imation

DEFENDER
COLLECTION

ACCESS STANDARD™

User Guide

Copyright 2011 Imation Corp.

Imation, the Imation logo, Defender and the Defender Collection logo are trademarks of Imation Corp. ACCESS Standard is a trademark of MXI Security. All other trademarks are the property of their respective owners.

Imation Enterprises Corp.
1 Imation Way
Oakdale, MN 55128-3414 USA

www.imation.com

Support: http://www.Imation.com/support

CONTENTS

Introducing ACCESS Standard 4
About Imation Defender Collection Devices 4
Security 5
System requirements 6

Getting started 7
Starting ACCESS Standard 7
Personalizing a device 8
  1. Choosing and applying a device profile 8
  2. Creating the Administrator account 9
  3. Creating the first user 9
LED states 10

Accessing data on the device 11
Logging into and out of the device 11
Saving and opening files 12
Disconnecting the device 12

Managing users 13
Types of users 13
Creating a user 13
Deleting a user 14
Managing authentication methods 14
Rescuing a user 14
Viewing user information 15

Managing devices 16
Selecting a language 16
Viewing device information 16
Recycling a device 16

Protecting the device from viruses 18
Scanning the device and host computer 18
Updating the virus database 18
Logging ACCESS Antivirus Scanner events 19

Troubleshooting 20
I cannot eject my device 20
My biometric device will not authenticate my finger 20
Password or biometric access to my device is blocked 20
My device Drive Mappings do not appear 20
Data saved to the Application partition is not available 21

Device Policy Settings Appendix 22
  Password policies 24

Index 26

INTRODUCING ACCESS STANDARD

Imation Defender Collection Devices are USB (Universal Serial Bus) devices that provide secure portable storage. You can personalize and manage a device using Imation Defender ACCESS Standard™ software. ACCESS Standard provides step-by-step instructions to help you set up your device and start using it.

For large deployments of Imation Defender Collection Devices, use ACCESS Enterprise™—a scalable management solution that lets you control devices throughout their life cycle, from personalization through to delivery to end users and optional recycling and reuse by new users. For more information about ACCESS Enterprise, contact Imation.

This chapter provides information about the following:

- About Imation Defender Collection Devices
- Security
- System requirements

ABOUT IMATION DEFENDER COLLECTION DEVICES

The following table provides a brief description about each device. ACCESS Standard supports all listed devices.

Table 1: Imation Defender Collection Devices

Device image	Name	Description
	Defender™ F200 +BIO	• Biometric, password, and two-factor security • Built-in ACCESS Standard software (no installation required) • Private and application disk partitions
	Defender™ F100	• Password security • Built-in ACCESS Standard software (no installation required) • Private and application disk partitions

Table 1: Imation Defender Collection Devices

Device image	Name	Description
	Defender™ F150	• Password security • Built-in ACCESS Standard software (no installation required) • Private and application disk partitions
	Defender™ H100	• Built-in ACCESS Standard software (no installation required) • Private and application disk partitions • Ultra-high storage capacity
	Defender™ H200 +BIO	• Biometric, password, and two-factor security • Built-in ACCESS Standard software (no installation required) • Private and application disk partitions • Ultra-high storage capacity

Disk partitions

Your computer recognizes each device partition as a separate drive.

- Private partition—Stores private data for users. Users each have their own private partition that they can access after they log into the device. For more information, see “Saving and opening files” on page 12.
- Application partition—Contains preinstalled applications, such as ACCESS Standard. You cannot save data to or delete data from this partition.

SECURITY

Security options vary according to which Imation evice you are using. In general, the two main forms of security for each device are:

1 ***Access to the device***—controlled by the authentication mechanisms available to the device, including biometric (fingerprint), password, and two-factor. Two-factor authentication requires both a biometric and a password to unlock a device. Using only biometric authentication is not considered a FIPS-approved mode of operation.

2. ***Protection of private data***—provided by encrypting the information belonging to each user in his private partition.

Imation Defender Collection Devices encrypt private partition data using the AES algorithm (FIPS PUB 197) with a 256-bit key. Data is automatically encrypted or decrypted as it is transferred to or from the device. Encryption keys are unique to each user and are generated on-board the device each time you create a user.

