EasyLock

Manuale dell’utente

COSOSYS

Sommario

1. Introduzione

La protezione dei dati in transito è essenziale per garantire che nessun terzo ha accesso ai dati in caso di perdita, smarrimento o furto del dispositivo. EasyLock permette l'identificazione dei dispositivi portatili come dispositivi di fiducia (quando viene utilizzato insieme al programma di protezione Endpoint Protector) e protegge i dati sul dispositivo grazie alla crittografia in modalità AES CBC a 256 bit approvata dal Governo.

Mediante l'interfaccia intuitiva Trascina e Rilascia, i file possono essere copiati rapidamente dal e sul dispositivo, garantendo un flusso di lavoro veloce, sicuro ed efficace.

EasyLock è un'applicazione portatile che non richiede alcun'installazione sul PC host, ciò che gli conferisce una massima portabilità. Ovunque vi troverete, EasyLock rimarrà salvato sul dispositivo di archiviazione portatile e potrà essere utilizzato su qualsiasi computer con sistema operativo Windows, MAC o Linux.

2. Requisiti di Sistema

- Windows 7 (tutte le versioni)
- Windows Vista (tutte le versioni)
- Windows XP (Service Pack 2 consigliato)
- Mac OS 10.5 o ulteriore
- Linux - openSUSE 11.2 (compatibilità con altre versioni disponibile su richiesta)

Porta USB disponibile

Dispositivo di archiviazione USB rimovibile dal quale avviare l'applicazione (es. unità di memoria flash USB, hard disk esterno, scheda di memoria ecc.).

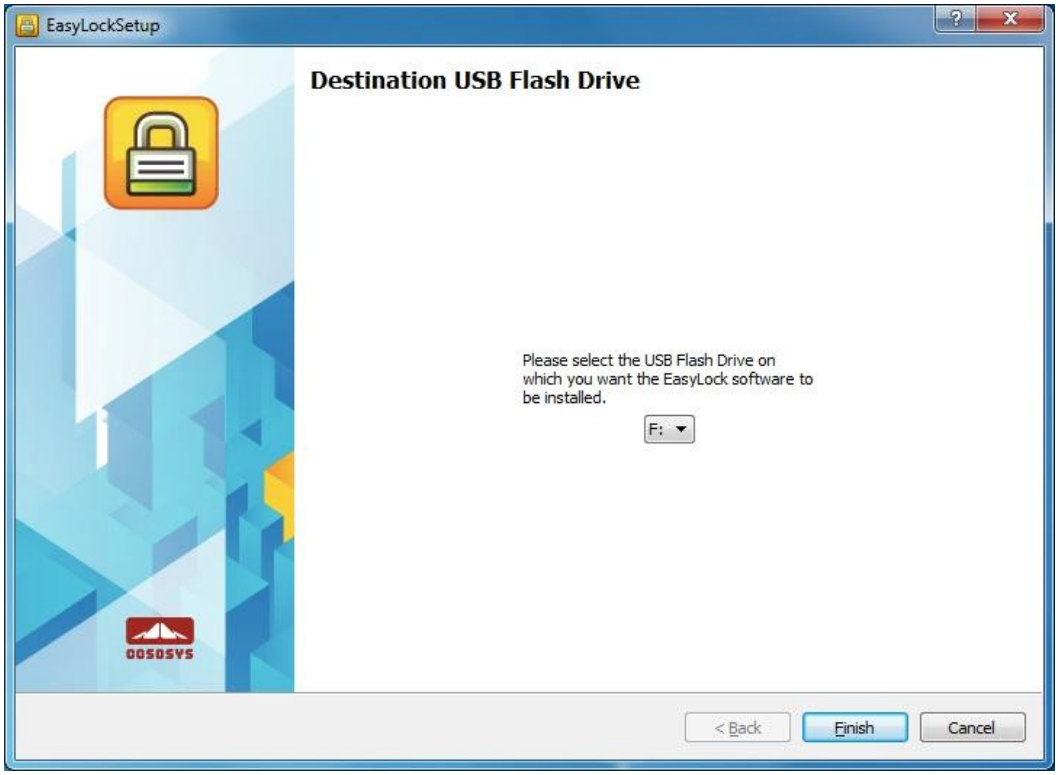
Se il dispositivo di archiviazione portatile è dotato di uno sportello con chiusura di sicurezza, tale sportello dovrà essere in posizione aperta (scrivibile) per poter usare EasyLock.

L'utilizzo di EasyLock non è sottoposto a diritti d'amministrazionebe able to use EasyLock.

