



Auto Provision Description

Version: <1.1>

Release date: <2018-05-11>



Contents

Contents.....	1
1 Introduction.....	2
1.1 Overview.....	2
1.2 Operation Process.....	2
2 Detailed Classifications.....	3
2.1 Classification of Configuration Files.....	3
2.2 Download Modes.....	3
2.3 Priorities of Download Modes.....	3
2.4 Download Protocols.....	3
2.5 Supported File Types.....	3
2.6 Auto Provision Operation Sequence.....	3
3 Environment Requirements.....	4
4 Auto Provision Details.....	5
4.1 Detailed Introduction to Classification of Configuration Files and Rules for Writing Configuration Files.....	5
4.2 URL.....	8
4.3 Download Modes.....	9
4.4 Supported File Types.....	18
4.5 Save Auto Provision Information.....	20
4.6 Auto Provision Access Table list.....	20

1 Introduction

1.1 Overview

1. Module description

In auto provision, a terminal learns the server address where the configuration file is stored and other auto provision parameters, downloads the configuration file from the corresponding server, and parses and saves the configuration file locally for updates, such as firmware update.

2. Advantages

With auto provision, a large number of telephone sets can be remotely upgraded concurrently, saving time and labor.

1.2 Operation Process

Fanvil terminals can obtain auto provision parameters using four methods: SIP PnP, DHCP Option, Static Provisioning Server, and TR069. If all the four methods are configured, a terminal selects an upgrade mode based on the priorities of the four methods when being started.

Four transmission protocols are supported: FTP, TFTP, HTTP, and HTTPS.

Process:

1. Edit the configuration file, modify the content to be updated, save the configuration file under the corresponding server directory, and ensure that the server is started.
2. Log in to the webpage or LCD (not supported by some telephone sets) and start the method (SIP PnP, DHCP Option, Static Provisioning Server, or TR069) for obtaining auto provision parameters.
3. Restart the telephone set. When being started, the telephone set obtains the URL containing the server address where the configuration file is stored.
4. The telephone set parses the URL and downloads the configuration file from the corresponding server. Usually two configuration files need to be downloaded: general configuration file and device configuration file. If the two configuration files share the same file name, only one needs to be downloaded.
5. After the configuration file is successfully downloaded to the cache of the telephone set, check whether the content in the configuration file is the same as that in the existing configuration file on the telephone set. If the content is the same, cancel the upgrade. If the content is different, update the configuration file.
6. Check whether the new configuration involves new download items such as version, phone book, and certificate. If yes, start a task to download the corresponding items.
7. The process ends.

2 Detailed Classifications

2.1 Classification of Configuration Files

1. By function
 - General configuration file
 - Configuration file named by users
 - Configuration file named after MAC addresses
2. By format
 - XML format
 - CFG format
 - TXT format
3. By encryption status
 - Unencrypted configuration file
 - Encrypted configuration file

2.2 Download Modes

SIP PnP, DHCP Option, Static Provisioning Server, and TR069

2.3 Priorities of Download Modes

The download modes are prioritized based on the configuration of a telephone set. Currently, the priorities of download modes cannot be modified on Android telephone sets. Specifically, the download modes are sorted in descending order of priority as follows: MDNS, FDPS, DHCP, TR069, SIP, and Flash.

2.4 Download Protocols

TFTP, FTP, HTTP, and HTTPS

2.5 Supported File Types

Firmware, phone book, etc, Background, and mmiset (Android telephone sets do not support logo and mmiset)

2.6 Auto Provision Operation Sequence

Write the configuration file correctly -> Configure a transmission protocol server -> Access the download mode preset for the telephone set -> Restart the device -> Obtain the configuration file -> Obtain the URL based on the configuration file and download upgrade files

3 Environment Requirements

DHCP server, SIP PnP, 3cx,TR069 server, HTTPS server, HTTP server, TFTP server, or FTP server

The used download protocol must match the server.

4 Auto Provision Details

4.1 Detailed Introduction to Classification of Configuration Files and Rules for Writing Configuration Files

1. By series

1) General configuration file

A general configuration file takes effect for all terminals. The general configuration file is named differently on different terminal models. The rules for naming the general configuration file are described as follows:

X series low-end color-screen, H series, and access control series telephone sets:

Model	Name of General Configuration File
X1	f0X1hw1.100.cfg
X2	f0X2hw1.100.cfg
X3S	f0X3Shw1.100.cfg
X4	f0X4hw1.100.cfg
H2S	f0H2Shw1.100.cfg
H3	f0H3hw1.100.cfg
H5	f0H5hw1.100.cfg
i16V	f0i16Vhw1.100.cfg
i20S	f0i20SVhw1.100.cfg
i30	f0i30hw1.100.cfg
i23S	f0i23Shw1.100.cfg
i31S	f0i31Shw1.100.cfg
i12	f0i12hw1.100.cfg
i18S	f0i18Shw1.100.cfg
PA2	f0PA2hw1.100.cfg
i13W	f0i13Whw1.100.cfg
I32V	f0i32Vhw1.100.cfg
I33V	f0i33Vhw1.100.cfg

Model	Name of General Configuration File
IW30	f0iW30hw1.100.cfg
EIM-01	f0EIM-01hw1.100.cfg

a) X series high-end color-screen telephone sets:

Model	Name of General Configuration File
X5S	F0V0X5S00000.cfg
X6	F0V00X600000.cfg
X7	F0V00X700000.cfg
X7C	F0V0X7C00000.cfg
X210	F0VX21000000.cfg

b) Android telephone sets:

Model	Name of General Configuration File
F600	f0F060000000.cfg
C600	f0C060000000.cfg
C400	f0C040000000.cfg

The general configuration file is helpful in automatic configuration deployment of a large number of terminals. For example, only a general configuration file F0V00X600000.cfg carrying firmware parameters needs to be placed on the automatic configuration server to automatically deploy firmware for 1000 X6 terminals.

2) Configuration file named by users

Users can define the name of a configuration file. For example, if a user names a device configuration file as name.cfg, the telephone set initiates a request to the server to download the general configuration file name.cfg. The user can enter the corresponding configuration file name and download the upgrade configuration from the server.

