

## BIOM34-EC Installation

### INTRODUCTION

APCs' Biometric Mouse Password Manager (BioM34, Figure 1) enables users to log on to a system or Internet website simply by placing their fingertip on the Biometric Sensor. Use the APC Biometric hardware and software to record and store fingerprint identification for use when accessing password-protected systems, applications, and web sites.



Figure 1. The APC BioM34

Caution: Do not allow metal or sharp objects to contact the sensor surface, as they could damage the unit.

### FEATURES

- Attached USB cable for easy connection to laptops and PCs
- Easy-to-use Master password for all types of Windows® applications, and on-line passwords
- Compatible with Microsoft Passport®
- Support for Internet Explorer®
- Compatible with Windows XP® Credential Manager
- User-friendly graphical user interface (GUI) that is easy to install, customize and use
- Full Windows OS support including Windows 2000®, and XP (Windows 95®, 98®, and ME® are not supported)
- International language support
- TruePrint™ compliant
- Full-Function mouse with rotating scroll wheel.

### SETUP

#### 1. Connect the BioM34.

Note: Before connecting the BioM34, uninstall any previously installed biometric hardware or related security software. To connect the BioM34, plug it into the USB port (Figure 2) of your laptop or CPU tower. You do not have to turn the computer off.



Note: Newer versions may have a black USB plug.

Figure 2. Connecting the BioM34

#### 2. Install the driver.

- Insert the software CD.
- The **Found New Hardware Wizard** screen appears. Select **Next**, then select **Search for a Suitable Driver**; select **Next**.
- Check the CD-ROM Drive's check box only; select **Next**.
- Once the driver is found, select **Next** to install it. The Hardware Wizard sends a message once installation is complete.

#### 3. Install the APC OmniPass® software.

Note: If an earlier version of the Omnipass software is installed on your computer, you should perform an **Export User** function in order to maintain your current database of websites and passwords.

Ensure to note your current **User Name, Domain, and Password**. You will need this information in order to perform an **Import**

**User** function when restoring your database after the software is installed. Please refer to the User Manual located on the software CD for more indepth information.

During software installation, the software will search for, and detect previous versions of the Omnipass software. If a previous version of the software is installed, you must use the **Uninstall Software** function in the computer's **Control Panel**, or the **Uninstall Omnipass** function - go to: **Start/Programs/Softex/Uninstall Omnipass**. Once the previous version of the software has been removed, you must restart your computer. Once the restart is complete, either re-install the software CD into the computer, or open the CD and double-click the **Setup.exe** icon. Advanced users perform the following:

**Start/Run/e://setup.exe.**

A. Insert the APC OmniPass software CD into the CDROM drive. The software will automatically start the installation proces. Within a few seconds, the **Starting InstallShield Wizard** screen will be displayed (Figure 3).



Figure 3. Starting InstallShield Wizard Screen

B. The software will then display the **Preparing Setup** screen (Figure 4). During setup, a progress bar is displayed.

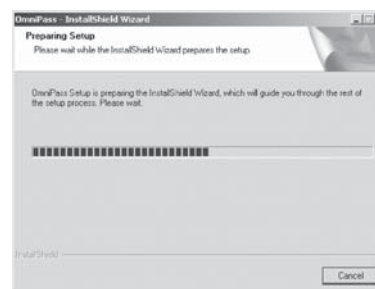


Figure 4. Preparing Setup Screen

C. Once the **InstallShield Setup** is complete, the software displays the **Welcome** screen (Figure 5). Click **Next** to continue installation.

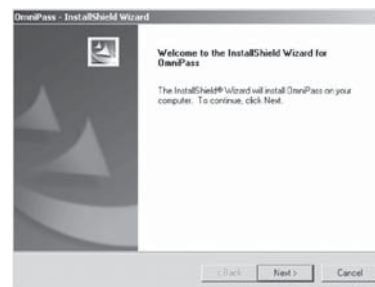


Figure 5. Welcome Screen

D. Once the **Setup Preparation** is complete, the software displays the **License Agreement** screen (Figure 6). Please read the entire agreement. If you agree to the terms, Click **Yes** to continue the installation. If you disagree with its terms, click **Cancel** to stop.

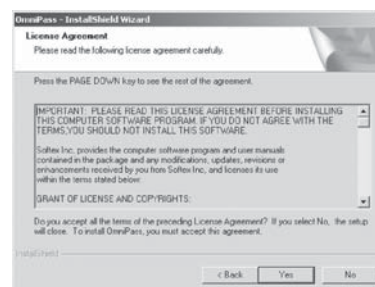


Figure 6. License Agreement Screen

E. Once you have accepted the terms of the License Agreement the **Choose Location Destination** screen is displayed (Figure 7).

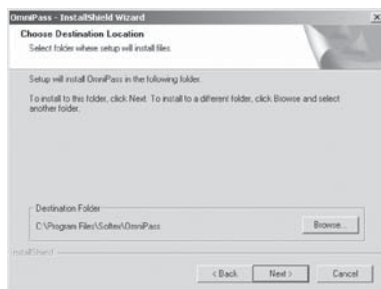


Figure 7. Choose Destination Location Screen

For most users, the destination location identified by the software is sufficient. If this is the case, click the **Next** button. Advanced users may want to select an alternate location for the software files by clicking the **Browse** button and locating the desired location. To stop the software installation, click the **Cancel** button.

F. Once you have chosen the destination location for the files, the **Setup Status** screen is displayed (Figure 8). During setup, a progress bar is displayed.

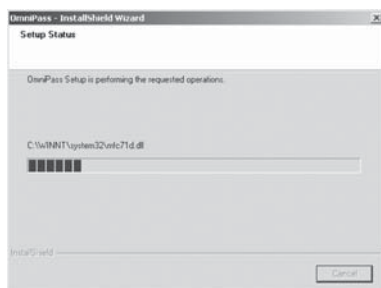


Figure 8. Setup Status Screen

G. Once setup is complete, the **Installing/Updating Driver for Devices...** screen is displayed (Figure 9).

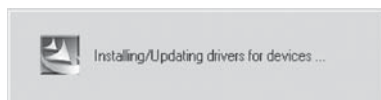


Figure 9. Installing/Updating Driver for Devices... Screen

H. After the software installation is complete, the **InstallShield Wizard Complete** screen is displayed (Figure 10). In order to the software installation to take affect, you must restart your computer. Click the circle next to **“Yes, I want to restart my computer now”**, then click **Finish** to perform a restart. To restart your computer at a later time, click the circle next to **“No, I will restart my computer later”**.

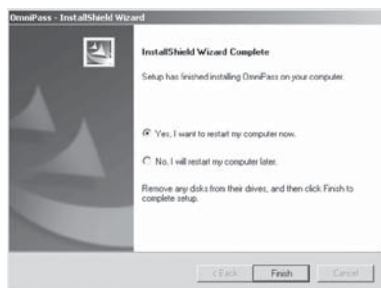


Figure 10. InstallShield Wizard Complete Screen

I. After restarting your computer, the Windows log-in screen will appear. The Omnipass software will also display a **Logon User Authentication** screen (Figure 11). Enter your User Name and Password in the Windows logon screen. You do not have to do anything with the Logon User Authentication screen at this time.



Figure 11. Logon User Authentication Screen

J. The software will then display the **Verify Username and Password** screen (Figure 12). Enter your Windows Username, Domain, and Password.



Figure 12. Verify User Name and Password Screen

K. Once logged into the Omnipass software, the **Select Authentication Device** screen is displayed (Figure13).



Figure 13. Select Authentication Device Screen

L. Click on the **APC Biometric Device** Icon (fingerprint graphic, Figure 13 and 14), the fingerprint box will change color (Figure 14).



Figure 14. Select Authentication Device Screen

#### 4 ENROLL FINGERPRINT

Once you have selected the APC Biometric Device icon, the **Choose Finger** screen (Figure 15) will be displayed.

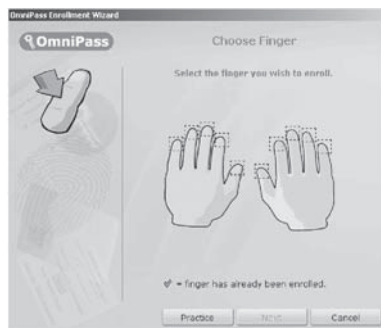


Figure 15. Choose Finger Screen

A. Click on the fingertip of the fingerprint you wish to enroll; a red arrow will appear above the selected finger (Figure 16). Click **Next** or **Cancel**.



Figure 16. Selected Finger Screen

B. The software will then display the Blank Capture Fingerprint screen (Figure 17). Place the chosen finger over the Sensor and Drive Ring (Figure 18).



