



*Evaluation guide*

# **GFI EndPointSecurity**<sup>™</sup>

*Control of USB sticks, iPods and other endpoint devices*

This document will guide you through the evaluation of GFI EndPointSecurity<sup>™</sup> to ensure you get the maximum benefit from your 30-day trial. It will also help you understand how the product can resolve real life needs and pain points.

## Contents

<b>Introduction</b> .....	<b>3</b>
<b>Obtaining and installing the product</b> .....	<b>3</b>
Obtaining the product.....	3
Installing the product.....	3
<b>First get an idea of what is going on in your network</b> .....	<b>3</b>
Why implement GFI EndPointSecurity.....	4
<b>Prevent data theft with GFI EndPointSecurity – monitor your endpoints</b> .....	<b>4</b>
The risks posed by common removable devices.....	5
<b>Report on device usage with GFI EndPointSecurity</b> .....	<b>6</b>
Knowing what is being connected to your network is the first step in taking control.....	6
Data theft – one of the largest security threats organizations face.....	7
<b>Block removable devices with GFI EndPointSecurity</b> .....	<b>7</b>
Data theft gets much harder if you deny access to the removable devices used to carry your data away.....	7
Common issues.....	8
<b>Concluding your trial</b> .....	<b>8</b>

## Introduction

This document will guide you through the evaluation of GFI EndPointSecurity to ensure you get the maximum benefit from your 30-day trial. It will also help you understand how the product can resolve real life needs and pain points.

If you are having any problems with GFI EndPointSecurity, remember that you can [click here for support](#).

## Obtaining and installing the product

### Obtaining the product

You can obtain the product by visiting the GFI EndPointSecurity web page [here](#).

You will receive an email with the download link and an evaluation key after you register on the website. Please follow the instructions in the email.

### Installing the product

The installation process is straightforward and consists of a click-to-proceed installation wizard. The wizard will gather all the required information in order to run the product. The items you will be required to input are:

- a. An evaluation key – available in the email you receive from GFI after the registration process
- b. Domain/local admin credentials to enable the product to function, deploy agents network wide, etc.
- c. The install path for the product

For more information, please use the GFI EndPointSecurity Installation Guide available [here](#).

## First get an idea of what is going on in your network

If you do nothing else with this trial, run a scan and take a look at how many unauthorized devices have been and are still being connected to your network.

1. Start by downloading the [Getting Started Guide](#); this covers system requirements, installation and setup
2. Once you have installed the product, the Quick Start Wizard will take you through all important steps of the setup
  - » Automatic discovery and deployment of agents
  - » Configuring power users
  - » Configuring user groups
  - » Configuring database backend
3. Launch the GFI EndPointSecurity Management Console
  - » Go to the 'Tools' tab
  - » Enter the name of the computer you want to scan
  - » You will see a list of all devices that have ever been connected to that computer including device details and their current status

