
EndPointScan

Manual

By GFI Software Ltd.



<http://www.gfi.com>
E-mail: info@gfi.com

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of GFI SOFTWARE Ltd.

Version 1.0 – Last updated April 18, 2007

Contents

Introduction	4
About portable media device threats	4
About EndPointScan	5
Supported device classes	5
Supported device connection ports.....	6
Key features	6
Installation	8
Introduction	8
System requirements	8
Installation procedure.....	8
Scanning computers	10
Introduction	10
Scanning procedures	10
Example 1: Scan the local computer	11
Example 2: Scan a computer on the LAN.....	12
Example 3: Scan a range of computers on the LAN.....	14
Example 4: Scan a list of computers on the LAN	15
Scan results	17
Risk level indicator	18
Device threat level	18
Computer protection level	19
Troubleshooting	20
Introduction	20
Knowledge Base	20
Web Forum	20
Request technical support via email	20
Index	21

Introduction

About portable media device threats

The key advantage of removable media devices (or portable devices) is easy access. In theory, this may be of great advantage for organizations. However, it is a well-reported fact that access and security are at opposite ends of the security continuum.

Developments in removable media technology are escalating. The newer versions of portable devices, such as flash memory, have been increasing in capacity and performance making them:

- Easy and fast to install
- Capable of storing huge amounts of data
- Physically small enough to carry in a pocket.

As a result, internal users may deliberately or accidentally:

- Remove sensitive data or expose confidential information
- Introduce malicious code (e.g. viruses, trojans) which can bring the entire corporate network down
- Transfer inappropriate or offensive material on to corporate hardware
- Make personal copies of company information and intellectual property
- Connect portable devices to corporate hardware and as a consequence get distracted during work hours.

In an attempt to control these threats some organizations prohibit the use of (personally-owned) portable devices at work. However, best practice dictates that you must never rely on voluntary compliance!

Tools are now available, such as EndPointScan, to help organizations identify device usage on the corporate networks.

Advanced tools, such as GFI EndPointSecurity, take this a step further by enabling organizations to establish complete control over which devices should be authorized for use over the corporate network. For more information on GFI EndPointSecurity, visit the GFI website at <http://www.gfi.com/endpointsecurity>.

About EndPointScan

EndPointScan is a free web-based utility which allows security administrators to identify and enumerate portable devices on their network computers, such as mass storage MP3 players.

EndPointScan transparently and rapidly queries organizational network endpoints, locating and reporting all devices that are or have been locally connected. The application granularly identifies endpoint devices connected on every machine, both currently and historically. Detailed scan results are viewed through a web-based interface.

To use EndPointScan administrators must access <http://www.endpointscan.com>. When the utility is being used for the first time, an ActiveX control must be downloaded and installed.

Supported device classes

EndPointScan portable device classes are organized into the following categories:

 **Floppy disk**

 **CD/DVD ROM**

- CD R/W ROM
- DVD R/W ROM

 **Storage Devices**

- USB Pen drives
- Digital Media Players (e.g. iPod, Creative Zen)
- Flash and Memory Card Readers
- Multi-drive USB devices – devices that don't mount as a single drive (spoofing)
- Other portable storage devices

 **Printers**

 **PDAs**

- Pocket PCs
- RIM Blackberry Devices
- Smart phones

 **Network Adapters**

- Bluetooth dongles/connections
- Infrared dongles/connections

 **Modems**

- Smart phones
- Mobile phones

 **Imaging Devices**

- Digital Cameras
- Webcams
- Scanners

 **Human Interface Devices**

- Keyboards
- Mice
- Game controllers



Other Devices

- Bluetooth dongles/ports
- Infrared dongles/ports
- MO (magneto optical) drives (internal and external)
- Zip drives
- Tape drives

Supported device connection ports

EndPointScan scans for devices which are or have been connected on the following ports:

- USB
- Firewire
- PCMCIA
- Bluetooth
- Secure Digital
- Serial & Parallel
- Infrared
- Internal (e.g. optical drives, floppy drives)

Key features

Ease of use

EndPointScan does not require complex installation or configuration procedures – almost click and go!

Comprehensive

EndPointScan provides administrators with complete and thorough information on all previously or currently connected devices. It scans for devices connected to a wide variety of ports that include USB, Firewire, PCMCIA and Bluetooth.

Intuitive results

Easy-to-understand results illuminate enterprise endpoint blind spots and provide organizations with the visibility they need to identify and effectively manage endpoint vulnerabilities.

Low resource consumption

EndPointScan is a client-less lightweight utility, with a very small memory footprint.

Low bandwidth consumption

Endpoint audits have a negligible effect on network performance.

Multi-threaded

EndPointScan scans multiple computers simultaneously.

