ENDPOINT PROTECTOR BASIC

User Manual Version 3.7

User Manual

COSOSYS

Table of Contents

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 on 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 from home PCs or MACs to 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 your data cannot be copied without authorization to unwanted devices.

Other products from the Endpoint Protector Product family include:

- My Endpoint Protector (a Software as a Service solution to secure PCs and MACs over an 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)

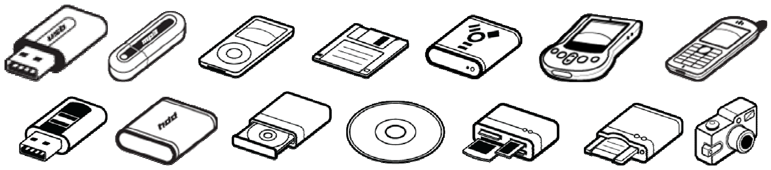
More information can be found here http://www.EndpointProtector.com

3. System Requirements

- Supported Operating Systems are:
  - Windows 7 (32bit / 64bit)
  - Windows Vista (32bit / 64bit)
  - Windows XP (Service Pack 2 is recommended)
  - Windows 2003
  - Administrative rights are required for installing the software on a PC and to be able to authorize or unauthorize 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
- Serial ATA Controllers

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.

EPPBasic.exe
2/15/2011 11:03 AM
This installer database contain...

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.

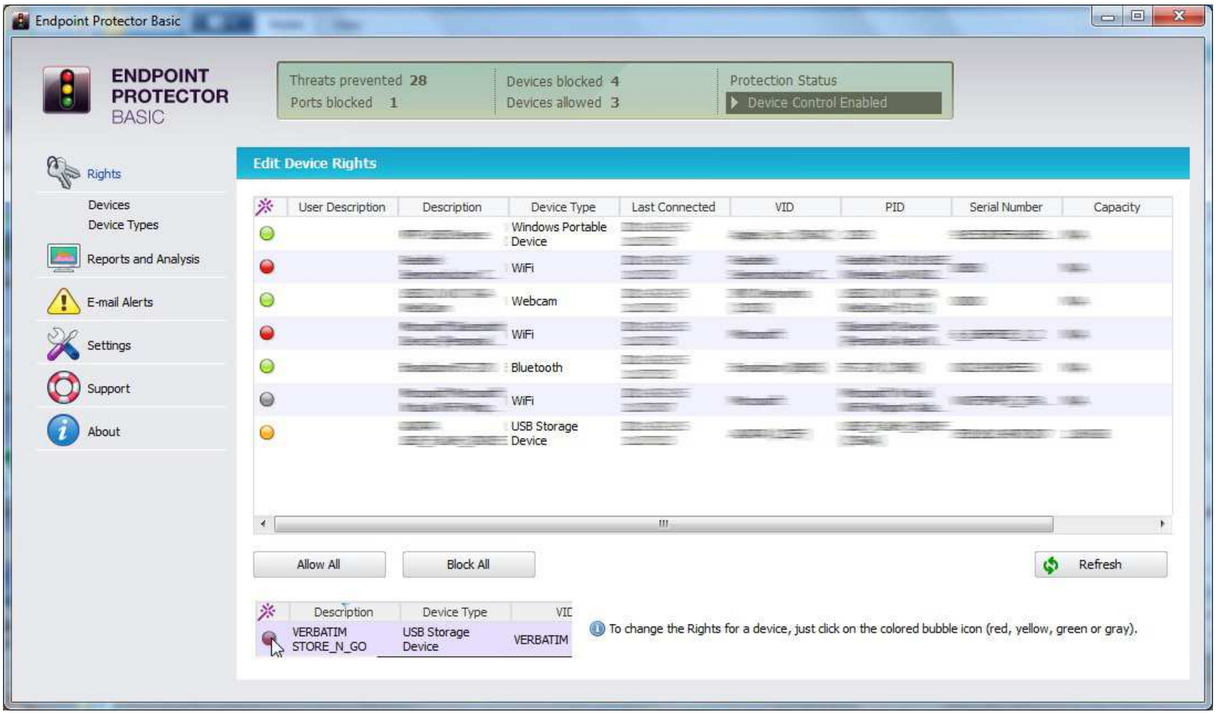
To start using Endpoint Protector Basic, go to Start > All Programs > Endpoint Protector Basic > Endpoint Protector Basic.

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.



Threats prevented 28
Ports blocked 1
Devices blocked 4
Devices allowed 3
Protection Status
Device Control Enabled

