



SIP-T2 Series/T19(P) E2/T4 Series/CP860 IP Phones Auto Provisioning Guide

Table of Contents

Table of Contents.....	iii
Summary of Changes.....	v
Changes for Release 80, Guide Version 80.61	v
Changes for Release 80, Guide Version 80.60	v
Changes for Release 80, Guide Version 80.20	v
Changes for Release 80, Guide Version 80.6	vi
Introduction.....	1
Getting Started.....	3
Obtaining Configuration Files.....	3
Obtaining Phone Information	4
Provisioning Yealink IP Phones	5
Auto Provisioning Process.....	5
Major Tasks for Auto Provisioning	5
An Instance of Auto Provision Configuration	6
Managing Configuration Files	11
Editing Common CFG File.....	11
Editing MAC-Oriented CFG File	12
Creating a New CFG File	13
Managing MAC-local CFG File.....	14
Encrypting Configuration Files.....	14
Customizing Resource Files	15
Configuring a Provisioning Server	17
Preparing a Root Directory.....	17
Configuring a TFTP Server.....	18
Obtaining the Provisioning Server Address	21
Zero Touch.....	21
Plug and Play (PnP) Server	23

DHCP Options.....	25
Phone Flash.....	26
Configuring Wildcard of the Provisioning Server URL.....	27
Triggering the IP Phone to Perform the Auto Provisioning	29
Power On.....	29
Repeatedly.....	30
Weekly.....	31
Auto Provision Now	32
Multi-mode Mixed	33
SIP NOTIFY Message	33
Auto Provisioning via Activation Code	34
Downloading and Verifying Configurations	37
Downloading Configuration Files.....	37
Resolving and Updating Configurations	37
Using MAC-local CFG File	38
Verifying Configurations	38
Troubleshooting	41
Glossary.....	43
Appendix	45
Configuring an FTP Server	45
Preparing a Root Directory	45
Configuring an FTP Server	46
Configuring an HTTP Server.....	48
Preparing a Root Directory	48
Configuring an HTTP Server	49
Configuring a DHCP Server	52

Summary of Changes

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

Changes for Release 80, Guide Version 80.61

This version is updated to incorporate CP860 IP phones. Documentations of the newly released SIP-T40P IP phones have also been added.

Changes for Release 80, Guide Version 80.60

Documentations of the newly released SIP-T19(P) E2 IP phones have been added.

The following sections are new:

- [Provisioning Yealink IP Phones](#) on page 5
- [Creating a New CFG File](#) on page 13

The following section is removed to [Yealink_SIP-T2_Series_T19\(P\) E2_T4_Series_IP_Phones_Administrator_Guide](#):

- Specific Scenarios-Keep User Personalized Settings

The following section is removed to [Yealink_SIP-T2_Series_T19\(P\) E2_T4_Series IP phones_Description of Configuration Parameters in CFG Files.xlsx](#):

- Description of Configuration Parameters in CFG file

Major updates have occurred to the following section:

- [Customizing Resource Files](#) on page 15

Changes for Release 80, Guide Version 80.20

This version is updated to incorporate SIP-T48G IP phones. Documentations of the newly released SIP-T27P and SIP-T21(P) E2 IP phones have also been added.

Major updates have occurred to the following sections:

- [Editing Common CFG File](#) on page 11
- [Editing MAC-Oriented CFG File](#) on page 12
- [Customizing Resource Files](#) on page 15
- [Obtaining the Provisioning Server Address](#) on page 21

Changes for Release 80, Guide Version 80.6

This version is updated to incorporate SIP-T46G, SIP-T42G, SIP-T41P and T29G IP phones.

Major updates have occurred to the following sections:

- [Customizing Resource Files](#) on page 15
- [Configuring Wildcard of the Provisioning Server URL](#) on page 27

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
- Yealink SIP-T46G
- Yealink SIP-T42G
- Yealink SIP-T41P
- Yealink SIP-T40P
- Yealink SIP-T29G
- Yealink SIP-T27P
- Yealink SIP-T23P/G
- Yealink SIP-T21(P) E2
- Yealink SIP-T19(P) E2
- Yealink CP860

The auto provisioning process outlined in this guide applies to Yealink SIP-T48G/T46G/T42G/T41P/T40P/T29G/T27P/T23P/T23G/T21(P) E2/T19(P) E2 and CP860 IP phones running firmware version 80 or later. We recommend that IP phones running the latest firmware CANNOT be downgraded to an earlier firmware version. The new firmware is compatible with old configuration parameters, but not vice versa.

Getting Started

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

- [Obtaining Configuration Files](#)
- [Obtaining Phone Information](#)

Obtaining Configuration Files

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

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

You can ask the distributor or Yealink FAE for Common CFG and MAC-Oriented files. You can also obtain the Common CFG file and MAC-Oriented file online:

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

To download Common CFG and MAC-Oriented 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		
Last modified date: 2015/08/11 views: 1983		
Datasheet	Datasheet	Yealink SIP-T23G Datasheet.pdf
Firmware & Release Note	Firmware & Release Note	Yealink_SIP_phones_Release_Notes_of_Version80.pdf New
Setup & Maintenance		T23-44.80.0.70.zip New
Documents		44.80.0.60.zip New
Other Documents		44.80.0.5.zip
User Documents	User Documents	Yealink_SIP-T23P & T23G_User_Guide_V80_60.pdf
		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_60.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.

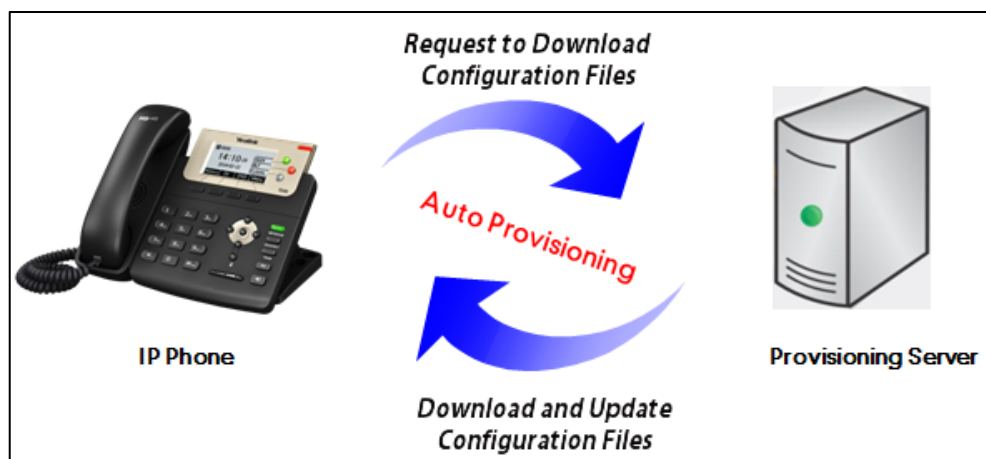
Provisioning Yealink IP Phones

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, it will request to download the configuration files from the provisioning server. During the auto provisioning process, the IP phone will download and update configuration files to the phone flash.

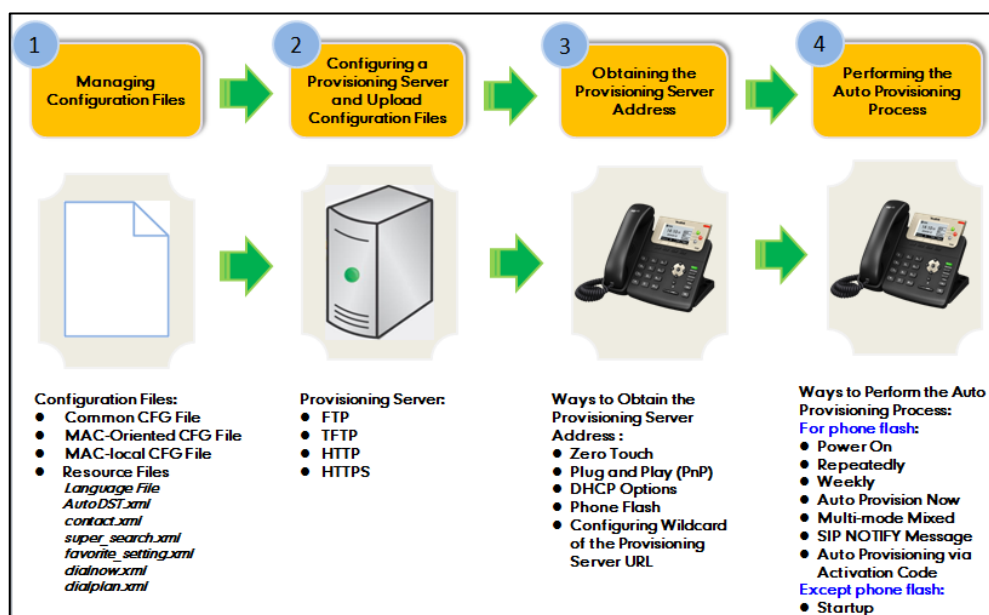
The following figure shows how the IP phone interoperates with the provisioning server:



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 configuration files, refer to [Managing Configuration Files](#) on page 11.

For more information on how to configure a provisioning server, refer to [Configuring a Provisioning Server](#) on page 17.

For more information on how to obtain the provisioning server address, refer to [Obtaining the Provisioning Server Address](#) on page 21.

For more information on how to perform the auto provisioning process, refer to [Triggering the IP Phone to Perform the Auto Provisioning](#) on page 29.

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 6.

An Instance of Auto Provision Configuration

This section shows an instance of auto provision configuration.

1. Manage configuration files.

Add/Edit the desired configuration parameters in the CFG file (e.g., y000000000044.cfg) you want the IP phone to download. For more information on how to manage configuration files, refer to [Managing Configuration Files](#) on page 11.

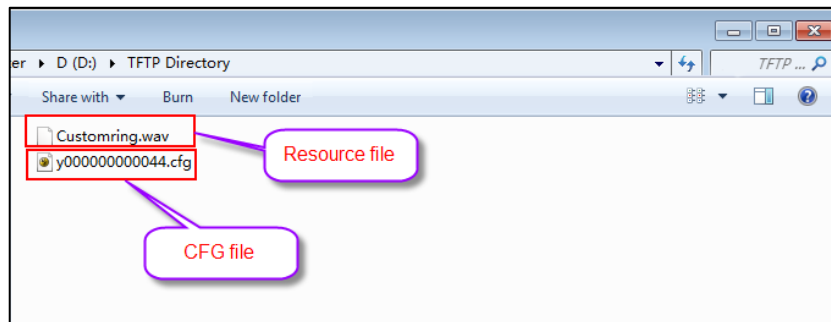
```

1 #!version:1.0.0.1
2 features.dnd_mode = 0
3 features.dnd.enable = 1
4 ringtone.url = tftp://192.168.1.100/Customring.wav

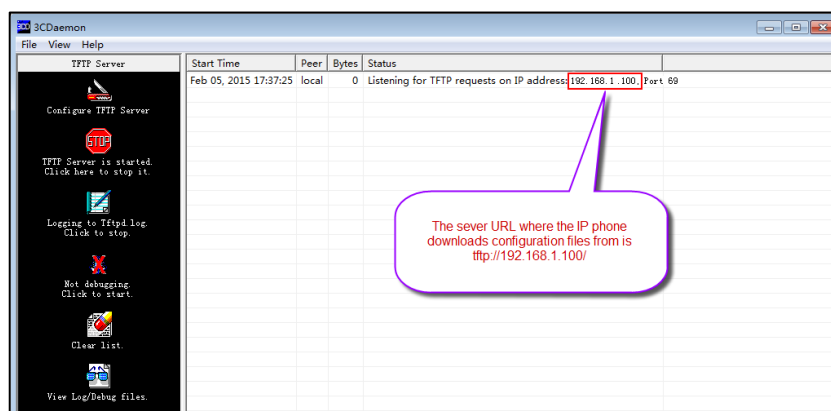
```


2. Configure the TFTP server.

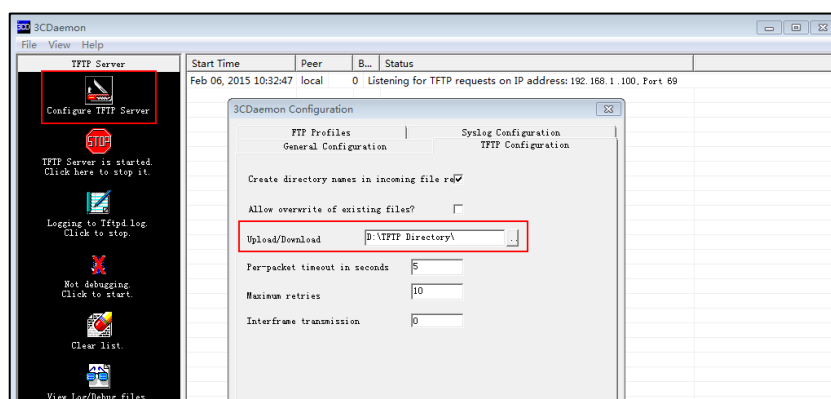
- 1) Place configuration files to TFTP root directory (e.g., D:\TFTP Directory).



