ICW-1000 Global

Admin's Manual

Rev; 1. 0. 3

INCOM Co., Ltd.

www.incominc.com

Copyright Notice

Information furnished herein by INCOM Co., Ltd., is believed to be accurate and reliable. The authors have used their best efforts in preparing this material. These efforts include the development, research, and testing of the theories and programs to determine their effectiveness.

However, INCOM assumes no liability for errors that may appear in this document, or for liability otherwise arising from the application or use of any such information or for any infringement of patents or other intellectual property rights owned by third parties which may result from such application or use. The products, their specifications, and the information appearing in this document are subject to change without notice.

Manual Introduction

Before use, kindly read this “Administrator Manual” thoroughly to have an understanding of the contents

After reading, place it within reach at all times such as at the side of this product.

This manual is for administrator who has working knowledge of fundamental terms and concepts of computer networking, converged voice and data networks to include LANs, WANs, and IP switching and routing.

Safety Precautions

Since this is provided to make safe and right use of ICW-1000G to prevent any accidents or risks, be sure to carefully read it, follow instructions, and keep it where it is easily noticed.

Warning

This mark is intended to warn users of the risk of a serious injury or death when they violate instructions.

 Do not put ICW-1000G in heating appliances such as heaters and microwave ovens to dry them if they are wet. It can cause explosions, deformation, or troubles. In this case, free services shall not be provided.

 Do not use ICW-1000G in places that are too hot or too wet (keep them indoors between 0 ℃ and + 50 ℃). If they get wet with rain, have drinks spilled, or are used in extremely hot/wet places such as public sauna bathroom, it can cause battery explosions.

 Put ICW-1000G and chargers in places out of reach of children or pets. If one puts batteries his or her mouth, or uses broken batteries, it can hurt his or her body, or cause electric shocks.

 Do not disassemble ICW-1000G, or apply shocks to them as you please. If they get damaged while you disassemble them, or inflict shocks on them, you cannot have free services.

 You should stop charging the phone and separate it from battery if the phone is overheating during charging the phone. Doing so may get burned.

 Be aware of much ESD (Electrostatic Discharge simulator) environment. The product may have the abnormal condition

 Be sure to use designated batteries and accessories only for ICW-1000G provided by our company. If you use unauthorized batteries or accessories, it can reduce the life of ICW-1000G, cause explosions, or damage them. In this case, you cannot have free services.

 Be careful for conductors such as necklaces, keys, and coins not to contact battery terminals (metal section). Since short circuits can cause explosions, be careful for such events never to take place.

 Neither throws batteries, which can inflict shocks on them, nor put them near to heating appliances such as heaters and microwave ovens. It can cause the leak of battery contents, or explosions.

 Use standard chargers that obtained INCOM authentication for batteries. Otherwise, batteries will have their life reduced, face explosions, or damage ICW-1000G. In this case, free services shall not be provided.

 Refrain from the use of ICW-1000G, and leave the power cord of chargers unplugged when thunders and lightening are severe. Thunderbolts can cause severe physical injuries, or fires.

 Do not hold ICW-1000G to your ears to turn on the power. It can cause hearing impairments, or physical injuries. Do not look at the infrared window in a direct way when using remote control. It can cause visual impairments.

 Do not use chemical detergents such as benzene, thinner, and alcohol to clean ICW-1000G. It can cause fires.

 Never push the power button when ICW-1000G are wet, nor touch ICW-1000G, chargers, or power cords with wet hands. It can cause fires or electric shocks.

 Precautions

This mark is intended to caution users against violating instructions since it can cause a slight physical injury or product damage.

 Correctly install ICW-1000G in compliance with instructions. Otherwise, it can cause an abnormal operation of ICW-1000G, or reduce their life.

 Be aware of radio interference. Since this radio equipment can have radio interference, services related to life safety are not provided.

 Do not install ICW-1000G in places exposed to direct sunlight, and on carpets or cushions. It can cause fires or troubles.

 Do not install ICW-1000G in narrow places with poor ventilation, or near heat sources. It can cause fires or troubles.

 Do not install ICW-1000G in places with much dust. It can cause operational problems, or reduce phone life.

 Install ICW-1000G on flat places, not on shelves or slopes. Otherwise, it can hurt you, or cause troubles when they drop.

 Since emergency calls are available only within call coverage, check in advance whether or not calls are available.

 Do not use ICW-1000G covered wrap or vinyl. Coating can be removed.

 Record and keep the information contained in ICW-1000G separately.

Since the important information stored in ICW-1000G can be removed due to unavoidable circumstances such as users' carelessness, maintenance, and product upgrade, please keep a record of important information. Take note that manufacturer will not take responsibility for any damage from the loss of information. If batteries are not used for a long time, keep them at room temperature after charging.

If you want to use again after leaving them for a long time, it is recommended to use them after fully charging.

Keep in mind that ICW-1000G can produce much heat while using for a long time.

Do not install ICW-1000G in heavily shaking places. It can cause performance degradation, or reduce the life of products.

After using ICW-1000G for a long time, they can produce a weak sound due to their liquid crystal protective vinyl covering the speaker.

If ICW-1000G is separated from AP or chargers for a long time, they cannot work due to battery discharge.

Contents

ICW-1000G at a Glance

Basic Key Function

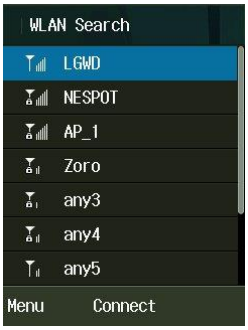
Key Name	Icon	Basic functions
Navigation key		Navigation Key – In the idle state, this button opens each function. Within a menu or a list, you can use this as direction keys.
Left selection key Right selection key		Left selection key – Search WLAN key / Scroll up in the menu list. Right selection key – Search grouped phone book.
Send key		Equivalent to “Answer” on a standard phone and “hold” during a call.
End key		Equivalent to “hang up” on a standard phone. Return to idle state. Pressing and holding the key in the idle state turns the handset On/Off.
OK key		Confirmation(OK), Select, View, Connect on each display screen
Search phonebook key		Search phonebook, trace call history and storage phonebook/ Scroll up in the menu list
Alarm key		Setting up alarm and wakeup call / Move to left in the menu.
My menu key		Set phone settings / Scroll down in the menu list
Message key		Using message function/ Move to right in the menu.
Speaker key		Using speaker function
Mute key		Mute key is used when calling on the phone. Pressing the key during a call turns “Mute” mode.
Vibration key		Pressing and holding the key in the idle state: Switch the ringer (buzzer) On/Off
Clear key		CLR Key is used to return to previous menu list. Cancel (ESC) and removing characters.
Lock key		The pound is for entering the pound sign. Pressing and holding the key in the idle state: Switches on the key lock.

