

IMW-C910W

User Manuel

Table of list

Chapter 1. Attention.....	4
Chapter 2. Introduction & Requirements.....	4
<i>Introduction of goods</i>	4
What is the IMW-C910W?	4
System Requirements.....	4
Specification	4
<i>The points of name & Components list</i>	5
Components List in the package.....	5
Points of name & Function.....	5
Chapter 3. How to use the IMW-C910W.....	7
<i>Power ON/OFF</i>	7
<i>How to charge battery</i>	7
<i>Setting of the WiFi AP</i>	8
Setting with Window XP.....	8
Setting with Window 7	9
Setting with Mac OS.....	9
<i>Setting of USB (RNDIS)</i>	10
Setting with Window XP	10
Setting with Window 7	11
Chapter 4 Configuring CM	12
<i>Connect to Web CM (Web Connection Manager)</i>	12
Start CM	12
Input ID/Password.....	12

<i>Description of Web User Interface</i>	12
Introduction	12
Home Menu	13
<i>LAN settings</i>	15
<i>WiMAX Configuration</i>	18
Parametric Data description.....	18
Network Information description.....	19
Device Information	20
Frequency Setting	20
Authentication Setting.....	21
Administration setting.....	22
Status description.....	22
Firmware information	23
Administration setting.....	23
Upgrade description	24
USB Driver description.....	24
Reboot button description	24

Chapter 1. Attention

- Don't use in high humidity place.
- Use in the clean place.
- Install on the safe place without dropping.
- Don't use and keep around electromagnetic waves.
- Don't put the goods on heavy things.
- Don't install and use in the Sun lights directly.
- Don't throw or dismantle the goods.
- Don't heat the goods and battery.
- Protect the goods from pets and children.
- Don't put the goods and battery in the water.
- Don't hold power adaptor in the wet hands.

Chapter 2. Introduction & Requirements

Introduction of goods

What is the IMW-C910W?

- ⇒ IMW-C910W is a very inventive product for Portable Mobile WiMAX & WiFi Dual CPE(Customer Premises Equipment) enabling solution of the problem of lack in user terminals possible to use Mobile WiMAX service.
When IMW-C910W is left in pocket or bag with its power on in the area where Mobile WiMAX service is available, user can make concurrent connection to many WiFi terminals by using WiFi transmitted by IMW-C910W, so it enables free use of wireless internet in any area.
- ⇒ IMW-C910W included WiFi AP support Mobile WiMAX Service through WiFi can be supported portable devices (Laptop, Desktop, PDA and Smart Phone etc.)

System Requirements.

- ⇒ User's device will be installed WiFi (IEEE 802.11b/g/n) LAN Card or module.
- ⇒ The PC will be Installed USB port.

Specification

	Items	Description
WiMAX	WiMAX Standard Compliance	IEEE 802.16e-2005
	Air Interface	Internal Antenna(0dBi)
	Max output Power	23dBm
WiFi	Network Standard	IEEE 802.11 b/g/n(HT20)
	Frequency/Channels	2.4GHz/11Ch.
Power	Battery	Built-in Li-Polymer(3.7V/1520mA)
	Adaptor	5V / 2A
Dimension / Weight		67.0mm x 67.0mm x 12.5mm/56g

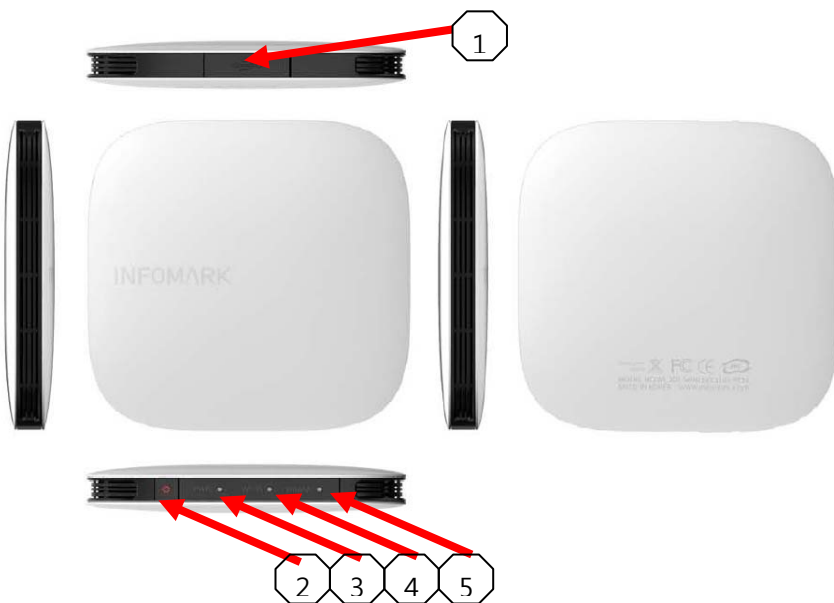
The points of name & Components list

Components List in the package.



- ① IMW-C910W
- ② Adaptor [5V / 2A] (Optional)
- ③ User's Manual
- ④ Plug
- ⑤ USB Cable

Points of name & Function



- ① USB Port : Battery charging and Tethered operation
- ② Power button: Power turn On/Off

- ③ Battery Status : battery status and power (Color : Yellow / Green / Red)
- ④ WiFi Status: WiFi On/Off Status USB Port : (Color : Green)
- ⑤ WiMAX Status: WiMAX Signal strength (Color : Yellow / Green / Red)

LED Status Scenario

WiMAX Signal LED

Off	Power Off
Yellow LED On and Off	Frequency scanning or ready
Red LED On and Off	Connecting with WiMAX network
Red LED On	WiMAX signal level 1
Yellow LED On	WiMAX signal level 2 ~ 3
Green LED On	WiMAX signal level 4 ~ 5

WiFi LED

WiFi AP turn On	Green color
-----------------	-------------

Power LED

Remained battery (100% ~ 60%)	Green color
Remained battery (60% ~ 30%)	Yellow color
Remained battery (30% ~ 0%)	Red color
Battery charging	Red color
Battery full charging	Green color

Chapter 3. How to use the IMW-C910W

Power ON/OFF

Power ON : Push the power button for 3 Seconds.

