PROTECTOR SUITE QL

version 5.8

Copyright Notice and Proprietary Information

UPEK®, Inc

http://www.upek.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 (eay@cryptsoft.com).

Trademarks

Chapter 1
Installing Protector Suite QL

Installing Protector Suite QL

Protector Suite QL can be installed on any computer with Windows 2000, Windows XP Home or Professional edition, Windows Vista and with a free USB port. Administrator rights are required to install or uninstall Protector Suite QL. If you have Protector Suite QL already preinstalled on your computer, you can skip this paragraph.

To install Protector Suite QL:

1. *When the Protector Suite QL autorun window is displayed, click on **Software Installation.** If this screen does not appear, run **Setup.exe** or **Setup.msi** manually.*
2. *Click **Next** to continue.*
3. *Confirm or click the **Browse** button to select another installation folder.*
4. *Ready to Install the Application dialog appears. Click **Next** to start the installation. During the Windows Vista installation, you may be prompted to confirm to continue with the installation.*

5 *When the installation has completed, click on the **Finish** button.*

6 *Click on **Yes** to restart your computer when prompted. You must reboot your computer before you begin to use Protector Suite QL.*

The installation is now completed. After you restart the computer, the fingerprint logon to Windows will be enabled. You must enroll your fingers to start using the software. See "Fingerprint Enrollment" on page 14.

Note: During installation, all necessary device drivers are installed. If you intend to use an external fingerprint sensor, we recommend that you connect it after completing the installation and restarting your computer.

Uninstalling Protector Suite QL

To uninstall Protector Suite QL:

1 *Click **Start > Control Panel***

2 *Double-click the **Add or Remove Programs** icon (**Programs and Features** in Windows Vista).*

3 *Select Protector Suite QL and click the **Change** button.*

4 *Click the **Remove** button.*

5 *You will be asked what to do with Protector Suite QL's data stored on your computer. There are two possibilities:*

- ***Leave Protector Suite QL data for later use** on your computer. This means that if you later re-install Protector Suite QL, You can continue using enrolled fingerprints for logging to your computer.*
- ***Remove all Protector Suite QL data** from your computer.*

Enrolled fingerprints will be permanently deleted.

6 *Click **Next** to continue.*

7 *Uninstall dialog is displayed, click on **Next** to confirm you want to continue with the uninstallation. Click **Cancel** to quit the uninstallation.*

8 *When uninstallation is completed, click on **Finish.***

9 *Click **Yes** to reboot your computer.*

Chapter 2
Getting started

Protector Suite QL is biometric software that protects the security of your data through the use of fingerprint verification. For greater security, fingerprint verification can be combined with different methods of user authentication (such as a smart card and PIN or your Windows password). Fingerprint verification is performed by swiping your finger over a fingerprint sensor.

After installing the software and restarting your computer you will need to enroll your fingerprints to create an association between your username, password and your fingerprints together with automatically generated security keys. During this process you need to choose the way you will authenticate to the computer (with fingerprint verification only or in combination with other methods, i.e. multifactor). All the data is stored in the user *passport*. This procedure is called **Fingerprint Enrollment.**

After you enroll your fingers you will be able to:

- *use the fingerprint sensor to securely manage both "pre-boot level" and Windows OS logon (see Chapter 3, “Fingerprint Logon”, on page 23)*
- *register web pages and Windows applications for password replacement (see Chapter 3, “Password Bank”, on page 27)*

- *launch your favorite application just by swiping your finger over the sensor (see Chapter 3, “Application Launcher”, on page 35)*
- *store confidential information in an encrypted form in a protected folder (see Chapter 3, “File Safe”, on page 38)*

This chapter will give you an overview of the main features of the software to help you to get started quickly. For a detailed description of all functions, refer to Chapter 3, “Using Protector Suite QL”, on page 13 and for a description of how to control and manage Protector Suite QL, refer to Chapter 4, “Managing Protector Suite QL”, on page 55).

 **Note:** Each Windows user must have a Protector Suite QL unique passport.

Fingerprint Enrollment

Each user identity in Protector Suite QL is represented by a “passport”, which contains biometric fingerprint data used to verify the identity of the user.

Before using the software for the first time, fingerprint samples for your passport must be created.

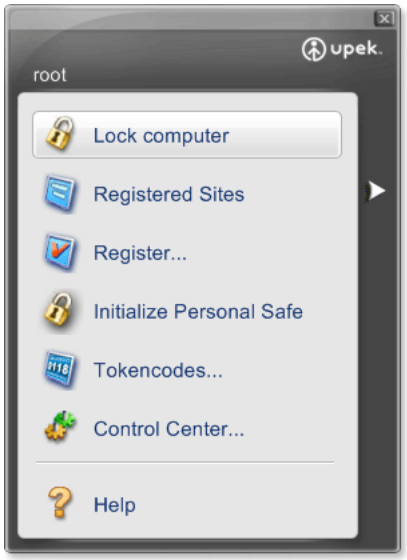
▶ To launch the Enrollment Wizard:

- *Select **Start > All Programs > Protector Suite QL > User Enrollment***

Verify yourself (Windows password will be required, if you have one) and choose a method of verification you would like to use (fingerprint only, fingerprint and a smart card etc.). For more information, please refer to Chapter 3, “Fingerprint Enrollment”, on page 14.

Accessing Main Features

The Biomenu



The **Biomenu** gives you a quick access to Protector Suite QL's features, such as locking your computer, launching registered sites and register web sites and dialogs, locking archive files or displaying **Help.**

To display the Biomenu:

- *After you have enrolled at least one finger, swipe it over the fingerprint sensor and the **Biomenu** will be displayed.*

Please refer to Chapter 4, "Biomenu", on page 79 to learn about the Biomenu items.

The Control Center

You can access the general **Settings** of Protector Suite QL and the **Fingerprints** management features (e.g. editing and deleting passports) in the **Control Center** dialog.

To display Control Center:

- *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center***
- *or swipe your finger to display the **Biomenu** and select **Control Center***
- *or right-click on the tray icon and select **Start Control Center...***

The Control Center main screen is displayed. In this dialog, the main functions of Protector Suite QL are displayed. Click the function name to display a screen listing the valid actions available. The functions include **Fingerprints**, **Applications, Settings**, and **Help**.

To learn more about the Control Center and its functions, please refer to Chapter 4, “Control Center”, on page 56.

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.

Right-click on the icon to display the menu:

To learn more about the System Tray Icon menu items, please refer to Chapter 4, “System Tray Icon”, on page 80.

Using Help

Protector Suite QL contains an HTML-based help system.

To display HTML help:

- *Select **Start** >**All Programs** > **Protector Suite QL** > **Help***
- *or select **Help** from the **Biomenu**,*
- *or right-click on the tray icon and select **Help***
- *or click on the Help icon in the Control Center dialog*

Displaying context-sensitive help is also available in most dialogs.

To display context-sensitive help:

- *Press F1 to display the HTML help in the dialog box for which you need help.*

Chapter 3
Using Protector Suite QL

This chapter describes features of Protector Suite QL in detail:

Fingerprint Enrollment

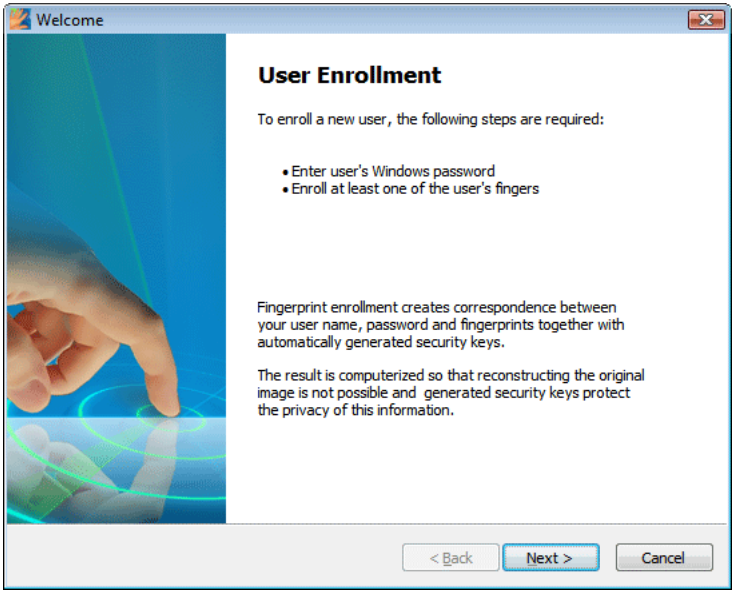
Before you can start using Protector Suite QL, you must *enroll* your finger or fingers. Fingerprint enrollment is a process of creating correspondence between your username, password and your fingerprints (computerized so that reconstructing the original image is not possible) together with automatically generated security keys. All the data is stored in your fingerprint *passport*.

For greater security, fingerprint verification can be combined with a smart card and PIN verification or in combination with your Windows password. You will be able to select a method for verification (e.g. fingerprint + a smart card, etc.) before you create your passport, i.e. enroll at least one finger.

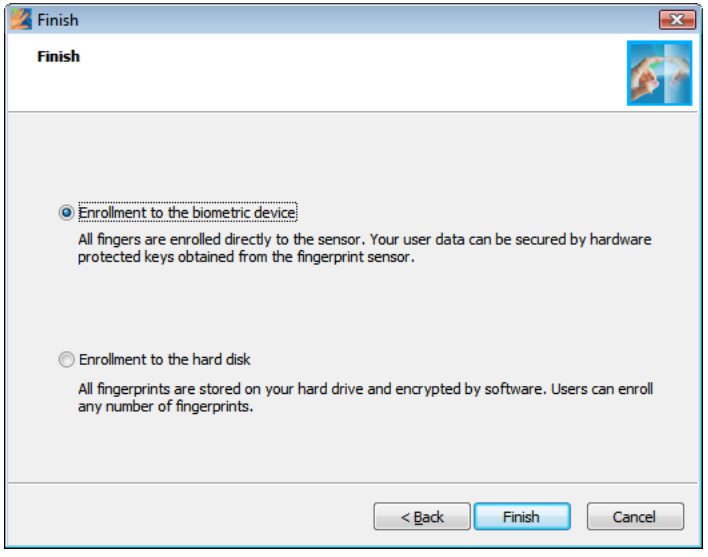
First Use

To create a new passport (enroll fingerprints):

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.*
2. *To launch the Enrollment wizard, go to*
   - ***Start > All Programs > Protector Suite QL > User Enrollment***
   - *or select* ***Fingerprints > Initialize*** *in the* ***Control Center***
   - *or right-click on the tray icon and select* ***Edit Fingerprints...***
   - *or swipe over the sensor, and click on* ***Start Fingerprint Enrollment*** *link in the* ***Starting Page.***
3. *The License Agreement is displayed. Read the License Agreement carefully.*
4. *Accept the License Agreement by selecting the appropriate radio button. You must agree to the License Agreement to install this product. Click* ***Cancel*** *to close the application if you do not agree to the Licence Agreement.*



5 *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.*



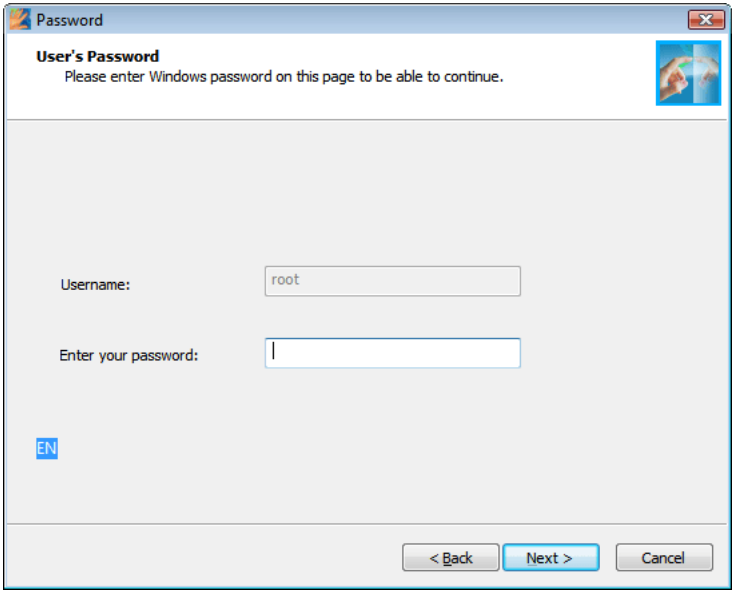
• If you select enrollment to your device memory, your data cannot be accessed without the corresponding fingerprint device. Authentication information will be protected by a software encryption key generated by your fingerprint software together with a hardware encryption key obtained directly from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

• The only limitation is size of the device memory. If you plan to enroll a larger number of fingerprints for several users, 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.