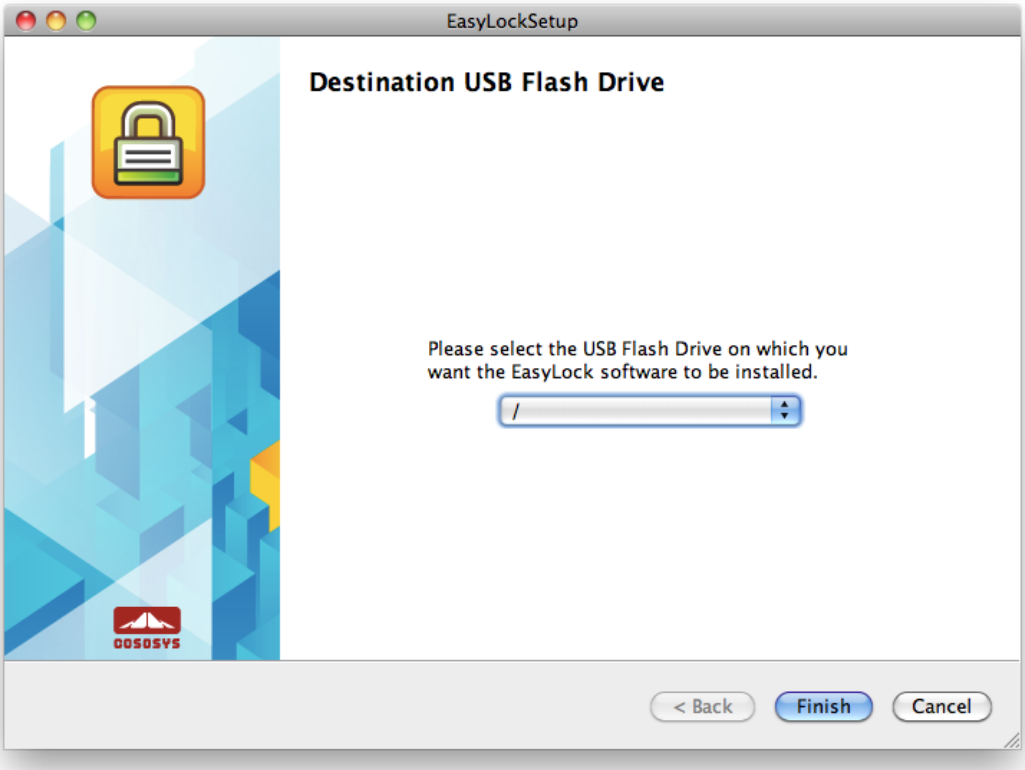
3. Installazione

Per installare EasyLock su un'unità di memoria flash USB (o un altro dispositivo di archiviazione USB portatile):

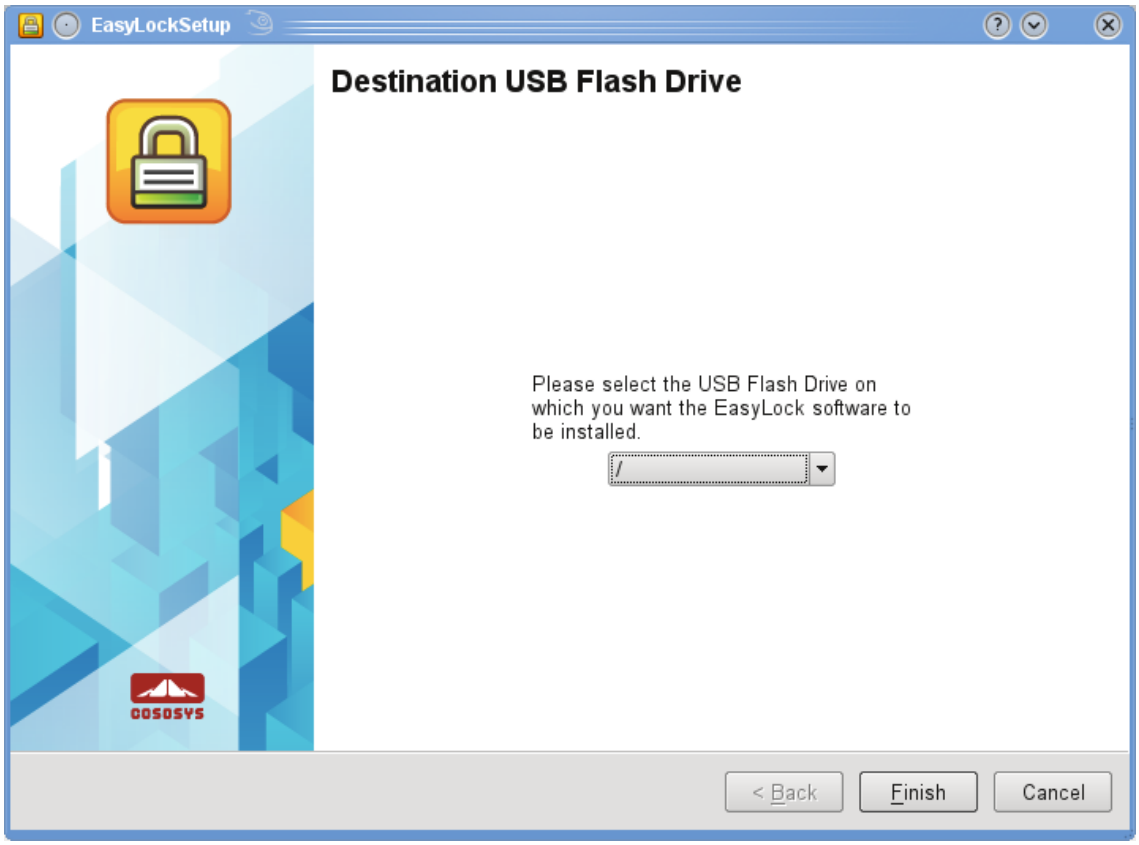
- **Per il sistema operativo Windows:** eseguire il file “EasyLockSetup.exe”, selezionare la lettera di unità corrispondente al dispositivo USB e scegliere <Fine>. L'applicazione EasyLock verrà installata automaticamente nella cartella principale del dispositivo selezionato.



