

Yealink W52P Auto Provisioning User Guide

Version 10.20 Jan 2012

Table of Contents

Table of Contents	iii
Introduction	5
Getting Started	7
Configuring a Provisioning Server	7
Configuring a TFTP Server	7
Obtaining Configuration Files	9
Managing Configuration Files	10
Editing the Common CFG File	10
Editing the MAC-Oriented CFG File	13
Encrypting Configuration Files	15
Preparing Resource Files	15
Customizing the Replace Rule File	15
Customizing the Local Contact File	17
Uploading the Firmware File	18
Obtaining Provisioning Server Address	21
Plug and Play (PnP)	21
DHCP Options	22
Phone Flash	25
Configuring the Updating Mode	26
Downloading Configuration Files	31
Troubleshooting	33
Appendix	35
Glossary	35
Configuring a FTP Server	
Configuring a HTTP Server	
Configuring a DHCP Server	42
Description of Configuration Parameters in CFG Files	

Introduction

Yealink 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.

This guide shows you 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 download and are configured by default to use TFTP (Trivial File Transfer Protocol).

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

Getting Started

This chapter shows you how to get ready for auto provisioning. The topics include:

- Configuring a Provisioning Server
- •
- Obtaining Configuration Files
- Managing Configuration Files
- Preparing Resource Files

Configuring a Provisioning Server

Yealink W52P IP DECT phones support using FTP, TFTP, HTTP and HTTPS protocols to download configuration files. You should configure a provisioning server for provisioning purpose. To download the configuration files using TFTP protocol, a TFTP server should be configured as the provisioning server. The following section introduces you how to configure a TFTP server.

For more information about configuring a FTP server or a HTTP server, refer to Configuring a FTP Server on page 36 and Configuring a HTTP Server on page 39.

Configuring a TFTP Server

We recommend that you use 3CDaemon or TFTPD32 application to configure a TFTP server. 3CDaemon and TFTPD32 are free applications for Windows platform. You can download the 3CDaemon application at:

http://www.oldversion.com/3Com-Daemon.html and TFTPD32 application at: http://tftpd32.jounin.net/.

Take 3CDaemon application as an example in this section.

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 assign the permissions: read, write, and modify files to the user or the group.

Administrators (VANSTD80\Administrators) CREATOR 0\VNER							
🔢 Everyone							
💈 Hill, James (jahill@my	servername	.com]					
SYSTEM				~			
<			>				
	4	\ <u>d</u> d	Bemove	•			
Permissions for Everyone		Allow	Deny				
Full Control				^			
Modify							
Read & Execute		~					
List Folder Contents		~					
Read							
Write							
Consist Dormissions				~			
For special permissions or fo click Advanced.	or advanced	settings,	Advance	d			

To configure a TFTP server:

- 1. Double click the 3CDaemon.exe to run the application.
- 2. Select Configure TFTP Server.

		1			
TFTP Server	Start Time	Peer	Bytes	Status	
	Feb 28, 2012 16:06:20) local	0	Listening for TFTP requests on IP address: 192.168.133.1, Port 69	
	Feb 28, 2012 16:06:20 Feb 28, 2012 16:06:20	local	0	Listening for IFIF requests on IF address, 102, 100, 100, 1, Fort 69 Listening for TFTP requests on TP address; 10,2, 11, 126, Port 69	
C. TRTD. C.	100 20, 2012 10:00:20	, rocar		instanting for first requests on in data cast to c. fit ico, for too	
nrigure frir Server					
STUP					
ck here to stop it.					
geing to Tftpd log					
Click to stop.					
Not debugging.					
Click to start.					
- 1					
Clear list.					
4.65					

3. Click to locate the TFTP root directory you have configured from the local system.

300 3CDaemon		
<u> </u> Eile <u>V</u> iew <u>H</u> elp		
TFTP Server	Start Time Peer Bytes Status	
Configure TFTP Server	Pab 24, 2012 08:59:47 local 0 Listening for TTP requests on IP address: 192:168 103.1, Fort 69 Fab 24, 2012 08:59:47 local 0 Listening for TTP requests on IP address: 192:168 103.1, Fort 69 Fab 24, 2012 08:59:47 local 0 Listening for TTP requests on IP address: 10.2.11.126, Fort 69	
T	3CDaemon Configuration	
TFTP Server is started. Click here to stop it.	FTP Profiles Syslog Configuration General Configuration TFTP Configuration	
Logging to Tftpd log. Click to stop.	Create directory names in incoming file re	
Not debugging. Click to start.	Upload/Bownload E: Matoplato Provision Mano	
Clear list.	Natings retries 10 Interframe transmission 0	
View Log/Debug files.		

4. Click Confirm to finish configuring the TFTP server.

The server URL "tftp://IP/" (Here "IP" means the IP address of your local system, for example, "tftp://192.168.1.100/") can be used for TFTP download.

Obtaining Configuration Files

Before the provisioning process, you need to obtain the configuration files of the phone. You can ask the Yealink field application engineer or the distributor for the 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. The phone tries to download these two configuration files from the provisioning server during the provisioning process.

The MAC-Oriented CFG file is only effectual for the specific phone. It uses the 12-digit MAC address of the phone as the file name. For example, if the MAC address of the phone is 0015651130F9, then the MAC-Oriented CFG file name must be 0015651130F9.cfg. However, the Common CFG file is effectual for all phones of the same phone model. It uses the fixed name "y00000000025.cfg".

Gathering the Following Information

You also need to gather the following information in advance:

MAC Address: The unique 12-digit serial number of the phone that you want to provision separately. You can obtain it from the bar code at the back of the base station.

Registration Information: The SIP credentials such as user name, password and the address of the account's registration server. Ask your system administrator for the information of SIP accounts you want to register. Configure the registration information in the MAC-Oriented file to register SIP accounts on a per-phone basis.

Managing Configuration Files

Auto provisioning allows the phones to be configured automatically via downloading the Common CFG file (y00000000025.cfg) and MAC-Oriented CFG file. You need to edit your configuration files and store them to the root directory of the TFTP server before provisioning.

When editing the configuration files, remember the following:

- Configurations in the configuration files override those stored in the phone's flash memory.
- The .cfg extension of the configuration files must be in lowercase.
- Each line in a configuration file 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 (y00000000025.cfg) contains configuration parameters which apply to all phones of the same phone model.

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

\square	Common. cfg X
	0
	#'version:1.0.0.1
2	
;	##File header "#!version:1.0.0.1" can not be edited or deleted.##
ļ	******
đ	## Network ##
,	***************************************
(
5	#Configure the WAN port type; 0-DHCP (default), 1-PPPoE, 2-Static IP Address;
10	#Require reboot;
1.	network.internet_port.type =
12	
1:	#Configure the static IP address, submask, gateway, primary DNS server (202.101.103.55 by
1,	#Require reboot;
1	network.internet_port.ip =
11	network.internet_port.mask =
1'	network.internet_port.gateway =
10	network.primary_dns =
19	network.secondary_dns =
21	
2. 	#Enable of disable the VLAN of WAN port; U-Disabled (default), 1-Enabled;
	#Require report;
	network.vian.internet_port_enable =
21	"Configure the VIAN ID, it renges from 0 to 4004, the default value is 0
21	#Demilyare the view iD, it langes from 0 to 4094, the default value is 0.
2'	meturic lebut,
-	necwork.vran.incernec_pore_vra -

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 "y00000000025.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:

######	#######################################	<i>t##########</i> #
##	Common CFG File	##
#######	#######################################	<i>!#########</i> #

#!version:1.0.0.1

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

#Configure the WAN port type. #Require 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 =

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

network.port.http =

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

network.port.https =

#Configure the recovery mode.

recovery_mode.getwayip=

recovery_mode.phone_ip=

recovery_mode.server_ip=

recovery_mode.netmask=

#Configure the URL of the auto provisioning server.

auto_provision.server.url =

#Configure the username and password for downloading.

auto_provision.server.username =

auto_provision.server.password =

#Configure the AES key (16 characters) for decrypting the Common CFG file.

auto_provision.aes_key_16.com =

#Configure the AES key (16 characters) for decrypting the MAC-Oriented CFG file.

auto_provision.aes_key_16.mac =

#Configure the pin code of the base station.

base.pin_code=

#Enable or disable the 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 which are only effectual for the specific phone.

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

```
MAC-Oriented.cfg ×
  #!version:1.0.0.1
  ##File header "#!version:1.0.0.1" can not be edited or deleted.##
  Account1 Settings
  #Enable or disable the account 1; 0-Disabled (default), 1-Enabled;
account.1.enable =
 #Configure the label displayed on the LCD screen for account 1. account.1.label =
15 #Configure the display name of account 1.
  account.1.display_name =
18 #Configure the username and password for register authentication.
19 account. 1. auth_name =
20 account.1.password =
22 #Configure the register user name.
23 account.1.user_name =
25 #Configure the SIP server address.
26 account.1.sip_server_host =
28 #Specify the port for the SIP server. The default value is 5060.
29 account. 1. sip_server_port =
31 #Enable or disable to use the outbound proxy server; 0-Disabled (default), 1-Enabled;
```

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 in the MAC-Oriented CFG file:

account.1.enable =

#Configure the label of account1 which will display on the 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 SIP server address and port (5060 by default). account.1.sip_server_host = account.1.sip_server_port = #Enable or disable the anonymous call feature; 0-Disabled (default), 1-Enabled; account.1.anonymous call = #Configure the on code and off code of the anonymous call feature. account.1.anonymous_call_oncode = account.1.anonymous_call_offcode = #Enable or disable the reject anonymous call feature; 0-Disabled (default), 1-Enabled; account.1.reject_anonymous_call = #Configure the on code and off code of the reject anonymous call feature.

account.1.anonymous_reject_oncode =

account.1.anonymous_reject_offcode =

Configure the DND feature on account1.

account.1.dnd.enable =

account.1.dnd.on_code =

account.1.dnd.off_code =

#Configure the 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 =

Encrypting Configuration Files

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

The AES keys must be configured on the phone before the auto provisioning process. You can configure the AES keys via web user interface at the path: **Phone**->**Auto Provision**.

Preparing Resource Files

When configuring some specified features, you need to prepare the required resource files beforehand. Store the resource files to the root directory of the TFTP server and specify the access URLs of the resource files in the configuration files. The phone will download the resource files and update the corresponding settings when reading the URLs from the configuration files.

The following sections introduce you how to prepare common resource files and specify the access URLs of the resource files.

Yealink provides some template resource files for customizing the specified features.

Customizing the Replace Rule File

You can create replace rules directly in the configuration files, or create multiple replace rules using the supplied template replace rule file (*DialPlan.xml*). When the phone downloads the replace rule file, the existing replace rules on the phone will be overwritten. You can create at most 20 replace rules for the phone.

When editing the template replace rule file, remember 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>.
- 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 comma.
- Do not modify the file name (DialPlan.xml).

-	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: "12 x " would match "12 1 ", "12 2 ", "12 3 ", "12 a ", etc.
-	Numeric ranges are allowed within the brackets: Digit "-" Digit. Example: "[5-7]" would match the number" 5 ", " 6 " or " 7 ".
0	The square bracket "[]" 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: "9([5-7]) (.)", Replace: "5\$2".
	When you dial out "96123" on your phone, the phone will replace the number as "5123" and then dial out. "\$2" means the characters in the second parenthesis, that is, "123".

The basic expression syntax of the replace rule is listed in the following table:

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 starting 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 leaving it blank or entering an invalid value, 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 a 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, you need to store the file to the root directory of the TFTP server, and then specify the access URL of the replace rule file in the configuration file. The parameter "*dialplan_replace_rule.url*" in the Common CFG file is used to specify the access URL of the replace rule file. Enter the URL in the field as following:

#########	***************************************	##
##	Configure the access URL of the replace rule file	##
#########	****	##
dialplan_repla	ce_rule.url = tftp://192.168.1.100/DialPlan.xml	

Customizing the 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 create multiple contacts using the supplied template local contact files (*contact_handsetx_list.xml* or *contact_handsetx_list.csv*).

When editing the template local contact file, remember 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>.
- The name of the contact file contact_handsetx_list.xml or contact_handsetx_list.csv should be modified according to your requirement ("x" ranges from 0-4 and corresponds to internal handset number 1-5. For example, if you want download this contact file to handset 1, the contact file name must be contact_handset0_list.xml or contact_handset0_list.csv).

To customize a local contact file:

- 1. Open the template file 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.
- Rename the file (e.g. contact_handset1_list.xml or contact_handset1_list.csv for handset 2).

The following shows an example of the contact_handset1_list.xml 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 the local contact file, you need to store the file to the root directory of the TFTP server, and then specify the access URL of the local contact file in the configuration file. The parameter "*handset.X.contact_list.url*" in the Common CFG file is used to specify the access URL of the local contact file. Enter the URL in the field as following:

#########	*######################################	ŧ##
##	Configure the access URL of the local contact file	##
#########	*######################################	ŧ##
handset.X.cont	act_list.url = tftp://192.168.1.100/contact_handset1_list.xml	

Uploading the Firmware File

You can update the firmware of the base station manually via web user interface. You can also automatically update the firmware of mass base stations via auto provisioning. Obtain the latest firmware file (e.g. 25.10.0.19.rom) from the Yealink FAE. Store the firmware file to the root directory of the TFTP server, and then specify the access URL of this firmware file in the configuration file.

The parameter "*firmware.url*" in the Common CFG file is used to specify the access URL of the firmware file. Enter the URL in the field as following:

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

firmware.url = tftp://192.168.1.100/25.10.0.19.rom

Obtaining Provisioning Server Address

To connect to the provisioning server and download the configuration files, the phone should obtain the provisioning server address beforehand. Yealink W52P IP DECT phones support obtaining the provisioning server address via three ways: Plug and Play (PnP), DHCP options and phone flash.

When the phone boots up, it will go by the three ways mentioned above to try to obtain the provisioning server address. The priority of ways for obtaining the provisioning server address is: PnP-->DHCP options (Custom option-->option 66 -->option 43) -->phone flash.

This chapter describes how to obtain the provisioning server address using each way and configure the updating modes for triggering the auto provisioning process in detail. The topics include:

- Plug and Play (PnP)
- DHCP Options
- Phone Flash
- Configuring the Updating Mode

Plug and Play (PnP)

Yealink W52P IP DECT phones support obtaining the provisioning server address from the PnP server. To obtain the provisioning server address from the PnP server, make sure the PnP feature is enabled.

