

# SIP-T2 Series/T19(P) E2/T4 Series/T5 Series/W5 Series

# **IP Phones Auto Provisioning Guide**

Version 81.70 Mar. 2017

# **Table of Contents**

Table of Contents	iii
Summary of Changes	1
Changes for Release 81, Guide Version 81.70	1
Introduction	
Getting Started	3
Obtaining the Boot File	
Obtaining Configuration Files	3
Obtaining Phone Information	4
Provisioning Yealink IP Phones	5
Auto Provisioning Process	5
Major Tasks for Auto Provisioning	6
An Instance of Auto Provision Configuration	7
Managing Boot Files	11
Editing Common Boot File	
Creating MAC-Oriented Boot File	
Managing Configuration Files	15
Editing Common CFG File	
Editing MAC-Oriented CFG File	
Creating a New CFG File	
Managing MAC-local CFG File	
Encrypting Configuration Files	
Customizing Resource Files	
Configuring a Provisioning Server	21
Preparing a Root Directory	
Configuring a TFTP Server	
<b>Obtaining the Provisioning Server Address</b>	25

Zero Touch	25
Plug and Play (PnP) Server	26
DHCP Options	27
Phone Flash	29
Configuring Wildcard of the Provisioning Server URL	30

## Triggering the IP Phone to Perform the Auto Provisioning....33

Power On	
Repeatedly	
Weekly	
Flexible Auto Provision	
Auto Provision Now	
Multi-mode Mixed	
SIP NOTIFY Message	
Auto Provisioning via Activation Code	
Downloading and Verifying Configurations	43
Downloading Boot Files and Configuration Files	
Resolving and Updating Configurations	
Using MAC-local CFG File	
Verifying Configurations	
Troubleshooting	47
Glossary	49
Appendix	51
Configuring an FTP Server	
Preparing a Root Directory	51
Configuring an FTP Server	
Configuring an HTTP Server	54
Preparing a Root Directory	54
Configuring an HTTP Server	
Configuring a DHCP Server	
Configuring the DHCP Turbo	59
Add the Option 66 via DHCP Turbo	
Add the Option 43 via DHCP Turbo	64

# **Summary of Changes**

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

## Changes for Release 81, Guide Version 81.70

Documentations of the newly released W56P/W52P/SIP-T58V/T58A/T56A/T40G IP phones have been added.

## 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.

The purpose of this guide is to serve as a basic guidance for provisioning Yealink IP phones, including:

- Yealink SIP-T58V/A
- Yealink SIP-T56A
- Yealink SIP-T48G/S
- Yealink SIP-T46G/S
- Yealink SIP-T42G/S
- Yealink SIP-T41P/S
- Yealink SIP-T40P/G
- Yealink SIP-T29G
- Yealink SIP-T27P/G
- Yealink SIP-T23P/G
- Yealink SIP-T21(P) E2
- Yealink SIP-T19(P) E2
- Yealink W52P/W56P

The auto provisioning process outlined in this guide applies to Yealink SIP-T48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T40G/T29G/T27P/T27G/T23P/T23G/ T21(P) E2/T19(P) E2, W52P and W56P IP phones running firmware version 81 or later and SIP-T58V/T58A/T56A IP phones running firmware version 80 or later. We recommend that IP phones running the latest firmware CANNOT 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 process, the following steps are required:

- Obtaining the Boot File
- Obtaining Configuration Files
- Obtaining Phone Information

### **Obtaining the Boot File**

You can use a boot file to customize the download sequence of configuration files. The configuration files 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. It is efficiently for you to provision your IP phones in different deployment scenarios, especially when you want to apply a set of features or settings to a group of phones.

Before beginning provisioning, you need to obtain the Yealink-supplied template boot file named as "y000000000000.boot". The IP phone tries to download the boot file first, and then download the configuration files referenced in the boot file in sequence during auto provisioning.

Yealink supports the following two types of boot files:

- MAC-Oriented boot file (e.g., 00156574b150.boot)
- Common boot file (y000000000000.boot)

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

## **Obtaining Configuration Files**

Before beginning 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. You can also create and name as many configuration files as you want (e.g., 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.

If boot file is found on the provisioning server, the IP phones download the boot file first, and then download the configuration files referenced in the boot file in sequence during auto provisioning. You can customize the download sequence of configuration files in the boot file as required. If boot file is not found on the provisioning server, IP phones download the common CFG file first, and then the MAC-Oriented CFG file during auto provisioning – i.e., the old mechanism for auto provisioning. You can select whether to use the boot file or not for auto provisioning according to your deployment scenario.

IP phones also support local configuration files named as <MAC>-local.cfg. When a user modifies configurations via web user interface or phone user interface, the non-static settings will be automatically saved to the MAC-local CFG file on the IP phone.

You can ask the distributor or Yealink FAE for template configuration files. You can also obtain the template configuration files online:

http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage.

#### To download template configuration files:

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

For example, the following illustration shows the template files available for SIP-T23G IP phones running firmware version 80.

	Li	IP Phone SIP-T23G ast modified date: 2015/08/11   views: 1983
Datasheet	Datasheet	Yealink SIP-T23G Datasheet.pdf
Firmware & Release Note		
Setup & Maintenance	Firmware &	Yealink_SIP_phones_Release_Notes_of_Version80.pdf New
Documents	Note	T23-44.80.0.70.zip New
Other Documents		44.80.0.60.zip New
User Documents		44.80.0.5.zip
	User	Yealink_SIP-T23P & T23G_User_Guide_V80_60.pdf
	Documents	Yealink_SIP-T2_Series_T19(P) E2_T4_Series_IP_Phones_Administrator_Guide_V80_60.pdf
		Yealink_SIP_Phones_Description of Configuration Parameters in CFG Files_V80_60.zip
		Yealink_SIP-T2_Series_T19(P) E2_T4_Series_IP_Phones_XML_Browser_Developer's_Guide_V80_6 0.pdf
		Yealink AutoProvisioning Template V80.zip
		Yealink_SIP-T2 Series_T19(P) E2_T4 Series_IP_Phones_Auto_Provisioning_Guide_V80_60.pdf

3. Open the folder you extracted and identify the files you will edit.

### **Obtaining Phone Information**

Before beginning 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 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.

### **Auto Provisioning Process**

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 process, 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

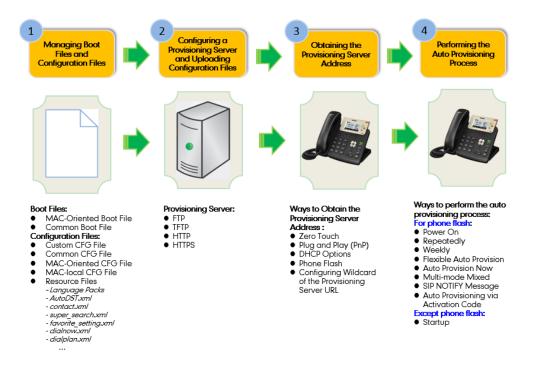


**Provisioning Server** 

## **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 on page 11. For more information on how to manage configuration files, refer to Managing Configuration Files on page 15.

For more information on how to configure a provisioning server, refer to Configuring a Provisioning Server on page 21.

For more information on how to obtain the provisioning server address, refer to Obtaining the Provisioning Server Address on page 25.

For more information on how to perform the auto provisioning process, refer to Triggering the IP Phone to Perform the Auto Provisioning on page 33.

If you are not familiar with auto provisioning process on Yealink IP phones, you can refer to An Instance of Auto Provision Configuration on page 7.

## **An Instance of Auto Provision Configuration**

This section shows an instance of auto provision configuration.

1. Manage boot files.

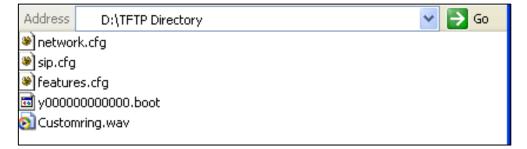
Specify the desired download path (e.g., tftp://10.2.5.193/network.cfg) of the configuration files in the boot file (e.g., y0000000000.boot). For more information, refer to Managing Boot Files on page 11.

```
#!version:1.0.0.1
## The header above must appear as-is in the first line
    include:config <tftp://10.2.5.193/network.cfg>
    include:config <../sip.cfg>
    include:config "features.cfg"
overwrite_mode = 1
```

2. Manage configuration files.

Add/Edit the desired configuration parameters in the CFG file (e.g., features.cfg) you want the IP phone to download. For more information on how to manage configuration files, refer to Managing Configuration Files on page 15.

- 3. Configure the TFTP server.
  - 1) Place boot files and configuration files to TFTP root directory (e.g., D:\TFTP Directory).