Figure 17. Blank Capture Fingerprint Screen

Note: Place the finger on the BioM34 sensor and drive ring (Figure 18) for scanning. Use light, but firm and steady pressure. Ensure the finger makes contact with the BioM34 sensor and the surrounding drive ring. APC OmniPass works best when it has an image of the center of a fingerprint (core image). Capture the full area of the fingerprint by placing the finger flat on the BioM34 sensor. Do not place only the fingertip on the sensor, as it contains insufficient image data for a high-quality fingerprint

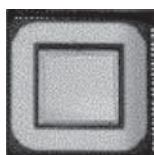


Figure 18. Sensor and Drive Ring

C. As you place your fingertip on the Sensor and Drive Ring (Figure 19), the system will record your fingerprint and display it in the gray box (Figure 20) and the box numbered "1" will turn green. You must raise the finger straight up and put it back on the sensor up to 8 times before the fingerprint is successfully recorded. Each time the fingerprint is recorded, another numbered box will turn green.



Figure 19. Finger Placement



Figure 20. Capture Fingerprint Screen

D. Once the device has successfully recorded your fingerprint, the system will display the **Verify Fingerprint** screen (Figure 21). Place your finger on the Sensor and Drive Ring.



Figure 21. Verify Fingerprint Screen

E. After the system has verified your fingerprint, it will then ask if you would like to enroll additional fingerprints (Figure 22). To enroll additional fingerprints, click **Yes**. To stop, click **No**.

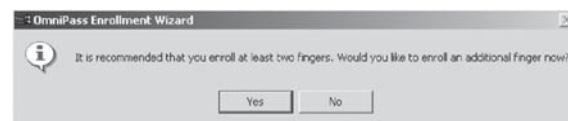


Figure 22. Additional Fingerprints Prompt

## 5. SELECT AUDIBLE AND TASKBAR SETTINGS

After enrolling and verifying your fingerprint, the system will allow you to set certain audible prompts, as well as what is displayed in the taskbar located at the bottomright side of your display (Figure 23).

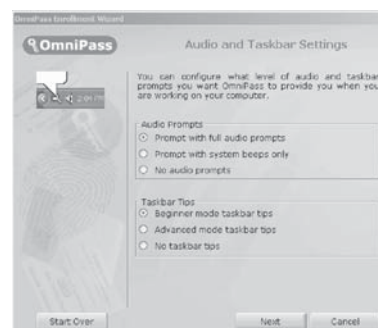


Figure 23. Audio and Taskbar Settings Screen

- A. Click on the circle next to the desired selection, then click on **Next**, **Cancel**, or **Start Over**.
- B. Once the settings have been chosen, select **Next** and the **Congratulations** screen (Figure 24) will be displayed. Click **Done** to complete the enrollment process; the **Logon New User** screen (Figure 25) is displayed. Click **Yes** to logon the new user, or click **No** to stop the installation process.

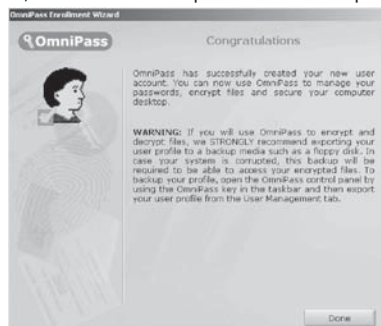


Figure 23. Congratulations Screen



Figure 24. Audio and Taskbar Settings Screen

- C. If you clicked on **Yes** to logon the new user, the **Logon User Authentication** screen (Figure 11) is displayed. Place your finger on the Sensor and Drive Ring. The system will read your fingerprint and log you onto your computer.

At this time, you should restart your computer to ensure the setup is complete. During restart, your Windows logon screen will appear. Within a few seconds, the **Logon User Authentication** screen (Figure 11) will also appear. You can either enter your Username and Password, or simply place your finger on the Sensor and Drive Ring of the BioM34. Upon authentication, the BioM34 will automatically fill in the Windows logon screen and log you onto the computer.

Once Windows has finished the restart process, a new icon will appear in the taskbar at the bottomright of your display (Figure 25).

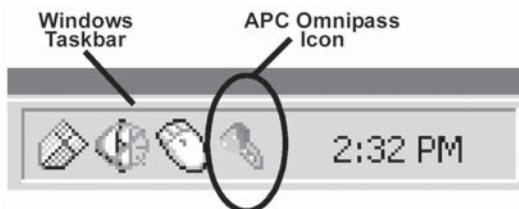


Figure 25. Taskbar and APC Omnipass Icon

- D. Hold your cursor over the APC Omnipass icon in the taskbar, and the system will display which user is currently logged on (Figure 26).



Figure 26. Logged On User Dialog

- E. Right-click on the APC Omnipass icon, and you can access other features and functions provided by the BioM34 (Figure 27).

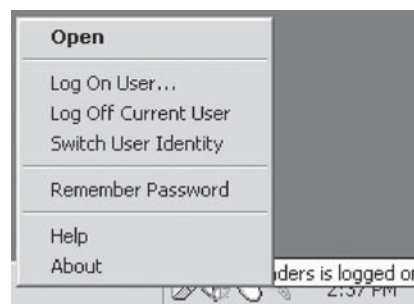


Figure 27. Features and Functions Drop-Down Menu

For information about how to use all of the features and functions of the BioM34, refer to the User's Manual located on the software CD-ROM. Additional functions include: **Open**, **Log On User**, **Log Off Current User**, **Switch User Identity**, **Remember Password**, as well as **Help**, and **About** information. Under the **Open** function, the screen displayed provides a tab which allows you to unmask a password in the **Password Vault**, which is helpful in instances where you to change an existing password because it will expire, or it has been compromised and you have forgotten the original password.

**Note:** You need to use the **Remember Password** function (shown in Figure 27) each time you go to a new website or database requiring a username and password entry.

- F. When APC Omnipass encounters a website or database requiring a username and password entry for the first time, enter your username and password, then right-click on the APC Omnipass icon. APC Omnipass will display the **Remember Password** dialog (Figure 28), and your cursor will become an icon that looks like a key.

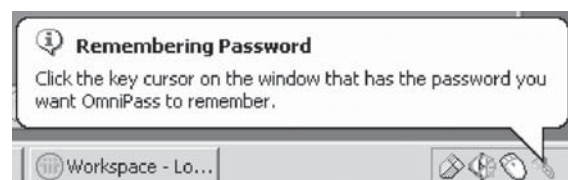


Figure 28. Remember Password Dialog

Place the key icon over the screen which now contains your username and password and rightclick the BioM34. The APC Omnipass software will then display the Friendly Name screen (Figure 29).

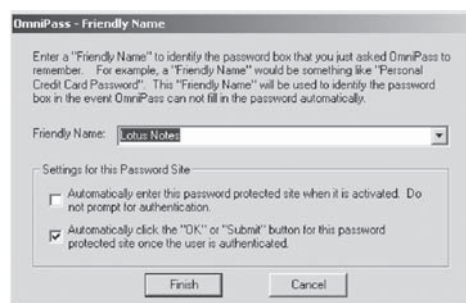


Figure 29. Friendly Name Screen

This screen provides two setting options:

1. Automatically enter the password protected sites when it is activated. Do not prompt for authentication.
2. Automatically click the "OK" or "Submit" button for this password protected site once the user is authenticated. Enter a name for the website or database, or leave the name entered by the APC Omnipass software, then select the desired setting for the website and click **Finish**.

The website or database username and password are now stored in the Password Vault, and will automatically be entered each time your fingerprint is verified.



## SCREENSAVER PASSWORD

If the Biometric hardware is installed on a system using a screensaver password, use a fingerprint to log back into Windows after the screensaver starts. APC Omnipass adds a fingerprint box to the screensaver password dialog box if it detects a Biometric sensor. Place the appropriate finger on the sensor to log in.

Place the finger on the BioM34 sensor and drive ring (Figure 18) for scanning. Use light, but firm and steady pressure. Ensure the finger makes contact with the BioM34 sensor and the surrounding drive ring. APC OmniPass works best when it has an image of the center of a fingerprint (core image).

Capture the full area of the fingerprint by placing the finger flat on the BioM34 sensor. Do not place only the fingertip on the sensor, as it contains insufficient image data for a high-quality fingerprint.

## LOGGING ON WITH THE BIOMETRIC HARDWARE

Each time a user logs on with the BioM34 installed, a fingerprint window is displayed with the **Logon User Authentication** screen (Figure 11). Simply place the correct finger on the Biometric Sensor and Drive Ring. If authentication is successful, the fingerprint will turn green. If authentication is not successful, the fingerprint will turn red. When this occurs, raise and slightly reposition your finger, then lower it again. Continue this process until authentication is successful.

## ENCRYPTING AND UNLOCKING FILES

To encrypt a file or folder:

- Browse to the file or folder, and right-click on it.
- From the drop-down menu, select Omnipass Encrypt File(s); left-click the mouse.
- Enter the user name and password/fingerprint scan when prompted to encrypt the file or folder. If a folder containing multiple files is selected, a window appears with a list of the files in the folder and their encryption status. Select **OK** when the encryption is complete.

