



ENDPOINT PROTECTOR BASIC

Benutzerhandbuch Version 3.6

Benutzerhandbuch



Inhaltsverzeichnis

1. Einführung	1
2. Endpoint Protector Produktfamilie	2
3. Systemanforderungen	3
4. Kontrollierte Gerätetypen	4
5. Installation	6
6. Erste Schritte	7
7. Rechte	8
7.1. Geräte (Devices)	8
7.2. Geräte Typ (Device Class)	11
8. Einstellungen	12
8.1. Datei Überwachung (File Tracing)	13
8.2. Passwortschutz	14
9. Berichte und Analysen	15
10. E-Mail Benachrichtigungen	16
10.1. E-Mail Einstellungen	16
11. System Tray Benachrichtigungen	18
12. Über	20
12.1. Lizenzschlüssel Registrierung	20
12.2. Update-Mechanismus	20
13. Deinstallation	22
14. Hilfe / Support	23

1. Einführung

Endpoint Protector Basic™ hilft Ihnen, Ihre PC Endpunkte durch die Kontrolle und Überwachung von tragbaren Datenspeichern und anderen Geräten zu schützen. Sie können damit den Einsatz von USB-, FireWire-Schnittstellen und anderen tragbaren Gerät an Ihrem Computer überwachen. Damit verhindert Sie effektiv, das unerwünscht Daten kopiert oder Datendiebstahl an Ihrem PC über tragbare Datenspeicher stattfinden kann. Im Kapitel „4. Kontrollierte Gerätetypen“ finden Sie eine vollständige Liste aller kontrollierten Gerätetypen.

Mit Endpoint Protector Basic können Sie:

- Die Nutzung von USB-Speichermedien oder anderen tragbaren Speichergerät auf Ihrem Computer erlauben oder beschränken.
- Alle USB-Speichergerät die im Zusammenhang mit Ihrem Computer verwendet werden Identifizieren.
- Sie erhalten Details aller USB-Speichergeräte die zu einem bestimmten Zeitpunkt an den Computer angeschlossen sind.
- Als PC-Administrator können Sie sich per E-Mail benachrichtigen lassen, wenn eine nicht autorisiertes Gerät mit einem Geschützten Computer verbunden wird.
- Mit der Dateiprotokollierung („File Tracing“) können Sie überprüfen welche Daten von oder zu tragbaren Datenspeichern kopiert wurden.

2. Endpoint Protector Produktfamilie

Die Endpoint Protector Produktfamilie bietet Gerätemanagement (Device Control) und Endpunkt Sicherheit (Endpoint Security) für verschiedene Netzwerk Umgebungsart an, für PCs oder MACs im privaten gebrauch, für klein und mittelständische Firmen oder gar Grossunternehmen.

Endpoint Protector Basic ist ein Lösung der Produktfamilie und bietet Ihren Privat-und Büro-PCs die beste Lösung um die Verwendung von mobilen Geräten und Datenträgern zu steuern, damit Ihre Daten geschützten sind, so dass Sie nicht unerlaubt auf unerwünschte tragbare Datenspeicher kopiert werden.

Weitere Produkte aus der Endpoint Protector Produktfamilie sind:

- My Endpoint Protector (Geräteüberwachung und USB Schnittstellen Sicherheit als SaaS Lösung für PCs und MACs über das Internet).
<https://my.EndpointProtector.com>
- Endpoint Protector (Client - Server Gerätemanagement-Lösung für kleine und mittlere Unternehmen).
- Endpoint Protector Appliance (Hardware-Appliance für die einfache „out-of-the-Box“ Gerätemanagement-Lösung für Unternehmen).

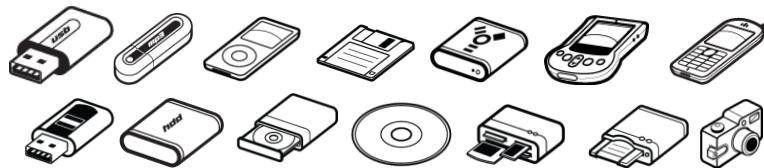
Weitere Informationen finden Sie hier <http://www.EndpointProtector.com>.

3. Systemanforderungen

- Unterstützte Betriebssysteme sind:
 - Windows 7 (32bit / 64bit)
 - Windows Vista (32bit / 64bit)
 - Windows XP (Service Pack 2 wird empfohlen)
 - Windows 2003
 - Administratoren Rechte sind erforderlich um die Software zu installieren und um Geräte zu autorisieren
- 32 MB freier Festplattenspeicher
- Mindestens 256 MB RAM Arbeitsspeicher empfohlen

4. Kontrollierte Gerätetypen

Endpoint Protector Basic schützt vor einer breite Anzahl von Gerätetypen, die die größten Quellen von Verstöße gegen Sicherheitsrichtlinien darstellen. Folgende Geräte können überwacht und verwaltet werden. Es ist damit möglich zu sehen welcher Benutzer Geräte verwendet und deren Inhalt im bezug auf übertragene Daten von autorisierten Geräten zu kontrollieren.



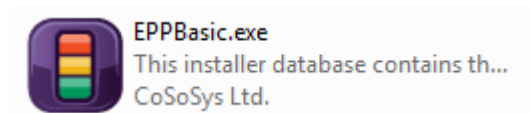
- Tragbare Datenspeicher
- Normal USB Flash Sticks, U3 and Autorun Geräte, etc.
- USB 1.1, USB 2.0, USB 3.0
- Speicherkarten - SD Karten, MMC Karten und Compact Flash Karten, etc.
- Kartenlesegeräte - interne und externe
- CD / DVD-Player / Brenner - interne und externe
- Digitalkameras
- Smartphones / Handhelds / PDAs (mit Nokia N-Series, BlackBerry und Windows CE)-kompatible Geräte, Windows Mobile-Geräte, etc.
- iPods / iPhones / iPads
- MP3-Player / Media Player Geräte
- Externe Festplatten / portable Festplatten

- FireWire-Geräte
- PCMCIA-Geräte
- Biometrische Geräte
- Bluetooth
- Drucker (gilt für serielle, USB Anschluss und LTP-Verfahren)
- ExpressCard (SSD)
- Wireless USB
- LPT / Parallel-Schnittstelle(Durch die Steuerung der Parallel-Ports eines PCs mit Endpoint Protector Basic, kann der PC-Administrator den Zugriff auf dort angeschlossene Speichergeräte sperren)
- Diskettenlaufwerke

5. Installation

Zur Installation von Endpoint Protector Basic ist es erforderlich, dass Sie mit Administrator-Rechten am PC angemeldet sind.

Führen Sie die Datei EPPBasic.exe aus.



In einigen Fällen kann es erforderlich sein, dass Sie Ihren PC neu starten müssen, um die Installation von Endpoint Protector Basic erfolgreich zu beenden.