SYSTEM REQUIREMENTS

The following list describes the requirements to use your device with ACCESS Standard. Devices include a pre-installed version of ACCESS Standard on the application partition.

- A USB port (Type A)
- An operating system that supports USB 2.0 or 1.1 Mass Storage Devices

Operating systems

- Microsoft Windows 7
- Windows XP Pro SP2
- Windows XP Pro SP3
- Windows XP Home SP3
- Windows Vista (Home, Business and Enterprise editions SP2)
- Mac OS X 10.5 and 10.6

GETTING STARTED

ACCESS Standard is an application that lets you personalize a new or recycled device. You can also use ACCESS Standard to manage users and the device. You must personalize a new or recycled device the first time you use it.

You can use the light emitting diodes (LEDs) on the device to identify the current state of the device. For example, a solid green light indicates either that the device needs to be personalized or that a user is currently logged into the device.

This chapter provides information about the following topics:

- Starting ACCESS Standard
- Personalizing a device
- LED states

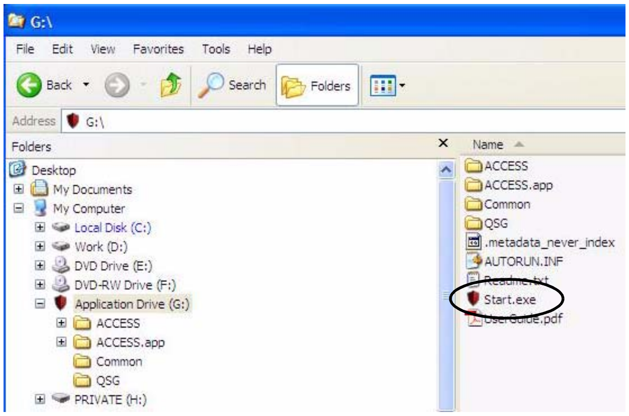
STARTING ACCESS STANDARD

ACCESS Standard starts automatically when you plug in a new or recycled device. If autorun is not configured for your computer, you can start ACCESS Standard from the application drive on the device.

To start ACCESS Standard

1. If the device is new or recycled, plug the device into the USB port of the computer. ACCESS Standard should start automatically.

   If Autorun does not automatically start ACCESS Standard, double-click the **Start.exe** file from the root directory on the application partition. (If necessary, in the notification area at the far right of the taskbar, click the Imation Defender icon, and then click **Personalize Device** from the menu.)


G:\
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
Address
G:\
Folders
Desktop
My Documents
My Computer
Local Disk (C:)
Work (D:)
DVD Drive (E:)
DVD-RW Drive (F:)
Application Drive (G:)
ACCESS
ACCESS.app
Common
QSG
PRIVATE (H:)
Name
ACCESS
ACCESS.app
Common
QSG
.metadata_never_index
AUTORUN.INF
Readme.txt
Start.exe
UserGuide.pdf

2. Follow the steps in the procedure “To personalize a device” on page 8.
3. If the device has already been personalized, you can start ACCESS Standard by clicking the Defender icon—in the notification area at the far right of the taskbar—and then choosing from the menu.

Note: If you are using a computer running Mac OS X, open a file manager and click the application drive for the device. Double-click the ACCESS Standard application.

PERSONALIZING A DEVICE

The device personalization process involves three main steps—applying a device profile, creating the Administrator account, and creating users.

To personalize a device

1. Start ACCESS Standard (see “Starting ACCESS Standard” on page 7).
2. On the **Device Personalization** page, click one of the device profile options.
3. Complete the instructions on the pages that follow to set the Administrator password (if applicable) and create a user.

Note: After you successfully complete the personalization process, you can access your private partition using a file manager. For more information about logging in and saving files to or opening files from the private partition, see “Accessing data on the device” on page 11. If you do not complete the full personalization process you may have to repeat some steps the next time you connect the device.

1. Choosing and applying a device profile

Device profiles determine the type of authentication method to use, for example biometric, password, or two-factor, and other device policies, such as number of users, password length, biometric and password retry limits and so on. When you apply a device profile, you can choose from two options: Typical and Custom.

