

SIP-T2 Series/T19(P) E2/T4 Series IP Phones Auto Provisioning Guide

Version 81.20 Nov. 2016

Table of Contents

Table of Contents	iii
Introduction	1
Getting Started	3
Obtaining the Boot File	3
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	
Obtaining the Provisioning Server Address	25
Zero Touch	
Plug and Play (PnP) Server	
DHCP Options	

Phone Flash	
Configuring Wildcard of the Provisioning Server URL	

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	
Configuring an FTP Server	
Configuring an HTTP Server	54
Preparing a Root Directory	
Configuring an HTTP Server	
Configuring a DHCP Server	
Configuring the DHCP Turbo	
Add the Option 66 via DHCP Turbo	
Add the Option 43 via DHCP Turbo	

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

The auto provisioning process outlined in this guide applies to Yealink SIPT48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T29G/T27P/T27G/T23P/T23G/ T21(P) E2/T19(P) E2 IP phones running firmware version 81 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

Yealink IP phones running firmware version 81 or later support a new boot file in which you can 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 (y00000000000.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.

		IP Phone SIP-T23G
	L	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	Release 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

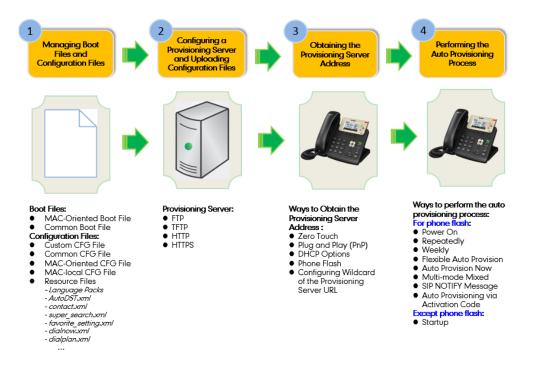


Provisioning Server

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).



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

300 3CDaemon					
<u>File View H</u> elp					
TFTP Server	Start Time	Peer	Bytes	Status	
Configure IFIF Server	Jul 12, 2016 09:30:13	local	0	Listening for TFTP requests on IP address: 10.2.5.193 Port 69	
IFTP Server is started.				server URL where the IP phone	
Click here to stop it.				vnloads boot files and configuration	
			files	s from is tftp://10.2.5.193/	
Logging to Tftpd log. Click to stop.					
X					
Not debugging. Click to start.					
Clear list.					
Clear list.					
View Log/Debug files.					

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

... utton to locate the TFTP root directory

300 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 TFTP Server	3CDaemon Configurat			
	FTP Profil			Syslog Configuration
5TOP	General Con	figura	tion	TFTP Configuration
TFTP Server is started. Click here to stop it.	Create directory n	ames in	n incomi	ng file re <mark>v</mark>
	Allow overwrite of	existi	ing file	s?
Logging to Tftpd.log. Click to stop.	Upload/Download	Ī	D:\TFTP	Directory\
	Per-packet timeout	in sec	onds	5
Not debugging. Click to start.	Maximum retries			10
Clear list.	Interframe transmis	ssion		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.

ealink 1236	Status	Account	Network	DSSKey	Features	Settings	Director	ry Security
Preference	,	Auto Provision					NOTE	
Time & Date		PNP Active DHCP Active		 On Off On Off 			Auto Pro	ovision hone can interoperate
Call Display	(Custom Option(128-	~254)					visioning server using
Upgrade	(DHCP Option Value				_	the IP ph	iones.
Auto Provision	5	Server URL		tftp://10.2.5.193/			perform a	e IP phone triggers to auto provisioning, it wi
Configuration		User Name			1			tion files from the
	ţ	Password			Ente	r the access	URI of	o server. During the oning process, the
Dial Plan	, d	Attempt Expired Tim	ne(s)	5	the p	rovisioning s	erver in	ill download and figuration files to th
Voice	(Common AES Key		•••••		Server URL		·
Ring	1	MAC-Oriented AES K	iey	•••••				an click here to get
	2	Zero Active		Disabled	*		more gui	ides.
Tones	1	Wait Time(1~100s)		5				
Softkey Layout		Power On		● On ◎ 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	ish(English) +	
	CMIIIIK 11236	Status	Account	Network	DSSKey	Features	Settings	Directory	Security	
I	Preference		Auto Provision					NOTE	•	
			PNP Active		🖲 On 🔘 Off			100000000		Γ.
	Time & Date		DHCP Active		🔹 On 🔘 Off			Auto Provision The IP phone	can interoperate	
	Call Display		Custom Option(12	8~254)					ng server using ng for deploying	
	Upgrade		DHCP Option Value					the IP phones		
ſ	Auto Provision		Server URL		tftp://10.2.5.193/				ohone triggers to provisioning, it will	
	Auto Provision		User Name					request to do configuration f	wnload the	
	Configuration		Password					provisioning se	rver. During the	
	Dial Plan		Attempt Expired T	ime(s)	5			IP phone will d		
	Voice		Common AES Key					update config phone flash.	aration files to the	
	and the second se		MAC-Oriented AES	Key				D You can d	ick here to get	
	Ring		Zero Active		Deabled	-		more guides.	in the e wyer	
	Tones		Walt Time(1~100s	0	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 In	terval(0~12week)	4					
			Inactivity Time Exp	pire(0~120min)	0					
			Time		00 : 00 - 00	: 00				
			Day of Week		 ✓ Sunday ✓ Monday ✓ Tuesday ✓ Wednesday ✓ Thursday ✓ Friday ✓ Friday ✓ Saturday 	perfor	m the au	rovision No to provisio	ning	
			Flexible Auto Prove	sion	🗢 on 💌 off	pr	rocess im	mediately.		
			Flexible Interval Da	ys	30	7		-		
			Flexible Time		02 : 00 -					
			Cor	nferm	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.*

