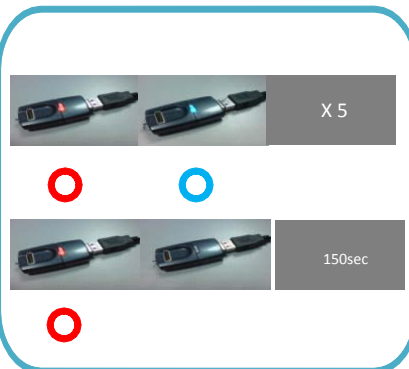


## iDEA Matrix Device Status

### Device Status - 1

#### Device with no finger print (Factory Mode)

- Connect the to USB
- Alternative **BLUE** & **RED** light blinking X 5
- Follow by blinking **RED** light



This light sequence indicate that there is no finger print store in the device

### Device Status - 2

#### Device with Admin Finger print

- Connect to USB
- Steady **RED** & **BLUE** light for 1 second
- Follow by blinking **RED** light



This light sequence indicates that 2 Admin Finger have already enrolled, **RED** light blinking waiting for another 4 user finger to enroll.

### Device Status - 3

#### Device Enroll standby

- Connect to USB
- Blinking **RED** light



This light sequence indicate that device is waiting for finger to enroll

### Device Status - 4

#### Device Authenticate Standby

- Connect to USB
- Blinking **BLUE** Light



This light sequence indicate that device is waiting for finger for authenticate or finger erase depend on switch is up for authenticate, or switch down for finger erase.

### Device Introduction

#### Device Intro



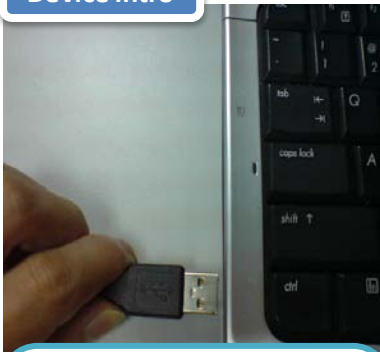
iDEA Matrix Unit

#### Device Intro - 2



USB Cable

#### Device Intro



Connect the male connector of the USB cable to PC

#### Device Intro - 4



Connect the female connector of the USB cable to iDEA Matrix Unit

## Device Intro



iDEA Matrix will send to user in factory mode , user can check the this device status according to the light sequence by steps below :

- Connect the to USB
- Alternative **BLUE** & **RED** light blinking X 5
- Follow by blinking **RED** light

**Note :** If user receive iDEA Matrix is not in factory mode , please contact your distributor

## Biometric Sensor - Enrollment Mode

### Enrollement - 1



Connect device to USB, **BLUE** and **RED** light flash alternately and followed by the **RED** light blinking

## Enrollement - 2



**RED** light blinking waiting for finger enrollment

**Note :** the available time for user to complete 6 finger enrollment is 150 seconds , device will shut down if enrollment process cannot be complete within 150 seconds time limit

## Enrollement - 3



Swipe finger as the arrow direction shown

First 2 finger enroll will be Admin Finger, the rest 4 finger enroll will be User Finger, all 6 finger must be enroll before device can be used

**Note:** if disconnect device after 2 Admin Finger is enrolled, device need only enroll for 4 User Finger for next time



Successful enrollment will denote a short **BLUE** light



Unsuccessful enrollment will denote a short **RED** light

**Note:** 3 times unsuccessful enroll will cause device auto shut down, it need to plug out and plug in to USB again to continue the enrollment

#### Enrollement - 4



After successful enrollment for all 6 fingers, the device will connect to PC and ready to be used

**Note:**  
Please refer to Disk Manager Software after successful enrollment

### Biometric Sensor - Authentication Mode (Normal Mode)

#### Authentication - 1



Switch the slide switch to the up position.

#### Authentication - 2



Connect the device to USB; blinking **BLUE** light indicates that the device is waiting for an enrolled finger for authentication

**Note:** the available time for user to complete 1 finger authentication is 60 seconds, device will shut down if authenticate process cannot be complete within 60 seconds time limit

### Authentication - 3



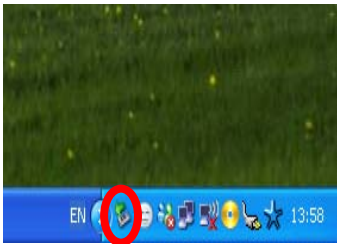
Begin the authentication process by swiping any enrolled finger on the sensor as the direction show

