Administrator Guide

GFI EndPointSecurity™

Find out how to configure GFI EndPointSecurity in different environments and how to set up advanced features.

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accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors.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): 09/01/2016

Contents

1 Installing GFI EndPointSecurity

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

1.1 System requirements

1.1.1 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

1.1.2 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 (page 131).
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.

1.2 Deployment scenarios

GFI EndPointSecurity deployments depend on the location of the machines that you need to monitor. Refer to the following deployment scenarios to determine which setup fits best your needs.

1.2.1 Deploy GFI EndPointSecurity on a domain controller

GFI EndPointSecurity installed on a Domain Controller can only monitor machines that are part of the same domain.

When installed on an Active Directory environment, GFI EndPointSecurity creates AD groups which can be used to allow or deny access to all the machines. Therefore if a user needs specific access to a device, the administrator just needs to add the user to the group, and changes will be made available when AD settings are updated locally on machines.

1.2.2 Deploy GFI EndPointSecurity on a member server

When GFI EndPointSecurity is installed on a Member Server it can monitor machines that are part of the domain as well as machines that are part of a workgroup.

This setup is preferable in the case you have the computers that are part of a domain together with computers that are members of a workgroup. It adds some complexity to the administration but gives more flexibility and a wider range of machines that can be controlled from a single console.

1.2.3 Deploy GFI EndPointSecurity on a workgroup machine

GFI EndPointSecurity can also be installed on a workgroup environment. If this option is used, GFI EndPointSecurity monitors only the machines that are members of the same group.

In this scenario, local groups need to be created on the GFI EndPointSecurity machine. The same groups need to be created also in the monitored machine so that permissions can be granted.

For more information, refer to Configuring access permissions on workgroups (page 56).

In this table you can have an overview of the options available:

Installation	Monitor Domain machines	Monitor Workgroup machines
Domain Controller	✓	✗
Member Server	✓	✓
Workgroup	✗	✓

1.3 GFI EndPointSecurity Components

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

- GFI EndPointSecurity Management Console
- GFI EndPointSecurity Agent.

1.3.1 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.

1.3.2 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 (page 9).

1.4 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.

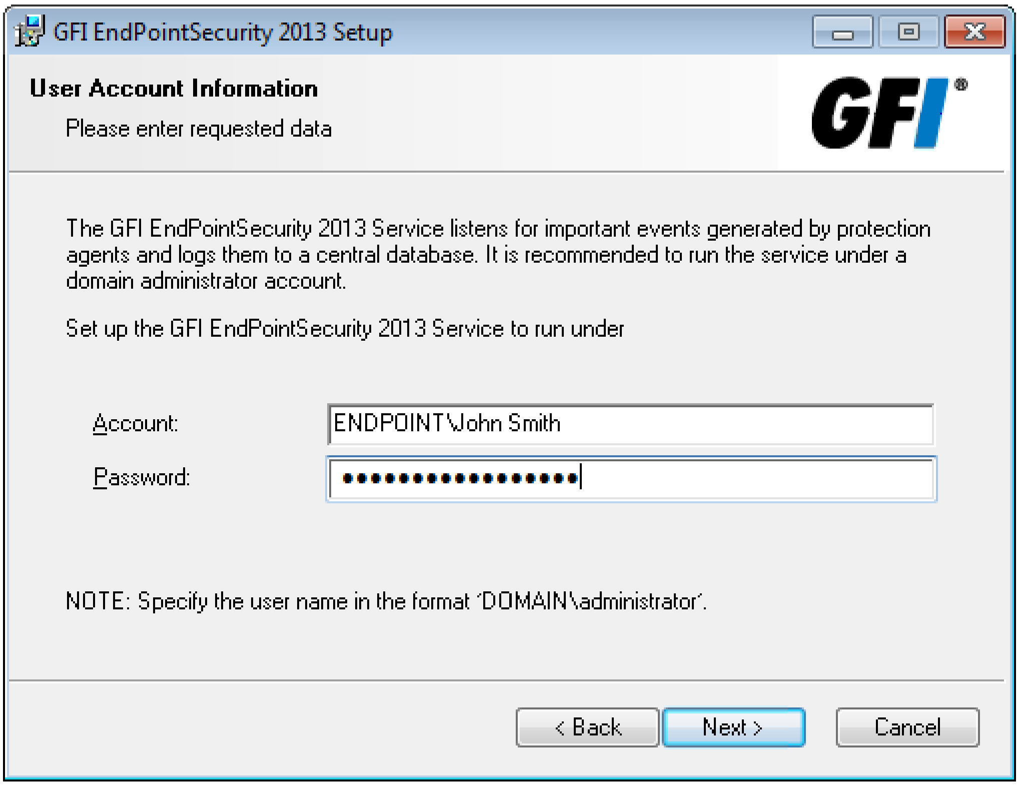
2. Right-click the GFI EndPointSecurity installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.

3. Launch the GFI EndPointSecurity installer.

4. Select the language you want to install and click **OK**.

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

6. 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**.


GFI EndPointSecurity 2013 Setup

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

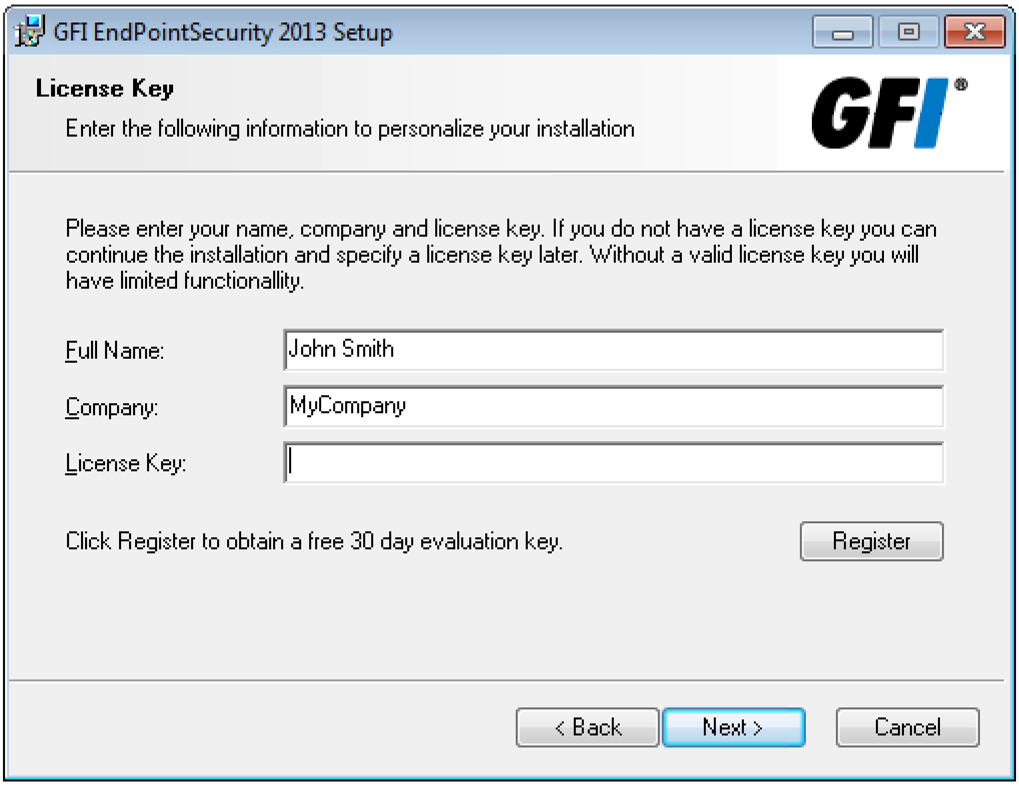
Account: ENDPOINT\John Smith

Password: ••••••••••••••••••

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

Screenshot 1: GFI EndPointSecurity installation: domain administrator account setup

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


GFI EndPointSecurity 2013 Setup

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 2: GFI EndPointSecurity installation: license key details

8. 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.

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

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

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

1.5 How to install the 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 (page 9).

The GFI EndPointSecurity Agent needs a machine with a minimum set of hardware and software requirements. For more information, refer to System requirements (page 5).

The installation of the GFI EndPointSecurity Agent should be a transparent process. However, if you encounter any issues with the installation, ensure the following are configured correctly:

1.5.1 File and Printer Sharing for Microsoft Networks

Enable **File and Printer Sharing for Microsoft Networks** on the local network card interfaces on the GFI EndPointSecurity Management Console server and on client machines.

This is configured from **Control Panel > Network and Internet > Network Connections > Local Area Connection > Properties.**

1.5.2 Enable File and printing sharing exception

Enable **File and Printing sharing** exception on the Windows Firewall of the GFI EndPointSecurity Agent machines.

If Microsoft Windows Firewall is enabled:

- Open **Windows Firewall > Exceptions tab** and select **File and Print Sharing**.

This allows the GFI EndPointSecurity main application to copy all required files in order to deploy the agent onto the remote Agent machine.

If this exception is disabled, the Agent installation will fail and the following error message will be displayed on the main application Deployment Report:

- *Failed to contact remote computer. Computer might be offline or the specified credentials are invalid.*

If you have another firewall client replacing the Microsoft Windows firewall, similar exceptions are necessary.

1.5.3 Network Firewalls

If you have a network firewall in the communication path between the GFI EndPointSecurity Management Console server and the Agent machines, make sure SMB communications is allowed. This is done over the following TCP ports:

- 135
- 139
- 445

1.5.4 Firewall port exception

Add the following exceptions to any firewall enabled on the GFI EndPointSecurity server:

- TCP Port 1116

The GFI EndPointSecurity Agents periodically send back status information to the GFI EndPointSecurity server. This includes a "beep" that is a CRC check of the policy (so that the Console knows if the policy is up to date) and the events that the Agent sent back to the Console for storage in the SQL backend database.

By default, this connection is done on port 1116, but can be changed from:

- **GFI EndPointSecurity configuration > Options > Advanced Options > Communication**

1.5.5 Access to the Remote Registry Service

GFI EndPointSecurity needs access to the registry service on the target machine where the Agent is going to be installed. Detailed information on how to enable access to the Remote Registry service of the target machine is discussed in the following article: http://go.gfi.com/?pageid=esec_remoteregistry.

1.5.6 Windows Services

The following services are required to be running on the agent machines:

- Server service
- Workstation service
- Remote Registry Service
- Remote Procedure Call

1.5.7 Hidden Shares and Server Permissions

Ensure that the following are met:

- The account under which the GFI EndPointSecurity service is running has administrative rights on the GFI EndPointSecurity server as well as the target machines.
- Access to the C$ hidden share is required to install/uninstall the agent, ensure you can browse to this hidden share from the GFI EndPointSecurity server.
- Access to the ADMIN$ hidden share is also required to update the Agent. Ensure you can browse to this hidden share from the GFI EndPointSecurity server.

1.5.8 Change the behavior of UAC

UAC policies may block the installation of the main installation or the agent. It is recommended to set UAC to run elevated tasks without a prompt.

> **NOTE**
> This setting can also be set via GPO.

To change the behavior of UAC:

1. Go to **Start** and run `secpol.msc`

2. If the **User Account Control** dialog box appears click **Yes**.

3. In the console tree, go to **Local Policies > Security Options**.

4. In the details pane, scroll to the Group Policy setting and double-click **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode**.

5. Select **Elevate without prompt** and click **OK**

1.6 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.

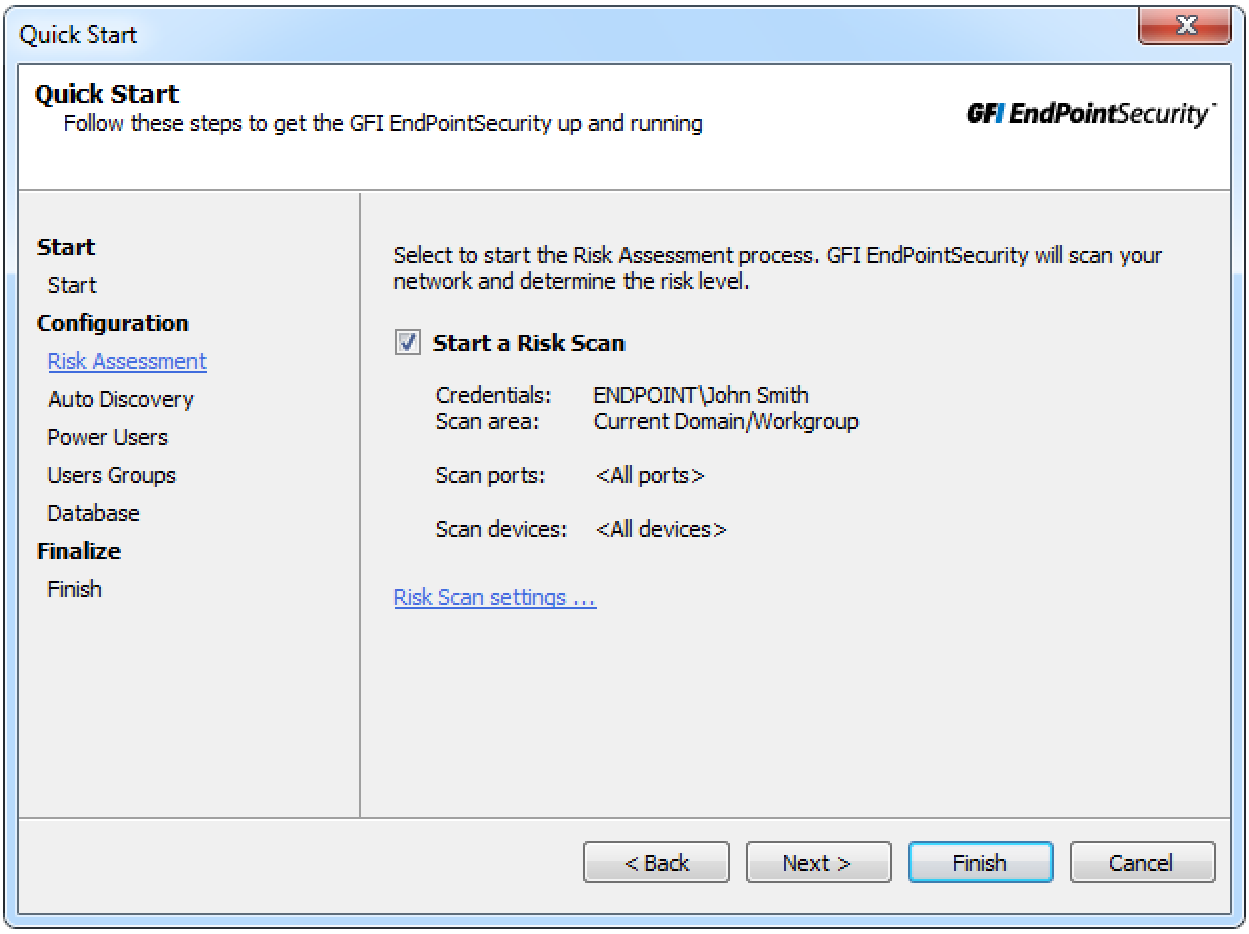
The Quick Start wizard consists of the following steps and guides you to configure:

- 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.



Quick Start

Follow these steps to get the GFI EndPointSecurity up and running

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

☑ **Start a Risk Scan**

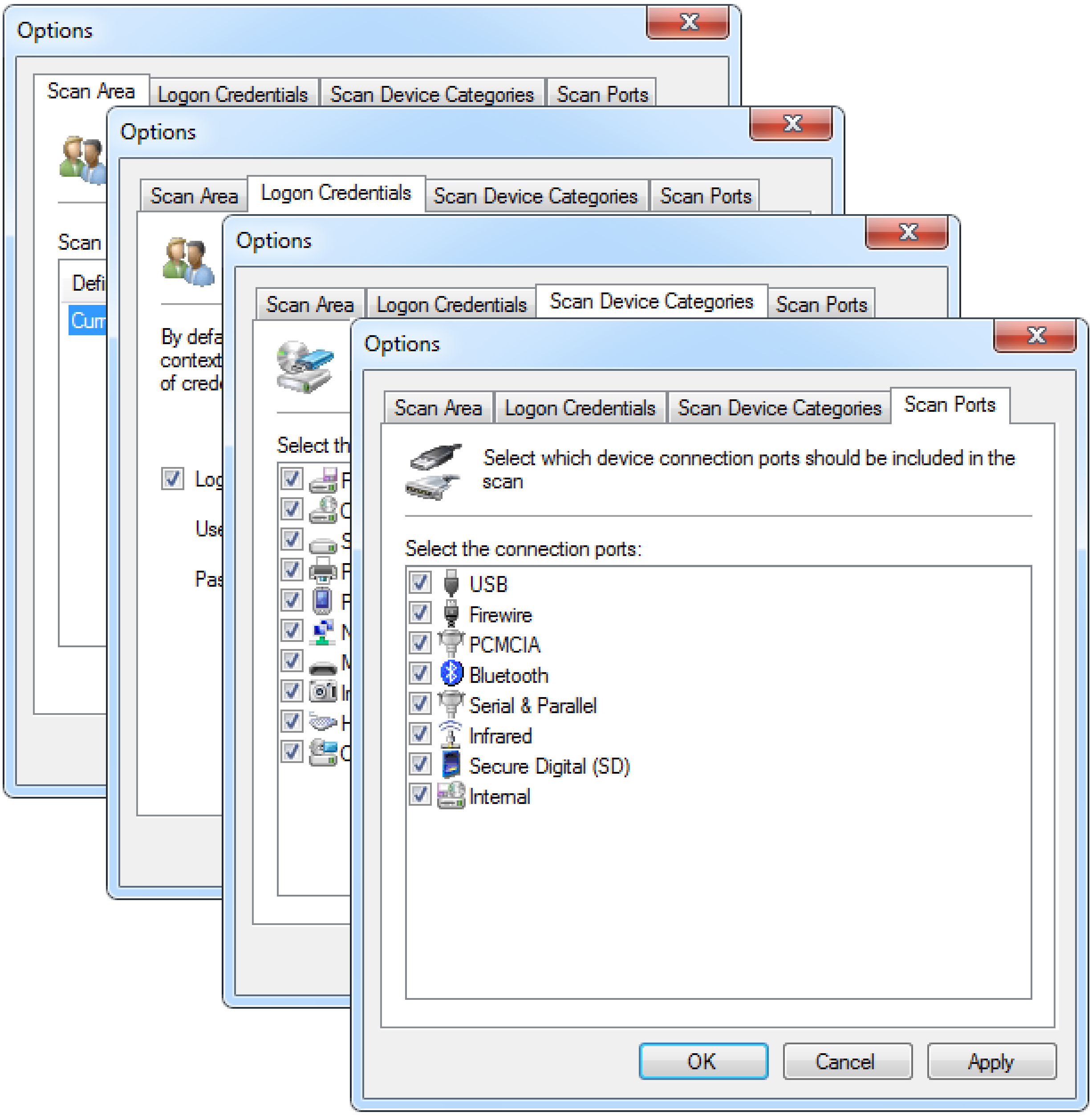
Credentials: ENDPOINT\John Smith
Scan area: Current Domain/Workgroup

Scan ports: <All ports>

Scan devices: <All devices>

Screenshot 3: 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

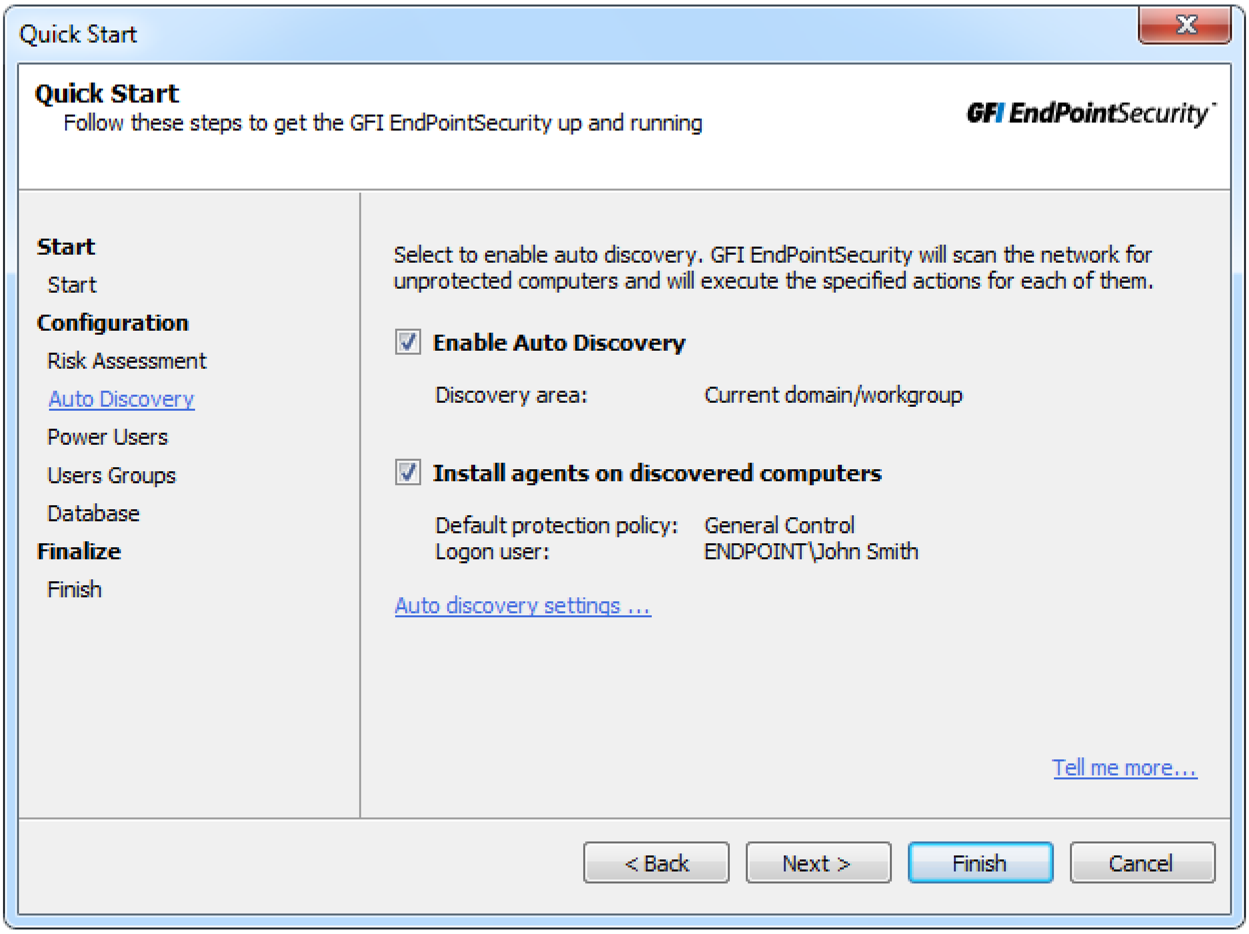
Screenshot 4: Post installation tasks: Configure scan settings

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.



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**

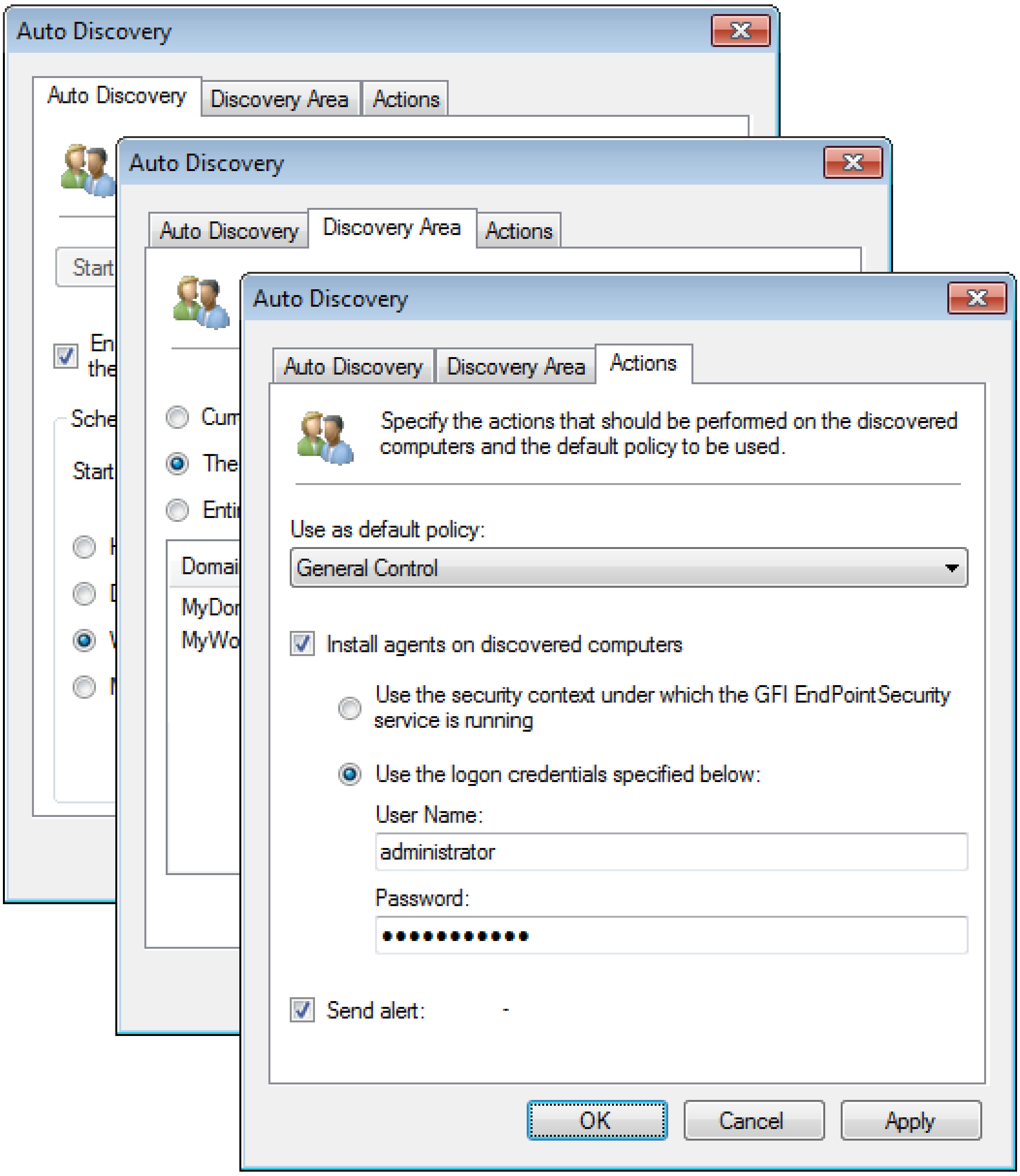
Default protection policy: General Control

Logon user: ENDPOINT\John Smith

Screenshot 5: 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.



Auto Discovery

Auto Discovery | Discovery Area | Actions

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: ●●●●●●●●●●●

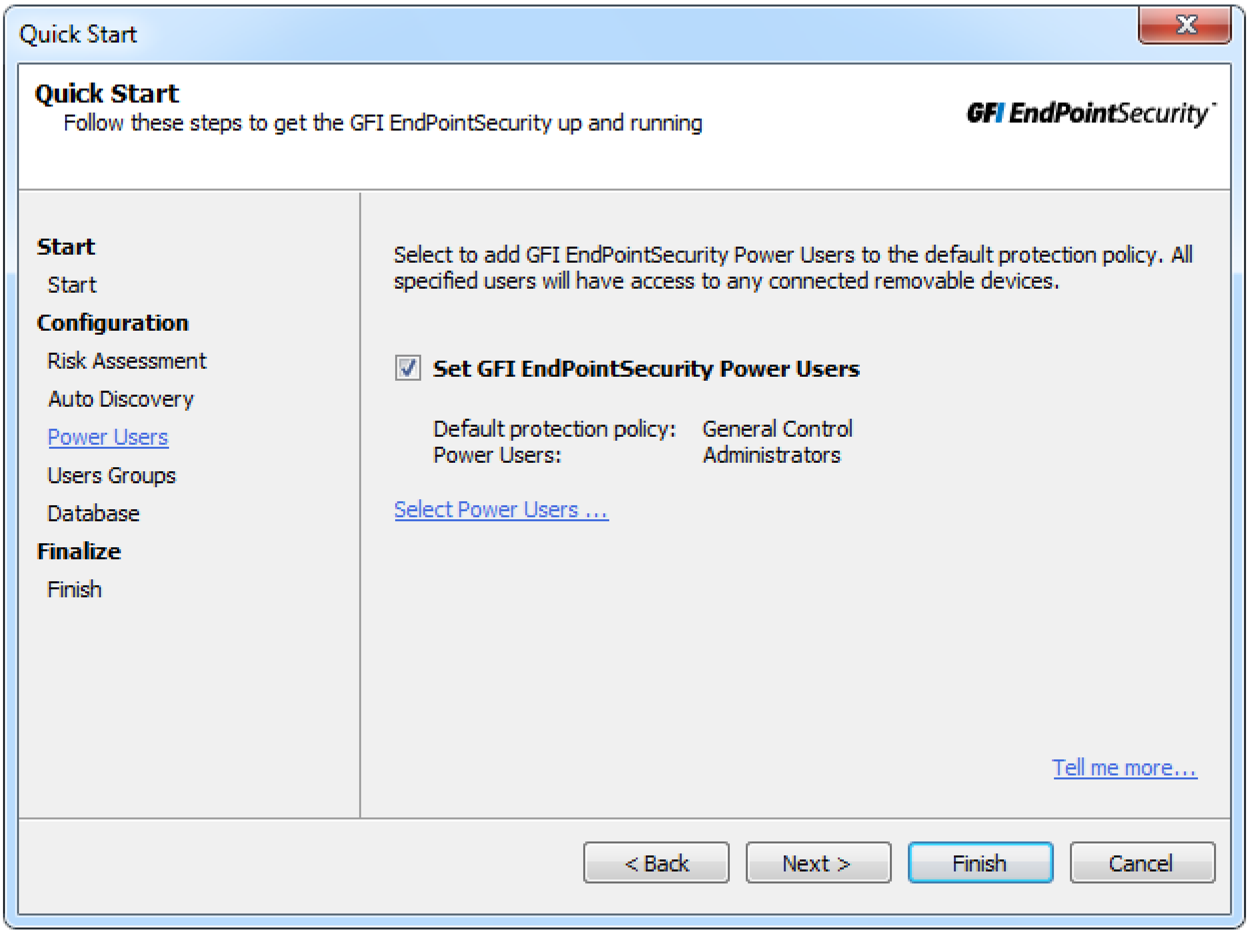
☑ Send alert: -

Screenshot 6: 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.



Quick Start

Quick Start

Follow these steps to get the GFI EndPointSecurity up and running

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**

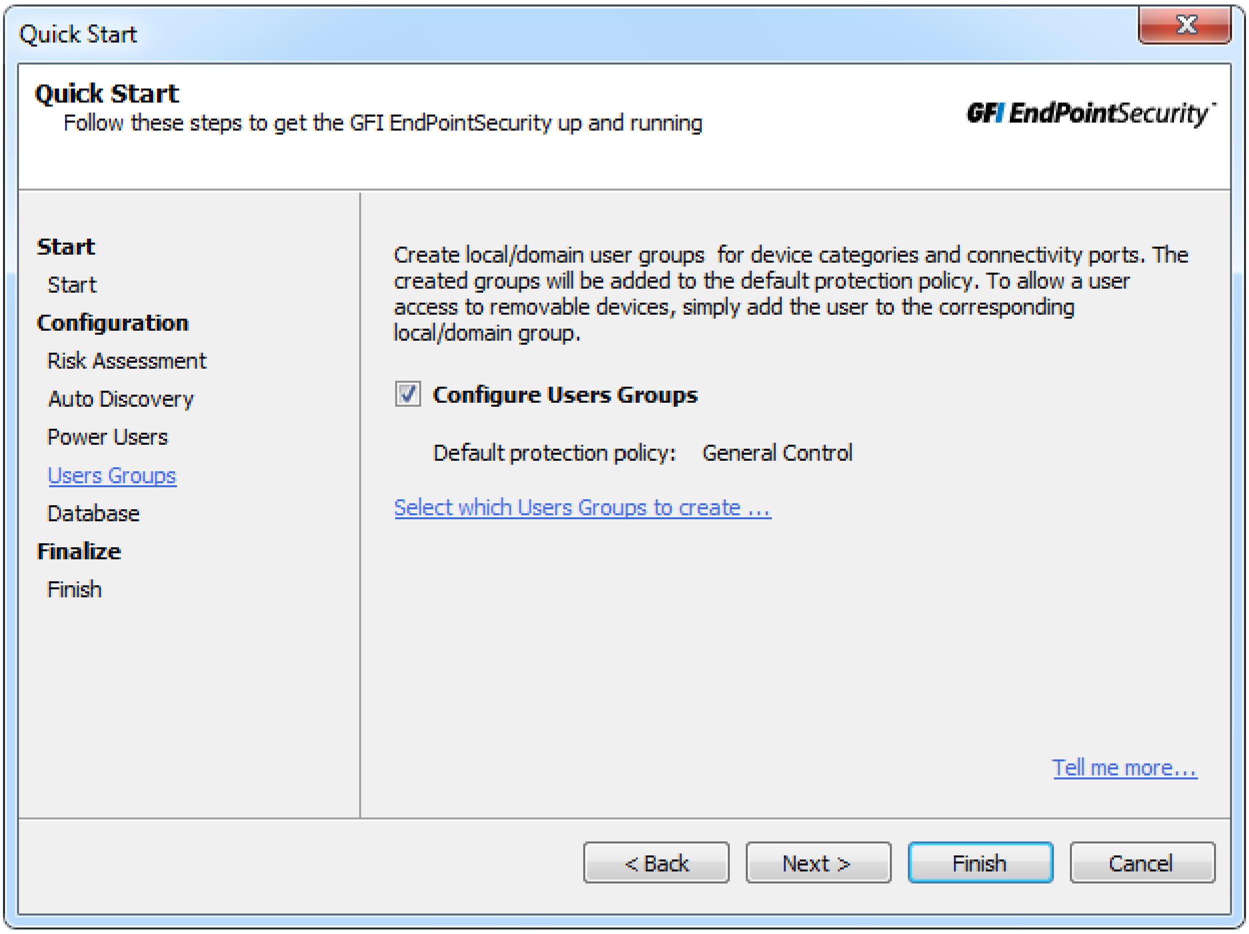
Default protection policy: General Control
Power Users: Administrators

Screenshot 7: 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

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**

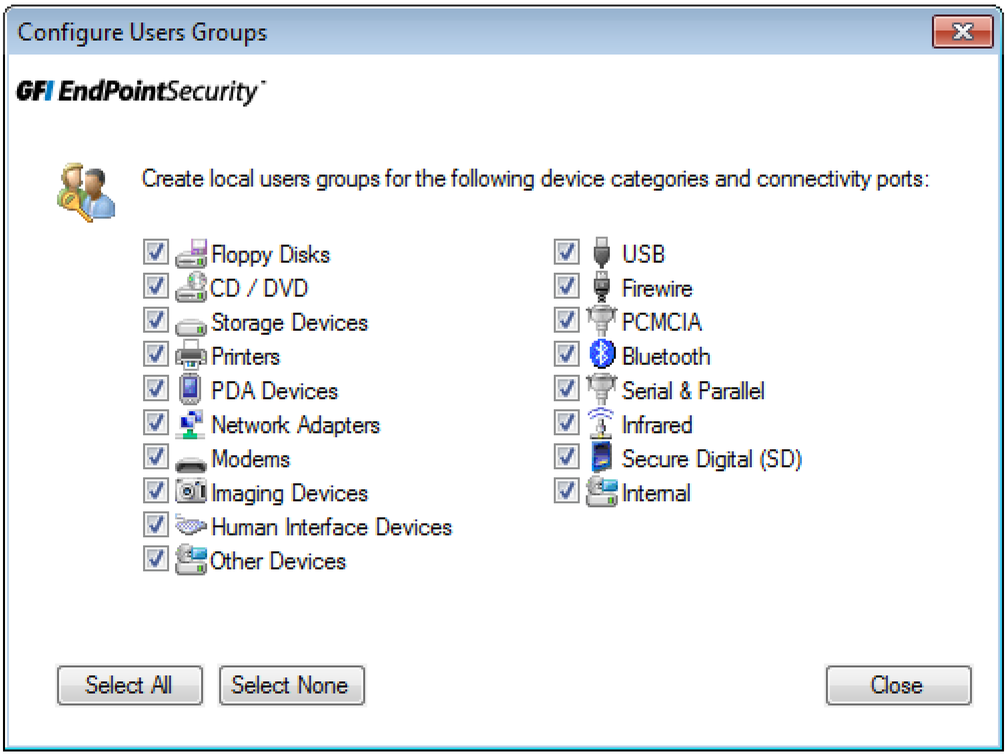
Default protection policy: General Control

Select which Users Groups to create ...

Tell me more...

Screenshot 8: 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.