The phone can only obtain the provisioning server address from the PnP server during bootup by default.

Make sure the provisioning server address is preconfigured on the PnP server.

To enable the PnP feature via web user interface:

1. Click on Phone->Auto Provision.

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

💿 On 🔘 Off
🔿 On 💿 Off
••••
•••••
•••••

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

To obtain the provisioning server address from the PnP server:

1. Reboot the phone.

The phone will send SIP SUBSCRIBE messages to a multicast address to request the provisioning server address during bootup. Any PnP server understanding the messages will response with a SIP NOTIFY message. The provisioning server address is contained in the message body. The phone will strip out the provisioning server address in the message.

You can monitor the request and response messages using a WinPcap tool. The following figure shows the example messages of obtaining the TFTP server address from the PnP server:

📶 Realtek	10/100/1000 Etherne	t NIC	(Microsoft's P	acket Scheduler)	[Wireshark 1.6.7	(SVM Rev 41973 from /trunk-1.	6)] 🔤 🗖 🗙
Ele Edit Vie	ew Go Capture Analyze	e <u>S</u> tatistics Telephony <u>T</u>	ools Internals Help					
		: 🖴 🔍 🔶 🧄 🙆	중 盘 🗐 🖬 Q	ର୍ ଉ 🖭 🎆	: 🕅 🥵 % 💢			
Filter: (sip#	whip.addr==10.2.10.182) &&	(ip. sre != 10.2.1.23)	Y Expression	Clear Apply				
No. Tine		Source	Destination	Protocol	Length Info			
1579 58.4	150035	10.2.10.182	224.0.1.75	SIP	555 Request:	SUBSCRIBE sip:MACO01	5653828d80224.0.1.75	
1580 58.4	162058	10.2.1.96	10.2.10.182	SIP	507 Request:	NOTIFY S1p:MACUU1565	382808010.2.10.182:5059	
1581 58.4	10/819	10.2.3.154	10.2.10.182	SIP	509 Status: 2	DU OK	2020-00010 2 10 102-5050	
1501 58 8	259791	10.2.0.194	10.2.1.96	STP	327 Status: 2	NOTIFY STPREACOULSUS	382808010.2.10.182.3039	
1593 58.9	276669	10.2.3.154	10.2.10.182	SIP	509 Request :	NOTIEY S10:MAC001565	3828d8010.2.10.182:5059	
1605 59.5	29031	10.2.10.182	10.2.3.154	SIP	328 Status: 2	00 OK		
1617 60.1	L87542	10.2.10.182	10.2.3.154	SIP	328 Status: 2	00 OK		
■ Frame 151 ■ Ethernet ■ S02.1Q V ■ Internet ■ User Dat: ■ Request ■ Rescalar ■ V1a: ■ V1a: ■ V1a: ■ V1a: B From ■ SII SII ■ SII ■ SI	BU: SOZ Bytes on with II, SPC: Cfsc.40:01 Hrtual LuA, PRI: O, Protocol Version 4, Agram Protocol, SPC: Header SIP/J.CV upp SIP/J.CV upp	re (4036 bfts), 507 dis55 (cf:30441401 CF1: 0, 10: 77 src: 10.2.1.66 (10 Port: sfp (1060), 0 execol1655382840840.2 .96:5060; branch=29kG .1.96 B550b6523ba4587d24267 Bd08224.0.1.75; tag=42 accol15653828d08224.0 10.182	byces captured (405 4155), bst: xlameru st Port: sdb (5039) .10.182:5059 s1P/2. 4bk-d29a8356bb627ba a7dd465 e0ff942d30 .0.1.75 037973 1.73	6 bfts) e_38:28:d8 (00 .10.182 (10.2. 0 4587d24267a7dd	0:15:65:38:28:d8) .10.182) d465:rport			
Sei	quence Number: 53621	1						
Met	thod: NOTIFY							
Max-	Forwards: 70							
Subse	cription-state: terr	=inaceu;reason=nores	ource					
Conta	ent_Type: annlicatio	on/url						
Conte	ent-Length: 24	any an i						
E Message	e Body							
http	://10.2.1.96:80/pro	v						

DHCP Options

Yealink W52P IP DECT phones support obtaining the provisioning server address by

detecting DHCP options.

You can configure the phone to obtain the provisioning server address from a custom DHCP option, or the phone will automatically detect the option 66 or option 43. 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.

To obtain the provisioning server address via DHCP options, configure a DHCP server beforehand and make sure that the DHCP option is set properly.

For more information about configuring a DHCP server, refer to Configuring a DHCP Server on page 42.

To configure a custom 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.

Auto	Provision	
	PNP	🔿 On 💿 Off
	DHCP Option	⊙ On ○ Off
	Custom Option(128~254)	128
	DHCP Option Value	
	Provisioning Server	
	User Name	
	Password	••••
	Common AES Key	•••••
	MAC-Oriented AES Key	•••••

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

If you only mark the **On** radio box in the **DHCP Option** field and leave the **Custom Option (128~254)** field blank, the phone will automatically detect option 66 or option 43.

A valid Custom Option value is from 128 to 254. The custom option must be in accordance with the one defined when configuring the DHCP server.

To enable the Power On mode via web user interface:

In order to obtain the provisioning server address using DHCP options during bootup, make sure the Power On mode is activated before rebooting the phone.

1. Click on Phone->Auto Provision.

2. Mark the On radio box in the Check New Config field.

Check New Config	💿 On 🔘 Off
Repeatedly	🔿 On 💿 Off
Interval (minutes)	60
Weekly	🔘 On 💿 Off
Time	02 : 00 03 : 00
Day of week	Sunday Monday Tuesday Wednesday Thursday Friday Saturday Autoprovision Now

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

To obtain the provisioning server address via DHCP options:

1. Reboot the phone.

The phone will send DHCP request with DHCP options to request the provisioning server address and receive DHCP response during bootup. The provisioning server address will be embedded inside the DHCP options of the DHCP response received.

You can monitor the request and response messages using a WinPcap tool. The following figure shows the example messages of obtaining the TFTP server address via the custom DHCP option:

<pre>Ele Edit yew Go Capture Analyze Statistics Telephony Tools Internais Help Filter: dip libootp Filter: dip libootp Expression Clear Apply No. Time Source Destination Protocol Length Info 14 17, 367476 0.0.0.0 255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x88e96872 15 18.137781 10.2.8.105 10.2.8.106 DHCP 342 DHCP Offer - Transaction ID 0x88e96872 17 18.178902 10.2.8.105 10.2.8.106 DHCP 342 DHCP AKK - Transaction ID 0x88e96872 17 18.178902 10.2.8.105 10.2.8.106 DHCP 342 DHCP AKK - Transaction ID 0x88e96872 17 18.178902 10.2.8.105 10.2.8.106 DHCP 342 DHCP AKK - Transaction ID 0x88e96872 17 18.178902 10.2.8.105 10.2.8.105 (10.2.8.105) DHCP 342 DHCP AKK - Transaction ID 0x88e96872 17 18.178902 10.2.8.105 (10.2.8.105 (10.2.8.105), Dst: 110.2.8.106 (10.2.8.106) B User Datagram Protocol, srcr Port: bootps (67), Dst Port: bootpc (68) Bootstrap Protocol Message type: Boot Reply (2) Hardware type: Ethernet Hardware silength: 6 Hops: 0 Transaction ID: 0x88e96872 Seconds elapsed: 100 B Bootp flags: 0.0.0.0 (0.0.0.0) Vour (client) IP address: 0.0.2.8.106 (10.2.8.106) Next server IP address: 0.0.0.0 (0.0.0.0) Client Mac address I mid0171-for3xon Boot file name not given Magic cookie: State Pack = 255.255.255.05 DHCP B Option: (t-s], 1-4) IP Address Lease Time = 6 hours D option: (t-s], 1-4) IP Address Lease Time = 6 hours D option: (t-s], 1-4) PR Address Lease Time = 6 hours D option: (t-s], 1-4) PR Address Lease Time = 6 hours D option: (t-s], 1-4) PR Address Lease Time = 6 hours D option: (t-s], 1-4) PR Address Lease Time = 6 hours D option: (t-s], 1-4) PR Address Lease Time = 6 hours D option: (t-s], 1-4) PR Address Lease Time = 6 hours D option: (t-s], 1-4) PR Address Lease Time = 6 hours D option: (t-s], 1-4) PR Address Lease Time = 6 hours D option: (t-s], 1-4] PR Address Lease Time = 6 hours D option: (t-s], 1-4] PR Address Lease Time = 6 hours D option: (t-s], 1-4] PR Address Lease Time = 6 hours D option: (t-s], 1-4] PR Address Lease Time = 6 hours D option: (t-s], 1-4] PR Address Lease Time = 6 hou</pre>	File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help Image: Statistics Telephony Iools Ioo	DHCPserver-tftp.pcap [Wireshark	x 1.6.7 (SVN Rev 41973 from /trunk-1.6)]	
Image: Source Destination Protocol Length Info 14 17.967476 0.0.0.0 255.255.255.255.04CP 590 0HCP Discover - Transaction ID 0x88e96872 15 18.137781 10.2.8.105 10.2.8.106 DHCP Discover - Transaction ID 0x88e96872 16 18.177701 0.0.0.0 255.255.255.255.255.255.255.255.255.255	Image: Source Destination Protocol Length Info 14 17.967476 0.0.0.0 255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x88e96872 15 18.137781 10.2.8.105 10.2.8.106 DHCP 342 DHCP Offer - Transaction ID 0x88e96872 16 18.177701 0.0.0.0 255.255.255.255.255.255 DHCP 590 DHCP Request - Transaction ID 0x88e96872 17 18.178902 10.2.8.105 10.2.8.106 DHCP 342 DHCP ACK - Transaction ID 0x88e96872 18 18.137781 0.0.0.0 255.255.255.255.255.255 DHCP 590 DHCP Request - Transaction ID 0x88e96872 18 178902 10.2.8.105 10.2.8.106 DHCP 342 DHCP ACK - Transaction ID 0x88e96872 19 Ethernet IT, Src: Vmware_09:51:fa (00:0c:29:09:51:fa), Dst: Xiamenve_38:28:d8 (00:15:65:38:28:d8) 19 Internet Protocol Version 4, Src: 10.2.8.105 (10.2.8.105), Dst: 10.2.8.106 (10.2.8.106) 19 User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) 19 Bootstrap Protocol Message type: Boot Reply (2) Hardware type: Ethernet Hardware type: Ethernet Hardware type: Ethernet	<u>File Edit View Go Capture Ana</u>	alyze <u>S</u> tatistics Telephon <u>y</u> <u>T</u> ools <u>I</u> nternals <u>H</u> elp	
Filter: ip bootp Expression Clear Apply Expression Clear Apply If 17, 95745 0, 0, 0, 0 255, 255, 255, 255 0HCP 342 DHCP Offer: Transaction ID 0x88e96872 16, 137781 10, 2, 8, 105 10, 2, 8, 106 DHCP 342 DHCP Offer: Transaction ID 0x88e96872 16, 137781 10, 2, 8, 105 10, 2, 8, 106 DHCP State Apply Ethernet II, Src: Ymware-09:51:fa (00:00:29:09:51:fa), Dst: Xiamenve_38:28:d8 (00:15:55:38:28:d8) Internet Protocol Version 4, Src: 10, 2, 8, 105 (10, 2, 8, 105 (10, 2, 8, 105 (10, 2, 8, 106 (10, 2, 8, 106 (10, 2, 8, 106)) Bootstrap Protocol Message type: Boot Reply (2) Hardware type: Ethernet Hardware address length: 6 Hops: 0 Transaction ID: 0x88e96872 Seconds elapsed: 100 Bootp flags: (X0000 (unicat) Client IP address: 0.0, 0, 0 (0, 0, 0, 0) Client IP address: 10.2, 8, 106 (10.2, 8, 106) Next server IP address: 10.2, 8, 106 (10, 2, 8, 105) Relay agent IP address: 0, 0, 0, 0 (0, 0, 0, 0) Client MAC address: xiameve_38:28:d8 (00:15:65:38:28:d8) Client MAC address teap Time = 6 hours Doption: (t=3, 1=4) IP Address Lease Time = 6 hours Doption: (t=38, 1=4) Rebinding time value = 3 hours Doption: (t=28, 1=4) Rebinding time value = 5 hours Doption:	Filter sip bootp Expression Clear Apply No. Time Source Destination Protocol Length Info 14 17,967476 0.0.0.0 255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x88e96872 15 18.137781 10.2.8.105 DHCP 342 DHCP Offer - Transaction ID 0x88e96872 16 18.177701 0.0.0.0 255.255.255 DHCP 590 DHCP Request - Transaction ID 0x88e96872 17 18.177802 10.2.8.106 DHCP 342 DHCP ACK - Transaction ID 0x88e96872 18 Ethernet II, Src: Vmware_09:51:fa (00:0c:29:09:51:fa), Dst: xiamenYe_38:28:d8 (00:15:65:38:28:d8) B B Ethernet Protocol Version 4, Src: 10.2.8.105 (10.2.8.105), Dst: 10.2.8.106 (10.2.8.106) B B User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) B B Bost Datagram Protocol, Sco Reply (2) Hardware type: Ethernet Hardware type: Sco Reply (2) Hardware type: Sco Reply (2)		# = < + + + + 7 ± □ = < < 0, 0, 11 ≝ ⊠ 5 % 12	
No. Time Source Destination Protocol Length Info 14 17,96746 0.0.0.0 255.255.255 DHCP 500 0HCP Discover - Transaction ID 0x88e96872 15 18.137781 10.2.8.105 10.2.8.106 DHCP 342 DHCP Offer - Transaction ID 0x88e96872 15 18.137781 10.2.8.105 10.2.8.106 DHCP 342 DHCP ACK - Transaction ID 0x88e96872 17 18.177802 10.2.8.105 10.2.8.105 DHCP 342 DHCP ACK - Transaction ID 0x88e96872 18 Ethernet II, Src: Vmware_09:51:fa (00:0c:29:09:51:fa), Dst: XiamenYe_38:28:d8 (00:15:65:38:28:d8) Immerret Protocol Version 4, Src: 10.2.8.105 (10.2.8.105), Dst: 10.2.8.106 (10.2.8.106) 19 User Datagram Protocol Message type: Boot Reply (2) Hardware type: Ethernet Hardware type: Ethernet Hardware type: Ithernet Hardware type: Ithernet Hardware type: S0 0.0.0.0 (0.0.0.0) Your (client) P address: 10.2.8.105 (10.2.8.106) Next sage: VP obtion 10: 0x88e96872 Second Playse: 0.0.0.0 (0.0.0.0) Your (client) P address: 0.0.0.0 (0.0.0.0) Your (client) P address: 0.0.0.0 (0.0.0.0) Your (client) P address: 0.0.0.0 (0.0.0.0) Second Playse address Playse Relay agent IP address: 10.2.8.105 (10.2.8.105) <td< th=""><th>No. Time Source Destination Protocol Length Info 14 17, 967476 0.0.00 255, 255, 255 DHCP 590 DHCP Discover - Transaction ID 0x88e96872 15 18,137781 10.2.8.105 10.2.8.106 DHCP 342 DHCP Offer - Transaction ID 0x88e96872 16 18,177701 0.0.0.0 255, 255, 255 DHCP 590 DHCP Request - Transaction ID 0x88e96872 17 18,177802 10.2, 8.105 10.2, 8.106 DHCP 342 DHCP ACK - Transaction ID 0x88e96872 17 18,177802 10.2, 8.105 10.2, 8.106 DHCP 342 DHCP ACK - Transaction ID 0x88e96872 18 Ethernet II, Src: Vmware_09:51:fa (00:0c:29:09:51:fa), Dst: XiamenYe_38:28:d8 (00:15:65:38:28:d8) Distribution Transaction A, src: 10.2, 8.105 (10.2, 8.105), Dst: 10.2, 8.106 (10.2, 8.106) Descent Datagram Protocol, src Port: bootps (67), Dst Port: bootpc (68) 19 User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) Message type: Bot Reply (2) Hardware type: Ethernet Hardware type: Ethernet 6 Finder address lanoth: 6 Finder address lanoth: 6</th><th>Filter: sip bootp</th><th>Expression Clear Apply</th><th></th></td<>	No. Time Source Destination Protocol Length Info 14 17, 967476 0.0.00 255, 255, 255 DHCP 590 DHCP Discover - Transaction ID 0x88e96872 15 18,137781 10.2.8.105 10.2.8.106 DHCP 342 DHCP Offer - Transaction ID 0x88e96872 16 18,177701 0.0.0.0 255, 255, 255 DHCP 590 DHCP Request - Transaction ID 0x88e96872 17 18,177802 10.2, 8.105 10.2, 8.106 DHCP 342 DHCP ACK - Transaction ID 0x88e96872 17 18,177802 10.2, 8.105 10.2, 8.106 DHCP 342 DHCP ACK - Transaction ID 0x88e96872 18 Ethernet II, Src: Vmware_09:51:fa (00:0c:29:09:51:fa), Dst: XiamenYe_38:28:d8 (00:15:65:38:28:d8) Distribution Transaction A, src: 10.2, 8.105 (10.2, 8.105), Dst: 10.2, 8.106 (10.2, 8.106) Descent Datagram Protocol, src Port: bootps (67), Dst Port: bootpc (68) 19 User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) Message type: Bot Reply (2) Hardware type: Ethernet Hardware type: Ethernet 6 Finder address lanoth: 6 Finder address lanoth: 6	Filter: sip bootp	Expression Clear Apply	
14 17.967476 0.0.0.0 255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x88e96872 15 18.137781 10.2.8.105 10.2.8.106 DHCP 010 DHCP Request - Transaction ID 0x88e96872 16 18.177701 0.0.0.0 255.255.255 DHCP 590 DHCP Nequest - Transaction ID 0x88e96872 17 18.178902 10.2.8.105 10.2.8.106 DHCP 342 DHCP ACK - Transaction ID 0x88e96872 18 Ethernet II, Src: Ymware_09:51:fa (00:0c:29:09:51:fa), Dst: Xiamenve_38:28(8 (00:15:65:38:28:d8) 10 19 Internet Protocol version 4, Src: 10.2.8.105 (Dc.2.8.105), Dst: 10.2.8.106 (Dc.2.8.106) 10.2.8.106 19 User Datagram Protocol Ser Datagram Protocol 10 10 Bootstrap Protocol Ser Contage 100 10.2.8.106 (Dc.2.8.105) 10 Bootstrap Protocol Sec Contage 100 10.2.8.106 (Dc.2.8.105) 10 Hardware type: Ibhornet Hardware type: Soot Reply (2) Hardware address length: 6 Hops: 0 Transaction ID: 0x88e96872 Seconds elapsed: 100 10 Bootstraver paddress: 10.2.8.105 (Dc.2.8.106) Next server IP address: 10.2.8.105 (Dc.2.8.106) Next server IP address: 10.2.8.105 (Dc.2.8.106) Relay agent IP address: Niamerve_38:28:48 (00:15:55:38:28:48) 11 client Hardware address padding: 000000000000000000000000000000000000	14 17.967476 0.0.0.0 255.255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x88e96872 15 18.137781 10.2.8.105 10.2.8.106 DHCP 342 DHCP Offer - Transaction ID 0x88e96872 16 18.177701 0.0.0 255.255.255.DHCP 590 DHCP Request - Transaction ID 0x88e96872 17 18.178902 10.2.8.105 10.2.8.106 DHCP 342 DHCP ACK - Transaction ID 0x88e96872 17 18.178902 10.2.8.105 10.2.8.106 DHCP 342 DHCP ACK - Transaction ID 0x88e96872 19 Ethernet IT, Src: Vmware_09:51:fa (00:0c:29:09:51:fa), Dst: XiameNCe, 38:28:d8 (00:15:65:38:28:d8) 10 10 10 Internet Protocol Version 4, src: 10.2.8.105 (0.2.8.105), Dst: 10.2.8.106 (10.2.8.106) 10 10 19 User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) 10 10 10 10 Message type: Boot Reply (2) Hardware type: Ethernet Hardware type: Ethernet 10 10 Hardware address lamoth: 6 10 10 10 10 10 10	No. Time Source	Destination Protocol Length Info	
15 18.137781 10.2.8.105 10.2.8.106 DHCP 342 DHCP AFF Transaction 1D 0x88e96872 17 18.17701 0.0.0.0 255.255.255 DHC 590 DHCP Request - Transaction 1D 0x88e96872 17 18.178902 10.2.8.105 10.2.8.106 DHCP 342 DHCP ACK Transaction 1D 0x88e96872 18 Ethernet II, src: Vmware_09:51:fa (00:0c:29:09:51:fa), Dst: 1X:imenve_38:28:d8 (00:15:65:38:28:d8) 11 19 Internet Protocol Version 4, src: 10.2.8.105 (10.2.8.105), Dst: 10.2.8.106 (10.2.8.106) 10 Message type: Boot Reply (2) Hardware type: Ethernet Hardware type: Ethernet Hardware type: Ithernet Hard	1518.137781 10.2.8.105 10.2.8.106 DHCP 342 DHCP offer - Transaction 1D 0x88e96872 1618.177701 0.0.0.0 255.255.255 DHCP 590 DHCP Request - Transaction 1D 0x88e96872 1718.178902 10.2.8.105 10.2.8.106 DHCP 342 DHCP ACK - Transaction 1D 0x88e96872 19 Ethernet II, Src: Vmware_09:51:fa (00:0c:29:09:51:fa), Dst: Xiamenve_38:28:d8 (00:15:65:38:28:d8) - - 19 Internet Protocol Version 4, Src: 10.2.8.105 (10.2.8.105), Dst: 10.2.8.106 (10.2.8.106) - - 10 User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) - - Message type: Boot Reply (2) - - - Hardware type: Ethernet - - - Hardware type: State Reply (2) - - -	14 17.967476 0.0.0.0	255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x88e968	2
16 18.177701 0.0.0.0 255.255.255.255.25 DHCP 590 DHCP Request - Transaction 10 0x88e96872 17 18.178902 10.2.8.105 10.2.8.106 DHCP ACK Transaction 10 0x88e96872 B Ethernet II, Src: Vmware_09:51:fa (00:0c:29:09:51:fa), Dst: XiamenYe_38:28:d8 (00:15:65:38:28:d8) Internet Protocol version 4, Src: 10.2.8.105 (10.2.8.105), Dst: 10.2.8.106 (10.2.8.106) B User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) Bootstrap Protocol Message type: Boot Reply (2) Hardware type: Ethernet Hardware address length: 6 Haydware si long Internet Protocol (unicast) Client IP address: 10.0.0 (0.0.0.0) Your (client) IP address: 10.2.8.106 (10.2.8.106) Next sagent IP address: 0.0.0.0 (0.0.0.0) Client Madress: xiamerve_38:28:d8 (00:15:65:38:28:d8) Client Mack address: xiamerve_38:28:d8 (00:15:65:38:28:d8) Client Mack address: xiamerve_38:28:d8 (00:15:65:38:28:d8) Client Mack address protent Magic cookie: DHCP Magic cookie: DHCP Message Type = DHCP ACK B Option: (t=51, 1=4) Rebinding Time value = 5 hours, 15 minutes B Option: (t=53, 1=4) Rehead Time value = 5 hours, 15 minutes B Option: (t=53, 1=4) Rehead Time value = 5 hours, 15 minutes B Option: (t=53, 1=4) Rehead Time value = 5 hours, 15 minutes B Option: (t=53, 1=4) Rehead Time value = 5 hours, 15 min	16 18.177701 0.0.0.0 255.255.255 DHCP 590 DHCP Request - Transaction ID 0x88e96872 17 18.178902 10.2.8.105 10.2.8.106 DHCP 342 DHCP ACK - Transaction ID 0x88e96872 18 Ethernet II, Src: Vmware_09:51:fa (00:0c:29:09:51:fa), Dst: Xiamenve_38:28:48 (00:15:65:38:28:48)	15 18.137781 10.2.8.105	10.2.8.106 DHCP 342 DHCP offer - Transaction ID 0x88e9687	2
17 18:178902 10:2:8:105 10:2:8:105 10:2:8:106 DRCP 342 DRCP Ack - Transaction 10 0x88896872 B Ethernet II, Src: Ymware_09:51:fa (00:0c:29:09:51:fa), Dst: Xiamenye_38:28:d8 (00:15:65:38:28:d8) 10:10:10:10:10:10:10:10:10:10:10:10:10:1	1/ 18.1/8902 10.2.8.105 10.2.8.105 DECP 342 DECP ACK - Transaction ID 0x8890872 IB Ethernet II, Src: Vmware_09:51:fa (00:0c:29:09:51:fa), Dst: xiamenYe_38:28:d8 (00:15:65:38:28:d8) ID IB Internet Protocol Version 4, Src: 10.2.8.105 (10.2.8.105, Dst: 10.2.8.106 (10.2.8.106) ID ID user Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) Decostrap Protocol Message type: Boot Reply (2) Hardware type: Ethernet Hardware address lamoth: 6 ID	16 18.177701 0.0.0.0	255.255.255.255 DHCP 590 DHCP Request - Transaction ID 0x88e9687	2
□ Ethernet II, Src: Vmware_09:51:fa (00:0C:29:09:51:fa), Dst: Xiamenve_38:28:d8 (00:15:65:38:28:d8) □ Internet Protocol version 4, Src: 10.2.8.105 (10.2.8.105), Dst: 10.2.8.106 (10.2.8.106) □ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) ■ Bootstrap Protocol Message type: Boot Reply (2) Hardware address length: 6 Hopps: 0 Transaction ID: 0x88e96872 Seconds elapsed: 100 ■ Bootp flags: 0x0000 (Unicast) Client IP address: 10.2.8.105 (10.2.8.106) Next Server IP address: 10.2.8.105 (10.2.8.106) Next Server IP address: 10.2.8.105 (10.2.8.105) Relay agent IP address: 10.2.8.105 (10.2.8.105) Relay agent IP address: xiamery_38:28:48 (00:15:65:38:28:48) Client MAC address x stamery_38:28:48 (00:15:65:38:28:48) Client MAC address x stamery_38:28:48 (00:15:65:38:28:48) Client hardware address padding: 000000000000000000000000000000000000	 Bthernet II, Src: Vmware_09:51:fa (00:0c:29:09:51:fa), Dst: Xiamenve_38:28:d8 (00:15:65:38:28:d8) B Internet Protocol Version 4, Src: 10.2.8.105 (10.2.8.105), Dst: 10.2.8.106 (10.2.8.106) B User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) Message type: Boot Reply (2) Hardware type: Ethernet Hardware address langth: 6 	1/ 18.1/8902 10.2.8.105	10.2.8.106 DHCP 342 DHCP ACK - Transaction ID 0x88e968/	2
	<pre>Hops: 0 Hops: 0 Transaction ID: 0x88e96872 Seconds elapsed: 100 B Bootp flags: 0x0000 (unicast) Client IP address: 0.0.0.0 (0.0.0.0) Your (client) IP address: 10.2.8.106 (10.2.8.106) Next server IP address: 10.2.8.105 (10.2.8.105) Relay agent IP address: 0.0.0.0 (0.0.0.0) Client Mac address: xiamenve_38:28:d8 (00:15:65:38:28:d8) Client hardware address padding: 00000000000000000 Server host name: mid0171-for3xon Boot file name not given Magic cookie: DHCP B Option: (t=51,1=4) Subnet Mask = 255.255.0 B Option: (t=51,1=4) Rebinding Time value = 5 hours, 15 minutes B Option: (t=51,1=4) Rebinding Time value = 5 hours, 15 minutes B Option: (t=28,1=4) Rehewal Time value = 5 hours, 15 minutes B Option: (t=128,1=14) DDCSIS full security server IP [TODO] Option: (t=12,1=4) DDCSIS full security server IP [TODO] Length: 18 Value: 7466747032727634004232082631302576 </pre>	■ Ethernet II, Src: Vmware_ ■ Internet Protocol Version ■ User Datagram Protocol, Si ■ Bootstrap Protocol Message type: Boot Repl; Hardware type: Ethernet Hardware address length Hops: 0 Transaction ID: 0x88e96. Seconds elapsed: 100 ■ Bootp flags: 0x0000 (Un Client IP address: 0.0., Your (client) IP address: Relay agent IP address: Relay agent IP address: Server host name: mid01 Boot file name not give Magic cookie: DHCP ■ Option: (t=1,1=4) Subne ■ Option: (t=59,1=4) Rebi ■ Option: (t=58,1=4) Rene ■ Option: (t=1,1=4) IP A ■ Option:	09:51:fa (00:0c:29:09:51:fa), D5t: xiamenye_38:28:d8 (00:15:65:38:28:d8) i4, src: 10.2.8.105 (10:2.8.105), Dst: 10.2.8.106 (10.2.8.106) rc Port: bootps (67), Dst Port: bootpc (68) y (2) : 6 :872 ricast) 0.0 (0.0.00) : 10.2.8.106 (10.2.8.106) 10.2.8.105 (10.2.8.105) 10.2.8.105 (10.2.8.105) 10.0.0.0 (0.0.0.0) merve_38:28:d8 (00:15:65:38:28:d8) : padding: 00000000000000000 7.1-for3xon m Y Message Type = DHCP ACK tt Mask = 255.255.255.0 dddress Lease Time = 6 hours nding Time Value = 3 hours, 15 minutes wal Time Value = 3 hours, 15 minutes wal Time Value = 3 hours ddress Lease Time = 6 hours rCSIS Full security server IP [TODO] full security server IP [TODO] full security server IP [TODO]	

Right click the root node of the custom option (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://10.2.8.105/.

