

Quick Start Guide

Welcome to **DeviceDefender™**, **Version 3.1** software from EncryptX Corporation (www.encryptX.com). DeviceDefender allows you to encrypt and protect sensitive information on removable devices such as USB flash drives, removable hard drives, CompactFlash cards, SD cards, Memory Sticks & CDs/DVDs. Encryption prevents unauthorized access to confidential data stored on your removable drives. This Quick Start Guide discusses how to use DeviceDefender. Summary information on SecurFlash is provided for informational purposes to understand how the products work together. The SecurFlash QuickStart Guide can be found on any removable device that has been encrypted by DeviceDefender.

DeviceDefender™ - Is a Microsoft Windows File System Driver application. It is installed on a user's PC. DeviceDefender is designed for users that want to automatically protect removable devices. DeviceDefender runs from the user's PC or corporate server and automatically detects any removable drives connected to it. When a removable drive is detected, the software prompts the user to set a password for the drive. If the user proceeds, any data written to the drive is automatically and transparently encrypted. The user does not have to change their behavior - they work with files on the encrypted device exactly as if they were in the clear. Any files on the device that the user is opening or modifying are automatically decrypted and re-encrypted when the user is finished making their changes. If the user chooses to cancel the set password dialog, then the drive is set to a READ ONLY mode unless the user has permissions to choose whether to encrypt it or not. If the drive is set to READ ONLY, files may be read from the device but no files can be written to it.

SecurFlash™ - Is a portable application installed directly on the removable device. A copy of SecurFlash is installed automatically by the DeviceDefender driver application on the removable device that is encrypted. SecurFlash executes and runs from the removable drive when the user double-clicks on the **OpenSecureFiles.exe** program. SecurFlash is used to encrypt and decrypt files on the removable drive on PCs that do not have DeviceDefender installed. Since this application runs from the removable drive, it does not install on the PC, and does not require any special PC administrative rights to run. SecurFlash is designed to protect information on drives that are portable – such as those used on multiple PCs. SecurFlash can also decrypt and open files encrypted on the removable device that have been automatically encrypted by the DeviceDefender driver. Any new files that are encrypted with SecurFlash on the removable drive can also be decrypted by the DeviceDefender driver application.

Supported Operating Systems

DeviceDefender is supported on Microsoft Windows 2000, XP Home, XP Pro, and Vista as well as Windows Server 2000, 2003 & 2008. The software is not supported on 64-bit operating systems, nor on Windows 95, Windows 98, Windows Me, Linux, or any of the Macintosh operating systems. You can encrypt any type of file supported by the Microsoft Windows Operating System through the DeviceDefender and SecurFlash software.

Important Note: You must have JAVA Run Time Environment Version 6 or higher installed on your PC in order to use DeviceDefender™. If DeviceDefender does not run automatically for you, check your Windows > Control Panel > Program Files to see if Java 6.0 or higher is installed on your PC. If it is not, you can download JAVA 6.0 for free from <http://www.java.com/en/download/index.jsp>

License Restrictions

DeviceDefender Personal Edition allows you to encrypt up to 20 removable devices and up to 250 CD/DVDs per year.


DeviceDefender Server Edition allows you to encrypt up to 250 removable devices and up to 1500 CD/DVDs per year.

To view your current license counts, select About > License from the DeviceDefender menu.

