Getting Started Guide

GFI EndPointSecurity™

Learn how to deploy GFI EndPointSecurity

GFI®

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or 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 warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

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

Document Version: 1.2.0

Last updated (month/day/year): 02/22/2016

Contents

1 Introduction

The proliferation of consumer devices such as iPods, USB devices and smartphones has dramatically increased the risk of deliberate and unintentional data leaks and other malicious activity: It is very simple for an employee to copy large amounts of sensitive data onto an iPod or USB stick, or to introduce malicious and illegal software onto your network through these devices. GFI EndPointSecurity quickly and easily helps you combat these critical threats without needing to lock down all ports.

To control access, GFI EndPointSecurity automatically installs a tamper-proof, hidden agent on the machines in your network. This agent delivers protection even against users with admin rights, enabling IT admins to remain in control no matter what.

Topics in this chapter

1.1 Key Features

GFI EndPointSecurity offers the following main features:

GFI EndPointSecurity 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 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.

GFI EndPointSecurity features	
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.
Device encryption	For maximum security, GFI EndPointSecurity can be configured to encrypt storage devices using AES 256 encryption. Encryption can be enforced on specific computers running agents over the network.
Data leakage risk assessment	The dashboard enables users to see potential data leakage risk for each endpoint. Use the provided tips and perform suggested actions to reduce risks levels.
Content awareness	The content awareness feature enables users to look into files entering the endpoints via removable Devices. Content is identified based on predefined (or custom) regular expressions and dictionary files. By default the feature looks for secure confidential details such as passwords and credit card numbers.

1.2 How GFI EndPointSecurity works

GFI EndPointSecurity is the 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 (example: Flash and Memory card readers, pen drives)
- Firewire ports (example: digital cameras, Firewire card readers)
- Wireless data connections (example: Bluetooth and Infrared dongles)

- Floppy disk drives (internal and external)
- Optical drives (example: 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:

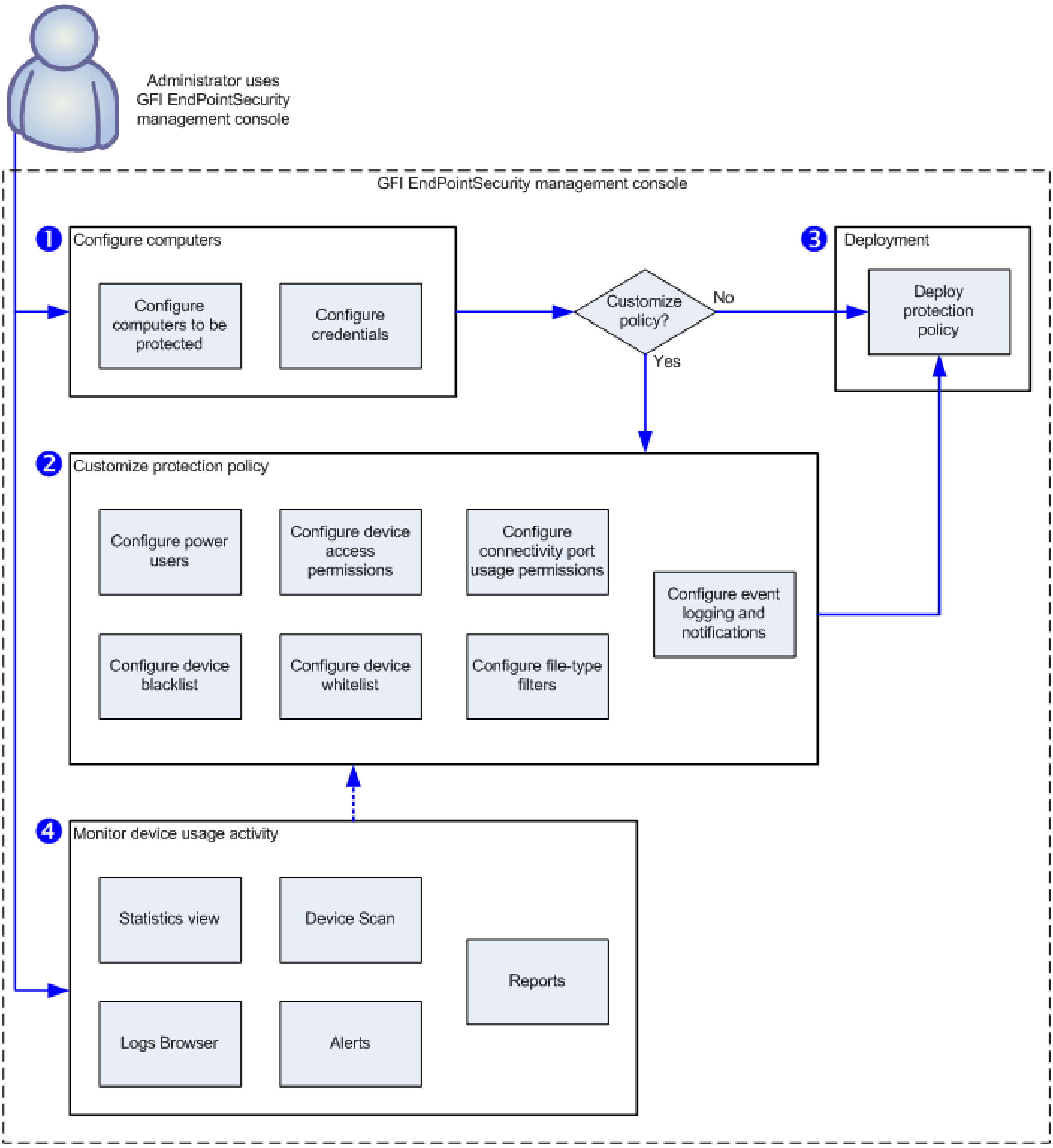
- Devices (example: CD/DVD drives, PDAs)
- Local or Active Directory users/user groups.

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).

Devices are controlled through an agent that is automatically installed as a service on the machines in your network. This agent delivers protection even against users with admin rights, enabling IT admins to remain in control no matter what. For more information, refer to GFI EndPointSecurity Components (page 9).

1.3 How GFI EndPointSecurity works - Deployment and Monitoring

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


Administrator uses GFI EndPointSecurity management console
GFI EndPointSecurity management console
1
Configure computers
Configure computers to be protected
Configure credentials
Customize policy?
No
Yes
3
Deployment
Deploy protection policy
2
Customize protection policy
Configure power users
Configure device access permissions
Configure connectivity port usage permissions
Configure event logging and notifications
Configure device blacklist
Configure device whitelist
Configure file-type filters
4
Monitor device usage activity
Statistics view
Device Scan
Reports
Logs Browser
Alerts

Screenshot 1: Protection policy - Deployment and Monitoring

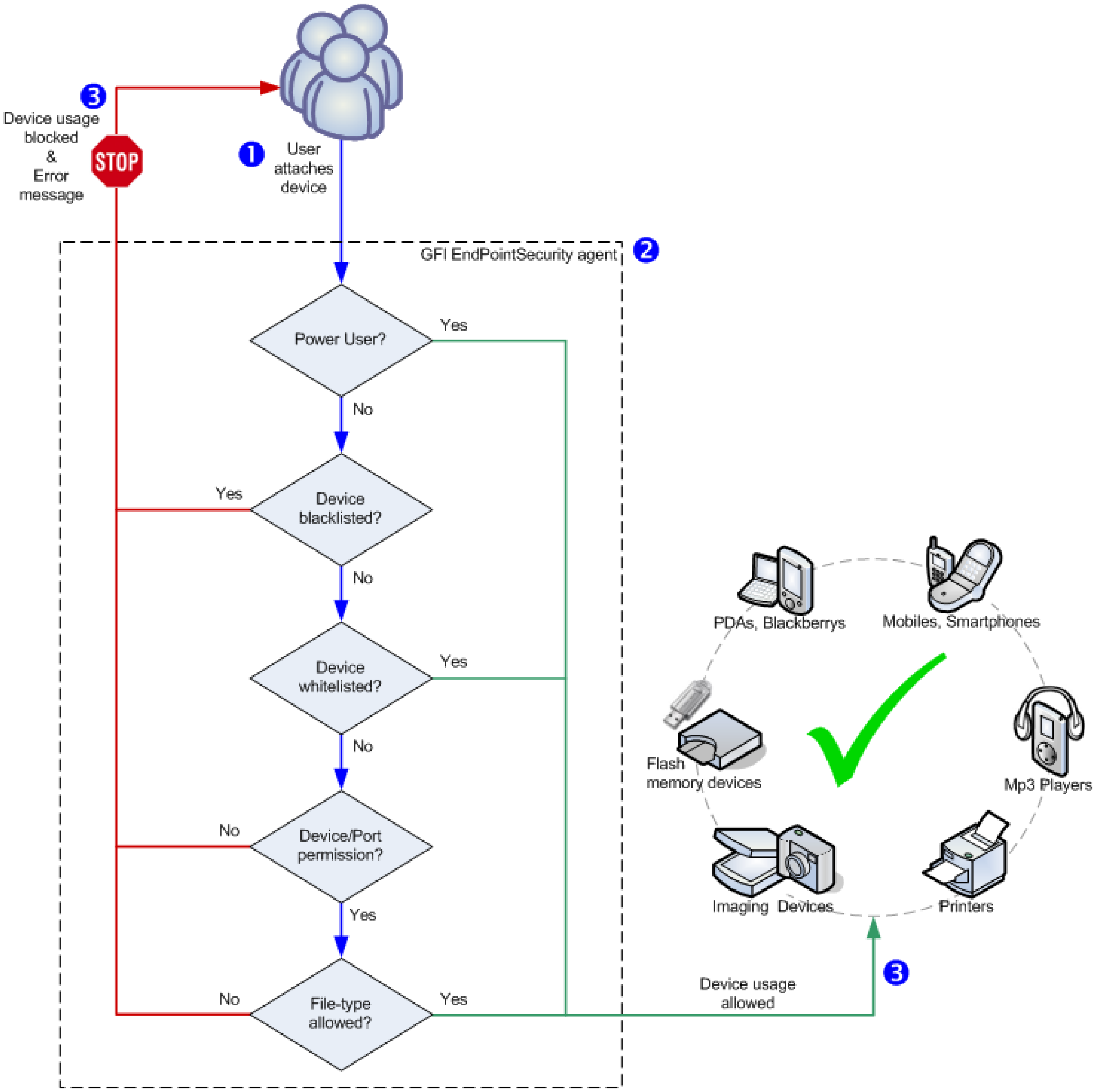
The table below describes the stages depicted above:

Stage	Description
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	Description
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 Management Console; receive alerts and generate reports through GFI EndPointSecurity Report Pack.