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-T48S/T46S/T42S/T41S	y0000000066.cfg
SIP-T48G	y0000000035.cfg
SIP-T46G	y0000000028.cfg
SIP-T42G	y0000000029.cfg
SIP-T41P	y0000000036.cfg
SIP-T40P	Y0000000054.cfg
SIP-T29G	y0000000046.cfg
SIP-T27P	y0000000045.cfg
SIP-T27G	y0000000069.cfg
SIP-T23P/G	y00000000044.cfg
SIP-T21(P) E2	y0000000052.cfg
SIP-T19(P) E2	y0000000053.cfg

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

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:

#!version:1.0.0.1
**File header "#!version:1.0.0.1" can not be edited or deleted, and must be placed in the first line.##
##This template file is applicable to IP phones running firmware version 81 or later.##
##For more information on configuration parameters, refer to Description of Configuration Parameters in CFG Files.xlsx.##
Hostname
static.network.dhcp host name =

Network Advanced

##It enables or disables the PC port.0-Disabled,1-Auto Negotiation.
##The default value is 1.It takes effect after a reboot.
<pre>static.network.pc_port.enable =</pre>
##It configures the transmission mode and speed of the Internet (WAN) port.
##0-Auto Negotiate
##1-Full Duplex 10Mbps
##2-Full Duplex 100Mbps
##3-Half Duplex 10Mbps
##4-Half Duplex 100Mbps
##5-Full Duplex 1000Mbps (only applicable to SIP-T48G/T46G/T46G/T42G/T29G/T23G/CP860 IP phones)
##The default value is 0.It takes effect after a reboot.
static.network.internet_port.speed_duplex =
to configures the transmission mode and speed of the PC (LAN) port.
##0-Auto Negotiate
##1-Full Duplex 10Mbps
##2-Full Duplex 100Mbps

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
<pre>##File header "#!version:1.0.0.1" can not be edited or deleted, and must be placed in the first line.##</pre>
##This template file is applicable to IP phones running firmware version 81 or later.##
##For more information on configuration parameters, refer to Description of Configuration Parameters in CFG Files.xslx##
Accountl Basic Settings

account.1.enable =
account.1.label =
account.1.display_name =
account.1.auth_name =
account.1.user_name =
account.1.password =
account.1.outbound proxy enable =
account.1.outbound host =
account.1.outbound port =
account.1.dial tone =
_
##It configures the transport type for account 1. 0-UDP,1-TCP,2-TLS,3-DNS-NAPTR
##The default value is 0.
account.1.sip server.1.transport type =
account.1.sip server.2.transport type =
Failback
account.1.naptr build =
account.1.fallback.redundancy type =
account.1.fallback.timeout =
account.1.sip server.1.address =

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-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, SIP-T40P/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 16.

2. Copy configuration parameters from the template configuration files and set the valid values for them.

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*.

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*.

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
Language Packs	For example, 000.GUI.English.lang 1.English_note.xml 1.English.js
Replace Rule	dialplan.xml
Dial-now	dialnow.xml
Softkey Layout	CallFailed.xml CallIn.xml Connecting.xml Dialing.xml (not applicable to SIP-T48G/S IP phones) RingBack.xml Talking.xml
Directory	favorite_setting.xml
Super Search in dialing	super_search.xml
Local Contact File	contact.xml
Remote XML Phone Book	Department.xml Menu.xml
Ring Tone	None
Logo customization	None
Wallpaper	None

Feature	Template File Name
	X.81.0.XX.rom
Firmware	For example,
	44.81.0.15.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*.

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		strators)	
Everyone			
🖸 Hill, James (jahill@m	yservername.	.com]	
SYSTEM			5
<			>
	4	\dd	Remove
Permissions for Everyone		Allow	Deny
Full Control			
Modify		~	
Read & Execute		~	
List Folder Contents		~	
Read		~	
Write		~	
Consist Dormissions		(F)	
or special permissions or	for 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:

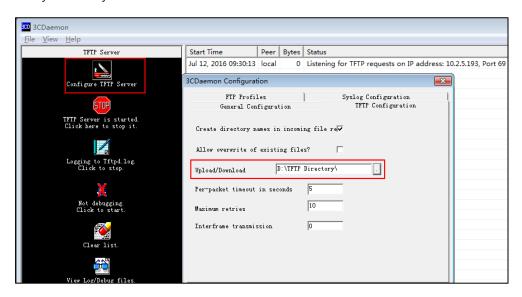
1. Double click **3CDaemon.exe** to start the application.

A configuration page is shown as below:

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

2. Select **Configure TFTP Server**. Click the 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.

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.
- Enter the desired wait time in the Wait Time(1~100s) field.
 The default value is 5.

Yealink 17236				Log Out English(English) 🔻		
	Status Account Networ	k DSSKey Features	Settings	Directory Security		
Preference	Auto Provision			NOTE		
Time & Date	PNP Active DHCP Active	 On Off On Off 		Auto Provision The IP phone can interoperate		
Call Display	Custom Option(128~254)	admin		with provisioning server using 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 Password	•••••		configuration files from the provisioning server. During the auto provisioning process, the IP phone will download and update configuration files to the phone flash.		
Dial Plan	Attempt Expired Time(s)	5				
Voice	Common AES Key	•••••		You can click here to get		
Ring	MAC-Oriented AES Key	•••••		more guides.		
Tones	Zero Active	Enabled 🔻				
Softkey Layout	Wait Time(1~100s)	5				
Sourcey Layout	Power On	🖲 On 🔍 Off				
TR069	Repeatedly	🔍 On 🖲 Off				

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.

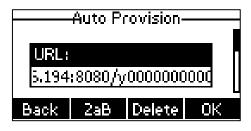
The network parameters are configurable via phone user interface:

Network					
IP Me	ode:				
IPv4	ŀ		41		
Back		Switch	Ne:	_ xt	

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:

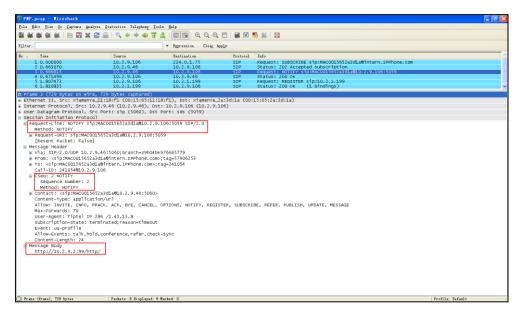
1. Click on Settings->Auto Provision.

