



# EasyLock

Benutzerhandbuch Version 2.0.0.0

# Benutzerhandbuch



## Inhaltsverzeichnis

1. Einführung .....	1
2. Systemanforderungen.....	2
3. Installation.....	3
3.1. EasyLock Einrichten.....	6
3.2. Passwort Eingeben .....	7
3.3. Passwort Eingabe bei Login .....	9
3.4. Bedienoberfläche Einstellungen.....	9
3.5. Drag & Drop beim Kopieren der Dateien .....	10
3.6. Das Öffnen und Verändern der Dateien mit EasyLock .....	12
3.7. Sicherheitseinstellungen .....	13
4. Wie EasyLock mit EPP oder My EPP funktioniert	
14	
4.1. Daten Protokollierung auf EasyLock TD .....	15
5. TrustedDevice Konfigurierung auf EPP oder	
MyEPP.....	16
6. Hardware Sicher Entfernen .....	17
7. Support .....	19
8. Wichtige Anmerkungen / Disclaimer.....	20

# 1. Einführung

Verschlüsselung beim Transfer von Daten ist unbedingt erforderlich um sicherzustellen dass kein Dritter Zugriff zu Daten hat die Sie auf einem Mobilten Datenträger abspeichern. Im Fall das ein Mobiler Datenträger, wie ein USB Stick verloren geht, verlegt wird oder gestohlen wurde ist EasyLock dafür da die Sicherheit Ihrer Daten zu gewährleisten. Mit der anerkannten 256bit AES CBS – Verschlüsselung sind Ihre Daten sicher.

Mit der intuitiven Drag & Drop Bedienungs Oberfläche, können Daten sehr schnell, sicher und mit einem effizienten Arbeitsfluss auf und von dem Gerät kopiert werden.

EasyLock ist eine portable Applikation, die keine Installation auf dem Computer benötigt und ist immer portable. Immer wenn das portable Speichergerät mit dem Computer verbunden ist kann EasyLock auf Windows, MAC oder Linux Computern verwendet werden.

# 2. Systemanforderungen

## Betriebssysteme:

- Windows 7 (alle Versionen)
- Windows Vista (alle Versionen)
- Windows XP (Service Pack 2 ist empfohlen)
- Mac OS 10.5 oder neuere Version
- Linux -openSUSE 11.2 (andere Distributionen stehen auch zur Verfügung)

## Vorhandener USB Port

Löschbare USB Speichergeräte (z.B USB Flash Drive, Externe Festplatte, Speicherkarte usw.) um von dieser die Applikation zu starten.

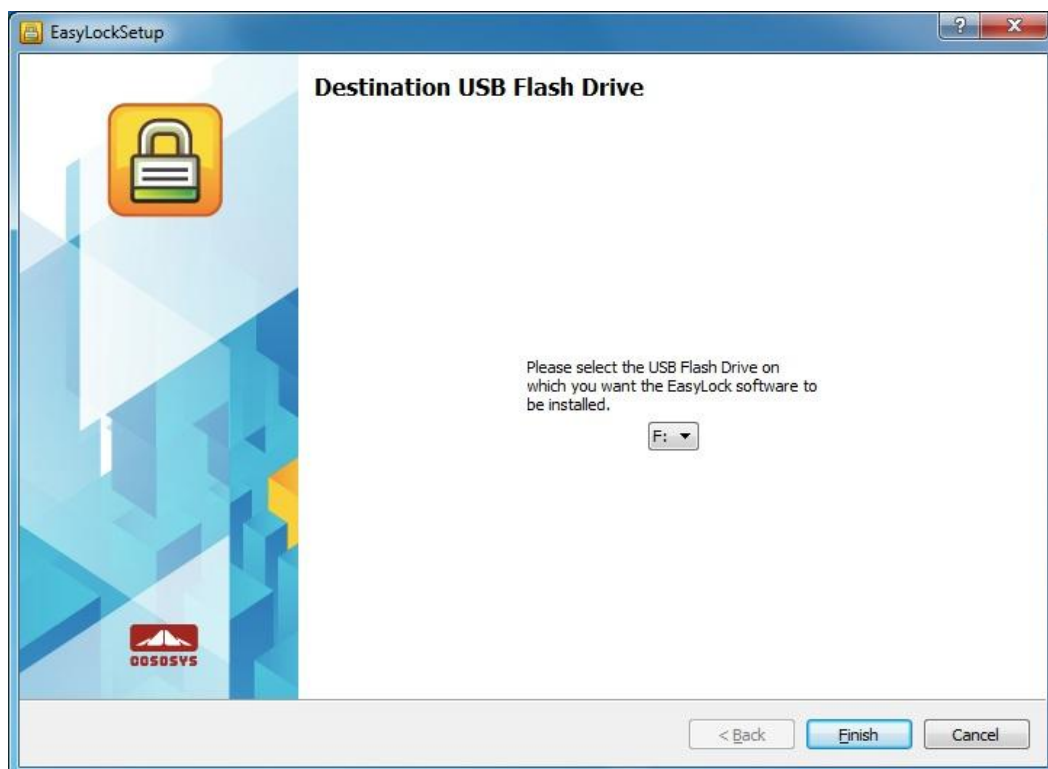
Wenn das portable Speichergerät einen manuellen Schreibschutzschalter (Sperrung) besitzt, muss dieser auf die freigegeben (schreibbare) Position gestellt sein, damit es möglich ist EasyLock zu benutzen.