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

---

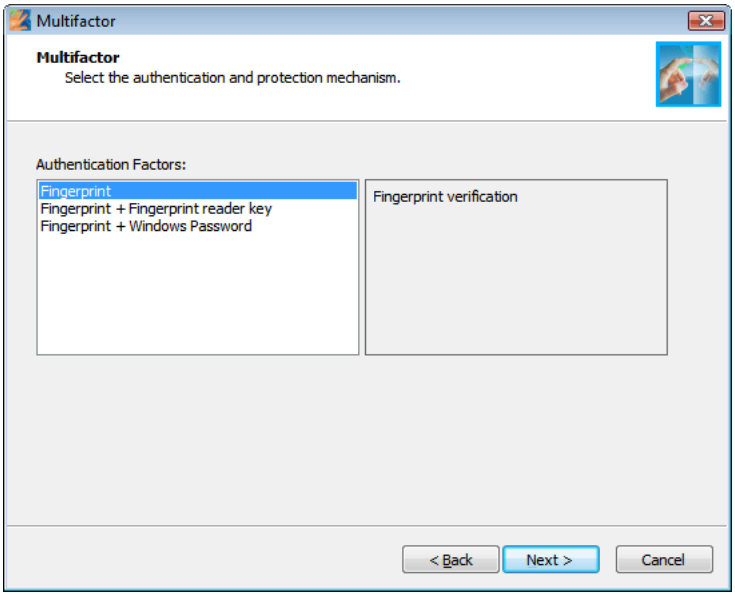
6 *Enter your username, password, and domain (if applicable) and click **Next**.*



7 *The **Multifactor** dialog appears. Security of Protector Suite QL can be increased with additional encryption. The types of encryption available depend on your hardware.*

Multifactor methods

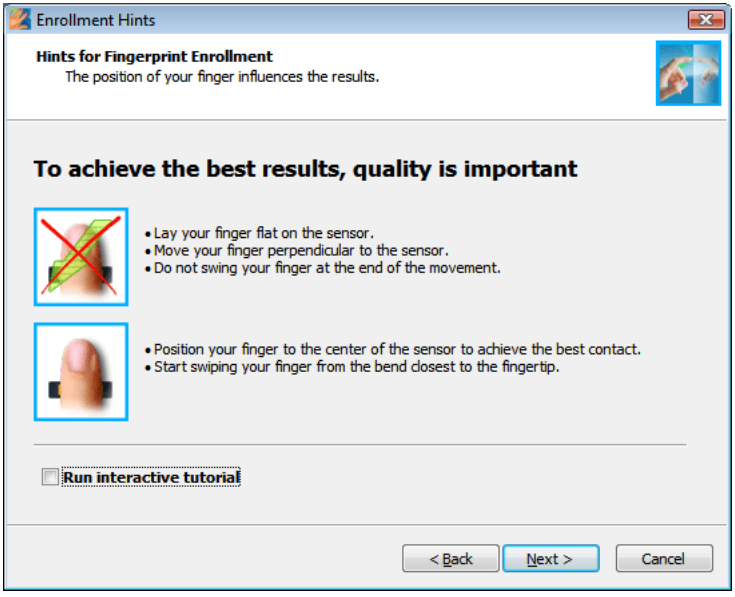
Choose a method of authentication. Next time you are prompted for verification, the selected method will be required (e.g. logging to you computer, registering web pages etc.). This will apply for all enrolled fingers.



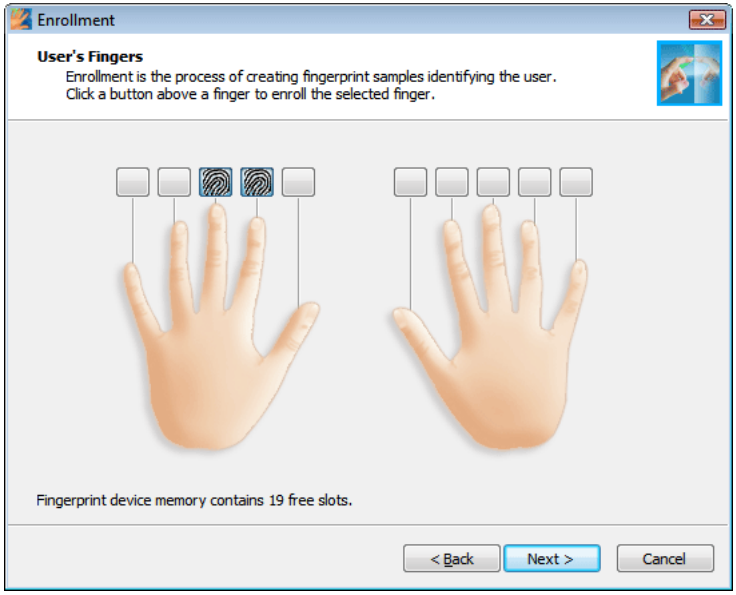
- ***Fingerprint:*** *Only fingerprint verification will be required.*
- ***Fingerprint + Fingerprint reader key:*** *User secret data is encrypted using a key stored in the fingerprint device and accessed only after successful fingerprint verification. You may use a backup password in the event of injury or a device problem. If you do not define the backup password, you can loose your data in the event of authentication hardware failure.*
- ***Fingerprint + Smart Card:*** *Both fingerprint verification and insertion of the registered smart card are required. Enter a backup password in the event of injury or a device problem. In the next dialog, select a smart card reader and insert the card. Enter a PIN that will be saved and automatically replayed during verification.*
- ***Fingerprint + Smart Card + PIN:*** *This combination enhances security of the former method by prompting the user to enter their PIN each time verification is required. Enter a backup password in the event of injury or a device problem.*

- ***Fingerprint + Windows password:*** *Fingerprint verification and entering the Windows password will be required for each verification.*
- ***Fingerprint + TPM with Fingerprint reader key:*** *Improved hardware-based security. Encrypted channel between TPM security chip and fingerprint reader further enhances security of user secret data. Recommended for highest security.*
- ***Fingerprint + TPM Key:*** *User secret data will be protected by the TPM security chip. Recommended for higher convenience.*
- ***Fingerprint + 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.*

8 *Click **Next** to choose whether you want to proceed with the fingerprint tutorial or skip it by unchecking the **Run interactive tutorial** check box and click **Next** to skip the tutorial (see "Fingerprint Tutorial" on page 20 for tutorial instructions).*



9 *Click on a box above the finger you wish to enroll.*



Create five scans of the selected finger according to the instructions in the tutorial (see “Fingerprint Tutorial” on page 20). These samples will be combined into a single fingerprint passport. A warning is displayed if the created samples cannot be matched and you will have to repeat the procedure.

10 *(Optional) If enrollment to the device was selected and your system configuration supports power-on security, all enrolled fingerprints will be also used for power-on security.*

11 *(Optional) If enrollment to hard drive is selected and your system configuration supports power-on security, enrolled fingerprints will be also used for power-on security.*

The device memory is limited. If some of the enrolled fingerprints in the passports are not assigned for power-on security in the device (e.g. another device is connected), ***Power-on*** *button is displayed above each finger. The Power-on button is displayed in a "depressed" state by default. The corresponding finger will be used for power-on security. If you do not want to use a finger for power-on security, but only for logon, click the Power-on button to delete it from the device memory.*

12 *(Optional) 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 or changed.*

13 *Select another finger to enroll. You can enroll up to 10 fingerprints. **It is strongly recommended that you enroll more than one finger in the event of injury.** Click **Next** when done.*

14 *For fingers added for power-on security, you must perform operations described on the final page:*
- *Power-off your computer.*
- *Turn on your computer.*

15 *When you are done, click **Finish.***

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

Introduction

The Starting Page is shown when you swipe your finger over the sensor when no fingerprints are enrolled. It contains a link to the Protector Suite QL product tour and a link to fingerprint enrollment. It can be accessed later from **Control Center** > **Help** > **Introduction.**

Fingerprint Tutorial

It is highly recommended that you go through the fingerprint tutorial. The tutorial will show you a short video demonstrating correct and incorrect fingerprint scanning. Then you will try to create your first fingerprint samples.

To run the tutorial:

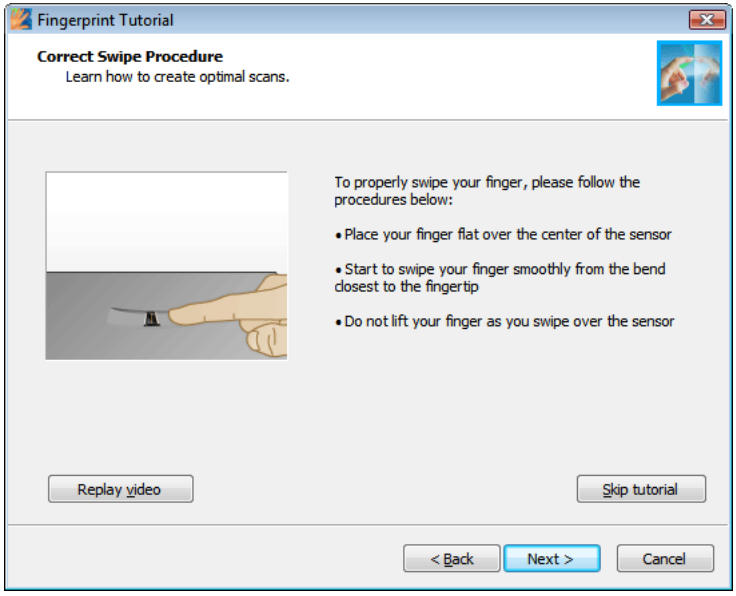
1 *To launch the tutorial go to* **Start > All Programs > Protector Suite QL > Fingerprint Tutorial.**

or run it from the fingerprint enrollment wizard

*or select **Help > Tutorial** in the **Control Center** dialog.*

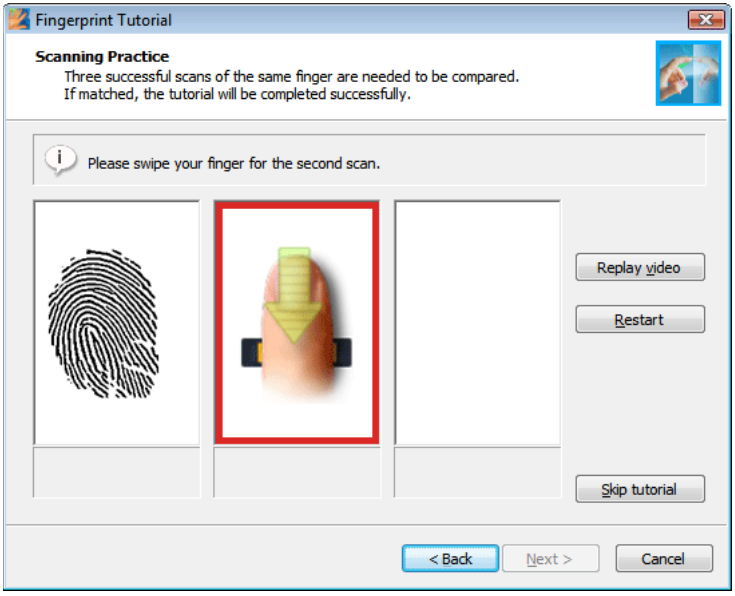
2 *The opening page explains the purpose of the tutorial.*

3 *The next page explains the correct scanning procedure and shows a short video demonstration:*



- *Place your finger flat over the center of the sensor.*
- *Start to swipe your finger smoothly from the bend closest to the fingertip.*
- *Do not lift your finger as you swipe over the sensor.*

4 *In the next page, try creating samples of your fingerprint. If the samples do not match, we recommend that you click the* ***Restart*** *button to repeat the scanning. Use the* ***Replay video*** *button to replay the video demonstration. After you successfully create your samples, click* ***Finish*** *to close the tutorial or to go back to the enrollment wizard.*



Fingerprint Logon

To enable fingerprint logon, you must enroll your fingerprints (see “Fingerprint Enrollment” on page 14). During user enrollment, fingerprint samples are scanned and the connection between fingerprint samples and the Windows user account is created. When you restart your computer and wish to log on again, the logon dialog will prompt you to verify yourself. You can bypass the fingerprint verification by pressing **Ctrl + Alt + Del** to log on using the Windows password.

Biometric logon also protects your screensaver and wake-up from power-saving features (password protected resume from screensaver and standby must be set on your system).

To set the screensaver password go to **Start > Control Panel**, click on **Display** and select the **Screen Saver** tab.

If you are using Windows Vista go to **Start > Control Panel** > click on the **Personalization icon** and then the **Screen Saver** icon.

To disable Fingerprint Logon:

- *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center***
  *or swipe your finger to display the **Biomenu** and select **Control Center***
- *Select **Settings > System Settings > Logon***
- *Select the **Standard Windows logon** radio button. The fingerprint logon will be disabled and you will log on into your system using the standard Windows logon.*

To enable Fingerprint Logon:

- *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center***
  *or swipe your finger to display the **Biomenu** and select **Control Center***
- *Select **Settings > System Settings > Logon***
- *Select the Fingerprint Logon radio button and the system logon using your fingerprint instead of the Windows password is now enabled.*

For more information about the Logon settings, please refer to Chapter 4, Control Center, “Logon” on page 64.

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.

Protector Suite QL also interoperates with the Novell network logon. In order for Protector Suite QL to log you on automatically to a Novell network, your Windows username and password must match your Novell username and password. The following Novell clients do not work with Protector Suite QL: 4.83, 4.90.

Fast User Switching

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

To enable Fast User Switching (FUS):

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center***
2. *Select **Settings** > **System Settings**.*
3. *Select the **Logon** tab.*
4. *Windows XP only: Select the **Enable Fast User Switching** option. If this option is not visible, your system does not support FUS (e.g. your computer is a member of a domain. To enable FUS support, you must remove your computer from the domain.).*

To remove a computer from a domain:

1. *Right-click **My Computer** (**Computer** in Windows Vista) on your Desktop or in the **Start** menu and select **Properties.***
2. *In Windows Vista click the **Change settings** link and authorize yourself as an administrator.*
3. *Select the **Computer Name** tab.*
4. *Click the **Change** button (or **Rename**) and select the **Workgroup** radio button in the **Member of** pane.*

Note: Only an administrator can remove a computer from a domain.

Windows Password Change (Reset)

The Windows logon password can be changed both by a user (through the control panel or the **Ctrl+Alt+Del** dialog) or by an administrator (through password reset). There is no difference between both types of password change with respect to Protector Suite QL. The scenarios differ according to what type of user account is used and the way users log on to their computers.

This applies to Windows 2000 and XP (on Windows Vista the functionality is similar, but a different GUI is displayed).

When a local user account is used on a computer in a workgroup or in a domain, there are two possible scenarios:

1. *A user logs on using the Windows username and password and the password is then changed.*
   - *The user locks the computer or logs off.*
   - *The user swipes an enrolled fingerprint.*
   - *A warning is displayed that a wrong username or password is used is displayed.*
   - *The user must enter the new password. This password is then stored into the fingerprint passport, the passport is updated and the user is logged on to the computer. The fingerprint logon will proceed as usual the next time.*
2. *A user logs on using an enrolled fingerprint and the password is then changed.*
   - *The password is stored into the fingerprint passport. There is no need to enter the new password again later.*
   - *The user locks or logs off*
   - *User swipes enrolled fingerprint*
   - *The computer is unlocked or the user is logged on*

When a domain user account is used in a domain:

User logs on using the Windows username and password or an enrolled fingerprint. The password is then changed.

