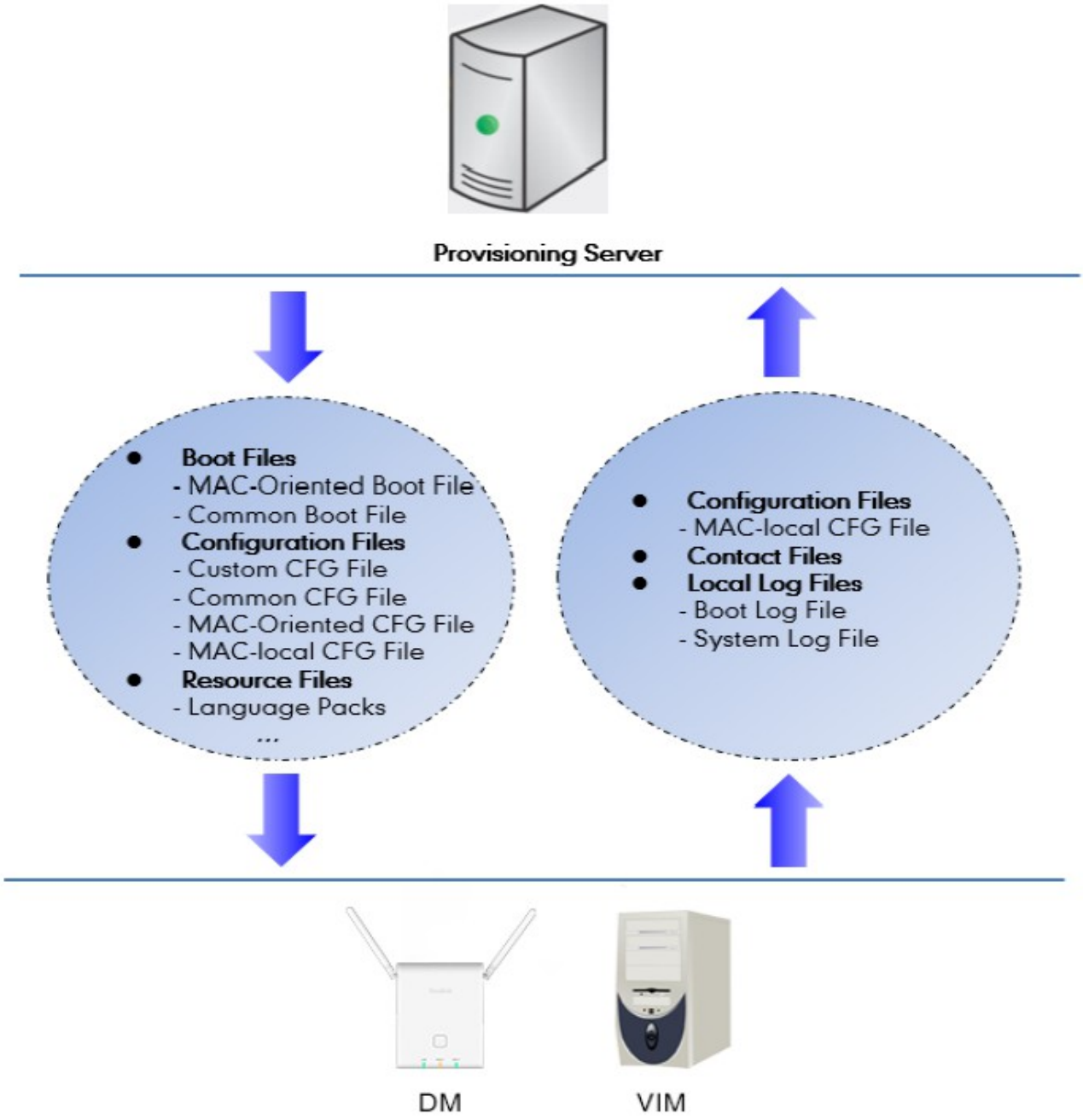
Parameter	Permitted Values	Default	Description
static.wui.http_enable[1]	**0**-Disabled **1**-Enabled	1	It enables or disables to access the web user interface of the phone over a non-secure tunnel (HTTP).
static.network.port.http[1]	Integer from 1 to 65535	80	It configures the port used to access the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

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

Central Provisioning

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.

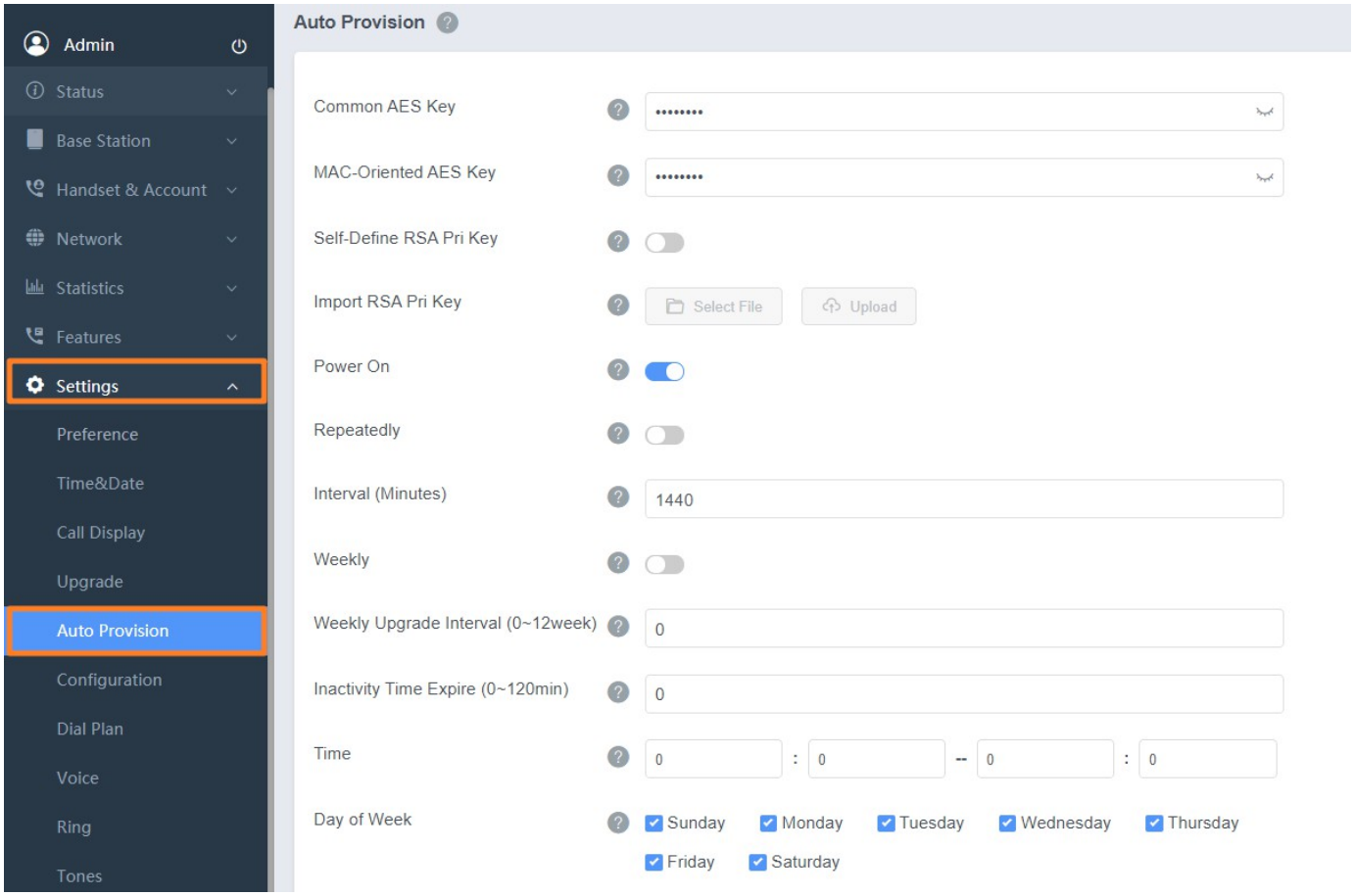
The phones can be configured to upload log files (log files provide a history of phone events), call log files, and contact files to the provisioning server. You can also configure a directory for each of these

three files.

Auto Provisioning Settings Configuration

Set via the Web User Interface

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



Configuration Parameter

static.auto_provision.attempt_expired_time
static.network.attempt_expired_time
static.auto_provision.attempt_before_failed
static.auto_provision.retry_delay_after_file_transfer_failed
static.auto_provision.reboot_force.enable
static.auto_provision.power_on
static.auto_provision.repeat.enable
static.auto_provision.repeat.minutes
static.auto_provision.weekly.enable
static.auto_provision.weekly_upgrade_interval
static.auto_provision.inactivity_time_expire
static.auto_provision.weekly.dayofweek

```
static.auto_provision.weekly.begin_time
static.auto_provision.weekly.end_time
static.auto_provision.flexible.enable
static.auto_provision.flexible.interval
static.auto_provision.flexible.begin_time
static.auto_provision.flexible.end_time
static.auto_provision.dns_resolv_nretry
static.auto_provision.dns_resolv_timeout
```

Parameter	Permitted Values	Default	Description
static.auto_provision.attempt_expired_time	Integer from 1 to 300	20	It configures the timeout (in seconds) to transfer a file via auto provisioning. It has a higher priority than the value defined by the parameter "static.network.attempt_expired_time".
static.network.attempt_expired_time[1]	Integer from 1 to 20	10	It configures the timeout (in seconds) to transfer a file for an HTTP/HTTPS connection. It has a lower priority than the value defined by the parameter "static.auto_provision.attempt_expired_time".
static.auto_provision.att	Integer from 1 to 10	3	It configures the maximum number of attempts to transfer a file before the transfer fails during auto provisioning.

empt_before_failed			
static.auto_provision.retry_delay_after_file_transfer_failed	Integer from 0 to 300	5	It configures the time (in seconds) to wait after a file transfer fails before retrying the transfer via auto provisioning.
static.auto_provision.reboot_force.enable[1]	**0**-Disabled **1**-Enabled	Blank	It enables or disables the phone to reboot after auto provisioning, even if there is no specific configuration requiring a reboot. 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).

static.auto_provision.power_on	**0**-Off **1**-On, the phone performs auto provisioning when powered on.	1	It triggers the power on feature to turn on or off.
static.auto_provision.repeat.enable	**0**-Off **1**-On	0	It triggers the repeated feature to turn on or off.
static.auto_provision.repeat.minutes	Integer from 1 to 43200	1440	It configures the interval (in minutes) for the phone to perform auto provisioning repeatedly. It works only if "static.auto_provision.repeat.enable" is set to 1 (On).
static.auto_provision.weekly.enable	**0**-Off **1**-On, the phone performs an auto provisioning process weekly.	0	It triggers the weekly feature to turn on or off.
static.auto_provision.weekly_u	Integer from 0 to 12	0	It configures the time interval (in weeks) for the phone to perform auto provisioning. If it is set to 0, the phone performs auto provisioning on

pgrade_interval			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 "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	Integer from 0 to 120	0	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 provisioning when you are using the phone during office hour. It works only if "static.auto_provision.weekly.enable" is set to 1 (On). The operations on the handset will not change the inactive status; only the functional operations related base station, such as calling, will change the inactive status.
static.auto_provision.weekly.dayofweek	0,1,2,3,4,5,6 or a combination of these digits **0**-Sunday **1**-Monday **2**-Tuesday **3**-Wednesday **4**-Thursday **5**-Friday **6**-Saturday	01 23 45 6	It configures the days of the week for the phone to perform auto provisioning weekly. Example: static.auto_provision.weekly.dayofweek = 01 If static.auto_provision.weekly_upgrade_interval is set to 0, it means the phone performs auto provisioning every Sunday and Monday. If static.auto_provision.weekly_upg

			rade_interval is set to other value (for example, 3), it means the phone performs auto provisioning by randomly selecting a day from Sunday and Monday every three weeks. It works only if "static.auto_provision.weekly.enable" is set to 1 (On).
static.auto_provision.weekly.begin_time static.auto_provision.weekly.end_time	Time from 00:00 to 23:59	00:00	It configures the starting/ending time of the day for the phone to perform auto provisioning weekly. It works only if "static.auto_provision.weekly.enable" is set to 1 (On).
static.auto_provision.flexible.enable	**0**-Off **1**-On, the phone performs auto provisioning at random between a starting time configured by the parameter static.auto_provision.flexible.begin_time and an ending time configured by the parameter static.auto_provision.flexible.end_time on a random day within the period configured by the parameter	0	It triggers the flexible feature to turn on or off. The day within the period is based on the phone's MAC address and does not change with a reboot, whereas the time within the start and end is calculated

	static.auto_provision.flexible.interval.		again with every reboot. The timer starts again after each auto provisioning.
static.auto_provision.flexible.interval	Integer from 1 to 1000	30	It configures the interval (in days) for the phone to perform auto provisioning. The auto provisioning occurs on a random day within this period based on the phone's MAC address. The phone performs auto provisioning on a random day (for example, 18) based on the phone's MAC address. It works only if "static.auto_provision.flexible.enable" is set to 1 (On).
static.auto_provision.flexible.begin_time	Time from 00:00 to 23:59	02:00	It configures the starting time of the day for the phone to perform auto provisioning at random. It works only if "static.auto_provision.flexible.enable" is set to 1 (On).
static.auto_provision.flexible.end_	Time from 00:00 to 23:59	Blank	It configures the ending time of the day for the phone to perform auto provisioning at random. If it is left blank or set to a specific value equal to the

time			starting time configured by the "parameter static.auto_provision.weekly.begin_time", the phone performs auto provisioning at the starting time. If it is set to a specific value greater than 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_reso	Integer from 1 to 10	2	It configures the retry times when the phone fails to resolve the access URL of the provisioning server. For each different DNS server, it works only if

lv_nretry			"static.auto_provision.dns_resolv_nosys" is set to 1 (Enabled).
static.auto_provision.dns_resolv_timeout	Integer from 1 to 60	5	It configures the timeout (in seconds) for the phone to retry to resolve the access URL of the provisioning server. For each different DNS server, it works only if "static.auto_provision.dns_resolv_nosys" is set to 1 (Enabled).

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

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	Permitted Values	Default	Description
static.auto_provision.server.type	**1**-http **2**-https **3**-ftp **4**-	tftp	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".

	sftp **Other values**- tftp		
static.auto_provision.user_agent_mac.enable[1]	**0**-Disabled **1**-Enabled	1	It enables or disables the phone's MAC address to be included in the User-Agent header of HTTP/HTTPS requests via auto provisioning.

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

Supported Provisioning Server Discovery Methods

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

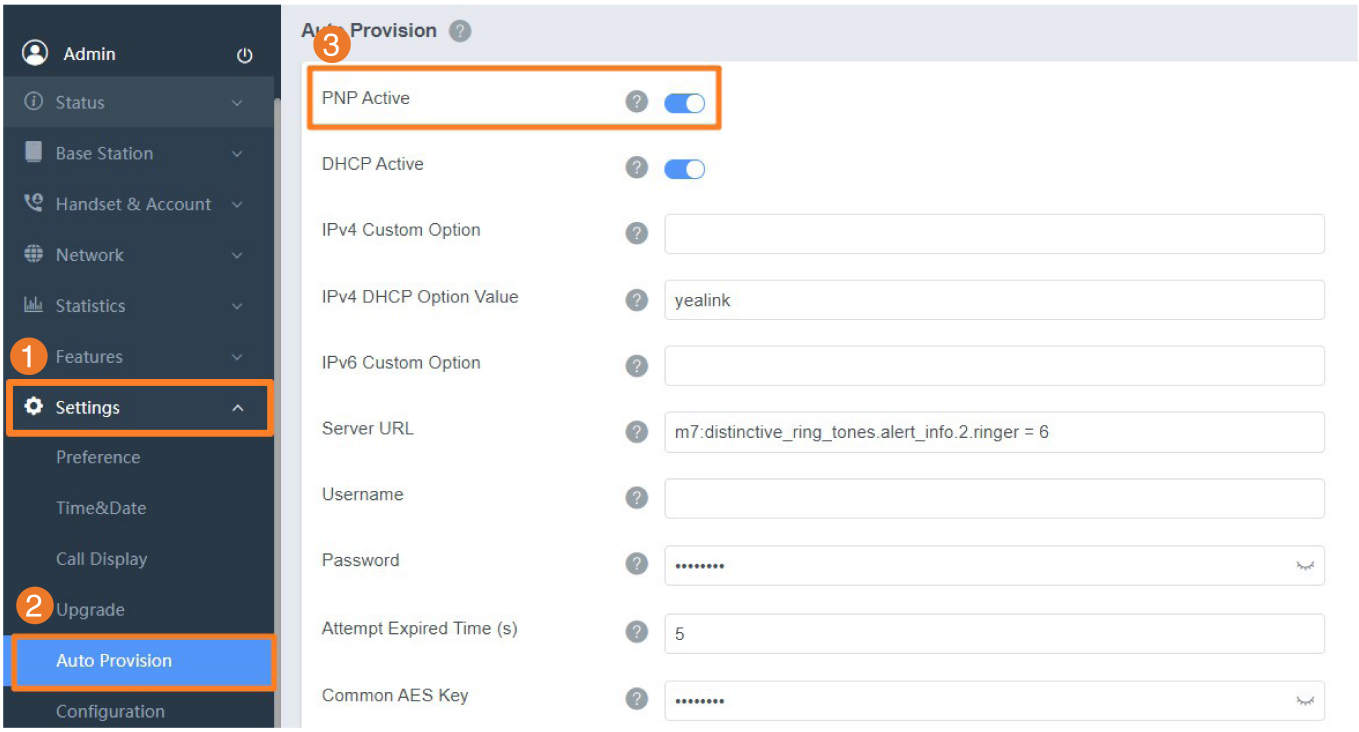
The IP phone supports the following methods to discover the provisioning server address:

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

PnP Provision Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Auto Provision** > **PNP Active**.



Configuration Parameter

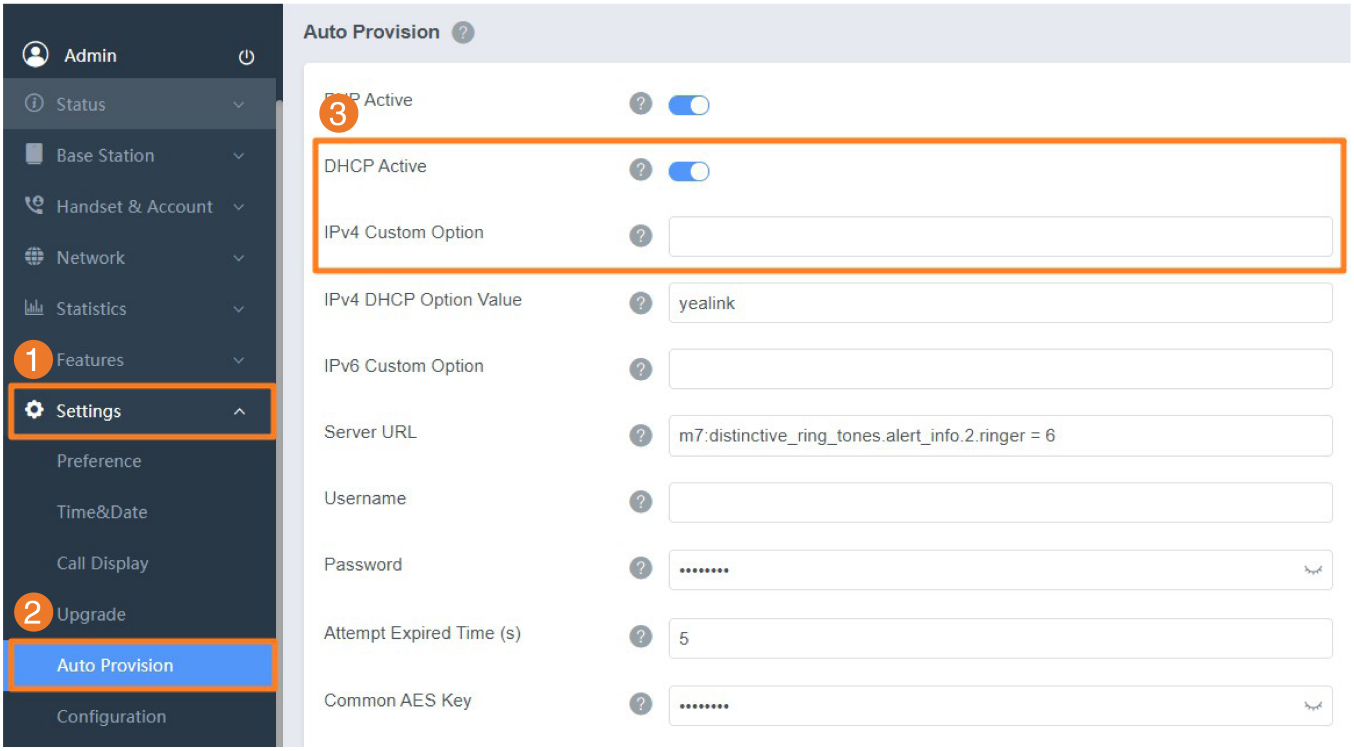
static.auto_provision.pnp_enable

Parameter	Permitted Values	Default	Description
static.auto_provision.pnp_enable	**0**-Off **1**-On, the phone broadcasts SIP SUBSCRIBE messages to obtain a provisioning server URL where the phone can request the configuration from during startup.	1	It triggers the Plug and Play (PnP) feature to turn on or off.

DHCP Provision Configuration

Set via the Web User Interface

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



Configuration Parameter

static.auto_provision.dhcp_option.enable
static.auto_provision.dhcp_option.list_user_options
static.auto_provision.url_wildcard.pn

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

static.auto_provision.url_wildcard.pn	String within 32 characters	Blank	It configures the characters to replace the wildcard $PN in the received URL of the provisioning server. The configured characters must be in accordance with the actual directory name of the provisioning server.

Static Provision Configuration

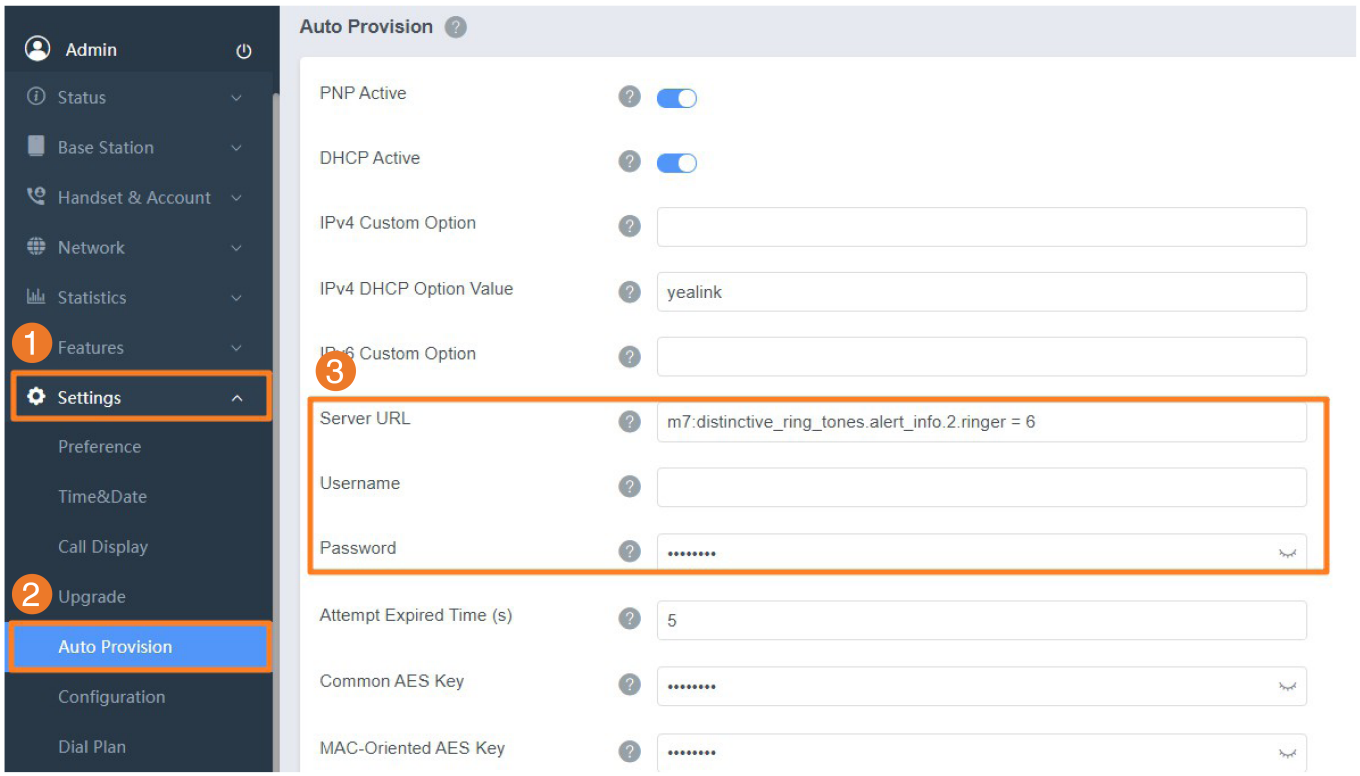
To use the static provision method, you need to obtain the provisioning server address first when configuring a provisioning server.

The provisioning server address can be an IP address, a domain name, or a 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.

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**.



Configuration Parameter

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

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

Configure a Provisioning Server

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

To set up the provisioning server:

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

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 timely maintain company phones via auto provisioning, yet some users would like to keep the personalized settings after auto provisioning.

Keep User's Personalized Settings Configuration

The following table lists the parameters you can use to keep the user's personalized settings.

```
static.auto_provision.custom.protect
static.auto_provision.custom.sync
static.auto_provision.custom.sync.path
static.auto_provision.custom.upload_method
static.auto_provision.handset_configured.enable
static.auto_provision.custom.handset.protect
```

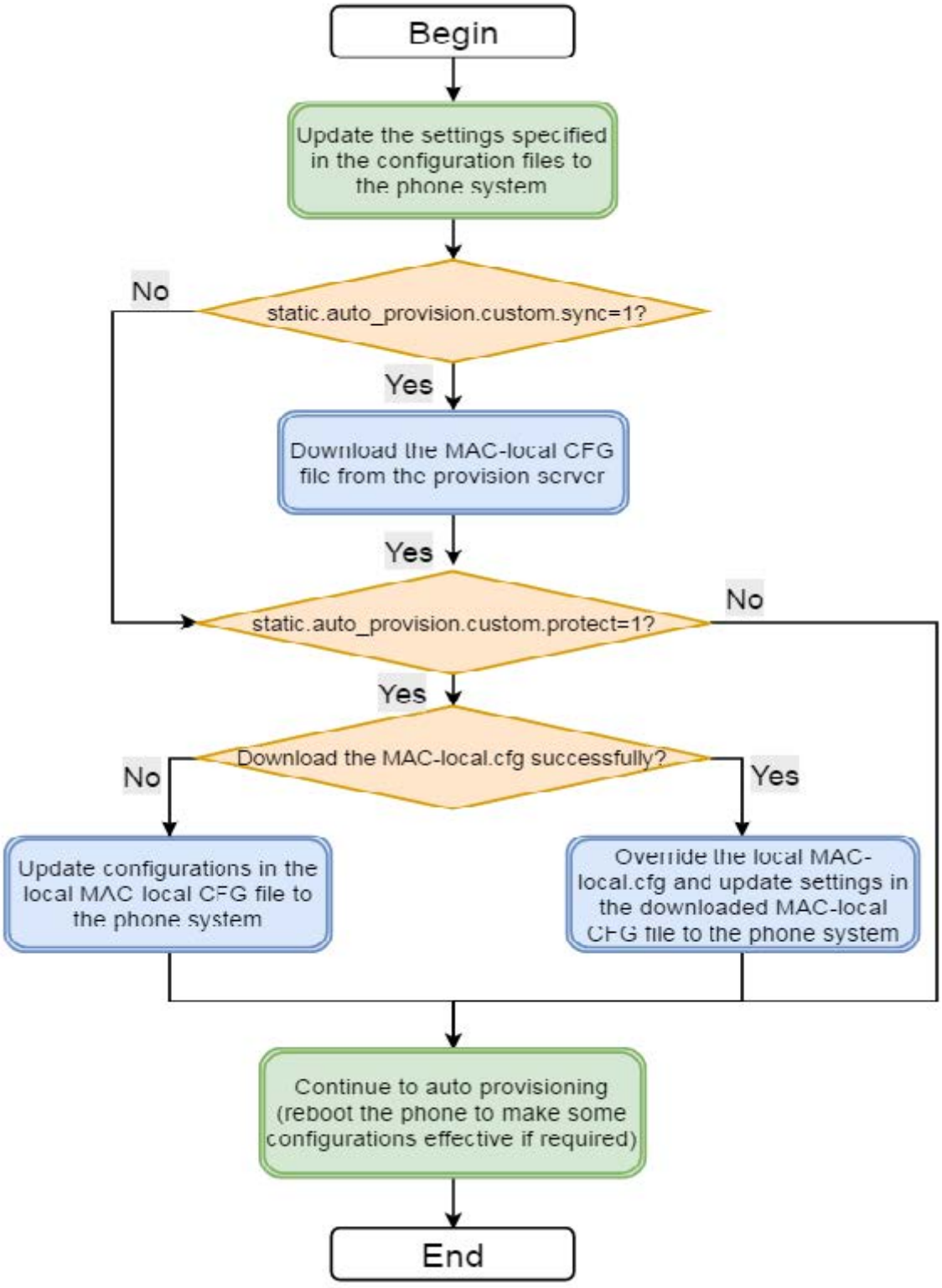
Parameter	Permitted Values	Default	Description
static.auto_provision.custom.protect	**0**-Disabled **1**-Enabled, <MAC>-local.cfg file generates and personalized non-static settings configured via the web or handset user interface will be kept after auto provisioning.	0	It enables or disables the phone to keep the user's personalized settings after auto provisioning. The provisioning priority mechanism (**handset/web user interface** > **central provisioning** > **factory defaults**) takes effect only if the value of this parameter is set to 1 (Enabled). If "overwrite_mode" is set to 1 in the boot file, the value of this parameter will be set to 1 (Enabled). It is not applicable to the custom

			handset related configurations.
static.auto_provision.custom.sync	**0**-Disabled **1**-Enabled	0	It enables or disables the phone to upload the <MAC>-local.cfg file to the server each time the file updates, and to download the <MAC>-local.cfg file from the server during auto provisioning. It works only if "static.auto_provision.custom.protect" is set to 1 (Enabled). The upload/download path is configured by the parameter "static.auto_provision.custom.sync.path".
static.auto_provision.custom.sync.path	URL	Blank	It configures the URL for uploading/downloading the <MAC>-local.cfg file. If it is left blank, the phone will try to upload/download the <MAC>-local.cfg file to/from the provisioning server. It works only if "static.auto_provision.custom.sync" is set to 1 (Enabled).
static.auto_provision.custom.upload_method	**0**-PUT **1**-POST	0	It configures the way the phone uploads the <MAC>-local.cfg file, <MAC>-calllog.xml file or <MAC>-contact.xml file to the provisioning server (for HTTP/HTTPS server only).
static.auto_provision.handset_confi	**0**-Disabled, the custom handset settings can be only changed via the handset user interface. **1**-Enabled, when the parameter	1	It enables or disables the base station to deliver custom handset configurations to the handset via auto provisioning/handset reboot/handset registration.

gured.enable	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.		It is only applicable to the custom handset related configurations.
static.auto_provision.custom.handset.protect	**0**-Disabled **1**-Enabled	1	It enables or disables the handsets to keep user personalized settings after auto provisioning/handset reboot/ handset registration. 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 users' 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 user interface or web user interface, the MAC-local.cfg file with non-static personal settings is generated locally.

Scenario: Keep the users' 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, and then update settings in MAC-local.cfg file 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 the users' personalized settings after factory reset

The phone requires a factory reset when it breaks down, but the user wishes to keep the personalized 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 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 locally are cleared, 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, and 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 Users' Personalized Configuration Settings

When the IP phone is given to a new user, but many personalized configuration 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 next auto provisioning.

Custom Handset Related Configurations

This section shows you the custom handset-related configurations.

Parameter	Related Topic
custom.handset.date_format	Time and Date Format Configuration
custom.handset.time_format	Time and Date Format Configuration
custom.handset.auto_answer.enable	Auto Answer Configuration
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 Backlight Configuration
custom.handset.backlight_out_of_charger.enable	Handset Backlight Configuration
custom.handset.screen_saver.enable	Handset Screen Saver Configuration
custom.handset.language	Language Display Configuration

Backup to an SFTP Provisioning Server

Introduction

The phone supports automatic periodic backups of contacts, call history, and CFG files containing all settings to a specified SFTP server.

Configuration Parameter

auto_provision.server.type
auto_provision.period_backup.enable

Parameter	Permitted Values	Default	Description
auto_provision.server.type	**1**-http **2**-https **3**-ftp **4**-sftp **Other values**-tftp	tftp	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" .
auto_provision.period_backup.enable	**0**-Disabled **1**-Enabled	0	It configures the enable/disable setting for the scheduled backup feature.
auto_provision.backup.period	1-365, represents 1 to 365 days	0	It configures the repetition interval of the scheduled backups.
auto_provision.backup.time	hh:mm or hh:mm-hh:mm (hh:mm value is 00:00 to 23:59) When the configuration	00:00	It configures the repetition time of the scheduled backups.

	value is set to hh:mm, it indicates the exact time it takes effect. When set to hh:mm-hh:mm, it indicates a random time within that period.		

DECT Manager and Base Update

Introduction

You can upgrade the DM/Base via auto-provision and web user interface.

Firmware Version

You can download the latest firmware online: Yealink Support.

- For the W80 Multi-Cell system, if your firmware version is very old, you need to contact the Yealink technical staff and ask for an interim version (103.83.0.79) to upgrade.
- After updating W80DM or W80B to the latest firmware version 103.83.0.90. Due to company policy and specific external reasons, switching mode between Base and DM is no longer allowed, and neither is DM-Base mode. Please make sure that you will have at least one DM as a manager for all base stations.

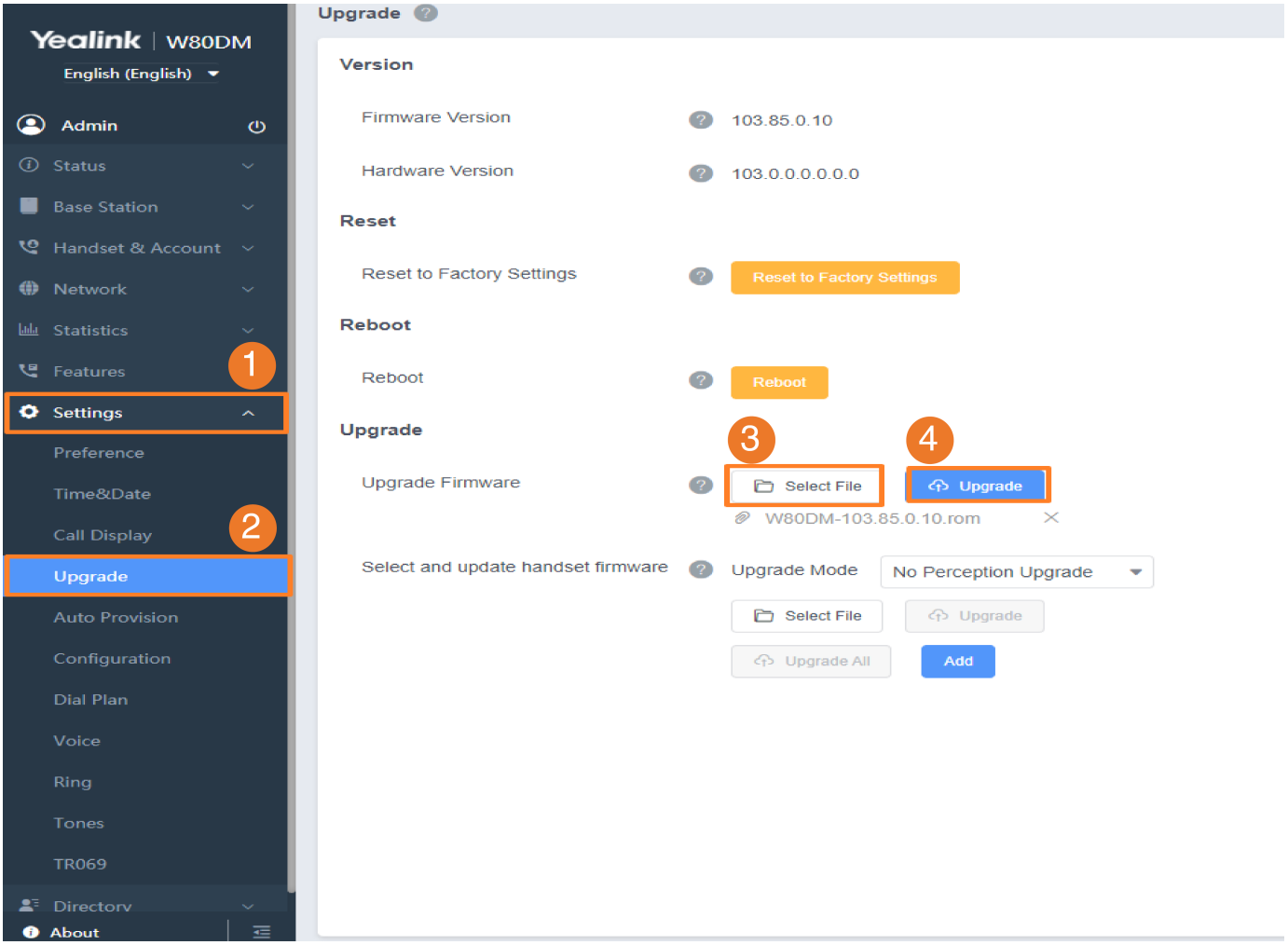
Firmware Upgrade Configuration

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 cables and power cables when the device is upgrading firmware.

Set via the Web User Interface

1. On the DM/Base web user interface, go to **Settings** > **Upgrade** >**Upgrade Firmware**.
2. Click **Select File**.
3. Click **Upgrade**.



Configuration Parameter

static.firmware.url

Parameter	Permitted Values	Default	Description
static.firmware.url	URL within 511 characters	Blank	It configures the access URL of the firmware file. When upgrading the DM, the registered base station will be upgraded automatically.

Update DD Phone

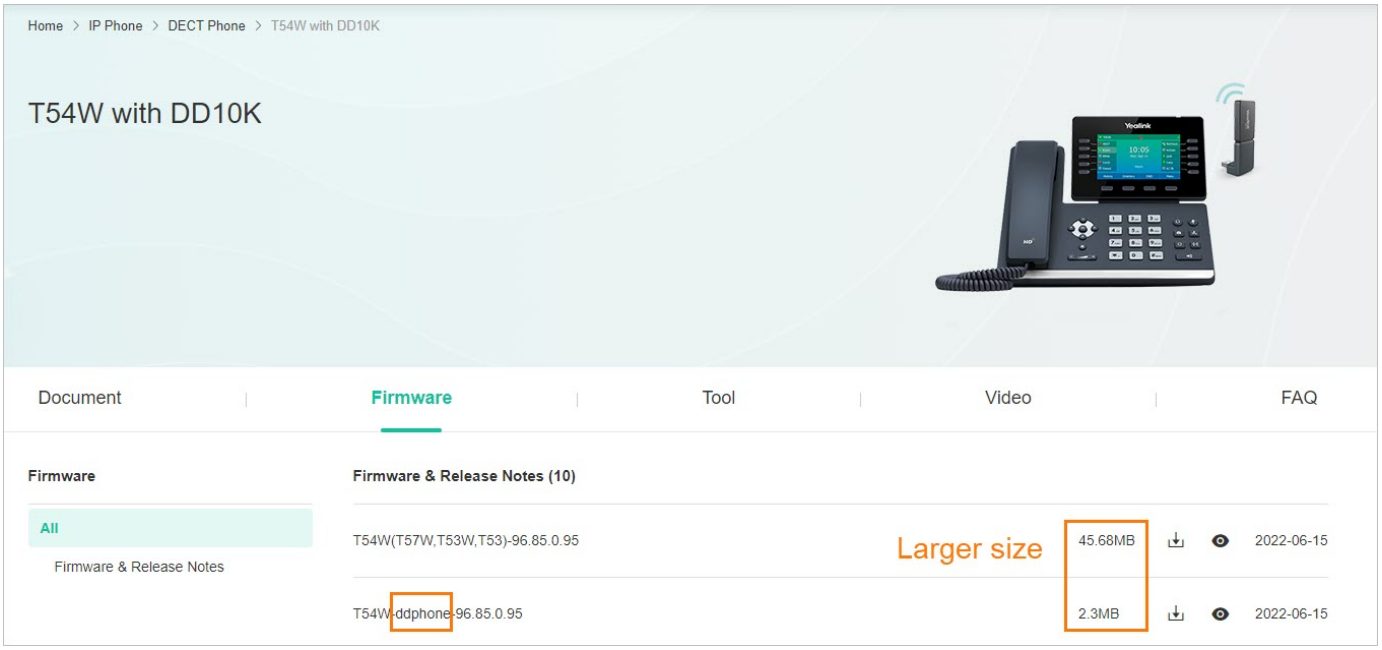
Before You Begin

Understand Two Upgrading Modes

There are two modes to upgrade firmware: SIP mode and DD phone mode. Therefore, the firmware ROM files for the two modes are different.

Please use the correct ROM file for the corresponding mode. Otherwise, it may fail to upgrade the firmware.

Mode	Introduction	Required Firmware ROM File	Differences between two ROM files
SIP mode	You have not turned the phone into a DD phone.	The ROM file with a larger size.	This ROM file supports the functions of both modes.
DD phone mode	You have turned the phone into a DD phone.	The ROM file with a smaller size and has a *"ddphone"* for identification.	This ROM file supports OTA (Over-the-Air) updates and only the DD phone mode.



Check the Firmware Version

To check the firmware version via the device user interface:

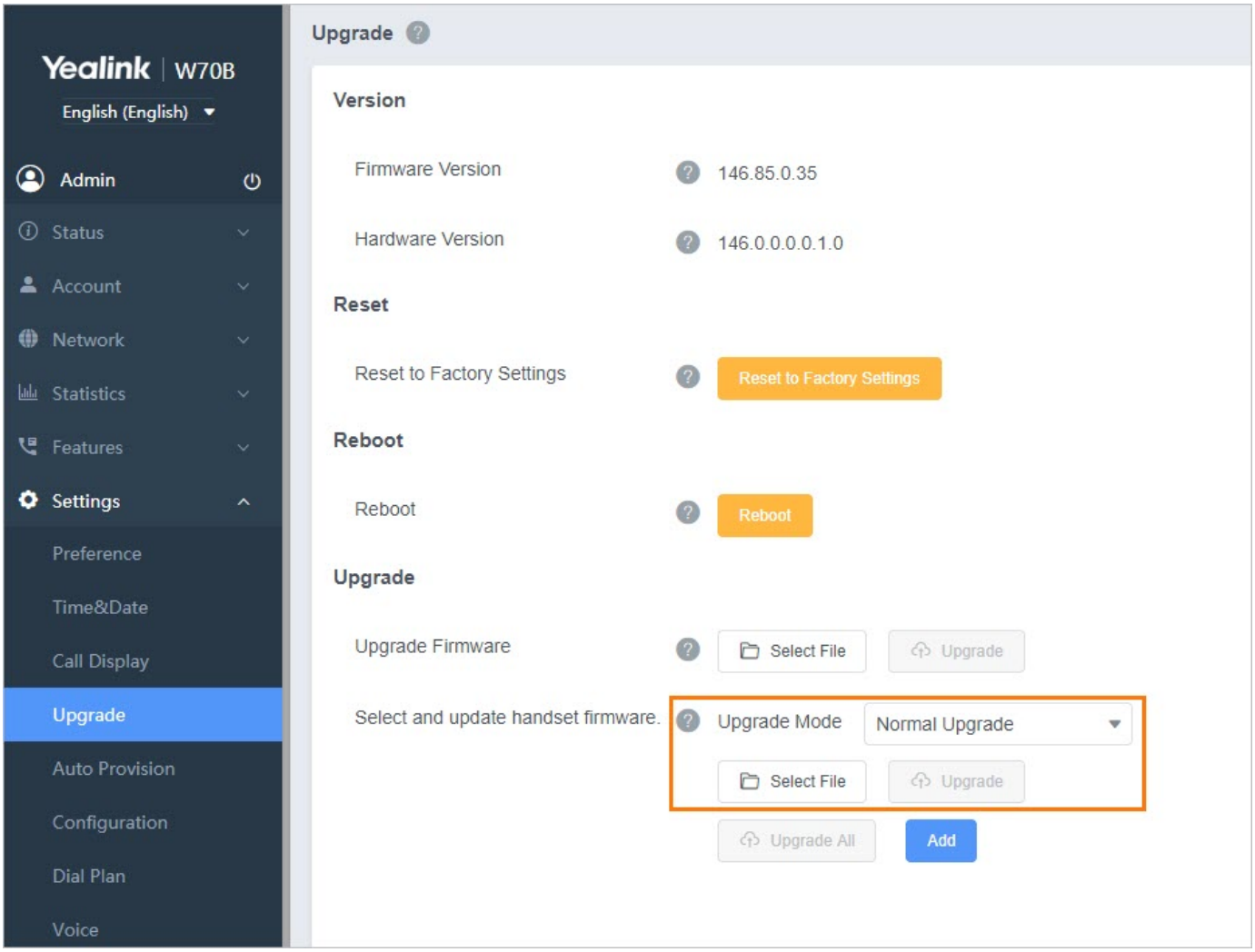
- In the DD phone mode, go to **Menu** >**Status** > **Phone Status** > **OTA Version (T41S/T42S)/ Firmware(T54W)**.
- In the SIP mode, press the OK key when the phone is idle.

Upgrade in the DD Phone Mode

If you have turned the phone into DD phone mode, you can upgrade the phone using the **smaller-size** ROM file.

Via Web User Interface

1. Press the OK key when the phone is idle to obtain the base's IP address.
2. Enter the IP address into a web browser on your computer to access the base web user interface.
3. Go to **Settings** > **Upgrade** > **Select and upgrade handset firmware**.
4. Select the desired mode from the drop-down menu of **Upgrade Mode**.
5. Click **Select File** to select the smaller-size ROM file.
6. Click **Upgrade** and click **OK** to upgrade the firmware.