**Note:** Certain files and folders cannot be encrypted, such as those inside the Windows directory and the program files directory, as well as the folder where the APC OmniPass software is installed.

To unlock an encrypted file or folder:

- Browse to the file or folder, and right-click on it.
- From the drop-down menu, select OmniPass Decrypt File(s); left-click the mouse.
- Enter the user name and password/fingerprint scan when prompted to unlock the file or folder. If a folder containing multiple files is selected, a window appears with a list of the files and their status. Select **OK** once all files are unlocked.

## CLEANING THE BIOM34 SENSOR

To clean the BioM34 sensor and drive ring:

- Disconnect the BioM34 from the computer.
- Wet one end of a cotton swab with a water-based household cleaner (Formula 409®, Windex®, or Fantastik®). DO NOT use chlorine-based cleaners such as bleach, or solvents such as acetone, paint thinner or turpentine.
- Gently rub the sensor surface and the drive ring with the cotton swab. Do not allow any cleaner to drip into the electronics around the sensor.
- After cleaning, gently rub the surface again with a dry cotton swab.

**Note:** Cleaning is not required on a regular basis. If material does accumulate, the normal wiping action of a finger is usually adequate to clean the sensor.

## TROUBLESHOOTING

Windows 2000 and Windows XP users may experience a problem adding a Windows user to the APC OmniPass database. If this happens, adjust the local security settings, as follows:

- Log into Windows as an administrator.
- From the Windows Start menu, select: **Start> Settings> Control Panels> Administrative Tools> Local Security Settings> Security Options.**
- Then select:  
**Network Access: Sharing and Security Model for Local Accounts.**  
 The setting should be: **Classic - local users authenticate as themselves.**

If the fingerprint sensor does not work while logging into Windows XP, try changing the Windows user settings:

- From the Windows Start menu, select **Start> Settings> Control Panels> User Accounts.**
- Select **Change the way users log on or off**, and ensure the settings for both the **Logon Screen** and **Fast User Switching options** are the same (enabled or disabled).

## WARRANTY

The standard warranty is two (2) years from the date of purchase. APC's standard procedure is to replace the original unit with a factory reconditioned unit. APC will ship the replacement unit once the defective unit has been received by the repair department, or cross-ship upon the receipt of a valid credit card number. The customer pays for shipping the unit to APC. APC pays ground freight transportation costs to ship the replacement unit to the customer.

## WARRANTY REGISTRATION

To register this product for purposes of the warranty, please go to [warranty.apc.com](http://warranty.apc.com).

## BIOPOD Installation

### INTRODUCTION

The APC Biopod (Figure 1) enables users to log on to a system simply by placing their fingertip on the Biopod sensor. Use the Biopod hardware and software to provide fingerprint identification to access password-protected systems, applications, and web sites, without password authorization.



Figure 1. The APC Biopod

**Caution:** Do not allow metal or sharp objects to come in contact with the sensor surface, as they could damage the unit.

### FEATURES

- Attached USB cable for easy connection to laptops and PCs
- Easy-to-use Master password for all types of Windows, application, and on-line passwords
- Compatible with Microsoft Passport®
- Support for Internet Explorer®
- Compatible with Windows XP® Credential Manager
- User-friendly graphical user interface (GUI) that is easy to install, customize and use
- Full Windows OS support including Windows 98®, ME®, 2000®, and XP® (Windows 95® is not supported)
- International language support
- TruePrint™ compliant

### SETUP

#### 1. Connect the Biopod.

Note: Before connecting the Biopod, remove any previously installed biometric or related security software. To connect the Biopod, plug the Biopod into the USB port as shown in Figure 2. You do not have to turn the computer off.

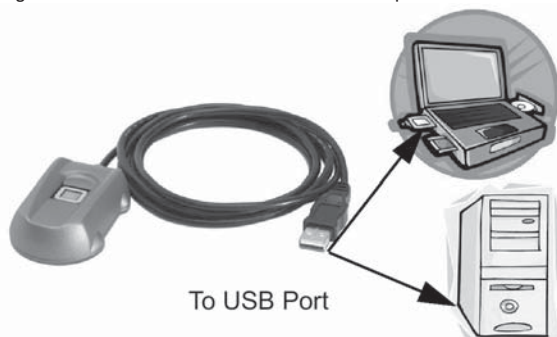


Figure 2. Connecting the Biopod

#### 2. Install the driver.

- Insert the software CD.
- The **Found New Hardware Wizard** screen appears. Select **Next**, then select **Search for a Suitable Driver**, and select **Next**.
- Check the **CD-ROM Drives** check box only, and select **Next**.
- Once the driver is found, select **Next** to install it. The

Hardware Wizard sends a message once installation is complete.

#### 3. Install the APC OmniPass software.

If a previous version of the software is installed on the system, it must be removed before installing the APC OmniPass software.

- Insert the APC OmniPass software CD into the CD-ROM drive and follow the on-screen installation instructions.
  - Specify a path name for the location of software when prompted.
  - Restart the system when prompted. An **APC OmniPass** icon appears on the Windows Control Panel, the Windows Start menu, and in the task bar.
4. Select the **Enroll Wizard** to add fingerprints to the database. The Enroll Wizard initial screen appears (Figure 3).



Figure 3. The Enroll Wizard Initial Screen

- Select the **Enroll** button. The **Verify Password** screen (Figure 4) appears.



Figure 4. The Verify Password Screen

- On some systems, the current Windows user name is filled in. (Windows 98/ME users must type the user name.) If a user does not have a Windows user name, one is created during this process.

Enter the Windows password in the **Password** field. This is the same password that is used to log into Windows. Select **Next** to **continue** or **Cancel** to exit.

The **Choose a Finger** screen (Figure 5) appears. Select a finger to enroll by highlighting and selecting the finger. A green check mark indicates that a particular finger has already been enrolled.

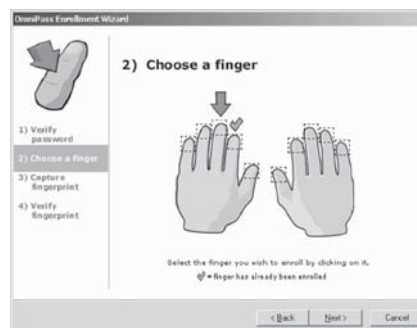


Figure 5. The Choose a Finger Screen

7. Place the finger on the Biopod for scanning. Use light, but firm and steady pressure. Make sure that the finger makes contact with the Biopod sensor and the surrounding drive ring (Figure 6). APC OmniPass works best when it has an image of the center of a fingerprint (core image).

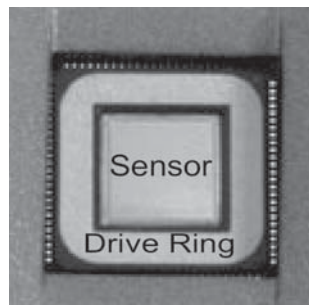


Figure 6. The Biopod Sensor and Drive Ring

Capture the full area of the fingerprint by placing the finger flat on the Biopod, as shown in Figure 7. Do not place only the fingertip on the sensor, as it contains insufficient image data for a high-quality fingerprint.



Figure 7. Proper Finger Placement

From the **Choose a Finger** screen, select **Next**. The **Capture Fingerprint** screen appears (Figure 8).



Figure 8. The Capture Fingerprint Screen

Keep the finger on the sensor and hold it down until the flashing green box below the fingerprint display is a solid green. Lift the finger and replace it on the sensor. Repeat this procedure until a message appears indicating that the enrollment process is complete. For improved performance, place the finger in slightly different locations on the sensor for each of the enrollment placements to allow the software to create a composite image of the finger.

**Do not** roll the finger as when taking an ink and paper image. Keep the finger flat and motionless against the sensor during the imaging process. After completing the required number of captures, the **Verify Fingerprint** screen appears (Figure 9).

## Biometric Password Managers

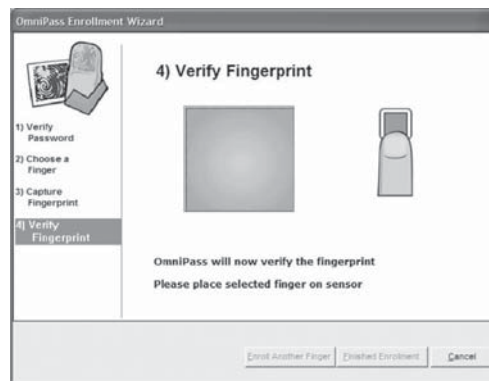


Figure 9. The Verify Fingerprint Screen

Place the finger on the sensor again. A message appears indicating whether the fingerprint enrollment was successful. Users may need to place their finger on the sensor several times to determine if enrollment was successful.

