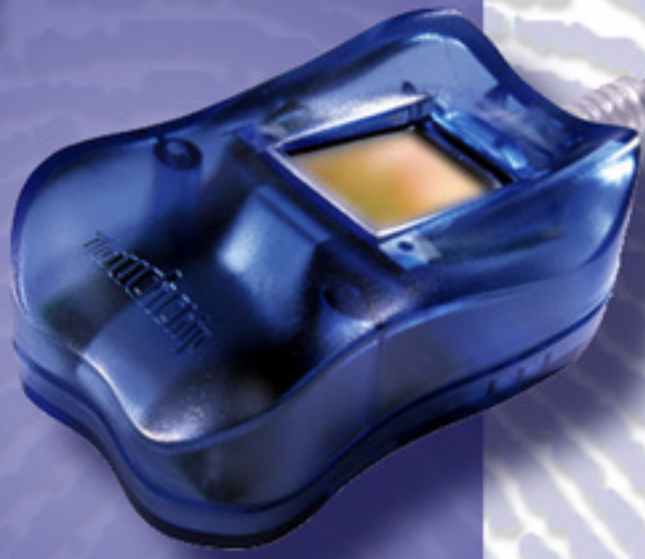
PROTECTOR SUITE



Quick Start Guide

version 4.1

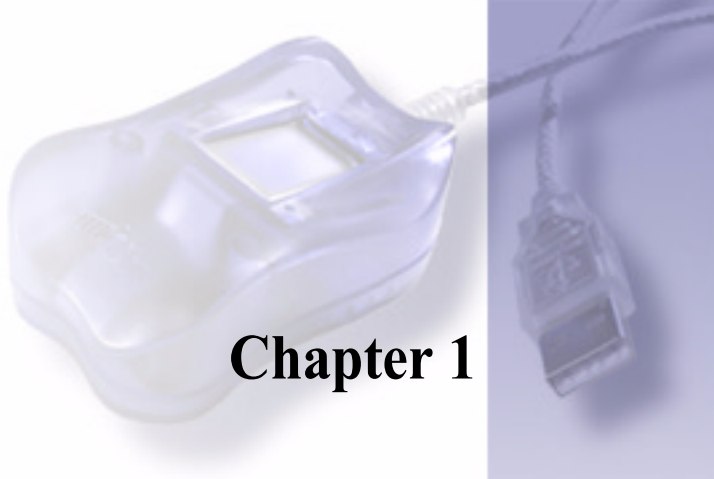
TouchChip

Copyright Notice and Proprietary Information

Trademarks

TouchChip, Protector Suite, Logon Protector, Filedisk Protector, Password Protector, PKI Protector, Web Protector, and Wizard Manager are trademarks of STMicroelectronics. All other products described in this publication are trademarks of their respective holders and should be treated as such.

Contents



Chapter 1

Overview

Protector Suite is a sophisticated software solution designed for computer security. This product provides a high level of user convenience and gives you a set of powerful tools for securing your computer and protecting your private data.

Logon Protector

FileDisk Protector

Password Protector

Control Center

Authentication Hardware

Logon Protector

Logon Protector secures access to your computer and simplifies the logon process by making it extremely easy and convenient. Put your finger on the sensor and access is granted. Nobody can imitate your fingerprints. If you want to leave your workplace, use the secure screensaver option to automatically lock your unattended system. When you return, simply put your finger on the sensor again, and you will be in.

FileDisk Protector

You certainly do not want to expose your data to anybody. Your hard disk may contain your private mail, your personal, financial, and other sensitive data. FileDisk Protector helps you to create special files which are stored in an encrypted form. Access to the stored data is granted only after your identity is verified using your fingerprint.

Password Protector

It is so boring to remember many passwords for various applications. Maybe you tried to use only one password for all of the programs. But this practice is unsecure. So how do you avoid this problem? Your user credentials can be entered automatically just by putting your finger on the scanner.

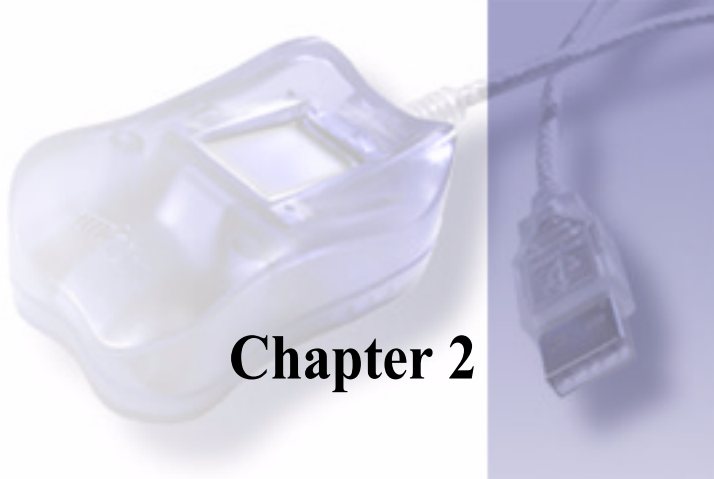
Control Center

All the security features of Protector Suite can be easily used and set from the common user interface. The Control Center is an access point to all the necessary information, it includes wizards which will help you to complete all the required steps.

Authentication Hardware

To get all the benefits of Protector Suite in the most convenient way, you will need a fingerprint reader. STMicroelectronics offers you TouchChip silicon sensor which can be integrated in notebooks, hanheld devices, or PC peripherals.