3) Configuration file named after MAC addresses

A configuration file named after a terminal MAC address is valid only for the terminal with the MAC address contained in the configuration file name. For a configuration file named after a MAC address, the MAC address contained in the file name is one for which the connectors are removed. For example, the MAC address of an X6 terminal is 00:15:65:11:3a:f8 and the configuration file name is 001565113af8.cfg. A user can upgrade the specified telephone set with this file.

2. By format

1) Supported file formats include cfg, txt, and xml.

2) Internal file format

➤ The file header is 64 characters long and ends with a carriage return character (\r\n).

For example, <<VOIP CONFIG FILE>>Version:2.0002

Pay attention to the part "Version: 2.0002". If a telephone set is successfully upgraded using the auto provision mode, the version number (for example 2.0002) is displayed in the version number position on the webpage. If no version is carried, the digest of the configuration file is displayed.

➤ End of file

For example, <<END OF FILE>>

To update an option, the module header of this option must be carried.

For example, to modify "Host Name : ", <GLOBAL CONFIG MODULE> must be carried.

<<VOIP CONFIG FILE>>Version:2.0002

<GLOBAL CONFIG MODULE>

Host Name :VOIP (not less than 20 characters)

<<END OF FILE>>

3. By encryption status

1) Unencrypted configuration file

The content of an unencrypted configuration file is displayed in plaintext, as shown in Figure 1.

<<VOIP CONFIG FILE>>Version:2.0002

<GLOBAL CONFIG MODULE>

Time Zone :32

<AUTOUPDATE CONFIG MODULE>

Auto Pbook Url :tftp://123:123@172.16.6.70/500.csv

Auto Image Url :http://123:123@172.16.6.70:8000/x4.z

Auto Etc Url :tftp://172.16.6.70/sips.pem

<<END OF FILE>>

Figure 1

2) Encrypted configuration file

➤ The content of an encrypted configuration file is not displayed in plaintext, as shown in Figure 2.

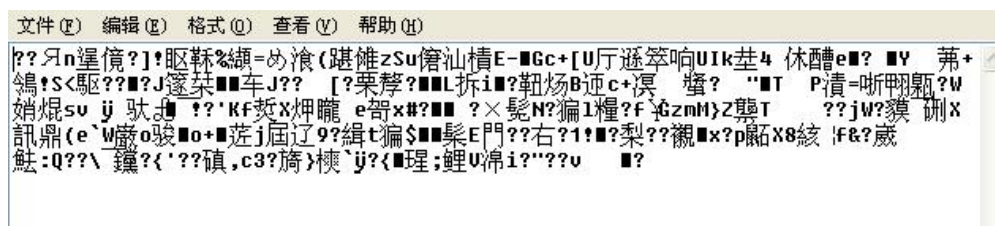


Figure 2

If a downloaded configuration file is encrypted using AES, an AES key is required to decrypt the configuration file. The key must contain 64 hexadecimal characters (0 to F). All configuration files can be encrypted. Log in to the webpage and choose Maintenance > Auto Provision. Enter the key in config Encryption Key if an encrypted general configuration file is to be downloaded and in Common Config Encryption Key if other encrypted configuration files are to be downloaded, as shown in Figure 3. If a configuration file to be downloaded is not encrypted but you enter a key in the corresponding position, the telephone set considers the configuration file as an encrypted one.

The screenshot shows the 'Auto Provision Settings' page. It contains the following fields and values:

Current Config Version	2.0002
Common Config Version	2.0002
CPE Serial Number	00100400XH020010000000010e597052
User	<input type="text"/>
Password	<input type="text"/>
Config Encryption Key	<input type="text"/>
Common Config Encryption Key	<input type="text"/>

Below the encryption key fields is a checkbox labeled 'Save Auto Provision Information' which is currently unchecked. At the bottom of the page, there are links for 'DHCP Option Settings >>', 'Plug and Play (PnP) Settings >>', 'Phone Flash Settings >>', and 'TR069 Settings >>'.

Figure 3

4.2 URL

1. URL format

A URL indicates the information obtained by DHCP Option and SIP PnP through the server.

The URL format is as follows:

Server protocol://user:password@Server IP:port/path/Configuration name.

For example, `http://user:password@172.16.1.3:8080/X4/$mac.cfg`

2. URL parsing

The following describes the functions and settings of different parts of a URL.

- 1) Server Protocol: transmission protocol used by the server. FTP, TFTP, HTTP, and HTTPS are supported. This part is mandatory.
- 2) User and Password: user name and password required for requesting information from the server. The two items are not mandatory when no user name and password are required for logging in to the server or the user name and password are entered on the webpage (Web > Maintenance > Auto Provision) of the telephone set. If the user name and password are required but you forget to enter them, or you enter the user name and

password incorrectly on the webpage, the telephone set requires you to enter the user name and password again on the LCD unless you abandon the upgrade.

Format of a URL without a user name and password: Server protocol:// Server IP:port/path/Configuration name

Auto Provision Settings

Current Config Version	2.0002
Common Config Version	2.0002
CPE Serial Number	00100400XH020010000000010e597052
User	<input type="text"/>
Password	<input type="text"/>
Config Encryption Key	<input type="text"/>
Common Config Encryption Key	<input type="text"/>
Save Auto Provision Information	<input type="checkbox"/>

[DHCP Option Settings >>](#)

[Plug and Play \(PnP\) Settings >>](#)

[Phone Flash Settings >>](#)

[TR069 Settings >>](#)

Figure 4

- 3) Server Ip: IP address of the server, for example, 172.16.1.3 This part is mandatory.
- 4) Port: port number of the server, for example, 8080. This item is not mandatory. It is required only when the server defines a special port number.
Format of a URL without a port number: Server protocol:// Server Ip/path/Configuration name
- 5) Path: save path of the configuration file. This item is mandatory if a level-2 or level-3 directory exists.
- 6) Configuration name: name of the configuration file. Here it refers to the name of the device configuration file. The name of the general configuration file is unchangeable. This item can be set as follows:
Left blank: If this item is left blank, the device configuration file (mac.cfg) named after the MAC address is downloaded by default.
 - \$mac.cfg: The device configuration file (mac.cfg) named after the MAC address is downloaded.
 - \$input.cfg: The user is required to manually enter the device configuration file name on the LCD. (\$input.xml/\$input.txt)
 - Specify the device configuration file name, for example, name1.cfg or name2.cfg.