Configuration Parameter

```
over_the_air.url
```

Example, over_the_air.url = http://192.168.1.20/T54W-ddphone-96.85.0.95.rom

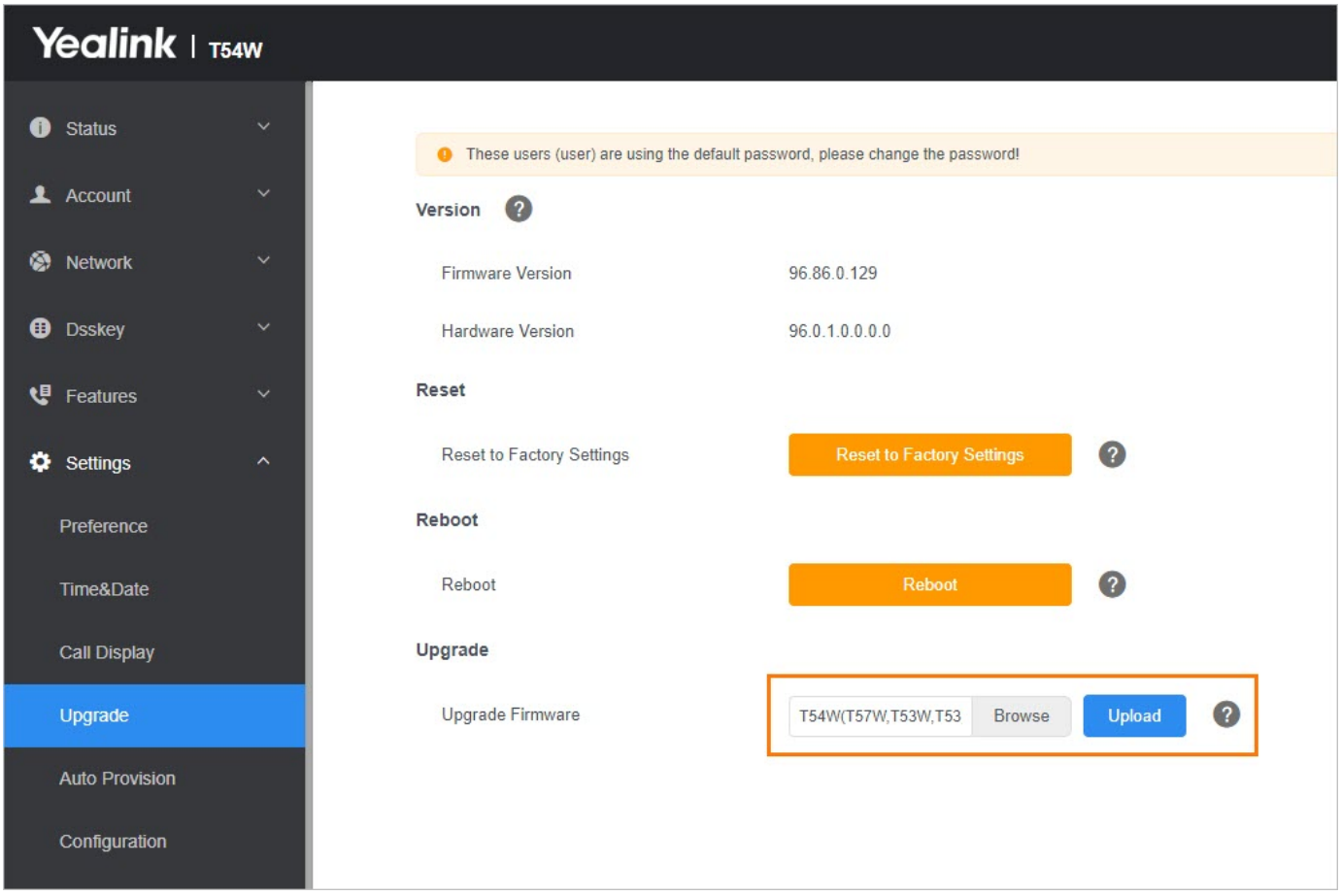
Parameters	Permitted Values	Description
over_the_air.url	URL within 511 characters	It configures the access URL of the firmware file.

Upgrade the SIP Phone Mode

If you have not turned the phone into DD phone mode, you can upgrade the phone using the **larger-size** ROM file.

Via Web User Interface

1. Press the OK key when the phone is idle to obtain the IP address of the phone.
2. Enter the phone's IP address into the web browser on your computer to access the T41S/T42S/T54W web user interface.
3. Go to **Settings** > **Upgrade** > **Select And Upgrade Firmware/Upgrade Firmware**.
4. Click **Browse** to select a larger-size ROM file.



5. Click **Upload** and click OK to upgrade the firmware.
6. After upgrading successfully, disconnect the Ethernet cable and attach the DD10K to the IP phone.

7. The phone screen prompts you whether to switch to the DD phone mode.

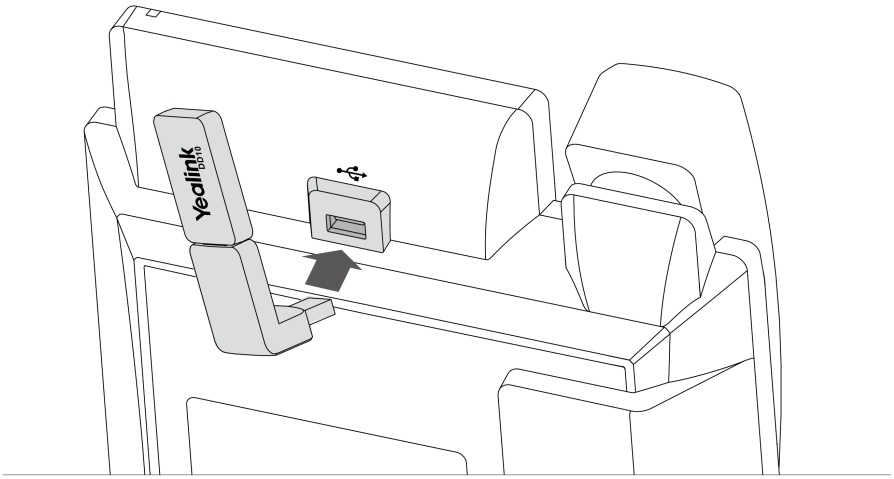
7. Press the **OK** soft key to continue, and the phone switches to the DD phone mode after rebooting.

Configuration Parameter

1. Push the following configuration line to the T41S/T42S/T54W.
2. static.firmware.url
3. Example, static.firmware.url= http://192.168.1.20/T54W/T54W(T57W,T53W,T53)-96.85.0.95.rom

Parameters	Permitted Values	Description
static.firmware.url	URL within 511 characters	It configures the access URL of the firmware file.

2. After upgrading successfully, disconnect the Ethernet cable and attach the DD10K to the IP phone.
3. The phone screen prompts you to switch to the DD phone mode.



3. Press the **OK** soft key to continue, and the phone switches to the DD phone mode after rebooting.

Update Handset

Introduction

You can upgrade the handsets via auto provisioning and a web user interface.

Firmware Version

You can download the latest firmware online: Yealink Support.

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 cables and power cables when the device is upgrading firmware.

Set via the Web User Interface

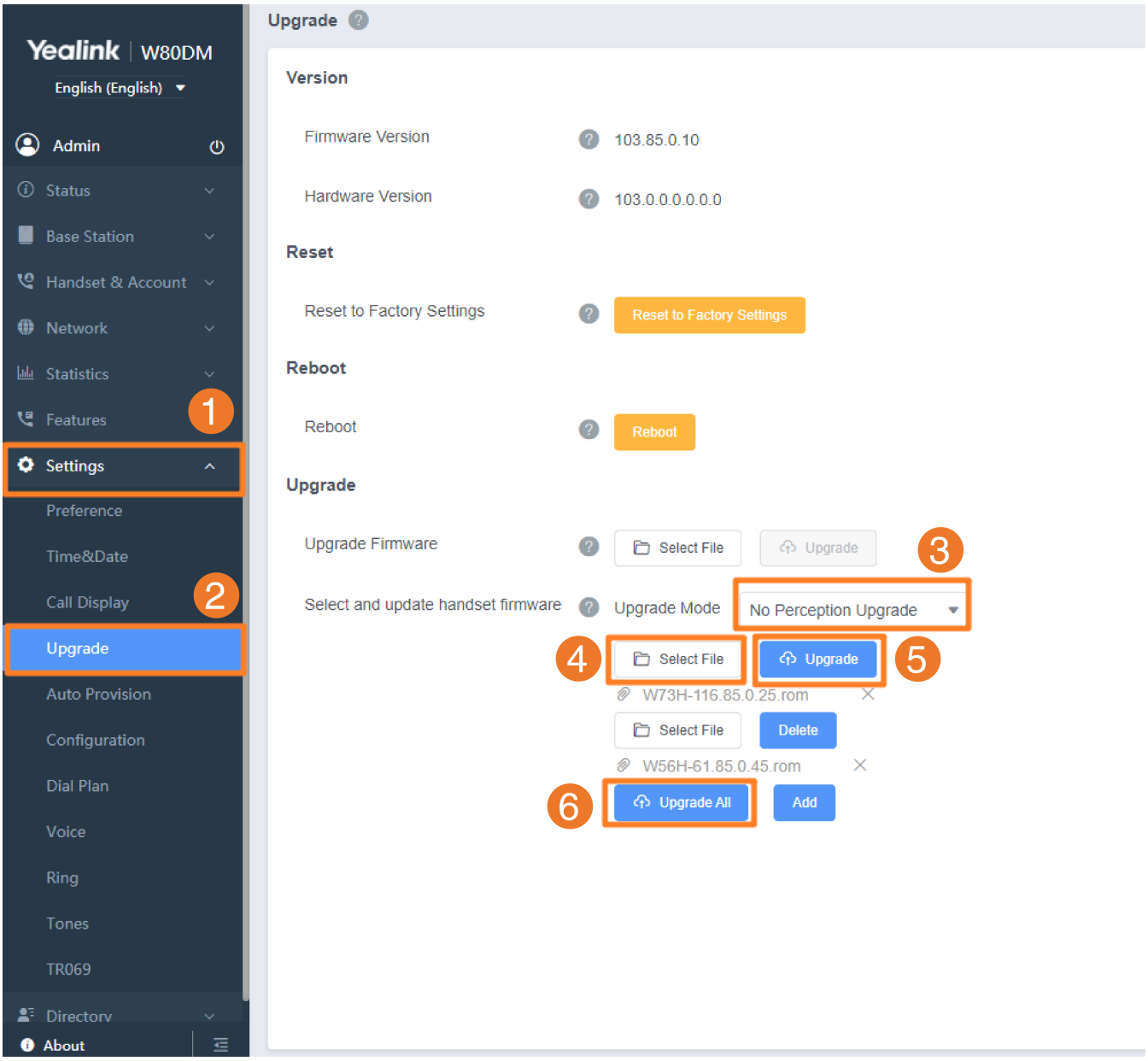
You can upgrade the handsets on the web user interface, and there are upgrade modes for you to select.

The following table compares the handset affection during the firmware transmission and upgrade process of the three models: **Normal Upgrade**, **Grayscale Upgrade**, and No Perception Upgrade.

	Transmission Process		Upgrading Process	
	handset to be upgraded can use normally	other handsets can use normally	handset to be upgraded can use normally	other handsets can use normally
Normal Upgrade	NA*	NA*	✗	✗
Grayscale Upgrade	NA*	NA*	✗	✓
No Perception Upgrade	✓	✓	✗	✓

Procedure

1. On the DM/Base web user interface, go to **Settings** > **Upgrade** >**Select and update handset firmware**.
2. Select the desired upgrading mode in the **Upgrade Mode** field.
3. Click **Select File** and then **Upgrade**.
4. If you want to upgrade more than one handset together, click **Add** and then **Upgrade All**. The system will upgrade the handset one by one according to the order in which you import the firmware.



Configuration Parameter

```
over_the_air.url
over_the_air.url.w56h
over_the_air.url.w53h
over_the_air.url.cp930w
over_the_air.url.cp935w
over_the_air.url.t41s_dd10k
over_the_air.url.w59r
over_the_air.url.w57r
over_the_air.url.w73h
over_the_air.url.w78h
```

over_the_air.url.w59r_pro

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 the parameter "over_the_air.url.w56h" 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 the parameter "over_the_air.url.w53h" 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 the parameter "over_the_air.url.cp930w" is higher than "over_the_air.url".
over_the_air.url.cp935w	URL within 512 characters	Blank	It configures the access URL of the CP935W phone firmware file. The priority of the parameter "over_the_air.url.cp935w" 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 the parameter "over_the_air.url.t41s_dd10k" 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 the parameter "over_the_air.url.w59r" is higher than "over_the_air.url".
over_the_air.url.w57r	URL within 512 characters	Blank	It configures the access URL of the W57R handset firmware file. The priority of the parameter "over_the_air.url.w57r" is higher than "over_the_air.url".
over_the_air.url.w73h	URL within 512 characters	Blank	It configures the access URL of the W73H handset firmware file. The priority of the parameter "over_the_air.url.w73h" is higher than "over_the_air.url".
over_the_air.url.w78h	URL within 512 characters	Blank	It configures the access URL of the W78H handset firmware file. The priority of the parameter "over_the_air.url.w78h" is higher than "over_the_air.url".
over_the_air.url.w59r_pro	URL within 512 characters	Blank	It configures the access URL of the W59R Pro handset firmware file. The priority of the parameter "over_the_air.url.w59r_pro" is higher than "over_the_air.url".

Update Headset

Introduction

You can upgrade the headsets via auto-provision and web user interface.

Firmware Version

You can download the latest firmware online: Yealink Support.

Firmware Upgrade Configuration

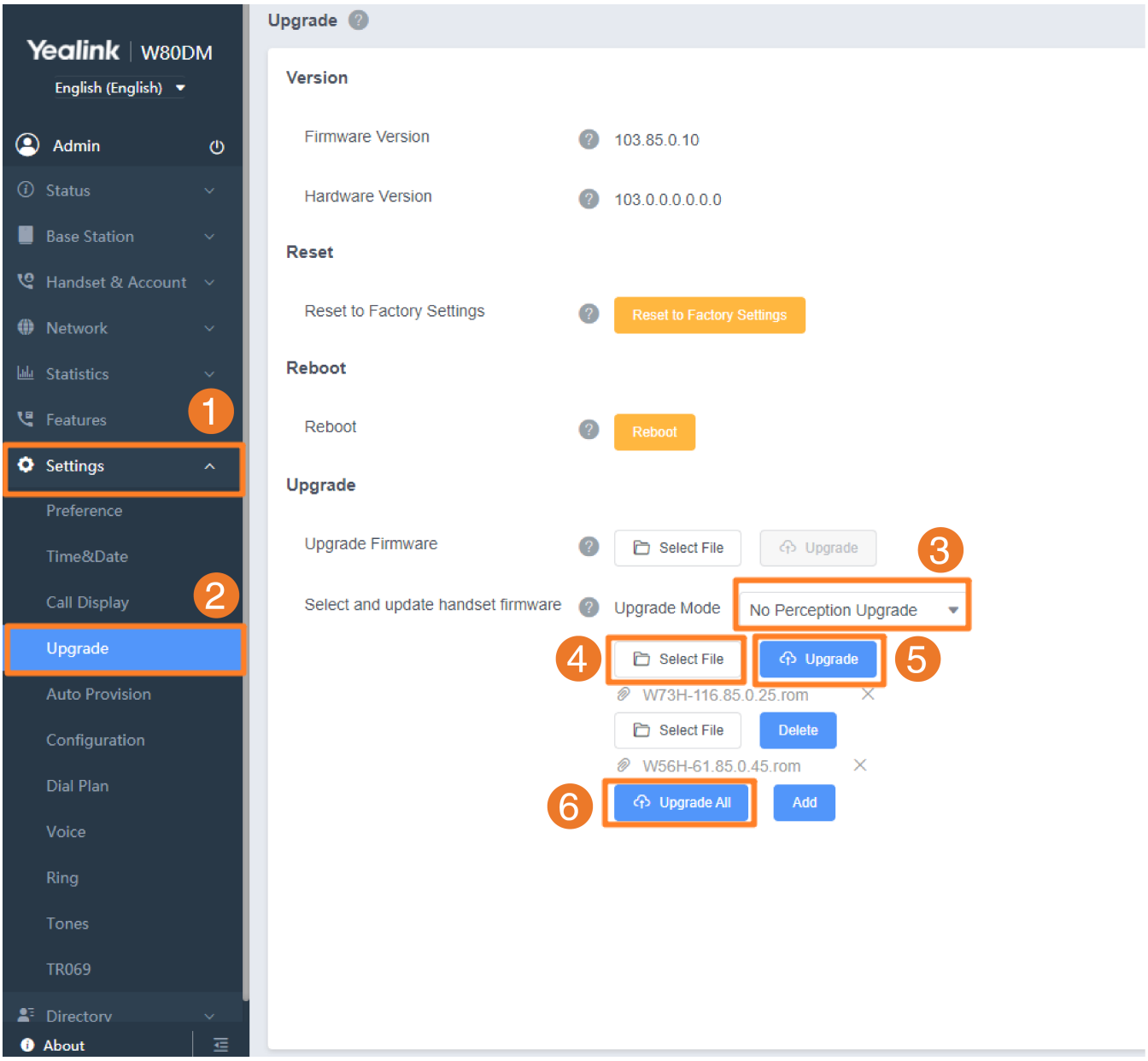
Before upgrading firmware, you need to know the following:

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

Set via the Web User Interface

Procedure

1. On the DM web user interface, go to **Settings** > **Upgrade** >**Select and update handset firmware**.
2. Select the desired upgrading mode in the **Upgrade Mode** field.
3. Click **Select File** and then **Upgrade**.
4. If you want to upgrade more than one handset together, click **Add** and then **Upgrade All**.



Configuration Parameter

over_the_air.url
over_the_air.url.wh62

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.ur	URL within 512	Blan	It configures the access URL of the headset firmware file. Applicable Device: WH62/WH63/WHM621 with Charging Cable/

l.wh62	characters	k	WHD622 with Charging Cable/WHM631 with Charging Cable/WH62 Portable/WH63 Portable The priority of parameter "over_the_air.url.wh62" is higher than "over_the_air.url".

No Perception Upgrade

Introduction

No Perception Upgrade for handsets is a new upgrade mode that separates the process of firmware transmission and firmware upgrading. Firmware transmission will not affect the normal use of the handset. You can upgrade the handset during working hours, greatly reducing the handset unavailability time. The upgrade of the handset will be completed within 2 minutes.

No Perception Upgrade Working Process

1. **Base station download firmware**: The base station supports downloading the firmware of multiple handsets at the same time. The firmware can be imported through the web user interface, or auto provisioning triggers the base station to download the firmware.
2. **Base station transfer firmware**: The base station supports simultaneous transmission of multiple types of handset firmware; the transmission process will not affect the call under the base station, and the handset can still receive calls and access LA normally. However, once the handset has a call or accesses LA during the transmission, the transfer is interrupted until the handset returns to the idle interface and resumes the transfer after 1 minute. Normally (without any interruption of transmission) base station transmits a single firmware for about wide-band 60mins and narrow-band 90mins. In the case of simultaneous transmission, multiple handsets or multiple firmware upgrades together will take 10 minutes longer.
3. **Handset installs the firmware**: The handset is installed and upgraded locally and does not need to interact with the base station during installation. The handset will prompt whether to upgrade, select Yes, and the handset will install the transferred ROM package. It will take 1-2 minutes, and the handset will be unavailable during the process, but other handsets are not affected, and the base station is working properly.

The following table compares the handset affection during the firmware transmission and upgrade process of the three models: **Normal Upgrade**, **Grayscale Upgrade**, and **No Perception Upgrade**.

	Transmission Process		Upgrading Process	
	handset to be upgraded can use normally	other handsets can use normally	handset to be upgraded can use normally	other handsets can use normally
Normal Upgrade	NA*	NA*	✗	✗
Grayscale Upgrade	NA*	NA*	✗	✓
No Perception Upgrade	✓	✓	✗	✓

The firmware transmission and upgrading process is performed simultaneously.

Applicable Handsets

This feature is only applicable to W73H, W78H, W57R, W59R, W59R Pro, W71H, and W74H.

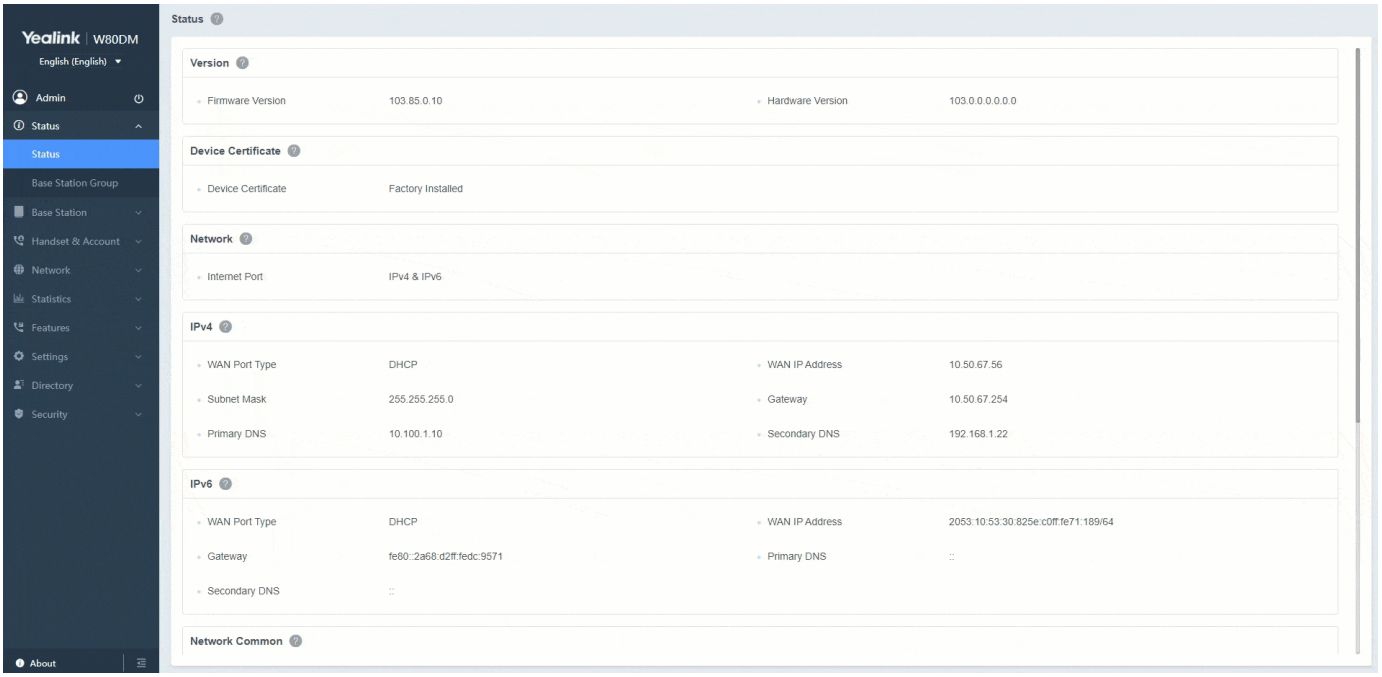
Download the Handset Firmware to the Base Station

You can trigger a no-perception upgrade mode and download the handset firmware from the web user interface or via auto-provision.

Set via the Web User Interface

Procedure

1. On the web user interface, go to **Settings** > **Upgrade**.
2. Select **No perception Upgrade** from the **Upgrade Mode** drop-down menu.
3. Click **Select File** to upload the desired firmware. You can upload up to the firmware of five handsets to upgrade a time.
4. Click **Upgrade All**. The base will download the firmware.



Configuration Parameter

Procedure

1. On the web user interface, go to **Settings** > **Auto Provision**.
2. Enter the configuration files URL in the **Server URL** field to upload the desired firmware via auto-provision.
3. Click **Auto Provision Now**. It will perform auto-provisioning immediately.

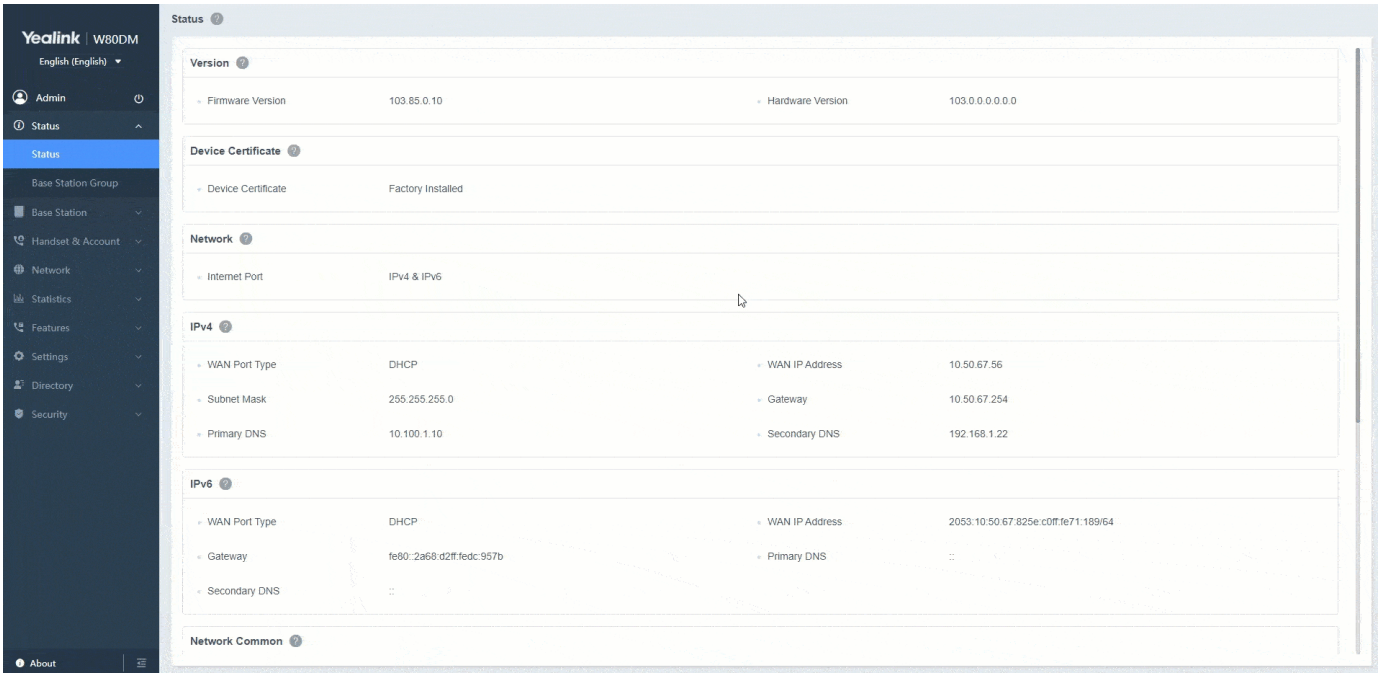
Configuration Parameter

```
over_the_air.mode
over_the_air.url.w73h
over_the_air.url.w78h
over_the_air.url.w57r
over_the_air.url.w59r
over_the_air.url.w71h
over_the_air.url.w74h
```

Parameter	Permitted Values	Default	Description
over_the_air.mode	**0**-Grayscale Upgrade, two handsets per base station one time. The upgrade does not affect the use of the remaining handsets. **1**-Normal, four handsets per base station, one time. During upgrading, other handsets are not available for the base-related operations. For example, calling, accessing the directory. **2**-No Perception Upgrade, firmware transfer is completed before launching handset upgrade.	1	It configures the mode for upgrading the handset via the web user interface/ auto provisioning.
over_the_air.url.w73h	URL within 512 characters	Blank	It configures the access URL of the W73H handset firmware file. The priority of parameter "over_the_air.url.w73h" is higher than "over_the_air.url".
over_the_	URL within 512 characters	Blank	It configures the access URL of the W78H handset firmware file.

air.url.w78h			The priority of parameter "over_the_air.url.w78h" is higher than "over_the_air.url".
over_the_air.url.w57r	URL within 512 characters	Blank	It configures the access URL of the W57R handset firmware file. The priority of parameter "over_the_air.url.w57r" 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.w71h	URL within 512 characters	Blank	It configures the access URL of the W71H handset firmware file. The priority of parameter "over_the_air.url

			.w71h" is higher than "over_the_air.url" .
over_the_air.url.w74h	URL within 512 characters	Blank	It configures the access URL of the W74H handset firmware file. The priority of parameter "over_the_air.url.w74h" is higher than "over_the_air.url" .

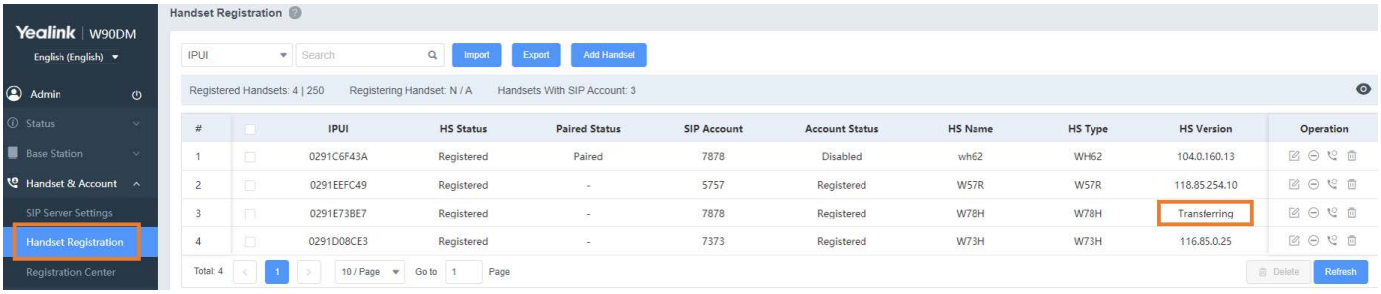


Check the Handset Firmware Transmission Status

After the base downloads the firmware, it will transmit the firmware to the handset automatically.

Procedure

1. Go to **Handset & Account** > **Handset Registration** > **HS Version** on the web user interface to check the transmitting status.



The transmitting process has two statuses: **Transferring** and **Waiting for transmission** (The transmitting process is interrupted).

- On W78H/W59R Pro: Any keystroke will interrupt the transmission.
- On W73H/W59R/W57R: When the handsets access the LA menu or establish a call will interrupt the transmission.
- If the transmission is interrupted passively by the other handsets registered on the same base (access the LA menu or establish a call, etc.), the transmission will resume within 10 minutes.
- If the handset itself actively interrupts, the transmission will resume within 1 minute.

Upgrade the Firmware

After the transmission is completed, you can upgrade the firmware on the handsets.

When the Handset is on the Charging Cradle

If the handset is on the charging cradle when the base completes the firmware transmission, it starts the firmware update process.



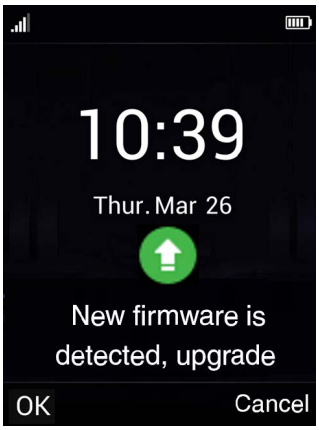
When the Handset is not on the Charging Cradle

You can manually install the firmware to the handset if the handset is not placed on the charging cradle or the handset is disabled the related parameter.

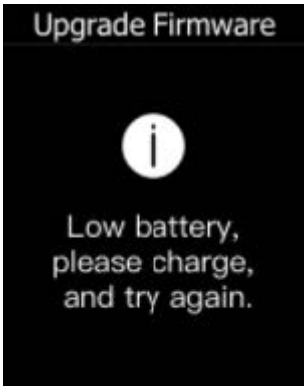
When the transmission is completed, the handset detects new firmware. It will prompt you to upgrade to the latest firmware.

- Tap **OK** to upgrade to the latest firmware.

- Tap **Cancel** to ignore.



If the handset battery is lower than 40%, when you tap **OK**, it will not upgrade.



Troubleshooting Solutions

Introduction

This section describes solutions to common issues that may occur while using the device. Upon encountering a case not listed in this section, contact your Yealink reseller for further support.

Fail to Upgrade the Phone Firmware

Do one of the following:

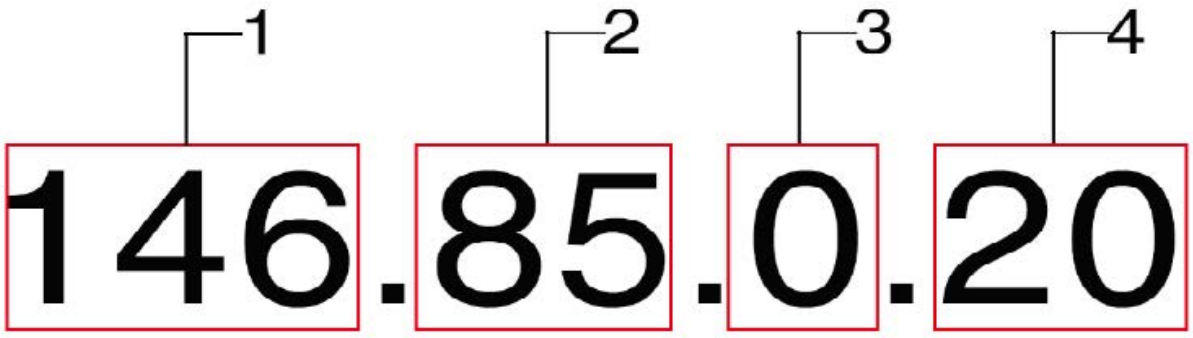
- Ensure that the target firmware is not the same as the current firmware.
- Ensure that the target firmware is applicable to the IP phone model.
- Ensure that the current or the target firmware is not protected.
- Ensure that the power is on and the network is available during the process of upgrading.
- Ensure that the web browser is not closed or refreshed when upgrading firmware via the web user interface.

Verify the Firmware Version

Go to **OK** > **Status** > **Base/Handset** when the handset is idle to check the firmware version.

For CP930W-Base phones, go to **Menu** > **Status** > **Base/Phone**.

For CP935W-Base phones, go to **More** > **Status** > **Base Status/Phone Status**. For example 146.85.0.20.



Item	Description
146	Firmware ID. The firmware ID for each device is 146.
85	Major version. The larger it is, the newer the major version is.

0	A fixed number. Generally, there is an update limitation between different numbers.
20	Minor version. With the same major version, the larger it is, the newer the minor version is.

The Phone does not Update the Configurations

Do one of the following:

- Ensure that the configuration is set correctly.
- Reboot the phone. Some configurations require a reboot to take effect.
- Ensure that the configuration is applicable to the IP phone model.
- The configuration may depend on support from a server.

Why doesn't the DECT Phone Upgrade Firmware Successfully?

Do one of the following:

- Ensure that the target firmware version is not the same as the current one.
- Ensure that the target firmware is applicable to the DECT IP phone model.
- Ensure that the current or the target firmware is not protected.
- Ensure that the power is on and the network is available in the process of upgrading.
- Ensure that the web browser is not closed or refreshed when upgrading firmware via the web user interface.
- For the handset, ensure the handset battery should not be less than 40% and is connected to the base station.

Connect DECT Devices to YDMP or YMCS

Introduction

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

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

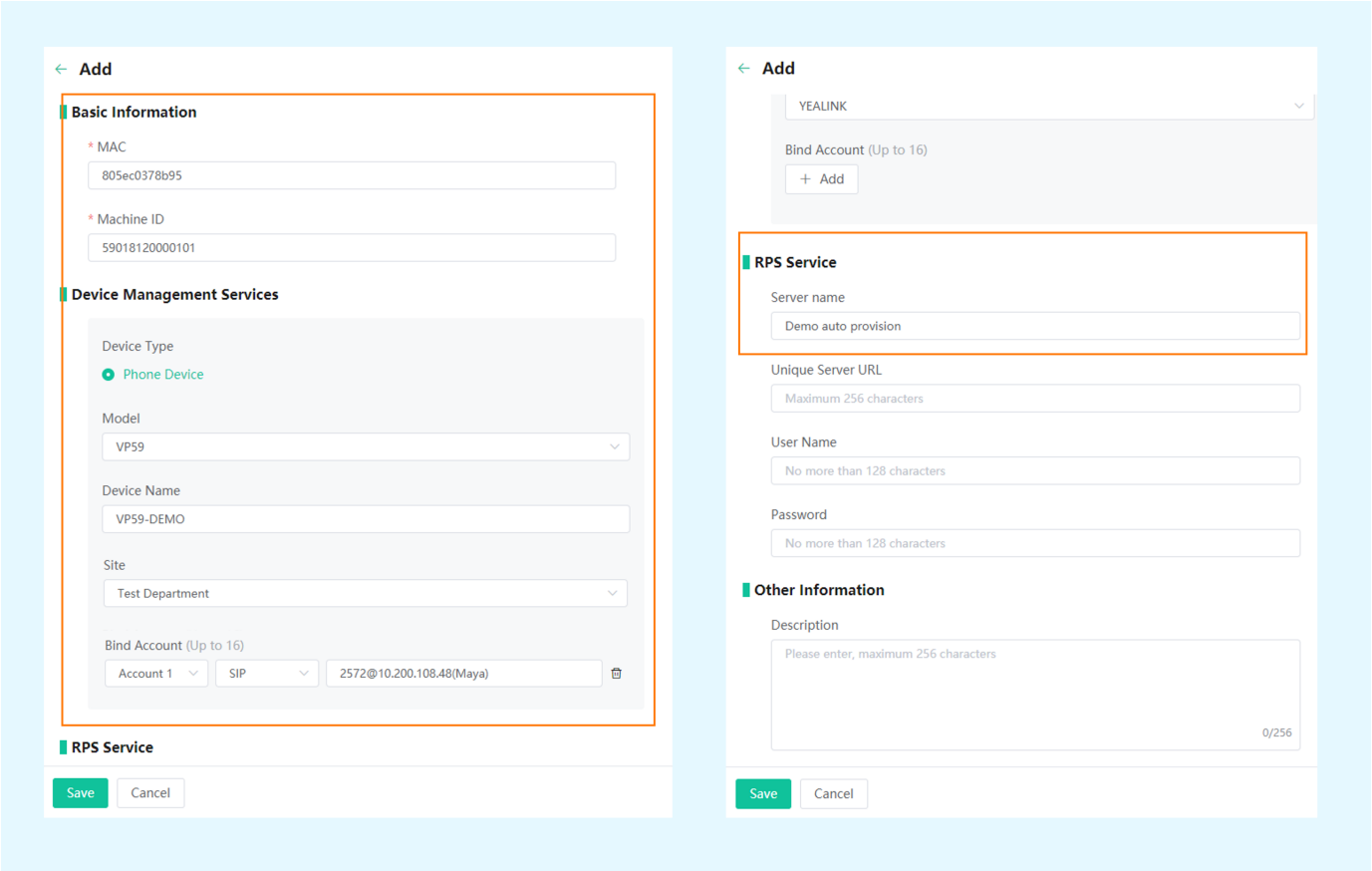
How to Connect W70B/W75DM/W80DM/W90DM to YMCS/YDMP

You can connect W70B/W75DM/W80DM/W90DM to YMCS by the following methods:

Step 1: Add Devices to the Device List (YMCS/YDMP Portal)

Add a Single Device

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

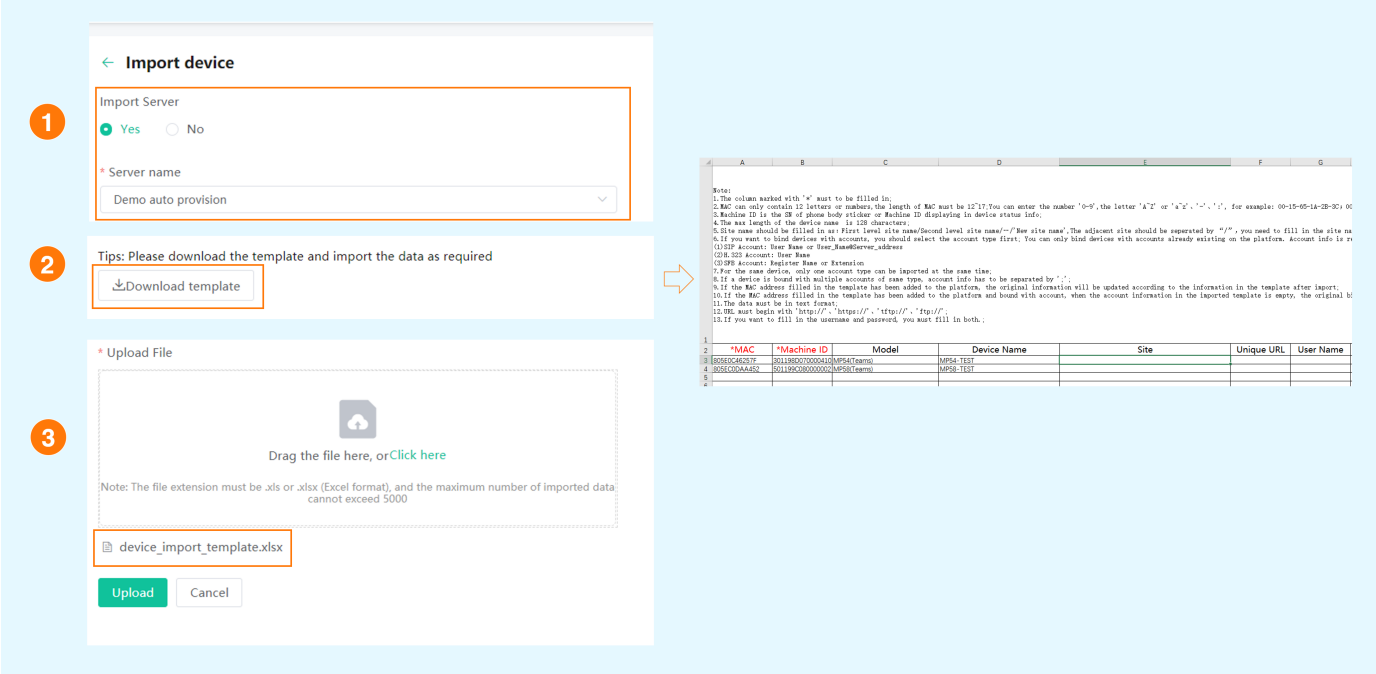


Parameter	Introduction
MAC	Enter the device's MAC address.
Machine ID	Enter the device machine ID.
Device Type	Select the device type.
Model	Select the device model.
Device Name	Enter a descriptive name for the device.
Site	Select a site for the device.
Bind Account	Select an account to bind with this device.
Server name	Select the server you added from the drop-down list. If you do not connect devices via Yealink RPS, you do not need to set this parameter.
Unique Server URL	If you do not add a server, you can add a server URL. • If you select an added server and set the unique server URL, the unique server has a higher priority than the added server. Therefore, YMCS will send the unique server URL to the device. • If you do not connect devices via Yealink RPS, you do not need to set this parameter.

User Name	Enter the user name that can access the unique server.
Password	Enter the user password.
Description	Enter the description.

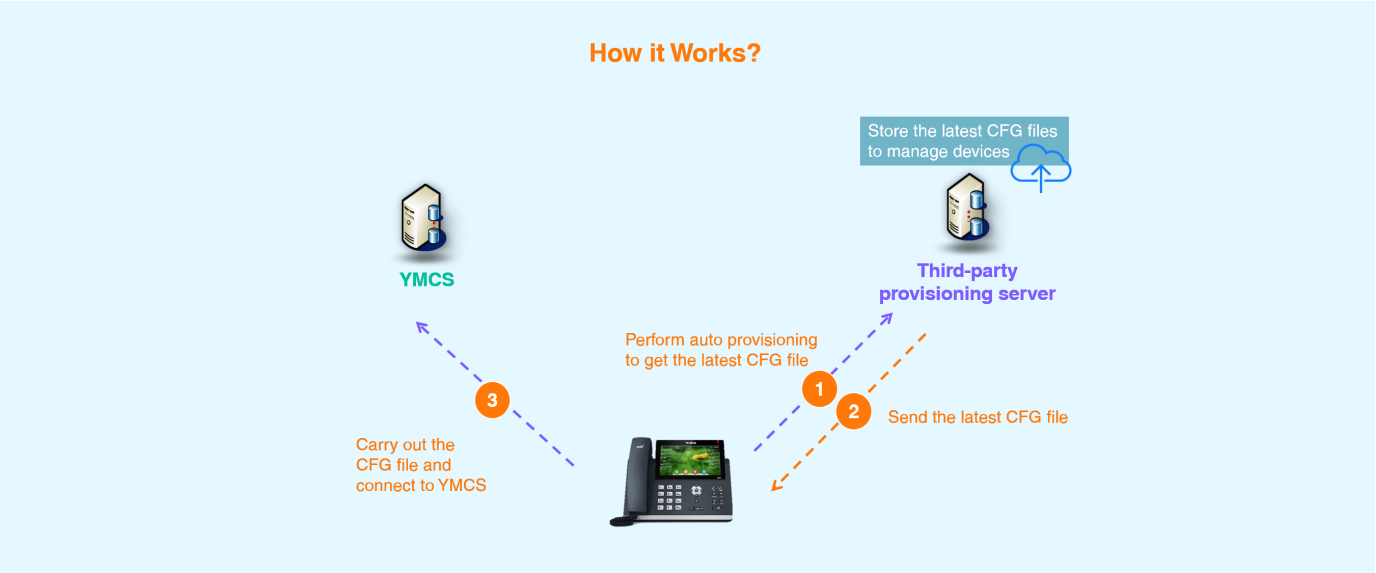
Add Multiple Devices

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



Configure Parameters via Auto Provisioning

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



Prerequisites

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

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

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

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

1. Configure the following commands:

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

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

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

Parameters	Permitted Values	Default	Description
dm.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the device management feature.
dm.server.add	String within 512	Blan	It configures the server address of the YDMP/

ress	characters	k	YMCS.
dm.server.port	Integer from 0 to 65535	443	It configures the server port of the YDMP/YMCS.

Report Handset Abnormal Status

Introduction

The handset reports its status to the base every 5 minutes through a time synchronization mechanism. The base processes this information and reports any abnormal statuses or changes to the YMCS platform.

Only applicable to W70B.

Configuration Parameter

phone_setting.auto_sync.enable
features_base.auto_send_ymcs.enable

Parameter	Permitted Values	Default	Description
phone_setting.auto_sync.enable	**0**-Disabled **1**-Enabled	0	It configures to enable/disable the handset to periodically synchronize its status information with the base.
features_base.auto_send_ymcs.enable	**0**-Disabled **1**-Enabled	0	It configures the base to report handset information, with the reporting mechanism set to trigger when there is a change in the information.

Recovery Mode

Overview

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

There are four recovery modes:

1. Using an HTTP server
2. Using a TFTP server (not applicable to CP960 IP phones)
3. Running backup system

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

Getting Started

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

1. Preparing the firmware and other resource files
2. Configuring the HTTP server, configuring the TFTP server, or connecting the USB flash drive to the IP phone

Preparing the Firmware (ROM file) and other Resource Files

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

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

The filename of the firmware used for recovery mode is strictly required. For example, to use recovery mode on W80B, you must rename the firmware file as W80.rom.