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



- 3) Select **Configure TFTP Server**. Click the  button to locate the TFTP root directory from your local system.



For more information on how to configure a provisioning server, refer to [Configuring a Provisioning Server](#) on page 17.

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

The screenshot shows the Yealink T236 web interface. The 'Settings' tab is selected. In the left sidebar, 'Auto Provision' is highlighted. The main content area shows the 'Auto Provision' configuration page. The 'Server URL' field is highlighted with a red box, and a callout bubble points to it with the text: "Enter the access URL of the provisioning server in the Server URL field." The 'Server URL' field contains the text "tftp://192.168.1.100/". Other fields include 'PHP Active', 'DHCP Active', 'Custom Option(128~254)', 'DHCP Option Value', 'User Name', 'Password', 'Attempt Expired Time(s)', 'Common AES Key', 'MAC-Oriented AES Key', 'Zero Active', 'Wait Time(1~100s)', 'Power On', 'Repeatedly', 'Interval(Minutes)', 'Weekly', 'Time', and 'Day of Week'. A 'NOTE' section on the right explains the auto provisioning process.

For more information on how to obtain the provisioning server address, refer to [Obtaining the Provisioning Server Address](#) on page 21.

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

The screenshot shows the Yealink T236 web interface. The 'Settings' tab is selected. In the left sidebar, 'Auto Provision' is highlighted. The main content area shows the 'Auto Provision' configuration page. The 'Autoprovision Now' button is highlighted with a red box, and a callout bubble points to it with the text: "Click the Autoprovision Now to perform the auto provisioning process immediately." The 'Server URL' field contains the text "tftp://192.168.1.100/". Other fields are the same as in the previous screenshot. A 'NOTE' section on the right explains the auto provisioning process.

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 29.

Managing Configuration Files

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

You can edit the template 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_CP860 IP phones_Description of Configuration Parameters in CFG Files.xlsx](#).

Editing Common CFG File

The Common CFG file is effectual for all phones of the same model. It uses a fixed name "y0000000000XX.cfg" as the file name, where "XX" equals to the first two digits of the hardware version of the IP phone model.

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

Phone Model	Common CFG File
SIPT48G	y000000000035.cfg
SIPT46G	y000000000028.cfg
SIPT42G	y000000000029.cfg
SIP-T41P	y000000000036.cfg
SIP-T40P	Y000000000054.cfg
SIP-T29G	y000000000046.cfg
SIP-T27P	y000000000045.cfg
SIP-T23P/G	y000000000044.cfg
SIP-T21(P) E2	y000000000052.cfg
SIP-T19(P) E2	y000000000053.cfg
CP860	y000000000037.cfg

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

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

```
#!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 80 or later.##
##For more information on configuration parameters, refer to Description of Configuration Parameters in CFG Files.xslx##

#####
##                               Hostname                               ##
#####
network.dhcp_host_name =

#####
##                               PPPoE(Except T41P/T42G Models)          ##
#####
network.pppoe.user =
network.pppoe.password =

#####
##                               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.
network.pc_port.enable =

##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 100Mbps (only applicable to SIP-T42G, SIP-T46G and SIP-T48G IP phones)
##The default value is 0.It takes effect after a reboot.
network.internet_port.speed_duplex =

##It configures the transmission mode and speed of the PC (LAN) port.
##0-Auto Negotiate
##1-Full Duplex 10Mbps
```

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 are only effectual for the specific phone. They use the 12-digit MAC address of the IP phone as the file name. For example, if the MAC address of the IP phone is 0015651130F9, the MAC-Oriented CFG file has to be named as 0015651130f9.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:

```
#!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 80 or later.##
##For more information on configuration parameters, refer to Description of Configuration Parameters in CFG Files.xlsx.##

#####
##                               Account1 Basic Settings                               ##
#####
account.1.enable =
account.1.label =
account.1.display_name =
account.1.auth_name =
account.1.user_name =
account.1.password =
account.1.outbound_proxy_enable =
account.1.outbound_host =
account.1.outbound_port =
account.1.dial_tone =

##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 =
```

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/T46G/T29G IP phones support 16 accounts, SIP-T42G IP phones support 12 accounts, SIP-T41P/T27P 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 and CP860 IP phones support only one account.

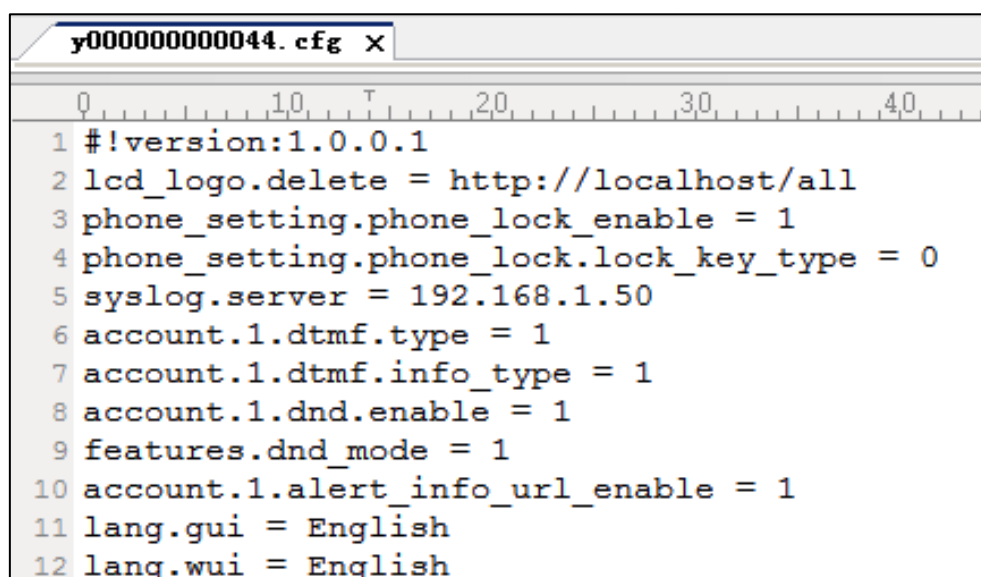
Creating a New CFG File

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 11 or [Editing MAC-Oriented CFG File](#) on page 12.

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



```
y0000000000044.cfg x
1 #!version:1.0.0.1
2 lcd_logo.delete = http://localhost/all
3 phone_setting.phone_lock_enable = 1
4 phone_setting.phone_lock.lock_key_type = 0
5 syslog.server = 192.168.1.50
6 account.1.dtmf.type = 1
7 account.1.dtmf.info_type = 1
8 account.1.dnd.enable = 1
9 features.dnd_mode = 1
10 account.1.alert_info_url_enable = 1
11 lang.gui = English
12 lang.wui = English
```

3. Save the changes and close the CFG file.

Managing MAC-local CFG File

MAC-local CFG file automatically stores configurations modified via web user interface or phone user interface. The file is stored locally on the IP phone, but a copy can also be uploaded to the provisioning server. The 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 0015651130F9, MAC-local CFG file has to be named as 0015651130f9-local.cfg (case-sensitive) respectively.

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 CP860 IP Phones Administrator Guide](#).

We recommend you do not edit the MAC-local CFG file. If you really want to edit MAC-local CFG file, you can export and then edit it. For more information on how to export this file, refer to [Yealink SIP-T2 Series T19\(P\) E2 T4 Series CP860 IP Phones Administrator Guide](#).

Encrypting Configuration Files

To protect against unauthorized access and tampering of sensitive information (e.g., login password, registration information), you can encrypt configuration files using

Yealink Configuration Encryption Tool. AES keys must be 16 characters and the supported characters contain: 0 ~ 9, A ~ Z, a ~ 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) 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
Firmware	X.80.0.XX.rom For example, 44.80.0.60.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_CP860_IP_Phones_Administrator_Guide*](#).

Configuring a Provisioning Server

Yealink IP phones support using FTP, TFTP, HTTP and HTTPS protocols to download 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 TFTP32 as a TFTP server. 3CDaemon and TFTP32 are free applications for Windows. You can download 3CDaemon online:

<http://www.oldversion.com/3Com-Daemon.html> and TFTP32 online:

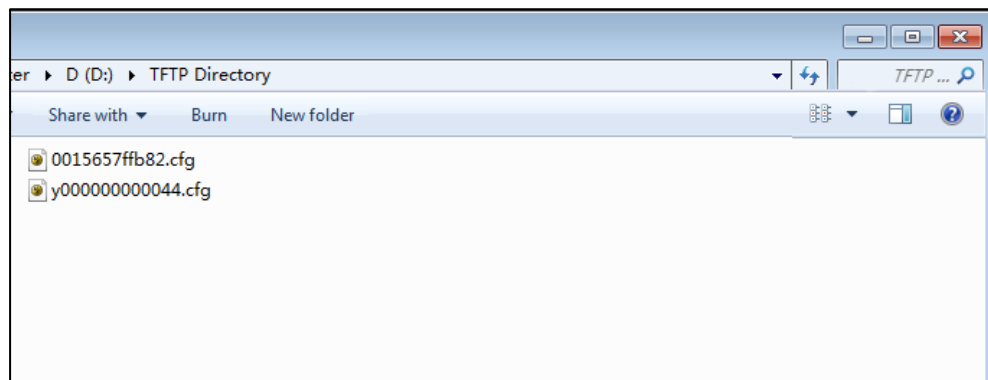
<http://tftpd32.jounin.net/>.

For more information on how to configure FTP and HTTP servers, refer to [Configuring an FTP Server](#) on page 45 and [Configuring an HTTP Server](#) on page 48.

Preparing a Root Directory

To prepare a root directory:

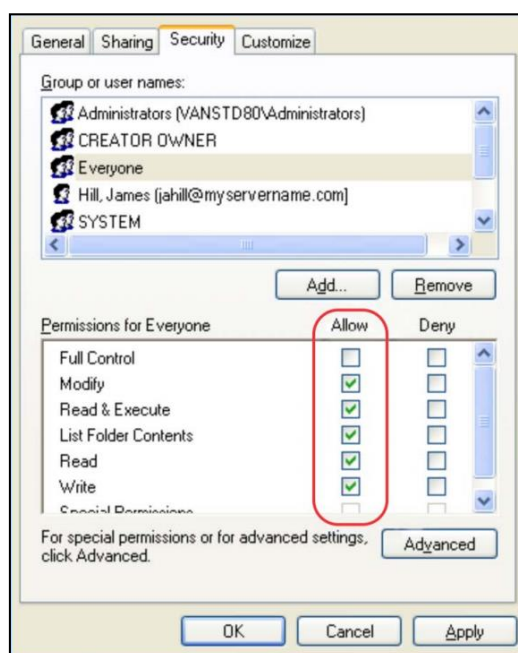
1. Create a TFTP root directory on the local system (e.g., D:\TFTP Directory).
2. Place configuration files to this root directory.



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.