In addition to the Power On mode, you can also trigger the phone to obtain the provisioning server address via DHCH options using other updating modes. For more information about the other updating modes, refer to Configuring the Updating Mode on page 26.

Phone Flash

Yealink W52P IP DECT phones support obtaining the provisioning server address from the phone flash. To obtain the address from the phone flash, you need to configure the TFTP server address manually via web user interface in advance.

To specify the provisioning server URL via web user interface:

If the phone wants to connect to a FTP server, the username and password are required.

- 1. Click on Phone->Auto Provision.
- 2. Enter the URL of the TFTP server in the **Provisioning Server** field.
- 3. (Optional.) Enter the username of the provisioning server in the User Name field.
- 4. (Optional.) Enter the password of the provisioning server in the Password field.

Auto	Provision	
	PNP	🔘 On 💿 Off
	DHCP Option	🔿 On 💿 Off
	Custom Option(128~254)	
	DHCP Option Value	
	Provisioning Server	tftp://192.168.2.100
	User Name	
	Password	••••
	Common AES Key	•••••
	MAC-Oriented AES Key	•••••

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

To enable the Power On mode via web user interface:

In order to obtain the provisioning server address from the phone flash during bootup, make sure the Power On mode is activated before rebooting the phone.

1. Click on Phone->Auto Provision.

2. Mark the On radio box in the Check New Config field.

Check New Config	💿 On 🔘 Off
Repeatedly	🔿 On 💿 Off
Interval (minutes)	60
Weekly	🔘 On 💿 Off
Time	02 : 00 03 : 00
Day of week	Sunday Monday Tuesday Wednesday Thursday Friday Saturday Autoprovision Now

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

To obtain the provisioning server address from the phone flash:

1. Reboot the phone.

The phone will obtain the provisioning server address by reading the corresponding parameter you have configured via web user interface during bootup.

The following figure shows the example messages of obtaining the provisioning server address from the phone flash and connecting to the provisioning server:



In addition to the Power On mode, you can also trigger the phone to obtain the provisioning server address via the phone flash using other updating modes. For more information about the other updating modes, refer to Configuring the Updating Mode on page 26.

Configuring the Updating Mode

In addition to the Power On mode, the following five updating modes can also be used to trigger the auto provisioning process:

- Repeatedly
- Weekly

- Auto Provision Now
- Multi-mode mixed
- SIP Notify Message

This section introduces each update mode in detail.

When the phone is during a call, it will keep on asking for the configuration files with an interval of 30 seconds for up to 2 hours.

Repeatedly

You can activate Repeatedly mode via web user interface. The phone will perform auto provisioning process at regular intervals. You can configure the interval for the Repeatedly mode. 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.

Check New Config	🔘 On 💿 Off
Repeatedly	💿 On 🔘 Off
Interval (minutes)	60
Weekly	🔿 On 💿 Off
Time	02 : 00 03 : 00
Day of week	Sunday Monday Tuesday Wednesday Thursday Friday Saturday
	Autoprovision Now

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

Weekly

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

Check New Config	🔿 On 💿 Off
Repeatedly	🔿 On 💿 Off
Interval (minutes)	60
Weekly	⊙ On ○ Off
Time	02 : 00 03 : 00
Day of week	 ✓ Sunday Monday Tuesday Wednesday Thursday ✓ Friday Saturday
	Autoprovision Now

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

Auto Provision Now

You can use Auto Provision Now mode to manually trigger the phone to perform the auto provisioning process 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.

Check New Config	🔘 On 💿 Off
Repeatedly	🔿 On 💿 Off
Interval (minutes)	60
Weekly	🔿 On 💿 Off
Time	02 : 00 03 : 00
Day of week	Sunday Monday Uednesday Thursday Friday Saturday
	<u> </u>

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 will perform the auto provisioning process when receiving a SIP Notify message which contains the header "Event:check-sync". If the header of SIP Notify message contains an additional string "reboot=true", the phone will reboot immediately and then perform the auto provisioning process. This updating mode requires server support.

The following figure shows the message flow:



Downloading Configuration Files

Downloading Configuration Files from the Provisioning Server

Once obtaining the provisioning server address via one of the ways introduced above, the phone will connect to the provisioning server and download the configuration files. The phone will try to download the Common CFG file first from the root directory of the provisioning server, and then download the MAC-Oriented CFG file. If resource files need to be updated and the access URLs has been specified in the configuration files, the phone will then try to download and update the resource files.

Resolving and Applying the Configurations

After downloading the configuration files, the phone calculates the MD5 values of the two configuration files respectively. If the MD5 values are the same to those of the last downloaded ones, the phone gives up updating the configurations. If the MD5 values are different, the phone applies the configurations, resolves the access URLs of the resource files and downloads the resource files.

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

The phone reboots only when applying some specific parameters, you can refer to the section "Description of Configuration Parameters in CFG Files" for more information.

Verifying Configurations

After auto provisioning, you can verify the update on your handset or via web user interface.

You can also monitor the downloading request and response messages by a WinPcap tool during the auto provisioning process. The following are some examples.

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

	/000 D 41000 8	1				
Zu titp2.pcap [Wireshark 1.6.7	(SWN Rev 41973 from	/trunk-1.6)]				
Elle Edit View Go Capture Analyze	Statistics Telephony Tools	Internals Help				
R R R R R R 🖻 🖬 X 😂 (🖴 🔍 🔶 🏟 🤹 🐺 ;	2 I 🗐 🖬 I Q Q Q	🖭 🕷	M 🚳 🗱 🗒		
Filter:		Zxprezzion Clear	Apply			
So. Tine	Source	Destination	Protocol	Length Info		
1 0.000000	10.2.10.182	10.2.1.89	TFTP	73 Read Request, File: /y00000000025.cfg, Transfer type: octet		
2 0.002874	10.2.1.89	10.2.10.182	TFTP	319 Data Packet, Block: 1 (last)		
3 0.014326	10.2.10.182	10.2.1.89	TETP	68 Acknowledgement, Block: 1		
4 0.137569	10.2.10.182	10.2.1.89	TFTP	72 Read Request, File: /0015653828d8.cfg, Transfer type: octet		
5 0.138681	10.2.1.89	10.2.10.182	TFTP	65 Error Code, Code: File not found, Message: File not found	1.00	
Frame 1: 73 bytes on wire (58-	4 bits), 73 bytes cap	ured (584 bits)				
Ethernet II, Src: ×1amenYe_38	:28:d8 (00:15:65:38:2)	8:d8), Dst: Cisco_40:o	a:55 (60	::50:4d:40:da:55)		
■ 802.1Q virtual LAN, PRI: 0, Cl	FI: 0, ID: 77					
Internet Protocol Version 4, :	Src: 10.2.10.182 (10.)	2.10.182), Dst: 10.2.1	.89 (10.	.2.1.89)		
User Datagram Protocol, Src P	ort: 51868 (51868), D	st Port: tftp (69)				
Source port: 51868 (51868)						
Destination port: tftp (69)	Destination port: tftp (69)					
Length: 35					I	
	n disabled]					
E Trivial File Transfer Protoco						
[Source File: /y0000000002	S.cfg]					
Opcode: Read Request (1)						
Source File: /y00000000025	. cfg					
Type: octet						

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

d ftp.pcap [Vireshark 1.6.7]	(SWN Rev 41973 from /	trunk-1.6)]			×
Ele Edit View Go Capture Analyze	Statistics Telephony Tools	Internals Help			
察察察察 (1) 12 22 22 22 22 22 22 22 22 22 22 22 22	≞ ↔ ↔ ⊕ 🐼 ;	<u>ଥ</u> ା 🔳 🔳 🔍 ପ୍ ପ୍ ପ୍	🖂 🕷	M 🥦 🗱 🛛	
Filter:		Expression Clear	Apply		
So. Tine	Source	Bestination	Protocol	Length Info	
1 0.000000	10.2.1.89	10.2.10.182	FTP	93 Response: 220 FTP Server ready.	
2 0.012772	10.2.10.182	10.2.1.89	FTP	86 Request: USER anonymous	
3 0.015130	10.2.1.89	10.2.10.182	FTP	145 Response: 331 Anonymous login ok, send your complete email address as your password	
4 0.015135	10.2.10.182	10.2.1.89	FTP	77 Request: PASS	
5 0.017493	10.2.1.89	10.2.10.182	FTP	115 Response: 230 Anonymous login ok, restrictions apply.	
6 0.024409	10.2.10.182	10.2.1.89	FTP	/8 Request: TYPE I	
7 0.025083	10.2.1.89	10.2.10.182	FTP	89 Response: 200 Type set to I	
8 0.026075	10.2.10.182	10.2.1.89	FTP	76 Request: PASV	
9 0.026705	10.2.1.89	10.2.10.182	FTP	118 Response: 227 Entering Passive Mode (10,2,1,89,212,109).	
10 0.035522	10.2.10.182	10.2.1.89	FTP	95 Request: SIZE /y00000000025.crg	
11 0.036198	10.2.1.89	10.2.10.182	FTP	79 Response: 213 269	
12 0.045420	10.2.10.182	10.2.1.89	FTP	95 Request: RETR /y00000000025.crg	
13 0.046902	10.2.1.89	10.2.10.182	FTP	146 Response: 150 Opening BINARY mode data connection for /y000000000025.ctg (269 bytes)	
14 0.064873	10.2.1.89	10.2.10.182	FTP	93 [TCP ACKed lost segment] Response: 226 Transfer complete	
15 1.944870	10.2.1.89	10.2.10.182	FTP	93 Response: 220 FTP Server ready.	
16 1.948611	10.2.10.182	10.2.1.89	FTP	86 Request: USER anonymous	
17 1.951771	10.2.1.89	10.2.10.182	FTP	145 Response: 331 Anonymous login ok, send your complete email address as your password	~
181 002008	10 2 10 182	10 2 1 89	ETD	77 Banilact + BASS	<
					22
Frame 1: 93 bytes on wire (7)	44 bits), 93 bytes cap	tured (744 bits)		45.55.20.20.40	
Ethernet 11, Src: Cisco_40:0	a:55 (6C:50:4d:40:da:5	oj, ost: xiamenYe_38:	28:08 (0	112102128128108)	
# 802.10 VIFTUAL LAN, PRI: 0,	CFI: 0, 10: 77			40.403	
Internet Protocol Version 4,	SFC: 10.2.1.89 (10.2.	1.89), DSt: 10.2.10.1	82 (10.2.	10.1823	
Iransmission Control Protoco	a, and port: ftp (21),	DST POPT: 41021 (410	ZIJ, Seq	: 1, ACK: 1, Len: 23	
■ F1le Transfer Protocol (FTP)					

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

📶 HTTP. pcap 🛛 [Vireshark	1.6.7 (SWN Rev 41973 fr	om /trunk-1.6)]			a X
Ele Edit View Go Capture &	analyze Statistics Telephony To	ools Internals Help			
EK EM EM EM her E7 1	🗶 😂 📇 🔍 🔶 🧇 🥝 🎖	F 🛓 🗐 🗐 🔍 🤇	२. 🔍 🖭 । 🕷	19 😼 🖗 💢	
Filter:		Expression	Clear Apply		
So. Tine	Source	Destination	Protocol	Length Info	
1 0.000000	10.2.10.182	10.2.1.89	HTTP	181 GET /yealink/y00000000025.ctg HTTP/1.1	
2 0.004937	10.2.1.89	10.2.10.182	HTTP	827 HTTP/1.1 401 Authorization Required (text/ntml)	
3 0.030094	10.2.10.182	10.2.1.89	HITP	220 GET /yearink/you000000025.crg HTP/1.1	
4 0.039097 5 0.190700	10.2.10.193	10.2.1.90	HTTO	190 CET Available (001565292949 cfa WTTO /1 1	
6.0.191672	10.2.10.102	10.2.10.182	WTTD	827 HTTP/1 1 401 Authorization Required (text/html)	
7.0.216393	10.2.10.182	10.2.1.89	HTTP	219 GET /vealink/0015653828d8.cfn HTTP/1.1	
8 0.234142	10.2.1.89	10.2.10.182	HTTP	585 HTTP/1.1 404 Not Found (text/html)	
Ethernet II, SrC: Xiame 802.1Q Virtual LAN, PRI Internet Protocol Versi Transmission Control Pr Hypertext Transfer Prot	nre_38:28:d8 (00:15:65:38 : 0, CFI: 0, ID: 77 on 4, Src: 10.2.10.182 (1 otocol, Src Port: 58040 (ocol	8:28:d8), Dst: Cisco .0.2.10.182), Dst: 1 (58040), Dst Port: P	0_40:da:55 (6c .0.2.1.89 (10. http (80), Seq	:50:4d:40:da:55) 2.1.89) : 1, Ack: 1, Len: 150	
GET /yeal1nk/y0000000	00025.cfg HTTP/1.1\r\n				
Expert Into (chat/	Sequence): GET /yearink/y	/00000000025.crg HI	16\T'T/L/U]		
Request Method. Gen	nk (v000000000025 cfa				
Request Version: HT	Tp/1 1				
Host: 10.2.1.89\r\n					
User-Agent: \r\n					
Accept: */*\r\n					
Connection: Keep-Aliv	e\r\n				
Authorization: Basic	dXNlcjE6MTI2NA==\r\n				
\r\n [Full request URI: ht	tp://10.2.1.89/yeal1nk/y0	00000000025.cfg1			

Troubleshooting

This chapter provides general troubleshooting information to help you solve the problems you might encounter when provisioning the Yealink W52P IP DECT phones. If you require additional information or assistance with the auto provision, contact your system administrator.