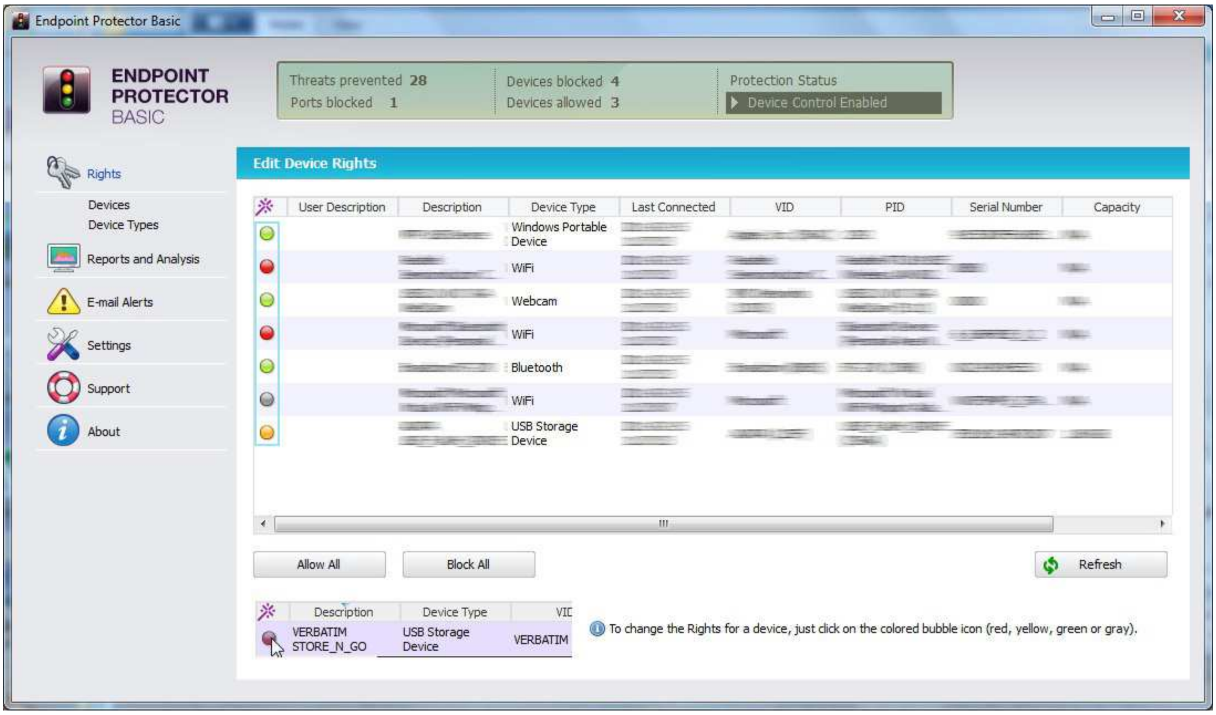
Edit Device Rights

	User Description	Description	Device Type	Last Connected	VID	PID	Serial Number	Capacity
🟢		[illegible]	Windows Portable Device	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
🔴		[illegible]	WiFi	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
🟢		[illegible]	Webcam	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
🔴		[illegible]	WiFi	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
🟢		[illegible]	Bluetooth	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
⚪		[illegible]	WiFi	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
🟡		[illegible]	USB Storage Device	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

	Description	Device Type	VID
●	VERBATIM STORE_N_GO	USB Storage Device	VERBATIM

To change the Rights for a device, just click on the colored bubble icon (red, yellow, green or gray).

The status column indicates the current rights for the devices.



Endpoint Protector Basic

ENDPOINT PROTECTOR BASIC

Threats prevented 28
Ports blocked 1
Devices blocked 4
Devices allowed 3
Protection Status
Device Control Enabled

Edit Device Rights

	User Description	Description	Device Type	Last Connected	VID	PID	Serial Number	Capacity
🟢		[redacted]	Windows Portable Device	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
🔴		[redacted]	WiFi	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
🟢		[redacted]	Webcam	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
🔴		[redacted]	WiFi	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
🟢		[redacted]	Bluetooth	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
●		[redacted]	WiFi	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
🟡		[redacted]	USB Storage Device	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

	Description	Device Type	VIC
🔴	VERBATIM STORE_N_GO	USB Storage Device	VERBATIM

To change the Rights for a device, just click on the colored bubble icon (red, yellow, green or gray).

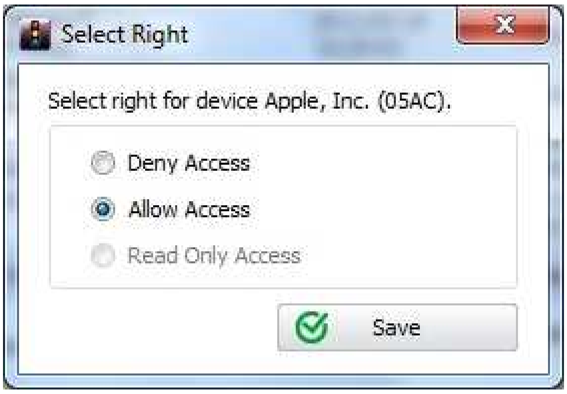
🔴 Red means that the device is blocked on your PC

🟢 Green means that the device is allowed on your PC

🟡 Yellow means that the device has read only rights on your PC

● Gray 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:



Select Right

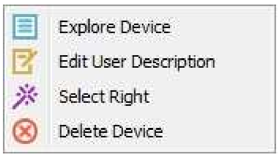
Select right for device Apple, Inc. (05AC).

○ Deny Access
● Allow Access
○ Read Only Access

Option	Explanation
Deny Access	The device will be blocked 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

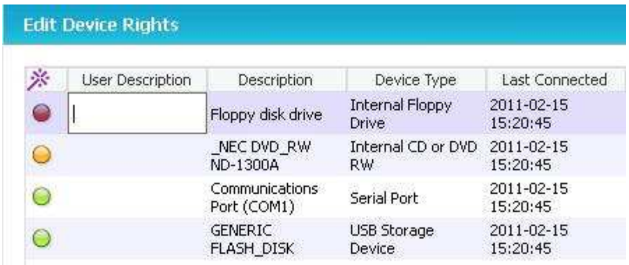
The options Allow All and Block All offer the possibility to allow access to all devices and, respectively, block all devices by a simple click of a button.

You can set rights for a specific device also by right-clicking on it in the list of devices and choosing the Select Right option from the displayed menu.



The Explore Device option will open a new window displaying the content of the selected device. In case that a specific device is blocked, disconnected or it does not have a drive letter assigned to it, the above option will not be available.

The Edit User Description option will allow you to insert a short description for a selected device.

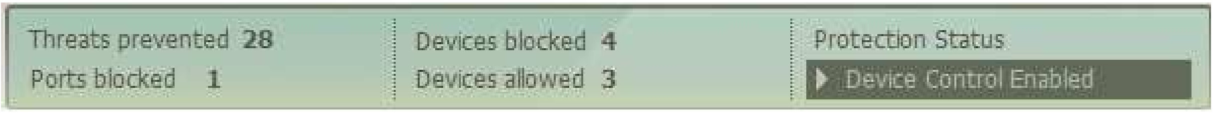


Edit Device Rights

	User Description	Description	Device Type	Last Connected
🔴	|	Floppy disk drive	Internal Floppy Drive	2011-02-15 15:20:45
🟠		_NEC DVD_RW ND-1300A	Internal CD or DVD RW	2011-02-15 15:20:45
🟢		Communications Port (COM1)	Serial Port	2011-02-15 15:20:45
🟢		GENERIC FLASH_DISK	USB Storage Device	2011-02-15 15:20:45

The Delete Device option will remove the selected device form the list of devices.

The Status header displayed at the top of each window allows you to check at any moment the exact number of blocked and allowed devices or ports and the current Protection status.