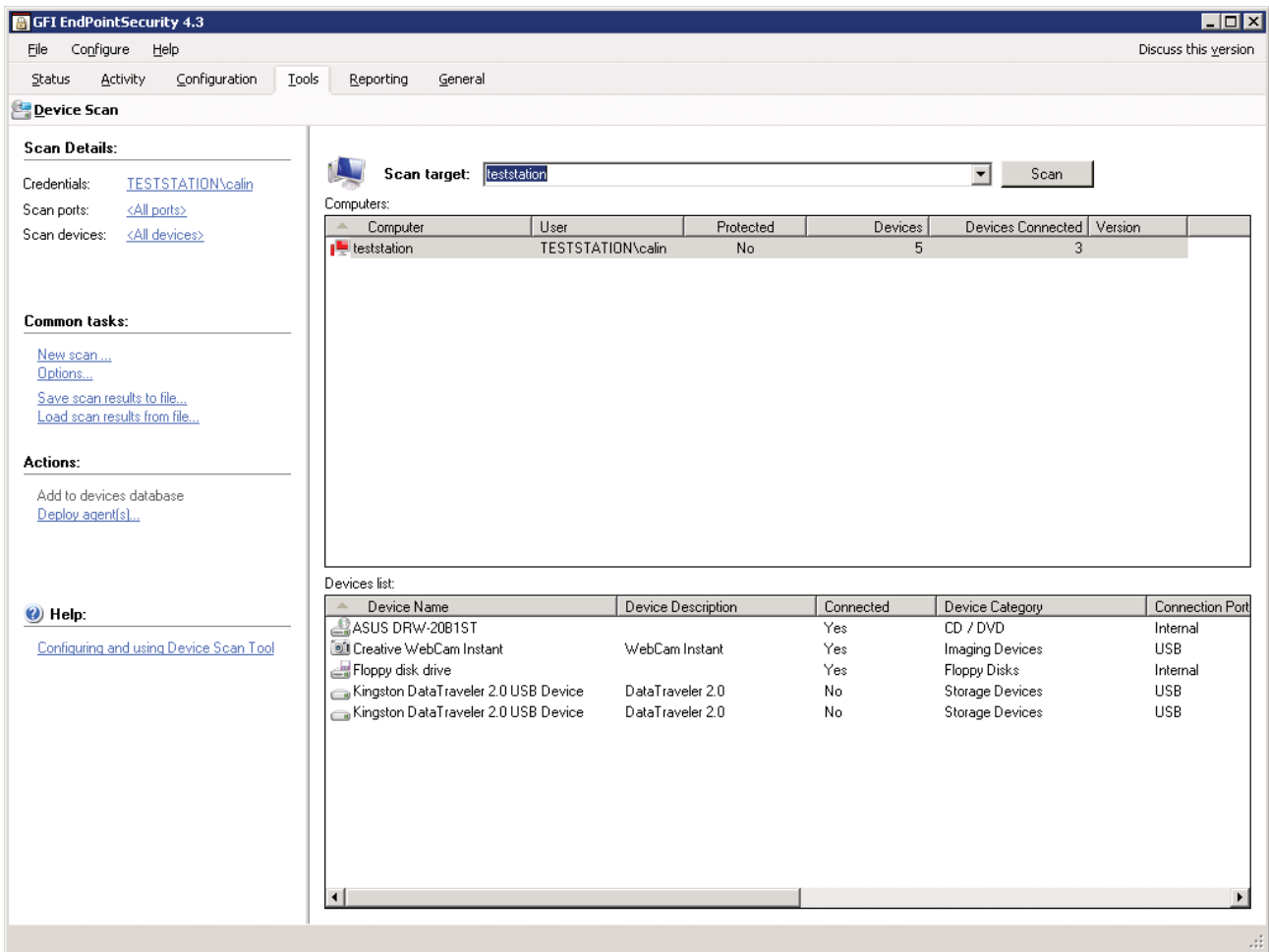


Figure 1: Device enumeration tool

**How many of these devices do you recognize? How many of these devices are safe to be used in your environment?**

### Why implement GFI EndPointSecurity

According to the Information Security Breaches Survey 2010

- » 46% of larger organizations suffered from loss or leakage of confidential information
- » The top reason for security expenditure was to protect customer information
- » 80% of large and 42% of small organizations reported staff related incidents

### **GFI EndPointSecurity won the 'Software Product of the Year' award in the 2010 Network Computing Awards – Network Computing, March 2010**

Controlling data leakage is a big step towards PCI DSS compliance.

Proving your ability to prevent data theft will go a long way towards meeting compliance requirements. We have produced a free white paper that can help you understand the requirements of PCI DSS: [Download white paper.](#)

### **Prevent data theft with GFI EndPointSecurity – monitor your endpoints**

We would like to help you look at more of the computers connected to your network and start to build a larger picture of which removable devices are regularly being connected to company computers. We will then introduce you to some of the very real risks these devices can pose to your network and business operations.

