



ClipDrive Bio User Guide

Version 1.0
ClipDrive Bio 4.0



Copyright © 2004 Memory Experts International. All rights reserved. This document may not be reproduced or transmitted in any form (whether now known or hereinafter discovered or developed), in whole or in part, without the express prior written consent of Memory Experts International.

ClipDrive Bio User Guide version 1.0

Document Number: MSW1015-M-USR01-10

Date of Publication: October 31, 2004

Support: support@memoryexpertsinc.com

Web site: <http://www.memoryexpertsinc.com>

Contents

1: Introducing ClipDrive Bio	5
System requirements	6
Version information	6
Partitions	6
Types of users	6
2: Getting started	9
Authenticating to ClipDrive Bio	9
3: Working with ClipDrive Bio	13
Saving and opening files	13
Locking and disconnecting ClipDrive Bio	13
Cleaning ClipDrive Bio	14
Viewing device information	15
Using ClipDrive Bio with Outbacker	18
4: Troubleshooting	19
I can not eject my ClipDrive Bio	19
My user name is not in the list for biometric verification	19
My user name is not in the list for password verification	20
ClipDrive Bio will not authenticate my finger	20
My password access to ClipDrive Bio is blocked	20
The ClipDrive Bio drive does not display in the file manager window	20

1 Introducing ClipDrive Bio

ClipDrive Bio is a USB (Universal Serial Bus) portable flash drive with biometric security, data encryption, and management software. ClipDrive Bio works with any computer that supports USB mass storage devices; see “System requirements” on page 6 for more details.

Biometric security allows you to control access to sensitive information stored on the device using your fingerprint. Data encryption provides another level of security by protecting documents saved to a private storage area on ClipDrive Bio. Admin Console, a user-friendly management program, lets you create and manage users and configure the device.

Figure 1-1: ClipDrive Bio



This guide contains information to help you get started using ClipDrive Bio. For information about creating users, configuring the device and so on, see the *ClipDrive Bio Administration Guide*.

This chapter contains information about the following topics:

- System requirements
- Version Information
- Partitions
- Types of users

System requirements

The following list describes the requirements you need to use ClipDrive Bio:

- A USB port (Type A)
- Microsoft® Windows® 2000 SP 4, Microsoft® Windows® XP SP 1 or SP 2
- An operating system that supports USB 2.0 or 1.1 Mass Storage Devices

Version information

You can view information about the version of both hardware and software that is included with ClipDrive Bio.

► **To view version information**

- 1 Plug ClipDrive Bio into the USB port of your computer.
- 2 From the **Main** page of Admin Console, click **View Device Information**.
- 3 Click **View Version Information**.

Partitions

Partitions are sections of disks (or mass storage) that the operating system recognizes as separate drives. ClipDrive Bio contains one public disk partition that all users can access. ClipDrive Bio also provides a private partition for each user. Users must successfully authenticate to the device before they can access their private partition. Data saved to a private partition is encrypted.

Types of users

ClipDrive Bio allows two types of users to be registered on the device: administrators and general users.

- **Administrator**—a user with full privileges for Admin Console. Administrators can manage users, configure the device, and set security policies.
- **General users**—users who can access their private data by authenticating to ClipDrive Bio. They can also use Admin Console to change their passwords and update finger enrollments.

Important This guide assumes that an administrator has already created a user account and configured a private partition for you. For information about creating users, see the *ClipDrive Bio Administration Guide*.

2 Getting started

Out of the box, ClipDrive Bio has no users registered in its user database. In this state, anyone can access the device without authenticating. You can leave the device in this “open” state or you can use the authentication features available with ClipDrive Bio to control who can access the device. You, or an administrator, must create user accounts to use the authentication features. Once a user is created, authentication is always required to access ClipDrive Bio.