Threats prevented **28**

Ports blocked **1**

Devices blocked **4**

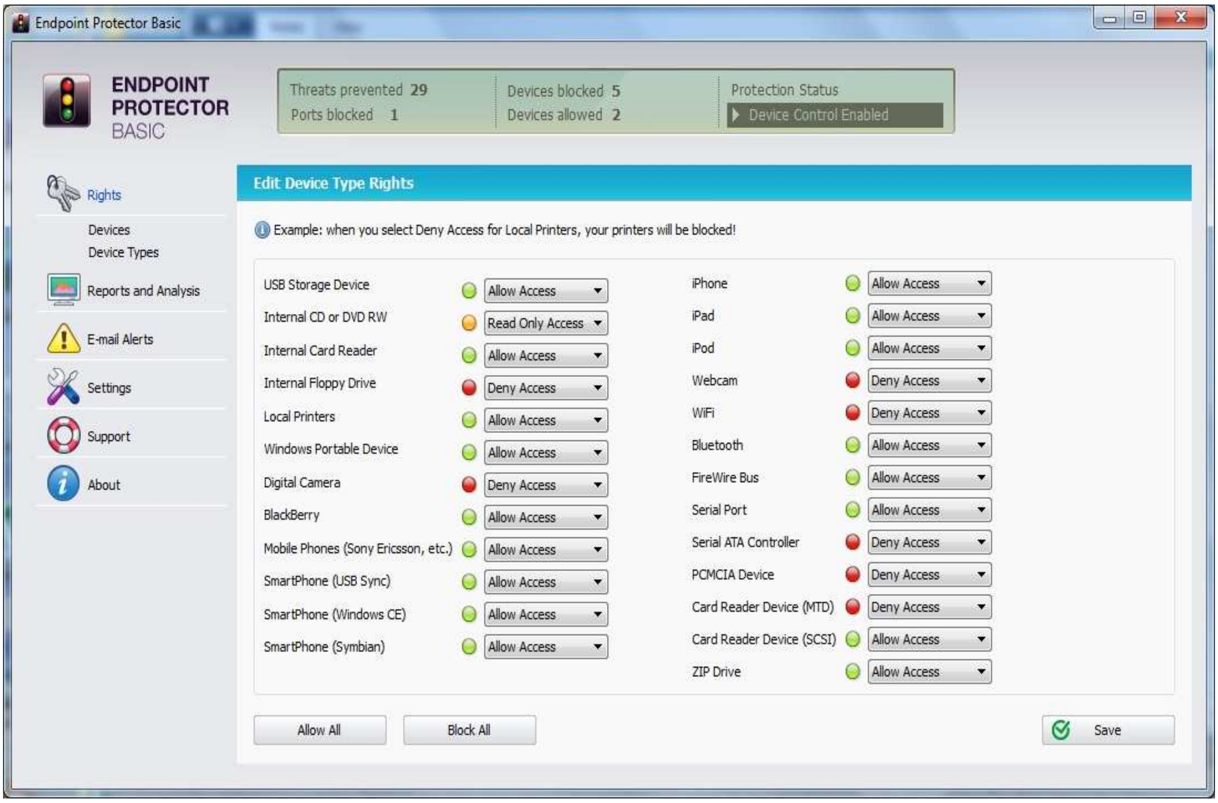
Devices allowed **3**

Protection Status

▶ Device Control Enabled

7.2. Device Types

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



Threats prevented 29
Ports blocked 1
Devices blocked 5
Devices allowed 2
Protection Status
Device Control Enabled

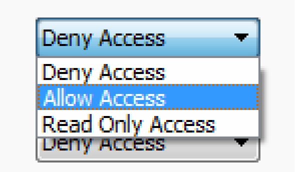
Edit Device Type Rights

Example: when you select Deny Access for Local Printers, your printers will be blocked!

USB Storage Device	Allow Access	iPhone	Allow Access
Internal CD or DVD RW	Read Only Access	iPad	Allow Access
Internal Card Reader	Allow Access	iPod	Allow Access
Internal Floppy Drive	Deny Access	Webcam	Deny Access
Local Printers	Allow Access	WiFi	Deny Access
Windows Portable Device	Allow Access	Bluetooth	Allow Access
Digital Camera	Deny Access	FireWire Bus	Allow Access
BlackBerry	Allow Access	Serial Port	Allow Access
Mobile Phones (Sony Ericsson, etc.)	Allow Access	Serial ATA Controller	Deny Access
SmartPhone (USB Sync)	Allow Access	PCMCIA Device	Deny Access
SmartPhone (Windows CE)	Allow Access	Card Reader Device (MTD)	Deny Access
SmartPhone (Symbian)	Allow Access	Card Reader Device (SCSI)	Allow Access
		ZIP Drive	Allow Access

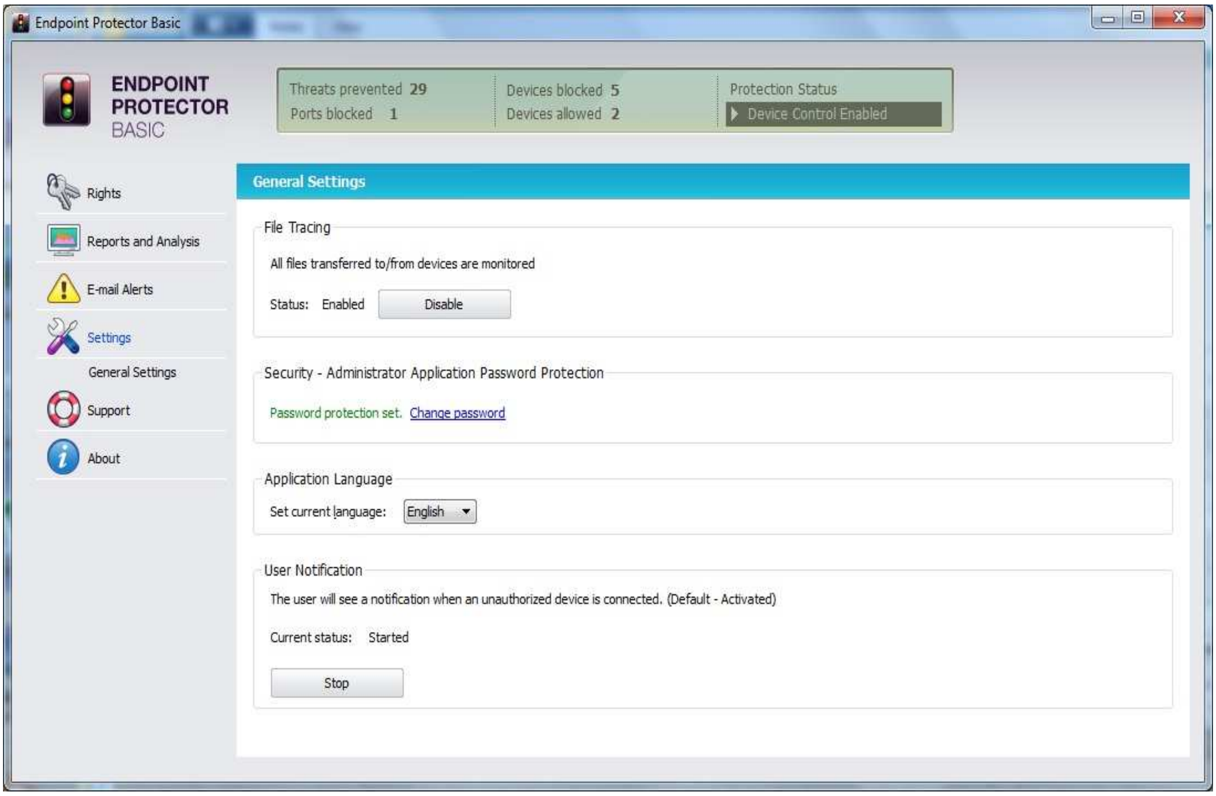
By default the following device types will have Allow Access rights: WiFi, Local Printers, Webcams and CD-ROMs.