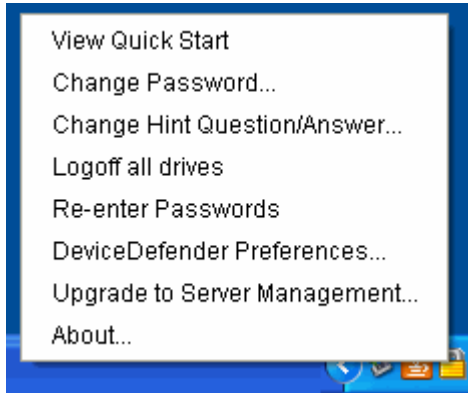
Important Product Use Concepts


1. **When DeviceDefender is installed on your PC, data encryption of your removable drives by the DeviceDefender software is automatic.** DeviceDefender will encrypt any data saved to a removable device by an application, a DOS command window, or by Windows Explorer. Data encryption is completely automatic. If you have been given the “Choose to Encrypt” permission, you may turn the automatic encryption off for a particular device.
2. **If you choose NOT to encrypt data on a device, or choose not to enter the password for a device that is already encrypted, your access to the device may be limited.** When a removable device is connected to your PC, you will be prompted for an encryption password. If you do not have the “Choose to Encrypt” option enabled for your DeviceDefender installation, and you decline to provide a password, the device will be made read-only and only unencrypted files will be accessible. This allows you to copy files from your removable device to your PC, but you will be prevented from writing any data to the removable device.
3. **If you forget both your password and password recovery hint answer, you will not be able to access the encrypted files on the drive unless you have upgraded to the optional server management software.** You will need to remember either your password or your recovery hint question to be able to access your encrypted files. If you forget both of these values, the optional Central Management Server software provides remote password recovery capability. Your Security Administrator can assist you in recovering your password through the Security Manager application if it has been deployed.
4. **Accessing encrypted data when you are not working on a PC with the DeviceDefender driver installed must be done through the SecurFlash application on the device.** The encrypted files that have been protected through the DeviceDefender driver software are not directly accessible to applications or the Microsoft Windows Operating System when you are not working on a PC with the DeviceDefender driver installed. The files appear on the drive, but they are encrypted. The only way to access these files is to run the EncryptX SecurFlash application by double clicking the **OpenSecureFiles.exe** located on the device and providing the correct password. The OpenSecureFiles.exe will also auto-run on most operating systems, depending on your user privileges. When SecurFlash is running, you can open the files and modify them by double clicking the files that are shown in the DeviceDefender application window.

About the DeviceDefender Application

Once the DeviceDefender software is installed, it will appear as a  icon in your system tray (typically located in the lower right corner of your desktop on the Task bar). The software is automatically initiated during system startup and therefore should always be available.

Occasionally, informational messages will be displayed using temporary pop-up boxes to provide you with instructions or inform you of events that have been detected. You do not need to click on the messages to close them, they will disappear by themselves.



Right-clicking on the  icon will display a context menu of the functions available in DeviceDefender.

I. Setting Passwords for New Devices

The DeviceDefender software will automatically detect any removable devices connected to your PC. If a drive has not already been encrypted, you will be prompted with the User Setup dialog. The User Setup establishes both the encryption password for the drive as well as the password recovery hint question and answer. Using a personal pass phrase instead of a simple password provides significantly greater security. Your Hint Answer is case sensitive, so don't forget how you type it in. You will need to type it exactly the same if you use it later for password recovery.

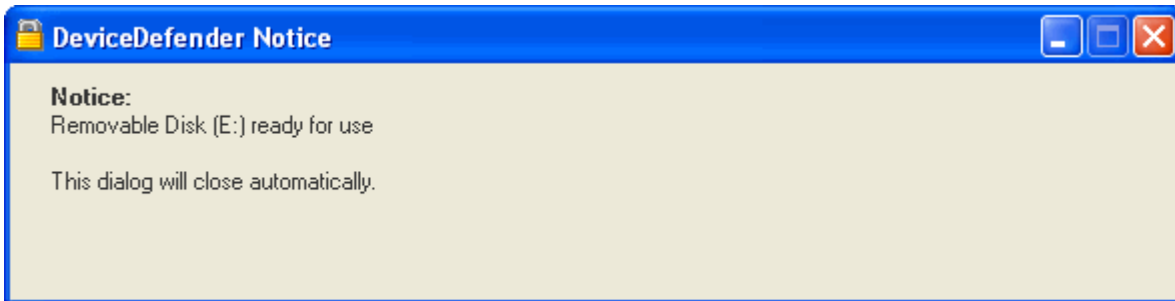
Standalone Mode (unmanaged devices)

Managed Devices

If DeviceDefender was installed with the option for centrally managing your encrypted devices, then the User Setup dialog will contain fields for your Email Address and a Personal ID. Your email address is used for user identification and for server-based password recovery. Use the Personal ID field to uniquely identify your drive. If you have more than one drive, put in a different Personal ID for each one.



