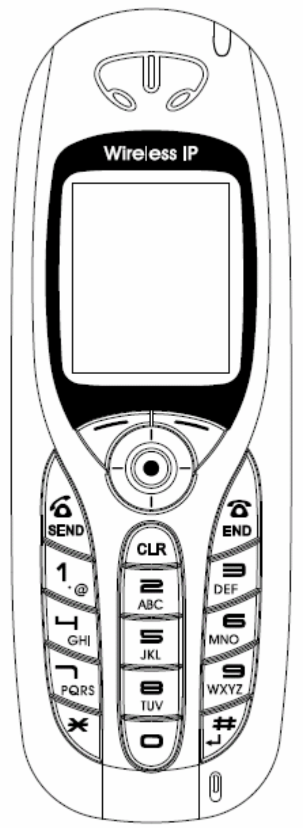
TD61-2896E

WirelessIP5000E-A
Administrator Manual

Thank you for purchasing the WirelessIP5000E-A.

- 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.



Product is certified to comply with technical standards.

CONTENTS

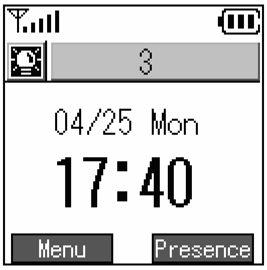
Chapter 1 Administrator Settings

Administrator Menu

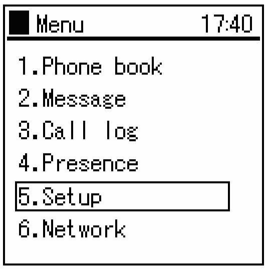
Makes required settings for using the phone. Only administrators are able to set items on the Administrator Menu.

1

Press the key to select Menu.

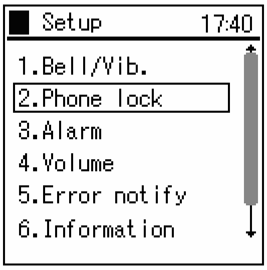


Select “5. Setup” using the ▲▼ keys of the key,
and confirm using the ◎ key.



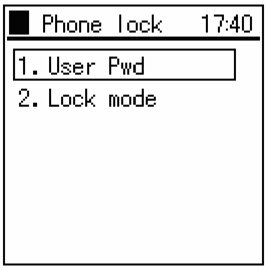
From the Setup menu,

Select “2. Phone lock” using the ▲▼ keys of the key,
and confirm using the ◎ key.



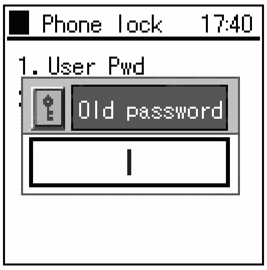
From the Phone lock menu,

Select “1. User Pwd” using the ▲▼ keys of the key,
and confirm using the ◎ key.



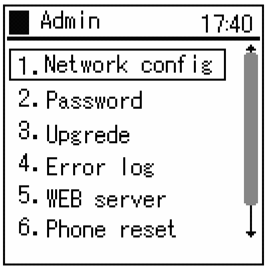
When you select "1. User Pwd", the system asks you for the current password. Enter the Admin password. The default value is 000000 (6 zeroes).

Set this using the ◎ key.



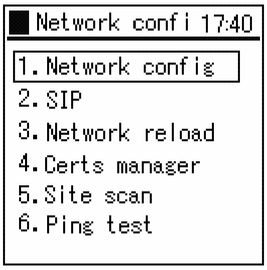
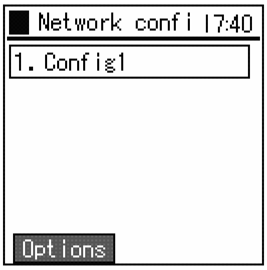
Network

This configures network-related settings.

1	From the Admin menu, Select “1. Network config” using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key.	 Admin 17:40 1. Network config 2. Password 3. Upgrede 4. Error log 5. WEB server 6. Phone reset

Network config

You can check the settings for the type of connected network as well as information about settings.

1	From the Network config menu, Select “1. Network config” using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key. The list of profiles (network settings) is displayed.	 Network confi 17:40 1. Network config 2. SIP 3. Network reload 4. Certs manager 5. Site scan 6. Ping test  Network confi 17:40 1. Config1 Options

■ Addition

New network profiles can be created

1 When making additions to the profile,

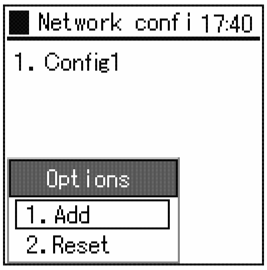
press the key on Network confi screen to select the submenu.

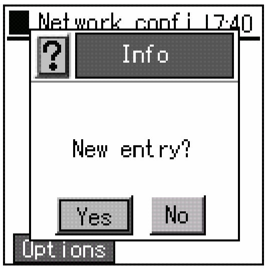
Select “1. Add”, and press the ◎ key.

A confirmation message is displayed.

Select "Yes" using the ◀▶ keys of the ⊕ key, and set this using the ◎ key.

Notice Registration Wizard starts if you select "2. Reset".





2 The network profile registration wizard is started.

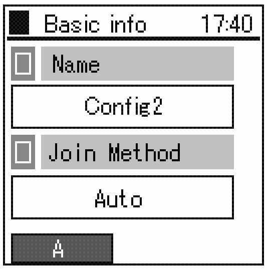
Input the profile name.

For the “Join Method”, select “Auto” or “Manual” using the ◀▶ keys.

After completion of editing, press the ◎ key.

Notice If you chose “Manual” by "Join method", you have to operate WirelessIP to connect to a network.

Reference P1-22 Network Connection



□ Name
Config2
□ Join Method
Auto

3 Input the SSID value of the wireless LAN to connect to.

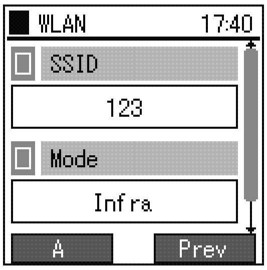
Notice If left blank, connection is made to the access point having the strongest wave signal from among the access points that can be connected to.

For the “Mode”, select “Infra” or “Ad-Hoc” using the ◀▶ keys.

Notice Usually select "Infra”.

After completion of editing, press the ◎ key.

If returning to the previous screen, press the key.



□ SSID
123
□ Mode
Infra

4

Select encryption type.

Select “None”, “WEP”, “WPA-PSK”, “WPA2-PSK”, “WPA-EAP” or “WPA2-EAP” using the ◀▶ keys of the ⊕ key, and confirm using the ◎ key.

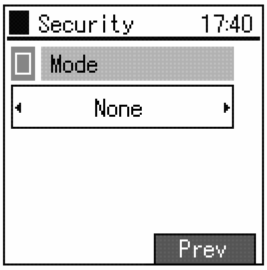
If returning to the previous screen, press the ↩ key.

If “WEP” is selected, a screen for performing settings related to WEP is displayed. Input the values as prompted on screen.

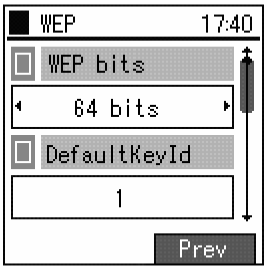
If “WPA-PSK” or “WPA2-PSK” is selected, a screen for inputting a pre-shared key is displayed. Input the values as prompted on screen.

Finally, press the ◎ key.

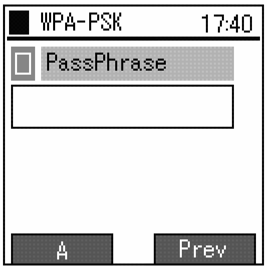
Reference P1-10 Encryption



Security 17:40
Mode
◂ None ▸
Prev



WEP 17:40
WEP bits
◂ 64 bits ▸
DefaultKeyId
1
Prev



WPA-PSK 17:40
PassPhrase

A Prev

5

Configure the settings for TCP/IP.

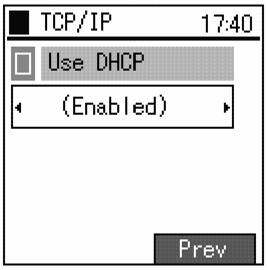
For “Use DHCP”, select “Disabled” or “Enabled” using the ◀▶ keys.

If returning to the previous screen, press the ↩ key.

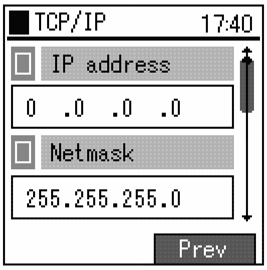
If “Disabled” is selected, the screen for setting the IP address is selected. Input the value as prompted on screen.

Finally, press the ◎ key.

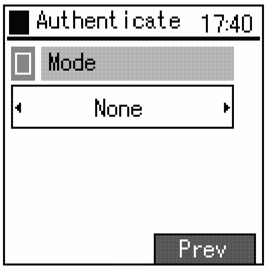
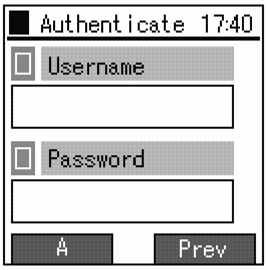
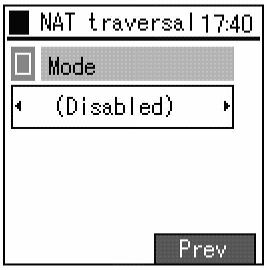
Reference P1-14 TCP/IP



TCP/IP 17:40
Use DHCP
◂ (Enabled) ▸
Prev



TCP/IP 17:40
IP address
0 .0 .0 .0
Netmask
255.255.255.0
Prev

6	Configure the settings for the network authentication method. For “Mode”, select “Disable”, “WEB”, “8021X-MD5”, “8021X-TLS”, “8021X-PEAP”, or “8021X-TTLS” using the ◀▶ keys. If returning to the previous screen, press the key. If anything other than “Disabled” is selected, the screen for setting the user ID and password is displayed. Input the values as prompted on screen. Finally, press the ◎ key. Reference P1-13 Authentication Method	 Authenticate 17:40 Mode None  Authenticate 17:40 Username Password
7	Configure the settings for NAT Traversal. For “Mode”, select “Disable”, “SNAT”, “UPnP”, or “STUN” using the ◀▶ keys. If returning to the previous screen, press the key. If “SNAT” or “STUN” is selected, the respective setting screens are displayed. Input the values as prompted on screen. Finally, press the ◎ key. Reference P1-16 Nat Traversal	 NAT traversal 17:40 Mode (Disabled)

8

The Advanced settings screen is displayed.

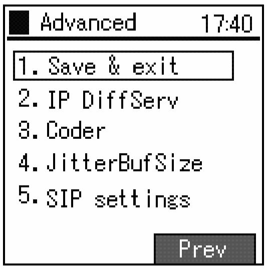
Other advanced settings can be made using the ▲▼ keys of the key.

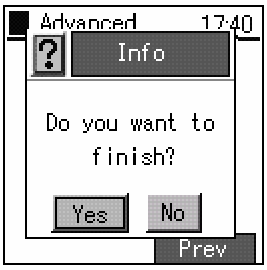
When the settings are completed, select “1. Save & Exit”, and press the ◎ key.

Select "Yes" using the ◀▶ keys of the key, and set this using the ◎ key.

The profile is saved and network reconnection is performed.

Up to a maximum of 5 profiles can be created.





Do you want to finish?

■ Deletion

Network profiles can be deleted.

1

When deleting a profile, from the Network confi screen

select the profile to be deleted using the ▲▼ keys of the key,

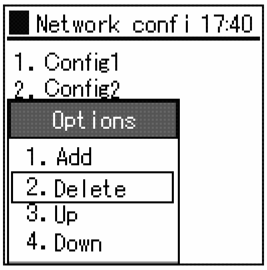
and press the key to select the submenu.

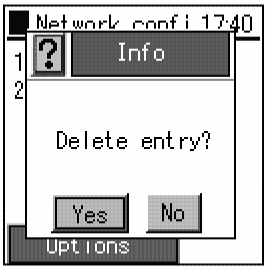
Select “2. Delete”, and press the ◎ key.

A confirmation message is displayed.

Select "Yes" using the ◀▶ keys of the key, and confirm using the ◎ key.

Deletion of all profiles is not possible.

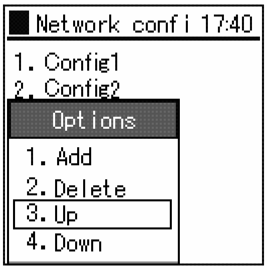




Delete entry?

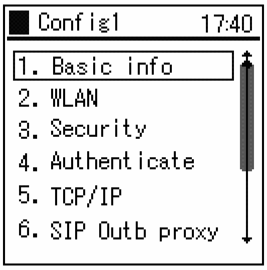
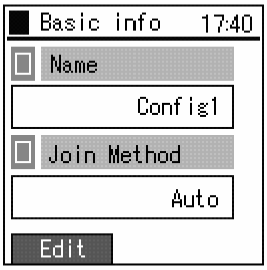
■ Priority-Level Settings

The priority level of a profile can be set.

1	When setting the priority level of a profile, from the profile-list screen Select the profile to be set using the ▲▼ keys of the key, and press the key to select the submenu. Select "3. Up" or "4. Down", and press the ◎ key. **Notice** WirelessIP tries connection with the profile whose priority is higher.	 Network confi 17:40 1. Config1 2. Config2 Options 1. Add 2. Delete 3. Up 4. Down

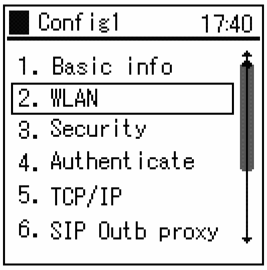
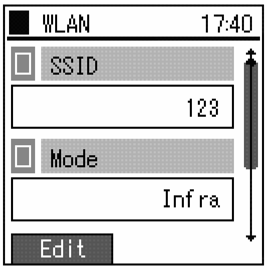
■ Basic Information

A profile's name and its connection method can be set.

1	From the Config1(profile name) menu, Select "1. Basic info" using the ▲▼ keys of the key, and confirm using the ◎ key.	 Config1 17:40 1. Basic info 2. WLAN 3. Security 4. Authenticate 5. TCP/IP 6. SIP Outb proxy
2	When editing the "Name", select "Edit" using the key. For the "Join Method", select "Auto" or "Manual" using the ◀▶ keys. After completion of editing, save using the ◎ key.	 Basic info 17:40 Name Config1 Join Method Auto Edit

■ Wireless LAN

The SSID that identifies the access point can be set.

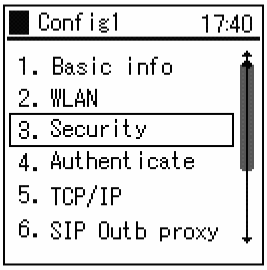
1	From the Config1(profile name) menu, Select “2. WLAN” using the ▲▼ keys of the ⊕ key, and set using the ◎ key.	 Config1 17:40 1. Basic info 2. WLAN 3. Security 4. Authenticate 5. TCP/IP 6. SIP Outb proxy
2	Select “Edit” using the key. Input the SSID value of the wireless LAN to be connected to. **Notice** If left blank, connection is made to the access point having the strongest wave signal from among the access points that can be connected to. For the “Mode”, select “Infra” or “Ad-Hoc” using the ◀▶ keys. **Notice** Usually select "Infra”. Finally, save using the ◎ key.	 SSID 123 Mode Infra

Encryption

These settings are related to encryption. This product supports encryption based on WEP (64/128/256 bits).