Successful authenticate would denote a short **BLUE** light

Unsuccessful authentication would denote a short **RED** light

**Note: 3 times unsuccessful authenticate will cause device auto shut down, it need to plug out and plug in to USB again to continue the authenticate**

### Authentication - 4



After successful authenticate, the device will connect to PC and ready to be used

**Note: Please refer to Disk Manager Software after successful authenticate**

## Biometric Sensor - Finger Erase Mode

### Finger Erase - 1



Switch the slide switch to the down position

### Finger Erase - 2



Connect the device to USB; blinking **BLUE** light indicates that the device is waiting for an enrolled finger for authentication

**Note: the available time for user to complete 1 Admin Finger erase is 60 seconds, device will shut down if finger erase process cannot be complete within 60 seconds time limit**

### Finger Erase - 3



Connect device to USB , blinking **BLUE** light indicates that the device is waiting for any Admin Finger , swipe either one of the Admin Finger on the sensor to erase all 6 finger store in the device



The **BLUE** and **RED** light will blink alternately and followed by the **RED** light blinking. This indicates that the device is reset to factory mode; all fingerprints stored in the device are being removed

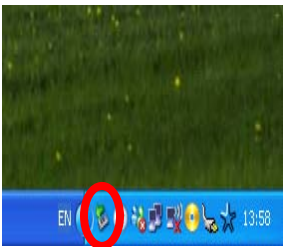


Unsuccessful detect an Admin Fingerprint after swipe would denote a short **RED** light

**Note: 3 times unsuccessful detect Admin Fingerprint will cause device auto shut down, it need to plug out and plug in to USB again to continue the Finger Erase.**

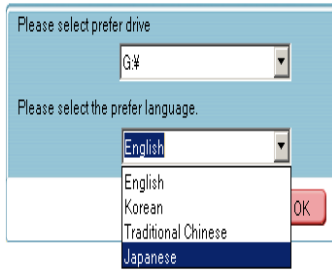
## Disk Manager Software - Introduction

### Disk Manager Intro - 1



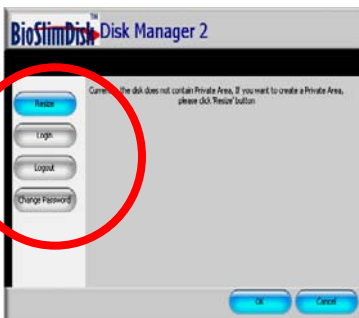
After Enrollment or Authenticate process is complete, device will connected to PC

## Disk Manager Intro - 2



**Language selection for Disk Manager Software will pop up after device connected to PC**

## Disk Manager Intro - 3



**After the language selection, Disk Manager User Interface will pop up, there are total 4 functions can be used**

- Resize
- Login
- Logout
- Change Password

**Click on the cancel button will to close the Disk Manager interface**

## Disk Manager Intro - 4



**Disk Manager Interface can also be opened from the right bottom taskbar Disk Manager Icon**

## Disk Manager Intro - 5

USB\_Drive (G:)

PRIVACYZONE (G:)

Flash Memory drive will change it's name for Public Area drive to USB\_Drive and for Private Area drive to PRIVACYZONE after Resize function

Public Area - Protect by Fingerprint sensor, no need Disk Manager to activate

Private Area - Protect by Fingerprint sensor and AES 256 encryption, need Disk Manager Software to activate

## Disk Manager Software - Resize Function

### Resize - 1



'Resize' function is used to partition flash memory into desired section

### Resize - 2



Click on the 'Resize' button to choose any 1 of 3 options to change

- One Disk (Only Public Area)
- One Disk (1 Public Area + 1 Private Area)
- Two Disk (2 Public Areas + 1 Private Area)

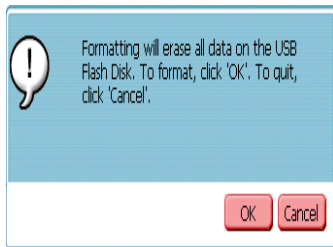
After choose 1 of the option click 'OK' button

### Resize - 3



For choosing One Disk ( 1 Public Area + 1 Private Area ) or Two Disk ( 2 Public Area + 1 Private Area ), User will require changing the flash memory space by drag the cursor left or right, after change the flash memory to user desired space, click 'OK' button to continue

### Resize - 4



A message will pop up to indicate that all data will be erasing during partition process, click 'OK' button to continue

**Note: User must backup data store in flash memory earlier to prevent data lost during memory partition**

### Resize - 5



After resize flash memory device must be restart to take effect, plug out the device from USB and connect again to continue

**Note: Device will work abnormal without restart after resize**

## Disk Manager Software - Login Function

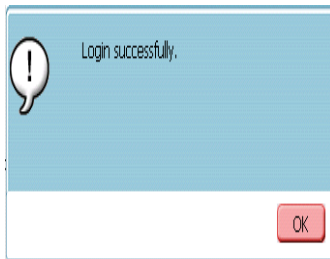
### Login - 1



'Login' function is used to login to Private Area from Public Area. Open the Disk Manager interface and click on the 'Login' button, type the password in the password field and click 'OK' button to login to Private Area.