EasyLock benötigt keine Administratorrechte.

# 3. Installation

EasyLock auf einem USB Laufwerk zu installieren (oder auf einem anderen USB Speichergerät):

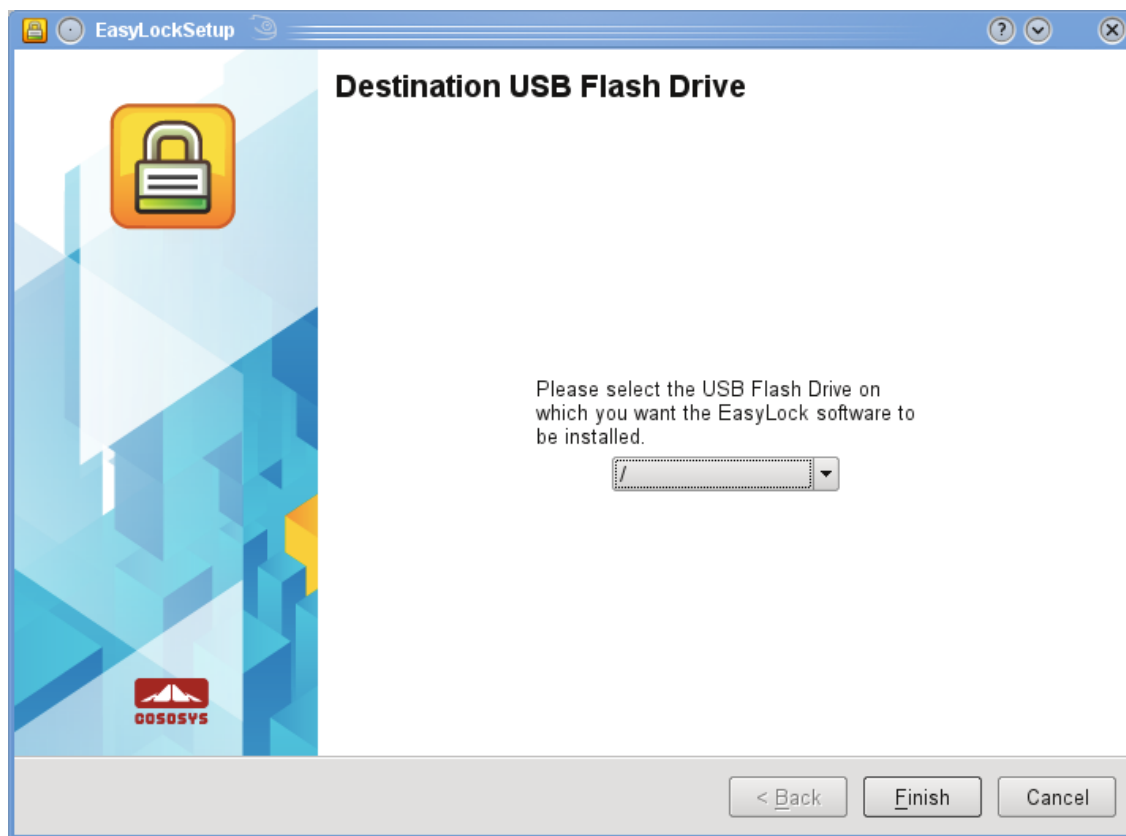
- **Auf Windows Betriebssystem:** "EasyLockSetup.exe" Datei ausführen, den Laufwerksbuchstaben entsprechend dem USB Gerät auswählen und danach <Ende> anklicken. Die EasyLock Applikation wird sich automatisch im Root Verzeichnis des ausgewählten Gerätes installieren.