Typical

The Typical option uses only password authentication for Defender H100, Defender™ F100, and Defender™ F150, and password OR biometric authentication for Defender™ F200 +BIO and Defender™ H200 +BIO. Only one user is allowed on the device (not including the administrator account). The Typical option applies the following default authentication settings (if applicable):

- Private partition uses the total available disk space
- Two Factor authentication: Off
- Biometric Security Level: 1 in 4,500
- Minimum password length: 6
- Password Retry Limit: 10
- Password Re-use Threshold: 3
- User Rescue: Enabled
- Data Destruction: Off
- Administrator Account: Enabled
- Biometric Retry Limit: Infinite

Custom

The Custom option lets you choose which authentication method to use with the device and also customize device policies. The policies that are available depend on the type of device you have, for example, the biometric retry limit applies to only biometric devices. If the device profile that you create allows multiple users, by default, the private partition space is divided equally among all users (excluding the administrator account). You can set a specific private partition size for each user when you create the user. The device policies that you set in a custom profile apply to all users on the device.

Possible authentication methods include:

- Password or Biometrics
- Password and Biometrics
- Password Only
- Biometric Only

Possible device policies include:

- Maximum number of users (you can create up to 10 users, not including the Administrator account.
- Biometric security level
- Biometric retry limit
- Password retry limit
- Data Destruction—the action to take if a user account becomes blocked
- Password policies
- Device Management Code
- Ability to disable Administrator account

For more information about device policy settings, see “Device Policy Settings Appendix” on page 22.

Note: If you choose to disable the Administrator account, you can create only one user on the device. You cannot create the Administrator account at a later time. Without an Administrator account, the ability to perform administrative functions is also prohibited. For example, if the user can no longer authenticate to the device, the user cannot be rescued and the device must be recycled.

2. Creating the Administrator account

Only the Administrator can perform certain operations on a device, such as adding, removing, and rescuing users. During the personalization process, the Administrator account is created automatically when you set the Administrator password. If you choose a Custom profile and disable the Administrator account, you will not be prompted to provide an Administrator password. In this case, you cannot create the account at a later time.

It is very important that you memorize or store the Administrator password in a safe place. Without the password, you cannot change some device settings.

For more information about the Administrator, see “Types of users” on page 13.

3. Creating the first user

After you set the Administrator password (if applicable), you are automatically prompted to create a user and provide authentication credentials by enrolling fingers, creating a password, or both. The authentication method varies according to the device and profile being used. For more information about creating users, see “Creating a user” on page 13.

Note: If you do not create a user at this time, the device stores the personalization information (including the Administrator password) that you have provided. The next time you plug in the device, you must finish the task of creating the user.

LED STATES

All Imation Defender Collection Devices use one or more light emitting diodes (LEDs) to indicate the operational status of the device. The LED states vary depending on the device you are using.

Table 2: LED states for devices

State	Description of state
Solid green	Open—the device has not been personalized and no authentication mechanisms are set. User has logged into the device—if users exist, it indicates that the device has authenticated a user.
Flashing green	The flash frequency is approximately once per second and indicates that the device is waiting for a finger due to one of the following situations: • The device has just been plugged in and no user is currently logged into the device. • Software has initiated a biometric authentication or enroll operation. • A user has initiated a finger authentication operation for example, by touching the device when it is in the "idle" waiting-for-finger state. A device will remain in an idle state for only two minutes before the LED turns red to indicate the device is locked.
Flashing red once	Failed fingerprint authentication attempt. The device will go back to waiting for a finger (flashing green normal) after the failed signal finishes.
Flashing LED alternating between red and green	The device is waiting for a finger to authenticate but this is also the last chance to authenticate before biometric access is blocked. The frequency is approximately twice per second.
Flashing red	The device is either powering up or is totally blocked. When totally blocked, no authentication methods are available to allow a user to log into the device; this indicates that the device needs to be recycled.
Solid red	The device is locked.
Blue LED	Indicates a data transfer activity for all devices.
Flashing red and blue	Indicates that a fatal internal error occurred.