The TouchChip reader built around the TouchChip sensor is used to enter fingerprints. This device looks much like a computer mouse, but, instead of having mouse buttons, it has a touch-sensitive pad. When prompted during log-on or when accessing password-protected applications or data, the user places a finger on the pad of the reader. An image of the fingerprint is generated and characteristic properties are extracted. A matrix of unique fingerprint minutia is created and then compared to a storted template of that fingerprint.



Chapter 2

Installation

Protector Suite 4.1 brings you both the authentication hardware - typically a TouchChip fingerprint reader - and the Protector Suite software. The installation CD contains a Readme.txt file with information about the latest changes to the product. To find hints and tips for installation and usage of various authentication hardware, check the Readme.txt file located in the Biometry directory on your installation CD.

NOTE: *Drivers for your authentication hardware will be installed during the Protector Suite installation. It is not necessary to install them separately.*

Software Installation

Software Installation

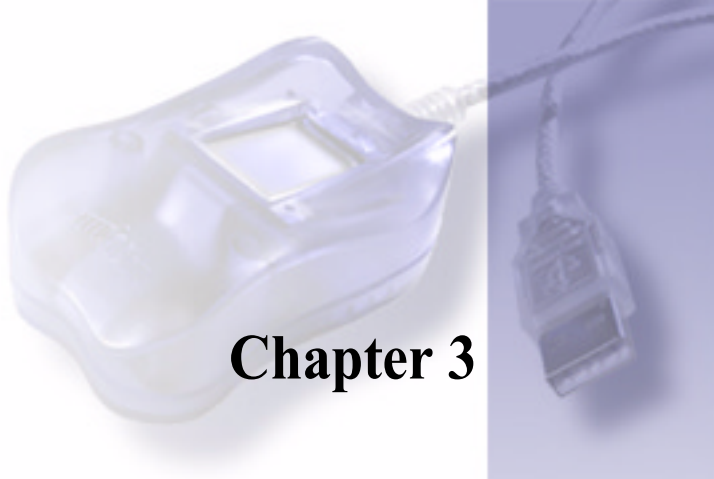
The Protector Suite installation program will guide you through all the steps necessary to successfully install the included applications and necessary hardware support.

TouchChip Protector Suite can be installed on Windows 98/ME/NT/2000. It was successfully pre-tested with Windows XP Beta 2. TouchChip authentication hardware requires special third-party USB support on Windows NT.

Only administrators can install the TouchChip Protector Suite.

To Install Protector Suite

1. *Insert your installation CD into the CD-ROM drive. If Autorun is enabled, setup will begin automatically, if Autorun is not active, run Setup.exe manually.*
2. *The Welcome dialog is displayed. Click **Next** to continue.*
3. *The License Agreement is displayed. Read it carefully and accept it by selecting the corresponding radio button. (If you do not agree to the license agreement, you cannot install the product. Click **Cancel** to close the installation.)*
4. *The User Information dialog is displayed. Enter your name and organization (if applicable). Click **Next** to continue.*
5. *Select the installation directory or confirm the default directory.*
6. *The installation process can begin. Click the **Next** button to start copying files.*
7. *The next step is hardware setup. Setup tries to detect the reader. A message box is displayed if it is necessary to attach or re-attach your reader.*
8. *You will be prompted to reboot your computer.*
9. *Your installation is finished. After reboot, the logon dialog is displayed. All the necessary procedures are described in the following chapters.*



Chapter 3

First Steps

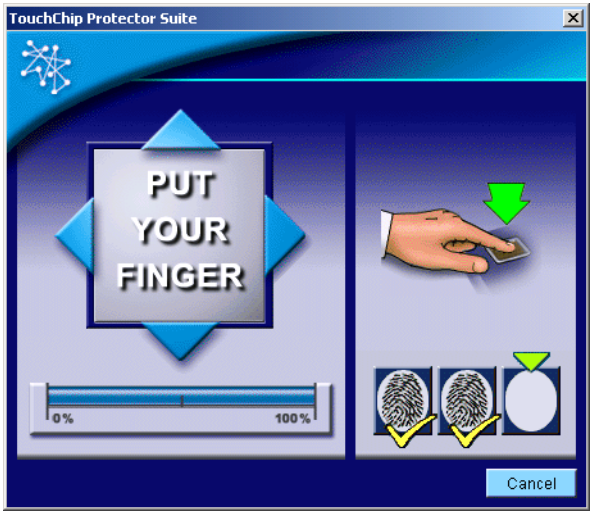
This chapter describes your first steps after you have installed Protector Suite and restarted your computer.

First Logon

You have just finished Protector Suite installation. A safe screen is displayed on your computer. A dialog is displayed asking you either to put your finger on the sensor, or to logon using the standard Microsoft logon procedure.

Put your finger on the sensor. If it is your first logon after the first installation, no user is enrolled yet. A message box is displayed warning that there are no existing passports in Protector Suite. You must first create your passport. Click the **Enroll** button in the message box and continue.

