Acer eDataSecurity Management

Applicando le tecnologie di crittografia più avanzate, Acer eDataSecurity Management offre agli utenti Acer PC una maggiore protezione dei dati personali e la possibilità di crittografare i file e i dati trasmessi tramite messaggi istantanei o email.

Avvertenza: File da non crittografare:
Per assicurare la massima stabilità del sistema, non crittografare le seguenti cartelle, o i file in esse contenuti:
**** C:\WINDOWS***
**** C:\Cartella del programma***
**** Acer eDataSecurity Management***

La crittografia di suddette cartelle o dei file in esse contenuti potrebbe causare seri problemi di instabilità che potrebbero richiedere la re-installazione del sistema operativo, e la conseguente eliminazione di tutti i dati personali.

Uso di Acer eDataSecurity Management

È possibile avviare Acer eDataSecurity Management in diversi modi:

- Dal menu Start, andare a **Start > (Tutti i) Programmi > Empowering Technology > Acer eDataSecurity Management**.
- Facendo clic sull'icona **Empowering Technology** dal desktop, o premendo il tasto < > è possibile avviare l'interfaccia utente **Empowering Technology**. Selezionare l'icona **Acer eDataSecurity Management** .

Questo consente di aprire la pagina principale di Acer eDataSecurity Management.

Password

Le password configurate sono chiavi di crittografia/decrittografia file. Assicurarsi di conservare le password in un luogo sicuro, e preferire password non facili da intuire.

Configurazione delle password

Prima di utilizzare Acer eDataSecurity Management, è necessario configurare la password di crittografia predefinita e la password supervisore. Durante l'installazione di Acer eDataSecurity Management, o al primo utilizzo, viene richiesta la configurazione di queste password.

Se si dimenticano le password, non è consentito decrittografare o recuperare i dati. Per questa ragione, è importante conservare le password in un luogo sicuro.

Regole per password

Le password selezionate devono avere una lunghezza compresa tra i 4 e i 12 caratteri. Utilizzare esclusivamente lettere, numeri e i seguenti caratteri speciali:

=	Uguale
-	Meno
[	Parentesi quadra aperta
]	Parentesi quadra chiusa
.	Punto
,	Virgola
;	Punto e virgola
/	Barra
\	Barra rovesciata

Password supervisore

La password supervisore può essere utilizzata per decrittografare tutti i file crittografati. Questa rappresenta l'"ultima risorsa" nel caso di perdita della password utilizzata nella crittografia del file. Non consentire a terzi di conoscere la password supervisore.

La password supervisore funziona solo sul computer usato originariamente per crittografare il file.

Importante: La password supervisore può essere utilizzata anche al posto della password predefinita per modificare un'impostazione qualsiasi di Acer eDataSecurity.

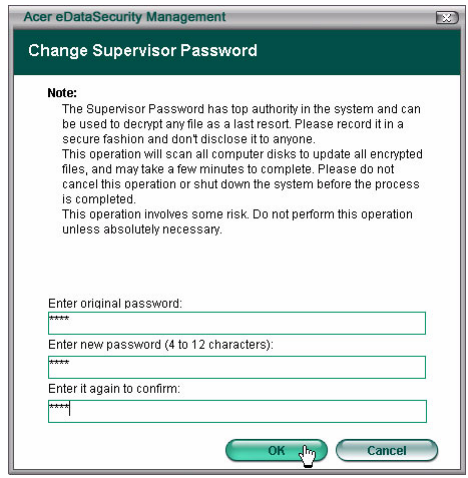
È possibile modificare la password supervisore in qualsiasi momento, dalla finestra di configurazione di sistema; tuttavia, questo processo richiede tempo, e non è privo di rischi.

Modifica della password supervisore

Punto 1: Dalla finestra di impostazioni di sistema, scegliere **Modifica password supervisore**.

Punto 2: Fare clic su **Modifica password supervisore** .

Punto 3: È necessario immettere la password supervisore esistente, quindi immettere due volte la stessa password.

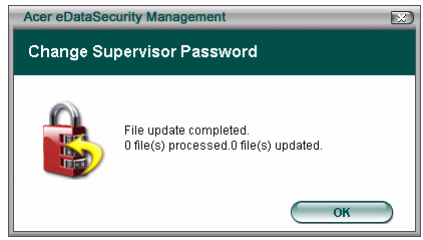


Punto 4: Una volta fatto, Acer eDataSecurity Management esegue la ricerca di tutti i file crittografati, e esegue la modifica.

Evitare di interrompere il processo, o di consentire a Windows® di arrestarsi prima del completamento del processo. In caso contrario, il processo viene portato a termine al successivo avvio del computer.

Se il programma non è in grado di elaborare tutti i file crittografati, l'utente viene informato in merito ai file non elaborati e alle cause di ciò. Chiudere i programmi che potrebbero utilizzare al momento i file crittografati, e riavviare il sistema. Quindi fare clic su **Ripeti aggiornamento file** per completare il processo.

Punto 5: Aggiornamento file completato



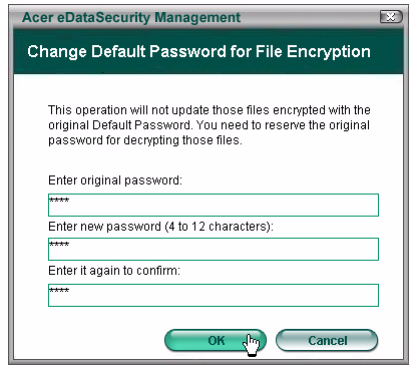
Password di crittografia predefinita

La password di crittografia predefinita è utilizzata per ogni crittografia, a meno di aver specificato una password particolare per ogni tipo di operazione. Per aprire i file crittografati dopo la modifica della password, è necessario immettere la nuova password. Per aprire i file crittografati prima della modifica della password, è necessario immettere la password originale.