- **Per il sistema operativo MAC:** eseguire il file "EasyLockSetup.dmg", selezionare la lettera di unità corrispondente al dispositivo USB e scegliere <Fine>. L'applicazione EasyLock verrà installata automaticamente nella cartella principale del dispositivo selezionato.



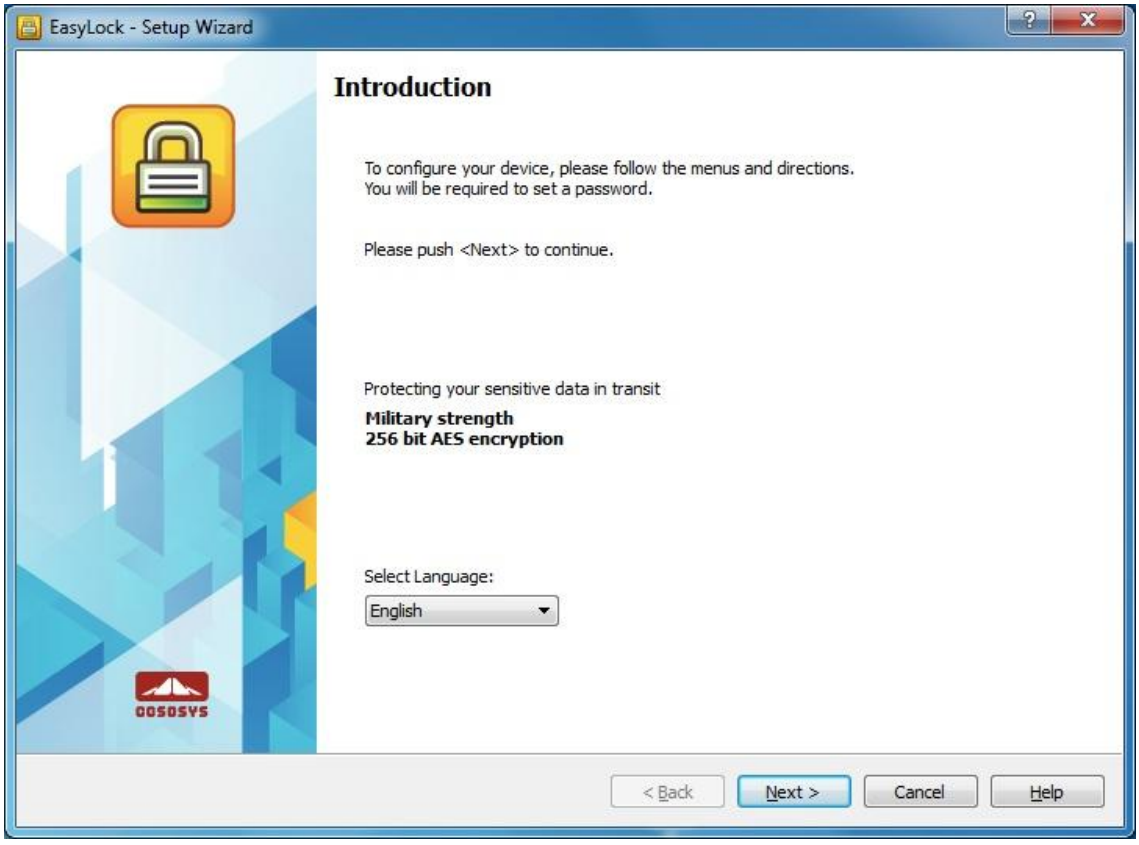
- **Per il sistema operativo Linux:** eseguire il file EasyLockSetup, selezionare la lettera di unità corrispondente al dispositivo USB e scegliere <Fine>. L'applicazione EasyLock verrà installata automaticamente nella cartella principale del dispositivo selezionato.