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

Phone Model	The Resource Files Required
Base for W52P/W56P	W52P.rom, W5X.bin, and W5X.rfs
W60B	W60B.rom, W60B.bin, and W60B.rfs
W70B	W70B.rom, W70B.bin, and W70B.rfs

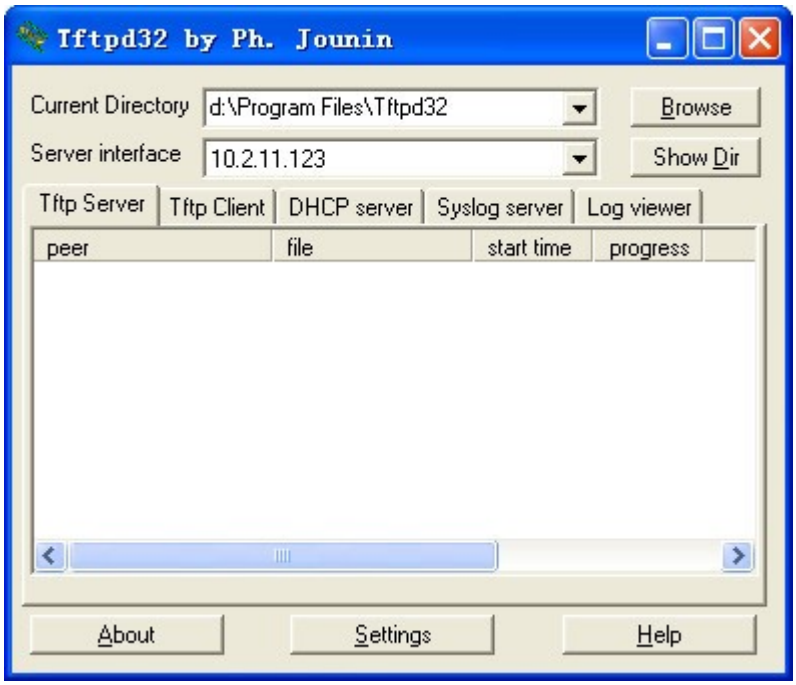
W75DM/W75B	W75B.rom, W75B.bin, and W75B.rfs
W80DM/W80B	W80B.rom, W80B.bin, and W80B.rfs
W90DM/W90B	W90B.rom and W90B.bin

Configuring the TFTP Server

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

Procedure

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



Using Recovery Mode on Yealink IP Phones (TFTP Server)

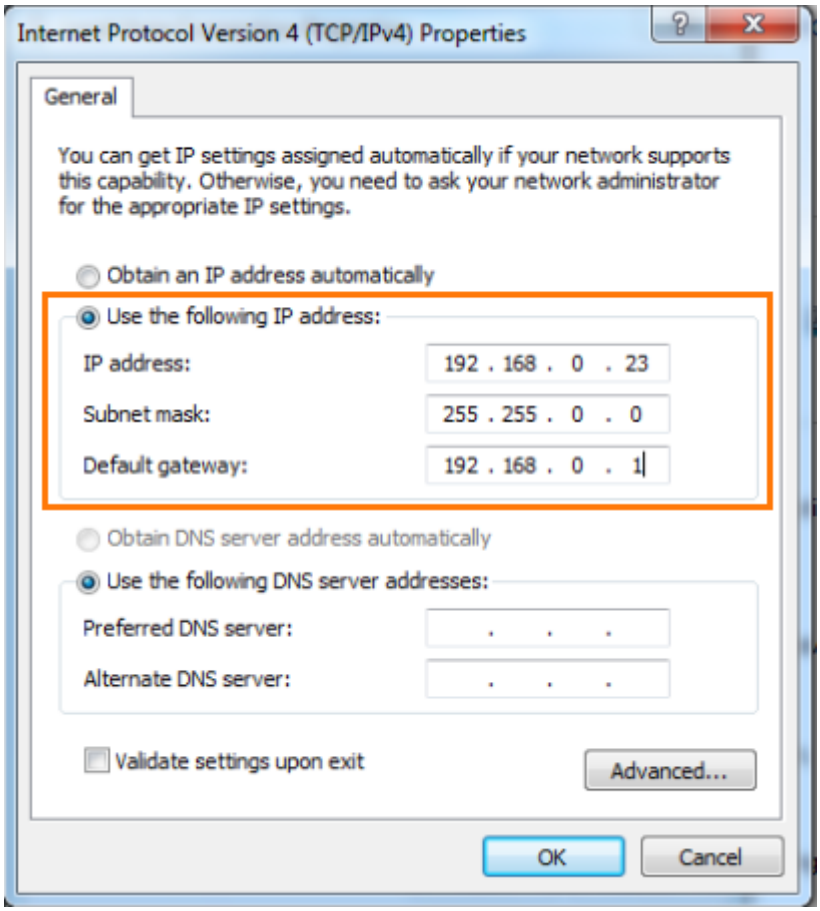
This section introduces how to perform recovery mode using the TFTP server on Yealink IP phones step by step.

For W52P/W56P/W60B/W70B Base

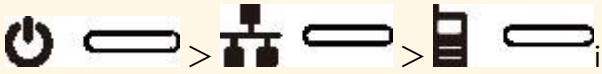
For the W52P/W56P/W60B base, there is no screen to show information for you. The W52P/W56P/W60B base uses 192.168.0.100 as its default IP address, so you need to configure a static IP address for your local PC where you have the TFTP server installed.

Procedure

1. Configure the static IP address on your local PC.
2. It must be configured as below:

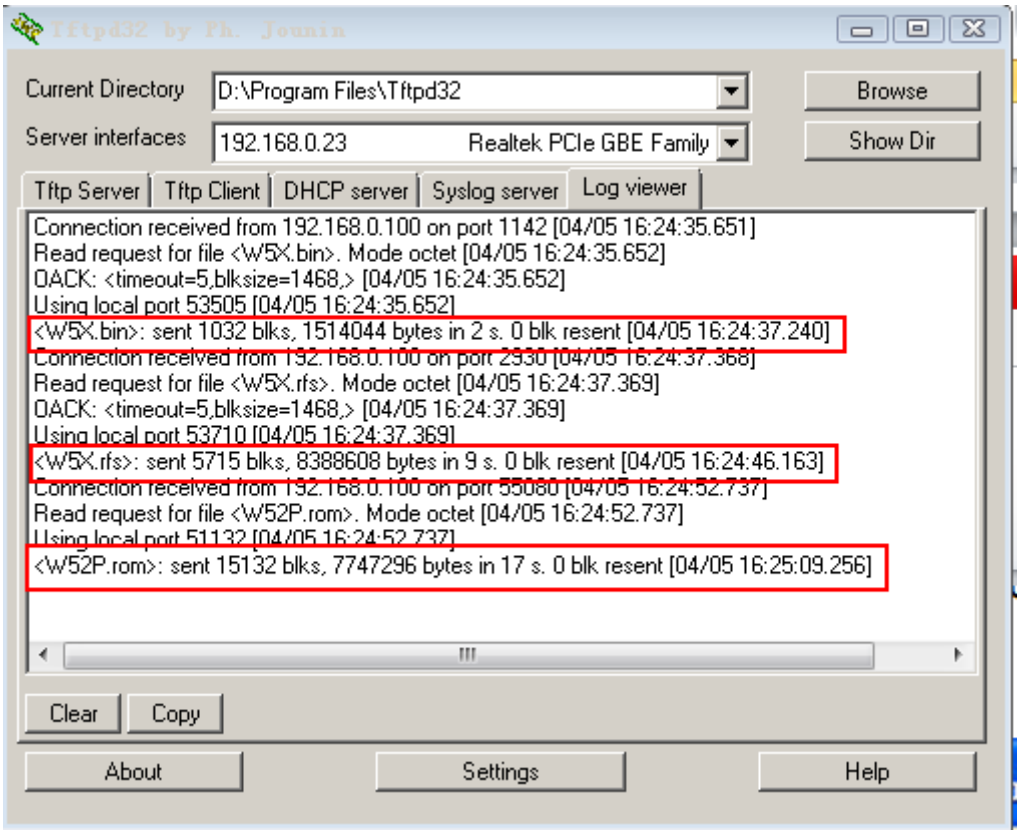


2. Click **OK** twice to save the settings.
3. Long press  (for W52P/W56P base) or  (for W60B base) and reconnect the power adapter to trigger the recovery mode.

Do not release  (for W52P/W56P base) or  (for W60B base) until three LED indicators ( in turn) are all turned on.

The W52P/W56P/W60B base will download and upgrade the firmware from the TFTP server.

You can view the syslog of the TFTP server to check if the W52P/W56P/W60B base downloads the firmware successfully, as shown below:



4. After a handset is registered, press OK (for W52P/W56P base) or OK (for W60B base) on the handset to verify the current firmware version.

For W75DM/W75B

For the W75DM/W75B, there is no screen to show information for you. The W75DM/W75B uses 192.168.0.23 as its default IP address, so you need to configure a static IP address for your local PC where you have the TFTP server installed.

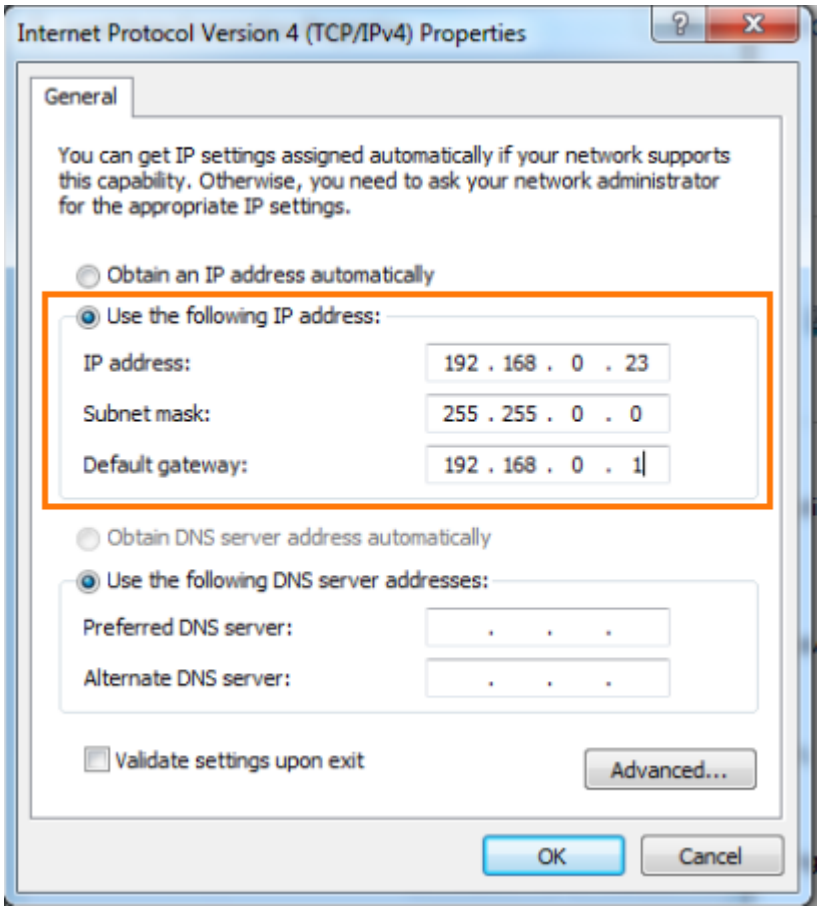
Before You Begin

Please do the following before you recover your W75DM/W75B.

- For W75DM: To initiate the recovery and upgrade process for the DM, please repeat the power-on procedure 7 to 9 times consecutively.
- For W75B: Press and hold the ≡ button to power on to enter the recovery upgrade.

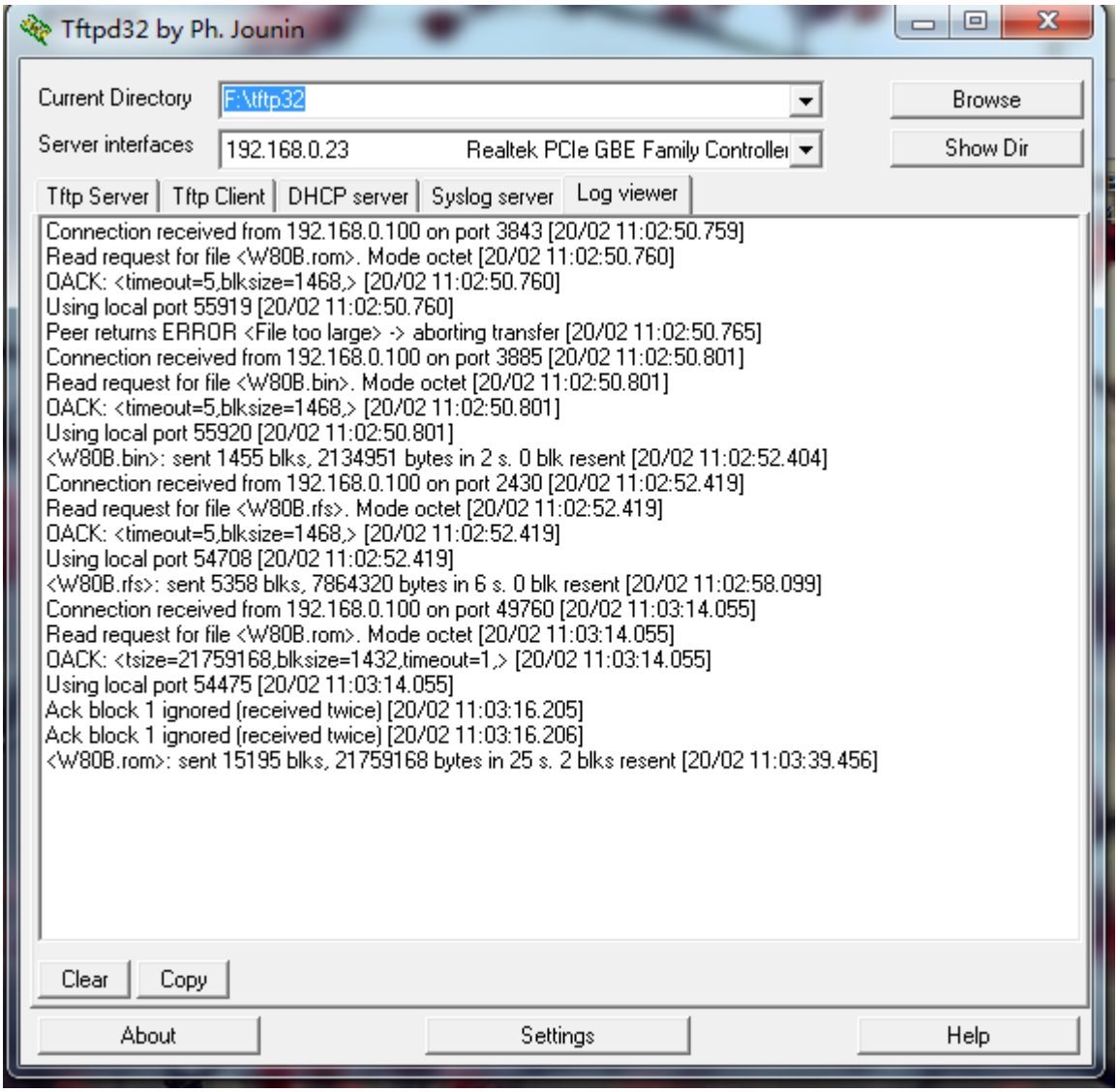
Procedure

1. Configure the static IP address on your local PC.
2. It must be configured as below:



2. Click **OK** twice to save the settings.

3. Long press  and reconnect the power adapter to trigger the recovery mode.
4. The W75DM/W75B will download and upgrade the firmware from the TFTP server.
5. You can view the syslog of the TFTP server to check if the W75DM/W75B downloads the firmware successfully, as shown below:



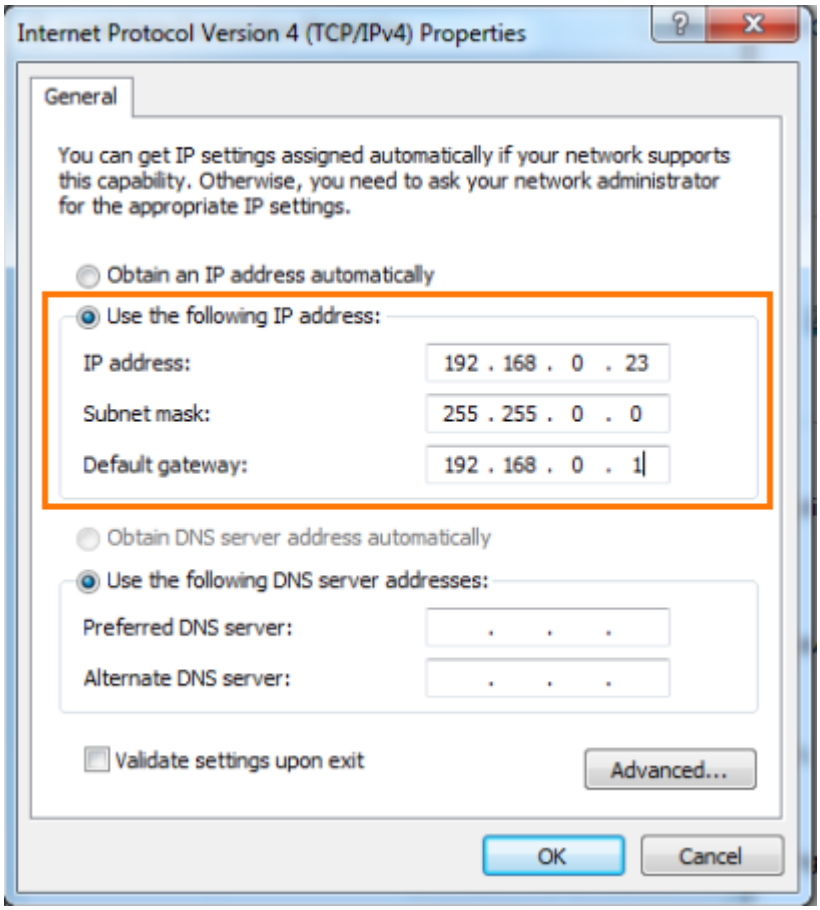
4. Find the current IP address of the device on the DHCP server in the list of registered DHCP clients.

For W80DM/W80B

For the W80DM/W80B, there is no screen to show information for you. The W80DM/W80B uses 192.168.0.23 as its default IP address, so you need to configure a static IP address for your local PC where you have the TFTP server installed.

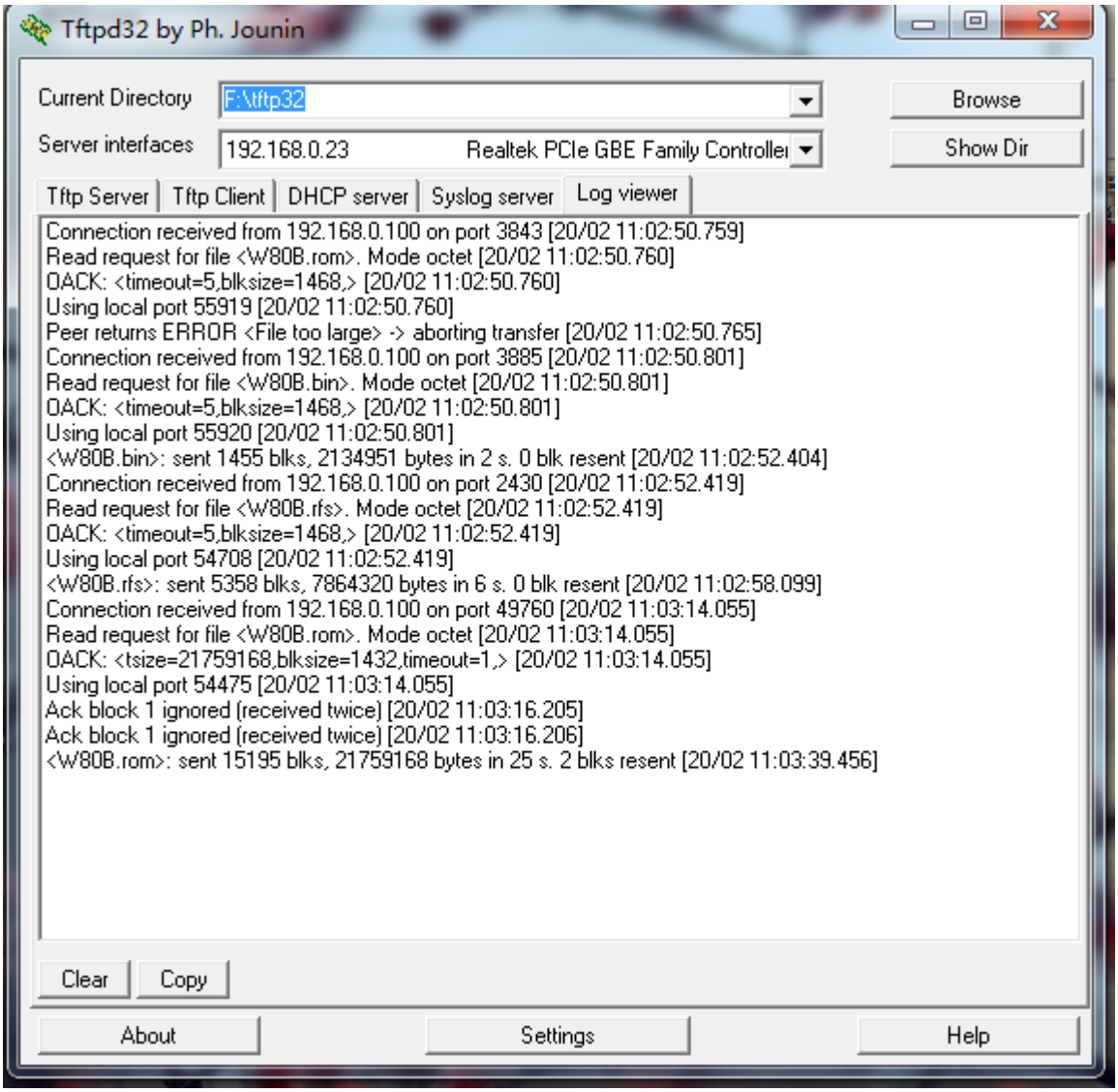
Procedure

1. Configure the static IP address on your local PC.
2. It must be configured as below:



2. Click **OK** twice to save the settings.

3. Long press  and reconnect the power adapter to trigger the recovery mode.
4. The W80DM/W80B will download and upgrade the firmware from the TFTP server.
5. You can view the syslog of the TFTP server to check if the W80DM/W80B downloads the firmware successfully, as shown below:



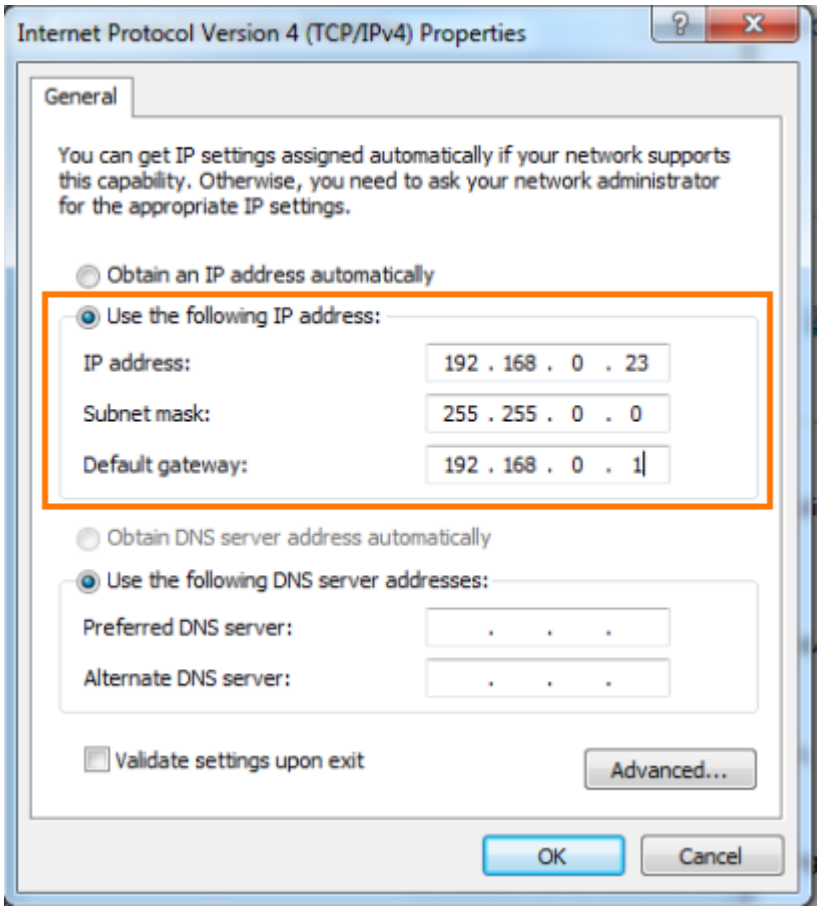
4. Find the current IP address of the device on the DHCP server in the list of registered DHCP clients.

For W90DM/W90B

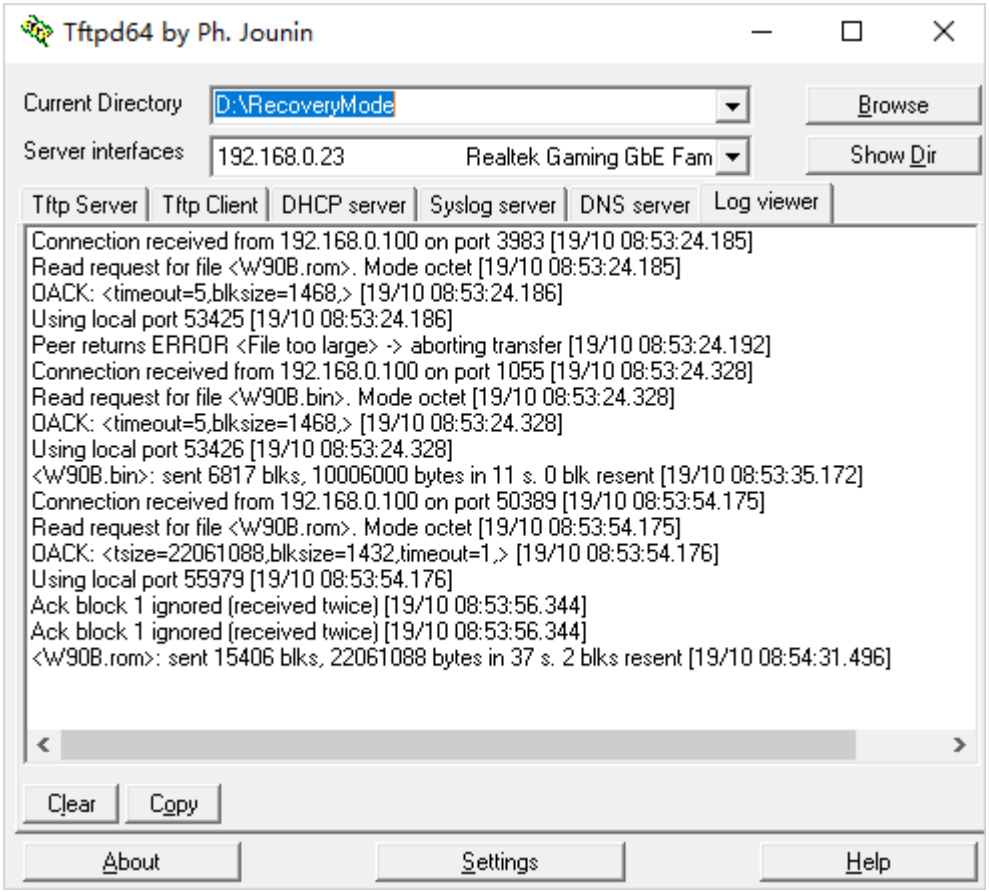
For the W90DM/W90B, there is no screen to show information for you. The W90DM/W90B uses 192.168.0.23 as its default IP address, so you need to configure a static IP address for your local PC where you have the TFTP server installed.

Procedure

1. Configure the static IP address on your local PC.
2. It must be configured as below:



2. Click **OK** twice to save the settings.
3. Long press  and reconnect the power adapter to trigger the recovery mode.
4. The W90DM/W90B will download and upgrade the firmware from the TFTP server. You can view the syslog of the TFTP server to check if the W90DM/W90B downloads the firmware successfully, as shown below:



4. Find the current IP address of the device on the DHCP server in the list of registered DHCP clients.

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)
W90	Yes (85 or later)	No
W60P	Yes (81 or later)	No
W53P	Yes (83 or later)	No
CP930W-Base	Yes (83 or later)	No
W52P W56P	Yes (81 or later)	No
W73P W76P W79P	Yes (85 or later)	No
W79P Pro	Yes (87 or later)	No
CP935W-Base	Yes (85 or later)	No

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:

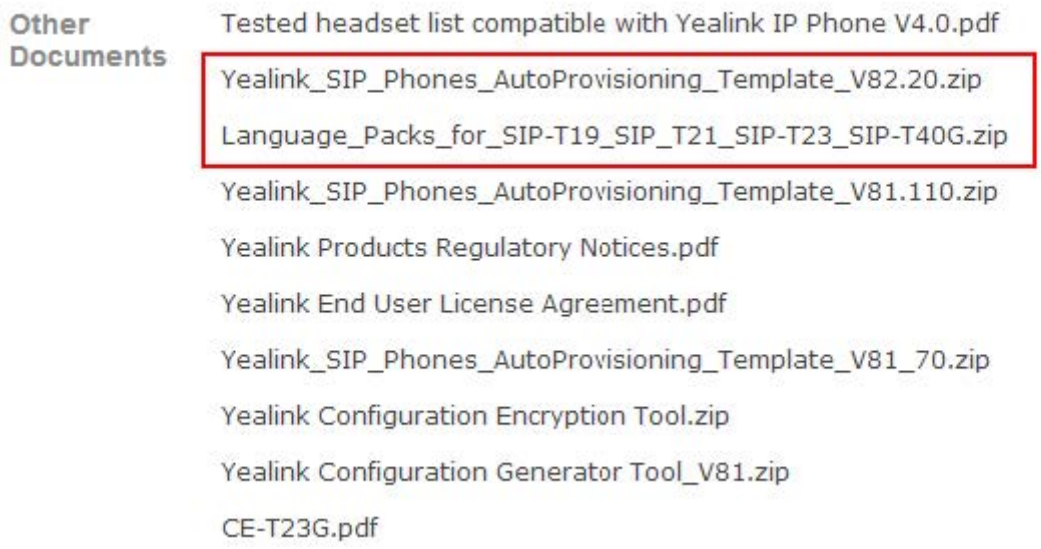
Feature	Template File Name
DST	AutoDST.xml
Language Packs	For example, 000.GUI.English.lang 1.English_note.xml 1.English.js
Replace Rule	dialplan.xml
Dial-now	dialnow.xml
Directory	favorite_setting.xml
Super Search in dialing	super_search.xml
Local Contact File	contact.xml
Remote XML Phone Book	Department.xml Menu.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.

To download template boot, configuration, and resource files:

1. Go to the Yealink Document Download 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 bar code on the back of the IP phone.
- **SIP Account Information**: This may include SIP credentials such as user name, password, and IP address of the SIP server. Ask your system administrator for SIP account information.

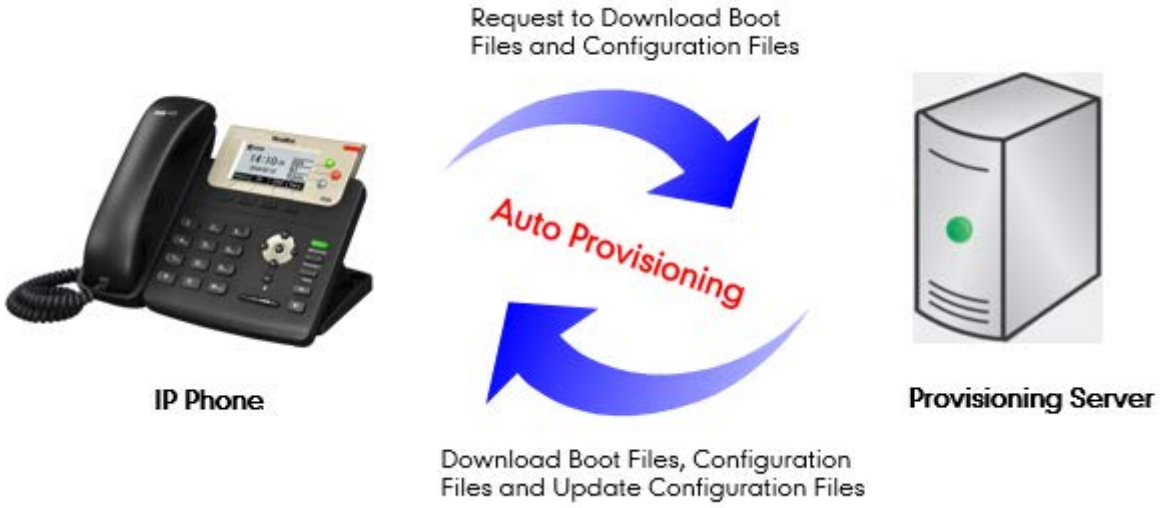
Provision Yealink IP Phones

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.

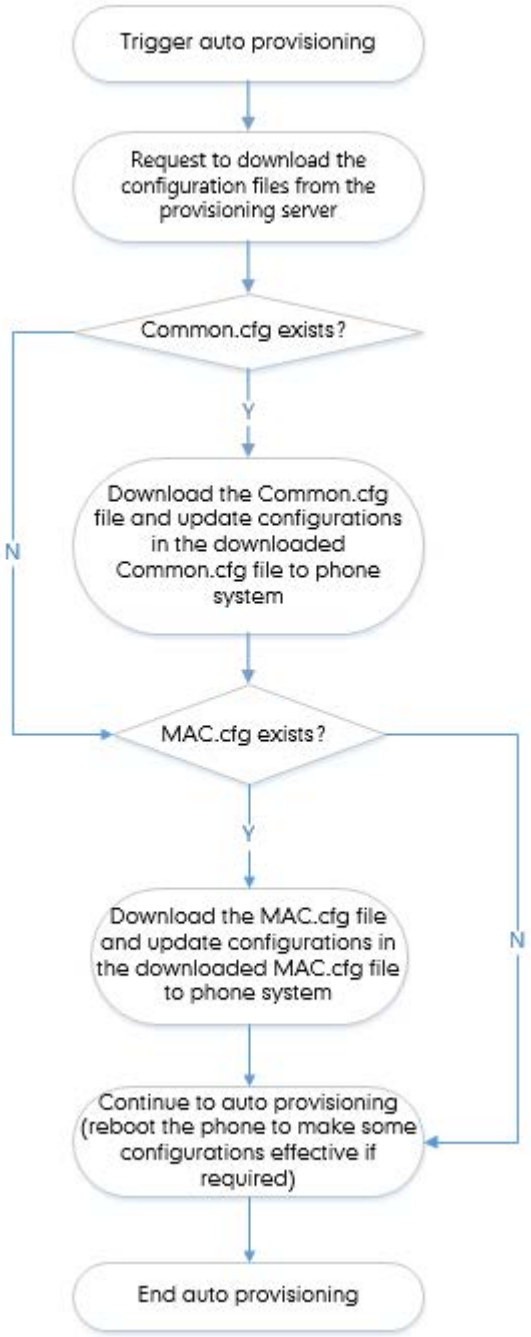
The following figure shows how the IP phone interoperates with the provisioning server:



Auto Provisioning Process

Old Mechanism – Without Boot Files

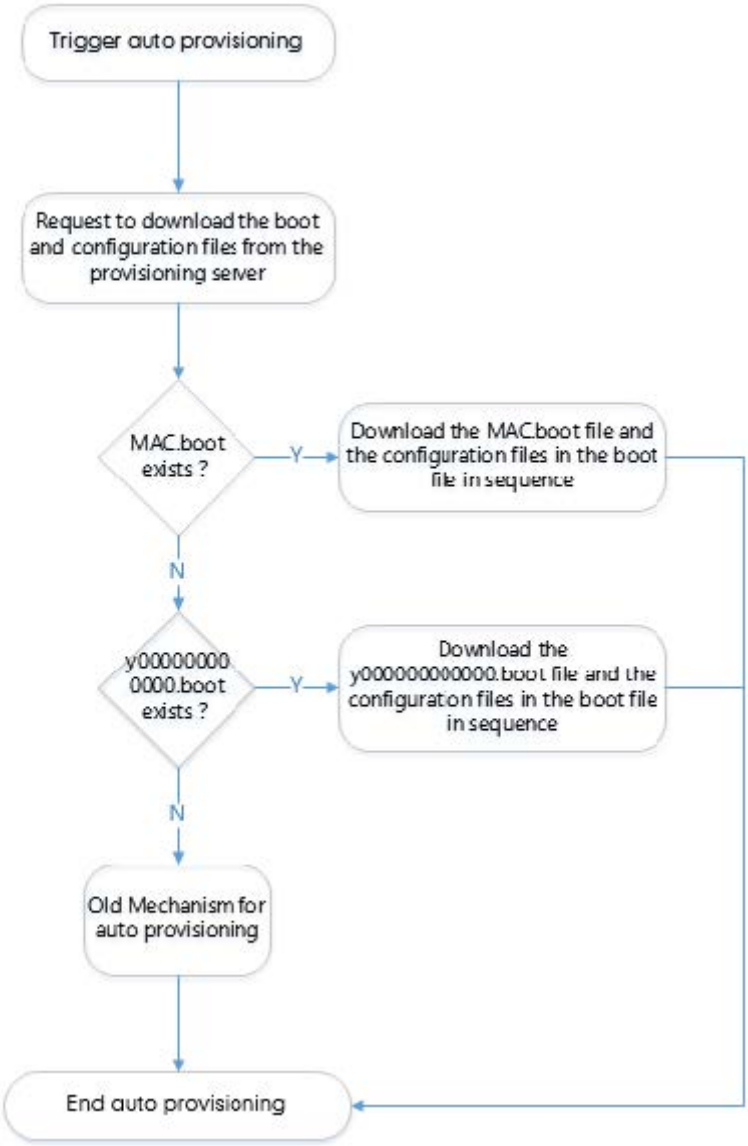
The following flowchart shows how Yealink IP phones perform auto provisioning when using configuration files only:



New Mechanism – With Boot Files

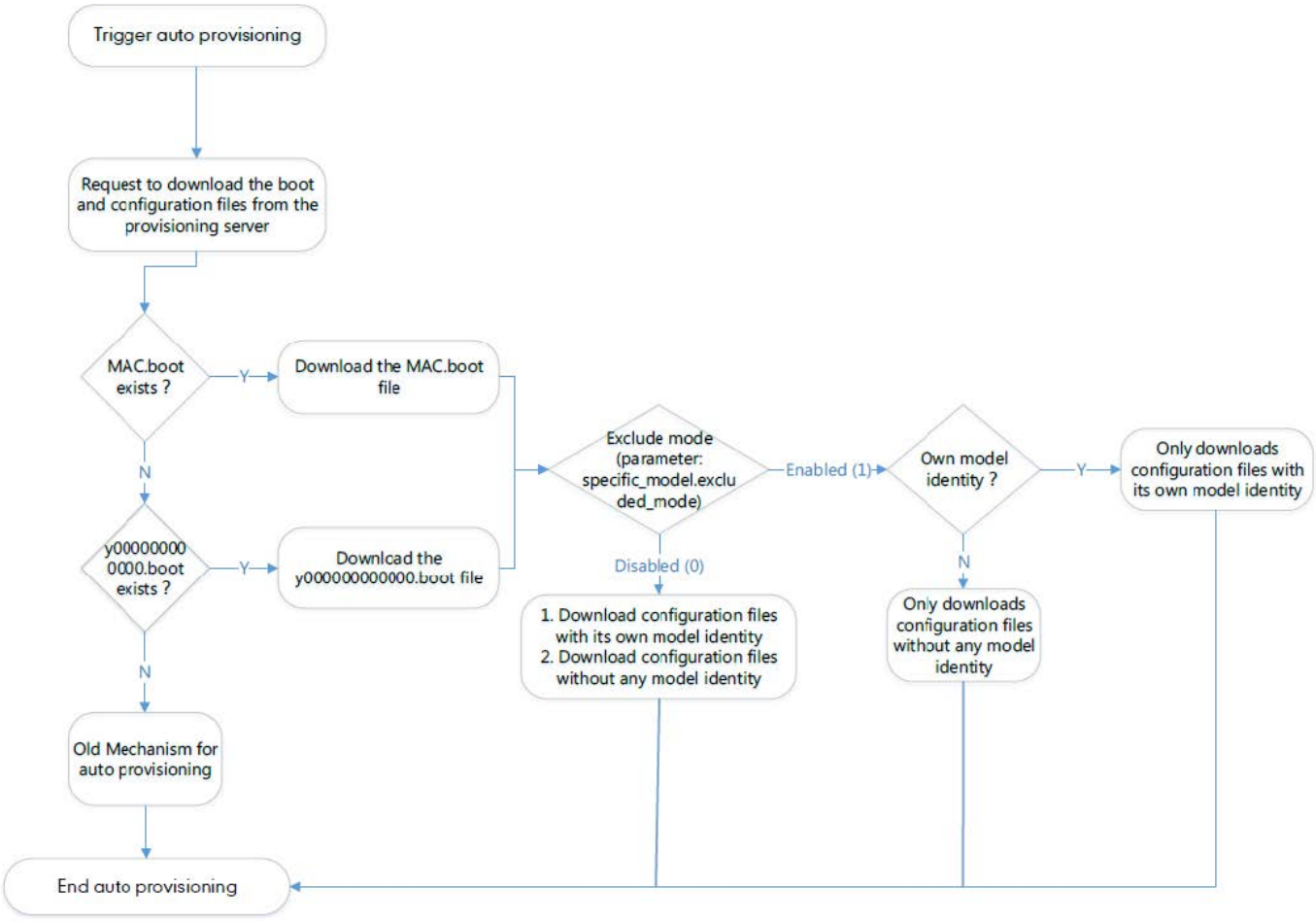
The following figure shows auto-provisioning flowcharts for Yealink IP phones when using boot files:

Scenario A – Do Not Support Exclude Mode



Scenario B – Support Exclude Mode

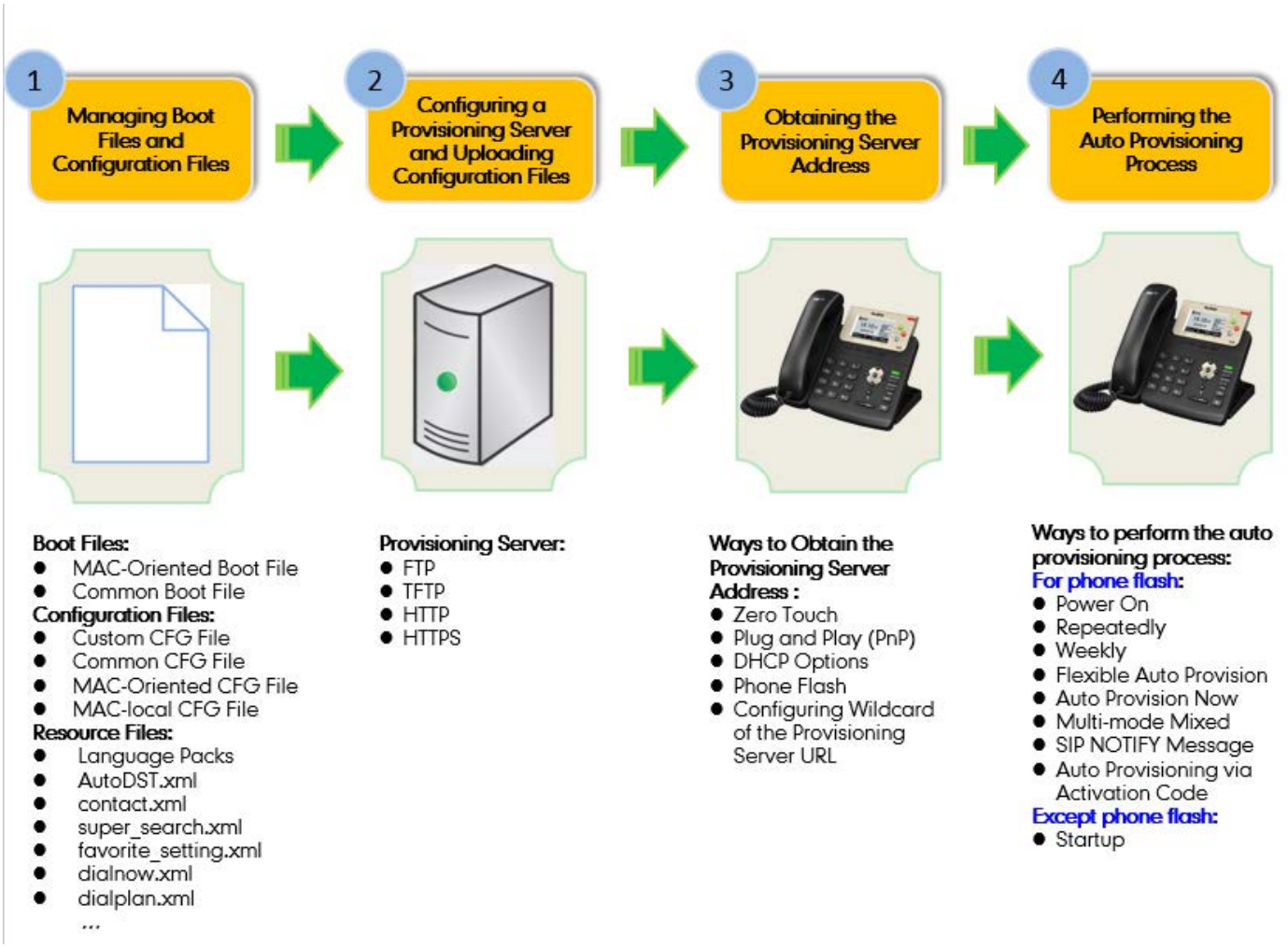
This scenario is only applicable to IP phones (except W52P/W56P IP phones) running firmware version 83 or later.



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.