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.



Threats prevented 29
Ports blocked 1
Devices blocked 5
Devices allowed 2
Protection Status
Device Control Enabled

General Settings

File Tracing

All files transferred to/from devices are monitored

Status: Enabled

Security - Administrator Application Password Protection

Password protection set.

Application Language

Set current language: English

User Notification

The user will see a notification when an unauthorized device is connected. (Default - Activated)

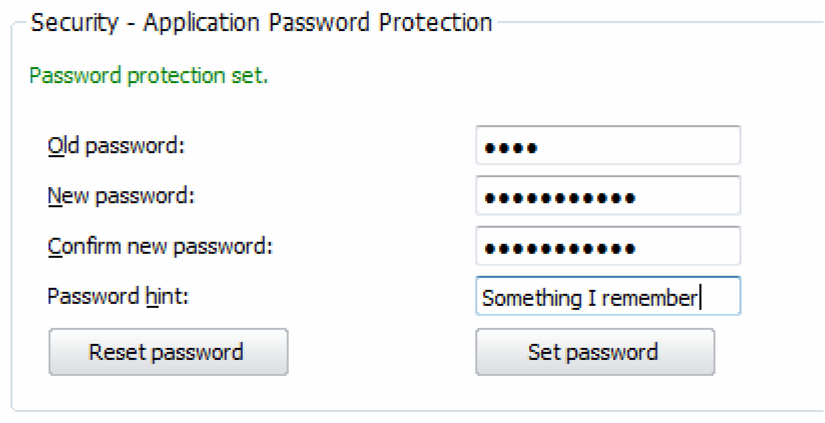
Current status: Started

Here you can also password protect the access to the Endpoint Protector Basic User Interface, select your Language settings or enable/disable the option of notifying the user when an unauthorized device is connected to the computer.

8.1. 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: ●●●●●●●●●●●

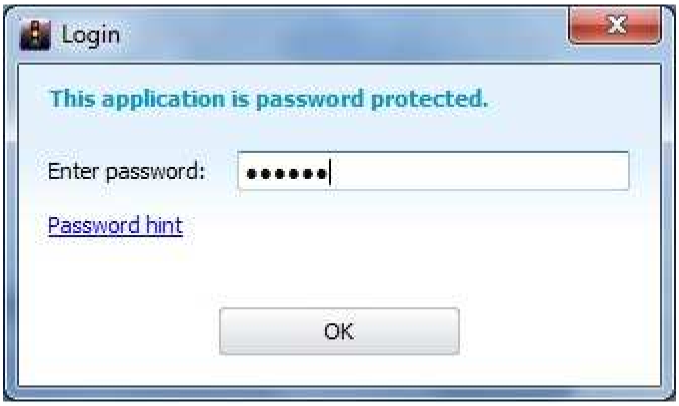
Confirm new password: ●●●●●●●●●●●

Password hint: Something I remember

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.



Login

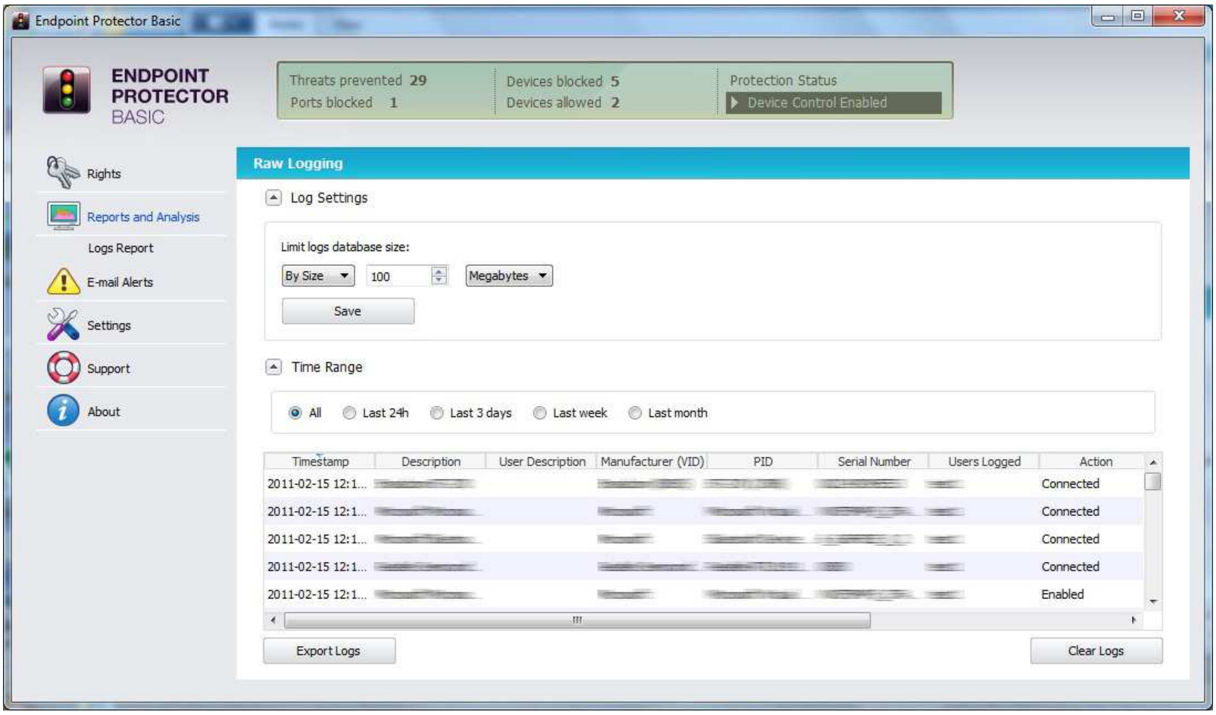
This application is password protected.

Enter password: ●●●●●●

In case that no 'Hint' is saved, the 'No hint defined!' text will be displayed when clicking on Password hint.

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.



