

## 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 limit for class B digital devices, pursuant to parts 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 exigences 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 TÉLPHONIQUES 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.



# Appendix A: WLAN User's Guide

## **FCC Regulatory Information**

Please note the following regulatory information related to the optional wireless LAN device.

### **Regulatory Notes and Statements**

#### **Wireless LAN, Health and Authorization for use**

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions, however, are far much less than the electromagnetic energy emissions from wireless devices such as mobile phones. Wireless LAN devices are safe for use by consumers because they operate within the guidelines found in radio frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments, such as:

- On board an airplane, or
- In an explosive environment, or
- In situations where the interference risk to other devices or services is perceived or identified as harmful.

In cases in which the policy regarding use of Wireless LAN devices in specific environments is not clear (e.g., airports, hospitals, chemical/oil/gas industrial plants, private buildings), obtain authorization to use these devices prior to operating the equipment.

#### **Regulatory Information/Disclaimers**

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution or attachment of connecting cables and equipment other than those specified by the manufacturer. It is the responsibility of the user to correct any

interference caused by such unauthorized modification, substitution or attachment. The manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failure to comply with these guidelines.

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

**For IEEE 802.11a Wireless LAN:** For operation within 5.15~5.25 GHz frequency range, it is restricted to indoor environments, and the antenna of this device must be integral.

### **Federal Communications Commission statement**

This device complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions: (1) This device may not cause interference, and, (2) This device must accept any interference, including interference that may cause undesired operation of this device.

### **FCC Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it 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 and correct the interference by one or more of the following measures:

- 1** Reorient or relocate the receiving antenna.
- 2** Increase the distance between the equipment and the receiver.
- 3** Connect the equipment to an outlet on a circuit different from the one the receiver is connected to.
- 4** Consult the dealer or an experienced radio/TV technician for help.

### **FCC Radio Frequency Exposure statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the Wireless LAN antenna (located on the top edge of the LCD screen) and your body. The transmitters in this device must not be co-located or operated in conjunction with any other antenna or transmitter.

## **Export restrictions**

This product or software contains encryption code which may not be exported or transferred from the US or Canada without an approved US Department of Commerce export license. This device complies with Part 15 of FCC Rules., as well as ICES 003 B / NMB 003 B. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesirable operation. Modifications not expressly authorized by Fujitsu Computer Systems Corporation may invalidate the user's right to operate this equipment.

## **Canadian Notice**

The device for the 5150 - 5250 MHz band is only for indoor usage to reduce the potential for harmful interference to co-channel mobile satellite systems.

The maximum antenna gain of 6 dBi permitted (for devices in the 5250 - 5350 MHz, 5470 - 5725 MHz and 5725 - 5825 MHz bands) to comply with the e.i.r.p. limit as stated in A9.2 of RSS210.

In addition, users are cautioned to take note that high power radars are allocated as primary users (meaning they have priority) of 5250 - 5350 MHz and 5650 - 5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.



## Before Using the Optional 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 device" in the rest of the manual). Before using the WLAN device, read this manual carefully to ensure its correct operation. Keep this manual in a safe place for future reference.

### Wireless LAN Device Covered by this Document

This document is applicable to systems containing the following WLAN device:

- Integrated Intel WiFi Link 5300 (802.11a/b/g/draft-n)

### Characteristics of the WLAN Device

- The WLAN device is a Mini-PCI card attached to the main board of the mobile computer.
- The WLAN device operates in license-free RF bands, eliminating the need to procure an FCC operating license. The WLAN operates in the 2.4GHz Industrial, Scientific, and Medical (ISM) RF band and the lower, middle, and upper bands of the 5GHz Unlicensed National Information Infrastructure (UNII) bands.
- The Intel WiFi Link 5300 WLAN device is capable of four operating modes, IEEE802.11a, IEEE802.11b, IEEE802.11g, and IEEE802.11n (draft)
- The WLAN device is Wi-Fi certified and operate (as applicable) at a the maximum data rate of 540 Mbps (theoretical) in IEEE802.11n (draft) mode; 54 Mbps in IEEE802.11a or IEEE802.11g mode; and 11 Mbps in IEEE802.11b mode.
- The WLAN device supports the following encryption methods - WEP, TKIP, CKIP, and AES encryption.
- The Wireless LAN device is compliant with the following standards: WPA, WPA2, CCX1.0, CCX2.0, CCX3.0, and CCX4.0.

