NITGEN
biometric solutions

Driver Installation

for Fingerprint Sensors

NITGEN
biometric solutions

To Contact Us

Tel. 82-2-3415-1800

Fax. 82-2-3415-1601

Email: customer@nitgen.com

URL: http://www.nitgen.com

Contents

Contents

Chapter 1

Before You Begin

Features

The NITGEN FRD (Fingerprint Recognition Device) is a world-class fingerprint device that uses state-of-the-art technology, to facilitate biometric authentication of a user's fingerprint using a combination of quality hardware and software that is convenient and easy to use.

The FRD is equipped with high-performance and compact NITGEN fingerprint recognition module, which can transfer data to computers to reject any unauthorized user's access.

NITGEN FRD will provide the most reliable authentication by identifying fingerprints with exactness through its high-resolution fingerprint recognition technology that can be used to replace existing password-based security systems. NITGEN FRD is the security device for the next generation, where the security of personal data as well as corporate data is indispensable.

Typical Applications

Some typical applications for fingerprint authentication technology are as follows:

- Information Technology and Computer Network Security
- Internet Business
- Security for Banking and Financial System
- Medical Information Systems
- Further Security Field using Passwords

System Requirements

System requirements for FRD are as follows;

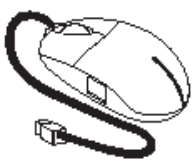
⊙ **USB Type**

- CD-ROM drive
- USB 1.1/2.0 port (If you are connecting the FRD Fingkey Mouse into a hub, you must use a self powered USB hub.)
- 16MB RAM
- 20MB available hard disk space
- MS Windows 98(Second Edition or later version)/ME/2000/XP/2003

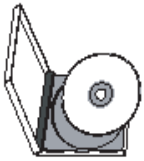
Package Contents

FRD Kits include the following; Please check the contents of your package.

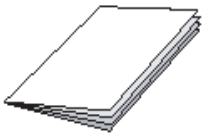
1. USB Type Fingerprint Recognition Fingkey Mouse (MFDU01)



MFDU01



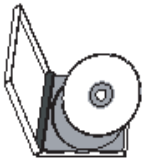
Installation CD



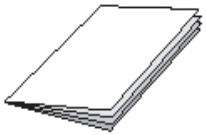
Installation Guide

2. USB Type Fingerprint Recognition Fingkey Hamster (HFDU01)

HFDU01



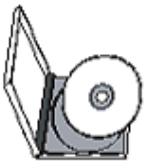
Installation CD



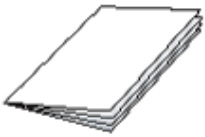
Installation Guide

3. USB Type Fingerprint Recognition Fingkey Hamster II (HFDU11)

HFDU11



Installation CD



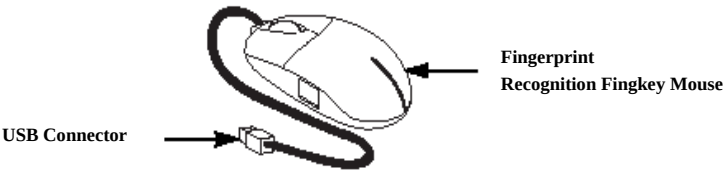
Installation Guide

Product Types

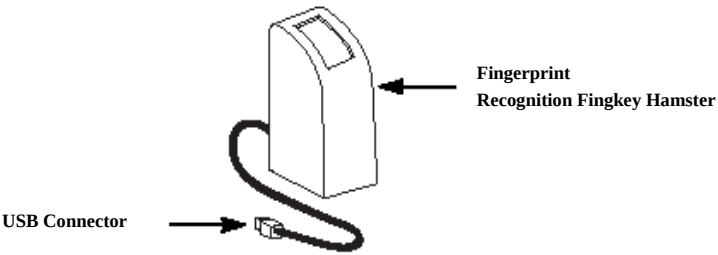
It is important to know the type of FRD you are installing prior to beginning the installation process in order to ensure that the device is configured correctly on your system. If you are not certain, please refer to the diagrams below or locate the model number on the bottom of the fingerprint device.

After you have identified the type of FRD that you are installing, follow the installation guide to install the drivers and use the FRD.