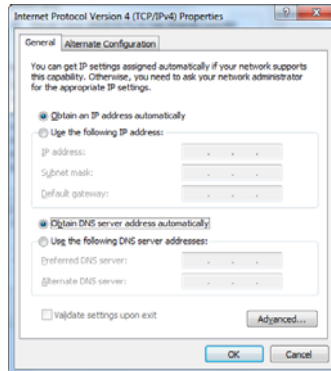
Power OFF : Push and hold the power button for 20 Seconds.

How to charge battery

The built-in battery can be charged from either USB cable or wall Charger (Optional)

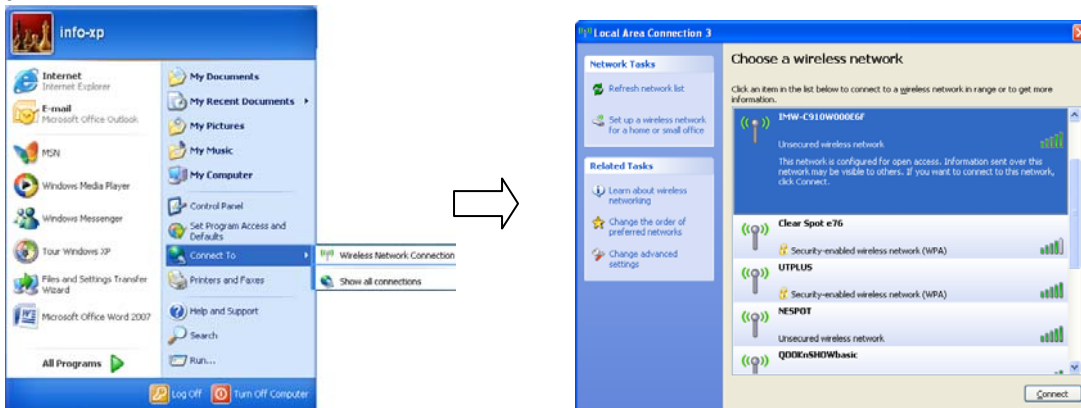
Setting of the WiFi AP

Notice : Configuration of WiFi AP has to be set to "Obtain IP address and DNS sever address automatically".



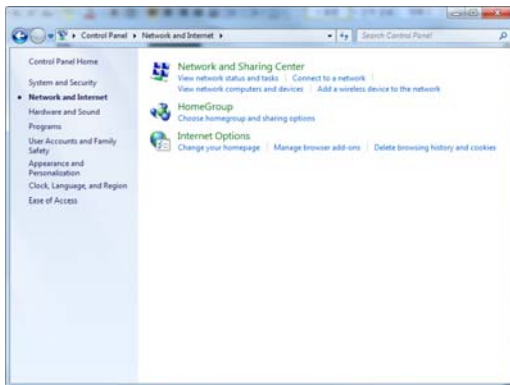
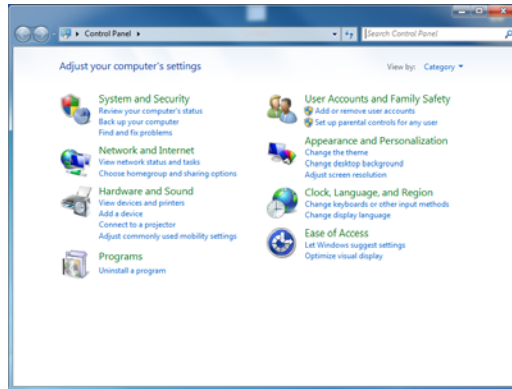
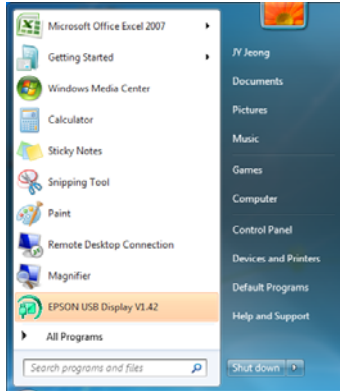
Setting with Window XP

● <Start>→<Connect to>→<Wireless Network Connection>→ Choose WiFi AP of IMW-C910W in the list



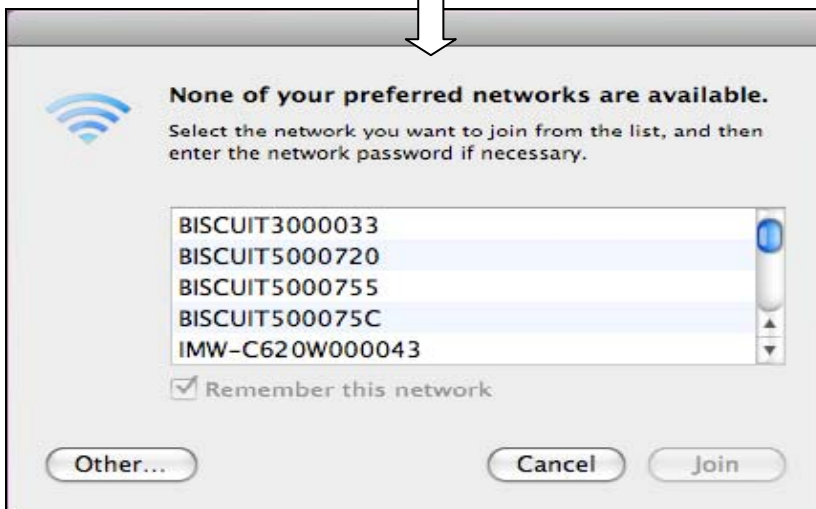
Setting with Window 7

- <Start> → <Control Panel> → <Network and Internet> → <Connect to Network>
→ Choose the WiFi AP of IMW-C910W in the list