Seamless compatibility

EndPointScan is fully compatible with existing network management or administrative tools such as Active Directory.

Installation

Introduction

This chapter will go through the procedures to install the ActiveX control and execute EndPointScan.

System requirements

EndPointScan can be installed on a computer that meets the requirements shown below.

- Windows 2000, XP, 2003 operating system
- Microsoft Internet Explorer 6 or later with Internet security settings set to Medium

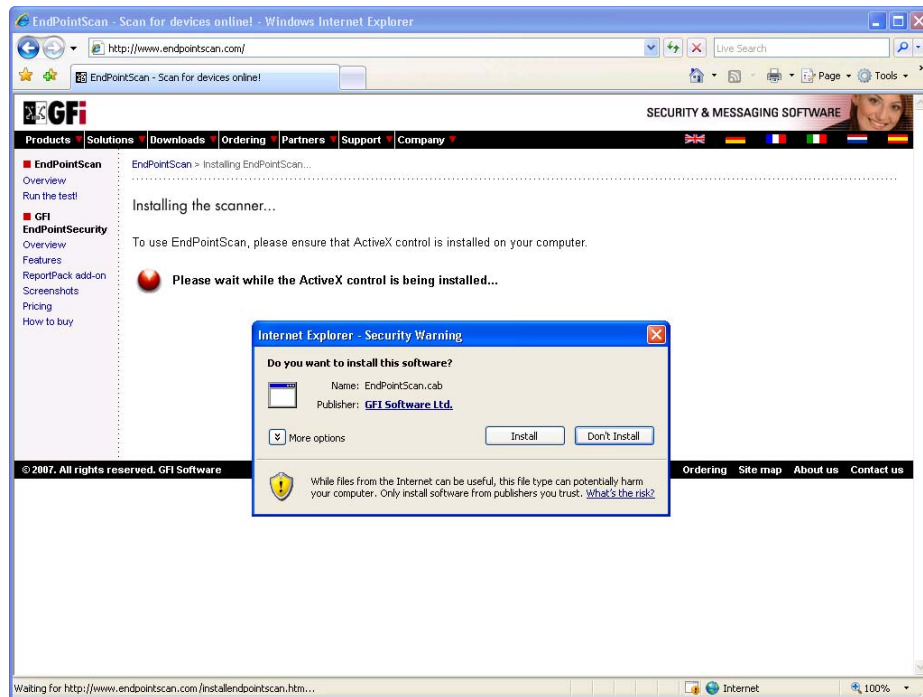
NOTE: You need administrator privileges to set Internet security settings and execute EndPointScan.

Installation procedure



Screenshot 1 – EndPointScan web page

1. When using EndPointScan for the first time, you must download and install an ActiveX control. To do this go to the EndPointScan web page at <http://www.endpointscan.com/>
2. Click **Scan my network!** to download the ActiveX control.



Screenshot 2 – EndPointScan: installing the ActiveX control

3. Click **Install** to finalize installation of the ActiveX control.
- NOTE:** Internet security settings must be set to medium for the ActiveX control to be installed successfully.

Scanning computers

Introduction

After downloading and installing the EndPointScan ActiveX control, you can immediately start scanning computers to locate and report all devices that are or have been locally connected.

This chapter will go through the procedures required to carry out a scan using EndPointScan.

Scanning procedures



Screenshot 3 – EndPointScan webpage

To scan one or more computers:

1. Go to the EndPointScan website at <http://www.endpointscan.com/>
2. Click on **Scan my network!** to specify scan target(s).
3. Click **Next** to initiate the scan.

GFI EndPointScan Results - Windows Internet Explorer

C:\Documents and Settings\Administrator.TW-TESTSERVER\Local Settings\Application Data\WebEndPointScan\20070418_1

Live Search

GFI EndPointScan Results

GFI SECURITY & MESSAGING SOFTWARE

EndPointScan is powered by GFI EndPointSecurity

GFI EndPointScan has finished scanning your computers for devices connected or previously connected. For advanced functionality in protecting your network against portable devices, please use **GFI EndPointSecurity**. 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

Help us improve GFI EndPointScan by sending us the summary of the findings. The data will be used for further research in EndPointSecurity technology. Thank you!

[Send information](#)

■ Scan Summary:

Scan Time: 04/18/07 11:45:18

Scan Target: localhost

Computers scanned: 1

Successful scans: 1

Computers not protected: 1

Devices discovered: 9

Devices currently connected: 1

■ Risk Level:

The average risk level for this scanning session is: **High**

What does this mean?

More information:
The average risk level for a scanning session is an average of the individual risk levels of the computers that were scanned.

Be aware that one single rogue device can compromise your entire network security!

To learn more about **pod sturping** and what risks presents to your organization [click here](#).

■ Device Threat Level:

High (100%)

What does this mean?