4.3 Download Modes

1. DHCP Option
 - 1) To use the DHCP Option mode, the network mode of the telephone set must be DHCP.
 - 2) DHCP Option has four options: DHCP Option 66, DHCP Option 43, Custom DHCP Option, and DHCP Option Disable.

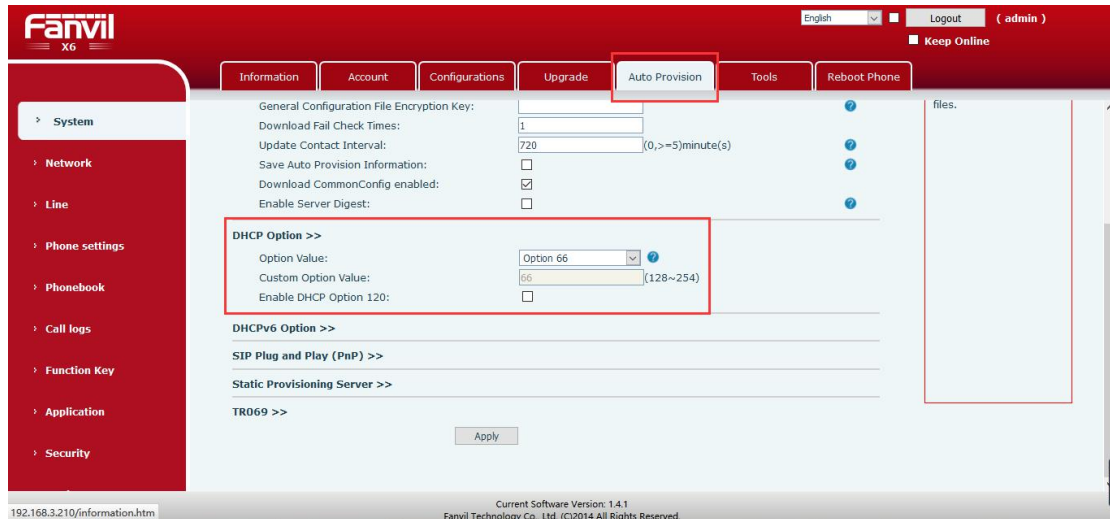


Figure 5

- 3) The value range of Custom DHCP option is 128–254. DHCP Option Disable indicates disabling DHCP Option.

After setup, the telephone set requests the DHCP server for option information when it is restarted or during DHCP renewal. If the server returns the requested option information, the telephone set obtains the URL based on the corresponding option information (filter BOOTP and view the ACK packet) in the captured packet and parses the URL. When auto provision parameters are obtained through DHCP, a user can choose any download mode. For example, if DHCP Option 43 is chosen when auto provision parameters are obtained through DHCP, the DHCP Discover and DHCP Request messages sent by the terminal to the server contain the following field values:

Option: (t=55,l=7) Parameter Request List

Option: (55) Parameter Request List

Length: 7

Value: 011c0302042b06

1 = Subnet Mask

28 = Broadcast Address

43 = Vendor-Specific Information

The DHCP Offer and DHCP ACK messages sent by the server to the terminal contain the following field values:

Option: (t=43,l=29) Vendor-Specific Information

Option: (43) Vendor-Specific Information

Length: 29

Value: 746674703a2f2f3139322e3136382e312e3131382f246d61...

Option: In (t=43,l=29) Vendor-Specific Information, the value is the hexadecimal format of the URL of the configuration file to be downloaded. That is, the value is [http://172.16.6.45/\\$mac.cfg](http://172.16.6.45/$mac.cfg). Fanvil terminals support replacing \$mac. The URL of Value can be [http://ip/\\$mac.cfg](http://ip/$mac.cfg) or [http://ip/mac.cfg?mac=\\$mac.cfg](http://ip/mac.cfg?mac=$mac.cfg).

The auto provision parameters of DHCP Option 66 and Custom DHCP are the same as those of DHCP Option 43.

Note:

Fanvil terminals also support the URL format of `http://ip/$input.cfg`. If in Option: (t=43,l=29) Vendor-Specific Information, Value is `http://172.16.6.45/$input.cfg`, the telephone set displays a dialog box for entering the ID of the configuration file, which is assigned by the administrator. After the user enters the configuration file ID, the terminal automatically downloads from the server the configuration file corresponding to the ID. Fanvil terminals support replacing \$input. The URL of Value can be `http://ip/$input.cfg` or `http://ip/input.cfg?input=$input.cfg`.

4) Operation method

Take DHCP Option 66 as an example.

- The network mode is set to DHCP for the telephone set.
- Log in to the webpage of the telephone set, access management setup, and select DHCP Option 66.
- Disconnect the external network, enable the DHCP server, and set Option 66 of the DHCP server to the URL where the configuration file is to be downloaded.
- Store the configuration file to be downloaded under the corresponding directory of the server.
- Restart the telephone set and capture packets.
- For example, if the configured URL indicates downloading a custom XML configuration file through the TFTP server, the configuration file setting is shown in the following figure:

```
<VOIP CONFIG FILE>
<Digests>2.0002</Digests>
<GLOBAL CONFIG MODULE>
<Time_Zone>32</Time_Zone>
</GLOBAL CONFIG MODULE>
<AUTOUPDATE CONFIG MODULE>
<Auto Image Url> tftp://172.16.6.45/x4.z</Auto Image Url>
</AUTOUPDATE CONFIG MODULE>
</VOIP_CONFIG_FILE>
```

Figure 6

If only the time zone and image are to be downloaded, BOOTP and TFTP packets can be captured during the upgrade process. The information is also displayed on the corresponding server, as shown in Figure 6.