Endpoint Protector Basic erstellt im Windows Startmenü eine Programm-Gruppe.

Nach der Installation wird der Schutz von Endpoint Protector nach jedem start von Windows automatisch im Hintergrund gestartet.

6. Erste Schritte

WICHTIG!

Vergewissern Sie sich das Sie als Administrator angemeldet sind. Die Endpoint Protector Basic Konfigurationsoberfläche ist nur für Administratoren auf dem PC aufrufbar. Standard-Benutzer (Gast-Benutzer) haben keine Ausreichende Berechtigung um die Konfigurationsoberfläche von Endpoint Protector Basic zu öffnen. Die PC-Anschlüsse sind geschützt und gesperrt für alle nicht zuvor zugelassenen Geräte.

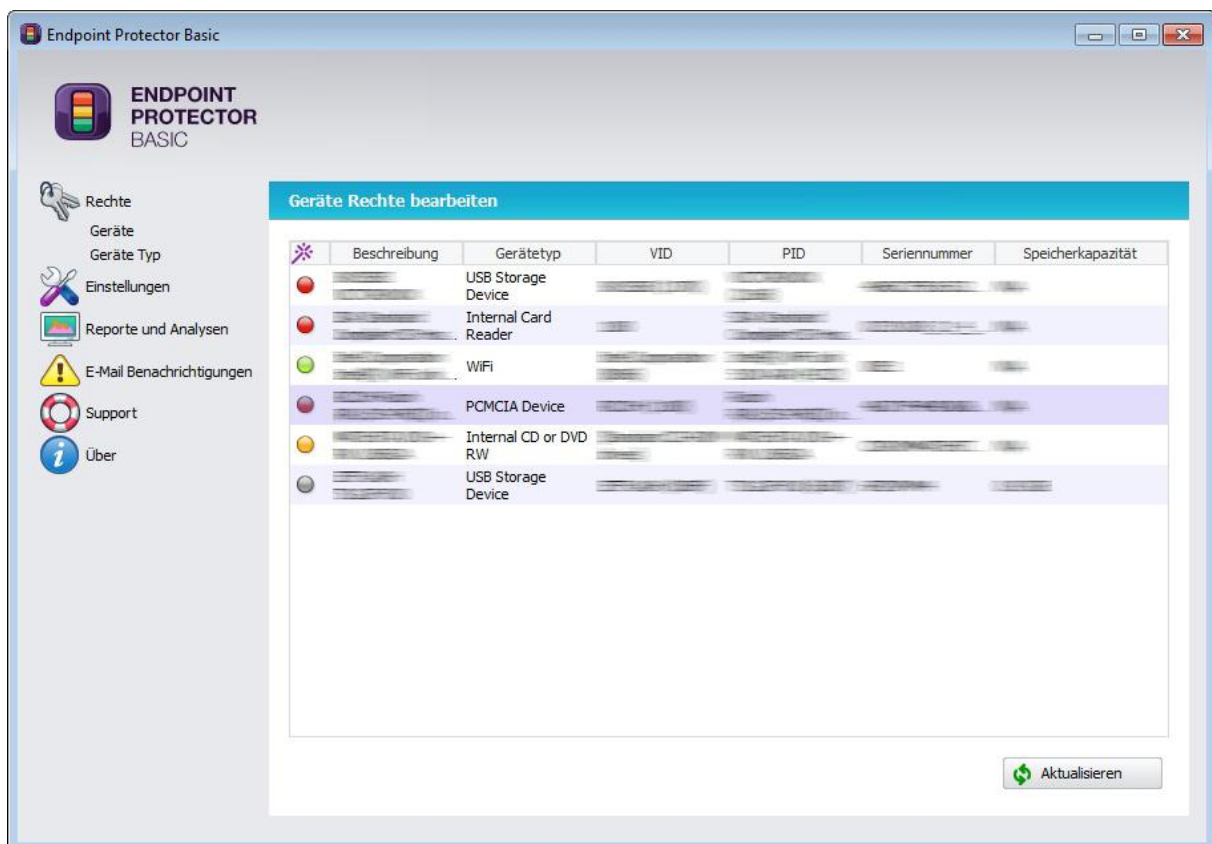
Zum Start von Endpoint Protector Basic, gehen Sie auf Start > Alle Programme > Endpoint Protector Basic > Endpoint Protector Basic.

7. Rechte

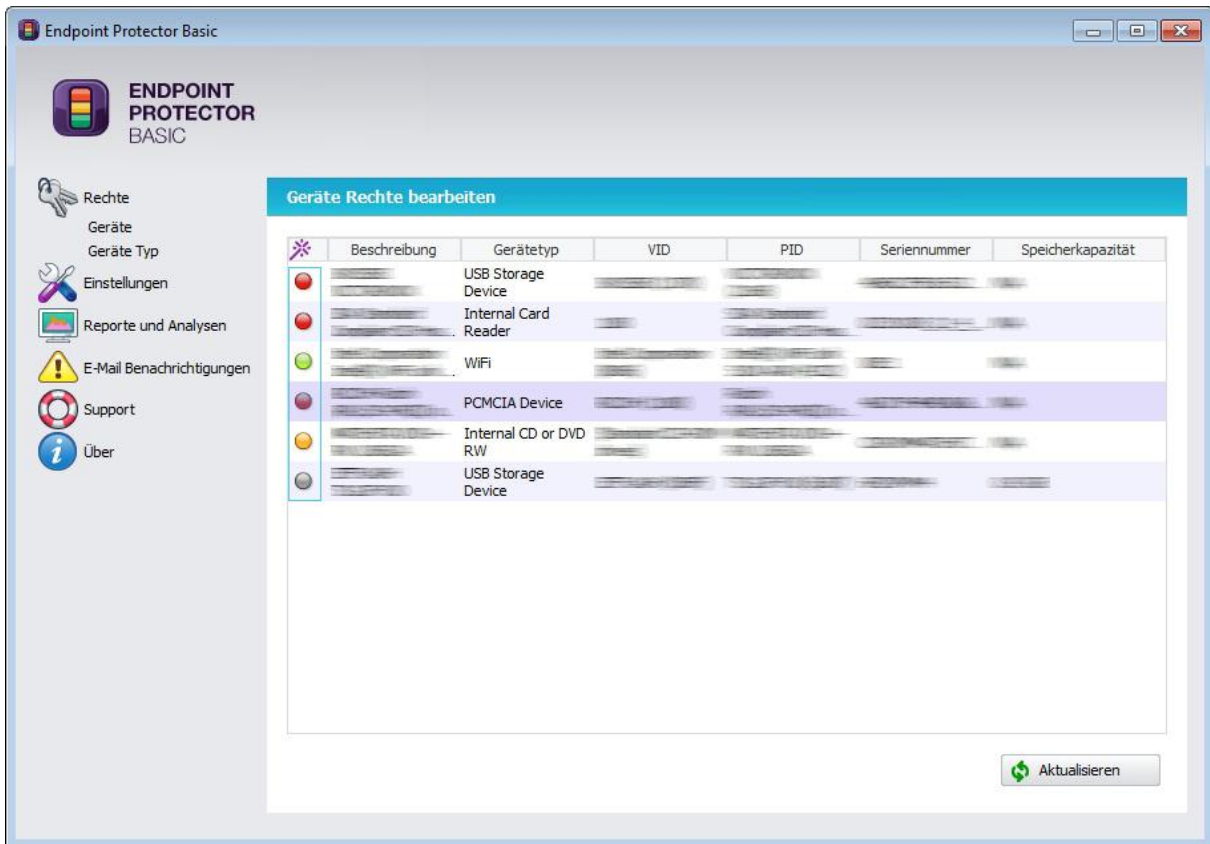
7.1. Geräte (Devices)





