Yealink

Yealink W52P IP DECT Phones

Auto Provisioning Guide

Table of Contents

Summary of Changes

This section describes changes to this guide for each release and guide version.

Changes for Release 73, Guide Version 73.27

Major updates have occurred to the following sections:

- Customizing Resource Files on page 14
- Obtaining Provisioning Server Address on page 21
- SIP Notify Message on page 30
- Description of Configuration Parameters in CFG Files on page 69
- Time Zones on page 169

Changes for Release 73, Guide Version 73.25

Major updates have occurred to the following sections:

- Description of Configuration Parameters in CFG Files on page 69

Changes for Release 73, Guide Version 73.20

Major updates have occurred to the following sections:

- Encrypting Configuration Files on page 14
- Obtaining Provisioning Server Address on page 21

Changes for Release 73, Guide Version 73.11

Major updates have occurred to the following section:

- Description of Configuration Parameters in CFG Files on page 69

Changes for Release 73, Guide Version 73.10

The following sections are new for this edition:

- Managing MAC-local CFG File on page 12
- Configuring Wildcard of the Provisioning Server URL on page 25

Changes for Release 50, Guide Version 50.20

Changes for Release 40, Guide Version 40.15

Changes for Release 30, Guide Version 30.40

Changes for Release 30, Guide Version 30.30

Introduction

Yealink W52P is a SIP cordless phone system designed for small business and SOHO who are looking for immediate cost saving but scalable SIP-based mobile communications system. W52P IP DECT phones are full-featured devices that can be plugged directly into an IP network and can be used easily without manual configuration. The W52P IP DECT phone consists of one base station and one or more handsets (at most five handsets).

This guide provides instructions on how to provision Yealink W52P IP DECT phones with the minimum settings required. Yealink W52P IP DECT phones support FTP, TFTP, HTTP and HTTPS protocols for file downloading and uploading.

The purpose of this guide is to serve as a basic guidance for provisioning Yealink W52P IP DECT phones.

> The auto provisioning process outlined in this guide applies to Yealink W52P IP DECT phones running firmware version 73 (25.73.x.x for the base station and 26.73.x.x for the handset) or later. We recommend that do not downgrade the latest phone firmware to an earlier firmware version. The new firmware is compatible with old configuration parameters, but not vice versa.

Getting Started

This chapter provides instructions on how to get ready for auto provisioning. The auto provisioning process discussed in this guide uses the TFTP server as the provisioning server.

To begin the auto provisioning process, the following steps are required:

- Configuring a Provisioning Server

- Obtaining Configuration Files

- Managing Configuration Files

- Customizing Resource Files

Configuring a Provisioning Server

Yealink W52P IP DECT phones support using FTP, TFTP, HTTP and HTTPS protocols to download configuration files. You can use any one of these protocols for provisioning. The following section provides instructions on how to configure a TFTP server.

For more information on configuring an FTP server or an HTTP server, refer to Configuring an FTP Server on page 54 and Configuring an HTTP Server on page 58.

Configuring a TFTP Server

We recommend that you use the 3CDaemon or TFTPD32 application as a TFTP server. 3CDaemon and TFTPD32 are free applications for Windows platform. You can download the 3CDaemon application online: http://www.oldversion.com/3Com-Daemon.html and TFTPD32 application online: http://tftpd32.jounin.net/.

The following introduction takes the 3CDaemon application as an example.

To create a root directory:

1. Create a TFTP root directory on the local system.

2. Configure the security permissions for the TFTP root directory.

You need to define a user or a group name, and set the permissions: read, write, and modify. Security permissions vary by organizations.
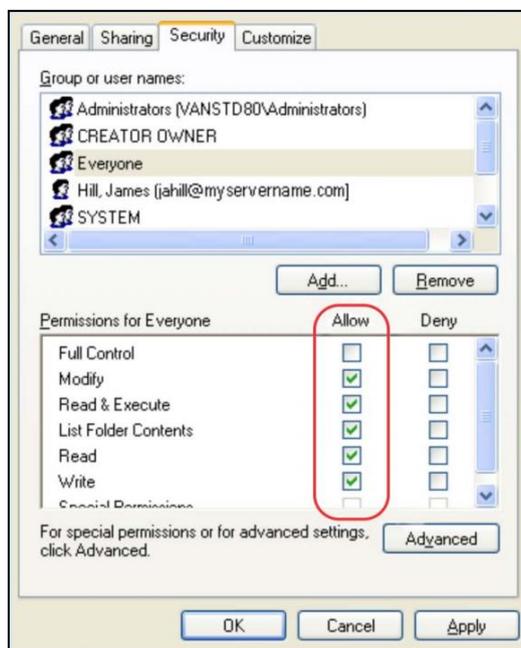
To configure a TFTP server:

1. Double click the 3CDaemon.exe to run the application.

2. Select **Configure TFTP Server**.
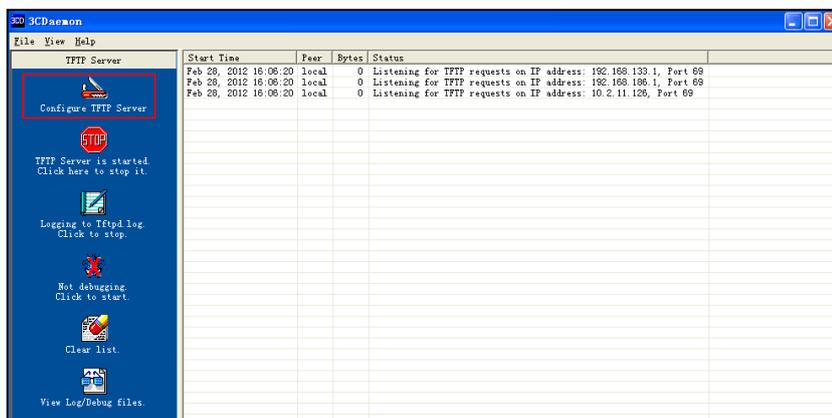
3. Click ▣ to locate the TFTP root directory you have configured from the local system.
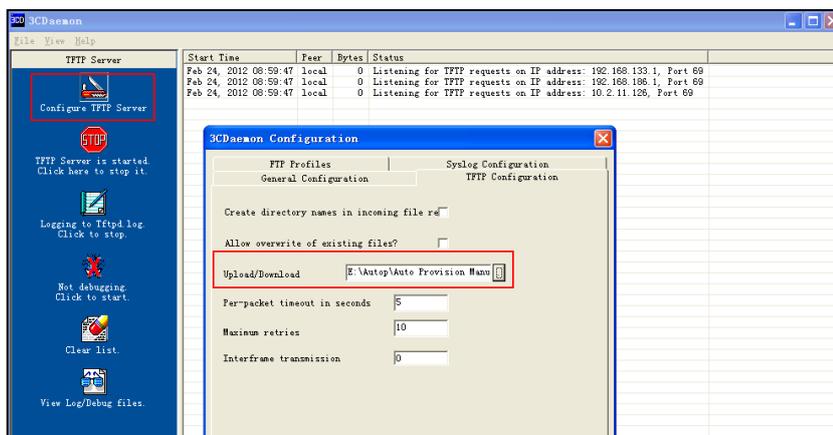
4. Click **Confirm** to finish configuring the TFTP server.

The server URL "tftp://IP address of provisioning server/" (e.g., tftp://192.168.1.100/) is where the IP phone downloads configuration files from.

Obtaining Configuration Files

Before auto provisioning, you need to obtain configuration files. There are 2 configuration files both of which are CFG-formatted. We call these two files Common CFG file and MAC-Oriented CFG file. IP phones try to download these two configuration files from the provisioning server during auto provisioning.

IP phones with firmware version 73 or later also support a local configuration file named as <MAC>-local.cfg. When a user modifies configurations of the base station via the handset or web user interface, the configurations will be automatically saved to the <MAC>-local.cfg file on the IP phone.

The <MAC>-local.cfg file only saves configurations of the base station configured via the handset or web user interface. Configurations of the handset cannot be saved to the <MAC>-local.cfg file.

The <MAC>.cfg and <MAC>-local.cfg files are only effectual for the specific phone. They use the 12-digit MAC address of the phone as the file name. For example, if the MAC address of the phone is 0015651130F9, the <MAC>.cfg and <MAC>-local.cfg files have to be named as 0015651130F9.cfg and 0015651130F9-local.cfg respectively. However, the Common CFG file is effectual for all phones of the same phone model. The Common CFG file of the W52P IP DECT phone uses the fixed name "y000000000025.cfg".

You can export/import the <MAC>-local.cfg file via web user interface. For more information on how to export/import a local configuration file, refer to Scenario D Importing or exporting the local configuration file on page 48.

You can ask the distributor or Yealink FAE for the y000000000025.cfg and <MAC>.cfg

files. You can also obtain the y000000000025.cfg and <MAC>.cfg files online:

http://www.yealink.com/SupportDownloadfiles_detail.aspx?CateId=308&flag=142

To download y000000000025.cfg and <MAC>.cfg files:

1. Go to the Document Download page of Yealink website.

2. Click the phone model "W52P" under the **Documents and Download** tab.

3. Download the latest auto provisioning template package to your local system. For example, the following illustration shows the available template packages for W52P IP DECT phones with different firmware versions.
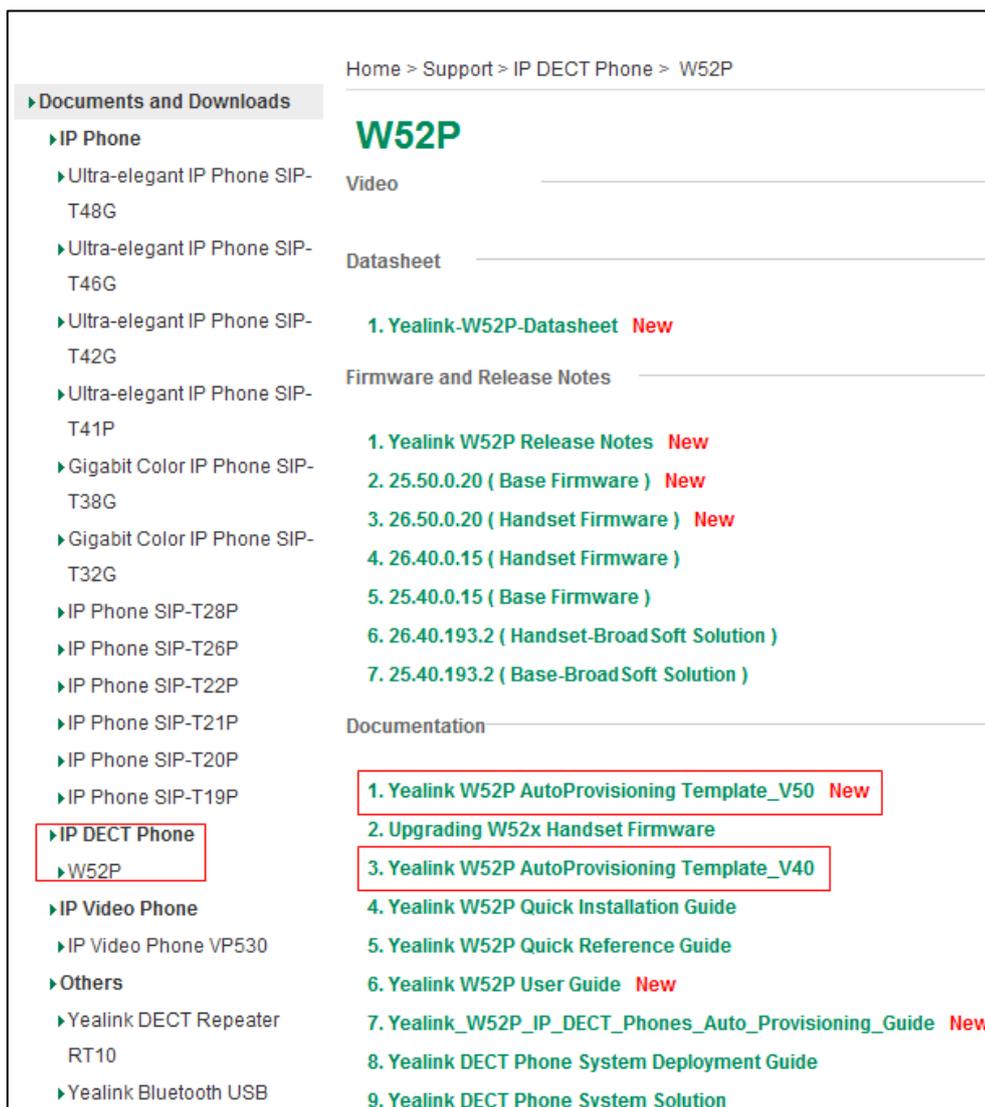
4. Uncompress the downloaded template package.

5. Open the folder you uncompressed the package to and identify the files you will edit.

> As of firmware version 73, the default value is no longer configured for each parameter in the template configuration files.

Obtaining Phone Information

Before auto provisioning, you also need the phone information. For example, MAC address of the phone and the SIP account information.

MAC Address: The unique 12-digit serial number of the phone. You can obtain it from the bar code on the back of the base station.

SIP Account Information: This may include SIP credentials such as user name, password and the address of the registration server. Ask your system administrator for SIP account information.

Managing Configuration Files

Auto provisioning enables W52P IP DECT phones to update themselves automatically via downloading the y000000000025.cfg and <MAC>.cfg files. Before auto provisioning, you may need to edit and customize your configuration files. IP phones can only recognize configuration files using UTF-8 or ANSI encoding. Open the configuration file using a text editor (e.g., UltraEdit). For more information on configuration parameters in configuration files, refer to Description of Configuration Parameters in CFG Files on page 69.

When editing the configuration files, learn the following:

- The extension ".cfg" of the configuration file name must be in lowercase.

- Each line in the configuration files must use the following format and adhere to the following rules:

```
variable-name = value
```

  - Associate only one value with one variable.

  - Separate variable name and value with an equal sign.

  - Set only one variable per line.

  - Put the variable and value on the same line, and do not break the line.

  - Comment the variable on a separated line. Use the pound (#) delimiter to distinguish the comments.

- The file header "#!version:1.0.0.1" in the configuration files is not a comment and Can Not be edited or deleted.

Editing the Common CFG File

Common CFG file (y000000000025.cfg) contains configuration parameters that are applied to IP phones of the same phone model, such as language, time and date.

The following figure shows a portion of the Common CFG file:

```
Common.cfg ×
    0         10        20        30        40        50        60        70        80        90
 1 #!version:1.0.0.1
 2
 3 ##File header "#!version:1.0.0.1" can not be edited or deleted.##
 4
 5 ###########################################################################################
 6 ##                                   Network                                          ##
 7 ###########################################################################################
 8
 9
10 #Configure the username and password for PPPOE connection.
11 #Require reboot;
12 network.pppoe.user =
13 network.pppoe.password =
14
15 #Enable or disable the VLAN of WAN port; 0-Disabled(default), 1-Enabled;
16 #Require reboot;
17 network.vlan.internet_port_enable =
18
19 #Configure the VLAN ID, it ranges from 1 to 4094, the default value is 1.
20 #Require reboot;
21 network.vlan.internet_port_vid =
22
23 #Configure the VLAN priority, it ranges from 0 (default) to 7.
24 #Require reboot;
25 network.vlan.internet_port_priority =
26
27 #Configure the HTTP port (80 by default) and the HTTPS port (443 by default) of the web server.
28 #Require reboot;
29 network.port.http =
30 network.port.https =
31
32 #Configure the maximum local RTP port. It ranges from 0 to 65535, the default value is 12780.
33 #Require reboot;
34 network.port.max_rtpport =
```

> The line beginning with "#" is considered to be a comment.
>
> The file header "#!version:1.0.0.1" is not a comment and must be placed in the first line. It cannot be edited or deleted.

To edit the Common CFG file:

1. Use an ASCII editor to open the file.

2. Edit the parameters in the file.

3. Save the change.

4. Rename the file to be "y000000000025.cfg".

5. Store the file to the root directory of the TFTP server.

The following lists the commonly edited parameters in the Common CFG file:

```
#################################################
##                 Common CFG File             ##
#################################################
#!version:1.0.0.1
##File header "#!version:1.0.0.1" cannot be edited or deleted.
```

#Configure the user name and password for PPPoE connection.
#Require a reboot;

network.pppoe.user =
network.pppoe.password =

#Configure the HTTP port (80 by default) of the web server. It ranges from 1 to 65535.
#Require a reboot.

network.port.http =

#Configure the HTTPS port (443 by default) of the web server. It ranges from 1 to 65535.
#Require a reboot.

network.port.https =

#Configure the URL of the auto provisioning server.

auto_provision.server.url =

#Configure the user name and password for downloading.

auto_provision.server.username =
auto_provision.server.password =

#Configure the AES key (16 characters) for decrypting the y000000000025.cfg file.

auto_provision.aes_key_16.com =

#Configure the AES key (16 characters) for decrypting the <MAC>.cfg file.

auto_provision.aes_key_16.mac =

#Configure the PIN code of the base station.

base.pin_code=

#Enable or disable call waiting feature; 0-Disabled, 1-Enabled (default);

call_waiting.enable =

#Enable or disable the playing of call waiting tone; 0-Disabled, 1-Enabled (default);

call_waiting.tone =

#Configure the area code.

dialplan.area_code.code =
dialplan.area_code.min_len =
dialplan.area_code.max_len =
dialplan.area_code.line_id =

Editing the MAC-Oriented CFG File

MAC-Oriented CFG file contains configuration parameters that are expected to be updated per phone, such as the account registration information.

The following figure shows a portion of the MAC-Oriented CFG file:
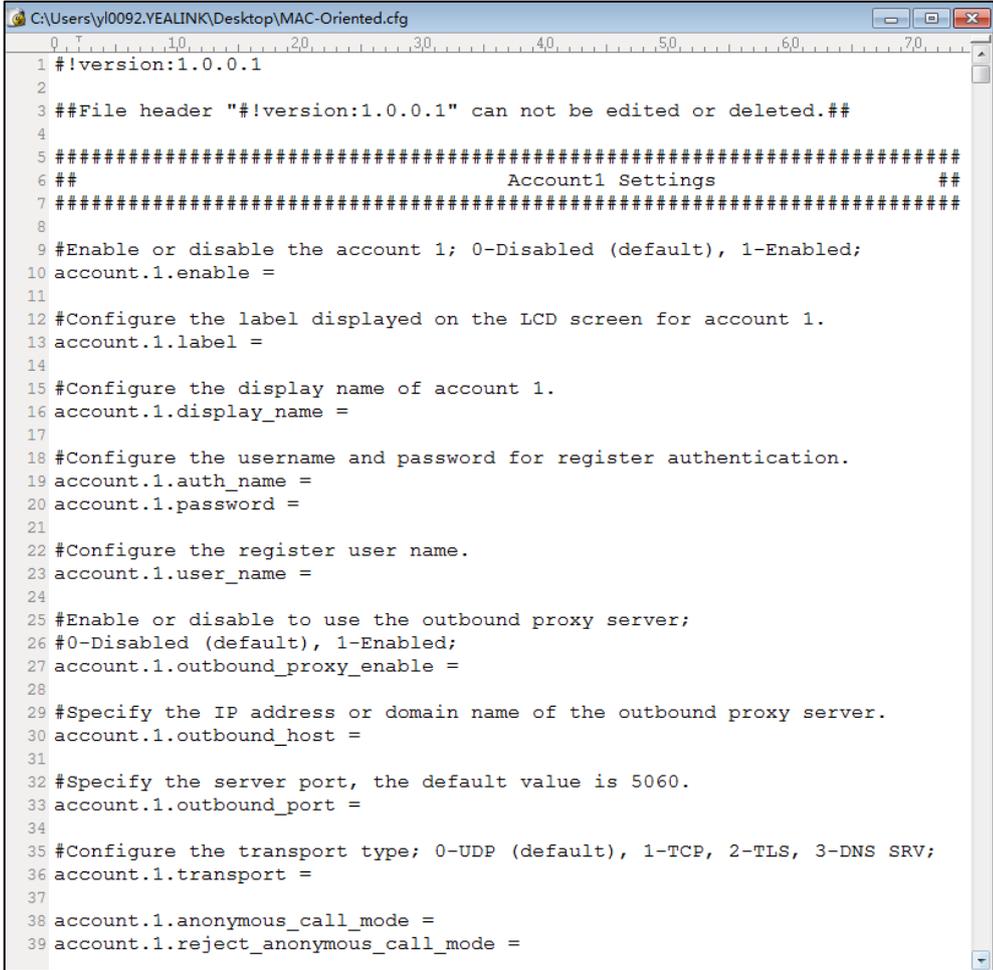
To edit the MAC-Oriented CFG file:

1. Use an ASCII editor to open the file.

2. Edit the parameters in the file.

3. Save the change.

4. Rename the file with the MAC address of the phone, such as "0015653828DA.cfg".

5. Store the file to the root directory of the TFTP server.

The following lists the commonly edited parameters of account1 and network in the MAC-Oriented CFG file:

```
###################################################
##              MAC-Oriented CFG File              ##
###################################################
```

#!version:1.0.0.1
##File header "#!version:1.0.0.1" cannot be edited or deleted.##

#Account 1 Settings
#Enable or disable the account1; 0-Disabled (default), 1-Enabled;

account.1.enable =

#Configure the label of account1 which will be displayed on the LCD screen.

account.1.label =

#Configure the display name of account1.

account.1.display_name =

#Configure the user name and password for register authentication.

account.1.auth_name =
account.1.password =

#Configure the register user name.

account.1.user_name =

#Configure the outbound SIP server address and port (5060 by default).

account.1.outbound_proxy_enable =
account.1.outbound_host =

#Configure the transport type for the SIP server; 0-UDP (default), 1-TCP, 2-TLS;

account.1.transport =

#Configure DND feature on account1.

account.1.dnd.enable =
account.1.dnd.on_code =
account.1.dnd.off_code =

#Configure always forward feature on account1.

account.1.always_fwd.enable =
account.1.always_fwd.target =
account.1.always_fwd.on_code =
account.1.always_fwd.off_code =

#Configure the WAN port type.
#Require a reboot.

network.internet_port.type =

#Configure the network settings of the base station.

network.internet_port.ip =

network.internet_port.mask =

network.internet_port.gateway =

network.primary_dns=

network.secondary_dns =

Managing MAC-local CFG File

<MAC>-local.cfg file is automatically filled with settings of the base station modified via the handset or web user interface, and is stored on the base station. If your base station is running firmware version prior to 25.73.0.1, the base station will automatically generate a <MAC>-local.cfg file after it is upgraded to the latest firmware.

Uploading and downloading the <MAC>-local.cfg file

You can configure whether the IP phone periodically uploads the <MAC>-local.cfg file to the provisioning server to back up this file, and downloads the <MAC>-local.cfg file from the provisioning server during auto provisioning to override the one stored on the phone. This process is controlled by the value of the parameter "auto_provision.custom.sync". When the value of the parameter "auto_provision.custom.sync" is set to 1, the IP phone will periodically upload the <MAC>-local.cfg file to the provisioning server, and download the <MAC>-local.cfg file from the provisioning server during auto provisioning.

For more information on how to configure this parameter, refer to Configuration Parameters on page 38.

Updating 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 "auto_provision.custom.protect". When the value of the parameter "auto_provision.custom.protect" is set to 1, the IP phone will update the configurations in the <MAC>-local.cfg file during auto provisioning. The configurations in the <MAC>-local.cfg file take precedence over the ones in the downloaded y000000000025.cfg /<MAC>.cfg file. As a result, the personalized settings of the base station configured via the handset or web user interface can be remained after auto provisioning.

For more information on how to configure this parameter, refer to Configuration

Note: The following configurations are defined never to be saved to the <MAC>-local.cfg file, even if users modify these configurations via the handset or web user interface.

- Configurations associated with the password.

  For example,

  #Configure the password for PPPoE connection.

  network.pppoe.password =

  For more information on the specific configurations which associated with the password, refer to Description of Configuration Parameters in CFG Files on page 69.

- Configurations requiring a reboot during auto provisioning.

  For example,

  # Enable or disable the VLAN of WAN port.

  network.vlan.internet_port_enable =

  For more information on the specific configurations which require a reboot during auto provisioning, refer to Description of Configuration Parameters in CFG Files on page 69.

- The following configuration parameters.

  #Configure always forward feature for account X.

  account.X.always_fwd.enable =

  account.X.always_fwd.target =

  account.X.always_fwd.on_code =

  account.X.always_fwd.off_code =

  #Configure busy forward feature for account X.

  account.X.busy_fwd.enable =

  account.X.busy_fwd.target =

  account.X.busy_fwd.on_code =

  account.X.busy_fwd.off_code =

  #Configure no answer forward feature for account X.

  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 =

  #Configure DND feature for account X.

  account.X.dnd.enable =

account.X.dnd.on_code =

account.X.dnd.off_code =

#Configure the access URL of the firmware file.

firmware.url =

#Configure the access URL of configuration files.

auto_provision.server.url=

Encrypting Configuration Files

To protect against unauthorized access and tampering of sensitive information (e.g., login passwords, registration information), you can encrypt the configuration files using the Yealink Configuration Encryption Tool. AES keys must be 16 characters and the supported characters are: 0 ~ 9, A ~ Z, a ~ z and the special characters # $ % * +, - . : = ? @ [ ] ^ _ { } ~. For more information on how to encrypt the configuration files, refer to *Yealink Configuration Encryption Tool User Guide*.

Customizing Resource Files

When configuring some particular features, you may need to upload resource files to IP phones. Yealink provides some resource file templates for the particular features. Ask the Yealink FAE or the distributor for the resource file templates or download them online:

http://www.yealink.com/SupportDownloadfiles_detail.aspx?CateId=308&flag=142

The following provides information on how to customize the resource files and specify the access URL of the resource files.

For some features, you can customize the filename as required. The following table lists the special characters supported by Yealink IP phones:

Platform / Server	HTTP/HTTPS	TFTP/FTP
Windows	**Support:** ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } (including space) **Not Support:** | < > : " / \ * ? # % & = +	**Support:** ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } % & = + (including space) **Not Support:** | < > : " / \ * ? #
Linux	**Support:** ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } | < > : " (including space) **Not Support:** / \ * ? # % & = +	**Support:** ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } | < > : " % & = + (including space) **Not Support:** / \ * ? #

Customizing a Replace Rule File

You can create replace rules directly in the configuration files, or create multiple replace rules using the supplied replace rule template file (*DialPlan.xml*). The existing replace rules on the phones will be overwritten by the new downloaded replace rules.

When editing the replace rule template file, learn the following:

- <dialrule> indicates the start of the template file and </dialrule> indicates the end of the template file.

- Create replace rules between <dialrule> and </dialrule>.

- At most 20 replace rules can be added to the IP phone.

- When specifying the desired line(s) to apply the replace rule, the valid values are 0 and line IDs. The digit 0 stands for all lines. Multiple line IDs are separated by commas.

Basic expression syntaxes of the replace rule are listed in the following table:

.	The dot "." can be used as a placeholder or multiple placeholders for any string. Example: "12." would match "123", "1234", "12345", "12abc", etc.
x	The "x" can be used as a placeholder for any character. Example: "12x" would match "121", "122", "123", "12a", etc.
-	Numeric ranges are allowed within the brackets: Digit "-" Digit. Example:

	"[5-7]" would match the number"**5**", "**6**"or "**7**".
[]	The square brackets "[]" can be used as a placeholder for a single character which matches any of a set of characters. Example: "91[5-7]1234" would match "91**5**1234", "91**6**1234", "91**7**1234", etc.
()	The parenthesis "()" can be used to group together patterns, for instance, to logically combine two or more patterns. Example: "([1-9])([2-7])3" would match "**92**3", "**15**3", "**67**3", etc.
$	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 IP phone will replace the number with "9001**235**4**599**". "$1" means 3 digits in the first parenthesis, that is, "235". "$2" means 2 digits in the second parenthesis, that is, "99".

