Panasonic®

Supplementary Instructions for Fingerprint Reader

Personal Computer

Model No. CF-19 / CF-30 Series

Contents

Terms and illustrations in this Manual

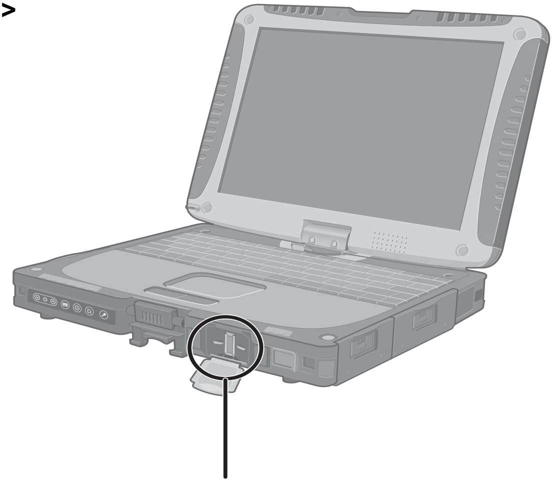
NOTE:	Useful and helpful information.
CAUTION:	Condition that may result in minor or moderate injury.
[start] - [Run]:	Click [start], and then click [Run]. You may need to double-click in some cases.
➔ :	Page in these Supplementary Instructions or in the Reference Manual for the computer.

- Some of the illustrations in this manual may differ slightly in shape from the actual items in order to make the explanation easier to understand.

Names and Functions of Parts

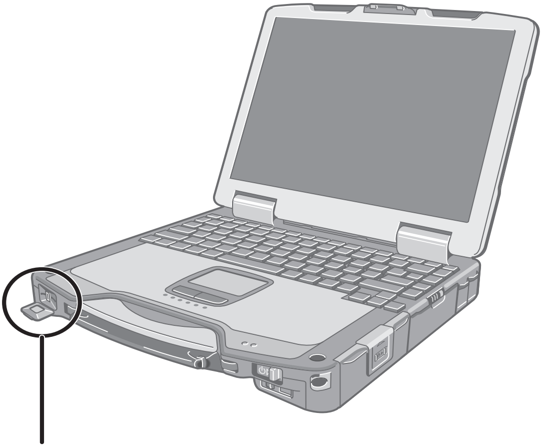
Except the following, refer to the Operating Instructions for the computer.

<CF-19 Series>



(Appearance may differ, depending on specifications.)

<CF-30 Series>

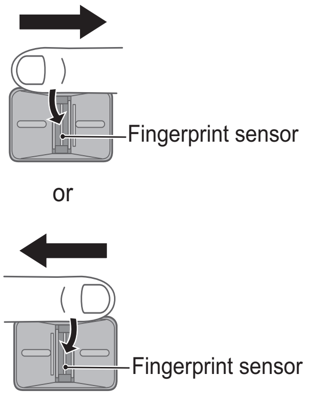


(Appearance may differ, depending on specifications.)

How to Use the Fingerprint Reader

This section explains how your fingerprints are enrolled and authenticated.

1 Slide your finger to the right or left.



- **To prevent a reading error.**

  ① Set the first joint of your finger on the sensor as illustrated to the right.

  ② Slide your finger to the right or left while keeping it in contact with the fingerprint sensor.

  ③ Slide your finger to the right or left until the sensor is visible.

- **When the fingerprint sensor does not enroll or authenticate your fingerprint properly:**

  · You slid your finger too fast or too slow.
  · Your finger was soiled or it has a scar on the surface.
  · Your finger was wet or extremely dry.
  · Your fingerprint does not have sufficient data for personal identification.