Why does the phone fail to download the configuration files?

- Ensure that the 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 a HTTP 404 error?

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

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

- Ensure that the root directory of the FTP server contains the full 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 a FTP Server

This section shows you how to configure a FTP server using 3CDaemon.

To create a root directory:

- 1. Create a FTP 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 assign the permissions: read, write, and modify files to the user or group.

Administrators MAN	STD90\Admin	istratore)		~
	3100040000	istratorsj		1
C Everuone				
G Hill, James fiahill@n	nvservername	.com]		-
SYSTEM	.,	line		~
<			>	-
				-
		<u>∧dd</u>	Hemove	
Permissions for Everyone		Allow	Deny	
Full Control				^
Modify				
Read & Execute				
List Folder Contents		~		
Read				
Write				
Consist Dermissions				~
For special permissions or click Advanced.	for advanced	settings,	Advanced	

3. Place the configuration files and resource files to this directory.

To configure a FTP server:

1. Double click the 3CDaemon.exe to start the application.
2. Click FTP Server on the left of the main page.

3CDaemon	1				_ = _
File View Help					
TFIP Server	Start Time	Peer	Bytes	Status	
FTP Server	Mar 13, 2012 14:26:34	local	0	Listening for FTP requests on IP address: 192.168.147.1, Port 21	
	Mar 13, 2012 14:26:34	local	0	Listening for FTP requests on IP address: 192.168.172.1, Port 21	
<u></u>	Mar 13, 2012 14:26:34	local	0	Listening for FTP requests on IP address: 10.2.11.101, Port 21	
Configure FTP Server					
5TOF					
FTP Server is started.					
Click here to stop it.					
Logging to Ftpd Log. Click to stop.					
. <u>X</u> .					
Not debugging.					
Click to start.					N
					hg
Clear list.					
46					
View Log/Debug files.					
Syslog Server					
TFIP Client					
For Help, press F1	1				NUM
Concept breeze r		-	_		Nom //

- 3. Select Configure FTP Server.
- 4. Click ... to locate the FTP root directory from the local system:

3CD aemon		
File Miew Help		
TFTP Server	Start Time Peer Bytes Status	
FTP Server	Mar 01, 2012 10:24:01 local 0 Listening for FTP requests on IP address: 192.168.133.1, Port 21 Mar 01, 2012 10:24:01 local 0 Listening for FTP requests on IP address: 192.168.138.1, Port 21	
Configure TIT Server TT Server is started Click here to stop it. Logging to Fighlog Clock to stop. Not dobuging Click to start. Click to start. Click to start. Click to start.	Re (0, 2012 (0.24 (0) local 0 Listing for FIF requests on H address: 102 (108 (06.1, pert 21 Re (0), 2012 (0.24 (0) local 0 Listing for FIF requests on H address: 102 (1.123, pert 21 SCDnemon Configuration General Configuration FIF Forfile Synlag Configuration FIF Forfile For	
Free Log Debug Filter.		
	3CDaemon 确定 取消 应用 (A)	
Syslog Server		
TFTP Client		
For Help, press F1		NUM ///

- 5. Enter the new authentication username in the **Profile** filed.
- 6. Click Set/Change user's password to set the password in the pop-up dialogue box.
- 7. Click **OK** to accept the change.

8. Check the check boxes of Login, Download and Upload to make sure the FTP user has the login, download and upload permission.

3CDaemon		
File View Help		
TFIP Server Start Time	Peer	Bytes Status
FTP Server Mar 13, 201 Mar 13, 201 Confi gure FTP Server	2 14:26:34 local 2 14:26:34 local 2 14:26:34 local	0 Listening for FIP requests on IP address 192.08.147.4, Port 21 0 Listening for FIP requests on address 192.08.27.2, Port 21 0 Listening for FIP requests on IP address: 10.211.101, Port 21
Fight a stor fed. Fight areas to stor fed. Logging to Fight log. Logging to Fight log. Kind absorption. Cited absorption. Cited absorption. Cited absorption. Cited absorption. Cited absorption. Store Log/Dobug files.	CDaemon C Ge T Noticy and For white Sowe Frr Esc edit Common	nnfiguration sred Cafigaraties THT Cafigaraties There Info Vere Info Sev/Change user's password Sev/Change User Password Wases construction Winese
Syulog Server TFTP Client For Help, press F1		

9. Click Save Profile to save the settings.

🔤 3CDaemon 📃 🗖 🗙
File Yiew Help
TFTP Server Start Time Peer Bytes Status
FTP Server Mw c01, 2012 10:24:01 local 0 Listening for FTP requests on IP address: 192.168.133.1, Pert 21 Mw c01, 2012 10:24:01 local 0 Listening for FTP requests on IP address: 192.168.168.1, Pert 21 Mw c01, 2012 10:24:01 local 0 Listening for FTP requests on IP address: 192.168.168.1, Pert 21
Configure FTP Server 3CDaemon Configuration
Image: Started configuration TFT Forlies System is started click here is top it Image: System click here is top it Loging to Flyd log Image: Started click here is a system click here is
Clear list. Delete files Save Profile User Leg/Bebag files. To add a profile. Highlight the profile, make your changes, then press
Syrlog Server TFTP Client
For Help, press Fi

10. Click **Confirm** to finish configuring the FTP server.

The server URL "ftp://username:password@IP/" (Here "IP" means the IP address of your local system, "username" and "password" are the authentication for FTP download. For example, "ftp://admin:123456@192.168.1.100/") can be used for FTP download.

Configuring a HTTP Server

This section shows you how to configure a HTTP server using HFS tool. You can download HFS tool at: 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 root directory.

You need to define a user or a group name, and assign the permissions: read, write, and modify files to the user or group.

Administrators (VANST	D80\Admini	strators)		
Everyone				
🖸 Hill, James (jahill@my:	servername	.com]		
SYSTEM				~
<			>	
		\ <u>d</u> d	Bemove	
Permissions for Everyone		Allow	Deny	
Full Control				^
Modify				
Read & Execute		~		
List Folder Contents				
Read				
Write				
Coosial Dormissions				~
For special permissions or fo click Advanced.	or advanced	settings,	Advanced	1

3. Place the configuration files to this root directory.

To configure a HTTP server:

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

The main configuration page is shown as below:

HFS ~ HTTP File Server 2.2f	Build 155	J
🛓 Menu 🛛 🖗 Port: 8080 🛛 🎎 You are in Expert mode 🛛		
Open in browser http://10.2.11.101:8080/		
	Top speed:0.0KB/s	
Virtual File System	Log	
	17:23:24 Check update: no new version	
🗊 IP 📃 Filename	Status Speed Time left %	1
Connections: 0 Out: 0.0 KB/s In: 0.0 KB/s Total Out: 0 B To	tal In: 0.B VFS: 0 items	
		-1

2. Click Menu in the main page and select the IP address of the PC from IP address.

🚔 HFS ~ HTTP File Server 2.2f	Build 155
📕 Menu 🕴 Port: 8080 🕵 Yo	u are in Expert mode
+ Self Test	18080/
Edit HTML template	Top speed: 0.0 KB/s
Other options	
Upload Stort/Evit	istem Log
Virtual File System	17:23:24 Check update: no new version
Limits	
Flash taskbutton	
Fingerprints •	
Tray icons	
IP address	This IP address is used only for URL building
Dynamic DNS updater	192.168.147.1
URL encoding	192.168.172.1
Updates •	
💚 Donate!	Custom
泸 Load file system Ctrl+O	Don't include port in URL Find external address
🚽 Save file system Ctrl+S	Constantly search for better address
X Clear file system	
Save options	
Help +	
Web links •	
Uninstall HFS	Filename i) Status Speed Time left %
V About	
Switch OFF F4	
Exit	
Connections: 0 Out: 0.0 KB/s In	: 0.0 KB/s Total Out: 0 B Total In: 0 B VFS: 0 items
Contraction of a data of a laboration of a	

The default HTTP port is 8080. You can also reset the HTTP port (make sure the port isn't in use before you reset).

HFS ~ HTTP File Server 2.2f	Build 155
🛓 Menu 🖑 Port: 8080 🥵 You are in Expert mode	
Open in browser http://10.2.11.101:8080/	
	Top speed: 0.0 KB/s
Virtual File System	Log
Port Port Specify a port to accept connection, or leave empty to decide automatically. 8088 OK Cance	17:23:24 Check update: no new version
Connections: 0 Out: 0.0 KB/s In: 0.0 KB/s Total Out: 0 B Tota	V Status Speed Time left %

3. Right click the 🏠 icon on the left of the main page, select Add folder from disk.

📾 HFS ~ HTTP File Server 2.2f	Build 155 📃 🗖 💌
🛓 Menu 🛛 🖗 Port: 8088 🛛 🥵 You are in Expert mode	
Open in browser http://10.2.11.101:8088/	
	Top speed: 0.0 KB/s
Virtual File System Log	
Add files	
E 🄌 Add folder from disk	
New empty folder Ins	
💙 New link	
Advanced	
Copy URL address Ctrl+C	
🔗 Browse it F9	
Comment	
Bind root to real-folder	
6 Set user/pass	
Sestrict access	
Customized realm	
✓ Archivable	
👍 Upload 🔹 🕨	
📥 Why is upload disabled?	
Hide tree	
Auto-hide empty folders	Speed Time left %
Hide file extention in listing	Speed Time left %
Connections: 0 Out: 0.0 KB/s In: 0.0 KB/s Total Out: 0.8 Total In: 0.8 VES: 55	1 items - not saver
	Thems needed at

4. Locate the root directory of the HTTP server from the local system. Select the kind of folder you want.

🚔 HFS ~ HTTP File Server 2.2f	Build 155	
🛓 Menu 🛛 🖑 Port: 8088 🛛 🕵 You are in Expert mode		
Open in browser http://10.2.11.101:8088/		
	Ţ	op speed: 0.0 KB/s
Virtual File System Log		
17:23:24 Check update: no new version		
What kind of folder do you want?		
45		
A real folder is faster, good for big folders		
Dirtual folder A virtual folder is easier, good for small folders		
Hint: most time you need real folders!		
	J	
i) Status	Speed Time left	*
	opoos mino lot	
Connections: 0 Out: 0.0 KB/s In: 0.0 KB/s Total Out: 0 B Total In: 0 B VFS: 550 it	ems - not savec	đ

The server URL "http:// IP:Port/" shown in the "Open in browser" address bar can be used for HTTP download. 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 about installing and configuring an Apache HTTPS Server, refer to the network resource.

Configuring a DHCP Server

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

Before configuring the DHCP server, make sure that:

- 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 **Login**.

a DHCP Turbo on localhost	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> indings <u>T</u> ools <u>H</u> elp	
■ オ 物 ■ 図 ※ や で 多 №	
Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Se	
Ready.	11

- 4. Right click localhost and select New Server to add a new DHCP server.
- 5. Enter the name of the new server in the Name field.

			0	\0
Pre gont yew gradings . Servers . Docaliost Database	DUCF Turbo	NT 6.1		
	Features Basic Build 1907	Edition		

- 6. Right click Scopes under Localhost and select New Scope.
- 7. Enter the name of the new scope in the **Name** field.
- 8. Enter valid values in the Start address, End address and Subnet Mask to specify a valid range of IP addresses.

9. Click **OK** to finish the configuration of the new scope.

DHCP Turbo on localhost (modifie	d)	0 X
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> indings <u>T</u> ools <u>H</u> e	lp	
	■ * Ø ♥ § N?	
Servers	New Scope X Scope Start address Mase Start address DMCTServer Description Less Segment Values Segment Days News D Address Days News Days Segment Days	

10. Click 🔄 to accept the change.

To add a custom option via DHCP Turbo:

- BHCP Turbo on localhost (modified) <u>File Edit View Bindings Tools H</u>elp Servers Filter Standard Options • localhost - ODatabase - MW Exclusions Option Magic cookie Home directory Named Policies Hardware address type Hardware address length Doot file Pad Subnet mask Time offset Gateways Time servers IEM116 name servers Log servers Log servers Log servers Hart servers Hart servers Hart servers Hostname Doot file size Merit damp file Domain name Swap servers Koot path Extensions path If forwarding Hor-local source routing Doline files New Option Type... Ctrl+V Hardware address type Hardware address length opes 🔊 Undo Ctrl+Z Redo Ctrl+Y IP Cut Ctrl+X D <u>С</u>ору Ctrl+C Paste Ctrl+V Delete Del Select <u>A</u>ll Ctrl+A 🥂 Eind... Ctrl+F 😤 Properties... Ctrl+P - <u>4</u>20 • Description Specifies a device's hardware address type. Þ
- 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.

DHCP Turbo on localhost (modified)
<u>File Edit View B</u> indings Iools <u>H</u> elp
Servers V Filter Standard Options V Filter Standard Options
→ Database Tag \ Option ▲
The Braned Policies I I Option Properties
-@Option Types Tag 128 -
DHCPServer Man Name TFTPServer
- #1 Type 8bit
- A Descri 16bit ABC 22bit
E i paddress
- <u>49</u> 7 54146 205
- E 9 bool main hardware_address
subencoded
-#16 Swap servers
-Æ17 Root path -Æ18 Extensions path
- E 19 IP forwarding
Mon Dollar Aller
Description
Specifies a device 5 nardware address type.

- 5. Click **OK** to finish setting the option properties.
- 6. Click 🔄 to accept the change.
- 7. Click Named Policies->Global, right click the main page and select New Option.