Threats prevented 29
Ports blocked 1
Devices blocked 5
Devices allowed 2
Protection Status
Device Control Enabled

Limit logs database size: By Size ▾ 100 Megabytes ▾

● All ○ Last 24h ○ Last 3 days ○ Last week ○ Last month

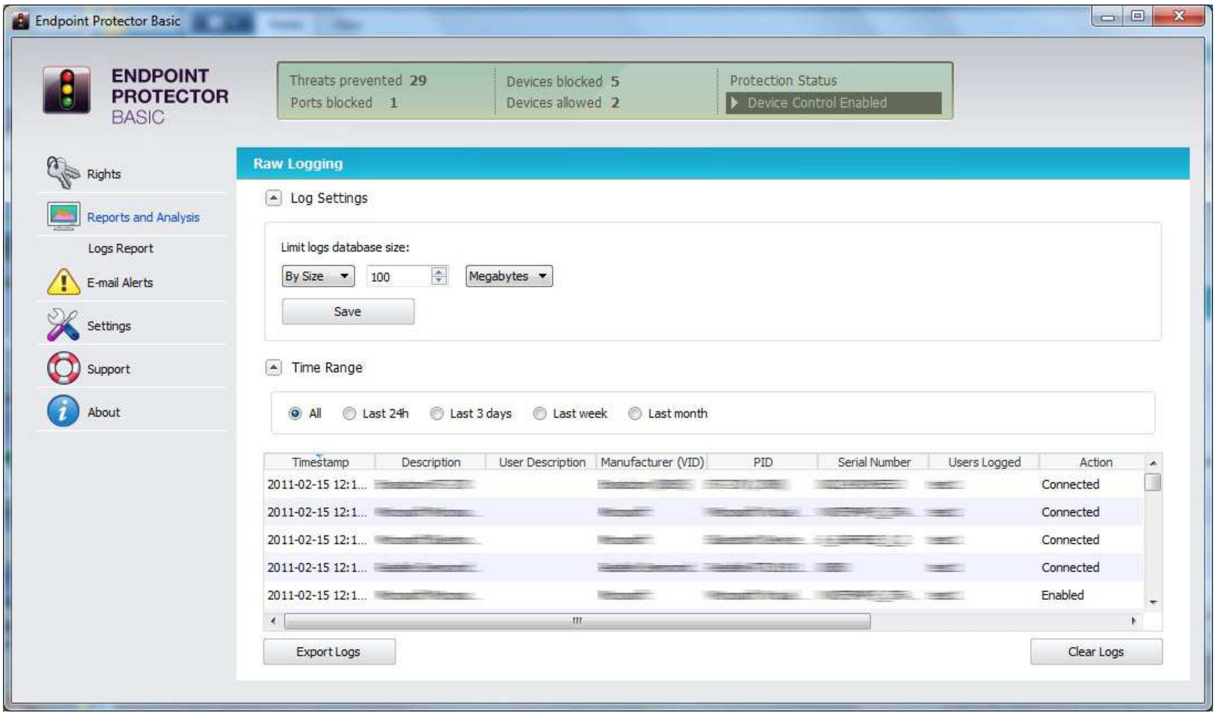
Timestamp	Description	User Description	Manufacturer (VID)	PID	Serial Number	Users Logged	Action
2011-02-15 12:1...	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	Connected
2011-02-15 12:1...	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	Connected
2011-02-15 12:1...	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	Connected
2011-02-15 12:1...	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	Connected
2011-02-15 12:1...	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	Enabled

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”.

9.1. 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.



Threats prevented 29
Ports blocked 1
Devices blocked 5
Devices allowed 2
Protection Status
▶ Device Control Enabled

Raw Logging

Log Settings

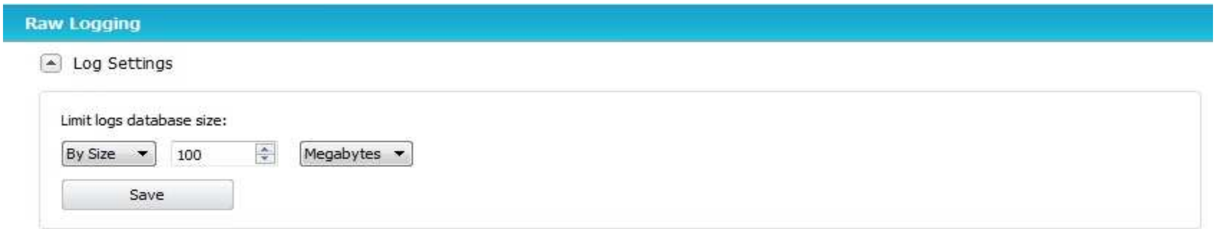
Limit logs database size: By Size | 100 | Megabytes

Time Range

● All ○ Last 24h ○ Last 3 days ○ Last week ○ Last month

Timestamp	Description	User Description	Manufacturer (VID)	PID	Serial Number	Users Logged	Action
2011-02-15 12:1...	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	Connected
2011-02-15 12:1...	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	Connected
2011-02-15 12:1...	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	Connected
2011-02-15 12:1...	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	Connected
2011-02-15 12:1...	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	Enabled

Additionally, you can select a limit for the log database size for space management considerations from the Log Settings section.

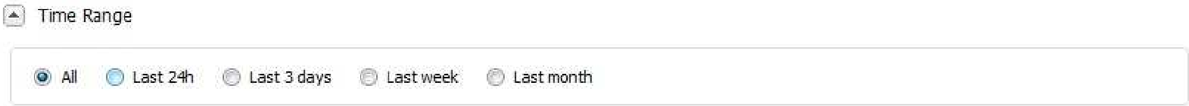


Raw Logging

Log Settings

Limit logs database size: By Size | 100 | Megabytes

The Time Range option allows you to verify the files that were accessed in a certain interval of time from the last 24 hours up to a month.



