Yealink

Teams® HD IP Phone
Auto Provisioning Guide

Table of Contents

Introduction

Yealink IP phones with Teams firmware enable a new era in unified communications. It is designed to work with Microsoft® Teams.

Yealink Teams 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 configure Yealink Teams IP phones with the minimum settings required. Yealink Teams IP phones support FTP, TFTP, HTTP, and HTTPS protocols for auto provisioning and are configured to use the TFTP protocol by default.

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

- Yealink T58A

- Yealink T56A

- Yealink T55A

- Yealink CP960

- Yealink VP59

- Yealink MP54

- Yealink MP56

- Yealink MP58

- Yealink MP58-WH

> The auto provisioning process outlined in this guide applies to Yealink T58A/T56A/T55A/CP960 Teams phones running firmware version x.15.0.20 or later, VP59 Teams phones running firmware version x.15.0.16 or later, MP56 Teams phones running firmware version x.15.0.6 or later, and MP54/MP58/MP58-WH Teams phones running firmware version x.15.0.33 or later. We recommend that Teams 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 Boot, Configuration and Resource Files

- Obtaining Phone Information

Obtaining Boot, Configuration and Resource Files

Boot Files

The phone tries to download the boot file first, and then download the configuration files referenced in the boot file during auto provisioning. You can select whether to use the boot file or not according to your deployment scenario. If required, you need to obtain the template boot file named as "y000000000000.boot" before auto provisioning.

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

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

Configuration Files

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

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

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

Resource Files

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

Yealink supplies the following resource file templates:

Feature	Template File Name
DST	AutoDST.xml
Language Packs	For example, 000.GUI.English.lang 1.English_note.xml 1.English.js

Obtaining Template Files

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

To download template boot, configuration and resource files:

1. Go to Yealink Document Download page and select the desired phone model.
2. Download and extract the combined template files to your local system.
3. Open the folder you extracted and identify the files you want to edit.

Obtaining Phone Information

Before beginning provisioning, you also need the phone information. For example: MAC address, hardware version and account information of the Teams IP phone.

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

Hardware version: The current hardware version of the Teams IP phone. You can view it via phone user interface or web user interface.

Online Account Information: Ask your system administrator Teams online account information.
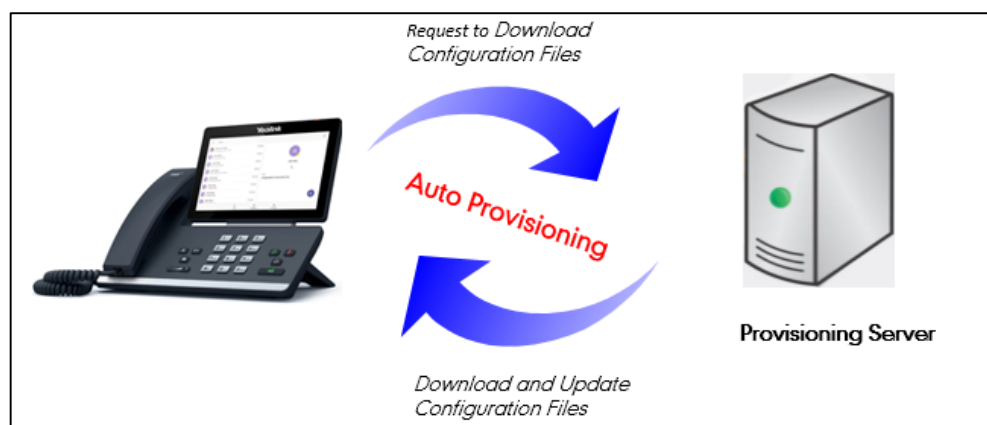
Provisioning Yealink Teams IP phones

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

Interoperating with Provisioning Server

When Teams 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 phone will download and update configuration files to the phone flash.

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

Auto Provisioning Process
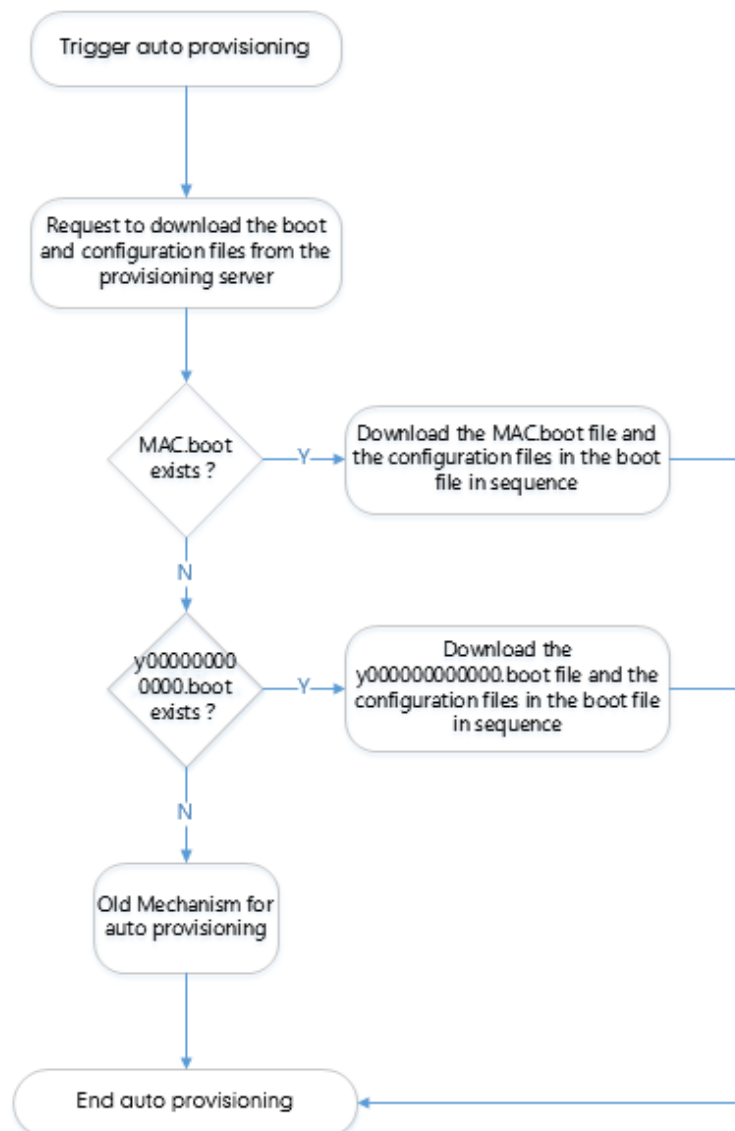
Without Boot Files (Old Mechanism)

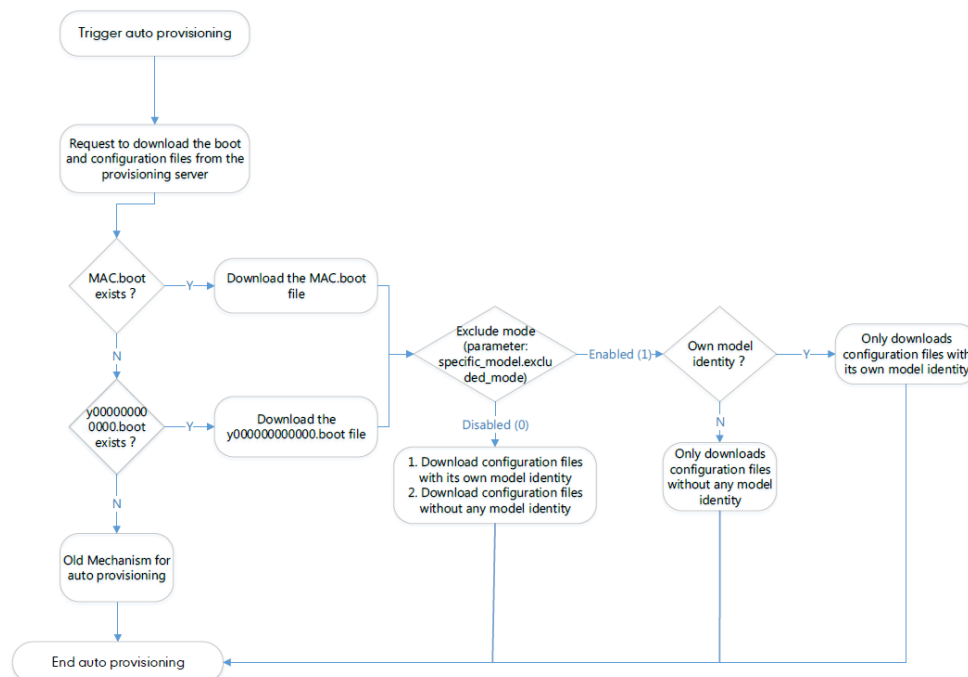The following flowchart shows how Teams IP phones perform auto provisioning when using configuration files only:

With Boot Files (New Mechanism)

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

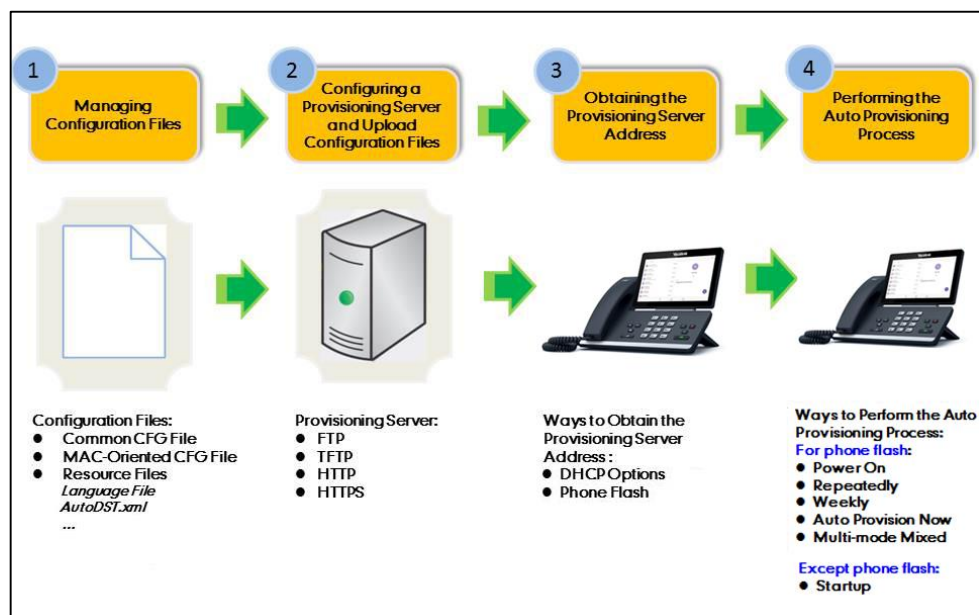**Scenario A – Do Not Support Exclude Mode**

Scenario B – Support Exclude Mode

Major Tasks for Auto Provisioning

You need to complete four major tasks to configure Yealink Teams IP phones.

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

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

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

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

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

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

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

An Instance of Auto Provision Configuration

This section shows an instance of auto provision configuration.

1. Manage boot files.

    Specify the desired URL (e.g., http://10.82.24.5/y000000000058.cfg) of the configuration files in the boot file (e.g., y000000000000.boot). For more information, refer to Managing Boot Files.

```
#!version:1.0.0.1
## The header above must appear as-is in the first line


##[$MODEL]include:config <xxx.cfg>
##[$MODEL,$MODEL]include:config "xxx.cfg"

[T58A]include:config <tftp://10.82.24.5/y000000000058.cfg>
[T58A,CP960]include:config <tftp://10.82.24.5/Autop.cfg>
include:config "features.cfg"

overwrite_mode = 1
specific_model.excluded_mode=0
```
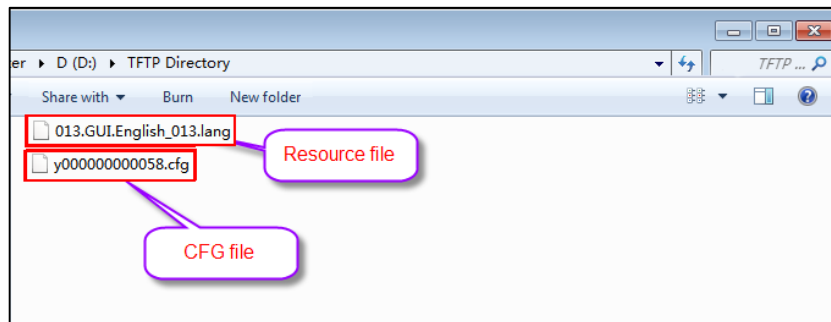
2. Manage configuration files.

    Add/Edit the desired configuration parameters in the CFG file (e.g., y000000000058.cfg) you want the phone to download. For more information on how to manage configuration files, refer to Managing Configuration Files.
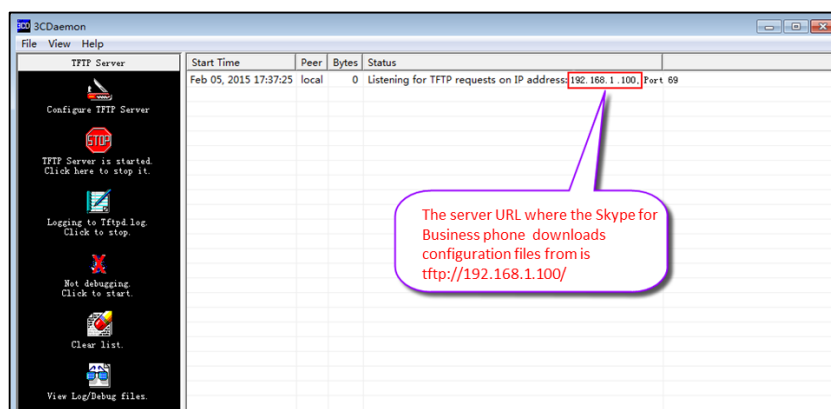
```
1 #!version:1.0.0.1
2 gui_lang.url =http://192.168.10.25/013.GUI.English_13.lang
```
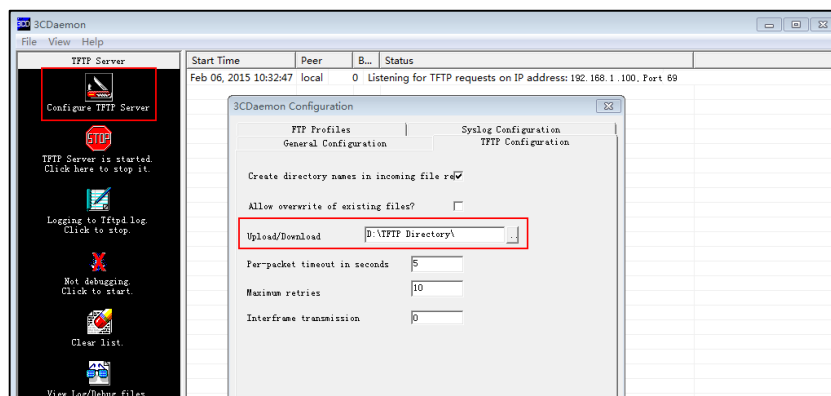
3. Configure the TFTP server.

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.

4. Configure the provisioning server address on the phone.

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

5. Trigger the phone to perform the auto provisioning.

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

Managing Boot Files

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

Yealink supports the following two types of boot files:

- Common boot file (y000000000000.boot)

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

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

Editing Common Boot File

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

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

```
1 #!version:1.0.0.1
2 ## The header above must appear as-is in the first line
3
4
5 ##[$MODEL]include:config <xxx.cfg>
6 ##[$MODEL,$MODEL]include:config "xxx.cfg"
7
8 include:config <xxx.cfg>
9 include:config "xxx.cfg"
10
11 overwrite_mode = 1
12 specific_model.excluded_mode=0
```

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

Item	Guidelines
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
## The header above must appear as-is in the first line	The line beginning with "#" is considered to be a comment. You can use "#" to make any comment in the boot file.
include:config <xxx.cfg> include:config "xxx.cfg"	1) Each "include" statement can specify a URL where a configuration file is stored. The configuration file format must be *.cfg. 2) The URL in <> or "" supports the following two forms: • Relative URL (relative to the boot file):

