

# Yealink SIP IP Phones Auto Provisioning Guide

# **Table of Contents**

Table of Contents	iii
Introduction	1
Supported Phones	1
Getting Started	3
Obtaining Boot, Configuration and Resource Files	
Boot Files	
Configuration Files	
Resource Files	
Obtaining Template Files	5
Obtaining Phone Information	5
Provisioning Yealink IP Phones	7
Interoperating with Provisioning Server	7
Auto Provisioning Process	
Old Mechanism – Without Boot Files	
New Mechanism – With Boot Files	9
Major Tasks for Auto Provisioning	
An Instance of Auto Provision Configuration	12
Managing Boot Files	15
Editing Common Boot File	
Creating MAC-Oriented Boot File	17
Managing Configuration Files	19
Editing Common CFG File	
Editing MAC-Oriented CFG File	
Creating a New CFG File	
Managing MAC-local CFG File	
Encrypting Configuration Files	
Managing Resource Files	25
Customizing Resource Files	

Configuring a Provisioning Server	27
Preparing a Root Directory	27
Configuring a TFTP Server	28
Obtaining the Provisioning Server Address	31
Zero Touch	31
Plug and Play (PnP) Server	33
DHCP Options	34
Phone Flash	35
Configuring Wildcard of the Provisioning Server URL	36
Triggering the IP Phone to Perform Auto Provisioning	39
Power On	39
Repeatedly	40
Weekly	41
Flexible Auto Provision	42
Auto Provision Now	43
Multi-mode Mixed	44
SIP NOTIFY Message	44
Auto Provisioning via Activation Code	45
Downloading and Verifying Configurations	49
Downloading Boot, Configuration and Resource Files	49
Resolving and Updating Configurations	49
Using MAC-local CFG File	50
Verifying Configurations	50
Troubleshooting	53
Glossary	55
Appendix	57
Configuring an FTP Server	57
Preparing a Root Directory	57
Configuring an FTP Server	58
Configuring an HTTP Server	60
Preparing a Root Directory	60

Configuring an HTTP Server61
------------------------------

# Introduction

Yealink IP phones are full-featured telephones that can be plugged directly into an IP network and can be used easily without manual configuration.

This guide provides instructions on how to provision Yealink IP phones with the minimum settings required. Yealink IP phones support FTP, TFTP, HTTP, and HTTPS protocols for auto provisioning and are configured by default to use the TFTP protocol.

# **Supported Phones**

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

The following table lists product names and available firmware versions for IP phones that use auto provisioning process outlined in this guide.

Product Name	Boot File	Exclude Mode
	(Available Firmware	(Available Firmware
	version)	version)
VP59	Yes (83 or later)	Yes (83 or later)
SIP-T58A	Yes (80 or later)	Yes (83 or later)
SIP-T33P/T33G/T31P/T31G/T31/T30P/T30	Yes (85 or later)	Yes (85 or later)
SIP- T57W/T54W/T53W/T53	Yes (84 or later)	Yes (84 or later)
SIP-T48U/T46U/T43U/T42U	Yes (84 or later)	Yes (84 or later)
SIP-T48G/S	Yes (81 or later)	Yes (83 or later)
SIP-T46G/S	Yes (81 or later)	Yes (83 or later)
SIP-T42G/S	Yes (81 or later)	Yes (83 or later)
SIP-T41P/S	Yes (81 or later)	Yes (83 or later)
SIP-T40P/G	Yes (81 or later)	Yes (83 or later)
SIP-T29G	Yes (81 or later)	Yes (83 or later)
SIP-T27G	Yes (81 or later)	Yes (83 or later)
SIP-T23P/G	Yes (81 or later)	Yes (83 or later)
SIP-T21(P) E2	Yes (81 or later)	Yes (83 or later)
SIP-T19(P) E2	Yes (81 or later)	Yes (83 or later)
CP860	Yes (81 or later)	No

Product Name	Boot File (Available Firmware Version)	Exclude Mode (Available Firmware Version)
CP960	Yes (80 or later)	Yes (83 or later)
CP920	Yes (81 or later)	No
W60P	Yes (81 or later)	No
W53P	Yes (83 or later)	No
CP930W-Base	Yes (83 or later)	No
W52P W56P	Yes (81 or later)	No

We recommend that IP phones running the latest firmware should not be downgraded to an earlier firmware version. The new firmware is compatible with old configuration parameters, but not vice versa.

## **Getting Started**

This section provides instructions on how to get ready for auto provisioning. To begin the auto provisioning, the following steps are required:

- Obtaining Boot, Configuration and Resource Files
- Obtaining Phone Information

## **Obtaining Boot, Configuration and Resource Files**

### **Boot Files**

The IP phone tries to download the boot file first, and then download the configuration files referenced in the boot file during auto provisioning. You can select whether to use the boot file or not according to your deployment scenario. If required, you need to obtain the template boot file named as "y0000000000000.boot" before auto provisioning.

You can use a boot file to specify which configuration files to be downloaded for specific phone groups by phone model identity, and customize the download sequence of configuration files. It is efficient for you to provision IP phones in different deployment scenarios, including all IP phones, specific phone groups, or a single phone.

The configuration files referenced in the boot file are flexible: you can rearrange the configuration parameters within the Yealink-supplied template configuration files or create your own configuration files from configuration parameters you want. You can create and name as many configuration files as you want and your own configuration files can contain any combination of configuration parameters.

### **Configuration Files**

Before provisioning, you also need to obtain template configuration files. There are two configuration files both of which are CFG-formatted. We call these two files Common CFG file and MAC-Oriented CFG file.

The configuration files contain parameters that affect the features of the phone. You can use the configuration files to deploy and maintain a mass of Yealink IP phones automatically.

You can create and name as many configuration files as you want (for example, account.cfg, sip.cfg, features.cfg) by using the template configuration files. The custom configuration files can contain the configuration parameters of the same feature modules for all phones.

## **Resource Files**

When configuring some particular features, you may need to upload resource files to IP phones, such as personalized AutoDST file, language package file, and local contact file. Resource files are optional, but if the particular feature is being employed, these files are required.

Yealink supplies the following resource file templates:

Feature	Template File Name
DST	AutoDST.xml
	For example,
Languago Packs	000.GUI.English.lang
Language racks	1.English_note.xml
	1.English.js
Replace Rule	dialplan.xml
Dial-now	dialnow.xml
	CallFailed.xml
Softkey Layout	CallIn.xml
(not applicable to	Connecting.xml
CP960/W52P/W53P/W5	Dialing.xml (not applicable to
6P/W60P/CP930W-Base	VP59/T58A/T57W/T48U/T48G/T48S phones)
phones)	RingBack.xml
	Talking.xml
Directory	favorite_setting.xml
Super Search in dialing	super_search.xml
Local Contact File	contact.xml
Remote XML Phone	Department.xml
Book	Menu.xml
Screen Saver	
(not applicable to	
VP59/T58A/CP960/W52	CustomScreenSaver.xml
P/W53P/W56P/W60P/C	
P930W-Base phones)	
	X.83.0.XX.rom
Firmware	For example,
	44.83.0.10.rom

### **Obtaining Template Files**

You can ask the distributor or Yealink FAE for template files. You can also obtain them online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage.

To download template boot, configuration and resource files:

- 1. Go to Yealink Document Download page and select the desired phone model.
- 2. Download and extract the combined template files to your local system.

For example, the following illustration shows the template files available for SIP-T23G IP phones running firmware version 82.



3. Open the folder you extracted and identify the files you want to edit.

## **Obtaining Phone Information**

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

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

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

# **Provisioning Yealink IP Phones**

This section provides instructions on how IP phones interoperate with provisioning server for auto provisioning, and shows you the auto provisioning process and the four major tasks to provision the phones. It will help users who are not familiar with auto provisioning to understand this process more easily and quickly.

# Interoperating with Provisioning Server

When IP phones are triggered to perform auto provisioning, they will request to download the boot files and configuration files from the provisioning server. During the auto provisioning, the IP phone will download and update configuration files to the phone flash.

The following figure shows how the IP phone interoperates with the provisioning server:



IP Phone

Request to Download Boot Files and Configuration Files



Download Boot Files, Configuration Files and Update Configuration Files



**Provisioning Server** 

# **Auto Provisioning Process**

### **Old Mechanism – Without Boot Files**

The following flowchart shows how Yealink IP phones perform auto provisioning when using configuration files only:



## **New Mechanism – With Boot Files**

The following figure shows auto provisioning flowcharts for Yealink IP phones when using boot files:





### Scenario B – Support Exclude Mode

This scenario is only applicable to IP phones (except W52P/W56P IP phones) running firmware version 83 or later.



## **Major Tasks for Auto Provisioning**

You need to complete four major tasks to provision Yealink IP phones.

The following figure shows an overview of four major provisioning tasks:



For more information on how to manage boot files, refer to Managing Boot Files.

For more information on how to manage configuration files, refer to Managing Configuration Files.

For more information on how to manage resource files, refer to Managing Resource Files.

For more information on how to configure a provisioning server, refer to Configuring a Provisioning Server.

For more information on how to obtain the provisioning server address, refer to Obtaining the Provisioning Server Address.

For more information on how to perform auto provisioning, refer to Triggering the IP Phone to Perform Auto Provisioning.

If you are not familiar with auto provisioning on Yealink IP phones, you can refer to An Instance of Auto Provision Configuration.

## An Instance of Auto Provision Configuration

This section shows an instance of auto provision configuration.

1. Manage boot files.

Specify the desired URL (for example, tftp://10.2.5.193/network.cfg) of the configuration files in the boot file (for example, y00000000000.boot). For more information, refer to Managing Boot Files.

```
#!version:1.0.0.1
## The header above must appear as-is in the first line
##[$MODEL]include:config <xxx.cfg>
##[$MODEL,$MODEL]include:config "xxx.cfg"
[T46S]include:config <tftp://10.2.5.193/network.cfg>
[T48S,T46G]include:config <../sip.cfg>
include:config "features.cfg"
overwrite_mode = 1
specific_model.excluded_mode=0
```

2. Manage configuration files.

Add/Edit the desired configuration parameters in the CFG file (for example, features.cfg) you want the IP phone to download. For more information on how to manage configuration files, refer to Managing Configuration Files.

features.cfg x i \_\_\_\_\_\_10\_\_\_\_20\_\_\_\_\_30\_\_\_\_40\_\_\_\_50\_\_\_\_\_
#!version:1.0.0.1
features.dnd\_mode = 0
features.dnd.enable = 1
ringtone.url = tftp://10.2.5.193/Customring.wav

- 3. Configure the TFTP server.
  - Place boot files, configuration files and resource files to TFTP root directory (for example, D:\TFTP Directory).



Daemon				
<u>V</u> iew <u>H</u> elp				
TFTP Server	Start Time	Peer	Bytes	Status
Configure IFTF Server	Jul 12, 2016 09:30:13	local	0	Listening for TFTP requests on IP address: 10.2.5.193 Port 69
TFIP Server is started.		_	The	server URL where the IP phone
Click here to stop it.		_	CI.	
			Tiles	s from is titp://10.2.5.193/
Logging to Tftpd log. Click to stop.				
×				
Not debugging. Click to start.				
Clear list.				
View Log/Debug files.				

2) Start the TFTP server. The IP address of the TFTP server is shown as below:

 Select Configure TFTP Server. Click the ... button to locate the TFTP root directory in your local system.

3CDaemon				
<u>File V</u> iew <u>H</u> elp				
TFTP Server	Start Time	Peer	Bytes	Status
	Jul 12, 2016 09:30:13	local	0	Listening for TFTP requests on IP address: 10.2.5.193, Port 69
Configure TFTP Server	3CDaemon Configurat	ion		×
<b>STP</b>	FTP Profil General Con	les figurat	ion	Syslog Configuration TFTF Configuration
TFTP Server is started. Click here to stop it.	Create directory n	ames in	. incomi	ng file re√
	Allow overwrite of	existi	ng file	s?
Logging to lftpd.log. Click to stop.	Upload/Download	I	): \TFTP	Directory\
	Per-packet timeout	in sec	onds	5
Not debugging. Click to start.	Maximum retries			10
Clear list.	Interframe transmis	sion		0
View Log/Debug files.				

