L-04D

ISSUE DATE:

NAME:

PHONE NUMBER:

MAIL ADDRESS:

INSTRUCTION MANUAL

This Device is not intended for the sale in U.S.A

Part 15.21 statement

" Change or Modifications that are not expressly approved by the manufacturer could void the user's authority to operate the equipment.

Part 15.105 statement

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:-Reorient or relocate the receiving antenna.-Increase the separation between the equipment and receiver.-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.-Consult the dealer or an experienced radio/TV technician for help.

FCC Part 15 Class B Compliance

This device and its accessories comply with part 15 of FCC rules and ICES-003 Class B digital apparatus requirements for Industry Canada. Operation is subject to the following two conditions:(1) This device and its accessories may not cause harmful interference, and (2) this device and its accessories must accept any interference received, including interference that may cause undesired operation.

Body-worn Operation

This device was tested for typical body-worn operations with the Wireless Router kept 0.20 inches(0.5cm) between the user's body and the Wireless Router.

To comply with FCC RF exposure requirements, a minimum separation distance of 0.20 inches(0.5cm) must be maintained between the user's body and the Wireless Router.

Third-party belt-clips, holsters and similar accessories containing metallic components should not be used. Body-worn accessories that cannot maintain 0.20 inches(0.5cm) separation distance between the user's body and the Wireless Router, and have not been tested for typical body-Worn operations may not comply with FCC RF exposure Limits and should be avoided.

Display Overview

The signs (icons) that appear on the display indicate these states (press any button to display the icons):

6 Wireless LAN function ON
It disappears when wireless LAN function is OFF.

7 Number of connecting terminals to wireless LAN

8 WPS function available

9 Wi-Fi auto off function set

■ Indicators
The display shows the charging state of battery pack, wireless LAN states, name of the connecting network, etc. (Examples are shown below.)

1 Levels of radio wave reception
Strong ⟷ Weak

圏外:Out of service area or where radio waves do not reach

2 Types of networks available during connection
LTE:LTE
3G: 3G (HSDPA/HSUPA, W-CDMA)

3 Activating global roaming

4 States of network connection
:Connecting
:Not connected
:Pending state of connection

5 Battery level
High ⟷ Low

Blinking: The battery is almost exhausted. Charge the battery.

Charging

Activating WPS function

Battery is exhausted

Activating Wi-Fi

Disconnecting Wi-Fi

Name of the connecting network

Outside the network service area

Using UIM

A UIM is an IC card that stores personal information such as your phone number. Without the UIM installed in this terminal, you cannot use data communication. For details on handling the UIM, refer to the UIM manual.

FOMA card cannot be used in this terminal. If you have the FOMA card, exchange it at a docomo Shop.

Inserting the UIM

When inserting the UIM, hold this terminal with both hands.

- Turn the power off and remove the battery pack before attaching the UIM (- "Attaching and Detaching the Battery Pack").

1 With the IC chip side down, insert a UIM under the UIM slot guide in the direction of arrow.

Removing the UIM

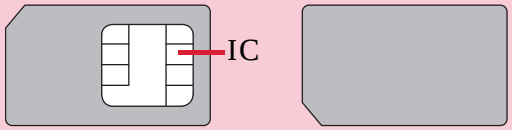
When removing the UIM, hold this terminal with both hands.

- Turn the power off and remove the battery pack before removing the UIM ("Attaching and Detaching the Battery Pack").

1 Slide the UIM in the direction of arrow to remove.

Note

- Do not lose the removed UIM.
- Check both sides of the UIM.



- Be careful not to touch or scratch the UIM IC.
- Inserting a UIM in the reverse direction may cause malfunction.
- Inserting or removing the UIM with an excessive force may cause malfunction to the UIM.
- Do not remove or insert the UIM while this terminal is connected to a PC. It may cause malfunction to the UIM.

For Windows Vista and Windows XP

Confirm that data transmission is terminated before removing the terminal.

1 Double-click  (computer) icon on the desktop.

For Windows XP, double-click My computer.

2 Right-click "リムーバブル ディスク (Removable disk)" icon, and then click "取り出し (Eject)".

3 Double-click "リムーバブル ディスク (Removable disk)" icon.

When the following screen appears, this terminal can be removed safely.