3.1. Impostazione di EasyLock

Per avviare l'applicazione EasyLock, basta fare doppio clic sul file EasyLock salvato nella cartella principale del dispositivo di archiviazione portatile.

Quando si utilizza il dispositivo di archiviazione portatile come dispositivo di fiducia insieme al programma di protezione Endpoint Protector, il Client PC al quale viene connesso il dispositivo dovrà ricevere l'autorizzazione dal server Endpoint Protector; in caso contrario, il dispositivo non sarà accessibile da un PC protetto da Endpoint Protector o l'applicazione EasyLock non sarà avviata automaticamente.



3.2. Impostare la password

Per garantire la protezione (crittografia) dei propri dati, occorre impostare una password. La password deve contenere almeno 6 (sei) caratteri.

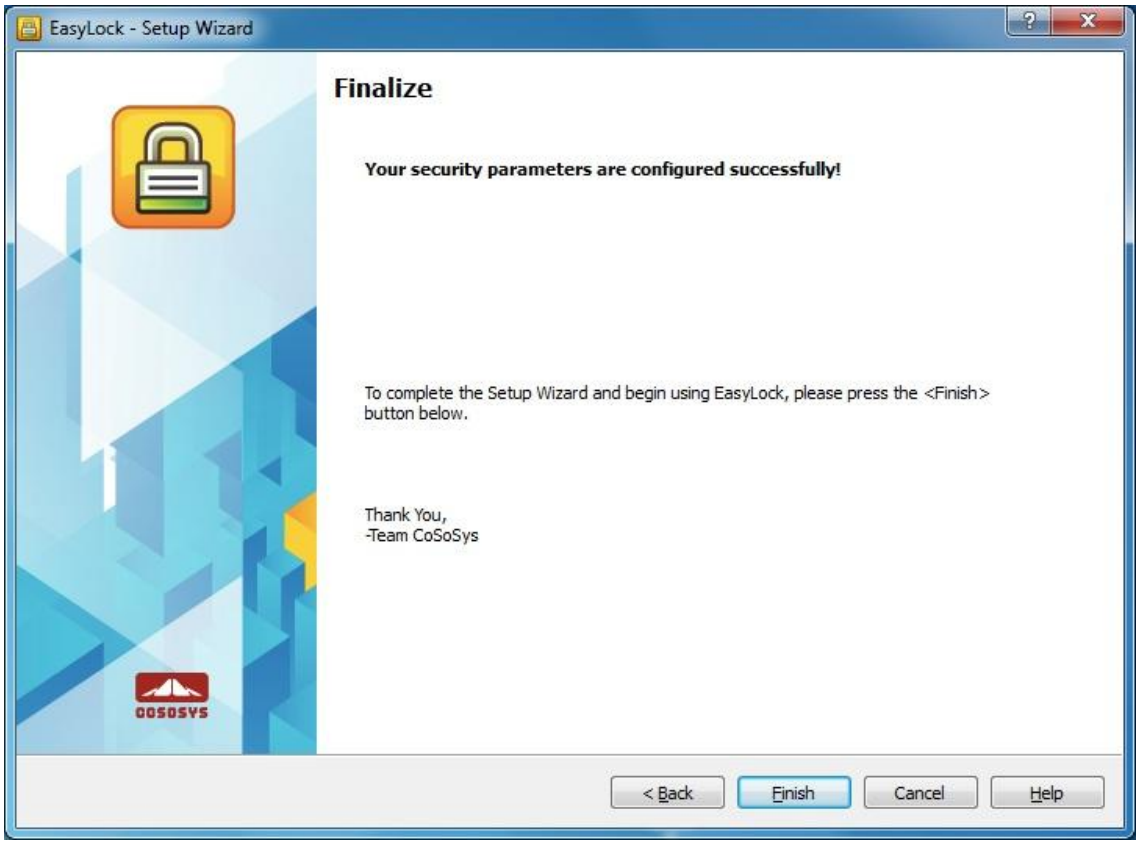
Per ragioni di sicurezza, è consigliato includere lettere, numeri e simboli nella password.

Inserire la password, quindi confermarla.

Si consiglia di impostare anche un promemoria della password da utilizzare qualora dimenticaste la password.

Fare clic su "Avanti" per continuare.

Fare clic su "Fine" per completare l'impostazione della password e iniziare ad utilizzare l'applicazione.



3.3. Tentativi d'inserimento della password

Ad ogni avvio dell'applicazione, verrà richiesto, per motivi di sicurezza, di inserire la propria password.

Per garantire la protezione dei dati in caso di perdita o furto del dispositivo, il numero di tentativi d'inserimento della password è limitato ad un massimo di 10 (dieci). Dopo aver inserito una password errata per 10 (dieci) volte di seguito, EasyLock effettuerà l'eliminazione sicura di tutti i file crittografati salvati sul dispositivo di archiviazione portatile.

