

Auto Config Instruction

Document Version: V2.1

1. Description	2
1.1 Purpose	2
1.2 Systematic structure.....	2
1.3 Install the software	2
1.4 Special precautions.....	2
2. File Description.....	2
2.1 Function Description.....	2
2.2 File Function Description:	2
2.3 MACList.txt Description	3
2.4 StandardCFG.dat Description.....	3
3. The Batch File Encrypting (MakeMACF.exe)	4
3.1 Function Description.....	4
3.2 Carry out the File to Encrypt.....	4
4. Single file encryption or decryption (Encrypt/Decrypt)	6
4.1 Function description	6
4.2 Carry out the file to encrypt	6
4.3 Carry out the file decryption.....	9
5. Carry out Auto Configuration	10
5.1 Auto Configuration Setting via TFTP Server.....	10
5.2 Auto Configuration Setting via FTP Server	11
5.3 Auto Configuration Setting via HTTP Server	12
5.4 Auto Configuration Setting via IP PBX	13
Appendix. The exposition of StandardCFG file	16

1. Description

1.1 Purpose

Offer it through TFTP / FTP / HTTP Server and IP PBX, doing the change of established file.

1.2 Systematic structure

1. There must be a TFTP / FTP / HTTP Server.

1.3 Install the software

1. Install Auto Provision program in the computer: Carry out encrypted Mac Address file.

1.4 Special precautions

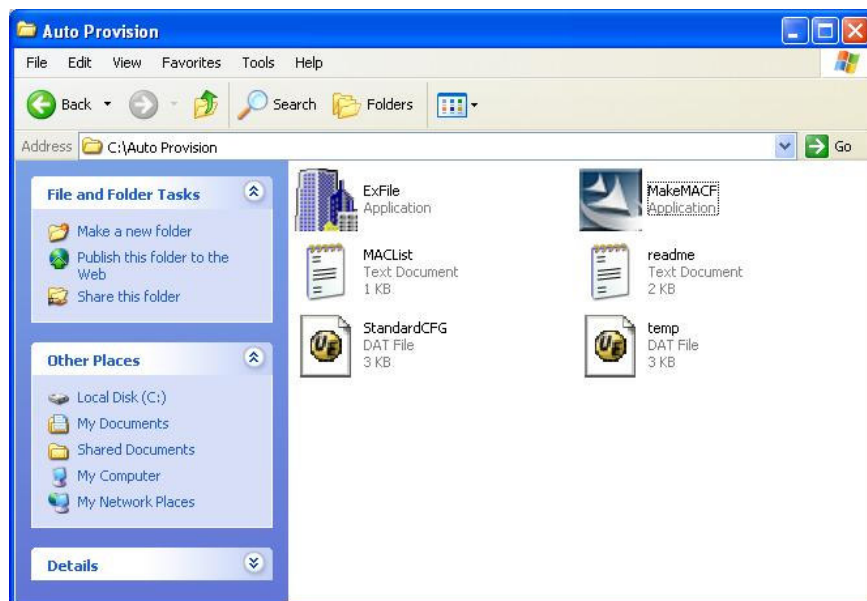
1. It provides one group MAC Address for testing only at present, MAC ID: 00aabbccdde.

2. File Description

2.1 Function Description

It produces a large number of encryption file data that this program only offers.

2.2 File Function Description:



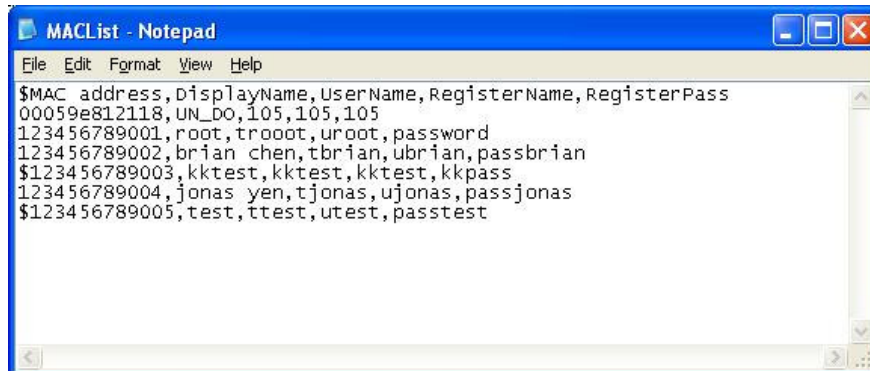
The Picture Description:

- ExFile.exe (program): Only provide single file encrypted or decrypted action.
- MACList.txt: Select the file name you want to load.
- MakeMACF.exe (program): Select the file name you want to load. The form of the file is dat file.
- Readme.txt: Select the file name you want to load .
- StandardCFG.dat: The standard example file that system preset. This file is to generate

MAC Address.DAT.

- Temp.dat: Example File form.

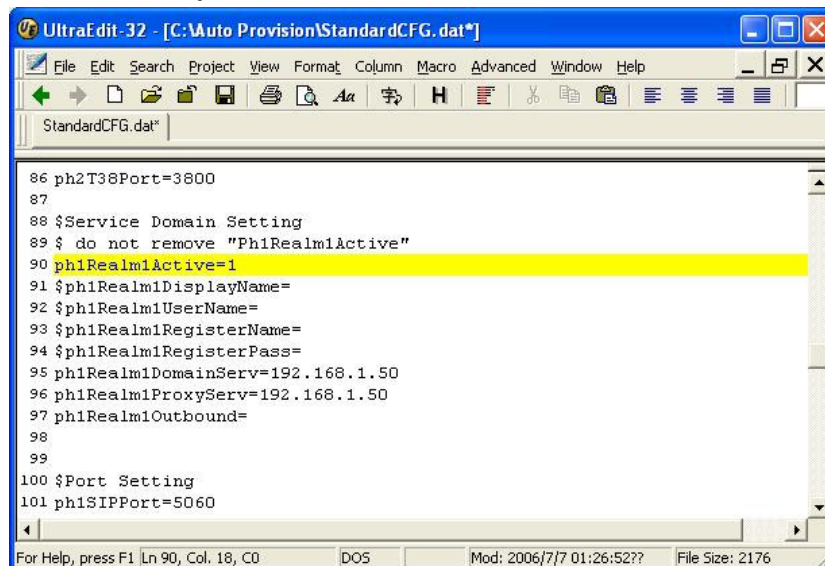
2.3 MACList.txt Description



The Picture Description:

- \$MAC address,DisplayName, UserName,RegisterName,RegisterPass.
 - \$: This behavior note does not use it.
 - MAC address: Input MAC Address ID data.
 - DisplayName: Input the registered account number name or data wanted to show.
 - UserName: Input the user name.
 - RegisterName: Input the account number.
 - RegisterPass: Input the account password.

2.4 StandardCFG.dat Description



The Picture Description: This file can not increase or reduce any data.

- (The 90th line) ph1Realm1Active= 1, the program will use this line to load [maclist.txt], and generate the relevant encryption file.