1 From the Config1(profile name) menu,

Select “3. Security” using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key.

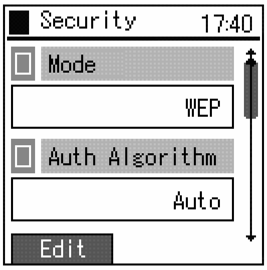


```
■ Config1          17:40
1. Basic info
2. WLAN
3. Security
4. Authenticate
5. TCP/IP
6. SIP Outb proxy
```

2 Select “Edit” using the key.

For “Mode”, select "Disabled", "WEP", "WPA-PSK", “WPA2-PSK”, “WPA-EAP” or “WPA2-EAP” using the ◀▶ keys of the ⊕ key.

Mode	Explanation
None	Wireless communications data does not be encrypt ed. With respect to security, we do not recommend this mode.
WEP	Based on the WEP key that was set, an effectively secure method for encrypting wireless communications data is made.
WPA-PSK WPA2-PSK	This is the method to encrypt wireless communications data based on a pre-shared key set in both this product and the connected device. As the encryption key is replaced automatically, strong security can be achieved.
WPA-EAP WPA2-EAP	This is the encryption method using IEEE802.1x. RADIUS server is needed for user authentication. This method is mostly for enterprise.



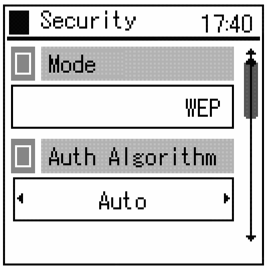
```
■ Security         17:40
□ Mode
                     WEP
□ Auth Algorithm
                    Auto
Edit
```

■ When WEP is selected for Mode

1

If “WEP” is selected as the Mode, for the “Auth Algorithm”,

Select “Auto”, “Open System”, or “Pre-shared Key” using the ◀▶ keys of the key .



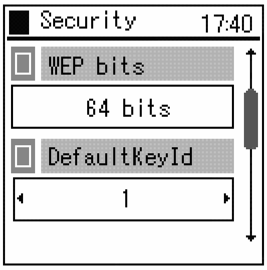
Security 17:40
Mode
WEP
Auth Algorithm
Auto

2

Select “WEP bits” and “Default Key Id”.

For the “WEP bits”, select “64 bits”, “128 bits”, or “256 bits” using the ◀▶ keys of the key.

For the “Default Key Id”, Select “1”, “2”, “3”, or “4” using the ◀▶ keys of the key.



Security 17:40
WEP bits
64 bits
DefaultKeyId
1

3

Input the WEP key as hexadecimal or alphanumeric. (Refer to the equivalence chart below)

Bit	Hexadecimal	Alphanumeric
128 bits	26 characters	13 characters
64 bits	10 characters	5 characters

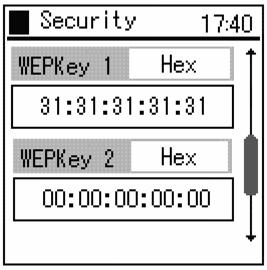
Encryption Bit Length	Hexadecimal (0 - 9, a - f)	Alphanumeric
128 bits	26 characters	13 characters
Input example	31:31:31:31:31:31:31:31:31:31:31:31:31	1111111111111
64 bits	10 characters	5 characters
Input example	31:31:31:31:31	11111

Notice

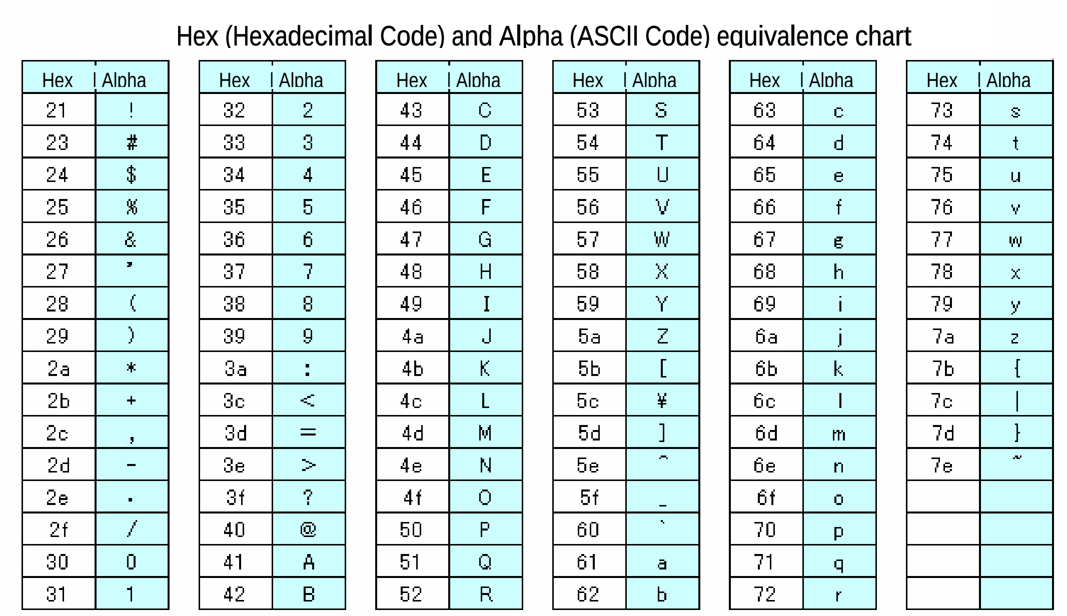
If the WEP key (hexadecimal, alphanumeric) that is input does not fill up the character count specified in the encryption bit length, the WEP key is generated by padding the hexadecimal number with additional zeros.

The longer the encryption bit length, the stronger the security.

Finally, set using the ◎ key.



Security 17:40
WEPKey 1 Hex
31:31:31:31:31
WEPKey 2 Hex
00:00:00:00:00



Hex (Hexadecimal Code) and Alpha (ASCII Code) equivalence chart

Hex	Alpha	Hex	Alpha	Hex	Alpha	Hex	Alpha	Hex	Alpha	Hex	Alpha
21	!	32	2	43	C	53	S	63	c	73	s
23	#	33	3	44	D	54	T	64	d	74	t
24	$	34	4	45	E	55	U	65	e	75	u
25	%	35	5	46	F	56	V	66	f	76	v
26	&	36	6	47	G	57	W	67	g	77	w
27	'	37	7	48	H	58	X	68	h	78	x
28	(	38	8	49	I	59	Y	69	i	79	y
29	)	39	9	4a	J	5a	Z	6a	j	7a	z
2a	*	3a	:	4b	K	5b	[	6b	k	7b	{
2b	+	3c	<	4c	L	5c	¥	6c	l	7c	|
2c	,	3d	=	4d	M	5d	]	6d	m	7d	}
2d	-	3e	>	4e	N	5e	^	6e	n	7e	~
2e	.	3f	?	4f	O	5f	_	6f	o		
2f	/	40	@	50	P	60	`	70	p		
30	0	41	A	51	Q	61	a	71	q		
31	1	42	B	52	R	62	b	72	r		

■ When WPA-PSK or WPA2-PSK is selected for Mode

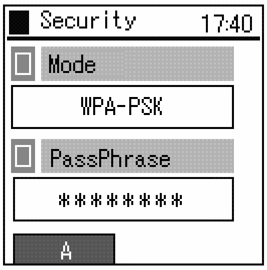
1 Select “Pre-shared key” (PassPhrase). Input the same value as the value set in the connection device.
Input the “PassPhrase” as single-byte alphanumeric characters with at least 8 characters but not more than 63 characters.

Finally, save using the ◎ key.

Notice

Starting from the input pre-shared key, the key is automatically changed to a new value every fixed period. This makes it more secure than WEP.

With WEB interface, Pre-shared key can be set in HEX.



Security 17:40

Mode
WPA-PSK

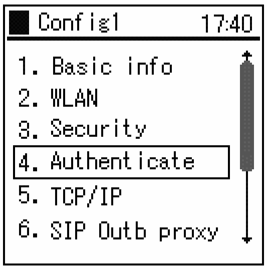
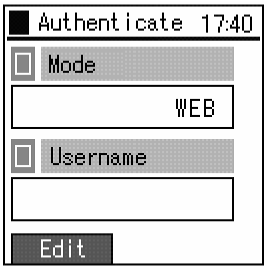
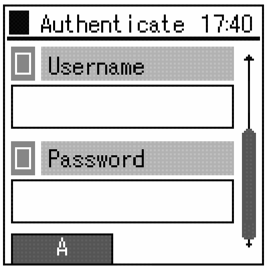
PassPhrase
****

A

■ Authentication Method

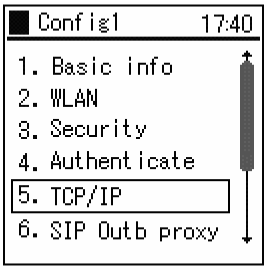
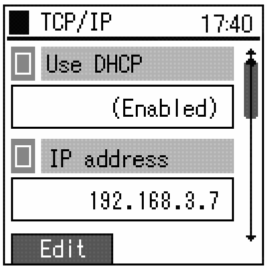
Authentication method is the settings related to network authentication.

Notice When “WPA-EAP” or “WPA2-EAP” is selected for Mode. This setting must be configured.

1	From the Config1(profile name) menu, Select “4. Authenticate” using the ▲▼ keys of the key, and confirm using the ◎ key.	 Config1 17:40 1. Basic info 2. WLAN 3. Security 4. Authenticate 5. TCP/IP 6. SIP Outb proxy
2	Select “Edit” using the key. For “Mode”, Select “Disable”, “WEB”, “8021X-MD5”, “8021X-TLS”, “8021X-PEAP”, or “8021X-TTLS” using the ◀▶ keys. When “WEB”, “8021X-MD5”, “8021X-TLS”, “8021X-PEAP”, or “8021X-TTLS” is selected, set “user identification” and “the password” for certification. **Notice** When downloading the private certificate, first, set the password for installation, and designate "Mode" as "None". After completing download, set "User name" and "Password" for certification. <u>Reference</u> P1-23 Certificate Management Finally, set using the ◎ key.	 Authenticate 17:40 □ Mode WEB □ Username Edit  Authenticate 17:40 □ Username □ Password A

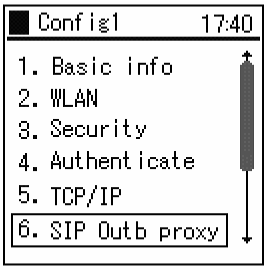
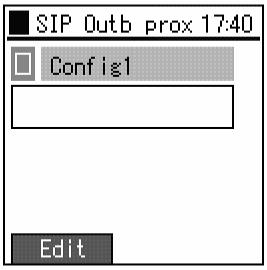
■ TCP/IP

The settings for DHCP, IP address, subnet mask, default gateway, and DNS can be configured.

1	From the Config1(profile name) menu, Select “5. TCP/IP” using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key.	 Config1 17:40 1. Basic info 2. WLAN 3. Security 4. Authenticate 5. TCP/IP 6. SIP Outb proxy
2	Select “Edit” using the key. For “Use DHCP”, Select “Enable” or “Disable” using the ◀▶ keys of the ⊕ key. When setting the IP address manually, set DHCP to “Disable” and input values for the items below: ・ IP address: IP address of the WirelessIP5000E-A ・ Subnet mask: Value of subnet mask ・ Default gateway: IP address of default gateway ・ DNS server 1: IP address of primary DNS ・ DNS server 2: IP address of secondary DNS Finally, set using the ◎ key. **Notice** When “DHCP” is set to “Enable”, the values of other setting parameters relating to TCP/IP do not apply.	 TCP/IP 17:40 Use DHCP (Enabled) IP address 192.168.3.7 Edit

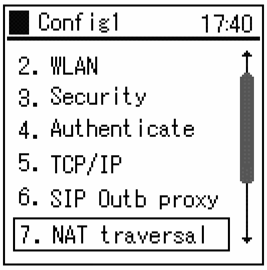
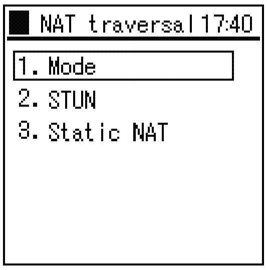
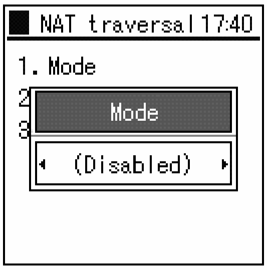
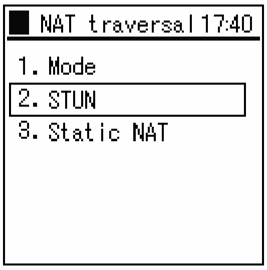
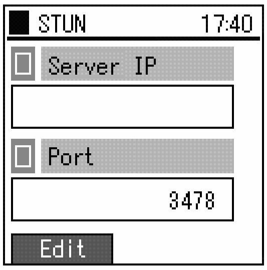
SIP Outb Proxy

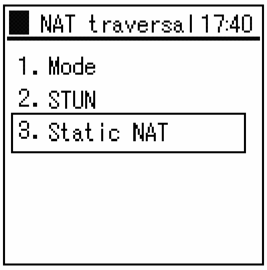
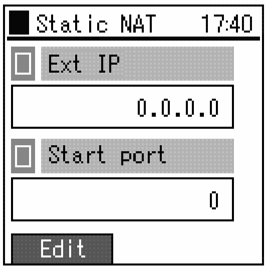
You can set the Outbound Proxy server settings. Depending on the system configuration it may not be necessary to set them.

1	From the Config1(profile name) menu, Select "6. SIP Outb Proxy" using the ▲▼ keys of the key, and confirm using the ◎ key.	 Config1 17:40 1. Basic info 2. WLAN 3. Security 4. Authenticate 5. TCP/IP 6. SIP Outb proxy
2	The screen for inputting the IP address of the SIP Outb Proxy is displayed. Select "Edit" using the key. Enter the IP address. Finally, save using the ◎ key.	 SIP Outb prox 17:40 Config1 Edit

■ NAT Traversal

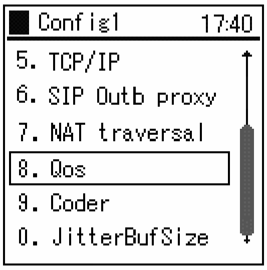
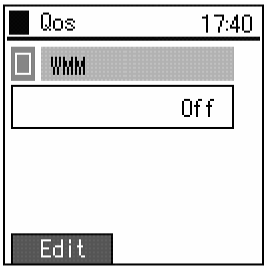
This product supports UPnP and Static NAT, and it is possible to make calls from within the LAN to outside the LAN via a NAT Box. At these times, the settings for UPnP and Static NAT can be made to match the settings of the NAT Box to be connected to.

