



ClipDrive Bio

Administration 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 Administration Guide version 1.0

Document Number: MSW1015-M-ADM01-10

Date of Publication: November 1, 2004

Support: support@memoryexpertsinc.com

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

Contents

1: Introducing ClipDrive Bio	3
The role of the administrator	4
System requirements	4
Version information	4
Partitions and storage options	5
Security	6
Encryption keys	7
Inter-operability with Outbacker	7
Third-party software integration	8
2: Using Admin Console	9
Installing Admin Console	9
Starting Admin Console	10
Navigating Admin Console	10
3: Managing users	13
Creating users	13
Enrolling and deleting fingerprints	14
Administering passwords	16
Editing users	17
Deleting users	18
Viewing user information	18
4: Managing partitions	21
Sizing partitions	21
Viewing partition information	23
5: Configuring authentication settings	25
Setting retry limits	25
Setting the biometric security level	27

Recycling ClipDrive Bio	28
Viewing device configuration details	29
6: Troubleshooting	31
Password access is blocked	31
Biometric verification access is blocked	31
Biometric identification access is blocked	32
Password and biometric access is blocked	32

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 4 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 robust management program, lets you create and manage users and configure the device.

Figure 1-1: ClipDrive Bio



This guide outlines the tasks required to set up ClipDrive Bio with security access. For general information such as saving files to and retrieving files from ClipDrive Bio, unlocking, removing, and cleaning the device, please refer to the *ClipDrive Bio User Guide*.

This chapter provides information about the following topics:

- The role of the administrator
- System requirements
- Version information
- Partitions and other storage options
- Security

- Interoperability with Outbacker
- Third-party software integration

The role of the administrator

Whether you use ClipDrive Bio for your personal storage device or in a corporate environment with multiple users, you must configure the device to take advantage of its authentication and data encryption features. Admin Console lets you configure ClipDrive Bio by completing the following actions:

- Creating users
- Enrolling fingers (and assigning passwords if applicable)
- Setting authentication preferences
- Creating private partitions for users

System requirements

The following list describes the requirements you need to use ClipDrive Bio and to manage users.

- 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
- Admin Console program to create users and enroll fingers, and to configure private partitions

Version information

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

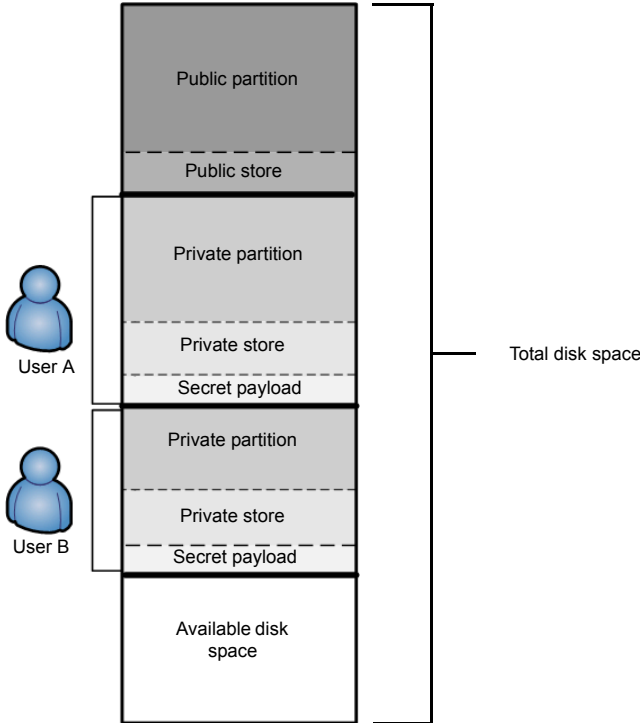
► To view version information

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

Partitions and storage options

The following illustration provides a conceptual overview of the private and public storage available with ClipDrive Bio.

Figure 1-2: Partitions and other storage areas on ClipDrive Bio



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.

For more information about partitions, see Chapter 5, “Managing partitions” on page 21.

Other storage options

ClipDrive Bio reserves some internal memory to enable programs to store information, such as passwords, PKI certificates, encryption keys and so on. You can access the following memory stores using the Secure Storage Software Developer Kit (SDK).

- **Public Store**—36,352 bytes of public memory. Data in the public store can always be read but only authenticated users with administrative privileges can write to the store.
- **Private Store**—164,352 bytes of private memory that is associated with each user (assumes the device has a maximum of 5 users). You can access data saved to a user's private store only after ClipDrive Bio successfully authenticates the user. Data saved to a private store is encrypted.
- **Secret Payloads**—146 bytes of memory that is stored with each fingerprint template. You can write data to a secret payload when you enroll a finger. However, the secret payload is released only after the device successfully authenticates the user. Secret payloads are not available with password authentication.

