

# Endpoint Protector Basic

User Guide



 Verbatim®

# Contents

---

English ..... 3

Français ..... 17

Deutsch ..... 31

# 1. Introduction

---

Endpoint Protector Basic™ will help you secure your PCs endpoints by controlling and monitoring device use. You will be able to restrict the use of USB, FireWire and other ports and control portable device use your computer. You can find a complete list of all controlled device types in the chapter "4. Controlled Device Types". Therefore you are effectively preventing unwanted data introduction or data theft from your PC.

- With Endpoint Protector Basic you can:
- Allow or restrict the use of any USB storage or other portable storage device on your computer
- Identify any USB storage device used in connection with your computer
- See the details of all USB storage devices connected to the computer at a certain moment
- Let the PCs administrator receive an e-mail message when an unauthorized USB storage device is connected to a workstation
- Use file tracing to monitor file accesses on any USB storage device

## 2. Endpoint Protector Product Family

---

The Endpoint Protector Product family offers device control and endpoint security for any environment for home PCs or MACs, medium sized offices or even entire enterprise networks.

Endpoint Protector Basic is part of it and offers your home and office PCs the best solution to control the use of portable devices on your protected PCs so you data cannot be copied unauthorized to unwanted devices.

Other products from the Endpoint Protector Product family included:

My Endpoint Protector (a Software as a Service solution to secure PCs and MACs over a internet portal <https://my.EndpointProtector.com>)

Endpoint Protector (a client - server device control solution for small and medium sized companies)

Endpoint Protector Appliance (a hardware appliance device control solution for small and medium sized companies and enterprises) More information can be found here <http://www.EndpointProtector.com>

### 3. System Requirements

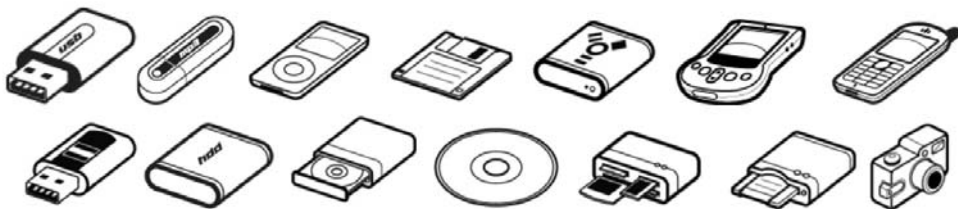
---

- Supported Operating Systems are:
  - o Windows 7 (32bit / 64bit)
  - o Windows Vista (32bit / 64bit)
  - o Windows XP (Service Pack 2 is recommended)
  - o Windows 2000
- o Administrative rights are required in install the software on a PC and to be able to authorize or unauthorized devices
- 32MB of available memory on the hard drive
- Minimum of 256MB RAM is recommended

### 4. Controlled Device Types

---

Endpoint Protector Basic supports a wide range of device types which represent key sources of security breaches. These devices can be authorized which makes it possible for the users to view, create or modify their content and for administrators to view the data transferred to and from the authorized devices.

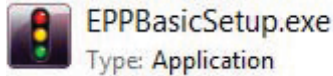


- Removable Storage Devices
- Normal USB Flash Drives, U3 and Autorun Drives, Disk on Key, etc.
- USB 1.1, USB 2.0, USB 3.0
- Memory Cards - SD Cards, MMC Cards, and Compact Flash Cards, etc.
- Card Readers - internal and external
- CD/DVD-Player/Burner - internal and external
- Digital Cameras
- Smartphones / Handhelds / PDAs (includes Nokia N-Series, Blackberry, and Windows CE compatible devices, Windows Mobile devices, etc.
- iPods / iPhones / iPads
- MP3 Player / Media Player Devices
- External HDDs / portable hard disks
- FireWire Devices
- PCMCIA Devices
- Biometric Devices
- Bluetooth
- Printers (applies to serial, USB and LTP connection methods)
- ExpressCard (SSD)
- Wireless USB
- LPT/Parallel ports (By controlling the Parallel ports of a PC using Endpoint Protector Basic, the network administrator can deny or allow users access to storage devices connected to these ports.) \*  
APPLIES ONLY TO STORAGE DEVICES
- Floppy disk drives

## 5. Installation

---

To install Endpoint Protector Basic it is required that you are logged on the workstation with full administrative rights. Run the EPPBasic.exe file.



Endpoint Protector Basic will install itself in the start menu and create the Endpoint Protector Basic program group. Endpoint Protector Basic will require in some cases that you restart your PC for a successful completion of the installation process.

After a successful installation Endpoint Protector Basic will always run in the background to protect your PCs endpoints when you or other users are logged into the PC.

## 6. Getting Started

---

**IMPORTANT!** Make sure you are logged in to the PC as administrator. Endpoint Protector Basic comes with a configuration Interface, which will be available for logged in Administrators ONLY. If a standard user (guest, restricted) logs into the system the configuration Interface will not be accessible and your PC ports are protected.

To start using Endpoint Protector Basic, go to Start > All Programs > Endpoint Protector Basic > Endpoint Protector Basic.

## 7. Rights

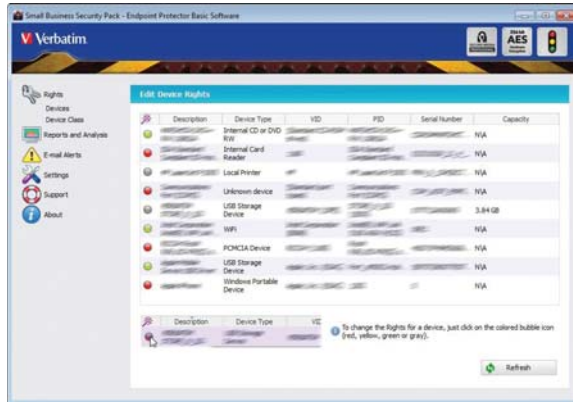
---

### 7.1. Devices





---

This module will allow you to specify what specific device can be accessible on your PC.