To customize a replace rule file:

1. Open the template file (*DialPlan.xml*) using an ASCII editor.
2. For each replace rule you wish to add, add the following string to the file. Each starts on a separate line:

   <data rule="" replace="" lines=""/>

   Where:

   rule="" specifies the number to be replaced.

   replace="" specifies the alternate string.

   lines="" specifies the desired line(s) for this rule. When you leave it blank or enter "0", this replace rule will apply to all lines.
3. Specify the values within double quotes.
4. Save the change.

The following is an example of the replace rule file:

```
<dialrule>
  <data rule="1" replace="05928665234" lines=""/>
  <data rule="2(xx)" replace="002$1" lines="0"/>
  <data rule="5([6-9])(.)" replace="3$2" lines="1,2,3"/>
  <data rule="0(.)" replace="9$1" lines="2"/>
  <data rule="1009" replace="05921009" lines="1"/>
</dialrule>
```

Specifying the Access URL

After editing the replace rule file, store the file to the directory of the provisioning server, and then specify the access URL of the replace rule file in the configuration file.

```
############################################################
##              Configure the access URL of the replace rule file              ##
############################################################
dialplan_replace_rule.url =
```

For example, configure the access URL (e.g., tftp://192.168.1.100/DialPlan.xml) of the replace rule file using the parameter "dialplan_replace_rule.url". During the auto provisioning process, the phone connects to the TFTP server "192.168.1.100", and downloads the replace rule file "DialPlan.xml".

Customizing a Local Contact File

You can add contacts manually on the handset. In some cases, you may want to add multiple contacts to the desired handset at the same time. You can add multiple contacts using the supplied local contact template file (ContactData.xml). When adding a contact, only the display name, office number and mobile number can be specified for the contact.

> Yealink IP phones support both *.xml and *.csv formats.

When editing the local contact template file, learn the following:

- <root_contact> indicates the start of the template file and </root_contact> indicates the end of the template file.

- Add local contacts between <root_contact> and </root_contact>.

To customize a local contact file:

1. Open the template file (ContactData.xml) using an ASCII editor.

2. For each contact that you wish to add, add the following string to the file, each starting on a separate line:

   <contact display_name="" office_number="" mobile_number=""/>

   Where:

   display_name="" specifies the name of the contact.

   office_number="" specifies the office number of the contact.

   mobile_number="" specifies the mobile number of the contact.

3. Specify the values within double quotes.

4. Save the change.

The following shows an example of the local contact file:

```
<root_contact>
  <contact display_name="Alice" office_number="2215"
mobile_number=""/>
  <contact display_name="Bob" office_number="2216" mobile_number=""/>
</root_contact>
```

Specifying the Access URL

After editing a local contact file, you need to store the file to the directory of the provisioning server, and then specify the access URL of the local contact file in the configuration file.

```
#####################################################
##              Configure the access URL of the local contact file              ##
#####################################################
##X ranges from 1 to 5 (corresponds to the internal handset 1-5).
handset.X.contact_list.url =
```

For example, you want to import a local contact file to the handset 2, configure the access URL (e.g., tftp://192.168.1.100/ContactData.xml) of the local contact file using the parameter "handset.2.contact_list.url =" (X is replaced by 2). During the auto provisioning process, the phone connects to the TFTP server "192.168.1.100", and downloads the contact file "ContactData.xml" for the handset 2.

Updating Firmware

You can update the firmware of the base station manually via web user interface. You can also update the firmware of base stations via auto provisioning in batches.

To update the firmware of base stations via auto provisioning in batches, ask the distributor for the firmware file, upload it to the root directory of the provisioning server,

and then specify the access URL in the configuration files.

```
###############################################
##            Configure the access URL of the Firmware File            ##
###############################################
```

firmware.url =

For example, configure the access URL (e.g., tftp://192.168.1.100/25.73.0.10.rom) of the firmware file using the parameter "firmware.url". During auto provisioning, the phone connects to the TFTP server "192.168.1.100" and downloads the firmware file "25.73.0.10.rom".

You can upgrade handset firmware via USB cable or over the air. For more information on upgrading handset firmware, refer to *Upgrading W52x Handset Firmware*.

Obtaining Provisioning Server Address

To connect to the provisioning server and download configuration files, the phone should obtain the provisioning server address beforehand. Yealink W52P IP DECT phones support obtaining the provisioning server address in the following ways:

- Plug and Play (PnP)

- DHCP Options

- Phone Flash

- Configuring Wildcard of the Provisioning Server URL

When the phone starts up, it will go by the three ways mentioned above to try to obtain the provisioning server address. The priority of the obtained provisioning server address is: PnP->DHCP Options (Custom option->option 66->option 43) ->Phone Flash.

The following sections detail the process of each way and the wildcard of the provisioning server the phone supports.

Plug and Play (PnP)

Yealink W52P IP DECT phones support obtaining the provisioning server address from the PnP server during startup. The phone broadcasts the PnP SUBCRIBE message to obtain a provisioning server address during startup. To use Plug and Play, make sure PnP feature is enabled on the IP phone.

> To obtain the provisioning server address from the PnP server, make sure the provisioning server address is preconfigured on the PnP server.

21

To enable PnP feature via web user interface:

1. Click on **Phone**->**Auto Provision**.
2. Mark the **On** radio box in the **PNP** field.
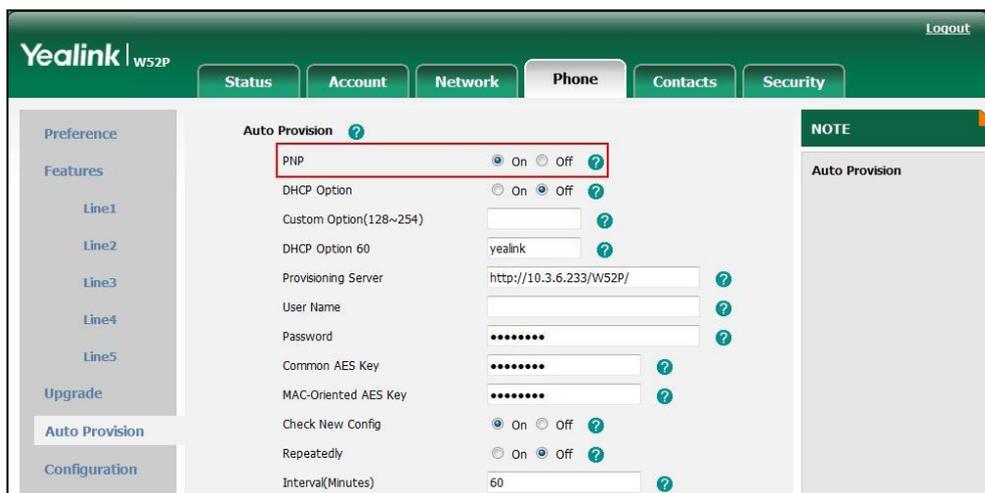
3. Click **Confirm** to accept the change.

To obtain the provisioning server address from the PnP server:

Any PnP server activated in the network responses with a **SIP NOTIFY** message, and an address of the provisioning server is contained in the message body.
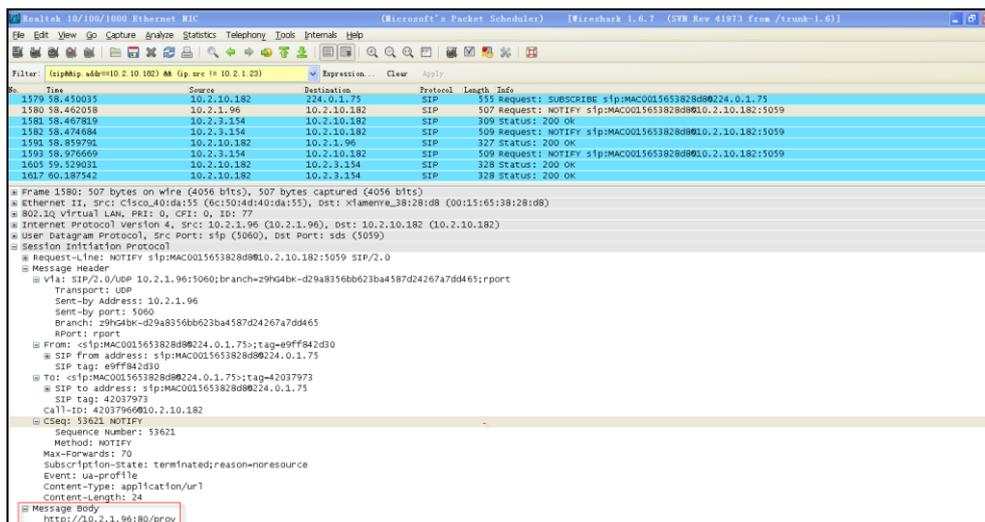
After the phone obtains the provisioning server address from the PNP server, it will connect to the provisioning server and perform the auto provisioning process during startup.

DHCP Options

Yealink W52P IP DECT phones support obtaining the provisioning server address by detecting DHCP options.

The phone will automatically detect the option 66 and option 43 for obtaining the provisioning server address. DHCP option 66 is used to identify the TFTP server. DHCP option 43 is a vendor-specific option, which is used to transfer the vendor-specific information. You can configure the phone to obtain the provisioning server address via a custom DHCP option. To obtain the provisioning server address via a custom DHCP option, make sure the DHCP option is properly configured on the phone.

The custom DHCP option must be in accordance with the one defined in the DHCP server. For more information on how to configure a DHCP server, refer to Configuring a DHCP Server on page 61.

To configure a custom DHCP option via web user interface:

1.   Click on **Phone**->**Auto Provision**.

2.   Mark the **On** radio box in the **DHCP Option** field.

3.   Enter the value in the **Custom Option (128~254)** field.

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

During startup, the phone will broadcast DHCP request with DHCP options for obtaining the provisioning server address. The provisioning server address will be found in the received DHCP response message.

After the phone obtains the provisioning server address from the DHCP server, it will connect to the provisioning server and perform the auto provisioning process during startup.

The following figure shows the example messages of obtaining the TFTP server address from a custom DHCP option:
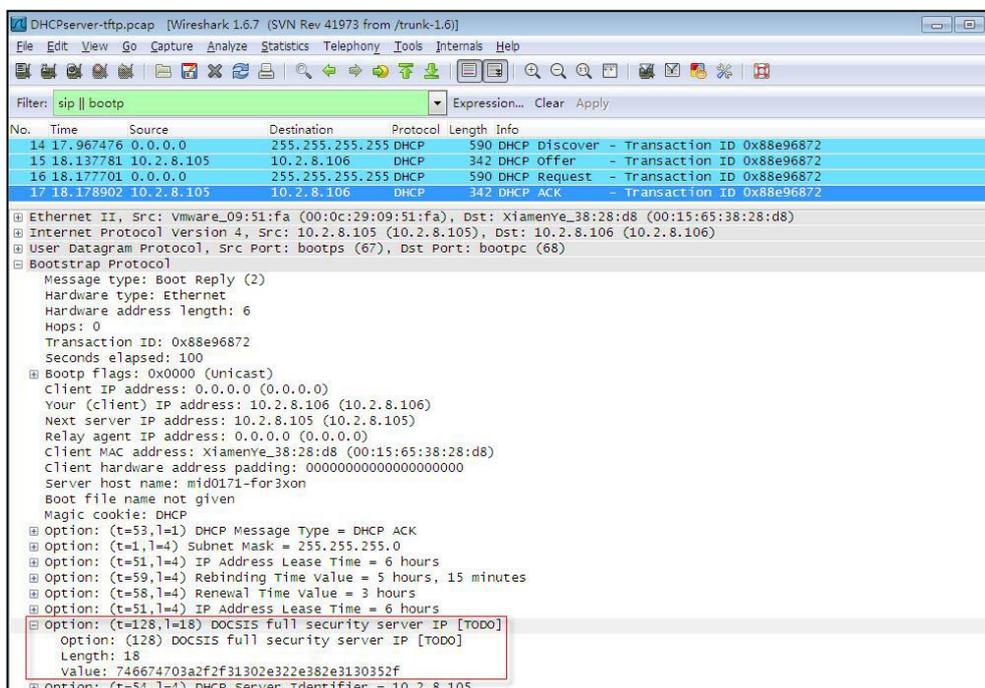
Right click the root node of the custom option (e.g., option 128) shown on the above figure, and select **Copy**->**Bytes**->**Printable Text Only**. Paste the copied text in your favorite text editor to check the address, for example, tftp://192.168.1.100/.

Phone Flash

Yealink W52P IP DECT phones support obtaining the provisioning server address from the phone flash. To obtain the provisioning server address by reading the IP phone flash, make sure the configuration is set properly.

To specify the provisioning server address via web user interface:

1. Click on **Phone**->**Auto Provision**.

2. Enter the address, user name and password of the provisioning server in the
    Provisioning Server, **User Name** and **Password** fields (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 the auto provisioning process by one of the following
update modes: Power On, Repeatedly, Weekly, Auto Provision Now, SIP NOTIFY
Message and Multi-mode Mixed. For more information on these update modes, refer to
Configuring the Updating Mode on Page 27.

Configuring 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 configuration files are located

*   **$MAC**: it is used to identify the MAC address of the IP phone.

The parameter "auto_provision.url_wildcard.pn" is used to configure the directory name
the configuration files located. For more information on the parameter, refer to
Description of Configuration Parameters in CFG Files on page 69.

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
"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 configuration files from the identified directory on the provisioning server.

> The value of the parameter "auto_provision.url_wildcard.pn" must be configured in accordance with the directory name of the provisioning server directory where the configuration files of the IP phones are located.

The following example assists in explaining the wildcard feature:

You want to deploy SIP-T28P and W52P IP phones simultaneously in your environment. IP phones are configured to obtain the provisioning server address via DHCP options. The following details how to deploy the W52P IP DECT phones using wildcard feature.

1. Create two directories on the root directory of provisioning server.
2. Configure the directory name of these two directories to be "T28P" and "W52P" respectively.
3. Place the associated configuration files to the directories created above.
4. Configure the provisioning server URL on the DHCP server as:
    tftp://192.168.1.100/$PN.
5. Configure the value of the parameter "auto_provision.url_wildcard.pn".

    The default value of the parameter "auto_provision.url_wildcard.pn" on the W52P IP DECT phones is "W52P". If the directory name is not configured as "W52P", you need to configure the value of this parameter to be the directory name on the W52P IP DECT 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 "W52P" for the W52P IP DECT phones. When performing auto provisioning, the W52P IP DECT phones request to download configuration files (y000000000025.cfg and <MAC>.cfg files) from the provisioning server address "tftp://192.168.1.100/W52P".

If the URL is configured as "tftp://192.168.1.100/$PN/$MAC.cfg" on the DHCP server, the W52P IP DECT phones will replace the characters "$PN" with "W52P" and "$MAC" with their MAC addresses. For example, the MAC address of one W52P IP DECT phone is 00156522f5g3. When performing auto provisioning, the IP phone will only request to download the 00156522f5g3.cfg file from the provisioning server address "tftp://192.168.1.100/W52P".

Configuring the Updating Mode

The following six updating modes can be used to trigger the auto provisioning process:

- Power On

- Repeatedly

- Weekly

- Auto Provision Now

- Multi-mode Mixed

- SIP Notify Message

In addition the six update modes, the IP phone also supports triggering auto provisioning via activation code. The following sections introduce the six update modes and auto provisioning via activation code method in detail.

> When there is an active call on the phone during provisioning, the auto provisioning process will detect the call status every 30 seconds. If the call is released within 2 hours, the auto provisioning process will be performed normally. Otherwise, the process will end, due to timeout.

Power On

The phone can perform the auto provisioning process when the IP phone is powered on. You can activate the Power On mode via web user interface. The Power On mode is activated by default.

To enable the Power On mode via web user interface:

1. Click on **Phone**->**Auto Provision**.
2. Mark the **On** radio box in the **Check New Config** field.

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

Repeatedly

The phone can perform auto provisioning at regular intervals. You can activate the Repeatedly mode and configure the interval for the Repeatedly mode via web user interface. The default interval is 60 minutes.

To activate Repeatedly mode via web user interface:

1. Click on **Phone**->**Auto Provision**.

2. Mark the **On** radio box in the **Repeatedly** field.

3. Enter the interval time (in minutes) in the **Interval (Minutes)** field.

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

Weekly

The phone can perform auto provisioning at the fixed time every week. You can activate Weekly mode via web user interface and configure what time of the day and which day of the week for the phone to perform auto provisioning. For example, you can configure the phone to check and update new configuration between 2 to 3 o'clock every Friday and Sunday.

To activate Weekly mode via web user interface:

1. Click on **Phone**->**Auto Provision**.

2. Mark the **On** radio box in the **Weekly** field.

3. Enter the desired time in the **Time** field.

4. Select one or more days of week in the **Day of week** field.

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

Auto Provision Now

You can use the Auto Provision Now mode to manually trigger the phone to perform auto provisioning immediately via web user interface.

To use Auto Provision Now mode via web user interface:

1. Click on **Phone**->**Auto Provision**.

2. Click the **Autoprovision Now** button.
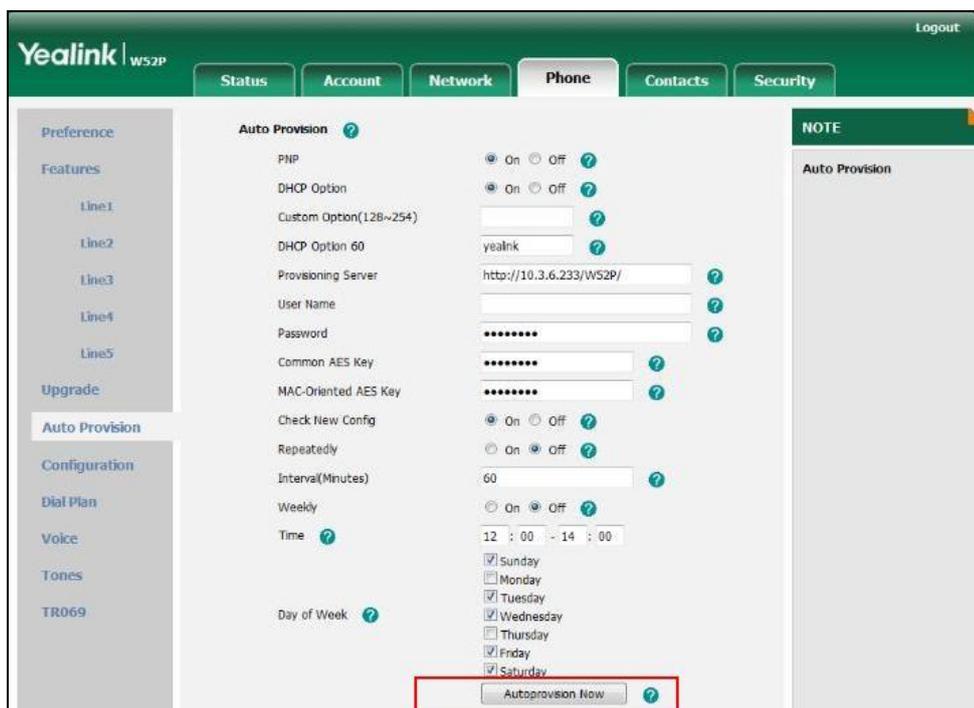
The phone will perform the auto provisioning process immediately.

Multi-mode Mixed

You can activate more than one updating mode for auto provisioning. For example, you can activate the "Check New Config" and "Repeatedly" modes simultaneously, the phone will perform the auto provisioning process when it is powered on and at a specified interval.

SIP Notify Message

The phone can perform the auto provisioning process when receiving a SIP NOTIFY message which contains the header "Event:check-sync". Whether the 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 Description of Configuration Parameters in CFG Files on page 69.

This update mode requires server support.

The following figure shows the message flow:
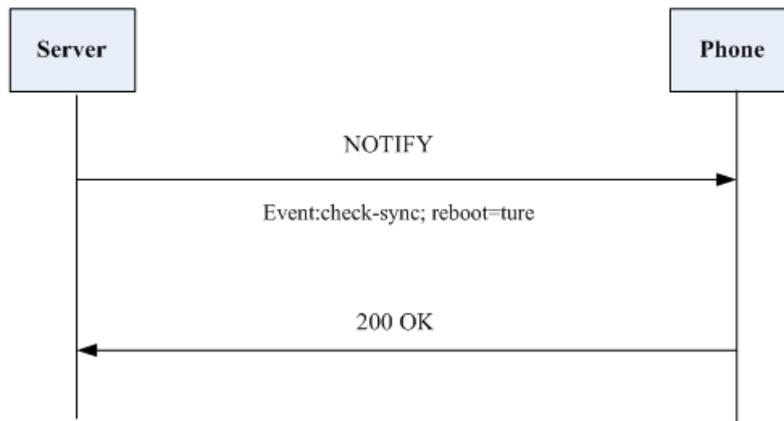
Auto Provisioning via Activation Code

In addition to the updating modes introduced above, users can trigger W52P IP DECT phones to perform auto provisioning by dialing an activation code. To use this method, the activation code and the provisioning server address need to be pre-configured on the IP phones. This method is normally used for IP phones distributed by retail sales. It has the advantage that the IP phones do not need to be handled (e.g., registering account) before sending them to end-users.
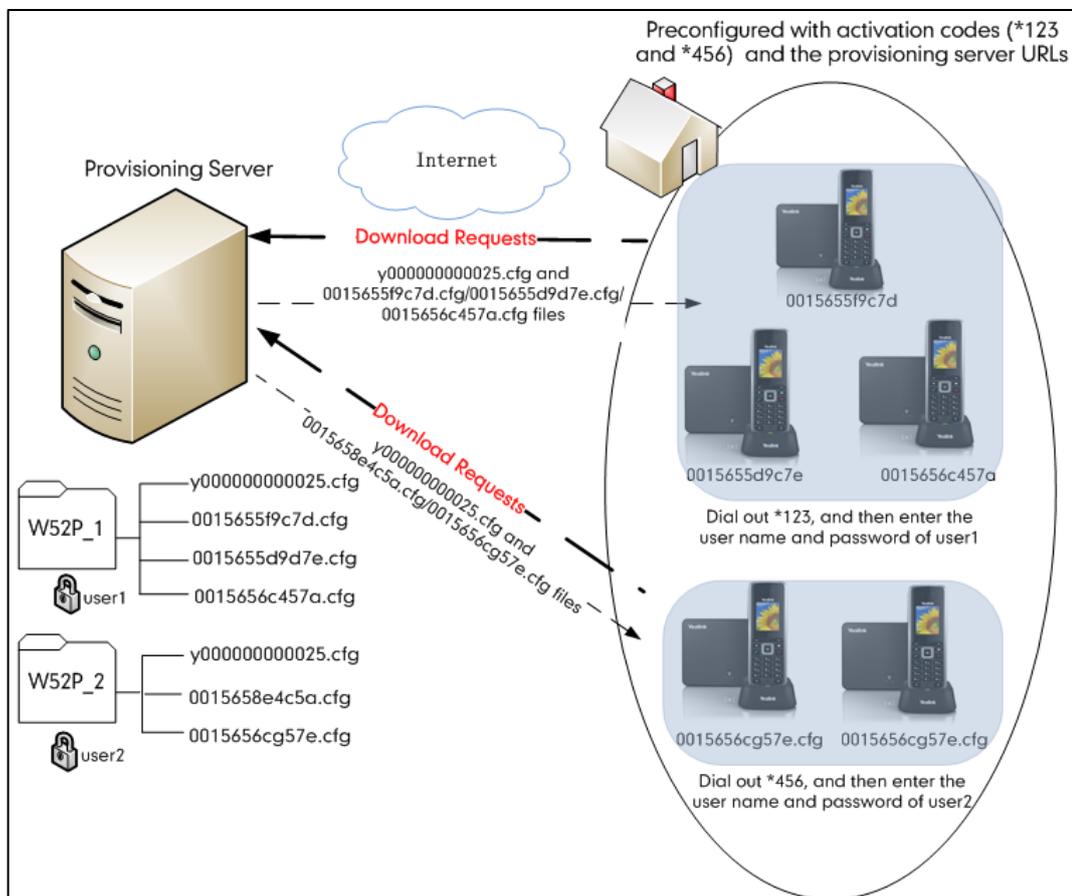
The following lists the processes for triggering auto provisioning via activation code:

1. Create multiple directories (e.g., two directories) on the provisioning server.

2. Store a common CFG file and multiple <MAC>.cfg files to each directory on the provisioning server.

3. Configure a user name and password for each directory.

   The user name and password provides a means of conveniently partitioning the configuration files for different base stations. To access the specified directory, you need to provide the correct user name 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 string and special characters "*", "#" with a maximum of 24 characters.

   The following are example configurations in the configuration file for IP phones:

   ```
   autoprovision.1.code = *123

   autoprovision.1.url = tftp://192.168.1.30/W52P_1/

   autoprovision.2.code = *456

   autoprovision.2.url = tftp://192.168.1.30/W52P_2/
   ```

5. Send the IP phone, specified activation code and associated user name and password to each end-user.

6. Set up the IP phone, and then dial the activation code after phone startup to trigger the IP phone to perform auto provisioning.

   The LCD screen will prompt for the user name and password.

7. Enter the user name and password.

   The entered user name and password must be correspond to the directory where the configuration files of the IP phone are located. If you enter invalid user name or password, the LCD screen will prompt the message "Wrong user name or password!". The prompt message will disappear in two seconds, and the LCD screen will return to the idle screen. You need to dial out the activation code again to trigger the auto provisioning process.

The IP phone downloads the y000000000025.cfg and the corresponding <MAC>.cfg files from the provisioning server to complete phone configurations.

The entered user name and password will be saved to the IP phone for next auto provisioning via activation code and auto provisioning via update modes.

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.

If more than one handset registered on the same base station triggers the auto provisioning process via the activation code simultaneously, the base station will perform the auto provisioning process when any handset enters the correct user name and password.

The following parameters are used to configure the auto provisioning via activation code method (X ranges from 1 to 50):

#Configure the auto provisioning name.

```
autoprovision.X.name
```

#Configure the activation code.

```
autoprovision.X.code
```

#Configure the URL of the provisioning server.

```
autoprovision.X.url
```

#Configure the username and password for downloading configuration files.

```
autoprovision.X.user
```

```
autoprovision.X.password
```

For more information on these parameters, refer to Description of Configuration Parameters in CFG Files on page .

Downloading and Updating Configuration Files

Downloading Configuration Files

After obtaining the provisioning server address in one of the ways introduced above, the phone will request to download the configuration files from the provisioning server when it is triggered to perform auto provisioning. During the auto provisioning process, the phone will try to download the y000000000025.cfg file firstly, and then the <MAC>.cfg file from the provisioning server. If the access URLs of the resource files have been specified in the configuration files, the phone will try to download and update the resource files.

Resolving and Updating Configurations

After downloading, the phone resolves the configuration files and resource files (if specified in the configuration files), and then updates the configurations and resource files to the phone flash. Generally, updated configurations will automatically take effect after the auto provisioning process is completed. For update of some specific configurations which require a reboot before taking effect, for example, network configurations, the phone will reboot to make the configurations effective after the auto provisioning process is completed.

The phone calculates the MD5 values of the downloaded files before updating them. If the MD5 values of the y000000000025.cfg and <MAC>.cfg configuration files are the same as those of the last downloaded configuration files, this means that these two configuration files on the provisioning server are not changed. The phone will complete auto provisioning without repeated update. This is used to avoid unnecessary restart and 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 reboot after auto provisioning. If you want to force the IP phone to perform a reboot after auto provisioning, you can configure "auto_provision.reboot_force.enable = 1" in the configuration file.

For more information on the specific configurations which require reboot during provisioning and the parameter "auto_provision.reboot_force.enable", refer to the section Description of Configuration Parameters in CFG Files on page 69.

If the configuration files have been AES encrypted, the phone uses the Common AES key to decrypt the y000000000025.cfg file and the MAC-Oriented AES key to decrypt the <MAC>.cfg file after downloading the configuration files.

Downloading and Updating <MAC>-local.cfg File

You can configure the IP phone whether to download the <MAC>-local.cfg file from the provisioning server, and update configurations in the <MAC>-local.cfg file to protect personalized settings after auto provisioning.