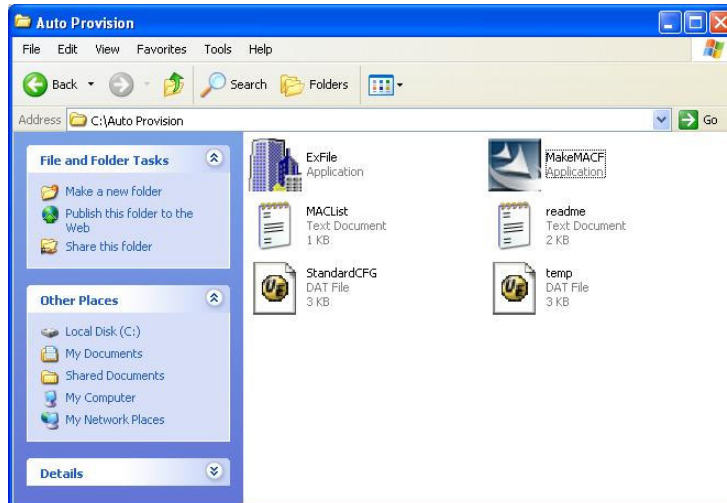
3. The Batch File Encrypting (MakeMACF.exe)

3.1 Function Description

It produces a large number of encryption file data that this program only offers.

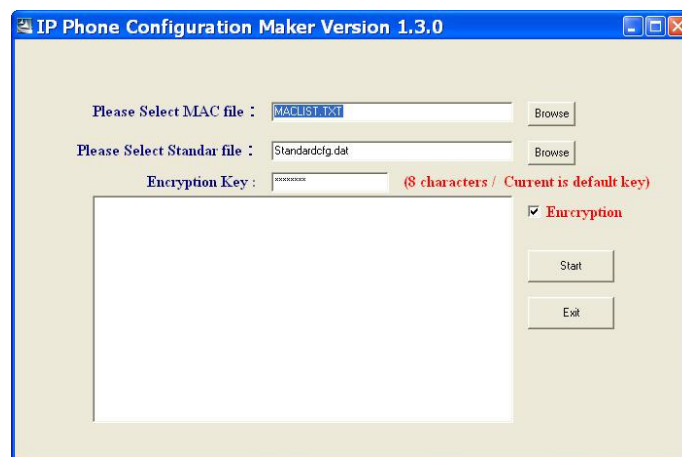
3.2 Carry out the File to Encrypt

Step 1: Open [Test _ Tools\AutoProvision] catalogue, click the program: [MakeMACF.exe] (as Fig. 1).



(Fig. 1)

Step 2: Enter [IP Phone Configuration Maker] , this program offers [batch file encryption] (as Fig. 2).



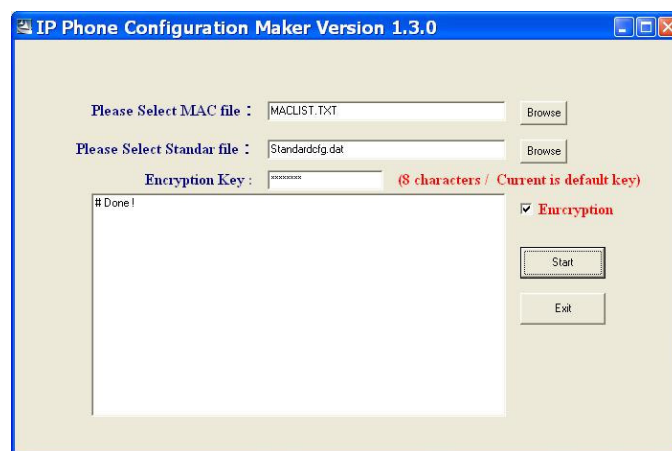
(Fig. 2)

The picture description:

- Please Select MAC File: Select the MAC file name you want to load, the form of the file is txt file. The system is set as in advance: MACLIST.txt.
- [Browse] button: Select the file name you want to load.
- Please Select Standard File: Select the standard file name you want to load, the form of the file is dat file, the system is set as in advance: Standard.dat.

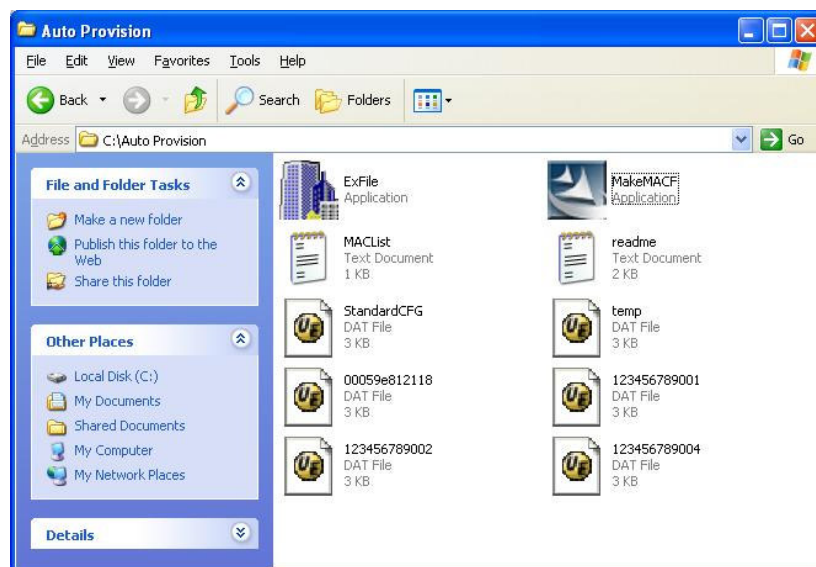
- [Browse] button: Select the file name you want to load.
- Encryption Key (8 characters / Currents is default Key): Input the word bunch you want to encrypt, offer the length of 8 words , it is set to default value currently.
- State district: Show the executive mode.
- Encryption: Carry out encryption.
- [Start] button: Carry out the batch file with encryption.
- [Exit] button: Close [IP Phone Configuration Maker] program.

Step 3: Set the file data which need to be encrypted. (for example: Please Select MAC file: MACLIST.txt, Please Select Standard file: Standardcfg.dat, Encryption Key: Current), cancels and selects [Encryption] item, generate encryption data; Press [Start] button, then start it; It shows [#Done!], it means ok (as Fig. 3).



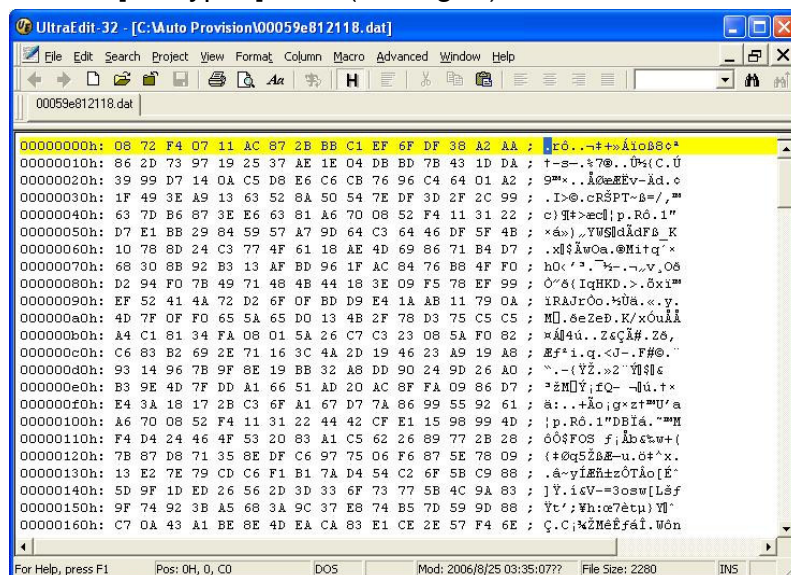
(Fig. 3)

Step 4: In [in D:\Test_Tools\AutoProvision] folder, generate several files: [MACAddress.dat] by (as Fig.4).