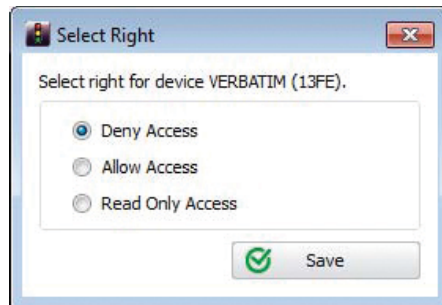
Each time a new device is connected to the PC while the Endpoint Protector Basic Settings application is open, you will see it automatically in the “Devices” list. In case you cannot see the device in the list, you can click the “Refresh” button from the bottom-right corner of the window.



The status column indicates the current rights for the devices.

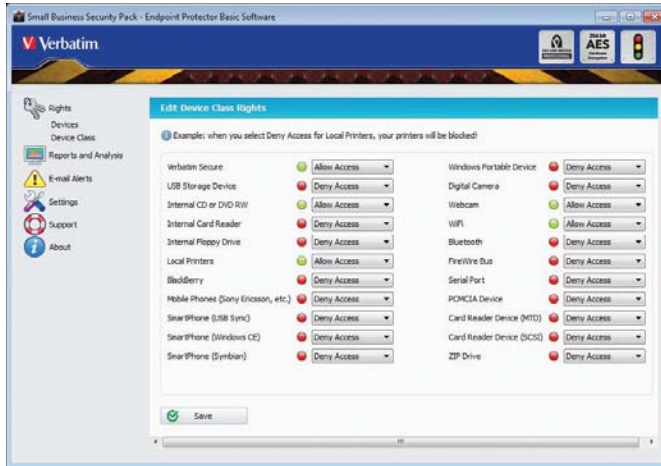
-  Red means that the device is blocked on your PC
-  Green means that the device is allowed on your PC
-  Yellow means that the device has read only rights on your PC
-  Grey means that the device is currently not connected to the PC

With a mouse click on a device's status dot, a menu will open. This menu will give you access to the following settings:



## 7.2. Device Class

This module will allow you to specify what device class can be accessible on your PC.



By default the following device types will have Allow Access rights: WiFi, Local Printers, Webcams and CD-ROMs.

In order to change the rights for a device class, you need to click the select box next to the device class name. The options you have are: "Deny Access", "Allow Access" and "Read Only Access".

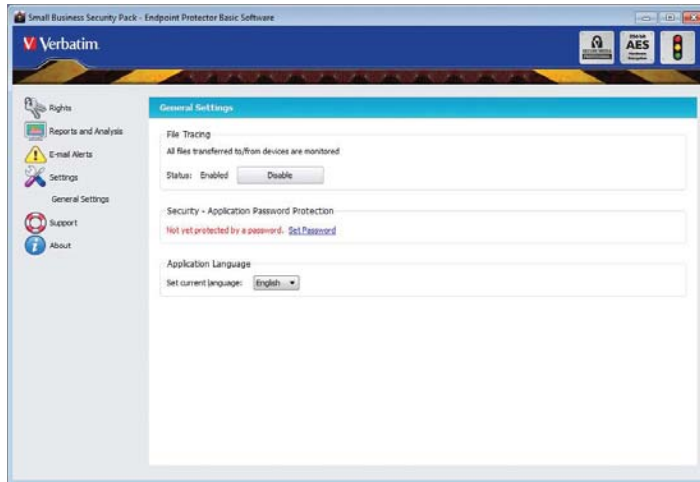


## 8. Settings

---

The General Settings module gives you the option to deactivate File Tracing, which is activated by default. You can deactivate this feature if you do not need this additional security level.

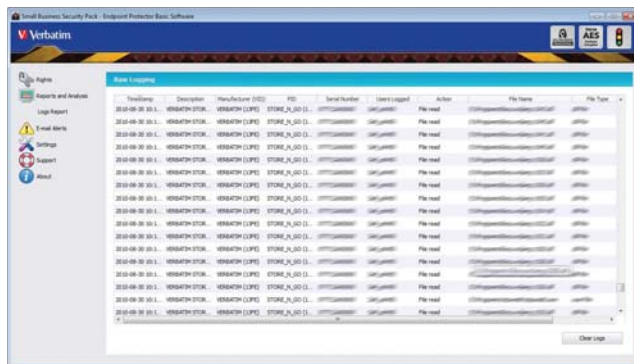
Here you can also password protect the access to the Endpoint Protector Basic User Interface, or select your Language settings.



## 8.1. File Tracing

The file tracing feature allows the administrator to record the file properties of files that are written or read from or to portable storage devices for later analysis.

You can then verify the files that have been accessed in the Logs Report, from the “Reports and Analysis” module.



## 8.2. Password protection

The access to the Endpoint Protector Basic User Interface can be password protected.

After introducing your password settings, you need to click “Set password” button in order to save it.

Security - Application Password Protection

Password protection set.

Old password:

New password:

Confirm new password:

Password hint:

You also have the option to save a 'Hint' (reminder) for the Password. This might be helpful when forgetting the password. To remove the Password protection, you have to click the "Reset password" button. After setting up a password, you will be asked to enter it each time you start Endpoint Protector Basic.



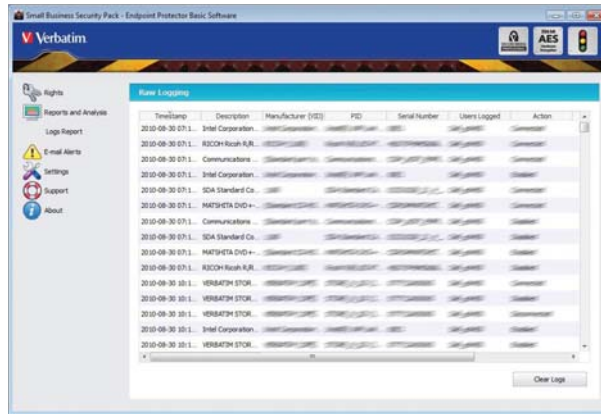
In case you didn't save a 'Hint', this functionality will be hidden in the Login dialog.