■ Device Usage:

Floppy Disks
CD / DVD
Storage Devices
Printers
PDAs
Network Adapters
Modems
Imaging Devices
Human Interface Devices
Other Devices

0 1 2 3 4 5 6 7 8

What does this mean?

■ Computers Protection Level:

Unprotected (100%)

What does this mean?

Computers

Computer	User	Protected by GFI EndPointSecurity	Risk Level	# Devices	# Devices connected
LOCALHOST	TW-TESTSERVER\administrator	No	High	9	1

[View Devices](#)

Computer: LOCALHOST, Devices: 9, Risk Level: High

Device Name	Device Information	Connected	Threat Level	Device Type	Port	Drive
IDE DVD-ROM 16X		Yes	High	CD / DVD	Internal	D:
Generic USB CF Reader USB Device	Mass Storage Device	No	High	Storage devices	USB	F:
Generic USB MS Reader USB Device	Mass Storage Device	No	High	Storage devices	USB	H:
Generic USB SD Reader USB Device	Mass Storage Device	No	High	Storage devices	USB	E:
Generic USB SM Reader USB Device	Mass Storage Device	No	High	Storage devices	USB	G:
Generic USB Storage-CFC USB Device	USB Storage Device	No	High	Storage devices	USB	
Generic USB Storage-MSC USB Device	USB Storage Device	No	High	Storage devices	USB	
Generic USB Storage-SDC USB Device	USB Storage Device	No	High	Storage devices	USB	
Generic USB Storage-SMC USB Device	USB Storage Device	No	High	Storage devices	USB	