ACCESSING DATA ON THE DEVICE

After you personalize a device, only registered users can authenticate to it. Authentication involves logging into the device using a password, fingerprint, or both. The authentication method that you must use depends on the capabilities of the device and the profile applied to the device.

After you successfully log in, you can save files to, and open files from your private partition. It is recommended that you log out of your device if you must leave it connected while you are away from your computer. Otherwise, another user could access your private partition while you are absent. You can also disconnect the device completely to bring the data with you.

This chapter provides information about the following topics:

- Logging into and out of the device
- Saving and opening files
- Disconnecting the device

LOGGING INTO AND OUT OF THE DEVICE

To log into the device

1. From the notification area, at the far right of the taskbar, right-click the Defender icon and click **Login**.
2. If you are using a computer running Mac OS X, open a file manager and click the application drive for the device. Double-click the **ACCESS Standard** application and on the main page of ACCESS Standard, under **Manage Device**, click **Login**.
3. Follow the prompts in the authentication wizard until the device successfully authenticates you. If you want to view the contents of the private partition in read-only mode, enable the **Use malware-proof mode** check box.

Tip: If your device uses only biometric authentication, you can log into it without starting ACCESS Standard by swiping your finger across the fingerprint sensor.

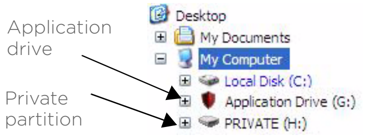
To log out of the device

1. From the notification area, at the far right of the taskbar, right-click the Defender icon and click **Logout**.
2. If you are using a computer running Mac OS X, open a file manager and click the application drive for the device. Double-click the **ACCESS Standard** application and on the main page of ACCESS Standard, under **Manage Device**, click **Logout**.

Tip: You can also log out by right-clicking the Defender icon, and then clicking **Eject Device**. For more information, see “Disconnecting the device” on page 12.

SAVING AND OPENING FILES

When you plug in your device both the application drive and the private partition display in a file manager, such as Windows® Explorer, with an associated drive letter for each partition.



Once you log into the device, you can open files on your private partition using the appropriate program or a file manager. When you save data to your private partition, the device encrypts the data using hardware-based AES 256-bit encryption. Data is automatically decrypted when you open the file.

Note: You cannot save data to or delete data from the application partition.

DISCONNECTING THE DEVICE

To disconnect the device

- From the notification area at the far right of the taskbar, right-click the Defender icon and click **Eject Device**.

  If you are using a computer running Mac OS X, drag the device drive on the desktop to the **Trash**. Release the mouse button when you see the **Eject** prompt.

Tip: You can also disconnect the device by clicking the **Safely Remove Hardware** icon in the notification area at the far right of the taskbar. Click the message “Safely remove USB Mass Storage Device - Drive (F:); where F is the letter of the drive in the file manager that is associated with the device. Disconnect the device when the following message displays, “The USB Mass Storage Device can now be safely removed from the system”.

Caution: Disconnecting the device, either accidentally or on purpose, without properly ejecting it, could corrupt the device and render it inoperable.

MANAGING USERS

An Administrator can create and delete users, and rescue users who can no longer authenticate to the device. Users can manage their authentication methods by enrolling or deleting fingers, changing their password, or both.

This chapter contains information about the following topics:

- Types of users
- Creating a user
- Deleting a user
- Managing authentication methods
- Rescuing a user
- Viewing user information

TYPES OF USERS

Imation Defender Collection Devices can register two types of users on the device:

- **Administrator**—this account is automatically created during the device personalization procedure when the Administrator password is provided. Only the Administrator account can manage users. The Administrator does not log into the device. Instead, ACCESS Standard will automatically prompt the user to provide the Administrator password when a user tries to perform a task that requires administrative privileges, such as adding or removing users, and rescuing users.

Note: If the device is personalized with a Custom profile in which the Administrator account is disabled, you cannot perform administrative functions. For more information, see "Device policy settings" on page 22.

- **General users**—typical device user who can authenticate to the device and save data to a private partition. Users can change their passwords and update finger enrollments.

CREATING A USER

Only the Administrator can create a user. The first device user is typically created during the device personalization process after the Administrator password is set. The Administrator can create subsequent users—if the device profile supports multiple users—during device personalization or at a later time. You can add a maximum of ten users and one Administrator.

