



Yealink Auto Provisioning User Guide

**Version 1.1
March 2012**

Table of Contents

Introduction.....	1
Getting Started	3
Obtaining Configuration Information	3
Obtaining Configuration Files.....	3
Obtaining Phone Information	4
Managing Configuration Files	4
Editing Common CFG File	4
Editing MAC-Oriented CFG File	7
Customizing Resource Files.....	10
Customizing a Ringtone	10
Customizing a LCD Language.....	11
Customizing a LCD Logo.....	12
Uploading Local Contacts	13
Updating Firmware	13
Configuring a TFTP Server.....	15
Preparing a Root Directory	15
Configuring a TFTP Server	16
Obtaining the Address of Provisioning Server	17
Zero-Sp-Touch	17
Plug and Play (PNP) Server	19
DHCP Options.....	20
Phone Flash	20
Downloading and Verifying Configurations.....	23
Downloading Configuration Files	23
Verifying Configurations	23
Troubleshooting.....	25
Glossary	27
Appendix.....	29

Configuring a FTP Server	29
Preparing a Root Directory	29
Configuring a FTP server	30
Configuring a HTTP Server	32
Preparing a Root Directory	32
Configuring a HTTP Server	32
Configuring a DHCP server	35
Customizing a Ringtone Using CoolEdit Pro	43
Customizing a Logo File Using PictureExDemo	44

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 shows you how to provision Yealink IP phones with the minimum settings required. Yealink IP phones support the FTP, TFTP, HTTP, and HTTPS protocols for file provisioning and are configured by default to use Trivial File Transfer Protocol (TFTP).

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

- Yealink SIP-T28(P)
- Yealink SIP-T26(P)
- Yealink SIP-T22(P)
- Yealink SIP-T20(P)
- Yealink SIP-T18(P)
- Yealink SIP-T12(P)
- Yealink SIP-T38(G)
- Yealink SIP-T32(G)
- Yealink VP530

The provisioning process outlined in this document applies to the firmware V70 or higher version of Yealink IP phones.

Getting Started

This section shows you how to get ready for the provisioning. The provisioning process discussed in this guide uses TFTP and a personal computer (PC) as the provisioning server.

To begin the provisioning process, the following are required:

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

Obtaining Configuration Information

Obtaining Configuration Files

Before you begin provisioning, you need to obtain the configuration files. There are 2 configuration files both of which are CFG formatted that the phone will try to download from the server during provisioning. We call them Common CFG file and MAC-Oriented CFG file.

The MAC-Oriented CFG file is only effectual for the specific phone. It uses the 12-digit MAC address of the phone as the file name. For example, if the MAC address of the phone is 0015651130F9, then the MAC-Oriented CFG file name must be 0015651130F9.cfg. However, the Common CFG file is effectual for all the phones with the same model. It uses a fixed name "y0000000000XX.cfg" as the file name, where "XX" equals to the hardware version of the phone model, except 0 for T28 which is special.

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

Phone Model	Common Configuration File
SIP-T28(P)	y000000000000.cfg
SIP-T26(P)	y000000000004.cfg
SIP-T22(P)	y000000000005.cfg
SIP-T20(P)	y000000000007.cfg
SIP-T12(P)	y000000000008.cfg
SIP-T18(P)	y000000000009.cfg
SIP-T38G	y000000000038.cfg
SIP-T32G	y000000000032.cfg
VP530	y000000000023.cfg

You can ask the distributor or the Yealink FAE for configuration files.

Obtaining Phone Information

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

MAC Address: The unique 12-digit serial number of the phone. You can obtain it from the phone's bar code at the back of the phone.

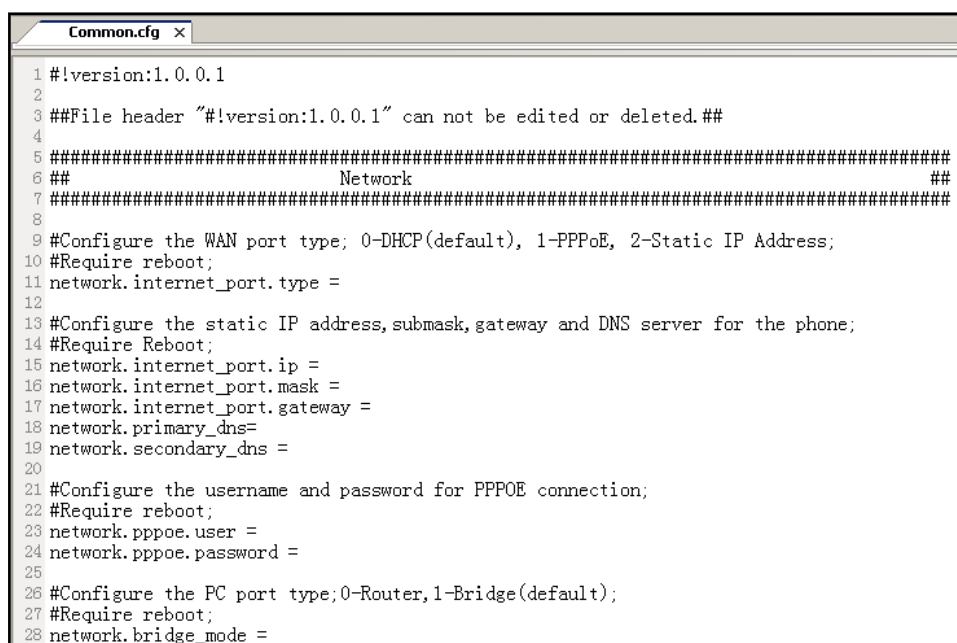
SIP Account: This may includes SIP credentials such as user name, password and the address of the phone's registration server. Ask your system administrator for SIP account information you need. Although SIP accounts may not be required to get the phone working, we strongly recommend using them.

Managing Configuration Files

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

Editing Common CFG File

Common CFG file contains configuration parameters which apply to all phones of the same phone model, such as the language displays on the phone LCD screen.



```
1 #!version:1.0.0.1
2
3 ##File header "#!version:1.0.0.1" can not be edited or deleted.##
4
5 #####
6 ##          Network          ##
7 #####
8
9 #Configure the WAN port type; 0-DHCP(default), 1-PPPoE, 2-Static IP Address;
10 #Require reboot;
11 network.internet_port.type =
12
13 #Configure the static IP address, submask, gateway and DNS server for the phone;
14 #Require Reboot;
15 network.internet_port.ip =
16 network.internet_port.mask =
17 network.internet_port.gateway =
18 network.primary_dns=
19 network.secondary_dns =
20
21 #Configure the username and password for PPPoE connection;
22 #Require reboot;
23 network.pppoe.user =
24 network.pppoe.password =
25
26 #Configure the PC port type;0-Router,1-Bridge(default);
27 #Require reboot;
28 network.bridge_mode =
```

The line beginning with “#” is considered to be a comment.

The parameters commonly edited in the Common CFG file (T2xP as an example) are detailed as following:

```
#####
##                               ##
#####

#!version:1.0.0.1
##File header "#!version:1.0.0.1" cannot be edited or deleted.##

#Configure the WAN port type; 0-DHCP(default), 1-PPPoE, 2-Static IP Address
#Require reboot;

network.internet_port.type = 0

#Configure the static IP address, submask, gateway and DNS server for the phone
#Require reboot

network.internet_port.ip = 192.168.1.10
network.internet_port.mask = 255.255.255.0
network.internet_port.gateway = 192.168.1.1
network.primary_dns = 202.101.103.55
network.secondary_dns = 202.101.103.54

#Configure the PC port type;0-Router,1-Bridge(default)
#Require reboot

network.bridge_mode = 1

#LAN port as Router settings
#Require reboot

network.pc_port.ip = 10.0.0.1
network.pc_port.mask = 255.255.255.0
network.pc_port.speed_duplex = 0
network.pc_port.dhcp_server = 1
network.dchp.start_ip = 10.0.0.10
network.dchp.end_ip = 10.0.0.100

#Enable or disable the Plug and Play feature; 0-Disabled, 1-Enabled (default)

auto_provision.pnp_enable = 1

#Set the auto provisioning mode (0-Disabled (default), 1-Power on, 4-Repeatedly,
#5-Weekly, Power on + Repeatedly, Power on + Weekly)

auto_provision.mode = 1
auto_provision.power_on_enable = 1
auto_provision.repeat.enable = 0
auto_provision.repeat.minutes = 1440
```

```

auto_provision.schedule.periodic_minute = 1
auto_provision.schedule.time_from = 00:00
auto_provision.schedule.time_to = 00:00
auto_provision.schedule.dayofweek = 0123456
auto_provision.server.url =
auto_provision.server.username =
auto_provision.server.password =
auto_provision.weekly.enable = 0
auto_provision.weekly.mask = 0123456
auto_provision.weekly.begin_time = 00:00
auto_provision.weekly.end_time = 00:00

```

#Set the AES key used for decrypting the Common CFG file

```
auto_provision.aes_key_16.com =
```

#Set the AES key used for decrypting MAC-Oriented CFG file;

```
auto_provision.aes_key_16.mac =
```

#Set the language used on the Web page

#The available values are: English, Chinese_S, Turkish, Portuguese, Spanish, Italian,
#French, Russian, Deutsch and Czech

```
lang.wui =
```

#Set the language used on the phone LCD screen

#The available values are: English (default), Chinese_S, Chinese_T, German, French,
#Turkish, Italiano, Polish, Spanish and Portuguese

```
lang.gui = English
```

#Set the web server access type (0-Disabled, 1-HTTP&HTTPS (default), 2-HTTP only,
#3-HTTPS only)

#Require reboot

```
network.web_server_type = 1
```

#Set the HTTP port (80 by default)

#Require reboot

```
network.port.http = 80
```

#Set the HTTPS port (443 by default)

#Require reboot

```
network.port.https = 443
```

#Set the new password (admin123) for the administrator

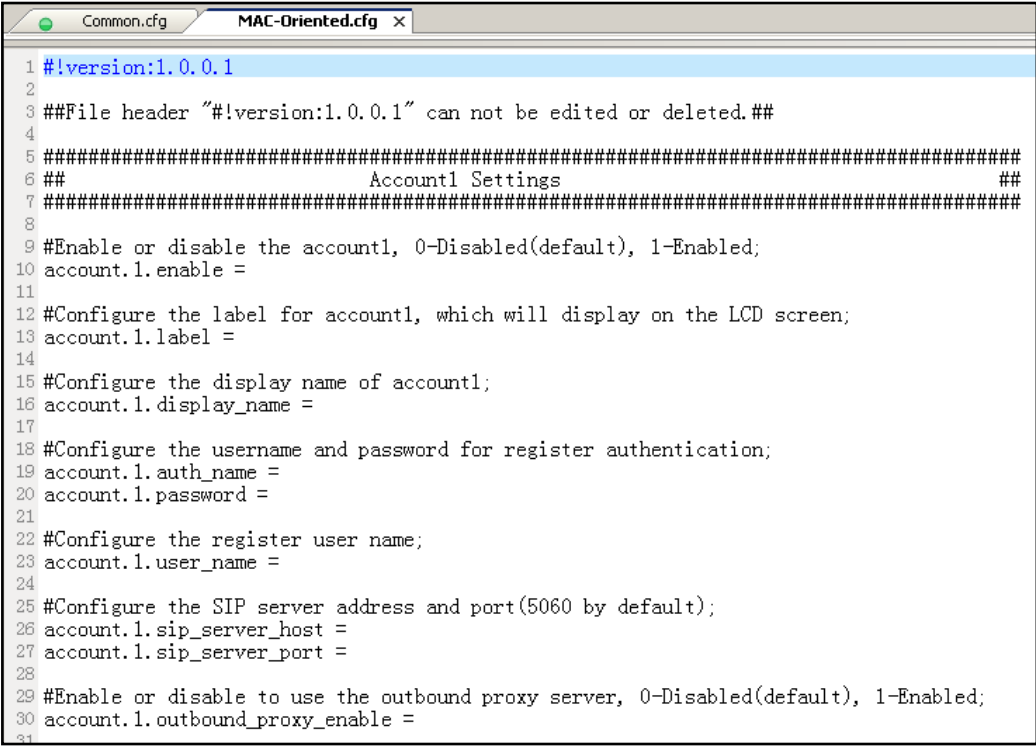
```
security.user_password = admin:admin123

#Set the new password (user123) for the user

security.user_password = user:user123
```