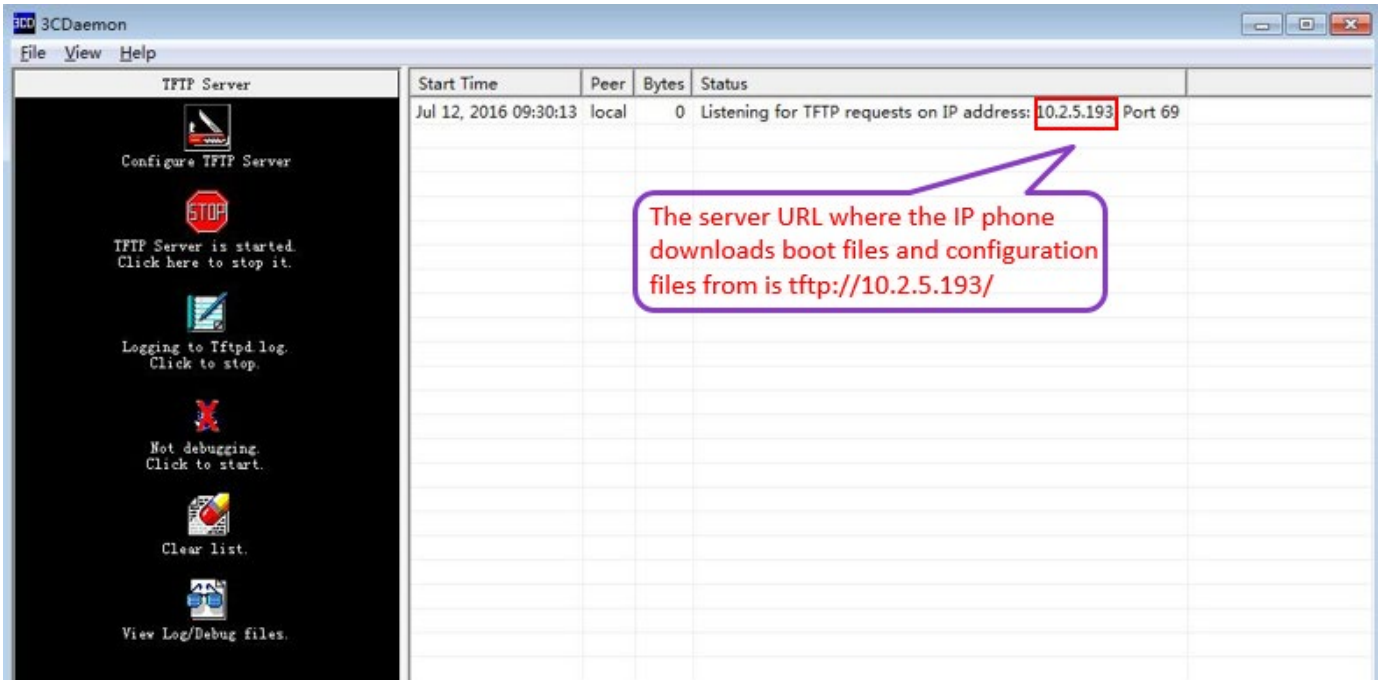
features.cfg

```
#!version:1.0.0.1
features.dnd_mode = 0
features.dnd.enable = 1
ringtone.url = tftp://10.2.5.193/Customring.wav
```

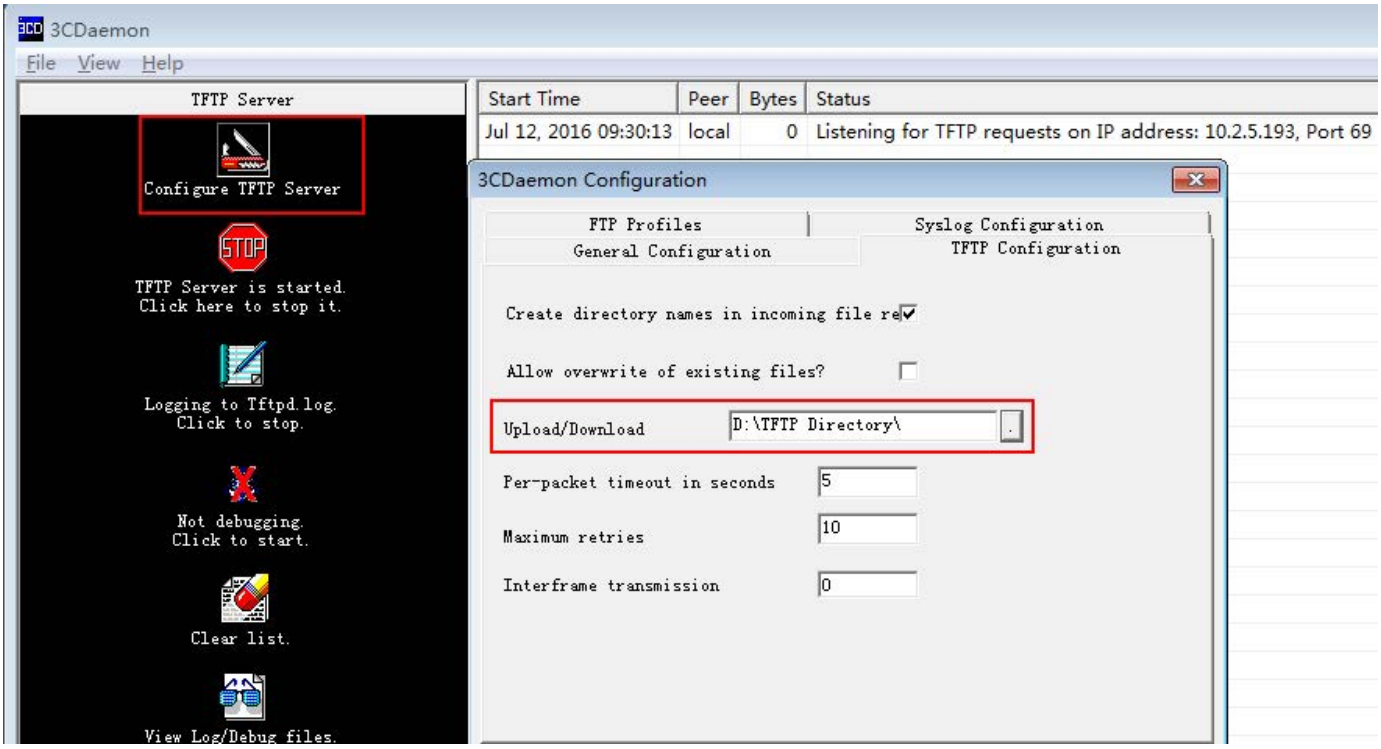
3. Configure the TFTP server.
4. ① Place boot files, configuration files, and resource files in the TFTP root directory (for example, D:\TFTP Directory).



6. ② Start the TFTP server. The IP address of the TFTP server is shown below:

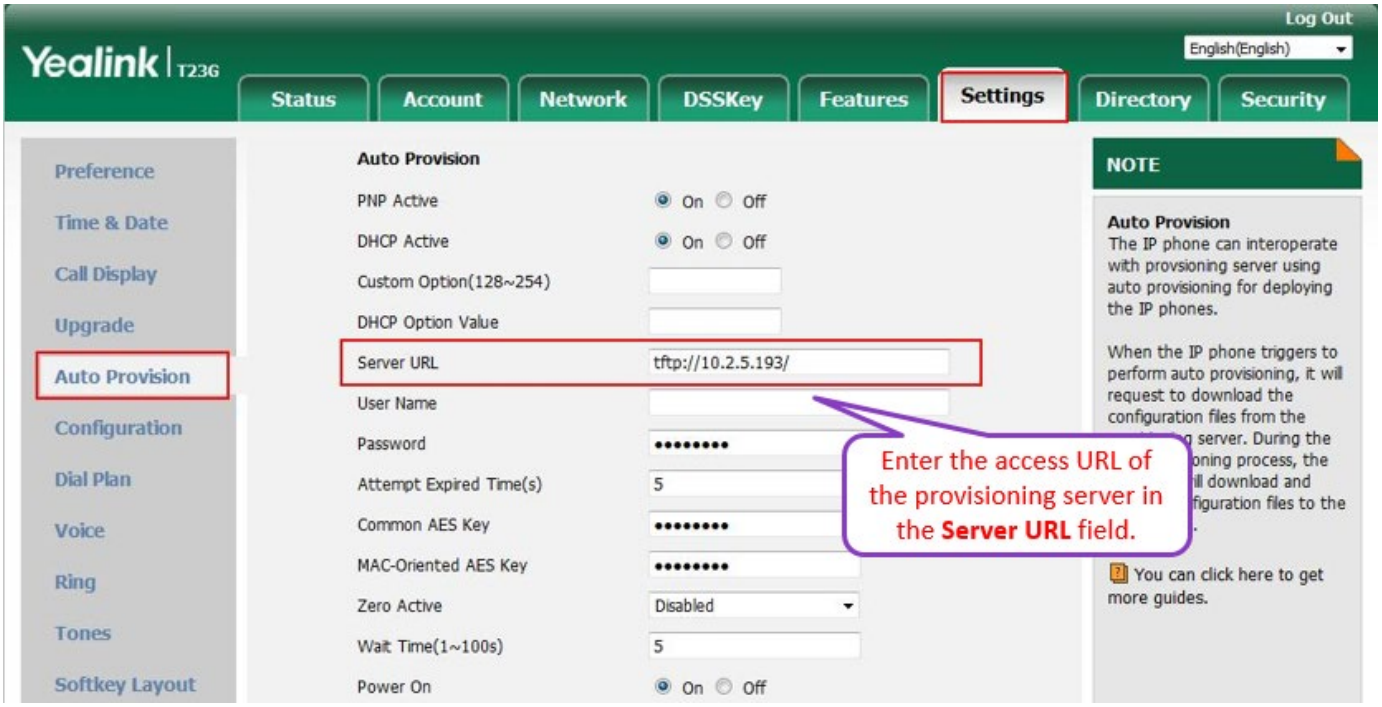


8. ③ Select Configure TFTP Server. Click the ... button to locate the TFTP root directory in your local system.



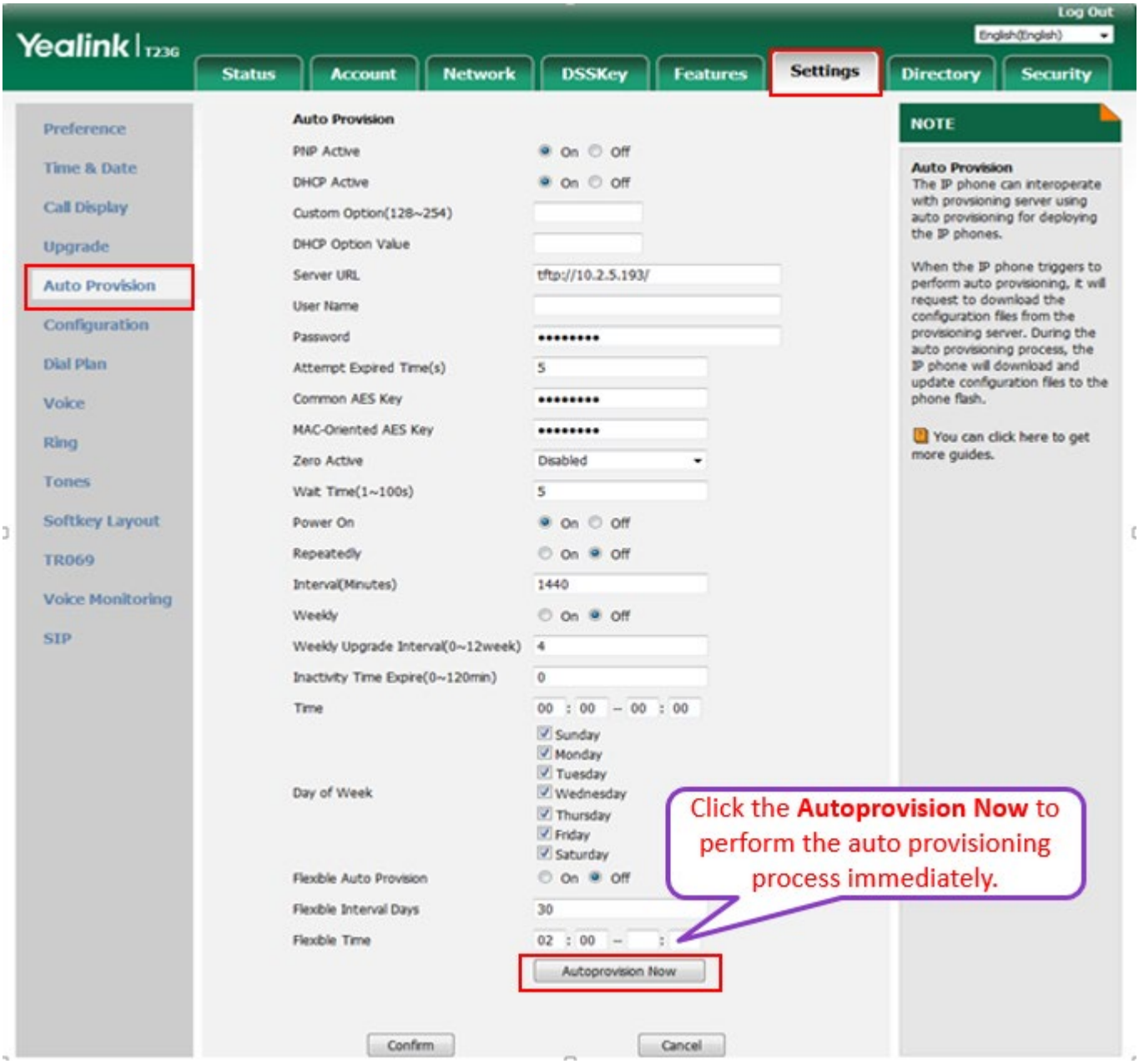
For more information on how to configure a provisioning server, refer to Configure a Provisioning Server.

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 must appear as-is in the first line	The line beginning with "#" is considered to be a comment. You can use "#" to make any comment in the boot file.
include:config <xxx.cfg> include:config "xxx.cfg"	1) Each "include" statement can specify a URL where a configuration file is stored. The configuration file format must be *.cfg. 2) The URL in <> or "" supports the following two forms: • Relative URL (relative to the boot file): For example, sip.cfg, HTTP Directory/sip.cfg • Absolute URL:

	For example, http://10.2.5.258/HTTP Directory/sip.cfg The URL must point to a specific CFG file. The CFG files are downloaded in the order listed (top to bottom). The parameters in the newly downloaded configuration files will override the duplicate parameters in files downloaded earlier. 3) The "include" statement can be repeated as many times as needed.
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. 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.

Create MAC-Oriented Boot File

The MAC-Oriented boot file is only effective for a specific phone. It uses the IP phone's 12-digit MAC address 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
W90	y000000000103.cfg
W53P/W60P/CP930W-Base	y000000000077.cfg
W52P/W56P	y000000000025.cfg
W71P/W73P/W74P/W76P/W77P/W78P/W79P/W79P Pro/CP935W-Base/W70B	y000000000146.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.

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.

- W90 DECT multi-cell system supports 2500 accounts.
- W71P/W73P/W74P/W76P/W77P/W78P/W79P/W79P Pro/CP935W-Base DECT IP phones support 10 assigned accounts.
- W53P/W60P DECT IP phones support 8 assigned accounts.
- CP930W-Base phones support only one assigned account.

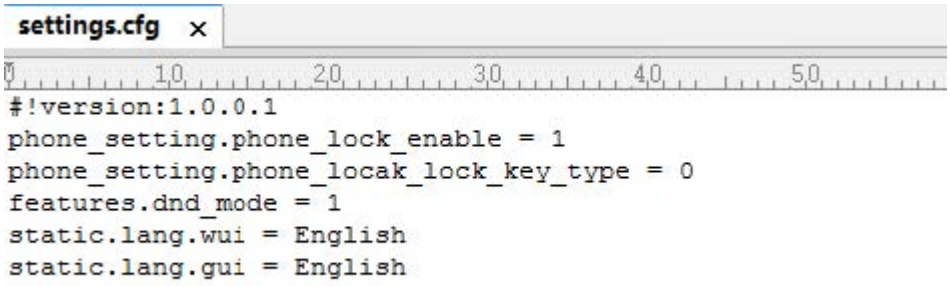
- W52P/W56P IP DECT phones support 5 accounts.

Create a New CFG File

If you want to create a new CFG file for your phone, follow these steps:

To create a new CFG file:

1. Create a CFG file for your phone. Ensure the file complies with the guidelines that are listed in Editing Common CFG File or Editing MAC-Oriented CFG File.
2. Copy configuration parameters from the template configuration files and set valid values for them.



3. (Optional.) Specify different parameter values for specific phone groups.
   For example:
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 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 users' personalization settings, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

We recommend that you do not edit the MAC-local CFG file. If you really want to edit the MAC-local CFG file, you can export and then edit it.

For more information on how to export CFG files, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

Encrypt Configuration Files

To protect against unauthorized access and tampering of sensitive information (for example, login password, 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.

Appendix-Configure an FTP Server

Wftpd and FileZilla are free FTP application software for Windows. This section mainly provides instructions on how to configure an FTP server using wftpd for Windows.

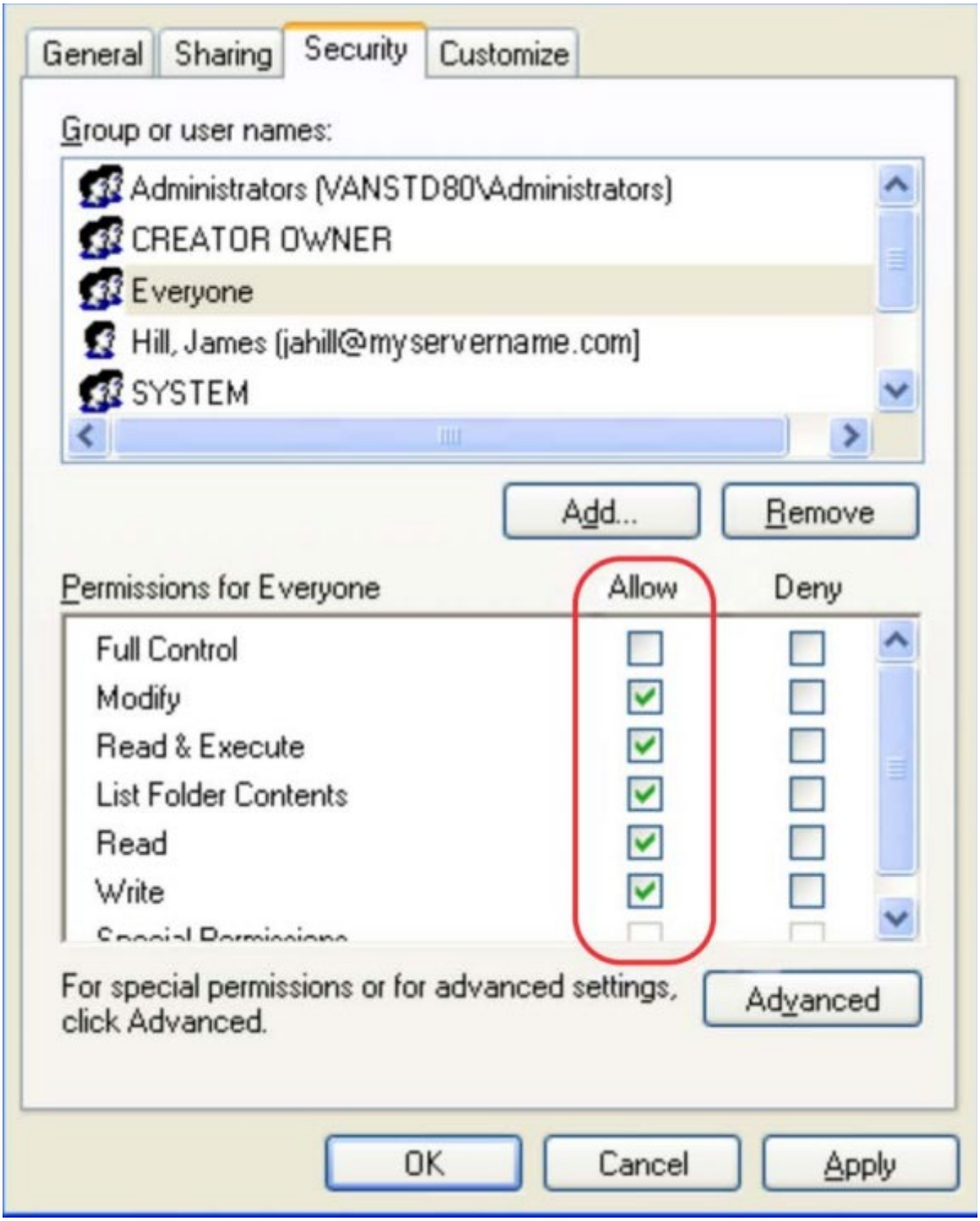
You can download wftpd online: http://www.wftpd.com/products/products.html or FileZilla online: https://filezilla-project.org.

We recommend that you use vsftpd as an FTP server for the Linux platform if required.

Prepare a Root Directory

To prepare a root directory:

1. Create an FTP root directory on the local system (for example, D:\FTP Directory).
2. Place the boot files and configuration files in this root directory.
3. Set the security permissions for the FTP directory.
   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 below:

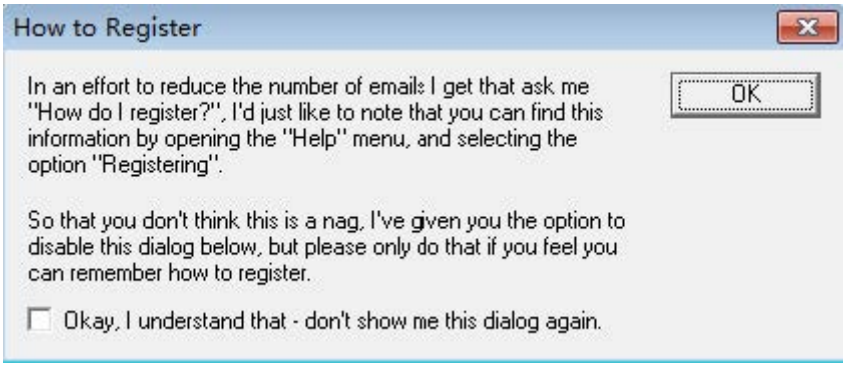


Configure an FTP Server

To configure a wftpd server:

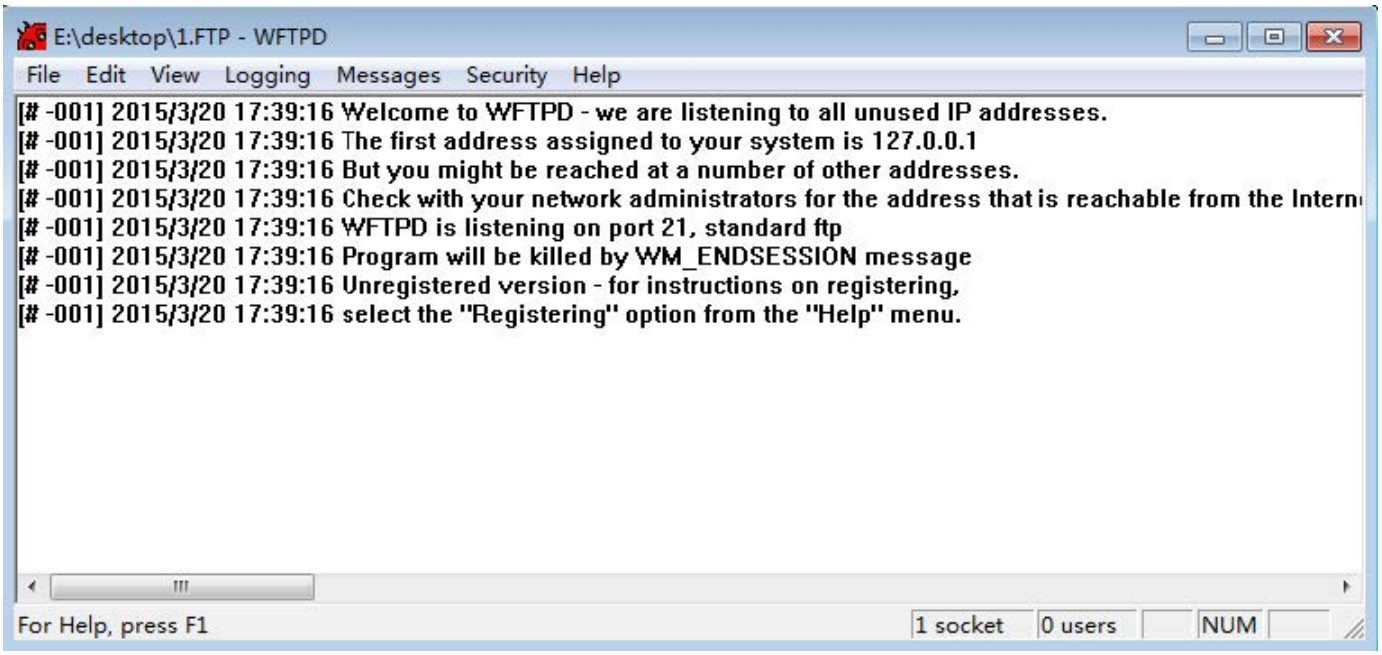
1. Download the compressed file of the wftpd application to your local directory and extract it.
2. Double-click the **Wftpd.exe**.

   The dialogue box for how to register is shown below:

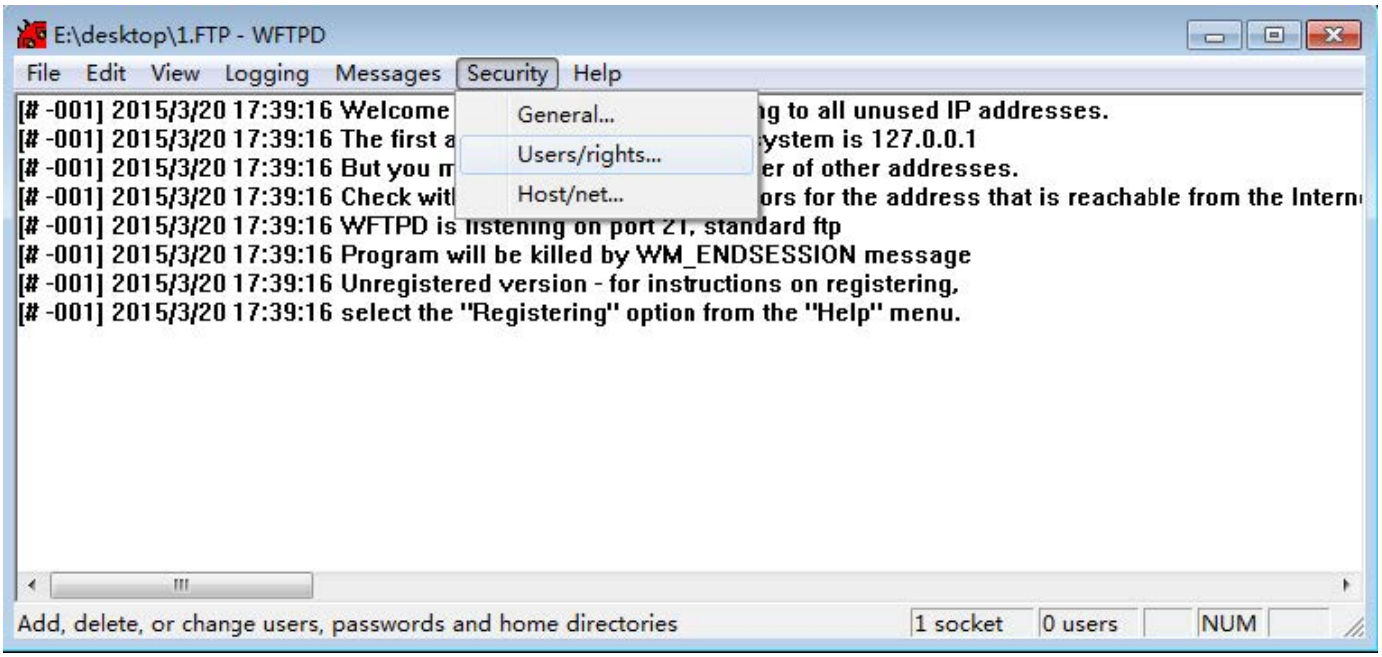


3. Check the check box and click **OK** in the pop-up box.

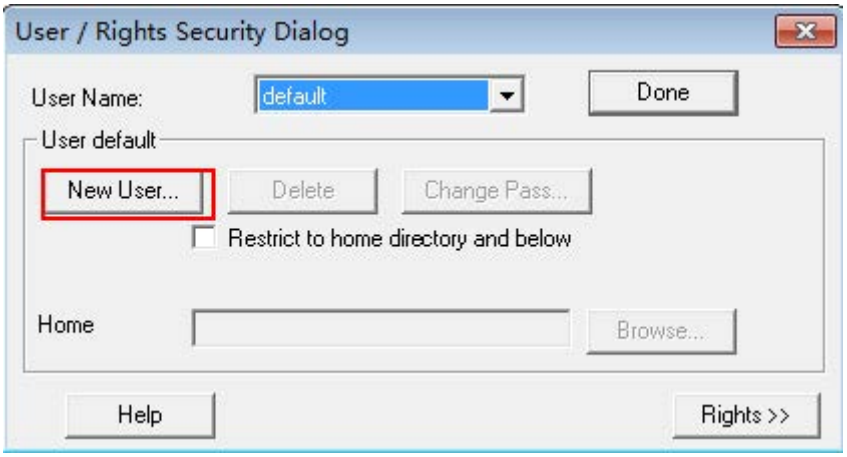
The log file of the wftpd application is shown below:



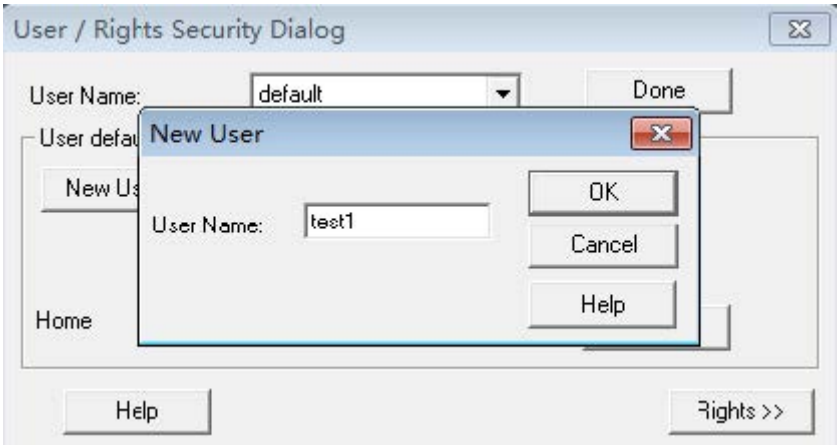
4. Click **Security** > **Users/rights**.



5. Click **New User**.



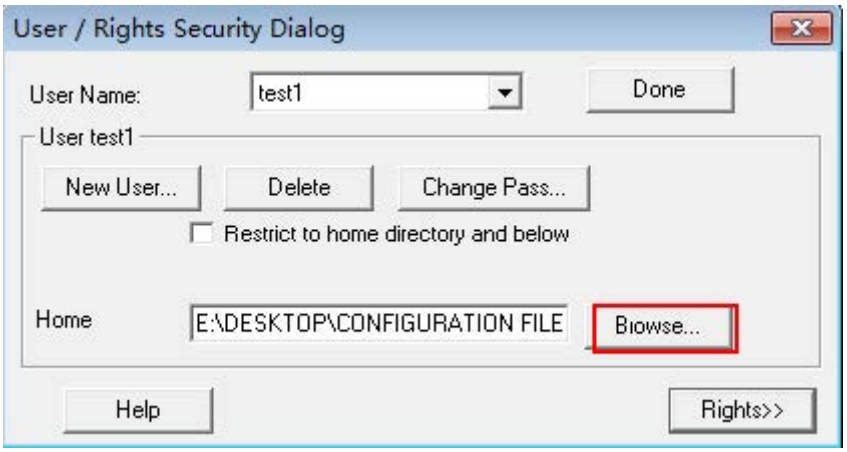
6. Enter a user name (for example, test1) in the **User Name** field and then click **OK**.



7. Enter the password of the user (for example, test1) created above in the **New Password** and **Verify Password** fields, 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 permissions.



11. Click **Done** to save the settings and finish the configurations.

The server URL "ftp://username:password@IP/" (Here "IP" means the IP address of the provisioning server, "username" and "password" are the authentication for FTP download. For example, "ftp://test1:123456@10.3.6.234/") is where the IP phone downloads boot files and configuration files from.

Before configuring a wftpd server, ensure that no other FTP servers exist in your local system.

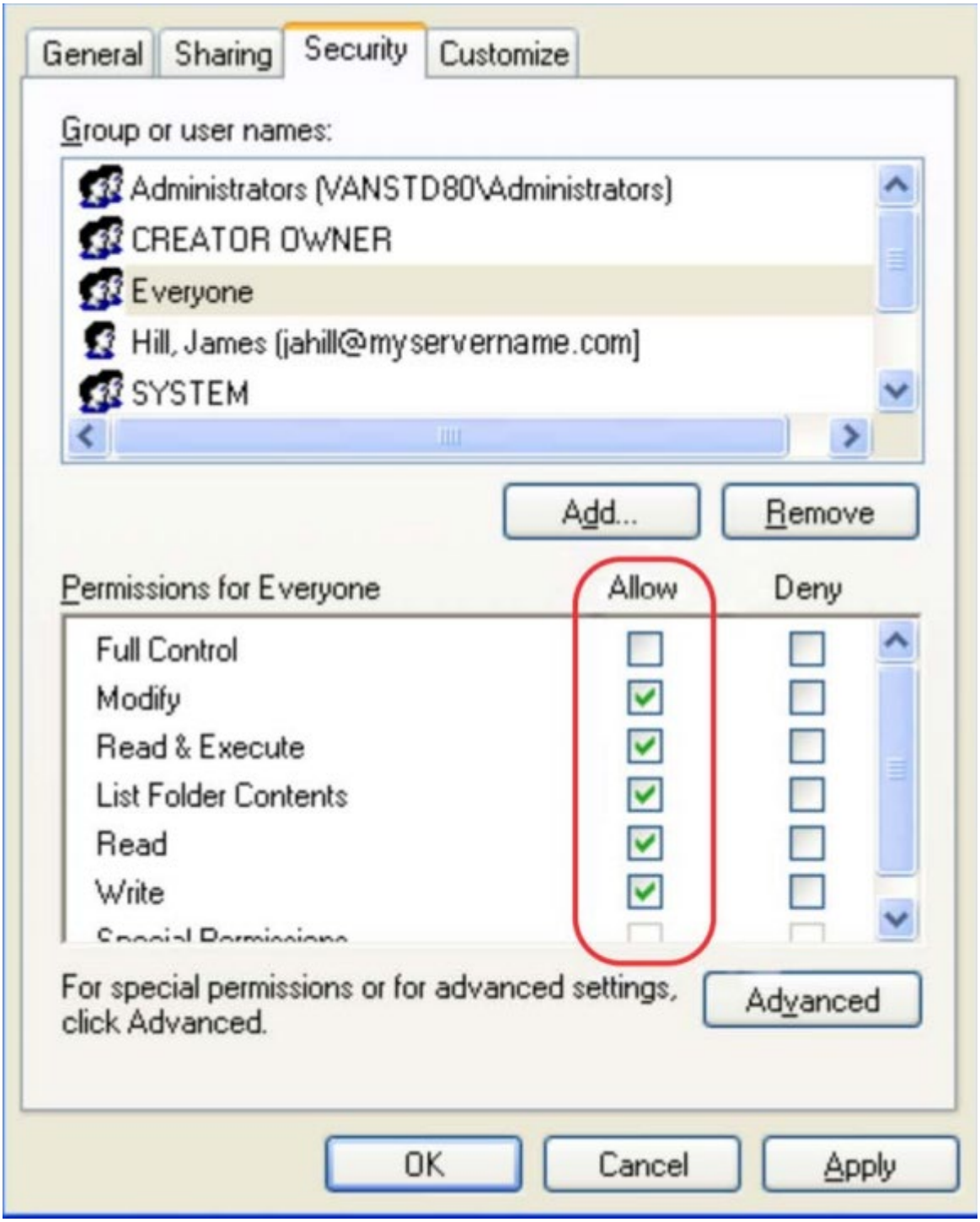
Appendix-Configure HTTPS Server

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 below:

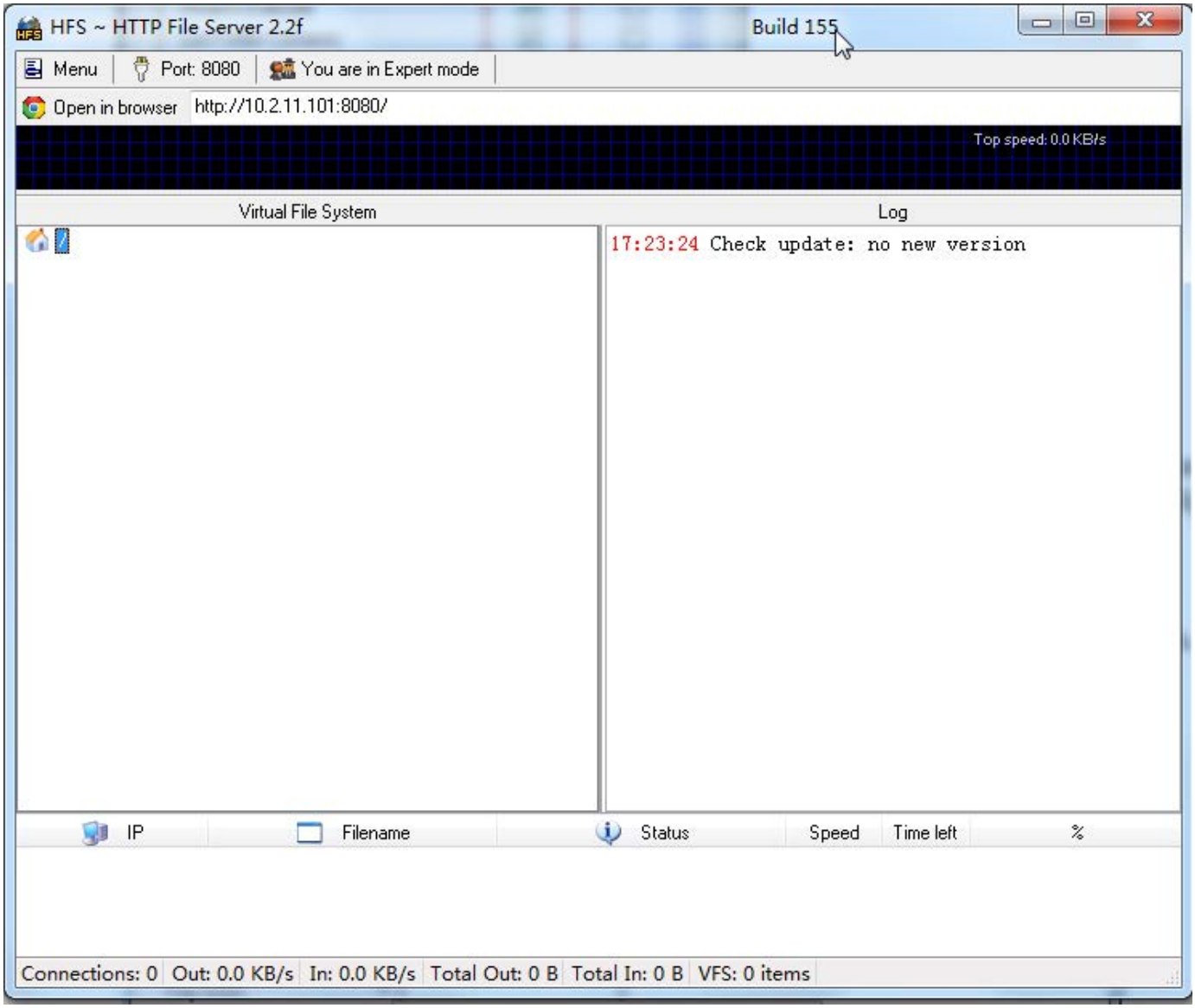


Configure an HTTPS Server

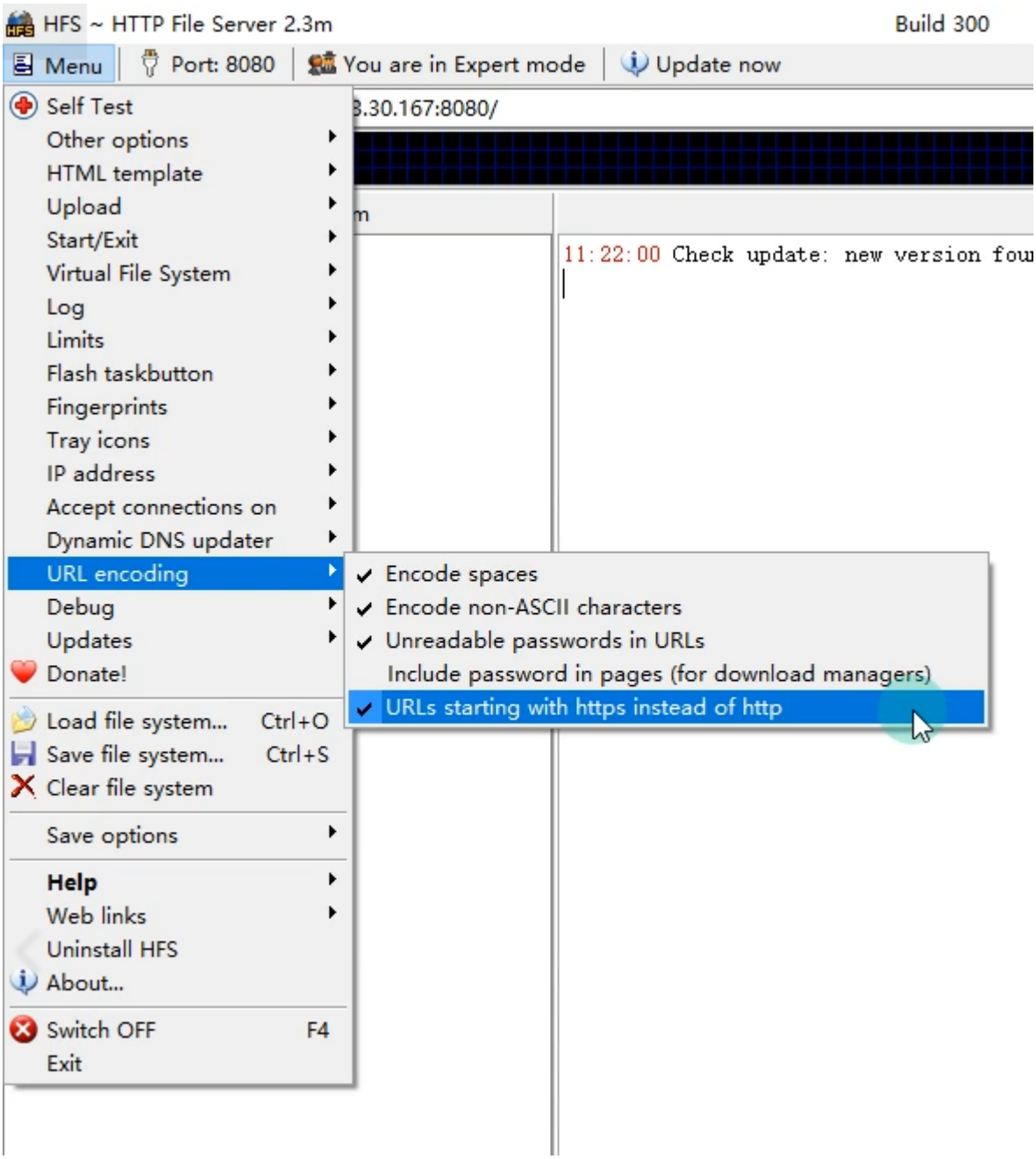
HFS tool is an executable application, so you don’ t need to install it.

To configure an HTTPS server:

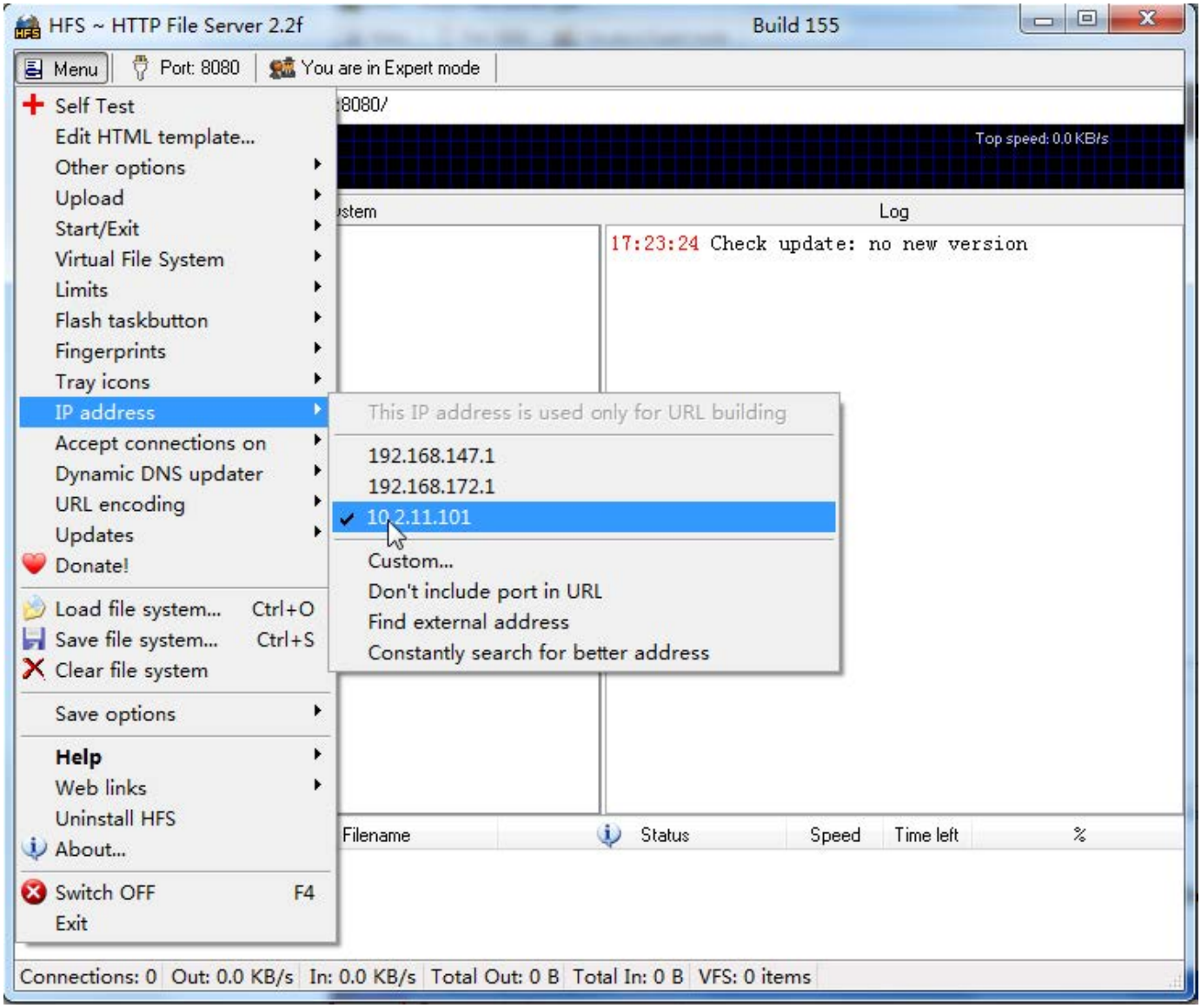
1. Download the application file to your local directory, and double-click the **hfs.exe**.
2. The main configuration page is shown below:



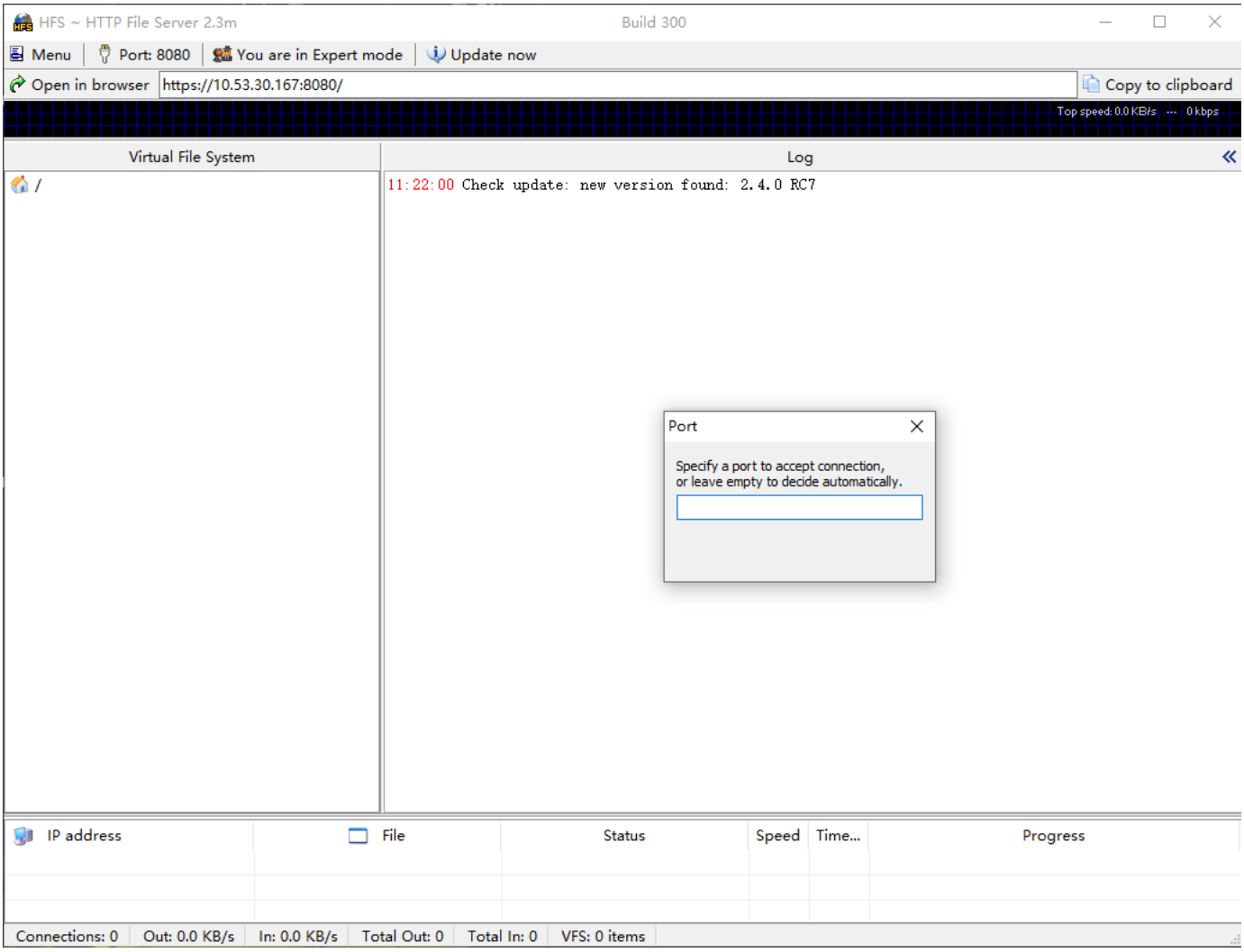
2. Click **Menu** > **URL encoding** > **URLs starting with https instead of http**.



