Acer eDataSecurity Management

By applying the most advanced cryptographic technologies, Acer eDataSecurity Management offers Acer PC users greater personal data security and encryption for files and data transmitted via instant messaging or email.

Warning: Files that you should not encrypt:
To ensure optimum system stability, you should not attempt to encrypt any of the following folders, or files in them:
**** C:\WINDOWS***
**** C:\Program Files***
**** Acer eDataSecurity Management program folder***

Encrypting any of these folders or files contained within them may cause serious system instability that could require you to re-install your operating system, which will delete all your personal data.

Using Acer eDataSecurity Management

You can launch Acer eDataSecurity Management in a number of ways:

- From the Start menu, go to **Start > (All) Programs > Empowering Technology > Acer eDataSecurity Management**.
- By clicking on the **Empowering Technology** icon from your desktop, or pressing the < > key to launch the **Empowering Technology** user interface. Select the **Acer eDataSecurity Management** icon.

This will open the Acer eDataSecurity Management main page.

Password

The passwords you set up are the keys to encrypting and decrypting files. Make sure you keep your passwords in a secure place, and try to choose passwords that are not easy to guess.

Setting up passwords

Before you can use Acer eDataSecurity Management, you will need to set up your default encryption password and your supervisor password. When you're installing Acer eDataSecurity Management, or when you use it for the first time, you will be prompted to set up these passwords.

If you forget these passwords, you will not be able to decrypt or recover your data, so it is important to keep your passwords in a safe place.

Password rules

The passwords you select must be between four and 12 characters in length. They can consist only of letters, numbers and the following special characters:

=	Equal sign
-	Minus sign
[	Left bracket
]	Right bracket
.	Period
,	Comma
;	Semi-colon
/	Forward slash
\	Backslash

Supervisor password

Your supervisor password can be used to decrypt any file that you have encrypted. This is a "last resort" in the event that you've forgotten the password you used to encrypt the file. You should not let other people know what your supervisor password is.

The supervisor password will only work on the computer that you originally used to encrypt the file.

Important: The supervisor password can also be used to override the default password for changing any settings in Acer eDataSecurity Management.

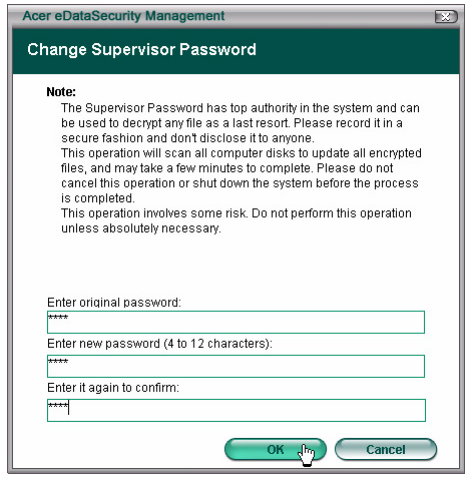
You can change your supervisor password at any time you wish, from the system setup window; however, this is a time-consuming process, and involves some degree of risk.

Changing the supervisor password

Step1: From the system settings window, choose **Change Supervisor Password**.

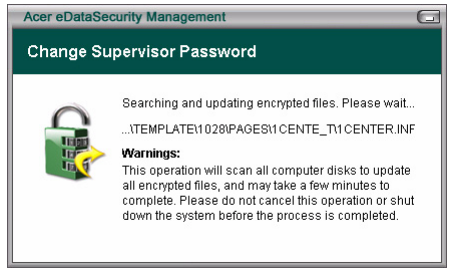
Step 2: Click on **Change Supervisor Password**.

Step 3: You will need to enter the existing supervisor password, and then enter the new password twice.



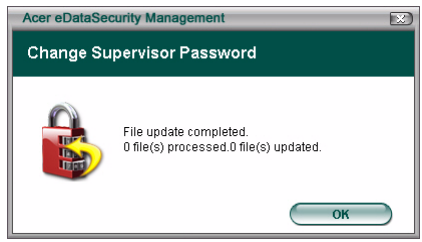
Step 4: Once you've done this, Acer eDataSecurity Management will scan your system for any encrypted files, and implement the change.

You should not abort this process, or allow Windows® to shut down before the process is complete. If the process is interrupted, it will continue next time you start up your computer.



If the program is unable to process all the encrypted files, you will be informed of which files were unable to be processed and the likely reasons why. You will need to close any programs that might be using the encrypted files, and reboot your system. Then click **Retry File Update** to complete the process.

Step 5: File update completed



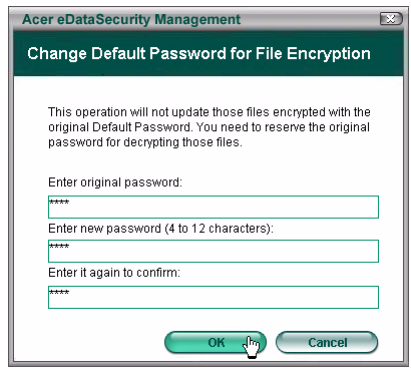
Default encryption password

Your default encryption password will be used for all encryption requirements, unless you specify a unique password. Any files encrypted after you change this password will require the new password to open them. Any files encrypted before you change the password will require the original password to open them.

Changing the default password

Step1: Click on **Change Default Password for File Encryption**

Step 2: Enter the original password and enter the new password twice.