For more information on how to configure a provisioning server, refer to Configuring a Provisioning Server.

4. Configure the provisioning server address on the IP phone.

Yealink							E	Log Out English(English) 🗸
	Status	Account	Network	DSSKey	Features	Settings	Directory	Security
Preference	A	uto Provision					NOTE	
Time & Data	PN	IP Active		🖲 On 🔘 Off			Auto Provi	ision
Time & Date	DH	ICP Active		🖲 On 💿 Off			The IP phor	ne can interoperate
Call Display	Cu	istom Option(128-	~254)				ing server using ning for deploying	
Upgrade	DF	ICP Option Value					the IP phon	ies.
Auto Provision	Se	erver URL		tftp://10.2.5.193/			When the I perform aut	P phone triggers to to provisioning, it will
	Us	er Name					request to a	download the n files from the
Configuration	Pa	ssword			Entor	r the access	LIPL of	server. During the
Dial Plan	At	tempt Expired Tim	ne(s)	5	the pr	ovisioning	server in	ill download and
Voice	Co	mmon AES Key			the	Server URL	field.	nguration files to the
Dise	MA	AC-Oriented AES K	ley				You can	click here to get
Rang	Ze	ro Active		Disabled	•		more guide	s.
Tones	W	ait Time(1~100s)		5				
Softkey Layout	Po	wer On		🖲 On 🔘 Off				

For more information on how to obtain the provisioning server address, refer to Obtaining the Provisioning Server Address.

									Log Out			
N	ealink m							Eng	glish(English) 🔹			
		Status	Account	Network	DSSKey	Features	Settings	Directory	Security			
1	Preference		Auto Provision					NOTE	•			
			PNP Active		🔹 On 💿 Off				100			
	Time & Date		DHCP Active		🖲 On 🔘 Off			The IP phone	can interoperate			
	Call Display		Custom Option(128	⊷254)				with provsional auto provisioni	ng server using ing for deploying			
	Upgrade		DHCP Option Value					the IP phones	ь.			
I	Auto Provision		Server URL		tftp://10.2.5.193/	r		When the IP phone triggers to perform auto provisioning, it will				
l	Contraction of the second s		User Name					request to do configuration f	wnload the files from the			
	Configuration		Password		•••••			provisioning se auto provision	ever. During the			
	Dial Plan		Attempt Expired Ti	me(s)	5			IP phone will a	download and			
	Voice		Common AES Key		•••••			phone flash.	unacion nes co che			
	Dino		MAC-Oriented AES	Key				You can d	lick here to get			
	kang		Zero Active		Disabled	-		more guides.				
	Tones		Wait Time(1~100s)	1	5							
	Softkey Layout		Power On		🖲 On 🔿 Off							
	TR069		Repeatedly		O On 💌 Off							
			Interval(Minutes)		1440							
	Voice Monitoring		Weekly		🔿 On 💌 Off							
	SIP		Weekly Upgrade In	terval(0~12week)	4							
			Inactivity Time Exp	re(0~120min)	0							
			Time		00 : 00 - 00	: 00						
			Day of Week		Sunday Monday Monday U Tuesday U tuesday U thursday U Friday Saturday U Saturday	Click th perfor	e <b>Autop</b> i m the au	rovision No to provisio	ow to oning			
			Flexible Auto Provis	ion	O on 🖲 off	pr	ocess im	mediately.				
			Flexible Interval Day	s	30	7	-					
			Flexible Time		- 00 : 50							
			Con	ferm	Autoprovision	Cancel						

5. Trigger the IP phone to perform auto provisioning.

For more information on how to trigger the phone to perform auto provisioning, refer to Triggering the IP Phone to Perform Auto Provisioning.

# **Managing Boot Files**

Yealink IP phones can download CFG files referenced in the boot files. Before provisioning, you may need to edit and customize your boot files.

Yealink supports the following two types of boot files:

- MAC-Oriented boot file (for example, 00156574b150.boot)
- Common boot file (y00000000000.boot)

You can edit the template boot file directly or create a new boot file as required. Open each boot file with a text editor such as Notepad++.

### **Editing Common Boot File**

The common boot file is effective for all phones. It uses a fixed name "y000000000000.boot" as the file name.

The following figure shows the contents of the common boot file:

```
#!version:1.0.0.1
## The header above must appear as-is in the first line
include:config <xxx.cfg>
include:config "xxx.cfg"
overwrite_mode = 1
```

The following table lists guidelines you need to know when editing the boot file:

Item	Guidelines
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
## The header above must appear as-is in the first line	The line beginning with "#" is considered to be a comment. You can use "#" to make any comment in the boot file.
include:config <xxx.cfg> include:config "xxx.cfg"</xxx.cfg>	<ol> <li>Each "include" statement can specify a URL where a configuration file is stored. The configuration file format must be *.cfg.</li> <li>The URL in &lt;&gt; or "" supports the following two forms:         <ul> <li>Relative URL (relative to the boot file): For example, sip.cfg, HTTP Directory/sip.cfg</li> <li>Absolute URL:</li> </ul> </li> </ol>

ltem	Guidelines					
	For example, http://10.2.5.258/HTTP Directory/sip.cfg The URL must point to a specific CFG file. The CFG files are downloaded in the order listed (top to bottom). The parameters in the newly downloaded configuration files will override the duplicate parameters in files downloaded earlier.					
	<ul> <li>3) The "include" statement can be repeated as many times as needed.</li> </ul>					
	4) The [\$MODEL] can be added to specify settings for specific phone models. \$MODEL represents the phone model name. The valid phone model names are: VP59, T58, CP960, T57W, T54W, T53W, T53, T48U, T48S, T48G, T46U, T46S, T46G, T43U, T42U, T42S, T42G, T41P, T41S, T40P, T40G, T33P, T33G, T31P, T31G, T31, T30P, T30, T29G, T27G, T23P, T23G, T21P_E2, T19P_E2 and CP920. Multiple phone models are separated by commas. For example, [T46S, T23G]. It is only applicable to IP phones (except W53P/W60P/CP930W-Base) running firmware version 83 or later.					
	<b>Note</b> : The phone model name T21P_E2 is applicable to T21P E2 and T21 E2 phones.					
ovorwrite, mede	Enable or disable the overwrite mode. <b>1</b> -(Enabled) - If the value of a parameter in configuration files is left blank, or if a non-static parameter in configuration files is deleted or commented out, the factory default value takes effect.					
overwrite_mode	<ul> <li>O-(Disabled) - If the value of a parameter in configuration files is left blank, deleted or commented out, the pre-configured value is kept.</li> <li>Note: This parameter can only be used in boot files. If a boot file is used but the value of the parameter "overwrite_mode" is not configured, the overwrite mode is enabled by default.</li> </ul>					
	Enable or disable the exclude mode. The exclude mode applies to the configuration files specified in the boot file.					
	<b>0</b> -Disabled (Append Mode), the phone downloads its own model-specific configuration files and downloads other model-unspecified configuration files.					
specific_model.excluded _mode	<b>1</b> -Enabled (Exclude Mode), the phone attempts to download its own model-specific configuration files; if there are no own model-specific configuration files found on the server, it downloads model-unspecified configuration files.					
	<b>Note</b> : Exclude mode can only be used in boot files. If a boot file is used but the value of the parameter "specific_model.excluded_mode" is not configured, the exclude mode is disabled by default. Exclude mode					

Item	Guidelines				
	feature is only applicable to IP phones (except				
	W53P/W60P/CP930W-Base) running firmware version 83 or later.				

## **Creating MAC-Oriented Boot File**

The MAC-Oriented boot file is only effective for the specific phone. It uses the 12-digit MAC address of the IP phone as the file name. For example, if the MAC address of the IP phone is 00156574B150, the MAC-Oriented boot file has to be named as 00156574b150.boot (case-sensitive) respectively.

If you want to create a MAC-Oriented boot file for your phone, follow these steps:

### To create a MAC-Oriented boot file:

- 1. Create a boot file for your phone. Ensure the file complies with the guidelines that are listed in the Editing Common Boot File.
- 2. Copy the contents from the common boot file and specify the configuration files to be downloaded.

One or more configuration files can be referenced in the boot file. The following takes two configuration files for example:

3. Save the changes and close the MAC-Oriented boot file.

You can also make a copy of the common boot file, rename it and then edit it.

# **Managing Configuration Files**

Auto provisioning enables Yealink IP phones to update themselves automatically via downloading Common CFG, MAC-Oriented CFG, custom CFG, and MAC-local CFG files. Before provisioning, you may need to edit and customize your configuration files.

You can edit the template configuration files directly or create a new CFG file as required. Open each configuration file with a text editor such as Notepad++.

For more information on the description of all configuration parameters in configuration files, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

## **Editing Common CFG File**

The Common CFG file is effective for all phones of the same model. It uses a fixed name "y000000000XX.cfg" as the file name, where "XX" equals to the first two digits of the hardware version of the IP phone model.

The names of the common C	G file requirements for the phone are:
---------------------------	--

Product Name	Common CFG File
CP960	y00000000073.cfg
VP59	y00000000091.cfg
SIP-T58A	y00000000058.cfg
SIP-T57W	y00000000097.cfg
SIP-T54W	y00000000096.cfg
SIP-T53W/T53	y00000000095.cfg
SIP-T48U	y00000000109.cfg
SIP-T46U	y00000000108.cfg
SIP-T43U	y00000000107.cfg
SIP-T42U	y00000000116.cfg
SIP-T48S	y00000000065.cfg
SIP-T46S	y00000000066.cfg
SIP-T42S	y00000000067.cfg
SIP-T41S	y0000000068.cfg
SIP-T48G	y00000000035.cfg
SIP-T46G	y00000000028.cfg

Product Name	Common CFG File
SIP-T42G	y00000000029.cfg
SIP-T41P	y00000000036.cfg
SIP-T40P	y00000000054.cfg
SIP-T40G	y00000000076.cfg
SIP-T33P/T33G	y00000000124.cfg
SIP-T31P/T31G/T31	y00000000123.cfg
SIP-T30P/T30	y00000000127.cfg
SIP-T29G	y00000000046.cfg
SIP-T27G	y00000000069.cfg
SIP-T23P/G	y00000000044.cfg
SIP-T21(P) E2	y00000000052.cfg
SIP-T19(P) E2	y00000000053.cfg
CP860	y00000000037.cfg
CP920	y00000000078.cfg
W53P/W60P/CP930W-Base	y00000000077.cfg
W52P/W56P	y00000000025.cfg

Common CFG file contains configuration parameters which apply to phones with the same model, such as language and volume.

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

The following table lists guidelines you need to know when editing the common CFG file:

-				
	•	10	-	
	-			

Guidelines

Item	Guidelines				
#	The line beginning with "#" is considered to be a comment.				
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.				
Filename	The filename complies with the requirements that are listed in the above table.				
	Each line must use the following format and adhere to the following rules: Configuration Parameter= Valid Value				
	<ul> <li>Separate each configuration parameter and value with an equal sign.</li> </ul>				
	Set only one configuration parameter per line.				
	• Put the configuration parameter and value on the same line, and do not break the line.				
Line formats and Rules	<ul> <li>The [\$MODEL] can be added to the front of the configuration parameter to specify the value for specific phone groups.</li> <li>\$MODEL represents the phone model. The valid phone models are: VP59, T58, CP960, T57W, T54W, T53W, T53, T48U, T48S, T48G, T46U, T46S, T46G, T43U, T42U, T42S, T42G, T41P, T41S, T40P, T40G, T33P, T33G, T31P, T31G, T31, T30P, T30, T29G, T27G, T23P, T23G, T21P_E2, T19P_E2 and CP920. Multiple phone models are separated by commas. For example, [T46S, T23G]. It is only applicable to IP phones (except W53P/W60P/CP930W-Base) running firmware version 83 or later.</li> </ul>				
	<b>Note</b> : The phone updates model-specific configurations and those model-unspecified configurations. The phone model name T21P_E2 is applicable to T21P E2 and T21 E2 phones.				