If the IP phone is configured to download the <MAC>-local.cfg file from the provisioning server, it will download the <MAC>-local.cfg file after downloading the y000000000025.cfg and <MAC>.cfg files.

If the IP phone is configured to protect personalized settings, it will update configurations in the <MAC>-local.cfg file. The IP Phone updates configuration files during auto provisioning in sequence: Common>MAC-Oriented>MAC-local. So when configuration items in the <MAC>-local.cfg file are duplicated with the ones in the downloaded y000000000025.cfg or the <MAC>.cfg file, the settings in the <MAC>-local.cfg file will take effect.

For more information on how to configure the IP phone, refer to Scenario A Protect personalized settings on page 41.

Verifying Configurations

After auto provisioning, you can then verify the update via phone user interface or web user interface of the phone.

During the auto provisioning process, you can monitor the downloading requests and response messages using a WinPcap tool. The following shows some examples.

Example1: Yealink W52P IP DECT phone downloads configuration files from the TFTP server.

Example 2: Yealink W52P IP DECT phone downloads the configuration files from the FTP server.

Example 3: Yealink W52P IP DECT phone downloads the configuration files from the HTTP server.

Specific Scenarios-Protect Personalized Settings

Generally, the administrator deploys IP phones in batch via auto provisioning, yet some users would like to remain the personalized settings (e.g., ring tone, dial plan and handset name) after auto provisioning. W52P IP DECT phones running firmware version 73 or later can be configured to protect personalized settings after auto provisioning. Several specific scenarios are illustrated in the following sections to assist in explaining the personalized settings protecting process.

> Yealink IP phones support FTP, TFTP, HTTP and HTTPS protocols for uploading the MAC-local CFG file. This section takes the TFTP protocol as an example. Before performing the following, make sure that the provisioning server supports uploading.
>
> If you are using the HTTP(S) server, you can specify the way the IP phone uploads the MAC-local CFG file to the provisioning server. It is determined by the value of the parameter "auto_provision.custom.upload_method". For more information, refer to
>
> Normally, the base station can delivtier the handset settings (configured via auto provisioning) after handset reboot or handset registration.

Configuration Parameters

The following table lists the configuration parameters used to determine the phone behavior for protecting personalized settings:

Parameters	Permitted Values	Default
auto_provision.custom.protect	**0 or 1**	**0**
Description: Enables or disables the IP phone to protect personalized settings after auto provisioning. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), personalized settings of the base station configured via the handset or web user interface and the handset settings configured via the handset will be remained after auto provisioning.		
auto_provision.custom.sync	**0 or 1**	**0**
Description: Enables or disables the IP phone to periodically (every 5 minutes) upload the <MAC>-local.cfg file to the provisioning server, and download the <MAC>-local.cfg file from the provisioning server during auto provisioning. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will periodically upload the <MAC>-local.cfg file to the provisioning server to back up this file. During auto provisioning, the IP phone will download the <MAC>-local.cfg file from the provisioning server to override the one stored on the phone. If it is set to 0 (Disabled), the IP phone will not upload the <MAC>-local.cfg file to the provisioning server. During auto provisioning, the IP phone will not download the <MAC>-local.cfg file from the provisioning server.		
auto_provision.custom.upload_method	**0 or 1**	**0**
Description: Configures the way the IP phone uploads the <MAC>-local.cfg file to the provisioning server (for HTTP/HTTPS server only). **0**-PUT **1**-POST		

Parameters	Permitted Values	Default
Note: It works only if the value of the parameter "auto_provision.custom.sync" is set to 1 (Enabled).		
auto_provision.handset_configured.enable	**0 or 1**	**0**

Description:

Enables or disables the base station to deliver handset settings configured via auto provisioning to the registered handset.

0-Disabled

1-Enabled

If it is set to 0 (Disabled), the base station will not deliver handset settings configured via auto provisioning to the handset. The handset settings can be only changed via the handset.

If it is set to 1 (Enabled), the base station will deliver the handset settings configured via auto provisioning to the handset. Handset reboot or registration will also trigger the base station to deliver the stored handset settings to the handset. If the parameter "auto_provision.custom.protect" is also set to 0 (Disabled), the personalized handset settings will be overridden, and other handset settings will be changed.

If it is set to 1 (Enabled), and the parameter "auto_provision.custom.protect" is set to 1 (Enabled), the personalized handset settings will not be overridden, but other handset settings will be changed.

For more information on how to configure these parameters in different scenarios, refer to the following introduced scenarios.

The following lists the configuration parameters for handset settings:

```
#Configures the language of the handset.
custom.handset.language
#Configures the time format of the handset.
custom.handset.time_format
#Configures the date format of the handset.
custom.handset.date_format
#Configures the color scheme of the handset.
custom.handset.color_scheme
#Enables or disables screen saver feature of the handset.
custom.handset.screen_saver.enable
#Enables or disables the handset to always turn on the backlight when it is in the
#charging state.
```

```
custom.handset.backlight_in_charger.enable
```

#Enables or disables the handset to always turn on the backlight when it is not in the

#charging state.

```
custom.handset.backlight_out_of_charger.enable
```

#Enables or disables the handset to turn on the keypad light when any key is pressed.

```
custom.handset.keypad_light.enable
```

#Enables or disables the handset to play a tone when any key is pressed.

```
custom.handset.keypad_tone.enable
```

#Enables or disables the handset to play a tone when a user saves settings or places

#the handset in the charger cradle.

```
custom.handset.confirmation_tone.enable
```

#Enables or disables the handset to play a tone when the capacity of the batteries is

#low.

```
custom.handset.low_battery_tone.enable
```

#Enables or disables the message key LED to flash red when the handset receives a

#voice mail.

```
custom.handset.voice_mail_notify_light.enable
```

#Enables or disables the message key LED to flash red when the handset misses a call.

```
custom.handset.missed_call_notify_light.enable
```

#Configures whether the IP phone automatically answers an incoming internal intercom

#call and plays a warning tone.

```
custom.handset.auto_intercom
```

#Enables or disables a user to answer incoming calls by lifting the handset from the

#charger cradle without having to press the off-hook key.

```
custom.handset.auto_answer.enable
```

#Enables or disables the eco mode to greatly reduce the transmission power and

#signal output when the handset is in the talk mode.

```
custom.handset.eco_mode.enable
```

The input method of the handset can be only configured via the handset.

Scenario A Protect personalized settings

Scenario (A) Protecting personalized settings of the base station (running firmware version prior to X.73.0.1)

The administrator wishes to upgrade firmware from the old version to the latest version. Meanwhile, protect personalized settings of the base station after auto provisioning and upgrade.

Scenario Conditions:

- The current firmware version of the base station is 25.50.0.20. This firmware version does not support protecting personalized settings and generating a <MAC>-local.cfg file.

- The target firmware version is 25.73.0.1. This firmware version supports protecting personalized settings after auto provisioning or upgrade.

- The MAC address of the IP phone is 001565221229.

- Provisioning server URL: tftp://192.168.1.211.

- Place the target firmware to the root directory of the provisioning server.

- Create a new directory "ProvisioningDir_new" under the root directory of the provisioning server.

The IP phone with old firmware does not support protecting personalized settings after auto provisioning and upgrade. You can configure the value of the parameter "auto_provision.custom.protect" to 1 in the configuration file to protect personalized settings after auto provisioning and upgrade.

Do the following operations:

1. Place the configuration files (y000000000025.cfg and 001565221229.cfg) that you want the IP phone to download to the new directory "ProvisioningDir_new" of the provisioning server.

2. Add/Edit the following parameters in the y000000000025.cfg file or the 001565221229.cfg file as follows.

   ```
   auto_provision.custom.protect = 1
   ```

3. Create a blank configuration file "y000000000025.cfg" on the root directory of the provisioning server and add the following parameters to this file.
   #Configure the access URL of the firmware file.
   ```
   firmware.url = tftp://192.168.1.211/25.73.0.1.rom
   ```
   #Configure the access URL of configuration files.
   ```
   auto_provision.server.url = tftp://192.168.1.211/ProvisioningDir_new
   ```

4. Trigger the IP phone to perform the auto provisioning process. For more information

on how to trigger the auto provisioning process, refer to Configuring the Updating Mode on page 27.

During auto provisioning, the IP phone first downloads the y000000000025.cfg file, and then downloads firmware from the root directory of the provisioning server.

The IP phone reboots to complete firmware upgrade, and then starts auto provisioning process again which is triggered by phone reboot (the power on mode is enabled by default). It downloads the y000000000025.cfg and 001565221229.cfg files in sequence from the new directory "ProvisioningDir_new" of the provisioning server. As no 001565221229-local.cfg file exists on the IP phone, the IP phone automatically generates a 001565221229-local.cfg file which saves the personalized settings of the old firmware. The IP phone updates configurations in the downloaded configuration files orderly to the IP phone system. As the value of the parameter "auto_provision.custom.protect" is set to 1, the phone also updates the configurations stored in the 001565221229-local.cfg file. As a result, the personalized settings of the old firmware are remained after upgrade and auto provisioning.

Scenario (B) Protecting personalized settings of the base station (IP phones are running firmware version X.73.0.1 or later)

The administrator wishes to upgrade firmware to the latest version. Meanwhile, protect personalized settings after auto provisioning and upgrade.

Scenario Conditions:

- The current firmware version of the base station is 25.73.0.1.

- The target firmware version: 25.73.0.20.

- The current and target firmware versions both support protecting personalized settings and generating a <MAC>-local.cfg file.

- The MAC address of the IP phone is 001565221229.

- Provisioning server URL: tftp://192.168.1.211

- Place the target firmware to the root directory of the provisioning server.

To protect personalized settings after auto provisioning and upgrade, you need to configure the value of the parameter "auto_provision.custom.protect" to 1 in the configuration file.

Do one of the following operations:

Operation I

1. Add/Edit the following parameters in the y000000000025.cfg file or the 001565221229.cfg file you want the IP phone to download:

```
auto_provision.custom.protect = 1

auto_provision.custom.sync = 1
```

#Configure the access URL of the firmware file.

```
firmware.url = tftp://192.168.1.211/25.73.0.20.rom
```

2. Trigger the IP phone to perform the auto provisioning process. For more information on how to trigger auto provisioning process, refer to Configuring the Updating Mode on page 27.

During auto provisioning, the IP phone first downloads the y000000000025.cfg file, and then downloads firmware from the root directory of the provisioning server.

The IP phone reboots to complete firmware upgrade, and then starts auto provisioning process again which is triggered by phone reboot (the power on mode is enabled by default). It downloads the y000000000025.cfg, 001565221229.cfg and the 001565221229-local.cfg file in sequence from the provisioning server, and then updates configurations in these downloaded configuration files orderly to the IP phone system. The IP phone starts up successfully, and the personalized settings are remained after auto provisioning.

When a user modifies configurations of the base station via the handset or web user interface, the IP phone will save the personalized settings to the 001565221229-local.cfg file on the phone, and then periodically (every 5 minutes) upload this file to the provisioning server.

Operation II

1. Add/Edit the following parameters in the y000000000025.cfg file or the 001565221229.cfg file you want the IP phone to download:

```
auto_provision.custom.protect = 1

auto_provision.custom.sync = 0
```

#Configure the access URL of the firmware file.

```
firmware.url = tftp://192.168.1.211/25.73.0.20.rom
```

2. Trigger the IP phone to perform the auto provisioning process. For more information on how to trigger auto provisioning process, refer to Configuring the Updating Mode on page 27.

During auto provisioning, the IP phone first downloads the y000000000025.cfg file, and then downloads firmware from the root directory of the provisioning server.

The IP phone reboots to complete firmware upgrade, and then starts auto provisioning process again which is triggered by phone reboot (the power on mode is enabled by default). It downloads the y000000000025.cfg and 001565221229.cfg files in sequence from the provisioning server, and then updates configurations in the downloaded configuration files orderly to the IP phone system. As the value of the parameter "auto_provision.custom.protect" is set 1, the IP phone will also update configurations in the 001565221229-local.cfg file saved on the IP phone. As a result, the personalized settings are remained after auto provisioning.

When a user modifies configurations of the base station via the handset or web user interface, the IP phone will save the personalized settings to the 001565221229-local.cfg file saved on the IP phone only.

<div style="border: 1px solid red; padding: 10px; color: red;">

If value of the parameter "auto_provision.custom.protect" is set to 0, the personalized settings will be overridden after auto provisioning, no matter what the value of the parameter "auto_provision.custom.sync" is.

For more information on the flowchart of protect personalized configuration settings, refer to Auto Provisioning Flowchart (Protect personalized settings) on page 68.

</div>

Scenario (C) Protecting personalized settings of the handset (IP phones are running firmware version X.73.0.1 or later)

The handset settings can be configured via the handset or auto provisioning. The personalized handset settings stand for the handset settings configured via the handset. The administrator wishes to change some handset settings via auto provisioning, but protect personalized handset settings after auto provisioning.

Scenario Conditions:

- The current firmware version of the base station and handset are 25.73.0.1 and 26.73.0.1 respectively. This firmware version supports protecting personalized handset settings after auto provisioning.

- Provisioning server URL: tftp://192.168.1.211

To configure the handset settings via auto provisioning, you need to configure the value of the parameter "auto_provision.handset_configured.enable" to 1. To protect personalized handset settings after auto provisioning, you need to configure the value of the parameter "auto_provision.custom.protect" to 1.

Do the following operations:

1. Add/Edit the following parameters in the y000000000025.cfg file or 001565221229.cfg file you want the IP phone to download:

   ```
   auto_provision.custom.protect = 1

   auto_provision.handset_configured.enable = 1
   ```

2. Trigger the IP phone to perform the auto provisioning process. For more information on how to trigger auto provisioning process, refer to Configuring the Updating Mode on page 27.

During auto provisioning, the IP phone will download the configuration files and update configurations in the configuration files. As the value of the parameter "auto_provision.handset_configured.enable" is set to 1, handset settings will be changed via auto provisioning. As the value of the parameter "auto_provision.custom.protect" is set to 1, the personalized handset settings will be

remained after auto provisioning.

If value of the parameter "auto_provision.custom.protect" is set to be 0, and the value of the parameter "auto_provision.handset_configured.enable" is set to 1, the personalized handset settings will be overridden after auto provisioning. If the value of the parameter "auto_provision.handset_configured.enable" is set to 0, the handset settings cannot be changed via auto provisioning no matter what the value of the parameter "auto_provision.custom.protect" is.

For more information on the configuration parameters of handset settings, refer to Configuration Parameters on page 38.

Scenario B Clear personalized settings

Clearing personalized settings of the base station (running firmware version 25.73.0.1 or later)

The administrator or user wishes to clear personalized settings of the base station.

Scenario Conditions:

- The MAC address of the IP phone is 001565221229.

- The current firmware of the base station is 25.73.0.1 or later.

- Provisioning server URL: tftp://192.168.1.211

- The value of the parameter "auto_provision.custom.protect" is 1.

> The **Reset Local Config** option on the web user interface and the handset is available only if the value of the parameter "auto_provision.custom.protect" was set to 1.
>
> If the value of the parameter "auto_provision.custom.sync" was set to 1, the configurations in the 001565221229-local.cfg file on the provisioning server will be also cleared after resetting personalized settings of the base station.

Operations:

You can clear the personalized settings of the base station via the handset or web user interface.

To clear personalized settings of the base station via the handset:

1. Press ⟦OK⟧ to enter the main menu.
2. Select ⟦🛠⟧ ->**System Settings**.
3. Select **Reset Local Config**, and then press the **OK** soft key.
4. Enter the system PIN (default: 0000).
5. Press the **Done** soft key.

   The LCD screen prompts "Reset Base Local Configuration Now?".
6. Press the **Yes** soft key.

To clear personalized settings of the base station via web user interface:

1.   Click on **Phone**->**Upgrade**.

2.   Click **Reset Local Config**.

      The web user interface prompts "Are you sure to reset the local configuration?".

3.   Click **OK**.

Configurations in the 001565221229-local.cfg file saved on the phone will be cleared.

Clearing personalized settings of the handset

The administrator or user wishes to clear personalized settings of the specified handset.

Scenario Conditions:

•   The handset 1 was registered to the base station.

> You can only clear the personalized settings of the handset via the handset itself.

Operations:

To clear personalized settings of the handset:

1.   Press $\boxed{\text{OK}}$ to enter the main menu.

2.   Select $\boxed{\times}$ ->**System Settings**.

3.   Select **Handset Reset**, and then press the **OK** soft key.

      The LCD screen prompts "Reset handset to default?".

4.   Press the **Yes** soft key.

> If the value of the parameter "auto_provision.handset_configured.enable" is set to 1, the handset settings (configured via auto provisioning) stored on the base station will be delivered to the handset after handset reset. If the value of this parameter is set to 0, the handset settings will not be delivered to the handset after handset reset.

Scenario C Protecting personalized settings after reset

The base station requires factory reset when it has a breakdown, but the user wishes to remain personalized settings of the base station after factory reset. You can reset the base station via factory reset or base reset.

Scenario Conditions:

- The MAC address of the IP phone is 001565221229.

- Provisioning server URL: tftp://192.168.1.211.

- The value of the parameter "auto_provision.custom.sync" is 1.

- The value of the parameter "auto_provision.custom.protect" is 1.

As the parameter "auto_provision.custom.sync" was set to 1, the 001565221229-local.cfg file on the IP phone will be uploaded to the provisioning server at tftp://192.168.1.211.

Factory reset and base reset will only reset the settings of the base station to factory defaults. The handset settings will not be reset.

Operation I

To reset the base station to factory via web user interface:

1. Click on **Phone**->**Upgrade**.

2. Click **Reset Now**.

   The web user interface prompts "Do you want to reset to factory?".
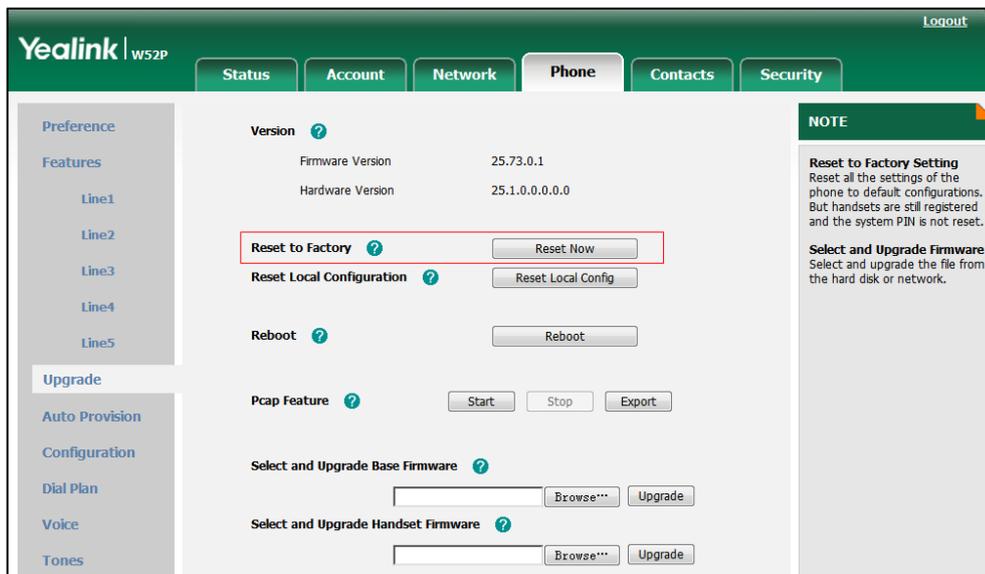
3. Click **OK**.

Operation II

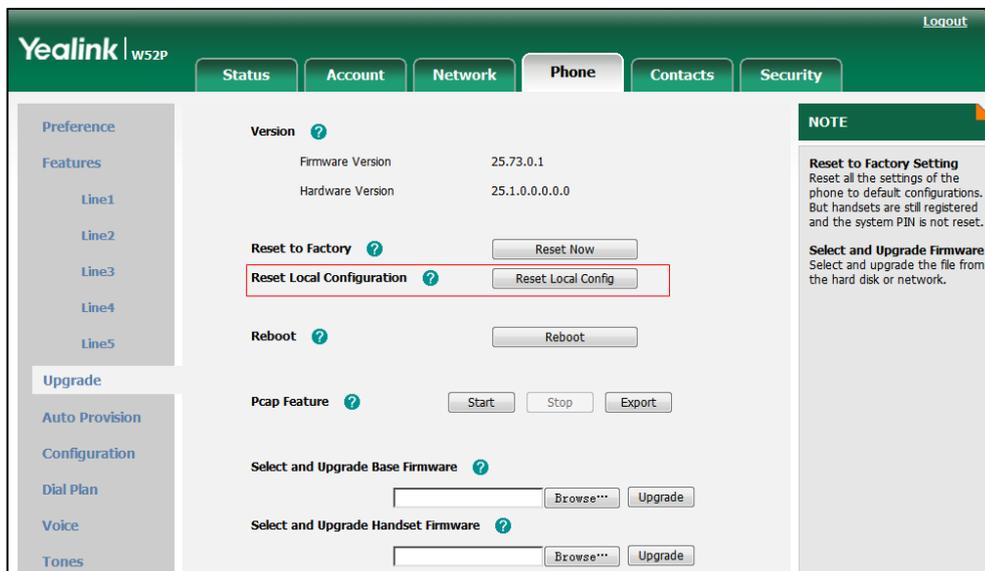**To reset the base station via the handset:**

1. Press [OK] to enter the main menu.

2. Select [🔧] ->**System Settings**.

3. Select **Base Reset**, and then press the **OK** soft key.

4. Enter the system PIN (default: 0000).

5. Press the **Done** soft key.

After startup, all configurations of base station will be reset to factory defaults. Configurations in the 001565221229-local.cfg file saved on the IP phone will also be cleared. But configurations in the 001565221229-local.cfg file stored on the provisioning server (tftp://192.168.1.211) will not be cleared after reset.

To retrieve personalized settings of the base station after factory reset:

1. Set the values of the parameters "auto_provision.custom.sync" and "auto_provision.custom.protect" to be 1 in the configuration file (y000000000025.cfg or 001565221229.cfg).

2. Trigger the phone to perform the auto provisioning process.

The IP phone will download the 001565221229-local.cfg file from the provisioning server, and then update configurations in it during auto provisioning. As a result, the personalized settings of the base station are retrieved after factory reset.

Scenario D Importing or exporting the local configuration file

The administrator or user can export the local configuration file to check the personalized settings of the base station configured by the user, or import the local configuration file to configure or change settings of the base station.

Scenario Conditions:

- The MAC address of the IP phone is 001565221229.

- The current firmware of the base station is 25.73.0.1 or later.

- Provisioning server URL: tftp://192.168.1.211.

> The <MAC>-local.cfg file can only store personalized settings of the base station. You cannot export or import the handset settings.
>
> As the personalized settings of the base station cannot be changed via auto provisioning when the value of the parameter "auto_provision.custom.protect" is set to 1, it is cautious to change the settings in the <MAC>-local.cfg file before importing it.

Scenario Operations:

To export local configuration file via web user interface:

1. Click on **Phone**->**Configuration**.

2. In the **Local Configuration** field, click **Export** to open file download window.

3. Save the 001565221229-local.cfg file to the local system.
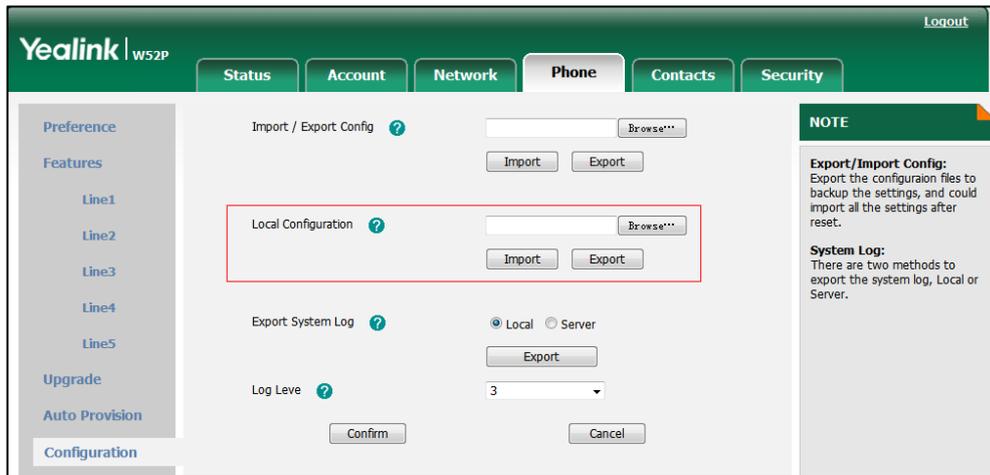
The administrator or user can edit the 001565221229-local.cfg file after exporting.

To import local configuration file via web user interface:

1. Click on **Settings**->**Configuration**.

2. In the **Local Configuration** field, click **Browse** to locate the 001565221229-local.cfg file from your local system.
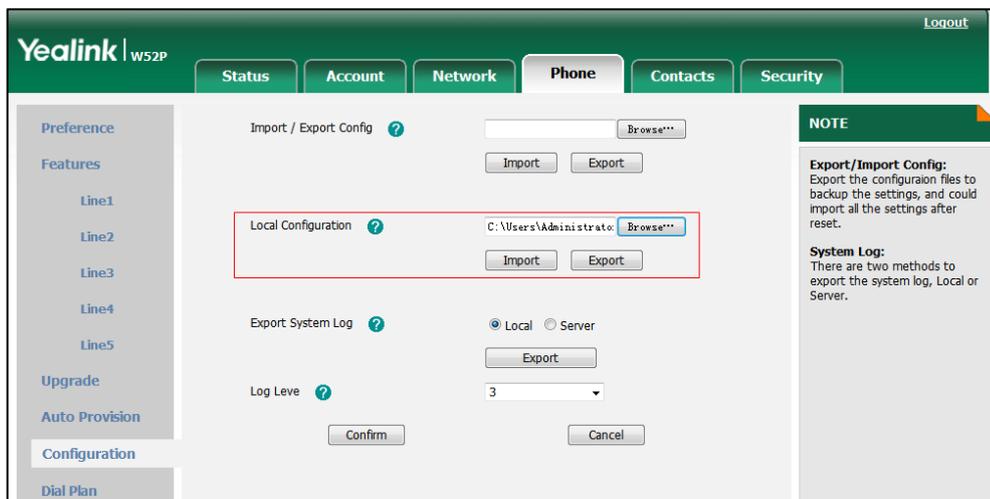
3. Click **Import**.

The web user interface prompts "Upload local configuration succeeded!".
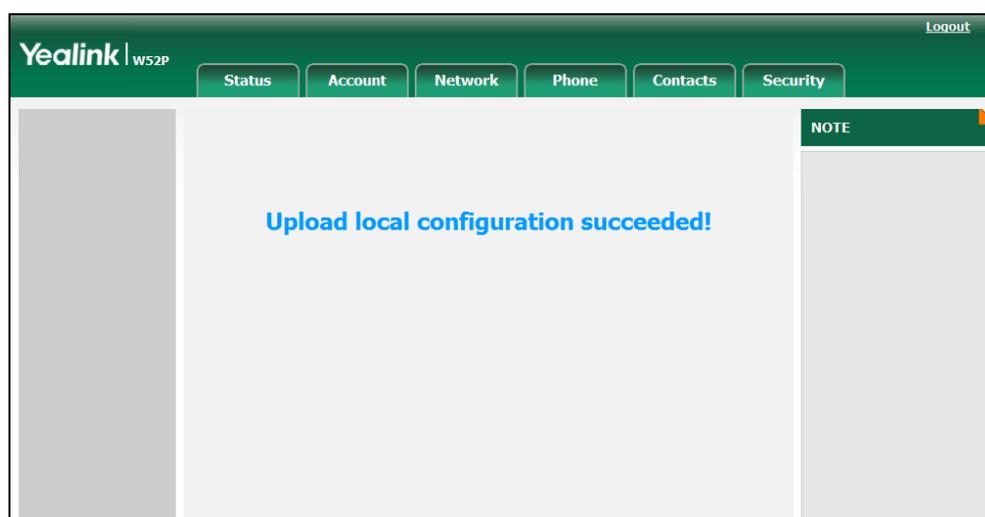
The existing local configuration file will be overridden by the imported one after importing. The configurations in the importing 001565221229-local.cfg file will be saved to the phone flash and take effect.