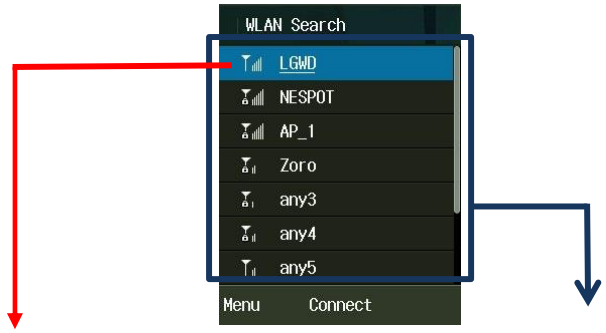
Admin Menu and Changing Password

2

1	Press the down key ▼ on navigation and directly access “Phone setting”.	
2	Press “8” or find “Admin. Menu” with scroll down.	
3	Default administrator password is 000000 and user password is 0000	
4	Administrator can only change the Administrator password and User password. To change Password, select “Admin Password” or “User Password”	

Searching an available Access Point

1.	Press ● L -> shortcuts to search an available Wi-Fi Access Points	
2.	Select an access point from the list that you will connect then press OK.	
3.	If you using password for connect to AP then select configuring security as 64-bits WEP and Enter the password into line number 1, then press OK. Select authentication and network type then press OK. Please refer to Configuring Security (p.15 Configuring Security and Authentication)	

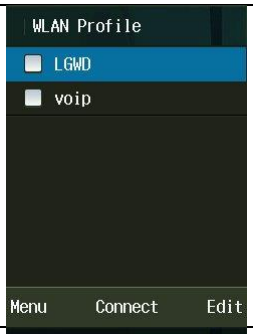


Registered or added AP
(Default Registered AP is VoIP.)

Search results of AP

Creating a new Access Point

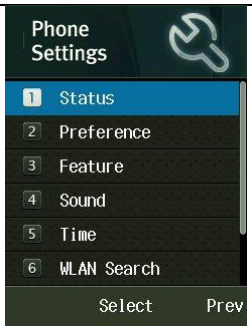
If there is no AP that you're connecting for from the list, you can refresh the search or add access point.

1.	Press the down key on navigation and directly access "Phone setting".	
2.	Press "1" or find "Status" with scroll down.	
3.	Press "2" or find "WLAN Profile" with scroll down.	
4.	You can input the special characters as well. Press left selection key L and select symbol. To change Alphanumeric to numeric, press the right selection key R.	
5.	L "Menu" and "1. Add Profile" using with navigation or press "1"	

6.	Enter SSID, security and authentication type of access point. If 4 Access Points are saved already, it is not able to add.	
7.	Enter network type of Wi-Fi access point. Please refer to Security and TCP/IP chapter (p.17 TCP/IP)	

Deleting Registered Access Point

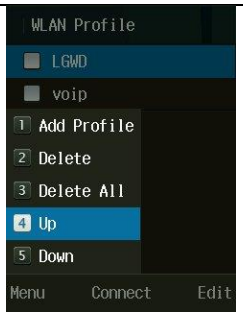
ICW-1000G supports to delete saved Access Point. In WLAN search mode, select Menu then 4.Delete to remove Wi-Fi Access Point. After confirm with entering administrator password, select “Yes”, it will be deleted.

1.	Press the down key ▼ on navigation and directly access “Phone setting”.	
2.	Press “1” or find “Status” with scroll down.	
3.	Press “2” or find “WLAN Profile” with scroll down.	
4.	● L “Menu” and “3. Add Profile” using with navigation or press “3”	
5.	Press OK then Delete All WLAN Profile	

Changing Priority Access Point

The higher position of Access Point in the registered screen has higher priority when connect automatically

→ 1. Status → 2. WLAN Profile.

1.	Select the Access Point from the registered list that you want to change priority, press Left selection key L then select Up or Down in menu to change the position for priority. Default Access Point "VoIP" can be changed by the Auto-provisioning configuration only	

Configuring Security

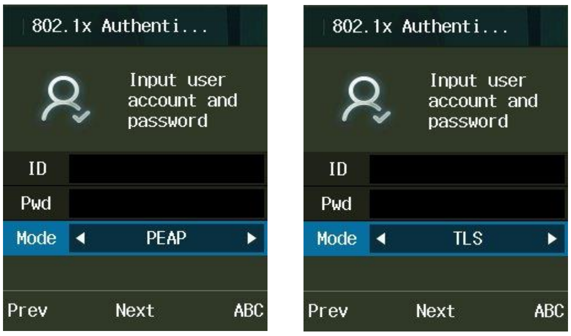
While creating a new access point or edit existing access point, security option can be set.

For setting up the type of security, press R as "add" at WLAN Search screen when you're sure to setting the type of security. ICW-1000G supports various types of security 64-bits WEP, 128-bits WEP, WPA-PSK, WPA2-PSK, WPA-EAP, WPA2-EAP and Dynamic WEP.

If your AP does not necessary to these kinds of security, this procedure can be passed.

Authentication

If you and your Access Point are using 802.1x authentication then select “Yes” to configure. Enter your ID and Password for authentication and select your types of authentication among the mode list.



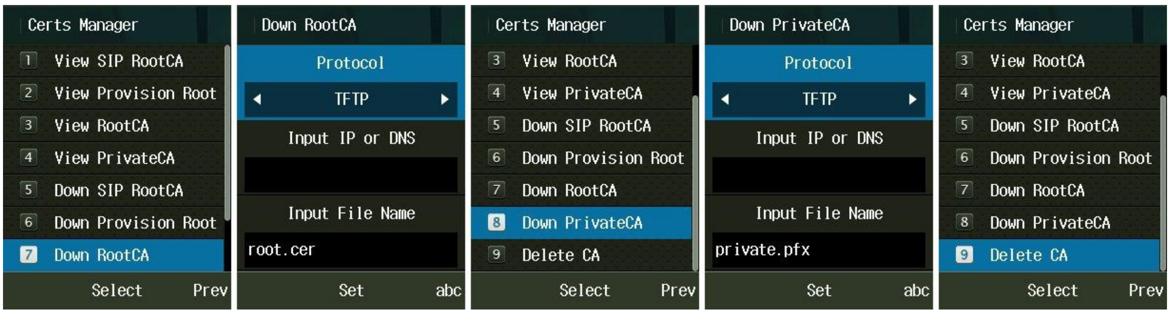
Certification Manager

In case of EAP-TLS, Select “Certs manger” in administrator menu.

→ 8. Admin Menu → Enter Password → 5. Certs Manager

SIP Root certificate	Supporting .der, .cer and .pem Encode system
Provision Root certificate	Supporting .der, .cer and .pem Encode system
Root certificate	Supporting .der, .cer and .pem Encode system
Private certificate	Supporting .pfx and .p12 Encode system

Reference and download of the Root CA and Private CA are possible in order to use 802.1x (EAP-TLS, PEAP, TTLS). You can select which of TFTP, HTTP or HTTPS as a download system.

