



Skype for Business® HD IP Phone Auto Provisioning Guide



Version 9.25
Oct.2017

Table of Contents

Table of Contents.....	iii
Introduction.....	1
Getting Started.....	3
Obtaining Configuration Files.....	3
Obtaining Phone Information.....	3
Provisioning Yealink Skype for Business Phones.....	5
Auto Provisioning Process.....	5
Major Tasks for Auto Provisioning.....	5
An Instance of Auto Provision Configuration	6
Managing Configuration Files	11
Editing Common CFG File.....	11
Editing MAC-Oriented CFG File.....	12
Creating a New CFG File.....	13
Encrypting Configuration Files.....	14
Customizing Resource Files	14
Configuring a Provisioning Server	17
Preparing a Root Directory	17
Configuring a TFTP Server	18
Obtaining the Provisioning Server Address	21
DHCP Options	21
Phone Flash	23
Triggering the Phone to Perform the Auto Provisioning	25
Power On.....	25
Repeatedly	26
Weekly	27
Auto Provision Now	28
Multi-mode Mixed.....	29

Auto Provisioning via Activation Code.....	29
Downloading and Verifying Configurations	33
Downloading Configuration Files.....	33
Resolving and Updating Configurations	33
Verifying Configurations	34
Troubleshooting.....	37
Glossary.....	39
Appendix.....	41
Configuring an FTP Server.....	41
Preparing a Root Directory	41
Configuring an FTP Server.....	42
Configuring an HTTP Server	44
Preparing a Root Directory	44
Configuring an HTTP Server	45
Configuring a DHCP Server.....	49
Configuring the DHCP Turbo.....	49
Add the Option 66 via DHCP Turbo	53
Add the Option 43 via DHCP Turbo	55

Introduction

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

Yealink Skype for Business 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 Skype for Business phones with the minimum settings required. Yealink Skype for Business 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 Skype for Business phones, including:

- Yealink T48S
- Yealink T46S
- Yealink T42S
- Yealink T41S

The auto provisioning process outlined in this guide applies to Yealink T48S/T46S/T42S/T41S Skype for Business phones running firmware version 9 or later. We recommend that Skype for Business phones running the latest firmware CANNOT be downgraded to an earlier firmware version. The new firmware is compatible with old configuration parameters, but not vice versa.

Getting Started

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

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

Obtaining Configuration Files

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

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

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

To download Common CFG and MAC-Oriented files:

1. Go to Yealink [Microsoft Skype for Business](#) page.
2. Download and extract the combined configuration files to your local system.

	<div>Other Documents</div> <div>Yealink BToE Connector for Lync(3.0.0.29).zip</div> <div>CFG_Templates.zip</div> <div>Resource Files.zip</div>
--	---

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

Obtaining Phone Information

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

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

Hardware version: The current hardware version of the Skype for Business phone. You can view it via phone user interface or web user interface.

Account Information: Ask your system administrator Skype for Business account information.

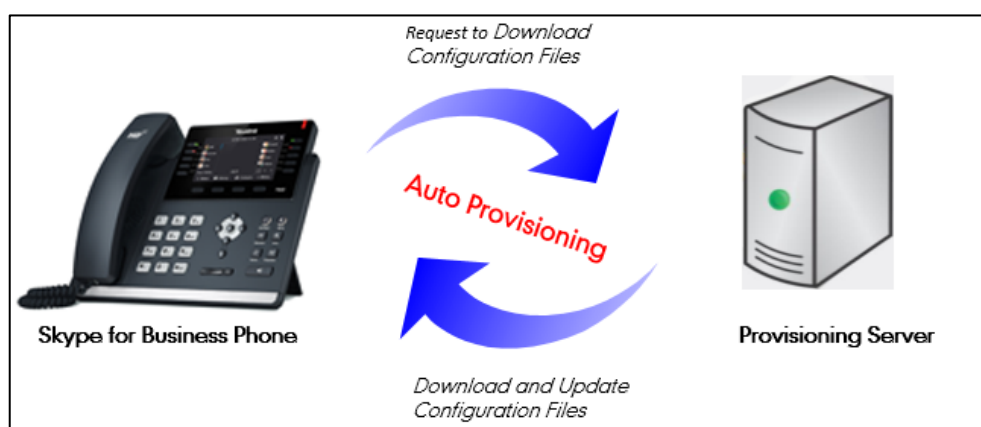
Provisioning Yealink Skype for Business Phones

This section provides instructions on how Skype for Business 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.

Auto Provisioning Process

When Skype for Business 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 Skype for Business phone will download and update configuration files to the phone flash.

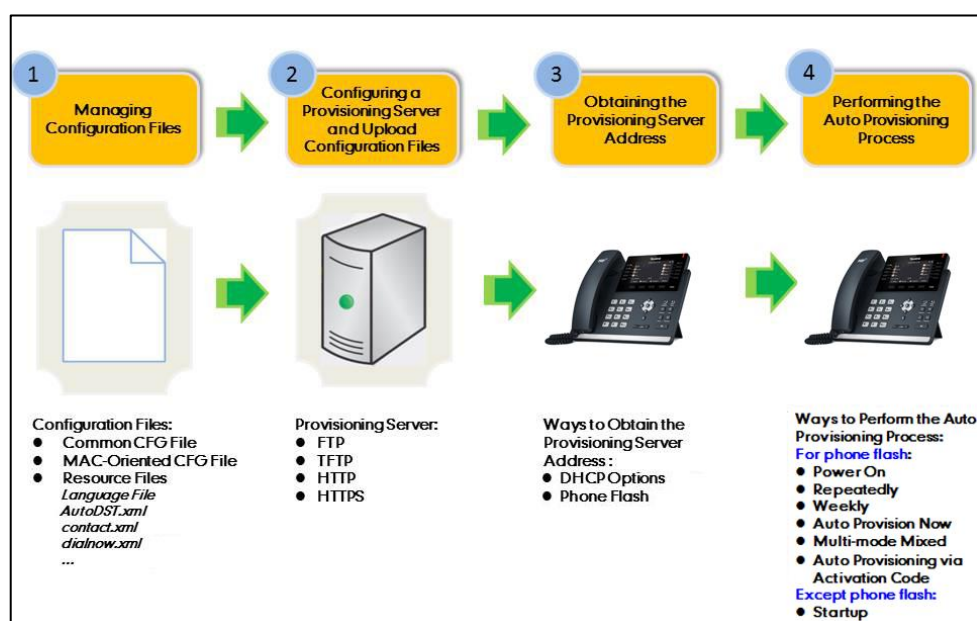
The following figure shows how the Skype for Business phone interoperates with the provisioning server:



Major Tasks for Auto Provisioning

You need to complete four major tasks to configure Yealink Skype for Business phones.

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



For more information on how to manage configuration files, refer to [Managing Configuration Files](#) on page 11.

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

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

For more information on how to perform the auto provisioning process, refer to [Triggering the Phone to Perform the Auto Provisioning](#) on page 25.

If you are not familiar with auto provisioning process on Yealink Skype for Business phones, you can refer to [An Instance of Auto Provision Configuration](#) on page 6.

An Instance of Auto Provision Configuration

This section shows an instance of auto provision configuration.

1. Manage configuration files.

Add/Edit the desired configuration parameters in the CFG file (e.g., y000000000066.cfg) you want the Skype for Business phone to download. For more information on how to manage configuration files, refer to [Managing Configuration Files](#) on page 11.

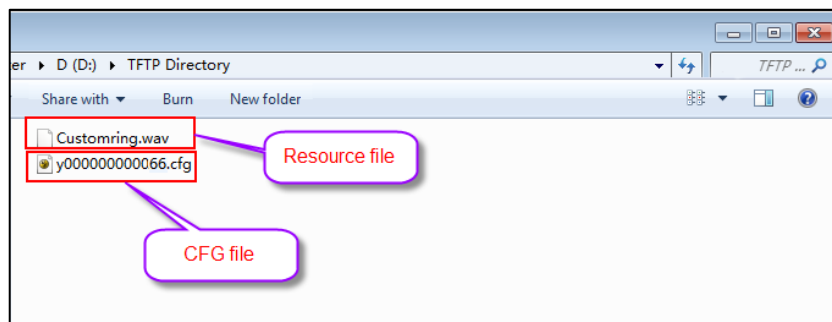
```

0 10 20 30 40 50 60
1 #!version:1.0.0.1
2 ringtone.url = tftp://192.168.1.100/Customring.wav

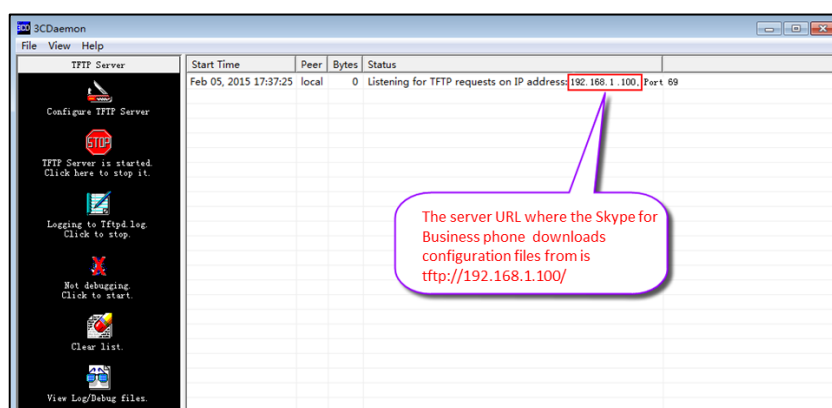
```

2. Configure the TFTP server.

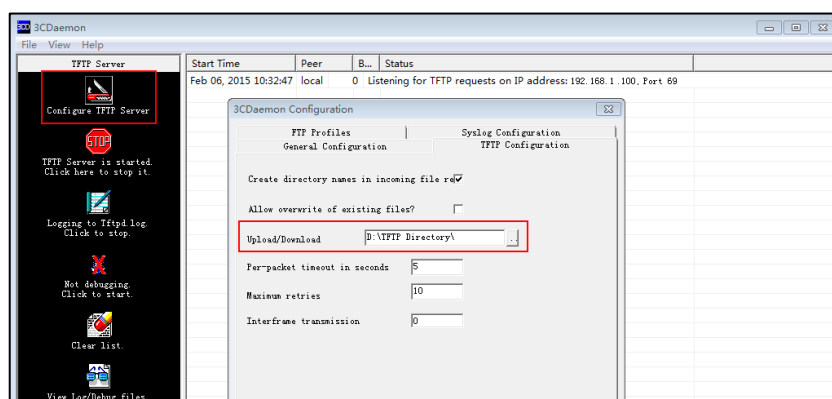
1) Place configuration files to TFTP root directory (e.g., D:\TFTP Directory).



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



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



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

- Configure the provisioning server address on the Skype for Business phone.

The screenshot shows the Yealink T46G web interface. The 'Settings' tab is selected, and the 'Auto Provision' sub-tab is active. The 'Server URL' field is highlighted with a red box. A callout bubble points to this field with the text: "Enter the access URL of the provisioning server in the Server URL field". The 'Server URL' field contains the text "http://192.168.1.100/". Other fields like 'User Name', 'Password', 'Common AES Key', and 'MAC-Oriented AES Key' are also visible but not highlighted. The 'Auto Provision' section includes various settings like 'PNP Active', 'DHCP Active', 'Custom Option(128~254)', 'DHCP Option Value', 'Wait Time(0~100s)', 'Power On', 'Repeatedly', 'Interval(Minutes)', 'Weekly', 'Time', and 'Day of Week'.

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

- Trigger the Skype for Business phone to perform the auto provisioning.

The screenshot shows the same Yealink T46G web interface as the previous one. The 'Auto Provision' sub-tab is still active. The 'Autoprovision Now' button at the bottom of the settings list is highlighted with a red box. A callout bubble points to this button with the text: "Click the Autoprovision Now to perform the auto provisioning process immediately". The 'Server URL' field is still visible and contains the same text as in the previous screenshot.