Tali dati non potranno essere recuperati o ricreati in seguito. Andranno persi definitivamente.

3.4. Impostazioni di visualizzazione

Nella barra degli strumenti di EasyLock ci sono alcune opzioni per personalizzare il modo di visualizzazione della finestra di EasyLock.

Scambia pannelli – per passare dal pannello dell'unità di memoria USB al pannello di Risorse del computer e viceversa

Mostra/nascondi Pannello di Risorse del computer – per visualizzare il pannello di Risorse del computer

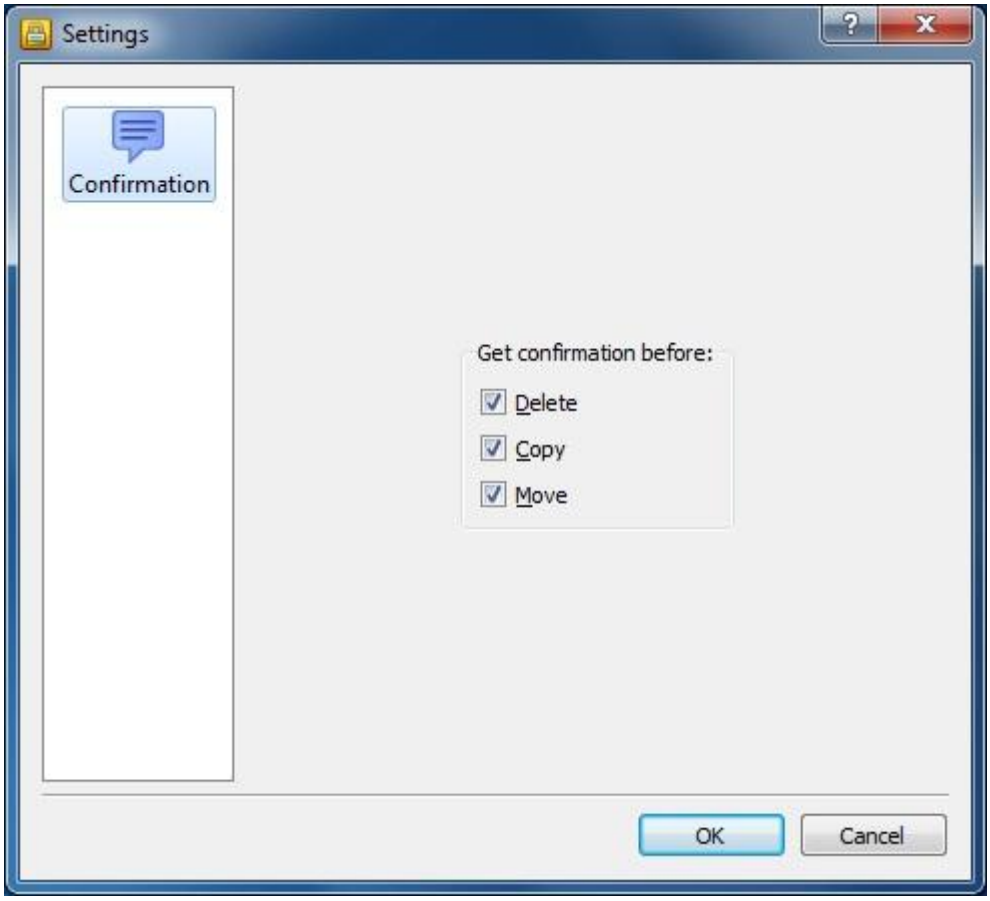
Mostra struttura ad albero – per visualizzare una struttura ad albero dei file