- *The user locks the computer or logs off.*
- *The user swipes an enrolled fingerprint.*

• A warning is displayed that a wrong username or password is used is displayed.

• The user must enter the new password. This password is then stored into the fingerprint passport, the passport is updated and the user is logged on to the computer. The fingerprint logon will proceed as usual the next time.

Special cases:

“User must change password at next logon” is set or password expiration is defined on domain.

• On a client computer a user logs on using an enrolled fingerprint.

• A dialog prompting the user to change their password will appear. This password is then stored into the fingerprint passport, the passport is updated and the user is logged on to the computer. The fingerprint logon will proceed as usual the next time.

Important: If you change your Windows username, your Protector Suite QL user passport will be deleted (i.e. your enrolled fingerprints) and you will be able to access you encrypted files only by entering your backup password and web registration by importing them in case you have created a backup.

Password Bank

Password Bank is an optional feature of Protector Suite QL. When installed, the Password Bank stores registrations (usernames, passwords and other settings) of your web sites and application dialogs so that you can access frequently visited web sites & applications (web mail, bank accounts, e-commerce, etc.) securely, without the hassle of re-entering usernames, passwords and form data. You enter the required information only once, during web page or password dialog registration. When the window is displayed again, you can replay the data by using the sensor. Registered web sites can also be accessed directly from the Biomenu.

The Password Bank supports the following browsers: Internet Explorer 5.0 and higher, Firefox 1.0 - 2.0. Support for Internet Explorer is installed automatically. When Protector Suite QL is started for the first time or without any fingerprints enrolled, a prompt is shown whether to install a Firefox plug-in to turn the support on. Alternatively, the Firefox plug-in installation can be run from the **Control Center** > **Applications** > **Password Bank** > **Alerts** tab.

Note: Registration of 32bit applications running on 64bit systems is not supported.

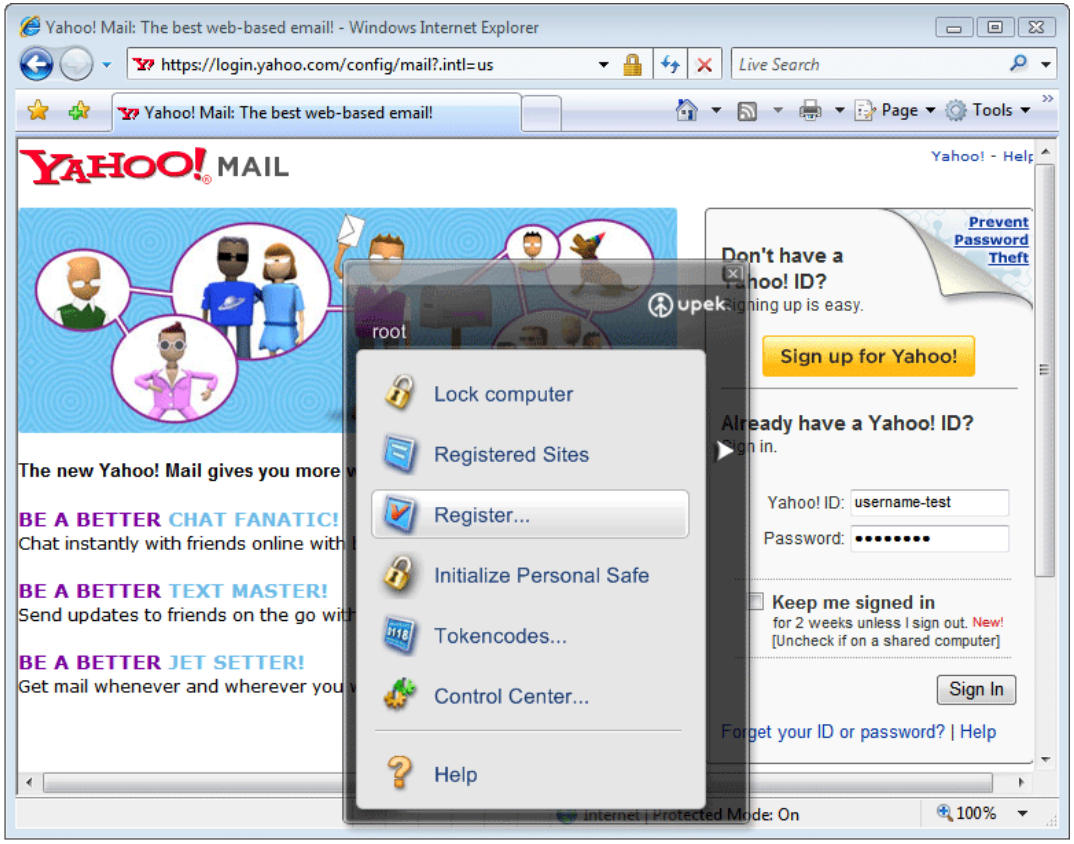
(Windows Vista only.) If user account name is "Administrator" (Note: this is built-in account, which is by default disabled), Internet Explorer is not supported with **Password Bank**.

Registering Web Pages and Dialogs

You must register a web site or a dialog to store registrations (usernames, passwords and other settings) of your web sites and password dialogs so that it can be later replayed, i.e.automatically filled in after you verify yourself (swipe your finger over the sensor).

To create a new registration:

1. *Display a web page or a dialog you want to register.*
2. *Populate the username, password, and any other necessary fields.*
3. *Swipe your enrolled finger over the sensor to display the **Biomenu**. Select **Register**.*
   OR
   *For Web pages containing a password field, a dialog appears automatically on submit asking you whether you want to register the entered data with Password Bank. Click **Yes.***



All your data is stored. After creating a registration, a hint is displayed in the corner of your browser confirming your registration has been created.

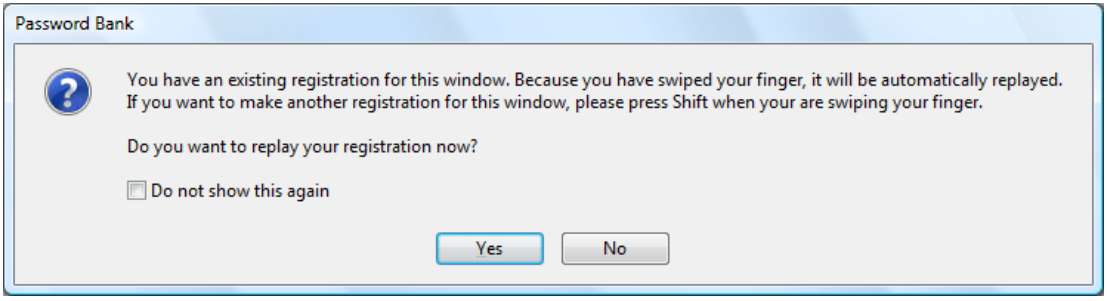
Note: If you would like to turn these hints on/off, or you have turned off the dialog promoting you for registration and would like to turn it back on, see “Turning Password Bank Hints On/Off” on page 33.

Replaying Registrations

Replaying a registration will launch the registered web site and automatically log you on using the registered credentials.

To replay a registration:

1. *Display the registered dialog or web site.*
2. *Verify yourself.*
3. *(Optional)A Password Bank dialog appears informing you that submitting the registration is available. Click **Yes** to replay the registration. Check **Do not show this again** to skip this step next time.*

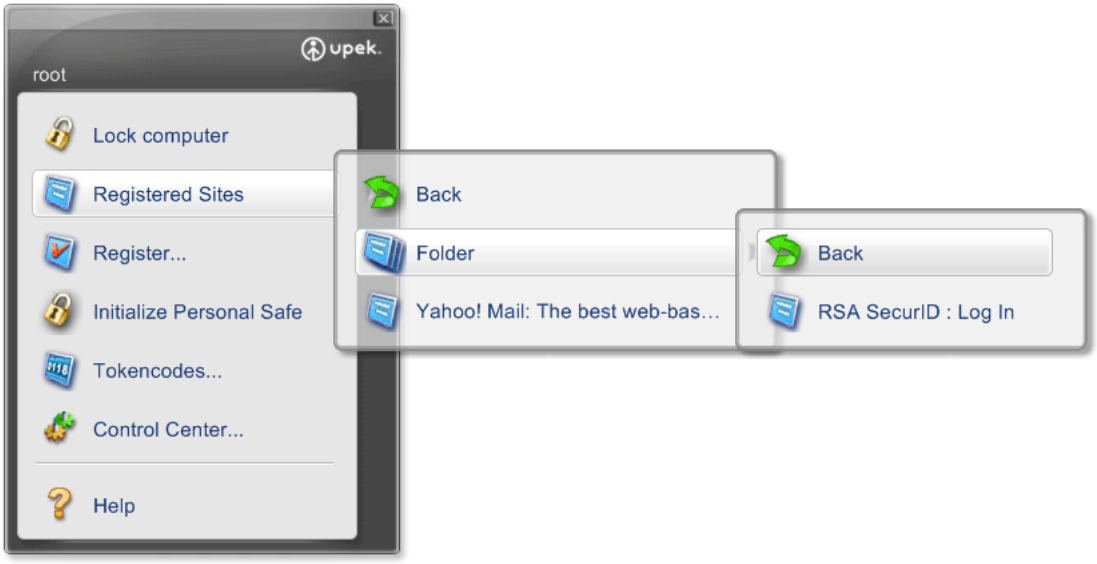


4. *The registration is replayed.*

To launch a registered web site, you can also use the Biomenu.

1. *Swipe your finger to display the **Biomenu.***
2. *Select **Registered Sites.** A list of registered sites will display.*
3. *Select a page you want to display and replay.*

4 *Browser border flashes magenta when the page is loaded and this registration is being replayed.*



Registering Web Sites and Dialogs with Several Forms

Registering web sites with several forms

Password Bank registers individual forms. If a site contains several forms, each form requires a separate registration. This means that only a form that is active 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.)

- *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 over 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 over 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 over the sensor. You will be prompted to select the target form for registration.

D. You have just filled in form A and clicked outside the form so that no form is active, but you are using earlier version of IE. No action is taken.

Replaying Web Sites Registrations with several forms:

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 over the sensor.

- *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 of the registered forms is active, this form is replayed.*
- *If there is no active form, all the existing registration for the page are offered for replay.*

Registering and Replaying Complex Dialogs

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

More complex dialogs may not be supported. 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 use 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 controls before they are used, but only draw them. The typical examples are some of the 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.

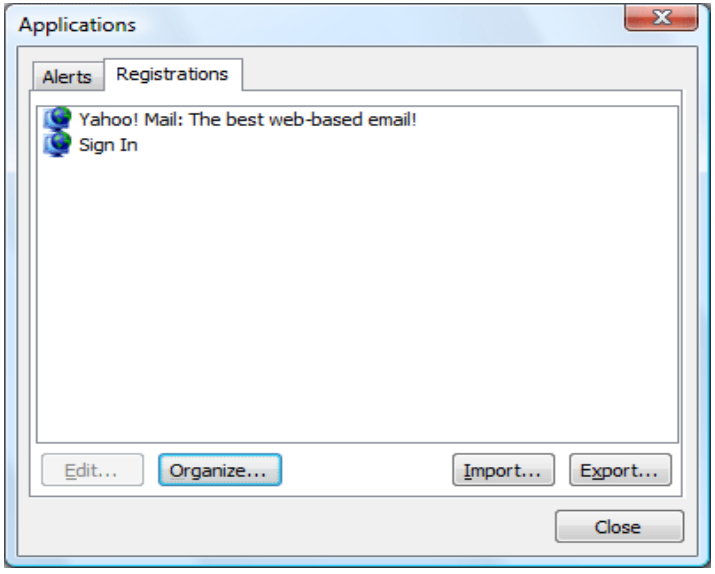
Managing Your Registrations

It may be useful to edit your existing registration - e.g. if your company's mailbox has changed and you want to update your registrations. You can also delete your registration or turn on/off automatic submission of replayed registration. You can export your registration for use on another computer. An exported registration is a file with a ***.pb** extension and can be imported later. If you want to organize your registrations into folders, you will be able to do it in this dialog tab as well.

To manage registrations:

1 *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center***

2 *Select **Applications > Password Bank**. Authentication is required.*



3 *Select the **Registrations** tab.*

4 *Select a registration you want to work with.*

*• Click the **Edit...** button to change the stored registration details (e.g. your username or password have changed and you want to reflect this in the existing registration.) The **Auto submit form** check box controls*

automatic submission of the form after replaying the registration. If checked, the registration will be replayed automatically after you verify yourself. If unchecked, a dialog will appear asking you to confirm the replaying. This will happen each time you access the registered dialog or site.

*• Click the **Organize...** button to organize the registrations into folders, move registrations up and down the list and create or delete folders. The same structure will appear in the Biomenu web shortcuts.*

*• Click the **Export...** button to export your registration e.g. for use on another computer. Either choose the registrations to be exported or all existing registrations will be exported automatically.To select more registrations, hold the **Ctrl** or **Shift** key when selecting registrations. Then select a destination file and enter a password. This password will be required when importing these registrations. The 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. You can replace all existing registrations with imported ones, or you can append the imported ones. When appending a registration with the same name again, it will be automatically renamed so that both the old one and the imported one are preserved.Enter the password created during export.*

5 *Click **OK** to finish.*

Turning Password Bank Hints On/Off

The 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 **Control Center** > **Applications** > **Password Bank** dialog. If the user logs into Windows using username and password, the hints are not active until a successful fingerprint verification is performed.

To turn hints on/off:

1 *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center***

2 *Select **Applications > Password Bank**. Authentication is required.*

3 *Select **Alerts**.*

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 begin. This alert is useful in cases where you want to create more registrations for 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 the password field will be displayed in a readable form.*

• ***Ask me if form data should be remembered*** *- Turn on/off the dialog prompting for Password Bank registration after a form (on a web page or a dialog) is submitted.*

• ***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 a web site could be replayed*** *- This hint informs the user that replaying the registration is possible.*

• ***Alert me if a web site is suitable for registration*** *- This hint informs the user that the page contains a password field that can be registered.*

Application Launcher

The Application Launcher is an optional feature of Protector Suite QL.