Dieses Modul ermöglicht es Ihnen, festzulegen, welche spezifischen Gerät in Verbindung mit Ihrem PC verwendet werden dürfen.

Jedes Mal, wenn ein neues Gerät am PC angeschlossen wird, wird dieses automatisch in Geräte-Liste erscheinen. Falls Sie ein Gerät nicht in der Liste sehen, klicken Sie auf die Schaltfläche "Aktualisieren".

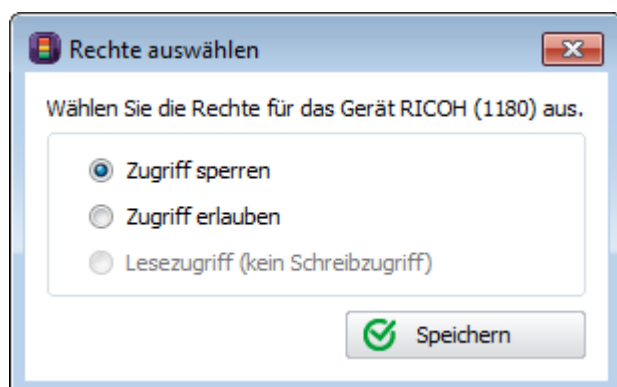


Die Status-Spalte zeigt die aktuellen Rechte für die Geräte an.



-  Rot bedeutet, dass das Gerät am PC gesperrt ist.
-  Grün bedeutet, dass das Gerät am PC freigegeben ist und verwendet werden darf.
-  Gelb bedeutet, dass das Gerät auf dem PC nur Lesezugriff hat.
-  Grau bedeutet, dass das Gerät momentan nicht mit dem PC verbunden ist.

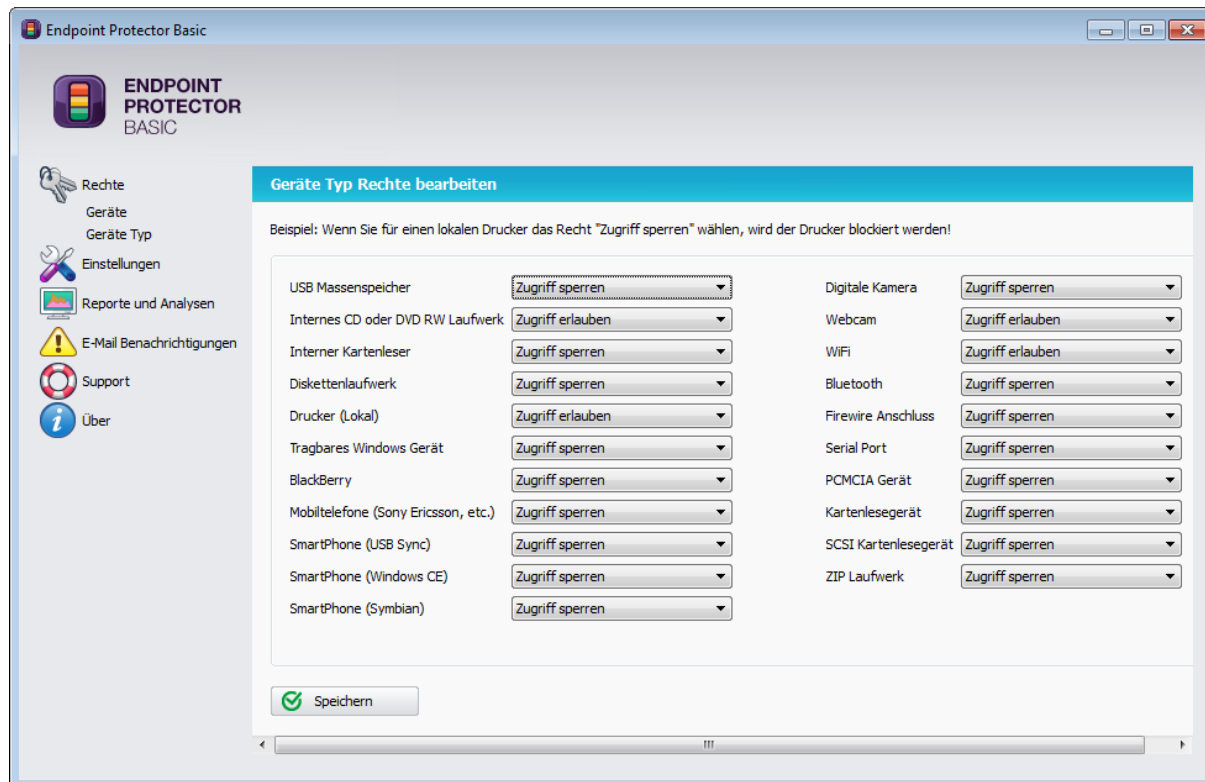
Mit einem Mausklick auf den Geräte Status, öffnet sich das Rechte Menü. Dieses Menü gibt Ihnen Zugriff auf die folgenden Einstellungen:



Option	Beschreibung
Zugriff sperren	Das das Gerät wird am PC gesperrt sein.
Zugriff erlauben	Das Gerät ist am PC freigegeben und kann verwendet werden.
Lesezugriff (kein Schreibzugriff)	Der Benutzer hat am PC nur Lesezugriff auf das Gerät. Daten können nicht auf das Gerät geschrieben werden.

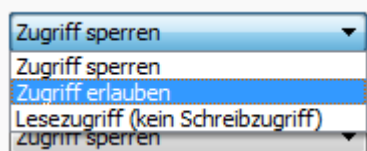
7.2. Geräte Typ (Device Class)

Dieses Modul ermöglicht es Ihnen, festzulegen, welche Geräteklasse am PC allgemein zugelassen sind.