For more information on how to trigger the phone to perform the auto provisioning, refer to [Triggering the Phone to Perform the Auto Provisioning](#) on page 25.

Managing Configuration Files

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

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

For more information on description of all configuration parameters in configuration files, refer to

[*Yealink_Skype_for_Business_Edition_HD_IP_Phones_Description_of_Configuration_Parameters_in_CFG_Files.*](#)

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 Skype for Business phone model.

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

Phone Model	Common CFG file
T48S	y000000000065.cfg
T46S	y000000000066.cfg
T42S	y000000000067.cfg
T41S	y000000000068.cfg

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

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

```
#!version:1.0.0.1

#####
##                               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.ipv4_static_dns_enable =
```

When editing the Common CFG file, learn the following:

- The line beginning with “#” is considered to be a comment.
- The file header “#!version:1.0.0.1” is not a comment and must be placed in the first line. It cannot be edited or deleted.
- The file format must be *.cfg.
- The filename complies with the requirements that are listed in the above table.
- Each line must use the following format and adhere to the following rules:

Configuration Parameter=Valid Value

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

Editing MAC-Oriented CFG File

The MAC-Oriented CFG 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:

```
#!/version:1.0.0.1

#####
##                               Account                               ##
#####

##Username
account.1.sign_in.server_address =
account.1.sign_in.user_name =
account.1.sign_in.password =

###PIN
account.1.sign_in.pin_number =
account.1.sign_in.pin_password =

##It configures the login authentication method.
account.1.auth_method=

#####
##                               Account                               ##
#####
account.1.ews.auth_address=
account.1.ews.auth_user=
account.1.ews.auth_pwd=
```

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

- The line beginning with “#” is considered to be a comment.
- The file header “#!/version:1.0.0.1” is not a comment and must be placed in the first line. It cannot be edited or deleted.
- The file format must be *.cfg.
- The filename matches the MAC address of your phone.
- Each line must use the following format and adhere to the following rules:
Configuration Parameter=Valid Value
 - Separate each configuration parameter and value with an equal sign.
 - Set only one configuration parameter per line.
 - Put the configuration parameter and value on the same line, and do not break the line.

Creating a New CFG File

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

To create a new CFG file:

1. Create a CFG file for your phone. Ensure the file complies with the guidelines that are listed in [Editing Common CFG File](#) on page 11 or [Editing MAC-Oriented CFG File](#) on page 12.

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

```
#!version:1.0.0.1

#####
##                               Call Waiting                               ##
#####
call_waiting.enable = 1
call_waiting.tone = 1

#####
##                               Key Lock                                ##
#####

sfb.phone_lock.time_out = 10
sfb.phone_lock_with_pc.enable = 1
sfb.phone_lock.max_attempts = 5
```

3. Save the changes and close the CFG file.

Encrypting Configuration Files

To protect against unauthorized access and tampering of sensitive information (e.g., login password, registration information), you can encrypt configuration files using Yealink Configuration Encryption Tool. AES keys must be 16 characters and the supported characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # \$ % * + , - . : = ? @ [] ^ _ { } ~. For more information on how to encrypt configuration files, refer to [Yealink Configuration Encryption Tool User Guide](#).

Customizing Resource Files

When configuring some particular features, you may need to upload resource files to Skype for Business 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
Keypad Input Method File	ime.txt
Dial-now Template	dialnow.xml
Contact File	contact.xml

Ask the distributor or Yealink FAE for resource file templates. For more information on

explanations of the configuration parameters, refer to
[*Yealink_Skype_for_Business_HD_IP_Phones_Administrator_Guide.*](#)

Configuring a Provisioning Server

Yealink Skype for Business phones support using FTP, TFTP, HTTP and HTTPS protocols to download configuration files. You can use one of these protocols for provisioning. The TFTP protocol is used by default. The following section provides instructions on how to configure a TFTP server.

We recommend that you use 3CDaemon or TFTP32 as a TFTP server. 3CDaemon and TFTP32 are free applications for Windows. You can download 3CDaemon online:

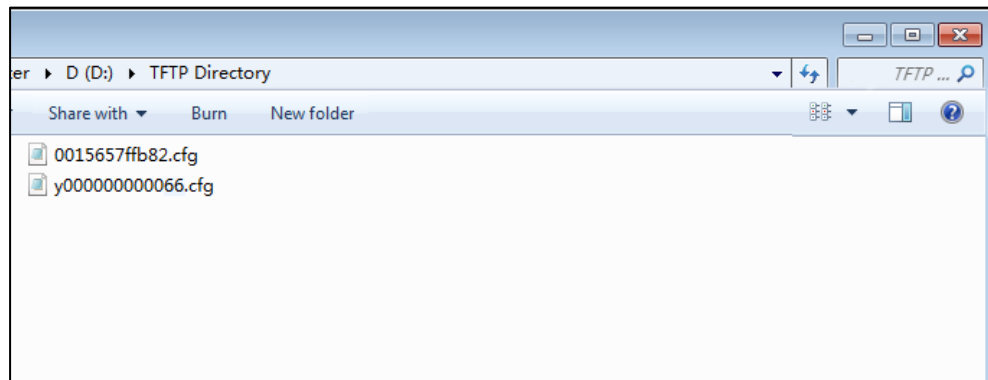
<http://www.oldversion.com/3Com-Daemon.html> and TFTP32 online: <http://tftpd32.jounin.net/>.

For more information on how to configure FTP and HTTP servers, refer to [Configuring an FTP Server](#) on page 41 and [Configuring an HTTP Server](#) on page 44.

Preparing a Root Directory

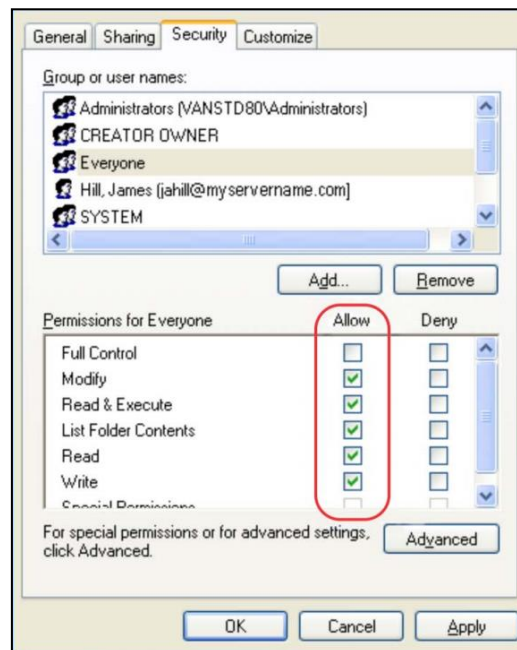
To prepare a root directory:

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



3. (Optional.) Set security permissions for the TFTP directory folder.
You need to define a user or a group name, and set the permissions: read, write or modify.
Security permissions vary by organizations.

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

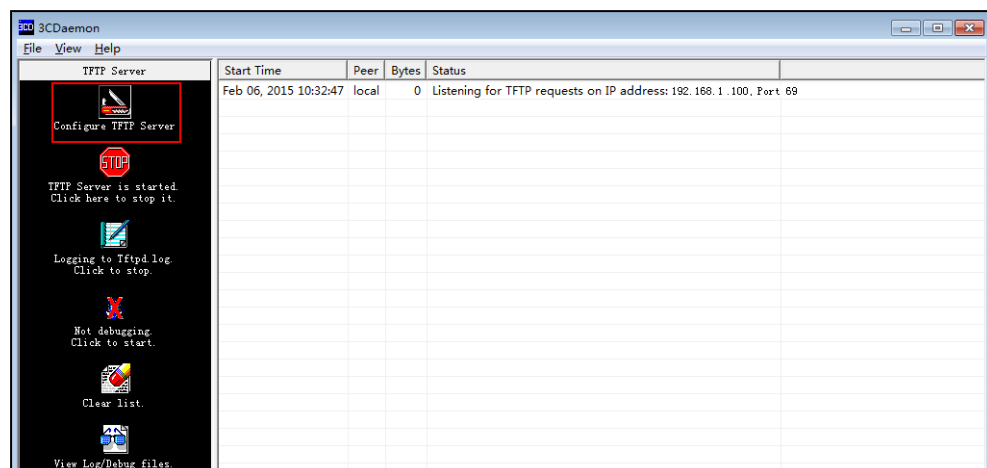



Configuring a TFTP Server

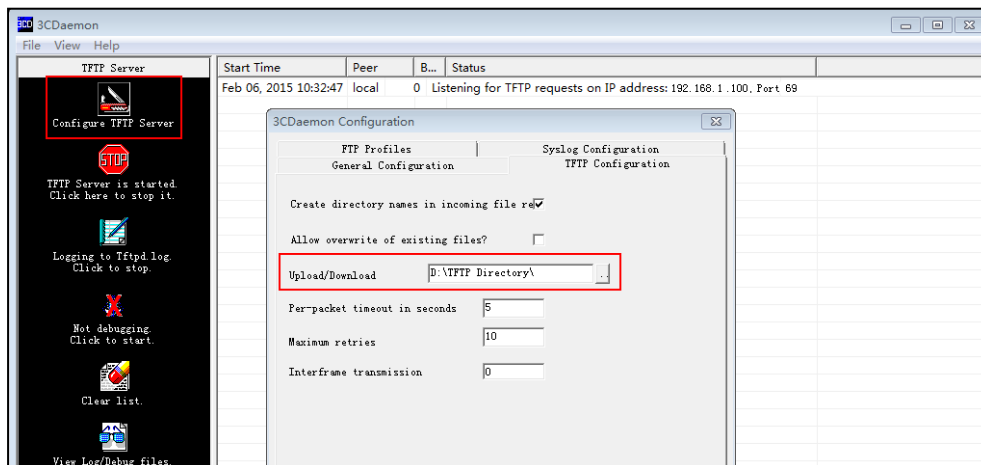
If you have a 3CDaemon application installed on your local system, use it directly. Otherwise, download and install it.

To configure a TFTP server:

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



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



3. Click the **Confirm** button to finish configuring the TFTP server.

The server URL "tftp://IP/" (Here "IP" means the IP address of the provisioning server, for example, "tftp://192.168.1.100/") is where the Skype for Business phone downloads configuration files from.

Obtaining the Provisioning Server Address

Yealink Skype for Business 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 T46S Skype for Business phone as an example).

DHCP Options

Yealink Skype for Business 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](#) on page 49.

To configure the DHCP option via web user interface:

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

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

The screenshot shows the Yealink T46G web interface with the 'Settings' tab selected. The 'Auto Provision' section is expanded, showing various configuration options. The 'Custom Option(128~254)' field is highlighted with a red box and contains the value '160,161'. Other visible settings include PNP Active (On), DHCP Active (On), DHCP Option Value (MS-UC-Client), Server URL, User Name, Password, Common AES Key, MAC-Oriented AES Key, Zero Active (Disabled), Wait Time (5s), Power On (On), Repeatedly (Off), Interval (1440), Weekly (On), Time (00:00 -- 00:00), and Day of Week (all days selected). A 'NOTE' box on the right states: 'Auto Provision The auto provision parameters for administrator. You can click here to get more guides.'