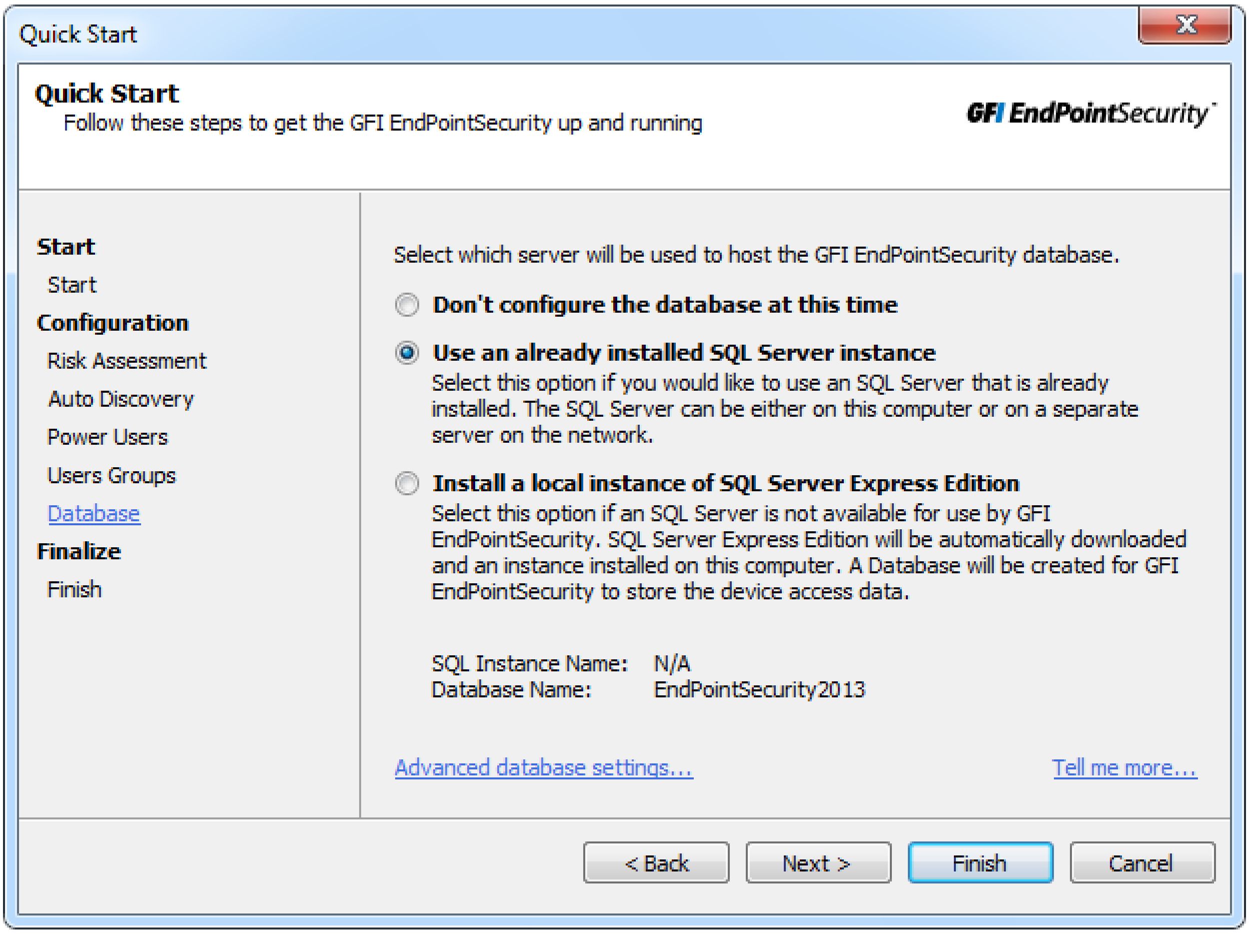
Create local users groups for the following device categories and connectivity ports:

☑ 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 9: 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.

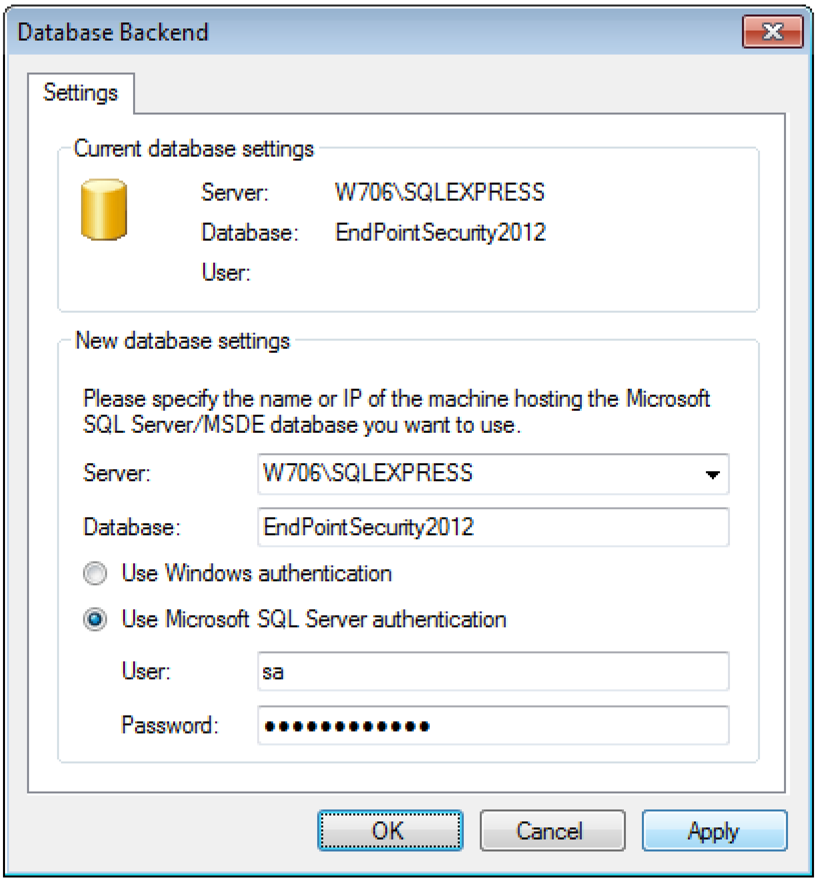
○ **Install a local instance of SQL Server Express Edition**
Select this option if an SQL Server is not available for use by GFI EndPointSecurity. SQL Server Express Edition will be automatically downloaded and an instance installed on this computer. A Database will be created for GFI EndPointSecurity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

SQL Instance Name: N/A
Database Name: EndPointSecurity2013

Screenshot 10: 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.



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 11: 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.

1.7 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

1.7.1 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.

1.7.2 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.

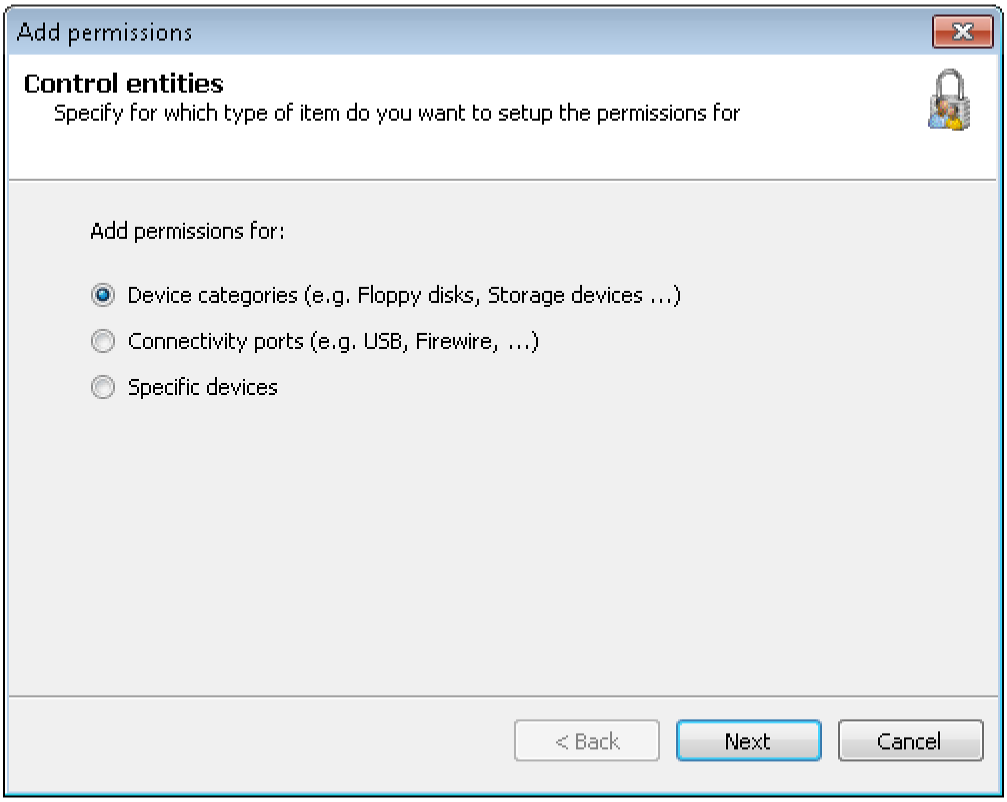
3. Click on the **Configuration** tab.

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:

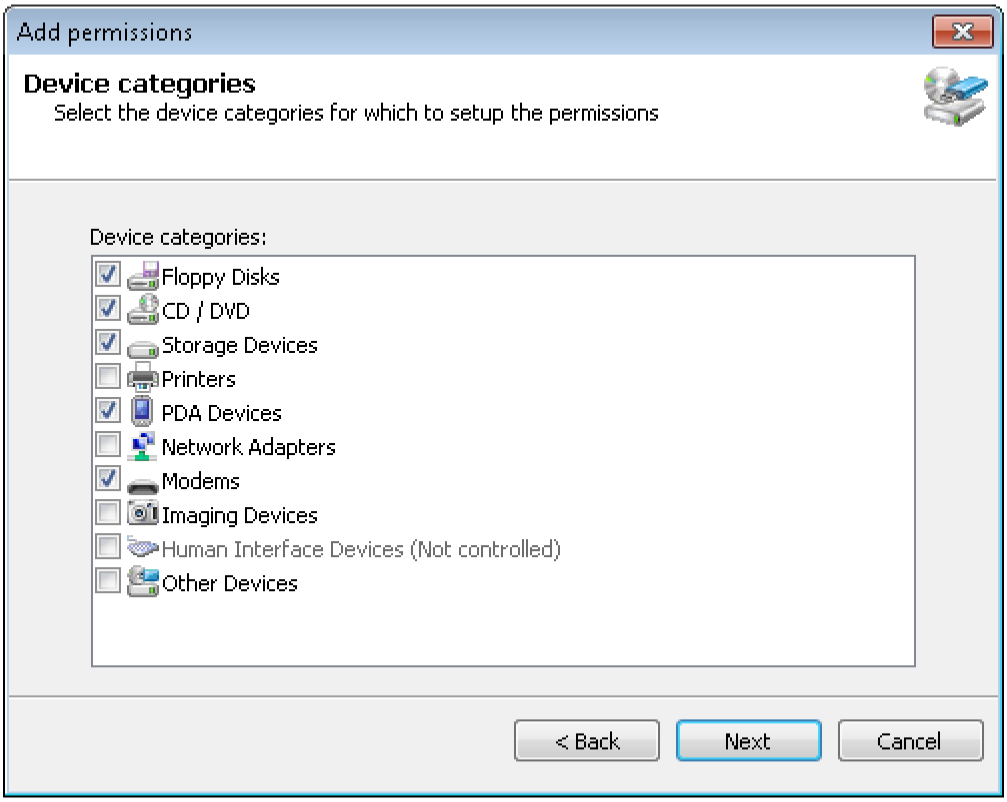
● Device categories (e.g. Floppy disks, Storage devices ...)

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

○ Specific devices

Screenshot 12: Selecting control entities

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



Add permissions

Device categories

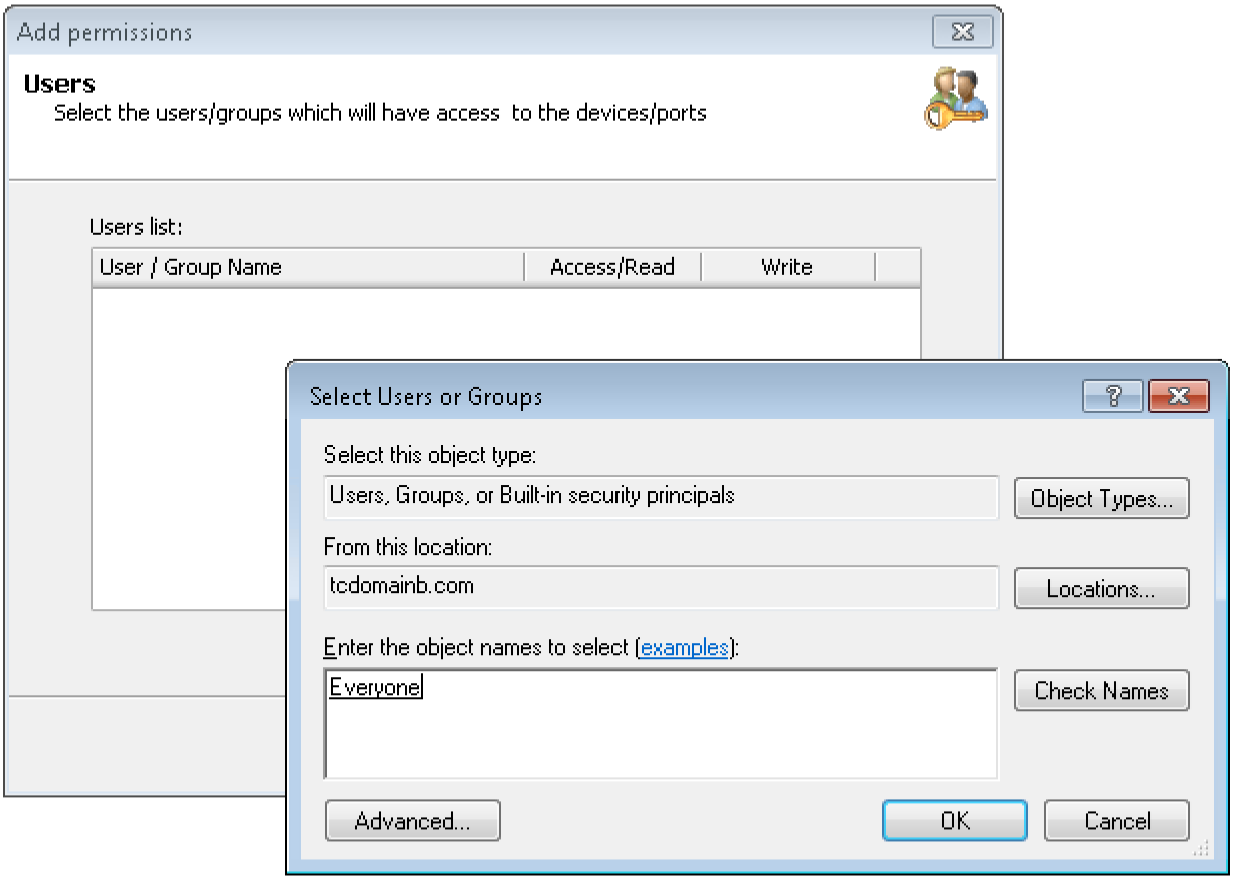
Select the device categories for which to setup the permissions

Device categories:

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

Screenshot 13: Selecting device categories to assign permissions

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



Add permissions

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:

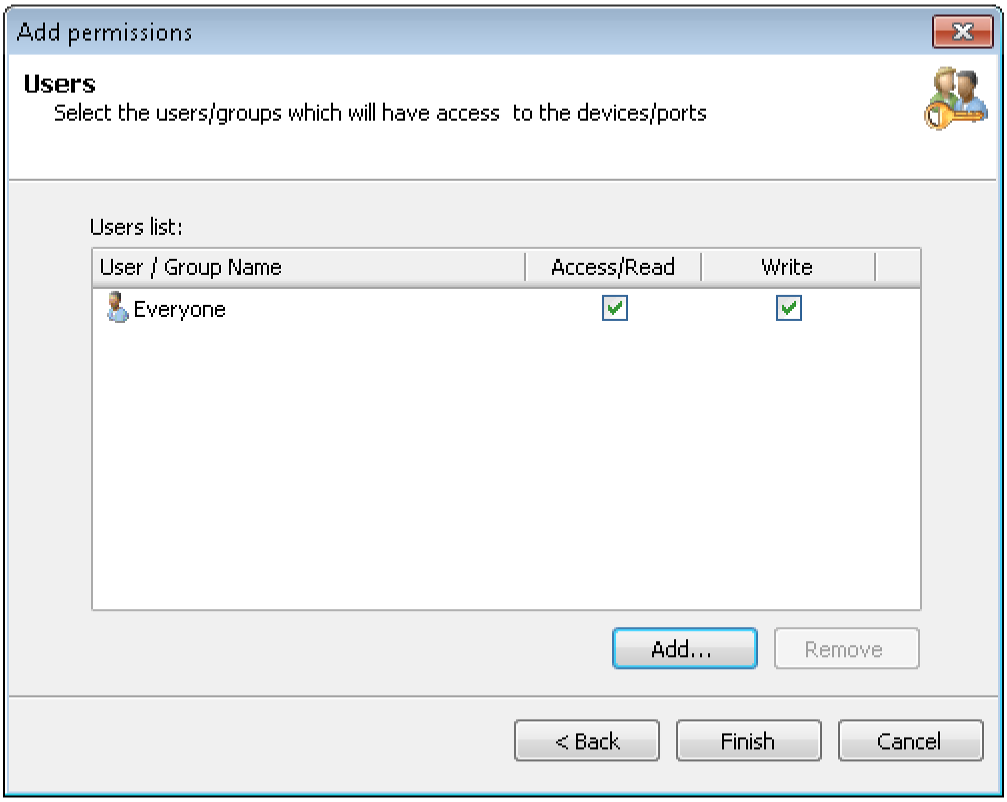
tcdomainb.com

Enter the object names to select (examples):

Everyone

Screenshot 14: 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**



Add permissions

Users

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

Users list:

User / Group Name	Access/Read	Write
Everyone	☑	☑

Screenshot 15: 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.

1.7.3 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.

1.8 Upgrading to the latest version while retaining all settings

This section describes how to upgrade a GFI EndPointSecurity installation to the latest version while retaining all settings.

Important notes when upgrading

- Upgrade is not reversible; you cannot downgrade to the previous version that you had installed.
- It is recommended to export the GFI EndPointSecurity settings before upgrade. Go to **File > Import and export configurations...** and select **Export the desired configurations to a file**. Follow the wizard steps to specify an export filename and the features to export.
- Log in to the GFI Customer Area to get a new license key. Click the blue key icon on the right and select **Upgrade License Key**, or click **Renewal** to extend your maintenance agreement.
- During upgrade, GFI EndPointSecurity services and operation are stopped.
- Check that the machine you are installing GFI EndPointSecurity on meets the latest version's system and hardware requirements.
- Log on as Administrator or use an account with administrative privileges.
- Save any pending work and close all open applications on the machine.
- Disable anti-virus software on the server machine during the upgrade installation. Re-enable it once upgrade is complete.

Upgrade procedure

1. Download the latest build of GFI EndPointSecurity on the server where GFI EndPointSecurity is currently installed. Go to http://go.gfi.com/?pageid=esec_trial, click **Login** and key in your GFI Account credentials.

2. Right-click the newly downloaded installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.

3. Launch the newly downloaded installer and follow on-screen instructions. The wizard installs any missing pre-requisites, uninstalls the current version and installs the latest GFI EndPointSecurity version. When prompted, use the license key obtained from the GFI Customer Area.

4. When prompted to import configurations from the previous version, click **Yes** and choose the configurations to import.

5. Run a test to ensure that GFI EndPointSecurity is functioning correctly. You can either test an existing policy which was previously configured in the old installation or create a dedicated test protection policy. For more information, refer to Testing your installation (page 19).

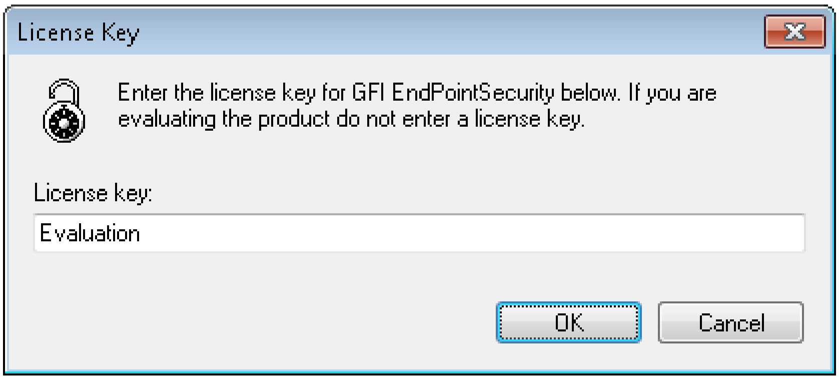
1.9 Product licensing

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 16: 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.

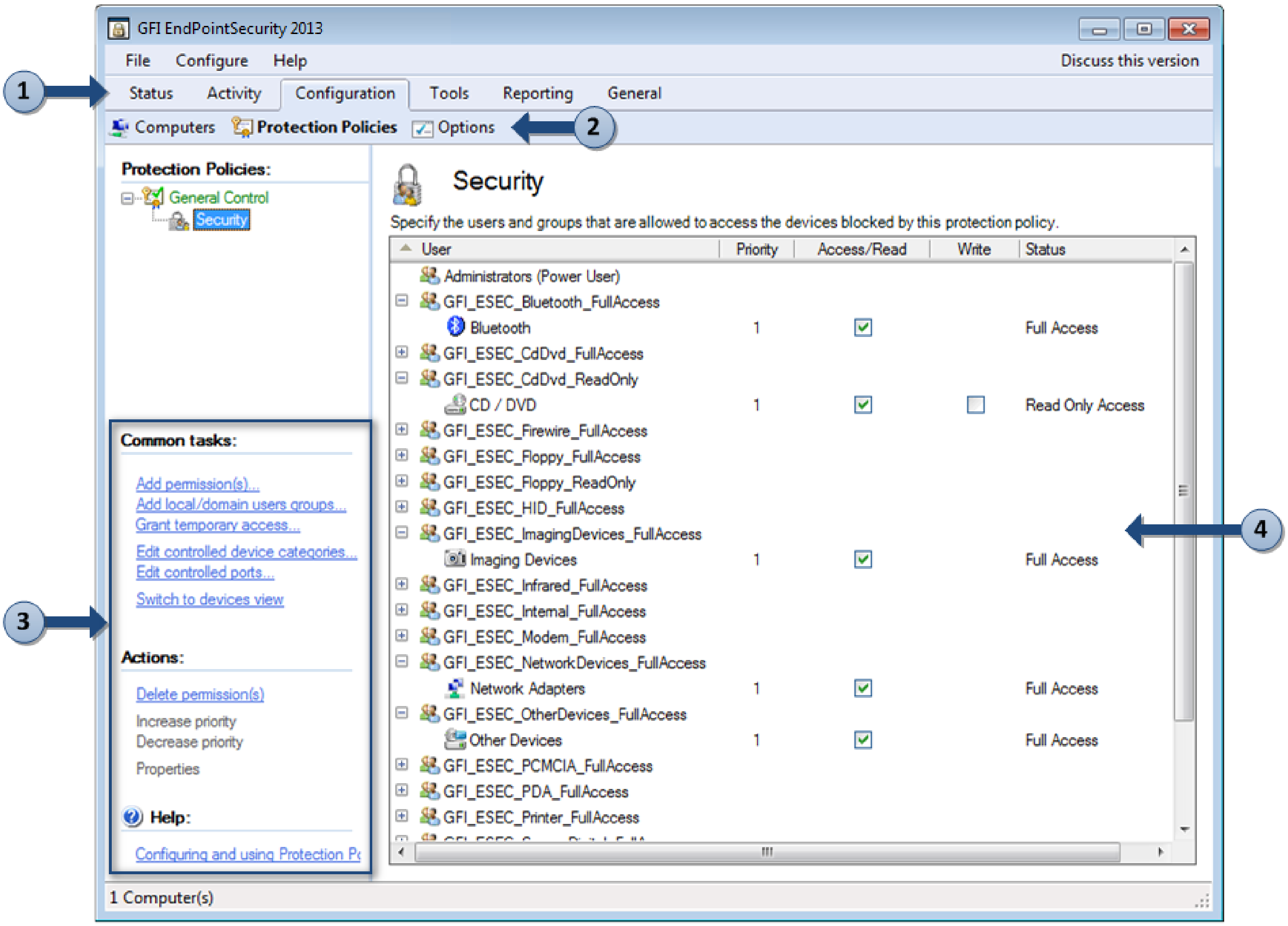
5. Click **OK** to apply the license key.

2 Using

GFI EndPointSecurity is the solution that helps you maintain data integrity by preventing unauthorized access and transfer of content to and from devices or connection ports. The following topics provide information on how to use GFI EndPointSecurity:

2.1 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				

Screenshot 17: 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.

Section	Description
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.

3 Adding Target Computers

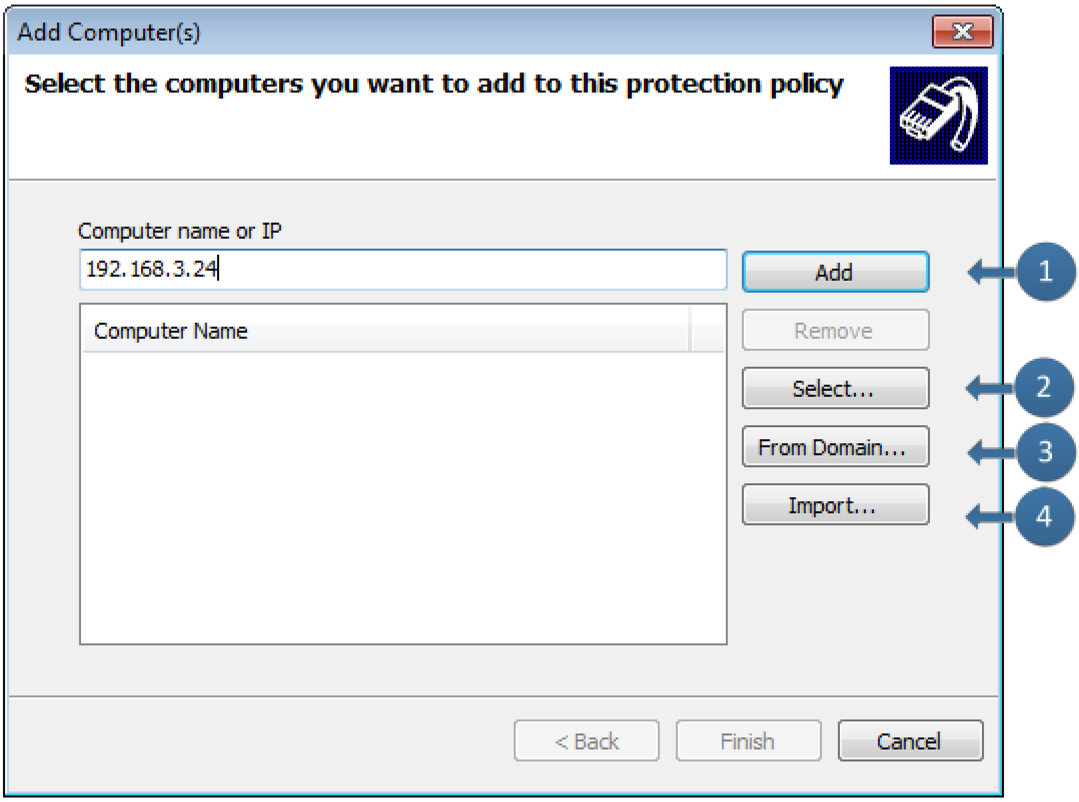
GFI EndPointSecurity enables you to specify the computers you intend to deploy agents and protection policies on.

3.1 Adding computers manually

To manually add a target computer:

1. Click **Configuration** tab **> Computers**.

2. From **Common tasks**, click **Add computer(s)…**.



Screenshot 18: Adding computers manually

3. The table below describes the available options of the **Add Computer(s)** dialog:

Option	Description
1	Key in the name/IP of the target computer to add and click **Add**. Repeat this step for each target computer you want to add to this protection policy.

Option	Description
2	Click **Select…**. In the **Select Computers** dialog select the relevant Domain/Workgroup from the drop-down list and click **Search**. Enable the required computer(s) and click **OK**.
3	Click **From Domain…**. Specify the required computer(s) from within the domain/workgroup where GFI EndPointSecurity resides.
4	Click **Import**. Browse to the location of the text file that contains a list of computers to be imported. **Note** Specify ONLY one computer name/IP per line.

4. Click **Finish**.

3.2 Adding computers automatically

GFI EndPointSecurity enables you to search for and add new computers when they are connected to your network at specified time intervals. This enables you to automatically add computers as soon as they are detected on the network. Through Auto Discovery features, you can configure:

» The frequency and schedule of the searches

» The discovery domain/workgroup to scan

» The policy assigned to newly discovered target computers and the logon credentials.

By default:

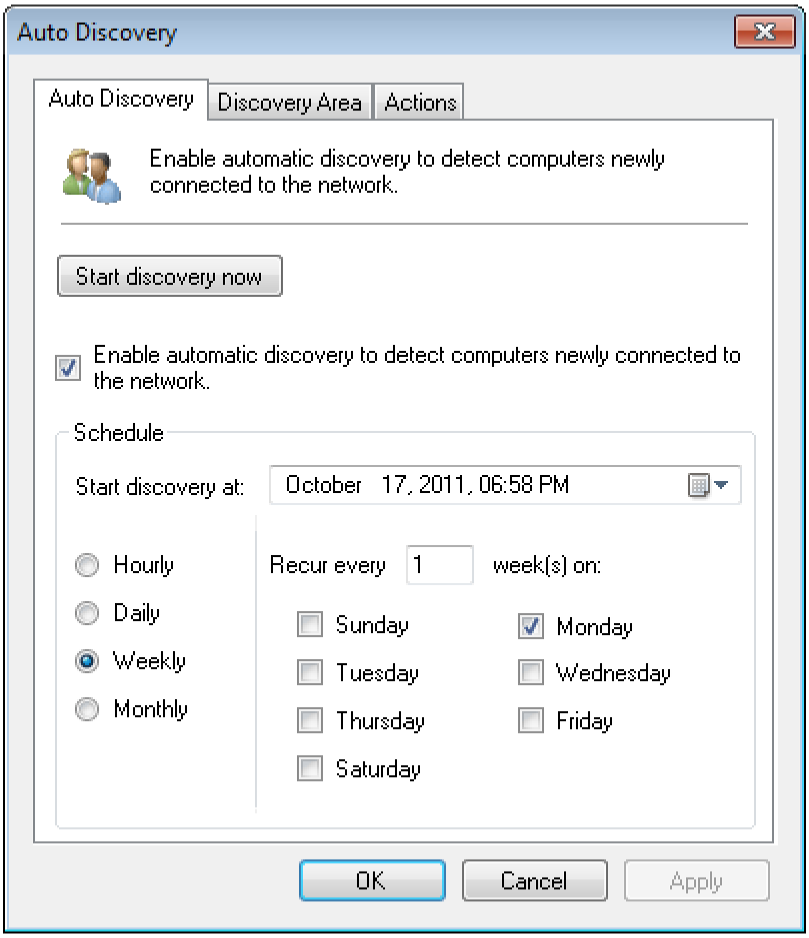
» Auto discovery settings are set to scan the Current domain/workgroup (domain/workgroup where GFI EndPointSecurity resides)

» Install agent’s settings are set to assign the **General Control** protection policy (shipping default protection policy) on to the newly discovered computers.

To configure the Auto Discovery settings:

1. Click **Configuration** tab > **Computers**.

2. From **Common tasks**, click **Auto discovery settings…**.



Enable automatic discovery to detect computers newly connected to the network.

☑ Enable automatic discovery to detect computers newly connected to the network.

Schedule

Start discovery at: October 17, 2011, 06:58 PM

○ Hourly
○ Daily
● Weekly
○ Monthly

Recur every 1 week(s) on:

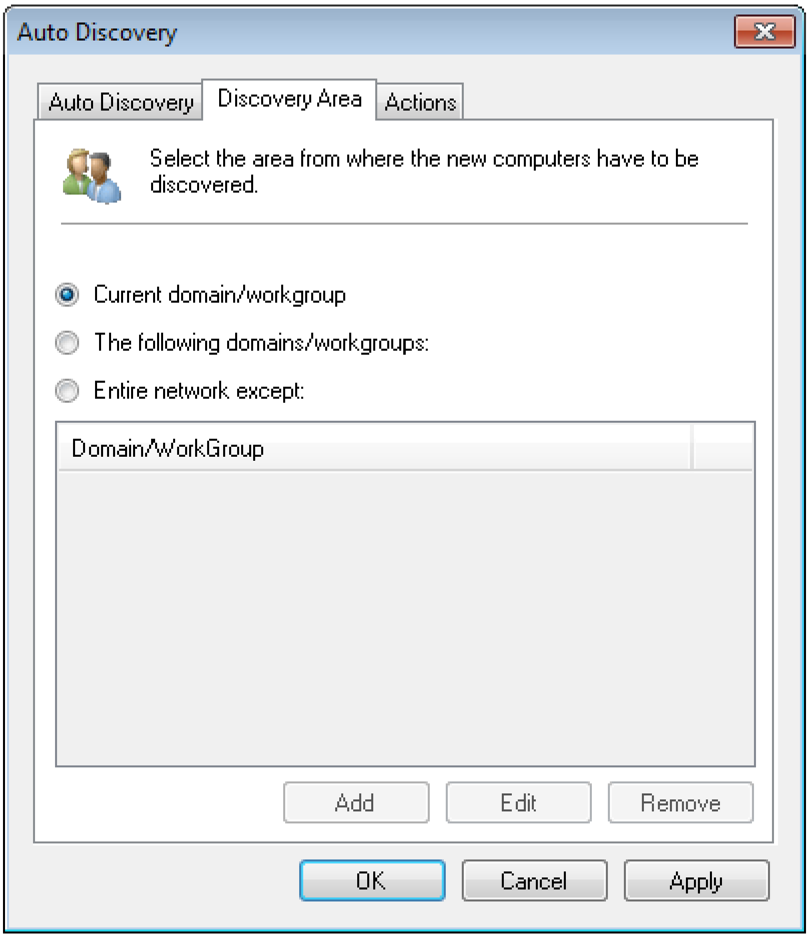
□ Sunday ☑ Monday
□ Tuesday □ Wednesday
□ Thursday □ Friday
□ Saturday

Screenshot 19: Auto Discovery options - Auto Discovery tab

3. Click **Start discovery now** to run auto discovery immediately.

4. Select/unselect **Enable automatic discovery to detect computers newly connected to the network**, to enable/disable Auto Discovery.

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



Auto Discovery

Auto Discovery | Discovery Area | Actions

Select the area from where the new computers have to be discovered.

● Current domain/workgroup

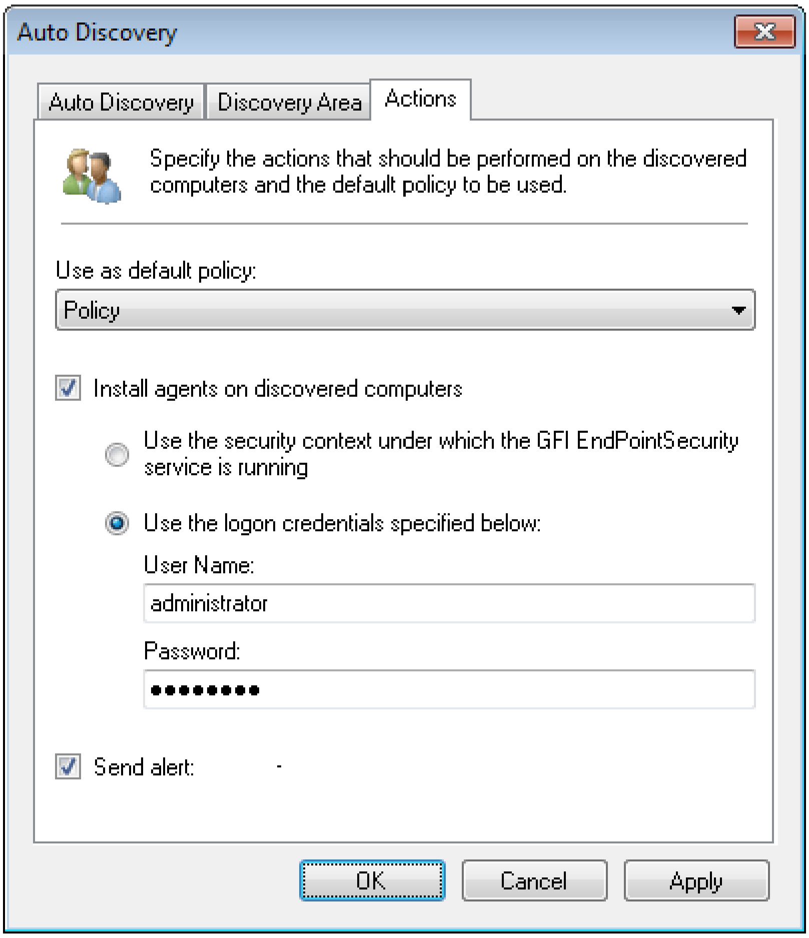
○ The following domains/workgroups:

○ Entire network except:

Domain/WorkGroup

Screenshot 20: Auto Discovery options - Discovery Area tab

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


Auto Discovery

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

Use as default policy: Policy

☑ 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 21: Auto Discovery options - Actions tab

7. Click **Actions** tab and from the **Use as default policy** drop-down menu, select the policy you want to assign to newly discovered computers.

