"Highest Performance
Lowest Price"

Microsoft
GOLD CERTIFIED
Partner

GFI EndPointSecurity 4.3

Getting Started Guide

http://www.gfi.com

E-mail: info@gfi.com

Last updated: 30 June 2010

Version number: ESEC-GSG-EN-01.00.01

Contents

1 Introduction

1.1 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, but still, 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. Newer versions of portable devices, such as flash memory, have increased in:

- Better storage capacity
- Improved performance
- Easier and faster to install
- Physically small enough to carry in a pocket.

As a result, internal users may deliberately or accidentally:

- Take away sensitive data
- Expose confidential information
- Introduce malicious code (e.g. viruses, Trojans) that can bring the entire corporate network down
- Transfer inappropriate or offensive material on to corporate hardware
- Make personal copies of company data and intellectual property
- Get distracted during work hours.

In an attempt to control these threats, organizations have started to prohibit the use of (personally-owned) portable devices at work. Best practice dictates that you must never rely on voluntary compliance and the best way to ensure complete control over portable devices is by putting technological barriers.

1.2 GFI EndPointSecurity – the solution

GFI EndPointSecurity is the security solution that helps you maintain data integrity by preventing unauthorized access and transfer of content to and from the following devices or connection ports:

- USB Ports (e.g. Flash and Memory card readers, pen drives)
- Firewire ports (e.g. digital cameras, Firewire card readers)
- Wireless data connections (e.g. Bluetooth and Infrared dongles)
- Floppy disk drives (internal and external)

- Optical drives (e.g. CD, DVD)
- Magneto Optical drives (internal and external)
- Removable USB hard-disk drives
- Other drives such as Zip drives and tape drives (internal and external).

Through its technology, GFI EndPointSecurity enables you to allow or deny access and to assign 'full' or 'read only' privileges to:

- Devices (e.g. CD/DVD drives, PDAs).
- Local or Active Directory users/user groups.

With GFI EndPointSecurity you can also record the activity of all devices or connection ports being used on your target computers (including the date/time of usage and by whom the devices were used).

1.3 Using this manual

This user manual is a comprehensive guide aimed at assisting you in installing, and testing GFI EndPointSecurity. It describes how to use and configure GFI EndPointSecurity to achieve the best possible corporate security.

This manual contains the following chapters:

Chapter 1	**Introduction** Introduces this manual.
Chapter 2	**About GFI EndPointSecurity** Provides basic information on GFI EndPointSecurity and how it works.
Chapter 3	**Installing GFI EndPointSecurity** Provides information on system requirements and how to install the GFI EndPointSecurity.
Chapter 4	**Getting Started** Provides information on how to configure the installation of GFI EndPointSecurity using the Quick Start wizard.
Chapter 5	**Testing GFI EndPointSecurity** Provides information on how to test your GFI EndPointSecurity installation.
Chapter 6	**Miscellaneous** Provides information on licensing and versioning.
Chapter 7	**Troubleshooting** Provides all the necessary information on how to deal with any problems encountered while using GFI EndPointSecurity. Also provides extensive support information.
Chapter 8	**Glossary** Defines technical terms used within GFI EndPointSecurity.

Chapter 9	Appendix 1 - Deployment error messages Provides a list of errors displayed during deployment of agents from the management console.

Administration and Configuration Manual

Detailed administration and configuration guidelines are provided in the **GFI EndPointSecurity - Administration and Configuration Manual**, which is installed with the product or separately downloadable from the GFI website:

http://www.gfi.com/esec/esec4manual.pdf

The Administration and Configuration Manual complements this Getting Started Guide and provides more information on how to use and customize the features provided by GFI EndPointSecurity.

1.4 Terms used in this manual

The following terms are used in this manual:

- **"NOTE:"**
  - Provides additional information and references essential for the operation of GFI EndPointSecurity.
- **"IMPORTANT:"**
  - Provides important information such as warnings and cautions regarding potential issues commonly encountered.

For any technical terms and their definitions as used in this manual, refer to the Glossary chapter in this manual.

1.5 GFI EndPointSecurity licensing

For more information on licensing and evaluation, refer to the GFI website at:

http://www.gfi.com/products/gfi-endpointsecurity/pricing/licensing

2 About GFI EndPointSecurity

2.1 Introduction

This chapter provides you with the following information:

- The key features and components of GFI EndPointSecurity
- How GFI EndPointSecurity works
- The device categories and connectivity ports supported by GFI EndPointSecurity

2.2 Key features

GFI EndPointSecurity offers the following main features:

Group-based protection control

In GFI EndPointSecurity you can configure and place computers into groups that are governed by one protection policy. This allows you to configure a single protection policy and apply it to all the computers that are members of that group.

Granular access control

GFI EndPointSecurity enables you to allow or deny access to a specific device as well as to assign (where applicable) 'full' or 'read only' privileges over every supported device (e.g. CD/DVD drives, PDAs) on a user by user basis.

Scheduled deployment

GFI EndPointSecurity allows you to schedule the deployment of protection policies and any related configuration changes without the need to keep to the GFI EndPointSecurity management console open. The deployment feature also handles failed deployments through automatic rescheduling.

Access control

Apart from blocking a range of device categories, GFI EndPointSecurity also allows blocking:

- By file type - for example, allow the user to read *.doc files but block access to all *.exe files.
- By physical port - all devices connected to particular physical ports, for example, all devices connected to USB ports.
- By device ID – block access to a single device based on the unique Hardware ID of the device.

NOTE: In Microsoft Windows 7, a feature called **BitLocker To Go** can be used to protect and encrypt data on removable devices. GFI EndPointSecurity performs checks on real file types encrypted with Windows 7 BitLocker To Go.

Device whitelist and blacklist

The administrator can define a list of specific devices that are permanently allowed and others that are permanently banned.

Power users

The administrator can specify users or groups who would always have full access to devices that are otherwise blocked by GFI EndPointSecurity.

Temporary access

The administrator is able to grant temporary access to a device (or group of devices) on a particular computer. This feature allows the administrator to generate an unlock code that the end-user can use to obtain a time-limited access to a particular device or port, even when the GFI EndPointSecurity agent is not connected to the network.

Status dashboard

The dashboard's user interface shows the statuses of live and deployed agents, database and alerting servers, the GFI EndPointSecurity service as well as statistical data with charts.

The main application keeps track of the live agent status by communicating with its deployed agents. Maintenance tasks are performed automatically once an agent goes online.

Active Directory deployment through MSI

From the GFI EndPointSecurity management console it is possible to generate MSI files that can be later deployed using the Group Policy Object (GPO) feature within the Active Directory or other deployment options. An MSI file will contain all the security settings configured in a particular protection policy.

Agent management password

Agent management functions (such as update and un-install) are protected by a user-configurable password. This means that any other GFI EndPointSecurity instances will not have access to the agent management options.

Device discovery

The GFI EndPointSecurity engine can be used to scan and detect the presence of devices on the network, even on computers that are not assigned any protection policy. The information gathered about detected devices can then be used to build security policies and assign access rights for specific devices.

Logs browser

An in-built tool allows the administrator to browse logs of user activity and device usage that is detected by GFI EndPointSecurity.

Alerting

GFI EndPointSecurity allows you to configure e-mail alerts, network messages and SMS messages that can be sent to specified recipients when devices are connected or

disconnected, when device access is allowed or blocked and upon service generated events.

Custom messages

When users are blocked from using devices, they are shown popup messages explaining the reasons why the device was blocked. GFI EndPointSecurity allows the customization of these messages.

Database maintenance

To maintain the size of the database backend, GFI EndPointSecurity can be set to backup or delete events older than a custom number of hours or days.

2.3 Components of GFI EndPointSecurity

When you install GFI EndPointSecurity, the following components are set up:

- GFI EndPointSecurity management console
- GFI EndPointSecurity agent.

GFI EndPointSecurity management console

Through the GFI EndPointSecurity management console you can:

- Create and manage protection policies and specify which device categories and connectivity ports are to be controlled.
- Remotely deploy protection policies and agents on to your target computers Grant temporary access to target computers to use specific devices.
- View the device protection status of every computer that is being monitored.
- Carry out scans on target computers to identify devices currently or previously connected.
- Check logs and analyze what devices have been connected to every network computer.
- Keeps track of which computers have an agent deployed and which agents need to be updated.

GFI EndPointSecurity agent

The GFI EndPointSecurity agent is a client-side service responsible for the implementation of the protection policies on the target computer(s). This service is automatically installed on the remote network target computer after the first deployment of the relevant protection policy through the GFI EndPointSecurity management console. Upon the next deployments of the same protection policy, the agent will be updated and not re-installed.

2.4 How GFI EndPointSecurity works - Deployment and monitoring

GFI EndPointSecurity protection policy deployment and monitoring operations can be divided in four logical stages:

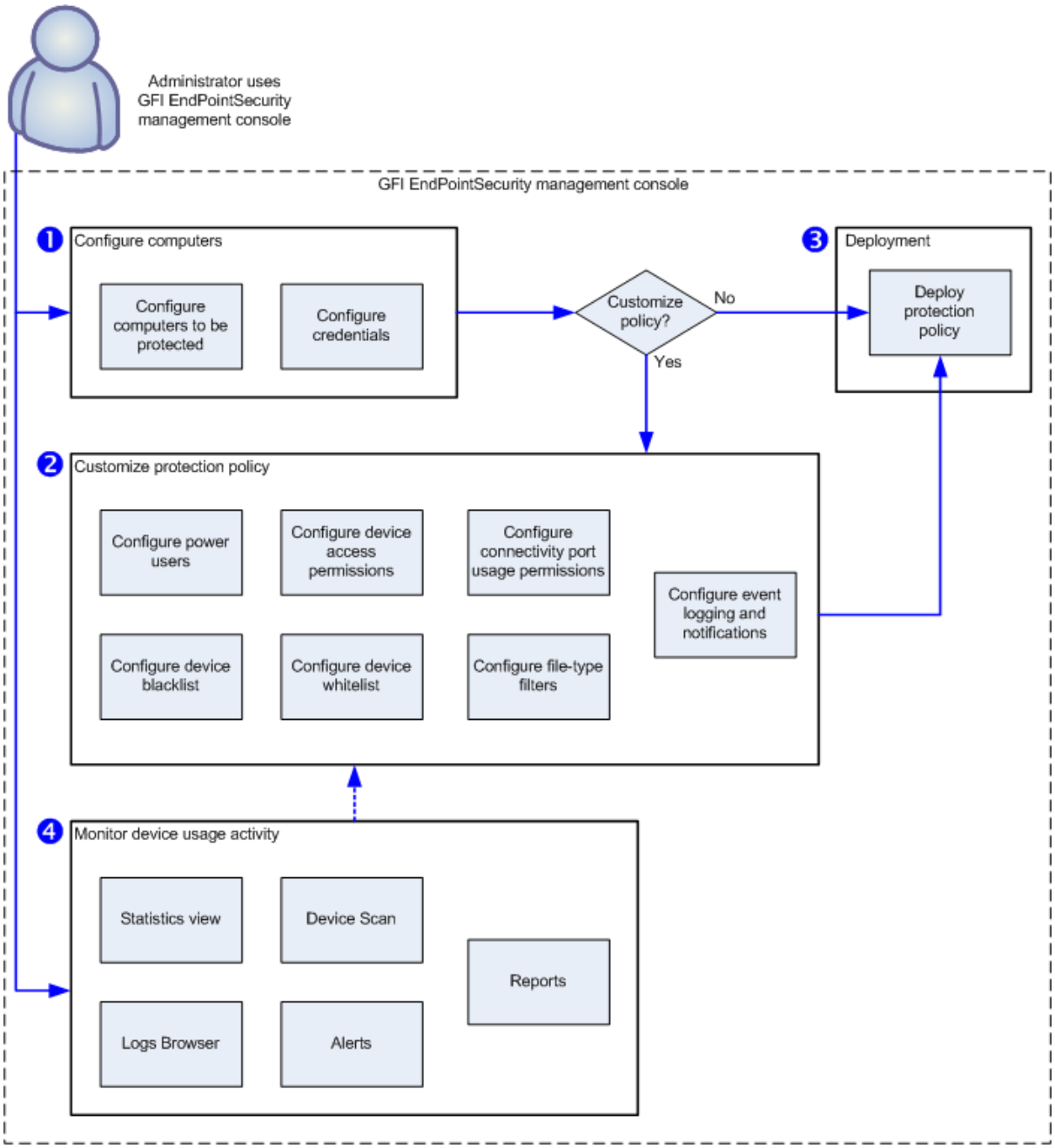


Figure 1 - Protection policy deployment and monitoring

Stage 1 - Configure computers: The administrator specifies which protection policy is assigned to which computers, and the log-on credentials to be used by GFI EndPointSecurity to access the target computers and deploy the agents.

Stage 2 - Customize protection policy: The administrator can customize a protection policy before or after deploying it. Customization options include the creation of power users, addition of blacklisted/whitelisted devices and device access permissions.

Stage 3 - Deploy protection policy: The administrator deploys the protection policy. Upon the first deployment of a protection policy, a GFI EndPointSecurity agent is automatically installed on the remote network target computer. Upon the next deployments of the same protection policy, the agent will be updated and not re-installed.

Stage 4 - Monitor device access: When agents have been deployed, the administrator can monitor all device access attempts via the GFI EndPointSecurity management console, receive alerts and generate reports through the GFI EndPointSecurity ReportPack.

