EasyLock

Manual do Usuário Versão 2.0.0.0

Manual do Usuário

COSOSYS

Sumário

1. Introdução

A proteção dos dados em trânsito é essencial para garantir que nenhum terceiro ganha acesso aos seus dados caso um dispositivo seja perdido, posto em lugar errado ou roubado. EasyLock permite aos dispositivos portáteis serem identificados como TrustedDevices (Dispositivos Confiáveis) (por combinação com Endpoint Protector) e protege os dados do dispositivo por meio duma criptografia AES modo CBC de 256 bits, aprovado pelo Estado.

Com a sua interface intuitiva de tipo "Arrastar e Soltar", os arquivos podem ser copiados no dispositivo e fora do dispositivo muito rápido, para poder assegurar um fluxo de trabalho rápido, seguro e eficiente.

EasyLock é um aplicativo portátil que não precisa de nenhum processo de instalação para o PC host, mantendo-se sempre portátil. O EasyLock é salvo no dispositivo, e vai para onde ele vai, podendo ser usado de qualquer computador com Windows, MAC ou Linux.

2. Requisitos do Sistema

Sistemas operacionais:

Windows 7 (todas as versões)

Windows Vista (todas as versões)

Windows XP (Service Pack 2 é recomendado)

Mac OS 10.5 ou uma versão mais nova

Linux - openSUSE 11.2 (outras distribuições podem ser disponíveis sob demanda)

Porta USB disponível

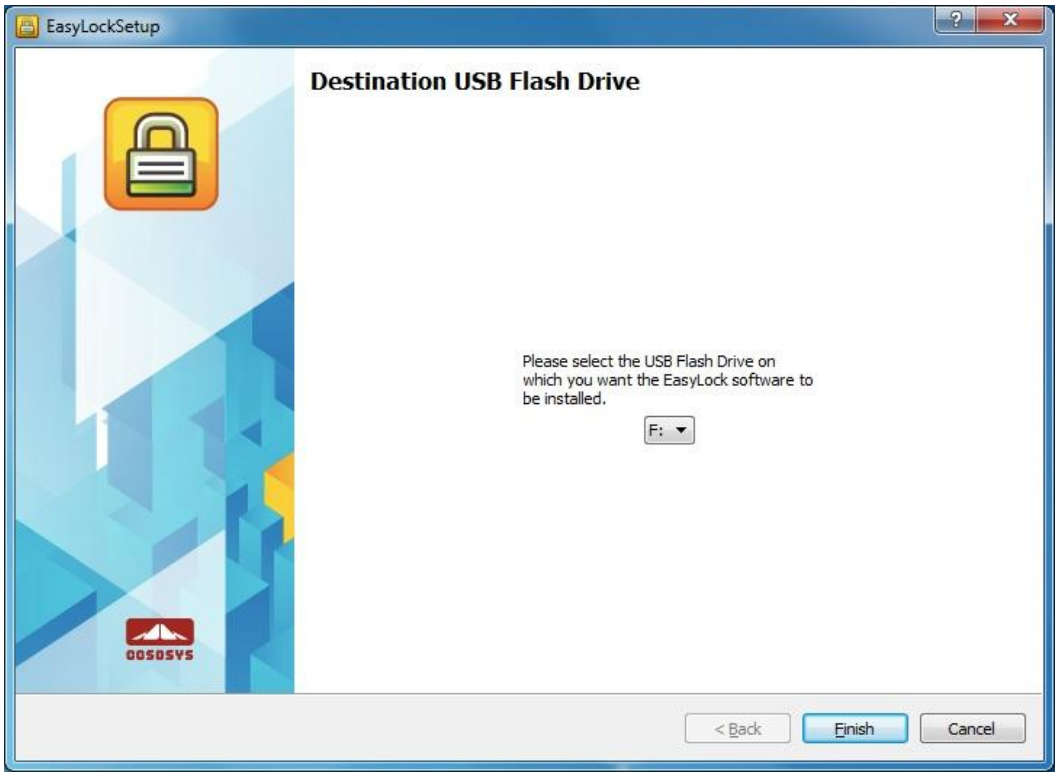
Um Dispositivo USB Removível de Memória que contenha o aplicativo (ex. unidade flash USB, Unidade HDD Externa, Cartão de Memória etc.).

Se o dispositivo portátil de memória tiver um comutador manual de proteção contra a gravação (bloqueio), este comutador deve permanecer na posição "sem proteção" (gravável), para que o EasyLock possa ser usado. EasyLock não requere direitos administrativos.