8. Select/unselect **Install agents on discovered computers** to enable/disable auto, agent deployment. Click **Yes** to confirm the enabling of Automatic Protection.

9. Select the logon mode that GFI EndPointSecurity uses to log on to the target computer(s) and deploy agents/protection policies. 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.

10. Select/unselect **Send alert**, to enable/disable alerting options. For more information, refer to Configuring alerting options (page 121).

11. Click **Apply** and **OK**

3.3 Configuring log on credentials

GFI EndPointSecurity requires to log on to the target computers in order to:

- Deploy agents and protection policy updates
- Keep track of the protection status of all target computers.

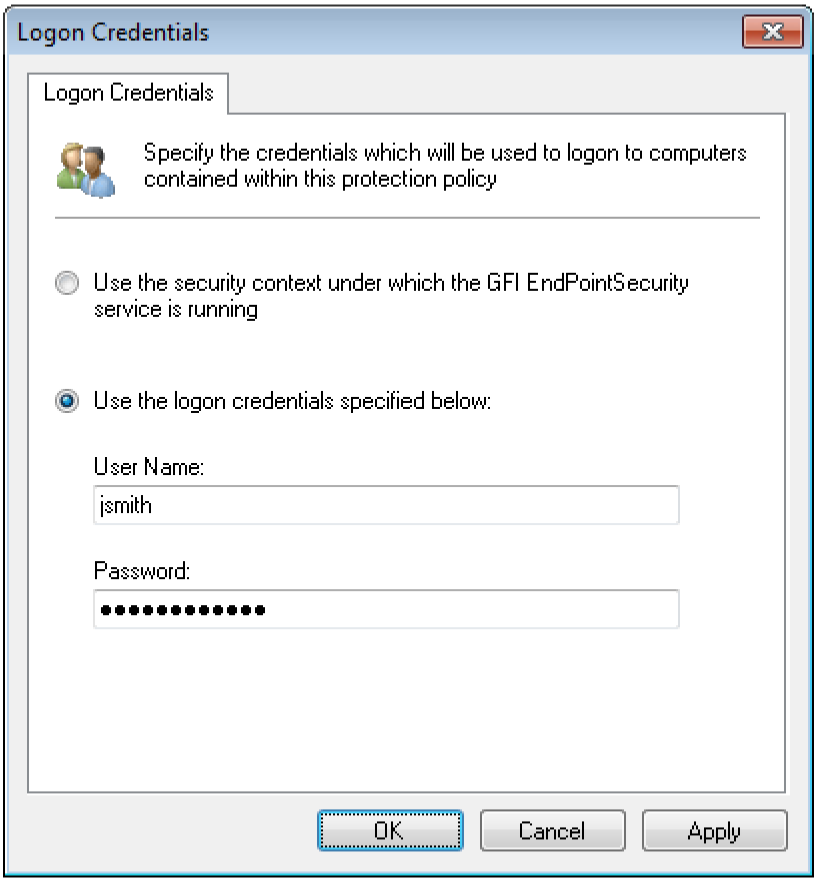
This requires that GFI EndPointSecurity is run under an account that has administrative privileges over your network target computers (example: a domain administrator account).

To specify logon credentials for a target computer:

1. Click **Configuration** tab > **Computers**.

2. Right-click on a computer from the list and click **Set logon credentials...**.

> **Note**
>
> If you want to set multiple computers to log on using the same credentials, highlight the required computers, right-click on one of them and click **Set logon credentials...**. Alternatively, click **Set logon credentials...** from **Actions**.



Specify the credentials which will be used to logon to computers contained within this protection policy

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

● Use the logon credentials specified below:

User Name: jsmith

Password: •••••••••••••

Screenshot 22: Logon Credentials dialog options

3. The table below describes the available logon credentials options:

Option	Description
Use the security context under which GFI EndPointSecurity service is running	Use the same credentials that are running GFI EndPointSecurity.
Use the logon credentials specified below	Specify alternate credentials to use when logging in remote target computers. **Note** Specify credentials which have administrative privileges over scan targets.

4. Click **Apply** and **OK**

Note

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

4 Managing Protection Policies

This chapter describes how to deploy newly created protection policies and schedule them. Prior to deployment you can also modify the settings of your protection policy.

Topics in this chapter

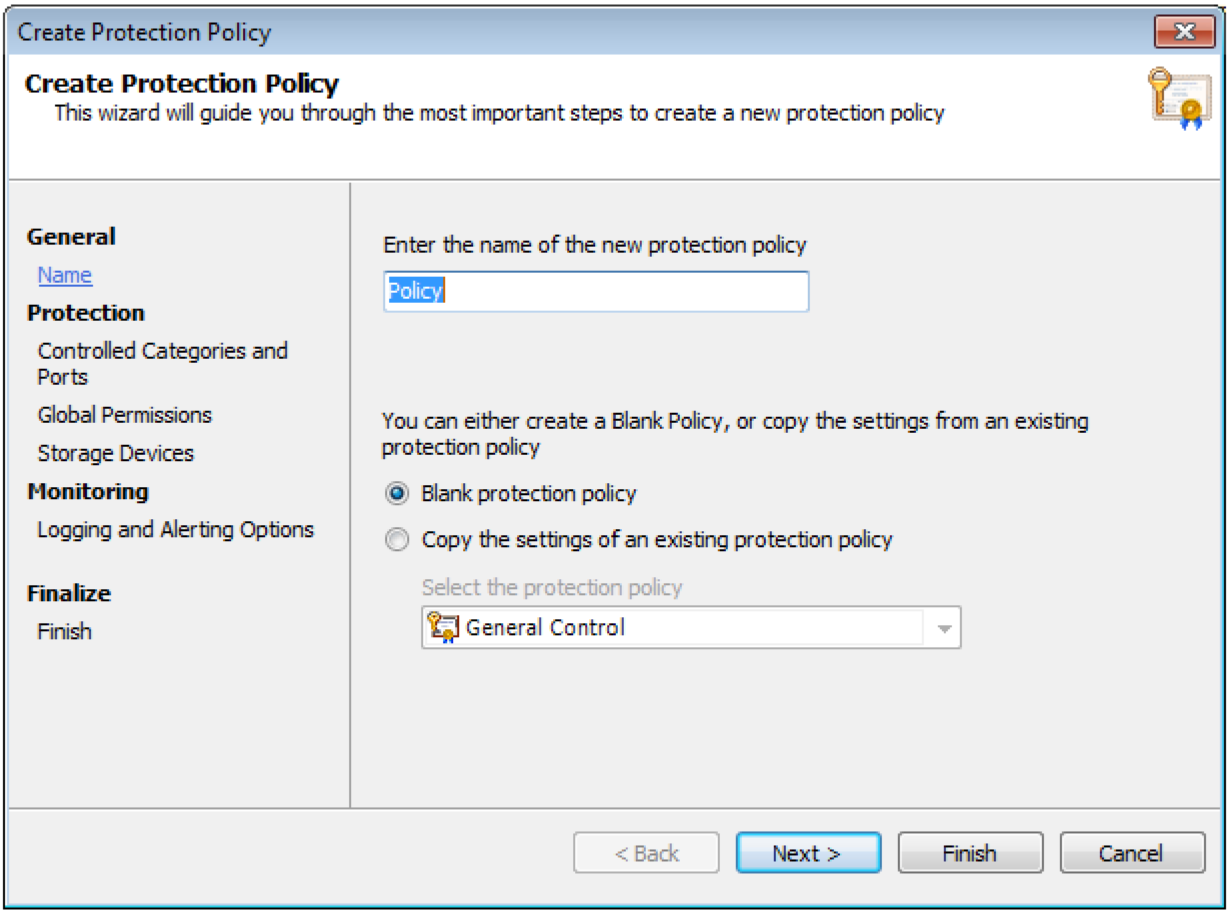
4.1 Creating a new protection policy

GFI EndPointSecurity ships with a default protection policy so that the software is operational upon installation. You can create further protection policies to suit your company's device access security policies.

To create a new protection policy:

1. Click **Configuration** tab **> Protection Policies**.

2. From **Common tasks**, click **Create new protection policy…**.



Create Protection Policy

Create Protection Policy

This wizard will guide you through the most important steps to create a new protection policy

Enter the name of the new protection policy

Policy

You can either create a Blank Policy, or copy the settings from an existing protection policy

● Blank protection policy

○ Copy the settings of an existing protection policy

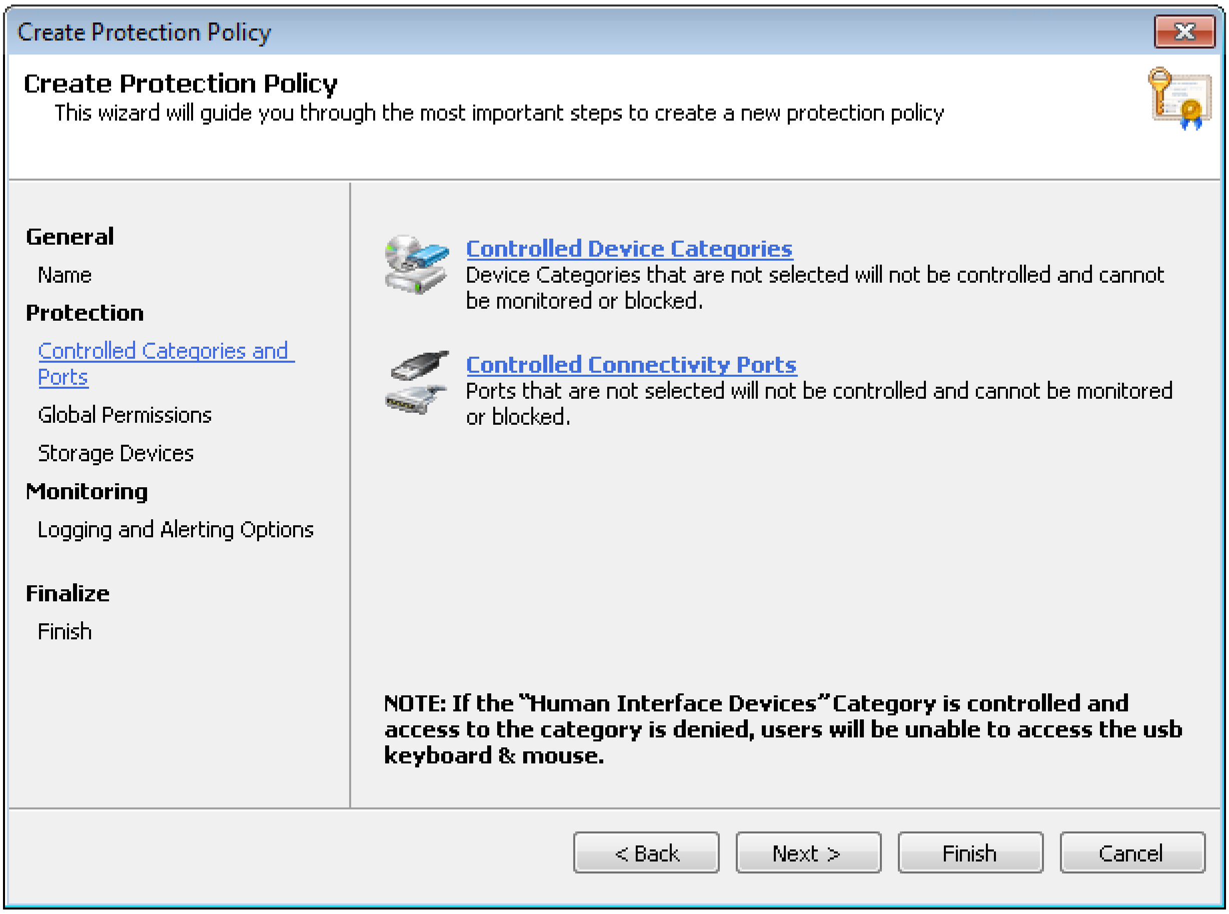
Select the protection policy

General Control

Screenshot 23: Creating a new policy - General settings

3. Key in a unique name for the new protection policy.

4. Select whether you want to create a blank policy or copy the settings from an existing policy. Click **Next**.In the settings area select the required settings inheritance option from:



Create Protection Policy

Create Protection Policy

This wizard will guide you through the most important steps to create a new protection policy

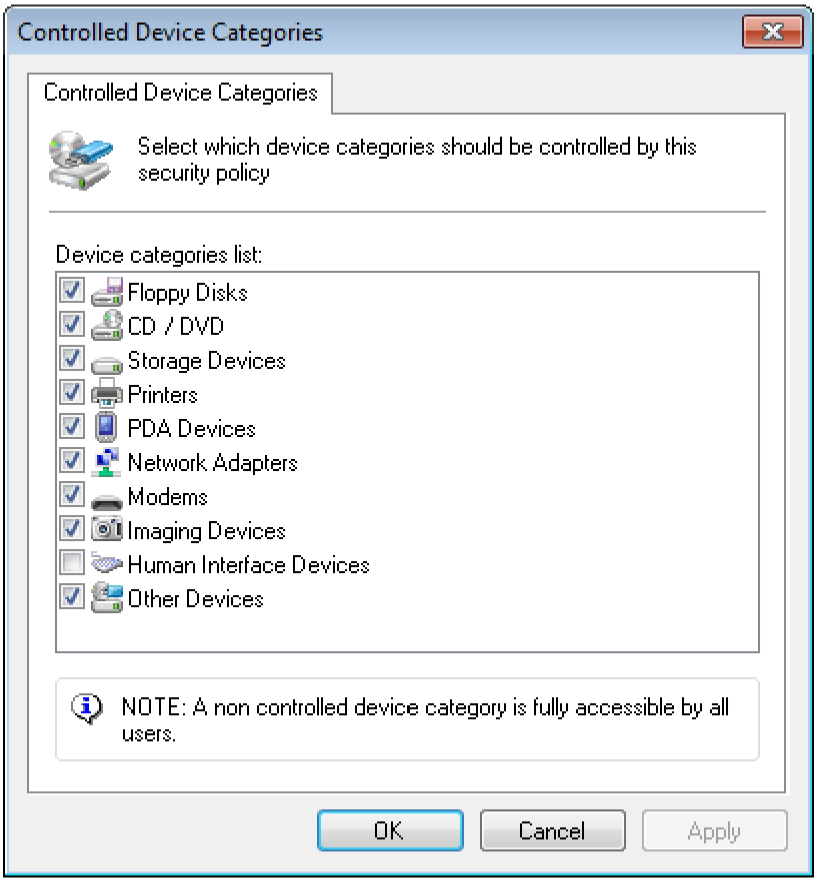
Controlled Device Categories
Device Categories that are not selected will not be controlled and cannot be monitored or blocked.

Controlled Connectivity Ports
Ports that are not selected will not be controlled and cannot be monitored or blocked.

NOTE: If the "Human Interface Devices" Category is controlled and access to the category is denied, users will be unable to access the usb keyboard & mouse.

Screenshot 24: Creating a new policy - Controlled Categories and Ports settings

5. Click **Controlled Device Categories**.



Controlled Device Categories

Select which device categories should be controlled by this security policy

Device categories list:

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

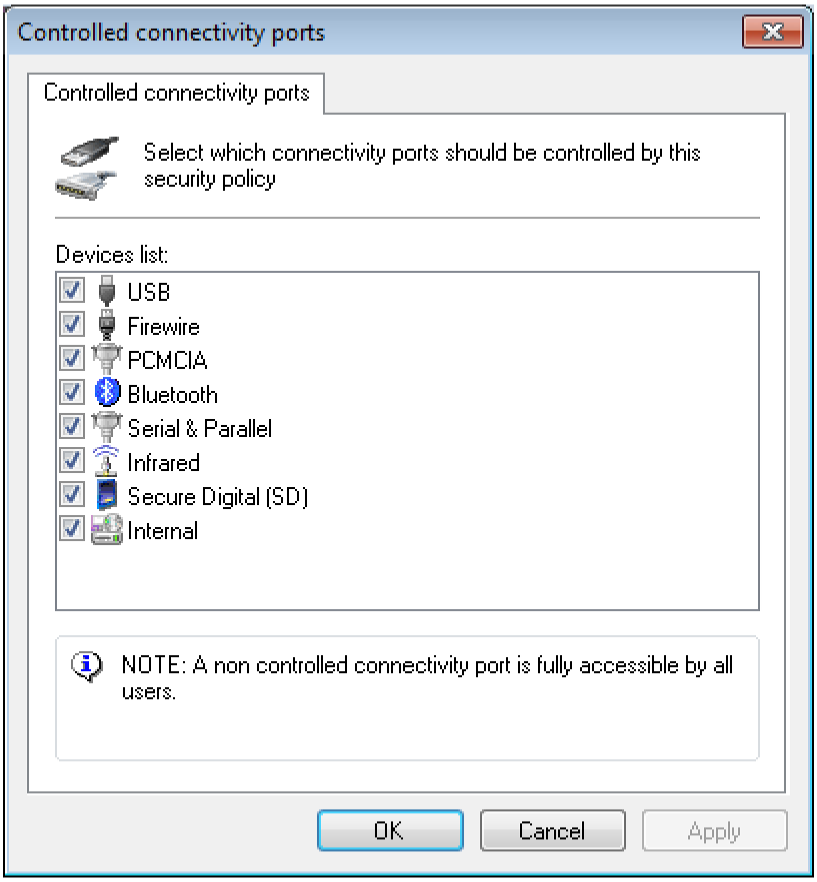
NOTE: A non controlled device category is fully accessible by all users.

Screenshot 25: Controlled Device Categories options

6. From the **Controlled Device Categories** dialog, select the required device categories you want to control by this new policy. Click **OK** to close the **Controlled device categories** dialog and return to the wizard.

> **Important**
>
> If Human Interface Devices is enabled and access is denied, users will not be able to use USB keyboards and mice connected to target computers protected by this policy.

7. Click **Controlled Connectivity Ports**.



Select which connectivity ports should be controlled by this security policy

Devices list:

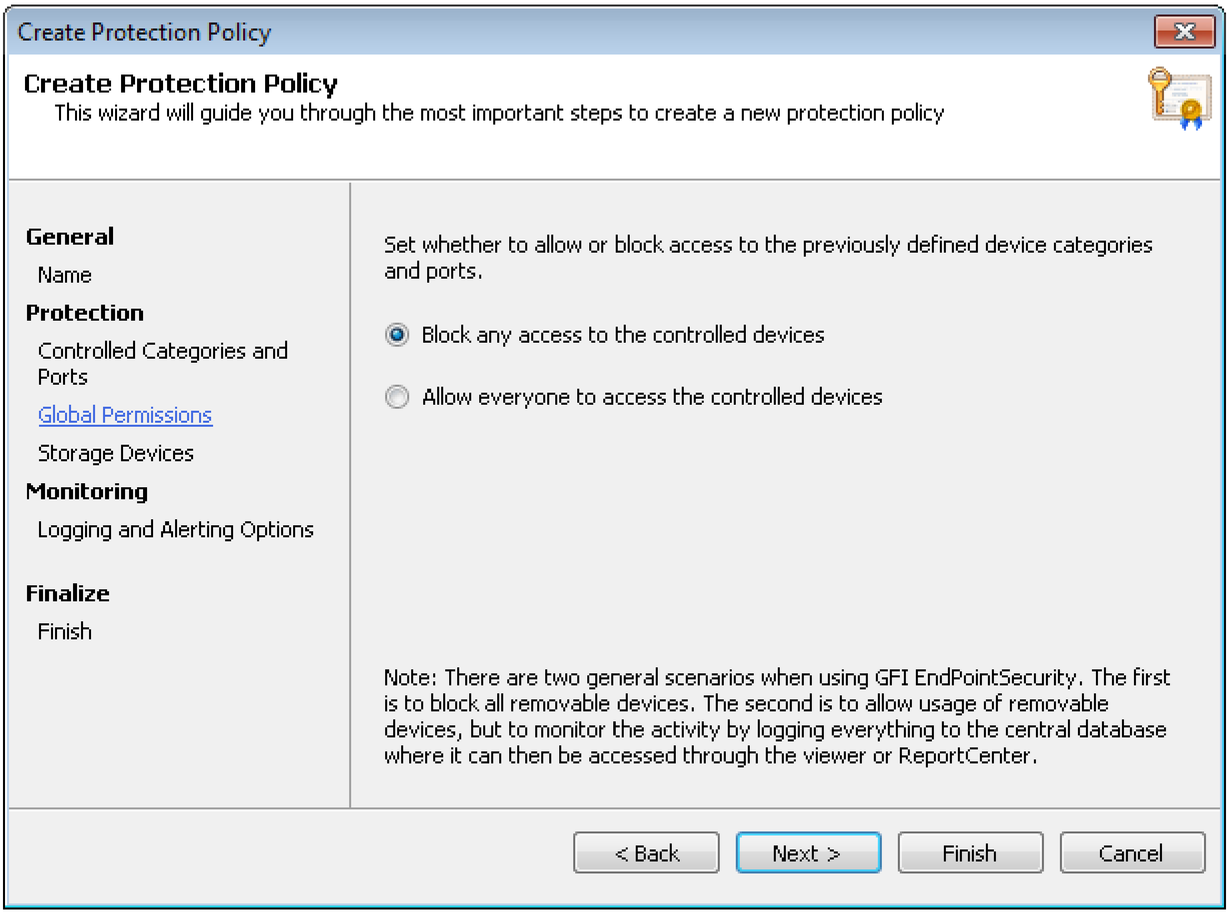
- ☑ USB
- ☑ Firewire
- ☑ PCMCIA
- ☑ Bluetooth
- ☑ Serial & Parallel
- ☑ Infrared
- ☑ Secure Digital (SD)
- ☑ Internal

NOTE: A non controlled connectivity port is fully accessible by all users.

Screenshot 26: Controlled connectivity ports options

8. From the **Controlled connectivity ports** dialog, select the required connectivity ports that you want to control by this new policy. Click **OK** to close the **Controlled connectivity ports** dialog and return to the wizard.

9. Click **Next**.



Create Protection Policy

Create Protection Policy

This wizard will guide you through the most important steps to create a new protection policy

General

Name

Protection

Controlled Categories and Ports

Global Permissions

Storage Devices

Monitoring

Logging and Alerting Options

Finalize

Finish

Set whether to allow or block access to the previously defined device categories and ports.

● Block any access to the controlled devices

○ Allow everyone to access the controlled devices

Note: There are two general scenarios when using GFI EndPointSecurity. The first is to block all removable devices. The second is to allow usage of removable devices, but to monitor the activity by logging everything to the central database where it can then be accessed through the viewer or ReportCenter.

Screenshot 27: Creating a new policy - Global Permissions settings

10. From the **Global Permissions** dialog, select the required global access permissions from:

- **Block any access to the controlled devices** - to block access to all selected devices/ports.
- **Allow everyone to access the controlled devices** - to allow access to all selected devices/ports. If this option is selected, activity monitoring will still be carried out on target computers covered by the protection policy.

11. Click **Next**.

12. Click **File-Type Filter** and add the file-types to block/allow by this policy.

> **Note**
>
> GFI EndPointSecurity enables you to restrict access based on file-types. It is also able to identify the real content of most common file-types, (example: .DOC or .XLS files), and take the necessary actions applicable for the true file-type. This is most useful when file extensions are maliciously manipulated. For more information, refer to Configuring file-type filters (page 69).

13. Click **OK** to close the **File-Type Filter** dialog and return to the wizard.

14. Click **Encryption** and enable/configure the preferred encryption engine.

> **Note**
>
> In addition, GFI EndPointSecurity can also allow or block Active Directory (AD) users and/or user groups, from accessing 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. For more information, refer to Configuring security encryption (page 76).

15. Click **OK** to close the **Encryption** dialog and return to the wizard.

16. Click **Next**.

17. From **Storage Devices**, select the required options that you want to control from the tabs described below:

Tab	Description
File-Type Filter	GFI EndPointSecurity enables you to specify file-type restrictions on files, such as .DOC or .XLS files, being copied to/from allowed devices. You can apply these restrictions to Active Directory (AD) users and/or user groups.
Content Awareness	GFI EndPointSecurity enables you to specify the file content restrictions for a particular protection policy. The content awareness feature looks into files transiting the endpoints via removable devices and it \identifies content based on pre-configured and custom regular expressions and dictionary files. By default the module looks for secure confidential details such as social security numbers and primary account numbers as well as information related to companies and enterprises such as names of diseases, drugs, dangerous chemicals and also trivial language or ethnic / racist terms. » You can configure content checking as a global policy in a similar fashion to the file checking module.
File Options	GFI EndPointSecurity enables you to specify the options required to block or allow files based on size. GFI EndPointSecurity also enables you to ignore large files when checking file type and content and archived files.
Encryption	GFI EndPointSecurity enables you to configure settings that specifically cater for encrypted devices. It also enables you to encrypt devices that are not yet secured.

> **Note**
>
> For more information refer to For more information, refer to Customizing Protection Policies (page 45).

18. Configure logging and alerting options for this policy and click **Next**.

> **Note**
>
> For more information, refer to Configuring event logging and Configuring alerts.

19. Review the summary page for information about your policy and click **Finish**.

4.2 Assigning a Protection Policy

The next step is to link the relevant set of device access and connectivity port permissions to each target computer. You can do this by assigning protection policies to target computers.

> **Note**
>
> Target computers can only be assigned one protection policy at a time.

To assign a protection policy on to a target computer:

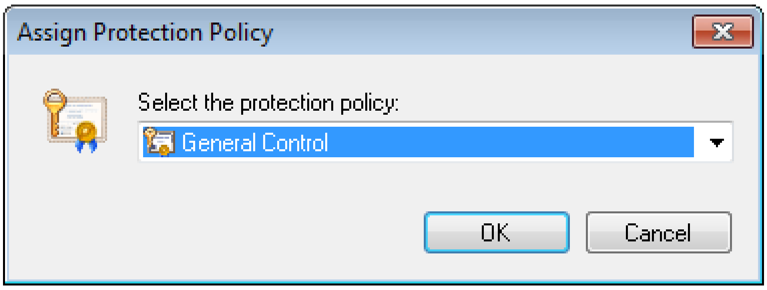
1. From the GFI EndPointSecurity management console, select **Configuration**.

2. Click **Computers**.

3. Highlight the required target computer(s).

> **Note**
>
> If assigning the same policy to more than one target computer, select all the required target computers and then specify the protection policy for the selected set of target computers.

4. From the left pane, click the **Assign Protection Policy**hyperlink in the **Actions** section.



Select the protection policy: General Control

Screenshot 28: Assign Protection Policy Options

5. In the **Assign Protection Policy** dialog select the required protection policy from the drop down list, and click **OK**

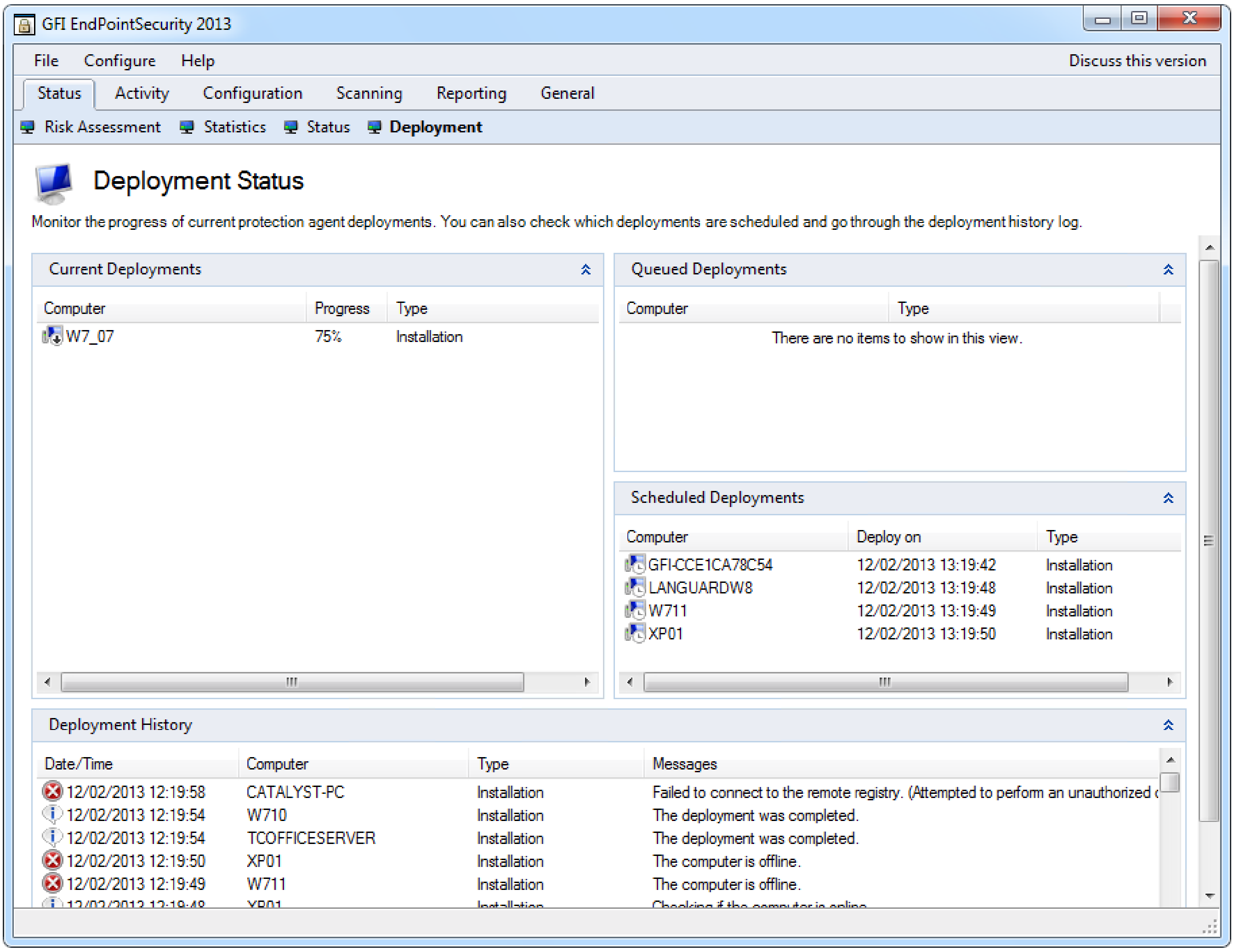
4.2.1 Deploy immediately

To immediately deploy a protection policy on target computers:

1. Click **Configuration** tab > **Computers** sub-tab.

2. Highlight the required target computer(s). If more than one deployment is required, you can highlight all the required target computers at once and then deploy the protection policies to the selected set of target computers.

3. From **Actions**, click **Deploy now…**. The view should automatically change to **Status > Deployment**.



Deployment Status

Monitor the progress of current protection agent deployments. You can also check which deployments are scheduled and go through the deployment history log.

Current Deployments

Computer	Progress	Type
W7_07	75%	Installation

Queued Deployments

Computer	Type

There are no items to show in this view.

Scheduled Deployments

Computer	Deploy on	Type
GFI-CCE1CA78C54	12/02/2013 13:19:42	Installation
LANGUARDW8	12/02/2013 13:19:48	Installation
W711	12/02/2013 13:19:49	Installation
XP01	12/02/2013 13:19:50	Installation

Deployment History

Date/Time	Computer	Type	Messages
12/02/2013 12:19:58	CATALYST-PC	Installation	Failed to connect to the remote registry. (Attempted to perform an unauthorized (
12/02/2013 12:19:54	W710	Installation	The deployment was completed.
12/02/2013 12:19:54	TCOFFICESERVER	Installation	The deployment was completed.
12/02/2013 12:19:50	XP01	Installation	The computer is offline.
12/02/2013 12:19:49	W711	Installation	The computer is offline.
12/02/2013 12:19:48	XP01	Installation	Checking if the computer is online

Screenshot 29: Deploying a policy immediately - Deployment sub-tab

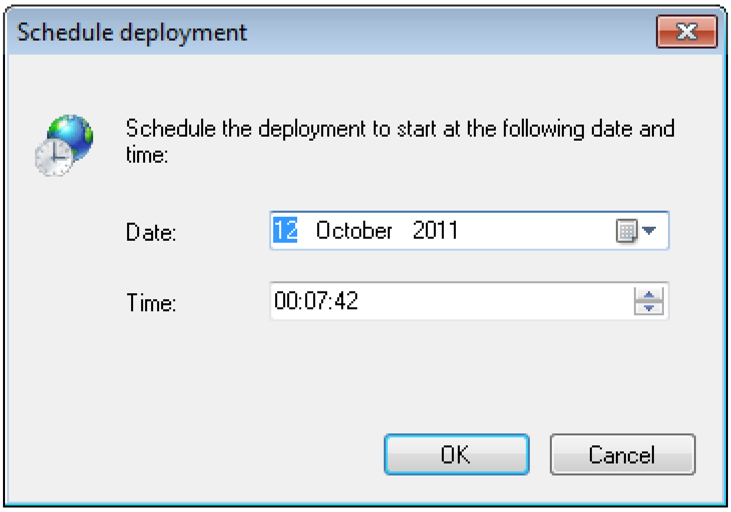
4.2.2 Scheduled policy deployment

To schedule deployment of a protection policy:

1. Click **Configuration** tab **> Computers**.

2. Highlight the required target computer(s). If more than one deployment is required, you can highlight all the required target computers at once and then deploy the policies to the selected set of target computers.

3. From **Actions**, click **Schedule deployment…**.



Schedule the deployment to start at the following date and time:

Date: 12 October 2011

Time: 00:07:42

Screenshot 30: Schedule deployment options

4. From **Schedule deployment** dialog select the deployment date and time, and click **OK**

> **Note**
> If the 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.

4.2.3 Deploying policies through Active Directory

You can create a Windows installer package (.msi installation file) that you can then deploy through Active Directory Group Policies across target computers in your domain.

To create the Windows installer package:

1. Click **Configuration** tab **> Protection Policies**.

2. From the left pane, select the protection policy for which you want to create the Windows installer package.

3. From the right pane, click **Deploy through Active Directory** in the **Deployment** section.

4. Key in the **File name** of the .msi file and browse to select the destination path.

5. Click **Save**.

> **Note**
> For information on how to deploy software using Active Directory Group Policies in Microsoft Windows Server 2003 and Microsoft Windows Server 2008, refer to http://support.microsoft.com/kb/816102

4.3 Verifying protection policy deployment

Once a protection policy is deployed, it is recommended to verify that target computers were affected by the policy. Verify if the deployment was successful from:

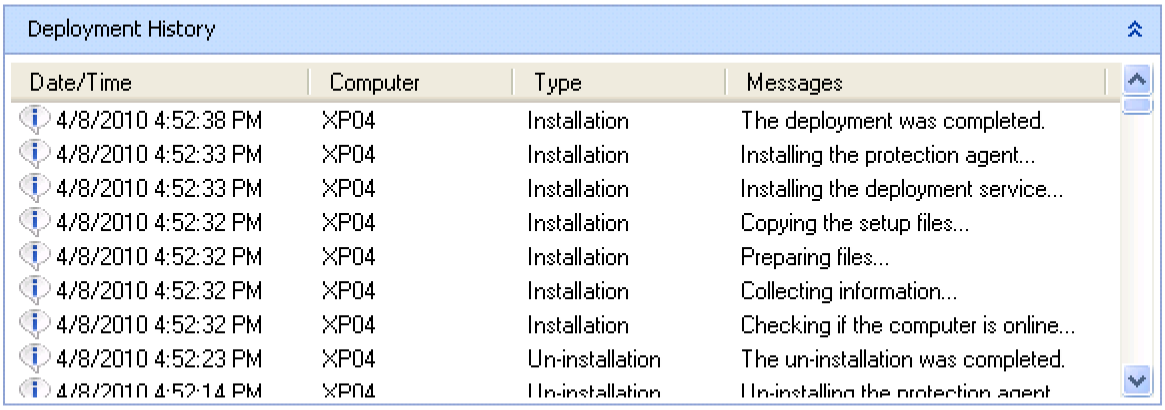
- Deployment history area
- Agents' status area

4.3.1 Deployment History

Use the information displayed in the Deployment History area to determine whether deployment for each target computer completed successfully, or whether errors were encountered.

To view the deployment history:

1. Click **Status> Deployment**.



Deployment History

Date/Time	Computer	Type	Messages
4/8/2010 4:52:38 PM	XP04	Installation	The deployment was completed.
4/8/2010 4:52:33 PM	XP04	Installation	Installing the protection agent...
4/8/2010 4:52:33 PM	XP04	Installation	Installing the deployment service...
4/8/2010 4:52:32 PM	XP04	Installation	Copying the setup files...
4/8/2010 4:52:32 PM	XP04	Installation	Preparing files...
4/8/2010 4:52:32 PM	XP04	Installation	Collecting information...
4/8/2010 4:52:32 PM	XP04	Installation	Checking if the computer is online...
4/8/2010 4:52:23 PM	XP04	Un-installation	The un-installation was completed.
4/8/2010 4:52:14 PM	XP04	Un-installation	Un-installing the protection agent

Screenshot 31: Deployment History area

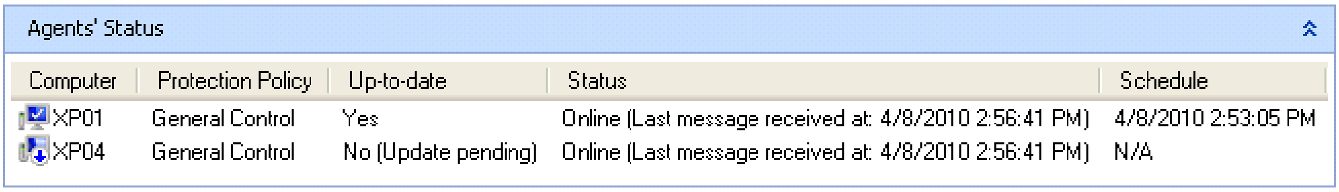
2. From **Deployment History**, confirm the successful completion of the update onto the local computer. For more information, refer to Deployment status view (page 109).

