SecuGen® USB Fingerprint Reader User Guide

Installation, Usage, Diagnostic Tools and Troubleshooting

SG1-0007B-015 (01/13)

Contents

Consumer Notices

FCC NOTICE

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: (1) Reorient or relocate the receiving antenna; (2) Increase the separation between the equipment and receiver; (3) Connect the equipment into an outlet on a circuit different from that to which the receiver is connected; or (4) Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance to Part 15 of the FCC Rules could void the user's authority to operate the equipment.

CE NOTICE

This equipment has been tested and found to comply with the limits for a Class B or Class 2 digital device, pursuant to EN 55022 Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at the expense of the user.

Changes or modifications not expressly approved by the party responsible for compliance to EN 55022 Rules could void the user's authority to operate the equipment.

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences due Réglement sur le matériel brouilleur du Canada.

Before You Begin

Biometrics Overview

Biometrics is an automated method of recognizing a person based on physical or behavioral characteristics. Biometric information that can be used to accurately identify people includes fingerprint, voice, face, iris, handwriting, and hand geometry.

There are two key functions offered by a biometric system. One method is **identification**, a “one-to-many” matching process in which a biometric sample is compared sequentially to a set of stored samples to determine the closest match. The other is **verification**, a “one-to-one” matching process in which the biometric system checks previously enrolled data for a specific user to verify whether that individual is who he or she claims to be. The verification method provides the best combination of speed and security, especially where multiple users are concerned, and requires a user ID or other identifier for direct matching.

With an increasing reliance on online technology and other shared resources, the information age is quickly revolutionizing the way transactions are initiated and completed. Business transactions of all types are increasingly being handled online and remotely. This unprecedented growth in electronic transactions has underlined the need for a faster, more secure, and more convenient method of user verification than passwords can provide.

Using biometric identifiers offers several advantages over traditional and current methods. This is because only biometric authentication is based on the identification of an intrinsic part of a human being. Tokens such as smart cards, magnetic stripe cards, and physical keys, can be lost, stolen, duplicated, or left behind; passwords can be forgotten, shared, hacked or unintentionally observed by a third party. By eliminating all of these potential trouble spots, only biometric technology can provide the security and convenience needed for today’s complex electronic landscape.

Advantages of Using Fingerprints

The advantages of using fingerprints include widespread public acceptance, convenience, and reliability. It takes little time and effort to acquire one’s fingerprint with a fingerprint identification device, and so fingerprint recognition is considered among the least intrusive of all biometric verification techniques. Ancient officials used thumbprints to seal documents thousands of years ago, and law enforcement agencies have been using fingerprint identification since the late 1800s. Fingerprints have been used so extensively and for so long, there is a great accumulation of scientific data supporting the idea that no two fingerprints are alike.

About SecuGen

SecuGen (www.secugen.com) provides biometric solutions for physical and network security employing advanced fingerprint recognition technology. The company’s comprehensive product line includes quality optical fingerprint sensors and peripherals, software, and development kits used for a variety of innovative applications including Internet, enterprise network and desktop security, physical access control, time and attendance management, and financial and medical records control. SecuGen patented products feature the industry’s best warranty and are renowned for their accuracy, reliability and versatility. Based in Silicon Valley, SecuGen has been serving the biometric community since 1998 and is an active member of the Biometrics Consortium (www.biometrics.org), the BioAPI Consortium (www.bioapi.org), and the International Biometrics & Identification Association (IBIA) (www.ibia.org).

About SecuGen Products

SecuGen Sensor Qualities

- **Excellent Image Quality:** Clear, distortion-free fingerprint images are generated using advanced, patent-pending optical methods. Quality imaging yields better sampling for minutiae data extraction.
- **Durability:** Mechanical strength tests show resistance to impact, shock and scratches.
- **Powerful Software:** Precise, fast processing algorithm ensures efficiency and reliability.
- **Ruggedness and Versatility:** Solid engineering and superior materials allows for use under extreme conditions.
- **Ergonomic Design:** Compact, modular design for seamless integration into small devices, ease of use, and compatibility make it ideal for a broad range of applications.
- **Low Cost:** Products are developed to deliver high performance, zero maintenance at very affordable prices for general and industrial use.