No.	Time	Source	Destination	Protocol	Length	Info
56	2014-03-12 11:00:02.528780	0.0.0.0	192.168.2.43	DHCP	309	DHCP Discover - Transaction ID 0xc794b77c
58	2014-03-12 11:00:02.784965	192.168.2.43	0.0.0.0	DHCP	351	DHCP offer - Transaction ID 0xc794b77c
64	2014-03-12 11:00:07.779459	0.0.0.0	192.168.2.43	DHCP	321	DHCP Request - Transaction ID 0xc794b77c
65	2014-03-12 11:00:08.014926	192.168.2.43	0.0.0.0	DHCP	351	DHCP ACK - Transaction ID 0xc794b77c
11518	2014-03-12 11:02:23.287981	0.0.0.0	192.168.2.43	DHCP	309	DHCP Discover - Transaction ID 0xc794b77c
11519	2014-03-12 11:02:23.540799	192.168.2.43	0.0.0.0	DHCP	351	DHCP offer - Transaction ID 0xc794b77c
11521	2014-03-12 11:02:28.538457	0.0.0.0	192.168.2.43	DHCP	321	DHCP Request - Transaction ID 0xc794b77c
11523	2014-03-12 11:02:28.832719	192.168.2.43	0.0.0.0	DHCP	351	DHCP ACK - Transaction ID 0xc794b77c

```

Message type: boot Reply (2)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0xc794b77c
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 192.168.16.1 (192.168.16.1)
Next server IP address: 192.168.2.43 (192.168.2.43)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Securew_a9:b4:86 (00:03:07:a9:b4:86)
Client hardware address padding: 00000000000000000000
Server host name: l23-
Boot file name not given
Magic cookie: DHCP
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=1,l=4) Subnet Mask = 255.255.0.0
Option: (t=3,l=4) Router = 192.168.1.1
Option: (t=46,l=4) NetBIOS over TCP/IP Node Type = H-node
Option: (t=6,l=4) Domain Name Server = 192.168.1.1
Option: (t=51,l=4) IP Address Lease Time = 1 day
Option: (t=94,l=4) DHCP Server Identifier = 192.168.2.43
Option: (t=66,l=30) TFTP Server Name = "tftp://192.168.2.45/$input.xml"
Option: (66) TFTP Server Name
Length: 30
Value: 746674703a2f2f3139322e3136382e322e34352f24696e70...
End option
TFTP = Maxilla Firewall
  
```

Figure 7

No.	Time	Source	Destination	Protocol	Length	Info
98	2014-03-12 11:00:28.669306	192.168.16.1	192.168.2.45	TFTP	96	Read Request, File: f0C00620000.cfg, Transfer type: octet, tsize
99	2014-03-12 11:00:28.670583	192.168.16.1	192.168.2.45	TFTP	87	Read Request, File: ll.xml, Transfer type: octet, tsize\000=0,000
100	2014-03-12 11:00:28.750543	192.168.2.45	192.168.16.1	TFTP	529	Data Packet, Block: 1 (last)
101	2014-03-12 11:00:28.752106	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 1
102	2014-03-12 11:00:28.752555	192.168.2.45	192.168.16.1	TFTP	348	Data Packet, Block: 1 (last)
103	2014-03-12 11:00:28.754296	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 1
112	2014-03-12 11:00:38.765034	192.168.16.1	192.168.2.45	TFTP	85	Read Request, File: 62.2, Transfer type: octet, tsize\000=0,000,
113	2014-03-12 11:00:38.767251	192.168.2.45	192.168.16.1	TFTP	558	Data Packet, Block: 1
114	2014-03-12 11:00:38.768835	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 1
115	2014-03-12 11:00:38.768935	192.168.16.1	192.168.2.45	TFTP	558	Data Packet, Block: 2
116	2014-03-12 11:00:38.809249	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 2
117	2014-03-12 11:00:38.809418	192.168.2.45	192.168.16.1	TFTP	558	Data Packet, Block: 3
118	2014-03-12 11:00:38.810939	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 3
119	2014-03-12 11:00:38.811025	192.168.2.45	192.168.16.1	TFTP	558	Data Packet, Block: 4
120	2014-03-12 11:00:38.813277	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 4
121	2014-03-12 11:00:38.813348	192.168.2.45	192.168.16.1	TFTP	558	Data Packet, Block: 5
122	2014-03-12 11:00:38.814872	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 5
123	2014-03-12 11:00:38.814941	192.168.2.45	192.168.16.1	TFTP	558	Data Packet, Block: 6
124	2014-03-12 11:00:38.816503	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 6
125	2014-03-12 11:00:38.816598	192.168.2.45	192.168.16.1	TFTP	558	Data Packet, Block: 7
126	2014-03-12 11:00:38.818239	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 7
127	2014-03-12 11:00:38.818334	192.168.2.45	192.168.16.1	TFTP	558	Data Packet, Block: 8
128	2014-03-12 11:00:38.819893	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 8
129	2014-03-12 11:00:38.820028	192.168.2.45	192.168.16.1	TFTP	558	Data Packet, Block: 9
130	2014-03-12 11:00:38.821577	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 9
131	2014-03-12 11:00:38.821665	192.168.2.45	192.168.16.1	TFTP	558	Data Packet, Block: 10
132	2014-03-12 11:00:38.823697	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 10
133	2014-03-12 11:00:38.823756	192.168.2.45	192.168.16.1	TFTP	558	Data Packet, Block: 11
134	2014-03-12 11:00:38.825298	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 11
135	2014-03-12 11:00:38.825431	192.168.2.45	192.168.16.1	TFTP	558	Data Packet, Block: 12
136	2014-03-12 11:00:38.826948	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 12
137	2014-03-12 11:00:38.827064	192.168.2.45	192.168.16.1	TFTP	558	Data Packet, Block: 13
138	2014-03-12 11:00:38.828682	192.168.16.1	192.168.2.45	TFTP	60	Acknowledgement, Block: 13
139	2014-03-12 11:00:38.828750	192.168.2.45	192.168.16.1	TFTP	558	Data Packet, Block: 14

```

Frame 99: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
Ethernet II, Src: Securew_a9:b4:86 (00:03:07:a9:b4:86), Dst: Giga-Byt_48:c0:ef (50:e5:49:48:c0:ef)
Internet Protocol Version 4, Src: 192.168.16.1 (192.168.16.1), Dst: 192.168.2.45 (192.168.2.45)
User Datagram Protocol, Src Port: 1028 (1028), Dst Port: tftp (69)
Trivial File Transfer Protocol
  
```

Figure 8

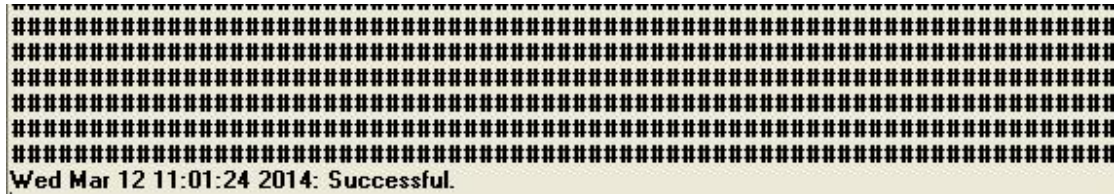


Figure 9

The URL download modes of DHCP Option 43 and Custom DPCH Option are the same as that described above.