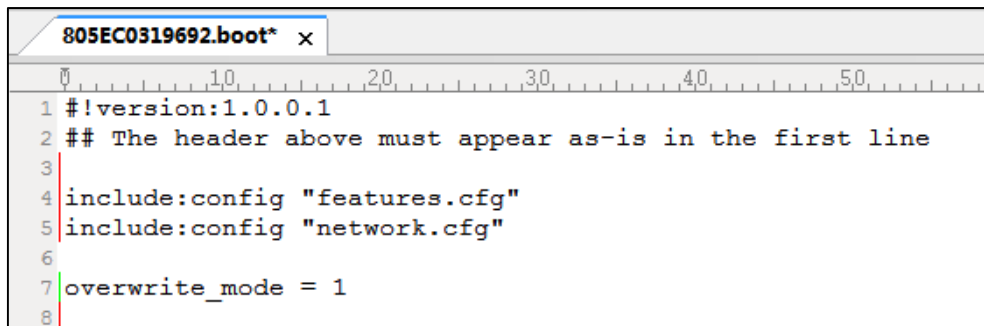| Item	Guidelines
	For example, sip.cfg, HTTP Directory/sip.cfg ● Absolute URL: For example, http://10.2.5.258/HTTP Directory/sip.cfg The URL must point to a specific CFG file. The CFG files are downloaded in the order listed (top to bottom). The parameters in the new downloaded configuration files will override the duplicate parameters in files downloaded earlier. 3) The "include" statement can be repeated as many times as needed. 4) The [$MODEL] can be added to specify settings for specific phone models. $MODEL represents the phone model name. The valid phone model names are: MP54, MP56, MP58, MP58-WH, T58A, T56A, T55A, VP59 and CP960. Multiple phone models are separated by commas. For example, [T58A, CP960]
overwrite_mode	Enable or disable the overwrite mode. The overwrite mode is applied to the configuration files specified to download. Note that it only affects the parameters pre-provisioned via central provisioning. **1**-(Enabled) - If the value of a parameter in configuration files is left blank, or if a non-static parameter in configuration files is deleted or commented out, the factory default value takes effect. **0**-(Disabled) - If the value of a parameter in configuration files is left blank, deleted or commented out, the pre-configured value is kept. **Note**: This parameter can only be used in boot files. If a boot file is used but the value of the parameter "overwrite_mode" is not configured, the overwrite mode is enabled by default.
specific_model.excluded _mode	Enable or disable the exclude mode. The exclude mode applies to the configuration files specified in the boot file. **0**-Disabled (Append Mode), the phone downloads its own model-specific configuration files, and downloads other model-unspecified configuration files. **1**-Enabled (Exclude Mode), the phone attempts to download its own model-specific configuration files; if there is no own model-specific configuration files found on the server, it downloads model-unspecified configuration files. **Note**: Exclude mode can only be used in boot files. If a boot file is used but the value of the parameter "specific_model.excluded_mode" is not configured, the exclude mode is disabled by default.

Creating MAC-Oriented Boot File

The MAC-Oriented boot file is only effective for the specific phone. It uses the 12-digit MAC address of the IP phone as the file name. For example, if the MAC address of the phone is 805EC0319692, the MAC-Oriented boot file has to be named as 805EC0319692.boot (case-sensitive) respectively.

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

To create a MAC-Oriented boot file:

1. Create a boot file for your phone. Ensure the file complies with the guidelines that are listed in Editing Common Boot File.

2. Copy the contents from the common boot file and specify the configuration files to be downloaded.

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

```
805EC0319692.boot*  ×
0.........1.0.........2.0.........3.0.........4.0.........5.0.........
1 #!version:1.0.0.1
2 ## The header above must appear as-is in the first line
3
4 include:config "features.cfg"
5 include:config "network.cfg"
6
7 overwrite_mode = 1
8
```

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

You can edit the template 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 the latest Administrator Guide for your phone on Yealink Technical Support.

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 Teams IP phone model.

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

Phone Model	Common CFG file
T58A	y000000000058.cfg
T56A	y000000000056.cfg
T55A	y000000000099.cfg
CP960	y000000000073.cfg
VP59	y000000000091.cfg
MP58/MP58-WH	y000000000135.cfg
MP56	y000000000122.cfg
MP54	y000000000134.cfg

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

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

```
#!version:1.0.0.1

####################################################################################
##                                    lync                                        ##
####################################################################################
##It is used for importing license.
lync_license_dat.url =

####################################################################################
##                                  Hostname                                      ##
####################################################################################
##It configures the DHCP option 12 hostname on the IP phone.
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.
static.network.pc_port.enable =

##The default value is 0.It takes effect after a reboot.
static.network.internet_port.speed_duplex =
static.network.pc_port.speed_duplex =

##It enables or disables the phone to use manually configured static IPv4 DNS when Internet (WAN) port type for IPv4 is configured as DHCP.
##0-Disabled (use the IPv4 DNS obtained by DHCP)   1-Enabled
##The default value is 0.It takes effect after a reboot.
static.network.static_dns_enable =
static.network.ipv6_static_dns_enable =
```

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

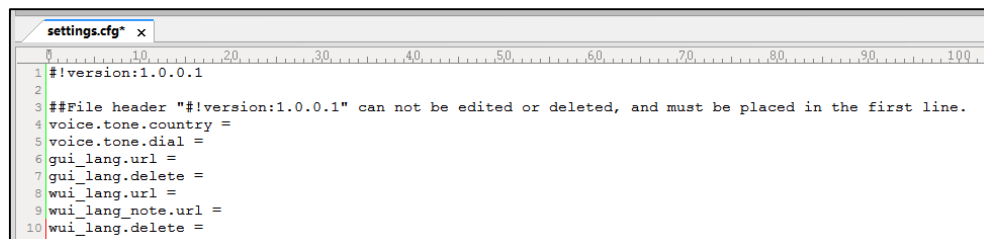| Item	Guidelines
#	The line beginning with "#" is considered to be a comment.
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
Filename	The filename complies with the requirements that are listed in the above table.
Line formats and Rules	Each line must use the following 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. • The [$MODEL] can be added to the front of configuration parameter to specify the value for specific phone groups. $MODEL represents the phone model. The valid phone models are: MP54, MP56, MP58, MP58-WH, T58A, T56A, T55A and CP960. Multiple phone models are separated by commas. For example, [T58A, CP960]. **Note**: The phone updates model-specific configurations and those model-unspecified configurations.

Editing MAC-Oriented CFG File

The MAC-Oriented CFG files are only effectual for the specific phone. They use the 12-digit MAC address of the phone as the file name. For example, if the MAC address of the 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:

```
1    #!version:1.0.0.1
2
3    ##File header "#!version:1.0.0.1" can not be edited or deleted, and must be placed in the first line.##
4
5    ##############################################################################
6    ##                              Time                                        ##
7    ##############################################################################
8    ##It configures the time zone.For more available time zones, refer to Time Zones on page 215.
9    ##The default value is +8.
10   local_time.time_zone =
11   ##It configures the time zone name.For more available time zone names, refer to Time Zones on page 215.
12   ##The default time zone name is China(Beijing).
13   local_time.time_zone_name =
14
15
16   local_time.ntp_server1 =
17   local_time.ntp_server2 =
18   ##It configures the update interval (in seconds) when using the NTP server.
19   ##The default value is 1000.Integer from 15 to 86400
20   local_time.interval =
21
22   ##It enables or disables daylight saving time (DST) feature.
23   ##0-Disabled,1-Enabled,2-Automatic.
24   ##The default value is 2.
25   local_time.summer_time =
26
27   ##It configures the way DST works when DST feature is enabled.
28   ##0-DST By Date ,1-DST By Week.
29   ##The default value is 0.
30   local_time.dst_time_type =
```

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

Item	Guidelines
#	The line beginning with "#" is considered to be a comment.
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
Filename	The filename matches the MAC address of your phone.
Line formats and Rules	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.

Item	Guidelines
	• The [$MODEL] can be added to the front of configuration parameter to specify the value for specific phone groups. $MODEL represents the phone model. The valid phone models are: MP58, MP58-WH, MP56, MP54, T58A, T56A, T55A, VP59 and CP960. Multiple phone models are separated by commas. For example, [T58A, CP960]. **Note**: The phone updates model-specific configurations and those model-unspecified configurations.

Creating a New CFG File

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

To create a new CFG file:

1. Create a CFG file for your phone. Ensure the file complies with the guidelines that are listed in Editing Common CFG File or Editing MAC-Oriented CFG File.

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. This file enables the phone to keep user's personalization settings, even after auto provisioning. As with the MAC-Oriented CFG files, MAC-local CFG files are only effective for the specific phone. They use the 12-digit MAC address of the IP phone as the file name. For example, if the MAC address of the phone is 00156574B150, MAC-local CFG file has to be named as 00156574b150-local.cfg (case-sensitive).