4 Click "キャンセル (Cancel)", and then remove USB Extension Cable from the PC.

5 Remove USB Extension Cable from this terminal.

Turning Power On/Off

Turning Power On

1 When this terminal is turned off, press the power button for approx. 1 second.

When turning power on, wireless LAN function automatically turns ON and network search starts. When this terminal is connected to the network, the network name appears on the display.

Turning Power Off

1 When this terminal is turned on, press the power button for approx. 1 second.

Connecting to Windows PC

The setting procedure when security mode of this terminal is set to "WPA2-PSK/AES" is described here.

For Windows 7 / Windows Vista

1 Press the power button of this terminal for approx. 1 second.

This terminal turns on, and the wireless LAN function turns on.

2 Turn on the wireless LAN function of a PC.

3 (Start) ▶ Click "コントロールパネル (Control panel)" ▶ "ネットワークとインターネット (Network and Internet)" ▶ "ネットワークと共有センター (Network and sharing center)".

"ネットワークと共有センター (Network and sharing center)" window appears.

4 Click "ネットワークに接続 (Connect to a network)".

5 Click the item which shows SSID (Default: "L04D_XXXXXXXX",) set to this terminal, and click "接続 (Connect)".

6 In "セキュリティキーまたはパスフレーズ (Security key or pass phrase)", enter Pre-shared key (WPA2 shared key) set to this terminal, and click "OK".

7 Select "このネットワークを保存します (Save this network)" and "この接続を自動的に開始します (Start this connection automatically)", and then click "閉じる (Close)".
For Windows 7, skip procedure 7.

For Windows XP

1 Press the power button of this terminal for approx. 1 second.
This terminal turns on, and the wireless LAN function turns on.

2 Turn on the wireless LAN function of a PC.

3 Click スタート (Start) ▶ "コントロールパネル (Control panel)" ▶ "ネットワークとインターネット 接続 (Network and Internet)" ▶ "ネットワーク接続 (Network connection)".

4 Double-click "ワイヤレス ネットワーク接続 (Wireless network connection)".

"ワイヤレス ネットワーク接続 (Wireless network connection)" window appears.

5 Click the item which shows SSID (Default: "L04D_XXXXXXXX",) set to this terminal, and click "接続 (Connect)".

6 In "ネット ワークキー (Network key)" and "ネット ワークキーの確認入力 (Confirmation of Network key)", enter WPA2 shared key set to this terminal, and click "接続 (Connect)".

Connecting to Mac

The setting procedure for Mac OS X 10.6 when security mode of this terminal is set to "WPA2-PSK/AES" is described here.

1 Press the power button of this terminal for approx. 1 second.

This terminal turns on, and the wireless LAN function turns on.

2 In the Apple menu, click "システム環境設定… (System environment setting...)" ▶ " ネットワーク (Network)".

3 Select "AirMac", and click "AirMacを入にする (Turn AirMac on)".

The wireless LAN function of Mac turns on.

4 Click "ネットワーク名 (Network name)" and select the item which shows SSID (Default: "L04D_XXXXXXXX",) set to this terminal.

5 In "パスワード (Password)", enter Pre-shared key (WPA2 shared key) set to this terminal, and click "OK".

6 Confirm that SSID of this terminal appears in "ネットワーク名 (Network name)", and click "適用 (Apply)".

Making Other Settings

You can change the settings of this terminal according to your environment by starting Web browser on the PC connected via wireless LAN and displaying the setting page of this terminal.

* You can change this terminal's setting with the console other than a PC, which is equipped with a browser. However, some menus and some browser types may be unavailable.

For details, see "Settings" .

■ WLAN

You can change the settings of wireless LAN and the basic settings of LAN.

■ NETWORK

You can change the settings of access point and UIM.

■ SECURITY

You can set the firewall function of this terminal.

■ SYSTEM

You can use management functions of this terminal, such as saving the settings, confirmation of firmware version, etc.

Internet Connection

To connect to the Internet with this terminal, the subscription to the Internet service provider (mopera U, etc.) compatible with the service and data communication is required.
For details, visit website.