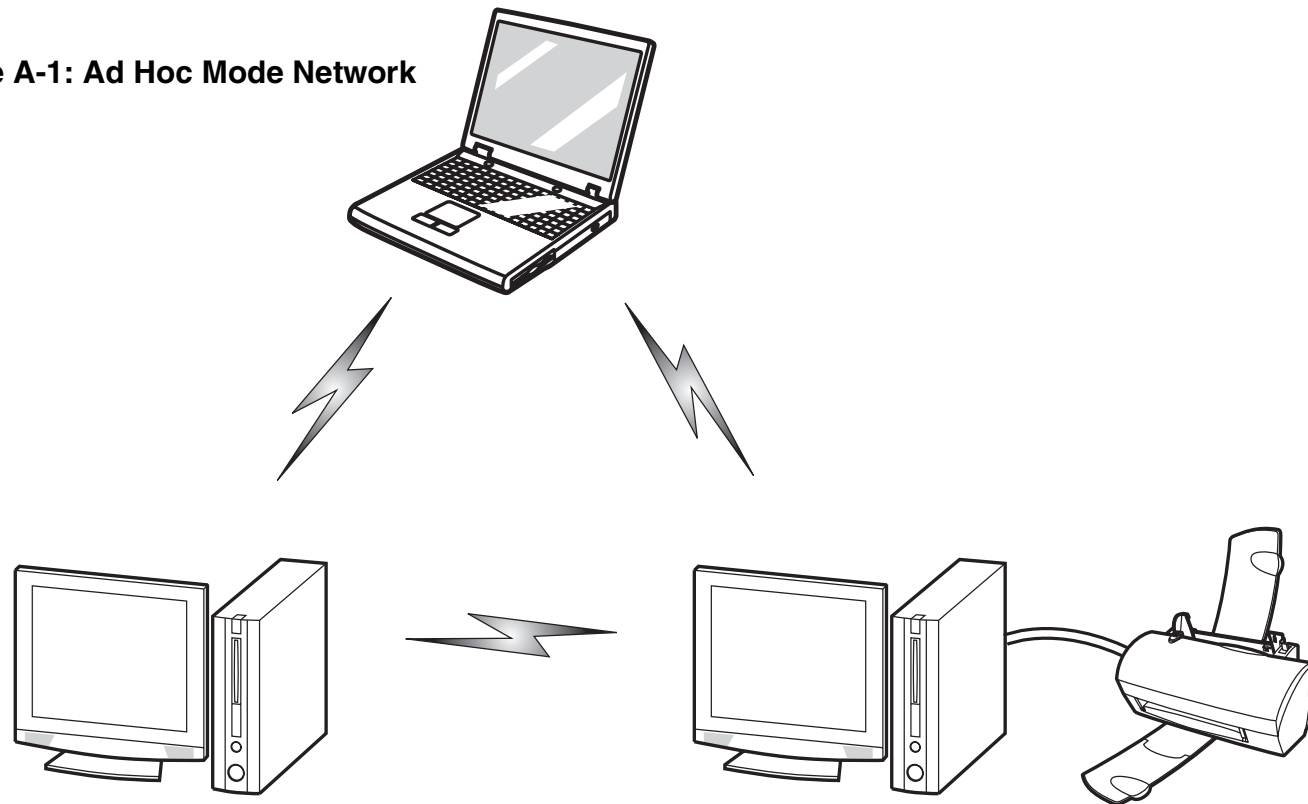
## Wireless LAN Modes Using this Device

### Ad Hoc Mode

(See Figure A-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.