2.5 How GFI EndPointSecurity works - Device access

GFI EndPointSecurity device access operations can be divided in three logical stages:

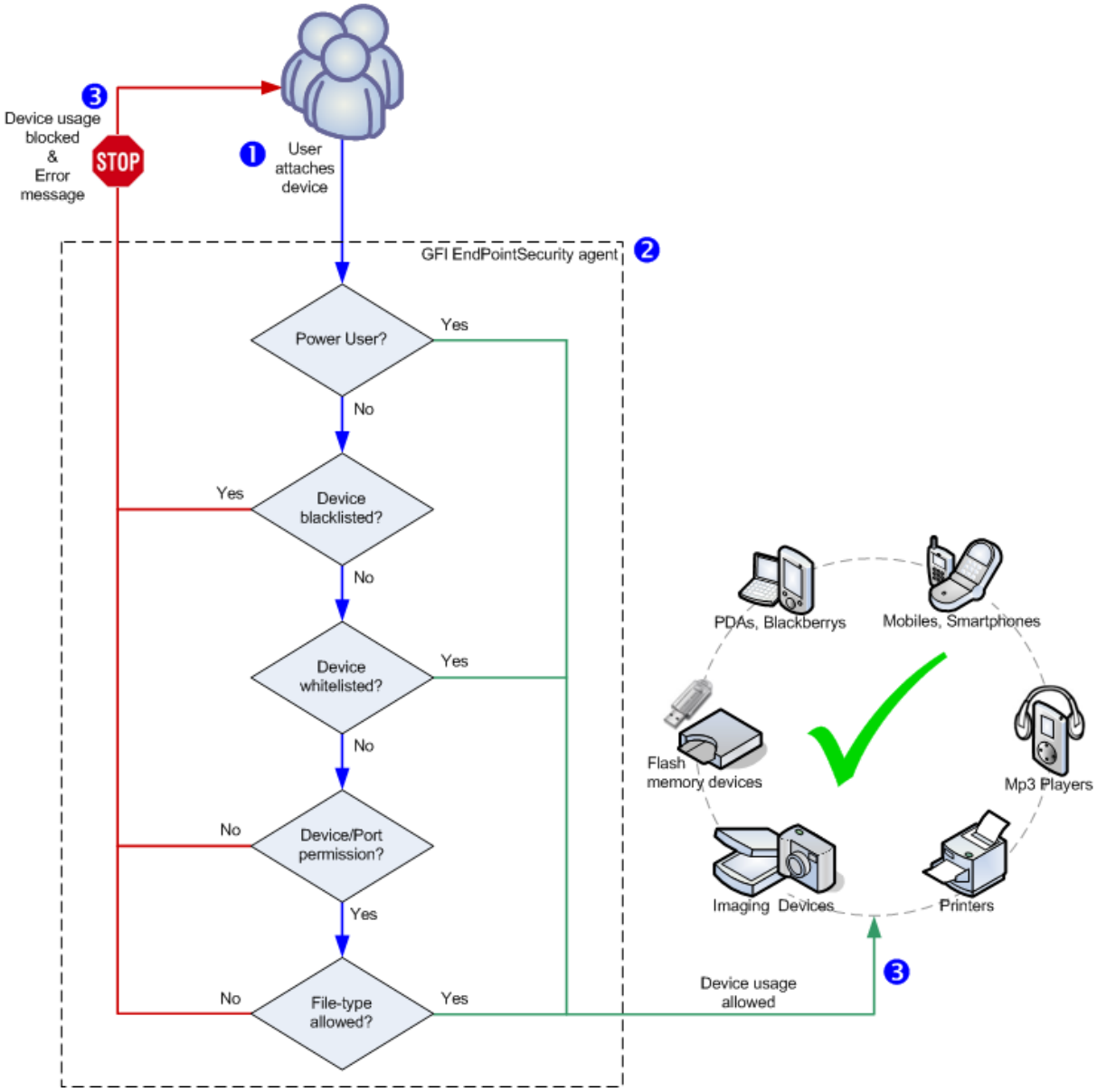


Figure 2 - Device access

Stage 1 - Device attached to computer: The user attaches a device to a target computer protected by GFI EndPointSecurity.

Stage 2 - Protection policy enforcement: The GFI EndPointSecurity agent installed on the target computer detects the attached device and goes through the protection policy rules applicable to the computer/user. This operation determines whether the device is allowed or blocked from being accessed.

Stage 3 - Device usage allowed/blocked: The user either receives an error message indicating that device usage has been blocked, or else is allowed to access the device.

2.6 How GFI EndPointSecurity works - Temporary access

GFI EndPointSecurity temporary access operations can be divided in three logical stages:

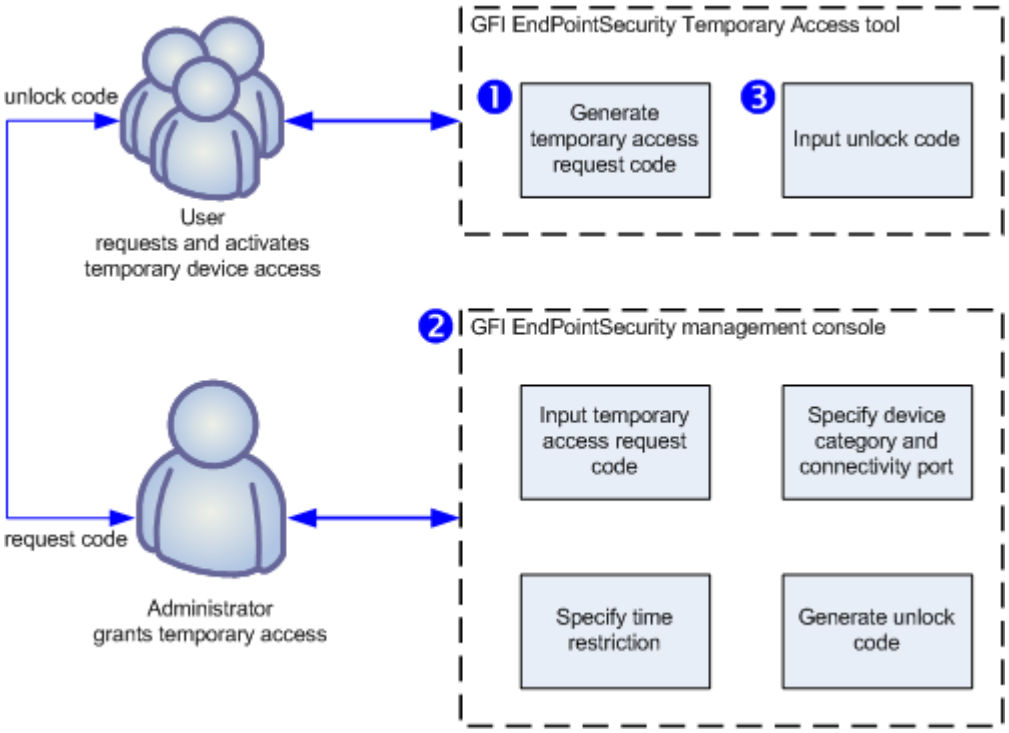


Figure 3 -Requesting/granting temporary access

Stage 1 - User requests temporary device access: The user executes the GFI EndPointSecurity Temporary Access tool from the computer on which the device is to be accessed. The tool is used to generate a request code, which the user communicates with the administrator. The user also needs to inform the administrator on the device types or connection ports that need to be accessed, and for how long will devices/ports access be required.

Stage 2 - Administrator grants temporary access: The administrator uses the Temporary Access feature within the GFI EndPointSecurity management console to enter the request code, specify devices/ports and time restrictions. An unlock code is generated which the administrator then communicates with the user.

Stage 3 - User activates temporary device access: Once the user receives the unlock code sent by the administrator, this code is entered in the GFI EndPointSecurity Temporary Access tool to activate the temporary access and to be able to use the required devices/ports.

2.7 Supported device categories

In GFI EndPointSecurity device categories are organized into the following categories:

- Floppy disks
- CD / DVD
- Storage Devices
  - USB Pen drives
  - Digital Media Players (e.g. MP3/MP4 players)
  - Flash and Memory Card Readers
  - Multi-drive USB devices (i.e. devices that do not mount as a single drive)
  - Other portable storage devices
- Printers
- PDAs
  - Pocket PCs
  - Smart phones
- Network Adapters
  - Wi-Fi
  - Removable Network Adapters (e.g. USB, Firewire, PCMCIA)
- 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.

2.8 Supported connectivity ports

GFI EndPointSecurity scans for devices that are or have been connected on the following ports:

- USB
- Firewire
- PCMCIA
- Bluetooth
- Serial & Parallel
- Infrared
- Secure Digital (SD)
- Internal (e.g. optical drives connected internally on PCI).

3 Installing GFI EndPointSecurity

3.1 Introduction

This chapter provides you with the following information:

- The system requirements of GFI EndPointSecurity
- How to upgrade from GFI EndPointSecurity 3 or later and from GFI LANguard Portable Storage Control
- How to install GFI EndPointSecurity

3.2 System requirements

The following are the system requirements to install GFI EndPointSecurity:

3.2.1 Hardware requirements

- Processor: 2GHz processor clock speed or better
- RAM: 512 MB (minimum); 1 GB (recommended)
- Hard disk: 100 MB of available space (further disk space is required for the database backend)

3.2.2 Software requirements

Supported operating systems

GFI EndPointSecurity can be installed on the following operating systems (x86 or x64):

- Microsoft Windows Server 2008 R2 (x64) (Standard or Enterprise edition)
- Microsoft Windows Server 2008 (Standard or Enterprise edition)
- Microsoft Windows Server 2003 (Standard, Enterprise or Web edition)
- Microsoft Windows 7 (Professional, Enterprise or Ultimate edition)
- Microsoft Windows Vista (Enterprise, Business or Ultimate edition)
- Microsoft Windows XP Professional
- Microsoft Windows Small Business Server 2008 (Standard edition)
- Microsoft Windows Small Business Server 2003

Other required components

- Microsoft Internet Explorer 5.5 or later
- Microsoft .NET Framework 2.0

- TCP port 1116 (default) - required by the GFI EndPointSecurity agents to notify the GFI EndPointSecurity management console about their statuses and send device access events. Without this port open to receive events, the administrator will have to either manually monitor the events in the Event Viewer of each target computer or use GFI EventsManager to automatically collect and monitor events from the target computers on the server. For more information about GFI EventsManager, refer to the GFI website at: http://www.gfi.com/eventsmanager.

NOTE: Ensure that your firewall settings enable communications between all the target computers where the GFI EndPointSecurity agents are installed and the GFI EndPointSecurity server.

Optional components

- Microsoft SQL Server 2000, 2005, 2008 (database backend)

NOTE: A database backend is required for storing device access data and for reporting purposes. GFI EndPointSecurity provides the option to either use an available Microsoft SQL Server or else to automatically download and install Microsoft SQL Server 2005 Express on the same computer where GFI EndPointSecurity management console is installed.

3.2.3 Agent - Hardware requirements

- Processor: 1GHz processor clock speed or better
- RAM: 256 MB (minimum); 512 MB (recommended)
- Hard Disk: 50 MB of available space

3.2.4 Agent - Software requirements

Supported operating systems

GFI EndPointSecurity agent can be installed on the following operating systems (x86 or x64):

- Microsoft Windows Server 2008 R2 (x64) (Standard or Enterprise edition)
- Microsoft Windows Server 2008 (Standard or Enterprise edition)
- Microsoft Windows Server 2003 (Standard, Enterprise or Web edition)
- Microsoft Windows 7 (Professional, Enterprise or Ultimate edition)
- Microsoft Windows Vista (Enterprise, Business or Ultimate edition)
- Microsoft Windows XP Professional
- Microsoft Windows Small Business Server 2008 (Standard edition)
- Microsoft Windows Small Business Server 2003

3.3 Upgrading from earlier versions

If you have GFI LANguard Portable Storage Control, or an earlier version of GFI EndPointSecurity, it is possible to upgrade to GFI EndPointSecurity 4.3.

3.3.1 Upgrading from GFI EndPointSecurity 3 or later

Upgrading from GFI EndPointSecurity 3 or later to GFI EndPointSecurity 4.3 is straightforward. The upgrade process is part of the GFI EndPointSecurity 4.3 installation process, and includes:

- Uninstalling GFI EndPointSecurity 3 or later
- Importing GFI EndPointSecurity 3 configuration settings.

Importing configuration settings from GFI EndPointSecurity 3 or later

When installing GFI EndPointSecurity, you are asked to confirm whether you want to import configurations from the previous version. Click **Yes** to import configurations. You are then prompted to specify which of the following configurations to import:

- Protection Policies:
  - Computer
  - Security settings
- Options:
  - Logging options
  - Database options

3.3.2 Upgrading from GFI LANguard Portable Storage Control

If the computer on which you are installing GFI EndPointSecurity is protected by a GFI LANguard Portable Storage Control agent, you first need to uninstall that agent. To do this:

1. Open GFI LANguard Portable Storage Control configuration console.

2. Delete the agent from the computer where GFI EndPointSecurity will be installed.

NOTE: This process should be done only for the computer where GFI EndPointSecurity 4.3 will be installed.

3. Close the GFI LANguard Portable Storage Control configuration console application and proceed to installing GFI EndPointSecurity.

4. When installing GFI EndPointSecurity, you are asked to confirm whether you want to import configurations from the previous version. Click **Yes** to import configurations.

