



Lenovo Security Solution FP



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

The Upek logo is a registered trademark of Upek, Inc. TouchChip, TouchStrip, PerfectPrint, PerfectMatch, PerfectTrust, Protector Suite and Protector Suite QL, Protector Suite 2009 are trademarks or registered trademarks of Upek, Inc. All other products described in this publication are trademarks of their respective holders and should be treated as such.

Upek, Inc. <http://www.upek.com>
Copyright © 2009 Upek, Inc - All Rights Reserved

Table of Contents

1	Installation	1
1.1	Installing Lenovo Security Solution FP	1
1.2	Uninstalling Lenovo Security Solution FP	1
2	Introduction	3
2.1	Fingerprint Enrollment	3
3	Identity	5
3.1	Manage Fingerprints	5
3.1.1	Fingerprint Enrollment	5
3.1.2	Add or Delete Fingerprints	7
3.2	Status	8
3.3	Account Operations	9
3.3.1	Export	9
3.3.2	Import	10
3.3.3	Delete	10
3.3.4	Backup Password	11
3.3.5	Reveal Windows password	12
4	Applications	13
4.1	Application Launcher	14
4.1.1	Creating association between a fingerprint and applications	15
4.1.2	Managing Associated Applications	16
4.2	Password Bank	17
4.2.1	Registering Web Pages and Dialogs	17
4.2.1.1	Registration Wizard	19
4.2.2	Replaying Registrations	21
4.2.3	Manage Registrations	21
4.2.4	Settings	23
4.3	Strong Password Generator	24
4.3.1	Generator	24
4.3.2	Generated Passwords	25
4.4	Encrypted Archives	26
4.4.1	File Safe	26
4.4.1.1	Creating File Safe	27
4.4.1.2	Managing File Safe	28
4.4.1.3	Locking and Unlocking File Safe	30
4.4.1.4	Decrypting Files from a File Safe	30
4.4.2	Personal Safe	31
4.5	E-Wallet	32
4.5.1	Creating E-Wallet records	32
4.5.2	Managing E-Wallet records	34
4.5.3	Filling forms with E-Wallet	35
4.6	Biomenu	35
4.7	Device Lock	36
5	Settings	38
5.1	Windows Logon	38
5.2	Storage Inspector	39
5.3	Select Skin	39
5.4	Sound	40
5.5	Update	40
5.6	Advanced Settings	41
5.6.1	Policies	41
5.6.2	Biometry Settings	42

5.6.3 Sensor Calibration (Optional)	42
6 Other Tools	43
6.1 Fingerprint Tutorial	43
6.2 System Tray Icon	44
6.3 Using Help	44
6.4 Introduction Screen	45
6.5 Managing other users	45



Chapter 1. Installation

1.1. Installing Lenovo Security Solution FP

To install Lenovo Security Solution FP :

1. When the Lenovo Security Solution FP autorun window is displayed, click on **Software Installation**. If this screen does not appear, run **Setup.exe** from the installation folder 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 Lenovo Security Solution FP.

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.



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.

1.2. Uninstalling Lenovo Security Solution FP

To uninstall Lenovo Security Solution FP:

1. Click **Start > Control Panel**.
2. Double-click the **Add or Remove Programs** icon (**Programs and Features** in Windows Vista).
3. Select Lenovo Security Solution FP and click the **Change** button.
4. Click the **Remove** button.
5. You will be asked what to do with Lenovo Security Solution FP data stored on your computer. There are two possibilities:

- **Leave Lenovo Security Solution FP data for later use on your computer.**

This means that if you later re-install Lenovo Security Solution FP, you can continue using the enrolled fingerprints for logging to your computer and accessing data of the fingerprint applications.

- **Remove all Lenovo Security Solution FP data from your computer.**

Enrolled fingerprints and all data in fingerprint applications 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. Introduction

Lenovo Security Solution FP is biometric software that protects the security of your data through the use of fingerprint authentication. Fingerprint authentication is performed by scanning your finger on 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. All the data is stored in the user passport.

This procedure is called Fingerprint Enrollment. To learn how to enroll, see Fingerprint Enrollment.

After you enroll, you will be able to use your fingerprints to:

- replace your windows logon password (see Windows Logon)
- launch favorite applications using your fingerprint sensor (see Application Launcher)
- replace passwords of your favorite web sites or applications by fingerprint (see Password Bank)
- generate strong and complex passwords (see Strong Password Generator)
- encrypt your files and folders (see Encrypted Archives)
- protect private information such as credit card details, account numbers etc.. (see E-Wallet)
- have a quick access to Lenovo Security Solution FP's features through a pop-up menu (see Biomenu)

In case you are not using a full licensed version of Lenovo Security Solution FP all features may not be available or will be available only in a limited mode. When you access a feature that is not fully available in the limited version of Lenovo Security Solution FP, you will be prompted to upgrade. Click on the link to upgrade online.

2.1. Fingerprint Enrollment

Each user identity in Lenovo Security Solution FP is represented by a user account or "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. This process is called fingerprint enrollment.

To create a new user passport (enroll fingerprints):

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan your finger and click on the **Enroll your fingers now** link in the Introduction Screen.
2. Authenticate (Windows password will be required, if you have one). For more detailed instructions, please refer to Fingerprint Enrollment.



Tip

If you experience problems with scanning your fingerprints, see [Fingerprint Tutorial](#).

Chapter 3. Identity

In the Identity section you can work with your user account. You can enroll and delete your fingerprint templates, import, export or delete the complete user's account. The backup password can also be set here.

Before you can start using Lenovo Security Solution FP you must enroll your fingers, i.e. create your fingerprint templates. See Fingerprint Enrollment to get started.

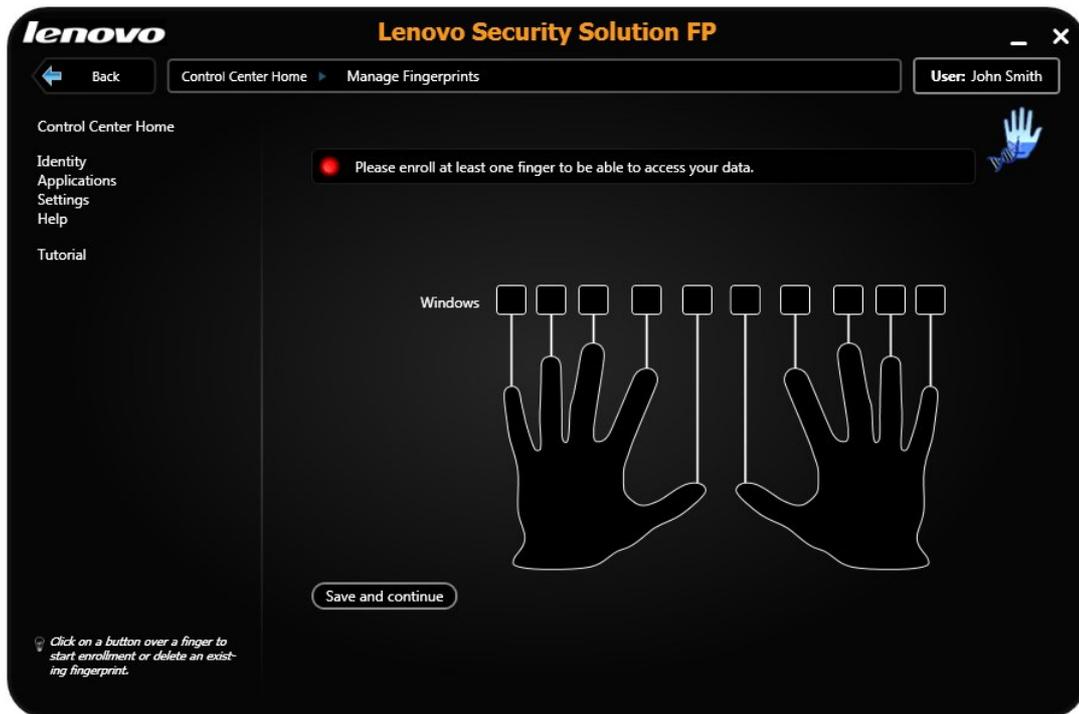
3.1. Manage Fingerprints

Before you can start using Lenovo Security Solution FP you must enroll your 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.

