



# GFI EndPointSecurity

Comprehensive control on use of iPods, USB drives and other portable devices

GFI EndPointSecurity allows administrators to actively manage user access and log the activity of:

- Media players, including iPods, Creative Zen and others
- USB drives, CompactFlash, memory cards, CDs, floppies & other portable storage devices
- PDAs, BlackBerry handhelds, mobile phones, smart phones and similar communication devices
- Network cards, laptops and other network connections.

## ■ How it works

To control access, GFI EndPointSecurity installs a small footprint agent on the machine. This agent is only 1.2 MB in size – the user will never know it is there. GFI EndPointSecurity includes a remote deployment tool based on GFI LANguard technology, allowing you to deploy the agent to hundreds of machines with just a few clicks. After installation, the agent queries Active Directory when the user logs on and sets permissions to the different nodes accordingly. If the user is not a member of a group that allows him/her access, then access to the device is blocked.

## Benefits

### Why choose GFI EndPointSecurity?

- Prevents data leakage/theft by comprehensively controlling access to portable storage devices with minimal administrative effort
- Prevents introduction of malware and unauthorized software on the network
- Gives administrators greater control by being able to block devices by class, file extensions, physical port or device ID
- Allows administrators to grant temporary device or port access for a stipulated time-frame
- Support for 32 & 64-bit platforms: Including Windows Vista and latest RC of Windows Server 2008.

## ■ Control user access and protect your network against the threats posed by portable storage media

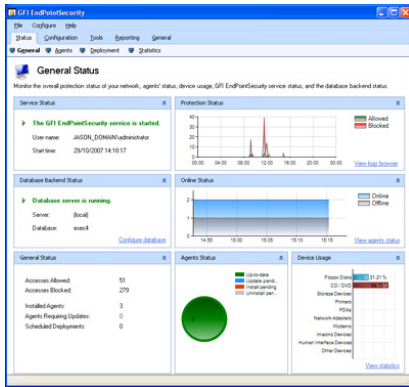
Using GFI EndPointSecurity you can centrally disable users from accessing portable storage media preventing users from stealing data or bringing in data that could be harmful to your network, such as viruses, trojans and other malware. Although you can switch off portable storage devices such as CD and/or floppy access from the BIOS, in reality this solution is impractical: You would have to physically visit the machine to temporarily switch off protection and install software. In addition, advanced users can hack the BIOS. GFI EndPointSecurity allows you to take control over a wide variety of devices including:

- Floppy disks
- CDs and DVD ROMs
- iPods
- Storage devices
- Printers
- PDAs
- Network adapters
- Modems
- Imaging devices
- And more!

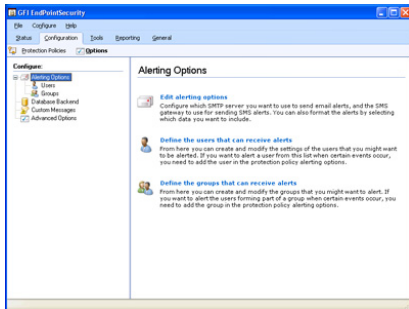
## ■ Log the activity of portable storage media like USB memory sticks, SD cards and more

USB sticks are one of the main threats as they are small, easily hidden and can store up to 4 GB of data. For example, plugging a digital camera into a USB port gives users access to storage on an SD card; SD cards are available in several sizes including 2 GB and over. In addition to blocking access to portable storage media, GFI EndPointSecurity logs device-related user activity to both the event log and a central SQL Server. A list of files that have been accessed (or read/written) on a device is recorded whenever a user plugs in a device to the network.