Setting with Mac OS

- Click the wireless Icon on the menu → Choose the WiFi AP of IMW-C910W in the list



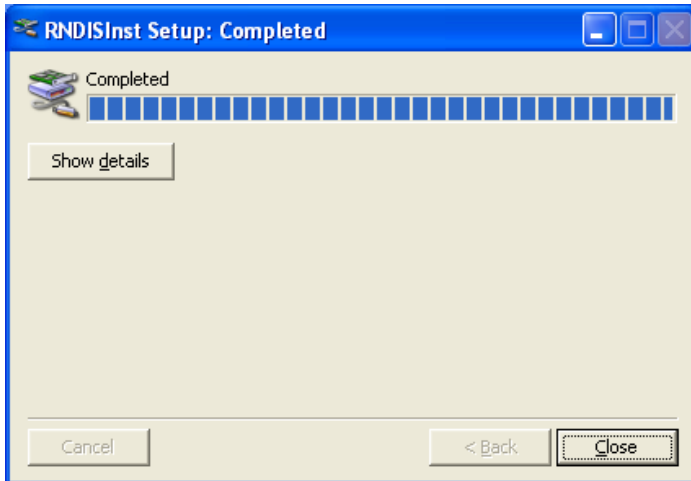
Setting of USB (RNDIS)

Notice :

1. Your PC connected to web server of IMW-C910W through WiFi.
2. Driver of RNDIS can down load from web sever of IMW-C910W.
3. Refer to USB Driver Page No. XX for download.

Setting with Window XP

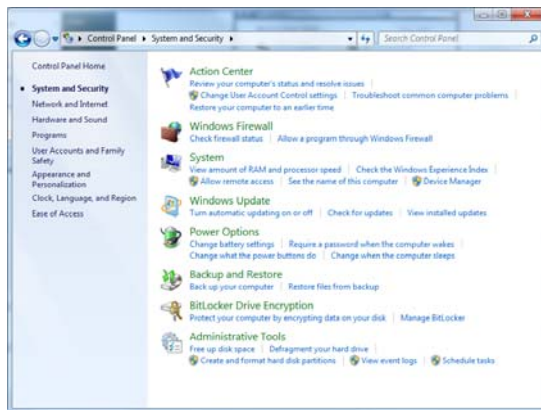
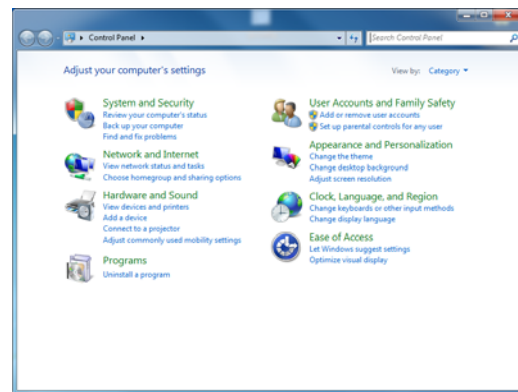
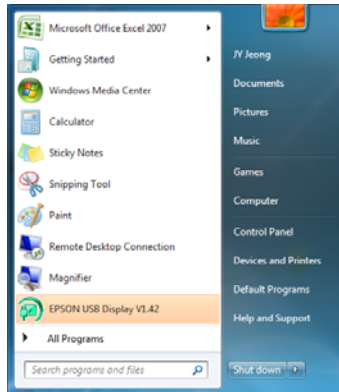
1. IMW-C910W should be connected with PC by USB cable.
2. Below is each step of RNDIS installation.



Setting with Window 7

1. IMW-C910W should be connected with PC by USB cable.
2. Below is each step of RNDIS installation.

<Start>→<Control Panel>→<Network and Internet>→<Connect to Network>

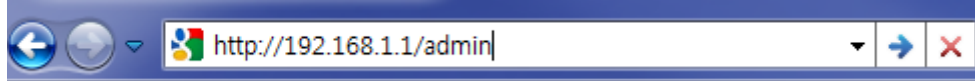


Chapter 4 Configuring CM

Connect to Web CM (Web Connection Manager)

Start CM

- Use web browser to connect Web CM
- Type Address 192.168.1.1/admin

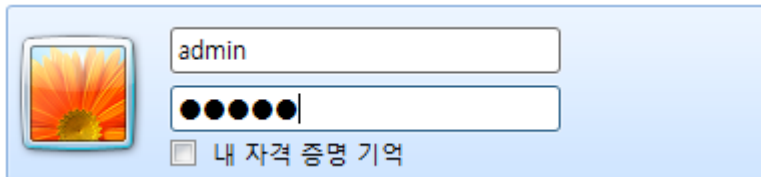


※ Microsoft Internet Explorer is recommended

Input ID/Password

- A Pop-up window will requests for specific ID and Password to enter into Web CM