- **Auf MAC Betriebssystem:** die Datei "EasyLockSetup.dmg" ausführen, den Laufwerksbuchstaben entsprechend dem USB Gerät auswählen und danach <Ende> anklicken. Die EasyLock Applikation wird sich automatisch im Root Verzeichnis des ausgewählten Gerätes installieren.



- **Auf Linux Betriebssystem:** die EasyLock 2 Setup Datei ausführen, den Laufwerksbuchstaben entsprechend dem USB Gerät auswählen und danach <Ende> anklicken. Die EasyLock Applikation wird sich automatisch im Root Verzeichnis des ausgewählten Gerätes installieren.



## 3.1. EasyLock Einrichten

Um EasyLock zu starten, einfach auf die EasyLock Datei doppelklicken, die im Root Verzeichnis des portablen Speichergerätes gespeichert ist.

Wenn wir den portablen Speichergerät als einen TrustedDevices in Kombination mit Endpoint Protector als Client PC benutzen, zu welchem das Gerät verbunden ist, muss man die Berechtigung vom Endpoint Protector Administrator erhalten, ansonsten wird das Gerät an dem Computer an dem Endpoint Protector installiert ist, nicht verfügbar sein, oder EasyLock wird nicht automatisch starten.



## 3.2. Passwort Eingeben

Um Ihre Daten zu verschlüsseln, müssen Sie ein Passwort eingeben. Das Passwort muss mindestens 6 (sechs) Stellen haben.

Aus Sicherheitsgründen, empfehlen wir Ihnen, Buchstaben, Zahlen oder Symbole in das Passwort einzubinden.



The screenshot shows a window titled "EasyLock - Einrichtungs-Assistent" with a blue header bar. On the left, there is a vertical sidebar with a blue and yellow geometric pattern, a padlock icon, and the "00505YS" logo. The main content area is titled "Passwort festlegen" and contains three input fields: "Passwort:", "Passwort Bestätigen:", and "Passwort Hinweis:". Below these is a "Passwort Info" box with instructions: "Bitte neues Passwort angeben. Passwort muss mindestens 6 Zeichen haben. Es wird empfohlen, Buchstaben, Zahlen und Sonderzeichen für maximale Sicherheit zu verwenden." At the bottom left of the main area, it says "Feststell taste: AUS". The bottom of the window has a grey bar with four buttons: "< Zurück", "Weiter >", "Abbrechen", and "Hilfe".

Geben Sie Ihrem Passwort ein, und bestätigen Sie es.

Es ist empfohlen, dass Sie auch einen Passwort Hinweis eingeben der Ihnen hilft im Fall dass Sie Ihr Passwort vergessen.

Klicken Sie auf "Weiter" um fortzufahren.



Klicken Sie "Abschließen" um die Passwort Einstellungen zu beenden und starten Sie die Applikation.



### 3.3. Passwort Eingabe bei Login

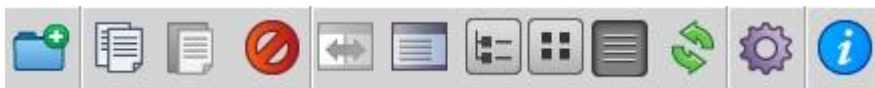
Jedes Mal wenn die Applikation startet, werden Sie aus Sicherheitsgründen angefordert, das Passwort einzugeben.