NOTE: The GFI LANguard Portable Storage Control agents that were protecting your computers will be automatically added to a protection policy called LegacyAgents in GFI EndPointSecurity.

3.4 Installing GFI EndPointSecurity

To install GFI EndPointSecurity:

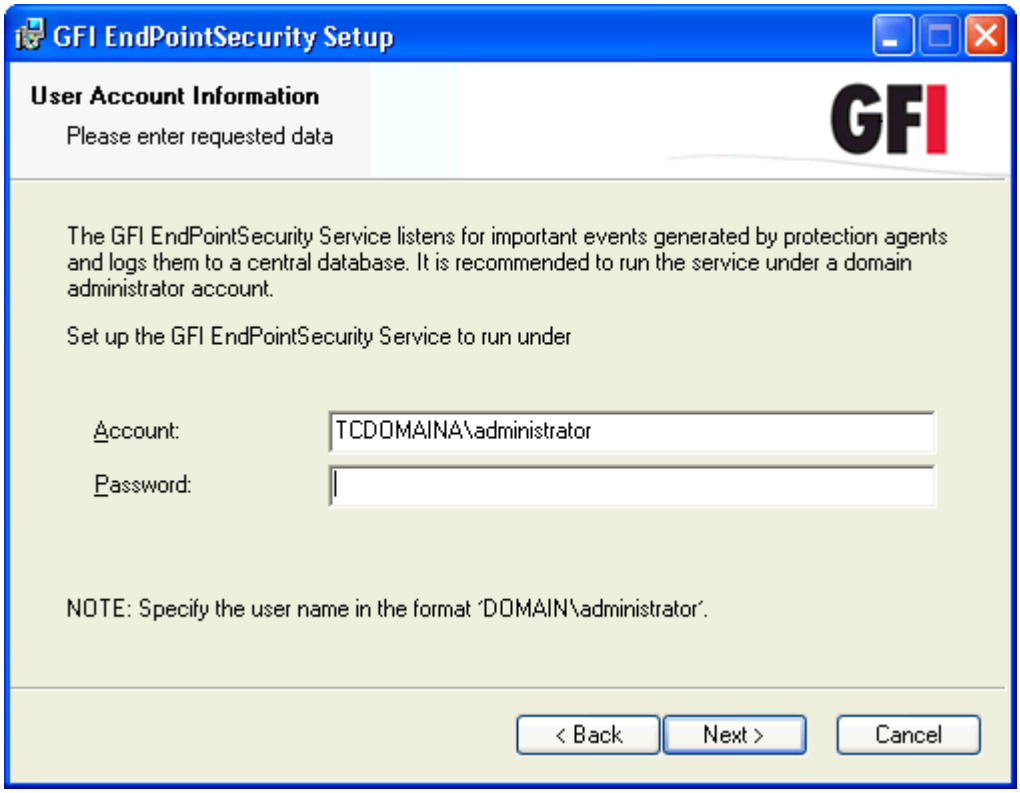
NOTE: Run the installer as a user with administrative privileges on the computer.

1. Double-click on the GFI EndPointSecurity executable file.

2. Select language, and click **OK**.

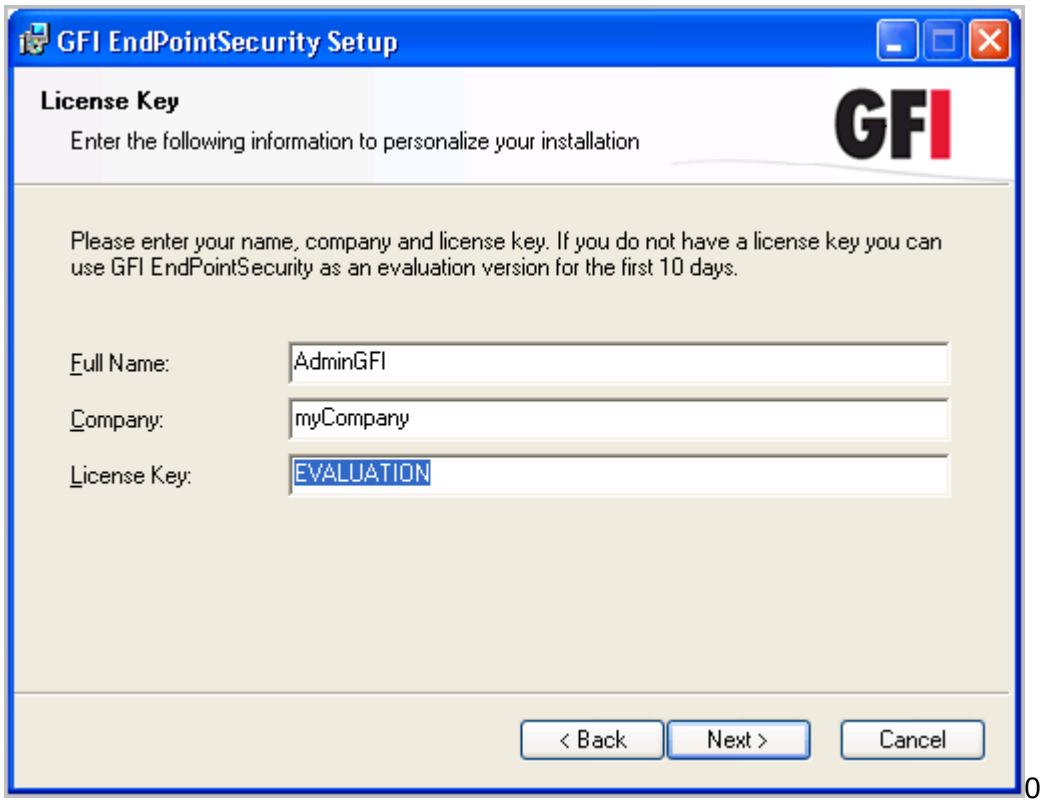
3. Click **Next** at the Welcome screen to start setup.

4. Read carefully the End-User License Agreement. If you agree to the terms laid out in the agreement, select **I accept the license agreement** and click **Next**.



Screenshot 1 - GFI EndPointSecurity installation: domain administrator account setup

5. Key in the logon credentials of an account with administrative privileges and click **Next** to continue.



Screenshot 2 - GFI EndPointSecurity installation: license key details

6. Key in the **Full Name** and **Company**. If you have a license key, update the **License Key** details and click **Next**.

NOTE: The license key can be keyed in after installation or expiration of the evaluation period of GFI EndPointSecurity. For more information, refer to the Entering your license key after installation section in the Miscellaneous chapter.

7. Key in or browse to select an alternative installation path or click **Next** to use the default path and proceed with the installation.

8. Click **Back** to re-enter installation information or click **Next** and wait for the installation to complete.

9. Upon installation completion, enable or disable the **Launch GFI EndPointSecurity** checkbox and click **Finish** to finalize installation.

4 Getting Started

4.1 Introduction

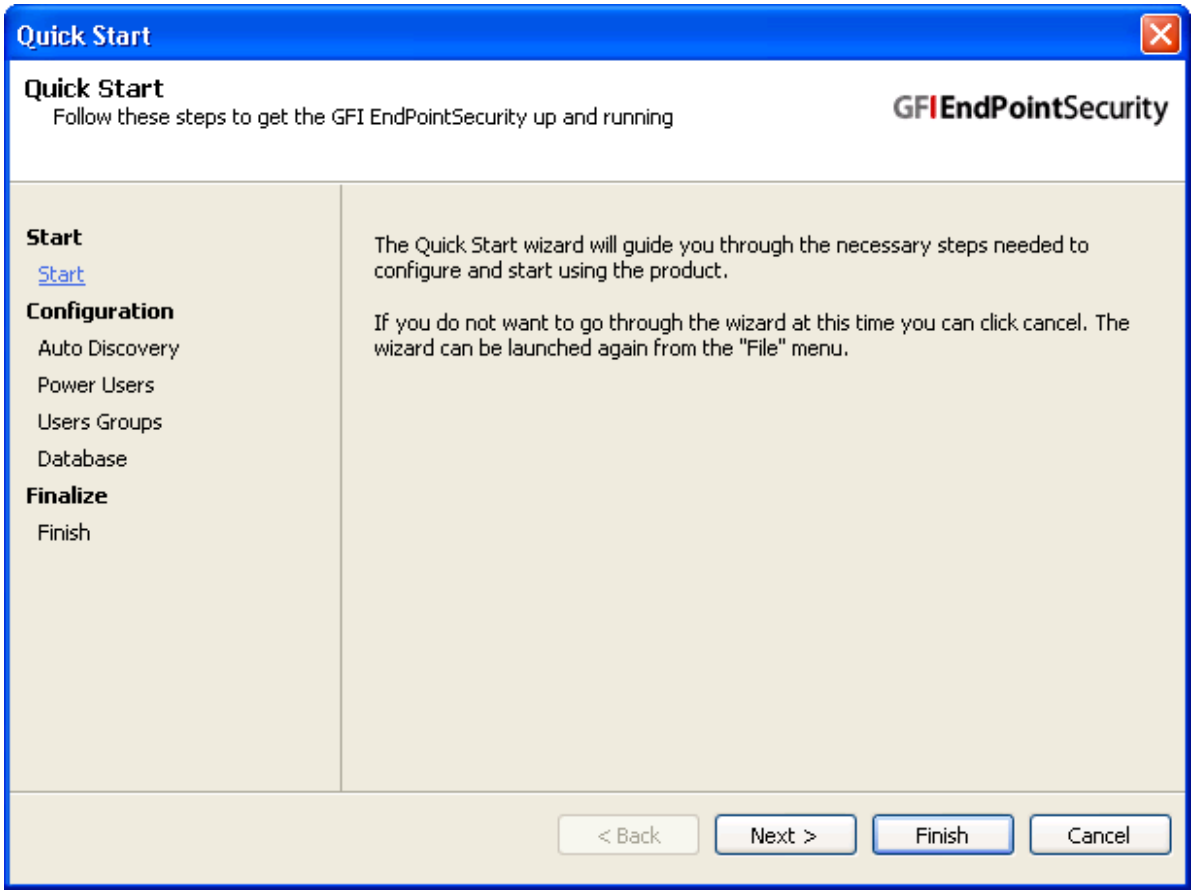
Upon the initial launch of GFI EndPointSecurity management console, the Quick Start wizard will automatically be launched. This will enable you to configure GFI EndPointSecurity for first time use.

The Quick Start wizard will guide you in configuring the following settings:

- automatic discovery
- power users
- users groups
- database backend.

4.2 Using the Quick Start wizard

The Quick Start wizard can also be launched from **File ► Quick Start Wizard…**.



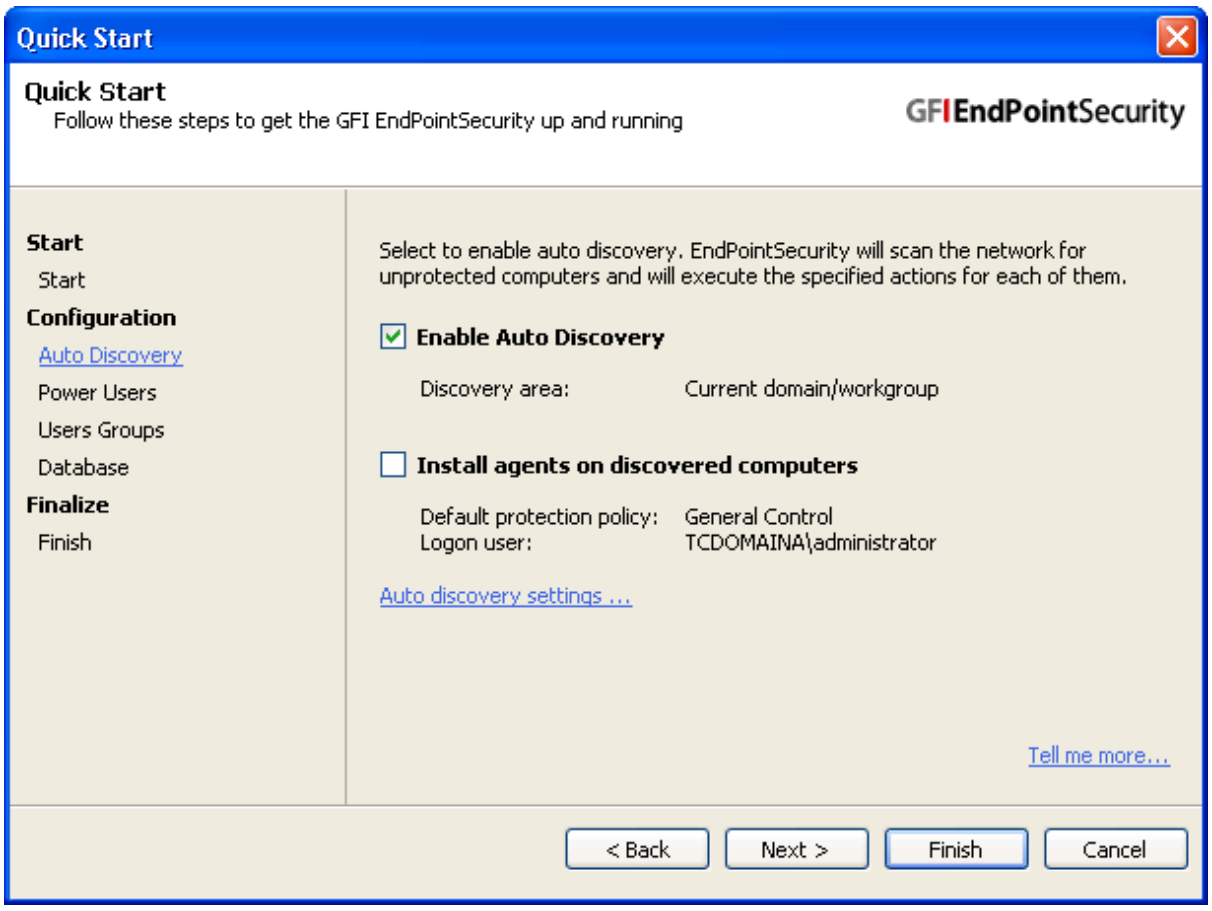
Screenshot 3 - GFI EndPointSecurity Quick Start wizard: Start step

Step 1. Configuring automatic discovery

GFI EndPointSecurity provides you with the facility to search for newly connected computers to the network at configured scheduled times through the auto discovery feature. In addition, you can also instruct the agent deployment feature to assign the default protection policy to the newly discovered computers.