Note For more information about accessing these storage areas using the Secure Storage Software Developer Kit (SDK), see the *Secure Storage SDK documentation*.

Security

ClipDrive Bio provides two levels of protection:

- User authentication—by fingerprint or password—to access private data on the device
- Automatic data encryption of each user's private data

Private partitions are only visible after the user successfully authenticates to ClipDrive Bio. When a user saves data to a private partition, ClipDrive Bio encrypts the file using the FIPS-approved AES algorithm. Data is automatically decrypted when the user opens the file.

Encryption keys

ClipDrive Bio supports the following AES key sizes: 128, 192, and 256 bits. The encryption key used to encrypt data on a user's private partition or private store, is unique to the user. ClipDrive Bio generates an encryption key when you create a user.

Recovering encryption keys

In some circumstances, an organization may need access to a user's private data, for example, if the user has left the company or the user can not authenticate to the device. If a user can not authenticate, ClipDrive Bio can not access the user's encryption key. Without the encryption key, ClipDrive Bio can not decrypt the data in the user's private partition and private store.

You can only recover private encrypted data if you have a backup of the encryption key. Admin Console does NOT backup encryption keys. Once they are generated, the keys exist only on ClipDrive Bio. A key backup or key escrow system for the ClipDrive Bio can be implemented using the MXI Software Developers Kit (SDK).

Note Once you delete a user, the user's data is permanently lost even if a key recovery system exists.

For more information about implementing a key backup system, contact MXI.

Inter-operability 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.

Third-party software integration

You can integrate ClipDrive Bio with other applications using the Secure Storage SDK. In addition to its secure mass storage capabilities, you can use ClipDrive Bio for strong authentication, single sign-on, data replication, and PKI solutions.

The Secure Storage SDK provides a complete interface for the following areas:

- Device control
- Partition management
- User management
- Biometric and password enrollment and verification
- Configuration of device security
- Private store, secret payload, and public store access

2 Using Admin Console

You must install Admin Console before you can create and manage ClipDrive Bio users. Admin Console also lets you create and resize private partitions, configure authentication preferences, and view device information.

This chapter provides information about the following topics:

- Installing Admin Console
- Starting Admin Console
- Navigating the Admin Console interface

Note Admin Console is a common application for all MXI Secure Storage products. Therefore, some features may only be available for some devices.

Installing Admin Console

You need to install Admin Console on at least one computer so you can set biometric and password security access to ClipDrive Bio. Typically, general users (not administrators) do not need Admin Console to use ClipDrive Bio. However, if you grant certain privileges, such as allowing general users to enroll their fingers, they will require access to the program to complete those tasks. General users can access only limited functions using Admin Console.

System requirements

The following list describes the system requirements you need to install Admin Console:

- Microsoft® Windows 2000® Professional Service Pack (SP) 4
- Microsoft® Windows XP® Home Edition SP 1 or SP 2
- Microsoft® Windows XP® Professional SP 1 or SP 2

► To install Admin Console

- 1 Insert the ClipDrive Bio CD in the CD-ROM drive of the computer.
- 2 Locate the ClipDrive Bio drive using the file manager.
- 3 Open the Setup directory, and then double-click the file Setup.exe file.

- 4 Follow the instructions in the Install wizard.

Starting Admin Console

When you first start Admin Console, there are no users registered in the user database for ClipDrive Bio. The first person to start Admin Console, is automatically given administrative privileges to create users and enroll fingers. Once you create a user and enroll their finger (or set a password), authentication is required to access data on ClipDrive Bio.

You must complete the following tasks in Admin Console to use ClipDrive Bio with biometric or password authentication.

- Create your administrator account, enroll your finger, and set a password.
- Create user accounts for other ClipDrive Bio users and enroll their fingers (and set passwords as required).
- Set authentication preferences for ClipDrive Bio

Note For information about creating users, see “Creating users” on page 5. For information about setting authentication preferences, see Chapter 4, “Configuring authentication settings” on page 19.