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

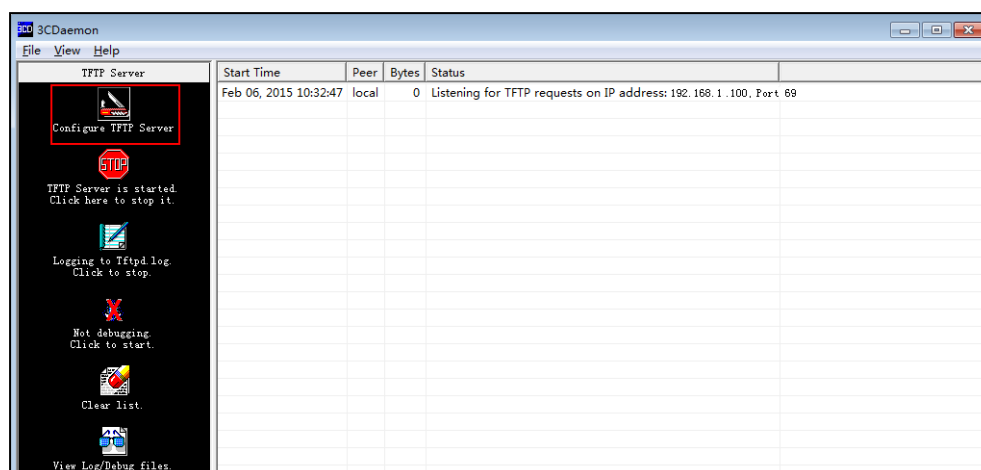



Configuring a TFTP Server

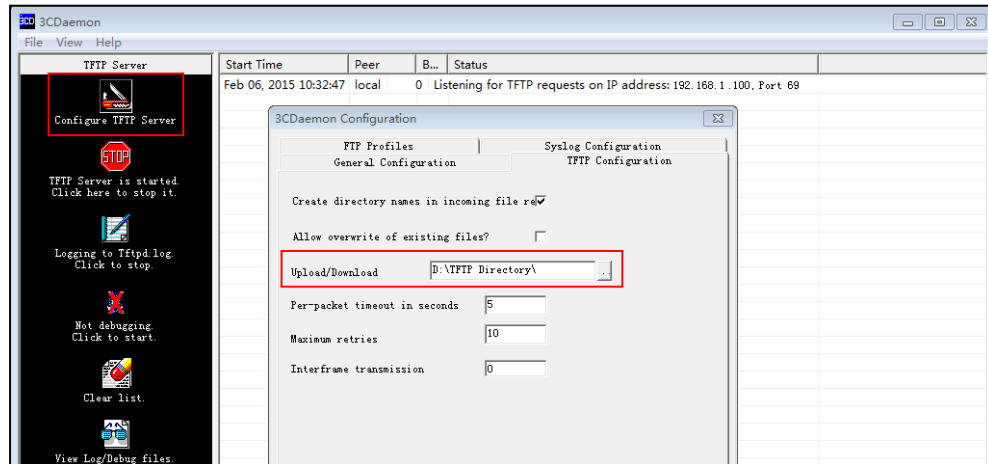
If you have a 3CDaemon application installed on your local system, use it directly. Otherwise, download and install it.

To configure a TFTP server:

1. Double click 3CDaemon.exe to start the application. A configuration page is shown as below:



2. Select **Configure TFTP Server**. Click the  button to locate the TFTP root directory from your local system:



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://192.168.1.100/") 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**.

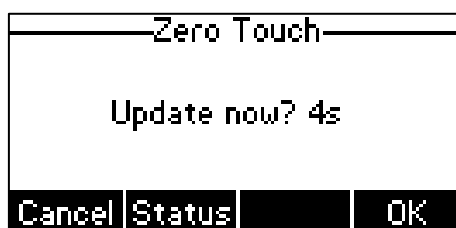
- Enter the desired wait time in the **Wait Time(1~100s)** field.

The default value is 5.

The screenshot shows the Yealink T236 web interface. The 'Auto Provision' section is active, showing various settings. The 'Zero Active' dropdown is set to 'Enabled' and the 'Wait Time(1~100s)' field is set to '5'. A red box highlights these two fields. The interface includes a sidebar with navigation options like Preference, Time & Date, Call Display, Upgrade, Auto Provision, Configuration, Dial Plan, Voice, Ring, Tones, Softkey Layout, TR069, Voice Monitoring, and SIP. The main content area has tabs for Status, Account, Network, DSSKey, Features, Settings, Directory, and Security. A 'NOTE' section on the right explains the auto provisioning process.

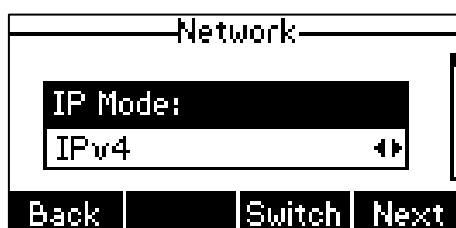
- Click **Confirm** to accept the change.

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:



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.

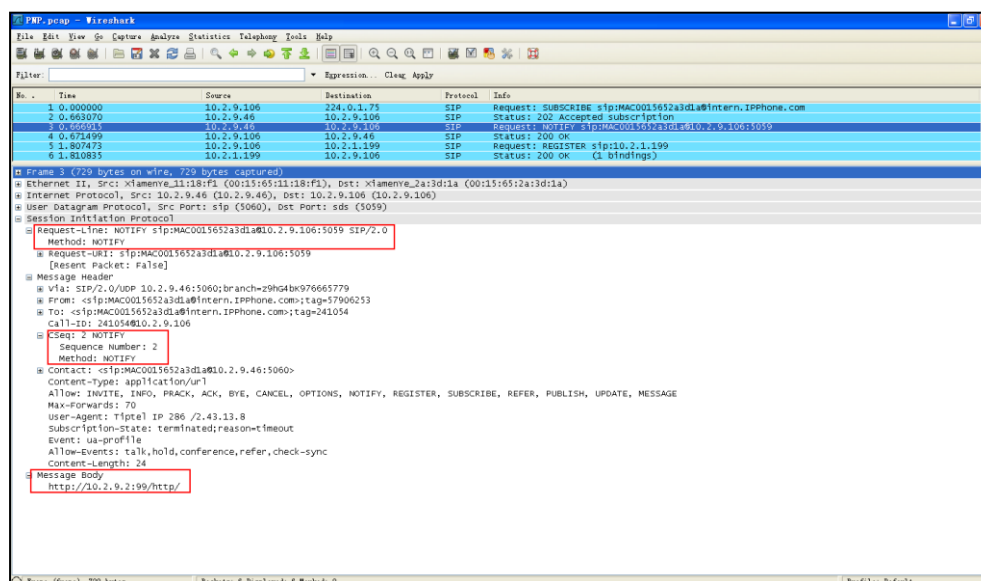
To configure PnP via web user interface:

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

The screenshot shows the Yealink T236 web interface. The 'Settings' tab is selected, and the 'Auto Provision' sub-tab is active. The 'PNP Active' field has the 'On' radio button selected, which is highlighted with a red box. Other settings like 'DHCP Active', 'Custom Option(128~254)', 'DHCP Option Value', 'Server URL', 'User Name', 'Password', 'Attempt Expired Time(s)', 'Common AES Key', 'MAC-Oriented AES Key', 'Zero Active', 'Wait Time(1~100s)', 'Power On', 'Repeatedly', 'Interval(Minutes)', 'Weekly', 'Time', and 'Day of Week' are also visible. A 'NOTE' box on the right states: 'Auto Provision The IP phone can interoperate with provisioning server using auto provisioning for deploying the IP phones. When the IP phone triggers to 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 update configuration files to the phone flash. You can click here to get more guides.'

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 52.

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.

The screenshot displays the 'Auto Provision' configuration page in the Yealink T236 web interface. The 'Settings' tab is active, and the 'Auto Provision' sub-tab is selected. The 'DHCP Active' field is highlighted with a red box, showing the 'On' radio button selected. The 'Custom Option(128~254)' field contains the value '128'. Other settings like 'DHCP Option Value', 'Server URL', 'User Name', 'Password', 'Attempt Expired Time(s)', 'Common AES Key', 'MAC-Oriented AES Key', 'Zero Active', 'Wait Time(1~100s)', 'Power On', 'Repeatedly', 'Interval(Minutes)', 'Weekly', 'Time', and 'Day of Week' are also visible.

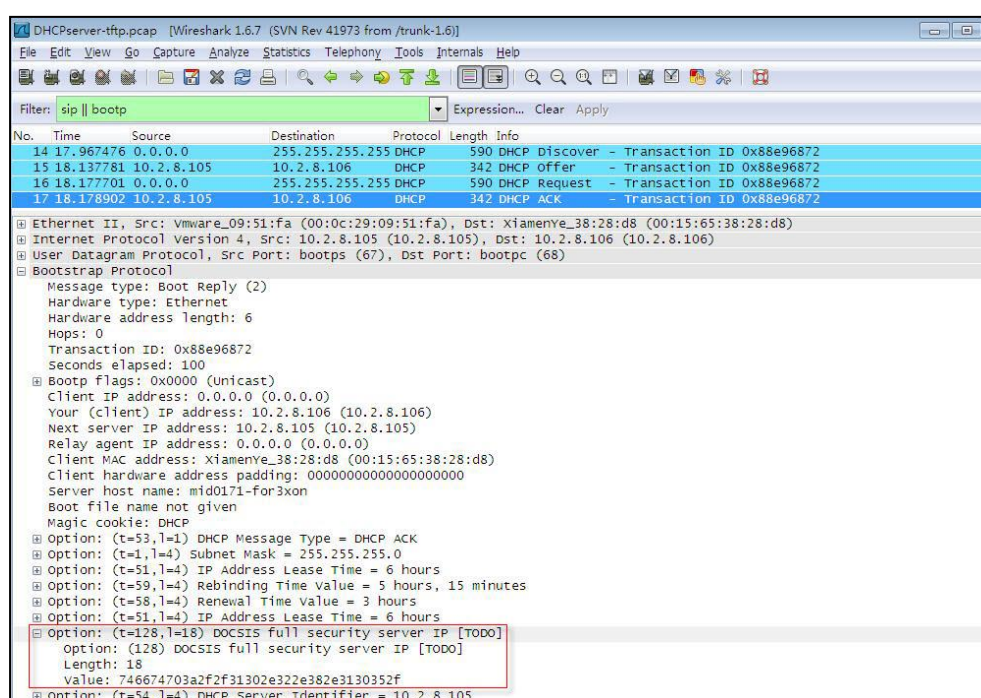
4. Click **Confirm** to accept the change.

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_CP860_IP_Phones_Administrator_Guide](#).

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



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

Phone Flash

Yealink 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** fields respectively (the user name and password are optional).

The screenshot shows the Yealink 1236 web interface. The 'Auto Provision' tab is selected in the top navigation bar. The 'Auto Provision' settings are displayed in the main area. The 'Server URL', 'User Name', and 'Password' fields are highlighted with a red box. The 'Server URL' field contains the text 'http://10.3.6.133:8080/y0000000000/'. The 'User Name' and 'Password' fields are empty. The 'Auto Provision' settings include options for 'PHP Active', 'DHCP Active', 'Custom Option(128~254)', 'DHCP Option Value', 'Attempt Expired Time(s)', 'Common AES Key', 'MAC-Oriented AES Key', 'Zero Active', 'Wait Time(1~100s)', 'Power On', 'Repeatedly', 'Interval(Minutes)', 'Weekly', 'Time', and 'Day of Week'. A 'NOTE' section on the right explains the Auto Provision process.

- 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, 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 29.

Configuring Wildcard of the Provisioning Server URL

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

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

The parameter "auto_provision.url_wildcard.pn" is used to configure the directory name the configuration files located. For more information on the parameter, refer to [Yealink_SIP-T2_Series_T19\(P\)_E2_T4_Series_CP860_IP_phones_Description_of_Configuration_Parameters_in_CFG_Files.xlsx](#).

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

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

The following example assists in explaining the wildcard feature:

You want to deploy SIP-T42G and SIP-T46G IP phones simultaneously in your environment. IP phones are configured to obtain the provisioning server address 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 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 "auto_provision.url_wildcard.pn".

The default value of the parameter "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 request to download configuration files (<MAC>.cfg files, y0000000000029.cfg for the SIP-T42G IP phones, and y0000000000028.cfg for the SIP-T46G IP phones) 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.cfg" 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.cfg file from the provisioning server address "tftp://192.168.1.100/T42G".

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](#)
- [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.

The screenshot shows the Yealink T236 web interface with the 'Settings' tab selected. The 'Auto Provision' section is active. The 'Power On' radio button is selected and highlighted with a red box. The 'Repeatedly' radio button is also selected. The 'Interval(Minutes)' is set to 1440. The 'Day of Week' section shows all days of the week checked. The 'Autoprovision Now' button is visible at the bottom right of the settings area.

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.

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

The screenshot shows the Yealink T236 web interface with the 'Settings' tab selected. The 'Auto Provision' section is active, displaying various configuration options. The 'Interval(Minutes)' field is highlighted with a red box and contains the value 1440. The 'Repeatedly' radio button is selected, and the 'Weekly' section is expanded, showing the 'Time' field set to 00:00-00:00 and the 'Day of Week' field with all days of the week selected. A 'NOTE' box on the right explains the auto provisioning process.

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

Weekly

The IP phone performs the auto provisioning process at the fixed time every week. 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. For example, you can configure the IP phone to check and update new configuration between 2 to 3 o'clock every Friday and Sunday.