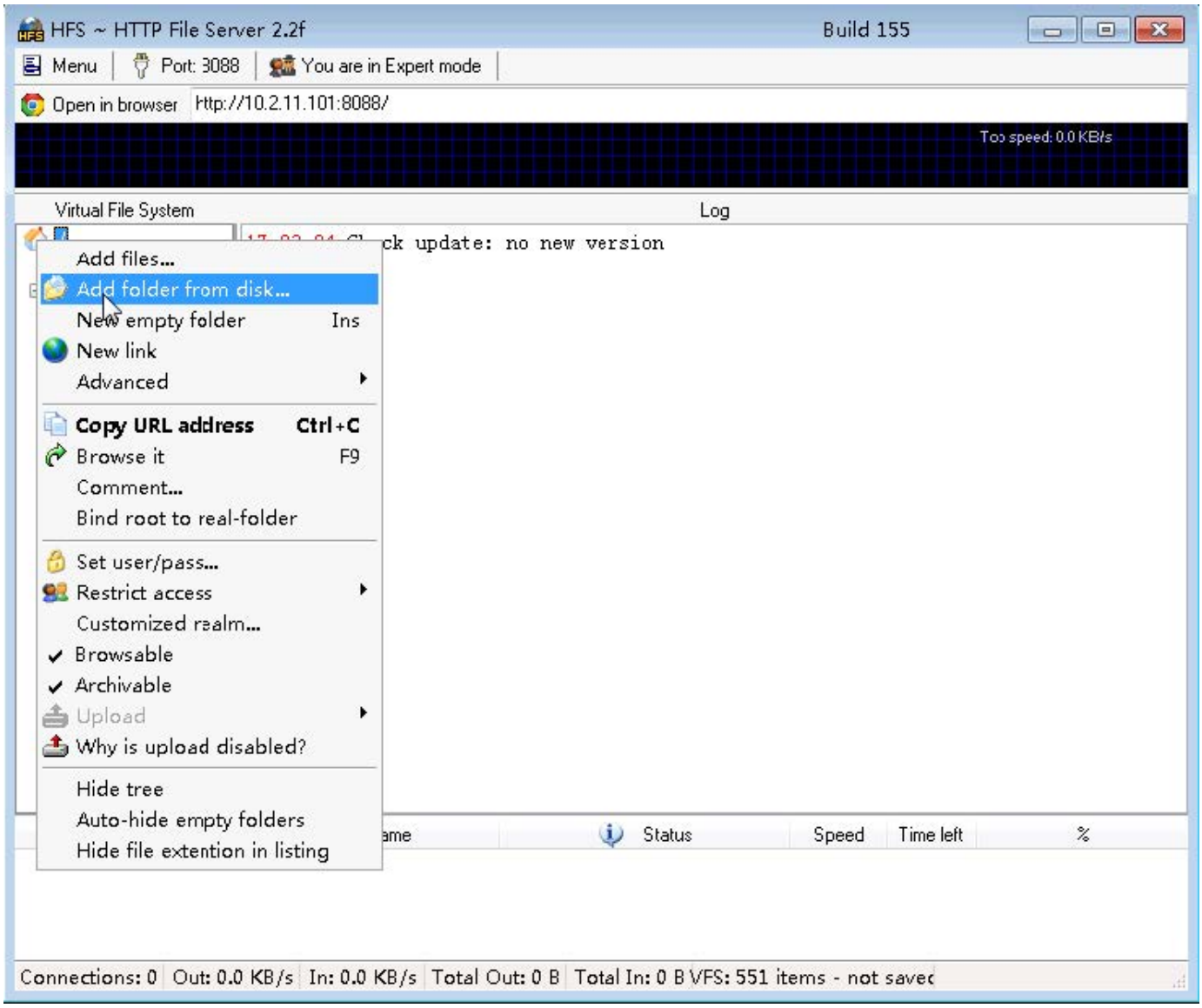
3. Click **Menu** on the main page and select the IP address of the PC from the **IP address**.



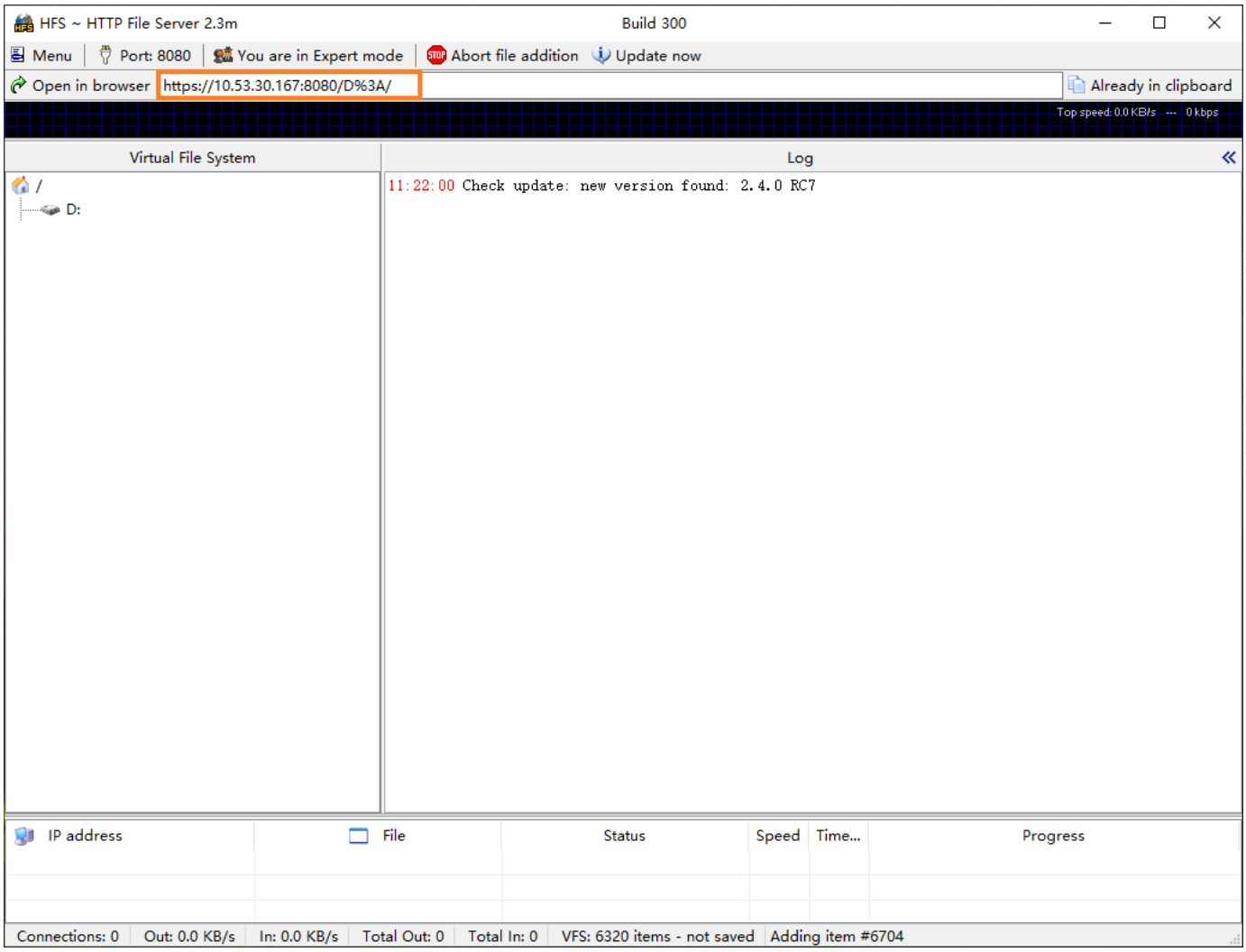
5. The default HTTP port is **8080**. You can also reset the HTTP port (make sure there is no port conflict).



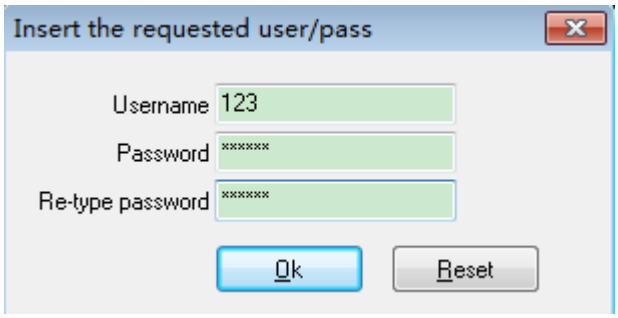
4. Right-click the icon on the left of the main page, select Add folder from disk to add the HTTPS Server root directory.



5. Locate the root directory from 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**.



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.

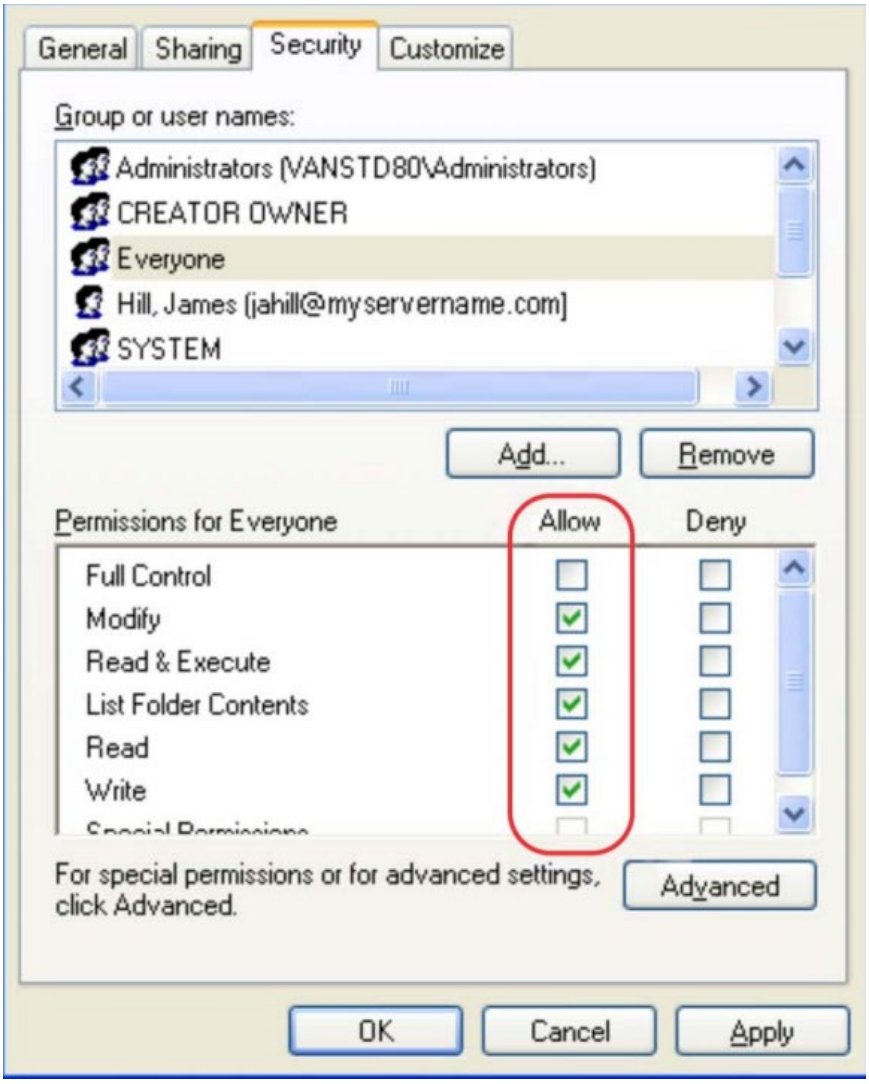
Prepare a Root Directory

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:



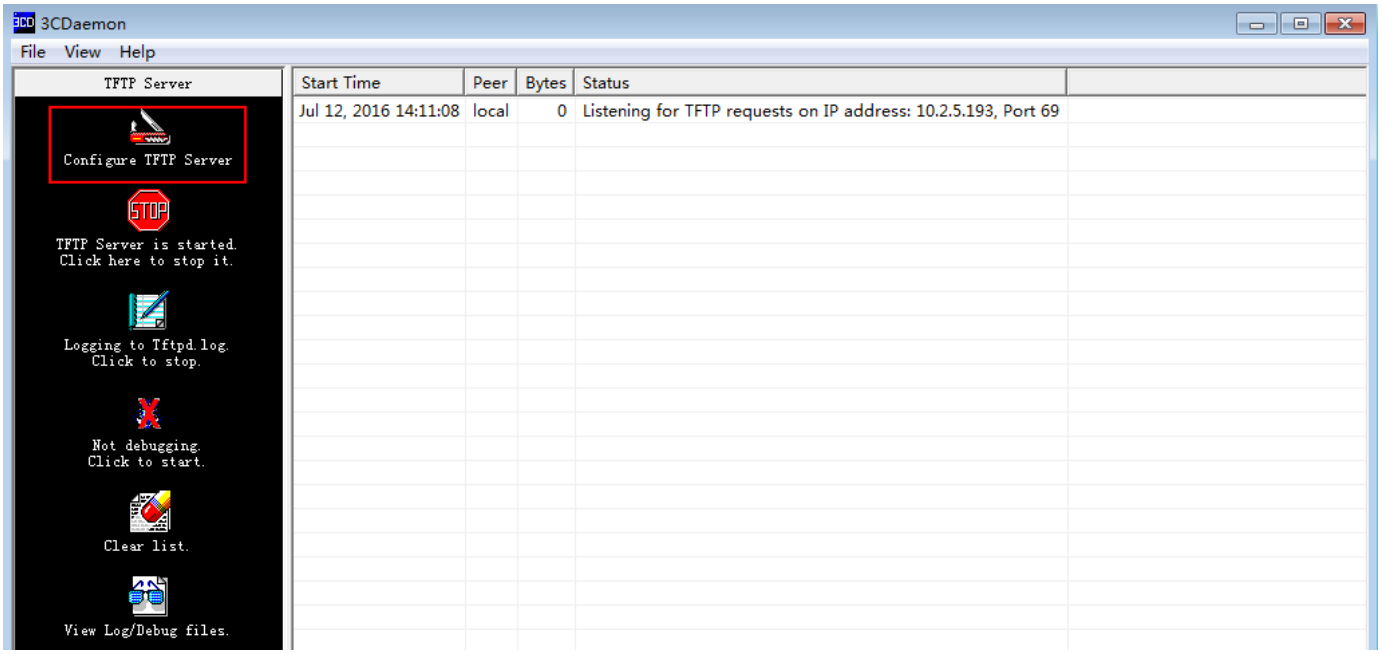
Configure a TFTP Server

If you have a 3CDaemon application installed on your local system, use it directly. Otherwise, download and install it.

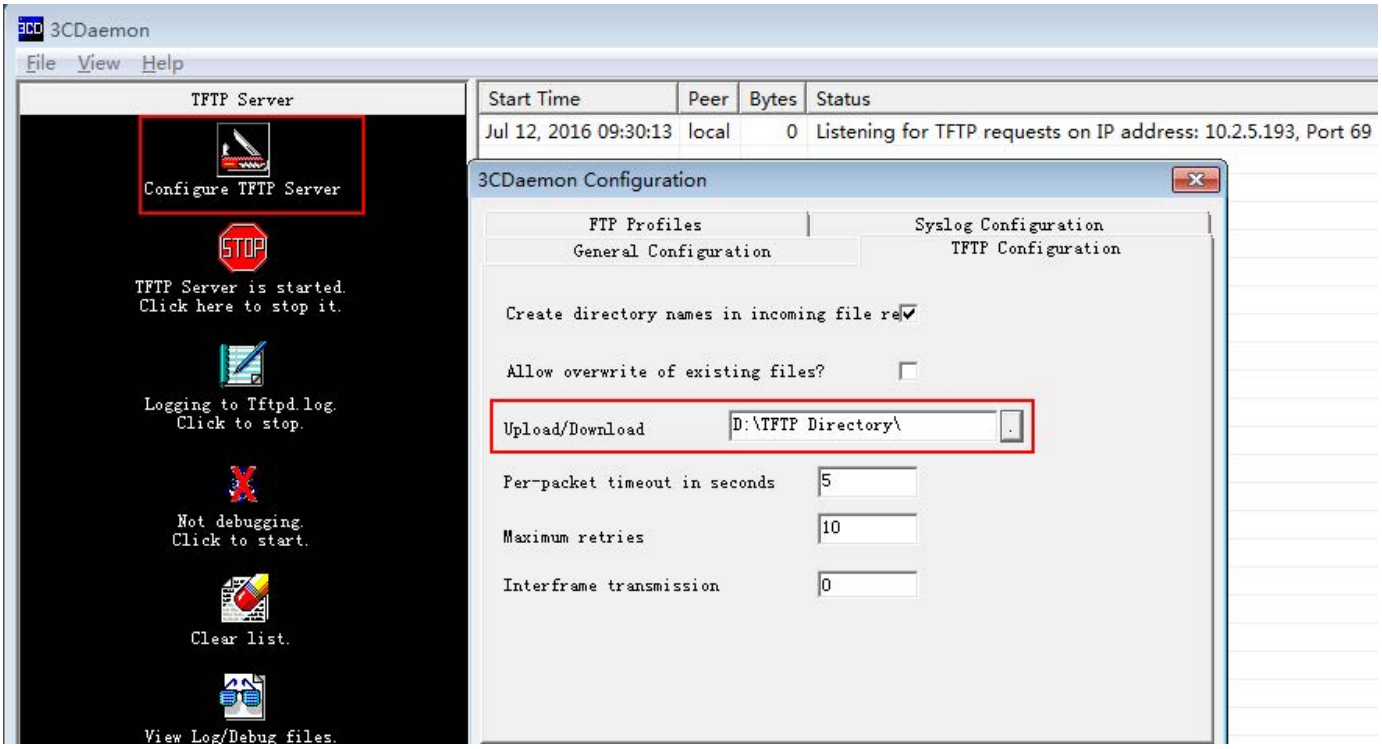
To configure a TFTP server:

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

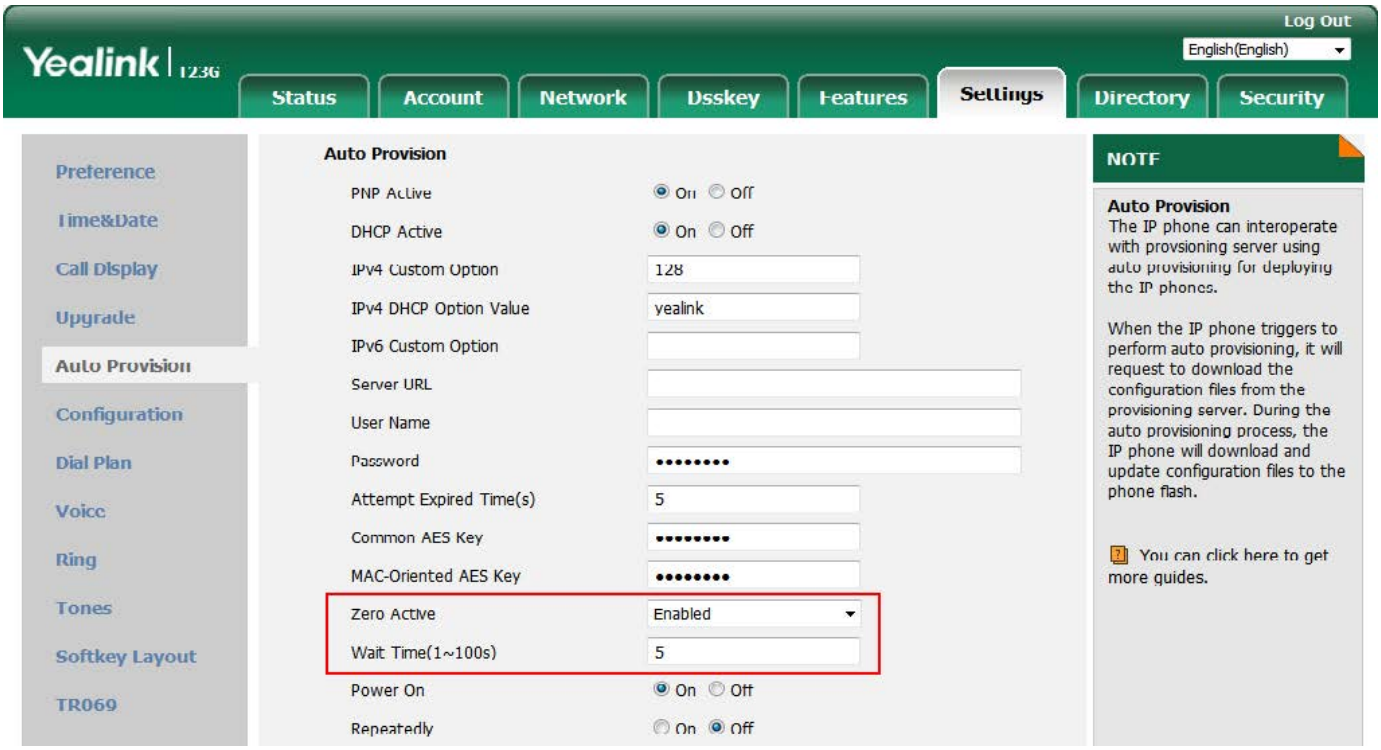
The priority of obtaining the provisioning server address is as follows: Zero Touch>PnP Server>DHCP Options (for IPv4: IPv4 Custom option>option 66>option 43; for IPv6: IPv6 Custom option>option 59) >Phone Flash. The following sections detail the process of each way (take the SIP-T23G IP phone as an 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.

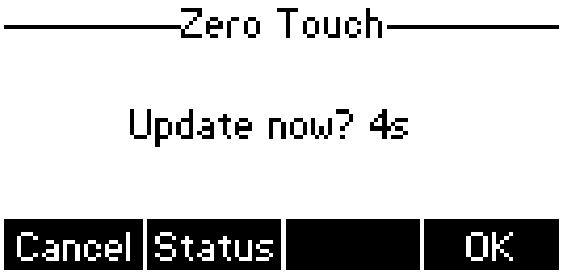
To configure zero touch via the web user interface:

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**.



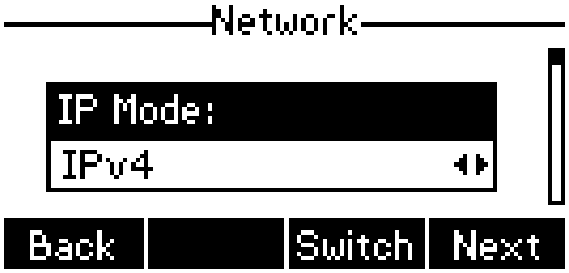
4. Click **Confirm** to accept the change.

   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.

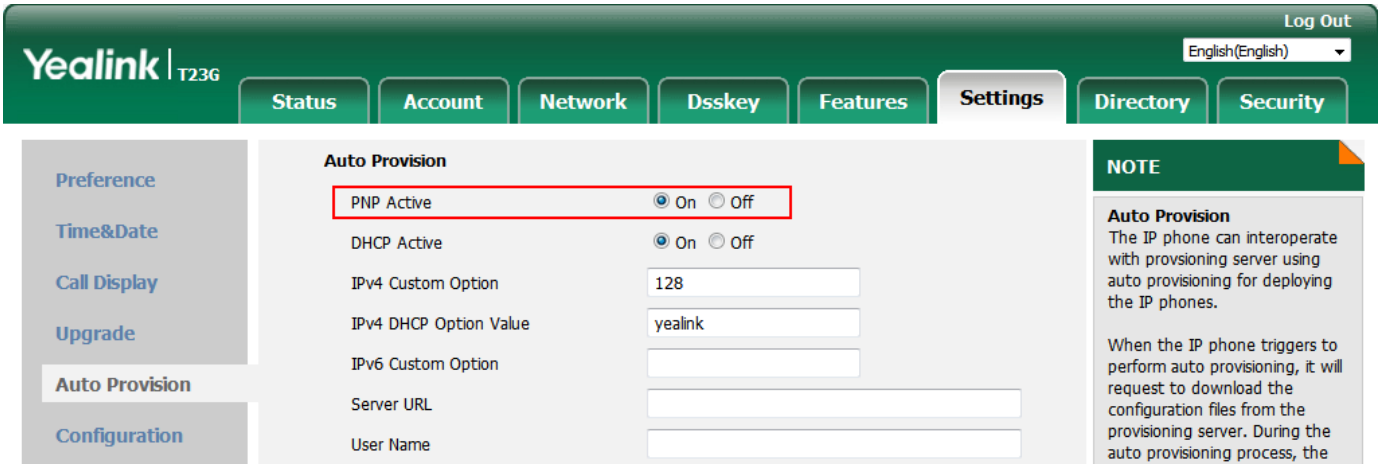
    After the above configuration is completed, the IP phone will connect to the configured provisioning server and perform auto-provisioning during startup.

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.

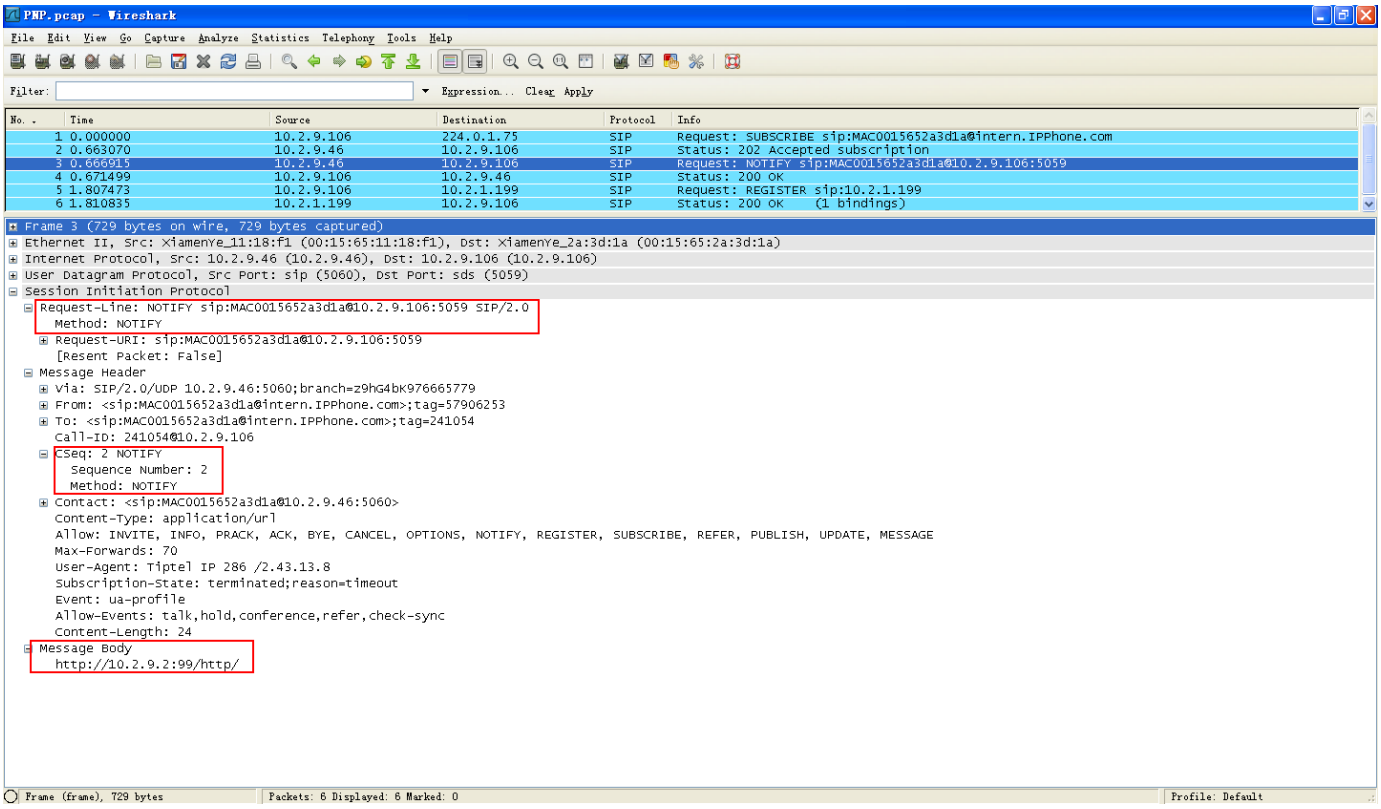
To configure PnP via the web user interface:

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.

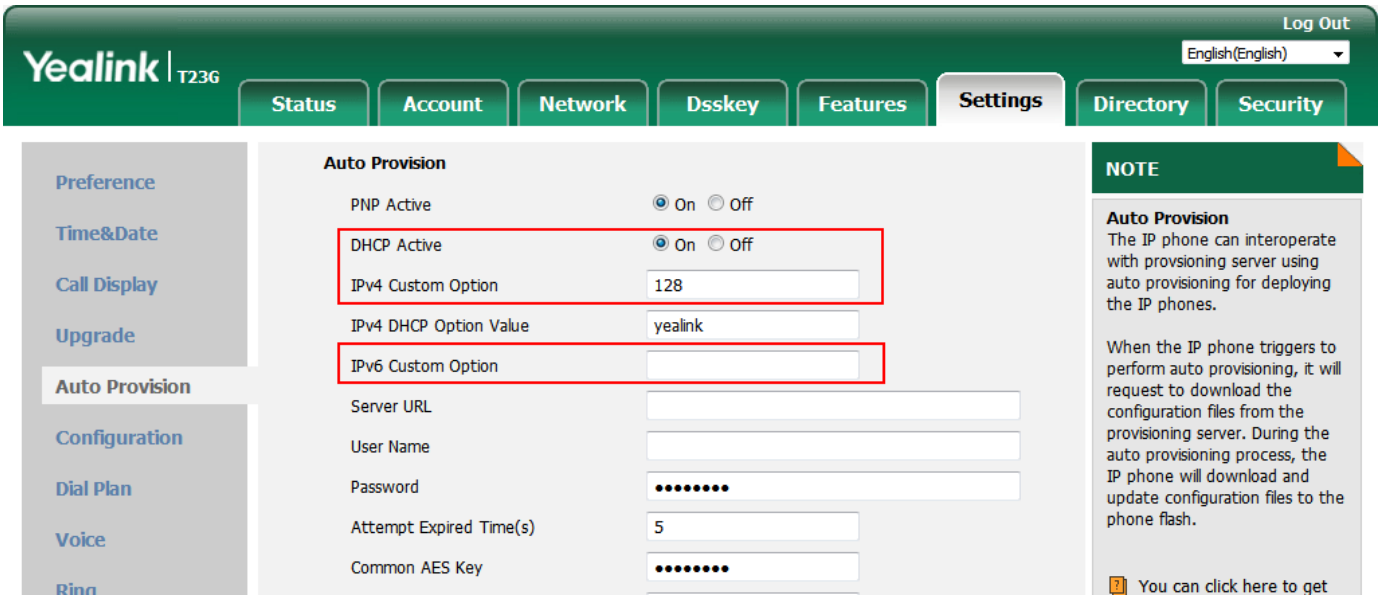
If you are using an IPv6 network, the phone will automatically detect option 59 for obtaining the provisioning server address. DHCP option 59 is used to specify a URL for the boot file to be downloaded by the client.

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.

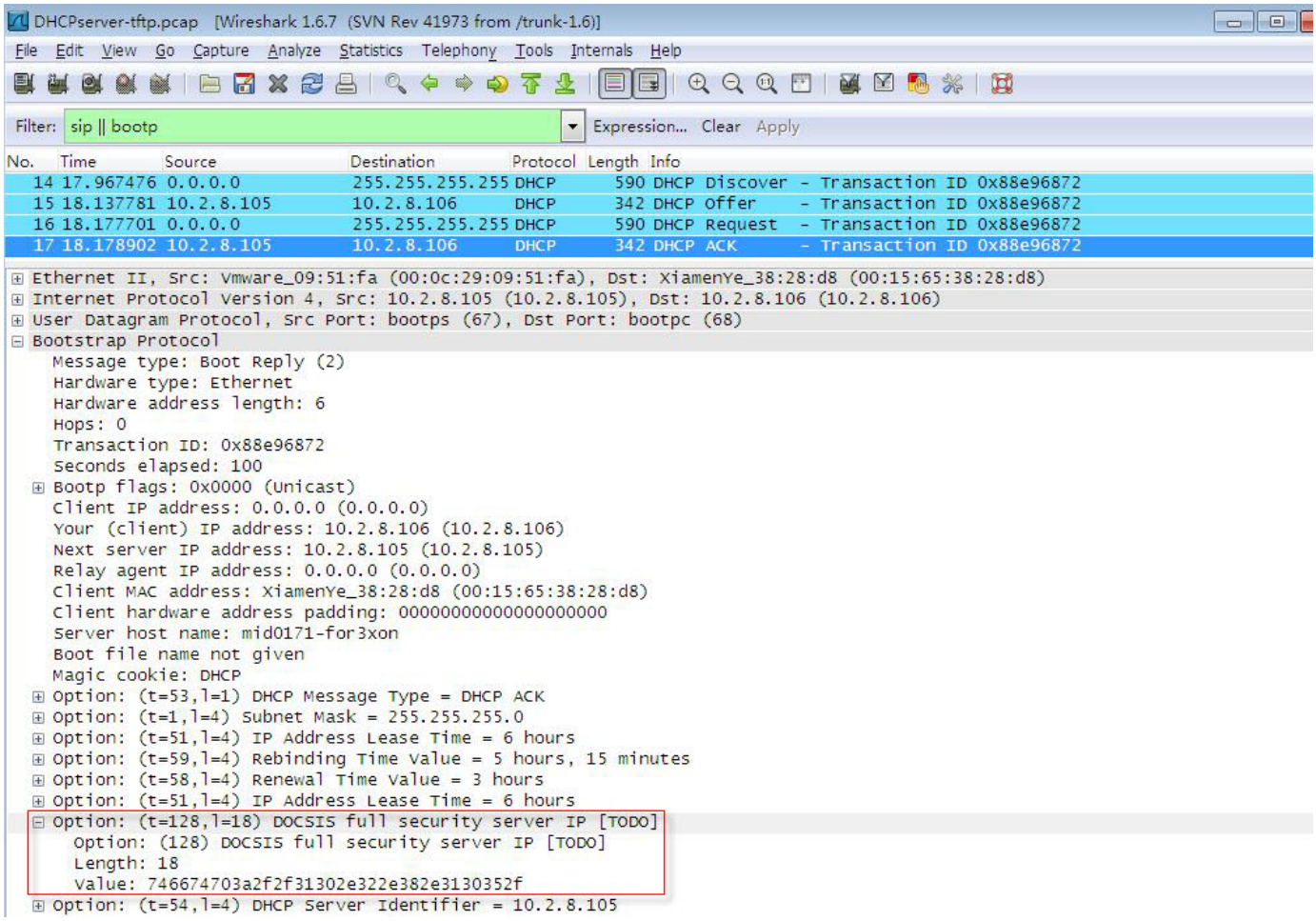
To configure the DHCP option via the web user interface:

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:



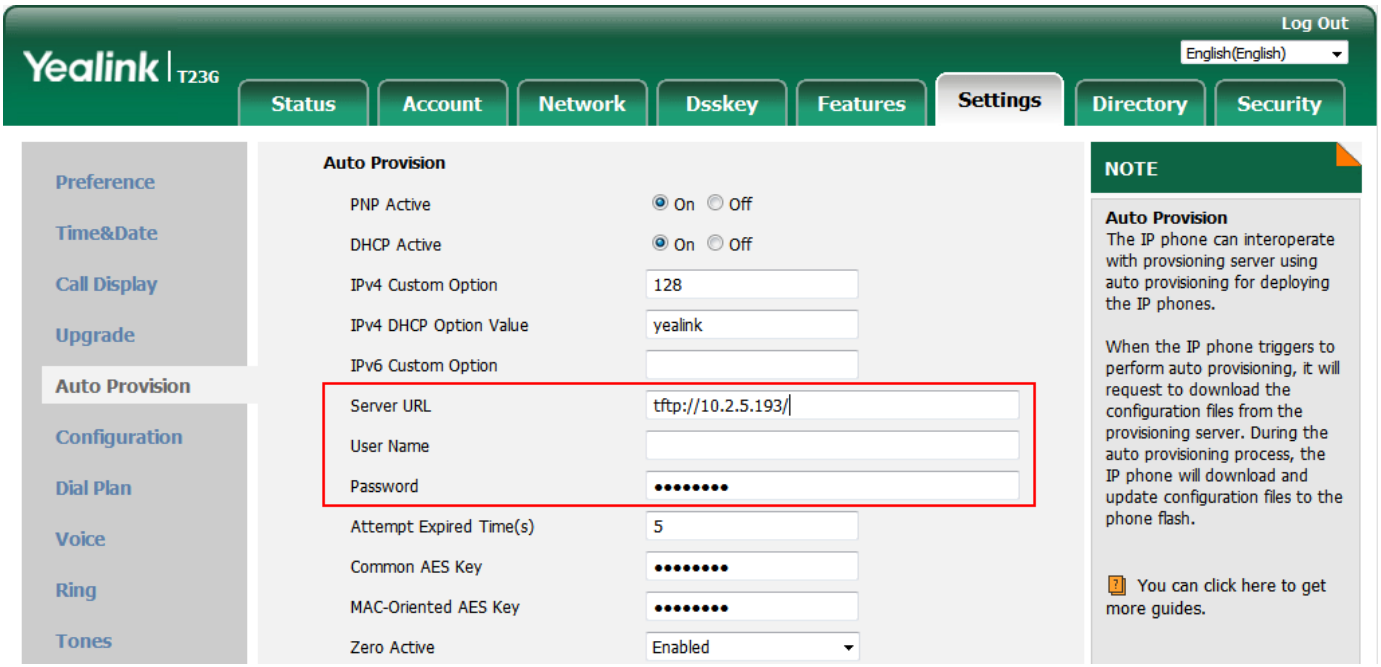
Right-click the root node of the custom option (for example, option 128) shown in the above figure, and select **Copy** > **Bytes** > **Printable Text Only**. Paste the copied text in your favorite text editor to check the address, for example, tftp://192.168.1.100/.

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

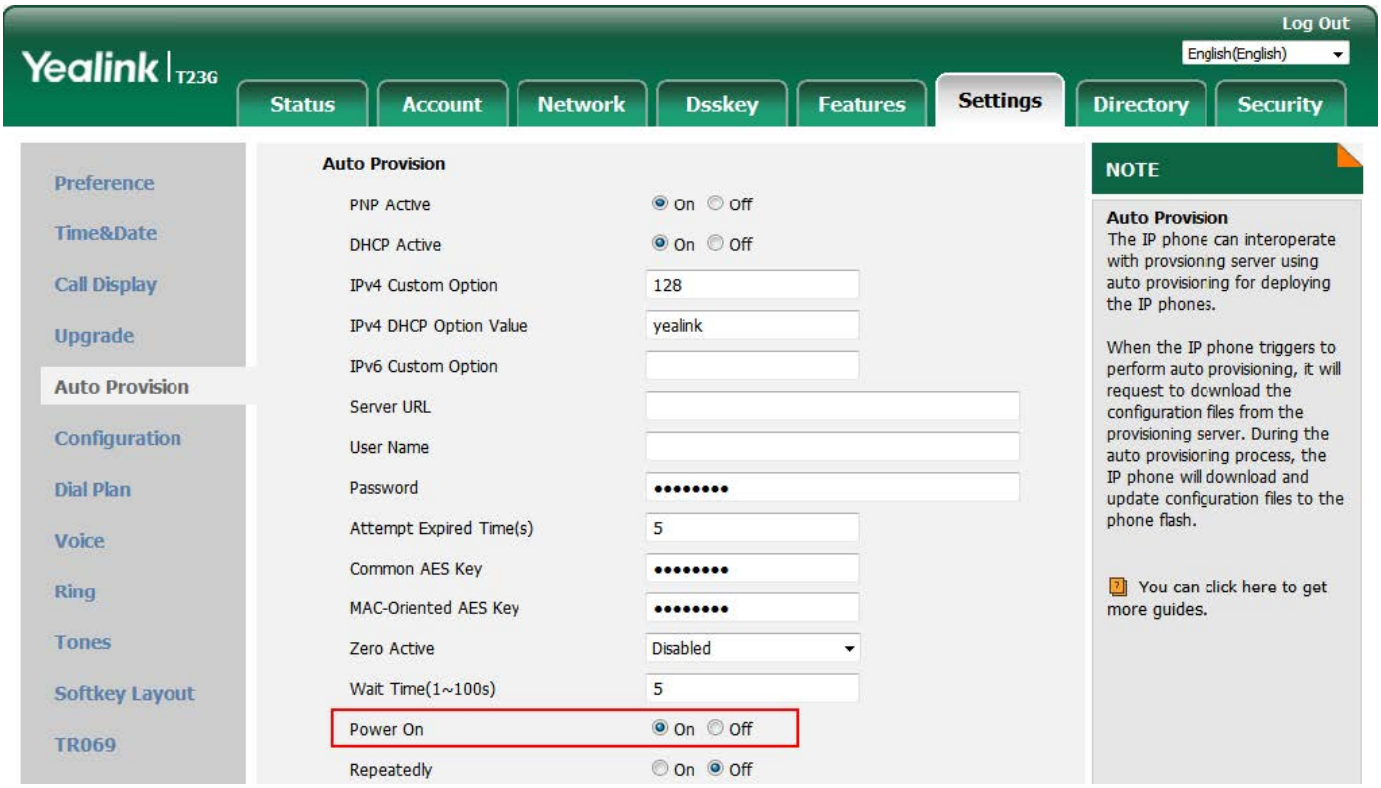
When there is an active call on the IP phone during auto provisioning, the IP phone will detect the call status every 30 seconds. If the call is released within 2 hours, the auto-provisioning will be performed as usual. Otherwise, the process will end due to a timeout.

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.