ClipDrive Bio provides the following two types of authentication:

- Biometric (fingerprint)
- Password

Authenticating to ClipDrive Bio

You can authenticate to ClipDrive Bio using a fingerprint or a password (provided that your administrator has granted you password privileges). For biometric authentication, you must first enroll your finger so that ClipDrive Bio can identify or verify you as a valid user. ClipDrive Bio has two types of biometric authentication:

- **Biometric identification**—where the device identifies you by comparing your finger to all enrolled fingerprints
- **Biometric verification**—where you provide your user name and the device verifies your finger against only your enrolled fingerprints

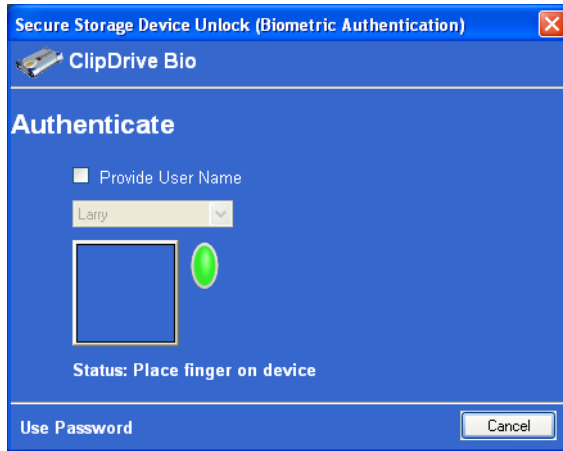
Passwords are typically used only for emergency situations where biometric authentication is not possible—for example, the fingerprint sensor is damaged, or you injured your finger.

Note For information about enrolling fingers and setting passwords, see the *ClipDrive Bio Administration Guide*.

► **To access ClipDrive Bio using a fingerprint**

- 1 Plug ClipDrive Bio into the USB port of the computer

The Unlock program starts automatically to allow you to complete the biometric authentication process. By default, the authentication starts in biometric identification mode. No user name is required.



- 2 Place your enrolled finger on the sensor.
- 3 Follow the prompts in the authentication dialog box until ClipDrive Bio successfully identifies your finger.

Note If ClipDrive Bio is blocked for biometric identification you will have to select your user name from the list. If your fingerprint is blocked from using biometric verification, then your name will not appear in the user list.

► **To access ClipDrive Bio using a password**

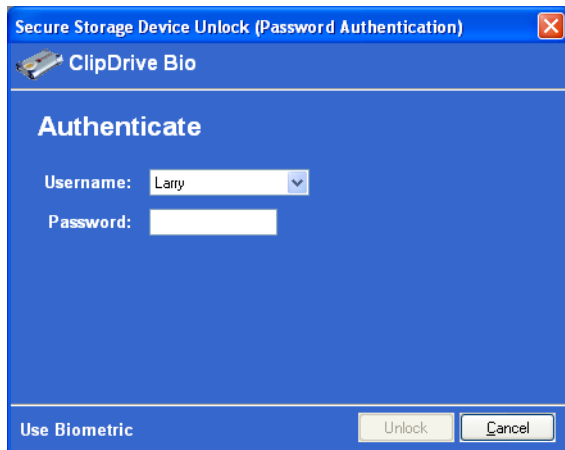
- 1 Plug ClipDrive Bio into the USB port of the computer.

The **Unlock** program starts automatically.

- 2 On the Secure Storage Device Login dialog box, click **Use Password**.

- 3 Select your user name from the **Username** list.

If you do not have a password, or your password is blocked, your name will not appear in the list.



- 4 Type your password in the **Password** box. Passwords are case-sensitive.
- 5 Click **Unlock**.

Note You can also start the Unlock program from the **Start** menu. Click the **Start** button, and then click **All Programs, MXI, Unlock device**. You can use this method when ClipDrive Bio is locked but still plugged in.

3 Working with ClipDrive Bio

ClipDrive Bio lets you save files to and open files from a private partition. You can lock ClipDrive Bio to ensure that only authenticated users can access the device while you are away from the computer. You can disconnect the device completely to bring the data with you.

Care and cleaning of ClipDrive Bio is extremely important to maintain the function and security of the device.

You can view device information, about users, device configuration, and version number.

This chapter contains information about the following topics:

- Saving and opening files
- Locking ClipDrive Bio and disconnecting it from the computer
- Care and cleaning of ClipDrive Bio
- Viewing information about users and the device
- Using ClipDrive Bio with Outbacker

Saving and opening files

You can save files to a shared public partition on ClipDrive Bio or to a private partition that only you can access. When you save data to your private partition, ClipDrive Bio encrypts the file using the FIPS-approved AES algorithm. Data is automatically decrypted when you open the file.

Once you authenticate to ClipDrive Bio, you can access files on your private partition using the appropriate program or a file manager, such as Windows® Explorer.

Locking and disconnecting ClipDrive Bio

Locking ClipDrive Bio requires you to disconnect your private partition. If you leave your computer without locking ClipDrive Bio, any user can access the information stored on your private partition.

