Softex OmniPass
Version 3.0

Users' Guide

http://www.softexinc.com

Copyright

Disclaimer of Warranty

Softex Incorporated makes no representations or warranties with respect to the documentation herein described and especially disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, Softex Incorporated reserves the right to revise this document and to make changes from time to time in the content without obligation of Softex Incorporated to notify any person of such revisions or changes.

Trademarks

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this document, and Softex Incorporated were aware of a trademark claim, the designations have been printed in initial caps or all caps. References may be made to Softex, which is a trademark of Softex Incorporated. All other trademarks observed.

Document Inquiries

When referring to this document, please refer to the title and publication date.
For additional information about Softex products, visit the Softex website at: http://www.softexinc.com.
Comments are welcome and may be addressed to:

Softex, Inc.
9300 Jollyville Rd., Suite 201
Austin, TX. 78759

When you send information to Softex, you grant Softex a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

Introducing Softex OmniPass

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 an 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"

Conventions and Typefaces Used in this Document

"Choose", "Select", "Click"

The terms "choose", "select", and "click" are used interchangeably. They all mean either: hovering your mouse over the selection and left-click once, or hitting the <TAB> button until the selection is highlighted and hitting <ENTER>.

Start

Bold-faced default typeface (Arial) text indicates menu options, commands and dialog titles.

Chapter 3.2.2

Italicized text indicates example text and references to other chapters or sections within this document.

WARNING

All caps indicates text that deserves special attention.

⚠

This icon indicates special notice should be taken to prevent future confusion.

✖

This icon indicates special notice should be taken or risk data loss, sensitive data exposure, or possibility of being refused access to your system

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 introduction 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.

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 you system. Once your system has rebooted you will be able to use OmniPass. If you choose not to restart immediately after installation, OmniPass will not be available for use until the next reboot.

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

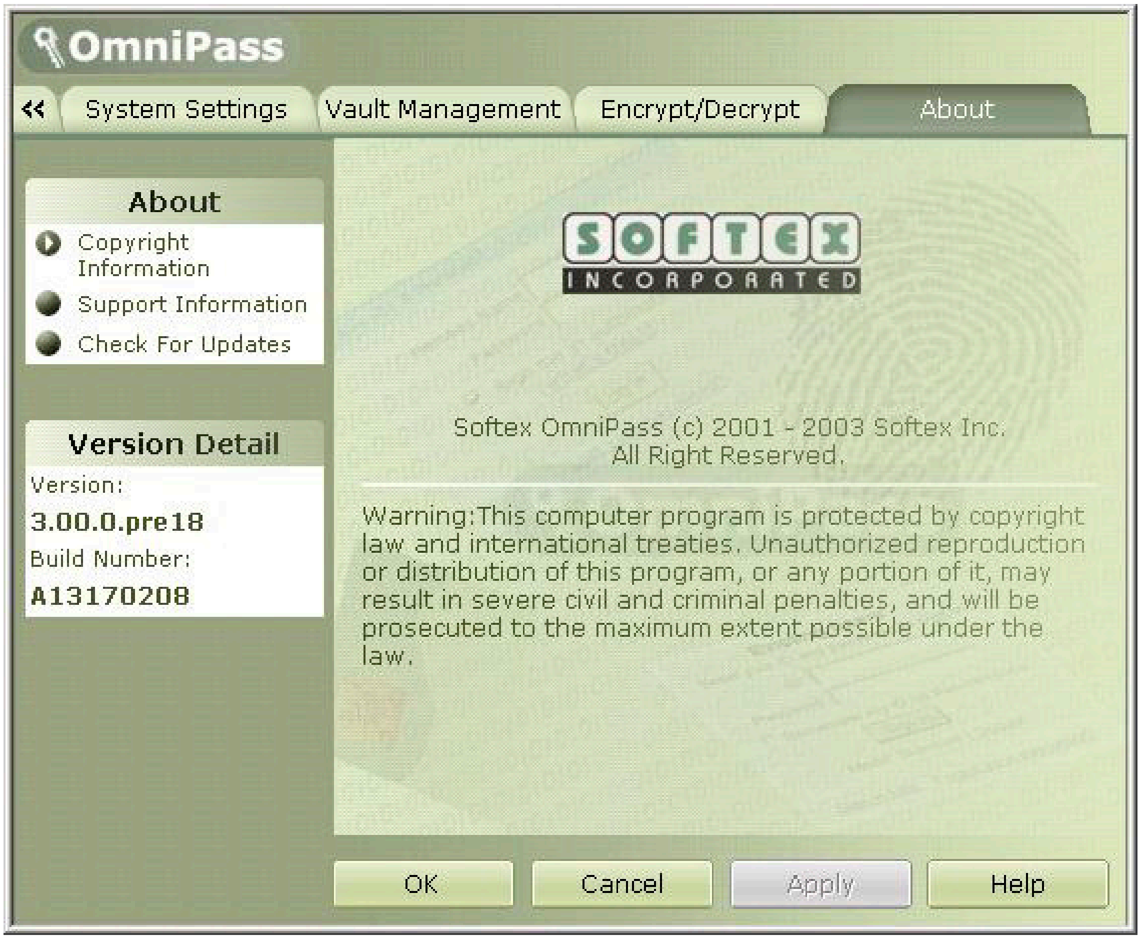
   Click the **Start** button, select **Settings**, and click **Control Panel** (if you are using Windows XP you will see the Control Panel directly in the Start menu; click it, then click **Switch to Classic View**). Double-click

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 (see Figure 1).



Version:
3.00.0.pre18
Build Number:
A13170208

Softex OmniPass (c) 2001 - 2003 Softex Inc.
All Right Reserved.

Warning:This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Figure 1: The About Tab Window of the OmniPass Control Panel

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 “warriors”), 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 (“Ikari” 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.*

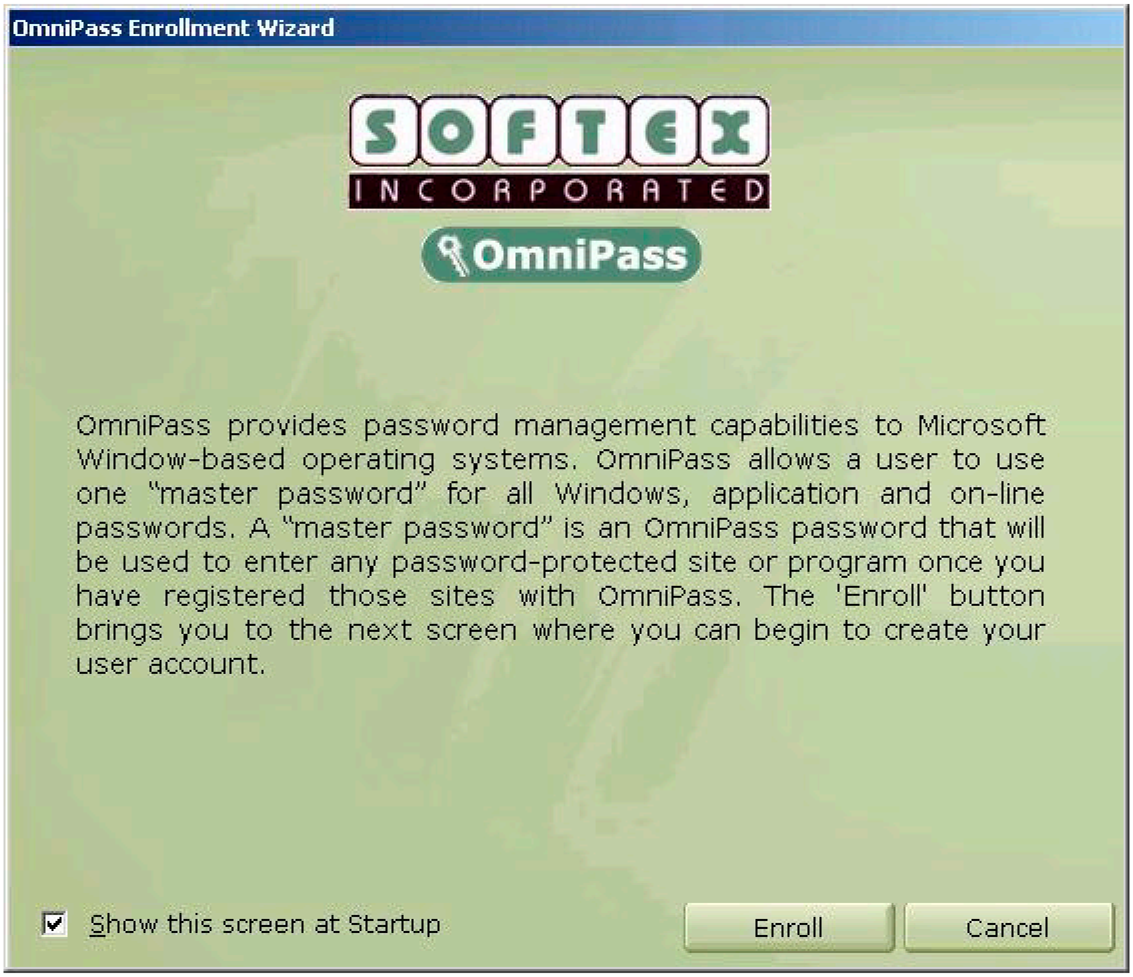
Continue to the next section to begin OmniPass user enrollment.

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** (see Figure 2).

2.2.1 Enroll



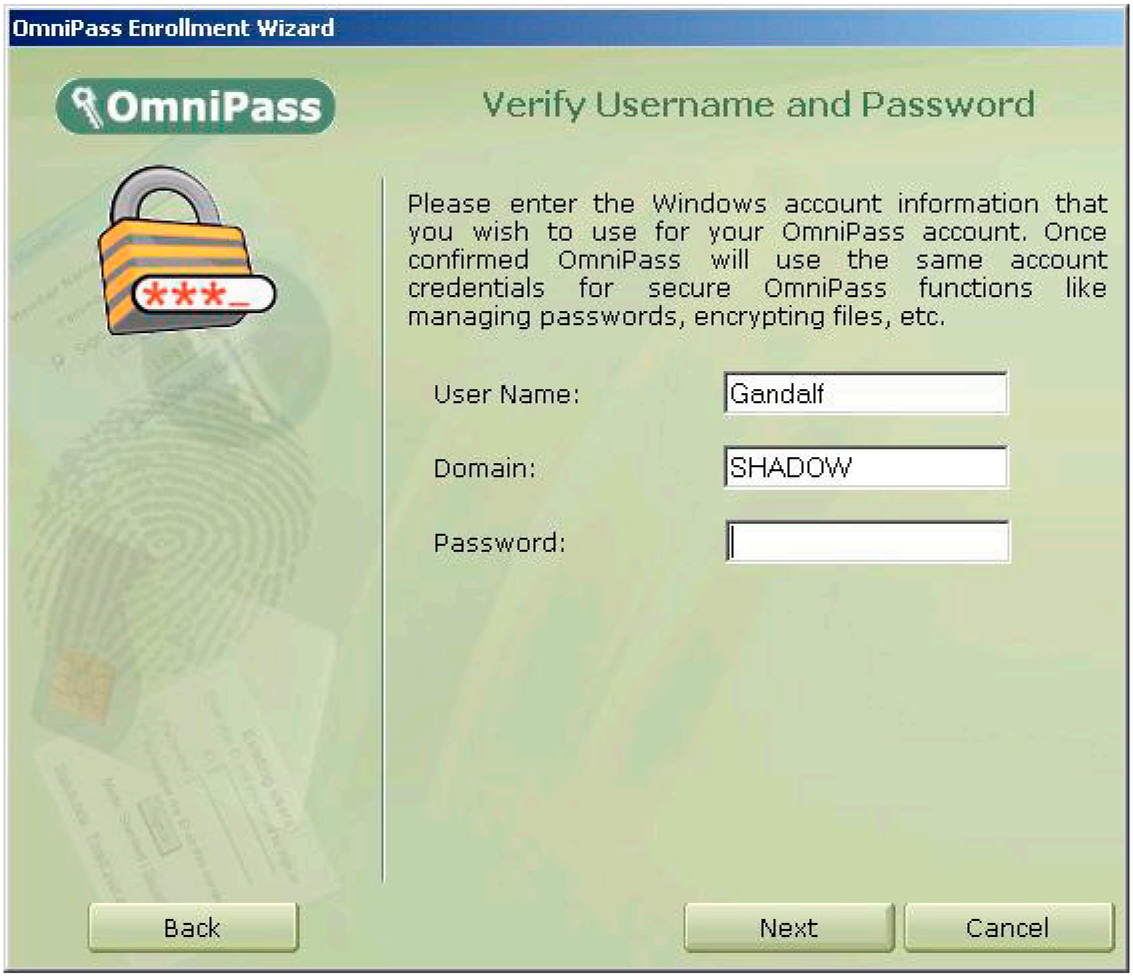
OmniPass provides password management capabilities to Microsoft Window-based operating systems. OmniPass allows a user to use one "master password" for all Windows, application and on-line passwords. A "master password" is an OmniPass password that will be used to enter any password-protected site or program once you have registered those sites with OmniPass. The 'Enroll' button brings you to the next screen where you can begin to create your user account.

☑ Show this screen at Startup

Figure 2: OmniPass Enrollment Wizard - Welcome

Click **Enroll** to proceed to username and password verification (see Figure 3). By default, the OmniPass Enrollment Wizard enters the credentials of the currently logged in Windows user.

2.2.2 Verify Credentials



OmniPass Enrollment Wizard

Verify Username and Password

Please enter the Windows account information that you wish to use for your OmniPass account. Once confirmed OmniPass will use the same account credentials for secure OmniPass functions like managing passwords, encrypting files, etc.

User Name: Gandalf

Domain: SHADOW

Password:

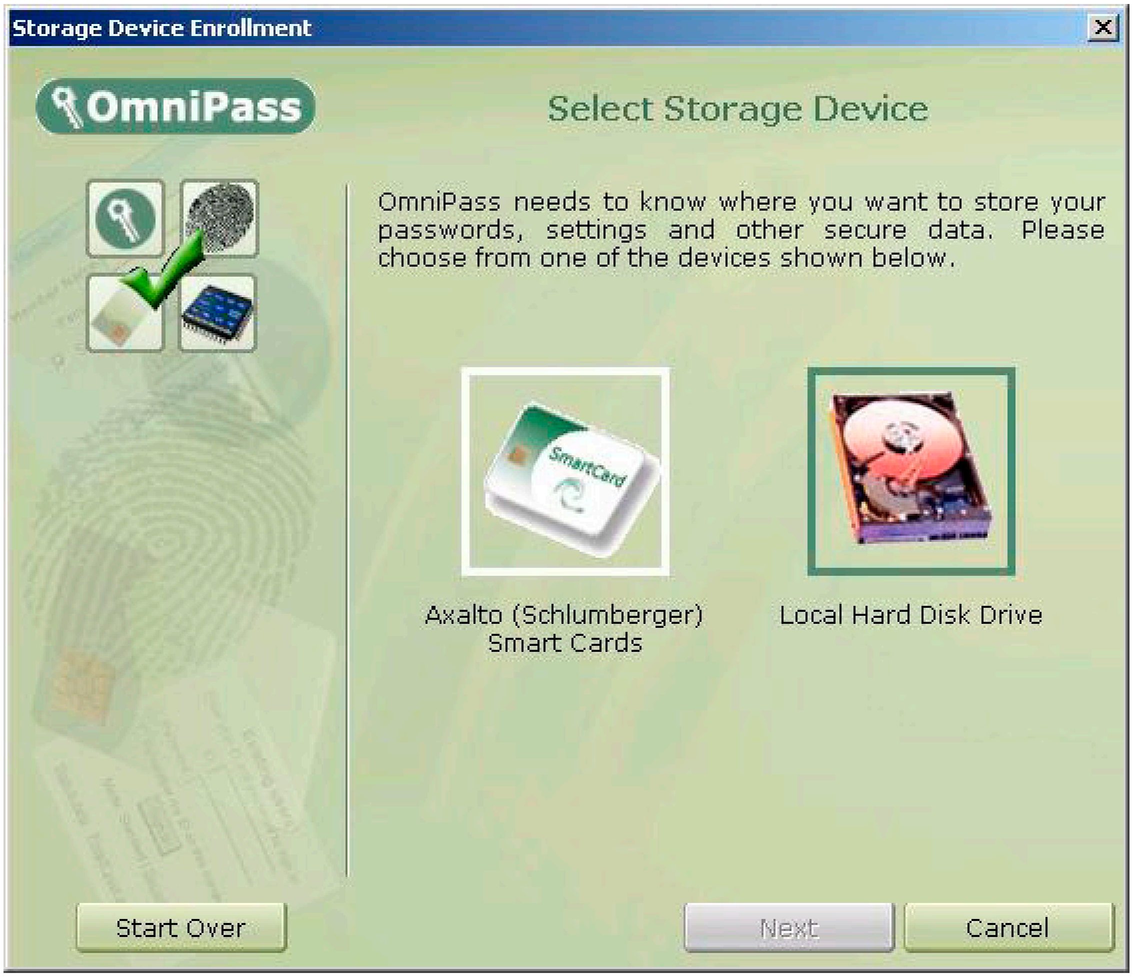
Figure 3: OmniPass Enrollment Wizard - Verify Username and Password

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 (see Figure 4).