1. *A User Enrollment dialog is displayed. Enter your user ID. Each user ID must be unique in the Protector Suite installation. Enter your backup password. This password can be used for logon in case of authentication hardware failure. Click **Next** to continue.*
2. *A dialog woth hands is displayed. Select a finger to be enrolled. You can either click its picture, or select in the combo box. Click the **Enroll** button.*
3. *The User Enrollment dialog now displays a fingerprint enrollment part. You must create three samples of the selected finger. These three samples are combined into one fingerprint template. Animated display graphics will guide you through the enrollment procedure.*



Simply put your finger on the scanner, wait until the yellow checkmark is displayed on the fingerprint display and then remove your finger from the scanner

4 *After fingerprint enrollment, the window with hands is displayed again. You can select more fingers to be enrolled, or click the* ***Next*** *button to continue user enrollment. You can enroll up to ten fingers. However, two passports cannot include the same finger.*

5 *Encryption keys will be generated.*

6 *You will be asked to enter your Windows credentials. This data will be stored in the passport and the next time, your fingerprint will perform the whole logon procedure.*

Control Center

After you first logon, the Control Center is displayed. The Control Center is a common user interface for all the Protector Suite components. Use it to get basic information and to access various functions. Control Center pages allow you to switch between a text view and a wizard view. The wizard view lists all the wizards for the corresponding component. For the list of all wizards, see the next chapter.

To Start Using the Control Center

1 *Select* ***Start - Programs - Protector Suite****.*

2 *The* ***Control Center*** *window is displayed. By default, the text view of the* ***Welcome*** *page is displayed.*

3 *The left part of the window contains the list of groups. Clicking a group displays a corresponding page in the right pane. If it is your first acccess to the group, the text view is displayed. Later the displayed view depends on the last used page.*

Creating FileDisks

Protector Suite enables storing your sensitive information in a secure, encrypted form. If you want to use this feature, you need to create a FileDisk host file and mount it as a disk drive.

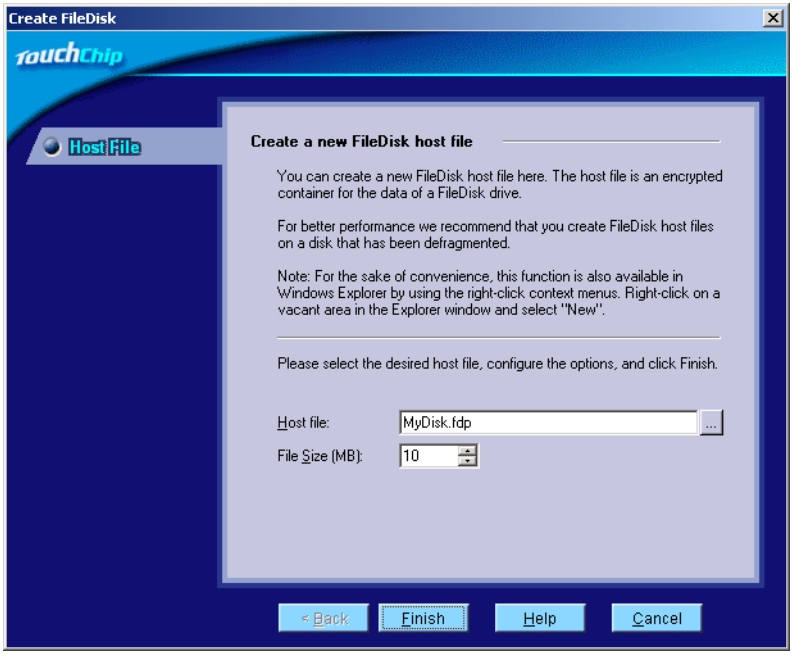
To create your first FileDisk

1 *Click the **FileDisk** group. Switch to the wizard view, if it is not displayed.*

2 *Click the **Create FileDisk** wizard.*

3 *The **Create New FileDisk** dialog is displayed. Select a host file name (.fdp extension is added automatically), size, and encryption type. You can use the default settings. To learn more about these items, see*

*"FileDisk Protector" on page 19, or consult the online help. Click **OK** to continue.*



4 *A newly created FileDisk host file must be mounted as a disk drive and formatted for the file system of your computer. Select the drive letter. You can also decide whether you want to mount this file automatically on computer startup. Click **OK** to continue.*

5 *Select the file system type. Click **OK** to perform formatting.*

TIP: *A FileDisk host file can be created from the Windows Explorer. This procedure is described on page 26. For more information about FileDisk, see the online help system.*

The newly created, mounted and formatted FileDisk can be used in the same way as your normal disk drive. It will appear as a Removable Disk. Data stored on the FileDisk is not accessible without successful identity verification..

WARNING: FileDisk can be accessed only using the corresponding passport. If you delete the passport for which FileDisk was created or if you uninstall the whole Protector Suite, you data stored on the FileDisk is lost.

Registering Windows

Password Protector allows you to securely store your passwords for various applications including web accounts. Registered information can be filled in a window automatically. To enable this process, you need to register the window.

To register a window:

1 *Click the **Password** group.*

2 *Start Password Protector.*
*Click the corresponding link in the text view, or click the **Start** wizard on the Password Protector page (wizard view).*
Password Protector is not started after installation. Running Password Protector is indicated by the key icon in the taskbar.

3 *Click the key icon in the taskbar.*

Select the mode of registration.
***Automatic** mode allows automatic replaying of stored information into the dialog. However, this mode does not work correctly for complex dialogs (e.g. web pages) with context-sensitive items.*
***Manual** mode is recommended for complex dialogs with a lot of items. However, replaying registration must be initialized manually.*
***One-field** mode is intended for simple dialogs with only one item - a password.*

4 *Click the window you want to register. Possible windows are indicated by a red frame. Fill in the necessary fileds. Use mouse to position cursor to the first field. Do not use the mouse during registration process (use Tab key instead). The next mouse-click closes the registration process.*

5 *Select a name for your registration or confirm the default one.*

Recorded information is stored in a secure form inaccessible to users. Registration can be replayed only after successful verification..