<b>Option</b>	<b>Description</b>
Deny Access	The device will be locked on your PC
Allow Access	The device will be allowed on your PC
Read Only Access	The device will have only read only rights on your PC

## 9. Reports and Analysis

---

The most powerful and detailed representation of activity recordings can be achieved using this module. It allows the administrator to see exactly what actions took place at what time. This information also contains the computer name, user and device used and also the action taken and the files accessed.



You can sort the events by date & time, user, action, file type, product ID (PID), vendor ID (VID), etc. by clicking on the correspondent table header, e.g. "Timestamp".

## 10. E-mail Alerts

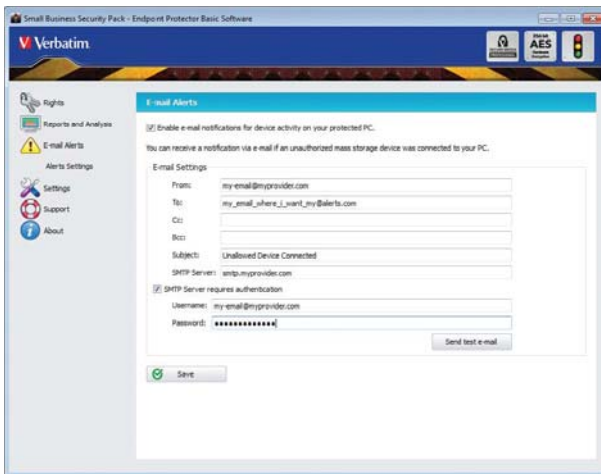
---

You have the option to receive a system alert in the form of an e-mail notification, each time an unauthorized device is connected to the PC that is protected with Endpoint Protector Basic.

To enable Alerts by e-mail notification, you must configure the e-mail server host and provide a user name and password to that mail server. You can do that by accessing "System Alerts" in the "Alerts Setup" module.

## 10.1. Alerts Settings

If you enable the e-mail notification option you have to provide Endpoint Protector Basic with an SMTP e-mail account that will be used to send the e-mail notifications to a specified e-mail address.



Please specify a sender and a recipient e-mail address. Enter your SMTP server address along with your username and password in case that your SMTP server requires this information in order to send an e-mail.

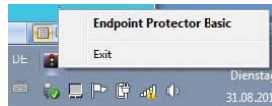
You can also verify if your settings are correct by clicking the "Send test e-mail" button.

If a firewall is installed on the PC that you are protecting with Endpoint Protector Basic, the firewall will request you for authorization that Endpoint Protector Basic is accessing the internet. Please grant Endpoint Protector Basic this authorization so you will be able to send and receive e-mail notification.

# 11. Notification Messages

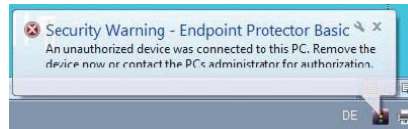
---

In order to see notifications, the EPP Basic Notifier needs to be running. In case your Notifier is running, you will see its icon in the System Tray. When you right click the icon, you will have the option to launch the application, or to exit the Notifier.



You can restart the Notifier from Start > All Programs > Endpoint Protector Basic.

Every time a new device or an unauthorized device is connected to the protect PC, a message will pop up in the right corner of the screen. The message will notify the PC user about the unauthorized use of a portable device.



You will be also notified from time to time, by a similar message, about the trial period of Endpoint Protector Basic if you are testing the software as a trial.

## 12. About

---

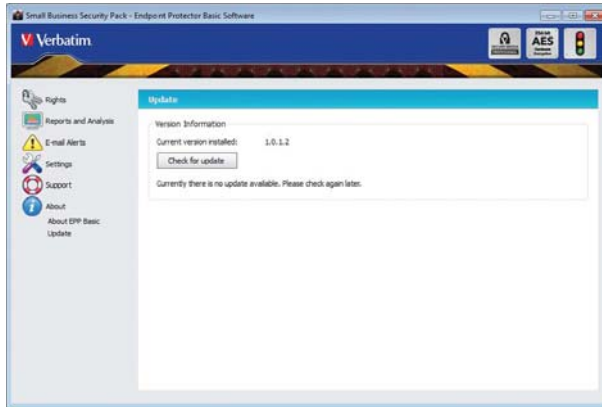
### 12.1. License Key Registration

---

Your version of Endpoint Protector Basic comes with a lifetime license; therefore you will be able to use the full functionality of the application on your PC.

## 12.2. Update Mechanism

You can check for the availability of a newer Endpoint Protector Basic version by clicking the “Check for Update” button in the “About” module, “Update” menu.



If there is a newer version available you will be asked if you want to download it.

The application will be downloaded directly to your PC.

After download is complete, you will have the option to “Install it” by clicking the button.

## 13. Uninstall

To remove Endpoint Protector Basic from your PC, please go to Control Panel > Add or Remove Programs > Endpoint Protector Basic > Remove. Before doing this you have to close Endpoint Protector Basic Settings.

Uninstalling Endpoint Protector Basic will require entry of the Endpoint Protector Basic password even for users that have administrative rights on the protected PC.

**IMPORTANT!** Uninstalling the application will give full access to all USB drives that were and will be plugged into your PC.

# 14. Support

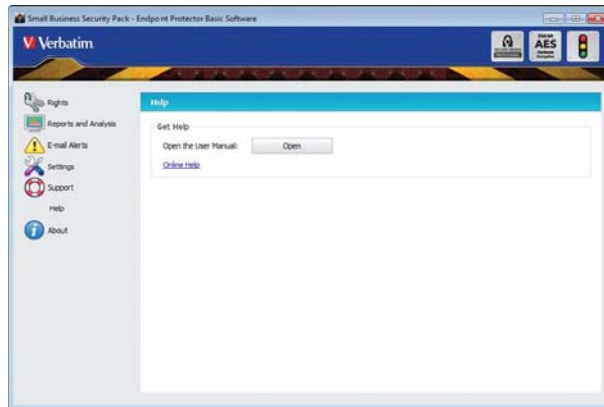
---

Visit [http://www.verbatim-europe.co.uk/en\\_1/support\\_usb-devices\\_1.html](http://www.verbatim-europe.co.uk/en_1/support_usb-devices_1.html)

One of our team members will contact you in the shortest time possible.