Visualizza dettagli – per visualizzare informazioni aggiuntive sui file

Visualizza elenco – per visualizzare i file nella forma di un elenco

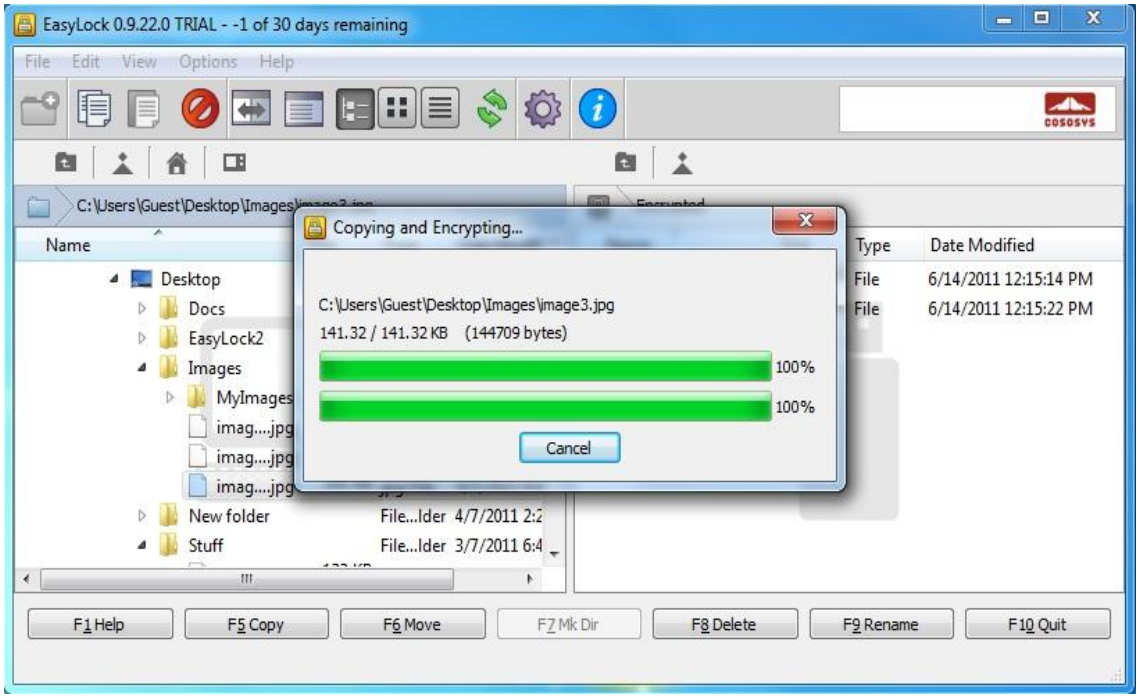
Le varie opzioni disponibili possono essere selezionate anche direttamente dal menu principale, sotto la sezione Visualizza.

E' possibile scegliere se si desidera visualizzare un messaggio di conferma prima di eliminare, copiare o spostare i file.

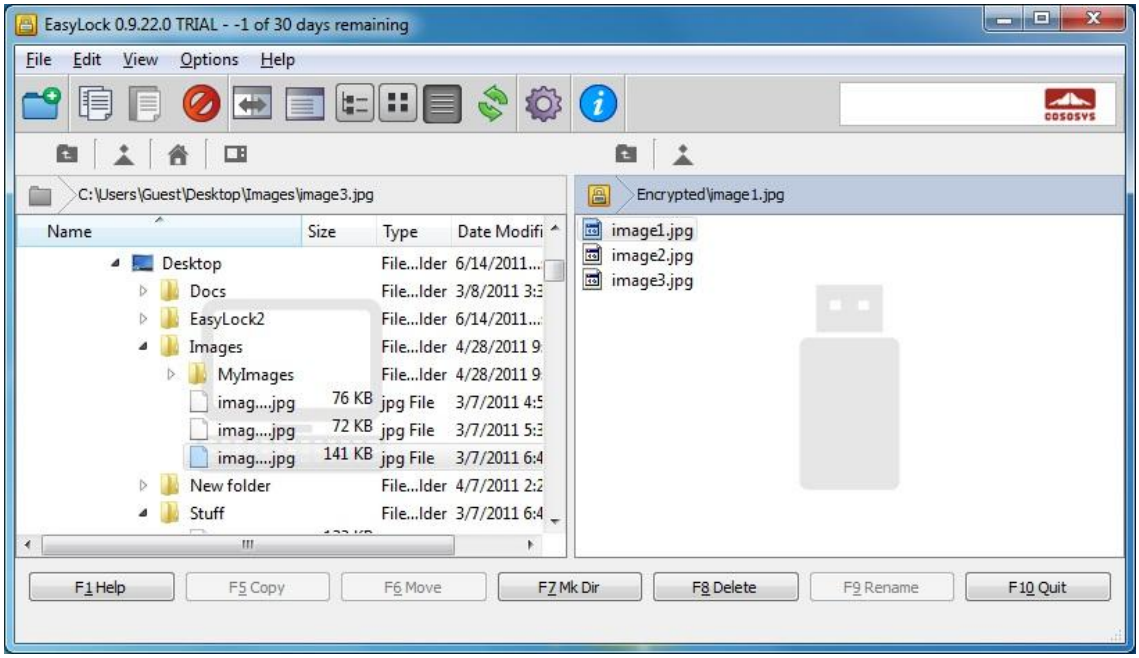


3.5. Utilizzare la funzione Trascina e Rilascia per copiare i file

Una della caratteristiche principali di EasyLock è la funzione Trascina e Rilascia che permette di trascinare semplicemente i file e/o le cartelle che si desidera copiare sul dispositivo e rilasciarle nella finestra di EasyLock. I file copiati vengono crittografati automaticamente, garantendo la protezione e la riservatezza dei dati.



Lo stato della crittografia e del trasferimento dei file può essere visualizzato grazie all'indicatore di stato. Quando l'indicatore arriva alla fine, la copia e la crittografia dei file è stata completata.



