



GFI LANguard

Portable Storage Control

Network-wide control of portable storage devices such as USB sticks, etc

You have invested in network anti-virus software, firewalls, email and web content security. Yet any user can come into the office, plug in a USB stick the size of the average keychain and take in/out 1GB of data. This poses a tremendous threat: Users can take confidential data or they can introduce viruses, Trojans, illegal software and more – actions that can affect your network and company severely. Yet, as an administrator you have no way to control this! Group policy offers no control.

■ The need to control entry and exit of data via USB sticks and other devices

In the 2003 CSI/FBI Computer Crime and Security Survey, 80% of all respondents cited insider abuse of network access as a most pressing security concern for companies. The survey also showed that theft of proprietary information caused the greatest financial loss to companies (totaling over \$70m in one year) and disgruntled employees are the most likely source of attack for companies.

Technology analyst Gartner warns that portable devices containing a USB or FireWire connection are a serious new threat to businesses. In a July 2004 report, Gartner named removable media devices as a significant security risk in the workplace and advised that these can be used both to download confidential data, and also to introduce a virus into the company network. Gartner's report listed pocket-sized hard drives that connect using FireWire or USB hard drive or keychain drive, disk-based MP3 players such as the iPod, and digital cameras with smart media cards, memory sticks, compact flash and other memory media as potential security threats.

■ Regain control with GFI LANguard Portable Storage Control (P.S.C.)

GFI LANguard Portable Storage Control (P.S.C.) offers you network-wide control of which users can:

Benefits

Insider abuse of network access is an urgent security concern for 80% of companies (2003 CSI/FBI Computer Crime and Security Survey)

Controls access to all types USB sticks, SD cards & more

Controls access to CDs and floppies

Easy user management via Active Directory

Affordable pricing.

- Plug in a USB stick
- Connect a smartphone, MP3 player, handheld
- Download/upload data to a digital camera
- Access CDs
- Access floppies.

GFI LANguard P.S.C. allows you to define which users can use removable media centrally from Active Directory – simply by making them a member of three pre-defined groups.

■ How it works

To control access, GFI LANguard P.S.C. installs a small footprint agent on the machine. This agent is only 1.2MB in size – the user will never know it is there. GFI LANguard P.S.C. includes a remote deployment tool, 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 removable storage accordingly. If the user is not a member of a group that allows him/her access, then access to the device/CD/floppy is blocked.

■ Controls access to all types USB sticks, SD cards (digital cameras) and more

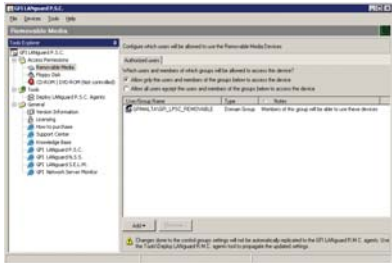
USB sticks are one of the main threats as they are small, easily hidden and can store up to 1GB of data. GFI LANguard P.S.C. recognizes all USB sticks. In addition, it can control access to any device that can be mounted as a hard disk (whether accessed via USB, FireWire, etc.). For example, plugging a digital camera into a USB port gives users access to storage on an SD card; SD cards are available in several sizes including 512MB and over.

■ Controls access to CDs and floppies

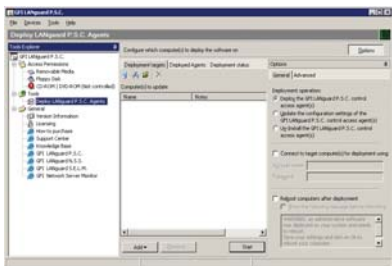
You can centrally disable users from reading or writing data to/from a CD or floppy. This way, you can block normal users from bringing in data that could be harmful to your network, such as viruses, Trojans and other malware. Although you can switch off CD and/or floppy access from the BIOS, in reality 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.



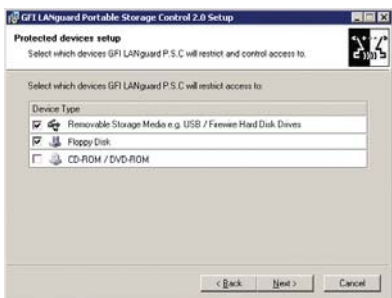
GFI LANguard P.S.C. configuration



Configure which Active Directory groups are allowed or denied access



Easy network-wide deployment of agents



Configure which devices you wish to control

System requirements

- Server/clients which are to be monitored must be running Windows 2000/2003 or XP.
- It is recommended that users do not have administrative rights on their local machine, to avoid tampering with the process (by killing it from Task Manager).

■ Easily configure users who can have access via Active Directory

To grant a user access to any one or all three types of devices, simply make that user a member of pre-defined Active Directory groups for each of the three kinds of devices. You can also leverage the power of groups and make an entire department a member of the group. 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. Configuration of GFI LANguard P.S.C. is effortless and leverages the power of Active Directory.

■ Includes remote deployment tool

The GFI LANguard P.S.C. remote deployment tool can deploy the agent network-wide in minutes. You can also 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.

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

GFI Software Ltd UK
Unit 2, St. John's Mews
St. John's Road, 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 USA, Inc.
15300 Weston Parkway
Suite 104
Cary, NC 27513
USA
Tel +1 (888) 2 GFI FAX
Fax +1 (919) 388 5621
sales@gfiusa.com

GFI Software GmbH
Bargkoppelweg 72
22145 Hamburg
Germany
Tel +49 (0)700306810 00
Fax +49 (0)700306810 10
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 Ltd
GFI House
San Andrea Street
San Gwann SGN 05 Malta
Tel +356 2138 2418
Fax +356 2138 2419
sales@gfi.com

Microsoft
GOLD CERTIFIED
Partner



www.gfi.com