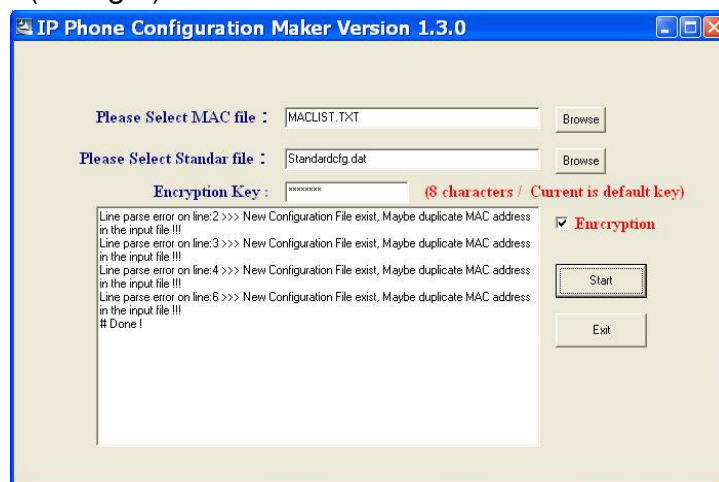
(Fig. 4)

Step 5: Check whether the file produced is a form encrypted , open [00059e812118.dat] file, can see this file is [encrypts] form (as Fig. 5).



(Fig. 5)

Step 6: In encryption stage, there is a error message in [state district]. It means the file has to be generated. (as Fig.6).



(Fig. 6)

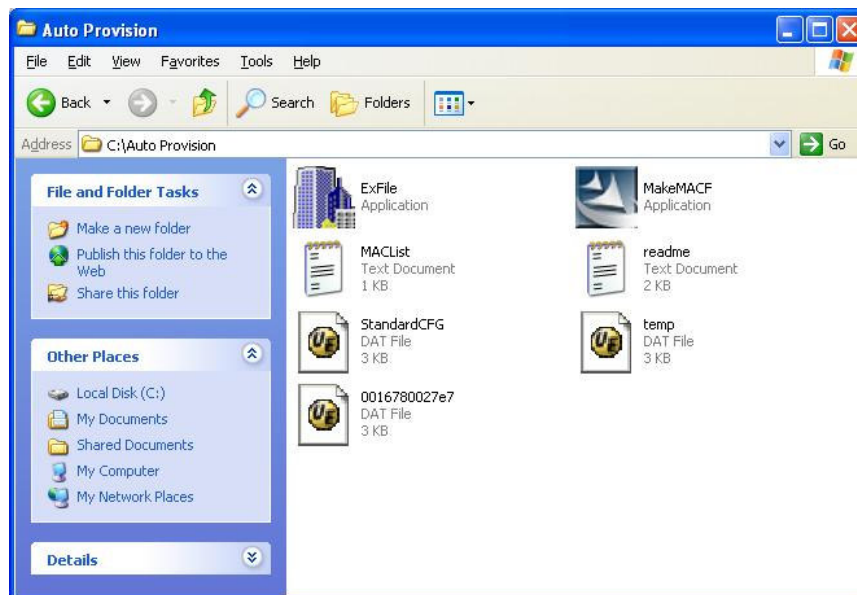
4. Single file encryption or decryption (Encrypt/Decrypt)

4.1 Function description

This program only offers a small amount of files encryption or decryption; if you want to carry out a large number of files encryption, please use [MakeMACF.exe] program.

4.2 Carry out the file to encrypt

Step 1: Open [Test _ Tools\AutoProvision] catalog, click [ExFile.exe] program (as Fig. 7).



(Fig. 7)

Step 2: Enter [Encrypt/Decrypt] screen, this program offers files encryption & decryption (as Fig. 8).



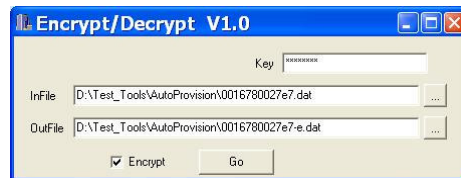
(Fig. 8)

The picture description:

- Key: Input word bunch which need to be encrypted, Key field data is program default value “Current “can’t be modified.
- InFile: The file path and file name which needs to be encrypted or decrypted; the form of the file is dat file.
 - The data on this field which is not encrypted, no matter whether Encrypt have started, it’s the encryption.
 - The encrypted data in field of In file, when chooses Disable Encrypt, it will carry out encryption once again.
 - The encrypted data in field of In file, when chooses Enable Encrypt, it will carry out description.
- [Browse] button: chose the file path and name which has to be loaded.
- OutFile: Produce encrypted or decrypted file path and file name; the form of the file is dat file.
- [Browse] button: Choose the file name path and file name which has to be loaded.
- Encrypt: choose encryption or decryption.
- [Go] button: It produces encrypted or decrypted file.

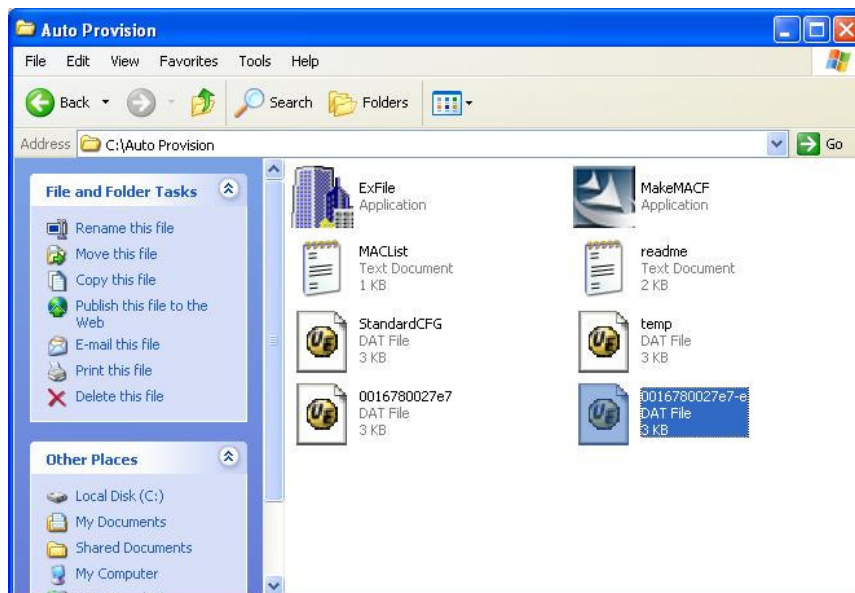
Remarks: StandardCFG.dat offers the standard file form, can change attached file to MAC Address, for example: 0016780027e7.dat.

Step 3: Set the file data which need to be encrypted. (for example: InFile: D:\Test_Toos\AutoProvision\0016780027e7. dat, OutFile: D:\Test_Toos\AutoProvision\0016780027e7-e.dat), selects [Encrypt] item, it produces encrypted data; Press [Go] button, carry out and produce encrypted file. (as Fig. 9).



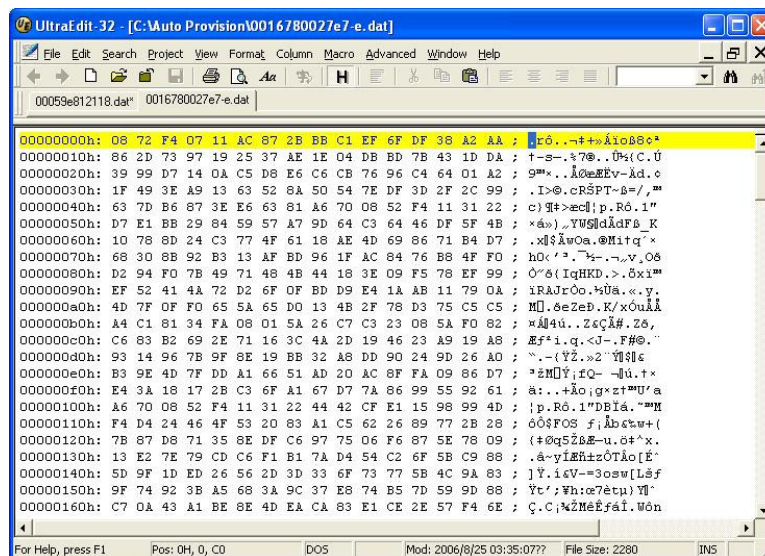
(Fig. 9)

Step 4: In [D:\Test_Toos\AutoProvision] folder, it produces one file [0016780027e7-e.dat] (as Fig.10).