If enrollment was successful, select **Enroll Another Finger** to add additional fingerprints to the APC OmniPass database. If enrollment was not successful, repeat the enrollment process as needed.

Once enrollment is completed, select **Finished Enrollment**, then select **Done** on the Registration screen. Log in to APC OmniPass to use the software.

## LOGGING ON WITH THE BIOPOD

When a user logs on with the Biopod installed, a fingerprint window is displayed with the **Login User** dialog box (Figure 10).

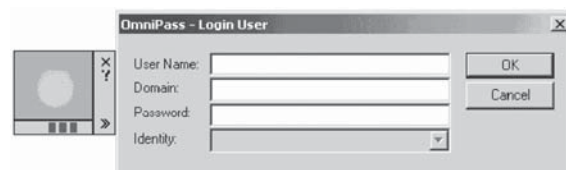


Figure 10. Login User Dialog Box with Fingerprint Window

If a fingerprint has been enrolled for a user, he or she can log into APC OmniPass by placing a finger on the Biopod device. The scrolling blue boxes indicate that APC OmniPass is waiting for a fingerprint device to be pressed.

Once a finger is placed on the device, the fingerprint is displayed in the window, and appears in green if recognized, or red if not recognized.

**Note:** It may take a few tries to get the software to recognize a fingerprint.

## SCREENSAVER PASSWORD

If the Biopod is installed on a system that uses a screensaver password, use a fingerprint to log back into Windows after the screensaver starts. APC OmniPass adds a fingerprint box to the screensaver password dialog box if it detects a fingerprint sensor. Place the appropriate finger on the sensor to log back in.

## WINDOWS 98/ME CONFIGURATION

In Windows 98/ME, APC OmniPass replaces the login screen to make the operating system more secure. To take advantage of this feature, do the following:

1. From the Windows Start menu, select **Start> Settings> Control Panel**.
2. Select the APC **OmniPass** control panel.
3. Select the Enable Desktop Security box.

Users should ensure that they know their password; otherwise, they will be unable to log into the computer.

When using a Windows 98/ME machine to log on to a network, users should make sure that their Windows password and user name are identical to their network password and user name.

To modify user information in Windows 98/ME:

1. From the Windows Start menu, select **Start> Settings> Control Panel**.
2. Select **Users**. From here, you can modify all user names and passwords.

## ENCRYPTING AND UNLOCKING FILES

To encrypt a file or folder:

1. Browse to the file or folder, and right-click on it.
2. From the drop-down menu, select **OmniPass Encrypt File(s)** and left-click the mouse.
3. Enter the user name and password/fingerprint scan when prompted to encrypt the file or folder. If a folder containing multiple files is selected, a window appears with a list of the files in the folder and their encryption status. Select **OK** when the encryption is complete.

Note: Certain files and folders cannot be encrypted, such as those inside the Windows directory and the program files directory, and the folder where the APC OmniPass software is installed.

To unlock an encrypted file or folder:

1. Browse to the file or folder, and right-click on it.
2. From the drop-down menu, select **OmniPass Decrypt File(s)** and left-click the mouse.
3. Enter the user name and password/fingerprint scan when prompted to unlock the file or folder. If a folder containing multiple files is selected, a window appears with a list of the files and their status. Select **OK** once all files are unlocked.

## CLEANING THE BIOPOD SENSOR

To clean the Biopod sensor and drive ring:

1. Disconnect the Biopod from the computer.
2. Wet one end of a cotton swab with a water-based household cleaner such as Formula 409®, Windex®, or Fantastik®. **DO NOT** use chlorinebased cleaners such as bleach, or solvents such as acetone, paint thinner or turpentine.
3. Gently rub the sensor surface and the finger drive with the cotton swab. Do not allow any cleaner to drip into the electronics around the sensor.
4. After cleaning, gently rub the surface again with a dry cotton swab.

Note: Cleaning is not required on a regular basis. If material does accumulate, the normal wiping action of a finger is usually adequate to clean the sensor.

## TROUBLESHOOTING

If a customer replaces the Biopod with another APC Biopod and encounters problems while enrolling fingers, it may be necessary to recalibrate the new Biopod by running the ATDiag.exe utility on the software CD. For information on using this utility, consult the ATDiag.txt file on the software CD. Windows 2000/XP users may experience a problem adding a Windows user to the APC OmniPass database. If this happens, adjust the local security settings:

1. Log into Windows as an administrator.
2. From the Windows Start menu, select **Start> Settings> Control Panels> Administrative Tools> Local Security Settings> Security Options**.
3. Select **Network Access: Sharing and Security Model for Local Accounts**. The setting should be **Classic - local users authenticate as themselves**.

If the fingerprint sensor does not work while logging into Windows XP, try changing the Windows user settings:

1. From the Windows Start menu, select **Start> Settings> Control Panels> User Accounts**.
2. Select **Change the way users log on or off**, and make sure that the settings for both the **Logon Screen** and **Fast User Switching** options are the same (enabled or disabled).

## WARRANTY

The standard warranty is two (2) years from the date of purchase. APC's standard procedure is to replace the original unit with a factory reconditioned unit. APC will ship the replacement unit once the defective unit has been received by the repair department, or cross-ship upon the receipt of a valid credit card number. The customer pays for shipping the unit to APC. APC pays ground freight transportation costs to ship the replacement unit to the customer.

## WARRANTY REGISTRATION

To register this product for purposes of the warranty, please go to [warranty.apc.com](http://warranty.apc.com).



## BIOPOD & BIOM34-EC - User Manual

Softex OmniPass provides password management capabilities to Microsoft Windows operating systems. OmniPass enables you to use a "master password" for all Windows, application and on-line passwords. A "master password" is an OmniPass authentication method which simplifies all your authentication needs. This "master password" will be used to enter any password protected site or program once you have registered those resources with OmniPass.

OmniPass extends the Windows interactive logon model by requiring users to authenticate themselves before granting access to the Windows desktop. OmniPass enables strong authentication by allowing users to authenticate with single or multiple authentication methods. Fingerprint recognition devices or SmartCard devices are some of the hardware security devices that can be integrated with OmniPass. Integrating these devices with OmniPass results in a multi-tiered authentication system for restricting access to your computer, applications, websites, and other password protected resources.

Furthermore, OmniPass enables file encryption on your Windows-based system. The data in these encrypted files cannot be viewed by other users. OmniPass enables you to share your OmniPass encrypted files with other OmniPass users while restricting access to others.

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

### Features of OmniPass

OmniPass augments your Windows-based system with a rich feature set, enhancing your computing experience with the following characteristics:

- Easy to use "master password" for all Windows, application, and online passwords
- Easy to import and export existing passwords
- Secure storage of unlimited passwords and related information
- Extensible security through integration with hardware security devices - such as fingerprint recognition or SmartCard devices
- Compatible with Microsoft Passport support for Internet Explorer and Windows XP Credential Manager
- User-friendly GUI for password, user and identity management
- Integrated file encryption and encrypted-file-sharing
- Seamless integration with Windows, providing secure Windows Logon
- Full support for Windows platforms including Windows 2000, XP (Home and Professional), and 2003
- International language support.

### How This Document is Organized

This document proceeds from basic to advanced. Outlined steps initially assume a very inexperienced user. Towards the end of the document outlined steps are less explicit, the assumption being that the user will be more familiar with application-specific concepts.

- Part 1, "Start"
  - Chapter 1, "Installing OmniPass" describes system requirements of the software, and shows install, uninstall, and upgrade procedures.
  - Chapter 2, "User Enrollment" walkthrough of how to enroll users into OmniPass, and how to integrate devices with OmniPass
- Part 2, "Use"
  - Chapter 3, "Password Replacement" describes how to use identities and the password replacement function
  - Chapter 4, "File and Folder Locking" describes how to use the encryption/decryption function

- Part 3, "Configure"
  - Chapter 5, "Exporting and Importing Users" describes how to use the export/import function
  - Chapter 6, "Overview of the OmniPass Control Center" survey of the remaining OmniPass functions
- Appendix A, "Troubleshooting"

### Part 1. Start

Part 1 guides you through the preparation of your Windows-based system for the OmniPass 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. If you have a supported hardware security device installed, its enrollment into OmniPass will also be shown. Upon completion of Part 1, you will be ready to start using OmniPass.

### Chapter 1. Installing OmniPass

In the preface of this document are described some of the features OmniPass will provide you once installed on your system. It is possible that OmniPass was provided pre-installed by your system manufacturer or distributor. Evidence of this would be:

- The presence of the golden key shaped OmniPass icon in the taskbar
- The launching of the OmniPass Enrollment Wizard upon system boot
- The presence of the Softex program group in the Programs group of the Start menu (the Softex program group may be nested within another program group)

If one of the cases above is true for your system, then you may skip down to *Chapter 2. User Enrollment*. Otherwise, please continue with this chapter which will cover the following:

- Notifying of system requirements for OmniPass
- Installing of OmniPass
- Verifying version information of OmniPass
- Upgrading from a previous OmniPass version
- Uninstalling of OmniPass

Before you can install OmniPass, you must determine whether or not your system will support it.