3CDaemon				
<u>File View H</u> elp TFTP Server	Start Time	Peer	Bytes	Status
Configure TFTF Server	Jul 12, 2016 09:30:13			Listening for TFTP requests on IP address: 10.2.5.193 Port 69
TFTP Server is started. Click here to stop it.			dov	server URL where the IP phone vnloads boot files and configuration
Logging to Tftpd log. Click to stop.			Tiles	s from is tftp://10.2.5.193/
XX Wot debugging Click to start.				
Clear list.				
View Log/Debug files.				

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

**3)** Select **Configure TFTP Server**. Click the from your local system

... utton to locate the TFTP root directory

from your lo	ocal system.
--------------	--------------

3CDaemon				
<u>File View 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 IFTP Server	3CDaemon Configurat	ion		×
	FTP Profi	les		Syslog Configuration
<b>STOP</b>	General Con	figura	tion	TFTP Configuration
TFTP Server is started. Click here to stop it.	Create directory n	ames ir	n incomi	ng file re <mark>v</mark>
	Allow overwrite of	existi	ng file	s?
Logging to Tftpd.log. Click to stop.	Upload/Download	Ī	):\TFTP	Directory\
X.	Per-packet timeout	in sec	onds	5
Not debugging. Click to start.	Maximum retries			10
Clear list.	Interframe transmi:	sion		0
View Loz/Debuz files.				

For more information on how to configure a provisioning server, refer to Configuring a Provisioning Server on page 21.

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

	Status	Account	Network	DSSKey	Features	Settings	Director	y Security	
Preference		Auto Provision					NOTE		
Time & Date	e & Date DHCP Active			<ul> <li>On Off</li> <li>On Off</li> </ul>			Auto Provision The IP phone can interoperate		
Call Display						with provisioning server using auto provisioning for deploying			
Upgrade		OHCP Option Value					the IP phones. When the IP phone triggers perform auto provisioning, it		
Auto Provision		Server URL		tftp://10.2.5.193/					
Configuration		Jser Name						o download the tion files from the	
Configuration	Password					r the access	access URL of point process, th		
Dial Plan		Attempt Expired Tin				has beelewood li			
Voice	Common AES Key			•••••		the Server URL field.		nguration nies to the	
Ring	MAC-Oriented AES Key		(ey	•••••			🚺 You c	an click here to get	
rung	2	Zero Active		Disabled	• m		more gui	e guides.	
Tones		Wait Time(1~100s)		5					
Softkey Layout		Power On		• On O Off					

For more information on how to obtain the provisioning server address, refer to Obtaining the Provisioning Server Address on page 25.

									Log Out			
1	ealink 1236							Eng	sish(English) 👻			
		Status	Account	Network	DSSKey	Features	Settings	Directory	Security			
	Preference		Auto Provision					NOTE	•			
			PNP Active		🔹 On 🔘 Off							
	Time & Date		DHCP Active		🖲 On 🔘 Off				can interoperate			
	Call Display		Custom Option(128	~254)				with provisioning server usit auto provisioning for deplo				
	Upgrade		DHCP Option Value					the IP phones				
1	Auto Provision		Server URL		thp://10.2.5.193/			perform auto	phone triggers to provisioning, it will			
1	Contraction of the second s		User Name					request to do configuration if				
	Configuration		Password		•••••			provisioning se	rver. During the ing process, the			
	Dial Plan		Attempt Expired Tir	ne(s)	5			IP phone will o	fownload and			
	Voice		Common AES Key					phone flash.	uration files to the			
	and the second se		MAC-Oriented AES	(ey				They can d	You can click here to get			
	Ring								more guides.			
	Tones		Wait Time(1~100s)		5							
	Softkey Layout		Power On		e on O off					١.		
1	TR069		Repeatedly		O On 💌 Off					P		
			Interval(Minutes)		1440							
	Voice Monitoring		Weekly		🔿 On 💌 Off							
	SIP		Weekly Upgrade Int	erval(0~12week)	4							
			Inactivity Time Expir	e(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> <li>✓ Saturday</li> </ul>	perfor	m the au	<b>ovision N</b> etto provisio	ning			
			Flexible Auto Provisio	00	🗢 On 🖲 Off	l pr	rocess im	mediately.				
			Flexible Interval Day		30	7						
			Flexible Time		02 : 00 -							
			Conf		Autoprovision	Now						

5. Trigger the IP phone to perform the auto provisioning.

For more information on how to trigger the phone to perform the auto provisioning, refer to Triggering the IP Phone to Perform the Auto Provisioning on page 33.

## **Managing Boot Files**

Yealink IP phones support downloading CFG files referenced in the boot files in sequence. Before beginning provisioning, you may need to edit and customize your boot files.

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 UltraEdit.

### **Editing Common Boot File**

The common boot file is effectual 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
```

#### When editing the boot file, learn the following:

- The line beginning with "#" is considered to be a comment.
- The file header "#!version:1.0.0.1" is not a comment and must be placed in the first line. It cannot be edited or deleted.
- The file format must be \*.boot.
- Each "include" statement can reference a configuration file. The referenced configuration file format must be \*.cfg. The "include" statement can be repeated as many times as needed. It means one or more CFG files can be referenced in the boot file.
- Each "include" statement must use the following format:

include:config < *download path of the CFG file*> or include:config "*download path of the CFG file*"

The download path of the CFG file must point to a specific CFG file. It supports the following path forms:

- Relative path (relative to the boot file):

For example, sip.cfg, HTTP Directory/sip.cfg, ../sip.cfg, etc.

- Absolute path (or URL):

For example, http://10.2.5.258/HTTP Directory/sip.cfg.

• The CFG files are downloaded in the order listed (top to bottom). The parameters in the

new downloaded configuration files will override the duplicate parameters in files downloaded earlier.

- "overwrite\_mode = 1" means overwrite mode is enabled. The overwrite mode will be applied to the configuration files specified to download. This parameter can only be used in boot files. Overwrite mode includes the following features:
  - The NULL values take effect (if the value of a parameter in configuration files is left blank, the factory default value can take effect.)

For example, the label for account 1 is "abc", and the value of the parameter "account.1.label" is left blank in the configuration files (e.g., account.1.label = or account.1.label = ""). The factory default value Blank takes effect after auto provisioning. So the label for account 1 will be deleted.

- The deletions of the configuration parameters take effect (if a parameter in configuration files is deleted, the factory default value can take effect immediately.)

For example, account.1.enable = 1 is deleted or commented out in the configuration files. The factory default value 0 takes effect after auto provisioning. So account 1 is disabled.

- Note that if a boot file is used but the value of the parameter "overwrite\_mode" is not configured, the default value 1 will take effect. If you want to disable the overwrite mode, configure "overwrite\_mode = 0" in the boot file.
- Note

Overwrite mode only affects the non-static settings configured using configuration files. If you do not use the boot file for auto provisioning, overwrite mode is disabled by default and you are not allowed to enable it.

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

The MAC-Oriented boot file is only effectual for the specific phone. It 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, the MAC-Oriented boot file has to be named as 00156574b150.boot (case-sensitive) respectively.

The IP phones try to download the MAC-Oriented boot file first from the server during auto provisioning first. If no matched MAC-Oriented boot file is found on the server, the IP phones try to download the common boot file.

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 Editing Common Boot File on page 11.
- **2.** Copy the contents from the common boot file and specify the configuration files to be downloaded.

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

#### 00156574b150.boot ×

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

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

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

## **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 beginning 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 UltraEdit.

For more information on description of all configuration parameters in configuration files, refer to *Yealink\_SIP-T2\_Series\_T19(P) E2\_T4\_Series IP Phones\_Description of Configuration Parameters in CFG Files\_V81.xlsx, Yealink IP DECT Phones Description of Configuration Parameters in CFG Files.xlsx* or *Yealink\_SIP-T5\_Series\_Smart\_Media\_Phones\_Description of Configuration Parameters in CFG Files.xlsx.* 

### **Editing Common CFG File**

The Common CFG file is effectual 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.

Phone Model	Common CFG File
SIP-T58V/A	y0000000058.cfg
SIP-T56A	y00000000056.cfg
SIP-T48S	y0000000065.cfg
SIP-T46S	y0000000066.cfg
SIP-T42S	y0000000067.cfg
SIP-T41S	y0000000068.cfg
SIP-T48G	y0000000035.cfg
SIP-T46G	y0000000028.cfg
SIP-T42G	y0000000029.cfg
SIP-T41P	y0000000036.cfg
SIP-T40P	y0000000054.cfg
SIP-T40G	y00000000076.cfg
SIP-T29G	y0000000046.cfg
SIP-T27P	y0000000045.cfg

The names of the common CFG file requirements for the phone model are:

Phone Model	Common CFG File
SIP-T27G	y0000000069.cfg
SIP-T23P/G	y00000000044.cfg
SIP-T21(P) E2	y0000000052.cfg
SIP-T19(P) E2	y0000000053.cfg
W52P/W56P	y0000000025.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:

#### When editing the common CFG file, learn the following:

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

- Separate each configuration parameter and value with an equal sign.
- Set only one configuration parameter per line.
- Put the configuration parameter and value on the same line, and do not break the line.

### **Editing MAC-Oriented CFG File**

The MAC-Oriented CFG file is only effectual for the specific phone. It 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, 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##
*****
## Account1 Basic Settings ##
*************
account.1.enable =
account.1.label =
account.1.display_name =
account.1.auth_name =
account.1.user name =
account.1.password =
account.1.outbound proxy enable =
account.1.outbound host =
account.1.outbound_port =
account.1.dial_tone =
<pre>##It configures the transport type for account 1. 0-UDP,1-TCP,2-TLS,3-DNS-NAPTR</pre>
##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 =

#### When editing the MAC-Oriented CFG file, learn the following:

- The line beginning with "#" is considered to be a comment.
- The file header "#!version:1.0.0.1" is not a comment and must be placed in the first line. It cannot be edited or deleted.
- The file format must be \*.cfg.
- The filename matches the MAC address of your phone.
- Each line must use the following format and adhere to the following rules:

Configuration Parameter= Valid Value

- Separate each configuration parameter and value with an equal sign.
- Set only one configuration parameter per line.
- Put the configuration parameter and value on the same line, and do not break the line.

SIP-T58V/T58A/T56A/T48G/T48S/T46G/T46S/T29G IP phones support 16 accounts, SIP-T42G/S IP phones support 12 accounts, SIP-T41P/T41S/T27P/T27G IP phones support 6 accounts, W52P/W56P IP DECT phones support 5 accounts; SIP-T40P/T40G/T23P/T23G IP phones support 3 accounts, SIP-T21(P) E2 IP phones support 2 accounts, SIP-T19 (P) E2 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 on page 15 or Editing MAC-Oriented CFG File on page 17.
- **2.** Copy configuration parameters from the template configuration files and set the valid values for them.

settings.cfg ×