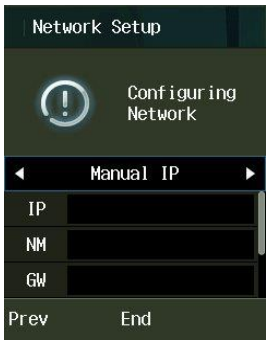


Certificate will be deleted when select “Delete CA”

TCP/IP

ICW-1000G supports DHCP and manual IP. You can select “DHCP” automatically or “Manual IP” manually to configuring network at WLAN Search screen.

IP, Net mask, Gateway and DNS should be entered in case of using manual IP in network setup.



OpenVPN

ICW-1000G supports OpenVPN.

Generating certificate files for the OpenVPN server and ICW-1000G(linux)

1. Install OpenVPN package and easy-rsa
   # sudo apt-get install openvpn
   # sudo apt-get install easy-rsa
2. Edit vars. The variables to edit are:

```
# Don't leave any of these fields blank.
export KEY_COUNTRY="KR"
export KEY_PROVINCE="NA"
export KEY_CITY="Seoul"
export KEY_ORG="Incom"
export KEY_EMAIL="me@incominc.com"
export KEY_OU="MyOrganizationalUnit"

# X509 Subject Field
export KEY_NAME="server"
```

3. Make certificate for the server and client
   # cd /etc/openvpn/easy-rsa/
   # source vars
   # ./clean-all
   # ./build-ca
   # ./build-key-server server
   # ./build-key client
   # ./build-dh

Configuring Server

Uploading the OpenVPN zip file for the VPN client on ICW-1000G

OpenVPN requires using certificates to establish the authenticity of clients connecting to an OpenVPN server. You need to upload the files: ca.crt, client.crt, client.key and client.conf.

1. Create a new directory client
   # mkdir /etc/openvpn/client
2. Copy the certificate files required for the client
   # cp easy-rsa/keys/ca.crt /etc/openvpn/client
   # cp easy-rsa/keys/client.crt /etc/openvpn/client
   # cp easy-rsa/keys/client.key /etc/openvpn/client
3. Copy the file “client.conf” in the sample-config-files directory
   # cp sample-config-files/client.conf /etc/openvpn/client
4. Edit the “client.conf”. Following figure shows the client.conf for reference

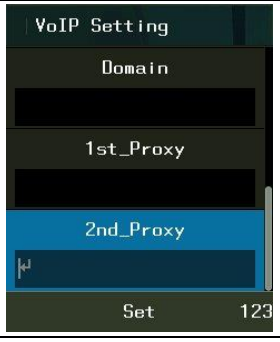
5. Make a zip file
   # zip client.zip *
6. Upload the “client.zip” via Web Interface

Enable the OpenVPN

You can enable the OpenVPN via Admin Menu
Phone Settings > Admin. Menu > OpenVPN

SIP Setting

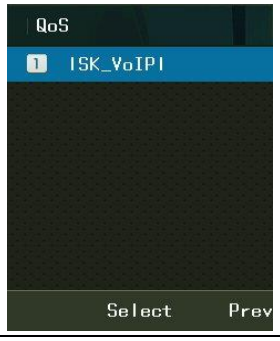
▼ → 8. Admin Menu → Enter Password → 2. VoIP Setting.

1	Select “2.VoIP setting” in System mode	
2	Display name: type the display name of phone User name: type phone number or user name registered in SIP. Auth. User name: User ID for SIP Proxy	
3	Auth. Password: User Password for SIP Proxy Domain: Domain Server	
4	If you have secondary or backup proxy server, you can also input IP address in 2nd_Proxy section. ⚠ In Domain section, you should put the domain name server only if SIP header includes Domain Name.	

QoS

Qos: Quality of Service

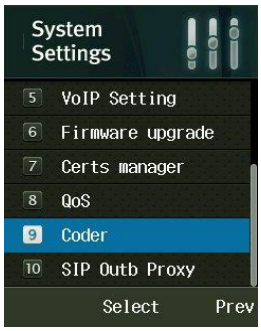
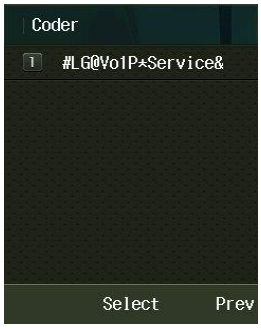
→ 8. Admin Menu → Enter Password → 8. QoS → VoIP .

1	Select “8.QoS” in System menu	
2	Select “VoIP” in QoS menu	
3	Enter Signal DSCP and Voice DSCP.	

Coder

▼ → 8. Admin Menu → Enter Password → 9. Coder → 1. VoIP .

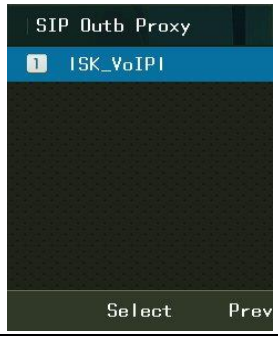
ICW-1000G supports G.711-ALaw-64K, G.729 and G729-uLaw-64K.

1	Select “9. Coder” in System menu	
2	Select “VoIP” in Coder menu	
3	Press the OK key to set Multi-frame. Select the coder type you wish to set.	 
4	Press ● L in VoIP mode to set the priority then select Up or Down in menu list to change the position for priority. Set the priority order of audio coder.	