1	From the Config1(profile name) menu, Select “7. NAT Traversal” using the ▲▼ keys of the key, and confirm using the ◎ key.	 Config1 17:40 2. WLAN 3. Security 4. Authenticate 5. TCP/IP 6. SIP Outb proxy 7. NAT traversal
2	From the NAT Traversal menu, Select “1. Mode” using the ▲▼ keys of the key, and confirm using the ◎ key. Select “Edit” using the key. For “Mode”, select “SNAT”, “UPnP”, “STUN”, or “Disabled”. Finally,save using the ◎ key.	 NAT traversal 17:40 1. Mode 2. STUN 3. Static NAT  NAT traversal 17:40 1. Mode Mode ◂ (Disabled) ▸
3	From the NAT Traversal menu, Select “2. STUN” using the ▲▼ keys of the key , and confirm using the ◎ key. Select “Edit” using the key. Input the values for server IP and port number. Finally, save using the ◎ key.	 NAT traversal 17:40 1. Mode 2. STUN 3. Static NAT  STUN 17:40 Server IP Port 3478 Edit

4	From the NAT Traversal menu, Select “3. Static NAT” using the ▲▼ keys of the key, and confirm using the ◎ key. Select “Edit” using the key. Input the values for external IP and port number. Finally, save using the ◎ key.	 NAT traversal 17:40 1. Mode 2. STUN 3. Static NAT  Static NAT 17:40 Ext IP 0.0.0.0 Start port 0 Edit

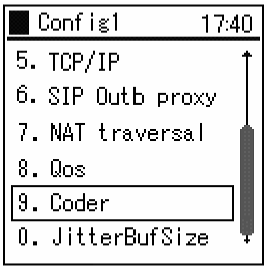
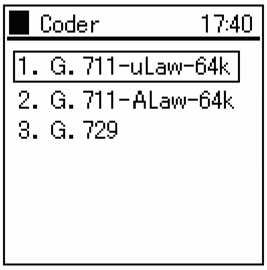
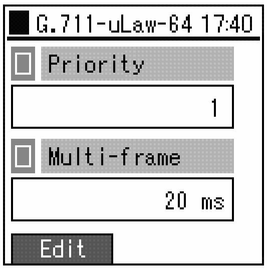
■ QoS

Settings related to QoS can be configured.

1	From the Config1(profile name) menu, Select “8. QoS” using the ▲▼ keys of the key, and confirm using the ◎ key.	 Config1 17:40 5. TCP/IP 6. SIP Outb proxy 7. NAT traversal 8. Qos 9. Coder 0. JitterBufSize
2	Select “Edit” using the key. For WMM, Select “On” or “Off” using the ◀▶ keys of the key. Finally, save using the ◎ key.	 Qos 17:40 WMM Off Edit

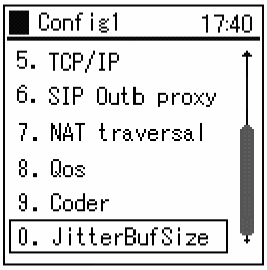
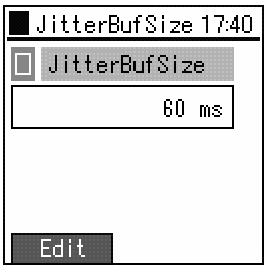
■ Coding

You can set the CODEC (priority and transmission interval) to match the system configuration.

1	From the Config1(profile name) menu, Select "9. Coder" using the ▲▼ keys of the key, and confirm using the ◎ key.	 Config1 17:40 5. TCP/IP 6. SIP Outb proxy 7. NAT traversal 8. Qos 9. Coder 0. JitterBufSize
2	From the Coder menu, Select one codec using the ▲▼ keys of the key, and confirm using the ◎ key. Detailed information is displayed. Select "Edit" using the key. Set the priority (1- 3) and the RTP "Multiframe" interval (20- 40 ms). Finally, save using the ◎ key.	 Coder 17:40 1. G.711-uLaw-64k 2. G.711-ALaw-64k 3. G.729  Priority 1 Multi-frame 20 ms

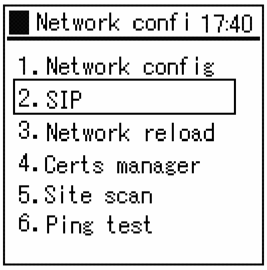
■ Jitter Buffer

Settings related to jitter buffer can be configured.

1	From the Config1(profile name) menu, Select "0. JitterBufSize" using the ▲▼ keys of the key, and confirm using the ◎ key.	 Config1 17:40 5. TCP/IP 6. SIP Outb proxy 7. NAT traversal 8. Qos 9. Coder 0. JitterBufSize
2	Select "Edit" using the key. For jitter buffer value, use the ◀▶ keys of the key to select a value from 20- 200 ms. Finally, save using the ◎ key.	 JitterBufSize 60 ms

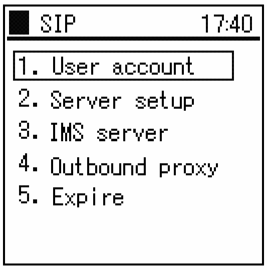
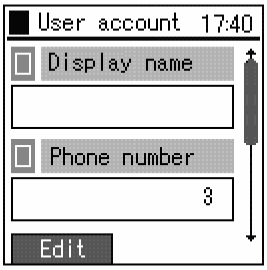
SIP

SIP settings can be configured.

1	From the Network menu, Select “2. SIP” using the ▲▼ keys of the key, and confirm using the ◎ key.	 Network confi 17:40 1. Network config 2. SIP 3. Network reload 4. Certs manager 5. Site scan 6. Ping test

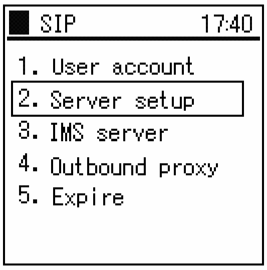
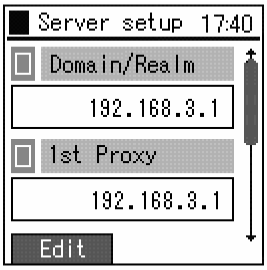
User account

Configures the settings for the display name, phone number, user ID, and URL Scheme.

1	From the SIP menu, Select “1. User account” using the ▲▼ keys of the key, and confirm using the ◎ key.	 SIP 17:40 1. User account 2. Server setup 3. IMS server 4. Outbound proxy 5. Expire
2	Select “Edit” using the key. The following information is displayed: · Display name · Phone number · User ID · User password · URL Scheme The phone number is mandatory, while display name, user ID, and URL Scheme should be input as needed. Finally, save using the ◎ key.	 User account 17:40 Display name Phone number 3 Edit

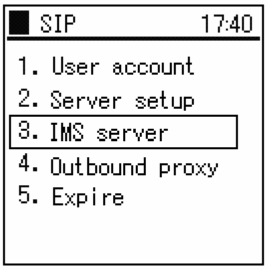
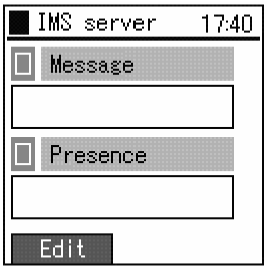
Server

Settings the SIP server

1	From the SIP menu, Select “2. Server setup” using the ▲▼ keys of the key, and confirm using the ◎ key.	 SIP 17:40 1. User account 2. Server setup 3. IMS server 4. Outbound proxy 5. Expire
2	Select “Edit” using the key. Input values for the following items: · SIP domain · Proxy server 1 · Register server 1 · Proxy server 2 · Register server 2 Finally, save using the ◎ key.	 Server setup 17:40 Domain/Realm 192.168.3.1 1st Proxy 192.168.3.1 Edit

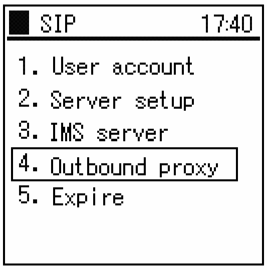
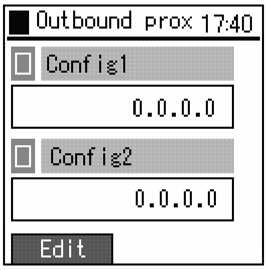
IMS Server

Settings the IMS server and Presence server
IM server is the server in order to exchange instant message.
Presence server is the server in order to exchange status information.

1	From the SIP menu, Select “3. IMS server” using the ▲▼ keys of the key, and confirm using the ◎ key.	 SIP 17:40 1. User account 2. Server setup 3. IMS server 4. Outbound proxy 5. Expire
2	Select “Edit” using the key. Input IP address for "Message" and "Presence". Finally, save using the ◎ key.	 IMS server 17:40 Message Presence Edit

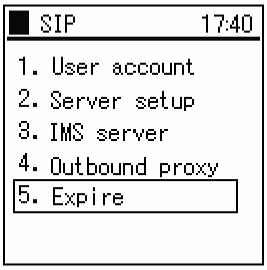
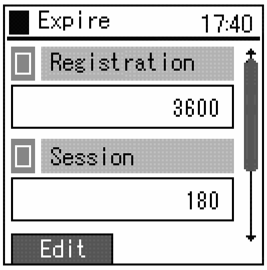
■ Outbound Proxy

The settings for the outbound proxy server can be configured. Depending on the system configuration it may not be necessary to set them.

1	From the SIP menu, Select “4. Outbound proxy” using the ▲▼ keys of the key, and confirm using the ◎ key.	 SIP 17:40 1. User account 2. Server setup 3. IMS server 4. Outbound proxy 5. Expire
2	Select “Edit” using the key. Input the IP address for outbound proxy server. Finally, save using the ◎ key.	 Outbound prox 17:40 Config1 0.0.0.0 Config2 0.0.0.0 Edit

■ Expire

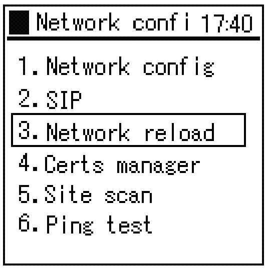
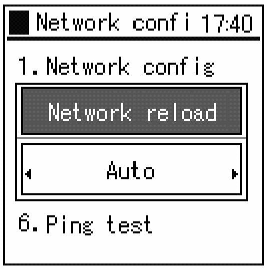
The settings for Regist Expire Timer, Session Timer, and Presence Expire Timer can be configured.

1	From the SIP menu, Select “5. Expire” using the ▲▼ keys of the key, and confirm using the ◎ key.	 SIP 17:40 1. User account 2. Server setup 3. IMS server 4. Outbound proxy 5. Expire
2	Select “Edit” using the key. Input values for the following items: ・Regist Expire (second) ・Session Expire (second) ・Presence Expire (second) Finally, save using the ◎ key.	 Expire 17:40 Registration 3600 Session 180 Edit

Network Connection

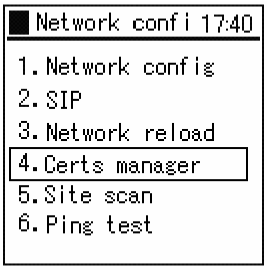
■ Network Connection

When adding, deleting, and changing settings of profiles, reconnection can be done manually.

1	From the Network menu, Select “3. Network reload” using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key.	 ■ Network confi 17:40 1. Network config 2. SIP 3. Network reload 4. Certs manager 5. Site scan 6. Ping test
2	Select “Auto”, “Suspend”, “Disconnect”, or “Profile name” using the ◀▶ keys of the ⊕ key, and confirm using the ◎ key. Reload commences.	 ■ Network confi 17:40 1. Network config Network reload ◂ Auto ▸ 6. Ping test

Certificate Management

Certificate settings can be configured.

1	From the Network menu, Select “4. Certs manager” using the ▲▼ keys of the key, and confirm using the ◎ key.	 Network confi 17:40 1. Network config 2. SIP 3. Network reload 4. Certs manager 5. Site scan 6. Ping test

Reference and download of the route certificate and the private certificate is possible in order to use 802.1x （EAP-TLS, PEAP, TTLS）.

From v2.4.0, you can select which of TFTP or HTTP as a download system with 【UPGRADE】 Request_Mode. Because each setting method differs, refer the chart under.

STOP Do not use “%” and space for file name.

download system	setting method	Example of input
TFTP	Setting IP address of TFTP server	192.168.0.1
HTTP	Setting URL and filename of HTTP server http://IP address of HTTP server / filename	http://192.168.0.1/1234.cer

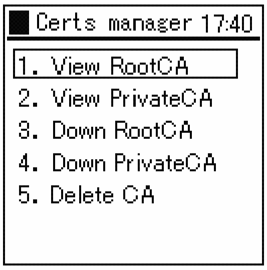
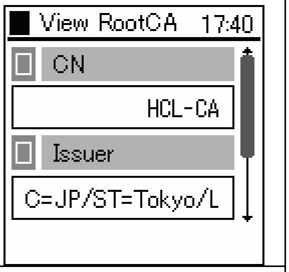
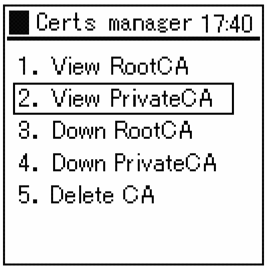
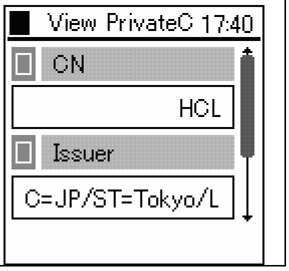
Notice When installing the private certificate, record the password for installation, user identification for certification and its password.

Beforehand insert the certificate in the directory of the server.

route certificate： Supporting .der, .cer and .pem Encode system
private certificate： Supporting .pfx and .p12 Encode system

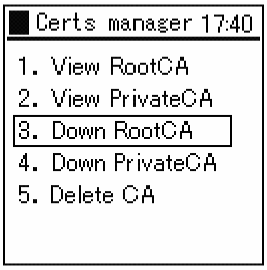
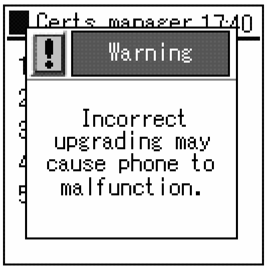
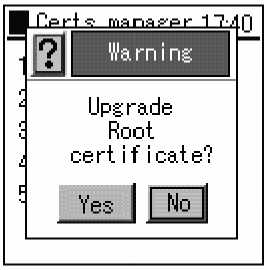
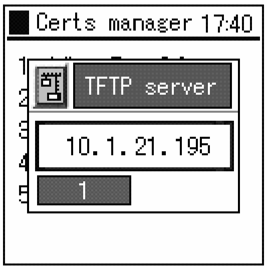
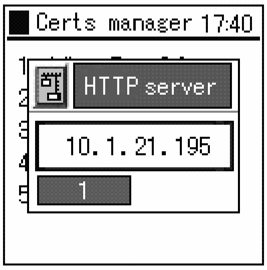
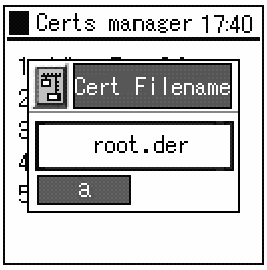
■ View RootCA , View PrivateCA

View the route certificate and the private certificate

1	From the Certs manager menu, Select “1. View RootCA” using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key.	 Certs manager 17:40 1. View RootCA 2. View PrivateCA 3. Down RootCA 4. Down PrivateCA 5. Delete CA  View RootCA 17:40 CN HCL-CA Issuer C=JP/ST=Tokyo/L
2	From the Certs manager menu, Select “2. View PrivateCA” using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key. **Notice** Beforehand it is necessary to set “password” for certification with “Authenticate” menu. Reference P1-13 Authentication Method	 Certs manager 17:40 1. View RootCA 2. View PrivateCA 3. Down RootCA 4. Down PrivateCA 5. Delete CA  View PrivateC 17:40 CN HCL Issuer C=JP/ST=Tokyo/L

■ Download RootCA

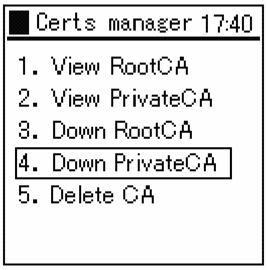
Download the route certificate

1	From the Certs manager menu, Select “3. Download RootCA” using the ▲▼ keys of the ✛ key, and confirm using the ◎ key.	 Certs manager 17:40 1. View RootCA 2. View PrivateCA 3. Down RootCA 4. Down PrivateCA 5. Delete CA
	A warning message is displayed.	 Certs manager 17:40 Warning Incorrect upgrading may cause phone to malfunction.
	Select “Yes” or “No” using the ◀▶ keys of the ✛ key.	 Certs manager 17:40 Warning Upgrade Root certificate? Yes No
	<In case of TFTP server> If “Yes” is selected, there is a prompt for input of the IP address of the download destination TFTP server. After inputting the IP address, press the ◎ key.	 Certs manager 17:40 TFTP server 10.1.21.195 1
	<In case of HTTP server> If “Yes” is selected, there is a prompt for input of the URL of the download destination HTTP server and filename. After inputting them, press the ◎ key. Reference P1-13 Authentication Method	 Certs manager 17:40 HTTP server 10.1.21.195 1
	Input of “certificate file name” is required. After the verifying or the editing, press the ◎ key and download starts.	 Certs manager 17:40 Cert Filename root.der a

■ Download PrivateCA

Download the route certificate

1 **Notice** Beforehand it is necessary to input “password” for Installation with “Authenticate” menu, and to designate "Mode" as "None".