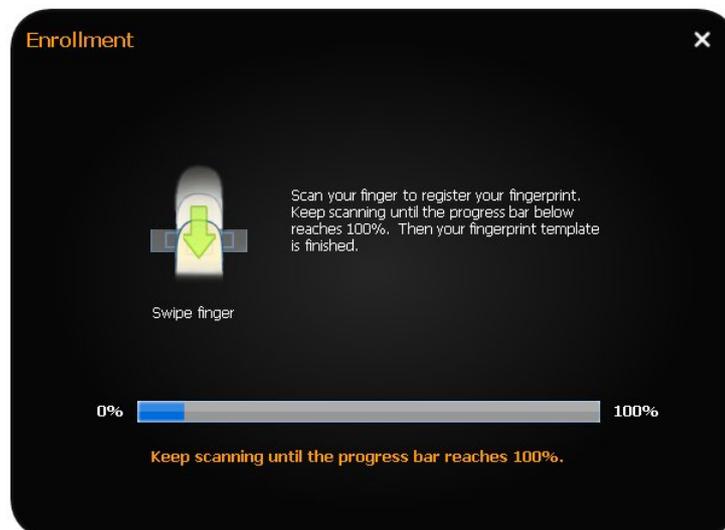
3.1.1. Fingerprint Enrollment

To create a new user passport (enroll fingerprints):

1. If you want to use an external fingerprint sensor, connect your device. All the necessary drivers are installed with Lenovo Security Solution FP. An informational message that the sensor was connected and is ready to use is usually displayed in the lower right corner of your screen.
2. To launch Enrollment, go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan your finger and click on the **Enroll your fingers now** link in the Introduction Screen.
3. The License Agreement is displayed. Read the License Agreement carefully. You must agree to the License Agreement to use this product. Click on **Accept** to continue or click **Do not accept** to close the application if you do not agree to the Licence Agreement.
4. Enter your Windows password and click **Submit**.
5. A dialog with two hands appears. Select a finger to enroll by clicking the button above the finger.



6. Scan the selected finger. Good quality matching fingerprints are required. 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.



Tip

If you experience problems with scanning your fingerprints, see Fingerprint Tutorial.

7. Select another finger to enroll. It is strongly recommended that you enroll more than one finger in the event of injury.



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.

3.1.2. Add or Delete Fingerprints

You can add more fingers into your user account later. It is highly recommended to enroll more fingers in the event of injury. You can delete fingers one by one or delete the complete account (including all your application data).

Add or delete fingerprints of an existing user (manage fingerprints):

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center** .
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Go to **Identity > Manage Fingerprints**.
4. A dialog with two hands appears.
5. **To enroll a new fingerprint:**
 - Select a finger to enroll by clicking the button over the finger.
 - Scan the selected finger until a template is finished. Good quality matching fingerprints are required.

To delete a fingerprint:

- Select a finger to delete by clicking the button over the finger.
- Click **Yes**.

To delete an existing user account (all user's data):



Important

This will delete the complete user account at once including all user data, not just your fingerprints.

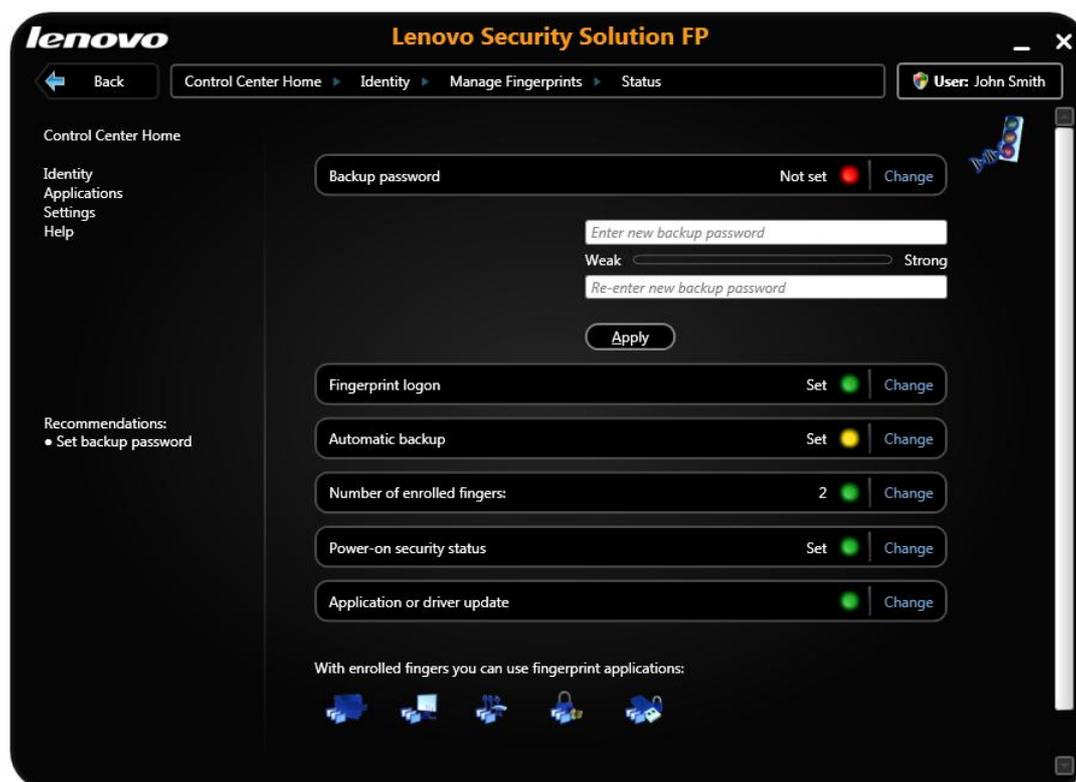
1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center** .
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Go to **Identity > Account Operations > Delete User Data**.

- Click **Yes** to confirm.

3.2. Status

The status page gives you an overview of the software settings and informs you what fingerprint applications are available once you are enrolled.

Red icon signalize that a setting is not in an optimal state. Yellow indicates there is something to be done and green marks a correct setting.



- **Backup password.** Set a backup password and click the **Apply** button. Learn more about Backup Password.
- **Fingerprint logon** will be automatically set after you enroll your fingerprints. When you restart your computer and wish to log on again, scan your finger and you will be logged on automatically. Click **Change** to go to the Windows Logon page and to edit logon settings.
- **Automatic backup** will be automatically set when you enroll your fingerprints and set up the backup password. Your data will be backed up each time you make any changes of your user passport. Click **Change** to go to the Export and set an export mode.
- **Number of enrolled fingers** shows you the number of fingerprints enrolled by the current user. It is recommended to enroll more fingers in the event of injury. Click **Change** to go to the Fingerprint Enrollment and enroll more fingers.
- **Application or driver update.** Click **Change** to go to Update page.

The second part of the summary page gives you information about applications that can be used when fingers are enrolled. If you mouse-over an application picture, you can see a description for each application. Click a picture to go to the application page.

3.3. Account Operations

Import, export or delete current user data.

These operation will affect the current user account (passport). To add or delete an individual fingerprint go to Fingerprint Enrollment.



3.3.1. Export

Existing user data (including fingerprints, encryption keys, logon credentials) can be exported to a file and imported back into your fingerprint software. The file is encrypted and protected by your backup password. Learn more about Backup Password.

To set an export mode:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center .**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit..**
3. Select **Identity > Account Operations > Export user data.**
4. If the backup password is not set, define a password now. Learn more about the Backup Password.
5. Choose a backup mode:

- Click on the **Export Now** button and enter your Backup Password to perform the export immediately. Select a destination folder and set a file name.
- Select **Automatic backup**. Automatic export will backup your passport (i.e. all your data including keys, passwords, enrolled fingers etc.) each time any changes are made to the passport. The default location of the backup file is C:\Users\your username\AppData\Local on Windows Vista and C:\Document and Settings\your username\Local Settings\Application Data on Windows XP. Click **Apply** to save the changes.

Note

Exporting your passport is highly recommended for backup purposes, e.g. in the event of system crash, reinstallation of your system or if you accidentally delete or lose your data.

3.3.2. Import

To import user data (user passport):

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center .**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenue and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Select **Identity > Account Operations > Import user data**.
4. Browse for the passport file (*.vtp).
5. Enter the Backup Password and click **OK**.

Note

You cannot import a passport of an enrolled user. If you want to plan to replace the passport with a backup, it is necessary to delete the current one first.