To activate the weekly mode via web user interface:

- Click on **Settings->Auto Provision**.
- Mark the **On** radio box in the **Weekly** field.
- Enter the desired time in the **Time** field.

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

The screenshot shows the Yealink T236 web interface with the 'Settings' tab selected. The 'Auto Provision' section is active, and the 'Day of Week' field is highlighted with a red box. The 'Weekly' checkbox is checked, and the 'Time' is set to 02:00 - 03:00. The 'Autoprovision Now' button is visible at the bottom of the highlighted section. The 'Confirm' and 'Cancel' buttons are at the bottom of the page.

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**.

2. Click **Autoprovision Now**.

The screenshot shows the Yealink T236 web interface. The 'Settings' tab is selected, and the 'Auto Provision' section is active. The left sidebar lists various settings categories, with 'Auto Provision' highlighted. The main content area displays the 'Auto Provision' configuration options, including checkboxes for 'PHP Active' and 'DHCP Active', text fields for 'Custom Option(128~254)', 'Server URL', 'User Name', and 'Password', and dropdown menus for 'Attempt Expired Time(s)', 'Common AES Key', 'MAC-Oriented AES Key', and 'Zero Active'. There are also input fields for 'Wait Time(1~100s)', 'Power On', 'Repeatedly', 'Interval(Minutes)', and 'Weekly'. A 'Day of Week' section allows selecting days from Sunday to Saturday. At the bottom, the 'Autoprovision Now' button is highlighted with a red box. A 'NOTE' section on the right explains the auto provisioning process and provides a link to more guides.

The IP phone will perform the auto provisioning process immediately.

Multi-mode Mixed

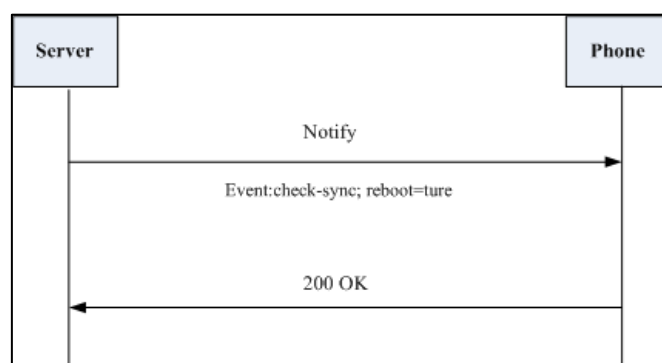
You can activate more than one method for auto provisioning. For example, you can activate the “Power On” and “Repeatedly” modes simultaneously. The IP phone will perform the auto provisioning process when it is powered on and at a specified interval.

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_CP860_IP_phones_Description_of_Configuration_Parameters_in_CFG_Files.xlsx](#).

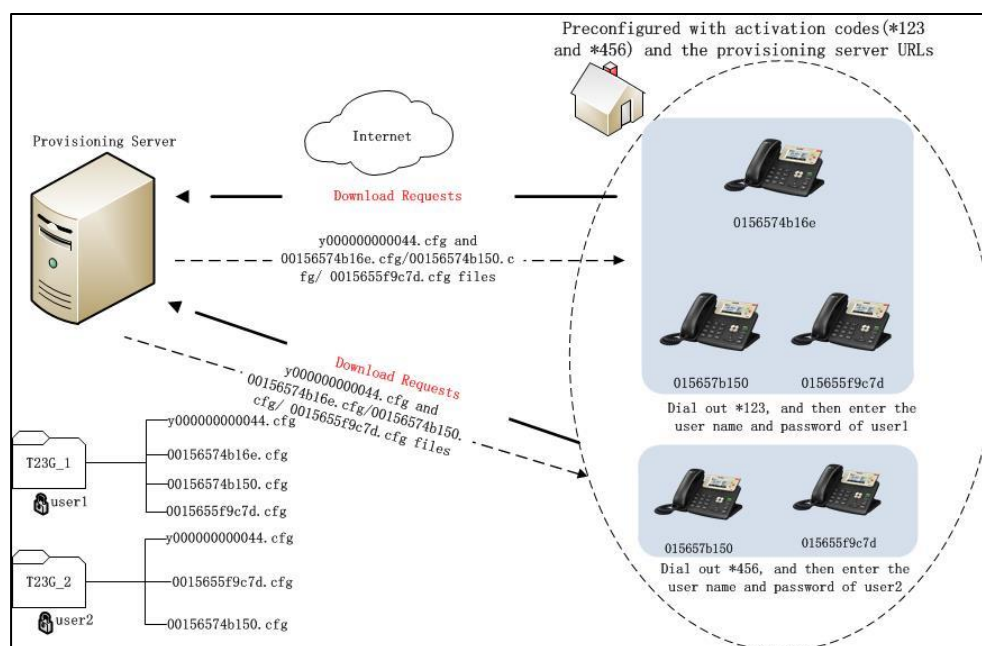
This method requires server support.

The following figure shows the message flow:



Auto Provisioning via Activation Code

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



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

1. Create multiple directories (e.g., T23G_1 and T23G_2) on the provisioning server.
2. Store a common CFG file and multiple <MAC>.cfg files to each directory on the provisioning server.
3. Configure a user name and password for each directory.

The user name and password provides a means of conveniently partitioning the

configuration files for different 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
```

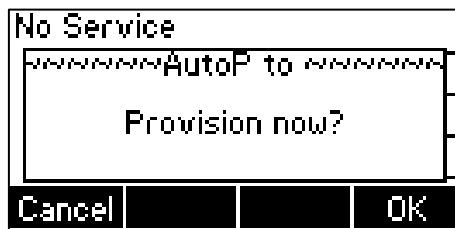
```
autoprovision.1.url = tftp://192.168.1.30/T23G_1/
```

```
autoprovision.2.code = *456
```

```
autoprovision.2.url = tftp://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 after the phone startup.

The LCD screen will prompt the following dialog box:



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

The LCD screen will prompt the following input box:



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

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

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

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

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):

#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 configuration files.

autoprovision.X.user

autoprovision.X.password

Downloading and Verifying Configurations

Downloading Configuration Files

After obtaining the provisioning server address in one of the ways introduced above, the phone will request to download the configuration files from the provisioning server when it is triggered to perform auto provisioning. During the auto provisioning process, the 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 "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 "auto_provision.reboot_force.enable", refer to [Yealink SIP-T2 Series_T19\(P\) E2_T4_Series_CP860 IP phones_Description of Configuration Parameters in CFG Files.xlsx](#).

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

User Guide.

Using MAC-local CFG File

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

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

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

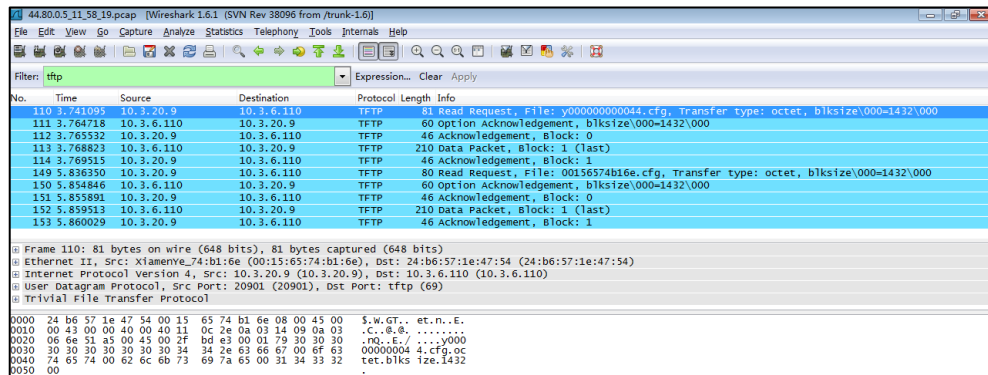
You can configure whether the IP phone updates configurations in the <MAC>-local.cfg file during auto provisioning. This process is controlled by the value of the parameter "auto_provision.custom.protect". If the IP phone is configured to keep user personalized settings (by setting the value of the parameter "auto_provision.custom.protect" to 1), it will update configurations in the <MAC>-local.cfg file. The IP Phone updates configuration files during auto provisioning in sequence: Common>MAC-Oriented>MAC-local. The configurations in the <MAC>-local.cfg file take precedence over the ones in the downloaded Common CFG file or <MAC>.cfg file. As a result, the personalized settings of the phone configured via the phone or web user interface can be kept after auto provisioning.

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.

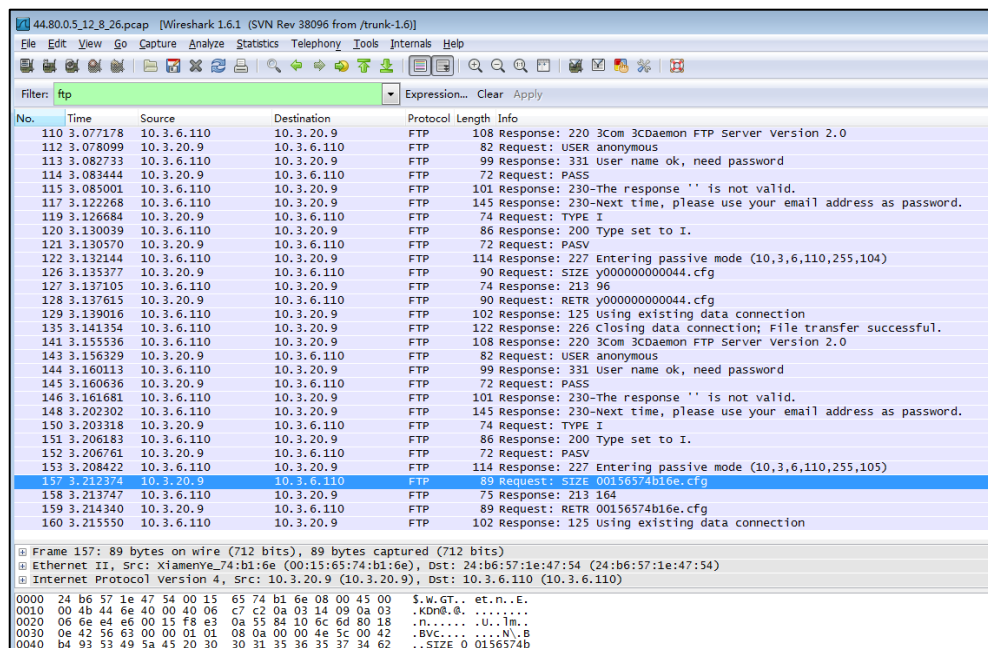
Example1: Yealink SIP-T23G IP phone downloads configuration files from the TFTP server.



Wireshark 1.6.1 (SVN Rev 38096 from/trunk-1.6) capture of TFTP traffic. The filter is 'tftp'. The packet list shows a sequence of TFTP messages between 10.3.20.9 and 10.3.6.110. The packet details pane shows the selected packet (No. 110) as a Read Request for file y0000000000044.cfg, transfer type: octet, blksize=000=1432\000. The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
110	3.741095	10.3.20.9	10.3.6.110	TFTP	81	Read Request, File: y0000000000044.cfg, Transfer type: octet, blksize=000=1432\000
111	3.764718	10.3.6.110	10.3.20.9	TFTP	60	Option Acknowledgement, blksize=000=1432\000
112	3.765532	10.3.20.9	10.3.6.110	TFTP	46	Acknowledgement, Block: 0
113	3.768823	10.3.6.110	10.3.20.9	TFTP	210	Data Packet, Block: 1 (last)
114	3.769515	10.3.20.9	10.3.6.110	TFTP	46	Acknowledgement, Block: 1
149	5.836350	10.3.20.9	10.3.6.110	TFTP	80	Read Request, File: 00156574b16e.cfg, Transfer type: octet, blksize=000=1432\000
150	5.854846	10.3.6.110	10.3.20.9	TFTP	60	Option Acknowledgement, blksize=000=1432\000
151	5.855891	10.3.20.9	10.3.6.110	TFTP	46	Acknowledgement, Block: 0
152	5.859513	10.3.6.110	10.3.20.9	TFTP	210	Data Packet, Block: 1 (last)
153	5.860029	10.3.20.9	10.3.6.110	TFTP	46	Acknowledgement, Block: 1

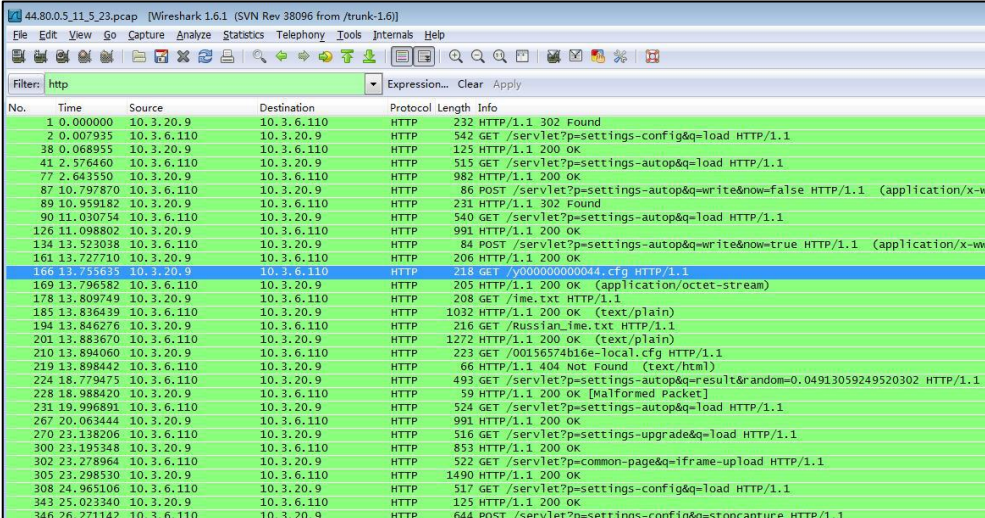
Example 2: Yealink SIP-T23G IP phone downloads configuration files from the FTP server.