(Fig. 10)

Step 5: Can check whether the file produced is a encrypted form, open [0016780027e7-e.dat] file, can see this form is a encrypted form (as Fig. 11).



(Fig. 11)

4.3 Carry out the file decryption

Step 1: In [Encrypt / decrypt] picture, this program offers [the file encryption and decryption] (as Fig. 12).



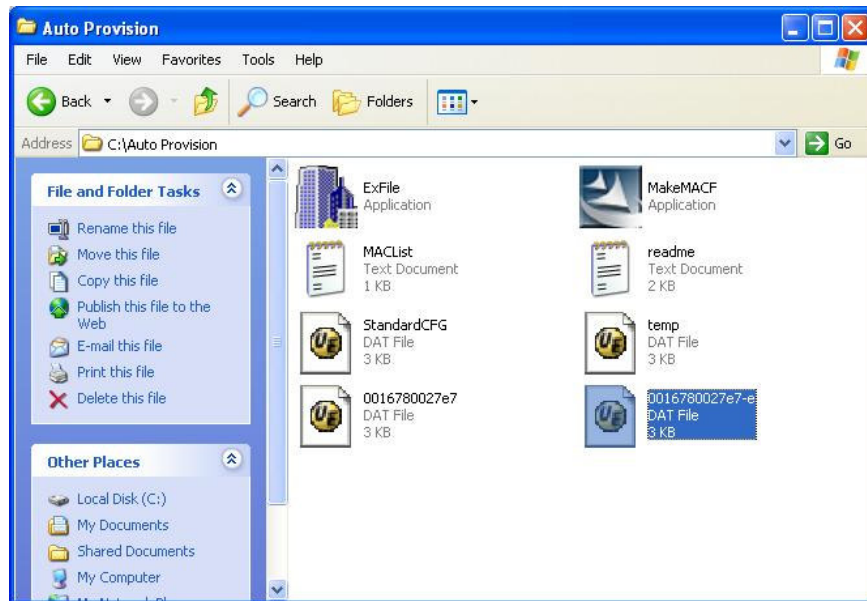
(Fig. 12)

Step 2: Set the file data has to be decrypted (for example: OutFile: D:\Test_Toos\AutoProvision\0016780027e7-e. dat, OutFile: D:\Test_Toos\AutoProvision\0016780027e7.dat), selects [Encrypt] item, it produces decrypted data; Press [Go] button, carry out and produce decrypted file (as Fig. 13).



(Fig. 13)

Step 3: In [D:\Test_Toos\AutoProvision] folder, it produces one file [0016780027e7.dat] file (as Fig.14).



(Fig. 14)

Step 4: Can check its form is a decrypted form, open [0016780027e7.dat] file, this file is a non [encrypt] form.

5. Carry out Auto Configuration

Current test MAC Address is 00aabbccdde, please be sure to make MAC Address into 00aabbccdde.

5.1 Auto Configuration Setting via TFTP Server

Step 1: Please log on ATA via web browser and browse to “**Advanced Settings → Auto Config**” menu, select the TFTP method and fill the TFTP Server IP address in <TFTP Server> field. Then press <Submit> button (as Fig. 15).

Auto Configuration Settings

You could enable/disable the auto configuration setting in this page.

Auto Configuration: ☐ Off ☐ TFTP ☐ FTP ☐ HTTP ☒ IP-PBX

TFTP Server:	<input type="text"/>	
HTTP Server:	<input type="text"/>	Exp. 60.35.187.30
HTTP File Path:	<input type="text"/>	Exp. /download/

FTP Server:	<input type="text"/>	Exp. 60.35.17.1
FTP Username:	<input type="text"/>	
FTP Password:	<input type="text"/>	
FTP File Path:	<input type="text"/>	Exp. /file/load

(Fig. 15)

Step 2: Browse to “**Save & Reboot**” menu and press <Save> button, ATA will connect to TFTP Server for setting altering after system boots up successfully.

Step 3: The altered setting is there when going to SIP Setting page.

Service Domain Settings

You could set information of service domains in this page.

Realm 1 (Default)	
Active:	<input checked="" type="radio"/> On <input type="radio"/> Off
Display Name:	<input type="text" value="UN_DO"/>
Line Number:	<input type="text" value="105"/>
Register Name:	<input type="text" value="105"/>
Register Password:	<input type="password" value="..."/>
Domain Server:	<input type="text" value="192.168.1.50"/>
Proxy Server:	<input type="text" value="192.168.1.50"/>
Outbound Proxy:	<input type="text"/>
Status:	Registered

(Fig. 16)

5.2 Auto Configuration Setting via FTP Server

Step 1: Please log on ATA via web browser and browse to “**Advanced Settings → Auto Config**” menu, select the FTP method and fill the FTP Server IP address/ Username/ Password out <FTP related> fields. Then press <Submit> button (as Fig. 17).

Auto Configuration Settings

You could enable/disable the auto configuration setting in this page.

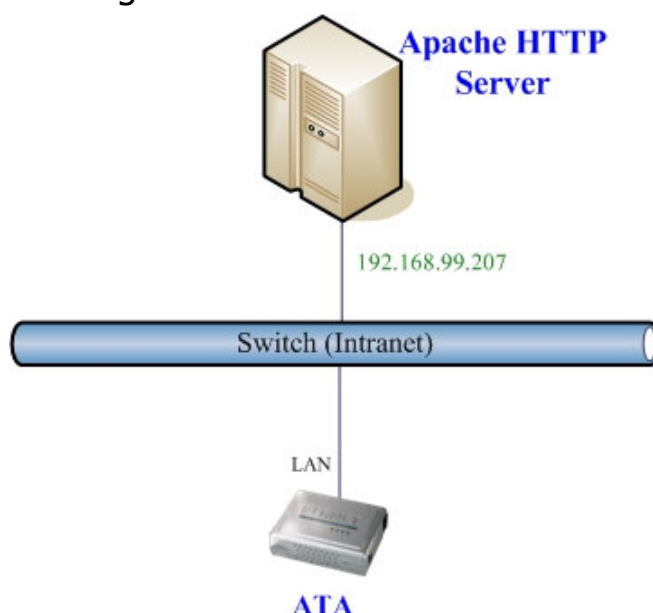
Auto Configuration: ☐ Off ☐ TFTP ☒ FTP ☐ HTTP ☐ IP-PBX

TFTP Server:	<input type="text"/>	
HTTP Server:	<input type="text"/>	Exp. 60.35.187.30
HTTP File Path:	<input type="text"/>	Exp. /download/
FTP Server:	<input type="text" value="192.168.99.207"/>	Exp. 60.35.17.1
FTP Username:	<input type="text" value="admin"/>	
FTP Password:	<input type="password" value="..."/>	
FTP File Path:	<input type="text"/>	Exp. /file/load

(Fig. 17)

Step 2: Browse to “**Save & Reboot**” menu and press <Save> button, ATA will connect to FTP Server for setting altering after system boots up successfully.