# **Editing MAC-Oriented CFG File**

The MAC-Oriented CFG file is only effective for the specific phone. It uses the 12-digit MAC address of the IP phone as the file name. For example, if the MAC address of the IP phone is 00156574B150, the MAC-Oriented CFG file has to be named as 00156574b150.cfg (case-sensitive) respectively.

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

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

1#!version:1.0.0.1
##File header "#!version:1.0.0.1" can not be edited or deleted, and must be placed in the first line.##
##This template file is applicable to IP phones running firmware version 81 or later.##
##For more information on configuration parameters, refer to Description of Configuration Parameters in CFG Files.xslx##
## Accountl Basic Settings ##
account.1.enable =
account.1.label =
account.1.display_name =
account.1.auth_name =
account.1.user_name =
account.1.password =
account.1.outbound_proxy_enable =
account.1.outbound_host =
account.1.outbound_port =
account.1.dial_tone =
##It configures the transport type for account 1. 0-UDP,1-TCP,2-TLS,3-DNS-NAPTR
##The default value is 0.
account.1.sip_server.1.transport_type =
account.1.sip_server.2.transport_type =
## Failback ##
***************************************
account.1.naptr_build =
account.1.fallback.redundancy_type =
account.1.fallback.timeout =
account.1.sip_server.1.address =

The following table lists guidelines you need to know when editing the MAC-Oriented CFG file:

Item	Guidelines					
#	The line beginning with "#" is considered to be a comment.					
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.					
Filename	The filename matches the MAC address of your phone.					
	Each line must use the following format and adhere to the following rules: <i>Configuration Parameter= Valid Value</i> • Separate each configuration parameter and value with an equal					
	<ul> <li>Set only one configuration parameter per line.</li> <li>Put the configuration parameter and value on the same line, and</li> </ul>					
Line formats and Rules	<ul> <li>do not break the line.</li> <li>The [\$MODEL] can be added to the front of the configuration parameter to specify the value for specific phone groups.</li> <li>\$MODEL represents the phone model. The valid phone models are: VP59, T58, CP960, T57W, T54W, T53W, T53, T48U, T48S, T48G, T46U, T46S, T46G, T43U, T42U, T42S, T42G, T41P, T41S, T40P, T40G, T33P, T33G, T31P, T31G, T31, T30P, T30, T29G, T27G, T23P, T23G, T21P_E2, T19P_E2 and CP920. Multiple phone models are separated by commas. For example, [T46S, T23G]. It is only applicable to IP phones (except W53P/W60P/CP930W-Base) running firmware version 83 or</li> </ul>					

Item	Guidelines
	later.
	Note: The phone updates model-specific configurations and those
	model-unspecified configurations. The phone model name T21P_E2
	is applicable to T21P E2 and T21 E2 phones.

VP59/SIP-T58A/T57W/T54W/T48U/T48G/T48S/T46U/T46G/T46S/T29G IP phones support 16 accounts, SIP-T53W/T53/T43U/T42G/T42S IP phones support 12 accounts, W53P/W60P DECT IP phones support 8 assigned accounts, CP930W-Base phones support only one assigned account. SIP-T42U/T41P/T41S/T27G IP phones support 6 accounts, W52P/W56P IP DECT phones support 5 accounts; SIP-T31P/T31G/T31 IP phones support 4 accounts; SIP-T40P/T40G/T23P/T23G IP phones support 3 accounts, SIP-T31P/T31G/T31/T21(P) E2 IP phones support 2 accounts, CP960/CP920/CP860/SIP-T19(P) E2/T30P/T30 IP phones support only one account.

## **Creating a New CFG File**

If you want to create a new CFG file for your phone, follow these steps:

#### To create a new CFG file:

- 1. Create a CFG file for your phone. Ensure the file complies with the guidelines that are listed in Editing Common CFG File or Editing MAC-Oriented CFG File.
- Copy configuration parameters from the template configuration files and set valid values for them.

3. (Optional.) Specify different parameter values for specific phone groups.

For example:

[T46S] features.dnd\_mode = 1 [T48G, T23G] features.dnd\_mode = 0

4. Save the changes and close the CFG file.

You can also make a copy of the template configuration file, rename it and then edit it.

## Managing MAC-local CFG File

By default, MAC-local CFG file automatically stores non-static settings modified via web user interface or phone user interface. This file is stored locally on the IP phone, but a copy can also be uploaded to the provisioning server (or a specified URL configured by "static.auto\_provision.custom.sync.path"). This file enables the phone to keep the user's personalization settings, even after auto provisioning. As with the MAC-Oriented CFG files, MAC-local CFG files are only effective for the specific phone. They use the 12-digit MAC address of the IP phone as the file name. For example, if the MAC address of the IP phone is 00156574B150, MAC-local CFG file has to be named as 00156574b150-local.cfg (case-sensitive).

If your IP phone with the current firmware version cannot generate a <MAC>-local.cfg file, the IP phone will automatically generate a MAC-local CFG file after it is upgraded to the latest firmware.

For more information on how to keep user's personalization settings, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

We recommend you do not edit the MAC-local CFG file. If you really want to edit MAC-local CFG file, you can export and then edit it.

For more information on how to export CFG files, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

## **Encrypting Configuration Files**

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

# **Managing Resource Files**

Before provisioning, you may need to edit and customize your resource files.

You can edit the template resource files directly or create a new resource file as required. Open each resource file with a text editor such as Notepad++.

## **Customizing Resource Files**

The resource files are effective for all phones of the same model or the specific phone. If the resource file is to be used for all IP phones of the same model, the access URL of resource file had better be specified in the common CFG file. However, if you want to specify the desired phone to use the resource file, the access URL of the resource file should be specified in the MAC-Oriented CFG file.

Refer to Resource Files to get support resource files:

For more information on how to customize these template resource files and an explanation of the configuration parameters that related to these features, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

# **Configuring a Provisioning Server**

Yealink IP phones support using FTP, TFTP, HTTP, and HTTPS protocols to download boot files and configuration files. You can use one of these protocols for provisioning. The TFTP protocol is used by default. The following section provides instructions on how to configure a TFTP server.

We recommend that you use 3CDaemon or TFTPD32 as a TFTP server. 3CDaemo and TFTPD32 are free applications for Windows. You can download 3CDaemon online:

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

For more information on how to configure FTP and HTTP servers, refer to Configuring an FTP Server and Configuring an HTTP Server.

## **Preparing a Root Directory**

### To prepare a root directory:

- 1. Create a TFTP root directory on the local system (for example, D:\TFTP Directory).
- 2. Place the boot files, configuration files and resource files to this root directory.

Address [	):\TFTP Directory	🗙 🌛 Go		
🔌 network.cfg				
🛎 sip.cfg				
Features.cfg				
🖻 y00000000	)000.boot			
🔊 Customring.	wav			

3. (Optional.) Set security permissions for the TFTP directory folder.

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

Administrators (VANS	TD80\Admini	strators)	^
22 Evervone			
🖸 Hill, James (jahill@my	/servername.	.com]	
SYSTEM			~
<			>
	4	\ <u>d</u> d	<u>R</u> emove
Permissions for Everyone		Allow	Deny
Full Control			
Modify			
Read & Execute		~	
List Folder Contents		~	
Read		~	
Write		~	
Cossial Dormissions			
or special permissions or f	or advanced	settings,	Advanced

An example of configuration on the Windows platform is shown as below:

# **Configuring a TFTP Server**

If you have a 3CDaemon application installed on your local system, use it directly. Otherwise, download and install it.

### To configure a TFTP server:

1. Double click **3CDaemon.exe** to start the application.

A configuration page is shown as below:

2 3CDaemon						
nie view Heip						
TFTP Server	Start Time	Peer	Bytes	Status		
Configure TFTP Server	Jul 12, 2016 14:11:08	local	0	Listening for TFTP requests on IP address: 10.2.5.193, Port 69		
TFTP Server is started. Click here to stop it.						
Logging to Tftpd.log. Click to stop.						
Not debugging. Click to start.						
Clear list.						
View Log/Debug files.						

2. Select Configure TFTP Server. Click the ... from your local system:

button to locate the TFTP root directory

r.					
I	3CDaemon				
I	<u>File View H</u> elp				
I	TFTP Server	Start Time	Peer	Bytes	Status
I		Jul 12, 2016 09:30:13	local	0	Listening for TFTP requests on IP address: 10.2.5.193, Port 69
I	Configure TFTP Server	3CDaemon Configurat	ion		
I		FTP Profit	les		Syslog Configuration
I	(STOP)	General Con	figura	tion	TFTP Configuration
	TFTP Server is started. Click here to stop it.	Create directory n	ames iz	n incomi	ng file re🗸
		Allow overwrite of	existi	ing file	s?
I	Logging to Irtpa.log. Click to stop.	Upload/Download	1	D:\TFTP	Directory\
I	X	Per-packet timeout	in sec	onds	5
I	Not debugging. Click to start.	Maximum retries			10
	Clear list.	Interframe transmi	sion		0
	View Log/Debug files.				

3. Click the **Confirm** button to finish configuring the TFTP server.

The server URL "tftp://IP/" (Here "IP" means the IP address of the provisioning server, for example, "tftp://10.2.5.193/") is where the IP phone downloads configuration files from.

# **Obtaining the Provisioning Server Address**

Yealink IP phones can obtain the provisioning server address in the following ways:

- Zero Touch
- Plug and Play (PnP) Server
- DHCP Options
- Phone Flash
- Configuring Wildcard of the Provisioning Server URL

The priority of obtaining the provisioning server address is as follows: Zero Touch>PnP Server>DHCP Options (for IPv4: IPv4 Custom option>option 66>option 43; for IPv6: IPv6 Custom option>option 59) >Phone Flash. The following sections detail the process of each way (take the SIP-T23G IP phone as an example).

## **Zero Touch**

Zero Touch allows you to configure the network parameters and provisioning server address via phone user interface during startup. This feature is helpful when there is a system failure on the IP phone. To use Zero Touch, make sure this feature is enabled. This feature is not applicable to W52P/W53P/W56P/W60P/CP930W-Base IP phones.

To configure zero touch via the web user interface:

- 1. Click on Settings->Auto Provision.
- 2. Select Enabled from the pull-down list of Zero Active.
- 3. Enter the desired waiting time in the Wait Time(1~100s) field.

Veglink							Log Out English(English) 🗸		
	Status	Account	Network	Dsskey	Features	Settings	Directory Security		
Preference	Auto	Provision					NOTE		
Time&Date	PN DH	P Active CP Active		● On ◎ Off ● On ◎ Off			Auto Provision The IP phone can interoperate		
Call Display	IΡν	4 Custom Option		128			with provisioning server using auto provisioning for deploying the IB phones		
Upgrade	IPv	4 DHCP Option Val	ue	yealink			When the IP phone triggers to		
Auto Provision	IΡv	IPv6 Custom Option				perform auto provisioning, it will request to download the			
Configuration	Ser	rver URL er Name					configuration files from the provisioning server. During the auto provisioning process, the		
Dial Plan	Pas	ssword		•••••			IP phone will download and update configuration files to the		
Voice	Att	tempt Expired Time	e(s)	5			phone flash.		
Ring	Cor	mmon AES Key		•••••			You can click here to get		
ning	MA	C-Oriented AES Ke	у	•••••			more guides.		
Tones	Zei	ro Active		Enabled	•				
Softkey Layout	Wa	ait Time(1~100s)							
TR069	Por	wer On		🖲 On 🔘 Off					
	Rep	peatedly		© On ● Off					

The default value is 5.

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

When Zero Touch is enabled, there will be a configuration wizard during startup:

Zero Touch_	
Update now? 4s	
Cancel Status	OK

Press the **OK** soft key.

The network parameters are configurable via phone user interface:



Press the Next soft key after finishing network settings.

Configure the provisioning server address, authentication user name (optional) and password (optional) in the **Auto Provision** screen.

An example of the screenshot is shown as below:



Press the **OK** soft key.

After the above configuration is completed, the IP phone will connect to the configured provisioning server and perform auto provisioning during startup.

## Plug and Play (PnP) Server

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

### To configure PnP via web user interface:

- 1. Click on Settings->Auto Provision.
- 2. Mark the On radio box in the PNP Active field.