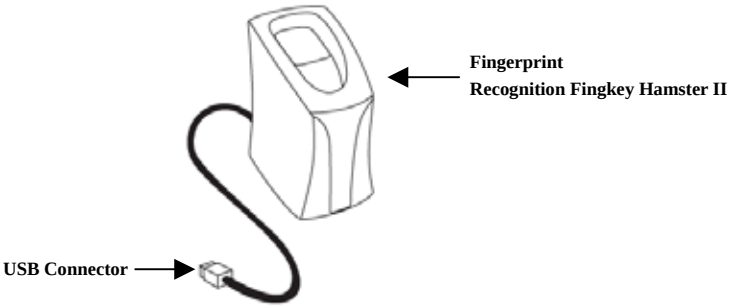
1. USB Type Fingerprint Recognition Fingkey Mouse (MFDU01)



2. USB Type Fingerprint Recognition Fingkey Hamster (HFDU01)



3. USB Type Fingerprint Recognition Fingkey Hamster II (HFDU11)



Chapter 2

Driver Installation

USB Driver Installation

USB Driver Installation

If you are installing the USB Fingkey Mouse in the Windows 98 environment, the Windows 98 Installation CD will be required if there are no Human Interface Device (HID) drivers installed on your system.

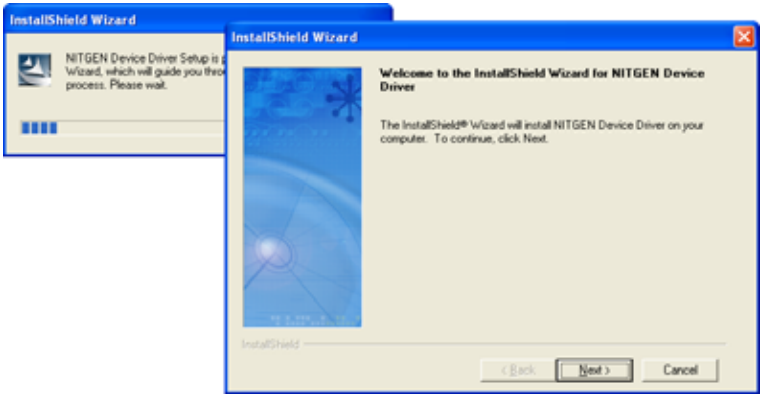
1. Prior to beginning the installation, please close all applications that are running.

2. Do not plug in the USB FRD until after the drivers have been installed on your system.

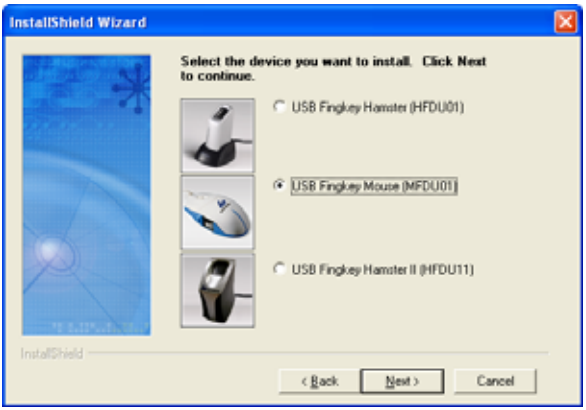
3. Insert the Installation CD in your CD-ROM drive. The installation program will start automatically. Click 'USB Driver' to continue.

The USB FRD Fingkey Mouse will be enabled after the driver is installed, so it may be necessary to install the driver using a PS/2 mouse or the <Tab> key on the keyboard.

4. Follow the instructions presented by the InstallShield Wizard during the driver installation process..



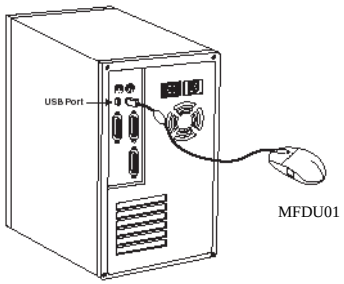
5. Select the device you are using and click “Next”.



These examples in this guide are based on selection of the USB Fingkey Mouse (MFDU01) as an example.