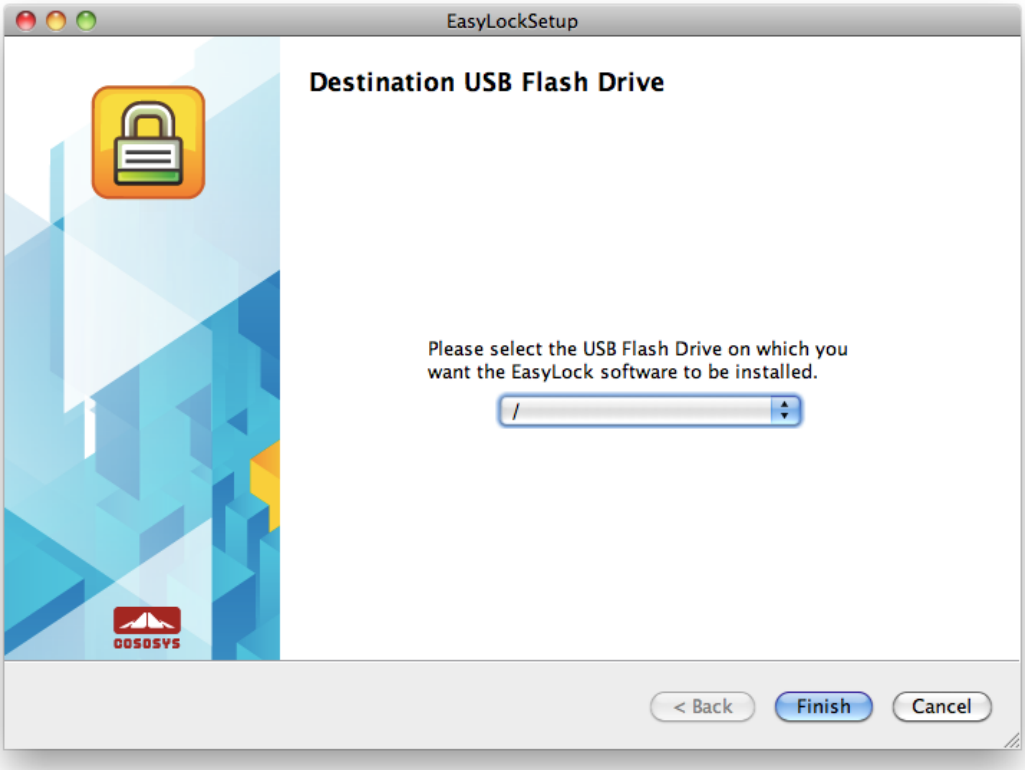
3. Instalação

Para instalar o EasyLock numa unidade flash USB (ou qualquer outro dispositivo USB portátil de memória):

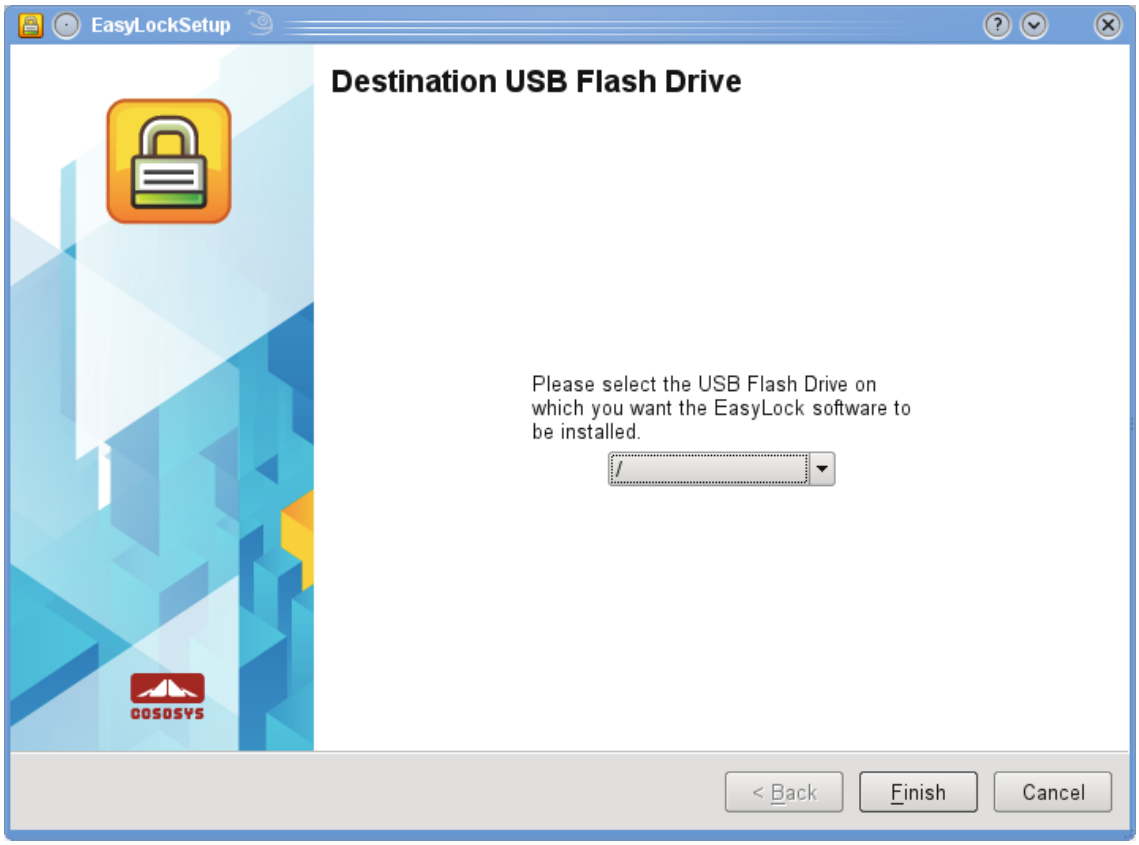
- **Para Windows OS**: execute o arquivo "EasyLockSetup.exe", selecione a letra correspondente à unidade USB e clique em <Acabar>. O aplicativo EasyLock será instalado automaticamente no diretório raiz do dispositivo selecionado.