Even if you do not have a problem but miss some feature or just want to leave us general comment we would love to hear from

you. Your input is much appreciated and we welcome any input to make computing with portable devices safe and convenient.



© 2004 - 2010 CoSoSys Ltd. All rights reserved. Windows is registered trademark of Microsoft Corporation. All other names and trademarks are property of their respective owners.

# 1. Introduction

---

Endpoint Protector Basic™ vous aidera à sécuriser les points terminaux de vos PC en contrôlant et surveillant l'utilisation des périphériques. Vous pourrez restreindre l'utilisation de l'USB, FireWire et d'autres ports et de contrôler l'utilisation des dispositifs portables sur votre ordinateur. Vous pouvez trouver une liste complète de tous les types de dispositifs contrôlés dans le chapitre "0. 4. Types de Dispositifs Contrôlés". Ainsi, vous prévenez efficacement l'introduction des données indésirables ou le vol de données de votre PC.

- Avec Endpoint Protector Basic vous pouvez:
- Permettre ou restreindre l'utilisation de n'importe quel dispositif de stockage USB ou d'autre dispositif de stockage portable sur votre ordinateur
- Identifier tout dispositif de stockage USB utilisé en relation avec votre ordinateur
- Voir les détails de tous les dispositifs de stockage USB connectés à l'ordinateur à un certain moment
- Permettre à l'administrateur du PC de recevoir un e-mail quand un dispositif de stockage USB non-autorisé est connecté à un poste de travail
- Utiliser le traçage des fichiers pour surveiller l'accès aux fichiers sur n'importe quel dispositif de stockage USB

## 2. Famille de Produits Endpoint Protector

---

La famille de produits Endpoint Protector offre le contrôle des dispositifs et la sécurité des points terminaux pour tout environnement pour des ordinateurs à domicile ou des MACs, des bureaux de taille moyenne ou même des réseaux d'entreprise.

Endpoint Protector Basic est une partie d'elle et il offre à vos PC à domicile et au bureau la meilleure solution pour contrôler l'utilisation des dispositifs portables sur vos PC protégés afin que vos données ne puissent pas être copiées sans autorisation sur des dispositifs indésirables.

Autres produits de la famille Endpoint Protector incluent:

- My Endpoint Protector (une solution Software as a Service pour sécuriser les PC et les MACs à travers un portail internet <https://my.EndpointProtector.com>)
- Endpoint Protector (une solution client - serveur pour le contrôle des dispositifs pour les

entreprises de taille petite et moyenne)

- Endpoint Protector Appliance (une solution appareil matériel pour le contrôle des dispositifs pour les entreprises de taille petite et moyenne)

Plus d'informations peuvent être trouvées ici <http://www.EndpointProtector.fr>.

### 3. Configuration Requise

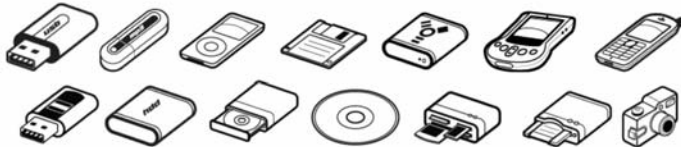
---

- Systèmes d'exploitation supportés:
  - o Windows 7 (32bit / 64bit)
  - o Windows Vista (32bit / 64bit)
  - o Windows XP (Service Pack 2 est recommandé)
  - o Windows 2000
  - o Des droits d'administration sont requis pour installer le logiciel sur un ordinateur et pour autoriser ou bloquer des dispositifs
- 32MB de mémoire disponible sur le disque dur
- Un minimum de 256MB RAM est recommandé

### 4. Types de Dispositifs Contrôlés

---

Endpoint Protector Basic supporte une large gamme de types de dispositifs qui représentent les sources clé des brèches de sécurité. Ces dispositifs peuvent être autorisés ce qui fait possible que les utilisateurs voient, créent ou modifient leur contenu et que les administrateurs voient les données transférées vers et depuis les dispositifs autorisés.



- Dispositifs de Stockage Amovibles
- Dispositifs USB Flash Normales, Dispositifs U3 et Auto-exécutables, Disque sur Clé, etc.
- USB 1.1, USB 2.0, USB 3.0
- Cartes de mémoire - Cartes SD, Cartes MMC et Cartes Flash Compact, etc.
- Lecteurs de Cartes - interne et externe
- Lecteur/Graveur CD/DVD - interne et externe
- Caméra Numérique
- dispositifs compatibles avec Smartphones / Handhelds / PDAs (incluant Nokia N-Series, Blackberry, et Windows CE), dispositifs Windows Mobile, etc.
- iPods / iPhones / iPads
- Lecteur MP3 / Dispositifs Media Player
- Disques durs externes / Disques durs portables
- Dispositifs FireWire
- Dispositifs PCMCIA
- Dispositifs Biométriques
- Bluetooth
- Imprimantes (s'applique pour les connexions série, USB et LTP)
- ExpressCard (SSD)
- Wireless USB
- Ports LPT/Parallèles (En contrôlant les ports parallèles d'un PC avec Endpoint Protector Basic, l'administrateur du réseau peut bloquer ou permettre l'accès des utilisateurs aux dispositifs de stockage connectés à ces ports.) \*S'APPLIQUE UNIQUEMENT AUX DISPOSITIFS DE STOCKAGE
- Disquettes

## 5. Installation

---

Pour installer Endpoint Protector Basic il est nécessaire d'être connecté sur le poste de travail avec des droits d'administration complets.

Exécutez le fichier EPPBasic.exe.



EPPBasicSetup.exe

Type: Application

Endpoint Protector Basic va s'installer dans le start menu et va créer le groupe Endpoint Protector Basic. Endpoint Protector Basic va demander dans certains cas de redémarrer votre PC pour l'aboutissement du processus d'installation.

Après une installation avec succès Endpoint Protector Basic s'exécutera toujours dans le background pour protéger les points terminaux de vos PCs quand vous ou d'autres utilisateurs sont connectés sur le PC.

