

PROTECTOR SUITE QL

version 5.4

TouchChip

Copyright Notice and Proprietary Information

Information furnished is believed to be accurate and reliable. However, UPEK[®], Inc assumes no responsibility for the consequences of use of such information not for any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of UPEK, Inc. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. UPEK, Inc's products are not authorized for use as critical components in life support devices or systems without express written approval of UPEK, Inc.

The UPEK logo is a registered trademark of UPEK, Inc.

© 2004-2006 UPEK[®], Inc - All Rights Reserved

All other names are the property of their respective owners.

UPEK[®], Inc

<http://www.uek.com>

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).

Trademarks

TouchChip[®], Protector Suite[™] are trademarks of UPEK, Inc. All other products described in this publication are trademarks of their respective holders and should be treated as such.

A close-up photograph of a person's right index finger pressing down on a circular fingerprint sensor. The sensor is part of a device with a yellow and white grid pattern. The background is a soft, out-of-focus yellow and white.

Chapter 1

Installation

Welcome to Protector Suite QL. This software product is intended for Windows 2000 and Windows XP (with a special support for the Fast User Switching feature). Protector Suite QL introduces biometric fingerprint methods to offer you more user convenience.

Enroll your fingerprint and you will be able to use your finger for:

- *accessing and locking your computer,*
- *displaying and filling in your favorite web pages,*
- *filling in frequently used dialogs,*
- *protecting your sensitive files,*
- *running your favorite applications,*
- *scrolling using your sensor instead of a mouse wheel.*

Installation

Protector Suite QL can be installed on any computer with Windows 2000 or Windows XP Home or Professional edition and a free USB port. Administrator rights are required to install or uninstall Protector Suite QL.

To install Protector Suite QL:

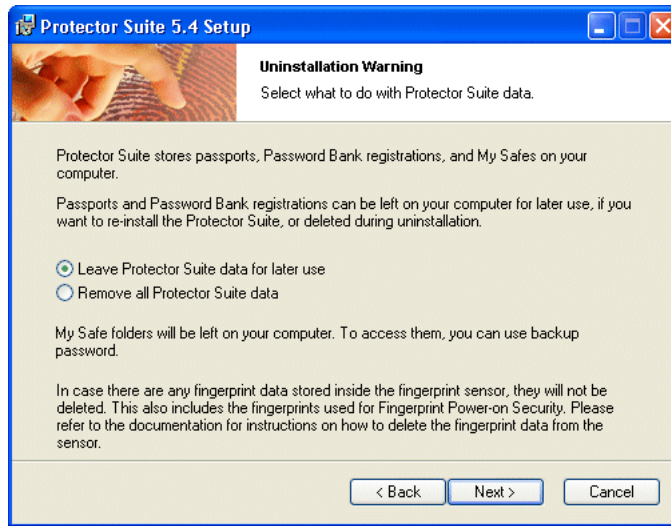
- 1 *Software may be already pre-installed for you. The installation wizard will guide you through the process.*
- 2 *Read and confirm the license agreement. If you do not agree with the license conditions, the installation cannot proceed.*
- 3 *Enter your user name and organization.*
- 4 *Select Protector Suite QL's installation directory (the default is Program Files\Protector Suite QL).*
- 5 *At the end of installation, you will be asked to reboot your computer. Protector Suite QL will be active only after reboot.*

During installation, all necessary hardware drivers are pre-installed. Connect your hardware after reboot (if you do not have an integrated fingerprint reader) and you can begin using Protector Suite QL.

Removal

To uninstall Protector Suite QL, select **Start - Settings - Control panel** and open **Add or Remove Programs**.

Select Protector Suite QL and click the **Change** button. Select the **Remove** option.



You will be asked what to do with Protector Suite QL's data stored on your computer.

There are two options:

You can leave all the data on your computer. This means that if you later re-install the Protector Suite QL, you can continue using the enrolled fingerprints and Password Bank registrations.

OR

You can remove the Protector Suite QL data from your computer. Enrolled fingerprints and Password Bank registrations will be permanently deleted.

Note: If you have used enrollment to your fingerprint reader option, data remains in the device memory. Instructions on how to clear the device memory from Protector Suite QL can be found in Chapter 3.

Files and folders stored in **My Safe** folders are not deleted during program removal. You can use them later if you reinstall Protector Suite QL. They can be accessed using the backup password entered when creating **My Safe**. However, if you (or some other user) have created a large **My Safe** folder and you do not plan to use it later, we recommend deleting it before you uninstall the product. (To delete **My Safe**, click the **Delete** button in the **Control Center - Settings - User Settings - My Safe** dialog.)

A hand is shown pointing at a fingerprint being scanned on a device. The background is a warm, yellowish-orange gradient.

Chapter 2

Let's Start

You have just finished installing Protector Suite QL, or the product is pre-installed on your computer. This chapter guides you through your first steps in using Protector Suite QL. For this chapter, let's suppose the simplest scenario - you are the only user of your computer, you have administrator's rights, and the default convenient mode of the Protector Suite QL is set.

For a detailed description of individual Protector Suite QL features and differences of other scenarios, see the next chapter.

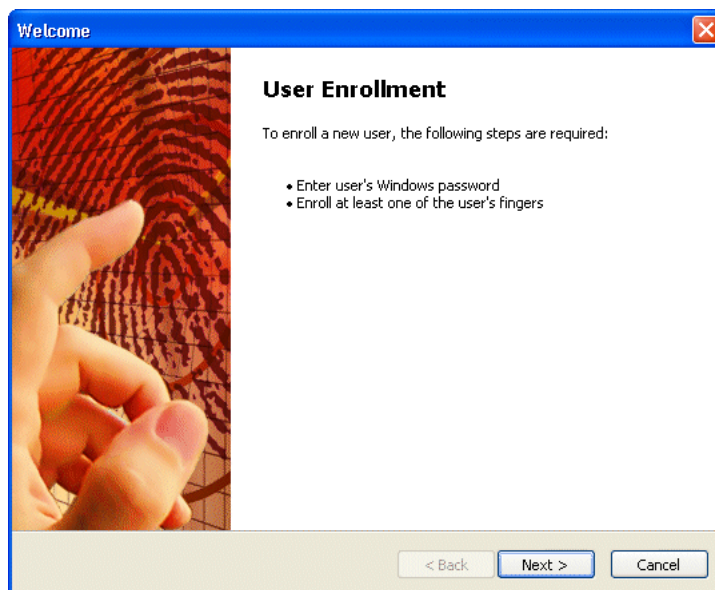
First Use - User Enrollment

- 1 *If you want to use an external fingerprint sensor, connect your device. All the necessary drivers are installed with Protector Suite QL. An informational message that the sensor was connected and is ready to use is displayed in the lower right corner of your screen. If you encounter any problems with your hardware, see the **Troubleshooting** chapter of this guide.*
- 2 *Start **User Enrollment** from the **Start** menu. You will be asked to select the enrollment type. If your device supports enrollment to the device memory, you can select whether to store your authentication data to the device memory, or to your hard disk.*

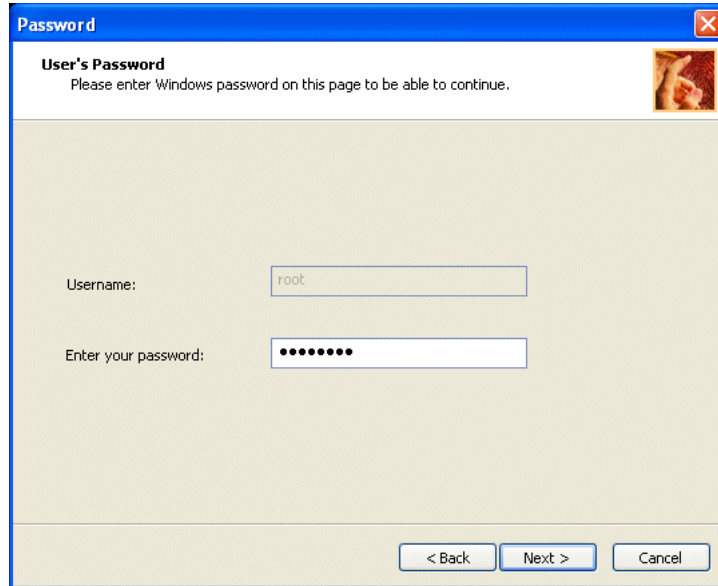
If you select enrollment to your device memory, your data cannot be accessed without the corresponding fingerprint device. Authentication information will be protected by a software encryption key generated by your fingerprint software together with a hardware encryption key obtained directly from your device.

Begin with enrollment. Only after you enroll at least one of your fingers, can you fully use all the features of Protector Suite QL.

The enrollment wizard will guide you through the enrollment procedure.



3 *Enter your Windows password.*

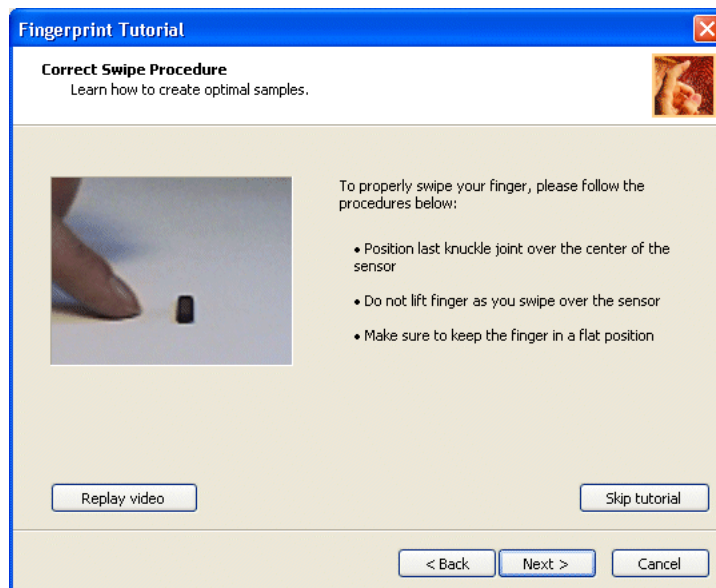
A screenshot of a Windows Password dialog box. The title bar is blue and says "Password". The main area has a white header with the text "User's Password" and "Please enter Windows password on this page to be able to continue." Below this is a large beige area. In the center, there are two input fields. The first is labeled "Username:" and contains the text "root". The second is labeled "Enter your password:" and contains ten black dots. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

If you do not use a Windows password (you have an empty Windows password), you are informed about it and prompted as to whether you want to create a new password.