```
10 20 30 40 50
#!version:1.0.0.1
phone_setting.phone_lock_enable = 1
phone_setting.phone_locak_lock_key_type = 0
features.dnd_mode = 1
static.lang.wui = English
static.lang.gui = English
```

3. 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 user personalization settings, even after auto provision. As with the MAC-Oriented CFG files, MAC-local CFG files are only effectual for the specific phone too. 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's current firmware version doesn't support generating 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 personalization settings, refer to Yealink\_SIP-T2\_Series\_T19(P) E2\_T4\_Series\_IP\_Phones\_Administrator\_Guide\_V81, Yealink IP DECT Phone Administrator Guide\_V81 or Yealink\_SIP-T5\_Series\_Smart\_Media\_Phones\_Administrator\_Guide.

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 *Yealink\_SIP-T2\_Series\_T19(P) E2\_T4\_Series\_IP\_Phones\_Administrator\_Guide\_V81*, *Yealink IP DECT Phone Administrator Guide\_V81* or *Yealink\_SIP-T5\_Series\_Smart\_Media\_Phones\_Administrator\_Guide*.

### **Encrypting Configuration Files**

To protect against unauthorized access and tampering of sensitive information (e.g., 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*.

### **Customizing Resource Files**

When configuring some particular features, you may need to upload resource files to IP phones, such as personalized ring tone file, language package file and logo file. Yealink supplies the following resource file templates:

Feature	Template File Name
DST	AutoDST.xml
	For example,
Languago Dacks	000.GUI.English.lang
Language Packs	1.English_note.xml
	1.English.js
Replace Rule	dialplan.xml
Dial-now	dialnow.xml (not applicable to W56P IP DECT phones)
	CallFailed.xml
Softkey Layout	CallIn.xml
(not applicable to	Connecting.xml
W52P/W56P IP DECT	Dialing.xml (not applicable to SIP-T58V/T58A/T56A/T48G/T48S IP
phones)	phones)
	RingBack.xml

Feature	Template File Name
	Talking.xml
Directory (not applicable to SIP-T58V/T58A/T56A IP phones)	favorite_setting.xml
Super Search in dialing	super_search.xml
Local Contact File	contact.xml
Remote XML Phone Book	Department.xml Menu.xml
Ring Tone (not applicable to W56P IP DECT phones)	None
Logo customization (not applicable to W56P IP DECT phones)	None
Wallpaper (not applicable to W56P IP DECT phones)	None
Firmware	For SIP-T48G/T48S/T46G/T46S/T42/T42S/T41P/T41S/T40P/T29G/T27 P/T27G/T23P/T23G/T21(P) E2/T19(P) E2: X.81.0.XX.rom For example, 44.81.0.15.rom For SIP-T58V/T58A/T56A: X.80.0.XX.rom For example, 58.80.0.10.rom

Ask the distributor or Yealink FAE for resource file templates. For more information on an explanation of the configuration parameters that relate to these features, refer to *Yealink\_SIP-T2\_Series\_T19(P) E2\_T4\_Series\_IP\_Phones\_Administrator\_Guide\_V81*, *Yealink IP DECT Phone Administrator Guide\_V81* or *Yealink\_SIP-T5\_Series\_Smart\_Media\_Phones\_Administrator\_Guide*.

## **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 on page 51 and Configuring an HTTP Server on page 54.

### **Preparing a Root Directory**

#### To prepare a root directory:

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



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

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

Administrators (VANS	TD80\Admini	strators)	^
CREATOR OWNER			
Hill, James (jahill@my	corvornamo	coml	
SYSTEM	ser verhame.	comj	~
< C			>
		\dd	Remove
Permissions for Everyone		Allow	Deny
Full Control			<b>_</b> ^
Modify			
Read & Execute			
List Folder Contents		~	
Read		~	
Write		~	
Consist Dormissions			
For special permissions or fo	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:

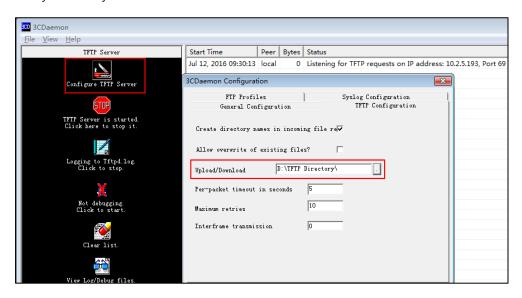
1. Double click **3CDaemon.exe** to start the application.

A configuration page is shown as below:

• 3CDaemon					
File View Help					
TFTP Server	Start Time	Peer	Bytes	Status	
Configure IFTP 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 your local system:

... utton to locate the TFTP root directory from



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 support obtaining 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 (Custom option-->option 66-->option 43) -->Phone Flash. The following sections detail the process of each way (take the SIP-T23G IP phone as an example).

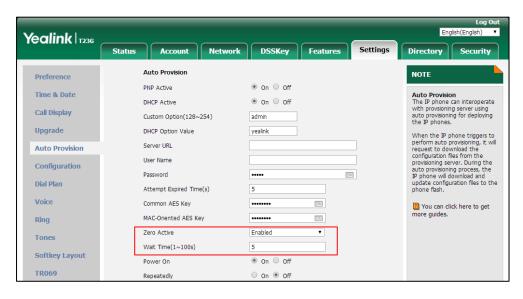
### **Zero Touch**

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/W56P IP phones.

#### To configure zero touch via web user interface:

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

The default value is 5.



4. Click Confirm to accept the change.

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



Press the **OK** soft key.

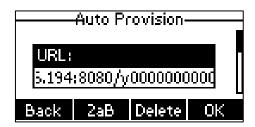
The network parameters are configurable via phone user interface:

	——Neti	work——	
IP M	ode:		
IPv4	1		41
Back		Switch	Next

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 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 the auto provisioning process 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:

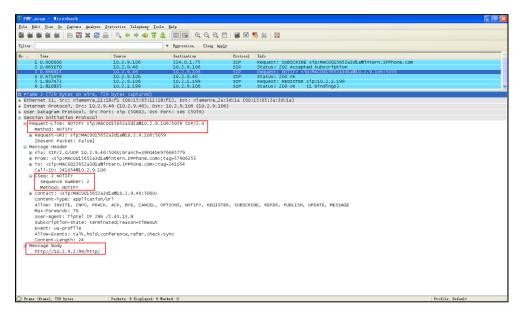
1. Click on Settings->Auto Provision.

Yealink 1236					Log Out English(English) ▼
	Status Account Network	DSSKey	Features	Settings	Directory Security
Preference	Auto Provision				NOTE
Time & Date	PNP Active	🖲 On 🔍 Off			Auto Provision
	DHCP Active	🖲 On 🔍 Off			The IP phone can interoperate with provsioning server using
Call Display	Custom Option(128~254)	admin			auto provisioning for deploying the IP phones.
Upgrade	DHCP Option Value	yealink			When the IP phone triggers to
Auto Provision	Server URL				perform auto provisioning, it will request to download the
Configuration	User Name				configuration files from the provisioning server. During the
<u> </u>	Password	•••••	1.11		auto provisioning process, the IP phone will download and
Dial Plan	Attempt Expired Time(s)	5			update configuration files to the phone flash.
Voice	Common AES Key	•••••	<u></u>		You can click here to get
Ring	MAC-Oriented AES Key	•••••	<u></u>		more guides.
_	Zero Active	Enabled	¥		
Tones	Wait Time(1~100s)	5			
Softkey Layout	Power On	🖲 On 🔍 Off			
TR069	Repeatedly	🔍 On 🖲 Off			
Voice Monitoring	Interval(Minutes)	1440			
STP	Weekly	🔍 On 🖲 Off			
Jar .	Weekly Upgrade Interval(0~12week)	4			
	Inactivity Time Expire(0~120min)	0			

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

#### **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.



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

## **DHCP Options**

Yealink IP phones support obtaining the provisioning server address by detecting DHCP options during startup.

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

You can configure the phone to obtain the provisioning server address via a custom DHCP option. To obtain the provisioning server address via a custom DHCP option, make sure the DHCP option is properly configured on the phone. The custom DHCP option must be in accordance with the one defined in the DHCP server.

For more information on how to configure a DHCP server, refer to Configuring a DHCP Server on page 58.

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

- 1. Click on Settings->Auto Provision.
- 2. Mark the **On** radio box in the **DHCP Active** field.
- 3. Enter the desired value in the Custom Option(128~254) field.

Yealink 1236							Eng	Log Out Jish(English) 🔻
	Status	Account	Network	DSSKey	Features	Settings	Directory	Security
Preference	А	uto Provision					NOTE	
Time & Date		NP Active		<ul> <li>On</li> <li>Off</li> <li>On</li> <li>Off</li> </ul>	_		Auto Provisio The IP phone	on can interoperate
Call Display	с	ustom Option(128~	254)	128			with provsionin auto provisionin the IP phones.	ng for deploying