Time Range

● All ○ Last 24h ○ Last 3 days ○ Last week ○ Last month

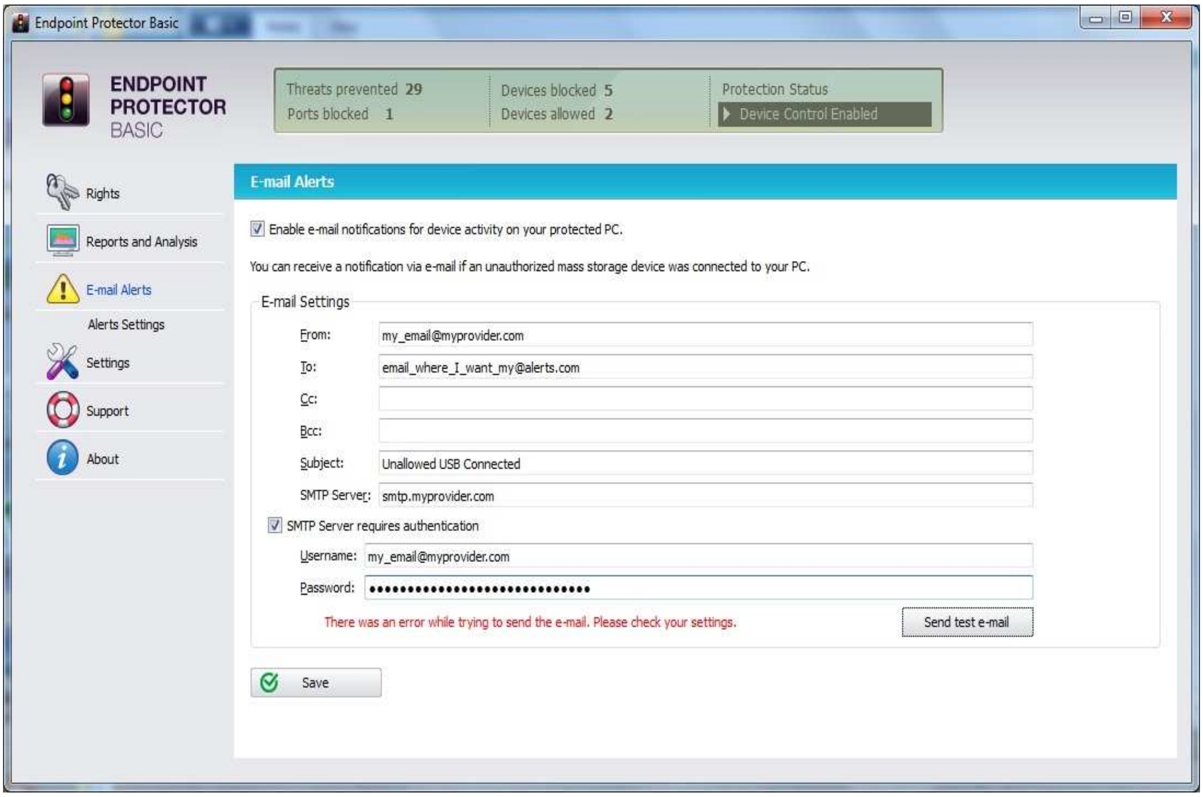
10. E-mail Alerts

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.



☑ Enable e-mail notifications for device activity on your protected PC.

You can receive a notification via e-mail if an unauthorized mass storage device was connected to your PC.

E-mail Settings

From: my_email@myprovider.com

To: email_where_I_want_my@alerts.com

Cc:

Bcc:

Subject: Unallowed USB Connected

SMTP Server: smtp.myprovider.com

☑ SMTP Server requires authentication

Username: my_email@myprovider.com

Password: ••••••••••••••••••••••••••••

There was an error while trying to send the e-mail. Please check your settings.

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.

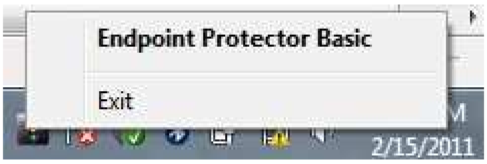
If a firewall is installed on the PC that you are protecting with Endpoint Protector Basic, the firewall will request you for authorization that Endpoint Protector Basic is accessing the internet. Please grant Endpoint Protector Basic this authorization so you will be able to send and receive e-mail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

11. Notification Messages

In order to see notifications, the EPP Basic Notifier needs to be running.

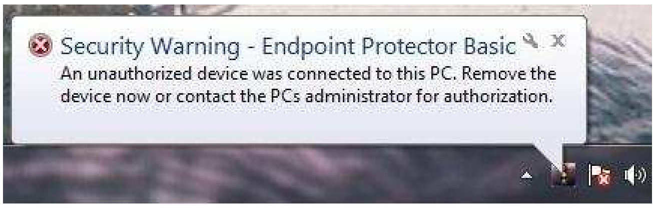
In case your Notifier is running, you will see its icon in the System Tray.

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.



Security Warning - Endpoint Protector Basic

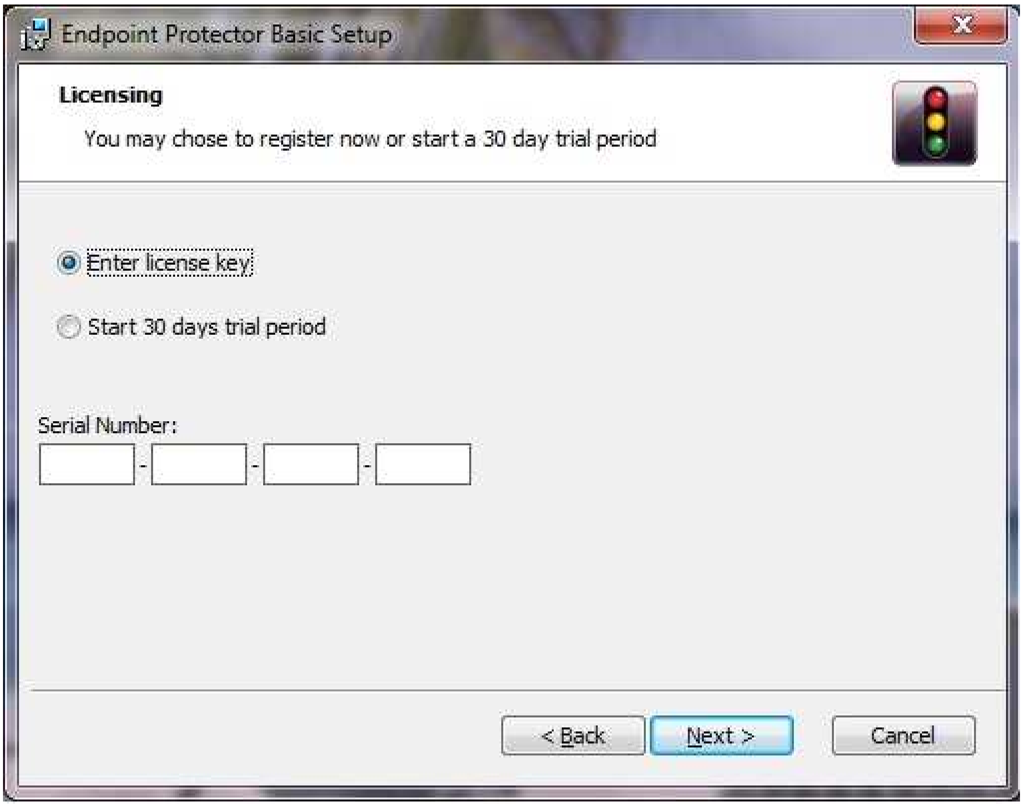
An unauthorized device was connected to this PC. Remove the device now or contact the PCs administrator for authorization.

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 as a 30 days trial version; therefore you will be able to choose between testing the full functionality of the application on your PC for a period of 30 days and registering directly the application by entering your license key.