If the administrator or user deletes the configurations in the 001565221229-local.cfg file and then import the file to the phone, the IP phone will remain the original configurations. But the configurations can be change via next auto provisioning.

> If the value of the parameter "auto_provision.custom.sync" is set to 1, and the 001565221229-local.cfg file is successfully imported, the imported 001565221229-local.cfg file will be uploaded to the provisioning server and overrides the existing one on the server.

Troubleshooting

This chapter provides general troubleshooting information to help you solve problems you might encounter when deploying Yealink W52P IP DECT phones.

If you require additional information or assistance with the deployment, contact your system administrator.

Why does the phone fail to download configuration files?

- Ensure that Auto Provisioning feature is enabled.
- Ensure that the provisioning server or the network is reachable.
- Ensure that authentication credentials configured on the phone are correct.
- Ensure that the configuration files exist on the provisioning server.

Why does the provisioning server return an HTTP 404 error?

- Ensure that the HTTP server is properly set up.
- Ensure that the access URL is correct.
- Ensure that the requested configuration files exist on the HTTP server.

Why the permission is denied when uploading files to an FTP server?

- Ensure that the root directory of the FTP server contains the complete directory path.
- On the provisioning server, check the file permissions, if necessary, change the file permission.
- Contact your system administrator for more information.

Why does the phone display "Network unavailable"?

- Ensure that the Ethernet cable is plugged into the Internet port on the phone and the Ethernet cable is not loose.
- Ensure that the switch or hub in your network is operational.
- Ensure the configurations of network are properly set in the configuration files.

Why does not the phone obtain the IP address from DHCP server?

- Ensure that your settings are right on the DHCP server.
- Ensure your phone is configured to obtain the IP address via DHCP server.
- Contact your system administrator for more information.

Why does not the phone apply the configurations?

- Ensure the phone have downloaded the configuration files.

- Ensure the file header in the configuration file is not deleted.

- Ensure the parameters are correctly set in the configuration files.

- Contact your system administrator for more information.

Appendix

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 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.

Configuring an FTP Server

Wftpd and FileZilla are free FTP application softwares for Windows. This section mainly provides instructions on how to configure an FTP server using wftpd on Windows. You can download wftpd online: http://www.greenxf.com/soft/24769.html.

> We recommend that you use vsftpd as an FTP server for Linux platform if required.

Preparing a Root Directory

To prepare a root directory:

1. Create an FTP root directory on the local system.

2. Place the configuration files to this root directory.

3. Set the security permissions for the FTP directory folder.

   You need to define a user or group name, and set the permissions: read, write, and modify. Security permissions vary by organizations.

   An example of configuration on the Windows platform is shown as below:
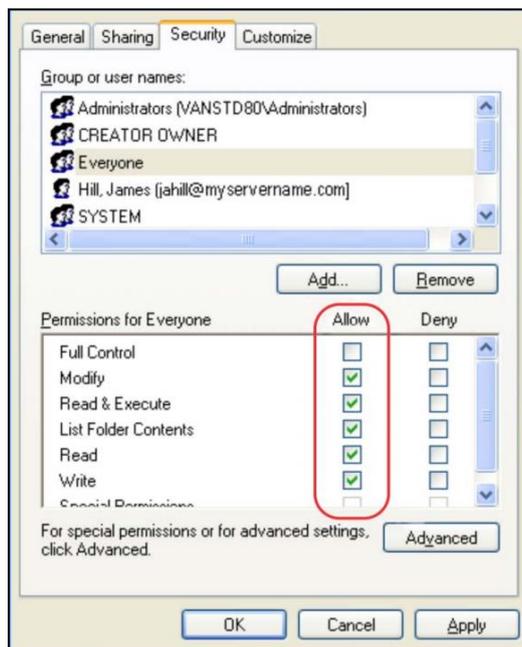
Configuring an FTP Server

Before configuring a wftpd server, ensure that no other FTP servers exist in your local system.

To configure a wftpd server:

1.   Download the compressed file of the wftpd application software to your local system and uncompress it.

2.   Double click the CRYPT.EXE.

3.   Double click the WFTPD.EXE.

     The log file of the wftpd application software is shown as below:
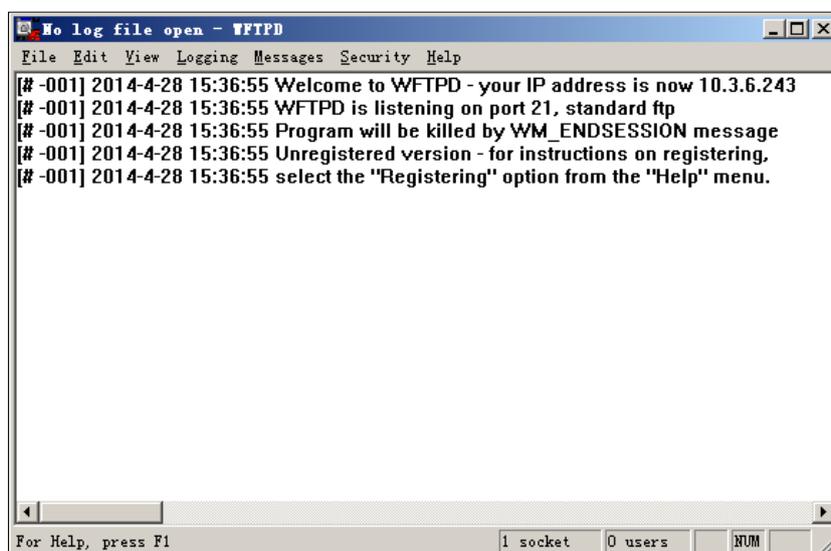
4.   Click **Security->Users/rights**.
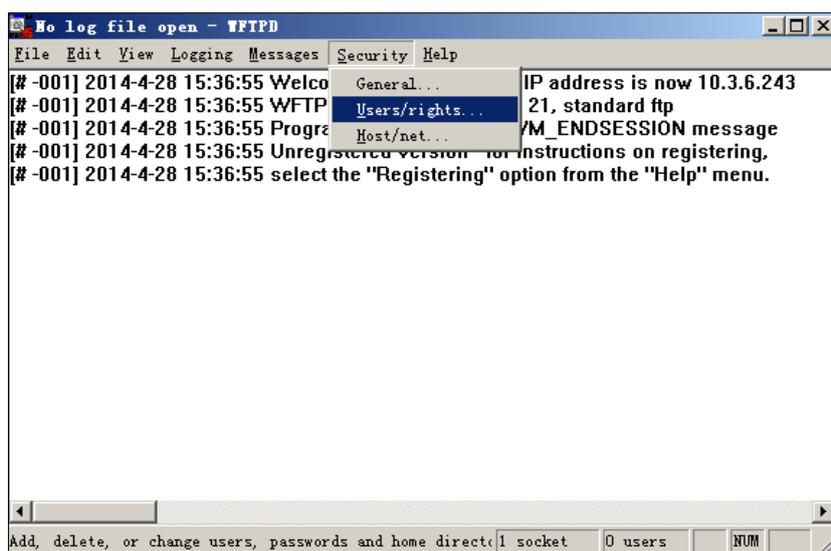
5. Click **New User.**

6. Enter a user name (e.g., test1) in the **User Name** field, and then click **OK**.

7. Enter the password of the user (e.g., test1) created above in the **New Password** and **Verify Password** fields respectively, and then click **OK**.

8. Click **Browse** to locate a directory from your local system as the home directory of the FTP server.

9. Click **Rights>>** and assign the desired permission for the user (e.g., 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 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 downloading. For example, "ftp://test1:123456@10.3.6.234/") is where the IP phone downloads configuration files.

Configuring an HTTP Server

This section shows you how to configure an HTTP server using HFS tool. You can download HFS tool online: http://www.snapfiles.com/get/hfs.html.

To create a root directory:

1. Create a HTTP root directory on the local system.

2. Configure the security permissions for the TFTP directory folder.

   You need to define a user or a group name and set the permissions: read, write, and modify. Security permissions vary by organizations.

   An example of configuration on the Windows platform is shown as below:
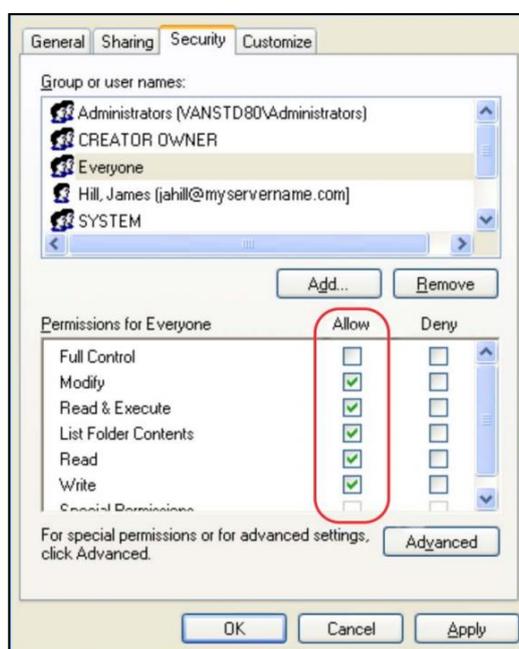
3. Place the configuration files to this root directory.

To configure an HTTP server:

HFS tool is an executable application, so you don't need to install it.

1. Double click the hfs.exe to start the application.

   The main configuration page is shown as below:
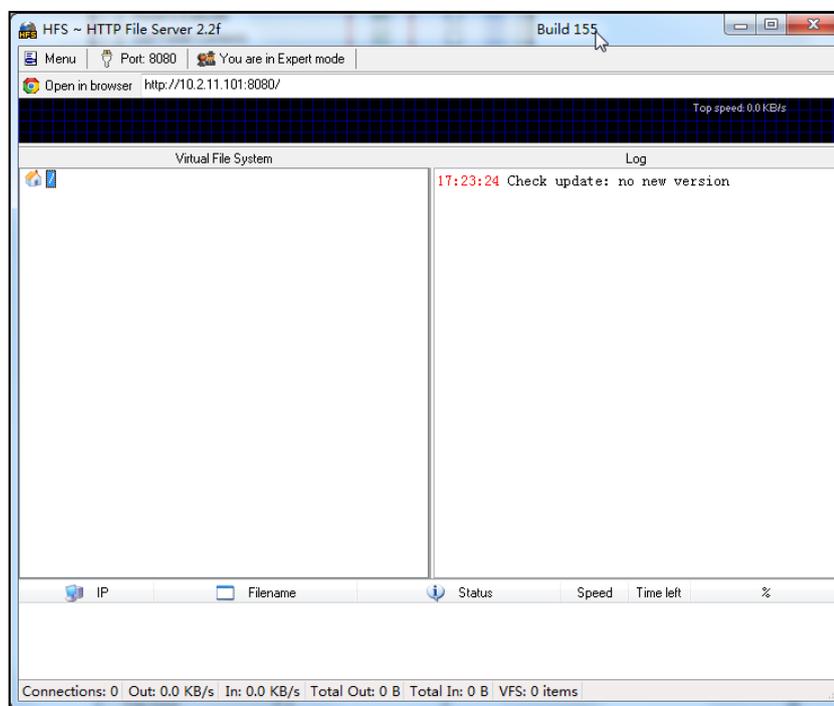
2. Click **Menu** in the main page and select the IP address of the PC from **IP address**.
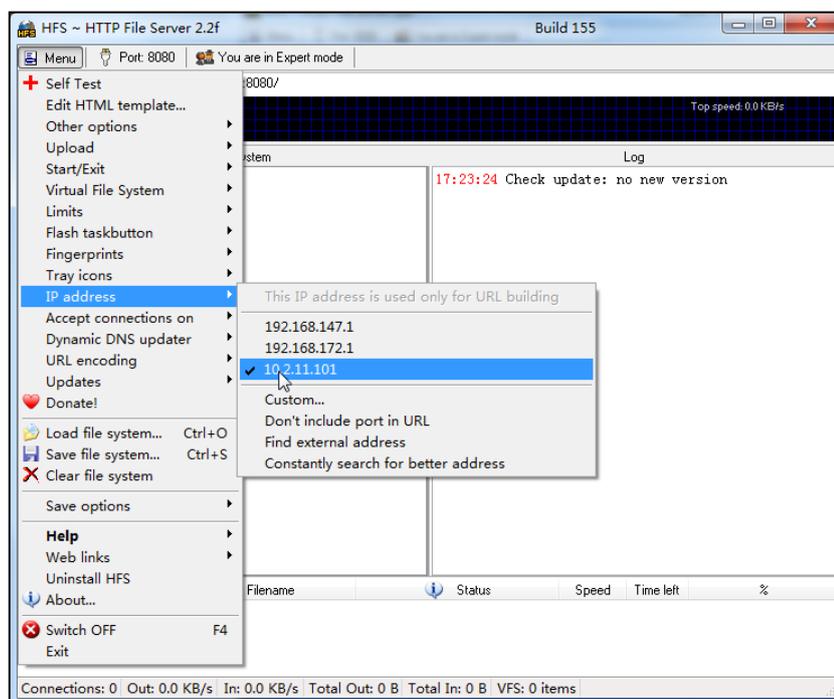
The default HTTP port is 80. You can also reset the HTTP port (make sure there is no port conflict).
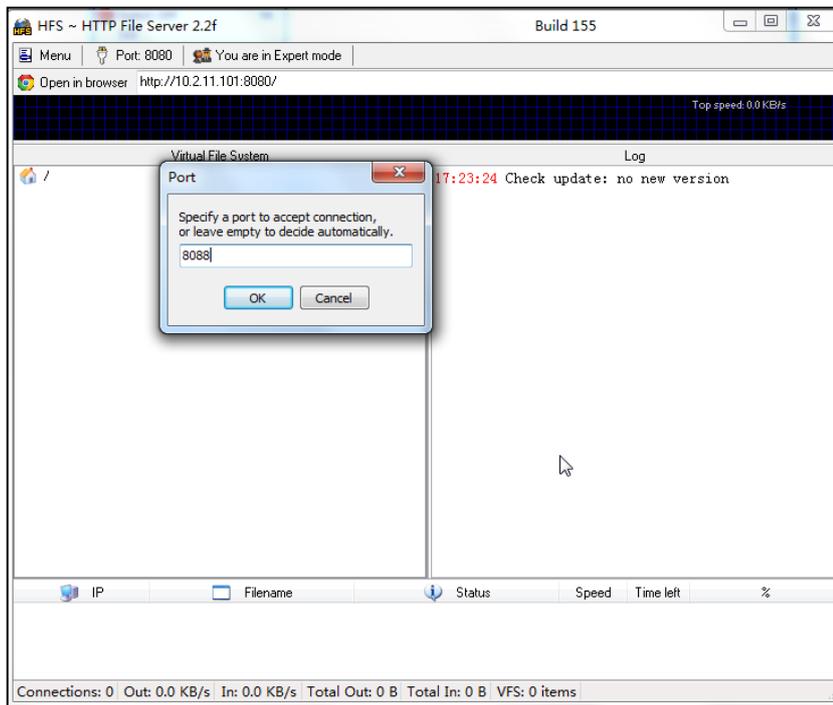
3.   Right click the ![icon] icon on the left of the main page, select **Add folder from disk** to add the HTTP Server root directory.
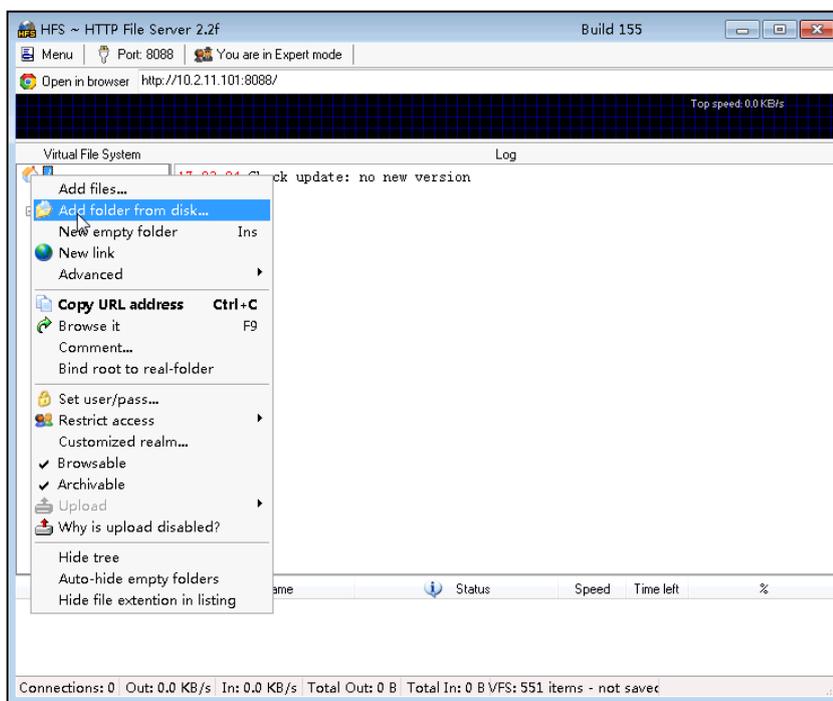
4. Locate the directory of the HTTP server from the local system. Select the kind of folder you want.
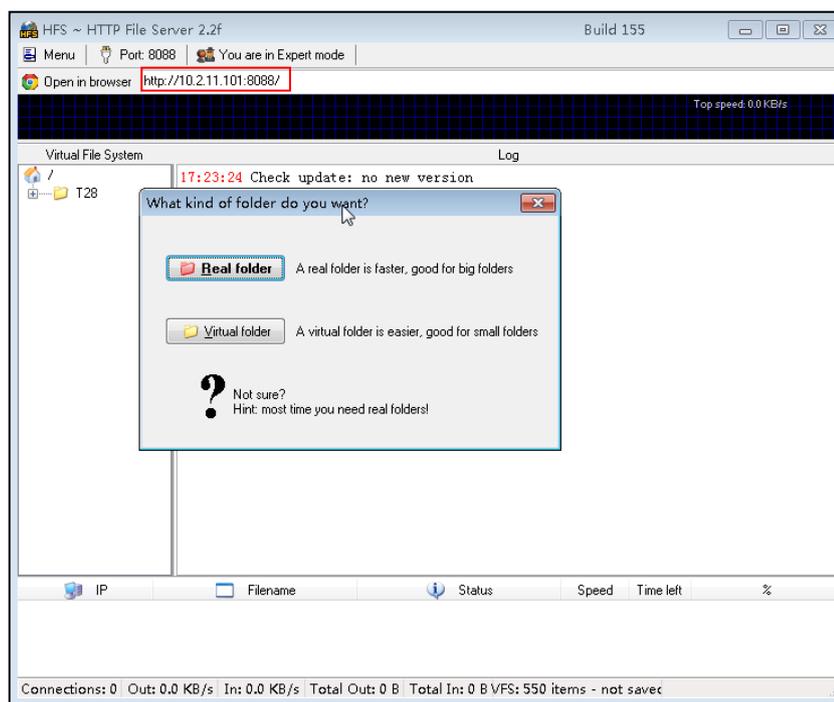
Check the server URL "http:// IP:Port/" in the **"Open in browser"** address bar (For example, the server URL "http:// 10.2.11.101:8088/" is shown on the screenshot) . We recommend that you can fill the server URL in the address bar of the web browser and then press <Enter> key to check if the HTTP server is accessible before provisioning.

> Yealink W52P IP DECT phone also supports the Hypertext Transfer Protocol with SSL/TLS (HTTPS) protocol for auto provisioning. HTTPS protocol provides the encrypted communication and secure identification. For more information on installing and configuring an Apache HTTPS Server, refer to the network resource.

Configuring a DHCP Server

This section provides instructions on how to configure a DHCP server for Windows platform using DHCP Turbo. You can download this software online: http://www.tucows.com/preview/265297 and install it following the setup wizard.

Before configuring the DHCP server, make sure:

● The firewall on the PC is disabled.

● There is no DHCP server in your local system.

To configure a DHCP server:

1. Double click the dhcpt.exe (known as DHCP Turbo) to run the application.
2. Double click **localhost** in the **Servers** sidebar.

3. Leave the **Password** field blank and click the **Login** button.
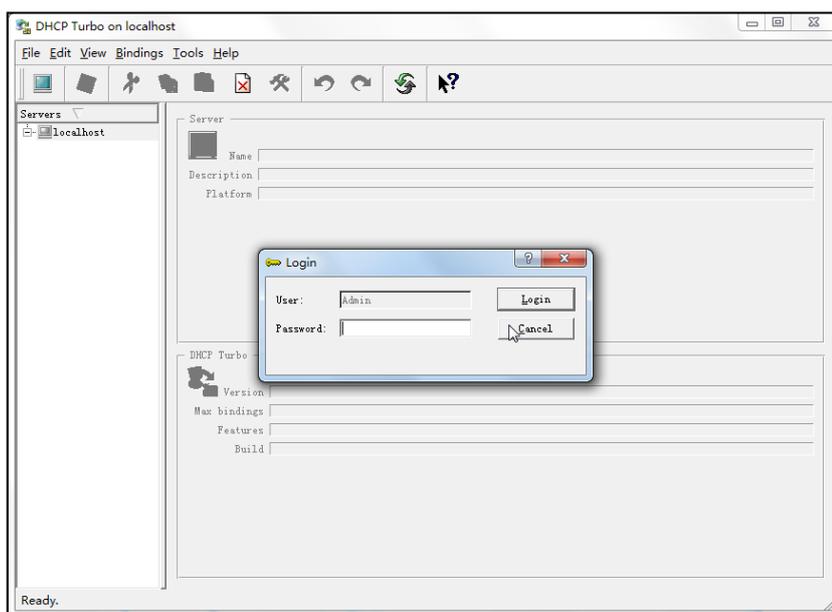
4. Right click **Scopes** under **localhost** and select **New Scope**.

5. Enter the name of the new scope in the **Name** field.

6. Enter valid values in the **Start address**, **End address** and **Subnet Mask** to specify a valid range of IP addresses.

7. Click **OK** to finish the configuration of the new scope.
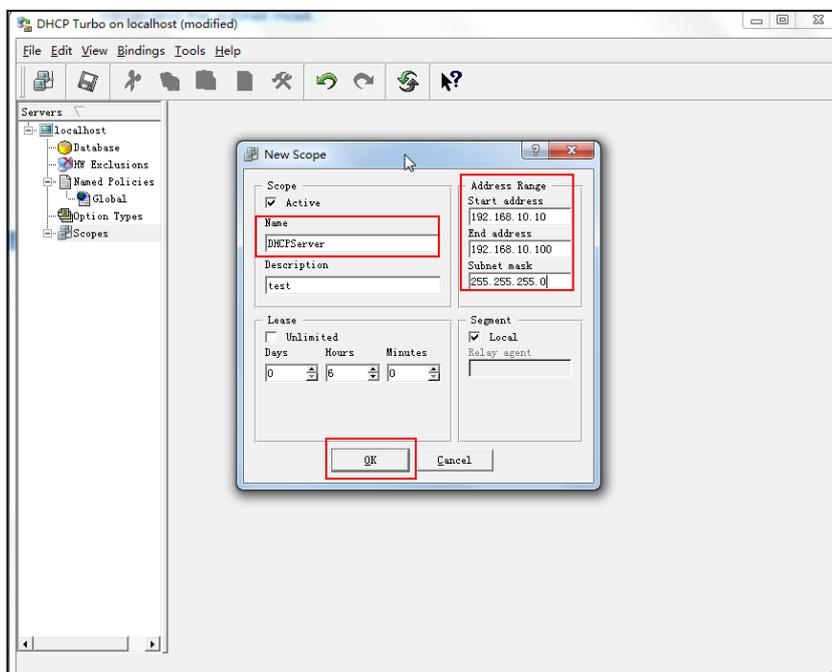
8. Click to accept the change.

To add a custom option via DHCP Turbo:

1. Right click **Option Types** under **localhost** and select **New Option Type**.
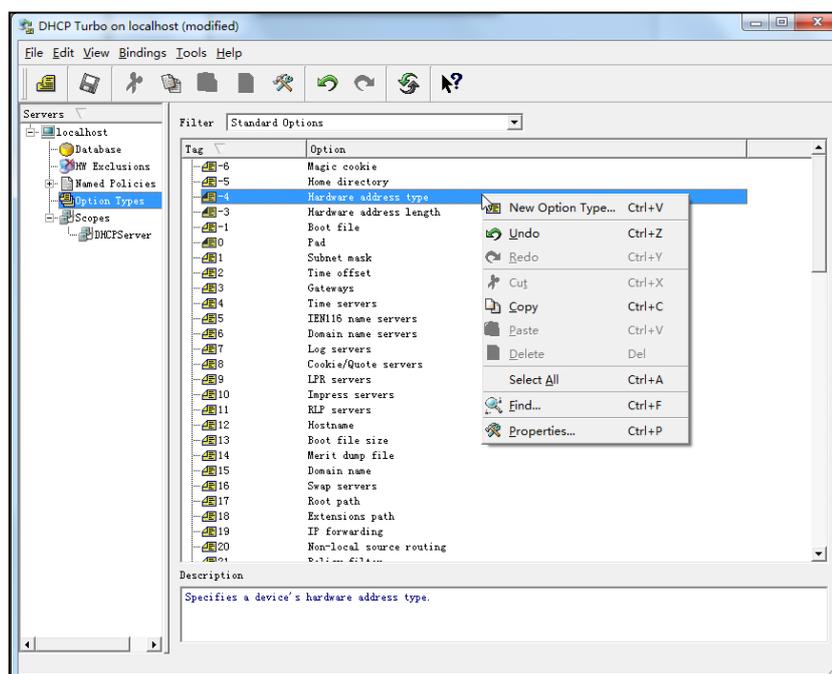
2. Enter the desired tag number of the custom DHCP option in the **Tag** field. For example, 128. Custom DHCP option tag number ranges from 128 to 254.

3. Enter the name of the custom DHCP option in the **Name** field.

4. Select the option type from the pull-down list of **Type**. Commonly, **string** is selected. Yealink W52P IP DECT phones support **string** and **ipaddress** option types only.
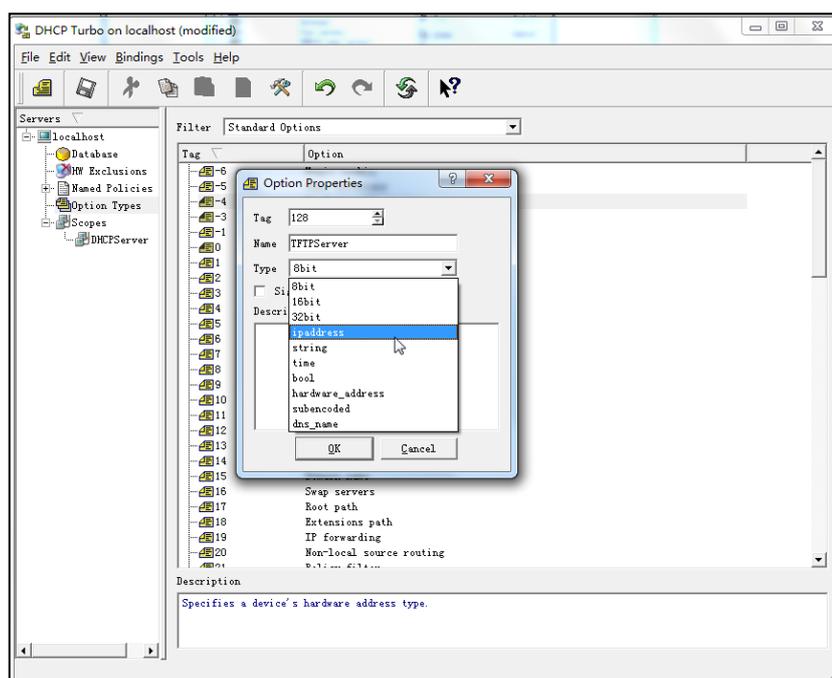
5. Click **OK** to finish setting the option properties.