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

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

> We recommend you do not edit the MAC-local CFG file. If you really want to edit MAC-local CFG file, you can export and then edit it.
> For more information on how to export CFG files, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

Encrypting Configuration Files

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

Managing Resource Files

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

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

Customizing Resource Files

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

Template File	File Name
AutoDST Template	AutoDST.xml
Language Packs	For example, 000.GUI.English.lang 1.English.js

Ask the distributor or Yealink FAE for resource file templates. For more information on explanations of the configuration parameters, refer to *Yealink Teams HD IP Phones Administrator Guide*.

Configuring a Provisioning Server

Yealink Teams 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 TFTPD32 as a TFTP server. 3CDaemon and TFTPD32 are free applications for Windows. You can download 3CDaemon online: *http://www.oldversion.com/3Com-Daemon.html* and TFTPD32 online: *http://tftpd32.jounin.net/*.

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

Preparing a Root Directory

To prepare a root directory:

1. Create a TFTP root directory on the local system (e.g., D:\TFTP Directory).

2. Place the boot files, configuration files and resource 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 phone downloads configuration files from.

Obtaining the Provisioning Server Address

Yealink Teams IP phones support obtaining the provisioning server address in following ways:

- DHCP Options

- Phone Flash

The priority of obtaining the provisioning server address is as follows: DHCP Options (Custom option-->option 66-->option 43)-->Phone Flash.

The following sections detail the process of each way (take the T58A Teams IP phone as an example).

DHCP Options

Yealink Teams 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.

If DHCP option 66 and 43 are not available, you can configure the phone to obtain the provisioning server address via a custom DHCP option 160 or 161. 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.

To configure the DHCP option via web user interface:

1. Click on **Settings**->**Auto Provision**.
2. Enable the **DHCP Active**.

3. Enter the desired value in the **Custom Option(128~254)** field.

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 Teams 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 Teams HD IP Phones Administrator Guide*.

The following figure shows the example messages of obtaining the TFTP server address from a custom DHCP option 128:

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

To configure the phone flash via web user interface:

1. Click on **Settings**->**Auto Provision**.

2. 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).

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

After the above configuration is completed, the 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 and Multi-mode Mixed. For more information on these methods, refer to Triggering the Phone to Perform the Auto Provisioning.

Triggering the Phone to Perform the Auto Provisioning

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

● Power On

● Repeatedly

● Weekly

● Auto Provision Now

● Multi-mode Mixed

> When there is an active call on the 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 phone performs the auto provisioning process when the phone is powered on.

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

1. Click on **Settings**->**Auto Provision**.

2. Enable the **Power On**.

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

Repeatedly

The 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. Enable the **Repeatedly**.

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

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

Weekly

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

To activate the weekly mode via web user interface:

1. Click on **Settings**->**Auto Provision**.

2. Enable the **Weekly**.

3. Enter the desired time in the **Time** field.

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

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

Auto Provision Now

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

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

1. Click on **Settings**->**Auto Provision**.

2. Click **Auto Provision Now**.

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

Downloading and Verifying Configurations

Downloading Boot, Configuration and Resource Files

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

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

The phone downloads configuration files referenced in the boot file based on the value of the parameter "specific_model.excluded_mode". For more information, refer to With Boot Files (New Mechanism).

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 phone will reboot to make the configurations effective after the auto provisioning process is completed.

The 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 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 phone will update configurations.

The latest values applied to the phones are the values that take effect.

The phone will reboot when there is at least a specific configuration requiring a reboot after auto provisioning.

For more information on the specific configuration which require a reboot during auto provisioning, refer to the latest Administrator Guide for your phone on Yealink Technical Support.

If configuration files have been AES encrypted, the 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 phone decrypts configuration files, refer to *Yealink Configuration Encryption Tool User Guide*.

Using MAC-local CFG File

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

You can configure whether the 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 phone is configured to keep user's personalized settings (by setting the value of the parameter "static.auto_provision.custom.protect" to 1), it will update configurations in the <MAC>-local.cfg file. If the value of the parameter "overwrite_mode" is set to 1 in the boot file, the 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 the latest Administrator Guide for your phone on Yealink Technical Support.

Verifying Configurations

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

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

Example1: Yealink T58A Teams IP phone downloads configuration files from the TFTP server.

Example 2: Yealink T58A Teams IP phone downloads configuration files from the FTP server.

Example 3: Yealink T58A Teams IP phone downloads configuration files from the HTTP server.

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 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 phone are correct.

- Ensure that configuration files exist on the provisioning server.

Why does the 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 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 phone display "Network unavailable"?

- Ensure that the Ethernet cable is plugged into the Internet port on the phone and the Ethernet cable is not loose.

- Ensure that the switch or hub in your network is operational.

- Ensure 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 can't the phone obtain an IP address from the DHCP server?

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

Why can't the phone download the ring tone?

- Ensure that the file format of the ring tone is *.wav.
- Ensure that the size of the ring tone file is not larger than that the phone supports.
- Ensure that the properties of the ring tone for the 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 can't the phone update configurations?

- Ensure that the configuration files are different from the last ones.
- Ensure that the 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

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

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.

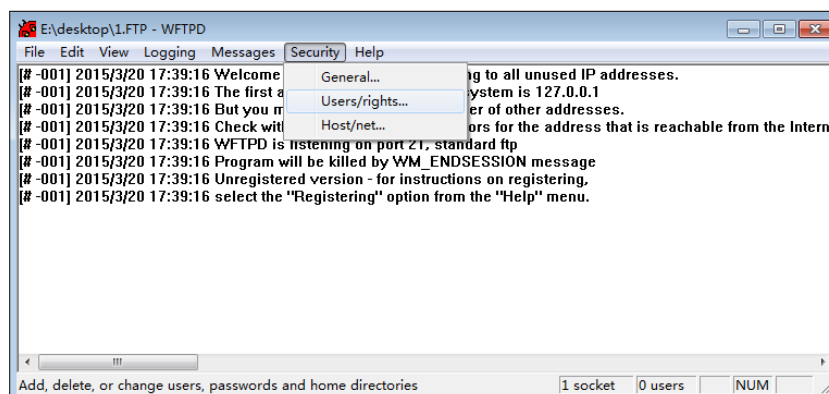   The dialogue box of how to register is shown as below:

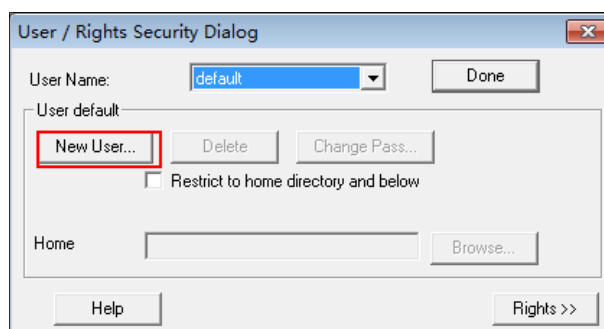3. Check the check box and click **OK** in the pop-up dialogue box.

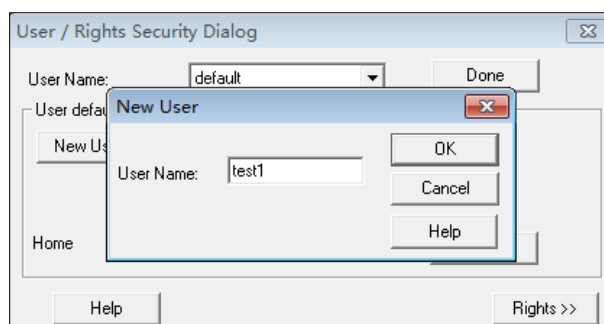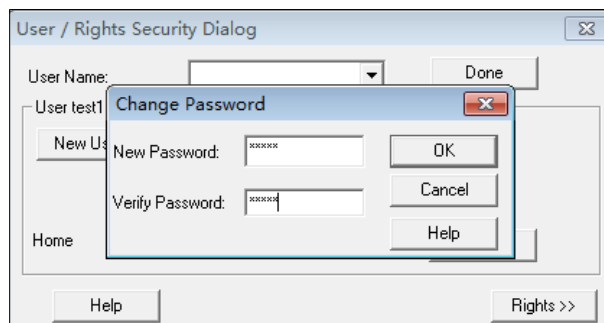   The log file of the wftpd application is shown as below:

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

5. Click **New User**.

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

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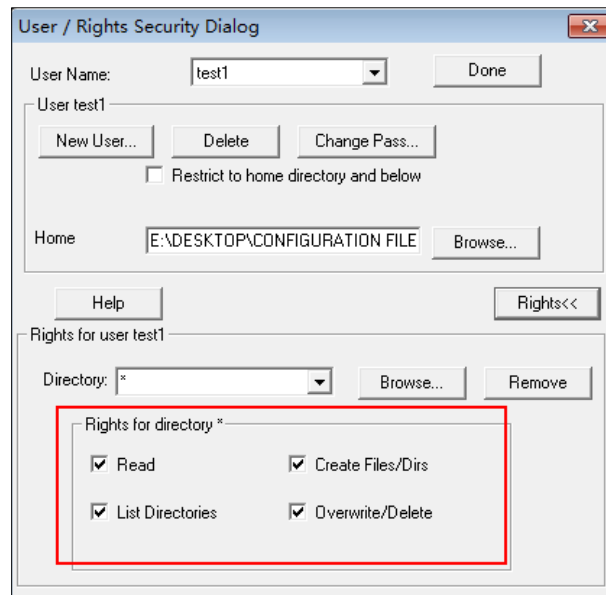

8. Click **Browse** to locate the FTP root directory from your local system.

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.

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 phone downloads configuration files from.

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.

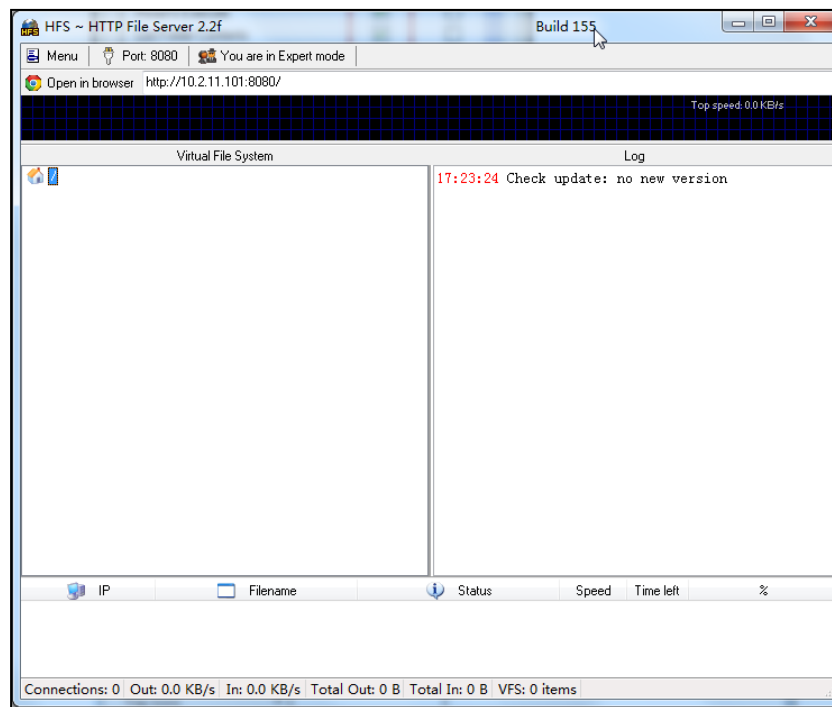An example of configuration on the Windows platform is shown as below:

Configuring an HTTP Server

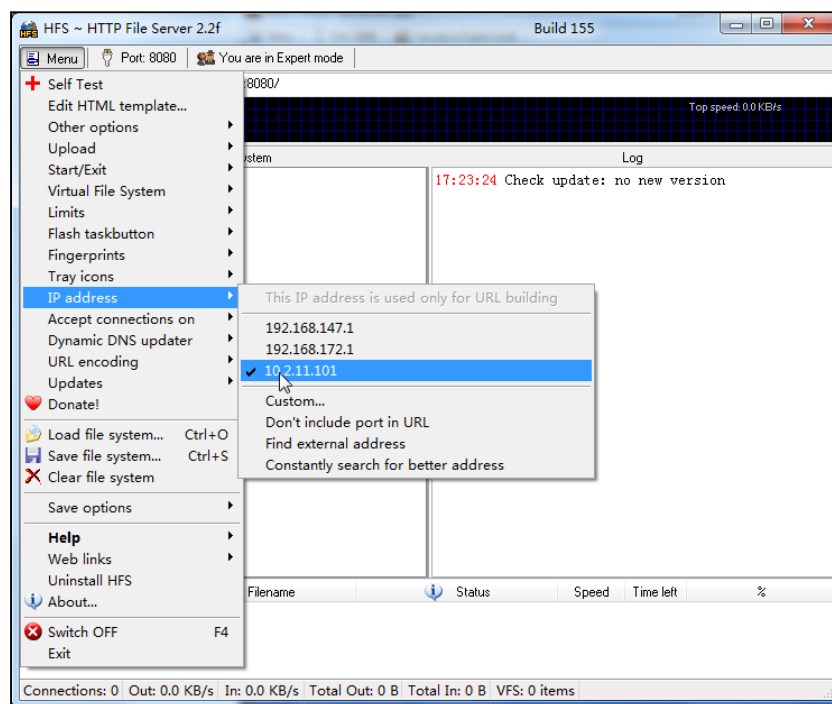HFS tool is an executable application, so you don't need to install it.

To configure an HTTP server:

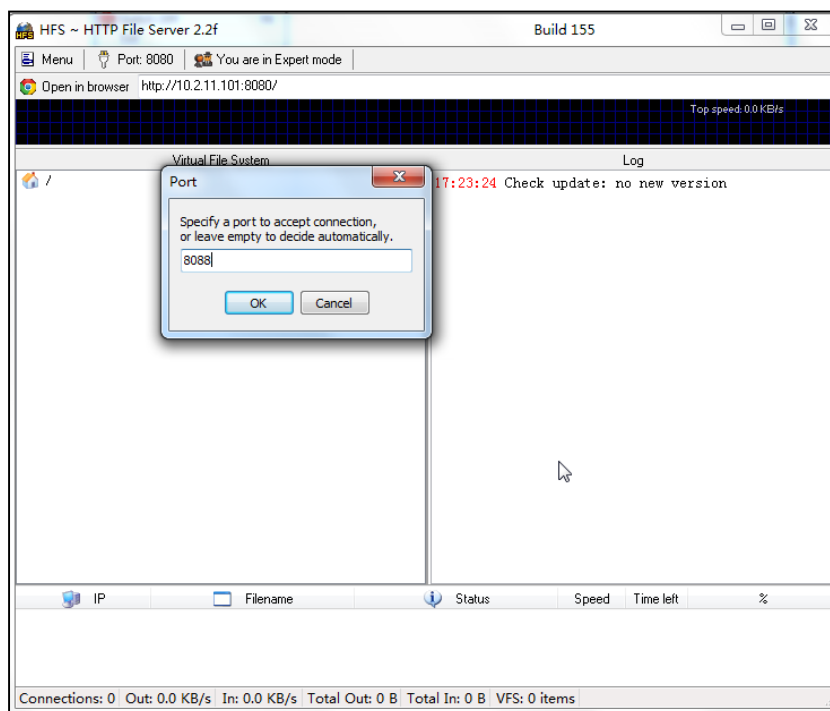1.   Download the application file to your local directory, double click the hfs.exe.
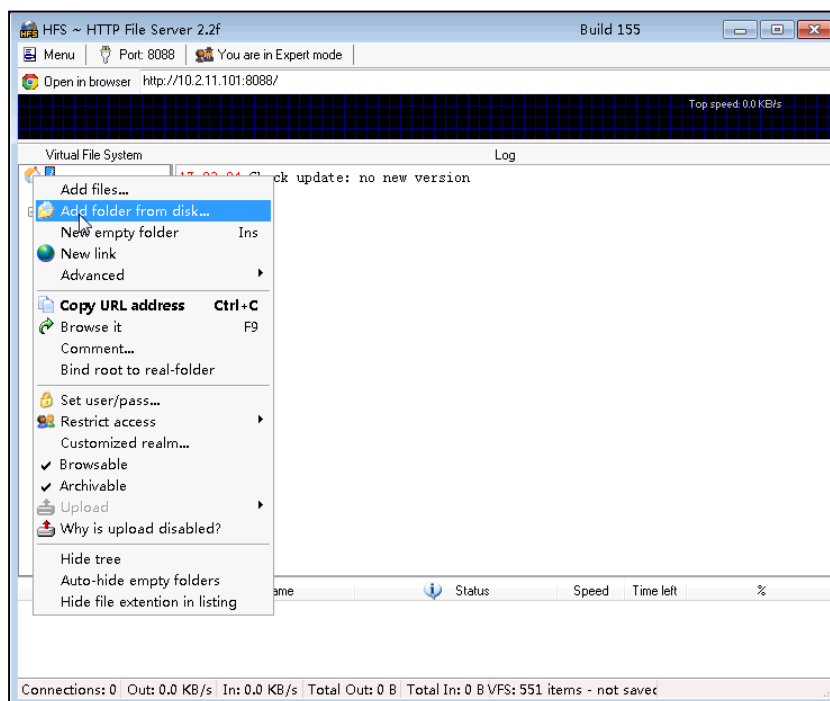
The main configuration page is shown as below:

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).
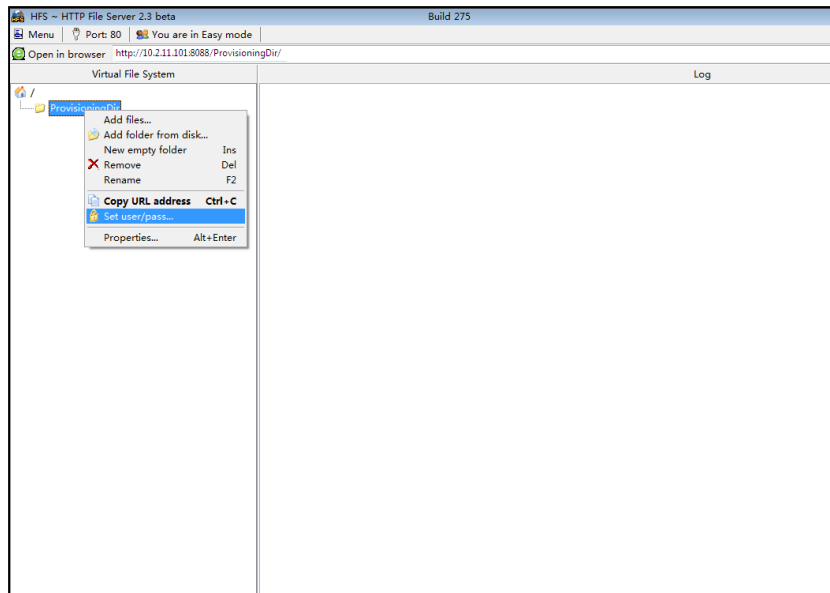

3. Right click the icon on the left of the main page, select **Add folder from disk** to add the HTTP Server root directory.
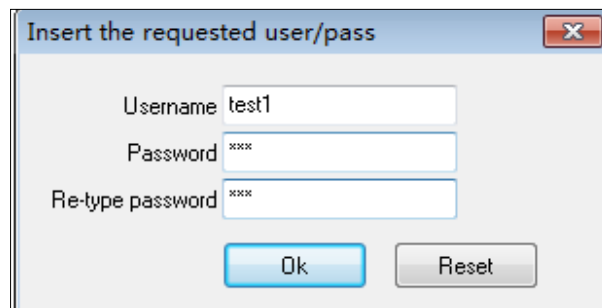

4. (Optional) Right-click on the directory to select **Set user/pass…** to configure a user name and password for the directory.

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

51

configuration files for different phones. To access the specified directory, you need to provide the correct user name and password configured for the directory.

5.   Enter a user name (e.g., test1) and password in the **User Name**, **New Password** and **Verify Password** fields respectively.

6.   Click **Ok**.

7. Locate the root directory from your local system.

8. Check the server URL (e.g., http:// 10.2.11.101:8088/ProvisioningDir) by clicking "**Open in browser**".

> Yealink Teams 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.

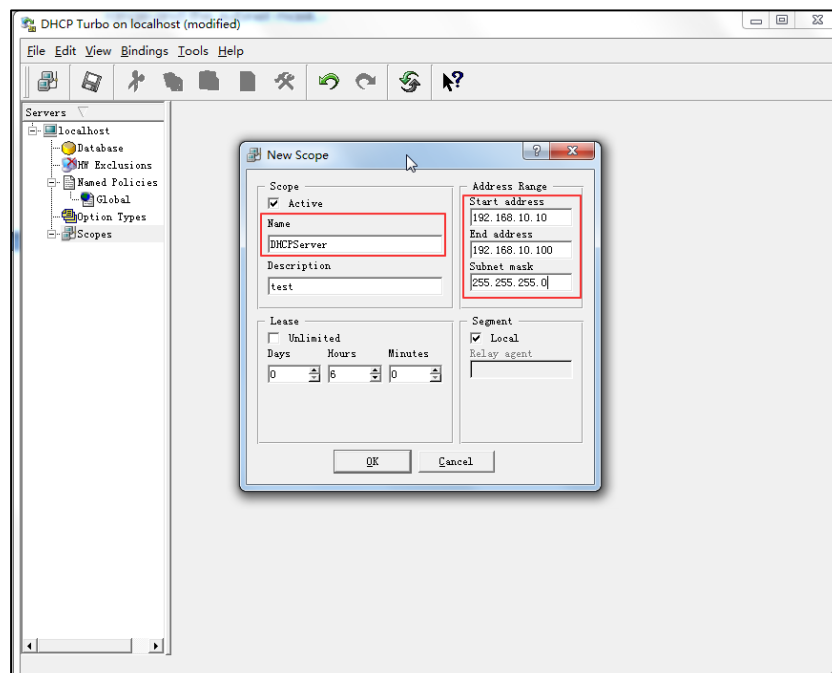- There is no DHCP server in your local system.

To configure the DHCP Turbo:

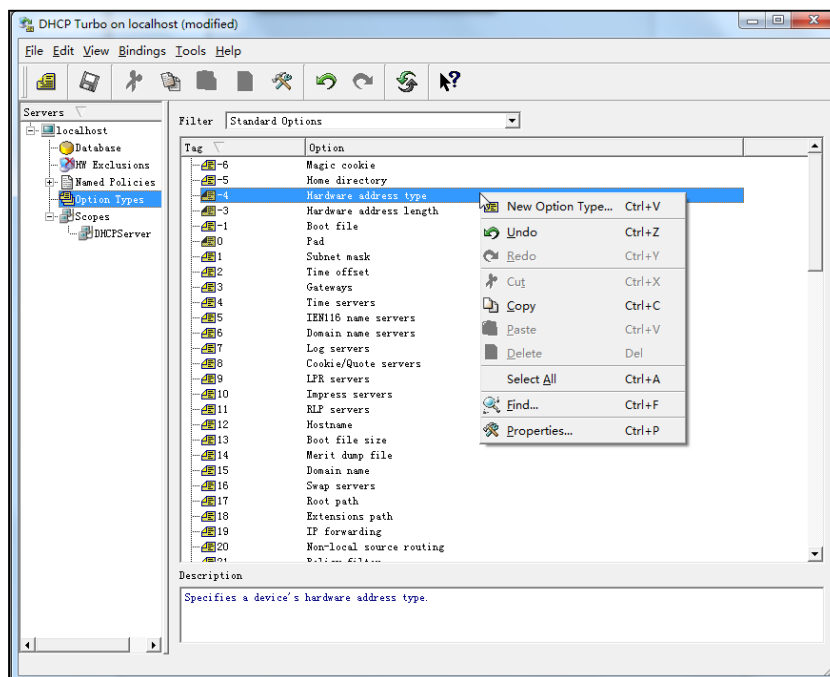**1.** To start the DHCP Turbo application, double click **localhost**.