4.3.2 Agents' status

Use the information displayed in the Agents' Status area to determine the status of all deployment operations performed on your network target computers.

To view agents' status:

3. Click **Status> Agents**.



Agents' Status

Computer	Protection Policy	Up-to-date	Status	Schedule
XP01	General Control	Yes	Online (Last message received at: 4/8/2010 2:56:41 PM)	4/8/2010 2:53:05 PM
XP04	General Control	No (Update pending)	Online (Last message received at: 4/8/2010 2:56:41 PM)	N/A

Screenshot 32: Agent's Status area

4. From **Agents' Status**, confirm the successful assignment of the correct protection policy to the target computer(s) and that agent deployment is up-to-date.

Note

Each agent sends its online status to the main GFI EndPointSecurity installation at regular intervals. If this data is not received by the main installation, the agent is considered to be offline.

Note

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.

For more information about the agents status area, refer to the Agents status view section in the Monitoring statuses chapter.

5 Customizing Protection Policies

This topic provides you with information related to modifying the settings of your pre-configured protection policies. This enables you to tweak settings by time, as you discover new security obstacles and possible vulnerabilities.

5.1 Configuring controlled device categories

GFI EndPointSecurity enables you to select which supported device categories should be controlled or not by a protection policy. You can do this on a policy-by-policy basis.

> **Note**
>
> Unspecified devices will be fully accessible from the target computers covered by the protection policy. As a result, GFI EndPointSecurity cannot monitor and block devices falling in a category that is not controlled by the protection policy.

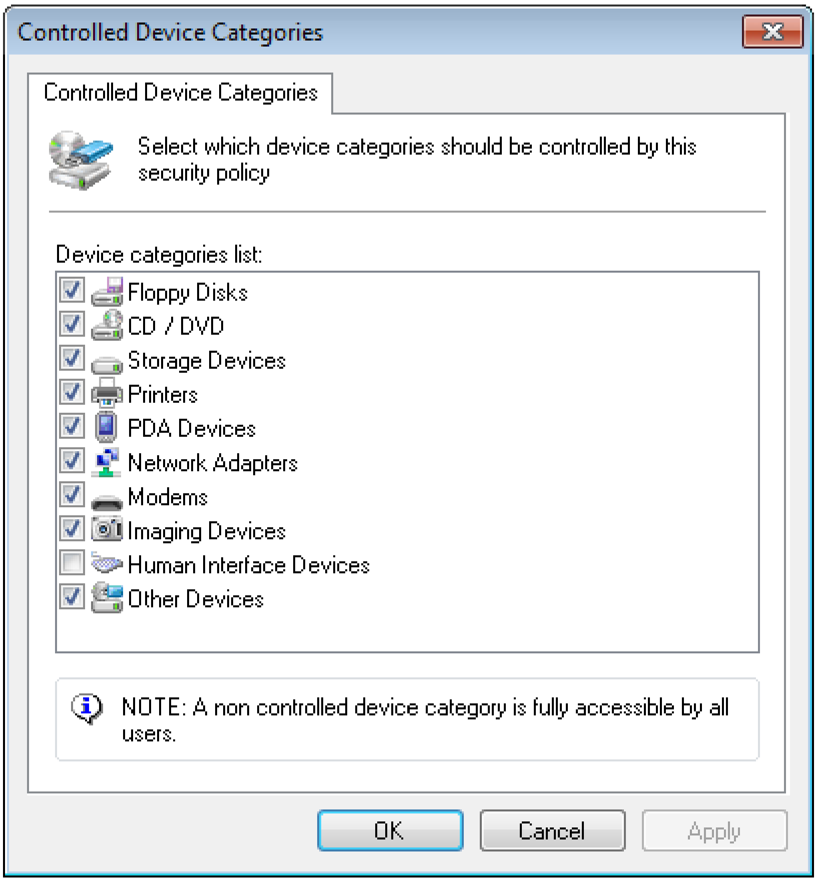
To configure devices controlled by a protection policy:

1. Click **Configuration** tab **> Protection Policies**.

2. From **Protection Policies > Security**, select the protection policy to configure.

3. Click **Security**.

4. From **Common tasks**, click **Edit controlled device categories…**.



Select which device categories should be controlled by this security policy

Device categories list:

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

NOTE: A non controlled device category is fully accessible by all users.

Screenshot 33: Controlled Device Categories options

5. From the **Controlled Device Categories** dialog, select/unselect the required device categories that will be controlled by the protection policy, and click **OK**.

> **Important**
> If you enable Human Interface Devices and deny access such devices, users will not be able to use USB keyboards and mice connected to target computers protected by this policy.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.

2. From **Common tasks**, click **Deploy to all computers…**.

5.2 Configuring controlled connectivity ports

GFI EndPointSecurity enables you to select which supported connectivity ports should be controlled or not by a protection policy. You can do this on a policy-by-policy basis.

> **Note**
> Unspecified ports will be fully accessible from the target computers covered by the protection policy. As a result, GFI EndPointSecurity cannot monitor and block devices connected to a port that is not controlled by the protection policy.

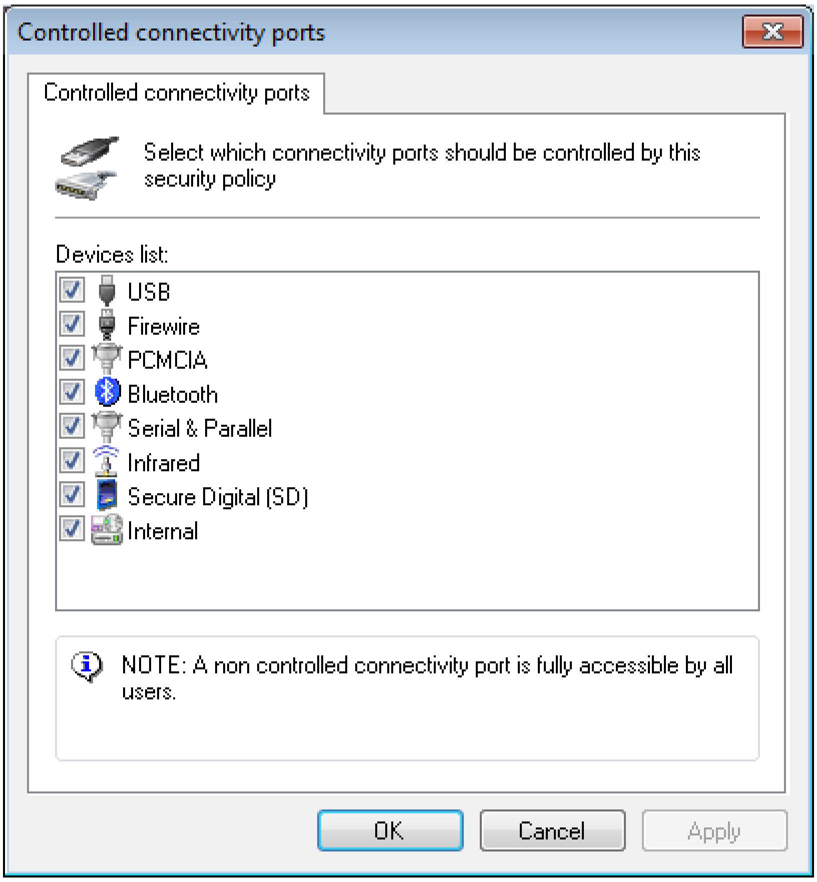
To configure which ports will be controlled by a specific protection policy:

1. Click **Configuration** tab **> Protection Policies**.

2. From **Protection Policies > Security**, select the protection policy to configure.

3. Click **Security**.

4. From **Common tasks**, click **Edit controlled ports…**.



Select which connectivity ports should be controlled by this security policy

Devices list:

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

NOTE: A non controlled connectivity port is fully accessible by all users.

Screenshot 34: Controlled connectivity ports options

5. From the **Controlled connectivity ports** dialog, select/unselect the required connectivity ports that will be controlled by the protection policy, and click **OK**

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.

2. From **Common tasks**, click **Deploy to all computers…**.

5.3 Configuring power users

GFI EndPointSecurity enable you to specify Active Directory (AD) users and/or user groups, as power users. Power users are automatically given full access to devices connected to any target computer covered by a protection policy. You can define sets of power users on a policy-by-policy basis.

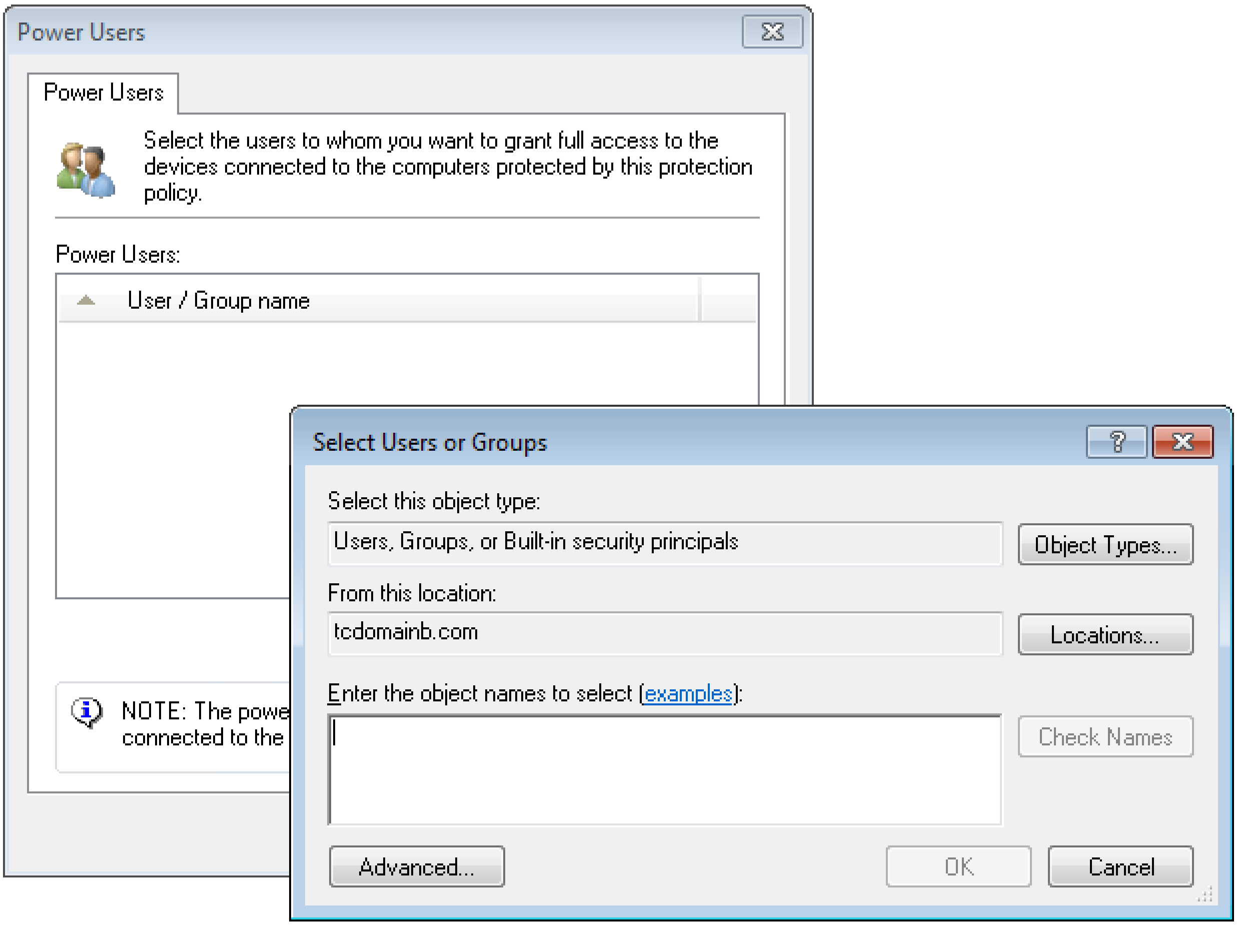
You should exercise caution when using this feature, since incorrectly specifying a user as a power user will lead to that user overriding all restrictions of the relevant protection policy.

To specify power users of a protection policy:

1. Click **Configuration** tab > **Protection Policies**.

2. From **Protection Policies > Security**, select the protection policy to configure.

3. From the right pane, click **Power users** in the **Security** section.



Power Users
Power Users
Select the users to whom you want to grant full access to the devices connected to the computers protected by this protection policy.
Power Users:
User / Group name
NOTE: The powe
connected to the
Select Users or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
tcdomainb.com
Locations...
Enter the object names to select (examples):
Check Names
Advanced...
OK
Cancel

Screenshot 35: Power users options

4. In the Power Users dialog:

» **Option 1**: Click **Add…** to specify the user(s)/group(s) that 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**

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.

2. From **Common tasks**, click **Deploy to all computers…**.

5.4 Configuring access permissions for device categories

GFI EndPointSecurity enables you to set permissions by device categories to Active Directory (AD) users and/or user groups. You can do this on a policy-by-policy basis.

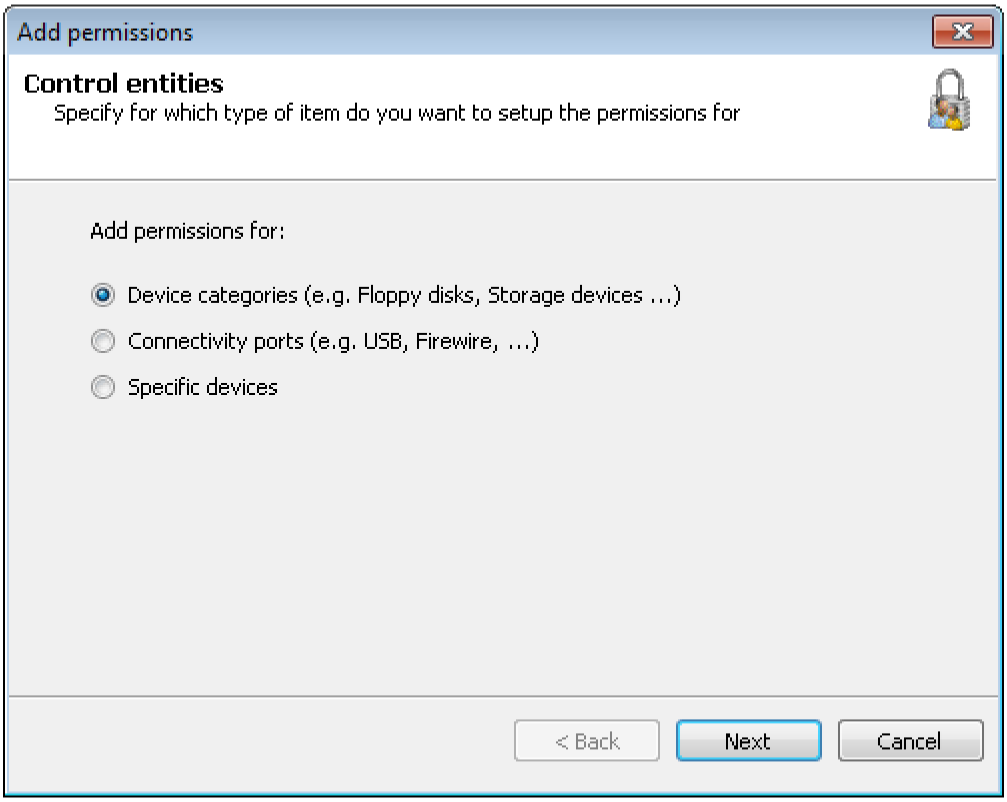
When a device category is not set to be controlled by the particular security policy, the relevant entry is disabled. For more information, refer to Configuring controlled device categories (page 45).

To configure device category access permissions for users in a protection policy:

1. Click **Configuration** tab > **Protection Policies**.

2. From **Protection Policies > Security**, select the protection policy to configure.

3. From **Common tasks**, click **Add permission(s)…**.



Add permissions

Control entities

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

Add permissions for:

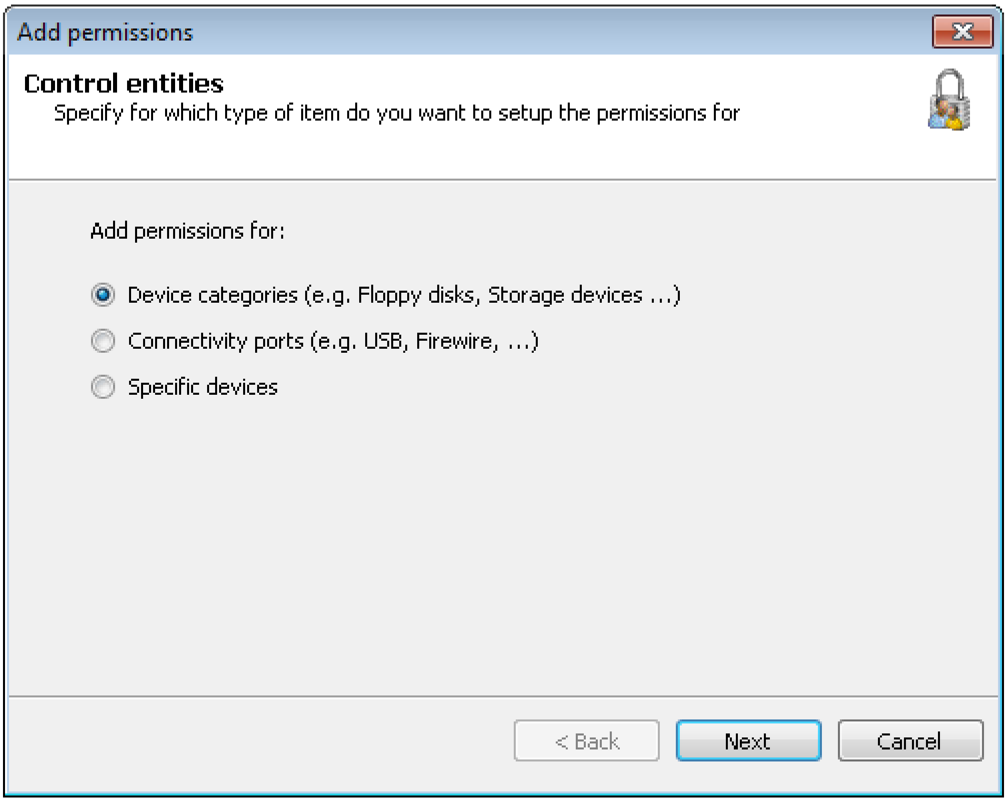
● Device categories (e.g. Floppy disks, Storage devices ...)

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

○ Specific devices

Screenshot 36: Add permissions options - Control entities

4. In the **Add permissions** dialog select **Device categories** and click **Next**.


Add permissions

Control entities

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

Add permissions for:

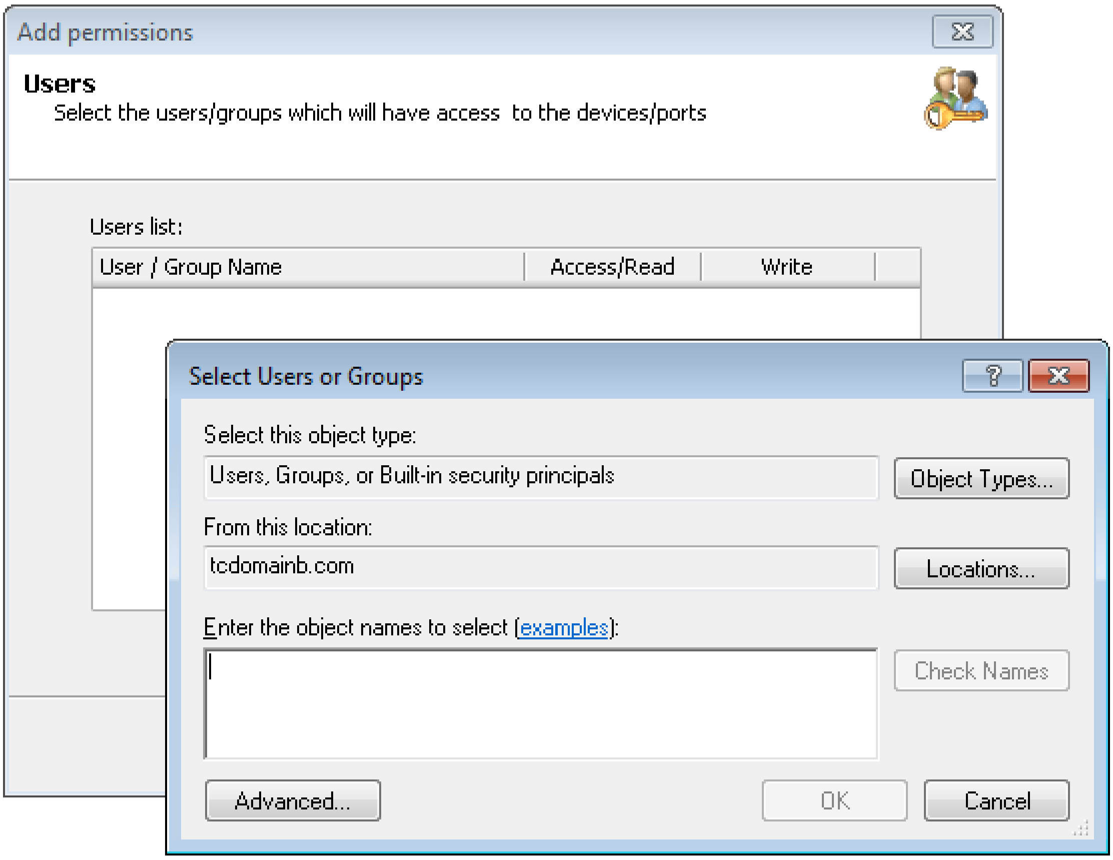
● Device categories (e.g. Floppy disks, Storage devices ...)

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

○ Specific devices

Screenshot 37: Add permissions options - Device categories

5. Enable or disable the required device categories for which to configure permissions, and click **Next**.


Add permissions

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

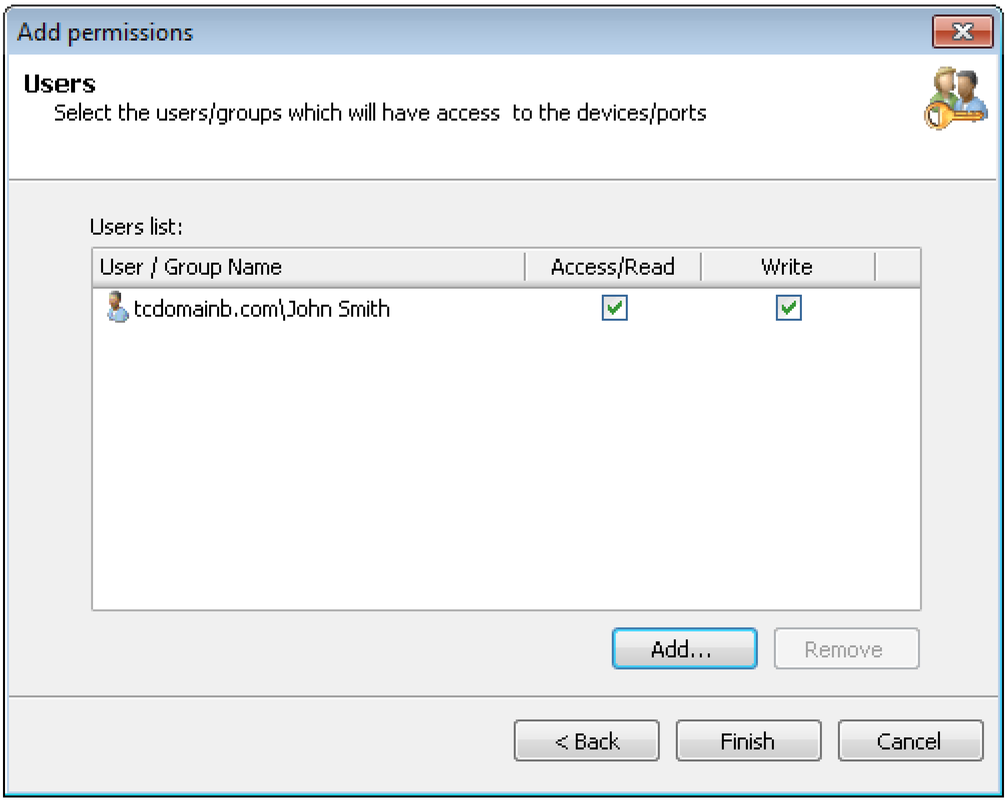
From this location:

tcdomainb.com

Enter the object names to select (examples):

Screenshot 38: Add permissions options - Users

6. Click **Add…** to specify the user(s)/group(s) that will have access to the device categories specified in this protection policy, and click **OK**



Add permissions

Users

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

Users list:

User / Group Name	Access/Read	Write
tcdomainb.com\John Smith	☑	☑

Screenshot 39: Add permissions options - Users

7. Enable or disable Access/Read and Write permissions for each user/group you specified and click **Finish**.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.

2. From **Common tasks**, click **Deploy to all computers…**.

5.5 Configuring access permissions for connectivity ports

GFI EndPointSecurity provides you with the facility to set permissions by connectivity ports to Active Directory (AD) users and/or user groups. You can do this on a policy-by-policy basis.

When a connectivity port is not set to be controlled by a protection policy, the relevant permission is disabled. For more information, refer to Configuring controlled connectivity ports (page 46).

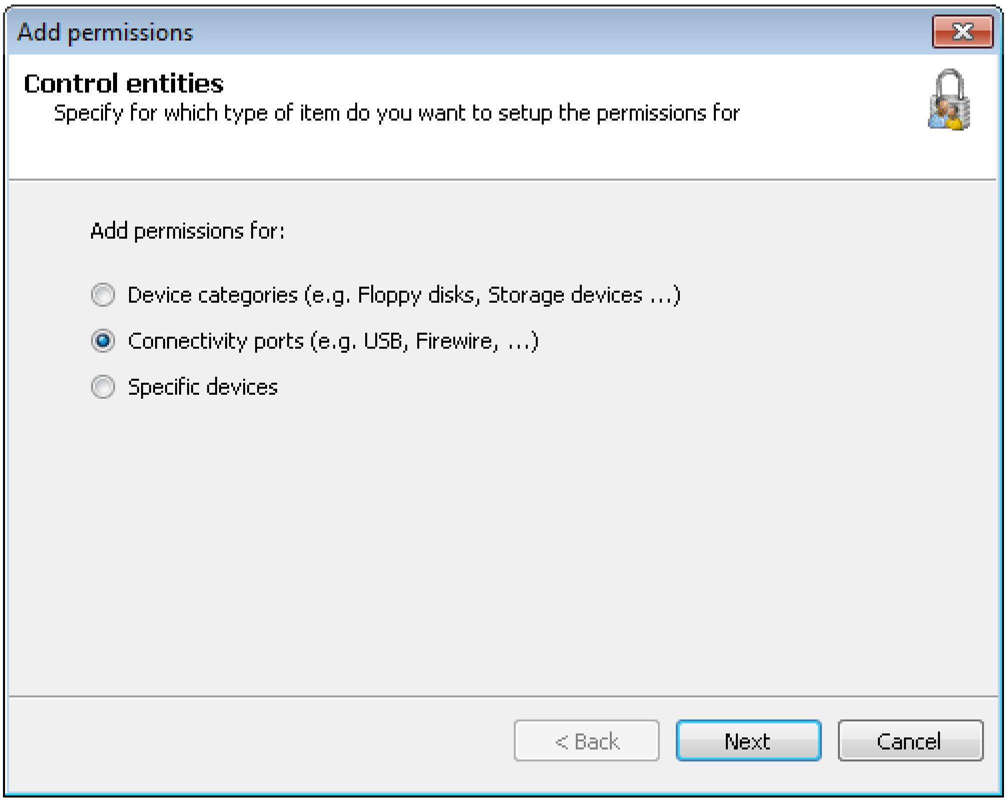
To configure connectivity port usage permissions for users within a specific protection policy:

1. Click **Configuration** tab **> Protection Policies**.

2. From **Protection Policies > Security**, select the protection policy to configure.

3. Click **Security** > **Set Permissions**

4. From **Common tasks**, click **Add permission(s)…**.



Add permissions

Control entities

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

Add permissions for:

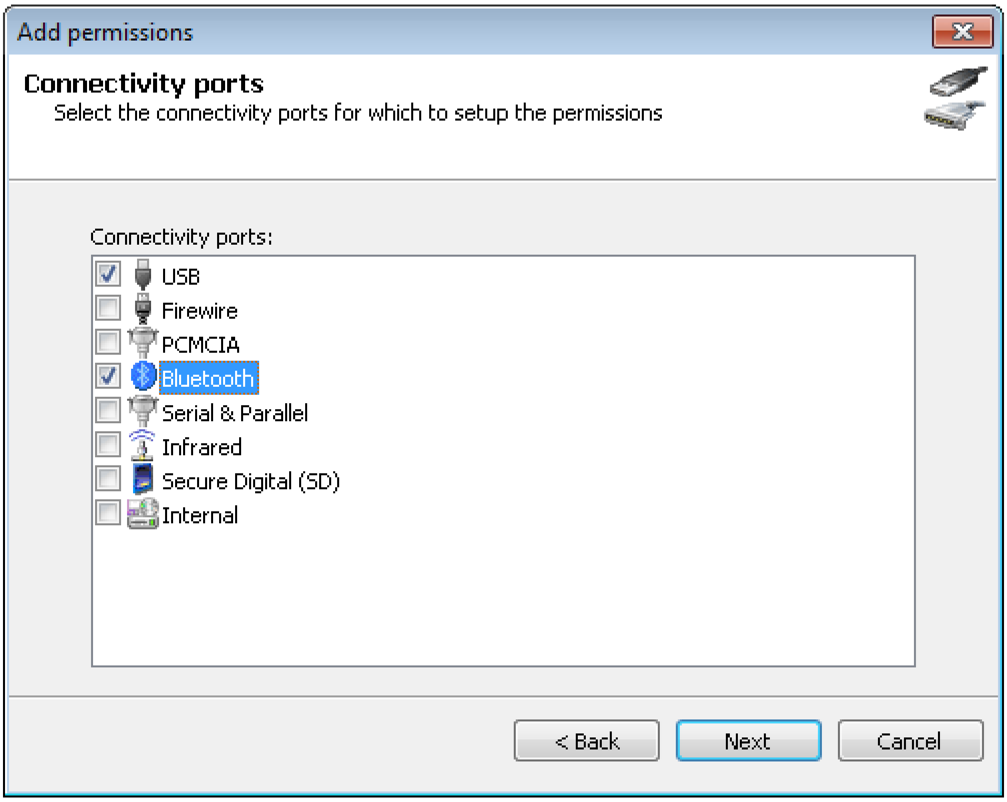
○ Device categories (e.g. Floppy disks, Storage devices ...)

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

○ Specific devices

Screenshot 40: Add permissions options - Control entities

5. In the **Add permissions** dialog select **Connectivity ports** and click **Next**.



Add permissions

Connectivity ports

Select the connectivity ports for which to setup the permissions

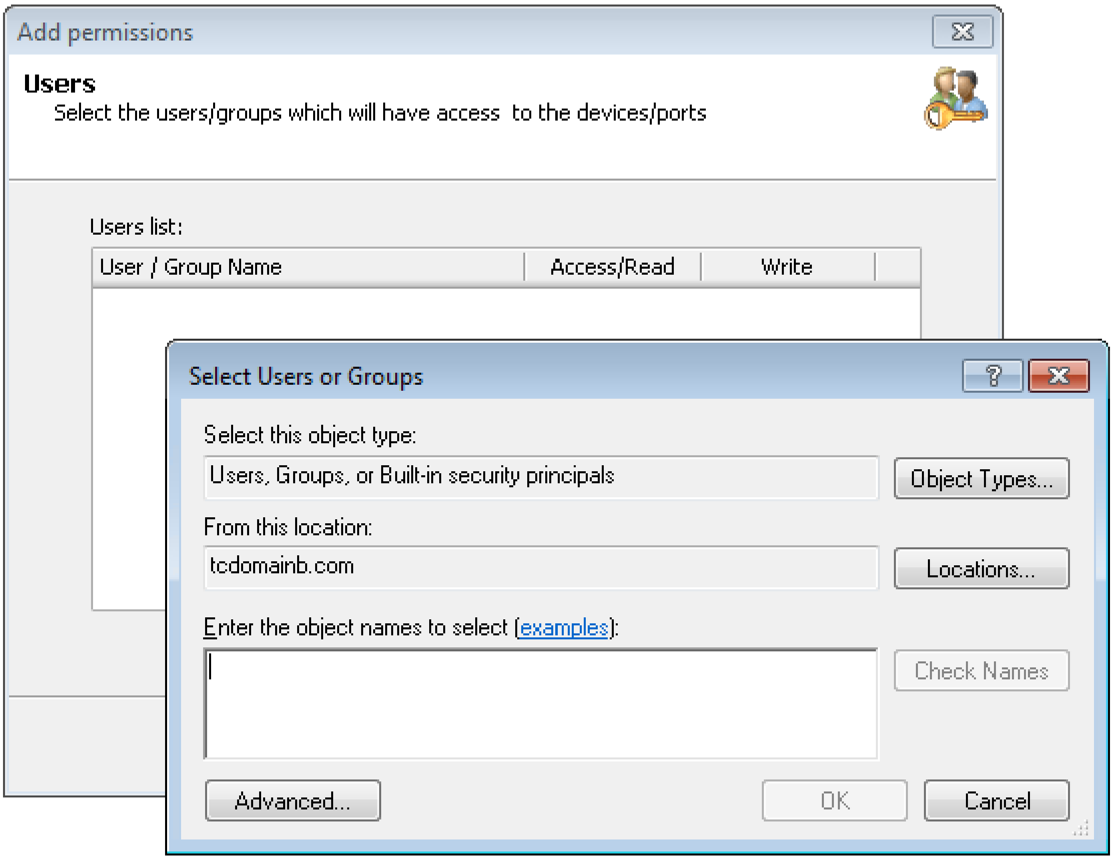
Connectivity ports:

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

Screenshot 41: Add permissions options - Connectivity ports

6. Enable or disable the required connectivity ports for which to configure permissions, and click **Next**.

7. Click **Add…** to specify the user(s)/group(s) that will have access to the connectivity ports specified in this protection policy, and click **OK**



Screenshot 42: Add permissions options - Users

8. Enable or disable Access/Read permissions for each user/group you specified, and click **Finish**.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.

2. From **Common tasks**, click **Deploy to all computers…**.

5.6 Configuring access permissions for specific devices

GFI EndPointSecurity enables you to set permissions by specific devices to Active Directory (AD) users and/or user groups. You can do this on a policy by policy basis.

For example, you can assign read-only permissions to a specific company approved USB pen drive. Attempts to use any other non-approved USB pen drives will be blocked.

> **Note**
> For an updated list of devices currently connected to the target computers, run a device scan and add the discovered devices to the devices database prior to configuring access permissions for specific devices. For more information, refer to Discovering Devices (page 89).