Yealink			Log Out English(English) 🗸
	Status Account Ne	twork Dsskey Features	Settings Directory Security
Preference	Auto Provision		NOTE
Time&Date	PNP Active	On ○ Off	Auto Provision The IP phone can interoperate
Call Display	IPv4 Custom Option	128	with provsioning server using auto provisioning for deploying
Upgrade	IPv4 DHCP Option Value	yealink	the IP phones. When the IP phone triggers to
Auto Provision	IPv6 Custom Option		perform auto provisioning, it will request to download the
Configuration	User Name		contiguration files from the provisioning server. During the auto provisioning process, the

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

Any PnP server activated in the network responses with a **SIP NOTIFY** message, and an address of the provisioning server is contained in the message body.

🖾 PNP.pcap - Vireshark					💶 🖻 🔀
File Edit View Go Capture And	lyze Statistics Telephony T	ools Help			
雙壓酸酸酸 医丁酮 22 %	😂 📇   🔍 💠 🌳 🦓 7	2 I II II Q Q Q	🖂   🎆 🕅	8 %   🛱	
Filter:		<ul> <li>Eggression Cleag A</li> </ul>	pply		
Bo Time	Source	Destination	Protocol	Info	4
1 0.000000	10.2.9.106	224.0.1.75	SIP	Request: SUBSCRIBE sip:MAC0015652a3dla@intern.IPPhone.com	
2 0.663070	10.2.9.46	10.2.9.106	SIP	Status: 202 Accepted subscription	
4 0.671499	10.2.9.106	10.2.9.46	SIP	Status: 200 oK	
5 1.807473	10.2.9.106	10.2.1.199	SIP	Request: REGISTER sip:10.2.1.199	
6 1.810835	10.2.1.199	10.2.9.106	SIP	Status: 200 OK (1 bindings)	~
<pre>D Frame 3 (720 bytes on with a Ethernet II, Src: Xlammer B Internet Protocol, Src: 1 User Datagen Protocol, Src: 1 B sesion Initiation Protocol Research (Internet) Research (Internet) B Research (Internet) Research (Internet) B Via: Str. 2000 (Inter</pre>	<ul> <li>739 bytes captured)</li> <li>736 bytes captured)</li> <li>9.46 (10.2.9.46), or</li> <li>9.46 (10.2.9.46), or</li> <li>9.10 byte (10.552a)d1.4610.2.5</li> <li>9.46 (5060) branch-29hold</li> <li>9.100</li> <li>100</li> <l< td=""><th>18:f1), Dst: x1amenre T: 10.2.9.106 (10.2.4) Fort: dds (2059) 0059 SIP/2.0 0059 SIP/2.0 0059 D:tag-57000253 tag-57000253 tag-541054 0 OPTIONS, NOTIFY, REGI: kk-sync</th><td>ra:3d:1a (00: 106)</td><td>15:65:2a:3d:1a) BE, REFER, PUBLISH, UPOATE, MESSAGE</td><td></td></l<></ul>	18:f1), Dst: x1amenre T: 10.2.9.106 (10.2.4) Fort: dds (2059) 0059 SIP/2.0 0059 SIP/2.0 0059 D:tag-57000253 tag-57000253 tag-541054 0 OPTIONS, NOTIFY, REGI: kk-sync	ra:3d:1a (00: 106)	15:65:2a:3d:1a) BE, REFER, PUBLISH, UPOATE, MESSAGE	
🔿 Frame (frame), 729 bytes	paper         Statistic         Total         Note         Note         Note           Secret				

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

# **DHCP Options**

Yealink IP phones can obtain the provisioning server address by detecting DHCP options during startup.

If you are using the IPv4 network, the phone will automatically detect the option 66 and option 43 for obtaining the provisioning server address. DHCP option 66 is used to identify the TFTP server. DHCP option 43 is a vendor-specific option, which is used to transfer the vendor-specific information.

If you are using IPv6 network, the phone will automatically detect the option 59 for obtaining the provisioning server address. DHCP option 59 is used to specify a URL for the boot file to be downloaded by the client.

You can configure the phone to obtain the provisioning server address via a custom DHCP option. You can select to use IPv4 or IPv6 custom DHCP option according to your network environment. To obtain the provisioning server address via an IPv4 or IPv6 custom DHCP option, make sure the DHCP option is properly configured on the phone. The IPv4 or IPv6 custom DHCP option must be in accordance with the one defined in the DHCP server.

### To configure the DHCP option via the web user interface:

- 1. Click on Settings->Auto Provision.
- 2. Mark the On radio box in the DHCP Active field.
- 3. If you are using IPv4 network, enter the desired value in the IPv4 Custom Option field.
- 4. If you are using IPv6 network, enter the desired value in the IPv6 Custom Option field.

Yealink   1236	Status Account Netwo	ork Dsskey Features	Log Out Engleh(Engleh) • Settings Directory Security
Preference	Auto Provision PNP Active	◉ On ☉ Off	NOTE
Time&Date	DHCP Active	🖲 On 💿 Off	Auto Provision The IP phone can interoperate with provsioning server using
Call Display	IPv4 Custom Option	128	auto provisioning for deploying the IP phones.
Upgrade	IPv4 DHCP Option Value	yealink	When the IP phone triggers to
Auto Provision	IPv6 Custom Option		perform auto provisioning, it will request to download the
Auto Fronzion	Server URL		configuration files from the
Configuration	User Name		auto provisioning process, the
Dial Plan	Password	•••••	IP phone will download and update configuration files to the
Voice	Attempt Expired Time(s)	5	phone flash.
Ring	Common AES Key	•••••	You can click here to get

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

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

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

For more information on the DHCP options, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

The following figure shows the example messages of obtaining the TFTP server address from an IPv4 custom DHCP option:

DHCPserver-tftp.pcap [Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)]	
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help	
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 10.2.8.106 DHCP 342 DHCP Offer - Transaction ID 0x88e96872	
10 18.17/701 0.0.00 253.253.253 DRCP 390 DRCP Request - Transaction ID 0x86e906/2 17 18 178902 10 2 8 105 10 2 8 105 DRCP 342 DRCP ACK - Transaction ID 0x88e96872	
Enternet II, SrC: VMWAFe_09511Ta (00:0c:29:99:11Ta), DST: X1amenYe_38:28:08 (00:15:05:38:28:08)     Enternet 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 type: Ethernet	
Hope: 0	
Transaction ID: 0x88e96872	
Seconds elapsed: 100	
Bootp flags: 0x0000 (Unicast)	
Your (client) IP address: 0.2.8.106 (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: XiamenYe_38:28:08 (00:15:65:38:28:08)	
Server host name: midlo121-for3xon	
Boot file name not given	
Magic cookie: DHCP	
Option: (t=53,1=1) DHCP Message Type = DHCP ACK	
B Option: (L=1, 1=4) Subject mask = 203.203.203.00	
B Option: (t=59,1=4) Rebinding Time Value = 5 hours, 15 minutes	
⊕ Option: (t=58,1=4) Renewal Time value = 3 hours	
Option: (t=51,1=4) IP Address Lease Time = 6 hours	
option: (128) pocsts full security server iP [T000]	
Length: 18	
value: 746674703a2f2f31302e322e382e3130352f	
B Option: (t=54, l=4) DHCP Server Identifier = 10.2.8.105	

Right-click the root node of the custom option (for example, option 128) shown on the above figure, and select **Copy->Bytes->Printable Text Only**. Paste the copied text in your favorite text editor to check the address, for example, tftp://192.168.1.100/.

# **Phone Flash**

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

To configure the IP phone flash via web user interface:

1. Click on Settings->Auto Provision.

Enter the URL, user name and password of the provisioning server in the Server URL,
 User Name and Password field respectively (the user name and password are optional).

Yealink   1236	Status Account Network	Dsskey Features Setting	Log Out English(English) • Directory Security
Dreference	Auto Provision		NOTE
Treference	PNP Active	On Off	Auto Devicing
Time&Date	DHCP Active	◉ On ◎ Off	The IP phone can interoperate
Call Display	IPv4 Custom Option	128	auto provisioning for deploying
Upgrade	IPv4 DHCP Option Value	yealink	the ip phones.
Auto Drovision	IPv6 Custom Option		perform auto provisioning, it will
Auto Provision	Server URL	tftp://10.2.5.193/	configuration files from the
Configuration	User Name	Network Dsskey Features Settings Directory Security © On © Off © On © Off © On © Off © On © Off On © Off On © Off On © Off Directory Security NOTE Auto Provisioning for deploying the IP phone can interoperate with provisioning for deploying the IP phones. When the IP phone triggers to perform auto provisioning process, the IP phone fungers to the provisioning process, the IP phone funger sto the phone fungers to the phone fungers to the provisioning process, the IP phone fungers to the provisioning process, the IP phone fungers to the provisioning process, the IP phone fungers to the phone fungers to the phone fungers to the phone function the provisioning process, the IP phone function the phone function the provision the phone function the provision the phone function the phone funct	
Dial Plan	Password	•••••	IP phone will download and update configuration files to the
Voice	Attempt Expired Time(s)	5	phone flash.
	Common AES Key	•••••	
Ring	MAC-Oriented AES Key	•••••	more guides.
Tones	Zero Active	Enabled -	

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

After the above configuration is completed, the IP phone will connect to the configured provisioning server and perform auto provisioning by one of the following methods: Power On, Repeatedly, Weekly, Flexible Auto Provision, Auto Provision Now, SIP NOTIFY Message and Multi-mode Mixed. For more information on these methods, refer to Triggering the IP Phone to Perform Auto Provisioning.

### **Configuring Wildcard of the Provisioning Server URL**

Normally, many phone models may be deployed in your environment. To deploy many phone models using a unified provisioning server, it is convenient for the administrator to configure a unified provisioning server URL for different phone models. On the provisioning server, many directories need to be configured for different phone models, each with a unique directory name. Yealink IP phones support the following wildcards in the provisioning server URL:

- **\$PN**: it is used to identify the directory name of the provisioning server directory where the corresponding boot files and configuration files are located.
- \$MAC: it is used to identify the MAC address of the IP phone.

The parameter "static.auto\_provision.url\_wildcard.pn" is used to configure the directory name where the boot files and configuration files located. For more information on the parameter, refer to the latest IP Phones Description of Configuration Parameters in CFG Files or Administrator Guide for your phone on Yealink Technical Support.

When the IP phone obtains a provisioning server URL containing the wildcard \$PN, it automatically replaces the character \$PN with the value of the parameter "static.auto\_provision.url\_wildcard.pn" configured on the IP phone. When the IP phone is triggered to perform auto provisioning, it will request to download the boot files and configuration files from the identified directory on the provisioning server.

The value of the parameter "static.auto\_provision.url\_wildcard.pn" must be configured in accordance with the directory name of the provisioning server directory where the boot files and configuration files of the IP phones are located.

The following example assists in explaining the wildcard feature:

You want to deploy SIP-T42G and SIP-T46G IP phones simultaneously in your environment. IP phones are configured to obtain the provisioning server URL via DHCP option 66. The following details how to deploy the SIP-T42G and SIP-T46G IP phones using the wildcard feature.

- 1. Create two directories on the root directory of the provisioning server.
- 2. Configure the directory names of these two directories to be "T42G" and "T46G".
- 3. Place the associated boot files and configuration files to the directory created above.
- 4. Configure the value of DHCP option 66 on the DHCP server as tftp://192.168.1.100/\$PN.
- 5. Configure the value of the parameter "static.auto\_provision.url\_wildcard.pn".

The default value of the parameter "static.auto\_provision.url\_wildcard.pn" is "T42G" for the SIP-T42G IP phones and "T46G" for the SIP-T46G IP phones. If the default value is different from the directory name, you need to configure the value of this parameter to be the directory name on the IP phones in advance.