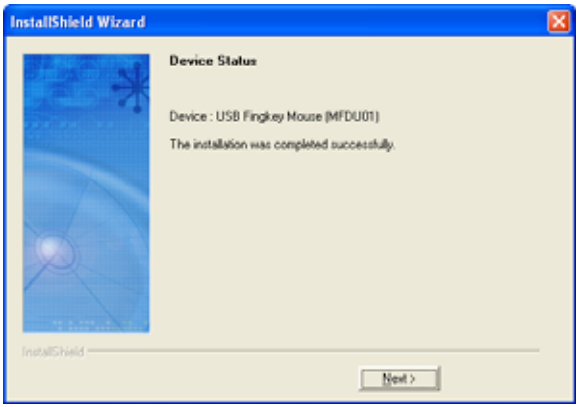
6. When driver installation is completed, it is necessary to check the device status to ensure that it was installed correctly. You will be prompted to connect the USB FRD as shown in the diagram below:

7. Connect the FRD to the USB port, and wait a moment. You can also click “Plug in later” to install it at a later time.

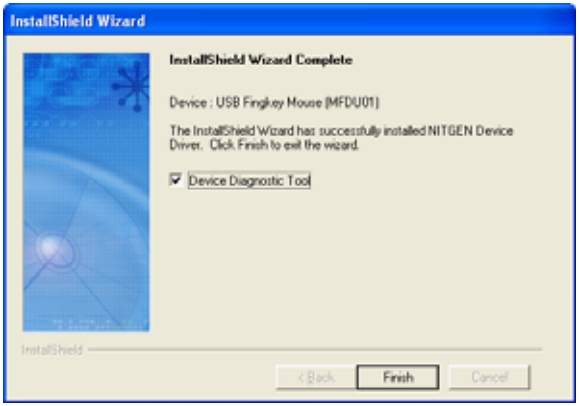


8. The New Hardware Installation Wizard will automatically show you the process of installing USB Composite, HID and FRD drivers. If you are installing a USB Fingkey Hamster, only the FRD driver will be installed.

9. When the device installation process is completed, a window will be displayed indicating that “the device is successfully installed.” Click the “Next” button.



10. Check the ‘Device Diagnostic Tool’ check box and click “Finish”. At this time the installation process will be completed, and the hardware test utility will be run automatically.



Refer to Chapter 3 ‘How to use the Device Diagnostic Tool’ for more information on using device diagnostic tool to ensure that the FRD is successfully installed.

Chapter 3

How To Use The Device Diagnostic Tool

Running the Diagnostic Tool

Device

Enroll

Verify

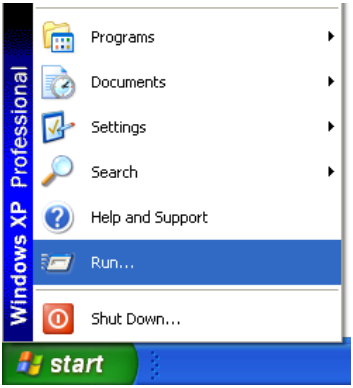
Fingerprint Quality Check

General

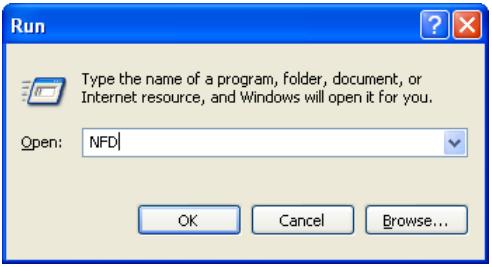
About

Running the Diagnostic Tool

1. Click Start-Run to run the testing program.



2. Type ‘NFD’ and click “OK”.



Device

1. Select a device you wish to use and then initialize.

2. Click “Device Scan” to display the list of all devices in the system.

3. Choose a certain device from the list and click “Init” to initialize the device, which makes it possible to capture or use other functionalities of the tab. Without initialization, other functionalities of the tab cannot be used.
4. Click “Init” to output device information.

5. Click “Save” or right-click on the image to save the fingerprint image as BMP. If the fingerprint is not input, the image will not be saved.

6. There are options in capturing fingerprints. If the fingerprint is dry or wet, resulting in poor image quality, the fingerprint cannot be input properly. In this case, uncheck the “Latent Fingerprint Check” and then capture the image to view the fingerprint image.

USB Device:

At present, devices that can be supported are USB-typed HFDU01, MFDU01 and HFDU11. Click “Device Scan” with a driver installed to display types of USB devices that are connected to the system.