Upgrade	D	HCP Option Value		yealink			When the IP p	hone triggers to
Auto Provision	S	erver URL					request to dov	
Configuration	-	iser Name assword					auto provisioni	rver. During the ng process, the
Dial Plan		ttempt Expired Tim	e(s)	5			IP phone will d update configu phone flash.	ownload and iration files to the
Voice	с	ommon AES Key		•••••	2000 c		You can cli	ck here to get
Ring	м	IAC-Oriented AES K	еу	•••••			more guides.	
Tones	Z	ero Active		Enabled	¥			
Cafilian Lanaut	v	Vait Time(1~100s)		5				
Softkey Layout	P	ower On		🖲 On 🔍 Off				
TR069	R	epeatedly		🔍 On 🖲 Off				
Voice Monitoring	Ir	nterval(Minutes)		1440				
SIP	v	Veekly		🔍 On 🖲 Off				
	v	Veekly Upgrade Inte	rval(0~12week)	4				
	Ir	nactivity Time Expire	(0~120min)	0				

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

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

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

For more information on the DHCP options, refer to *Yealink\_SIP-T2\_Series\_T19(P) E2\_T4\_Series\_IP\_Phones\_Administrator\_Guide\_V81*, *Yealink IP DECT Phone Administrator Guide\_V81* or *Yealink\_SIP-T5\_Series\_Smart\_Media\_Phones\_Administrator\_Guide*. The following figure shows the example messages of obtaining the TFTP server address from a custom DHCP option:

DHCPserver-tftp.pcap [Wireshark 1.6				
<u>Eile E</u> dit <u>V</u> iew <u>Go</u> <u>C</u> apture <u>A</u> nalyze	Statistics Telephony Loois In			
3 🗑 2 🗑 🕷 🕷   🖻 🔀 X 😂			🖭   🍇 🗹 🕵 %   😫	1
Filter: sip    bootp		Expression Clear App	ly	
lo, Time Source	Destination Protocol	Length Info		
14 17,967476 0.0.0.0	255, 255, 255, 255 DHCP		- Transaction ID 0x8	8e96872
15 18.137781 10.2.8.105	10.2.8.106 DHCP	342 DHCP Offer	- Transaction ID 0x8	8e96872
16 18.177701 0.0.0.0	255.255.255.255 DHCP	590 DHCP Request	- Transaction ID 0x8	8e96872
17 18.178902 10.2.8.105	10.2.8.106 DHCP	342 DHCP ACK	- Transaction ID 0x8	8e96872
■ Internet Protocol Version 4, ⊌ User Datagram Protocol, Src Bootstrap Protocol Massage type: Boot Reply ( Hardware type: Ethernet Hardware type: Ethernet Hardware in Die XokSe96872 Seconds elapsed: 100 Bootp flags: 0x0000 (unica Client IP address: 0.0.0.0 Your (client) IP address: 0. Client IP address: 0.0.0 Client MAC address: xiamen Client MAC address: xiamen Client hardware address pa Server host name: mid0171- Boot file name not given Magic cookie: DHCP Boption: (t=1,1=4) Subnet M Boption: (t=5,1,=1) DHCP Me Boption: (t=5,1,=4) Rebindi Doption: (t=1,2,1=4) Dec SE Doption: (t=1,2,1=4) Dec SE Doption: (t=1,2,1=4) Dec SE Doption: (t=5,1,=4) Dec SE Doption: (t=5,1,	Port: bootps (67), Dst Po 2) st) (0.0.0.0) 10.2.8.106 (10.2.8.106) 1.2.8.105 (10.2.8.105) 0.0.0 (0.0.0.0) ve_38:28:40 (00:15:65:38: dding: 00000000000000000 for 3xon ssage Type = DHCP ACK ask = 255.255.255.0 ess Lease Time = 6 hours. nd fime value = 3 hours. st Lease Time = 6 hours. s full security server IP [Tot 02e322e382e3130352f	ort: bootpc (68) :28:d8) )000 15 minutes ? [Торо]]	06 (10.2.8.106)	

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

## **Phone Flash**

Yealink IP phones support obtaining 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).

ealink 17236				Log O English(English)		
	Status Account Network	DSSKey Features	Settings	Directory Security		
Preference	Auto Provision			NOTE		
	PNP Active	🖲 On 🔘 Off				
Time & Date	DHCP Active	🖲 On 🔘 Off		Auto Provision The IP phone can interoperate		
Call Display	Custom Option(128~254)			with provsioning server using auto provisioning for deploying		
Upgrade	DHCP Option Value			the IP phones.		
Auto Provision	Server URL	tftp://10.2.5.193/		When the IP phone triggers to perform auto provisioning, it w		
	User Name			request to download the configuration files from the		
Configuration	Password	•••••		provisioning server. During the		
Dial Plan	Attempt Expired Time(s)	5		auto provisioning process, the IP phone will download and		
Voice	Common AES Key	•••••		update configuration files to phone flash.		
Ring	MAC-Oriented AES Key	•••••		You can click here to get		
King	Zero Active	Disabled 👻		more guides.		
Tones	Wait Time(1~100s)	5				

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

After the above configuration is completed, the IP phone will connect to the configured provisioning server and perform the auto provisioning process by one of the following 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 the Auto Provisioning on Page 33.

### **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 the boot files and configuration files located. For more information on the parameter, refer to *Yealink\_SIP-T2\_Series\_T19(P) E2\_T4\_Series IP Phones\_Description of Configuration Parameters in CFG Files\_V81.xlsx, Yealink IP DECT Phones Description of Configuration Parameters in CFG Files.xlsx* or *Yealink\_SIP-T5\_Series\_Smart\_Media\_Phones\_Description of Configuration Parameters in CFG Files.xlsx.* 

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 wildcard feature.

- 1. Create two directories on the root directory of 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 on page 11.

# **Triggering the IP Phone to Perform the Auto Provisioning**

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

- 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 auto provisioning process will detect the call status every 30 seconds. If the call is released within 2 hours, the auto provisioning process will be performed normally. Otherwise, the process will end, due to timeout.

## **Power On**

The IP phone performs the auto provisioning process 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.

Yealink 1236							Englis	Log Ou h(English) ▼
	Status	Account	Network	DSSKey	Features	Settings	Directory	Security
Preference	Auto P	Provision					NOTE	
Time & Date	PNP Ac			● On ○ Off			Auto Provision	
Call Display	DHCP A Custom	Active h Option(128~2	254)	On Off     128			The IP phone ca with provisioning auto provisioning	server using
Upgrade	DHCP O	Option Value		yealink			the IP phones. When the IP pho	one triagers to
Auto Provision	Server I	URL		tftp://10.2.5.169/	1		perform auto pro request to down	load the
Configuration	User Na	ame					configuration file provisioning serve auto provisioning	er. During the
Dial Plan	Passwor	rd ot Expired Time	e(s)	5			IP phone will dov update configura phone flash.	wnload and
Voice	Commo	on AES Key		•••••	1		You can click	, here to get
Ring	MAC-Or	riented AES Ke	у	•••••	1.1.1.1 1.1.1.1		more guides.	
Tones	Zero Ac	ctive		Enabled	٣			
Softkey Layout	Wait Ti	ime(1~100s)		5				
Softkey Layout	Power	On		🖲 On 🔍 Off				
TR069	Repeat	edly		🔍 On 🖲 Off				
Voice Monitoring	Interval	l(Minutes)		1440				
SIP	Weekly	r		🔘 On 🖲 Off				
	Weekly	Upgrade Inter	val(0~12week)	4				
	Inactivit	ty Time Expire(	(0~120min)	0				

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

# Repeatedly

The IP phone performs the auto provisioning process 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   1236	Status	Account	Network	DSSKey	Features	Settings	Directory Security
Preference		Auto Provision					NOTE
Time & Date		PNP Active		🖲 On 🔍 Off			Auto Provision
		DHCP Active		🖲 On 🔍 Off			The IP phone can interoperate with provsioning server using
Call Display		Custom Option(128	~254)	128			auto provisioning for deploying the IP phones.
Upgrade		DHCP Option Value		yealink			When the IP phone triggers to
Auto Provision		Server URL		tftp://10.2.5.169/			perform auto provisioning, it wi request to download the
o. C:		User Name					configuration files from the provisioning server. During the
Configuration		Password					auto provisioning process, the IP phone will download and
Dial Plan		Attempt Expired Tin	ne(s)	5			update configuration files to th phone flash.
