

EMC Technologies Report Number: M061025_Cert_AR5BXB6_NII_BT

APPENDIX I2

FUJITSU NOTEBOOK USER MANUAL (part 2)



Before Using the Wireless LAN

This manual describes the procedures required to properly set up and configure the optional integrated Wireless LAN Mini-PCI device (referred to as "WLAN"). Before using the WLAN device, read this manual carefully to ensure it's correct operation. Keep this manual in a safe place for future reference.



Prior to using the wireless LAN device, be sure to run the Click Me! utility, as detailed in "Installing Click Me!" on page 26.

Wireless LAN Devices Covered by this Document

This document is applicable to systems containing one of the following devices. Most of the procedures are identical. Sections that differ between the devices have been noted in the text:

Intel PRO/Wireless 3945ABG Network Connections (WM3945ABG)

Atheros AR5006EXS Mini-Card Wireless network card (AR5BXB6)

Characteristics of the WLAN Device

The WLAN device is a Mini-PCI card attached to the main board of the mobile computer.

The WLAN devices operate in license-free RF bands, therefore eliminating the need to procure an FCC license to operate. The WLAN devices operate in the 2.4GHz Industrial, Scientific, and Medical (ISM) RF band and in the lower and middle bands of the 5GHz Unlicensed National Information Infrastructure (UNII) bands.

The WLAN devices are capable of three operating modes, IEEE802.11a, IEEE802.11b and IEEE802.11g.

Encoding of data is modulated using Direct Sequence Spread Spectrum (DSSS) and Complementary Code Keying (CCK) when the WLAN device is operating in IEEE 802.11b mode and Orthogonal Frequency Division Multiplexing (OFDM) when operating in IEEE802.11a or IEEE802.11g mode.

The WLAN device is Wi-Fi certified and operates at the maximum data transfer rate of 54 Mbps in IEEE802.11a or IEEE802.11g mode and 11 Mbps in IEEE802.11b mode.

The maximum communication range indoors is approximately 80 feet (25 meters). However, that range will increase or decrease depending on factors such as number of walls, reflective material, or interference from external RF sources.

The WLAN device supports the following encryption methods - WEP, CKIP, TKIP, and AES encryption.

WIRELESS LAN MODES USING THIS DEVICE

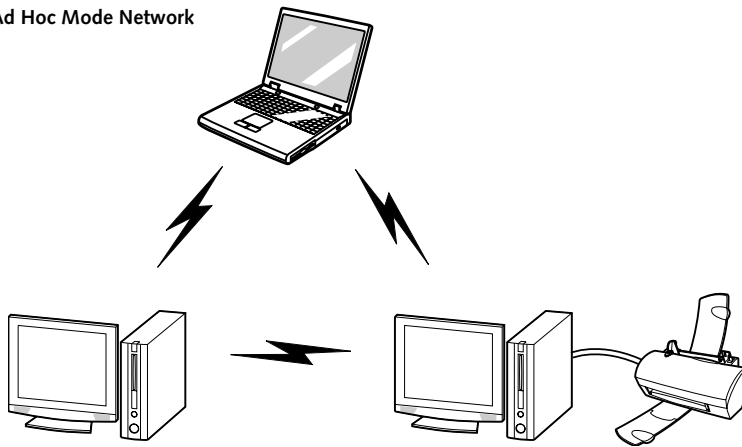
Ad Hoc Mode

(See Figure 5-1)

"Ad Hoc Mode" refers to a wireless network architecture where wireless network connectivity between multiple computers is established without a central wireless network device, typically known as Access Point(s). Connectivity is accomplished using only client devices in a peer-to-peer fashion. That is why Ad Hoc networks are also known as peer-to-peer networks. Ad Hoc networks are an easy and inexpensive method for establishing network connectivity between multiple computers.

Ad Hoc mode requires that the SSID, network authentication, and encryption key settings are identically configured on all computers in the Ad Hoc network.

Figure 5-1. Ad Hoc Mode Network



Access Point (Infrastructure) Mode

(See Figure 5-2)

Infrastructure mode refers to a wireless network architecture in which devices communicate with wireless or wired network devices by communicating through an Access Point. In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. Corporate wireless networks operate in infrastructure mode because they require access to the wired LAN in order to access computers, devices, and services such as file servers, printers, and databases.

How to Handle This Device

The WLAN device comes pre-installed in your mobile computer. Under normal circumstances, it should not be necessary for you to remove or re-install it. The Operating System that your mobile computer comes with has been pre-configured to support the WLAN device.

WIRELESS NETWORK CONSIDERATIONS

- The Intel PRO/Wireless 2915ABG and Atheros AR5002X WLAN devices support IEEE802.11a, IEEE802.11b and IEEE802.11g.
- The WLAN devices operate in the 2.4GHz ISM band and the 5 GHz lower, middle, and upper UNII bands.
- The maximum range of the WLAN device indoors is typically 80 feet (25 meters). Please note that the maximum range you achieve may be shorter or longer than 80 feet, depending on factors such as access point

transmit power, number and density of obstructions, or external RF interference.

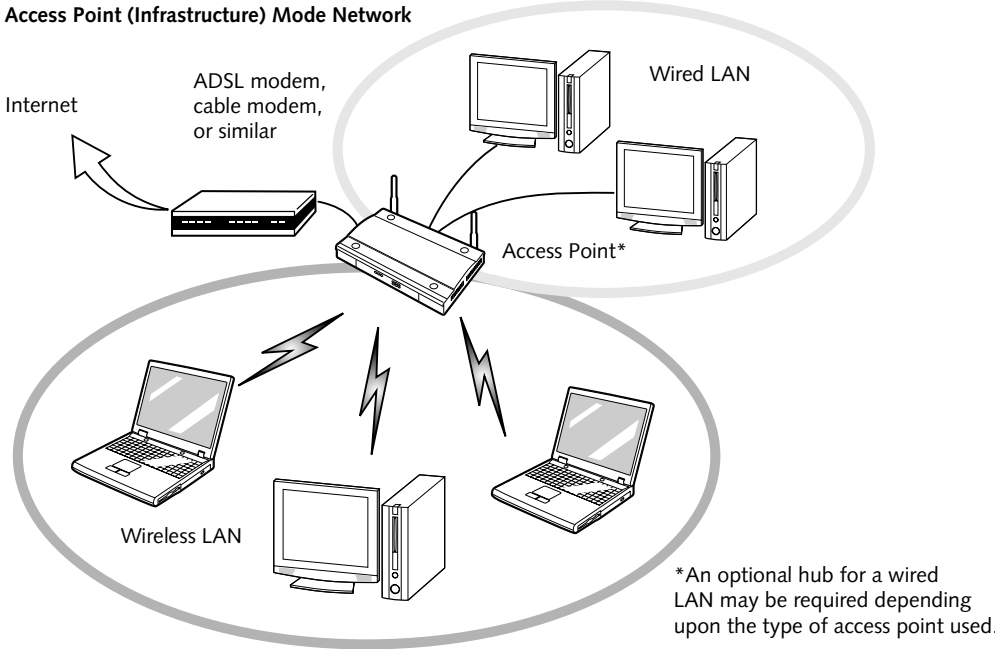
- Microwave ovens will interfere with the operation of WLAN device as microwave ovens operate in the same 2.4GHz frequency range that IEEE802.11b/g devices operate in. Interference by microwaves does not occur with IEEE802.11a radio which operates in the 5 GHz RF band.
- Wireless devices that transmit in the 2.4GHz frequency range may interfere with the operation of WLAN devices in IEEE802.11b/g modes. Symptoms of interference include reduced throughput, intermittent disconnects, and large amounts of frame errors. It is HIGHLY recommended that these interfering devices be powered off to ensure the proper operation of the WLAN device.

DEACTIVATING THE WLAN DEVICE

Deactivation of the WLAN device may be desired in certain circumstances (to extend battery life) or where certain environments require it (i.e. hospitals, clinics, airplanes, etc.). Fujitsu mobile computers employ two methods with which to deactivate the WLAN device:

- Using the Wireless On/Off Switch
- In Windows, using the Intel PROSet Software or Atheros Client Utility software.

Figure 5-2. Access Point (Infrastructure) Mode Network



Deactivation using the Wireless On/Off Switch

The WLAN device can be deactivated quickly and efficiently by toggling the Wireless On/Off Switch to the Off position. (Figure 5-3)

The Wireless On/Off switch has no effect on non-Wireless LAN models.

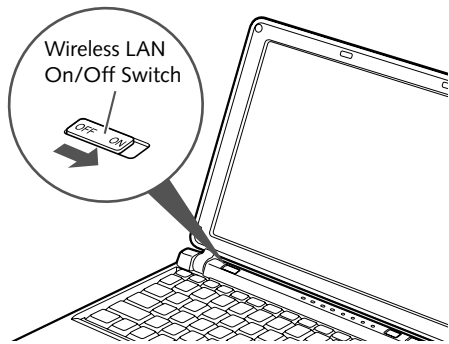


Figure 5-3. Wireless LAN On/Off Switch Location

Deactivation using the Intel PROSet Software

The WLAN device can also be deactivated in Windows using the Intel PROSet Software. The procedure to accomplish this:

1. Click [Start]-> [All Programs].
2. Select Intel ProSet Wireless, then click on Intel ProSet Wireless from the menu that appears. The Intel ProSet Wireless utility will be displayed.
3. At the bottom left corner of the window, select Wireless Off from the dropdown list.

Deactivation using Atheros Client Utility software

1. Right-click on Atheros Client Utility icon in the system tray. Select "Open Atheros Client Utility" from the menu.
2. Choose Action and click Disable Radio.

ACTIVATING THE WLAN DEVICE

Activation of the WLAN device can be accomplished using the same methods as the deactivation process

- Using the Wireless On/Off Switch
- In Windows using the Intel PROSet Software or Atheros Software

Configuration of the WLAN Device

The WLAN Device can be configured to establish wireless network connectivity using one of the following tools:

- **Intel PROSet Software** - The Intel PROSet Software allows for multiple profile setup and supports automatic profile switching. Support for most industry standard security solutions is contained in this software.
- **Atheros Client Utility** - The Atheros Client Utility software allows for multiple profile setups and supports automatic profile switching. Support for most industry standard security solutions is contained in this software.

FLOW OF OPERATIONS

1. Activate the WLAN Device (See Activating the WLAN Device on page 50 for more information).
2. Configure the Wireless Network parameters (See Configure Wireless Network Parameters on page 51 for more information).
 - Enter the network name (SSID)
 - Choose the appropriate WLAN architecture (Ad Hoc or Infrastructure)
 - Choose Authentication method: Open, Shared, WPA-Enterprise, WPA2-Enterprise, WPA-Personal, or WPA2-Personal
 - If using static WEP keys, enter static WEP key and choose key index.
3. Configure network settings (See Configure Network Parameters on page 51 for more information)
 - TCP/IP settings
 - Workgroup or Domain settings.

CONFIGURATION USING INTEL PROSET SOFTWARE

This section explains the procedure to properly configure the WLAN device using the Intel PROSet Software. Pre-defined parameters will be required for this procedure. Please consult with your network administrator for these parameters:

Network Name - Also known as the SSID

Network Key (WEP) - Required if using static WEP keys.

Authentication Type - Open, Shared, WPA, or WPA-PSK

Procedure

1. Activate the WLAN device using either the Wireless On/Off Switch or the Intel PROSet software.
2. Click the [Start] button first and then [All Programs].
3. Click the icon [Intel PROSet Wireless] to execute the Intel PROSet Wireless software.
4. Click the [Add] button. The General Settings dialog displays.
5. Enter a profile name in the Profile Name field.
6. Enter the network SSID, in the Network Name (SSID) field.
7. Click Infrastructure or Ad Hoc for the operating mode.
8. Click [Advanced].
9. The Mandatory Access Point option is only used if Infrastructure mode is selected. Use this option to connect to a specific access point. Enter the MAC address for the access point. Click OK to save the setting and return to the General Settings page.
10. Click [Next].
11. If you are using Cisco CCX, click Cisco Options to enable Cisco CKIP data encryption on the Security Settings page. Check the Cisco Compatible Extensions Options. If you have checked the Cisco's "Mixed-Cell" box in the Advanced Setting, this option must also be checked.
12. Click [OK].
13. Click Next.
14. Select Open, Shared, WPA-Enterprise, WPA2-Enterprise, WPA-Personal, or WPA2-Personal in the Network Authentication options.
15. Select either None, WEP, CKIP (if Enable Cisco Client eXtensions is enabled, use CKIP or WEP), or TKIP for the data encryption.
16. If WEP is selected, select either 64 or 128-bit for the Encryption Level.
17. Select the key index 1, 2, 3 or 4.
18. Enter the WEP key if required. If your network does not employ a 802.1x/EAP security mechanism, please skip to step 24.

19. Click the Enable 802.1x checkbox to enable the 802.1x security option. Please contact your network administrator if configuration of this setting is required.
20. Select the appropriate Authentication Type. Please contact your network administrator if configuration of this setting is required.
21. After selecting your authentication type, enter the user name, domain, and password of the user you have created on the authentication server. The user name and password do not have to be the same as name and password of your current Windows user login.
22. Click [OK] to save the settings.
23. From the Intel ProSet Wireless page, click the new profile name shown in the Profile List. Use the up and down arrows to position the priority of the new profile in the priority list.
24. Click the Connect button to connect to the network.
25. Click [Close] if you want to close the Intel(R) PROSet for Wireless window.

CONFIGURATION USING ATHEROS CLIENT UTILITY SOFTWARE

This section explains the procedure to properly configure the WLAN device using the Atheros Client Utility. Pre-defined parameters will be required for this procedure. Please consult with your network administrator for these parameters:

Network Name - Also known as the SSID

Network Key (WEP) - Required if using static WEP keys.

Authentication Type - Open, Shared, WPA, or WPA-PSK

Procedure

1. Activate the WLAN device using either the Wireless On/Off Switch or the Atheros Client Utility
2. Right-click on the “Atheros Client Utility” icon in the system tray, and select “Open Atheros Client Utility” from the menu.
3. From the Current Status page, click the Profile Management tab.
4. If this is your first time using this utility, highlight the profile [Default] and Click the [Modify] button, otherwise Click the [New] button. The General Settings dialog displays.

5. From the General page, enter a profile name in the Profile Name field.
6. Enter the network SSID, in the SSID1 field. If you wish to create a profile that can connect to up to 3 different wireless networks, SSID's can be entered in the SSID2 and SSID3 fields as well.
7. Click the Security tab.
8. The Security tab allows for the configuration of the Security modes listed in the table below. Please select the radio button of the desired security mode. If these settings are not known to you, please consult with your network administrator for the correct settings.

Field Name	Description
WPA	Enables the use of Wi-Fi Protected Access. Choosing WPA opens the WPA EAP drop-down menu. Options include TLS and PEAP. If these settings are not known to you, please consult with your network administrator for the correct settings.
WPA-PSK	Enables WPA-Pre-Shared Key. Click on the Configure button to enter the WPA Passphrase. If these settings are not known to you, please consult with your network administrator for the correct settings.
802.1x	Enables 802.1x security. If these settings are not known to you, please consult with your network administrator for the correct settings. Choosing this option opens the 802.1x EAP type drop-down menu. Options include TLS, PEAP, and LEAP
Pre-Shared Key	Enables the use of pre-shared keys that are defined on both the access point and the station. This is where static WEP keys are entered. Click the Configure button to fill in the Define Pre-Shared Keys window.
None	No security

9. Click OK
10. Click the Advanced tab
11. The Advanced tab allows for the configuration of the options detailed in the table below.

Field Name	Description
Power Save Mode	Options are Maximum, Normal, or Off
Network Type	Options are AP (Infrastructure) or Ad Hoc
802.11b Preamble	Specifies the preamble setting in 802.11b. The default setting is Short and Long (Access Point mode), which allows both short and long headers in the 802.11b frames. Set to Long Only to override allowing short frames.
Transmit Power Level	Options are 100 mW, 63 mW, 50 mW, and 40 mW.
Wireless Mode	Specifies 5 GHz 54 Mbps, 5 GHz 108 Mbps, 2.4 GHz 11 Mbps, or 2.4 GHz 54 Mbps operation in an access point network.
Wireless Mode when Starting Ad Hoc Network	Specifies 5GHz 54 Mbps, 5 GHz 108 Mbps, 2.4 GHz 11 Mbps, or 2.4 GHz 54 Mbps to start an Ad Hoc network if no matching network name is found after scanning all available modes.

- Click OK
- If the profile you just created does not activate immediately, click the Profile Management tab, highlight the desired Profile, and click Activate.
- Click [Close] if you want to close the Atheros Client Utility.

CONNECTION TO THE NETWORK

This section explains connection to the network.

If there is an administrator of the network, contact the network administrator for data settings.

Setting the network

Perform the “Setting TCP/IP” and “Confirming the computer and work group names” operations required for network connection.

Setting TCP/IP



To change the setting of the IP address, you need to be logged in from Windows as an administrator.

- Click the [Start] button first and then [Control Panel].

- If the Control Panel is in Category view, switch to Classic view by clicking “Switch to Classic View” under Control Panel the left frame. (If you are already in Classic view, “Switch to Category View” will be displayed.)
- Double-click [Network Connections]. A list of currently installed networks will be displayed.
- Right-click [Wireless Network Connection] in the list, and then click [Properties] in the menu displayed. The [Wireless Network Connection Properties] window will be displayed.
- Click the [General] tab if it is not already selected.
- Click [Internet Protocol (TCP/IP)] and then click [Properties]. The [Internet Protocol (TCP/IP) Properties] window will be displayed.
- Set the IP address as follows:
 - For ad hoc connection:** Select [Use the following IP address:] and then enter data for [IP address] and [Subnet mask]. See page 60 for IP address setting.
 - For access point (infrastructure) connection:** If your network uses DHCP, select [Obtain an IP address automatically] and [Obtain DNS server address automatically]. If your network uses static IP addresses, consult with your network administrator for the correct IP address settings.
- Click the [OK] button. Processing will return to the [Wireless Network Connection Properties] window.
- Click the [OK] button.
- Close the [Network Connection] window.

Following this operation, confirm the names of the computer and the workgroup as follows.

Confirming the computer and work group names



To modify the computer name and/or the work group name, you need to be logged in from Windows as an administrator.

- Click the [Start] button, then [Control Panel].
- If the Control Panel is in Category view, switch to Classic view by clicking “Switch to Classic View” under Control Panel the left frame. (If you are already in Classic view, “Switch to Category View” will be displayed.)
- Double-click the [System] icon. The [System Properties] window will be displayed.
- Click the [Computer Name] tab.