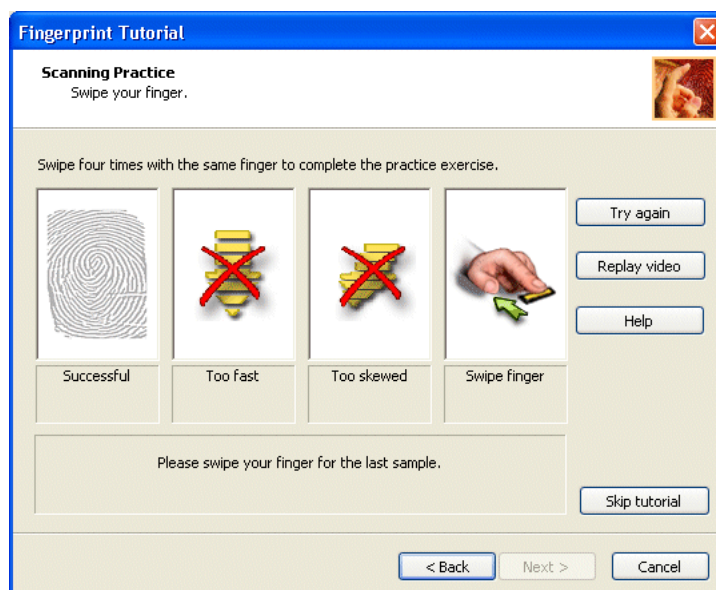
Hint: Defining a Windows password increases security of your Windows account.

- 4 *It is highly recommended that you go through the fingerprint tutorial. The tutorial can be started from the enrollment wizard, or from the **Start** menu. The tutorial consists of three pages:*
- *The first page explains the purpose of the tutorial.*

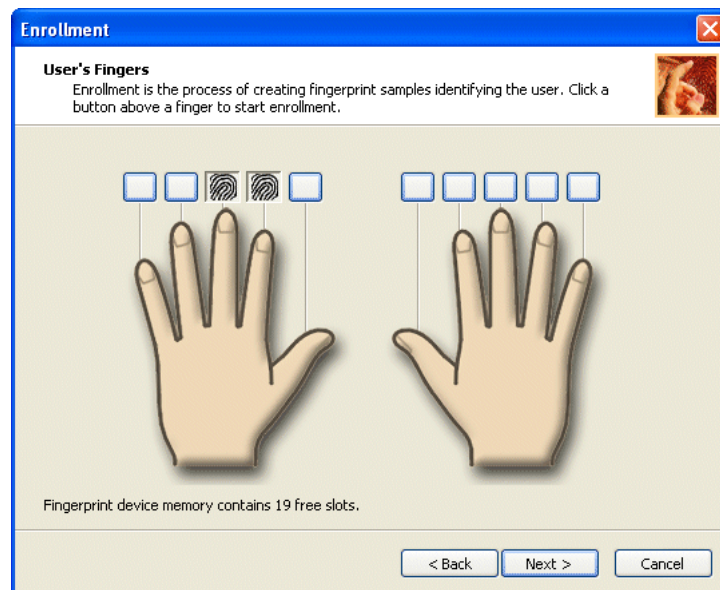
- The second page displays the correct scanning procedure.



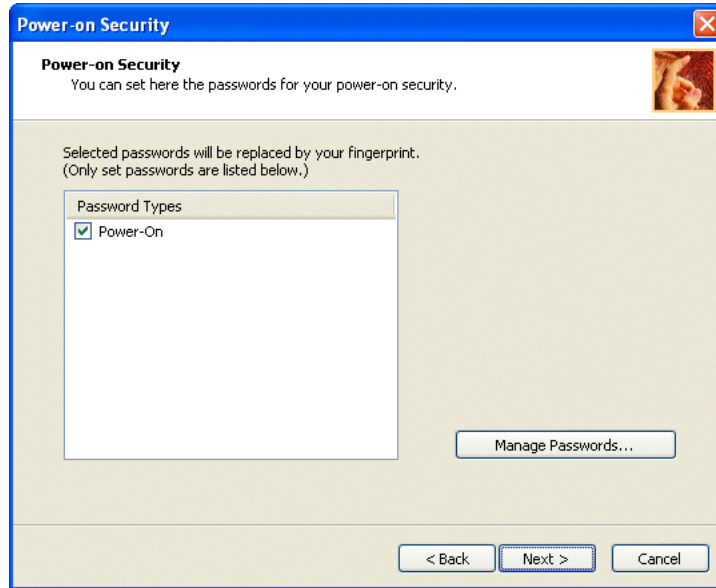
- On the third page, you can try to create four samples of your fingerprint and match them. Use the **Replay video** button to remind yourself of the correct motion. After you successfully create your samples, click **Finish** to close the tutorial and to return to the enrollment wizard.



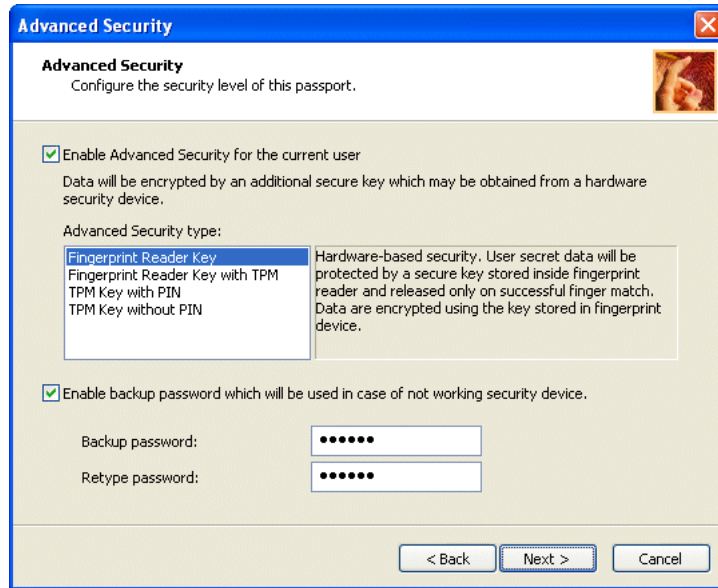
- 5 Click the button above the finger you want to scan.
Create three samples of your finger as you were instructed by the tutorial.
The final template will be created using these three samples. A warning is displayed if the three created samples cannot be matched. In this case, it is recommended that you go through the tutorial once more.
You can enroll up to 10 fingerprints. **It is strongly recommended that you enroll more than one finger in the event of an injury** - this will allow you to pass the biometric verification necessary for Protector Suite QL functions.



- 6 If your BIOS supports secure BIOS passwords, a **Power-on security** page is displayed. Select passwords which will be replaced by your fingerprints. (You will be asked to enter the password after you select it.) Local administrators can also manage BIOS passwords from here. Clicking the **Manage passport** button opens the **BIOS passwords** dialog where passports can be set, unset, or changed.



- 7 *Some hardware configurations provide additional data security through encryption. In these configurations, an additional dialog with an Advanced Security type is displayed. Select the Advanced security type. For more information about advanced security, see Chapter 3. **It is recommended that you set the backup password.** It may help you in case of biometric authentication failure.*



- 8 After you finish the enrollment wizard, an **Introduction** screen displays the possible ways you can use fingerprints with Protector Suite QL.

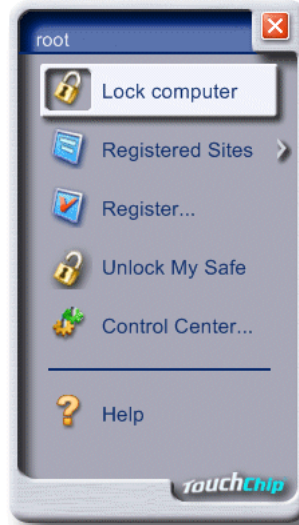
After you enroll your fingerprints, you can use your finger:

- to gain access to your computer account,
- to display the Biomenu with all its functions (locking computer, registering pages, dialogs, accessing My Safe folder etc.) Navigation in the Biomenu can be performed by moving your finger on the sensor.
- to fill in the registered web forms or dialogs.
- to launch your favorite applications.

NOTE: Each Windows user can have only one passport. To create a user account, select **Start - Settings - Control Panel**, and click **User Accounts**. Follow the on-screen instructions.

Biomenu - Accessing Main Features

Now that your fingerprints are enrolled, you can start initiating various actions with your finger. Swipe your finger to display the **Biomenu**.