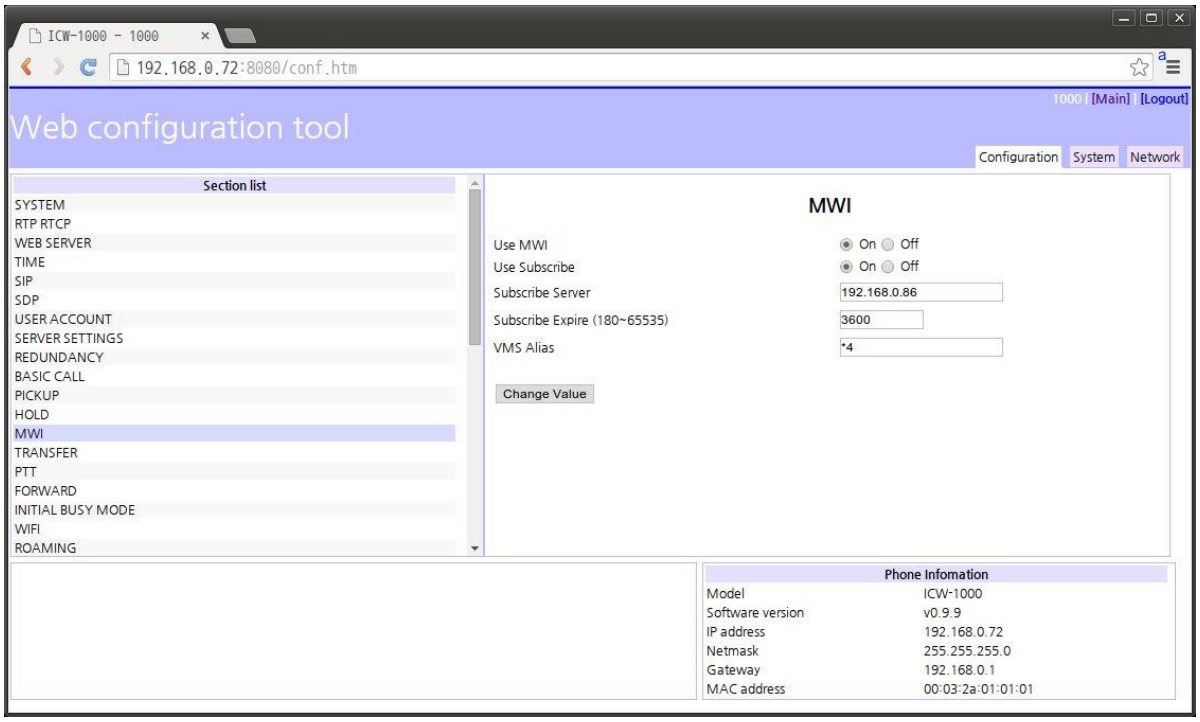
SIP Outbound Proxy

 → 8. Admin Menu → Enter Password → 10. SIP Outb Proxy → 1. VoIP .

1	Select “10. SIP Outb Proxy” in System menu.	
2	Select “VoIP” in SIP Outb Proxy menu	
3	Put the SIP Outbound Proxy.	

MWI(Message Waiting Indicator) settings can be done through Web Interface(PC-Sync).

- Set ‘on’ Use MWI (default value is on)
- Set ‘on’ Use Subscribe (default value is off)
- Set Subscribe Server (Usually 1st Proxy Server IP address)
- Set VMS Alias (Voice Message check dial code)



Or setting can be done by provisioning. Set MWI section in e1_common.ini file like below example.

[MWI]

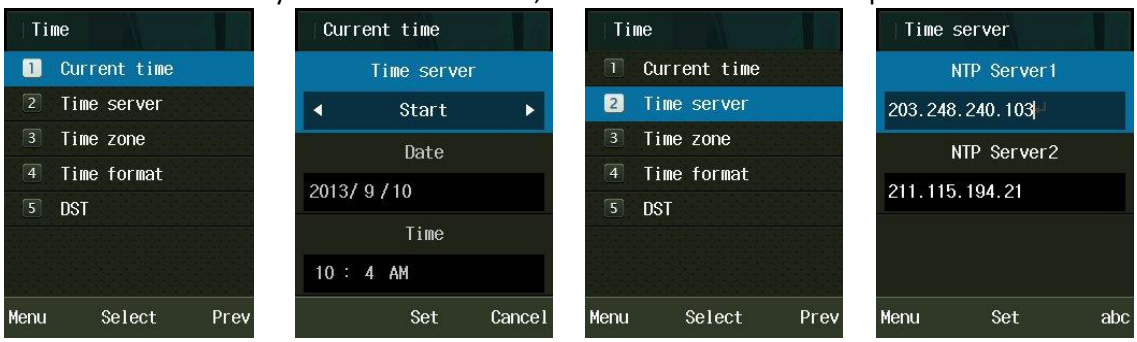
Use_MWI = 1
Use_Subscribe = 1
Subscribe_Server = 192.168.0.86
Subscribe_Expire = 3600
VMS_Alias = *4

TIME

→ 5. Time

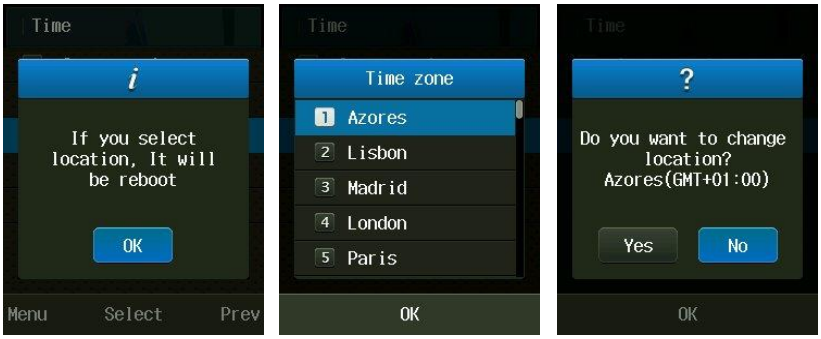
You can set the date and time automatically and manually.

To set Current time automatically select Current time > Time Sever > Start otherwise must set current time manually. To use NTP server, select Time server and Input the NTP IP in NTP Server1 and Server2.



⚠ We strongly recommend using NTP server. It would be re-set the time after reboot if you don't use NTP server.

ICW-1000G supports 52 0f principal capital cities in the world time. To setup the Time zone service, select 3.Time Zone and select your location of GMT.

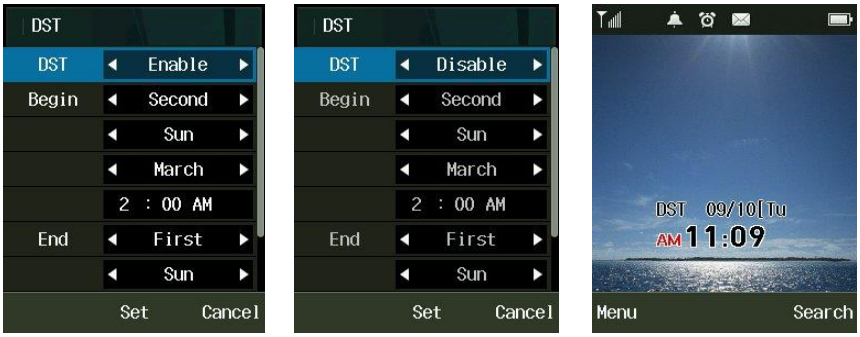


Finally the phone will be rebooted.

To define the Daylight Saving Time, select DST and choose Disable or Enable.

After set Start time, the End time should be settled by time which is applied DST time.

After set DST time will be displayed on the screen.