Call Display Upgrade Auto Provision	Auto Provision PNP Active DHCP Active Custom Option(128 DHCP Option Value Server URL	~254)	On Off On Off on Off admin yealnk			NOTE Auto Provision The IP phone can interoperate with provisioning server using auto provisioning for deploying the IP phones.	
Time & Date Call Display Upgrade Auto Provision Configuration	DHCP Active Custom Option(128- DHCP Option Value Server URL	~254)	On Off admin			The IP phone can interoperate with provsioning server using auto provisioning for deploying	
Call Display Upgrade Auto Provision	Custom Option(128- DHCP Option Value Server URL	~254)	admin			The IP phone can interoperate with provsioning server using auto provisioning for deploying	
Upgrade Auto Provision	DHCP Option Value	~254)				auto provisioning for deploying	
Auto Provision	Server URL		yealink				
						When the IP phone triggers to	
Configuration						perform auto provisioning, it wi request to download the	
	User Name	User Name Password			configuration files from the provisioning server. During the		
Connguration	Password			1.11	3	auto provisioning process, the IP phone will download and	
Dial Plan	Attempt Expired Time(s)		5		update configuration files to th phone flash.		
Voice	Common AES Key		•••••	<u></u>		You can click here to get	
Ring	MAC-Oriented AES Key		•••••			more guides.	
5	Zero Active		Enabled	•			
Tones	Wait Time(1~100s)		5				
Softkey Layout	Power On		● On ○ Off				
TR069	Repeatedly		🔍 On 🖲 Off				
Voice Monitoring	Interval(Minutes)		1440				
SIP	Weekly		○ On ● Off				
51P	Weekly Upgrade Int	erval(0~12week)	4				

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		● On ○ Off	_		Auto Provisio	
Call Display	-	HCP Active ustom Option(128~	254)	On Off 128			with provsionin auto provisionin	ng for deploying
Upgrade	D	HCP Option Value		yealink			the IP phones. When the IP n	hone triggers to
Auto Provision	S	erver URL					perform auto p request to dov	vrovisioning, it will vnload the
Configuration	U	ser Name					configuration fi provisioning ser auto provisionir	rver. During the
Dial Plan		assword		••••			IP phone will d update configu	ownload and iration files to the
Dian Fian	A	ttempt Expired Tim	e(s)	5			phone flash.	
Voice	C	ommon AES Key		•••••				ck here to get
Ring	MAC-Oriented AES		еу	•••••	1000 m		more guides.	
Tones	Z	ero Active		Enabled	Ŧ			
	W	/ait Time(1~100s)		5				
Softkey Layout	P	ower On		🖲 On 🔍 Off				
TR069	R	epeatedly		🔾 On 🖲 Off				
Voice Monitoring	In	nterval(Minutes)		1440				
SIP	W	/eekly		🔾 On 🖲 Off				
SIF	W	/eekly Upgrade Inte	erval(0~12week)	4				
	In	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*. The following figure shows the example messages of obtaining the TFTP server address from a custom DHCP option:

UHCPserver-tftp.pcap [Wireshark 1.6		
<u>File Edit View Go Capture Analyze</u>	<u>S</u> tatistics Telephony <u>T</u> ools Internals <u>H</u> elp	
en en en en en e 🛛 🛪 🕾	Q ♀ ♀ ♀ <mark>♀ <mark>♀</mark> ½ □ 🖃 </mark>	
Filter: sip bootp	Expression Clear Apply	
lo, Time Source	Destination Protocol Length Info	
14 17,967476 0.0.0.0	255,255,255,255 DHCP 590 DHCP Discover - Transaction ID 0	0x88e96872
15 18.137781 10.2.8.105	10.2.8.106 DHCP 342 DHCP Offer - Transaction ID 0	
16 18.177701 0.0.0.0	255.255.255.255 DHCP 590 DHCP Request - Transaction ID 0	
17 18.178902 10.2.8.105	10.2.8.106 DHCP 342 DHCP ACK - Transaction ID 0	0x88e96872
Buser Datagram Protocol, Src Bootstrap Protocol Message type: Boot Reply (Hardware type: Ethernet Hardware address length: 6 Hops: 0 Transaction ID: 0x88e96872 Seconds elapsed: 100 Bootp flags: 0x0000 (Unica Client IP address: 0.0.0.0 Your (client) IP address: 10 Relay agent IP address: 10 Relay agent IP address: 0. Client MAC address: xiamen Client MAC address: xiamen Client Hardware address pa Server host name: mfd0171- Boot file name not given Magic cookie: DHCP Boption: (t=1,1=4) Subnet M Boption: (t=5,1=1) DHCP Me Doption: (t=58,1=4) Renewal Option: (t=58,1=4) Renewal Doption: (t=151,1=4) IP Addr Doption: (t=12,1=4) IP Addr Doption: (t=12,1=18) DOCST	<pre>st) (0.0.0.0) 10.2.8.105 (10.2.8.105) 0.0.0 (0.0.0.0) ve_38:28:d8 (00:15:65:38:28:d8) dding: 0000000000000000000 for3xon ssage type = DHCP ACK ask = 255.255.255.0 ess Lease Time = 6 hours ng Time Value = 3 hours, 15 minutes Time Value = 3 hours, 15 minutes Time Value = 3 hours ss Lease Time = 6 hours 5 full security server IP [TODO] l security server IP [TODO] l security server IP [TODO] 02e322e382e3130352f</pre>	

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)					
Upgrade	DHCP Option Value			auto provisioning for deploying 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 the 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*.