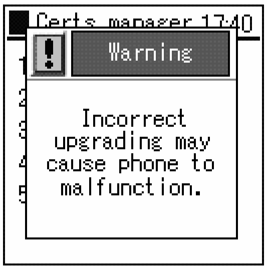
■ Certs manager 17:40
1. View RootCA
2. View PrivateCA
3. Down RootCA
4. Down PrivateCA
5. Delete CA

<u>Reference</u> P1-13 Authentication Method

From the Certs manager menu,

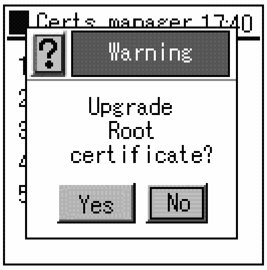
Select “4. Download PrivateCA” using the ▲▼ keys of the key, and confirm using the ◎ key.

A warning message is displayed.



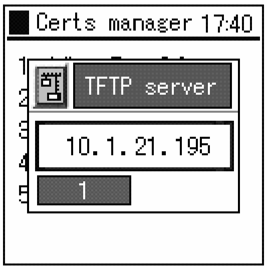
Certs manager 17:40
Warning
Incorrect upgrading may cause phone to malfunction.

Select “Yes” or “No” using the ◀▶ keys of the key.



Certs manager 17:40
Warning
Upgrade Root certificate?
Yes No

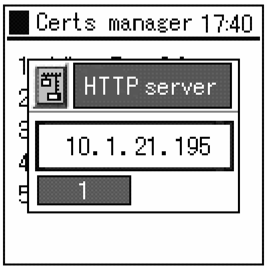
<In case of TFTP server>
If “Yes” is selected, there is a prompt for input of the IP address of the download destination TFTP server. After input of the IP address, press the ◎ key and the download is started.



■ Certs manager 17:40
TFTP server
10. 1. 21. 195
1

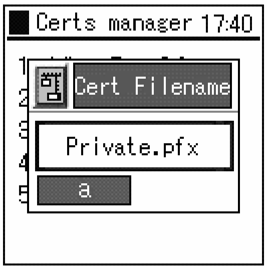
<In case of HTTP server>
If “Yes” is selected, there is a prompt for input of the URL of the download destination HTTP server and filename. After inputting them, press the ◎ key.

<u>Reference</u> P1-13 Authentication Method



■ Certs manager 17:40
HTTP server
10. 1. 21. 195
1

Input of “certificate filename” is required.
Verify or edit the filename, and press the ◎ key then download starts.

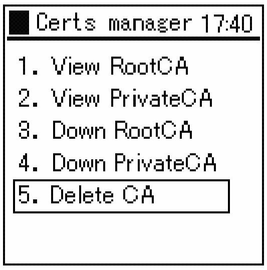
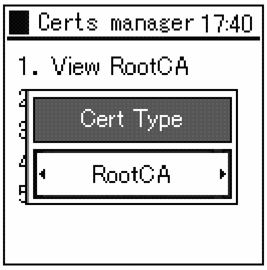


■ Certs manager 17:40
Cert Filename
Private.pfx
a

Notice After completing download, set "User name" and "Password" for certification.

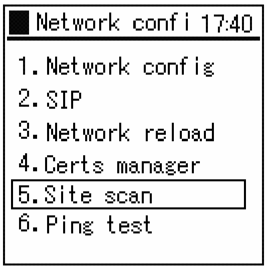
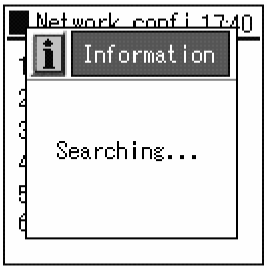
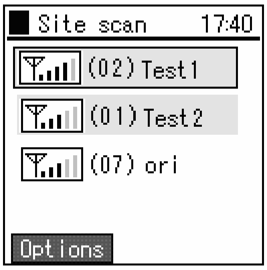
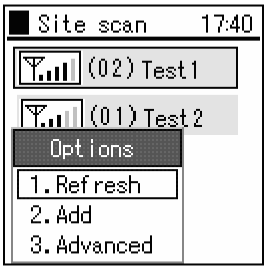
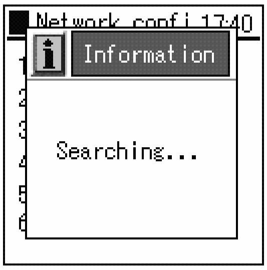
■ Delete CA

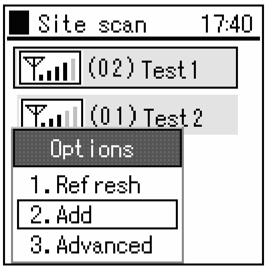
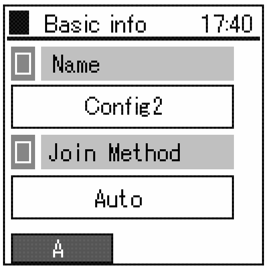
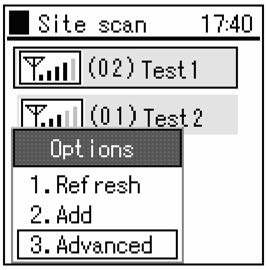
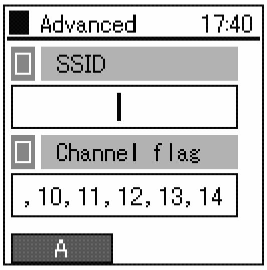
Delete the certificate

1	From the Certs manager menu, Select “5. Delete CA” using the ▲▼ keys of the key, and confirm using the ◎ key. Select “RootCA”, “PrivateCA”, or “Delete all” using the ◀▶ keys of the key.	 Certs manager 17:40 1. View RootCA 2. View PrivateCA 3. Down RootCA 4. Down PrivateCA 5. Delete CA  Certs manager 17:40 1. View RootCA Cert Type ◂ RootCA ▸

Network Search

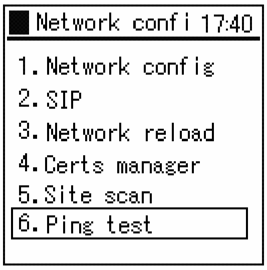
Information on detected signals can be displayed.

1	From the Network menu, Select “5. Site scan” using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key.	Network confi 17:40 1. Network config 2. SIP 3. Network reload 4. Certs manager 5. Site scan 6. Ping test
2	A message indicating a search is in progress appears. Several seconds later, the SSIDs of the detected access points are displayed. When detailed information needs to be viewed, select the SSID using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key. **Notice** Access points that are set to ‘reject ANY’ connection are not displayed in the detection result listing. If the detected access point is encrypted, the SSID is displayed with a net overlay. In addition, access points can be displayed for up to a maximum of 20 locations.	Network confi 17:40 Information Searching... Site scan 17:40 (02) Test1 (01) Test2 (07) ori Options
3	To refresh the network search information, press the key to select the submenu and then select “1. Refresh”. The network search is started again.	Site scan 17:40 (02) Test1 (01) Test2 Options 1. Refresh 2. Add 3. Advanced Network confi 17:40 Information Searching...

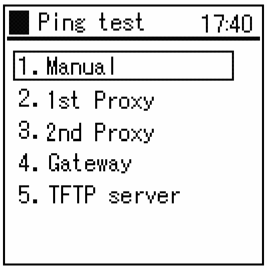
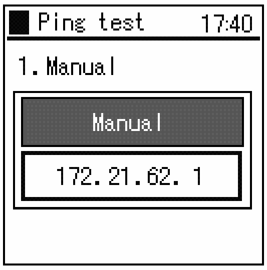
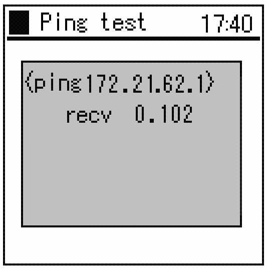
4	Refer to the list of SSIDs for detected access points, select the SSID to be connected to, select submenu by pressing the key, and select “2. Add”. Follow the wizard as in the screen displayed to the right, and each of the network settings can be performed in order.	 Site scan 17:40 (02) Test1 (01) Test2 Options 1. Refresh 2. Add 3. Advanced  Basic info 17:40 Name Config2 Join Method Auto A
5	When checking specific SSID and channel, select the submenu by pressing the key, and select “3. Advanced”. For example, inputting the detected SSID into the “SSID” column in the right-hand diagram and pressing the ◎ key starts the search for that SSID, and the result is displayed. (Also other SSID which has the response is displayed.) In addition, inputting the channel number to be checked into the “Search channel” column and pressing the ◎ key starts the search for that channel, and the result is displayed.	 Site scan 17:40 (02) Test1 (01) Test2 Options 1. Refresh 2. Add 3. Advanced  Advanced 17:40 SSID | Channel flag ,10,11,12,13,14 A

Ping test

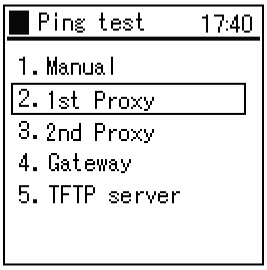
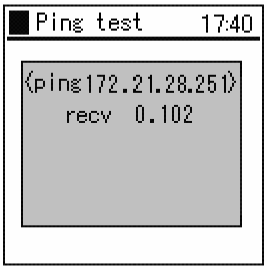
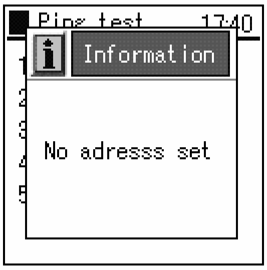
A Ping can be executed for any IP address.

1	From the Network menu, Select “6. Ping test” using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key.	 Network confi 17:40 1.Network config 2.SIP 3.Network reload 4.Certs manager 5.Site scan 6.Ping test

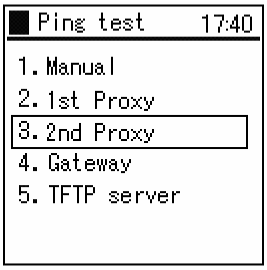
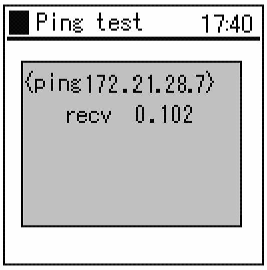
■ Manual Operations

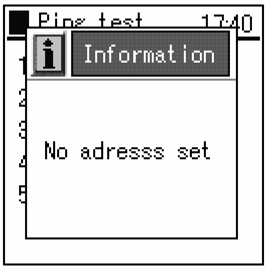
1	From the Ping test menu, Select “1. Manual” using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key.	 Ping test 17:40 1.Manual 2.1st Proxy 3.2nd Proxy 4.Gateway 5.TFTP server
2	Input the IP address to ping, and the ping is started when the ◎ key is pressed. recv : Shows the response to the ping. The following digits show the response time (seconds). time out : Shows that there was no response to the ping. To end the ping, press either the ☎ or the CLR key.	 Ping test 17:40 1.Manual Manual 172.21.62. 1  Ping test 17:40 (ping172.21.62.1) recv 0.102

■ Proxy Server 1

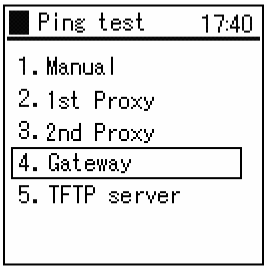
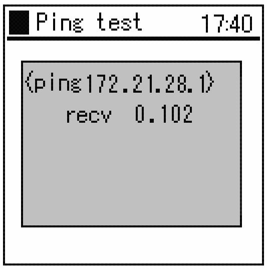
1	From the Ping test menu, Select “2. 1st Proxy” using the ▲▼ keys of the ✥ key, and confirm using the ◎ key.	 Ping test 17:40 1. Manual 2. 1st Proxy 3. 2nd Proxy 4. Gateway 5. TFTP server
2	Proxy server 1 is pinged. **recv** : Shows the response to the ping. The following digits show the response time (seconds). **time out** : Shows that there was no response to the ping. To end the ping, press either the END or the CLR key.	 Ping test 17:40 ⟨ping172.21.28.251⟩ recv 0.102
3	If proxy server 1 is not set, a message as in the diagram on the right is displayed.	 Ping test 17:40 Information No adresss set

■ Proxy Server 2

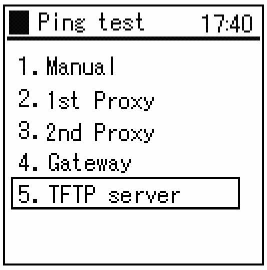
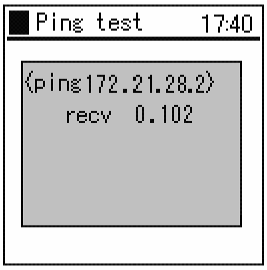
1	From the Ping test menu, Select “3. 2nd Proxy” using the ▲▼ keys of the ✥ key, and confirm using the ◎ key.	 Ping test 17:40 1. Manual 2. 1st Proxy 3. 2nd Proxy 4. Gateway 5. TFTP server
2	Proxy server 2 is pinged. **recv** : Shows the response to the ping. The following digits show the response time (seconds). **time out** : Shows that there was no response to the ping. To end the ping, press either the END or the CLR key.	 Ping test 17:40 ⟨ping172.21.28.7⟩ recv 0.102

3	If proxy server 2 is not set, a message as in the diagram on the right is displayed.	 Ping test 17:40 Information No adress set

■ Default Gateway

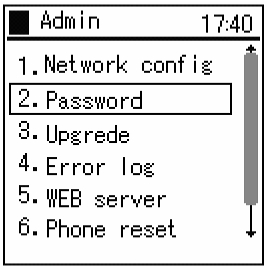
1	From the Ping test menu, Select “4. Gateway” using the ▲▼ keys of the key, and confirm using the ◎ key.	 Ping test 17:40 1. Manual 2. 1st Proxy 3. 2nd Proxy 4. Gateway 5. TFTP server
2	The default gateway is pinged. recv : Shows the response to the ping. The following digits show the response time (seconds). time out : Shows that there was no response to the ping. To end the ping, press either the END or the CLR key.	 Ping test 17:40 ⟨ping172.21.28.1⟩ recv 0.102

■ TFTP Server

1	From the Ping test menu, Select “5. TFTP server” using the ▲▼ keys of the key, and confirm using the ◎ key.	 Ping test 17:40 1. Manual 2. 1st Proxy 3. 2nd Proxy 4. Gateway 5. TFTP server
2	The TFTP server is pinged. recv : Shows the response to the ping. The following digits show the response time (seconds). time out : Shows that there was no response to the ping. To end the ping, press either the END or the CLR key.	 Ping test 17:40 ⟨ping172.21.28.2⟩ recv 0.102

Password

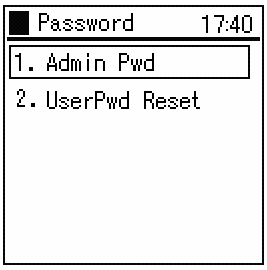
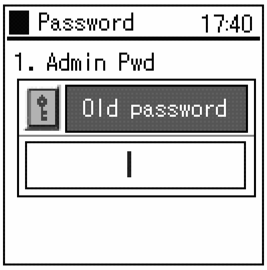
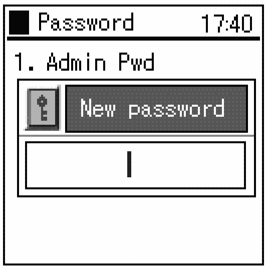
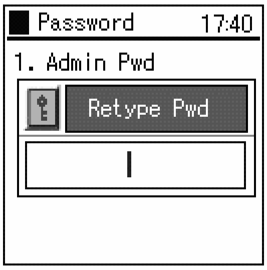
The settings for changing administrator password and resetting user password are configured.