1.4 How GFI EndPointSecurity works - Device Access

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



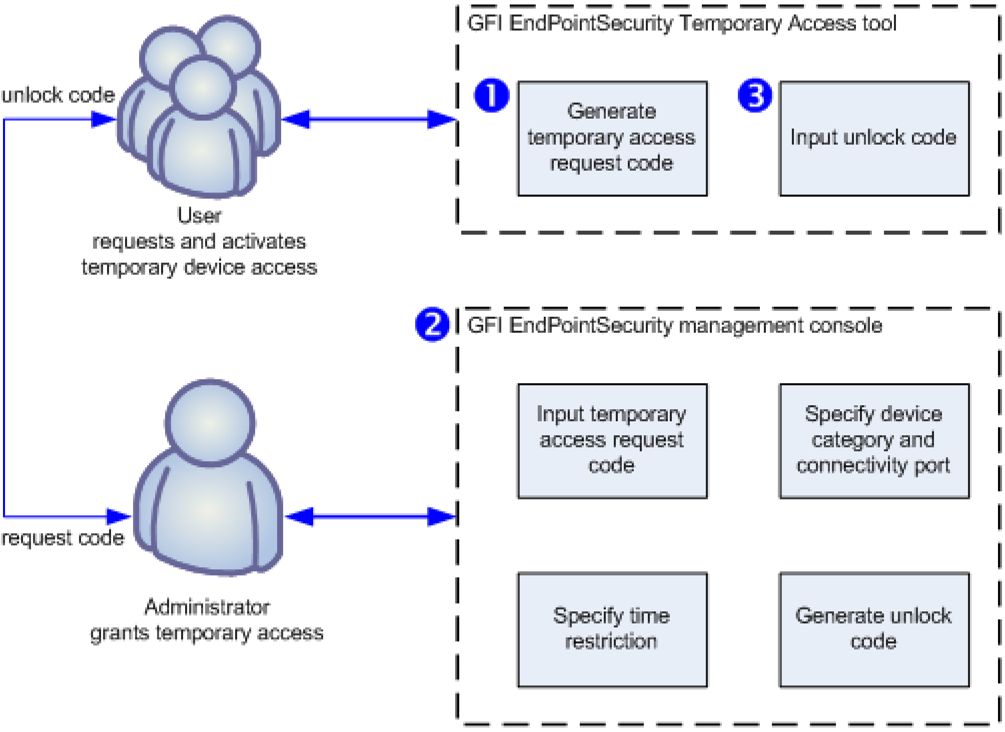
Screenshot 2: Device access

The table below describes the stages depicted above:

Stage	Description
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.

1.5 How GFI EndPointSecurity works - Temporary Access

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



GFI EndPointSecurity Temporary Access tool
1
Generate temporary access request code
3
Input unlock code
unlock code
User
requests and activates
temporary device access
2
GFI EndPointSecurity management console
Input temporary access request code
Specify device category and connectivity port
Specify time restriction
Generate unlock code
request code
Administrator
grants temporary access

Screenshot 3: Requesting/granting temporary access

The table below describes the stages depicted above:

Stage	Description
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.

1.6 Supported connectivity ports

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

- USB
- Secure Digital (SD)
- Firewire
- Bluetooth

- Infrared
- PCMCIA
- Serial & Parallel
- Internal (example: optical drives connected internally on PCI).

1.7 Supported device categories

In GFI EndPointSecurity devices are organized into the following categories:

- Floppy disks
- CDs/DVDs
- Printers
- PDAs, including:
  - Pocket PCs
  - Smart-phones
- Network Adapters, including:
  - Ethernet adapters
  - Wi-Fi adapters
  - Removable adapters (USB, Firewire, PCMCIA)
- Modems, including:
  - Smart-phones
  - Mobile phones
- Imaging Devices:
  - Digital cameras
  - Webcams
  - Scanners
- Human Interface Devices:
  - Keyboards
  - Mice
  - Game controllers
- Storage Devices, including:
  - 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 Devices:

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

1.8 GFI EndPointSecurity Components

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

» GFI EndPointSecurity Management Console

» GFI EndPointSecurity Agent.

1.8.1 GFI EndPointSecurity Management Console

Through the 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.

1.8.2 GFI EndPointSecurity Agent

The GFI EndPointSecurity agent is a client-side service responsible for the implementation of the protection policies on target computers. 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. For more information refer to How to install the GFI EndPointSecurity Agent.

2 Installing GFI EndPointSecurity

This topic provides you with information about preparing your network environment to successfully deploy GFI EndPointSecurity.

2.1 System requirements

2.1.1 Hardware requirements

The table below lists the hardware requirements for GFI EndPointSecurity and GFI EndPointSecurity Agent:

OPTION	GFI EndPointSecurity	GFI EndPointSecurity Agent
Processor	Minimum: 2 GHz Recommended: 2GHz	Minimum: 1 GHz Recommended: 1 GHz
RAM	Minimum: 512 MB Recommended: 1 GB	Minimum: 256 MB Recommended: 512 MB
Free space	Minimum: 100 MB Recommended: 100 MB	Minimum: 50 MB Recommended: 50 MB

2.1.2 Software requirements

OPTION	DESCRIPTION
Supported operating systems (x64/x86)	GFI EndPointSecurity and GFI EndPointSecurity Agent can be installed on a machine running any of the following operating systems: » Microsoft Windows Server 2012 » Microsoft Windows Small Business Server 2011 (Standard edition) » Microsoft Windows Server 2008 R2 (Standard or Enterprise edition) » Microsoft Windows Server 2008 (Standard or Enterprise edition) » Microsoft Windows Small Business Server 2008 (Standard edition) » Microsoft Windows Server 2003 (Standard, Enterprise or Web edition) » Microsoft Windows Small Business Server 2003 » Microsoft Windows 10 (Professional or Enterprise) » Microsoft Windows 8 (Professional or Enterprise) » Microsoft Windows 7 (Professional, Enterprise or Ultimate edition) » Microsoft Windows Vista (Enterprise, Business or Ultimate edition) » Microsoft Windows XP Professional Service Pack 3.
Other software components	GFI EndPointSecurity requires the following software components for a fully functional deployment: » Microsoft Internet Explorer 5.5 or higher » Microsoft .NET Framework 2.0 or higher » Microsoft SQL Server 2000, 2005 or 2008 as the backend database Note A database backend is required for storing device access data and for reporting purposes. For more information refer to Managing the Database Backend.
Firewall ports	**TCP port 1116** (default) - required by GFI EndPointSecurity Agents to notify GFI EndPointSecurity their statuses and to send device access events. Without this port open, the administrator has to either manually monitor events of each target computer or automatically via GFI EventsManager. For more information, refer to http://www.gfi.com/eventsmanager.

2.2 Upgrading GFI EndPointSecurity

Upgrading from GFI EndPointSecurity 3 or later

If you have GFI LanGuard Portable Storage Control, or an earlier version of GFI EndPointSecurity, it is possible to upgrade to the latest version of GFI EndPointSecurity. Upgrading from GFI EndPointSecurity 3 or later is straightforward. The upgrade process is part of the GFI EndPointSecurity installation process, and includes:

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

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.

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 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**
> GFI LanGuard Portable Storage Control agents that were protecting your computers will be automatically added to a protection policy called **LegacyAgents** in GFI EndPointSecurity.

2.3 How to install the GFI EndPointSecurity Management Console

To install GFI EndPointSecurity:

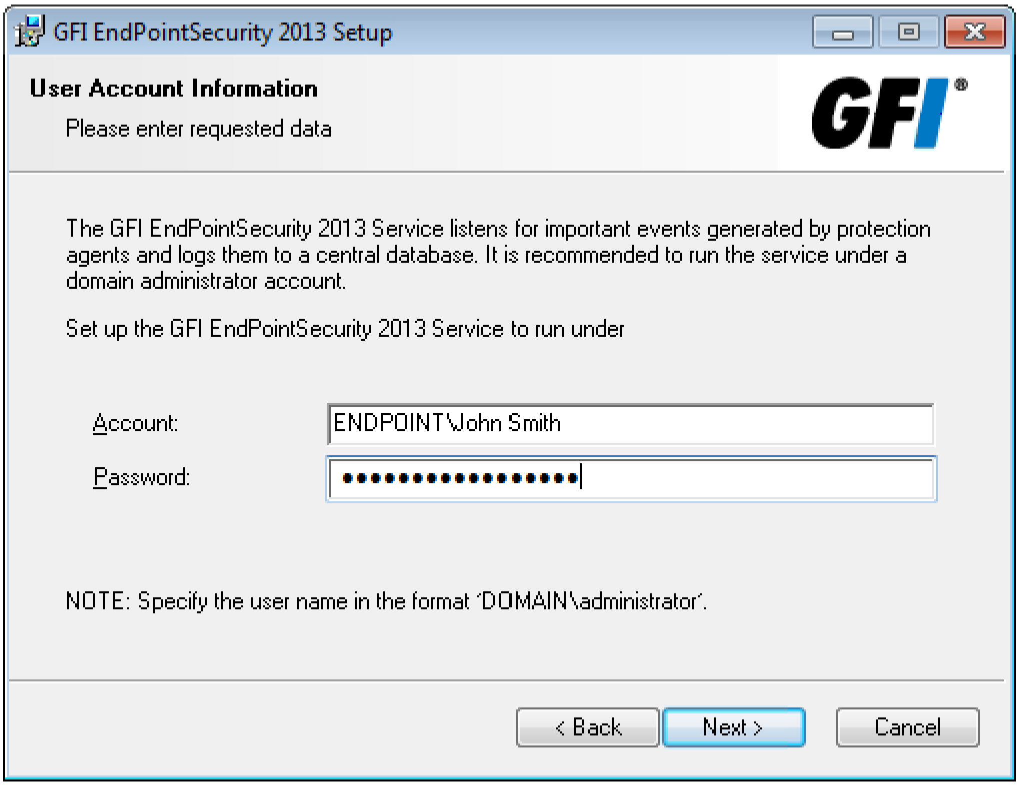
1. Logon the machine where GFI EndPointSecurity is going to be installed, using administrative privileges.

2. Double-click the GFI EndPointSecurity executable file.

2. Select the language you want to install 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**.



User Account Information

Please enter requested data

The GFI EndPointSecurity 2013 Service listens for important events generated by protection agents and logs them to a central database. It is recommended to run the service under a domain administrator account.