Register the settings for connection with the Internet service provider to Profile of this terminal.
For details on the setting method, refer to "Registering the Access Point Settings (Profile)" .

- Profile can be registered up to 10.
- When connecting this terminal to mopera U, this setting is not necessary.

Connecting to the Internet

You can use the Internet by turning on this terminal to connect automatically to the access point set to the Profile. Check if your wireless LAN terminal is connected to the Internet.
For selection method of access point when multiple Profiles are registered, refer to "Selecting an Access Point (Searching network)" .

Logging-in to L-04D Connection Manager

You can make various settings by starting Web browser on a PC connected via wireless LAN and displaying the setting page (L-04D Connection Manager).

Note

- You can change this terminal's setting with the console other than a PC, which is equipped with a browser. However, some menus and some browser types may be unavailable.
- The setting page of this terminal supports the following Web browsers.
  Windows: Microsoft Internet Explorer 6, 7, 8, 9, Firefox, Chrom
  Mac OS X: Safari 3, 4, 5
  * Depending on the browser, some screens and items may not be displayed.

1 Press the power button of this terminal for approx. 1 second.

This terminal turns on, and the wireless LAN function turns on.

2 Turn on a PC and the wireless LAN function.

This terminal is connected to the PC via wireless LAN.

- When connecting for the first time, wireless LAN setup is required. For setting up, refer to "Connecting to a Wireless LAN Terminal"

3 Start a Web browser, enter "http://192.168.2.1/" in the address entry field and press [Enter].

"Login" screen appears.

- "192.168.2.1" is the default setting of the private IP address of this terminal. When the setting has been changed, enter the private IP address you set ("Setting DHCP Function (DHCP)").

4 Enter "Admin" in [Username] field, enter the log-in password (default: "1234") in [Password] field, and then click [Login].

- In [Language], you can select the language on the setting page.

"Status" screen of the setting page or "PIN verification" screen appears.

5 When "PIN verification" screen appears, enter PIN1 code in [PIN code] field, and then click [Apply].

For details on PIN1 code, see "Security Codes"

"Status" screen of the setting page appears.

The Setting Page Screen

1 Top menu

Click a menu item to switch the setting page.
You can select the following items.

- STATUS
- WLAN
- NETWORK
- SECURITY
- SYSTEM

The submenu appears for some items, and you can switch the setting screen.

2 [Logout]

Click to log out from the setting page.

3 Setting screen

The setting items for the function selected from the menu items appear.

Confirming Connection/Setting Conditions of this Terminal

1 Click [STATUS] in the top menu.

"Status" screen appears.

- Click [Refresh] to refresh the information.

Network selection*:	The connecting band is displayed.
Network name*:	The connecting network name is displayed.
Signal strength*:	The current level of radio wave reception is displayed.
Wi-Fi status:	The status of the wireless LAN function is displayed.
Connected clients:	The number of currently connected terminals via wireless LAN is displayed.
Wi-Fi auto off:	The setting status of the Wi-Fi auto off function is displayed.
WPS:	The operating status of the WPS function is displayed.
UIM card:	The status whether a valid UIM is inserted is displayed.

* When the UIM is not inserted, the items do not appear. On the "Status" screen, "The UIM card has not been detected or is invalid." appears.

Setting Basic Functions of Wireless LAN (Basic setting)

1 In the top menu, click [WLAN].

2 In the submenu, click [Basic setting].

3 On the setting screen, set the required items.

4 Click [Apply] to save the setting.

Setting Wi-Fi auto off Function (Wi-Fi auto off)

1. In the top menu, click [WLAN].
2. In the submenu, click [Wi-Fi auto off].
3. On the setting screen, set the required items.

Wi-Fi auto off (Default: Enable)
Select whether to set the wireless LAN function to off automatically and power saving mode when no client connection is made in a certain period.

- Enable: The wireless LAN function is set to off
- Disable: The wireless LAN function is not set to off

■ When Enable is set

Wi-Fi off time (Default: 10)
When "Enable" is set to Wi-Fi auto off, select the time (minutes) to set automatically to off.