5. Confirm the settings of [Full computer name:] and [Workgroup:].

- a. The setting of [Full computer name:] denotes the name for identifying the computer. Any name can be assigned for each personal computer.



To change the name, click [Change] and then proceed in accordance with the instruction messages displayed on the screen.

Enter the desired name in less than 15 ASCII character code format. Identifiability can be enhanced by entering the model number, the user name, and other factors.

- b. [Workgroup name] is the group name of the network. Enter the desired name in less than 15 ASCII character code format.

For ad hoc connection: Assign the same network name to all personal computers existing on the network.

For access point (infrastructure) connection: Assign the name of the work group to be accessed.

6. Click the [OK] button. If a message is displayed that requests you to restart the personal computer, click [Yes] to restart the computer.

Setting the sharing function

Set the sharing function to make file and/or printer sharing with other network-connected personal computers valid.

This operation is not required unless the sharing function is to be used.

The folder and printer for which the sharing function has been set will be usable from any personal computer present on the network.



To share a file and/or the connected printer, you need to be logged in as an administrator.

Setting the Microsoft network-sharing service

1. Click the [Start] button first and then [Control Panel].
2. If the Control Panel is in Category view, switch to Classic view by clicking “Switch to Classic View” under Control Panel the left frame. (If you are already in Classic view, “Switch to Category View” will be displayed.)

3. Double-click [Network Connections]. A list of currently installed networks will be displayed.

4. Right-click [Wireless Network Connection] in the list, and then click [Properties] in the menu displayed. The [Wireless Network Connection Properties] window will be displayed.

5. **If [File and Printer Sharing for Microsoft Networks] is displayed, proceed to step 6.** If [File and Printer Sharing for Microsoft Networks] is not displayed, skip to step 7.

6. Make sure that the [File and Printer Sharing for Microsoft Networks] check box is checked, and then click the [OK] button. Skip to “Setting file-sharing function”.

7. Click [Install]. The [Select Network Component Type] window will be displayed.
8. Click [Service], then click the [Add] button. The [Select Network Service] window will be displayed.
9. Click [File and Printer Sharing for Microsoft Networks] and then click the [OK] button. Processing will return to the [Wireless Network Connection Properties] window, and [File and Printer Sharing for Microsoft Networks] will be added to the list.

10. Click the [Close] button.

Setting the file-sharing function

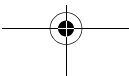
The procedure for setting the file-sharing function follows, with the “work” folder in drive C: as an example.

1. Click the [Start] button first and then [My Computer].
2. Double-click [Local disk (C:)].
3. Right-click the “work” folder (or whichever folder you want to share), and then click [Sharing and Security...] in the menu displayed. The [Folder Name Properties] window will be displayed.

Setting the file-sharing function for the file which has been used to execute Network Setup Wizard is suggested on the screen. For the wireless LAN, however, since security is guaranteed by entry of the network name (SSID) and the network key, the steps to be taken to set the file-sharing function easily without using Network Setup Wizard are given below.



4. Click [Sharing] if it isn’t already selected.





- Click the link stating “If you understand the security risks, but want to share files without running the wizard, click here”.
- Click “Just enable file sharing” and click [OK].
- Check the [Share this folder on the network] check box.



To specify the corresponding folder as a read-only folder, select the [Read only] checkbox under the General tab.

- Click the [OK] button. The folder will be set as a sharable folder, and the display of the icon for the “work.” folder will change.

Setting the printer-sharing function

- Click the [Start] button first and then [Printers and FAX]. A list of connected printers will be displayed.
- Right-click the printer for which the sharing function is to be set, and then click [Sharing] in the menu displayed. The property window corresponding to the selected printer will be displayed.



Setting the printer-sharing function when Network Setup Wizard has been executed is suggested on the screen. For the wireless LAN, however, since security is guaranteed by entry of the network name (SSID) and the network key, the steps to be taken to set the printer-sharing function without using Network Setup Wizard are laid down below.

- Click the [Sharing] tab.
- Click [Share this printer].
- Enter the sharing printer name in [Share name].
- Click the [OK] button.

Confirming connection

After you have finished the network setup operations, access the folder whose sharing has been set for other personal computers. Also, confirm the status of the radio waves in case of trouble such as a network connection failure.



In the case of access point (infrastructure) connection, enter the necessary data for the access point before confirming connection. Refer to the manual of the access point for the access point setup procedure.

Connecting your personal computer to another personal computer

- Click [Start] first and then [My Computer]. The [My Computer] window will be displayed in the left frame.
- Click [My Network Places] in the “Other Places” list. The window [My Network Places] will be displayed.
- Click [View workgroup computers] under Network Tasks in the left frame.
- Double-click the personal computer to which your personal computer is to be connected. The folder that was specified in “Setting the file-sharing function” on page 54 will be displayed.
- Double-click the folder to be accessed.

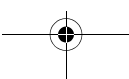
Confirming the status of the radio

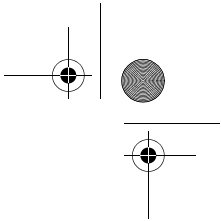
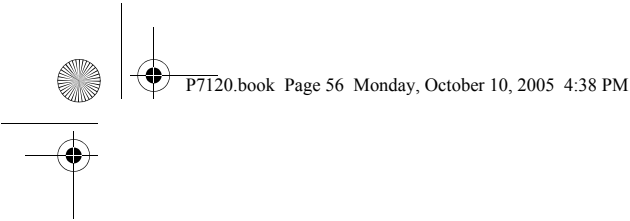
- Right-click the Intel PRO Wireless icon in the lower right corner of the screen.
- Click [Open Intel PROSet for Wireless]. The Intel PROSet for Wireless window opens.
- Contained within the General tab and the Details section (accessed by pressing the [Details] button), you will find the current operating status of the radio. (When the radio is turned off or the computer is not yet connected, some of the conditions will not be displayed.)

- Profile Name**
The current configuration profile is displayed.
- Network Name (SSID)**
Displays the Network Name (SSID) currently used by the radio.
- IP Address**
The IP address of the current profile.
- Signal Quality**
Displays a message stating the current quality of the signal.
- Signal Strength**
Displays a graphic representation of the current signal strength.

Additionally, in the lower section of the display, you will see a variety of different measurements related to the WLAN. For additional information about the items, click on the “Help?” button:

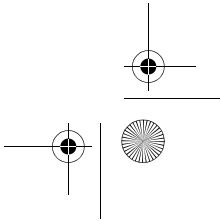
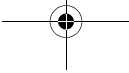
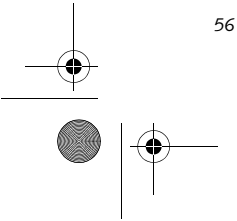
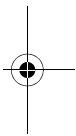
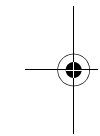
- Adapter MAC Address
- Band
- Supported Data Rates





LifeBook P7000 Series Notebook - Section Five

- Radio Frequency
- Channel Number
- Network Authentication
- Data Encryption
- 802.1x Authentication Type
- 802.1x Authentication Protocol
- CCX Version
- CCX TPC
- CCX Power Levels
- Access Point MAC Address
- Mandatory Access Point

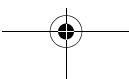


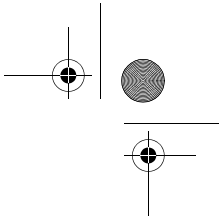
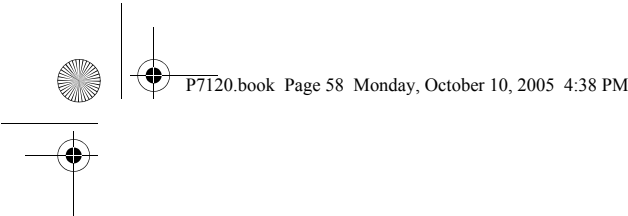


Troubleshooting

Causes and countermeasures for troubles you may encounter while using your wireless LAN are described in the following table.

Problem	Possible Cause	Possible Solution
Unavailable network connection	Incorrect network name (SSID) or network key	Ad hoc connection: verify that the network names (SSID's) and network keys (WEP) of all computers to be connected have been configured correctly. SSID's and WEP key values must be identical on each machine. Access Point (Infrastructure) connection: set the network name (SSID) and network key to the same values as those of the access point. Set the Network Authentication value identically to that of the Access Point. Please consult your network administrator for this value, if necessary. For the method of setting network authentication, refer to the following page:·"Assigning parameters" on page 51·
	Weak received signal strength and/or link quality	Ad hoc connection: Retry connection after shortening the distance to the destination computer or removing any obstacles for better sight. Access Point (Infrastructure) connection: Retry connection after shortening the distance to the access point or removing any obstacles for better sight. To check the wave condition, refer to the following page:· "Confirming the status of the radio waves" on page 55.
	The WLAN device has been deactivated or disabled	Check if the wireless switch is turned ON. Also verify "Disable Radio" is not checked in "Network setting" window. Refer to "Starting Transmission" on page 50.
	The computer to be connected is turned off	Check if the computer to be connected is turned ON.
	RF interference from Access Points or other wireless networks	The use of identical or overlapping RF channels can cause interference with the operation of the WLAN device. Change the channel of your Access Point to a channel that does not overlap with the interfering device.
	Wireless network authentication has failed	Re-check your Network Authentication, Encryption, and Security settings. Incorrectly configured security settings such as an incorrectly typed WEP key, a mis-configured LEAP username, or an incorrectly chosen authentication method will cause the LAN device to associate but not authenticate to the wireless network.
	Incorrectly configured network settings	Recheck the configuration of your network settings. For the method of checking, refer to the following page:·"Connection to the Network" on page 53.
	Incorrect IP address configuration	This only applies to networks using static IP addresses. Please contact your network administrator for the correct settings.





Wireless LAN Glossary

Ad Hoc Mode

Ad Hoc Mode refers to a wireless network architecture where wireless network connectivity between multiple computers is established without a central wireless network device, typically known as Access Points. Connectivity is accomplished using only client devices in a peer-to-peer fashion. For details, refer to “Ad hoc connection” on page 48.

Channel

Range of narrow-band frequencies used by the WLAN device to transmit data. IEEE802.11b/g - 11 channels, 22 MHz wide channels.

DHCP (Dynamic Host Configuration Protocol)

A protocol that provides a means to dynamically allocate IP addresses to computers on a local area network.

DNS (Domain Name System)

A data query service that provides a mechanism with which to translate host names into Internet addresses.

IEEE802.11a

Wireless LAN standard that supports a maximum data rate of 54 Mbps. 802.11a devices operate in the 5 GHz lower and middle UNII bands.

IEEE802.11b

Wireless LAN standard that supports a maximum data rate of 11 Mbps. 802.11b devices operate in the 2.4 GHz ISM band.

Access point

Wireless network device used to bridge wireless and wired network traffic.

IP address

The logical 32-bit host address defined by the Internet Protocol that uniquely identifies a computer on a network. The IP address is usually expressed in dotted decimal notation.

LAN (Local Area Network)

A LAN or Local Area Network is a computer network (or data communications network) which is confined to a limited geographical area.

MAC address (Media Access Control Address)

A MAC address (also called an Ethernet address or IEEE MAC address) is the 48-bit address (typically written as twelve hexadecimal digits, 0 through 9 and A through F, or as six hexadecimal numbers separated by periods or colons, e.g., 0080002012ef, 0:80:0:2:20:ef) which uniquely identifies a computer that has an Ethernet interface.

MTU (Maximum Transmission Unit)

The maximum size of data which can be transmitted at one time in networks including the Internet. In an environment whose maximum size of data is too large to correctly receive data, normal communications can be restored by setting the size of MTU to a smaller value.

Network key

Data that is used for encrypting data in data communication. The personal computer uses the same network key both for data encryption and decryption, therefore, it is necessary to set the same network key as the other side of communication.

Network name (SSID: Security Set Identifier)

When a wireless LAN network is configured, grouping is performed to avoid interference or data theft. This grouping is performed with “Network name (SSID)”. In order to improve security, the network key is set allowing no communication unless “Network name (SSID)” coincides with the network key.

Open system authentication

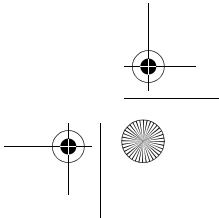
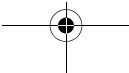
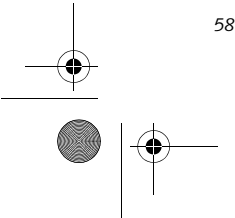
Null authentication method specified in the 802.11 standard that performs no authentication checks on a wireless client before allowing it to associate.

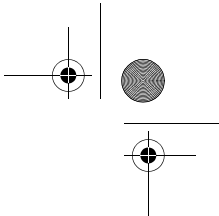
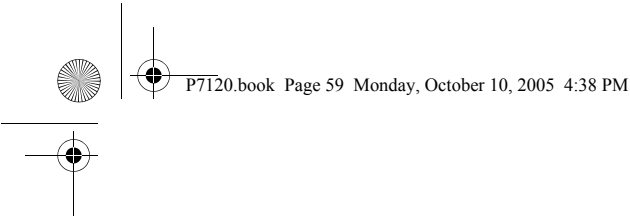
PPPoE (Point to Point Protocol over Ethernet)

A method of allowing the authentication protocol adopted in telephone line connection (PPP) to be used over an Ethernet.

Protocol

A procedure or rule of delivering data among computers. Ordered data communication is allowed by making all conditions required for communication including the method of data transmission/reception and actions upon communication errors into procedures.





Shared key authentication

802.11 network authentication method in which the AP sends the client device a challenge text packet that the client must then encrypt with the correct WEP key and return to the AP. If the client has the wrong key or no key, authentication will fail and the client will not be allowed to associate with the AP. Shared key authentication is not considered secure, because a hacker who detects both the clear-text challenge and the same challenge encrypted with a WEP key can decipher the WEP key.

SSID (Service Set Identifier)

Service Set Identifier, a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because the SSID is broadcast in plain text, it does not supply any security to the network.

Subnet mask

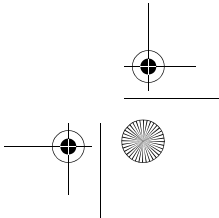
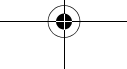
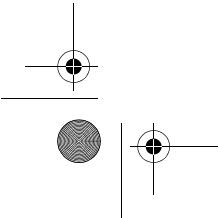
TCP/IP network is controlled by being divided into multiple smaller networks (subnets). IP address consists of the subnet address and the address of each computer. Subnet mask defines how many bits of IP address comprise the subnet address. The same value shall be set among computers communicating with each other.

TCP/IP (Transmission Control Protocol/Internet Protocol)

A standard protocol of the Internet.

Wi-Fi

Wi-Fi, or Wireless Fidelity, is a set of standards for wireless local area networks (WLAN) based on the IEEE 802.11 specifications. Certified products can use the official Wi-Fi logo, which indicates that the product is interoperable with any other product also showing that logo.





IP address information



IP addressing is much more complicated than can be briefly explained in this document. You are advised to consult with your network administrator for additional information.

If IP address is unknown, set IP address as follows:

If you have an access point (DHCP server) on the network, set the IP address as follows:

[Obtain an IP address automatically]



A DHCP server is a server that automatically assigns IP addresses to computers or other devices in the network. There is no DHCP server for the AdHoc network.

If the IP address is already assigned to the computer in the network, ask the network administrator to check the IP address to be set for the computer.

If no access point is found in the network:

An IP address is expressed with four values in the range between 1 and 255.

Set the each computer as follows: The value in parentheses is a subnet mask.

<Example>

Computer A: 192.168.100.2 (255.255.255.0)

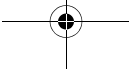
Computer B: 192.168.100.3 (255.255.255.0)

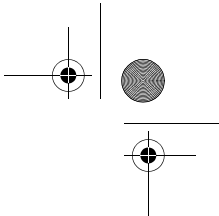
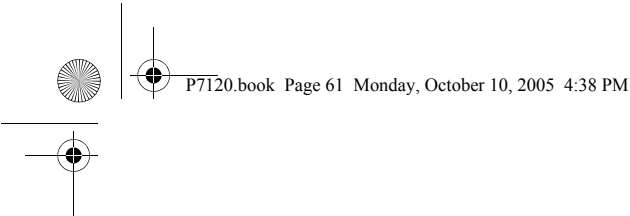
Computer C: 192.168.100.4 (255.255.255.0)

:

:

Computer X: 192.168.100.254 (255.255.255.0)





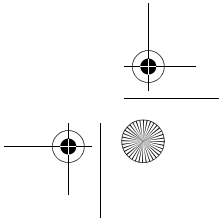
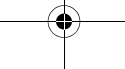
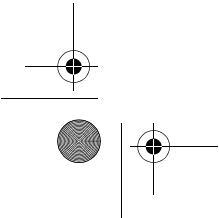
Specifications

Item	Specification
Type of network	The Atheros AR5002X and the Intel PRO/Wireless 2915ABG Network Connections WLAN devices conform to IEEE 802.11a and 802.11b/g (Wi-Fi based)*.
Transfer rate	(Automatic switching) IEEE 802.11a/g: 54 Mbps maximum data rate IEEE 802.11b: 11 Mbps maximum data rate
Active frequency	802.11b/g: 2400~2473 MHz 802.11a: 4900 ~ 5850 MHz
Number of channels	802.11a: 8 independent channels 802.11b/g: 11 channels, 3 non-overlapping channels
Security	Encryption Types - CKIP, WEP, TKIP, AES** WPA 1.0 compliant Encryption Key lengths Supported: 64 bits, 128 bits, and 152 bits (Atheros module using AES encryption only) 802.1x/EAP
Maximum recommended number of computers to be connected over wireless LAN (during ad hoc connection)	10 units or less ***

* “Wi-Fi based” indicates that the interconnectivity test of the organization which guarantees the interconnectivity of wireless LAN (Wi-Fi Alliance) has been passed.

** Encryption with network key (WEP) is performed using the above number of bits, however, users can set 40 bits/104 bits after subtracting the fixed length of 24 bits.

*** Depending on practical environments, the allowable number of computers to be connected may be decreased.





Using the Bluetooth Device

The Integrated Bluetooth module (EYTF3CSFT) is an optional device available for Fujitsu mobile computers.

WHAT IS BLUETOOTH

Bluetooth technology is designed as a short-range wireless link between mobile devices, such as laptop computers, phones, printers, and cameras. Bluetooth technology is used to create Personal Area Networks (PANs) between devices in short-range of each other.