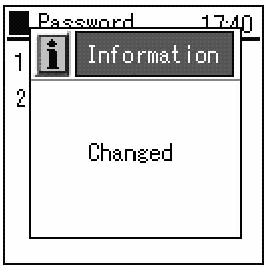
1	From the Admin menu, Select “2. Password” using the ▲▼ keys of the ◉ key, and confirm using the ◎ key.	 Admin 17:40 1. Network config 2. Password 3. Upgrede 4. Error log 5. WEB server 6. Phone reset

Administrator Password

Caution ıf the administrator password is forgotten, contact the sales agent where the purchase was made.

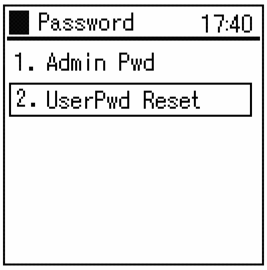
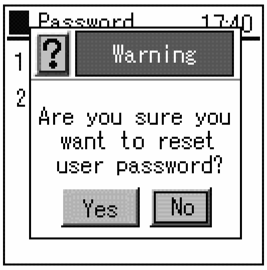
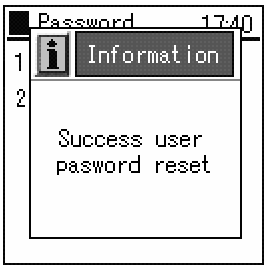
This sets the administrator password.

1	From the Password menu, Select “1. Admin Pwd” using the ▲▼ keys of the ◉ key, and confirm using the ◎ key.	 Password 17:40 1. Admin Pwd 2. UserPwd Reset
2	When “Admin Pwd” is selected, there is a prompt for the current password. Input the correct value, and confirm using the ◎ key. **Notice** The initial value of password is 000000 (6 zeroes).	 Password 17:40 1. Admin Pwd Old password
3	When you input the correct password, the system asks you to input the new password. **Notice** The only characters that can be entered are numerals (0- 9) only. Input a 5 to 7 digit long password.	 Password 17:40 1. Admin Pwd New password
4	For verification, the system asks you to input the new password a second time.	 Password 17:40 1. Admin Pwd Retype Pwd

5	When you input the password, a screen like that on the right is displayed for a few seconds.	 Password 17:40 1 2 Information Changed

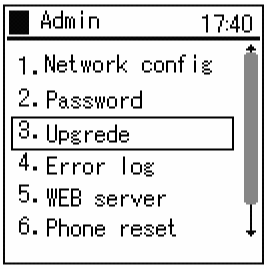
User Password Reset

This resets the user password.

1	From the Password menu, Select “2. UserPwd Reset” using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key.	 Password 17:40 1. Admin Pwd 2. UserPwd Reset
2	Select “Yes” or “No” using the ◀▶ keys of the ⊕ key, and confirm using the ◎ key. **Notice** When the user password is reset, it reverts to the initial value of 0000 (4 zeroes).	 Password 17:40 1 2 Warning Are you sure you want to reset user password? Yes No
3	When “Yes” is selected, the message as shown in the diagram on the right is displayed, and returns to the Password menu.	 Password 17:40 1 2 Information Success user pasword reset

Version Upgrade

Execute version upgrade of firmware / configuration or setting for version upgrade.

1	From the Admin menu, Select "3. Upgrade" using the ▲▼ keys of the key, and confirm using the ◎ key.	 Admin 17:40 1.Network config 2.Password 3.Upgrede 4.Error log 5.WEB server 6.Phone reset

From v2.4.0, you can select which of TFTP or HTTP as a download system with 【UPGRADE】 Request_Mode. Because each setting method differs, refer the chart under.

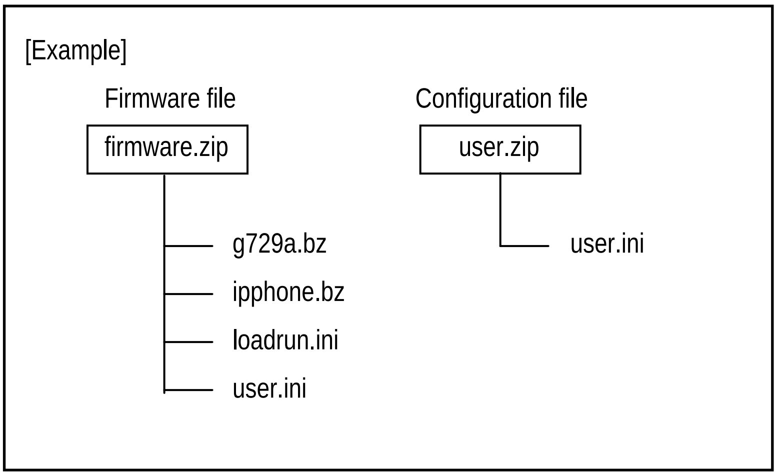
STOP Do not use "%" and space for file name.

download system	setting method	Example of input
TFTP	Setting IP address of TFTP server	192.168.0.1
HTTP	Setting URL and filename of HTTP server http://IP address of HTTP server / filename	http://192.168.0.1/1234.zip

Notice

Beforehand insert the firmware file / configuration file in the directory of the server.

When using HTTP server, each of firmware files (g729a.bz/ipphone.bz/loadrun.ini/user.ini) and configuration file (user.ini) has the necessity to be archive with non compression and the zip type.



[Example]

Version Upgrade

Program

Upgrade the firmware files (g729a.bz/ipphone.bz/loadrun.ini/user.ini) with network connection.

Caution

When upgrading firmware files, present configuration file is overwrited by the configuration file "user.ini" inside the folder. (All items where “∗” is added)

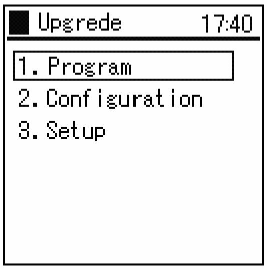
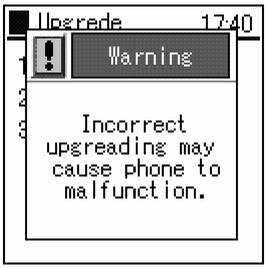
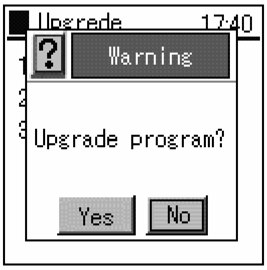
Do backup of the present configuration file (user.ini) to the folder with “Download Configuration File” function of Web settings.

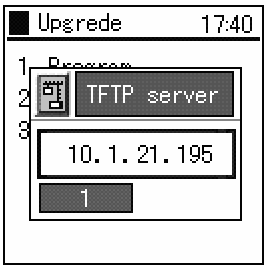
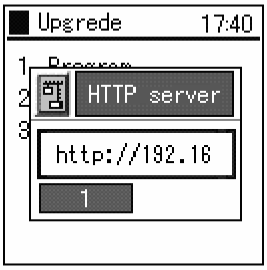
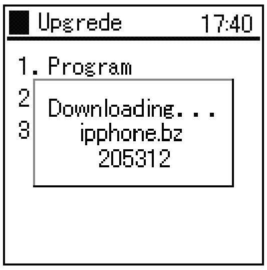
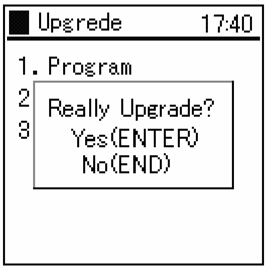
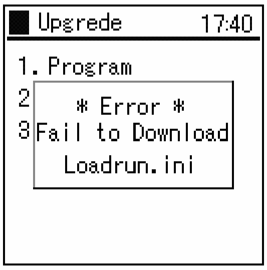
When doing backup, password becomes blank. Set present password to “Vednor_Password". In addition, “Vednor_ID" and “Vednor_Password" in "system" classification must have "∗" like below.

Concerning the editing method of user.ini, refer to the "WirelessIP5000-A User.ini Manual".

```
[SYSTEM]
∗Vendor_ID=
∗Vendor_Password=
```

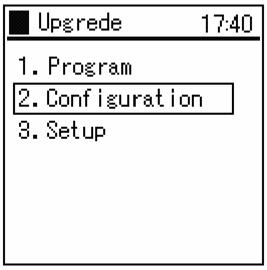
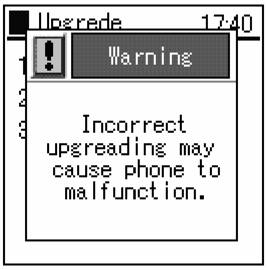
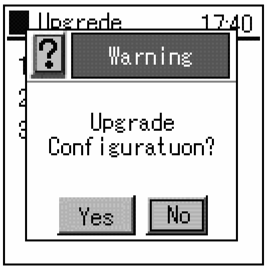
Reference P2-10 Download Configuration File

1	Select “1. Program” by pressing the ◎ key .	 Upgrede 17:40 1. Program 2. Configuration 3. Setup
2	A message is displayed. Press the ◎ key. Select “Yes” or “No” using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key.	 Upgrede 17:40 Warning Incorrect upgreading may cause phone to malfunction.  Upgrede 17:40 Warning Upgrade program? Yes No

3	<In case of TFTP server> If “Yes” is selected, there is a prompt for input of the IP address of the download destination TFTP server. After inputting it, press the ◎ key. <In case of HTTP server> If “Yes” is selected, there is a prompt for input of the URL of the download destination HTTP server and filename. After inputting them, press the ◎ key. Reference P1-35 Version Upgrade Downloading of firmware commences.	 Upgrede 17:40 1. Program 2 3 TFTP server 10.1.21.195 1  Upgrede 17:40 1. Program 2 3 HTTP server http://192.16 1  Upgrede 17:40 1. Program 2 3 Downloading... ipphone.bz 205312
4	When the downloading of firmware completes, a confirmation message is displayed. If “Yes” is selected by pressing the ◎ key, version upgrade of firmware starts. When it completes, the WirelessIP5000E-A is automatically restarted. Caution When in the midst of firmware upgrade, do not cut off power to this product as this may cause failure. **Notice** If the version upgrade fails, message in the right figure is displayed.	 Upgrede 17:40 1. Program 2 3 Really Upgrade? Yes(ENTER) No(END)  Upgrede 17:40 1. Program 2 3 * Error * Fail to Download Loadrun.ini

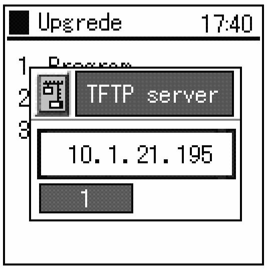
Configuration

Upgrade the configuration file (user.ini) with network connection.

1	Select "2. Configuration" by pressing the ◎ key .	 Upgrede 17:40 1. Program 2. Configuration 3. Setup
2	A message is displayed. Press the ◎ key. Select "Yes" or "No" using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key.	 Upgrede 17:40 Warning Incorrect upgreading may cause phone to malfunction.  Upgrede 17:40 Warning Upgrade Configuratuon? Yes No

3

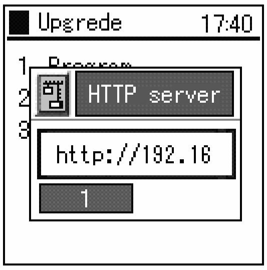
<In case of TFTP server>
If “Yes” is selected, there is a prompt for input of the IP address of the download destination TFTP server. After inputting it, press the ◎ key.



Upgrede 17:40
1 Program
2
3
TFTP server
10. 1. 21. 195
1

<In case of HTTP server>

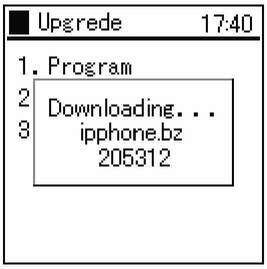
If “Yes” is selected, there is a prompt for input of the URL of the download destination HTTP server and filename. After inputting them, press the ◎ key.



Upgrede 17:40
1 Program
2
3
HTTP server
http://192.16
1

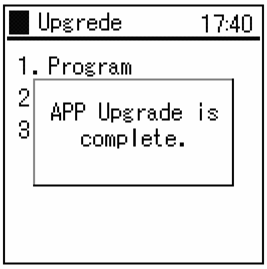
Reference P1-35 Version Upgrade

Downloading of configuration commences.



Upgrede 17:40
1. Program
2
3
Downloading...
ipphone.bz
205312

When it completes, the WirelessIP5000E-A is automatically restarted.



Upgrede 17:40
1. Program
2
3
APP Upgrade is complete.

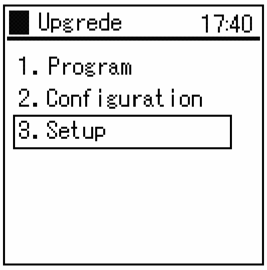
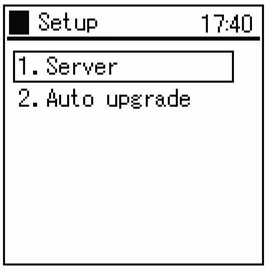
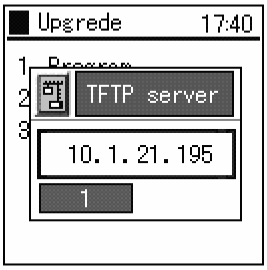
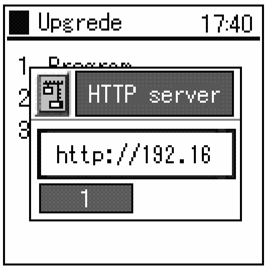
Caution When in the midst of configuration upgrade, do not cut off power to this product as this may cause failure.