- 10
- 30
- 60

4. Click [Apply] to save the setting.

Setting Security Mode of Wireless LAN (Security)

1. In the top menu, click [WLAN].
2. In the submenu, click [Security].
3. On the setting screen, set the required items.

Security mode (Default: WPA2-PSK)
Select the security mode of wireless LAN.

- Open
- WEP
- WPA-PSK
- WPA2-PSK
- WPA/WPA2-PSK mixed

Depending on the Security mode setting, the following setting items are different.

■ When Open is set

Limitation of clients (Default: 1)
The number of terminals which can be connected is displayed (it cannot be changed.).

■ When WEP is set

WEP key1-4 (Default: XXXXX)
Enter WEP key.
You can enter 5, 10, 13 or 26 letters as a key with one-byte alphanumeric, ". (period)", "- (hyphen)", "_ (under bar)" and "(one-byte space)".
For 10-letter or 26-letter key, use hexadecimal numbers (0-9, A-F).

Current WEP key (Default: 1)
Select the number of WEP key to use.

Limitation of clients (Default: 10)
The number of terminals which can be connected is displayed.

■ When WPA-PSK is set

Encryption type (Default: TKIP)
Select the encryption type.
- AES
- TKIP

WPS shared key (Default: XXXXXXXX)
Enter pre-shared key of WPA.
You can enter 8-64 letters as a key with one-byte alphanumeric, ". (period)", "- (hyphen)", "_ (under bar)" and "(one-byte space)".
For 64-letter key, use hexadecimal numbers (0-9, A-F).

Limitation of clients (Default: 10)
The number of terminals which can be connected is displayed.

■ When WPA2-PSK is set

Encryption type (Default: AES)
Select an encryption type.
- AES
- TKIP

WPA2 shared key (Default: →P41)
Enter pre-shared key of WPA2.
You can enter 8-64 letters as a key with one-byte alphanumeric, ". (period)", "- (hyphen)", "_ (under bar)" and "(one-byte space)".
For 64-letter key, use hexadecimal numbers (0-9, A-F).

Limitation of clients (Default: 10)
The number of terminals which can be connected is displayed.

■ When WPA/WPA2-PSK mixed is set

WPA/WPA2 shared key (Default: XXXXXXXX)
Enter pre-shared key of WPA/WPA2.
You can enter 8-64 letters as a key with one-byte alphanumeric, ". (period)", "- (hyphen)", "_ (under bar)" and "(one-byte space)".
For 64-letter key, use hexadecimal numbers (0-9, A-F).

Limitation of clients (Default: 10)
The number of terminals which can be connected is displayed.

4 Click [Apply] to save the setting.

Setting WPS Function (WPS)

1 In the top menu, click [WLAN].

2 In the submenu, click [WPS].

3 On the setting screen, set the required items.

WPS (Default: Enable)
Select whether to use WPS function.

- Enable: WPS function is used
- Disable: WPS function is not used

■ When Enable is set

WPS type (Default: Push button)
Select a type of WPS function.

- Enable only: When the system is not specified
- Push button: When the terminal has a push button
- WPS PIN: When PIN code for WPS is specified

■ When WPS PIN is set

WPS PIN
Enter the specified PIN code.

4 Click [Apply] to save the setting.

Setting MAC Address Filter (MAC address filter)

1 In the top menu, click [WLAN].

2 In the submenu, click [MAC address filter].

3 On the setting screen, set the required items.

Restrict mode (Default: Disable)
Select an operation mode of MAC address filter function.

- Disable: MAC address filter is not used
- Allow: Allows the connection only to this terminal with the specified MAC address
- Deny: Prohibits the connection to this terminal with the specified MAC address

■ When Allow or Deny is set

Mac address entry field appears.
Enter the specified terminal's MAC address.
You can specify up to 10 MAC addresses.

4 Click [Apply] to save the setting.

Setting DHCP Function (DHCP)

1 In the top menu, click [WLAN].

2 In the submenu, click [DHCP].

3 On the setting screen, set the required items.

IP address (Default: 192.168.2.1)
Set private IP address of this terminal.

Subnet mask (Default: 255.255.255.0)
Set subnet mask of LAN.