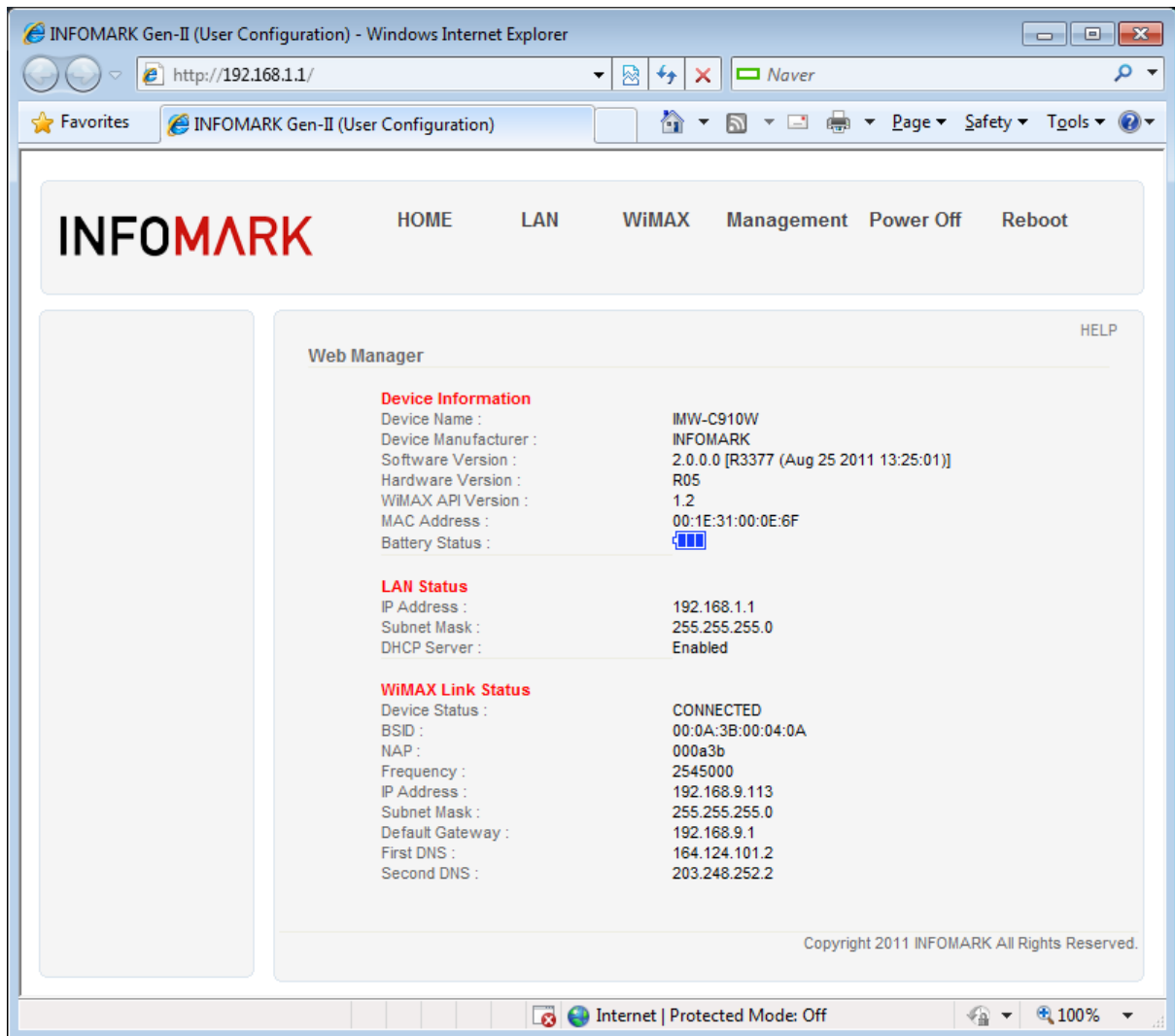
ID : admin / Password : admin

A screenshot of a login form. On the left is a square icon with a sunflower. To the right are two input fields. The top field contains the text "admin". The bottom field contains six black dots, representing a password. Below the password field is a checkbox with the Korean text "내 자격 증명 기억" (Remember my credentials).

Description of Web User Interface

Introduction

This is to describe user interface of Biscuit



- ① Main Menu
Main Menu help user to choose settings of LAN/WLAN, WiMAX frequency, Authentications, Device management.
- ② Sub Menu
Sub Menu shows detail categories of Main Menu
- ③ Main Window
Main Window shows status of device or setting parameters
- ④ Help Display
It shows additional description of Main Window

Home Menu

- ① Device Information
It shows description of Device such as name of device, manufacturer, software version, hardware version, API version and MAC address
- ② LAN information

It shows IP Address, Subnet Mask and setting of DHCP Server

③ WiMAX status information



It shows connection status of WiMAX and Network

[HELP](#)

Connection Information

Auto Refresh

WiMAX Connection Status

Connection Status :	CONNECTED
Signal strength :	 RSSI:-50 , CINR:30
Connection Up Time :	01:02:10
Battery Status :	

WiMAX IP Information

IP Address :	192.168.9.113
Subnet Mask :	255.255.255.0
Gateway :	192.168.9.1
Primary DNS Server :	164.124.101.2
Secondary DNS Server :	203.248.252.2
MAC Address :	00:1E:31:00:0E:6F

WiMAX Device Information

Model :	IMW-C910W
Software Version :	2.0.0.0 [R3377 (Aug 25 2011 13:25:01)]
Firmware Version :	2.1.5.4

Producer Information

Copyright :	INFOMARK
Terminal Manufacturers Website :	http://www.infomark.co.kr

Copyright 2011 INFOMARK All Rights Reserved.