2.2.3 Select Secure Storage Device (default)


Storage Device Enrollment

Select Storage Device

OmniPass needs to know where you want to store your passwords, settings and other secure data. Please choose from one of the devices shown below.

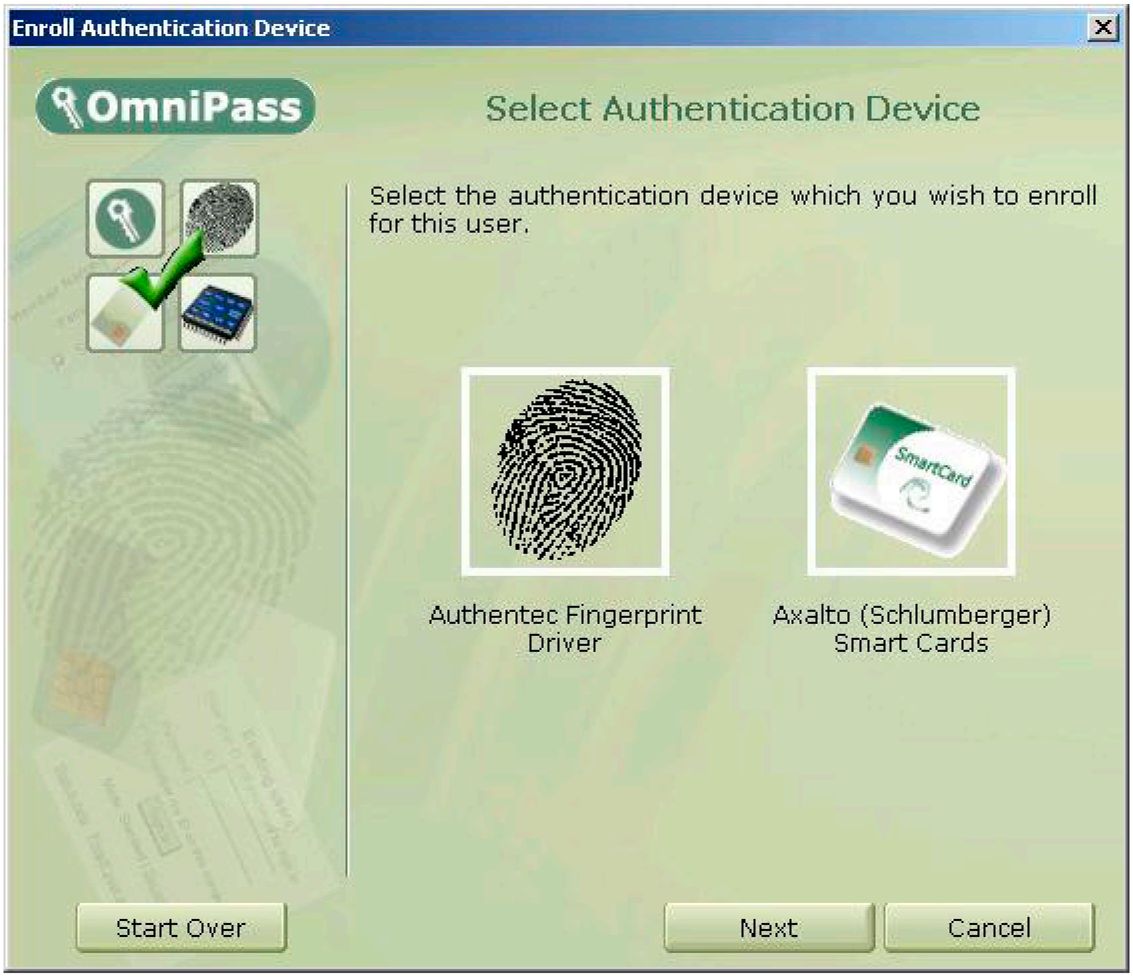
Figure 4: OmniPass Enrollment Wizard - Secure Storage Device Selection

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 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 (see Figure 5).

2.2.4 Enrolling an Authentication Device (default)



Select Authentication Device

Select the authentication device which you wish to enroll for this user.

Authentec Fingerprint Driver

Axalto (Schlumberger) Smart Cards

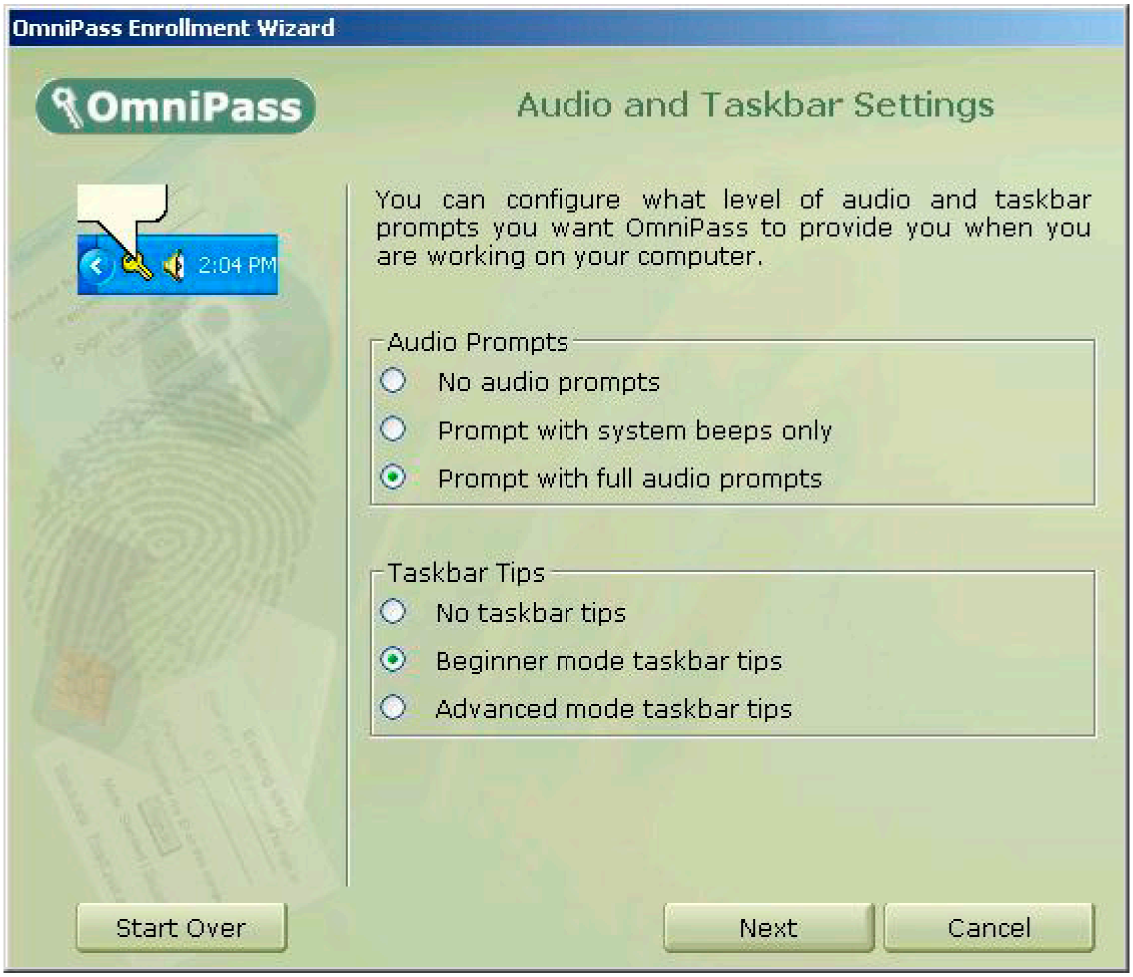
Figure 5: OmniPass Enrollment Wizard - Authentication Device Selection

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 (see Figure 6). You will be prompted to confirm that you are not enrolling any authentication devices.

2.2.5 User Notification Settings



OmniPass Enrollment Wizard

Audio and Taskbar Settings

You can configure what level of audio and taskbar prompts you want OmniPass to provide you when you are working on your computer.

Audio Prompts

○ No audio prompts

○ Prompt with system beeps only

● Prompt with full audio prompts

Taskbar Tips

○ No taskbar tips

● Beginner mode taskbar tips

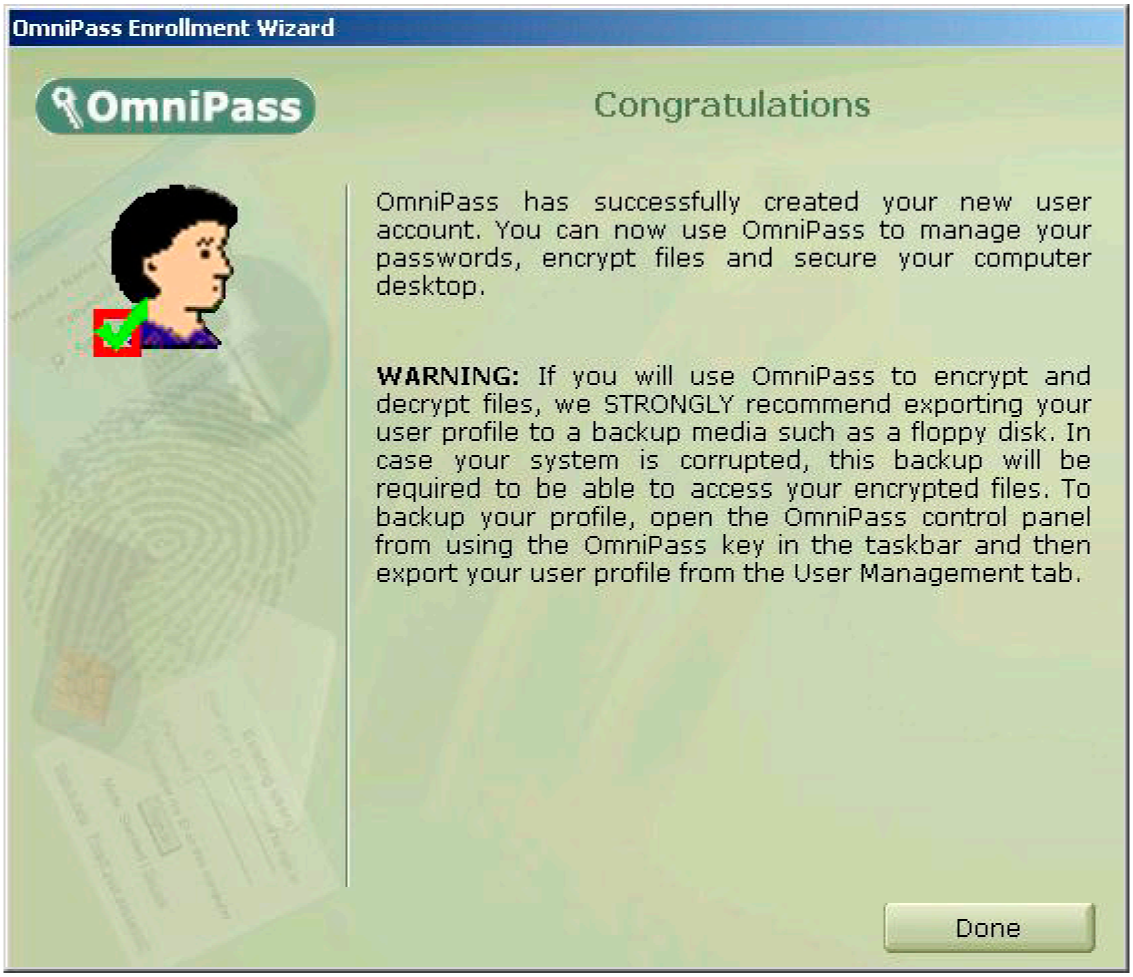
○ Advanced mode taskbar tips

Figure 6: OmniPass Enrollment Wizard - Audio and Taskbar Settings

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 Prompts** 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 (see Figure 7).

2.2.6 Congratulations



OmniPass has successfully created your new user account. You can now use OmniPass to manage your passwords, encrypt files and secure your computer desktop.

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. To backup your profile, open the OmniPass control panel from using the OmniPass key in the taskbar and then export your user profile from the User Management tab.

Figure 7: OmniPass Enrollment Wizard - Congratulations

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.

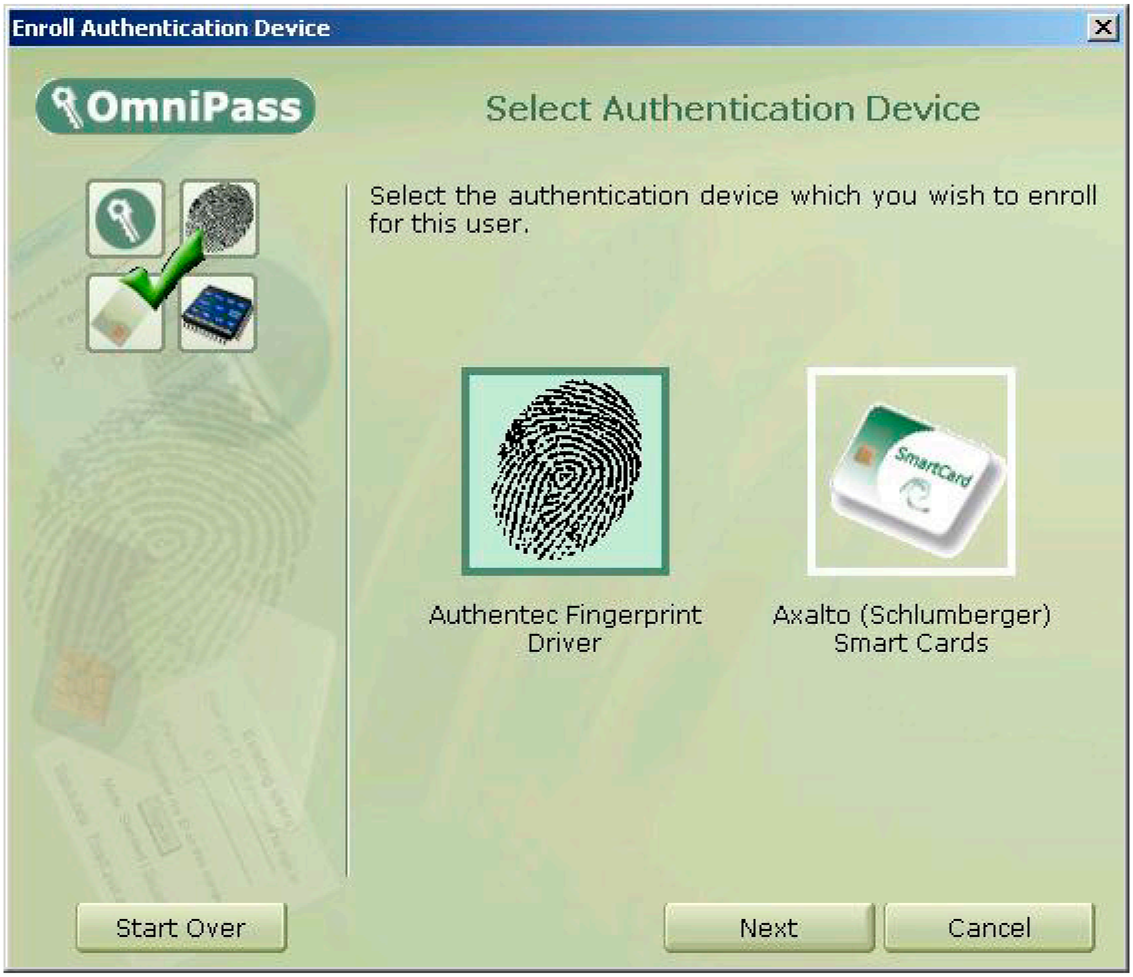
2.3 Enrolling an Authentication Device (Optional)

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 so access is restricted entirely unless your authentication devices are used. 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 **Enrollment** 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** (see Figure 8).



