BIOCENTRIC
SOLUTIONS
INCORPORATED

GuardDog Biometric Reader

Owner's Guide

Notice

Information in this publication is provided for reference and is believed to be accurate and complete. Biocentric Solutions Incorporated is not liable for errors in this publication or for incidental or consequential damage in connection with the furnishing or use of the information in this publication.

Biocentric Solutions Incorporated makes no warranty regarding the material in this publication, including, but not limited to any implied warranty of fitness or merchantability for any particular use.

Biocentric Solutions Incorporated reserves the right to make changes to this publication and to the products described in it without notice. All specifications and information concerning products are subject to change without notice. Reference in this publication to information or products protected by copyright or patent does not convey any license under the rights of Biocentric Solutions Incorporated or others. Biocentric Solutions Incorporated assumes no liability arising from infringements of patents or any other rights of third parties.

Part Number: 269-1010-01

First published June 2001
Revised October 2001

Contents

Safety Precautions

CAUTION

This unit contains no user-replaceable parts. Do not attempt to open the unit or make any internal repairs yourself. Only Biocentric Solutions-trained service technicians may make repairs to the unit. Breaking a seal will void the warranty.

Never provide unauthorized modifications to this system.

WARNING

Units should be installed only by authorized installers.

This product is intended to be supplied by a listed direct plug-in power unit marked “Class 2” and rated 8–16 VDC, 250 mA.

Desktop units are powered by an adaptor that plugs into any standard receptacle. The adaptor is for indoor use only and must be UL approved.

To disconnect power from a desktop unit, you must remove the plug from the receptacle. Therefore, you must ensure that the receptacle is easily accessible.

About This Guide

This Biocentric Solutions guide is written for individuals responsible for the use of the GuardDogs. Although this guide includes information about the end use of the GuardDog, much of the information is not generally needed by end users. End users should refer to the quick reference guide for the type of GuardDog they are using. (Information for all GuardDog models are included in this guide.)

This guide includes the following chapters:

Chapter 1, “Introducing the GuardDog” describes the GuardDog and provides an overview of the many ways it can be used.

Chapter 2, “Using the GuardDog” includes detailed instructions for using the iButton™ and contactless GuardDog in day-to-day activities.

Chapter 3, “Maintaining the GuardDog” includes information about keeping the GuardDog in peak operating condition.

Chapter 4, “Product Specifications” lists GuardDog specifications that include sizes, operating environment, power, and digital interface information.

Conventions Used in This Guide

The following safety notice conventions are followed throughout this guide:

WARNING

A WARNING contains an operating or maintenance procedure, practice, condition, statement, etc., which, if not strictly observed, could result in injury or death of personnel.

CAUTION

A CAUTION contains an operating or maintenance procedure, practice, condition, statement, etc., which, if not strictly observed, could result in damage to, or destruction of, equipment or data.

NOTE

A NOTE contains an essential operating or maintenance procedure, condition or statement, which is considered important enough to be highlighted.

Related Documents

For a quick reference about using the GuardDog, refer to the following documents:

- *Using the iButton GuardDog* (269-1009) describes, in three easy steps, how to authenticate yourself using an iButton GuardDog. This laminated 14 cm × 19.68 cm (5.5″ × 7.75″) reference also includes general finger placement tips and tables that describe the GuardDog's normal operating and error conditions.

- *Using the Contactless GuardDog* (269-1014) describes how to authenticate yourself using a contactless GuardDog. This laminated 14 cm × 19.68 cm (5.5″ × 7.75″) reference also includes general finger placement tips and tables that describe the GuardDog's normal operating and error conditions.

Getting Help

If you encounter problems or questions with your Biocentric Solutions GuardDog, please take the following steps:

1. Refer to the documentation and other materials that came with your product. Most often you can find the answer to your question in this way.

2. Be sure to check the GuardDog specification and installation planning requirements to make sure the power and other wiring requirements are met.

3. Be sure to check the hardware and software requirements for the GuardDog to make sure your computer, software, and related components meet the minimal system requirements.

4. Consult with your Sales Representative. These trained personnel are familiar with the most-asked questions and can usually provide you with the information you need.

5. If your question cannot be answered by reading the documentation or by your direct representative, contact the Biocentric Solutions representative from whom you purchased the GuardDog. Before calling, gather as much information as possible about your problem or question. Have your GuardDog's serial or model numbers and software version numbers available when you call.