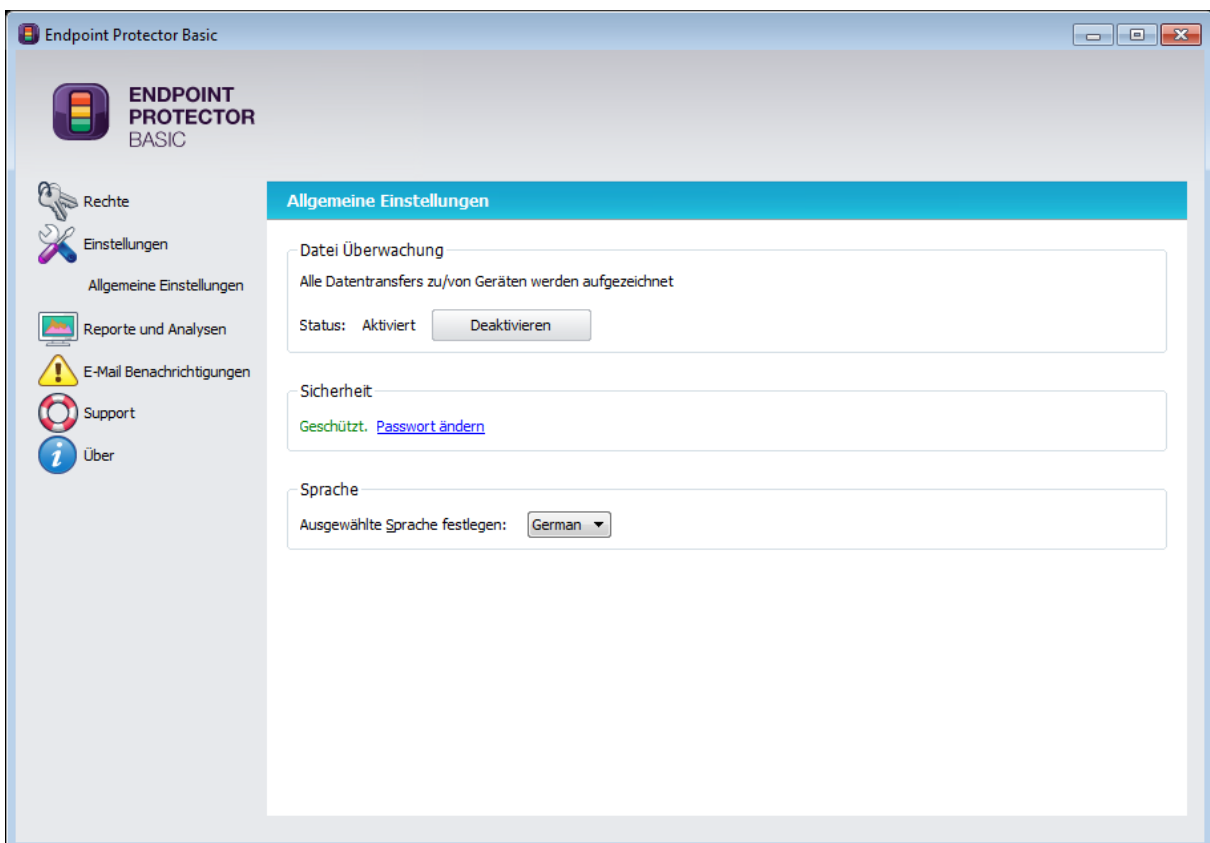
Standardmäßig sind folgende Gerätetypen am PC freigegeben: WiFi, lokale Drucker, Webcams und CD-ROMs.

Um die Rechte eines Geräte Typs festzulegen, müssen Sie im Auswahlfeld neben dem Gerät Typ eine der Möglichkeiten „Zugriff sperren“, „Zugriff erlauben“ oder „Lesezugriff (kein Schreibzugriff)“ auswählen.



8. Einstellungen

Unter Einstellungen gibt es die Möglichkeit die Datei Überwachung (File Tracing) zu aktivieren/deaktivieren. Datei Überwachung ist standardmäßig aktiviert. Sie können diese Funktion auch deaktivieren sollten Sie diese zusätzliche Sicherheitsstufe nicht benötigen.

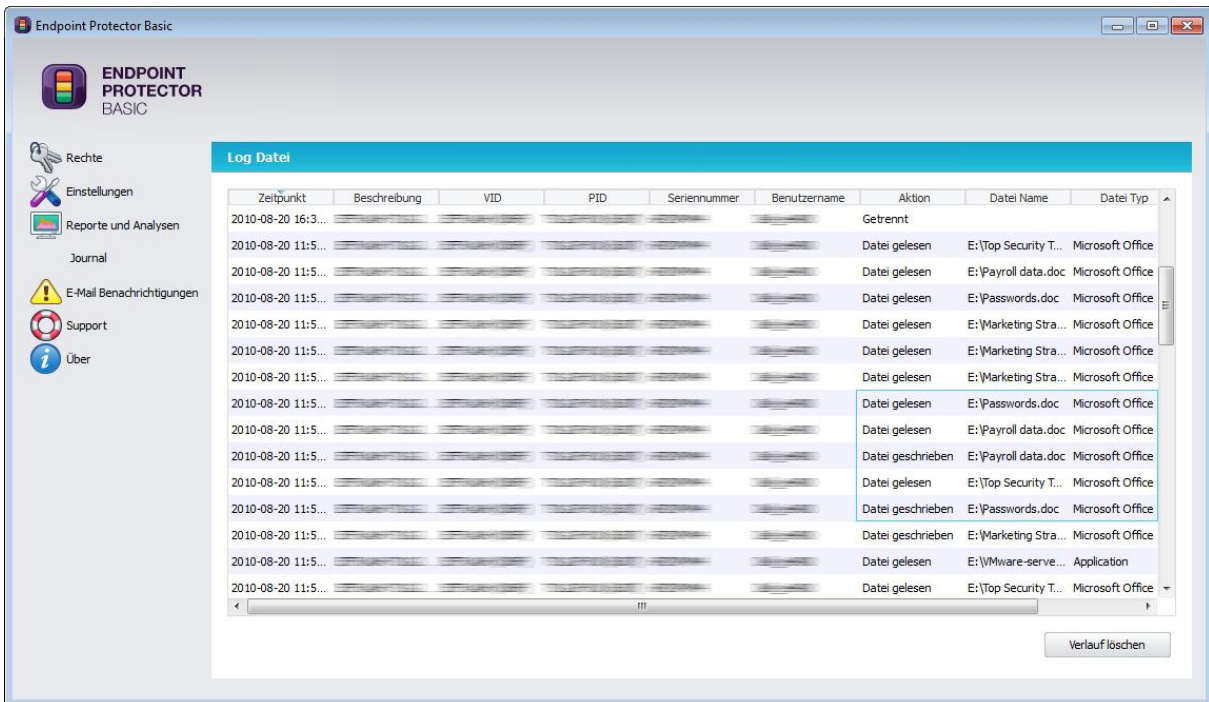


Hier können Sie auch den Zugriff auf die Endpoint Protector Basic Konfigurationsoberfläche mit einem Passwort schützen sowie die Sprache der Konfigurationsoberfläche ändern.