You can disconnect ClipDrive Bio from your computer using the eject operation.


► **To lock ClipDrive Bio**

- From the file manager window, right-click your private partition and click **Eject**.

You can also lock ClipDrive Bio from Admin Console. From the **Main** page of Admin Console, click **Lock Device**.

Note To eject a drive from the file manager you must have Administrative privileges on the computer. This limitation is documented by Microsoft in the following article <http://support.microsoft.com/default.aspx?scid=kb;en-us;192785>.

► **To disconnect ClipDrive Bio**

- 1 From the Windows task bar, click the **Safely Remove Hardware**  icon.
- 2 When you see the following prompt, you can safely disconnect the device from the USB port.



Caution Disconnecting ClipDrive Bio, either accidentally or on purpose, without using the safely remove hardware operation, could cause corruption of the data on the device.

Cleaning ClipDrive Bio

Always transport ClipDrive Bio in its case to protect the fingerprint sensor. Direct contact with metal objects, like keys, can permanently damage the fingerprint sensor and adversely affect the fingerprint capture process. It is recommended that you clean the fingerprint sensor surface each month.

► **To clean the fingerprint sensor**

- 1 Disconnect ClipDrive Outbacker from the computer.
- 2 Slightly dampen part of the cloth supplied with ClipDrive Outbacker with any type of household kitchen or window cleaner.
- 3 Gently rub the sensor surface with the cloth. Slowly rotate the cloth so a clean section of the cloth is constantly exposed to the sensor surface.

4 After cleaning, gently rub the sensor again with a dry section of the cloth.

5 Thoroughly clean the cloth.

Important 1 Do NOT clean the sensor with chlorine-based cleaners, such as bleach, non-chlorine bleach, or chlorine-based bathroom or mildew cleaners. Chlorine-based cleaners will discolor the finger drive ring and can damage the circuitry.

Important 2 Do NOT clean the sensor with solvents, such as acetone, MEK, TCE, paint thinner, turpentine, and so on. Solvents can damage the enclosure surrounding the sensor and components peripheral to the sensor.

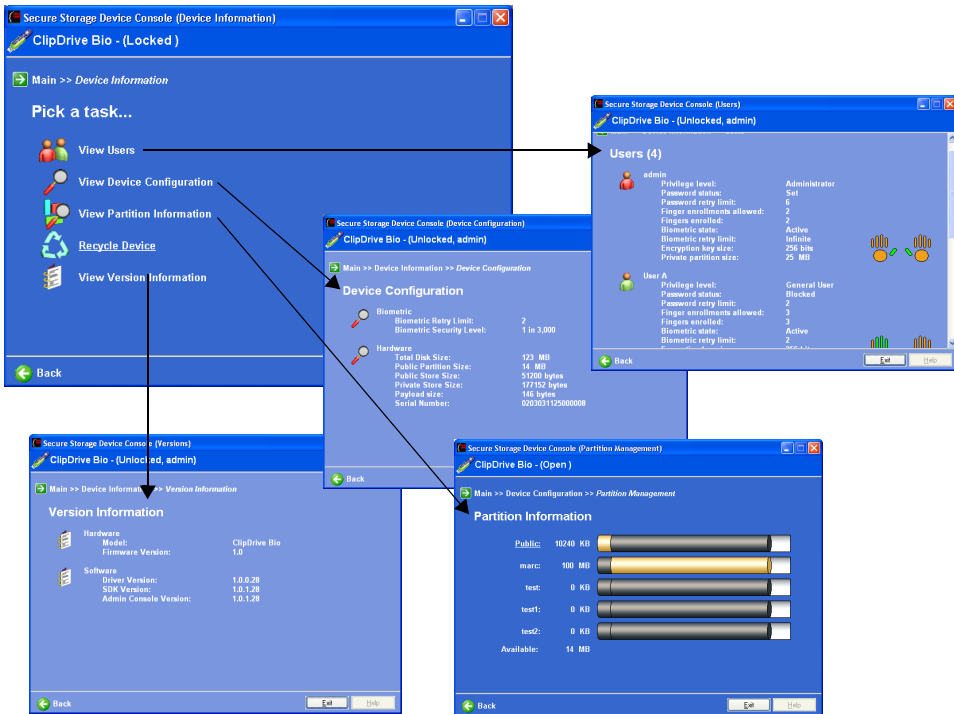
Viewing device information

Admin Console is the administrative program that lets administrators create and manage users and configure the device. You can use Admin Console to view information about other users and the device itself. Device information is read-only. You can not edit the data.