**Note to users of OmniPass Enterprise Edition:** During Installation and initial restart of your version of OmniPass additional configuration screens may appear. These screens are to configure your OmniPass client software to communicate with an OmniPass Server. For assistance in this configuration, you need to contact your network administrator. Network administrators should consult the OmniPass Enterprise Edition Administrators' Guide. Foregoing communication with an OmniPass Server, the client will function almost identically as outline in this users' guide.

#### 1.1 System Requirements

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

- One of these OS's: Windows 2000, Windows XP (Home or Professional), or Windows 2003
- Internet Explorer 5.0 or greater
- At least 35 MB available hard disk space

If your system meets the above requirements then it is capable of running OmniPass.

#### 1.2 Installing the OmniPass Application

If OmniPass is already installed on your system, please refer to either *Chapter 2. User Enrollment* or *Chapter 1.4 Upgrading from a Previous Version of OmniPass*. Otherwise please continue with this section on software installation.

NOTE: For installation on Windows 2000, Windows XP, or Windows 2003, 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, the OmniPass installation program should automatically launch and provide directions for you to follow.

*NOTE: If you are not using CD or DVD media to install OmniPass or if the OmniPass installation program does not automatically launch, then you may have to perform a manual installation. Files may need to be extracted before you can manually launch SETUP.EXE.*

2. Follow the directions provided in the OmniPass installation program. Specify a location to which you would like OmniPass installed.

*WARNING: It is recommended that you NOT install OmniPass in the root directory (e.g. C:\). OmniPass file encryption does not permit the encryption of files within the OmniPass installation directory. Installing OmniPass to root will seriously limit where files can be encrypted on your system.*

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. This concludes OmniPass installation. If you would like to proceed with using OmniPass, skip to *Chapter 2. User Enrollment*. Otherwise continue this chapter to learn more about upgrading or uninstalling OmniPass.

## 1.3 Verifying Information about the OmniPass Application

After you have completed installing OmniPass and restarted your system, you may wish to check the version of OmniPass and that it is properly installed 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 Panel 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. If the About tab is not visible, you will need to navigate along the tabs until you find it. The About tab window appears with version information about OmniPass.

## 1.4 Upgrading from a Previous Version of OmniPass

If you already have a version of OmniPass installed on your system, you can upgrade OmniPass to a more recent version. OmniPass installation supports automatic upgrading of the software. To upgrade OmniPass, refer to *Chapter 1.2 Installing the OmniPass Application* for directions. If you want to uninstall OmniPass and then reinstall it then:

*WARNING: 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. Exporting and Importing Users).*

1. Uninstall the previous version of OmniPass. Follow the steps outlined in *Chapter 1.5 Uninstalling the OmniPass Application*.
2. After the system has been rebooted, you can install the new version of OmniPass. For directions refer to *Chapter 1.2 Installing the OmniPass Application*.
3. Reboot your system. Now you can use the new version of OmniPass.

Proceed to the next chapter to start user enrollment.

## 1.5 Uninstalling the OmniPass Application

If you would like to remove the OmniPass application from your system, or migrate your licensed version of OmniPass to another system, then you should:

*WARNING: 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. Exporting and Importing Users).*

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

## Chapter 2. User Enrollment

OmniPass is now installed on your system, but before you can use any OmniPass features you have to enroll a user into OmniPass. *Chapter 2.2 Basic Enrollment* is where you should start your enrollment process. If you would like to use an optional authentication device (e.g. fingerprint recognition or SmartCard device) then you will also need to consult *Chapter 2.3 Enrolling an Authentication Device (Optional)*. If you would like to use an optional alternate storage location for OmniPass secured data (e.g. SmartCard device, USB key, OmniPass Server) then you will also need to consult *Chapter 2.4 Alternate Storage Location*.

### 2.1 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 single "master password" is created for the enrolled user. This master password "replaces" all other passwords for sites you register with OmniPass (the process of registering sites with OmniPass will be discussed in *Part 2. Use*).

*Example - A user, Shinji, installs OmniPass on his system (his home computer) and enrolls an OmniPass user with the username "Eva\_01" and the password "eschaton". He then goes to his webmail site to log on to his account. He inputs his webmail credentials as usual (username "Ikari" and password "warrior"), but instead of clicking Submit, he directs OmniPass to Remember Password. Now whenever he returns to that webmail site, OmniPass will prompt him to supply access credentials. He then enters his OmniPass user credentials ("Eva\_01" and "eschaton") in the OmniPass authentication prompt, and he will be allowed into his webmail account. He can do this with as many websites or password protected resources he likes, and he will gain access to all those sites with his OmniPass user credentials ("Eva\_01" and "eschaton"). This*

is assuming he is accessing those sites with the system he enrolled his OmniPass user onto. OmniPass does not actually change the credentials of the password protected resource. If he were to go to an Internet café to access his webmail, he would need to enter his original webmail credentials ("lkari" and "warriors") to gain access. If he attempts his OmniPass user credentials ("Eva\_01" and "eschaton") on a system other than where he enrolled that OmniPass user, he will not gain access.

Continue to the next section to begin OmniPass user enrollment.

## 2.2 Basic Enrollment

The basic 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 after reviewing this section.

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

- 2.2.1 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.
- 2.2.2 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.
- 2.2.3 In this step you are selecting where OmniPass will be securely storing your OmniPass data. Do not be alarmed if there are devices listed as selections that you do not have or that you have not installed on your system. The selections displayed on this screen are dependent upon the version of OmniPass you have installed. These selections are not necessarily dependent upon which devices are attached to your system. Although, if an applicable device (e.g. SmartCard, USB key) is installed but not attached to your system, it may not be visible as a selection. Regardless of where you choose to store OmniPass data, the data are stored in an encrypted format and their content will not be viewable to others. If you would like to use a secure storage device other than **Local Hard Disk Drive** then please review *Chapter 2.4 Alternate Storage Location* to see how your enrollment procedure will differ. Otherwise click **Local Hard Disk Drive** and click **Next** to proceed.
- 2.2.4 In this step you can select which authentication devices you would like to integrate with OmniPass. Just as in the secure storage device selection screen, there may be devices listed that are not present on your system. Also, installed devices that are not attached may not appear on this screen. If you would like to enroll an authentication device then please review *Chapter 2.3 Enrolling an Authentication Device (Optional)* to see how your user enrollment procedure will differ. If you do not want to enroll any authentication devices right now then do not select any, and click **Next** to proceed. You will be prompted to confirm that you are not enrolling any authentication devices.
- 2.2.5 In this step you can choose how OmniPass notifies you of various OmniPass 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. You should heed the warning stated.

- 2.2.6 **WARNING:** *If you will use OmniPass to encrypt and decrypt files, we STRONGLY recommend exporting your user profile to a backup media such as a floppy disk. In case your system is corrupted, this backup will be required to be able to access your encrypted files.*

The export user profile function will be described in *Chapter 5. Exporting and Importing Users*. Click **Done** to exit the OmniPass Enrollment Wizard. You will be asked if you would like to log in to OmniPass with your newly enrolled user; click Yes and then proceed to Part 2 to start using OmniPass.

## 2.3 Enrolling an Authentication Device (Optional)

Integrating a hardware authentication device will both, increase the security of your OmniPass system, and streamline the OmniPass authentication procedure. Security is enhanced in that if your "master password" becomes compromised, you can restrict access to OmniPass (and the sites remembered) via a hardware security device. You can configure OmniPass to restrict access entirely via the authentication device. When decrypting files or visiting remembered websites, instead of manually typing your "master password" each time, you could authenticate with the security device (e.g. use your fingerprint).

You can enroll devices manually 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 **Enroll** under the **User Settings** area. Click **Enroll Authentication Device** and authenticate at the OmniPass authentication prompt to start device enrollment.

- 2.3.1 **Enrolling a Fingerprint Recognition Device** During initial user enrollment, at Select **Authentication Device** select the security device which you want to enroll and click **Next**.
  - 2.3.1.1 **Choosing a Finger** 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**.
  - 2.3.1.2 **Capturing the Fingerprint** *It is now time for OmniPass to capture your selected fingerprint. It may take up to eight captures before OmniPass can acquire your fingerprint. Should OmniPass fail to acquire your fingerprint, or if the fingerprint capture screen times out, you can click Back to restart the fingerprint enrollment process. There are several types of fingerprint sensors (e.g. "swipe" or "touchpad"), and each type requires a different action for capturing. The "core" of the fingerprint is the ideal area for capture. The core of your fingerprint is usually aligned with the base of your cuticle. It is where the concentric whorls of your fingerprint converge. To start fingerprint capturing, follow the directions on the Capture Fingerprint screen.*

Touchpad sensors are square, and they require you to place your fingertip on the sensor and hold it there until it is captured. During a successful fingerprint capture the text, **Place the selected finger on the sensor**, will be replaced with the text, **Lift and replace your finger on the sensor**. You will also see a black fingerprint in the capture window turn and stay green, and the counter under the capture window will increment. Lift and replace your fingertip as many times necessary for OmniPass to acquire your fingerprint.