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 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			Log Out English(English) V
	Status Account Network	DSSKey Features	Settings Directory Security
Preference	Auto Provision		NOTE
Time & Date	PNP Active	• On Off	Auto Provision
Call Display	DHCP Active Custom Option(128~254)	On Off	The IP phone can interoperate with provisioning server using auto provisioning for deploying
Upgrade	DHCP Option Value	yealink	the IP phones. When the IP phone triggers to
Auto Provision	Server URL	tftp://10.2.5.169/	perform auto provisioning, it will request to download the
Configuration	User Name		configuration files from the provisioning server. During the auto provisioning process, the
Dial Plan	Password Attempt Expired Time(s)	5	IP phone will download and update configuration files to the phone flash.
Voice	Common AES Key	•••••	You can click here to get
Ring	MAC-Oriented AES Key	•••••	more guides.
Tones	Zero Active	Enabled	
Softkey Layout	Wait Time(1~100s)	5	
Softkey Layout	Power On	🖲 On 🔍 Off	
TR069	Repeatedly	🔘 On 🖲 Off	
Voice Monitoring	Interval(Minutes)	1440	
SIP	Weekly	🔘 On 🖲 Off	
	Weekly Upgrade Interval(0~12week)	4	
	Inactivity 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.

	Status	Account	Network	DSSKev	[]	C			
Preference Time & Date	А			DSSRey	Features	Settings	Directory	Security	
Time 0 Date		uto Provision					NOTE		
Time & Date	PI	NP Active		🖲 On 🔍 Off			Auto Provisio	on	
	DI	HCP Active		🖲 On 🔍 Off			The IP phone with provisionin		
Call Display	Cu	ustom Option(128~	254)	128			auto provisionir the IP phones.	ng for deploying	
Upgrade	DI	HCP Option Value		yealink			When the IP p		
Auto Provision	Server URL User Name Password			tftp://10.2.5.169/			perform auto provisioning, it will request to download the configuration files from the provisioning server. During the auto provisioning process, the IP phone will download and		
Configuration.									
Configuration					1.1	1			
Dial Plan	At	ttempt Expired Tim	e(s)	5			update configu phone flash.	ration files to t	
Voice	Co	ommon AES Key		•••••			You can cli	ick here to get	
Ring	M	AC-Oriented AES K	еу	•••••			more guides.	en nere to get	
Tones	Ze	ero Active		Enabled	¥				
	w	/ait Time(1~100s)		5					
Softkey Layout	Po	ower On		🖲 On 🔍 Off					
TR069	Re	epeatedly		🖲 On 🔍 Off					
Voice Monitoring	In	terval(Minutes)		1440					
SIP	W	/eekly		🔍 On 🖲 Off					
	w	/eekly Upgrade Inte	rval(0~12week)	4					

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 can interoperate with provisioning server using auto provisioning for deploying the IP phones.			
Call Display		Custom Option(128~	254)							
Upgrade		DHCP Option Value		yealnk						
Auto Provision		Server URL		tftp://192.168.1.1	100/		When the IP phone triggers to perform auto provisioning, it will request to download the configuration files from the			
NAMES OF TAXABLE PARTY.		User Name								
Configuration	Password						provisioning server. During the			
Dial Plan		Attempt Expired Tim	e(s)	s			auto provisioning process, the IP phone will download and update configuration files to the phone flash.			
Voice		Common AES Key								
Ring		MAC-Oriented AES K	ey				You can click here to get			
Rong	Zero Active			Enabled			in the congre			
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	Status	Account	Network	DSSKey	Features	Settings	Directory	Security
Preference		Auto Provision					NOTE	
Time & Date		PNP Active		💌 On 🗇 Off			Auto Provisi	00
		DHCP Active		🖲 On 🗇 Off			The IP phone	can interoperate
Call Display		Custom Option(128	~254)	admin			auto provision	ng server using ing for deploying
Upgrade		DHCP Option Value					the IP phones	
Auto Provision		Server URL		tftp://192.168.1.1	00/			phone triggers to provisioning, it w
and the second second		User Name					request to do configuration	
Configuration		Password					provisioning se	ever. During the ing process, the
Dial Plan		Attempt Expired Tir	me(s)	5			IP phone will a	download and
Voice		Common AES Key					phone flash.	uration files to th
-		MAC-Oriented AES	Key				B You can c	lick here to get
Ring		Zero Active		Disabled			more guides.	
Tones		Wait Time(1~100s)		5				
Softkey Layout		Power On		● On ② Off				
TR069		Repeatedly		O on 🖲 Off				
		Interval(Minutes)		1440				
Voice Monitoring		Weekly		O on . Off				
SIP		Weekly Upgrade Int	erval(0~12week)	4				
		Inactivity Time Expl	e(0~120min)	0				
		Time		00 : 00 - 00	: 00			
		Day of Week		 ✓ Sunday ✓ Monday ✓ Tuesday ✓ Wednesday ✓ Thursday ✓ Friday ✓ Friday ✓ Saturday 				
	ſ	Flexible Auto Provisi	on	🖲 On 🔘 Off				
		Flexible Interval Day	5	30				
		Flexible Time		01 : 00 - 05	: 00			
	1.1			Autoprovision	Now			

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.