## 6. Démarrer

---

**IMPORTANT!** Assurez-vous que vous êtes connecté sur le PC en tant qu'administrateur. Endpoint Protector Basic vient avec une Interface de configuration, qui sera disponible uniquement pour les Administrateurs connectés. Si un utilisateur standard se connecte dans le système l'Interface de configuration ne sera pas accessible.

Pour commencer à utiliser Endpoint Protector Basic, allez dans Start > All Programs > Endpoint Protector Basic > Endpoint Protector Basic.Droits

## 7. Droits





---

Ce module vous permettra de préciser quel dispositif spécifique peut être accessible sur votre PC.

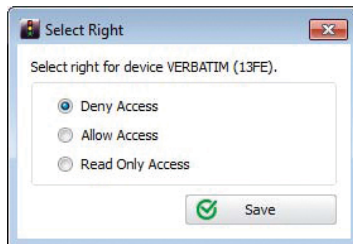
Chaque fois qu'un nouveau dispositif est connecté à l'ordinateur pendant que l'application Endpoint Protector Basic Settings est ouverte, vous allez le voir automatiquement dans la liste "Dispositifs". Au cas où vous ne pouvez pas voir le dispositif dans la liste, vous pouvez cliquer le bouton "Actualiser" dans le coin inférieur à droite de la fenêtre.



La colonne du statut indique les droits actuels pour les dispositifs.

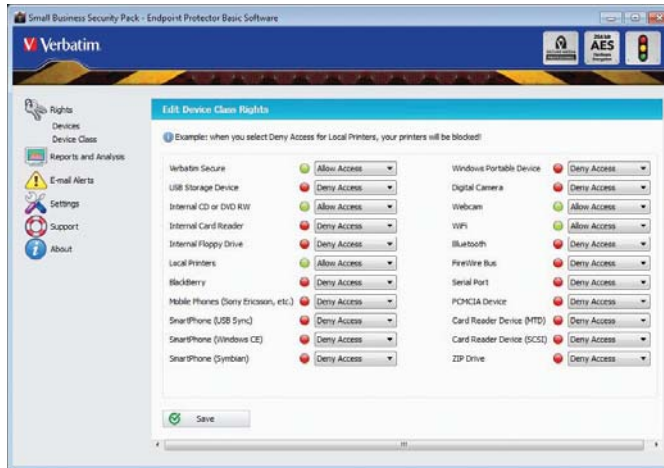
-  Rouge signifie que le dispositif est bloqué sur votre PC.
-  Vert signifie que le dispositif est autorisé sur votre PC.
-  Jaune signifie que le dispositif a des droits de lecture seule sur votre PC.
-  Gris signifie que le dispositif n'est pas actuellement connecté au PC.

Avec un click de souris sur le point de statut d'un dispositif, un menu s'ouvrira. Ce menu vous donne accès aux paramètres suivants:



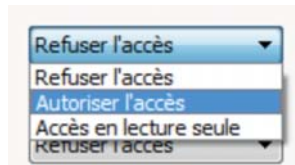
## 7.2 Classe de Dispositifs

Ce module vous permettra de spécifier quelle classe de dispositifs peut être accessible sur votre PC.



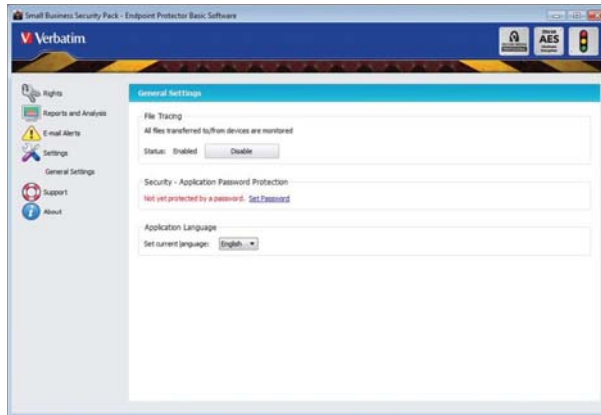
Les types de dispositifs suivants auront des droits Permettre l'Accès implicites: WiFi, Imprimantes Locales, Webcams et lecteurs de CDs.

Afin de changer les droits pour une classe de dispositifs, vous devez cliquer la boîte de sélection à côté du nom de la classe de dispositifs. Les options que vous avez sont: "Refuser l'Accès", "Permettre l'Accès" et "Accès en Lecture Seule".



## 8. Paramètres

L'étiquette Paramètres Généraux vous donne l'option de désactiver le Traçage des Fichiers, qui est activé implicitement. Vous pouvez désactiver cette option si vous n'avez pas besoin de cet niveau supplémentaire de sécurité.

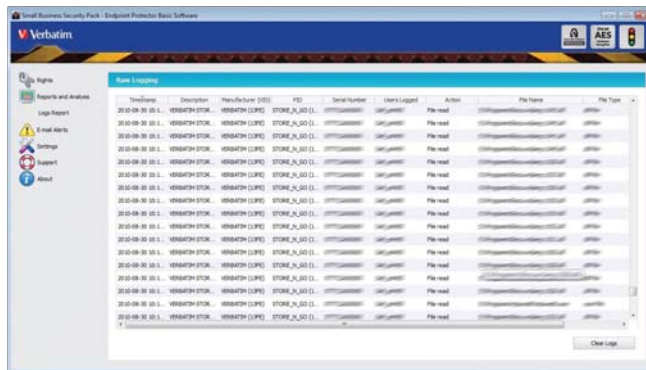


Ici vous pouvez aussi protéger par mot de passe l'accès à l'Interface Utilisateur Endpoint Protector Basic ou sélectionner vos paramètres de langue.

## 8.1 Traçage des Fichiers

La fonctionnalité de Traçage des Fichiers permet à l'administrateur d'enregistrer les caractéristiques des fichiers qui sont écrits ou lus de ou vers les dispositifs de stockage portable pour une analyse ultérieure.

Vous pouvez vérifier ultérieurement les fichiers qui ont été accédés dans Rapports des Journaux, du module "Rapports et Analyses".