Für den Fall dass Ihr Laufwerk verloren oder gestohlen wird, ist die Anzahl der Passworteingabeversuche auf 10 (zehn) Versuche beschränkt. Nachdem dass Passwort 10 (zehn) Mal hintereinander falsch eingetragen wurde, wird EasyLock sicher alle verschlüsselten Dateien die auf dem portablen Laufwerk gespeichert sind, löschen.

Die Daten von dem portablen Speichergerät können nachdem nicht mehr wiederhergestellt werden. Die Daten sind unwiderruflich gelöscht.

### 3.4. Bedienoberfläche Einstellungen

In dem Toolbar Bereich von EasyLock gibt es einige Optionen um die Oberfläche anzupassen.



**Bereiche Wechseln** – um die Ebene des USB Laufwerk und Mein Computer auszutauschen.

**Arbeitsplatz ein- oder ausblenden** – um Mein Computer Panel anzeigen.

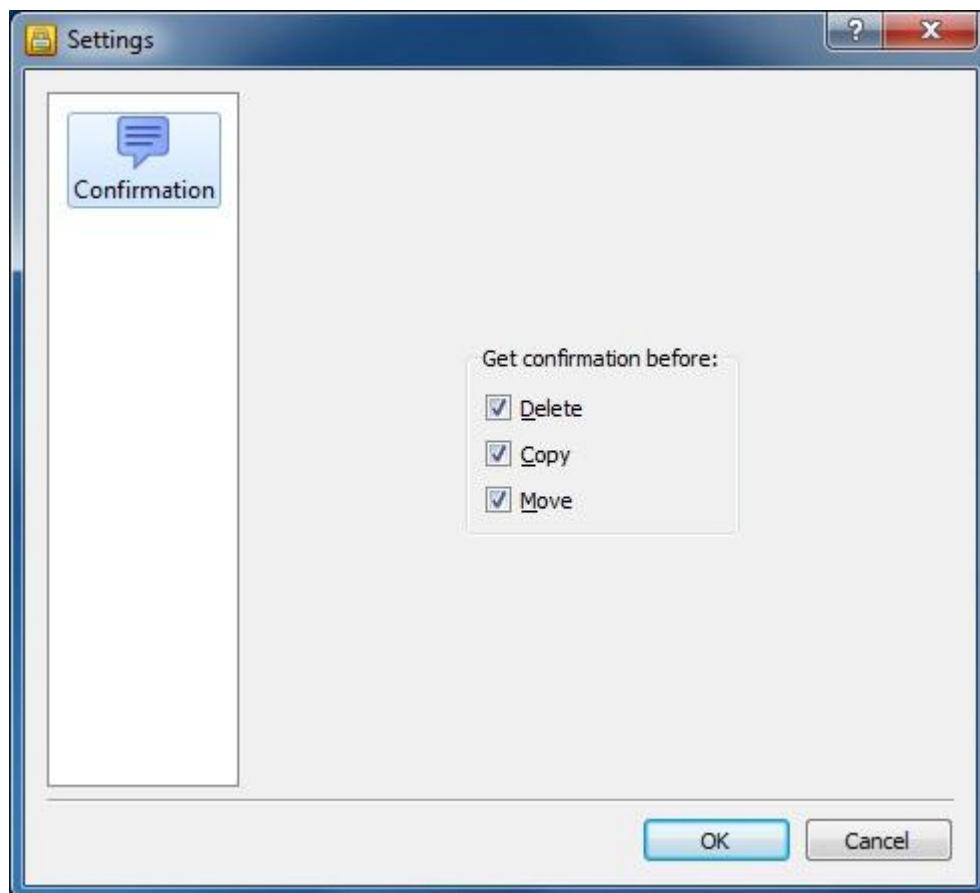
**Datenbaum Ansicht anzeigen** – um eine Baum-Struktur anzeigen.