LAN settings

① LAN Status

It shows web address of local area network information.

LAN Status

Information

IP Address :	192.168.1.1
Subnet Mask :	255.255.255.0
DHCP Server :	Enabled

Attached Devices

IP Address	MAC Address	IP TYPE
192.168.1.10	00:26:66:40:C1:FA	DHCP

② LAN Setting

LAN Setting

Modify

IP Address :	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
Subnet Mask :	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
DHCP Server :	<input type="text" value="Enabled"/> ▼
DHCP Range :	192.168.1. <input type="text" value="10"/> ~ 192.168.1. <input type="text" value="250"/>
IP Lease Time :	<input type="text" value="86400"/> sec

IP Reservation Settings

IP Address	MAC Address	Client List	
192.168.1. <input type="text"/>	<input type="text"/>	<< Client MAC ▼	Clear
192.168.1. <input type="text"/>	<input type="text"/>	<< Client MAC ▼	Clear
192.168.1. <input type="text"/>	<input type="text"/>	<< Client MAC ▼	Clear
192.168.1. <input type="text"/>	<input type="text"/>	<< Client MAC ▼	Clear
192.168.1. <input type="text"/>	<input type="text"/>	<< Client MAC ▼	Clear

- Local IP Address:

Input desired IP address that user want to use for Local Area Network

- Subnet Mask:

Input subnet mask to allocated IP address

- DHCP Server:

When DHCP is 'Disabled', please set IP address of client with static address.

For example, when the IP address is set as 192.168.1.1, set the client address as follow.

IP Address: from 192.168.1.2 to 192.168.1.253

Subnet Mask" 255.255.255.0

Gateway IP: 192.168.1.1

③ WiFi Status

Wi-Fi Status

Wireless (Wi-Fi) LAN

Default Network Name (SSID) : IMW-C910W000E6F

SSID Broadcast : On

Current Users : [Show Detail](#)

Wi-Fi Network Range : Short (best battery life)

Wi-Fi Channel : Auto (Ch. 5)

Mode : 802.11bg

Wi-Fi Security : Off

It shows Wi-Fi's SSID, Channel and Tx Power

④ WiFi Setting

Wi-Fi Settings

Wi-Fi Setting Information

Wi-Fi Radio On/Off : On

Network Name :

SSID Broadcast : Enable

Mode :

Channel :

Wi-Fi Network Range :

Wi-Fi Max Clients :

Security Setting :

- Network Name:

User can set preferred name of network name

The device comes with SSID of 'IMW-C910W'. This SSID can be changed as preferred.

- Security Setting:

Default setting of Security is 'Disabled'. If changed, 'Apply and Save' button should be clicked.

- WEP (Wired Equivalent Privacy): is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio and are thus more susceptible to eavesdropping than wired networks.

This Device provides 64/128 bit encryption for network protection.

- Authentication type: In case of selecting WEP, default setting is 'Auto'.

▶ Auto : This support both open system and shared key.

▶ Open System: Open system allow link to all clients but permit communication to clients that have same WEP key.

▶ Shared Key: Shared Key allow link and communication to clients that have identical shared key as AP.

- Key Length: For user convenience, select 64bit or 128 bit encryption.

- Key Pass Phrase: WEP Key is generated automatically. Input random character to generate key. Please make a separate note the key in order to connect to the device.
- WPA: The WPA protocol implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. This Device provides WPA, WPA2 and USB both.
- WPA Type : This Device provides WPA, WPA2.
 - ▶ WPA(Wi-Fi Protected Access) : WPA protocol implements the majority of the IEEE 802.11i standard. WPA is based on TKIP(Temporal Key Integrity Protocol) and it provide higher security of wireless communication.
 - ▶ WPA2 : AES(Advanced Encryption Standard) use additional encryption algorithm and it comply with WAP.
 - ▶ Use Both: It provide both WPA and WPA2 and it is default value when selecting WPA.
 - Encryption: It is to encrypt Unicast packets and support Auto, TKIP, AES-CCMP. Default is Auto.
 - Key Pass Phrase: Input WPA key value to blank and click 'Apply and Save'

⑤ NAT Setting

NAT Setting

Port Forwarding

Enabled	Name	Host IP	Service Port	Protocol
<input checked="" type="checkbox"/>	<input type="text"/>	192.168.1. <input type="text"/>	<input type="text"/> : <input type="text"/>	BOTH ▾

Port Forwarding List

DMZ Host

Enabled	Host IP	<input type="button" value="Save Settings"/>
<input type="checkbox"/>	192.168.1. <input type="text"/>	

Remote Admin

Enabled	Remote Admin Port	<input type="button" value="Save Settings"/>
<input type="checkbox"/>	<input type="text" value="80"/>	

UPnP

Enabled	Port	<input type="button" value="Save Settings"/>
<input type="checkbox"/>	<input type="text" value="5000"/>	

Application

Enabled	Applications	<input type="button" value="Save Settings"/>
<input checked="" type="checkbox"/>	FTP	
<input type="checkbox"/>	SIP	

VPN Passthrough

Enabled	<input type="button" value="Save Settings"/>
<input type="checkbox"/>	Enabled

- Port Forwarding setting:
Port forwarding is the practice of forwarding a TCP/IP packet in a network address translator gateway to a predetermined network port on a host within a masqueraded, typically private network based on the port number on which it was received from the originating host. The

technique is used to permit communications by external hosts with services provided within a private local area network.