By default:

- the **Enable Auto Discovery** checkbox is enabled
- the auto discovery settings are set to scan the **Current domain/workgroup**
- the install agents settings are set to assign the **General Control** protection policy (shipping default protection policy) on to the newly discovered computers.

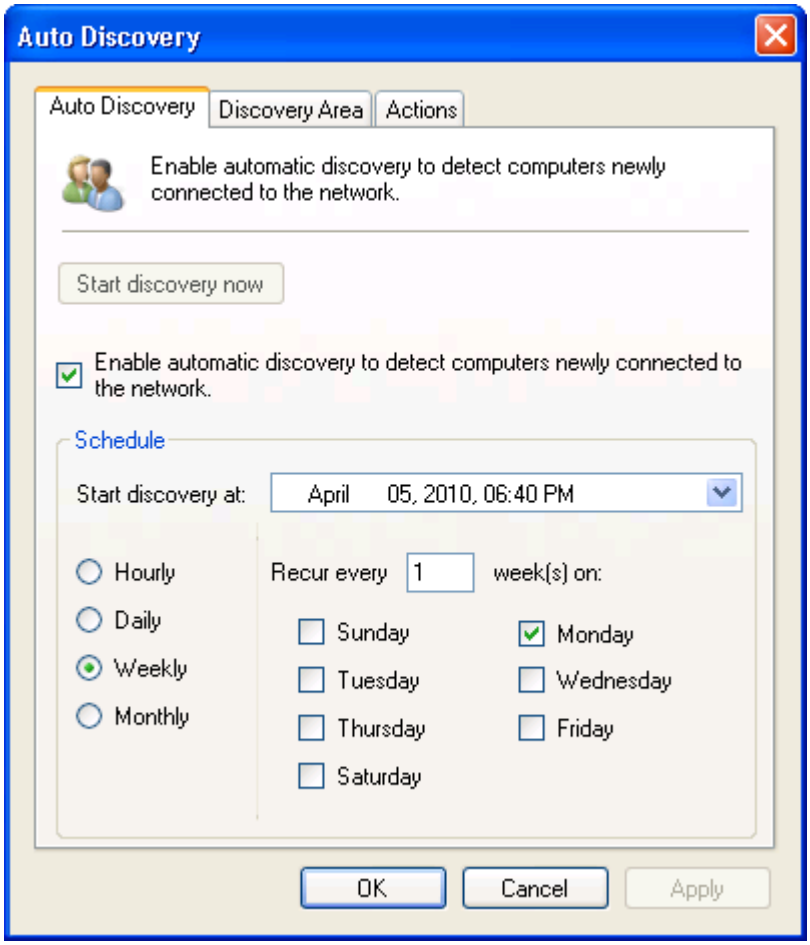


Screenshot 4 - GFI EndPointSecurity Quick Start wizard: Auto Discovery step

To configure the Auto Discovery feature:

1. Enable or disable the **Enable Auto Discovery** and **Install agents on discovered computers** checkboxes.

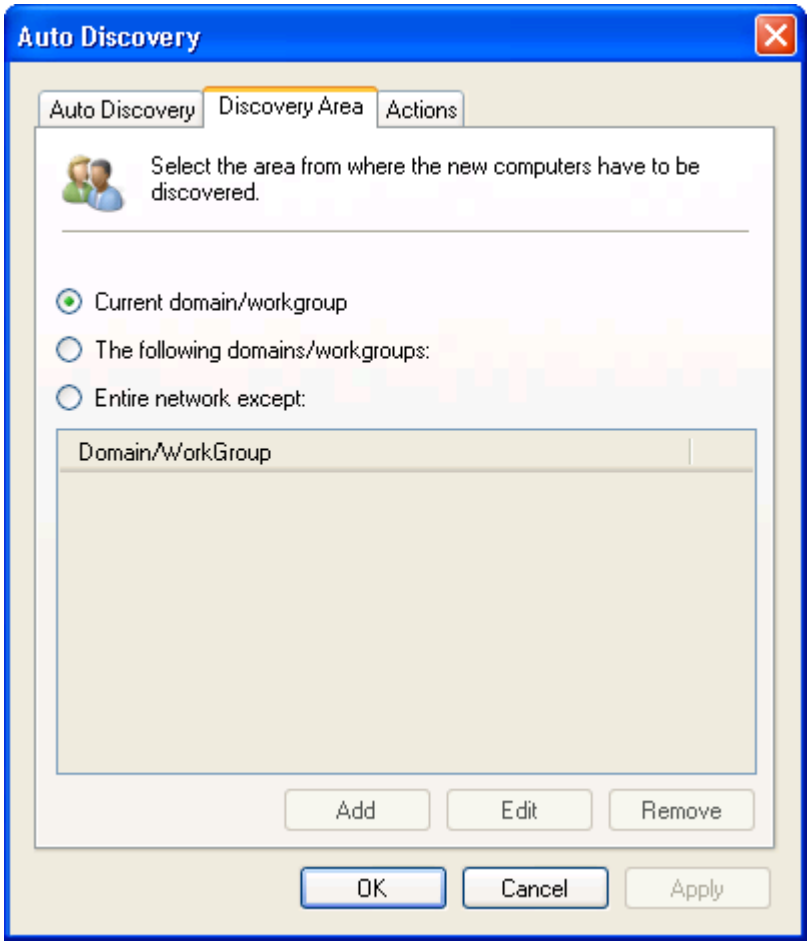
2. Click the **Auto discovery settings…** hyperlink to configure the auto discovery settings.



Screenshot 5 - Auto Discovery options

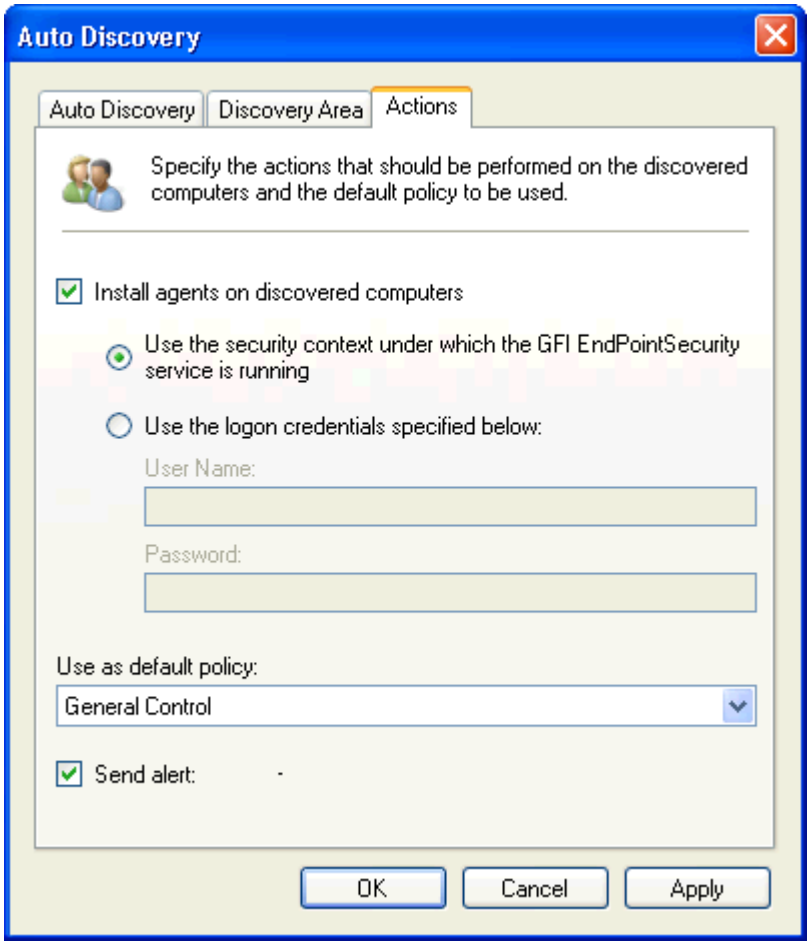
3. In the **Auto Discovery** dialog select the **Auto Discovery** tab and enable or disable the **Enable automatic discovery to detect computers newly connected to the network** checkbox.

4. In the **Schedule** section select the start date and set frequency of the searches from **Hourly**, **Daily**, **Weekly** or **Monthly**.



Screenshot 6 - Discovery Area options

5. Select the **Discovery Area** tab and select the area to be covered by the discovery feature. For **The following domains/workgroups** and **Entire network except** click **Add** and key in the **Domain/workgroup name**.



Screenshot 7 - Actions options

6. Select the **Actions** tab and enable or disable **Install agents on discovered computers.** If enabled, click **Yes** to confirm the enabling of the Automatic Protection feature. Select the logon credentials that GFI EndPointSecurity requires to physically log on to the target computer(s).

NOTE: By default, GFI EndPointSecurity is configured to use the logon credentials of the currently logged-on user account from which GFI EndPointSecurity application is running.

7. Select the protection policy from the drop-down list to be automatically applied to newly discovered target computers.

8. Enable or disable **Send alert**, and click **OK**.

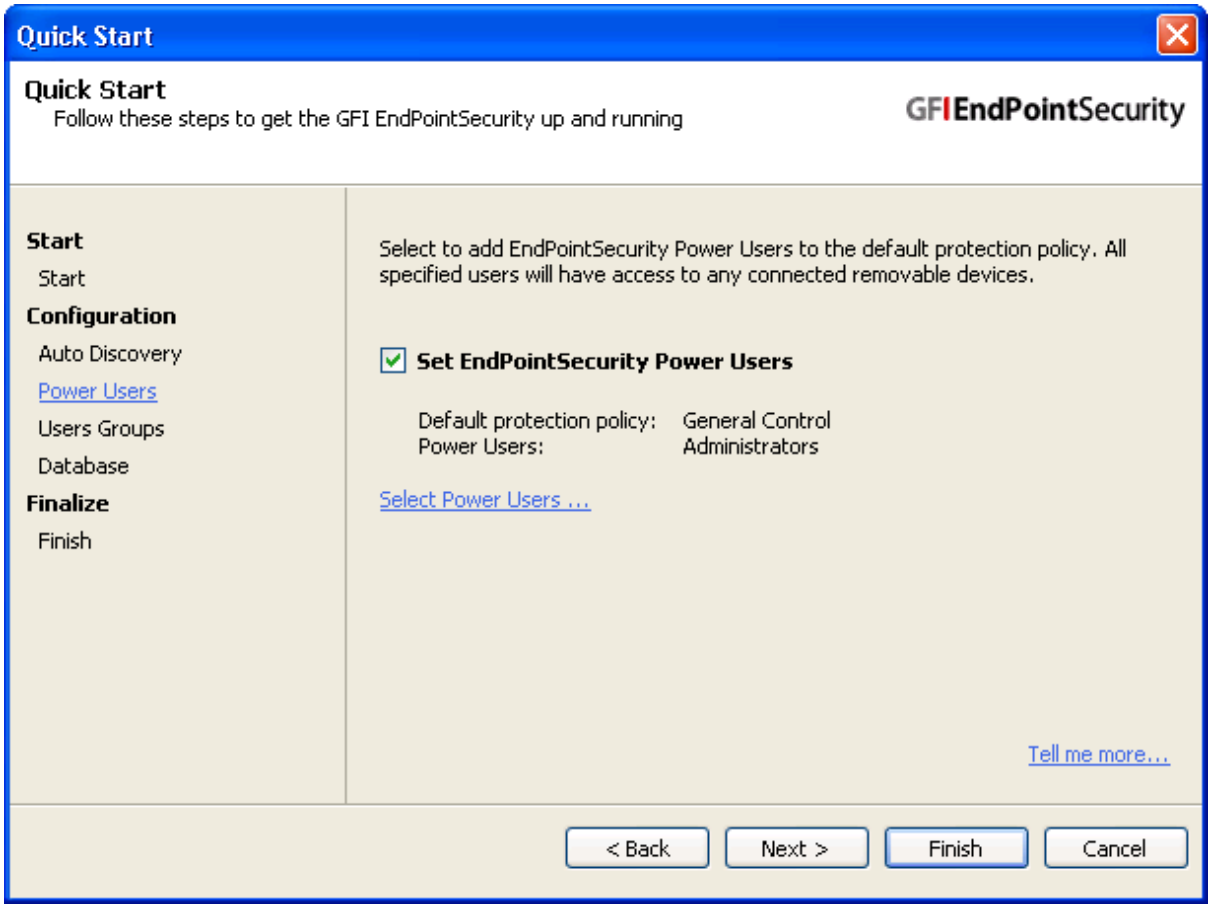
9. Click **Next**.