Admin Console contains four information pages:

- **User Information**—tells you how many fingerprints you can enroll, which users have administrative privileges or passwords assigned to them, and so on
- **Device Configuration**—contains biometric and hardware information such as retry limits, and partition size
- **Partition Information**—provides information about the overall allocation of disk space for partitions on ClipDrive Bio
- **Version Information**—lists the version for all software and hardware associated with ClipDrive Bio

Figure 3-1: Viewing device information



► **To view device information**

- 1 Plug ClipDrive Bio into the USB port of the computer.
- 2 From the **Start Menu**, click **All Programs, MXI, Admin Console**.
- 3 Click **View Device Information**.
- 4 Click one of the following options:
 - **View Users**
 - **View Device Configuration**
 - **View Partition Information**
 - **View Version Information**

The following table provides a more detailed description of the information available on each page.

Table 3-1: Device Information pages

Page	Description of labels
User Information	<ul style="list-style-type: none"> • Privilege level—indicates the type of user • Password Status—identifies if a password is set for the user • Password Retry Limit—number of password authentication retries allowed before the user is blocked from using a password to access the device • Finger enrollments allowed—total number of fingers a user can enroll • Fingers enrolled—total number of fingers enrolled • Biometric state—indicates whether the user has biometric access • Biometric retry limit—number of fingerprint authentication retries allowed before the user is blocked from the device • Encryption key size • Private partition size
Device Configuration	<p>Biometric</p> <ul style="list-style-type: none"> • Biometric Retry Limit—number of fingerprint authentication retries allowed before all users are blocked from the device • Biometric Security Level—increases or decreases the accuracy of the fingerprint comparison <p>Hardware—indicates the total disk size, and the size of the public partition, private and public stores, an payload. Also identifies the serial number.</p>
Partition Information	<p>Identifies the disk space allocated to the public partition and each private partition. Also indicates the total amount of available space on the device.</p>
Version Information	<p>Hardware</p> <ul style="list-style-type: none"> • Model—names the secure storage device • Firmware version—the version of the embedded software <p>Software</p> <ul style="list-style-type: none"> • Driver version • SDK version—Software Developer Kit version number • Admin Console—version of the program used to manage users and the device

Using ClipDrive Bio with Outbacker

Outbacker 1.0 works with ClipDrive Bio 4.0 software. If you install Outbacker software, installing ClipDrive Bio 4.0 updates the Outbacker software.

You can not manage both Outbacker and ClipDrive Bio at the same time. Admin Console recognizes only the first device that you plug in. To switch devices, you must remove the first device and then plug in the other.

If you need to use both Outbacker and ClipDrive Bio simultaneously, for example, you want to copy files from one device to the other, complete the following steps:

- Plug in ClipDrive Bio and unlock it
- Plug in Outbacker and unlock it using only biometric authentication

When both devices are unlocked you can copy files between devices. For example, you can copy a file from your private partition on ClipDrive Bio to your MXI Private Disk on Outbacker.

You can not unlock ClipDrive Bio if you first plug in and unlock Outbacker. However you can still use the public partition on ClipDrive Bio.

4 Troubleshooting

If you have problems using ClipDrive Bio, you may find a solution in one of the following scenarios. For technical assistance, contact support@memoryexpertsinc.com.

I can not eject my ClipDrive Bio

When you try to eject ClipDrive Bio from the file manager, you may encounter the following error:

“Cannot Unmount Volume—An error was encountered trying to unmount 'Removable Disk (F:)' Check to make sure there are no open files or windows from that volume.”

If you are not an administrator on the computer then this message will always appear and prevent you from ejecting the drive. This is a limitation documented by Microsoft in the following article:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;192785>

To work around this issue, you can lock the device using Admin Console or safely remove the device from the status area of the taskbar.

My user name is not in the list for biometric verification

If your user name is not in the list of users when you attempt to authenticate using biometric verification, then you either do not have any fingers enrolled, or your biometric access is blocked.

Contact your ClipDrive Bio administrator to unblock your biometric access or enroll fingers.

My user name is not in the list for password verification

If your user name is not in the list of users when you attempt to authenticate using password verification, then either you do not have a password, or it is blocked. Contact your ClipDrive Bio administrator to have a password set for you or to have your password unblocked.