ealink 1236	1	n	0		(and 1)	Settings		ish(English)
	Status	Account	Network	DSSKey	Features	Settings	Directory	Security
Preference		Auto Provision					NOTE	
Time & Date		PNP Active		🖲 On 🕐 Off			Auto Provisio	on -
	1	DHCP Active		🖲 On 🗇 Off			The IP phone	can interoperate
Call Display		Custom Option(128~	-254)	admin			with provisioning server using auto provisioning for deployin	
Upgrade	9	DHCP Option Value					the IP phones	
Auto Provision	1	Server URL		tftp://192.168.1.1	00/		perform auto p	hone triggers to provisioning, it will
Configuration	1	User Name					request to dov configuration f	
and the first sector of the	1	Password		•••••				rver. During the ng process, the
Dial Plan		Attempt Expired Tim	ne(s)	5			IP phone will d undate config	lownload and aration files to the
Voice		Common AES Key					phone flash.	
Ring		MAC-Oriented AES K	ley .					ick here to get
	4	Zero Active		Disabled			more guides.	
Tones	1	Wait Time(1~100s)		5				
Softkey Layout	3	Power On		🖲 On 🔘 Off				
TR069		Repeatedly		🔿 On 💌 Off				
Voice Monitoring	1	Interval(Minutes)		1440				
voice Provincorning	1	Weekly		🗇 On 兽 Off				
SIP		Weekly Upgrade Inte	erval(0~12week)	4				
	1	Inactivity Time Expire	e(0~120min)	0				
		Time		00 : 00 - 00	: 00			
	1	Day of Week		Sunday Monday Monday U Tuesday U Wednesday U Thursday V Friday V Friday V Saturday				
	1	Flexible Auto Provisio	n	🖲 On 🗇 Off				
	1	Flexible Interval Days		30				
	1	Flexible Time	1	01 : 00 - 06	: 00			
				Autoprovision I	low			

2. Click Autoprovision Now.

The IP phone will perform the auto provisioning process immediately.

Multi-mode Mixed

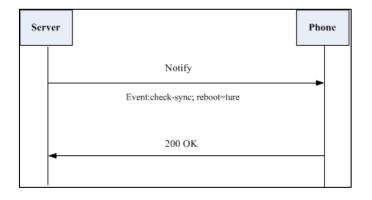
You can activate more than one method for auto provisioning. For example, you can activate the "Power On" and "Repeatedly" modes simultaneously. The IP phone will perform the auto provisioning process when it is powered on and at a specified interval.

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.

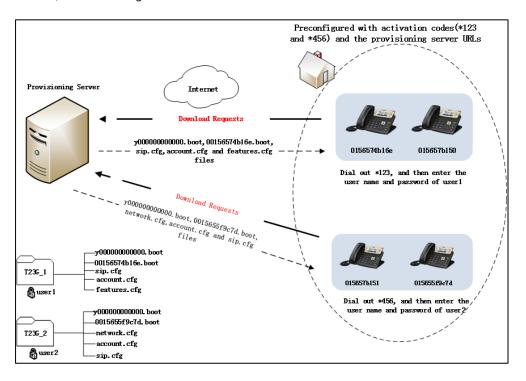
This method requires server support.

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:

autoprovision.1.code = *123

autoprovision.1.url = http://192.168.1.30/T23G_1/

autoprovision.2.code = *456

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:

No Service								
wwwwwAutoP to wwwww								
	Provision now?							
Cancel			OK					

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

The LCD screen will prompt the following input box:

^	iutoP A	uthority	
User	Name:		
Cancel	2aB	Delete	ΟK

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.

autoprovision.X.name

#Configure the activation code.

autoprovision.X.code

#Configure the URL of the provisioning server.

autoprovision.X.url

#Configure the username and password for downloading boot files and configuration files. If

configured, the LCD screen will not prompt for user name and password.

autoprovision.X.user

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.*

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.

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.

File Ed	t View Go Cantu	re Analyze Statistics	Telephony Tools Internal	k Help	
••	📕 📓 🙇 🗁	📋 🗙 🔁 🔍 🌾	· 🔅 💫 7 👱 🔲 🖻	$\Theta = \Theta$	🖭 👹 🔟 🎭 🧮
Filter: t	a		-	ession Clear	Analy Ann
ritter:	πр		Expr	ession Clear	Apply save
No.	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
	12.389499000	10.2.20.73	10.2.5.193	TETP	81 Read Request, File: 00156574b16e.boot, Transfer type: octet, b1ks12e\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
	12.410097000	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
	17.440553000	10.2.20.73	10.2.5.193	TETP	82 Read Request, File: y00000000000.boot, Transfer type: octet, b1Ks12e\000=1432\000 82 Read Request, File: y00000000000.boot, Transfer type: octet, b1Ks12e\000=1432\000
	17.462578000	10.2.5.193	10.2.3.193	TETP	57 Option Acknowledgement, blksize\000=1432\000
	17.462889000	10.2.5.193	10.2.20.73	TETP	60 Option Acknowledgement, blksize\000=1432\000
	17.464898000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 0
	17.464989000		10.2.5.193	TETP	60 Acknowledgement, Block: 0
	17.465642000	10.2.5.193	10.2.20.73	TETP	428 Data Packet, Block: 1 (last)
	17.466974000	10.2.5.193	10.2.20.73	TETP	428 Data Packet, Block: 1 (last)
	17.469270000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 1
	17.469359000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 1
	17.483306000	10.2.20.73	10.2.5.193	TETP	71 Read Request, File: sip.cfg, Transfer type: octet, blksize\000=1432\000
	17.483401000	10.2.20.73	10.2.5.193	TETP	71 Read Request, File: sip.cfg, Transfer type: octet, blksize\000=1432\000
	17.506728000	10.2.5.193	10.2.20.73	TETP	57 Option Acknowledgement, blksize\000=1432\000
	. 17.506988000	10.2.5.193	10.2.20.73	TETP	60 Option Acknowledgement, blksize\000=1432\000
	5 17.511914000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 0
	17.512005000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 0
	17.512439000	10.2.5.193	10.2.20.73	TETP	625 Data Packet, Block: 1
	17.513683000	10.2.5.193	10.2.20.73	TETP	625 Data Packet, Block: 1
	17.515113000	10.2.20.73	10.2.5.193	TETP	60 Acknowledgement, Block: 1
	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
	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.