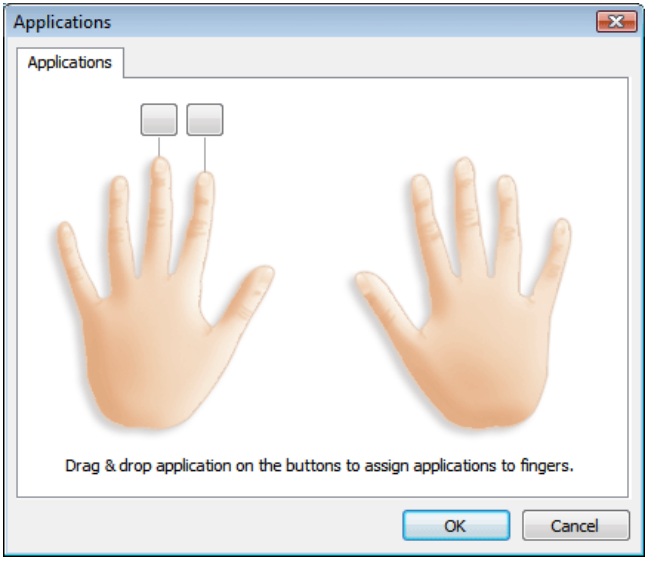
When installed, it enables you to launch registered applications and files by simply swiping your finger over the sensor. Drag and drop (or browse for) an application shortcut from your desktop, a file, etc. and it will be launched next time you swipe the assigned finger over the sensor. (e.g. drag and drop the file “document.doc” you have on your desktop, it will be opened in Word when you swipe the assigned finger next time).

One enrolled finger must remain unassigned, as it is reserved to display the Biomenu. The maximum number of applications you can launch this way is equal to number of enrolled fingers - 1.

If you want to override launching the application (and invoke the **Biomenu** instead), hold **Shift** when swiping the finger.

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

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center***
2. *Select **Applications > Application Launcher**. Authentication is required.*
3. *A dialog with two hands appears. There is a button above each enrolled finger.*



4 *Drag and drop an application or a file.The **Application dialog** opens, change any information if needed and optionally enter the application parameters (see below for examples). Click **OK**.*

OR

*Click a button over a finger. The **Application** dialog opens.*

Enter a title of the application.

In the Application line click on the button on the right to browse for a file you want to launch. This can be any executable file (e.g. Iexplorer.exe).

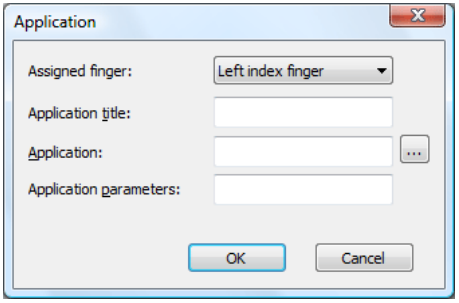
Optionally, additional parameters may be entered into the Application parameters field. If you are not sure, leave this field empty. See below for examples of application parameters.

5 *Click **OK**.*

The association has been created. Next time you verify (swipe the finger over the sensor), the application you selected will be launched.

Examples of Application Parameters

- *A web site can be opened when launching a web browser such as Internet Explorer. Type in a web site address (such as www.upek.com) into the application parameters field and the web site will be launched each time you verify (swipe your assigned finger) and launch the browser.*



- *A file may be opened by an application such as Microsoft Word documents. Type in a path to the file in quotes (e.g. "C:\Documents and Settings\your.account\My Documents\document.doc"). The file document.doc will be open by Word each time you swipe your finger. More than one parameter can be used for one application.*

To delete the fingerprint/application association:

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center***
2. *Select **Applications > Application Launcher**.. Authentication is required.*
3. *Click on the application icon in the button above the assigned finger.*
4. *Click on **Delete...** .*
5. *Click **Yes** to confirm deleting the association.The finger is now free for another application.*

To edit the fingerprint/application association:

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center***
2. *Select **Applications > Application Launcher**. Authentication is required.*
3. *Click on the application icon in the button above the assigned finger.*
4. *Make any desired changes.*
5. *Click **OK.***

File Safe

File Safe is an optional feature of Protector Suite QL.

File Safe allows you to store your files in an encrypted archive on your hard drive. Encrypted archives can contain files or folders and are protected by fingerprint verification or a File Safe backup password if you set it when you are creating an archive. When a File Safe archive is unlocked, you can work with the archive file as with a standard folder (delete, copy, or rename files, etc.). Drag and drop is also supported. You can simply copy and paste or drag your files to your unlocked archive and when you lock it again, your files will be encrypted. When only one file is encrypted in an archive and it is unlocked, clicking on the file will launch it. You can also share your encrypted archives with other users that have enrolled fingerprints.

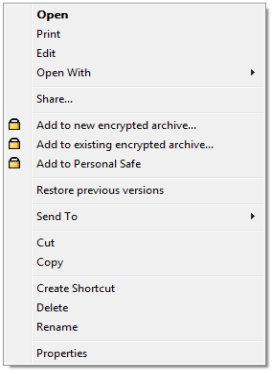
Encrypting Files

You are logged into your computer and you want to add your files to an encrypted archive.

Note: You must have your fingerprints enrolled before creating an archive. Otherwise, a warning that no users are selected will appear. See Fingerprint Enrollment to learn how to enroll your fingerprints.

To add files or folders to a new File Safe archive:

1. *Display the files or folders you would like to encrypt (using Windows Explorer or other Windows dialog).*
2. *Select the files and/or folders (using your mouse and **Shift** or **Ctrl** key) and right-click to display the context menu.*
3. *Select **Add to new encrypted archive.***



4 *A dialog will appear asking you to*

*• Choose a destination folder (click **...** to browse and select a folder)*

• Choose a password. See more below.

*• **Advanced >>** Select users that can have access to the encrypted files.*

*• Press **OK**. Authentication is required.*

5 *After encrypting the files a dialog will prompt you to choose what to do with the original files:*

*• **Keep original files** will not delete the original files and they will be saved both in the encrypted archive and left unencrypted in their original location.*

*• **Delete original files** will delete the original files and will keep the files just in the encrypted form in the archive.*

*• Check the **Wipe files before deleting** check box to overwrite the files you are deleting with a random content and then delete them. This will prevent anybody from recovering the deleted files.*

6 *The encrypted archive is now created (with an ***.uea** extension or ***.ueaf** if only one file was encrypted).*

Password Types:

- ***No backup password** will leave the archive protected by fingerprint only. There is no way how to access the files stored in the File Safe archive when fingerprint verification is not possible (in the event of finger injury, device problem, etc.).*
- ***Use Global Backup Password** will set a global password, i.e. a backup password that will be common for all your archives. This is convenient if you want to avoid using a different password each time you create an archive. If you have not set your Global Backup Password yet, this option will be grayed out. Learn how to set or change the Global Backup Password in “Managing File Safe Archive” on page 45.*
- ***Use following backup password** will let you create a new password for the current File Safe archive.*

It is recommended to use a backup password because otherwise you will not be able to unlock your archives when fingerprint verification is not possible (in the event of finger injury, device problem, etc.). Use a strong password, i.e. at least eight characters long, including non-alphanumerical characters etc.)

In cases when fingerprint verification is not possible, a dialog asking for a backup password will appear. You can force this dialog to appear, and skip the fingerprint verification by closing the dialog asking you to swipe your finger.

Note: If you do not set a backup password and delete your enrolled fingerprints, you will not be able to open locked File Safe archives. Unlock File Safe archives and move out the files before deleting your fingerprints or set a backup password.

To add files or folders to an existing File Safe archive:

1. *Display the files or folders you would like to encrypt (using Windows Explorer or other Windows dialog).*
2. *Select the files and/or folders (using your mouse and **Shift** or **Ctrl** key) and right-click to display the context menu.*
3. *Select **Add to existing encrypted archive.***
4. *Browse and select the archive you would like to save the files to (a file with ***.uea** extension).*
5. *Select **Open**.*
6. *Authentication is required.*
7. *After encrypting the files a dialog will prompt you to choose what to do with the original files:*

   *• **Keep original files** will not delete the original files and they will be saved both in the encrypted archive and left unencrypted in their original location.*

   *• **Delete original files** will delete the original files and will keep the files just in the encrypted form in the archive.*

   *• Check the **Wipe files before deleting** check box to overwrite the files you are deleting with a random content and then delete them. This will prevent anybody from recovering the deleted files.*
8. *The files are now added to your encrypted File Safe archive.*

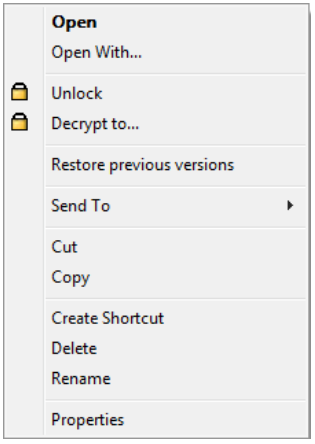
Locking and Unlocking a File Safe Archive

You are logged into your computer and you want to lock or unlock your encrypted File Safe archive.

When a File Safe archive is unlocked, you can work with the archive file as with a standard folder (delete, copy, or rename files, etc.). Drag and drop is also supported. When only one file is encrypted in an archive and it is unlocked, clicking on the file will launch it.

To unlock and open a File Safe archive:

1. *Select the archive file **(*.uea or *.ueaf)** you want to open and right-click to display the context menu.*
2. *Choose **Open** or **Unlock**.*



3. *You will be prompted to verify by swiping your finger or entering the backup password to verify your identity. (This depends on what you set when creating the archive.)*
4. *The archive is now unlocked and you can work with it like with a standard folder (delete, copy, or rename files etc.) or if it is a single-file archive (*.ueaf) the file in the archive will launch (e.g. a text document will open).*

Note: If you double-click on an archive:

• if it is locked it will prompt for authentication and then will unlock and open the archive folder.

• if it is already unlocked it will open the archive folder.

• if there is only one file encrypted and it is locked, it will prompt for authorization and then launch the file.

• if there is only one file encrypted and it is unlocked, it will launch the file.

To Lock a File Safe archive:

1. *Select an unlocked archive file **(*.uea** or ***.ueaf)** and right-click to display the context menu.*
2. *Choose **Lock.** No verification is needed this time.*
3. *The archive is now locked.*

To lock all File Safe archives:

1. *Swipe your finger over the sensor to display **the Biomenu.***
2. *Select **Lock all archives** from the menu. No verification is needed this time.*
3. *All your unlocked archives are now locked.*

Decrypting Files from a File Safe Archive

You are logged into your computer and you want to decrypt files or folders from a File Safe archive. You can either select the entire File Safe archive file and decrypt all files in it or select separate files from the archive and decrypt them.

To decrypt all files or folders in a File Safe archive at once

1. *Select the archive file **(*.uea** or ***.ueaf)** you want to decrypt and right-click to display the context menu.*
2. *Choose **Decrypt to...***
3. *Choose a destination location where the decrypted files will be saved.*
4. *Authentication is required. (This depends on what options you set when creating the archive.)*

5 *Your files are now decrypted in the destination location.*

To encrypt them again or create a new archive, see “Encrypting Files” on page 38.

To decrypt selected files or folders from a File Safe archive

1 *Select the archive file **(*.uea)** you want to decrypt and open it (double-click and if locked, verify yourself).*
2 *Select the file or files you want to decrypt (using your mouse and the **Shift** or **Ctrl** key) and right-click to display the context menu.*
3 *Select **Decrypt to...**.*
4 *Choose a destination location where the decrypted file/s will be saved.*
5 *Choose what to do with the original files in the archive:*
__Delete original files__ - will delete the decrypted files from the archive.
__Keep original files__ - the files in the encrypted archive will be kept.
6 *Your files are now decrypted in the destination location.*
To encrypt them again or create a new archive, see “Encrypting Files” on page 38.

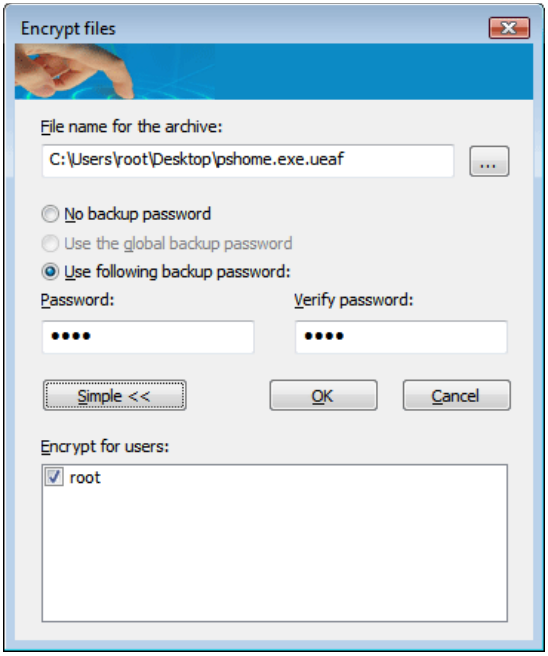
Sharing Access to File Safe Archive

Users can share a File Safe archive. When you are creating an archive you can choose users that will have access to the shared archive using their enrolled fingerprints. Users can be also granted (or denied) access later in the File Safe **Properties**. Anybody (not only users with rights to share the archive) can access the archive using a valid backup password.

Important: All users sharing an archive have the same access rights, including the ability to delete and add files, change password for access to the archive, or deny access for other users, etc.

To grant access for users when creating an archive:

1 *Right-click on the files you would like encrypt and select **Add to new encrypted archive** from the menu.*
2 *Choose a backup password. All users will use the same backup password.*
3 *Click on **Advanced >>***



4 *Encrypt for users window with a list of enrolled users will by displayed. Click on users that will share the archive.*

5 *Click **OK**. All the selected users can unlock the archive by swiping their finger over the sensor.*

To grant or deny access for users in File Safe properties:

1 *Select an archive file **(*.uea** or ***.ueaf)**.*

2 *Right-click to display the context menu and select **Properties.***

3 *If the archive is locked, click on **Unlock** to be able access the properties options. Verify yourself with a fingerprint or a backup password.*

4 *Here you can change password for the archive. This will change password for all users. In the **Grant access to users** window select whom you would like to grant or deny access. All the selected users can unlock the archive by swiping their finger over the sensor.*

5 *If you want to lock the archive, click on **Lock.***

If you use the **Global Backup Password,** the password from the **Applications > File Safe** dialog of the user who created the archive is set. Changing this password does not affect already created File Safe archive/s.