Creating a user involves creating a user name and having the user provide authentication details by enrolling fingers, typing passwords, or both. When you add users to a biometric device, a maximum of 10 fingerprint templates can be enrolled among all users. Each user must enroll at least one fingerprint.

To create a user

1. On the main page of ACCESS Standard, under **User Management**, click **Create User**.

2. If you are prompted for the Administrator password, type the password in the **Password** box.
3. Complete the instructions on the **Create User** page to add the user and authentication credentials.

DELETING A USER

Only the Administrator can remove a user from a device. Once a user is deleted, the user's data is permanently lost even if a key recovery system exists.

To delete a user

1. On the main page of ACCESS Standard, under **User Management**, click **Delete User**.
2. If you are prompted for the Administrator password, type the password in the **Password** box.
3. Complete the instructions on the following pages to delete the user.

MANAGING AUTHENTICATION METHODS

Before users can update their authentication details, such as update a finger enrollment or change a password, they must authenticate to the device. Administrators cannot change the Administrator password once it has been set.

Once the total number of enrolled fingers allowed for the device or the user account is reached, no more fingers can be enrolled.

To update a finger enrollment

1. On the main page of ACCESS Standard, under **User Management**, click **Manage Authentication Methods**.

   If you use only biometric authentication, proceed to Step 2.
2. Click **Manage Your Finger Enrollments**. Follow the instructions to enroll a finger or update a finger enrollment.

   If you have enrolled the maximum number of fingers allowed, you must delete a fingerprint before you can update your finger enrollments.

Note: Biometric devices may require a user to perform five separate finger swipes per enrollment.

To change a password

1. On the main page of ACCESS Standard, under **User Management**, click **Manage Authentication Methods**.

   If you use only password authentication, proceed to Step 2.
2. Click **Manage Your Password** and complete the instructions on the page that follows to set a new password.

   If you are using two-factor authentication, the device will prompt you to authenticate using a biometric before opening the **Set Password** page.

RESCUING A USER

Rescuing a user resets the user's authentication method by deleting finger enrollments, resetting a password, or both. Users can then enroll fingers and set a password as required. For more information, see "Managing authentication methods" on page 14.

Only the Administrator account can rescue a user if the user can no longer authenticate to the device. For example, a user may be prevented from authenticating if she exceeds the number of authentication attempts allowed for the device or she forgets her password.

To rescue a user

1. On the main page of ACCESS Standard, under **User Management**, click **Rescue User**.
2. In the **Password** box, type the Administrator password and click **Next**.
3. If there are multiple users on the device, select the user who cannot authenticate to the device from the **User Name** list and click **Next**.
4. Complete the instructions on the pages that follow to add new authentication information.

VIEWING USER INFORMATION

You can view information about device users including authentication and partition details, such as the number of finger enrollments allowed, password and two-factor status, and private partition size. All information is read-only.

To view user information

- On the main page of ACCESS Standard, under **User Management**, click **Users**.

MANAGING DEVICES

You can set the language for device software and view device information to verify device configuration, partition, and version information. Recycling a device removes all users and data from the device.

This chapter provides information about the following topics:

- Selecting a language
- Viewing device information
- Recycling a device

SELECTING A LANGUAGE

You can choose the language that you want to use with ACCESS Standard.

To select a language

1. On the main page of ACCESS Standard, click **Language Selection**.
2. Click the language you want to use from the list.

VIEWING DEVICE INFORMATION

You can view information about the device. All information is read-only.

To view device information

1. On the main page of ACCESS Standard, click **Hardware and Software Information**.
2. Click one of the following categories:
   - **Device Settings—**contains biometric and hardware information such as retry limits and security levels, and the device serial number.
   - **Disk Partitions—**outlines the overall allocation of disk space on the device.
   - **Product Versions—**lists the version for all software and hardware associated with the device.

RECYCLING A DEVICE

Recycling a device returns it to a default state by deleting all users and authentication mechanisms. All data and security keys are unrecoverable. The Administrator or any user who knows the device management code can recycle a device. You must personalize a recycled device to reapply a device profile and recreate users. For more information, see “Personalizing a device” on page 8.