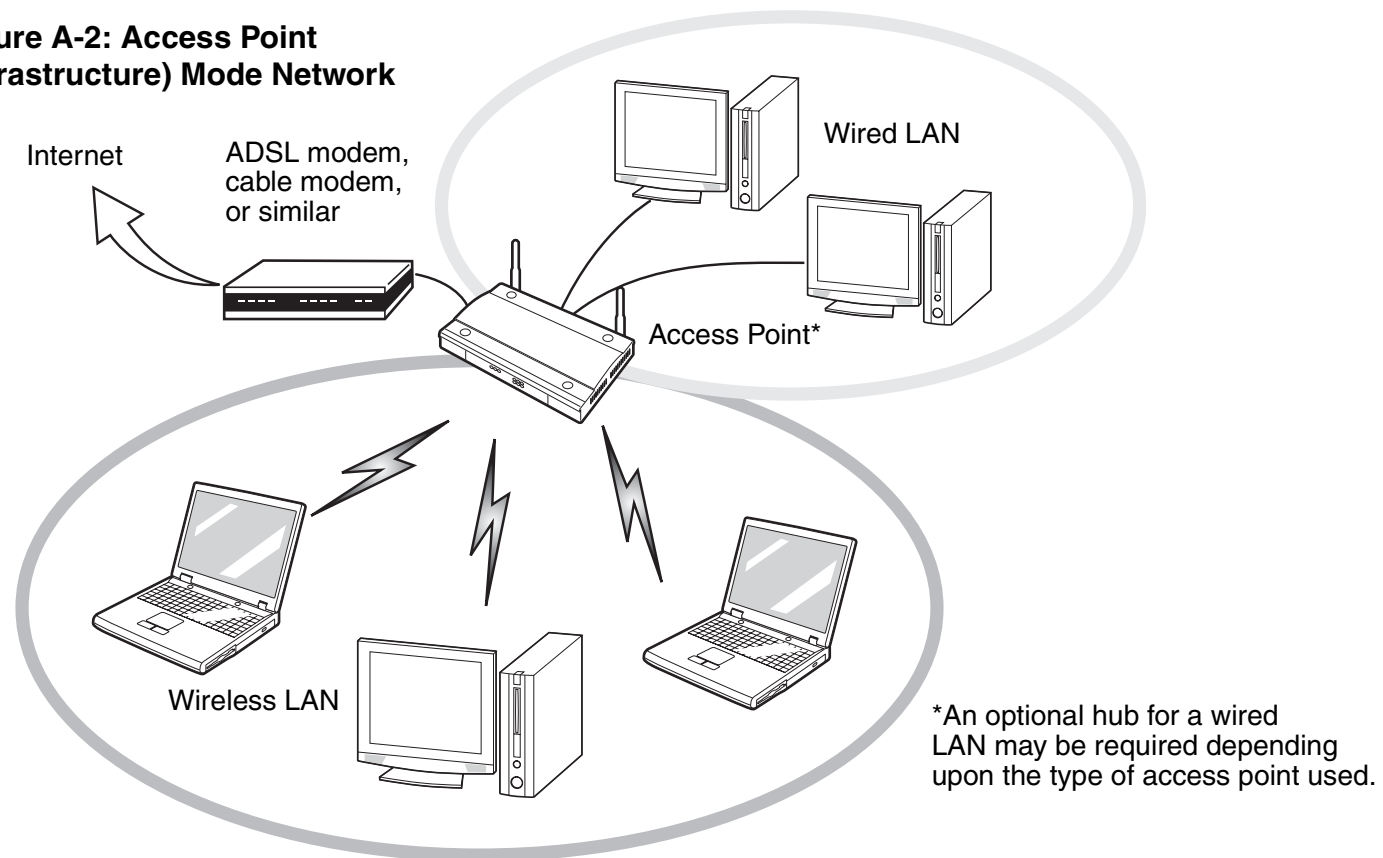
**Figure A-1: Ad Hoc Mode Network**



## Access Point (Infrastructure) Mode

(See Figure A-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 with a wired network. Corporate wireless networks operate in infrastructure mode because they require access to the WLAN in order to access services, devices, and computers (e.g., file servers, printers, databases).