🐁 DHCP Turbo o	on locall	nost (m	nodifie	d)					
		<u>s 1</u> 00		, ip	×	5	Ċ,	G	₩?
Servers Databas Dat	:e usions bal Jppes FServer	Tag	7		New New Cut Cop Pasts Coc Sele Sele Prov	y Option o o y y ce ete ct All 	n Cf Cf Cf Cf Cf Cf Cf Cf Cf Cf Cf	rl+V rl+Z rl+Y rl+Y	Yalue
Add a new optic	on to this	s polic	у						

8. Scroll down and double click the custom option 128.

Ele Edit View Bindings Iools Help	Contraction and the second sec	dified)	
Servers Teg Name Option Selector Pace Value Option Stelector Pace Value Option Stelector Pace Value Option Selector Pace Value Option Selector Pace Value Option Stelector Pace Value Option Stelector Pace Value Option Stelector Pace Value Option Stelector Pace Value Option Stelector Pace Value Option Stelector Option Stelector Op	<u>File Edit View Bindings T</u> ools	; <u>H</u> elp	
Servers Teg Value Servers Teg Option Selector Phatabase Phataba			
Servers Tag Name Value Option Selector Place Aboxt Mase Tolicies Mase Tolicies Clobal Scopes Scopes DECForver DECFOR DE			
Copion Selector Copion Selector Copion Selector Copion Selector Copion Selector Copion Selector Copion Streament inte Copion Types Copion Types Copion Types Copion Streament inte Copion Selector Copion Sele	Servers Tag	Name Value	
Polatabase P		Coption Selector	
Filter Standard Options Global Name Global X Window system font servers Global X Window system font servers Global Stoops Global DEF advests lease time Global Stoops Global DEF advests lease time Global Global Global DEF advest lease time Global Global Global DEF advest lease time Global Global Global DEF advest lease time Global Global Global DEF servers Global Global servers Global sellabs Clobal Global servers Global server Global server	🥥 Database		
Maned Folicies Image of Folicies		Filter Standard Options 🔻	
Image: Scope state Image: Scope state Image: Scope state Image: State Image: Scope state Image: State Image: Scope state Image: State Image: State Image:	- Named Policies	Tag V Name	
Image: Second		47 NBT scope	
Image: Scopes Image: Scopes Image: Scopes	Option Types	- Æ 48 X Window system font servers	
- Si DDCF address lacse time - SS DDCF reaval time - SS DDCF reaval -	E- Copes		
Image: Second	BUALIServer		
Image: Second			
- 655 WIS' servers - 669 Mobile IP home agent - 669 SMT servers - 670 POTS servers - 671 MMT servers - 677 Wist servers - 677 Viser servers - 677 User servers - 677 User talk DA servers - 6		- 484 MIS+ domain	
		-Æ65 NIS+ servers	
-2009 SMT servers -2017 DOS servers -2017 WWT servers -2017 WWT servers -2017 Finger servers -2017 Finger servers -2017 Strettalk servers -2017 Strettalk Diservers -2017 User class -2012 Cablelabs Clie_C Configuration -2012 TDEServer -2012 Totalsever -2012 Totalsever -2012 Totalsever -2012 Totalsever -2013 Totalsever			
Image: Servers Image: Server			
Image: Servers Image:			
Image: Servers Image: S			
- 180 Servers - 1975 Streettalk servers - 1976 Streettalk Asservers - 1976 User class - 1976 User class - 2010 SIP Server - 2122 Cabledabe Clid - 2125 TIPEServer - 2125 TIPEServer - 2127 Legacy PacketCable Description		ATT3 Finger servers	
- 275 Streettalk norvers - 276 Streettalk DA servers - 277 User class - 2120 SIP Server Defiles TPHIServer - 2120 Cablabet Cliely Configuration - 2128 TPHIServer - 2128 TPHISER - 21			
Image: Constraint of the servers Image: Constraint of the servers Image: Constraint of the server		- Æ 75 Streettalk servers	
Image: Construction Image: Constr			
Image: Configuration Image: Configuration		- Æ 77 User class	
Ended as class clas			
Description		122 Calify Configuration	
Description		🖭 🖅 📕 Hegacy PacketCable 💌	
		Decarintian (6)	
		Jescription 3	
DK Cancel		OK Cancel	
		Zu Zancer	

- 9. Enter the TFTP server address in the input field.
- 10. Click \boldsymbol{OK} to finish setting a custom option.
- **11.** Click [a] to accept the change.

DHCP Turbo on localhost (m	nodified)				- • ×
File Edit View Bindings Loc		0 0 %	N?		
Servers Servers Detabase Off Exclusions Off Exclusi			R?	Value	
4 >					

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.

🚰 DHCP Turbo on localhost							
<u>File Edit View Bindings Tools H</u> elp							
Servers 🗸 Tag	V Name Value						
🖹 💷 localhost 🖉 128 — 🕒 Database	P Option Selector	<u>-</u>]					
	Filter TFTP Options						
- Slobal	Tag 🗸 Name						
	- 48-20 Server name						
	- IS MS option 66						
	Description 4						
	The base success of a TRTP common the denies should use denies ()	-					
	its boot process. Unless you know your device requires this option, you should use option -14 (as IP address) or option -20 (as host name) to define the TFTP server.						
۰	<u>OK</u> Cancel	1					

4. Enter the TFTP server address in the input field.

🐴 DHCP Turbo on localh	ost							x
<u>Eile Edit V</u> iew <u>B</u> indings <u>T</u> ools <u>H</u> elp								
/ 🖉 🖉 🖉	h h	•	90		h ?			
Servers localhost Jord base Made Policies Control States Scopes DM/PServer Made Policies DM/PServer			Nane TFTFServer stion 66 //192.168.1.1 xpression	000/	Puild	Value tftp://192.168.1.100/		

- 5. Click **OK** to finish setting the option 66.
- 6. Click [a] 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.

A DHCP Turbo on localhost		- • ×						
Eile Edit View Bindings Tools Help								
Servers Ta	Value Value							
💷 localhost 🧧	Option Selector							
Database 🖉								
	Filter Standard Options 💌							
- 🔛 Named Policies	Tag 🗸 Name							
Global	24 Path MTU aging timeout							
Uption Types								
- Scopes								
	27 All subnets are local							
	20 Droadcast address							
	- #30 Mark supplier							
	- 234 Trailer encapsulation							
	235 Arp cache timeout							
	44 RDI name servers							
	Description 🔗							
	Head by devices and servers to exchange vendor-specific information							
	set by define and bering to the spectra factor and the							
	<u>QK</u> <u>Cancel</u>							

3. Enter the provisioning server address in the input field.

BHCP Turbo on localhost	Tools Help	-		
		* • •	S	k ?
Servers T Docalhost Docalhost Database Mased Policies Coloral Scobal - Option Types - Scopes	•sg ∇ ■128 ■-15	Name TFTPServer MS option 66		Value tftp://192.168.1.100/ tftp://192.168.1.100/
L- MDHCPServer		Vendor specific http://192.16 Expression <u>QK</u>	c info 38. 1. 100, n <u>C</u> an	Paild. Baild.
د				

- 4. Click OK to finish setting the option 43.
- 5. Click [a] to accept the change.

Description of Configuration Parameters in CFG Files

Parameter	Permitted Values	Descriptions	Web Setting Path
network.inte rnet_port.typ e =	0, 1 or 2	It configures the Internet port type. 0 -DHCP 1 -PPPoE 2 -Static IP Address The default value is 0. It takes effect after reboot.	Network->Basic
network.inte rnet_port.ip =	IP Address	It configures the IP address when the Internet (WAN) port type is defined as Static IP Address. The default value is blank. It takes effect after reboot.	Network->Basic-> WAN->Static IP Address->IP Address
network.inte rnet_port.ma sk =	IP Address	It configures the subnet mask when the Internet (WAN) port type is defined as Static IP Address.	Network->Basic-> WAN->Static IP Address->Subnet

		The default value is blank.	Mask
network.inte rnet_port.ga teway =	IP Address	It configures the default gateway when the Internet (WAN) port type is defined as Static IP Address. The default value is blank. It takes effect after reboot.	Network->Basic-> WAN->Static IP Address->Default Gateway
network.pri mary_dns =	IP Address	It configures the primary DNS server when the Internet (WAN) port type is defined as Static IP Address. The default value is blank. It takes effect after reboot.	Network->Basic-> WAN->Static IP Address->Primary DNS
network.sec ondary_dns =	IP Address	It configures the secondary DNS server when the Internet (WAN) port type is defined as Static IP Address. The default value is blank. It takes effect after reboot.	Network->Basic-> WAN->Static IP Address-> Secondary DNS
network.ppp oe.user =	String	It configures the username for PPPoE connection. The default value is blank. It takes effect after reboot.	Network->Basic-> PPPoE->User
network.ppp oe.passwor d =	String	It configures the password for PPPoE connection. The default value is blank. It takes effect after reboot.	Network->Basic-> PPPoE->Password
network.vla n.internet_p ort_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 reboot.	Network-> Advanced-> VLAN->Active
network.vla n.internet_p ort_vid =	Integer from 1 to 4094	It configures VLAN ID of the Internet (WAN) port. The default value is 1. It takes effect after reboot.	Network-> Advanced-> VLAN->VID
network.vla n.internet_p	Integer from 0 to 7	It configures VLAN priority of the Internet (WAN) port.	Network-> Advanced->

ort_priority		The default value is 0.	VLAN->Priority
=		It takes effect after reboot.	
network.port .http =	Integer from 1 to 65535	It configures the HTTP port of the web server. The default value is 80. It takes effect after 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. The default value is 443. It takes effect after reboot.	Network-> Advanced-> Web Server Type->HTTPS Port
wui.https_en able =	0 or 1	It enables or disables the phone to use HTTPS protocol to access the web user interface. 0 -Disables 1 -Enabled The default value is 1. It takes effect after reboot.	Network-> Advanced-> Web Server Type->HTTPS
wui.http_ena ble =	0 or 1	It enables or disables the phone to use HTTP protocol to access the web user interface. 0 -Disables 1 -Enabled The default value is 1. It takes effect after reboot.	Network-> Advanced-> Web Server Type->HTTP
network.port .max_rtpport =	Integer from 0 to 65535	It configures the maximum local RTP port. The default value is 12780. It takes effect after reboot.	Network-> Advanced->Local RTP Port-> Maximum RTP Port
network.port .min_rtpport =	Integer from 0 to 65535	It configures the minimum local RTP port. The default value is 11780. It takes effect after 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 40. It takes effect after 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.	Network-> Advanced->Voice

		It takes effect after reboot.	QoS->SIP QoS
network.802 _1x.mode =	0 or 1	It configures the 802.1x mode. 0 -Disabled 1 -Enabled (EAP-MD5) The default value is 0. It takes effect after reboot.	Network-> Advanced->802.1x ->802.1x Mode
network.802 _1x.identity =	String	It configures the username for 802.1x authentication. The default value is blank. It takes effect after reboot.	Network-> Advanced->802.1x ->Identity
network.802 _1x.md5_pa ssword =	String	It configures the password for 802.1x authentication. The default value is blank. It takes effect after reboot.	Network-> Advanced->802.1x ->MD5 Password
network.vpn _enable =	0 or 1	It enables or disables the VPN feature. 0 -Disabled 1 -Enabled The default value is 0. It takes effect after reboot.	Network-> Advanced->vpn-> Active
network.lldp .enable =	0 or 1	It enables or disables the LLDP feature. 0 -Disabled 1 -Enabled The default value is 1. It takes effect after reboot.	Network-> Advanced->LLDP-> Active
network.lldp .packet_inte rval =	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 reboot.	Network-> Advanced->LLDP-> Packet Interval
syslog.mode =	1 or 2	It configures the uploading location for the system log. 1 -Loacl 2 -Server The default value is 1. It takes effect after reboot.	Phone-> Configuration-> Export System Log
syslog.serve	IP Address	It configures the IP address of the syslog server when the syslog mode is	Phone->

r =		configured as Server.	Configuration->
		The default value is blank.	Server Name
		It takes effect after reboot.	
syslog.log_le vel =	Integer from 0 to 6	It configures the detailed level of the system log. The default value is 3. It takes effect after reboot.	Phone-> Configuration-> Log Level
voice.vad=	0 or 1	It enables or disables the VAD feature on the phone. 0 -Disabled 1 -Enabled The default value is 0.	Phone-> Voice&Eco->Echo Cancellation->VAD
voice.cng =	0 or 1	It enables or disables the CNG feature on the phone. 0 -Disabled 1 -Enabled The default value is 1.	Phone-> Voice&Eco->Echo Cancellation->CN G
voice.jib.ad aptive =	0 or 1	It configures the type of jitter buffer. 0 -Fixed 1 -Adaptive The default value is 1.	Phone-> Voice&Eco ->Jitter Buffer->Type
voice.jib.min =	Integer	It configures the minimum delay (in milliseconds) of jitter buffer. The default value is 0.	Phone-> Voice&Eco ->Jitter Buffer->Minimum Delay
voice.jib.ma x =	Integer	It configures the maximum delay (in milliseconds) of jitter buffer. The default value is 300.	Phone-> Voice&Eco ->Jitter Buffer->Maximum Delay
voice.jib.nor mal =	Integer	It configures the normal delay (in milliseconds) of jitter buffer. The default value is 120.	Phone-> Voice&Eco ->Jitter Buffer->Normal
redirect.ena ble =	0 or 1	It enables or disables the HTTP(S) and (T)FTP redirection. 0 -Disabled 1 -Enabled The default value is 0.	