Filter:	ftp		Expre	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
317	5 28.952342000	10.2.20.73	10.2.5.193	FTP	91 Request: RETR y0000000000.boot
	6 28.952453000	10.2.20.73	10.2.5.193	FTP	91 LTCP Retransmissionj Request: RETR y000000000000.boot
	9 28.958927000	10.2.5.193	10.2.20.73	FTP	102 Response: 125 Using existing data connection
	0 28.959253000	10.2.5.193	10.2.20.73	FTP	102 [TCP Retransmission] Response: 125 Using existing data connection
319	0 28.963510000	10.2.5.193	10.2.20.73	FTP	122 Response: 226 Closing data connection; File transfer successful.
	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	10.2.20.73	10.2.5.193	FTP	76 Request: USER 123
	6 28.992302000	10.2.20.73	10.2.5.193	FTP	76 [TCP Retransmission] Request: USER 123
	9 28.993908000	10.2.5.193	10.2.20.73	FTP	99 Response: 331 User name ok, need password
	0 28.994220000	10.2.5.193	10.2.20.73	FTP	99 [TCP Retransmission] Response: 331 User name ok, need password
	1 28.994857000	10.2.20.73	10.2.5.193	FTP	78 Request: PASS admin
	2 28.994966000	10.2.20.73	10.2.5.193	FTP	78 [TCP Retransmission] Request: PASS admin
	5 28.995764000	10.2.5.193	10.2.20.73	FTP	91 Response: 530 Login access denied
	6 28.996077000	10.2.5.193	10.2.20.73	FTP	91 [TCP Retransmission] Response: 530 Login access denied
	7 28.996878000	10.2.20.73	10.2.5.193	FTP	82 Request: USER anonymous
	8 28.996979000	10.2.20.73	10.2.5.193	FTP	82 [TCP Retransmission] Request: USER anonymous
	1 28.997855000	10.2.5.193	10.2.20.73	FTP	99 Response: 331 User name ok, need password
	2 28.998113000	10.2.5.193	10.2.20.73	FTP	99 [TCP Retransmission] Response: 331 User name ok, need password
	4 28.998745000	10.2.20.73	10.2.5.193	FTP	73 Request: PASS
	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.
	4 29.039357000	10.2.20.73	10.2.5.193	FTP	72 Request: PASV
	8 29.040715000	10.2.5.193	10.2.20.73	FTP	114 Response: 227 Entering passive mode (10,2,5,193,211,172)
	9 29.041000000	10.2.5.193	10.2.20.73	FTP	114 [TCP Retransmission] Response: 227 Entering passive mode (10,2,5,193,211,172)
	9 29.054116000	10.2.20.73	10.2.5.193	FTP	80 Request: SIZE sip.cfg
328	0 29.054212000	10.2.20.73	10.2.5.193	FTP	80 [TCP Retransmission] Request: SIZE sip.ctg

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

Ele	e <u>E</u> d	it <u>V</u> iew <u>G</u> o <u>C</u> aptur	e Analyze Statistics	Telephony Tools Internals	; <u>H</u> elp	
10				🖕 🗛 🛣 🐥 🗐 🕞		Q. 🖂 📓 🕺 🥵 % 🙀
-	~				~~~~	
File	ter: I	http		 Expression 	ession Clear	ar Apply Save
No.	_	Time	Source	Destination	Protocol	Length Info
140.		3 1, 962425000	10.2.5.193	10, 2, 20, 73	HTTP	1882 POST /servlet?p=settings-autop&g=write&now=true HTTP/1.1 (application/x-www-form-urlencoded
Г		1 2.267524000	10.2.20.73	10.2.5.193	HTTP	234 GET /HTTP%20Directory/00156574b16e, boot HTTP/1.1
Γ.	142	2 2.26//50000	10.2.20.73	10.2.5.193	нттр	234 [ICP RETRANSMISSION] GET /HITPSZUDIRECTORY/UUID05/4016e.boot HTTP/1.1
	149	9 2.270563000	10.2.5.193	10.2.20.73	HTTP	66 HTTP/1.1 404 Not Found (text/html)
Г	182	2 2.305531000	10.2.20.73	10.2.5.193	HTTP	235 GET /HTTP%20Directory/y0000000000.boot HTTP/1.1
Γ-	18	3 2.305723000	10.2.20.73	10.2.5.193	HTTP	235 [TCP Retransmission] GET /HTTP%20Directory/y00000000000.boot HTTP/1.1
		3 2.321164000	10.2.5.193	10.2.20.73	HTTP	448 HTTP/1.1 200 OK (application/octet-stream)
	279	9 2.359293000	10.2.5.193	10.2.20.73	HTTP	574 GET /js/define.js?44.81.254.71 HTTP/1.1
		7 2.373167000	10.2.20.73	10.2.5.193		1514 [TCP Previous segment not captured] Continuation or non-HTTP traffic
		8 2.374421000	10.2.20.73	10.2.5.193	HTTP	1514 Continuation or non-HTTP traffic
		4 2.376198000	10.2.20.73	10.2.5.193	HTTP	1133 Continuation or non-HTTP traffic
		8 2.377011000	10.2.5.193	10.2.20.73	HTTP	570 GET /js/aes.js?44.81.254.71 HTTP/1.1
		6 2.380821000	10.2.5.193	10.2.20.73	HTTP	581 GET /js/zeropadding-min.js?44.81.254.71 HTTP/1.1
		7 2.380973000	10.2.5.193	10.2.20.73	HTTP	571 GET /js/jsbn.js?44.81.254.71 HTTP/1.1
		8 2.381075000	10.2.5.193	10.2.20.73	HTTP	573 GET /js/prng4.js?44.81.254.71 HTTP/1.1
		9 2.381175000	10.2.5.193	10.2.20.73	HTTP	569 GET /js/rng.js?44.81.254.71 HTTP/1.1
		0 2.381293000	10.2.5.193	10.2.20.73	HTTP	569 GET /is/rsa.is?44.81.254.71 HTTP/1.1
		8 2.408422000	10.2.20.73	10.2.5.193	HTTP	224 GET /HTTP%20Directory/sip.cfg HTTP/1.1
		9 2.408639000	10.2.20.73	10.2.5.193	HTTP	224 [TCP Retransmission] GET /HTTP%20Directory/sip.cfg HTTP/1.1
		3 2.412543000	10.2.5.193	10.2.20.73	HTTP	66 HTTP/1.1 404 Not Found (text/html)
		4 2.442529000	10.2.20.73	10.2.5.193	HTTP	229 GET /HTTP%20Directory/features.cfg HTTP/1.1
		5 2.442/25000	10.2.20.73	10.2.5.193	HTTP	229 [TCP_Retransmission] GET /HTTP%20Directory/features.cfg HTTP/1.1
		0 2.455300000	10.2.5.193	10.2.20.73	HTTP	645 HTTP/1.1 200 OK (application/octet-stream)
		0 2.458812000	10.2.5.193	106.120.188.46	HTTP	1046 POST /q?h=A36B528EBBE894F17A1F12E8A58FE660&r=0000&v=5.2.5.17503 HTTP/1.1 (application/x-www
		1 2.508429000	10.2.5.193	10.2.20.73	HTTP	492 GET /note/1.English_note.xml HTTP/1.1
		2 2.509486000	10.2.5.193	10.2.20.73	HTTP	492 [TCP Retransmission] GET /note/1.English_note.xml HTTP/1.1
			106.120.188.46	10.2.5.193	HTTP	296 нттр/1.1 200 ок (text/plain)
	505	9 2.643723000	10.2.5.193	36.110.147.36	HTTP	1433 GET /websearch/features/yun6.jsp?pid=sogou-brse-d2a452edff079ca6&w=1440&v=7400&st=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*.