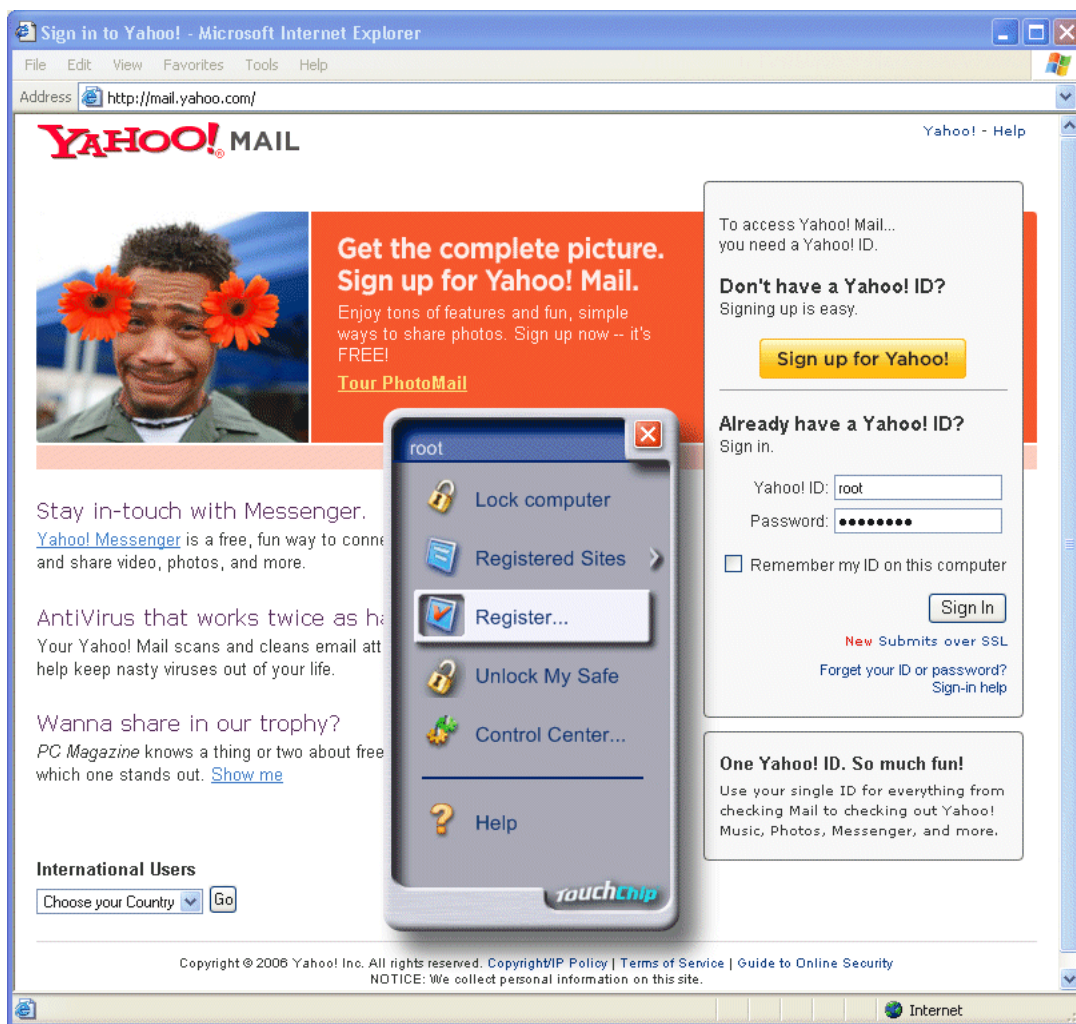


The **Biomenu** gives you access to Protector Suite QL's features. To force displaying the **Biomenu** in situations when swiping your finger defaults to another action (e.g. a registered window is active), hold the **Shift** key and swipe your finger. The **Biomenu** supports bio-navigation. This means that you can use your sensor to navigate instead of your mouse. Move your finger to navigate through the **Biomenu** and tap the highlighted item to run the corresponding action.

Password Bank - Registering Web Pages and Dialogs

Many web pages and other applications require entering various data - user names, password, and other information - each time you display them. The Password Bank is the right solution for such situations. You fill in the information (or set necessary options) and register the window. When you access the page or the dialog later, you can replay the stored information by swiping your finger over the sensor.

Open your browser and go to the page you want to register (or display the dialog you want to register). Enter all the information you want to have in the registration. Swipe your finger to display the **Biomenu**. Select **Register...**



All your data is stored. A message is displayed informing you that the registration was successfully created.

The registered web page can be accessed directly from **Biomenu - Registered Sites**.



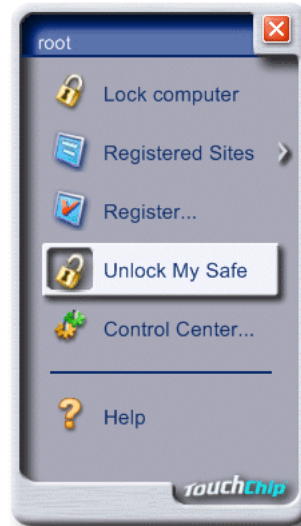
To replay the information that you registered in a dialog or web page simply swipe your finger over the sensor when the dialog or the web page is displayed. Data stored in the registration will be filled in the form automatically.

For more information about Password Bank and possible settings, see “Password Bank” on page 27 and “Settings” on page 39.

My Safe - Protecting Sensitive Files

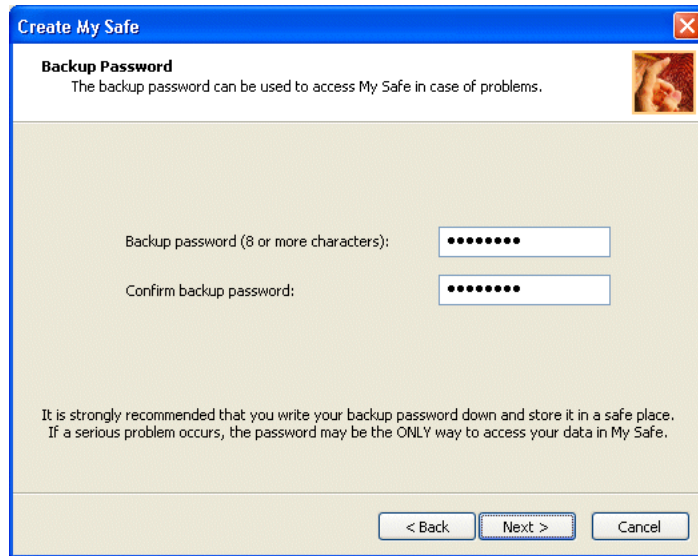
If your computer can be accessed also by other users, you have the option of creating an encrypted storage area. My Safe is a place where you can store your sensitive files which are then accessible only by using your fingerprint.

To use My Safe, swipe your finger and select **Unlock My Safe** from the **Biomenu**



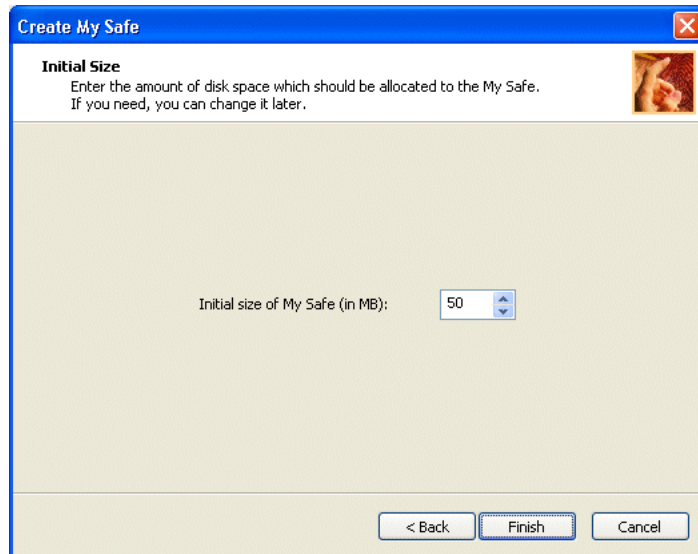
Before the first use, **My Safe** must be created. A wizard will guide you through this process.

You will be asked to define a My Safe backup password. This password can be used to open **My Safe** in case of failure of your biometric device. The backup password must be at least 8 characters long.



The screenshot shows a Windows-style dialog box titled "Create My Safe". The main heading is "Backup Password" with a subtext: "The backup password can be used to access My Safe in case of problems." Below this, there are two text input fields. The first is labeled "Backup password (8 or more characters):" and the second is labeled "Confirm backup password:". Both fields contain eight dots, indicating masked text. At the bottom, there is a paragraph of text: "It is strongly recommended that you write your backup password down and store it in a safe place. If a serious problem occurs, the password may be the ONLY way to access your data in My Safe." and three buttons: "< Back", "Next >", and "Cancel".

Set a size for **My Safe**. The default size is 50 MB. The **My Safe** folder can be resized later. Resizing does not affect stored data.



The screenshot shows the same "Create My Safe" dialog box, but at the "Initial Size" step. The heading is "Initial Size" with subtext: "Enter the amount of disk space which should be allocated to the My Safe. If you need, you can change it later." Below this, there is a label "Initial size of My Safe (in MB):" followed by a spin box containing the number "50". At the bottom, there are three buttons: "< Back", "Finish", and "Cancel".

You can place any files or folders in **My Safe** folder, just as in any other folder. **My Safe** can be found under **My Documents**. After you finish your work, simply select **Lock My Safe** from the **Biomenu** and your sensitive files will not be visible nor accessible for any other user.

To learn more about working with **My Safe**, see “**My Safe**” on page 32.

Control Center

The Control Center provides a common user interface for all the Protector Suite QL settings. For a list of all available functions, see page 35.

To use Protector Suite QL Control Center:

- Select **Start - All Programs - Protector Suite QL - Control Center**,
- or select **Control Center** from the **Biomenu**,
- or select **Start Control Center...** from the tray icon menu.

Launching Applications

You can start an application (any executable file) on your computer by swiping the assigned finger. For more information about Application launcher, see page 44.

To create an association between the enrolled finger and an application:

- 1 Open the **Control Center**, select **Settings - User Settings**. Swipe your finger to perform verification.
- 2 Select the **Applications** tab.
- 3 Click the **Add** button. The **Application** dialog opens.
- 4 Select an enrolled finger from the list.
- 5 Enter the descriptive name of the application. (This name is displayed in the **Applications** page in **User Settings**.)
- 6 Browse for an application you want to launch. This can be any executable file.
- 7 Optionally, enter any necessary application parameters.
- 8 Click **OK**.

Fast User Switching

The Fast User Switching (FUS) feature of Windows XP is also supported. If user A is logged on and user B (who is already enrolled) puts a finger on the sensor, Protector Suite QL recognizes the fingerprints and switches the users.

To turn Fast User Switching support on, run the **Control Center - Settings - System Settings** and select the **Enable Fast User Switching support** check box. (This option is visible only if you use Windows XP. It is available only on computers that are not members of a domain.) If your system currently does not support FUS, please follow the on-screen instructions. Reboot may be required after this change.



Chapter 3

Reference

This chapter describes all the features of Protector Suite QL in detail.