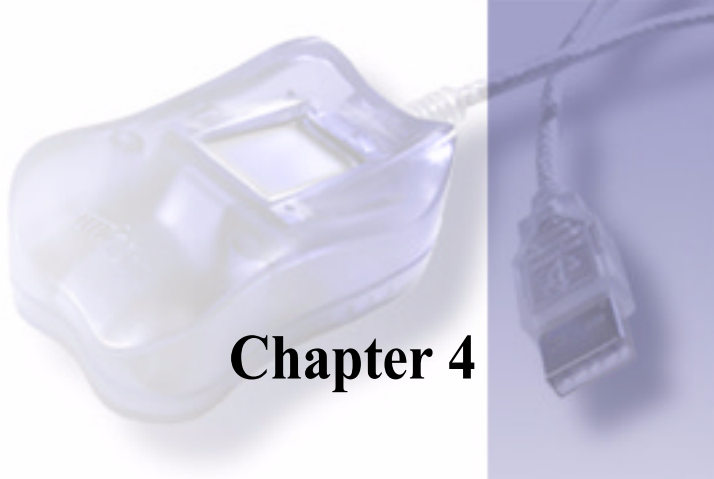
WARNING: Registration of a window in Password Protector can be replayed only using the corresponding passport. If you delete the passport for which the window was registered, or if you uninstall the whole Protector Suite, you registrations are lost.

To replay registration:

1 *The registered window is displayed.*

2 *Registrations in **Automatic** mode are replayed automatically if **Auto Replay** is enabled..*
*Replaying registrations in **Manual** and **One-field** modes (and also registrations in Automatic mode if Auto Replay is disabled) must be initiated manually by pressing the shortcut key. The default shortcut is Ctrl+F9.*

For more information about Password Protector, see page 29 and online help system.



Chapter 4

Components and Procedures

This chapter describes Protector Suite procedures and functions.

Logging on to the System

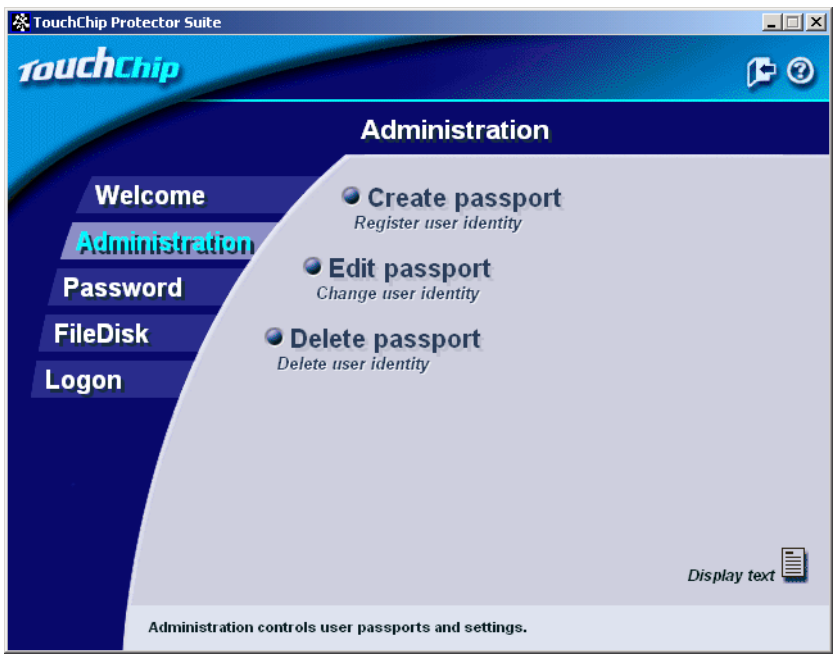
A Safe screen is displayed on your computer. A dialog is displayed asking you either to put your finger on the sensor, or to logon using the standard Microsoft logon procedure.

Put your finger on the sensor. After successful verification, you will be logged on. You can also use standard Windows logon. Use Ctrl+Alt+Del combination (Ctrl+Alt+End on Windows 98).

(If it is your first logon after the first installation, no user is enrolled yet. A message box is displayed warning that there are no existing passports in Protector Suite. You must first create your passport. Click the **Enroll** button in the message box and continue.)

Control Center

Most of the Protector Suite settings and actions are performed from the Control Center. This window can also serve as a source of information and an access point to the online help system.



To start the Control Center

1 *Select **Start - Programs - Protector Suite**.*

The Control Center window consists of the list of groups in the left part and pages in the right pane. Clicking a group displays the corresponding page. Pages contain necessary information and wizards which will guide you through necessary steps for the selected procedure. The following table lists all available groups and possible actions.

Group	Description
Welcome	Basic information about the product. Use this group to access the help system.
Administration	User and token administration. You can add or delete a user, enroll your fingerprints.
Password	Password Protector settings.
FileDisk	Management of your FileDisks. Use this group to create, mount, and dismount your FileDisks.
Logon	Settings for Logon Protector. This group contains wizards for enabling Logon Protector, setting the screensaver protection etc.

All the wizards including detailed procedures are listed later in this chapter.

Administration

This group contains wizards for enrolling, editing and deleting passports, setting verification level, and fingerprint peripheral settings.

User identity in Protector Suite is represented by a passport. The passport is a combination of user ID and user's fingerprints. One physical user can have several passports. As Protector Suite performs biometric identification, you **cannot have two passports created with the same fingerprint**. Passports are accessed during the verification procedure.