Advantages of SecuGen Sensors Over Other Optical Sensors

- Unique optical method captures fine details, even from dry skin
- Extremely low image-distortion
- Reinforced materials
- Wear resistance
- Attractively small size
- Ease of integration
- Ready-to-use
- Low cost through longer life and no maintenance requirements

Advantages of SecuGen Sensors Over Semiconductor (Capacitive) Sensors

- Non-metal, non-silicon components make it less susceptible to corrosion when exposed to salts, oil and moisture from skin and environment
- Superior surface properties eliminate need for costly coating and processing procedures
- Greater mechanical strength, wear-resistance, and durability
- Broader range of applicability, especially for use in extreme conditions and climates
- Immunity from electrostatic discharge
- Low cost through longer life and no maintenance requirements

Strengths of SecuGen Software and Algorithms

- Unique image processing algorithm extracts fingerprint minutiae very accurately
- High signal-to-noise ratio processing algorithm screens out false features
- Highly efficient matching algorithm
- Fast overall process of extraction, matching and verification
- Encryption function to protect user privacy
- Compatibility with existing desktop, laptop PCs interface computers
- Ease in developing applications for various purposes

1. Introduction & Installation

Thank you for choosing SecuGen® USB Fingerprint Readers!

You will find many uses for SecuGen readers – versatile, high quality scanning devices that can be used for a variety of security applications. This guide explains the different types of SecuGen readers, guides you through installation, and provides tips on usage, care and troubleshooting.

Types of USB Fingerprint Readers

It is important to know which sensor your fingerprint reader is based on to ensure that it is correctly installed and configured on your system. If you are not certain, please refer to the chart below, which lists the model numbers and product names.

Sensor	Type	Model Number	Product Name
FDU04 SDU04P	Hamster	HFDU04, HSDU04P	SecuGen Hamster IV
	ID	XFDU04SC, XSDU04PSC	SecuGen iD-USB SC/PIV
FDU03 FDU03FR FDU03FRS SDU03M SDU03P	Hamster	HFDU03, HFDU03FR, HFDU03FRS, HSDU03M, HSDU03P	SecuGen Hamster Plus
	ID	XSDU03MSC	SecuGen iD -USB SC
	Keyboard	KSDU03M	SecuGen Keyboard Plus
	Mouse	MSDU03M2	SecuGen OptiMouse Plus
FDU02 FDU01	Hamster	HFDU01, HFDU02	SecuGen Hamster III
	Mouse	MFDU01, MFDU02	SecuGen OptiMouse III
	Keyboard	KFDU01, KFDU02	SecuGen Keyboard III

Note: We use the terms **reader** and **device** interchangeably to refer to the SecuGen fingerprint reader itself.

System Requirements for Windows

USB 1.1 port or hub (self-powered for OptiMouse or Keyboard) or USB 2.0 port (Hamster IV)
32MB RAM
20MB available hard disk space

If you are installing an application based on platforms other than Windows, such as Windows CE or Linux, please refer to the documentation provided by the maker of the application program.

Driver Installation

Before using your SecuGen fingerprint reader, drivers must be installed.

For Windows users

Drivers are automatically installed after you plug in the reader for the first time.

If you have software for your reader

Drivers may already be included with the installation media.

To manually install device drivers

You may download them from SecuGen's website at www.secugen.com/download.

2. Tips on Use and Care of Your Fingerprint Reader

Why is image quality important?

SecuGen fingerprint recognition technology is based on minutiae, the feature points found in a fingerprint. When a fingerprint image is captured, a sampling of minutiae are extracted and processed into a template, which will be used for the biometric software functions of enrollment and matching. If the captured image is not clear or does not have enough contrast, the minutiae may be inconsistently sampled, thus resulting in less accuracy and poor performance.

Certain environments and skin conditions, such as wet, dry, or aged skin, can initially cause a fingerprint image to appear too light or dark. By adjusting the image quality for your device, it is possible to overcome the enrollment or matching problems that have commonly occurred with fingers that “don’t seem to work”.

Proper placement is the key to good results

SecuGen's fingerprint extraction algorithm is capable of extracting the correct minutiae even without benefit of a perfect print. However, the proper placement of your finger during fingerprint input can help produce more consistent results for any biometric application. The following tips on usage and care will help you obtain an optimal fingerprint image quality that ensures better performance and reduces the chances for failure to enroll and match correctly.

Important Notes:

Fingerprint images are never stored

SecuGen fingerprint technology is based on minutiae, the feature points around the core of your fingerprint. When a fingerprint is captured, only a portion of the minutiae are sampled, and then processed by an extraction algorithm and converted into a secure template. After the template is formed, the fingerprint image is deleted. All fingerprints are used in the form of templates enrollment and matching.