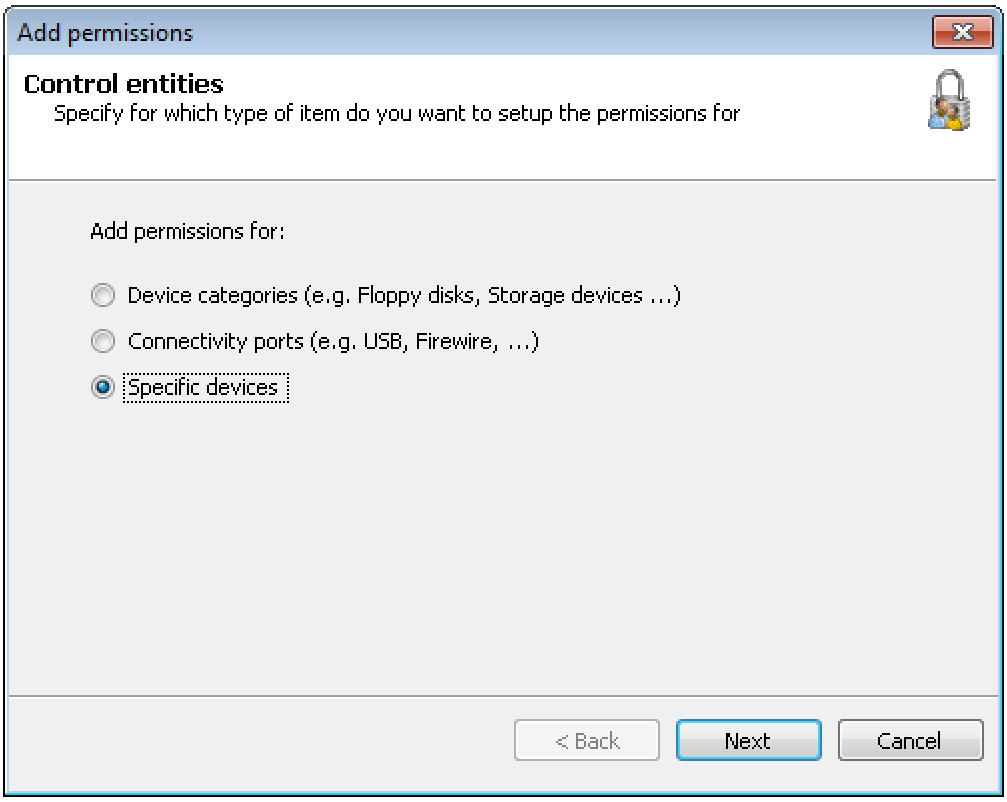
To configure specific device access permissions for users in a protection policy:

1. Click **Configuration** tab **>** **Protection Policies**.

2. From **Protection Policies** **>** **Security**, select the protection policy to configure.

3. Click **Security** sub-node.

4. From the left pane, click **Add permission(s)…** 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:

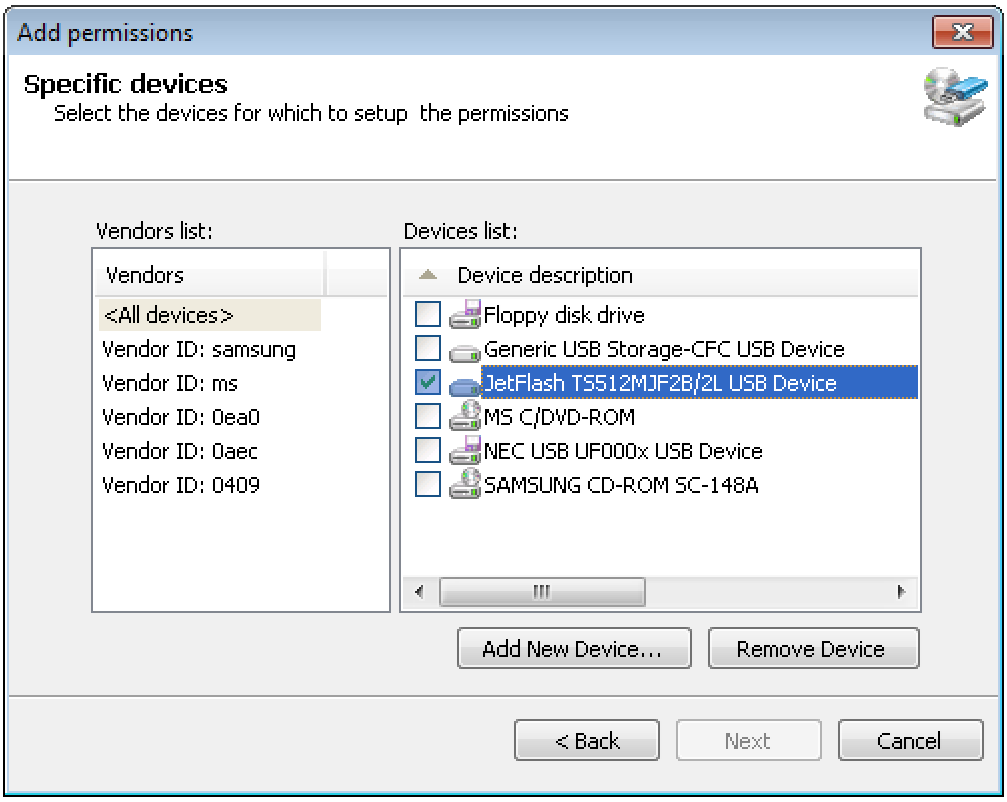
○ Device categories (e.g. Floppy disks, Storage devices …)

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

● Specific devices

Screenshot 43: Add permissions options - Control entities

5. In the **Add permissions** dialog select **Specific devices** and click **Next**.



Add permissions

Specific devices

Select the devices for which to setup the permissions

Vendors list:

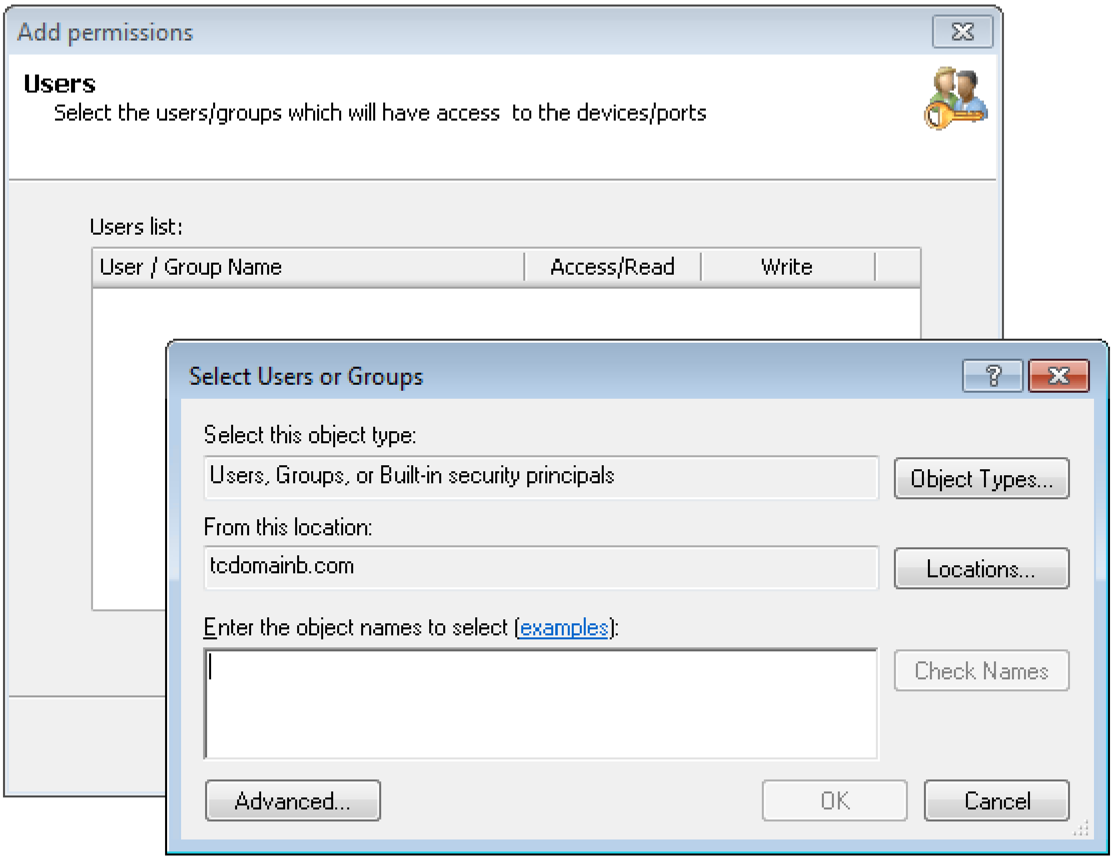
Vendors
<All devices>
Vendor ID: samsung
Vendor ID: ms
Vendor ID: 0ea0
Vendor ID: 0aec
Vendor ID: 0409

Devices list:

Device description
□ Floppy disk drive
□ Generic USB Storage-CFC USB Device
☑ JetFlash TS512MJF2B/2L USB Device
□ MS C/DVD-ROM
□ NEC USB UF000x USB Device
□ SAMSUNG CD-ROM SC-148A

Screenshot 44: Add permissions options - Specific devices

6. Enable or disable the required devices from the Devices list, for which to configure permissions, and click **Next**. If a required device is not listed, click **Add New Device…** to specify the details of the device for which to configure permissions, and click **OK**



Add permissions

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

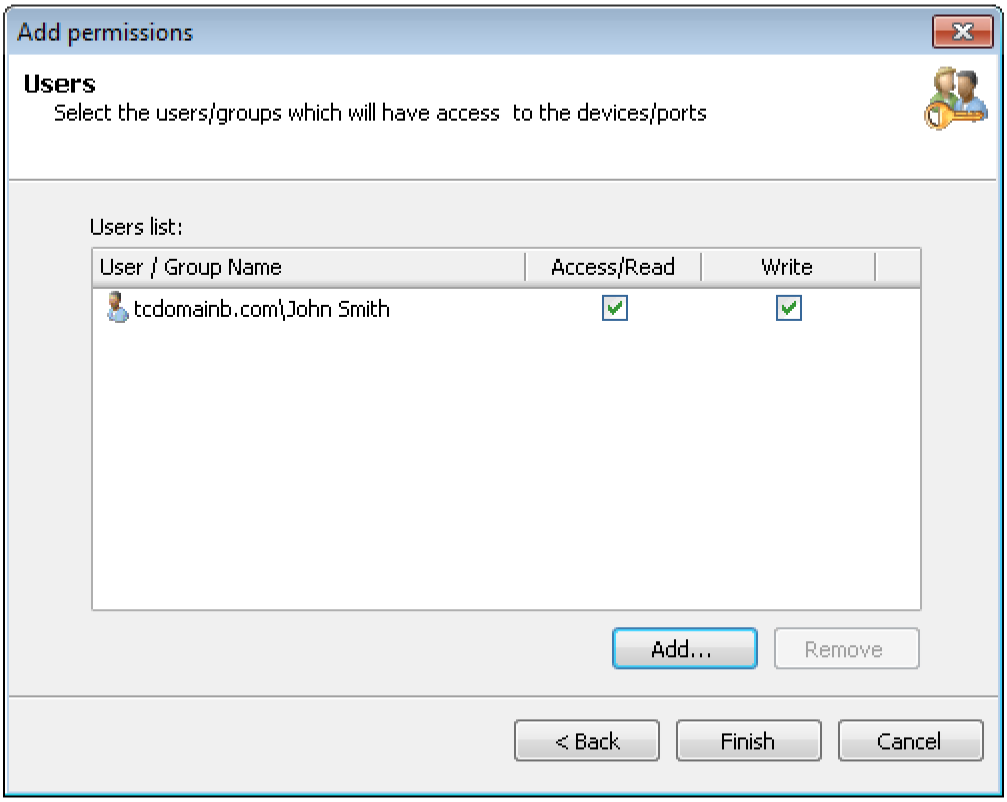
From this location:

tcdomainb.com

Enter the object names to select (examples):

Screenshot 45: Add permissions options - Users

7. Click **Add…** to specify the user(s)/group(s) that will have access to the specific devices 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
tcdomainb.com\John Smith	☑	☑

Screenshot 46: Add permissions options - Users

8. Enable or disable Access/Read and Write permissions for each user/group you specified and click **Finish**.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Deploy to all computers…**.

5.7 Configuring access permissions on workgroups

GFI EndPointSecurity allows administrators to control and monitor machines that are part of a workgroup. When installed in a workgroup, create groups of users to assign permissions at group level.

> **NOTE**
>
> It is not possible to monitor machines in a workgroup if GFI EndPointSecurity is installed in a Domain Controller.

Create the same local group on the target machine and on the GFI EndPointSecurity server to be able to apply permissions to the users.

5.7.1 Creating users group on target machines

1. Click **start**.
2. Type: `Edit local users and groups`.
3. Right-click **Groups** and select **New Group**.
4. Give a name and a description of the group.
5. Add members to the group.

5.7.2 Creating users group on the GFI EndPointSecurity server

1. Create a local group with the same name that was created on the target machine.

2. Open the GFI EndPointSecurity console.

3. Open the **Configuration** tab and click **Protection Policy**.

4. Select the policy to apply to the workgroup.

5. Under **Common task** click **Add Permissions**.

6. Under the **User** option add the group that was created on number 2.

7. Deploy the policy to the target machine.

5.8 Viewing access permissions

GFI EndPointSecurity enables you to view all permissions assigned to Active Directory (AD) users and/or user groups. You can do this on a policy-by-policy basis.

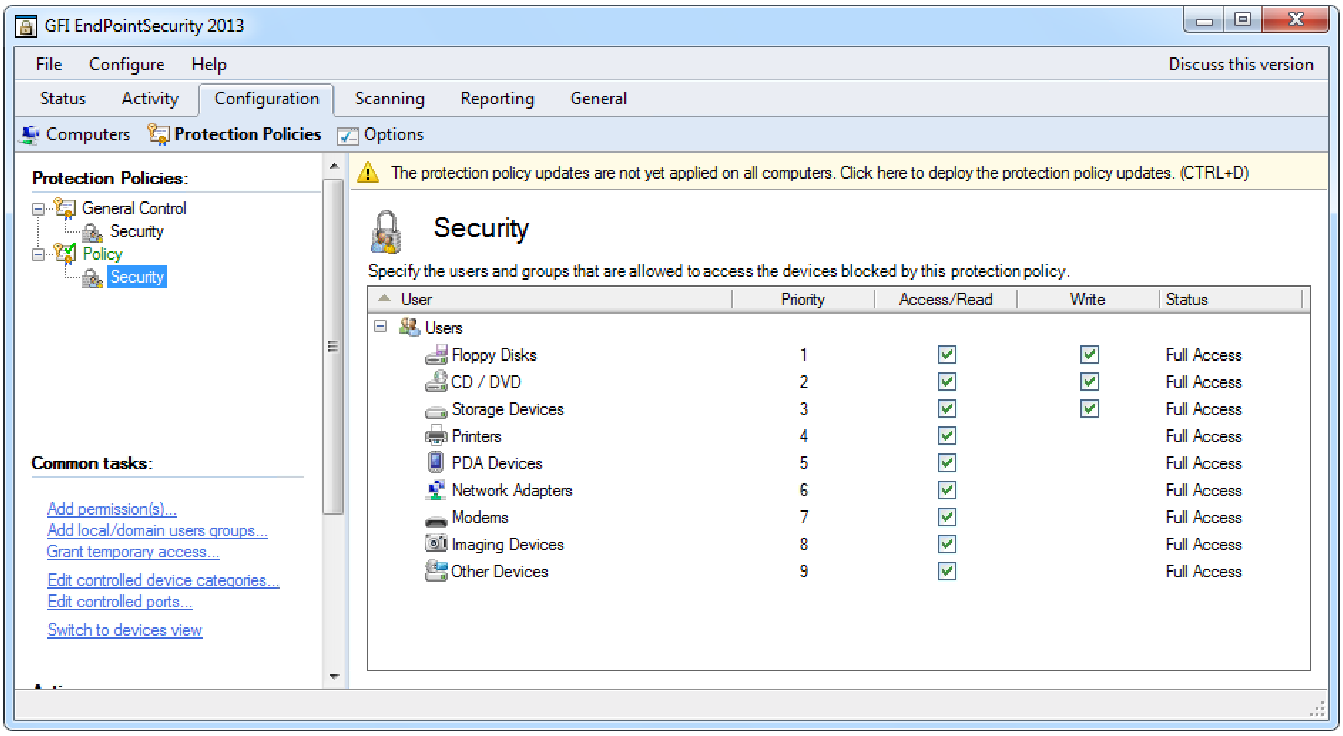
When a device category or connectivity port is not set to be controlled by the particular security policy, the relevant permission is disabled. For more information, refer to Configuring controlled device categories or Configuring controlled connectivity ports.

To view all permissions assigned to users in a protection policy:

1. Click **Configuration** tab > **Protection Policies**.

2. From **Protection Policies** > **Security**, select the protection policy to configure.

3. Click **Security**. In the right pane you can view all the set permissions for this protection policy.



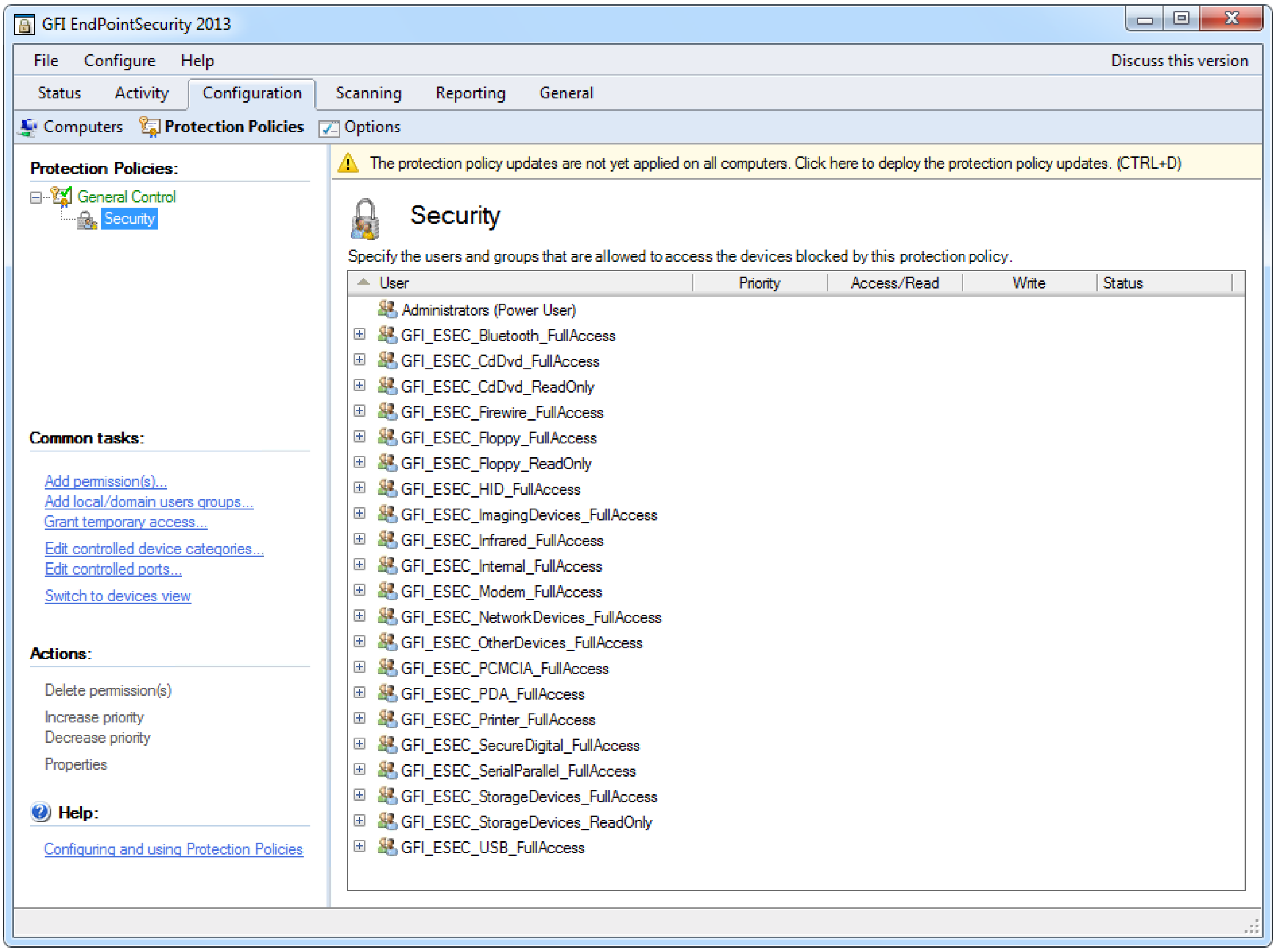
The protection policy updates are not yet applied on all computers. Click here to deploy the protection policy updates. (CTRL+D)

Security

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

User	Priority	Access/Read	Write	Status
Users				
Floppy Disks	1	☑	☑	Full Access
CD / DVD	2	☑	☑	Full Access
Storage Devices	3	☑	☑	Full Access
Printers	4	☑		Full Access
PDA Devices	5	☑		Full Access
Network Adapters	6	☑		Full Access
Modems	7	☑		Full Access
Imaging Devices	8	☑		Full Access
Other Devices	9	☑		Full Access

Screenshot 47: Protection Policies sub-tab - devices view



The protection policy updates are not yet applied on all computers. Click here to deploy the protection policy updates. (CTRL+D)

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				
GFI_ESEC_CdDvd_FullAccess				
GFI_ESEC_CdDvd_ReadOnly				
GFI_ESEC_Firewire_FullAccess				
GFI_ESEC_Floppy_FullAccess				
GFI_ESEC_Floppy_ReadOnly				
GFI_ESEC_HID_FullAccess				
GFI_ESEC_ImagingDevices_FullAccess				
GFI_ESEC_Infrared_FullAccess				
GFI_ESEC_Internal_FullAccess				
GFI_ESEC_Modem_FullAccess				
GFI_ESEC_NetworkDevices_FullAccess				
GFI_ESEC_OtherDevices_FullAccess				
GFI_ESEC_PCMCIA_FullAccess				
GFI_ESEC_PDA_FullAccess				
GFI_ESEC_Printer_FullAccess				
GFI_ESEC_SecureDigital_FullAccess				
GFI_ESEC_SerialParallel_FullAccess				
GFI_ESEC_StorageDevices_FullAccess				
GFI_ESEC_StorageDevices_ReadOnly				
GFI_ESEC_USB_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 Policies

Screenshot 48: Protection Policies sub-tab - users view

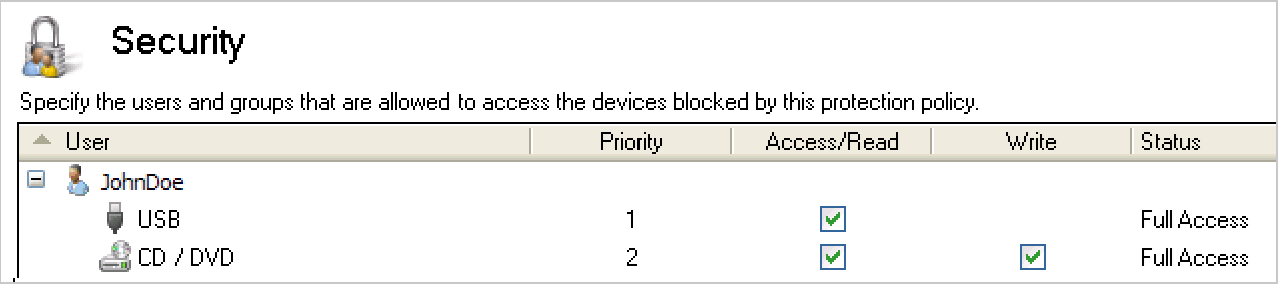
4. From the left pane, click **Switch to devices view** or **Switch to users view** in the **Common tasks** section, to switch grouping of permissions by devices/ports or users.

> **Note**
>
> In users view, you will also see any power users specified within the policy.

5.9 Configuring priorities for permissions

GFI EndPointSecurity enables you to prioritize any permissions assigned to Active Directory (AD) users and/or user groups. You can do this on a policy-by-policy basis and on a user-by-user basis.

For example, for a specific user specified within a specific protection policy, you may decide to give priority 1 to USB port permissions, and priority 2 to CD/DVD drive permissions. This means that if the user connects an external CD/DVD drive via the USB port to the target computer, permissions for the USB port will take precedence over permissions for the CD/DVD drive.



Security

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

User	Priority	Access/Read	Write	Status
JohnDoe				
USB	1	☑		Full Access
CD / DVD	2	☑	☑	Full Access

Screenshot 49: Protection Policies sub-tab - Security area

To prioritize permissions assigned to users in a protection policy:

1. Click **Configuration** tab **>** **Protection Policies**.

2. From **Protection Policies > Security**, select the protection policy to configure.

3. Click **Security** sub-node.

4. From the left pane, click **Switch to users view** in the **Common tasks** section, to switch grouping of permissions by users.

5. Right-click the **Security** section and select **Expand all**.

6. Highlight the required device or port.

7. From the left pane, click **Increase priority** or **Decrease priority** in the **Actions** section.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.

2. From **Common tasks**, click **Deploy to all computers…**.

5.10 Configuring device blacklist

GFI EndPointSecurity enables you to specify which device(s) can be made inaccessible to everyone. The blacklist is granular, so you can even blacklist a specific device with a specific serial number. You can do this on a policy-by-policy basis.

For an updated list of devices currently connected to the target computers, run a device scan and add the discovered devices to the devices database prior to configuring blacklisted devices. For more information, refer to Discovering Devices (page 89).

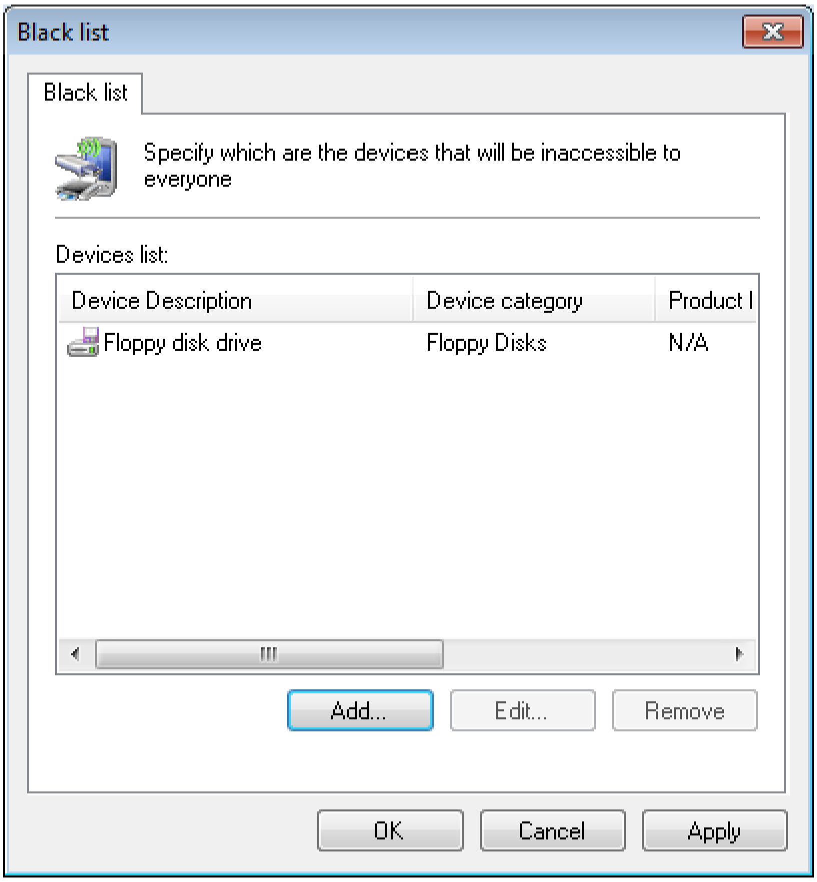
> **Note**
> Power users will override any blacklisted devices, and thus will be able to access blacklisted devices.

To add devices to the blacklist of a specific protection policy:

1. Click **Configuration** tab **>** **Protection Policies**.

2. From **Protection Policies > Security**, select the protection policy to configure.

3. From the right pane, click **Devices Blacklist** in the **General Control** section.



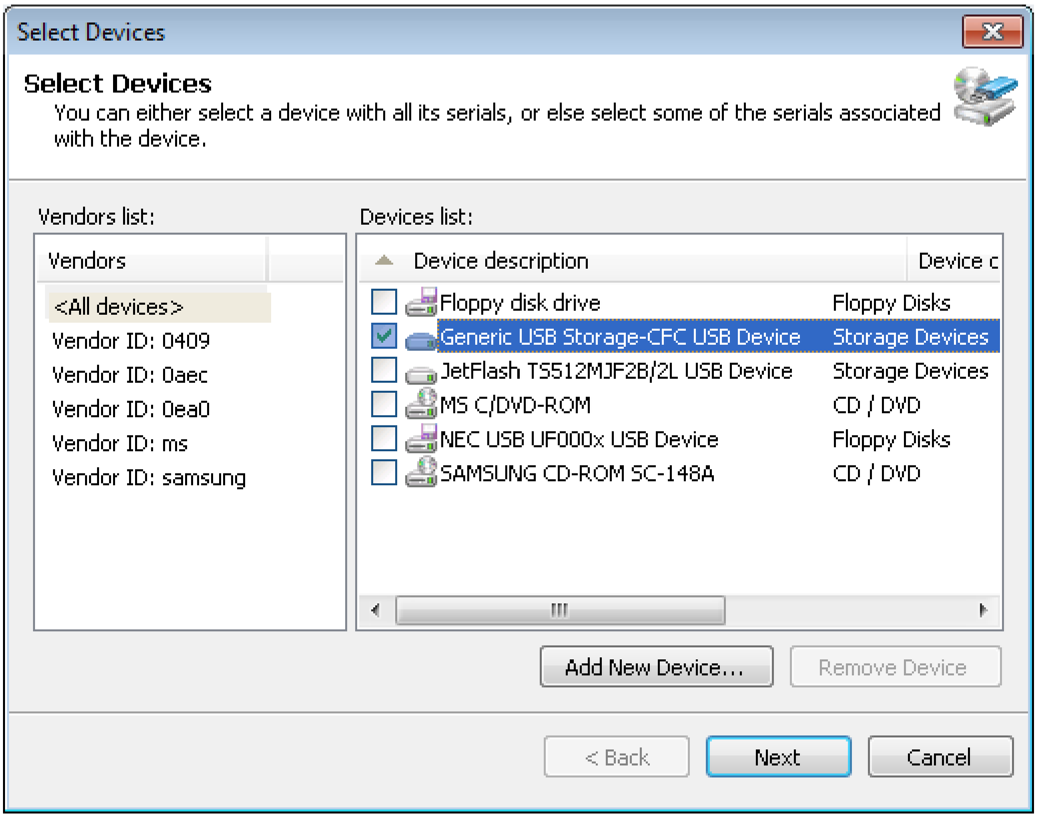
Specify which are the devices that will be inaccessible to everyone

Devices list:

Device Description	Device category	Product I
Floppy disk drive	Floppy Disks	N/A

Screenshot 50: Black list options

4. In the **Black list** dialog, click **Add…** to select devices to add to the blacklist.



Select Devices

You can either select a device with all its serials, or else select some of the serials associated with the device.

Vendors list:

Vendors
<All devices>
Vendor ID: 0409
Vendor ID: 0aec
Vendor ID: 0ea0
Vendor ID: ms
Vendor ID: samsung

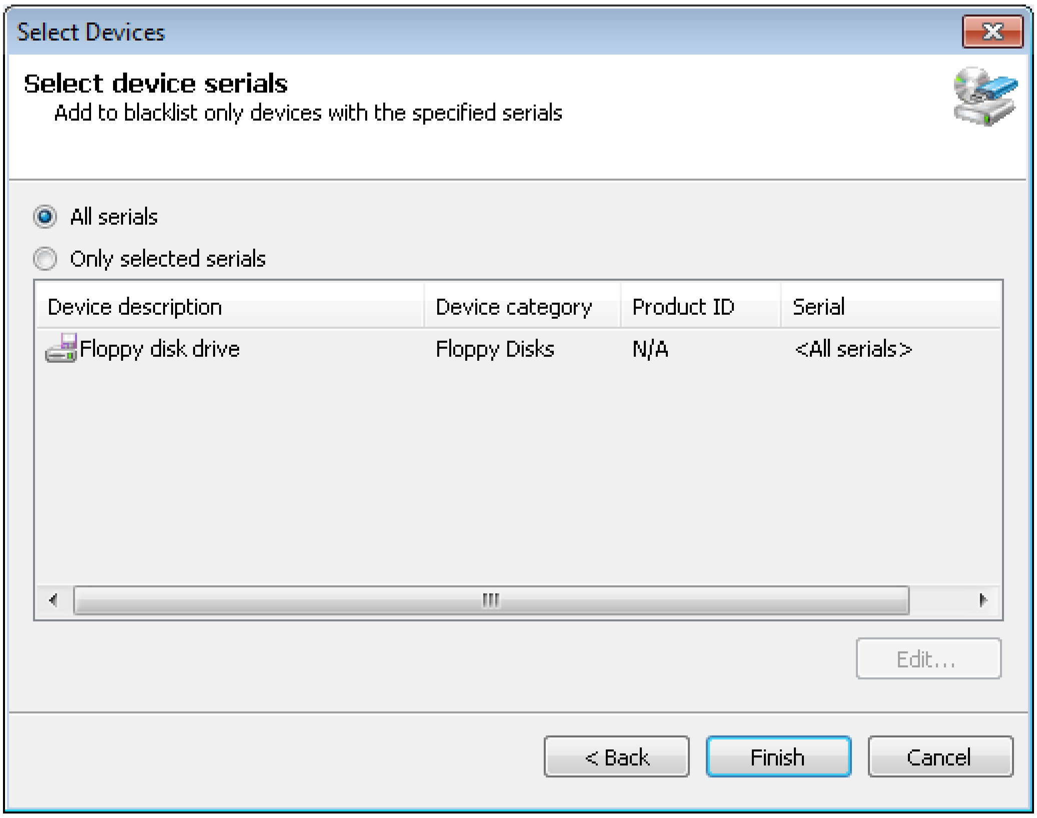
Devices list:

	Device description	Device c
☐	Floppy disk drive	Floppy Disks
☑	Generic USB Storage-CFC USB Device	Storage Devices
☐	JetFlash TS512MJF2B/2L USB Device	Storage Devices
☐	MS C/DVD-ROM	CD / DVD
☐	NEC USB UF000x USB Device	Floppy Disks
☐	SAMSUNG CD-ROM SC-148A	CD / DVD

Screenshot 51: Select Devices options

5. In the **Select Devices** dialog enable or disable the devices to add to the blacklist from the Devices list and click **Next**.

> **Note**
>
> If a required device is not listed, click **Add New Device…** to specify the details of the device you want to add to the blacklist, and click **OK**



Select device serials

Add to blacklist only devices with the specified serials

● All serials

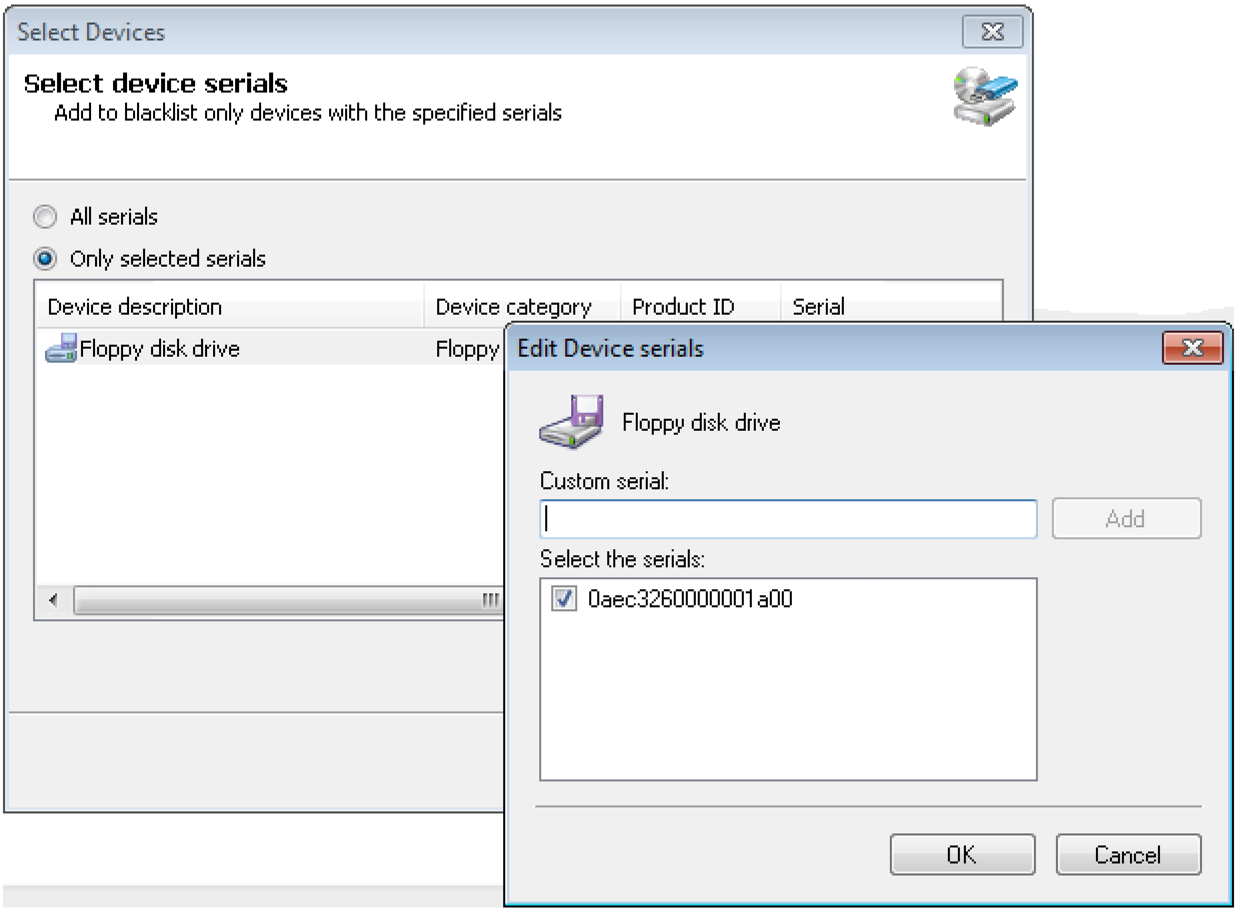
○ Only selected serials

Device description	Device category	Product ID	Serial
Floppy disk drive	Floppy Disks	N/A	<All serials>

Screenshot 52: Select Devices options - Select device serials

6. Select the required serials related option from:

- **All serials** - to blacklist all serial numbers of a specific device. Click **Finish** and **OK**
- **Only selected serials** - to specify particular device serial number(s) to be added to the blacklist. Next, highlight the device and click **Edit…** to specify the serial number(s). Click **OK**, **Finish** and **OK**



Select Devices

Select device serials

Add to blacklist only devices with the specified serials

○ All serials

● Only selected serials

Device description	Device category	Product ID	Serial
Floppy disk drive	Floppy		

Edit Device serials

Floppy disk drive

Custom serial:

Select the serials:

☑ 0aec3260000001a00

Screenshot 53: Select Devices options - Edit Device serials

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.