Editing MAC-Oriented CFG File

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



```
Common.cfg  MAC-Oriented.cfg x
1 #!version:1.0.0.1
2
3 ##File header "#!version:1.0.0.1" can not be edited or deleted.##
4
5 #####
6 ## Account1 Settings ##
7 #####
8
9 #Enable or disable the account1, 0-Disabled(default), 1-Enabled;
10 account.1.enable =
11
12 #Configure the label for account1, which will display on the LCD screen;
13 account.1.label =
14
15 #Configure the display name of account1;
16 account.1.display_name =
17
18 #Configure the username and password for register authentication;
19 account.1.auth_name =
20 account.1.password =
21
22 #Configure the register user name;
23 account.1.user_name =
24
25 #Configure the SIP server address and port(5060 by default);
26 account.1.sip_server_host =
27 account.1.sip_server_port =
28
29 #Enable or disable to use the outbound proxy server, 0-Disabled(default), 1-Enabled;
30 account.1.outbound_proxy_enable =
31
```

The parameters commonly edited in the MAC-Oriented CFG file are detailed as following:

```
#####
## MAC-Oriented CFG File ##
#####
#!version:1.0.0.1
#File header "#!version:1.0.0.1" cannot be edited or deleted.##
#Line1 settings
#Activate/Deactivate the account1, 0-Disabled (Default), 1-Enabled
account.1.enable = 0
#Configure the label of account1 which will display on the LCD screen
account.1.label =
#Configure the display name of account1
account.1.display_name =
```

```
#Configure the user name and password for register authentication
```

```
account.1.auth_name =
```

```
account.1.password =
```

```
#Configure the register user name
```

```
account.1.user_name =
```

```
#Configure the SIP server address and port (5060 by default)
```

```
account.1.sip_server_host =
```

```
account.1.sip_server_port = 5060
```

```
#Line2 settings
```

```
#Activate/Deactivate account2, 0-Disabled(Default), 1-Enabled
```

```
account.2.enable = 0
```

```
#Configure the label of account2 which will display on the LCD screen
```

```
account.2.label =
```

```
#Configure the display name of account2
```

```
account.2.display_name =
```

```
#Configure the user name and password for register authentication
```

```
account.2.auth_name =
```

```
account.2.password =
```

```
#Configure the register user name
```

```
account.2.user_name =
```

```
#Configure the SIP server address and port(5060 by default)
```

```
account.2.sip_server_host =
```

```
account.2.sip_server_port = 5060
```

```
#Line3 settings
```

```
#Activate/Deactivate the account3, 0-Disabled(Default), 1-Enabled
```

```
account.3.enable = 0
```

```
#Configure the label of account3 which will display on the LCD screen
```

```
account.3.label =
```

```
#Configure the display name of account3
```

```
account.3.display_name =
```

```
#Configure the user name and password for register authentication
```

```
account.3.auth_name =
```

```
account.3.password =
```

```
#Configure the register user name
```

```
account.3.user_name =
```

```
#Configure the SIP server address and port (5060 by default)
```

```
account.3.sip_server_host =
account.3.sip_server_port = 5060

#Line4 settings (For T28P, T38G and VP phone only)

#Activate/Deactivate the account4, 0-Disabled(Default), 1-Enabled
account.4.enable = 0

#Configure the label of account4 which will display on the LCD screen
account.4.label =

#Configure the display name of account4
account.4.display_name =

#Configure the user name and password for register authentication
account.4.auth_name =
account.4.password =

#Configure the register user name
account.4.user_name =

#Configure the SIP server address and port (5060 by default)
account.4.sip_server_host =
account.4.sip_server_port = 5060

#Line5 settings (For T28P and T38G only)

#Activate/Deactivate account5, 0-Disabled(Default) 1-Enabled
account.5.enable = 0

#Configure the label of account5 which will display on the LCD screen
account.5.label =

#Configure the display name of account5
account.5.display_name =

#Configure the user name and password for register authentication
account.5.auth_name =
account.5.password =

#Configure the register user name
account.5.user_name =

#Configure the SIP server address and port (5060 by default)
account.5.sip_server_host =
account.5.sip_server_port = 5060

#Line6 settings (For T28P and T38G only)

#Activate/Deactivate the account6, 0-Disabled(Default), 1-Enabled
account.6.enable = 0

#Configure the label of account6 which will display on the LCD screen.
```

```

account.6.label =
#Configure the display name of account6
account.6.display_name =
#Configure the user name and password for register authentication
account.6.auth_name =
account.6.password =
#Configure the register user name
account.6.user_name =
#Configure the SIP server address and port (5060 by default)
account.6.sip_server_host =
account.6.sip_server_port = 5060

```

Customizing Resource Files

You can configure the phone features via the parameters in the configuration files. You can also customize your phone with a personalized ringtone, language or logo.

Customizing a Ringtone

Yealink IP phones have built-in system ringtones and the default ring type is Ring1. You can change the ring type, or you can customize your personal ringtone and make it take effect via auto provisioning.

The ringtone file must use PCMU audio format, mono channel, 8K sample rate and 16 bit resolution.

The ringtone file format must be .wav.

All ringtone files uploaded must be within 100KB.

```

#####
##          Configure the access URL of the customizing ringtone          ##
#####
ringtone.url =
#ringtone.delete=http://localhost/all
#Delete all the custom ringtones uploaded through auto provision
ringtone.delete =

```

For example: enter “ftp://192.168.1.100/Ring9.wav” in the “ringtone.url =” field. During the auto provisioning process, the phone links to the provisioning server “192.168.1.100”, and downloads the ringtone file “Ring9.wav”.

You’d better check that the ringtone file has been uploaded to the root directory of the server before provisioning.

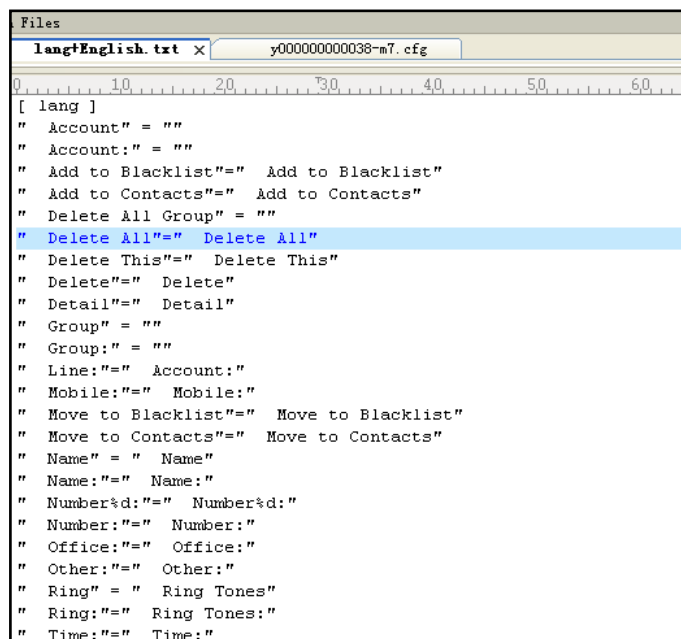
For more information about customizing a ringtone file, you can refer to the [Customizing a](#)

Ringtone Using CoolEdit Pro in this guide.

Customizing a LCD Language

Yealink IP phones allow you to modify the translation of the existing languages on the LCD screen, but you cannot add new language to the phone. To modify the existing language, you need to edit the language file and upload it to the root directory of the provisioning server, then specify the access URL in the configuration file.

The following figure shows a portion of the language file:



```
#####
##          Configure the access URL of the LCD language file          ##
#####
```

gui_lang.url =

```
#gui_lang.delete = http://localhost/all
```

```
#Delete all custom languages downloaded through auto provision
```

gui_lang.delete =

For example: enter "ftp://192.168.1.100/lang+English.txt" in the "gui_lang.url =" field.

During the auto provisioning process, the phone links to the provisioning server "192.168.1.100", and download the language file "lang+English.txt".

Available languages may be different between different firmware versions. Ask the distributor for the language template file.

Customizing a LCD Logo

Yealink SIP-T2xP/T1xP IP phones allow you to customize the logo displayed on the phone LCD screen (The SIP-T20P IP phone only supports displaying the text logo). Ask the distributor for the logo file, or you can customize a .dob logo file. Upload the logo file to the root directory of the provisioning server and then specify the access URL in the configuration file:

```
#####
##          Configure the access URL of the Logo File          ##
#####
#(SIP-T2xP/T1xP only, not applicable to T20P)

lcd_logo.url =
#lcd_logo.delete = http://localhost/all
#Delete all custom logo files
```

lcd_logo.delete =

For example: enter "ftp://192.168.1.100/logo.dob" in the "lcd_logo.url =" field. During the auto provisioning process, the phone links to the provisioning server "192.168.1.100", and downloads the logo file "logo.dob".

The following table lists the logo file format for each phone model:

Phone model	Logo file format	Resolution
SIP-T28P	.dob	<=236*82 2 gray scale
SIP-T26P	.dob	<=132*64 2 gray scale
SIP-T22P	.dob	<=132*64 2 gray scale
SIP-T18P	.dob	<=132*64 2 gray scale
SIP-T12P	.dob	<=132*64 2 gray scale

Upload the logo file to the root directory of the provisioning server. After provisioning, the phone boots up, and you will then find that the customized logo displays on the phone LCD screen.

For more information about customizing a Logo file, refer to [Customizing a Logo File Using PictureExDemo](#) in this guide.

Uploading Local Contacts

Yealink IP phones allow you to batch upload contact data by auto provisioning. Edit the contactData.xml file, upload the file to the root directory of the provisioning server and then specify the access URL in the configuration file.

The following shows an example of the contactData.xml file:

```
<contactData>
  <group>
    <contact sDisplayName="Mary" sOfficeNumber="1234"
sMobilNumber="12345678901" sOtherNumber="2231" sLine="0" sRing="Auto"/>
    <contact sDisplayName="Damy" sOfficeNumber="1235"
sMobilNumber="12345678902" sOtherNumber="2232" sLine="0" sRing="Auto"/>
    <contact sDisplayName="John" sOfficeNumber="1236"
sMobilNumber="12345678903" sOtherNumber="2233" sLine="0" sRing="Auto"/>
  </group>
  <blacklist>
    <contact sDisplayName="Mili" sOfficeNumber="7788"
sMobilNumber="44444444444" sOtherNumber="2222" sLine="0" sRing="Auto"/>
  </blacklist>
</contactData>
```

```
#####
##                               Upload local contact file          ##
#####
```

local_contact.data.url =

For example: enter "ftp://192.168.1.100/ ContactData.xml" in the "local_contact.data.url =" field. During the auto provisioning process, the phone links to the provisioning server "192.168.1.100", and download the contact file "ContactData.xml".

Yealink IP phones support both the .xml and .csv formats.

Updating Firmware

Yealink IP Phones allow you to update the firmware manually via web user interface, or batch update the firmware via the auto provisioning. To batch update the phones' firmware via auto provisioning, ask the distributor for the firmware file, upload it to the root directory of the provisioning server, and then specify the access URL in the configuration files.

```
#####
##                               Configure the access URL of the firmware file          ##
#####
```

firmware.url =

For example: enter "ftp://admin:password@192.168.1.100/2.61.0.80.rom" in the "firmware.url =" field. During the auto provisioning process, the phone links to the provisioning server "192.168.1.100" ("admin" as the authentication user name and "password" as the authentication password), and download the firmware file 2.61.0.80.rom.

Configuring a TFTP Server

Yealink IP Phones support using the FTP, TFTP, HTTP and HTTPS protocols to download the configuration files. TFTP server is used by default. You can use any protocol for provisioning. The following section takes the TFTP server as an example.

We recommend that you can use 3CDaemon or TFTP32 tool as a TFTP server. 3CDaemon and TFTP32 are free applications for Windows. You can download the 3CDaemon software at: <http://www.oldversion.com/3Com-Daemon.html> and TFTP32 at: <http://tftpd32.jounin.net/>.

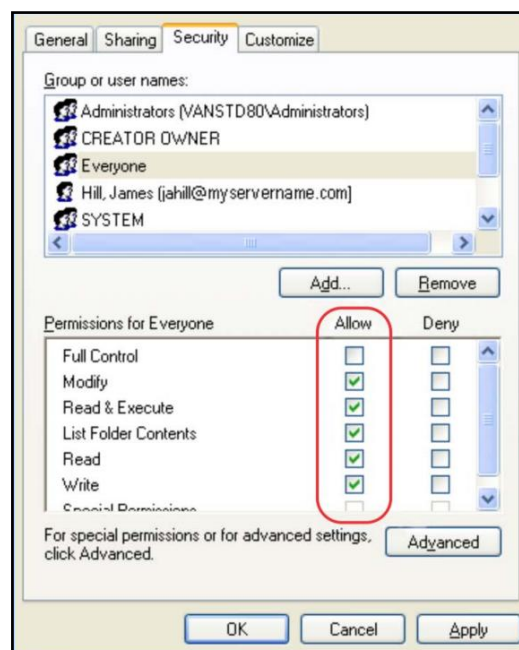
We provide a simple instruction of configuring a TFTP server using 3CDaemon tool in the [Configuring a FTP server](#) section.