HTTPS to upgrade

Since our locally built DHCP server does not support HTTPS upgrade, 1.3 server is needed, which is separately introduced here. The operation method is as follows (take option 66 as an example) :

cd /etc Enter the etc directory, cd /etc, via the SecureCRT.EXE telnet link to the server

Open the file, vi dhcpd.conf

Press I after enter to edit and modify the corresponding item

After the modification, press Esc to exit the modification

Shift+ : to enter the save command (q! Do not save, wq save)

Restart DHCP server for the changes to take effect, service dhcpd restart

The configuration files to be downloaded are placed in the directory specified by the server

Choose option 66

restart

caught

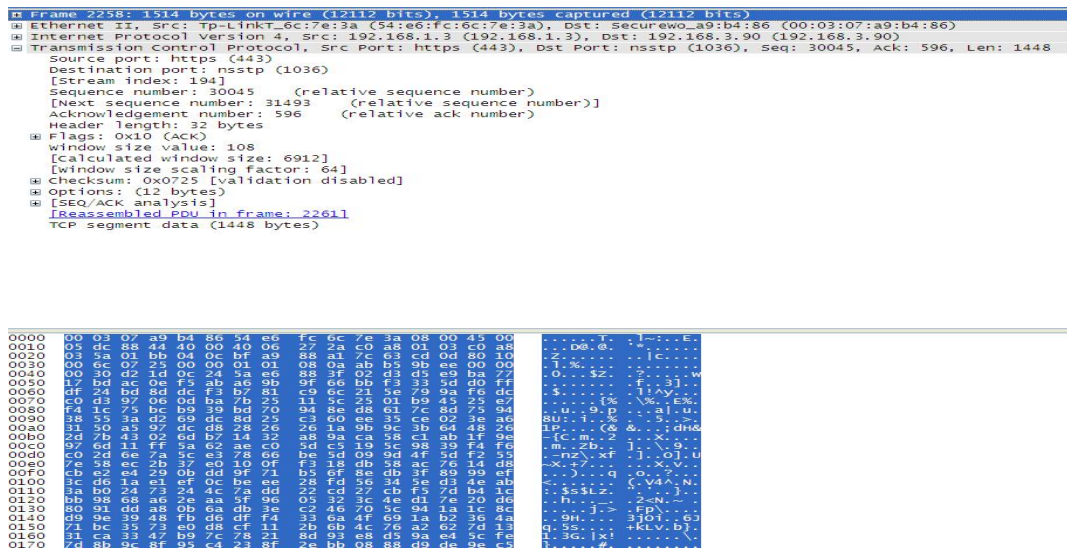


Figure 10

2. PnP

- 1) PnP provides a SIP-based configuration upgrade/deployment method. Enter the server IP address and port and select Enable SIP PnP.

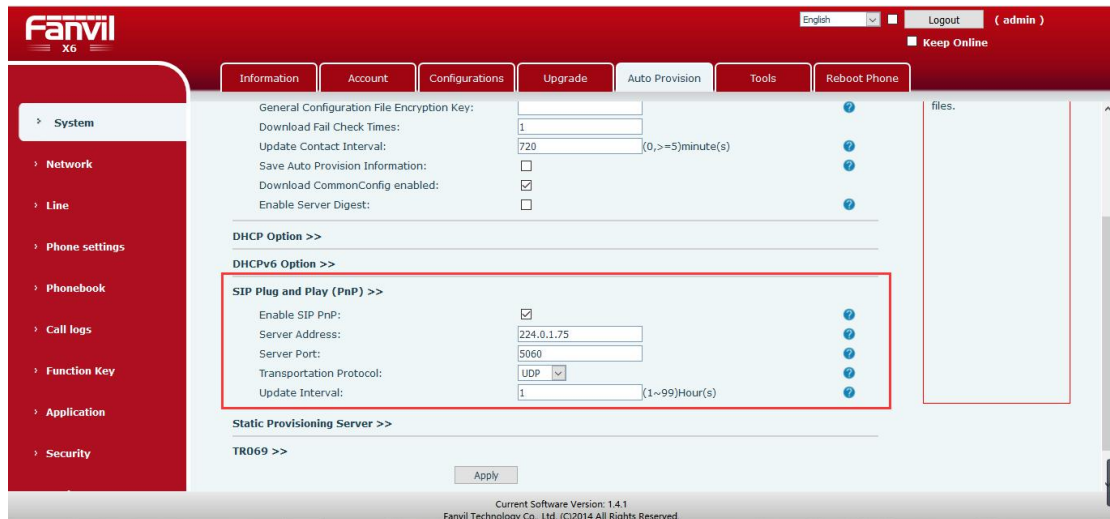


Figure 11

If PnP is enabled for a terminal, the terminal sends a SIP SUBSCRIBE message periodically in multicast mode. A SIP server supporting this message responds to the message and returns a SIP NOTIFY message carrying the path of the auto configuration/deployment server. The terminal can obtain the configuration file to be downloaded from this path. This auto configuration/deployment method applies to scenarios without a default auto configuration/deployment server or scenarios where a terminal uses a static IP address and cannot automatically obtain related parameters through DHCP Option. In version X4 or later versions, if a terminal fails to obtain the address parameter from the PnP server, it continues to obtain the parameter through other processes, as shown in Figure 11.