**Detail Ansicht Anzeigen** – um zusätzliche Informationen über die Dateien anzeigen.

**Listen Ansicht Anzeigen** – um die Objekte als eine Liste anzeigen.

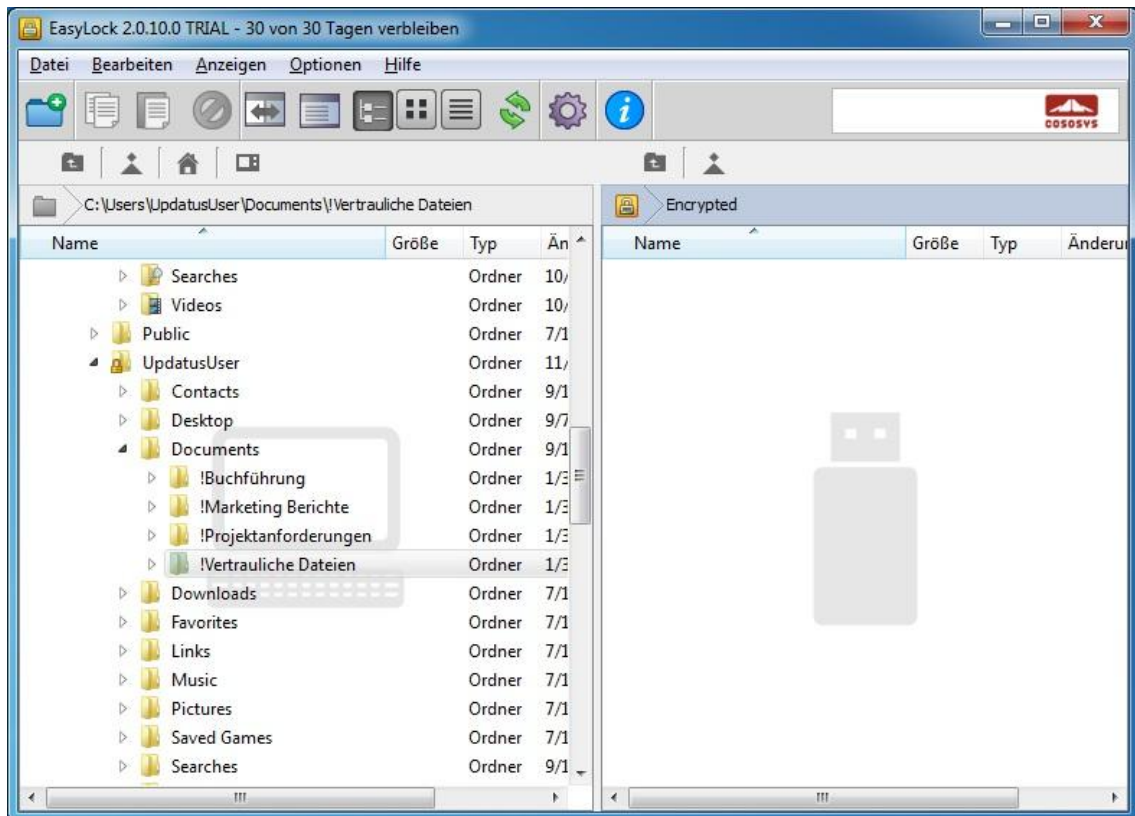
Die vorhandenen Optionen können unter der Anzeige Sektion direkt von dem Hauptmenü ausgewählt werden.

Wenn Sie möchten, können Sie einstellen das Ihnen eine Bestätigungsnachricht angezeigt wird bevor Sie etwa Daten Löschen, Kopieren oder Dateien verschieben.