- **Para MAC OS**: execute o arquivo "EasyLockSetup.dmg", selecione a letra correspondente à unidade USB e clique em <Acabar>. O aplicativo EasyLock será instalado automaticamente no diretório raiz do dispositivo selecionado.



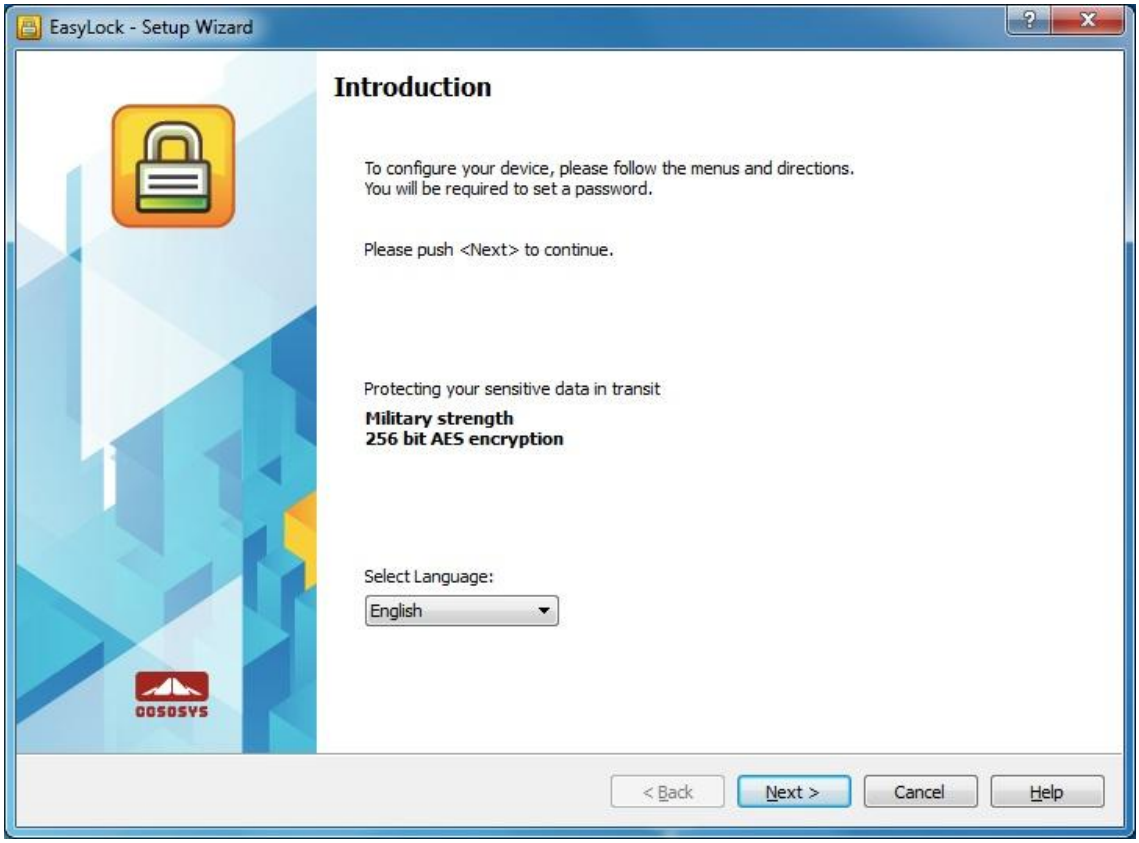
- **Para Linux OS**: execute o arquivo EasyLockSetup, selecione a letra correspondente à unidade USB e clique em <Acabar>. O aplicativo EasyLock será instalado automaticamente no diretório raiz do dispositivo selecionado.