Enrollment

Biomenu

Fingerprint Logon

Password Bank

My Safe

Application Launcher

Control Center

System Tray Icon

Enrollment

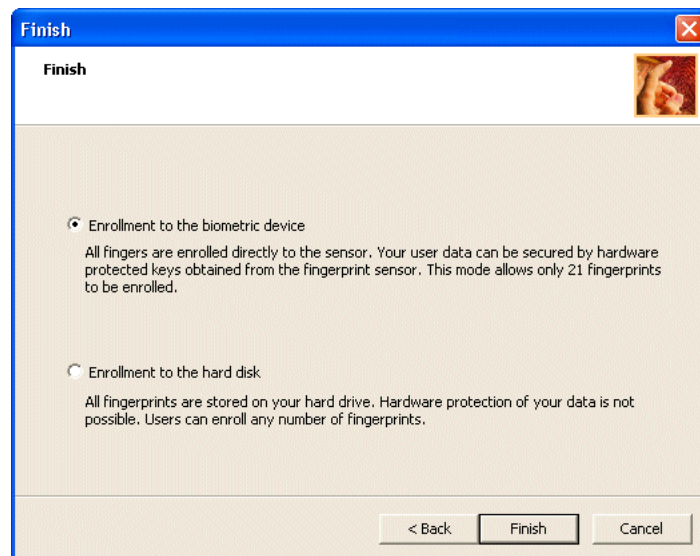
Before you can start using Protector Suite QL with all its features, you must *enroll*. Enrollment is a process of creating correspondence between your user name and password and your fingerprints (computerized so that it reconstructing the original image is impossible) together with automatically generated security keys. All the data is stored in your *passport*.

The Protector Suite QL starts automatically. To get access to its features and settings, use the **Start** menu shortcuts (**Start - All Programs - Protector Suite** contains shortcuts for the **Control Center**, **User Enrollment**, **Fingerprint Tutorial**, and **Help**), **Biomenu**, or the tray icon menu.

Enrollment Type

Protector Suite QL stores your authentication data derived from your fingerprint samples either to the device memory, or to your hard disk. The data is stored in an encrypted form in both cases.

Before the first enrollment after installation, device initialization may be necessary. During the initialization, you will be asked to select an enrollment type. (Initialization is performed automatically for some device types.) The enrollment process is started immediately after initialization.



If you select enrollment to your device memory, your data cannot be accessed without the corresponding fingerprint device. Authentication information will be protected by a software encryption key generated by your fingerprint software together with a hardware encryption key obtained directly from your device.

The only limitation is size of the device memory. If you plan to enroll a larger number of fingerprints for several users (usual device memory size is sufficient for 21 fingerprints), enrollment to the hard disk is necessary.

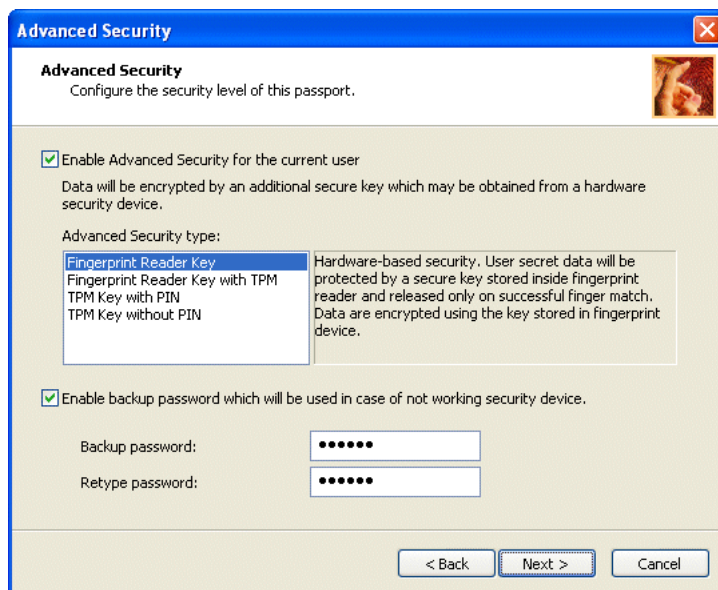
If you select enrollment to your hard disk, data will be encrypted using a software key. Biometric verification can be performed using any fingerprint reader.

WARNING: Selected enrollment type cannot be changed later. The only way to change it is uninstalling the Protector Suite QL and reinstalling it again.

For a detailed description of how to enroll your fingerprints and how to manage your passport, see page 35.

Advanced Security

Security in Protector Suite QL can be increased with additional encryption. The types of this encryption available depend upon your hardware. Advanced security can be enabled (or later also disabled) per user at the end of the Edit/Enroll fingerprints wizard. Types of encryption can be changed in this dialog to adjust the necessary level of security and user convenience in your installation.



Fingerprint Reader Key with TPM

Provides improved hardware-based security. An encrypted channel between the TPM Security Chip and the fingerprint reader further enhances security of user secret data. Recommended for highest security.

Fingerprint Reader Key

Provides hardware-based security. User secret data will be protected by a secure key stored inside the fingerprint reader and released only on successful finger match. Data is encrypted using the key stored in fingerprint device.

TPM Key with PIN

User secret data will be protected by the TPM Security Chip with PIN. Requires the user to enter a PIN during every identity verification. Recommended for high security.

TPM Key without PIN

User secret data will be protected by the TPM Security Chip. Recommended for higher convenience.

Support for Logon

Protector Suite QL supports Novell network logon. In order for Protector Suite QL to log you on automatically to a Novell network, your Windows user name and password must match your Novell user name and password. Some Novell clients have problems with supporting 3rd party logon applications. The following clients versions are not supported: 4.83, 4.90.

Biomenu

The **Biomenu** contains links to the most useful Protector Suite QL functions which require biometric verification. After you finish the enrollment, swipe your finger to invoke the **Biomenu**. Now, you have access to your registered sites, you can register a new form, web site, or a dialog (see “**Password Bank**” on page 28). You can lock/unlock **My Safe** (see “**My Safe**” on page 32). You can also lock your computer, run the **Control Center** (see “**Control Center**” on page 35), or display **Help**.

Fingerprint Logon

Replacing the standard Windows logon with fingerprints can both improve security of your computer and give you a higher convenience during the logon process. Biometric logon also protects your screensaver (password protected resume from screensaver must be set in your system.) and wake-up from power-saving features (standby, hibernation - **Prompt for password after resume from power save** must be set on your system).

Note: You must establish a Windows password to protect your computer. If a Windows password is not established, Protector Suite QL cannot secure access to your computer.

To control the level of security and convenience of the Protector Suite QL, set one of the security modes.

In the **convenient mode**, all users are equal and have the same rights. This means that each user enrolls and manages his/her own passport.

The **secure mode** brings an administrator role to the passport management. Administrators of Protector Suite QL are by default all members of the local administrators group; more users can be added from the **Security Mode** page of the **System Settings** using the **Administrators' Groups** button. Administrators of Protector Suite QL create and manage passports of all users and (those who are members of the Local administrators group) also perform system settings - the settings common for all. Therefore, in the secure mode, not all the features and settings described later are accessible for everyone.

Note: Membership in the Administrators of Protector Suite QL group is necessary for the following actions: enrolling users, deleting user (without verification), exporting/importing data of any user, power-on security management, deleting fingerprints of other users using the **Fingerprint storage inspector** (enrollment to the fingerprint device only), logon using username and password.

For the detailed description of fingerprint logon settings, see page 40

Password Bank

The Password Bank records data entered into a web page or an application dialog into a registration and replays the stored registration later. The registration can contain a web form (e.g. a login page with entered user name and password to your mail account, internet banking, e-shop), or a Windows application dialog (e.g. Windows Explorer dialog for accessing a net share, dialog for logon to a database program or an e-mail client). You enter your logon information only once - when creating the registration - and store it to your passport using your fingerprint. When the dialog or web page is displayed again, swiping your finger will automatically fill in your data.

The Password Bank supports the following browsers: Internet Explorer 5.0 and higher, Mozilla 1.3 - 1.7, Netscape 7.0 - 8.0.4, Firefox 1.0 - 1.5. Support for Internet Explorer is installed automatically. When Protector Suite QL detects Mozilla/Firefox/Netscape, it prompts the user whether to turn the support on. Alternatively, the Mozilla/Firefox/Netscape support can be turned on from the **Control Center - Settings - Users Settings - Password Bank**. If you want to enable Password Bank's support for a browser, check the corresponding check box. (Only local administrators can see this option and enable more browsers.)

Password Bank displays hints for the user when an action like registering a dialog, replaying a dialog, etc. is possible. These hints can be turned on/off in the Protector Suite QL **User Settings**. However, these hints are not active if the user logs on using user name and password, without fingerprint authentication, until the successful fingerprint verification is performed.

To set the Hints Displayed:

- 1 Click **Start - All Programs - Protector Suite QL - Control Center**.
- 2 Select **User Settings**. Authentication is required.
- 3 Select **Password Bank**.
- 4 Select the hints you want to display.
 - **Alert me when a registration is replayed** - This hint informs the user that replaying of the registration is about to be started. This alert is useful in cases you want to create more registrations of the same form or dialog and do not want to overwrite already entered data.
 - **Alert me after a registration was created** - This hint informs the user that the registration has been successfully created.
 - **Alert me if a password field is edited** - This hint informs the user that password field will be displayed in a readable form.
 - **Alert me if a dialog could be replayed** - This hint informs the user that replaying the registration is possible.
 - **Alert me if a dialog is suitable for registration** - This hint informs the user that the dialog contains a password field that can be registered.
 - **Alert me if an internet page could be replayed** - This hint informs the user that replaying the registration is possible.
 - **Alert me if an internet page is suitable for registration** - This hint informs the user that the page contains a password field that can be registered.

Registering Pages

Open the web browser and go to the page you want to register. Enter all the information you want to have in the registration, swipe your finger, and select **Register window** from the **Biomenu**. All your data will be stored. The registered page can be accessed directly from **Biomenu - Registered sites**.

Registrations of web pages use the same format for all supported browsers. Registrations created in e.g. Internet Explorer can be later replayed in Mozilla.

Password Bank registers individual forms. If a page contains several forms, each form requires a separate registration. This means that only the active form is registered. To register a form on a page for which a registration already exists (a page with multiple forms), hold the **Shift** key and swipe your finger to display the **Biomenu**. (If the page is already registered, swiping your finger across the sensor without holding the **Shift** key replays the existing registration.)

When registering pages with multiple forms, the following steps are used:

- *An active form is registered.*
- *If no form is active, and Internet Explorer 5.5 or higher is used, the user is prompted to select the form for registration.*
- *If none of the previous is true, no action is taken.*

Sample scenarios:

Suppose that there are no registrations for a page. The page contains form A and form B.

A. You have just filled in form A, and this form is still active. You swipe your finger across the sensor. Form A is registered.

B. You have just filled in form A and moved to form B so that form B is active. You swipe your finger across the sensor. Form B is registered (but still empty).