Version Upgrade

Setup

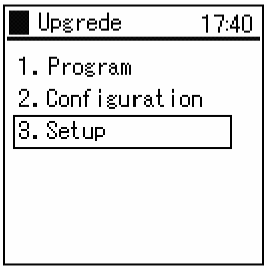
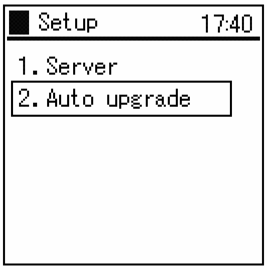
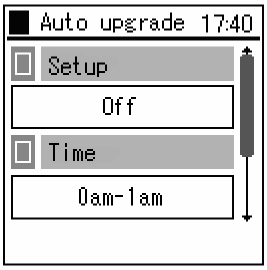
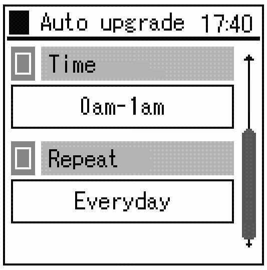
Input setting for version upgrade.

■Server

1	Select "3. Setup" by pressing the ◎ key.	
2	Select "1. Server" by pressing the ◎ key. <In case of TFTP server> Input the IP address of the download destination TFTP server. After inputting it, press the ◎ key. <In case of HTTP server> Input the URL of the download destination HTTP server and filename. After inputting them, press the ◎ key. Reference P1-35 Version Upgrade	  TFTP server 10.1.21.195  HTTP server http://192.16

Version Upgrade

■Auto upgrade

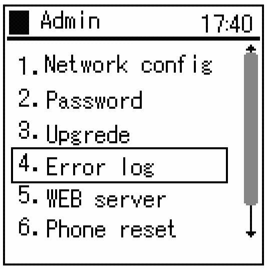
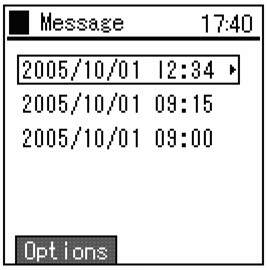
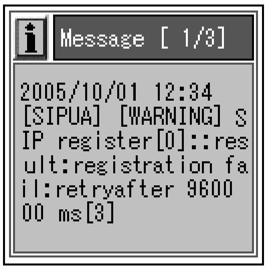
1	Select "3. Setup" by pressing the ◎ key.	 Upgrede 17:40 1. Program 2. Configuration 3. Setup
2	Select "2. Auto upgrade" by pressing the ◎ key. For "Setup", Select "On" or "Off" using the ◀▶ keys of the ⊕ key. For "Time", Select one from "0am-1am" to "11pm-0amf" using the ◀▶ keys of the ⊕ key. **Notice** If selecting "0am-1am" for "Time" at 00:30am, "Auto upgrade" does not operate immediately. When "every day" is selected for "Repeat", "Auto upgrade" operates between 00:00am and 01:00am on next day. When one of day of the week is selected for "Repeat", "Auto upgrade" operates between 00:00am and 01:00am on next week. For "Repeat", Select one from "Everyday" to "Sat" using the ◀▶ keys of the ⊕ key. For "Repeat", "Everyday" or day of the week is selectable. Finally, save using the ◎ key.	 Setup 17:40 1. Server 2. Auto upgrade  Auto upgrade 17:40 Setup Off Time 0am-1am  Auto upgrade 17:40 Time 0am-1am Repeat Everyday

Error Log

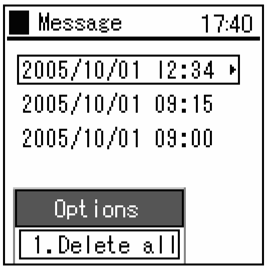
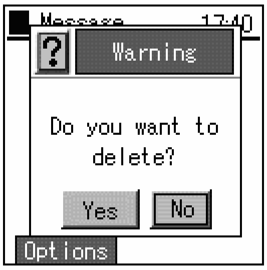
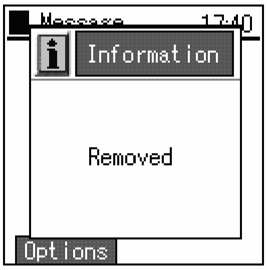
The contents of the error log can be checked.

Notice Error log is displayed, when "Syslog" is available only.

Reference P3-2 Error Log Information

1	From the Admin menu, Select "4. Error log" using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key.	 Admin 17:40 1. Network config 2. Password 3. Upgrede 4. Error log 5. WEB server 6. Phone reset
2	The history for error messages is displayed.	 Message 17:40 2005/10/01 12:34 2005/10/01 09:15 2005/10/01 09:00 Options
3	When an error message is selected from the list, the details for the error are displayed. The first and last error details can be displayed using the ◀▶ keys of the ⊕ key.	 Message [1/3] 2005/10/01 12:34 [SIPUA] [WARNING] S IP register[0]::res ult:registration fa il:retryafter 9600 00 ms[3]

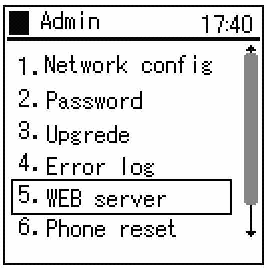
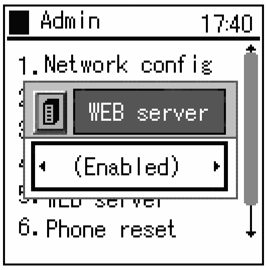
Error Log

4	When deleting error messages, Select “Edit” by pressing the key. select “1. Delete all”, and press the ◎ key. Select “Yes” using the ◀▶ keys of the key, and press the ◎ key. All the error messages are deleted.	 Message 17:40 2005/10/01 12:34 2005/10/01 09:15 2005/10/01 09:00 Options 1.Delete all  Warning Do you want to delete? Yes No Options  Information Removed Options

Notice Error message is retained up to 500.

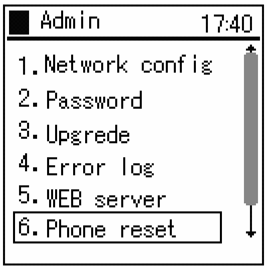
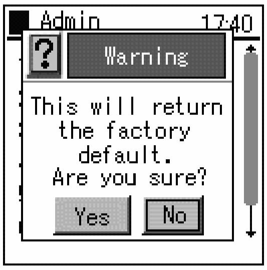
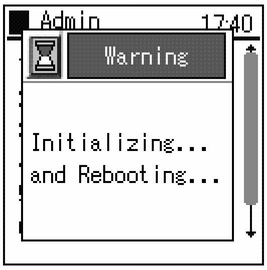
Web Server

Here, the functions of the Web server can be switched ON/OFF.

1	From the Admin menu, Select “4. Web server” using the ▲▼ keys of the ✥ key, and confirm using the ◎ key.	 Admin 17:40 1.Network config 2.Password 3.Upgrede 4.Error log 5.WEB server 6.Phone reset
2	Select “Enabled” or “Disabled” using the ◀▶ keys of the ✥ key, and confirm using the ◎ key.	 Admin 17:40 1.Network config WEB server (Enabled) 6.Phone reset

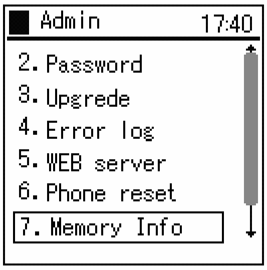
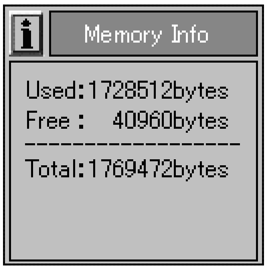
Initializing

Reverts settings to the configuration last uploaded.

1	From the Admin menu, Select “6. Phone reset” using the ▲▼ keys of the key, and confirm using the ◎ key.	 Admin 17:40 1. Network config 2. Password 3. Upgrede 4. Error log 5. WEB server 6. Phone reset
2	Select “Yes” or “No” using the ◀▶ keys of the key, and confirm using the ◎ key. When “Yes” is selected, initialization is started and reverts to the configuration conditions uploaded previously. When initialization completes, the WirelessIP5000E-A is automatically restarted. **Notice** When "Phone reset" is executed, the contents which are modified after last uploading are entirely eliminated.	 Admin 17:40 Warning This will return the factory default. Are you sure? Yes No  Admin 17:40 Warning Initializing... and Rebooting...

Memory Info (Memory Usage)

This displays the memory usage.

1	From the Admin menu, Select “7. Memory Info” using the ▲▼ keys of the ⊕ key, and confirm using the ◎ key.	 Admin 17:40 2. Password 3. Upgrede 4. Error log 5. WEB server 6. Phone reset 7. Memory Info
2	Memory usage is displayed.	 Used:1728512bytes Free : 40960bytes ------------------- Total:1769472bytes

Chapter 2 Web Settings

WirelessIP5000E-A Web Settings

Overview

The WirelessIP5000E-A is able to be configured with Web browser via the Internet. The WirelessIP5000E-A Web settings can configure detailed settings more than key operation

Notice When using web settings, the web server of this product must be set to “Enable”.

The recommended browser is IE5.0 and above

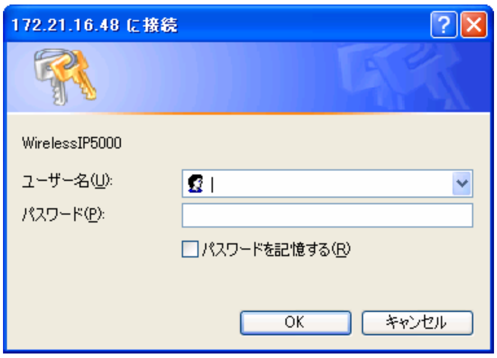
.

When setting via Browser:

Firstly, prepare a PC to be used to configure the WirelessIP5000E-A.
Next, connect the PC to an ethernet port of the access point which WirelessIP5000E-A is connecting to.
Start the browser from the PC to start the WirelessIP5000E-A Web settings, http://<host>: <port> Enter the IP address or host name for the device into <host> and enter the port number into <port>. (the port number is 8080 and cannot be omitted).

Access restrictions

The authentication screen for logging in to the WirelessIP5000E-A web settings is displayed.
Input the username and password that are set in the WirelessIP5000E-A phone and log in.



172.21.16.48 に接続

WirelessIP5000

ユーザー名(U):

パスワード(P):

□パスワードを記憶する(R)

	Management User
Username	admin (default)
Password	000000 (default)
Authority	• setting changes • firmware upgrade and configuration upgrade • admin password changes • stopping the web server

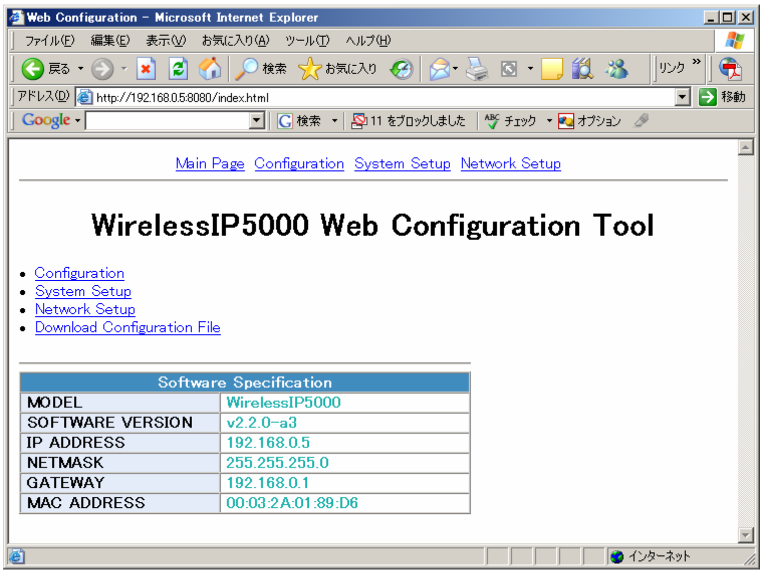
(Note) Simultaneous login of the same user, general user, and management user is possible with multiple browsers (clients).
But it is not recommended.

Management User Menu

You can change settings for the phone, upgrade firmware/configuration, change admin passwords, and stop the web server.

Main

The basic information regarding the phone such as its software version and TCP/IP settings is displayed.


Web Configuration - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る
検索
お気に入り
リンク
アドレス(D)
http://192.168.0.5:8080/index.html
移動
Google
検索
11 をブロックしました
チェック
オプション
インターネット

Main Page Configuration System Setup Network Setup

WirelessIP5000 Web Configuration Tool

- Configuration
- System Setup
- Network Setup
- Download Configuration File

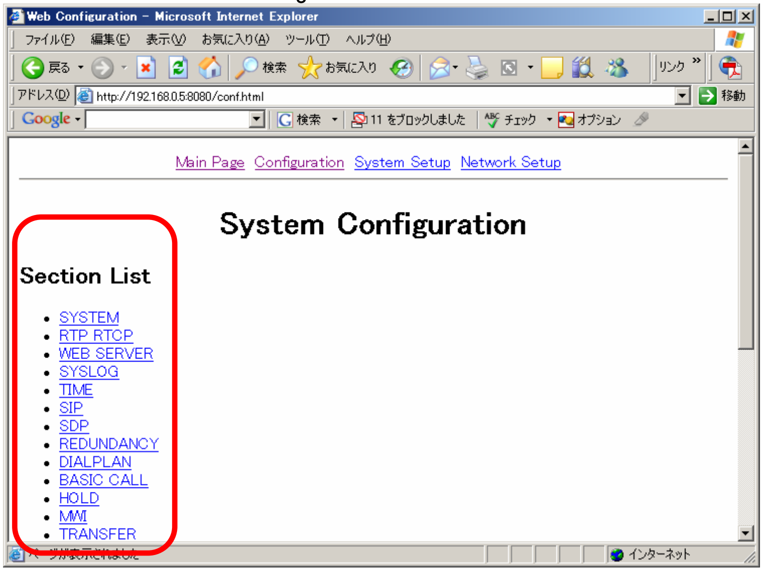
Software Specification	
MODEL	WirelessIP5000
SOFTWARE VERSION	v2.2.0-a3
IP ADDRESS	192.168.0.5
NETMASK	255.255.255.0
GATEWAY	192.168.0.1
MAC ADDRESS	00:03:2A:01:89:D6

[Display Items]
- Model: displays model name
- Software version: displays software version of the WirelessIP5000E-A
- IP address: displays IP address of the phone
- Net mask: displays net mask of the phone
- Default gateway: displays default gateway of the phone
- MAC address: displays MAC address of the phone

Configuration

This is the menu for configuring the product.