6. Click [icon] to accept the change.

7. Click **Named Policies->Global**, right click the main page and select **New Option**.
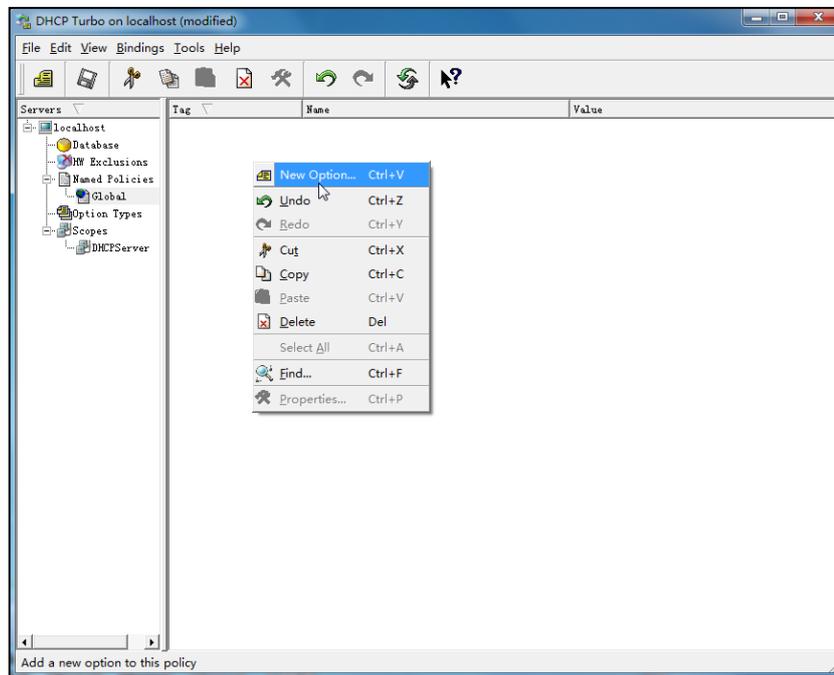
8. Scroll down and double click the custom option **128**.
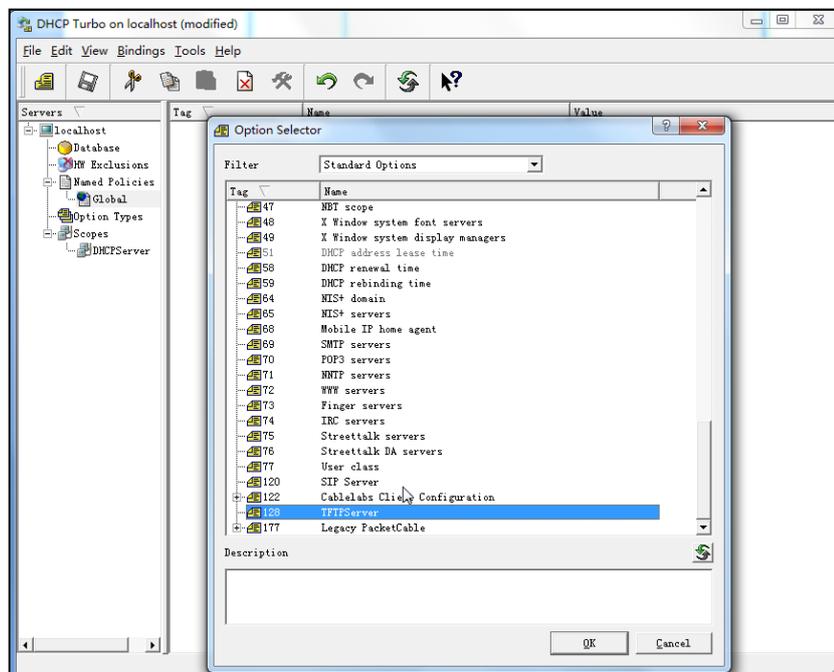
9. Enter the TFTP server address in the input field.

10. Click **OK** to finish setting a custom option.

11. Click ⬚ to accept the change.
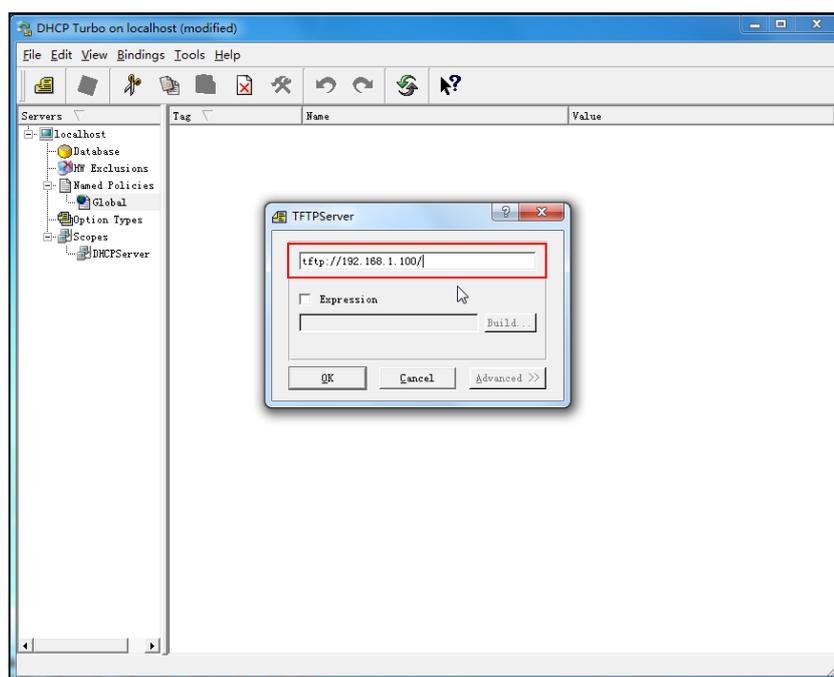
To add the option 66 via DHCP Turbo:

1. Click **Named Policies**->**Global**, right click the main page and select **New Option**.
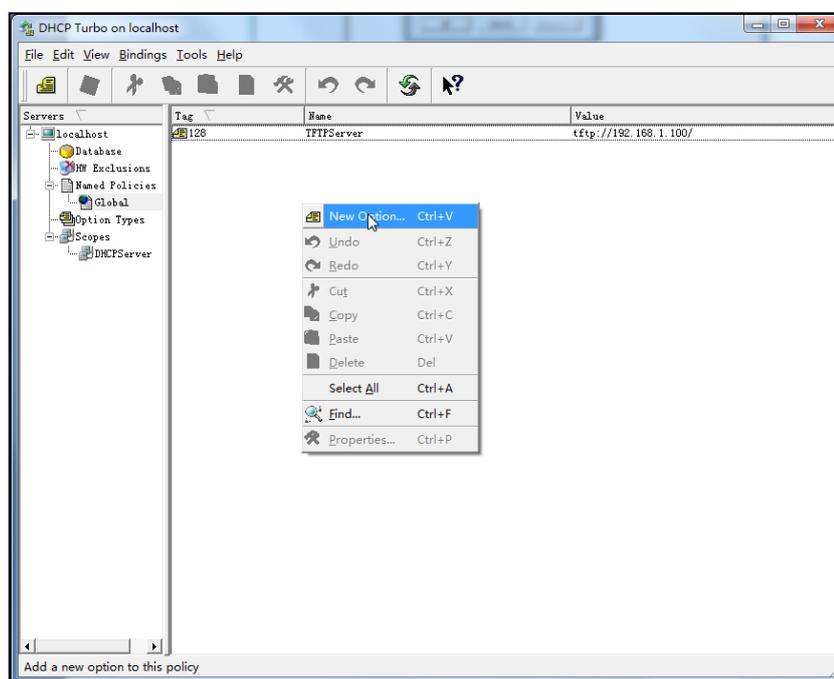
2. Enter **TFTP Options** in the **Filter** field.

3. Double click the option 66.
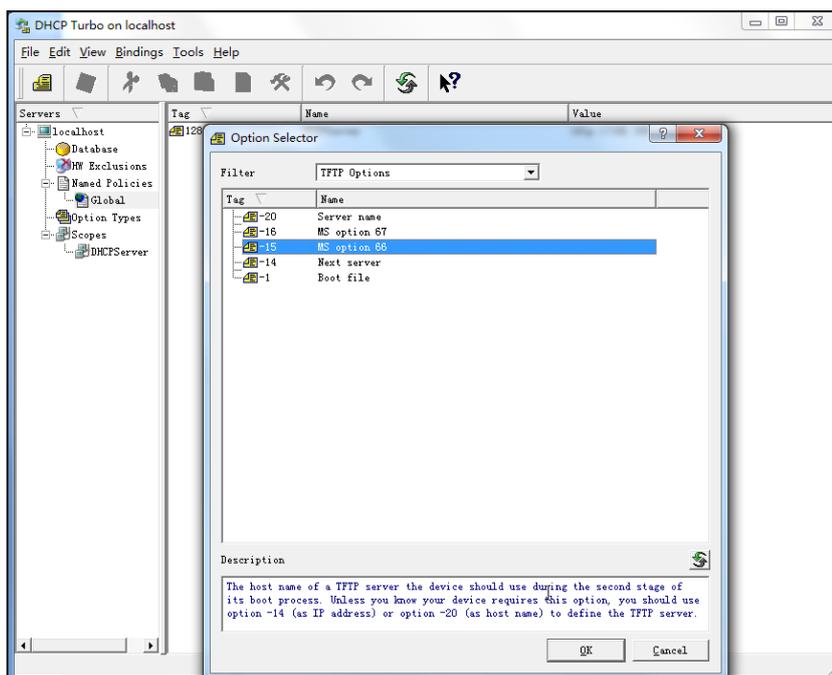
4. Enter the TFTP server address in the input field.
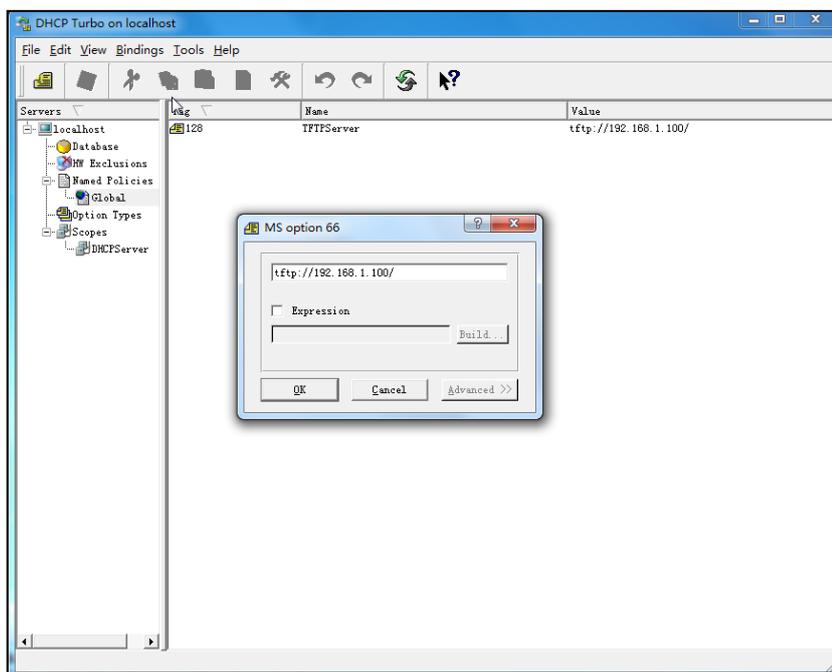
5. Click **OK** to finish setting the option 66.

6. Click ![save icon] to accept the change.

To add the option 43 via DHCP Turbo:

1. Click **Named Policies**->**Global**, right click the main page and select **New Option**.

2. Double click the option 43.
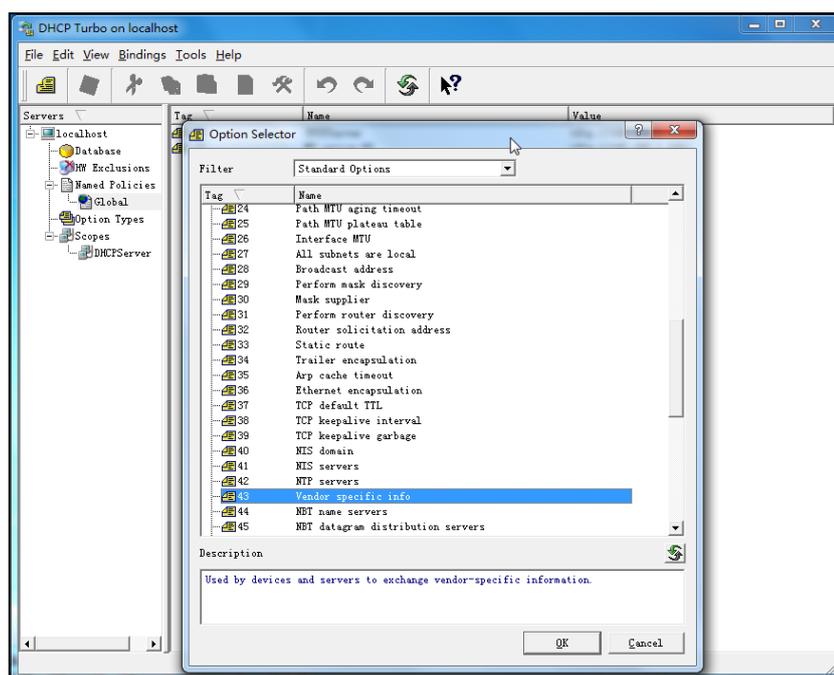
3. Enter the provisioning server address in the input field.
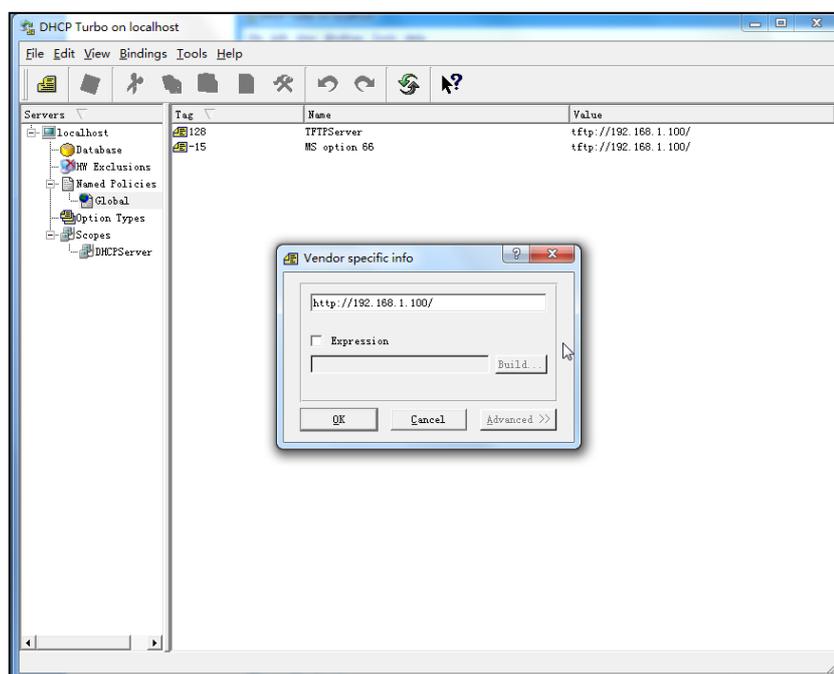
4. Click **OK** to finish setting the option 43.

5. Click ![save icon] to accept the change.

Auto Provisioning Flowchart (Protect personalized settings)

The following shows the auto provisioning flowchart for Yealink W52P IP DECT phones protecting personalized settings of the base station.
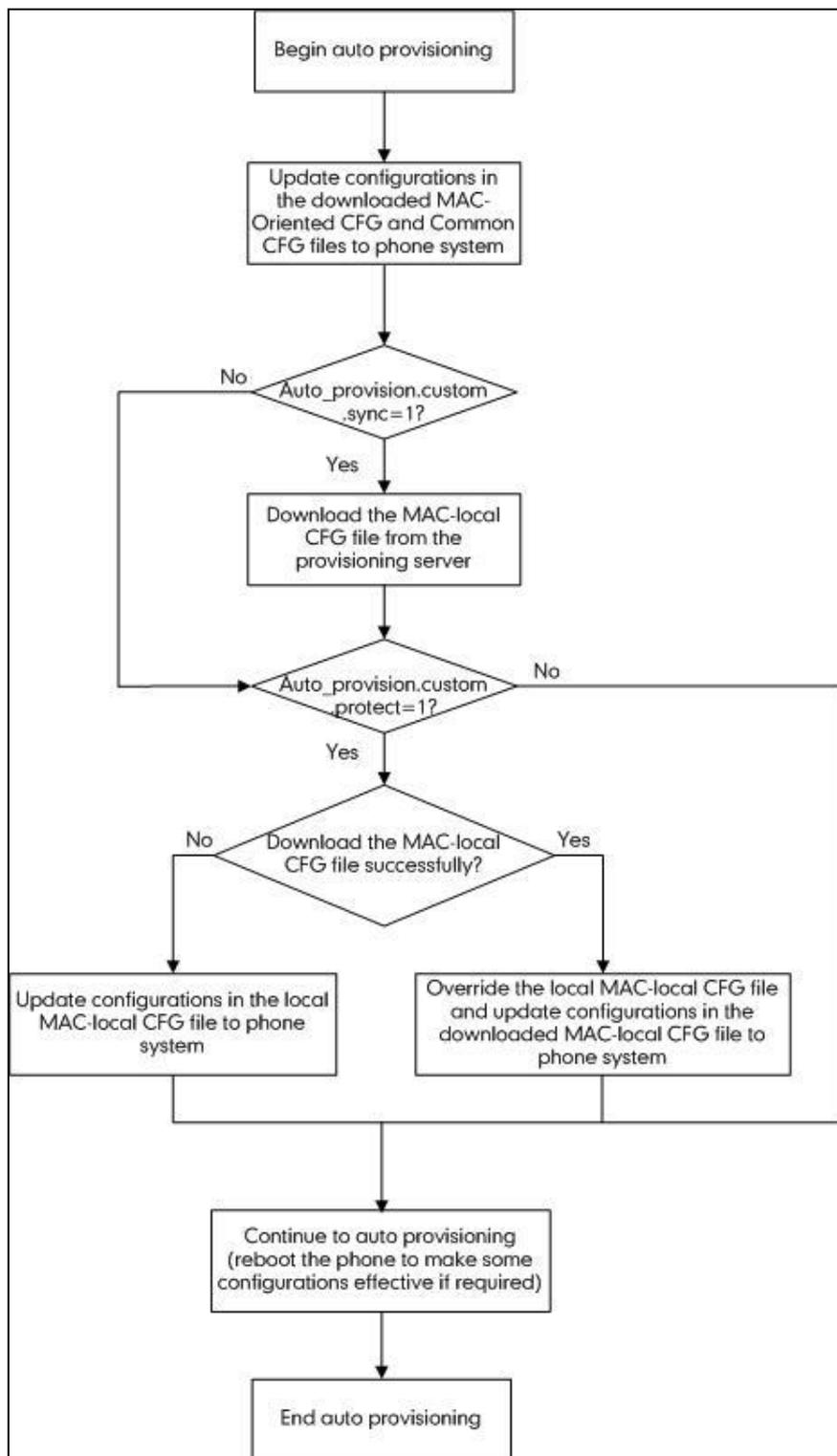
Description of Configuration Parameters in CFG Files

If you want to reset the configuration of a parameter to factory setting, set the value of the parameter to be !NULL! or %NULL%. For example, local_time.ntp_server1 = %NULL%. After the auto provisioning process is completed, the NTP server 1 will be reset to "cn.pool.ntp.org".

Parameter	Permitted Values	Descriptions	Web Setting Path
network.internet_port.type	0, 1 or 2	It configures the Internet (WAN) port type. **0**-DHCP **1**-PPPoE **2**-Static IP Address The default value is 0. It takes effect after a reboot.	Network->Basic
network.static_dns_enable	0 or 1	It enables or disables the IP phone to use manually configured static DNS when the Internet (WAN) port type is configured as DHCP. **0**-Disabled (use the DNS obtained by DHCP) **1**-Enaled If it is set to 1, you need to configure the primary and secondary DNS addresses using the parameter "network.primary_dns" and "network.secondary_dns".	Network->Basic->Static DNS

Parameter	Permitted Values	Descriptions	Web Setting Path
		The default value is 0.	
network.internet_port.ip	IP address	It configures the IP address when the Internet (WAN) port type is configured as Static IP Address. The default value is blank. It takes effect after a reboot.	Network->Basic->Internet Port- Static IP Address->IP Address
network.internet_port.mask	IP address	It configures the subnet mask when the Internet (WAN) port type is configured as Static IP Address. The default value is blank. It takes effect after a reboot.	Network->Basic->Internet Port->Static IP Address- Subnet Mask
network.internet_port.gateway	IP address	It configures the default gateway when the Internet (WAN) port type is configured as Static IP Address. The default value is blank. It takes effect after a reboot.	Network->Basic->Internet Port->Static IP Address->Default Gateway
network.primary_dns	IP address	It configures the primary DNS server when the Internet (WAN) port type is configured as Static IP Address or static DNS feature is enabled. The default value is blank. It takes effect after a reboot.	Network->Basic->Internet Port->Static IP Address->Primary DNS
network.secondary_dns	IP address	It configures the secondary DNS server when the Internet (WAN) port type is configured as Static IP	Network->Basic->Internet Port->Static IP Address->Secondary DNS

Parameter	Permitted Values	Descriptions	Web Setting Path
		Address or static DNS feature is enabled. The default value is blank. It takes effect after a reboot.	
network.pppoe.user	String within 32 characters	It configures the user name for PPPoE connection when the Internet (WAN) port type is configured as PPPoE. The default value is blank. It takes effect after a reboot.	Network->Basic->PPPoE->User
network.pppoe.password	String within 99 characters	It configures the password for PPPoE connection when the Internet (WAN) port type is configured as PPPoE. The default value is blank. It takes effect after a reboot.	Network->Basic->PPPoE->Password
network.vlan.internet_port_enable	0 or 1	It enables or disables VLAN for the Internet (WAN) port. **0**-Disabled **1**-Enabled The default value is 0. It takes effect after a reboot.	Network->Advanced->VLAN->Active

Parameter	Permitted Values	Descriptions	Web Setting Path
network.vlan.internet_port_vid	Integer from 1 to 4094	It configures VLAN ID of the Internet (WAN) port. The default value is 1. It takes effect after a reboot.	Network->Advanced->VLAN->VID
network.vlan.internet_port_priority	Integer from 0 to 7	It configures VLAN priority of the Internet (WAN) port. The default value is 0. 7 is the highest priority. It takes effect after a reboot.	Network->Advanced->VLAN->Priority
network.dhcp_host_name	String within 99 characters	It configures the host name of the IP phone for DHCP option 12. The default value is SIP-W52P. It takes effect after a reboot.	Phone->Features->DHCP Hostname
network.vlan.dhcp_enable	0 or 1	It enables or disables the phone to obtain VLAN settings from the DHCP server. **0**-Disabled **1**-Enabled The default value is 1. It takes effect after a reboot.	Network->Advanced->VLAN->DHCP VLAN ->Active
network.vlan.dhcp_option	Integer from 128 to 254	It configures the DHCP option from which the phone will obtain the VLAN settings. You can configure at most five DHCP options and separate them by commas.	Network->Advanced->VLAN->DHCP VLAN ->Option

Parameter	Permitted Values	Descriptions	Web Setting Path
		The default value is 132. It takes effect after a reboot.	
wui.https_enable	0 or 1	It enables or disables the phone to use HTTPS protocol for access of the web user interface. **0**-Disabled **1**-Enabled The default value is 1. It takes effect after a reboot.	Network->Advanced->Web Server Type->HTTPS
wui.http_enable	0 or 1	It enables or disables the phone to use HTTP protocol for access of the web user interface. **0**-Disabled **1**-Enabled The default value is 1. It takes effect after a reboot.	Network->Advanced->Web Server Type->HTTP
network.port.http	Integer from 1 to 65535	It configures the HTTP port of the web server access. The default value is 80. It takes effect after a reboot.	Network->Advanced->Web Server Type->HTTP Port
network.port.https	Integer from 1 to 65535	It configures the HTTPS port of the web server access.	Network->Advanced->Web Server Type->HTTPS Port

Parameter	Permitted Values	Descriptions	Web Setting Path
		The default value is 443. It takes effect after a reboot.	
network.port.max_rtpport	Integer from 1 to 65535	It configures the maximum local RTP port. The default value is 12780. It takes effect after a reboot.	Network->Advanced->Local RTP Port-> Maximum RTP Port
network.port.min_rtpport	Integer from 1 to 65535	It configures the minimum local RTP port. The default value is 11780. It takes effect after a reboot.	Network->Advanced->Local RTP Port-> Minimum RTP Port
network.qos.rtptos	Integer from 0 to 63	It configures the voice QoS. The default value is 46. It takes effect after a reboot.	Network->Advanced->Voice QoS->Voice QoS
network.qos.signaltos	Integer from 0 to 63	It configures the SIP QoS. The default value is 26. It takes effect after a reboot.	Network->Advanced->Voice QoS->SIP Qos
network.802_1x.mode	0, 1, 2 or 3	It configures the 802.1x authentication mode. **0**-Disabled **1**- EAP-MD5 **2**-EAP-PEAP/GTC	Network->Advanced->802.1x->802.1x Mode

Parameter	Permitted Values	Descriptions	Web Setting Path
		3-EAP-TTLS/EAP-GTC The default value is 0. It takes effect after a reboot.	
network.802_1x.identity	String within 32 characters	It configures the user name for 802.1x authentication. The default value is blank. It takes effect after a reboot. **Note:** It works only if the value of the parameter "network.802_1x.mode" is set to 1, 2, 3.	Network-> Advanced->802.1x->Identity
network.802_1x.md5_password	String within 32 characters	It configures the password for 802.1x authentication. The default value is blank. It takes effect after a reboot. **Note:** It works only if the value of the parameter "network.802_1x.mode" is set to 1, 2, 3.	Network->Advanced->802.1x->MD5 Password
network.802_1x.client_cert_url	URL within 511 characters	It configures the access URL of the CA certificate when the 802.1x authentication method is configured as EAP-PEAP/GTC or EAP-TTLS/EAP-GTC. The default value is blank. It takes effect after a reboot. **Note:** The format of the certificate must be *.pem, *.crt, *.cer or *.der.	Network->Advanced->802.1x->CA Certificate

Parameter	Permitted Values	Descriptions	Web Setting Path
		It works only if the value of the parameter "network.802_1x.mode" is set to 2, 3.	
network.vpn_enable	0 or 1	It enables or disables VPN feature. **0**-Disabled **1**-Enabled The default value is 0. It takes effect after a reboot.	Network-> Advanced->VPN->Active
openvpn.url	URL within 511 characters	It configures the access URL of the openVPN tar file.	Network->Advanced->VPN->Upload VPN Config
network.lldp.enable	0 or 1	It enables or disables LLDP feature. **0**-Disabled **1**-Enabled The default value is 1. It takes effect after a reboot.	Network->Advanced->LLDP->Active
network.lldp.packet_interval	Integer from 1 to 3600	It configures the interval (in seconds) the phone broadcasts the LLDP request. The default value is 60. It takes effect after a reboot.	Network->Advanced->LLDP->Packet Interval

Parameter	Permitted Values	Descriptions	Web Setting Path
sip.reg_surge_prevention	Integer from 0 to 60	It configures the maximum duration (in seconds) for account register after startup. The default value is 0.	Network->Advanced->Registration random
sip.send_response_by_request	0 or 1	It configures from where the IP phone retrieves the destination address for response. The IP phone will then send all SIP response messages to the destination address. **0**-from VIA header in the request message **1**-from source address of the request message The default value is 1. It takes effect after a reboot.	
sip.notify_reboot_enable	0, 1or 2	It configures the phone behavior when the IP phone receives a SIP NOTIFY message containing the header "Event: check-sync". **0**-The IP phone will reboot only if the SIP NOTIFY message contains an additional string "reboot=true". **1**-The IP phone will be forced to reboot. **2**-The IP phone will ignore the SIP NOTIFY message. The default value is 1.	