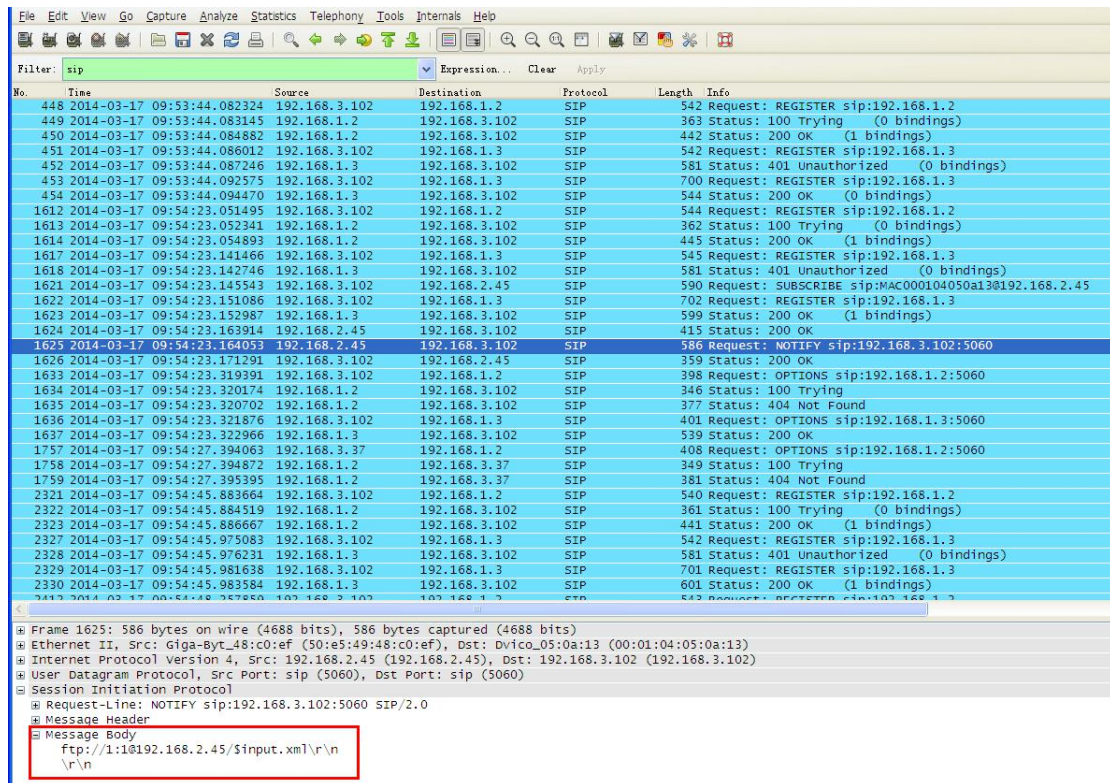


Figure 12

```

<!CDATA[
NOTIFY sip:[remote_ip]:5060 SIP/2.0
Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch]
From: [\$2]
To: [\$1]
[last_Call-ID:]
CSeq: 1 NOTIFY
Max-Forwards: 70
Content-Type: application/url
Subscription-State: terminated;reason=timeout
Event: ua-profile;profile-type="device";vendor="lishuai";model="VOIP PHONE ";ve1
Content-Length: [len]

tftp://172.16.6.45/\$input.txt edit URL become you want in here

]]>
</send>

<recv response="200" crlf="true">
</recv>

</scenario>

```

Figure 13

How to do it (for example, 3cx)

Log in phone web, turn on PNP, fill in PNP server address, PNP port, PNP protocol (udp, TCP), PNP cycle (generally default), restart phone

Log in 3cx, find the corresponding phone, send the configuration, and the server send notify to the phone, as shown in the figure

No.	Time	Source	Destination	Protocol	Length	Info
14	2016/200 10:02:54.3	172.16.7.87	172.16.2.243	SIP	622	Request: NOTIFY sip:172.16.2.243:5060
15	2016/200 10:02:54.8	172.16.7.87	172.16.2.243	SIP	622	Request: NOTIFY sip:172.16.2.243:5060
16	2016/200 10:02:54.9	172.16.2.243	172.16.7.87	SIP	305	Status: 200 OK
17	2016/200 10:02:55.6	172.16.2.243	172.16.7.87	SIP	305	Status: 200 OK


```

> Frame 15: 622 bytes on wire (4976 bits), 622 bytes captured (4976 bits) on interface 0
> Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Barracud_04:00:2b (00:03:00:04:00:2b)
> Internet Protocol Version 4, Src: 172.16.7.87, Dst: 172.16.2.243
> User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
v Session Initiation Protocol (NOTIFY)
  > Request-Line: NOTIFY sip:172.16.2.243:5060 SIP/2.0
  > Message Header
  v Message Body
    http://172.16.7.87:5000/provisioning/zheisBy8jij2/

```

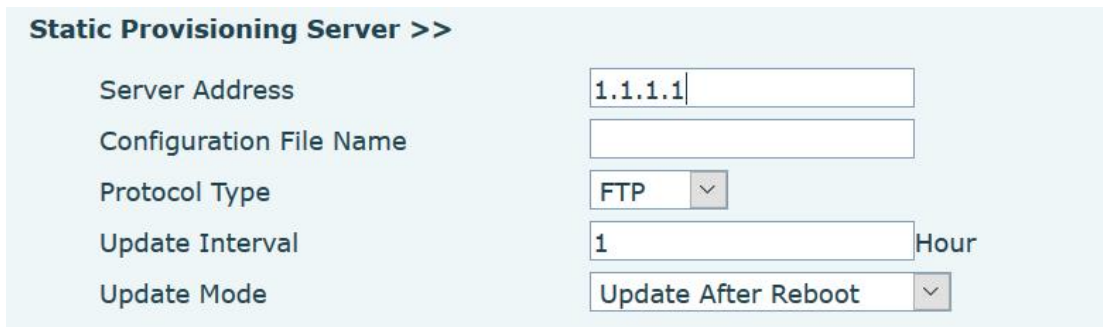
Figure 14

3. Static Provisioning Server

- 1) This process involves detecting and downloading server parameters.

The process depends on the setting of the configuration detection mode. If configuration detection is disabled, the terminal directly downloads the server parameters in the saved configurations without detection. This process supports HTTP, HTTPS, FTP, and TFTP. The user name and password are used for authentication by the server as required. The configurations can be downloaded after authentication. If a terminal fails to download a configuration file through the static provisioning server, the process of obtaining auto provision parameters automatically ends and the terminal no longer carries out the auto

configuration/upgrade deployment process.