Endpoint Protector Basic Setup

Licensing

You may chose to register now or start a 30 day trial period

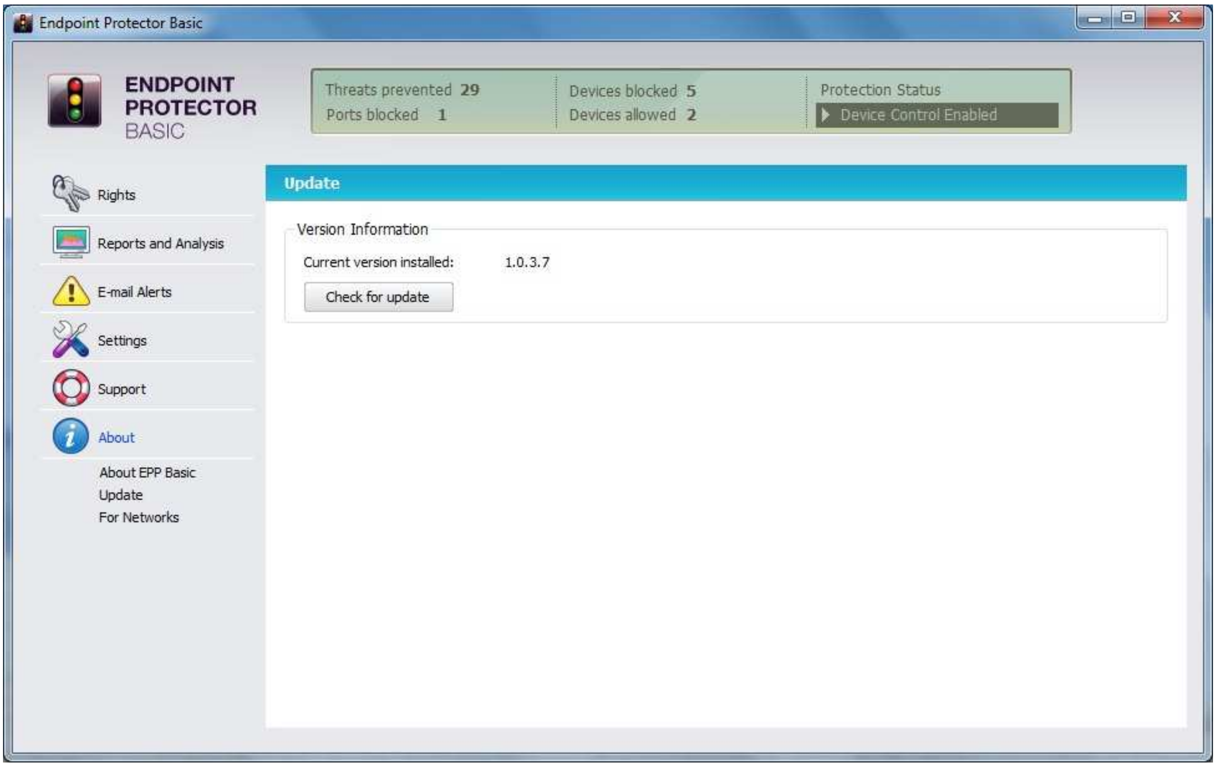
● Enter license key

○ Start 30 days trial period

Serial Number: □ - □ - □ - □

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.



Current version installed: 1.0.3.7

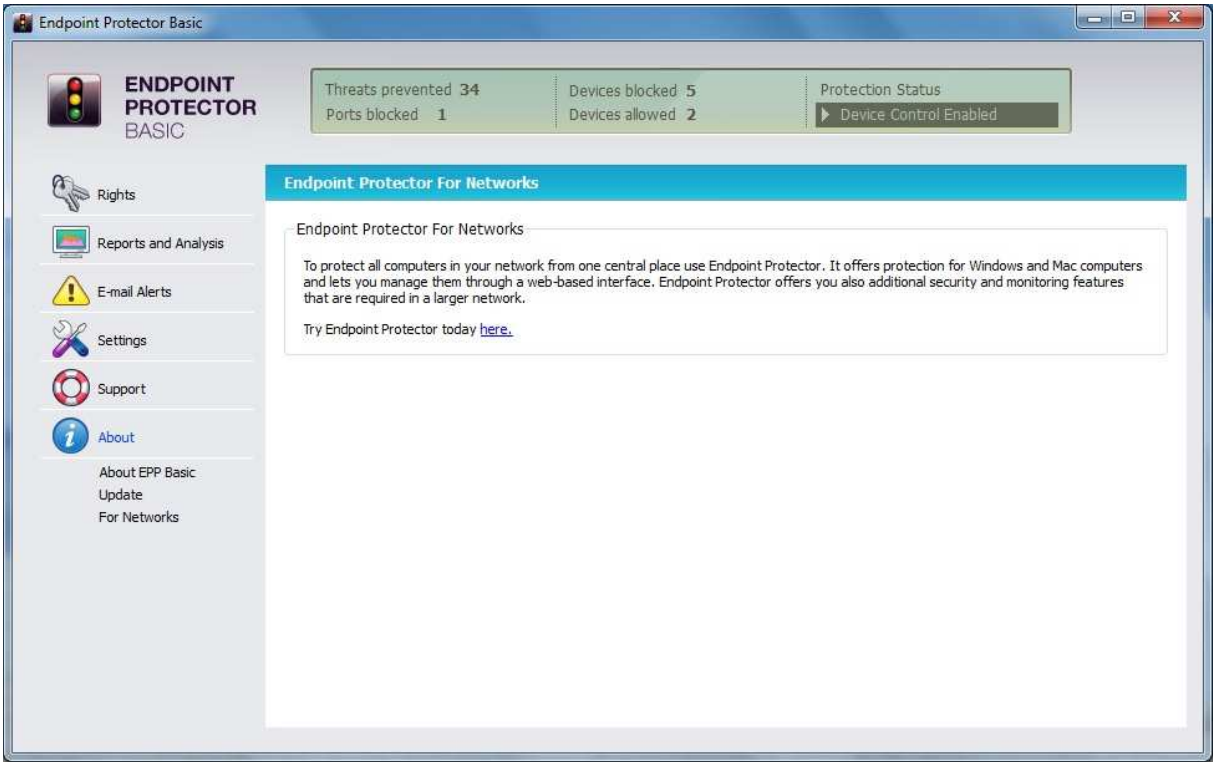
If there is a newer version available you will be asked if you want to download it.

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.

12.3. Upgrade for Networks

In case that you wish to protect and control all the computers from your network from one central place, you have the option to upgrade to Endpoint Protector, which offers a larger set of additional features required for ensuring security and proper monitoring of larger networks.