Parameter	Permitted Values	Descriptions	Web Setting Path
sip.use_23_as_pound	0 or 1	It enables or disables the IP phone to reserve the pound sign when dialing out. **0**-Disabled (convert the pound sign into "%23") **1**-Enabled The default value is 1.	
sip.rfc2543_hold	0 or 1	It enables or disables the IP phone to use RFC 2543 (c=0.0.0.0) outgoing hold signaling. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), SDP media direction attributes (such as a=sendonly) per RFC 3264 is used when placing a call on hold. If it is set to 1 (Enabled), SDP media connection address c=0.0.0.0 per RFC 2543 is used when placing a call on hold. The default value is 0.	Phone->Features->RFC 2543 Hold
syslog.mode	0 or 1	It configures the phone to export log files to a syslog server or the local system. **0**-Local **1**-Server	Phone->Configuration->Export System Log

Parameter	Permitted Values	Descriptions	Web Setting Path
		The default value is 0. It takes effect after a reboot.	
syslog.server	IP address or domain name	It configures the IP address or domain name of the syslog server where to export log files of the IP phone. It takes effect only if the value of the parameter "syslog.mode" is configured as 1 (Server). The default value is blank. It takes effect after a reboot.	Phone->Configuration->Server Name
syslog.log_level	Integer from 0 to 6	It configures the detail level of syslog information to be exported. **0**: system is unusable **1**: action must be taken immediately **2**: critical condition **3**: error conditions **4**: warning conditions **5**: normal but significant condition **6**: informational The default value is 3. It takes effect after a reboot.	Phone->Configuration->Log Level

Parameter	Permitted Values	Descriptions	Web Setting Path
voice.vad	0 or 1	It enables or disables VAD (Voice Activity Detection) feature on the phone. **0**-Disabled **1**-Enabled The default value is 0.	Phone->Voice->Echo Cancellation->VAD
voice.echo_cancellation	0 or 1	It enables or disables AEC (Acoustic Echo Canceller) feature on the phone. **0**-Disabled **1**-Enabled The default value is 1.	
voice.cng	0 or 1	It enables or disables CNG (Comfortable Noise Generation) feature on the phone. **0**-Disabled **1**-Enabled The default value is 1.	Phone->Voice->Echo Cancellation->CNG
voice.jib.adaptive	0 or 1	It configures the type of jitter buffer. **0**-Fixed **1**-Adaptive The default value is 1.	Phone->Voice->Jitter Buffer->Type

Parameter	Permitted Values	Descriptions	Web Setting Path
voice.jib.min	Integer	It configures the minimum delay (in milliseconds) of jitter buffer. The default value is 0.	Phone->Voice->Jitter Buffer->Minimum Delay
voice.jib.max	Integer	It configures the maximum delay (in milliseconds) of jitter buffer. The default value is 300.	Phone->Voice->Jitter Buffer->Maximum Delay
voice.jib.normal	Integer	It configures the normal delay (in milliseconds) of jitter buffer. The default value is 120.	Phone->Voice->Jitter Buffer->Nominal
auto_provision.reboot_force.enable	0 or 1	It enables or disables the IP phone to reboot after auto provisioning even though there is no specific configuration requiring reboot in configuration files. **0**-Disabled **1**-Enabled The default value is 0. **Note**: It works only for the current auto provisioning process. If you want the IP phone to reboot after every auto provisioning process, the parameter must be always contained in the configuration file and set to 1.	

Parameter	Permitted Values	Descriptions	Web Setting Path
auto_provision.power_on	0 or 1	It triggers the Power On feature to on or off. If it is set to 1(On), the phone will perform an auto provisioning process when powered on. **0**-Off **1**-On The default value is 1. **Note**: The old parameter "auto_provision.mode" is also applicable to the IP phone.	Phone->Auto Provision->Check New Config
auto_provision.pnp_enable	0 or 1	It triggers the Plug and Play feature to on or off. If it is set to 1(On), the phone will broadcast PnP SUBSCRIBE messages to obtain a provisioning server address during startup. **0**-Off **1**-On The default value is 1.	Phone->Auto Provision->PNP
auto_provision.repeat.enable	0 or 1	It triggers the Repeatedly feature to on or off. If it is set to 1(On), the phone will check new configuration repeatedly. **0**-Off **1**-On	Phone->Auto Provision->Repeatedly

Parameter	Permitted Values	Descriptions	Web Setting Path
		The default value is 0.	
auto_provision.repeat.minutes	Integer from 1 to 43200	It configures the interval (in minutes) for the phone to check the new configuration repeatedly. The default value is 60. **Note:** It works only if the value of the parameter "auto_provision.repeat.enable" is set to 1 (On).	Phone->Auto Provision->Interval(Minutes)
auto_provision.weekly.enable	0 or 1	It triggers the Weekly feature to on or off. If it is set to 1(On), the phone will check the new configuration weekly. **0**-Off **1**-On The default value is 0.	Phone->Auto Provision->Weekly
auto_provision.weekly.dayofweek	0, 1, 2, 3, 4, 5, 6 or a combination of these digits	It configures the days of week for the phone to check the new configuration weekly. **Example**: auto_provision.weekly.dayofweek = 01 This means that the phone will check new configuration every Sunday and Monday. The default value is 0123456.	Phone->Auto Provision->Day of Week

Parameter	Permitted Values	Descriptions	Web Setting Path
		Note: The old parameter "auto_provision.weekly.mask" is also applicable to the IP phone.	
auto_provision.weekly.begin_time	Time from 00:00 to 23:59	It configures the begin time of the day for the phone to check the new configuration weekly. The default value is 00:00. **Note**: It works only if the value of the parameter "auto_provision.weekly.enable" is set to 1(On).	Phone->Auto Provision->Time
auto_provision.weekly.end_time	Time from 00:00 to 23:59	It configures the end time of the day for the phone to check the new configuration weekly. The default value is 00:00. **Note**: It works only if the value of the parameter "auto_provision.weekly.enable" is set to 1(On).	Phone->Auto Provision->Time
auto_provision.server.url	URL within 511 characters	It configures the URL of the auto provisioning server. The default value is blank.	Phone->Auto Provision->Provisioning Server
auto_provision.server.username	String within 32 characters	It configures the user name for authentication during auto provisioning. The default value is blank.	Phone->Auto Provision->User Name
auto_provision.server.password	String within 32	It configures the password for authentication during	Phone->Auto Provision->Password

Parameter	Permitted Values	Descriptions	Web Setting Path
	characters	auto provisioning. The default value is blank.	
auto_provision.dhcp_option.enable	0 or 1	It triggers the DHCP Option feature to on or off. If it is set to 1(On), the phone will obtain the provisioning server address by detecting DHCP options. **0**-Off **1**-On The default value is 1.	Phone->Auto Provision->DHCP Option
auto_provision.dhcp_option.option60_value	String within 99 characters	It configures the value (vendor name of the device) of DHCP option 60. The default value is yealink.	Phone->Auto Provision->DHCP Option 60
auto_provision.dhcp_option.list_user_options	Integer from 128 to 254	It configures the custom DHCP option number for the provisioning server address. The default value is blank.	Phone->Auto Provision->Custom Option (128~254)
auto_provision.aes_key_in_file	0 or 1	It enables or disables the phone to decrypt configuration files using the encrypted AES keys. **0**-Disabled **1**-Enabled If it is set to 1, the phone will download	

Parameter	Permitted Values	Descriptions	Web Setting Path
		<y000000000025_Security>.enc and <MAC_Security>.enc files during auto provisioning, and then decrypts these files into the plaintext keys (e.g., key2, key3) respectively using the phone built-in key (e.g., key1). The phone then decrypts the encrypted configuration files using corresponding key (e.g., key2, key3). If it is set to 0 (Disabled), the IP phone will decrypt the encrypted configuration files using plaintext AES keys configured on the IP phone. The default value is 0. For more information, refer to *Yealink Configuration Encryption Tool User Guide*.	
auto_provision.update_file_mode	0 or 1	Enables or disables the phone to update encrypted configuration settings only during auto provisioning. **0**-Disabled **1**-Enabled The default value is 0. For more information, refer to *Yealink Configuration Encryption Tool User Guide*.	
auto_provision.aes_key_16.com	16 characters	It configures the AES key for decrypting the Common CFG file.	Phone->Auto Provision->Common AES Key

Parameter	Permitted Values	Descriptions	Web Setting Path
		The valid characters contain: 0 ~ 9, A ~ Z, a ~ z,#$%*+,-.:=?@[]^_{}~. **Example:** auto_provision.aes_key_16.com = 0123456789abcdef The default value is blank. **Note**: It works only if the value of the parameter "auto_provision.aes_key_in_file" is set to 0 (Disabled). For more information, refer to *Yealink Configuration Encryption Tool User Guide*.	
auto_provision.aes_key_16.mac	16 characters	It configures the AES key for decrypting the MAC-Oriented CFG file. The valid characters contain: 0 ~ 9, A ~ Z, a ~ z,#$%*+,-.:=?@[]^_{}~. The default value is blank. **Note**: It works only if the value of the parameter "auto_provision.aes_key_in_file" is set to 0 (Disabled). **Example:** auto_provision.aes_key_16.mac = 0123456789abmins	Phone->Auto Provision->MAC_Oriented AES Key

Parameter	Permitted Values	Descriptions	Web Setting Path
		For more information, refer to *Yealink Configuration Encryption Tool User Guide*.	
auto_provision.custom.protect	0 or 1	It enables or disables the IP phone to protect personalized settings after auto provisioning. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), personalized settings of the base station configured via the handset or web user interface will be reserved after auto provisioning. The default value is 0.	
auto_provision.custom.sync	0 or 1	It enables or disables the IP phone to periodically (every 5 minutes) upload the <MAC>-local.cfg file to the provisioning server and download the <MAC>-local.cfg file from the provisioning server during auto provisioning. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will periodically upload the MAC-local CFG file to the provisioning server. During auto provisioning, the IP phone will download the MAC-local CFG file from the	

Parameter	Permitted Values	Descriptions	Web Setting Path
		provisioning server. If it is set to 0 (Disabled), the IP phone will not upload the MAC-local CFG file to the provisioning server. During auto provisioning, the IP phone will not download the MAC-local CFG file from the provisioning server. The default value is 0.	
auto_provision.custom.upload_method	0 or 1	It configures the way the IP phone uploads the MAC-local CFG file to the provisioning server (for HTTP(S) server only). **0**-PUT **1**-POST The default value is 0. **Note:** It works only if the value of the parameter "auto_provision.custom.sync" is set to 1 (Enabled).	
auto_provision.handset_configured.enable	0 or 1	It enables or disables the phone to change the local handset settings via auto provisioning. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the local handset settings	

Parameter	Permitted Values	Descriptions	Web Setting Path
		can be only changed via the handset. If it is set to 1 (Enabled) and the parameter "auto_provision.custom.protect" is set to 0 (Disabled), the locally personalized handset settings will be overridden and other local handset settings can be changed via auto provisioning, or the base station will deliver the stored handset settings to the handset after handset reboot or registration. If it is set to 1 (Enabled) and the parameter "auto_provision.custom.protect" is set to 1 (Enabled), the locally personalized handset settings will not be overridden after auto provisioning, handset reboot or registration. But other local handset settings can be changed. The default value is 0.	
auto_provision.url_wildcard.pn	String within 32 characters	It configures the characters to replace the wildcard $PN in the received URL of the provisioning server. The default value is W52P. **Note**: The configured characters must be in accordance with the actual directory name of the provisioning server.	

Parameter	Permitted Values	Descriptions	Web Setting Path
autoprovision.X.name (X ranges from 1 to 50.)	String within 100 characters	It configures the name of the activation code for triggering auto provisioning. The maximum length of the name is 100 characters. The default value is blank. It takes effect after a reboot.	
autoprovision.X.code (X ranges from 1 to 50.)	String within 24 characters	It configures the activation code to trigger auto provisioning. The activation code must be a combination of numeric characters and special characters # *. The default value is blank. It takes effect after a reboot.	
autoprovision.X.url (X ranges from 1 to 50.)	URL within 511 characters	It configures the URL of provisioning server. The default value is blank. It takes effect after a reboot.	
autoprovision.X.user (X ranges from 1 to 50.)	String within 64 characters	It configures the authentication user name for provisioning server access for auto provisioning via activation code. The default value is blank. It takes effect after a reboot.	
autoprovision.X.password	String within	It configures the password for authentication during	

Parameter	Permitted Values	Descriptions	Web Setting Path
(X ranges from 1 to 50.)	32 characters	auto provisioning. The default value is blank. It takes effect after a reboot.	
autoprovision.X.com_aes (X ranges from 1 to 50.)	16 characters	It configures the AES key for decrypting the Common CFG file. The default value is blank. It takes effect after a reboot.	
autoprovision.X.mac_aes (X ranges from 1 to 50.)	16 characters	It configures the AES key for decrypting the MAC-Oriented CFG file. The default value is blank. It takes effect after a reboot.	
sip.rfc2543_hold	0 or 1	It enables or disables the phone to support RFC 2543 hold (c=0.0.0.0). **0**-Disabled **1**-Enabled The default value is 0.	Phone->Features->RFC 2543 Hold
sip.use_out_bound_in_dialog	0 or 1	It enables or disables the phone to keep sending SIP messages to the outbound server in a dialog. **0**-Disabled **1**-Enabled	Phone->Features->Use Outbound Proxy in Dialog

Parameter	Permitted Values	Descriptions	Web Setting Path
		If it is set to 1 (Enabled), all the SIP request messages from the IP phone will be forced to send to the outbound proxy server in a dialog. The default value is 1.	
transfer.semi_attend_tran_enable	0 or 1	It enables or disables the transfer-to party's phone not to prompt a missed call on the LCD screen before displaying the caller ID when completing a semi-attended transfer. **0**-Disabled **1**-Enabled The default value is 1.	Phone->Features->Semi-Attended Transfer
transfer.blind_tran_on_hook_enable	0 or 1	It enables or disables the phone to complete the blind transfer through on-hook. **0**-Disabled **1**-Enabled The default value is 0.	Phone->Features->Blind Transfer On Hook
transfer.on_hook_trans_enable	0 or 1	It enables or disables the phone to complete the attended transfer through on-hook. **0**-Disabled **1**-Enabled	Phone->Features->Attend Trans OnHook

Parameter	Permitted Values	Descriptions	Web Setting Path
		The default value is 0.	
features.intercom.headset_prior.enable	0 or 1	It configures the channel mode when an incoming intercom call is answered through the handset. The headset should be connected in advance. **0**-Speaker Mode **1**-Headset Mode The default value is 0.	
features.dtmf.hide	0 or 1	It enables or disables the IP phone to suppress the display of DTMF digits. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the DTMF digits are displayed as asterisks. The default value is 0.	Phone->Features->Suppress DTMF Display
features.dtmf.hide_delay	0 or 1	It enables or disables the IP phone to display the DTMF digits for a short period before displaying asterisks. **0**-Disabled **1**-Enabled	Phone->Features->Suppress DTMF Display Delay

Parameter	Permitted Values	Descriptions	Web Setting Path
		The default value is 0.	
lang.wui	English, Turkish, Portuguese, Spanish, Italian, French, Deutsch, Polski, Czech or Russian	It configures the language of the web user interface.	Phone->Preference->Web Language
local_time.time_zone	From -12 to +13 (in increments of 30 minutes), +5:45 or +12:45	It configures the time zone. The default value is +8. **Example**: local_time.time_zone = +9:30 For more available time zones, refer to Time Zones on page 169.	Phone->Preference->Time Zone
local_time.time_zone_name	String within 32 characters	It configures the time zone name. The default time zone name is China(Beijing). The available time zone names depend on the time zone configured by the parameter "local_time.time_zone". For more information on the	Phone->Preference->Location

Parameter	Permitted Values	Descriptions	Web Setting Path
		available time zone names for each time zone, refer to Time Zones on page 169. **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 2 (Automatic) and the parameter "local_time.time_zone" should be configured in advance.	
local_time.ntp_server1	Domain name or IP address	It configures the domain name or IP address of the NTP server 1. The default value is cn.pool.ntp.org.	Phone->Preference->Time Server
local_time.ntp_server2	Domain name or IP address	It configures the domain name or IP address of the NTP server 2. The default value is time.windows.com.	
custom.handset.language	Integer from 0 to 11	It configures the language of the handset. **0**-English **1**-French **2**-Deutsch **3**-Italian **4**-Polski **5**-Portuguese **6**-Spanish **7**-Turkish **8**-Czech	

Parameter	Permitted Values	Descriptions	Web Setting Path
		9-Svenska **10**-Hebrew **11**-Russian The default value is 0. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	
custom.handset.date_format	0, 1, 2, 3, 4, 5 or 6	It configures the 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 The default value is 0. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	
local_time.interval	Integer from 60 to 86400	It configures the interval (in seconds) for the phone to synchronize local time with the NTP server. The default value is 86400.	Phone->Preference->Synchronization Period

Parameter	Permitted Values	Descriptions	Web Setting Path
local_time.summer_time	0, 1 or 2	It enables or disables the IP phone to use daylight saving time (DST). **0**-Disabled (not use DST) **1**-Enabled (use the DST configured manually) **2**-Automatic (use the DST of the configured time zone name) The default value is 2. **Note:** If there is no available time zone name for the configured time zone, you can set the value of the parameter "local_time.summer_time" to be 1 (Enabled), and configure the DST time manually.	Phone->Preference->Daylight Saving Time
local_time.dst_time_type	0 or 1	It configures the DST time type. **0**-By Date **1**-By Week The default value is 0. **Note:** It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled).	Phone->Preference->Fixed Type
local_time.start_time	Time	I It configures the start time of the DST. **Value formats are:** ● Month/Day/Hour (for By Date)	Phone->Preference->Start Date

Parameter	Permitted Values	Descriptions	Web Setting Path
		• Month/Week of Month/Day of Week/Hour of Day (for By Week) If "local_time.dst_time_type" is set to 0 (By Date), use the 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 If "local_time.dst_time_type" is set to 1 (By Week), use the mapping: Month: 1=January, 2=February,…, 12=December Week of Month: 1=First In Month,…, 5=Last In Month Day of Week: 1=Monday, 2=Tuesday,…, 7=Sunday Hour of Day: 0=0am, 1=1am,…, 23=11pm The default value is 1/1/0. **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled).	
local_time.end_time	Time	It configures the end time of the DST. **Value formats are:** • Month/Day/Hour (for By Date)	Phone->Preference->End Date

Parameter	Permitted Values	Descriptions	Web Setting Path
		• Month/Week of Month/Day of Week/Hour of Day (for By Week) If "local_time.dst_time_type" is set to 0 (By Date), use the 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 If "local_time.dst_time_type" is set to 1 (By Week), use the mapping: Month: 1=January, 2=February,…, 12=December Week of Month: 1=First In Month,…, 5=Last In Month Day of Week: 1=Monday, 2=Tuesday,…, 7=Sunday Hour of Day: 0=1am, 1=1am,…, 23=11pm The default value is 12/31/23. **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled).	
local_time.offset_time	Integer from -300 to 300	It configures the offset time (in minutes). The default value is 60. **Note**: It works only if the value of the parameter	Phone->Preference->Offset

Parameter	Permitted Values	Descriptions	Web Setting Path
		"local_time.summer_time" is set to 1 (Enabled).	
local_time.dhcp_time	0 or 1	It enables or disables the phone to update time with the offset time obtained from the DHCP server. It is only available to the time zone 0. **0**-Disabled **1**-Enabled The default value is 0.	Phone->Preference->DHCP Time
dialplan.area_code.code	String within 16 characters	It configures the area code to be added before the entered numbers when dialing out. The default value is blank. **Note**: The length of the area code must be between the minimum length depending on the value of the parameter "dialplan.area_code.min_len" and the maximum length which depending on the value of the parameter "dialplan.area_code. max_len".	Phone->Dial Plan->Area Code->Code
dialplan.area_code.min_len	Integer from 1 to 15	It configures the minimum length of the area code. The default value is 1.	Phone->Dial Plan->Area Code->Minimum Length(1-15)
dialplan.area_code.max_len	Integer from 1 to 15	It configures the maximum length of the area code. The value must be larger than the minimum length. The default value is 15.	Phone->Dial Plan->Area Code->Maximum Length(1-15)

Parameter	Permitted Values	Descriptions	Web Setting Path
dialplan.area_code.line_id	Integer from 0 to 5	It configures the lines applying the area code. The digit 0 stands for all lines. If it is left blank, the area code will apply to all lines on the IP phone. Multiple line IDs are separated by commas. The default value is blank.	Phone->Dial Plan->Area Code->Account
dialplan.block_out.number.X (X ranges from 1 to 10.)	String within 32 characters	It configures the block out number X. The default value is blank.	Phone->Dial Plan->Block Out->BlockOut NumberX
dialplan.block_out.line_id.X (X ranges from 1 to 10.)	Integer from 0 to 5	It configures the lines applying the block out number X. 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. The default value is blank.	Phone->Dial Plan->Block Out->Account
dialplan.replace.prefix.X (X ranges from 1 to 20.)	String within 32 characters	It configures the alternate number to replace the entered number. The default value is blank.	Phone->Dial Plan->Replace Rule->Prefix
dialplan.replace.replace.X (X ranges from 1 to 20.)	String within 32 characters	It configures the alternate string instead of what the user enters. The default value is blank.	Phone->Dial Plan->Replace Rule->Replace
dialplan.replace.line_id.X	Integer form	It configures the lines applying the replace rule. The	Phone->Dial Plan->Replace Rule->Account

Parameter	Permitted Values	Descriptions	Web Setting Path
(X ranges from 1 to 20.)	0 to 5	digit 0 stands for all lines. If it is left blank, the replace rule will apply to all lines on the IP phone. Multiple line IDs are separated by commas. The default value is blank.	
call_waiting.enable	0 or 1	It enables or disables call waiting feature. **0**-Disabled **1**-Enabled The default value is 1.	Phone->Features->Call Waiting
call_waiting.tone	0 or 1	It enables or disables the phone to play call waiting tone. **0**-Disabled **1**-Enabled The default value is 1.	Phone->Features->Call Waiting Tone
features.dnd_refuse_code	404, 480 or 486	It configures the return code when DND mode is activated. **404**-No Found **480**-Temporarily not available **486**-Busy here The default value is 480.	Phone->Features->Return Code When DND

Parameter	Permitted Values	Descriptions	Web Setting Path
features.normal_refuse_code	404, 480 or 486	It configures the return code when refusing a call. **404**-No Found **480**-Temporarily not available **486**-Busy here The default value is 486.	Phone->Features->Return Code When Refuse
features.relog_offtime	Integer from 1 to 1000	It configures the web login timeout (in minutes). The default value is 5.	Phone->Features->Login Timeout(1~1000) (Minutes)
features.save_call_history	0 or 1	It enables or disables the phone to save call history. **0**-Disabled **1**-Enabled The default value is 1.	Phone->Features->Save Call Log
phone_setting.is_deal180	0 or 1	It enables or disables the phone to deal with the 180 SIP message received after the 183 SIP message. **0**-Disabled **1**-Enabled The default value is 0.	Phone->Features->180 Ringing
phone_setting.emergency.number	String within 99 characters	It configures the emergency numbers. Multiple emergency numbers are separated by commas.	Phone->Features->Emergency Numbers

Parameter	Permitted Values	Descriptions	Web Setting Path
		The default value is blank.	
features.voice_mail_tone_enable	0 or 1	It enables or disables the IP phone to play a warning tone when receiving a voice mail. **0**-Disabled **1**-Enabled The default value is 1.	Phone->Features->Voice Mail Tone
features.busy_tone_delay	0, 3 or 5	It configures the duration time (in seconds) of the busy tone. When one party releases the call, a busy tone is audible to the other party indicating that the call connection breaks. If it is set to 3 (3s), a busy tone is audible for 3 seconds on the IP phone. The default value is 3.	Phone->Features->Busy Tone Delay
features.direct_ip_call_enable	0 or 1	It enables or disables the IP phone to place or receive direct IP calls. A direct IP call is dialing the IP address of the destination phone directly. **0**-Disabled **1**-Enabled The default value is 1.	
managementserver.enable	0 or 1	It enables or disables TR069 feature.	Phone->TR069->TR069

Parameter	Permitted Values	Descriptions	Web Setting Path
		0-Disabled **1**-Enabled The default value is 0.	
managementserver.username	String within 128 characters	It configures the user name for the phone to authenticate with the ACS (Auto Configuration Servers). This string is set to the empty string if no authentication is required. The default value is blank.	Phone->TR069->ACS Username
managementserver.password	String within 64 characters	It configures the password for the phone to authenticate with the ACS (Auto Configuration Servers). This string is set to the empty string if no authentication is required. The default value is blank.	Phone->TR069->ACS Password
managementserver.url	URL within 511 characters	It configures the access URL of the ACS (Auto Configuration Servers). The default value is blank.	Phone->TR069->ACS URL
managementserver.periodic_inform_enable	0 or 1	It enables or disables the phone to report its configuration information to the ACS (Auto Configuration Servers). **0**-Disabled	Phone->TR069->Periodic Inform

Parameter	Permitted Values	Descriptions	Web Setting Path
		1-Enabled The default value is 1.	
managementserver.periodic_inform_interval	Integer from 5 to 4294967295	It configures the interval (in seconds) for the phone to report its configuration to the (Auto Configuration Servers). The default value is 60.	Phone->TR069->Periodic Inform Interval (seconds)
managementserver.connection_request_username	String within 128 characters	It configures the user name for the phone to authenticate the connection requests. The default value is blank.	Phone->TR069->Connection Request Username
managementserver.connection_request_password	String within 64 characters	It configures the password for the phone to authenticate the connection requests. The default value is blank.	Phone->TR069->Connection Request Password
firmware.url	URL within 511 characters	It configures the access URL of firmware file. The default value is blank. It takes effect after a reboot. For more information on upgrading firmware, refer to Updating Firmware on page 18.	Phone->Upgrade
security.user_name.user	String within 32 characters	It configures the user name of the user for phone's web user interface access. The default value is user.	