Once you have established your password and password recovery hint question/answer, DeviceDefender will install the mobile edition of the software onto the device. When finished, a message will appear indicating the device is ready for use.



II. Pressing Cancel in the User Setup or Login Dialogs

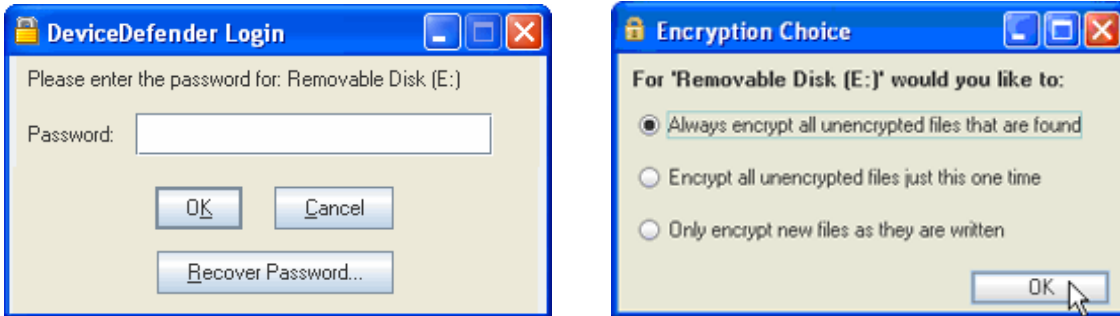
If you press the cancel button or close either the User Setup or Login dialog boxes and you have been given the option to choose if you do not want to always encrypt removable devices, then a Cancel dialog will be shown. If you choose to Never encrypt files on this device, your setting will be remembered the next time you use this device and the password dialog will be suppressed.

If you have not been given the option to choose whether or not to encrypt removable devices, then canceling will place the device into a read only state which will let you open and copy files from the device, but you will be prevented from writing any new files to the device.



III. Logging On to Devices Already Encrypted

If DeviceDefender detects that a drive has already been encrypted, it will prompt you for the encryption password when the drive is mounted. If you decline to provide a password by clicking on the Cancel button or by closing the dialog box, then the drive will be mounted in read-only mode.



If the drive contains any files that are not encrypted, DeviceDefender will prompt you to choose if you wish to encrypt them or not. If you choose to always encrypt unencrypted files, DeviceDefender will remember this setting for this device.

Once the drive is ready for use, DeviceDefender will intercept all file operations to the drive and encrypt/decrypt automatically as necessary.

Note: Any attempt to access the files on the encrypted device before the encryption password has been entered will result in an error. Typical errors may indicate access is denied or that the file cannot be opened because it does not exist. Difficulties accessing these files may persist even after entering the correct password due to Windows file system caching. Ejecting and reinserting the drive will clear these issues.

IV. Using the DeviceDefender Application

Change Password

This option allows you to change the encryption password for any mounted encrypted drives.

Change Hint Question/Answer

This option allows you to change the password recovery Hint Question/Answer for any mounted encrypted drives.