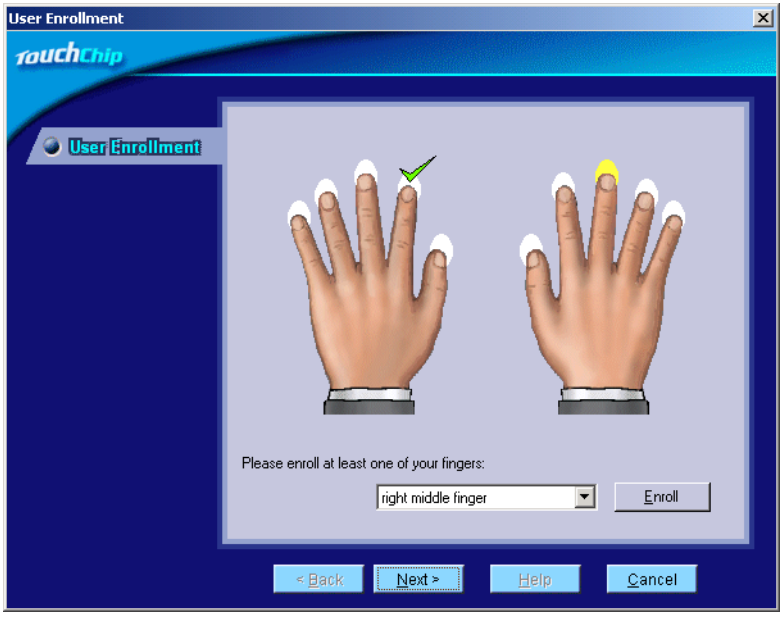
To enroll a new passport:

1 *Switch to the wizard view, if it is not displayed.*

2 *Click the **Create passport** wizard.*

3 *A User Enrollment dialog is displayed. Enter your user ID. Each user ID must be unique in the Protector Suite installation.*

4 *Select a finger to be enrolled. You can either click its picture, or select in the combo box.*



*Click the **Enroll** button.The **User Enrollment** dialog now displays a fingerprint enrollment part. Enroll the selected finger.*

5 *The User Enrollment dialog now displays a fingerprint enrollment part. You must create three samples of the selected finger. These three samples are combined into one fingerprint template. Animated display graphics will guide you through the enrollment procedure. Simply put your finger on the scanner, wait until the yellow checkmark is displayed on the fingerprint display and then remove your finger from the scanner*

6 *After fingerprint enrollment, the window with hands is displayed again. You can select more fingers to be enrolled, or click the **Finish** button to finish user enrollment. You can enroll up to ten fingers. However, two passports cannot include the same finger.*

7 *Encryption keys will be generated.*

8 *A new user was enrolled.*

9 *During the first logon using the newly created passport, the user will be asked to enter his/her Windows credentials.*

To add a new fingerprint to your passport:

1 *Switch to the wizard view, if it is not displayed.*

2 *Click the **Edit passport** wizard. User identification is performed.*

3 *A **User Enrollment** dialog is displayed. Your user ID si pre-filled and cannot be changed. Select a finger to be enrolled. You can either click its picture, or select in the combo box. Click the **Enroll** button.*

4 *The **User Enrollment** dialog now displays a fingerprint enrollment part. Enroll the selected finger.*

5 *After fingerprint enrollment, the window with hands is displayed again. You can select more fingers to be enrolled, or click the **Finish** button to finish the editing.*

To delete an existing passport:

1 *Switch to the wizard view, if it is not displayed.*

2 *Click the **Delete passport** wizard.*

3 *(Only administrator can delete passports of other users. A standard user can delete only his own passport after identification process.)*

4 *A list of existing passports is displayed. Select the passport(s) you want to delete. Click the **Next** button to continue.*

5 *A list of selected passports is displayed. Confirm the operation by pressing the **Finish** button.*

Logon Protector

Logon Protector secures access to your computer.

Logon Protector also protects your password protected Windows screen saver. If you leave your workplace and a screen saver appears on your screen, nobody can access your computer without successful identification. If you want to use the screen saver protection, you must set a password

protected screen saver in Windows. Select **Start - Settings - Control Panel - Display** and select the **Screen Saver** tab. Set the screen saver and check the **Password protected** check box.

Logon Protector can provide verification information to other applications (FileDisk Protector and Password Protector in this version). This feature is called Unilogon. Unilogon must be enabled per application. This process is described later for each application.

Logon Page

This page contains three wizards - **Logon settings** for global Logon settings, **Personal settings** for options valid for the current user, and **Protected screen saver** for setting secure screen saver.

Global Logon Protector settings include enabling and disabling Logon Protector and enabling and disabling graphics and animations during logon.

If you disable Logon, no fingerprints will be used during logon to your computer. Standard Microsoft logon procedure will be performed instead.

A Safe screen is normally displayed during logon process with animations on successful logon. These graphics can be disabled. You can disable animations, or the whole background picture.

To set global Logon Protector settings:

1 *Switch to the wizard view, if it is not displayed.*

2 *Click the **Logon settings** wizard.*

3 *Select or clear the corresponding check box.*

4 *Click **Finish** to close the wizard. Enabling/disabling Logon Protector requires reboot.*

Personal settings allow you to use the same passport even if your Windows credentials (e.g. password) are changed. If you click the **Unsave Windows password** button, you will be able to change your password or other user data during your next logon.