If you want other users to be able to access your File Safe, the archive file must be placed in a shared folder on your computer.

Note: When a logged on user unlocks an archive and then users switch without logging off or restarting the computer, the user now logged on will not be able to access the archive even if the access is shared. If you want to share the archive, lock it before switching users.

Managing File Safe Archive

To access Properties of File Safe archives

1. *Select an archive file **(*.uea** or ***.ueaf)**.*
2. *Right-click to display the context menu and select **Properties.***
3. *Select the **File Safe** tab.*
4. *If the archive is locked, click on **Unlock** to be able access the properties options. Verify yourself with a fingerprint or a backup password.*

   Here you can change the type of password used for the archive and grant or deny access to other users.
5. *Click on **Lock** to lock the archive again.*

Note: The archive must be unlocked to access the properties. If you want to unlock the archive, click Unlock in Properties or see Unlocking/Locking archives.

To change the backup password for File Safe:

1. *Select an archive file **(*.uea** or ***.ueaf)**.*
2. *Right-click to display the context menu and select **Properties.***
3. *Select the **File Safe** tab.*
4. *If the archive is locked, click on **Unlock** to be able access the properties options. Verify yourself with a fingerprint or a backup password**.***
5. *Choose:*

   *• **Erase backup password** to delete the backup password.*

   OR

• ***Set backup password*** *to set a new password or to change it if it has been already set. Select:*

- ***Use Global Backup Password*** *to use a backup password that is common for all archives you select as protected by the Global Backup Password. This password can be changed in File Safe dialog.*
- ***Use following backup password*** *to create a new password for the archive.*

Important: Changing the backup password for the archive will change it for all users. Any of the users that have an access to the archive can change the password.

To change Global Backup Password in File Safe

1. *Select* ***Start*** > ***All Programs*** > ***Protector Suite QL*** > ***Control Center*** *or swipe your finger to display the* ***Biomenu*** *and select* ***Control Center***
2. *Select* ***Applications > File Safe****. Authentication is required.*
3. *Here you can change or set the* ***Global Backup Password****. This password is common for all archives you select as protected by the* ***Global Backup Password*** *(when creating an archive or in* ***Properties****).*

   Changing this password does not affect already created File Safe archive/s. The archives that are currently locked will still be protected by the old password.

Personal Safe

Personal Safe allows you to encrypt your files in a hidden folder. The folder can be shown on your Desktop or in My Computer. This folder will not be visible for other users sharing the computer. Before using the Personal Safe folder, it must be initialized first (see below).

To initialize Personal Safe

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center***
2. *Select **Applications > File Safe**. Authentication is required.*
3. *Select the **Personal Safe** tab.*
4. *Check/Uncheck where you want to show the Personal Safe folder.*
5. *Click on the **Initialize** button.*
6. *Set a backup password.*
7. *Click **OK**.*

   Your Personal Safe is now ready to use and you can see it either on your Desktop or in My Computer or both (see below how to show or hide Personal Safe).

Tip: Alternatively, you can Initialize Personal Safe from the Personal Safe icon. Right-click on the Personal Safe icon (e.g. on your Desktop) and click on Initialize or swipe your finger to display **the Biomenu** and select Initialize..

To Hide/Show Personal Safe

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center***
2. *Select **Applications > File Safe**. Authentication is required.*
3. *Select the **Personal Safe** tab.*

4 *Check/Uncheck where you want to show the Personal Safe folder. It can be shown either on your **Desktop** or in **My Computer** folder or in both at the same time. Even if shown in both places, it will still be the same folder.*

To Set/Change backup password

1 *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center***

2 *Select **Applications > File Safe**. Authentication is required.*

3 *Select the **Personal Safe** tab.*

4 *In the text fields under **Backup Password for Personal Safe** fill in or rewrite your password (twice for verification).*

5 *Verify yourself (e.g. swipe your finger, or swipe finger and enter password) if prompted.*

Adding or removing files is similar to File Safe. When the Personal Safe folder is unlocked, you can work with it as with a standard folder (delete, copy, or rename files, etc.). To encrypt files, select one or more files (or folders) and right-click to display the context menu. Select **Add to Personal Safe.** Drag and drop is also supported. To lock/unlock the folder, select it and right-click to display the context menu and select **Lock** or **Unlock**.

Note: To delete Personal Safe and all its contents, go to **Control Center** and select **Applications > File Safe** and the **Personal Safe** tab. Click on the **Delete and Reset** button. All data in the Personal Safe will be deleted. If you want to use Personal Safe later, it will have to be initialized again.

Security Tokens

Tokencodes are one-time-passwords used for accessing online resources. Protector Suite QL enables tokencode generation and automatic form filling after you swipe your finger over the fingerprint sensor.

The tokencode generation can be carried out by the fingerprint hardware chipset or by software. Hardware-based generation is dependent on the type of fingerprint sensor. Please note that not all sensors are supported.

To use this feature you must be registered with a provider that accepts tokencodes.

RSA SecurID Token Import

To obtain a tokencode

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center***

   OR

   *Swipe your finger to display the **Biomenu** and select **Control Center.***
2. *Select **Applications > Security Tokens** and verify yourself (e.g. swipe your finger, or swipe finger and enter password) if prompted.*
3. *The **Security Tokens** tab appears. Click on the **Add** button.*
4. ***RSA SecurID Token Import** tab appears.*
5. *Fill in a name for the token and click on **Next.***

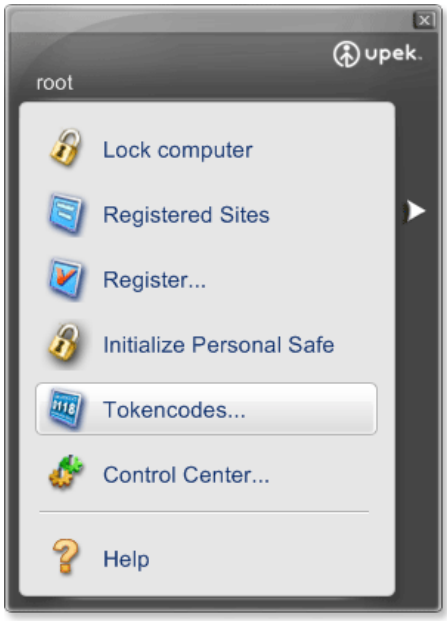
   In the next dialog browse for the SecurID file (.sdtid) you received from your provider. If prompted, enter the file password and click on **Next.***
6. *The security token will be activated. After the activation is finished, click **Next.***
7. *When the token is ready, click on the **Finish** button.*

Tokencodes Generator

You can generate tokencodes either by registering a token with the Password Bank application (see below) or by using the Tokencodes Generator. The Tokencodes Generator is a simple dialog which allows you to select a security token and generate a tokencode using this token. Then you can copy it to clipboard and paste it where needed.

To generate a tokencode

1 *Swipe your finger over the sensor to display the **Biomenu** and select **Tokencodes** from the menu.*



2 *Select the token you want to use. If you have just one token, the tokencode will be generated automatically.*

A dialog will be displayed indicating the valid duration of the generated tokencode. The tokencode is time-based and it expires after a certain time (typically one minute).

*According to your service provider requirements, select whether the tokencode will be generated **with PIN** or **without PIN**.*

*Select **Next** if another tokencode is required by your service provider (e.g. to confirm your identity after entering an invalid logon data).*

3 *Click on the **Close** button.*

Managing Security Tokens

You can edit the name of each security token as it appears in the dialogs or delete tokens.

To edit a token:

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center***

   OR

   *Swipe your finger to display the **Biomenu** and select **Control Center.***
2. *Select **Applications > Security Tokens** and verify yourself (e.g. swipe your finger, or swipe finger and enter password) if prompted.*
3. *The **Security Tokens** tab appears. Select a token you want to edit.*
4. *Click on the **Rename...** button and enter a new name for the token.*

   OR

   *Click on the **Remove...** button. When a token is deleted then the data in user passport is removed.*
5. *Click **OK** to confirm the changes and close the dialog.*

Tokencode registration and replaying (with Password Bank)

The Password Bank application is able to detect a web page or an application dialog where tokencodes are used. After you register a web site or application, you can use the Password Bank to automatically fill in your logon data including tokencodes when you swipe your finger over the sensor. Your credentials will then be protected by fingerprint verification, which is both secure and convenient.

The Password Bank recognizes pages containing a password field and displays a hint that the page can be registered. These hints can be turned off in the Password Bank Settings dialog. See “Turning Password Bank Hints On/Off” on page 33.

To register credentials with Password Bank

1. *Display a web page or application containing a tokencode form.*
2. *Swipe your finger over the sensor to display the **Biomenu**.*
3. *Select **Register** from the menu.*

4 ***Tokencode Registration Wizard*** *appears. Click on* ***Select...*** *to select a security token from the list. If you are using just one token, tokencode will be filled automatically.*

5 *Click* ***OK*** *to confirm and close.*

6 *The credentials are now registered and can be replayed automatically next time. If you checked the* ***Fill and submit the web form now*** *you will be logged in to your application.*

To replay a tokencode registration with Password Bank

1. *Display a web page or application you have registered.*
2. *A Password Bank hint appears informing you about an existing registration.*
3. *Swipe your finger over the sensor.*
4. *(Optional) A Password Bank dialog appears informing you that submitting the registration is available. Click **Yes** to replay the registration. Check **Do not show this again** to skip this step next time.*
5. *The browser windows flashes and the registration is replayed and you are logged in.*

Note: Tokencode Time-out dialog appears when a time-out is needed before a token is submitted, wait for the indicated amount of time before you try to replay the registration again.

If Tokenkodes authentication fails, you will be asked for next tokencode. A dialog appears asking whether you want Password Bank to generate a new tokencode and sumbit it. Select **Yes** generate it, select **No** to cancel and **RunTokencodes Generator** to generate and place a tokencode manually.

Chapter 4
Managing Protector Suite QL

There are three ways to manage Protector Suite QL's functions and settings: through the Control Center dialog, the system tray icon and the Biomenu (that is displayed after you swipe an enrolled finger over the sensor). This chapter will guide you through their functions.

Protector Suite QL functions can be also accessed through the Windows **Start** menu. Select **Start > All Programs > Protector Suite QL** to see a list of available features.

Control Center

The Control Center contains various functions for fingerprint management and setting up your fingerprint software. The available options depend on the software status, hardware used and installed applications.

To display Control Center:

- *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center***
- *or swipe your finger to display the **Biomenu** and select **Control Center***
- *or right-click on the tray icon and select **Start Control Center...***

Fingerprints

You can enroll, edit and delete users' fingerprints and, if power-on security is implemented, also manage fingerprints present in the device memory. The list of available features depends on the installed version of Protector Suite QL, the fingerprint sensor, existing passports and administrative privileges of the current user.

Note: The features differ according to the administrative privileges of the current user. In the Secure mode, users defined as fingerprint administrators (see "Security Mode" on page 67) can enroll or edit passports for all enrolled users. In the Convenient mode, users can enroll or edit only their own passports.

Enroll or Edit Fingerprints

Fingerprint enrollment is a process of creating correspondence between your username, password and your fingerprints (computerized so that reconstructing the original image is not possible) together with automatically generated security keys. All the data is stored in a user fingerprint passport.

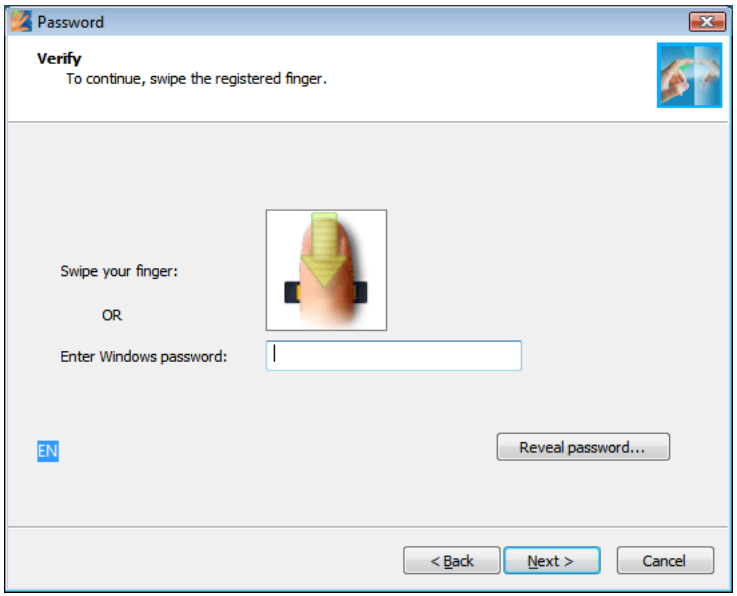
After you enroll, you can use your fingerprints instead of typing your username and password. Please note that if you change your Windows username, your passport will be deleted.