Set up the GFI EndPointSecurity 2013 Service to run under

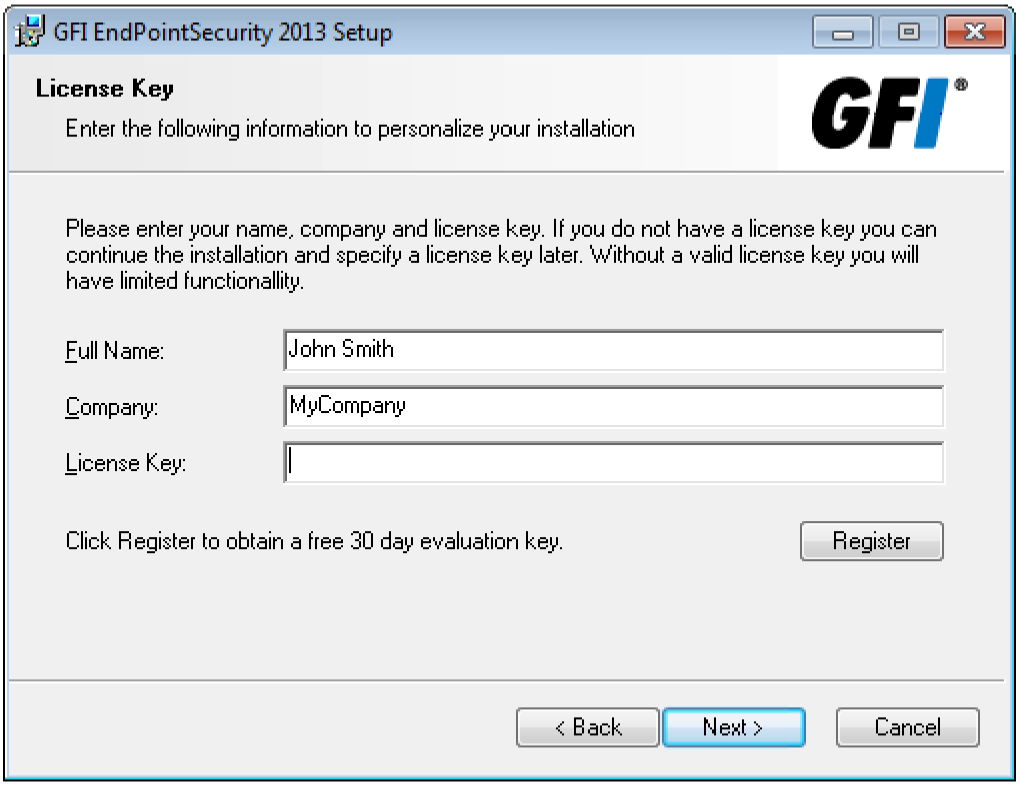
Account: ENDPOINT\John Smith

Password: ••••••••••••••••••

NOTE: Specify the user name in the format 'DOMAIN\administrator'.

Screenshot 4: GFI EndPointSecurity installation: domain administrator account setup

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



License Key

Enter the following information to personalize your installation

Please enter your name, company and license key. If you do not have a license key you can continue the installation and specify a license key later. Without a valid license key you will have limited functionallity.

Full Name: John Smith

Company: MyCompany

License Key:

Click Register to obtain a free 30 day evaluation key.

Screenshot 5: 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.

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.

2.4 Post-install configurations

On the initial launch of GFI EndPointSecurity management console, the Quick Start wizard is automatically launched. This enables you to configure important GFI EndPointSecurity settings for first time use.

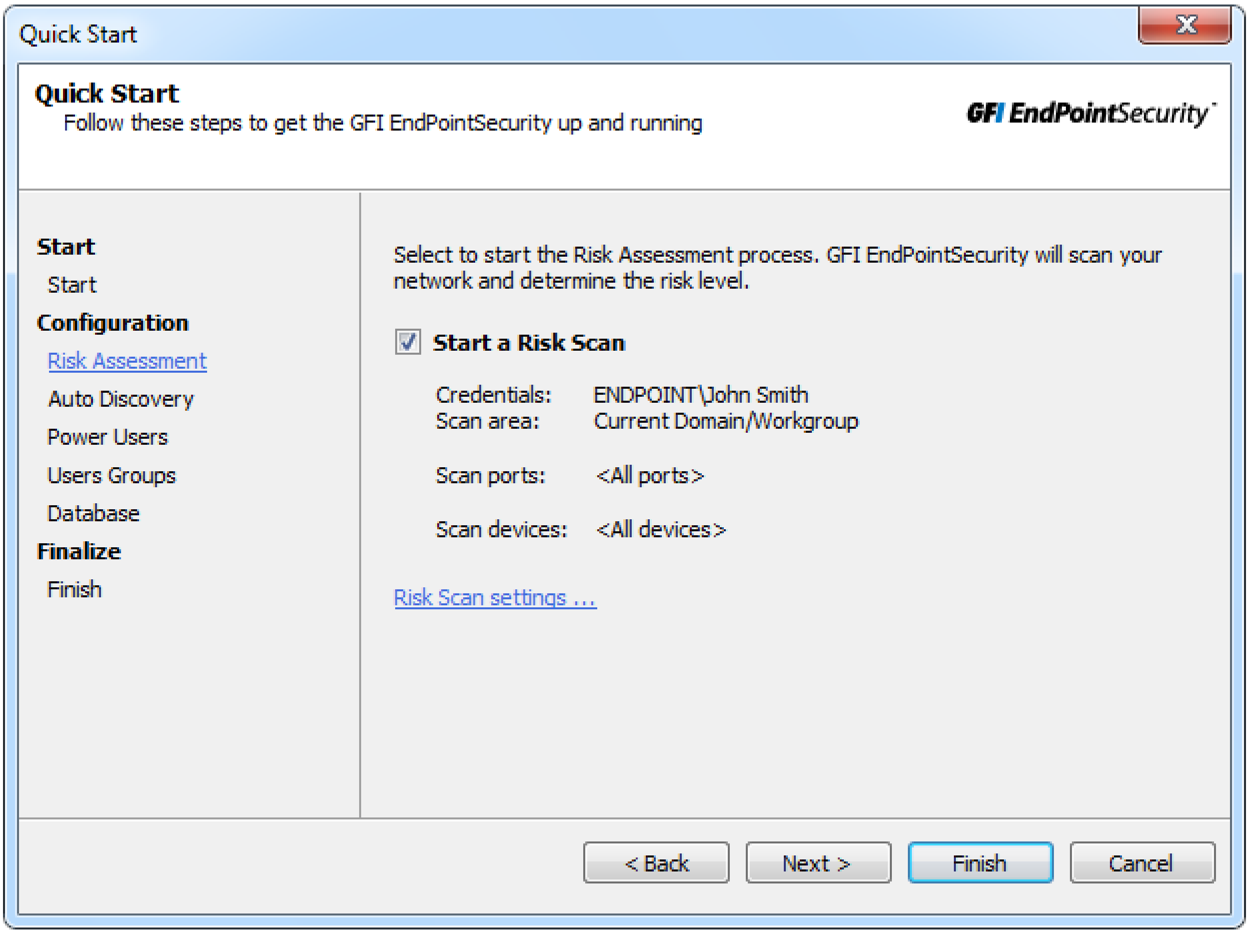
The Quick Start wizard consists of the following steps and guides you to configure:

- Risk Assessment
- Automatic discovery
- Power users
- Users groups
- Database backend.

> Note
> The Quick Start Wizard can be re-launched from **File > Quick Start Wizard**.

To use the Quick Start Wizard:

1. Click **Next** at the wizard welcome screen.



Select to start the Risk Assessment process. GFI EndPointSecurity will scan your network and determine the risk level.

☑ Start a Risk Scan

Credentials: ENDPOINT\John Smith
Scan area: Current Domain/Workgroup

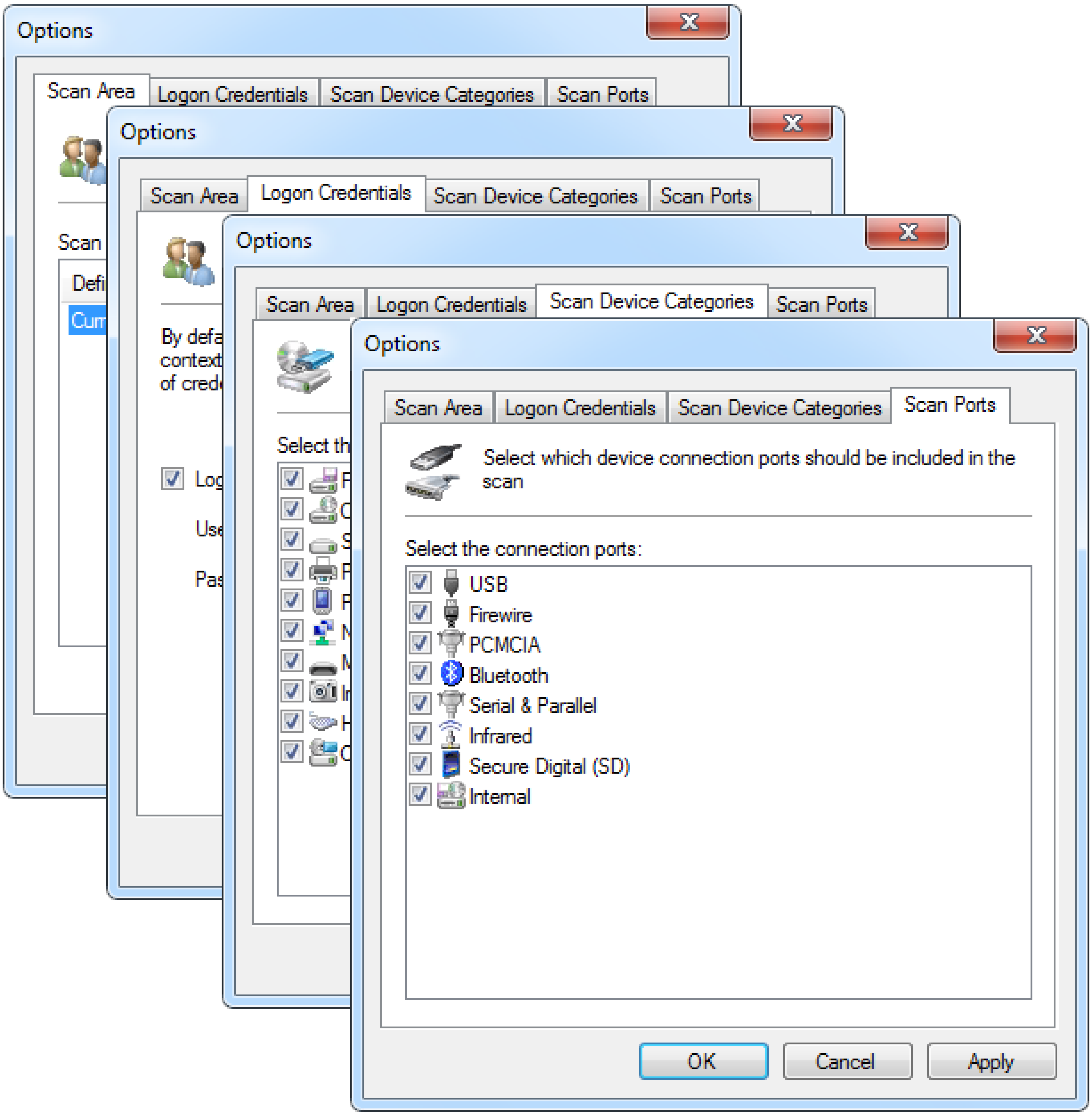
Scan ports: <All ports>

Scan devices: <All devices>

Risk Scan settings ...