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

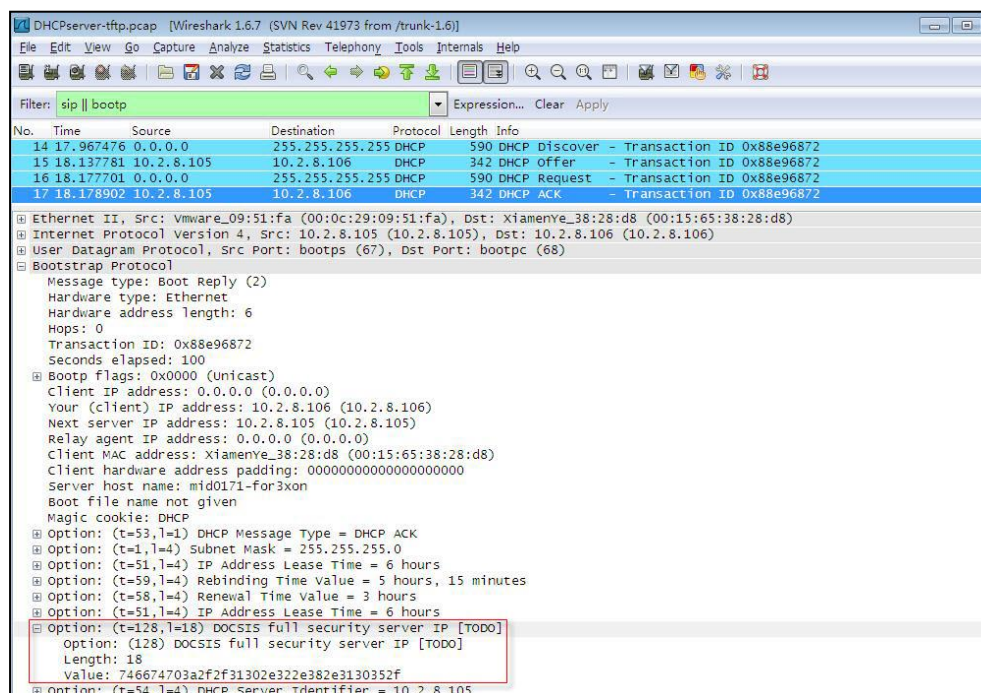
During startup, the phone will broadcast DHCP request with DHCP options for obtaining the provisioning server address. The provisioning server address will be found in the received DHCP response message.

After the Skype for Business 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_Skype_for_Business_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 Skype for Business 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**.

- Enter the URL, user name and password of the provisioning server in the **Server URL**, **User Name** and **Password** fields respectively (the user name and password are optional).

The screenshot shows the Yealink T46S web interface with the 'Auto Provision' settings page. The 'Server URL', 'User Name', and 'Password' fields are highlighted with a red box. The 'Server URL' field contains 'http://192.168.1.100/y00000000066.cf'. The 'User Name' and 'Password' fields are empty. The 'Auto Provision' section includes various settings like PNP Active, DHCP Active, Custom Option, DHCP Option Value, Common AES Key, MAC-Oriented AES Key, Zero Active, Wait Time, Power On, Repeatedly, Interval, Weekly, and Time.

- 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](#) on Page 25.

Note

You can also enter "M7:configuration parameter" (for example: **M7:local_time.manual_time_enable = 1**) in the **Server URL** field, and then trigger the phone to perform the auto provisioning directly.

Triggering the Phone to Perform the Auto Provisioning

This chapter introduces the following methods to trigger the Skype for Business phone to perform the auto provisioning process:

- [Power On](#)
- [Repeatedly](#)
- [Weekly](#)
- [Auto Provision Now](#)
- [Multi-mode Mixed](#)
- [Auto Provisioning via Activation Code](#)

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 Skype for Business 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. Mark the **On** radio box in the **Power On** field.

The screenshot shows the Yealink T46S web interface with the 'Settings' tab selected. The 'Auto Provision' section is active, displaying various configuration options. The 'Power On' field, which includes radio buttons for 'On' and 'Off', is highlighted with a red rectangular box. Other visible settings include PNP Active, DHCP Active, Custom Option(128~254), DHCP Option Value, Server URL, User Name, Password, Common AES Key, MAC-Oriented AES Key, Zero Active, Wait Time(1~100s), Repeatedly, Interval(Minutes), Weekly, and Time. A 'NOTE' section on the right explains the auto provision parameters for administrators.

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

Repeatedly

The Skype for Business phone performs the auto provisioning process at regular intervals. You can configure the interval for the repeatedly mode. The default interval is 1440 minutes.

To activate the repeatedly mode via web user interface:

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

2. Mark the **On** radio box in the **Repeatedly** field.
3. Enter the desired interval time (in minutes) in the **Interval(Minutes)** field.

The screenshot shows the Yealink T46S web interface with the 'Settings' tab selected. The 'Auto Provision' section is active, displaying various configuration options. The 'Repeatedly' radio button is selected and highlighted with a red box. The 'Interval(Minutes)' field is set to 1440. Other visible settings include PNP Active, DHCP Active, Custom Option(128~254), DHCP Option Value, Server URL, User Name, Password, Common AES Key, MAC-Oriented AES Key, Zero Active, Wait Time(1~100s), Power On, and Weekly. A 'NOTE' section on the right states: 'Auto Provision The auto provision parameters for administrator. You can click here to get more guides.'

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

Weekly

The Skype for Business 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 Skype for Business phone to perform the auto provisioning process. For example, you can configure the Skype for Business 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. Mark the **On** radio box in the **Weekly** field.
3. Enter the desired time in the **Time** field.

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

The screenshot shows the Yealink T46S web interface with the 'Settings' tab selected. The 'Auto Provision' section is active, and the 'Day of Week' subsection is highlighted with a red box. In this subsection, the 'Weekly' radio button is selected, and the 'Time' is set to 00:00. All days of the week (Sunday through Saturday) are checked under the 'Day of Week' field. The 'Autoprovision Now' button is located at the bottom of this section. Other settings visible include PNP Active, DHCP Active, Custom Option (128~254) set to 160,161, DHCP Option Value set to MS-UC-Client, Server URL, User Name, Password, Common AES Key, MAC-Oriented AES Key, Zero Active set to Disabled, Wait Time (1~100s) set to 5, Power On set to On, Repeatedly set to Off, and Interval (Minutes) set to 1440.

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 **Autoprovision Now**.

The screenshot shows the Yealink T46S web interface with the 'Settings' tab selected. The left sidebar lists various configuration categories, with 'Auto Provision' highlighted. The main content area displays the 'Auto Provision' settings, including options for PNP Active, DHCP Active, Custom Option, DHCP Option Value, Server URL, User Name, Password, Common AES Key, MAC-Oriented AES Key, Zero Active, Wait Time, Power On, Repeatedly, Interval, Weekly, Time, and Day of Week. At the bottom of the settings list, the 'Autoprovision Now' button is highlighted with a red rectangular box. A 'NOTE' section on the right side of the interface provides additional information about the auto provision parameters.

The Skype for Business phone will perform the auto provisioning process immediately.

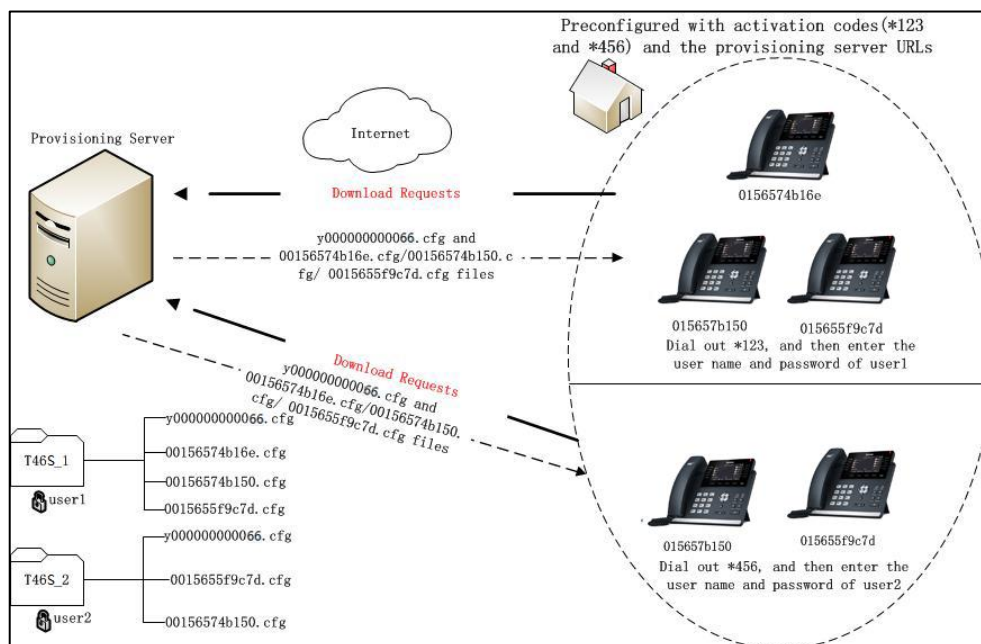
Multi-mode Mixed

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

Auto Provisioning via Activation Code

In addition to the updating modes introduced above, users can trigger Skype for Business phones to perform auto provisioning by dialing an activation code. To use this method, the activation code and the provisioning server address need to be pre-configured on the Skype for Business phones.

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



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

1. Create multiple directories (e.g., T46S_1 and T46S_2) on the provisioning server.
2. Store a common CFG file and multiple <MAC>.cfg files to each directory on the provisioning server.
3. (Optional) Configure a user name and password for each directory.

The user name and password provides a means of conveniently partitioning the configuration files for different phones. To access the specified directory, you need to provide the correct user name and password configured for the directory. For more information on how to configure a user name and password using HTTP server, refer to [Configuring an HTTP Server on page 45](#).
4. Configure unique activation codes and the provisioning server URLs on Skype for Business phones.

The activation code can be numeric characters, special characters "#", "*" or a combination of them within 32 characters.

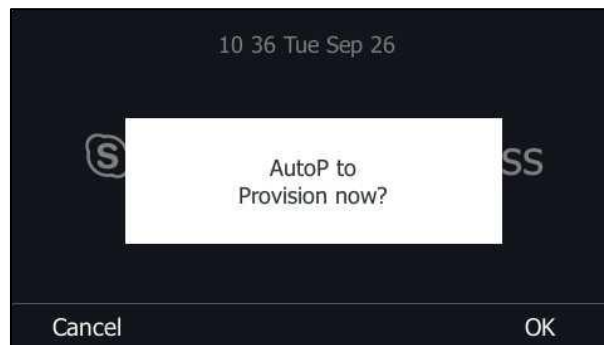
The following are example configurations in the configuration file for Skype for Business phones:

```
static.autoprovision.1.code = *123
static.autoprovision.1.url = http://192.168.1.30/T46S_1/
static.autoprovision.2.code = *456
static.autoprovision.2.url = http://192.168.1.30/T46S_2/
```

5. Send the specified activation code, associated user name and password to each end-user.

6. The user can set up the Skype for Business phone, and then input the activation code (for example: *123) after the phone startup (make sure no one has signed in).

The LCD screen will prompt the following dialog box:



7. Press the **OK** soft key to trigger the Skype for Business phone to perform auto provisioning.

The LCD screen will prompt the following input box:

 A screenshot of a phone's LCD screen titled 'Autop Authority'. It contains two input fields: '1. User Name:' and '2. Password:'. Below these fields, there are four buttons: 'Cancel', '2aB', 'Delete', and 'OK'.

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

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

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

The entered user name and password will be saved to the Skype for Business phones for next auto provisioning.

The LCD screen will not prompt for user name and password if the provisioning server does not require authentication, or the user name and password are already saved on the Skype for Business phones.

The following parameters are used to configure the auto provisioning via activation code method (X ranges from 1 to 50):

#(Optional.) Configure the code name for triggering auto provisioning.

static.autoprovision.X.name

#Configure the activation code.

static.autoprovision.X.code

#Configure the URL of the provisioning server.

static.autoprovision.X.url

#Configure the username and password for the directory where the configuration files are located. If configured, the LCD screen will not prompt for user name and password.

static.autoprovision.X.user

static.autoprovision.X.password

Downloading and Verifying Configurations

Downloading Configuration Files

After obtaining the provisioning server address in one of the ways introduced above, the phone will request to download the configuration files from the provisioning server when it is triggered to perform auto provisioning. During the auto provisioning process, the Skype for Business phone will try to download the Common CFG file firstly, and then try to download the MAC-Oriented CFG file from the provisioning server. If the access URLs of the resource files have been specified in the configuration files, the phone will try to download the resource files.

Resolving and Updating Configurations

After downloading, the phone resolves the configuration files and resource files (if specified in the configuration files), and then updates the configurations and resource files to the phone flash. Generally, updated configurations will automatically take effect after the auto provisioning process is completed. For update of some specific configurations which require a reboot before taking effect, for example, network configurations, the phone will reboot to make the configurations effective after the auto provisioning process is completed.