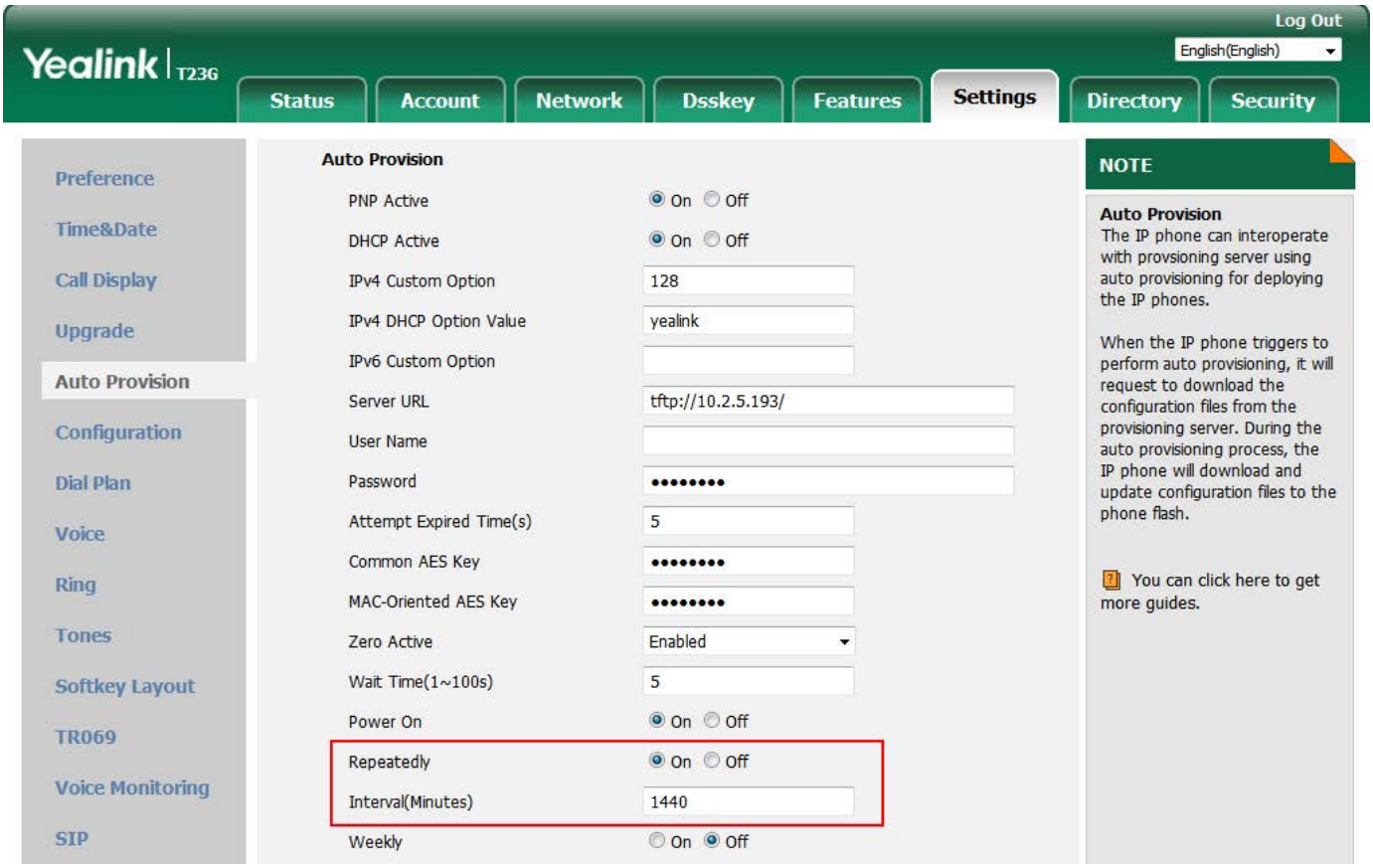
3. Click **Confirm** to accept the change.

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.

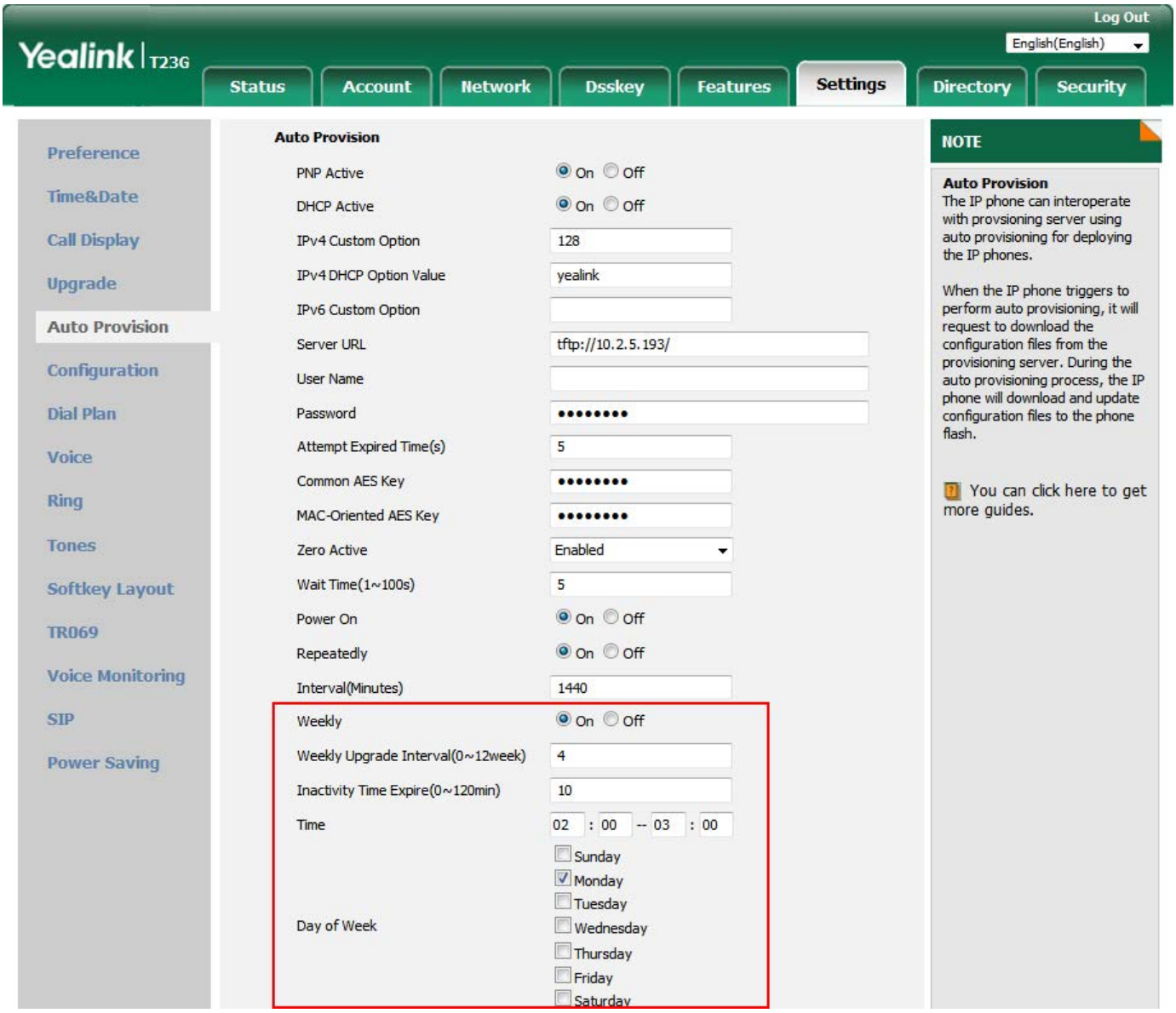
Weekly

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.

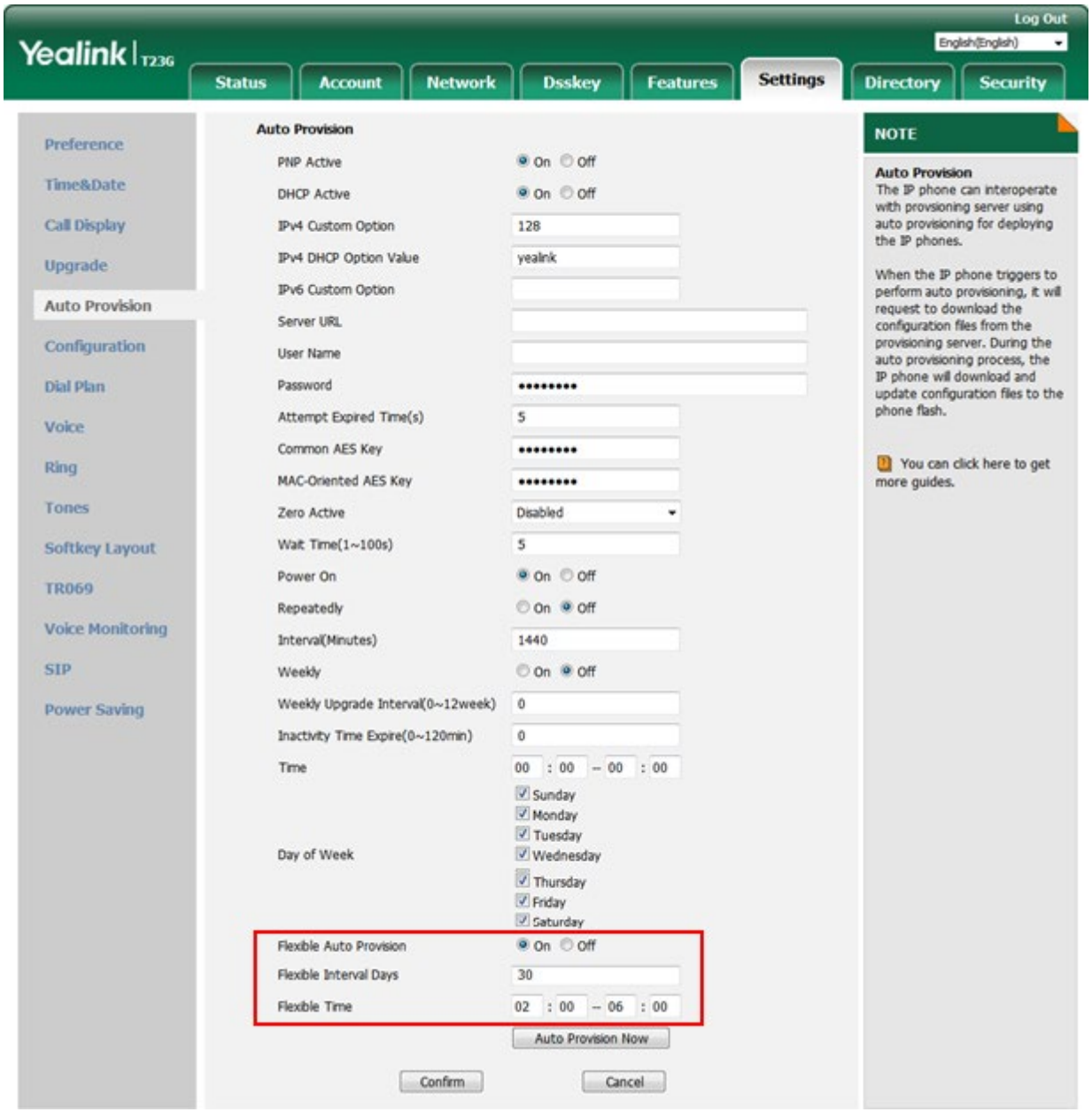
Note that the update time will be recalculated if auto provisioning occurs (for example, Auto Provision Now) during this specific period of time.

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.

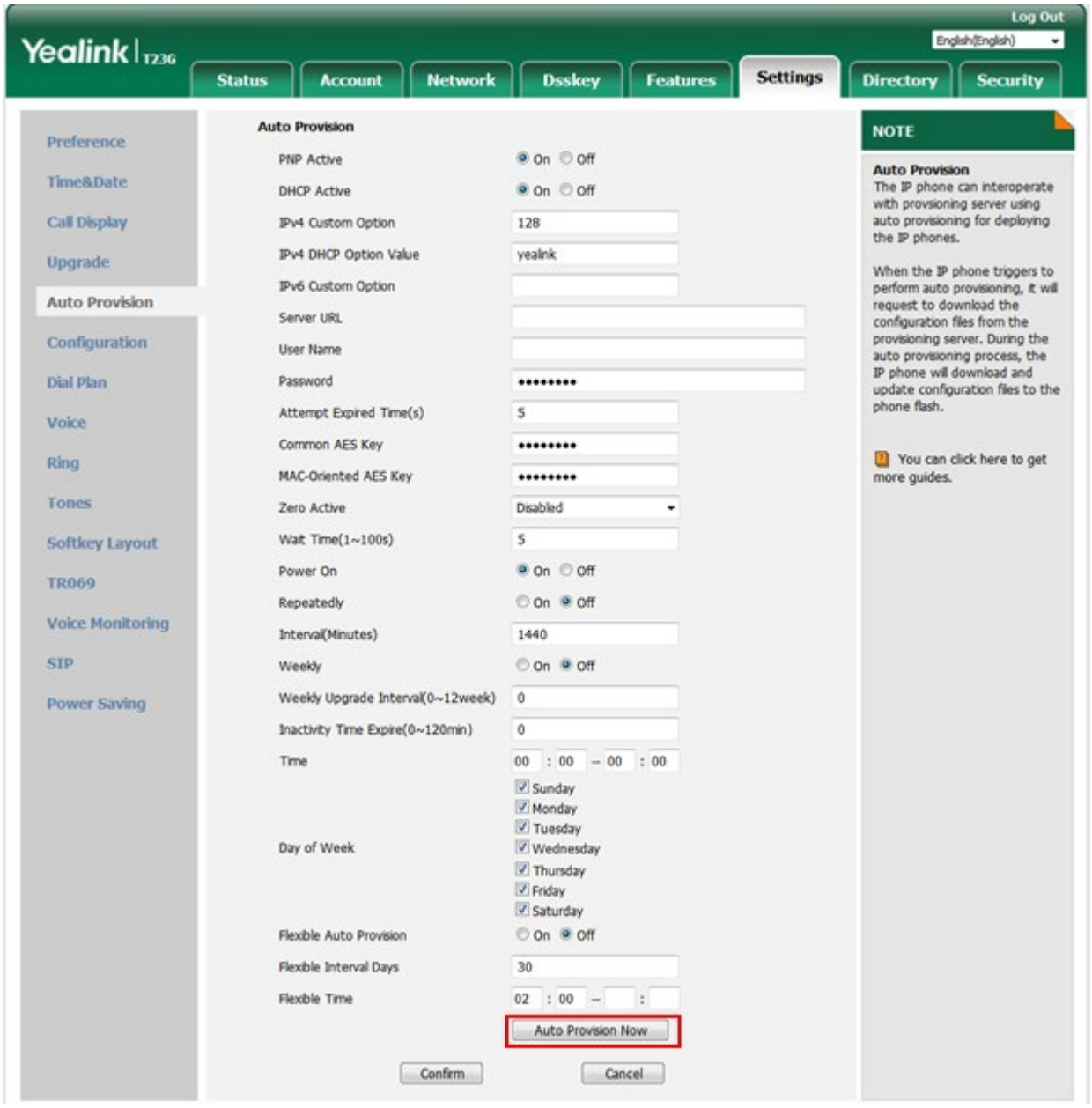
Auto Provision Now

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.

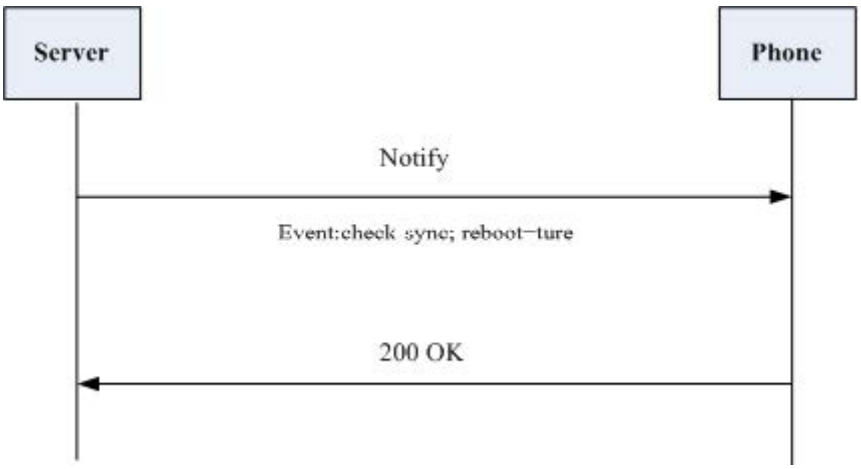
SIP NOTIFY Message

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 "sip.notify_reboot_enable". If the value is set to 1, or the value is set to 0 and the header of the SIP NOTIFY message contains an additional string “reboot=true”, the IP phone will reboot immediately.

For more information on the parameter sip.notify_reboot_enable, refer to the latest IP Phones

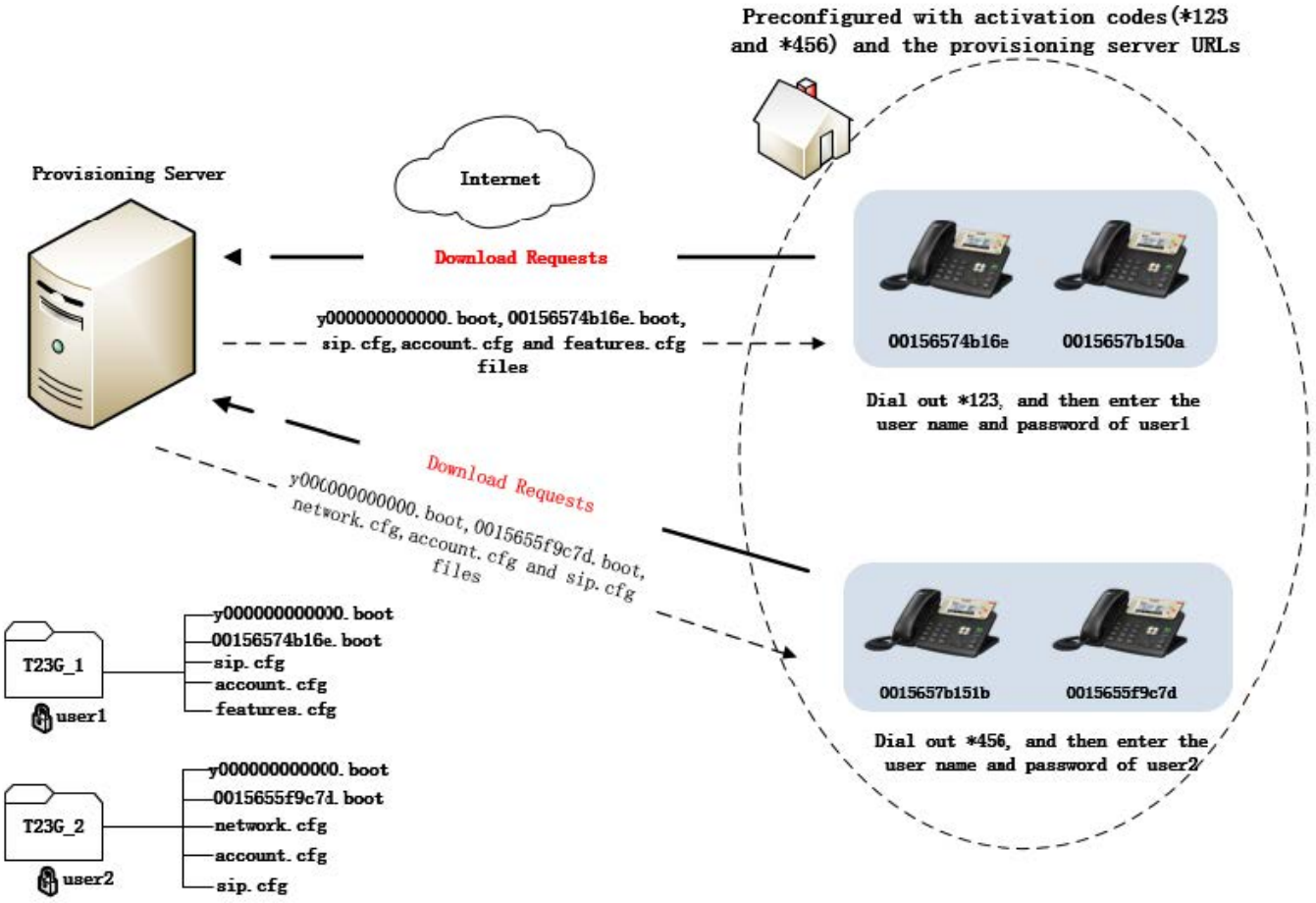
Description of Configuration Parameters in CFG Files or Administrator Guide for your phone on Yealink Technical Support. This method requires server support.

The following figure shows the message flow:



Auto Provisioning via Activation Code

In addition to the updating modes introduced above, users can trigger IP phones to perform auto provisioning by dialing an activation code. To use this method, the activation code and the provisioning server URL need to be pre-configured on the IP phones. This method works only if there is no registered account on the IP phone. It is usually used for IP phones distributed by retail sales. It has the advantage that the IP phones do not need to be handled (for example, registering an account) before sending them to end-users.



The following lists the processes for triggering auto provisioning via activation code:

1. Create multiple directories (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):

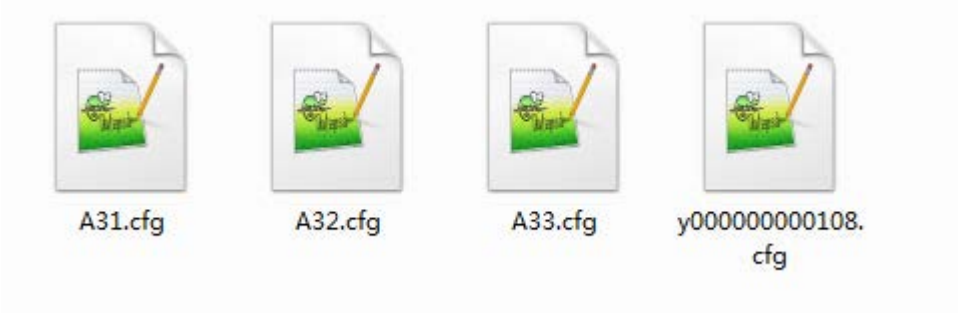
```
#(Optional.) Configure the code name for triggering auto provisioning.
static.autoprovision.X.name
#Configure the activation code.
static.autoprovision.X.code
#Configure the URL of the provisioning server.
static.autoprovision.X.url
#Configure the username and password for downloading boot files 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.

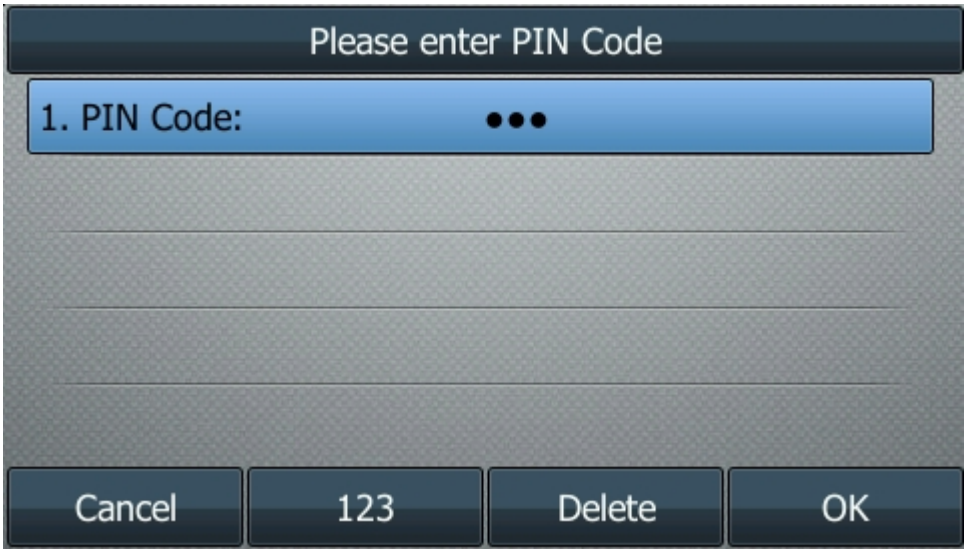
The following lists the processes for triggering auto provisioning via PIN code:

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.

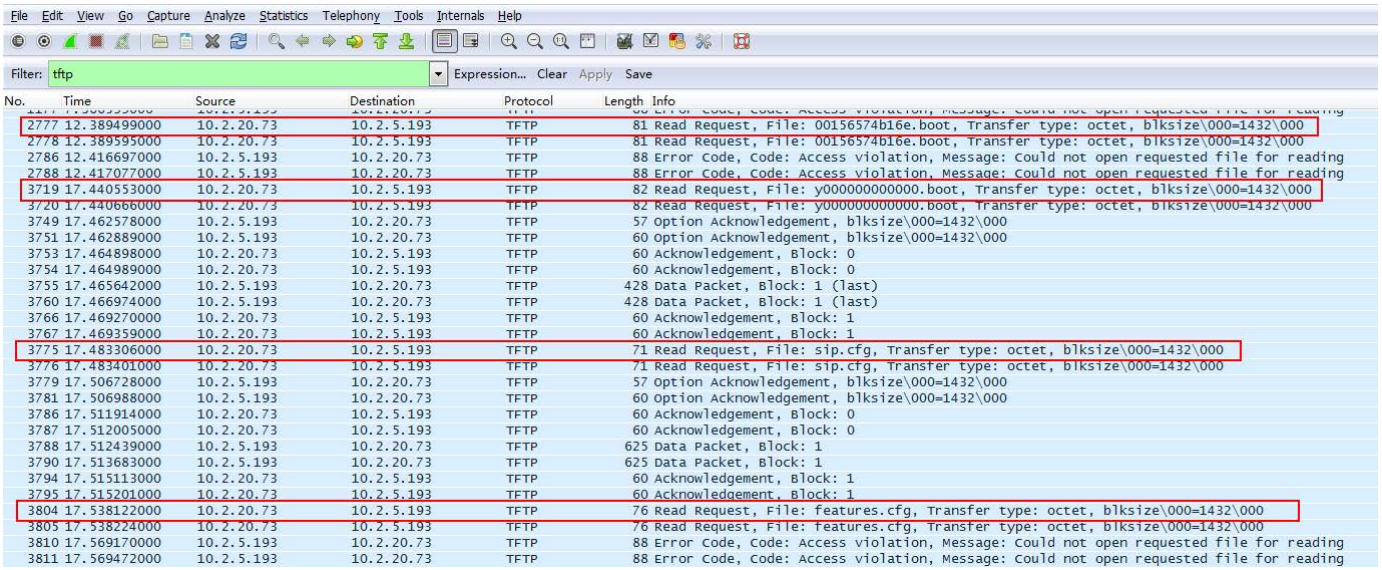
Note that if the personalized settings are static settings, they cannot be kept after auto-provisioning because the static settings will never be saved in the <MAC>-local.cfg file. For more information, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

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.

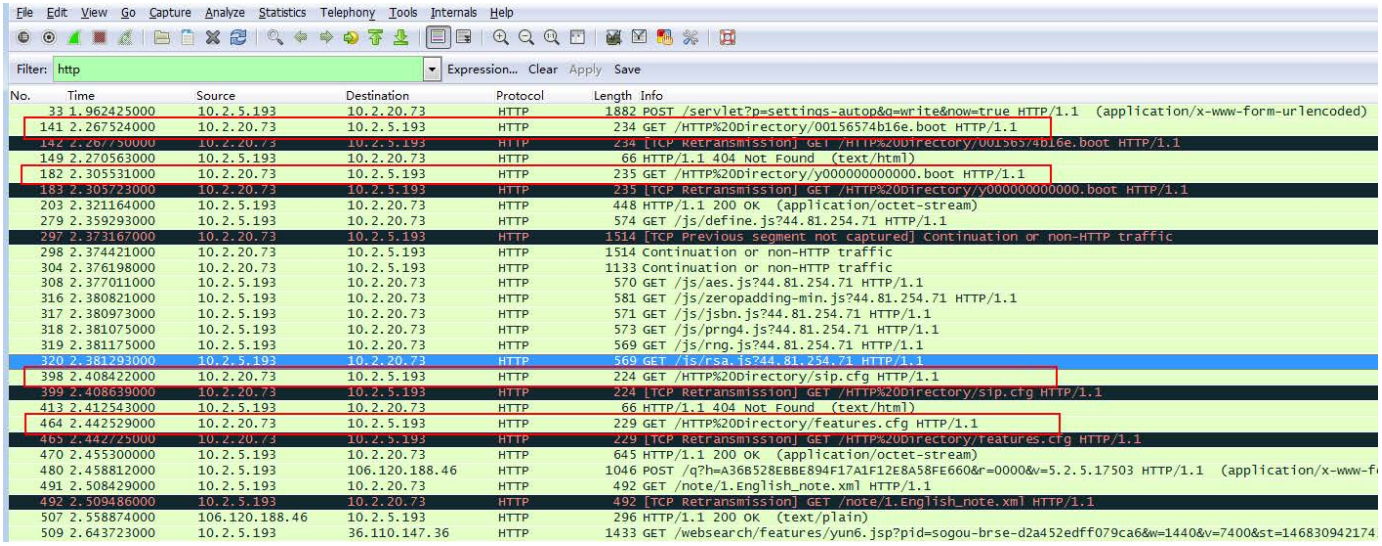
Example 1: Yealink SIP-T23G IP phone downloads the boot file and configuration files from the TFTP server.



Example 2: Yealink SIP-T23G IP phone downloads the boot file and configuration files from the FTP server.



Example 3: Yealink SIP-T23G IP phone downloads 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&q=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.

Log Files

Introduction

Yealink IP phone can log events into two different log files: boot log and system log. You can choose to generate the log files locally or send the log to a syslog server in real time, and use these log files to generate informational, analytic, and troubleshooting phones.

The following table lists the log files generated by the phone:

Local		Syslog Server	Description
<MAC>-all.tgz	boot.log	<MAC>-boot.log	It can only log the last reboot events. It is required to report the logs with all severity levels.
	sys.log	<MAC>-sys.log	It reports the logs with a configured severity level and higher. For example, if you have set the severity level to 4, then the logs with a severity level of 0 to 4 will all be reported.

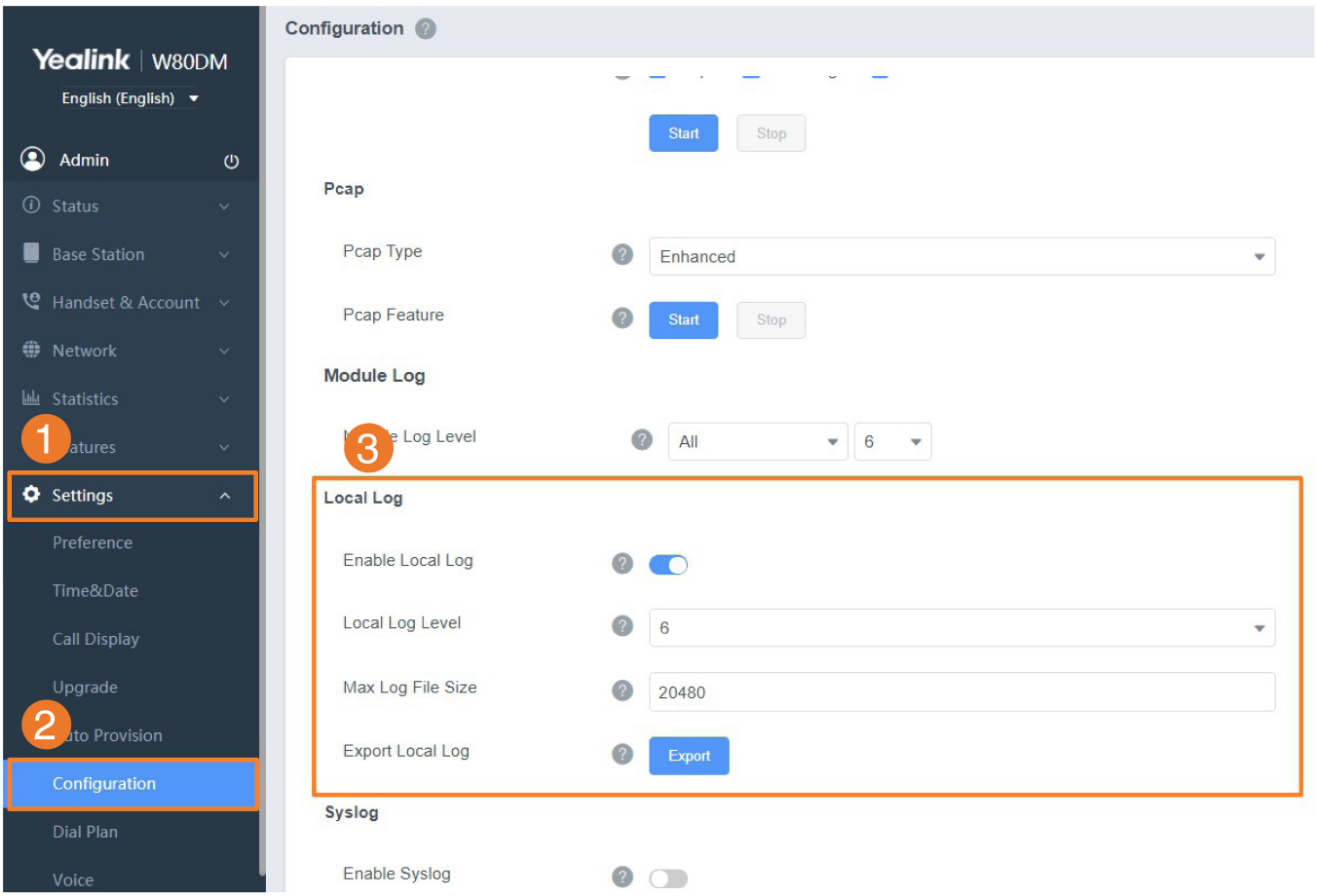
Local Logging

You can enable local logging, specify the severity level, and choose to keep the log locally or upload the local log files to the provisioning server.

Local Logging Configuration

Set via the Web User Interface

1. On the web user interface, go to **Settings** > **Configuration** > **Local Log**.



Configuration Parameter

static.local_log.enable
static.local_log.level
static.local_log.max_file_size
static.auto_provision.local_log.backup.enable
static.auto_provision.local_log.backup.upload_period
static.auto_provision.local_log.backup.path
static.auto_provision.local_log.backup.append
static.auto_provision.local_log.backup.append.limit_mode
static.auto_provision.local_log.backup.append.max_file_size
static.auto_provision.local_log.backup.bootlog.upload_wait_time

Parameter	Permitted Values	Default	Description
static.local_lo	**0**-Disabled, the phone will stop recording log to the log files (<MAC>-	1	It enables or disables the phone from recording the log locally.

g.enable	boot.log and <MAC>-sys.log) locally. The log files recorded before are still kept on the phone. **1**-Enabled, the phone will continue to record log to the log files (<MAC>-boot.log and <MAC>-sys.log) locally. You can upload the local log files to the provisioning server or a specific server, or export them to the local system.		We recommend that you do not disable this feature.
static.local_log.level	**0**-the system is unusable **1**-action must be taken immediately **2**-critical condition **3**-error conditions **4**-warning conditions **5**-normal but significant condition **6**-informational	3	It configures the lowest level of local log information to be rendered to the <MAC>-sys.log file. When you choose a log level, it includes all events of an equal or higher severity level and excludes events of a lower severity level. The logging level you choose determines the lowest severity of events to log.
static.local_log.max_file_size	Integer from 256 to 2048	2048	It configures the maximum size (in KB) of the log files (<MAC>-boot.log and <MAC>-sys.log) can be stored on the IP phone. When this size is about to be exceeded, (1) If the local log files are configured to be uploaded to the server by the parameter static.auto_provision.local_log.backup.enable, the phone will clear all the local log files on the phone once successfully backing up. (2) If static.auto_provision.local_log.backup.enable is set to 0 (Disabled), the phone will erase half of the logs from the oldest log information on the

			phone. **Example**: static.local_log.max_file_size = 1024
static.auto_provision.local_log.backup.enable	**0**-Disabled **1**-Enabled, the phone will upload the local log files to the provisioning server or the specific server to back up these files when one of the following happens: - Auto provisioning is triggered; - The size of the local log files reaches the maximum configured by the parameter static.local_log.max_file_size; - It’ s time to upload local log files according to the upload period configured by the parameter static.auto_provision.local_log.backup.upload_period.		It enables or disables the phone to upload the local log files (<MAC>-boot.log and <MAC>-sys.log) to the provisioning server or a specific server. Note: The upload path is configured by the parameter static.auto_provision.local_log.backup.path.
static.auto_provision.local_log.backup.upload_period	Integer from 30 to 86400	30	It configures the period (in seconds) of the local log files (<MAC>-boot.log and <MAC>-sys.log) uploads to the provisioning server or a specific server. It works only if "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled).
static.auto_provision.local_log.backup.path	URL within 1024 characters	Blank	It configures the upload path of the local log files (<MAC>-boot.log and <MAC>-sys.log). If you leave it blank, the phone will upload the local log files to the provisioning server. If you configure a relative URL (for example, /upload), the phone will

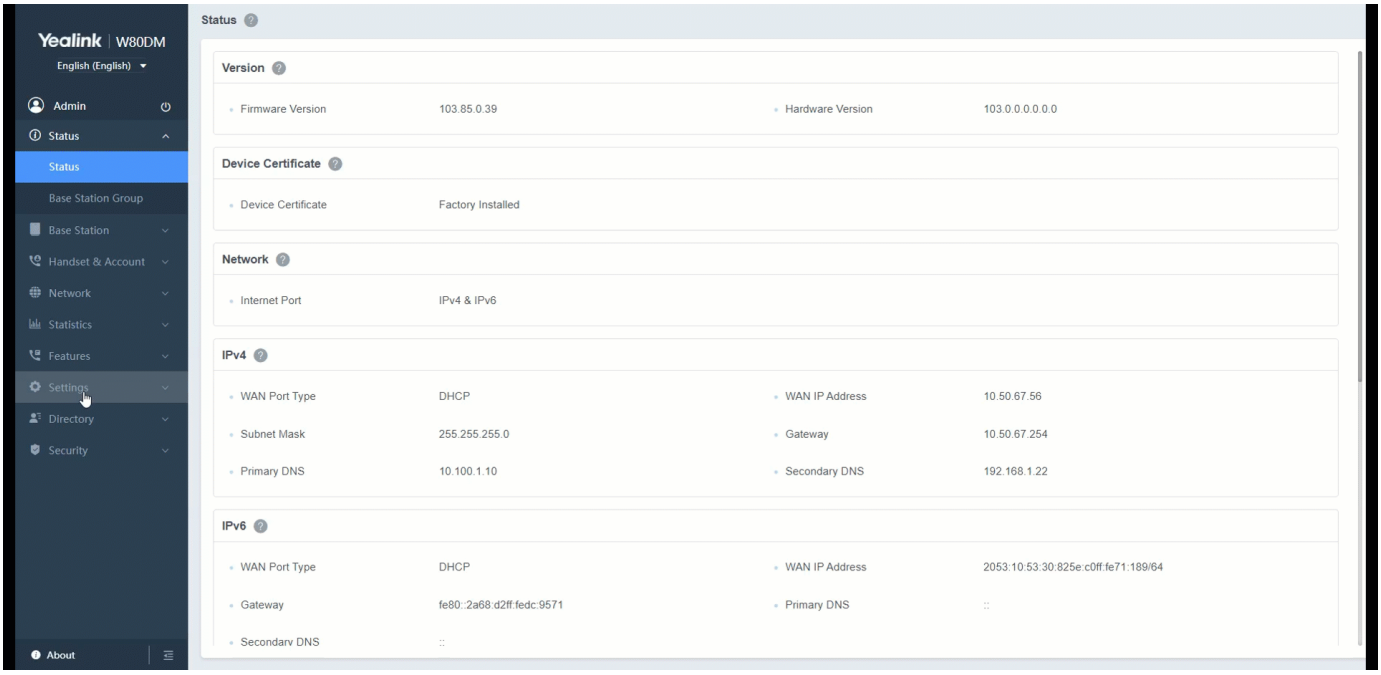
			upload the local log files by extracting the root directory from the access URL of the provisioning server. If you configure an absolute URL with the protocol (for example, tftp), the phone will upload the local log files using the desired protocol. If no protocol, the phone will use the same protocol with auto provisioning for uploading files. **Example**: static.auto_provision.local_log.backup.path = tftp://10.3.6.133/upload/ It works only if "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled).
static.auto_provision.local_log.backup.append	**0**-Overwrite **1**-Append (not applicable to TFTP Server)	0	It configures whether the uploaded local log files (<MAC>-boot.log and <MAC>-sys.log) overwrite the existing files or are appended to the existing files.
static.auto_provision.local_log.backup.append.limit_mode	**0**-Append Delete, the server will delete the old log, and the phone will continue uploading the log. **1**-Append Stop, the phone will stop uploading the log.	0	It configures the behavior when local log files (<MAC>-boot.log and <MAC>-sys.log) on the provisioning server or a specific server reach the maximum file size.
static.auto_pr	Integer from 200 to 65535	1024	It configures the maximum size (in KB) of the local log files (<MAC>-boot.log

ovision.local_log.backup.append.max_file_size			and <MAC>-sys.log) that can be stored on the provisioning server or a specific server.
static.auto_provision.local_log.backup.bootlog.upload_wait_time	Integer from 1 to 86400	120	It configures the waiting time (in seconds) before the phone uploads the boot log file (<MAC>-boot.-log) to the provisioning server or a specific server after startup.

Export the Log Files to a Local PC

Procedure

1. From the web user interface, go to **Settings** > **Configuration**.
2. In the **Enable Local Log** field, select **Enabled** or **ON**.
3. Select **6** from the **Local Log Level** drop-down menu.
   The default local log level is "3".
4. Enter the limit size of the log files in the **Max Log File Size** field.
5. Click **Confirm** to accept the change.
6. Reproduce the issue.
7. Click **Export** to open the file download window, and then save the file to your local system.



View the Log Files

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

- <0+emerg >
- <1+alert >
- <2+crit >
- <3+error >
- <4+warning >
- <5+notice >
- <6+info >

The default local log level is 3.

The following figure shows a portion of a boot log file (for example, 00156574b150-boot.log):

```
Jan  1 00:00:24 syslogd started: BusyBox v1.10.3
Jan  1 00:00:25 sys [655]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
Jan  1 00:00:25 sys [655]: ANY <0+emerg > ANY =3
Jan  1 00:00:25 sys [655]: ANY <0+emerg > Version  :7.2.0.10 for release
Jan  1 00:00:25 sys [655]: ANY <0+emerg > Built-at :Apr 20 2016,11:32:02
May 26 00:00:02 Log [706]: ANY <0+emerg > Log  log :sys=1,cons=1,time=0,E=3,W=4,N=5,I=6,D=7
May 26 00:00:02 Log [706]: ANY <0+emerg > ETLL=3
May 26 00:00:02 auto[706]: ANY <0+emerg > autoServer log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
May 26 00:00:02 auto[706]: ANY <0+emerg > ANY =3
May 26 00:00:02 auto[706]: ANY <0+emerg > Version  :6.1.0.8 for release
May 26 00:00:02 auto[706]: ANY <0+emerg > Built-at :May 25 2016,10:26:42
May 26 00:00:02 sys [706]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
May 26 00:00:02 sys [706]: ANY <0+emerg > LSYS=3
May 26 00:00:02 ATP [706]: ANY <0+emerg > ATP log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
May 26 00:00:02 ATP [706]: ANY <0+emerg > ANY =3
May 26 00:00:05 sys [835]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
May 26 00:00:05 sys [835]: ANY <0+emerg > LSYS=3
May 26 00:00:05 sua [835]: ANY <0+emerg > sua  log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
May 26 00:00:05 sua [835]: ANY <0+emerg > ANY =5
May 26 00:00:05 sua [835]: ANY <0+emerg > ANY =3
May 26 00:00:06 Log [884]: ANY <0+emerg > Log  log :sys=1,cons=0,time=0,E=3,W=4,N=5,I=6,D=7
May 26 00:00:06 Log [884]: ANY <0+emerg > ANY =5
May 26 00:00:07 ipvp[887]: ANY <0+emerg > 807.194.980:ipvp log :type=1,time=1,E=3,W=4,N=5,I=6,D=7
May 26 00:00:07 ipvp[887]: ANY <0+emerg > 807.196.179:Version  :1.0.0.8 for release
May 26 00:00:07 ipvp[887]: ANY <0+emerg > 807.197.104:Built-at :Feb 29 2016,14:11:35
May 26 00:00:07 ipvp[887]: ANY <0+emerg > 807.198.138:ANY =4
May 26 00:00:07 sys [887]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
May 26 00:00:07 sys [887]: ANY <0+emerg > LSYS=3
May 26 00:00:08 TR9 [897]: ANY <0+emerg > TR9  log :sys=1,cons=0,time=0,E=3,W=4,N=5,I=6,D=7
```

The boot log file reports the logs with all severity levels.

The following figure shows a portion of a sys log file (for example, 00156574b150-sys.log):

```
May 31 09:02:05 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
May 31 09:02:37 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
May 31 09:03:16 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
May 31 09:03:27 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
May 31 09:03:41 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
May 31 09:03:47 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
May 31 19:28:18 sys [1076]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
May 31 19:28:18 sys [1076]: ANY <0+emerg > LSYS=3
Jun  1 02:33:52 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
Jun  1 07:28:17 sys [1111]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
Jun  1 07:28:17 sys [1111]: ANY <0+emerg > LSYS=3
Jun  1 11:34:57 sua [835]: SUB <3+error > [000] BLF Can't find js by sid(0)
Jun  1 11:34:57 sua [835]: SUB <3+error > [000] BLF Can't find js by sid(0)
[ web ]
step = 2
```

The -sys.log file reports the logs with a configured severity level and higher. For example, if you have configured the severity level of the log to be reported to the -sys.log file to 4, then the log with a severity level of 0 to 4 will all be reported.

Syslog Logging

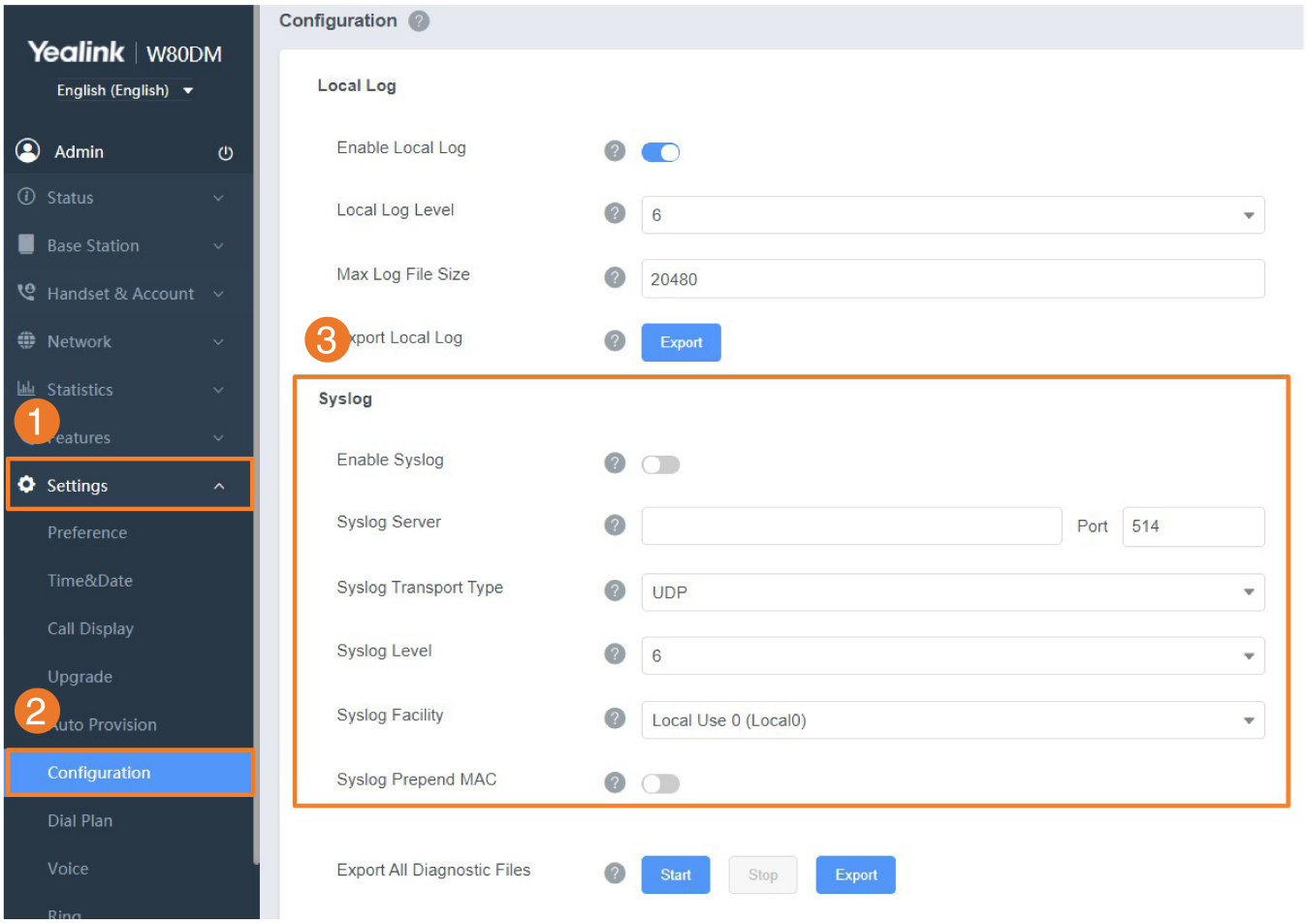
You can also configure the to send syslog messages to a syslog server in real time.

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

Syslog Logging Configuration

Set via the Web User Interface

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



Configuration Parameter