© 2007. All rights reserved. GFI Software Ltd

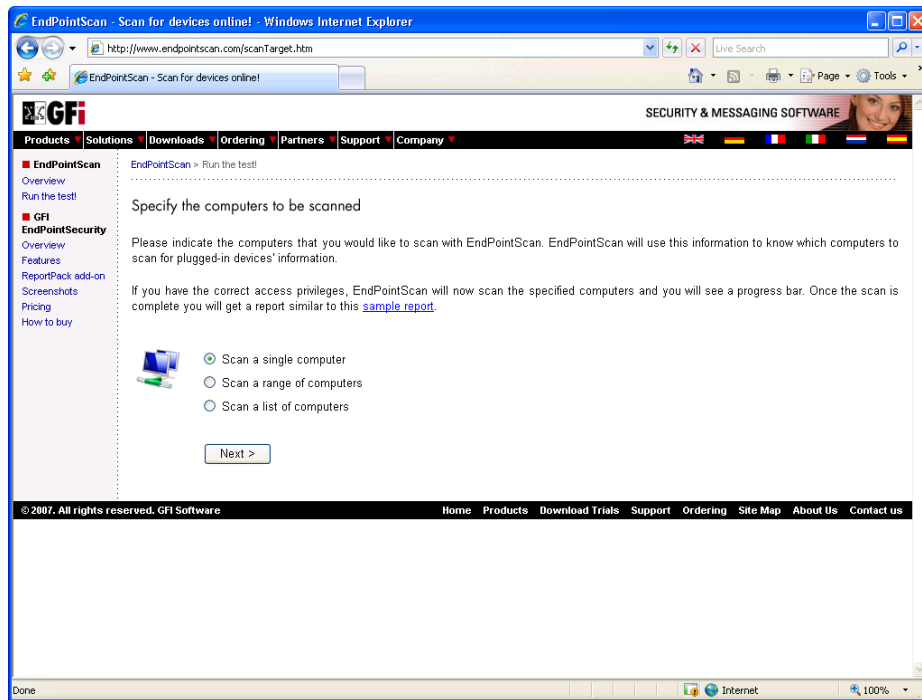
Home Products Support Ordering About Us

Screenshot 4 – Detailed scan results

4. On completion of the scan, detailed scan results are automatically displayed in the browser window.

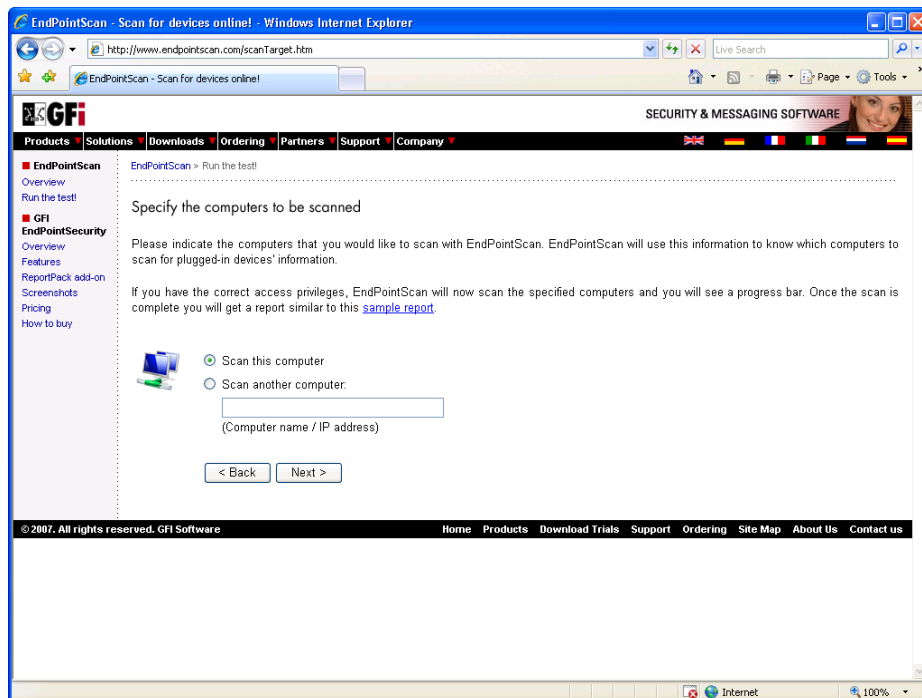
Example 1: Scan the local computer

1. Go to the EndPointScan website at <http://www.endpointscan.com/>
2. Click on **Scan my network!** to specify scan target(s).



Screenshot 5 – Scan a single computer

3. Select the 'Scan a single computer' option and click **Next** to continue.



Screenshot 6 – Ready to scan this computer

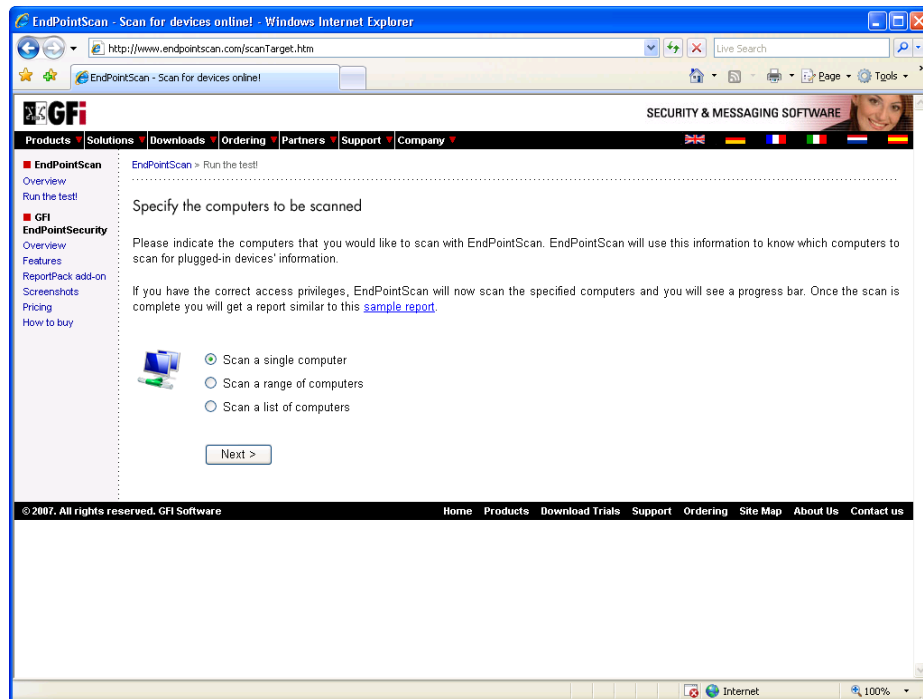
4. Select the 'Scan this computer' option and click **Next** to initiate the scan.