Step 2. Configuring power users

GFI EndPointSecurity provides you with the facility to specify users as power users. Power Users are automatically given full access to devices connected to any target computer covered by the protection policy. You can define sets of power users for any protection policy.

By default:

- the **Set EndPointSecurity Power Users** checkbox is enabled
- the system's **Administrators** group is set as a GFI EndPointSecurity Power User in the **General Control** protection policy (shipping default protection policy).

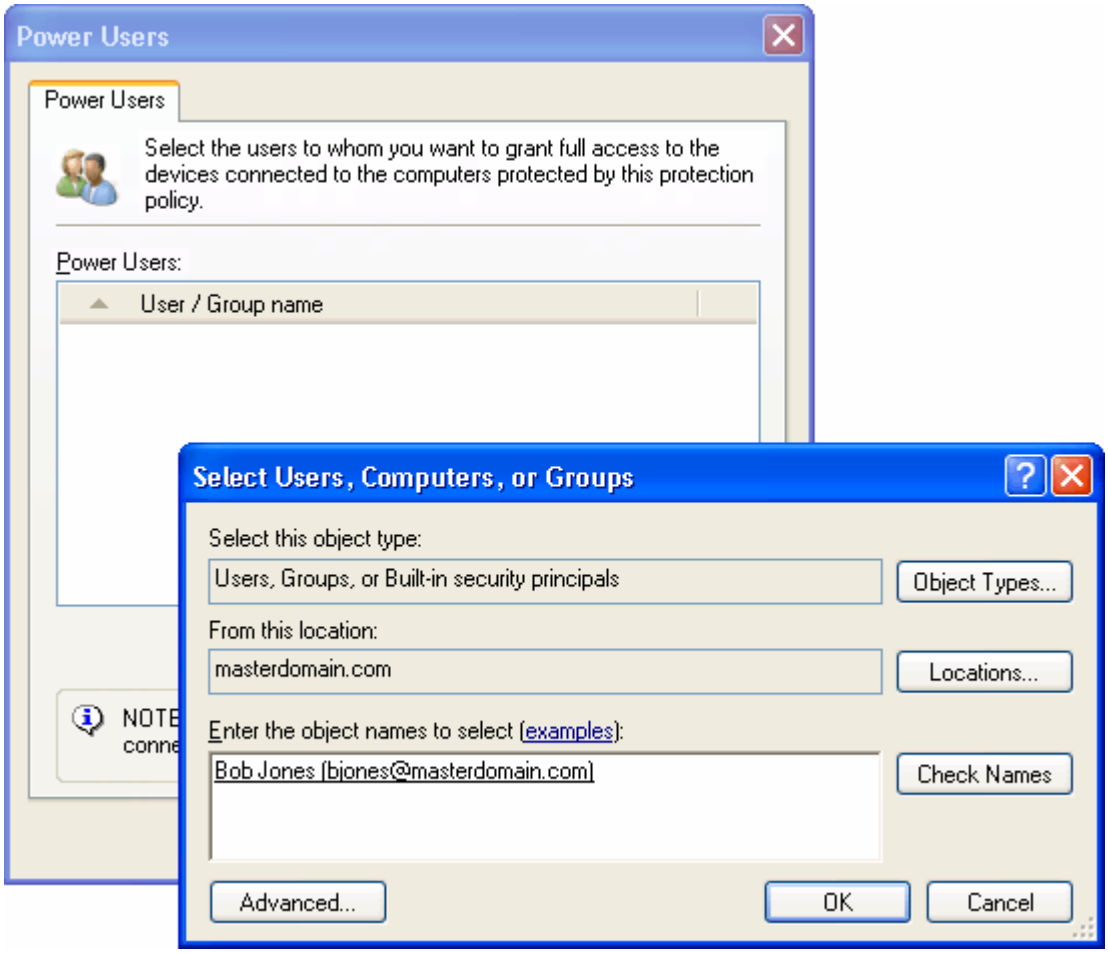


Screenshot 8 - GFI EndPointSecurity Quick Start wizard: Power Users step

To configure the Power Users feature:

1. Enable or disable the **Set EndPointSecurity Power Users** checkbox.

2. Click **Select Power Users…** to customize the list of power users.



Screenshot 9 - Power users options

3. In the **Power Users** dialog:

- Option 1: Click **Add…** to specify the user(s)/group(s) which will be set as power users for this protection policy, and click **OK**.
- Option 2: Highlight user(s)/group(s) and click **Remove** to demote from power users, and click **OK**.

4. Click **Next**.

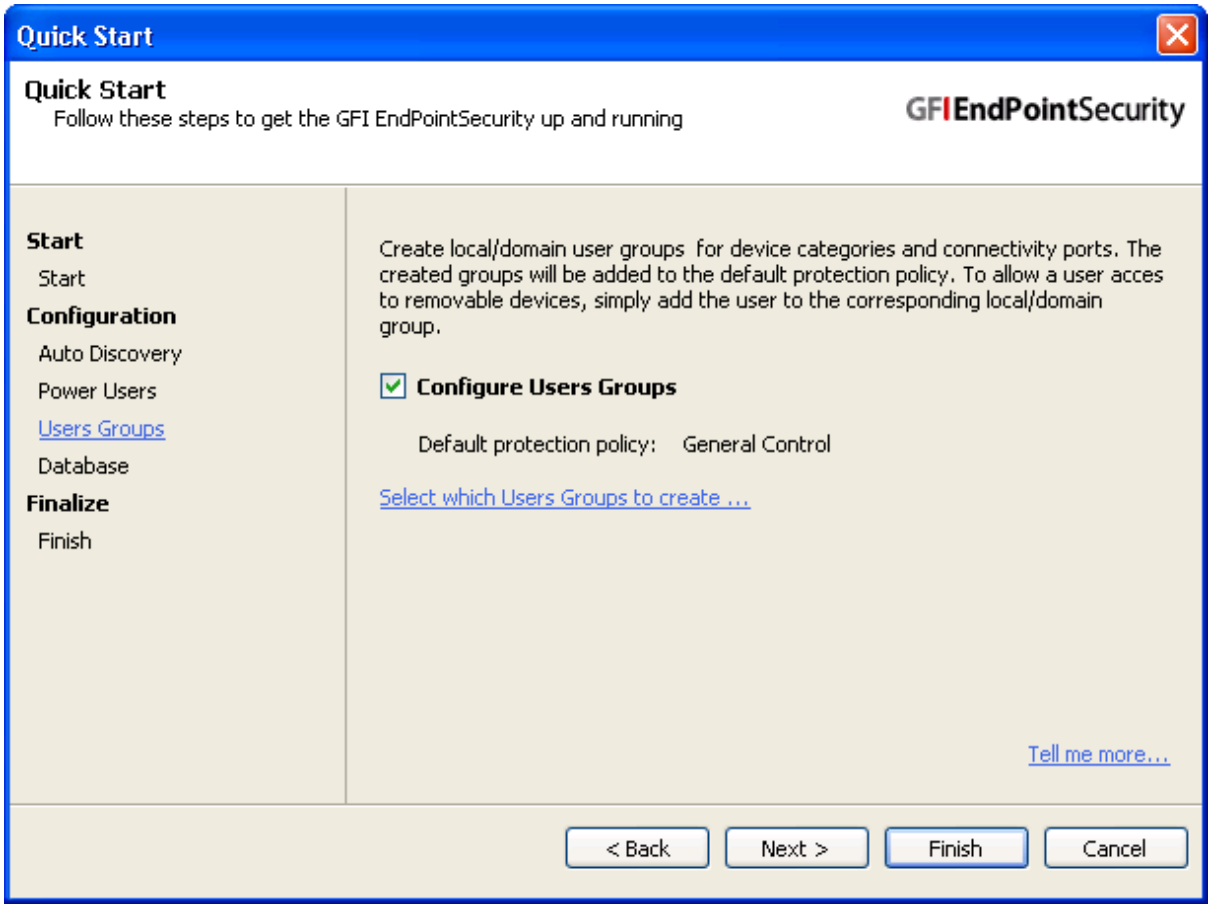
Step 3. Configuring users groups

GFI EndPointSecurity provides you with the facility to create user groups with specific rights for each device category and connectivity port selected by the administrator. In an environment where GFI EndPointSecurity is installed on a computer joined to an Active Directory domain, GFI EndPointSecurity creates Active Directory domain groups whereas in an environment where GFI EndPointSecurity is installed on a computer joined to a workgroup, GFI EndPointSecurity creates local system groups.

New users can be added directly to a specific user group from Active Directory Users and Computers (Active Directory domain environment) or Computer Management (workgroup environment), without having to specify user permissions within the relevant policies and then deploy the updates through GFI EndPointSecurity.

By default:

- the **Configure Users Groups** checkbox is enabled
- the created Active Directory domain groups/local system groups are added to the **General Control** protection policy (shipping default protection policy).

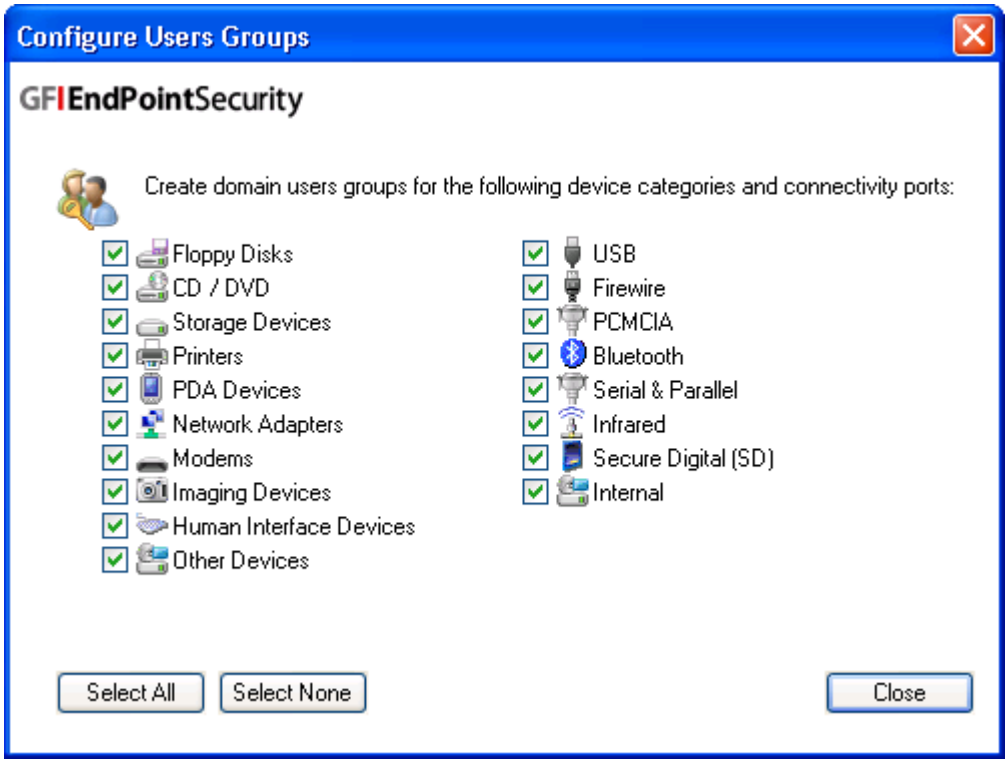


Screenshot 10 - GFI EndPointSecurity Quick Start wizard: Users Groups step

To configure the Users Groups feature:

1. Enable or disable the **Configure Users Groups** checkbox.

2. Click the **Select which Users Groups to create…** hyperlink to configure which devices and ports will be controlled by a specific protection policy.



Screenshot 11 - Users Groups options

3. In the **Configure Users Groups** dialog, enable or disable the required device categories and connectivity ports which will be controlled by the protection policy and click **Close**.