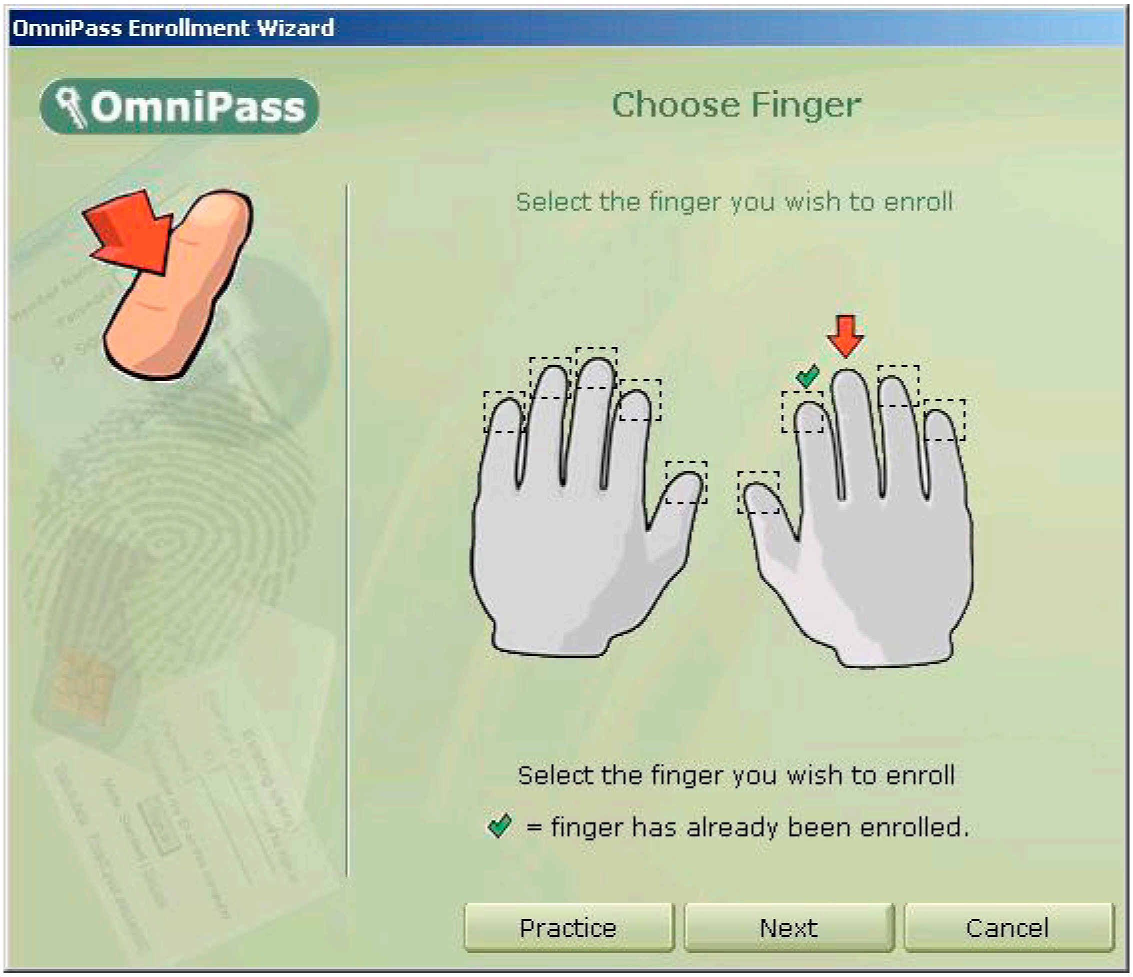
Enroll Authentication Device
OmniPass
Select Authentication Device
Authentec Fingerprint Driver
Axalto (Schlumberger) Smart Cards
SmartCard
Start Over
Next
Cancel

Select the authentication device which you wish to enroll for this user.

Figure 8: OmniPass Enrollment Wizard - Enrolling an Authentication Device

2.3.2 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** (see Figure 9).



OmniPass Enrollment Wizard

Choose Finger

Select the finger you wish to enroll

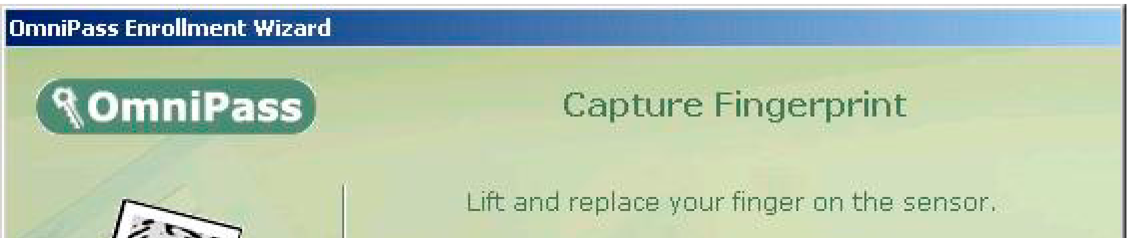
Select the finger you wish to enroll

✓ = finger has already been enrolled.

Figure 9: Enrolling an Authentication Device - Choose a Finger

2.3.3 Capturing the Fingerprint

It is now time for OmniPass to capture your selected fingerprint (see Figure 10). 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.



OmniPass Enrollment Wizard

Capture Fingerprint

Lift and replace your finger on the sensor.

Figure 10: Enrolling an Authentication Device - Capture Fingerprint

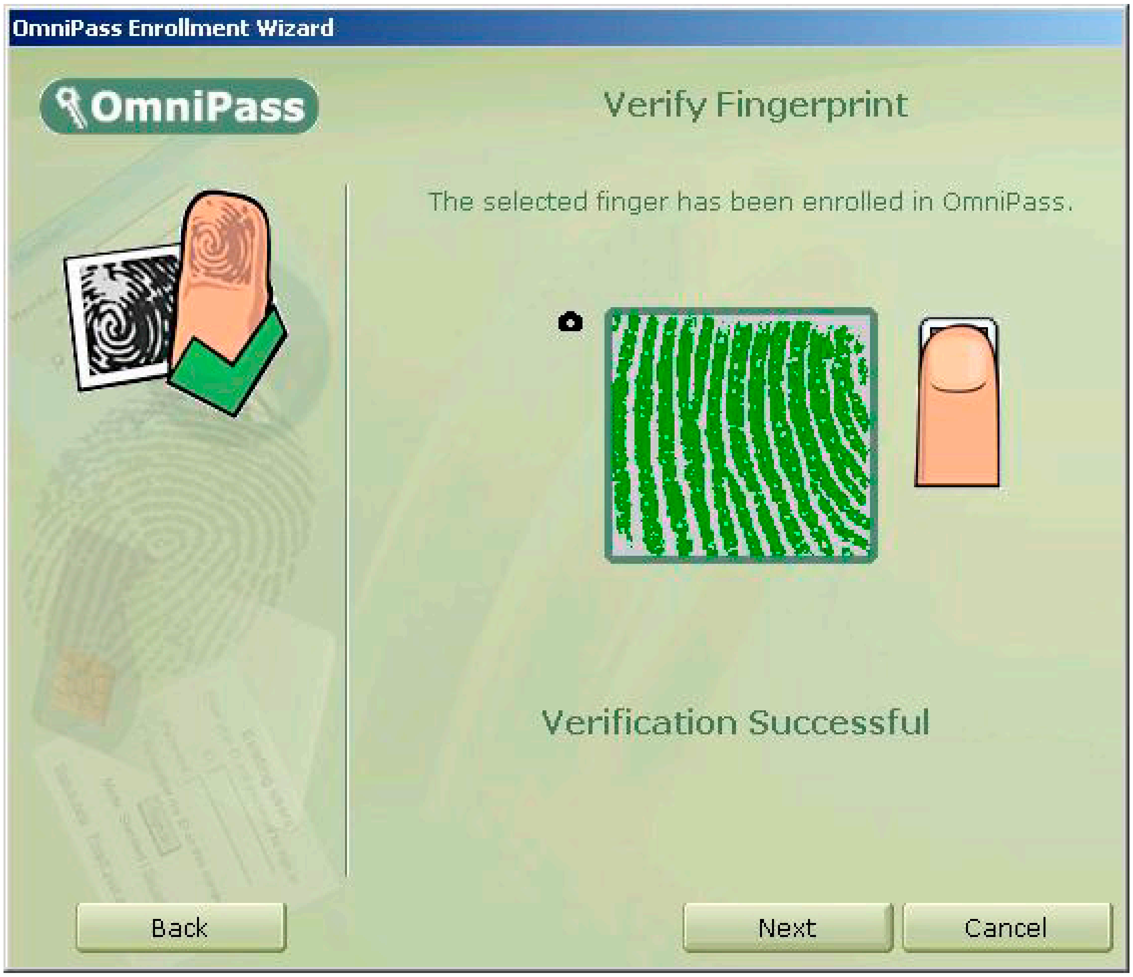
There are several types of fingerprint sensors (e.g. "swipe" or "touchpad"), and each type requires a different action for capturing. The "core" of the fingerprint is the ideal area for capture. The core of your fingerprint is usually aligned with the base of your cuticle. It is where the concentric 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 windows 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 (see Figure 9) 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.

2.3.4 Verifying the Fingerprint

Once OmniPass has successfully acquired the fingerprint, the **Verify Fingerprint** screen will automatically appear (see Figure 11).



The selected finger has been enrolled in OmniPass.

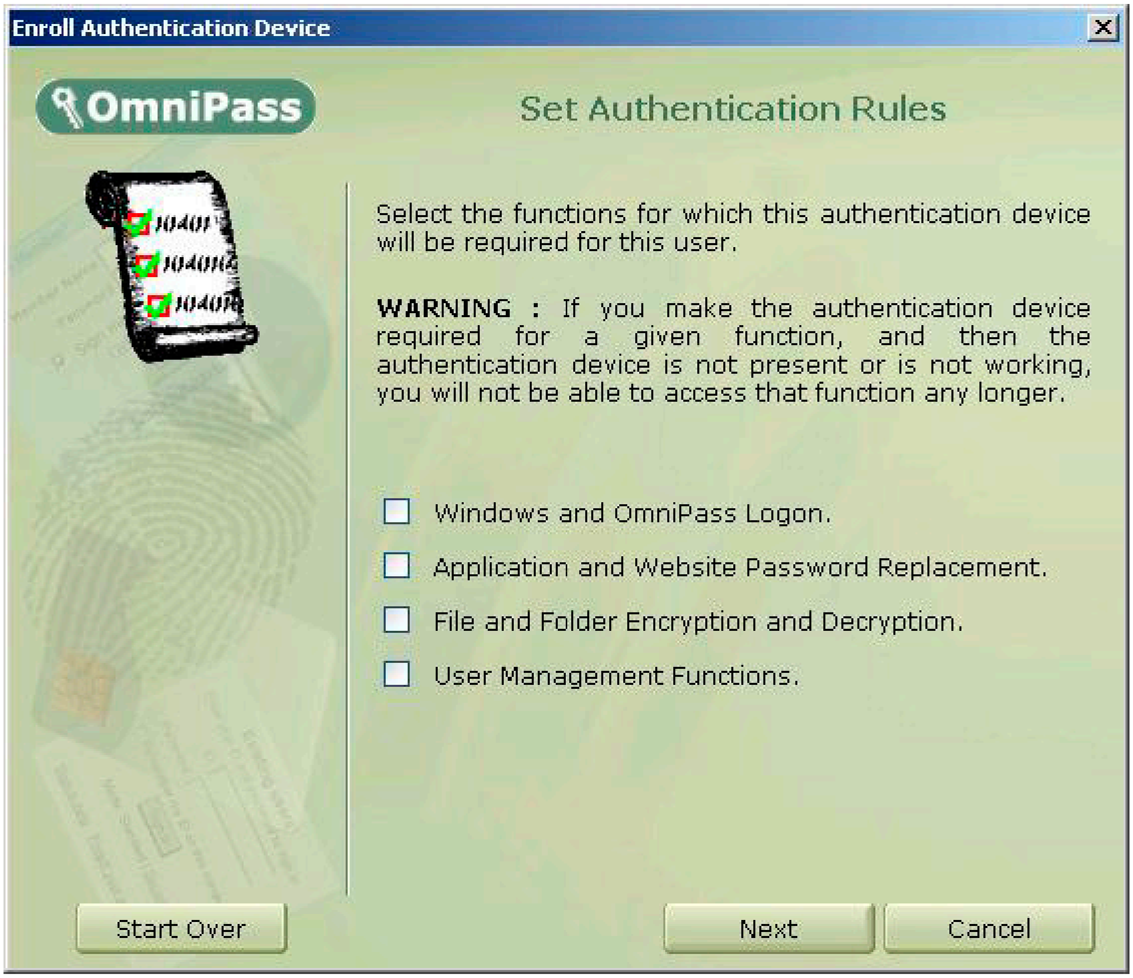
Verification Successful

Figure 11: Enrolling an Authentication Device - Verify Fingerprint

To verify your enrolled fingerprint, place or swipe your fingertip on the sensor 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.

2.3.5 Setting Authentication Rules (default)

After fingerprint verification, the **Set Authentication Rules** screen will automatically appear (see Figure 12). 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.



Set Authentication Rules

Select the functions for which this authentication device will be required for this user.

WARNING : If you make the authentication device required for a given function, and then the authentication device is not present or is not working, you will not be able to access that function any longer.

□ Windows and OmniPass Logon.

□ Application and Website Password Replacement.

□ File and Folder Encryption and Decryption.

□ User Management Functions.

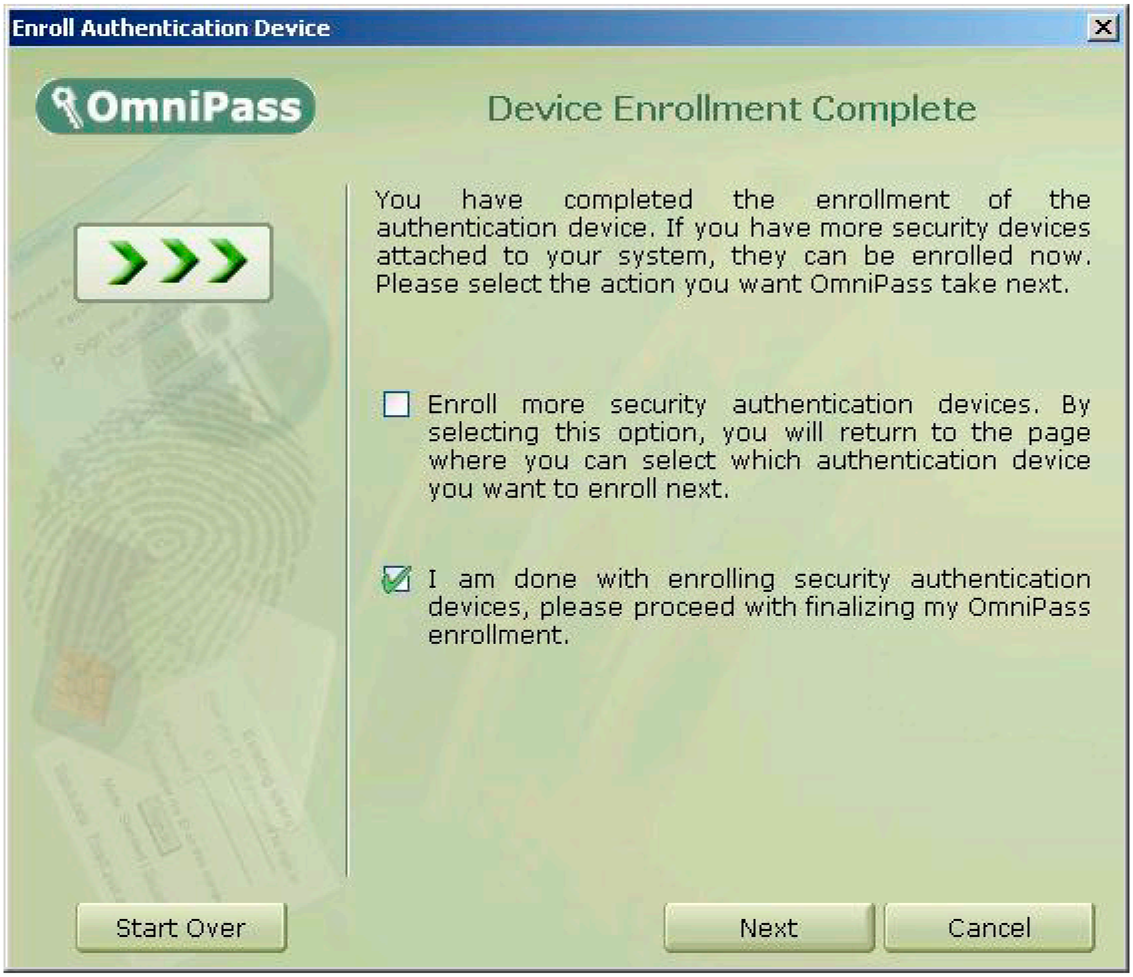
Figure 12: Enrolling an Authentication Device - Set Authentication Rules

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.