Chapter 1 • Introducing the GuardDog

The GuardDog is a miniature, fingerprint authentication unit that compares stored fingerprint templates with fingerprint data acquired in real time. The GuardDog is part of Biocentric Solutions CombiFamily of products, which includes the CombiReader™, CombiMemory™, and CombiSmart™.

All Combis, including the GuardDog, are intelligent devices that can verify the identity of an individual by scanning his or her actual fingerprint and comparing the scanned print with fingerprint data (called a template) printed or stored on a personal token. The verification is performed at the device, so no fingerprint data need be stored in or transmitted to a central database.

The GuardDog offers a simple, easy to use, and reliable solution for a variety of security and access control challenges in harsh environments. It is especially designed to withstand moisture, heat, and cold and can be operated as a stand-alone unit or included in a network.

Typical GuardDog applications include:

- **Stand-alone identity verification** where the GuardDog confirms that a person is the rightful holder of a token (an iButton or contactless smart card) that he or she is carrying.

- **Access control** where the GuardDog confirms the identity of the carrier of a token and interfaces with other access control devices, such as alarms and door latches. The comparison of the scanned print with the fingerprint data is done in the GuardDog so no fingerprint information is transmitted to another computer. In an access control application, the GuardDog can work autonomously (storing all access control information locally) or in a network configuration with critical information (other than fingerprint information) stored on a security server.

- **Time and attendance** where the GuardDog confirms the identity of a token carrier and also generates a log entry for each transaction. Just as it can in an access control application, the GuardDog can work autonomously or in a network configuration in a time and attendance application.

GuardDog Models

Two types of GuardDogs are currently available:

- The iButton GuardDog requires a Dallas Semiconductor iButton be used for enrollment and authentication. The iButton is extremely rugged and sturdy because the computer chip is protected by a metal enclosure.

- The contactless GuardDog requires a contactless smart card that operates on the Philips MIFARE® communication standard (ISO 14443A). While not as rugged as the iButton, the contactless smart card offers the convenience of proximity cards without compromising security.

Figure 2 shows the two GuardDog models.