  For further information, refer to “Troubleshooting (For Devices)”. (➔ page 14)

CAUTION

- **To protect the fingerprint sensor, be sure to close the cover when not using the fingerprint reader.**
- **We shall not be liable for any loss or damage whatsoever resulting from your Fingerprint device or neglect of Fingerprint device use, or any data loss resulting from such developments as Fingerprint authentication device malfunctioning.**

Overview

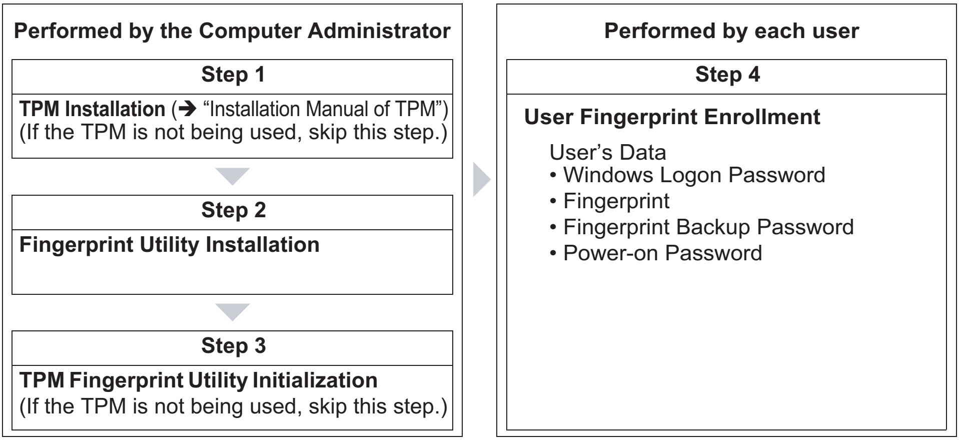
Fingerprint’s Outline

The conventional security systems use ID/passwords and token devices such as IC cards to authenticate users. Therefore the passwords and token devices are exposed to the risk of being lost, stolen and hacking.

The Fingerprint authentication method uses user’s fingerprints instead of passwords for security authentication. You can use your fingerprints to start up your computer and log on Windows.

We recommend you use the Fingerprint Reader in combination with the TPM (Trusted Platform Module) to increase the security level of your computer.

Recommended Installation Procedure



Performed by the Computer Administrator

Step 1

TPM Installation (➔ “Installation Manual of TPM”)
(If the TPM is not being used, skip this step.)

Step 2

Fingerprint Utility Installation

Step 3

TPM Fingerprint Utility Initialization
(If the TPM is not being used, skip this step.)

Performed by each user

Step 4

User Fingerprint Enrollment

User’s Data
- Windows Logon Password
- Fingerprint
- Fingerprint Backup Password
- Power-on Password

This manual describes Steps 2, 3 and the initial part of Step 4.

For further steps, refer to the UPEK Protector Suite QL Help menu. (Click [start] - [All Programs] - [Protector Suite QL] - [Help].)

Precautions

Security Functions

- Fingerprint Authentication Technology does not guarantee complete authentication and individual identification. Please acknowledge we shall not be liable for any loss or damage whatsoever resulting from the use of, or inability to use your Fingerprint device.
- The Fingerprint authentication method uses multiple fingerprints, encryption keys, credentials data and passwords. You might not be able to use your data if you lose fingerprints, keys, credentials and passwords, so keep them in a safe place. For further information, refer to “Backup”. (➔page 10)
- **General interaction with third-party applications: There is no guarantee that there will not be any negative interaction with any third-party software, and will not accept any responsibility for such an interaction.**

- **You cannot use this function at the same time as the SD security function is being used. When SD security is set, disable SD security function in the following order before initial setting of fingerprint authentication.**

① Log on to Windows as an Administrator.

② Click [start] - [All Programs] - [Panasonic] - [SD Card Setup].

③ Add a check mark for [Use the SD card when starting the computer].

④ Click [OK].

· Follow the on-screen instructions.

· SD security is disabled and all registered SD memory cards become unavailable when your computer starts up.

Installation

Step1 TPM Installation

Refer to on-screen manuals “Installation Manual Trusted Platform Module (TPM)”. (Click [start] - [Run], enter [C:\util\drivers\tpm\README.pdf], and click [OK].)

- ● If the TPM is not being used, skip this step.

Step2 Fingerprint Utility Installation

Performed by the Computer Administrator.

Preparation

[Only CF-19 series with Windows XP Tablet PC Edition]
Move Tablet PC Input Panel from upper right to the bottom right or bottom left .