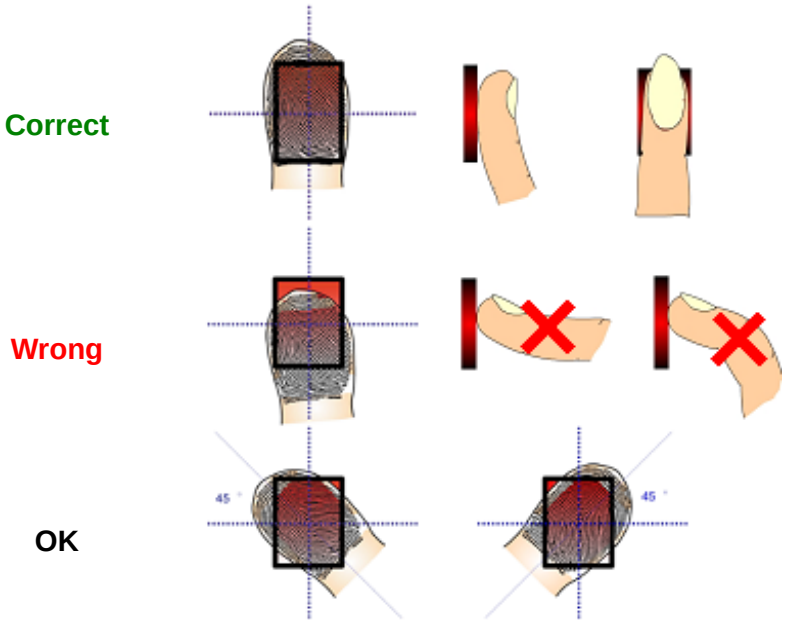
Fingerprint images cannot be reconstructed from minutiae or templates

The minutiae sampled from a fingerprint do not have enough information to recreate an image of the fingerprint. Additionally, minutiae cannot be extracted from a template because the mathematical conversion from minutiae to template is irreversible. As a final measure of security, templates are secured using advanced encryption to prevent data from being “hacked.”

2.1. Usage

Place the pad of your finger at the center of the sensor

The pad is the fleshy part of the finger, located near the middle of the first segment of the finger. Be sure that the pad (not the tip) covers as much of the sensor window as possible so that the ***core*** of your fingerprint can be scanned. It is okay to place your finger at an angle.



Apply light pressure

Apply pressure lightly and evenly during the capturing process. Use as much pressure needed to hold a piece of paper between your fingers. Pressing too hard may result in an overly dark or blurred image.

Keep your finger still

Wait for the LED to light up. This indicates that the device is activated. Keep your finger in place while the fingerprint is captured.

How to find the core of your fingerprint

The fingerprint generally consists of lines or ridges that form a pattern. The core of a fingerprint is defined as the topmost point on the innermost ridge that curves downward. The core can usually be found at or just below the center of the first segment of your finger. The following image shows examples of core points on different fingerprint patterns.

The core of your fingerprint is located in the pad of the first segment of your finger. An easy way to ensure that the core is capture when scanning is to place the finger so that the first joint of the finger aligns with the bottom edge of sensor window.

If you cut or injure your finger

As a precaution, it is best to enroll more than one finger so that if one finger becomes unavailable for authentication, you will have an alternate finger to use. Most biometric applications provide the option to enroll multiple fingers. If your application features a password or PIN back-up, you can use this feature in case no finger or fingerprint device is available. If none of these options work, please contact your IT administrator or technical support provider for help.

Problematic fingerprints

By following the above guidelines, you should be able to get consistently good results. Sometimes, however, certain skin conditions or environments may cause poor fingerprint images. Damp skin may cause fingerprints that are too dark or smudged, but can be remedied by wiping fingers before input. If your finger is extremely dry, you can safely use a moisturizing lotion before input. Alternatively, if these problems are persistent, you can by adjust the brightness settings for your device to get the best contrast and brightness levels. For more instructions, refer to Section 4.2.