Click **Next** to proceed.

2.3.6 Completing Device Enrollment

After you set the authentication rules for the enrolled device, the **Device Enrollment Complete** screen will automatically appear (see Figure 13).



Device Enrollment Complete

You have completed the enrollment of the authentication device. If you have more security devices attached to your system, they can be enrolled now. Please select the action you want OmniPass take next.

□ Enroll more security authentication devices. By selecting this option, you will return to the page where you can select which authentication device you want to enroll next.

☑ I am done with enrolling security authentication devices, please proceed with finalizing my OmniPass enrollment.

Figure 13: Enrolling an Authentication Device - Device Enrollment Complete

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*.

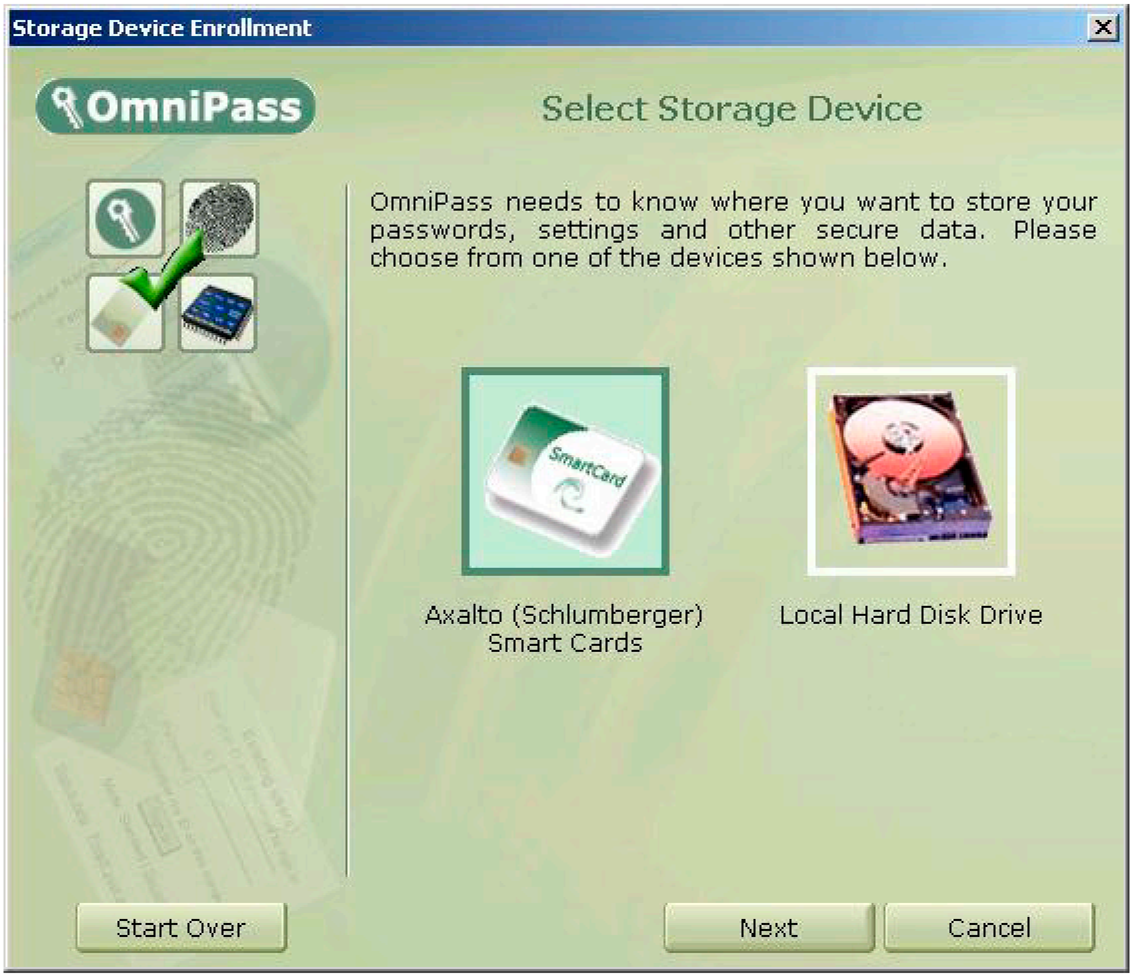
2.4 Alternate Storage Location (Optional)

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 Selecting a Storage Device

During initial user enrollment, at **Select Storage Device** select the storage device which you wish to use and click **Next** (see Figure 14).If a SmartCard is not present in the reader when you click **Next**, you will be prompted to insert it.



OmniPass needs to know where you want to store your passwords, settings and other secure data. Please choose from one of the devices shown below.

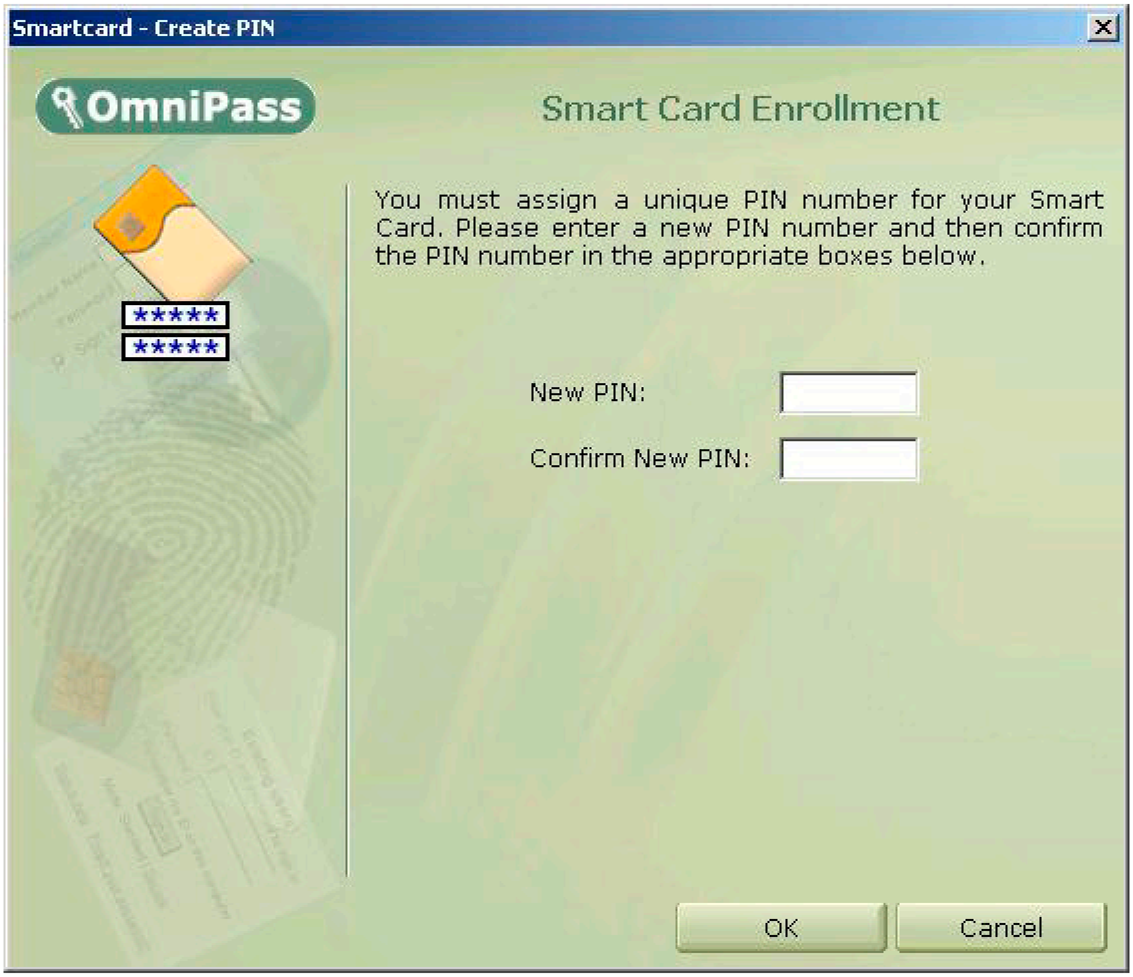
Figure 14: Alternate Storage Location - Select Storage Device

2.4.2 SmartCard Enrollment - Set PIN

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 (see Figure 15). 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**.



You must assign a unique PIN number for your Smart Card. Please enter a new PIN number and then confirm the PIN number in the appropriate boxes below.

New PIN:

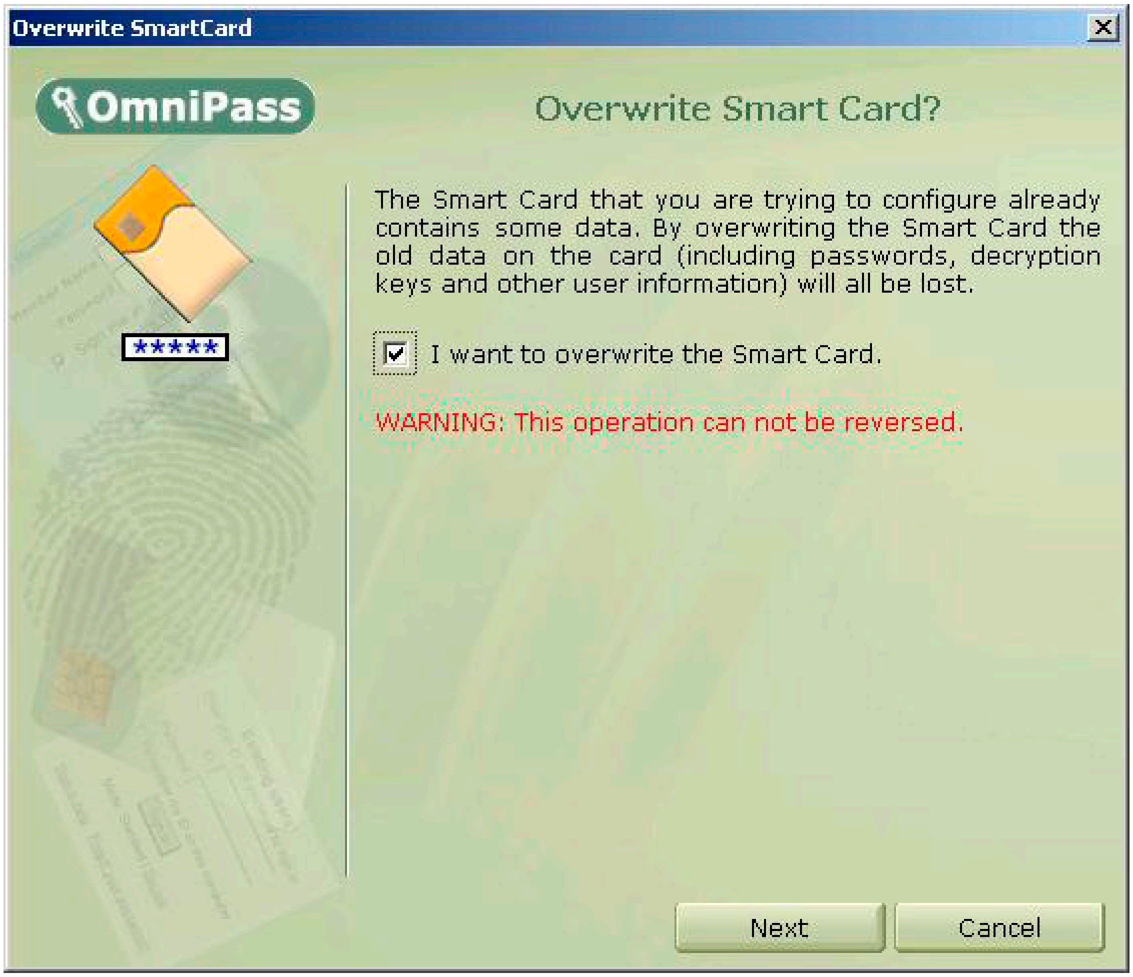
Confirm New PIN:

Figure 15: SmartCard Enrollment - Establish PIN

SmartCard Enrollment then directs you back to the next step of the OmniPass Enrollment Wizard, *2.2.4 Select Enrollment Device*.

2.4.3 SmartCard Enrollment - Overwrite Confirmation

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** (see Figure 16).



Overwrite Smart Card?

The Smart Card that you are trying to configure already contains some data. By overwriting the Smart Card the old data on the card (including passwords, decryption keys and other user information) will all be lost.

☑ I want to overwrite the Smart Card.

WARNING: This operation can not be reversed.

Figure 16: SmartCard Enrollment - Overwrite Confirmation

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.

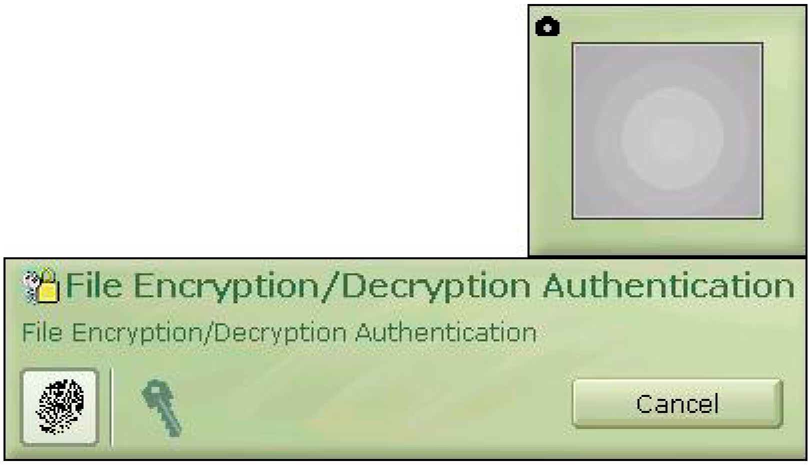
Part 2. Use covers basic OmniPass functionality. Review this section to quickly get familiar with the OmniPass functions you will most use. If your system is shared among several users (often the case in a home PC or SOHO environment) then you may find some additional useful features in *Part 3. Configure*.

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 (see Figure 17). 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.