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:

General Sharing Security Customize	1									
Group or user names:										
🕵 Administrators (VANSTD80\Administrators)										
CREATOR OWNER										
🔢 Everyone										
📓 Hill, James (jahill@myservername	.com]									
SYSTEM		~								
		>								
	\ <u>d</u> d	<u>R</u> emove								
Permissions for Everyone	Allow	Deny								
Full Control										
Modify	~									
Read & Execute	~									
List Folder Contents	~									
Read	✓									
Write	~									
Cossial Dormissions										
For special permissions or for advanced click Advanced.	settings,	Advanced								
ОК	Cancel									

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	— 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		<u> </u>
File Edit View Logging Messa	ages Security Help	
# -001] 2015/3/20 17:39:16 The f # -001] 2015/3/20 17:39:16 But y # -001] 2015/3/20 17:39:16 Chec # -001] 2015/3/20 17:39:16 WFT # -001] 2015/3/20 17:39:16 Prog	come to WFTPD - we are listening to all unused IP addresses. first address assigned to your system is 127.0.0.1 you might be reached at a number of other addresses. k with your network administrators for the address that is reachable from the lu PD is listening on port 21, standard ftp ram will be killed by WM_ENDSESSION message gistered version - for instructions on registering,	ntern
	ct the "Registering" option from the "Help" menu.	

4. Click Security->Users/rights.

🔚 E:\desktop\1.FTP - WFTPD	
File Edit View Logging Messages Se	ecurity Help
[#-001] 2015/3/20 17:39:16 Welcome [#-001] 2015/3/20 17:39:16 The first a [#-001] 2015/3/20 17:39:16 Butyou m [#-001] 2015/3/20 17:39:16 Check witi [#-001] 2015/3/20 17:39:16 WFTPD is me [#-001] 2015/3/20 17:39:16 Porgram will	General Ig to all unused IP addresses. Users/rights vstem is 127.0.0.1 er of other addresses. er of other addresses. Host/net ors for the address that is reachable from the Internet steming on port 21, standard tip be killed by WM ENDSESSION message
	d version - for instructions on registering, Registering" option from the "Help" menu.

5. Click New User.

User / Rights Se	curity Dialog	×
User Name: User default	default	lone
New User	Delete Change Pass Restrict to home directory and below	
Home [Bro	wse
Help		Rights >>

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: Cancel	
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 Name: test1 User test1 User test1 New User Delete Change Pass Restrict to home directory and below Home E:\DESKTOP\CONFIGURATION FILE Browse Help Rights for user test1 Directory: * Rights for directory * Rights for	User / Rights Se	curity Dialog				×
Home E:\DESKTOP\CONFIGURATION FILE Browse Help Rights for user test1 Directory: * Browse Rights for directory * Image: Create Files/Dirs		test1		-	Done	,
Help Rights Rights for user test1 Browse Rights for directory * Remove Rights for directory * Create Files/Dirs	New User					
Rights for user test1 Directory: * Rights for directory * Rights for directory * Image: Read Image: Read	Home	E:\DESKTOP\C	ONFIGURATIO	DN FILE	Browse	
Rights for directory * ✓ Read ✓ Create Files/Dirs	· · · ·	t1				Rights<<
Read Create Files/Dirs	Directory: ×		•	Browse		Remove
	🔽 Read	I				

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:

<u>G</u> roup or user names:	Iministrators)
CREATOR OWNER	
😥 Everyone	
🛛 🖸 Hill, James (jahill@myservern	ame.com]
SYSTEM	~
<	>
(Add <u>R</u> emove
Permissions for Everyone	Allow Deny
Full Control	
Modify	
Read & Execute	
List Folder Contents	
Read	
Write	
Coosial Dormissions	
For special permissions or for advan click Advanced.	ced settings, Advanced

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:

Build 155	
15	
Tops	peed: 0.0 KB/s
Log	
17:23:24 Check update: no new versio	n
Status Speed Time left	%
tal In: 0 B VFS: 0 items	
	Log 17:23:24 Check update: no new versio

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
 ➢ Load file system Ctrl+O Gave file system Ctrl+S X Clear file system 	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/		
		op speed: 0.0 KB/s
Virtual File System Log		
Add files		
E Add folder from disk		
New empty folder Ins		
🕥 New link		
Advanced •		
Copy URL address Ctrl+C		
🔗 Browse it F9		
Comment		
Bind root to real-folder		
6 Set user/pass		
Sestrict access		
✓ Browsable		
✓ Archivable		
👍 Upload 🔹 🕨		
📥 Why is upload disabled?		
Hide tree		
Auto-hide empty folders	Speed Time left	%
Hide file extention in listing	spece filleleit	~*
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 saver	
		-11

4. Locate the root directory from your local system.

🔮 HFS ~ HTTP File Server 2.3 beta		Build 275			
🛓 Menu 🚏 Port: 80 🖓 👥 You	u are in Easy mode				
🖉 Open in browser http://10.2.11	.101:8088/ProvisioningDir/			Already i	n clipboard
Virtual File Syste	:m	Log			
✓ / └── ProvisioningDir					
舅 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	123	
Password	*****	
Re-type password	*****	
	<u>O</u> k <u>B</u> e	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.