To enroll or edit a passport (enroll or edit fingerprints):

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center***
   *or swipe your finger to display the **Biomenu** and select **Control Center***
   *or right-click on the tray icon and select **Start 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.)*
   OR
   *or right-click on the tray icon and select **Edit Fingerprints...***
4. *(Optional) In the Secure mode (see "Security Mode" on page 67), a list of existing passports is displayed. Select the user and click the **Edit** button to edit fingerprint of an existing user or click **Enroll** to enroll a new user.*

5 *The **Enrolment Wizard** screen is displayed.*

6 *Swipe your finger over the fingerprint sensor or enter your Windows password, and click **Next.***



*The **Multifactor** dialog appears. Choose a method of authentication. Next time you are prompted for verification, the selected method will be required (e.g. logging to you computer, registering web pages etc.). This will apply for all enrolled fingers. See Chapter 3, “Multifactor methods” , on page 17 for more information.*

7 *Do one of the following:*

- *To enroll a new fingerprint:*
  - *Select a finger to enroll by clicking the box above the finger.*
  - *Swipe the selected finger over the fingerprint sensor. Fivesuccessful images are required to enroll one fingerprint (see Chapter 3, “Fingerprint Enrollment” , on page 14 for more instructions).*
- *To delete a fingerprint:*
  - *Select a finger to delete by clicking the box above the finger.*
  - *Click **OK**.*

8 *(Optional) If enrollment to the device was selected and your system configuration supports power-on security, all enrolled fingerprints will be also used for power-on security.*

9 *(Optional) If enrollment to hard drive is selected and your system configuration supports power-on security, enrolled fingerprints will be also used for power-on security.*

10 *The device memory is limited. If some of the enrolled fingerprints in the passports are not assigned for power-on security in the device (e.g. another device is connected),* ***Power-on*** *button is displayed above each finger. The Power-on button is displayed in a "depressed" state by default. The corresponding finger will be used for power-on security. If you do not want to use a finger for power-on security, but only for logon, click the Power-on button to delete it from the device memory.*

11 *Click* ***Next*** *to finish the enrollment.*

Delete

The features differ according to administrative privileges of the current user. In the Secure mode (see “Security Mode” on page 67), only users defined as fingerprint administrators can delete user passports.

To delete an existing passport (all user’s data):

1 *Select* ***Start*** > ***All Programs*** > ***Protector Suite QL*** > ***Control Center*** *or swipe your finger to display the* ***Biomenu*** *and select* ***Control Center*** *or right-click on the tray icon and select* ***Start Control Center...***

2 *Click* ***Fingerprints*** > ***Delete****.*
In the Convenient mode, verify yourself 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 Passport

Existing user data (including fingerprints, encryption keys, logon credentials) can be exported to a *.vtp file (a passport file) and imported back into your fingerprint software. The *.vtp file is encrypted and protected by a password defined during export. You cannot import a passport of an existing user. In this case it is necessary to first delete the user's passport.

Tip: We recommend exporting your passport for backup purposes, e.g. if you change your Windows username and so delete your passport, you can import the backup later.

To export an existing passport:

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center** or right-click on the tray icon and select **Start Control Center...***
2. *Click **Fingerprints > 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 on **Export**.*
3. *Select the destination file **(*.vtp)**.*
4. *Define a password which will protect the exported data.*
5. *Verify the finger (contained in the passport you are exporting).*

To import a passport:

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center** or right-click on the tray icon and select **Start Control Center...***
2. *Click **Fingerprints** > **Import or Export User Data**. In the Secure mode, a list of existing passports is displayed. Click on **Import.***
3. *Browse for the passport file **(.vtp).***
4. *Enter the password (defined during export).*

Applications

You can configure fingerprint application (i.e. Application Launcher, Pasword Bank and File Safe) in this section. In case you not enrolled, please follow the link and enroll at least one finger.

Application Launcher

Displays applications that can be launched by your fingerprints.

At least one enrolled finger must remain unassigned to display the Biomenu. The maximum number of applications you can launch is equal to number of enrolled fingers minus one, e.g. if you want to launch two applications, you need to have at least three fingers enrolled.

To launch an application by an enrolled fingerprint:

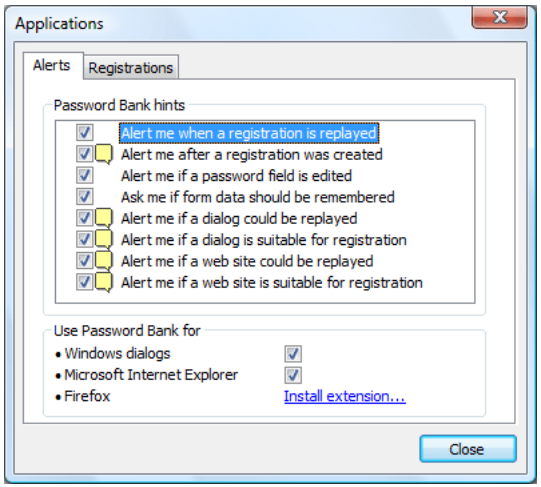
1. *Click the **Add** button. The Application dialog opens.*
2. *Select an enrolled finger that is free. A dialog appears prompting you to enroll more fingers, if none are available.*
3. *Enter a name of the application.*
4. *Browse for a file you want to launch. This can be any executable file (e.g. Iexplore.exe).*
5. *Optionally, additional parameters may be entered into the **Application parameters** field (see page 35).*
6. *Click **OK**.*

For more detailed information on Application launcher and Application parameters, see Chapter 3, “Application Launcher” , on page 35.

Password Bank

This dialog consists of two parts. The first contains settings of hints that are displayed to inform a user about Password Bank actions. Check or uncheck the check box before each hint description to display or hide the hint.

The second part contains information about using Password Bank.



Checking the **Windows Dialog** check box will enable using Password Bank for storing credentials of standard Windows application. Support of web credentials in Internet Explorer is always present, the check box enables or disables using the browser for the current user. For Firefox browser, a plug-in installation is required. Click on the link to start the installation. Firefox must be set as your default browser. If you upgrade Firefox after the plug-in installation, Firefox informs you that the Password Bank plug-in is not compatible anymore and offers to find a current one. Confirm and install the new plug-in.

For more information about Password Bank, refer to Chapter 3, “Password Bank” , on page 27.

Registrations

This dialog lists all your existing Password Bank registrations. Both registered pages and dialogs are displayed. Select a registration from the list and click one of the buttons buttons below to **Edit** the registration, **Organize** the list of registrations (as they appear in the Biomenu) or click **Export** to export your registrations for use on another computer or backup, and **Import** to import registrations from an exported file.

For more information see Chapter 3, “Managing Your Registrations” , on page 32.

File Safe

You can set or modify the password protecting your files stored in encrypted File Safe archives. This password will protect all your archives that are set to be protected by the Global Backup Password. It is recommended to use a backup password because if you do not there is no way how to access the files stored in the File Safe archive when fingerprint

verification is not possible (in the event of finger injury, device problem, etc.). Use a strong password, i.e. at least eight characters long, including non-alphanumerical characters etc.)

Note: Changing this password does not affect already created File Safe archive(s).

For more details on passwords and File Safe see Chapter 3, “Encrypting Files” , on page 38.

Security Tokens

This dialog starts Security Token import. To be able to use this feature you must be registered with a provider that is accepting and providing security token services. Please read “Security Tokens” on page 49 to learn how to proceed with the import step by step.

Settings

The Protector Suite QL Settings dialog contains various options for setting up Protector Suite QL. Not all the functions of the Settings described here may be visible, the available functions vary according to installed version of Protector Suite QL and administrative privileges of the current user.

System Settings

System Settings contain settings common for all users. Access to these settings is limited to administrators. The following features can be set up in System Settings:

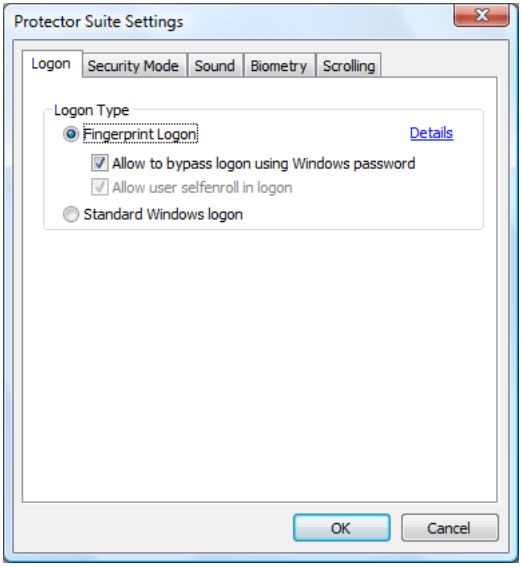
Logon, Security Mode, Sound, Biometry, TPM (optional), Scrolling.

If you are using Windows Vista, click the **Edit...** button with the shield icon to get administrative rights to make changes in System Settings. When Vista Control User Account dialog appears, enter your credentials to authenticate to the system (or just allow the program to continue if you are already logged as an administrator). The button is not visible in case that elevation is not required or impossible.

Logon

Only an administrator can change logon settings. Some changes require you to restart the computer. The Logon Settings screen enables you to:

- *Replace Windows logon with fingerprint protected logon*
- *Automatically log on a user verified by power-on security (optional)*
- *Enable fast user switching support (optional).*



To change your logon settings:

1 *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center** or right-click on the tray icon and select **Start Control Center...***

2 *Go to **Settings** > **System Settings > Logon.***

3 *Select:*

• ***Fingerprint Logon***
When this option is selected the fingerprint logon to your computer is enabled.

•***Do not show Ctrl+Alt+Del message***
*The **Ctrl+Alt+Del** message will not be displayed. (The logon dialog for entering username/domain/password can be invoked by pressing **Ctrl+Alt+Del** so that users are able to log on using username and password.)*

•***Allow to bypass logon using Windows password****- If this option is checked, the standard Windows logon can be used. If unchecked, only fingerprint administrators can logon using username and password.*

•***Allow user to self-enroll on logon*** *- users are allowed to enroll their fingers themselves when logging in the computer.*

*•If you are using Windows Vista, click on **Details** to see the settings of credential providers, i.e. how user authentication is managed by the system. See "Credential Providers in Windows Vista" below for more information*

• ***Fast User Switching***
When this option is selected, biometric fast user switching controlled by your fingerprint is enabled (if supported on your system). When fast user switching is supported but not enabled, you will be asked to enable it on your system. Fast user switching cannot be enabled when the computer is a member of a domain.

If you are using Windows Vista, this option is always on by default and cannot be changed.

• ***Standard Windows logon*** *- When this option is selected the fingerprint logon is disabled and the standard Windows logon is used.*

• ***Allow power-on security single sign-on***
Select this option to perform power-on and logon fingerprint authentication in one step. Users verified at the BIOS level are automatically logged on to Windows.

4 *Click **OK** and restart your computer.*

Credential Providers in Windows Vista

Credential providers allow various ways how you can authenticate to the system. The Microsoft Password Provider requires user username and password, the Fingerprint Provider swiping users' finger over the sensor. The list of credential providers will vary according to configuration of a particular system.

To display a provider's settings:

1 *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center** or right-click on the tray icon and select **Start Control Center...***

2 *Choose **Settings > System Settings> Logon.***

3 *Click on **Details.***

4 *The following features are defined by the Credential providers:*

*• **Logon** defines how users will authenticate when logging into the system (e.g. by fingerprint only, by name and password, etc.)*

*• **Unlock** defines how users will authenticate when unlocking the computer.*

*• **Run as administrator** is a feature of Windows Vista. A user logged as a limited user can authenticate as an administrator and run an application restricted to administrators.*

*• **Change Password** defines type of authentication required to change user password (e.g. fingerprint verification, username and password).*

5 *Select:*

*• **Mark enrolled user tile picture** to display a fingerprint icon over the picture in the user account tile to mark that a user is enrolled and logon will be managed by a fingerprint. If not selected, the account tile will appear as usual. This will set the Microsoft Password Provider to the "wrapped" state (see below).*

*• **Allow users to self-enroll in logon** to allow users that have a valid password but no fingerprints enrolled to enroll their fingers themselves when logging in the computer.*

6 *To view a provider's settings, select a provider from the list and click on **Details**…(or double-click on the provider).*

Note: The Fingerprint Provider and the Microsoft Password Provider cannot be set up by the user. Their settings are predefined.

7 *A dialog will appear allowing you to see the settings of the selected provider. The options are the following:*

*• **On** will turn the provider on. For example, when On is set for the Fingerprint Provider in the Logon section, users will be prompted to authenticate by swiping their finger over the sensor when logging into the computer.*

*• **Off** will turn the Provider off. For example, when in Logon section Microsoft Password Provider is set to Off and the Fingerprint Provider to On, only fingerprint verification will be allowed on logon.*

*• **Wrapped** - for a user the wrapped provider seems to be still On, but control of its functions will be taken over by the Fingerprint provider.*

Note: The Fingerprint Provider cannot be set as wrapped but wraps other providers (such as Microsoft Password Provider).

Security Mode

Protector Suite QL can operate in three security modes:

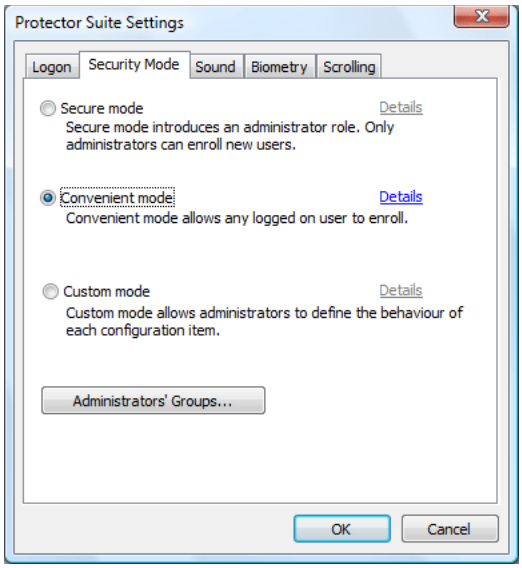
Secure mode, Convenient mode and **Custom mode.**

The security modes differ in rights granted to users. These rights include e.g. permissions to enroll users, delete or edit fingerprints, etc.

Click on **Details** to see the settings of security policies in each mode. Only the policies in the Custom mode can be edited.

Fingerprint Administrators' Groups

Contains a list of local or domain security groups of users defined as “fingerprint administrators” . These users are granted administrative rights for managing Protector Suite QL. Their rights are defined in the Security mode policies (see below).