- » Launch the GFI EndPointSecurity Management Console: The 'Status' tab should be open
- » Select 'All Computers' in the drop down menu
- » Here you get an at-a-glance view of protection status, device usage by type and by connectivity port
- » You may not have started blocking any devices or ports yet so all data may be in the allowed column

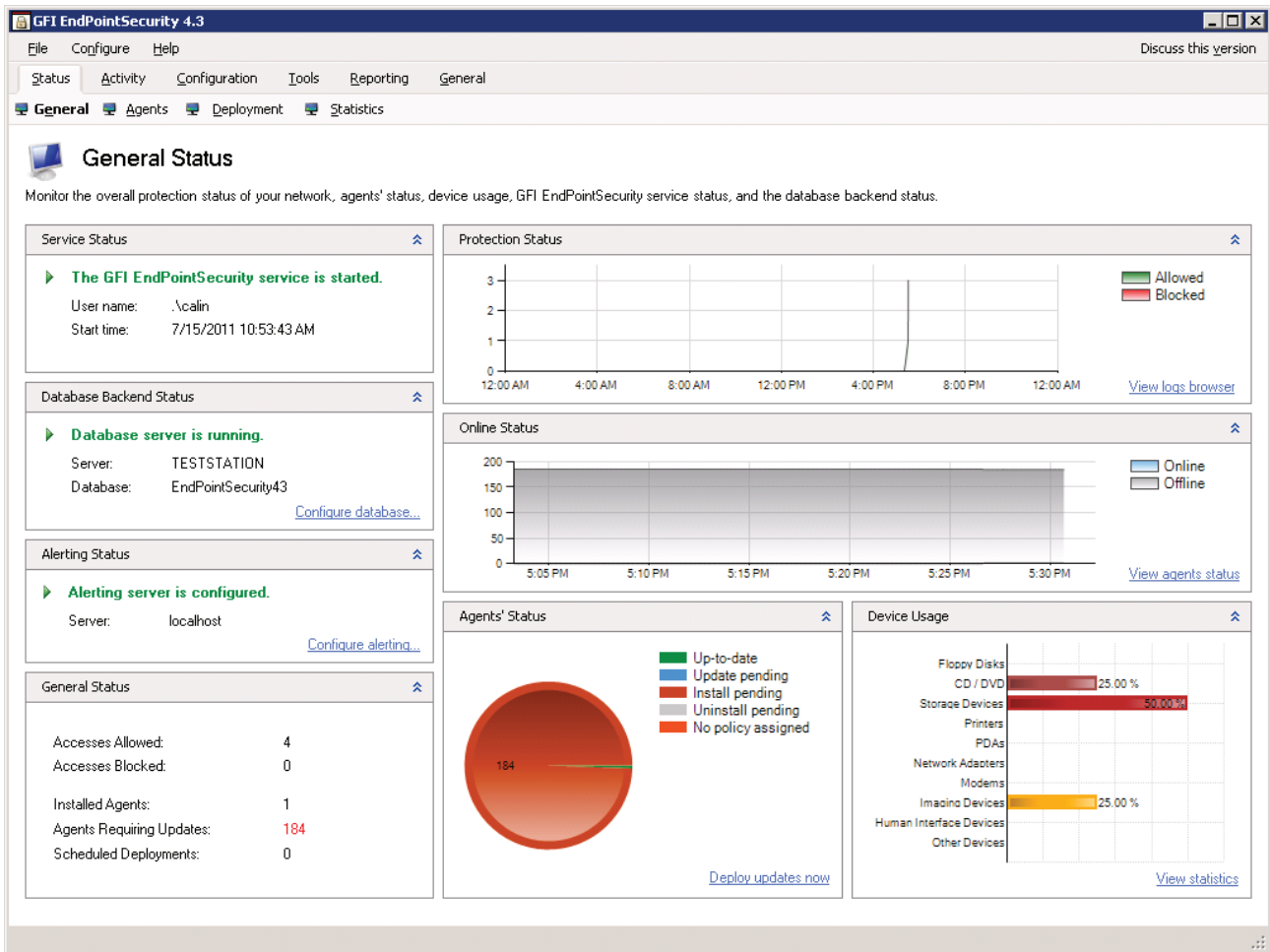


Figure 2: Monitoring Device Activity

### The risks posed by common removable devices

- » Personal USB flash drives – Used at home, maybe taken to school by the children, they can rapidly become exposed to a range of malware threats on computers with unknown protection status. They are then often plugged directly into the company PC or laptop, bypassing all network layers of defense. Available with 32GB and more of storage, these devices can easily be used to copy complete customer databases, financial reports and other company sensitive data.
- » iPods & MP3 players – These are still seen by the computer as memory devices and can be used in the same way as the USB flash drive. In addition it is common for people to copy their music onto the company PC to listen to during working hours and save the iPod batteries for later. If people around the office start asking for copies of those music tracks, soon a significant portion of the files entering the company backup system are pirated music files. They are now on company systems and the company has liability for the copyright infringement.
- » Personal smartphones – Again these are seen by the computer as memory storage, so everything mentioned so far applies equally. People usually connect their phones to the USB port just to recharge the battery, but unless controls are in place they can also be used to add to the huge statistics on insider data theft.

“We tried to block the use of USB mass storage devices using the operating system (Windows Server 2003) and while the blocking was partially successful, it wasn’t practical to use or manage; we couldn’t give temporary access to certain devices, and had no way to generate usage reports.” Mr Gustavo Rendon, Network & Security Administrator – Multiplicas Casa de Bolas