Wireshark 1.6.1 (SVN Rev 38096 from/trunk-1.6) capture of FTP traffic. The filter is 'ftp'. The packet list shows a sequence of FTP messages between 10.3.20.9 and 10.3.6.110. The packet details pane shows the selected packet (No. 157) as a Request for file 00156574b16e.cfg. The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
110	3.077178	10.3.6.110	10.3.20.9	FTP	108	Response: 220 3com 3Cdaemon FTP Server version 2.0
112	3.078099	10.3.20.9	10.3.6.110	FTP	82	Request: USER anonymous
113	3.082733	10.3.6.110	10.3.20.9	FTP	99	Response: 331 User name ok, need password
114	3.083444	10.3.20.9	10.3.6.110	FTP	72	Request: PASS
115	3.085001	10.3.6.110	10.3.20.9	FTP	101	Response: 230-The response '' is not valid.
117	3.122268	10.3.6.110	10.3.20.9	FTP	145	Response: 230-Next time, please use your email address as password.
119	3.126684	10.3.20.9	10.3.6.110	FTP	74	Request: TYPE I
120	3.130039	10.3.6.110	10.3.20.9	FTP	86	Response: 200 Type set to I.
121	3.130570	10.3.20.9	10.3.6.110	FTP	72	Request: PASV
122	3.132144	10.3.6.110	10.3.20.9	FTP	114	Response: 227 Entering passive mode (10,3,6,110,255,104)
126	3.135377	10.3.20.9	10.3.6.110	FTP	90	Request: SIZE y0000000000044.cfg
127	3.137105	10.3.6.110	10.3.20.9	FTP	74	Response: 213 96
128	3.137615	10.3.20.9	10.3.6.110	FTP	90	Request: RETR y0000000000044.cfg
129	3.139016	10.3.6.110	10.3.20.9	FTP	102	Response: 125 Using existing data connection
135	3.141354	10.3.6.110	10.3.20.9	FTP	122	Response: 226 Closing data connection; File transfer successful.
141	3.155536	10.3.6.110	10.3.20.9	FTP	108	Response: 220 3com 3Cdaemon FTP Server version 2.0
143	3.156329	10.3.20.9	10.3.6.110	FTP	82	Request: USER anonymous
144	3.160113	10.3.6.110	10.3.20.9	FTP	99	Response: 331 User name ok, need password
145	3.160636	10.3.20.9	10.3.6.110	FTP	72	Request: PASS
146	3.161681	10.3.6.110	10.3.20.9	FTP	101	Response: 230-The response '' is not valid.
148	3.202302	10.3.6.110	10.3.20.9	FTP	145	Response: 230-Next time, please use your email address as password.
150	3.203318	10.3.20.9	10.3.6.110	FTP	74	Request: TYPE I
151	3.206183	10.3.6.110	10.3.20.9	FTP	86	Response: 200 Type set to I.
152	3.206761	10.3.20.9	10.3.6.110	FTP	72	Request: PASV
153	3.208422	10.3.6.110	10.3.20.9	FTP	114	Response: 227 Entering passive mode (10,3,6,110,255,105)
157	3.213747	10.3.6.110	10.3.20.9	FTP	90	Request: RETR 00156574b16e.cfg
158	3.213747	10.3.6.110	10.3.20.9	FTP	75	Response: 213 164
159	3.214340	10.3.20.9	10.3.6.110	FTP	89	Request: RETR 00156574b16e.cfg
160	3.215550	10.3.6.110	10.3.20.9	FTP	102	Response: 125 Using existing data connection

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



44.80.0.5_11_5_23.pcap [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.3.20.9	10.3.6.110	HTTP	232	HTTP/1.1 302 Found
2	0.007935	10.3.6.110	10.3.20.9	HTTP	542	GET /servlet?p=settings-config&q=load HTTP/1.1
38	0.068955	10.3.20.9	10.3.6.110	HTTP	125	HTTP/1.1 200 OK
41	2.576460	10.3.6.110	10.3.20.9	HTTP	515	GET /servlet?p=settings-autop&q=load HTTP/1.1
77	2.643550	10.3.20.9	10.3.6.110	HTTP	982	HTTP/1.1 200 OK
87	10.797870	10.3.6.110	10.3.20.9	HTTP	86	POST /servlet?p=settings-autop&q=write&now=false HTTP/1.1 (application/x-www-form-urlencoded)
89	10.959182	10.3.20.9	10.3.6.110	HTTP	231	HTTP/1.1 302 Found
90	11.030754	10.3.6.110	10.3.20.9	HTTP	540	GET /servlet?p=settings-autop&q=load HTTP/1.1
126	11.098802	10.3.20.9	10.3.6.110	HTTP	991	HTTP/1.1 200 OK
134	13.523038	10.3.6.110	10.3.20.9	HTTP	84	POST /servlet?p=settings-autop&q=write&now=true HTTP/1.1 (application/x-www-form-urlencoded)
161	13.727710	10.3.20.9	10.3.6.110	HTTP	206	HTTP/1.1 200 OK
166	13.755695	10.3.20.9	10.3.6.110	HTTP	218	GET /y0000000000044.cfg HTTP/1.1
169	13.796582	10.3.6.110	10.3.20.9	HTTP	205	HTTP/1.1 200 OK (application/octet-stream)
178	13.809749	10.3.20.9	10.3.6.110	HTTP	208	GET /ime.txt HTTP/1.1
185	13.836439	10.3.6.110	10.3.20.9	HTTP	1032	HTTP/1.1 200 OK (text/plain)
194	13.846276	10.3.20.9	10.3.6.110	HTTP	216	GET /Russian_ime.txt HTTP/1.1
201	13.883670	10.3.6.110	10.3.20.9	HTTP	1272	HTTP/1.1 200 OK (text/plain)
210	13.894060	10.3.20.9	10.3.6.110	HTTP	223	GET /00156574b1ee-local.cfg HTTP/1.1
219	13.898442	10.3.6.110	10.3.20.9	HTTP	66	HTTP/1.1 404 Not Found (text/html)
224	18.779475	10.3.6.110	10.3.20.9	HTTP	493	GET /servlet?p=settings-autop&q=result&random=0.04913059249520302 HTTP/1.1
228	18.988420	10.3.20.9	10.3.6.110	HTTP	59	HTTP/1.1 200 OK [Malformed Packet]
231	19.996891	10.3.6.110	10.3.20.9	HTTP	524	GET /servlet?p=settings-autop&q=load HTTP/1.1
267	20.063444	10.3.20.9	10.3.6.110	HTTP	991	HTTP/1.1 200 OK
270	23.138206	10.3.6.110	10.3.20.9	HTTP	516	GET /servlet?p=settings-upgrade&q=load HTTP/1.1
300	23.195348	10.3.20.9	10.3.6.110	HTTP	853	HTTP/1.1 200 OK
302	23.278964	10.3.6.110	10.3.20.9	HTTP	522	GET /servlet?p=common-page&q=iframe-upload HTTP/1.1
305	23.298530	10.3.20.9	10.3.6.110	HTTP	1490	HTTP/1.1 200 OK
308	24.965106	10.3.6.110	10.3.20.9	HTTP	517	GET /servlet?p=settings-config&q=load HTTP/1.1
343	25.023340	10.3.20.9	10.3.6.110	HTTP	125	HTTP/1.1 200 OK
346	26.271142	10.3.6.110	10.3.20.9	HTTP	644	POST /servlet?p=settings-config&q=stopcapture HTTP/1.1

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.

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.

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.

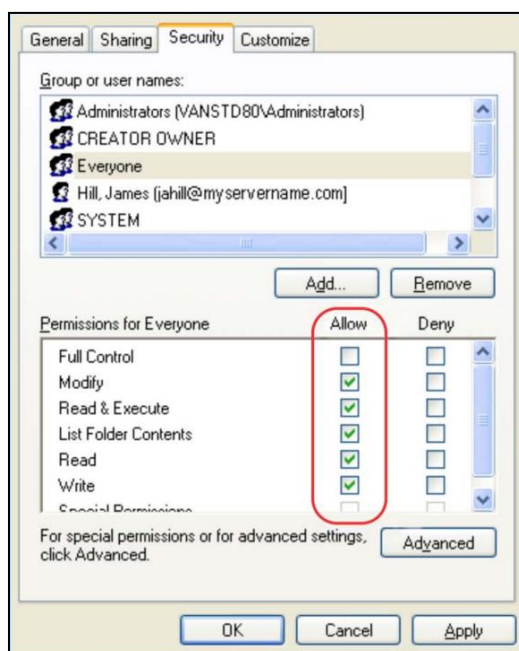
Preparing a Root Directory

To prepare a root directory:

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

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

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

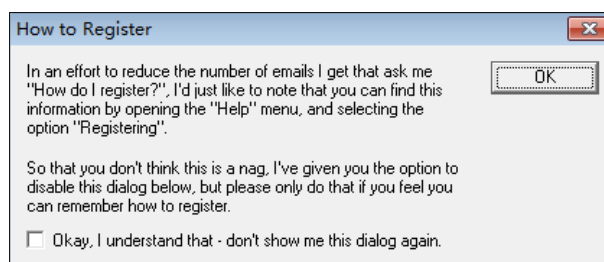


Configuring an FTP Server

To configure a wftpd server:

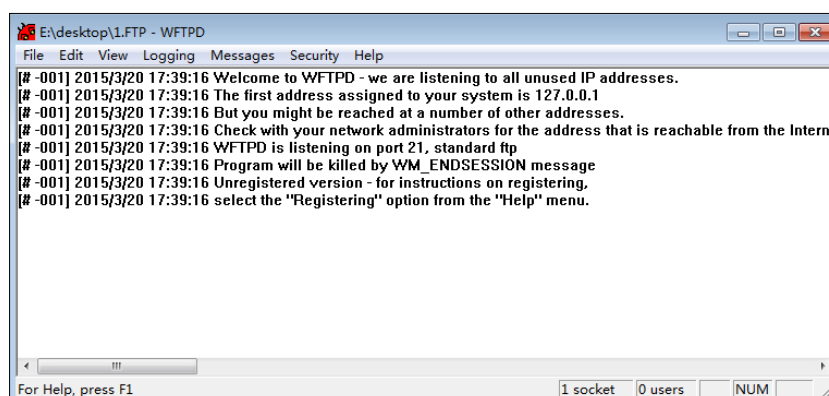
1. Download the compressed file of the wftpd application to your local directory and extract it.
2. Double click the WFTPD.EXE.