The Wireless LAN/Bluetooth On/Off Switch will power off both the optional wireless LAN and Bluetooth devices at the same time. To enable or disable either one of the devices individually, perform the following steps:

1. Slide the Wireless LAN/Bluetooth on/off switch to On position.
2. In the Control Panel, double-click the Fujitsu Radio Control icon.
3. In the window that appears, click the button associated with Bluetooth and/or Wireless LAN Status to enable or disable the individual devices.
4. Click [OK].

WHERE TO FIND INFORMATION ABOUT BLUETOOTH

The Bluetooth module contains a robust Help user's guide to assist you in learning about operation of the Bluetooth device.

To access the Help file, click [Start] -> All Programs, and click on Toshiba. Select Bluetooth, then select User's Guide.

For additional information about Bluetooth Technology, visit the Bluetooth Web site at: www.bluetooth.com.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

The transmitters in this device must not be co-located or operated in conjunction with any other antenna or transmitter.

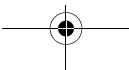
Canadian Notice

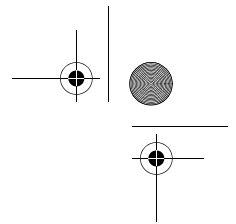
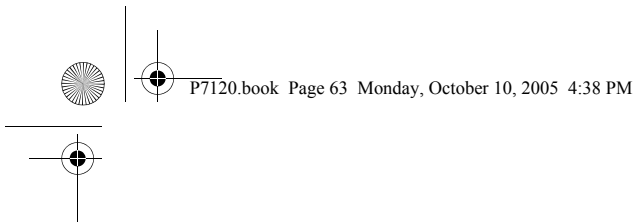
To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

Warranty

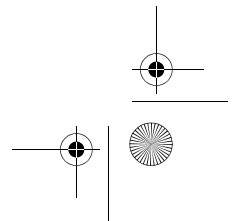
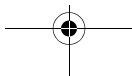
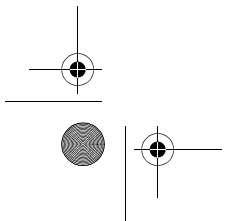
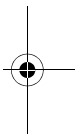
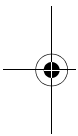
Users are not authorized to modify this product. Any modifications invalidate the warranty.

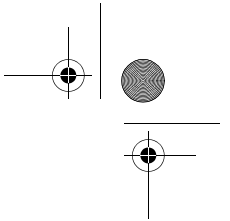
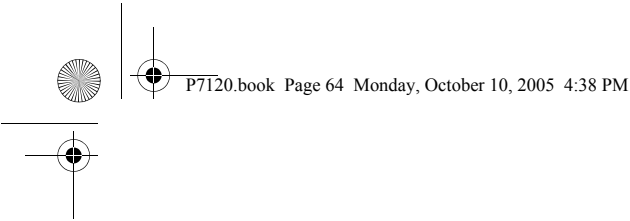
This equipment may not be modified, altered, or changed in any way without signed written permission from Fujitsu. Unauthorized modification will void the equipment authorization from the FCC and Industry Canada and the warranty.



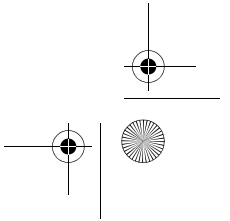
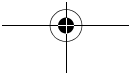
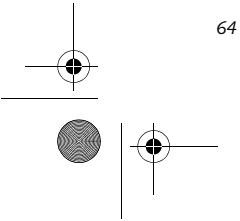
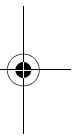
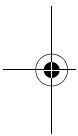


6 Troubleshooting





LifeBook P7000 Notebook – Section Six





Troubleshooting

Troubleshooting

Your Fujitsu LifeBook notebook is sturdy and subject to few problems in the field. However, you may encounter simple setup or operating problems that you can solve on the spot, or problems with peripheral devices, that you can solve by replacing the device. The information in this section helps you isolate and resolve some of these straightforward problems and identify failures that require service.

IDENTIFYING THE PROBLEM

If you encounter a problem, go through the following procedure before pursuing complex troubleshooting:

1. Turn off your LifeBook notebook.
2. Make sure the AC adapter is plugged into your notebook and to an active AC power source.
3. Make sure that any card inserted in the PC Card slot is seated properly. You can also remove the card from the slot, thus eliminating it as a possible cause of failure.
4. Make sure that any devices connected to the external connectors are plugged in properly. You can also disconnect such devices, thus eliminating them as possible causes of failure.
5. Turn on your notebook. Make sure it has been off at least 10 seconds before you turn it back on.
6. Go through the boot sequence.
7. If the problem has not been resolved, refer to the Troubleshooting Table, that follows, for more detailed troubleshooting information.
8. If you are still having problems after referring to the Troubleshooting Table, go to the Fujitsu Computer Systems Support website (<http://www.computers.us.fujitsu.com/support>), and search the list of Frequently Asked Questions (FAQs) contained there.



If you keep notes about what you have tried, your support representative may be able to help you more quickly by giving additional suggestions over the phone.

9. If you have tried the solutions suggested above without success, contact your support representative:
Toll free: 1-800-8Fujitsu (1-800-838-5487)
Fax: 408-764-2724
E-mail: 8fujitsu@us.fujitsu.com
Web site:
<http://www.computers.us.fujitsu.com/support>

Before you place the call, you should have the following information ready so that the customer support representative can provide you with the fastest possible solution:

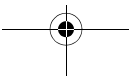
- Product name
- Product configuration number
- Product serial number
- Purchase date
- Conditions under which the problem occurred
- Any error messages that have occurred
- Type of device connected, if any

See the Configuration Label on the bottom of your notebook for configuration and serial numbers.

SPECIFIC PROBLEMS

Using the Troubleshooting Table

When you have problems with your LifeBook notebook, try to find the symptoms under the Problem column of the troubleshooting table for the feature giving you difficulty. You will find a description of common causes for that symptom under the column Possible Cause and what, if anything, you can do to correct the condition under Possible Solutions. All possible causes or solutions may not apply to your notebook.

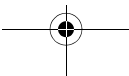




TROUBLESHOOTING TABLE

Problem	Page	Problem	Page
Audio Problems	page 66	USB Device Problems	page 68
Optical Drive Problems	page 66	PC Card Problems	page 68
Floppy Disk Drive Problems	page 67	Power Failures	page 69
Hard Drive Problems	page 67	Shutdown and Startup Problems	page 70
Keyboard or Mouse Problems	page 67	Video Problems	page 71
Memory Problems	page 68	Miscellaneous Problems	page 72
Modem Problems	page 68		

Problem	Possible Cause	Possible Solutions
Audio Problems		
There is no sound coming from the built-in speakers.	The software volume control is set too low.	Adjust the sound volume control settings in your software, operating system and applications. You can also use the [Fn+F9] key combination. Pressing [F9] repeatedly while holding [Fn] will increase the notebook volume.
	Headphones are plugged into your notebook.	Plugging in headphones disables the built-in speakers; remove the headphones.
	BIOS audio settings are incorrect.	Set the BIOS setup utility to the default values within the Multimedia Device Configuration menu. (See BIOS Setup Utility on page 25 for more information)
	Software driver is not configured correctly.	Refer to your application and operating system documentation for help.
	Sound may be set to Mute.	Click on the Volume icon in the system tray and verify that the Mute checkbox is not set. You can also use the [Fn+F3] key combination. Pressing [F3] while holding [Fn] will toggle the audio Mute on and off.
	Device Manager may not be set correctly.	Go to the Control Panel -> System, and click on the Hardware tab. Click the [Device Manager] button and scroll down to “Sound, Video and Game Controllers”. Click the “+” symbol and scroll down the list that appears to see if there is a yellow exclamation point next to any of the items. If there is, you will need to reload the related driver.
DVD/CD-RW Drive Problems		
LifeBook notebook fails to recognize disc in optical drive.	Protective sheet is still in the optical drive tray.	Remove the protective sheet from the tray.
	The disc is not pushed down onto the center of the drive.	Open optical drive tray and re-install the disc properly.
	Optical drive tray is not latched shut.	Push on the front of the optical drive tray until it latches.
	Incorrect DVD Player or no player software is installed.	Install DVD Player software. (See “Using the Optical Drive Software” on page 35 for more information.)
	Wrong drive designator was used for optical drive in the application.	Verify the drive designator used by the application is the same as the one used by the operating system. When the operating system is booted from a DVD/CD, drive designations are automatically adjusted.
	DVD/CD disc is dirty or defective.	Wipe disc with non-abrasive cleaning cloth and reinsert. If it still will not work try a different disc.





Troubleshooting

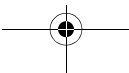
Problem	Possible Cause	Possible Solutions
The Optical Drive Access indicator on the Status Indicator Panel blinks at regular intervals when no disc is in the tray or the drive is not installed.	The Windows auto insertion function is active and is checking to see if a disc is ready to run.	This is normal. However, you may disable this feature. (See <i>Auto Insert Notification Function on page 36 for more information</i>)
Floppy Disk Drive Problems		
You cannot access your optional floppy disk.	You tried to write to a write protected floppy disk.	Eject the floppy disk and set it to write enable. (See <i>Preparing a Disk for Use on page 33 for more information</i>)
	Floppy disk is not loaded correctly.	Eject floppy disk, check orientation and re-insert. (See <i>Ejecting a Disk on page 33 for more information</i>)
	Security is set to protect access to floppy disk data.	Verify your password and security settings.
Hard Drive Problems		
You cannot access your hard drive.	The setup utility is incorrectly set for your internal (Primary Master) or optional second hard drive (Primary Slave).	Revise BIOS settings to set both Primary Master and Primary Slave correctly. (See <i>BIOS Setup Utility on page 25 for more information</i>)
	The wrong drive designator was used by an application when a bootable CD-ROM was used to start the notebook.	Verify drive designator used by application is in use by the operating system. When the operating system is booted from a CD, drive designations are automatically adjusted.
	Security is set so your operating system cannot be started without a password.	Verify your password and security settings.
Keyboard or Mouse Problems		
The built-in keyboard does not seem to work.	The notebook has gone into Suspend mode.	Push the Suspend/Resume/Power On button.
	Your application has locked out your keyboard.	Try to use your integrated pointing device to restart your system. If this fails, turn your notebook off by pressing the Power/Suspend/Resume button for several seconds. After the system has been off for at least 10 seconds, turn it back on.
The characters that appear do not match those which you typed.	NumLk is set in the BIOS.	Go to the BIOS and make sure that NumLk is disabled. (See <i>BIOS Setup Utility on page 25 for more information</i>)
You have installed an external keyboard or mouse, and it does not seem to work.	Your external device is not properly installed.	Re-install your device. (See <i>Device Ports on page 42 for more information</i>)
	Your operating system software is not setup with the correct software driver for that device.	Check your device and operating system documentation and activate the proper driver.





LifeBook P7000 Notebook – Section Six

Problem	Possible Cause	Possible Solutions
You have connected an external keyboard or a mouse and it seems to be locking up the system.	Your operating system software is not setup with the correct software driver for that device.	Check your device and operating system documentation and activate the proper driver.
	Your system has crashed.	Try to restart your notebook. If this fails, turn your notebook off by pressing the Power/Suspend/Resume button for several seconds. After the system has been off for at least 10 seconds, turn it back on.
Memory Problems		
Your Power On screen or Info menu of the BIOS setup utility information do not show the correct amount of memory.	Your memory upgrade module is not properly installed.	Remove and re-install your memory upgrade module. (See <i>Memory Upgrade Module on page 40 for more information</i>)
	You have a memory failure.	Check for Power On Self Test (POST) messages. (See <i>Power On Self Test Messages on page 73 for more information</i>)
Modem Problems		
Messages about modem operation.	Messages about modem operation are generated by whichever modem application is in use.	See your application software documentation for additional information.
USB Device Problems		
You have installed a USB device but your LifeBook notebook does not recognize the device, or the device does not seem to work properly.	The USB port is not enabled in the BIOS.	Verify the USB port is set to Enabled in the BIOS. (See <i>BIOS Setup Utility on page 25 for more information</i>)
	The device is not properly installed.	Remove and re-install the device. (See <i>Device Ports on page 42 for more information</i>)
	The device may have been installed while an application was running, so the notebook is not aware of its installation.	Close the application and restart your notebook.
	Your software may not have the correct software driver active.	See your software documentation and activate the correct driver.
	You may have the wrong I/O address selected for your device.	See your device documentation and software documentation to determine the required I/O address. Change the settings in the BIOS setup utility. (See <i>BIOS Setup Utility on page 25 for more information</i>)
	Your device and another device are assigned the same I/O address.	Check all I/O addresses located within the BIOS setup utility and any other installed hardware or software to make sure there are no duplications.
PC Card Problems		
Card inserted in the PC Card slot does not work or is locking up the system.	The card is not properly inserted.	Remove and re-insert the card. (See <i>PC Cards on page 37 for more information</i>)



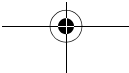
Troubleshooting

Problem	Possible Cause	Possible Solutions
A card inserted in the PC Card slot does not work or is locking up the system. (continued)	The card may have been inserted while an application was running, so your notebook is not aware of its insertion.	Close the application and restart your notebook.
	Your software may not have the correct software driver active.	See your software documentation and activate the correct driver.
	You may have the wrong I/O address selected for your PC Card device.	See your PC Card documentation to determine the required I/O address. Change the settings in the BIOS. (See <i>BIOS Setup Utility on page 25 for more information</i>)
	Your PC Card device and another device are assigned the same I/O address.	Check all I/O addresses located within the BIOS setup utility and any other installed hardware or software to make sure there are no duplications.
Power Failures		
You turn on your notebook and nothing seems to happen.	The installed primary battery is completely discharged, there is no optional second battery installed or there is no Power adapter installed.	Check the Status Indicator Panel to determine the presence and condition of the batteries. (See <i>Status Indicator Panel on page 12 for more information</i>) Install a charged battery or a Power adapter.
	The primary battery is installed but is faulty.	Use the Status Indicator panel to verify the presence and condition of the batteries. (See <i>Status Indicator Panel on page 12 for more information</i>) If a battery is indicating a short, remove that battery and operate from another power source or replace that battery.
	The battery or batteries are low.	Check the Status Indicator Panel to determine the presence and condition of the batteries. (See <i>Status Indicator Panel on page 12 for more information</i>) Use a Power adapter to operate until a battery is charged or install a charged battery.
	The adapter (AC or auto/airline) is not plugged in properly.	Verify that your adapter is connected correctly. (See <i>Power Sources on page 23 for more information</i>)
	The Power adapter (AC or auto/airline) has no power from the AC outlet, airplane seat jack, or the car's cigarette lighter.	Move the AC cord to a different outlet, check for a line switch or tripped circuit breaker for the AC outlet. If you are using an auto/airline adapter in a car make sure the ignition switch is in the On or Accessories position.
	The Power adapter (AC or auto/airline) is faulty.	Try a different Power adapter or install a charged optional second battery.
Your LifeBook notebook turns off all by itself.	The power management parameters are set for auto timeouts which are too short for your operating needs.	Press any button on the keyboard, or move the mouse to restore operation. If that fails, push the Suspend/Resume button. Check your power management settings, or close your applications and go to the Power Savings menu of the setup utility to adjust the timeout values to better suit your operation needs.
	Your power adapter has failed or lost its power source.	Make sure the adapter is plugged in and the outlet has power.



LifeBook P7000 Notebook – Section Six

Problem	Possible Cause	Possible Solutions
Your LifeBook notebook turns off all by itself. (continued)	You are operating on battery power and have ignored a low battery alarm until the battery is at dead battery state and system has gone into Dead Battery Suspend mode.	Install a power adapter and then push the Suspend/Resume button. <i>(See Power Sources on page 23 for more information)</i>
	You have a battery failure.	Verify the condition of the batteries using the Status Indicator panel, and replace or remove any batteries that are shorted. <i>(See Status Indicator Panel on page 12 for more information)</i>
Your LifeBook notebook will not work on battery alone.	The installed batteries are dead.	Replace the battery with a charged one or install a Power adapter.
	No batteries are installed.	Install a charged battery.
	The batteries are improperly installed.	Verify that the batteries are properly connected by re-installing them.
	Your installed batteries are faulty.	Verify the condition of the batteries using the Status Indicator panel and replace or remove any batteries that are shorted. <i>(See Status Indicator Panel on page 12 for more information)</i>
The batteries seem to discharge too quickly.	You are running an application that uses a lot of power due to frequent hard drive or media drive access, or use of a modem or LAN PC card.	Use both the primary battery and an optional second battery and/or use a power adapter for this application when at all possible.
	The power savings features may be disabled.	Check the power management and/or setup utility settings in the Power Savings menu and adjust according to your operating needs.
	The brightness is turned all the way up.	Turn down the brightness adjustment. The higher the brightness the more power your display uses.
	The batteries are very old.	Replace the batteries.
	The batteries were exposed to high temperatures.	Replace the batteries.
	The batteries are too hot or too cold.	Restore the notebook to normal operating temperature. The Charging icon on the Status Indicator panel will flash when the battery is outside its operating range.
Shutdown and Startup Problems		
The Suspend/Resume/Power On button does not work.	Suspend/Resume/Power On button is disabled from the Power menu -> Advanced submenu of the setup utility.	Enable the button from the setup utility.
	You did not hold the button in long enough.	Hold the button longer. This may need to be a few seconds if your application is preventing the CPU from checking for button pushes.
	There may be a conflict with the application software.	Close all applications and try the button again.