Endpoint Protector For Networks

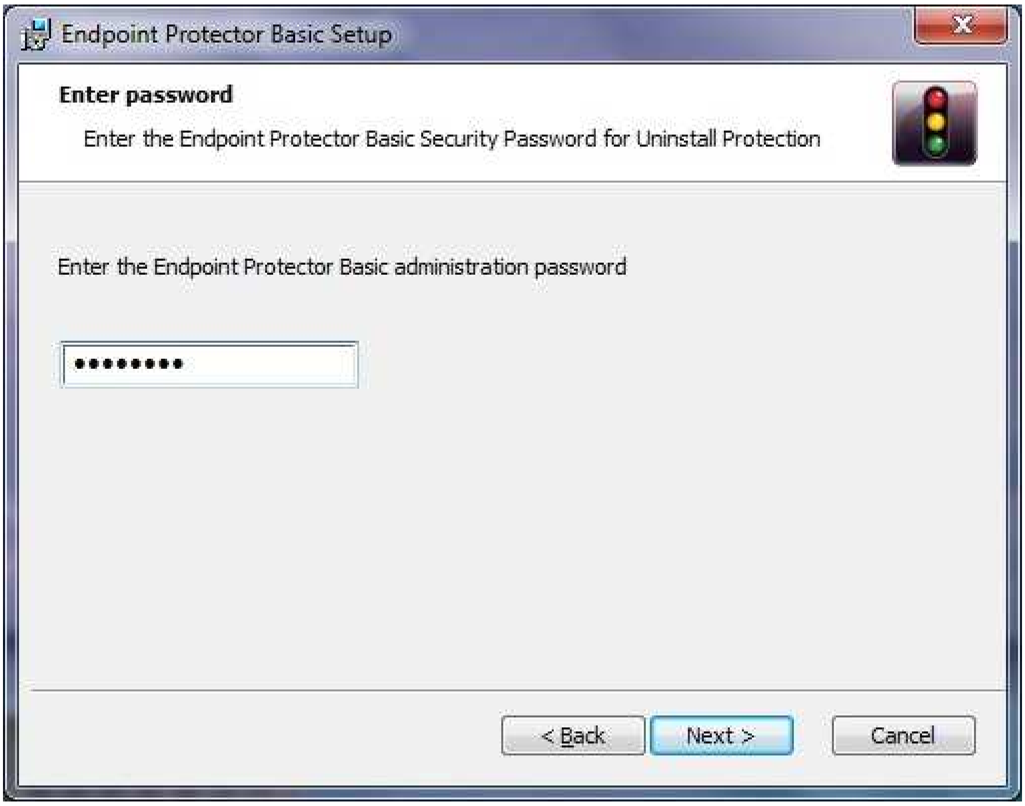
To protect all computers in your network from one central place use Endpoint Protector. It offers protection for Windows and Mac computers and lets you manage them through a web-based interface. Endpoint Protector offers you also additional security and monitoring features that are required in a larger network.

Try Endpoint Protector today here.

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.

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



Endpoint Protector Basic Setup

Enter password

Enter the Endpoint Protector Basic Security Password for Uninstall Protection

Enter the Endpoint Protector Basic administration password

•••••••••

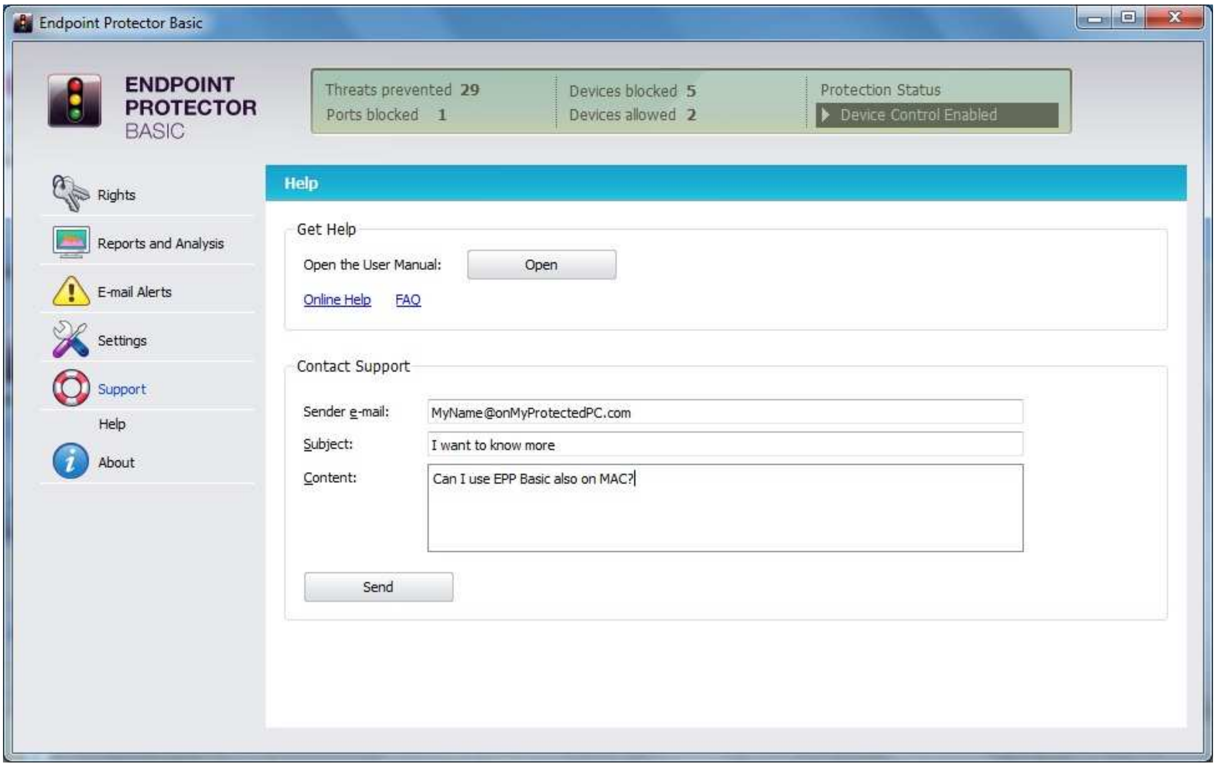
IMPORTANT!

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

14. Support

In this module you can complete an e-mail which will be sent directly to our support system at support@cososys.com. 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.



Sender e-mail: MyName@onMyProtectedPC.com
Subject: I want to know more
Content: Can I use EPP Basic also on MAC?

In case additional help, such as the FAQs or e-mail support is required, please visit our support website directly at http://www.cososys.com/help.html.