Swipe sensors are a type of fingerprint sensor that are operated by placing your finger on the scanner and pulling the finger across the sensor firmly with even speed. Swiping too fast or too slow will result in a failed fingerprint capture. For better results, it is recommended that you use the practice fingerprint selection before enrolling the first time. 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 you may proceed to enroll a finger.

**2.3.1.3 Verifying the Fingerprint** 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.

**2.3.1.4 Setting Authentication Rules** After enrolling a fingerprint you may wish to set the Authentication Rules which you can access in the OmniPass Control Center. These settings allow you to restrict access to OmniPass functions. By default, with no security devices enrolled, all OmniPass functions require "master password" authentication. Once you enroll a security device, you can set OmniPass to require authentication via that security device to access OmniPass functions. More about these settings and their ramifications can be found under Chapter 6.2 User Settings. For now, keep the default selection (no boxes checked) and click Next. This setting will allow you to access OmniPass functions with your enrolled finger, but fingerprint authentication will not be required.

***WARNING:** You should leave these settings to default (no boxes checked) until you are familiar with OmniPass. If you require an authentication device to access an OmniPass function, and that device fails or is not present, you will lose access to that restricted OmniPass function.*

In a Windows XP environment, the **Windows and OmniPass Logon** selection may be grayed out. This depends on your Windows logon configuration during OmniPass installation. For more details about this feature consult *Chapters 6.2 and 6.3*. Click **Next** to proceed.

**2.3.1.5 Completing Device Enrollment** After you set the authentication rules for the enrolled device, the **Device Enrollment Complete** screen will automatically appear. If you check the first box, **Enroll more security authentication devices ...**, upon clicking **Next**, you will be directed back to the **Select Authentication Device** screen (see 2.2.4 or 2.3.1). If you check the second box, **I am done with enrolling security authentication devices ...**, upon clicking **Next**, you will be directed to the **Audio and Taskbar Settings** (see 2.2.5). Continue the OmniPass Enrollment Wizard, resuming the procedure at 2.2.4 or 2.2.5.

**2.3.2 Enrolling the Phoenix TrustConnector** During initial user enrollment, at **Select Authentication Device** select the security device, which you want to enroll and click **Next**. For product information about the TrustConnector please consult the Phoenix Technologies documentation.

***NOTE:** You must be logged onto the Windows system with the account you wish to enroll into Omnipass. Enrollment will fail if you attempt to enroll a user that is not currently logged onto the machine. If you are logged onto a Domain (e.g. with user account username@domain.com) and you attempt to enroll a local user (e.g. COMPUTERNAME\localuser), user enrollment will fail*

Clicking **Next** or **Cancel** will return you to the **Select Authentication Device** screen. To enter the credentials of a

user that can legitimately enroll the TrustConnector as an authentication device you must hit **Start Over** at the **Select Authentication Device** screen so the credentials of the currently logged on user may be entered. Alternatively, the **Cancel** button could be selected exiting the OmniPass Enrollment Wizard completely.

Once you enter the credentials of the currently logged on user at the **Verify Username** and Password screen, then the TrustConnector may be enrolled as an authentication device and you can continue to 2.3.2.1 to proceed with device enrollment.

**2.3.2.1 Configure Digital Certificate** During enrollment of the TrustConnector a digital certificate must be specified. The digital certificate that is chosen during authentication device enrollment will be bound to the enrolled user for use in various OmniPass authentication procedures (e.g. Encrypt/Decrypt files, Password Replacement).

Unless an IT administration function has preloaded a digital certificate using the TrustConnector CSP there will be no digital certificates to choose from on the **Configure Digital Certificate Authentication** screen. You will have to select **Use the digital certificate that OmniPass has automatically created for me** and click **Next**.

**2.3.2.2 TrustConnector Prompts** Once you have selected the digital certificate that is to be associated with the OmniPass user you will be prompted to set the security level with respect to accessing the digital certificate for various authentication procedures.

Setting the security level to **Medium** will notify the OmniPass user when the certificate is being accessed for authentication purposes. Setting the security level the **High** forces the user to set a TrustConnector password associated with the digital certificate. Authentication procedures that access the digital certificate will prompt the user to enter the TrustConnector password set for that certificate.

Acknowledge the certificate access prompts displayed for TrustConnector enrollment and proceed to 2.3.2.3.

**2.3.2.3 Completion of Digital Certificate Enrollment** After the TrustConnector configures the digital certificate a screen will be displayed indicating that portion of device enrollment was successful. Click **Next** to proceed with OmniPass user enrollment. The OmniPass user enrollment procedure resumes at 2.2.5.

## 2.4 Alternate Storage Location (Optional)

The Storage Location is where OmniPass user-specific data is stored. These data are your remembered sites, user identities, OmniPass settings, and data used to securely encrypt or decrypt files, all of which constitute your user profile. You may wish to have your user profile stored in a location other than your local hard drive. You can choose to store your user profile in a removable storage device (e.g. SmartCard, USB key). That way you can remove your storage device when you are away from your system and carry it with you. This portability is an added convenience in that you may have access to your user profile on other OmniPass-enabled systems.

In this example we will be using a SmartCard as the alternate storage location.

**2.4.1** During initial user enrollment, at **Select Storage Device** select the storage device which you wish to use and click **Next**. If a SmartCard is not present in the reader when you click **Next**, you will be prompted to insert it.

**2.4.2** This example assumes you are using a fresh, blank SmartCard. If you are using a SmartCard that has already been used with OmniPass or another application, you will be prompted to enter your PIN.



*WARNING: Depending upon how the SmartCard was initially configured, a limited number of failed PIN attempts may be enforced. If this is the case, and you exceed the maximum failed PIN attempts, the card may become locked and permanently unusable. To find out more, contact whoever configured your SmartCard for you, or the SmartCard manufacturer*

If you are using a fresh SmartCard you will be greeted with a screen prompting you to establish your PIN. Please take note of this PIN, if you forget it you risk being locked out of your SmartCard. Enter your PIN in both fields and click **Next**. SmartCard Enrollment then directs you back to the next step of the OmniPass Enrollment Wizard, 2.2.4 *Select Enrollment Device*.

- 2.4.3 If your SmartCard already contains data when you select it as a storage device (from 2.4.1 of SmartCard Enrollment), you will be warned that the current data on the SmartCard will be overwritten. This may also happen if you try to use a SmartCard as a storage device that is already being used as such by another OmniPass user. There is a limitation of one OmniPass user per SmartCard. To proceed, check the box next to **I want to overwrite the SmartCard** and click **Next**. SmartCard Enrollment then directs you back to the next step of the OmniPass Enrollment Wizard, 2.2.4 *Select Enrollment Device*.

## Part 2. Use

You are now ready to begin using OmniPass. Used regularly, OmniPass will streamline your authentication procedures. For the credentials registered with it, OmniPass is a secure repository. In the event you forget any of those passwords, you can find them in OmniPass.

*Part 2. Use* covers basic OmniPass functionality. Review this section to quickly get familiar with the OmniPass functions you will most use. If your system is shared among several users (often the case in a home PC or SOHO environment) then you may find some additional useful features in *Part 3. Configure*.

## Chapter 3. Password Replacement

You will often use the password replacement function of OmniPass. 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 OmniPass to gain access. OmniPass prompts you for your "master password", and that single password gains you access to any site you have "taught" OmniPass. Or you could login with any hardware authentication device you have enrolled into OmniPass. This functionality is not limited to restricted access websites. OmniPass can learn any set of credentials that you are prompted to provide (e.g. your Intranet email, your ftp login, any of your client logins, any restricted access network resource).

### 3.1 The OmniPass Authentication Toolbar

After installing OmniPass and restarting, you may have noticed a dialog you had 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. You see the OmniPass Authentication Toolbar upon Windows Logon because the OmniPass authentication system is seamlessly integrated with Windows. When you see this toolbar, OmniPass is prompting you to authenticate.

The bold-faced text **"File Encryption/Decryption Authentication"**,

next to the lock and keys icon, shows what OmniPass-restricted function you are attempting. The non-bold-faced text beneath may give you additional instructions regarding authentication. The icons in the lower left (fingerprint and key in this example) 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, a PIN for the SmartCard PIN prompt, your master password for the master password prompt (the key icon). Depending on your Authentication Rules (see 6.2 *User Settings*), you may have to satisfy several different authentication prompts to gain access (e.g. fingerprint AND SmartCard PIN).