3.1. Configurar o EasyLock

Para iniciar o EasyLock simplesmente clique duas vezes no arquivo EasyLock salvo no diretório raiz do dispositivo portátil de memória.

Quando você estiver a usar o dispositivo como TrustedDevice (Dispositivo Confiável) por combinação com o Endpoint Protector, o PC Cliente ao qual o dispositivo está conectado deve ter recebido uma autorização do Servidor do Endpoint Protector; em caso contrário, o dispositivo não será acessível num PC protegido por Endpoint Protector, ou o EasyLock não será iniciado automaticamente.



3.2. Configurar uma senha

Para segurar (criptografar) os seus dados, é necessário configurar uma senha. A senha deve ter pelo menos 6 (seis) caracteres.

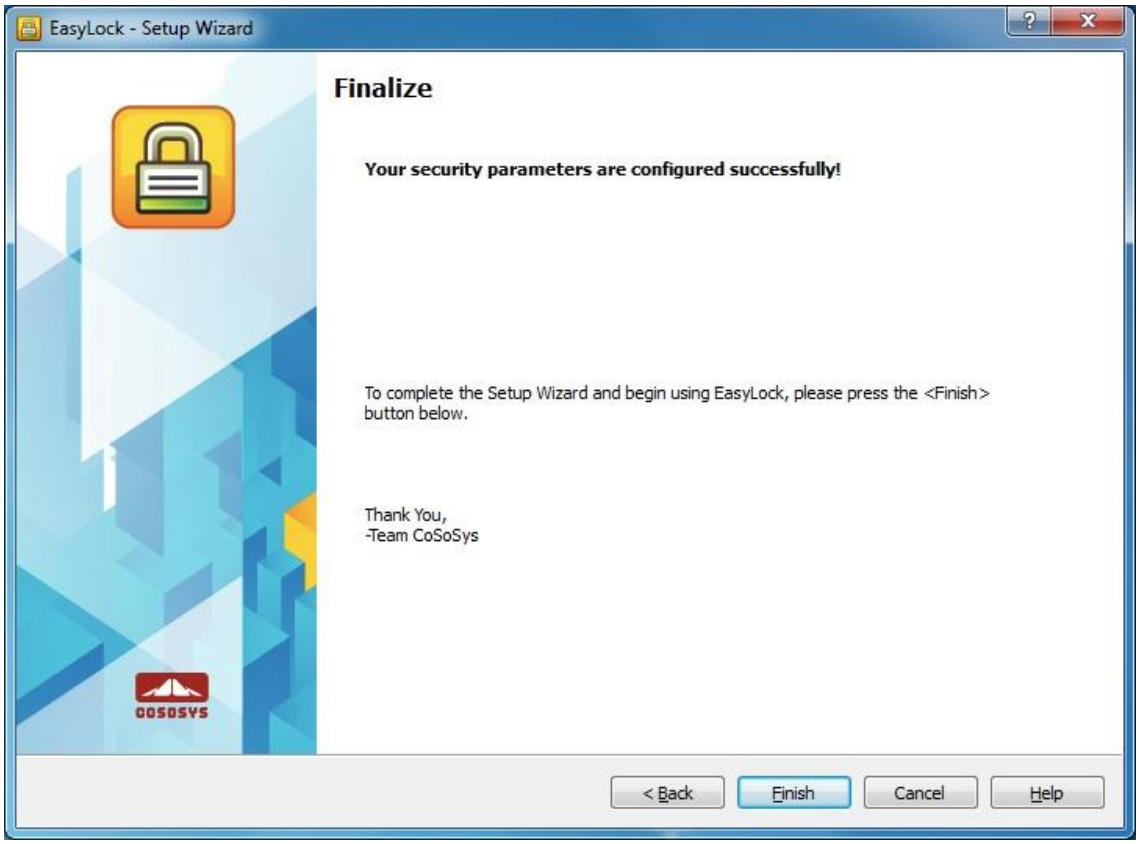
Por motivos de segurança, recomendamos incluir letras, números e símbolos na sua senha.

Digite a sua senha, depois confirme a senha.

Recomendamos também configurar um lembrete para a senha, que pode ajudar se você esquecer a senha.

Clique em “Avançar” para continuar.

Clique em "Finalizar" para finalizar as configurações da senha e começar usar o aplicativo.