Voice		Common AES Key		•••••			You can click here to get
Rina		MAC-Oriented AES k	(ey	•••••			more guides.
3		Zero Active		Enabled	T		
Tones		Wait Time(1~100s)		5			
Softkey Layout		Power On		● On ○ Off			
TR069	Г	Repeatedly		• On Off			
Voice Monitoring		Interval(Minutes)		1440			
	L	Weekly		◯ On ◉ Off			
SIP							

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 the auto provisioning process 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 the auto provisioning process. You can also configure a regular week interval to trigger the IP phone to perform the auto provisioning process. You can specify the delay time to perform an auto provisioning process 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 for 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 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.

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

ealink   1236							Ere	lish(English)
	Status	Account	Network	DSSKey	Features	Settings	Directory	Security
Preference		Auto Provision					NOTE	2
		PNP Active		🖲 On 🔿 Off				
Time & Date	1	DHCP Active		🖲 On 🔿 Off			Auto Provision The IP phone	on can interoperate
Call Display		Custom Option(128~	254)					ng server using ing for deploying
Upgrade		DHCP Option Value		yealnk			the IP phones	
Auto Provision		Server URL		tftp://192.168.1.1	100/			phone triggers to provisioning, it wi
NAMES OF TAXABLE PARTY.		User Name					request to do configuration f	wnload the
Configuration	1	Password					provisioning se	ever. During the
Dial Plan		Attempt Expired Tim	e(s)	5			IP phone will d	
Voice		Common AES Key					phone flash.	uration files to the
Ring		MAC-Oriented AES K	ey				You can d	lick here to get
Rong		Zero Active		Enabled			more guides.	
Tones		Wait Time(1~100s)		5				
Softkey Layout		Power On		🖲 On 🗇 Off				
TR069		Repeatedly		🔿 on 💌 off				
	1	Interval(Minutes)		1440				
Voice Monitoring		Weekly		🖲 On 🗇 Off				
SIP		Weekly Upgrade Inte	erval(0~12week)	4				
	1	Inactivity Time Expire	(0~120min)	10				
		Time		02 : 00 - 03	: 00			
		Day of Week		Sunday V Monday Tuesday Wednesday Thursday Friday Saturday				

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

## **Flexible Auto Provision**

The IP phone performs the auto provisioning process 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 the auto provisioning process.

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

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

#### To activate the flexible auto provision mode via 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.

ealink   1236	itatus Account Network	DSSKey	Features	Settings	Directory	Security
Preference	Auto Provision				NOTE	
	PNP Active	🖲 On 🗇 Off				
Time & Date	DHCP Active	🖲 on 🗇 off			Auto Provisio The IP phone	on can interoperate
Call Display	Custom Option(128~254)	admin				ng server using ing for deploying
Upgrade	DHCP Option Value				the IP phones	
Auto Provision	Server URL	tftp://192.168.1.100	N.			phone triggers to provisioning, it wi
and the second	User Name				request to do configuration f	wnload the
Configuration	Password				provisioning se	ever. During the
Dial Plan	Attempt Expired Time(s)	5			IP phone will d	fownload and
Voice	Common AES Key				phone flash.	uration files to th
Ring	MAC-Oriented AES Key				Tou can cl	ick here to get
long	Zero Active	Disabled			more guides.	
Tones	Wait Time(1~100s)	5				
Softkey Layout	Power On	🔹 On 🗇 Off				
TR069	Repeatedly	🔿 On 💌 Off				
	Interval(Minutes)	1440				
Voice Monitoring	Weekly	🗇 On 💌 Off				
SIP	Weekly Upgrade Interval(0~12week)	4				
	Inactivity Time Expire(0~120min)	0				
	Time	00 : 00 - 00 :	00			
	Day of Week	Sunday Monday M				
	Flexible Auto Provision	🖲 On 🔘 Off				
	Flexible Interval Days	30				
	Flexible Time	01 : 00 - 05 :	00			
		Autoprovision No	w			

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 the auto provisioning process immediately.

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

1. Click on Settings->Auto Provision.

	tus Account Network	DSSKey	Features	Settings	Directory Security
Preference	Auto Provision				NOTE
	PNP Active	🖲 On 🔿 Off			
Time & Date	DHCP Active	🖲 On 🔘 Off			Auto Provision The IP phone can interoperate
Call Display	Custom Option(128~254)	admin			with provisioning server using auto provisioning for deploying
Upgrade	DHCP Option Value				the IP phones.
	Server URL	tftp://192.168.1.100	/		When the IP phone triggers to
Auto Provision	User Name				perform auto provisioning, it will request to download the
Configuration	Password				configuration files from the provisioning server. During the
Dial Plan	Attempt Expired Time(s)	s			auto provisioning process, the IP phone will download and
Voice	Common AES Key				update configuration files to the phone flash.
VOICE	MAC-Oriented AES Key				
Ring	Zero Active	Disabled			You can click here to get more guides.
Tones	Wait Time(1~100s)	5			
Softkey Layout	Power On	● On ◎ Off			
	Repeatedly	On Off			
TR069					
Voice Monitoring	Interval(Minutes)	1440			
SIP	Weekly	🗇 On 兽 Off			
	Weekly Upgrade Interval(0~12week)				
	Inactivity Time Expire(0~120min)	0			
	Time	00 : 00 - 00 :	00		
	Day of Week	Sunday Monday Monday U Huesday U Wednesday U Thursday V Friday Saturday			
	Flexible Auto Provision	🔹 On 🗇 Off			
	Flexible Interval Days	30			
	Flexible Time	01 : 00 - 05 :	00		
		Autoprovision No	w		

2. Click Autoprovision Now.

The IP phone will perform the auto provisioning process 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 the auto provisioning process when it is powered on and at a specified interval.

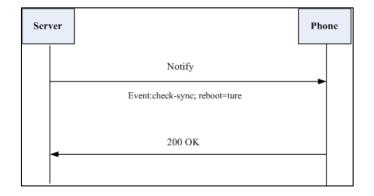
## **SIP NOTIFY Message**

The IP phone will perform the auto provisioning process 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 Yealink\_SIP-T2\_Series\_T19(P) E2\_T4\_Series IP Phones\_Description of Configuration Parameters in CFG Files\_V81.xlsx, Yealink IP DECT Phones

*Description of Configuration Parameters in CFG Files.xlsx* or *Yealink\_SIP-T5\_Series\_Smart\_Media\_Phones\_Description of Configuration Parameters in CFG Files.xlsx.* 

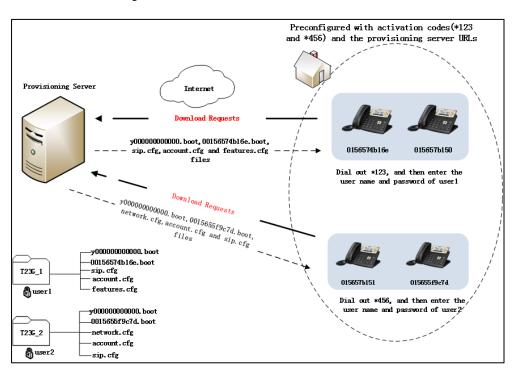
This method requires server support.

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 normally used for IP phones distributed by retail sales. It has the advantage that the IP phones do not need to be handled (e.g., registering account) before sending them to end-users.



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

- 1. Create multiple directories (e.g., 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 (e.g., \*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:

	AutoP /	Authority∙	
Use	r Name:		
Cance	l 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 the auto provisioning

process.

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 on page 11 and Managing Configuration Files on page 15.

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

# **Downloading and Verifying Configurations**

## **Downloading Boot Files and Configuration 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 in sequence from the provisioning server during the auto provisioning process. 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 in sequence. 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.

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 the auto provisioning process is completed. For 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 the auto provisioning process 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 repeated update. This is used to avoid unnecessary restart and impact of phone use. On the contrary, the IP phone will update configurations.

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