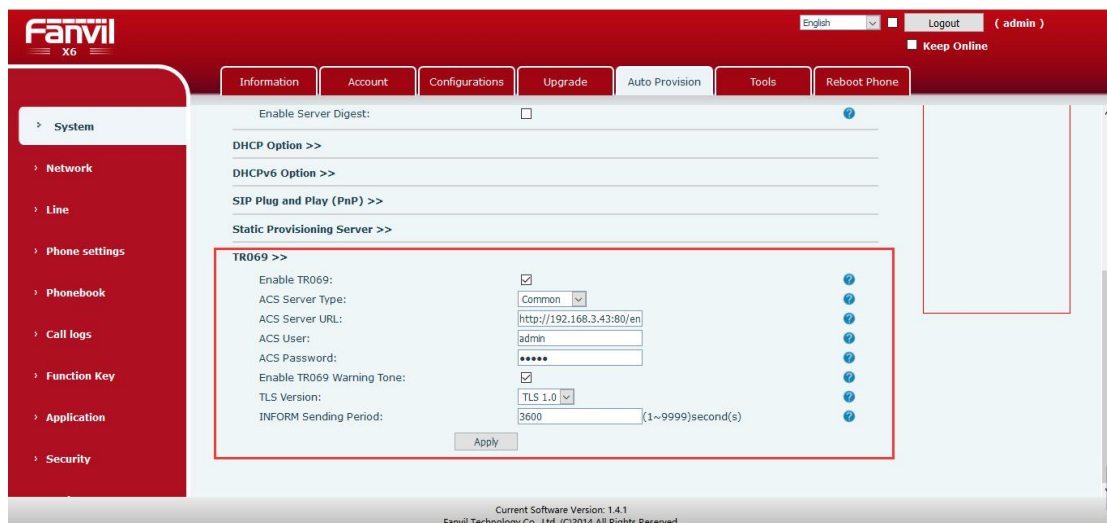


Server Address	1.1.1.1
Configuration File Name	
Protocol Type	FTP
Update Interval	1 Hour
Update Mode	Update After Reboot

Figure 15

- 2) Operation method
 - Configure the static provisioning server.
 - Store the configuration file under the corresponding directory of the server.
 - Restart the telephone set.
4. TR069

TR069 is a CPE WAN management protocol. It implements communication between the CPE and the ACS. It defines a piece of end user equipment of the application-layer protocol for remote management. An effective ACS is required before TR069 deployment. Two types of Fanvil endpoint ACSs are supported: CTC and common. Different ACSs provide different functions. CTC supports the XML format whereas common ACSs support SIP information, configuration file, and firmware configurations. If it is disabled, a telephone set cannot detect TR069.



Enable TR069:

ACS Server Type: Common

ACS Server URL: http://192.168.3.43:80/en

ACS User: admin

ACS Password: *****

Enable TR069 Warning Tone:

TLS Version: TLS 1.0

INFORM Sending Period: 3600 (1~9999)second(s)

Apply

Figure 16

After TR069 is enabled and the telephone set is restarted, capture HTTP packets. It is found that the telephone set sends a connection request and then an authentication request to the server. For an authentication success, the server returns a 200 OK message carrying script content for operating the telephone set. To perform corresponding operations on the telephone set, log in to the TR069 server (http://172.16.1.16:8081/openacs) and perform related configuration.

For example, download a configuration file.

- Log in to the TR069 server. Find the Download option on the Configuration scripts page, copy the content to the default option, and modify the path for downloading the configuration file based on the actual situation.
- Start the corresponding server.
- Store the configuration file under the specified directory.
- Enable TR069 for the telephone set and restart it.
- Restart the telephone set and capture packets.

The screenshot displays a network traffic capture in Wireshark. The top pane shows a SOAP message structure:

```

</SOAP-ENV:Header>
<SOAP-ENV:Body>
  <cwmp:Download
    xmlns:cwmp="urn:ietf:params:xml:ns:cwmp"
    <CommandKey>
      M Download
    </CommandKey>
    <FileType>
      3 vendor Configuration File
    </FileType>
    <URL>
      ftp://192.168.2.45/config.txt
    </URL>
    <Username>
      1
    </Username>
    <Password>
      1
    </Password>
    <FileSize>
      38864
    </FileSize>
    <TargetFileName>
      config.txt
    </TargetFileName>
  </cwmp:Download>
</SOAP-ENV:Body>

```

The bottom pane shows a list of captured packets with the following columns: No., Time, Source, Destination, Protocol, Length, and Info. The filter is set to 'http@ip.addr==192.168.3.227'. The selected packet (No. 1024) is a POST request to /openacs/acs HTTP/1.1.

No.	Time	Source	Destination	Protocol	Length	Info
550	2014-03-20 16:44:24.026089	192.168.3.227	192.168.2.80	HTTP/XML	383	POST /openacs/acs HTTP/1.1
553	2014-03-20 16:44:24.072927	192.168.2.80	192.168.3.227	HTTP/XML	931	HTTP/1.1 200 OK
555	2014-03-20 16:44:24.085523	192.168.3.227	192.168.2.80	HTTP	297	POST /openacs/acs HTTP/1.1
560	2014-03-20 16:44:24.176453	192.168.2.80	192.168.3.227	HTTP/XML	1184	HTTP/1.1 200 OK
573	2014-03-20 16:44:24.700657	192.168.3.227	192.168.2.80	HTTP/XML	1054	POST /openacs/acs HTTP/1.1
576	2014-03-20 16:44:24.711166	192.168.3.227	192.168.2.80	HTTP/XML	951	POST /openacs/acs HTTP/1.1
2344	2014-03-20 16:44:29.718727	192.168.2.80	192.168.3.227	HTTP/XML	1171	HTTP/1.1 200 OK
3503	2014-03-20 16:44:34.728476	192.168.2.80	192.168.3.227	HTTP	260	HTTP/1.1 204 No Content
3551	2014-03-20 16:44:36.746601	192.168.3.227	192.168.2.80	HTTP/XML	1054	POST /openacs/acs HTTP/1.1
5893	2014-03-20 16:44:41.759777	192.168.2.80	192.168.3.227	HTTP	260	HTTP/1.1 204 No Content
32360	2014-03-20 16:45:35.708614	192.168.3.227	192.168.2.80	HTTP/XML	390	POST /openacs/acs HTTP/1.1
32363	2014-03-20 16:45:35.753126	192.168.2.80	192.168.3.227	HTTP/XML	930	HTTP/1.1 200 OK
32365	2014-03-20 16:45:35.760074	192.168.3.227	192.168.2.80	HTTP/XML	1120	POST /openacs/acs HTTP/1.1
32367	2014-03-20 16:45:35.773870	192.168.2.80	192.168.3.227	HTTP/XML	825	HTTP/1.1 200 OK
32369	2014-03-20 16:45:35.777379	192.168.3.227	192.168.2.80	HTTP	297	POST /openacs/acs HTTP/1.1
32371	2014-03-20 16:45:35.800500	192.168.2.80	192.168.3.227	HTTP	260	HTTP/1.1 204 No Content
42648	2014-03-20 16:46:36.707904	192.168.3.227	192.168.2.80	HTTP/XML	381	POST /openacs/acs HTTP/1.1
42652	2014-03-20 16:46:36.733902	192.168.2.80	192.168.3.227	HTTP/XML	930	HTTP/1.1 200 OK
42654	2014-03-20 16:46:36.741470	192.168.3.227	192.168.2.80	HTTP	297	POST /openacs/acs HTTP/1.1
42657	2014-03-20 16:46:36.812133	192.168.2.80	192.168.3.227	HTTP/XML	1044	HTTP/1.1 200 OK
42659	2014-03-20 16:46:36.817114	192.168.3.227	192.168.2.80	HTTP/XML	1214	POST /openacs/acs HTTP/1.1
43513	2014-03-20 16:46:41.834938	192.168.2.80	192.168.3.227	HTTP/XML	1185	HTTP/1.1 200 OK
43515	2014-03-20 16:46:41.839255	192.168.3.227	192.168.2.80	HTTP/XML	973	POST /openacs/acs HTTP/1.1
43519	2014-03-20 16:46:41.890554	192.168.2.80	192.168.3.227	HTTP/XML	1184	HTTP/1.1 200 OK
43539	2014-03-20 16:46:42.695922	192.168.3.227	192.168.2.80	HTTP/XML	1054	POST /openacs/acs HTTP/1.1