## 8.2 Mot de passe de protection

L'accès à l'Interface Utilisateur d'Endpoint Protector Basic peut être protégé par mot de passe.

Après saisir vos paramètres de mot de passe, vous devez cliquer le bouton "Etablir Mot de Passe" afin de les sauver.



The screenshot shows a 'Sécurité' (Security) window titled 'Protégé par mot de passe.' (Protected by password). It contains the following fields and buttons:

- Ancien mot de passe: [password field]
- Nouveau mot de passe: [password field]
- Confirmer le mot de passe: [password field]
- Suggestion de mot de passe: [password field] (containing 'se dont je me souviendrai')
- Réinitialiser mot de passe: [button]
- Etablir le mot de passe: [button]

Vous avez aussi l'option de sauver un 'Indice' (rappel) pour le Mot de Passe. Ce peut être utile si vous oubliez le mot de passe.

Pour enlever la protection par Mot de Passe, vous devez cliquer le bouton "Réinitialiser Mot de Passe".

Après avoir établi un mot de passe, on va vous demander de le saisir chaque fois que vous démarrez Endpoint Protector Basic.



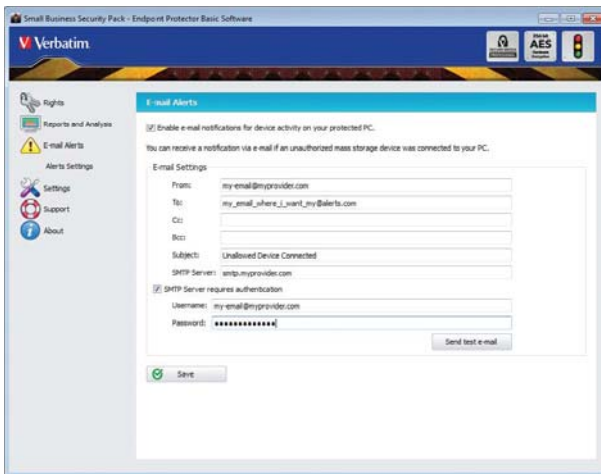
Au cas où vous n'avez pas sauvé un 'Indice', cette fonctionnalité sera cachée dans le dialogue de Connexion.

<b>Option</b>	<b>Explication</b>
Réfuser l'Accès	Le dispositif sera bloqué sur votre PC
Permettre l'Accès	Le dispositif sera autorisé sur votre PC
Accès en lecture seule	Le dispositif aura uniquement des droits de lecture seule sur votre PC



## 10.1 Paramètres des Alertes

Si vous activez l'option de notification e-mail vous devez fournir un compte e-mail SMTP dans Endpoint Protector Basic qui sera utilisé pour envoyer les notifications à une adresse e-mail spécifiée.



Veillez préciser les adresses e-mail expéditeur et destinataire. Saisissez l'adresse de votre serveur SMTP avec votre nom d'utilisateur et mot de passe pour le cas où votre serveur SMTP requiert ces informations afin d'envoyer un e-mail.

Vous pouvez aussi vérifier si vos paramètres sont corrects en cliquant sur le bouton "Envoyer e-mail de test".

Si un pare-feu est installé sur le PC que vous protégez avec Endpoint Protector Basic, le pare-feu vous demandera d'autoriser que Endpoint Protector Basic accède à l'Internet. Veuillez donner à Endpoint Protector Basic cette autorisation afin de pouvoir envoyer et recevoir des notifications e-mail.

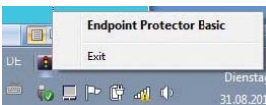
# 11. Messages de Notification

---

Pour voir les notifications, le Notifiant EPP Basic doit être en exécution.

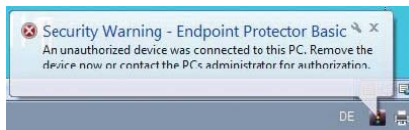
Dans le cas où votre Notifiant est en exécution, vous allez voir son icône dans le System Tray.

Quand vous cliquez droite sur l'icône, vous allez avoir l'option de lancer l'application ou de quitter le Notifiant.



Vous pouvez redémarrer le Notifiant de Start > All Programs > Endpoint Protector Basic.

Chaque fois qu'un nouveau dispositif ou un dispositif non-autorisé est connecté à l'ordinateur protégé, un message apparaîtra dans le coin à droite de l'écran. Le message notifiera l'utilisateur du PC sur l'utilisation non-autorisée d'un dispositif portable.



Vous serez également notifié de temps en temps, par un message similaire, sur la période d'essai de Endpoint Protector Basic si vous testez le logiciel comme essai.

## 12. À propos de

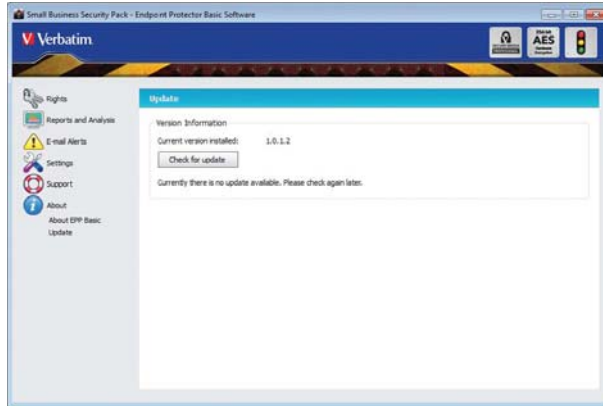
---

### 12.1 Enregistrement des Clés de Licences

---

Votre version Endpoint Protector Basic vient avec une licence à vie, donc vous pouvez utiliser toutes les fonctionnalités de l'application sur votre PC.

## 12.2 Mécanisme des Mises à Jour



Vous pouvez vérifier la disponibilité d'une version plus récente d'Endpoint Protector Basic en cliquant sur le bouton "Chercher Mises à Jour" dans l'étiquette "À propos de", menu "Mise à Jour".

S'il y a une version plus récente disponible on va vous demander si vous souhaitez la télécharger.

L'application sera téléchargée directement sur votre PC.