- ● If this procedure is skipped, the “Please swipe you finger” message may overlap the Tablet PC Input Panel.

1 Log on to Windows as an Administrator.

2 Close all other programs.

3 Click [start] - [Run], enter [C:\util\drivers\fngprint\psql\setup.exe], and click [OK].

The “Protector Suite QL ∗.∗ Setup” screen appears.

4 Click [Next].

Installation starts. Carefully read the License Agreement, select “I accept the license agreement”, and click [Next]. Follow the on-screen instructions.

5 When the “Protector Suite ∗.∗ has been successfully installed.” message appears, click [Finish] - [OK].

The computer restarts.

6 Log on to Windows as an Administrator.

The “Protector Suite QL Icon” appears in the notification area.

Step 3 TPM Fingerprint Utility Initialization

Performed by the Computer Administrator.

The “Invalid TPM status” message is displayed by the “Protector Suite QL Icon” in the notification area.

- ● If the TPM is not being used, skip this step.

1 Click on the “Invalid TPM status” message to start “Advanced Security Initialization Wizard”.

Follow the on-screen instructions.

NOTE

If the “Invalid TPM status” message is not displayed, click [start] - [All Programs] - [Protector Suite QL] - [Control Center] - [Settings] - [System Settings] - [TPM] - [Initialized TPM].

Step 4 User Fingerprint Enrollment

Performed by each user.

1 Click [start] - [All Programs] - [Protector Suite QL] - [User Enrollment].

The “Welcome” message appears, read the description carefully.

2 Click [Next].

3 Select an enrollment mode, and click [Finish].

● **Enrollment mode**

You can make the configuration for the enrollment only once during this initialization phase.

· **Enrollment to the biometric device**

All enrolled fingerprints are stored directly in the fingerprint sensor. The user data will be secured by the hardware protection keys obtained by the fingerprint sensor. This mode allows up to 21 fingerprints to be enrolled.

· **Enrollment to the hard disk**

All enrolled fingerprints are stored on the hard disk. Hardware protection of the user data is not possible, but multiple users can enroll their fingerprints.

● When the “Finish” screen appears, read the description carefully.

● “User Enrollment” wizard starts. Follow the on-screen instructions.

NOTE

Enroll at least two fingers. Even if one of them is injured, you can use another one to access your account and secret data. For further information about the enrollment, refer to “How to Use the Fingerprint Reader” (➔page 3) and “Fingerprint Tutorial”. (Click [start] - [All Programs] - [Protector Suite QL] - [Fingerprint Tutorial].)

Installation

- **We recommend you use the Power-on Security feature. This feature prevents unauthorized access to the user's computer at the BIOS level.**

  After first finger enrollment, "Power-on Security" message appears. Select [Yes].

  ① When the "Power-on Security" screen appears, click [Manage Passwords...].

  ② Select [Power-On] in [Password Types], and click [Set password...].

  ③ Enter the password for "Power-on Security", and click [OK].

  ④ Click [Close].

  ⑤ Add a check mark for [Power-On] in [Password Types].

  ⑥ Enter the password (step ③), and click [OK].

  ⑦ Click [Next].

  · Follow the on-screen instructions.

NOTE

The number of fingerprints for "Power-on Security" is maximum of 21, because they are stored in the fingerprint sensor regardless of the selected enrollment mode.

More Advanced Security

You can increase your computer's security level by setting the BIOS level described in this section.
Performed by the Computer Administrator.

1 Register the Supervisor Password.

You have to register the Supervisor Password to proceed to the next step.
If you have already registered the Supervisor Password, you can skip this step, and move on to step **2**.
If you have not done this, have enrolled your fingerprint using Protector Suite QL, and have already made Power-on Security effective, after step ②, your fingerprint authentication will be necessary.

① Turn on or restart the computer.

② Press **F2** several times while [Panasonic] boot screen is displayed soon after the computer starts the startup procedure.

③ Select the [Security] menu.

④ Select [Set Supervisor Password], and press **Enter** .

⑤ Enter your password in the [Enter New Password], and press **Enter** .
· The password will not be displayed on the screen.

· You can use up to 32 alphanumeric characters (including spaces).