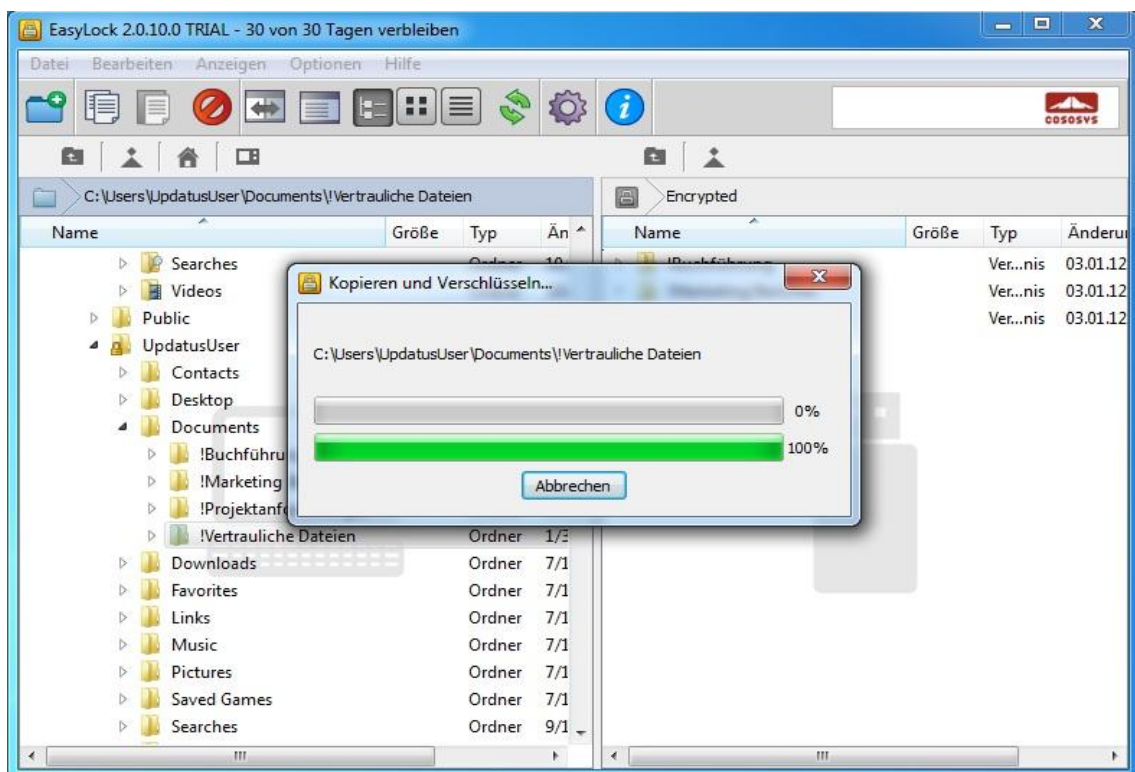


### 3.5. Drag & Drop beim Kopieren der Dateien

Die Hauptfunktion von EasyLock ist die Drag & Drop Funktionalität, welche Ihnen gestattet einfach die Dateien oder die Ordner, die Sie auf dem Gerät gespeichert haben, zu ziehen (Drag) und in das EasyLock Fenster einzufügen (Drop). Die auf das Gerät verschobenen Dateien werden automatisch verschlüsselt, um Ihre Daten zu schützen.



Der Status/Fortschritt der Verschlüsselung und der Transfer der Dateien ist mit Hilfe des Fortschrittbalkens ersichtlich. Wenn der Balken bis zum Ende gefüllt ist, sind die Dateien kopiert und verschlüsselt.



Beim Anklicken eines Objektes mit der rechten Mausetaste, wird Ihnen Zugriff zu den Optionen wie "aktualisieren", "kopieren" und "löschen" gewährt.

Dateien die von Ihrem Computer zu dem portablen Speichergerät mit Windows Explorer kopiert werden sind nicht verschlüsselt und dies wird **NICHT empfohlen!**

Wir empfehlen Ihnen entweder die Drag & Drop Funktion oder die Tastenkombination für kopieren und einfügen zu benutzen, STRG+C und STRG+V um die Daten zu Ihrem portablen Gerät durch die EasyLock Bedienungsoberfläche zu kopieren.

In dem Toolbar Bereich können Sie zusätzliche Schaltflächen, die Sie auch zum Kopieren oder Verschlüsseln Ihrer Dateien verwenden können finden.

Beachten Sie bitte dass die Dateien auf Ihrem portablen Speichergerät nur sichtbar sind, wenn EasyLock gestartet ist und nachdem Sie das korrekte Passwort eingegeben haben.

Um EasyLock zu schließen, wählen Sie das Datei Menü und wählen Sie „Schließen“, oder betätigen Sie das "X" Symbol rechts-oben im Applikationsfenster.

## 3.6. Das Öffnen und Verändern der Dateien mit EasyLock

Kopierte Daten auf dem Gerät können aus EasyLock heraus dargestellt oder direkt editiert werden. Diese Funktion ist erreichbar durch den "Öffnen" Befehl oder durch Doppel-Klick der Datei.