Après l'aboutissement du téléchargement, vous aurez l'option de "Installer" en cliquant le bouton.

## 13. Désinstaller

Pour enlever Endpoint Protector Basic de votre PC, veuillez aller dans Control Panel > Add or Remove Programs > Endpoint Protector Basic > Remove. Avant de le faire vous devez fermer Endpoint Protector Basic Settings.

La désinstallation d'Endpoint Protector Basic va demander de saisir le mot de passe Endpoint Protector Basic même pour les utilisateurs qui ont des droits administratifs sur le PC protégé.

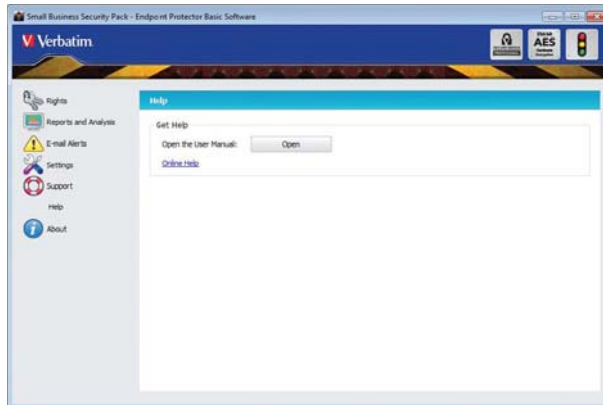
**IMPORTANT!** Désinstaller l'application donnera des droits complets à tous les dispositifs USB qui ont été et seront connectés à votre PC.

# 14. Support

---

[http://www.verbatim-europe.co.uk/en\\_1/support\\_usb-devices\\_1.html](http://www.verbatim-europe.co.uk/en_1/support_usb-devices_1.html)

Même si vous n'avez pas un problème, mais vous manquez certaines caractéristiques ou vous souhaitez simplement nous laisser un commentaire général, nous aimerions entendre de vous. Votre contribution est très appréciée et nous accueillons favorablement toute contribution afin de rendre l'utilisation des dispositifs portables sécuritaire et pratique.



© 2004 - 2010 CoSoSys Ltd. Tous droits réservés. Windows est une marque enregistrée de Microsoft Corporation. Tout autre nom et marque sont propriété de leurs propriétaires respectifs.

# 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 „0. 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.de>.

### **3. Systemanforderungen**

---

- Unterstützte Betriebssysteme sind:
  - o Windows 7 (32bit / 64bit)
  - o Windows Vista (32bit / 64bit)
  - o Windows XP (Service Pack 2 wird empfohlen)
  - o Windows 2000
  - o 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.



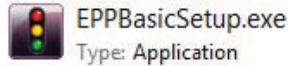
- Tragbare Datenspeicher
- Normal USB Flash Sticks, U3 and Autorun Geräte, etc.
- USB 1.1, USB 2.0, USB 3.0
- Speicherkarten - SD Karten, MMC Karten und Compact Flash Karten, etc.
- Kartenlesegeräte - interne und externe
- CD / DVD-Player / Brenner - interne und externe
- Digitalkameras
- Smartphones / 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, dass 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 Geräte in Verbindung mit Ihrem PC verwendet werden dürfen.

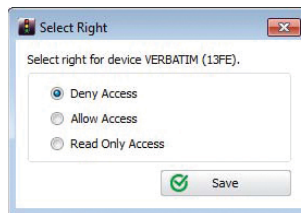
Jedes Mal, wenn ein neues Gerät am PC angeschlossen wird, wird dieses automatisch in Geräte-Liste erscheinen. Falls Sie ein Gerät nicht in der Liste sehen, klicken Sie auf die Schaltfläche "Aktualisieren".



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

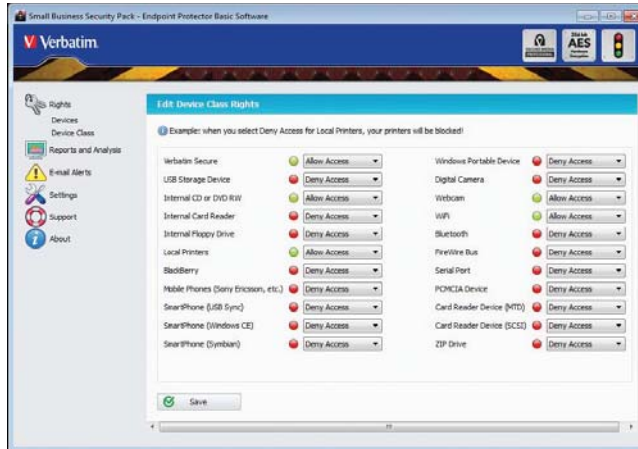
- Rot bedeutet, dass das Gerät am PC gesperrt ist.
- Grün bedeutet, dass das Gerät am PC freigegeben ist und verwendet werden darf.
- Gelb bedeutet, dass das Gerät auf dem PC nur Lesezugriff hat.
- Grau bedeutet, dass das Gerät momentan nicht mit dem PC verbunden ist.

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



## 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.

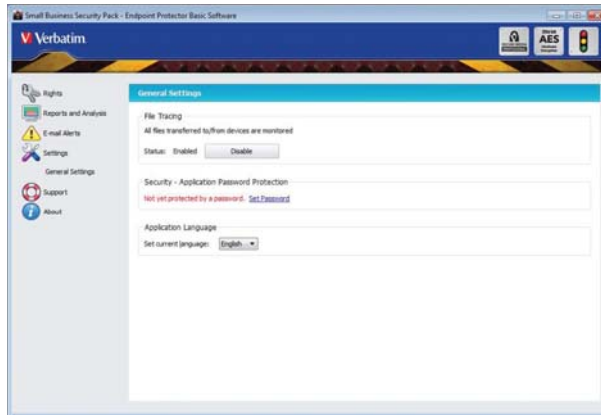
Um die Rechte eines Geräte Typs festzulegen, müssen Sie im Auswahlfeld neben dem Gerät Typ eine der Möglichkeiten „Zugriff sperren“, „Zugriff erlauben“ oder „Lesezugriff (kein Schreibzugriff)“ auswählen.