Modifica della password predefinita

Punto 1: Fare clic su **Modifica password predefinita per crittografia file**

Punto 2: Immettere la password originale e immettere due volte la nuova password.



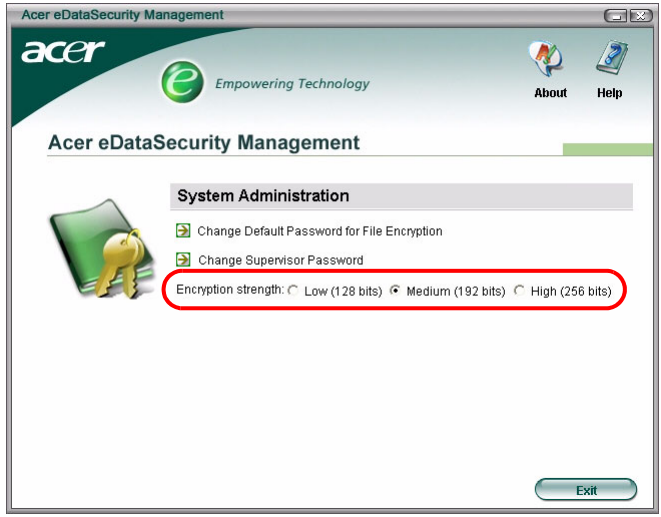
Robustezza crittografia

Acer eDataSecurity Management mette a disposizione tre livelli di crittografia:

- Bassa (128 bit)
- Media (192 bit)
- Alta (256 bit)

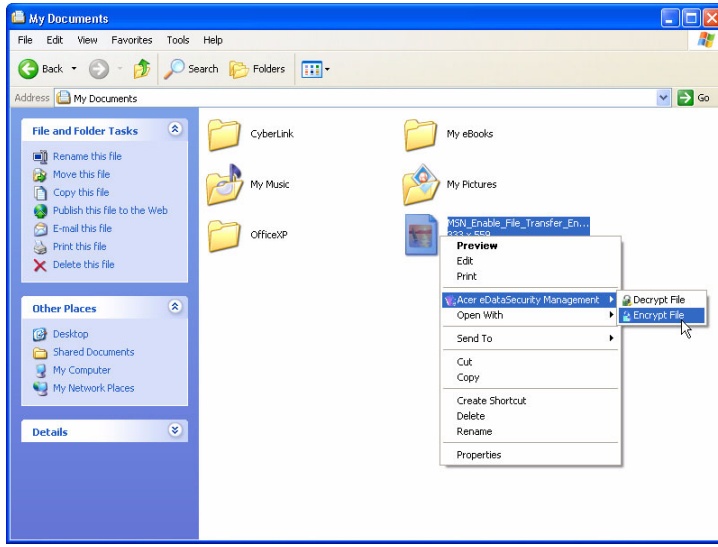
Nota: L'impostazione predefinita è Media.

Tutti e tre i livelli assicurano un elevato grado di protezione, ma è presente una differenza nel tempo impiegato nella crittografia/decrittografia dei file: più elevato è il livello di crittografia scelto, più lungo il tempo di elaborazione.

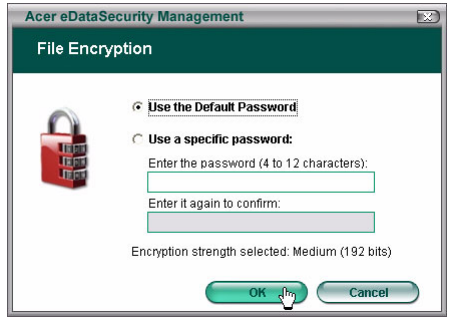


Crittografia file e cartella

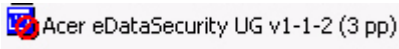
Acer eDataSecurity Management garantisce maggiore protezione di file e cartelle personali protetti da password, o di file inviati tramite messaggi istantanei o email. Lo strumento di crittografia file è integrato nella funzione di clic col tasto destro di Microsoft® Windows®, rendendo semplice eseguire la crittografia/decrittografia di file in qualsiasi momento.



Quando si seleziona un file per eseguirne la crittografia, è necessario scegliere se utilizzare la password di crittografia predefinita, o se specificare una password differente.



Il file crittografato viene visualizzato con un'icona diversa e con l'estensione file.



Decrittografia file e cartella

Fare clic col tasto destro sul file crittografato, e selezionare la funzione Decrittografa. Viene richiesto di immettere la password corretta, e selezionare se aprire o meno il file una volta eseguita la decrittografia. Una volta immessa la password, Acer eDataSecurity procede alla decrittografia del file e, se selezionata l'opzione apposita, apre il file.

Invio a terzi di file crittografati

È possibile scegliere se crittografare file da inviare a terzi utilizzando MSN Messenger o Microsoft® Outlook.

Come impostazione predefinita, Acer eDataSecurity Management attiva la crittografia di file inviati tramite MSN Messenger. Per disattivare questa funzione, aprire MSN Messenger, fare clic su Strumenti e deselezionare Attiva crittografia file da trasferire.

È possibile scegliere di crittografare i file che si desidera inviare tramite email. Acer eDataSecurity Management è integrato nella barra degli strumenti di Microsoft® Outlook, consentendo la crittografia degli allegati con un solo clic.

Il file crittografato viene inviato come file autodecomprimente '.exc', per questo il destinatario non deve essere necessariamente in possesso di Acer eDataSecurity Management per aprire il file. Il destinatario è tenuto a salvare il file sul disco rigido, e modificare l'estensione file in '.exe' prima di procedere alla decrittografia del file medesimo.