3.3.3. Delete

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

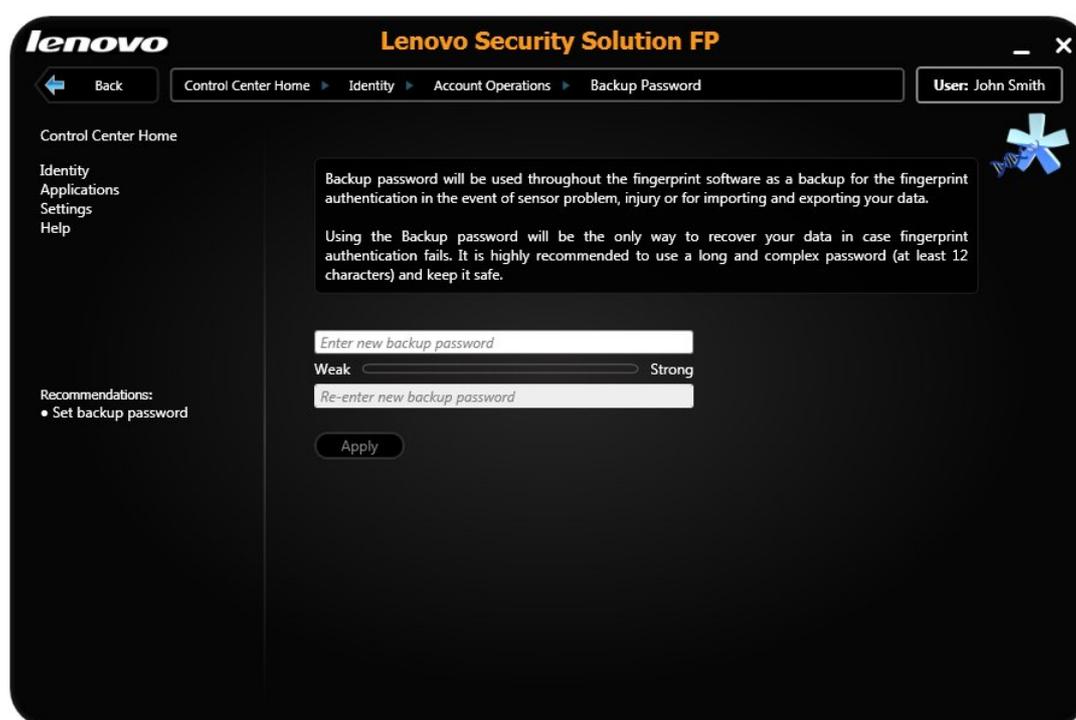
1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center .**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenue and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Go to **Identity > Account Operations > Delete user data**.
4. Click **Yes** to confirm.

⚠ Important

This will delete all data of the current users. Go to Export to backup your data for later use.

3.3.4. Backup Password

Here you can set or edit the backup password. This password will be used throughout the fingerprint software as a backup for the fingerprint authentication (e.g. for exported files).



⚠ Important

Backup password will allow access to your data in the event of a device problem. It is highly recommended to use a long and complex password (at least 12 characters) and keep it safe. A short password may compromise security.

To set the backup password:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center .**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Go to **Identity > Account Operations > Backup password**.
4. Enter and retype the backup password.
5. Click **Apply** to save the changes.

- Click the **Reveal Backup Password** button to see the password in plain text after fingerprint authentication. A dialog will pop-up, click **Reveal** and the password will be shown on your screen so make sure to keep it private and prevent its abuse.

3.3.5. Reveal Windows password

You can see your password after fingerprint authentication. Be aware that your password will be shown in plain text on the screen so make sure to prevent its abuse.

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Select **Identity > Account Operations > Reveal Windows password**.
4. Click the **Reveal** button to see the password in plain text.
5. Authenticate (scan your finger).

Chapter 4. Applications

Make most of your fingerprint sensor by using it for everyday work with your computer. You can make your data more secure and work faster by using fingerprint authentication. After you enroll your fingers, you will be able to use your fingerprint to replace passwords of frequently used web sites and dialogs, launch applications just by scanning your finger, create a secure, convenient storage for your credit cards, PINS and much more.

The fingerprint applications:

- Application Launcher: launch favorite applications simply with your fingerprint scan
- Password Bank: replace passwords of your favorite web sites or applications by a fingerprint scan
- Strong Password Generator: generate strong and complex passwords
- Encrypted Archives: create encrypted archives of your private files and folders
- E-Wallet: protect private information such as credit card details, account numbers etc. and used them to fill web forms more easily
- Biomenu: have a quick access to Lenovo Security Solution FP's features through a pop-up menu
- Device Lock: Lock your connected USB printers and USB storage devices. Each connected device can be then enabled only by scanning your finger.



4.1. Application Launcher

The Application Launcher is an optional feature of Lenovo Security Solution FP. When installed, it enables you to launch registered applications and files by simply scanning your finger. To link an application to a finger, drag and drop (or browse for) an application, a file, etc. and it will be launched next time you scan the assigned finger (e.g. drag and drop the file "document.txt" you have on your desktop, it will be opened in your text editor when you scan the assigned finger next time).



Note

You must enroll at least two fingerprints to be able to use Application Launcher. One enrolled finger is reserved to display the Biomenu.



4.1.1. Creating association between a fingerprint and applications

To link an application to a finger:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Select **Applications > Application Launcher**.
4. A dialog with two hands appears. There is a button above each enrolled finger.



Note

If there is no button available you must enroll your fingers first. If only one button is left it is reserved for the Biomenu and you must enroll more fingers. See Fingerprint Enrollment to learn how to enroll your fingers.

5. Click a button over a finger. The application dialog opens.
6. Click the **Add** button.
7. Enter a title of the application. Click the **...** button to browse for a file you want to launch. This can be any executable file (e.g. calc.exe). Optionally, additional parameters may be entered in the **Advanced** options. See below for examples of application parameters.

- Click **OK**.
- The association has been created. Next time you scan the assigned finger, the application or applications you linked to it will be launched.



Tip

You can also create an association by drag and drop. Drag and drop an application or a file to a button over the hands. The application icon will appear in the button. You can drag and drop the preset applications available from the menu. **Control Center** will launch Lenovo Security Solution FP, **Lock** will lock the computer, **Log off** will log off the current user by scanning the assigned finger and **Web registrations** will launch web sites registered with Password Bank.



Note

If you want to temporarily override launching the application (and invoke the Biomenue instead), hold the **Shift** key when scanning the finger.

Advanced

- 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 scan your assigned finger.

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 opened by Word each time you scan the assigned finger. More than one parameter can be used for one application.
- Startup path:**
An alternative path the application will start in.
- Launch when:**
Choose optional hotkey combination. Only after you press this combination and scan the associated finger, the application will be launched.

4.1.2. Managing Associated Applications

To delete the fingerprint/application association:

- Go to
 - Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenue and select **Control Center...** (skip the next step).
- Authenticate (scan your finger or enter your password) and click **Submit**.
- Select **Applications > Application Launcher**.
- Click on the application icon in the button above the assigned finger.
- Click on the **Delete** button under the application you wish to delete.

6. Click **Yes** to confirm deleting the association. The finger is now free for another application.

To edit the fingerprint/application association:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Select **Applications > Application Launcher**.
4. Click on the application icon in the button above the assigned finger.
5. Select an application and make any desired changes.
6. Click **OK**.

4.2. Password Bank

When installed, the Password Bank stores registrations (usernames, passwords and other settings) of your web sites and application dialogs. You can access frequently visited web sites and applications (web mail, bank accounts, e-commerce, etc.) securely, without the hassle of re-entering passwords, usernames 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.

Password Bank supports the following browsers: Internet Explorer 5.0 and higher, Firefox 1.0 - 3.0. Support for Internet Explorer is installed automatically. When Firefox is set as the default browser and Lenovo Security Solution FP 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 **Applications > Password Bank > Settings**.

Note

Password Bank is intended to store simpler web pages and dialogs (e.g. login credentials).

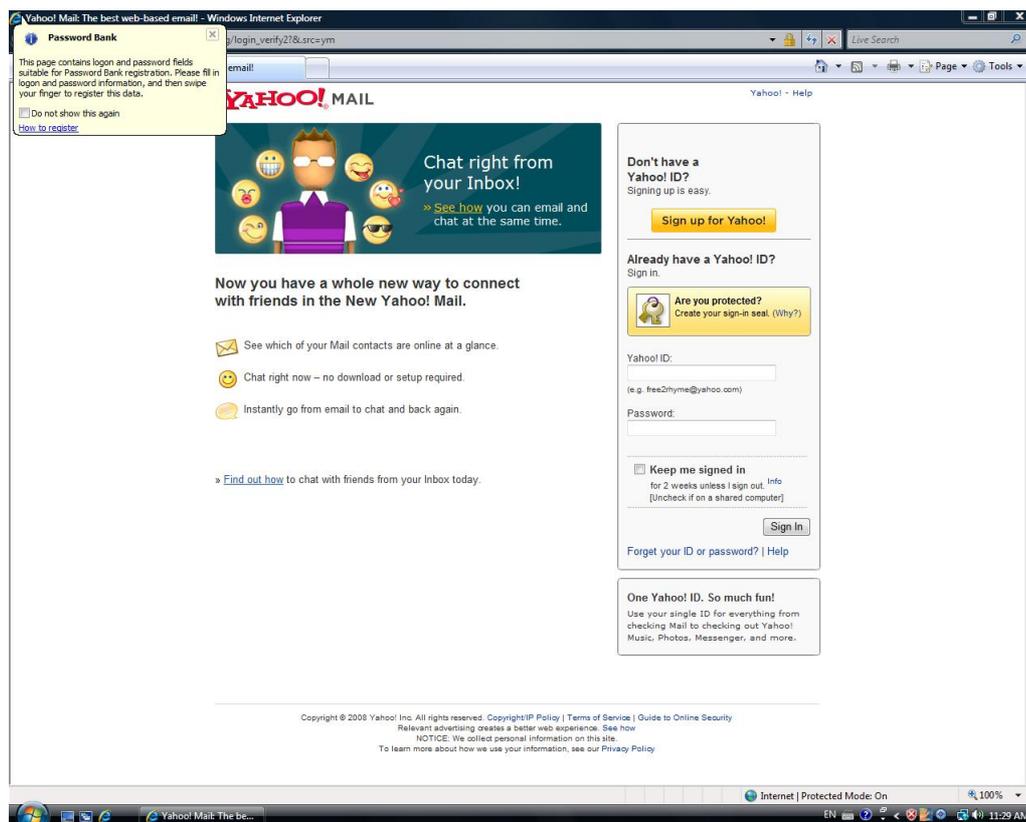
To fill in more complex forms automatically, use the E-Wallet application.