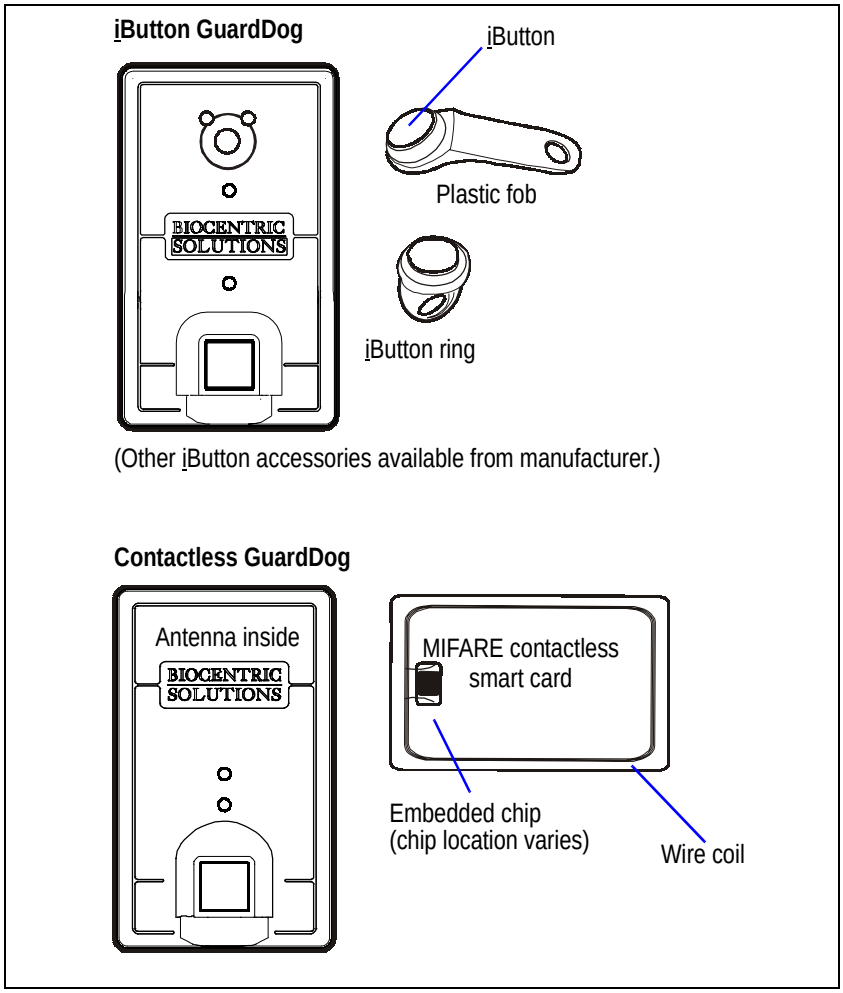


Figure 2 • GuardDog Models

Data Encryption and Digital Signing

Information stored in the iButton and contactless smart cards is encrypted using an industry-standard encryption algorithm. In addition, the data is digitally signed. The GuardDog accepts only tokens signed with the correct digital signature.

Digital Interfaces

GuardDogs are designed to operate as stand-alone devices or connected to a central system via an RS-232 or RS-485 interface. The RS-232 interface allows connection of a single GuardDog to the serial port of a standard PC located close to the unit. The RS-485 interface allows connection of multiple GuardDogs to a twisted pair LAN extending up to several hundred feet. Multiple GuardDogs can be connected in a single network, with multiple security groups.

The GuardDogs also include an industry standard Wiegand output interface that supports the connection of electronic door locks.

User Interfaces

Both GuardDogs have two LEDs and a buzzer to provide both visual and audible indicators for authentication success/failure.

Chapter 2 • Using the GuardDog

Figure 3 identifies the operating features of the iButton and contactless GuardDogs.

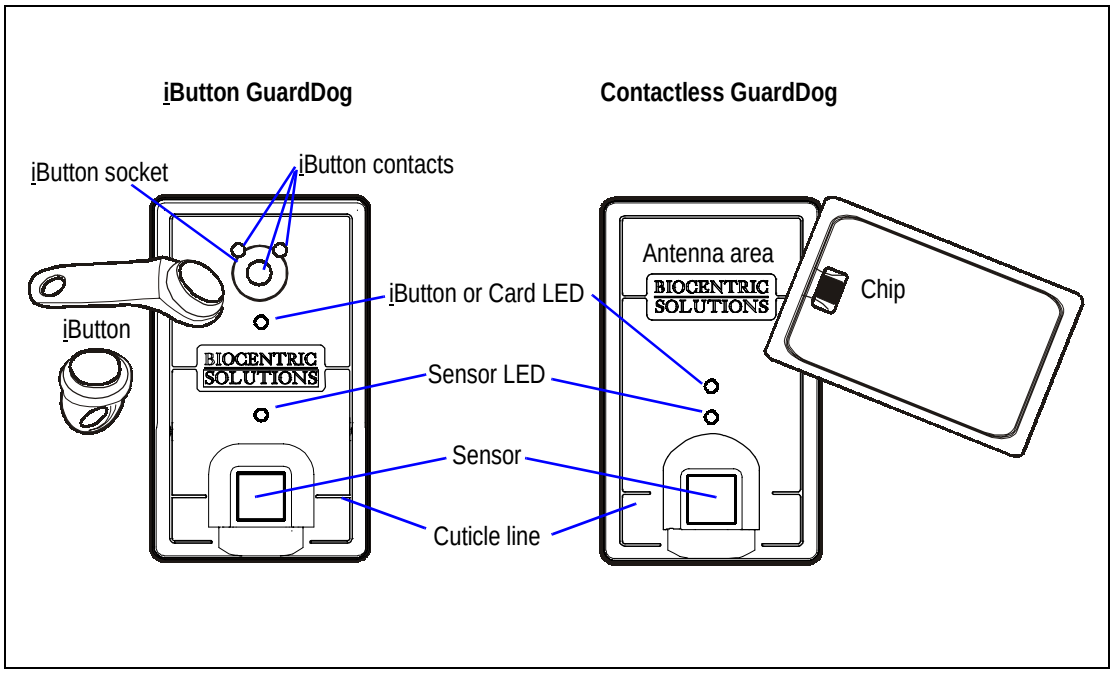


Figure 3 • GuardDog Operating Features

Power up Sequence

When a GuardDog first receives power, it perfoms internal self-test and initialization procedures. Upon sucessful completion, the GuardDog's top LED blinks red, amber, and green; and the unit "chirps" twice.