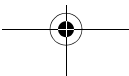
Troubleshooting

Problem	Possible Cause	Possible Solutions
The system powers up, and displays power on information, but fails to load the operating system.	Boot sequence settings of the setup utility are not compatible with your configuration.	Set the operating source by pressing [F12] while the Fujitsu logo is on screen or use the [F2] key and enter the setup utility and adjust the source settings from the Boot menu. <i>(See BIOS Setup Utility on page 25 for more information)</i>
	You have a secured system requiring a password to load your operating system.	Make sure you have the right password. Enter the setup utility and verify the Security settings and modify them as accordingly. <i>(See BIOS Setup Utility on page 25 for more information)</i>
	Internal hard drive was not detected.	Use the BIOS setup utility to try to auto detect the internal hard drive. If this does not work, contact Fujitsu Service and Support at 1-800-8FUJITSU.
An error message is displayed on-screen during the notebook (boot) sequence.	Power On Self Test (POST) has detected a problem.	See the Power On Self Test (POST) messages to determine the meaning and severity of the problem. Not all messages are errors; some are simply status indicators. <i>(See Power On Self Test Messages on page 73 for more information)</i>
Your notebook appears to change setup parameters when you start it.	BIOS setup changes were not saved when you made them and exited the BIOS setup utility returning it to previous settings.	Make sure you select Save Changes And Exit when exiting the BIOS setup utility.
	The BIOS CMOS hold-up battery has failed.	Contact your support representative for repairs. This is not a user serviceable part but has a normal life of 3 to 5 years.
Video Problems		
The built-in display is blank when you turn on your LifeBook notebook.	The notebook is set for an external monitor only.	Pressing [F10] while holding down the [Fn] key allows you to change your selection of where to send your display video. Each time you press the combination of keys you will step to the next choice. The choices, in order are: built-in display only, external monitor only, both built-in display and external monitor.
	The display angle and brightness settings are not adequate for your lighting conditions.	Move the display and the brightness control until you have adequate visibility.
	Power management timeouts may be set for short intervals and you failed to notice the display come on and go off.	Press any button the keyboard, or move the mouse to restore operation. If that fails, push the Suspend/Resume button. (The display may be shut off by Standby mode, Auto Suspend or Video Timeout)
	The notebook is set for S-Video display only.	While holding down the [Fn] key, click on the [F11] key to toggle the S-Video display off.
The notebook turned on with a series of beeps and your built-in display is blank.	Power On Self Test (POST) has detected a failure which does not allow the display to operate.	Contact your support representative.
The display goes blank by itself after you have been using it.	The notebook has gone into Video timeout, or Standby, Suspend, or Hibernation modes because you have not used it for a period of time.	Press any button on the keyboard, or move the mouse to restore operation. If that fails, push the Suspend/Resume button. Check your power management settings to adjust the timeout values to better suit your operation needs. <i>(See BIOS Setup Utility on page 25 for more information)</i>



LifeBook P7000 Notebook – Section Six

Problem	Possible Cause	Possible Solutions
The display goes blank by itself after you have been using it. (continued)	The power management timeouts may be set for very short intervals and you failed to notice the display come on and go off.	Press any button on the keyboard, or move the mouse to restore operation. If that fails, push the Suspend/Resume button. (The display may be shut off by Standby Mode, Auto Suspend or Video Timeout)
The Built-in Display does not close.	A foreign object, such as a paper clip, is stuck between the display and the keyboard.	Remove all foreign objects from the keyboard.
The Built-in Display has bright or dark spots.	If the spots are very tiny and few in number, this is normal for a large LCD display.	This is normal; do nothing.
	If the spots are numerous or large enough to interfere with your operation needs.	Display is faulty; contact your support representative.
The application display uses only a portion of your screen and is surrounded by a dark frame.	You are running an application that does not support 800 x 600/1024 x 768 pixel resolution display and display compression is enabled.	Display compression gives a clearer but smaller display for applications that do not support 800 x 600/1024 x 768 pixel resolution. You can fill the screen but have less resolution by changing your display compression setting, (See the Video Features submenu, located within the Advanced menu of the BIOS. (See <i>BIOS Setup Utility on page 25 for more information</i>)
The display is dark when on battery power.	The default is set on low brightness to conserve power.	Press [Fn] + [F7] to increase brightness and adjust Power Control under battery settings.
You have connected an external monitor and it does not display any information.	Your BIOS setup is not set to enable your external monitor.	Toggle the video destination by pressing [Fn] and [F10] together, or check your BIOS setup and enable your external monitor. (See the Video Features submenu, located within the Advanced Menu of the BIOS. (See <i>BIOS Setup Utility on page 25 for more information</i>)
	Your external monitor is not properly installed.	Reinstall your device. (See <i>External Video Port on page 44 for more information</i>)
	Your operating system software is not setup with the correct software driver for that device.	Check your device and operating system documentation and activate the proper driver.
You connected an external monitor but it doesn't come on.	Your external monitor is not compatible with your LifeBook notebook.	See your monitor documentation and the External Monitor Support portions of the Specifications section. (See <i>Specifications on page 85 for more information</i>)
Miscellaneous Problems		
An error message is displayed on the screen during the operation of an application.	Application software often has its own set of error message displays.	See your application manual and help displays screens for more information. Not all messages are errors some may simply be status.





Troubleshooting

POWER ON SELF TEST MESSAGES

The following is an alphabetic list of error-and-status messages that the Phoenix BIOS and/or your operating system can generate and an explanation of each message. Error messages are marked with an *. If an error message is displayed that is not in this list, write it down and check your operating system documentation both on screen and in the manual. If you can find no reference to the message and its meaning is not clear, contact your support representative for assistance.

nnnn Cache SRAM Passed

Where nnnn is the amount of system cache in kilobytes success-fully tested by the Power On Self Test. (This can only appear if you have an SRAM PC Card inserted.)

*Diskette drive A error or Diskette drive B error

Drive A: or B: is present but fails the BIOS Power On Self Test diskette tests. Check to see that the drive is defined with the proper diskette type in the Setup Utility, (*See BIOS Setup Utility on page 25 for more information*) and that the diskette drive is installed correctly. If the disk drive is properly defined and installed, avoid using it and contact your support representative.

*Extended RAM Failed at offset: nnnn

Extended memory not working or not configured properly. If you have an installed memory upgrade module, verify that the module is properly installed. If it is properly installed, you may want to check your Windows Setup to be sure it is not using unavailable memory until you can contact your support representative.

nnnn Extended RAM Passed

Where nnnn is the amount of memory in kilobytes successfully tested.

*Failing Bits: nnnn The hex number nnnn

This is a map of the bits at the memory address (in System, Extended, or Shadow memory) which failed the memory test. Each 1 (one) in the map indicates a failed bit. This is a serious fault that may cause you to lose data if you continue. Contact your support representative.

*Fixed Disk x Failure or Fixed Disk Controller Failure (where x = 1-4)

The fixed disk is not working or not configured properly. This may mean that the hard drive type identified in your setup utility does not agree with the type detected by the Power On Self Test. Run the setup utility to check for the hard drive type settings and correct them if necessary. If the settings are OK and the message appears when you restart the system, there may be a serious fault which might cause you to lose data if you continue. Contact your support representative.

*Incorrect Drive A type – run SETUP

Type of floppy drive A: not correctly identified in Setup. This means that the floppy disk drive type identified in

your setup utility does not agree with the type detected by the Power On Self Test. Run the setup utility to correct the inconsistency.

*Incorrect Drive B type – run SETUP

Type of floppy drive B: not correctly identified in Setup. This means that the floppy disk drive type identified in your setup utility does not agree with the type detected by the Power On Self Test. Run the setup utility to correct the inconsistency.

*Invalid NVRAM media type

Problem with NVRAM access. In the unlikely case that you see this message you may have some display problems. You can continue operating but should contact your support representative for more information.

*Keyboard controller error

The keyboard controller test failed. You may have to replace your keyboard or keyboard controller but may be able to use an external keyboard until then. Contact your support representative.

*Keyboard error

Keyboard not working. You may have to replace your keyboard or keyboard controller but may be able to use an external keyboard until then. Contact your support representative.

*Keyboard error nn

BIOS discovered a stuck key and displays the scan code for the stuck key. You may have to replace your keyboard but may be able to use an external keyboard until then. Contact your support representative.

*Monitor type does not match CMOS – Run SETUP

Monitor type not correctly identified in Setup. This error probably means your BIOS is corrupted, run the setup utility and set all settings to the default conditions. If you still get this error, contact your support representative.

*Operating system not found

Operating system cannot be located on either drive A: or drive C: Enter the setup utility and see if both the fixed disk, and drive A: are properly identified and that the boot sequence is set correctly. Unless you have changed your installation greatly, the operating system should be on drive C:. If the setup utility is correctly set, your hard drive may be corrupted and your system may have to be re-installed from your back up media.

*Parity Check 1 nnnn

Parity error found in the system bus. BIOS attempts to locate the address and display it on the screen. If it cannot locate the address, it displays ?????. This is a potentially data destroying failure. Contact your support representative.





***Parity Check 2 nnnn**

Parity error found in the I/O bus. BIOS attempts to locate the address and display it on the screen. If it cannot locate the address, it displays ????. This is a potentially data-destroying failure. Contact your support representative.

***Press <F1> to resume, <F2> to SETUP**

Displayed after any recoverable error message. Press the [F1] key to continue the boot process or the [F2] key to enter Setup and change any settings.

***Previous boot incomplete –**

Default configuration used

Previous Power On Self Test did not complete successfully. The Power On Self Test will load default values and offer to run Setup. If the previous failure was caused by incorrect values and they are not corrected, the next boot will likely fail also. If using the default settings does not allow you to complete a successful boot sequence, you should turn off the power and contact your support representative.

***Real time clock error**

Real-time clock fails BIOS test. May require board repair. Contact your support representative.

***Shadow RAM Failed at offset: nnnn**

Shadow RAM failed at offset nnnn of the 64k block at which the error was detected. You are risking data corruption if you continue. Contact your support representative.

nnnn Shadow RAM Passed

Where nnnn is the amount of shadow RAM in kilobytes successfully tested.

***System battery is dead – Replace and run SETUP**

The BIOS CMOS RAM memory hold up battery is dead. This is part of your BIOS and is a board mounted battery which requires a support representative to change. You can continue operating but you will have to use setup utility default values or reconfigure your setup utility every time you turn off your notebook. This battery has an expected life of 2 to 3 years.

System BIOS shadowed

System BIOS copied to shadow RAM.

***System CMOS checksum bad – run SETUP**

BIOS CMOS RAM has been corrupted or modified incorrectly, perhaps by an application program that changes data stored in BIOS memory. Run Setup and reconfigure the system.

***System RAM Failed at offset: nnnn**

System memory failed at offset nnnn of in the 64k block at which the error was detected. This means that there is a fault in your built-in memory. If you continue to operate, you risk corrupting your data. Contact your support representative for repairs.

nnnn System RAM Passed

Where nnnn is the amount of system memory in kilobytes successfully tested.

***System timer error**

The timer test failed. The main clock that operates the computer is faulty. Requires repair of system board. Contact your support representative for repairs.

UMB upper limit segment address: nnnn

Displays the address of the upper limit of Upper Memory Blocks, indicating released segments of the BIOS memory which may be reclaimed by a virtual memory manager.

Video BIOS shadowed

Video BIOS successfully copied to shadow RAM.

EMERGENCY DVD TRAY RELEASE

If for some reason the eject button fails, you can open the DVD/CD-RW tray with a paper clip or similar tool inserted into the eject hole in the far right side of the front of the tray. Straighten one side of a paper clip and push it gently into the hole. The tray will pop out a short distance.

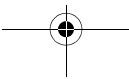
MODEM RESULT CODES

The operating system and application software that is factory installed detects the modem characteristics and provides the necessary command strings to operate the modem. The internal modem operation is controlled by generic AT commands from the operating system and application software. The standard long form result codes may, in some cases, be displayed on your screen to keep you informed of the actions of your modem. The operating system and application software may suppress display of the result codes.

Examples of result codes are:

- OK
- NO CARRIER
- NO DIALTONE
- CONNECT 53000 (Connection complete at 53,000 bps.)
- ERROR
- FAX
- RING (This means an incoming call.)
- BUSY
- NO ANSWER

When using the internal modem with applications that are not factory installed refer to the application documentation.





Restoring Your Pre-installed Software

The Drivers and Applications Restore (DAR) CD contains sets of device drivers and Fujitsu utilities (in specific directories) that are unique to your notebook configuration for use as documented below.



If you have access to the internet, visit the Fujitsu Support web site at <http://www.computers.us.fujitsu.com/support> to check for the most current information, drivers and hints on how to perform recovery and system updates. (See *Automatically Downloading Driver Updates* on page 76 for more information)

Re-Installing Individual Drivers and Applications

The Drivers and Applications CD can be used to selectively re-install drivers and/or applications that may have been un-installed or corrupted.



There may be certain free third-party applications pre-installed on your system that are not on the DAR CD. The latest versions of the applications can be downloaded from the third-party's website.

To re-install drivers and/or applications:

1. Boot up the system and insert the DAR CD after Windows has started. A Fujitsu Installer screen is displayed after the CD is inserted.
2. After reading the License Agreement, click [I agree].
3. A window will appear containing a list of applications, drivers, and utilities that you can install from the Drivers and Applications CD.



The components listed are color-coded in terms of their install status. Blue indicates that the component can be installed. Green indicates that the component needs to be installed separately. Grey indicates a component that is already installed; grey items can be reinstalled, but prior to installation you will receive a reminder that the component is already installed.

4. In the list, check off all the components you want to install. If you want to install all components, click [Select All]. Clicking [Select All] will select all of the blue-coded components; you must select grey and green components separately.
5. Once you have selected the components you wish to install, click [Install Selected Subsystems]; the components will be installed.

6. After the components are installed, click [OK], then click [Yes] when asked if you want to reboot the system.

RESTORING THE FACTORY IMAGE

The Restore Disc that came with your system contains two utilities:

- The **Recovery** utility allows you to restore the original contents of the C: drive.
- The **Hard Disk Data Delete** utility on this disc is used to delete all data on your hard disk and prevent it from being reused. Do not use the Hard Disk Data Delete utility unless you are absolutely certain that you want to erase your entire hard disk, including all partitions.



- The use of this disc requires that you have a device capable of reading DVDs attached to your system. If you do not have a built-in DVD player, you will need to attach an external player. For more information on available external devices, visit our Web site at: us.fujitsu.com/computers.

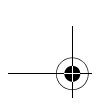
- This disc can only be used with the system with which it was purchased.

BOOT Priority Change

Before restoring an image, you must first verify that your system is set up to boot from the DVD drive. To verify/change the boot-up priority (rather than booting-up from the hard drive or an external floppy disk drive), perform the following steps:

1. Start your system and press the [F2] key when the Fujitsu logo appears. You will enter the BIOS Setup Utility.
2. Using the arrow keys, go to the Boot menu.
3. Arrow down to the Boot Device Priority submenu. Press [Enter].
4. If "Optical Media Drive" or "CD-ROM Drive" is not at the top of the list, arrow down to the drive in the list, and press the space bar (or the + key) to move it to the top of the list. (The system attempts to boot from the devices in the order in which they are listed.). Note that the BIOS for some systems will indicate "CD-ROM Drive", even when a DVD drive is connected.
5. If you have an *external* DVD drive connected, proceed to step 6; otherwise, proceed to step 7.
6. If you have an external DVD drive connected:
 - Select the Advanced menu in the BIOS window.
 - Scroll down to the USB Features submenu and press the Enter key to open it.





- If Legacy USB Support is disabled, press the space bar to enable it.
 - Scroll down to SCSI SubClass Support and press the space bar to enable it.
7. Press [F10], then click on [Yes] to exit the BIOS Setup Utility and return to the boot process.

After you have changed the boot priority, you can restore a backup image when you are booting up.

Procedure

1. Turn on the power to your system.
2. Ensure that you have a device that can read DVDs either installed in your system or attached externally to it.
3. Insert the Restore Disc into the drive tray.
4. Reboot your system.
5. After the system reboots, follow the instructions that appear to either restore your system image or erase all data from your hard disk.

AUTOMATICALLY DOWNLOADING DRIVER UPDATES

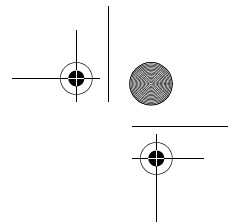
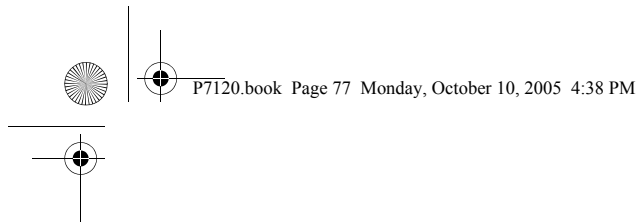
Your system has a convenient tool called the Fujitsu Driver Update (FDU) utility. With FDU, you can choose to automatically or manually go to the Fujitsu site to check for new updates for your system.

The FDU icon  should appear in the system tray at the bottom right of your screen (roll the cursor over the icons to find the correct one). If the FDU icon does not appear in the system tray, it can be started by going to [Start] -> All Programs, and clicking on Fujitsu Driver Update; this will create the icon automatically.

To invoke the FDU menu, right-click on the FDU icon. The menu contains the following items:

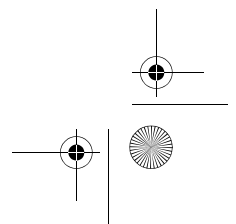
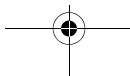
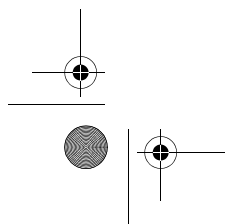
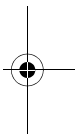
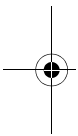
- **Check for updates now**
Allows for manual driver update search. The first time it is used, you are prompted to agree to a user agreement. After clicking on the icon, the FDU automatically connects with the Fujitsu site to check for updates and downloads them. While downloading, the icon has a red bar through it, indicating that it cannot be used while the download is in process. When the update is complete, a message appears informing you of the fact.
- **Enable Automatic Update Notifications**
Automatically searches for new updates on a regular basis (approximately every 3 days).
- **Show update history**
Brings up a screen that displays a history of updates that have been made via the FDU.
- **About Fujitsu Driver Update**
Displays the FDU version number and copyright information
- **Fujitsu Driver Update Readme**
Displays the FDU readme.

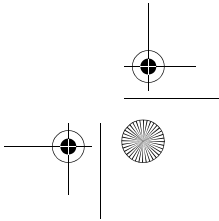
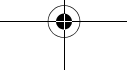
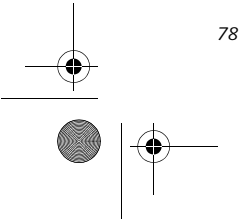
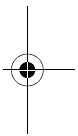
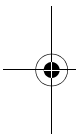
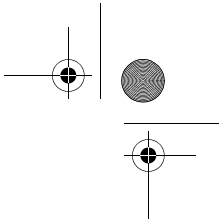
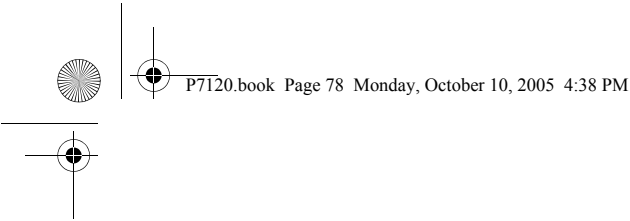




7

Care and Maintenance







Care and Maintenance

If you use your Fujitsu LifeBook notebook carefully, you will increase its life and reliability. This section provides some tips for looking after the notebook and its devices.