Se si fa clic con il pulsante destro del mouse su qualsiasi elemento, vengono visualizzate opzioni come "Aggiorna", "Copia" o "Elimina".

Non è consigliato copiare file dal disco rigido sul dispositivo di archiviazione portatile utilizzando il programma Explorer!

Si consiglia di utilizzare la funzione Trascina e Rilascia o i tasti di scelta rapida copia-incolla (Ctrl+C e Ctrl+V) per trasferire i dati sul dispositivo mediante l'interfaccia di EasyLock.

Sulla barra degli strumenti di EasyLock sono inoltre disponibili delle icone aggiuntive che possono essere utilizzate per copiare e crittografare i file.

Si tenga presente che i file copiati sul dispositivo non saranno visibili dopo essere stati crittografati se l'applicazione EasyLock non è in esecuzione.

Per uscire dall'applicazione EasyLock, fare clic sul menu File e poi su Esci oppure fare semplicemente clic sulla "X" nell'angolo superiore destro della finestra dell'applicazione.

3.6. Aprire e modificare i file con EasyLock

I dati copiati possono essere visualizzati e modificati direttamente all'interno dell'applicazione EasyLock. A tale proposito, utilizzare il comando "Apri" o fare doppio clic sul file desiderato.

L'utente deve aprire i documenti presenti sul dispositivo utilizzando l'applicazione associata. EasyLock tenterà di chiudere i documenti una volta chiusa l'applicazione. Se un documento viene modificato (salvato con lo stesso nome o anche nella stessa cartella), esso verrà crittografato e salvato sul dispositivo. Se un documento viene modificato e salvato ma non può essere crittografato, ad esempio se il dispositivo viene rimosso improvvisamente, esso verrà crittografato al prossimo avvio dell'applicazione EasyLock.

Attenzione !!! Quando l'applicazione EasyLock è avviata dal programma Endpoint Protector come applicazione di fiducia, l'apertura dei documenti dal dispositivo sarà disattivata perché l'applicazione associata non ha accesso ai file.

3.7. Impostazioni di sicurezza

Le impostazioni di sicurezza possono essere modificate mediante l'applicazione EasyLock. Dopo l'accesso, sarà possibile cambiare la password. A tal fine, occorre aprire il menu delle impostazioni di sicurezza. Per accedere al menu, fare clic su Opzioni->Impostazioni di sicurezza sulla barra degli strumenti o premere i tasti di scelta rapida Ctrl + O.

4. Como funziona EasyLock insieme a EPP/MyEPP

Quando l'applicazione EasyLock viene utilizzata su un dispositivo di archiviazione portatile come dispositivo di fiducia (TrustedDevices) di livello 1 insieme al programma Endpoint Protector (o la soluzione SaaS My Endpoint Protector), tutti i dati copiati da un Client PC protetto da Endpoint Protector al dispositivo saranno crittografati.

Utilizzo normale di un dispositivo di fiducia (TrustedDevices) di livello 1.

1. L'utente connette il dispositivo al Client PC protetto da Endpoint Protector.
2. Viene controllata l'autorizzazione del dispositivo (il Client PC comunica con il server Endpoint Protector per controllare l'autorizzazione).
3. Se il dispositivo è un dispositivo di fiducia (TrustedDevices) di livello 1 e l'utente o il computer è autorizzato ad utilizzare tale dispositivo di fiducia di livello 1, l'applicazione software EasyLock salvata sul dispositivo sarà avviata automaticamente.
4. L'utente può trasferire dei file nell'applicazione EasyLock con il metodo Trascina e Rilascia.
5. I dati trasferiti sui dispositivi sono crittografati in modalità AES a 256 bit.
6. L'utente non può accedere al dispositivo direttamente utilizzando Windows Explorer o un'applicazione simile (es. Total Commander); questo serve a impedire la copia di dati non crittografati correttamente sul dispositivo portatile.

7. L'utente non ha la possibilità di copiare dati non crittografati sul dispositivo di fiducia (TrustedDevices) (connesso ad un Client PC protetto da Endpoint Protector).

8. Se nel programma Endpoint Protector vengono attivate le funzionalità di traccia e shadowing dei file, tutti i trasferimenti di file da un Client PC protetto da Endpoint Protector al dispositivo saranno registrati. Inoltre saranno registrate tutte le operazioni di eliminazione o rinomina dei file.

9. Gli amministratori potranno in seguito controllare quale utente, con quale dispositivo e su quale PC ha trasferito i vari file.

Un dispositivo di fiducia (TrustedDevices) che non ottiene l'autorizzazione da Endpoint Protector non potrà essere utilizzato dall'utente. Il dispositivo sarà bloccato e l'utente non lo potrà aprire.