2. From **Common tasks**, click **Deploy to all computers…**.

5.11 Configuring device whitelist

GFI EndPointSecurity enables you to specify which device(s) can be accessed by everyone. The whitelist is granular, so you can even whitelist a specific device with a specific serial number. You can do this on a policy-by-policy basis.

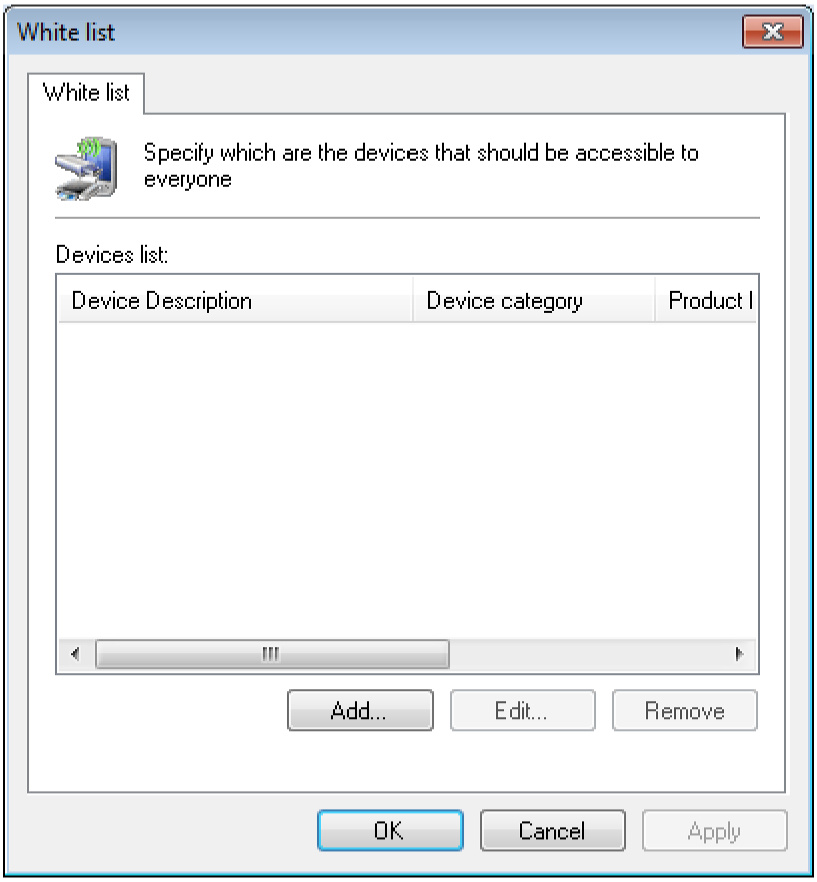
For an updated list of devices currently connected to the target computers, run a device scan and add the discovered devices to the devices database prior to configuring whitelisted devices. For more information, refer to Discovering Devices (page 89).

To add whitelist devices to a protection policy:

1. Click **Configuration** tab **> Protection Policies**.

2. From **Protection Policies > Security**, select the protection policy to configure.

3. From the right pane, click **Devices WhiteList** in the **General Control** section.



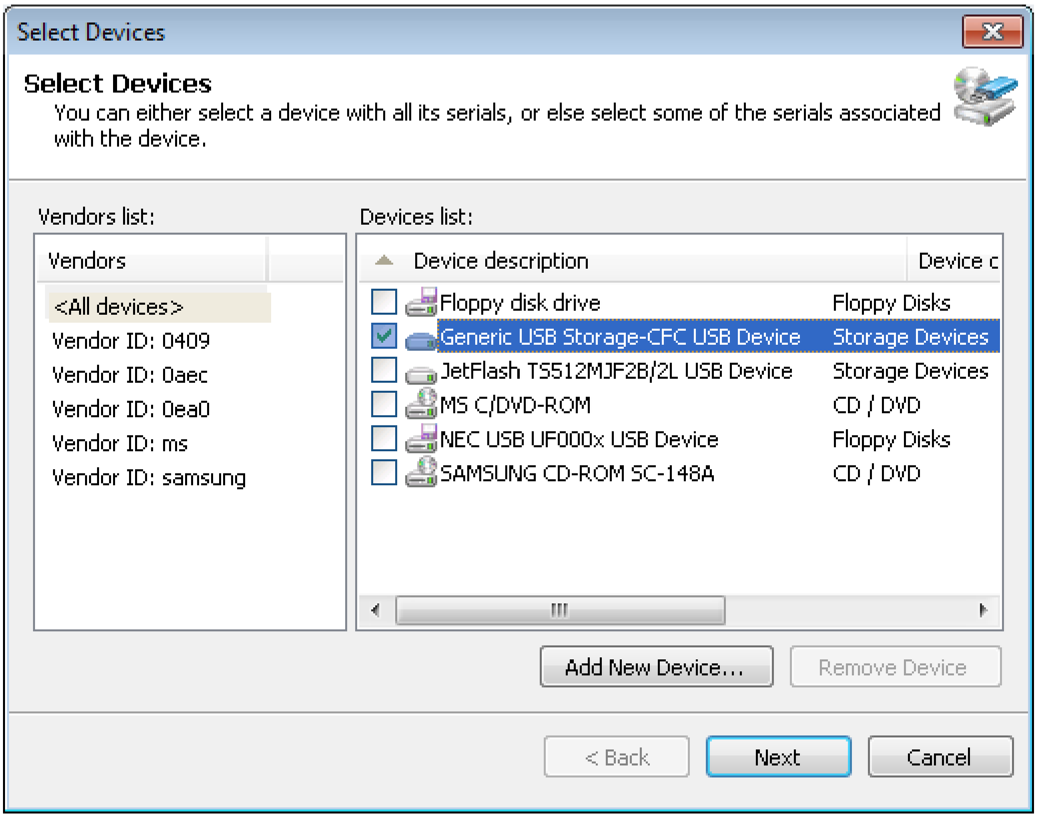
Specify which are the devices that should be accessible to everyone

Devices list:

Device Description	Device category	Product I

Screenshot 54: White list options

4. In the **Whitelist** dialog, click **Add…** to select devices to add to the whitelist.



Select Devices

You can either select a device with all its serials, or else select some of the serials associated with the device.

Vendors list:

Vendors
<All devices>
Vendor ID: 0409
Vendor ID: 0aec
Vendor ID: 0ea0
Vendor ID: ms
Vendor ID: samsung

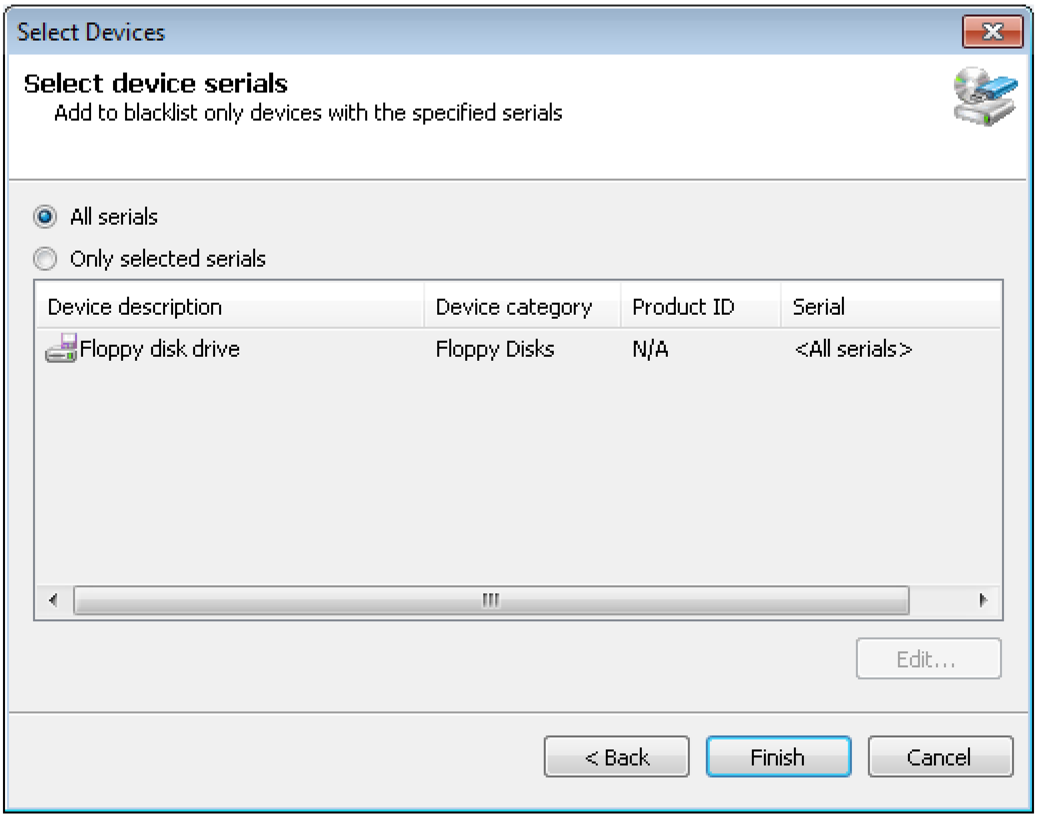
Devices list:

Device description	Device c
□ Floppy disk drive	Floppy Disks
☑ Generic USB Storage-CFC USB Device	Storage Devices
□ JetFlash TS512MJF2B/2L USB Device	Storage Devices
□ MS C/DVD-ROM	CD / DVD
□ NEC USB UF000x USB Device	Floppy Disks
□ SAMSUNG CD-ROM SC-148A	CD / DVD

Screenshot 55: Select Devices options

5. In the **Select Devices** dialog enable or disable the devices to add to the whitelist from the Devices list, and click **Next**.

> **Note**
>
> If a required device is not listed, click **Add New Device…** to specify the details of the device you want to add to the whitelist, and click **OK**



Select Devices

Select device serials

Add to blacklist only devices with the specified serials

● All serials

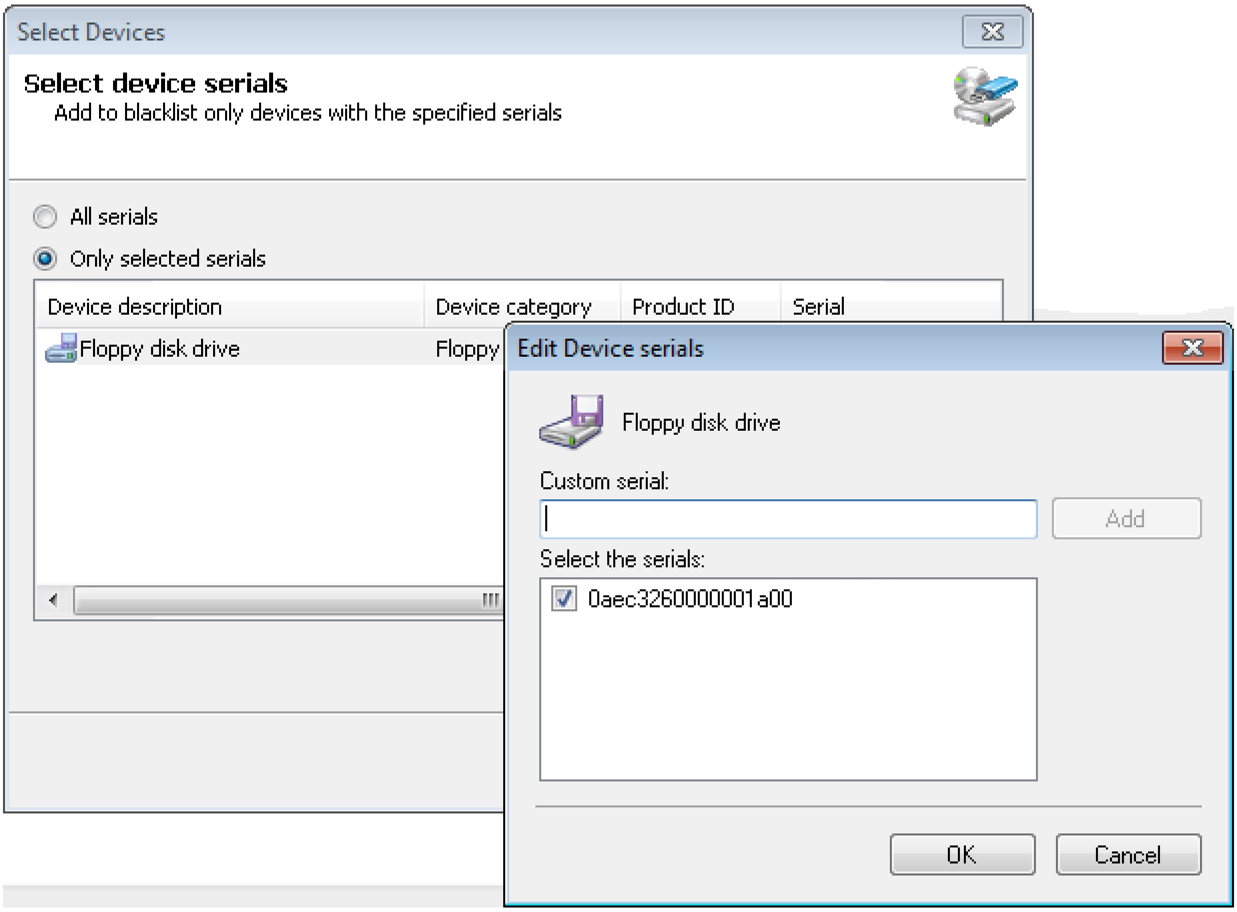
○ Only selected serials

Device description	Device category	Product ID	Serial
Floppy disk drive	Floppy Disks	N/A	<All serials>

Screenshot 56: Select Devices options - Select device serials

6. Select the required serials related option from:

- **All serials** - to whitelist all serial numbers of a specific device. Click **Finish** and **OK**
- **Only selected serials** - to specify that only particular device serial number(s) are to be added to the whitelist. Next, highlight the device and click **Edit…** to select the serial number(s) to whitelist. Click **OK**, **Finish** and **OK**



Select Devices

Select device serials

Add to blacklist only devices with the specified serials

○ All serials

● Only selected serials

Device description	Device category	Product ID	Serial
Floppy disk drive	Floppy		

Edit Device serials

Floppy disk drive

Custom serial:

Select the serials:

☑ 0aec3260000001a00

Screenshot 57: Select Devices options - Edit Device serials

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.

2. From **Common tasks**, click **Deploy to all computers…**.

5.12 Configuring temporary access privileges

GFI EndPointSecurity enables you to grant temporary access to users. This enables them to access devices and connection ports on protected target computers for a specified duration/time window. You can do this on a policy-by-policy basis.

When temporary access is granted, any permissions and settings (e.g. file-type filters) set in the protection policy applicable for the target computer, are temporarily overridden.

For more information refer to How works - Temporary Access.

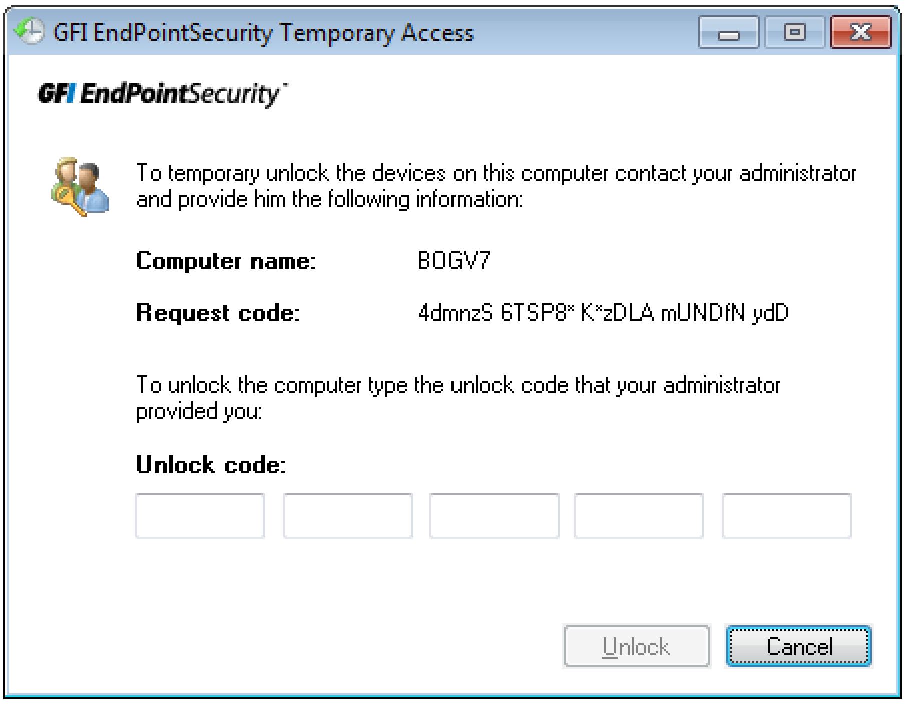
- Requesting temporary access for a protected computer
- Granting temporary access to a protected computer.

5.12.1 Requesting temporary access for a protected computer

To generate a request code: tool:

Screenshot 58: Devices Temporary Access icon

1. From the **Control Panel** click **Devices Temporary Access**.



To temporary unlock the devices on this computer contact your administrator and provide him the following information:

Computer name: B0GV7

Request code: 4dmnzS 6TSP8* K*zDLA mUNDfN ydD

To unlock the computer type the unlock code that your administrator provided you:

Unlock code:

Screenshot 59: GFI EndPointSecurity Temporary Access tool

2. In the**GFI EndPointSecurity Temporary Access** dialog take note of the **Request code** generated. Communicate the following details to your security administrator:

- Request code
- Device/connection port type
- When you require access
- For how long you require access.

Keep the GFI EndPointSecurity Temporary Access tool open.

3. When the administrator sends the unlock code, key it in the **Unlock code** field.

> **Note**
> An unlock code keyed in on the protected target computer outside the specified validity period will not activate temporary access.

4. Click **Unlock** to activate temporary access. You are now able to access the required device and/or connection port.

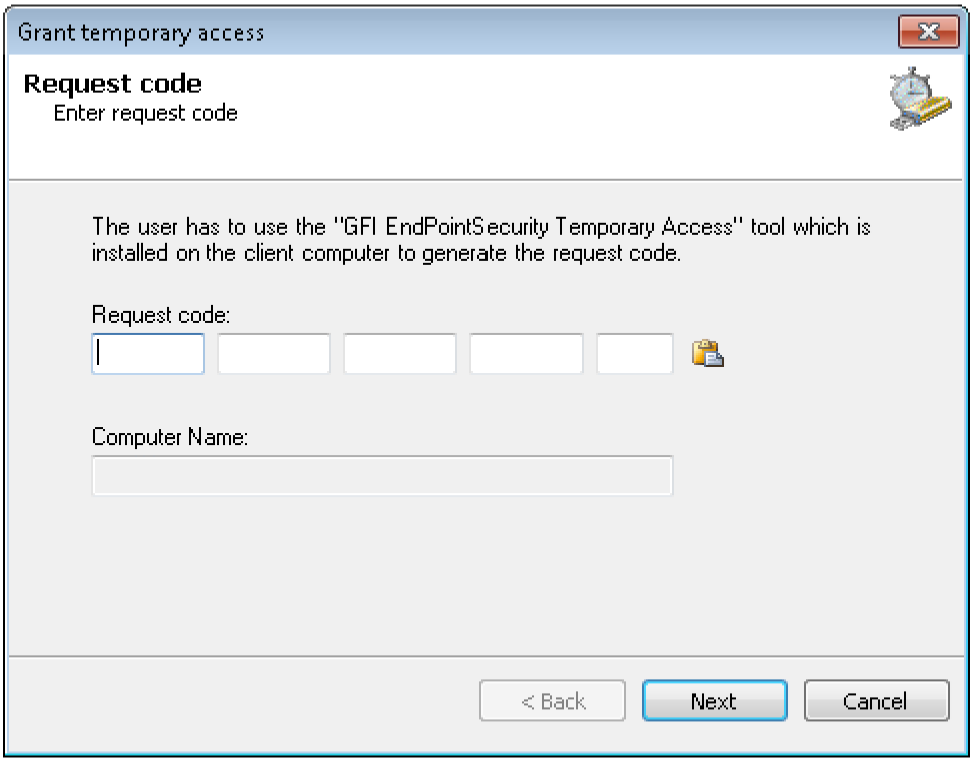
5.12.2 Granting temporary access to a protected computer

To grant temporary access:

1. From GFI EndPointSecurity management console, click **Configuration** tab > **Protection Policies** sub-tab.

2. From the left pane, select the protection policy that includes the computer on which temporary access needs to be granted.

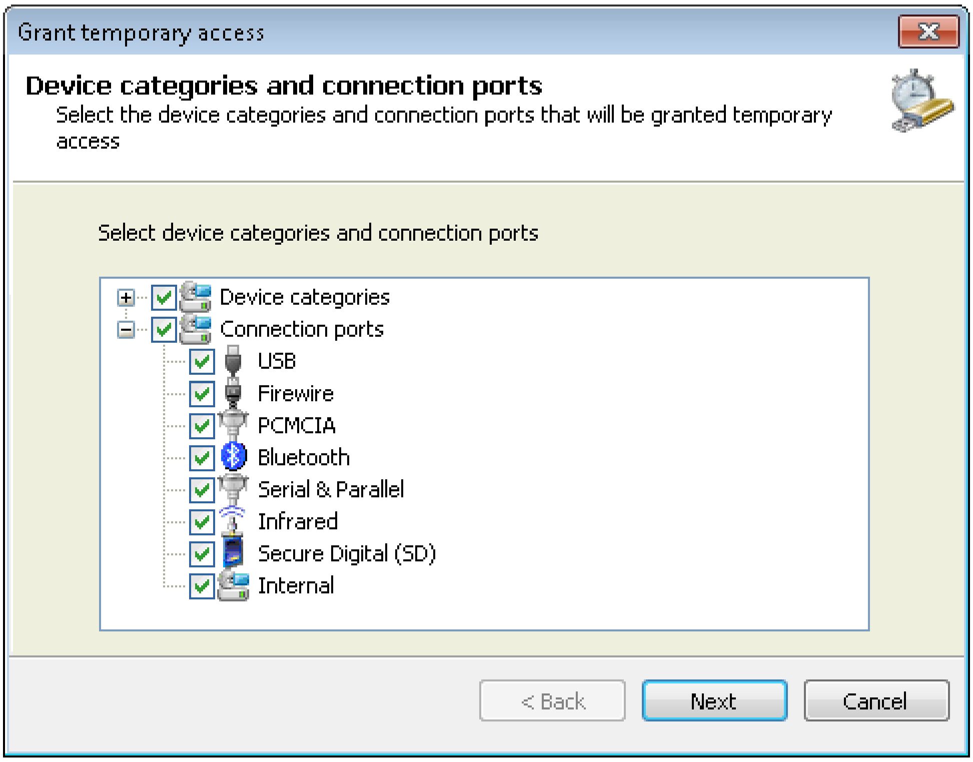
3. From the right pane, click **Grant temporary access** in the **Temporary Access** section.



The user has to use the "GFI EndPointSecurity Temporary Access" tool which is installed on the client computer to generate the request code.

Screenshot 60: Grant temporary access options - Request code

4. In the **Grant temporary access** dialog key in the request code received from the user, in the **Request code** field. The computer name from which the request code was generated, is displayed in the **Computer Name** field. Click **Next**.


Grant temporary access

Device categories and connection ports

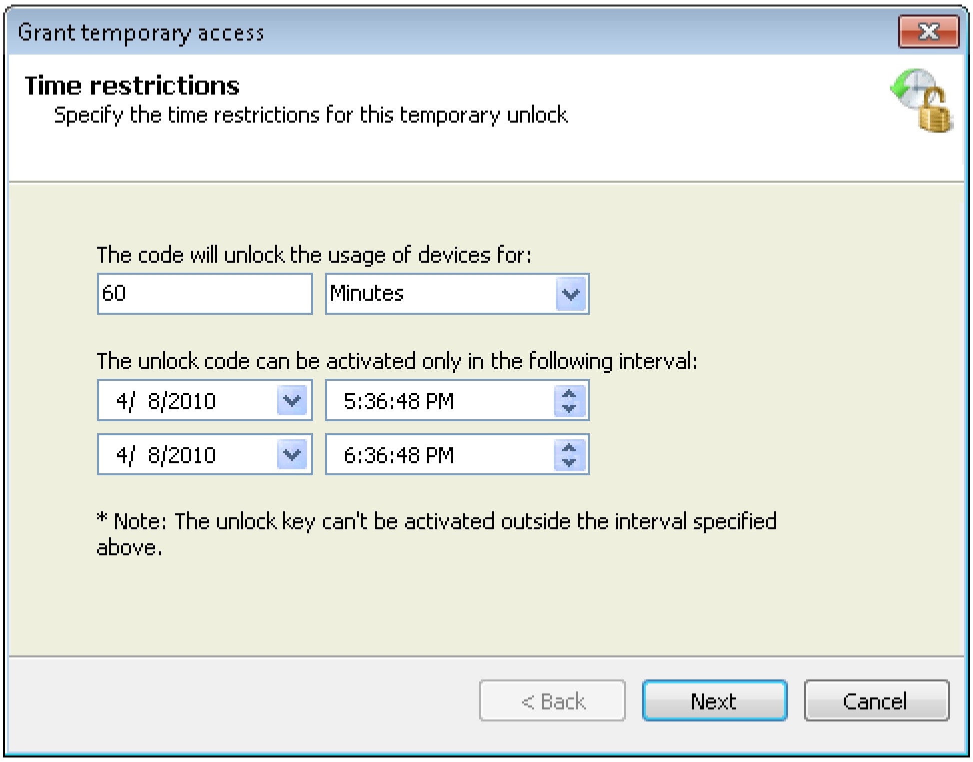
Select the device categories and connection ports that will be granted temporary access

Select device categories and connection ports

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

Screenshot 61: Grant temporary access options - Device categories and connection ports

5. Enable the required device categories and/or connection ports from the list, to which you will be granting temporary access, and click **Next**.


Grant temporary access

Time restrictions

Specify the time restrictions for this temporary unlock

The code will unlock the usage of devices for:

60 Minutes

The unlock code can be activated only in the following interval:

4/ 8/2010 5:36:48 PM

4/ 8/2010 6:36:48 PM

* Note: The unlock key can't be activated outside the interval specified above.

Screenshot 62: Grant temporary access options - Time restrictions

6. Specify the duration during which access is allowed, and the validity period of the unlock code, and click **Next**.

7. Take note of the **Unlock code** generated. Communicate the code to the user requesting temporary access and click **Finish**.

5.13 Configuring file-type filters

GFI EndPointSecurity enables you to specify file-type restrictions on files, such as .DOC or .XLS files, being copied to/from allowed devices. You can apply these restrictions to Active Directory (AD) users and/or user groups. You can do this on a policy-by-policy basis.

Filtering is based on file extension checks and real file type signature checks. Real file type signature checking can be done on the following file types:

AVI	BMP	CAB	CHM	DLL	DOC	EMF	EXE	GIF	HLP
HTM	JPE	JPEG	JPG	LNK	M4A	MDB	MP3	MPEG	MPG
MSG	MSI	OCX	P7M	PDF	PPT	RAR	RTF	SCR	SYS
TIF	TIFF	TXT	URL	WAV	XLS	ZIP	DOCX	XLSX	PPTX

> **Note 1**
>
> For any other file type not specified above, filtering is based only on the file extension.

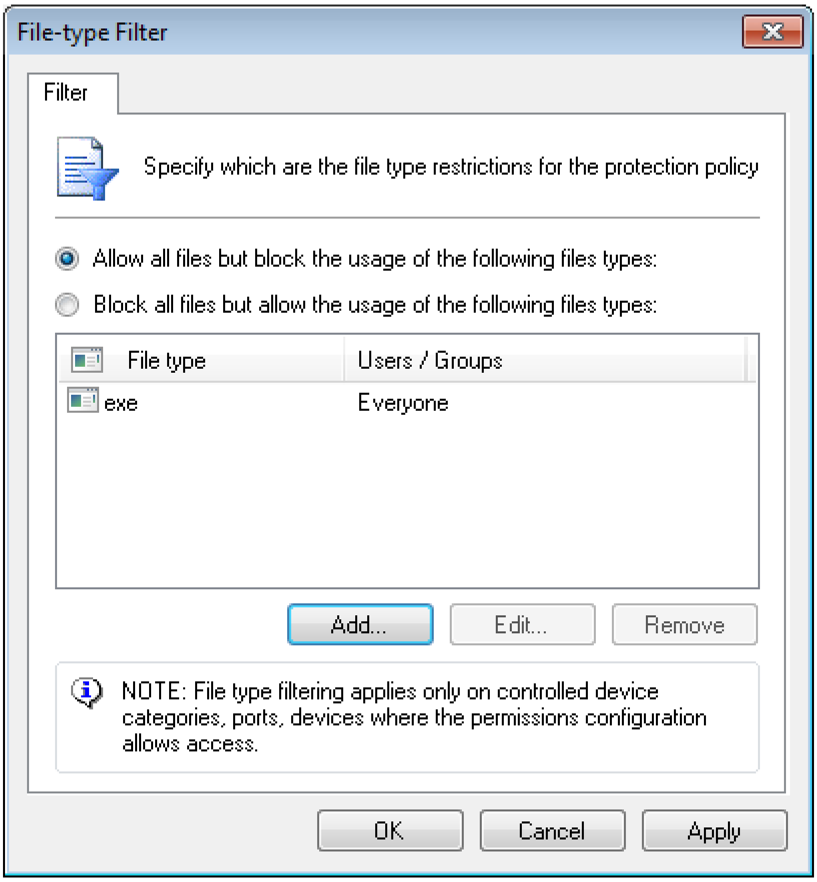
> **Note 2**
>
> File-type filtering is only applied to device categories and/or ports for which permissions have been set to allow access.

To configure file-type restrictions for users in a specific protection policy:

1. From GFI EndPointSecurity management console, click **Configuration** tab **> Protection Policies**.

2. From the left pane, select the protection policy for which you want to specify file-type restrictions.

3. From the right pane, click **File-type Filter** in the **File control** section.



Specify which are the file type restrictions for the protection policy

● Allow all files but block the usage of the following files types:

○ Block all files but allow the usage of the following files types:

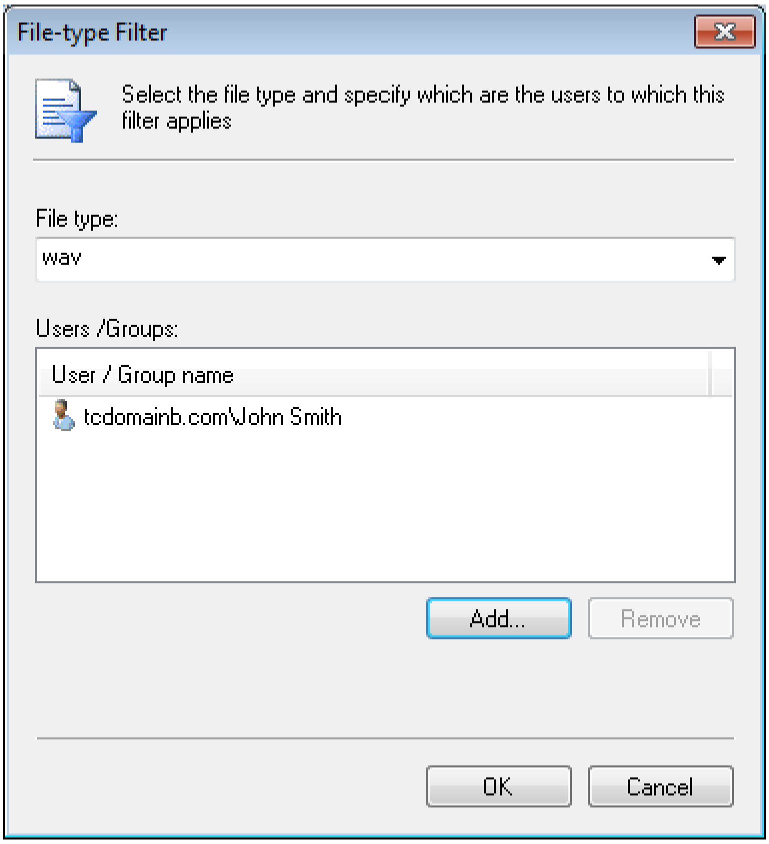
File type	Users / Groups
exe	Everyone

NOTE: File type filtering applies only on controlled device categories, ports, devices where the permissions configuration allows access.

Screenshot 63: File-type Filter options

4. In the File-type Filter dialog select the restriction to apply to this policy:

- Allow all files but block the usage of the following file types
- Block all files but allow the usage of the following file types.


File-type Filter
Select the file type and specify which are the users to which this filter applies
Add...
Remove
OK
Cancel

File type: wav

Users /Groups:

User / Group name
tcdomainb.com\John Smith

Screenshot 64: File-type Filter and user options

5. Click **Add…** and select or key in the file-type from the **File type** drop-down list.

6. Click **Add…** to specify the user(s)/group(s) who are allowed/blocked from accessing the specified file-type, and click **OK** Repeat the preceding two sub-steps for each file type to restrict.

7. Click **OK** twice.

To deploy protection policy updates on target computers specified in the policy:

1. From GFI EndPointSecurity management console, click **Configuration** tab **>** **Computers** sub-tab.

2. From the left pane, click **Deploy to all computers…** in the **Common tasks** section.

5.14 Configuring content awareness

GFI EndPointSecurity enables you to specify the file content restrictions for a particular protection policy. The content awareness feature looks into files transiting the endpoints via removable devices and it \identifies content based on pre-configured and custom regular expressions and dictionary files. By default the module looks for secure confidential details such as social security numbers and primary account numbers as well as information related to companies and enterprises such as names of diseases, drugs, dangerous chemicals and also trivial language or ethnic / racist terms.

» You can configure content checking as a global policy in a similar fashion to the file checking module.

5.14.1 Managing content awareness options

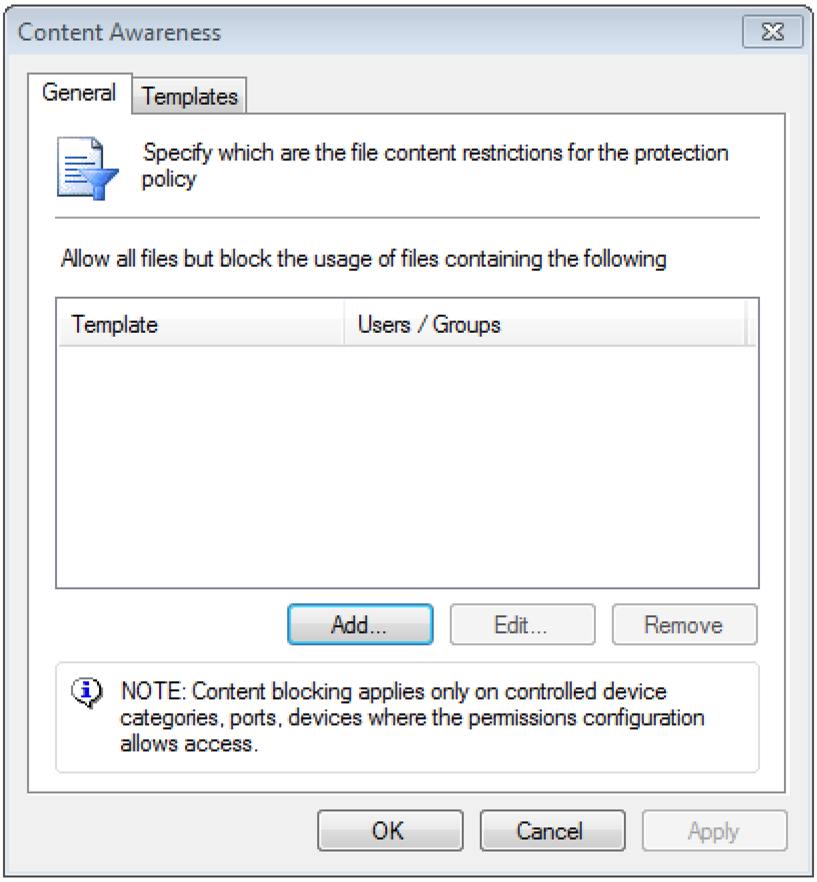
To configure content awareness options for users

in a specific protection policy:

1. From GFI EndPointSecurity management console, click **Configuration** tab > **Protection Policies**.

2. From the left pane, select the protection policy for which to specify content restrictions.

3. From the right pane, click **Content awareness** in the **File control** section.



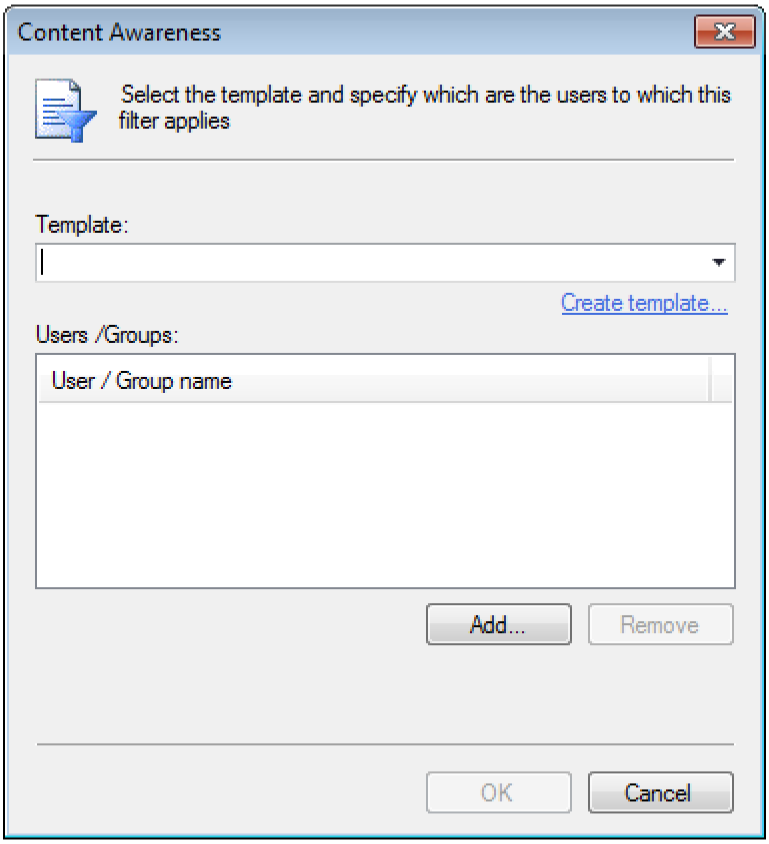
Specify which are the file content restrictions for the protection policy

Allow all files but block the usage of files containing the following

NOTE: Content blocking applies only on controlled device categories, ports, devices where the permissions configuration allows access.