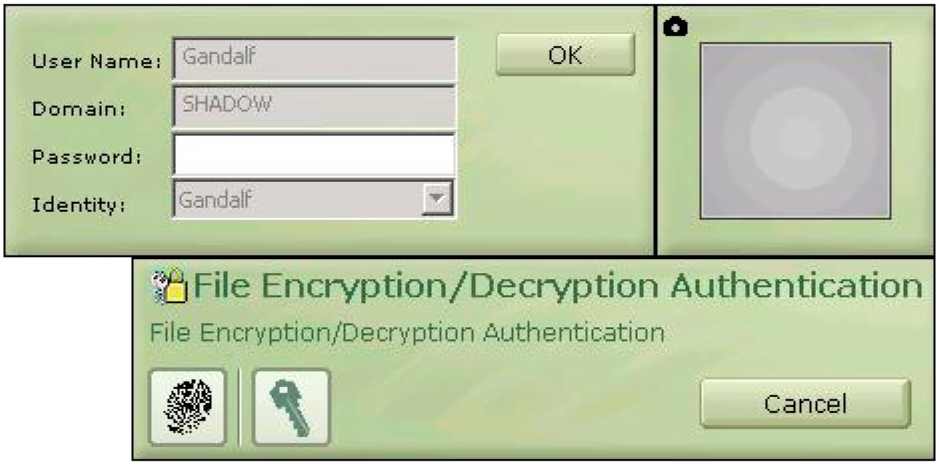


File Encryption/Decryption Authentication

File Encryption/Decryption Authentication

Figure 17: The OmniPass Authentication Toolbar

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 (see Figure 18).



File Encryption/Decryption Authentication

File Encryption/Decryption Authentication

User Name: Gandalf

Domain: SHADOW

Password:

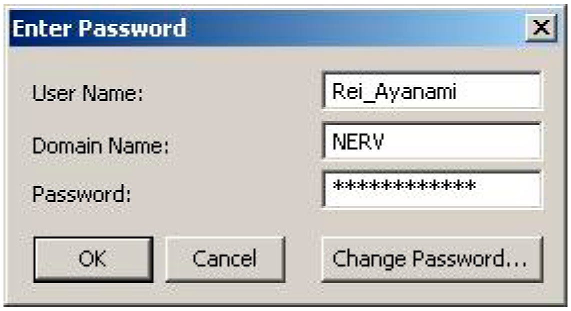
Identity: Gandalf

Figure 18: OmniPass Authentication Toolbar - Fully Expanded

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 (See Figures 19 and 20).



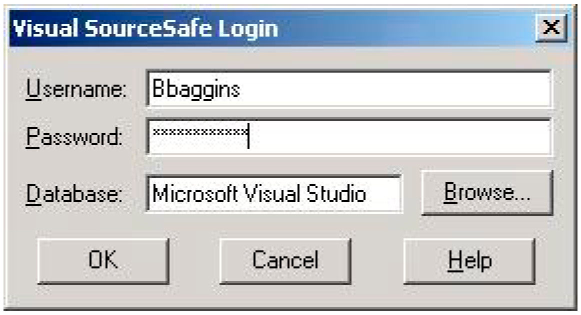
Enter Password

User Name: Rei_Ayanami

Domain Name: NERV

Password: ************

Figure 19: Microsoft Outlook Login



Visual SourceSafe Login

Username: Bbaggins

Password: ************

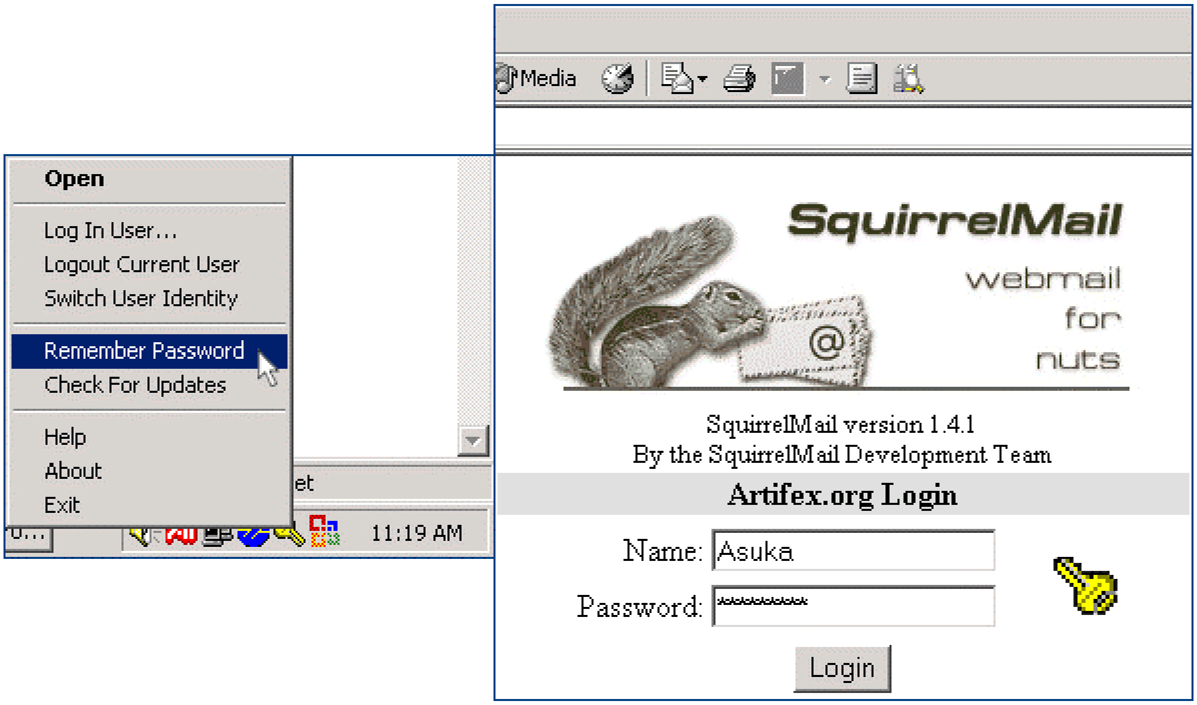
Database: Microsoft Visual Studio

Figure 20: Microsoft Visual SourceSafe Login

Both of the above dialogs represent application login prompts that OmniPass will recognize as candidates for password replacement. If you have configured your Taskbar Tips to do so, OmniPass will notify you of when you have an opportunity to remember a password.

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* (see Figure 21).



SquirrelMail version 1.4.1
By the SquirrelMail Development Team

Artifex.org Login

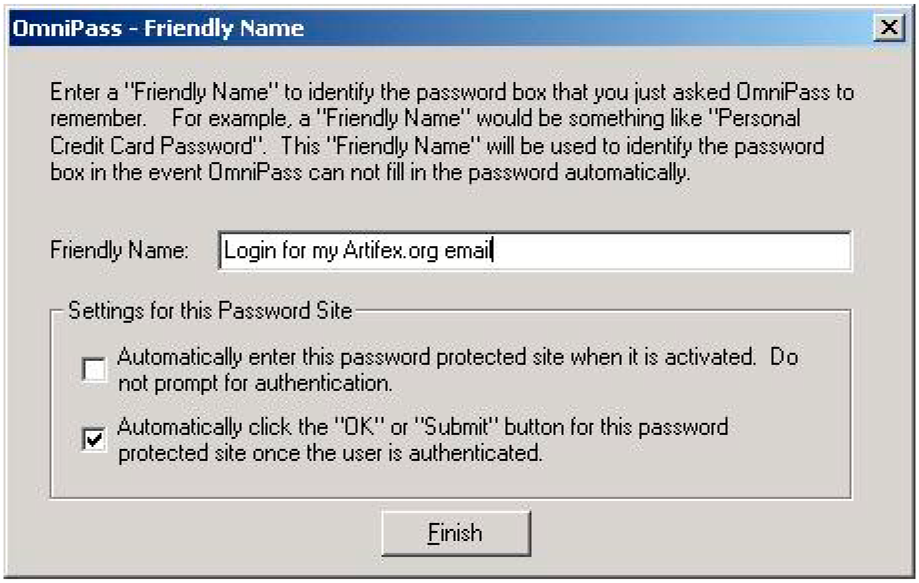
Name: Asuka

Password: **********

Figure 21: The Two Step Remember Password Procedure

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 (see Figure 22). 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.



Enter a "Friendly Name" to identify the password box that you just asked OmniPass to remember. For example, a "Friendly Name" would be something like "Personal Credit Card Password". This "Friendly Name" will be used to identify the password box in the event OmniPass can not fill in the password automatically.

Friendly Name: Login for my Artifex.org email

Settings for this Password Site

□ Automatically enter this password protected site when it is activated. Do not prompt for authentication.

☑ Automatically click the "OK" or "Submit" button for this password protected site once the user is authenticated.

Figure 22: Remember Password Options

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 (see Figure 22). 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 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*).

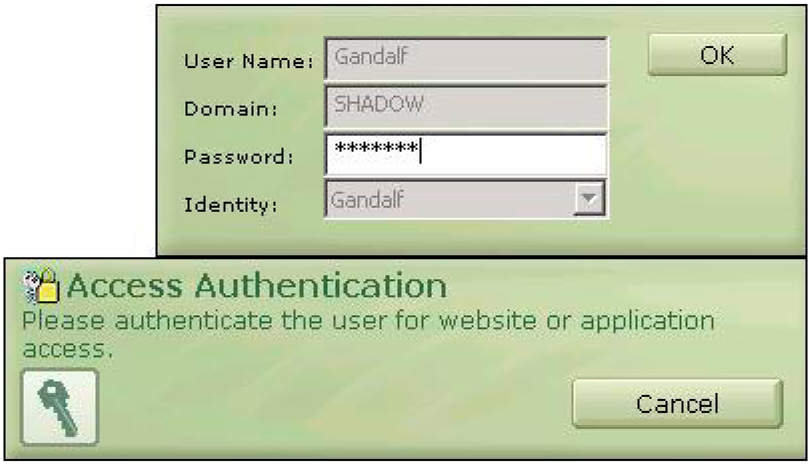
3.3 Logging in to a Remembered Site …

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 (see Figure 23). Enter your "master password" and you will be allowed into the site.



User Name: Gandalf

Domain: SHADOW

Password: *******

Identity: Gandalf

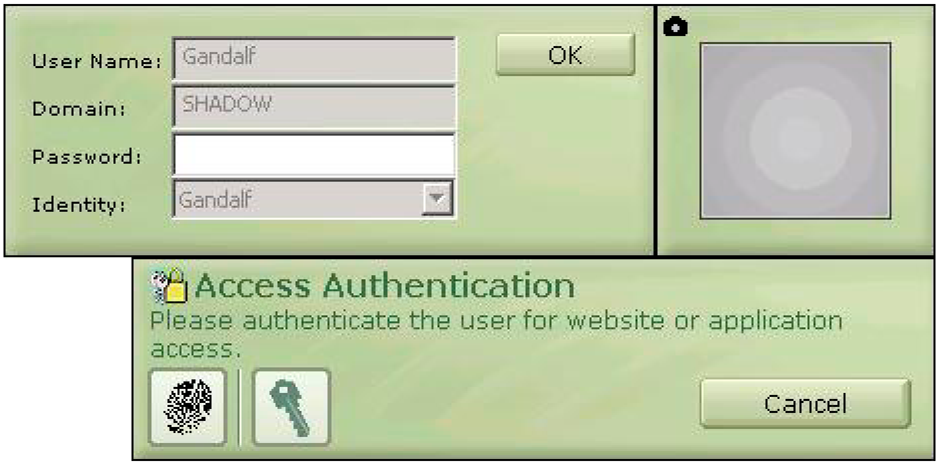
Access Authentication

Please authenticate the user for website or application access.

Figure 23: Authentication Prompt for Remembered Site

3.3.2 With Multiple Authentication Methods

Or you may be presented with an OmniPass authentication prompt that has several different authentication methods (see Figure 24).



User Name: Gandalf

Domain: SHADOW

Password:

Identity: Gandalf

Access Authentication

Please authenticate the user for website or application access.

Figure 24: Authentication Prompt - Multiple 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 or swipe 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 or swipe 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.

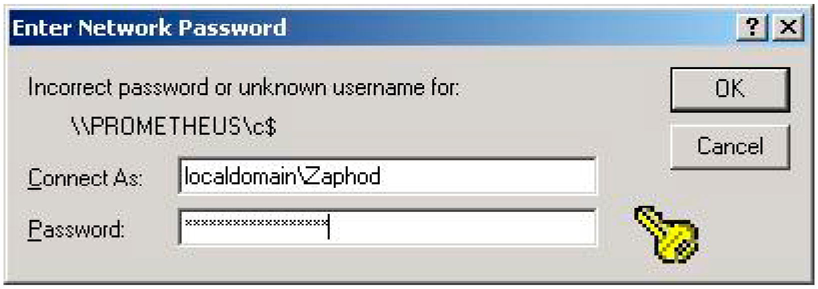
NOTE: If a machine is locked and OmniPass detects a different user logging back in with a fingerprint, the first user will be logged out and the second user logged in.

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".


Enter Network Password

Incorrect password or unknown username for:
\\PROMETHEUS\c$

Connect As: localdomain\Zaphod

Password: ******************

Figure 25: Authentication Prompt for a Network Share

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**.

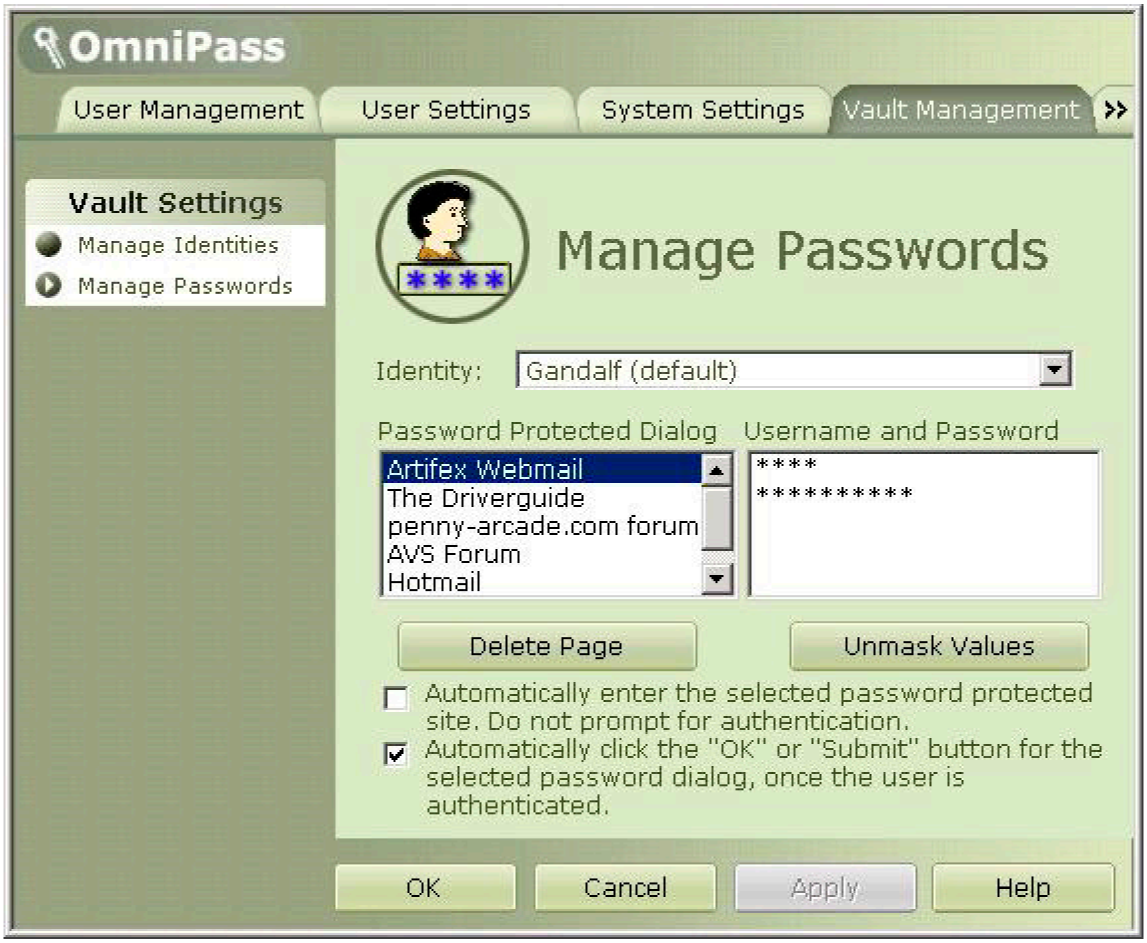
You will see the **Manage Passwords** interface, with a list of your friendly names (see Figure 26).