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

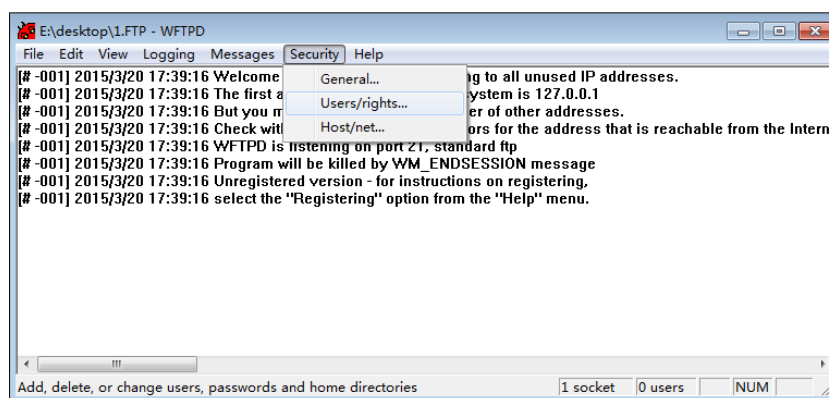


3. Check the check box and click **OK** in the pop-up dialogue box.

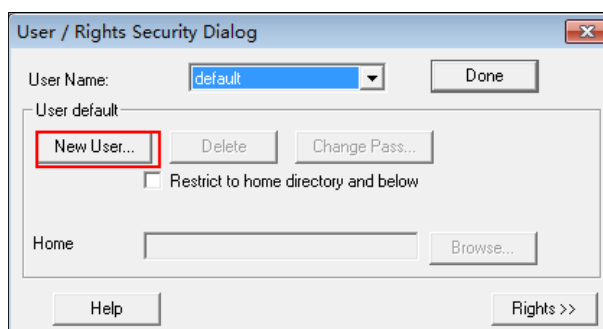
The log file of the wftpd application is shown as below:



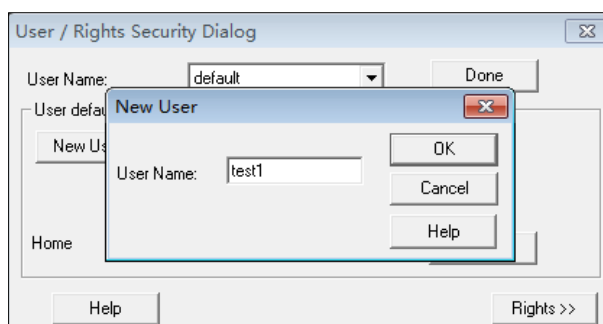
4. Click **Security->Users/rights**.



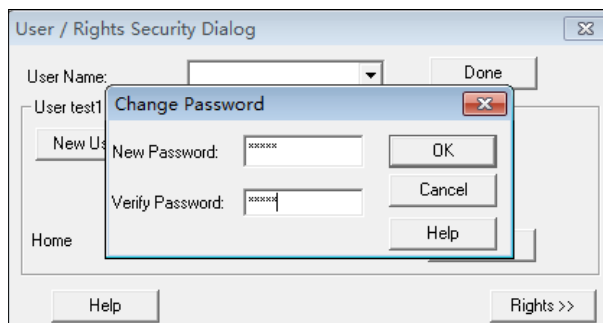
- Click **New User**.



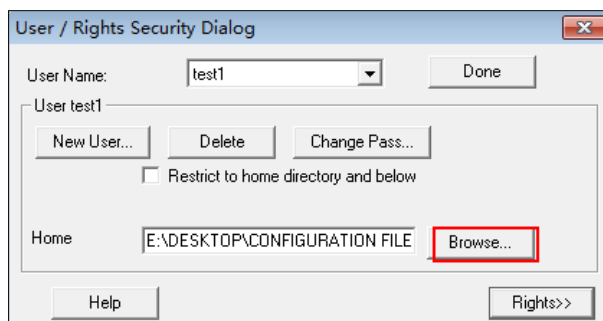
- Enter a user name (e.g., test1) in the **User Name** field and then click **OK**.



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



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



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



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 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>.

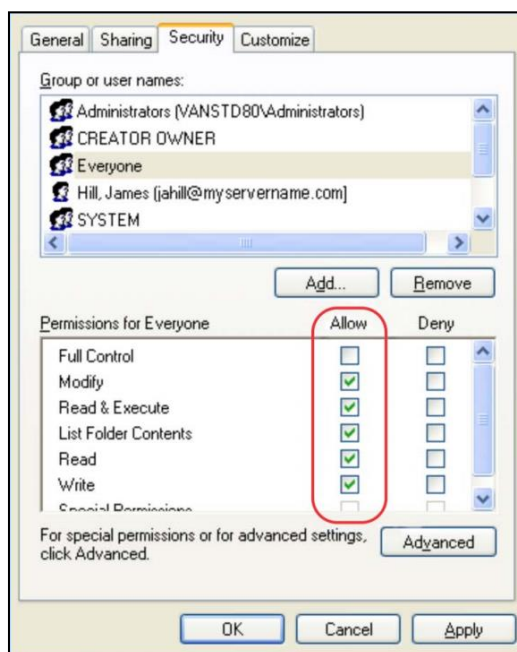
Preparing a Root Directory

To prepare a root directory:

1. Create an HTTP root directory on the local system (e.g., D:\HTTP Directory)..
2. Place 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:



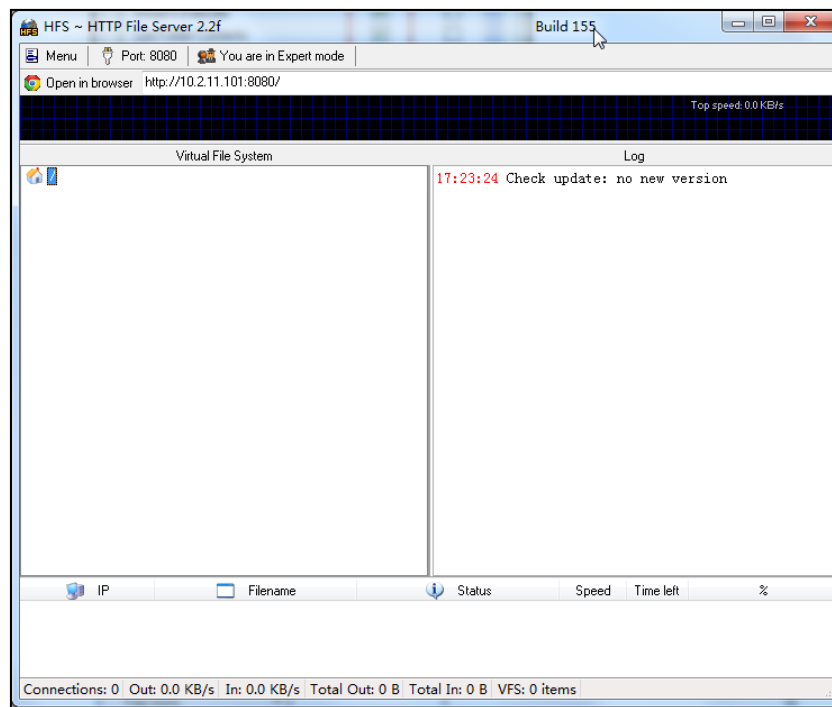
Configuring an HTTP Server

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

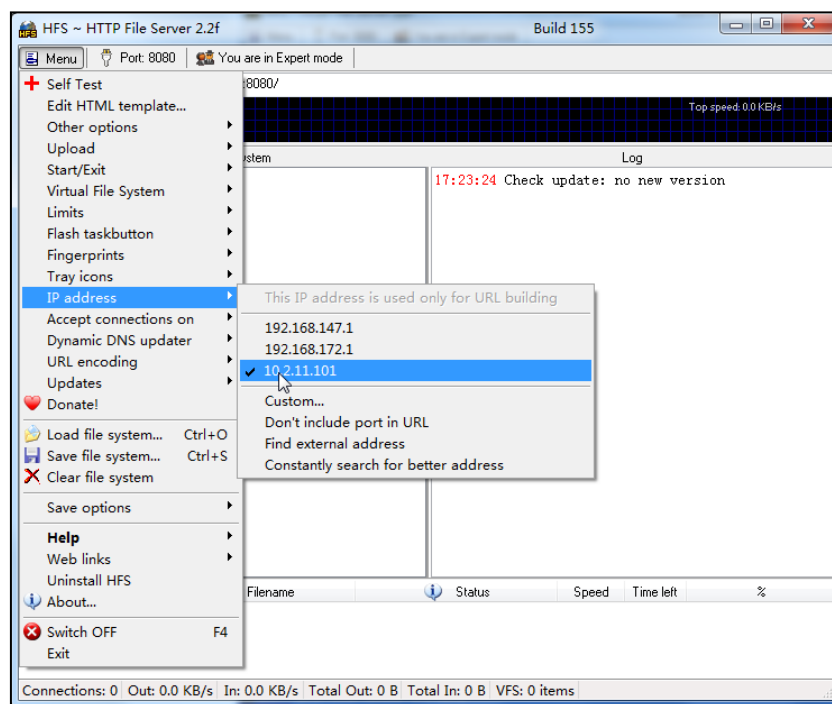
To configure an HTTP server:

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

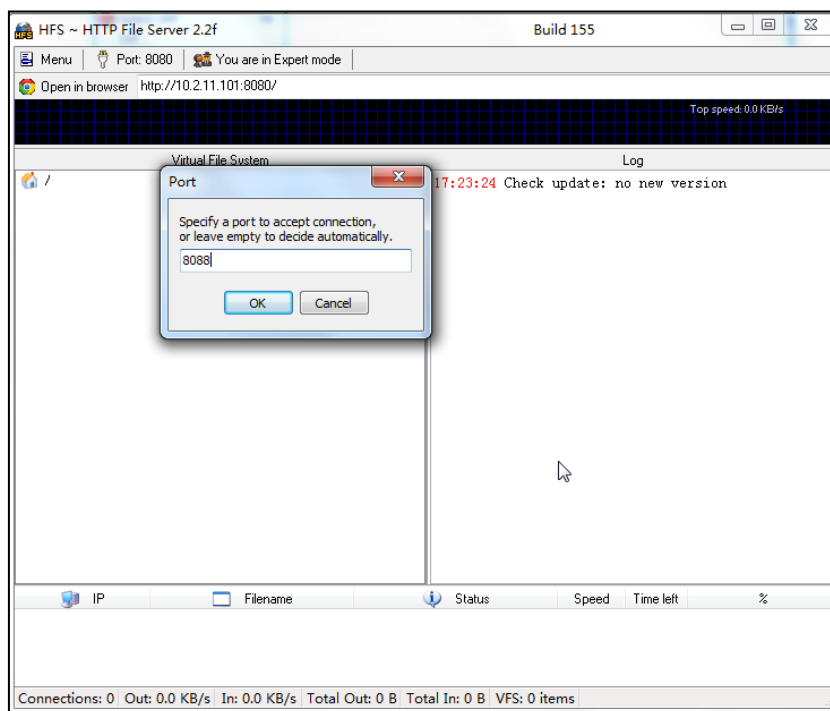
The main configuration page is shown as below:




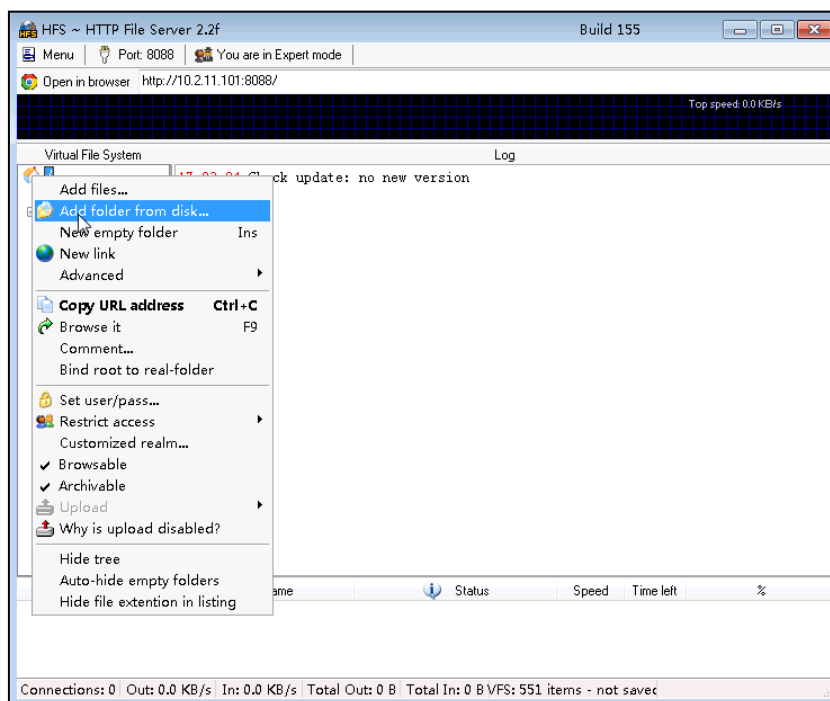
2. Click **Menu** in the main page and select the IP address of the PC from **IP address**.