base.pin_co de =	String	It configures the system pin of the base station. The default value is 0000.	Security->Base PIN->Base Unit PIN
auto_provisi on.mode =	0 or 1	It enables or disables the phone to check the new configuration when powered on. 0 -Disabled 1 -Enabled The default value is 1.	
auto_provisi on.pnp_ena ble =	0 or 1	It enables or disables the Plug and Play feature. The phone broadcasts the PNP subscribe message to obtain a provisioning server address during bootup. 0 -Disabled 1 -Enabled The default value is 1.	Phone->Auto Provision->PNP
auto_provisi on.pnp_dom ain_name =	Domain Name	It configures the domain name of the PNP server. The default value is 224.0.1.75.	
auto_provisi on.pnp_eve nt_vendor =	String	It configures the vendor name of the device. The default value is yealink.	
auto_provisi on.repeat.en able =	0 or 1	It enables or disables the phone to check the new configuration repeatedly. 0 -Disabled 1 -Enabled The default value is 0.	Phone->Auto Provision-> Repeatedly
auto_provisi on.repeat.mi nutes =	Integer from 1 to 43200	It configures the interval (in minutes) the phone repeatedly checks the new configuration. The default value is 1440.	Phone->Auto Provision->Interval (Minutes)
auto_provisi on.weekly.e nable =	0 or 1	It enables or disables the phone to check the new configuration weekly. 0 -Disabled 1 -Enabled The default value is 0.	Phone->Auto Provision->Weekly

auto_provisi on.weekly.m ask =	Combination of 0, 1, 2, 3, 4, 5 and 6	It configures the days of week the phone checks the new configuration weekly. The default value is 0123456.	Phone->Auto Provision->Day of week
auto_provisi on.weekly.b egin_time =	Time format	It configures the begin time of day the phone checks the new configuration weekly. The default value is 02:00.	Phone->Auto Provision->Time
auto_provisi on.weekly.e nd_time =	Time format	It configures the end time of day the phone checks the new configuration weekly. The default value is 03:00.	Phone->Auto Provision->Time
auto_provisi on.server.url =	URL	It configures the URL of the auto provisioning server. The default value is blank.	Phone->Auto Provision->Provisio ning Server
auto_provisi on.server.us ername =	String	It configures the username for authentication during auto provisioning. The default value is blank.	Phone->Auto Provision->User Name
auto_provisi on.server.pa ssword =	String	It configures the password for authentication during auto provisioning. The default value is blank.	Phone->Auto Provision-> Password
auto_provisi on.common_ file_name =	String	It configures the fixed file name of the Common CFG file.	
auto_provisi on.dhcp_opt ion.enable=	0 or 1	It enables or disables the phone to obtain the provisioning server address by detecting DHCP options. 0 -Disabled 1 -Enabled The default value is 1.	Phone->Auto Provision->DHCP Option
auto_provisi on.dhcp_opt ion.option60 _value =	String	It configures the value (vendor name of the device) of DHCP option 60. The default value is yealink.	Phone->Auto Provision->DHCP Option Value
auto_provisi on.dhcp_opt ion.list_user_ options =	Integer from 128 to 254	It configures the custom DHCP option number. The default value is blank.	Phone->Auto Provision->Custom Option(128~254)

auto_provisi on.aes_key_ 16.com =	String	It configures the AES key (16 characters) for decrypting the Common CFG file. The valid characters contain: $0 \sim 9$, $A \sim Z$, $a \sim z$,#\$%*+,-:=?@[]^_{}~. The default value is blank.	Phone->Auto Provision-> Common AES Key
auto_provisi on.aes_key_ 16.mac =	String	It configures the AES key (16 characters) for decrypting the MAC-Oriented CFG file. The valid characters contain: $0 \sim 9$, $A \sim Z$, $a \sim z$,#\$%*+,:=?@[]^_{}~. The default value is blank.	Phone->Auto Provision-> MAC-Oriented AES Key
sip.rfc2543_h old =	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-> General Information->RFC 2543 Hold
sip.use_out_ bound_in_di alog =	0 or 1	It enables or disables the phone to keep sending the SIP messages to the outbound server in a dialog. 0-Disabled 1-Enabled The default value is 1.	Phone->Features-> General Information->Use Outbound Proxy In Dialog
sip.reg_surg e_preventio n =	Integer from 0 to 60	It configures the time for the SIP registration. The phone registers an account at random in the time after bootup. The default value is 0.	Network->Advanc ed->Registration random-> Registration random
recovery_m ode.gatewa yip =	IP Address	It configures the IP address of the gateway when using the recovery mode for provisioning. The default value is 192.168.0.1.	Phone->Upgrade ->Recovery Mode>GatewayIP
recovery_m ode.phone_i p =	IP Address	It configures the IP address of the phone when using the recovery mode for provisioning. The default value is 192.168.0.100.	Phone->Upgrade ->Recovery Mode->IP
recovery_m ode.server_i p =	IP Address	It configures the IP address of the TFTP server when using the recovery mode for provisioning. The default value is 192.168.0.23.	Phone->Upgrade- >ServerIP

recovery_m ode.netmas k =	String	It configures the netmask when using the recovery mode for provisioning. The default value is 255.255.0.0.	Phone->Upgrade ->Recovery Mode->Netmask
handset.X.in coming_line s = (X ranges from 1 to 5.)	Number	It configures the lines to receive incoming calls for handset X. Each line ID should be separated by comma.	Account->Number Assignment-> Incoming lines
handset.X.n ame = (X ranges from 1 to 5.)	String	It configures the name of handset X. The default value is HX.	Account->Handset Name
handset.X.di al_out_defa ult_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.di al_out_lines = (X ranges from 1 to 5.)	Number	It configures the lines to place outgoing calls for handset X. Each line ID should be separated by comma.	Account->Number Assignment-> Outgoing lines
transfer.semi _attend_tran _enable =	0 or 1	It enables or disables the phone LCD screen of the transferee to display the missed call prompt when receiving a semi_attended transfer call. 0 -Disabled 1 -Enabled The default value is 1.	Phone->Features-> General Information-> Semi-Attended Transfer
transfer.blin d_tran_on_h ook_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-> General Information->Blind Transfer On Hook
transfer.on_h ook_trans_e nable =	0 or 1	It enables or disables the phone to complete the attended transfer through on-hook.	Phone->Features-> General Information ->Attended Trans

		0-Disabled 1-Enabled	OnHook
security.trust _certificates =	0 or 1	It enables or disables the phone to only accept the certificates in the Trusted Certificates list. 0-Disabled 1-Enabled The default value is 1.	Security->Trusted Certs->Only Accept Trusted Certificates
security.user _password =	String	It configures the login password of the user, var and administrator. The valid value format is username: password.	Security->Password
lang.wui =	English, Chinese_S, Turkish, Portuguese, Spanish, Italian, French or Deutsch	It configures the language of the web user interface.	Phone->Preference ->WEB Language
local_time.ti me_zone =	Integer from -11 to 12	It configures the time zone. The default value is +8.	Phone->Preference ->Time Zone
local_time.ti me_zone_na me =	String	It configures time zone name. The default time zone name is China(Beijing).	Phone->Preference ->Time Zone
local_time.nt p_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.	
local_time.nt p_server2 =	Domain Name or IP Address	It configures the domain name or IP address of the NTP server 2. The default value is cn.pool.ntp.org.	
local_time.in terval =	Integer	It configures the update interval (in seconds) when using the NTP server. The default value is 1000.	
local_time.s ummer_time =	0, 1 or 2	It enables or disables the daylight saving time (DST) feature. 0 -Disabled	Phone->Preference ->Daylight Saving Time

		1-Enabled	
		2-Automatic	
		The default value is 2	
local_time.d st_time_type =	0 or 1	It configures the DST type when the DST feature is enabled. 0 -By Date 1 -By Week The default value is 0.	Phone->Preference ->Fixed Type
local_time.st art_time =	MM/DD/HH	It configures the month, day and hour of day that DST starts. Value formats are: Month/Day/Hour (for By Date) Month/ Day of Week/ Day of Week Last in Month/ Hour of Day (for By Week) The default value is 1/1/0.	Phone->Preference ->Start Month/Start Date/Start Hour of Day (for By Date) Phone->Preference ->Start Month/Start Week Last in Month/ Start Day of Week/ Start Hour of Day (for By Week)
local_time.e nd_time =	MM/DD/HH	It configures the month, day and hour of day that DST ends. Value formats are: Month/Day/Hour (for By Date) Month/Week Last in Month/Day of Week/Hour of Day (for By Week) The default value is 12/31/23.	Phone->Preference ->Stop Month/ Stop Date/ End Hour of Day (for By Date) Phone->Preference ->Stop Month/ Stop Week Last in Month/ Stop Day of Week/ End Hour of Day (for By Week)
local_time.of fset_time =	Integer from -300 to 300	It configures the offset time (in seconds). The default value is 60	Phone->Preference ->Offset(minutes)
local_time.d hcp_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
local_time.m anual_time_	0 or 1	It configures the phone to set the time manually or obtain the time from the NTP	

enable =		server. 0 -Manual time 1 -NTP time The default value is 1.	
dialplan.are a_code.cod e =	Integer	It configures the area code. The default value is blank.	Phone->Dial Plan->Area Code->Code
dialplan.are a_code.min_ len =	Integer from 1 to 15	It configures the minimum length of the number prefixed with the area code. The default value is 1.	Phone->Dial Plan->Area Code->Minimum Length(1-15)
dialplan.are a_code.max _len =	Integer from 1 to 15	It configures the maximum length of the number prefixed with 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)
dialplan.are a_code.line_ id =	Number	It configures the lines applying the area code. Each line ID should be separated by comma. The default value is blank.	Phone->Dial Plan->Area Code->Account
dialplan.blo ck_out.numb er.X = (X ranges from 1 to 10.)	Number or String	It configures the block out number X. The default value is blank.	Phone->Dial Plan->Block Out->BlockOut NumberX
dialplan.blo ck_out.line_i d.X = (X ranges from 1 to 10.)	Number	It configures the lines applying the block out number X. Each line ID should be separated by comma. The default value is blank.	Phone->Dial Plan->Block Out->Account
dialplan.repl ace.prefix.X = (X ranges from 1 to 20.)	String	It configures the string to be replaced. The default value is blank.	Phone->Dial Plan->Replace Rule->Number
dialplan.repl ace.replace.	String	It configures the alternate string instead of what the user enters.	Phone->Dial Plan->Replace

X = (X ranges		The default value is blank.	Rule->Replace
from 1 to 20.)			
dialplan.repl ace.line_id.X = (X ranges from 1 to 20.)	Number	It configures the lines applying the replace rule. Each line ID should be separated by comma. The default value is blank.	Phone->Dial Plan->Replace Rule->Account
bw.feature_k ey_sync =	0 or 1	It enables or disables the feature key synchronization. 0 -Disabled 1 -Enabled The default value is 0.	
call_waiting. enable =	0 or 1	It enables or disables the call waiting feature. 0 -Disabled 1 -Enabled The default value is 1.	Phone->Features-> General Information->Call Waiting
call_waiting. tone =	0 or 1	It enables or disables the phone to play the call waiting tone. 0 -Disabled 1 -Enabled The default value is 1.	Phone->Features-> General Information->Call Waiting Tone
features.dnd _refuse_cod e =	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-> General Information-> Return Code When DND
features.nor mal_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-> General Information-> Return Code When Refuse
features.relo g_offtime =	Integer from 1 to 1000	It configures the overtime (in minutes) of logging the web user interface.	Phone->Features-> General

		The default value is 5.	Information-> logout_time(1~100 0)(minutes)
features.sav e_call_histor γ =	0 or 1	It enables or disables the phone to save call history. 0 -Disabled 1 -Enabled The default value is 1.	Phone->Features-> General Information->Save Call Log
phone_settin g.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 1.	Phone->Features-> General Information->180 Ringing Workaround
phone_settin g.emergenc y.number =	String	It configures the emergency numbers. The default value is blank.	Phone->Features-> General Information-> Emergency Numbers
firmware.url =	URL	It configures the access URL of firmware file.	
trusted_certif icates.url =	URL	It configures the access URL of the trusted certificate file.	
trusted_certif icates.delet e =	URL	It deletes all the trusted certificate files.	
server_certifi cates.url =	URL	It configures the access URL of the server certificate file.	
server_certifi cates.delete =	URL	It deletes all the server certificate files.	
auto_dst.url =	URL	It configures the access URL of the DST Time file.	
dialplan_rep lace_rule.url =	URL	It configures the access URL of the replace rule file.	
custom_fact ory_configur	URL	It configures the access URL of the customized factory configuration file.	

ation.url =			
configuratio n.url =	URL	It configures the access URL of the configuration file.	
openvpn.url =	URL	It configures the access URL of the openVPN tar file.	
custom_mac _cfg.url =	URL	It configures the access URL of the custom MAC-Oriented CFG file.	
blacklist.url =	URL	It configures the access URL of the blacklist file.	
handset.X.c ontact_list.ur l = (X ranges from 1 to 5.)	URL	It configures the access URL of the contact t file of handset X.	
xsi.user =	String	It configures the username provided on the Xtended Services Platform server. The default value is blank.	Contacts->Network Directories->XSI-> XSI Server
xsi.passwor d =	String	It configures the password provided on the Xtended Services Platform server. The default value is blank.	Contacts->Network Directories->XSI-> XSI Username
xsi.host =	URL	It configures the URL of the Xtended Services Platform server. The default value is blank.	Contacts->Network Directories->XSI-> XSI Password
bw_phoneb ook.group_e nable =	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 Directories->Direct ories->Group
bw_phoneb ook.group_c ommon_ena ble =	0 or 1	It enables or disables the GroupCommon item to be added to the BroadSoft phonebook. 0 -Disabled 1 -Enabled The default value is 0.	Contacts->Network Directories->Direct ories->GroupCom mom

bw_phoneb ook.enterpri se_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 Directories->Direct ories->Enterprise
bw_phoneb ook.enterpri se_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 Directories->Direct ories->EnterpriseC ommom
bw_phoneb ook.call_log _enable =	0 or 1	It enables or disables the network call log feature. 0 -Disabled 1 -Enabled The default value is 0.	Contacts->Network Directories->Direct ories->Network CollLog
remote_pho nebook.dat a.1.url =	URL	It configures the access URL of the remote phonebook.	Contacts->Remote Phone Book->Name
remote_pho nebook.dat a.1.name =	String	It configures the display name of the remote phonebook.	Contacts->Remote Phone Book->Phone Book URL
directory.up date_time_i nterval =	Integer from 60 to 86400	It configures the interval (in seconds) for the phone to update the data of the remote phonebook from the remote phonebook server. The default value is 1440.	Contacts->Remote Phone Book-> SRemoteNameFlas hTime(Minutes)(60- 86400)
voice.tone.c ountry =	Custom, Australia, Austria, Brazil, Belgium, China, China, Czech, Denmark, Finland, France,	It configures the tone type for the phone. The default value is Custom.	Phone->Tones