- Port Forwarding List :
- DMZ Host :
- Remote Admin :

WiMAX Configuration

The parameter of WiMAX configuration are listed as Parametric Data, Network Info, Device Info, Frequency and Authentication

Parametric Data description

- Auto Refresh: When check box of enable is marked, real time values of WiMAX will be shown.
- Reset stat: This function initialize WiMAX monitoring value with 'Reset stat' button.
- Link Status Info
 - Device State: It shows current status of WiMAX connection.
 - Freq: It shows current connection frequency.
 - BSID: It shows BSID of connected WiMAX BS.
 - Tx Power: It shows output power of device.
 - RSSI: It stands for Receive Signal Strength Indicator. (Higher value states bad signal)
 - CINR: It stands for carrier to interference ratio. (Lower value states more noise)

- MAC Statistics Information

BW Req :	733	BW Req Retry :	12
[SDU]			
Tx Packet :	37	Rx Packet :	40
Tx Dropped :	0	Rx Dropped :	0
Tx Bytes :	2622	Rx Bytes :	6765
Tx Bytes Dropped :	0	Rx Bytes Dropped :	0
[PDU]			
Tx Packets :	1846	Rx Packets :	24
Tx Bytes :	28583	Rx Bytes :	3356
Rx CRC Error :	136	Rx ICV Error :	0
Rx HCS Error :	440	Rx KEY Error :	0
Rx Length Error :	5		

- This indicates Tx/Rx Packet information

- PHY Status

[Link Information]			
BSID :	F7-08-02-1C-30-70	Frequency :	2600000
Bandwidth :	10000		
[Basic PHY Parameters]			
Frame num :	10077014	DL Symbol :	29
FCH :	0xfd2200	UL Symbol :	18
TTG :	296	Curr PI :	23
RTG :	168	Prev PI :	0
[Link Quality]			
CINR main :	17	CINR diversity :	17
CINR mean :	20	CINR std dev :	10
CINR A mean :	21	CINR B mean :	14
RSSI main :	-77	RSSI diversity :	-76
RSSI mean :	-73	RSSI std dev :	-83
[Power Control]			
Mode :	open loop(retention)		
Tx Total Pwr(avg) :	9	Tx Sub Pwr(avg) :	-4
Tx Total Pwr(last) :	11	Tx Sub Pwr(last) :	-2
Tx Total Pwr(max) :	9	Tx Sub Pwr(max) :	-4
Tx Total Pwr(min) :	18	Tx Sub Pwr(min) :	0

- This indicates antenna level information of device

● PHY Statistics Information

DL MAP :	52660	DL MAP Error :	1340
UL MAP :	52660	UL MAP Error :	1340
FFB :	51320	ACK :	34
I-RNG :	1	P-RNG :	0
B-RNG :	807	H-RNG :	0

- This indicates statistics of antenna level of device.

● PHY Burst Statistics Information

DL Burst :	216	DL Burst Error :	0
DL HARQ Burst :	24	DL HARQ Dropped :	0
UL Burst :	1323	UL HARQ Burst :	791
UL HARQ Retry :	4		

DIUC0: QPSK (CTC) 1/2 R0 (N:0/8) (num: 8, err: 0)
 DIUC0: QPSK (CTC) 1/2 R6 (N:0/1) (num: 1, err: 0)
 DIUC1: QPSK (CTC) 3/4 R0 (N:0/6) (num: 6, err: 0)
 DIUC2: 16-QAM (CTC) 1/2 R0 (N:0/176) (num: 176, err: 0)
 DIUC3: 16-QAM (CTC) 3/4 R0 (N:0/1) (num: 1, err: 0)
 DIUC5: 64-QAM (CTC) 2/3 R0 (A:0/4) (num: 4, err: 0)
 DIUC6: 64-QAM (CTC) 3/4 R0 (A:1/10) (num: 10, err: 1)
 DIUC7: 64-QAM (CTC) 5/6 R0 (A:9/20) (num: 20, err: 9)
 UIUC1: QPSK (CTC) 1/2 R0 (N:0/1323) (num: 1323, err: 0)

- This indicates modulation information of device.

Network Information description

- Auto Refresh : When check box is enabled, Network and MAC status of device is monitored in real time.


● WiMAX Link Status

Device Status :	CONNECTED
BSID :	F7:08:02:1C:30:70
NAP :	f70802
Frequency :	2600000
IP Address :	175.255.249.203
Subnet Mask :	255.255.255.0
Default Gateway :	175.255.249.1
First DNS :	168.126.63.1
Second DNS :	168.126.63.2

- Device Status: This indicates connection status of WiMAX device.
- BSID: This indicates BSID of WiMAX network.
- NAP(Network Access Provider): This indicates operator's ID.
- Frequency: This indicates connected frequency.
- IP Address: This indicates Static IP Address acquired from BS.
- Subnet Mask: This indicates Static Subnet Mask acquired from BS.
- Default Gateway: This indicates Gateway acquired from BS.
- First DNS: This indicates the first DNS acquired from BS.
- Second DNS: This indicates second DNS acquired from BS.
- Service Flow
 - This indicates QoS status information of device in detail.

Device Information

● Device Information

Device Information	
Device Name :	IMW-C910W
Device Manufacturer :	INFOMARK
Software Version :	2.0.0.0 [R3377 (Aug 25 2011 13:25:01)]
Hardware Version :	R05
WiMAX API Version :	1.2
MAC Address :	00:1E:31:00:0E:6F
Battery Status :	

- Device Name: This indicates model name of device.
- Device Manufacturer: This indicates manufacturer of device.
- Software Version: This indicates firmware information of device.
- Hardware Version: This indicates hardware version of device..
- MiMAX API Version: This indicates WiMAX Common API Version.
- MAC Address: This indicates MAC address of device.