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 will overwrite an old set of credentials for a website if you attempt to use **Remember Password** on an already remembered site. *Example – You had OmniPass remember the website "artifex.org" with the login "Akasaka" and the password "Nutmeg". You then go back to artifex.org, but instead of letting OmniPass log you in, you enter the login "Akasaka" and the password "Cinnamon". You do NOT click Submit, and you use* ***Remember Password*** *to turn the cursor into the OmniPass key, and you click near the login prompt. OmniPass will prompt you for confirmation and then overwrite the login credentials for "artifex.org". The login "Akasaka" is the same, but the password has been changed from "Nutmeg" to "Cinnamon". In the event your password is changed, this is how you update OmniPass with the new password.*

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



Identity: Gandalf (default)

Password Protected Dialog	Username and Password
Artifex Webmail The Driverguide penny-arcade.com forum AVS Forum Hotmail	**** **********

□ Automatically enter the selected password protected site. Do not prompt for authentication.

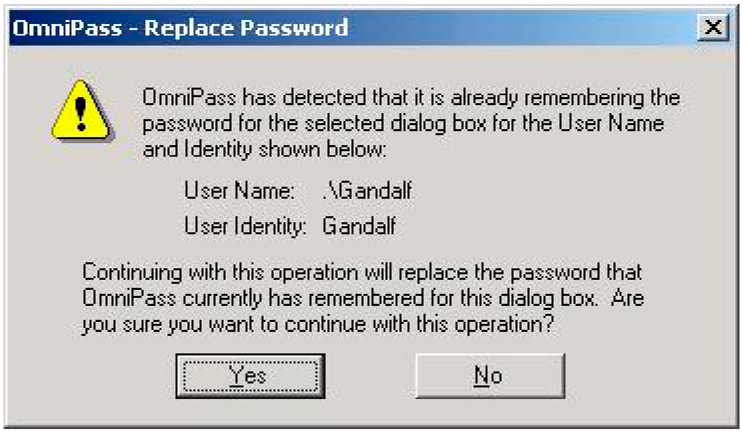
☑ Automatically click the "OK" or "Submit" button for the selected password dialog, once the user is authenticated.

Figure 26: Vault Management - Manage Passwords

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

Identities allow OmniPass users to have multiple accounts to the same site (e.g. *frodo@hobbitmail.com* and *smeagle@hobbitmail.com*). If OmniPass did not provide you identities, you would be limited to remembering one account per site. Let us say you have a user enrolled into OmniPass named *Player1* and you have only one identity for this user (when you go to Vault Management tab, you see only *Player1 (default)* in the Manage Identities field). You go to your favorite webmail site, *www.hobbitmail.com*, and you remember the username *frodo* and password *ringbearer*. Now whenever you go to *www.hobbitmail.com* OmniPass prompts you to authenticate, and then you are granted access to your *frodo@hobbitmail.com* Inbox. Now let us say you registered for another email account at *www.hobbitmail.com* with the username *smeagle* and password *gollum.* You then go to *www.hobbitmail.com* and you hit **Cancel** on the OmniPass authentication prompt instead of authenticating. You fill in the webmail login prompt with your other credentials (*smeagle* and *gollum*) and you use **Remember Password** to register the credentials with OmniPass. OmniPass will notify you that you have already remembered a set of credentials for this site, and will ask you if you wish to proceed (See Figure 27).



OmniPass - Replace Password

OmniPass has detected that it is already remembering the password for the selected dialog box for the User Name and Identity shown below:

User Name: .\Gandalf
User Identity: Gandalf

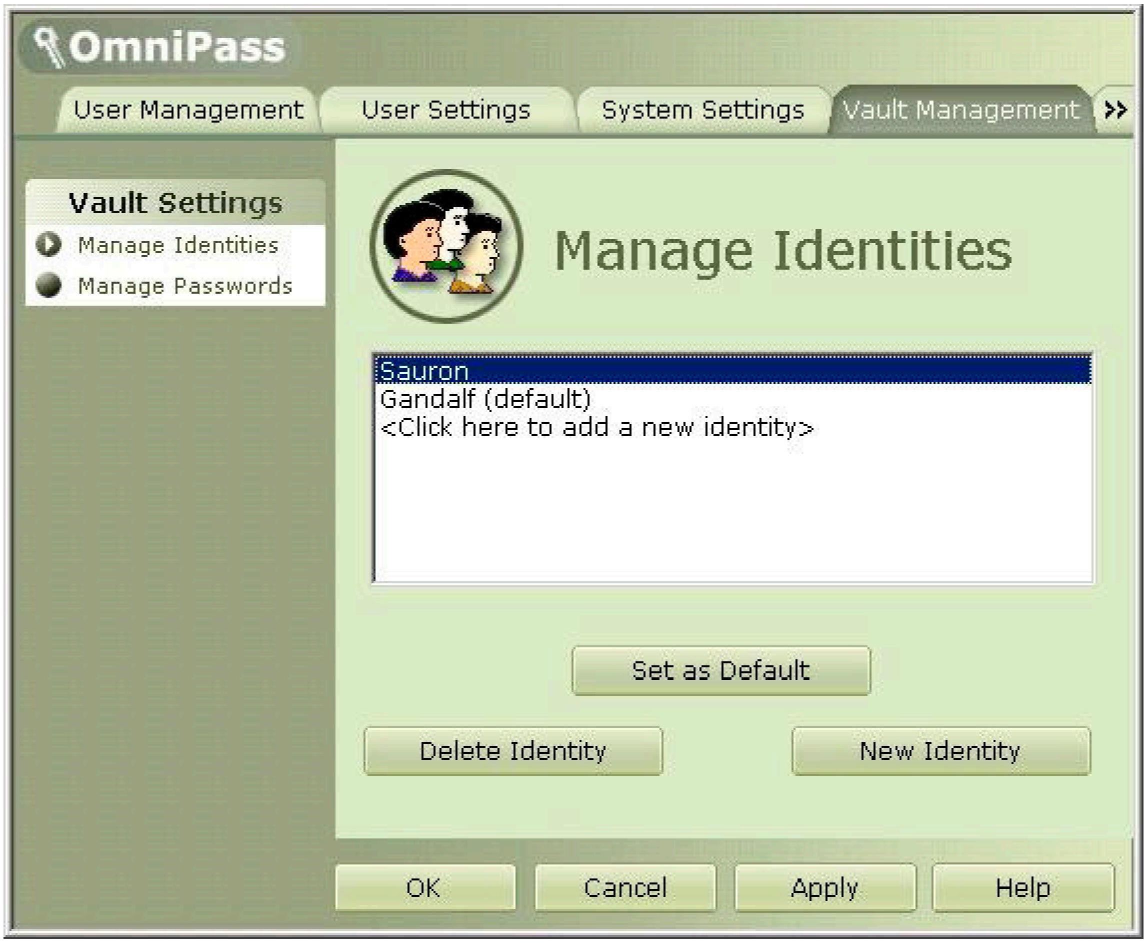
Continuing with this operation will replace the password that OmniPass currently has remembered for this dialog box. Are you sure you want to continue with this operation?

Figure 27: Overwrite Credentials

If you click **Yes** OmniPass will remember the new credentials (overwriting the old credentials), and whenever you go to *www.hobbitmail.com* you will be prompted to authenticate, and granted access to your *smeagle@hobbitmail.com* Inbox. If you click **No** OmniPass will not remember the new credentials (keeping your old credentials), and whenever you go to *www.hobbitmail.com* you will be prompted to authenticate, and granted access to your *frodo@hobbitmail.com*. Please continue to find out how to use identities to remember multiple sets of credentials to the same site.

Should you want to remember more than one login to a site (e.g. you have two or more Hotmail accounts you would like to remember), OmniPass can provide this functionality through User Identities. The following example shows how two OmniPass User Identities are used to remember two distinct logins to the same website.

Example - You have one email account, sauron@wizardmail.com*, for professional use and another email account,* gandalf@wizardmail.com*, for personal use. Each account has a distinct username/password combination. You store one username/password combination for the email client under the* Sauron *identity, and you store the other username/password combination under the* Gandalf *identity. When you are using your email for work, choose the* Sauron *identity. When you go to* www.wizardmail.com *to access your webmail, authenticating via OmniPass will log you into your work email account (*sauron@wizardmail.com*). Switching to your* Gandalf *identity, and going back to* www.wizardmail.com *to authenticate via OmniPass, You will be logged into your personal email account (*gandalf@wizardmail.com*).*



Sauron
Gandalf (default)
<Click here to add a new identity>

Figure 28: Vault Management - Manage 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 28). You can only manage the identities of the currently logged in OmniPass user

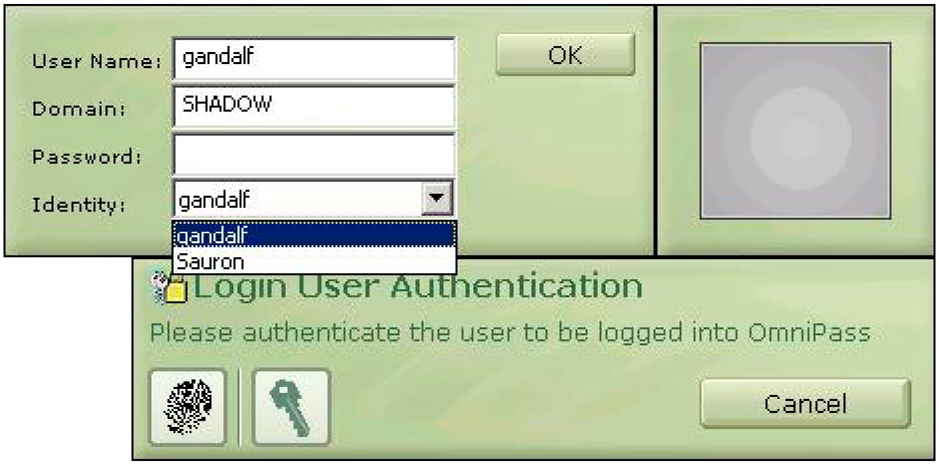
To add a new identity, click **New Identity** or double-click **<Click here to add a new identity>**. Name the new identity and click **OK**. Click **Apply** to ensure the settings are saved. You can now switch to the new identity and start remembering passwords.

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 (see Figure 29).



User Name: gandalf

Domain: SHADOW

Password:

Identity: gandalf

OK
gandalf
Sauron
Login User Authentication
Please authenticate the user to be logged into OmniPass
Cancel

Figure 29: Choose Identity During 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 (see Figure 30). The **Switch Identity** dialog will appear (see Figure 31). Select the desired identity and then click **OK**.

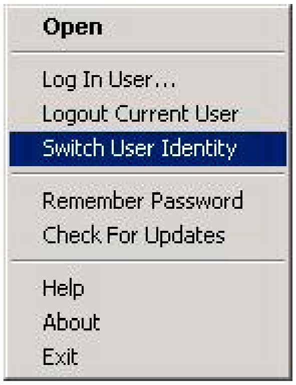
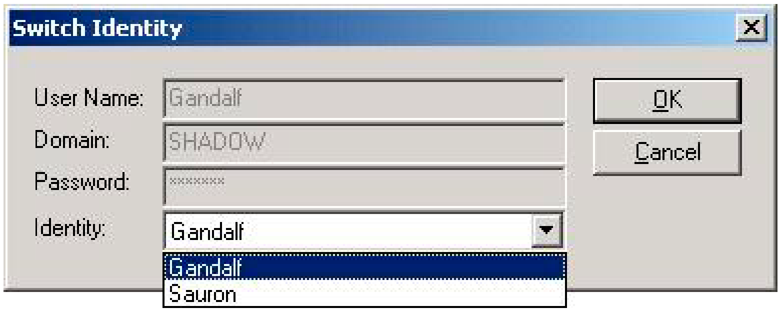


Figure 30: Switch User Identity



Switch Identity

User Name: Gandalf

Domain: SHADOW

Password: *******

Identity: Gandalf

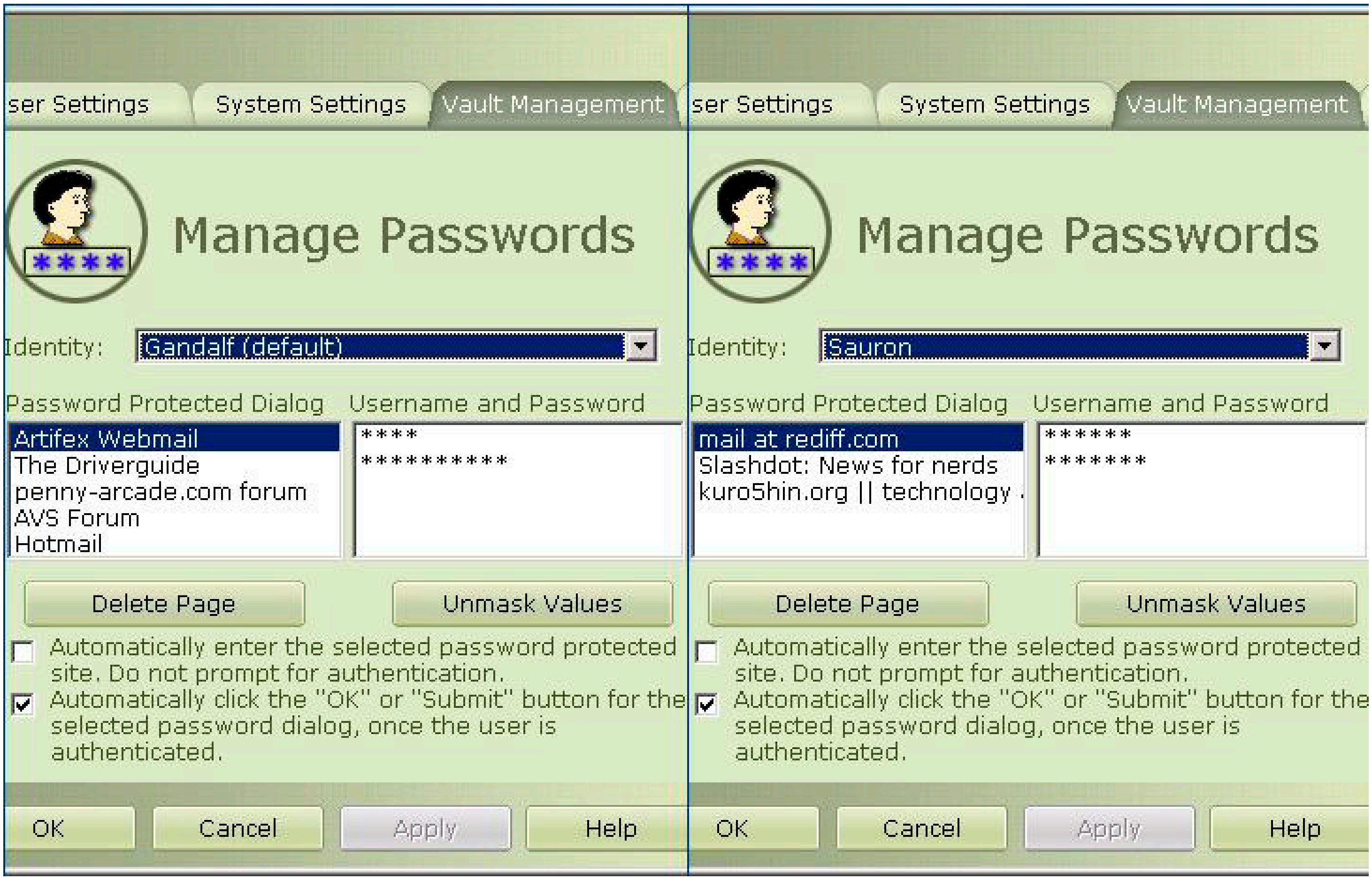
Gandalf

Sauron

Figure 31: Select Identity

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 (see Figure 32). You can perform all the functions explained in *Chapter 3.5 Password Management*.



Identity: Gandalf (default)

Password Protected Dialog	Username and Password
Artifex Webmail	****
The Driverguide	**********
penny-arcade.com forum	
AVS Forum	
Hotmail	

□ Automatically enter the selected password protected site. Do not prompt for authentication.

☑ Automatically click the "OK" or "Submit" button for the selected password dialog, once the user is authenticated.