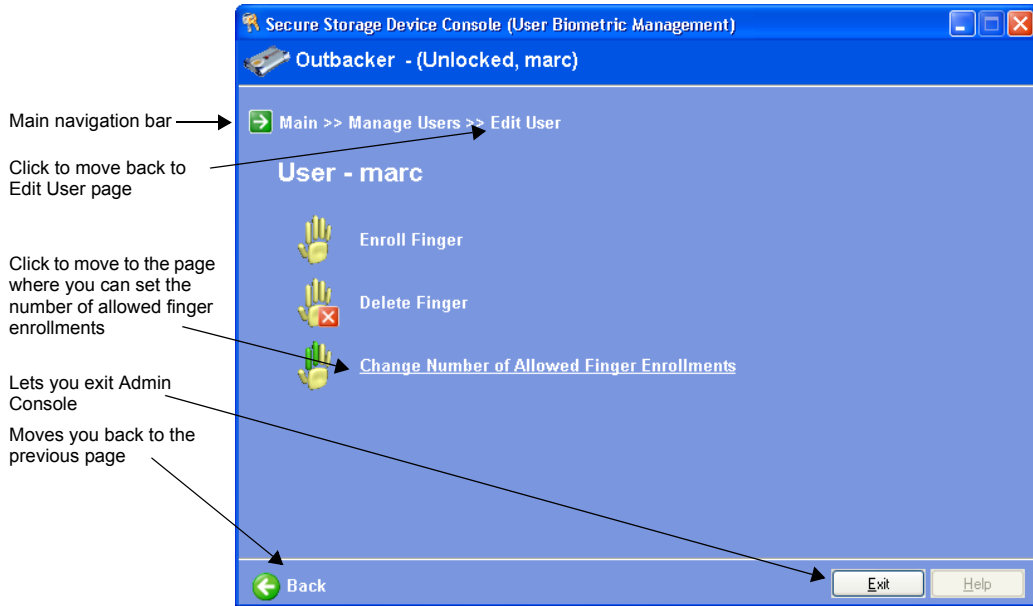
► To start Admin Console

- 1 Plug ClipDrive Bio into the USB port of the computer.
- 2 From the **Start** menu, click **All Programs**, and then click **MXI**.
- 3 Click **Admin Console**.

Navigating Admin Console

The Admin Console interface is intuitive and task based. When you click a task you move to the page that lets you perform that function. A navigation bar tells you where you are in the program in relation to the **Main** page. The navigation bar is dynamic so that when you click a title, it moves to that page. The following illustration demonstrates how to navigate within Admin Console.

Figure 2-1: Navigating Admin Console



3 Managing users

ClipDrive Bio allows you to create and manage two types of users; administrators and general users. You can set biometric and password access for each user. Providing biometric access involves enrolling one or more fingers of a user on the device. Providing password access involves setting a password for the user.

You can also view a summary of information about all ClipDrive Bio users.

This chapter provides information about the following topics:

- Creating users
- Enrolling and deleting fingerprints
- Administering passwords
- Editing users
- Viewing user information

Creating users

When you create a user, you must specify whether the user is an administrator or a general user.

- **Administrator**—a user with full privileges. 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.

You can create up to five users. After you create a user, you need to enroll a finger or set a password before the user can authenticate to ClipDrive Bio. For information about enrolling fingers, see “Enrolling and deleting fingerprints” on page 14. For information about setting passwords, see “Administering passwords” on page 16.

Note All users can start Admin Console and view device-specific information without authenticating to ClipDrive Bio.

► **To create a user**

- 1 From the **Main** menu in Admin Console, click **Manage Users**.
- 2 Click **Create User**.
- 3 Type the user name in the **User Name** text box.
A user name must contain a minimum of 1 character and a maximum of 40.
- 4 From the **Privilege Level** list, click one of the following user types:
By default, the first user you create is an administrator.
 - **General**
 - **Administrator**
- 5 Click **Create**.

Enrolling and deleting fingerprints

You must enroll a user's finger before the user can access ClipDrive Bio using biometric authentication. Fingerprint enrollments are called templates. ClipDrive Bio lets you enroll a maximum of ten fingerprint templates among all users.

Enrolling an accurate finger image increases the usability and security of the device, and reduces the probability of false identification. For best results, choose a section of the finger with clear ridge and valley patterns, typically the center of the fingertip as shown in the following illustration.

Figure 3-1: Finger placement



You can monitor finger enrollment for all users or you can let users enroll their own fingers. Users who self-enroll their fingers can access only their own fingerprint templates. You must assign a password to users who will enroll their own fingers. The password lets a user unlock ClipDrive Bio to enroll the finger. You can remove password privileges after the fingers are enrolled. For information about assigning passwords, see “Administering passwords” on page 16.

Once you set an authentication method (biometric or password) for the user, the user must first authenticate to the device before you can enroll additional fingers. Requiring the user to authenticate, ensures that an administrator can not enroll fingers in the user's enrollment set that do not belong to the user.

You can delete fingerprint templates as required. Users can also delete their own templates.

► **To enroll a finger**

- 1 From the **Manage Users** page, click the user whose finger you want to enroll.
- 2 Click **Manage Biometric**, and then click **Enroll Finger**.
- 3 Select a finger to enroll and follow the instructions on the screen.
Make sure the center of your finger is on the center of the fingerprint sensor and ensure firm contact with the sensor.

Tip You can also use the Arrow keys to select a finger to enroll. Press Spacebar to start the enrollment process.

Note Each user should enroll at least two different fingers—the default value. This ensures that a backup fingerprint is available. If you create two user accounts for the same person, you can not enroll the same finger for each account.