The Skype for Business 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

[Yealink_Skype_for_Business_Edition_HD_IP_Phones_Description_of_Configuration_Parameters_in_CFG_Files](#).

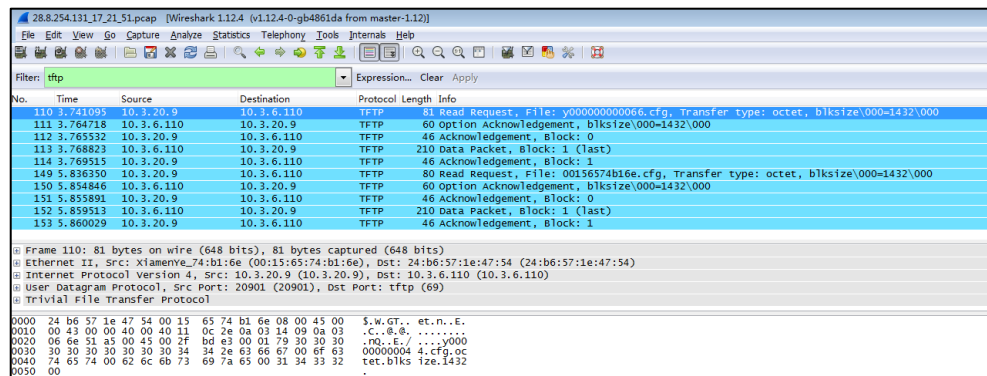
If configuration files have been AES encrypted, the phone will use the Common AES key to decrypt the Common CFG file and the MAC-Oriented AES key to decrypt the <MAC>.cfg file after downloading the configuration files. For more information on how the phone decrypts configuration files, refer to [Yealink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

Verifying Configurations

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

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

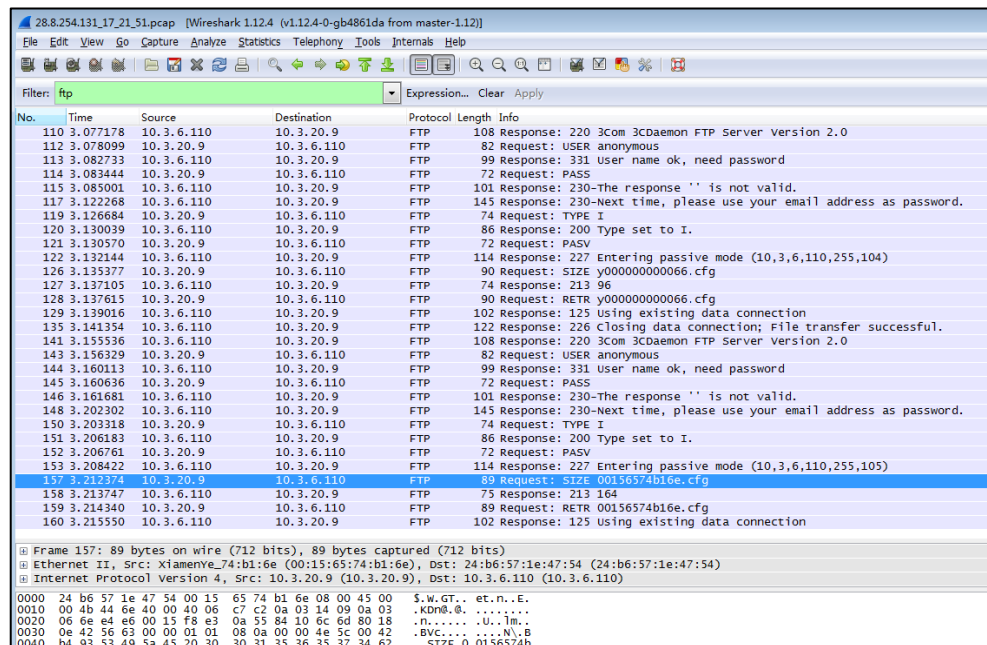
Example1: Yealink T46S Skype for Business phone downloads configuration files from the TFTP server.



Wireshark 1.12.4 capture of TFTP traffic. The filter is 'tftp'. The packet list shows a Read Request for file 'y0000000000066.cfg' and several Acknowledgements. The packet details pane shows the Read Request structure with fields like File, Transfer type, and Block size.

No.	Time	Source	Destination	Protocol	Length	Info
110	3.741095	10.3.20.9	10.3.6.110	TFTP	61	Read Request, File: y0000000000066.cfg, Transfer type: octet, blksize\000=1432\000
111	3.764718	10.3.6.110	10.3.20.9	TFTP	60	option Acknowledgement, blksize\000=1432\000
112	3.765532	10.3.20.9	10.3.6.110	TFTP	46	Acknowledgement, Block: 0
113	3.768823	10.3.6.110	10.3.20.9	TFTP	210	Data Packet, Block: 1 (last)
114	3.769515	10.3.20.9	10.3.6.110	TFTP	46	Acknowledgement, Block: 1
149	5.836350	10.3.20.9	10.3.6.110	TFTP	80	Read Request, File: 00156574b16e.cfg, Transfer type: octet, blksize\000=1432\000
150	5.854846	10.3.6.110	10.3.20.9	TFTP	60	option Acknowledgement, blksize\000=1432\000
151	5.855891	10.3.20.9	10.3.6.110	TFTP	46	Acknowledgement, Block: 0
152	5.859513	10.3.6.110	10.3.20.9	TFTP	210	Data Packet, Block: 1 (last)
153	5.860029	10.3.20.9	10.3.6.110	TFTP	46	Acknowledgement, Block: 1

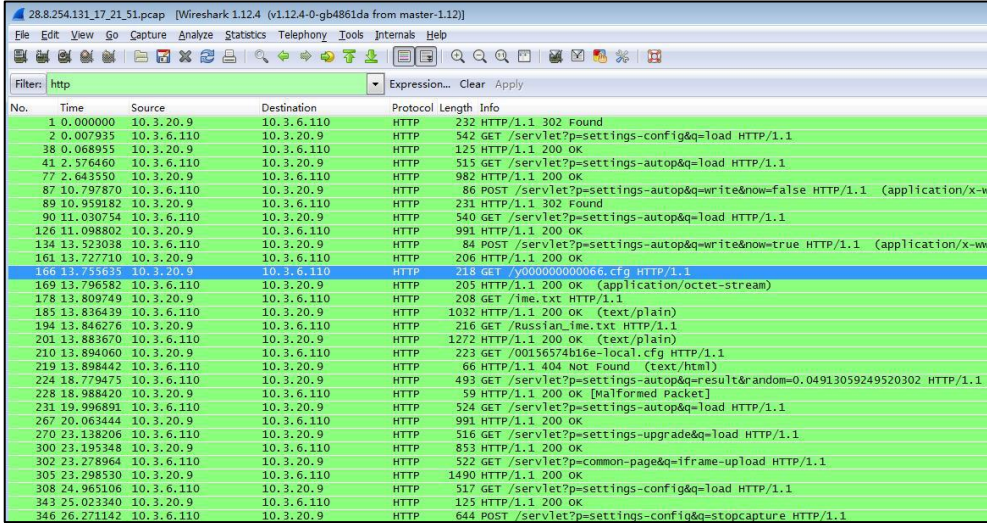
Example 2: Yealink T46S Skype for Business phone downloads configuration files from the FTP server.



Wireshark 1.12.4 capture of FTP traffic. The filter is 'ftp'. The packet list shows a series of commands and responses, including USER, PASS, TYPE, and RETR. The packet details pane shows the FTP structure with fields like Command, Response, and File name.

No.	Time	Source	Destination	Protocol	Length	Info
110	3.077178	10.3.6.110	10.3.20.9	FTP	108	Response: 220 3com 3Cdaemon FTP Server version 2.0
112	3.078099	10.3.20.9	10.3.6.110	FTP	82	Request: USER anonymous
113	3.082733	10.3.6.110	10.3.20.9	FTP	99	Response: 331 user name ok, need password
114	3.083444	10.3.20.9	10.3.6.110	FTP	72	Request: PASS
115	3.085001	10.3.6.110	10.3.20.9	FTP	101	Response: 230-The response '' is not valid.
117	3.122268	10.3.6.110	10.3.20.9	FTP	145	Response: 230-Next time, please use your email address as password.
119	3.126684	10.3.20.9	10.3.6.110	FTP	74	Request: TYPE I
120	3.130039	10.3.6.110	10.3.20.9	FTP	86	Response: 200 Type set to I.
121	3.130570	10.3.20.9	10.3.6.110	FTP	72	Request: PASV
122	3.132144	10.3.6.110	10.3.20.9	FTP	114	Response: 227 Entering passive mode (10,3,6,110,255,104)
126	3.135377	10.3.20.9	10.3.6.110	FTP	90	Request: SIZE y0000000000066.cfg
127	3.137105	10.3.6.110	10.3.20.9	FTP	74	Response: 213 96
128	3.137615	10.3.20.9	10.3.6.110	FTP	90	Request: RETR y0000000000066.cfg
129	3.139016	10.3.6.110	10.3.20.9	FTP	102	Response: 125 using existing data connection
135	3.141354	10.3.6.110	10.3.20.9	FTP	122	Response: 226 Closing data connection; File transfer successful.
141	3.155536	10.3.6.110	10.3.20.9	FTP	108	Response: 220 3com 3Cdaemon FTP Server version 2.0
143	3.156329	10.3.20.9	10.3.6.110	FTP	82	Request: USER anonymous
144	3.160113	10.3.6.110	10.3.20.9	FTP	99	Response: 331 user name ok, need password
145	3.160636	10.3.20.9	10.3.6.110	FTP	72	Request: PASS
146	3.161681	10.3.6.110	10.3.20.9	FTP	101	Response: 230-The response '' is not valid.
148	3.202302	10.3.6.110	10.3.20.9	FTP	145	Response: 230-Next time, please use your email address as password.
150	3.203318	10.3.20.9	10.3.6.110	FTP	74	Request: TYPE I
151	3.206183	10.3.6.110	10.3.20.9	FTP	86	Response: 200 Type set to I.
152	3.206761	10.3.20.9	10.3.6.110	FTP	72	Request: PASV
153	3.208422	10.3.6.110	10.3.20.9	FTP	114	Response: 227 Entering passive mode (10,3,6,110,255,105)
157	3.244374	10.3.20.9	10.3.6.110	FTP	90	Request: RETR 00156574b16e.cfg
158	3.213747	10.3.6.110	10.3.20.9	FTP	75	Response: 213 164
159	3.214340	10.3.20.9	10.3.6.110	FTP	89	Request: RETR 00156574b16e.cfg
160	3.215550	10.3.6.110	10.3.20.9	FTP	102	Response: 125 using existing data connection