4. Click **Next**.

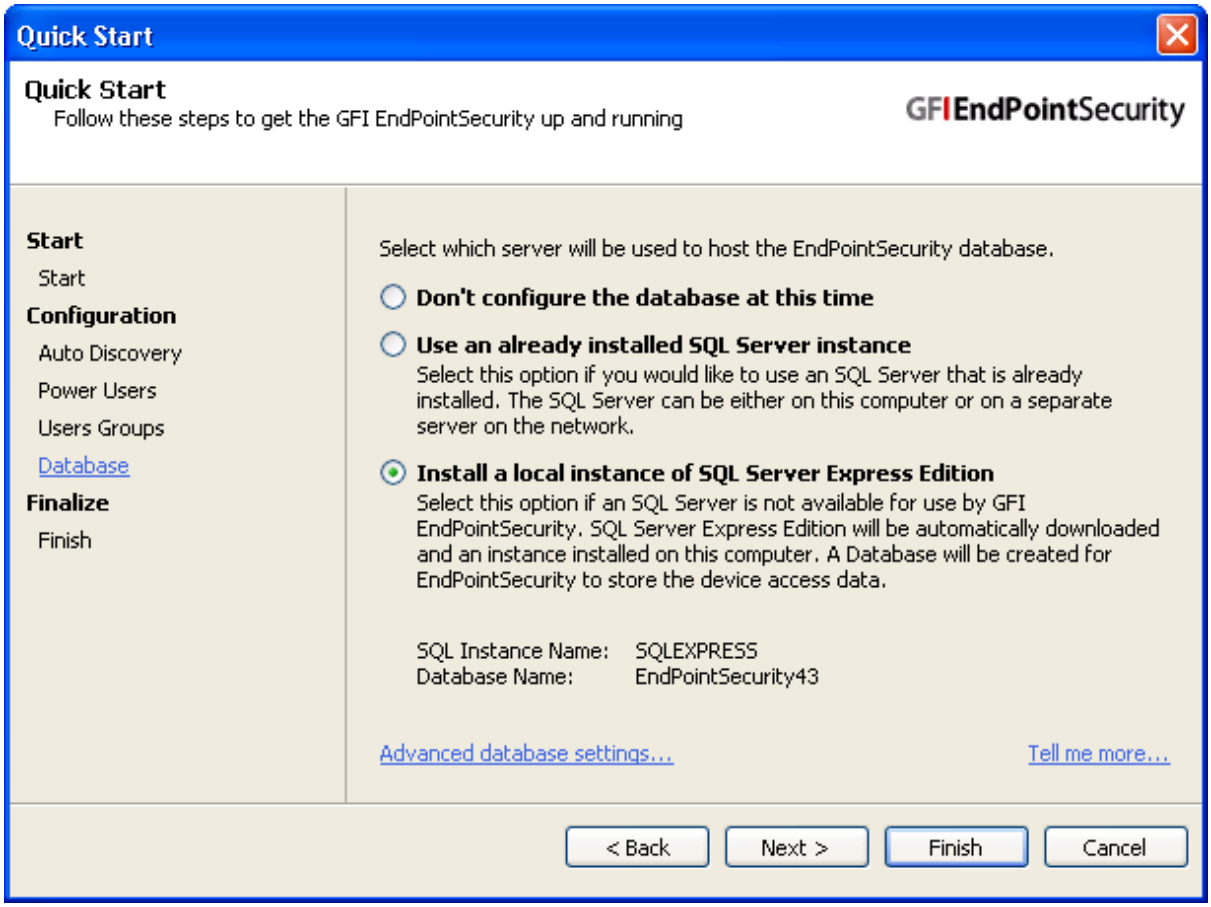
Step 4. Configuring database backend

GFI EndPointSecurity provides you with the facility to keep an audit trail of all events generated by GFI EndPointSecurity agents deployed on target computers. In this step, you can choose:

- Not to configure a database
- To download and install an instance of Microsoft SQL Server Express Edition, as well as to automatically create a database for GFI EndPointSecurity upon completion of the database installation.
- To connect to an available Microsoft SQL Server instance and then you can either connect to an existing database or else create a new one.

By default:

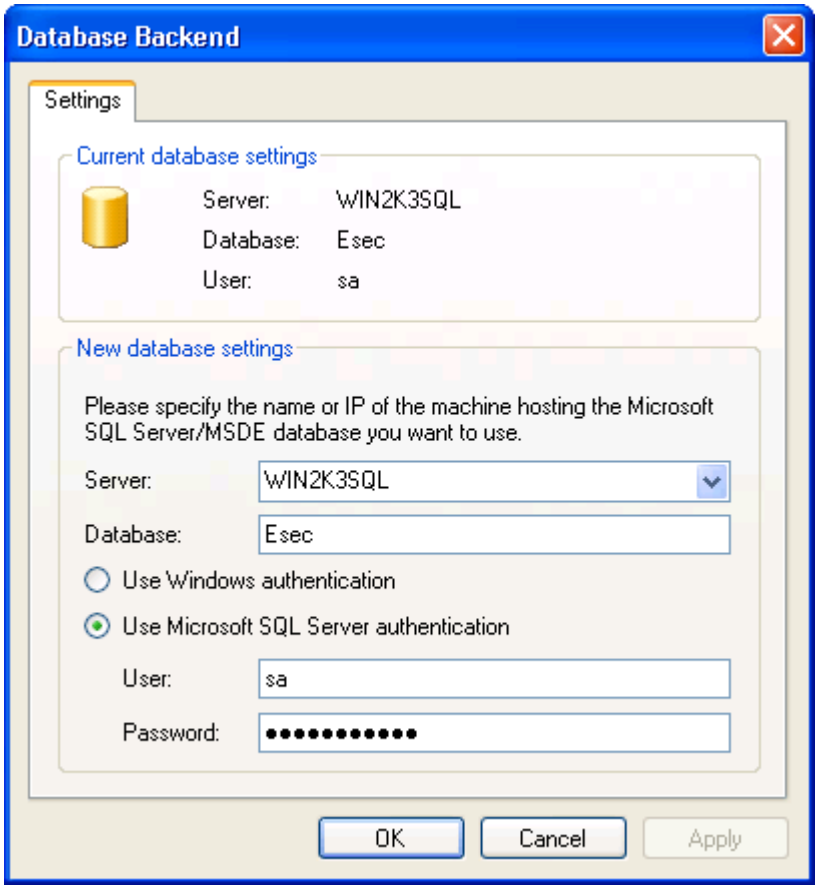
- GFI EndPointSecurity will pre-select the best option, based on your current environment setup, to better guide you in your selection.



Screenshot 12 - GFI EndPointSecurity Quick Start wizard: Database step

To configure the Database feature:

1. Select the server or instance which will host the GFI EndPointSecurity database. For **Use an already installed SQL Server instance** and **Install a local instance of SQL Server Express Edition** click the **Advanced database settings…** hyperlink.



Screenshot 13 - Database setup options

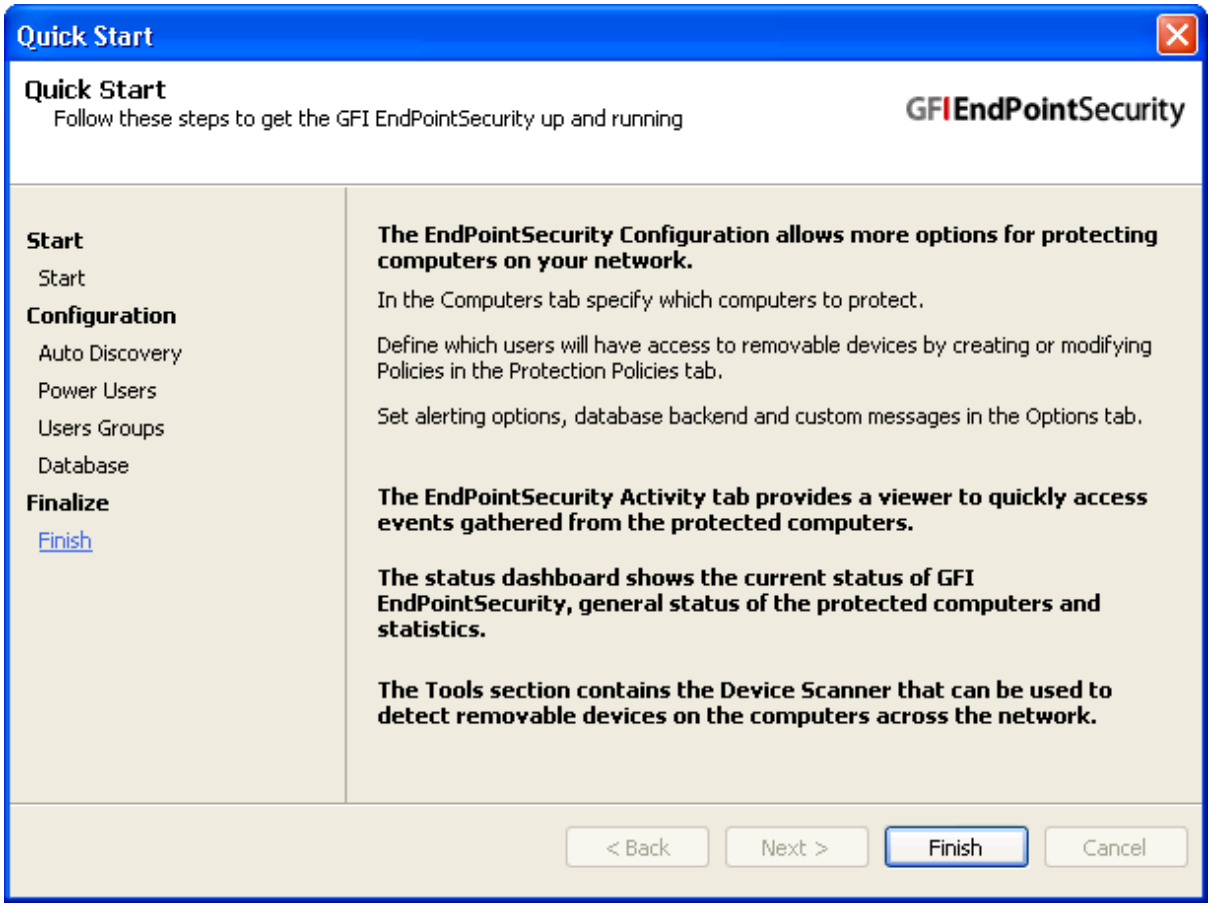
2. In the **Database Backend** dialog select or key in the server name/IP address of an available database server or of a new SQL instance from the **Server** dropdown list.

3. Key in the database name in the **Database** field.

4. Select the authentication method to be used when connecting to the database backend server, and click **OK**.

NOTE: If **Use Microsoft SQL Server authentication** is selected, key in the login username and password of the database backend server.

5. Click **Next** and wait for the wizard setup to complete.



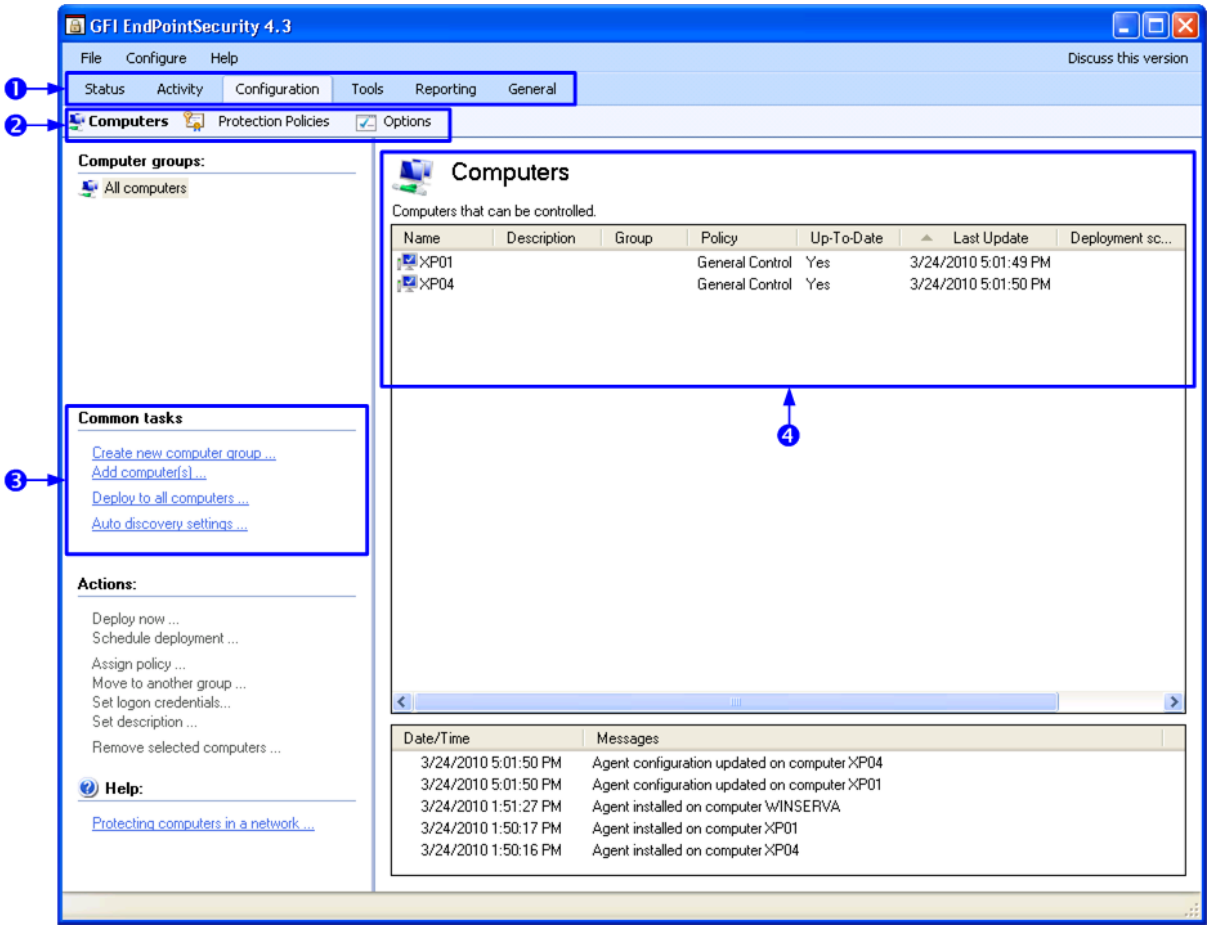
Screenshot 14 - GFI EndPointSecurity Quick Start wizard: Finish step

6. Upon wizard completion, review the guidelines page.

7. Click **Finish** to complete the wizard.

4.3 Navigating the GFI EndPointSecurity management console

GFI EndPointSecurity management console provides you with all the administrative functionality to monitor and manage device access usage.



