

Acer eDataSecurity Management

Using advanced cryptographic technologies, Acer eDataSecurity Management offers you 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.

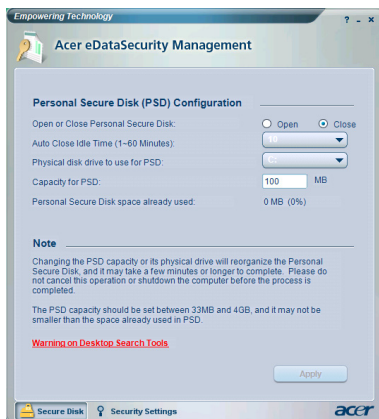
Using Acer eDataSecurity Management

To launch Acer eDataSecurity Management:

- Click on the Acer eDataSecurity icon in the Empowering Technology toolbar shown on your desktop.
- From the Start menu, go to **(All) Programs > Acer Empowering Technology > Acer eDataSecurity Management**.



This will open the Acer eDataSecurity Management main page.



Passwords

The passwords you use 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.

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.

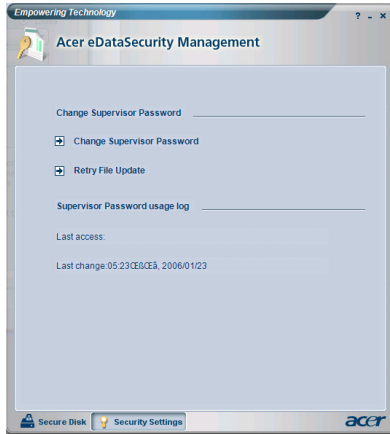


Important: The supervisor password can also be used to override the default password for changing any settings in Acer eDataSecurity Management.

You can change your supervisor password at any time you wish, using the **Security Settings** page of Acer eDataSecurity Management. This is a time-consuming process and involves some degree of risk, and therefore, is not recommended.

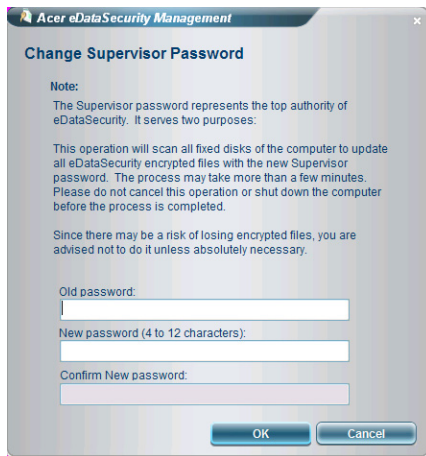
Changing the supervisor password

Step 1: From the Security Settings page, 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.

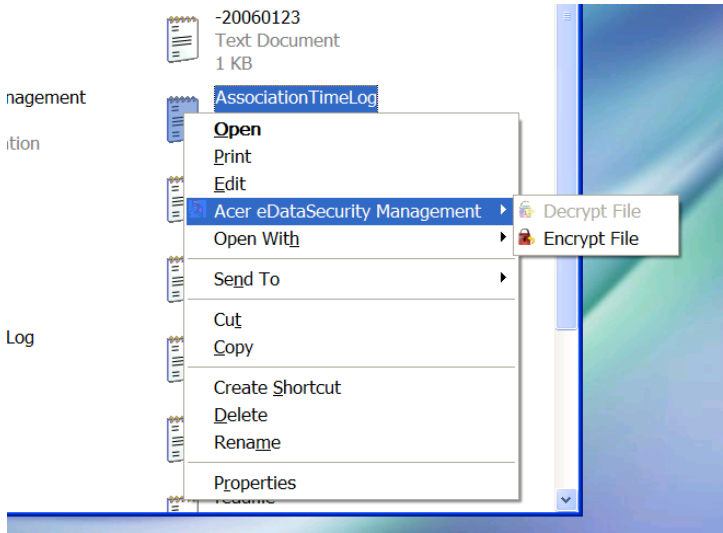
If the program is unable to process all the encrypted files, you will be informed of which files were unable to be processed and the likely reasons why. You will need to close any programs that might be using the encrypted files, and reboot your system. Then click **Retry File Update** to complete the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



Step 5: File update completed.

File and Folder Encryption

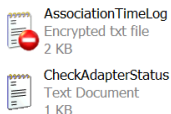
Acer eDataSecurity Management allows you to password-protect personal files and folders, or files sent via instant messenger or email. The file encryption tool is integrated into the right-click context menu of Microsoft Windows, making it easy for you to encrypt or decrypt a file at any time.



When you select a file to encrypt, you will need to specify a password for encryption.

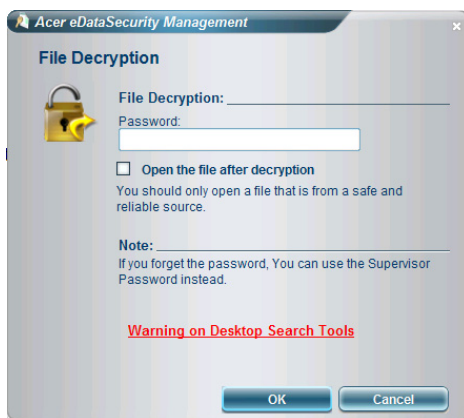


A file that has been encrypted will be displayed with a different icon, and file extension.



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, Microsoft Outlook or Lotus Notes.

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 Microsoft Outlook and Lotus Notes, 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.