3.3. Tentativas para a senha

Cada vez, ao iniciar o aplicativo, você terá de digitar a sua senha, por motivos de segurança.

Caso o seu dispositivo seja perdido ou roubado, o número de tentativas para a senha será limitado a 10 (dez). Se uma senha errada for digitada por 10 (dez) vezes consecutivas, o EasyLock apagará todos os arquivos criptografados depositados no dispositivo portátil de memória.

Ulteriormente, os dados do dispositivo portátil de memória não poderão ser recuperados ou recriados. Eles serão apagados permanentemente.

3.4. Configurações de exibição

Na área da barra de ferramentas do EasyLock há várias opções disponíveis para personalizar a janela de exibição do EasyLock.

Alternar Painéis – para alternar a exibição dos painéis Unidade USB e Meu Computador.

Mostrar ou ocultar o Painel Meu Computador – para exibir o Painel Meu Computador

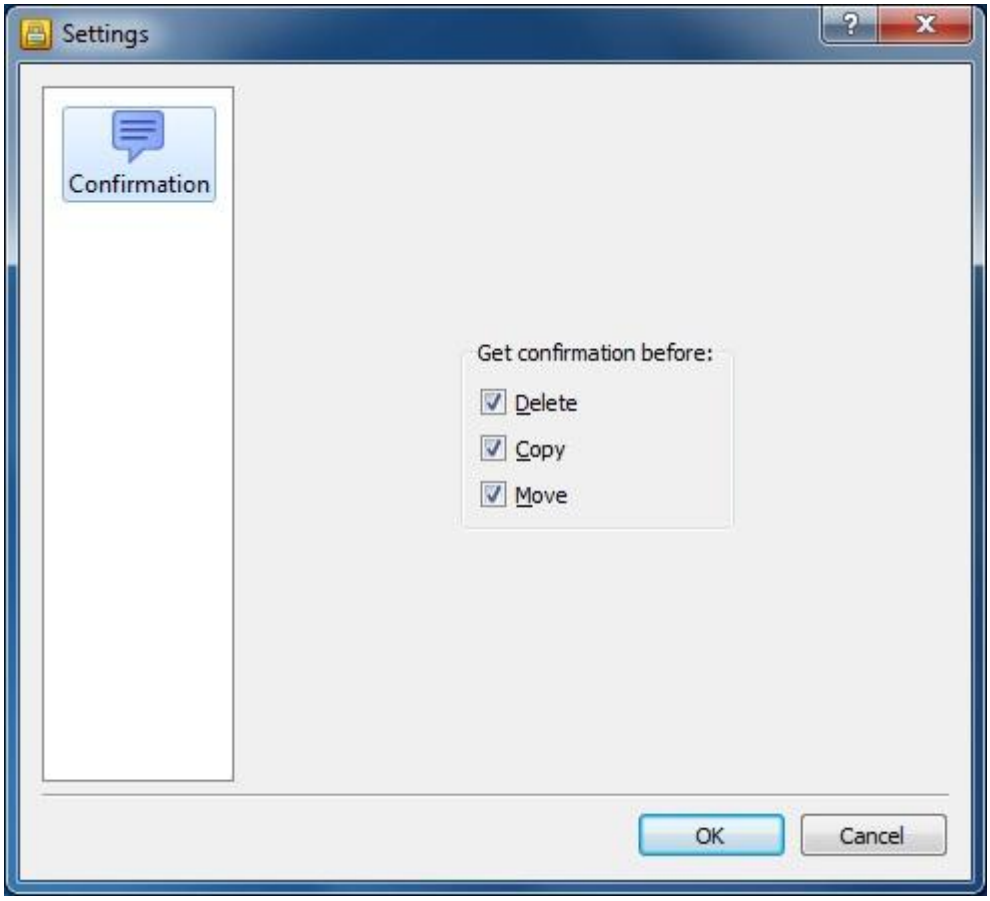
Mostrar Modo de Exibição de Árvore – para exibir uma estrutura semelhante a uma árvore

Mostrar Exibição Detalhada – para mostrar informações adicionais sobre os arquivos