Screenshot 6: Post installation tasks: Launching the wizard

2. From Risk Assessment, select/unselect Start a Risk Scan to enable / disable the function to start a scan on your network to determine the risk level.



Select which device connection ports should be included in the scan

Select the connection ports:

- ☑ USB
- ☑ Firewire
- ☑ PCMCIA
- ☑ Bluetooth
- ☑ Serial & Parallel
- ☑ Infrared
- ☑ Secure Digital (SD)
- ☑ Internal

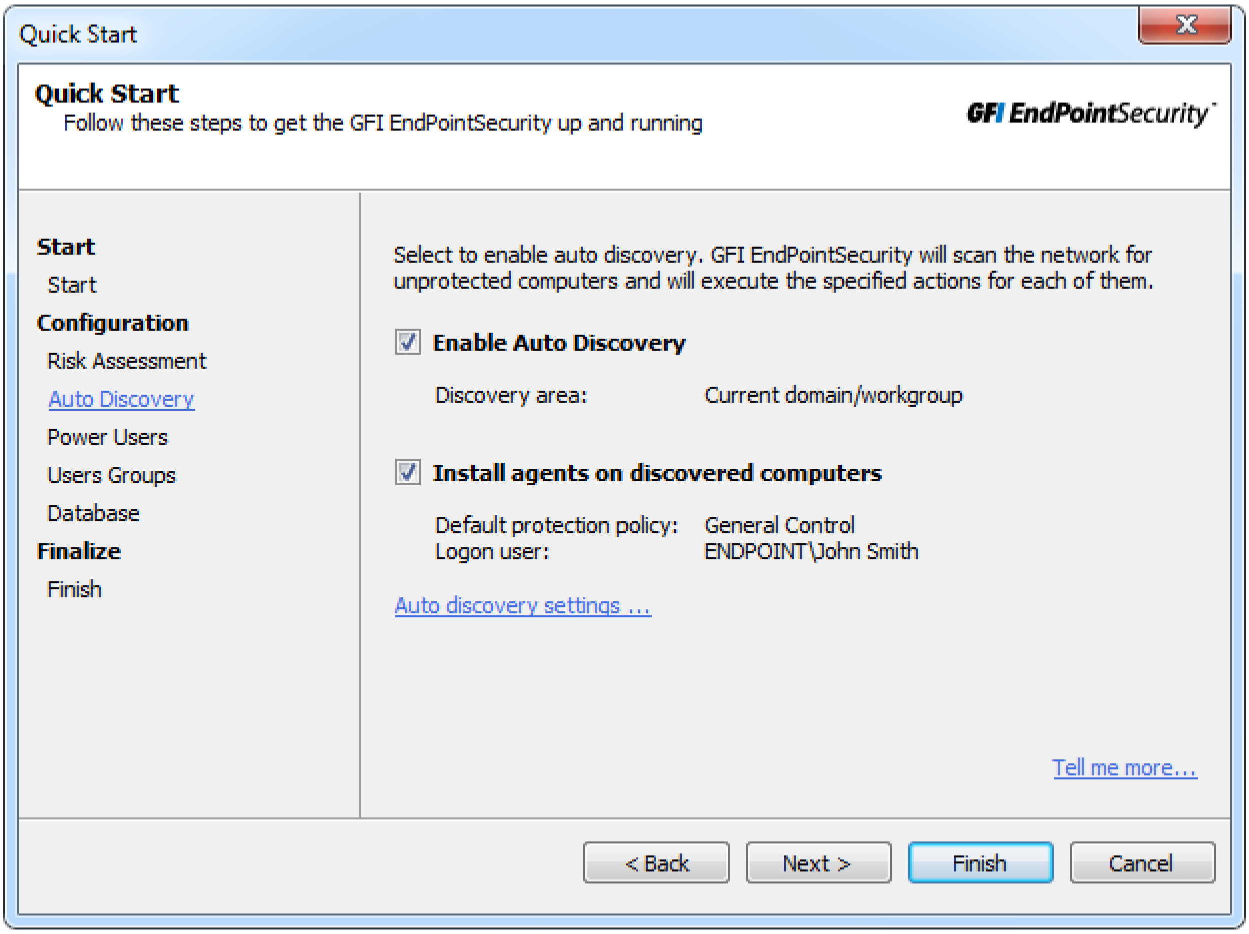
Screenshot 7: Post installation tasks: Configure scan settings

3. (Optional) Click **Risk scan settings...** and configure settings from the tabs described below:

Tab	Description
Scan Area	Select the target area on which GFI EndPointSecurity scans the computers on the network. » **Current domain/workgroup** - GFI EndPointSecurity searches for new computers within the same domain/-workgroup where it is installed » **The following domains/workgroups** - Select this option and click **Add**. Specify the domains where GFI EndPointSecurity searches for new computers and click **OK**. » **Entire network except** - Select this option and click **Add**. Specify the domain/workgroup that should be excluded during auto discovery and click **OK**. » **IP range** - Select this option and click **Add**. Specify the range of IP addresses that should be included or excluded during auto discovery and click **OK**. » **Computer list** - Select this option and click **Add**. Specify the domain/workgroup that should be included or excluded during auto discovery and click **OK**.

Tab	Description
Logon Credentials	Enable/disable **Logon using credentials below** and specify a set of credentials that GFI EndPointSecurity will use to access computers that will be scanned.
Scan Device Categories	Select the device categories that GFI EndPointSecurity will include in the scan.
Scan ports	Select the device connection ports that GFI EndPointSecurity will include in the scan.

4. Click **Apply** and **OK** to close the Risk Assessment dialog and click **Next** at the Quick Start Wizard.


Quick Start

Quick Start

Follow these steps to get the GFI EndPointSecurity up and running

Select to enable auto discovery. GFI EndPointSecurity will scan the network for unprotected computers and will execute the specified actions for each of them.

☑ **Enable Auto Discovery**

Discovery area: Current domain/workgroup

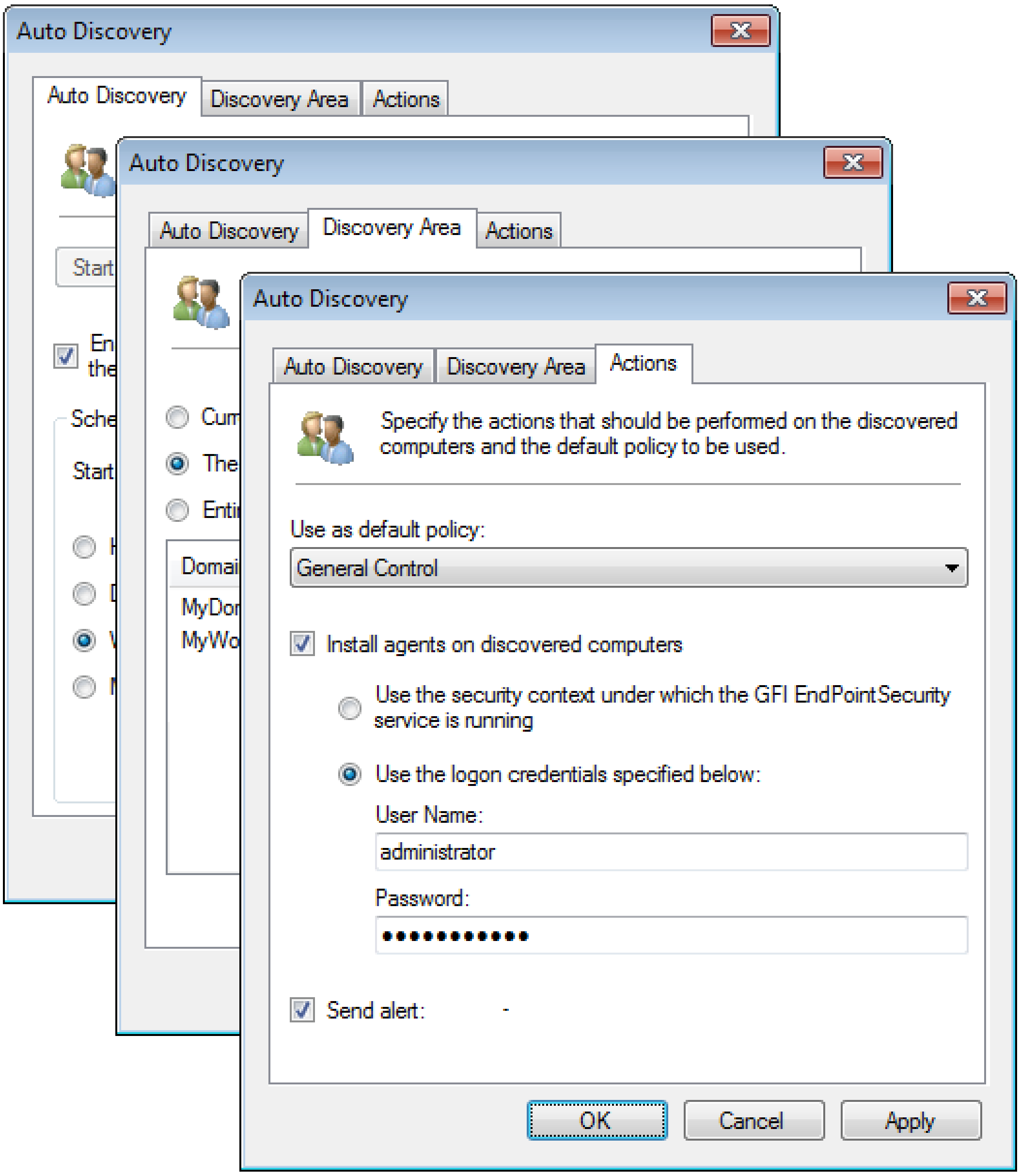
☑ **Install agents on discovered computers**

Default protection policy: General Control
Logon user: ENDPOINT\John Smith

Screenshot 8: Post installation tasks: Enabling auto discovery

5. From **Auto Discovery**, select/unselect **Enable Auto Discovery** to turn on/off auto discovery. When Auto Discovery is enabled, GFI EndPointSecurity periodically scans your network for new computers.

6. Select/unselect **Install agents on discovered computers** to turn on/off automatic deployment of GFI EndPointSecurity Agents on newly discovered computers.



Specify the actions that should be performed on the discovered computers and the default policy to be used.