Der Benutzer muss Dokumente von dem Gerät mit der verknüpften Applikation öffnen. EasyLock wird versuchen diese Dokumente zu schließen wenn Sie die Applikation verlassen. Wenn ein Dokument verändert wurde (gespeichert unter dem gleichen Namen oder mit einem anderen Namen) wird es verschlüsselt und auf dem Gerät gespeichert. Wenn ein Dokument verändert und gespeichert wird, aber die Verschlüsselung fehlschlägt, zum Beispiel wenn ein Gerät unerwartet entfernt wurde, wird EasyLock nochmals versuchen die Datei zu verschlüsseln wenn EasyLock wiederholt gestartet wird.

**Achtung!** Wenn EasyLock durch den Endpoint Protector als eine vertraute Applikation gestartet wurde, ist das Öffnen der Dokumente von den Geräteroptionen gesperrt solange die Applikation die mit der Datei verknüpft ist keinen Zugriff zu der Datei hat.

## 3.7. Sicherheitseinstellungen

Die Sicherheitseinstellungen können innerhalb von EasyLock verändert werden. Nach der Passwordeingabe, können Sie das Passwort verändern. Dazu müssen Sie das Sicherheitsmenü öffnen. Das können Sie entweder über die Optionen - Sicherheitseinstellungen im Toolbar Bereich machen oder durch Drücken der Tastenkombination STRG+O.



Passwort Info

Passwort ändern

Altes Passwort:

Neues Passwort:

Passwort bestätigen:

Neuer Passwort Hinweis:

Passwort Info

Bitte altes Passwort angeben.

Feststelltaste: AUS

OK Abbrechen

# 4. Wie EasyLock mit EPP oder My EPP funktioniert

Wenn Sie EasyLock auf ein portables Speichergerät als ein TrustedDevice Level 1 Gerät in Kombination mit Endpoint Protector (oder My Endpoint Protector) verwenden, wird sichergestellt dass alle kopierten Daten von Endpoint Protector gesicherten Client PC zu dem Gerät verschlüsselt werden.

Normale Verwendung von EasyLock als TrustedDevice Level 1:

1. Der Benutzer verbindet das Gerät zu einem mit Endpoint Protector geschütztem PC.
2. Das Gerät wird auf Berechtigungen geprüft (der Client PC kommuniziert mit Endpoint Protector Server um die Berechtigung zu prüfen).
3. Wenn das Gerät ein TrustedDevice Level 1 Gerät ist und der Benutzer oder die Maschine berechtigt ist TrustedDevice Level 1 zu benutzen, wird die EasyLock Software automatisch auf dem Gerät gestartet.
4. Der Benutzer kann Dateien durch Drag & Drop in EasyLock übertragen.
5. Die Daten die auf das Gerät übertragen werden, sind mit 256bit AES verschlüsselt.
6. Der Benutzer kann nicht das Gerät direkt von Windows Explorer oder ähnlichen Applikationen zugreifen (z.B Total Commander), um sicher zu stellen dass keine Daten aus dem portablen Gerät ohne eine Verschlüsselung kopiert werden.

7. Benutzer haben keine Möglichkeit, Daten in eine nicht verschlüsselte Weise auf ein TrustedDevice (auf einem mit Endpoint Protector Client geschützten PC) zu kopieren.
8. Alle übertragenen Dateien, die von einem Endpoint Protector Client auf ein Gerät kopiert wurden, können mit Dateiprotokollierung (File Tracing) und der Dateimitschnitt (File Shadowing) Funktion von Endpoint Protector aufgezeichnet werden. Aktionen wie Datei-Löschung oder Umbenennungen werden auch aufgezeichnet.
9. Administratoren können später prüfen, was für ein Benutzer, was für ein Gerät und was für ein PC, die Dateien kopiert hat.

Wenn ein Gerät mit TrustedDevice Status scheitert, eine Berechtigung vom Endpoint Protector Server zu erhalten, kann der Benutzer nicht auf das Gerät zugreifen.

## 4.1. Daten Protokollierung auf EasyLock TD

Daten Protokollierung (File Tracing) mit EasyLock TrustedDevices ist ein Feature von Endpoint Protectors 4. Es ermöglicht die Überwachung von kopierten Dateien.