Preparing a Root Directory

To prepare a root directory:

1. Create a root TFTP directory on the local computer.
2. Store the configuration files to this root directory.
3. Set the security permissions for the TFTP directory folder.
4. You need to define a user or a group name, and set the permissions: read, write, and modify files. Security permissions vary by organization.

An example of using the Windows platform is shown as below:

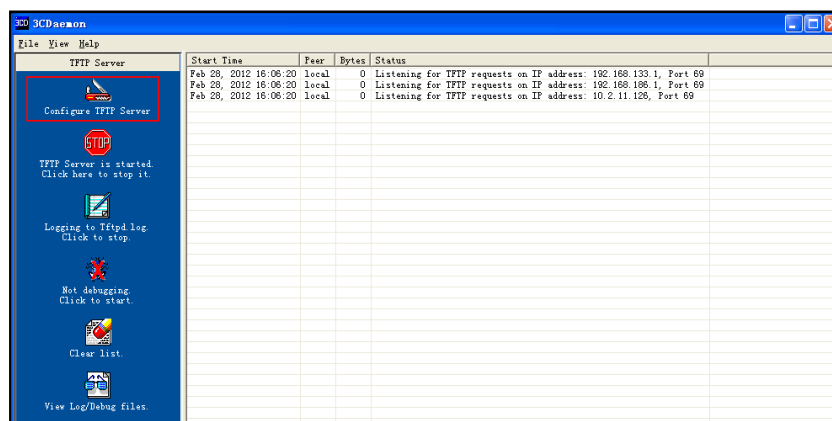


Configuring a TFTP Server

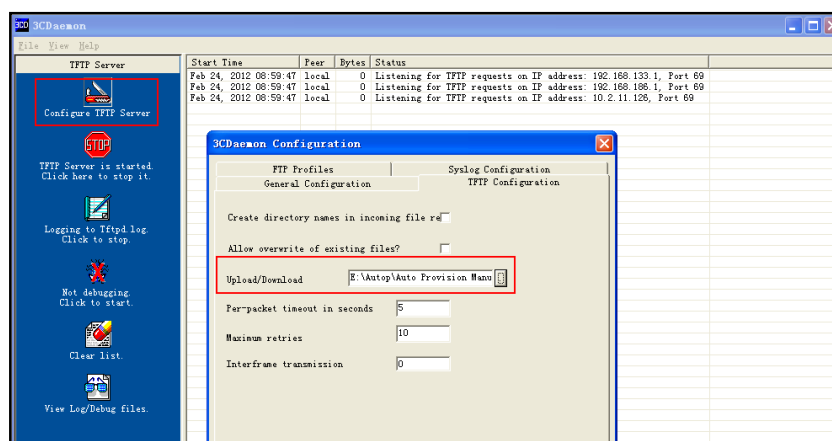
If you have a 3CDaemon application installed on your computer, use it directly. Otherwise, download and install it.

To configure a TFTP server:

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



2. Select **Configure TFTP Server**. Click the  button to locate the TFTP root directory on the computer:



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 capable of TFTP downloading.

Obtaining the Address of Provisioning Server

Yealink IP phones support to obtain the provisioning server address during bootup process in the following ways:

- [Zero-Sp-Touch](#)
- [Plug and Play \(PNP\) Server](#)
- [DHCP Options](#)
- [Phone Flash](#)

When the phone boots up, it will go by the following process to obtain the provisioning server address step by step: Zero-Sp-Touch --> PNP server --> DHCP options (Custom option --> option 66 --> option 43) --> Phone Flash.

The following sections detail each process.

Zero-Sp-Touch

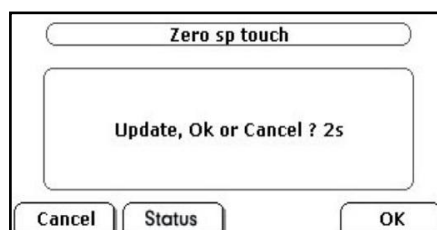
Zero-Sp-Touch allows you to configure the network and provisioning server address via phone user interface during bootup. This feature is helpful when there is a system failure on the phone. To use Zero-Sp-Touch, you need to make sure that this feature is enabled.

To configure the Zero-Sp-Touch via web user interface:

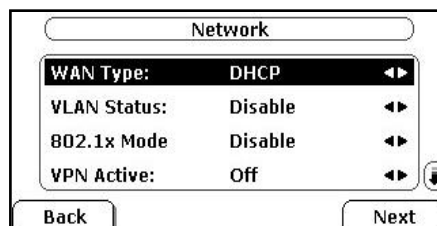
1. Click on **Upgrade** -> **Advanced**.
2. Select **Enabled** from the pull-down list of **Zero Active**.
3. Set the waiting time(in seconds) in the **Wait Time** filed.

The screenshot shows the Yealink web interface with the 'Upgrade' tab selected. Under the 'Advanced' sub-tab, the 'Zero Active' dropdown is set to 'Enabled' and the 'WaitTime' is set to 5. The 'Custom Option' section is visible, showing fields for Custom Option Type, URL, Account, Password, Common AES Key, and MAC-Oriented AES Key. The 'PNP Config' section shows 'Enabled' for PNP Config and 'Disabled' for Check New Config. The 'Export / Import Config' section shows a file selection button and 'Import' and 'Export' buttons. The 'Export System Log' section shows a dropdown set to 'Local'. A 'NOTE' section on the right provides additional information about Custom Option, AES Key, and System Log.

When the Zero-Sp-Touch is enabled, there will be a configure wizard during the bootup:

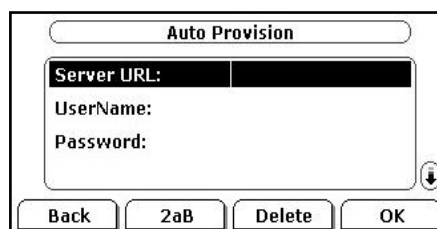


Press the **OK** soft key. Then you can configure the network on the LCD screen:



Press the **Next** soft key after finishing the network configuration. Configure the provisioning server address, authentication username (optional) and password (optional) in the Auto Provision interface.

A sample screenshot is shown below:



Plug and Play (PNP) Server

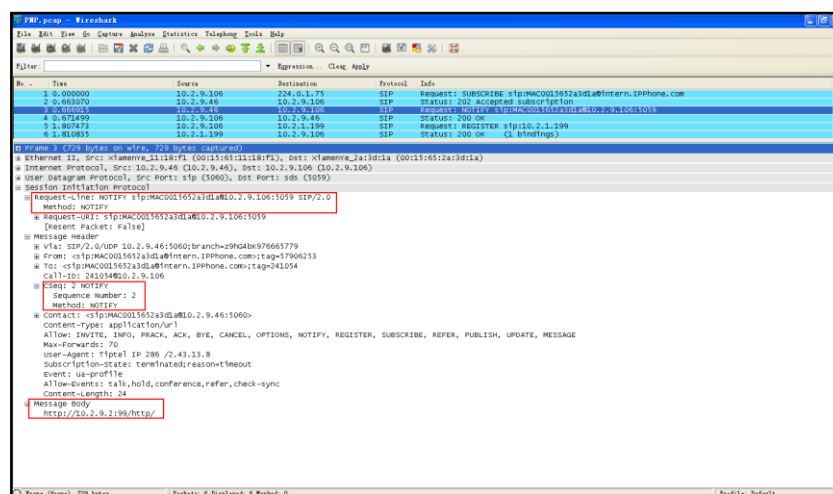
Yealink IP phones support obtaining the provisioning server address from the PNP server. The phone broadcast the PNP Subscribe message to obtain a provisioning server address during bootup. To use Plug and play, make sure this feature is enabled.

To configure the PNP via web user interface:

1. Click on **Upgrade** -> **Advanced**.
2. Select **Enabled** from the pull-down list of **PNP config**.

The screenshot shows the 'Upgrade' tab in the web interface, specifically the 'Advanced' sub-tab. The 'PNP config' dropdown menu is highlighted with a red box and set to 'Enabled'. Other visible fields include 'Custom Option' (128 ~ 254), 'Custom Option Type' (String), 'URL', 'Account', 'Password', 'Common AES Key', 'MAC-Oriented AES Key', 'Check New Config' (Disabled), 'Click this button to auto provision immediately' (Auto provision), 'Export / Import Config' (with a file browser button), 'Export System Log' (Local), and 'PCAP Trace' (Start, Stop, Export buttons). A 'Confirm' button is at the bottom.

Any PNP server activated in the network responses with a **SIP NOTIFY** message and an address of the provisioning server contained in the message body. The phone can then link to the provisioning server and performs the provisioning process.



DHCP Options

Yealink IP phones support obtaining the provisioning server address from DHCP options. You can configure the phone to obtain a provisioning server address from a custom DHCP option, or the phone will automatically detect the Option 66 or Option 43.

To obtain a provisioning server by a custom DHCP option, make sure that the DHCP option is set properly.

To configure the DHCP option via web user interface:

1. Click on **Upgrade** -> **Advanced**.
2. Enter the value (128-254) in the **Custom Option** field.
3. Select the desired type from the pull-down list of **Custom Option Type**.

A valid Custom Option is from 128 to 254. The Custom Option Type must be in accordance with the one defined in the DHCP server.

Phone Flash

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

To configure the Phone Flash via web user interface:

1. Click on **Upgrade** -> **Advanced**.
2. Enter the URL, username and password of the provisioning server in the **URL**, **Account** and **Password** fields (the authentication username and password is optional).

3. Select **Power on** from the pull-down list of **Check New Config**.

The screenshot shows the Yealink web interface with the 'Check New Config' configuration page. The 'Check New Config' dropdown is set to 'Power on'. Other fields include URL (http://192.168.1.100/), Account (admin), Password (*****), Common AES Key (*****), and MAC-Oriented AES Key (*****). The 'Check New Config' dropdown is highlighted with a red box, and the 'Power on' option is selected. The 'Auto provision' button is also visible.

If the configuration files have been AES encrypted, the AES Keys will be needed. The Common AES Key is for decrypting the Common CFG file. The MAC-Oriented AES Key is for decrypting the MAC-Oriented CFG file. The keys must be 16 bytes and the supported characters are: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # \$ % * + , - . : = ? @ [] ^ _ { } ~.

Reboot the phone after the above configurations. During bootup, the phone will link to the provisioning server "192.168.1.100", using the authentication user name and password filled in the **Account** and **Password** fields. If the phone fails to get any information from the phone flash, the current round of obtaining the provisioning server address will stop.

Downloading and Verifying Configurations

Downloading Configuration Files

Once obtains a provisioning server address from one of the way introduced above. The phone will link to the provisioning server and download the configuration files. During the provisioning process, the phone will try to download the Common CFG file first, and then try to download the MAC-Oriented CFG file from the root directory of the provisioning server. If resource files need to be updated and the access URL has been specified in the configuration file. The phone will then try to download and update the resource files.

Verifying Configurations

After auto provisioning, the phone boots up. You can then verify the update via phone user interface, or you can verify it via web user interface of the phone. For more information, refer to the user guide of the Yealink IP phones.

During the auto provisioning process, you can monitor the downloading request and response message by a WinPcap tool.

If the MD5 value of the CFG file is different from that of the last one, the phone updates the configuration and then reboots. Otherwise, the phone gives up update and doesn't reboot.