To set personal Logon Protector settings:

1 *Switch to the wizard view, if it is not displayed.*

2 *Click the **Personal settings** wizard.*

3 *To allow changing your Windows credentials during your next logon, click the **Unsave Windows password** button.*

4 *Click the **Finish** button to close the wizard.*

Logon Protector secures also your screen saver. To enable this feature, Password protected option must be set in screen saver options in Windows. This wizard displays standard Windows dialog for settings options for your screen saver.

To set protected screen saver:

1 *Switch to the wizard view, if it is not displayed.*

2 *Click the **Protected screen saver** wizard.*

3 *If you want to review or change settings for your screen saver, check the **Run system display properties on Finish** check box and click the **Finish** button.*

FileDisk Protector

FileDisk Protector enables storing your sensitive data in an encrypted form in special host files. These host files are accessible only after mounting as disk drives. Access to your FileDisk is allowed only after successful verification.

WARNING: FileDisk can be accessed only using the corresponding passport. If you delete the passport for which FileDisk was created or if you uninstall the whole Protector Suite, you data stored on the FileDisk is lost.

To create a FileDisk host file, you can use two procedures. FileDisks can be created from the Control Center, of from the Windows Explorer.

To create a FileDisk from the Control Center:

1 *Switch to the wizard view, if it is not displayed.*

2 *Click the **Create FileDisk** wizard.*

3 *Select the host file name and size. FileDisk host files have extension .fdp and they are by default created in the My Documents folder. For more information about possible FileDisk size, see the online help system.*

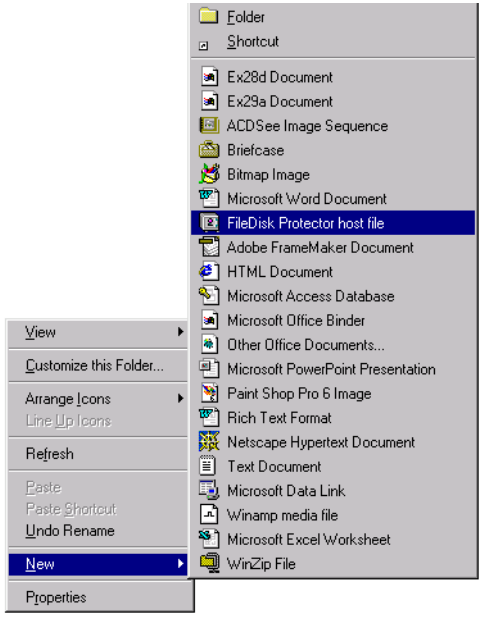
4 *Click the **Next** button to continue. The verification procedure is carried out.*

5 *After creating a new FileDisk host file, you must mount it as a disk drive and format it. Select the drive name (default names are Z:, Y:,...) and select whether you want to mount this drive automatically after logon. For formatting, select your file system.*

To create a FileDisk from Microsoft Explorer:

1 *Right-click the free space in the right pane of Microsoft Explorer to display the context menu.*

2 *Select **New - FileDisk Protector** host file. Continue as described above.*



An already existing host file must be mounted before it can be used. You can select an option for autmatic mount on logon when creating the FileDisk. The mounting procedure can be initiated from the Control Center, or from Microsoft Explorer.

To mount a FileDisk host file from the Control Center:

1. *Switch to the wizard view, if it is not displayed.*
2. *Click the **Mount FileDisk** wizard.*
3. *Select the host file name. Its size and encryption type are automatically displayed.*
4. *Select the drive name. You can select check boxes for Read-only disk and for automatic mount on logon.*
5. *Click the **Finish** button. After the verification procedure, your FileDisk will be mounted.*

To mount a FileDisk host file from Microsoft Explorer:

1. *Display the contents of the folder containing your FileDisk host file in Microsoft Explorer.*
2. *Right-click the host file.*
3. *Select **Mount/Dismount**.*
4. *Select the host file name. Its size and encryption type are automatically displayed.*
5. *Select the drive name. You can select check boxes for Read-only disk and for automatic mount on logon.*
6. *Click the **Finish** button. After the verification procedure, your FileDisk will be mounted.*

After you finish your work with FileDisk, you would probably want to dismount it (and this way to make it inaccessbile to other users). this procedure can be carried out from the Control Center or from Microsoft Explorer.

FileDisk host files are dismounted automatically on logoff. For more information about the behaviour of FileDisks in use at logoff, see online help.

To dismount a FileDisk from the Control Center:

1 *Switch to the wizard view, if it is not displayed.*

2 *Click the **Dismount FileDisk** wizard.*

3 *Select the FileDisk drive you want to dismount. You can select whether you want to mount the drive automatically on logon.*

4 *Click the **Finish** button.*

To dismount a FileDisk from Microsoft Explorer:

1 *Display the contents of the folder with your FileDisk host file in Microsoft Explorer.*

2 *Right-click the host file.*

3 *Select **Mount/Dismount**.*

4 *Select the FileDisk drive you want to dismount. You can select whether you want to mount the drive automatically on logon.*

5 *Click the **Finish** button.*

Your FileDisks are protected by your fingerprint. To access it, a verification procedure must be performed. If you do not want to perform the authentication procedure whenever you want to mount your FileDisk, you can use UniLogon. UniLogon is a single sign-on function which allows using logon information by other components of Protector Suite.

WARNING: Logon Protector must be enabled if you want to use UniLogon.

To enable UniLogon for FileDisk Protector:

1 *Display the Control Center.*

2 *Switch to the wizard view, if it is not displayed.*

3 *Click the FileDisk settings wizard.*

4 *Select desired options. You can set UniLogon for automatic mounting, manual mounting, and for creating FileDisks.*

5 *Click the **Finish** button.*

Password Protector

Password Protector learns your passwords and other data which you repetitively fill in various dialog. It can later enter them automatically.