Important: If a device does not have a management code, any user can recycle the device even if they are not logged into the device. For more information about the management code, see “Custom” on page 8.

To recycle a device

1. On the main page of ACCESS Standard, click **Recycle Device**.

2. Read the warning on the **Recycle Device** page, and then type the management code in the **Management Code** box.
3. Click **Next**.

   ACCESS Standard will automatically recycle the device.

PROTECTING THE DEVICE FROM VIRUSES

If you have licensed the ACCESS Antivirus Scanner™, you can further protect data on the device. The scanner looks for viruses on the host computer and on the private partition of the device. You can also update the virus database to ensure that the scanner is reviewing the content for new viruses. An intrusion log allows you to track all scanning events that occur.

This chapter provides information about the following:

- Scanning the device and host computer
- Updating the virus database
- Logging ACCESS Antivirus Scanner events

SCANNING THE DEVICE AND HOST COMPUTER

You can set the ACCESS Antivirus Scanner to regularly scan the private partition and the host computer each time you access the device or manually as necessary.

To scan the private partition

1. In the notification area at the far right of the taskbar, click the Defender icon, and then click **Manage Anti-virus Scanner**.
2. In the **Private Partition** area, do one of the following:
    - Click the **On-access scan** check box if you want the scanner to check the private partition each time you access the device.
    - Click **Scan** to immediately scan the private partition.

To scan the host computer

1. In the notification area at the far right of the taskbar, click the Defender icon, and then click **Manage Anti-virus Scanner**.
2. In the **Host System** area, do one of the following:
    - Click the **Scan host system on startup** check box if you want the scanner to check the host computer each time you plug in the device.
    - Click **Scan** to immediately scan the host computer.

UPDATING THE VIRUS DATABASE

You can update the virus definition file automatically whenever an update is available. The scanner updates the device if necessary each time you log in. You can also manually update the database as needed.

To update the virus database

1. In the notification area at the far right of the taskbar, click the Defender icon, and then click **Manage Anti-virus Scanner**.
2. In the **Virus Database** area, do one of the following:

- Click the **Automatic updates** check box to if you want to update the virus definition file automatically.
- Click **Update** to force an update of the file.

LOGGING ACCESS ANTIVIRUS SCANNER EVENTS

When enabled, the ACCESS Antivirus Scanner records a log of all scanning events.

To enable the intrusion log

1. In the notification area at the far right of the taskbar, click the Defender icon, and then click **Manage Antivirus Scanner**.
2. In the **Intrusion Log** area, click the **Enabled** check box.

To view the log file

1. In the notification area at the far right of the taskbar, click the Defender icon, and then click **Manage Antivirus Scanner**.
2. In the **Intrusion Log** area, click **View**.

Tip: Click **Clear** to delete all entries from the intrusion log.

TROUBLESHOOTING

If you have problems using your device, you may find a solution in one of the following scenarios. For further technical assistance, contact Imation.com/support.

I CANNOT EJECT MY DEVICE

When you try to eject your device 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 log out or eject the device using ACCESS Standard or safely remove the device using the taskbar icon, see "To disconnect the device" on page 12.

MY BIOMETRIC DEVICE WILL NOT AUTHENTICATE MY FINGER

A device 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 extra finger enrollments, you can enroll another finger or delete an existing fingerprint and enroll a new one. For more information, see "Managing authentication methods" on page 14. If the sensor is broken, contact the administrator or Imation.

PASSWORD OR BIOMETRIC ACCESS TO MY DEVICE IS BLOCKED

You will receive a warning message when you have only one remaining password or biometric attempt left before you reach the retry limit. When you exceed the retry limit, the device blocks you from authenticating to it using that authentication method. You must contact your administrator to unblock your user account. For more information, see "Rescuing a user" on page 14.

MY DEVICE DRIVE MAPPINGS DO NOT APPEAR

Sometimes a drive letter for a partition of an Imation Device does not get mapped. This occurs when a network drive mapping occupies a letter typically assigned to one of the drives of ACCESS Standard.