5.3 Auto Configuration Setting via HTTP Server



Step 1: Please log on ATA via web browser and browse to “**Advanced Settings** → **Auto Config**” menu, select the HTTP method and fill the HTTP Server IP address/ File Path out <HTTP Server> and <File Path> fields. Then press <Submit> button (as Fig. 18).

Auto Configuration Settings

You could enable/disable the auto configuration setting in this page.

Auto Configuration: ☐ Off ☐ TFTP ☐ FTP ☒ HTTP ☐ IP-PBX

TFTP Server:	<input type="text"/>	
HTTP Server:	<input type="text" value="192.168.99.207"/>	Exp. 60.35.187.30
HTTP File Path:	<input type="text" value="/"/>	Exp. /download/

FTP Server:	<input type="text"/>	Exp. 60.35.17.1
FTP Username:	<input type="text"/>	
FTP Password:	<input type="text"/>	
FTP File Path:	<input type="text"/>	Exp. /file/load

(Fig. 18)

Notice: The configuration files were placed in the root of Apache HTTP Server, so that the File Path need fills in </>. If the configuration files were placed in the other subdirectory, it needs input the correct file path. For example, if the configuration files were placed in “123” subdirectory, the correct file path is </123/>.

Step 2: Browse to “**Save & Reboot**” menu and press <Save> button, ATA will connect to HTTP Server for setting altering after system boots up successfully.

5.4 Auto Configuration Setting via IP PBX



■ ATA A IP Address: 192.168.0.1
Line Number: 1001

■ ATA B IP Address: 192.168.0.2
Line Number: 2002

Device configurations on the IPX-2000:

STEP 1: Log in IPX-2000 and browse to the **Srvice** → **DHCP Service** menu and create new options list for the auto configuration.

:: DHCP SERVICE

DHCP POOL

lan

☒ Enable ☐ Disable
On-board LAN

Show Leased Clients

☒ Range ☐ Single-host

Pool Name: lan

IP: 192.168.1.101 ~ 192.168.1.200

Options: 150,192.168.1.1

Code,Value: 151 http://192.168.0.50/tftpboot/

Code: please insert **151** as the DHCP server option.

Value: http://LAN IP for IPX-2000/tftpboot/

An example option 151 would be option=**151** value= **http://192.168.0.50/tftpboot/**

STEP 2: Log in IPX-2000 and browse to the **Device** → **IP Phone** menu and create new device.
And press the **EDIT** button for set up the Auto Config configuration.

:: DEVICE PHONE MANAGEMENT				
Device ID		Device Administration URL		ADD
<input type="text"/>		<input type="text"/>		
DEL				
Device ID	Associated Extension	Device Administration URL	Auto Client Conf	
<input type="checkbox"/> auto_dev_vip156		<input type="text"/> LINK	Disabled	EDIT APPLY
<input type="checkbox"/> auto_dev_vip157		<input type="text"/> LINK	Disabled	EDIT APPLY

STEP 3: Please fill out the Vendor Prefix code and MAC Address of ATA.

Enable Automatic Client Configuration	
Device	auto_dev_vip156
Vendor Prefix	<input type="text" value="pla156"/> (a-zA-Z0-9_)
MAC Address	<input type="text" value="00"/> <input type="text" value="30"/> <input type="text" value="4f"/> <input type="text" value="aa"/> <input type="text" value="bb"/> <input type="text" value="dd"/>
Supplementary Configuration	<input type="button" value="v"/>
Codec Preference	
1st codec	<input type="text" value="g711ulaw"/> <input type="button" value="v"/>
1st packet time	<input type="text" value="20"/> <input type="button" value="v"/>
2nd codec	<input type="text" value="g711alaw"/> <input type="button" value="v"/>
2nd packet time	<input type="text" value="20"/> <input type="button" value="v"/>
3rd codec	<input type="text" value="g729"/> <input type="button" value="v"/>
3rd packet time	<input type="text" value="30"/> <input type="button" value="v"/>
<input type="checkbox"/> Enable Voice Activity Detection (VAD)	
DTMF Mode	<input type="text" value="Inband"/> <input type="button" value="v"/>
<input type="button" value="ENABLE"/> <input type="button" value="BACK"/>	

①Note:

The following are the Vendor Prefix of devices:

1. VIP-154 series: **pla154**
2. VIP-156: **pla156**
3. VIP-157/VIP-157S: **pla157**

STEP 4: Please browse to the **Device → Extension of IP Phone** menu to create the two extension accounts/password: **1001/123** (for ATA A), and **1002/123**(for ATA B) for the voice calls.

:: EXTENSION MANAGEMENT

Extension Number	<input type="text" value="1001"/>	
Associated Device	<input type="text" value="auto_dev_vip156"/>	
Password	<input type="password" value="..."/>	
User	<input type="text" value="admin(admin)"/>	
Pickup Group	<input type="text" value="UG_DEF"/>	
Line Type	<input type="text" value="Wired"/>	
Language	<input type="text" value="English"/>	
Voicemail	<input type="text" value="Enable"/>	
Voicemail PIN	<input type="password" value="..."/>	
Unavailable Timeout	<input type="text" value="10"/> sec.	
<input type="checkbox"/> Allow LAN Use Only		
Try Peer-to-peer RTP	<input type="text" value="NO"/>	
DTMF Mode	<input type="text" value="inband"/>	<input type="button" value="ADD"/> <input type="button" value="BACK"/>
<input type="checkbox"/> Advanced Options		

STEP 5: After setting up the parameters, please browse to the **Service → IP PBX service** menu, and press **RELOAD** of IP PBX configuration reload selection for activating the settings.

:: IP PBX SERVICE

Service & Configuration
Advance

IP PBX will reload configuration as soon as possible.
 Currently active calls will be disconnected in 3 minutes.
 Do you really want to Continue?

☐ PBX Settings Only

Device configurations on the ATA:

STEP 6: Please log on ATA via web browser and browse to “**Advanced Settings → Auto Config**” menu, select the IP PBX method. Then press <Submit> button (as Fig. 19).

Auto Configuration Settings

You could enable/disable the auto configuration setting in this page.

Auto Configuration: ☐ Off ☐ TFTP ☐ FTP ☐ HTTP ☒ IP-PBX

TFTP Server:	<input type="text"/>	
HTTP Server:	<input type="text"/>	Exp. 60.35.187.30
HTTP File Path:	<input type="text"/>	Exp. /download/
FTP Server:	<input type="text"/>	Exp. 60.35.17.1
FTP Username:	<input type="text"/>	
FTP Password:	<input type="text"/>	
FTP File Path:	<input type="text"/>	Exp. /file/load

(Fig. 19)

STEP 7: After enabling the auto-config feature, the ATA shall be able to obtain IP address and SIP extension information from IP PBX system IPX-2000 information. To verify the auto-config results, you may connect telephone set to ATA; press **#120#** to check if the IP address is obtained from IPX-2000. And **#122#** can be used to verify the extension number assigned by IPX-2000.

STEP 8: Repeat the same configuration steps on ATA B, and check if the ATA B is successfully registered with the IPX-2000 as one of the IP extensions.

Appendix. The exposition of StandardCFG file

The bellows are the original contents of StandardCFG file and the descriptions of configuration.