Parameter	Permitted Values	Descriptions	Web Setting Path
security.user_name.admin	String within 32 characters	It configures the user name of the administrator for phone's web user interface access. The default value is admin.	
security.user_name.var	String within 32 characters	It configures the user name of the var for phone's web user interface access. The default value is var.	
security.user_password	String within 32 characters	It configures the login password of the user, var and administrator. The valid value format is user name:new password **Example**: security.user_password = admin:password123 means that the password of administrator (current user name is "admin") is set to password123. The default value is blank. **Note:** IP phones support ASCII characters 32-126(0x20-0x7E) in passwords. You cannot set the password to be empty via the configuration parameter.	Security->Password
base.pin_code	Integer from 0 to 9999	It configures the system PIN of the base station. The default value is 0000.	Security->Base PIN->Base Unit PIN

Parameter	Permitted Values	Descriptions	Web Setting Path
security.var_enable	0 or 1	It enables or disables the 3-level access permissions (admin, user, var). **0**-Disabled **1**-Enabled The default value is 0. It takes effect after a reboot. For more information, refer to *Yealink W52P IP DECT Phones Configuration Guide for User Access Level*.	
web_item_level.url	URL within 511 characters	It configures the access URL of the file used to define 3-level permissions. The default value is blank. It takes effect after a reboot. For more information, refer to *Yealink IP phones Configuration Guide for User Access Level*.	
security.trust_certificates	0 or 1	It enables or disables the phone to authenticate the connecting server based on the trusted certificates list. **0**-Disabled **1**-Enabled The default value is 1.	Security->Trusted Certificates->Only Accept Trusted Certificates

Parameter	Permitted Values	Descriptions	Web Setting Path
		It takes effect after a reboot.	
security.ca_cert	0, 1 or 2	It configures the type of certificates the phone used to authenticate the connecting server. **0**-Default Certificates **1**-Custom Certificates **2**-All Certificates The default value is 2. It takes effect after a reboot.	Security->Trusted Certificates->CA Certificates
security.cn_validation	0 or 1	It enables or disables the phone to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the connecting server. **0**-Disabled **1**-Enabled The default value is 0. It takes effect after a reboot.	Security->Trusted Certificates->Common Name Validation
security.dev_cert	0 or 1	It configures the type of certificates the phone sends for authentication. **0**-Default Certificates **1**-Custom Certificates	Security->Server Certificates->Device Certificates

Parameter	Permitted Values	Descriptions	Web Setting Path
		The default value is 0. It takes effect after a reboot.	
trusted_certificates.url	URL within 511 characters	It configures the access URL of the custom trusted certificate used to authenticate the connecting server. **Example**: trusted_certificates.url = http://192.168.1.20/tc.crt The default value is blank. **Note**: The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format.	Security->Trusted Certificates
trusted_certificates.delete	http://localh ost/all	It deletes all uploaded trusted certificate files. The valid value is: http://localhost/all The default value is blank.	
server_certificates.url	URL within 511 characters	It configures the access URL of the certificate the IP phone sends for authentication. **Example**: server_certificates.url = http://192.168.1.20/ca.pem The default value is blank. **Note**: The certificate you want to upload must be in *.pem or *.cer format.	Security->Server Certificates

Parameter	Permitted Values	Descriptions	Web Setting Path
server_certificates.delete	http://localhost/all	It deletes all uploaded server certificates. The valid value is: http://localhost/all The default value is blank.	
auto_dst.url	URL within 511 characters	It configures the access URL of the DST file (AutoDST.xml). The default value is blank. **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 2 (Automatic).	
dialplan_replace_rule.url	URL within 511 characters	It configures the access URL of the replace rule file. The default value is blank.	
custom_factory_configuration.url	URL within 511 characters	It configures the access URL of the custom factory configuration files. The default value is blank. It takes effect after a reboot.	
configuration.url	URL within 511 characters	It configures the access URL for the custom config files. The default value is blank. It takes effect after a reboot.	
custom_mac_cfg.url	URL within	It configures the access URL of the custom	Phone->Auto Provision

Parameter	Permitted Values	Descriptions	Web Setting Path
	511 characters	MAC-Oriented CFG file. The default value is blank.	
blacklist.url	URL	It configures the access URL of the blacklist file.	
voice.tone.country	Custom, Australia, Austria, Brazil, Belgium, China, Czech, Denmark, Finland, France, Germany, Great Britain, Greece, Hungary, Lithuania, India, Italy, Japan, Mexico,	It configures the country tone for the phone. The default value is Custom.	Phone->Tones->Select country

Parameter	Permitted Values	Descriptions	Web Setting Path
	New Zealand, Netherlands, Norway, Portugal, Spain, Switzerland, Sweden, Russia, United States, Chile or Czech ETSI		
voice.tone.ring	String	It customizes the ring tone. **tone list** = element[,element] [,element]…Where **element** = [!]Freq1[+Freq2][+Freq3][+Freq4] /Duration The value format is Freq/Duration or !Freq/Duration. **Freq**: the frequency of the tone (ranges from 200 to 4000 Hz). If it is set to 0Hz, it means the tone is not played. **Duration**: the time duration (in milliseconds, ranges	Phone->Tones->Ring back

Parameter	Permitted Values	Descriptions	Web Setting Path
		from 0 to 4000ms) of playing the tone. You can configure at most eight different tones for one condition, each tone is separated by comma (e.g., 250/200,0/1000,200+300/500). You can configure the phone to play tones once by adding exclamation mark before the value ((e.g., !250/200,0/1000,200+300/500). The default value is blank. **Note:** It works only if the value of the parameter "voice.tone.country" is set to Custom.	
voice.tone.busy	String	It customizes the busy tone. The value format is Freq/Duration or !Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.ring". The default value is blank. **Note:** It works only if the value of the parameter "voice.tone.country" is set to Custom.	Phone->Tones->Busy
voice.tone.callwaiting	String	It customizes the call waiting tone. The value format is Freq/Duration or !Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.ring".	Phone->Tones->Call Waiting

Parameter	Permitted Values	Descriptions	Web Setting Path
		The default value is blank. **Note:** It works only if the value of the parameter "voice.tone.country" is set to Custom.	
voice.tone.dial	String	It customizes the dial tone. The value format is Freq/Duration or !Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.ring". The default value is blank. **Note:** It works only if the value of the parameter "voice.tone.country" is set to Custom.	Phone->Tones->Dial
handset.X.contact_list.url (X ranges from 1 to 5.)	URL within 511 characters	It configures the access URL of the contact file of handset X.	Contacts->Contacts
remote_phonebook.data.X.url (X ranges from 1 to 5.)	within 511 characters	It configures the access URL of the remote phone book. The default value is blank.	Contacts->Remote Phone Book-> RemoteURL
remote_phonebook.data.X.name (X ranges from 1 to 5.)	String within 99 characters	It configures the display name of the remote phone book. The default value is blank.	Contacts->Remote Phone Book->Display Name

Parameter	Permitted Values	Descriptions	Web Setting Path
directory.update_time_interval	Integer from 60 to 86400	It configures the interval (in minutes) for the phone to update the data of the remote phone book from the remote phone book server. The default value is 1440.	Contacts->Remote Phone Book->Update Time Interval (60-86400) (Minutes)
over_the_air.url	within 511 characters	It configures the access URL of the handset firmware file. The default value is blank.	Phone->Upgrade
over_the_air.base_trigger	0 or 1	It enables or disables base trigger feature. **0**-Disabled **1**-Enabled The default value is 1.	
over_the_air.handset_tip	0 or 1	It enables or disables new version tip feature. **0**-Disabled **1**-Enabled The default value is 1. **Note**: It works only when the value of the parameter "over_the_air.base_trigger" is set to 0 (Disabled).	
handset.X.incoming_lines (X ranges from 1 to 5.)	Integer	It configures the lines to receive incoming calls for handset X. Multiple line IDs are separated by commas.	Account->Number Assignment->Incoming lines

Parameter	Permitted Values	Descriptions	Web Setting Path
		The default incoming line for handset X is line X, such as line 2 for the handset 2.	
handset.X.name (X ranges from 1 to 5.)	String within 24 characters	It configures the name of handset X. The default handset for handset 1-5 is H1-5.	Account->Handset Name
handset.X.dial_out_default_line (X ranges from 1 to 5.)	Integer from 1 to 5	It configures the default line to place outgoing calls for handset X. The default value is 1.	Account->Number Assignment->Outgoing lines->Default
handset.X.dial_out_lines (X ranges from 1 to 5.)	Integer	It configures the lines to place outgoing calls for handset X. Multiple line IDs are separated by commas. The default outgoing line for handset X is line X, such as line 2 for the handset 2.	Account->Number Assignment->Outgoing lines
local_time.manual_time_enable	0 or 1	It enables or disables the IP phone to obtain time from manual settings. **0**-Diabled (obtain time from NTP server) **1**-Enabled (obtain time from manual settings) The default value is 0.	Phone->Preference->Time Synchronization
local_time.manual_ntp_srv_prior	0 or 1	Configures the priority of the IP phone to use the NTP server offered by DHCP.	Phone->Preference->NTP By DHCP Priority

Parameter	Permitted Values	Descriptions	Web Setting Path
		0-High (use the NTP server offered by DHCP preferentially) **1**-Low(use the NTP server offered manually preferentially) The default value is 0.	
custom.handset.time_format	0 or 1	It configures the time format. **0**-12 Hour **1**-24 Hour If it is set to 0 (12 Hour), the time will be displayed in 12-hour format with AM or PM specified. If it is set to 1 (24 Hour), the time will be displayed in 24-hour format (e.g., 2:00 PM displays as 14:00). The default value is 1. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	
custom.handset.color_scheme	0 or 1	It configures the color scheme of the handset. **0**-color scheme 1 **1**-color scheme 2 The default value is 0.	

Parameter	Permitted Values	Descriptions	Web Setting Path
		Note: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	
custom.handset.auto_intercom	0, 1 or 2	It configures whether the IP phone automatically answers an incoming internal intercom call and plays a warning tone. **0**-Off **1**-Beep Off **2**-Beep On If it is set to 0, users need to answer incoming internal intercom calls manually. If it is set to 1, the handset will answer an incoming internal intercom call automatically without a warning tone. If it is set to 2, the handset will answer an incoming internal intercom call automatically and play a warning tone. The default value is 0. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	

Parameter	Permitted Values	Descriptions	Web Setting Path
custom.handset.screen_saver.enable	0 or 1	It enables or disables screen saver feature. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), an analog clock will be activated and appears on the LCD screen if no user activity is sensed for approximately 10 seconds. The default value is 1. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	
custom.handset.backlight_in_charger.enable	0 or 1	It enables or disables the handset to always turn on the backlight when it is in the charging state. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the backlight will be turned off after the handset is idle for a period of time when it is in the charging state. The default value is 1. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	

Parameter	Permitted Values	Descriptions	Web Setting Path
custom.handset.backlight_out_of_charger.enable	0 or 1	It enables or disables the handset to always turn on the backlight when it is not in the charging state. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the backlight will be turned off after the handset is idle for a period of time when it is not in the charging state. The default value is 0. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	
custom.handset.keypad_light.enable	0 or 1	It enables or disables the handset to turn on the keypad light when any key is pressed. **0**-Disabled **1**-Enabled The default value is 1. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	
custom.handset.keypad_tone.enable	0 or 1	It enables or disables the handset to play a tone when any key is pressed.	

Parameter	Permitted Values	Descriptions	Web Setting Path
		0-Disabled **1**-Enabled The default value is 1. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	
custom.handset.confirmation_tone.enable	0 or 1	It enables or disables the handset to play a tone when a user saves settings or places the handset in the charger cradle. **0**-Disabled **1**-Enabled The default value is 1. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	
custom.handset.low_battery_tone.enable	0 or 1	It enables or disables the handset to play a tone when the capacity of the batteries is low. **0**-Disabled **1**-Enabled The default value is 0. **Note**: It works only if the value of the parameter	

Parameter	Permitted Values	Descriptions	Web Setting Path
		"auto_provision.handset_configured.enable" is set to 1 (Enabled).	
custom.handset.voice_mail_notify_light.enable	0 or 1	It enables or disables the message key LED to flash red when the handset receives a voice mail. **0**-Disabled **1**-Enabled The default value is 1. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	
custom.handset.missed_call_notify_light.enable	0 or 1	It enables or disables the message key LED to flash red when the handset misses a call. **0**-Disabled **1**-Enabled The default value is 1. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	
custom.handset.auto_answer.enable	0 or 1	It enables or disables a user to answer incoming calls by lifting the handset from the charger cradle without having to press the off-hook key.	

Parameter	Permitted Values	Descriptions	Web Setting Path
		0-Disabled **1**-Enabled The default value is 1. **Note**: It works if the handset is placed in the charger cradle and the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	
custom.handset.eco_mode.enable	0 or 1	It enables or disables the eco mode to greatly reduce the transmission power and signal output when the phone is in the talk mode. **0**-Disabled **1**-Enabled The default value is 0. **Note**: It works only if the value of the parameter "auto_provision.handset_configured.enable" is set to 1 (Enabled).	
base.eco_mode.enable	0 or 1	It enables or disables the eco mode+ to turn off the transmission power when the phone is in the standby mode. **0**-Disabled **1**-Enabled	

Parameter	Permitted Values	Descriptions	Web Setting Path
		If it is set to 1 (Enabled), there will be no signal interaction between the handset and the base station, the color of the signal strength indicator on the idle screen displays in green. The default value is 0. It takes effect after a reboot.	
base.repeater_mode.enable	0 or 1	It enables or disables the repeater mode to extend the radio coverage of the base station. **0**-Disabled **1**-Enabled The default value is 0. It takes effect after a reboot.	
account.X.enable (X ranges from 1 to 5.)	0 or 1	It enables or disables the account X. **0**-Disabled **1**-Enabled The default value is 0.	Account->Basic->Line Active
account.X.label (X ranges from 1 to 5.)	String within 99 characters	It configures the label displayed on the LCD screen for account X. The default value is blank.	Account->Basic->Label

Parameter	Permitted Values	Descriptions	Web Setting Path
account.X.display_name (X ranges from 1 to 5.)	String within 99 characters	It configures the display name for account X. The default value is blank.	Account->Basic->Display Name
account.X.auth_name (X ranges from 1 to 5.)	String within 99 characters	It configures the user name for register authentication for account X. The default value is blank.	Account->Basic->Register Name
account.X.password (X ranges from 1 to 5.)	String within 99 characters	It configures the password for register authentication for account X. The default value is blank.	Account->Basic->Password
account.X.user_name (X ranges from 1 to 5.)	String within 32 characters	It configures the register user name for account X. The default value is blank.	Account->Basic->User Name
account.X.transport (X ranges from 1 to 5.)	0, 1, 2 or 3	It configures the transport type for account X. **0**-UDP **1**-TCP **2**-TLS **3**-DNS-SRV The default value is 0.	Account->Basic->Transport
account.X.outbound_proxy_enable (X ranges from 1 to 5.)	0 or 1	It enables or disables the phone to use the outbound proxy server for account X.	Account->Basic->Enable Outbound Proxy Server

Parameter	Permitted Values	Descriptions	Web Setting Path
		0-Disabled **1**-Enabled The default value is 0.	
account.X.outbound_host (X ranges from 1 to 5.)	Domain Name or IP Address	It configures the domain name or IP address of the outbound proxy server for account X. The default value is blank.	Account->Basic->Outbound Proxy Server
account.X.outbound_port (X ranges from 1 to 5.)	Integer from 0 to 65535	It configures the port of the outbound proxy server for account X. The default value is 5060.	Account->Basic->Outbound Proxy Server->Port
account.X.proxy_require (X ranges from 1 to 5.)	String within 256 characters	It configures the proxy server for account X. The default value is blank.	Account->Basic->Proxy Require
account.X.nat.nat_traversal (X ranges from 1 to 5.)	0 or 1	It enables or disables the NAT traversal for account X. **0**-Disabled **1**-STUN The default value is 0.	Account->Basic->NAT Traversal
account.X.nat.stun_server (X ranges from 1 to 5.)	Domain name or IP address	It configures the domain name or IP address of the STUN server for account X. The default value is blank.	Account->Basic->STUN Server

Parameter	Permitted Values	Descriptions	Web Setting Path
account.X.nat.stun_port (X ranges from 1 to 5.)	Integer from 1024 to 65000	It configures the port of the STUN server for account X. The default value is 3478.	Account->Basic->STUN Server->Port
voice_mail.number.X (X ranges from 1 to 5.)	String within 99 characters	It configures the voice mail number for account X. The default value is blank. **Note**: It works only if the value of the parameter "account.X.subscribe_mwi_to_vm" is set to 1 (Enabled).	Phone->Features->LineX->Voice Mail
account.X.anonymous_call_mode (X ranges from 1 to 5.)	0 or 1	It configures the anonymous call feature mode when users configure anonymous call feature via the handset for account X. **0**-Local **1**-Server The default value is 0. If it is set to 0 (Local), the phone-side anonymous call feature is configured when users configure anonymous call feature for account X via the handset. If it is set to 1 (Server), the server-side anonymous call feature is configured when users configure anonymous call feature for account X via the	

Parameter	Permitted Values	Descriptions	Web Setting Path
		handset. In this mode, the IP phone is triggered to send the preconfigured anonymous call on code/off code to the server to activate/deactivate the server-side anonymous call feature when the user configures anonymous call feature via the handset. **Note**: If it is set to 1 (Server), the anonymous call on code and off code must be configured on the phone. In this mode, users can only configure the phone-side anonymous call feature via web user interface or the parameter "account.X.anonymous_call".	
account.X.anonymous_call (X ranges from 1 to 5.)	0 or 1	It enables or disables phone-side anonymous call feature for account X. **0**-Disabled **1**-Enabled The default value is 0.	Account->Basic->Anonymous Call
account.X.send_anonymous_code (X ranges from 1 to 5.)	0 or 1	It configures the type of anonymous call code for the IP phone to send to the server for account X. **0**-Off Code **1**-On Code If it is set to 0 (Off Code), the IP phone will send anonymous call off code to deactivate the	Phone->Features->LineX->Anonymous Call->Anonymous code

Parameter	Permitted Values	Descriptions	Web Setting Path
		server-side anonymous call feature. If it is set to 1 (On Code), the IP phone will send anonymous call on code to activate the server-side anonymous call feature. The default value is 0. **Note**: If the value of the parameter "account.X.anonymous_call_mode" is set to 1, the type of anonymous call code sent to the server will be accordingly changed when users configure anonymous call feature via the handset.	
account.X.anonymous_call_oncode (X ranges from 1 to 5.)	String within 32 characters	It configures the anonymous call on code for account X. The default value is blank. **Note:**	Phone->Features->LineX->Anonymous Call->Anonymous code On Code
account.X.anonymous_call_offcode (X ranges from 1 to 5.)	String within 32 characters	It configures the anonymous call off code for account X. The default value is blank.	Phone->Features->LineX->Anonymous Call->Anonymous code Off Code
account.X.reject_anonymous_call_mode (X ranges from 1 to 5.)	0 or 1	It configures the anonymous call rejection mode when users configure anonymous call rejection feature via the handset for account X. **0**-Local	

Parameter	Permitted Values	Descriptions	Web Setting Path
		1-Server The default value is 0. If it is set to 0 (Local), the phone-side anonymous call rejection feature is configured when users configure anonymous call rejection feature for account X via the handset. If it is set to 1 (Server), the server-side anonymous call rejection feature is configured when users configure anonymous call rejection feature for account X via the handset. In this mode, the IP phone is triggered to send the preconfigured anonymous call rejection on code/off code to the server to activate/deactivate the server-side anonymous call rejection feature when the user configures anonymous call rejection feature via the handset. **Note**: If it is set to 1 (Server), the anonymous call rejection on code and off code must be configured on the phone. In this mode, users can only configure the phone-side anonymous call rejection feature via web user interface or the parameter "account.X.reject_anonymous_call".	

Parameter	Permitted Values	Descriptions	Web Setting Path
account.X.reject_anonymous_call (X ranges from 1 to 5.)	0 or 1	It enables or disables phone-side anonymous call rejection feature for account X. **0**-Disabled **1**-Enabled The default value is 0.	Account->Basic->Anonymous Call Rejection
account.X.send_anonymous_rejection_code (X ranges from 1 to 5.)	0 or 1	It configures the type of anonymous call rejection code for the IP phone to send to the server for account X. **0**-Off Code **1**-On Code If it is set to 0 (Off Code), the IP phone will send anonymous call rejection off code to deactivate the server-side anonymous call rejection feature. If it is set to 1 (On Code), the IP phone will send anonymous call rejection on code to activate the server-side anonymous call rejection feature. The default value is 0. **Note**: If the value of the parameter "account.X.reject_anonymous_call_mode" is set to 1, the type of anonymous call rejection code sent to the server will be accordingly changed when users	Phone->Features->LineX->Anonymous Call->Anonymous rejection code

Parameter	Permitted Values	Descriptions	Web Setting Path
		configure anonymous call rejection feature via the handset.	
account.X.anonymous_reject_oncode (X ranges from 1 to 5.)	String within 32 characters	It configures the anonymous call rejection on code for account X. The default value is blank.	Phone->Features->LineX->Anonymous Call->Anonymous rejection code On Code
account.X.anonymous_reject_offcode (X ranges from 1 to 5.)	String within 32 characters	It configures the anonymous call rejection off code for account X. The default value is blank.	Phone->Features->LineX->Anonymous Call->Anonymous rejection code Off Code
account.X.auto_dial_enable (X ranges from 1 to 5.)	0 or 1	It enables or disables the phone to automatically dial out a pre-configured number first when the user places a call using the account X. **0**-Disabled **1**-Enabled The default value is 0. If it is set to 1(Enabled), the phone will automatically dial out the pre-configured number (configured by the parameter "account.X.auto_dial_num") before dialing a call. **Note**: The server may prompt the user to enter an activation code to use this account for call service. This feature requires support from the SIP server.	

Parameter	Permitted Values	Descriptions	Web Setting Path
account.X.auto_dial_num (X ranges from 1 to 5.)	String within 32 characters	It configures the number that the phone automatically dials out first when the user places a call. The default value is blank. **Note**: It works only if the value of the parameter "account.X.auto_dial_enable" is set to 1 (Enabled).	
account.X.cid_source_privacy (X ranges from 1 to 5.)	0 or 1	It enables or disables the IP phone to process the PRIVACY header field in the 180 or 200 OK message for account X. **0**-Disabled **1**-Enabled The default value is 1.	
account.X.cid_source_ppi (X ranges from 1 to 5.)	0 or 1	It enables or disables the IP phone to process the P-Preferred-Identity header for caller identity presentation when receiving an incoming call for account X. **0**-Disabled **1**-Enabled The default value is 1.	
account.X.cp_source	0, 1 or 2	It configures the presentation of the callee's identity	

Parameter	Permitted Values	Descriptions	Web Setting Path
(X ranges from 1 to 5.)		for account X. 0-PAI-RPID (Derives the name and number of the callee from the "PAI" header preferentially. If the server does not send the "PAI" header, it will derive from the "RPID" header). 1-Dialed Digits (Preferentially displays the dialed digits on the caller's phone). 2-RFC4916 (Derives the name and number of the callee from "From" header in the Update message). When the RFC 4916 is enabled on the IP phone, 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 callee, and displays the identity in the From header. The default value is 0.	
account.X.naptr_build (X ranges from 1 to 5.)	0 or 1	It configures the way of SRV query for the IP phone to be performed when no result is returned from NAPTR query for account X. 0-SRV query using UDP only 1-SRV query using UDP, TCP and TLS. The default value is 0.	

Parameter	Permitted Values	Descriptions	Web Setting Path
		For more information, refer to *Server Redundancy on Yealink IP Phones*.	
account.X.fallback.redundancy_type (X ranges from 1 to 5.)	0 or 1	It configures the registration mode for account X in fallback mode. **0**-Concurrent registration **1**-Successive registration The default value is 0. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
account.X.fallback.timeout (X ranges from 1 to 5.)	Integer from 10 to 2147483647	It configures the time interval (in seconds) for the IP phone to detect whether the working server is available by sending the registration request for account X after the fallback server takes over call control. It is only applicable to successive registration mode. The default value is 120. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
account.X.sip_server.Y.address (X ranges from 1 to 5.	IP address or domain name	It configures the IP address or domain name of the SIP server Y for account X. **Example**:	Account->Basic->SIP Server 1/2->Server Host

Parameter	Permitted Values	Descriptions	Web Setting Path
Y ranges from 1 to 2.)		account.1.sip_server.1.address = 10.2.1.128 The default value is blank. **Note**: The old parameter "account.X.sip_server_host" is also applicable to IP phones.	
account.X.sip_server.Y.port (X ranges from 1 to 5. Y ranges from 1 to 2.)	Integer from 1 to 65535	It configures the port of SIP server Y for account X. The default value is 5060. **Note**: The old parameter "account.X.sip_server_port" is also applicable to IP phones.	Account->Basic->SIP Server 1/2->Port
account.X.sip_server.Y.expires (X ranges from 1 to 5. Y ranges from 1 to 2.)	Integer from 30 to 2147483647	It configures the registration expiration time (in seconds) of SIP server Y for account X. The default value is 3600. **Note**: The old parameter "account.X.expires" is also applicable to IP phones.	Account->Basic->SIP Server 1/2->Server Expires
account.X.sip_server.Y.retry_counts (X ranges from 1 to 5. Y ranges from 1 to 2.)	Integer from 0 to 20	It configures the retry times for the IP phone to resend requests when the SIP server Y is unavailable or there is no response from the SIP server Y for account X. The default value is 3. For more information, refer to *Server Redundancy on*	Account->Basic->SIP Server 1/2->Server Retry Counts

Parameter	Permitted Values	Descriptions	Web Setting Path
		Yealink IP Phones.	
account.X.sip_server.Y.failback_mode (X ranges from 1 to 5. Y ranges from 1 to 2.)	0, 1, 2 or 3	It configures the mode for the IP phone to retry the primary server in failover mode for account X. **0**-newRequests: all requests are forwarded to the primary server first, regardless of the last used server. **1**-DNSTTL: the IP phone retries to send requests to the primary server after the timeout of the DNSTTL configured for the server that the IP phone is registered to. **2**-Registration: the IP phone retries to send REGISTER requests to the primary server when registration renewal. **3**-duration: the IP phone retries to send requests to the primary server after the timeout defined by the parameter "account.X.sip_server.Y.failback_timeout". The default value is 0. For more information, refer to *Server Redundancy on Yealink IP Phones.*	

Parameter	Permitted Values	Descriptions	Web Setting Path
account.X.sip_server.Y.failback_timeout (X ranges from 1 to 5. Y ranges from 1 to 2.)	Integer 0, from 60 to 65535	It configures the timeout (in seconds) for the IP phone to retry to send requests to the primary server after failing over to the current working server for account X when the value of the parameter "account.X.sip_server.Y.failback_mode" is set to 3 (duration). If you set the parameter to 0, the IP 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. The default value is 3600. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
account.X.sip_server.Y.register_on_enable (X ranges from 1 to 5. Y ranges from 1 to 2.)	0 or 1	It enables or disables the IP phone to send registration requests to the secondary server for account X when encountering a failover. **0**-Disabled **1**-Enabled The default value is 0. For more information, refer to *Server Redundancy on*	

Parameter	Permitted Values	Descriptions	Web Setting Path
		Yealink IP Phones.	
account.X.static_cache_pri (X ranges from 1 to 5.)	0 or 1	It configures whether preferentially to use the static DNS cache for domain name resolution of the SIP server for account X. **0**-Use domain name resolution from server preferentially **1**-Use static DNS cache preferentially The default value is 0. For more information, refer to *Server Redundancy on Yealink IP Phones.*	
account.X.dns_cache_type (X ranges from 1 to 5.)	0, 1 or 2	It configures the content that the DNS cache records for account X. **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 record the additional records. The default value is 1. For more information, refer to *Server Redundancy on Yealink IP Phones.*	

Parameter	Permitted Values	Descriptions	Web Setting Path
dns_cache_a.X.name (X ranges from 1 to 12.)	Domain name	It configures the domain name in A record X. The default value is blank. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
dns_cache_a.X.ip (X ranges from 1 to 12.)	IP address	It configures the IP address that the domain name in A record X maps to. The default value is blank. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
dns_cache_a.X.ttl (X ranges from 1 to 12.)	Integer from 30 to 2147483647	It configures the time interval (in seconds) that A record X may be cached before the record should be consulted again. The default value is 300. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
dns_cache_srv.X.name (X ranges from 1 to 12.)	Domain name	It configures the domain name in SRV record X. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
dns_cache_srv.X.port (X ranges from 1 to 12.)	Integer from 0 to 65535	It configures the port to be used in SRV record X. The default value is 0. For more information, refer to *Server Redundancy on*	

Parameter	Permitted Values	Descriptions	Web Setting Path
		Yealink IP Phones.	
dns_cache_srv.X.priority (X ranges from 1 to 12.)	Integer from 0 to 65535	It configures the priority for the target host in SRV record X. Lower priority is more preferred. The default value is 0. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
dns_cache_srv.X.target (X ranges from 1 to 12.)	Domain name	It configures the domain name of the target host for an A query in SRV record X. The default value is blank. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
dns_cache_srv.X.weight (X ranges from 1 to 12.)	Integer from 0 to 65535	It configures the weight of the target host in SRV record X. When priorities are equal, weight is used to differentiate the preference. Higher weight is more preferred. The default value is 0. For more information, refer to *Server Redundancy on Yealink IP Phones*.	