```
static.syslog.enable
static.syslog.server
static.syslog.server_port
static.syslog.transport_type
static.syslog.level
static.syslog.facility
static.syslog.prepend_mac_address.enable
```

Parameter	Permitted Values	Default	Description
static.syslog.enable	**0**-Disabled **1**-Enabled	0	It enables or disables the phone from uploading log messages to the syslog server in real time.

static.syslog.server	String within 99 characters	Blank	It configures the IP address or domain name of the syslog server when exporting logs to the syslog server.
static.syslog.server_port	Integer from 1 to 65535	514	It configures the port of the syslog server.
static.syslog.transport_type	**0**-UDP **1**-TCP **2**-TLS	0	It configures the transport protocol that the IP phone uses when uploading log messages to the syslog server.
static.syslog.level	**0**-Emergency: system is unusable **1**-Alert: action must be taken immediately **2**-Critical: critical conditions **3**-Critical: error conditions **4**-Warning: warning conditions **5**-Warning: normal but significant condition **6**-Information	3	It configures the lowest level of syslog information that displays in the syslog. When you choose a log level, it includes all events of an equal or higher severity level and excludes events of a lower severity level. The logging level you choose determines the lowest severity of events to log.

	al: informational messages		
static.syslog.facility	**0**-Kernel Messages **1**-User-level Messages **2**-Mail System **3**-System Daemons **4**-Security/ Authorization Messages (Note 1) **5**-Messages are generated internally by syslog **6**-Line Printer Subsystem **7**-Network News Subsystem **8**-UUCP Subsystem **9**-Clock Daemon (note 2) **10**-	16	It configures the facility that generates the log messages. For more information, refer to RFC 3164.

	Security/ Authorization Messages (Note 1) **11**-FTP Daemon **12**-NTP Subsystem **13**-Log Audit (note 1) **14**-Log Alert (note 1) **15**-Clock Daemon (Note 2) **16**-Local Use 0 (Local0) **17**-Local Use 1 (Local1) **18**-Local Use 2 (Local2) **19**-Local Use 3 (Local3) **20**-Local Use 4 (Local4) **21**-Local Use 5 (Local5)		

	22-Local Use 6 (Local6) **23**-Local Use 7 (Local7) ① Various operating systems have been found to utilize Facilities 4, 10, 13 and d		

		14 for security/ authorization, audit, and alert messages which seem to be similar. ② Various operating		

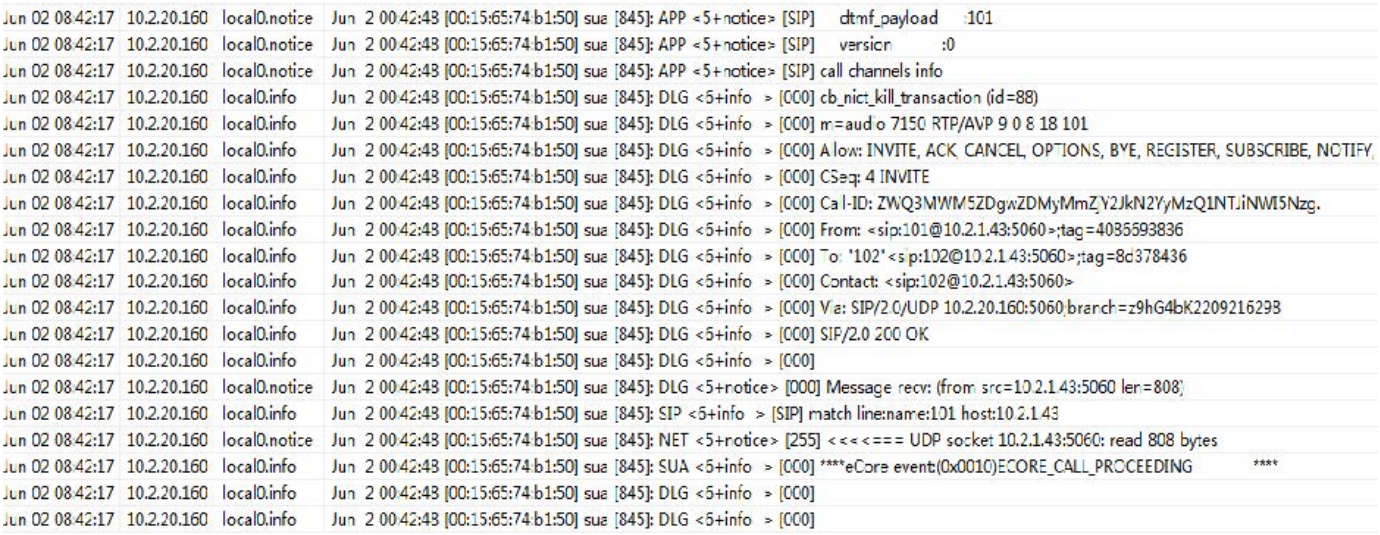
	systems have been found to utilize both Facilities 9 and 15 for clock (cron/at) messages.		
static.sy	**0**-Disabled	0	It enables or disables the phone from prepending the MAC

slog.prepend_mac_address.enable	**1**-Enabled		address to the log messages exported to the syslog server.

View the Syslog Messages on Your Syslog Server

You can view the syslog file in the desired folder on the syslog server. The location of the folder may differ from the syslog server. For more information, refer to the network resources.

The following figure shows a portion of the syslog:



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. (The same operation to reset W70B/W75B/W80B/W90B.)

Five ways to reset the phone:

- **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.
- **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. All configurations saved in the <MAC>-local.cfg configuration file on the phone will be reset.
- **Reset to Factory**: All configurations on the phone will be reset.

You can reset the 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.

- The **Reset local settings**/**Reset non-static settings**/**Reset static settings**/**Reset user data & local config** option on the web user interface appears only if "static.auto_provision.custom.protect" is set to 1.
- You can also press and hold the device key on the W90DM/W90B for 20 seconds to reset the device to factory configurations. (Hard reset) Please note that the hard reset will delete all the bases and handsets.
- You can press and hold the device key on the W75DM/W75B for 20 seconds to reset the DM to factory configurations or 30 seconds to reset the Base to factory configurations. (Hard

reset) Please note that the hard reset will delete all the bases and handsets. Power on 4-6 times repeatedly, and do not power off for more than 5 seconds each time.

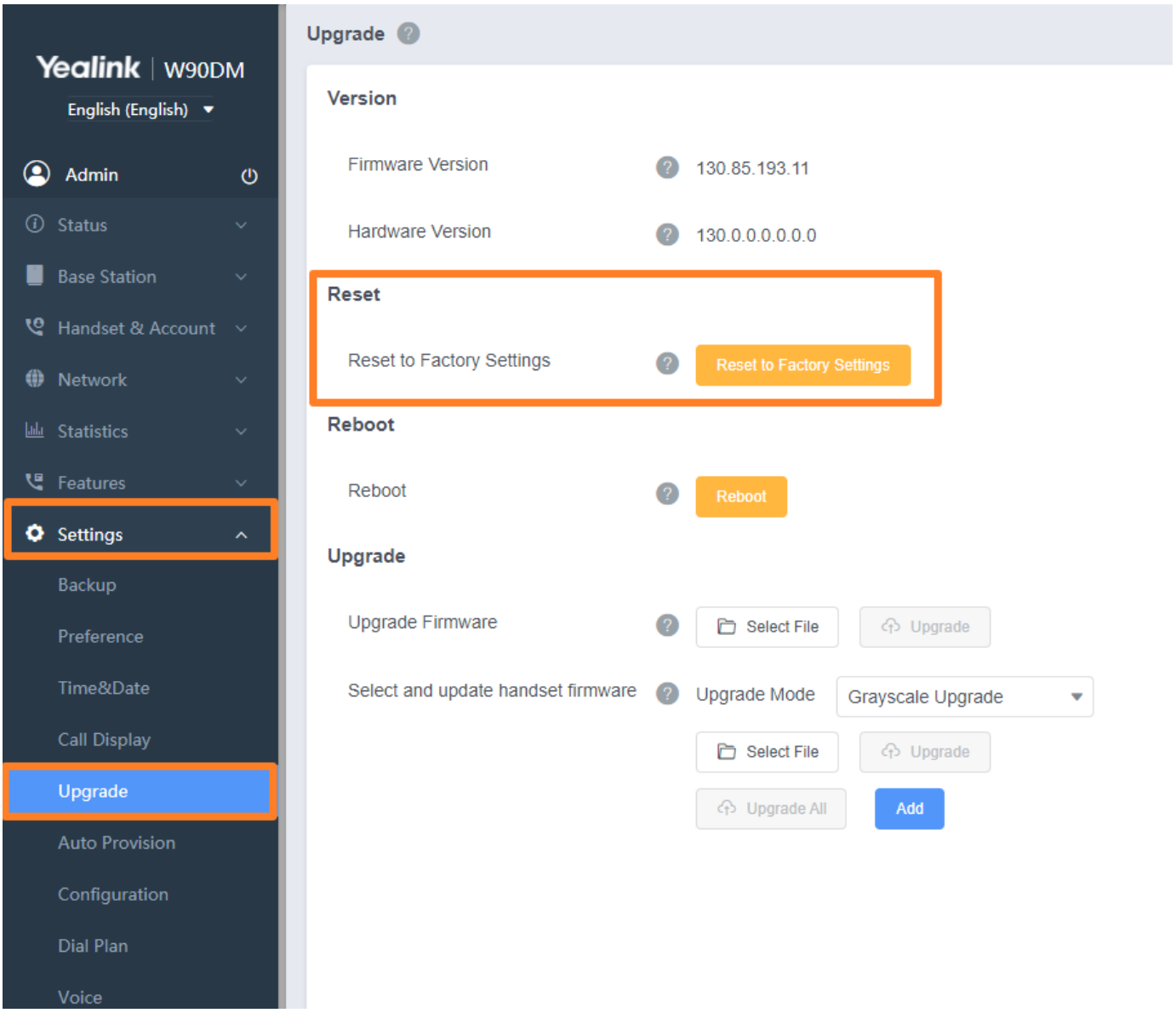
- Primary DM: LAN/ROLE/DECT light turns solid orange.
- Secondary DM: LAN light turns solid orange, ROLE light turns solid green, DECT light turns solid orange.

Reset the Phone to 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 on the web user interface will only reset the configuration, and the bases and handsets will not be deleted.

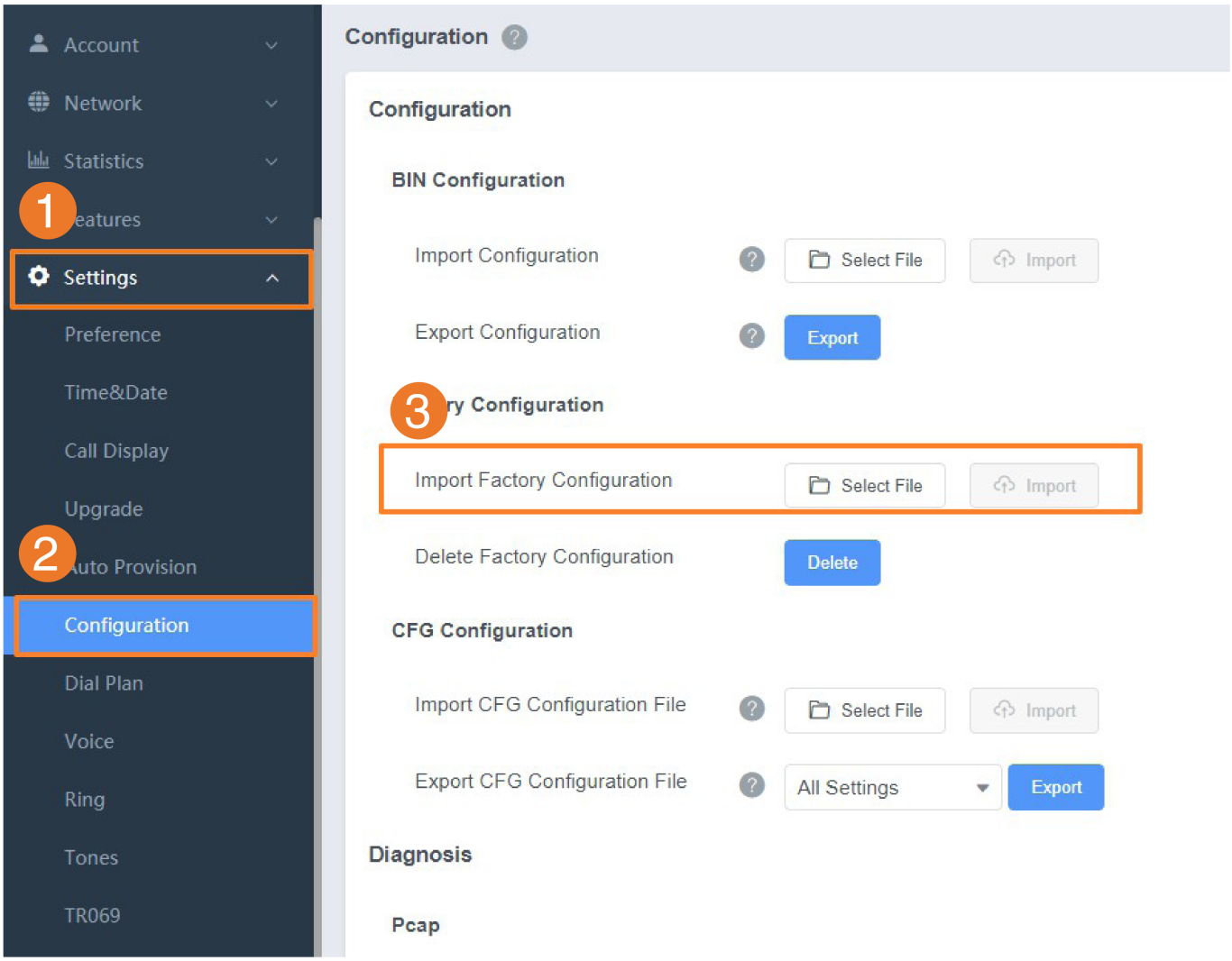


Reset the IP phone to Custom Factory Settings

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**.



Configuration Parameter

static.features.custom_factory_config.enable
static.custom_factory_configuration.url

Parameter	Permitted Values	Default	Description
static.features.custom_factory_config.enable	**0**-Disabled **1**-Enabled, Import Factory Configuration item will be displayed on the 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	It enables or disables the Custom Factory Configuration feature.
static.	URL within 511 characters	Bl	It configures

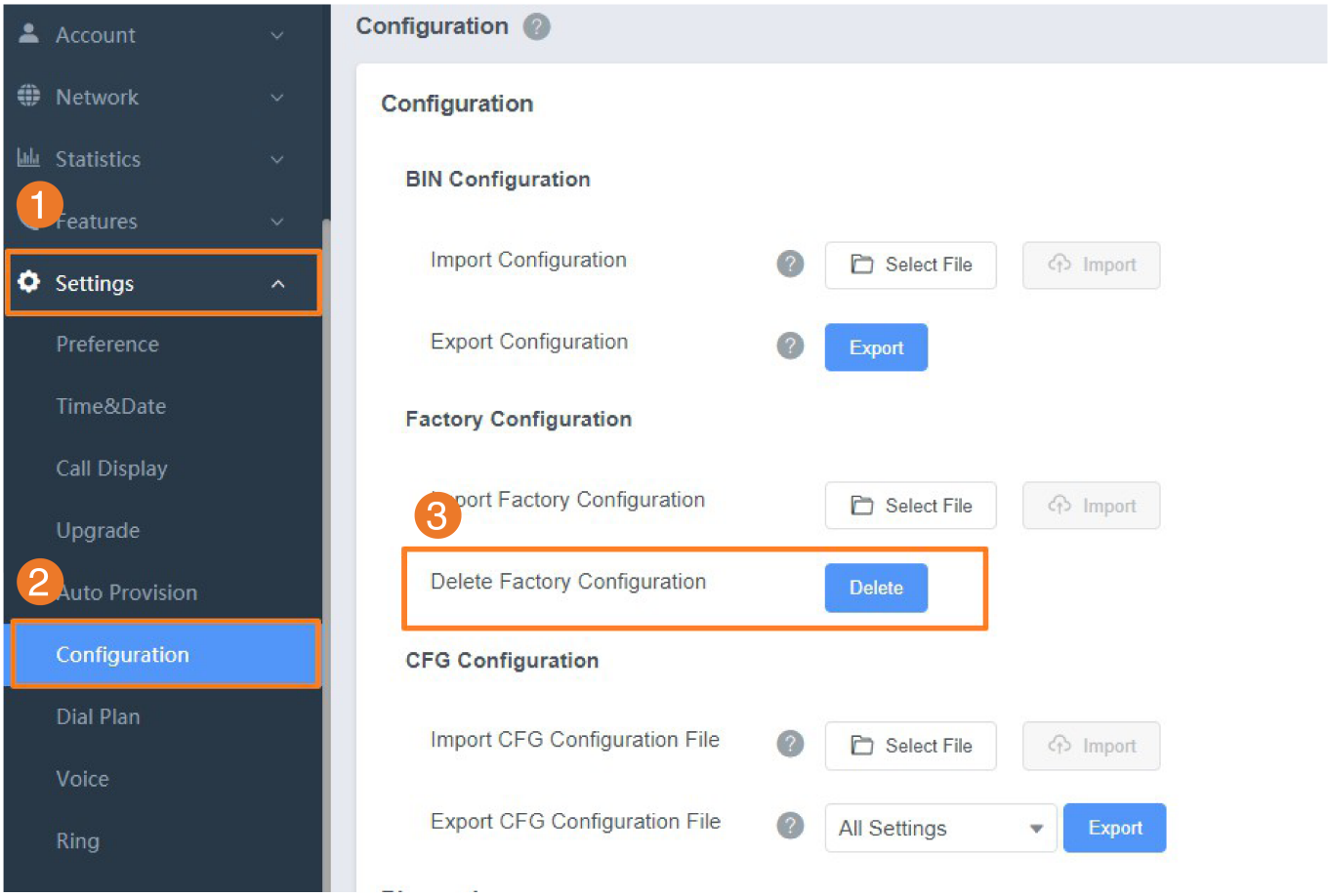
custom_factory_configuration.url		ank	the access URL of the custom factory configuration files. It works only if "static.features.custom_factory_config.enable" is set to 1 (Enabled), and the file format of the custom factory configuration file must be *.bin.

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 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.



Packets Capture

Introduction

You can capture packets in two ways: by capturing the packets via the web user interface or by using the Ethernet software.

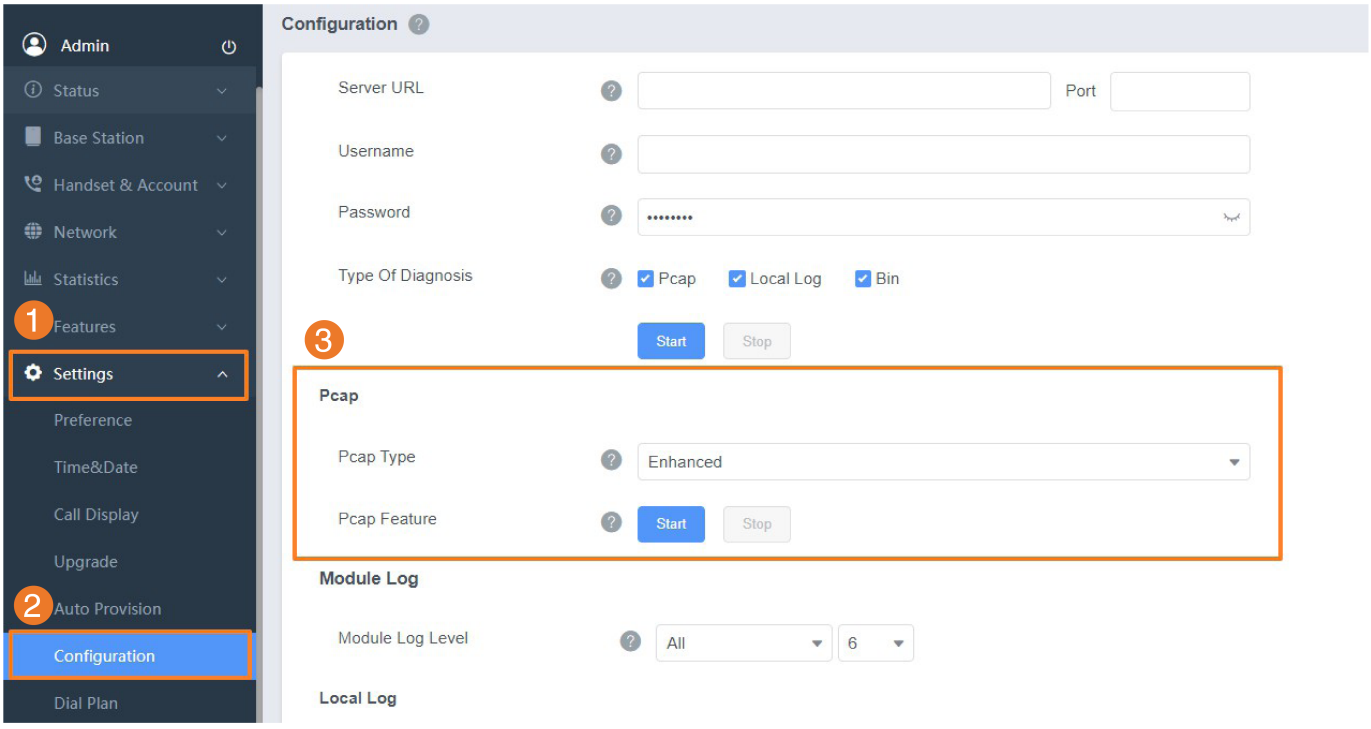
You can analyze the packet captured for troubleshooting purposes.

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.



Watch Dog

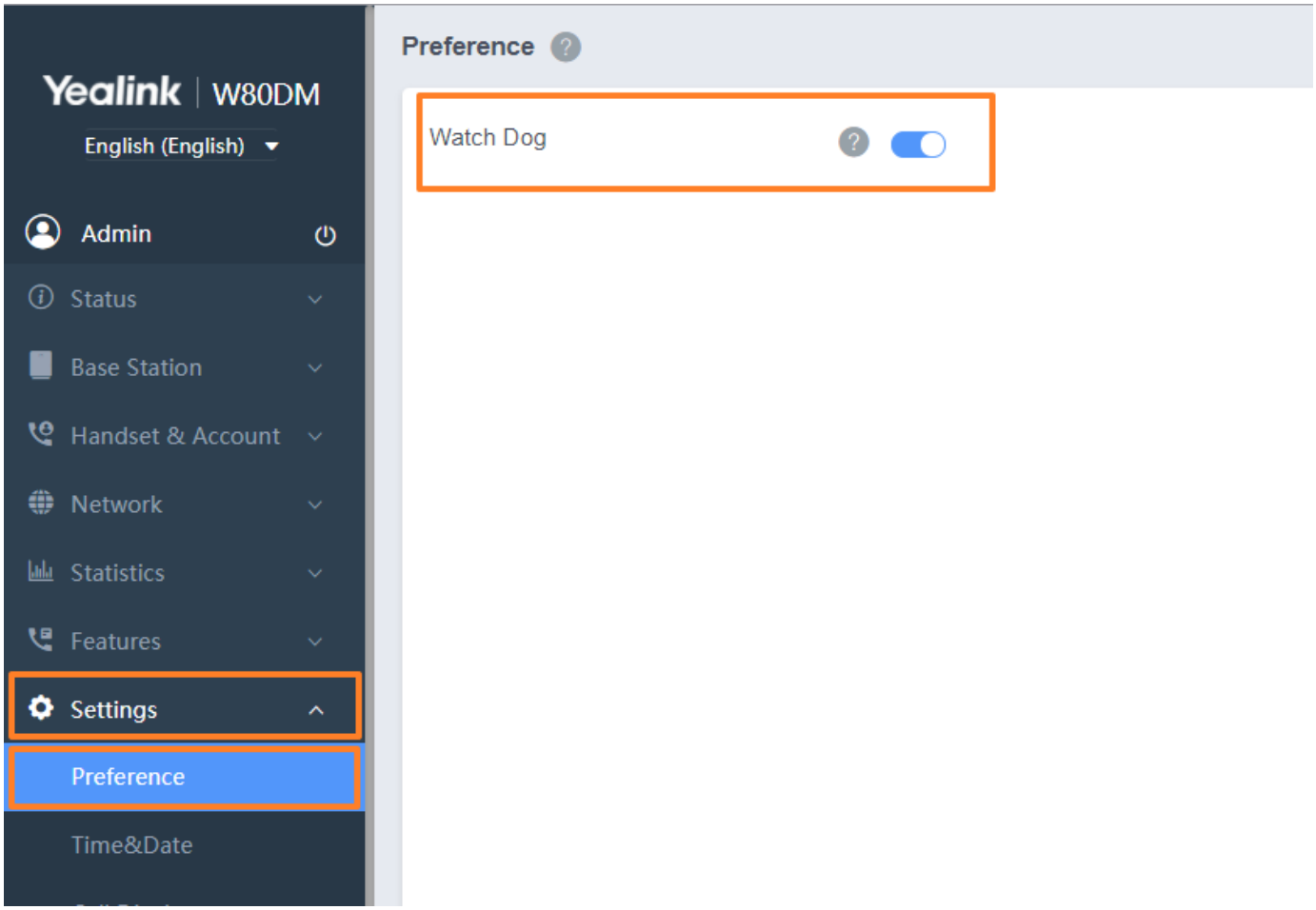
Introduction

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**.



Configuration Parameter

static.watch_dog.enable

Parameter	Permitted Values	Default	Description

		t	
static.watch_dog.enable	**0**-Disabled **1**-Enabled, the phone will reboot automatically when the system crashes.	1	It enables or disables the Watch Dog feature.

Analyze Configuration Files

Introduction

Wrong configurations may have an impact on phone use. You can export configuration file(s) to check the current configuration of the IP phone and troubleshoot if necessary. You can also import configuration files for a quick and easy configuration.

We recommend that you edit the exported CFG file instead of the BIN file to change the phone’ s current settings.

The config.bin file is an encrypted file. For more information on config.bin file, contact your Yealink reseller.

Export CFG Configuration Files from Phone

You can export the phone’ s configuration file to the local and make changes to the phone’ s current feature settings.

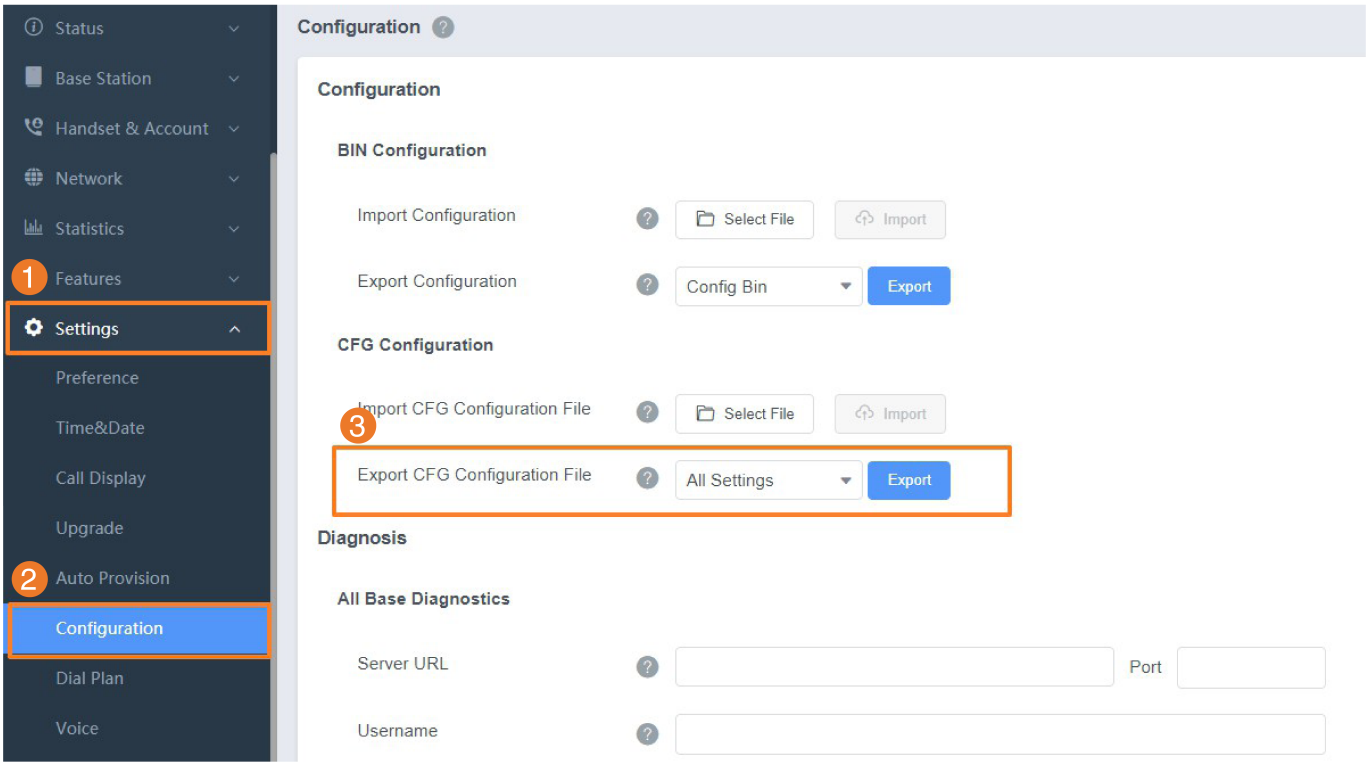
You can apply these changes to any phone by importing the configuration files via the web user interface.

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

Procedure

1. Go to **Settings** > **Configuration**.
2. In the **Export CFG Configuration File** field, click **Export** to open the file download window, and then save the file to your local system.

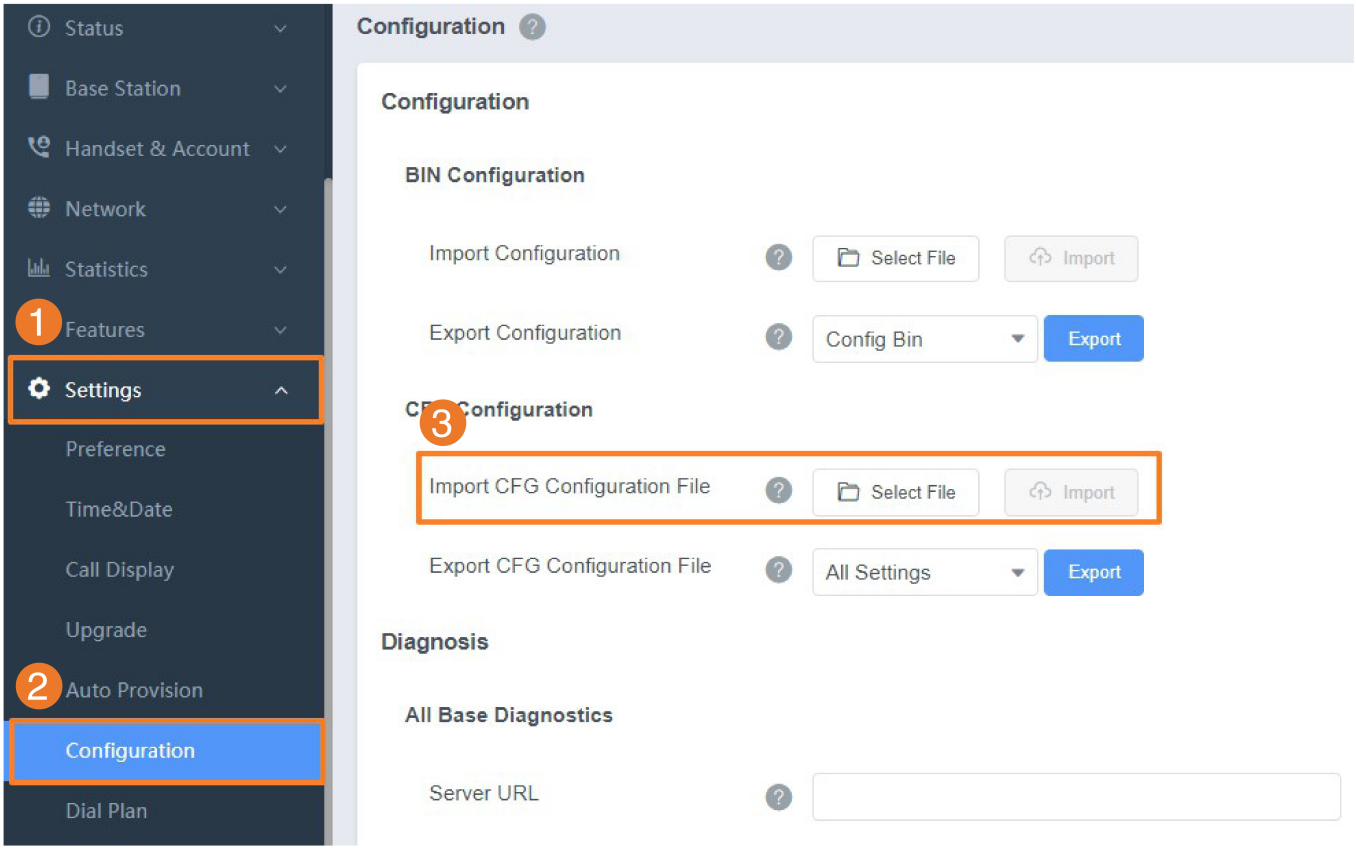


Import CFG Configuration Files to Phone

You can import the configuration files from 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	Permitted Values	Default	Description
static.custom_mac_cfg.url	URL within 511 characters	Blank	It configures the access URL of the custom MAC-Oriented CFG file.

Export BIN Files from the Phone

Procedure

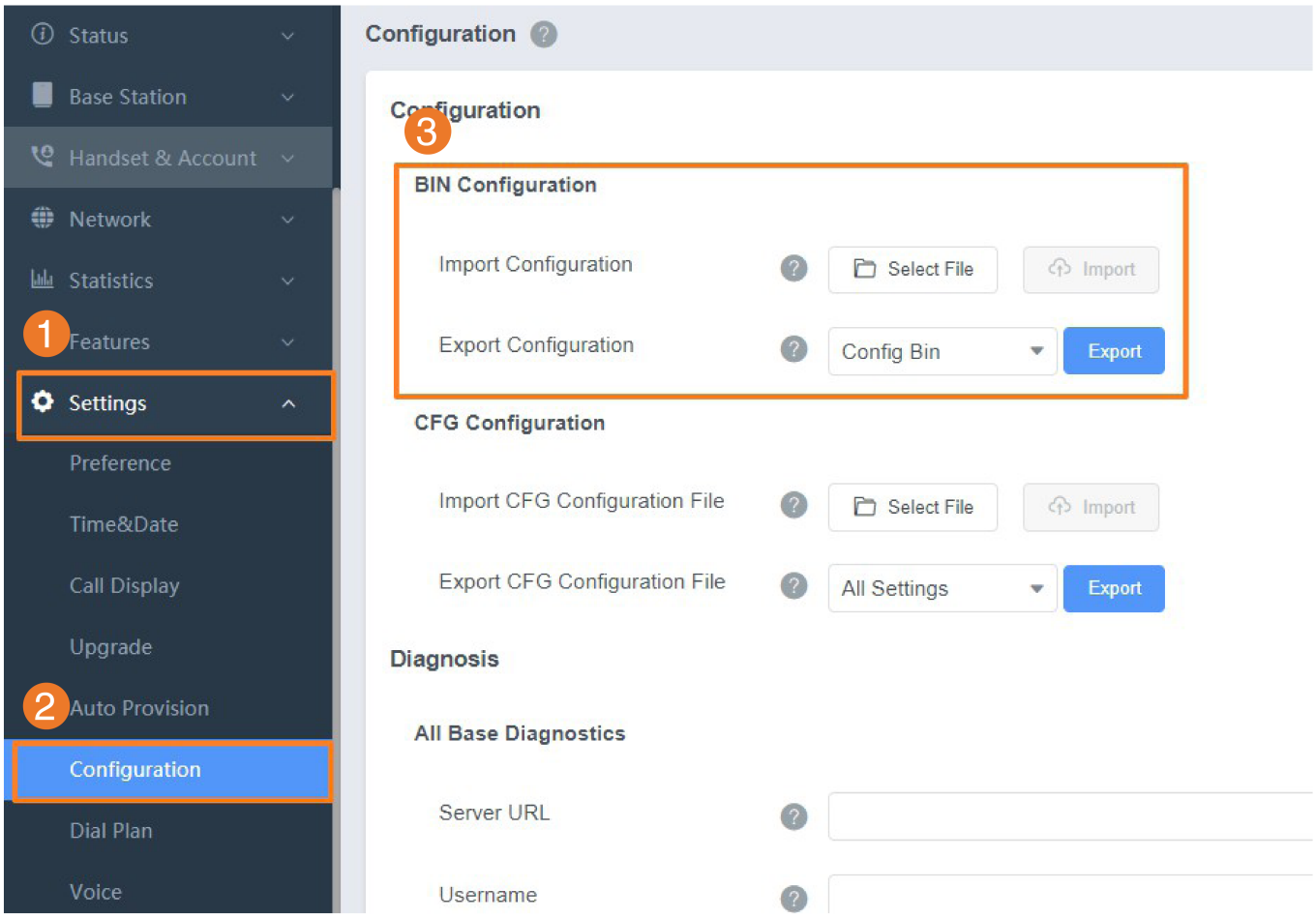
1. From the web user interface, click **Settings** > **Configuration** > **BIN Configuration**.
2. In the **Export Configuration** field, click **Export** to open the file download window, and then save the file to your local system.

Import BIN Files from the Phone

Procedure

1. From the web user interface, click **Settings** > **Configuration** > **BIN Configuration**.

2. In the **Import Configuration** field, click **Browse** to locate a BIN configuration file from your local system.
3. Click **Import** to import the configuration file.



BIN Files Import URL Configuration

static.configuration.url

Parameter	Permitted Values	Default	Description
static.configuration.url[1]	URL within 511 characters	Blank	It configures the access URL for the custom configuration files. The file format of the custom configuration file must be *.bin.

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

Export All the Diagnostic Files

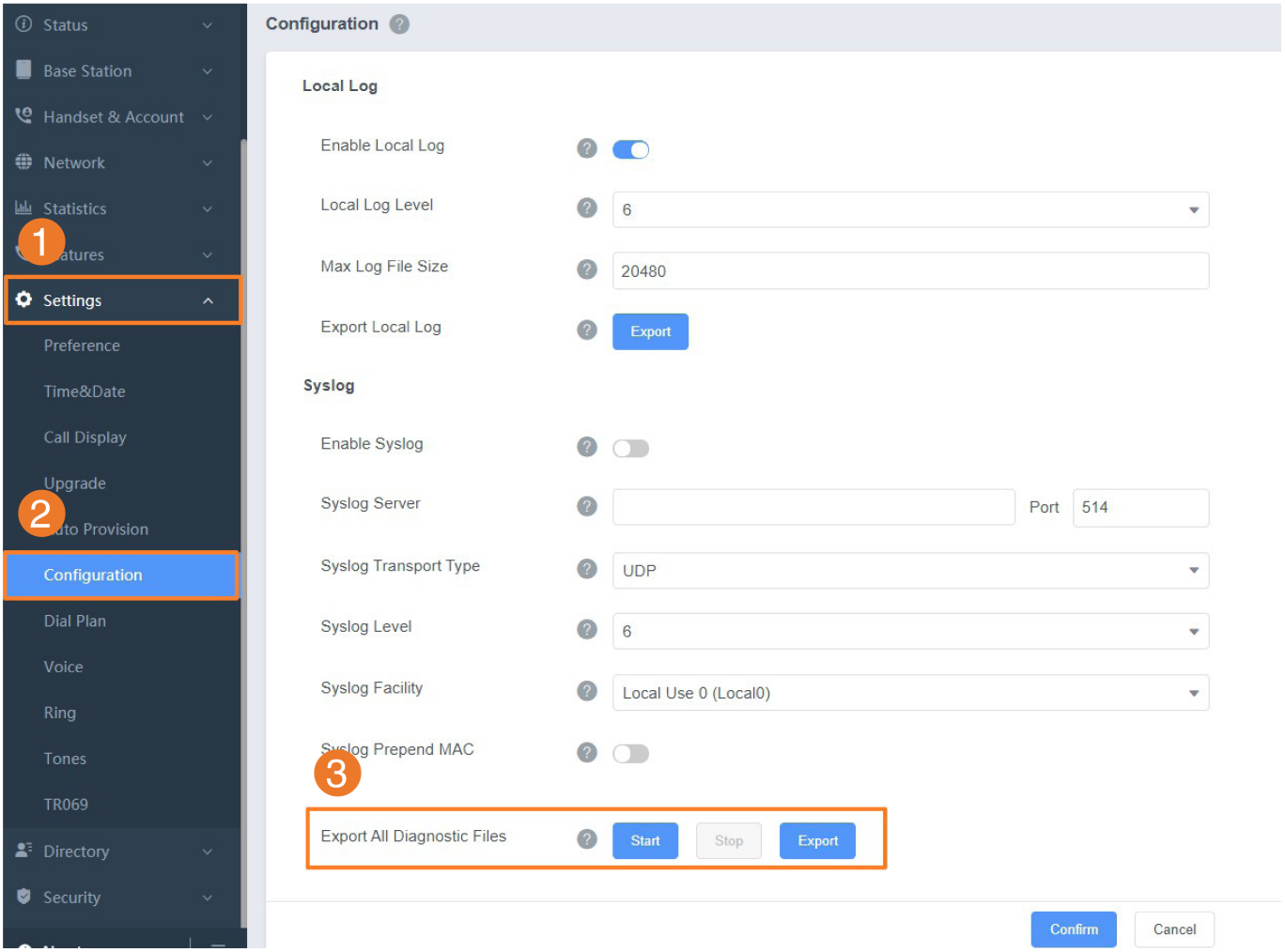
Introduction

Yealink phones support three types of diagnostic files (including Pcap trace, log files (boot.log and sys.log), and BIN configuration files) to help analyze your problem. You can export these files at a time and troubleshoot if necessary. The file format of the exported diagnostic file is *.tar.

Video Tutorial

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 the Yealink support team will help you locate the root cause.

Device Status

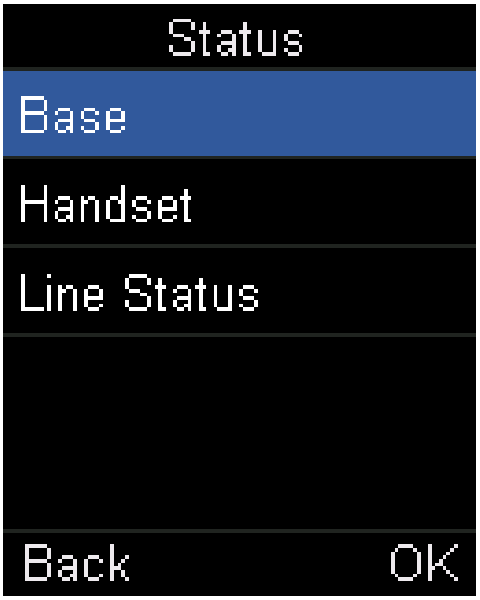
Introduction

Available information on device status includes:

- Base station status (IPv4 status or IPv6 status, firmware version, MAC address, machine ID and device certificate status, RFPI, and network information).
- Handset (or Phone) status (handset model, hardware version, firmware version, IPUI code, SN code, and area).
- Line status
- Power status (only applicable to CP930W-Base/CP935W-Base phones).

View Device Status

You can view device status via the handset user interface by going to **OK** > **Status**.



- For CP930W-Base phones, you can go to **Menu** > **Status**.
- For CP935W-Base phones, you can go to **More** > **Status**.

You can also view the device status via the web user interface.

Procedure

1. Open a web browser on your computer.
2. Enter the IP address in the browser's address bar, and then press **Enter**.
   For example, "http://192.168.0.10" for IPv4 or "http://[2005:1:1:1:215:65ff:fe64:6e0a]" for IPv6.
3. Enter the user name (admin) and password (admin) in the login page.
4. Click **Login** to log in.

The device status is displayed on the first page of the web user interface.

Phone Reboot

Introduction

You can reboot the phone remotely or locally.

Reboot the Phone Remotely

You can reboot the phones remotely using a SIP NOTIFY message with "Event: check-sync" header. Whether the IP phone reboots or not depends on "sip.notify_reboot_enable". If the value is set to 1, or the value is set to 0 and the header of the SIP NOTIFY message contains an additional string "reboot=true", the phone will reboot immediately.

The NOTIFY message is formed as shown:

```
NOTIFY sip:<user>@<dsthost> SIP/2.0
To: sip:<user>@<dsthost>
From: sip:sipsak@<srchost>
CSeq: 10 NOTIFY
Call-ID: 1234@<srchost>
Event: check-sync;reboot=true
```

Notify Reboot Configuration

