



GFI EndPointSecurity

Network-wide control of iPods, USB sticks & other endpoint devices

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

- Media players, including iPod, Creative Zen and others
- USB sticks, CompactFlash, memory cards, CDs, floppies & other storage devices
- PDAs, BlackBerry handhelds, mobile phone 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?

- Blocks insider data theft by fully controlling access to portable storage devices like memory cards, CDs and more
- Prevents the introduction of viruses and unauthorized software by controlling all endpoint connectable devices such as PDAs, laptops and more
- Allows administrators to exercise group-based control over a wide array of portable devices without affecting authorized users
- Prevents productivity loss by blocking unauthorized uploads of games and other personal files from portable storage devices
- Ships with three protection policies: for laptops, workstations and servers.

■ Control user access and 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. GFI EndPointSecurity recognizes USB storage sticks in addition to any device that can be mounted as a hard disk (whether accessed via USB, FireWire, etc.). 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.

■ Control access to CDs and floppies

You can centrally disable users from accessing CD/DVD drives as well as from reading or writing data to and from floppy disks. This way, you can block normal users from bringing in data that could be harmful to your network, such as viruses, trojans and other malware. Although you can switch off 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.

■ Protect your network against the threats posed by non-removable media devices

GFI EndPointSecurity protects your network against non-removable media devices by allowing you to lock down a machine to a specific hardware level, guaranteeing protection against Bluetooth devices, network cards and more.

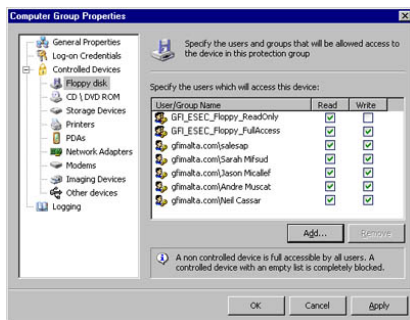
■ Easily configure group-based protection control via Active Directory

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.

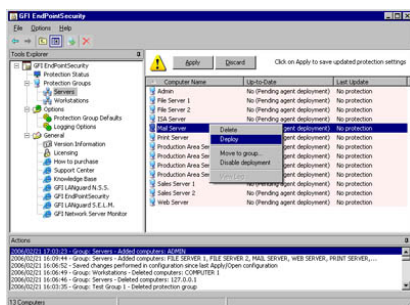
GFI EndPointSecurity



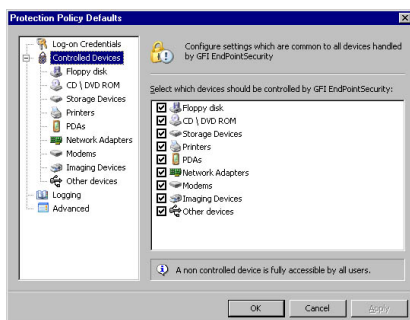
GFI EndPointSecurity configuration



Allow/deny access to Active Directory groups

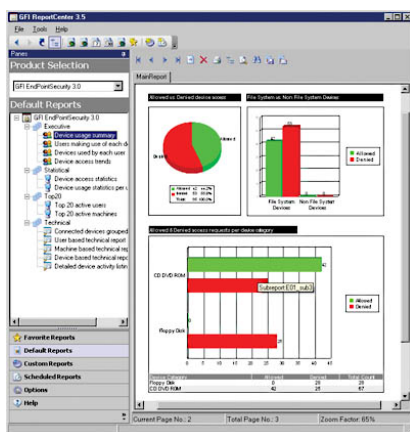


Easy network-wide deployment of agents



Configure which devices you wish to control

GFI EndPointSecurity ReportPack



Device usage report

■ Granular access control

GFI EndPointSecurity enables you to allow or deny access to a device as well as to assign read only or full access privileges (where applicable) over every supported device (such as PDAs) on a user by user basis.

■ Log device-related user activity

With GFI EndPointSecurity you can log device-related user activity to both the event log and a central SQL Server. A list of files accessed to/from the device is recorded whenever users plug in devices both successfully and unsuccessfully.

■ 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, device usage trends, files copied to and from devices (including actual names of files copied!) and much more.

■ Includes remote deployment tool

The GFI EndPointSecurity remote deployment tool can deploy the agent network-wide in a few minutes. You can configure to deploy domain-wide, per computer or to a list of computers.

■ Centralized control facilitates temporary access

Because you can easily add/remove a user to a group in Active Directory, it is simple to grant temporary access to a removable media, floppy or CD. Temporary access may be occasionally required, but should not mean that you cannot control access the rest of the time.

■ Other features:

- 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, Aarum Funds and many more.

System requirements

- Windows 2000/2003 or Windows XP Pro.

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

GFI Software
Unit 2, St. John's Mews
St. John's Rd. Hampton Wick
Kingston-upon-Thames
Surrey KT1 4AN, 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 Software GmbH
Bargkoppelweg 72
22145 Hamburg
Germany
Tel +49(0) 40 3068 1000
Fax +49(0) 700 3068 1010
sales@gfisoftware.de

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 05 Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

Microsoft
GOLD CERTIFIED
Partner