Use as default policy: General Control

☑ Install agents on discovered computers

○ Use the security context under which the GFI EndPointSecurity service is running

● Use the logon credentials specified below:

User Name: administrator

Password: ●●●●●●●●●●●

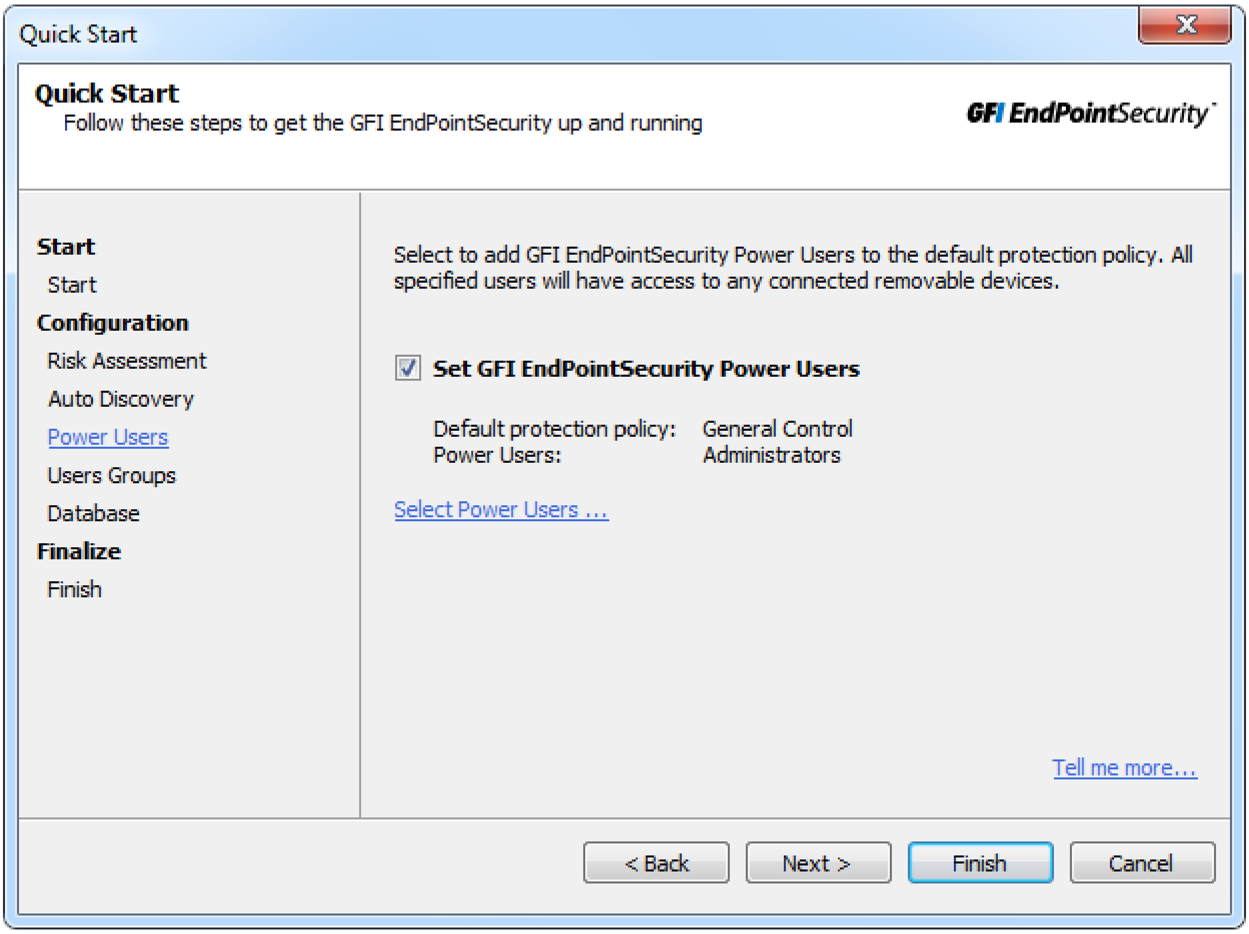
☑ Send alert:

Screenshot 9: Post installation tasks: Configure auto discovery options

7. (Optional) Click **Auto discovery settings...** and configure settings from the tabs described below:

Tab	Description
Auto Discovery	Enable/disable auto discovery and configure a schedule when GFI EndPointSecurity scans your network for new computers.
Discovery Area	Select where GFI EndPointSecurity searches for new computers. Select from: » **Current domain/workgroup** - GFI EndPointSecurity searches for new computers within the same domain/workgroup where it is installed » **The following domains/workgroups** - Select this option and click **Add**. Specify the domains where GFI EndPointSecurity searches for new computers and click **OK**. » **Entire network except** - Select this option and click **Add**. Specify the domain/workgroup that should be excluded during auto discovery and click **OK**.
Actions	Configure the actions taken by GFI EndPointSecurity when a new computer is discovered. Also select the policy that these settings apply to.

8. Click **Apply** and **OK** to close the Auto Discovery dialog and click **Next** at the Quick Start Wizard.



Select to add GFI EndPointSecurity Power Users to the default protection policy. All specified users will have access to any connected removable devices.

☑ **Set GFI EndPointSecurity Power Users**

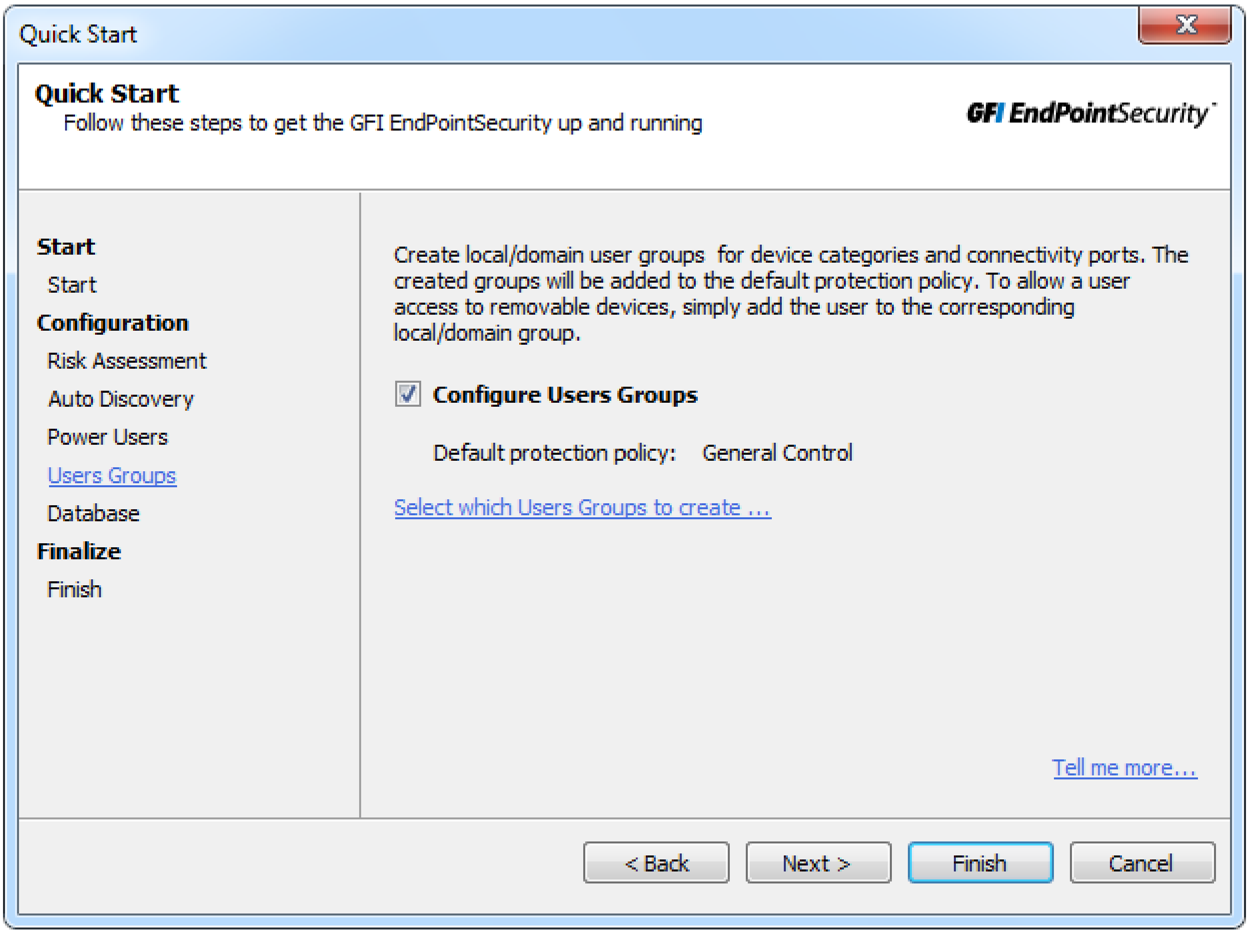
Default protection policy: General Control
Power Users: Administrators

Screenshot 10: Post installation tasks: Configure power users

9. From **Power Users** select/unselect **Set GFI EndPointSecurity Power Users** to enable/disable power users features. Members of the power users group have access to any connected device effected by this policy.

10. Click **Select Power Users...** and from the Power Users dialog, click **Add...** to add users from your domain/workgroup.

11. Click **Apply** and **OK** to close the Power Users dialog and click **Next** at the Quick Start Wizard.



Quick Start

Quick Start

Follow these steps to get the GFI EndPointSecurity up and running

Create local/domain user groups for device categories and connectivity ports. The created groups will be added to the default protection policy. To allow a user access to removable devices, simply add the user to the corresponding local/domain group.

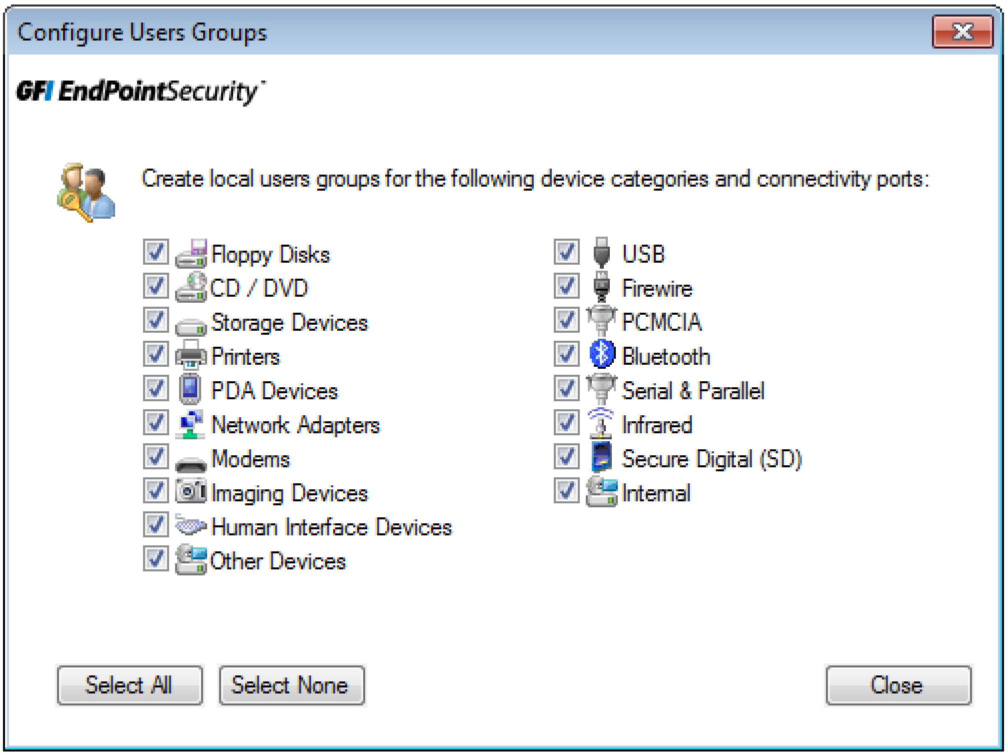
☑ **Configure Users Groups**

Default protection policy: General Control

Select which Users Groups to create ...