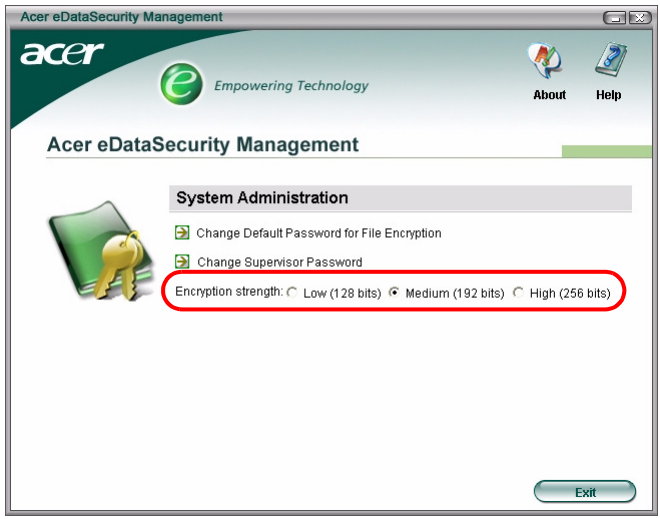
Encryption strength

Acer eDataSecurity Management offers you three levels of encryption:

- Low (128 bits)
- Medium (192 bits)
- High (256 bits)

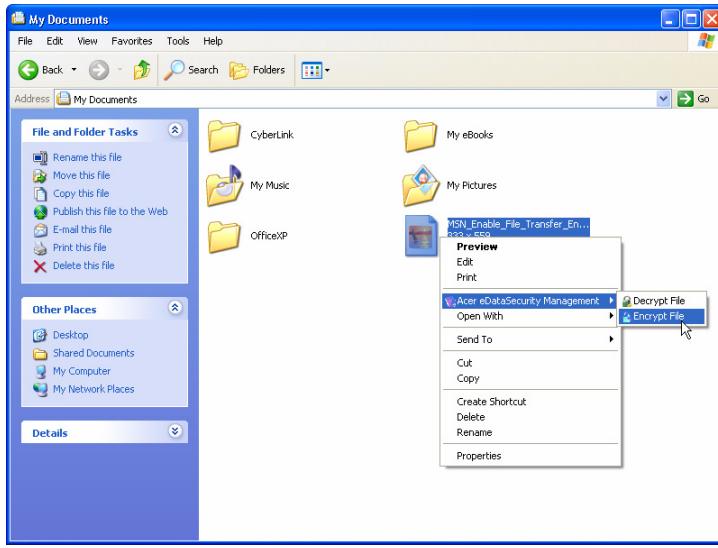
Note: The default setting is Medium.

All three levels offer a high degree of security, but there is a trade-off in terms of the amount of time it takes to encrypt and decrypt the files: the higher the level of encryption chosen, the longer the processing time.

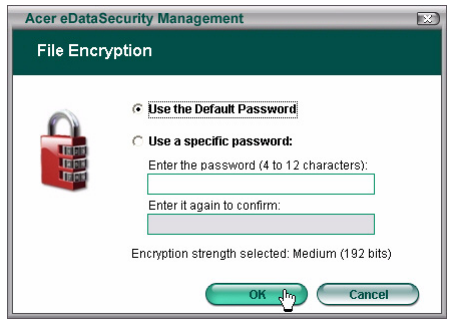


File and Folder Encryption

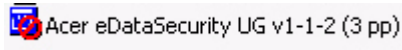
Acer eDataSecurity Management offers you the added security of password-protecting personal files and folders, or files sent via instant messenger or email. The file encryption tool is integrated into the right-click function of Microsoft® Windows®, making it easy for you to encrypt or decrypt a file at any time.



When you select a file to encrypt, you're asked if you want to use your default encryption password, or if you want to specify a different password for encryption.

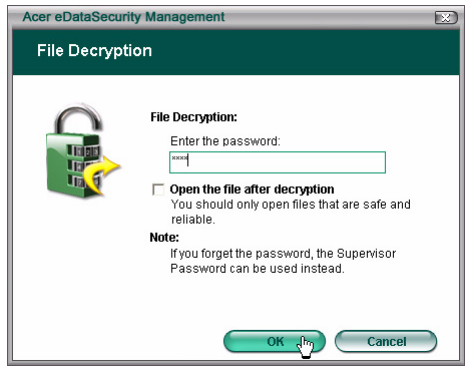


A file that has been encrypted will be displayed with a different icon, and file extension.



File and Folder Decryption

Right-click on an encrypted file, and select the decrypt function. You will be required to enter the correct password, and select whether you want the file opened once it's been decrypted. Once the password has been entered, Acer eDataSecurity will decrypt the file, and if selected, open the file.



Sending Other People Encrypted Files

You can choose to encrypt any file that you send to someone using MSN Messenger or Microsoft® Outlook.

By default, Acer eDataSecurity Management activates encryption of files sent via MSN Messenger. To disable this feature, open MSN Messenger, click Tools and uncheck Enable File Transfer Encryption.

You can select to encrypt files that you send by email. Acer eDataSecurity Management is integrated into the Microsoft® Outlook toolbar, offering you one-click attachment encryption.

The encrypted file will be sent as a self-extracting '.exc' file, so there is no need for the receiver to have Acer eDataSecurity Management installed on their computer. The receiver will need to save the file to their hard disk, and change the file extension to '.exe' before they are able to decrypt the file.