C. You have just filled in form A and clicked outside the form so that no form is active. You are using Internet Explorer 5.5 or higher. You swipe your finger across the sensor. You will be prompted to select the target form for registration.

D. The same situation as in C, but you are using earlier version of IE, Mozilla, or Netscape. No action is taken.

Replaying Web Page Registrations

An existing registration is replayed automatically if the page is displayed from **Biomenu - Registered Sites**. If you displayed the page manually and now you want to replay the registration, swipe your finger across the sensor.

When replaying registrations of pages with multiple forms:

- *If there is only one registration for the page (regardless of the total number of existing forms), the registration is replayed.*
- *If there are multiple registered forms, and one from the registered forms is active, this form is replayed.*
- *If there is no active form, all the existing registrations for the page are offered for replaying. Select the registration you want to replay.*

Registering and Replaying Dialogs

The Password Bank is primarily intended for registering simple dialogs containing a user name and a password field, typically dialogs for logging into various applications.

More complex dialogs may have some issues. Text fields and password fields can always be registered. Registrations save controls which are not hidden, disabled, minimized etc. Radio buttons, check boxes, combo boxes, and selections in list boxes are registered for applications that are using standard Windows controls (e.g. system dialogs). All the registered information can be edited (e.g. when a password change is forced).

You may encounter problems with dialogs containing multiple pages. In some cases, all the pages are registered in one registration. The Password Bank cannot correctly handle dialogs which do not create some controls before they are used, but only draw them. The typical examples are some dialogs in Microsoft Office.

When replaying a registered dialog, if some control change invokes an action requiring user reaction, the Password Bank waits (with the dialog), and replaying is completed only after the action is finished.

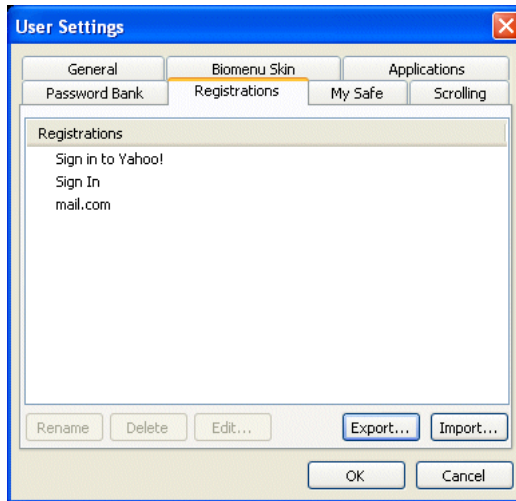
Managing your Registrations

All your registrations are visible in the **Control Center - Settings - User Settings - Registrations** dialog. You can change the contents of your registrations to reflect changes of your data, or of the registered pages. You can also turn on/off automatic submitting of replayed registration. Your registrations can be exported for use as backup or on another computer, or imported to your computer.

To manage registrations:

- 1 Click **Start - All Programs - Protector Suite QL - Control Center**.
- 2 Select **User Settings**. Authentication is required.

3 Select **Registrations**.



4 Select a registration you want to work with.

- Click the **Rename** button to change the descriptive name of registration displayed in **Registrations**.
- Click the **Delete** button to delete the registration.
- Click the **Edit** button to change the data stored in the registration. (e.g. your password or address has changed and you want to reflect this in existing registration.)
- Select the **Auto submit form** check box to submit the selected registration of a form automatically after replaying the registration. Select the **Auto submit** check box to submit the selected registration of a dialog to click the default dialog button (usually **OK**).
- Click the **Export** button to export the selected registrations. All registrations are exported if you do not select any. You will be asked to select a destination file and to enter a password which will protect your registrations. A file extension of password bank files is **.pb**.
- Click the **Import** button to import registrations from a password bank file. Select the source **.pb** file. Select whether you want to overwrite your existing registrations by the imported ones, or to add imported registrations to your registrations list. Enter the password (created during export).

My Safe

My Safe is a folder protected by your fingerprint. Its size can be changed at any time. **My Safe** is stored under your **My Documents** folder. Its contents are not visible to other users (including other logged users if you are using FUS).

For better accessibility, a shortcut is created on your desktop and under **My Computer**.



Lock/Unlock My Safe commands are accessible in the context menu **My Safe** (or its shortcut) and in the **Biomenu**.

Before you unlock **My Safe** for the first time, **My Safe** must be created. During its creation, you must define **My Safe** backup password and set its initial size. You can change it later. The maximum size of **My Safe** is 2047 MB.

Backup Password

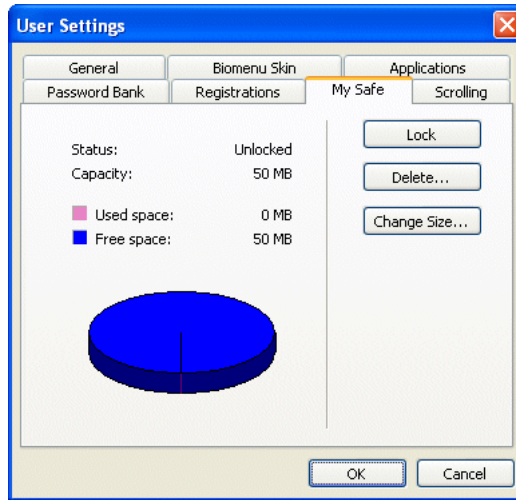
When you created **My Safe**, you were asked to enter a backup password. This password can be used to access the data stored in **My Safe** in case of fingerprint sensor failure or if your enrolled fingerprint cannot otherwise be used. Try to access **My Safe** as you did before. A dialog will inform you about the problem and ask you to enter the backup password.

TIP: If you forgot your backup password, you can delete the old **My Safe** from this dialog and create a new one. (You will lose all the data stored in your existing My Safe.)

To manage My Safe:

- 1 Click **Start - All Programs - Protector Suite QL - Control Center**.
- 2 Select **User Settings**. Authentication is required.

3 Select **My Safe**.



Information about **My Safe** status (locked/unlocked) and size (or free and used space, if **My Safe** is open) is displayed. Some buttons are not available in all situations. Change **My Safe** status to make the other options available.

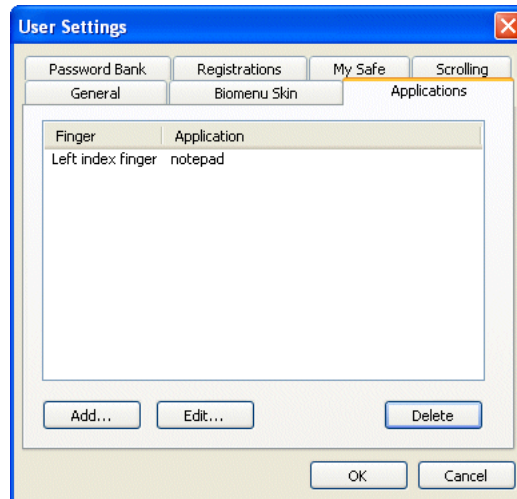
- Click the **Create** button to create **My Safe**. This button is available only when there is no **My Safe** folder.
- Click the **Unlock** button to unlock **My Safe**. This button is available only when **My Safe** is locked. You can access your data stored in **My Safe** only when it is unlocked.
- Click the **Lock** button to lock **My Safe**. This button is available only when **My Safe** is unlocked.
- Click the **Delete** button to delete **My Safe**. All your data stored in **My Safe** will be permanently deleted and cannot be restored.
- Click the **Change Size** button to change the size of **My Safe**. This operation does not affect data stored in **My Safe**.

Do not forget that all the files stored in **My Safe** are accessible if it remains unlocked and you are logged on. **My Safe** is locked automatically whenever you finish your session (you log off). In all other cases, lock **My Safe** manually to secure your sensitive files.

Application Launcher

You can start an application (any executable file) on your computer by swiping the assigned finger. At least one enrolled finger must remain unassigned for displaying the **Biomenu**. If you want to override launching the application (and invoke the **Biomenu** instead), hold **Shift** when swiping the finger.

To create or change an association between the enrolled finger and application, open the **Control Center**, select **Settings - User Settings** and select the **Applications** tab.



To create the association between an enrolled finger and an application:

- 1 Click the **Add** button. The **Application** dialog opens.
- 2 Select an enrolled finger that is free.
- 3 Enter the name of the application. (This name is displayed in the **Applications** dialog in **User Settings**.)
- 4 Browse for a file you want to launch. This can be any executable file.
- 5 Optionally, if your application requires additional parameters, type them into the **Application parameters** field.
- 6 Click **OK**.

To edit the fingerprint/application combination later:

- 1 Select an application in the **Applications** dialog.
- 2 Click the **Edit** button.
- 3 Perform necessary changes in the **Application** dialog.

4 Click **OK**.

To delete the fingerprint/application combination:

- 1 Select an application in the **Applications** dialog.
- 2 Click the **Delete** button.

Changes made on the **Applications** tab are saved only after you click **OK** in the **User Settings** dialog.

Control Center

The Control Center main screen is displayed. On this screen, topics are displayed. Click the topic to display a list of valid actions available for that topic. The topics include **Fingerprints**, **Settings**, and the **Help**.

Fingerprints

The Fingerprints section enables you to enroll, edit and delete passports, and to export/import them. The list of available actions might differ depending on your authentication hardware, the existing passports, and the access privileges of the current user.



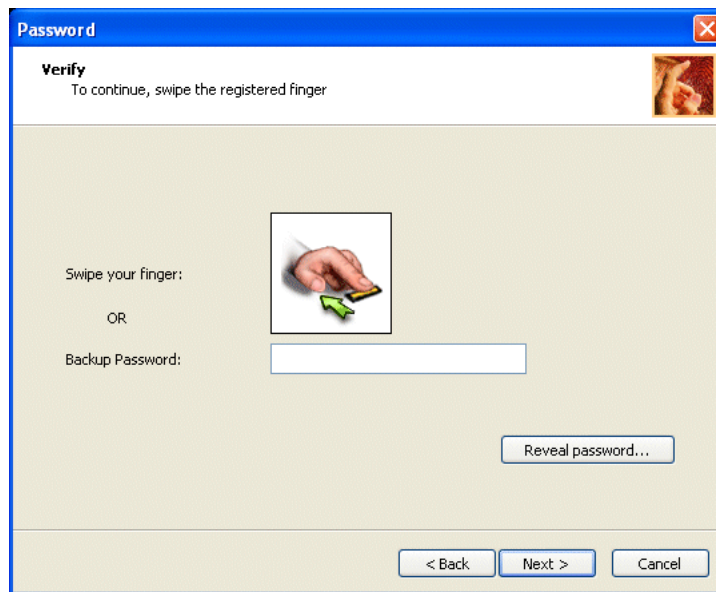
Each user identity in Protector Suite QL is represented by a passport, which contains biometric fingerprint data used to authenticate the user to the computer. Each Windows user can have only one passport. Two passports cannot include the same finger.