► **To allow users to enroll their fingers**

- 1 Assign a password for the user to use to unlock ClipDrive Bio. For information about assigning a password, see “To assign a password” on page 16.
- 2 Instruct the user to start Admin Console and follow all of the steps in the procedure, “To enroll a finger” on page 15.

► **To delete a fingerprint template**

- 1 From the **Manage Users** page, click the user whose template you want to delete.
- 2 Click **Manage Biometric**, and then click **Delete Fingerprint Template**.
- 3 Select a finger to delete.

Caution If you delete the user's last fingerprint template and no password exists for the user, you will permanently prevent the user from accessing data on the private partition and in the private store. For information about recovering data, see “Recovering encryption keys” on page 7.

Administering passwords

You can assign passwords to users so they can unlock ClipDrive Bio when biometric authentication is not possible. For example, ClipDrive Bio may fail to authenticate a fingerprint if the biometric sensor is damaged, or a user's finger ages or is altered due to environmental factors or injury.

If a user has already enrolled fingers, the user must authenticate to the device before you can set a password. Requiring the user to authenticate, ensures that an administrator can not set a password without the user knowing about it.

Admin Console allows users to unlock the device using a password, or to change or remove a password. Password authentication provides the user with the same access privileges as biometric authentication. Users with no password privileges can unlock ClipDrive Bio using only biometric authentication.

► To assign a password

- 1 From the **Manage Users** page, click the user to whom you want to assign a password.
- 2 Click **Manage Password**, and then click **Set Password**.
- 3 Type the password in the **Password** text box.

► To change a password

- 1 From the **Manage Users** page, click the user to whom you want to assign a password.
- 2 Click **Manage Password**, and then click **Change Password**.
- 3 In the **Current Password** text box, type your current password.
- 4 In the **New Password** text box, type your new password, and then type it again in the **Confirmed Password** text box.
- 5 Click **Apply**.

► To remove password privileges

- 1 From the **Manage Users** page, click the user for whom you want to assign a password.
- 2 Click **Manage Password**, and then click **Remove Password**.

Caution If you remove a password for a user who does not have biometric authentication privileges, you will permanently prevent the user from accessing data on the private partition or in the private store. For information about recovering data, see “Recovering encryption keys” on page 7.

Editing users

ClipDrive Bio lets you rename existing users. You can also edit the user privilege level. For example, you can change a general user to an administrator.

The default number of fingerprint templates per user is two. You can edit the default value for each user. For example, if you have only two users, you can allow each user to enroll up to five fingers.

Note ClipDrive Bio lets you enroll a maximum of ten fingers among all users.

► To rename a user

- 1 From the **Manage Users** page, click the user you want to rename.
- 2 Click **Rename User**.
- 3 Type a new name for the user in the **User Name** text box, and then click **Rename**.

► To edit the user privilege level

- 1 From the **Manage Users** page, click the user whose privilege level you want to change.
- 2 Click **Change User Privilege Level**.
- 3 From the **Privilege Level** list, click the appropriate level, and then click **Apply**.

► To edit the number of fingerprints

- 1 From the **Manage Users** page, click the user for whom you want to change the number of fingerprints.
- 2 Click **Manage Biometric**, and then click **Change number of allowed fingerprints**.
- 3 Type the number of fingerprints in the **Maximum Allowed Fingerprints** text box.
- 4 Click **Apply**.

Deleting users

You can delete users who no longer require access to ClipDrive Bio. When you delete a user, ClipDrive Bio automatically removes all fingerprint templates and passwords associated with the user. Data on the user's private partition becomes permanently inaccessible. The private partition becomes part of the available unallocated disk space.

► **To delete a user**

- 1 From the **Manage Users** page, click the user to delete.
- 2 Click **Delete User**.