Electrical equipment may be hazardous if misused. Operations of this product or similar products, must always be supervised by an adult. Do not allow children access to the interior of any electrical products and do not permit them to handle any cables.

Caring for your LifeBook notebook

- Your LifeBook notebook is a durable but sensitive electronic device. Treat it with respect and care.
- Make a habit of transporting it in a suitable carrying case.
- Do not attempt to service the computer yourself. Always follow installation instructions closely.
- To protect your notebook from damage and to optimize system performance, be sure to **keep all air all vents unobstructed, clean, and clear of debris**. This may require periodic cleaning, depending upon the environment in which the system is used.
- Keep the computer away from food and beverages.
- If you accidentally spill liquid on your LifeBook notebook:
 1. Turn it off.
 2. Position it so that the liquid can run out.
 3. Let it dry out for 24 hours, or longer if needed.
 4. If your notebook will not boot after it has dried out, call your support representative.
- Do not use your Fujitsu LifeBook notebook in a wet environment (near a bathtub, swimming pool).
- Always use the AC adapter and batteries that are approved for your notebook.
- Avoid exposure to sand, dust and other environmental hazards.
- Do not expose your notebook to direct sunlight for long periods of time as temperatures above 140° F (60° C) may damage your notebook.
- Keep the covers closed on the connectors and slots when they are not in use.
- Do not put heavy or sharp objects on the computer.
- If you are carrying your LifeBook notebook in a briefcase, or any other carrying case, make sure that there are no objects in the case pressing on the lid.
- Never position your notebook such that the DVD/CD-RW drive is supporting the weight of the notebook.

- Do not drop your notebook.
- Do not touch the screen with any sharp objects.

Cleaning your LifeBook notebook

- Always disconnect the power plug. (Pull the plug, not the cord.)
- Clean your LifeBook notebook with a damp, lint-free cloth. Do not use abrasives or solvents.
- Use a soft cloth to remove dust from the screen. Never use glass cleaners.

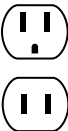
Storing your LifeBook notebook

- If storing your notebook for a month or longer, turn your LifeBook notebook off, charge the battery, then remove and store all Lithium ion batteries.
- Store your notebook and batteries separately. If you store your LifeBook with a battery installed, the battery will discharge, and battery life will be reduced. In addition, a faulty battery might damage your LifeBook.
- Store your Fujitsu LifeBook in a cool, dry location. Temperatures should remain between 13°F (-10°C) and 140°F (60°C).

Traveling with your LifeBook notebook

- Do not transport your notebook while it is turned on.
- Do not check your notebook as baggage. Carry it with you.
- Always bring your backup disk and Drivers and Applications CD that came with your notebook when you travel. If you experience system software problems while traveling, you may need it to correct any problems.
- Never put your notebook through a metal detector. Have your notebook hand-inspected by security personnel. You can however, put your notebook through a properly tuned X-ray machine. To avoid problems, place your notebook close to the entrance of the machine and remove it as soon as possible or have your notebook hand-inspected by security personnel. Security officials may require you to turn your notebook On. Make sure you have a charged battery on hand.
- When traveling with the hard drive removed, wrap the drive in a non-conducting materials (cloth or paper). If you have the drive checked by hand, be ready to install the drive if needed. Never put your hard drive through a metal detector. Have your hard drive hand-inspected by security personnel. You can however, put your hard drive through a properly tuned X-ray machine.
- Take the necessary plug adapters if you're traveling overseas. Check the following diagram to determine which plug adapter you'll need or ask your travel agent.



Outlet Type	Location
	United States, Canada, parts of Latin America, Mexico, Japan, Korea, the Philippines, Taiwan
	Russia and the Commonwealth of Independent States (CIS), most of Europe, parts of Latin America, the Middle East, parts of Africa, Hong Kong, India, most of South Asia
	United Kingdom, Ireland, Malaysia, Singapore, parts of Africa
	China, Australia, New Zealand

BATTERIES

Caring for your Batteries

- Always handle batteries carefully.
- Do not short-circuit the battery terminals (that is, do not touch both terminals with a metal object). Do not carry lose batteries in a pocket or purse where they may mix with coins, keys, or other metal objects. Doing so may cause an explosion or fire.
- Do not drop, puncture, disassemble, mutilate or incinerate the battery.
- Recharge batteries only as described in this manual and only in ventilated areas.
- Do not leave batteries in hot locations for more than a day or two. Intense heat can shorten battery life.
- Do not leave a battery in storage for longer than 6 months without recharging it.

Increasing Battery Life

- Power your LifeBook notebook through the AC or optional auto/airline adapter whenever possible.
- If your notebook is running on battery power all day, connect it to the AC adapter overnight to recharge the battery.
- Keep brightness to the lowest level comfortable.
- Set the power management for maximum battery life.

- Put your notebook in Suspend mode when it is turned on and you are not actually using it.
- Limit your media drive access.
- Disable the DVD/CD-RW Combo Drive auto insert notification function.
- Always use fully charged batteries.
- Eject PCMCIA™ cards when not in use.

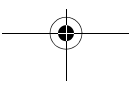
FLOPPY DISKS AND DRIVES

Caring for your Floppy Disks

- Avoid using the floppy disks in damp and dusty locations.
- Never store a floppy disk near a magnet or magnetic field.
- Do not use a pencil or an eraser on a disk or disk label.
- Avoid storing the floppy disks in extremely hot or cold locations, or in locations subject to severe temperature changes. Store at temperatures between 50° F (10°C) and 125°F (52°C).
- Do not touch the exposed part of the disk behind the metal shutter.

Caring for your Floppy Disk Drive

- To clean, wipe the floppy disk drive clean with a dry soft cloth, or with a soft cloth dampened with water or a solution of neutral detergent. Never use benzene, paint thinner or other volatile material.
- Avoid storing the floppy disk drive in extremely hot or cold locations, or in locations subject to severe temperature changes. Store at temperatures between 50° F (10° C) and 125°F (52° C).
- Keep the floppy disk drive out of direct sunlight and away from heating equipment.
- Avoid storing the floppy disk drive in locations subject to shock and vibration.
- Never use the floppy disk drive with any liquid, metal, or other foreign matter inside the floppy disk drive or disk.
- Never disassemble or dismantle your floppy disk drive.





Care and Maintenance

MEDIA CARE

Caring for your Media Discs

Media discs are precision devices and will function reliably if given reasonable care.

- Always store your media disc in its case when it is not in use.
- Always handle discs by the edges and avoid touching the surface.
- Avoid storing any media discs in extreme temperatures.
- Do not bend media discs or set heavy objects on them.
- Do not spill liquids on media discs.
- Do not scratch media discs.
- Do not get dust on media discs.
- Never write on the label surface with a ballpoint pen or pencil. Always use a felt pen.
- If a media disc is subjected to a sudden change in temperature, cold to warm condensation may form on the surface. Wipe the moisture off with a clean, soft, lint free cloth and let it dry at room temperature. DO NOT use a hair dryer or heater to dry media discs.
- If a disc is dirty, use only a DVD/CD cleaner or wipe it with a clean, soft, lint free cloth starting from the inner edge and wiping to the outer edge.

Caring for your Optical Drive

Your optical drive is durable but you must treat it with care. Please pay attention to the following points:

- The drive rotates the compact disc at a very high speed. Do not carry it around or subject it to shock or vibration with the power on.
- Avoid using or storing the drive where it will be exposed to extreme temperatures.
- Avoid using or storing the drive where it is damp or dusty.
- Avoid using or storing the drive near magnets or devices that generate strong magnetic fields.
- Avoid using or storing the drive where it will be subjected to shock or vibration.
- Do not disassemble or dismantle the DVD/CD-RW drive.
- Occasional use of a commercially available lens cleaner kit is recommended to maintain your drive.

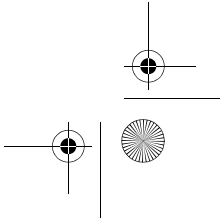
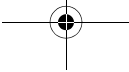
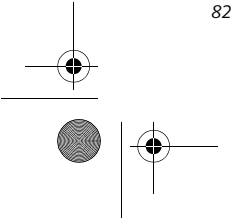
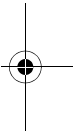
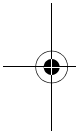
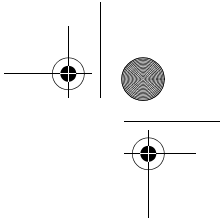
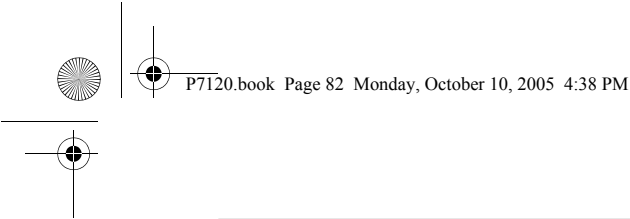
PC CARDS

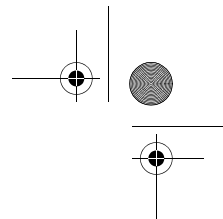
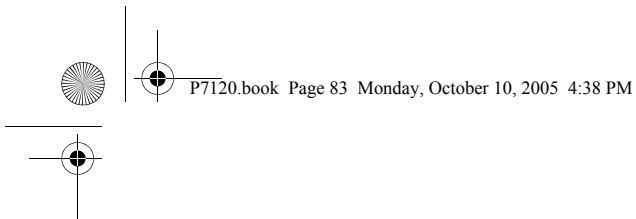
Caring for your PC Cards

PC Cards are durable, but you must treat them with care. The documentation supplied with your PC Card will provide specific information, but you should pay attention to the following points:

- To keep out dust and dirt, store PC Cards in their protective sleeves when they are not installed in your LifeBook notebook.
- Avoid prolonged exposure to direct sunlight or excessive heat.
- Keep the cards dry.
- Do not flex or bend the cards, and do not place heavy objects on top of them.
- Do not force cards into the slot.
- Avoid dropping cards, or subjecting them to excessive vibration.

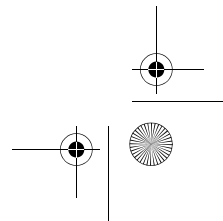
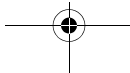
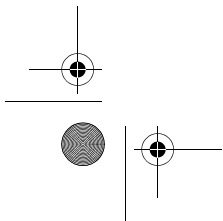
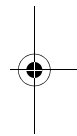
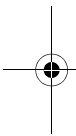


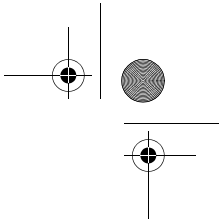
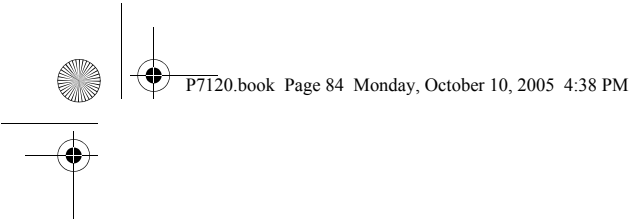




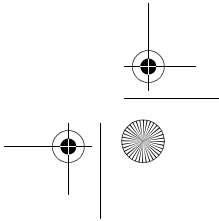
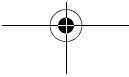
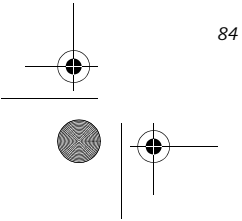
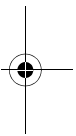
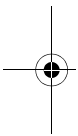
8

Specifications





LifeBook P7000 Notebook – Section Eight





Specifications

Specifications

This section provides the hardware and environmental specifications for your Fujitsu LifeBook notebook. Specifications of particular configurations will vary.

CONFIGURATION LABEL

The configuration label located on the bottom of your LifeBook notebook (*See figure 2-7 on page 11 for location*) contains information regarding the options you've chosen for your notebook. Following is an example label and information on how to read your own configuration label.

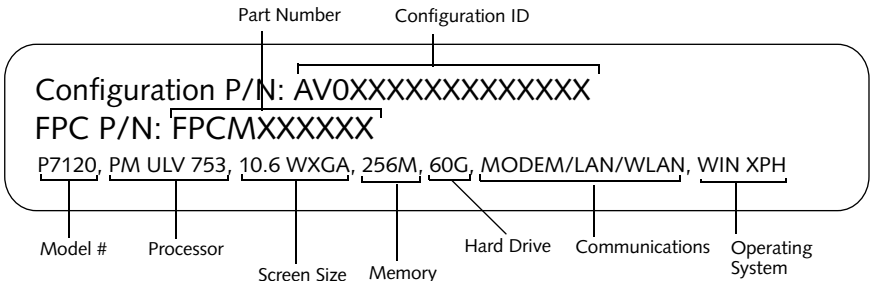


Figure 8-1 Configuration Label

MICROPROCESSOR

Intel® Pentium® M Processor ULV 753 (1.2 GHz, 2 MB L2 Cache, 400 MHz Front Side Bus)

MEMORY

System Memory

- 256 MB minimum, 2GB maximum, micro-DIMM DDR2-400 SDRAM
- Two micro-DIMM slots (one accessible)
- 256 MB, 512 MB, and 1GB memory modules available

BIOS Memory

1 MB Firmware Hub (FWH) Flash ROM

VIDEO

Built-in color 10.6" Wide XGA Crystal View TFT active matrix LCD display with simultaneous display capability.

Intel® 915GMS video graphics chip with integrated 32-bit 3D/2D gfx core and Accelerated Graphics Port (AGP) support.

Up to 128 MB shared video memory using Dynamic Video Memory Technology 2.0.

Video Color and Resolution

10.6" TFT Wide XGA

- Internal: 1280 x 768 pixel resolution, 16M colors
- External: 1600 x 1200 pixel resolution, 16M colors
- Simultaneous Video: 1024 x 768, 16M colors, XGA, SVGA and VGA compatible

AUDIO

- Realtek ALC260 codec with 18-bit stereo audio
- Stereo headphone/line-out port
- Mono microphone jack, 100 mV_{rms} max.
- Dolby Headphone signal processing utility (in the InterVideo DVD software)

- Two built-in stereo speakers, 25 mm x 14 mm, bass reflex
- Built-in microphones one either side of the display.

MASS STORAGE DEVICE OPTIONS

Hard Drive

20 GB, 30 GB, or 60 GB, fixed hard drive, 1.8", Ultra DMA 100

Modular DVD/CD-RW Combo Drive

8x DVD / 10x CD-RW / 24x CD-R / 24x CD-ROM

Modular Dual-Layer Multi-Format DVD Writer

2.4x DVD+R DL, 4x DVD-R, 2x DVD-RW, 4x DVD+R, 2.4x DVD+RW, 2x DVD-RAM, 8x DVD-ROM, 24x CD-R, 10x CD-RW, 24x CD-ROM

FEATURES

Communications

- Modem: Internal V.90 standard 56K fax/modem (ITU V.90, 56K data, 14.4K fax)
- LAN: 10/100 Base-TX Ethernet
- Integrated Intel PRO/Wireless 2915ABG Network Connections (Tri-mode 802.11a/b/g*) with Antenna On/Off switch (available in LifeBook P7120 model), or,
- Integrated Atheros Super AG Wireless LAN (802.11a/b/g*) with Antenna On/Off switch (available in LifeBook P7120D model)
- Optional Bluetooth device for wireless personal area network communication

* Operates at 2.4 GHz and 5.0 GHz; communications range may vary, depending upon environment.

Integrated Pointing Device

Touchpad pointing device with combination fingerprint sensor*/scroll button.

* Fingerprint Sensor: AuthenTec fingerprint slide sensor (AES2501)





Theft Prevention Lock Slot

Slot for use with physical restraining security systems.

DEVICE PORTS

- PC Card slot for one Type II card: PCMCIA Standard 2.1 with CardBus support
- One connector for external monitor (see Display specifications)
- One Memory Stick/SD/xD slot
- Three USB 2.0 connectors for input/output devices
- One S-Video Out port
- One modular modem (RJ-11) connector
- One LAN (RJ-45) port
- One IEEE 1394 port
- One stereo headphone/line-out jack. (See Audio specifications)
- One mono microphone jack. (See Audio specifications)

KEYBOARD

Built-in keyboard with all functions of 101 key keyboards.

- Total number of keys: 82
- Function keys: [F1] through [F12]
- Feature extension key: [Fn]
- Two Windows keys: one Start and one application key
- Key pitch: 17.5 mm
- Key stroke: 2 mm
- Built-in Touchpad pointing device with left and right buttons and scroll button.
- Built-in palm rest

External Keyboard Support

USB-compatible

External Mouse Support

USB-compatible

POWER

Batteries

- One standard 4-cell high-capacity Lithium ion battery, rechargeable, 7.2V, 5200 mAh
- Optional high-capacity 6-cell Lithium ion battery, rechargeable, 7.2V, 7800 mAh
- Optional second bay battery: 4-cell Lithium ion battery, rechargeable, 10.8V, 2300 mAh

AC Adapter

Autosensing 100-240V AC, 60W, supplying 16V DC, 3.75A to the LifeBook notebook, which includes an AC cable.

Power Management

Conforms to ACPI (Advanced Configuration and Power Interface)

DIMENSIONS AND WEIGHT

Overall Dimensions

Approximately 10.28"(w) x 7.83"(d) x 1.26/1.43"(h)
(261mm x 199 mm x 32/36 mm)

Weights

Approximately 3.0 lbs (1.50 kg) with standard battery and DVD/CD-RW combo drive

ENVIRONMENTAL REQUIREMENTS

Temperature

Operating: 41° to 95° F (5° to 35° C)

Non-operating: 5° to 140° F (–15° to 60° C)

Humidity

Operating: 20% to 85%, relative, non-condensing

Non-operating: 8% to 85%, relative, non-condensing

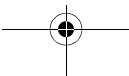
Altitude

Operating: 10,000 feet (3,048 m) maximum

POPULAR ACCESSORIES

For ordering or additional information on Fujitsu accessories please visit our Web site at:

www.shopfujitsu.com or call 1-800-FUJITSU.





Specifications

PRE-INSTALLED SOFTWARE

Depending on your pre-installed operating system, your Fujitsu LifeBook notebook comes with pre-installed software for playing audio and video files of various formats. In addition there is file transfer software, virus protection software and Power Management software.