Original contents	Descriptions and Examples
<pre>\$Phone Book function: \$speed dial phone \$Keep "line0Name=" at first line line0Name= line0Url= line1Name= line1Url=</pre>	<p>Descriptions:</p> <p>line0Name ~ line9name: name or number <max length=31></p> <p>line0Url ~ line9url: Dial number or ip address <max length=63></p> <p>Examples:</p> <p>line0name=0, line0Url=192.168.1.20;</p> <p>line1name=1, line1Ur1=0800024365</p>

line2Name= line2Url= line3Name= line3Url= line4Name= line4Url= line5Name= line5Url= line6Name= line6Url= line7Name= line7Url= line8Name= line8Url= line9Name= line9Url=	
\$Phone Setting function: \$Call forward Setting AllFwd=0 BusyFwd=0 NoAnsFwd=0 AllFwdName= AllFwdUrl= BusyFwdName= BusyFwdUrl= NoAnsFwdName= NoAnsFwdUrl= NoAnsTimeOut=3	Description: AllFwd=0(Default); All forward: 0~1 (0:Disable, 1:Enable) BusyFwd=0(Default); Busy forward: 0~1 (0:Disable, 1:Enable) NoAnsFwd=0(Default); No Answer forward: 0~1 (0:Disable, 1:Enable) AllFwdName=; All fwd no Name: Dial number or name <maxlength=31> AllFwdUrl=; All fwd no RUL: ipaddress or Dial number <maxlength=63> BusyFwdName=; Busy fwd no Name: Dial number or name <maxlength=31> BusyFwdUrl=; Busy fwd no RUL: ipaddress or Dial number <maxlength=63> NoAnsFwdName=; No Answer fwd no Name: Dial number or name <maxlength=31> NoAnsFwdUrl=; No Answer fwd no RUL ipaddress or Dial number <maxlength=63> NoAnsTimeOut=3(Default); No Answer Fwd Time Out: 2~8 Ring Example: Allfwd:1, AllFwdName=brian, AllFwdUrl=2206 BusyFwd=1, BusyFwdName=Family, BusyFwdUrl=0800123456 NoAnsFwd=1, NoAnsFwdName=adsl, NoAnsFwdUrl=192.168.1.6
\$SNTP setting SNTPEnable=1	Description: SNTPEnable=1(Default); SNTP: 0~1 (1:On, 0:Off)

SNTP1stServ=time.window.com SNTP2ndServ=208.184.49.9 SNTPTimeZone=+08:00 SNTPSyncTime=1:00:00	SNTP1stServ=time.window.com(Default); Primary Server: ipaddress or domain address <maxlength=63> SNTP2ndServ=208.184.49.9(Default); Secondary Server: ipaddress or domain address <maxlength=63> SNTPTimeZone=+08:00(Default); Time Zone:GMT +/- hh:mm (hh:00~13, mm:00~59) SNTPSyncTime=1:00:00(Default); Sync Time: dd:hh:mm (dd:00~10, hh:00~13, mm:00~59)
\$Volume Setting HandsetVol=10 SpeakerVol=10 RingerVol=6 PSTNVol=10 HandsetGain=10 SpeakerGain=9 PSTNGain=10	Description: HandsetVol=10(Default); Handset Volume: 0~15 SpeakerVol=10(Default); Speaker Volume: 0~15 RingerVol=6(Default); Ringer Volume: 0~10 PSTNVol=10(Default); PSTN-Out Volume:0~12 (for fxo port) HandsetGain=10(Default); Handset Gain: 0~15 SpeakerGain=9(Default); Speaker Gain: 0~15 PSTNGain=10(Default); PSTN-In Gain: 0~15 (for fxo port)
\$Melody setting -> for phone RingerEnable=0 RingerType=0	Description: RingerEnable=0(Default); Ringer: 0~1 (0:Off, 1:On) RingerType=0(Default); Ringer Type: 0~3 (0:Ringer1, 1:Ringer2, 2:Ringer3, 3:Ringer4)
\$DND Setting AlwayBlock=0 BlockPeriod=0 BlockFrom=00:00 BlockTo=00:00	Description: AlwayBlock=0(Default); DND Always: 0~1 (0:off, 1:On) BlockPeriod=0(Default); DND Period: 0~1 (0:off, 1:On) BlockFrom=00:00(Default); DND Period Form: 00:00~23:59 (hh:mm) BlockTo=00:00(Default); DND Period To: 00:00~23:59 (hh:mm)
\$Caller ID Setting CIDType=1 CIDSINGLE=1 CIDWithoutTime=1	Description: CIDType=1(Default); Caller ID: 0~3 (0:Don't show caller ID, 1:Caller ID after 1st Ring (FSK),2:Caller ID before 1st Ring (FSK), 3:Caller ID before 1st Ring (DTMF) CIDSINGLE=1(Default); Single Caller ID: 0~1 (1:No, 1: Yes) CIDWithoutTime=1(Default); CID Without Time: 0~1 (1:No, 1: Yes)
\$Auto Answer Setting (for FXO Port) AutoAnsEnable=0 AutoAnsCounter=3	Description: AutoAnsEnable=0(Default); Auto Answer: 0~1 (0:off, 1:IP IN, 2: FXO IN, 3: Both) AutoAnsCounter=3(Default); Auto Answer Counter: 0~8
\$Dial Plan Setting wDropCode1=0 wInsertCode1= wDialRule1= wDropCode2=0	Description: wDropCode1=0, Drop prefix: 0~1 (0:No-->insert, 1:Yes--> drop) wInsertCode1=; Replace reule 1: Dial number <maxlength=8> wDialRule1=; Replace reule 1 +: Dial Number <maxlength=40> wDropCode2=0, Drop prefix: 0~1 (0:No-->insert, 1:Yes--> drop)

wInsertCode2= wDialRule2= wDropCode3=0 wInsertCode3= wDialRule3= wDropCode4=0 wInsertCode4= wDialRule4= AutoDialTime=5	wInsertCode2=; Replace reule 2: Dial number <maxlength=8> wDialRule2=; Replace reule 2 +: Dial number <maxlength=40> wDropCode3=0, Drop prefix: 0~1 (0:No-->insert, 1:Yes--> drop) wInsertCode3=; Replace reule 3: Dial number <maxlength=8> wDialRule3=; Replace reule 3 +: Dial number <maxlength=40> wDropCode4=0, Drop prefix: 0~1 (0:No-->insert, 1:Yes--> drop) wInsertCode4=; Replace reule 4: Dial number <maxlength=8> wDialRule4=; Replace reule 4 +: Dial number <maxlength=40> AutoDialTime=5(default); Auto Dial Time: 3~9 sec Example: wDropCode1=0, wInsertCode1=002, wDialRule1=8613+8662+xxxx
\$Flash Time Setting (for FXS Port) FlashTime=60	Description: FlashTime=60(Default); Max Flash Time: 4~255 (x10MS) <maxlength=3>
\$Call Waiting Setting CallWaiting=1	Description: CallWaiting=1(Default); Call Waiting: 0~1 (0:Off, 1:On)
\$T.38(FAX) Setting T38=1 ph1T38Port=6000 ph2T38Port=6000	Description: T38=1(Default); T.38(FXS): 0~1 (0:Off, 1:On) ph1T38Port=6000(Default); T.38 Port/T.38 Phone1 Port: 1024~65533 <maxlength=5> ph2T38Port=6000(Default); T.38 Port/T.38 Phone2 Port: 1024~65533 <maxlength=5>
\$ Hot Line Setting HotLineEnable=0 HotLineNumber=	Description: HotLineEnable=0(Default); Use Hot Line: 0~1 (0:Disable, 1:Enable) HotLineNumber=; Hot Line number: ipaddress or Dial number <maxlength=63>
\$Network function: IPType=1 IPAddress= IPMask= IPGateway= IPDNS0=0.0.0.0 IPDNS1=0.0.0.0	Description: IPType=1(Default); IP Type: 0~2 (0:Fixed IP, 1:DHCP Client, 2:PPPoE) IPAddress=; IP: Fxied IP address <maxlength=15> IPMask=; Mask: Sunbet Mask address <maxlength=15> IPGateway=: Default Gateway IP address <maxlength=15> IPDNS0=0.0.0.0(Default); DNS Server1: 0.0.0.0 ~ 255.255.255.255 (0.0.0.0: get server) <maxlength=15> IPDNS1=0.0.0.0(Default); DNS Server2: 0.0.0.0 ~ 255.255.255.255 (0.0.0.0: get server) <maxlength=15>
\$VLAN Setting VLANEnable=0 VLANTag=136 VLANPriority=0	Description: VLANEnable=0(Default); VLAN Packets: 0~1 (0:Off, 1:On) VLANTag=136(Default); VID (802.1Q/TAG): 2~4094 <maxlength=4>