Mostrar Exibição de Lista – para exibir os elementos dentro de uma lista

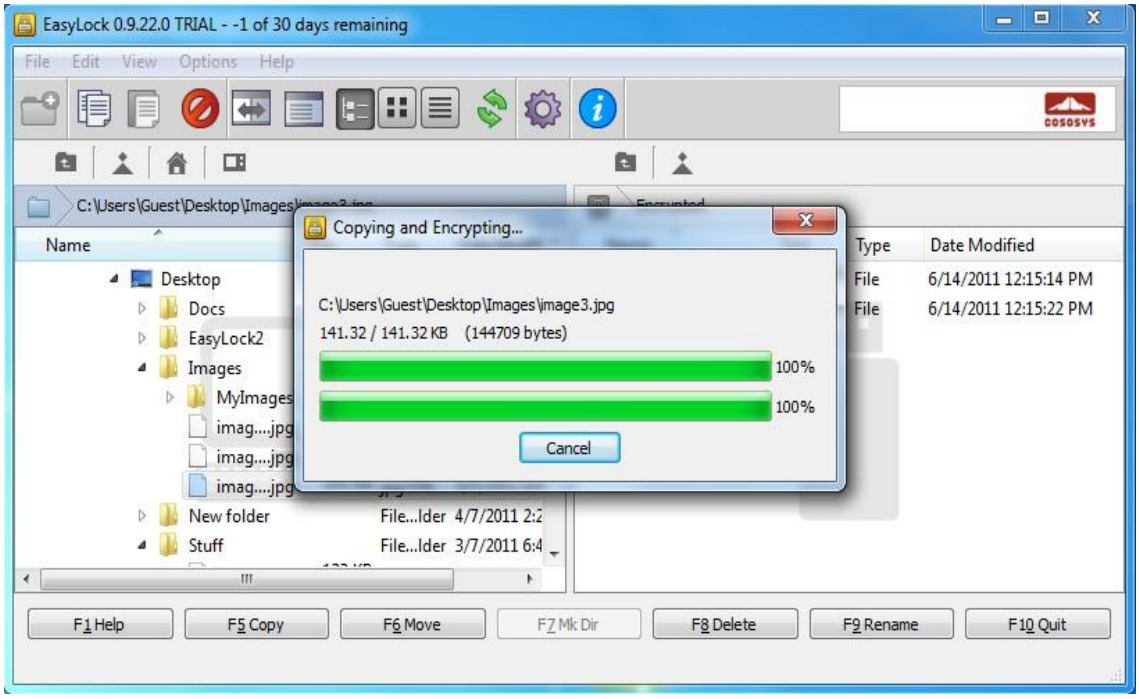
As opções disponíveis podem ser selecionadas também do menu principal, da seção Exibição.

Pode escolher se uma mensagem de confirmação será exibida antes de excluir, copiar ou mover arquivos.

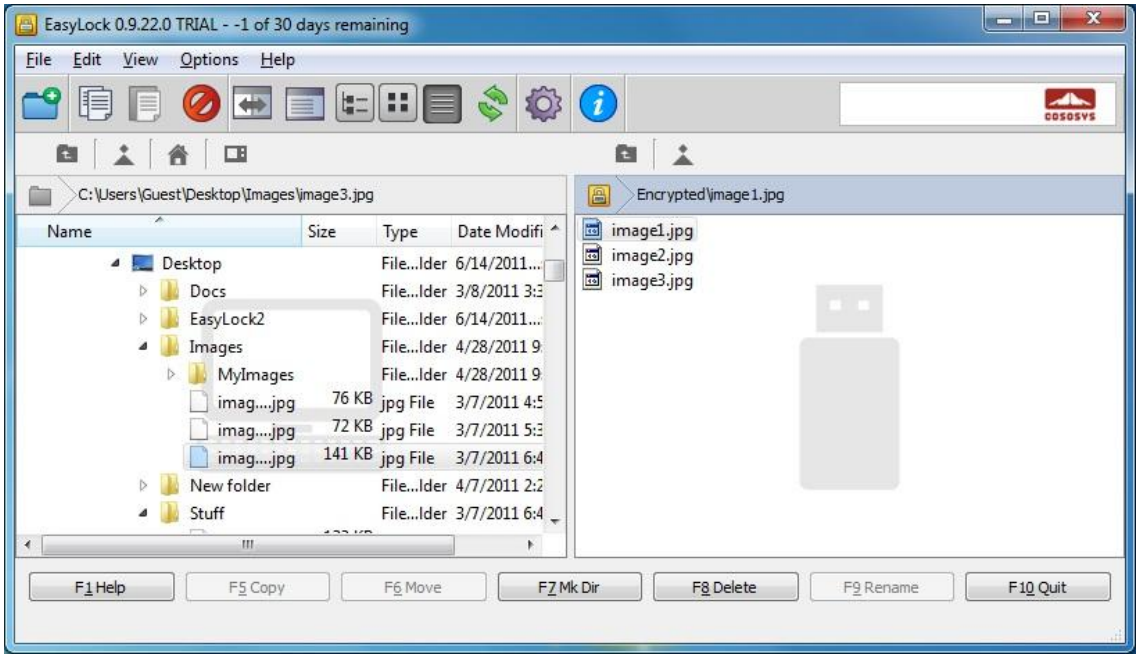


3.5. Usar "Arrastar e Soltar" para copiar arquivos

Um recurso principal do EasyLock é a funcionalidade "Arrastar e Soltar"; você pode simplesmente arrastar o(s) arquivo(s) e/ou diretório(s) que quer copiar para o dispositivo e soltá-los na janela do EasyLock. Estes arquivos serão criptografados automaticamente, garantindo a segurança e privacidade dos seus dados.