Standard Operation

The GuardDog is ready to be used when the top LED is blinking green.The color of the LEDs generally indicates the conditions listed in the table below.

Table 1: LED Colors and Conditions

Color	Conditions
Green	Ready or accepted
Red	Rejected
Amber	Reading or scanning in progress

Using the iButton GuardDog

The iButton GuardDog operates with the iButton token illustrated in Figure 4. The iButton is a metal button that can be attached to various accessories, such as the plastic fob.

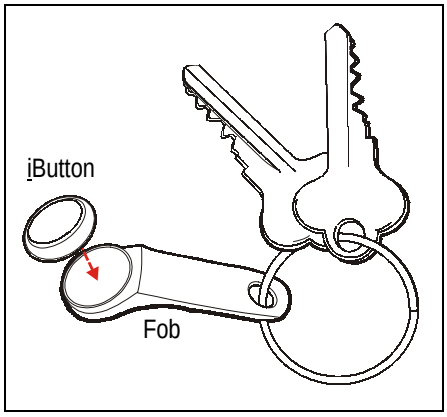


Figure 4 • iButton Token and Fob

To use the iButton GuardDog for authentication:

1. Insert the iButton in the GuardDog's socket. The iButton must touch the center contact and at least one of the top contacts. (See Figure 5.)

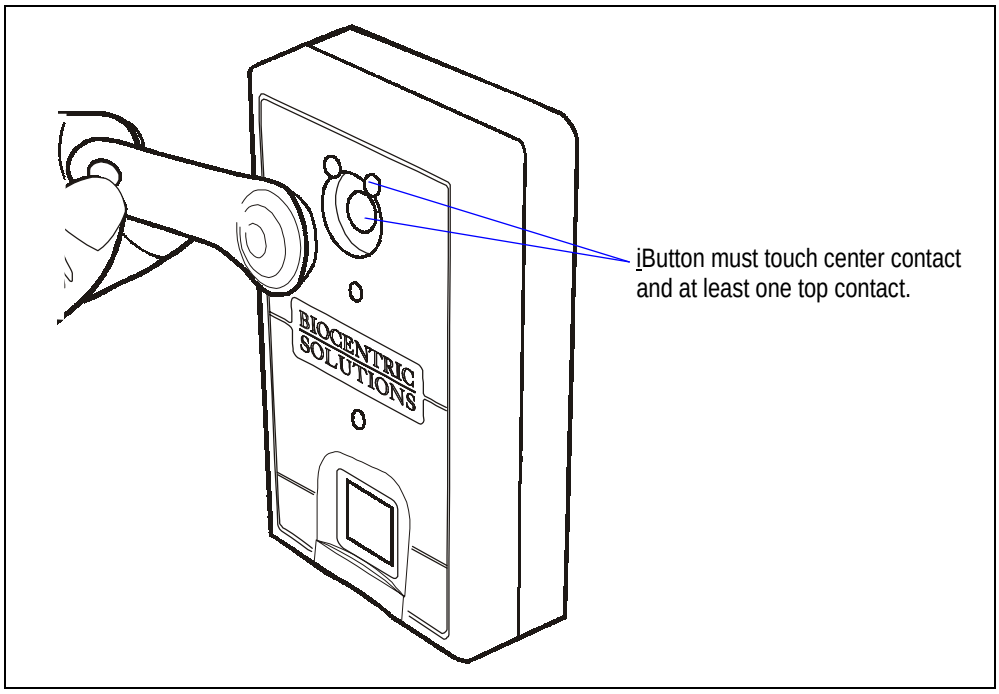


Figure 5 • iButton Contacts

   The LED turns amber when the GuardDog is reading the button.

2. After the "chirp" and when the Fingerprint Sensor LED is blinking green, remove the iButton from the socket and place your finger on the sensor.

   The LED turns amber when the GuardDog is scanning your finger.

3. After the chirp and when the LED turns off, remove your finger.

   The GuardDog emits three very quick chirps and both LEDs blink green to indicate that you have been successfully verified.