Screenshot 11: Post installation tasks: Configure users groups

12. From Users Groups, select/unselect Configure Users Groups to create domain/workgroup users and bind them to device categories and connectivity ports settings selected in the next step.



Configure Users Groups

Create local users groups for the following device categories and connectivity ports:

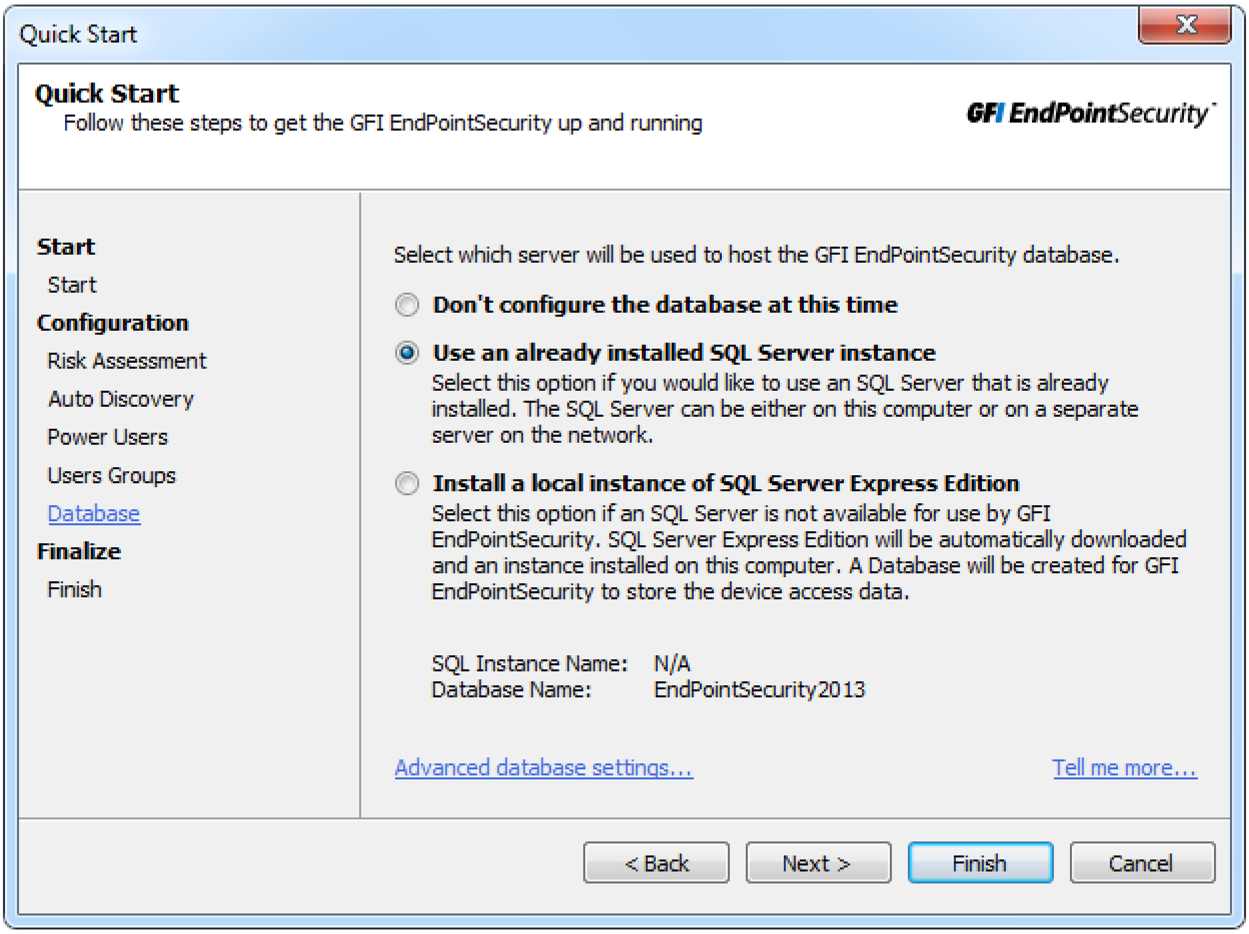
☑ Floppy Disks
☑ CD / DVD
☑ Storage Devices
☑ Printers
☑ PDA Devices
☑ Network Adapters
☑ Modems
☑ Imaging Devices
☑ Human Interface Devices
☑ Other Devices

☑ USB
☑ Firewire
☑ PCMCIA
☑ Bluetooth
☑ Serial & Parallel
☑ Infrared
☑ Secure Digital (SD)
☑ Internal

Screenshot 12: Post installation tasks: Select device categories for users groups

13. Click **Select which Users Groups to create....** From the Configure Users Groups dialog, select the devices and/or connection ports for which users are created on. To manage every supported device and port from this policy, click **Select All**.

14. Click **Close** to close the **Configure Users Groups** and click **Next** at the Quick Start Wizard.



Select which server will be used to host the GFI EndPointSecurity database.

○ **Don't configure the database at this time**

● **Use an already installed SQL Server instance**
Select this option if you would like to use an SQL Server that is already installed. The SQL Server can be either on this computer or on a separate server on the network.

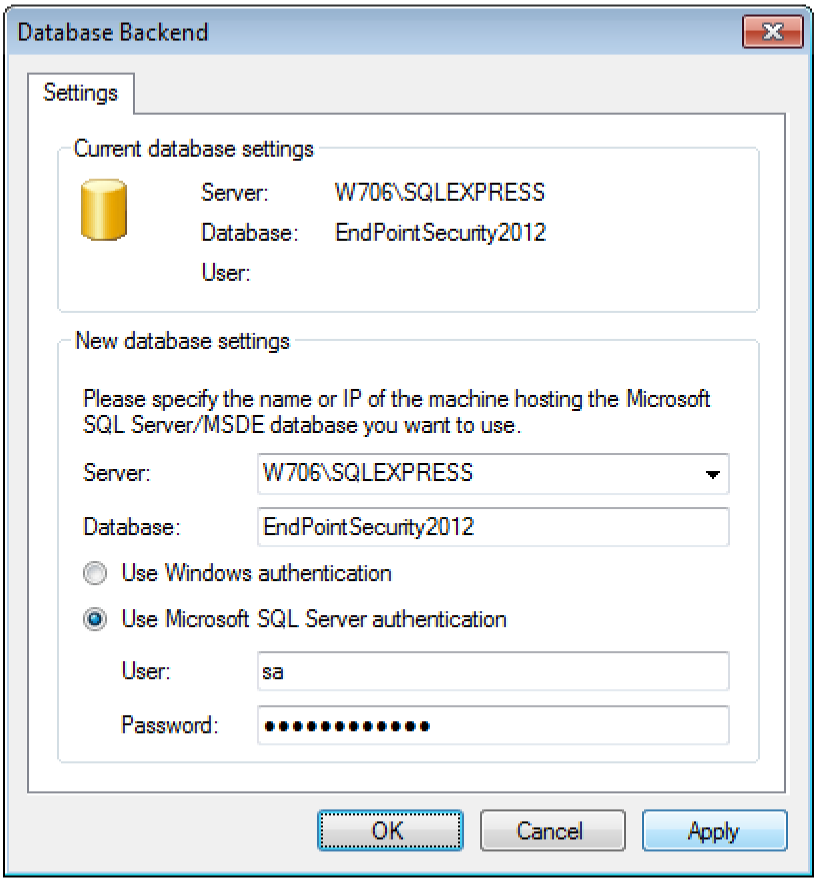
○ **Install a local instance of SQL Server Express Edition**
Select this option if an SQL Server is not available for use by GFI EndPointSecurity. SQL Server Express Edition will be automatically downloaded and an instance installed on this computer. A Database will be created for GFI EndPointSecurity to store the device access data.

SQL Instance Name: N/A
Database Name: EndPointSecurity2013

Screenshot 13: Post installation tasks: Configure database settings

15. From Database, select the database type you want to use as the database backend. Select from the options described below:

Option	Description
Don't configure the database at this time	Finalize the Quick Start Wizard and configure the database backend later. For more information, refer to ACM
Use an already installed SQL Server instance	Use an instance of Microsoft SQL Server already installed on the same machine you are installing GFI EndPointSecurity or any other machine on the network.
Install a local instance of SQL Express Edition	Select this option to download and install an instance of Microsoft SQL Server Express on the same machine you are installing GFI EndPointSecurity. An Internet connection is required.



Database Backend

Current database settings

Server: W706\SQLEXPRESS

Database: EndPointSecurity2012

User:

New database settings

Please specify the name or IP of the machine hosting the Microsoft SQL Server/MSDE database you want to use.

Server: W706\SQLEXPRESS

Database: EndPointSecurity2012

○ Use Windows authentication

● Use Microsoft SQL Server authentication

User: sa

Password: ●●●●●●●●●●●●●

Screenshot 14: Post installation tasks: Configure advanced database settings

16. (Optional) Click **Advanced database settings...** to specify the SQL Server address, database name, logon method and the respective credentials. Click **Apply** and **OK** to close the Database Backend dialog.

17. Click **Next** and wait for the settings to be applied. Click **Finish** to close the Quick Start Wizard.

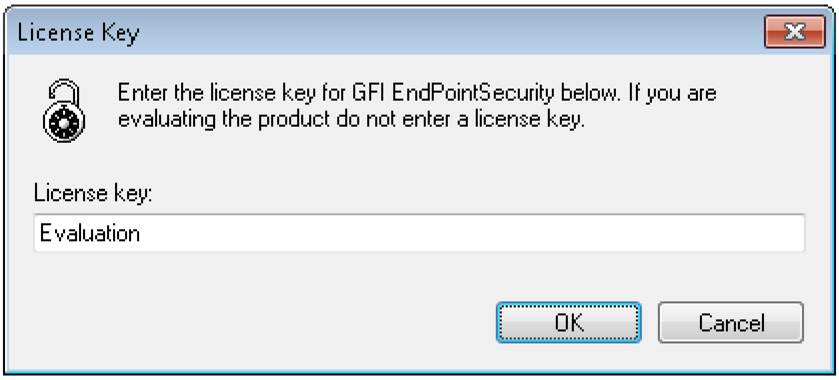
2.5 Product licensing

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 **General** tab.