Frequency Setting

- ① No: Please register frequency that desired to be used in sequenc.
- ② First Freq.(kHz): Please register the first frequency NAP operator's range.
- ③ Last Freq.(kHz): Please register last frequency NAP operator's range.
- ④ Next Freq.(kHz): Please register step of frequency range.
- ⑤ Bandwidth(kHz): Please register bandwidth of NAP operator's frequency.
- ⑥ FFTSize: Please register FFTSize of NAP
- ⑦ After all through from ① to ⑥, click 'M/ADD' for modification or add.
- ⑧ this indicates registered frequency list of device.
- ⑨ In order to remove selected frequency, click 'DEL' button.

※ Example of frequency register

- Bandwidth of NAP : 5MHz,10MHz
- NAP의 FFTSize : 1024
- 1. ① Type 1 to register No1 (To modify pre-exist No, inout same No. to modify)
- 2. ② Input 2500000 as starting frequency
- 3. ③ Input 2650000 for last frequency
- 4. ④ Input step of frequency as 20000, (Increase in 20MHz steps)

5. ⑤ Input Bandwidth as 10000.
6. ⑥ Input FFTSize as 1024
7. Select ⑦
8. Select 'Reboot' in main window

Authentication Setting

PKM : Enable Disable ①

Alpha Delimiter : Enable Disable

EAP Method : EAP-TLS ②

EAP Fragment Size : 1300 bytes

CA Certificate #1 : installed: root.pem , subca.pem ③

CA Certificate #2 : ④

CA Certificate #3 : ④

Client Certificate : installed: client_only.pem ⑤

Private Key : installed: client_private_key_only.pem ⑥

Private Password : ●●●●●●●● ⑦

Inner NAI (ID) : socswmschap ⑧

Inner NAI Password : ●●●●●●●● ⑨

Outer NAI (Anonymous ID): random

Erase Certificate : CA Certificate ⑧ Erase ⑨

Save ⑩

- ① PKM: Please select if the certificate is desired to be used..
- ② EAP Method: When PKM is available, select the authentication method as EAP-AKA/EAP-TLS/EAP-TTLS.
- ③ CA Certificate #1: Register certificate in Root CA.
- ④ CA Certificate #2/#3: Register #2 and #3 certificate in Sub CA successively.
- ⑤ Client Certificate: Register Client Certificate
- ⑥ Private Key: Register Private Key Certificate
- ⑦ Private Password: Input Private Password acquired from NAP
- ⑧ Inner NAI (ID): Input Inner NAI (ID) acquired from NAP.
- ⑨ Inner NAI Password: Input NAI Password acquired from NAP.
- ⑩ Outer NAI (Anonymous ID): Input Outer NAI acquired from NAP.
- Ⓐ Erase Certificate: In order to erase certificate (CA Certificate, Client Certificate, Private Key Certificate), select and click 'Erase' to remove.
- Ⓑ Click Save to store the configuration.

※ Example: EAP-AKA

1. Select ① as Enable
 2. ② Select EAP-AKA
 3. Select ⑩ to save configuration
 4. Click 'Reboot' in main window
- (Warning: This EAP-AKA works with UICC include version of device.)

※ Example: EAP-TLS

1. Select ① as Enable
2. ② Select EAP-TLS
3. ③ Register Root CA Certificate
4. In case there is Sub CA Certificate, register in ④
5. ⑤ Register Client Certificate file
6. ⑦ Input private password
7. @ input Outer NAI (Anonymous ID)
(ex:random@infomark.co.kr or MAC Address@infomark.co.kr)
8. Select © to save configuration
9. Click 'Reboot' in main window

※ Example: EAP-TTLS


1. Select ① as Enable
2. ② Select EAP-TTLS/MSCHAPV2 (Select TTLS provided from NAP)
3. In case there is Root CA Certificate, register with ③
4. In case there is Sub CA Certificate, register with ④
5. Input inner NAI (ID) with ⑧.
6. Input inner NAI password with ⑨
7. @ input Outer NAI (Anonymous ID)
(ex:random@infomark.co.kr or MAC Address@infomark.co.kr)
8. Select © to save configuration
8. Select © to save configuration
9. Click 'Reboot' in main window

Administration setting

Items of Administrator settings are consist of Status, Firm info., Administration, Upgrade and USB Driver

Status description

Web Manager

Device Information	
Device Name :	IMW-C910W
Device Manufacturer :	INFOMARK
Software Version :	2.0.0.0 [R3377 (Aug 25 2011 13:25:01)]
Hardware Version :	R05
WiMAX API Version :	1.2
MAC Address :	00:1E:31:00:0E:6F
Battery Status :	
LAN Status	
IP Address :	192.168.1.1
Subnet Mask :	255.255.255.0
DHCP Server :	Enabled
WiMAX Link Status	
Device Status :	CONNECTED
BSID :	00:0A:3B:00:04:0A
NAP :	000a3b
Frequency :	2545000
IP Address :	192.168.9.113
Subnet Mask :	255.255.255.0
Default Gateway :	192.168.9.1
First DNS :	164.124.101.2
Second DNS :	203.248.252.2

① Device information

- This provides model name, manufacturer and version of software and hardware

② LAN setting information

- This provides IP Address, Subnet Mask and DHCP Server setting information

③ WiMAX status information

- This provides WiMAX connection status information.