· The case (upper/lower) is ignored.

· To input numbers for the password, use the numbered keys on the keyboard.

· You cannot use **Shift** and **Ctrl** to input a password.

⑥ Enter your password again in [Confirm New Password], and press **Enter** .

⑦ In [Setup Notice], press **Enter** .

2 Set the High Security Level.

① Select [Fingerprint Security Sub-Menu], and press **Enter** .

② Select [Security mode:], and select [High].

· Default setting: Simple

③ Press **ESC** to close the sub-menu.

④ Press **F10** , select [Yes], and press **Enter** to exit the Setup Utility.

NOTE

- In the "High" security mode, you have to enter the Supervisor or User Password even after fingerprint authentication.
In the "Simple" security mode, you do not have to enter the Supervisor or User password after fingerprint authentication.

Useful Information

Backup

The file described below is necessary for recovering the Fingerprint authentication data. Back up this file periodically in a safe location such as removable disk to avoid data loss resulting from some accidents. We recommend you to store the file in a removable disk or network drive because the benefit of Fingerprint authentication security can be reduced if you keep the file in the internal hard disk drive.
The backup password described below is necessary for bypassing the Fingerprint authentication. We recommend you set the backup password using the "User Enrollment" wizard. If you do not define the backup password, you may lose your data in case of authentication hardware failure.

● **File used by each user**

· **Backup user passport data**

(Default name: <UserAccount>.vtp)
You need this file when you replace the embedded fingerprint chip, or the hard disk drive, or when reinstalling Windows.
This file contains the fingerprints, encryption keys, and logon authentication data.

NOTE

How to Backup:
Select "Export" in "Import or Export User Data" to save the user data. (Click [start] - [All Programs] - [Protector Suite QL] - [Control Center] - [Fingerprints])
For further information, refer to the UPEK Protector Suite QL Help menu. (Click [start] - [All Programs] - [Protector Suite QL] - [Help])

● **Password used by each user**

· **Backup Password for Enrollment**

This backup password can be used in case of hardware failure to bypass the fingerprint authentication.

CAUTION

- The passwords other than those explained above are also used for security, so do not lose them. For further information, refer to the UPEK Protector Suite QL Help menu (Click [start] - [All Programs] - [Protector Suite QL] - [Help]).

Limitations in Use

- My Safe*1: Antivirus software should be configured to ignore the “My Safe” data file (C:\Documents and Settings\(user account)\Application Data\Protector Suite\My Safe.fdp). Otherwise the user may experience problems when unlocking “My Safe”. “My Safe” data file cannot be backed up by using File back up function in Recover Pro. To back up “My Safe” data file, use Quick Backup/Complete Backup functions in Recover Pro and back up each data.
- **Password Bank*1 limitations: The following web pages cannot be supported.** Web pages which are created by the following technologies:
  - Web forms created on the fly using javascript.
  - Web forms which looks as one form (e.g. login field, password field), but internally created with two independent forms.
  - There can be auto submit problems with web forms which do not have Submit button. All forms that you cannot submit with **Enter** will be entered by Password Bank, but not submitted.
- **Password Bank*1 limitations: The following Windows applications cannot be supported.**
  - Applications which do not use standard Windows controls and draw controls by their own.
  - This includes any Java based application.

*1 For information of these functions, refer to the UPEK Protector Suite QL Help menu (Click [start] - [All Programs] - [Protector Suite QL] - [Help]).

Handling & Maintenance

- **The enrolling and authentication sensitivity may decline under the conditions below. Wipe off stains or moisture on the sensor surface with a soft cloth.**
  - The surface of the fingerprint sensor is soiled with dust, skin oil, or sweat.
  - The surface of the fingerprint sensor is wet as a result of moisture or condensation.
- **Static electricity may also cause the sensor to malfunction. To make your finger static-free, touch a metal surface before placing it on the fingerprint sensor. Exercise caution against static electricity in winter and other dry conditions.**
- **Malfunction or damage may occur when:**
  - The fingerprint sensor surface was damaged by the strong rubbing of a solid material, scratches, or being pecked with a pointed item.
  - The sensor was touched with a finger soiled with mud, damaging the sensor surface with a tiny substance, and staining the surface.
  - The sensor surface was covered with a seal, or soiled with ink.