Figure 17

4.4 Supported File Types

1. Firmware

Telephone set version. The function of comparing the digests of supported versions is automatically deployed. During upgrade, modify the digest of the version; otherwise, a version can be downloaded only once.

Example of the URL in the configuration file (txt format):

Auto Image Url :ftp://172.16.6.70:8000/x4.z

```
<<VOIP CONFIG FILE>>Version:2.0002

<AUTOUPDATE CONFIG MODULE>

Auto Image Url      :ftp://123:123@172.16.6.70:8000/x4.z

<<END OF FILE>>
```

Figure 18

2. Phone book

The phone book supports three formats: xml, vcf, and csv.

Auto Pbook Url :tftp://123:123@172.16.6.70/500.vcf

```
<<VOIP CONFIG FILE>>Version:2.0002

<AUTOUPDATE CONFIG MODULE>

Auto Pbook Url     :tftp://123:123@172.16.6.70/500.csv

<<END OF FILE>>
```

Figure 19

3. etc

The certificate file supports a range of suffixes: bin, crt, key, ovpn, and xml.

Auto etc Url :ftp://1:1@172.16.6.70/sips.pem

```
<<VOIP CONFIG FILE>>Version:2.0002 |

<AUTOUPDATE CONFIG MODULE>

Auto Etc Url       :tftp://172.16.6.70/sips.pem

<<END OF FILE>>
```

Figure 20

4. Background

Background image, fixed with background name, BMP format.

Auto Logo Url :tftp://172.16.6.70/background.bmp

```
<<VOIP CONFIG FILE>>Version:2.0002

<AUTOUPDATE CONFIG MODULE>

Auto Logo Url      :tftp://172.16.6.70/background.bmp

<<END OF FILE>>
```

Figure 21

5. mmiset

The mmiset file contains all webpage and customization information about a telephone set. The .mmiset format is not supported in auto provision of telephone sets. Compress the .mmiset file in .z format for upgrade.

Auto Mmiset Url :

tftp://123:123@172.16.6.45/mmiset6_SpanishT20131206171925.z

```
<<VOIP CONFIG FILE>>Version:2.0002

<AUTOUPDATE CONFIG MODULE>
Auto Mmiset Url    :tftp://123:123@172.16.6.45/mmiset6_SpanishT20131206171925.z

<<END OF FILE>>
```

Figure 22

6. Dialpeer.csv(**industry support only**)

Dialing rules, fixed to dialPeer name, in CSV format.

Auto DPeer Url :ftp://123:123@172.16.6.45:8080/dialPeer.csv

```
<<VOIP CONFIG FILE>>Version:2.0002

<AUTOUPDATE CONFIG MODULE>

Auto DPeer Url    :ftp://123:123@172.16.6.45:8080/dialPeer.csv

<<END OF FILE>>
```

Figure 23

7. Access table(**only the supported models of access control series are i31s, i30, i23s, i20s, i32v and i33V**)

Automatically update accessList, fixed to accessList name, for CSV format

Auto AList Url :ftp://123:123@172.16.6.45:8080/accessList.csv

```
<<VOIP CONFIG FILE>>Version:2.0002
<AUTOUPDATE CONFIG MODULE>
Auto AList Url :ftp://123:123@172.16.6.45:8080/accessList.csv
<<END OF FILE>>
```

Figure 24

4.5 Save Auto Provision Information

Select this item on the webpage, as shown in Figure 25.

Auto Provision Settings	
Current Config Version	2.0002
Common Config Version	2.0002
CPE Serial Number	00100400FV0200100000000307a9b486
User	<input type="text"/>
Password	<input type="text"/>
Config Encryption Key	<input type="text"/>
Common Config Encryption Key	<input type="text"/>
Save Auto Provision Information	<input checked="" type="checkbox"/>

Figure 25

If a telephone set uses a custom configuration file for upgrade, the telephone set displays a dialog box for entering the configuration file ID at initial upgrade and then the telephone set downloads the configuration file. At the second upgrade, the telephone set remembers the configuration file ID and directly downloads the configuration file.

Note: The auto provision application is updated and the internal format of the configuration file is no longer restricted.

A configuration file cannot be downloaded twice consecutively. To achieve this purpose, modify the time zone or add spaces.

4.6 Auto Provision Access Table list

First click export access list, edit the information to be imported in the table, and upgrade the list through automatic upgrade. After the upgrade, you can see the import details in the access list.

Import Access Table

Select File (accessList.csv)

Access Table >> [Click here to Save Access Table](#)

Total: 1 Page: 1

<input type="checkbox"/>	Index	Name	ID	Department	Position	Location	Number	Fwd Number	Access Code	Double Auth	Profile	Type	Issuing Date	Card State
<input type="checkbox"/>	1	豆豆							123456789	Disable	None	Guest	2019/07/16 13:39:49	Enable

Figure 26