For Hamster readers equipped with Auto-On™

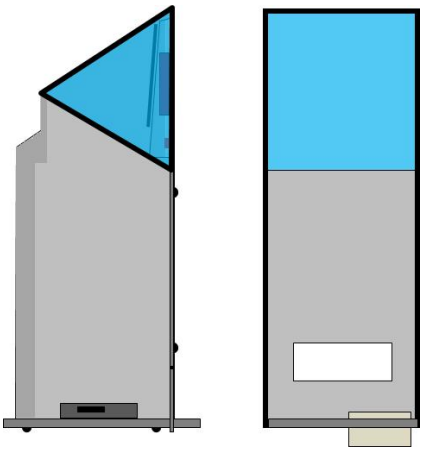
Do not place your finger too slowly or too softly

The Auto-On sensor might not detect your finger when it's placed too slowly or too softly on the reader. If the LED does not turn on, ***remove your finger and wait for 5 seconds*** to allow the sensor to reset. Then try again.

Do not wrap your fingers or hand around the top of the reader near the sensor

The Auto-On sensor might not detect your finger if your fingers are wrapped around the sides or back of the top of the Hamster. If the LED does not turn on, ***remove your finger and wait for 5 seconds*** to allow the sensor to reset. Then try again.

Avoid touching the sides and back of the blue circled area



Fingerprint sensor inside the Hamster
(Left: Side view. Right: Rear view)
Avoid touching the blue areas.

2.2. Care

Normal oil, residue or smudges on the fingerprint sensor window will not cause problems or interfere with capturing fingerprints. The sensor window was designed to withstand heavy use and extreme conditions including heat and cold. It does not have any coatings and is made of a hard, quartz-like material that resists scratches, etching, and damage from environmental elements.

If you wish to clean the surface of the sensor window

- You can safely use a dry or wet paper towel or cloth to wipe off the window. To remove stubborn dirt, you can rub the window with a cloth dampened with a soap solution. Squeeze out excess liquid before rubbing with the damp cloth.
- Cleaning agents like glass cleaners and anti-bacterial wipes may be used without harming the sensor. However, the plastic housing of the unit may be damaged if strong solvents, acids or caustic solutions are used.
- Do not pour liquids directly onto the sensor or device, as the liquid might seep into the underlying components and cause damage.

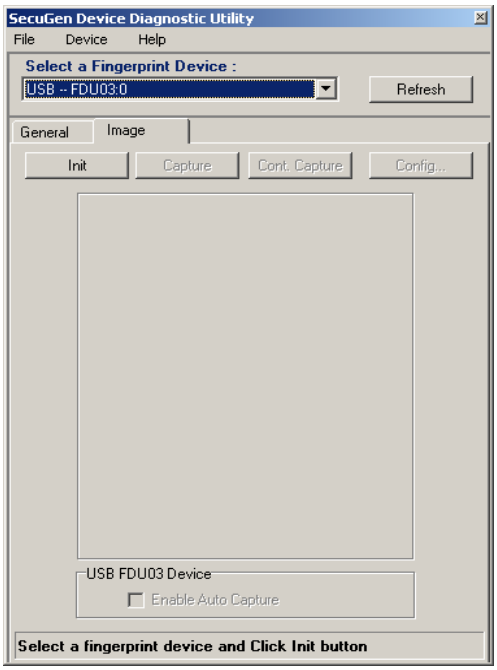
3. Device Diagnostic Utility (SGDX)

The Device Diagnostic Utility is a user-friendly tool that provides several important functions:

- To practice capturing fingerprints and test your reader for proper functioning
- To optimize the image quality of fingerprints for improved accuracy
- To get basic information about your system and hardware configuration.
  *** This is important if you need to return a product for warranty repair. ***

To run the Device Diagnostic Utility

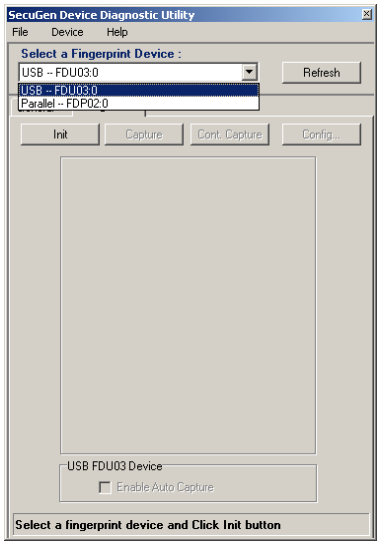
Click on the Windows Start button, type "**sgdx**" in the search box, and click enter.