8.1. Datei Überwachung (File Tracing)

Die Datei Überwachungs-Funktion ermöglicht dem PC Administrator, eine detaillierte Analyse aller Datei-Eigenschaften von Dateien die auf überwachte Gerätetypen geschrieben oder von diesen gelesen wurden.

Die einzelnen Datentransfers sind unter "Reporte und Analysen" einzusehen.



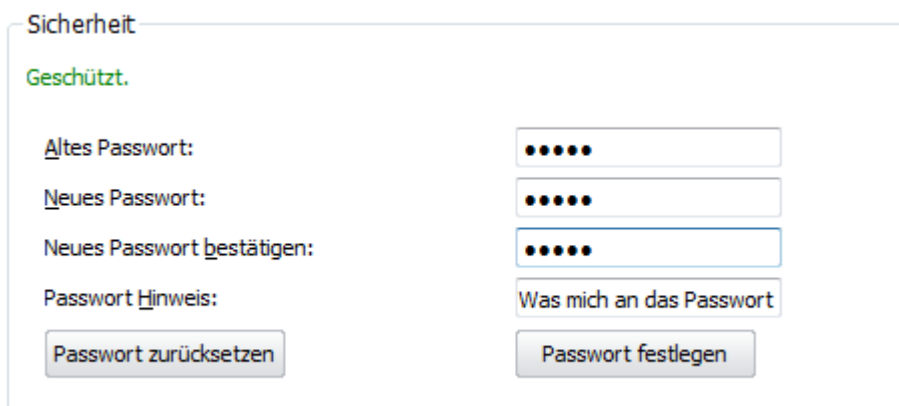
The screenshot shows the 'Log Datei' window in the Endpoint Protector Basic interface. The window title is 'Endpoint Protector Basic'. On the left, there is a navigation menu with icons for 'Rechte', 'Einstellungen', 'Reporte und Analysen', 'Journal', 'E-Mail Benachrichtigungen', 'Support', and 'Über'. The main area displays a table of file operations with the following columns: Zeitpunkt, Beschreibung, VID, PID, Seriennummer, Benutzername, Aktion, Datei Name, and Datei Typ. The table contains 18 rows of data, with the last row selected. A 'Verlauf löschen' button is located at the bottom right of the table area.

Zeitpunkt	Beschreibung	VID	PID	Seriennummer	Benutzername	Aktion	Datei Name	Datei Typ
2010-08-20 16:3...						Getrennt		
2010-08-20 11:5...						Datei gelesen	E:\Top Security T...	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Payroll data.doc	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Passwords.doc	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Marketing Stra...	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Marketing Stra...	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Passwords.doc	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Payroll data.doc	Microsoft Office
2010-08-20 11:5...						Datei geschrieben	E:\Payroll data.doc	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Top Security T...	Microsoft Office
2010-08-20 11:5...						Datei geschrieben	E:\Passwords.doc	Microsoft Office
2010-08-20 11:5...						Datei geschrieben	E:\Marketing Stra...	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\W\ware-serve...	Application
2010-08-20 11:5...						Datei gelesen	E:\Top Security T...	Microsoft Office

8.2. Passwortschutz

Der Zugriff auf die Endpoint Protector Basic Konfigurationsoberfläche sollte mit einem Passwort geschützt werden.

Nach Eingabe des Passworts müssen Sie auf das Schaltfläche "Passwort festlegen" klicken um es zu speichern.



Sicherheit

Geschützt.

Altes Passwort:

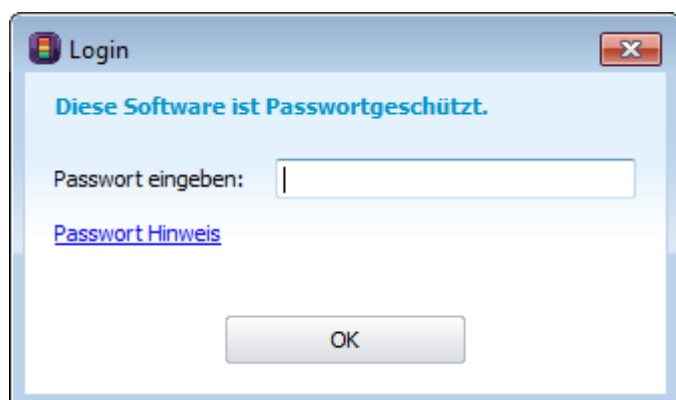
Neues Passwort:

Neues Passwort bestätigen:

Passwort Hinweis:

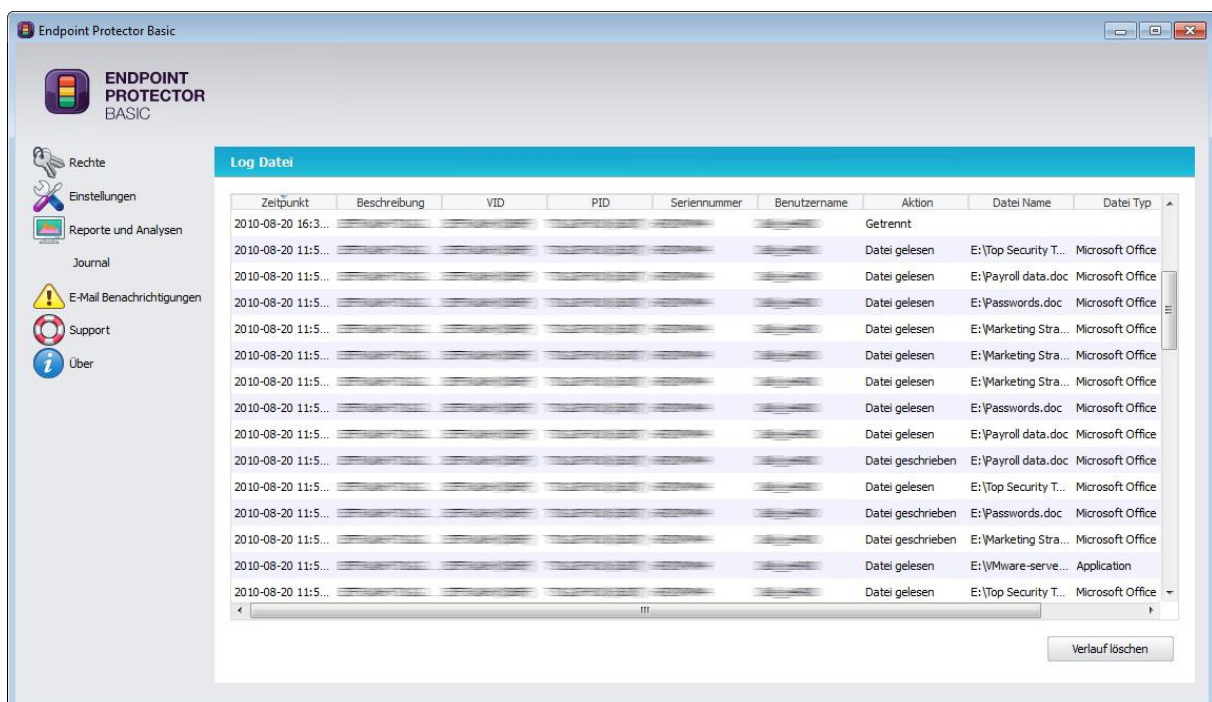
Um den Passwortschutz zu entfernen klicken Sie auf die Schaltfläche "Passwort zurücksetzen".