Parameter	Permitted Values	Descriptions	Web Setting Path
dns_cache_srv.X.ttl (X ranges from 1 to 12.)	Integer from 30 to 2147483647	It configures the time interval (in seconds) that SRV record X may be cached before the record should be consulted again. The default value is 300. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
dns_cache_naptr.X.name (X ranges from 1 to 12.)	Domain name	It configures the domain name to which NAPTR record X refers. The default value is blank. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
dns_cache_naptr.X.flags (X ranges from 1 to 12.)	S, A, U or P	It configures the flag of NAPTR record X. (Always "s" for SIP, which means to do an SRV lookup on whatever is in the replacement field) **S**-Do an SRV lookup next. **A**-Do an A lookup next. **U**-No need to do a DNS query next. **P**-Service customized by the user The default value is blank. For more information, refer to *Server Redundancy on Yealink IP Phones*.	

Parameter	Permitted Values	Descriptions	Web Setting Path
dns_cache_naptr.X.order (X ranges from 1 to 12.)	Integer from 0 to 65535	It configures the order of NAPTR record X. NAPTR record with lower order is more preferred. The default value is 0. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
dns_cache_naptr.X.preference (X ranges from 1 to 12.)	Integer from 0 to 65535	It configures the preference of NAPTR record X. NAPTR record with lower preference is more preferred. The default value is 0. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
dns_cache_naptr.X.replace (X ranges from 1 to 12.)	Domain name	It configures a domain name to be used for the next SRV query in NAPTR record X. The default value is blank. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
dns_cache_naptr.X.service (X ranges from 1 to 12.)	String within 32 characters	It configures the transport protocol available for the SIP server in NAPTR record X. The default value is blank. For more information, refer to *Server Redundancy on Yealink IP Phones*.	

Parameter	Permitted Values	Descriptions	Web Setting Path
dns_cache_naptr.X.ttl (X ranges from 1 to 12.)	Integer from 30 to 2147483647	It configures the time interval (in seconds) that NAPTR record X may be cached before the record should be consulted again. The default value is 300. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
account.X.srv_ttl_timer_enable (X ranges from 1 to 5.)	0 or 1	It enables or disables the IP phone to refresh the DNS-SRV query records at regular time for account X. **0**-Disabled **1**-Enabled The default value is 0. It takes effect after a reboot. For more information, refer to *Server Redundancy on Yealink IP Phones*.	
account.X.sip_listen_port (X ranges from 1 to 5.)	Integer	It configures the SIP port for account X. The default value is 5062.	Account->Advanced->Local SIP Port
account.X.100rel_enable (X ranges from 1 to 5.)	0 or 1	It enables or disables 100 reliable retransmission feature for account X. **0**-Disabled **1**-Enabled	Account->Advanced->100 Reliable Retransmission

Parameter	Permitted Values	Descriptions	Web Setting Path
		The default value is 0.	
account.X.precondition (X ranges from 1 to 5.)	0 or 1	It enables or disables the resource reservation for account X. **0**-Disabled **1**-Enabled The default value is 0.	Account->Advanced->Enable Precondition
account.X.subscribe_register (X ranges from 1 to 5.)	0 or 1	It enables or disables the phone to subscribe to the register status for account X. **0**-Disabled **1**-Enabled The default value is 0.	Account->Advanced->Subscribe Register
account.X.subscribe_mwi (X ranges from 1 to 5.)	0 or 1	It enables or disables the phone to subscribe the message waiting indicator for account X. **0**-Disabled **1**-Enabled The default value is 0.	Account->Advanced->Subscribe for MWI
account.X.cid_source (X ranges from 1 to 5.)	0,1,2,3,4 or 5	It configures the presentation of the caller identity when receiving an incoming call for account X. **0**-FROM (Derives the name and number of the caller	Account->Advanced->Caller ID Header

Parameter	Permitted Values	Descriptions	Web Setting Path
		from the "From" header). **1**-PAI (Derives the name and number of the caller from the "PAI" header. If the server does not send the "PAI" header, it will display "anonymity" on the callee's phone). **2**-PAI-FROM (Derives the name and number of the caller from the "PAI" header preferentially. If the server does not send the "PAI" header, it will derive from the "From" header). **3**-PRID-PAI-FROM **4**-PAI-RPID-FROM, **5**-RPID-FROM The default value is 0.	
account.X.session_timer.enable (X ranges from 1 to 5.)	0 or 1	It enables or disables the session timer for account X. **0**-Disabled **1**-Enabled The default value is 0.	Account->Advanced->Use Session Timer
account.X.session_timer.expires (X ranges from 1 to 5.)	Integer from 30 to 7200	It configures the interval (in seconds) for refreshing the SIP session for account X. The default value is 1800.	Account->Advanced->Session Timer (seconds)

Parameter	Permitted Values	Descriptions	Web Setting Path
account.X.session_timer.refresher (X ranges from 1 to 5.)	0 or 1	It configures the refresher of the session timer for account X. **0**-Uac (Refreshing the session is performed by the IP phone). **1**-Uas (Refreshing the session is performed by a SIP server). The default value is 0.	Account->Advanced->Refresher
account.X.enable_user_equal_phone (X ranges from 1 to 5.)	0 or 1	It enables or disables the "user=phone" for account X. **0**-Disabled **1**-Enabled The default value is 0.	Account->Advanced->Use user=phone
account.X.srtp_encryption (X ranges from 1 to 5.)	0 or 1	It configures whether to use voice encryption service for account X. **0**-Disabled **1**-Optional **2**-Compulsory If it is set to 1 (Optional), the IP phone will negotiate with the other IP phone what type of encryption to utilize for the session.	Account->Advanced->Voice Encryption(SRTP)

Parameter	Permitted Values	Descriptions	Web Setting Path
		If it is set to 2 (Compulsory), the IP phone is forced to use SRTP during a call. The default value is 0.	
account.X.ptime (X ranges from 1 to 5.)	0 (Disabled), 10, 20, 30, 40, 50 or 60	It configures the ptime (in milliseconds) for the codec for account X. The default value is 20.	Account->Advanced->Ptime(ms)
account.X.subscribe_mwi_expires (X ranges from 1 to 5.)	Integer from 0 to 84600	It configures the interval (in seconds) of MWI subscription for account X. The default value is 3600.	Account->Advanced->MWI Subscription Period (Scope:0~84600) (seconds)
account.X.subscribe_mwi_to_vm (X ranges from 1 to 5.)	0 or 1	It enables or disables the phone to subscribe to the voice mail for the message waiting indicator for account X. **0**-Disabled **1**-Enabled The default value is 0.	Account->Advanced->Subscribe MWI to VM
account.X.register_mac (X ranges from 1 to 5.)	0 or 1	It enables or disables the phone to carry the MAC address in the REGISTER message for account X. **0**-Disabled **1**-Enabled The default value is 0.	Account->Advanced->SIP Send MAC

Parameter	Permitted Values	Descriptions	Web Setting Path
account.X.register_line (X ranges from 1 to 5.)	0 or 1	It enables or disables the phone to carry the line number in the REGISTER message for account X. **0**-Disabled **1**-Enabled The default value is 1.	Account->Advanced->SIP Send Line
account.X.reg_fail_retry_interval (X ranges from 1 to 5.)	Integer from 0 to 1800	It configures the interval (in seconds) the phone to retry to register account X when registration fails. The default value is 30.	Account->Advanced->SIP Registration Retry Timer(Scope:0~1800)(seconds)
account.X.srtp_encryption (X ranges from 1 to 5.)	0 or 1	It enables or disables the IP phone to use voice encryption service for account X. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone is forced to use SRTP during a call. The default value is 0.	Account->Advanced->Voice Encryption (SRTP)
account.x.shared_line (X ranges from 1 to 5.)	0 or 1	It enables or disables BroadSoft shared call appearance feature. **0**-Disabled **1**-BroadSoft_SCA The default value is 0.	Account->Advanced->Shared Line

Parameter	Permitted Values	Descriptions	Web Setting Path
account.X.dtmf.type (X ranges from 1 to 5.)	0, 1, 2 or 3	It configures the DTMF type for account X. **0**-INBAND **1**-RFC2833 **2**-SIP INFO **3**-AUTO+SIP INFO The default value is 1.	Account->Advanced->DTMF Type
account.X.dtmf.dtmf_payload (X ranges from 1 to 5.)	Integer from 96 to 127	It configures the telephone-event payload for account X. The default value is 101.	Account->Advanced->DTMF Payload(scope:96~127)
account.X.dtmf.info_type (X ranges from 1 to 5.)	0, 1, 2 or 3	It configures the DTMF info type when the DTMF type is configured as "SIP INFO" or "AUTO+SIP INFO" for account X. **0**-Disabled **1**-DTMF-Relay **2**-DTMF **3**-Telephone-Event The default value is 1.	Account->Advanced->How to INFO DTMF
account.X.nat.udp_update_enable (X ranges from 1 to 5.)	0, 1, 2 or 3	It configures the type of keep-alive packets sent to the Register/Proxy port to keep the port open so that the phone can remain reachable.	Account->Advanced->Keep Alive Type

Parameter	Permitted Values	Descriptions	Web Setting Path
		0-Disabled **1**-Default (the IP phone sends UDP packets to the server). **2**-Option (the IP phone sends SIP OPTION packets to the server). **3**-Notify (the IP phone sends SIP NOTIFY packets to the server). The default value is 1.	
account.X.nat.udp_update_time (X ranges from 1 to 5.)	Integer from 15 to 2147483647	It configures the keep-alive interval (in seconds) for account X. The default value is 30.	Account->Advanced->UDP Keep Alive Interval(seconds)
account.X.nat.rport (X ranges from 1 to 5.)	0 or 1	It enables or disables NAT Rport feature for account X. **0**-Disabled **1**-Enabled The default value is 0.	Account->Advanced->Rport
account.X.advanced.timer_t1 (X ranges from 1 to 5.)	Float from 0.5 to 10	It configures the session timer T1 (in seconds) for account X. The default value is 0.5.	Account->Advanced->SIP Session Timer T1 (seconds)
account.X.advanced.timer_t2	Float from 2	It configures the session timer T2 (in seconds) for	Account->Advanced->SIP Session Timer T2

Parameter	Permitted Values	Descriptions	Web Setting Path
(X ranges from 1 to 5.)	to 40	account X. The default value is 4.	(seconds)
account.X.advanced.timer_t4 (X ranges from 1 to 5.)	Float from 2.5 to 60	It configures the session timer T4 (in seconds) for account X. The default value is 5.	Account->Advanced->SIP Session Timer T4 (seconds)
account.X.conf_type (X ranges from 1 to 5.)	0 or 2	It configures the conference type for account X. **0**-Local Conference (Conferences are set up on the IP phone locally). **2**-Network Conference (Conferences are set up by the server). The default value is 0.	Account->Advanced->Conference Type
account.X.conf_uri (X ranges from 1 to 5.)	SIP URI within 511 characters	It configures the network conference URI for account X. The default value is blank. **Note**: It works only if the value of the parameter "account.X.conf_type" is set to 2 (Network Conference).	Account->Advanced->Conference URI
account.X.sip_server_type (X ranges from 1 to 5.)	0, 2, 4 or 6	It configures the type of the SIP server for account X. **0**-Default **2**-BroadSoft	

Parameter	Permitted Values	Descriptions	Web Setting Path
		4-Cosmocom **6**-UCAP The default value is 0.	
account.X.unregister_on_reboot (X ranges from 1 to 5.)	0 or 1	It enables or disables the IP phone to first unregister the account X, and then re-register the account X after rebooting the IP phone. **0**-Disabled **1**-Enabled The default value is 0.	
account.X.sip_trust_ctrl (X ranges from 1 to 5.)	0 or 1	It enables or disables the IP phone to only accept the message from the trusted server for account X. **0**-Disabled **1**-Enabled The default value is 0.	
account.X.codec.Y.enable (X ranges from 1 to 5. Y ranges from 1 to 9.)	0 or 1	It enables or disables the specified codec for account X. **0**-Disabled **1**-Enabled **Example**: account.1.codec.1.enable = 1	Account->Codec

Parameter	Permitted Values	Descriptions	Web Setting Path
		This means that the codec PCMU is enabled on the phone. The default value is: When Y=1, the default value is 1; When Y=2, the default value is 1; When Y=3, the default value is 0; When Y=4, the default value is 0; When Y=5, the default value is 1; When Y=6, the default value is 1; When Y=7, the default value is 0; When Y=8, the default value is 0; When Y=9, the default value is 0.	
account.X.codec.Y.payload_type (X ranges from 1 to 5. Y ranges from 1 to 9.)	PCMU, PCMA, G723_53, G723_63, G729, G722, G726-32, iLBC_13_3, iLBC_15_2	It configures the payload type of the specified codec for account X. **Example**: account.1.codec.1.payload_type = PCMU The default value is: When Y=1, the default value is PCMU; When Y=2, the default value is PCMA; When Y=3, the default value is G723_53;	Account->Codec

Parameter	Permitted Values	Descriptions	Web Setting Path
		When Y=4, the default value is G723_63;	
		When Y=5, the default value is G729;	
		When Y=6, the default value is G722;	
		When Y=7, the default value is G726-32;	
		When Y=8, the default value is iLBC_13_3;	
		When Y=9, the default value is iLBC_15_2;	
account.X.codec.Y.priority (X ranges from 1 to 5. Y ranges from 1 to 9.)	Integer from 0 to 10	It configures the priority of the enabled codec for account X. **Example**: account.1.codec.1.priority = 2 This means that the priority of the codec PCMU is 2. The default value is: When Y=1, the default value is 2; When Y=2, the default value is 3; When Y=3, the default value is 4; When Y=4, the default value is 0; When Y=5, the default value is 4; When Y=6, the default value is 1; When Y=7, the default value is 0; When Y=8, the default value is 0;	Account->Codec

Parameter	Permitted Values	Descriptions	Web Setting Path
account.X.codec.Y.rtpmap (X ranges from 1 to 5. Y ranges from 1 to 9.)	Integer 0 to127	It configures rtpmap of the audio codec for account X. **Example**: account.1.codec.1.rtpmap = 0 The default value is: When Y=1, the default value is 0; When Y=2, the default value is 8; When Y=3, the default value is 4; When Y=4, the default value is 4; When Y=5, the default value is 18; When Y=6, the default value is 9; When Y=7, the default value is 2; When Y=8, the default value is 97; When Y=9, the default value is 97.	
account.X.dnd.enable (X ranges from 1 to 5.)	0 or 1	It enables or disables DND feature for account X. **0**-Disabled **1**-Enabled The default value is 0.	Phone->Features->LineX->DND->DND
account.X.dnd.on_code	String within 32	It configures the DND on code to activate the server-side DND feature for account X. The IP phone	Phone->Features->LineX->DND->On Code

Parameter	Permitted Values	Descriptions	Web Setting Path
(X ranges from 1 to 5.)	characters	will send the DND on code to the server when the user activates the DND feature for account X. The default value is blank.	
account.X.dnd.off_code (X ranges from 1 to 5.)	String within 32 characters	It configures the DND off code for account X. The IP phone will send the DND off code to the server when the user deactivates the DND feature for account X. The default value is blank.	Phone->Features->LineX->DND->Off Code
account.X.always_fwd.enable (X ranges from 1 to 5.)	0 or 1	It enables or disables always forward feature for account X. **0**-Disabled **1**-Enabled The default value is 0.	Phone->Features->LineX->Forward->Always
account.X.always_fwd.target (X ranges from 1 to 5.)	String within 32 characters	It configures the target number of always forward feature for account X. The default value is blank.	Phone->Features->LineX->Forward->Always->Target
account.X.always_fwd.off_code (X ranges from 1 to 5.)	String within 32 characters	It configures always forward off code to deactivate the server-side always forward feature for account X. The IP phone will send the always forward off code and the pre-configured target number to the server when the user deactivates always forward feature for account X.	Phone->Features->LineX->Forward->Always->Off Code

Parameter	Permitted Values	Descriptions	Web Setting Path
		The default value is blank.	
account.X.always_fwd.on_code (X ranges from 1 to 5.)	String within 32 characters	It configures the always forward on code to activate the server-side always forward feature for account X. The IP phone will send the always forward on code and the pre-configured target number to the server when the user activates always forward feature for account X. The default value is blank.	Phone->Features->LineX->Forward->Always->On Code
account.X.busy_fwd.enable (X ranges from 1 to 5.)	0 or 1	It enables or disables busy forward feature for account X. **0**-Disabled **1**-Enabled The default value is 0.	Phone->Features->LineX->Forward->Busy
account.X.busy_fwd.target (X ranges from 1 to 5.)	String within 32 characters	It configures the target number of busy forward feature for account X. The default value is blank.	Phone->Features->LineX->Forward->Busy->Target
account.X.busy_fwd.off_code (X ranges from 1 to 5.)	String within 32 characters	It configures the busy forward off code to deactivate the server-side busy forward feature for account X. The IP phone will send the busy forward off code and the pre-configured target number to the server when	Phone->Features->LineX->Forward->Busy->Off Code

Parameter	Permitted Values	Descriptions	Web Setting Path
		the user deactivates busy forward feature for account X. The default value is blank.	
account.X.busy_fwd.on_code (X ranges from 1 to 5.)	String within 32 characters	It configures the busy forward on code to activate the server-side busy forward feature for account X. The IP phone will send the busy forward on code and the pre-configured target number to the server when the user activates busy forward feature for account X. The default value is blank.	Phone->Features->LineX->Forward->Busy ->On Code
account.X.timeout_fwd.enable (X ranges from 1 to 5.)	0 or 1	It enables or disables no answer forward feature for account X. **0**-Disabled **1**-Enabled The default value is 0.	Phone->Features->LineX->Forward->No Answer
account.X.timeout_fwd.target (X ranges from 1 to 5.)	String within 32 characters	It configures the target number of the no answer forward feature for account X. The default value is blank.	Phone->Features->LineX->Forward->No Answer->Target
account.X.timeout_fwd.timeout (X ranges from 1 to 5.)	Integer from 0 to 20	It configures ring times (N) to wait before forwarding incoming calls for account X. Incoming calls will be forwarded when it is not	Phone->Features->LineX->Forward->No Answer->After Ring Time(seconds)

Parameter	Permitted Values	Descriptions	Web Setting Path
		answered after N*6 seconds. The default value is 0.	
account.X.timeout_fwd.off_code (X ranges from 1 to 5.)	String within 32 characters	It configures the no answer forward off code to deactivate the server-side no answer forward feature for account X. The IP phone will send the no answer forward off code and the pre-configured target number to the server when the user deactivates no answer forward feature for account X. The default value is blank.	Phone->Features->LineX->Forward->No Answer->Off Code
account.X.timeout_fwd.on_code (X ranges from 1 to 5.)	String within 32 characters	It configures the no answer forward on code to activate the server-side no answer forward feature for account X. The IP phone will send the no answer forward on code and the pre-configured target number to the server when the user activates no answer forward feature for account X. The default value is blank.	Phone->Features->LineX->Forward->No Answer->On Code

The following table lists configuration parameters that are integrated with BroadSoft platform. For more information on BroadSoft features, refer to *Yealink_W52P_IP_DECT_Phones_Deployment_Guide_for_BroadSoft_UC-One_Environment*.

Parameter	Permitted Values	Descriptions	Web Setting Path
bw.enable	0 or 1	It enables or disables BroadSoft features for IP phones. 0-Disabled 1-Enabled The default value is 0 for the neutral firmware version (x.73.0.x), and 1 for the UC-One firmware version (x.73.193.x). It takes effect after a reboot.	
sip.authentication_for_xsi	0 or 1	It configures the authentication method the IP phone uses for XSI access. 0- User Login Credentials for XSI Authentication 1-SIP Credentials for XSI Authentication If it is set to 0, the IP phone uses the XSI user ID and password for XSI authentication. If it is set to 1, the IP phone uses the XSI user ID, the register name and password of the SIP account for XSI authentication. The default value is 0.	Contacts->Network Directory->XSI->Allow SIP Authentication for XSI

Parameter	Permitted Values	Descriptions	Web Setting Path
xsi.user	String	It configures the user name provided on the Xtended Services Platform server. The default value is blank.	Contacts->Network Directory->XSI->XSI Username
xsi.password	String	It configures the password provided on the Xtended Services Platform server. The default value is blank. **Note**: It works only if the value of the parameter "sip.authentication_for_xsi" is set to 0 (User Login Credentials for XSI Authentication)	Contacts->Network Directory->XSI->XSI Password
xsi.host	within 511 characters	It configures the access URL of the Xtended Services Platform server. The default value is blank.	Contacts->Network Directory->XSI->XSI Server
Xsi.port	Integer from 1 to 65535	It configures the access port of the Xtended Services Platform server. **Example**: xsi.port = 80 The default value is 80.	Contacts->Network Directory->XSI->XSI Port
xsi.server_type	"http" or "https"	It configures the access protocol of the Xtended Services Platform server. **Example**:	Contacts->Network Directory->XSI->XSI Server Type

Parameter	Permitted Values	Descriptions	Web Setting Path
		xsi.server_type = http The default value is http.	
bw_phonebook.personal_enable	0 or 1	It enables or disables the Personal item to be added to the BroadSoft phonebook. **0**-Disabled **1**-Enabled The default value is 0.	Contacts->Network Directory->Directory->Personal Enable
bw_phonebook.personal_displayname	String within 99 characters	It configures the display name on the LCD screen for the personal directory. The default value is Personal.	Contacts->Network Directory->Directory->Personal Display Name
bw_phonebook.group_enable	0 or 1	It enables or disables the Group item to be added to the BroadSoft phonebook. **0**-Disabled **1**-Enabled The default value is 1.	Contacts->Network Directory->Directory->Group Enable
bw_phonebook.group_displayname	String within 99 characters	It configures the display name on the LCD screen for the group directory. The default value is Group.	Contacts->Network Directory->Directory->Group Display Name
bw_phonebook.group_common_enable	0 or 1	It enables or disables the GroupCommon item to be added to the BroadSoft phonebook.	Contacts->Network Directory->Directory->GroupCommon Enable

Parameter	Permitted Values	Descriptions	Web Setting Path
		0-Disabled **1**-Enabled The default value is 0.	
bw_phonebook.group_common_displayname	String within 99 characters	It configures the display name on the LCD screen for the group common directory. The default value is GroupCommon.	Contacts->Network Directory->Directory->GroupCommon Display Name
bw_phonebook.enterprise_enable	0 or 1	It enables or disables the Enterprise item to be added to the BroadSoft phonebook. **0**-Disabled **1**-Enabled The default value is 0.	Contacts->Network Directory->Directory->Enterprise Enable
bw_phonebook.enterprise_displayname	String within 99 characters	It configures the display name on the LCD screen for the enterprise directory. The default value is Enterprise.	Contacts->Network Directory->Directory->Enterprise Display Name
bw_phonebook.enterprise_common_enable	0 or 1	It enables or disables the EnterpriseCommon item to be added to the BroadSoft phonebook. **0**-Disabled **1**-Enabled The default value is 0.	Contacts->Network Directory->Directory->EnterpriseCommon Enable

Parameter	Permitted Values	Descriptions	Web Setting Path
bw_phonebook.enterprise_common_displayname	String within 99 characters	It configures the display name on the LCD screen for the enterprise common directory. The default value is EnterpriseCommon.	Contacts->Network Directory->Directory->EnterpriseCommon Display Name
bw_phonebook.update_interval	Integer from 60 to 86400	It configures the interval (in minutes) for the phone to update the data of the BroadSoft phonebook. The default value is 1440.	Contacts->Network Directory->Directory->Update Time Interval (60~86400)(Minutes)
bw_phonebook.call_log_enable	0 or 1	It enables or disables network call log feature. **0**-Disabled **1**-Enabled The default value is 0.	Contacts->Network Directory->Directory->Network Call Log
bw.feature_key_sync	0 or 1	It enables or disables the feature key synchronization. **0**-Disabled **1**-Enabled The default value is 0.	Phone->Features->Feature Synchronization

The following parameters are not applicable to IP phones running firmware version 73 or later, so the description of these parameters has been deleted in this guide.

network.snmp.enable

network.snmp.port

network.snmp.trust_ip

account.X.backup_outbound_host

account.X.backup_outbound_port

account.X.enable_signal_encode

account.X.signal_encode_key

Time Zones

Time Zone	Time Zone Name
−12	
−11:30	
−11	Samoa
−10:30	
−10	US-Hawaii-Aleutian、US-Alaska-Aleutian
−9:30	
−9	US-Alaska Time
−8:30	
−8	Canada(Vancouver,Whitehorse), Mexico(Tijuana,Mexicali), US-Pacific Time
−7:30	
−7	Canada(Edmonton,Calgary), Mexico(Mazatlan,Chihuahua), US-MST no DST, US-Mountain Time
−6:30	
−6	Canada-Manitoba(Winnipeg), Chile(Easter Islands), Mexico(Mexico City,Acapulco), US-Central Time
−5:30	
−5	Bahamas(Nassau), Canada(Montreal,Ottawa,Quebec), Cuba(Havana), US-Eastern Time
−4:30	Venezuela(Caracas)
−4	Canada(Halifax,Saint John), Chile(Santiago), Paraguay(Asuncion), UK(Falkland Islands), UK-Bermuda(Bermuda), Trinidad&Tobago
−3:30	Canada-New Foundland(St.Johns)
−3	Argentina(Buenos Aires), Brazil(DST), Brazil(no DST), Denmark-Greenland(Nuuk)
−2:30	
−2	Brazil(no DST)
−1:30	
−1	Portugal(Azores)
−0:30	

Time Zone	Time Zone Name
0	Denmark-Faroe Islands(Torshavn), GMT, Greenland, Ireland(Dublin), Morocco, Portugal(Lisboa,Porto,Funchal), Spain-Canary Islands(Las Palmas),UK(London)
+0:30	
+1	Albania(Tirane), Austria(Vienna), Belgium(Brussels), Caicos, Chad, Croatia(Zagreb), Czech Republic(Prague), Denmark(Kopenhagen), France(Paris), Germany(Berlin), Hungary(Budapest), Italy(Rome), Luxembourg(Luxembourg), Macedonia(Skopje), Namibia(Windhoek), Netherlands(Amsterdam)
+1:30	
+2	Estonia(Tallinn), Finland(Helsinki), Gaza Strip(Gaza), Greece(Athens), Israel(Tel Aviv), Jordan(Amman), Latvia(Riga), Lebanon(Beirut), Moldova(Kishinev), Romania(Bucharest), Russia(Kaliningrad), Syria(Damascus), Turkey(Ankara), Ukraine(Kyiv, Odessa)
+2:30	
+3	East Africa Time, Iraq(Baghdad), Russia(Moscow)
+3:30	Iran(Teheran)
+4	Armenia(Yerevan), Azerbaijan(Baku), Georgia(Tbilisi), Kazakhstan(Aktau), Russia(Samara)
+4:30	Afghanistan
+5	Kazakhstan(Aqtobe), Kyrgyzstan(Bishkek), Pakistan(Islamabad), Russia(Chelyabinsk)
+5:30	India(Calcutta)
+5:45	
+6	Kazakhstan(Astana, Almaty), Russia(Novosibirsk,Omsk)
+6:30	
+7	Russia(Krasnoyarsk), Thailand(Bangkok)
+7:30	
+8	China(Beijing)、Singapore(Singapore)、Australia(Perth)
+8:30	
+9	Korea(Seoul)、Japan(Tokyo)
+9:30	Australia(Adelaide), Australia(Darwin)
+10	Australia(Brisbane), Australia(Hobart), Australia(Sydney,Melboume,Canberra), Russia(Vladivostok)

Time Zone	Time Zone Name
+10:30	Australia(Lord Howe Islands)
+11	New Caledonia(Noumea)
+11:30	
+12	New Zealand(Wellington, Auckland)
+12:30	
+12:45	New Zealand(Chatham Islands)
+13	Tonga(Nukualofa)

Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocsFeedback@yealink.com.