Example 3: Yealink T46S Skype for Business phone downloads configuration files from the HTTP server.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.3.20.9	10.3.6.110	HTTP	232	HTTP/1.1 302 Found
2	0.007935	10.3.6.110	10.3.20.9	HTTP	542	GET /servlet?p=settings-config&q=load HTTP/1.1
38	0.068955	10.3.20.9	10.3.6.110	HTTP	125	HTTP/1.1 200 OK
41	2.576460	10.3.6.110	10.3.20.9	HTTP	515	GET /servlet?p=settings-autop&q=load HTTP/1.1
77	2.643550	10.3.20.9	10.3.6.110	HTTP	982	HTTP/1.1 200 OK
87	10.797870	10.3.6.110	10.3.20.9	HTTP	86	POST /servlet?p=settings-autop&q=write&now=false HTTP/1.1 (application/x-www-form-urlencoded)
89	10.959182	10.3.20.9	10.3.6.110	HTTP	231	HTTP/1.1 302 Found
90	11.030754	10.3.6.110	10.3.20.9	HTTP	540	GET /servlet?p=settings-autop&q=load HTTP/1.1
126	11.098802	10.3.20.9	10.3.6.110	HTTP	991	HTTP/1.1 200 OK
134	13.523038	10.3.6.110	10.3.20.9	HTTP	84	POST /servlet?p=settings-autop&q=write&now=true HTTP/1.1 (application/x-www-form-urlencoded)
161	13.727710	10.3.20.9	10.3.6.110	HTTP	206	HTTP/1.1 200 OK
166	13.755695	10.3.20.9	10.3.6.110	HTTP	218	GET /y0000000000066.cfg HTTP/1.1
169	13.796582	10.3.6.110	10.3.20.9	HTTP	205	HTTP/1.1 200 OK (application/octet-stream)
178	13.809749	10.3.20.9	10.3.6.110	HTTP	208	GET /ime.txt HTTP/1.1
185	13.836439	10.3.6.110	10.3.20.9	HTTP	1032	HTTP/1.1 200 OK (text/plain)
194	13.846276	10.3.20.9	10.3.6.110	HTTP	216	GET /Russian_ime.txt HTTP/1.1
201	13.883670	10.3.6.110	10.3.20.9	HTTP	1272	HTTP/1.1 200 OK (text/plain)
210	13.894060	10.3.20.9	10.3.6.110	HTTP	223	GET /00156574b1ee-local.cfg HTTP/1.1
219	13.898442	10.3.6.110	10.3.20.9	HTTP	66	HTTP/1.1 404 Not Found (text/html)
224	18.779475	10.3.6.110	10.3.20.9	HTTP	493	GET /servlet?p=settings-autop&q=result&random=0.04913059249520302 HTTP/1.1
228	18.988420	10.3.20.9	10.3.6.110	HTTP	59	HTTP/1.1 200 OK [Malformed Packet]
231	19.996891	10.3.6.110	10.3.20.9	HTTP	524	GET /servlet?p=settings-autop&q=load HTTP/1.1
267	20.063444	10.3.20.9	10.3.6.110	HTTP	991	HTTP/1.1 200 OK
270	23.138206	10.3.6.110	10.3.20.9	HTTP	516	GET /servlet?p=settings-upgrade&q=load HTTP/1.1
300	23.195348	10.3.20.9	10.3.6.110	HTTP	853	HTTP/1.1 200 OK
302	23.278964	10.3.6.110	10.3.20.9	HTTP	522	GET /servlet?p=common-page&q=iframe-upload HTTP/1.1
305	23.298530	10.3.20.9	10.3.6.110	HTTP	1490	HTTP/1.1 200 OK
308	24.965106	10.3.6.110	10.3.20.9	HTTP	517	GET /servlet?p=settings-config&q=load HTTP/1.1
343	25.023340	10.3.20.9	10.3.6.110	HTTP	125	HTTP/1.1 200 OK
346	26.271142	10.3.6.110	10.3.20.9	HTTP	644	POST /servlet?p=settings-config&q=stopcapture HTTP/1.1

Troubleshooting

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

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

Why does the 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.

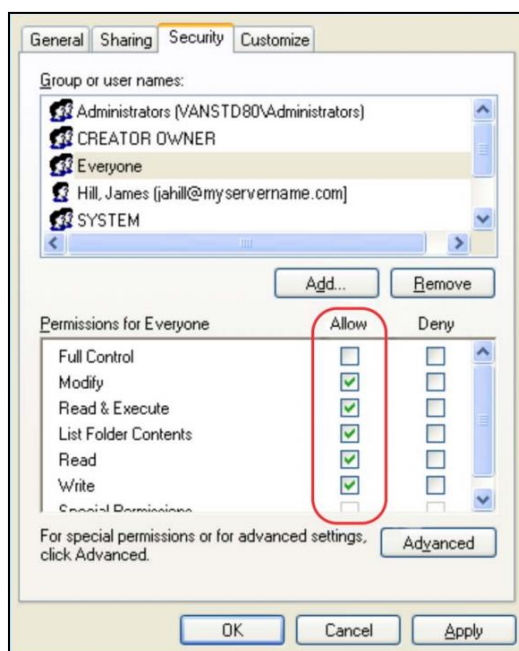
Preparing a Root Directory

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:

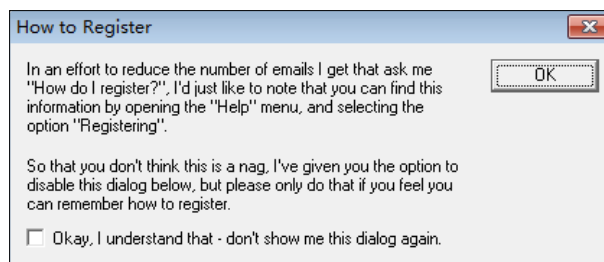


Configuring an FTP Server

To configure a wftpd server:

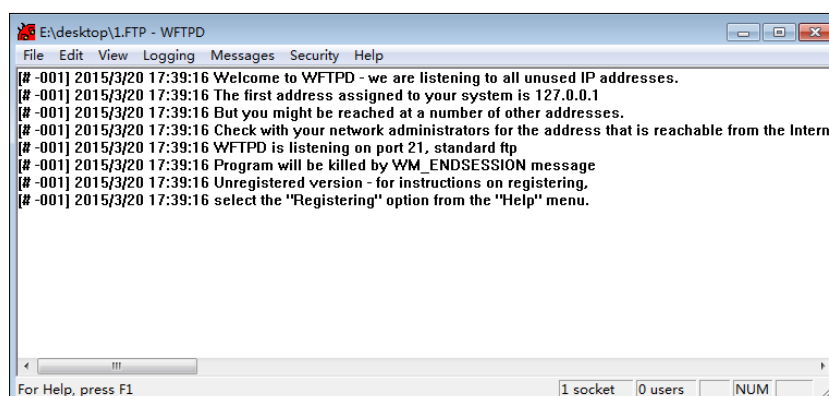
1. Download the compressed file of the wftpd application to your local directory and extract it.
2. Double click the WFTPD.EXE.

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

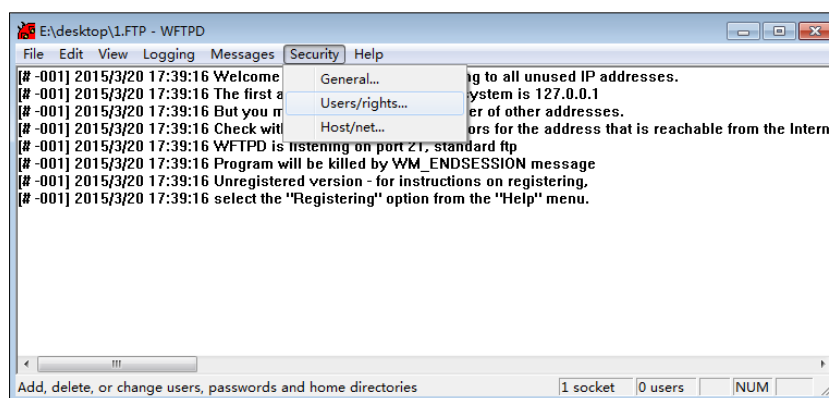


3. Check the check box and click **OK** in the pop-up dialogue box.

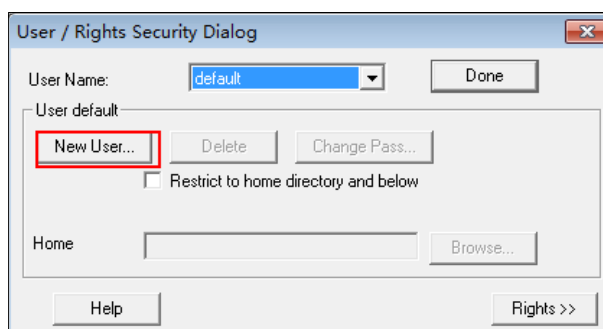
The log file of the wftpd application is shown as below:



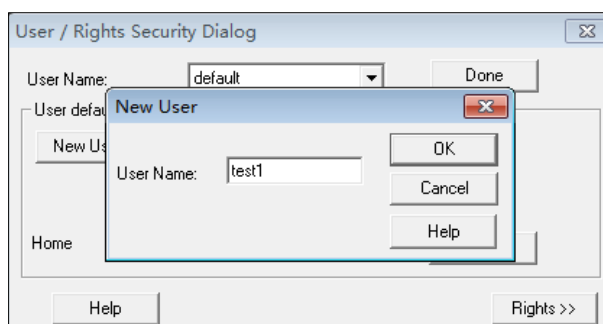
4. Click **Security->Users/rights**.



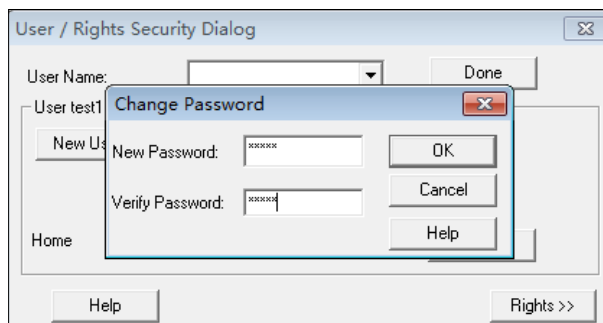
5. Click **New User**.



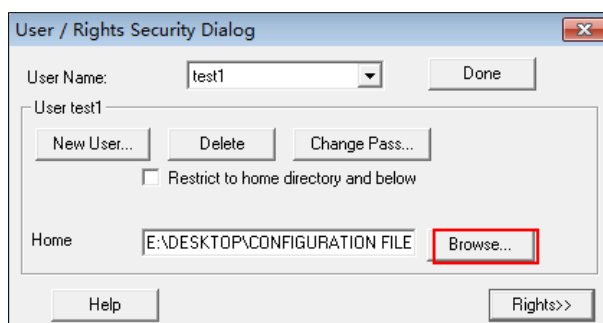
6. Enter a user name (e.g., test1) in the **User Name** field and then click **OK**.



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**.

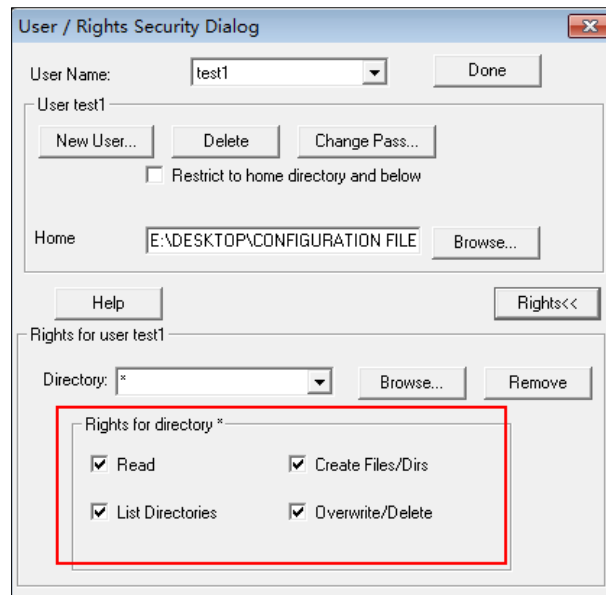


8. Click **Browse** to locate the FTP root directory from your local system.



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.

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

Configuring an HTTP Server

This section provides instructions on how to configure an HTTP server using HFS tool. You can download the HFS software online: <http://www.snapfiles.com/get/hfs.html>.