Screenshot 15 - GFI EndPointSecurity: management console

1 **Tabs** - Use this feature to navigate between the different tabs within GFI EndPointSecurity management console. The available tabs are:

- **Status** - To monitor the status of GFI EndPointSecurity and statistical information on device access.
- **Activity** - To monitor devices used on the network.
- **Configuration** To access and configure the default protection policies.
- **Tools** - To scan target computers and discover connected devices
- **Reporting** - To see information regarding the GFI EndPointSecurity ReportPack.
- **General** - To check for GFI EndPointSecurity updates, as well as version and licensing details.

2 **Sub-tabs** - Use this feature to access more information and settings within GFI EndPointSecurity management console.

3 **Left pane** - Use this pane to access the configuration options provided in GFI EndPointSecurity. The configuration options are grouped into several sections, including **Common Tasks**, **Actions** and **Help** sections. Available only for some tabs.

4 **Right pane** - Use this pane to configure the configuration options selected from the left pane. Available only for some tabs.

5 Testing GFI EndPointSecurity

5.1 Introduction

Once GFI EndPointSecurity is installed and the Quick Start wizard is completed, test your installation to ensure that GFI EndPointSecurity is working correctly. Follow the instructions in this section to verify the correctness of both the GFI EndPointSecurity installation as well as the operations of the shipping default protection policy.

5.2 Verifying operations of the shipping default protection policy

The following test pre-conditions and settings are required ONLY for the purpose of this test. For detailed information about how to configure and deploy device access protection policies and about the options provided by GFI EndPointSecurity, refer to the GFI EndPointSecurity - Administration and Configuration Manual.

5.2.1 Test pre-conditions

Device setup

For the following test you require:

- a CD/DVD drive connected to the local computer
- a CD/DVD disc containing accessible contents (preferably a disc the contents of which were accessible prior to the installation of GFI EndPointSecurity).

NOTE: Other devices and media may be used, such as Floppy Disks or pen drives.

User accounts

For this test ensure the availability of two user accounts on the local computer (same computer where GFI EndPointSecurity application is installed):

- one with no administrative privileges
- one with administrative privileges.

Configuration settings

The configuration of the Quick Start wizard allows you to fine tune GFI EndPointSecurity to suit your company's needs which may not match the pre-test settings required by this test. As a result, some GFI EndPointSecurity configuration settings need to be set as indicated below for this test to succeed:

- the local computer is listed in the **Status ► Agents** view

  NOTE: If the local computer is not listed, then manually include it within the computers list. For more information, refer to the GFI EndPointSecurity - Administration and Configuration Manual.

- the shipping default protection policy is deployed on the local computer and is up-to-date. To verify check in the **Status ► Agents** view that:
  - the protection policy is set to **General Control**
  - the deployment is **Up-to-date**
  - the local computer is **Online**

  NOTE: If the deployment of the agent on to the local computer is not up-to-date, then manually deploy the agent on to it. For more information, refer to the GFI EndPointSecurity - Administration and Configuration Manual.

- the user account with no administrative privileges is not set as a power user in the **General Control** protection policy (shipping default protection policy).

  NOTE: If the user account is set as a power user, then manually remove it from the power users group of the **General Control** protection policy (shipping default protection policy). For more information, refer to the GFI EndPointSecurity - Administration and Configuration Manual.

5.2.2 Test case

Accessing a CD/DVD disc

Upon compliance with the previously outlined test pre-conditions, non-administrative users are no longer allowed access to any devices or ports connected to the local computer.

To verify that both the device and media are inaccessible to the non-administrative user:

1. Log in to the local computer as the user with no administrative privileges.

2. Insert the CD/DVD disc in the CD/DVD drive.

3. From **Windows Explorer** locate the CD/DVD drive and confirm that you are unable to view and open the contents stored on the CD/DVD disc.

Assign permissions to user with no administrative privileges

To assign CD/DVD device access permissions to the user with no administrative privileges:

1. Log in to the local computer as the user with administrative privileges.

2. Launch GFI EndPointSecurity.

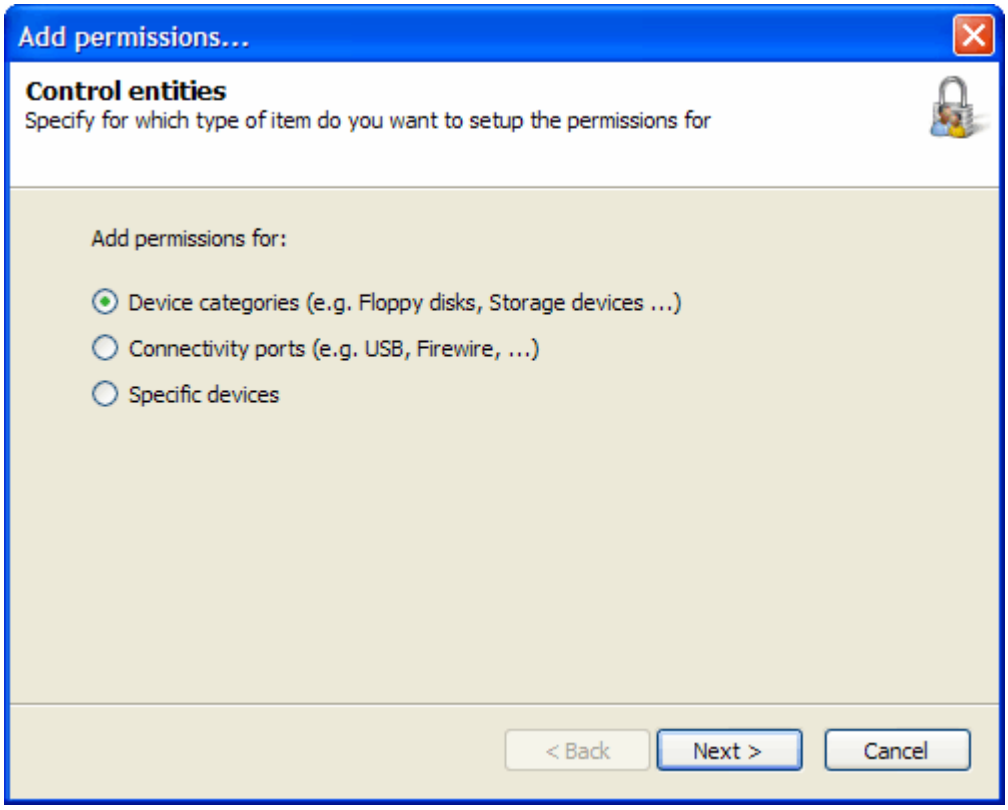
3. Click on the **Configuration** tab.

4. Click on the **Protection Policies** sub-tab.

5. From the left pane, select the **General Control** protection policy.

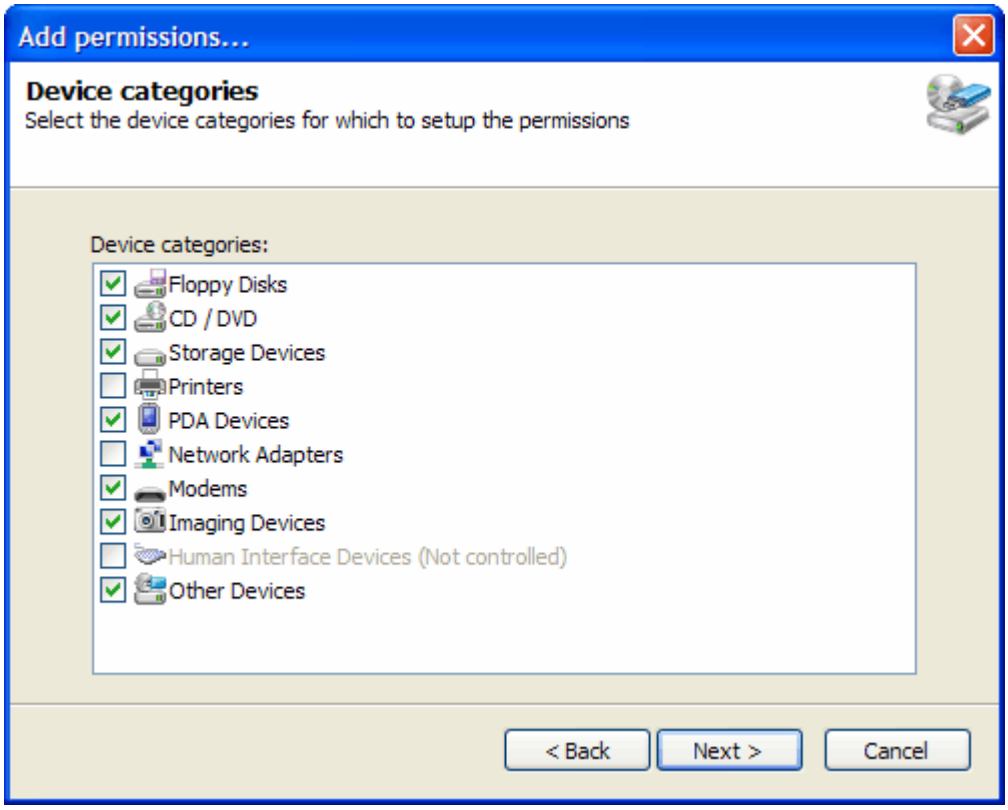
6. Click on the **Security** sub-node.

7. From the left pane, click the **Add permission(s)…** hyperlink in the **Common tasks** section.



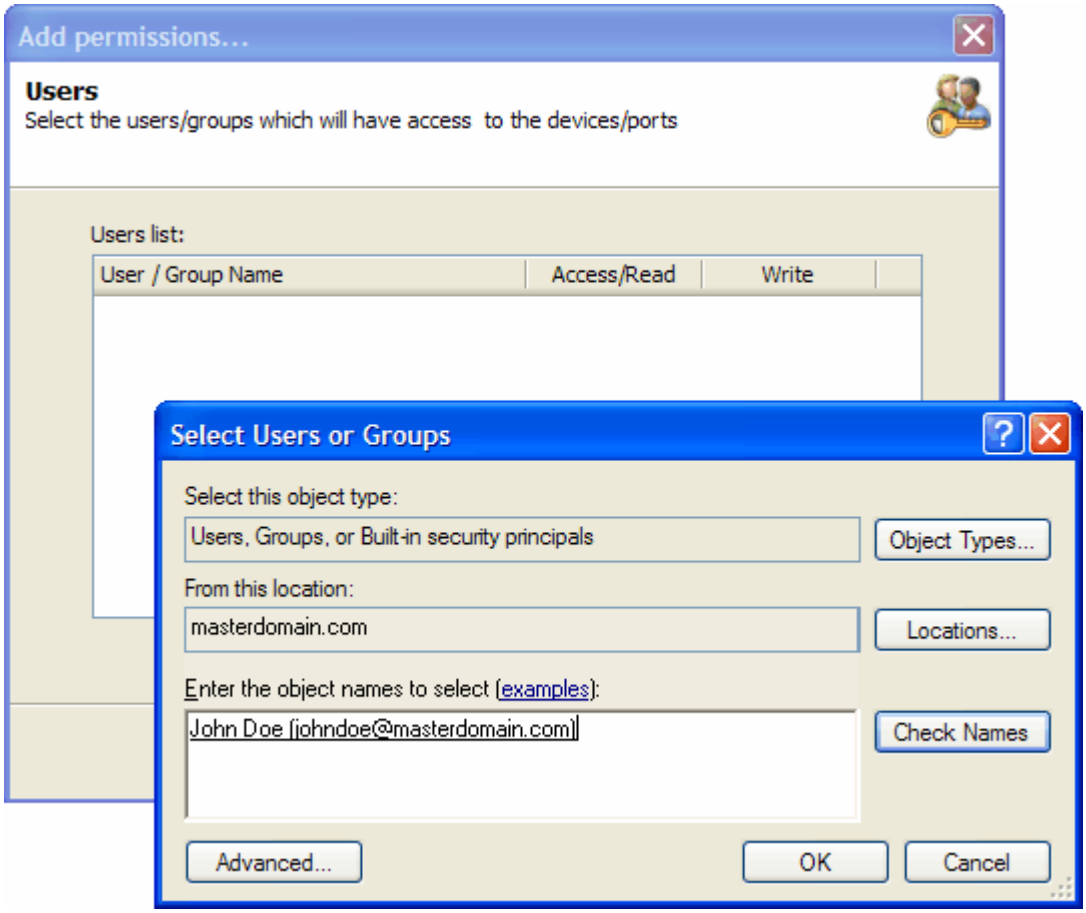
Screenshot 16 – Selecting control entities