4.2.1. Registering Web Pages and Dialogs

You must register a web site or a dialog to store your credentials (such as usernames and passwords) to replay it later, i.e. automatically fill it in after you authenticate (scan your finger).

To create a new registration:

1. Display a web page or a dialog you want to register.



2. Fill in the username, password, and any other necessary fields.
3. Scan an enrolled finger to display the Biomenue. 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**.



4. The **Registration Wizard** (see below) appears to guide you through the new registration. Click **Next** to review and edit your registration. You can also check the checkbox at the bottom of the dialog to store your registration as it is and click **Finish** to skip the wizard.

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.

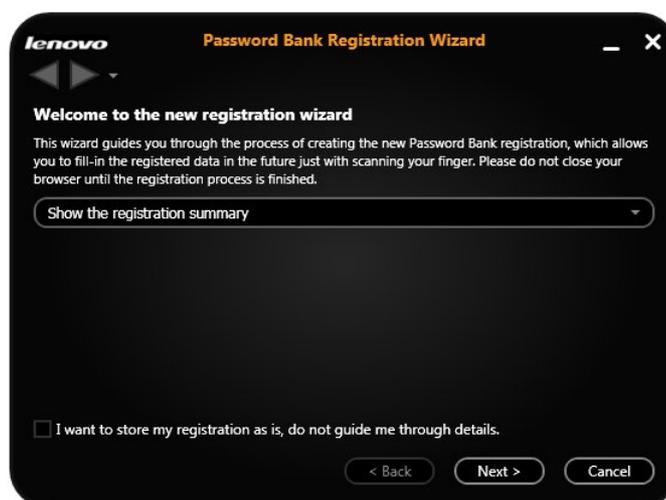
Note

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 Password Bank Settings

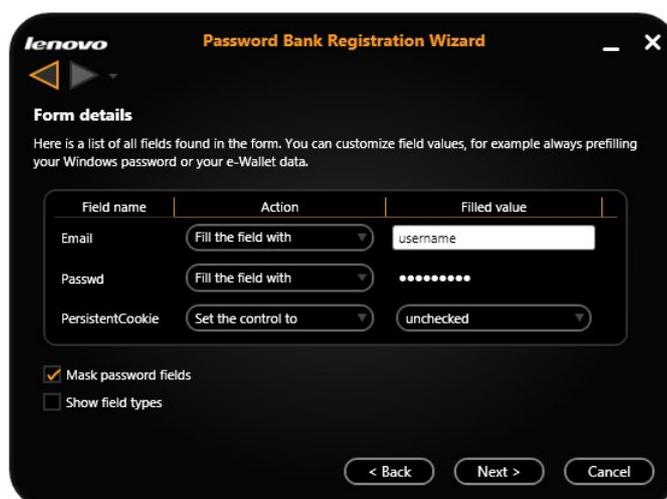
4.2.1.1. Registration Wizard

The **Registration Wizard** appears to guide you through a new registration.

1. A dialog is shown with the web page name and data just filled in. If this is correct click **Next**. If this is not the page you want to register, click **Cancel** to quit the wizard and start a new registration.
2. Click **Next** to review and edit your registration.



3. **Form details** page is showing all the items that are to be registered.



You can change the value of the form fields that were registered. Select **Set the control to** to select from a list of predefined values or disable filling this field by selecting **Do not set this control**.

- **Fill the field with.** This will fill the field with the value you entered in the web browser. You can rewrite it now if required.
- **Do not fill this field.** This will not fill anything in this field automatically when replaying the registration.
- Use filling the Windows username, password or domain in this form field when replaying the registration. This is convenient as if the credentials are changed, this value will be updated automatically and you do not have to change your registration.
- You can also use other fingerprint applications for filling the form fields such as Strong Password Generator for filling a password field with a strong password you generated. Select an application from the list. Only applications currently available will appear in the list.

i Note

Unchecking the **Mask password** checkbox will show all passwords in plain text.

4. Click **Next** to continue.
5. In **Form submission method** page choose how the registered form will be submitted after authentication. Uncheck the field to fill the form but not to submit it.

Click **Show advanced options** to select the way forms will be submitted. As default, Password Bank submits the form as if the Enter key was pressed. If this does not work, select the option to choose a button manually. Drag and drop the pointer icon to a button on the page. This button will be used to submit the page instead.

6. In the next page test the registration. This will try to replay your new registration in the web browser. Check if everything works as expected. If there is a problem with the registration, go back and edit the registered fields or follow the troubleshoot steps.
7. Click **Next** to continue.
8. In the next page you can choose a registration name and folder as it will appear in the **Control Center** where you can manage your registrations later.

9. Click **Finish**.

4.2.2. 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. Authenticate yourself (scan your finger).
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. Scan 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.



Tip

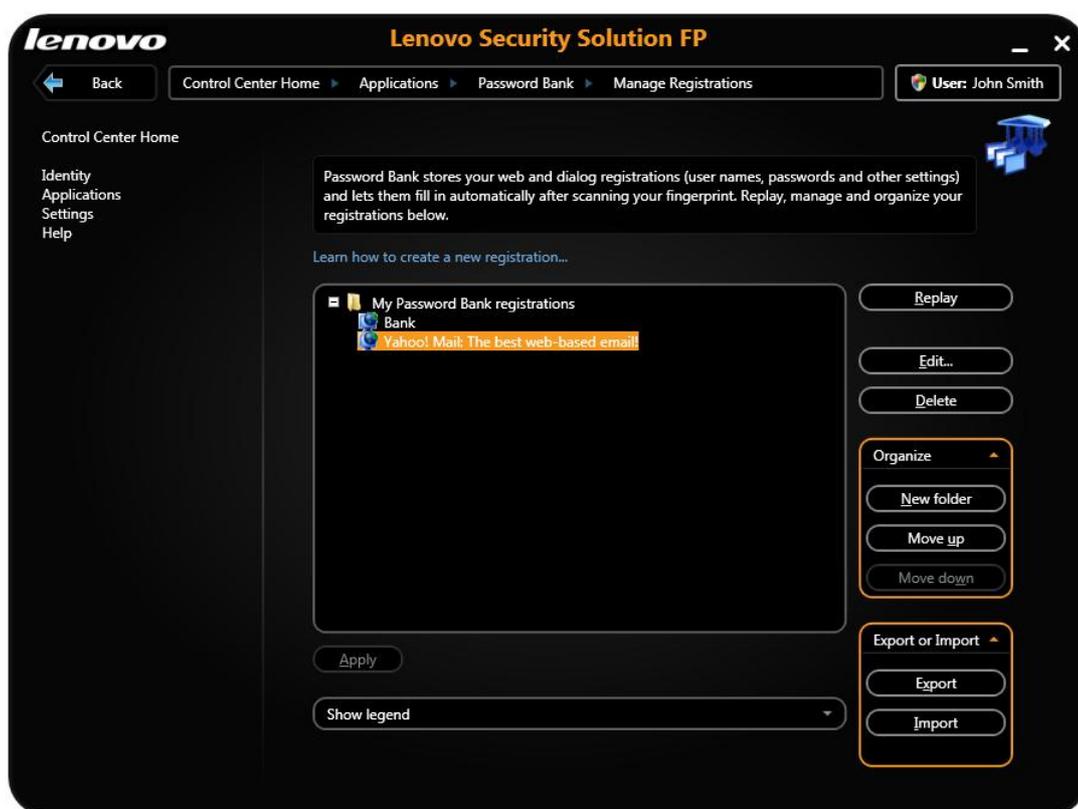
You can also replay registrations by selecting a registration and clicking on the **Replay** button in the **Control Center > Applications > Password Bank > Manage Registrations**. See Manage Registrations for more information.

4.2.3. Manage Registrations

It may be useful to edit your existing registration - e.g. if you changed the password of your mailbox. You can also delete your registrations, organize them into folders 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 or *.xml extension and can be imported later.

To manage registrations:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Select **Applications > Password Bank > Manage Registrations**.