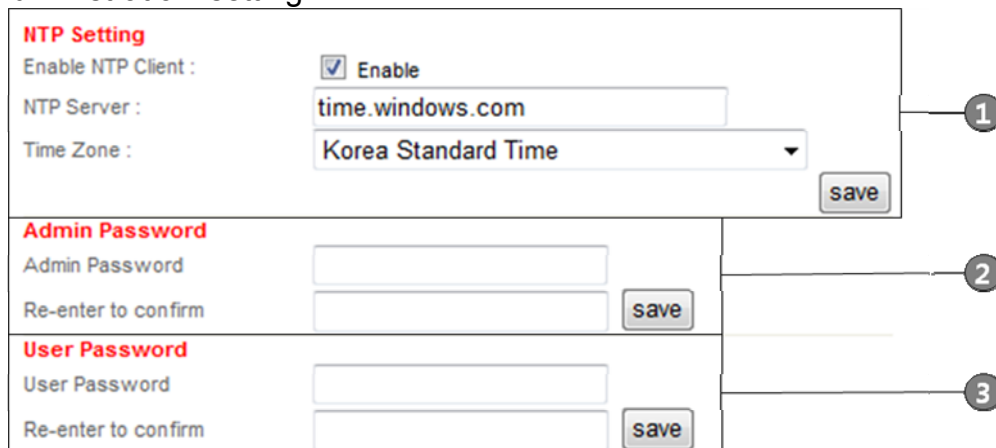
Firmware information

Firmware	
Firmware Information	
Software Version :	2.0.0.0 [R3377 (Aug 25 2011 13:25:01)]
Firmware Version :	2.1.5.4

- kernel version: This indicates version of device OS
- roots version: This indicates system file version
- firmware version: This indicates software (firmware) version
- WCM version: This indicates Web CM version

Administration setting

NTP Setting	
Enable NTP Client :	<input checked="" type="checkbox"/> Enable
NTP Server :	<input type="text" value="time.windows.com"/>
Time Zone :	<input type="text" value="Korea Standard Time"/>
<input type="button" value="save"/>	
Admin Password	
Admin Password	<input type="text"/>
Re-enter to confirm	<input type="text"/>
<input type="button" value="save"/>	
User Password	
User Password	<input type="text"/>
Re-enter to confirm	<input type="text"/>
<input type="button" value="save"/>	



① NTP Setting

- Enable NTP Client: In case of using NTP Client, enable check box of Enable NTP client
- NTP Server: Input URL of NTP Server URL
- Time Zone: Select Time Zone
- Click save to store the configuratio.

② Admin Password

- Item to change Web CM Password of Web CM of Admin
- Used to enter URL of http://192.168.1.1/admin/
- Enter same password twice
- Click 'save' to store configuration

③ User Password

- Item to change Web CM Password of Web CM of User
- Used to enter URL of http://192.168.1.1
- Enter same password twice
- Click 'save' to store configuration

Upgrade description

The screenshot shows a configuration page titled 'Upgrade'. It contains four rows of settings:

- Factory Reset : [Factory Reset button]
- Firmware Upgrade : [text input] [찾아보기... button] [Update button]
- Primary FOTA URL : [text input] [Save button] [Execute button]
- Secondary FOTA URL : [text input] [Save button] [Execute button]

- ① This is to return to factory default configuration.
- ② Device supports firmware update with binary file
 - When check box of Keep WiMAX config files is selected, the previous configuration will remain after update
 - After selecting file and click 'update' to start upgrade
- ③ Device supports zImage file update
- ④ Device supports ramdisk.jffs file update
- ⑤ Device supports Parameter bin file update
- ⑥ Device supports VPOS bin file update
- ⑦ FOTA URL setting
 - FOTA URL: Input URL of the site and save click to restore
 - When Enable Auto Upgrade is checked, device will compare the firmware version and on server and update if the firmware is new.

USB Driver description

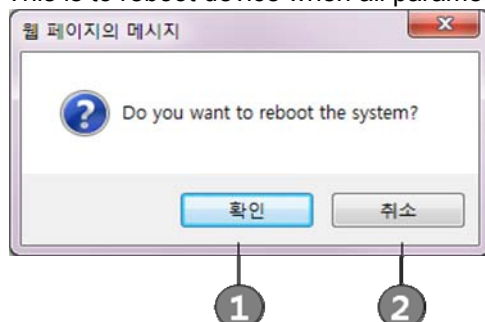
The screenshot shows a configuration page titled 'RNDIS'. It contains three sections:

- Enable CD-ROM (radio button) / Enable RNDIS (radio button, selected) [Save button]
- Driver(Windows XP/Vista/7) [Download button]
- Wi-Fi turn off when rndis is being connected [Save button]

- ① This is driver file when USB is used on Windows XP/Vista/7
- ② When used only with RNDIS, select checkbox of Wi-Fi off and save.
- ③ Reboot system in main window
- ※ This will make Wi-Fi off with reboot.

Reboot button description

This is to reboot device when all parameter is set



- ① Reboot system
- ② Cancel reboot

User Information

This device complies with part 15 of FCC Rules. Operation is subject to the following two conditions: 1. This device may not cause harmful interference, and 2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, Pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio Frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected

WARNING:

During transmitter operation, in order to meet RF Maximum permissible Exposure Safety Guidelines, a minimum distance of 20cm shall be maintained between this device and personnel.

This equipment may generate or use radio frequency energy. Changes or modifications to this equipment may cause harmful interference unless the modifications are expressly approved in the instruction manual. The user could lose the authority to operate this equipment if an unauthorized change or modification is made.