5. When the scan is complete, detailed scan results are displayed.

Example 2: Scan a computer on the LAN

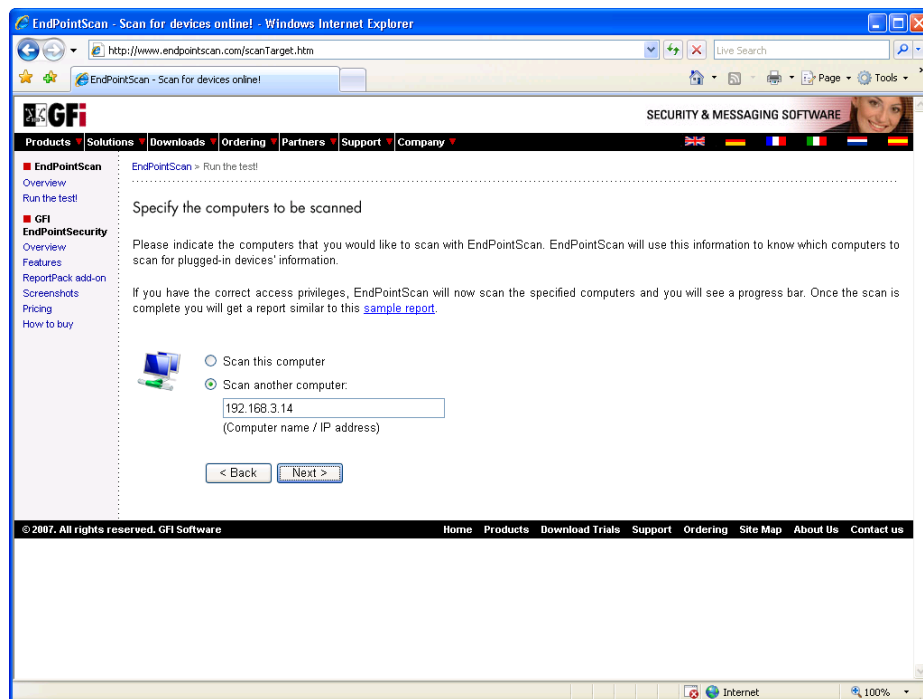
1. Go to the EndPointScan website at <http://www.endpointscan.com/>

2. Click on **Scan my network!** to specify scan target(s).



Screenshot 7 – Scan a single computer

3. Select the 'Scan a single computer' option and click **Next** to continue.



Screenshot 8 – Ready to scan another computer

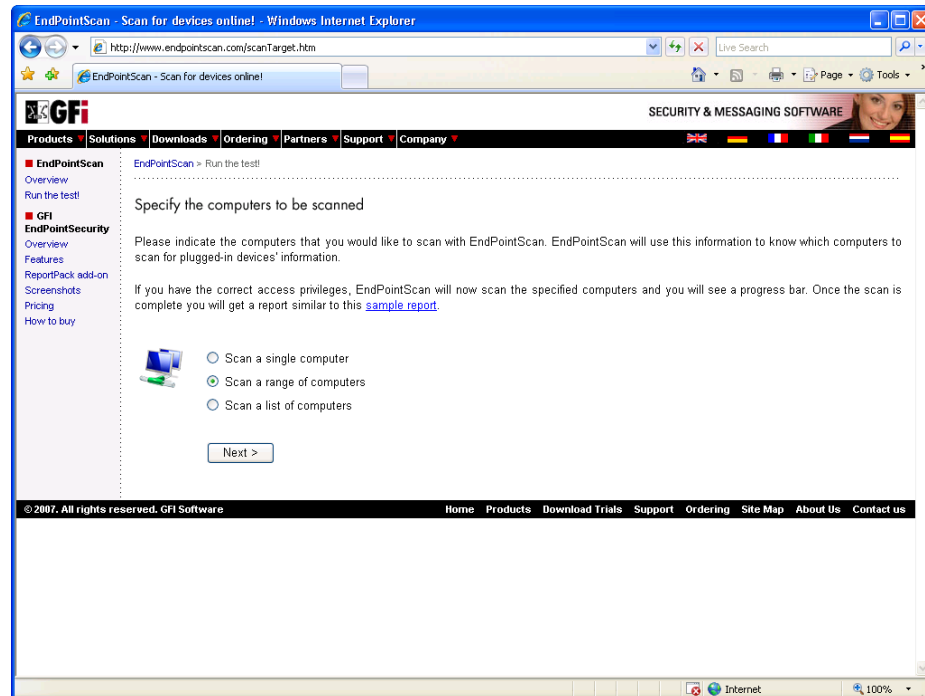
4. Select the 'Scan another computer' option and enter the IP address or computer name of the scan target. Click **Next** to initiate the scan.