**Figure A-2: Access Point (Infrastructure) Mode Network**



The WLAN device is an optional device that may come 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

- Intel WiFi Link 5300 device supports IEEE802.11a, IEEE802.11b, IEEE802.11g, and IEEE802.11n.
- The WLAN device operates in the 2.4 GHz ISM band and the 5 GHz lower, middle, and upper UNII bands.
- Microwave ovens may interfere with the operation of WLAN devices since they operate in the same 2.4 GHz frequency range as IEEE802.11b/g/n devices. Interference by microwaves does not occur with IEEE802.11a radio which operates in the 5 GHz RF band.
- Wireless devices that transmit in the 2.4 GHz range may interfere with operation of WLAN devices in IEEE802.11b/g/n modes. Symptoms of interference include reduced throughput, intermittent disconnects, and many frame errors. It is **HIGHLY** recommended that these interfering devices be powered off to ensure proper operation of the WLAN device.

## Deactivating/Disconnecting the WLAN Device

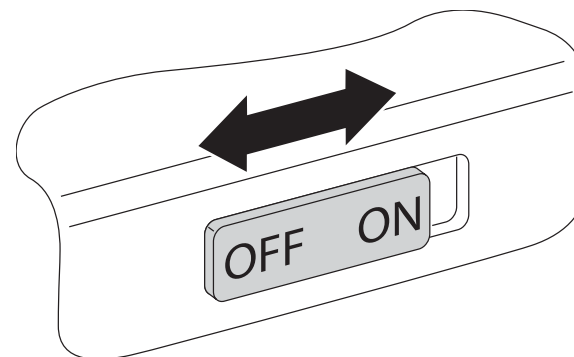
Deactivation of the WLAN device may be desired in certain circumstances (to extend battery life) or where certain environments require it (i.e. hospitals, clinics, airplanes, etc.).



BEFORE USING THE WIRELESS LAN DEVICE, YOU MUST FIRST INSTALL **CLICKME!** TO ENSURE THAT THE CORRECT SOFTWARE FOR YOUR DEVICE IS INSTALLED. SEE “INSTALLING CLICK ME!” ON PAGE 57.

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



**Figure 30. Wireless LAN On/Off Switch**

THE WIRELESS LAN/BLEETOOTH ON/OFF SWITCH WILL POWER OFF BOTH THE OPTIONAL WIRELESS LAN AND BLEETOOTH 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** Use the Bluetooth icon in the system tray to disable Bluetooth radio.
- 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].

## Activating the WLAN Device

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

# Configuring the Wireless LAN

The optional WLAN device can be configured to establish wireless network connectivity using the software that is built into Windows Vista. Support for most industry standard security solutions is contained in this software.

Pre-defined parameters will be required for this procedure. Please consult with your network administrator for these parameters:

## Configuring the WLAN Using Windows Vista

- 1** Click the Start button, then select Control Panel.
- 2** If the Control Panel is not in Classic View, select Classic View from the left panel. Double-click the Network and Sharing Center icon.
- 3** Select “Manage wireless networks” from the left panel.
- 4** Click on the [Add] button.
- 5** Depending upon what type of connection you would like to make, make a selection. For an infrastructure network, select “Manually create a network profile. For ad hoc network, select “Create an ad hoc network”.
- 6** Enter the required information. It may be necessary to consult with your network administrator for some of the information.
- 7** In the event you require assistance, go to the Network and Sharing Center window (Start -> Control Panel -> Network and Sharing Center), and type in relevant keywords in the Search box.

## Connecting to a Network

After you have configured your computer, you can connect to an active network by performing the following steps:

- 1** Click on the WLAN icon in the system tray.
- 2** Select “Connect to a network”.
- 3** Select a network from the list that appears, and click the [Connect] button.

## Configuring the WLAN Using Windows XP

### Procedure

- 1** Click the Start button, then select Control Panel.
- 2** If the Control Panel is not in Classic View, select Classic View from the left panel. Double-click the Network Connections icon.
- 3** Select “New Connection” wizard.
- 4** Click the [Next] button.
- 5** Select “Connect to the Internet”, then click [Next].
- 6** Depending upon what type of connection you would like to make, make a selection. For an infrastructure network, select “Manually create a network profile. For ad hoc network, select “Choose from a list of Internet service providers”.
- 7** Enter any required information. It may be necessary to consult with your network administrator for some of the information.
- 8** In the event you require assistance, go to [Start] -> Help and Support -> Networking and the Web. Select the main topic in which you are interested, then type in relevant keywords in the Search box.