1. Select the item to be changed.


Web Configuration – Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り リンク
アドレス(D) 移動
Google 検索 11 をブロックしました チェック オプション
ページが表示されました インターネット

http://192.168.0.5:8080/conf.html

Main Page Configuration System Setup Network Setup

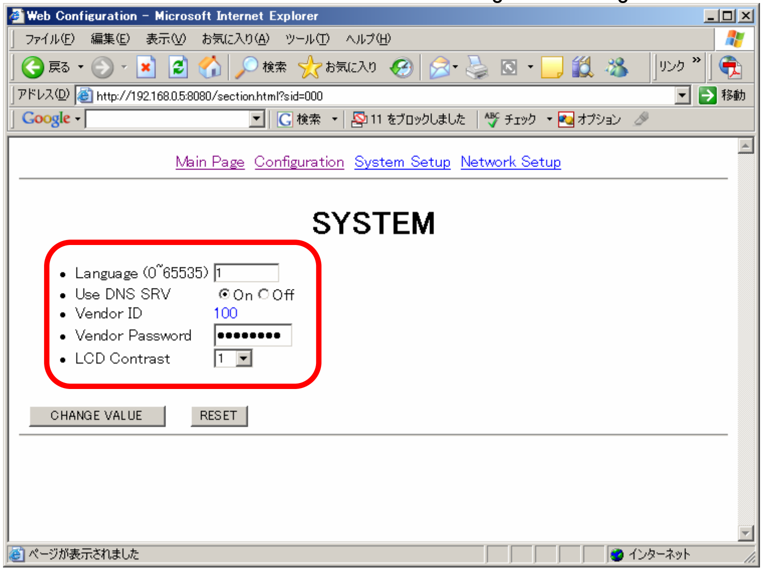
System Configuration

Section List

- SYSTEM
- RTP RTCP
- WEB SERVER
- SYSLOG
- TIME
- SIP
- SDP
- REDUNDANCY
- DIALPLAN
- BASIC CALL
- HOLD
- MWI
- TRANSFER

2. Edit the value. (Example on screen is “SYSTEM”)

3. Click the “CHANGE VALUE” button and change the settings.


Web Configuration – Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り リンク
アドレス(D) 移動
Google 検索 11 をブロックしました チェック オプション
CHANGE VALUE
RESET
ページが表示されました インターネット

http://192.168.0.5:8080/section.html?sid=000

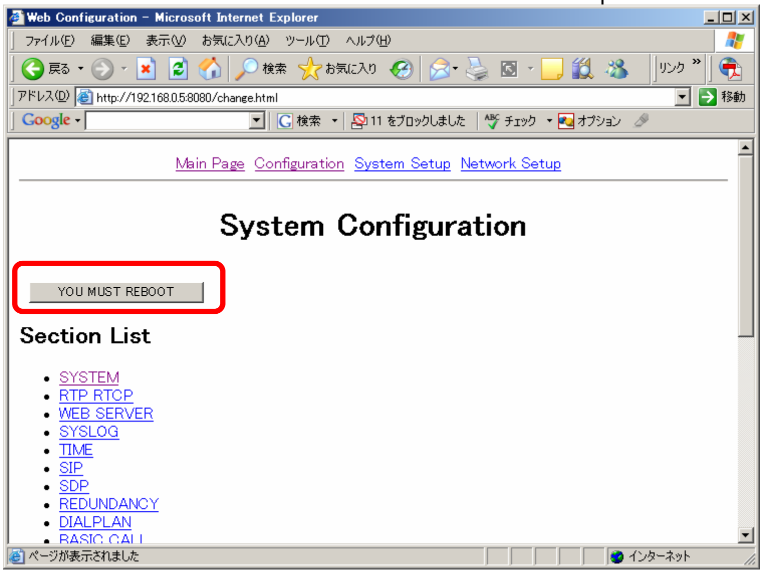
Main Page Configuration System Setup Network Setup

SYSTEM

- Language (0~65535) 1
- Use DNS SRV ● On ○ Off
- Vendor ID 100
- Vendor Password ●●●●●●●●
- LCD Contrast 1

Management User Menu

4. Click the “YOU MUST REBOOT” button and reboot this product.



Web Configuration - Microsoft Internet Explorer
http://192.168.0.5:8080/change.html

Main Page Configuration System Setup Network Setup

System Configuration

YOU MUST REBOOT

Section List

- SYSTEM
- RTP RTCP
- WEB SERVER
- SYSLOG
- TIME
- SIP
- SDP
- REDUNDANCY
- DIALPLAN
- BASIC CALL

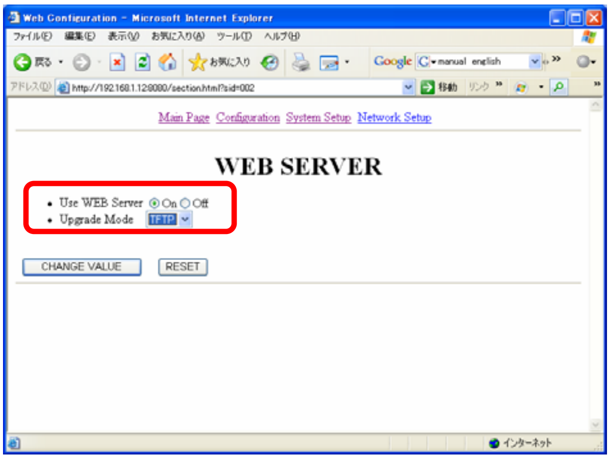
* If this product is not rebooted, the settings are not applied.

* Depending on the item, "YOU MUST REBOOT" button may not be displayed.
For those cases, the settings are applied after the “CHANGE VALUE” button is clicked.

System Setup

The phone’s firmware/configuration can be upgraded, admin user password changed, and the web server can be stopped.

From v2.4.0, you can select which of TFTP or HTTP as a upgrade system of firmware/configuration with 【UPGRADE】 Request_Mode.



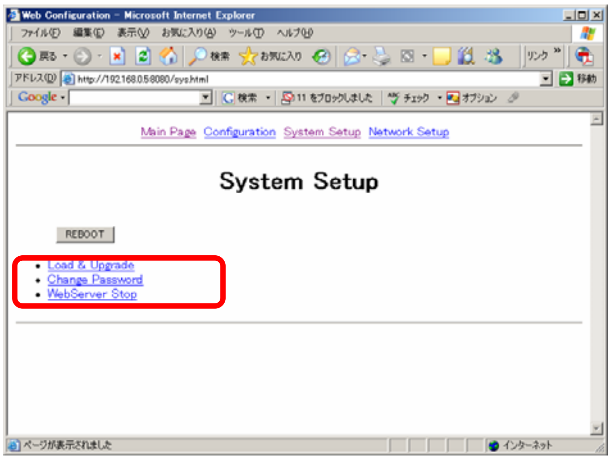
Main Page Configuration System Setup Network Setup

WEB SERVER

- Use WEB Server ● On ○ Off
- Upgrade Mode TFTP

CHANGE VALUE RESET

<In case of TFTP server>



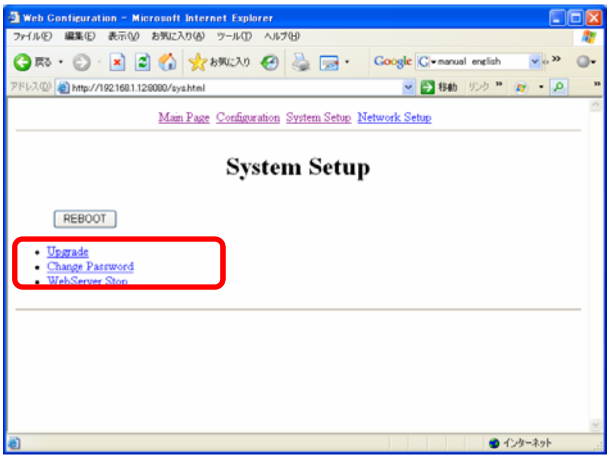
Main Page Configuration System Setup Network Setup

System Setup

REBOOT

- Load & Upgrade
- Change Password
- WebServer Stop

<In case of HTTP server>



Main Page Configuration System Setup Network Setup

System Setup

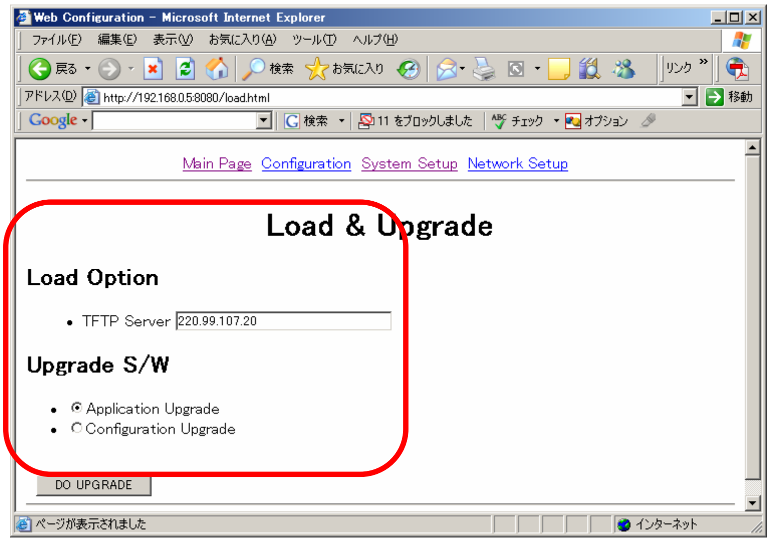
REBOOT

- Upgrade
- Change Password
- WebServer Stop

■ Load & Upgrade

Upgrade the firmware and configuration of this product.

1. Enter the IP address of the TFTP server where the firmware is located.
2. Indicate the type of upgrade (software/config).
3. Click the “DO UPGRADE” button.


Web Configuration – Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り リンク
アドレス(D) http://192.168.0.5:8080/load.html 移動
Google 検索 11 をブロックしました チェック オプション
Main Page Configuration System Setup Network Setup
ページが表示されました
インターネット

Load & Upgrade

Load Option

- TFTP Server 220.99.107.20

Upgrade S/W

- ● Application Upgrade
- ○ Configuration Upgrade

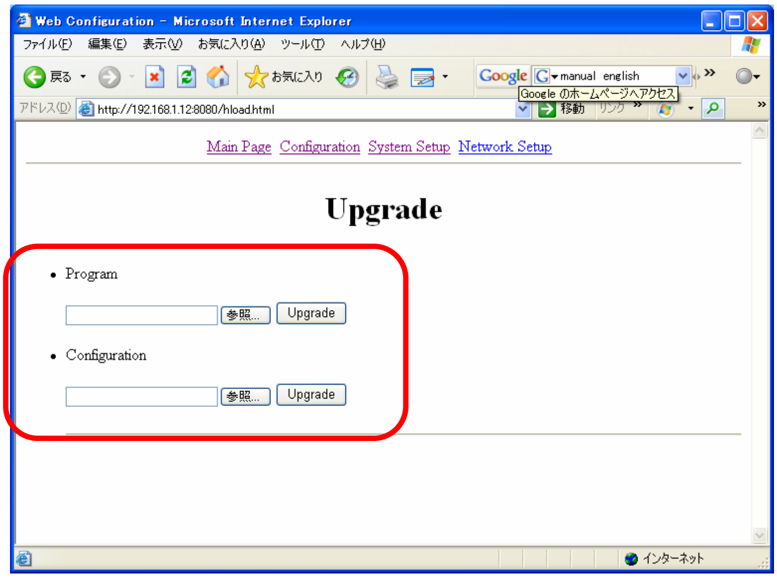
DO UPGRADE

■ Upgrade

Upgrade the firmware and configuration of this product.

Select a firmware file or a configuration file for upgrading, and click the “Upgrade” button.

Notice Each of firmware files (g729a.bz/ipphone.bz/loadrun.ini/user.ini) and configuration file (user.ini) has the necessity to be archive with non compression and the zip type.


Web Configuration – Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る お気に入り
Google manual english
Google のホームページへアクセス
アドレス(D) http://192.168.1.12:8080/hload.html 移動 リンク
Main Page Configuration System Setup Network Setup
インターネット

Upgrade

- Program

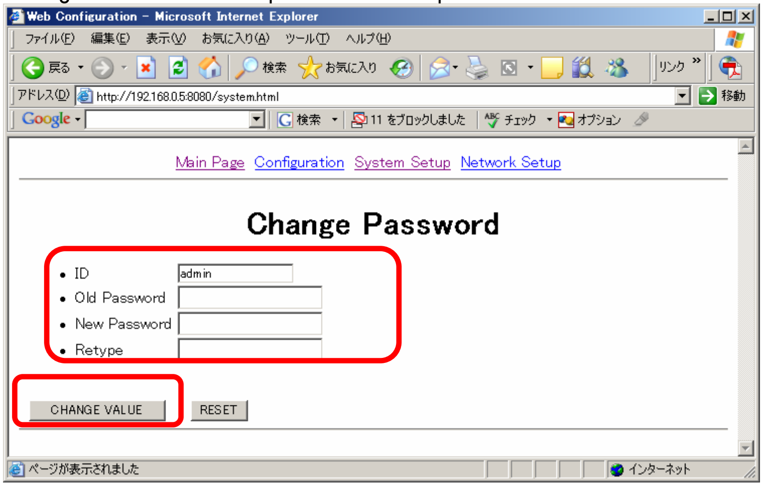
参照... Upgrade

- Configuration

参照... Upgrade

■ Change Password

Change the administrator password of the phone.



Web Configuration - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り リンク
アドレス(D) http://192.168.0.5:8080/system.html 移動
Google 検索 11 をブロックしました チェック オプション
ページが表示されました インターネット

Main Page Configuration System Setup Network Setup

Change Password

- ID admin
- Old Password
- New Password
- Retype

CHANGE VALUE RESET

- Username (admin) is displayed in the ID column. Username cannot be changed.
- Input old password.
- Input new password.
- Input new password (to confirm).

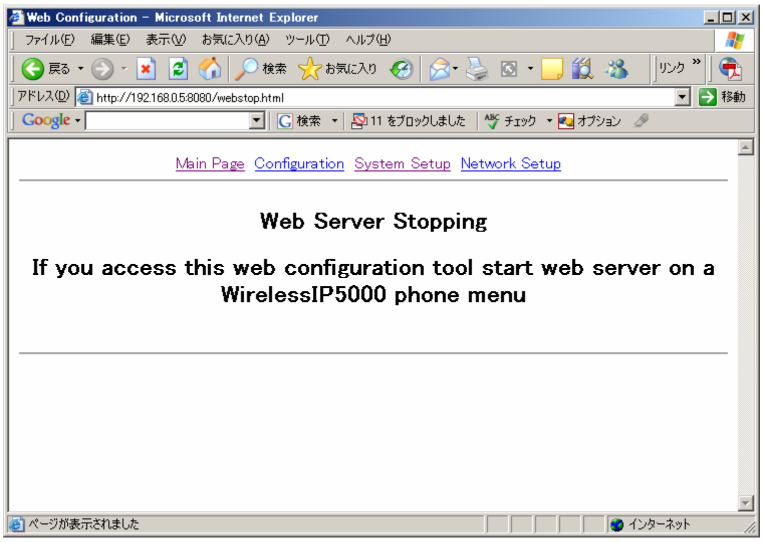
Click the “CHANGE VALUE” button.

* If the inputted information is to be reset, click the “RESET” button.

* Set passwords as 5 -7 digit numerals.

■ Web Server Stop

This stops the web server used for accessing the WirelessIP5000E-A web settings.
Note that access via WWW is not possible during the time the “Web Server Stop” button is clicked.