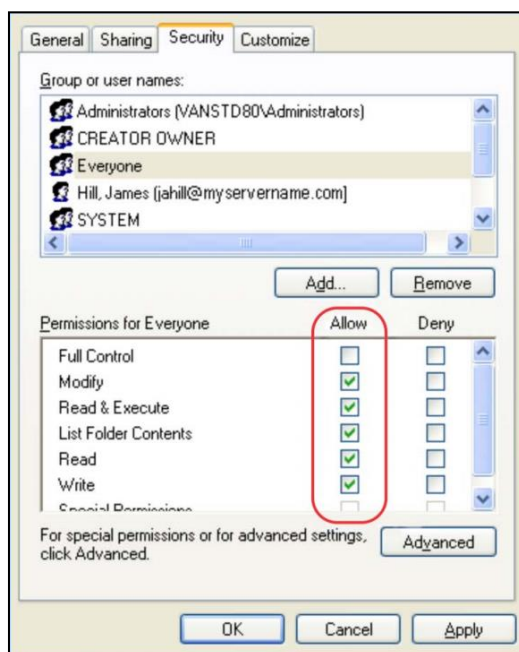
Preparing a Root Directory

To prepare a root directory:

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

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

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



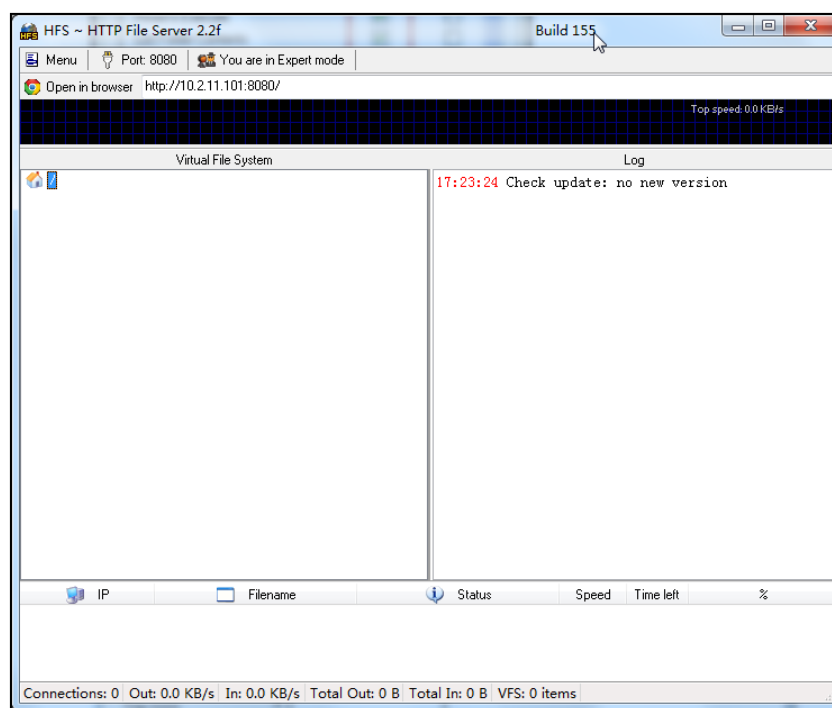
Configuring an HTTP Server

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

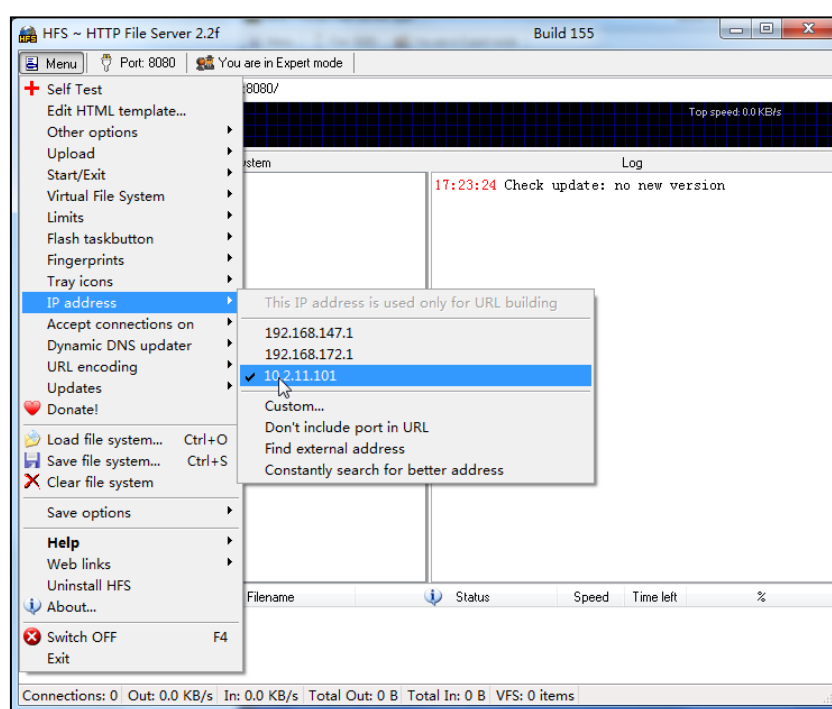
To configure an HTTP server:

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

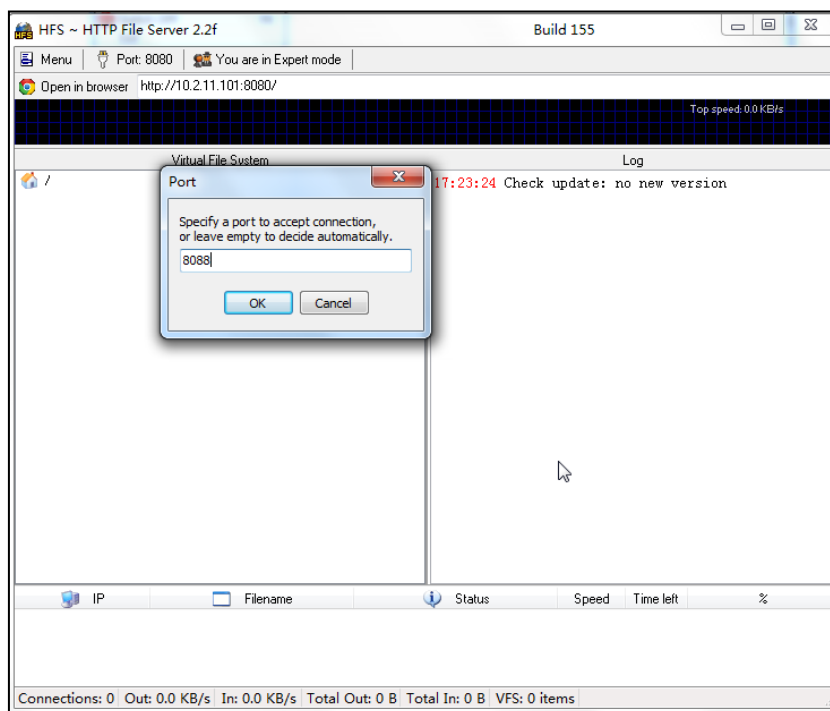
The main configuration page is shown as below:




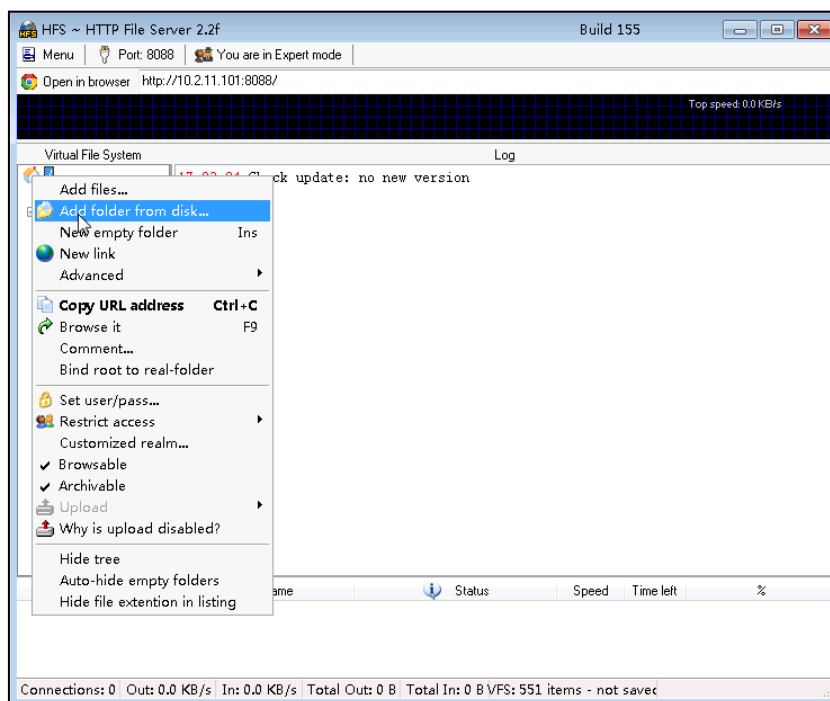
2. Click **Menu** in the main page and select the IP address of the PC from **IP address**.



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



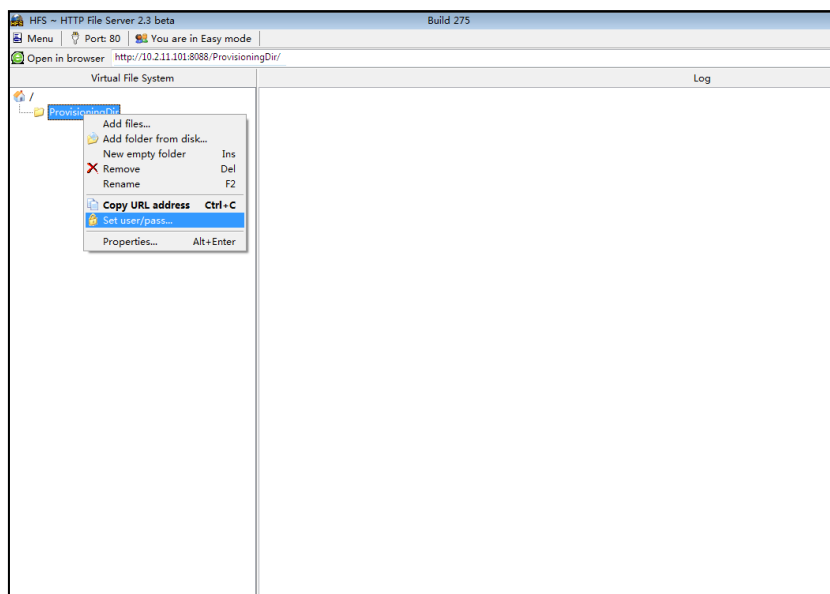
3. Right click the  icon on the left of the main page, select **Add folder from disk** to add the HTTP Server root directory.



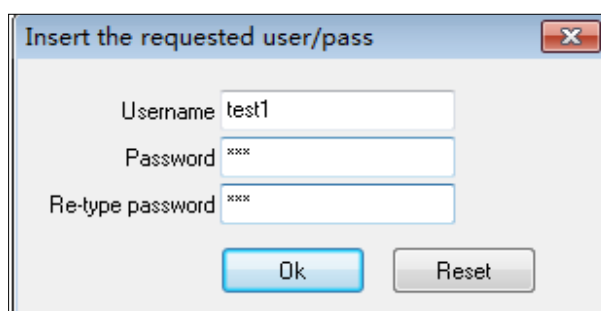
4. (Optional) Right-click on the directory to select **Set user/pass...** to configure a user name and password for the directory.

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

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

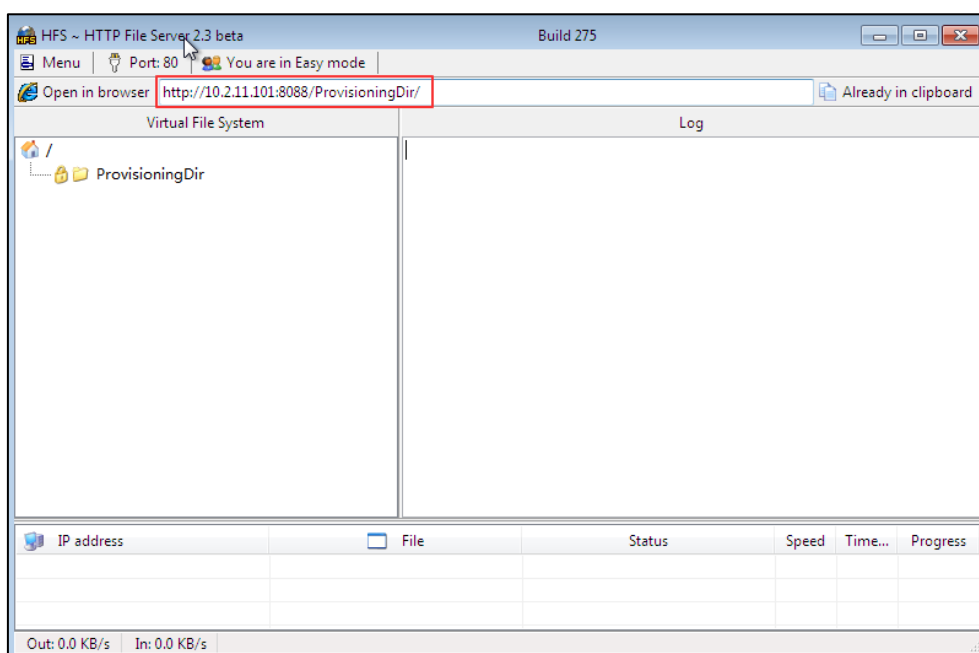


5. Enter a user name (e.g., test1) and password in the **User Name**, **New Password** and **Verify Password** fields respectively.