### 3.2 Remembering a Password and ...

Most examples of password replacement used in this document show the remembering of websites, but OmniPass can remember any set of credentials used to access any restricted resource. Any application you use, any GUI client, any password protected resource that manifests a password prompt, OmniPass can remember.

Using the following procedure, you can store a set of credentials into OmniPass. These credentials will then be linked to your "master password" or any enrolled authentication devices.

Go to a site that requires a login (username and password), but DO NOT LOGIN 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** or click **Submit** or **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.

- 3.2.1 **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 remembered 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.

You can remember multiple different logins to the same password protected resource. To do this you must specify different friendly names for each set of credentials. If you use the same friendly name then OmniPass will overwrite the previous set of credentials associated with the application or website. If you have several credentials remembered for the same site, OmniPass will prompt you to select among the available friendly names.

- 3.2.2 **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 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.

*WARNING: 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, unlocked, 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 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 OmniPass' secure database. The OmniPass authentication settings (**Settings for this Password Site**) can always be changed in **Vault Management** (see Chapter 3.5 Password Management).

### 3.3 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** (see 3.2.2) and can be changed in **Vault Management** (see 3.5). The authentication methods required for access to password protected resources are determined by **Authentication Rules** (see Chapter 6.2 User Settings).

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

**3.3.1 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.

**3.3.2 With Multiple Authentication Methods --** Or you may be presented with an OmniPass authentication prompt that has several different authentication methods. If multiple authentication methods are shown at the authentication prompt, you may have to authenticate multiple times (fingerprint reader AND SmartCard reader) to gain access.

*NOTE: It may take a few tries for a fingerprint reader to capture your fingerprint. Try to place your fingertip on the sensor as you did during fingerprint enrollment.*

**3.3.3 Logging into Windows with a Biometric Device --** When logging into Windows with a biometric 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 with Windows 2000, or Windows XP, and the biometric device can be used to log back in as stated above.

*NOTE: 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.

### 3.4 OmniPass Can Also Remember ...

Examples have been limited to websites so far, but OmniPass can remember any authentication event that prompts you to login. So long as you choose to keep some form of **Taskbar Tips**, OmniPass will always notify you when you have an opportunity to "remember a password".

### 3.5 Password Management

OmniPass provides an interface that allows you to manage your passwords. To access this GUI, 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 Passwords** under **Vault Settings**. You will see the **Manage Passwords** interface, with a list of your 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 (see 3.2.2).

OmniPass may have difficulty properly recognizing some authentication prompts. This is because software developers are free to deviate from commonly accepted Windows application programming standards. Under these circumstances, users can take advantage of the Password Wizard feature to remember passwords. The **Password Wizard** can only be used in conjunction with password protected applications, and it will not work with websites. If OmniPass fails to remember a set of credentials, you will be given the option to run the Password Wizard. You can use the Password Wizard to manually assign your user credentials into the fields of the authentication prompt.

Finally, you can manage passwords for all your OmniPass user identities using the Identities drop-down box (see Chapter 3.6 OmniPass User Identities for more information).

### 3.6 OmniPass User Identities

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** (see Figure 27). 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**. Click **Apply** to ensure the settings are saved. 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** to ensure the settings are saved. When you delete an identity, all the remembered sites and password protected dialogs associated with the identity 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 biometric 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".

**3.6.1 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 become available. Select the identity you wish to login as and then click **OK** to login.

**3.6.2 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**.

### 3.7 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 *Chapter 3.5 Password Management*.

## Chapter 4. File and Folder Locking (File Encryption)

To protect yourself from theft or unauthorized viewing of sensitive material, OmniPass allows you to securely lock files or entire folders on your machine. These files are locked with a method called encryption, in which the data are converted to a form that unauthorized users cannot read. Once encrypted, the files can only be unlocked, or decrypted with your master password or enrolled hardware security device.

OmniPass encrypted files will have the extension ".opf". You can always search your hard drive for \*.opf to find all OmniPass encrypted files. We recommend that you dedicate a new folder in which to put all your OmniPass encrypted files. OmniPass encrypted folders take the name of the original folder but end in ".opx".

### 4.1 Encrypting Files or Folders

To encrypt a file or folder, right-click the file or folder that you would like to prevent unauthorized access to. Click **OmniPass Encrypt File(s)** in the contextual menu. OmniPass will prompt you to authenticate.

If a folder containing multiple files is encrypted, a window will appear with a list of the files in the folder and their encryption status. Click **OK** when encryption is complete.

There are certain folders that cannot be encrypted because it would have a negative impact on your system and your installed programs. The contents of **C:\Windows** and **C:\Program Files** cannot be encrypted, nor can the folder where OmniPass is installed be encrypted.

### 4.2 Decrypting File or Folders

To decrypt a file or folder, right-click the file or folder to which you would like to regain normal access. Click **OmniPass Decrypt File(s)** from the contextual menu. OmniPass will prompt you to authenticate. **OmniPass Decrypt File(s)** will not be available if the files are already encrypted, or if they are system files, unable to be encrypted.

Other ways to decrypt files are to right-click them and select **Open**, or double-click the files. Both of these actions will cause OmniPass to prompt you to authenticate. They will remain decrypted unless you decide to encrypt them again.

If you encrypt a folder containing multiple files, all the contained files will be encrypted. Files you copy or move to the encrypted folder will also be encrypted. You can open and edit the contents of these files, and so long as they stay in the encrypted folder, when you close and save these files they will automatically be encrypted. To decrypt a file contained in an encrypted folder right-click it and select **Decrypt To...**; select a location to which the decrypted file will be saved and click **OK**. A copy of the file will be decrypted to the target directory. The original encrypted file will remain in the encrypted folder.

### 4.3 OmniPass Encrypted File Sharing

Once you have encrypted a file or folder, you have prevented anyone from viewing the contents without first decrypting the file or folder. OmniPass allows you to selectively share your encrypted files with other enrolled OmniPass users.

To share an encrypted file or folder with another OmniPass user, right-click the encrypted resource and select **OmniPass Sharing...** from the contextual menu. OmniPass will prompt you to authenticate.

Upon successful authentication, the **OmniPass Encrypted File Sharing** dialog automatically opens (see Figure 37). Select the OmniPass user with whom you want to share this encrypted file or folder. Click **Add User(s)**, and click **OK**. The encrypted resource has been shared.

*NOTE: Sharing an OmniPass encrypted file effectively gives full control of the shared resource to whomever you shared it with. The users with whom you share these files can open, copy, delete, and modify all files you share. They can also remove you from the list of authorized OmniPass users, effectively taking control of the encrypted resource away from you.*

### 4.4 Encrypted Files

Files that are encrypted by OmniPass have a new icon. These files cannot be accessed until they are decrypted. Icons of encrypted folders are also updated with a lock graphic

### 4.5 A Special Warning for those who Encrypt ...

*If you are reading this then you are taking steps to safeguard your information. You will probably start encrypting your files with OmniPass soon (if you haven't already). IMMEDIATELY export your current user profile (the one you have used and are going to use to encrypt) and save it on SEVERAL floppy disks and perhaps some places on your hard disk. Email it to yourself and save it in your Inbox.*

*If your system crashes (or you mistakenly remove or overwrite OmniPass), and you do not have the OmniPass user profile that encrypted all your archived data files, THEN YOU WILL LOSE THAT DATA.*

Creating another OmniPass user with the same name and password and settings will not do. It will not be the same user profile that you created before.

## Part 3. Configure

If Part 2 could be viewed as a "Getting Started Guide" then this part can be viewed as an "Administrators' Guide". This part will give an overview of both the Export/Import function and the OmniPass Control Center. Much of what is discussed in this part could be considered customization of OmniPass. Customizations can be made on a per-user basis, or globally. Authentication rules will be discussed; in OmniPass, authentication rules can be configured so as to require very stringent levels of authentication (Multi-Factor Authentication

## Chapter 5. 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.

*NOTE: You can, and should periodically export your user profile and store it in a safe place (e.g. on several floppies). Should anything happen to your system, you can import your OmniPass profile on your new system and have all your remembered sites, custom OmniPass settings, and enrolled fingerprints instantly. You would even be able to decrypt files that you had encrypted with that user profile (see 4.5).*

### 5.1 Exporting an OmniPass User Profile

To export an OmniPass 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.

## 5.2 Importing an OmniPass User Profile

*NOTE: 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 you will be directed to select the storage device from which to import the user profile.

If you did not enroll any alternate secure storage devices, 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 corporate environment your network administrator should know, and in a PC or SOHO environment **Domain** should be your computername.