To choose a security mode:

1 *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center** or right-click on the tray icon and select **Start Control Center...***

2 *Choose **Settings > System Settings***

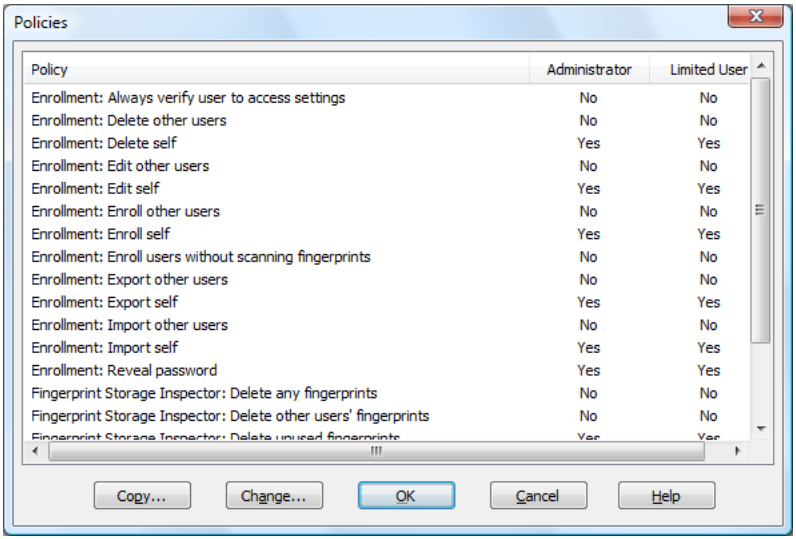
3 *Select the **Security Mode** tab. Choose:*

- ***Secure mode.** In the Secure mode only a fingerprint administrator has an unrestricted access to all fingerprint management functions (e.g. creating, deleting fingerprint passports for all users), including Fingerprint Storage Inspector and Power-on Security administration.*
- ***Convenient mode.** In the Convenient mode, all users share the same rights. For example, all users can create, edit or delete their own fingerprint passport.*
- ***Custom mode.** Custom mode policies' settings can be set up differently for an administrator and limited users.*

4 *Click **OK** to close the dialogs.*

Security Mode Policies

Policies in the Secure and Convenient mode are preset and cannot be modified. Only policies in the Custom mode can be changed. Select and double-click a policy to see the policy details.



To edit policies in the Custom mode:

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center** or right-click on the tray icon and select **Start Control Center...***
2. *Choose **Settings > System Settings***
3. *Select the **Security Mode** tab.*
4. *Click the **Custom** radio button, then click on **Details**. The policies window will appear. See details of policies below.*
5. *Click the **Change** button (or double-click) to edit the policy settings.*
6. *Click **OK** to close the dialogs.*

Policies can be defined differently for a Fingerprint Administrator and a Limited user accounts. Select **Allow/Deny** to set rights for each user group.

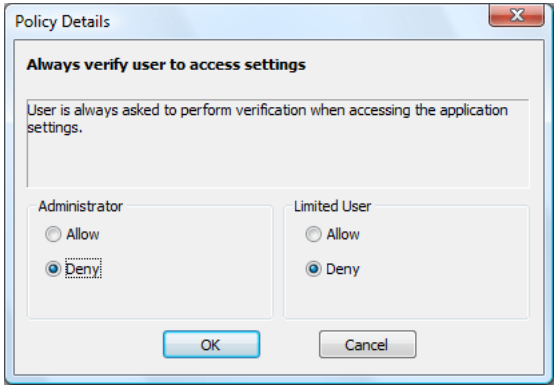
You can copy policies' settings from the Convenient or Secure mode to the Custom mode and then edit them further. This is convenient when you would like to make just a few changes to the policies' settings.

To copy policies from Convenient or Secure mode:

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center** or right-click on the tray icon and select **Start Control Center...***
2. *Click **Settings> System Settings***
3. *Select the **Security Mode** tab.*
4. *Click the **Custom** radio button, then click on **Details**. The policies window appears. See details of policies below.*
5. *Click the **Copy** button to copy the policies settings.*
6. *Choose the **Secure** or **Convenient mode** and the policies' settings will copy from the selected mode.*
7. *Now you can edit the policies using the **Change** button.*
8. *Click **OK** to close the dialogs.*

Details of Policies:

Select and double-click a policy to see the policy details.



Enrollment:

- Always verify user to access settings: *User is always asked to perform verification when accessing the application settings in the Control Center. This policy is enabled by default only in the Secure Mode.*

- Delete other users: *Allows a fingerprint passport to be deleted for any user enrolled on this computer. No verification is required before passports are deleted.*
- Delete self: *After verification allows a fingerprint passport to be deleted for the currently logged on user.*
- Edit other users: *Allows a fingerprint passport to be edited for any user enrolled on this computer, e.g. adding or deleting enrolled fingerprints.*
- Edit self: *Allows a fingerprint passport to be edited for the currently logged on user, e.g. adding or deleting enrolled fingerprints.*
- Enroll other users: *Allows other users to enroll fingerprints. Only users with a valid Windows account can be enrolled.*
- Enroll self: *Allows the currently logged on user to enroll fingerprints.*
- Enroll users without scanning fingerprints: *Allows users to be enrolled without scanning their fingerprints. Users will be prompted to scan their fingerprints the next time they logon.*
- Export other users: *Allows a fingerprint passport to be exported for any user enrolled on this computer.*
- Export self: *Allows a fingerprint passport to be exported for the currently logged on user.*
- Import other users: *Allows a fingerprint passport to be imported for any user enrolled on this computer.*
- Import self: *Allows a fingerprint passport to be imported for the currently logged on user.*
- Reveal password: *Allows the user's Windows password to be revealed during the fingerprint enrollment.*

Fingerprint Storage Inspector:

- Delete any fingerprints: *Allows any fingerprints to be deleted from your device. (The Use Fingeprint Storage Inspector policy must be enabled for this policy to take effect.)*
- Delete other users' fingerprints: *Allows fingerprints of other users to be deleted. However, at least one fingerprint must remain enrolled for each user. (The Use Fingeprint Storage Inspector policy must be enabled for this policy to take effect.)*

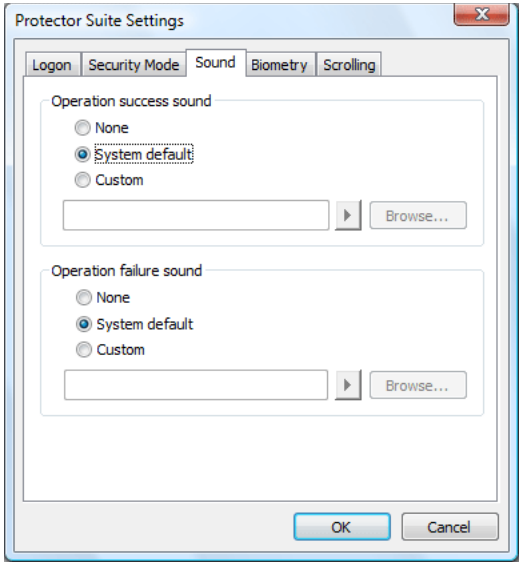
- Delete unused fingerprints: *Allows fingerprint records that do not belong to any locally enrolled user to be deleted, e.g. from previous installation. (The Use Fingeprint Storage Inspector policy must be enabled for this policy to take effect.)*
- Use Fingerprint Storage Inspector: *Allows use of the Fingerprint Storage Inspector, i.e. users can delete only their own fingerprints (except for the last one, i.e. at least one fingerprint must remain enrolled).*

Power-on Security:

- Add fingerprints to Power-on security: Allows *fingerprints to be added to Power-on security during enrollment. If disabled, enrolled fingerprints cannot be used for Power-on security verification.*
- Enable/Disable Power-on security: *Allows Power-on security to be enabled or disabled on this computer.*

Sound

Selected sound is played when a fingerprint operation succeeds or fails. You can use your default system sounds, disable sounds, or browse for your favorite audio file (.wav format).



Biometry

These settings allow you to modify the security level settings of the fingerprint sensor. A reboot is required each time you make any changes.

To change Biometric Settings:

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center** or swipe your finger to display the **Biomenu** and select **Control Center** or right-click on the tray icon and select **Start Control Center...***
2. *Click **Settings > System Settings** and go to **Security Mode > Biometry***

   *• **Intruder Lockout***

   *•**Lockout count:** sets the number of unsuccessful verification attempts are allowed before the device is locked.*

   *•**Lockout time:** sets the time the device will stay locked. After this time the fingerprint sensor can be used again.*

   *• **Biometric Performance** will set up how accurately a fingerprint scan must match the enrolled samples. Please note that using the lowest level may compromise the security of the device. The highest level, however, requires a perfect match with the enrolled sample and may result in repeated unsuccessful verifications for authorized users. The default (middle) level is recommended.*

TPM (optional)

This page is displayed when a third-party TPM-management application is detected. TPM initialization enables usage of the TPM security module by the Multifactor feature. See Chapter 3, “Multifactor methods” , on page 17 to see how to set the multifactor methods during the Fingerprint enrollment.

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, **Protector Suite QL** is able to use the additional TPM security.*
4. *Click **Finish** to close the wizard.*

Scrolling

You can use your fingerprint sensor for scrolling through the **Biomenu** (see page 82) and any Windows application instead of the mouse wheel.

Switch the scrolling on/off by checking the **Sensor Scrolling Features** option in the tray icon (right-click the tray icon and select the feature) or by pressing the **Scroll Switch Hotkey.**

When the Sensor Scrolling Feature is checked, the tray icon changes to indicate the scrolling feature is on. The hotkey is not defined by default after Protector Suite QL installation and must be set (see bellow).

To set up scrolling and the Scroll Switch Hotkey:

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center***
   *or swipe your finger to display the **Biomenu** and select **Control Center***
   *or right-click on the tray icon and select **Start Control Center...***
2. *Click **Settings** > **System Settings.***
3. *Select the **Scrolling** tab.*
   - *Click the **Test Scroll** button to test scrolling with selected values.*
   - ***Speed** - Move the slider to adjust the scrolling speed. This sets how much will the cursor move when you move your finger over the sensor.*
   - ***Acceleration** - Move the slider to set the scrolling acceleration. The faster you swipe over the sensor, the faster will be the scrolling.*
   - *To set the scroll switch hotkey, set focus to the **Scroll Switch Hotkey** field. Press the key(s) you want to use for turning the scroll feature on/off.*
4. *Click **OK** to close the dialog.*

User Settings

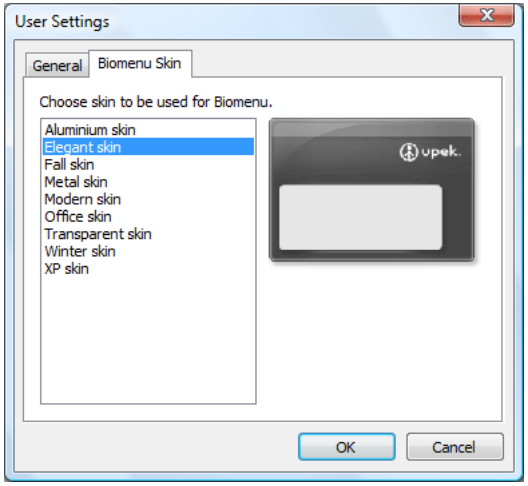
User Settings contain user-specific settings. The following features can be set up in User settings:

General

Check the **Show icon in tray** check box to display the tray icon which gives you quick access to some of Protector Suite QL functions. See “System Tray Icon” on page 80 for more information about the functions available in the tray icon.

Biomenu Skin

Select a skin (appearance) for Protector Suite QL's Biomenu. A sample is displayed on the right side of the dialog. (Skin preview is not supported on Windows 2000.)



Power-on security (optional)

The power-on security feature prevents unauthorized access to the user's computer at the BIOS-level. Computers with power-on security enabled will not load the operating system from the hard drive without successful fingerprint authentication.

Fingerprint samples are stored in the memory of your fingerprint device. During computer boot, you are asked for a fingerprint authentication. You have a limited time to swipe a finger over the sensor. The computer will boot only if the scanned fingerprint matches a sample stored in the memory of the device. After successful verification, the boot process continues normally.

Enabling power-on security in Protector Suite QL

Options for working with power-on security are displayed only if your computer supports this feature (supported mainly in laptops). In most configurations, power-on security is enabled automatically after enrolling the first user.

To enable/disable the power-on security:

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center***
   *or swipe your finger to display the **Biomenu** and select **Control Center***
   *or right-click on the tray icon and select **Start Control Center...***
2. *Click **Settings > Power-on Security**.*
3. *Select the **Enable power-on security using fingerprints** check box.*
4. *Click on **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. For adding fingerprints to power-on security, please refer to Chapter 3, “Fingerprint Enrollment” , on page 14).

Power-on security single sign-on

Power-on security can be configured to interoperate with the fingerprint logon. If a fingerprint used for BIOS power-on security feature matches a fingerprint on an existing passport, the corresponding user is logged on automatically without having to enter the Windows password or swipe a second time. Another authentication method may be required, it depends on what you have set in the Multifactor dialog (see Chapter 3, “Fingerprint Enrollment” , on page 14).

To enable automatic Windows logon for users verified by power-on security:

1. *Select **Start** > **All Programs** > **Protector Suite QL** > **Control Center***
   *or swipe your finger to display the **Biomenu** and select **Control Center***
   *or right-click on the tray icon and select **Start Control Center...***
2. *Click **Settings** > **System Settings***
3. *Select the **Logon** tab.*
4. *Select the **Allow power-on security single sign-on** check box.*

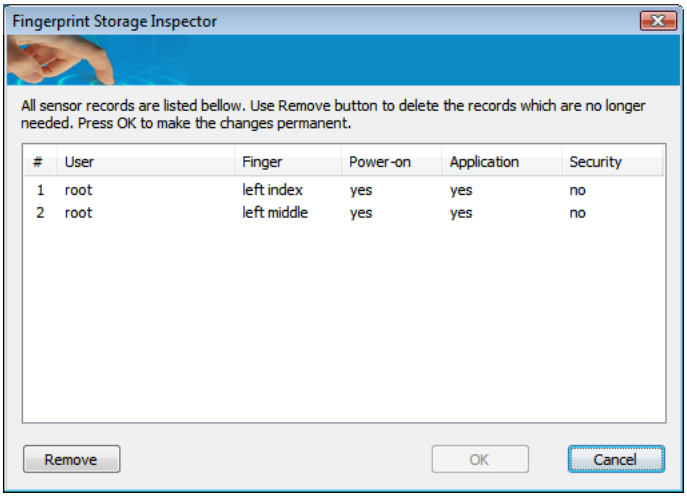
Note: Your hardware must support Power-on security to use this single sign-on feature and you must have administrative privileges to change the settings.