During startup, IP phones obtain the provisioning server URL "tftp://192.168.1.100/\$PN" via DHCP option 66 and then replace the character "\$PN" in the URL with "T42G" for the SIP-T42G IP phones and "T46G" for the SIP-T46G IP phones. When performing auto provisioning, the SIP-T42G IP phones, and the SIP-T46G IP phones first request to download the MAC-Oriented boot files and configuration files referenced in MAC-Oriented boot files from the provisioning server address "tftp://192.168.1.100/T42G" and "tftp://192.168.1.100/T46G" respectively. If no matched MAC-Oriented boot files are found on the server, the SIP-T42G IP phones and the SIP-T46G IP phones request to download the common boot files and configuration files referenced in the server, the SIP-T42G IP phones and the SIP-T46G IP phones request to download the common boot files and configuration files referenced in common boot files from the provisioning server address "tftp://192.168.1.100/T42G" and "tftp://192.168.1.100/T46G" respectively.

If the URL is configured as "tftp://192.168.1.100/\$PN/\$MAC.boot" on the DHCP server, the SIP-T42G IP phones, and the SIP-T46G IP phones will replace the characters "\$PN" with "T42G" and "T46G" respectively, and replace the characters "\$MAC" with their MAC addresses. For example, the MAC address of one SIP-T42G IP phone is 00156543EC97. When performing auto provisioning, the IP phone will only request to download the 00156543ec97.boot file and configuration files referenced in the 00156543ec97.boot file from the provisioning server address "tftp://192.168.1.100/T42G".

For more information on boot files, refer to Managing Boot Files.

# Triggering the IP Phone to Perform Auto Provisioning

This chapter introduces the following methods to trigger the IP phone to perform auto provisioning:

- Power On
- Repeatedly
- Weekly
- Flexible Auto Provision
- Auto Provision Now
- Multi-mode Mixed
- SIP NOTIFY Message
- Auto Provisioning via Activation Code

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

### **Power On**

The IP phone performs the auto provisioning when the IP phone is powered on.

To activate the power on mode via a web user interface:

1. Click on Settings->Auto Provision.

2. Mark the On radio box in the Power On field.

					Log Ou	it
Yealink					English(English)	•
1250	Status Account I	Network Dsskey	Features	Settings	Directory Security	
Preference	Auto Provision				NOTE	
Time&Date	PNP Active DHCP Active				Auto Provision The IP phone can interoperate	
Call Display	IPv4 Custom Option	128			with provsioning server using auto provisioning for deploying the IP phones	
Upgrade	IPv4 DHCP Option Value	yealink			When the IP phone triggers to	
Auto Provision	IPv6 Custom Option				perform auto provisioning, it will request to download the	1
Configuration	User Name				provisioning server. During the auto provisioning process, the	
Dial Plan	Password	•••••			IP phone will download and update configuration files to the	
Voice	Attempt Expired Time(s)	5			phone flash.	
Ring	Common AES Key	*******			You can click here to get	
Tones	MAC-Oriented AES Key	••••••	-		more guides.	
Softkey Layout	Wait Time(1~100s)	5				
TP060	Power On	🖲 On 💿 Off	1			
11009	Repeatedly	🔘 On 🔘 Off	-			

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

# Repeatedly

The IP phone performs the auto provisioning at regular intervals. You can configure the interval for the repeatedly mode. The default interval is 1440 minutes.

To activate the repeatedly mode via web user interface:

- 1. Click on Settings->Auto Provision.
- 2. Mark the **On** radio box in the **Repeatedly** field.

/ealink	L English(English)							Log Out ish(English) 🗸	
	Status	Account	Network	Dsskey	Features	Settings	Directory	Security	
Preference	Auto	Provision					NOTE		
Time%Date	PNP Active		🖲 On 🔘 Off			Auto Provisio	n		
Timeocoate	DH	ICP Active		🖲 On 🔘 Off			The IP phone with provsionin	can interoperate g server using	
Call Display	IP	v4 Custom Option		128			auto provisionir the IP phones.	ng for deploying	
Upgrade	IΡ	v4 DHCP Option Val	lue	yealink			phone triggers to		
Auto Provision	IΡ	v6 Custom Option					perform auto p	rovisioning, it will	
	Se	rver URL		tftp://10.2.5.193/	/		configuration files from the provisioning server. During the auto provisioning process, the		
Configuration	Us	er Name							
Dial Plan	Pa	ssword		•••••		IP phone will download and update configuration files to the			
Voice	At	tempt Expired Time	e(s)	5			phone flash.		
Ping	Co	mmon AES Key		•••••			You can cl	ick here to get	
King	MA	AC-Oriented AES Ke	ŀγ	•••••			more guides.	,	
Tones	Ze	ro Active		Enabled	•				
Softkey Layout	W	ait Time(1~100s)		5					
TR069	Po	wer On		🖲 On 🔘 Off					
Voice Monitoring	Re	peatedly		🖲 On 🔘 Off					
voice monitoring	Int	terval(Minutes)		1440					
SIP	W	eekly		🛇 On 💿 Off					

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

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

### Weekly

The IP phone performs auto provisioning at a random time every week/month/quarter. You can configure what time of the day and which day of the week to trigger the IP phone to perform auto provisioning. You can also configure a regular week interval to trigger the IP phone to perform auto provisioning. You can specify the delay time to perform auto provisioning when the IP phone is inactive at regular week. For example, you can configure the IP phone to check and update new configuration only when the IP phone has been inactivated for 10 minutes between 2 to 3 o'clock in the morning every Monday at a 4-week interval.

If you configure two or more days in a week, the auto provisioning only occurs at a random day.

To activate the weekly mode via the web user interface:

- 1. Click on Settings->Auto Provision.
- 2. Mark the On radio box in the Weekly field.
- 3. Enter the desired upgrade interval in the Weekly Upgrade Interval(0~12week) field.
- 4. Enter the desired value in the Inactivity Time Expire(0~120min) field.
- 5. Enter the desired time in the **Time** field.

			Log Out
Veglink			English(English) 👻
	Status Account Network	Dsskey Features	Settings Directory Security
Des (	Auto Provision		NOTE
Preference	PNP Active	On Off	Auto Provision
Time&Date	DHCP Active	◉ On ◎ Off	The IP phone can interoperate
Call Display	IPv4 Custom Option	128	auto provisioning server using auto provisioning for deploying the IP phases
Ungrade	IPv4 DHCP Option Value	yealink	ule reprotes.
opgrude	IPv6 Custom Option		When the IP phone triggers to perform auto provisioning, it will
Auto Provision	Server URL	tftp://10.2.5.193/	request to download the configuration files from the
Configuration	User Name		provisioning server. During the auto provisioning process, the IP
Dial Plan	Password	•••••	phone will download and update configuration files to the phone
Voico	Attempt Expired Time(s)	5	flash.
VOICE	Common AES Key	•••••	Vou can dick here to get
Ring	MAC-Oriented AES Key	•••••	more guides.
Tones	Zero Active	Enabled 👻	
Softkey Layout	Wait Time(1~100s)	5	
	Power On	◉ On ◎ Off	
TR069	Repeatedly	On Off	
Voice Monitoring	Interval(Minutes)	1440	
SIP	Weekly	● On ◎ Off	
Power Saving	Weekly Upgrade Interval(0~12week)	4	
roner oarnig	Inactivity Time Expire(0~120min)	10	
	Time	02 : 00 03 : 00	
		Sunday	
		Monday	
	Day of Week	U Tuesday	
	buy of treek	Thursday	
		Friday	
		Saturday	

6. Check one or more checkboxes in the Day of Week field.

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

## **Flexible Auto Provision**

The IP phone performs auto provisioning at a random time on a random day within a specific period of time. The random day is calculated on the basis of the phone's MAC address. You can specify an interval and configure what time of the day to trigger the IP phone to perform auto provisioning.

For example, you can configure the IP phone to check and update new configuration between 1 and 6 o'clock in the morning at a 30-day interval. The IP phone will perform auto provisioning at a random time (for example, 03:47) on a random day (for example, 18) based on the phone's MAC address.

Note that the update time will be recalculated if auto provisioning occurs (for example, Auto Provision Now) during this specific period of time.

To activate the flexible auto provision mode via the web user interface:

- 1. Click on Settings->Auto Provision.
- 2. Mark the On radio box in the Flexible Auto Provision field.
- 3. Enter the desired value in the Flexible Interval Days field.

	Status	Account	Network	Dsskey	Features	Settings	Directory	Security
Preference	Auto	o Provision					NOTE	
	P	NP Active		🖲 On 🔘 Off			Auto Provisio	ю
Time&Date	D	HCP Active		🖲 On 🗇 Off			The IP phone with provisionin	can interoperati g server using
Call Display	P	Pv4 Custom Option		128			auto provisioni the IP phones	ng for deploying
Upgrade	B	Pv4 DHCP Option Val	ue	yealnk			When the ID r	hone trippers to
Auto Provésion	J.	Pv6 Custom Option					perform auto p	rovisioning, it w
AULO PTOVISION	5	erver URL					configuration f	les from the
Configuration	U	iser Name					provisioning se auto provisioni	rver. During the ng process, the
Dial Plan	P	assword					IP phone will d update configu	ownload and iration files to th
Voice	A	ttempt Expired Time	(s)	5			phone flash.	
	c	ommon AES Key						
Ring	N	AC-Oriented AES Ke	y				more guides.	ick nere to get
Tones	z	ero Active		Disabled				
Softkey Layout	v	Valt Time(1~100s)		5				
	p	ower On		🤋 On 💿 Off				
11009	R	epeatedly		🗢 On 👻 Off				
Voice Monitoring	1	nterval(Minutes)		1440				
51P	v	Veekly		O on 💌 Off				
Dower Savino	v	Veekly Upgrade Inter	val(0~12week)	0				
Conce Corring	1	nactivity Time Expire(	(0~120min)	0				
	T	ime		00 : 00 - 00	: 00			
	D	ay of Week		Sunday Sunday Monday Tuesday Wednesday				
				Thursday Friday Saturday	_			
	F	lexible Auto Provision	6	🖲 On 💿 Off				
	F	lexible Interval Days		30				
	F	lexible Time	_	02 : 00 - 06	: 00			

4. Enter the desired start time and end time in the Flexible Time field.

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

# **Auto Provision Now**

You can use auto provision now mode to manually trigger the IP phone to perform auto provisioning immediately.

To use the auto provision now mode via web user interface:

1. Click on Settings->Auto Provision.

	Status Account Networ	k Dsskey Features	Settings Directory Security
	Auto Provision		NOTE
Preference	PNP Active	🖲 On 🔘 Off	
Time&Date	DHCP Active	On      Off	Auto Provision The IP phone can interoperat
Call Display	IPv4 Custom Option	128	with provisioning server using auto provisioning for deploying
Ungrade	IPv4 DHCP Option Value	yealnk	the IP phones.
ophrane	IPv6 Custom Option		When the IP phone triggers t perform auto provisioning, it w
Auto Provision	Server URL		request to download the configuration files from the
Configuration	User Name		provisioning server. During the auto provisioning process, the
Dial Plan	Password		IP phone will download and update configuration files to the
Volce	Attempt Expired Time(s)	5	phone flash.
voice	Common AES Key		
Ring	MAC-Oriented AES Key		You can click here to get more guides.
Tones	Zero Active	Disabled +	
Softkey Layout	Wait Time(1~100s)	5	
10050	Power On	🖲 On 💿 Off	
TRUTP	Repeatedly	On Off	
Voice Monitoring	Interval(Minutes)	1440	
SIP	Weekly	🔘 On 😐 Off	
Power Saving	Weekly Upgrade Interval(0~12week	0	
	Inactivity Time Expire(0~120min)	0	
	Time	00 : 00 - 00 : 00	
	Day of Week	<ul> <li>✓ Sunday</li> <li>✓ Monday</li> <li>✓ Tuesday</li> <li>✓ Wednesday</li> <li>✓ Thursday</li> <li>✓ Friday</li> </ul>	
	Flexible Auto Provision	O on I Off	
	Flexible Interval Days	30	
	Flexible Time	02 : 00 - :	
		Auto Provision Now	

2. Click Auto Provision Now.

The IP phone will perform auto provisioning immediately.

### **Multi-mode Mixed**

You can activate more than one method for auto provisioning. For example, you can activate the "Power On" and "Repeatedly" modes simultaneously. The IP phone will perform auto provisioning when it is powered on and at a specified interval.