4. Select a registration you want to work with.

- Click the **Replay** button to replay the selected web registration. It will be launched in your default browser.
- 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.)

Here you can change the name of the registration as it appears in the registration list and the Biomenu. 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 authenticate (scan your fingerprint).

To learn more about the registered fields see the Password Bank Registration Wizard.

Click **Apply** to save the changes.

- Click **Delete** to delete the registration completely.
- Click **Organize** to organize the registrations into folders, move registrations up and down the list and create folders. The same structure will appear in the Biomenu Registered sites.
- Click **Import or Export** to backup your registration or import saved registrations to the fingerprint software.

Click the **Export** button to export your registration e.g. for use on another computer. Either the selected registrations will be exported or all existing registrations will be exported at once. 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** or ***.xml**.

Click the **Import...** button to import registrations from a Password Bank file. Select the source ***.pb** or ***.xml** 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 **Apply** to save the changes.

4.2.4. Settings

Password Bank lets you use the fingerprint authentication to access protected websites and dialogs.

Select what you want to use Password Bank for...

- **Windows Dialogs** check box will enable using Password Bank for storing credentials of standard Windows applications.
- **Internet Explorer** support is always present, the check box enables or disables using the browser.
- 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.

Password Bank displays hints for the user when an action like registering a dialog, replaying a dialog, etc. is possible. If the user logs into Windows using username and password, the hints are not active until a successful fingerprint authentication is performed.

To turn Password Bank hints on/off:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Select **Applications > Password Bank > Settings**.
4. **Select the hint to be displayed to ask if:**
 - **submitted form data should be remembered.** This will turn on/off the dialog prompting for Password Bank registration after a form (on a web page or a dialog) is submitted.

Select the hints to be displayed to alert you if:

- **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.

- **a dialog could be replayed.** This hint informs the user that replaying the registration is possible.
- **a dialog is suitable for registration.** This hint informs the user that the dialog contains a password field that can be registered.
- **a web site could be replayed.** This hint informs the user that replaying the registration is possible.
- **a web site is suitable for registration.** This hint informs the user that the page contains a password field that can be registered.

4.3. Strong Password Generator

Strong Password Generator allows you to generate complex passwords immune to dictionary attacks. Generated passwords are saved and used where needed. They can also be used when registering web forms using the fingerprint.

4.3.1. Generator

To generate a strong password:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Select **Applications > Strong Password Generator > Generator**.



4. Enter a name into the **Password name** field.

5. Choose password length.

Check the **Mask generated password** checkbox if you do not want to show the generated password in plain text.

Check the **Do not store generated password** checkbox if you do not want to store the password in the Generated Passwords page. If not checked, all generated passwords will be listed there.

6. Click the **Generate** button.

7. Now you can drag and drop it, use the **Copy to clipboard** button or the right-click menu to copy the password to clipboard and paste it where desired.

Click **Advanced options** to generate passwords according to more detailed specifications, e.g. generate passwords composed from specific combinations of characters, hexadecimal passwords etc.



Note

The strength indicator shows you the strength of the password that will be generated. You can adjust the strength by changing password length or the advanced settings.

4.3.2. Generated Passwords

Review and manage your strong passwords. You can review the generation time, the related web site and find out whether the password is being used by any of your Password Bank registrations.

1. Go to

- **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
- or right-click on the tray icon and select **Start Control Center...**
- or scan a finger to display the Biomenue and select **Control Center...** (skip the next step).

2. Authenticate (scan your finger or enter your password) and click **Submit**.

3. Select **Applications > Strong Password Generator > Generated Passwords**. Authentication is required.

4. Select a password you want to work with. Click a button below:

Check the **Mask password fields** checkbox if you do not want to show the passwords in plain text.

Use the **Copy to Clipboard** button or the right-click menu to copy the password to clipboard and paste it where desired.

Delete. Will delete the selected password. Use **Ctrl+A** to select all passwords.

5. Click **Apply** to save the changes.

You can use generated complex passwords for web forms to increase the security of your credentials. You can use Password Bank to register your login credentials and replay it after fingerprint authentication. You will have a strong and complex password to make your registrations more secure without the hassle of remembering the complicated password. Just scan your finger and the registration will be replayed by Password Bank.

To register a strong password with Password Bank:

1. Generate a strong password. See Generator.
2. Display a web page you want to register.
3. Scan your finger to display the Biomenu.
4. Select **Register** from the menu.
5. Registration Wizard appears.
6. Existing generated passwords will be automatically detected. Choose a generated password or use the one that was detected as default.
7. Go through the rest of the registration with the Registration Wizard as usual. You can change the password in the **Form details** page when reviewing the registration.
8. Finish and test the registration.
9. The credentials are now registered and can be replayed automatically next time.

To replay a strong password registration with Password Bank:

1. Display a web page or application you have registered.
2. (Optional) A hint appears informing you about an existing registration.
3. Scan your finger.

4.4. Encrypted Archives

Encrypted Archives allows you to protect your private files and folders by fingerprint and backup password and keep them safe from an unauthorized access.

File Safe allows you to create encrypted archives of important files and folders that will be protected by your fingerprint and backup password. You can keep the files in their current location and by adding them to an File Safe archive protect them by fingerprint authentication.

Personal Safe is a protected folder on your Desktop or in My Computer where you can drop or copy your files and keep them conveniently in one place safely protected by fingerprint.



Note

You must enroll your fingerprints and setup the backup password before creating an archive. Otherwise, a warning that no users are selected will appear. See Fingerprint Enrollment to learn how to enroll your fingerprints.

4.4.1. File Safe

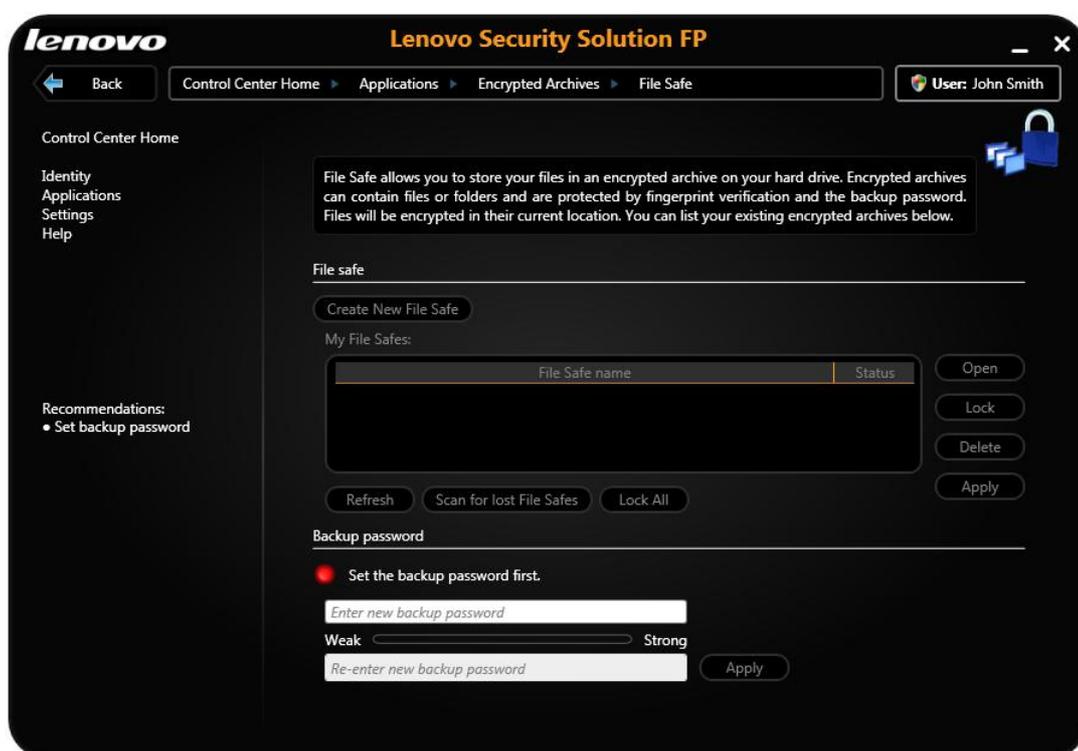
File Safe allows you to store your files in an encrypted archive on your hard drive. Encrypted archives can contain files or folders and are protected by fingerprint authentication and the backup password. When a File Safe archive is unlocked, you can work with the archive file as with a standard folder (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.

4.4.1.1. Creating File Safe

To create a new File Safe:

- Go to
 - Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
- Authenticate (scan your finger or enter your password) and click **Submit**.
- Select **Applications > Encrypted Archives > File Safe**.



- If the backup password is not set, enter a password and click **Apply**. Learn more about the Backup Password.
- Click the **Create New File Safe Archive** button.
- Set a name for the new archive.
- Now 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.
- Click **Lock** to lock the archive.