Enroll or Edit Fingerprints

Note: In the secure mode, the Protector Suite QL administrators can enroll passports for all users, or user self-enrolment during logon can be enabled. In the convenient mode, users can enroll or edit only their own passports.

To create a new passport and enroll fingerprints, complete the following procedure:

- 1 Click **Start - All Programs - Protector Suite QL - Control Center**.
- 2 Click **Fingerprints**.
- 3 Click **Enroll or Edit Fingerprints**. (After installation but before the first user is enrolled, only the **Initialize** wizard is displayed in this section. After you select the enrollment type, the enrollment wizard starts automatically.) In the secure mode, a list of existing passports is displayed. Click the **Enroll** button to start the enrollment of a new user.
- 4 Enter the Windows password and click **Next**.
In the secure mode, you can also enter the user name manually.



- 5 Read instructions on how to create fingerprint samples. Click **Next** to proceed with the fingerprint tutorial. Going through this tutorial is highly recommended for first-time users.
- 6 The tutorial will show you a short video showing correct and incorrect fingerprint scanning. Then you will try to create your first fingerprint samples. Simply follow the on-screen instructions. After you successfully go through the tutorial, click **Next** to continue the enrollment process.
- 7 A page with hands is displayed. Click a finger you want to enroll to select it and start fingerprint scanning.
- 8 You must scan the selected finger three times. The created samples are combined into a final fingerprint sample.
You can enroll up to ten fingers.
If your system supports power-on security, fingerprints are by default added to power-on verification. If enrollment to the hard disk is set, a **Power-on** button may be displayed above each finger in the case that device memory is full. Use these buttons to select fingers for power-on security.
- 9 Do one of the following:
 - Select another finger to enroll. (It is recommended that you enroll at least two fingers.)
 - Click **Next**.
- 10 If your BIOS supports secure BIOS passwords, a **Power-on security** page is displayed. Select passwords which will be replaced by fingerprints. (You will be asked to enter the password after you select it.) Local administrators can also manage BIOS passwords from here. Clicking the **Manage passport** button opens the **BIOS passwords** dialog where passwords can be set, unset, or changed.
- 11 Some fingerprint devices allow securing your data with additional encryption. If you are using such a device, select the Advanced security type. For more information about advanced security, see Chapter 3. **It is recommended that you set the backup password.** It may help you in case of impossible fingerprint authentication.
- 12 When you are done, click **Finish**.

To edit a passport and fingerprints, complete the following procedure:

- 1 Click **Start - All Programs - Protector Suite QL - Control Center**.
- 2 Click **Fingerprints**.
- 3 Click **Enroll or Edit Fingerprints**.
*In the secure mode, a list of existing passports is displayed. Select the user to be edited and click the **Edit** button.*
- 4 The **Opening user passport** screen is displayed.
- 5 Swipe your finger over the fingerprint sensor or enter your Windows/Advanced security backup password, and click **Next**.
- 6 Do one of the following:
 - To enroll a new fingerprint, complete the following procedure:
 - Select a finger to enroll by clicking the appropriate image.
 - Swipe the selected finger across the fingerprint sensor. Three successful images are required to enroll one fingerprint.
 - To delete a fingerprint, complete the following procedure:
 - Select a finger to delete by clicking the appropriate image.
 - Click OK to confirm the delete operation.*If enrollment to the hard disk is set, a **Power-on** button may be displayed above each finger in the case that device memory is full. Use these buttons to select fingers for power-on security.*
- 7 When done enrolling or deleting fingerprints, click **Next**.

Delete

Note: In secure mode, only administrators can delete passports.

To delete an existing passport:

- 1 Click **Start - All Programs - Protector Suite QL - Control Center**.
- 2 Click **Fingerprints**.
- 3 Click **Delete**.
In the convenient mode, swipe your finger to perform verification and confirm deleting the current passport.
In the secure mode, a list of existing passports is displayed. Select the passport that you want to delete and confirm deletion.

Import or Export User Data

Export creates a backup copy of your passport. If enrollment to the device is selected, exported passport can help you if you need to replace the sensor.

To export an existing passport:

- 1 Click **Start - All Programs - Protector Suite QL - Control Center**.
- 2 Click **Fingerprints**.
- 3 Click **Import or Export User Data**.
*In the secure mode, a list of existing passports is displayed. Select the passport that you want to export and click **Export**.*
- 4 Select the destination file (.vtp extension).
- 5 Define a password which will protect the exported data.
- 6 Verify the finger (contained in the just exported passport).

To import a passport archive:

- 1 Click **Start - All Programs - Protector Suite QL - Control Center**.
- 2 Click **Fingerprints**.
- 3 Click **Import or Export User Data**.
- 4 Browse for the passport file (.vtp extension).
- 5 Enter the password (defined during export).

Settings



System Settings

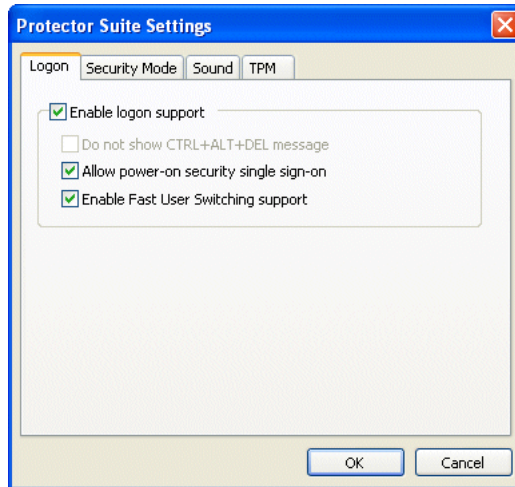
The System Settings dialog consists of several pages depending on your system configuration. Not all the described pages may be visible in your installation.

General

The **Show Control Center on Windows startup** check box toggles displaying the main program screen on the system startup.

Logon

Note: Only an administrator can change logon settings. Some changes require you to restart the computer.



To change your logon settings, complete the following procedure:

- 1 Click **Start - All Programs - Protector Suite QL - Control Center**.
- 2 Click **Settings**.
- 3 Click **System Settings**. Go to the **Logon** page.
- 4 Select or clear the check boxes for required options:

Replace Windows logon with fingerprint-protected logon

When this check box is marked, you can log onto your computer using fingerprint authentication. When this check box is clear, you must log onto your computer using your Windows password.

Do not show Ctrl+Alt+Del message

The standard Windows CTRL+ALT+DEL message will not be displayed if you select this option. Only a hint to swipe a finger will be shown. (The logon dialog for entering user name/domain/password can be invoked by pressing CTRL+ALT+DEL so that users are able to log on using user name and password.)

Automatically log on a user verified by power-on security (available only in configurations with power-on security support)

This check box binds your power-on authentication to your Windows authentication. If a fingerprint used for power-on security feature matches a fingerprint on an existing passport, the corresponding user is logged

onto Windows automatically. When this check box is clear and power-on authentication is enabled, you must provide your fingerprint for authentication both for BIOS and for Windows logon.

Enable Fast User Switching support

This check box enables and disables the fast user switching feature of Windows XP, if supported on your computer. When the fast user switching feature is supported, but not enabled, you will be prompted to enable it on your system.

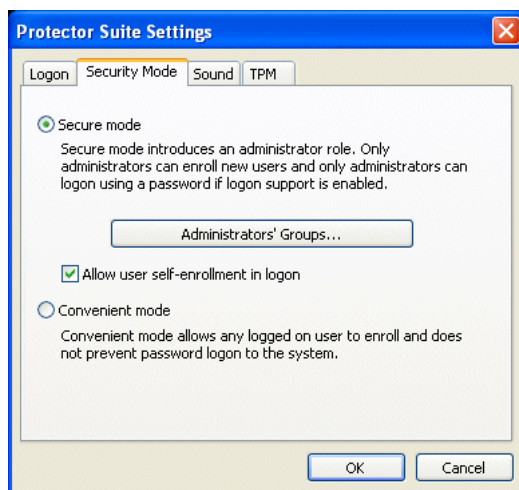
5 Click *Finish*.

Security Mode

Note: Only an administrator can change security mode.

The Security Mode screen enables you to control who has access to fingerprint security management controls. There are two security modes - convenient and secure. In the convenient mode, all users share the same privileges. For example, every user can create his own passport or log on using Windows user name and password.

However, if you toggle security to secure mode, the situation changes. Only administrator has an unrestricted access to administrative functions. Non-administrator users need to obtain passports from the administrator (unless user self-enrollment in logon is enabled). They can only edit their own passport.



To set a security mode, complete the following procedure:

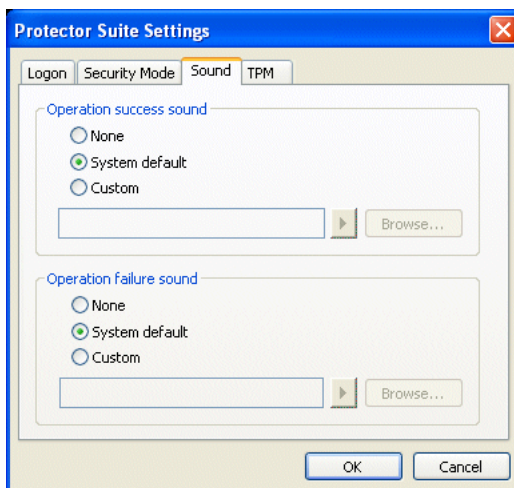
- 1 Click *Start* - *All Programs* - *Protector Suite QL* - *Control Center*.**
- 2 Click *Settings*.**

- 3 Click **System Settings**. Go to the **Security mode** page.
- 4 Select the desired security mode. The options are as follows:
 - **Secure mode** - the secure mode introduces an administrator role for performing Protector Suite QL management. Making sensitive functions (passport management) available only to administrators adds more security to the computer. Non-administrator users cannot logon using their Windows user name and password.
Click the **Administrators' Groups** button to edit the list of users with Protector Suite QL administrator rights.
Check the **Allow user selfenrollment in logon** to allow enrolling fingerprints during logon directly by users without Protector Suite QL administrator rights. In this case, non-administrator users enter their Windows user name and password during their first logon and they will be forced to enroll their passport before the actual logon is performed. (This means that logon is not successful until the user actually enrolls fingerprints.)
 - **Convenient mode** - the convenient mode is intended mostly for home usage where ease of use is more important than security.