## **SIP NOTIFY Message**

The IP phone will perform auto provisioning when receiving a SIP NOTIFY message which contains the header "Event: check-sync". Whether the IP phone reboots or not depends on the value of the parameter "sip.notify\_reboot\_enable". If the value is set to 1, or the value is set to 0 and the header of the SIP NOTIFY message contains an additional string "reboot=true", the IP phone will reboot immediately. For more information on the parameter "sip.notify\_reboot\_enable", refer to the latest IP Phones Description of Configuration

Parameters in CFG Files or Administrator Guide for your phone on Yealink Technical Support. This method requires server support.

The following figure shows the message flow:



## Auto Provisioning via Activation Code

In addition to the updating modes introduced above, users can trigger IP phones to perform auto provisioning by dialing an activation code. To use this method, the activation code and the provisioning server URL need to be pre-configured on the IP phones. This method works only if there is no registered account on the IP phone. It is usually used for IP phones distributed by retail sales. It has the advantage that the IP phones do not need to be handled (for example, registering account) before sending them to end-users.



The following lists the processes for triggering auto provisioning via activation code:

- 1. Create multiple directories (for example, T23G\_1 and T23G\_2) on the provisioning server.
- 2. Store boot files and configuration files to each directory on the provisioning server.
- 3. Configure a user name and password for each directory on the provisioning server.

The user name and password provides a means of conveniently partitioning the boot files and configuration files for different IP phones. To access the specified directory, you need to provide the correct user name and password configured for the directory.

4. Configure unique activation codes and the provisioning server URLs on IP phones.

The activation code can be numeric characters, special characters "#", "\*" or a combination of them within 32 characters.

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

static.autoprovision.1.code = \*123

static.autoprovision.1.url = http://192.168.1.30/T23G\_1/

static.autoprovision.2.code = \*456

static.autoprovision.2.url = http://192.168.1.30/T23G\_2/

- 5. Send the specified activation code, associated user name and password to each end-user.
- **6.** The user can set up the IP phone, and then input the activation code (for example, \*123) after the phone startup.

The LCD screen will prompt the following dialog box:



7. Press the **OK** soft key to trigger the IP phone to perform auto provisioning.

The LCD screen will prompt the following input box:

A	utoP A	Authority-	
User	Name:		
Cancel	2aB	Delete	ОK

8. Enter the user name and password in the User Name and Password field respectively.

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

The IP phone downloads the specified configuration files in sequence in boot files from the provisioning server to complete phone configurations. For more information on boot files and configuration files, refer to Managing Boot Files and Managing Configuration Files.

The entered user name and password will be saved to the IP phone for next auto provisioning.

The LCD screen will not prompt for user name and password if the provisioning server does not require authentication, or the user name and password are already saved on the IP phone.

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

#(Optional.) Configure the code name for triggering auto provisioning.
static.autoprovision.X.name
#Configure the activation code.
static.autoprovision.X.code
#Configure the URL of the provisioning server.
static.autoprovision.X.url
#Configure the username and password for downloading boot files and configuration files. If
configured, the LCD screen will not prompt for user name and password.
static.autoprovision.X.user
static.autoprovision.X.password

## Auto Provisioning via PIN Code

After the phone is powered on and connected to the network, users can trigger it to perform an auto provisioning by entering the PIN code. The phone will download the corresponding PIN CFG file according to the PIN code.

The following lists the processes for triggering auto provisioning via PIN code:

1. Prepare the common CFG file and PIN CFG files in your local system.

### Example:

Common CFG file: y00000000108.cfg

PIN CFG files: A31.cfg, A32.cfg, and A33.cfg.



- 2. Place the common CFG file and PIN CFG files on the provisioning server.
- Set the valid value for the following configuration parameter in the common CFG file. static.custom\_mac\_cfg.url = http://<serverlPaddress>/\$pin.cfg

### Example:

static.custom\_mac\_cfg.url = http://10.2.11.101/\$pin.cfg

- 4. Specify the provisioning server URL (for example, http://10.2.11.101/) for the DHCP option or PnP server.
- 5. After the phone is powered on and connected to the network, users enter the corresponding PIN code (for example, A31).

	Please ente	er PIN Code	
1. PIN Code:		•••	
Cancel	123	Delete	ОК

The IP phone downloads the specified configuration file (for example, A31.cfg) from the provisioning server to complete phone configurations.

# **Downloading and Verifying Configurations**

### **Downloading Boot, Configuration and Resource Files**

After obtaining the provisioning server address in one of the ways introduced above, the phone will request to download the boot files and configuration files from the provisioning server when it is triggered to perform auto provisioning.

The IP phone will try to download the MAC-Oriented boot file firstly and then download the configuration files referenced in the MAC-Oriented boot file from the provisioning server during the auto provisioning. If no MAC-Oriented boot file is found, the IP phone will try to download the common boot file and then download the configuration files referenced in the common boot file. If no common boot file is found, the IP phone will try to download the Common CFG file firstly, and then try to download the MAC-Oriented CFG file from the provisioning server – that is, the old mechanism for auto provisioning.

For more information about auto provisioning, refer to Auto Provisioning Process.

If the access URLs of the resource files have been specified in the configuration files, the phone will try to download the resource files.

### **Resolving and Updating Configurations**

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

The IP phone calculates the MD5 values of the downloaded files before updating them. If the MD5 values of the Common and MAC-Oriented configuration files are the same as those of the last downloaded configuration files, this means these two configuration files on the provisioning server are not changed. The IP phone will complete the auto provisioning without a repeated update. This is used to avoid unnecessary restart and the impact of phone use. On the contrary, the IP phone will update configurations.

The latest values to be applied to the IP phone are the values that take effect.

The phone only reboots when there is at least a specific configuration requiring a reboot after auto provisioning. If you want to force the IP phone to perform a reboot after auto provisioning, you can configure "static.auto\_provision.reboot\_force.enable = 1" in the configuration file. For more information on the specific configurations which require a reboot during auto provisioning and the parameter "static.auto\_provision.reboot\_force.enable", refer to the latest IP Phones Description of Configuration Parameters in CFG Files for your phone on Yealink Technical Support.

If configuration files have been AES encrypted, the IP phone will use the Common AES key to decrypt the Common CFG file and the MAC-Oriented AES key to decrypt the <MAC>.cfg file after downloading the configuration files. For more information on how the IP phone decrypts configuration files, refer to *Yealink Configuration Encryption Tool User Guide*.

## **Using MAC-local CFG File**

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

You can configure whether the IP phone uploads the <MAC>-local.cfg file to the provisioning server (or a specified URL configured by "static.auto\_provision.custom.sync.path") once the file changes for backing up this file, and downloads the <MAC>-local.cfg file from the provisioning server (or a specified URL configured by "static.auto\_provision.custom.sync.path") during auto provisioning to override the one stored on the phone. This process is controlled by the value of the parameter "static.auto\_provision.custom.sync".

### Updating configurations in the <MAC>-local.cfg file

You can configure whether the IP phone updates configurations in the <MAC>-local.cfg file during auto provisioning. This process is controlled by the value of the parameter "static.auto\_provision.custom.protect". If the IP phone is configured to keep the user's personalized settings (by setting the value of the parameter "static.auto\_provision.custom.protect" to 1), it will update configurations in the <MAC>-local.cfg file. If the value of the parameter "overwrite\_mode" is set to 1 in the boot file, the phone updates configurations in the <MAC>-local.cfg file downloaded from the server; if the value of the parameter "overwrite\_mode" is set to 0, the phone updates configurations in the <MAC>-local.cfg file stored on the phone.

The IP phone updates configuration files during auto provisioning in sequence: CFG files referenced in the boot file>MAC-local CFG file (if no boot file is found, Common CFG file>MAC-Oriented CFG file>MAC-local CFG file). The configurations in the <MAC>-local.cfg file take precedence over the ones in other downloaded configuration files. As a result, the personalized settings of the phone configured via the phone or web user interface can be kept after auto provisioning.

Note that if the personalized settings are static settings, they cannot be kept after auto provisioning because the static settings will never be saved in the <MAC>-local.cfg file.

For more information, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

## **Verifying Configurations**

After auto provisioning, you can then verify the update via phone user interface or web user interface of the phone. For more information, refer to *Yealink phone-specific user guide*.

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

**Example1:** Yealink SIP-T23G IP phone downloads the boot file and configuration files from the TFTP server.

<u>Elle Edit View Go Captu</u>	re <u>A</u> nalyze <u>S</u> tatistics	Telephony Tools Intern	ials <u>H</u> elp	
		🔺 📣 🛣 🕂 🗐 🗉		
Filter: tftp		💌 Exp	pression Clear	Apply Save
No. Time	Source	Destination	Protocol	Length Info
1111 1. JUUJJJUUU		10.1.20.75	11.11	to citor couc, couc. Access violation, ressaye, could not open requested the for reading
2/// 12.389499000	10.2.20.73	10.2.5.193	TETP	81 Read Request, File: 001565/4b16e.boot, Transfer type: octet, blks1ze\000=1432\000
2778 12.389595000	10.2.20.73	10.2.5.193	TETP	81 Read Request, File: 00156574b16e.boot, Transfer type: octet, blksize\000=1432\000
2786 12.416697000	10.2.5.193	10.2.20.73	TETP	88 Error Code, Code: Access violation, Message: Could not open requested file for reading
2788 12.417077000	10.2.5.193	10.2.20.73	TETP	88 Error Code, Code: Access violation, Message: Could not open requested file for reading
3719 17.440553000	10.2.20.73	10.2.5.193	TETP	82 Read Request, File: y00000000000.boot, Transfer type: octet, blksize\000=1432\000
3720 17.440666000	10.2.20.73	10.2.5.193	TETP	82 Read Request, File: y00000000000.boot, Transfer type: octet, blksize\000=1432\000
3749 17.462578000	10.2.5.193	10.2.20.73	TETP	57 Option Acknowledgement, b1ksize\000=1432\000
3751 17.462889000	10.2.5.193	10.2.20.73	TETP	60 Option Acknowledgement, blksize\000=1432\000
3753 17.464898000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 0
3754 17.464989000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 0
3755 17.465642000	10.2.5.193	10.2.20.73	TETP	428 Data Packet, Block: 1 (last)
3760 17.466974000	10.2.5.193	10.2.20.73	TETP	428 Data Packet, Block: 1 (last)
3766 17.469270000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 1
3767 17.469359000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 1
3775 17.483306000	10.2.20.73	10.2.5.193	TETP	71 Read Request, File: sip.cfg, Transfer type: octet, blksize\000=1432\000
3776 17.483401000	10.2.20.73	10.2.5.193	TETP	71 Read Request, File: sip.cfg, Transfer type: octet, blksize\000=1432\000
3779 17.506728000	10.2.5.193	10.2.20.73	TETP	57 Option Acknowledgement, blksize\000=1432\000
3781 17.506988000	10.2.5.193	10.2.20.73	TETP	60 Option Acknowledgement, blksize\000=1432\000
3786 17.511914000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 0
3787 17.512005000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 0
3788 17.512439000	10.2.5.193	10.2.20.73	TETP	625 Data Packet, Block: 1
3790 17.513683000	10.2.5.193	10.2.20.73	TETP	625 Data Packet, Block: 1
3794 17.515113000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 1
3795 17.515201000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 1
3804 17.538122000	10.2.20.73	10.2.5.193	TETP	76 Read Request, File: features.cfg, Transfer type: octet, blksize\000=1432\000
3805 17.538224000	10.2.20.73	10.2.5.193	TETP	76 Read Request, File: features.cfg, Transfer type: octet, blksize\000=1432\000
3810 17.569170000	10.2.5.193	10.2.20.73	TETP	88 Error Code, Code: Access violation, Message: Could not open requested file for reading
3811 17.569472000	10.2.5.193	10.2.20.73	TETP	88 Error Code, Code: Access violation, Message: Could not open requested file for reading