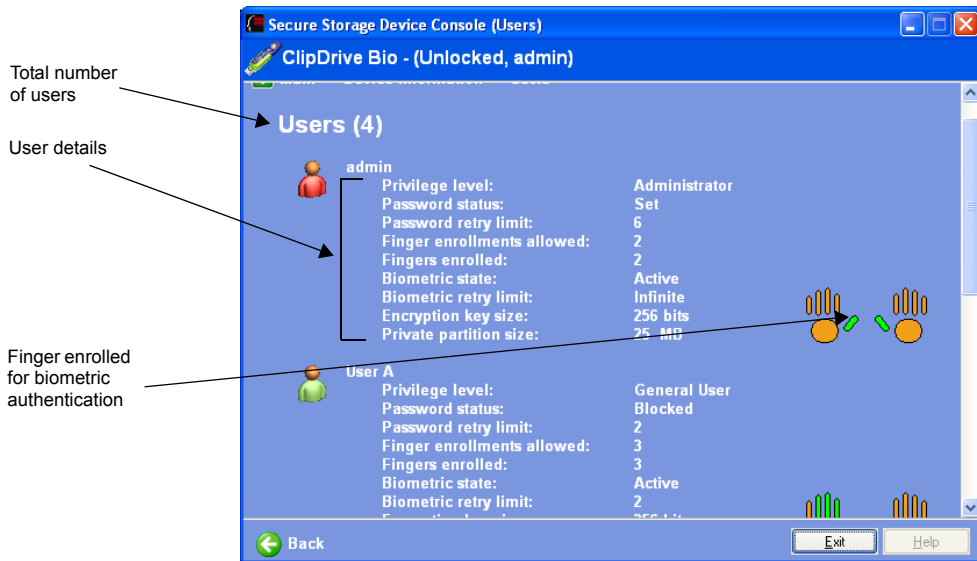
Viewing user information

You can view a summary of the settings associated with each user. Administrators can use this information to troubleshoot potential issues. For example, they can quickly determine the number of fingerprints and which fingers are enrolled for each user.

General users can view this information to find out how many fingers they can enroll and which users have administrative privileges.

The following illustration identifies key information on the User Information page.

Figure 3-2: User Information screen



► To view user information

- 1 From the **Main** page, click **View Device Information**.
- 2 Click **View Users**.

Note Users can also view device information, such as version numbers, capacity, and security settings, using Admin Console without authenticating to ClipDrive Bio.

4 Managing partitions

ClipDrive Bio lets you use both public and private partitions to save your data. ClipDrive Bio contains one public partition that all users can access without authenticating to the device.

When you create users, Admin Console automatically adds a private partition for each user on ClipDrive Bio. A user can access a private partition only after successfully authenticating to ClipDrive Bio.

You can re-size partitions. ClipDrive Bio provides a summary of partition details in Admin Console.

This chapter provides information about the following topics:

- Sizing partitions
- Viewing partition information

Sizing partitions

Re-sizing an existing partition always requires a format operation. Formatting a partition destroys all data on the partition. It is strongly recommended that you size the partitions correctly before you give ClipDrive Bio to users. Re-sizing partitions later requires you to back up user data first.

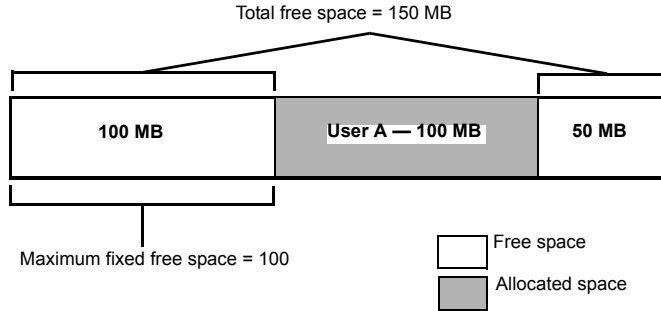
ClipDrive Bio provides information about disk space distribution to help you determine the amount of free space available when re-sizing partitions. If necessary, ClipDrive Bio can automatically move a partition to create adequate disk space for other partitions. Moving a partition does not require re-formatting, but can take time depending on the partition size.

ClipDrive Bio reports two types of free space:

- **Total free space**—the sum of all available unallocated space, regardless of how the space is organized. It may not be contiguous.
- **Maximum fixed free space**—the largest contiguous section of free space available.

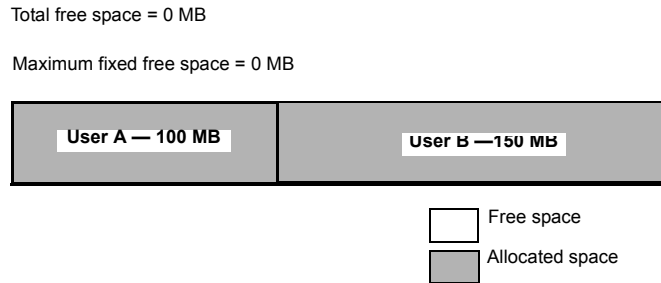
For example, say ClipDrive Bio contains the following disk space distribution: 100 MB of contiguous free space, followed by a partition of 100 MB for User A, followed by 50 MB of contiguous free space. ClipDrive Bio will report 150 MB of Total free space and 100 MB of Maximum fixed free space (see Figure 4-1).

Figure 4-1: Sample disk space distribution



If you want to add a new user—User B—with a private partition size of 100 MB or less, the new partition will fit in the Maximum fixed free space. ClipDrive Bio can quickly create a partition of this size because it does not have to move data. However, if the new partition size is larger than 100 MB—for example, 150 MB—ClipDrive Bio must move User A's partition to create adequate partition space for User B (see Figure 4-2).

Figure 4-2: Re-sized disk space



► **To size a partition**

- 1 From the **Main** menu in Admin Console, click **Configure Device**.
- 2 Click **Manage Partitions**, and then click the user whose private partition size you want to set.
- 3 Type the size of the private partition in the **Partition size** text box.