### Connection to the network

After you have configured your computer, you can connect to an active network by clicking on the Wireless Network icon in the system tray:

# Troubleshooting the WLAN

## 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	<p><b>Ad hoc connection:</b> 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.</p> <p><b>Access Point (Infrastructure) connection:</b> set the network name (SSID) and network key to the same values as those of the access point.</p> <p>Set the Network Authentication value identically to that of the Access Point. Please consult your network administrator for this value, if necessary.</p>
	Weak received signal strength and/or link quality	<p>Ad hoc connection: Retry connection after shortening the distance to the destination computer or removing any obstacles for better sight.</p> <p>Access Point (Infrastructure) connection: Retry connection after shortening the distance to the access point or removing any obstacles for better sight.</p>
	The WLAN device has been deactivated or disabled	Check if the wireless switch is turned On. Go to Start -> Control Panel, and double-click on Windows Mobility Center. If the wireless network is off, click the [Turn wireless on] button.



<b>Problem</b>	<b>Possible Cause</b>	<b>Possible Solution</b>
Unavailable network connection  (continued)	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.
	Incorrect IP address configuration	This only applies to networks using static IP addresses. Please contact your network administrator for the correct settings.

# WLAN Specifications

## Specifications

Item	Specification
Type of network	<p>The Intel WiFi Link 5300 WLAN device conforms to IEEE 802.11a, 802.11b/g, and 802.11n (draft-compliant), Wi-Fi based*.</p> <p>The Atheros SuperAG network card conforms to IEEE802.11a, IEEE802.11b, and IEEE802.11g, Wi-Fi based*</p>
Transfer rate	(Automatic switching) 54 Mbps maximum data rate (IEEE802.11n to be determined)
Active frequency	<ul style="list-style-type: none"> <li>• DTS:IEEE 802.11a / draft 802.11n Standard-20 MHz Channel mode / draft 802.11n Wide-40 MHz Channel mode: 5.745~5.825 GHz</li> <li>• IEEE 802.11b/g mode / draft 802.11n Standard-20 MHz Channel mode / draft 802.11n Wide-40 MHz Channel mode: 2.412~2.462 GHz</li> <li>• Bluetooth: 2402 ~ 2480 MHz</li> </ul>
Typical operating distances**	<ul style="list-style-type: none"> <li>• 802.11a: 40 ft. (12 m) @ 54 Mbps; 300 ft. (91 m) @ 6 Mbps</li> <li>• 802.11b: 100 ft. (30 m) @ 11 Mbps; 300 ft. (91 m) @ 1 Mbps</li> <li>• 802.11g: 100 ft. (30 m) @ 54 Mbps; 300 ft. (91 m) @ 1 Mbps</li> <li>• 802.11n (draft): Estimated double the operating distance of 802.11g and 802.11a in their respective frequencies.</li> </ul>
Number of channels	<ul style="list-style-type: none"> <li>• 802.11a: 8 independent channels</li> <li>• 802.11b/g: 11 channels, 3 non-overlapping channels</li> <li>• 802.11n (draft): 2.4 GHz - 3 non-overlapping channels when Channel Bonding is not used; 2 non-overlapping channels when Channel Bonding is used. 5 GHz - 12 non-overlapping UNII channels with or without Channel Bonding</li> </ul>
Security	<p>Encryption Types - WEP, TKIP, AES***, WPA 1.0 compliant</p> <p>Encryption Key lengths Supported: 64 bits and 128 bits 802.1x/EAP</p>
Maximum recommended number of computers to be connected over wireless LAN (during ad hoc connection)	10 units or less ****

Active frequency

UNII:

IEEE 802.11a / draft 802.11n Standard-20 MHz Channel mode / draft 802.11n Wide-40 MHz Channel mode: 5.18~5.24 GHz / 5.26~5.32 GHz / 5.50~5.70 GHz