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



License Key

Enter the license key for GFI EndPointSecurity below. If you are evaluating the product do not enter a license key.

License key: Evaluation

Screenshot 15: 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.

2.6 Product version information

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:

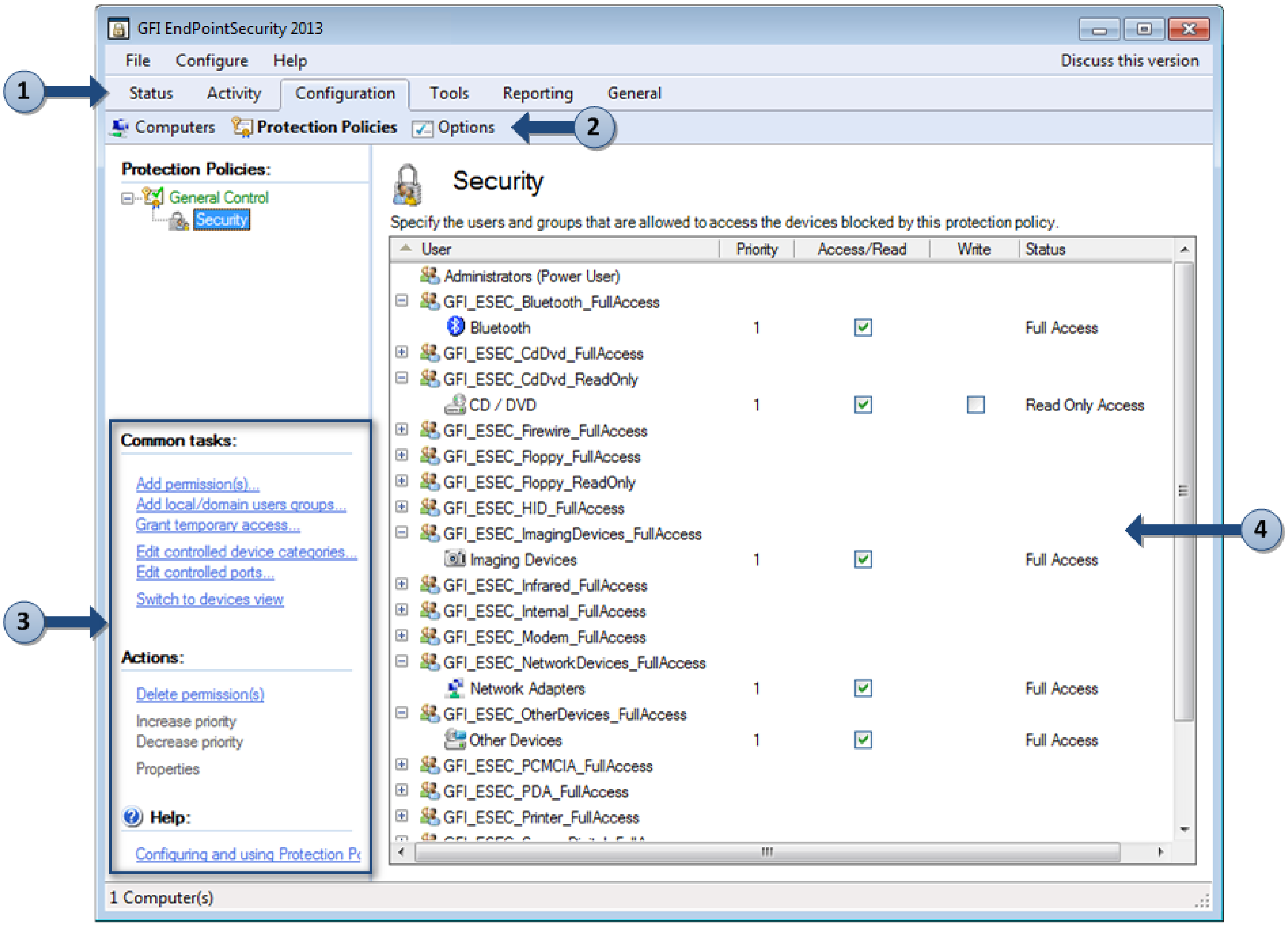
1. Click **General** tab.

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

3. From the right pane, click **Check for newer version** to manually check if a newer version of GFI EndPointSecurity is available. Alternatively, select **Check for newer version at startup** to automatically check if a newer version of GFI EndPointSecurity is available for download every time the management console is launched.

2.7 Using the Management Console

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



Security

Specify the users and groups that are allowed to access the devices blocked by this protection policy.

User	Priority	Access/Read	Write	Status
Administrators (Power User)				
GFI_ESEC_Bluetooth_FullAccess				
Bluetooth	1	☑		Full Access
GFI_ESEC_CdDvd_FullAccess				
GFI_ESEC_CdDvd_ReadOnly				
CD / DVD	1	☑	☐	Read Only Access
GFI_ESEC_Firewire_FullAccess				
GFI_ESEC_Floppy_FullAccess				
GFI_ESEC_Floppy_ReadOnly				
GFI_ESEC_HID_FullAccess				
GFI_ESEC_ImagingDevices_FullAccess				
Imaging Devices	1	☑		Full Access
GFI_ESEC_Infrared_FullAccess				
GFI_ESEC_Internal_FullAccess				
GFI_ESEC_Modem_FullAccess				
GFI_ESEC_NetworkDevices_FullAccess				
Network Adapters	1	☑		Full Access
GFI_ESEC_OtherDevices_FullAccess				
Other Devices	1	☑		Full Access
GFI_ESEC_PCMCIA_FullAccess				
GFI_ESEC_PDA_FullAccess				
GFI_ESEC_Printer_FullAccess				

Common tasks:

Add permission(s)...
Add local/domain users groups...
Grant temporary access...
Edit controlled device categories...
Edit controlled ports...
Switch to devices view

Actions:

Delete permission(s)
Increase priority
Decrease priority
Properties

Help:

Configuring and using Protection Po

Screenshot 16: Navigating GFI EndPointSecurity user interface

GFI EndPointSecurity Management Console consists of the sections described below:

Section	Description
1	Tabs Navigate between the different tabs of GFI EndPointSecurity management console. The available tabs are: » **Status** - Monitor the status of GFI EndPointSecurity and statistical information on device access. » **Activity** - Monitor devices used on the network. » **Configuration** - Access and configure the default protection policies. » **Scanning** -Scan target computers and discover connected devices » **Reporting** - Download or launch GFI EndPointSecurityReport Pack to generate your reports. » **General** - Check for GFI EndPointSecurity updates, as well as version and licensing detail.
2	Sub-tabs Access more settings and/or information about the selected tab from section 1.
3	Left Pane Access configuration options provided in GFI EndPointSecurity. The configuration options are grouped into three sections, including **Common Tasks**, **Actions** and **Help**. Available only for some tabs.
4	Right Pane Configure the configuration options selected from the left pane. Available only for some tabs.

2.8 Testing your installation

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.

This section contains the following information:

- Test preconditions
- Test case
- Reverting to default settings

2.8.1 Test preconditions

The following test pre-conditions and settings are required ONLY for the purpose of this test:

Device setup

For the following test you require:

- CD/DVD drive connected to the local computer
- 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 same computer where GFI EndPointSecurity 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:

- Ensure the local computer is listed in the **Status > Agents** view. 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.
- Ensure 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 - Administration and Configuration Manual.

- Ensure that 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.

2.8.2 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.

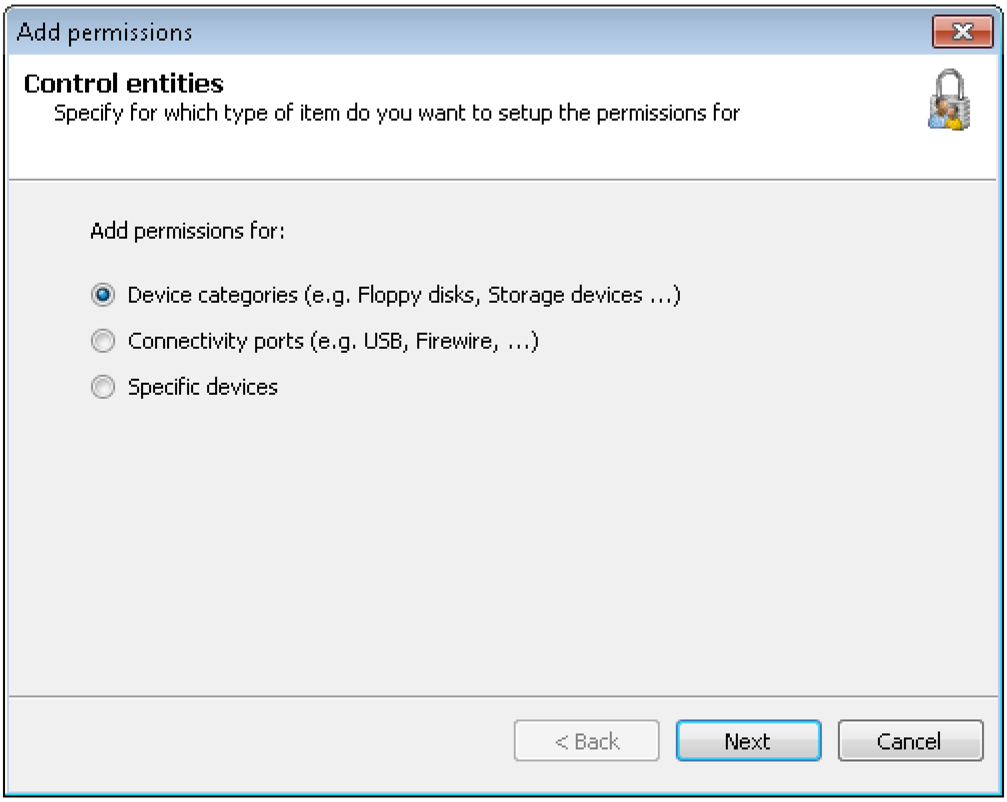
3. Click on the **Configuration** tab.

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.