## Report on device usage with GFI EndPointSecurity

A key benefit of GFI EndPointSecurity is its management reporting that quickly identifies which rogue devices are being used and who are the main culprits. Remediation can be as simple as popping up a message to inform the user that they are in breach of company policies.

If you have not yet downloaded GFI EndPointSecurity and GFI ReportPack, please [download it now](#).

### Knowing what is being connected to your network is the first step in taking control

GFI EndPointSecurity identifies both what is being connected and to which computers.

1. Launch the GFI ReportPack and have a look at the standard reports you can use. You can create your own but there are several that will meet your immediate need for information.
  - » Device usage summary : Users making use of each device : Devices used by each user : Device access trends
2. Choose a report that shows you the number and variety of removable object that have been connected to computers on your network. You should see USB flash drives, mobile phones, music players, SD cards and maybe others.

GFI EndPointSecurity		All devices used - grouped by device	
<b>Description:</b>	This report lists all devices detected by EndPointSecurity agents across the network together with the users who made use of each device.		
<b>Generated on:</b>	14-May-2010 10:31		
<b>Generated by:</b>	GFI User		
<b>Date range:</b>	1-January-2010 10:31 to 14-May-2010 10:31		
<b>Filters:</b>	None		
<b>CD / DVD</b>		<b>Total users:</b>	<b>10</b>
<b>0</b>	<b>Users:</b>	<b>5</b>	
Unknown			
\\GFI DOMAIN\Jane			
\\GFI DOMAIN\Bob			
\\GFI DOMAIN\John			
\\NT AUTHORITY\SYSTEM			
<b>1</b>	<b>Users:</b>	<b>5</b>	
\\GFI DOMAIN\Jane			
\\GFI DOMAIN\Bob			
\\GFI DOMAIN\John			
\\GFI DOMAIN\ReadOnly			
\\NT AUTHORITY\SYSTEM			
<b>Floppy Disk</b>		<b>Total users:</b>	<b>11</b>
<b>Unknown Device</b>		<b>Users:</b>	<b>5</b>
\\GFI DOMAIN\Jane			
\\GFI DOMAIN\Bob			
\\GFI DOMAIN\John			
\\GFI DOMAIN\ReadOnly			
\\NT AUTHORITY\SYSTEM			
<b>NEC USB UF00x</b>		<b>Users:</b>	<b>2</b>
\\GFI DOMAIN\Bob			
\\NT AUTHORITY\SYSTEM			

Figure 3: GFI EndPointSecurity device usage report

3. Send this report to all interested stakeholders along with your suggestions on how the problem should be controlled.

## Data theft – one of the largest security threats organizations face

Data theft by internal staff is one of the most common security breaches suffered by companies of all sizes.