	Germany, Great Britain, Greece, Hungary, Lithuania, India, Italy, Japan,		
	Mexico, New Zealand, Netherlands, Norway, Portugal, Spain, Switzerland, Switzerland, Sweden, Russia, United States,		
	Chile, Czech ETSI		
voice.tone.r ing =	String	It customizes the ring tone when "voice.tone.country" is configured as Custom. The value format is F/D. F: the frequency of the tone (ranges from 200 to 7000 Hz). D: the time duration (in milliseconds, ranges from 0 to 30000ms) of playing the tone. You can configure at most eight different tones for one condition, each tone separated by comma (e.g. 250/200, 0/1000, 200/500, 1000/2000). The default value is blank.	Phone->Tones
voice.tone. busy =	String	It customizes the busy tone when "voice.tone.country" is configured as Custom. The value format is F/D. The default value is blank.	Phone->Tones
voice.tone.c allwaiting =	String	It customizes the call waiting tone when "voice.tone.country" is configured as	Phone->Tones

		Custom.	
		The value format is F/D.	
		The default value is blank.	
account.X.e nable = (X ranges	0 or 1	It enables or disables the account X. 0 -Disabled 1 -Enabled	Account->Basic-> Account Active
from 1 to 5.)		The default value is 0.	
account.X.la bel = (X ranges from 1 to 5.)	String	It configures the label displayed on the LCD screen for account X. The default value is blank.	Account->Basic-> Label
account.X.di splay_name = (X ranges from 1 to 5.)	String	It configures the display name for account X. The default value is blank.	Account->Basic-> Name
account.X.a uth_name = (X ranges from 1 to 5.)	String	It configures the username for register authentication for account X. The default value is blank.	Account->Basic-> Name
account.X.p assword = (X ranges from 1 to 5.)	String	It configures the password for register authentication for account X. The default value is blank.	Account->Basic-> Password
account.X.us er_name = (X ranges from 1 to 5.)	String	It configures the register username for account X. The default value is blank.	Account->Basic-> Register Name
account.X.si p_server_ho st = (X ranges from 1 to 5.)	Domain Name or IP Address	It configures the domain name or IP address of the SIP server for account X. The default value is blank.	Account->Basic-> SIP Server
account.X.si p_server_po rt = (X ranges from 1 to 5.)	Integer	It configures the port of the SIP server for account X. The default value is 5060.	Account->Basic-> SIP Server->Port

account.X.tr ansport = (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.o utbound_pro xy_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. 0 -Disabled 1 -Enabled The default value is 0.	Account->Basic-> Enable Outbound Proxy Server
account.X.o utbound_hos t = (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.o utbound_por t = (X ranges from 1 to 5.)	Integer	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.b ackup_outb ound_host = (X ranges from 1 to 5.)	Domain Name or IP Address	It configures the domain name or IP address of the backup outbound proxy server for account X. The default value is blank.	Account->Basic-> Backup Outbound Proxy Server
account.X.b ackup_outb ound_port = (X ranges from 1 to 5.)	Integer	It configures the port of the backup outbound proxy server for account X. The default value is 5060.	Account->Basic-> Backup Outbound Proxy Server->Port
voice_mail.n umber.X = (X ranges from 1 to 5.)	String	It configures the voice mail access code for account X. The default value is blank.	Phone->Features-> LineX->voice mail
account.X.pr oxy_require	String	It configures the proxy server for account X.	Account->Basic-> Proxy Require

=		The default value is blank.	
(x ranges from 1 to 5.)			
account.X.a nonymous_c all = (X ranges from 1 to 5.)	0 or 1	It enables or disables the anonymous call feature for account X. 0 -Disabled 1 -Enabled The default value is 0.	Phone->Features-> LineX->Anonymous Call->Anonymous Call
account.X.a nonymous_c all_oncode = (X ranges from 1 to 5.)	String	It configures the anonymous call on code for account X. The default value is blank.	Phone->Features-> LineX->Anonymous Call->Anonymous Call On Code
account.X.a nonymous_c all_offcode = (X ranges from 1 to 5.)	String	It configures the anonymous call off code for account X. The default value is blank.	Phone->Features-> LineX->Anonymous Call-> Anonymous Call Off Code
account.X.re ject_anonym ous_call = (X ranges from 1 to 5.)	0 or 1	It enables or disables the anonymous call rejection feature for account X. 0 -Disabled 1 -Enabled The default value is 0.	Phone->Features-> LineX->Anonymous Call-> Anonymous Call Rejection
account.X.a nonymous_r eject_oncod e = (X ranges from 1 to 5.)	String	It configures the anonymous call rejection on code for account X. The default value is blank.	Phone->Features-> LineX->Anonymous Call->Anonymous Call Rejection On Code
account.X.a nonymous_r eject_offcod e = (X ranges from 1 to 5.)	String	It configures the anonymous call rejection off code for account X. The default value is blank.	Phone->Features-> LineX->Anonymous Call->Anonymous Call Rejection Off Code
account.X.si p_listen_port	Integer	It configures the SIP port for account X. The default value is 5060.	Account-> Advanced->Local

= (X ranges from 1 to 5.)			SIP Port
account.X.ex pires = (X ranges from 1 to 5.)	Integer	It configures the register expiry time (in seconds) for account X. The default value is 3600.	Account-> Advanced->Login Expire (seconds)
account.X.10 0rel_enable = (X ranges from 1 to 5.)	0 or 1	It enables or disables the 100 reliable retransmission feature for account X. 0 -Disabled 1 -Enabled The default value is 1.	Account-> Advanced->100 reliable retransmission
account.X.pr econdition = (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.su bscribe_regi ster = (X ranges from 1 to 5.)	0 or 1	It enables or disables the phone to subscribe the register status for account X. 0 -Disabled 1 -Enabled The default value is 0.	Account-> Advanced-> Subscribe Register
account.X.su bscribe_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.ci d_source = (X ranges from 1 to 5.)	0 or 1	It configures the SIP header(s) from which the phone reads the caller ID and presents on the LCD screen when receiving an incoming call. 0 -FROM 1 -PAI The default value is 0.	Account-> Advanced->Caller ID Header
account.X.se ssion_timer.e	0 or 1	It enables or disables the session timer for account X.	Account-> Advanced->Use

nable =		0-Disabled	Session Timer
(X ranges		1-Enabled	
from 1 to 5.)		The default value is 0.	
account.X.se ssion_timer.e xpires = (X ranges from 1 to 5.)	Integer from 1 to 9999	It configures the interval (in seconds) for refreshing the SIP session for account X. The default value is blank.	Account-> Advanced-> Session Timer (seconds)
account.X.se ssion_timer.r efresher = (X ranges from 1 to 5.)	0 or 1	It configures the refresher of the session timer for account X. 0 -Uac 1 -Uas The default value is 0.	Account-> Advanced-> Refresher
account.X.e nable_user_ equal_phon e = (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.srt p_encryptio n = (X ranges from 1 to 5.)	0 or 1	It enables or disables the voice encryption service for account X. 0 -Disabled 1 -Enabled The default value is 0.	Account-> Advanced->Voice Encryption(SRTP)
account.X.pt ime = (X ranges from 1 to 5.)	0 (Disabled), 10, 20, 30, 40, 50 or 60.	It configures the RTP packet time for account X. The default value is 20.	Account-> Advanced->Ptime (ms)
account.X.su bscribe_mwi _expires = (X ranges from 1 to 5.)	Integer from 0 to 84600	It configures MWI subscribe expiry time (in seconds) for account X. The default value is 3600.	Account-> Advanced->MWI Subscription Period (Scope:0~84600) (seconds)
account.X.su bscribe_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	Account-> Advanced-> SubscribeMWIToV M

		The default value is 0.	
account.X.re gister_mac = (X ranges from 1 to 5.)	0 or 1	It enables or disables the phone to send the MAC address in the register message for account X. 0 -Disabled 1 -Enabled The default value is 0.	Account-> Advanced->SIP Send MAC
account.X.re gister_line = (X ranges from 1 to 5.)	0 or 1	It enables or disables the phone to send 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.re g_fail_retry_i nterval = (X ranges from 1 to 5.)	Integer from 0 to 1800	It configures the interval (in seconds) the phone retries to register account X when registration fails. The default value is 30.	Account-> Advanced->SIP Registration Retry Timer(Scope:0~180 0)(seconds)
account.X.e nable_signal _encode = (X ranges from 1 to 5.)	0 or 1	It enables or disables the phone to encode SIP signal for account X. 0 -Disabled 1 -Enabled (RC4) The default value is 0.	Account-> Advanced->Signal Encode
account.X.si gnal_encod e_key = (X ranges from 1 to 5.)	String	It configures the key for the phone to encode the SIP signal with RC4 for account X. The default value is blank.	Account-> Advanced->Signal Encode Key
account.X.dt mf.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.dt mf.dtmf_pay	Integer from 96 to 225	It configures the RFC2833 payload for account X.	Account-> Advanced->DTMF

load = (X ranges from 1 to 5.)		The default value is 101.	Payload(scope:96~ 255)
account.X.dt mf.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.n at.nat_traver sal = (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.n at.stun_serv er = (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
account.X.n at.stun_port = (X ranges from 1 to 5.)	Integer	It configures the port of the STUN server for account X. The default value is 3478.	Account->Basic-> STUN Server->Port
account.X.n at.udp_upd ate_enable = (X ranges from 1 to 5.)	0 or 1	It enables or disables the NAT keep-alive for account X. 0 -Disabled 1 -Enabled The default value is 0.	Account-> Advanced->UDP Keep-alive Message
account.X.n at.udp_upd ate_time = (X ranges from 1 to 5.)	Integer	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.n at.rport = (X ranges from 1 to 5.)	0 or 1	It enables or disables the NAT Rport for account X. 0 -Disabled 1 -Enabled The default value is 0.	Account-> Advanced->Rport
---	--	--	---
account.X.a dvanced.tim er_t1 = (X ranges from 1 to 5.)	Float	It configures the session timer T1 (in seconds) for account X. The default value is 0.5.	Account-> Advanced->SIP Session Timer (seconds) T1
account.X.a dvanced.tim er_t2 = (X ranges from 1 to 5.)	Float	It configures the session timer T2 (in seconds) for account X. The default value is 4.	Account-> Advanced->SIP Session Timer (seconds) T2
account.X.a dvanced.tim er_t4 = (X ranges from 1 to 5.)	Float	It configures the session timer T4 (in seconds) for account X. The default value is 5.	Account-> Advanced->SIP Session Timer (seconds) T4
account.X.co dec.Y.enabl e = (X ranges from 1 to 5. Y ranges from 1 to 13.)	0 or 1	It enables or disables the specified codec for account X. 0 -Disabled 1 -Enabled	Account->Codecs
account.X.co dec.Y.paylo ad_type = (X ranges from 1 to 5. Y ranges from 1 to 13.)	PCMU, PCMA, G723_53, G723_63, G729, G722, G726-16, G726-24, G726-24, G726-32, G726-40	It configures the payload type of the specified codec for account X.	Account->Codecs
account.X.co dec.Y.priorit y = (X ranges	Integer from 0 to 10	It configures the priority of the enabled codec for account X.	Account->Codecs

from 1 to 5. Y ranges from 1 to 13.)			
account.X.co dec.Y.rtpma p = (X ranges from 1 to 5. Y ranges from 1 to 13.)	Integer	It configures rtpmap of the audio codec for account X.	
account.X.d nd.enable = (X ranges from 1 to 5.)	0 or 1	It enables or disables the DND feature for account X. 0 -Disabled 1 -Enabled The default value is 0.	Phone->Features-> LineX->DND ->DND
account.X.d nd.on_code = (X ranges from 1 to 5.)	String	It configures the DND on code for account X. The default value is blank.	Phone->Features-> LineX->DND->On Code
account.X.d nd.off_code = (X ranges from 1 to 5.)	String	It configures the DND off code for account X. The default value is blank.	Phone->Features-> LineX->DND->Off Code
account.X.al ways_fwd.e nable = (X ranges from 1 to 5.)	0 or 1	It enables or disables the always forward feature for account X. 0 -Enabled 1 -Disabled The default value is 0.	Phone->Features-> LineX->Forward-> Alawys
account.X.al ways_fwd.ta rget = (X ranges from 1 to 5.)	String	It configures the target number of the always forward feature for account X. The default value is blank.	Phone->Features-> LineX->Forward-> Always->Target
account.X.b usy_fwd.ena ble = (X ranges	0 or 1	It enables or disables the busy forward feature for account X. 0 -Enabled	Phone->Features-> LineX->Forward->B usy

from 1 to 5.)		1-Disabled	
		The default value is 0.	
account.X.b usy_fwd.targ et = (X ranges from 1 to 5.)	String	It configures the target number of the busy forward feature for account X. The default value is blank.	Phone->Features-> LineX->Forward->B usy->Target
account.X.ti meout_fwd. enable = (X ranges from 1 to 5.)	0 or 1	It enables or disables the timeout forward feature for account X. 0 -Enabled 1 -Disabled The default value is 0.	Phone->Features-> LineX->Forward-> No Answer
account.X.ti meout_fwd.t arget = (X ranges from 1 to 5.)	String	It configures the target number of the timeout forward feature for account X. The default value is blank.	Phone->Features-> LineX->Forward-> No Answer->Target
account.X.ti meout_fwd.ti meout = (X ranges from 1 to 5.)	0, 6, 12, 120	It configures the ring time before forwarding the incoming call for account X. The default value is 0.	Phone->Features-> LineX->Forward-> No Answer->After Ring Time(seconds)
account.X.al ways_fwd.of f_code = (X ranges from 1 to 5.)	String	It configures the always forward off code for account X. The default value is blank.	Phone->Features-> LineX->Forward-> Always->Off Code
account.X.al ways_fwd.o n_code = (X ranges from 1 to 5.)	String	It configures the always forward on code for account X. The default value is blank.	Phone->Features-> LineX->Forward-> Always->On Code
account.X.b usy_fwd.off_ code = (X ranges from 1 to 5.)	String	It configures the busy forward off code for account X. The default value is blank.	Phone->Features-> LineX->Forward->B usy->Off Code
account.X.b usy_fwd.on_	String	It configures the busy forward on code for account X.	Phone->Features-> LineX->Forward->B

code = (X ranges from 1 to 5.)		The default value is blank.	usy->On Code
account.X.ti meout_fwd. off_code = (X ranges from 1 to 5.)	String	It configures the timeout forward off code for account X. The default value is blank.	Phone->Features-> LineX->Forward-> No Answer->Off Code
account.X.ti meout_fwd. on_code = (X ranges from 1 to 5.)	String	It configures the timeout forward on code for account X. The default value is blank.	Phone->Features-> LineX->Forward-> No Answer->On Code