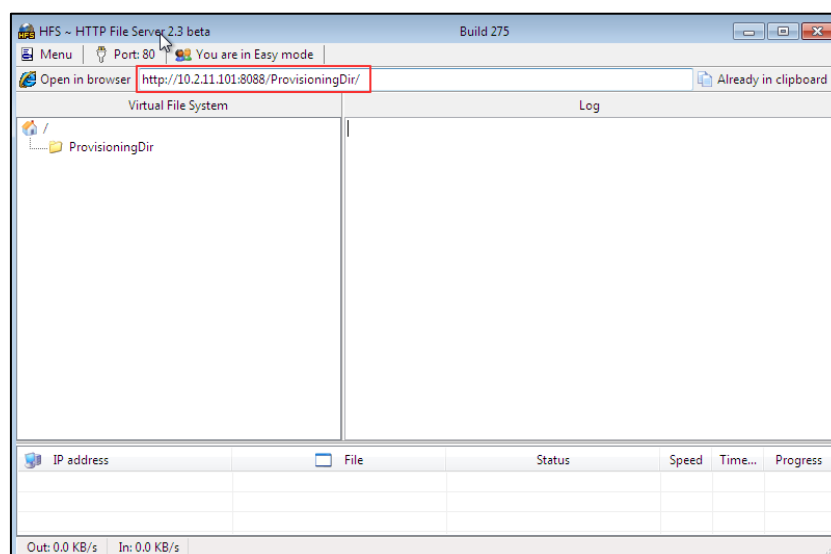
The default HTTP port is 8080. You can also reset the HTTP port (make sure there is no port conflict).



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



4. Locate the root directory from your local system.



5. Check the server URL (e.g., [http:// 10.2.11.101:8088/ProvisioningDir/](http://10.2.11.101:8088/ProvisioningDir/)) by clicking “Open in browser”.

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.

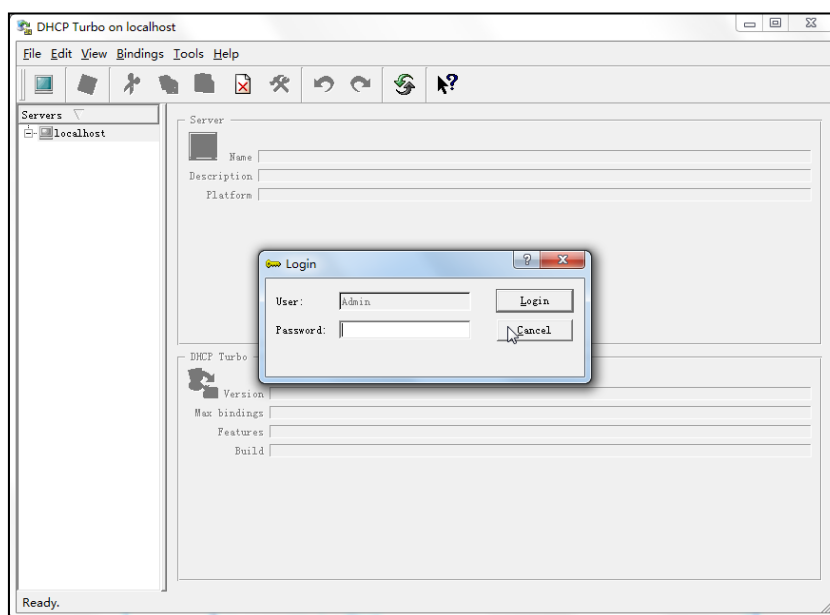
Before configuring the DHCP Turbo, make sure:

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

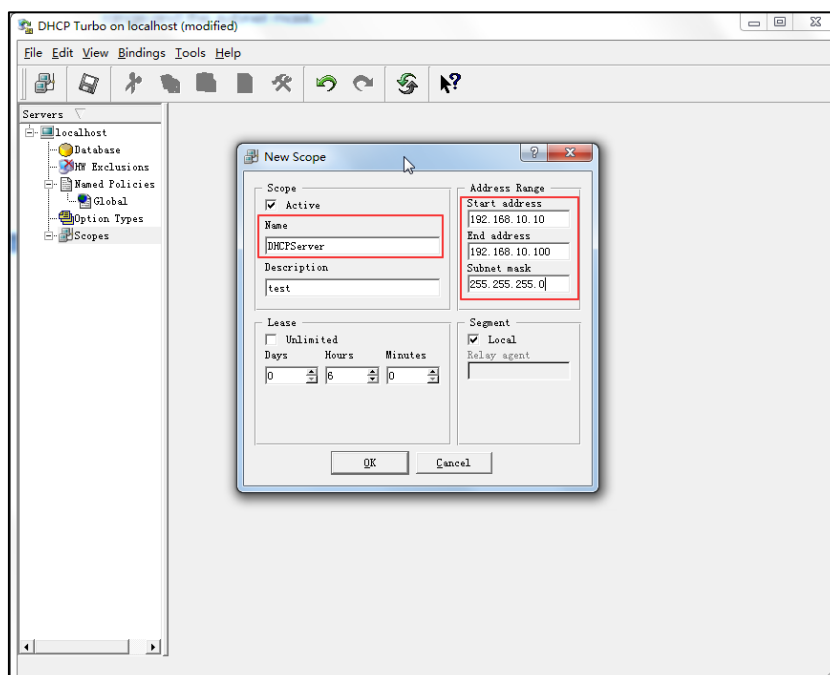
To configure the DHCP Turbo:

1. To start the DHCP Turbo application, double click **localhost**.

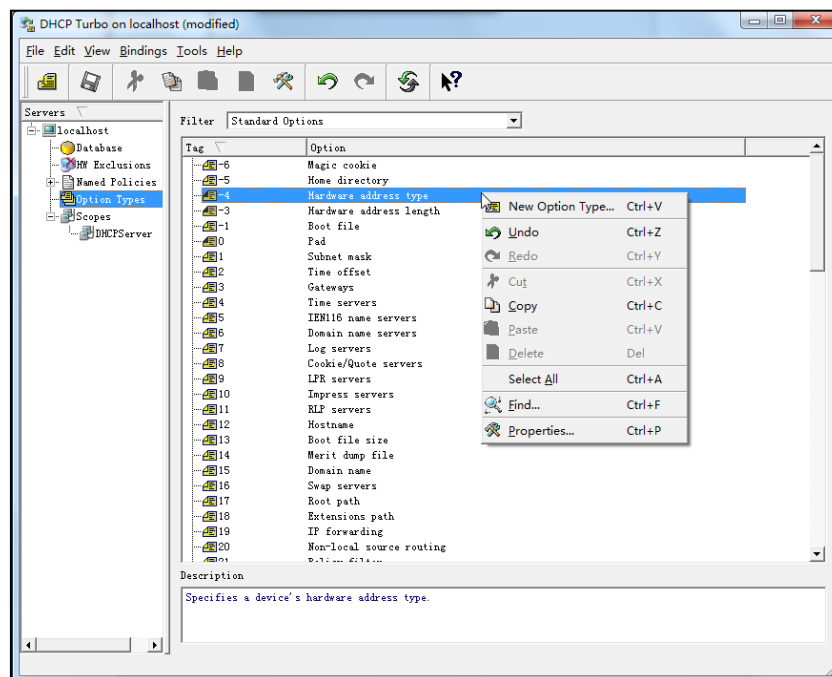
- Click the **Login** button (the login password is blank) to log in.




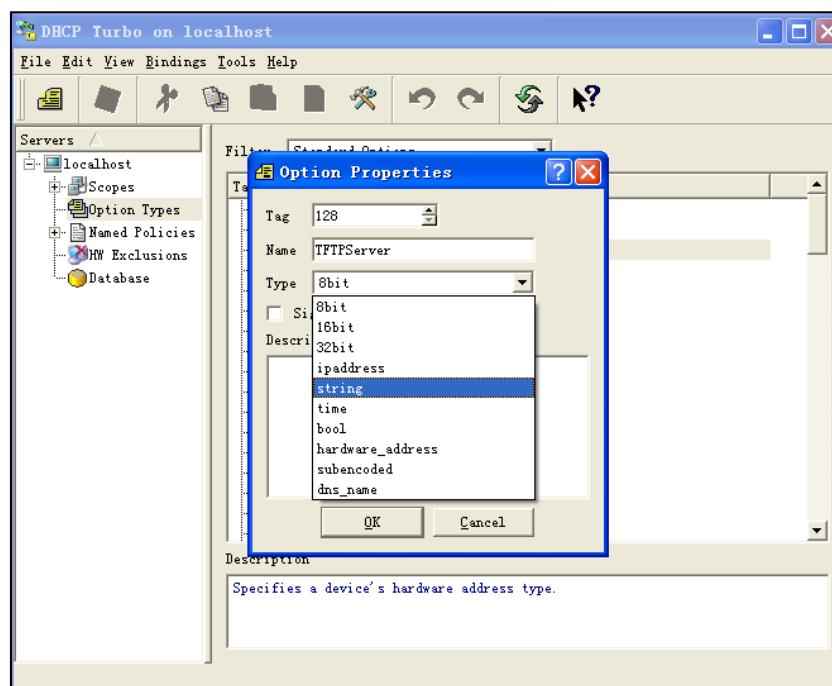
- Right click **Scopes** and select **New Scope**.
- Configure the DHCP server name, the DHCP IP range and the subnet mask.
- Click **OK** to accept the change.



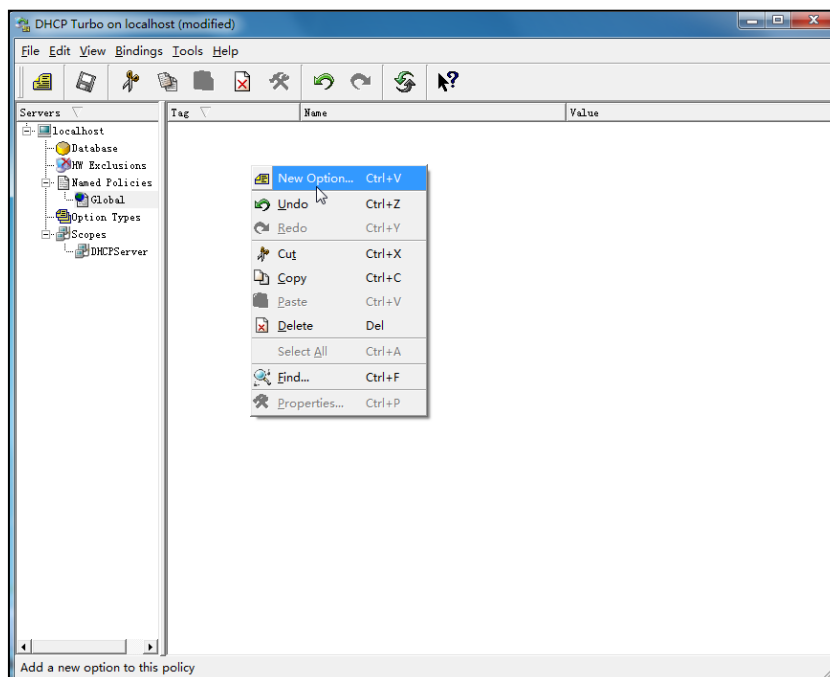
- You can add a custom option via DHCP Turbo. Select **Option Types**, right click one of the options on the right of the main page, and then select **New Option Type**.