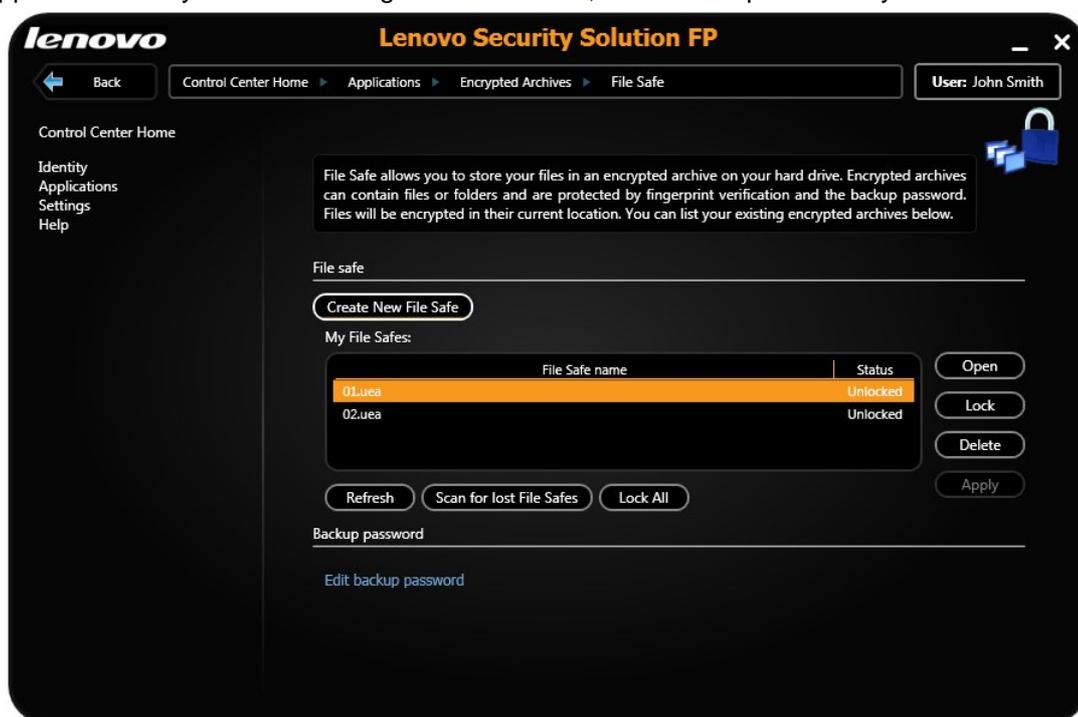
Note

You can also create or manage archives from the context menu. Display the files or folders you would like to encrypt (using Windows Explorer or other Windows dialog and right-click to display the context menu). Select **Add to new encrypted archive...** to add the selected file or folder to a new archive.

4.4.1.2. Managing File Safe

To manage existing File Safe:

- Go to
 - Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
- Authenticate (scan your finger or enter your password) and click **Submit**.
- Select **Applications > Encrypted Archives > File Safe**.
- Existing archives are listed. Select an archive or archives. Click a button to **Open**, **Lock**, or **Delete** the selected archive. You can also use the context menu. If an archive is opened, you can work with the archive as with a standard folder (delete, copy, or rename files, etc.). Drag and drop is also supported. When you finish working with the archive, lock it to be protected by authentication



To work with the list of File Safe archives, choose:

- Refresh** to get an up to date list of all listed archives associated with your fingerprints.
- Scan for lost File Safes**. Choose this option to list all archives including those that are not associated with your fingerprints or those that were moved. You can still open the unassociated

archives using your backup password. Use when you are not sure where are your archives or when you changed your fingerprint passport.

- **Lock All.** Will lock all listed archives at once.

5. Click **Apply** to save the changes.

Tip

You can manage archives from the context menu, such as adding files or folder directly from your file manager. Display the files or folders you would like to encrypt (using Windows Explorer or other Windows dialog and right-click to display the context menu. Select **Add to existing encrypted archive...** to add the selected file or folder to an existing archive. See below for detailed description.

To add files or folders to an existing File Safe:

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** or ***.ueaf** 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:
 - a. **Delete original files** will delete the original files and will keep the files just in the encrypted form in the archive.
 - b. 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.

- c. **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.
8. The files are now added to your encrypted File Safe archive.

4.4.1.3. Locking and Unlocking File Safe

To Lock or Unlock a File Safe:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Select **Applications > Encrypted Archives > File Safe**.
4. Existing archives are listed. Select an archive or archives. Click the **Lock** button to lock and archive or the **Open** button to unlock it.



Tip

You can also lock or unlock archives in their current location outside the Control Center. Display the archive you would like to lock or unlock (using Windows Explorer or other Windows dialog), select the archive file (*.uea or *.ueaf), right-click to display the context menu and select **Lock** or **Unlock**.

To lock all File Safe archives:

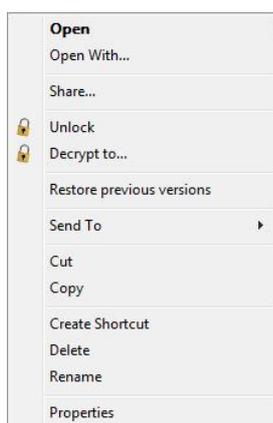
1. Scan your finger to display the Biomenu.
2. Select **Lock all archives** from the menu.
3. All your unlocked archives are now locked.

4.4.1.4. Decrypting Files from a File Safe

To remove a file or files from an encrypted archive, unlock the archive (see Locking and Unlocking File Safe) and then work with the files as if they were in a standard folder, you can delete, copy or drag them out of the archive. See below how to decrypt all files from the archive at once into a specified location.

To decrypt all files or folders in a File Safe 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.
5. Your files are now decrypted in the destination location.

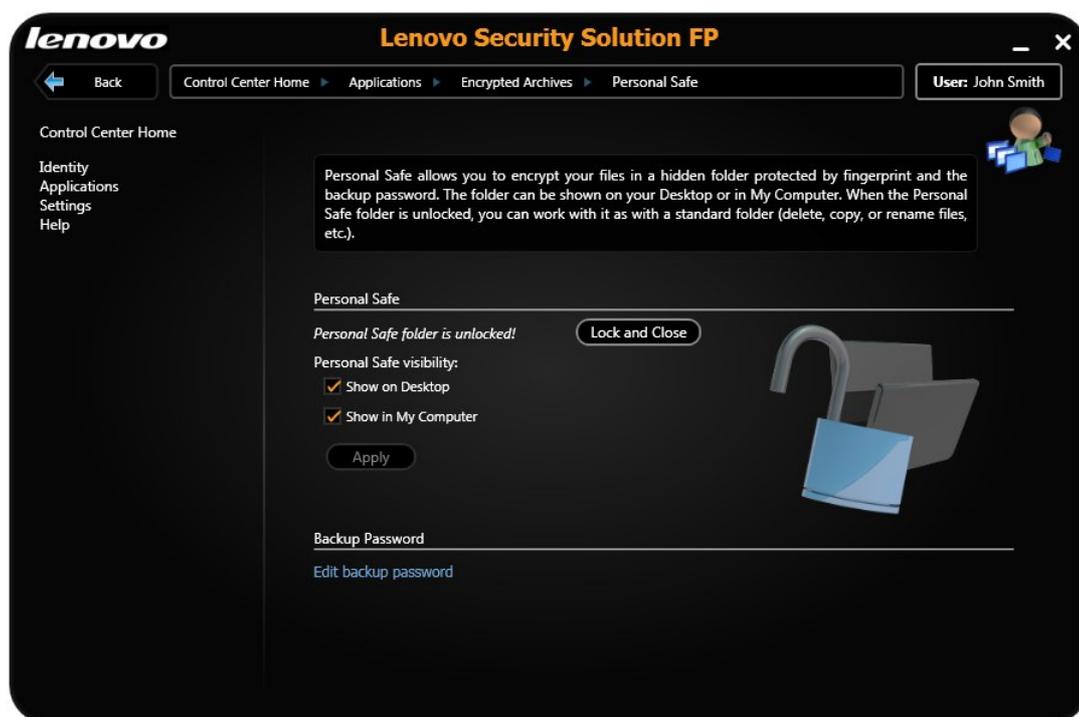
4.4.2. Personal Safe

Personal Safe allows you to encrypt your files in a protected 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.

When the Personal Safe folder is unlocked, you can work with it as with a standard folder (delete, copy, or rename files, etc.). It can be managed from the **Control Center** in **Applications > Encrypted Archives > Personal Safe** or through the context menu by right-clicking on the Personal Safe folder.

To lock/unlock Personal Safe

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Select **Applications > Encrypted Archives > Personal Safe**.



4. If the backup password is not set, enter a password and click **Apply**. Learn more about the Backup Password.
5. Click the **Unlock and Open** or **Lock and Close** button.