Log off All Drives

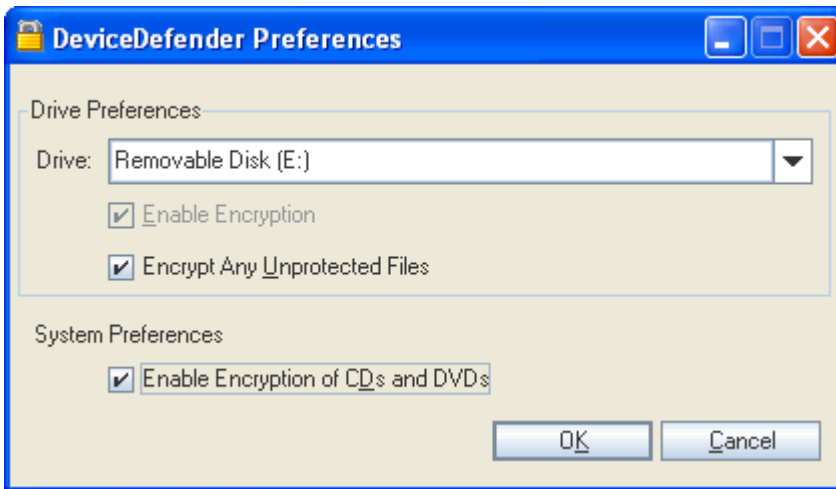
This option will log off all removable devices from DeviceDefender. You will need to either disconnect and reinsert a drive, or select the "Re-enter Passwords" menu option to regain access to the encrypted drives. Attempts to access files when the drives are logged off will result in an error indicating the file is unavailable. Any unencrypted files on the device will be limited to read-only access.

Drives are automatically logged off if they are disconnected from the PC.

Re-enter Password

This option prompts for the password of all mounted drives. This option can be used to enter a password for a device that was originally mounted read-only by cancelling or closing the password prompt.

DeviceDefender – Drive Preferences



Drive preferences are drive-specific. You may choose different settings for different drives. The Preferences option allows you to change the settings that were established when the drive was first initialized.

If the Enable Encryption checkbox is not enabled, it indicates that this setting is controlled by corporate policy in the central management server.

Clearing the “Encrypt All Unencrypted Files” checkbox will disable the scanning for, and automatic encrypting of unprotected files when the device is inserted into your PC.

DeviceDefender – System Preferences

If you choose to enable encryption of CDs and DVDs, then any discs that are burned using the built-in CD/DVD burning facility in Microsoft Windows XP and Vista will be automatically encrypted. When a blank disc is inserted, you will be prompted to establish an encryption password. With this option enabled, CDs & DVDs will be encrypted the same as any other removable device.

Note: Encryption of CDs/DVDs using third-party burning applications such as Nero, EZ CD Creator, etc. are not supported. Additionally, encrypting discs using the Windows Live File System on Vista is not supported.

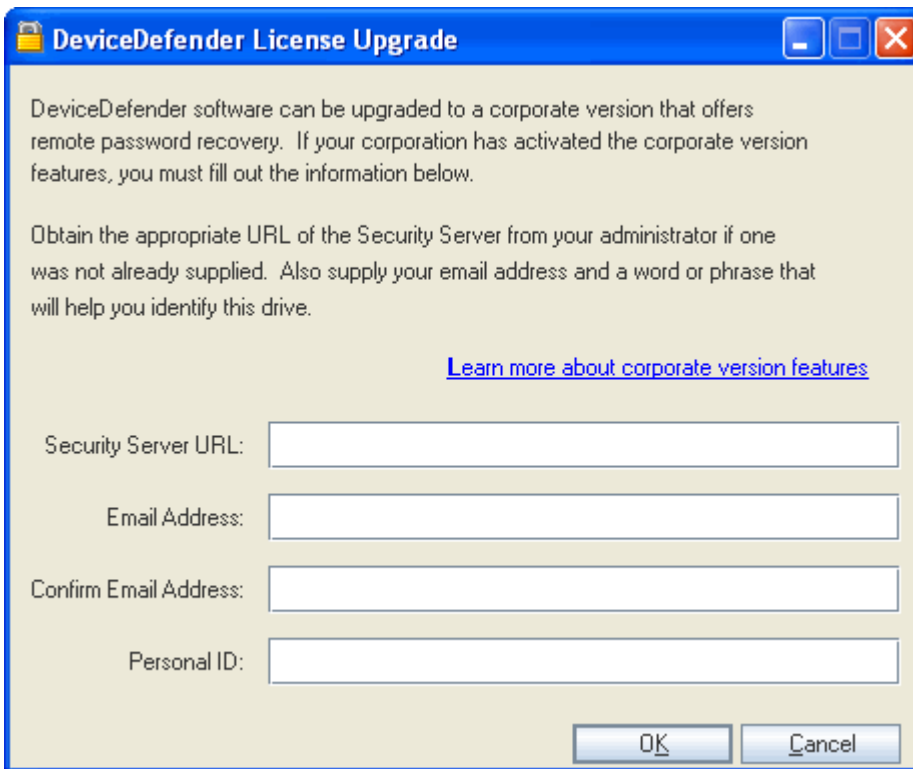
If the Enable Encryption of CDs and DVDs checkbox is not checked, then CD and DVD drives will be ignored by the DeviceDefender software and all files burned to them will be left unencrypted.