4.1. Traccia dei file sui dispositivi di fiducia (TrustedDevices) EasyLock

La traccia dei file sui dispositivi di fiducia (TrustedDevices) EasyLock e una nuova funzionalità del programma Endpoint Protector 4 utilizzato insieme ad EasyLock, che permette di monitorare i file copiati in maniera crittografata sui dispositivi portatili.

All'attivazione della Funzionalità di traccia, tutti i dati trasferiti da e sui vari dispositivi utilizzando EasyLock verranno registrati e salvati per controllo ulteriore. Le informazioni registrate sono inviate automaticamente al Server di Endpoint Protector se il computer in uso dispone del programma Endpoint Protector e di una connessione a Internet.

In assenza del programma Endpoint Protector, le informazioni sono salvate localmente sul dispositivo in formato crittografato e saranno inviate in seguito da qualsiasi altro computer che ha installato il programma Endpoint Protector.

Per più informazioni sull'attivazione e l'utilizzo della funzionalità di traccia sui dispositivi di fiducia (TrustedDevices) EasyLock, consultare il Manuale utente di Endpoint Protector 4.

NOTA

La funzionalità di traccia per i dispositivi di fiducia (TrustedDevices) EasyLock è attualmente disponibile soltanto per il sistema operativo Windows.

5. Configurazione dei TrsutedDevices per l'uso insieme a EPP/MyEPP

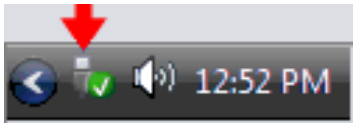
Per informazioni sulla configurazione dei dispositivi di fiducia per l'uso insieme a Endpoint Protector, consultare il Manuale utente di Endpoint Protector.

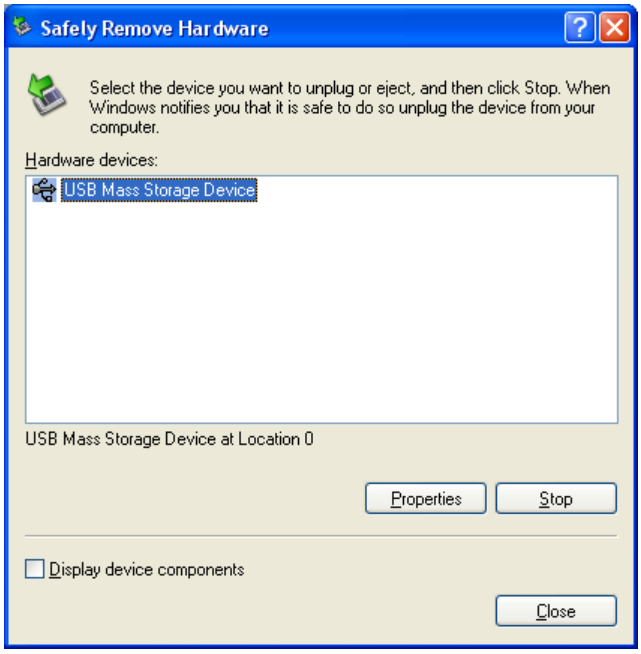
Per sapere di più su Endpoint Protector, visitare il sito:
www.EndpointProtector.com

6. Rimozione sicura dell'hardware

Prima di scollegare il dispositivo di archiviazione portatile dalla porta USB del computer, occorre utilizzare l'opzione "Rimozione sicura dell'hardware" presente sull barra delle applicazioni; in caso contrario, si rischia di danneggiare i dati presenti sull'unità di memoria USB.

Per effettuare la rimozione sicura dell'hardware, fare doppio clic sulla relativa icona nella barra delle applicazioni, quindi selezionare dall'elenco l'unità di memoria USB che si vuole rimuovere e fare clic su "Disattiva".





Verrà visualizzato un messaggio che informa l'utente che è possibile ora rimuovere il dispositivo di archiviazione portatile senza problemi. Se viene visualizzato il messaggio "Impossibile rimuovere il dispositivo '...' ", occorre chiudere Windows Explorer, EasyLock o qualsiasi altra applicazione che sta ancora utilizzando i dati dell'unità di memoria USB.

7. Supporto Tecnico

Se si ha bisogno di ulteriore assistenza come per esempio assistenza tramite e-mail o consultazione delle Domande frequenti, è possibile visitare direttamente il sito di supporto tecnico http://www.cososys.com/help.html

Avviso Importante / Declinazione di responsabilità

Se si ha bisogno di ulteriore assistenza come per esempio assistenza tramite e-mail o consultazione delle Domande frequenti, è possibile visitare direttamente il sito di supporto tecnico http://www.cososys.com/help.html

8. Avviso Importante / Declinazione di responsabilità

I sistemi di sicurezza sono, per natura, suscettibili a circonvenzione. CoSoSys non garantisce e non può garantire che i dati o i dispositivi non saranno violati da persone non autorizzate e CoSoSys declina qualsiasi responsabilità a tale proposito, nei limiti consentiti dalla legge.