Add permissions

Control entities

Specify for which type of item do you want to setup the permissions for

Add permissions for:

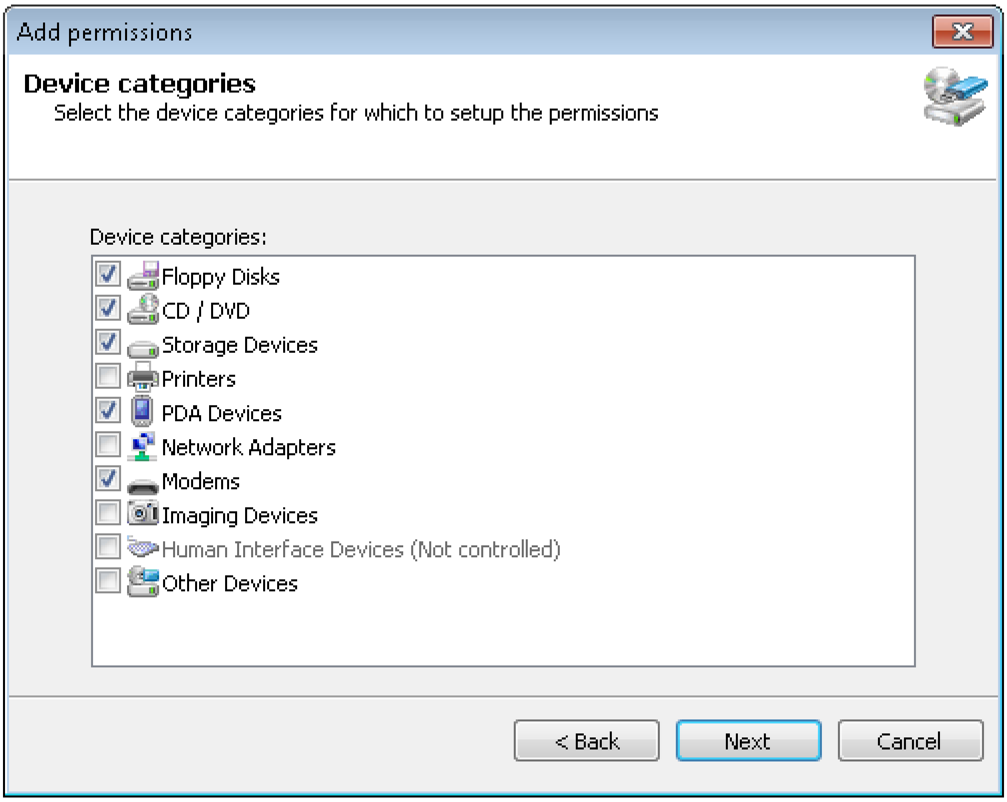
● Device categories (e.g. Floppy disks, Storage devices ...)

○ Connectivity ports (e.g. USB, Firewire, ...)

○ Specific devices

Screenshot 17: Selecting control entities

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



Add permissions

Device categories

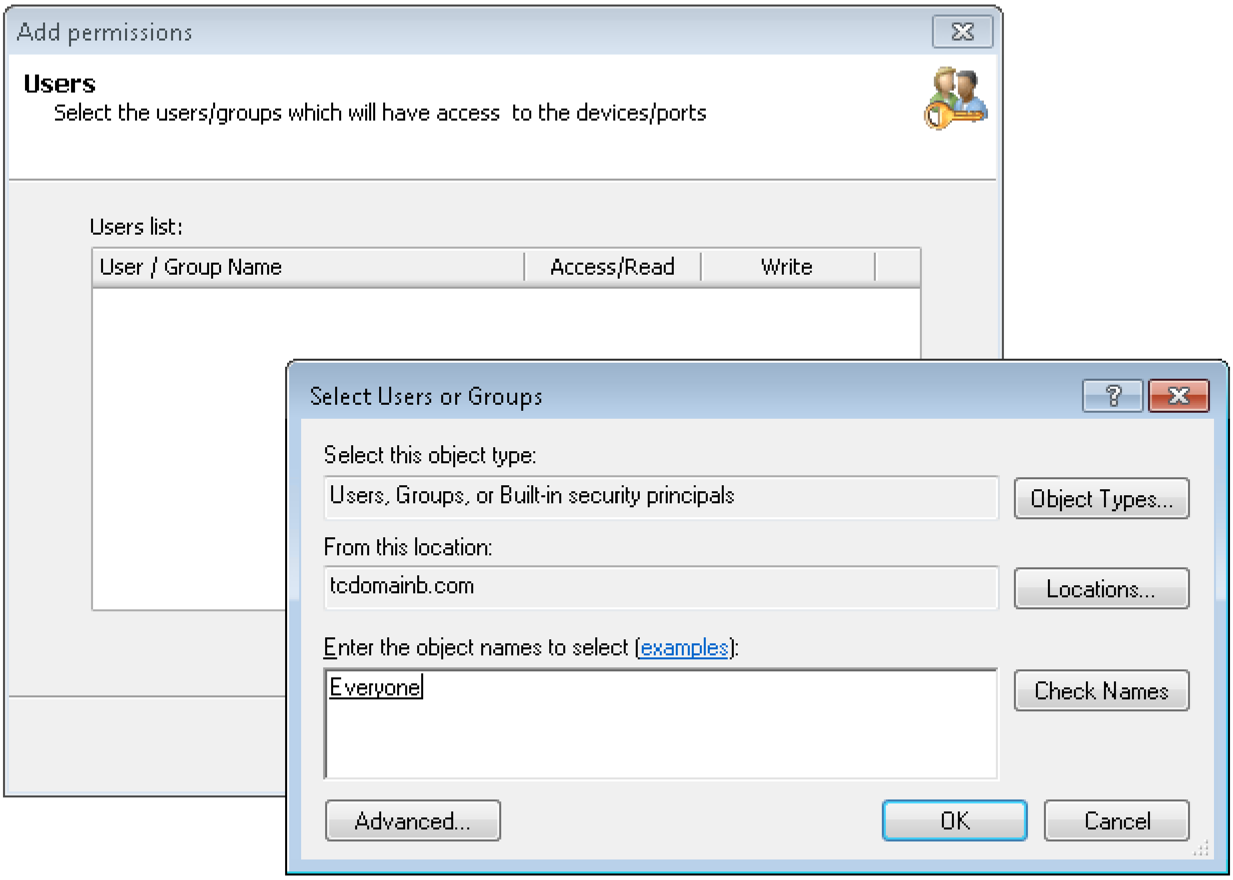
Select the device categories for which to setup the permissions

Device categories:

☑ Floppy Disks
☑ CD / DVD
☑ Storage Devices
□ Printers
☑ PDA Devices
□ Network Adapters
☑ Modems
□ Imaging Devices
□ Human Interface Devices (Not controlled)
□ Other Devices

Screenshot 18: Selecting device categories to assign permissions

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



Users

Select the users/groups which will have access to the devices/ports

Users list:

User / Group Name	Access/Read	Write

Select Users or Groups

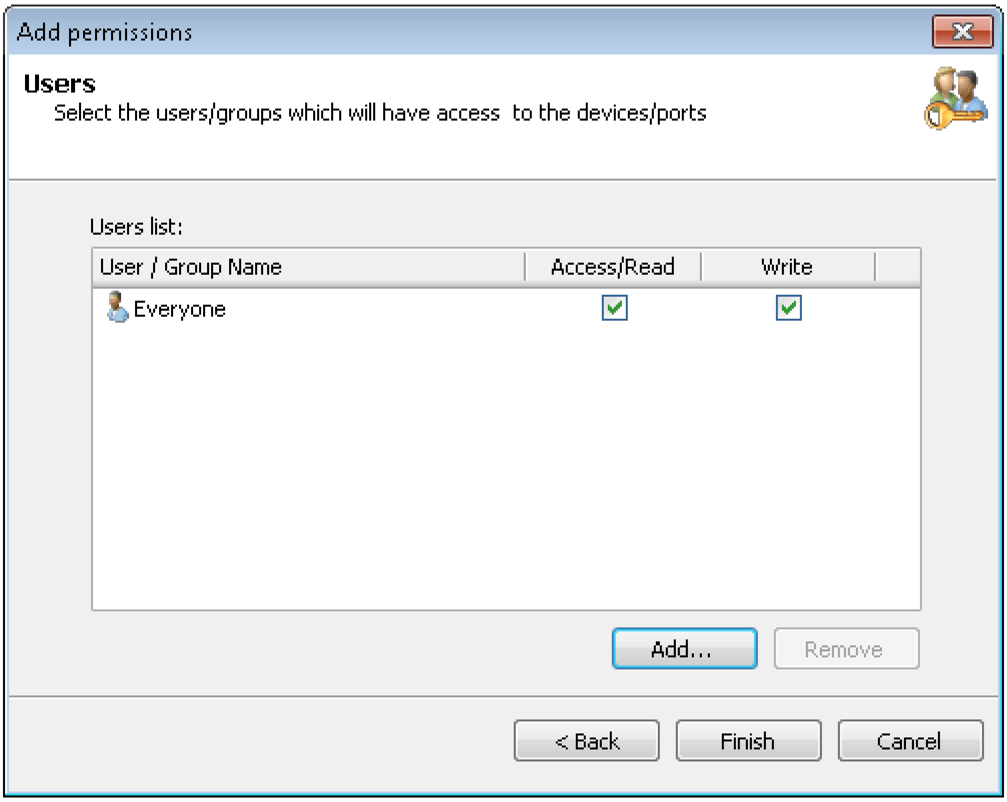
Select this object type:
Users, Groups, or Built-in security principals

From this location:
tcdomainb.com

Enter the object names to select (examples):
Everyone

Screenshot 19: 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**.



Users

Select the users/groups which will have access to the devices/ports

Users list:

User / Group Name	Access/Read	Write
Everyone	☑	☑

Screenshot 20: 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 **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.

2.8.3 Reverting to default 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.

3 Troubleshooting and Support

This chapter explains how to resolve any issues encountered during installation of GFI EndPointSecurity. The main sources of information available to solve these issues are:

This section and the rest of GFI EndPointSecurityAdministrator Guide contains solutions for all possible problems you may encounter. If you are not able to resolve any issue, please contact GFI Support for further assistance.

3.1 Common Issues

The table below lists the most common issues which you may encounter during the initial setup and first time use of GFI EndPointSecurity and a possible solution for each:

Issue	Possible Cause	Possible Solution
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. For more information refer to System Requirements.
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.
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://kb.gfi.com/articles/knowledge base_ Article/KBID003754?retURL=%2Fapex%2FSupportHome&popup=true
Timeout	Agent deployment onto the target computer is either taking too long to complete or else is blocked.	Try to deploy the GFI EndPointSecurity agent again.
Failed to install the deployment service. (error)	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.

Issue	Possible Cause	Possible Solution
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 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 EndPointSecurity2016 > GFI EndPointSecurity2016 Troubleshooter**.

4 Glossary

A

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.

B

BitLocker To Go

A Microsoft Windows 7 feature to protect and encrypt data on removable devices.

C

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.

D

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.

E

Event logging

A feature to record events related to attempts made to access devices and connection ports on target computers and service operations.

F

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.

G

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

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.

H

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.

M

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.

P

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.

Q

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.

S

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.

T

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.

U

User message

A message that is displayed by GFI EndPointSecurity agents on target computers, when devices are accessed.

5 Index

USA, CANADA AND CENTRAL AND SOUTH AMERICA

1005 Slater Road, Suite 300, Durham, NC 27703, USA
Telephone: +1 (888) 243-4329
Fax: +1 (919) 379-3402
ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK
Telephone: +44 (0) 870 770 5370
Fax: +44 (0) 870 770 5377
sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, Territorials Street, Mriehel BKR 3000, Malta
Telephone: +356 2205 2000
Fax: +356 2138 2419
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