O status da criptografia e da transferência do arquivo pode ser visto na barra de progresso. Quando a barra chegar ao fim, os seus arquivos já são copiados e criptografados.



Se fizer clique em qualquer elemento com o botão direito do mouse, terá acesso a opções como "Atualizar", "Copiar" ou "Excluir".

Não recomendamos copiar arquivos da sua unidade HDD para o dispositivo portátil de memória usando o Explorer!

Recomendamos usar a funcionalidade "Arrastar e Soltar" ou as teclas de atalho para copiar e colar, Ctrl+C e Ctrl+V para transferir dados no seu dispositivo usando a interface EasyLock.

Na área da barra de ferramentas do EasyLock pode encontrar vários ícones adicionais que pode usar para copiar e criptografar os seus arquivos.

Ressaltamos que os arquivos do dispositivo não serão visíveis depois da criptografia, a não ser que o EasyLock esteja ativo.

Para sair do EasyLock, selecione o menu Arquivo e escolha Sair, ou clique simplesmente no botão "X" do canto superior direito na janela do aplicativo.

3.6. Abrir e alterar arquivos dentro de EasyLock

Os dados copiados no dispositivo podem ser vistos e editados direto do EasyLock. Esta função pode ser acessada pelo comando "Abrir" ou clicando duas vezes no arquivo desejado.

O usuário deve abrir os documentos do dispositivo com o aplicativo associado. EasyLock tentará fechar estes documentos depois de sair do aplicativo. Se um documento for alterado (salvo com o mesmo nome ou no mesmo diretório) será criptografado e depositado no dispositivo. Se um documento for alterado e salvo, mas a sua criptografia tiver falhado, por exemplo, se o dispositivo tiver sido desconectado inesperadamente, o documento será criptografado a próxima vez que o EasyLock será iniciado.

Atenção!!! Se o EasyLock for iniciado por Endpoint Protector como aplicativo confiável, a opção para abrir documentos do dispositivo será desativada, porque o aplicativo associado não tem acesso aos arquivos.

3.7. Configurações de segurança

As configurações de segurança podem ser alterados do EasyLock. Depois de fazer logon, você pode alterar a sua senha. Por isso precisa acessar o menu de configurações de segurança. Isto pode acontecer ao selecionar Opções-> Configurações de Segurança da barra de ferramentas ou ao clicar na tecla de atalho Ctrl + O.

4. O funcionamento do EasyLock com o EPP ou MyEPP

Se o EasyLock for usado num dispositivo portátil de memória como TrustedDevice Level 1 (Dispositivo Confiável de Nível 1), por combinação com Endpoint Protector (ou My Endpoint Protector, a Solução SaaS hospedada), ele garantirá que todos os dados copiados dum PC Cliente protegido por Endpoint Protector para o dispositivo serão criptografados.

O cenário normal para o uso dum TrustedDevice Level 1 é.

1. O usuário conecta o dispositivo ao PC Cliente protegido por Endpoint Protector.

2. O dispositivo é verificado, buscando-se a autorização (o PC Cliente está a comunicar com o Servidor Endpoint Protector para buscar a autorização).

3. Se o dispositivo for um TrustedDevice Level 1, e o Usuário ou a Máquina tiver autorização para usar TrustedDevices Level 1, o software EasyLock do dispositivo será iniciado automaticamente.

4. O usuário pode transferir arquivos por "Arrastar e Soltar" no EasyLock.

5. Os dados transferidos para o dispositivo são criptografados via 256bit AES.

6. O usuário não pode acessar o dispositivo diretamente, usando Windows Explorer ou outros aplicativos semelhantes (ex. Total Commander), para garantir que nenhum dado é copiado no dispositivo portátil sem ser devidamente criptografado.

7. O usuário não tem a possibilidade de copiar dados não criptografados para o TrustedDevice (num PC Cliente protegido por Endpoint Protector).

8. Todas as transferências de arquivos do PC Cliente protegido por Endpoint Protector para o dispositivo podem ser registrados se as opções Rastreamento e Sombreamento de Arquivos forem ativos no Endpoint Protector. Ações como excluir ou renomear arquivos são registrados, também.

9. Ulteriormente, os administradores podem fiscalizar qual usuário transferiu quais arquivos, usando qual dispositivo e para qual PC.