Nach dem festlegen eines Passworts werden Sie bei jedem Zugriff auf die Endpoint Protector Basic Konfigurationsoberfläche zur Passworteingabe aufgefordert.



9. Reporte und Analysen

Die umfangreichste Darstellung der Geräte- und Datentransfer-Aktivität kann der Administrator unter „Reporte und Analysen“ einsehen und analysieren. Die detaillierten Aufzeichnungen umfassen Information zu Benutzername, Geräte Informationen, Geräte Details und Geräte Aktivitäten sowie Datei Transfer Details.



Zeitpunkt	Beschreibung	VID	PID	Seriennummer	Benutzername	Aktion	Datei Name	Datei Typ
2010-08-20 16:3...						Getrennt		
2010-08-20 11:5...						Datei gelesen	E:\Top Security T...	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Payroll data.doc	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Passwords.doc	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Marketing Stra...	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Marketing Stra...	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Marketing Stra...	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Passwords.doc	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Payroll data.doc	Microsoft Office
2010-08-20 11:5...						Datei geschrieben	E:\Payroll data.doc	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\Top Security T...	Microsoft Office
2010-08-20 11:5...						Datei geschrieben	E:\Passwords.doc	Microsoft Office
2010-08-20 11:5...						Datei geschrieben	E:\Marketing Stra...	Microsoft Office
2010-08-20 11:5...						Datei gelesen	E:\VMware-serve...	Application
2010-08-20 11:5...						Datei gelesen	E:\Top Security T...	Microsoft Office

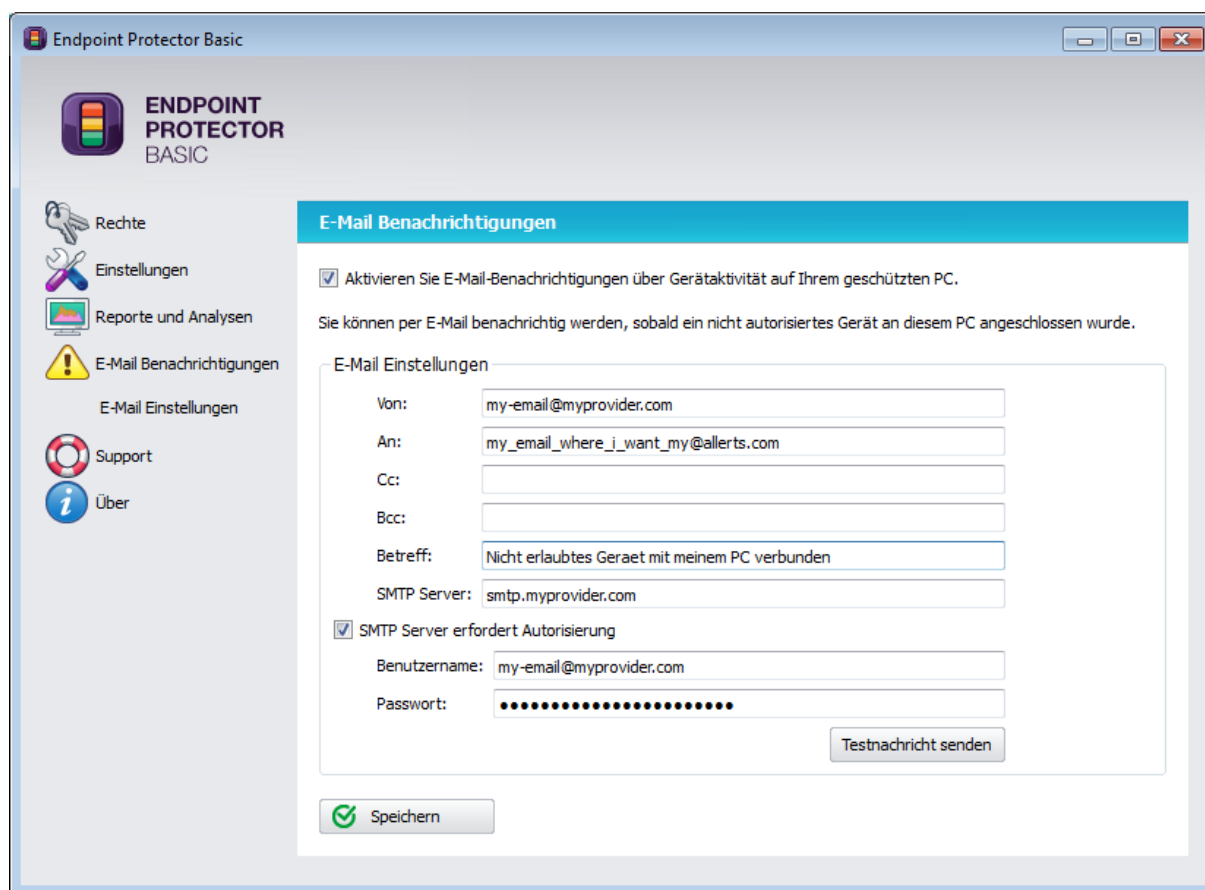
Sie können die einzelnen aufgezeichneten Events nach Datum & Uhrzeit, Benutzer, Aktion, Dateityp, Produkt-ID (PID), Hersteller-ID (VID), etc. mit einem Klick auf den Tabellenkopf sortieren.

10. E-Mail Benachrichtigungen

Sie haben die Möglichkeit bei jeder nicht berechtigten Verbindung eines Gerätes mit Ihrem geschützten PC eine Benachrichtigung per E-Mail zu erhalten, die Sie über einen möglichen Versuch Daten zu stehlen informiert.

10.1. E-Mail Einstellungen

Um diese Funktion zu aktivieren, müssen Sie die Angaben zu Ihrem E-Mail Anbieter (SMTP Server, Benutzernamen, Passwort) und die gewünschte Empfangsadresse für die Benachrichtigungen angeben.