Identity: Sauron

Password Protected Dialog	Username and Password
mail at rediff.com	******
Slashdot: News for nerds	*******
kuro5hin.org || technology .	

□ Automatically enter the selected password protected site. Do not prompt for authentication.

☑ Automatically click the "OK" or "Submit" button for the selected password dialog, once the user is authenticated.

Figure 32: Managing Passwords for Multiple Identities

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 (see Figure 33). OmniPass will prompt you to authenticate.

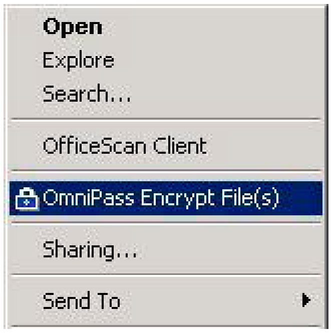
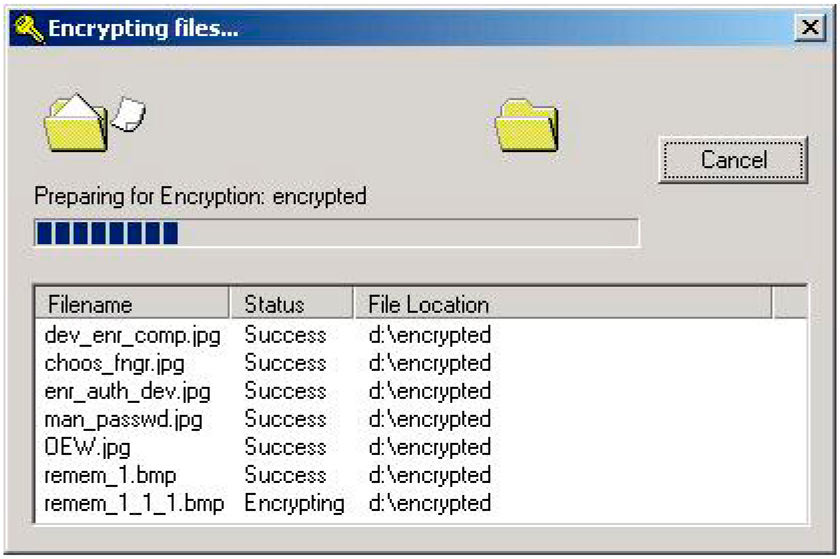


Figure 33: OmniPass Encrypt File(s)



Preparing for Encryption: encrypted

Filename	Status	File Location
dev_enr_comp.jpg	Success	d:\encrypted
choos_fngr.jpg	Success	d:\encrypted
enr_auth_dev.jpg	Success	d:\encrypted
man_passwd.jpg	Success	d:\encrypted
OEW.jpg	Success	d:\encrypted
remem_1.bmp	Success	d:\encrypted
remem_1_1_1.bmp	Encrypting	d:\encrypted

Figure 34: Encrypting a Folder Containing Multiple Files

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 (see Figure 34). 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.

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. Once decrypted, they will remain so 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** (See Figures 35 and 36). A copy of the file will be decrypted to the target directory. The original encrypted file will remain in the encrypted folder.

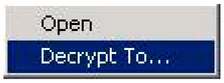


Figure 35: Decrypt To...

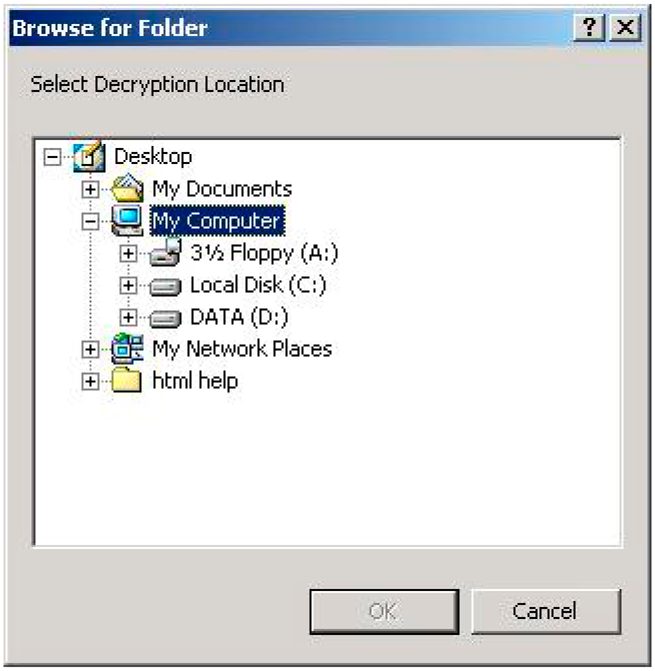


Figure 36: Select Decryption Location

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 (see Figure 37). OmniPass will prompt you to authenticate.

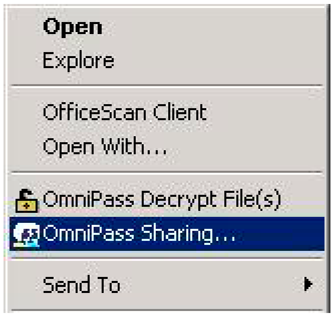
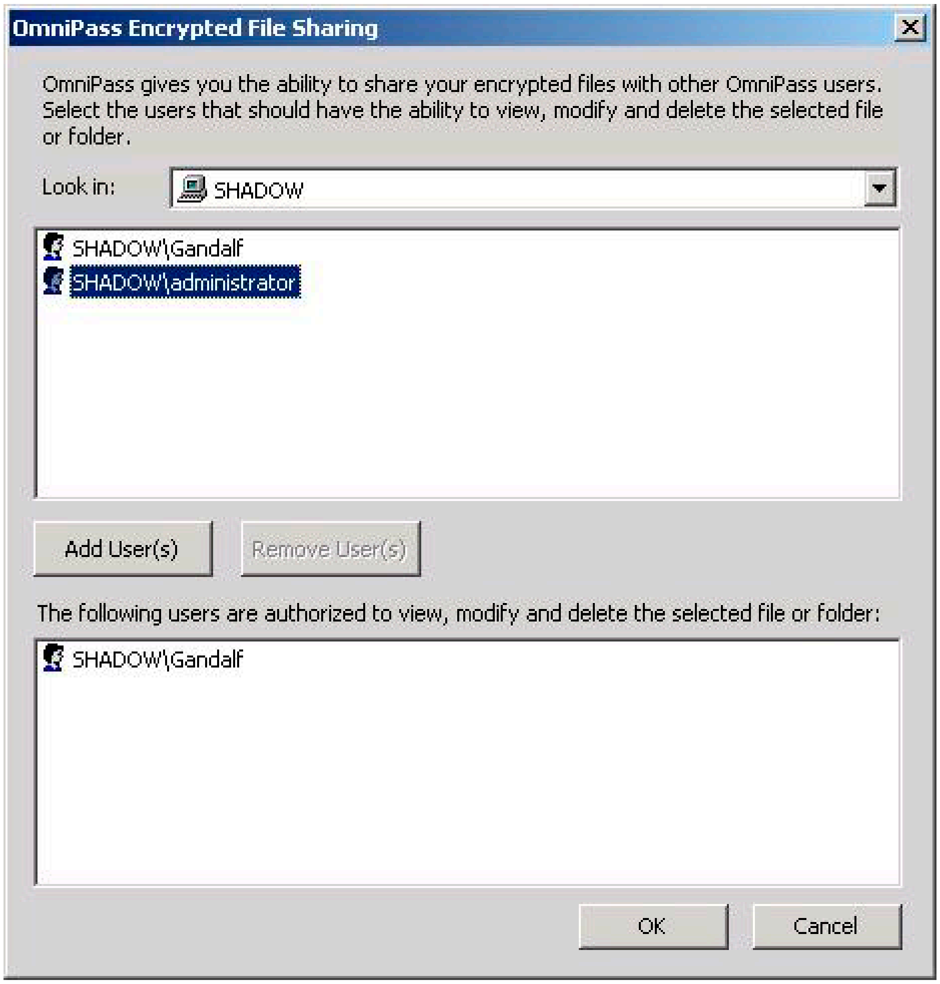


Figure 37: OmniPass Sharing

Upon successful authentication, the **OmniPass Encrypted File Sharing** dialog automatically opens (see Figure 38). 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.



OmniPass Encrypted File Sharing

OmniPass gives you the ability to share your encrypted files with other OmniPass users. Select the users that should have the ability to view, modify and delete the selected file or folder.

Look in: SHADOW

SHADOW\Gandalf
SHADOW\administrator

The following users are authorized to view, modify and delete the selected file or folder:

SHADOW\Gandalf

Figure 38: OmniPass Encrypted File Sharing

⚠ NOTE: Sharing an OmniPass encrypted file or folder 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 (see Figure 39). These files cannot be accessed until they are decrypted. Icons of encrypted folders are also updated with a lock graphic.

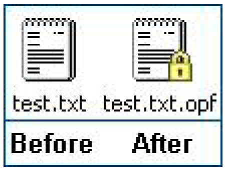


Figure 39: Locked File - Before and After

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 you 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 as the user profile originally created and with which you encrypted your files.

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** (see Figure 40).

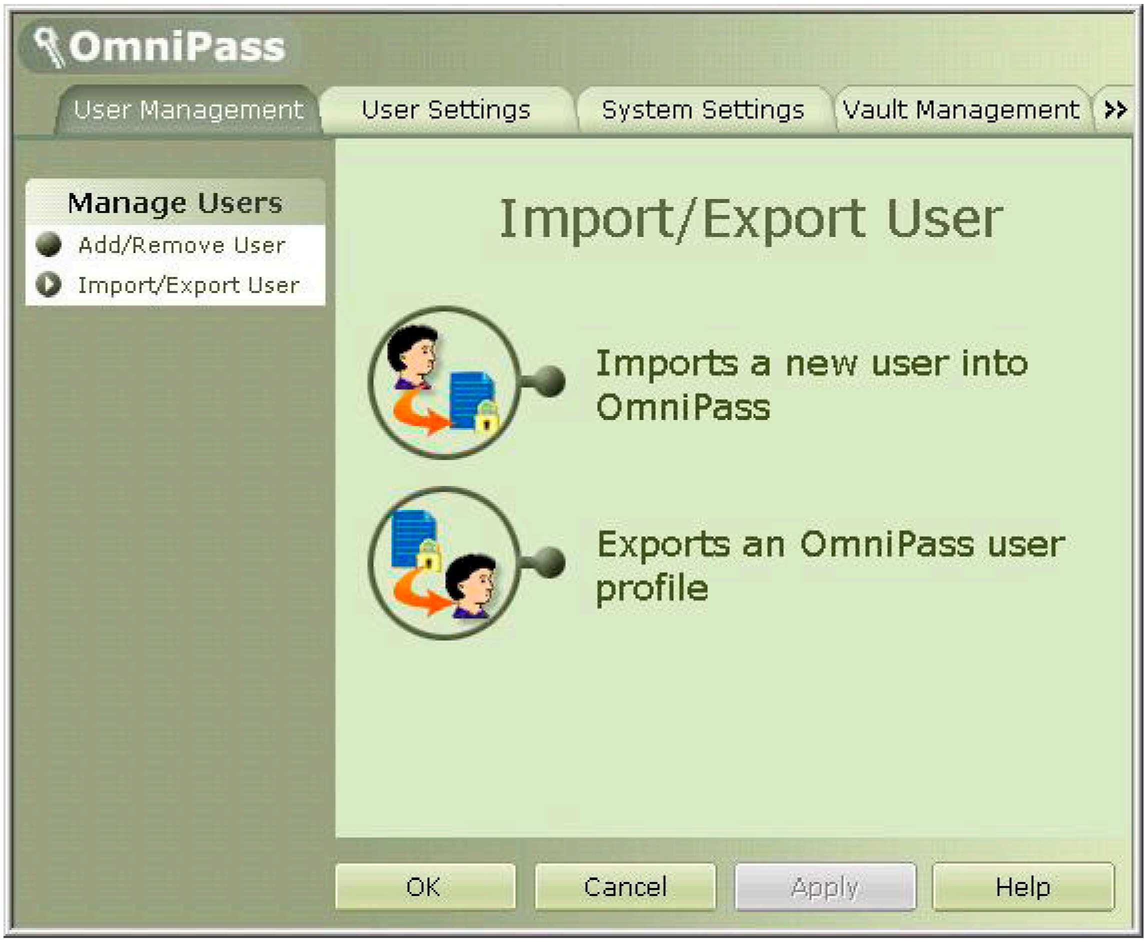


Figure 40: Import/Export User

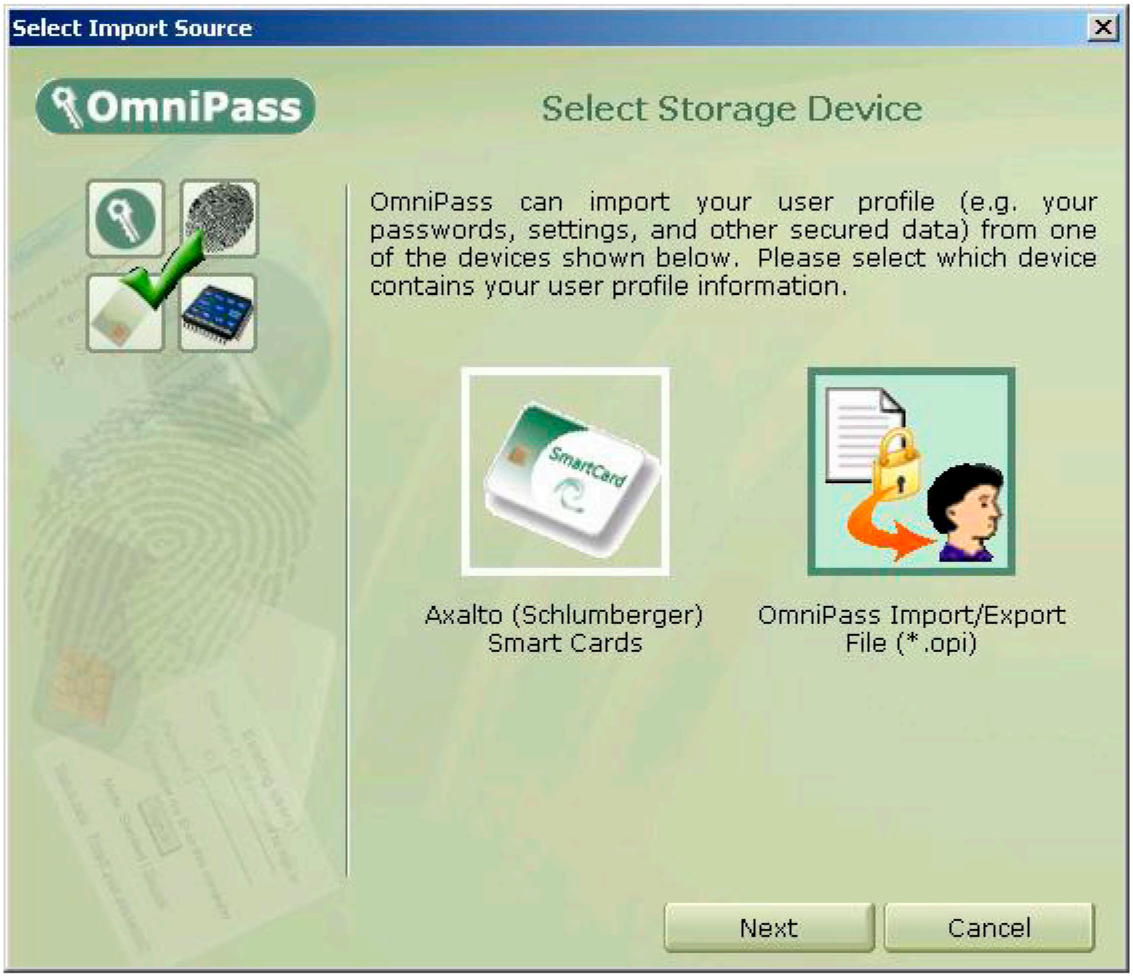
Click **Exports an OmniPass user profile**. OmniPass will prompt you to authenticate. Upon successfully authentication, you must name the OmniPass user profile and decide where to save it. An .opi file is generated, and you should store a copy of it in a safe place.