VLANCFI=0	<p>VLANPriority=0(Default); User Priority (802.1P): 0~7</p> <p>VLANCFI=0(Default); CFI: 0~1</p>
<p>\$PPTP Setting</p> <p>PPTPenable=0</p> <p>PPTPServer=</p> <p>PPTPUserName=</p> <p>PPTPPassword=</p>	<p>Description:</p> <p>PPTPenable=0(default); PPTP: 0~1 (0:Off, 1:On)</p> <p>PPTPServer=; PPTP Server: ipaddress or domain address</p> <p><maxlength=63></p> <p>PPTPUserName=; PPTP username: login pptp server account</p> <p><maxlength=63></p> <p>PPTPPassword=; PPTP password: login pptp server password</p> <p><maxlength=63></p>
<p>\$SIP Settings function:</p> <p>\$Service Domain Setting</p> <p>\$Don't remove "Ph1Realm1Active"</p> <p>ph1Realm1Active=1</p> <p>ph1Realm1DisplayName=</p> <p>ph1Realm1UserName=</p> <p>ph1Realm1RegisterName=</p> <p>ph1Realm1RegisterPass=</p> <p>ph1Realm1DomainServ=</p> <p>ph1Realm1ProxyServ=</p> <p>ph1Realm1Outbound=</p> <p>ph1Realm2DisplayName=</p> <p>ph1Realm2UserName=</p> <p>ph1Realm2RegisterName=</p> <p>ph1Realm2RegisterPass=</p> <p>ph1Realm2DomainServ=</p> <p>ph1Realm2ProxyServ=</p> <p>ph1Realm2Outbound=</p> <p>ph1Realm3DisplayName=</p> <p>ph1Realm3UserName=</p> <p>ph1Realm3RegisterName=</p> <p>ph1Realm3RegisterPass=</p> <p>ph1Realm3DomainServ=</p> <p>ph1Realm3ProxyServ=</p> <p>ph1Realm3Outbound=</p> <p>ph2Realm1Active=1</p> <p>ph2Realm1DisplayName=</p> <p>ph2Realm1UserName=</p> <p>ph2Realm1RegisterName=</p> <p>ph2Realm1RegisterPass=</p>	<p>Description:</p> <p>Line1 (FXS Port 1)--> Realm 1(Default)</p> <p>ph1Realm1Active=1(Default); Realm 1(Default) Active: 0~1 (0:Off, 1:On)</p> <p>ph1Realm1DisplayName=; Display Name: Dispaly register name</p> <p><maxlength=31></p> <p>ph1Realm1UserName=; User Name: register user name</p> <p><maxlength=31></p> <p>ph1Realm1RegisterName=; Register Name: register name</p> <p><maxlength=31></p> <p>ph1Realm1RegisterPass=; Register Password: register password</p> <p><maxlength=31></p> <p>ph1Realm1DomainServ=; Domain Server: ipaddress or domain address</p> <p><maxlength=63></p> <p>ph1Realm1ProxyServ=; Proxy Server: ipaddress or domain address</p> <p><maxlength=63></p> <p>ph1Realm1Outbound=; Outbound Proxy: ipaddress or domain address</p> <p><maxlength=63></p> <p>Line2 (FXS Port 2)--> Realm 1(Default)</p> <p>ph2Realm1Active=1(Default); Realm 1(Default) Active: 0~1 (0:Off, 1:On)</p> <p>ph2Realm1DisplayName=; Display Name: Dispaly register name</p> <p><maxlength=31></p> <p>ph2Realm1UserName=; User Name: register user name</p> <p><maxlength=31></p> <p>ph2Realm1RegisterName=; Register Name: register name</p> <p><maxlength=31></p> <p>ph2Realm1RegisterPass=; Register Password: register password</p> <p><maxlength=31></p> <p>ph2Realm1DomainServ=; Domain Server: ipaddress or domain address</p>

ph2Realm1DomainServ= ph2Realm1ProxyServ= ph2Realm1Outbound= ph2Realm2Active= ph2Realm2DisplayName= ph2Realm2UserName= ph2Realm2RegisterName= ph2Realm2RegisterPass= ph2Realm2DomainServ= ph2Realm2ProxyServ= ph2Realm2Outbound= ph2Realm3Active= ph2Realm3DisplayName= ph2Realm3UserName= ph2Realm3RegisterName= ph2Realm3RegisterPass= ph2Realm3DomainServ= ph2Realm3ProxyServ= ph2Realm3Outbound=	<maxlength=63> ph2Realm1ProxyServ =; Proxy Server: ipaddress or domain address <maxlength=63> ph2Realm1Outbound =; Outbound Proxy: ipaddress or domain address <maxlength=63>
\$Port Setting ph1SIPPort=5060 ph1RTPPort=60000 ph2SIPPort=5060 ph2RTPPort=60002	Description: ph1SIPPort =5060(Default); (Phone1) SIP Port: 10~65533 <maxlength=5> ph1RTPPort =60000(Default); (Phone1) RTP Port: 10~65533 <maxlength=5> ph2SIPPort =5060(Default); (Phone2)SIP Port: 10~65533 <maxlength=5> ph2RTPPort =60002(Default); (Phone2) RTP Port: 10~65533 <maxlength=5>
\$Codec Setting CodecPri1=1 CodecPri2=2 CodecPri3=3 CodecPri4=4 CodecPri5=5 CodecPri6=6 CodecPri7=7 CodecPri8=8 CodecPri9=9 G711G729pk1=2 G723pk1=3	Description: Codec Priority: Codec: 1:G.711 u-law, 2:G.711 a-law, 3:G.723, 4:G.729, 5:G.726 - 16, 6:G.726 - 24, 7:G.726 – 32, 8:G.726 – 40, 9:GSM CodecPri1 =1(Default); Codec Piroity 1: 1~9 CodecPri2 =2(Default); Codec Piroity 2: 1~9 CodecPri3 =3(Default); Codec Piroity 3: 1~9 CodecPri4 =4(Default); Codec Piroity 4: 1~9 CodecPri5 =5(Default); Codec Piroity 5: 1~9 CodecPri6 =6(Default); Codec Piroity 6: 1~9 CodecPri7 =7(Default); Codec Piroity 7: 1~9 CodecPri8 =8(Default); Codec Piroity 8: 1~9