- \* “Wi-Fi based” indicates that the interconnectivity test of the organization which guarantees the interconnectivity of wireless LAN (Wi-Fi Alliance) has been passed.
- \*\* The communication ranges shown above will increase or decrease depending on factors such as number of walls, reflective material, or interference from external RF sources.
- \*\*\* 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 Go to Start > **All Programs** > **Bluetooth**.
- 3 Click on **Options** under the Bluetooth menu and click on the **Bluetooth Radio Power** button.
- 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 Bluetooth, then select User's Guide. For additional information about Bluetooth Technology, visit the Bluetooth Web site at: [www.bluetooth.com](http://www.bluetooth.com).

**FCC Radiation Exposure Statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. The Bluetooth antenna is located on the right hinge of the LCD screen and is exempt from minimum distance criteria due to its low power.

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**

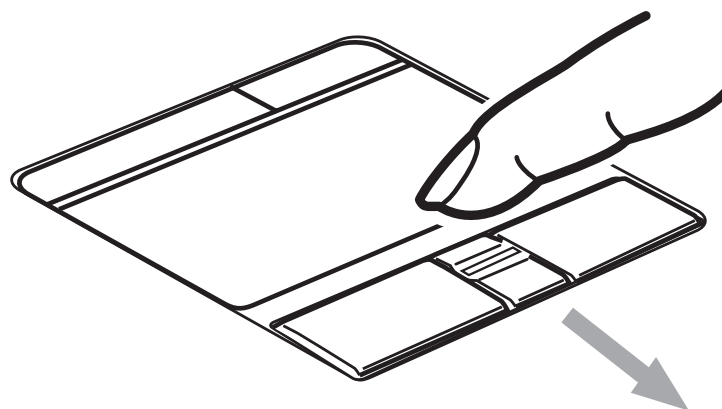
Users are not authorized to modify this product. Any modifications invalidate the warranty.

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.

# Appendix B: Fingerprint Sensor Device

## Introducing the Fingerprint Sensor Device

Your system may have an optional fingerprint sensor device below the Touchpad, between the left and right buttons. This also serves as a scroll button.



**Figure 31. 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
- Resume from sleep 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 173. You can determine whether OmniPass has already been installed by checking to see if the following are present:

- The gold key-shaped OmniPass icon in the system tray at the bottom right of the screen.
- 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 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 173. 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 you 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**. 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



BEFORE YOU UNINSTALL THE SOFTWARE, DECRYPT ALL OMNIPASS ENCRYPTED FILES AND EXPORT ALL OMNIPASS USER PROFILES. FAILURE TO DO SO MAY RESULT IN PERMANENT LOSS OF ENCRYPTED FILE DATA, AND PERMANENT LOSS OF ALL REMEMBERED PASSWORDS AND ASSOCIATED INFORMATION (SEE CHAPTER 5 OF THE OMNIPASS HELP DOCUMENT:: EXPORTING AND IMPORTING USERS).



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, 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 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") at 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 assumes 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 another computer without he OmniPass account 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 a system he's enrolled on, 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 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 175 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** 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** 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** 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 sleep 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 the OmniPass cursor in the login prompt area, but don’t click [Login] or [Submit].

### **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.

## 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.

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 when resetting the Windows password. If your password is reset in Windows, the next time you login to Windows, OmniPass will detect the password change and prompt you to “Update” or “Reconfirm” the password with OmniPass. Enter your new Windows password in the prompt and click **OK**. 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]. 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 to login as, then click **OK**.

### **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 179.

## **Configuring OmniPass**

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

### **Exporting and Importing Users**



YOU CANNOT IMPORT A USER INTO OMNIPASS IF THERE ALREADY IS A USER WITH THE SAME NAME ENROLLED IN OMNIPASS.

Using OmniPass Control Center, you can export and import users in and out of OmniPass. The export process backs up all remembered sites, credentials, and 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

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 181. 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 173.

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'RE SURE YOU WANT TO REMOVE 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, 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**, you will not be prompted 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 OmniPas

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.