Tip

A status message is shown whether the Personal Safe is locked or unlocked.

To add files to Personal Safe

1. Open Personal Safe. Either from Control Center (see above) or select the folder and right-click to display the context menu and select **Lock** or **Unlock**.
2. Drag and drop or copy files into the folder or select the files (or folders) and right-click to display the context menu and choose **Add to Personal Safe**.

4.5. E-Wallet

Biometric E-Wallet offers you a safe and convenient way to store all your important information (such as credit card details, account numbers etc.).

Your private data will be always at hand and safely protected by the fingerprint authentication.

E-Wallet can also help you with filling complex forms by storing details you are using frequently, e.g. when shopping online. You can save your data into a fingerprint-protected profile (see Creating E-Wallet records and later drag and drop them where needed (e.g. into web forms).

4.5.1. Creating E-Wallet records

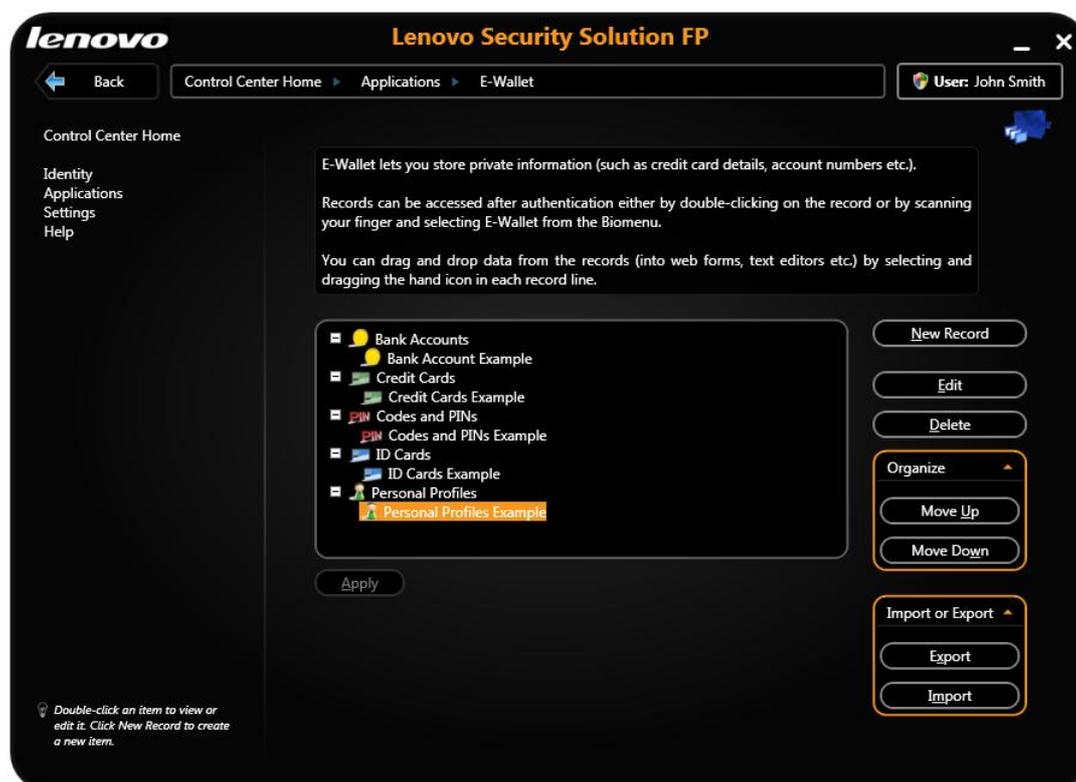
Use predefined categories to organize your data into folders or create new custom ones. All predefined categories have an example available. You can either open and rewrite the example or create a new

E-Wallet record (see below). Access records by double-clicking a record and authenticate by scanning your finger.



Tip

Use the **Personal Profiles** to create profiles to save information frequently used in complex web forms.



To create a new E-Wallet record

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Select **Applications > E-Wallet**.
4. Click the **New Record** button and select a predefined category from the drop down menu or select **New Category...** and choose a name and icon to create your own blank category.
5. **Enter or Edit your record data:**
 - Change the name of the record by retyping the **New Record** line.
 - To enter data, select the value and click the **Edit Value** button.

- Click the **Rename** button to change the title.
 - Click the **Add** button to add a new line at the end of the list.
 - Click the **Delete** button to delete the selected line.
6. Click **Apply** to save the changes.



Note

You can access your records by scanning your finger, displaying the Biomenu and selecting **E-Wallet**.

4.5.2. Managing E-Wallet records

To manage an E-Wallet record

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Select **Applications > E-Wallet**.
4. Select the record you want to work with
 - To edit double-click it or click the **Edit** button. Authentication is required (scan your finger).

Enter or Edit your record data:

- To enter data, select the value and double-click or click the **Edit Value** button.
 - Click the **Rename** button to change the title.
 - Click the **Add** button to add a new line at the end of the list.
 - Click the **Delete** button to delete the selected line.
 - Click **Organize...** and the **Move Up** or **Move Down** buttons to move records up and down the list and organize them into the folders.
 - Click **Import or Export** to backup your records or import saved records to the fingerprint software.
 - Click the **Export...** button to export your records e.g. for use on another computer. Then select a destination file. The file extension of E-Wallet files is ***.xml**.
 - Click the **Import...** button to import registrations from an E-Wallet file.
5. Click **Apply** to save the changes.

4.5.3. Filling forms with E-Wallet

E-Wallet is designed to help you with filling complex forms by using data you saved in it. To register simple credentials, such as a name and password, use the Password Bank application. See Registering Web Pages and Dialogs how to register login credentials.

To create strong and complex password, consider using Strong Password Generator.

To fill a form using E-Wallet:

1. First you need to create an E-Wallet record containing your profile information in the **Control Center > Applications > E-Wallet**. For detailed instructions see Creating E-Wallet records.
2. Display a web page with a form to be registered (e.g. registration form for an online shop).
3. Scan a finger to display the Biomenu and select **E-Wallet**.
4. Select a record you want to use (e.g. Personal Profiles > My Bookstore Profile) or select **Show entire E-Wallet** to display the E-Wallet page.
5. A page with all the record details will be displayed. Now drag and drop the hand icon before each item into a form field or where desired.

Note

You can also use E-Wallet to fill a form field when you are going through the Registration Wizard .

Records can be accessed after authentication either by double-clicking on the record or by scanning your finger and selecting E-Wallet from the Biomenu.

Tip

In the Biomenu select **E-Wallet > Show entire E-Wallet** to display the E-Wallet application as you can see it in the Control Center.

4.6. Biomenu

Biomenu is a pop-up menu that provides quick access to fingerprint software features and settings.



To display the Biomenue in a situation when finger authentication invokes another action (e.g. a registered page is replayed), hold the **Shift** key when scanning your finger.

- To display the Biomenue scan an enrolled finger.
- **Lock computer.** Provides a quick way to lock your computer. Scan your finger to unlock the computer again.
- **Unlock device (optional).** When the Device Lock is set, a list of locked devices is displayed. You can choose a device from the list to unlock it.
- **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 Settings.
- **Register...(optional).** Registers a new window (a web page or dialog). To learn more about Password Bank registration, see Password Bank
- **E-Wallet.** Gives a quick access to E-Wallet records. Select a record you want to use (e.g. Personal Profiles > My Bookstore Profile) or select **Show entire E-Wallet** to display the E-Wallet page
- **Unlock and Open/Lock Personal Safe (optional).** Gives access to the Personal Safe folder.
- **Strong Password Generator.** Opens the Strong Password Generator page where you can create strong complex passwords and copy them to clipboard.
- **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.
- **Help.** displays the HTML help. To display context-sensitive HTML help, press F1 in the dialog box for which you need help.

4.7. Device Lock

Device Lock protects data on your computer from being taken away or printed by an unauthorized person. Connected USB printers and USB storage devices can be enabled only by scanning your finger. No information is saved to the devices, authorization will be required only on your computer.



Important

When you set USB device locking, authentication will be required to unlock USB printers and USB storage devices you connect to your computer.

To set USB device locking:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenue and select **Control Center...** (skip the next step).

2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Select **Applications > Device Lock**.
4. If the **Edit** button is visible on Windows Vista, you must click it and elevate before you start to make changes in the individual setting pages.
5. Select a radio button:
 - **Do not use the device lock feature.** The device lock is off. The device can be used without fingerprint authentication.
 - **Connected devices can be unlocked by any enrolled user.** The device is locked when connected. Any user can unlock it after successful authentication (scanning an enrolled finger).
 - **Connected devices can be unlocked only by the current user.** The device is locked when connected. Only the current user can unlock it after successful authentication (scanning an enrolled finger).
 - **Connected devices can be unlocked only by an administrator.** The device is locked when connected. Only a user with administrative privileges can unlock it by scanning an enrolled finger.