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

No.	Time	Source	Destination	Protocol	Info
194	46.954819	10.2.11.119	10.2.11.126	TFTP	Read Request, File: y000000000000.cfg/000, Transfer type: octet/000
199	46.974859	10.2.11.126	10.2.11.119	TFTP	Data Packet, Block: 1
200	46.981090	10.2.11.119	10.2.11.126	TFTP	Acknowledgement, Block: 1
201	46.982020	10.2.11.126	10.2.11.119	TFTP	Data Packet, Block: 2
202	46.983900	10.2.11.119	10.2.11.126	TFTP	Acknowledgement, Block: 2
203	46.984250	10.2.11.126	10.2.11.119	TFTP	Data Packet, Block: 3
204	46.986221	10.2.11.119	10.2.11.126	TFTP	Acknowledgement, Block: 3
205	46.986388	10.2.11.126	10.2.11.119	TFTP	Data Packet, Block: 4
206	46.986806	10.2.11.119	10.2.11.126	TFTP	Acknowledgement, Block: 4
207	46.990045	10.2.11.126	10.2.11.119	TFTP	Data Packet, Block: 5
208	46.991977	10.2.11.119	10.2.11.126	TFTP	Acknowledgement, Block: 5
209	46.992153	10.2.11.126	10.2.11.119	TFTP	Data Packet, Block: 6
210	46.993832	10.2.11.119	10.2.11.126	TFTP	Acknowledgement, Block: 6
211	46.994354	10.2.11.126	10.2.11.119	TFTP	Data Packet, Block: 7
212	46.996015	10.2.11.119	10.2.11.126	TFTP	Acknowledgement, Block: 7
213	46.996245	10.2.11.126	10.2.11.119	TFTP	Data Packet, Block: 8
214	47.000510	10.2.11.119	10.2.11.126	TFTP	Acknowledgement, Block: 8
215	47.000704	10.2.11.126	10.2.11.119	TFTP	Data Packet, Block: 9
216	47.003985	10.2.11.119	10.2.11.126	TFTP	Acknowledgement, Block: 9
217	47.004139	10.2.11.126	10.2.11.119	TFTP	Data Packet, Block: 10 (last)
218	47.005370	10.2.11.119	10.2.11.126	TFTP	Acknowledgement, Block: 10
244	54.444367	10.2.11.119	10.2.11.126	TFTP	Read Request, File: 00156511185c.cfg/000, Transfer type: octet/000
245	54.462711	10.2.11.126	10.2.11.119	TFTP	Error Code, Code: Access violation, Message: could not open requested file for reading

Frame 415 (345 bytes on wire, 345 bytes captured)
 Ethernet II, Src: 6c:50:4d:40:da:4d (6c:50:4d:40:da:4d), Dst: x1amenve_11:18:5c (00:15:65:11:18:5c)
 Internet Protocol, Src: 10.2.11.254 (10.2.11.254), Dst: 10.2.11.244 (10.2.11.244)
 User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
 Bootstrap Protocol
 Message type: Boot Reply (2)
 Hardware type: ethernet
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0xbcc10503
 Seconds elapsed: 0
 Bootp Flags: 0x0000 (unicast)
 Client IP address: 0.0.0.0 (0.0.0.0)
 Your (Client) IP address: 10.2.11.244 (10.2.11.244)
 Next server IP address: 0.0.0.0 (0.0.0.0)
 Relay agent IP address: 0.0.0.0 (0.0.0.0)
 Client MAC address: x1amenve_11:18:5c (00:15:65:11:18:5c)
 Client hardware address padding: 00000000000000000000
 Server host name not given
 Boot file name not given

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

No.	Time	Source	Destination	Protocol	Info
151	34.500098	10.2.11.126	10.2.11.115	FTP	Response: 220 30cm 3cdaemon FTP Server version 2.0
153	34.507326	10.2.11.115	10.2.11.126	FTP	Request: USER tff
154	34.509003	10.2.11.126	10.2.11.115	FTP	Response: 331 user name ok, need password
155	34.513482	10.2.11.115	10.2.11.126	FTP	Request: PASS 111111
156	34.515044	10.2.11.126	10.2.11.115	FTP	Response: 230 user logged in
157	34.523305	10.2.11.115	10.2.11.126	FTP	Request: TYPE I
158	34.524405	10.2.11.126	10.2.11.115	FTP	Response: 200 Type set to I.
159	34.528402	10.2.11.115	10.2.11.126	FTP	Request: PASV
160	34.532697	10.2.11.126	10.2.11.115	FTP	Response: 227 Entering passive mode (10,2,11,126,5,189)
164	34.541081	10.2.11.115	10.2.11.126	FTP	Request: SIZE y00000000000.cfg
165	34.543288	10.2.11.126	10.2.11.115	FTP	Response: 213 1986
166	34.552631	10.2.11.115	10.2.11.126	FTP	Request: RETR y00000000000.cfg
167	34.554557	10.2.11.126	10.2.11.115	FTP	Response: 213 Using existing data connection
177	34.593926	10.2.11.126	10.2.11.115	FTP	Response: 226 Closing data connection; File transfer successful.
188	36.338570	10.2.11.115	10.2.11.126	FTP	Request: QUIT
189	36.340311	10.2.11.126	10.2.11.115	FTP	Response: 221 Service closing control connection
215	42.151291	10.2.11.126	10.2.11.115	FTP	Response: 220 30cm 3cdaemon FTP Server version 2.0
218	42.159981	10.2.11.115	10.2.11.126	FTP	Request: USER tff
219	42.160926	10.2.11.126	10.2.11.115	FTP	Response: 331 user name ok, need password
220	42.165441	10.2.11.115	10.2.11.126	FTP	Request: PASS 111111
221	42.166670	10.2.11.126	10.2.11.115	FTP	Response: 230 user logged in
222	42.170894	10.2.11.115	10.2.11.126	FTP	Request: TYPE I
223	42.171775	10.2.11.126	10.2.11.115	FTP	Response: 200 Type set to I.
224	42.172780	10.2.11.115	10.2.11.126	FTP	Request: PASV
225	42.176037	10.2.11.126	10.2.11.115	FTP	Response: 227 Entering passive mode (10,2,11,126,5,193)
229	42.172776	10.2.11.115	10.2.11.126	FTP	Request: SIZE 0015611185c.cfg
230	42.174476	10.2.11.126	10.2.11.115	FTP	Response: 213 Error accessing file
231	42.1746170	10.2.11.115	10.2.11.126	FTP	Request: RETR 0015611185c.cfg
232	42.174397	10.2.11.126	10.2.11.115	FTP	Response: 550 File unavailable
245	42.178586	10.2.11.126	10.2.11.115	FTP	Response: 220 30cm 3cdaemon FTP Server version 2.0
247	42.1736866	10.2.11.115	10.2.11.126	FTP	Request: USER tff
248	42.1737875	10.2.11.126	10.2.11.115	FTP	Response: 331 user name ok, need password
249	42.1742202	10.2.11.115	10.2.11.126	FTP	Request: PASS 111111
250	42.1743675	10.2.11.126	10.2.11.115	FTP	Response: 230 user logged in
251	42.1757760	10.2.11.115	10.2.11.126	FTP	Request: TYPE I
252	42.1759005	10.2.11.126	10.2.11.115	FTP	Response: 200 Type set to I.
253	42.1763681	10.2.11.115	10.2.11.126	FTP	Request: PASV
254	42.1767121	10.2.11.126	10.2.11.115	FTP	Response: 227 Entering passive mode (10,2,11,126,5,194)
258	42.1781389	10.2.11.115	10.2.11.126	FTP	Request: SIZE 0015611185c.cfg
259	42.1783227	10.2.11.126	10.2.11.115	FTP	Response: 213 Error accessing file
260	42.1783226	10.2.11.115	10.2.11.126	FTP	Request: RETR 0015611185c.cfg
261	42.1786745	10.2.11.126	10.2.11.115	FTP	Response: 550 File unavailable

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

Realtek 10/100/1000 Ethernet NIC		(Microsoft® Packet Scheduler) : Capturing WireShark			
File Edit View Go Capture Analysis Statistics Telephony Tools Help					
Filter: http		Expression: Class Apply			
No.	Time	Source	Destination	Protocol	Info
240	6.882104	10.2.11.126	10.2.11.244	HTTP	POST /cgi-bin/ConfigmanApp.com HTTP/1.1 (application/x-www-form-urlencoded)
241	6.903114	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.8358257313087566 HTTP/1.1
242	6.903114	10.2.11.126	10.2.11.244	HTTP	GET /y000000000000.cfg HTTP/1.1
243	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK (application/octet-stream)
244	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 404 Not Found (text/html)
245	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
246	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
247	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
248	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
249	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
250	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
251	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
252	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
253	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
254	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
255	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
256	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
257	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
258	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
259	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
260	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
261	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
262	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
263	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
264	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
265	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
266	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
267	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
268	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
269	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
270	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
271	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
272	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
273	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
274	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
275	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
276	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
277	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
278	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
279	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
280	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
281	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
282	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
283	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
284	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
285	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
286	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
287	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
288	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
289	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
290	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
291	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
292	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
293	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
294	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
295	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
296	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
297	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
298	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
299	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
300	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
301	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
302	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
303	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
304	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
305	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
306	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
307	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
308	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
309	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
310	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
311	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
312	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
313	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
314	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
315	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
316	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
317	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
318	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
319	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
320	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
321	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
322	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
323	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
324	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
325	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
326	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
327	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
328	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
329	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
330	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
331	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
332	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
333	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
334	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
335	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
336	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
337	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
338	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
339	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
340	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
341	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
342	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
343	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
344	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
345	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
346	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
347	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
348	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
349	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
350	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
351	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
352	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
353	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
354	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
355	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
356	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
357	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
358	6.910105	10.2.11.126	10.2.11.244	HTTP	POST /check_outchain.php HTTP/1.1
359	6.910105	10.2.11.126	10.2.11.244	HTTP	HTTP/1.1 200 OK
360	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9395627115025857 HTTP/1.1
361	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9884116270505 HTTP/1.1
362	6.910105	10.2.11.126	10.2.11.244	HTTP	GET /cgi-bin/ConfigmanApp.com?Id=76&ax=1&sid=0.9273850928056307 HTTP/1.1
363	6.910				

Troubleshooting

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

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

Why does the phone fail to download the configuration file?

- Ensure that the Auto Provisioning feature is enabled.
- Check that the provisioning server or the network is reachable.
- Check that authentication credentials configured on the phone are correct.
- Ensure that the configuration file exists on the provisioning server.

Why does the provisioning server return a HTTP 404?

- Check that the provisioning server is properly set up.
- Revisit the path configuration (URL rewriting, port).
- Ensure that the requested file exists on the provisioning server.

Why does the phone display "Network Unavailable"?

- Ensure that the Ethernet cable is plugged into the Internet port of the phone and the Ethernet cable is not loose.
- Ensure that the switch or hub in your network is operational.
- Check the configuration of network is properly set in the configuration files.
- Contact your system administrator for more information.

Why does the permission denied when uploading files to a FTP server?

- Ensure that the root directory of the FTP server contains the full directory path.
- On the provisioning server, check the file permissions, if necessary, change the file permission.
- Contact your system administrator for more information.

Why does not the phone obtain the IP address from DHCP server?

- Ensure that your settings are right on the DHCP Server.
- Ensure your phone is configured to obtain the IP address via DHCP server.
- Contact your system administrator for more information.

Why does not the phone download the ringtone?

- Make sure that the ringtone file's type is .wav format.
- Make sure that the size of the ringtone file is no larger than the phone support.
- Check the ringtone's properties are all right for the phone.
- Ensure the network is available and the root directory is right for downloading.
- Ensure that the ringtone file exists on the provisioning server.

Why does not the phone apply the configurations?

- Ensure the configuration files are different from the last ones.
- Ensure the phone have downloaded the configuration files.
- Ensure the parameters are correctly set in the configuration files.
- Contact your system administrator for more information.

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 a FTP Server

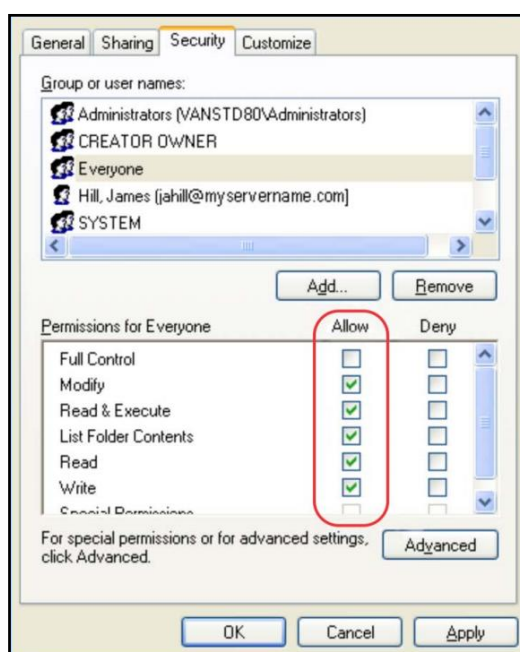
This chapter shows you how to configure a FTP server using 3CDaemon and how to configure a HTTP server using HFS tool. You can download the 3CDaemon software at: <http://www.oldversion.com/3Com-Daemon.html> and HFS at: <http://www.snapfiles.com/get/hfs.html>

Preparing a Root Directory

To prepare a root directory:

1. Create a root FTP directory on the local computer.
2. Store the configuration files to this root directory.
3. Set the security permissions for the FTP directory folder.
4. You need to define a user or group name, and set the permissions: read, write, and modify files. Security permissions vary by organization.