LEARNING ABOUT YOUR APPLICATION SOFTWARE

Tutorials

All operating systems and most application software have tutorials built into them upon installation. We highly recommend that you step through the tutorial before you use an application.

Manuals

Included with your notebook you will find manuals for your installed operating system and other pre-installed software. Any manuals that are not included, are available online through the help system of the software. We recommend that you review these manuals for general information on the use of these applications.

Adobe Reader

The Adobe Reader allows you to view, navigate, and print PDF files from across all of the major computing platforms.

Norton AntiVirus 2005

Your system is preinstalled with a free 90-day trial version of Symantec's Norton AntiVirus™ 2005. Norton AntiVirus is a program designed to protect your LifeBook notebook from computer viruses. It assists in the protection of the data currently residing on your hard disk from destruction or contamination. The 90-day trial version is activated upon your acceptance of software license agreement. After 90 days, it will be necessary to purchase a subscription from Symantec to download latest virus definitions.

(See your online help or manual for more information on how and when to run this program).

Fujitsu HotKey Utility

Utility for adjusting the brightness level on your LifeBook notebook.

Fujitsu Driver Update

The Fujitsu Driver Update (FDU) utility allows you to choose to automatically or manually go to the Fujitsu site to check for new updates for your system.

Quicken 2005 New User Edition

Quicken 2005 New User Edition by Intuit is a personal money management program. It has features such as portfolio management, account registries, on-line banking and bill paying. This application is for new users who are using Quicken software for the first time. Full version upgrade information is available on line.

MS Works

Microsoft Works is a suite of software containing the basic tools to write letters and reports, track family and friends with address books, manage home finances, and create a home inventory.

Depending upon your system configuration, one of the following applications will be installed on your notebook:

Microsoft Works 8.0

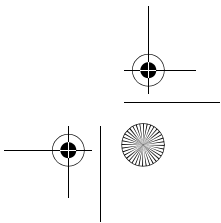
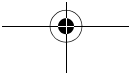
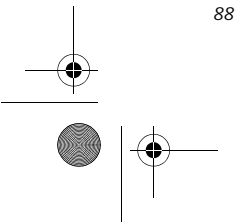
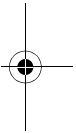
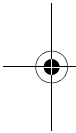
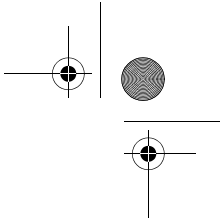
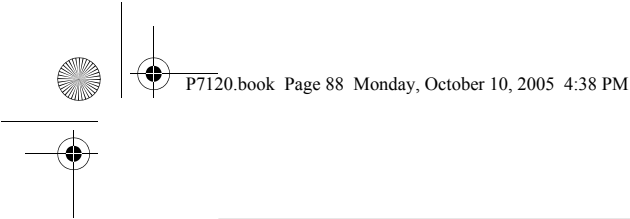
Microsoft Works 8.0 is a suite of software containing the basic tools to write letters and reports, track family and friends with address books, manage home finances, and create a home inventory.

Microsoft Office SBE

(On Microsoft Windows XP Professional models only)

Microsoft Small Business Edition (SBE) is a suite of applications designed to help run a small business while increasing productivity. Among the programs included in Microsoft SBE are Microsoft Word, Excel, and PowerPoint.







Regulatory Information

NOTICE

Changes or modifications not expressly approved by Fujitsu could void this user's authority to operate the equipment.

FCC NOTICES

Notice to Users of Radios and Television

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet that is on a different circuit than the receiver.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interconnect cables must be employed with this equipment to ensure compliance with the pertinent RF emission limits governing this device.

Notice to Users of the US Telephone Network

This equipment complies with Part 68 of the FCC rules, and the requirements adopted by ACTA. On the bottom of this equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment; or a product identifier in the format US:AAAEQ##TXXXX. If requested, this information or number must be provided to the telephone company.

This equipment is designed to be connected to the telephone network or premises wiring using a standard jack type USOC RJ11C. A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

The ringer equivalent number (REN) of this equipment is 0.1B as shown on the label. The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

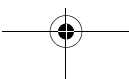
The telephone company may make changes in its facilities, equipment, operations or procedures that could effect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please refer to the manual or contact Fujitsu Computer Systems Corporation, Customer Service. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

The equipment cannot be used on public coin service provided by the telephone company. Connection to party line service is subject to state tariffs. (Contact the state public utility commission, public service commission or corporation commission for information).

If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this computer does not disable your alarm equipment. If you have any questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or other electronic device to send any message via a telephone fax machine unless such message clearly contains in a margin at the top or bottom of each transmitted page or on the first page of the transmission, the date and time it is sent and an identification of the business or other entity, or other individual sending the message and the telephone number of the sending machine or such business, other entity, or individual.





DOC (INDUSTRY CANADA) NOTICES
Notice to Users of Radios and Television

This Class B digital apparatus meets all requirements of Canadian Interference-Causing Equipment Regulations.

CET appareil numérique de la class B respecte toutes les exigence du Règlement sur le matériel brouilleur du Canada.

Notice to Users of the Canadian Telephone Network

NOTICE: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Before connecting this equipment to a telephone line the user should ensure that it is permissible to connect this equipment to the local telecommunication facilities. The user should be aware that compliance with the certification standards does not prevent service degradation in some situations.

Repairs to telecommunication equipment should be made by a Canadian authorized maintenance facility. Any repairs or alterations not expressly approved by Fujitsu or any equipment failures may give the telecommunication company cause to request the user to disconnect the equipment from the telephone line.

NOTICE: The Ringer Equivalence Number (REN) for this terminal equipment is 0.1B. The REN assigned to each terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.



For safety, users should ensure that the electrical ground of the power utility, the telephone lines and the metallic water pipes are connected together. Users should NOT attempt to make such connections themselves but should contact the appropriate electric inspection authority or electrician. This may be particularly important in rural areas.

Avis Aux Utilisateurs Du Réseau
Téléphonique Canadien

AVIS: Le présent matériel est conforme aux spécifications techniques d'Industrie Canada applicables au matériel terminal. Cette conformité est confirmée par le numéro d'enregistrement. Le sigle IC, placé devant le numéro d'enregistrement, signifie que l'enregistrement s'est effectué conformément à une déclaration de conformité et indique que les spécifications techniques d'Industrie Canada ont été respectées. Il n'implique pas qu'Industrie Canada a approuvé le matériel.

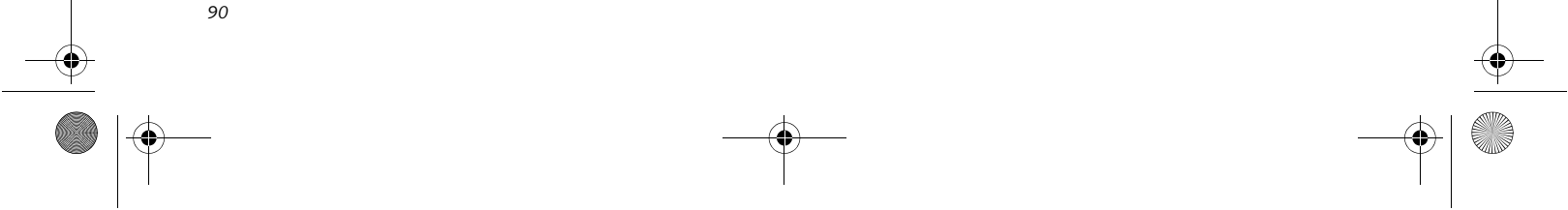
Avant de connecter cet équipement à une ligne téléphonique, l'utilisateur doit vérifier s'il est permis de connecter cet équipement aux installations de télécommunications locales. L'utilisateur est averti que même la conformité aux normes de certification ne peut dans certains cas empêcher la dégradation du service.

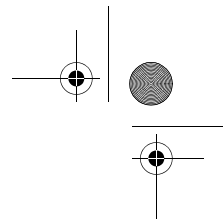
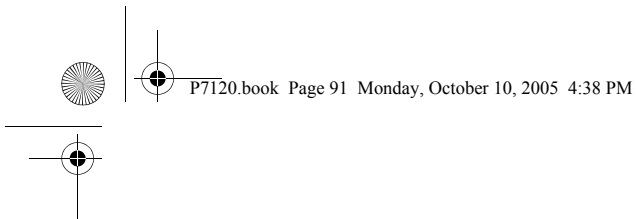
Les réparations de l'équipement de télécommunications doivent être effectuées par un service de maintenance agréé au Canada. Toute réparation ou modification, qui n'est pas expressément approuvée par Fujitsu, ou toute défaillance de l'équipement peut entraîner la compagnie de télécommunications à exiger que l'utilisateur déconnecte l'équipement de la ligne téléphonique.

AVIS: L'indice d'équivalence de la sonnerie (IES) du présent matériel est de 0.1B. L'IES assigné à chaque dispositif terminal indique le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

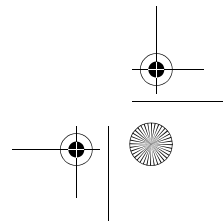
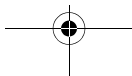
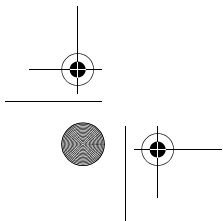
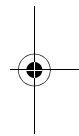
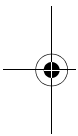


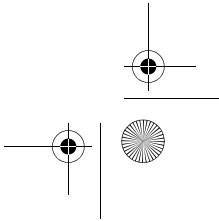
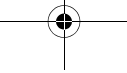
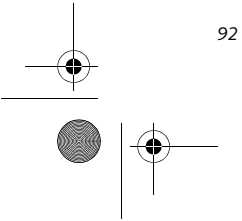
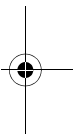
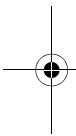
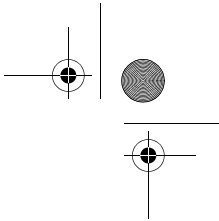
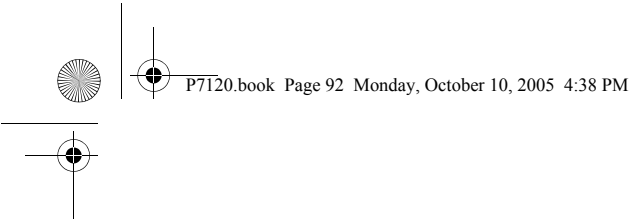
Pour assurer la sécurité, les utilisateurs doivent vérifier que la prise de terre du service d'électricité, les lignes téléphoniques et les conduites d'eau métalliques sont connectées ensemble. Les utilisateurs NE doivent PAS tenter d'établir ces connexions eux-mêmes, mais doivent contacter les services d'inspection d'installations électriques appropriés ou un électricien. Ceci peut être particulièrement important en régions rurales.





9 Glossary







Glossary

AC Adapter

A device which converts the AC voltage from a wall outlet to the DC voltage needed to power your LifeBook notebook.

ACPI

Advanced Configuration and Power Interface. An industry specification for the efficient handling of power consumption in mobile computers. ACPI determines how a computer's BIOS, operating system, and peripherals communicate with each other about power management.

Active-Matrix Display

A type of technology for making flat-panel displays which has a transistor or similar device for every pixel on the screen.

ADSL

Asymmetric Digital Subscriber Line. Technology for transporting high bit-rate services over ordinary phone lines.

APM

Advanced Power Management.

Auto/Airline Adapter

A device which converts the DC voltage from an automobile cigarette lighter or aircraft DC power outlet to the DC voltage needed to power your LifeBook notebook.

BIOS

Basic Input-Output System. A program and set of default parameters stored in ROM which tests and operates your LifeBook notebook when you turn it on until it loads your installed operating system from disk. Information from the BIOS is transferred to the installed operating system to provide it with information on the configuration and status of the hardware.

Bit

An abbreviation for binary digit. A single piece of information which is either a one (1) or a zero (0).

bps

An abbreviation for bits per second. Used to describe data transfer rates.

Boot

To start-up a computer and load its operating system from disk, ROM or other storage media into RAM.

Bus

An electrical circuit which passes data between the CPU and the sub-assemblies inside your LifeBook notebook.

Byte

8 bits of parallel binary information.

Cache Memory

A block of memory built into the micro-processor which is much faster to access than your system RAM and used in specially structured ways to make your overall data handling time faster.

CardBus

A faster, 32-bit version of the PC Card interface which offers performance similar to the 32-bit PCI architecture.

CD-ROM

Compact disc read only memory. This is a form of digital data storage which is read optically with a laser rather than a magnetic head. A typical CD-ROM can contain about 600MB of data and is not subject to heads crashing into the surface and destroying the data when there is a failure nor to wear from reading.

CMS

Code Morphing Software. Crusoe processor software architecture that results in longer battery life. For more information on CMS, click on the Technology link on the refer to the Transmeta web site at: www.transmeta.com.

Command

An instruction which you give your operating system. Example: run a particular application or format a floppy disk.

Configuration

The combination of hardware and software that makes up your system and how it is allocated for use.

Data

The information a system stores and processes.

DC

Direct current. A voltage or current that does not fluctuate periodically with time.

Default Value

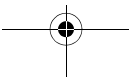
A pre programmed value to be used if you fail to set your own.

DIMM

Dual-in-line memory module.

Disk

A spinning platter of magnetic data storage media. If the platter is very stiff it is a hard drive, if it is highly flexible it is a floppy disk, if it is a floppy disk in a hard housing with a shutter it is commonly called a diskette.





Disk Drive

The hardware which spins the disk and has the heads and control circuitry for reading and writing the data on the disk.

Diskette

A floppy disk in a hard housing with a shutter.

DMA

Direct Memory Access. Special circuitry for memory to memory transfers of data which do not require CPU action.

DMI

Desktop Management Interface. A standard that provides PC management applications with a common method of locally or remotely querying and configuring PC computer systems, hardware and software components, and peripherals.

DOS

Disk Operating System (MS-DOS is a Microsoft Disk Operating System).

Driver

A computer program which converts application and operating system commands to external devices into the exact form required by a specific brand and model of device in order to produce the desired results from that particular equipment.

ESD

Electro-Static Discharge. The sudden discharge of electricity from a static charge which has built-up slowly. Example: the shock you get from a doorknob on a dry day or the sparks you get from brushing hair on a dry day.

Extended Memory

All memory more than the 640KB recognized by MS-DOS as system memory.

FCC

Federal Communication Commission.

Floppy Disk

A spinning platter of magnetic data storage media which is highly flexible.

GB

Gigabyte.

Hard drive

A spinning platter of magnetic data storage media where the platter is very stiff.

Hexadecimal

A decimal notation for the value of a 4 bit binary number. (0-9, A, B, C, D, E, F) Example: 2F in hexadecimal = 00101111 in binary = 47 in decimal.

I/O

Input/Output. Data entering and leaving your LifeBook notebook in electronic form.

I/O Port

The connector and associated control circuits for data entering and leaving your LifeBook notebook in electronic form.

IDE

Intelligent Drive Electronics. A type of control interface for a hard drive which is inside the hard drive unit.

IEEE 1394

The IEEE 1394 (also known as “Firewire” or “iLink”) standard allows you to connect devices that are compliant with IEEE standard 1394. This port is effectively a very fast communications port. This architecture is very good for transferring large files, such as those from digital cameras.

IRQ

Interrupt Request. An acronym for the hardware signal to the CPU that an external event has occurred which needs to be processed.

KB

Kilobyte.

LAN

Local Area Network. An interconnection of computers and peripherals within a single limited geographic location which can pass programs and data amongst themselves.

LCD

Liquid Crystal Display. A type of display which makes images by controlling the orientation of crystals in a crystalline liquid.

Lithium ion Battery

A type of rechargeable battery which has a high power-time life for its size and is not subject to the memory effect as Nickel Cadmium batteries.

MB

Megabyte.

Megahertz

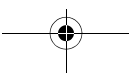
1,000,000 cycles per second.

Memory

A repository for data and applications which is readily accessible to your LifeBook notebook CPU.

MHz

Megahertz.





Glossary

Modem

A contraction for **MODulator-DEModulator**. The equipment which connects a computer or other data terminal to a communication line.

Monaural

A system using one channel to process sound from all sources.

NTSC

National TV Standards Commission. The standard for TV broadcast and reception for the USA.

Operating System

A group of control programs that convert application commands, including driver programs, into the exact form required by a specific brand and model of micro-processor in order to produce the desired results from that particular equipment.

Partition

A block of space on a hard drive which is set aside and made to appear to the operating system as if it were a separate disk, and addressed by the operating system accordingly.

PCMCIA

PCMCIA is a trademark of the Personal Computer Memory Card International Association. The Personal Computer Memory Card International Association is an organization that sets standards for add-in cards for personal computers.

Peripheral Device

A piece of equipment which performs a specific function associated with but not integral to a computer. Examples: a printer, a modem, a CD-ROM.

Pitch (keyboard)

The distance between the centers of the letter keys of a keyboard.

Pixel

The smallest element of a display, a dot of color on your display screen. The more pixels per area the clearer your image will appear.

POP3

Post Office Protocol. Protocol that is used to retrieve email from a mail server.

POST

Power On Self Test. A program which is part of the BIOS which checks the configuration and operating condition of your hardware whenever power is applied to your LifeBook notebook. Status and error messages may be displayed before the operating system is loaded. If the self test detects failures that are so serious that operation can not continue, the operating system will not be loaded.

PPPoE

Point to Point Protocol over Ethernet. A protocol for Ethernet, using a Point-to-Point Protocol (PPP), which is used for connection on the phone line.

Program

An integrated set of coded commands to your computers telling your hardware what to do and how and when to do it.

PS/2

A series of personal computers which established a number of standards for connecting external devices such as keyboards and monitors.

RAM

Random Access Memory. A hardware component of your LifeBook notebook that holds binary information (both program and data) as long as it has the proper power applied to it.

RAM Module

A printed circuit card with memory and associated circuitry which allows the user to add additional memory to the computer without special tools.

Reset

The act of reloading the operating system. A reset erases all information stored in RAM.

Restart

See Reset.

Resume

To proceed after interruption. In your LifeBook notebook, this refers to returning to active operation after having been in one of the suspension states.

ROM

Read Only Memory. A form of memory in which information is stored by physically altering the material. Data stored in this way can not be changed by your LifeBook notebook and does not require power to maintain it.

SDRAM

Synchronous Dynamic Random Access Memory.

Shadow RAM

A technique of copying data or applications stored in ROM (Read Only Memory) into RAM (Random Access Memory) for access during actual operation. RAM is much faster to access than ROM, however ROM contents are not lost when power is removed. Shadowing allows permanently stored information to be rapidly accessed.