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/](http://10.2.11.101:8088/ProvisioningDir/)) by clicking “**Open in browser**”.

Yealink Skype for Business 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

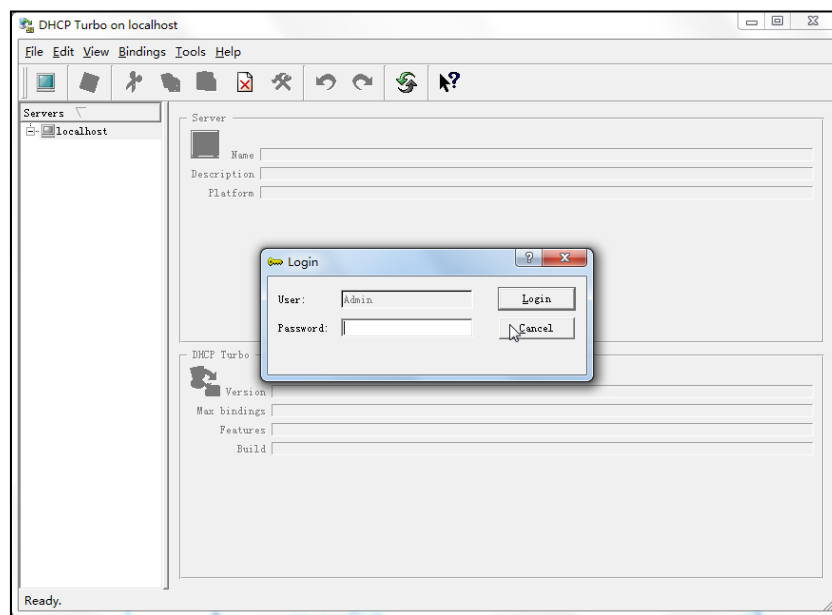
Before configuring the DHCP Turbo, make sure:

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

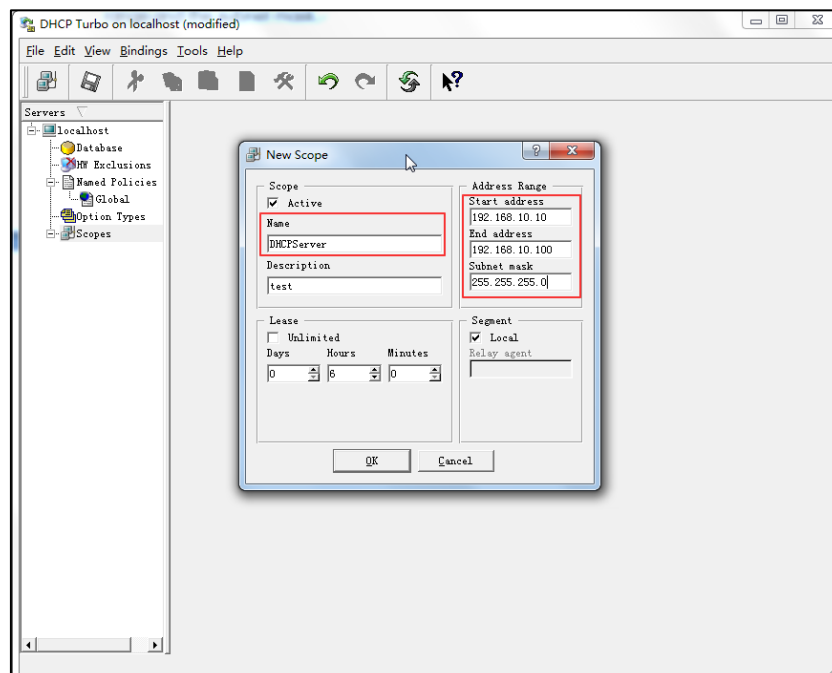
To configure the DHCP Turbo:

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

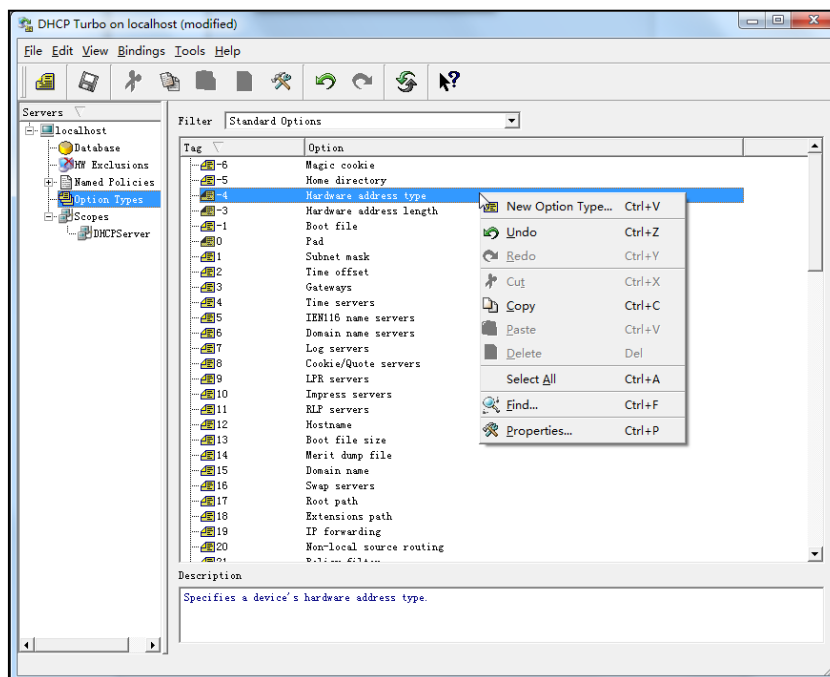
- Click the **Login** button (the login password is blank) to log in.




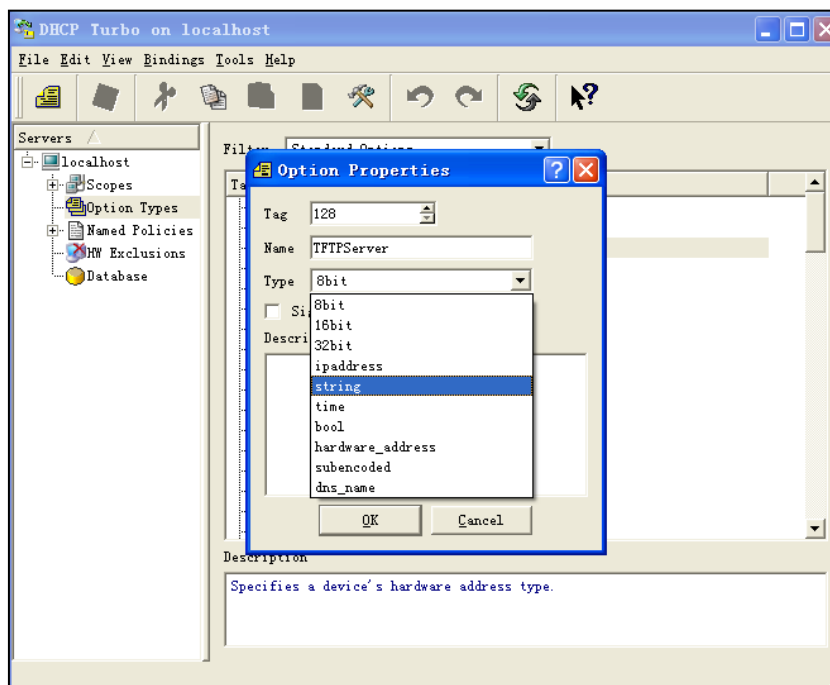
- Right click **Scopes** and select **New Scope**.
- Configure the DHCP server name, the DHCP IP range and the subnet mask.
- Click **OK** to accept the change.



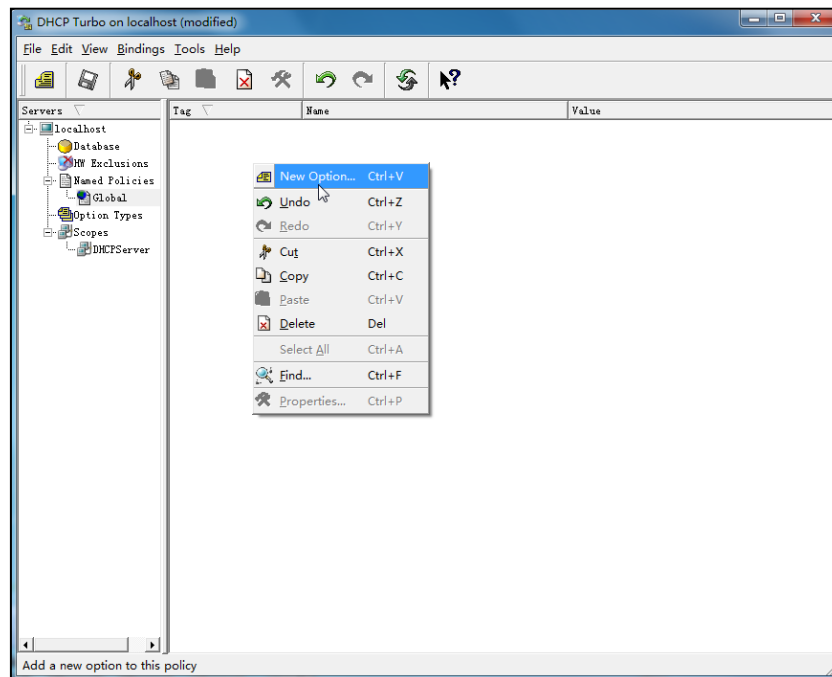
6. You can add a custom option via DHCP Turbo. Select **Option Types**, right click one of the options on the right of the main page, and then select **New Option Type**.



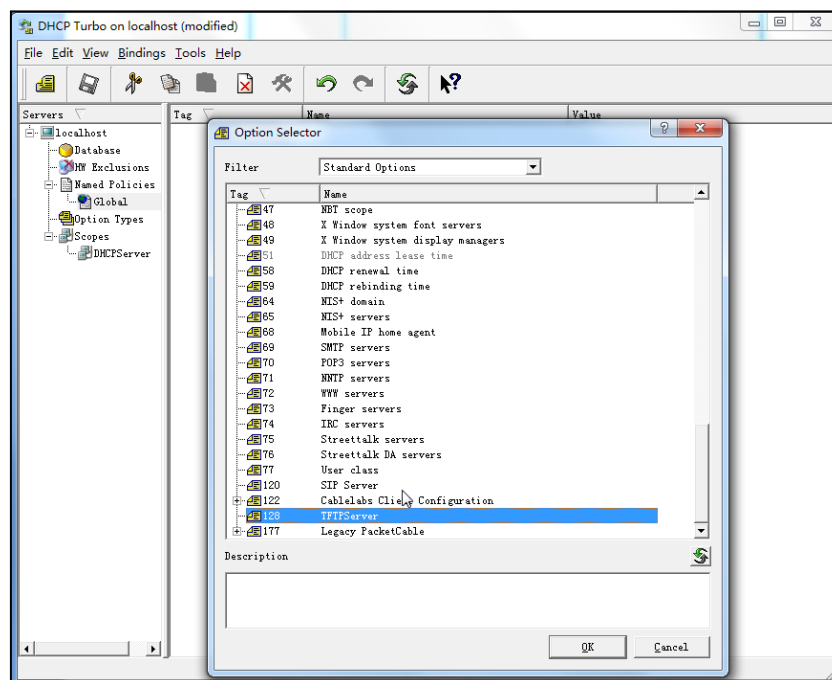
7. Set the custom DHCP option (custom DHCP option tag number ranges from 128 to 254) and select the option type (Yealink supports **string** and **ipaddress** option types only). Click the **OK** button to finish setting the option properties. Click  to save the change.