```
sip.notify_reboot_enable
```

Parameter	Permitted Values	Default	Description
sip.notify_reboot_enable	**0**-The phone will reboot only if the SIP NOTIFY message contains an additional string "reboot=true". **1**-The phone will reboot. **2**-The phone will ignore the SIP NOTIFY message.	1	It configures the IP phone behavior when receiving a SIP NOTIFY message that contains the header "Event: check-sync".

Reboot the Device via the Handset User Interface

You can reboot your device via the handset user interface.

Procedure

1. Press **OK** > **Settings** > **System Settings** > **Base Restart** (default PIN: 0000).

- For CP930W-Base phones, go to **Menu** > **Advanced Settings** (default PIN:0000) > **Reboot Config** > **Base Reboot**.
- For CP935W-Base phones, go to **More** > **Advanced** (default PIN:0000) > **Reboot** > **Base Reboot**.

2. Tap **Reboot**.

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

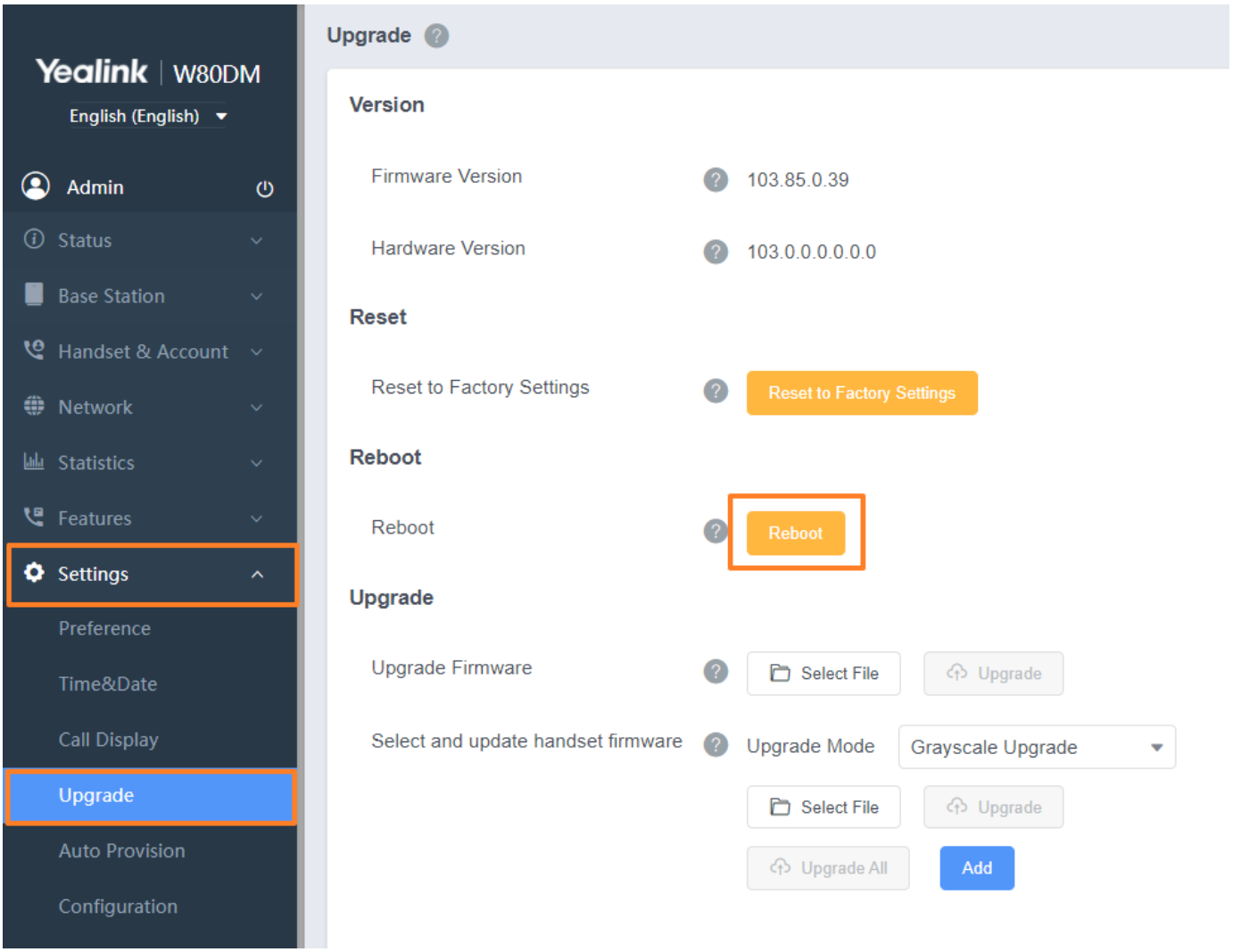
Reboot the Device via Web User Interface

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.



All Base Diagnostics

Introduction

You can export all DM and base diagnostic files (including Pcap trace, local log files, and BIN configuration files) at a time to help analyze the events that affect the DM and base stations.

Before You Begin

This feature is only applicable to the W75/W80/W90 Multi-Cell System.

Diagnostics File Type and Naming Rules

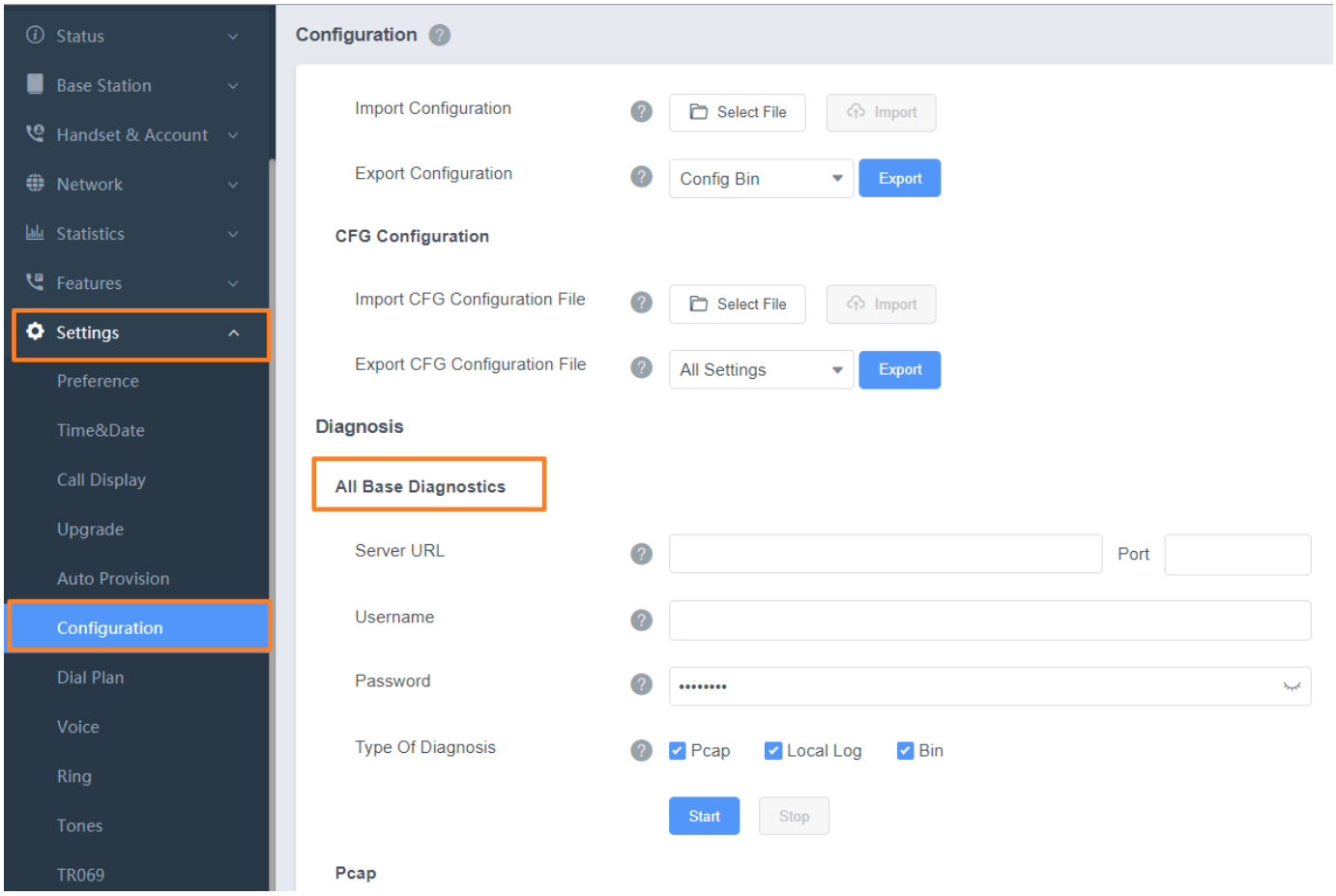
The following table displays the diagnostic file type and the naming rules:

Diagnostics File Type	Naming Rules
Pcap trace: saves the capture files of all bases (including DM).	1. DM: is named as DM_IP_STIME_TIME.xxx in W90 multi-cell system, INT_IP_STIME_DM Id_IP_TIME.xxx in VIM system. 2. Base: is named as "DM_IP_STIME_BASE_RPN_IP_TIME.xxx". Where .xxx refers to the suffix name of the file, such as .pcap, .log, or .bin. STIME indicates the time when you click Start on web user interface. TIME represents the time when the DM/Base uploads the files to the server. 3. Example: DM_10.81.6.81_20191205T093800Z_BASE_2_10.81.6.26_20191205T100458Z.pcap.
Local log: saves the log files of all bases (including DM).	
BIN file: saves the BIN files of all bases (including DM).	

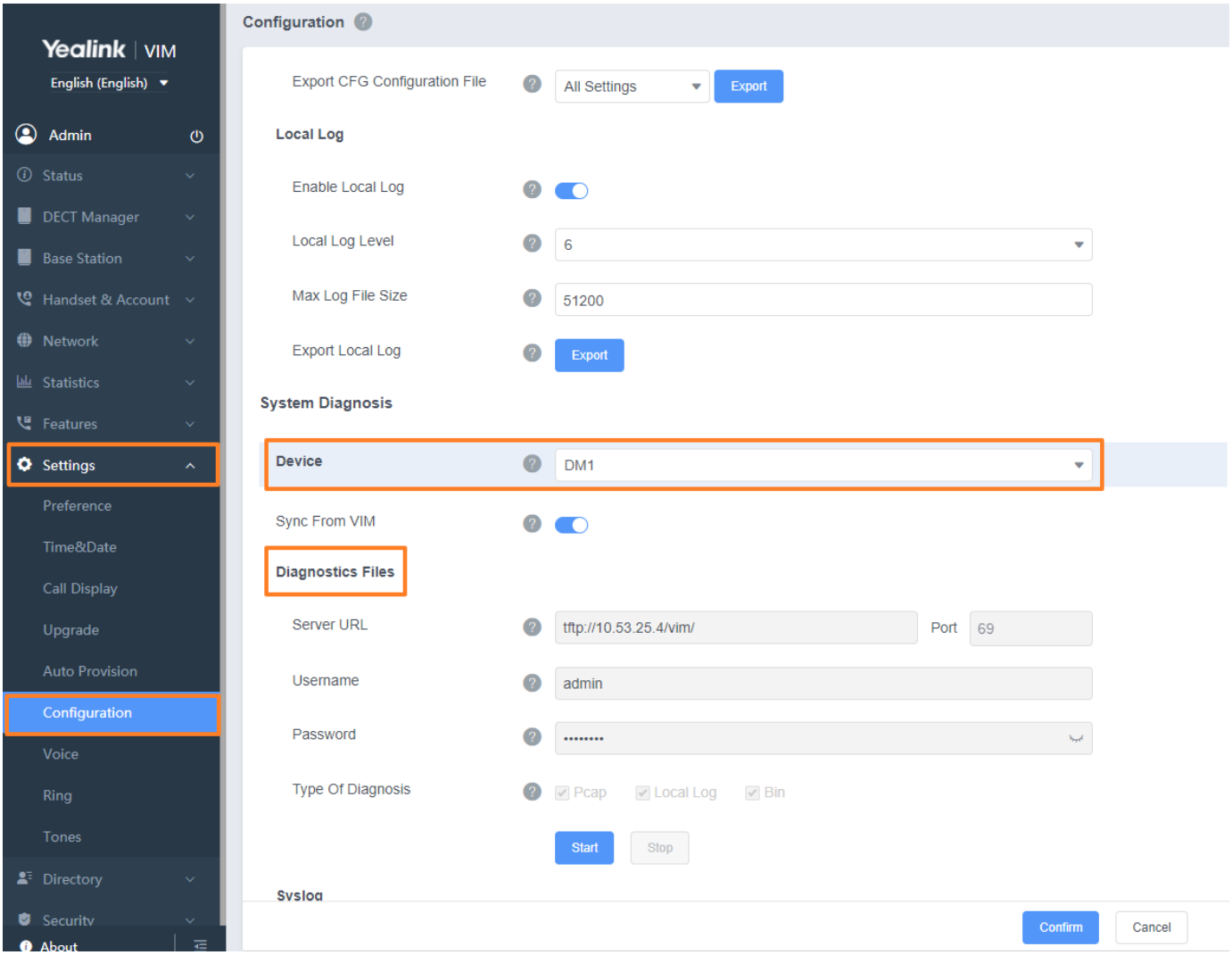
All Base Diagnostics Configuration

Set via the Web User Interface

1. On the web user interface of DM, go to **Settings** > **Configuration** > **All Base Diagnostics**.



2. On the web user interface, go to **Settings** >**Configuration** > **Device: VIM** > **Diagnostics Files**.



Configuration Parameter

static.diagnose.server.url
static.diagnose.server.port
static.diagnose.server.username
static.diagnose.server.password
static.diagnose.type
static.dm.X.diagnose.sync.enable
static.dm.X.diagnose.server.url
static.dm.X.diagnose.server.port
static.dm.X.diagnose.server.username
static.dm.X.diagnose.server.password
static.dm.X.diagnose.type
static.diagnose.pcap.max_size
static.diagnose.log.max_size

Parameter	Permitted Values	Default	Description
static.diagnose.server.url	String within 511 characters	Blank	It configures the server address of all DM/base diagnostic information uploads. The file uploading should be supported by the server, including http, https, tftp, ftp and ftps server. For example: http://10.82.24.8:69/upload/.
static.diagnose.server.port	Integer from 0 to 65535	Blank	It configures the server's port for all DM/base diagnostic information uploads.
static.diagnose.server.username	String within 64 characters	Blank	It configures the authentication username of the server that all DM/base diagnostic information uploads.
static.diagnose.server.password	String within 64 characters	Blank	It configures the authentication password of the server that all DM/base diagnostic information uploads.
static.diagnose.type	**1**-Pcap **2**-Local Log **3**-Bin Multiple types are separated by commas.	1,2,3	It configures the type of server which all DM/base diagnostic information uploads.
static.dm.X.diagnose.sync.enable[1]	**0**-Disabled **1**-Enabled	1	It enables and disables synchronizing VIM's all diagnosis and syslog configuration to DM.
static.dm.X.diagnose.server.url[1]	String within 511 characters	Blank	It configures the server address of base diagnostic information uploads for different DMs. The file uploading should be supported by the server, including http, https, tftp, ftp and ftps server.
static.dm.X.diag	Integer from 0	Bl	It specifies the port of the server to which the DM

nose.server.port[1]	to 65535	ank	uploads the base diagnostics information.
static.dm.X.diagnose.server.username[1]	String within 64 characters	Blank	It configures the authentication username of the server that bases diagnostic information uploads for different DMs.
static.dm.X.diagnose.server.password[1]	String within 64 characters	Blank	It configures the authentication password of the server that bases diagnostic information uploads for different DMs.
static.dm.X.diagnose.type[1]	**1**-Pcap **2**-Local Log **3**-Bin Multiple types are separated by commas. 1,2-Pcap,Local Log 1,3-Pcap,Bin 2,3-Local Log,Bin 1,2,3-Pcap,Local Log,Bin	1,2,3	It configures the type of server that bases diagnostic information uploads for different DMs.
static.diagnose.pcap.max_size	Integer from 1024 to 20480	5120	It configures the maximum size (KB) of each uploaded Pcap trace file. If it is set to 5120, the Pcap trace file will be uploaded to the server each time it reaches 5M.
static.diagnose.log.max_size	Integer from 1024 to 20480	4096	It configures the maximum size (KB) that one diagnosis process lasts. If it is set to 4096, the local log file will be uploaded to the server each time it reaches 4M.

[1]X is the registered DM id. X=1-10.

DECT Phone Problem Feedback Guidebook

Data Acquisition Instructions

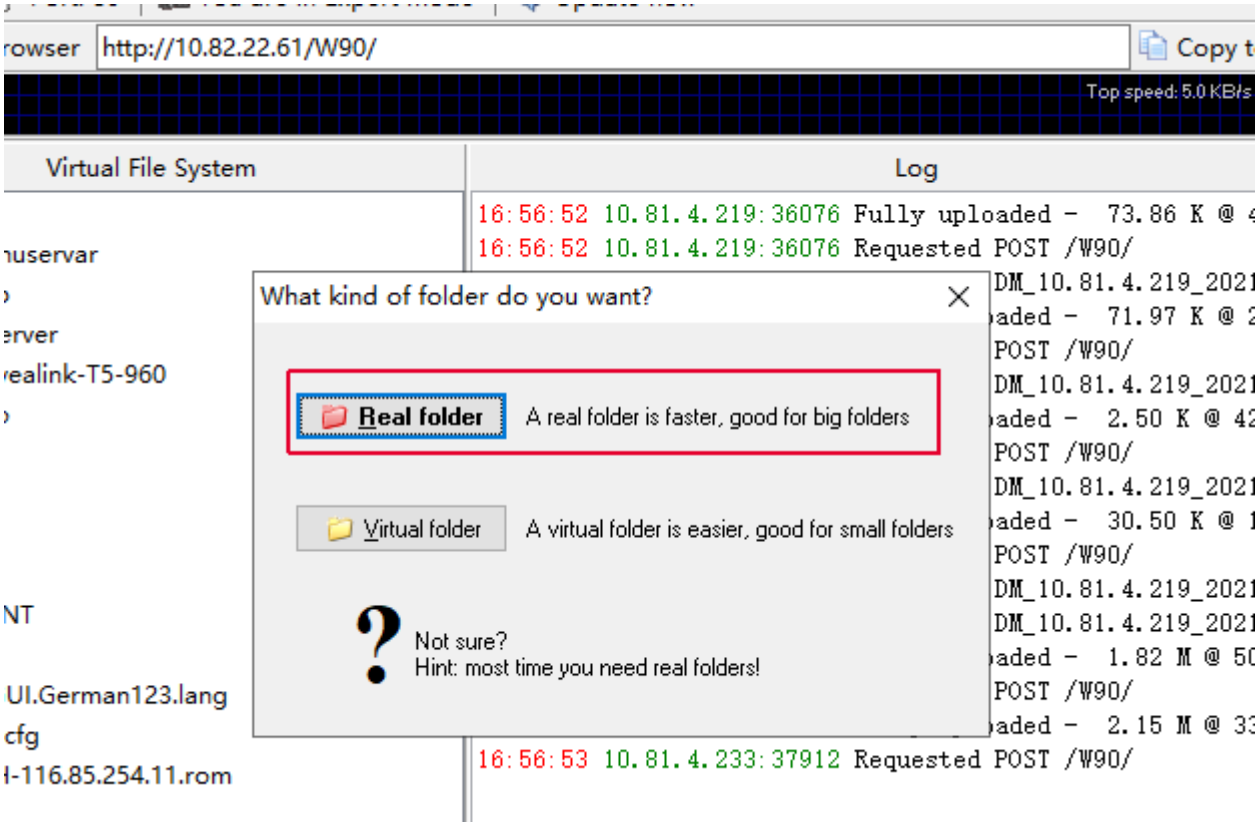
1. Rolling version: (W80: 103.83.0.104; W90: 130.85.0.29 or later) on the web user interface, go to **Settings** > **Configuration** > **All Base Diagnostics** and adjust all log levels to 6, and fill in the server and port where the log is saved (the Log server refers to HFS). After reproducing the problem, just compress and export the server log.
2. Description of when the exception occurred (Very Important).
3. Problem recurrence operation, phenomenon description (DM MAC, problem handset number), probability.
4. Performance of competing products (Optional)

Rolling Version Operating Instructions

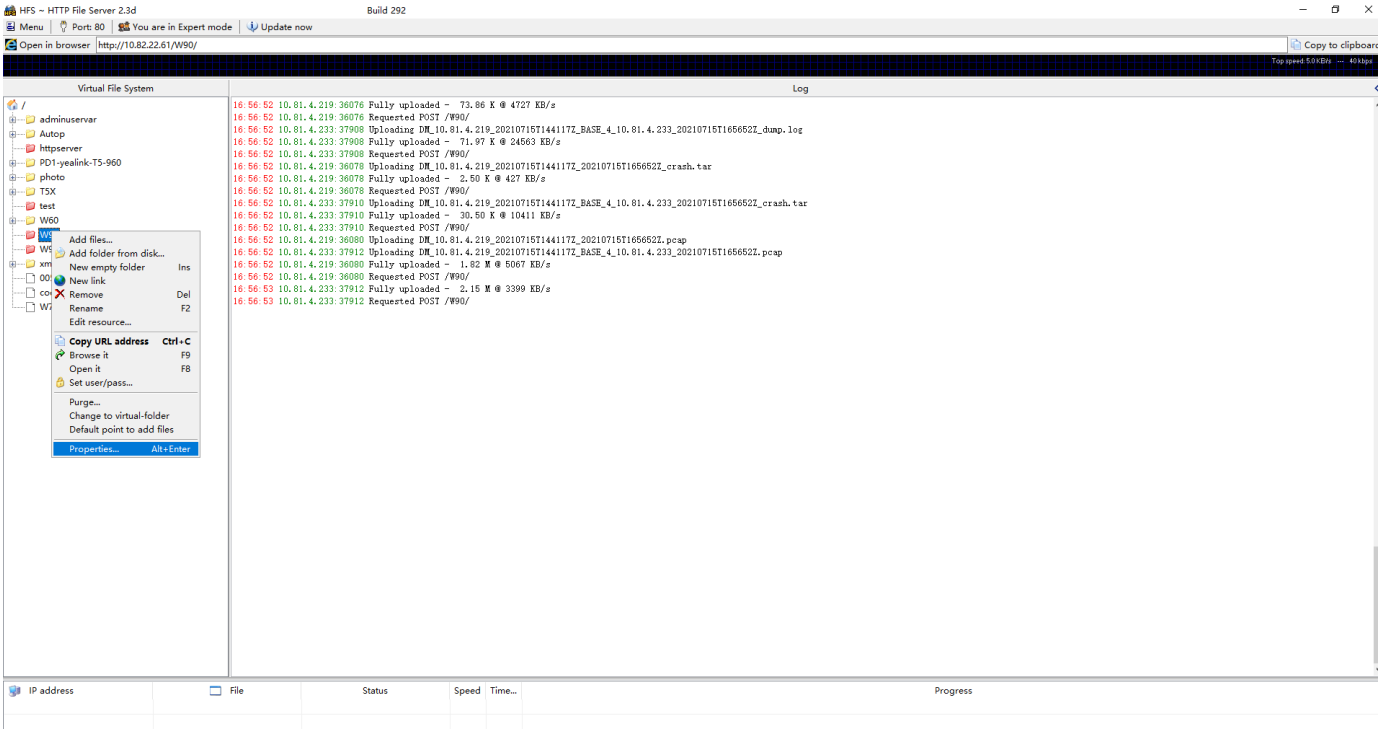
The log server should try to avoid using 3CD, because there are many logs and captured packets in the MC system; it is easy to lose the log when using 3CD, and use the HFS server to save the log of the MC system as much as possible.

The specific operation steps are as follows:

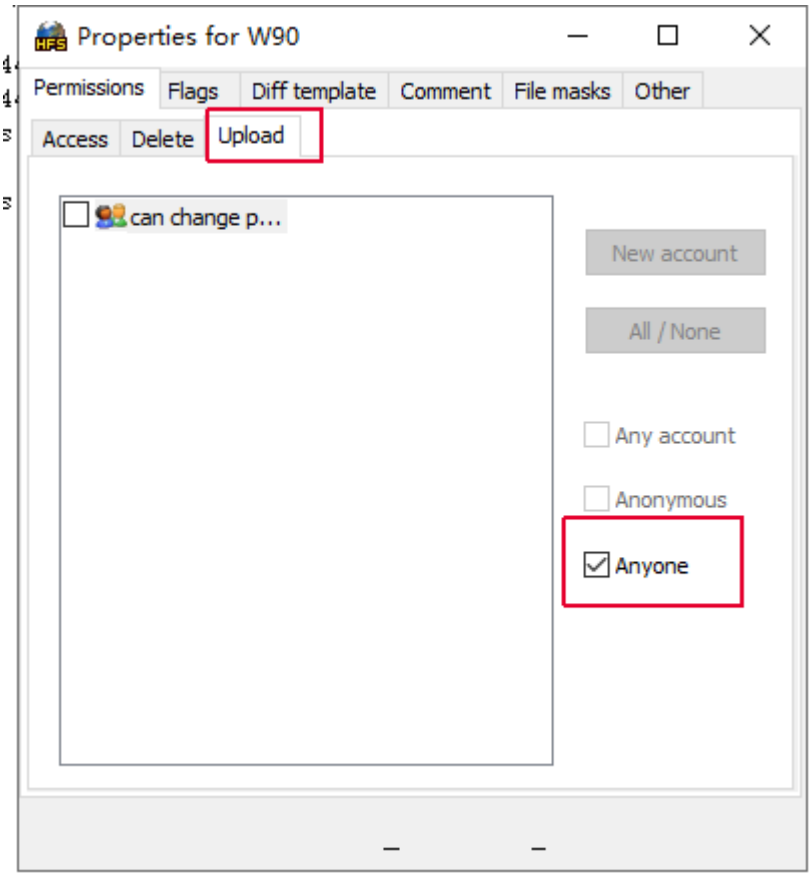
1. Create an empty folder locally (name it in English as much as possible)
2. Drag this folder to the HFS server, and select the folder format as a Real folder.



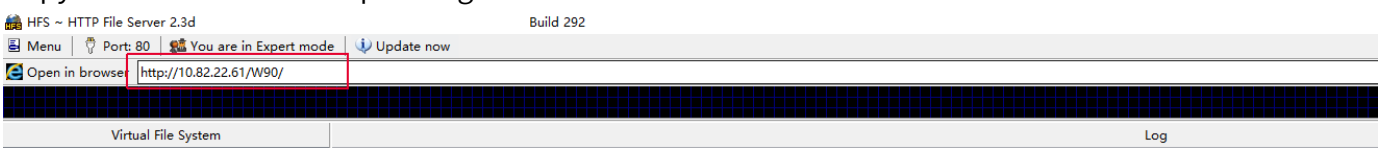
3. Right-click and select folder settings.



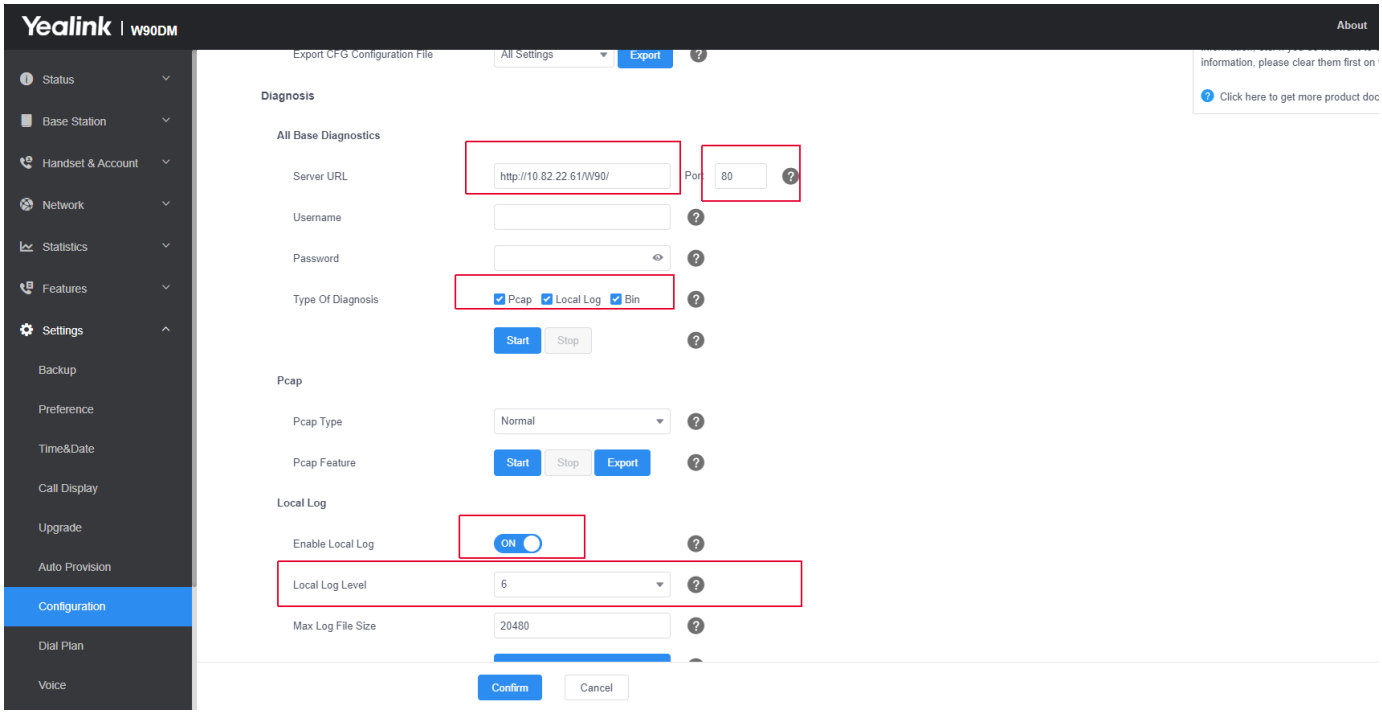
4. Go to **Upload** and select **Anyone**.



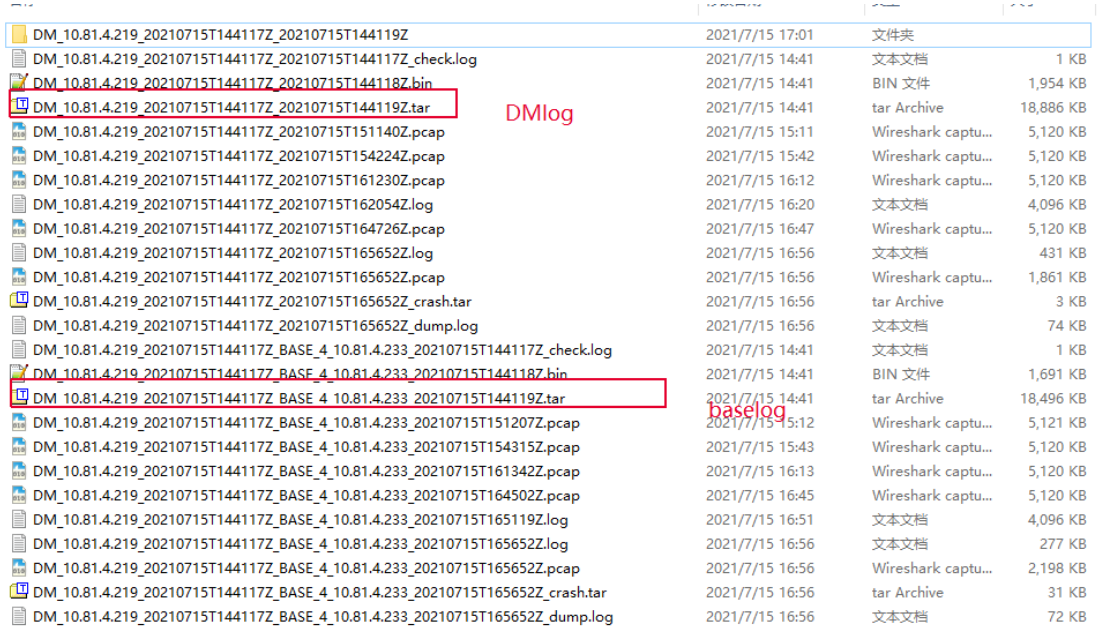
5. Copy the URL of the corresponding file.

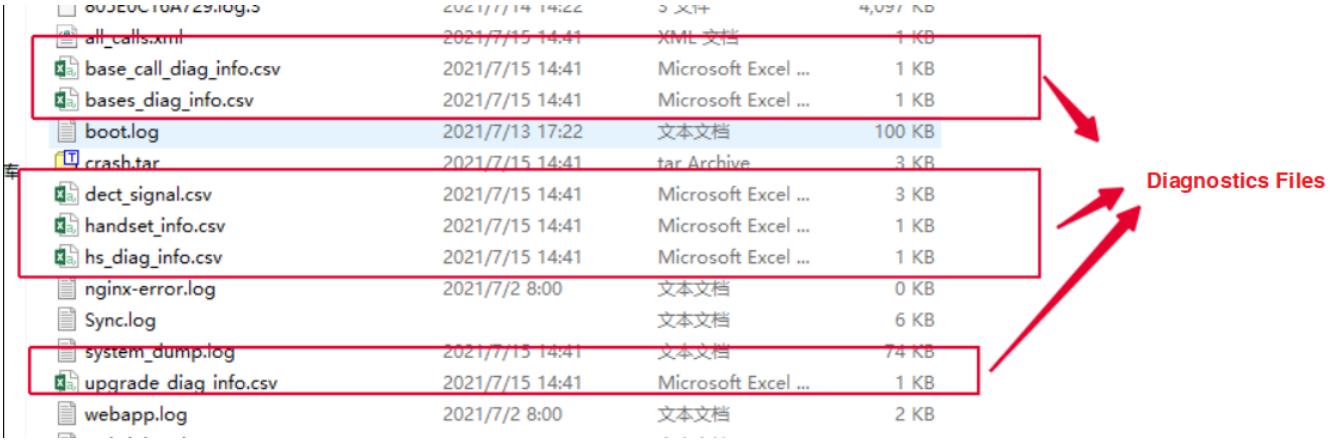


6. On the web user interface, go to **Settings** > **Configuration** > **All Base Diagnostics** and set the log level to 6, select the upload information including **Pcap**, **Local Log**, **Bin**, and fill in the **Server URL** and **Port** corresponding to HFS.



7. Click **Start** under **All Base Diagnostics** to reproduce the problem; click **Stop** after the reproduction is complete. The compressed folder will be provided back, which should contain the log, packet capture, and diagnostic files of DM and each base, and confirm whether there is a corresponding reproduction time point log.





Old Version Data Operating Instructions

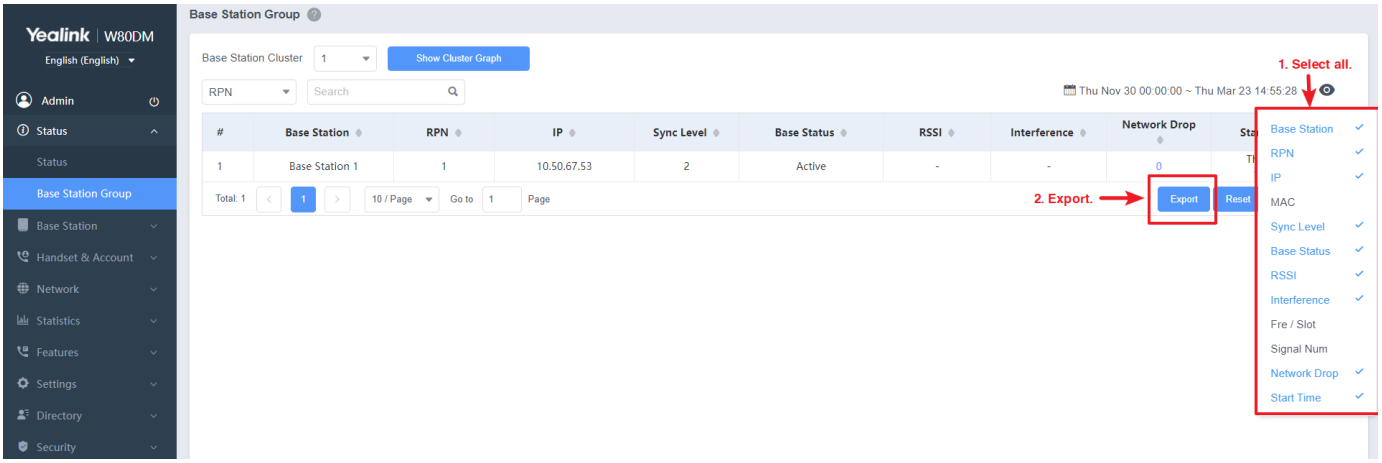
Generic Template

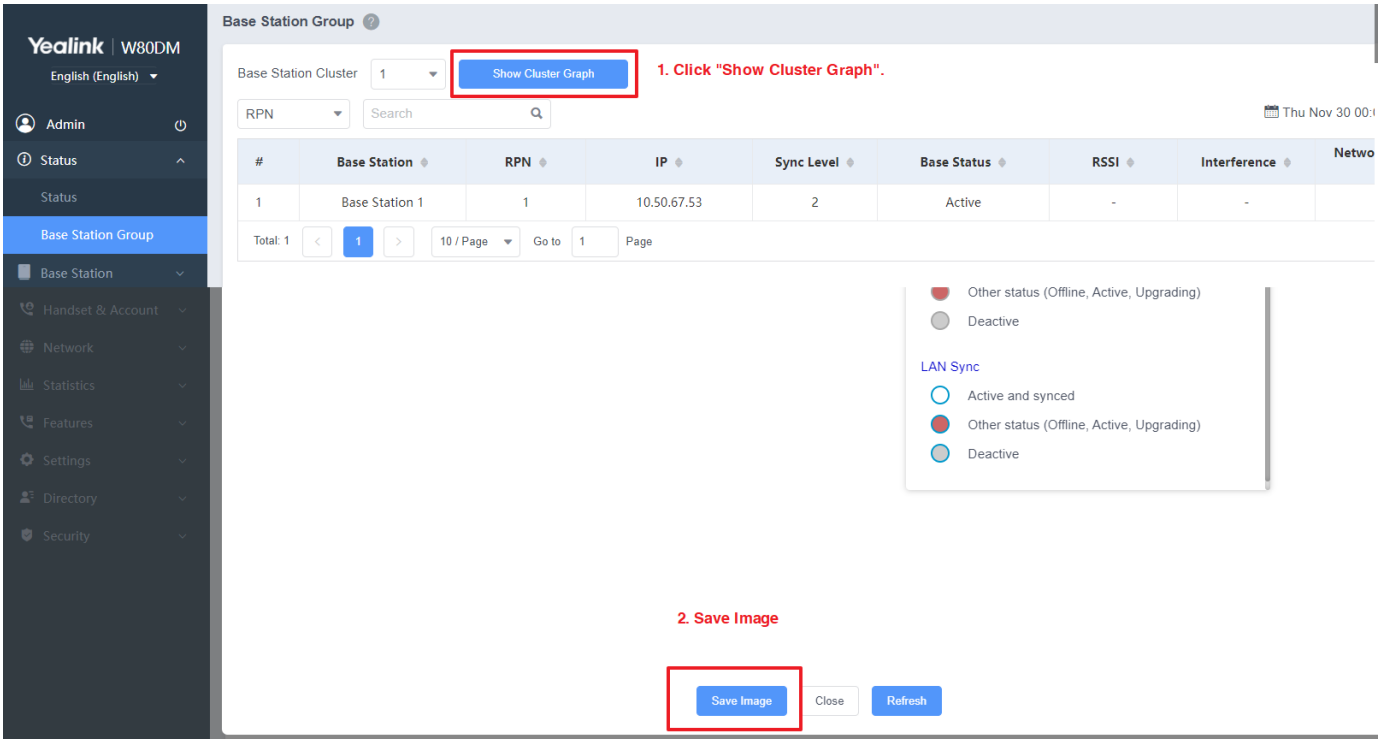
1. On the web user interface, go to **Settings** > **Configuration** > **All Base Diagnostics**, and click **Start** under **All Base Diagnostics** to reproduce the same problem as above, and export the data after the reproduction is complete.
2. Describe the point in time when the exception occurred (Very Important).
3. Problem recurrence operation, phenomenon description (DM IP, problem handset number), probability.
4. For comparison scenarios, please provide competing product information (Yealink products provide a three-piece set of information)

Deployment Issue Template

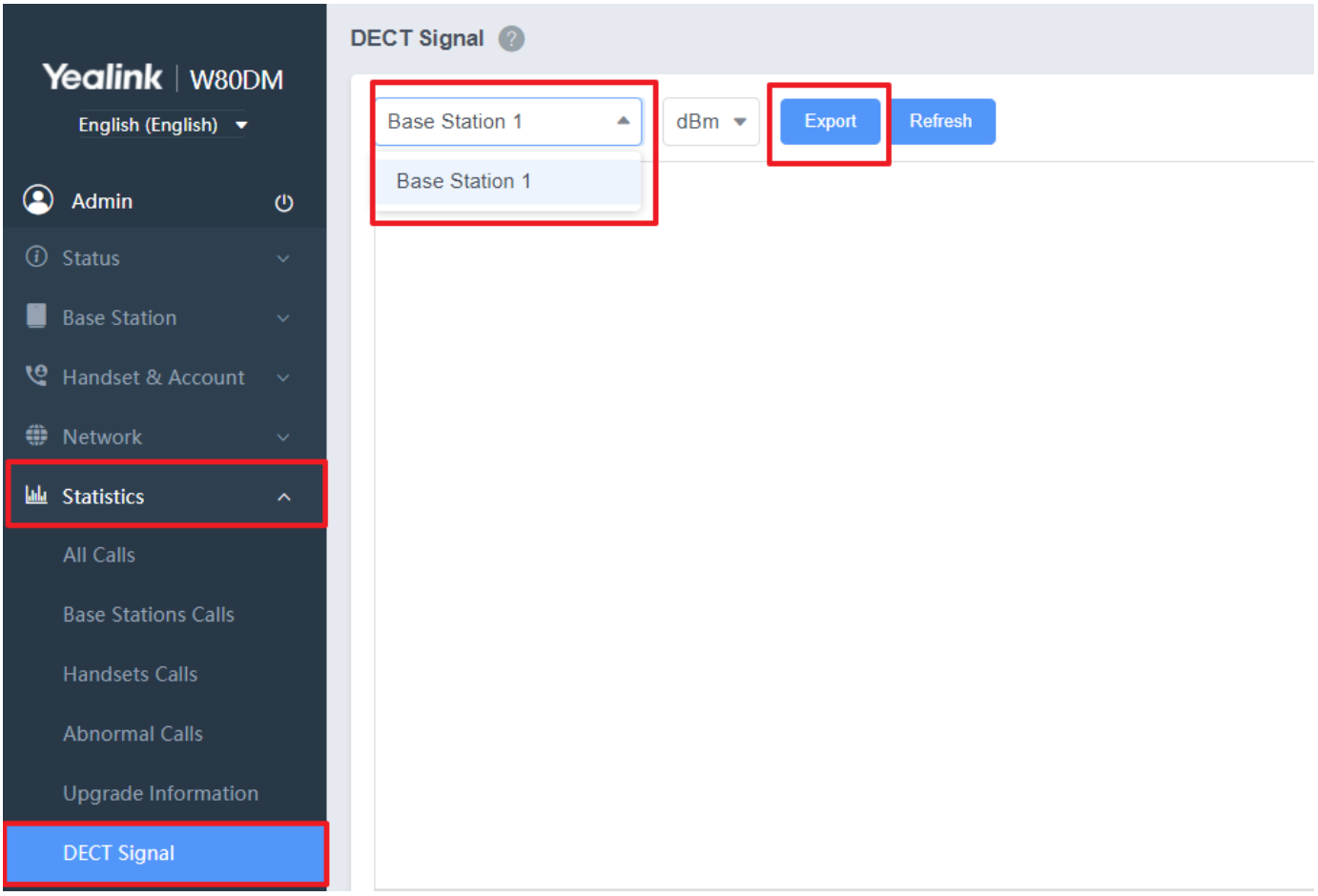
Deployment problems are mostly caused by unreasonable customer deployment. Deploying according to the instructions again can often solve the problem. If you still have questions, please provide information:

1. Generic Template..
2. Export data on the web user interface:
   - On the web user interface, go to **Status** > **Base Station Group**.





- On the web user interface, go to **Statistics** > **DECT Signal** > select the desired Base > **Export**. (The metering mode can determine which base the handset is currently registered in, and the Dect Signal of the base needs to ensure that it contains)



Sound Issue Template

1. Generic Template.

2. Probability occurs, need to provide:
   - Export data on the web user interface, the same as the operation of the Deployment Issue.
   - For the problem of abnormal sound (abnormal sound, noise), according to the DTMF and provide the operation time point during the reproduction process. The reproduction call should not be too short (keep 3 minutes).
   - If this issue must be present, provide a test account.

Signal Issue Template

1. Generic Template.
2. Enable the Metering Mode and check the dBm Code to eliminate environmental interference.
3. Provide video (take abnormal phenomena)
4. Deployment diagram (it is best to provide a floor plan)

Information required:

1. Base deployment by floor:

• Base location: Ceiling/Wall/Desktop

• Base Level relationship and distance between Bases

• Base environment: presence of metal doors, glass walls, solid walls, etc., in between

2. Nature of use of each floor: office area/storage area/kitchen, etc.

Handset Issue Template

1. Generic Template.
2. Check the dBm Code and turn on handset logs, reproduce the problem, and upload the handset logs (only if the handset is connected to Base properly).

Handset Blue Screen

When the handset shows a blue screen interface, please provide a picture of the blue screen interface or a video. You need to make sure the text on the screen is clear so that we can determine the cause of the problem. In the customer's environment, the handset's watchdog is on, and the handset stays on the blue screen for a very short time, which is not conducive to getting a picture of the interface.

Here are two ways to keep the handset on the blue screen.

1. Turn off the watchdog (watch_dog.enable=0) or go to the web user interface, **Preference** > **Watch Dog** (Enable->Disable).
2. **Method 1**:
3. (1) Power off the handset (press and hold the red hang-up button, release the button after the sound, and the handset is powered off).

4. (2) Press and hold the "#" button on the handset and put the handset into the charging cradle. Note that the handset can only be activated by pressing the "#" button, not any other button, including the red hang-up button.
5. (3) See the handset LCD display welcome after you can let go of the button, at this time the handset watchdog turns off, the blue screen will remain in the blue screen interface.

2. Turn off the watchdog (watch_dog.enable=0) or go to the web user interface, **Preference** > **Watch Dog** (Enable->Disable).
3. **Method 2**:
4. (1) Remove the battery from the handset.
5. (2) Press and hold the "#" button on the handset, put in the battery, and the handset will turn on automatically.
6. (3) See the handset LCD display welcome after you can let go of the button, at this time the handset watchdog turns off, the blue screen will remain in the blue screen interface.

Common Reasons for Invalid Information

1. Do not set the Log Level to 6.
2. After the problem has been reproduced, use one-click export of the web page. The one-click export of MC's log web page is often invalid. You need to export the log to the local folder and provide it back.
3. The problem reproduced halfway before you remembered to open the log and click **Start**.
4. Stop exporting immediately after the problem reappears, and there may be incomplete capture. It takes a little time for Multi-Cell to export logs to the PC. When the problem recurs, it is recommended to capture for a while (after a few minutes) before stopping the export, so as to ensure that the captured logs contain the complete process.