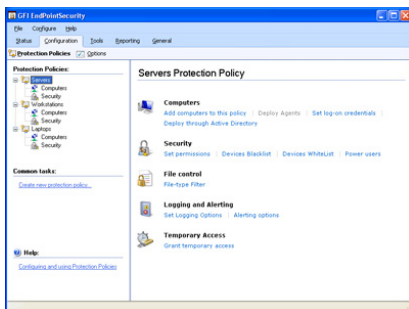
## GFI EndPointSecurity



GFI EndPointSecurity Management Console

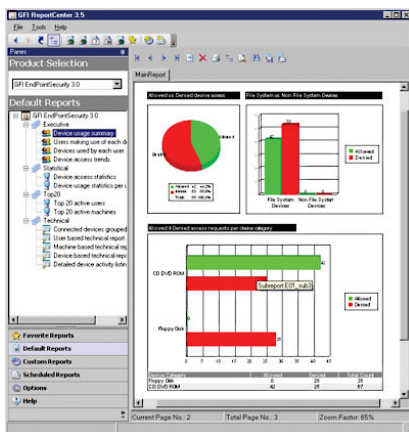


GFI EndPointSecurity configuration options



Default protection policies

## GFI EndPointSecurity ReportPack



Device usage report

## ■ Easily configure group-based protection control via Active Directory

You can configure and categorize computers into different protection groups: For each group you may specify different levels of protection and devices to allow or disallow access to. You can also leverage the power of groups and make an entire department a member of the group and easily change the settings for the entire group. Configuration of GFI EndPointSecurity is effortless and leverages the power of Active Directory and does not require the administrator to remember and keep track of which policies were deployed to which computers. Other storage control software requires cumbersome per-machine administration, forcing you to make the changes on a per-machine basis and update the configuration on each machine before the settings can take effect.

## ■ Advanced granular access control, whitelists and blacklists

GFI EndPointSecurity enables you to allow or deny access to a range of device classes, as well as blocking files transferred by file extension, by physical port and by device ID (the factory ID that tags each device). It is also possible to specify users or groups that should always have full access to devices. GFI EndPointSecurity also allows administrators to define a device whitelist and blacklist to allow only company-approved devices and block all others.

## ■ Real-time status monitoring and real-time alerts

GFI EndPointSecurity provides real-time status monitoring through its user interface that displays statistical data through graphical charts, the live status of the agent and more. GFI EndPointSecurity also allows you to send alerts when specific devices are connected to the network. Alerts can be sent to one or more recipients by email, network messages, and SMS notifications sent through an email-to-SMS gateway or service.

## ■ Get full reports on device usage with the GFI ReportPack add-on

The GFI EndPointSecurity ReportPack is a full-fledged reporting add-on to GFI EndPointSecurity. This reporting package can be scheduled to automatically generate graphical IT-level and management reports based on data collected by GFI EndPointSecurity, giving you the ability to report on devices connected to the network, user activity endpoint files copied to and from devices (including actual names of files copied!) and much more.

## ■ Easy unattended agent deployment

GFI EndPointSecurity provides the possibility to administrators to automatically schedule agent deployment after the administrator makes policy or configuration changes. If a deployment fails, it is rescheduled until deployed successfully. Furthermore, the GFI EndPointSecurity remote deployment tool can deploy the agent network-wide in a few minutes. GFI EndPointSecurity allows Active Directory deployment through MSI.

## ■ Temporary device access

Temporary access can be granted to users for a device (or group of devices) on a particular computer for a particular timeframe. This can be done even if the GFI EndPointSecurity agent is not connected to the network!

## ■ Other features:

- Scan and detect a list of devices that have been used or are currently still in use
- Password protected agents to avoid tampering
- Set up custom popup messages for users when they are blocked from using a device
- Browse user activity and device usage logs through a backend database
- Maintenance function that allows you to delete information that is older than a certain number of days
- Support for operating systems in any Unicode-compliant language

## ■ You're in good company...

Many leading companies have chosen GFI EndPointSecurity. Here are just a few: Best Western Sterling Inn, Fair Trades Ltd, Central Highlands Water, Aurum Funds and many more.

## System requirements

- Operating system: Windows 2000 (SP4), XP, 2003, Vista and 2008 (x86 and x64 versions)
- Internet Explorer 5.5 or later
- .NET Framework version 2.0
- Database Backend: SQL Server 2000, 2005, 2008
- Port: TCP port 1116 (default)

## Awards



Download your evaluation version from <http://www.gfi.com/endpointsecurity/>

GFI Software  
Magna House, 18 – 32 London Road  
Staines, Middlesex  
TW18 4BP  
UK  
Tel +44 (0) 870 770 5370  
Fax +44 (0) 870 770 5377  
sales@gfi.co.uk

GFI Software  
15300 Weston Parkway  
Suite 104  
Cary, NC 27513  
USA  
Tel +1 (888) 243-4329  
Fax +1 (919) 379-3402  
sales@gfiusa.com

GFI Asia Pacific Pty Ltd  
83 King William Road  
Unley 5061  
South Australia  
Tel +61 8 8273 3000  
Fax +61 8 8273 3099  
sales@gfiap.com

GFI Software  
GFI House  
San Andrea Street  
San Gwann SGN 1612  
Malta  
Tel +356 21 382418  
Fax +356 21 382419  
sales@gfi.com

**Microsoft**  
GOLD CERTIFIED  
Partner

The GFI logo, consisting of the letters "GFI" in a bold, sans-serif font. The "G" is black, the "F" is white with a black outline, and the "I" is black. Below the logo is the website address [www.gfi.com](http://www.gfi.com).