Note

Unless you select the first option, all devices will now be locked. Authentication will be required to unlock all USB printers and USB storage devices you connect to your computer.

6. Click **Apply** to save the changes.

To unlock USB devices:

When Device Lock is activated, you will be prompted for authentication when you connect a USB printer or a USB storage device to your computer. After authentication, the device will be unlocked and can be used as usual.

Or you can use the Biomenue to select a locked device and unlock it.

1. Scan a finger to display the Biomenue and select **Unlock Device**.
2. When the Device Lock is activated, a list of locked devices is displayed.
3. Choose a device from the list.

Chapter 5. Settings

The Settings contain various options for setting up Lenovo Security Solution FP. Not all the functions of the Settings described here may be visible, the available functions vary according to installed version of Lenovo Security Solution FP and administrative privileges of the current user. If the **Edit** button is visible on Windows Vista, you must click it and elevate before you start to make changes in the individual setting pages.



5.1. Windows Logon

To enable fingerprint logon, you must enroll your fingerprints (see Fingerprint Enrollment). 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, scan your finger and you will be logon automatically.

Fingerprint logon will be automatically set when you enroll your fingerprints.

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).

Biometric logon can be disabled in Windows in Biometric Devices Control Panel. Either enter biometric settings from the Windows Control panel or open it from Lenovo Security Solution FP:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Select **Settings > Windows Logon**.

4. Click on the **Biometric Devices Control Panel** link to open the Windows biometric settings.
5. You can adjust the biometric logon settings by selecting the **Allow to bypass logon using Windows password**. If this option is checked, the standard Windows logon can be used. If unchecked, only administrators can logon using username and password.

5.2. Storage Inspector

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 in Lenovo Security Solution FP.

To remove fingerprints from the device:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Go to **Settings > Storage Inspector**.
4. Select the record you want to delete and click the **Remove fingerprint** button. The list of records will be updated to reflect the change.
5. Click **Apply** to save the changes.



Note

The authorization to remove fingerprints is defined in the Security policies settings (see Policies). Some rights may be restricted to administrators only.

5.3. Select Skin

To select a look for Lenovo Security Solution FP

Lenovo Security Solution FP will restart with the new skin. To change the skin back, repeat the steps and select the desired skin.

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Go to **Settings > Select Skin**.
4. Select a skin from the menu.

5. Click **Apply** to save the changes.
6. Click **Yes** to restart the application. The application must be restarted to apply the new skin.

5.4. 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) .

To select sound for Lenovo Security Solution FP.

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to the Biomenu and select **Control Center...(skip the next step)**.
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Go to **Settings > Sound**.
4. Select **None** to switch off the sounds, **System default** to leave the default sounds for the operation or select **Custom** and browse for your own audio files (.wav format).
5. Click **Apply** to save the changes.

5.5. Update

When an update is available, click the Download button to get the latest version of the fingerprint software. When an automatic check for update is set, checking for a new update will be performed each time Control Center is started.

To set up Update:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Go to **Settings > Update**.
 - **Update Status.** Informs you about the current state of the software. When a newer version of Lenovo Security Solution FP is available, click the **Download Update** button to get the update.
 - **Update Check.** Check for current updates either manually by clicking the **Check for Update Now** button or check the **Check for updates automatically** checkbox to keep the status messages up to date. Checking for a new update will be performed each time Control Center is started.
 - Click **Apply** to save the changes.

5.6. Advanced Settings

Set advanced options for security policies, biometry security and performance.

To open Advanced Settings:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Go to **Settings > Advanced Settings**.

5.6.1. Policies

Policies settings can be set up differently for an administrator and limited users. Select and choose **Yes** or **No** to set a policy on or off.

Enrollment

- **Enroll self:** Allows the currently logged on user to enroll fingerprints.
- **Enroll other users:** Allows the currently logged on user to enroll other users' fingerprints. Only users with a valid Windows account can be enrolled.
- **Edit self:** Allows a fingerprint passport to be edited for the currently logged on user, e.g. adding or deleting enrolled fingerprints.
- **Edit other users:** Allows a fingerprint passport to be edited for any user enrolled on this computer, e.g. adding or deleting enrolled fingerprints.
- **Import self:** Allows a fingerprint passport to be imported for the currently logged on user.
- **Import other users:** Allows a fingerprint passport to be imported for any user enrolled on this computer.
- **Export self:** Allows a fingerprint passport to be exported for the currently logged on user.
- **Export other users:** Allows a fingerprint passport to be exported for any user enrolled on this computer.
- **Delete self:** After authentication allows a fingerprint passport to be deleted for the currently logged on user.
- **Delete other users:** Allows a fingerprint passport to be deleted for any user enrolled on this computer. No authentication is required before passports are deleted.
- **Reveal Windows password:** Allows the user's Windows password to be revealed.
- **Always verify user to access sensitive data:** User is always asked to perform verification when accessing sensitive data, eg. stored passwords, registrations.

- **Logon for self enroll:** Allow not enrolled limited users to logon using password when password logon is disabled for limited users.

Fingerprint Storage Inspector

- **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).
- **Delete any fingerprints:** Allows any fingerprints to be deleted from your device. (The Use Fingerprint 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 Fingerprint 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 Fingerprint Storage Inspector policy must be enabled for this policy to take effect.)

5.6.2. Biometry Settings

Lenovo Security Solution FP can operate in two security levels. Choosing one will set up how accurately a fingerprint scan must match the enrolled samples.

- **Convenient Level.** The default biometric processing level which keeps security and convenience in balance.
- **Secure Level.** Use when security is more important than convenience. It provides the highest security, but please note that a perfect match with the enrolled sample is required, which may result in repeated unsuccessful authentications for authorized users.

Lockout Settings

- **Number of failed attempts before lockout:** sets how many unsuccessful attempts for verification (finger scans) are allowed before the device is locked.
- **Duration of lockout:** sets for how much time (in seconds) the device will stay locked. After this time the fingerprint sensor can be used again.

5.6.3. Sensor Calibration (Optional)

This feature allows you to calibrate your fingerprint sensor. Use when you experience difficulties with scanning your finger. This will not affect your enrolled fingerprint samples or data of the applications.



Important

Do not touch the sensor during calibration.

If supported by your sensor, the **Calibrate Sensor...** button 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.

Chapter 6. Other Tools

This section describes other tools that can help you with using the Lenovo Security Solution FP such as Using Help .

6.1. Fingerprint Tutorial

It is highly recommended that you go through the fingerprint tutorial. The tutorial shows you short animations demonstrating correct and incorrect fingerprint scanning. You can try to create your fingerprint samples to practice the technique.

To run the tutorial:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Click the **Tutorial** link or authenticate (scan your finger or enter your password), click **Submit** and go to **Help > Tutorial**.
3. See animations to follow the correct scanning procedure. On the right side you can practice scanning your finger.



4. To achieve correct fingerprint scans:

For the swipe sensor:

- Position the last knuckle joint over the center of the sensor.
- Lay your finger flat on the sensor.
- Do not lift your finger as you swipe over the sensor.
- Do not swing your finger sideways at the end of the movement.
- Try creating samples of your fingerprint.

6.2. System Tray Icon

The Lenovo Security Solution FP 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:

**Tray icon items:**

- **Start Control Center...** Starts the main dialog of Lenovo Security Solution FP, where you can manage most features and applications and change the software settings.
- **Help.** Displays the complete help for Lenovo Security Solution FP. To display context-sensitive help for a specific page, press F1 in the page for which you need help.

6.3. Using Help

Lenovo Security Solution FP contains an HTML-based help system.

**Tip**

You can also right-click on the tray icon and select **Help** or scan a finger to display the Biomenu and select **Help**.

To display context-sensitive help:

- Press F1 to display the help in the page for which you need help.
1. Go to **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**

2. Click the **Help** link or authenticate (scan your finger or enter your password), click **Submit** and go to **Help > Help**.

6.4. Introduction Screen

The Introduction Screen is shown when you touch the sensor when no fingerprints are enrolled. It contains a link to the Lenovo Security Solution FP Product Tour and a link to fingerprint enrollment.

To access Product Tour later:

- Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
- Authenticate (scan your finger or enter your password) and click **Submit**.
- Go to **Help > Product Tour**.

6.5. Managing other users

As an administrator you can manage other users in Lenovo Security Solution FP. You can set or delete a new user, users' data can be deleted, imported or exported.

To manage other users:

1. Go to
 - **Start > All Programs > Lenovo > Lenovo Security Solution FP > Control Center**
 - or right-click on the tray icon and select **Start Control Center...**
 - or scan a finger to display the Biomenu and select **Control Center...** (skip the next step).
2. Authenticate (scan your finger or enter your password) and click **Submit**.
3. Go to **Identity** and click on the **Manage other users...** link.

OR

Click on the user button next to the navigation bar.
4. Select a user and choose an action using the buttons from the menu.