The reasons vary greatly:

- » Commercial staff taking copies of the customer database when they move on, often to a company within the same industry or to a direct competitor
- » Technical staff taking product development plans as they move to competitors
- » Development staff taking 'their' code when they leave the company
- » Management staff taking copies of customer and supplier data when they leave to set up in competition

Data is stolen for many other reasons, however, in the end the result is the same. Confidential company information ends up being used against the interests of the company and, in the case of customer data that includes personal information, the company is then in breach of its obligations under the Data Protection Act.

Data leakage prevention is also a key factor in proving compliance with PCI DSS, HIPAA and many other legislations.

*"We have been able to demonstrate that we can prevent unauthorized use of non-approved USB devices firm-wide. GFI EndPointSecurity also provides some audit information on the data that is being transferred to approved company issue USB storage devices." Mr. Keith Ross, IT Technical Director – Johnston Carmichael*

## Block removable devices with GFI EndPointSecurity

After 20 days of monitoring you should now have enough data to prove that you were correct in thinking there is a problem to solve and to see where the main threats are. In the last 10 days of your trial, it is time to start blocking access to devices.

### Data theft gets much harder if you deny access to the removable devices used to carry your data away

Launch the GFI EndPointSecurity Management Console: Open the Configuration tab:

- » Here you can see the standard policies available within GFI EndPointProtection and any new ones you create yourself.
- » Note the separate policies for servers, workstations and laptops. This caters for the different ways these computers would be expected to be used. Laptops especially are often considered person property by many of the people they are issued to and are used accordingly.
- » Consider preventing the movement of certain file types to and from removable media. If people want to charge their iPods from their workstation or laptop, they can do so without copying files backwards and forwards and compromising your data security and copyright policies.

**The result: You will start to see devices being blocked.**

## General Status

The General Status displays the primary monitoring requirements associated with GFI EndPointSecurity, displays the service and database status and other useful information.