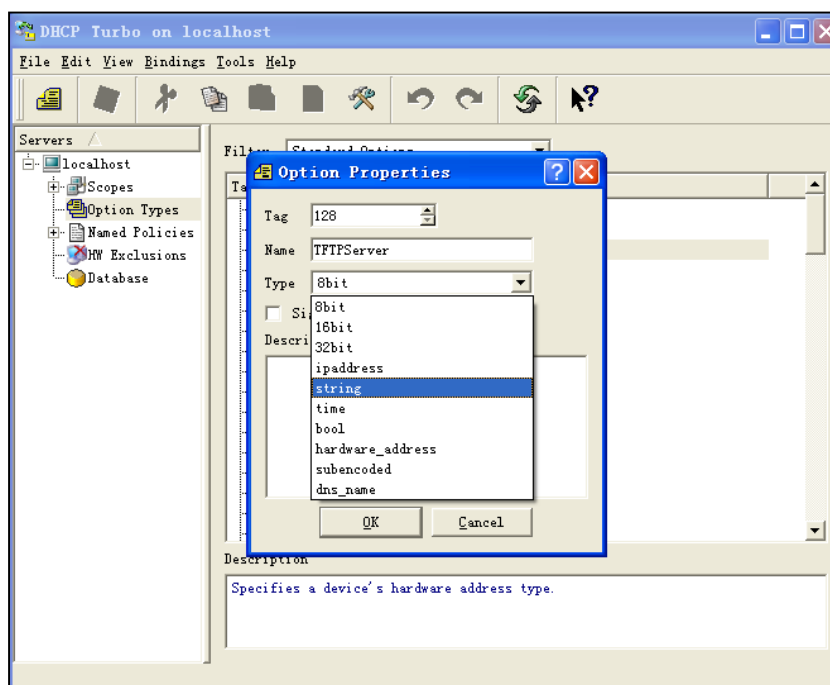**2.** Click the **Login** button (the login password is blank) to log in.

3. Right click **Scopes** and select **New Scope**.

4. Configure the DHCP server name, the DHCP IP range and the subnet mask.
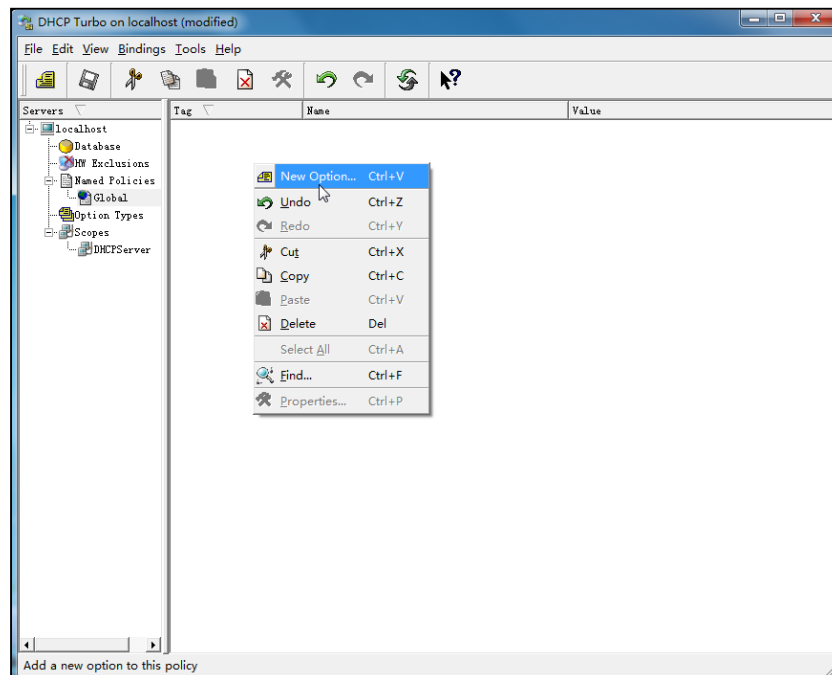
5. Click **OK** to accept the change.

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**.
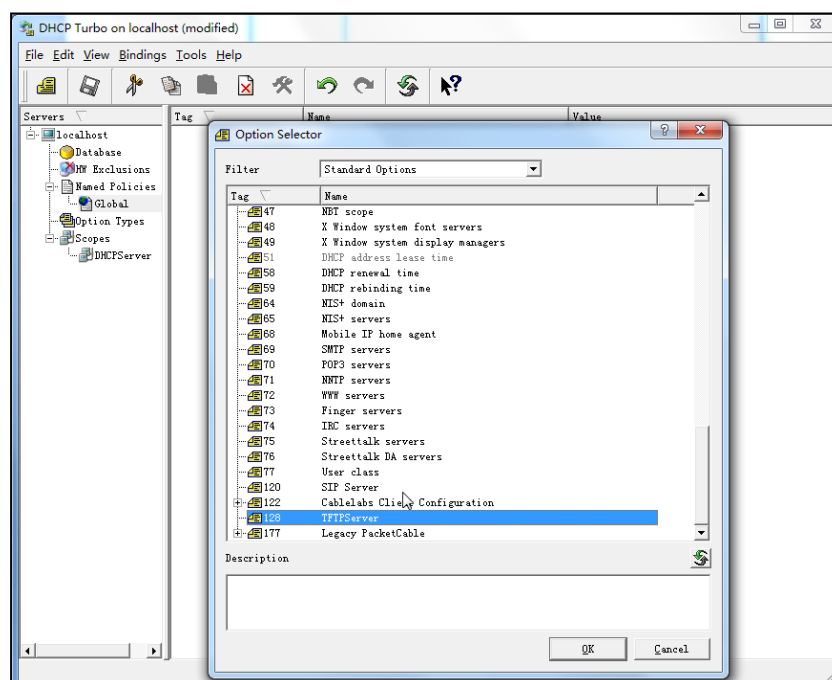

7. Set the custom DHCP option (custom DHCP option tag number ranges from 128 to 254) and select the option type (Yealink supports **string** and **ipaddress** option types only). Click the **OK** button to finish setting the option properties. Click to save the change.

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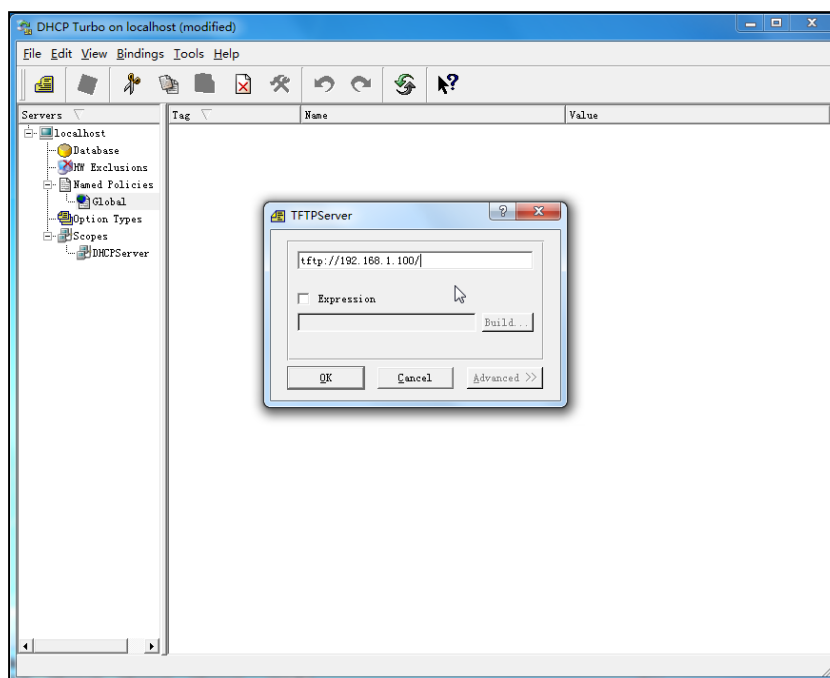