Useful Information

Deleting (Initializing) Owner’s Data

When you dispose of the computer or transfer the ownership, delete (initialize) the owner’s data to avoid unauthorized access.

NOTE

The data enrolled in the fingerprint sensor is not image data. You cannot restore fingerprint image data from the data enrolled in the fingerprint sensor.

1 Disable Power-on Security

Performed by the Computer Administrator.

① Click [start] - [All Programs] - [Protector Suite QL] - [Control Center].

· The “Fingerprint Software Management” screen appears.

② Click [Settings], and click [Power-on Security].

③ Remove the check mark from [Replace the power-on and hard drive passwords with the fingerprint reader.], and click [OK].

④ Click [Fingerprints], and click [Enroll or Edit Fingerprints].

· “User Enrollment” wizard starts. Follow the on-screen instructions.

⑤ When the “User’s Fingers” screen appears, click [Next] without deleting fingerprint samples.

⑥ Click [Manage Passwords...].

⑦ Select [Power-On] in [Password Types], and click [Unset password...].

⑧ Enter the password for Power-on Security, and click [OK].

⑨ Click [Close].

· Confirm that there is no item in [Password Types].

⑩ Click [Next].

· At the confirmation message, click [Yes].

⑪ Click [Next].

⑫ Click [Finish].

· Follow the on-screen instructions.

2 Delete Fingerprint Data

Performed by each user.

① Click [Fingerprints], and click [Delete]. The “Swipe finger” screen will appear.

② Swipe user’s finger.

· If the authentication is successfully completed, the confirmation message appears.

③ Click [Yes].

· Confirm that all users’ data was deleted.

NOTE

If the enrollment mode is set to “Enrollment to the hard disk” (➔page 7), you need to remove the fingerprints data after Step ***2***.
Performed by the Computer Administrator.

① Click [start]-[All Programs]-[Protector Suite QL]-[Control Center].

② Click [Settings], and click [Power-on Security].

③ Select the fingerprint, and click [Remove].

· Surely remove all of the fingerprints.

3 Uninstall Protector Suite

Performed by the Computer Administrator.

① Log on to Windows as an Administrator.

② Close all programs.

③ Click [start] - [Control Panel] - [Add or Remove Programs].

④ Click [Protector Suite ∗.∗], and click [Change].

⑤ Select [Remove], and click [Next].

⑥ Select [Remove all Protector Suite data], and click [Next].

· Uninstallation starts. Follow the on-screen instructions.

⑦ When the “Protector Suite ∗.∗ has been successfully uninstalled.” message appears, click [Finish].

· The computer restarts.

Troubleshooting

When a problem occurs, refer to this page. If you still cannot troubleshoot the problem, contact PANASONIC TECHNICAL SUPPORT.

For Devices

The sensor does not enroll or authenticate my fingerprint.	● Slide your finger correctly. (For further information about enrollment and authentication, refer to "How to Use the Fingerprint Reader" (➔page 3) and "Fingerprint Tutorial". (Click [start] - [All Programs] - [Protector Suite QL] - [Fingerprint Tutorial]) ● The sensor enrolls or authenticates no fingerprint, or performs authentication poorly, despite the correct way of finger sliding when your finger is in any of the conditions stated below: · Rough skin, or injured finger (with a cut or a skin inflammation) · Extremely dry · Soiled with mud or oil · Fingerprint has been worn and has faded · Wet with water or sweat <You can improve enrolling and authentication sensitivity by taking the following steps when any of the conditions described above exists> · Wash your hands or wipe them dry. · Use a different finger for registration or authentication. · Treat your finger with a hand cream when it is rough skin or dry. ● Clean the fingerprint sensor. (For further information, refer to "Handling & Maintenance" (➔page 11)) ● The fingerprint sensor may be malfunctioning when it continues to perform poorly after the steps described above have been performed. Contact PANASONIC TECHNICAL SUPPORT.

(Enrollment and authentication is unavailable to an extremely minority of people including those whose fingerprints give little data for personal identification.)