## 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.

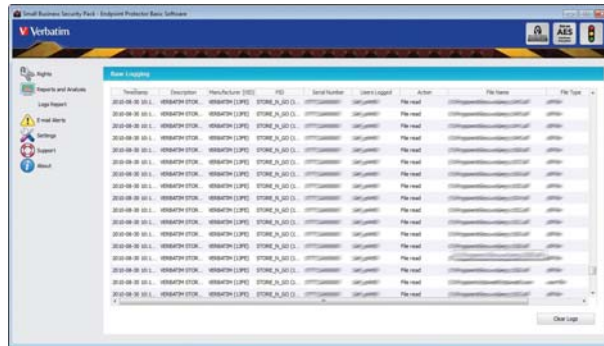


Hier können Sie auch den Zugriff auf die Endpoint Protector Basic Konfigurationsoberfläche mit einem Passwort schützen sowie die Sprache der Konfigurationsoberfläche ändern.

## 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.



## 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.



The screenshot shows a 'Sicherheit' (Security) dialog box with the status 'Geschützt.' (Protected). It contains the following fields and buttons:

- 'Altes Passwort:' (Old Password) with a masked input field (\*\*\*\*\*).
- 'Neues Passwort:' (New Password) with a masked input field (\*\*\*\*\*).
- 'Neues Passwort bestätigen:' (Confirm New Password) with a masked input field (\*\*\*\*\*).
- 'Passwort hinweis:' (Password Hint) with a text input field containing 'Was mich an das Passwort'.
- 'Passwort zurücksetzen' (Reset Password) button.
- 'Passwort festlegen' (Set Password) button.

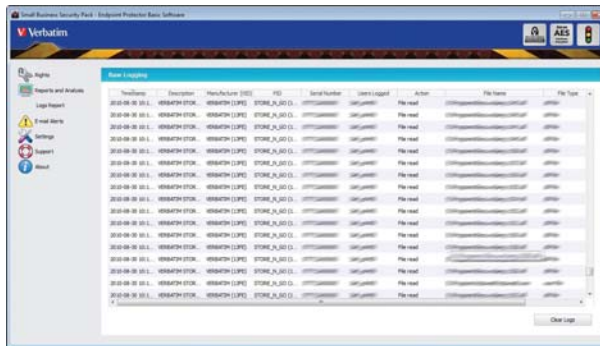
Um den Passwortschutz zu entfernen klicken Sie auf die Schaltfläche "Passwort zurücksetzen".

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

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

## 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.



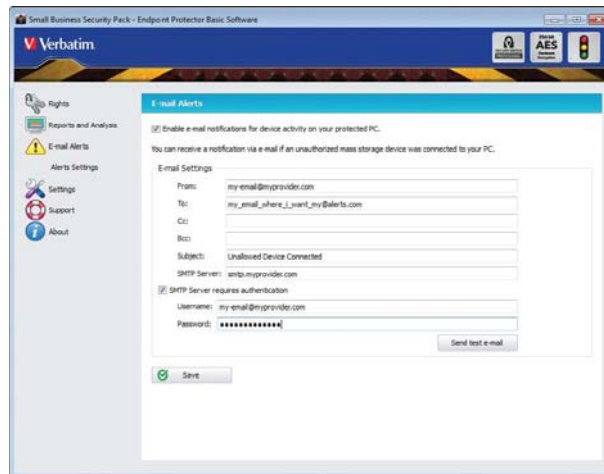
Sie können die einzelnen aufgezeichneten Events nach Datum & Uhrzeit, Benutzer, Aktion, Dateityp, Produkt-ID (PID), Hersteller-ID (VID), etc. mit einem Klick auf den Tabellenkopf sortieren.

## 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.

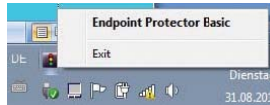
# 11. System Tray Benachrichtigungen

---

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

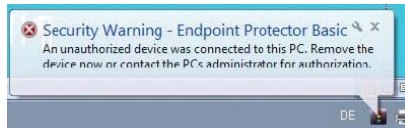
Der EPP Basic Notifier ist gestartet, wenn Sie das Endpoint Protector Basic System Tray Icon sehen können.

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

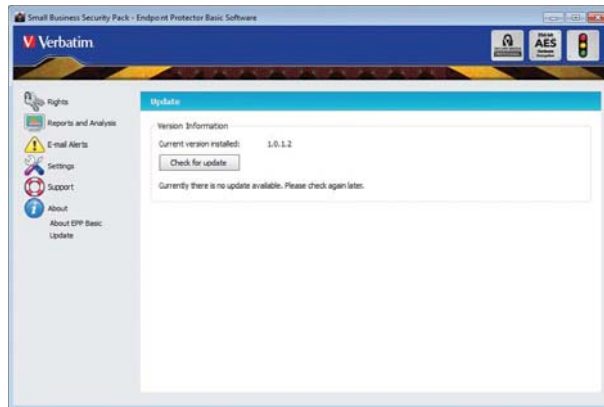
---

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.

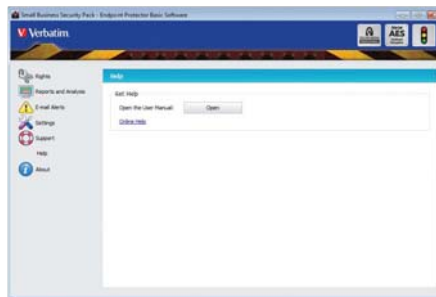
## 14. Hilfe / Support

---

Hilfe erhalten Sie unter folgender Webseite:

[http://www.verbatim-europe.co.uk/en\\_1/support\\_usb-devices\\_1.html](http://www.verbatim-europe.co.uk/en_1/support_usb-devices_1.html)

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.



© 2004 - 2010 CoSoSys Ltd. Alle Rechte vorbehalten. Windows ist ein eingetragenes Warenzeichen der Corporation Microsoft. Alle anderen Namen und Marken sind Eigentum ihrer jeweiligen Besitzer.