Durch die Aktivierung der File Tracing Option, werden alle übertragenen Dateien zu und von Geräten, wenn EasyLock verwendet wird, protokolliert. Die protokollierte Information wird automatisch zum Endpoint Protector Server gesendet, wenn der Endpoint Protector Client auf dem PC installiert ist.

Für den Fall, dass der Endpoint Protector Client nicht vorhanden ist, wird die Information lokal in einem verschlüsselten Format auf dem Gerät gespeichert und zu einem späteren Zeitpunkt, von einem anderen Computer, auf dem der Endpoint Protector Client installiert ist, übermittelt.

Für mehrere Details über die Aktivierung und die Nutzung der File Tracing auf EasyLock TrustedDevices, konsultieren Sie bitte das Endpoint Protector Benutzerhandbuch.

### **Bemerkung**

Das File Tracing Feature mit EasyLock TrustedDevices steht momentan nur für Windows Betriebssystem zur Verfügung.

# 5. TrustedDevice Konfigurierung auf EPP oder MyEPP

Um zu lernen wie die Nutzung als TrustedDevice in Kombination mit Endpoint Protector konfiguriert werden soll, konsultieren Sie bitte das Endpoint Protector Benutzerhandbuch.

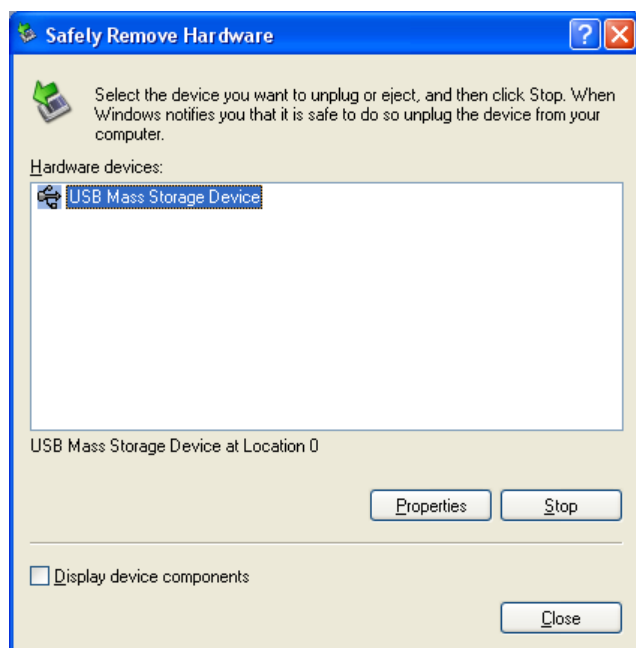
Um mehr über Endpoint Protector zu erfahren besuchen Sie bitte:  
[www.EndpointProtector.de](http://www.EndpointProtector.de)

# 6. Hardware Sicher Entfernen

Bevor Sie Ihr portables Speichergerät von dem USB Port Ihres Computers trennen, müssen Sie die "Hardware sicher entfernen" Option aus dem System Tray benutzen, ansonsten riskieren Sie Ihre Daten auf dem USB Laufwerk zu beschädigen.

Um Ihre Hardware sicher zu entfernen, doppelklicken Sie auf das System Tray Icon, und markieren Sie das USB Laufwerk auswelches Sie sicher entfernen wollen, und klicken Sie auf den "Stop" Knopf.





Eine Meldung wird erscheinen, dass das Speichergerät jetzt Sicher entfernt werden kann. Wenn die Meldung sagt dass das Gerät jetzt nicht gestoppt werden kann, müssen Sie Windows Explorer, EasyLock oder eine andere Applikation die noch auf Daten auf dem Gerät zugreift schließen.

# 7. Support

Für den Fall, dass Sie zusätzliche Hilfe brauchen, wie FAQs oder eine Mail an den Support senden möchten, können unsere Webseite direkt unter <http://www.cososys.com/help.html> besuchen.

# 8. Wichtige Anmerkungen / Disclaimer

Sicherheitsfunktionen, können von Natur aus umgegangen werden. CoSoSys kann nicht, und garantiert nicht dass die Daten oder das Geräte von unberechtigten Personen zugegriffen werden können, und CoSoSys lehnt jegliche Garantien und Haftung ab soweit dies gesetzlich vom Gesetzgeber zulässig ist.