🕦 DHCP Turbo on localhost	t		- D X
<u>File Edit View Bindings</u>	<u>T</u> ools <u>H</u> elp		
🔳 🔌 🗡 🐿	■ ≥ % 9 0 %	k ?	
Servers T	Nane Description Flatforn User: Admin Password: Version Hat bindings Features Build	Login	
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.

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**.

a a k 🛛	è 🖬	*	9	O		∖ ?						
vers 🗸	Filter St	andard Opt	ions					•				
localhost 	Tag V		Option					_			1	-
			Magic									-
🛨 🔛 Named Policies	🖅 -5			irector								
	<mark>421-4</mark>				ess type ess leng			New Option Type	Ctrl+V	h		
Scopes			Boot f					Undo	Ctrl+Z			
Dici Sei vei			Pad Subnet				-	Redo	Ctrl+V			
	<u>4</u> 2		Time o					-				
	/ 🖅 3		Gateway				r	Cu <u>t</u>	Ctrl+X			
	<u>4</u> 214 <u>422</u> 15		Time s TEN116	ervers name s	arvar 5		Ð	<u>C</u> opy	Ctrl+C			
			Domain					Paste	Ctrl+V			
			Log set					Delete	Del			
	<u>4</u> 28 <u>42</u> 19		LPR set		servers			Select All	Ctrl+A			
	🖅 10		Impres		rs		<u>_</u> ;;	Eind	Ctrl+F			
			RLP ser Hostnar				h- •					
				me ile siz	e		R	Properties	Ctrl+P			
	/ 🖅 14		Merit		le							
	Æ 15 Æ 16		Domain Swap s									
			Root p									
	🚝 18			ions pa								
				*arding								
	<u>42</u> 20			cal sou	rce rout	ing						
	Description											
	Specifies	a device's	har dwar	re 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.

<u>File Edit Yiew B</u> indings Tools <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.

1	gs <u>T</u> ools <u>H</u>		*	Ø	0	- Se	N ?	
	Tag ∇			Name		3	Yalue	
ocalhost	-		1.					
∋Database ≥HW Exclusions	1							
Named Policies		<u> </u>		Option	n Ct	rl+V		
- 🛃 Global Dption Types	1	5	<u>U</u> ndo	3	Ct	rl+Z		
Scopes		Ċ	<u>R</u> edo		Ct	rl+Y		
- DHCPServer	1	1	Cu <u>t</u>		Ct	rl+X		
		D	<u>C</u> opy			rl+C		
	1		Paste			rl+V		
	1	×	Delet		De		-	
	1		Select			rl+A	-	
		a. 1	Eind			rl+F	-	
		*	Prope	erties	. Ct	rl+P		

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	•	_ _	
	42 48 42 49 42 51 42 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.			
	42 72 42 73 42 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 (modified)		- X
<u>File Edit View Bindings Tools H</u> elp		
🛯 🖉 🥀 🐚 🗎 🗋	※ う ce 多 k?	
Servers Tag Tag Database Database Database Database Scopes Scopes - DMCFServer	Name Value	

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**.

DHCP Turbo on localho <u>File Edit View Bindings</u>			- (4	
		500	k ?		
Servers 🗸	Tag ∇	Name		Value	
- Decelhost - Detechost - Other Reclusions - Mewed Policies - Global - Glo	49 128	Redo C Redo C Paste C Delete I Select <u>A</u> II C	trl+Z trl+Y trl+X trl+C trl+V bel trl+A	tftp://192.168.1.100/	
			trt+F trt+P		
Add a new option to this	J policy				,
the shere option to this	F				

- 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	h ?		
Servers 🗸	Tag 🗸	Name		Value	
⊡-⊡localhost ⊙Database	🖅 128 🛃 Option Sele	ector		? ×	
	Filter	TFTP Options	•		
- 🛃 Global	Tag ∇	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.

🚰 DHCP Turbo on localhost		
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> indings]	<u>I</u> ools <u>H</u> elp	
	■ ■ ※ b c § k?	
Servers 🛆	Tag 🗸 Name Value	
- I localhost Scopes - Scopes - Option Types - Named Policies - Named Policies - Named Policies - Named Policies - Named Policies - Database	I28 TFTFServer tftp://192.168.1.1 Image: State of the	100/
]]	1.

- 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.

🎕 DHCP Turbo on localhost		- • X		
File Edit View Bindings Iools Help				
4 4 1	🖷 🗎 🛠 🔊 ୯≅ 🚱 😽			
Servers V	ag 🗸 Name Value			
Ilocalhost				
-WHW Exclusions	Filter Standard Options			
- Named Policies				
-Slobal	Tag V Name A			
- Dption Types	25 Path MTU plateau table			
	-26 Interface MTV			
DHCPServer	-Æ27 All subnets are local			
	- 28 35 Arp cache timeout 28 36 Ethernet encapsulation			
	- A 38 TCP keepalive interval			
	Description 🕱			
	Used by devices and servers to exchange vendor-specific information.			
	over by devices and servers to exchange vendor specific information.			
٠	QK <u>C</u> ancel			
4				

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

BHCP Turbo on localhos <u>File Edit V</u> iew <u>B</u> indings		
4 *	• ■ ■ ※ ゥ ⌒ � ¥	
Servers / Servers / Scopes		//192.168.1.100/ 58.1.100

- 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.