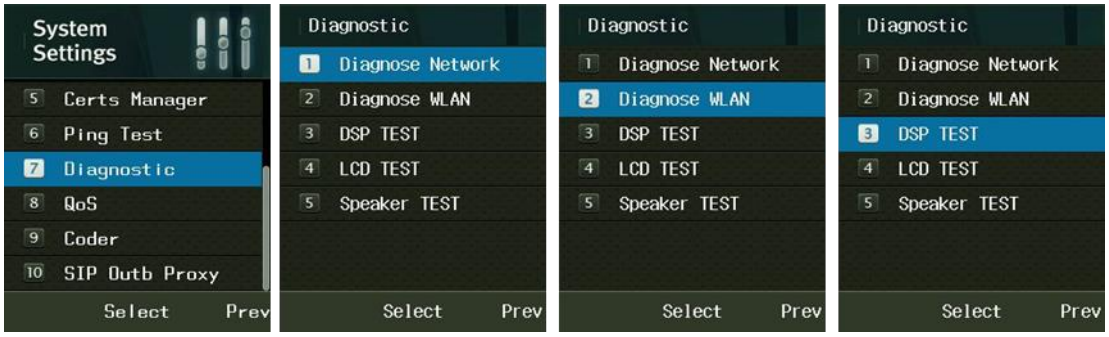


Diagnostic

6

Diagnose Network

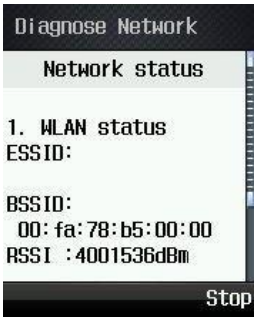
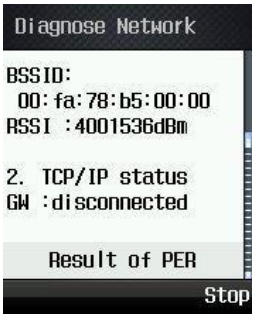
▼ → 8. Admin Menu → Enter Password → 7. Diagnostic → 1. Diagnostic Network. And then select Diagnose Network, WLAN to diagnostic that you need.



Results of Diagnose Network

It shows Network Status as WLAN, TCP/IP, and Packet Error Rate between Gateway and DNS.

It takes about three to five seconds to finish all the processes, and all input key shall be inactive until finish the diagnose network.

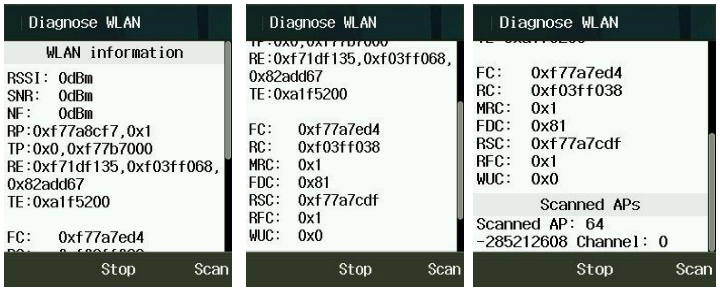
Diagnose Network explanation WANN status (Connection of wireless LAN) ESSID: Present-connected SSID of AP BSSID: Present-connected MAC Address of AP RSSI: Received Signal Strength Indication from the AP present- connected	
Result to PER (Ping Error Rate) PER to GW: packet error rate to GW. PER test to Gateway (ping to GW per 20ms period, 100 units) PER to DNS: ping error rate to DNS. PER test to DNS1 (ping to DNS1 per 20ms period, 100 units)	

Diagnose WLAN

→ 8. Admin Menu → Enter Password → 7. Diagnostic → 2. Diagnostic WLAN .

While diagnose WLAN, cannot receive the call while scan WLAN network.

Results of the Diagnose WLAN



The diagnosis of wireless communication surroundings is possible to find out the connection from ICW-1000G to AP, the units of AP around and inside of the present-connected channel, and variables of the surroundings through diagnosing the status of wireless local area

Each output information is automatically updated once per one minute, AP status around can be updated pressing on the soft key (searching). Automatic update of AP around net-time is not recommended, but need to press on the button when needed, because frequent updating by scanning could give bad influence, when engaged

Each information unit is, except for dBm, is (RSSI/SNR/NF) hexadecimal of them.

RSSI: Received Signal Strength Indication (dBm)

SNR: Signal to Noise Ratio (dBm)

NF: Noise Floor (dBm)

RP: Rx Packet Count/Rx Bytes

TP: Tx Packet Count/Tx Bytes

RE: Rx Error Count/Rx Dropped Count/Rx Length Error Count TE: Tx Error Count/Tx Dropped Count

FC : Tx Failed Count - Increments when a MSDU is not successfully transmitted

RC : Retry Count - Increments when a MSDU is successfully transmitted after one or more retransmissions

MRC : Multiple Retry Count - Increments when a MSDU is successfully transmitted after more than one retransmission

FDC : Frame Duplicate Count - Increments when a frame is received that the Sequence Control field is indicating a duplicate count

RSC : RTS Success Count - Increments when a CTS is received in response to an RTS

RFC : RTS Failure Count - Increments when a CTS is not received in response to an RTS

AFC : Ack Failure Count - Increments when an Ack is not received when expected

FEC : FCS Error Count - Increments when a FCS error is detected in a received MPDU

TFC : Transmitted Frame Count - Increments for each successfully transmitted MSDU

WUC : WEP Undecryptable Count - Increments when a frame is received with the WEP subfield of the Frame Control filed set to one The WEP On value for the key mapped to the TA's MAC address indicates that the frame is not encrypted or frame is discarded because the receiving station is not implementing the privacy option

Scanned AP

Scanned AP: Searched units of AP around.

0 channel: AP units of present-associated channel

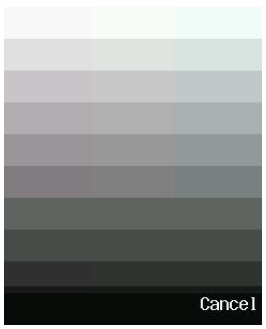
DSP Test

→ 8. Admin Menu → Enter Password → 7. Diagnostic → 3. DSP Test

1	Select “3. DSP TEST” in Diagnostic mode.	
2	Using key for controlling receiver volume.	

LCD Test

→ 8. Admin Menu → Enter Password → 7. Diagnostic → 4. LCD Test

1	Select “4.LCD TEST” in Diagnostic mode.	
2	Using key for controlling display.	

Speaker Test

- → 8. Admin Menu → Enter Password → 7. Diagnostic → 5. Speaker Test

1	Select “5. Speaker TEST” in Diagnostic mode.	
2	Using ▲ ▼ key or ● L key for controlling test mode.	

Ping Test

8. Admin Menu → Enter Password → 6. Ping test → 5. Speaker Test

1	Select “6. Ping test” in System menu. Ping Test is accessible for simple diagnosis of network.	
2	Select “1.Gateway, 2 . DNS server, 3 . APS address or 4 . Manual input” in Ping test mode.	