The phone only reboots when there is at least a specific configuration requiring 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 *Yealink\_SIP-T2\_Series\_T19(P) E2\_T4\_Series IP Phones\_Description of Configuration Parameters in CFG Files\_V81.xlsx, Yealink IP DECT Phones Description of Configuration Parameters in CFG Files.xlsx* or *Yealink\_SIP-T5\_Series\_Smart\_Media\_Phones\_Description of Configuration Parameters in Parameters in CFG Files.xlsx.* 

If configuration files have been AES encrypted, the IP phone will uses 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 user 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 value of the parameter "static.auto\_provision.custom.protect" will be forced to set to 1.

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 *Yealink\_SIP-T2\_Series\_T19(P) E2\_T4\_Series\_IP\_Phones\_Administrator\_Guide\_V81, Yealink IP DECT Phone Administrator Guide\_V81* or *Yealink\_SIP-T5\_Series\_Smart\_Media\_Phones\_Administrator\_Guide.* 

## **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 the auto provisioning process, 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>Ele E</u> d	it <u>V</u> iew <u>G</u> o <u>C</u> aptur	e <u>A</u> nalyze <u>S</u> tatistics	Telephony Tools Internal	ls <u>H</u> elp	
• •	🖌 🔳 🔬 📄 🗎	• ¥ 🗃   0 🍐	🍬 🥥 📅 👱 🗐 🖽		🗂 📓 🗹 🍕 🔆 📘
• •				444	
Filter: t	ftp		💌 Expr	ression Clear	Apply Save
lo.	Time	Source	Destination	Protocol	Length Info
	12,389499000	10.2.20.73	10.2.5.193	TETP	81 Read Request, File: 00156574b16e.boot, Transfer type: octet, blksize\000=1432\000
	12.389595000	10.2.20.73	10.2.5.193	TETP	81 Read Request, File: 00156574b16e.boot, Transfer type: octet, blksize/000=1432/000
	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
	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
	17,440553000	10.2.20.73	10.2.5.193	TETP	82 Read Request, File: v00000000000, boot, Transfer type: octet, blksize\000=1432\000
	1/.440666000	10.2.20.73	10.2.5.193	TETP	82 Read Request, File: y000000000000 boot, Transfer type: octet, b1R512(000-1432)000
	17,462578000	10.2.5.193	10.2.20.73	TETP	57 Option Acknowledgement, blksize\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.ctg, 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	5 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
	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
	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.

	ftp		<ul> <li>Expr</li> </ul>	ession 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
3175	5 28.952342000	10.2.20.73	10.2.5.193	FTP	91 Request: RETR y0000000000.boot
	5 28.952453000	10.2.20.73	10.2.5.193	FTP	91 [TCP Retransmission] Request: RETR y000000000000.boot
	9 28.958927000	10.2.5.193	10.2.20.73	FTP	102 Response: 125 Using existing data connection
	28.959253000	10.2.5.193	10.2.20.73	FTP	102 [TCP Retransmission] Response: 125 Using existing data connection
	0 28.963510000	10.2.5.193	10.2.20.73	FTP	122 Response: 226 Closing data connection; File transfer successful.
	3 28.963862000	10.2.5.193	10.2.20.73	FTP	122 [TCP Retransmission] Response: 226 Closing data connection; File transfer successful.
	2 28.991053000	10.2.5.193	10.2.20.73	FTP	108 Response: 220 3Com 3CDaemon FTP Server Version 2.0
	5 28.992201000 5 28.992302000	10.2.20.73	10.2.5.193	FTP	76 Request: USER 123 76 [TCP Retransmission] Request: USER 123
	3 28,993908000	10.2.5.193	10.2.20.73	ETP	76 [[CP Retrainsmission] Request: USER 123 99 Response: 331 User name ok, need password
	28,993908000	10.2.5.193	10.2.20.73	FTP	99 Response: 331 User name ok, need password 99 TrcP. Retransmission] Response: 331 User name ok, need password
	28,994857000	10.2.20.73	10, 2, 5, 193	ETP	78 Request: PASS admin Response: 331 User Hame ok, Heed password
	2 28,994966000	10.2.20.73	10.2.5.193	FTP	78 TCCP Retransmission] Request: PASS admin
	5 28,995764000	10.2.5.193	10, 2, 20, 73	ETP	91 Response: 530 Login access denied
	5 28,996077000	10.2.5.193	10.2.20.73	ETP	91 TCP Retransmission] Response: 530 Login access denied
	7 28,996878000	10, 2, 20, 73	10, 2, 5, 193	ETP	82 Request: USER anonymous
323	8 28,996979000	10.2.20.73	10.2.5.193	FTP	82 [TCP_Retransmission] Request: USER anonymous
	28,997855000	10, 2, 5, 193	10, 2, 20, 73	ETP	99 Response: 331 User name ok, need password
3242	2 28,998113000	10.2.5.193	10.2.20.73	FTP	99 [TCP Retransmission] Response: 331 User name ok, need password
	1 28.998745000	10.2.20.73	10.2.5.193	FTP	73 Request: PASS
3248	8 29.000393000	10.2.5.193	10.2.20.73	FTP	101 Response: 230-The response '' is not valid.
	9 29.000715000	10.2.5.193	10.2.20.73	FTP	101 [TCP Retransmission] Response: 230-The response '' is not valid.
	3 29.035465000	10.2.5.193	10.2.20.73	FTP	145 Response: 230-Next time, please use your email address as password.
	5 29.035867000	10.2.5.193	10.2.20.73	FTP	145 [TCP Retransmission] Response: 230-Next time, please use your email address as password.
	8 29.037118000	10.2.20.73	10.2.5.193	FTP	74 Request: TYPE I
	9 29.037213000	10.2.20.73	10.2.5.193	FTP	74 [TCP Retransmission] Request: TYPE I
	2 29.038460000	10.2.5.193	10.2.20.73	FTP	86 Response: 200 Type set to I.
	3 29.038702000	10.2.5.193	10.2.20.73	FTP	86 [TCP Retransmission] Response: 200 Type set to I.
	29.039357000	10.2.20.73	10.2.5.193	FTP	72 Request: PASV
	8 29.040715000 9 29.041000000	10.2.5.193	10.2.20.73	FTP	114 Response: 227 Entering passive mode (10,2,5,193,211,172) 114 [TCP Retransmission] Response: 227 Entering passive mode (10,2,5,193,211,172)
	9 29.041000000 9 29.054116000	10.2.20.73	10.2.5.193	FTP	114 [TCP Ketransmission] Kesponse: 227 Entering passive mode (10,2,5,193,211,172) 80 Request SIZE sig.cfo
	3 29.054116000 3 29.054212000	10.2.20.73	10.2.5.193	FTP	80 Request: SIZE STD.CTg 80 [TCP Retransmission] Request: SIZE sip.ctg
	3 29.055169000	10.2.5.193	10.2.20.73	ETP	75 Response: 213 579

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

Ele E	Edit <u>V</u> iew <u>G</u> o <u>C</u> aptu	ire Analyze Statistics	Telephony Tools Internals	Help					
		🗋 🗶 😥 🔍 🍬	🔹 🐢 🐺 生 🗐 🖼		🖭   🔐 🔟 🕵 쑳	( <b>M</b>			
	2 💻 🛤 🙉 i 🖂	- 60 H - 7 7	* • • • <b>•</b> •	444		25			
Filter:	http		<ul> <li>Expre</li> </ul>	ession Clear	Apply Save				
No.	Time	Source	Destination	Protocol	Length Info				
	33 1.962425000	10.2.5.193	10.2.20.73	HTTP	1882 POST /se	rvlet?p=settings-autop&g-	-write&now=true HTTP/	1.1 (application/x-	www-form-urlencoded
14	41 2.267524000	10.2.20.73	10.2.5.193	HTTP	234 GET /HTT	P%20Directory/00156574b10	6e.boot HTTP/1.1		
	42 2.26//50000	10.2.20./3	10.2.5.193	нттр		ransmission] GET /HTTP%20		6e.boot HTTP/1.1	
	49 2.270563000	10.2.5.193	10.2.20.73	HTTP		404 Not Found (text/htm			
1	82 2.305531000	10.2.20.73	10.2.5.193	HTTP	235 GET /HTT	P%20Directory/y000000000	000.boot HTTP/1.1		
	83 2.305723000	10.2.20.73	10.2.5.193	нттр		ransmissionJ GET /HTTP%20		000.boot HTTP/1.1	
	03 2.321164000	10.2.5.193	10.2.20.73	HTTP		200 OK (application/oct			
	79 2.359293000	10.2.5.193	10.2.20.73	HTTP		define.js?44.81.254.71 HT			
	97 2.373167000	10.2.20.73	10.2.5.193	нттр		vious segment not capture	ed] Continuation or n	on-HTTP traffic	
	98 2.374421000	10.2.20.73	10.2.5.193	HTTP		tion or non-HTTP traffic			
	04 2.376198000	10.2.20.73	10.2.5.193	HTTP		tion or non-HTTP traffic			
	08 2.377011000	10.2.5.193	10.2.20.73	HTTP		aes.js?44.81.254.71 HTTP)			
	16 2.380821000	10.2.5.193	10.2.20.73	HTTP		zeropadding-min.js?44.81.			
	17 2.380973000	10.2.5.193	10.2.20.73	HTTP		jsbn.js?44.81.254.71 HTTF			
	18 2.381075000	10.2.5.193	10.2.20.73	HTTP		prng4.js?44.81.254.71 HT			
	19 2.381175000	10.2.5.193	10.2.20.73	HTTP		rng.js?44.81.254.71 HTTP)			
	20 2.381293000	10.2.5.193	10.2.20.73	HTTP		rsa.is?44.81.254.71 HTTP			
	98 2.408422000	10.2.20.73	10.2.5.193	HTTP		P%20Directory/sip.cfg HT			
	99 2.408639000	10.2.20.73	10.2.5.193	HTTP		ransmission] GET /HTTP%20		TP/1.1	