   If the GuardDog emits only a single chirp and the Fingerprint Sensor LED starts to blink green again, the GuardDog was unable to verify you. Reposition your finger and repeat step 3. If, after three tries, the GuardDog cannot make a verification, both LEDs blink red and the unit emits three long beeps. See "Finger Selection and Placement Tips" on page 10 for more information about ensuring successful verification.

Using the Contactless GuardDog

The contactless GuardDog operates with a MIFARE contactless smart card, which is the industry standard. This card complies with ISO 144443A.

▸ To use the contactless GuardDog for authentication:

1. Hold the contactless smart card close to the top of the GuardDog. The card must be 4 cm (2″) or closer. (See Figure 5.)

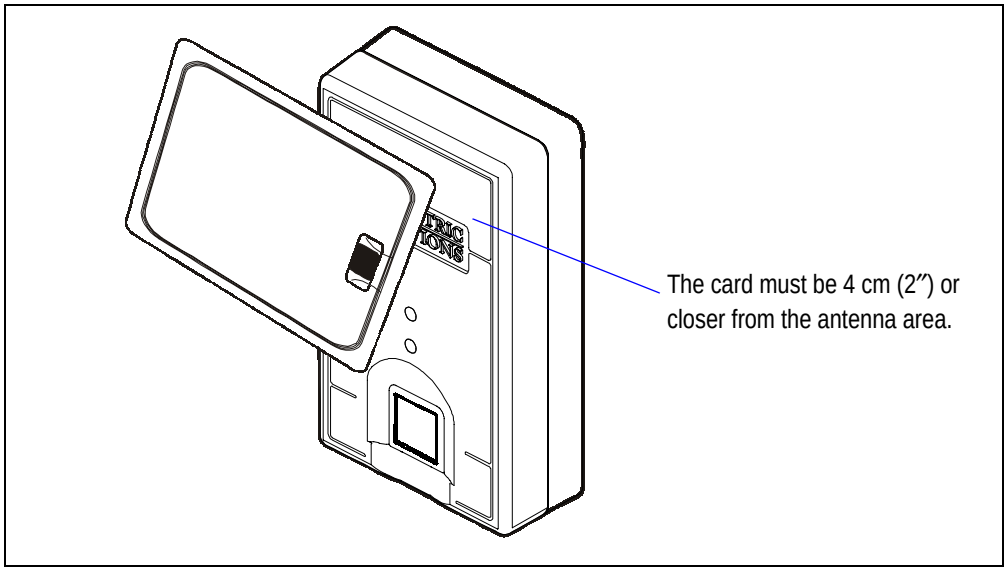


Figure 6 • MIFARE Contactless Card

   The LED turns amber when the GuardDog is reading the card.

2. After the “chirp” and when the Fingerprint Sensor LED is blinking green, place your finger on the sensor.

   The LED turns amber when the GuardDog is scanning your finger.

3. After the chirp and when the LED turns off, remove your finger.

   The GuardDog emits three very quick chirps and both LEDs blink green to indicate that you have been successfully verified.

   If the GuardDog emits only a single chirp and the Fingerprint Sensor LED starts to blink green again, the GuardDog was unable to verify you. Reposition your finger and repeat step 3. If, after three tries, the GuardDog cannot make a verification, both LEDs blink red and the unit emits three long beeps. See “Finger Selection and Placement Tips” on page 10 for more information about ensuring successful verification.

LED and Sound Conditions

The following tables list normal operating and error conditions. Usually, the end user can take action that corrects an error condition. If the action is unsuccessful, the user should notify the system administrator for assistance. If the system administrator cannot resolve the problem, he or she should call for authorized service.

Table 2: GuardDog Normal Operating Conditions

iButton or Card LED	Fingerprint Sensor LED	Sound	Indicates
Blinking green	Off	None	Okay to insert iButton or hold up card.
Amber	Off	None	Reading iButton or card.
Off	Blinking green	Single chirp	The iButton or card was read. Place or reposition finger on sensor.
Off	Amber	None	Reading fingerprint
Blinking green	Blinking green	Triple chirp	ID verified and access granted.