Once authentication is successful, OmniPass will prompt you to select a storage device for this users OmniPass data.

Unless you have an alternate secure storage device installed (USB key, SmartCard, etc.) select **Local Hard Disk Drive** and click **Next**. OmniPass will

## 5.3 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 "Kasahara" and the password "Motorcycle" on my system. I have enrolled Kasahara into OmniPass and remembered passwords. I want to take all my passwords to new system. I export Kasahara's OmniPass user profile. I go to my new system and using the Control Panel I create a user with the username "Kasahara" and the password "Motorcycle". I can now successfully import the OmniPass user data to the new system.*

When you export from OmniPass a Windows domain user, you can import that OmniPass user profile on any domain computer running OmniPass.

*Example - Balthasar and Melchior are computers on the "NERV" domain. I work on Balthasar with the username "Ikari" and the password "PenPen" on the NERV domain. I have enrolled this user, Ikari, in OmniPass and remembered passwords. I want to take all my passwords to Melchior. I export Ikari's user profile from OmniPass on Balthasar. I go to OmniPass on Melchior and import Ikari's OmniPass data. Since Balthasar and Melchior are on the same domain, the import is successful. If you do not know the domain you are using, you should contact your network administrator for assistance.*

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.

## Chapter 6. Overview of the OmniPass Control Center

Most of the functionality within the OmniPass Control Center has been touched upon in the previous two parts (*Start and Use*). This chapter will serve to explain functions within the OmniPass Control Center that weren't explained thoroughly

in the preceding parts of this users' guide. The Vault Management tab was exhaustively outlined in *Chapter 3.4 - 3.6* and will not be covered in this chapter.

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.

## 6.1 User Management

The User Management tab has two major interfaces: **Add/Remove User** and **Import/Export User**. Import/Export User functionality is well documented in *Chapter 5*. 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 well documented in *Chapter 2*. 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.

*WARNING: Removing a user will automatically destroy all OmniPass data associated with that user. All identities and remembered credentials associated with the user will be lost. Any remaining files encrypted by the user will be impossible to decrypt.*

If you are sure about removing the user, we recommend you

1. Decrypt all OmniPass encrypted files before removing the user
2. Export the user profile

## 6.2 User Settings

The User Settings tab has four interfaces: **Audio Settings**, **Taskbar Tips**, **Encrypt/Decrypt**, 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 **Encrypt/Decrypt** interface under **User Settings** allows you to choose either the Softex Roaming Profile or a Digital Certificate that is already installed on your system. If you choose Softex Roaming Profile then the keys used for encryption are part of your OmniPass User Profile. Portability of OmniPass encryption functions to other computers require only your OmniPass User Profile. If you choose Digital Certificate then the keys used for encryption are separate from your OmniPass User Profile. Portability of OmniPass encryption functions will require migration of both your OmniPass User Profile and the installed Digital Certificate. NOTE: Do not remove this Digital Certificate. If it is removed from the system, you will not be able to recover any of the encrypted files!

Within the **Encrypt/Decrypt** section you can also configure both the encryption algorithm and the key length (in bits). Changes you make to these settings are only applied to future encryptions. So if you already had files encrypted when you change the encryption settings, you will need to decrypt and re-encrypt those files to have your encryption settings apply to them. Decryptions using original encryption settings are handled transparently to the user.

The **Enrollment** interface allows you to enroll authentication devices, enroll fingerprints, and set authentication rules for enrolled devices. 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**. The rest of the procedure to enroll an additional finger can be found starting with *Chapter 2.3.2*.

If you click **Set Authentication Rules** in the Enrollment interface, you will be prompted to authenticate. Upon successful authentication you will see the **Set Authentication Rules** screen. The selections on the **Set Authentication Rules** screen determine which OmniPass functions require authentication via an enrolled security device.

You can individually set authentication rules for each enrolled security device. If you have not enrolled any hardware security devices, then you cannot set any authentication rules. All OmniPass functions are accessible via a master password authentication.

Setting **Windows and OmniPass Logon** will require the enrolled security device be authenticated against for the following functions: Windows Logon, OmniPass Logon, unlocking your workstation, resuming from standby or hibernate, and unlocking a password-enabled screensaver. In a Windows XP environment, this selection may not be available until you **Enable Logon Security**. See *Chapter 6.3* to see how this is done.

**WARNING:** *If this setting is enabled for an enrolled security device, and the device fails or is removed from the system, you will not be able to regain access to your system. Only through a successful authentication via the enrolled device will access be granted.*

*Example - You have a SmartCard device and a fingerprint recognition device enrolled. The SmartCard authentication rules are set independently of the fingerprint reader authentication rules, but rules are cumulative.*

1. *If there are no selections checked for any enrolled authentication devices, then there are no OmniPass authentication restriction, and you can access any OmniPass function using any method to authenticate (enrolled finger, master password, enrolled SmartCard).*
2. *For SmartCard authentication rules you checked **Windows and OmniPass Logon** and **File and Folder Encryption and Decryption**. For fingerprint reader authentication rules you checked **Windows and OmniPass Logon** and **Application and Website Password Replacement**.*
  - a. *If you visit a remembered website, OmniPass will prompt you to authenticate and will not grant you access to the website until you successfully authenticate with an enrolled finger. Successful authentications with master password or enrolled SmartCard are not sufficient.*
  - b. *If you attempt to encrypt or decrypt a file with OmniPass, you will be prompted to authenticate and OmniPass will not allow you to encrypt/decrypt until you successfully authenticate with an enrolled SmartCard. Successful authentications with master password or enrolled finger are not sufficient.*
  - c. *If you log out of Windows (or OmniPass) and attempt to log back in, you will be prompted to authenticate and OmniPass will not allow you to log back on until you successfully authenticate with BOTH a fingerprint reader AND a SmartCard. This dual authentication requirement is a Multi-Factor Authentication. Successful authentication with a master password, or with just the fingerprint reader are not sufficient. Neither are successful authentications with just the SmartCard. Loss or failure of either the SmartCard or the fingerprint reader will result in an inaccessible system.*

## 6.3 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.

In a Windows XP environment, the **Enable Strong Logon Security** interface will also be available. This allows you to enable restricted **Authentication Rules** functionality. If you would like to further strengthen Windows and OmniPass logon security, open the **Enable Strong Logon Security** interface and check the cleared checkbox. Select **OK** or **Apply**, and you will need to restart before the settings take effect. Under **User Settings**, you will now be able to set the **Authentication Rules** for **Windows and OmniPass Logon**.

The rest of this section pertains to settings under the **Startup Options** interface.

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.

OmniPass has a feature where any authentication device can be set as "Required" for Windows Logon. This feature is referred as **Strong Logon Authentication**.

*For **Strong Logon Authentication** to work on Windows XP the system has to be switched to the Classic Logon Mode. An unfortunate side effect of enabling the Classic Logon Mode is that Fast User Switching (FUS) and the XP Welcome Screen must be disabled. This is a Windows XP limitation. To **Enable Strong Logon Authentication** in OmniPass Control Center from the System Settings Tab. Once you have enabled Strong Logon Authentication you have to reboot the system for the setting to take effect.*

*To get back to the XP Welcome Screen or to turn FUS back on, the user will have to disable Strong Logon Authentication, reboot the system and then manually enable the XP Welcome Screen and FUS from the User Accounts in Windows Control Panel. Once this is done the fingerprint reader or other security device can no longer be made as a "Required" device for login to the PC.*

This feature is specific to Windows XP only. For Windows 2K and 2003 Server Strong Logon Authentication is always enabled.

## 6.4 Encrypt/Decrypt

The Encrypt/Decrypt tab provides a windows through which you can do encryption and decryption functions (see *Chapter 4*). Similar to the Windows Explorer, the Encrypt/Decrypt window presents the directory structure of your system. You can select files and folders and use the **Encrypt** and **Decrypt** buttons to encrypt and decrypt files. Some files and folders used by the Windows system or by other programs cannot be encrypted by OmniPass. Directing OmniPass to encrypt or decrypt a file will result in OmniPass prompting you for authentication. If you cannot authenticate successfully, the file will not be encrypted or decrypted. You can bypass the Encrypt/Decrypt tab by using the OmniPass encryption/decryption shell extension. In the normal course of browsing and accessing you files, if you right-click the file and see **OmniPass Encrypt File(s)** or **OmniPass Decrypt File(s)**, those OmniPass functions are available to you. Encryption/decryption will occur upon successful authentication.

## Appendix A: Troubleshooting

Most major problems can be avoided by paying special attention to the NOTES and WARNINGS distributed throughout this document. Other common problems are discussed in this appendix. For support not covered in this document contact support@softexinc.com.

### Windows 2000/Windows XP Issues

In Windows 2000 or Windows XP, 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 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

- The network connection is unavailable and the cached credentials could not be used
- 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. You should contact your network administrator for assistance.