An example of using the Windows platform is shown as below:



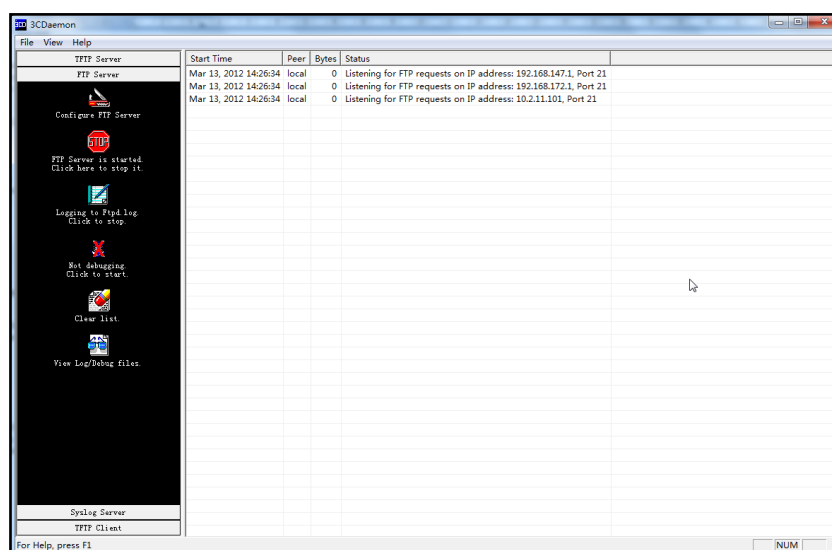
Configuring a FTP server

If you have a 3CDaemon application installed on your computer, open it now, or otherwise, download and install it.

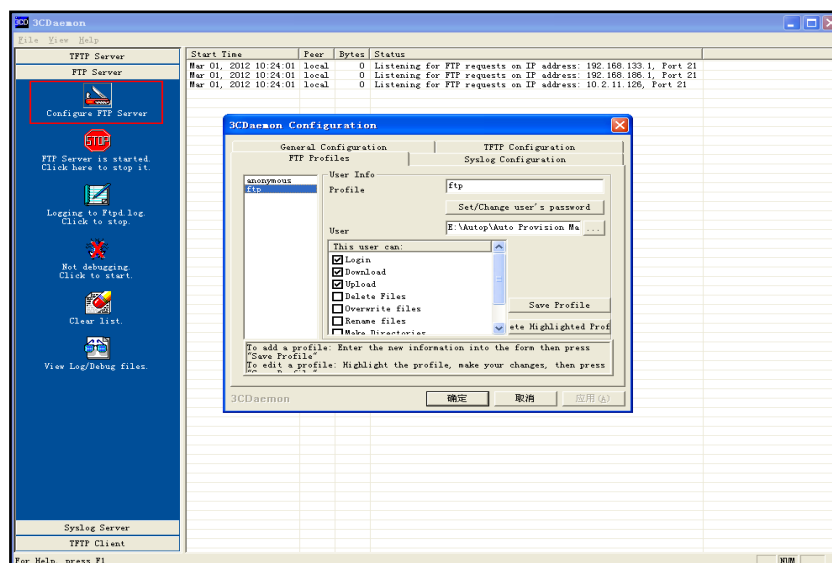
To configure a FTP server:

1. Double click the 3CDaemon.exe to start the application.
2. Click the FTP Server button on the left of the main page.

A screenshot is shown as below:



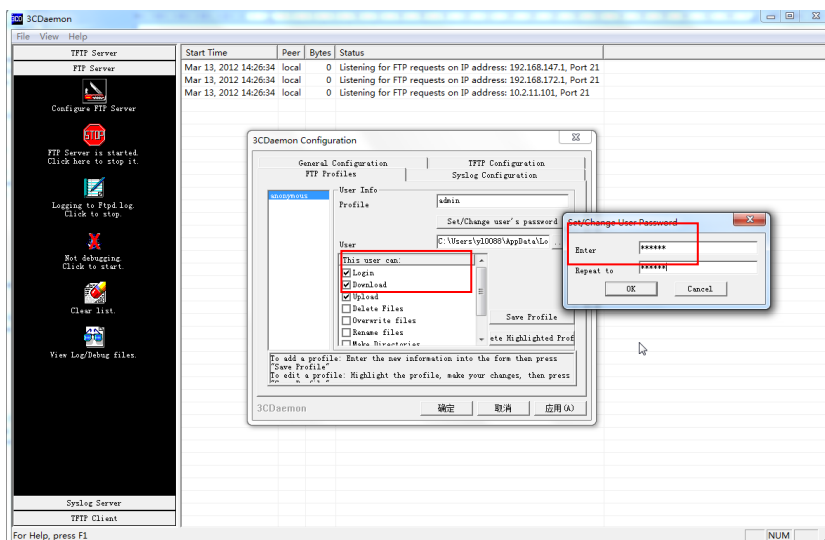
3. Select **Configure FTP Server**.
4. Click the  button to locate the TFTP root directory on the computer:



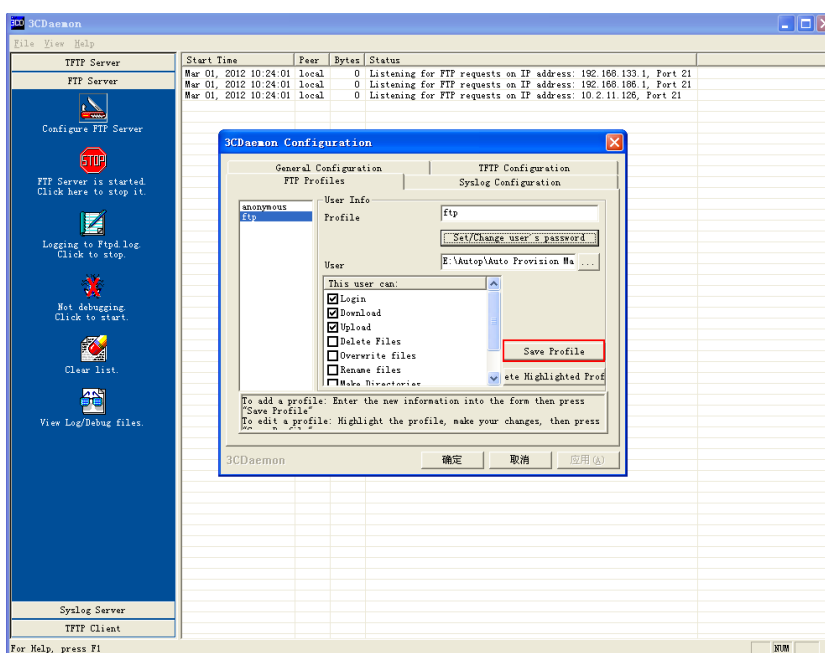
5. Enter the new authentication username in the **Profile** field.
6. Click the **Set/Change user's password** button to set the password in the pop-up

dialogue box.

7. Click the **OK** button to save.
8. Mark the check boxes of **Login**, **Download** and **Upload** to make sure the FTP user has the login, download and upload permission.



9. Click the **Save Profile** button to save the settings and finish the configurations.



10. Click the **Confirm** button to finish configuring the FTP server.

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://admin:123456@192.168.1.100/") is capable of TFTP download.

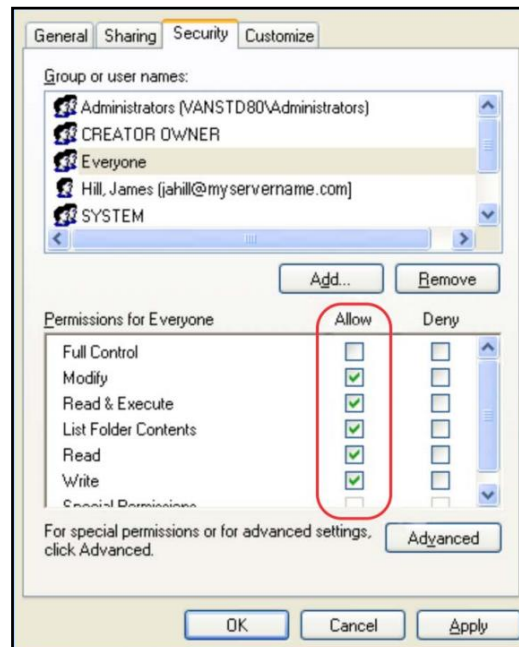
Configuring a HTTP Server

Preparing a Root Directory

To prepare a root directory:

1. Create a root HTTP directory on the local computer.
2. Store the configuration files to this root directory.
3. Set the security permissions for the FTP directory folder.
4. You need to define a user or group name and set the permissions: read, write, and modify files. Security permissions vary by organization.

An example of using the Windows platform is shown as below:



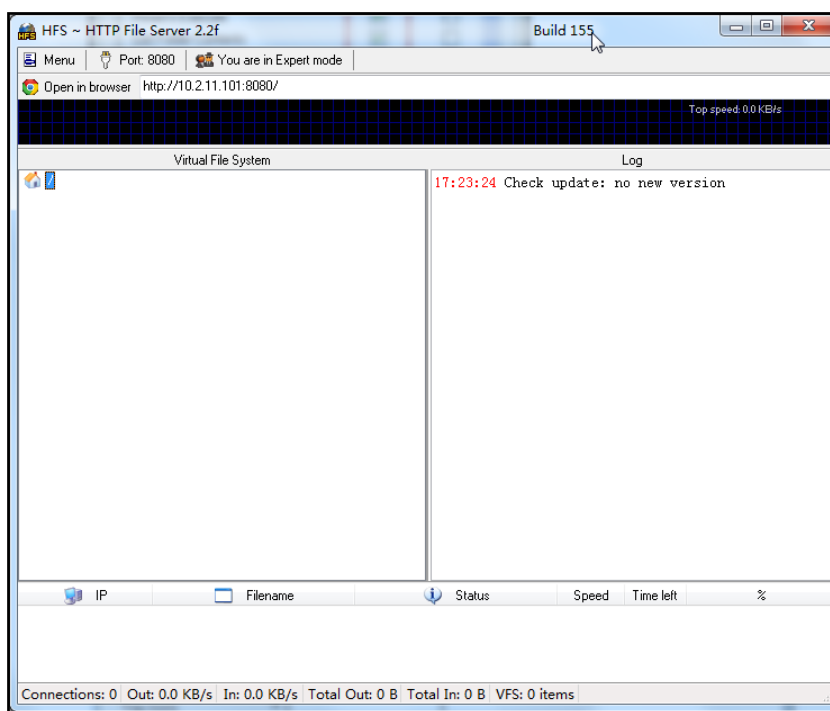
Configuring a HTTP Server

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

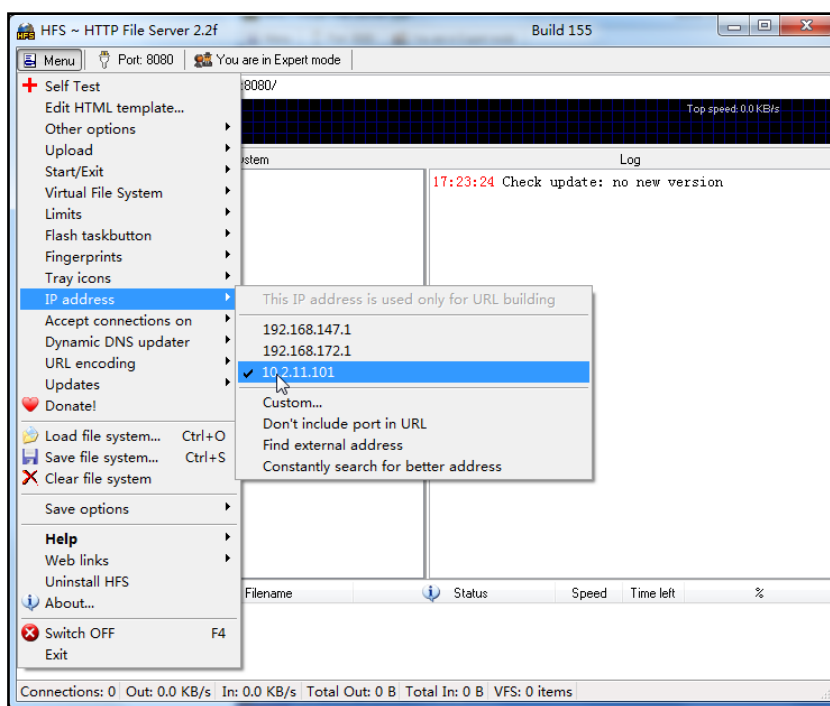
To configure a HTTP server:

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

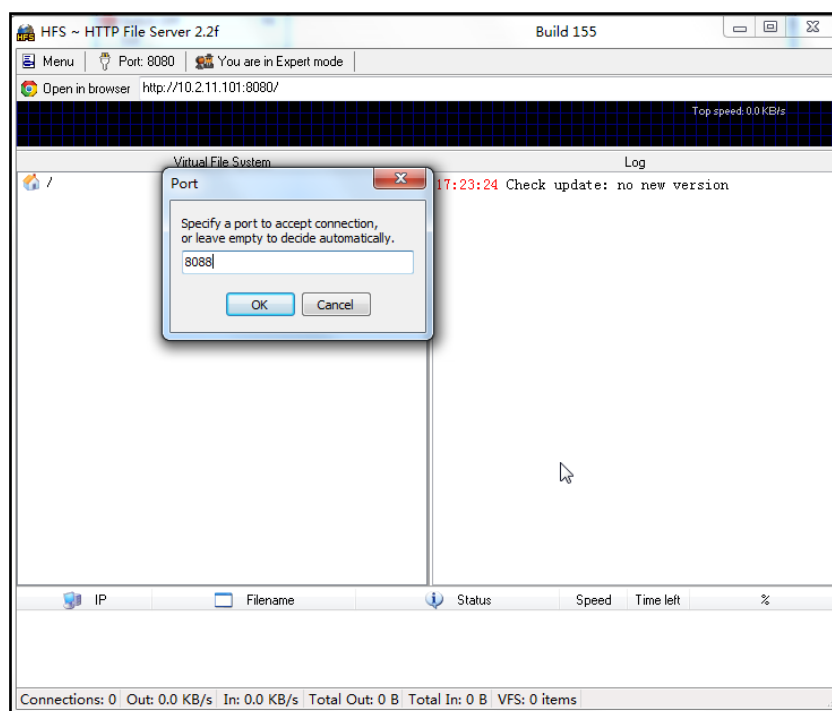
The main configuration page is shown as below:



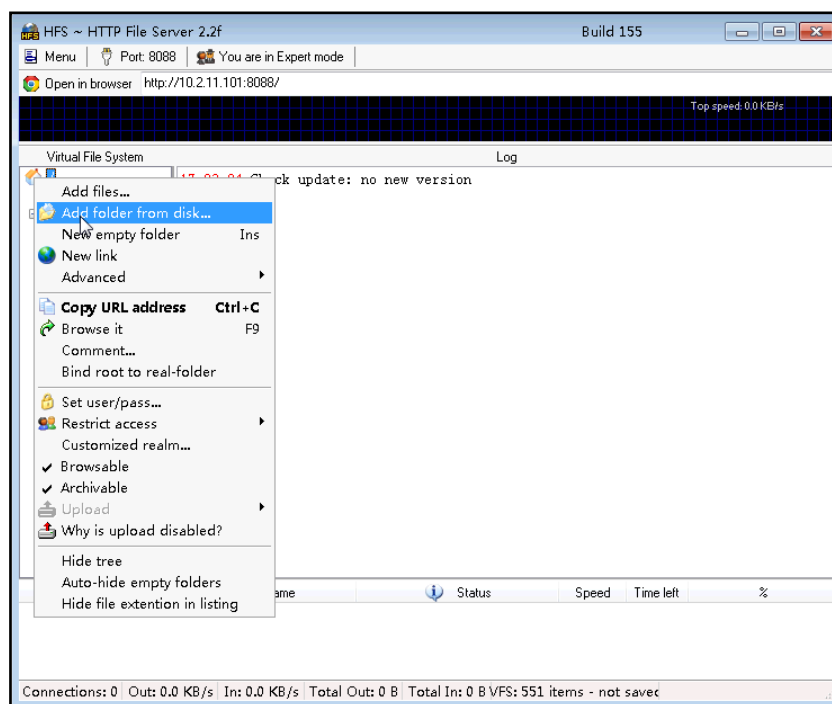
2. Click **Menu** in the main page and select the IP address of the PC from **IP address**.



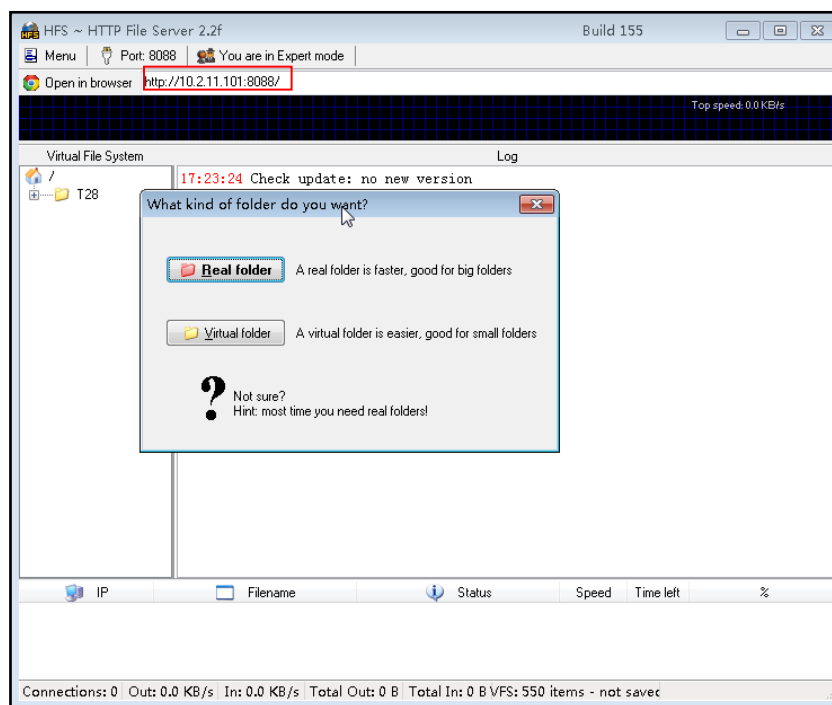
The default HTTP port is 8080. You can also reset the HTTP port (make sure the port isn't used before you reset).



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 the computer system. Select the kind of folder which you want.



5. Check the server URL "http:// IP:Port/" in the "Open in browser" address bar (For example, the server URL "http:// 10.2.11.101:8088/" is showed on the screenshot) . We recommend that you can fill the server URL in the address bar of the web browser and then press <Enter> key to check the HTTP server before provisioning.

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 about installing and configuring an Apache HTTPS Server, refer to the network resource.

Configuring a DHCP server

This section shows you how to configure a DHCP server for windows using DHCP Turbo. You can down this software from website at: <http://www.tucows.com/preview/265297> and install it following the setup wizard.

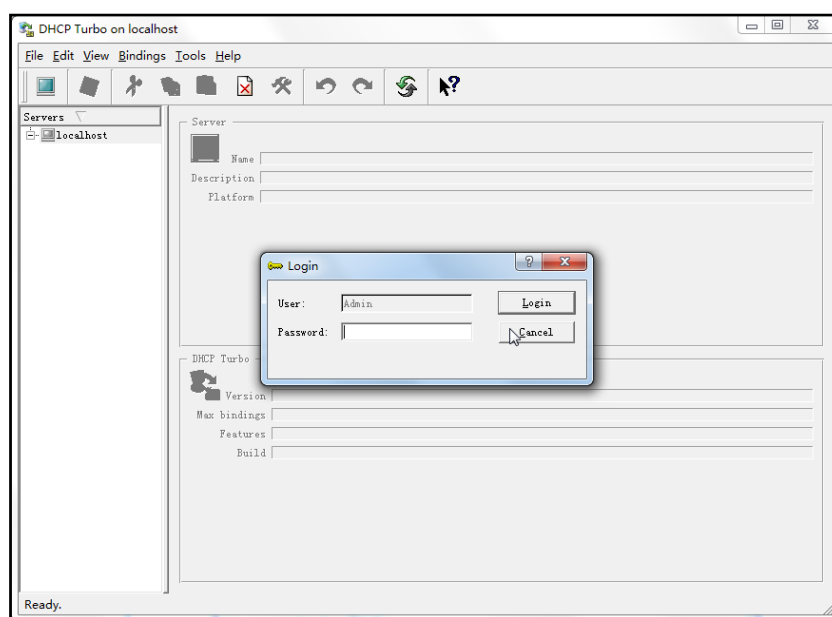
Before configuring the DHCP Turbo, make sure that:

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

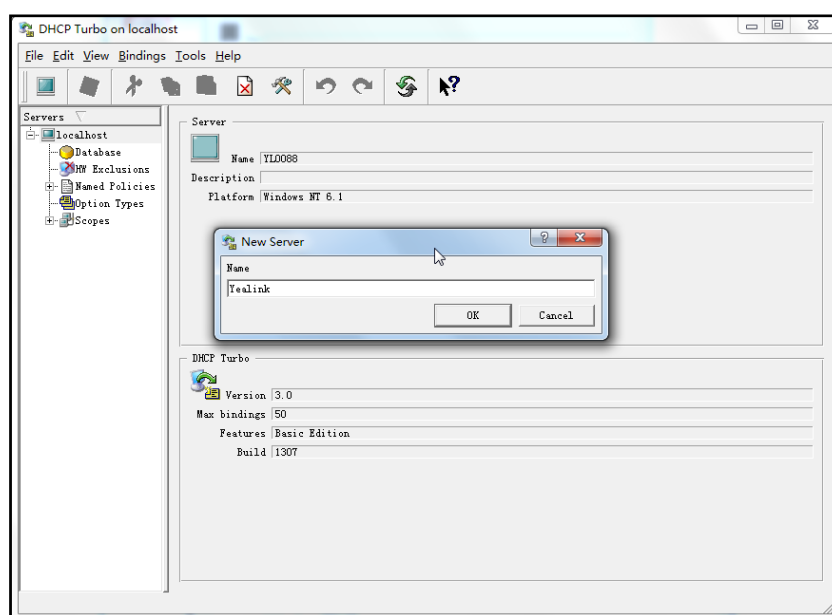
To configure the DHCP Turbo:

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

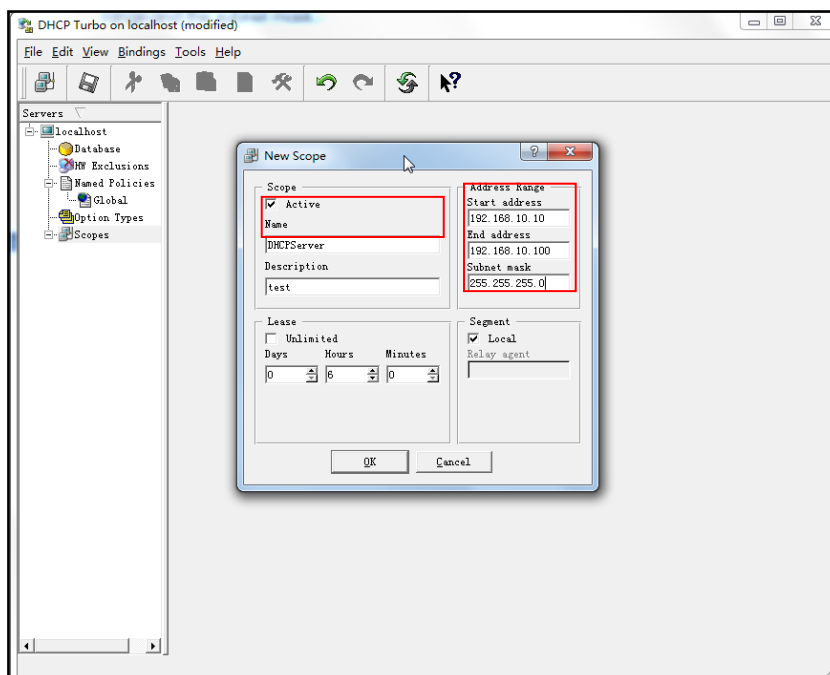
- Click the **Login** button (the login password is blank) to log in.