Table 3: GuardDog Error Conditions

iButton or Card LED	Fingerprint Sensor LED	Sound	Indicates	What to Do
Blinking red	Off	None	Cannot read iButton or card.	Wait until the top LED is blinking green and reinsert the iButton or hold up the card again.
Blinking red	Blinking red	Three long beeps	Access denied. The fingerprint template on the iButton or card did not match the scanned print.	Wait until the top LED is blinking green and try to authenticate yourself again. Refer to “Finger Selection and Placement Tips” for advice.
Off	Off	None	Unit is not receiving power.	Contact your system administrator.

Finger Selection and Placement Tips

If your thumbs have good prints, use your left and right thumbs for enrollment. (By using your thumbs, you don't have to remember which of your eight fingers you used.)

Always use more than one finger or thumb, and preferably at least one from each hand, so you have a backup in case you cut or injure yourself and can't use a finger for authentication.

When you place your thumb or finger on the sensor, position it so your cuticle is about in the center of the sensor. The GuardDog has an etched line on both sides of the sensor to help you properly position your thumb or finger.

Your finger or thumb should:

• Lie flat on the sensor

• Touch the edge of the sensor area

• Be parallel to the sensor's sides

Your finger or thumb should not be wet and don't move your finger when it is being scanned.

You need to apply some pressure but don't press too hard—you don't want to flatten your fingerprint so that it can't be scanned.

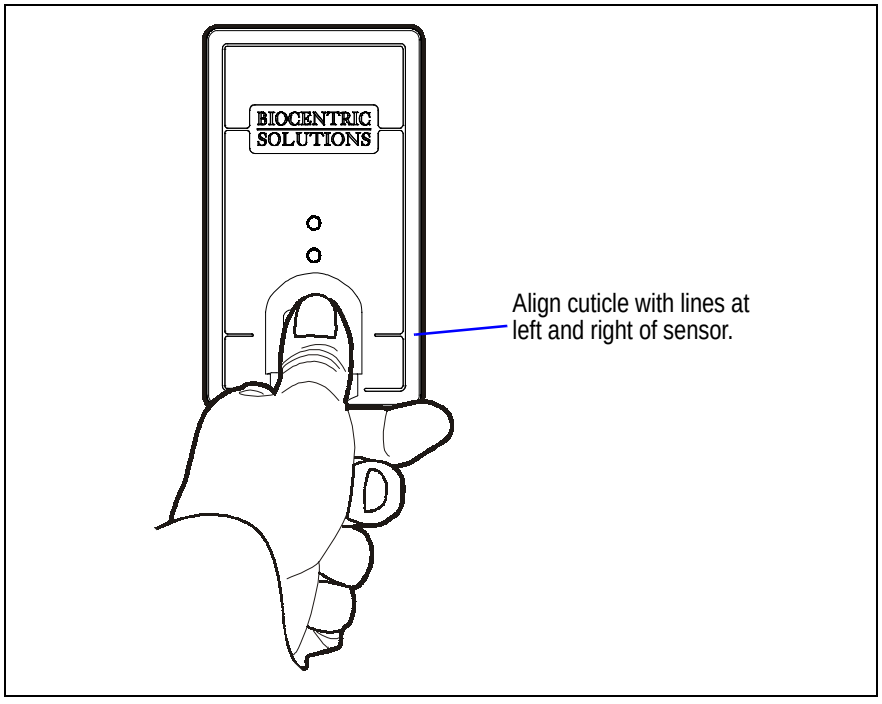


Figure 7 • Proper Finger Placement

Common Authentication Problems

Most authentication failures occur because of the following easily-corrected problems:

- Wrong finger—using one that doesn't have a template stored on the iButton or card
- Finger too wet or dry
- Pressing too heavily or lightly
- Cut finger or otherwise changed
- Finger moved during reading
- Finger positioned incorrectly

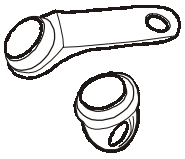
If an individual consistently has problems authenticating him or herself, you may want to re-enroll this individual using different fingers.

Chapter 3 • Maintaining the GuardDog

This chapter describes how to care for the tokens used in the GuardDog and other routine maintenance procedures that, when regularly performed, will keep your GuardDog biometric readers in top working order.

> **CAUTION**
>
> This unit contains no user-replaceable parts. Do not attempt to open the unit or make any internal repairs yourself. If the unit is not functioning properly, contact the Biocentric Solutions representative from whom you purchased the GuardDog. Breaking a seal will void the warranty.