For Application

Sensor does not work.	● **Exported passport can help you if you need to replace the sensor.** · Log on to Windows as an Administrator. You can always access the computer by using your Windows log on password. In convenient mode, any user can access the computer by using your Windows log on password. · To access “My Safe” “My Safe” can be always accessed by using the “My Safe” backup password. · Other functions Replace/Repair the sensor, then follow the instructions in section “Replacing sensor”. Some limited functions (e.g. deleting passport) is available without a functional sensor. In case of deleted operation, it is necessary to cancel the fingerprint verification operation to get to the password dialog.
User cannot use enrolled finger. (e.g. injury)	● **It is strongly recommended to enroll at least two fingers to avoid this problem.** If you enrolled multiple fingers, simply use other finger. If you only enrolled one finger that can be used, we recommend to use the “Enroll or Edit Fingerprints” wizard and enroll additional fingerprints. If none of your enrolled fingers can be used, follow this procedure: ① Log on to Windows as an Administrator. You can always access the computer by using your Windows log on password. In convenient mode, any user can access the computer by using your Windows log on password. ② Update the enrolled fingerprints. To be able to fully use Protector Suite QL, you need to have usable enrolled fingerprints. Enter the “Enroll or Edit Fingerprints” wizard.

User cannot use enrolled finger. (e.g. injury) (continued)	· If you do not use "Advanced Security", you can still enter using the Windows password. · If you use "Advanced Security" with backup password, you can enter using the backup password. · If you use "Advanced Security" without backup password, there is no other way to add a different fingerprint. In this case we recommend either to wait until your finger is usable again (e.g. the injury heals), or to delete the passport (Use "Delete" wizard) and then reenroll new fingerprints. Please note that in the latter case all your stored secret data (passwords, "My Safe" encryption keys) will be lost. To perform the delete operation it is necessary to cancel the fingerprint verification operation to get to the password dialog, then enter your Windows log on password. · **To access "My Safe"** If you did not perform the procedure in step ② or it did not work, you can still access "My Safe" by using the "My Safe" backup password.
TPM failure.	● If you use "Advanced Security" with TPM (Trusted Platform Module) and TPM is broken, erased or disabled, the "Advanced Security" will not work anymore. If you do not use the "Advanced Security" backup password, follow the instructions "Starting Over". Otherwise, if you use "Advanced Security" backup password, you can follow these steps: ① Enter the "Enroll or Edit Fingerprints" wizard using the backup password. ② Disable "Advanced Security" and finish. ③ After the TPM is repaired and enabled (or if you only erased its contents) you can enter the "Enroll or Edit Fingerprints" wizard again using your finger and enable the "Advanced Security" with TPM again.

Replacing sensor.	● If you need to replace a non-functioning fingerprint reader, follow this procedure: **Enrollment to the hard disk:** If enrollment to hard disk is used, “Protector Suite QL” has not stored any data on the device and therefore has no problem to continue after you replaced the sensor. However, in case 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:** If the fingerprint have been enrolled to the device, a new passport will be required. Follow the procedure in the section “Starting Over”.
Lost Advanced Security backup password.	● To change the “Advanced Security” backup password, go to the “Enroll or Edit Fingerprints” wizard and swipe your finger and go through the Fingerprint enrollment. On the Advanced Security page you can change the backup password.
Protector Suite QL reinstallation.	● During Protector Suite QL uninstallation, you can select whether to delete the Protector Suite Data - including passports. ● If you want to reinstall the product, select button to leave the Protector Suite QL data on the computer. After the new installation, you will be able to use your data again. ● If the Protector Suite QL was uninstalled including the passports, then in case of enrollment to device the fingerprints will still be stored in the device and the user can use them reenrollment.
Lost “My Safe” backup password.	● “My Safe” backup password cannot be changed directly. It is necessary to create a new “My Safe”. You have to: ① Unlock “My Safe”. ② Copy the data from “My Safe” to some other folder. ③ Delete “My Safe” from “My Safe” settings. ④ Create a new “My Safe” and define the new “My Safe” backup password.