5. When the scan is complete, detailed scan results are displayed.

Example 3: Scan a range of computers on the LAN

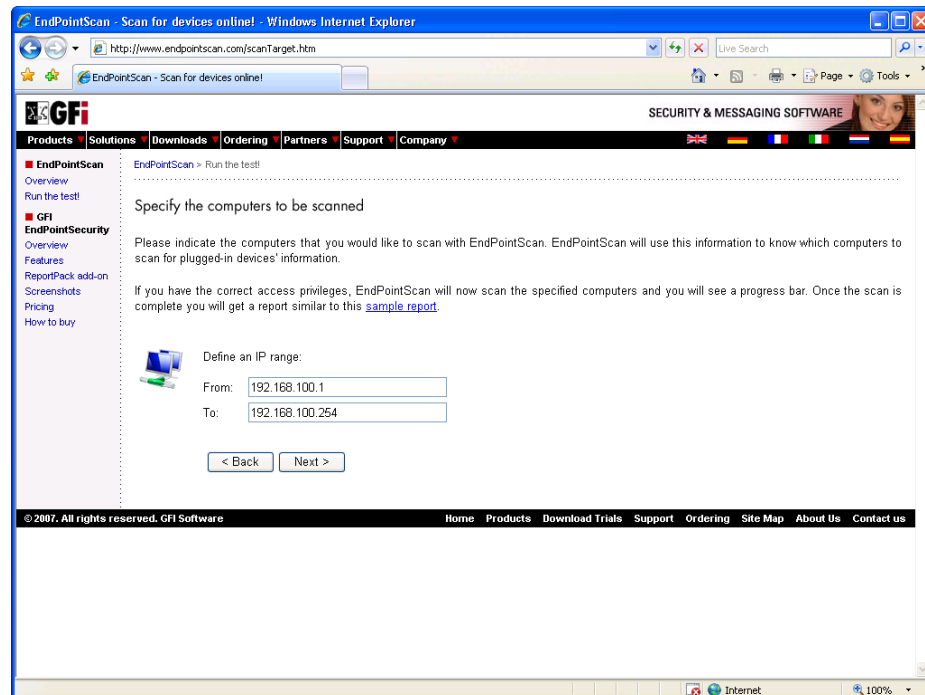
Use this option to scan computers within an IP range on the LAN.

1. Go to the EndPointScan website at <http://www.endpointscan.com/>
2. Click on **Scan my network!** to specify scan target(s).



Screenshot 9 – Scan a range of computers

3. Select the 'Scan a range of computers' option and click **Next** to continue.



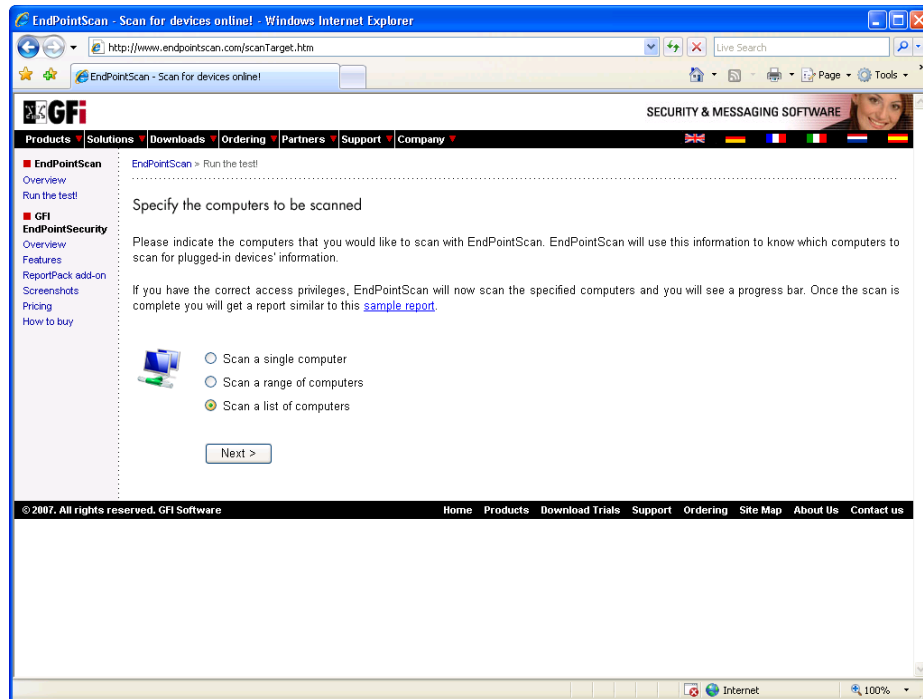
Screenshot 10 – IP range of computers to scan

4. Define the IP range of the scan targets. Click **Next** to initiate the scan.
5. When the scan is complete, detailed scan results are displayed.