If you map a network drive to a resource using the drive letter typically assigned to ACCESS Standard, you will not see the device drive in the file manager window when you connect the device. This problem occurs only if you map the drive while the device 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

DATA SAVED TO THE APPLICATION PARTITION IS NOT AVAILABLE

You cannot save data to the application partition of a device. Save data to only your private partition.

DEVICE POLICY SETTINGS APPENDIX

During the Custom personalization process, you can configure device policy settings, such as the number of device users, biometric security level, and password policies. The policy settings that are available vary according to the type of authentication the device uses. For more information about personalizing a device or to see a list of default device settings, see “Personalizing a device” on page 8 or “1. Choosing and applying a device profile” on page 8.

The following table describes each policy setting and indicates the devices to which these options apply. For information about password policies, see Table 4 on page 24.

Table 3: Device policy settings

Policy setting	Description	Applicable devices
Type of authentication	• Password or Biometrics • Password and Biometrics • Password Only • Biometric Only	*Biometric/ Password options:* • Defender™ F200 +BIO • Defender™ H200 +BIO *Password*: • Defender™ H100 • Defender™ F100 • Defender™ F150
Maximum number of Users	Total number of users you can add to the device to a maximum of 10. This does not include the Administrator account.	• All devices

Table 3: Device policy settings

Policy setting	Description	Applicable devices
Biometric Security Level	Applies to all device users. It is expressed as a False Match Rate (FMR) probability, such as “1 in 10,000”. FMR is the probability that two different fingers are incorrectly matched. 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 a user has difficulty authenticating to the device at the desired level of security, it is recommended that you also assign the user a password.	• Defender™ F200 +BIO • Defender™ H200 +BIO
Biometric Retry Limit	When the retry limit is reached, only the user whose biometric is blocked is prevented from accessing the device using biometric authentication. Password authentication is still available. For example, a retry limit of one will block users after two failed attempts. Retry limits can range from 1 to 254, or infinite. It is recommended that you set biometric retry limits higher than password retry limits since biometric authentication failures are not always the fault of the user. When a user exceeds a retry limit while trying to authenticate to the device, the following action occurs: Note: Biometric false rejections (when a genuine user is not validated during an authentication attempt even when using an enrolled finger) can occur with any biometric system. The false rejection rate increases with higher biometric security levels. Therefore, it is recommended that you set a high biometric retry limit to minimize the chances of blocking access to the device for biometric users due to false rejections. Setting a low retry limit can easily result in blocked access, especially if a low False Match Rate (FMR) is set for the biometric security level. See also, Biometric Security Level.	• Defender F200 +BIO • Defender H200 +BIO
Password retry limit	See Table 4 on page 24.	
Device Management Code	The management code is required to perform device management processes such as, recycling the device.	• All devices

Table 3: Device policy settings

Policy setting	Description	Applicable devices
Data Destruction	This setting determines the action to take if a user account becomes blocked. When you turn Data Destruction on, data cannot be recovered and the device cannot be rescued if a user can no longer authenticate to it. If the Administrator account is disabled, Data Destruction is automatically turned on.	• All devices
Disable Administrator's account	Does not include an Administrator account when you personalize the device. Without the Administrator account, however, you cannot rescue a user or perform other administrative functions. You can also create only one device user.	• All devices

Password policies

You can increase the strength of a password by changing the complexity of the rules that users must follow when setting the password. Complex password rules increase security by reducing the probability that an unauthorized person could breach the password and access a device. The following table describes the password rules available with ACCESS Standard.

Table 4: Password policies

Rule	Definition
Password retry limit	Number of failed password authentication attempts allowed before users are blocked from logging into the device. For example, a retry limit of one will block users after two failed attempts. Only the user whose password is blocked is prevented from using a password to log into the device. Biometric authentication (if applicable) is still available if the biometric retry limit has not been exceeded. Retry limits can range from 1 to 254, or infinite.
Minimum password length	Minimum number of valid characters (4–40) the password can contain.
Minimum special characters	Minimum number of special characters (0-15) required in the password. Valid characters include: ~ ‘ ! @ # $ % ^ * ( ) _ - + = { }[ ] | \ : ‘ “ , . / ? & ; < >.
Minimum numeric characters	Minimum number of numeric characters (0–15) required in the password, for example (1234567890).
Minimum alphabetical characters	Minimum number of alphabetical characters (0–15) required in the password (includes uppercase and lowercase).
Minimum uppercase characters	Minimum number of uppercase characters (0–15) required in the password.
Minimum lowercase characters	Minimum number of lowercase characters (0–15) required in the password.