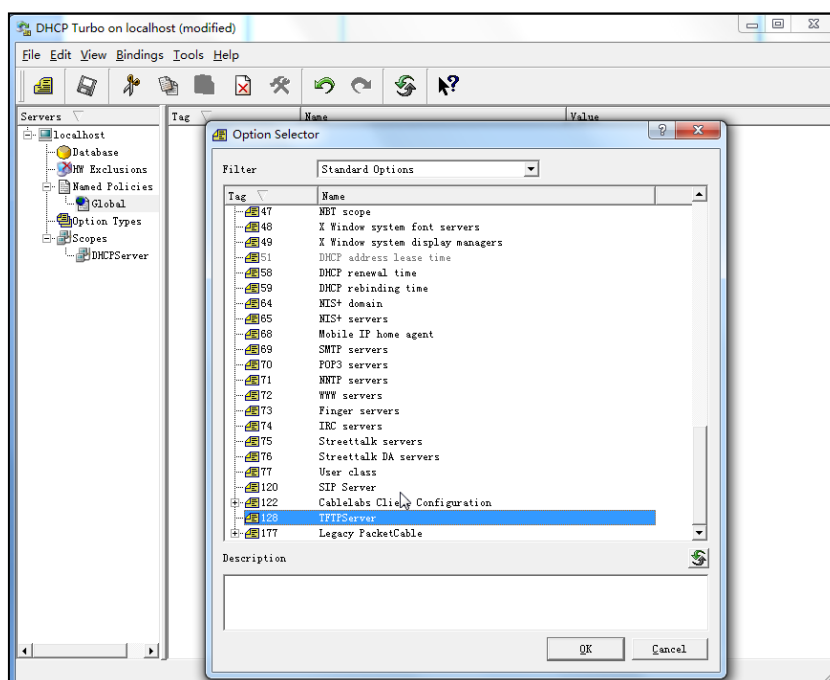
- Set the custom DHCP option (custom DHCP option tag number ranges from 128 to 254) and select the option type (Yealink supports **String** and **IP Address** option types only). Click the **OK** button to finish setting the option properties. Click  to save the change.



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

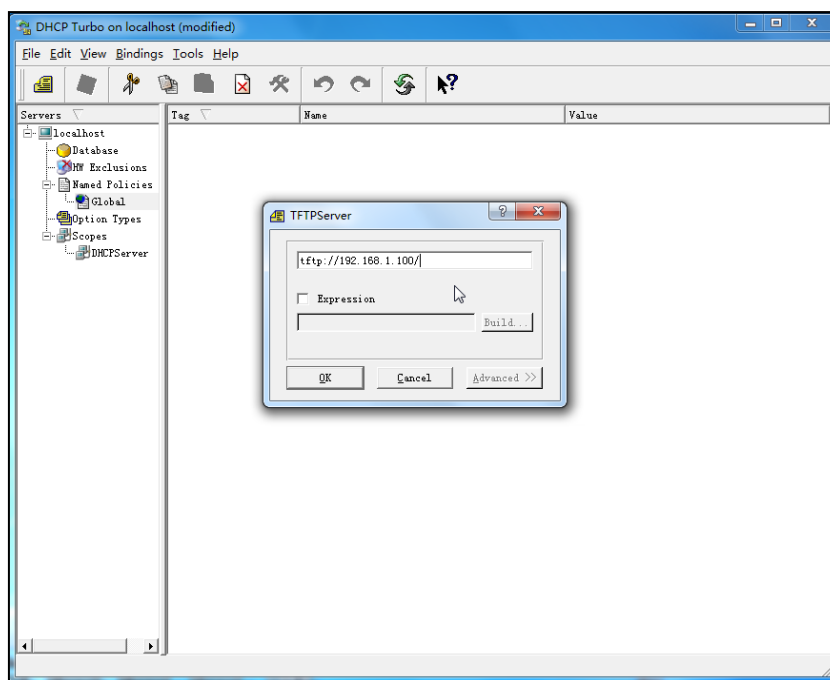



9. Scroll down and double click the custom option 128.



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

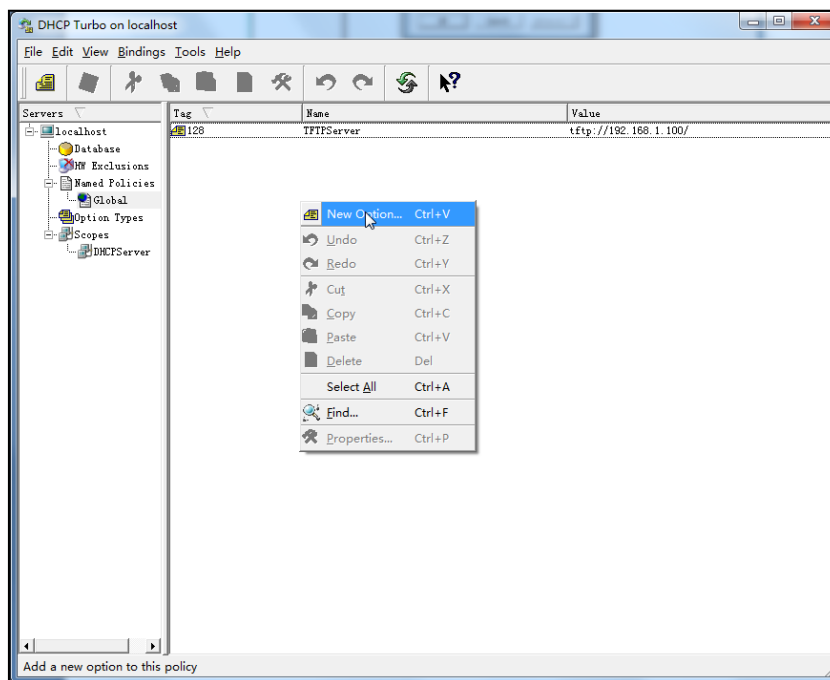
11. Click the **OK** button to finish setting a custom option.



12. Click  to save the change.

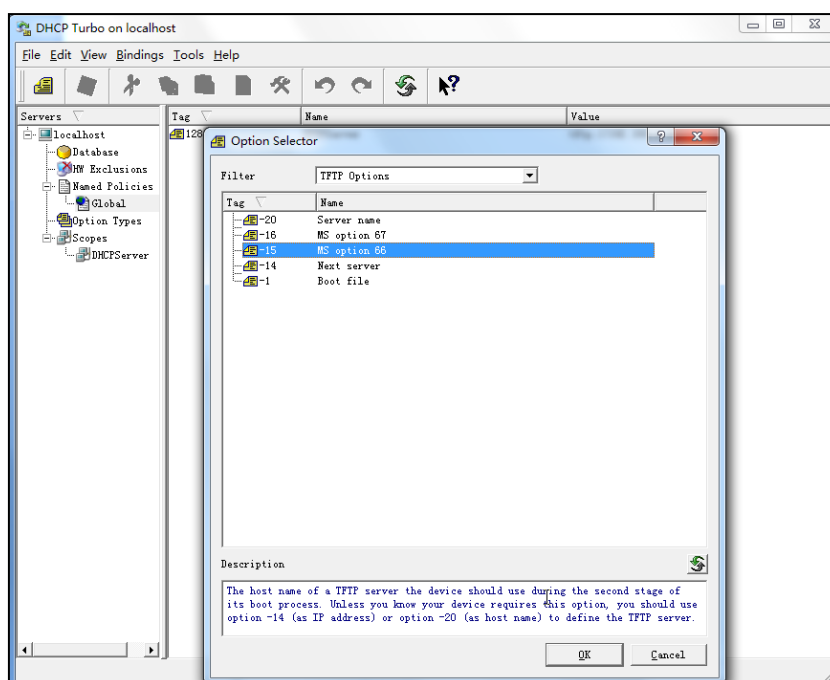
You can add the option 66 via DHCP Turbo. The following shows the detailed processes.

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

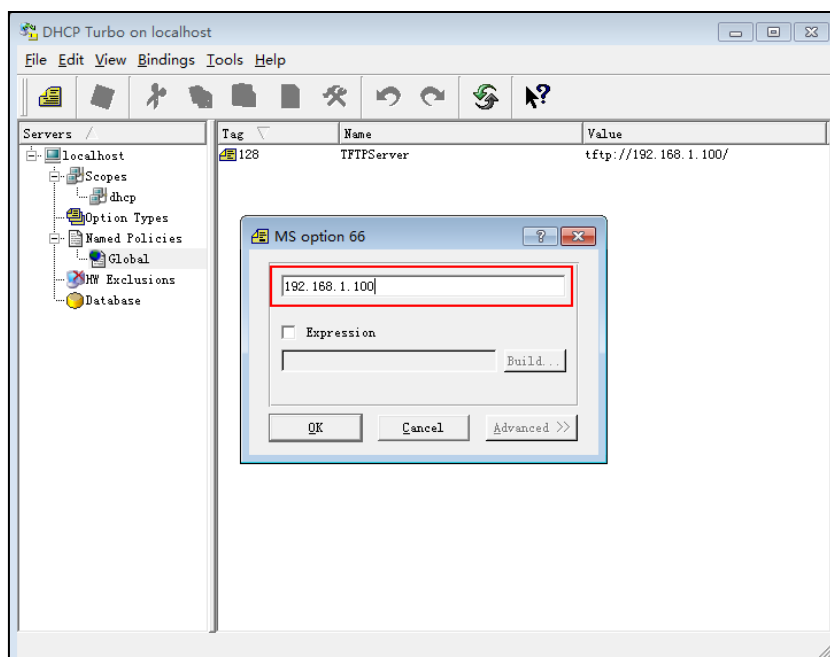



2. Select **TFTP Options** from the pull-down list of **Filter**.

3. Scroll down and double click **MS option 66**.



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

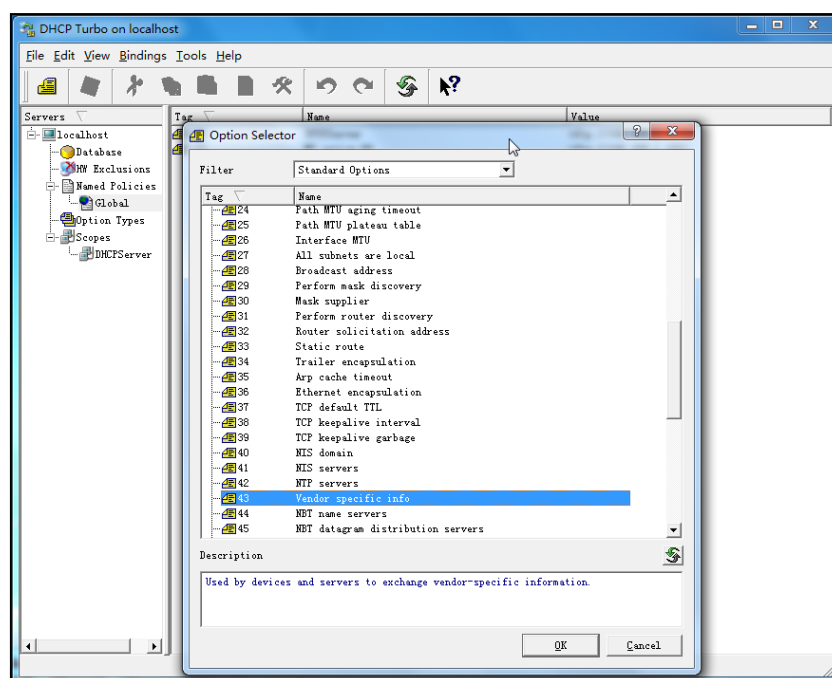


5. Click the **OK** button to finish setting a custom option.
6. Click  to save the change.

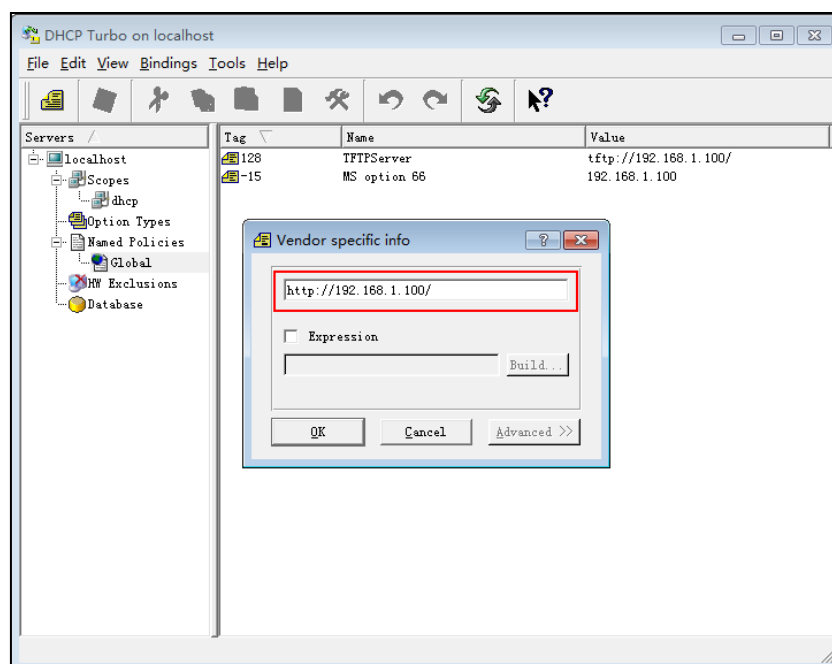
You can also add the option 43. The following shows the detailed processes.


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.



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



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.