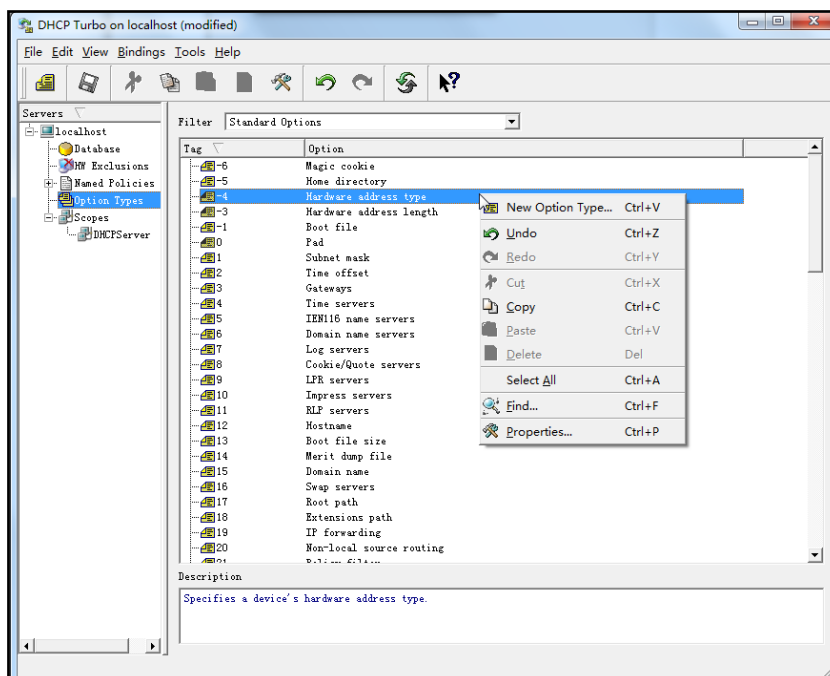
- You can then edit the existed DHCP server, or you can right click the **localhost** and select **"New Server"** to add a new DHCP server.



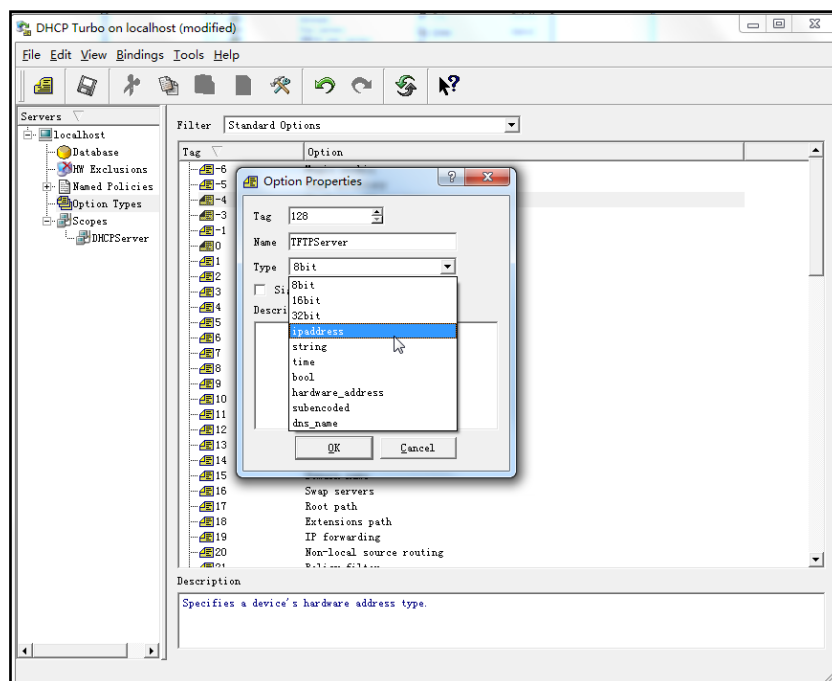
4. Right click the **Scopes** and select **New Scope**.
5. Configure the DHCP server name, the DHCP IP range and the subnet mask.



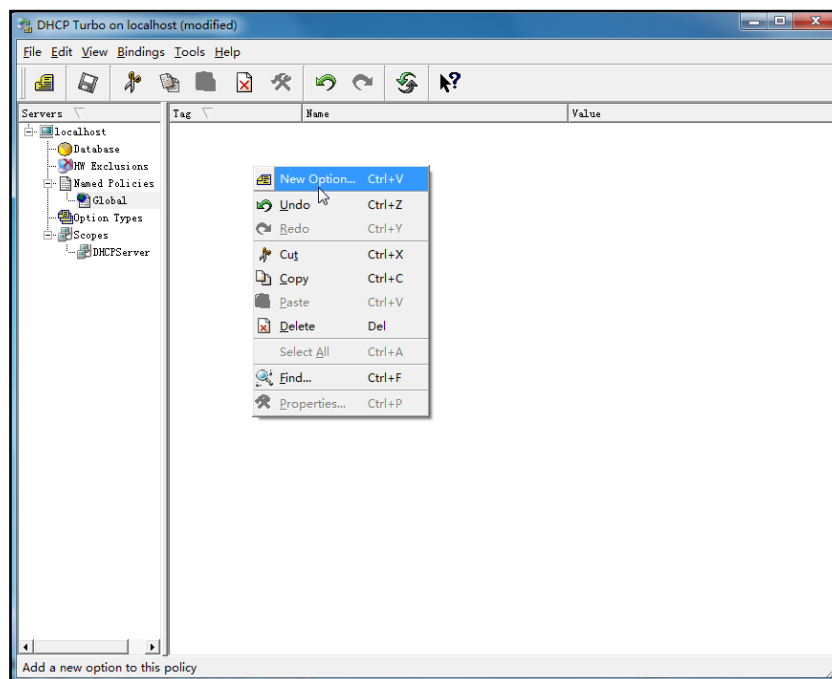
6. You can add a custom option via DHCP Turbo. Click **Option Type**, right click and select the **New Option Type** on the right of the main page.



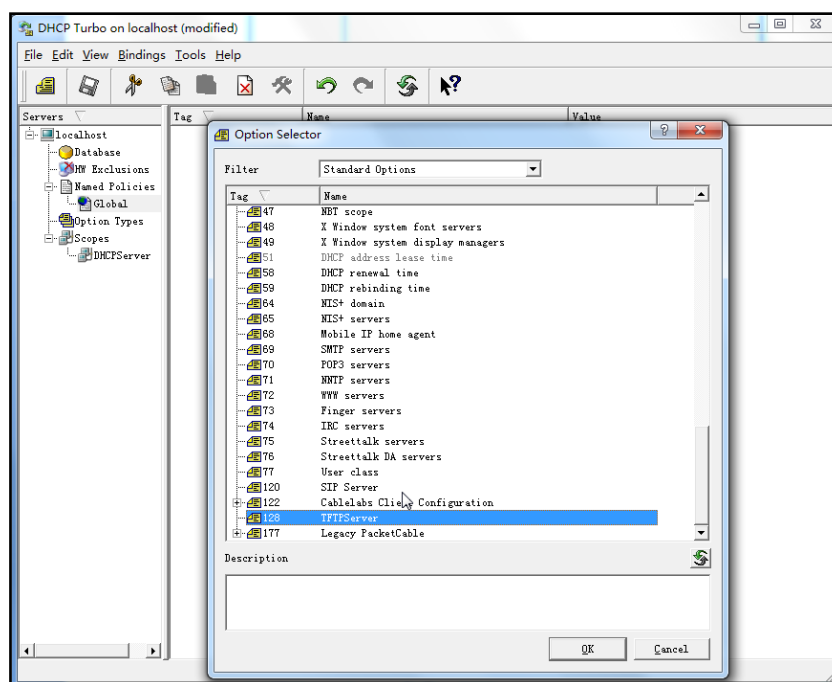
- Set the custom DHCP option (custom DHCP option tag number ranges from 128 to 254) and select the option type (Yealink support the **String** and **IP Address** option type only). Click the **OK** button to finish setting the option properties. Click  to save the change.



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



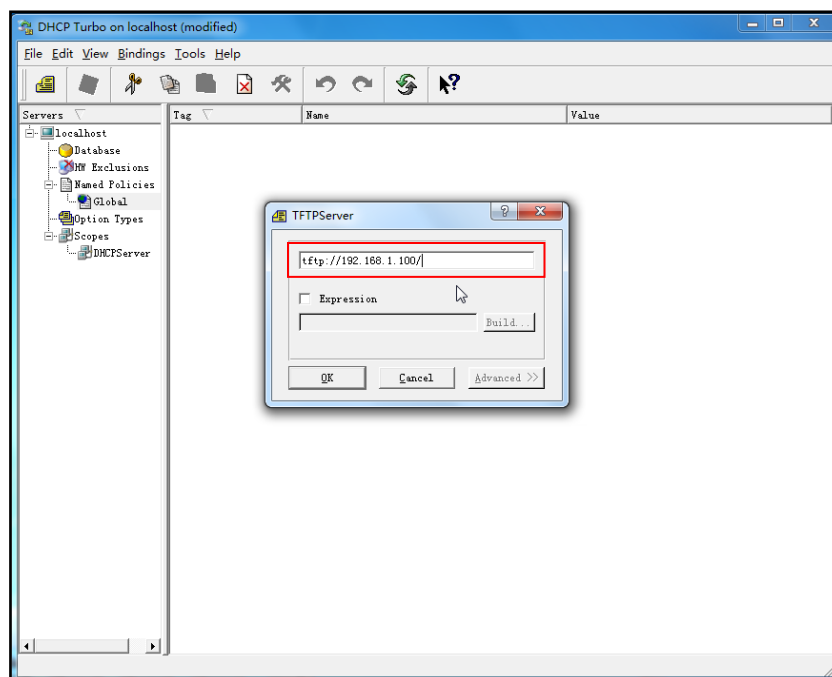
9. Scroll down and double click the custom option 128.



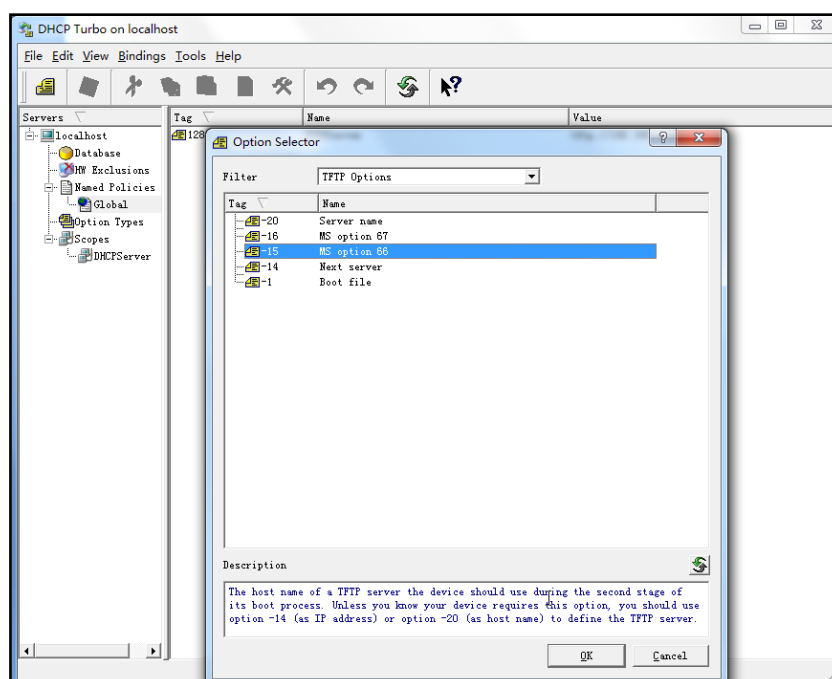
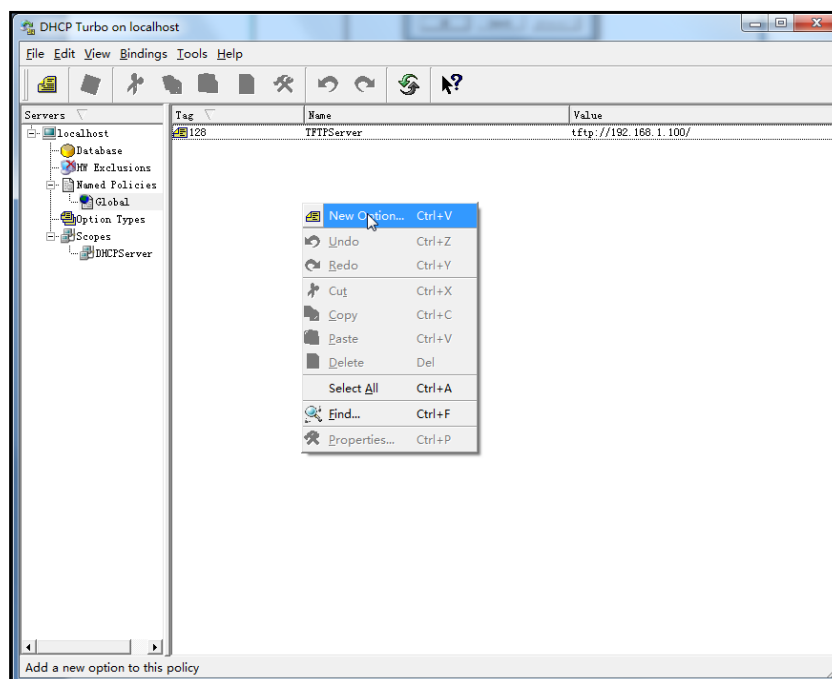
10. Fill the provisioning server address in the input field.