8. In the **Add permissions...** dialog select the **Device categories** option and click **Next** to continue.



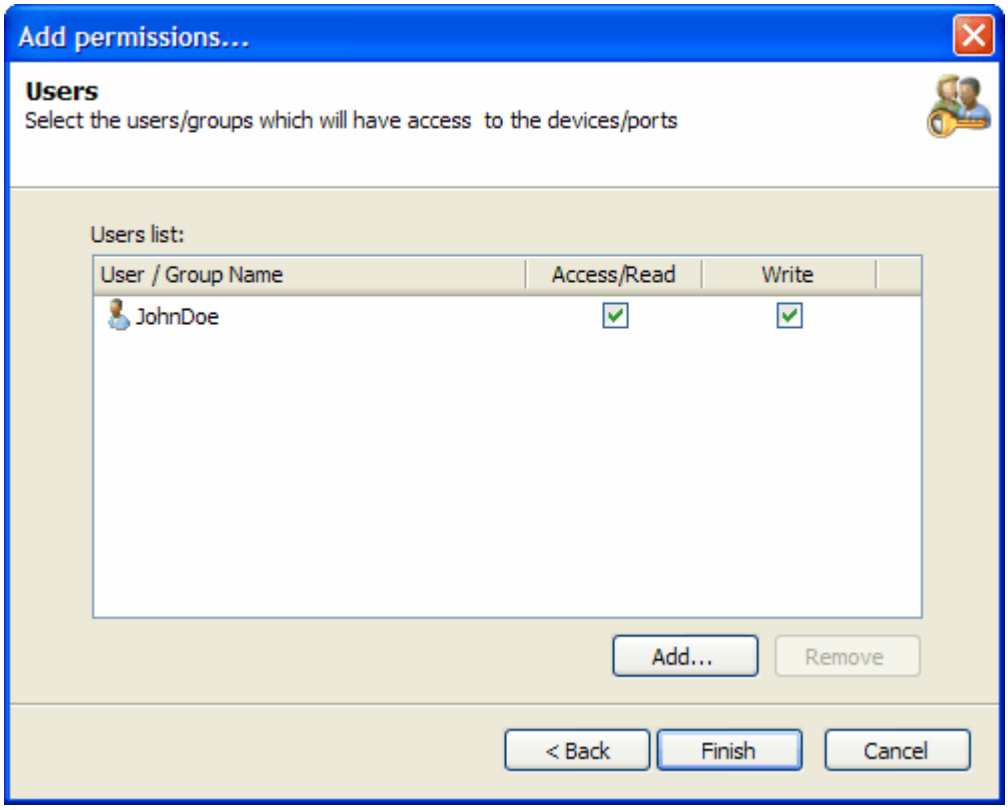
Screenshot 17 - Selecting device categories to assign permissions

9. Enable the **CD/DVD** device category, and click **Next**.



Screenshot 18 - Adding users or groups

10. Click **Add…** and specify the user with no administrative privileges, to have access to the **CD/DVD** device category specified in this protection policy, and click **OK**.



Screenshot 19 - Selecting permission types per user or group

11. Enable the **Access/Read** and **Write** permissions and click **Finish**.

To deploy the protection policy updates on to the local computer:

1. From the right pane, click on the top warning message to deploy the protection policy updates. The view should automatically change to **Status ► Deployment**.

2. From the **Deployment History** area, confirm the successful completion of the update onto the local computer.

Re-accessing a CD/DVD disc

Upon the assignment of user permissions, the specified user with no administrative privileges should now be allowed to access CD/DVD discs through CD/DVD drives connected to the local computer.

To verify that both the device and media are now accessible to the non-administrative user:

1. Log in to the local computer as the user with no administrative privileges.

2. Insert the same CD/DVD disc in the CD/DVD drive.

3. From the **Windows Explorer** locate the CD/DVD drive and confirm that you are now able to view and open the contents stored on the CD/DVD disc.

5.2.3 Reverting settings

To revert any GFI EndPointSecurity configuration settings back to the pre-test scenario, do the following for the user with no administrative privileges:

1. Remove the user account from the local computer, if it was created only for this test and is no longer required.

2. Manually include the user in the power users list, if it was set as a power user prior to this test. For more information, refer to the GFI EndPointSecurity - Administration and Configuration Manual.

3. Delete the CD/DVD device access permissions to the user, if it was not assigned CD/DVD device access permissions prior to this test. For more information, refer to the GFI EndPointSecurity - Administration and Configuration Manual.

6 Miscellaneous

6.1 Introduction

The miscellaneous chapter gathers all the other information that falls outside the initial configuration of GFI EndPointSecurity.

6.2 Entering your license key after installation

After installing GFI EndPointSecurity you can enter your license key without re-installing or re-configuring the application.

To enter your license key:

1. Click on the **General** tab.

2. From the left pane select **Licensing**.

Screenshot 20 - Editing license key

3. From the right pane click **Edit …**

4. In the **License Key** text box, key in the license key provided by GFI Software Ltd.

5. Click **OK** to apply the license key.

6.3 Checking for newer GFI EndPointSecurity versions

GFI Software Ltd. releases product updates which can be manually or automatically downloaded from the GFI website.

To check if a newer version of GFI EndPointSecurity is available for download:

1. Click on the **General** tab.

2. From the left pane, select **Version Information**.

3. From the right pane click **Check for newer version** hyperlink to manually check if a newer version of GFI EndPointSecurity is available. Alternatively, enable the **Check for**

newer version at startup checkbox to automatically check if a newer version of GFI EndPointSecurity is available for download every time GFI EndPointSecurity is launched.

7 Troubleshooting

7.1 Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- The manual - most issues can be solved by reading this manual.
- GFI Knowledge Base articles
- Web forum
- Contacting the GFI Technical Support

7.2 Common Issues

ISSUE ENCOUNTERED	SOLUTION
Errors are displayed within the **Status ► Deployment ► Deployment History** section upon deployment of GFI EndPointSecurity agents from the GFI EndPointSecurity management console.	For more information about error messages, possible causes and possible solutions, refer to the Appendix 1 - Deployment error messages chapter in this manual.

7.3 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 technical support questions and patches. To access the Knowledge Base, visit http://kbase.gfi.com/.

7.4 Web Forum

User to user technical support is available via the web forum. The forum can be found at: http://forums.gfi.com/.

7.5 Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online**: Fill out the support request form from: http://support.gfi.com/supportrequestform.asp.
- **Phone**: To obtain the correct technical support phone number for your region please visit: http://www.gfi.com/company/contact.htm.

NOTE: Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at: http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

7.6 Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit: http://www.gfi.com/pages/productmailing.htm.

7.7 Documentation

If this manual does not satisfy your expectations, or if you think that this documentation can be improved in any way, let us know via email on: documentation@gfi.com.

8 Glossary

Access permissions	A set of permissions (access, read and write) that are assigned to users and groups per device category, connectivity port or a specific device.
Active Directory	A technology that provides a variety of network services, including LDAP-like directory services.
Alert recipient	A GFI EndPointSecurity profile account to hold the contact details of users intended to receive e-mail alerts, network messages and SMS messages.
Alerts	A set of notifications (e-mail alerts, network messages or SMS messages) that are sent to alert recipients when particular events are generated.
Alerts administrator account	An alert recipient account that is automatically created by GFI EndPointSecurity upon installation.
Automatic discovery	A GFI EndPointSecurity feature to search and discover computers that were newly connected to the network at configured scheduled times.
BitLocker To Go	A Microsoft Windows 7 feature to protect and encrypt data on removable devices.
Connectivity port	An interface between computers and devices.
Create Protection Policy wizard	A wizard to guide you in the creation and configuration of new protection policies. Configuration settings include the selection of device categories and ports to be controlled and whether to block or allow all access to them. This wizard also allows the configuration of file-type based filters, encryption permissions as well as logging and alerting options.
Database backend	A database used by GFI EndPointSecurity to keep an audit trail of all events generated by GFI EndPointSecurity agents deployed on target computers.
Deployment error messages	Errors that can be encountered upon deployment of GFI EndPointSecurity agents from the GFI EndPointSecurity management console.
Device blacklist	A list of specific devices whose usage is blocked when accessed from all the target computers covered by the protection policy.
Device category	A group of peripherals organized in a category.
Device scan	A GFI EndPointSecurity feature to search for all devices that are or have been connected to the scanned target computers.
Device whitelist	A list of specific devices whose usage is allowed when accessed from all the target computers covered by the protection policy.
Digest report	A summary report giving an account of the activity statistics as detected by GFI EndPointSecurity.
Event logging	A feature to record events related to attempts made to access devices and connection ports on target computers and service operations.
File-type filters	A set of restrictions that are assigned to users and groups per file-type. Filtering is based on file extension checks and real file type signature checks.
GFI EndPointSecurity agent	A client-side service responsible for the implementation/enforcement of the protection policies on the target computer(s).

GFI EndPointSecurity application	A server-side security application that aids in maintaining data integrity by preventing unauthorized access and transfer of content to and from devices and connection ports.
GFI EndPointSecurity management console	The user interface of the GFI EndPointSecurity server-side application.
GFI EndPointSecurity Temporary Access tool	A tool which is available on the target computers. It is used by the user to generate a request code and later to enter the unlock code in order to activate the temporary access once it is granted by the administrator. Upon activation, the user will have access to devices and connection ports (when such access is normally blocked) on his protected target computer for the specified duration and time window.
Global permissions	A Create Protection Policy wizard step that prompts the user to either block or else to allow access to all devices falling in a category or which are connected to a port of the target computers covered by the protection policy.
GPO	*See* Group Policy Objects.
Group Policy Objects	An Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.
Human Interface Devices	A specification that is part of the universal serial bus (USB) standard for a class of peripheral devices. These devices, such as a mice, keyboards, and joysticks, enable users to input data or to interact directly with the computer.
MSI file	A file generated by GFI EndPointSecurity for later deployment using GPO or other deployment options. It can be generated for any protection policy and contains all the relevant configured security settings, including installation settings for unprotected target computers.
Power user	A power users is automatically given full access to devices connected to any target computer covered by the protection policy.
Protection policy	A set of device access and connectivity port permissions that can be configured to suit your company's device access security policies.
Quick Start wizard	A wizard to guide you in the configuration of GFI EndPointSecurity with custom settings. It is launched upon the initial launch of GFI EndPointSecurity management console and is intended for first time use.
Security encryption	A set of restrictions configured to either block or else to allow users/groups to access specific file-types stored on devices that are encrypted with BitLocker To Go. These restrictions are applied when the encrypted devices are connected to the target computers covered by the protection policy.
Target computer	A computer that is protected by a GFI EndPointSecurity protection policy.
Temporary access	A period of time during which users are allowed to access devices and connection ports (when such access is normally blocked) on protected target computers, for a specified duration and time window.
User message	A message that is displayed by GFI EndPointSecurity agents on target computers, when devices are accessed.

9 Appendix 1 - Deployment error messages

9.1 Introduction

This section provides a list of errors that can be encountered when deploying agents or protection policies, possible causes for these errors and possible solutions. The deployment status can be accessed from the GFI EndPointSecurity management console by navigating to **Status ► Deployment ► Deployment History**.

9.2 Deployment error messages

NOTE: In the following table, some error messages are in the format "GFI EndPointSecurity error (system error)". The errors within the parenthesis are reported by the system and may vary according to the cause of the error.

MESSAGE	POSSIBLE CAUSES	POSSIBLE SOLUTIONS
The computer is offline.	GFI EndPointSecurity management console pings the target computer at deployment to determine whether it is online, and if not this message is displayed.	If a target computer is offline, the deployment of the relevant policy is rescheduled for an hour later. GFI EndPointSecurity keeps trying to deploy that policy every hour, until the target computer is back online. Ensure that the target computer is switched on and connected to the network.
Failed to connect to the remote registry. (error)	GFI EndPointSecurity was not able to extract data from the registry of the target computer.	Ensure that your firewall settings enable communication between the target computers and the GFI EndPointSecurity server.
Failed to gather required information. (error)	GFI EndPointSecurity was not able to extract version related data from the target computer (Operating System version and GFI EndPointSecurity agent version).	For more details about the cause of the error and a possible solution, refer to the system error message within the parenthesis.
Failed to build the required installation files. (error)	GFI EndPointSecurity was not able to add the necessary configuration files within the deployment file (.msi installation file) of the GFI EndPointSecurity agent. This error occurs before the deployment file is copied onto the target computer.	For more details about the cause of the error and a possible solution, refer to the system error message within the parenthesis.

MESSAGE	POSSIBLE CAUSES	POSSIBLE SOLUTIONS
Failed to copy the files to the remote computer. (error)	GFI EndPointSecurity was not able to copy the deployment file (.msi installation file) onto the target computer. A possible cause can be that, the administrative share (C$) that GFI EndPointSecurity is using to connect to the target computer, is disabled.	For more details about the cause of the error and a possible solution, refer to the system error message within the parenthesis. For further information about network connectivity and security permissions, refer to: http://kbase.gfi.com/showarticle.asp?id=KBID003754
Timeout	Agent deployment onto the target computer is either taking too long to complete or else is blocked..	Please try to deploy the GFI EndPointSecurity agent again.
Failed to install the deployment service. (error)	The GFI EndPointSecurity agent was not able to be installed or uninstalled by the service running on the target computer.	For more details about the cause of the error and a possible solution, refer to the system error message within the parenthesis.
Installation failed.	Installation of the GFI EndPointSecurity agent is complete, but is not marked as installed within the registry. The version and build numbers of the GFI EndPointSecurity agent are not the same as those of the GFI EndPointSecurity management console.	For more details about the cause of the error and a possible solution, refer to the agent installation log files on the target computer at: %windir%\EndPointSecurity.
Un-installation failed.	Uninstallation of the GFI EndPointSecurity agent is complete, but is not marked as uninstalled within the registry.	For more details about the cause of the error and a possible solution, refer to the agent installation log files on the target computer at: %windir%\EndPointSecurity.
The operation failed due to an unknown exception.	GFI EndPointSecurity has encountered an unexpected error.	Please use the Troubleshooter Wizard to contact the GFI Technical Support team. To open the Troubleshooter Wizard navigate to **Start ► Programs ► GFI EndPointSecurity 4.3 ► GFI EndPointSecurity 4.3 Troubleshooter**.

Index

U

V

W