4 Click a unit of measurement from the list box, for example KB, or megabyte (MB).

5 Click **Apply**.

Note 1 Admin Console informs you prior to confirming a partition re-sizing operation if ClipDrive Bio will be moving data. Moving data can take some time.

Note 2 If you change a partition size you must format it before you can use the partition.

► To format a partition

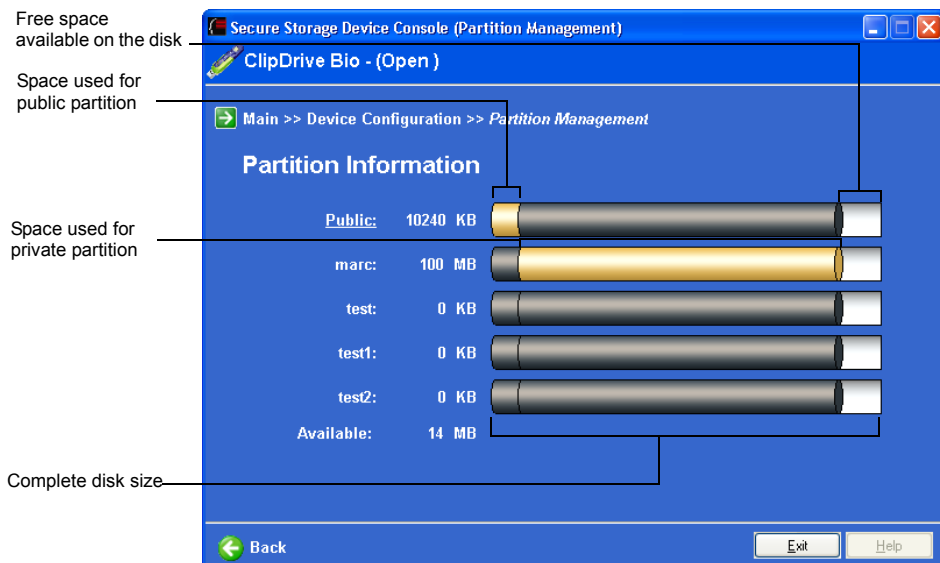
1 Open the file manager and right-click the partition.

2 Click **Format**, and then complete the appropriate options.

Viewing partition information

Admin Console provides information about the overall allocation of disk space for existing partitions on ClipDrive Bio.

Figure 4-3: Partition layout



► **To view partition information**

- 1 From the **Main** menu in Admin Console, click **View Device Information**.
- 2 Click **View Partition Information**.

5 Configuring authentication settings

You can configure biometric and password authentication settings to control the security of ClipDrive Bio.

There are two types of biometric authentication: identification and verification. By default, ClipDrive Bio uses biometric identification to authenticate users. With biometric identification, ClipDrive Bio compares a user's finger to all fingerprint enrollments. ClipDrive Bio can identify the user only after a fingerprint match is found.

With biometric verification, the user identifies himself—by selecting his name from a list—before presenting a finger for authentication. ClipDrive Bio then compares the user's finger to only his fingerprint enrollments. Typically biometric verification is used when access to ClipDrive Bio using biometric identification is blocked.

This chapter contains information about the following topics:

- Setting the retry limits for accessing ClipDrive Bio
- Setting the biometric security level
- Viewing device configuration settings

Setting retry limits

A retry limit is the number of failed authentication attempts allowed before the user is blocked from unlocking ClipDrive Bio. For example, a retry limit of one will block a user after two failed attempts.

The biometric identification retry limit applies to all users. For biometric verification and password, you set individual retry limits for each user. When a user exceeds a retry limit while trying to authenticate to ClipDrive Bio, the following action occurs:

Authentication type	Action
Biometric Identification	All users are automatically blocked from accessing ClipDrive Bio using biometric identification—password authentication and biometric verification are still available.
Biometric Verification	Only the user who attempted biometric verification is blocked from using this method to access ClipDrive Bio. Password authentication is still available. Biometric identification and verification are still available for other users.
Password	Only the user whose password is blocked is prevented from using a password to unlock the ClipDrive Bio. The user can still use biometric authentication if he has fingers enrolled and ClipDrive Bio is not blocked.

Retry limits for both biometric and password authentication can range from 1 to 254, or infinite. For information about unblocking users when the retry limit is reached, see “Troubleshooting” on page 31.

Note It is recommended that you set a very high, if not infinite, biometric retry limit to minimize the chances of blocking access to the device by all users.

► **To set the biometric identification retry limit**

- 1 From the **Main** page in Admin Console, click **Configure Device**.
- 2 Click **Biometric Identification Retry Limit**.
- 3 If you want to set a value other than infinite, clear the **Infinite** check box, and then type the number for the retry limit in the **Biometric Retry Limit** text box.
- 4 Click **Apply**.

► **To set the biometric verification retry limit**

- 1 From the **Manage Users** page, click the user for whom you want to set the retry limit.
- 2 Click **Manage Biometric**, and then click **Change Biometric Verification Retry Limit**.