Sound

Note: Only an administrator can change sound settings.

Selected sound is used when a fingerprint operations succeed or fail. You can use your default system sounds, disable sounds, or browse for your favorite audio file (.wav format).



TPM

Note: Only an administrator can initialize TPM module.

This page is displayed when a third-party TPM-management application is detected. TPM initialization enables usage of the TPM security module by the Protector Suite QL Advanced Security feature.

To initialize the TPM module:

- 1 Click the **Initialize TPM** button to run the TPM initialization wizard.
- 2 Click **Next** on the **Welcome** screen. The initialization is performed.
- 3 The result of the operation is displayed. If the operation succeeds, the Protector Suite QL is able to use the additional TPM security. Click **Finish** to close the wizard.

User Settings

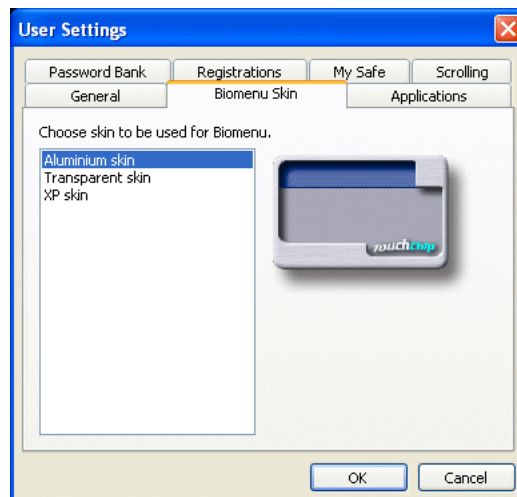
Note: Accessing the **User Settings** requires biometric verification.

General

Check the **Show icon in tray** check box to display the tray icon which gives you quick access to some Protector Suite functions. For a detailed description of the tray icon menu, see page 49.

Biomenu Skin

The Biomenu can be displayed in several designs - skins. Select your favorite one.



Password Bank

This page consists of two parts.

The **Hints** part is visible to all users. It contains settings that control when hints are displayed to inform a user about possible actions.

The second part is visible only to administrators. It is displayed in case you have installed Mozilla, Netscape, or Firefox. When Protector Suite QL detects Mozilla/Netscape/Firefox, it prompts the user whether to turn support on. Alternatively, the Mozilla/Netscape/Firefox support can be turned on here. If you want to enable the Password Bank's support for a browser, check the corresponding check box.

For more information, see page 28.

Registrations

This dialog lists all your existing registrations. Both the registered pages and dialogs are displayed.

For more information, see page 28.

Scrolling

You can use your sensor to scroll through various windows, e.g. long documents.

When you want to use fingerprint scrolling e.g. in a long document, press the selected scroll switch hotkey (this is not set by default, you must set it before the first use) to enable scrolling. When you are using the scrolling feature, you cannot use the sensor for invoking the **Biomenu** at the same time. To enable the standard Protector Suite QL behavior, you must press the hotkey again after you finish scrolling.

The **Scrolling** page allows you to adjust the speed and acceleration of scrolling and setting of the scroll hotkey. This hotkey turns the scrolling feature on/off. By default, no key is used.

- Move the **Speed** slider to adjust the speed of movement (*The faster your finger moves, the faster the scrolling. This setting controls how much faster*).
- Move the **Acceleration** slider to adjust the acceleration. (*The longer your finger moves in the same direction, the faster the scrolling. This setting controls how much faster*).
- Test your settings. Click the **Test Scroll** button and try your settings.

- *If you want to set/change the scroll switch hotkey, set focus to the corresponding field and press the desired key combination. Available hotkeys are listed in the dialog.*

My Safe

This page contains options for **My Safe** management. Information about **My Safe** status (locked/unlocked) and size (or free and used space, if **My Safe** is open) is displayed.

For more information, see page 32.

Application Launcher

Displays applications that can be launched by your fingerprints. The application launcher can contain up to (number of your enrolled fingerprints -1) applications.

For more information, see page 34.

Power-on security

The optional power-on security feature uses the computer BIOS to prevent unauthorized access to the computer. Computers that have the power-on security feature enabled will not load the operating system prior to successful fingerprint authentication at the BIOS level.

The computer will power-on only if the scanned fingerprint matches an enrolled fingerprint for the current user. After successful verification, the power-on process continues normally. If fingerprint authentication fails a specified number of times (depending on your BIOS) in a row, access is blocked and the computer must be restarted.

Enabling power-on security in the fingerprint software

The power-on security feature can be enabled in the fingerprint software in the power-on security wizard when power-on security is supported by your system. The power-on security feature is enabled by default.

To enable/disable the power-on security feature using the Protector Suite QL interface, complete the following procedure:

- 1 *Click **Start - All Programs - Protector Suite QL - Control Center**.*
- 2 *Click **Settings**.*
- 3 *Click **Power-on Security**.*
- 4 *Select the **Replace the power-on and hard drive passwords with the fingerprint reader** check box.*

- 5 *The power-on security implementation depends on your hardware. For more detailed information, click the **Learn more** link.*
- 6 *Click **Finish**.*

If enrollment to your hard disk is set, more options are available in the **Power-on Security** dialog. Fingerprints in the power-on security memory are listed in the **Authorized fingerprints for power-on security** window. You can remove fingers from the power-on security memory here.

Note: Changing a passport (adding or deleting a fingerprint) automatically adds or removes the fingerprint for power-on security use.

Enabling automatic logon of users verified by power-on security

The power-on security feature can also be set to log the user onto Windows. When this feature is enabled, if the power-on security fingerprint matches a fingerprint on an existing passport, the corresponding user is logged onto Windows automatically. This feature saves the user from having to authenticate twice when starting the computer: once for the power-on security feature and again to log onto Windows.

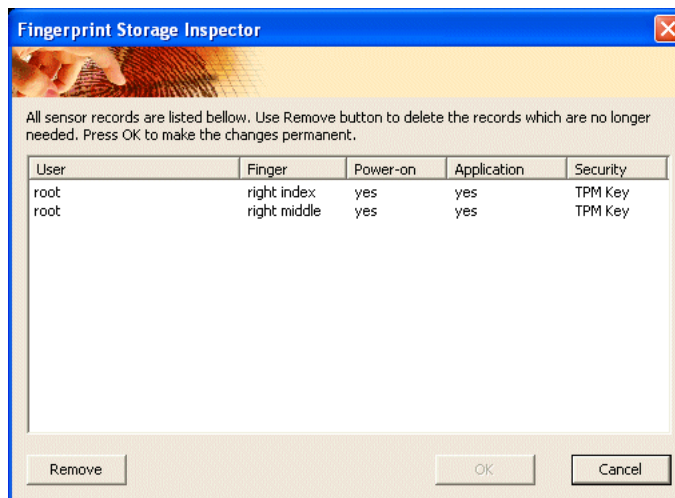
To enable automatic Windows logon of users verified by power-on security, complete the following procedure:

- 1 *Click **Start - All Programs - Protector Suite QL - Control Center**.*
- 2 *Click **Settings**.*
- 3 *Click **System Settings** and go to the **Logon** page.*
- 4 *Select the **Allow power-on security single sign-on** check box.*

Fingerprint Storage Inspector

The fingerprint storage inspector is a tool for viewing and editing the contents of the storage in your fingerprint reader device. All the records stored in your device are shown.

For each fingerprint, its description is shown together with information about its usage for power-on security (pre-boot authentication), applications (e.g. Logon), and advanced security status (TPM or no advanced security).



To remove fingerprints from the device:

- 1 Select the record you want to delete and click the **Remove** button. The list of records will be updated to reflect the change.
- 2 After you remove all unnecessary records, click the **OK** button to make the changes permanent or click **Cancel** to discard the changes.

Note: In the secure mode, only administrators can remove records. In the convenient mode, users can remove their own fingerprints, or fingerprints that are not included in any existing passport. At least one fingerprint must remain for each passport. To manage or delete the whole passport, use the **Enroll or Edit fingerprints** wizard.

Help

Introduction

All the basic Protector Suite QL features are summarized in the **Introduction** screen. Links from the dialog will guide you directly to the corresponding help topics.

Tutorial

To help you correctly use the fingerprint device, a tutorial is available where you can practice and learn the correct fingerprint scanning technique.

This tutorial can be run any time from the **Control Center**, or from the **Start** menu, **All Programs - Protector Suite QL - Fingerprint Tutorial**.

This tutorial shows a short video with samples of correct and incorrect fingerprint scanning technique. You will learn some hints about how to achieve the best possible quality of scanned samples.

You can try to create your first samples and watch the resulting images. This helps you to improve positioning of fingers, applied pressure, speed, and smoothness of scanning.

System Tray Icon

The Protector Suite QL icon in the system tray indicates that the program is running and gives access to functions that do not require fingerprint authentication.



Edit Fingerprints...

Opens the fingerprint enrollment wizard to register additional fingers. You can also launch this wizard from the **Biomenu** by selecting **Settings - Fingers**.

Start Control Center...

Starts the Protector Suite QL's Control Center.

Don't use sensor/Use sensor

Note: This feature is only for advanced users; e.g. developers of other biometric applications.

Allows you to detach Protector Suite QL from your fingerprint device. This command temporarily frees the device only for the current user session. (The device can be used only exclusively by one application at a time. This option is intended for cases where you plan to develop or use another biometric application and want Protector Suite QL to release the device.)

If you select the **Don't use sensor** option, no fingerprint verification is performed by Protector Suite QL.

Help

Displays the help system.

About

Displays information about the program and its version.

A hand is shown pointing at a fingerprint on a document. The fingerprint is a latent print, and the hand is pointing to it with the index finger. The document has a grid pattern.

Chapter 4

Troubleshooting

This chapter provides information for users who have difficulties when using Protector Suite QL.