Se um TrustedDevice não obtiver a autorização do Endpoint Protector, ele não será utilizável para o usuário. O dispositivo será bloqueado e o usuário não terá acesso ao dispositivo.

4.1. O Rastreamento de Arquivos para TrustedDevices com EasyLock

O Rastreamento de Arquivos para TrustedDevices com EasyLock é um novo recurso do Endpoint Protector 4, usado por combinação com EasyLock, que permite monitorizar os arquivos copiados por meio de criptografia para dispositivos portáteis.

Se a opção Rastreamento de Arquivos for ativa, todos os dados transferidos de e para os dispositivos que usam EasyLock serão registrados e salvados num log, para poderem ser fiscalizados. As informações salvas no log serão transmitidas automaticamente para o Servidor do Endpoint Protector, se o Cliente do Endpoint Protector for presente naquele computador e uma conexão à Internet for disponível.

Se o respectivo Cliente do Endpoint Protector não for presente, as informações serão depositadas localmente num formato criptografado no dispositivo, e serão transmitidas mais tarde de qualquer outro computador com um Cliente de Endpoint Protector instalado.

Para mais detalhes relativos à ativação e o uso do Rastreamento de Arquivos para TrustedDevices com EasyLock, por favor consulte o Manual do Usuário do Endpoint Protector 4.

Note

No momento, o recurso para Rastreamento de Arquivos para TrustedDevices com EasyLock é disponível somente para Windows OS.

5. Configurar o uso do TrustedDevice no EPP ou MyEPP

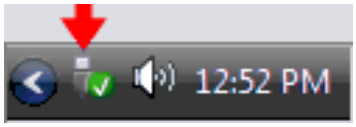
Para perceber como configurar o uso do TrustedDevice junto com o Endpoint Protector, por favor consulte o Manual do Usuário do Endpoint Protector.

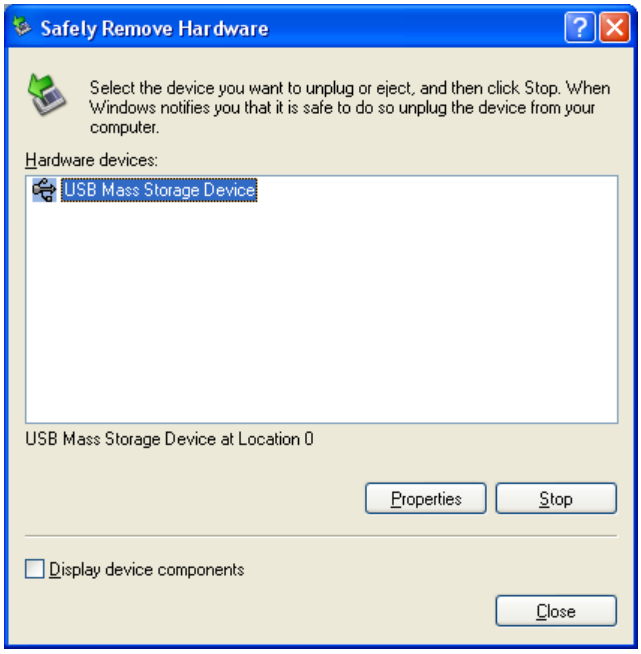
Para saber mais sobre Endpoint Protector, visite: www.EndpointProtector.com

6. Remover Hardware com Segurança

Antes de desconectar o dispositivo portátil de memória da porta USB do seu computador, você deve usar a opção "Remover Hardware com Segurança" da Bandeja do Sistema. Em caso contrário, há um risco de corromper os dados da sua unidade USB.

Para Remover Hardware com Segurança, clique duas vezes no ícone da Bandeja do Sistema, depois selecione a unidade USB que deseja remover da lista e clique no botão "Parar".





Uma mensagem vai aparecer, indicando que o dispositivo portátil de memória pode ser removido com segurança. Se uma mensagem com o conteúdo "O dispositivo '...', não pode ser parado neste momento" aparecer, você deverá fechar o seu Windows Explorer, o EasyLock ou qualquer outro aplicativo que esteja a acessar os dados na sua unidade USB.

7. Suporte

Se precisar mais ajuda, como, por exemplo, as Perguntas Frequentes ou suporte por e-mail, pode visitar o sítio Web de suporte em
http://www.cososys.com/help.html

8. Aviso importante/ Aviso de isenção de responsabilidade

As guardas de segurança são passiveis de engano, pela sua natureza. CoSoSys não pode garantir e não garante que os dados ou os dispositivos não serão acessado por pessoas não autorizadas, e CoSoSys declara-se completamente isento de todas as garantias neste sentido, até aos limites estabelecidos pela lei.