SPDIF

Sony Philips Digital Interface. Technology that allows you to download digital audio data onto a MiniDisc recorder.





SSID

Service Set Identifier. Specifies which network you are joining. Some systems allow you to specify any SSID as an option so you can join any network.

Status Indicator

A display which reports the condition of some portion of your hardware. On your LifeBook notebook this is an LCD screen just above the keyboard.

Stereo (audio)

A system using two channels to process sound from two different sources.

Stroke (keyboard)

The amount of travel of a key when it is pressed from resting to fully depressed.

Suspend

To make inoperative for a period of time. Your LifeBook notebook uses various suspension states to reduce power consumption and prolong the charge of your battery.

SVGA

Super VGA. Standard that provides 800x600 pixel resolution and a palette of 16M colors.

S-Video

Super Video. A component video system for driving a TV or computer monitor.

System Clock

An oscillator of fixed precise frequency which synchronizes the operation of the system and is counted to provide time of day and date.

TFT

Thin Film Transistor. A technology for flat display panels which uses a thin film matrix of transistors to control each pixel of the display screen individually.

UL

Underwriters Laboratories – An independent organization that tests and certifies the electrical safety of devices.

USB

Universal Serial Bus. An external bus standard that allows for fast data transfer. A single USB port can be used to connect up to 127 peripheral devices, such as

mice, modems, and scanners. USB 1.1 has a transfer speed of a maximum of 12Mb/s. USB 2.0 is much faster, transferring at up to 480Mb/s. USB 2.0 is backward-compatible to work with USB 1.1 devices.

VGA

Video Graphics Array. A video display standard which provides resolutions of 720 x 400.

VRAM

Video Random Access Memory. A memory dedicated to video display data and control.

WEP

Wired Equivalent Privacy. WEP is a protocol for increasing privacy over wireless LANs. The protocol works by encrypting data while being transmitted over radio waves.

WFM

Wired for Management is Intel's broad-based initiative to reduce the total cost of ownership (TCO) of business computing without sacrificing power and flexibility.

Wi-Fi Compatible

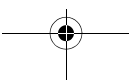
Wi-Fi (**Wireless Fidelity**) identifies that the product has passed the interoperability test, supplied by the WECA (Wireless Ethernet Compatibility Alliance), which guarantees the interoperability of wireless IEEE 802.11 LAN products. For more information on the Wi-Fi standard, go to the WECA website at: www.wirelessethernet.com.

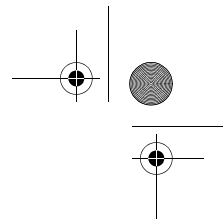
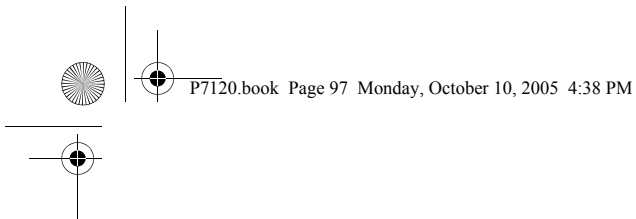
Write Protect

Prevent alteration of the binary state of all bits in a storage media. Example: all information on a device such as a floppy diskette; a block of space in a storage media such as a partition of a hard drive; a file or directory of floppy diskette or hard drive.

XGA

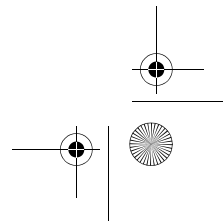
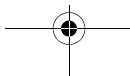
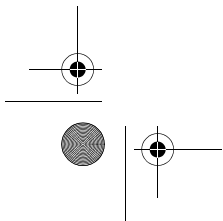
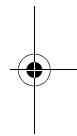
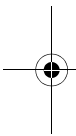
Extended graphics array. Standard that provides resolutions of 640x480 or 1024x764, supporting 64k colors.

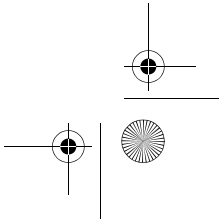
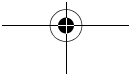
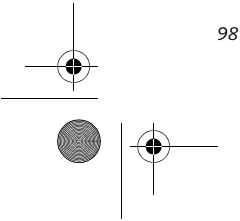
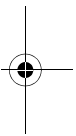
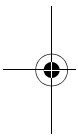
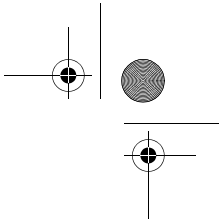
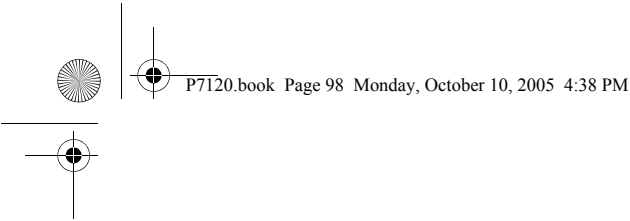




Appendix A

Using the Fingerprint Sensor





Fingerprint Sensor Device

INTRODUCING THE FINGERPRINT SENSOR DEVICE

Your system has an optional fingerprint sensor device below the Touchpad, between the left and right buttons. This also serves as a scroll button. (Figure 1)

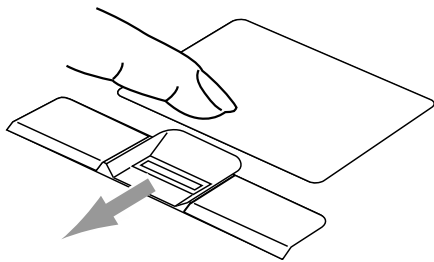


Figure A-1 Fingerprint sensor



Although the system may have a fingerprint sensor in place of a scroll button, the fingerprint sensor can be used for scrolling. Simply move your fingerprint over the sensor the same as you would use a scroll button.

With a fingerprint sensor, you can avoid having to enter a username and password every time you want to:

- Log onto Windows
- Recover from suspend mode
- Cancel a password-protected screen saver
- Log into homepages that require a username and password

After you have “enrolled” - or registered - your fingerprint, you can simply swipe your fingertip over the sensor for the system recognize you.

The fingerprint sensor uses Softex OmniPass which provides password management capabilities to Microsoft Windows operating systems. OmniPass enables you to use a “master password” for all Windows, applications, and on-line passwords.

OmniPass requires users to authenticate themselves using the fingerprint sensor before granting access to the Windows desktop. This device results in a secure authentication system for restricting access to your computer, applications, web sites, and other password-protected resources.

OmniPass presents a convenient graphical user interface, through which you can securely manage passwords, users, and multiple identities for each user.

GETTING STARTED

This section guides you through the preparation of your system for the OmniPass fingerprint recognition application. You will be led through the OmniPass installation process. You will also be led through the procedure of enrolling your first user into OmniPass.

INSTALLING OMNIPASS

If OmniPass has already been installed on your system, skip this section and go directly to “User Enrollment” on page 100. You can determine whether OmniPass has already been installed by checking to see if the following are present:

- The presence of the gold key-shaped OmniPass icon in the system tray at the bottom right of the screen.
- The presence of the Softex program group in the Programs group of the Start menu

System Requirements

The OmniPass application requires space on your hard drive; it also requires specific Operating Systems (OS's). The minimum requirements are as follows:

- Windows XP Home Edition or Windows XP Professional operating system
- At least 35 MB available hard disk space

Installing the OmniPass Application

If OmniPass is already installed on your system, go to “User Enrollment” on page 100. Otherwise continue with this section on software installation.



For installation, OmniPass requires that the user installing OmniPass have administrative privileges to the system. If your current user does not have administrative privileges, log out and then log in with an administrator user before proceeding with OmniPass installation.

To install OmniPass on your system you must:

1. Insert the installation media for the OmniPass application into the appropriate drive. If you are installing from CD-ROM or DVD-ROM, you must find and launch the OmniPass installation program (setup.exe) from the media.
2. Follow the directions provided in the OmniPass installation program. Specify a location to which you would like OmniPass installed. It is recommended that you NOT install OmniPass in the root directory (e.g. C:\).
3. Once OmniPass has completed installation you will be prompted to restart your system. Once your system has rebooted you will be able to use OmniPass. If you choose not to restart immediately after installation, OmniPass will not be available for use until the next reboot.



The installation program automatically places an icon (Softex OmniPass) in the Windows Control Panel as well as a golden key shaped icon in the taskbar.

Verifying Information about OmniPass

After you have completed installing OmniPass and restarted your system, you may wish to check the version of OmniPass on your system.

To check the version information of OmniPass:

1. From the Windows Desktop, double-click the key-shaped OmniPass icon in the taskbar (usually located in the lower right corner of the screen), or,
Click the **Start** button, select **Settings**, and click **Control Panel** (if you are using Windows XP you will see the Control Panel directly in the Start menu; click it, then click **Switch to Classic View**). Double-click **Softex OmniPass** in the Control Panel, and the OmniPass Control Center will appear. If it does not appear, then the program is not properly installed, or,
Click the **Start** button, select **Programs**, and from the submenu select the **Softex** program group, from that submenu click **OmniPass Control Center**.
2. Select the **About** tab at the top of the OmniPass Control Panel. The About tab window appears with version information about OmniPass.

Uninstalling OmniPass



For uninstallation, OmniPass requires that the user uninstalling OmniPass have administrative privileges to the system. If your current user does not have administrative privileges, log out and then log in with an administrator user before proceeding with OmniPass uninstallation.

To remove the OmniPass application from your system:

1. Click **Start** on the Windows taskbar. Select **Settings**, and then **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Select **OmniPass**, and then click **Change/Remove**.
4. Follow the directions to uninstall the OmniPass application.
5. Once OmniPass has finished uninstalling, reboot your system when prompted.

USER ENROLLMENT

Before you can use any OmniPass features you must first enroll a user into OmniPass.

Master Password Concept

Computer resources are often protected with passwords. Whether you are logging into your computer, accessing your email, e-banking, paying bills online, or accessing

network resources, you often have to supply credentials to gain access. This can result in dozens of sets of credentials that you have to remember.

During OmniPass user enrollment a "master password" is created for the enrolled user. This master password "replaces" all other passwords for sites you register with OmniPass.

Example: A user, John, installs OmniPass on his system (his home computer) and enrolls an OmniPass user with username "John_01" and password "freq14". He then goes to his webmail site to log onto his account. He inputs his webmail credentials as usual (username "John_02" and password "lifebook"), but instead of clicking [Submit], he directs OmniPass to **Remember Password**. Now whenever he returns to that site, OmniPass will prompt him to supply access credentials.

John enters his OmniPass user credentials ("John_01" and "freq14") in the OmniPass authentication prompt, and he is allowed into his webmail account. He can do this with as many web sites or password protected resources he likes, and he will gain access to all those sites with his OmniPass user credentials ("John_01" and "freq14"). This is assuming he is accessing those sites with the system onto which he enrolled his OmniPass user. OmniPass does not actually change the credentials of the password protected resource. If John were to go to an Internet cafe to access his webmail, he would need to enter his original webmail credentials ("John_02" and "lifebook") to gain access. If he attempts his OmniPass user credentials on a system other than where he enrolled that OmniPass user, he will not gain access.

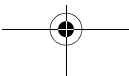


The enrollment procedure assumes you have no hardware authentication devices or alternate storage locations that you wish to integrate with OmniPass. If you desire such functionality, consult the appropriate sections of this document.

Basic Enrollment

The Enrollment Wizard will guide you through the process of enrolling a user. Unless you specified otherwise, after OmniPass installation the Enrollment Wizard will launch on Windows login. If you do not see the Enrollment Wizard, you can bring it up by clicking **Start** on the Windows taskbar; select **Programs**; select **Softex**; click **OmniPass Enrollment Wizard**.

1. Click **Enroll** to proceed to username and password verification. By default, the OmniPass Enrollment Wizard enters the credentials of the currently logged in Windows user.
2. Enter the password you use to log in to Windows. This will become the "master password" for this OmniPass user. In most cases, the **Domain:** value





Using the Fingerprint Sensor

- will be your Windows computer name. In a corporate environment, or when accessing corporate resources, the **Domain:** may not be your Windows computer name. Click [Next] to continue.
3. In this step OmniPass captures your fingerprint. Refer to “Enrolling a Fingerprint” on page 101 for additional information.
 4. Next, choose how OmniPass notifies you of various events. We recommend you keep **Taskbar Tips on Beginner mode taskbar tips** and **Audio Tips** on at least **Prompt with system beeps only** until you get accustomed to how OmniPass operates. Click [Next] to proceed with user enrollment. You will then see a Congratulations screen indicating your completion of user enrollment.
 5. Click [Done] to exit the OmniPass Enrollment Wizard. You will be asked if you’d like to log in to OmniPass with your newly enrolled user; click [Yes].

Enrolling a Fingerprint

Enrolling a fingerprint will increase the security of your system and streamline the authentication procedure.

You enroll fingerprints in the OmniPass Control Center. With an OmniPass user logged in, double-click the system tray OmniPass icon. Select the **User Settings** tab and click **Enrollment** under the **User Settings** area. Click **Enroll Authentication Device** and authenticate at the authentication prompt to start device enrollment.

1. During initial user enrollment, you will be prompted to select the finger you wish to enroll. Fingers that have already been enrolled will be marked by a green check. The finger you select to enroll at this time will be marked by a red arrow. OmniPass will allow you re-enroll a finger. If you choose a finger that has already been enrolled and continue enrollment, OmniPass will enroll the fingerprint, overwriting the old fingerprint. Select a finger to enroll and click [Next].
2. It is now time for OmniPass to capture your selected fingerprint. It may take a several capture attempts before OmniPass acquires your fingerprint. Should OmniPass fail to acquire your fingerprint, or if the capture screen times out, click [Back] to restart the fingerprint enrollment process.

Your system has a “swipe” fingerprint sensor. A swipe sensor is small and resembles a skinny elongated rectangle. To capture a fingerprint, gently swipe or pull your fingertip over the sensor (starting at the second knuckle) **towards yourself**. Swiping too fast or too slow will result in a failed capture. The **Choose Finger** screen has a [Practice] button; click it to practice capturing your fingerprint. When you are comfortable with how your fingerprint is captured, proceed to enroll a finger.

3. Once OmniPass has successfully acquired the fingerprint, the **Verify Fingerprint** screen will automatically appear. To verify your enrolled fingerprint, place your fingertip on the sensor and hold it there as if you were having a fingerprint captured. Successful fingerprint verification will show a green fingerprint in the capture window and the text **Verification Successful** under the capture window.

USING OMNIPASS

You are now ready to begin using OmniPass. Used regularly, OmniPass will streamline your authentications.

Password Replacement

You will often use the password replacement function. When you go to a restricted access website (e.g., your bank, your web-based email, online auction or payment sites), you are always prompted to enter your login credentials. OmniPass can detect these prompts and you can teach OmniPass your login credentials. The next time you go to that website, you can authenticate with your fingerprint to gain access.

OmniPass Authentication Toolbar

After installing OmniPass and restarting, you will notice a dialog you have not seen before at Windows Logon. This is the OmniPass Authentication Toolbar, and it is displayed whenever the OmniPass authentication system is invoked. The OmniPass authentication system may be invoked frequently: during Windows Logon, during OmniPass Logon, when unlocking your workstation, when resuming from standby or hibernate, when unlocking a password-enabled screensaver, during password replacement for remembered site or application logins, and more. When you see this toolbar, OmniPass is prompting you to authenticate.

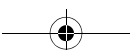
The **Logon Authentication** window indicates what OmniPass-restricted function you are attempting. The icons in the lower left (fingerprint and key) show what authentication methods are available to you. Selected authentication methods are highlighted while unselected methods are not. When you click the icon for an unselected authentication method, the authentication prompt associated with that method is displayed.

When prompted to authenticate, you must supply the appropriate credentials: an enrolled finger for the fingerprint capture window or your master password for the master password prompt (the key icon).

Remembering a Password

OmniPass can remember any application, GUI, or password protected resource that has a password prompt.

Using the following procedure, you can store a set of credentials into OmniPass. These credentials will then be linked to your “master password” or fingerprint.





Go to a site that requires a login (username and password), but *do not log in yet*. At the site login prompt, enter your username and password in the prompted fields, but *do not enter the site* (do not hit [Enter], [Submit], [OK], or Login). Right-click the OmniPass system tray icon and select **Remember Password** from the submenu. The Windows arrow cursor will change to a golden key OmniPass cursor. Click this OmniPass cursor in the login prompt area, but do not click the [Login] or [Submit] button.

Associating a Friendly Name

After clicking the OmniPass key cursor near the login prompt, OmniPass will prompt you to enter a “friendly name” for this site. You should enter something that reminds you of the website, the company, or the service you are logging into. In its secure database, OmniPass associates this friendly name with this website.

Additional Settings for Remembering a Site

When OmniPass prompts you to enter a “friendly name” you also have the opportunity to set how OmniPass authenticates you to this site. There are three effective settings for how OmniPass handles a remembered site.

The default setting is **Automatically click the “OK” or “Submit” button for this password protected site once the user is authenticated**. With this setting, each time you navigate to this site OmniPass will prompt you for your master password or fingerprint authentication device. Once you have authenticated with OmniPass, you will automatically be logged into the site.

Less secure is the option to **Automatically enter this password protected site when it is activated. Do not prompt for authentication**. Check the upper box to get this setting, and each time you navigate to this site OmniPass will log you into the site without prompting you to authenticate.



This setting is more convenient in that whenever you go to a site remembered with this setting, you will bypass any authentication procedure and gain instant access to the site. But should you leave your system unattended with your OmniPass user logged in, anyone using your system can browse to your password protected sites and gain automatic access.

If you uncheck both boxes in **Settings for this Password Site**, OmniPass will prompt you for your master password or fingerprint authentication device. Once you have authenticated with OmniPass your credentials will be filled in to the site login prompt, but you will have to click the website [OK], [Submit], or [Login] button to gain access to the site.

Click **Finish** to complete the remember password procedure. The site location, the credentials to access the site, and the OmniPass authentication settings for the site are now stored in the OmniPass secure database. The OmniPass authentication settings (**Settings for this Password Site**) can always be changed in **Vault Management**.

Logging in to a Remembered Site

Whether or not OmniPass prompts you to authenticate when you return to a remembered site is determined by **Settings for this Password Site** and can be changed in **Vault Management**.

The following cases are applicable to using OmniPass to login to: Windows, remembered web sites, and all other password protected resources.