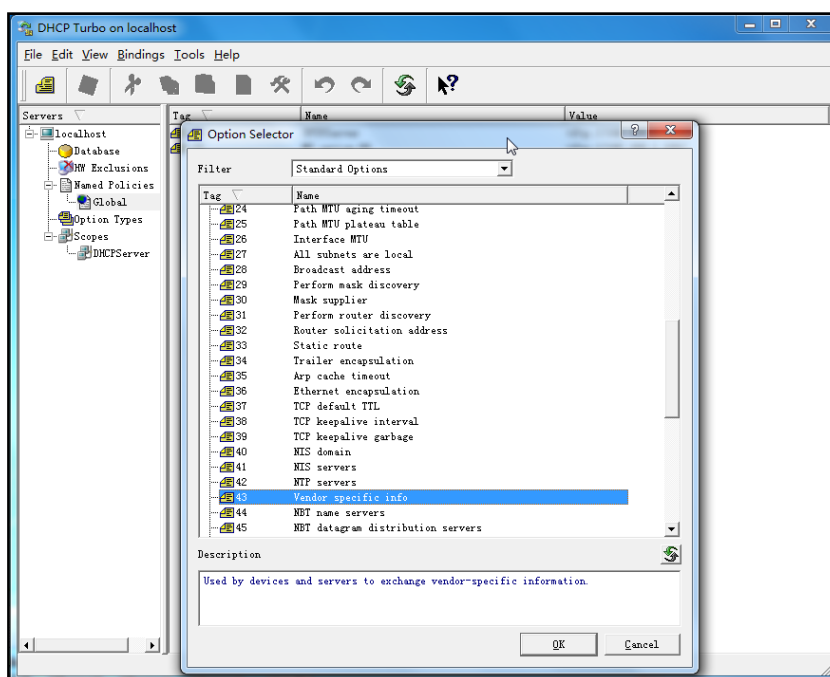
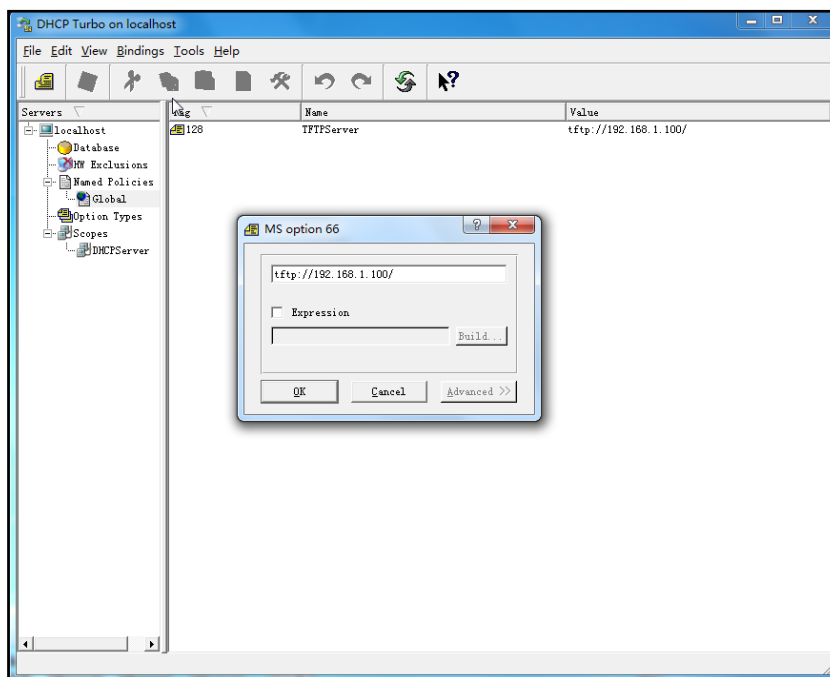
11. Click the **OK** button to finish setting a custom option.

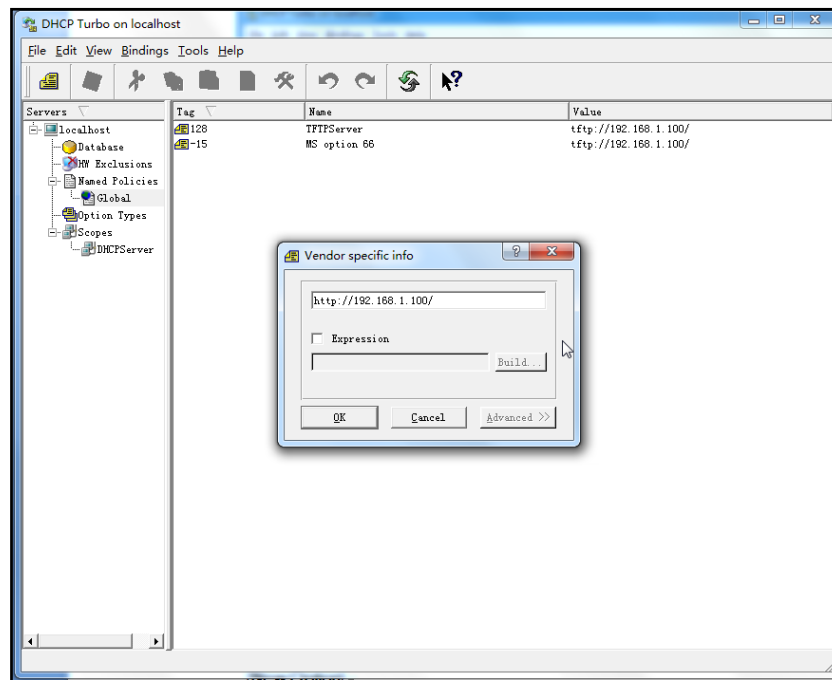
12. Click  to save the change.



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







Customizing a Ringtone Using CoolEdit Pro

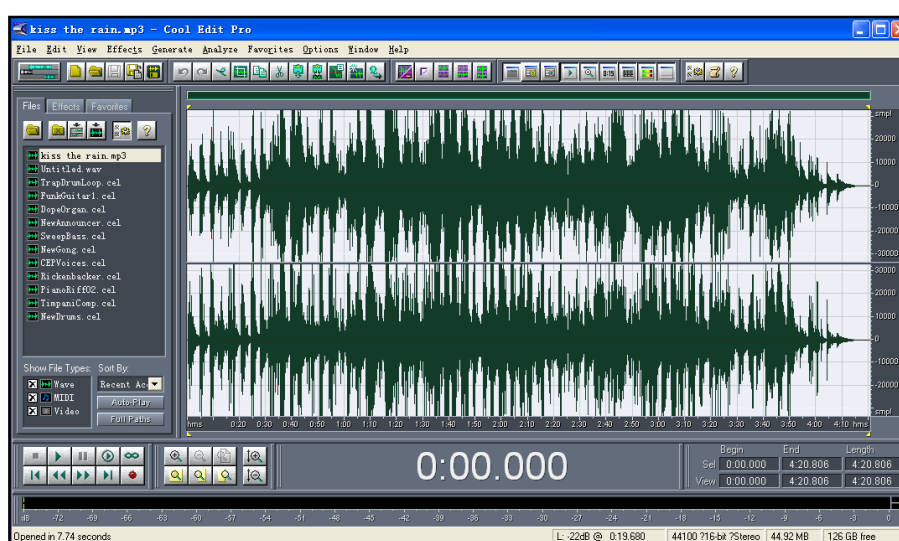
If you have installed the Cool Edit application, double click to open it. Otherwise, you can download the installation package from the website:

http://www.toggle.com/lv/group/view/k136218/Cool_Edit_Pro.htm and install it.

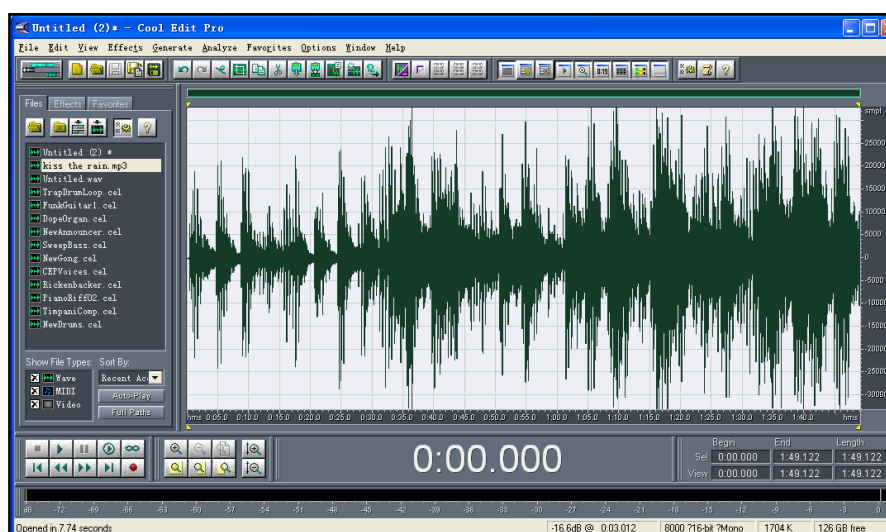
To customize a ringtone using Cool Edit Pro:

1. Open the **Cool Edit Pro** application.
2. Click **File** to open an audio file.
3. Locate the ringtone file, click **Open**, the file is uploaded as follows.

A sample audio file loaded is shown as below:



4. Select and copy the audio waveform.
5. Select **File->New** to create a new file, set the audio format as **PCMU**, the channels as **Mono**, the sample rate as **8000** and the resolution as **16-bit**.
6. Paste the audio waveform to the new file.

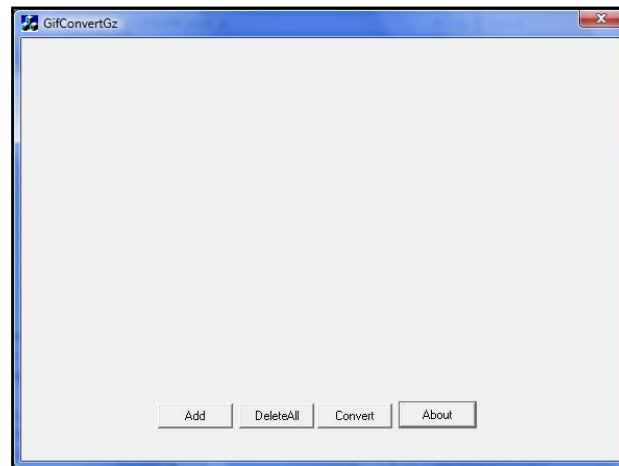


7. Select **File->Save as** to save the new audio file. On the Save waveform page, select the file format as **A/mu-law wave**.

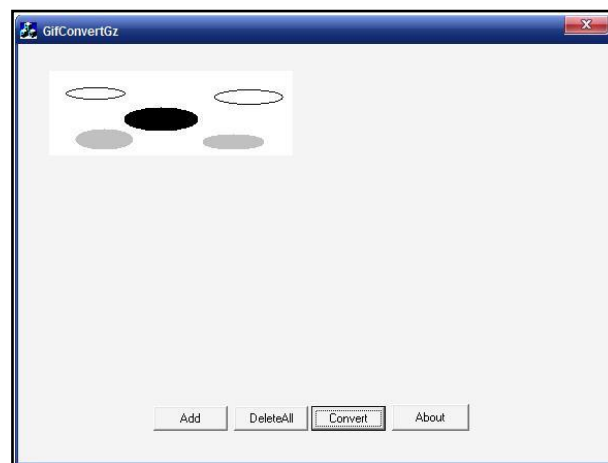
Customizing a Logo File Using PictureExDemo

The original picture format must be .bmp or .gif. We recommend placing all files and the PictureExDemo application to the root directory of the PC.

1. Double click the PictureExDemo.exe.



2. Click **Add** button to open a .bmp or .gif file.
You can repeat the second step to add multiple original picture files.
3. Click the **Convert** button.



Then you can find the **.dob** logo files in the **adv** directory.