Example 4: Scan a list of computers on the LAN

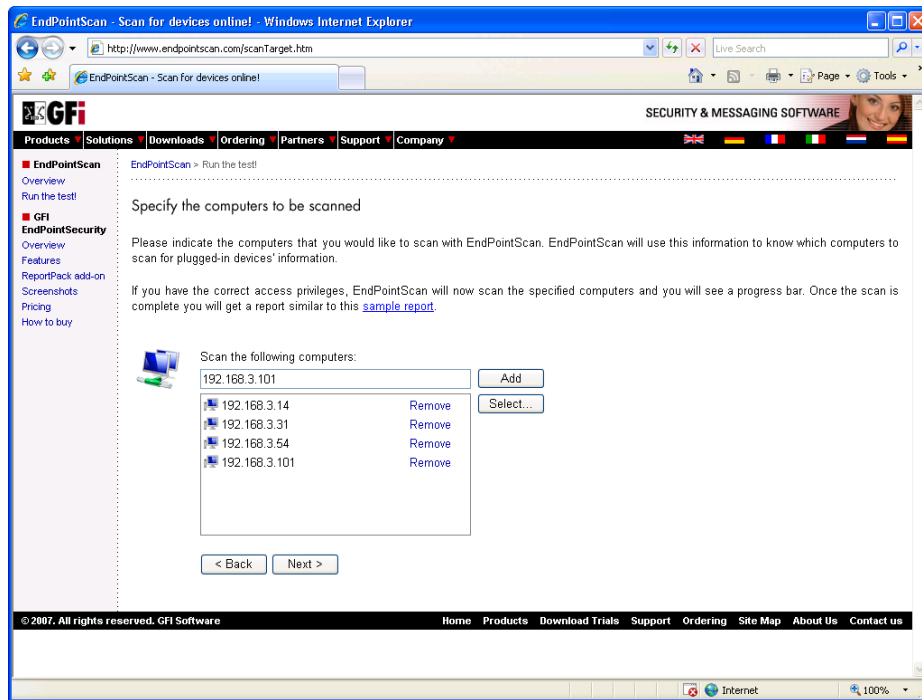
Use this option to scan computers with IP addresses which are not contiguous.

1. Go to the EndPointScan website at <http://www.endpointscan.com/>
2. Click on **Scan my network!** to specify scan target(s).



Screenshot 11 – Scan a list of computers on the LAN

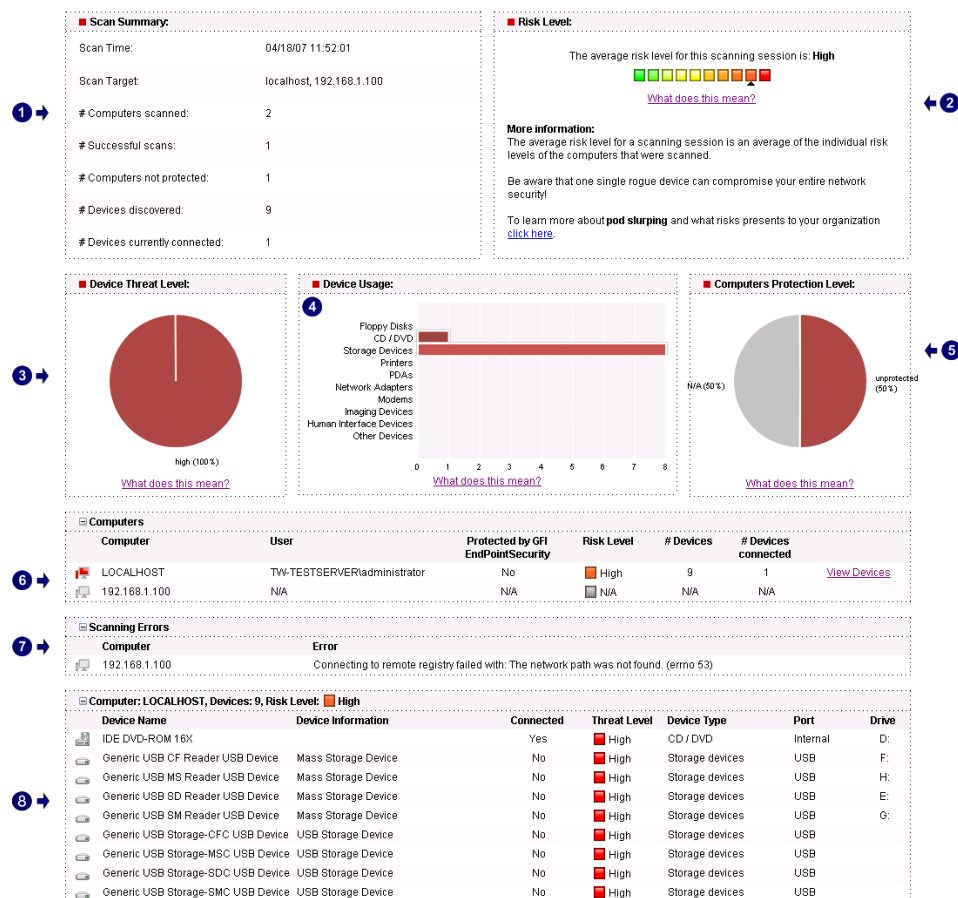
3. Select the 'Scan a list of computers' option and click **Next** to continue.



Screenshot 12 – List of computers to scan

4. Specify the IP addresses or computer names of the scan targets. Click **Next** to initiate the scan.
5. When the scan is complete, detailed scan results are displayed.