The active status of Password Protector is indicated by a yellow key icon in the taskbar. Click this icon to start registration of a window (see page 11). Right-click this icon to display Password Protector menu.

To run Password Protector:

Select one of the following procedures:

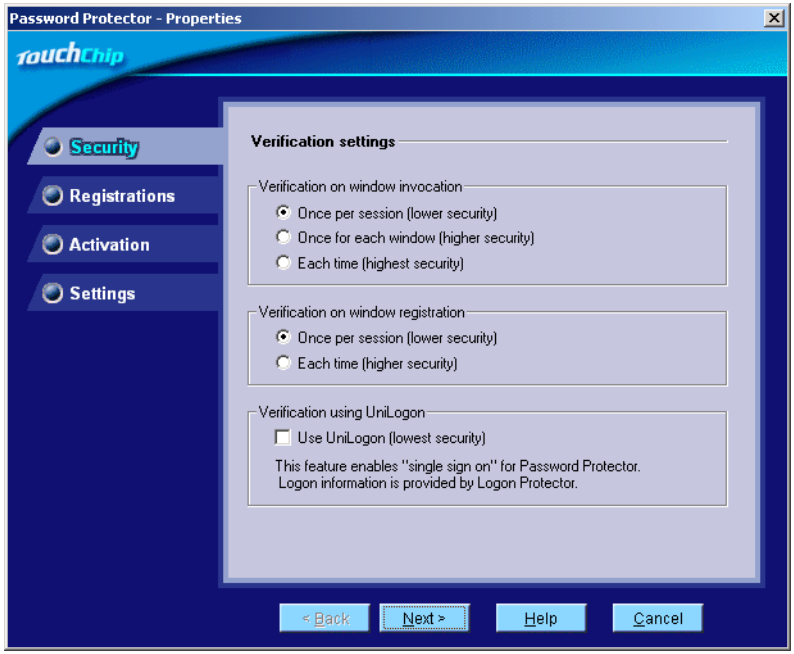
- *Click the **Start Password Protector** link in the text view of the Control Center (Password group).*
- *Click the **Start** wizard in the wizard view of the Control Center (Password group).*

To run Password Protector automatically on startup:

Select one of the following procedures:

- *Select the **Run at startup** check box in the text view of the Control Center (Password group).*
- *Click the **Properties** wizard in the wizard view of the Control Center (Password group). Go to the **Settings** page and select the corresponding check box.*
- *If the Password Protector is running, right-click the key icon in the taskbar and select **Properties**. Go to the **Settings** page and check the appropriate check box.*

Password Protector protects your registrations and used data by your fingerprint. To create and replay a window registration, a verification procedure must be performed. If you do not want to perform the authentication procedure whenever you use some Password Protector function, you can use UniLogon. UniLogon is a single sign-on function which allows using logon information by other components of Protector Suite.



To use UniLogon for Password Protector:

1 *Click the **Properties** wizard in the wizard view of the Control Center (Password group).*
or
*If the Password Protector is running, right-click the key icon in the taskbar and select **Properties**.*

2 *Go to the **Security** dialog/tab.*

3 *Select **Use UniLogon** check box.*

If you select UniLogon, other settings are not accessible. If you do not want to use UniLogon, you can decide how often verification process should be performed..

WARNING: Logon Protector must be enabled if you want to use UniLogon.

A list of all your existing registrations of windows is displayed in the Registrations dialog.

To set options for activation of registrations:

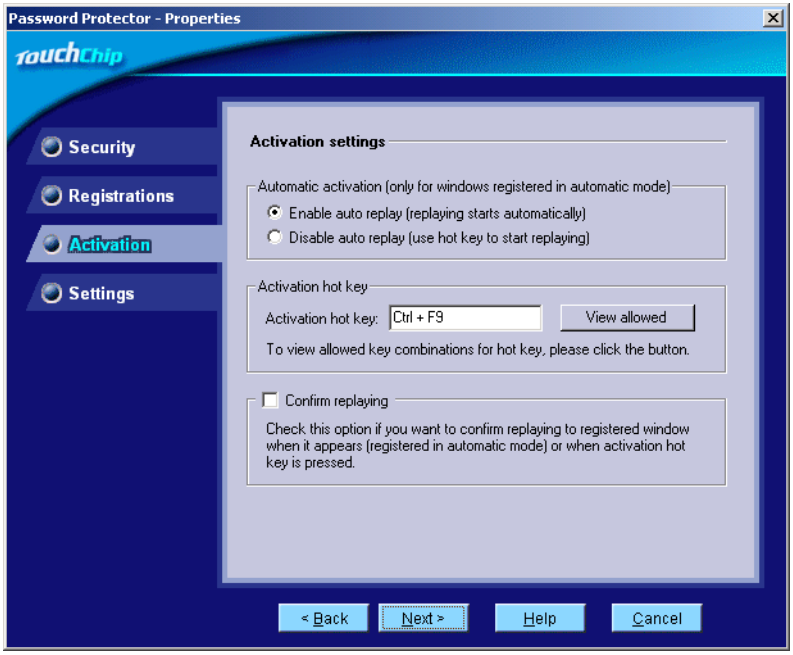
1 *Click the **Properties** wizard in the wizard view of the Control Center (Password group).*
or
*If the Password Protector is running, right-click the key icon in the taskbar and select **Properties**.*