DHCP server (Default: Enable)
Select whether to use DHCP function.

- Enable: DHCP function is used
- Disable: DHCP function is not used

■ When Enable is set

Start IP address (Default: 192.168.2.2)
Set the minimum IP address assigned to this terminal.

End IP Address (Default: 192.168.2.99)
Set the maximum IP address assigned to this terminal.

Primary DNS: (Default: 192.168.2.1)
Set IP address of primary DNS server.

Secondary DNS
Set IP address of secondary DNS server.

4 Click [Apply] to save the setting.

Confirming Connection Conditions of Wireless LAN (Connected clients)

1 In the top menu, click [WLAN].

2 In the submenu, click [Connected clients].

3 The connected terminal's information appears.

- Click [Refresh] to refresh the information.

4 To disconnect, click 

in the "Disconnect" field.

Setting uPnP Function (uPnP)

To use the application using the uPnP function, set to "Enable" the uPnP function.

1 In the top menu, click [WLAN].

2 In the submenu, click [uPnP].

3 On the setting screen, set the required items.

uPnP (Default: Disable)
Select whether to use the uPnP function.

- Enable: uPnP function is used
- Disable: uPnP function is not used

4 Click [Apply] to save the setting.

Setting Network

Selecting an Access Point (Searching network)

You can specify the access point network.

- This function is unavailable in Japan.

1 In the top menu, click [NETWORK].

2 In the submenu, click [Searching network].

3 On the setting screen, set the required items.

Mode (Default: Auto)
Select whether to specify the access point.

- Auto: The access point to connect is automatically selected.
- Manual: Select when you specify the access point. Click [Apply] to search the available access point and register it to [Operators].

■ When Manual is set

Operators (Default: none)
Select an access point to connect.

4 Click [Apply] to save the setting.

Registering the Access Point Settings (Profile)

Register, edit or delete the access point settings. You can register up to 10 access points.

- By default, the setting for mopera U is registered and you cannot delete it. When using mopera U, the following setting is not necessary.

1 In the top menu, click [NETWORK].

2 In the submenu, click [Profile].

3 To register a new access point, click [Add New].

■ To edit an existing access point

❶ In [Current profile], select an access point to edit.
❷ Make operation of Procedure 4.
❸ Make operation of Procedure 6.

■ To delete an existing access point

❶ In [Current profile], select an access point to delete.

❷ Click [Delete].

❸ Click [OK].

4 On the setting screen, set the required items.

Profile name (Default: None)
Enter an access point name.

Username (Default: None)
Enter the user name specified by the provider.

Password (Default: None)
Enter the password specified by the provider.

Authentication (Default: CHAP)
Select the authentication method of the access point.

- None
- PAP
- CHAP

APN (Default: Static)
Specify the selection method of the access point.

- Dynamic: The access point is automatically selected.
- Static: Specify the access point. Enter the domain name of the access point in the entry field displayed under the item.

IP type (Default: IPv4)
The IP communication type is displayed (it cannot be changed.).

5 To register a new access point, click [Save].

6 Click [Apply] to save the setting.

Protecting the Terminal with the Security Code (PIN lock)

When this function is set, network communication is locked and entering the security code (PIN1 code) is required when logging in to the setting page.

1 In the top menu, click [NETWORK].

2 In the submenu, click [PIN lock].

3 On the setting screen, set the required items.

PIN lock status
The current setting condition is displayed.

- Enable: PIN lock is set
- Disable: PIN lock is canceled

■ When Enable is set
PIN code to disable
Enter PIN1 code set to the UIM card.

■ When Disable is set
PIN code to enable
Enter PIN1 code set to the UIM card.

4 Click [Apply].

5 When "Enabled" is set, press the power button approx. 1 second to turn the power off, and then turn on again.

Unlocking PIN Lock

If you improperly enter the PIN1 code for 3 times in a row, further entry is locked automatically. In this case, enter "Unblocking PIN Code" to unlock.

1 Enter the unblocking PIN code in [PUK code] field.

If the PIN1 code is improperly entered for 3 times in a row and further entry is locked, enter the unblocking PIN code in [PUK code to unblock] field.