With Master Password

Once you return to a site you have remembered with OmniPass, you may be presented with a master password prompt. Enter your master password and you will be allowed into the site.

Logging into Windows with a Fingerprint Device

When logging into Windows with a fingerprint device, the fingerprint capture window will now appear next to the Windows Login screen. Place your enrolled fingertip on the sensor to authenticate. You will be simultaneously logged into Windows and OmniPass. The capture window will also appear if you have used **Ctrl-Alt-Del** to lock a system, and the fingerprint device can be used to log back in as stated above.



If a machine is locked and OmniPass detects a different user logging back in with a fingerprint, the first user will be logged out and the second user logged in.

In Windows XP, your login options must be set either for classic login, or for fast user switching and logon screen to be enabled to use your fingerprint to log on to Windows. To change this go to **Control Panel**, select **User Accounts** and then click **Change the way users log on or off**. If your Windows screensaver is password protected, the fingerprint capture window will now appear next to screensaver password dialog during resume. You can authenticate to your screensaver password prompt with your enrolled finger.

Password Management

OmniPass provides an interface that lets you manage your passwords. To access this GUI, double-click the OmniPass key in the system tray. Click **Vault Management**; you will be prompted to authenticate. Once you gain access to **Vault Management**, click **Manage Passwords** under **Vault Settings**. You will see the **Manage Passwords** interface, with a list of friendly names.





Using the Fingerprint Sensor

You can view the credentials stored for any remembered website by highlighting the desired resource under **Password Protected Dialog** and clicking **Unmask Values**. Should a password be reset, or an account expire, you can remove stored credentials from OmniPass. Highlight the desired resource under **Password Protected Dialog** and click **Delete Page**. You will be prompted to confirm the password deletion.

The two check boxes in **Manage Passwords** govern whether OmniPass prompts you to authenticate or directly logs you into the remembered site.

OmniPass will overwrite an old set of credentials for a website if you attempt to use **Remember Password** on an already remembered site.

The exception to the above rule is the resetting of your Windows password. If your password is reset in Windows, then the next time you login to Windows, OmniPass will detect the password change and prompt you to “Update” or “Reconfirm” your password with OmniPass. Enter your new Windows password in the prompt(s) and click **OK** and your OmniPass “master password” will still be your Windows password.

OmniPass User Identities

Identities allow OmniPass users to have multiple accounts to the same site (e.g., *bob@biblomail.com* and *boballen@biblomail.com*). If OmniPass did not provide you identities, you would be limited to remembering one account per site.

To create and manage identities, double-click the OmniPass key in the system tray. Click **Vault Management**; OmniPass will prompt you to authenticate. Once you gain access to **Vault Management**, click **Manage Identities** under **Vault Settings**. You can only manage the identities of the currently logged in OmniPass user

To add a new identity, click **New Identity** or double-click **Click here to add a new identity**. Name the new identity and click [OK], then click [Apply]. You can now switch to the new identity and start remembering passwords.

To delete an identity, highlight the identity you want to delete and click [Delete Identity], then click [Apply].



When you delete an identity, all of its associated remembered sites and password protected dialogs are lost.

To set the default identity, highlight the identity you want as default and click [Set as Default]; click [Apply] to ensure the settings are saved. If you log in to OmniPass with a fingerprint device, you will automatically be logged in to the default identity for that OmniPass user. You can choose the identity with which you are logging in if you login using “master password”.

Choosing User Identity during Login

To choose your identity during login, type your username in the **User Name:** field. Press [Tab] and see that the **Domain:** field self-populates. Click the **Password:** field to bring the cursor to it, and you will see the pull-down menu in the **Identity:** field. Select the identity you wish to login as and then click **OK** to login.

Switch User Identity

To switch identities at any time, right-click the OmniPass system tray icon and click **Switch User Identity** from the submenu. The **Switch Identity** dialog will appear. Select the desired identity and then click **OK**.

Identities and Password Management

On the **Manage Passwords** interface of the **Vault Management** tab of the OmniPass Control Center, there is a pull-down selection box labeled, **Identity**. This field lets you choose which identity you are managing passwords for. When you select an identity here, only those password protected dialogs that are associated with that identity are shown. You can perform all the functions explained in “Password Management” on page 102.

CONFIGURING OMNIPASS

This section gives an overview of both the Export/Import function and the OmniPass Control Center.

Exporting and Importing Users

Using the OmniPass Control Center, you can export and import users in and out of OmniPass. The export process backs up all remembered sites, credentials, and any enrolled fingerprints for an OmniPass user. All OmniPass data for a user is backed up to a single encrypted database file. During the import process, the Windows login of the exported user is required. If the proper credentials cannot be supplied, the user profile will not be imported.



- You should periodically export your user profile and store it in a safe place. If anything happens to your system, you can import your OmniPass profile to a new system and have all your remembered settings and fingerprints instantly.
- You don't forget the Windows login credentials when exporting. When you examine the importation, you are prompted for authentication. The credentials that will allow a user profile to be imported are the Windows login credentials of the exported user. They are the credentials that had to be submitted when the user profile was exported. You will need User Name, Password, and Domain.

Exporting an OmniPass User Profile

To export a user, open the OmniPass Control Center, and click **Import/Export User** under **Manage Users**.

Click **Exports an OmniPass user profile**. OmniPass will prompt you to authenticate. Upon successfully authentication, you must name the OmniPass user profile and decide where to save it. An .opi file is generated, and you should store a copy of it in a safe place.

This .opi file contains all your user specific OmniPass data, and it is both encrypted and password protected. This user profile does NOT contain any of your encrypted data files.

Importing an OmniPass User Profile



You cannot import a user into OmniPass if there already is a user with the same name enrolled in OmniPass.

To import an OmniPass user open the OmniPass Control Center, and click **Import/Export User** under **Manage Users**. Click **Imports a new user into OmniPass** and then select **OmniPass Import/Export File (*.opi)** and click **Next**. OmniPass will then prompt you to browse for the file you had previously exported (.opi file). When you select the .opi file for importation, OmniPass will prompt you for authentication. The credentials that will allow a user profile to be imported are the Windows login credentials of the exported user. They are the credentials that had to be submitted when the user profile was exported. You will need **User Name**, **Password**, and **Domain**. If you don't remember the value for **Domain**, in a PC or SOHO environment **Domain** should be your computer name.

OmniPass will notify you if the user was successfully imported.

Things to Know Regarding Import/Export

- Assume you export a local Windows User profile from OmniPass. You want to import that profile to another machine that has OmniPass. Before you can import the profile, a Windows user with the same login credentials must be created on the machine importing the profile.

Example: I have a Windows user with the username "Tom" and the password "Sunshine" on my system. I have enrolled Tom into OmniPass and remembered passwords. I want to take all my passwords to new system. I export Tom's OmniPass user profile. I go to my new system and using the Control Panel I create a user with the username "Tom" and the password "Sunshine". I can now successfully import the OmniPass user data to the new system.

- If you export an OmniPass-only user, you can import that user to any computer running OmniPass, provided that a user with that name is not already enrolled in OmniPass.
- If you attempt to import a user profile who has the same name as a user already enrolled in OmniPass, the OmniPass import function will fail.

OMNIPASS CONTROL CENTER

This section will serve to explain functions within the OmniPass Control Center that weren't explained earlier.

You can access the OmniPass Control Center any of three ways:

- Double-click the golden OmniPass key shaped icon in the Windows taskbar (typically in the lower-right corner of the desktop)
- Click the **Start** button; select the **Programs** group; select the **Softex** program group; and click the **OmniPass Control Center** selection.
- Open the Windows **Control Panel** (accessible via **Start** button --> **Settings** --> **Control Panel**) and double-click the **Softex OmniPass** icon.

User Management

The User Management tab has two major interfaces: **Add/Remove User** and **Import/Export User**. Import/Export User functionality is documented in "Exporting and Importing Users" on page 103. Add/Remove User functionality is straightforward.

If you click **Adds a new user to OmniPass** you will start the OmniPass Enrollment Wizard. The Enrollment Wizard is documented in "User Enrollment" on page 100.

If you click **Removes a user from OmniPass**, OmniPass will prompt you to authenticate. Authenticate with the credentials (or enrolled fingerprint) of the user you wish to remove. OmniPass will prompt you to confirm user removal. Click **OK** to complete user removal.



Removing a user will automatically destroy all OmniPass data associated with that user. All identities and credentials associated with the user will be lost.

If you are sure about removing the user, we recommend you export the user profile.

User Settings

The User Settings tab has four interfaces: **Audio Settings**, **Taskbar Tips**, and **Enrollment**. User settings allow users to customize OmniPass to suit their individual preferences. Under **User Settings (Audio Settings and Taskbar Tips)** you can set how OmniPass notifies the user of OmniPass events (e.g., successful login, access denied,



Using the Fingerprint Sensor

etc.). The details of each setting under the **Audio Settings** and **Taskbar Tips** interfaces are self-explanatory.

The **Enrollment** interface allows you to enroll fingerprints. For the procedure to enroll and authentication device refer to *Chapter 2.3*. To enroll additional fingerprints, click **Enroll Authentication Device**, and authenticate with OmniPass. Select the fingerprint recognition device in the **Select Authentication Device** screen (it should already be marked by a green check if you have a finger enrolled) and click **Next**.

System Settings

The OmniPass **Startup Options** interface can be found in the System Settings tab. With these options you can specify how your OmniPass Logon is tied to your Windows Logon.

The first option, **Automatically log on to OmniPass as the current user**, will do just as it says; during Windows login, you will be logged on to OmniPass using your Windows login credentials. If the user logging into Windows was never enrolled into OmniPass, upon login no one will be logged on to OmniPass. This setting is appropriate for an office setting or any setting where users must enter a username and password to log into a computer. This is the default setting.

With the second option, **Manually log on to OmniPass at startup**, OmniPass will prompt you to login once you have logged on to Windows.

With the third option, **Do not log on to OmniPass at startup**, OmniPass will not prompt for a user to be logged on.

You can manually log on to OmniPass by right-clicking the OmniPass taskbar icon and clicking **Log in User** from the right-click menu.

TROUBLESHOOTING

You cannot use OmniPass to create Windows users. You must first create the Windows user, and you will need administrative privileges to do that. Once the Windows user is created, you can add that user to OmniPass using the same username and password

Cannot add Windows users to OmniPass

If you experience difficulties adding a Windows user to OmniPass, you may need to adjust your local security settings. You can do this by going to **Start, Control Panel, Administrative Tools, and Local Security Settings**. Expand **Local Policies**, expand **Security Options**, and double-click **Network Access: Sharing and Security Model for Local Accounts**. The correct setting should be *Classic - Local Users Authenticate as Themselves*.

Cannot add a User with a Blank Password to OmniPass

If you experience difficulties adding a user with a blank password to OmniPass, you may need to adjust your local security settings. First attempt the procedure explained in the *Cannot add Windows user to OmniPass* section. If the difficulties persist, then try the following procedure.

Click **Start, Control Panel, Administrative Tools, and Local Security Settings**. Expand **Local Policies**, expand **Security Options**, and double-click **Accounts: Limit local account use of blank passwords to console login only**. This setting should be set to **Disabled**.

Dialog appears after OmniPass authentication during Windows Logon

After installing OmniPass on your system, you can choose to logon to Windows using OmniPass. You authenticate with OmniPass (via master password, or an enrolled security device) and OmniPass logs you into Windows. You may, during this OmniPass authentication, see a **Login Error** dialog box.

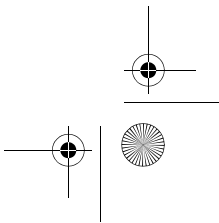
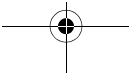
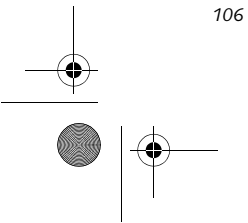
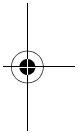
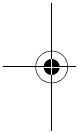
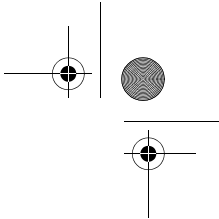
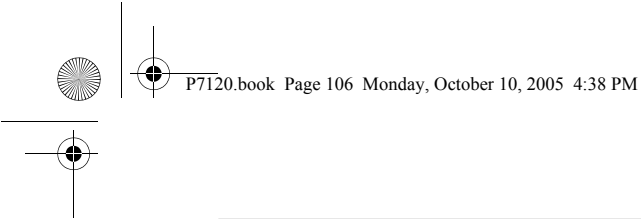
This dialog box occurs when OmniPass was unable to log you into Windows with the credentials supplied (username and password). This could happen for any of the following reasons:

- Your Windows password has changed
- Your Windows account has been disabled

If you are having difficulties due to the first reason, you will need to update OmniPass with your changed Windows account password. Click **Update Password** and you will be prompted with a dialog to reconfirm your password.

Enter the new password to your Windows user account and click **OK**. If the error persists, then it is unlikely the problem is due to your Windows user account password changing.







Index

A

AC	
adapter	23, 93
plug adapters	79
Auto Insert Notification	36
Auto/Airline Adapter	23, 93
Automatically Downloading Driver Updates	76

B

Battery	31
alarm	31
battery bay release button	11
care	80
charging indicator	12
conserving power	27
increasing life	80
level indicators	12
lithium ion battery	31, 94
low	31
recharging	31
replacing	32
shorted	32
suspend mode	31
swapping	32
BIOS	93
guide	26
setup utility	25
Bluetooth	62
Where to Find Information	62
Boot	93
sequence	25
built-in microphone	6

C

Cache Memory	93
CapsLock	12
Click Me!	26
Cold-swap	18
Contact Information	1
Cursor control	15
Cursor Keys	14

D

DC	
output cable	23
power jack	9, 23
Device Ports	42
DIMM	40
Disk care	80
Display Panel	6, 24
adjusting	24
brightness	24
closing	24
opening	24
Display Timeout	28
Dolby Headphone	35
Drivers and Application Restore CD	75
DVD/CD-RW drive	
control panel	35
loading	34
removing	35
software	35
tray release	74
using	36
DVD-RAM	34

E

ECO Button	27
Error Messages	73
Extended Memory	94
External Floppy Disk Drive	33
External Monitor Port	8, 44

F

FDU	26, 76, 87
Fingerprint Sensor Device	99
enrolling a fingerprint	101
getting started	99
installing OmniPass	99
logging into a remembered site	102
OmniPass authentication toolbar	101
password replacement	101
remembering a password	101
uninstalling OmniPass	100
user enrollment	100
using OmniPass	101





Firewire	8, 43
Flexible bay	8, 18
cold-swapping	18
hot-swapping	19
installing	18
release latch	11
removing	18
Floppy Disk	
ejecting	33
formatting	33
initializing	33
loading	33
preparing	33
write protect	33
Floppy Disk Drive	
care	80
Fujitsu Driver Update utility	26, 76, 87
Fujitsu HotKey Utility	87
Fujitsu LifeBook	
care and maintenance	79
traveling	79
Function Key	
F10	14
F3	14
F4	14
F5	14
F6	14
F7	14
F8	14
F9	14
Fn	14

G

Glossary	93
----------------	----

H

Hard Disk Timeout	28
Hard Disk/CD Access Indicator	12
Headphone Jack	7, 43
Hibernation Feature	28
disable/enable	28
Hot-swapping	19

I

IEEE 1394 port	8, 43
Integrated Wireless LAN	45
Internal LAN port	42

K

Keyboard	.6, 13
cursor keys	.13
function keys	.13
key indicator lights	.13
numeric keypad	.13
Windows keys	.13
windows keys	.13

L

LAN (RJ-45) port	8
LifeBook P7000 notebook	.5
unpacking	.5
Lithium ion Battery	.11

M

Memory	
capacity	.41
installing	.40
removing	.41
Memory Module Cover	.11
Memory Stick/SD Card	.9
installing	.38
removing	.39
slot	.9, 38
Memory Upgrade Module	.40
Microphone Jack	.6, 44
Modem	.8
port	.42
result codes	.74
Modular Devices	.18
installing	.18
removing	.18

N

Numeric Keypad	.13
NumLk	.12

O

Optical Drive	.34
care	.81
DVD/CD-RW combo	.34
emergency tray release	.36
Multi-Format DVD Writer	.34
software	.34



**Index****P**

PC Card	
care	81
installing	37
removing	37
slot	8
POST	73, 95
error messages	73
Power	
AC adapter	23
auto/airline adapter	23
management	27
off	28
sources	23
Power Management	27
Power On	25
Power On Self Test	73
Pre-Installed Software	87
Adobe Acrobat Reader	87
manuals	87
Norton AntiVirus 2004	87
Quicken New User Edition	87
tutorials	87
Pre-installed Software	
restoring	75
PS/2	95

R

Registration	26
Regulatory Information	89
Re-Installing Individual Drivers and Applications	75
Restarting	28
Restoring software	75
Restoring the Factory Image	75
RJ-11	8, 42
RJ-45	8, 42

S

ScrLk	12
SD Card	
installing	38
removing	39
SDRAM	40
Secure Digital Card	
removing	39
Serial Port	95

Specifications	85
audio	85
device ports	86
dimensions and weight	86
environmental requirements	86
features	85
keyboard	86
mass storage device options	85
memory	85
microprocessor	85
MS Works	87
popular accessories	86
power	86
video	85
Status Indicator Panel	6, 12
Stereo Speakers	10
Suspend	96
Suspend Mode	27
Suspend/Resume/Power On Button	6, 27
S-Video Out Port	8, 43
Swapping batteries	32
System Specifications	85

T

Touchpad	15
buttons	15
clicking	15
controls	16
double-clicking	15
dragging	16
pointing device	6
scroll button	6
scrolling	16
Troubleshooting	65
battery	70
built-in speakers	66
display panel	71
DVD/CD-RW drive	66
hard disk drive	67
identifying the problem	65
keyboard	67
memory	68
modem	68
mouse	67
PC card	68, 69
power	69, 70
USB	68
Troubleshooting Table	66





U

Universal Serial Bus Ports 43

USB

ports 8, 9, 43

V

Volume Control 17

W

Warranty 1

Windows keys 13

application key 13

start keys 13

Wireless LAN

access point (infrastructure) mode 49

activating the WLAN device 50

ad hoc mode 48

before using the wireless LAN 48

configuration 51

deactivating the WLAN device 49

Devices covered by this document 48

IP address information 60

modes 48

on/off switch 6

specifications 61

troubleshooting 57

using Atheros Client Utility software 52

using Intel PROSet software 51

wireless LAN glossary 58

wireless network considerations 49