Token Care



The iButton is virtually industructable. It should continue to work even if you drop it or step on it. It is also waterproof. If you are using a plastic fob, the fob may break but the iButton should withstand most abuse. Magnets cannot harm the iButton.

The MIFARE contactless smart card is waterproof but it should not be bent or folded to avoid breaking the wire coil that runs around the edge of the card. Magnets cannot harm the card. In extrememly rare situations, a device operating on the same radio frequency may interfere with its use.

Setting the Time

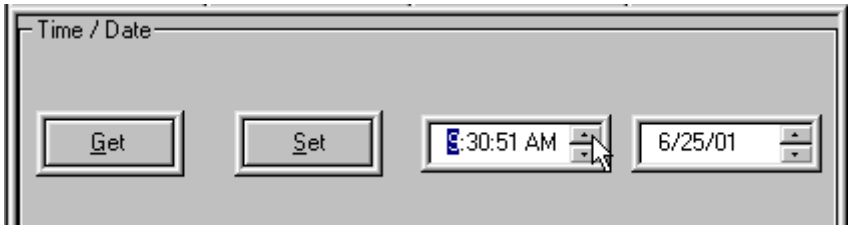
The GuardDog's internal clock needs to be reset any time the unit loses power. The following instructions tell how to set the time using the Admin program. To set the time in a GuardDog, it must be connected to a computer either directly or in a network.

To reset the time:

1. Start and log into the Biocentric Solutions Admin program.
2. Select the **Network** tab if that page is not already displayed.
3. From the **Port** drop-down list, select the communications port to which the GuardDog or network of GuardDogs is attached.
4. If an ID number does not appear in the **ID** drop-down list, select the **Enumerate** button to allow the program to identify and list the ID number(s) of the GuardDog(s).
5. In the **ID** drop-down list, select the ID number of the GuardDog in which you want to set the time or select the **Broadcast** button to set the time in all the GuardDogs at once.
6. If the displayed time and date is incorrect, change them to the correct settings.

Changing the Time and Date Settings

To change a unit of time or date, select the unit and then scroll up until it displays the correct value. For example, select the hour, and then scroll up to increase its value. Scroll down to decrease its value.



7. Select the **Set** button to set the time in the GuardDog(s).
8. Select the **Get** button to verify that the time and date is now properly set. After selecting the **Get** button, the time and date appear in the status bar at the bottom of the **Network** page.

Cleaning the GuardDog

Regular cleaning can help prevent authentication failures. The fingerprint sensor, in particular, should be regularly cleaned because dirt, dust, and other grime on the sensor can interfere with fingerprint imaging.

External Surfaces

Use a damp cloth to remove loose dirt and dust from the external surfaces of the GuardDog.

iButton Contacts

Use a cotton swab and isopropyl alcohol to clean the card slot or iButton contacts.

Fingerprint Sensor

Use a cotton wipe and isopropyl alcohol to clean the fingerprint sensor.

Chapter 4 • Product Specifications

This chapter lists specifications for the iButton and contactless GuardDog.