Bitte geben Sie einen Sender und einen Empfänger E-Mail-Adresse ein. Geben Sie Ihren SMTP Server-Details mit Ihrem Benutzernamen und Passwort für den Fall, dass Ihr SMTP Server diese benötigt.

Sie sollten überprüfen, ob Ihre Einstellungen korrekt sind. Klicken Sie dafür bitte auf "Testnachricht senden". Im Fall das die Angaben richtig waren, sollten Sie eine Test E-Mail erhalten haben.

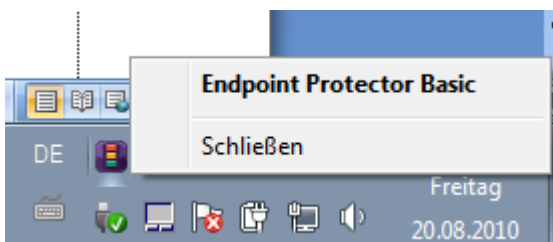
Sollte auf dem mit Basic Protector Basic geschützten PC auch eine Firewall installiert sein, müssen Sie Endpoint Protector Basic die Berechtigung geben E-Mails zu versenden, bzw. Internetzugang gewähren damit sie die E-Mail Benachrichtigungen erhalten können.

11. System Tray Benachrichtigungen

Um Benachrichtigungen aus dem System Tray zu erhalten muss der Basic Notifier gestartet sein.

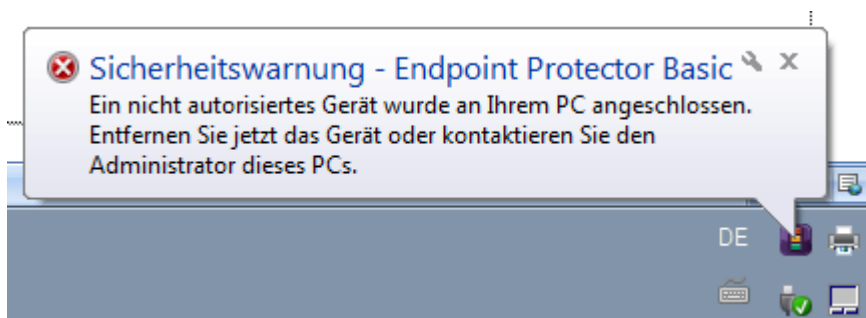
Der EPP Basic Notifier ist gestartet, wenn Sie das Endpoint Protector Basic System Tray Icon sehen können.

Durch einen rechten Maustaste auf das Endpoint Protector Basic Symbol, haben Sie die Option die Konfigurationsoberfläche zu öffnen oder den Endpoint Protector Basic Notifier durch das klicken von „Schließen“ bis zum nächsten PC Neustart auszuschalten.



Sie können den Notifier unter Start> Alle Programme> Endpoint Protector Basic neu starten.

Jedes Mal, wenn ein neues Gerät oder eine unbefugte Gerät mit dem PC verbunden wird, erscheint eine Warnung auf dem Bildschirm für den Benutzer klar ersichtlich. Die Nachricht informiert den PC-Nutzer über die unerlaubte Verwendung eines tragbaren Geräts.



Sie halten auf die gleiche weise eine ähnliche Meldung, über verbleibenden Testzeitraum von Endpoint Protector Basic, wenn Sie die Software als eine Trial Version testen.

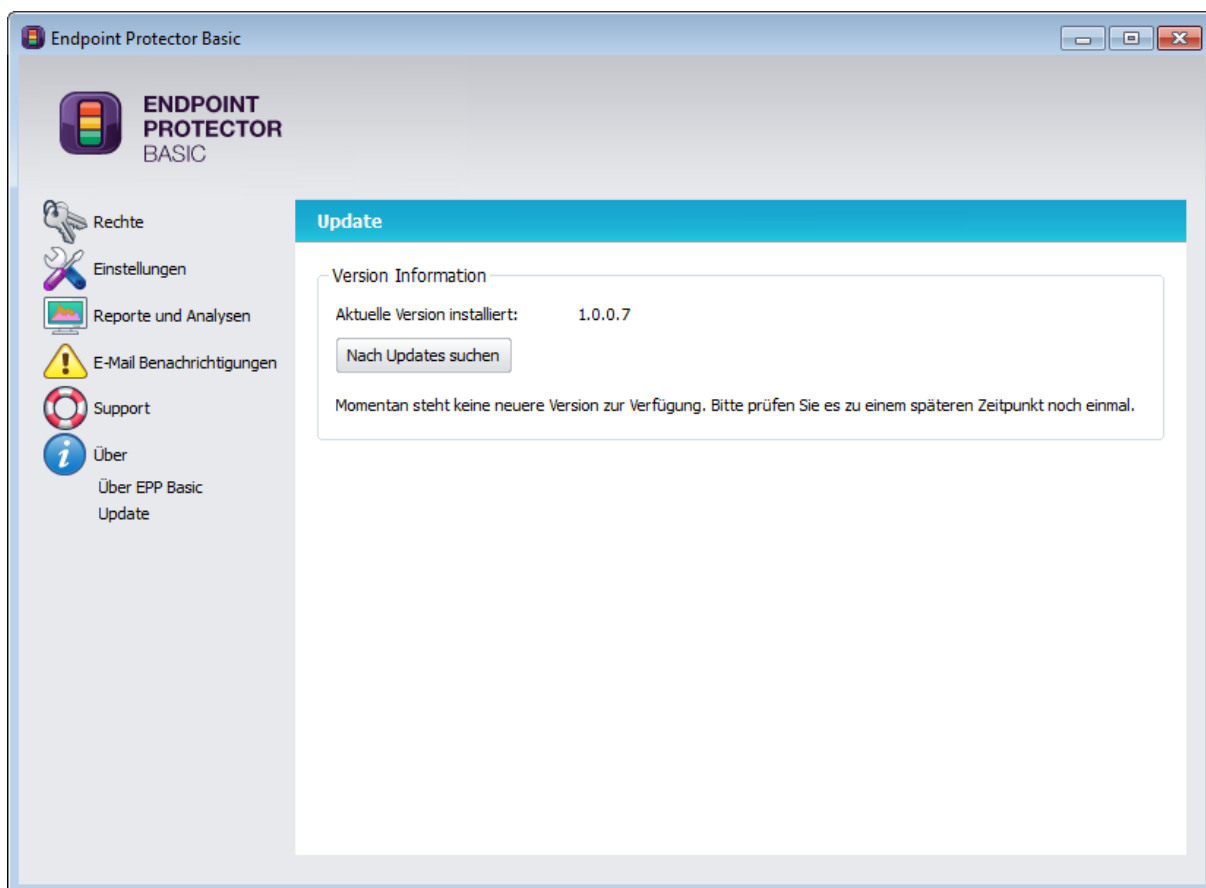
12. Über

12.1. Lizenzschlüssel Registrierung

Ihre Version von Endpoint Protector Basic enthält eine Lifetime-Lizenz. Daher können Sie die volle Funktionalität ohne ein Ablaufen der Software verwenden.