2 Enter the new PIN1 code in the [New PIN code] field.

3 In [Confirm PIN code] field, enter the same PIN1 code as [New PIN code] for confirmation.

4 Click [Apply].

Changing the Security Code (Modify PIN code)

You can change the security code (PIN1 code).

- Changing security code (PIN1 code) is available only when PIN lock is set to "Enabled".

1 In the top menu, click [NETWORK].

2 In the submenu, click [Modify PIN code].

3 On the setting screen, set the required items.

Current PIN code
Enter PIN1 code set to the UIM card.

New PIN code
Set the new PIN1 code.

Confirm PIN code
Enter the same code as [New PIN1 code] for confirmation.

4 Click [Apply].

PIN1 code is changed.

Setting Security Functions

Using Firewall Function (Firewall)

Unauthorized access via the Internet can be blocked by using the Firewall function. Also, you can set IP filter.

1 In the top menu, click [SECURITY].

2 In the submenu, click [Firewall].

3 On the setting screen, set the required items.

Firewall (Default: Disable)
Set whether to activate the Firewall function.

- Enable: Firewall function is activated. You can set IP filter.
- Disable: Firewall function is deactivated.

■ When Enable is set

You can set IP filter.
IP address
When registering IP filter, enter source or destination IP address.
Direction (Default: Destination)
Specify the direction of communication to interrupt.

- Source: Interrupt the access from the specified IP address.
- Destination: Interrupt the access to the specified IP address.

IP address filter list
List of registered IP filter appears.

- 

: Delete registered IP filter.

4 Click [Apply].

Discarding WAN Ping (WAN Ping blocking)

You can discard the Ping request to access from WAN to prevent answering and block the IP information leakage from this terminal and LAN terminals.

1. In the top menu, click [SECURITY].
2. In the submenu, click [WAN Ping blocking].
3. On the setting screen, set the required items.

WAN Ping blocking (Default: Disable)
Set whether to activate the WAN Ping blocking function.

- Enable: Activate the WAN Ping blocking function.
- Disable: Deactivate the WAN Ping blocking function.

4. Click [Apply].

Managing the System

Changing Log-in Password (Modify password)

You can change the log-in password of the setting page.
You can enter only a 4-digit number as a password.

1. In the top menu, click [SYSTEM].
2. In the submenu, click [Modify password].
3. On the setting screen, set the required items.

Current password
Enter the current password.

New password
Enter the new password.

Confirm password
Enter the same password as [New password] for confirmation.

4 Click [Apply].

5 Click [OK].

Saving/Restoring the Setting Data (Backup & Restore)

All setting data can be saved to a PC on which the setting page is opened. Also, saved setting data can be restored in this terminal.

1 In the top menu, click [SYSTEM].

2 In the submenu, click [Backup & Restore].

3 In the setting screen, make the following procedures.

Backup to file
Click [Backup], specify the file name and save the current setting.
* Depending on the browser, the file name cannot be specified.

Restore from file
Click [参照...] (Search), specify the file to restore and click [Apply].

Resetting the Settings (Reset)

You can reset all settings of the setting page to default.

- You can also reset the settings by pressing the buttons on this terminal. For details, see "Resetting this Terminal" (→P84).

1 In the top menu, click [SYSTEM].

2 In the submenu, click [Reset].

3 Click [Reset].

4 Click [OK].

You log out from the setting page and the communication is disconnected.

Confirming the Version Information (Version)

1 In the top menu, click [SYSTEM].

2 In the submenu, click [Version].

The version information of firmware and this terminal appears.

3 Make setting for Software Update.

Check new software (Default: Auto)

- Auto: Check the update file automatically.
- Manual: Check the update file manually.

■ When Auto is set

The confirmation message for software update appears each time you log in. To make the message not to appear, set to "Manual".

■ When Manual is set

Click [Check now] to check if you have any update files, and a message appears when a new file exists.
For update procedure, see "Updating Software" (→P82).

4 When you have changed software update setting, click [Apply].

Displaying the Inquiries (Help)

1 In the top menu, click [SYSTEM].

2 In the submenu, click [Help].

The information of the inquiry website, phone number and the URL of PDF for INSTRUCTION MANUAL appears.