About

This option displays information regarding the DeviceDefender software version, type of encryption and current drive status of all removable devices.

Upgrade to Server Management

This option will upgrade the DeviceDefender software to the Corporate Edition, which requires a connection to the corporate Security Server. This provides central management, additional password recovery mechanisms, and enforces corporate policies such as strong passwords, password expiration, offline re-authentication periods, and remote revocation in the event of loss of a device.



The screenshot shows a Windows-style dialog box titled "DeviceDefender License Upgrade". The dialog contains the following text and fields:

DeviceDefender software can be upgraded to a corporate version that offers remote password recovery. If your corporation has activated the corporate version features, you must fill out the information below.

Obtain the appropriate URL of the Security Server from your administrator if one was not already supplied. Also supply your email address and a word or phrase that will help you identify this drive.

[Learn more about corporate version features](#)

Security Server URL:

Email Address:

Confirm Email Address:

Personal ID:

At the bottom right, there are "OK" and "Cancel" buttons.

Security Server URL:

Your security administrator will provide you with the correct Security Server URL to connect to. Do not include the "http://" prefix on the URL. Example: `secureserver.mycompany.com`

Email Address:

Enter your valid email address. This is used to allow the security administrator to assist you in recovering your password if you forget it and/or your recovery hint question/answer. The confirmation text box helps prevent you from accidentally entering a typo in your email address.

Personal ID:

Your security administrator may provide you with corporate guidelines as to what value to enter into the Personal ID field. This field should be unique to each removable device you use. This value assists the security administrator in uniquely identifying each device should you encounter any issues in the future such as a lost device or a compromised password.

V. Accessing Encrypted Data without DeviceDefender

If you wish to access protected files that were encrypted with DeviceDefender from a PC that does not have the DeviceDefender driver installed, you will need to run the **OpenSecureFiles.exe** program on the device. This will run the SecurFlash application. This allows you to enter your encryption password and use the encrypted files from within the SecurFlash application window. The SecurFlash application does not automatically encrypt new files on your removable device like DeviceDefender does, but it provides you with a manual method to encrypt them.

Note: When using a PC that does not have DeviceDefender, if you copy files to your device without using the SecurFlash application, they will be written to the device unencrypted and without password protection.

VI. Copyright and Trademark Information

© 1999-2009, EncryptX Corporation.

All rights reserved.

DeviceDefender and SecurFlash are registered trademarks of EncryptX Corporation.

www.encryptx.com

VII. Contacting EncryptX Corporation

Toll Free Phone 888-431-4550

Email customersupport@encryptx.com

Website www.encryptx.com

Address 580 Burbank Street, Suite 110, Broomfield, Colorado 80020

Local Phone Number 303-464-8564