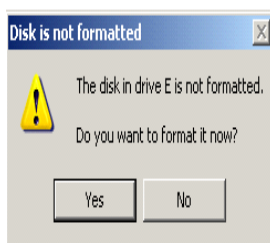
**Note: This function only available for flash memory has the Private Area partition**

### Login - 2



Successful password authenticate will pop up a message indicate user login to Private Area is success, Click 'OK' button to continue

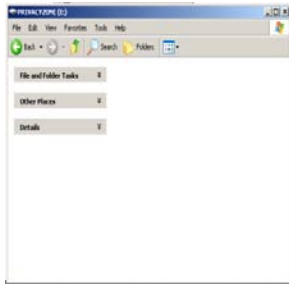
### Login - 3



For first time login to Private Area, it will request user to format the Private Area Memory,

Click 'Yes' to continue

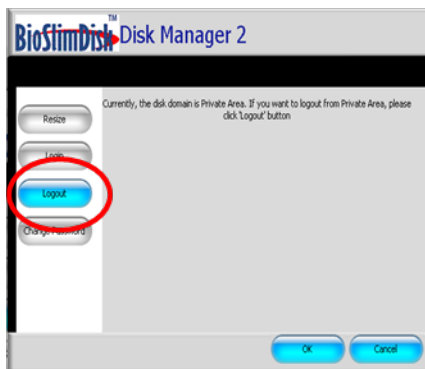
#### Login - 4



After format the Private Area, the Private Area is now ready to be used.

#### Logout - 1

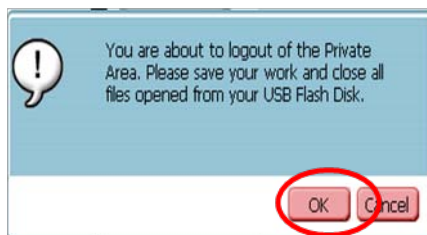
### Disk Manager Software - Logout Function



'Logout' function is used to logout from Private Area to Public Area

Open the Disk Manager interface and click on the 'Logout' button

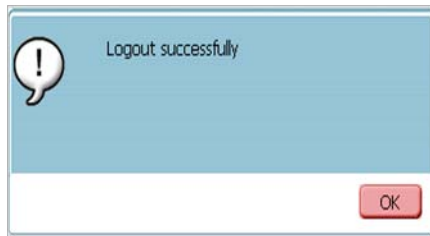
#### Logout - 2



A pop up message indicate user will logout from Private Area to Public Area , user must save data which save or open from the Private Area , click 'OK' to continue

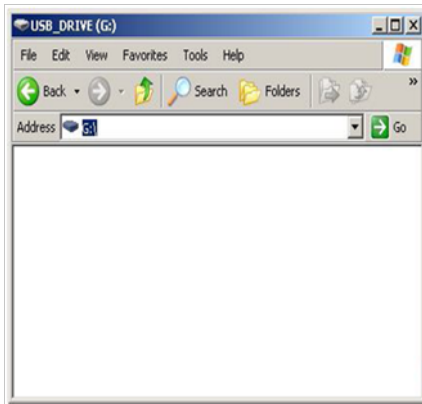
**Note : User must save all your data which save to or open from Private Area before logout or data might be lost**

### Logout - 3



A message will show that already logout from Private Area , click 'OK' to continue

### Logout - 4



Public Area is now ready to be used

## Disk Manager Software - Change Password Function

### Password - 1



'Change Password' function is used to change current password to new password

Open the Disk Manager interface and click on the 'Change Password' button

Note : Password here refer to User Administer Security Key is passed to the end administrator or user by keying in special password by themselves for the Private Area

## Password - 2

BioStimDisk™ Disk Manager 2  
Change Password

Reset  
Login  
Logout  
Change Password

Old Password:   
New Password:   
Confirm Password:   
Hint:

OK Cancel

**Fill in the 'Old Password' , 'New Password' and 'Confirm New Password' field accordingly , all those 3 field cannot be blank**

**The 'Hint' field is used to key in some words that help user to recall the password , this field can be blank , click 'OK' after fill in the require field**