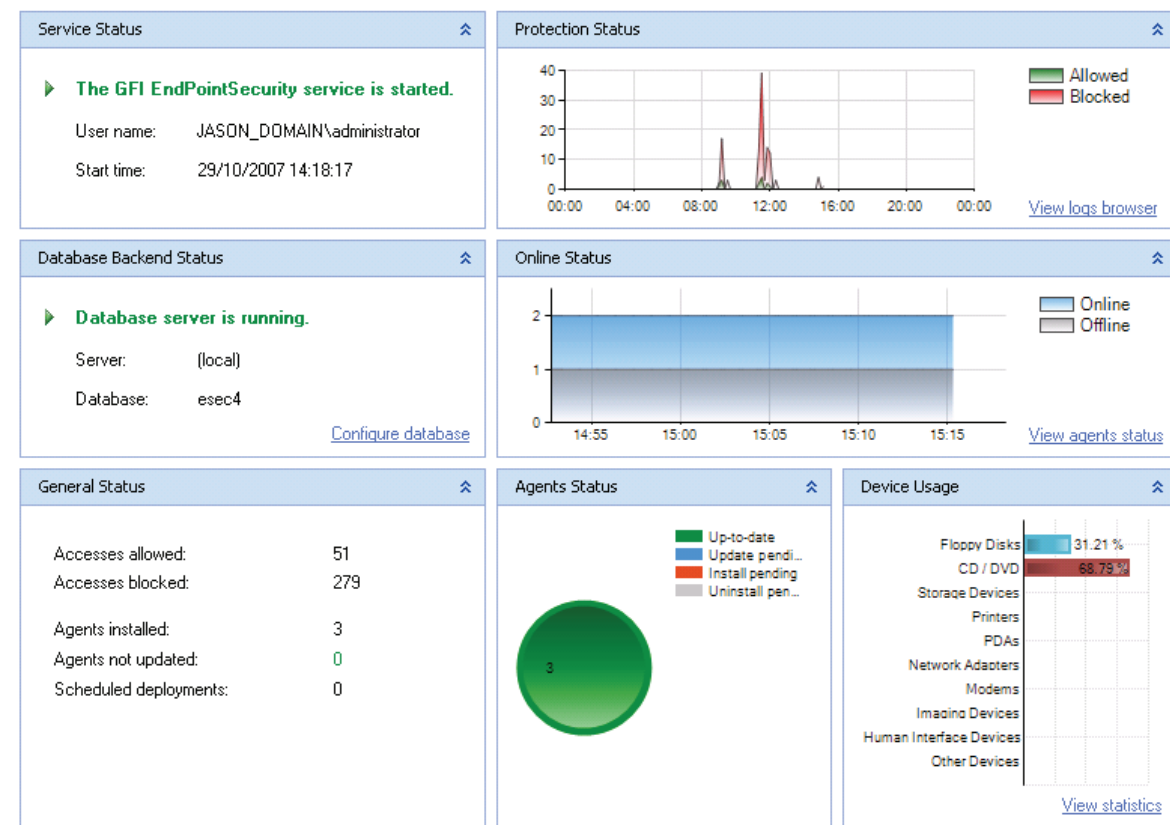


Figure 4: Devices get blocked

**Tip:** You can look at the log of files that have been copied to portable devices. You can also log file movements for authorized devices.

### Common issues

- » The chances are that you will block music and video files. The chances are there will be webcasts, podcasts and other legitimate audio and video files that you will have to make exceptions for. You can create a new policy and add those people who need access to these files types or you could grant temporary access rather than create a permanent hole in your security
- » Staff need to charge their personal portable devices at work. They still can as the computer may block access to the device while the USB port is still powered, able to charge any device connected to it; or you could provide mains USB adapter plugs as an alternative.

*"Prior to the installation of GFI EndPointSecurity, users were downloading and uploading all sorts of files to and from their PCs and servers. Now, with surgical precision, I can control and monitor what is happening on the network – who is doing what, when, how and where. Thanks GFI!" Mr. Tony Malvarez – Aerotecnica S.A.*

### Concluding your trial

Your trial of GFI EndPointSecurity lasts just 30 days and we hope you see the benefits of controlling removable devices on your network and wherever your company laptops travel.

Data theft and breaches of copyright place legal responsibility on the company. GFI EndPointSecurity is an essential part of providing and proving compliance.

It is the company's responsibility to protect personal information and to prevent breaches of copyright.

***If you have been impressed by the benefits of GFI EndPointSecurity – Buy now***

Reasons to implement GFI EndPointSecurity:

- » Improve productivity by preventing users from introducing unauthorized applications at work for personal use
- » Enforce security by preventing users from bypassing your perimeter security via USB modems and wireless
- » Prevent breaches of the Data Protection Act through the theft of company data via removable media
- » Protect the company from copyright legislation infringement by preventing music and video files from being copied onto company computers and entering the company backup system
- » Reduce the risk of malware infection by blocking access to removable devices

**Pod slurping – an easy technique for stealing data. [Click here to download PDF.](#)**

Uncontrolled use of iPods, USB sticks and flash drives on your network poses a problem.

*Multiplicas Casa de Bolsa C.A. is a financial services company in Venezuela and is therefore privy to sensitive information that they need to protect. They installed GFI EndPointSecurity which allowed them to exercise comprehensive control over what portable storage devices are connected to the network and what information is copied off the network and by whom, thereby preventing data leakage. [Click here to read the case study.](#)*

During the trial you used the full version of GFI EndPointSecurity; all you have to do to move to the retail product is purchase a key for as little as \$9 per seat and install it. **Buy now.**

## **USA, CANADA AND CENTRAL AND SOUTH AMERICA**

15300 Weston Parkway, Suite 104 Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

[ussales@gfi.com](mailto:ussales@gfi.com)

## **UK AND REPUBLIC OF IRELAND**

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

[sales@gfi.com](mailto:sales@gfi.com)

## **EUROPE, MIDDLE EAST AND AFRICA**

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

[sales@gfi.com](mailto:sales@gfi.com)

## **AUSTRALIA AND NEW ZEALAND**

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

[sales@gfiap.com](mailto:sales@gfiap.com)



### Disclaimer

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.