G723Enable=0 VoiceVADEnable=0	<p>CodecPri9=9(Default); Codec Piroity 9: 1~9</p> <p>RTP Packet Length:</p> <p>G711G729pkl=2(Default); G.711 & G.729: 1~9 (1:10ms, 2:20ms, 3:30ms, 4:40ms, 5:50ms, 6:60ms, 7:70ms, 8:80ms, 9:90ms)</p> <p>G723pkl=3(Default); G.723: 1, 2, 3 (1:30ms, 2:60ms, 3:90ms)</p> <p>G723Enable=0(Default), G.723 5.3K: 0~1 (0:Off, 1:On)</p> <p>VoiceVADEnable=0(Default); Voice VAD: 0~1 (0:Off, 1:On)</p>
\$DTMF Setting DTMF=0	<p>Description:</p> <p>DTMF=0(Default); DTMF: 0~2 (0:2883, 1:Inband, 2:Send DTMF SIP Info)</p>
\$RPort Setting ph1RportEanble=1 ph2RportEanble=1	<p>Description:</p> <p>ph1RportEanble=1(Default); (Phone1) Rport: 0~1 (0:Off, 1:On)</p> <p>ph2RportEanble=1(Default); (Phone2) Rport: 0~1 (0:Off, 1:On)</p>
\$Other Settings ph1HoldRFCEnable=0 ph2HoldRFCEnable=0 VoiceQoS=40 SIPQoS=40 SIPExpireTime=60	<p>Description:</p> <p>ph1HoldRFCEnable=0(Default); (Phone1) Hold by RFC: 0~1 (0:off, 1:On)</p> <p>ph2HoldRFCEnable=0(Default); (Phone1) Hold by RFC: 0~1 (0:off, 1:On)</p> <p>VoiceQoS=40(Default); Voice Qos (Diff-Serv): 0~63</p> <p>SIPQoS=40(Default); SIP Qos (Diff-Serv): 0~63</p> <p>SIPExpireTime=60(Default); SIP Expire Time: 30~86400 sec</p>
\$NAT Trans function: \$STUN Setting ph1STUNEnable=0 ph2STUNEnable=0 STUNServ=stun.xten.com STUNPort=3478	<p>Description:</p> <p>ph1STUNEnable=0(Default); (Phone1) STUN: 0~1 (0:off, 1:On)</p> <p>ph2STUNEnable=0(Default); (Phone2) STUN: 0~1 (0:off, 1:On)</p> <p>STUNServ=stun.xten.com(Default); STUN Server: ipaddress or domain address <maxlength=63></p> <p>STUNPort=3478(Default); STUN Port: 1024~65535</p>
\$Others function: \$FXS/FXO Port Setting → FXS/FXO use FXSCountry=63 FXOCountry=63	<p>Description:</p> <p>Country: 00:Argentina, 01:Australia, 02:Austria, 03:Bahrain, 04:Belgium, 05:Brazil, 06:Bulgaria, 07:Canada, 08:Chile, 09:China, 10:Colombia, 11:Czech Republic, 12:Denmark, 13:Ecuador, 14:Egypt, 15:El Salvador, 16:Finland, 17:France, 18:Germany, 19:Greece, 20:Hong Kong, 21:Hungary, 22:Iceland, 23:India, 24:Indonesia, 25:Ireland, 26:Israel, 27:Italy, 28:Japan, 29:Jordan, 30:Kazakhstan, 31:Kuwait, 32:Latvia, 33: Lebanon, 34:Luxembourg, 35:Macao, 36:Malaysia, 37:Mexico, 38:Morocco, 39:Netherlands, 40:New Zealand, 41:Norway, 42:Oman, 43:Peru, 44:Philippines, 45:Poland, 46:Portugal, 47:Romania, 48:Russia, 49:Saudi Arabia, 50:Singapore, 51:Slovakia, 52:Slovenia, 53:South Africa, 54:South Korea, 55:Spain, 56:Sweden, 57:Switzerland, 58:Taiwan, 59:TBR21, 60:Thailand, 61:UAE,</p>

	62:United Kingdom, 63:USA FXSCountry =63(Default); FXS Port: 00~63 FXOCountry =63(Default); FXO Port: 00~63
\$Advanced Setting CPCDelay=2 CPCDuration=50 SendFlashEvent=0 SIPRTPEncrypt=0	Description: CPCDelay =2(Default); CPC Delay: 2~5 seconds → for fxs port CPCDuration =50(Default); CPC Duration: 0~60 (x10ms) → for fxs port SendFlashEvent =0(Default); Send Flash event: 0~2 (0:Disabled, 1:DTMF EVENT, 2:SIP INFO) SIPRTPEncrypt =0; SIP Encrypt: 0~4 (0:Disabled, 1:INFINET, 2:AVS, 3:WALKERSUN1, 4:WALKERSUN2)
\$System Auth Function: \$System Authority Setting AdminUserName=root AdminUserPass=test NormalUserName=user NormalUserPass=test	Description: AdminUserName =root(Default), Administrator User Name <maxlength=63> AdminUserPass =test(Default), Administrator user Password <maxlength=63> NormalUserName =user(Default), Normal user Name <maxlength=63> NormalUserPass =test(Default), Normal user Password <maxlength=63>
\$Auto Provision & Update Function: \$AutoProvision Setting AutoConfigMode=0 TFTPServer= HTTPServer= HTTPPath= FTPServer= FTPUserName= FTPPassword= FTPPath=	Description: AutoConfigMode =0(Default); Auto Configuration: 0~3 (0:Off, 1:TFTP, 2:FTP, 3:HTTP) TFTPServer =; TFTP Server: ipaddress <maxlength=63> HTTPServer =; HTTP Server: ipaddress or domain address <maxlength=63> HTTPPath =; HTTP File Path: /File Path name/ <maxlength=63> FTPServer =; FTP Server: ipaddress or domain address <maxlength=63> FTPUserName =; FTP Username: Login FTP Server User name <maxlength=63> FTPPassword =; FTP Password: Login FTP Server User Password <maxlength=63> FTPPath =; FTP File Path: /File Path name/ <maxlength=63>
\$AutoUpdate Setting AutoUpdateMode=0 UTFTPServer= UHTTPServer= UHTTPPath= UFTPServer= UFTPUserName= UFTPPassword= UFTPPath= AutoUpdateCheckVer=1	Description: AutoUpdateMode =0(Default); Update via: 0~3 (0:Off, 1:TFTP, 2:FTP, 3:HTTP) UTFTPServer =; TFTP Server: ipaddress <maxlength=63> UHTTPServer =; HTTP Server: ipaddress or domain address <maxlength=63> UHTTPPath =; HTTP File Path: /forder name/ <maxlength=63> UFTPServer =; FTP Server: ipaddress or domain address <maxlength=63> UFTPUserName =; FTP Username: Login FTP Server User name

AutoUpdateDay=14 AutoUpdateTime=0 AutoUpdateNow=0 AutoUpdateFilePrefix=	<maxlength=63> UFTPPassword=; FTP Password: Login FTP Server User Password <maxlength=63> UFTPPath=; FTP File Path: /forder name/ <maxlength=63> AutoUpdateCheckVer=1(Default); Check new firmware: 0~1 (0:Power On, 1:Scheduling) AutoUpdateDay=14(Default); Scheduling (Date): 1~30 AutoUpdateTime=0(Default); Scheduling (Time): 0~3 (0:AM 00:00-05:59, 1:AM 06:00- 11:59, 2:PM 12:00- 17:59, 3:PM 18:00- 23:59) AutoUpdateNow=0(Default); Automatic Update: 0~1 (0:Notfiy only, 1:Automatic) AutoUpdateFilePrefix=Product name(Default); Firmware File Prefix: name <maxlength=8>
\$Version (Keyword) AutoConfigVersion=1	Description: AutoConfigVersion=1(Default) <maxlength=3>
ICMPE=0	Description: ICMPE=0(Default) Active: 0~1 (0:Off, 1:On)