Table 4: Password policies

Rule	Definition
Reuse threshold	Minimum number of different passwords (0-15) that a user must set before he can reuse a previous password.
Minimal lifetime (minutes)	Minimum number of minutes (0-120) the user must wait before a newly changed password can be changed again. This rule prevents users from changing their password and then quickly changing it back to the original password to avoid using the new password.
Maximum lifetime (days)	Maximum number of days (0–1000 or infinite) for which a newly changed password is valid. The user must change the password when the maximum lifetime expires.

INDEX

A

- adding
  - fingers 14
  - first user 9
  - users 13
- administrative privileges 13
- Administrator
  - about 9
  - disabling account 13
- antivirus scanner
  - scanning computer 18
  - scanning device 18
  - updating database 18
  - viewing log file 19
- application partition
  - devices 21
- authentication methods 14

B

- biometric
  - enrolling 14
  - false rejections 23
- biometric access blocked 20
- biometric profiles 8
- blocked
  - biometric or password access 20
- blue LED 10

C

- changing passwords 14
- contacting
  - Memory Experts International ii
- creating
  - new password 14
  - users 13
- creating an Administrator 9

D

- data destruction 24
- data not appearing
  - troubleshooting 21
- default
  - device settings 8
  - profile settings 8
- deleting
  - users 14
- devices
  - about profiles 8
  - adding users 13
  - application partition 21
  - default settings 8
  - personalizing procedure
  - recycling 16
  - rescuing users 14
- disconnecting the device 11

E

- editing
  - passwords 14
- ejecting device
  - troubleshooting 20
- enrolling fingers 14
- enrollment privileges 13
- error
  - Cannot Unmount Volume 20

F

- false rejection rate
  - biometric 23
- fingers
  - enrolling 14

G

- general users 13
- green LED 10

H

- hardware version 16

I

- initializing a device
  - *see* personalizing
- intrusion log
  - about 19

L

- language
  - setting for application 16
- LED
  - blue 10
  - flashing green 10
  - flashing green normal 10

  - flashing green slow 10
  - flashing red 10
  - solid green 10
  - solid red 10
- log file
  - for antivirus scanner 19
- logging into the device 11
- logging out of the device 11

M

- malware-proof mode 11
- Management code 8
- mapping network drives 20

N

- network drives
  - mapping 20

O

- opening files 12

P

- partitions
  - application 21
  - opening files 12
  - saving files 12
  - viewing size 16
- password
  - retry limit 24
- password profiles 8
- passwords
  - about retry limits 24
  - Administrator 9
  - changing 14
- personalizing a device
- private partition size 8
- profiles
  - about 8

R

- read-only mode 11
- recycling devices 16
- red LED 10
- removing
  - devices 11
  - users 14
- rescuing users 14
- resetting
  - user authentication methods 14
- retry limit
  - setting for password 24

S

- Safely Remove Hardware operation 11
- saving files 12
- scanner
  - recording events 19
  - updating virus database 18
- scanning
  - device for viruses 18
  - host computer 18
- setting
  - password retry limit 24
- software version 16
- support
  - technical assistance ii

T

- technical support ii
- troubleshooting
  - blocked access to device 20
  - data not appearing 21
  - ejecting device 20
  - finger authentication failed 20
  - network drive issue 20
  - password access blocked 20
  - unsafe removal event dialog 20
- two-factor profile 8

U

- unlocking the device 11
- unplugging the device 11
- unsafe removal event dialog 20
- updating
  - virus database 18
- users
  - adding 13
  - adding the first time 9
  - administrators 13
  - changing authentication methods 14
  - definition of 13
  - general 13
  - removing 14
  - rescuing 14
  - viewing number of 16

V

- version number 16
- viewing
  - device configuration 16
  - partition information 16
  - user information 16
  - version information 16
- virus database
  - updating 18