Fingerprint Storage Inspector (optional)

This feature is available only when Enrollment to device is used.

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

Description is shown for each finger together with information about its usage for power-on security (pre-boot authentication), applications (e.g. Logon), and multifactor authentication methods.



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.*

   *At least one fingerprint must remain for each passport. To manage or delete the whole passport, use the **Enroll or Edit fingerprints** or **Delete** wizard (see “Enroll or Edit Fingerprints” on page 57).*

Note: The authorization to remove fingerprints is defined in the Security mode policies settings (see “Security Mode” on page 67). Some rights may be restricted to fingerprint administrators only.

Sensor Calibration (optional)

If supported by your sensor, opens the calibration dialog. Click on the **Calibrate** button and wait until the calibration is finished. The calibration may be used in case you feel the sensor is not working properly. Do not touch the sensor during calibration.

Help

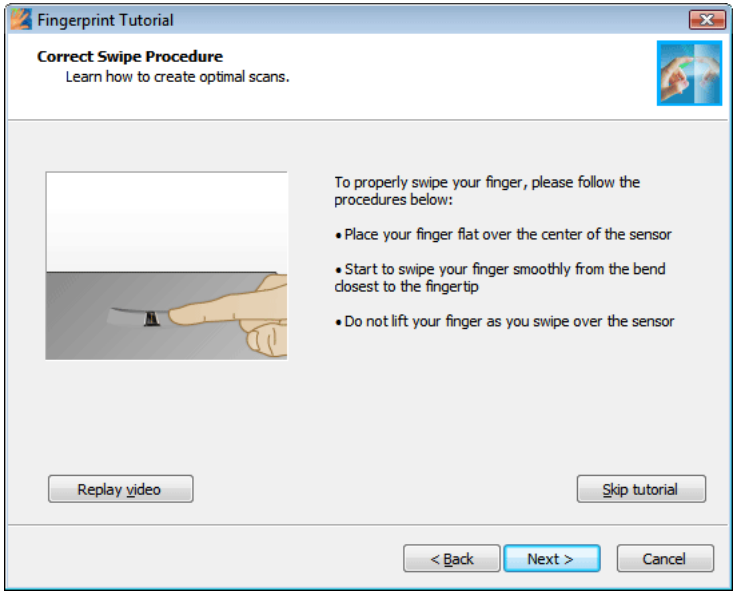
Introduction

The Starting Page is shown when you swipe your finger over the sensor when no fingerprints are enrolled. It contains a link to a Protector Suite QL product tour and a link to fingerprint enrollment. It can be accessed later from **Control Center > Help > Introduction.**

Tutorial

This will launch the Fingerprint Tutorial.

The tutorial will show you a short video demonstrating correct and incorrect fingerprint scanning. Then you will try to create your first fingerprint samples.



For more information, see Chapter 3, “Fingerprint Tutorial” , on page 20.

Note: To display HTML-based help Select **Start >All Programs > Protector Suite QL > Help** or click on the **Help** icon in the main Control Center dialog. To display context-sensitive HTML help, press F1 in the dialog box for which you need help.

Biomenu

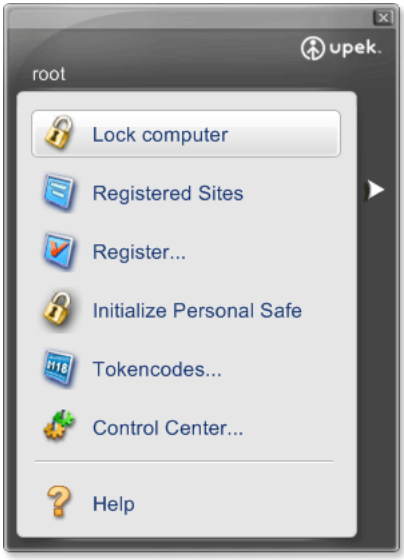
The **Biomenu** provides access to Protector Suite QL's features and settings. Available items depend on installed components.

To display the Biomenu:

- *swipe an enrolled finger over the fingerprint sensor.*

  *To display the **Biomenu** in a situation when finger verification invokes another action (e.g. a registered page is replayed), hold the **Shift** key when swiping your finger over the sensor.*

Use your mouse or the sensor to navigate. If you use your sensor, move your finger to navigate through the **Biomenu** and tap the highlighted item to run the corresponding action. You can set up scrolling settings in the System settings dialog (see“Scrolling” on page 74).



The Biomenu is available in several skins. To view or change skins, open the **Control Center > Settings > User Settings,** swipe your finger to verify and go to the **Biomenu skin** tab.

•Lock computer

*The first menu item contains the **Lock computer** command which locks your computer. Swipe your finger over the sensor to unlock the computer again*

***•Registered Sites** (optional)*

Displays lists of your web pages registered by Password Bank. To display and fill in a registered page in your default web browser, click the web page name in the list. The appearance of the list can be edited in the Password Bank tab in the System Settings. See Chapter 4, “Password Bank” , on page 61.

- ***Register...**(optional)*

  Registers a new window (a web page or dialog). To learn more about Password Bank registration, see Chapter 3, “Registering Web Pages and Dialogs” , on page 27.

- ***Personal Safe** (optional)*

*Depending on the current state, **Initialize Personal Safe**, **Lock Personal Safe** or **Unlock and open Personal Safe** will visible. Intialize will prepare Personal Safe for use and after that locking or unlocking and opening will be available.*

- ***Lock all archives** (optional)*

  Will lock all File Safe archives that are currently opened. This item will be displayed only when at least two archives are unlocked.

- ***Tokencodes...**(optional)*

  Displays the Tokencodes generator. The Tokencodes Generator is a simple dialog which allows you to select a security token and generate a tokencode using this token.

- ***Control Center...***

  Displays the Control Center Dialog (see “Control Center” on page 56).

- ***Help***

  Displays the HTML help. To display context-sensitive HTML help, press F1 in the dialog box for which you need help.

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.

You can also launch this wizard from the Control Center by selecting **Fingerprints** > **Enroll or Edit Fingerprints.** See **Chapter 3, “Fingerprint Enrollment” , on page 14** for detailed information on how to enroll fingers.

Start Control Center...

Starts Protector Suite QL's Control Center (see page 56).

Don't use sensor/Use sensor

Allows you to temporarily detach your fingerprint device from Protector Suite QL for use by another application. This command frees the device for the current user session. (The device can be used only by one application at a time.)

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

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

Sensor Scrolling Feature

When the Sensor Scrolling Feature is checked, the tray icon changes to indicate the scrolling feature is on. The hotkey is not defined by default after Protector Suite QL installation and must be set (see "Scrolling" on page 74). Uncheck to disable the scrolling.

Help

Displays the HTML help. To display context-sensitive HTML help, press F1 in the dialog box for which you need help.

About

Displays the product information about Protector Suite QL.

Fingerprint Reader Infopanel

The fingerprint reader info panel contains information about your sensor and a test window for fingerprint scanning. You can use this dialog to get details about your sensor in the event of a hardware problem for communication with the technical support etc.

To display the Fingerprint Reader Infopanel

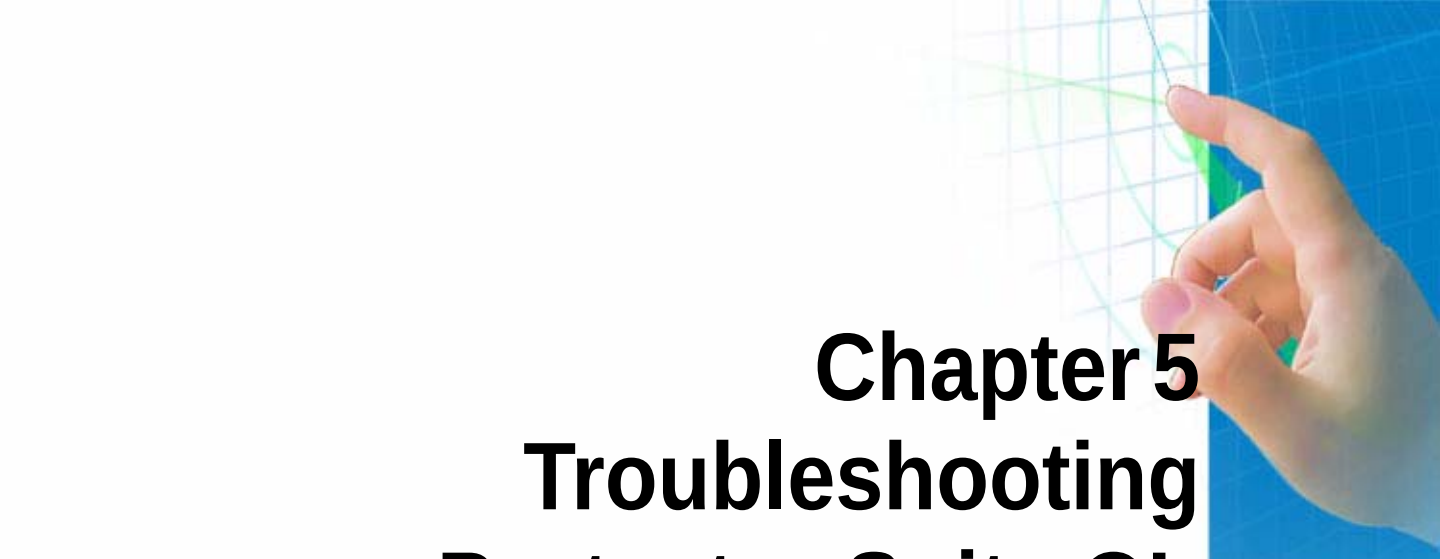
1. *Select **Start** > **Control Panel***
2. *Click on the **Fingerprint Sensor** icon. **Fingerprint Reader Infopanel** dialog will appear.*

*• Select the **Version** tab to display information about your sensor (such as device type, name, version etc.)*

*To export the information to a text file click on **Save** and choose a location where the file will be saved (FingerprintSensorVersion.txt by default).*

*• Select the **Finger Test** tab to see test images of the scanned fingerprints when swiping your finger over the sensor.*

3 *Click **Close** to close the dialog window.*



Chapter 5 Troubleshooting 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, 2003, Windows XP and Windows Vista 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** sub folder 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 selected to use the Windows password with the fingerprint as the authentication method when selecting multifactor, close the fingerprint verification window and enter your password.*
- *If you use fingerprint as the only one of the multifactor methods without the backup password, there is unfortunately no way 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 (go to **Control Center > Fingerprints > Delete** wizard) and then enroll new fingerprints. Please note that in this case all your stored secret data (passwords, encryption keys) will*

be lost! To perform the delete operation it is necessary that you 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 the multifactor method, you will be asked at the end of the enrollment to verify yourself to unlock secrets on the device.*

I cannot enroll a user in the secure mode.

- *Check for the existence of the user passport. The user is probably already enrolled. Each 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 a user passport?

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

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

I lost my backup password

- *To change the backup password for your multifactor methods, go to the **Enroll or Edit Fingerprints** wizard, verify yourself and go through the Fingerprint enrollment. In the Multifactor dialog, 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 the event 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 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, as 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.

When 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 adding unverified fingerprints).

My TPM module does not work.

If you use TPM (Trusted Platform Module) as the authentication method and the TPM module is broken, erased or disabled, the authentication will no longer work.

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

1. *Enter the **Enroll or Edit Fingerprints** wizard using the backup password.*
2. *Choose a different authentication method in the Multifactor window and click on **Finish** without the need to enroll additional fingers.*

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 authentication method 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 username and password.

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

I cannot changeProtector 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 username and password.*

Password Bank

Registered pages are replayed in Internet Explorer after a delay

Registrations are replayed only after the page in 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 username and password. Complex and non-standard dialogs may cause problems.*

My registration is not replayed correctly.

The Password Bank replay expects that the page used for replaying is exactly the same as it was when the registration was created.

You may encounter problems with pages created dynamically using JavaScript, or with forms which look the same, but the coding has changed.

Possible reasons:

- *Web form internal names have changed. Please edit your registration or create a new one.*
- *The registered dialog caption has changed. Unfortunatelly it is not possible to use the Password Bank registration in this case. Create a new registration.*
- *The registered dialog dimensions have change. Unfortunatelly it is not possible to use Password Bank with dialogs which have different dimensions every time they are displayed.*
- *The dialog does not use Windows controls API (usually dialogs that do not look like standard Windows applications). Unfortunatelly it is not possible to use Password Bank with these dialogs.*

Some registrations are correctly filled but submission fails.

Disable automatic submittion of forms and submit them manually.

1. *Go to the **Control Center > Application > Password Bank**.*
2. *Choose the **Registrations** tab.*
3. *Select a registration and click on **Edit**.*
4. *Uncheck the **Auto Submit Form** checkbox.*

Now when replaing your registration, the form will be filled, but not submitted. You must submit the form manually, i.e. click on the **Submit** button or press the **Enter** key to submit the registration.

Internet Explorer does not display the alert to be set as default browser when Control Center is running.

• Explanation: This is standard Internet Explorer's behaviour. If any instance of Internet Explorer is running (including Web Controls components, e.g. Control Center), Internet Explorer will not display the alert at startup.

Known Issues:

1. *"Registering of 32bit dialogs running on 64bit systems is not supported.*
2. *(Widnows Vista only.) If user account name is "Administrator" (Note: this is built-in account, which is by default disabled), Internet Explorer is not supported with Password Bank. This is because of Windows Vista limitation. Suggested solution: We recommend using different user account. Using the "Administrator" account for daily work is not recommended also for security reasons.*
3. *Sometimes some data can be omitted from a registration as Password Bank may not work correctly with web pages that contain inconsistent, non-standard or inappropriate coding. There is no simple workaround for these pages.*