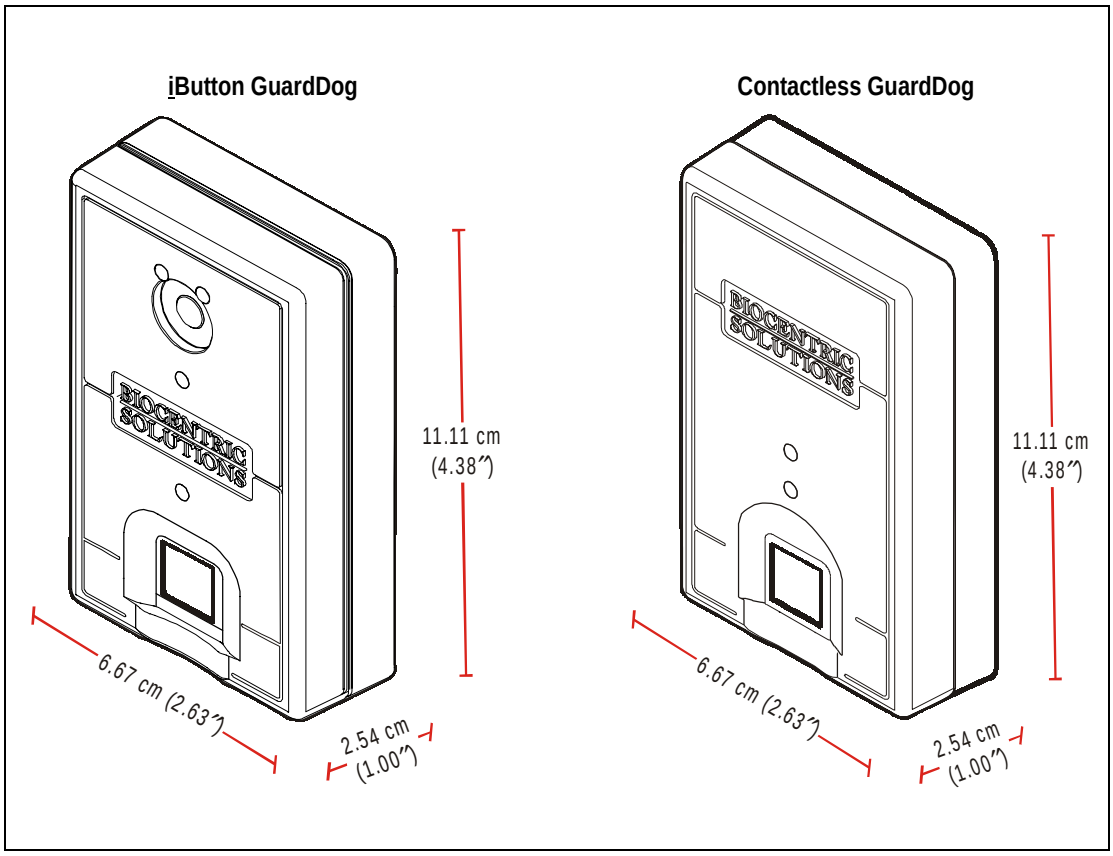


Figure 8 • GuardDog Dimensions

Tokens

iButtons: Dallas Semiconductor's (write-once) read-only and read-write iButtons, 16-kbit and 64-kbit, fob and ring (64-kbit only) mounts. The iButton must make contact with the GuardDog contact points to operate.

Contactless Smart Cards: Philips Semiconductors MIFARE contactless smart card that complies with the ISO/IEC 14443A standard and has at least 1 KB (8-Kbit) of memory. The card operates at distances up to 4 cm from the GuardDog.

Mechanical

	iButton Model	Contactless Smart Card Model
Width	6.67 cm (2.63 in)	Same
Height	11.11 cm (4.38 in)	Same
Depth	2.54 cm (1.00 in)	3.17 cm (1.25 in—see Figure 8)
Weight	Less than .45 kg (1.00 lb)	Same

Environmental

Operating Temperature: -20°C to 70°C (-4°F to 158°F)

Humidity: 5% to 90% (non-condensing)

Operating Altitude: 0 to 3048 m (0 to 10,000 ft)

Radio Frequency: 13.56 MHz (contactless model only)

Tamper Resistant: Two mounting points with one generic bracket

Power

Power: 12 VDC, 250 mA

WARNING

The 12 VDC power adaptor for desktop devices is for indoor use only and must be UL approved.

Digital Interface Signals

Selectable RS-232, RS-485 half duplex (default).

RS-232

- 38400 baud
- Complies with EIA/TIA-232E, V.28 specification
- Recommended maximum cable length is 15 m (about 50 ft)

RS-485

- 38400 baud
- Maximum of 32 units on each RS-485 network
- Recommended maximum cable length is 1220 m (about 4000 ft)

Wiegand Serial Data Output (Wall-Mount Only)

- 26-bit standard (others available on request)
- 50 mA maximum output current drive (output low)
- Recommended maximum cable length is 15 m (about 50 ft)

Free Exit Switch Inputs

Digital input:

- Activated with a normally-open (N.O.) switch to ground
- Maximum input voltage is 3.3 VDC (74LVCH244 input)

Data Memory

The number of records that a queue can hold depends on the record size. The main User queue typically holds at least 8,000 records. Check with the representative from whom you purchased the GuardDog for your installation’s capabilities.

Index

S

T

U

V

W