- 3 Type the number for the retry limit in the **Biometric Verification Retry Limit** box.

- 4 Click **Apply**.

► **To set the password retry limit**

- 1 From the **Manage Users** page, click the user for whom you want to set the retry limit.

- 2 Click **Manage Password**, and then click **Change Password Retry Limit**.

- 3 Type the number for the retry limit in the **Password Retry Limit** text box.

- 4 Click **Apply**.

Note When a user is about to exceed the password retry limit, a **Warning** dialog box appears to inform the user that only one password attempt remains.

Setting the biometric security level

Biometric authentication compares the finger placed on the sensor to all fingerprint templates stored on the device. The biometric security level is the strength of fingerprint authentication used by ClipDrive Bio. The probability that two different fingers are incorrectly matched is called the False Match Rate (FMR). The biometric security level is expressed as an FMR probability, such as “1 in 10,000”.

A low FMR means higher security because the device requires a closer match between two fingerprints. Therefore, “1 in 10,000” is more secure than “1 in 1,000”. However, a low FMR also means that the device may reject a genuine user because the sensor is less tolerant of small fingerprint deviations due to dirt, improper placement of the finger, and so on. Conversely, a high FMR means the device is less likely to reject a genuine user but more likely to incorrectly match two different fingerprints.

If some users have difficulty authenticating to the device at the desired level of security, it is recommended that you also assign them a password. The biometric security level you set applies to all users.

► **To set the biometric security level**

- 1 From the **Main** page of Admin Console, click **Configure Device**.

- 2 Click **Biometric Security Level**.

- 3 In the **Biometric Security Level** list, click the appropriate security level. The default is set to “1 in 55,000”.
- 4 Click **Apply**.

Recycling ClipDrive Bio

ClipDrive Bio enforces the authentication policies set up by administrators. It is very important that you—an administrator—can always access ClipDrive Bio to reconfigure the device, change security policies, or manage users.

If you lose access to ClipDrive Bio (for example, if your biometric and password access are blocked) then you can no longer manage the device. However, you can re-use the hardware by recycling ClipDrive Bio.

Recycling ClipDrive Bio leaves the device in an open state, ready for administration. The recycle operation deletes all user information, private stores, partition information, encryption keys, and authentication data from ClipDrive Bio. Encrypted data on partitions is unrecoverable.

You can control who can recycle the device using a recycle code. Setting the recycle code is optional. You can recycle ClipDrive Bio only after entering the correct code. You must set the code when the device is in the open state—that is, when no authentication is required to access the device. By default, there is no recycle code set for ClipDrive Bio.

► To set a recycle code

- 1 From the **Main** page of Admin Console, click **Configure Device**.
- 2 Click **Set Recycle Code**.
- 3 In the **Recycle Code** box, type the recycle code, and then click **Apply**.

There are no restrictions on the length or composition of the code.

Note When you set a recycle code make sure that you can remember it or record the code and keep it in a safe place for future reference.

► To recycle ClipDrive Bio

- 1 From the **Main** page of Admin Console, click **View Device Information**.
- 2 Click **Recycle Device**.
- 3 In the **Recycle code** box, type the recycle code, and then click **Recycle**.

Viewing device configuration details

Device configuration details include biometric and hardware information. The following table outlines the information on this page.

Section	Contains the following details
Biometric	<ul style="list-style-type: none">• Retry limit• Security level
Hardware	<ul style="list-style-type: none">• Total disk size• Public partition size• Public store size• Private store size• Payload size• Serial number

► **To view device configuration details**

- 1** From the **Main** page, click **View Device Information**.
- 2** Click **View Device Configuration**.

6 Troubleshooting

When a user exceeds the number of retries—called the retry limit—allowed for password authentication or for biometric verification, ClipDrive Bio prevents the user from authenticating to the device. When a user exceeds the retry limit for biometric identification, ClipDrive Bio blocks biometric identification access for all users.

Note For information about setting the biometric or password retry limits, see “Setting retry limits” on page 25.

This chapter provides information about the following topics:

- Unblocking password access
- Unblocking biometric verification
- Unblocking biometric identification

Password access is blocked

When a user enters a name and password, the device can identify the user by the user name. If the user exceeds the password retry limit, then ClipDrive Bio blocks only the user who is trying to authenticate.

► To unblock password access

- 1 From the **Manage Users** page, click the user who is currently blocked from the device.
- 2 Click **Manage Password**.
- 3 Click **Unblock User Password**, and then click **Apply**.

Biometric verification access is blocked

When a user exceeds the biometric verification retry limit, only the user who is trying to authenticate is blocked from accessing ClipDrive Bio using biometric verification. For more information about biometric verification, see page 25.