**Example 2:** Yealink SIP-T23G IP phone downloads the boot file and configuration files from the FTP server.

			-		
Filter:	ttp		<ul> <li>Expre</li> </ul>	ssion Clear	Apply Save
No.	Time	Source	Destination	Protocol	Length Info
317	3 28.950484000	10.2.5.193	10.2.20.73	FTP	75 [TCP_Retransmission]_Response: 213_382
317	5 28.952342000	10.2.20.73	10.2.5.193	FTP	91 Request: RETR y0000000000.boot
317	6 28.952453000	10.2.20.73	10.2.5.193	FTP	91 [TCP Retransmission] Request: RETR y000000000000.boot
317	9 28.958927000	10.2.5.193	10.2.20.73	FTP	102 Response: 125 Using existing data connection
318	0 28.959253000	10.2.5.193	10.2.20.73	FTP	102 [TCP Retransmission] Response: 125 Using existing data connection
319	0 28.963510000	10.2.5.193	10.2.20.73	FTP	122 Response: 226 Closing data connection; File transfer successful.
319	3 28.963862000	10.2.5.193	10.2.20.73	FTP	122 [TCP Retransmission] Response: 226 closing data connection; File transfer successful.
322	2 28.991053000	10.2.5.193	10.2.20.73	FTP	108 Response: 220 3Com 3CDaemon FTP Server Version 2.0
322	5 28.992201000	10.2.20.73	10.2.5.193	FTP	76 Request: USER 123
322	6 28.992302000	10.2.20.73	10.2.5.193	FTP	76 [TCP Retransmission] Request: USER 123
322	9 28.993908000	10.2.5.193	10.2.20.73	FTP	99 Response: 331 User name ok, need password
323	0 28.994220000	10.2.5.193	10.2.20.73	FTP	99 [TCP Retransmission] Response: 331 User name ok, need password
323	1 28.994857000	10.2.20.73	10.2.5.193	FTP	78 Request: PASS admin
323	2 28.994966000	10.2.20.73	10.2.5.193	FTP	78 [TCP Retransmission] Request: PASS admin
323	5 28.995764000	10.2.5.193	10.2.20.73	FTP	91 Response: 530 Login access denied
323	6 28.996077000	10.2.5.193	10.2.20.73	FTP	91 [TCP Retransmission] Response: 530 Login access denied
323	7 28.996878000	10.2.20.73	10.2.5.193	FTP	82 Request: USER anonymous
323	8 28.996979000	10.2.20.73	10.2.5.193	FTP	82 [TCP Retransmission] Request: USER anonymous
324	1 28.997855000	10.2.5.193	10.2.20.73	FTP	99 Response: 331 User name ok, need password
324	2 28.998113000	10.2.5.193	10.2.20.73	FTP	99 [TCP Retransmission] Response: 331 User name ok, need password
324	4 28.998745000	10.2.20.73	10.2.5.193	FTP	73 Request: PASS
324	8 29.000393000	10.2.5.193	10.2.20.73	FTP	101 Response: 230-The response ' is not valid.
324	9 29.000/15000	10.2.5.193	10.2.20.73	FTP	101 [TCP Retransmission] Response: 230-The response is not valid.
325	3 29.035465000	10.2.5.193	10.2.20.73	FTP	145 Response: 230-Next time, please use your email address as password.
325	5 29.03586/000	10.2.5.193	10.2.20.73	FTP	145 [TCP Retransmission] Response: 230-Next time, please use your email address as password.
325	8 29.03/118000	10.2.20.73	10.2.5.193	FIP	74 Request: TYPE 1
323	9 29.03/213000	10.2.20.73	10.2.5.193	FTP	74 [TCP Retransmission] Request: TYPE I
326	2 29.038460000	10.2.5.193	10.2.20.73	FTP	86 Response: 200 Type set to 1.
326	3 29.038/02000	10.2.3.193	10.2.20.73	FIP	To recent answers the second s
326	4 29.03935/000	10.2.20.73	10.2.5.193	FIP	72 REQUEST: PASY
320	8 29.040715000	10.2.5.193	10.2.20.73	FIP	114 kesponse: 227 Entering passive mode (10,7,5,195,211,172)
320	0.20.05411.6000	10.2.3.193	10.2.20.73	FIF	20 percentarismissioni kesponse. 227 Encering passive mode (10,2,5,193,211,172)
327	9 29.034116000	10.2.20.73	10.2.5.193	FIP	ov Request: SIZE STP.CT9
328	0 29.034212000	10.2.20.73	10.2.5.193	FIF	so LICP Retrainsmission Request: Size sip.crg

**Example 3:** Yealink SIP-T23G IP phone downloads boot file and configuration files from the HTTP server.

Ele	Edit	View Go	Capture	Analyze Statist	cs Telephony	Took ]	nternals <u>H</u> e	slp																
0	0			XRIQ	ia 🔹 📣 🏹	- <b>-</b> - I []					<b>5</b> . 34	1 12												
-												0.0												
Filt	er: htt	P					Expressio	n Clear	Apply	Save														
No.	т	ime		Source	Destin	ation	-	rotocol	Ler	oth Inf	0													
	33 1	1.962425	000	10.2.5.193	10.2	.20.73		TTP	1	882 PC	ST /se	rvlet?	p=sett	ings-a	utop&q=	write&r	now=true	HTTP/1	1.1 (	(applica	tion/>	k-www-f	orm-url	encoded)
Г	141 2	2.267524	000 :	10.2.20.73	10.2	.5.193		ITTP		234 G8	т /нтт	P%20Di	rector	y/00156	6574b16	ie.boot	HTTP/1.1	1						
	142 /	2.20//30	. 000	10.2.20.73	10.2	. 2. 1.83		4118		234 [1	CP Ret	ransmi	ssion]	GET /I	HTTP%20	wirecto	ory/00150	0574016	5e.boo	Ot HTTP/	1.1			
	149 2	2.270563	000 :	10.2.5.193	10.2	.20.73		ITTP		66 HT	TP/1.1	. 404 N	ot Fou	ind (te	ext/htm	1)								
	182 2	2.305531	000	10.2.20.73	10.2	.5.193		ITTP		235 GE	т /нтт	'P%20D1	rector	y/y000	0000000	00, boot	: HTTP/1.	.1						
	183 2	2.305723	000	10.2.20.73	10.2	.5.193		ITTP		235 [1	CP Ret	ransm	ssion	GET /I	нттр%20	Directo	bry/y0000	0000000	000.00	DOT HTTP	/1.1			
	203 4	2.321104	000 .	10.2.5.193	10.2	.20.73		1119		448 H	TP/1.1	200 0	K (ap	piicat	10n/oct	et-stre	eam)							
	2/9/	2.339293	100 .	10.2.3.193	10.2	5 102		11112	1	574 G	(	der me	. ]5 /44	. 01.25	4.71 HI	dl Cont	inustion	n or no	NT NT	ro traff	i.c.			
	298 2	2. 37 31 07	000	10.2.20.73	10.2	. 5. 193		TTP	1	514 C	intinua	tion o	r non-	HTTP TI	raffic	aj con	. muac roi		JII-111	ir ciaii	i c			
	304 2	2, 376198	000	10.2.20.73	10.2	. 5.193		TTP	1	133 C	ntinua	tion o	r non-	HTTP to	raffic									
	308 2	2. 377011	000	10.2.5.193	10.2	.20.73		ITTP		570 G	T /is/	aes. is	744.81	. 254.7	1 HTTP/	1.1								
	316 2	2.380821	000	10.2.5.193	10.2	.20.73		ITTP		581 GE	T /1s/	zeropa	dding-	min. js:	744.81.	254.71	HTTP/1.1	1						
	317 2	2.380973	000 :	10.2.5.193	10.2	.20.73		ITTP		571 GE	T /js/	jsbn.j	s?44.8	1.254.3	71 HTTP	9/1.1								
	318 2	2.381075	000 :	10.2.5.193	10.2	.20.73		ITTP		573 GE	T /js/	prng4.	js?44.	81.254.	.71 HTT	P/1.1								
	319 2	2.381175	000 :	10.2.5.193	10.2	.20.73	1	ITTP		569 G8	T /js/	rng.js	?44.81	.254.7	1 HTTP/	1.1								
	320 2	2.381293	000	10.2.5.193	10.2	.20.73		ITTP		569 G	T /15/	rsa. is	?44.81	. 254. 7:	1 HTTP/	1.1								
	398 2	2.408422	000	10.2.20.73	10.2	. 5.193		ITTP		224 GE	т /нт	P%20D1	rector	y/sip.	стд нтт	P/1.1			ro /1 1					
	233.	2.408039	000	10.2.20.73	10.2	20.72		TTO		224 U	CP REI	404 M	SSTORY	GET /I	ntre%20	UT ecco	ry/sip.o	cig mii	19/1.1					
Г	415 1	2 442520	000	10 2 20 73	10.2	5 1 9 3		TTP		229 68	T /HT	P%2001	rector	v/feat	unes of	A HTTP	1 1							
	465	2.442/25	100	10.2.20.73	10.2	. 5.193	_	ITTP		229 11	CP Ret	ransm	sston	GET /	HTTP://	Dinecto	rv/teati	ures.ct	ант	rp/1.1				
	470 2	2.455300	000	10.2.5.193	10.2	.20.73		ITTP		645 HT	TP/1.1	200 0	к (ар	plicat	ion/oct	et-stre	am)							
	480 2	2.458812	000	10.2.5.193	106.	120.188	.46	ITTP	1	.046 PC	ST /q?	h=A36B	528EBB	E894F1	7A1F12E	8A58FE	60&r=000	00&v=5.	2.5.1	L7503 HT	TP/1.1	L (app	licatio	n/x-ww-f
	491 2	2.508429	000	10.2.5.193	10.2	. 20.73		TTP		492 GE	T /not	e/1.En	glish_	note. xr	п] нттр	/1.1								
	492 2	2.509486	000 :	10.2.5.193	10.2	.20.73	1	ITTP		492 [1	CP Ret	ransmi	ssion]	GET /I	note/1.	English	_note.x	ml HTTP	P/1.1					
	507 2	2.558874	000	106.120.188.	6 10.2	.5.193	1	ITTP		296 HT	TP/1.1	200 0	K (te	xt/pla	in)									
	509 2	2.643723	000 :	10.2.5.193	36.1	10.147.	36 1	ITTP	1	.433 GE	T /web	search	/featu	ines/yui	n6.jsp?	pid=sog	jou-brse-	-d2a452	2edff(	)79ca6&w	=14408	§v=7400	åst=146	830942174

# **Troubleshooting**

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

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

### Why does the IP phone fail to download configuration files?

- Ensure that the auto provisioning feature is configured properly.
- Ensure that the provisioning server and network are reachable.
- Ensure that authentication credentials configured on the IP phone are correct.
- Ensure that configuration files exist on the provisioning server.
- Ensure that MAC-Oriented boot file and common boot file don't exist simultaneously on the provisioning server. If both exist, the IP phone only downloads MAC-Oriented boot file and the configuration files referenced in the MAC-Oriented boot file.

# Why does the IP phone fail to authenticate the provisioning server during auto provisioning?

- Ensure that the certificate for the provisioning server has been uploaded to the phone's trusted certificates list. If not, do one of the following:
  - Import the certificate for the provisioning server to the phone's trusted certificates list (at phone's web path Security->Trusted Certificates->Import Trusted Certificates).
  - Disable the IP phone to only trust the server certificates in the trusted certificates list (at phone's web path Security->Trusted Certificates->Only Accept Trusted Certificates).

#### Why does the provisioning server return HTTP 404?

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

#### Why does the IP phone display "Network unavailable"?

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

# Why is the permission denied when uploading files to the root directory of the FTP server?

- Ensure that the complete path to the root directory of the FTP server is authorized.
- Check security permissions on the root directory of the FTP server, if necessary, change the permissions.

### Why doesn't the IP phone obtain the IP address from the DHCP server?

- Ensure that settings are correct on the DHCP server.
- Ensure that the IP phone is configured to obtain the IP address from the DHCP server.

### Why doesn't the IP phone download the ring tone?

- Ensure that the file format of the ring tone is \*.wav.
- Ensure that the size of the ring tone file is not larger than that the IP phone supports.
- Ensure that the properties of the ring tone for the IP phone are correct.
- Ensure that the network is available and the root directory is right for downloading.
- Ensure that the ring tone file exists on the provisioning server.