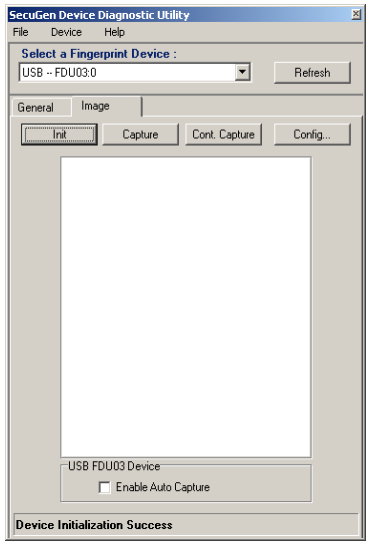
3.1. Practice capturing fingerprints

Important Note:
By default, fingerprint images are never stored. When a biometric software application requires you to input a fingerprint for enrollment or verification (i.e. for login), your fingerprint images are momentarily captured and then deleted after minutiae are extracted. Neither the minutiae nor the encrypted template, formed by the minutiae, can be used to reconstruct a fingerprint image.

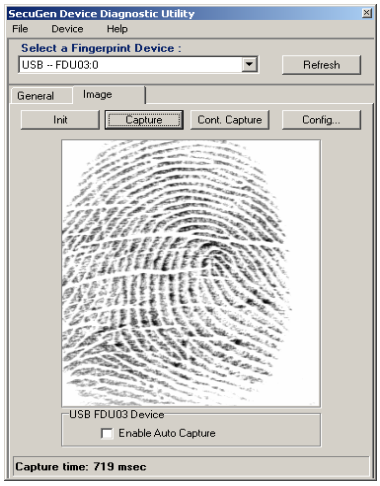
1. Select the reader you are using from the **Select a Fingerprint Device** drop-down menu.



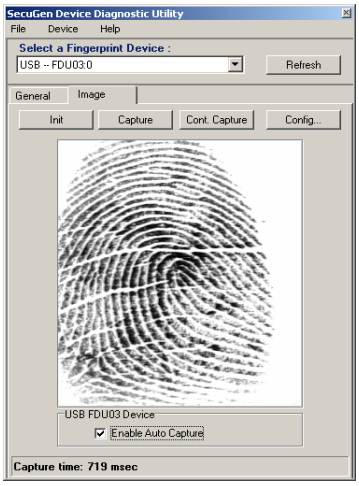
2. Click on the **Image** tab and then **Init** to initialize the reader. Initialization results are displayed at the bottom of the window.



3. Place your finger on the sensor of the reader and click **Capture**. When the LED of your reader lights up, an image will be captured and displayed in the main window.



4. To test the Auto-On™ function, click on the **Enable Auto Capture** checkbox. The reader will automatically capture a fingerprint when you place your finger on the sensor.

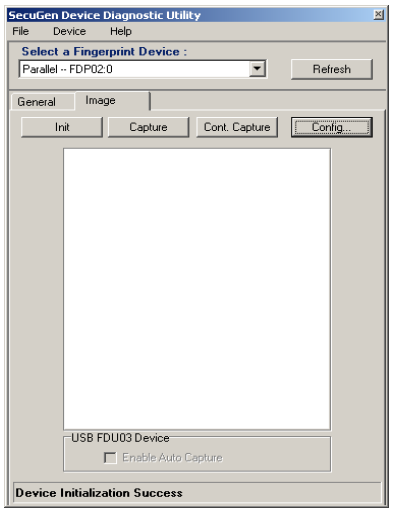


3.2. Adjust Image Quality

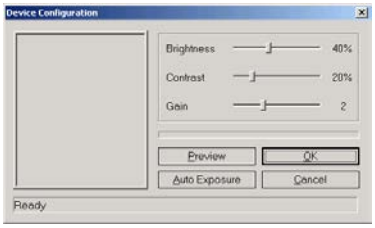
The Device Diagnostic Utility lets you adjust the fingerprint image quality settings of your reader for optimal performance. The importance of image quality is explained in the previous section.

Note: Some software applications made for SecuGen products may also have an image adjustment feature built-in to their program. In such case, please refer to the corresponding documentation.

1. From the window under the **Image** tab, and then click **Config…**. You may need to first click **Init** if your reader was not yet initialized.



2. When Device Configuration opens, place your finger on the device sensor window, and click **Preview** to view your fingerprint.



Example of image that needs to be adjusted

3. For manual adjustment, click and drag the Brightness or Contrast sliders, and then click **Preview** again.

   If the **images** are still too bright, you can further adjust the gain setting by moving the Gain slider.