Scan results



Screenshot 13 – Detailed scan results

When a scan is completed, EndPointScan automatically displays a detailed scan results report in the browser window. Scan results are organized as follows:

1	Scan summary – This section displays scan details such as duration and number of computers scanned.
2	Risk level – This section graphically displays the risk level based on the computer(s) scanned.
3	Device threat level – This section graphically displays vulnerability level distributions for devices detected during a scan.
4	Device usage – This section graphically displays the number of devices detected for each device type.
5	Computers protection level – This section graphically displays the number of computers detected which have endpoint protection software installed.
6	Computers – This section lists details for each computer scanned, including number of devices detected and the computer's risk level.
7	Scanning Errors – This section lists computers which could not be scanned and the reason for the scan failure.
8	Devices – This section lists device details for each computer scanned, grouped by computer.

Risk level indicator

The average risk level for this scanning session is: **High**



Screenshot 14 – Risk level indicator

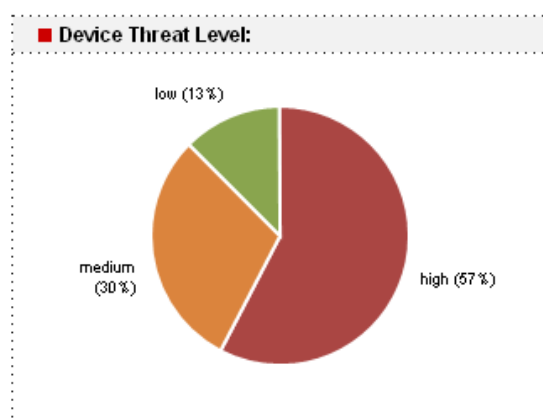
The risk level is a rating given by EndPointScan to each computer after it has been scanned. This rating indicates the vulnerability level of a computer, depending on the level of protection and the number and type of devices that are, or were, connected.

A computer with a high risk level is a result of devices detected whose threat level is categorized as high.

When a number of computers are scanned in a session, a measurement of the global risk level is based on an average of the individual risk levels of the computers scanned.

A graphical measurement using color-coding is provided to give a visual indicator of the risk level. A red color-code is used to indicate a high risk level, whilst a green color-code is used to indicate a low risk level.

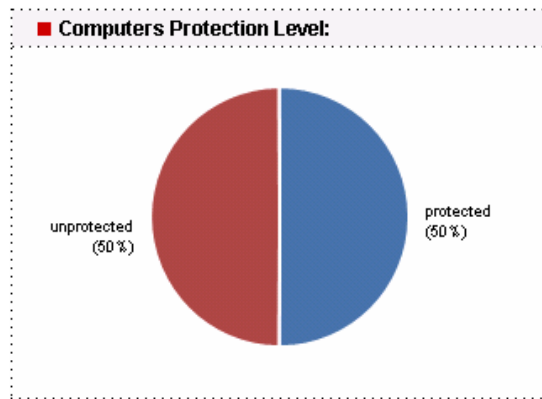
Device threat level



Screenshot 15 – device threat level

Portable devices in EndPointScan are organized into categories, such as storage devices, imaging devices and human interface devices. Each device category is assigned a high, medium or low risk level depending on the threat that device class may represent to a corporation. For example human interface devices such as keyboards have a low risk level whilst storage devices such as USB flash drives have a high risk level. The device threat level graph displays the distribution of high, medium and/or low risk level devices detected during a scan.

Computer protection level



Screenshot 16 – computer protection level

Computer protection level displays the percentage of computers scanned by EndPointScan, which are covered by endpoint protection provided by GFI EndPointSecurity. Computers not covered by GFI EndPointSecurity are shown as unprotected.

Troubleshooting

Introduction

The troubleshooting chapter explains how you should go about resolving issues you have. The main sources of information available to users are:

- The manual – most issues can be solved by reading the manual.
- The GFI Knowledge Base – accessible from the GFI website.
- The GFI web forum.

Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of support questions and patches.

The Knowledge Base can be found on <http://kbase.gfi.com/>.

Web Forum

User to user technical support is available via the web forum. The forum can be found at:

<http://forums.gfi.com/>.

Request technical support via email

If, after using the Knowledge Base, the Web Forum and this manual, you have any problems that you cannot solve, you can contact the GFI technical support team. The best way to do this is via email on support@gfi.com, since you can include vital information as an attachment that will enable us to solve the issues you have more quickly.

Index

B

Bluetooth 6

C

CD/DVD ROM 5
computer protection level 17,
19
Creative Zen 6

D

device threat level 17, 18
device usage 17

F

features 7
Firewire 6
flash memory 6
Floppy disk 5

I

iPod 6

M

MP3 player 5

P

PDA's 6
portable devices 3, 5
printers 6

R

risk level 17, 18

S

scan results 17
Scanning procedures 10
scanning errors 17
Secure Digital 6
Storage Devices 5
System requirements 8

T

Troubleshooting 20

U

USB 5, 6, 7, 18
USB Pen drives 5