### Why doesn't the IP phone update configurations?

- Ensure that the configuration files are different from the last ones.
- Ensure that the IP phone has downloaded the configuration files.
- Ensure that the parameters are correctly set in the configuration files.
- Ensure that the value of the parameter "static.auto\_provision.custom.protect" is set to 0. If it
  is set to 1, the provisioning priority is shown as follows: phone/web user interface >central
  provisioning >factory defaults. A setting you make using a lower-priority method does not
  apply to or override a duplicate setting made using a higher-priority method.

For more information, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

# Glossary

**MAC Address:** A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment.

**MD5:** The MD5 Message-Digest Algorithm is a widely used as a cryptographic hash function that produces a 128-bit (16-byte) hash value.

**DHCP:** Dynamic Host Configuration Protocol (DHCP) is a network configuration protocol for hosts on Internet Protocol (IP) networks. Computers that are connected to IP networks must be configured before they can communicate with other hosts.

**FTP:** File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet. It is often used to upload web pages and other documents from a private development machine to a public web-hosting server.

**HTTP:** The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

**HTTPS:** Hypertext Transfer Protocol Secure (HTTPS) is a combination of Hypertext Transfer Protocol (HTTP) with SSL/TLS protocol. It provides encrypted communication and secure identification of a network web server.

**TFTP:** Trivial File Transfer Protocol (TFTP) is a simple protocol to transfer files. It has been implemented on top of the User Datagram Protocol (UDP) using port number 69.

**AES:** Advanced Encryption Standard (AES) is a specification for the encryption of electronic data.

**URL:** A uniform resource locator or universal resource locator (URL) is a specific character string that constitutes a reference to an Internet resource.

**XML:** Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

# **Appendix**

## **Configuring an FTP Server**

Wftpd and FileZilla are free FTP application software for Windows. This section mainly provides instructions on how to configure an FTP server using wftpd for Windows. You can download wftpd online: http://www.wftpd.com/products/products.html or FileZilla online: https://filezilla-project.org.

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

### **Preparing a Root Directory**

### To prepare a root directory:

- 1. Create an FTP root directory on the local system (for example, D:\FTP Directory).
- 2. Place the boot files and configuration files to this root directory.
- 3. Set the security permissions for the FTP directory folder.

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

An example of configuration on the Windows platform is shown as below:

Administrators (VANS	TD80\Admini	strators)		^
🙀 Everyone				
🕵 Hill, James (jahill@my	servername	.com]		
5 SYSTEM				~
<			>	
	-	\ <u>d</u> d	<u>R</u> emove	•
Permissions for Everyone		Allow	Deny	
Full Control				^
Modify		<b>~</b>		
Read & Execute		~		
List Folder Contents		~		
Read		<b>v</b>		
Write				
Consist Dermissions				~
For special permissions or f click Advanced.	or advanced	settings,	Advance	d

# **Configuring an FTP Server**

### To configure a wftpd server:

- 1. Download the compressed file of the wftpd application to your local directory and extract it.
- 2. Double click the Wftpd.exe.

The dialogue box of how to register is shown as below:



3. Check the check box and click **OK** in the pop-up box.

The log file of the wftpd application is shown as below:

E:\desktop\1.FTP - WFTPD	_ 0 🔀
File Edit View Logging Messages Security Help	
<ul> <li>[#-001] 2015/3/20 17:39:16 Welcome to WFTPD - we are listening to all unused IP addresses.</li> <li>[#-001] 2015/3/20 17:39:16 The first address assigned to your system is 127.00.1</li> <li>[#-001] 2015/3/20 17:39:16 But you might be reached at a number of other addresses.</li> <li>[#-001] 2015/3/20 17:39:16 Check with your network administrators for the address that is reacha [#-001] 2015/3/20 17:39:16 WFTPD is listening on port 21, standard ftp</li> <li>[#-001] 2015/3/20 17:39:16 Program will be killed by WM_ENDSESSION message</li> <li>[#-001] 2015/3/20 17:39:16 Unregistered version - for instructions on registering.</li> <li>[#-001] 2015/3/20 17:39:16 select the "Registering" option from the "Help" menu.</li> </ul>	ble from the Intern
<	F
For Help, press F1 1 socket 0 users	NUM //

4. Click Security->Users/rights.

🕌 E:\desktop\1.FTP - WFTPD	- • •
File Edit View Logging Messages Security Help	
International         Control Science         Control Science         General           [# -001]         2015/3/20         17:39:16         The first a         General         General           [# -001]         2015/3/20         17:39:16         The first a         General         General           [# -001]         2015/3/20         17:39:16         But you n         Host/net         General           [# -001]         2015/3/20         17:39:16         KHTPD is Instrening on port 71;         Host/net           [# -001]         2015/3/20         17:39:16         WFTPD is Instrening on port 71;         Host/net           [# -001]         2015/3/20         17:39:16         WFTPD is Instrening on port 71;         Host/net           [# -001]         2015/3/20         17:39:16         Wregistered version - for instruction for the first of the select the "Registering" option for the first of the select the "Registering" option for the first of the select the "Registering" option for the first of the first of the first of the select	g to all unused IP addresses. ystem is 127.0.0.1 er of other addresses. prs for the address that is reachable from the Interni standard ftp NDSESSION message ctions on registering, rom the "Help" menu.
Add, delete, or change users, passwords and home directories	1 socket 0 users NUM

5. Click New User.

User / Rights Se	ecurity Dialog		×
User Name: User default	default	•	Done
New User	Delete Restrict to home	Change Pass directory and below	
Home			Browse
Help			Rights >>

6. Enter a user name (for example, test1) in the User Name field and then click OK.

User / Rigł	nts Security	/ Dialog			23
User Name User defau	New Use	default r	•	Done	
New Us	User Name	: test1		OK Cancel Help	
Home	elp				Rights >>

7. Enter the password of the user (for example, test1) created above in the **New Password** and **Verify Password** field respectively, and then click **OK**.

User / Rigl	nts Security	Dialog					8
User Name User test1	Change P	assword		•	Done		
New U:	New Passwo Verifu Passw	ord: ×***	:× :×		OK Cancel		
Home					Help		
He	elp					Rights	>>

8. Click Browse to locate the FTP root directory in your local system.

User / Rights S	Security Dialog		×
User Name: User test1	test1	•	Done
New User	Delete Restrict to home	Change Pass directory and below	
Home	E:\DESKTOP\CONF	FIGURATION FILE	Browse
Help			Rights>>

9. Click **Rights**>> and assign the desired permission for the user (for example, test1) created above.

10. Check the check boxes of Read, Create Files/Dirs, List Directories and

Overwrite/Delete to make sure the FTP user has the read and write permission.

User / Rights Secu	irity Dialog		
User Name: User test1	test1	•	Done
New User	Delete Restrict to hom	Change Pass he directory and below	
Home E:	DESKTOP\CO	INFIGURATION FILE	Browse
Help Rights for user test1			Rights<<
Directory: ×		■ Browse	Remove
Rights for dir	ectory *		
🔽 Read		🔽 Create Files/Dirs	
🔽 List Dire	ectories	🔽 Overwrite/Delete	•

11. Click Done to save the settings and finish the configurations.

The server URL "ftp://username:password@IP/" (Here "IP" means the IP address of the provisioning server, "username" and "password" are the authentication for FTP download. For example, "ftp://test1:123456@10.3.6.234/") is where the IP phone downloads boot files and configuration files from.

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

## **Configuring an HTTP Server**

This section provides instructions on how to configure an HTTP server using HFS tool. You can download the HFS software online: http://www.snapfiles.com/get/hfs.html.

### **Preparing a Root Directory**

### To prepare a root directory:

- 1. Create an HTTP root directory on the local system (for example, D:\HTTP Directory).
- 2. Place the boot files and configuration files to this root directory.
- 3. Set the security permissions for the HTTP directory folder.

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

> General Sharing Security Customize Group or user names: Administrators (VANSTD80\Administrators) CREATOR OWNER Everyone 🕵 Hill, James (jahill@myservername.com) SYSTEM > Add. <u>R</u>emove Permissions for Everyone Allow Deny Full Control Modify ~ Read & Execute ~ List Folder Contents ~ Read ~ Write ~ ~ Consist De For special permissions or for advanced settings, click Advanced. Advanced OK Cancel Apply

An example of configuration on the Windows platform is shown as below:

## **Configuring an HTTP Server**

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

### To configure an HTTP server:

1. Download the application file to your local directory, double click the **hfs.exe**.

The main configuration page is shown as below:

📾 HFS ~ HTTP File Server 2.2f	Build 155	- 0 <b>- X</b>
🔄 Menu   🖑 Port: 8080   🎎 You are in Expert mode	<i>ν</i> ζ.	
Open in browser http://10.2.11.101:8080/		
	Τορ sj	beed: 0.0 KB/s
Virtual File System	Log	
	17:23:24 Check update: no new versio	n
🔋 IP 🗖 Filename	Status Speed Time left	%
Connections: 0 Out: 0.0 KB/s In: 0.0 KB/s Total Out: 0 B Tot	al In: 0 B VFS: 0 items	.4

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   🕵 You	are in Expert mode
Self Test     Edit HTML template     Other options     Upload     Start/Exit     Virtual File System     Limits     Flash taskbutton	8080/ Top speed 00 KB/s stem Log 17:23:24 Check update: no new version
Fingerprints Tray icons IP address	This IP address is used only for URL building
Accept connections on Dynamic DNS updater URL encoding Updates Wondat	192.168.147.1 192.168.172.1 10.2.11.101 Custom
<ul> <li>j&gt; Load file system Ctrl+O</li> <li>j&gt; Save file system Ctrl+S</li> <li>X Clear file system</li> </ul>	Don't include port in URL Find external address Constantly search for better address
Save options	
Help Web links Uninstall HFS W About	Filename 🕡 Status Speed Time left %
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

The default HTTP port is 8080. You can also reset the HTTP port (make sure there is no port conflict).

HFS ~ HTTP File Server 2.2f	Build 155
🛓 Menu   🖑 Port: 8080   🎎 You are in Expert mode	
Open in browser http://10.2.11.101:8080/	
	Top speed: 0.0 KB/s
Virtual File Sustem Port Specify a port to accept connection, or leave empty to decide automatically. S088] OK Cancel	Log 17:23:24 Check update: no new version
	L <del>o</del>
谢 IP 📃 Filename	Status Speed Time left %
Connections: 0 Out: 0.0 KB/s In: 0.0 KB/s Total Out: 0 B To	tal In: 0 B VFS: 0 items

**3.** Right click the 🐔 icon on the left of the main page, select **Add folder from disk** to add the HTTP Server root directory.

📾 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/		
	Te	op speed: 0.0 KB/s
Virtual File System Log		
Add floa		
Add files		
New empty folder Ins		
S New link		
Advanced +		
Copy URL address Ctrl + C		
🔗 Browse it F9		
Comment		
Bind root to real-folder		
👌 Set user/pass		
Sestrict access		
Customized realm		
✓ Browsable		
A Why is unload disabled?		
Auto-bide empty folders		
Hide file extention in listing	Speed Time left	%
Connections: 0   Out: 0.0 KB/s   In: 0.0 KB/s   Total Out: 0 B   Total In: 0 B VFS: 55	51 items - not savec	H.

4. Locate the root directory from your local system.

📾 HFS ~ HTTP File Server 2.3 beta		Build 275			
📕 Menu   🖑 Port: 80 🌱 👥 You are i	in Easy mode				
Open in browser http://10.2.11.101:8088/ProvisioningDir/				Already i	n clipboard
Virtual File System		Log			
<pre></pre>					
🗿 IP address	🗖 File	Status	Speed	Time	Progress
Out: 0.0 KB/s In: 0.0 KB/s					

- 5. Check the server URL (for example, http://10.2.11.101:8088/ProvisioningDir) by clicking "Open in browser".
- 6. (Optional.) Right-click the root directory name (for example, ProvisioningDir), and then select Set user/pass....
- 7. (Optional.) Enter the desired user name and password for the root directory in the corresponding fields and then click **OK**.

Insert the reques	ted user/pass	<b>-X</b>
Username Password	123	
Re-type password	*****	
		<u>R</u> eset

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