Screenshot 65: Content awareness options

4. In the Content awareness dialog, click **Add** to select the template to apply to this policy:



Content Awareness

Select the template and specify which are the users to which this filter applies

Template:

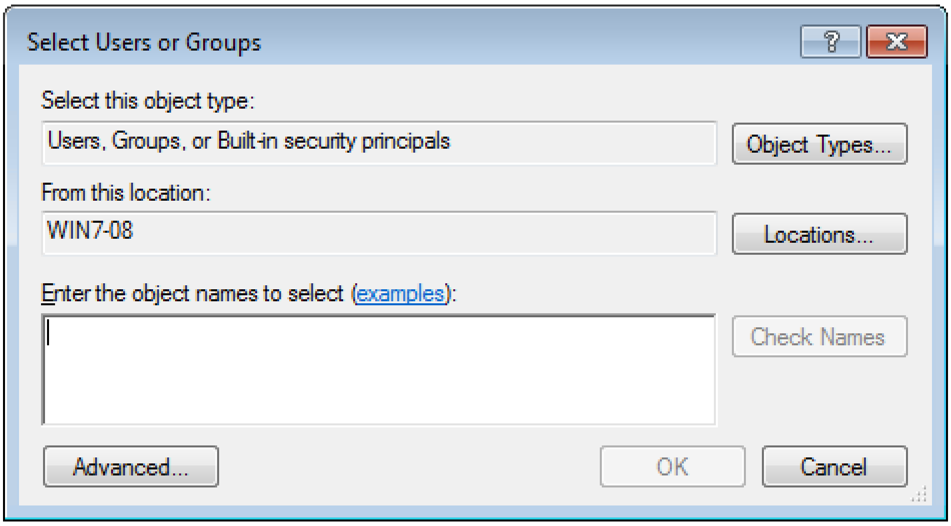
Users /Groups:

Screenshot 66: Add a new template

5. Click **Add…** and select or key in the template from the **Template** drop-down list.

6. Click **Add…** to specify the user(s)/group(s) and click **OK** Repeat the preceding two sub-steps for each template that will be applied.

7. Click **OK**



Select Users or Groups

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

From this location:
WIN7-08

Enter the object names to select (examples):

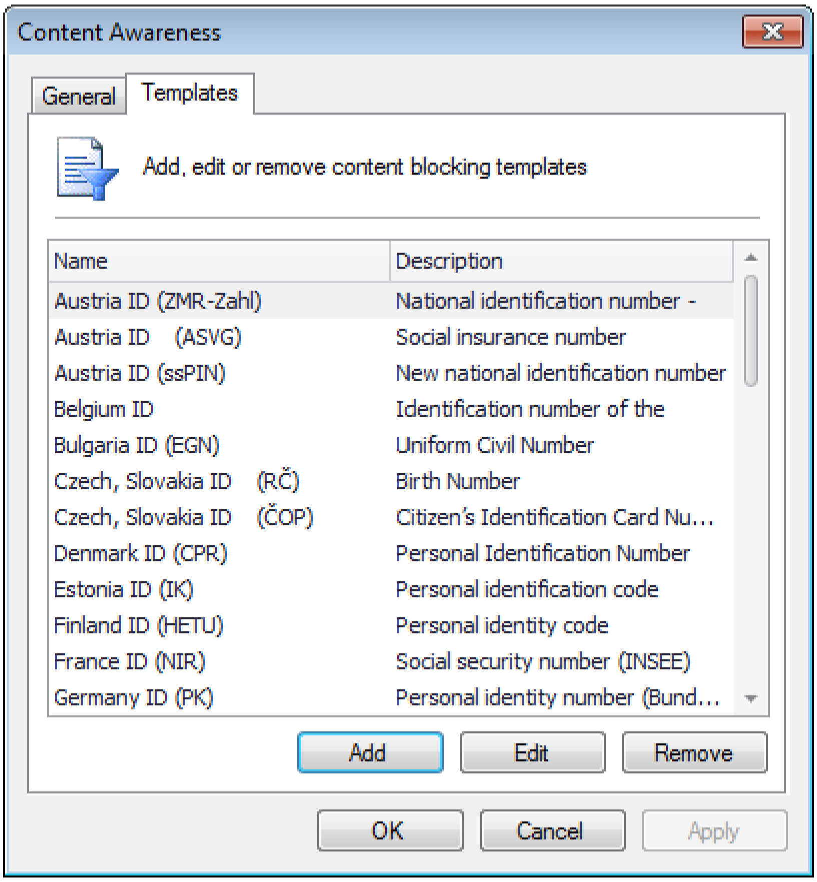
Screenshot 67: Selecting users or groups

5.14.2 Managing template options

To add, edit or remove predefined templates:

1. Click **Templates** and select a template from the **Template** list.

2. Click **Add**, **Edit** or **Remove** to change or delete templates.



Add, edit or remove content blocking templates

Name	Description
Austria ID (ZMR-Zahl)	National identification number -
Austria ID (ASVG)	Social insurance number
Austria ID (ssPIN)	New national identification number
Belgium ID	Identification number of the
Bulgaria ID (EGN)	Uniform Civil Number
Czech, Slovakia ID (RČ)	Birth Number
Czech, Slovakia ID (ČOP)	Citizen's Identification Card Nu...
Denmark ID (CPR)	Personal Identification Number
Estonia ID (IK)	Personal identification code
Finland ID (HETU)	Personal identity code
France ID (NIR)	Social security number (INSEE)
Germany ID (PK)	Personal identity number (Bund...

Screenshot 68: Managing templates

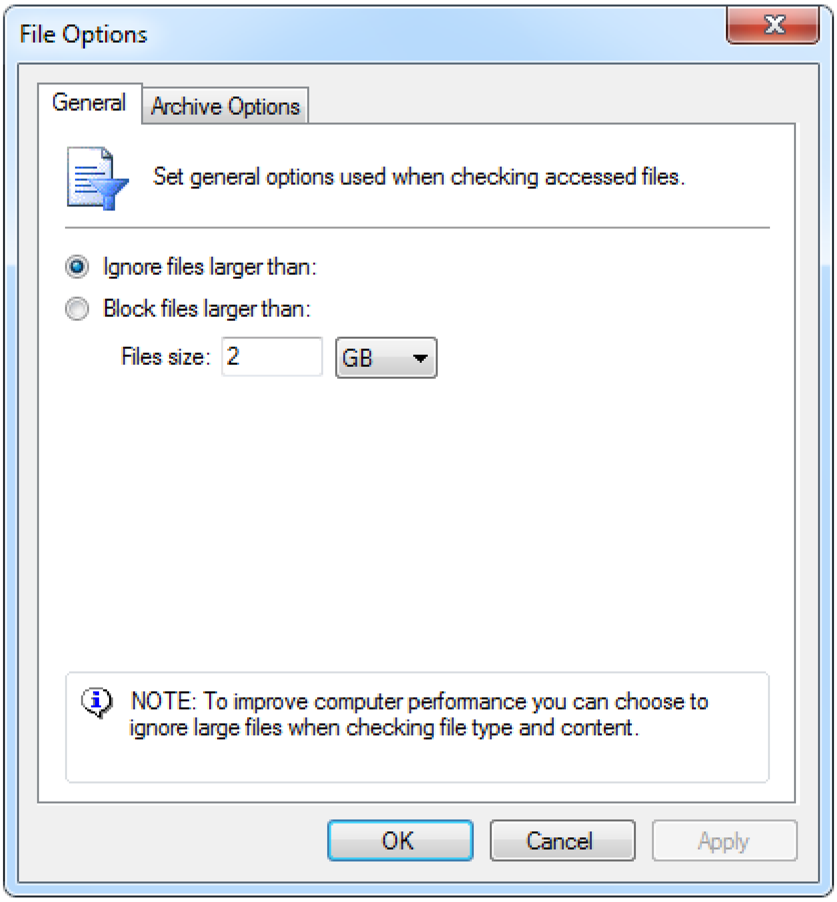
5.15 Configuring file options

GFI EndPointSecurity enables you to specify the options required to block or allow files based on size. GFI EndPointSecurity also enables you to ignore large files when checking file type and content and archived files.

1. From GFI EndPointSecurity management console, click **Configuration** tab **> Protection Policies**.

2. From the left pane, select the protection policy for which you want to specify file options restrictions.

3. From the right pane, click **File options** in the **File control** section.


File Options

General | Archive Options

Set general options used when checking accessed files.

● Ignore files larger than:

○ Block files larger than:

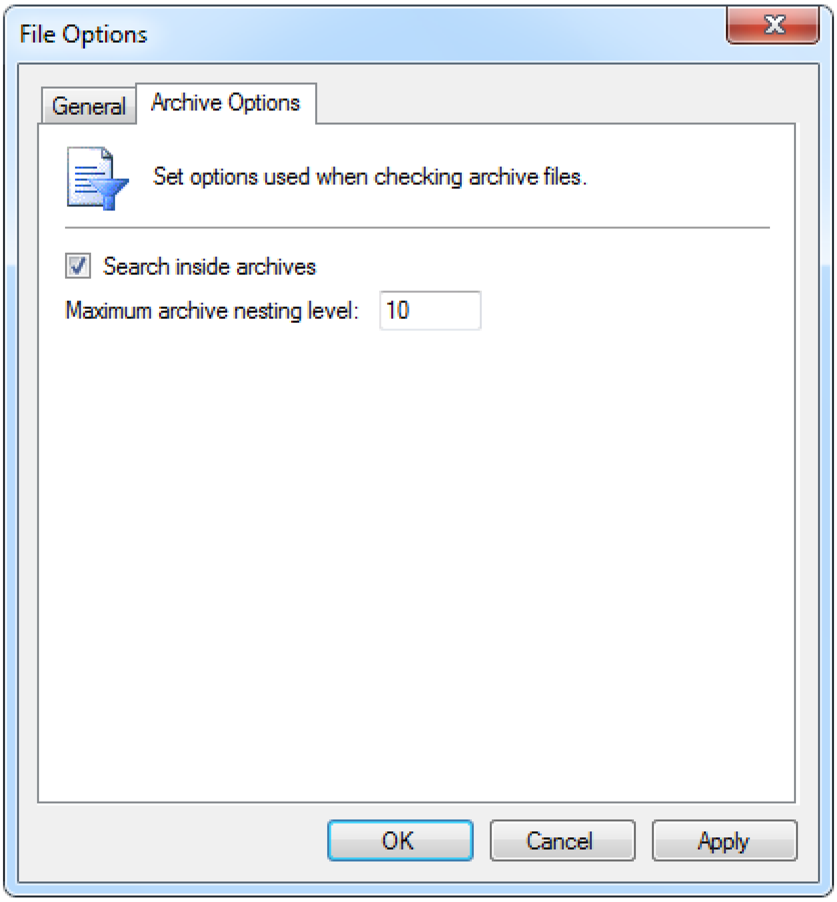
Files size: 2 GB

NOTE: To improve computer performance you can choose to ignore large files when checking file type and content.

Screenshot 69: File options

4. In the File options dialog select from the following options:

Option	Description
Ignore files larger than:	Ignores files larger than the specified size when checking accessed files
Block files larger than :	Blocks files larger than the specified size when checking accessed files



Set options used when checking archive files.

☑ Search inside archives

Maximum archive nesting level: 10

Screenshot 70: File-type Filter and user options

5. From the **Archive Options** tab, enable / disable **Search inside archives** and specify the archive nesting level to use when checking archive files.

6. Click **OK**

5.16 Configuring security encryption

GFI EndPointSecurity enables you to configure settings which specifically cater for encrypted devices. It also enables you to encrypt devices which are not yet secured.

- Configuring Microsoft BitLocker To Go devices
- Configuring Volume Encryption

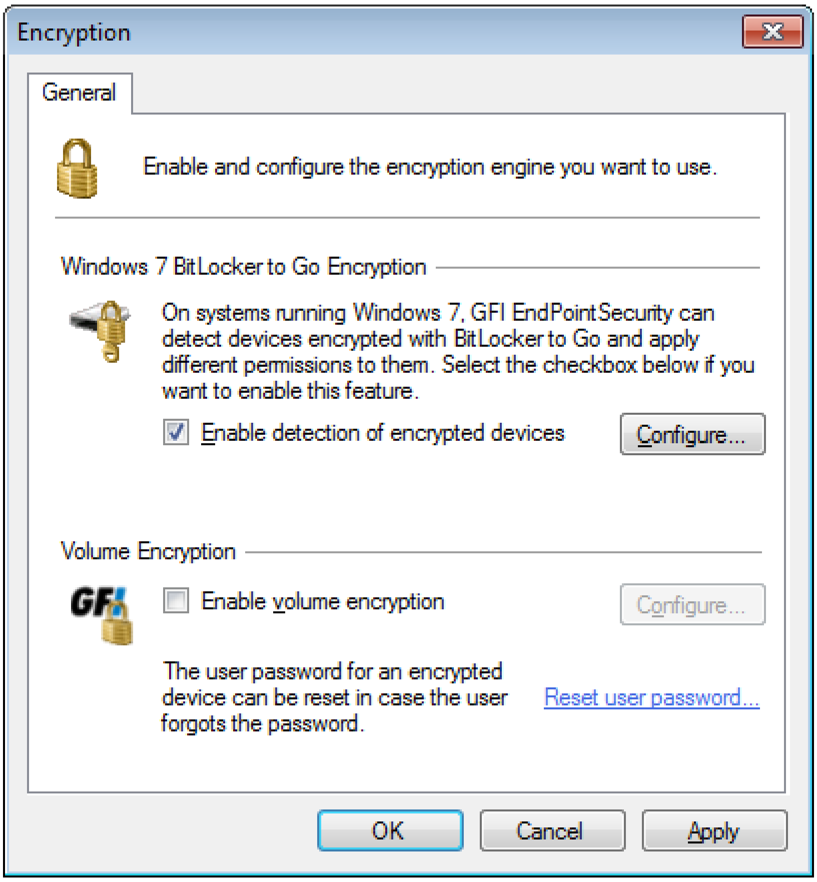
5.16.1 Configuring Microsoft BitLocker To Go devices

GFI EndPointSecurity can detect storage devices encrypted with Microsoft BitLocker To Go. This enables you to configure different permissions on such devices. To enable Microsoft BitLocker To Go detection:

1. From GFI EndPointSecurity management console, click **Configuration** tab **> Protection Policies**.

2. From the left pane, select the protection policy for which to apply the encryption policy.

3. From the right pane, click **Encryption** in the **Security** section.



Enable and configure the encryption engine you want to use.

Windows 7 BitLocker to Go Encryption

On systems running Windows 7, GFI EndPointSecurity can detect devices encrypted with BitLocker to Go and apply different permissions to them. Select the checkbox below if you want to enable this feature.

☑ Enable detection of encrypted devices

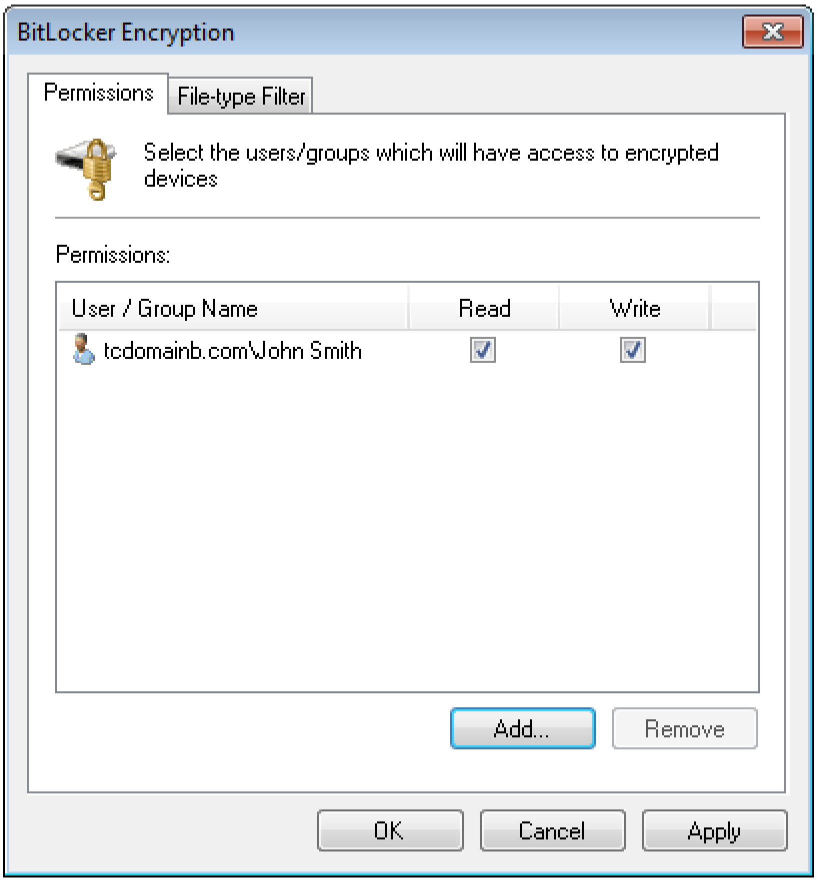
Volume Encryption

□ Enable volume encryption

The user password for an encrypted device can be reset in case the user forgots the password.

Screenshot 71: Encryption options - General tab

4. Select **Enable detection of encrypted devices** and click **Configure**.



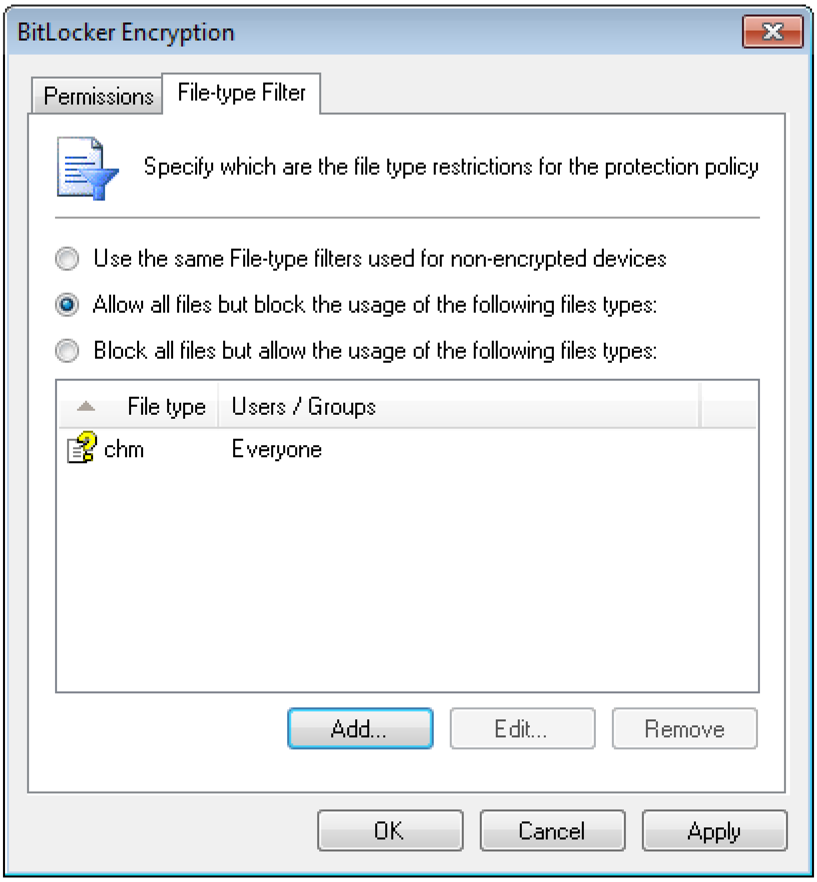
Select the users/groups which will have access to encrypted devices

Permissions:

User / Group Name	Read	Write
tcdomainb.com\John Smith	☑	☑

Screenshot 72: Encryption options - Permissions tab

5. Click **Add…** to specify the users and groups with access to encrypted devices.



Specify which are the file type restrictions for the protection policy

○ Use the same File-type filters used for non-encrypted devices

● Allow all files but block the usage of the following files types:

○ Block all files but allow the usage of the following files types:

File type	Users / Groups
chm	Everyone

Screenshot 73: Encryption options - File-type Filter tab

6. Select the **File-type Filter** tab to configure the file-types to restrict.

7. Select the restriction to apply to this policy:

- Use the same File-type filters used for non-encrypted devices
- Allow all files but block the usage of the following file types
- Block all files but allow the usage of the following file types.

8. Use the **Add**, **Edit** and **Remove** buttons, to manage file types.

9. Click **OK**

5.16.2 Configuring Volume Encryption

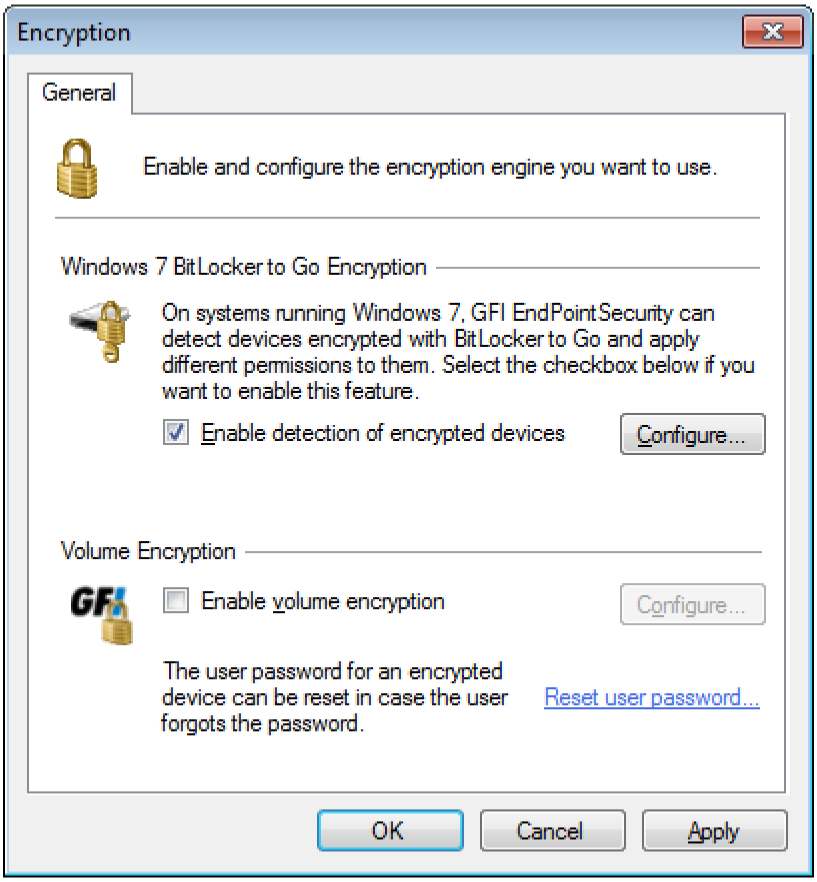
Volume Encryption enables you to encrypt the contents of USB devices using AES 256 encryption. When volume encryption is enforced, users must provide a password to encrypt or access storage devices data. To enforce Volume Encryption on installed agents:

> **Note**
> Encryption on demand is possible even if not forced by the administrator directly by the end user by clicking the **Encrypt...** entry from the shell context menu of a removable drive.

1. From GFI EndPointSecurity management console, click **Configuration** tab **> Protection Policies**.

2. From the left pane, select the protection policy for which to apply encryption policy.

3. From the right pane, click **Encryption** in the **Security** section.



Encryption

General

Enable and configure the encryption engine you want to use.

Windows 7 BitLocker to Go Encryption

On systems running Windows 7, GFI EndPointSecurity can detect devices encrypted with BitLocker to Go and apply different permissions to them. Select the checkbox below if you want to enable this feature.

☑ Enable detection of encrypted devices

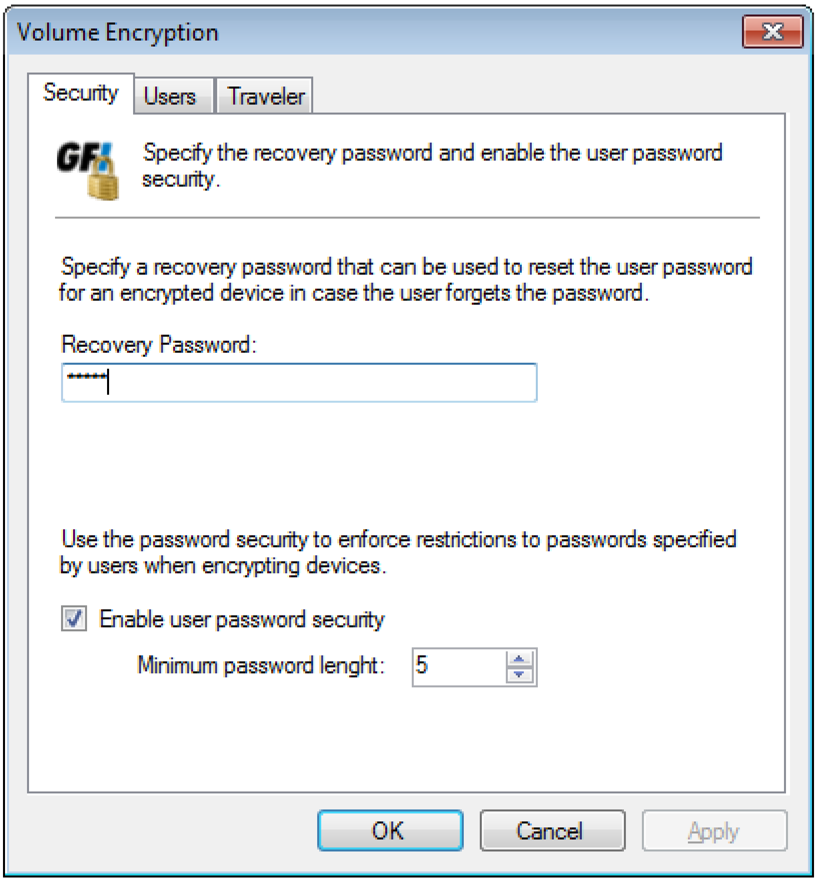
Volume Encryption

□ Enable volume encryption

The user password for an encrypted device can be reset in case the user forgots the password.

Screenshot 74: Encryption options - General tab

4. Select **Enable volume encryption**. Click **Configure**. Click **Reset user password** to reset the encryption password for a specific user.



Specify the recovery password and enable the user password security.

Specify a recovery password that can be used to reset the user password for an encrypted device in case the user forgets the password.

Recovery Password: *****

Use the password security to enforce restrictions to passwords specified by users when encrypting devices.

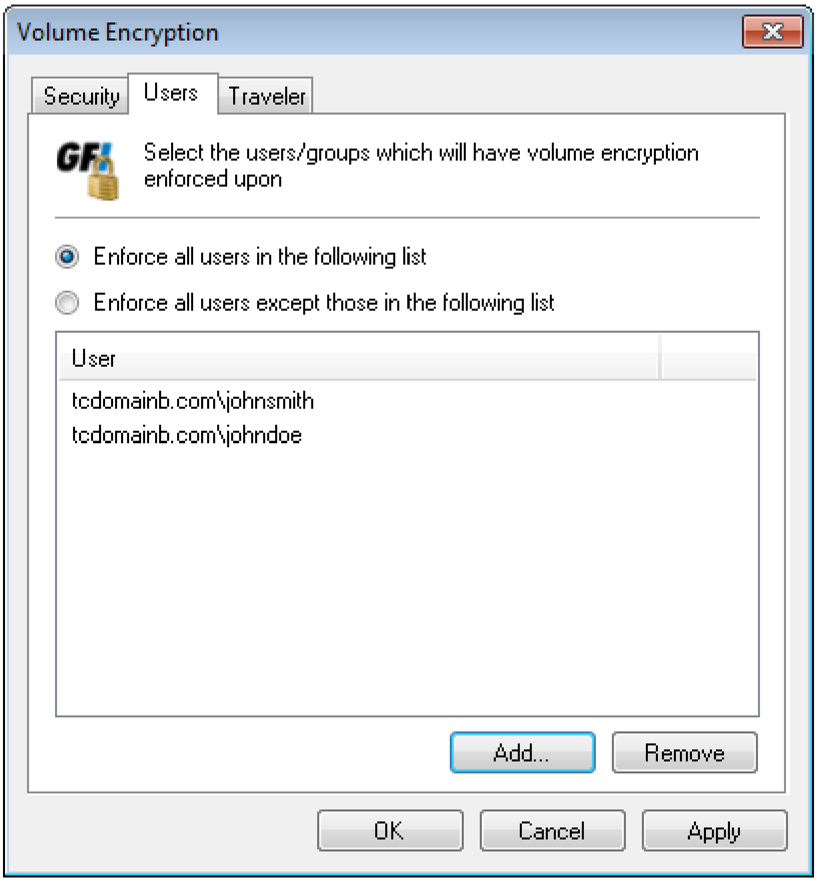
☑ Enable user password security

Minimum password lenght: 5

Screenshot 75: Encryption options -Security tab

5. From the **Security** tab, configure the features described below:

Option	Description
Recovery Password	Key in a password used if users forget or lose their passwords.
Enable user password security	Enforce restrictions to passwords specified by end users. In **Minimum password length**, specify the minimum acceptable password length.



Select the users/groups which will have volume encryption enforced upon

● Enforce all users in the following list

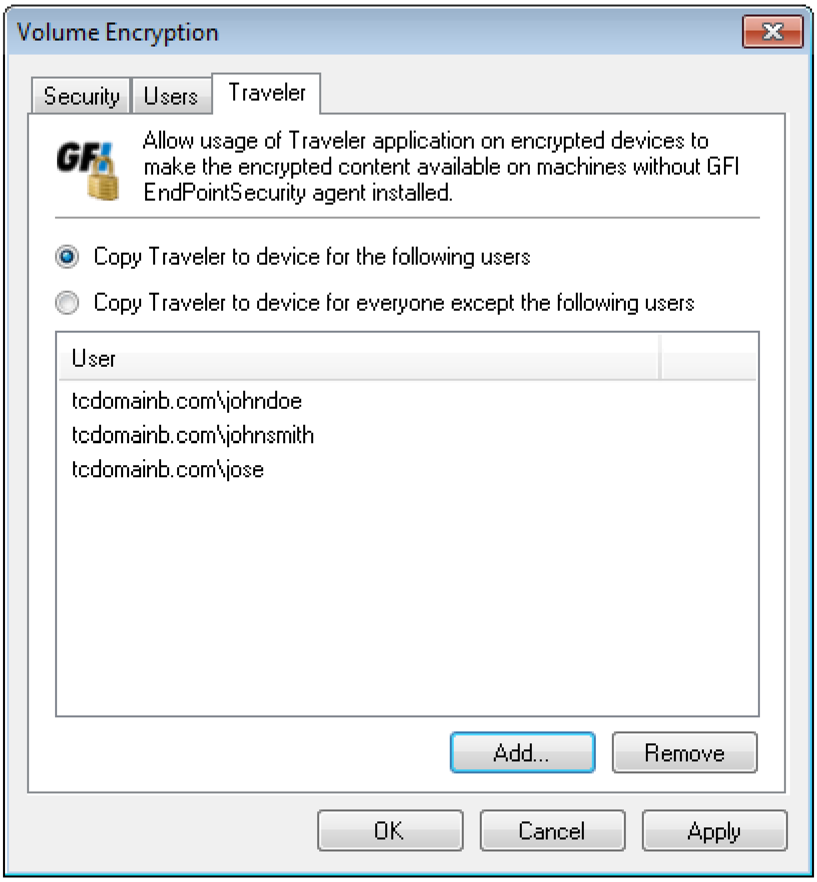
○ Enforce all users except those in the following list

User
tcdomainb.com\johnsmith
tcdomainb.com\johndoe

Screenshot 76: Encryption options - Users tab

6. Select **Users** tab and configure the following options:

Option	Description
Enforce all users in the following list	Select the users that will have volume encryption enforced on their portable devices. Use the **Add** and **Remove** buttons to manage selected users.
Enforce all users except those in the following list	Select the users that will be exempt from volume encryption. Use the Add and Remove buttons to manage selected users.



Allow usage of Traveler application on encrypted devices to make the encrypted content available on machines without GFI EndPointSecurity agent installed.

● Copy Traveler to device for the following users

○ Copy Traveler to device for everyone except the following users

User
tcdomainb.com\johndoe
tcdomainb.com\johnsmith
tcdomainb.com\jose

Screenshot 77: Encryption options - Traveler tab

> **Note**
>
> Traveler is an application that can be automatically installed on storage devices using GFI EndPointSecurity. This application enables you to un-encrypt data encrypted by GFI EndPointSecurity on storage devices, from computers that are not running a GFI EndPointSecurity Agent.

7. Select **Traveler** tab and configure the following options:

Option	Description
Copy Traveler to device for the following users	Select the users that will have Traveler installed on their machines. Use the **Add** and **Remove** buttons to manage selected users.
Copy Traveler to device for everyone except the following users	Select the users that will be exempt from having Traveler installed. Use the **Add** and **Remove** buttons to manage selected users.

8. Click **Apply** and **OK**

5.17 Configuring event logging

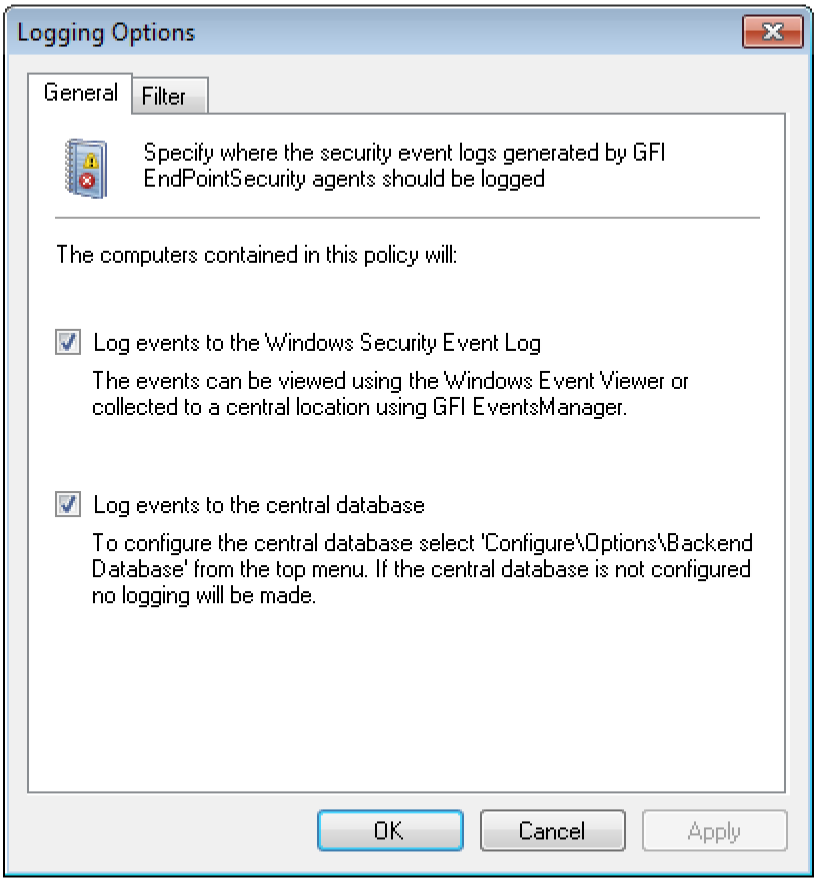
GFI EndPointSecurity agents record events related to attempts made to access devices and connection ports on target computers. The agents also record events related to service operations. You can specify where these events are to be stored, and also what types of events are to be logged. You can do this on a policy by policy basis.