Enroll

1. Enroll users using eNBSP SDK, based on the device selected from the Device tab. Enrolled fingerprint information is used to authenticate fingerprints in the Verify tab.

2. Click “Enroll” to display the UI for fingerprint enrollment. Select a fingerprint to register and click “finish”.

3. If the fingerprint is successfully input, the user ID is registered and “SUCCESS” is displayed.

4. A user ID automatically increments from 1000. A fingerprint ID is automatically selected from 1 to 10, each corresponding to from the thumb of the right hand to the little finger of the left hand in an orderly manner. A user ID can be changed within the range of 1000~9999. If a user ID and a fingerprint ID are identical, a message “Do you want to update it?” will be pop up.

5. Click “Delete FP” to remove the selected fingerprint information from the list. Click “Delete All” to delete all information in the list.

Verify

1. User information input from the Enroll tab is displayed on the list. Using this user information, verification is performed. There are two types of authentication: Verification(1:1) and Identification(1:N).

2. Select “Identification” and then click “Match” to perform verification. If there is a fingerprint that matches, related information is displayed.

3. Or select a user ID and a fingerprint ID to attempt verification. Choose “1000-6” as a fingerprint but use the fingerprint input as “1001-7”. Then attempt to match both. The system displays the result by comparing the two.

4. Matching Score is output when authentication attempted. It is a result of matching an input fingerprint with existing fingerprint data. The score range is 0 ~ 9. The score is compared with the security level value of the General tab, determining success or failure. If the security level is 5 and the matching score is lower than 5, verification fails. If the score is higher than 5, on the other hand, verification is passed. If a fingerprint input is too dry or to wet or it is not properly input, the score can turn out to be low.

Fingerprint Quality Check

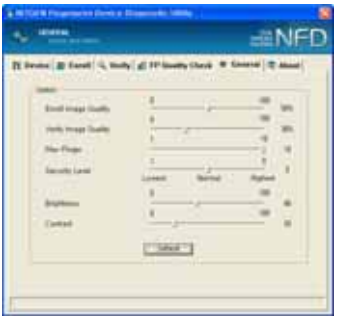
1. You can check the status of fingerprints before enrolling fingerprints or attempting verification.

2. Input the same fingerprint twice. The picture on the left is an example of an image of an improperly input fingerprint.

3. This is an image of a properly input fingerprint. Make sure to input the core of a fingerprint.

4. It is recommended that a minimum value required to enroll a fingerprint be bigger than 3. It can be less than 2 but it can bring about low verification ratio. The same fingerprint with different positions on the sensor can change values because fingerprint features are located differently.

General



1. Option values used in eNBSP SDK are set up. The values are applied to other tabs. If “Init” is not selected on the Device tab, Brightness and Contrast are set at “0”, which cannot be changed.

2. The pictures left shows images of a fingerprint with two different Brightness values. If a fingerprint is too dry or too wet, change Brightness and Contrast to get an optimal image.

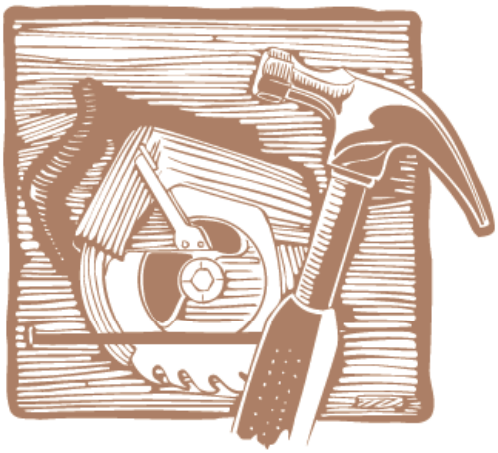
3. The maximum number of fingerprint that can be input is 10 as a default. If it is changed to “1”, only one fingerprint is allowed to be registered from the Enroll tab. The Security Level is important, determining success or failure of verification on the Verify tab.

   Click “Default” to initialize.