► **To unblock biometric verification access**

- 1 From the **Manage Users** page, click the user who is currently blocked from the device.
- 2 Click **Manage Biometric**.
- 3 Click **Unblock User Biometric Verification**, and then click **Apply**.

Biometric identification access is blocked

When a user places a finger on the fingerprint sensor, ClipDrive Bio captures the finger image and attempts to identify the user. If the user exceeds the biometric identification retry limit, ClipDrive Bio becomes blocked and all users are prevented from unlocking it using biometric identification. For more information about biometric identification, see page 25.

Note It is strongly recommended that you set password privileges for an administrator to prevent the device from becoming completely blocked—where neither biometric or password authentication is available. If a complete blockage occurs, contact Memory Experts International.

► **To unblock biometric identification access**

- 1 Start Admin Console and log on to ClipDrive Bio using your password—you must be an administrator to unlock a blocked device.
- 2 Click **Unblock Device**, and then click **Apply**.

Tip Users with password privileges can also authenticate to ClipDrive Bio using their password if the device is blocked.

Password and biometric access is blocked

You can no longer manage ClipDrive Bio because you can not access the device as an administrator using a biometric or a password. Furthermore, there are no other administrators who can access the device to unblock your access. If you want to manage this device again, your only option is to recycle it.

For more information about recycling ClipDrive Bio, see “Recycling ClipDrive Bio” on page 28.

Index

A

- about
 - Admin Console 9
 - ClipDrive Bio 3
- Admin Console
 - about 9
 - installing 9
 - navigating 10
 - starting 10
 - system requirements 4
 - viewing version of 4
- administrator
 - creating users 13
 - the role of 4
- assigning
 - passwords 16
- authentication
 - security of 6
 - setting security level 27
 - using biometric identification 26
 - using biometric verification 26
 - using password 26
- authentication attempts
 - exceeding 31

B

- biometric
 - identification 26
 - verification 26
- biometric authentication

- enrolling fingers 14
- biometric identification
 - exceeding retry limit 32
 - unblocking access 32
- biometric retry limit 25
- biometric security level
 - setting 27
- biometric verification
 - exceeding retry limit 31
- blocked
 - password and biometric access 32

C

- capturing fingerprints 14
- changing
 - passwords 16
 - user privilege level 17
- ClipDrive Bio
 - about 3
 - managing users 13
 - system requirements 4
 - unblocking 31
 - viewing device details 29
 - viewing version of 4
- contacting
 - Memory Experts International ii
- copying
 - files between devices 7
- creating users 13

D

- deleting
 - fingerprints 14
 - passwords 16
 - users 18
- device configuration
 - viewing 29
- devices
 - copying files 7
- disk space
 - capacity 5
 - private and public stores 6

E

- editing
 - number of fingerprints 17
 - passwords 16
 - user privilege level 17
 - users 17
- enrolling fingers 14
- enrollment privileges 13

F

- files
 - copying between devices 7
- fingerprint
 - deleting 14
 - editing the number of 17
 - enrolling 14
 - maximum number of templates 14
 - security 6
 - setting retry limit 26
- fingers
 - enrolling 14

G

- general users
 - creating 13

I

- identification

- using biometric 26

M

- managing users 13
- multiple devices
 - using Outbacker with ClipDrive Bio 7

N

- navigating
 - Admin Console 10

O

- opening
 - Admin Console 10
- Outbacker
 - using with ClipDrive Bio 7

P

- partitions 5
- password retry limit
 - exceeding 31
 - setting 25
- passwords
 - assigning 16
 - changing 16
 - removing 16
 - setting retry limits 26
- private disk space 5
 - private store 6
 - public store 6
 - secret payload 6
- private store 6
 - description of 6
- public store
 - description of 6

R

- recycle code
 - setting 28
- recycling ClipDrive Bio 28
- removing

- passwords 16
- users 18
- renaming users 17
- retry limit
 - biometric identification 32
 - biometric verification 31
 - password 31
- retry limits
 - setting 25

S

- secret payload 6
- security
 - fingerprint authentication 6
 - setting biometric security level 27
- setting
 - biometric security level 27
 - passwords 16
 - retry limits 25
- starting
 - Admin Console 10
- support
 - technical assistance ii
- system requirements
 - Admin Console 4
 - ClipDrive Bio 4

T

- technical support ii
- templates
 - deleting fingerprints 14
 - enrolling fingerprints 14
- troubleshooting
 - password and biometric access blocked 32

U

- unblocking
 - biometric identification access 32
 - biometric verification access 31
- unblocking ClipDrive Bio 31

- user information
 - viewing 18
- users
 - administrators 13
 - creating 13
 - definition of 13
 - deleting 18
 - editing 17
 - general 13
 - managing 13
 - renaming 17
 - viewing information about 18

V

- verification
 - using biometric 26
- version information
 - viewing 4
- viewing
 - device configuration information 29
 - user information 18
 - version information 4