ClipDrive Bio will not authenticate my finger

ClipDrive Bio may fail to authenticate a finger if the biometric sensor is damaged, or your fingerprint has aged or has been altered due to environmental factors or injury. If you have password privileges, you can use a password to authenticate to ClipDrive Bio to enroll a new finger. If the sensor is broken, contact your administrator or Memory Experts International.

My password access to ClipDrive Bio is blocked

If you received a warning indicating that you had only one remaining password attempt, you may have exceeded the password retry limit. When you exceed this limit, ClipDrive Bio blocks you from authenticating to the device using a password. You can still use biometric authentication if you have enrolled a fingerprint. You can also contact your administrator to unblock your user account.

The ClipDrive Bio drive does not display in the file manager window

If you map a network drive to a resource using the drive letter typically assigned to ClipDrive Bio, you will not see the ClipDrive Bio drive in the file manager window when you connect the device. This problem only occurs if you map the drive while ClipDrive Bio is disconnected from the computer. You need to disconnect the mapped network drive. To work around the mapping issue, it is recommended that you re-map the network drive using a drive letter from the end of the alphabet, for example, Z or Y. For more information about this Microsoft network drive issue, see the following Microsoft Web address:

<http://support.microsoft.com/?kbid=830238>

Index

A

- about ClipDrive Bio 5
- acetone
 - cleaning ClipDrive Bio 14
- Admin Console
 - version 17
 - viewing version of 6
- administrative privileges 6
- administrators 6
- alcohol
 - cleaning ClipDrive Bio 14
- authenticating
 - using finger 10
 - using password 10
- authentication
 - biometric 9
 - password 9

B

- biometric
 - authentication 5, 9
 - retry limit 17
 - security level 17
 - time-out 17

C

- cleaners
 - to use with ClipDrive Bio 14
- cleaning ClipDrive Bio 14

ClipDrive Bio

- about 5
- cleaning 14
- disconnecting 13
- locking 13
- opening files 13
- saving files 13
- starting 10
- version information 17
- version number 15
- viewing device information 15
- viewing version of 6
- working with 13
- contacting
 - Memory Experts International ii, 19
- copying
 - files between Outbacker and ClipDrive Bio 18

D

- device configuration
 - biometric information 17
 - hardware information 17
 - viewing 15
- device information
 - viewing 15
- devices
 - copying files 18
- disconnecting ClipDrive Bio 13
- disk space capacity 6

- drive
 - partitions 6
- driver version 17

E

- enrollment privileges 6

F

- files
 - copying between devices 18
- finger image
 - cleaning sensor 14
- fingerprint
 - authentication 9
 - cleaning sensor 14
 - maximum number of 17
- fingers
 - number of enrolled 17

G

- general users 6

H

- hands
 - user information 17
- hardware version 15

L

- LED 10
- locking ClipDrive Bio 13
- logging on to ClipDrive Bio 10

M

- mapping network drives 20
- multiple devices
 - using Outbacker with ClipDrive Bio 18

N

- network drives
 - mapping 20

O

- open state 9
- opening files 13
- operating system 6
- Outbacker
 - using with ClipDrive Bio 18

P

- partition size
 - viewing 15
- partitions 6
 - opening files 13
 - saving files 13
- password authentication 9, 10
- password retry limit 17
- password status
 - user information 17
- plugging in ClipDrive Bio 10
- privilege level
 - user information 17

R

- removing ClipDrive Bio 13
- requirements
 - system 6

S

- Safely Remove Hardware operation 13
- saving files 13
- SDK version 17
- sensor
 - cleaning 14
- software version 15
- starting ClipDrive Bio 10
- support
 - technical assistance ii
 - system requirements 6

T

- technical support ii, 19
- troubleshooting

- finger authentication failed 20
- network drive issue 20
- password access blocked 20
- unsafe removal event dialog 20

U

- unplugging ClipDrive Bio 13
- unsafe removal event dialog 20
- USB 5
- USB port
 - system requirements 6
- user database 9
- user information
 - detailed explanation of 17
 - viewing 15
- users
 - administrators 6
 - definition of 6
 - general 6
 - viewing number of 15

V

- version
 - hardware 17
 - software 17
- version information
 - viewing 6
- viewing
 - device configuration 15
 - device information 15
 - user information 15
 - version information 6, 15