Troubleshooting

Accessing "My Safe" after Protector Suite QL uninstallation.	● "My Safe" data can be accessed only using Protector Suite QL. If you accidentally uninstalled Protector Suite QL, you have to reinstall it. If passport data was not removed during uninstallation, everything will work automatically including "My Safe". If the passport data was removed during uninstallation the "My Safe" will recognize that the installation was changed and will offer to use the backup password, instead.
Accessing "My Safe" after computer crash.	● If you have an exported passport, import it now so you can access "My Safe" directly using fingerprints. Otherwise you can access "My Safe" using the "My Safe" backup password: "My Safe" will recognize that the installation was changed and will offer to use the backup password, instead.
"My Safe" data file cannot be backed up using Recover Pro.	● "My Safe" data file cannot be backed up by using File back up function in Recover Pro. To back up "My Safe" data file, use Quick Backup/Complete Backup functions in Recover Pro and back up each data.
Removing data from the reader.	● When enrollment to the device is used, passport data is stored to the device. To remove it, go to the "Delete" passport wizard and delete existing passports, and then use the "Fingerprint Inspector" to remove remaining fingerprints (e.g. left over from previous installations). ● In convenient mode, the "Fingerprint Inspector" does not allow deleting the last fingerprint for an existing passport and only user's own fingerprints can be deleted. Therefore it is necessary to delete passports first.
[Only CF-19 series with Windows XP Tablet PC Edition] **Tablet PC Input Panel is hidden under "Please wipe your finger " message.**	● Move Tablet PC Input Panel according to the following order. ①Log on to Windows. ②Click [start] - [All Programs] - [Protector Suite QL] - [Control Center] - [Settings] - [System Settings]. ③Remove a check mark for [Enable logon support], and click [OK]. ④Log off Windows. ⑤Move Tablet PC Input Panel to the bottom right or bottom left. ⑥Log on to Windows. ⑦Click [start] - [All Programs] - [Protector Suite QL] - [Control Center] - [Settings] - [System Settings]. ⑧Add a check mark for [Enable logon support], and click [OK].

Starting Over

If the specific solutions for your problem does not work, you can use these instructions as the last measure and start over. However, please note that you can lose your data - passwords, secret keys and fingerprints.

① Log on to Windows as an Administrator.

- You can always access the computer by using your Windows log on password. In convenient mode, any user can access the computer by using the Windows log on password.

② Try to export your passport to a file if you are planning to use your passwords, secret keys or enrolled fingers in the future.

- If you exported your passport recently, this step is not required.
- If biometrics authorization works and your finger is recognized, use “Import or Export User Data” wizard, swipe your finger and continue according to wizard’s instructions.
- If biometrics authorization works, but your finger is not recognized, you can start the “Import or Export User Data” wizard and export the passport even without using your fingerprint. You need to cancel fingerprint dialog, and you will be prompted for a password. If you do not use “Advanced Security”, enter your Windows log on password. Otherwise, enter your “Advanced Security” backup password.

CAUTION

If you used “Advanced Security” without a backup password, there is no way to backup your data.

● If biometrics authorization does not work, there is no way to backup your data.

③ Deleting the passport.

- Use the “Delete” wizard. Please note that all your stored secret data (passwords, “My Safe” encryption keys) will be lost. If you backed up the data, you can restore it in the next step; otherwise it will be lost permanently. To perform the delete operation it is necessary to cancel the fingerprint verification operation to get to the password dialog, then enter your Windows log on password or backup password.

④ Make sure your fingerprint sensor is working.

- Use the Tutorial wizard to verify that the fingerprint sensor works. If not, reboot and try again. If it still does not work, please contact PANASONIC TECHNICAL SUPPORT.

⑤ Restore or create passport.

- If you have a backup of your data, you can now use “Import or Export User Data” wizard to restore your data. Otherwise you can create a new passport by using the “Enroll or Edit Fingerprints” wizard.

Specifications

Array Size	248 x 4 pixels
Image Size	248 x 360 pixels
Image Resolution	508 DPI

Matsushita Electric Industrial Co., Ltd.

Web Site : http://panasonic.net

Printed in Japan

HS1206-0
DFQX5628ZA