	13 2.412543000	10.2.5.193	10.2.20.73	HTTP		404 Not Found (text/htm			
	64 2.442529000	10.2.20.73	10.2.5.193	HTTP		P%20Directory/features.cf			
	65 2.442725000	10.2.20.73	10.2.5.193	HTTP		ransmission] GET /HTTP%20		fg нттр/1.1	
	70 2.455300000	10.2.5.193	10.2.20.73	HTTP		200 OK (application/oct			
	80 2.458812000	10.2.5.193	106.120.188.46	HTTP		h=A36B528EBBE894F17A1F12E		.2.5.17503 HTTP/1.1	(application/x-www
	91 2.508429000	10.2.5.193	10.2.20.73	HTTP		e/1.English_note.xml HTTF			
	92 2.509486000	10.2.5.193	10.2.20.73	HTTP		ransmission] GET /note/1.	.English_note.xml HTT	P/1.1	
	07 2.558874000	106.120.188.46	10.2.5.193	HTTP		200 OK (text/plain)			
50	09 2.643723000	10.2.5.193	36.110.147.36	HTTP	1433 GET /web	search/features/yun6.jsp	pid=sogou-brse-d2a45?	2edff079ca6&w=1440&v	=7400&st=1468309421

# **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 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 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 no 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 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 *Yealink\_SIP-T2\_Series\_T19(P) E2\_T4\_Series\_IP\_Phones\_Administrator\_Guide\_V81*, *Yealink IP DECT Phone Administrator Guide\_V81* or *Yealink\_SIP-T5\_Series\_Smart\_Media\_Phones\_Administrator\_Guide*.

# Glossary

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

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

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

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

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

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

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

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

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

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

# **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 (e.g., 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:

How to Register	<b>—</b> X—
In an effort to reduce the number of emails I get that ask me "How do I register?", I'd just like to note that you can find this information by opening the "Help" menu, and selecting the option "Registering".	ОК
So that you don't think this is a nag, I've given you the option to disable this dialog below, but please only do that if you feel you can remember how to register.	
Okay, I understand that - don't show me this dialog again.	

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

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

E:\desktop\1.FTP - WFTPD		
File Edit View Logging	Messages Security Help	
# -001] 2015/3/20 17:39:16 # -001] 2015/3/20 17:39:16	Welcome to WFTPD - we are listening to all unused IP adding the first address assigned to your system is 127.0.0.1 But you might be reached at a number of other addresses Check with your network administrators for the address the WFTPD is listening on port 21, standard ftp Program will be killed by WM_ENDSESSION message Unregistered version - for instructions on registering,	
# -001] 2015/3/20 17:39:16	select the "Registering" option from the "Help" menu.	
<b>(#</b> -001) 2015/3/20 17:39:16	select the "Registering" option from the "Heip" menu.	,

#### 4. Click Security->Users/rights.

E:\desktop\1.FTP - WFTPD		
File Edit View Logging Messages	Security Help	
[#-001] 2015/3/20 17:39:16 Welcome [#-001] 2015/3/20 17:39:16 The first 4 #-001] 2015/3/20 17:39:16 But you n [#-001] 2015/3/20 17:39:16 Check wit [#-001] 2015/3/20 17:39:16 WFTPD is #-001] 2015/3/20 17:39:16 Unregiste [#-001] 2015/3/20 17:39:16 select the	Users/rights Host/net s listening on port 21, stand will be killed by WM_ENDSI rred version - for instruction	ESSIÓN message s on registering,
< <u> </u>		•

5. Click New User.

User / Rights Se	curity Dialog	×
User Name: User default	default Done	]
New User	Delete         Change Pass           Restrict to home directory and below	
Home [	Browse	]
Help	Rig	hts >>

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

User / Rigi	nts Securit	y Dialog					8
User Name User defau		default r	•	-	Done		
New Us	User Name	: test1		0 Car He	ncel	1	
He	elp				F	Rights :	>>>

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

User / Rigł	hts Security Dialog	23
User Name ⊢User test1	Change Password	
New Us	New Password: Concel	
Home		
He	elp	Rights >>

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

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

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

**10.** Check the check boxes of **Read**, **Create Files/Dirs**, **List Directories** and **Overwrite/Delete** to make sure the FTP user has the read and write permission.

User / Rights Se	ecurity Dialog		×
User Name: User test1	test1	•	Done
New User	Delete Restrict to ho	Change Pass me directory and below	
Home	E:\DESKTOP\C	ONFIGURATION FILE	Browse
Help Rights for user te	st1		Rights<<
Directory: ×		▼ Browse	e Remove
Rights fo	r directory *		
🔽 Rea	Ь	☑ Create Files/Dirs	3
☑ List I	Directories	🔽 Overwrite/Delete	e

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 (e.g., 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.

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

Administrators (VANSTD80	)\Admini:	strators)		^
🕵 Everyone				
🕵 Hill, James (jahill@myserv	ername.	com]		
SYSTEM				~
<			>	
	A	.dd	Bemov	e
Permissions for Everyone	-	Allow	Deny	
Full Control				^
Modify		~		
Read & Execute		~		
List Folder Contents		~		
Read				
Write				
Consist Permissions				~
For special permissions or for ad- click Advanced.	vanced	settings,	Advance	d

# **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	
🛃 Menu   📅 Port: 8080   🎎 You are in Expert mode	N2.	
© Open in browser http://10.2.11.101:8080/		
		peed: 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	8080/ Top speed.0.0 KE/s
Start/Exit  Virtual File System Limits Flash taskbutton Fingerprints Tray icons	stem Log 17:23:24 Check update: no new version
IP address     ▶       Accept connections on     ▶       Dynamic DNS updater     ▶       URL encoding     ▶       Updates     ▶       ❤ Donate!	This IP address is used only for URL building 192.168.147.1 192.168.172.1  102.111.01 Custom
<ul> <li>➢ Load file system Ctrl+O</li> <li>Gave 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	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 System	Log
Port     Specify a port to accept connection,     or leave empty to decide automatically.     8088     OK Cancel	17:23:24 Check update: no new version
VIP Tiename	Status Speed Time left %
Connections: 0 Out: 0.0 KB/s In: 0.0 KB/s Total Out: 0 B Tot	*

**3.** Right click the ficon 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/		
	To	op speed: 0,0 KB/s
Virtual File System Log		
Add files		
E 🖉 Add folder from disk		
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		
<ul> <li>✓ Browsable</li> <li>✓ Archivable</li> </ul>		
Archivable		
tabled? ■ Why is upload disabled?		
Hide tree		
Auto-hide 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 a	re in Easy mode				
🖉 Open in browser http://10.2.11.1	01:8088/ProvisioningDir/			Already i	n clipboard
Virtual File System		Log			
폜 IP address	🗖 File	Status	Speed	Time	Progress
Out: 0.0 KB/s In: 0.0 KB/s					

- Check the server URL (e.g., http://10.2.11.101:8088/ProvisioningDir) by clicking "Open in browser".
- (Optional.) Right click the root directory name (e.g., 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 request	ted user/pass	×
Username		]
Password Re-type password	*****	
		eset

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

# **Configuring a DHCP Server**

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

# **Configuring the DHCP Turbo**

Before configuring the DHCP Turbo, make sure:

- The firewall on the PC is disabled.
- There is no DHCP server in your local system.

#### To configure the DHCP Turbo:

- 1. To start the DHCP Turbo application, double click localhost.
- 2. Click the Login button (the login password is blank) to log in.

BHCP Turbo on localhost	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> indings <u>T</u> ools <u>H</u> elp	
■ オ N ■ 図 ※ ウ マ 多 N?	
Server Se	
Ready.	/

- 3. Right click Scopes and select New Scope.
- **4.** Configure the DHCP server name, the DHCP IP range and the subnet mask.

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

State DHCP Turbo on localhost (modified)	
<u>File Edit View Bindings Tools H</u> elp	
Bervers Berve	™ S K?
Obtabase     Mr Exclusions     Global     Option Types     Scopes     Scopes     Unlimited     Degr Hours     O    S     S	Address Range Start address [182:108:00:10] End address [192:108:01:00 Subset of the second sec
	QK

**6.** You can add a custom option via DHCP Turbo. Select **Option Types**, right click one of the options on the right of the main page, and then select **New Option Type**.

	*	۵ 🖿		* 5	0	9	₩?					
ers 🗸		Filter	Standard	Options					•			
localhost Databa		Tag V		Opti								 
					cookie							_
±- 🔂 Named					director	v						
Dotior				Har dw	are add	ress type					L	
						ress leng	th		New Option Type	Ctrl+V		
🛃 оно	PServer			Boot Pad	file			Ð	<u>U</u> ndo	Ctrl+Z		
					t mask			0	Redo	Ctrl+V		
					offset				-			
				Gatew	ays			r	Cu <u>t</u>	Ctrl+X		
					servers			D	Copy	Ctrl+C		
					6 name : n name :				Paste	Ctrl+V		
					n name : ervers	servers		Ξ.	-			
						servers		-	Delete	Del		
					ervers				Select <u>A</u> ll	Ctrl+A		
					22 Serv	ers		<u>نې</u>	Find	Ctrl+F	1	
				KLP s Hostr	ervers			h- V				
		-47 13			ame file si:	ze		R	Properties	Ctrl+P		
					dump f:			_				
			;	Domai	n name							
		🚛 16			servers							
				Root								
					sions p rwardin;							
						∍ mce rout	ing					
							0					
		Descript	ion									
	<b>&gt;</b>		es a devi	ce's hardw	are addr	ess type						

Set the custom DHCP option (custom DHCP option tag number ranges from 128 to 254) and select the option type (Yealink supports string and ipaddress option types only). Click the OK button to finish setting the option properties. Click to save the an end of the setting the option properties.

BDHCP Turbo on localhost	_ 🗆 🗙
<u>F</u> ile <u>E</u> dit <u>Y</u> iew <u>B</u> indings <u>T</u> ools <u>H</u> elp	
Servers	

**8.** Click **Named Policies**-->**Global**, right click the blank area on the right of the main page and then select **New Option**.

🔹 DHCP Turbo on localhost (modified)		
<u>File Edit View Bindings Tools H</u> elp		
4 🖉 🧚 🐚 🗎 😣	* • • 5	N?
Servers V Tag V	Name	Value
	图 New Option Ctrl+V	1
	🔊 Undo 🗟 Ctrl+Z	
	Redo Ctrl+Y	
	P Cu <u>t</u> Ctrl+X	
C	Copy Ctrl+C	
1	Paste Ctrl+V	
	<u>x</u> <u>D</u> elete Del	
	Select <u>A</u> ll Ctrl+A	
	💐 Eind Ctrl+F	
	Properties Ctrl+P	
Add a new option to this policy		

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

DHCP Turbo on localhost (mod						
<u>File Edit View Bindings T</u> ools	<u>H</u> elp					
	🖌 🔀	Ø 🕅	S N?			
Servers Tag		Name		Value		
- Iocalhost	🕂 Option Sele	ctor			? ×	
Database 	Filter Tag Tag 47	Standard O Name NBT scope	ptions	•	<b>_</b> _	
	<b>42</b> 48 <b>42</b> 49 <b>42</b> 51 <b>42</b> 58	X Window sy	vstem font servers vstem display managers ss lease time d time			
	<u>4</u> 259 <u>42</u> 64 <u>42</u> 65 <u>42</u> 68	DHCP rebind NIS+ domain NIS+ server Mobile IP h	s s			
	<u>45</u> 69 <u>45</u> 70 <u>45</u> 71	SMTP server POP3 server NNTP server	2.			
	<b>42</b> 72 <b>42</b> 73 <b>42</b> 74	WWW servers Finger serv IRC servers	vers			
		Streettalk Streettalk User class				
	<u>4</u> € 120 	SIP Server	lie Configuration			
		TFTPServer				
	🗄 - 🚝 177	Legacy Pack	cetCable		-	
	Description				<u>\$</u>	
4 Þ]				ŪK	Çancel	

- **10.** Fill the provisioning server address in the input field.
- 11. Click the **OK** button to finish setting a custom option.

n DHCP Turbo on localhost	t (modified)				 x
<u>File Edit View B</u> indings	<u>T</u> ools <u>H</u> elp				
/ 🖉 🔺 🖉	B 💼 🔀	* 50	9	<b>k</b> ?	
	Tag V	Nane TFTPServer ItEty://192.166. Zxpression OK		Velue	

**12.** Click **are the change**.

# Add the Option 66 via DHCP Turbo

You can add the option 66 via DHCP Turbo. The following shows the detailed processes.

1. Click **Named Policies**-->**Global**, right click the blank area on the right of the main page and then select **New Option**.

BHCP Turbo on localho			- 1.0	<i>a</i>	
		503	<b>ħ</b> ?		
Servers 🗸	Tag $\nabla$	Name		Value	
Iocalhost     Ottabase     Ottabase	J28	Cut	Ctrl+V           Ctrl+Z           Ctrl+Y           Ctrl+X           Ctrl+C           Ctrl+V	tftp://192.168.1.100/	
			Del Ctrl+A		
			Ctrl+F		
		-	Ctrl+P		
4					
Add a new option to this	policy				

- 2. Select TFTP Options from the pull-down list of Filter.
- 3. Scroll down and double click **MS option 66**.

DHCP Turbo on localho					
<u>File Edit View Bindings</u>	s <u>T</u> ools <u>H</u> elp		1		
🛯 🖉 🥻 🕈		€ 5 C	<b>h</b> ?		
Servers 🗸	Tag 🗸	Name		Value	
⊡-⊒localhost ⊙Database	🖅 128 🛃 Option Sele	ector		? ×	
	Filter	TFTP Options	•		
- 🛃 Global	Tag $\nabla$	Name			
Option Types	-42-20 -42-16	Server name MS option 67			
DHCPServer	-42-15	MS option 66			
		Next server Boot file			
		boot life			
	Description			5	
	The host nam	e of a TFTP server the	device should use dump:		
	its boot pro	ocess. Unless you know	your device requires th	is option, you should use o define the TFTP server.	
<u>۱</u>				<u>OK</u> <u>C</u> ancel	

4. Fill the provisioning server IP address in the input field.

State DHCP Turbo on localhost		
<u>File Edit View B</u> indings		
	■ ■ ※ ♡ ♡ § k?	
Servers 🛆	Tag 🗸 Name Value	
- I localhost - B Scopes - B dhcp - Option Types - Named Policies - C Global - WhW Exclusions - Database	Image: 128       TFTFServer       tftp://192.168.1         Image: 128       Image: 128       Image: 128         Image: 128       Image: 128       Image: 128	. 100/
		11.

- 5. Click the **OK** button to finish setting a custom option.
- 6. Click 🔄 to save the change.

# Add the Option 43 via DHCP Turbo

You can also add the option 43. The following shows the detailed processes.

- 1. Click **Named Policies**-->**Global**, right click the blank area on the right of the main page and then select **New Option**.
- 2. Select the Standard Options from the pull-down list of Filter.

3. Scroll down and double click 43.

n DHCP Turbo on localhost		<b>– –</b> X
<u>File E</u> dit <u>V</u> iew <u>B</u> indings <u>T</u>	iools. Help	
4 🖉 🤾 א	🖺 🗶 🕫 ભ⊂ 🚱 k?	
Servers V	ag V Name Value	
Ilocalhost	1 Option Selector	
- Database		
- MW Exclusions	Filter Standard Options	
- Named Policies	Filter Standard Options	
- Clobal	Tag 🗸 Name	
-Option Types	24 Path MTU aging timeout	
Scopes		
DHCPServer	All subnets are local	
Bonniberter	-4228 Broadcast address	
	AE 38 TCP keepalive interval	
	-4339 TCP keepalive interval	
	41 NIS servers	
	-43 Vendor specific info	
	Description 😽	
	Used by devices and servers to exchange vendor-specific information.	
۲ ( )	<u>OK</u> <u>Cancel</u>	

4. Fill the provisioning server address in the input field.

Su DHCP Turbo on localhost <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> indings ∶		
	■ ■ ☆ ♡ ♡ § №?	
Servers / Servers / Scopes	Tag       Name       Value         #128       TFTFServer       tftp://19         #15       MS option 66       192.168.1         # Vendor specific info       P         [http://192.168.1.100/       Puild         QK       Cancel	
		hi

- 5. Click the **OK** button to finish setting a custom option.
- 6. Click 🔊 to save the change.

# **Customer Feedback**

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