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

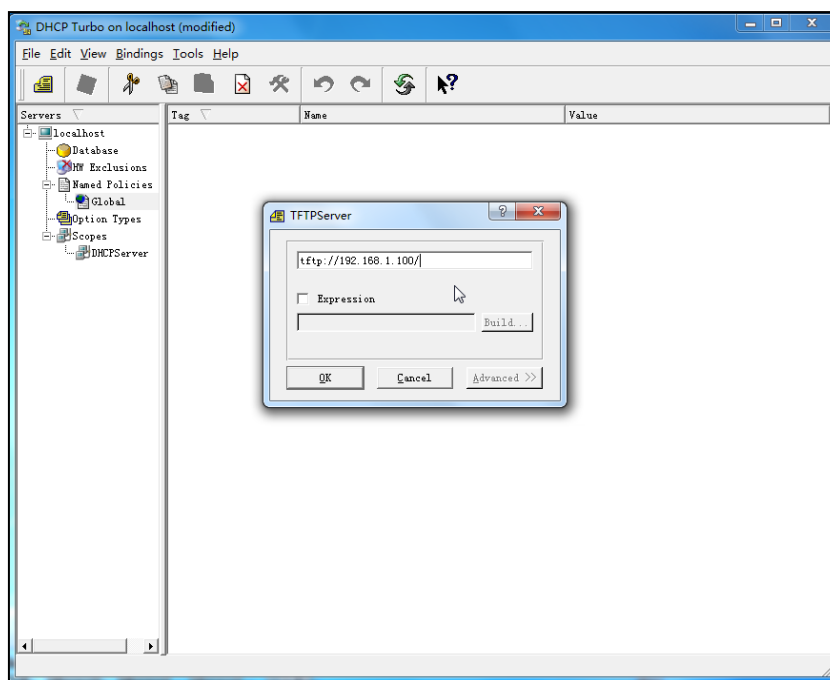



9. Scroll down and double click the custom option 128.



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

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

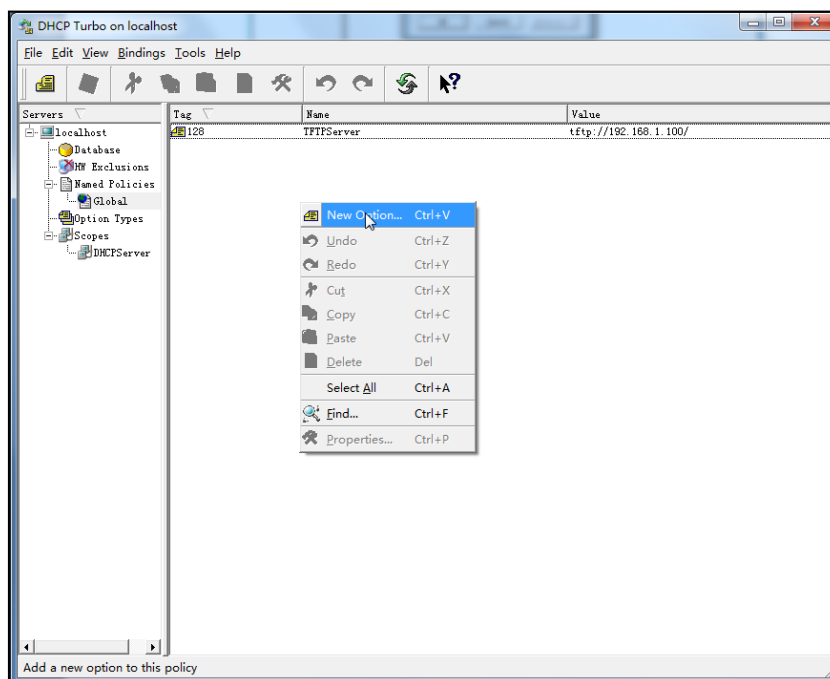


12. Click  to save the change.

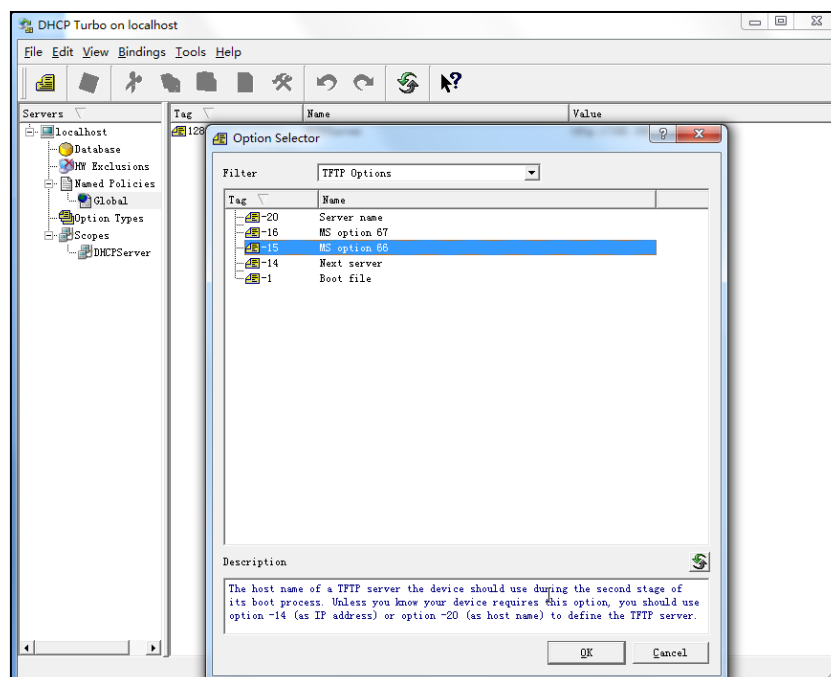
Add the Option 66 via DHCP Turbo

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

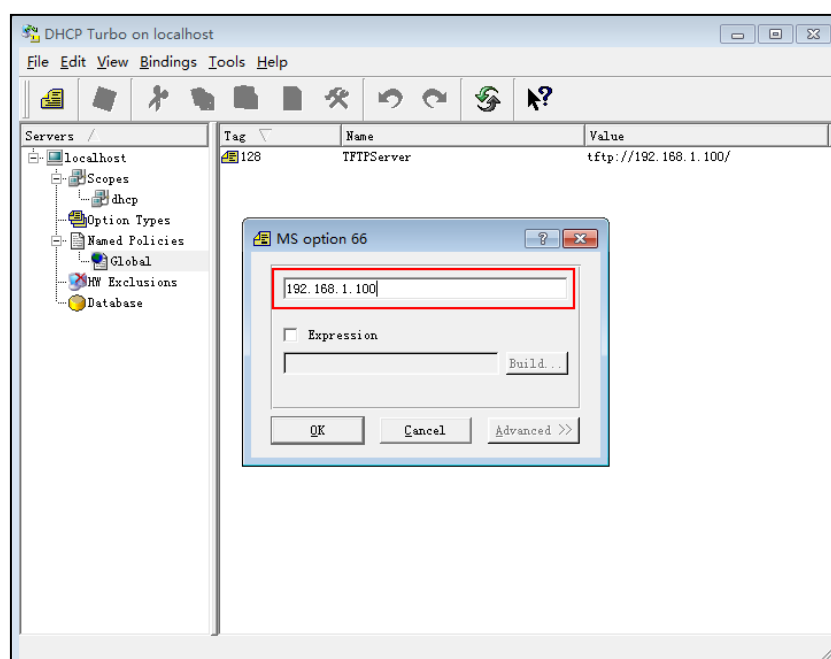
1. Click **Named Policies-->Global**, right click the blank area on the right of the main page and then select **New Option**.




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.

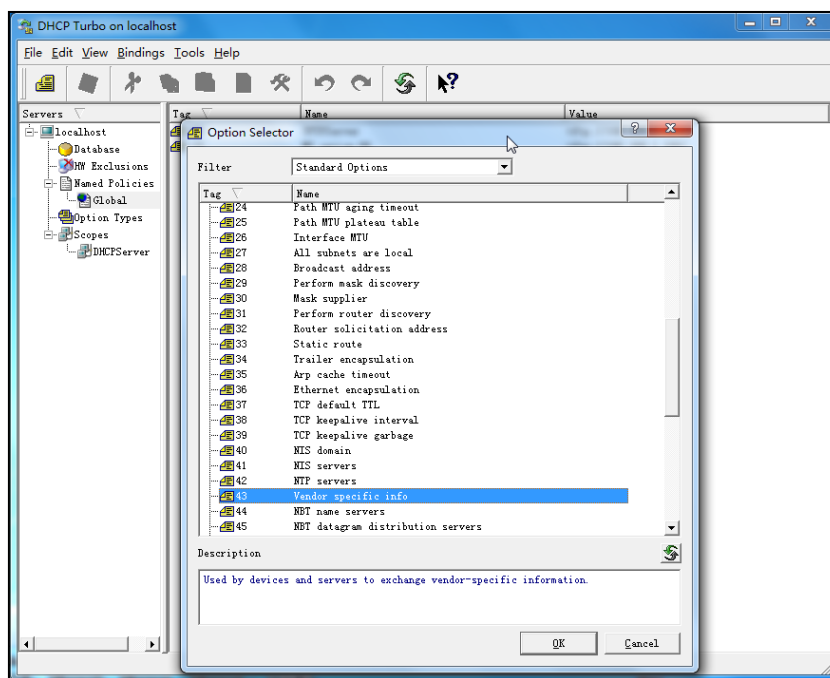


5. Click the **OK** button to finish setting a custom option.
6. Click  to save the change.

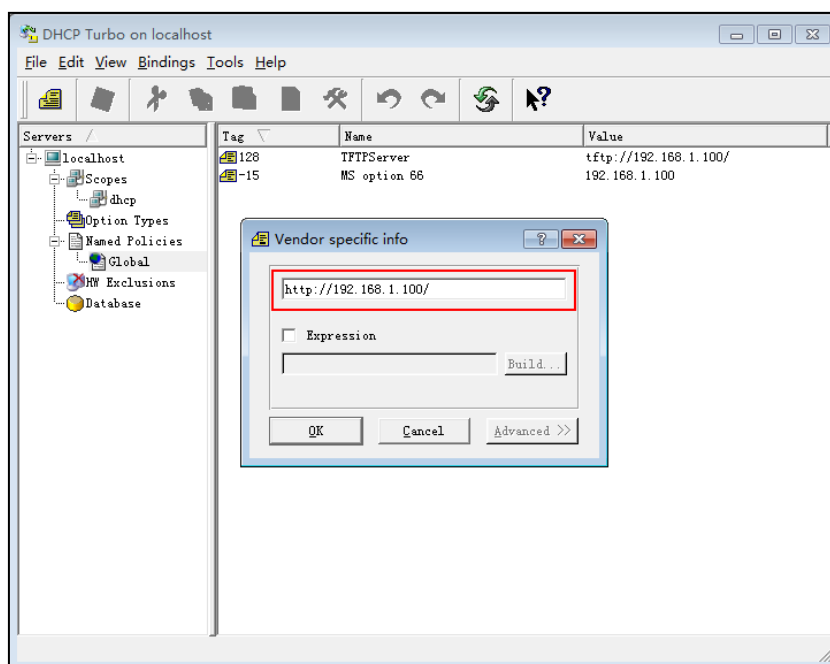
Add the Option 43 via DHCP Turbo


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.