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 (see Figure 41).



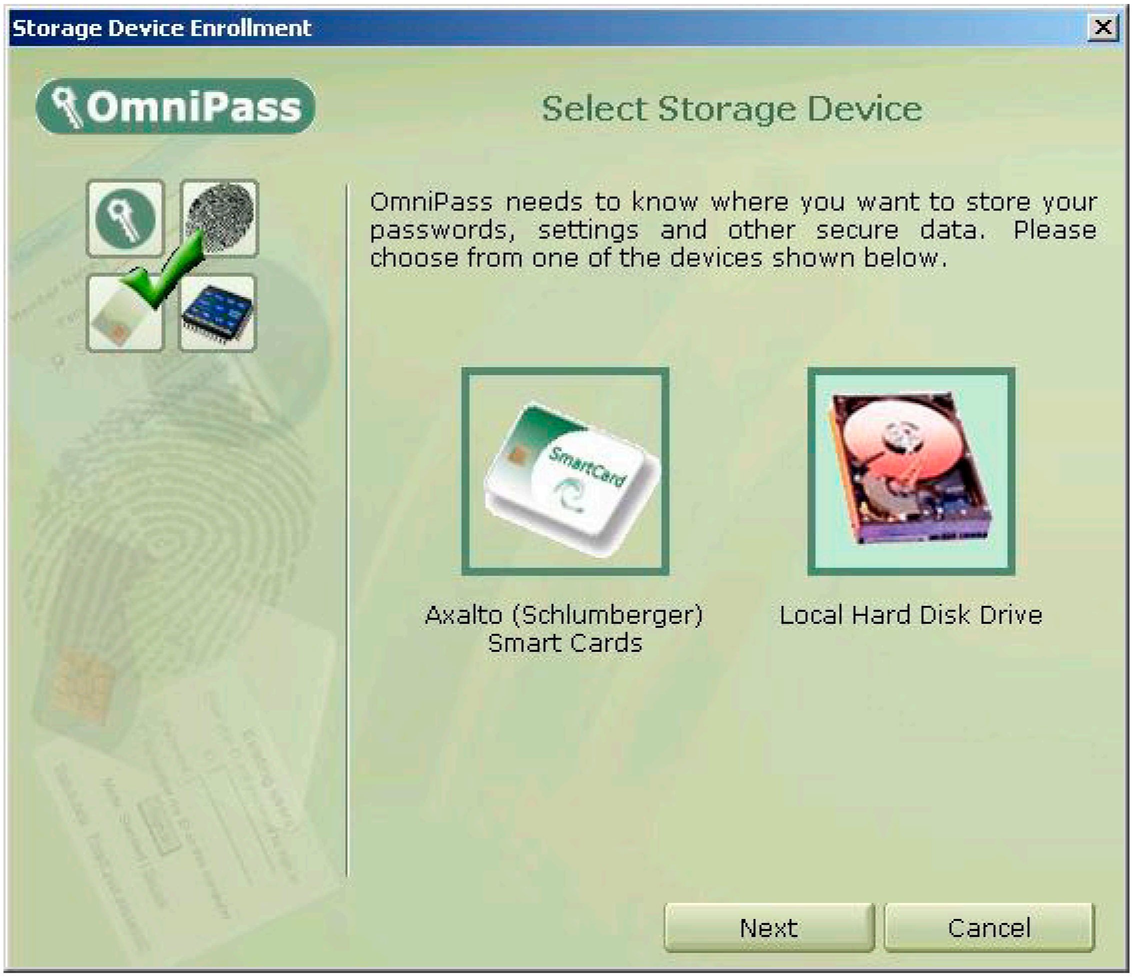
OmniPass can import your user profile (e.g. your passwords, settings, and other secured data) from one of the devices shown below. Please select which device contains your user profile information.

Select Import Source
OmniPass
Select Storage Device
SmartCard
Axalto (Schlumberger) Smart Cards
OmniPass Import/Export File (*.opi)
Next
Cancel

Figure 41: Import User Profile - Select Storage Device (Source)

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 (see Figure 42).



OmniPass needs to know where you want to store your passwords, settings and other secure data. Please choose from one of the devices shown below.

Figure 42: Import User Profile - Select Storage Device (Target)

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

5.3 Things to Know Regarding Import/Export

- Assume you export a local Windows User profile from OmniPass, and 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 3.5 – 3.7* 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

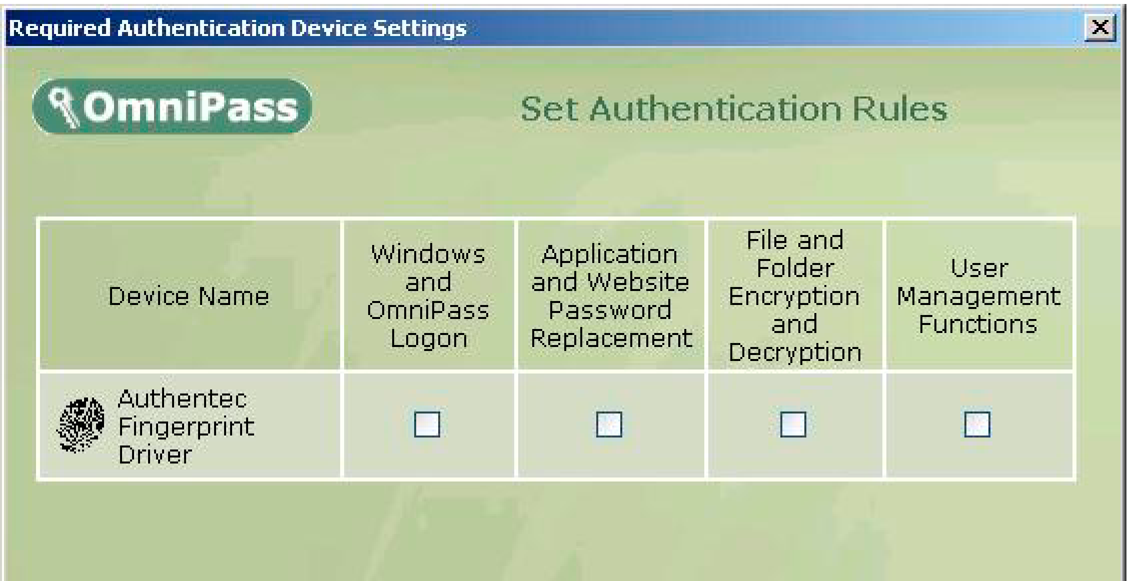
The User Settings tab has four interfaces: **Audio Settings**, **Taskbar Tips**, **Encrypt/Decrypt**, and **Enrollment**. User settings allow users to customize OmniPass to suit their individual preferences.

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 Certifcate. If it is removed from the system, you will not be able to recover any of the encrypted files!

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 (see Figure 43).



Required Authentication Device Settings

Set Authentication Rules

Device Name	Windows and OmniPass Logon	Application and Website Password Replacement	File and Folder Encryption and Decryption	User Management Functions
Authentec Fingerprint Driver	□	□	□	□

Figure 43: User Settings - Set Authentication Rules

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.

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

OmniPass startup options can be found in the System Settings tab. With these options you can specify how your OmniPass Logon is tied to your Windows Logon.

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

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

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

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

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 Files(s)**, those OmniPass functions are available to you. Encryption and decryption will occur upon successful authentication.

6.5 About

The About tab displays version information about OmniPass. If you click **Check For Updates** then the Softex Weblink application will launch.

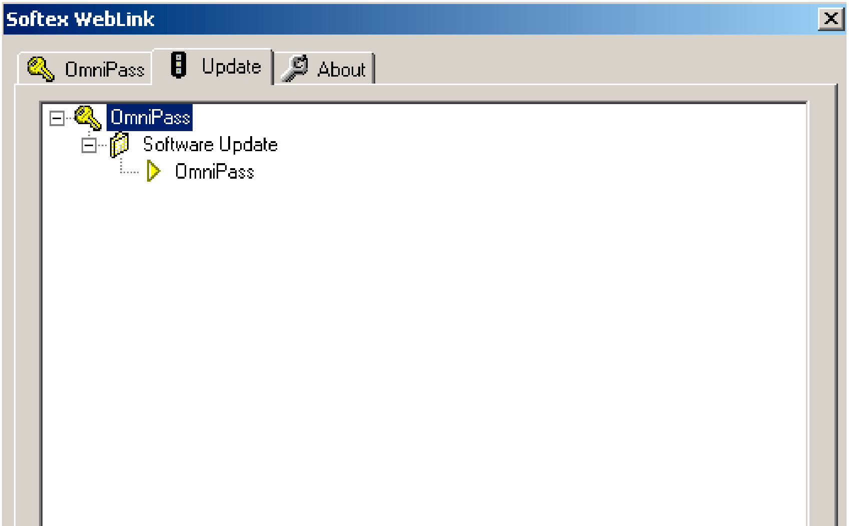


Figure 44: Softex Weblink

The OmniPass tab of the Weblink application allows you to configure how Weblink keeps OmniPass up to date.

To download an OmniPass update once you have been notified:

1. Go to the Update tab and double-click the update (see Figure 44).

   Or

   Select the OmniPass update and click the **Start Download** button on the right of the **Update Summary** section of the Weblink control panel.

2. Wait for the download to complete, as shown by the download progress bar. The **Start Download** button will become the **Install** button.

3. Click the **Install** button to extract the update and run the installation program. During file extraction make sure **When Done Unzipping Run:** is checked and click **Unzip**.

   Or

   Let us say that you do not want to install the update, and you do not want Weblink always notifying you of an update you never plan to install. Click the Update tab, select the OmniPass update and click the **Remove Update** button. This will delete the update downloaded by Weblink; OmniPass will not be updated.

Appendix A: Troubleshooting

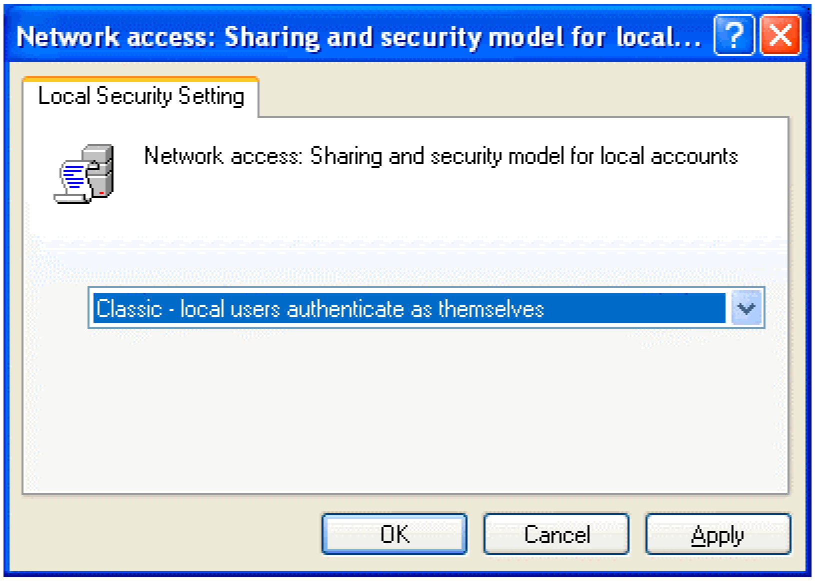
Most major problems can be avoided by paying special attention to the NOTES and WARNINGS distributed throughout this document. Other common problems are discussed in this appendix. For support not covered in this document contact support@softexinc.com.

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* (see Figure 45).



Network access: Sharing and security model for local accounts

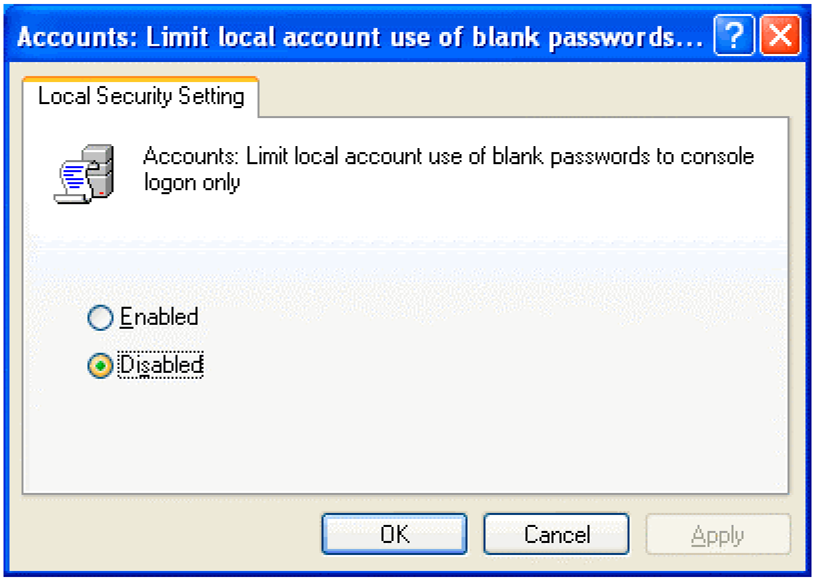
Classic - local users authenticate as themselves

Figure 45: Sharing and security model for local accounts

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 (see Figure 46).


Accounts: Limit local account use of blank passwords...

Local Security Setting

Accounts: Limit local account use of blank passwords to console logon only

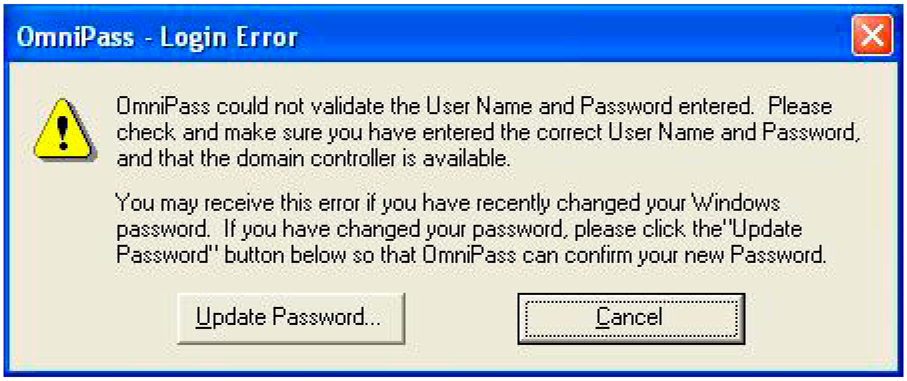
○ Enabled

● Disabled

Figure 46: Limit local account use of blank passwords ...

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 (see Figure 47).


OmniPass - Login Error

OmniPass could not validate the User Name and Password entered. Please check and make sure you have entered the correct User Name and Password, and that the domain controller is available.

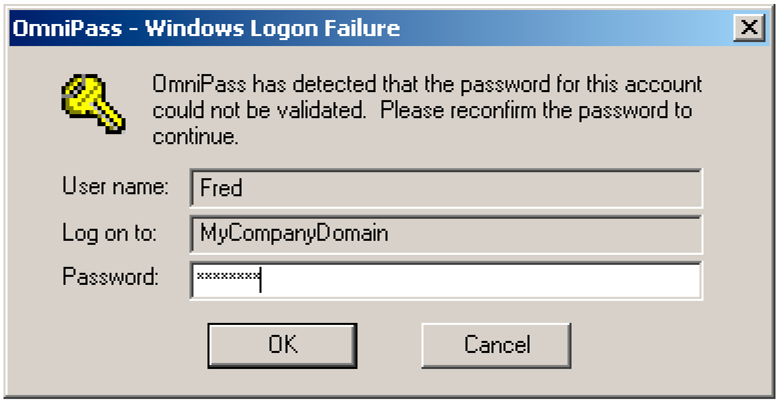
You may receive this error if you have recently changed your Windows password. If you have changed your password, please click the "Update Password" button below so that OmniPass can confirm your new Password.

Figure 47: OmniPass/Windows Login Error

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
- You 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 (see Figure 48).



OmniPass - Windows Logon Failure

OmniPass has detected that the password for this account could not be validated. Please reconfirm the password to continue.

User name: Fred

Log on to: MyCompanyDomain

Password: ********

Figure 48: OmniPass Reconfirm 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.

Index