About

1. It contains NFD version and copyright. Click the image to go to the NITGEN homepage. (http://www.nitgen.com)

Chapter 4
Troubleshooting



USB FRD Problems

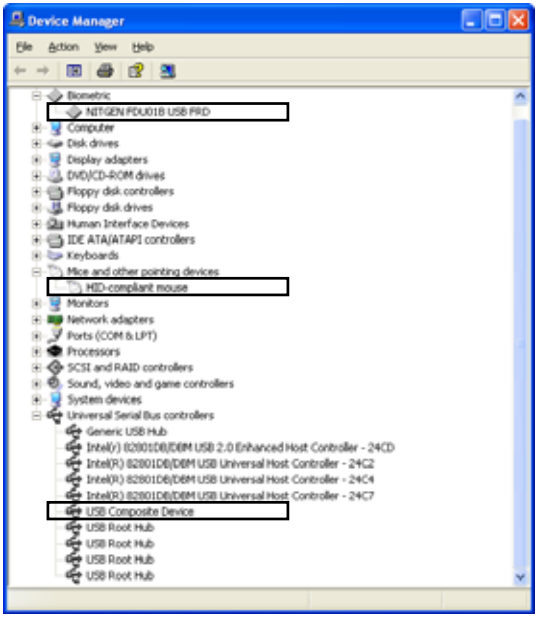
Driver Installation without Installshield wizard

USB FRD Problems

<When the USB FRD doesn't work >

1. Verify that the USB connector of FRD is connected to the USB port correctly.

2. Click **Start-Setting-Control Panel-System** icon and select the '**Device Manager**' tab to verify that the Fingkey Mouse driver is installed correctly. If it is not installed correctly as shown below, repeat the installation process and be sure to select the USB Fingkey Mouse.



3. If you are using the FRD connected to a USB port in a USB keyboard or Hub, verify that the USB keyboard or Hub has it's own power-supply. The USB FRD uses almost 110mA of electric power, so it should only be connected to hubs that are self-powered.

<When you use the FRD with any other high-speed USB devices>

1. When the FRD is connected on your computer together with any other high-speed USB devices such as USB Camera or USB Scanner etc., it cannot be used at the same time as these devices. Close the programs that are using these devices before using the FRD.

2. Because the FRD is a high-speed USB device and uses almost 66% of your system USB limit, the USB device will not function concurrently with any other device using more than 40% of the USB bandwidth.

3. Fingkey Hamster II adopts a bulk type, enabling the user to use other USB devices simultaneously. This, however, can degrade the quality of fingerprint images.

<When any other mouse driver is installed on your computer>

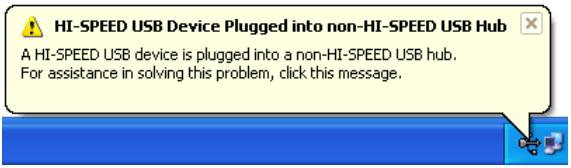
1. When the Logitech mouse driver is installed on your computer, FRD Fingkey Mouse performance is very slow.

2. Click **Start-Setting-Control Panel-Mouse** icon and "Motion" **tab** to adjust the speed of mouse pointer.

3. If you cannot adjust the speed of mouse pointer, remove the existing Logitech mouse driver to use FRD.

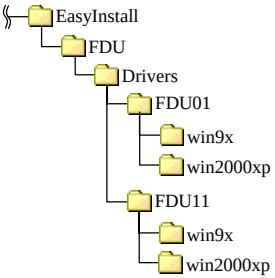
<When be connected to the USB 1.1>

1. Performance of Fingkey Hamster II is maximized in USB2.0. There should be no problem with connecting to the USB1.1 port but this can display the message below.



Driver Installation without Installshield wizard

1. There are device models below \EasyInstall\FDU\Drivers. Select a model and then an O/S folder for the system. Use the inf file below the O/S folder. The folder contains files required to install device models. In the FDU01 folder, fdu01.cat, Venus.dll and VenusDrv.sys exist, while fdu11.cat, NGStar.dll and NGStar.sys exist in the FDU11 folder. In the Win9x series, *.cat file do not exist. Below is the folder structure of EasyInstallation:



The path of EasyInstallation may change. So check the location before installation. The FDU01 folder contains Fingkey Mouse and the Fingkey Hamster driver, while the FDU11 folder has the Fingkey Hamster II driver in it.

FCC Certification

THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES.
OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS:
(1) THIS DEVICES MAY NOT CAUSE HARMFUL INTERFERENCE, AND
(2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE, RECEIVED, INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION.

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

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

NOTE: THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.