Installation

I cannot install Protector Suite QL.

- *Check your privileges. User who installs Protector Suite QL must have administrator privileges.*
- *Check if there is enough free space on your disk. To install Protector Suite QL, you need approximately 40 MB.*
- *Check your system. Only Windows 2000 and Windows XP are supported.*

Protector Suite QL does not work after installation.

- *Reboot is required after you install Protector Suite QL.*

Fingerprint Enrollment

My device does not work.

- *Check the device connection.*
- *Check whether the driver is correctly installed. Drivers are normally installed during Protector Suite QL installation. However, if there are some problems, necessary drivers can be found in the **Drivers** subfolder of your installation folder. For device-specific driver installation, consult Readme.txt in the **Drivers** folder. (To check the device status, right-click **My Computer**, select **Properties** - **Hardware**, and open the **Device Manager**.)*

I cannot enroll my fingerprints. My fingerprints are not correctly recognized.

- *Go through the fingerprint tutorial to learn how to create good samples. The fingerprint tutorial can be run as a part of fingerprint enrollment, or separately, from the **Start** menu.*
- *Try harder/softer pressure on the sensor.*
- *Try to change the speed of swiping.*
- *Clean your sensor. Use a damp lint-free cloth (use water or fragrance-free moisturizing lotion), and gently rub the cloth across the sensor. Do not use any abrasive materials.*
- *Try to wipe your finger. (Especially in hot weather.)*
- *Try to use another finger. The index-finger is usually easier to enroll than your little-finger.*

I cannot use fingerprint authentication because my only enrolled finger is injured. I want to enroll another finger.

To be able to fully use Protector Suite QL, you need to have usable enrolled fingerprints. It is strongly recommended to enroll at least two fingers to avoid this problem!

To update enrolled fingerprints, you need to enter the **Enroll or Edit Fingerprints** wizard.

- *If you do not use Advanced Security, you can enter using the Windows password.*
- *If you use Advanced Security with backup password, you can enter using the backup password.*
- *If you use Advanced Security without backup password, there is unfortunately no way how to add a different fingerprint. In this case we recommend to either wait until your finger is usable again (e.g. the injury heals), or to delete the passport (**Delete** wizard) and then re-enroll new fingerprints. Please note that in the latter case all your stored secret data (passwords, encryption keys) will be lost! To perform the delete operation it is necessary to cancel the fingerprint verification operation to get to the password dialog, then enter your Windows password.*
- *If **Fingerprint Reader Key** or **Fingerprint Reader Key with TPM** is set as an Advanced security type, you will be asked at the end of the enrollment to swipe your original finger to unlock secrets on the device. As you cannot do so, you have to disable the Advanced Security before exiting the wizard. After you exit the wizard, you can enter it again using the newly enrolled finger and then enable Advanced Security again. These steps are necessary to create a new set of keys connected to the new fingerprint.*

I was prompted to swipe my finger again after I finished the enrollment process. Why?

The prompt is displayed in cases when the Advanced security backup password was used to enter the **Enroll or Edit fingerprints** wizard, **Fingerprint Reader Key** or **Fingerprint Reader Key with TPM** is set as Advanced security types, and you added a new fingerprint to your passport.

- *This behavior is normal. This verification is necessary to create new sets of keys connected to the new fingerprint.*

I cannot enroll a user in the secure mode.

- *Check for the existence of the user passport. The user is probably already enrolled. Every user can have only one passport.*

User import does not work.

- *Check for the existence of the user passport. If you want to import data for an existing user, you must first delete the old passport.*
- *Check your device memory in the **Fingerprint Storage Inspector (Control Center - Settings - Fingerprint Storage Inspector)**. (Only if enrollment to the device is used.)*

Why should I export user passport?

Exported data contain fingerprint information, logon credentials, Password Bank registrations, encryption info for My Safe (but not My Safe data).

- *Export user data regularly as a backup of all this information.*

I lost my Advanced Security backup password

- *To change the Advanced Security backup password, go to the **Enroll or Edit Fingerprints** wizard, swipe your finger and go through the Fingerprint enrollment. On the Advanced Security page, you can change the backup password.*

I need to replace my sensor.

If you need to replace a non-functional fingerprint sensor or reader, follow this procedure:

Enrollment to the hard disk:

- *When enrollment to the hard disk is used, Protector Suite QL does not store any data on the device; therefore no action needs to be taken after replacing the sensor. In case that you use the Power-on security (Preboot Authentication), you may need to use the **Enroll or Edit Fingerprints** wizard to update the related data.*

Enrollment to the device:

- *There is a connection between your passport and your fingerprint device requiring that you replace the current passport with your previously exported passport.*

You can restore your passport by importing its backup to the new device:

- 1 *Delete your passport.*
- 2 *Connect the new (functional) device.*
- 3 *Import your passport from a backup file.*

Switching external readers:

- *The above described procedure applies also if you try to use multiple fingerprint readers with Protector Suite QL (e.g. one internal and one external, or swapping two external readers). If you use enrollment to the hard disk, there is generally no problem with the possible exception of the Power-on security (Preboot Authentication). If you use enrollment to device, you should not swap the readers unless you have a good reason, and you have to delete and recreate your passport.*

When enrollment to device is used and the reader contains data (from a different/previous Protector Suite QL installation) of a user which exists on the computer (and is not enrolled yet), a prompt is displayed whether to re-use this data.

If the new reader contains the data of a user who has been already enrolled, the data cannot be re-used. Instead, fingerprints are deleted from the device for security reasons (to avoid injecting fingerprints belonging to unverified persons).

My TPM module does not work.

If you use Advanced Security with TPM (Trusted Platform Module) and the TPM module is broken, erased or disabled, the Advanced Security will no longer work.

If you set the Advanced Security backup password, you can follow these steps:

- 1 *Enter the **Enroll or Edit Fingerprints** wizard using the backup password.*
- 2 *Disable Advanced Security and finish.*
- 3 *After the TPM is repaired, enabled, or if it was erased, you can enter the **Enroll or Edit Fingerprints** wizard again using your finger and re-enable the advanced security with TPM.*

Fast User Switching

Fast User Switching cannot be enabled.

This option is visible only on computers running Windows XP. The Fast User Switching feature can be used only on computers which are not members of a domain.

- *Verify that your computer is not in a domain.*
- *Installation of other software (e.g. Novell Client) can prevent Fast User Switching.*

Logon

I cannot log on using my user name and password.

- *Check the security mode. Logon using user name and password is possible for all users only in the convenient mode. In the secure mode, only administrators have this option.*

I cannot change Protector Suite QL System settings, although they are visible in the Control Center.

- *Check your user privileges. Only local administrators can change the **System settings**. Being the local administrator is not the same as membership in the **Administrator's group** of Protector Suite QL. Members of this group can manage passports, fingerprints, power-on security, and also log on using user name and password.*

Password Bank

Registered pages are replayed in Internet Explorer after a delay

Registrations are replayed (and can be made) only after the page is fully loaded.

Unfortunately, Internet Explorer sometimes incorrectly indicates that the page is already loaded (the animation in the upper-right corner is stopped), although the page is not loaded yet. If the user presses Stop to finish loading, IE sometimes ignores the command and does not stop. In such situations, please wait until the page load is complete. The same problem may occur with pages where mouse over some active item (e.g. Flash animation) starts loading the object, although the page has already been loaded.

- *Wait until the page is fully loaded.*

I cannot register a page which is already registered. Swiping a finger triggers replaying.

- *Press **SHIFT** when swiping your finger to register an already registered page or dialog (instead of replaying the registration).*

The Password Bank cannot register my dialog.

The Password Bank cannot correctly handle dialogs which do not contain standard controls. Examples include dialogs from Microsoft Office.

- *The Password Bank is intended primarily for simple standard dialogs containing user name and password. Complex and non-standard dialogs may cause problems.*

My registration is not replayed correctly.

- *The Password Bank replay expect that the page used for replaying is exactly the same as it was when the registration was created. Therefore you may encounter problems with pages created dynamically using JavaScript, or with forms which look the same, but differ internally.*

My Safe

I cannot start work with My Safe.

My Safe creation cannot complete when antivirus programs are active. This problem exists e.g. with Norton AntiVirus, or Sophos.

- *Set your antivirus program to ignore My Safe.fdp file. **My Safe** is stored in an encrypted form and therefore scanning its contents makes no sense.*

I cannot access My Safe using fingerprints.

- ***My Safe** can always be accessed using **My Safe** backup password.*

My Safe remained open (unlocked).

My Safe folder is closed automatically on logoff or shutdown. However, if you only lock your computer, close your file browser, or remove your biometric device, **My Safe** remains open.

- *It is always a good idea to close (lock) **My Safe** when you finish your work with stored data.*

I want to use My Safe in a different Protector Suite QL installation

- *It is possible to copy MySafe.fdp to another computer. However, as your authentication information (e.g. fingerprints, encryption keys) are unique for every installation, you will need the **My Safe** backup password. This backup password is defined when creating **My Safe**.*

I lost My Safe backup password.

My Safe backup password cannot be changed directly. It is necessary to create a new **My Safe**.

To create a new My Safe without losing your data:

- 1 *Unlock **My Safe**.*
- 2 *Copy the data from **My Safe** to some other folder.*
- 3 *Delete **My Safe** from **Control Center - Settings - User Settings - My Safe**.*
- 4 *Create a new **My Safe** and define the new **My Safe** backup password.*
- 5 *Copy your data back to the new **My Safe**.*

After I unlocked My Safe using the My Safe backup password, I cannot use some of My Safe features.

- *Using the backup password gives you only an emergency access to your data. It is not meant as a standard way of unlocking **My Safe**. Either access **My Safe** by using the fingerprint verification, or if you cannot do so, backup your data and create a new **My Safe** as described in the previous problem.*

My computer crashed. I want to restore data from My Safe.

In case of a computer or OS crash it is still possible to access My Safe data, assuming that the My Safe data file can be recovered. The data file is placed in "C:\Documents and Settings\<username>\Application Data\Protector Suite\My Safe.fdp".

- *On a target recovery system, place My Safe.fdp file into the same folder and install Protector Suite QL. If you have an exported passport, import it now and you can access **My Safe** directly using fingerprints. Otherwise you can access **My Safe** using the My Safe backup password: **My Safe** will recognize that the installation has changed and will offer to use the backup password.*