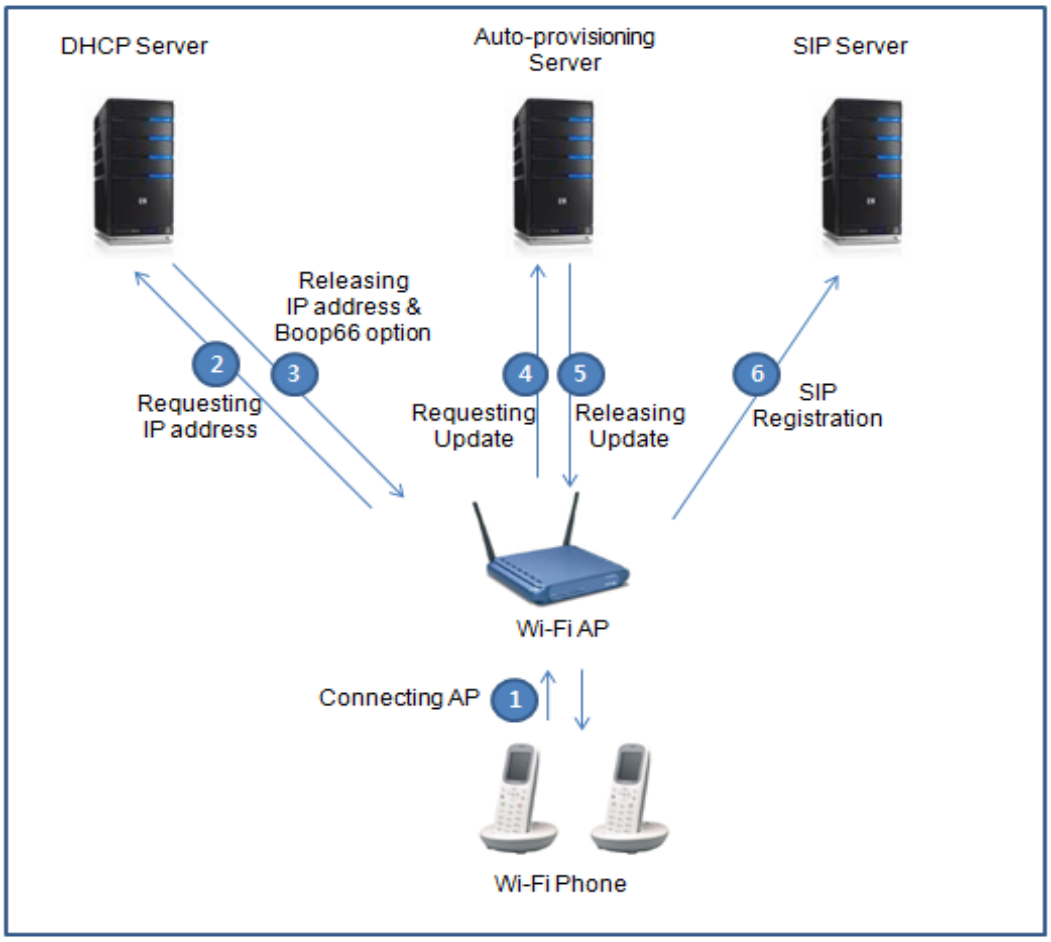
3	Send the ping through the Gateway, DNS server, APS address and Manual input. DNS server APS server Manual Input	   

Auto-Provisioning Guide

7

General Sequence of Auto-provisioning

ICW-1000G supports Auto-provisioning to configure update firmware. Below picture is interoperation between phone and servers.

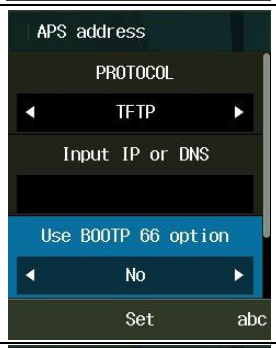


① VoIP phone connect to the nearest Wi-Fi Access Point.
② Phone request IP address to the registered DHCP server
③ DHCP server provide phone with IP address and Boot 66 option which indicate Auto provisioning server.
④ Phone connect Auto-provisioning server
⑤ Auto-provisioning server compare version of e1_common.ini and e1_mac.ini with phone and if server has higher version, phone started to download firmware files from server.
⑥ Phone connect SIP server and register IP address.

⚠ Please refer to Setting the .ini file in Auto-provisioning server.

Setting Auto provisioning Server Address

There are two way to set Auto provisioning Server address. The first one is input address in menu via the key pad; another one is getting the address by DHCP server with the bootp option 66.

1	Select “3. APS address” in System Settings’ menu.	
2	To set the address in manually, choose APS address in the administrator menu. Three protocols, HTTP, HTTPs and TFTP are available. Please make sure USE BOOTP 66 option is NO when using in manually setting the address.	
3	To set the address by DHCP BOOTP 66 option, please make empty in the input IP or DNS field. Make USE BOOTP 66 option filed to YES. ICW-1000G will get configuration file from auto-provisioning server in the next boot up.	

Setting Encrypted e1_mac.ms

To prevent hi-jacking account information during provisioning ICW-1000 serves the encrypted e1_mac.ms

① Prepare e1_common.ini, e1_mac.ini.

② Make e1_common.ini setting as follows

[PROVISION]

Use_Encrypt_On_MAC_Ini = 1

③ Encrypt e1_mac.ini file using qenc-ini.exe. (provided by INCOM)

Usage.

qenc-ini.exe e1_mac.ini e1_mac.ms (encrypted file’s extension should be .ms)

④ Upload e1_common.ini, e1_mac.ms to provisioning server

Setting the .ini file in Auto-Provisioning Server

You use the value of two Statements after modifying according to each condition.

Make sure that sever IP will be root directory of auto-provisioning server.

You can use the “e1_Common.ini” file if you want to set the all the same value.

You can use the “e1_000000000000(replace your phone mac).ini” file if you want to set different value individually.

(In every line’s # means just comment of value. You don’t need to apply it to each line.)

e1_Common .ini

[SYSTEM]

Language = 1

Admin_Password = 000000

Country_Tone_Type = 1

[RTP_RTCP]

Use_RTCP = 1

RTP_Port_Min = 9000

RTP_Port_Max = 9020

RTCP_Report_Interval = 5000

Last_RTP_Received_Timeout = 0

[TIME]

NTP_Refresh_Interval = 7200

NTP_Server1 = 203.248.240.103

NTP_Server2 = 203.254.163.74

[SIP]

Local_Port = 5060

[BASIC_CALL]

Use_Call_Waiting = 1

Session_Expire = 1800

Remove_DASH_On_Alias = 1

[MWI]

Use_MWI = 1

Use_Subscribe = 1

Subscribe_Server =

Subscribe_Expire = 3600

VMS_Alias =

[WIFI]

Enable_Check_Server_Cert = 0

Force_Enable_Short_Preamble = 0

[WIFI_SCAN]

Scan_Channel_List = 1,2,3,4,5,6,7,8,9,10,11,12,13

[ROAMING]