2 *Go to the **Activation** dialog/tab.*

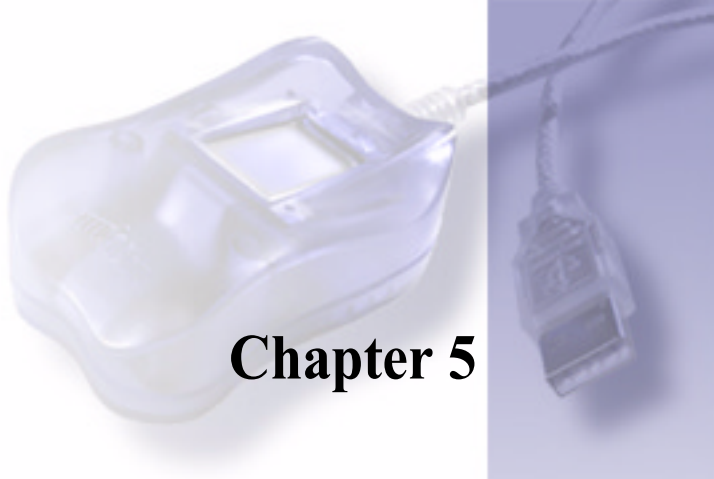
3 *Enable or disable automatic replaying of registrations in automatic mode.*

4 *Select the activation hot key used for replaying registrations in manual and one-field modes.*

5 *Select whether you want to display confirmation when replaying registrations.*



The process of registering a window and replaying an existing registration is described on page 16. Password Protector must be started (yellow key icon in the taskbar).



Chapter 5

Hardware Maintenance

This chapter describes TouchChip hardware and the most common maintenance procedures.

WARNING - Use a shielded power cord to connect AC power to the host computer.

CAUTION - No operator-serviceable parts inside unit.

Hardware

TouchChip Sensor

TouchChip high performance silicon sensor provides secure and convenient solution for authenticating the true identity of a person. Since fingerprints cannot be lost, duplicated, stolen or forgotten, the TouchChip product range is widely regarded as providing more reliable results than traditional security devices.

TouchChip Reader

Built on the TouchChip Silicon Fingerprint Sensor, the TouchChip reader is a fast, reliable and inexpensive fingerprint authentication peripheral. It is a revolutionary approach to personal authentication for computer and network security.

The TouchChip reader has been designed for demanding applications such desktop security, network security, commercial verification and identification systems.

Recommended Device Cleaning Procedures

The ultra-hard coating on the surface of the TouchChip sensor provides protection from scratching and abrasion due to normal contact with fingertips and any incidental contact with fingernails. The reader lifetime is expected to be at least 10 years based on extrapolation of accelerated life test data.

Key elements of image quality are the consistency within the actual image and the background of the image. Software algorithms are more accurate and generally faster when the image quality is consistent and the background has not changed dramatically. Dirty residue, oils, or other material on the surface of the TouchChip may obscure the image, leaving parts of the image unrecognizable, or creating false features within the image.

It is recommended that the sensor be visually inspected and periodically cleaned as described in the Periodic Cleaningsection. It is also recommended that before each touch, the sensor be cleaned as described in the User Cleaningsection.

Periodic Cleaning

Dampen a lint-free cloth or cotton swab with alcohol or acetone. Gently rub the cloth across the sensor surface in a left and right direction. Move slowly down the sensor to cover the entire surface area. Repeat this process 4 times. Visually observe that no residual solution remains on the sensor.

After performing the periodic cleaning operation, a surface conditioning is suggested to obtain the maximum performance from the TouchChip sensor. Dampen a lint-free cloth with fragrance-free moisturizing lotion, and gently rub the cloth across the sensor. Make sure that all the lotion will be removed as completion of the cleaning process.

Acid-based fluids, and abrasive materials are not recommended for cleaning the TouchChip.

User Cleaning

Before each authentication, it is recommended that the user simply wipe the sensor with her/his finger, and then position the finger for the authentication. With this action we assure that residue from previous usage will be removed hence giving the best surface conditioning.

For a Class B Digital Device or Peripheral

FCC NOTICE
INFORMATION FOR THE USER

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1) Reorient or relocate the receiving antenna.
2) Increase the separation between the equipment and receiver.
3) Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4) Consult the dealer of an experienced radio/TV technician for help.

The user may find the following publication prepared by the Federal Communications Commission helpful:

"How to Identify and Resolve Radio-TV Interference Problems" (Stock Number 004-000-00345-4).

Available exclusively from the Superintendent of Documents, Government Printing Office, Washington, DC 20402 (telephone 202-512-1800).

FCC WARNING

Changes or modifications not expressly approved by the party responsible for compliance to Part 15 of the FCC Rules could void the user's authority to operate the equipment.

For a Class B or Class 2 Digital Device

CE NOTICE
INFORMATION FOR THE USER

This equipment has been tested and found to comply with the limits for a Class B or Class 2 digital device, pursuant to EN 55022 Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The user may find the following publication prepared by the Federal Communications Commission helpful:

> "How to Identify and Resolve Radio-TV Interference Problems" (Stock Number 004-000-00345-4).

Available exclusively from the Superintendent of Documents, Government Printing Office, Washington, DC 20402 (telephone 202-512-1800).

WARNING

Changes or modifications not expressly approved by the party responsible for compliance to EN 55022 Rules could void the user's authority to operate the equipment.

ICAN Class B Digital Equipment

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

Cet appareil numérique de la classe B respecte toutes les exigences due Réglement sur le matériel brouilleur du Canada.