9. Scroll down and double click the custom option 128.

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

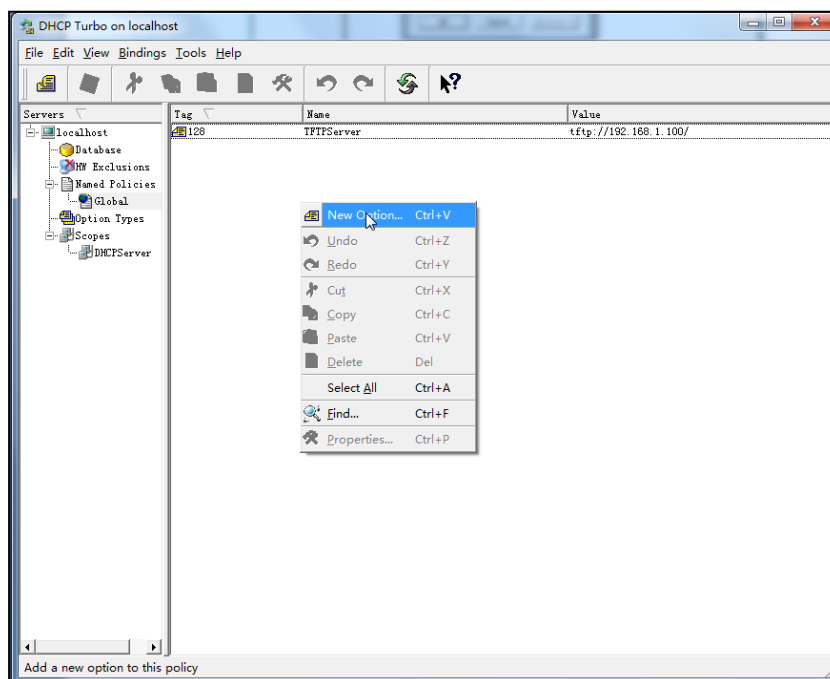**11.** Click the **OK** button to finish setting a custom option.
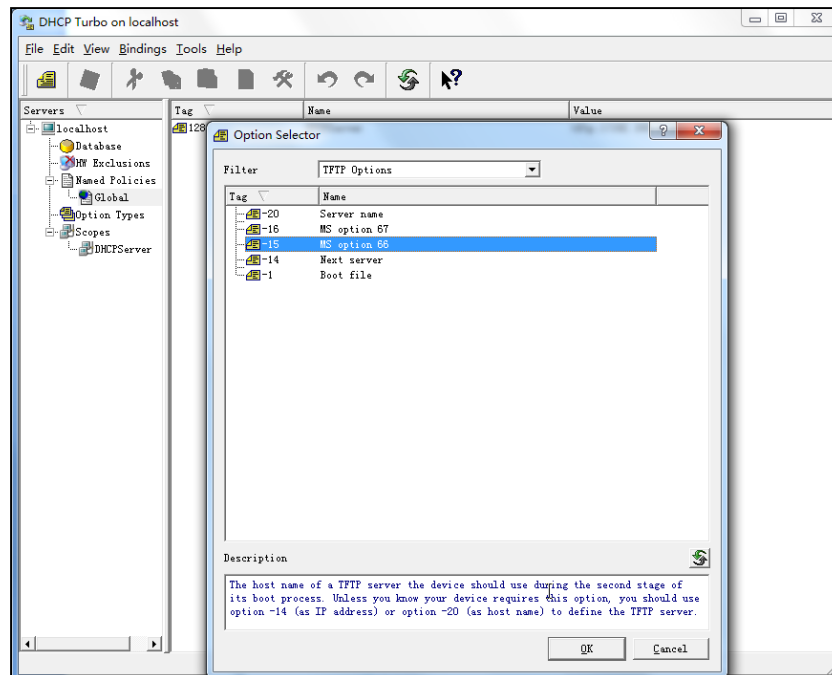

12. Click ![save icon] to save the change.

Add the Option 66 via DHCP Turbo

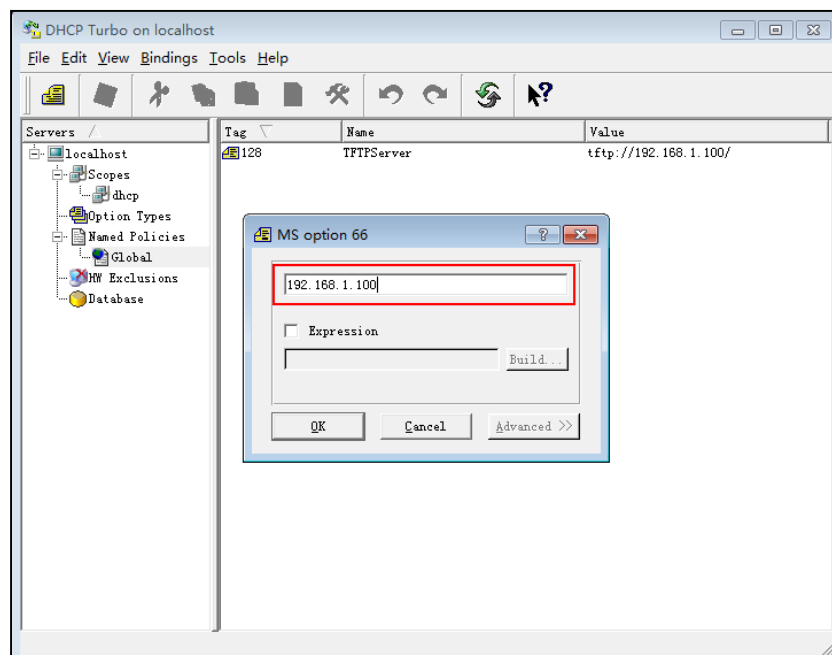You can add the option 66 via DHCP Turbo. The following shows the detailed processes.

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

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.
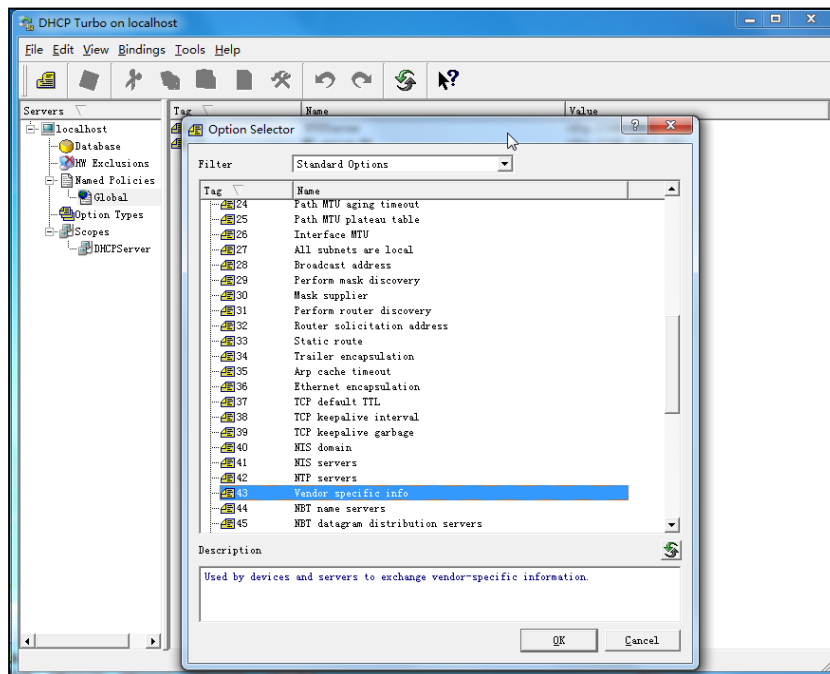

5. Click the **OK** button to finish setting a custom option.
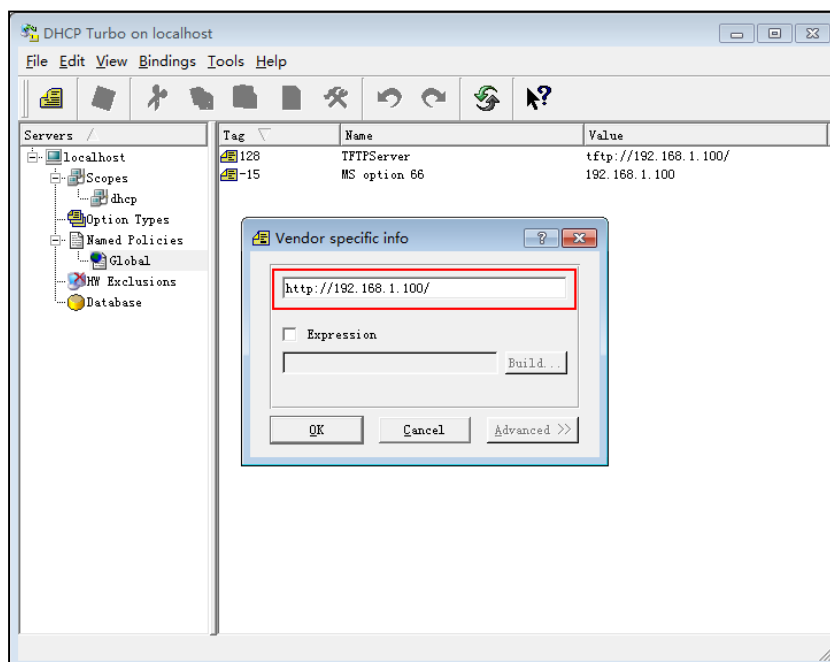
6. Click 🖫 to save the change.

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**.

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.