Try_Beacon_Signal_Level = -77

Try_Over_TxError_Count = 5

[NETWORK1]

Enable = 1

SIP_Outbound_Proxy = SSID

= VoIP

Enable_DHCP = 1

Address = 0.0.0.0

Netmask = 255.255.255.0

Gateway = 0.0.0.0

DNS1 = 0.0.0.0

DNS2 = 0.0.0.0

Security = 2

WEP_Bits = 0

Default_WEP_Key = 1

WEP_Key1 = WEP_Key2

= WEP_Key3 =

WEP_Key4 =

Post_Authentication_Mode = 0

8021X_Name =

80121X_Password =

WPA_PSK_PassPhrase = un1d4t4wpu7700

WPA_PSK_Key=5ae4b848d871fdcba8dda23716245901b0e5ea8047b06e4445e94d96ec27ee23

Use_WPA_PSK_Key_Hex_Mode = 1

Proactive_Key_Caching = 1

PMK_LifeTime = 43200

PMK_Max_Count = 32

DiffServ_Signal = 46

DiffServ_Media = 46

WMM = 1

Jitter_Buffer_Size = 60

Payload_Type = 8,18,0

Multiframe = 2,2,2

[NETWORK2]

Enable = 0

SIP_Outbound_Proxy =

SSID = wifi

Enable_DHCP = 1

Address = 0.0.0.0

Netmask = 255.255.255.0

Gateway = 0.0.0.0

DNS1 = 0.0.0.0

DNS2 = 0.0.0.0

Security = 1

WEP_Bits = 0

Default_WEP_Key = 1

WEP_Key1 = 123456789a

WEP_Key2 =

WEP_Key3 =

WEP_Key4 =

Post_Authentication_Mode = 0

8021X_Name = 8021X_Password =

WPA_PSK_PassPhrase =

WPA_PSK_Key =

Use_WPA_PSK_Key_Hex_Mode = 1

Proactive_Key_Caching = 1

PMK_LifeTime = 43200

PMK_Max_Count = 32

DiffServ_Signal = 46

DiffServ_Media = 46

WMM = 1

Jitter_Buffer_Size = 60

Payload_Type = 8,18,0

Multiframe = 2,2,2

[NETWORK3]

Enable = 0

SIP_Outbound_Proxy =

SSID = VoIP

Enable_DHCP = 1

Address = 0.0.0.0

Netmask = 255.255.255.0

Gateway = 0.0.0.0

DNS1 = 0.0.0.0

DNS2 = 0.0.0.0

Security = 2

WEP_Bits = 0

Default_WEP_Key = 1

WEP_Key1 =

WEP_Key2 =

WEP_Key3 =

WEP_Key4 =

Post_Authentication_Mode = 0

8021X_Name =

8021X_Password =

WPA_PSK_PassPhrase = un1d4t4wpu7700

WPA_PSK_Key = 5ae4b848d871fdcba8dda23716245901b0e5ea8047b06e4445e94d96ec27ee23
Use_WPA_PSK_Key_Hex_Mode = 1
Proactive_Key_Caching = 1

PMK_LifeTime = 43200

PMK_Max_Count = 32

DiffServ_Signal = 46

DiffServ_Media = 46

WMM = 1

Jitter_Buffer_Size = 60

Payload_Type = 8,18,0

Multiframe = 2,2,2

[NETWORK4]

Enable = 0

SIP_Outbound_Proxy =

SSID = VoIP

Enable_DHCP = 1

Address = 0.0.0.0

Netmask = 255.255.255.0

Gateway = 0.0.0.0

DNS1 = 0.0.0.0

DNS2 = 0.0.0.0

Security = 2

WEP_Bits = 0

Default_WEP_Key = 1

WEP_Key1 =

WEP_Key2 =

WEP_Key3 =

WEP_Key4 =

Post_Authentication_Mode = 0

8021X_Name =

8021X_Password =

WPA_PSK_PassPhrase = un1d4t4wpu7700

WPA_PSK_Key = 5ae4b848d871fdcba8dda23716245901b0e5ea8047b06e4445e94d96ec27ee23

Use_WPA_PSK_Key_Hex_Mode = 1

Proactive_Key_Caching = 1

PMK_LifeTime = 43200

PMK_Max_Count = 32

DiffServ_Signal = 46

DiffServ_Media = 46

WMM = 1

Jitter_Buffer_Size = 60

Payload_Type = 8,18,0

Multiframe = 2,2,2

[SOUND]

Bell_ID = 0x1

Bell_Volume = 6

Effects_Button_ID = 0x00010101

Effects_Button_Volume = 4

Effects_PowerOn_ID = 0x00030001

Effects_PowerOn_Volume = 4

Effects_PowerOff_ID = 0x00040001

Effects_PowerOff_Volume = 4

Info_Battery_ID = 0x00080001

Info_Battery_Volume = 2

Info_Window_ID = 0x00080002

Info_Window_Volume = 2

Info_Network_ID = 0x00080000

Info_Network_Volume = 2

[PROVISION]

Firmware_Version =

Firmware_Name =

Phonebook_Name =

e1_00:00:00:00:00:00(replace you phone MAC).ini(Configuration Entry)

[USER_ACCOUNT]

Displayname =

Phone_Number =

User_ID =

User_Password =

[SERVER_SETTINGS]