12.2. Update-Mechanismus

Sie können im Menü Update für die Verfügbarkeit einer neueren Endpoint Protector Basic-Version durch Klicken auf "Nach Update suchen" überprüfen.



Wenn es eine neuere Version verfügbar ist, können Sie diese herunterladen.

Die neue Version wird direkt auf Ihren PC heruntergeladen.

Nachdem der Download abgeschlossen ist, klicken Sie bitte "Jetzt installieren".

13. Deinstallation

Sie deinstallieren Endpoint Protector Basic von Ihrem PC aus, dem Menü Systemsteuerung > Programme hinzufügen oder entfernen. Vor der Deinstallation müssen Sie Endpoint Protector Basic schließen.

Während der Deinstallation ist es erforderlich das das Endpoint Protector Basic Passwort eingegeben wird.

Dieses Passwort ist erforderlich das der Endpoint Protector Basic Schutz nicht von unberechtigten Benutzern einfach deinstalliert wird.

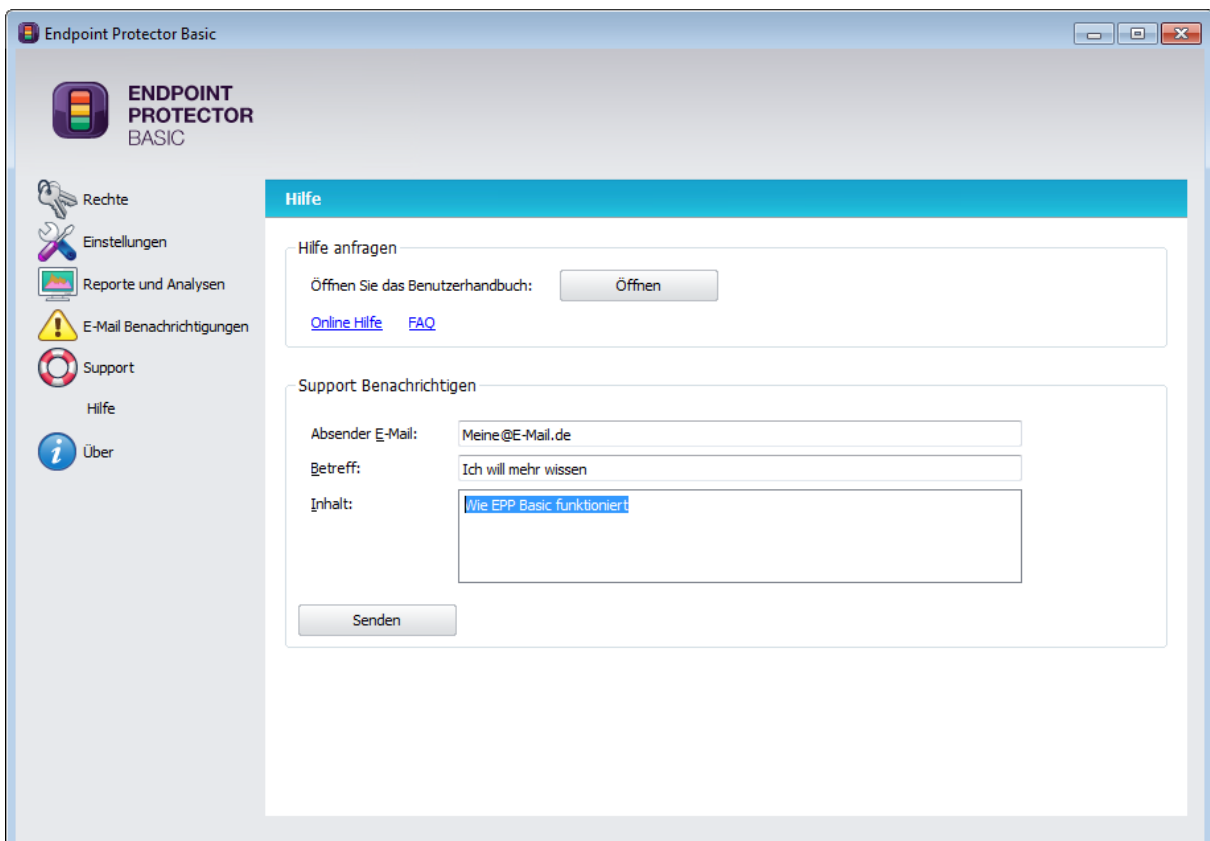
WICHTIG!

Deinstallieren der Software gibt vollen Zugriff auf alle USB und andere tragbare Datenspeicher die mit dem PC verbunden wurden.

14. Hilfe / Support

Unter Hilfe können Sie eine E-Mail direkt an unsere Supportabteilung unter support@cososys.com geschickt werden. Ein Teammitglied wird Sie dann in kürzester Zeit kontaktieren.

Selbst wenn Sie kein Problem haben sollten, eine Funktion in der Software vermissen oder uns einfach nur eine allgemeine Bemerkung zukommen lassen wollen, wir würden uns freuen von Ihnen zu hören. Ihr Input ist sehr willkommen und wir freuen uns über jeden Input der das Arbeiten mit tragbaren Geräten sicher und bequem macht.



The screenshot shows the 'Endpoint Protector Basic' application window. On the left is a sidebar with icons and labels: 'Rechte', 'Einstellungen', 'Reporte und Analysen', 'E-Mail Benachrichtigungen', 'Support', 'Hilfe', and 'Über'. The main area is titled 'Hilfe' and contains two sections:

- Hilfe anfragen:** A text box with the prompt 'Öffnen Sie das Benutzerhandbuch:' and an 'Öffnen' button. Below are links for 'Online Hilfe' and 'FAQ'.
- Support Benachrichtigen:** A form with three input fields:
 - 'Absender E-Mail:' with the value 'Meine@E-Mail.de'
 - 'Betreff:' with the value 'Ich will mehr wissen'
 - 'Inhalt:' with the value 'Wie EPP Basic funktioniert'A 'Senden' button is located at the bottom of this section.

Fuer zusätzliche Hilfe, wie FAQs oder E-Mail Hilfe besuchen Sie bitte unsere Support-Webseite direkt auf <http://www.cososys.com/help.html>.

© 2004 – 2010 CoSoSys Ltd.; Endpoint Protector Basic, EPP Basic, Endpoint Protector, My Endpoint Protector sind geschützt Warenzeichen von CoSoSys. Alle Rechte vorbehalten. Windows ist ein eingetragenes Warenzeichen der Corporation Microsoft. Alle anderen Namen und Marken sind Eigentum ihrer jeweiligen Besitzer.