Web Configuration - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り リンク
アドレス(D) http://192.168.0.5:8080/webstop.html 移動
Google 検索 11 をブロックしました チェック オプション
ページが表示されました インターネット

Main Page Configuration System Setup Network Setup

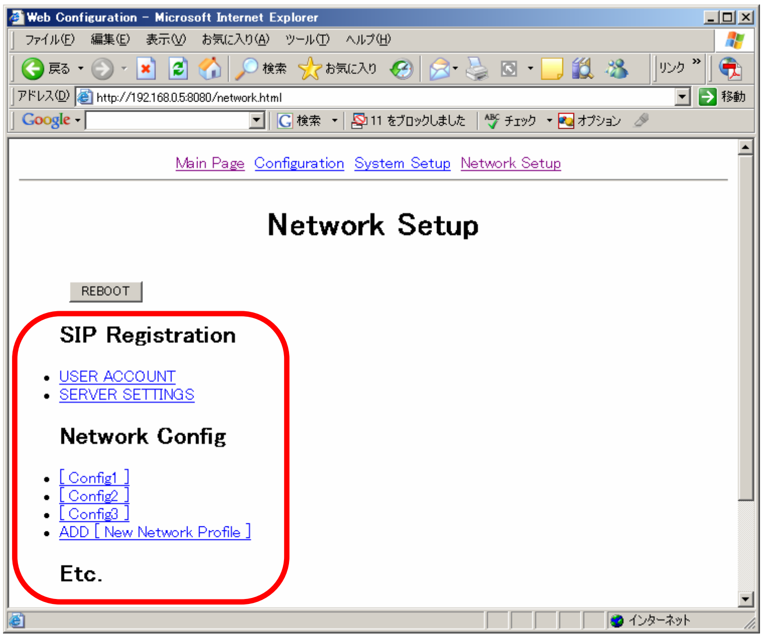
Web Server Stopping

If you access this web configuration tool start web server on a WirelessIP5000 phone menu

Network Setup

Setting Configuration of SIP/Network.

1. Select the item to be changed.


Web Configuration – Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り リンク
アドレス(D) http://192.168.0.5:8080/network.html 移動
Google 検索 11 をブロックしました チェック オプション
インターネット

Main Page Configuration System Setup Network Setup

Network Setup

REBOOT

SIP Registration

- USER ACCOUNT
- SERVER SETTINGS

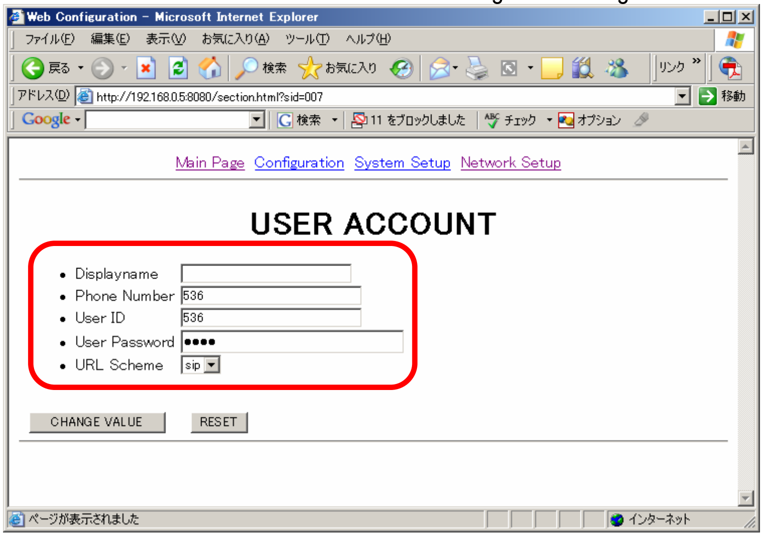
Network Config

- [Config1]
- [Config2]
- [Config3]
- ADD [New Network Profile]

Etc.

2. Edit the value. (Example on screen is “USER ACCOUNT”)

3. Click the “CHANGE VALUE” button and change the settings.


Web Configuration – Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り リンク
アドレス(D) http://192.168.0.5:8080/section.html?sid=007 移動
Google 検索 11 をブロックしました チェック オプション
ページが表示されました
インターネット

Main Page Configuration System Setup Network Setup

USER ACCOUNT

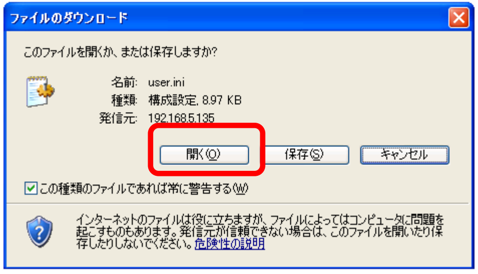
- Displayname
- Phone Number 536
- User ID 536
- User Password ●●●●
- URL Scheme sip

CHANGE VALUE RESET

Download Configuration File

Refer or save a configuration file.

1. Click the “Open” button to refer the configuration file.



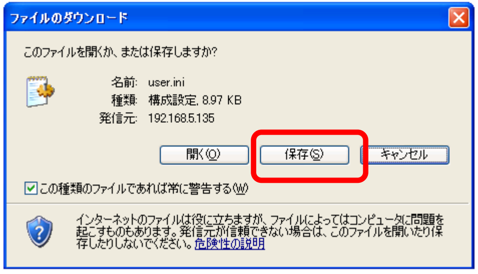
このファイルを開くか、または保存しますか?

名前: user.ini
種類: 構成設定, 8.97 KB
発信元: 192.168.5.135

☑ この種類のファイルであれば常に警告する(W)

インターネットのファイルは役に立ちますが、ファイルによってはコンピュータに問題を起こすものもあります。発信元が信頼できない場合は、このファイルを開いたり保存したりしないでください。危険性の説明

2. Click the “Save” button to save the configuration file.



このファイルを開くか、または保存しますか?

名前: user.ini
種類: 構成設定, 8.97 KB
発信元: 192.168.5.135

☑ この種類のファイルであれば常に警告する(W)

インターネットのファイルは役に立ちますが、ファイルによってはコンピュータに問題を起こすものもあります。発信元が信頼できない場合は、このファイルを開いたり保存したりしないでください。危険性の説明

Notice Password becomes blank, when a configuration file is downloaded.

Chapter 3 Appendix

Error Log Message

Log message	Level	Description
SIP connection Information : SRC IP(%s), PORT(%d)	Info	SIP registeration is completed.
DHCP bind succeeded : IP address(%s)	Info	DHCP binding is completed.
Program upgrade SUCCEEDED : version (%s)!!!	Info	Version up is succeeded.
Program upgrade FAILED : version (%s)!!!	Info	Version up is failed.
Configuration upgrade SUCCEEDED!!!	Info	Configuration update is succeeded.
Configuration upgrade FAILED!!!	Info	Configuration update is failed.
Network Binding : Program Version(%s), Bootrom Version(%s), H/W Version(%s)	Info	Network binding is succeeded after powered on.
Received invalid SIP message	Warning	Invalid SIP messasge is received.
ReINVITE : Non-Supported Payload Type, RemoteIP(%s), Remote Port(%d)	Warning	Non-supported payload type is received.
200OK : Call or Transaction does not exist	Warning	200OK for unknown transaction is received.
BYE : Call/Transaction does not exist	Warning	BYE for unknown transaction is received.
Failure response : Call/Transaction does not exist	Warning	4xx, 5xx or 6xx for unknown transaction is received.
Informative response : Call/Transaction does not exist	Warning	1xx, 2xx or 3xx for unknown transaction is received.
Fail to send SUBSCRIBE for pickup	Warning	Sending SUBSCRIBE for pickup is failed.
Fail to send SUBSCRIBE for presence	Warning	Sending SUBSCRIBE for Presence is failed.
Reigstration[%d] : authentication fail	Warning	Registration with authentication is failed.
Registration[%d] : no response, retry after %d millisecond	Warning	No response from SIP server.
Extension method : Non-supported SIP method(%s)	Warning	Non-supported SIP method is received.
Fail to send SUBSCRIBE for MWI	Warning	Sending SUBSCRIBE for MWI is failed.
Initial-INVITE : invalid ip address in sdp	Error	Initial INVITE with invalid IP address in SDP is received.
Fail to send Subscribe : Send to bad destination address (%s).	Error	Sending SUBSCRIBE with invalid destination address is failed.
DNS : host information for %s not found	Error	No answer from DNS server.

Glossary

ANY Connection	If the SSID of the wireless LAN client is set to ‘ANY connection’, any wireless LAN access point can be connected to. However, access points that reject LAN clients set to ‘ANY connection’ cannot be connected to.
CODEC (COder DECoder)	Algorithm for compressing and decompressing digital video and audio data. This product supports G.711μ-Law, G711A-Law, and G729.
DHCP (Dynamic Host Configuration Protocol)	This is the protocol (communication procedure) for automatically configuring the network settings. The DHCP server automatically configures the network settings for the network’s DHCP clients.
DHCP Server	This is the server that automatically assigns DHCP. Information that can be assigned to client such as IP address, subnet mask, IP address of gateway and DNS server, and the like are set; this information is provided to accessing clients; and when the communications are ended, the address is automatically recovered and assigned to other computers.
DNS (Domain Name System)	Used in TCP/IP networks, this is a system related to the actual IP address and the name affixed to computer.
DNS Server	This is the computer that possesses information related to IP address and name affixed to computer, and that responds to inquiries from outside.
DSCP (DiffServ Code Point)	This is the code (program) for deciding on the actions for routers, etc., in identifying and carrying out transaction processing to suits the types of services (traffic) on the internet with various features such as motion picture and voice. For this purpose, a TOS (type of service) field inside the IP packet is redefined as a DS (DiffServ) field, and in order to decide on actions that the DiffServ target node (such as router) performs on this DS field, a value is set which becomes the basis for quality of service.
IP address	This is the address (location number) affixed for the purpose of distinguishing all connected devices in networks built on TCP/IP protocol.
IP Diffserv	Technology that identifies the types of traffic (this traffic is called services) transmitted and received by internet users, and offers communications quality (QoS: Quality of Service) that satisfies that type.
LAN (Local Area Network)	This is the abbreviation for local area network. It refers to small-scale computer networks.
MAC address value	This is the ID number that is assigned to be unique for each Ethernet card. There is no duplication of this number in Ethernet cards worldwide. This phone also has a unique MAC address.
NAT-Traversal (NAT Translation Function)	This is the mechanism for carrying out address translation for communications between hosts within the organization which have private IP addresses and hosts on the internet having a global IP address. A global IP address is an IP address used on the global internet that is unique, while a private IP address refers to the IP address used only within architectures that are not connected to the internet.
Ping (Packet Internet Groper)	This is the program for diagnosing TCP/IP network such as internet and intranet. When an IP address to be investigated whether or not it is connected is specified, data is sent using ICMP, and the network is diagnosed based on whether the other party replies.
Private-CA	Private (user) certificate used for 802.1x authentication.
Root-CA	Root (certification authority) certificate used for 802.1x authentication.
RTP (Real-time Transport Protocol)	Real-time data transport protocol. RTP is designed on the assumption of being used in applications such as for remote conferencing making use of image and voice, and has the objective of transporting the image and voice data in a form appropriate for real time. In RTP, data is divided into packets based on unit time and transported with the time information of data added to the packets.
SIP (Session Initiation Protocol)	This is one of the call control protocols and used in internet calls employing VoIP, and the like. The transport function, caller number notification function and others, when compared to similar protocols, provide functions close to that of the public telephone network, and the time required for connection is also short.

Glossary

SIP Domain	This is the domain for offering services to the SIP user.
SSID	This is the ID used in wireless LAN communications for identifying the network.
Static NAT(SNAT)	This is the static NAT table settings. Refer to the NAT-Traversal column with regard to NAT.
STUN (Simple Traversal of UDP Through NATs)	Protocol used for traversing NAT using UDP. The traversing of NAT by UDP packets is realized through examining the router's mapping algorithm and the port number mapped to the external address of the NAT router.
Syslog server	Server that collects system logs.
TCP (Transmission Control Protocol)	This is the standard protocol used in internet. It bridges the IP of network layer and the protocols (HTTP, FTP, SMTP, POP, etc) above the session layer.
TCP/IP	This is the standard protocol used in the internet and intranets.
TFTP Server (Trivial File Transfer Protocol)	This is the simple protocol for transporting files between computers connected to the network. It is characterized by having no authentication function and allowing easy usage. It can be used for updating the settings file and firmware of WirelessIP5000E-A.
UPnP (Universal Plug and Play)	Technical specifications for enabling mutual recognition of devices connected to a network such as PC or peripheral devices. It was advocated by Microsoft® in 1999, and is being standardized by the Universal Plug and Play Forum. UPnP gathers together technologies such as XML, DHCP, SOAP, and GENA that are standard to the internet; and has the functionality for auto recognition of devices connected to a network, mutually exchanging information between devices, and exerting control.
Web Server	This refers to a computer that offers contents to be browsed through web browser.
Web Browser	This is an application for browsing web pages.
ciphering	This is the encryption of wireless LAN communications. This WirelessIP5000E-A product supports 5 types of encryption methods, which are "WEP", "WPA-PSK (TKIP)", "WPA2-PSK (AES)", "WPA-EAP (TKIP)" and "WPA2-EAP (AES)" for wireless LAN communications.
Subnet Mask	Within the IP address, this is the numeral that defines which bits are used in network address for distinguishing networks. The portion that is outside the network address becomes the host address for identifying the individual computers within the network.
Server	This is a computer or software that offers data or functionality in own possession to client computers in a computer network.
Signal (dBm)	Shows the wave strength of wireless LAN.
Jitter Buffer	The jitter size that can be tolerated in fulfilling the required quality of conversation differs according to the jitter buffer of the receiving device. The role of the jitter buffer is to store the arriving VoIP packets in the buffer and adjust the latency in the arrival times of packets prior to sending to end user. If the jitter buffer is made bigger the jitter certainly becomes less, but if the size is made too big intolerable delays in conversation are forced onto the end users.
Certificate	This is the data for authenticating the authenticity of the public key used for analyzing digital signatures. Although it is not possible, by the digital signature itself, to confirm whether the public key belongs to the person; based on the digital certificate belonging to the digital signature, it is possible via the certification authority to certify the creator of data as well as there being no tampering of data (this function can be realized by the digital signature itself).
Channel	Wireless LAN uses electromagnetic waves with frequencies in the 2.4 GHz band. The bandwidth is 2.400 to 2.497 GHz, and that range is used divided into 14 channels.
Default Gateway	This refers to device such as computer or router that represents the "entrance and exit" used when accessing computers outside the LAN. With regard to the IP address of an access location, if a specific gateway is not specified, data is sent to the host specified in the default gateway.
Beacon Interval	A Beacon is the packet sent at fixed intervals for the synchronization of wireless LAN communications. The beacon interval is the period of that fixed interval.
Firmware	This is the software incorporated into the device for the basic management of the hardware.

Glossary

Proxy Server	This is the computer that connects to the internet as an "agent" in place of internal computers that cannot directly connect to the internet, and is the boundary between the internet and the internal network of an enterprise.
Protocol	This is the communications procedure that must mutually be in accord when multiple computers are communicating. If the protocol differs, communications are not possible.
Router	This is the device for relaying data that flows in the network to other networks. It has the function of analyzing the protocol, looking at the address and selecting the route. In addition, all data of unsupported protocols is discarded.
Registration Server	This is the server for registering and managing the SIP user information.
IM Server	This is the server for sending or receiving short message in real time. It is possible todisplay the message which WirelessIP received.
Presence Server	This is the server for notifying status of both you and the person whom you want to telephone. It is possible to display the status (talking on the telephone, away from the telephone, etc.) of the person whom you want to telephone.

INDEX

NOTICE
This product is in accordance with the Japanese Foreign Exchange and Foreign Trade Law.

When you plan to export or take this product out to overseas, similar law(s) and/or regulation(s) applicable in your country may require approval or permission from a relative authority.

Our corporate homepage provides updated information and version upgrade services for each product. To use this product in the most appropriate manner it is recommended that this homepage is periodically visited.

Home page: http://www.WirelessIP5000.com/

Copyright© 2006
Hitachi Cable, LTD.

First Edition, February 2006
Second Edition, May 2006
Third Edition, April 2007
Forth Edition, April 2007

HitachiCable
Empowering Energy & Communication