1st_Proxy =

2nd_Proxy =

Domain_Realm =

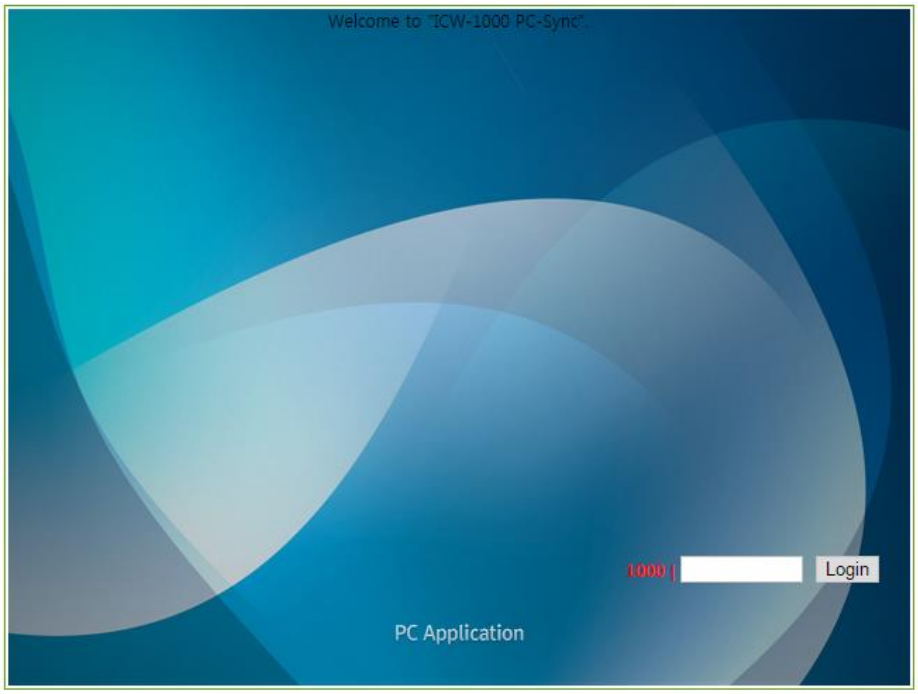
Register_Expire = 3600

Web Configuration Tool

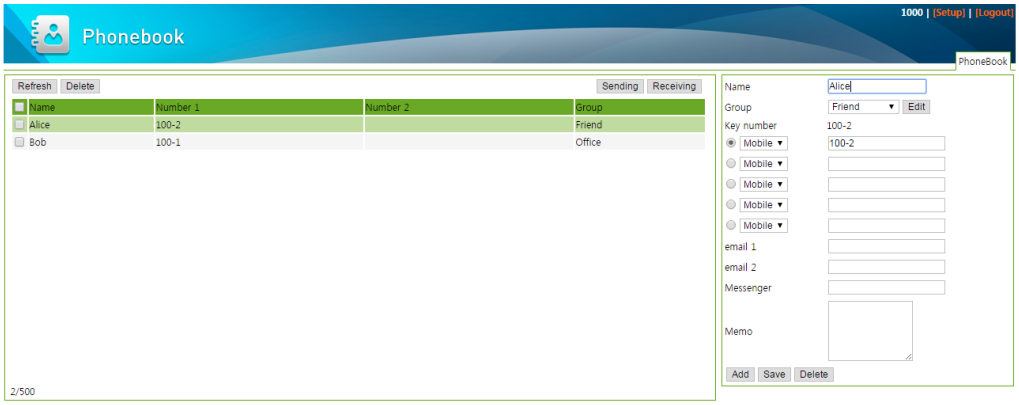
A PC browser can be used as an alternative to configuring system. Ensure that the PC is connected to the same AP as the phone and enable <Lock PC Sync>

Menu > Settings > Preference > Lock PC Sync >Enable > set the password for Web Configuration Tool

1. Enter the phone's IP address:8080 in the address bar of the PC's web browser and press <Enter>

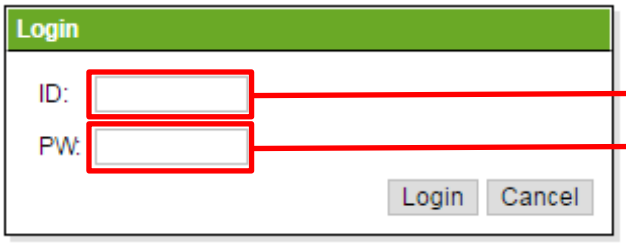


2. Follow screen prompts to enter the password for Web Configuration tool and then click <OK>



3. You can store frequently used phone number and names in the phonebook. You can also import or export saved information between PC and ICW-1000G.

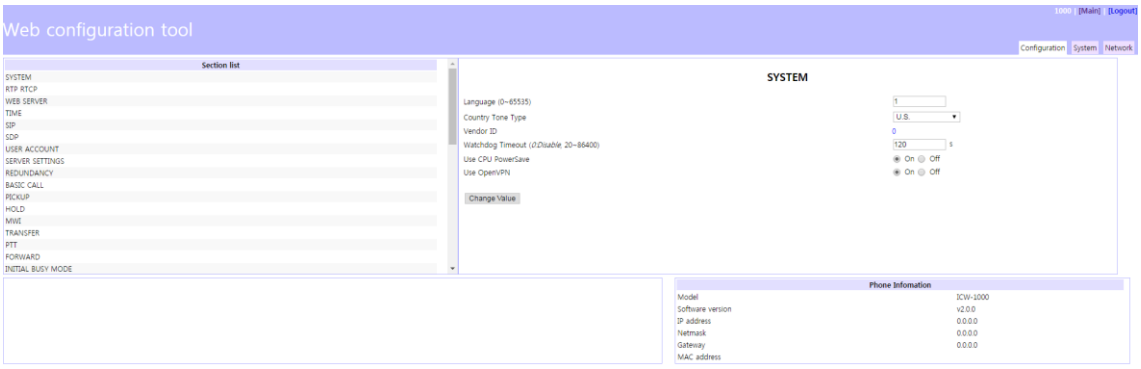
4. After displayed Web Configuration Tool, click <setup> button above the right side.



admin

Password you've set for admin on the phone

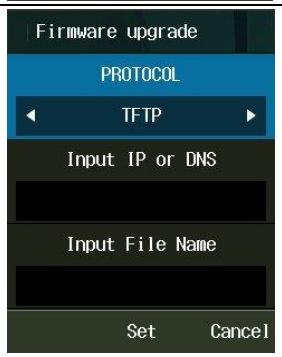
5. Follow screen prompts to enter the user name (admin) and password for admin and then click <OK>



Firmware Upgrade

There are two ways to set Firm ware update. The first one is input address in menu via the key pad; another one is upgraded by Auto-provisioning server automatically.

→ 8. Admin Menu → Enter Password → 4. Firmware upgrade

1	Select “4.Firmware Upgrade” in System Settings’ menu	
2	Select protocol, Enter IP and File name. Enter IP or DNS in “Input IP or DNS” Enter Firmware file name in “Input File Name” i.e Input IP or DNS: 192.168.10.10 Input File Name : example.zip Do not unzip the Firmware zip file which was provided by Unidata. Just load the zip file on the TFTP or HTTP server. The ICW-1000G pulls its configuration and upgrade when you turn the phone off and on. If the original zip file name is too long to input on the phone, you can replace it with simple one like 240.zip	
3	Firmware will be updated. It cannot be upgraded if the Firmware version is same or less than current version. Make sure that the server should be root directory. Don’t tune the phone off during update. Make sure battery is enough. Power off during update will cause phone malfunction.	

Incom Co., Ltd offers Wi- Fi phone and application based on stable VoIP solution technology. Incom which has the advantage of optimal customization for various customers' demands is to enjoy the better convenience of communication technology in both enterprise and home by the field-proven quality with a history for 14 years. We will be active partner of yours to enjoy the most advanced wireless communication technology and to create the higher productivity and value. For more information on Incom and its Wi-Fi solutions, visit **www.incominc.com**

Address: 27-2, Pureundeulpan-ro 567beon-gil, Paltan-myeon, Hwaseong-si, Gyeonggi-do, Republic of Korea

Tel: +82 – 2 – 839 – 7773 (General) / +82 – 70 – 4009 – 4215 (Overseas Sales & Marketing Team)