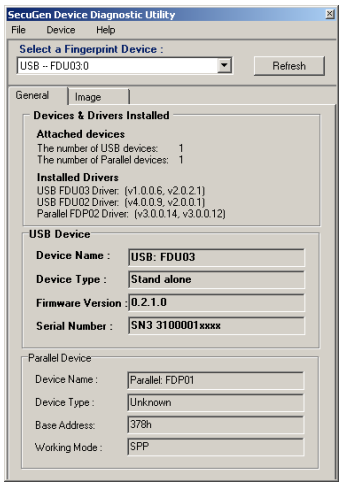
Example of image after manually changing settings

4. To let the system automatically determine optimal settings, click **Auto Exposure**. Hold your finger still on the sensor window during the entire process. The settings will automatically change incrementally, and a blue status bar will indicate the progress. Click **Preview** again to check the improvement of your fingerprint image.

Example of image after automatic setting adjustment

5. To keep the new settings, click **OK**. To go back to the original settings, click **Cancel**.

3.3. Get Information about Your Device



*** You may need this information before returning a product under warranty. ***

Select the **General** tab and select your device from the drop-down menu.

Devices & Drivers Installed
The number of devices and driver version(s) will be displayed.

USB Device
The Device Name, Device Type, Firmware Version, and Serial Number will be displayed. This information is available only when the reader is initialized.

4. Troubleshooting

Windows is warning me that the driver has not passed Windows Logo testing

If you are a Windows user and you see a warning box that says the SecuGen device driver has not passed Windows Logo testing, please click the “Continue Anyway” button. Our drivers have been tested thoroughly with all Windows version listed in System Requirements. Drivers are regularly updated for Windows compatibility and should be automatically downloaded from Microsoft's Windows Update web site and included in future Windows Service Packs. (www.windowsupdate.com).

My SecuGen USB reader does not power on

If you have connected the reader to a USB port in a USB keyboard or hub, verify that the USB keyboard or hub has its own power-supply. Some SecuGen readers use up to 150 mA of electric current, so if they are not already connected directly to the computer, then they should be connected to hubs that are self-powered.

My USB reader powers on but cannot capture fingerprints

When you have other high-speed USB devices, such as a digital camera or scanner, connected to your computer, the SecuGen reader cannot be used at the same time. SecuGen USB readers may use up to 66% of USB 1.1 bandwidth, and therefore cannot function concurrently with any other device using more than 40% of the bandwidth. Close the programs that use the other USB devices, and if necessary, disconnect those devices, before using the SecuGen reader.

My USB reader powers on but sometimes cannot capture fingerprints

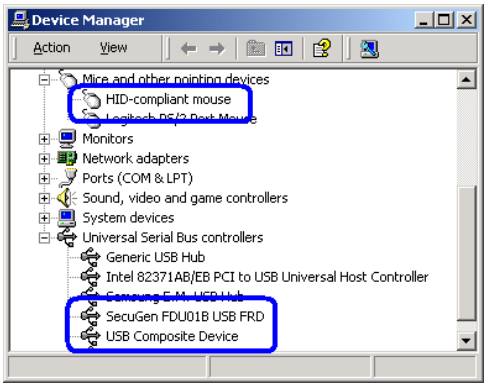
If you are using a reader that is equipped with the Auto-On™ feature, you might be experiencing interference with the Auto-On sensor. To reset the sensor, remove you finger from the sensor and wait 5 seconds to allow the sensor to reset. To prevent this problem, see the tips in section 2.1 Usage.

My OptiMouse is very slow

When certain other mouse drivers are installed on your computer, the USB OptiMouse response may be slow. Click **Start > Control Panel > Mouse** and the **Operation** tab to adjust the speed of mouse pointer. If you cannot adjust the speed of mouse pointer, remove the other mouse driver from the system.

My OptiMouse doesn’t work

First verify that the OptiMouse is connected to the USB port correctly. Then click **Start > Control Panel > System** and select the **Device Manager** tab to verify that the mouse drivers are installed correctly. If they are not installed correctly, repeat the driver installation process.



My USB reader is not recognized

If you are using an FDU01 or FDU02 based reader, be sure to use the appropriate device driver from SecuGen’s website at www.secugen.com/download. Although older FDU01 devices can work with FDU02 device drivers, readers based on FDU02 cannot work with FDU01 device drivers.