To specify logging options for users in a protection policy:

1. Click **Configuration** tab > **Protection Policies**.

2. From **Protection Policies > Security**, select the protection policy to configure.

3. From the right pane, click **Set Logging Options** in the **Logging and Alerting** section.



Logging Options

General | Filter

Specify where the security event logs generated by GFI EndPointSecurity agents should be logged

The computers contained in this policy will:

☑ Log events to the Windows Security Event Log

The events can be viewed using the Windows Event Viewer or collected to a central location using GFI EventsManager.

☑ Log events to the central database

To configure the central database select 'Configure\Options\Backend Database' from the top menu. If the central database is not configured no logging will be made.

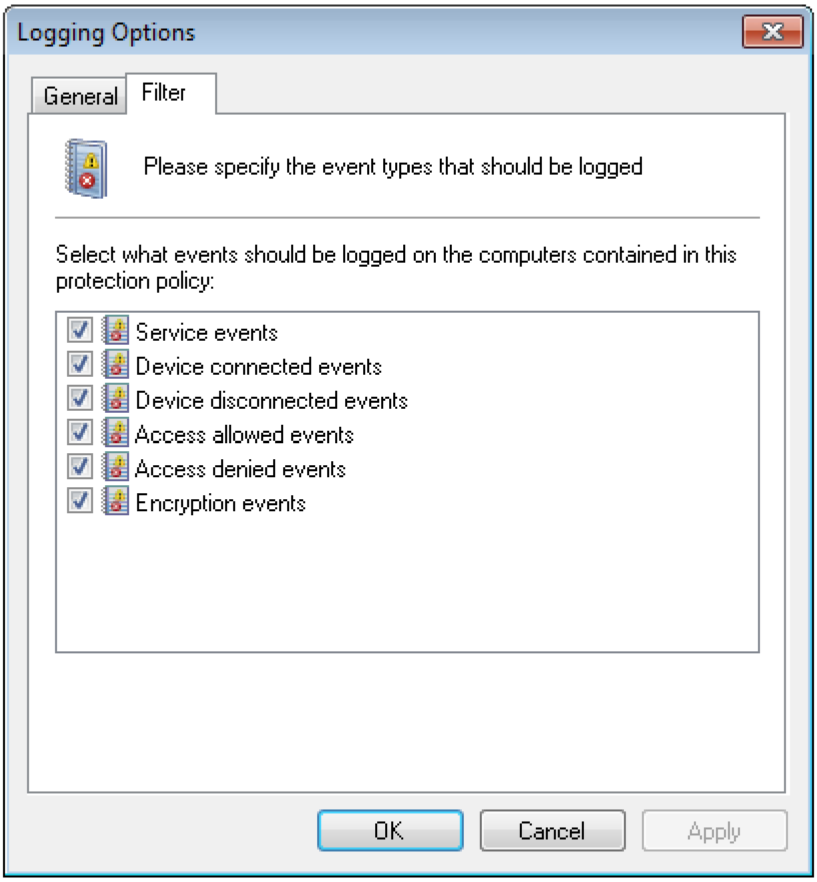
Screenshot 78: Logging Options - General tab

4. In the **Logging Options** dialog, click **General** tab.

5. Enable or disable the locations where to store events generated by this protection policy:

Option	Description
Log events to the Windows Security Event Log	you can view events through the Windows Event Viewer of every target computer or through GFI EventsManager after they are collected in a central location
Log events to the central database	you can view the events within the **Logs Browser** sub-tab in the GFI EndPointSecurity management console. This option requires the configuration of a central database. For more information, refer to Managing the Database Backend (page 131).

If both options are enabled, then the same data is logged in both locations.


Logging Options

Please specify the event types that should be logged

Select what events should be logged on the computers contained in this protection policy:

☑ Service events
☑ Device connected events
☑ Device disconnected events
☑ Access allowed events
☑ Access denied events
☑ Encryption events

Screenshot 79: Logging Options - Filter tab

6. Select **Filter** tab, and select any of the following event types to log by this protection policy. Click **OK**

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.

2. From **Common tasks**, click **Deploy to all computers…**.

5.18 Configuring alerts

GFI EndPointSecurity can be configured to send alerts to specified recipients when particular events are generated. You can configure alerts to be sent through several alerting options, and also specify the types of events for which alerts are sent. You can do this on a policy by policy basis.

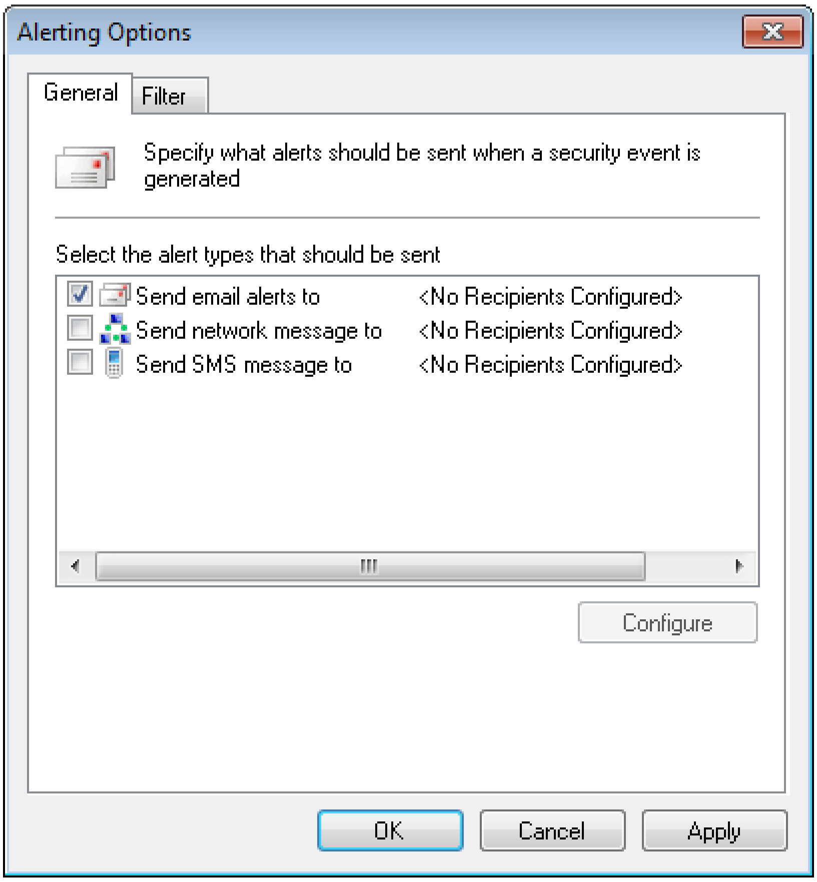
Alert recipients are not Active Directory (AD) users and/or user groups, but are profile accounts created by GFI EndPointSecurity to hold the contact details of users intended to alerts. It is best to create alert recipients prior to configuring alerts. For more information, refer to Configuring alerts recipients (page 128).

To specify alerting options for users in a protection policy:

1. Click **Configuration** tab **> Protection Policies**.

2. From **Protection Policies > Security**, select the protection policy to configure.

3. From the right pane, click **Alerting options** in the **Logging and Alerting** section.



Specify what alerts should be sent when a security event is generated

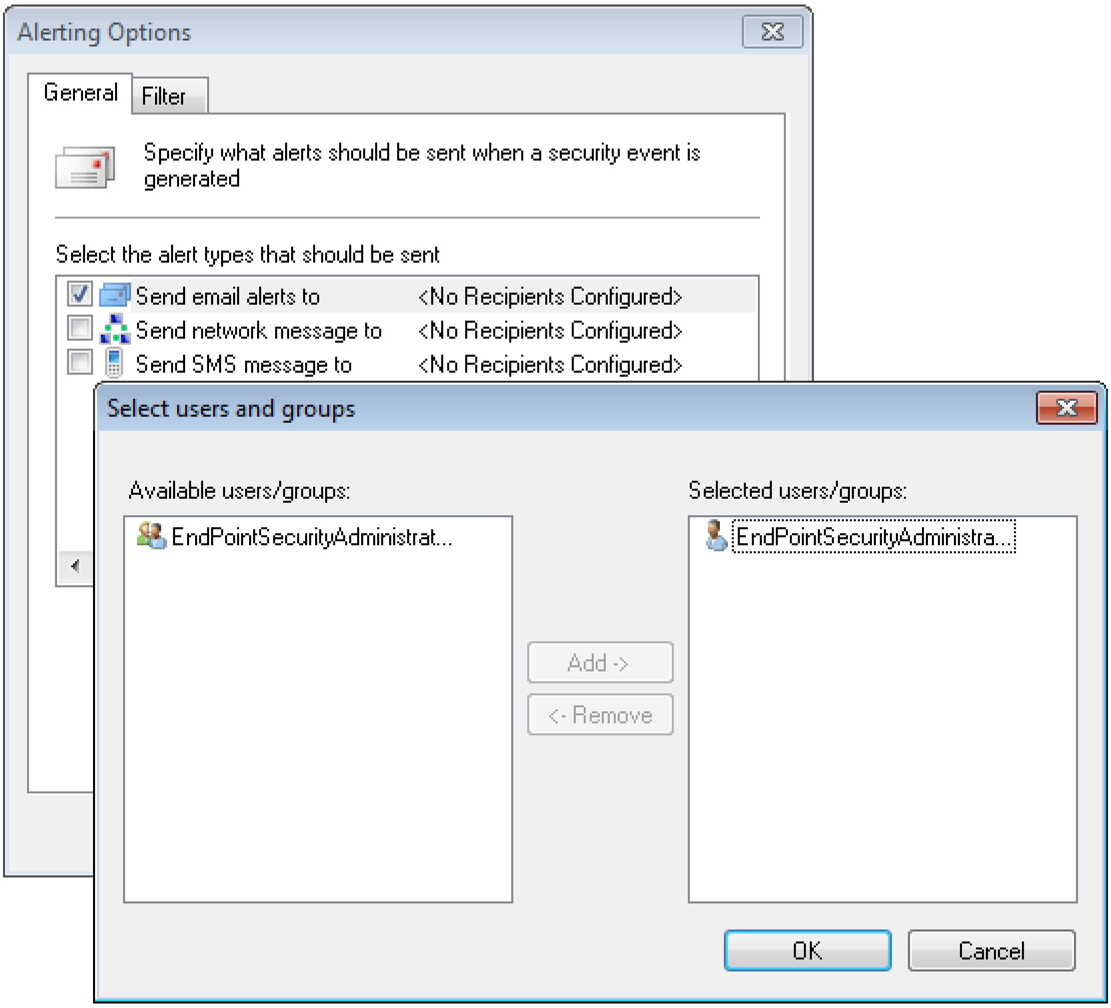
Select the alert types that should be sent

☑ Send email alerts to <No Recipients Configured>
☐ Send network message to <No Recipients Configured>
☐ Send SMS message to <No Recipients Configured>

Screenshot 80: Alerting Options - General tab

4. In the **Alerting Options** dialog, click **General** tab and select any of the following alert types to send:

- Email alerts
- Network messages
- SMS messages.



Specify what alerts should be sent when a security event is generated

Select the alert types that should be sent

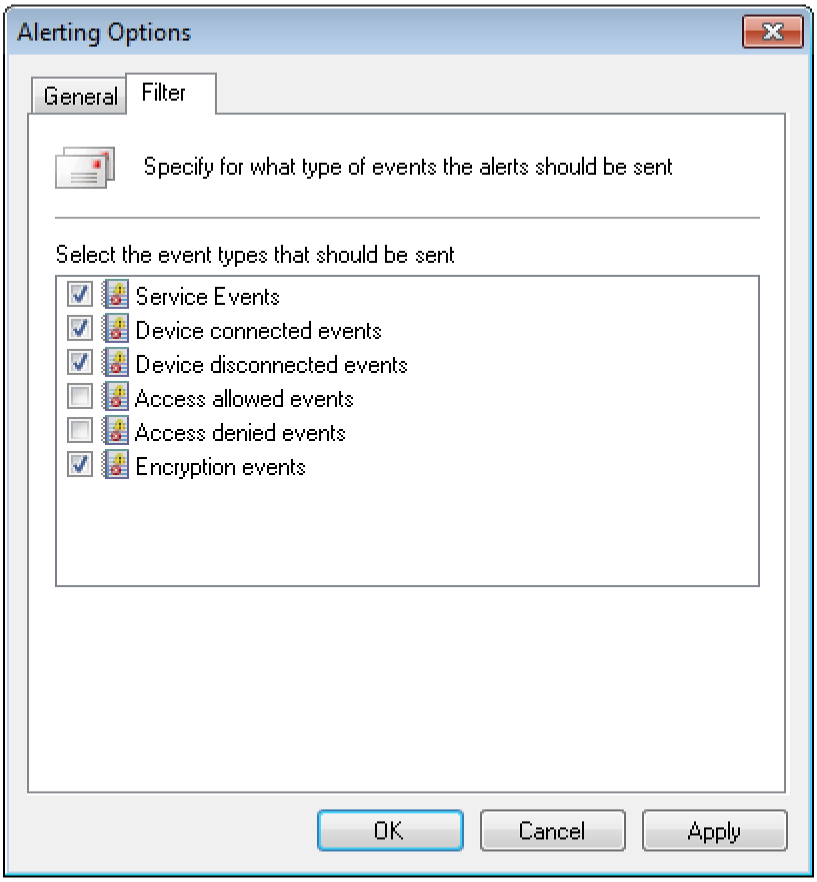
☑ Send email alerts to <No Recipients Configured>
□ Send network message to <No Recipients Configured>
□ Send SMS message to <No Recipients Configured>

Available users/groups: EndPointSecurityAdministrat...

Selected users/groups: EndPointSecurityAdministra...

Screenshot 81: Alerting Options - Configuring users and groups

5. For each alert type enabled, highlight the alert type and click **Configure** to specify alerts recipients. Click **OK**


Alerting Options

General | Filter

Specify for what type of events the alerts should be sent

Select the event types that should be sent

- ☑ Service Events
- ☑ Device connected events
- ☑ Device disconnected events
- □ Access allowed events
- □ Access denied events
- ☑ Encryption events

Screenshot 82: Alerting Options - Filter tab

6. Select **Filter** tab, select any of the following event types for which alerts are sent by this protection policy. Click **OK**

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.

2. From **Common tasks**, click **Deploy to all computers…**.

5.19 Setting a policy as the default policy

GFI EndPointSecurity provides you with the facility to define the protection policy that is assigned to newly discovered network computers by the agent deployment feature. You can do this on a policy by policy basis.

By default the agent deployment feature is set to use the **General Control** protection policy, but you can elect any other protection policy as the default policy.

To elect another protection policy as the default protection policy:

1. Click **Configuration** tab **> Protection Policies**.

2. From **Protection Policies > Security**, select the protection policy to configure.

3. From the left pane, click **Set as default policy** in the **Common tasks** section.

6 Discovering Devices

GFI EndPointSecurity enables you to transparently and rapidly query organizational network endpoints, locating and reporting all devices that are or have been connected to the scanned target computers. The application granularly identifies endpoint devices connected to the target computers, both currently and historically, and displays the detailed information on screen once the scan is complete.

Use the **Scanning** tab to scan target computers and discover connected devices. By default, GFI EndPointSecurity scans all supported device categories and connectivity ports.

A discovered target computer can be any computer on the network, and may not be included in any GFI EndPointSecurity protection policy. The device scan must be executed under an account that has administrative privileges over the target computer(s).

Topics in this chapter

6.1 Running a device scan

Running a device scan is essential in order to discover new devices. GFI EndPointSecurity enables you to search for new devices that are connected to your target computer. This enables you to add new devices as soon as they are detected on it.

> **Note:**
> A new security policy has been introduced in Microsoft Vista, Microsoft Windows 7 and Microsoft Windows 2008 which needs to be enabled in order for the GFI EndPointSecurity device scanner to enumerate the physical devices located on the machine.

To enable remote access to the Plug and play interface:

1. Logon to the Microsoft Windows Vista, 7 or Server 2008 computer with administrative privileges

2. Click **Start** > **Run**.

3. Type in **gpedit.msc**.

4. Browse to **Computer Configuration** > **Administrative Templates** > **System** > **Device Installation**.

5. Right click **Allow remote access to the PnP interface** and select **Properties**.

6. Under the **Settings** tab, select the **Enable** option.

7. Click **Ok** to save changes.

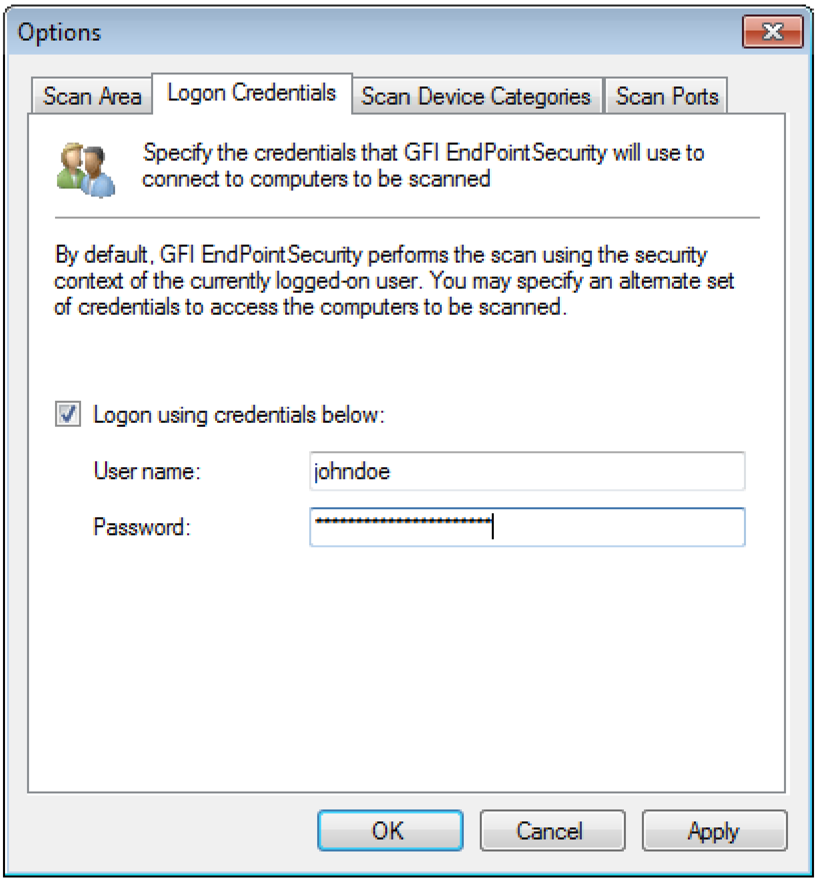
8. Restart the computer.

To run a device scan:

1. Click **Scanning** tab.

2. From **Common tasks**, click **Options**.

3. From the **Options** dialog, select **Logon Credentials** tab.



Specify the credentials that GFI EndPointSecurity will use to connect to computers to be scanned

By default, GFI EndPointSecurity performs the scan using the security context of the currently logged-on user. You may specify an alternate set of credentials to access the computers to be scanned.

☑ Logon using credentials below:

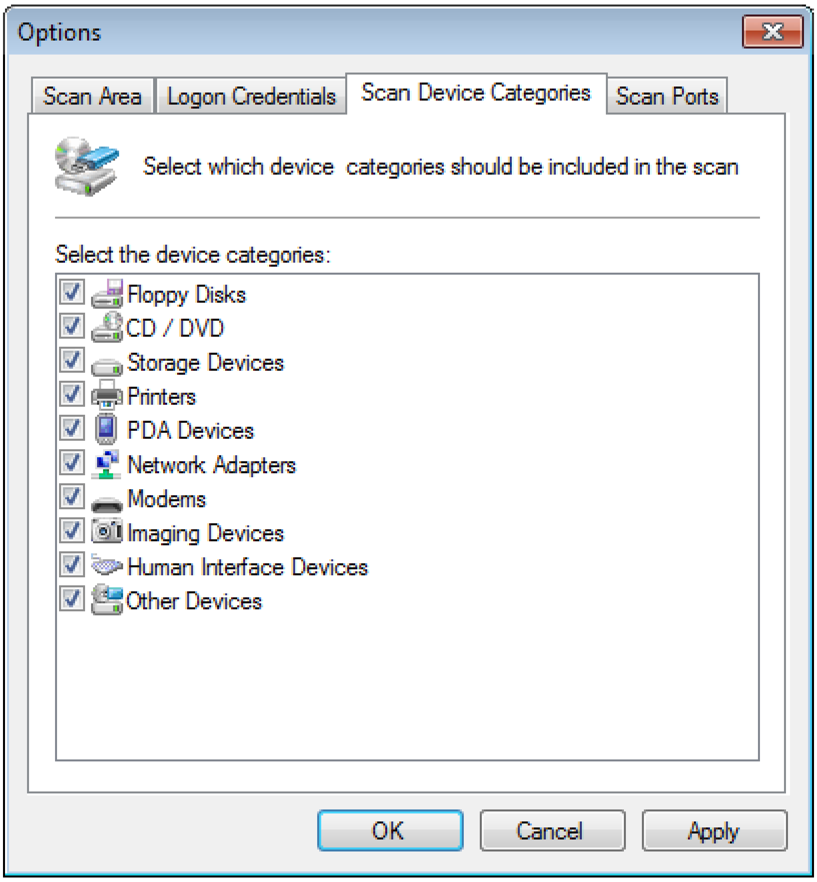
User name: johndoe

Password: ************************

Screenshot 83: Running a device scan - Logon credentials tab

4. From the **Logon Credentials** tab of the **Options** dialog, select/unselect **Logon using credentials below** to enable/disable use of alternate credentials.

> **Note**
>
> If you do not specify any logon credentials, GFI EndPointSecurity attempts to logon the target computer using the currently logged-on user.



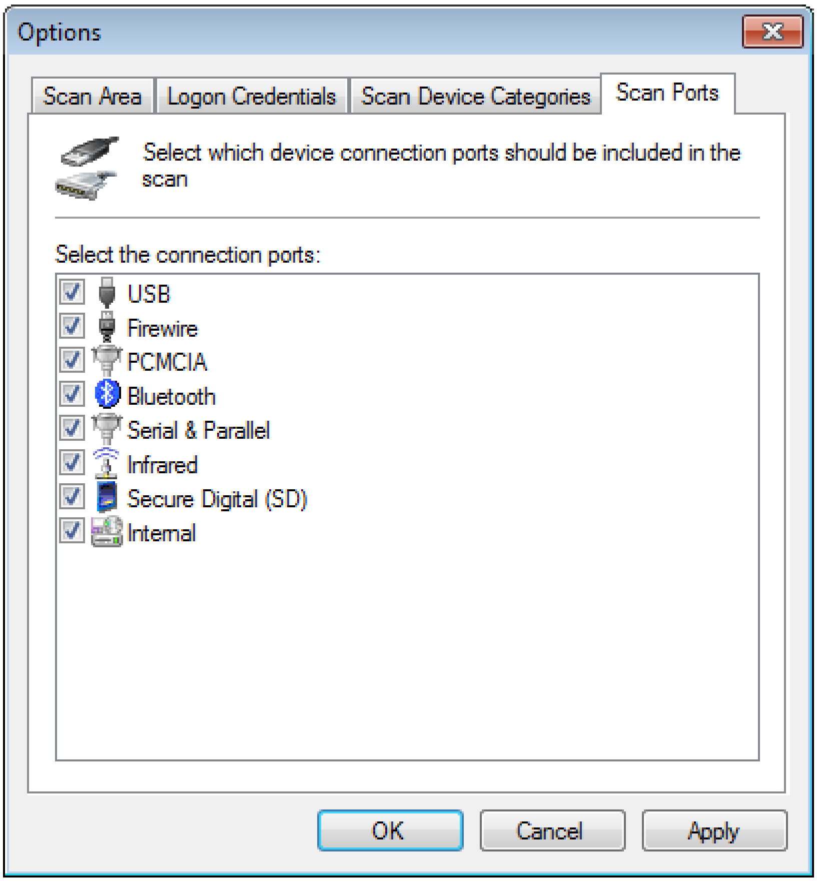
Select which device categories should be included in the scan

Select the device categories:

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

Screenshot 84: Running a device scan - Scan device categories tab

5. Click **Scan Device Categories** tab and select the device categories you want to include in the scan.



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 85: Running a device scan - Scan ports tab

6. Click **Scan Ports** tab and select the connection ports you want to include in the scan.

7. Click **Apply** and **OK**

8. To specify scan target computers:

» In the right pane, key in the computer name or IP address of the target computer(s) in the **Scan target** text box. Click **New Scan** to start scanning the specified computer.

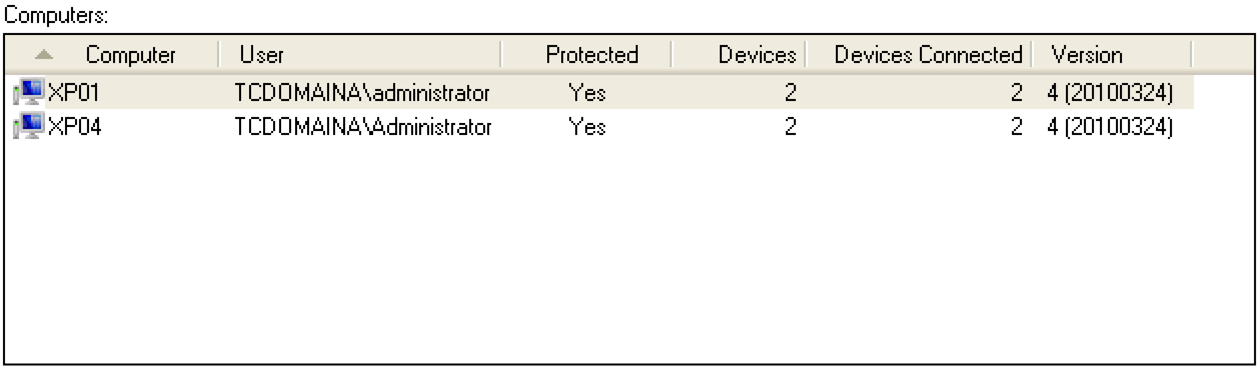
6.2 Analyzing device scan results

Device Scan results are displayed in two sections:

» Computers

» Devices list.

6.2.1 Computers



Computers:

Computer	User	Protected	Devices	Devices Connected	Version
XP01	TCDOMAINA\administrator	Yes	2	2	4 (20100324)
XP04	TCDOMAINA\Administrator	Yes	2	2	4 (20100324)

Screenshot 86: Computers area

This section displays device scan summary results for every scanned target computer, including:

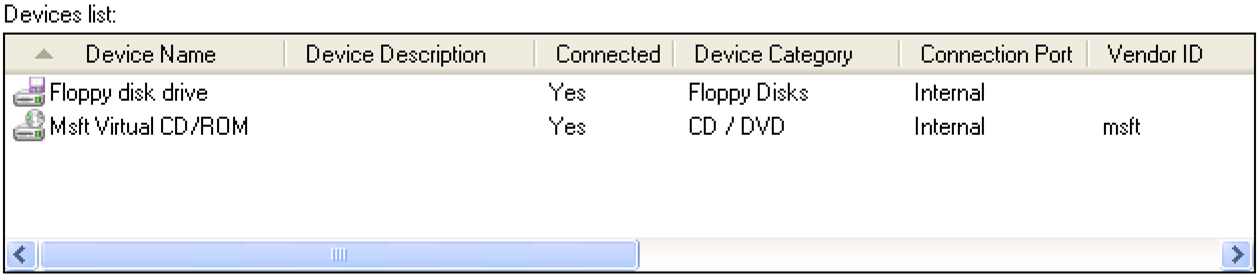
- The computer name / IP address
- The user currently logged on
- Protection status, i.e., whether the computer is included in a GFI EndPointSecurity protection policy
- Total number of devices currently and historically connected
- Number of devices currently connected.

If a scanned target computer is not included in any GFI EndPointSecurity protection policy, you can choose to deploy a protection policy to the computer. To do this:

1. Right-click on the relevant computer name / IP address under **Computer** column, and select **Deploy agent(s)…**

2. Select the protection policy to deploy. Click **Next** to continue and **Finish** to start deployment.

6.2.2 Devices list



Devices list:

Device Name	Device Description	Connected	Device Category	Connection Port	Vendor ID
Floppy disk drive		Yes	Floppy Disks	Internal	
Msft Virtual CD/ROM		Yes	CD / DVD	Internal	msft

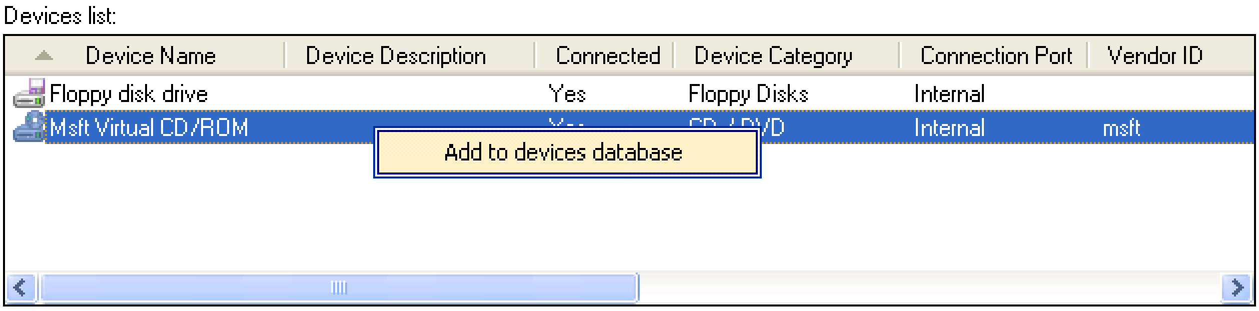
Screenshot 87: Devices list area

This section displays a detailed list of discovered devices for every scanned computer, including:

- Device name, description and category
- Connectivity port
- Connection status, i.e., whether the device is currently connected or not.

6.3 Adding discovered devices to the database

You can select one or more of the discovered devices from the **Devices** list and add them to the devices database. These devices are then retrieved from this database when GFI EndPointSecurity lists the devices currently connected to the target computers for the blacklist and whitelist. For information, refer to Configuring device blacklist or Configuring device whitelist.



Devices list:

Device Name	Device Description	Connected	Device Category	Connection Port	Vendor ID
Floppy disk drive		Yes	Floppy Disks	Internal	
Msft Virtual CD/ROM		Yes	CD / DVD	Internal	msft

Screenshot 88: Devices list area - Add device to devices database

To add devices to the devices database:

1. Select one or more devices to add to the devices database from the **Devices** list section.

2. Right-click on the selected devices and select **Add to devices database**.

3. Click **OK**

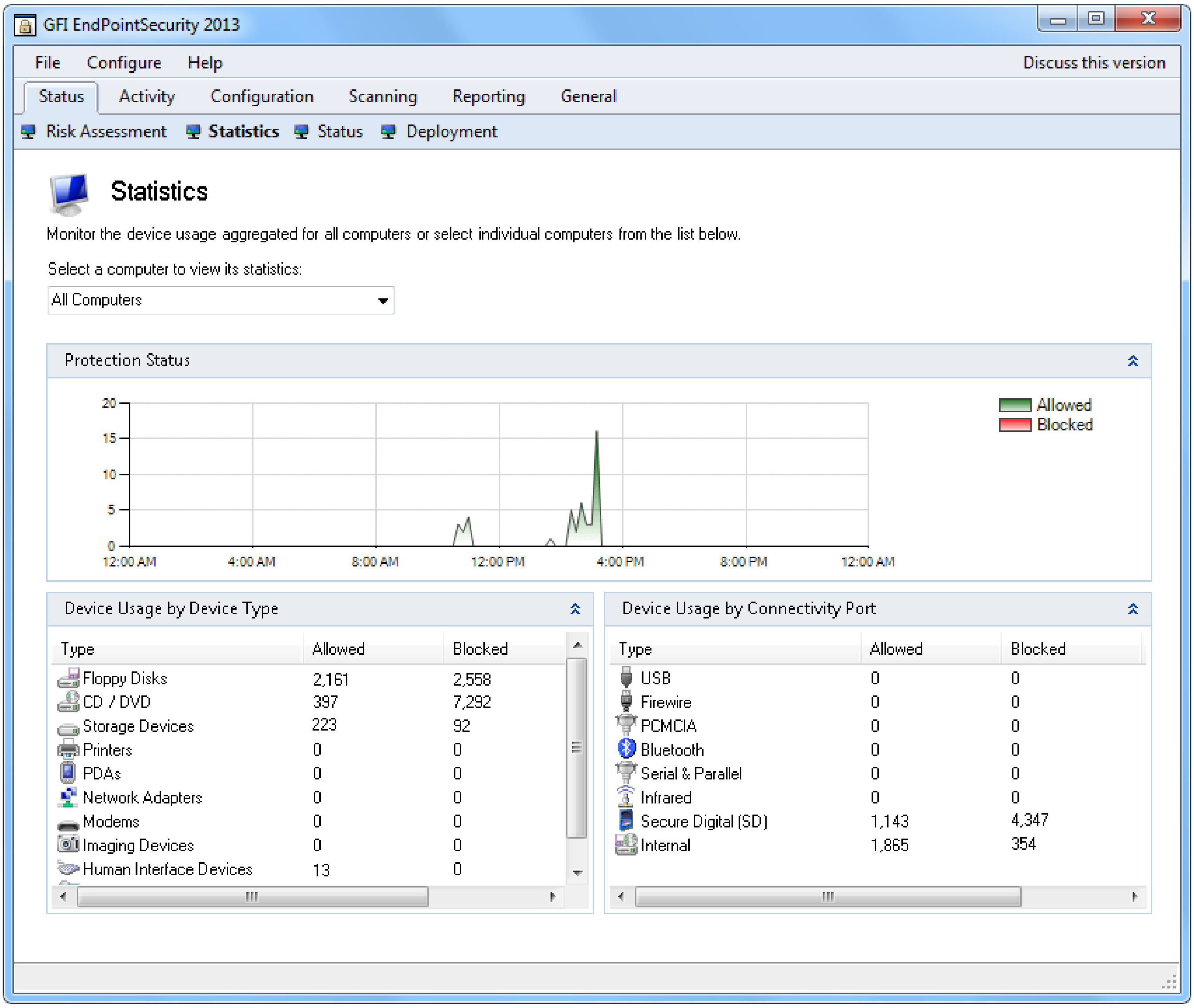
7 Monitoring Device Usage Activity

This chapter provides you with information about monitoring the activity of your network devices. GFI EndPointSecurity enables you to keep an audit trail of all events generated by GFI EndPointSecurity Agents deployed on network computers. To maintain an audit trail, you must enable logging. For more information, refer to Configuring event logging (page 83).

Topics in this chapter

7.1 Statistics

Use the Statistics sub-tab to view the daily device activity trends and statistics for a specific computer or for all network computers.



Statistics

Monitor the device usage aggregated for all computers or select individual computers from the list below.

Select a computer to view its statistics: All Computers

Device Usage by Device Type

Type	Allowed	Blocked
Floppy Disks	2,161	2,558
CD / DVD	397	7,292
Storage Devices	223	92
Printers	0	0
PDAs	0	0
Network Adapters	0	0
Modems	0	0
Imaging Devices	0	0
Human Interface Devices	13	0

Device Usage by Connectivity Port

Type	Allowed	Blocked
USB	0	0
Firewire	0	0
PCMCIA	0	0
Bluetooth	0	0
Serial & Parallel	0	0
Infrared	0	0
Secure Digital (SD)	1,143	4,347
Internal	1,865	354

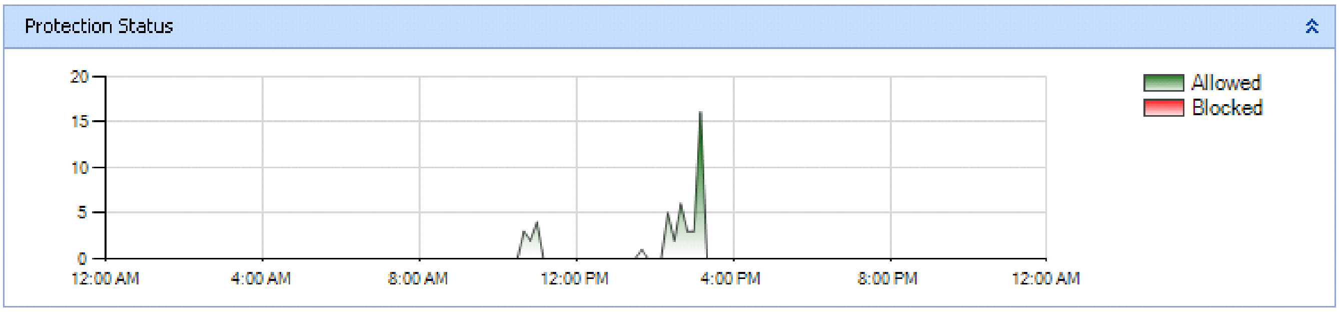
Screenshot 89: Statistics sub-tab

To access the Statistics sub-tab, from GFI EndPointSecurity management console click **Status** tab > **Statistics**.

The **Statistics** section contains information about:

- Protection Status
- Device Usage by Device Type
- Device Usage by Connectivity Port

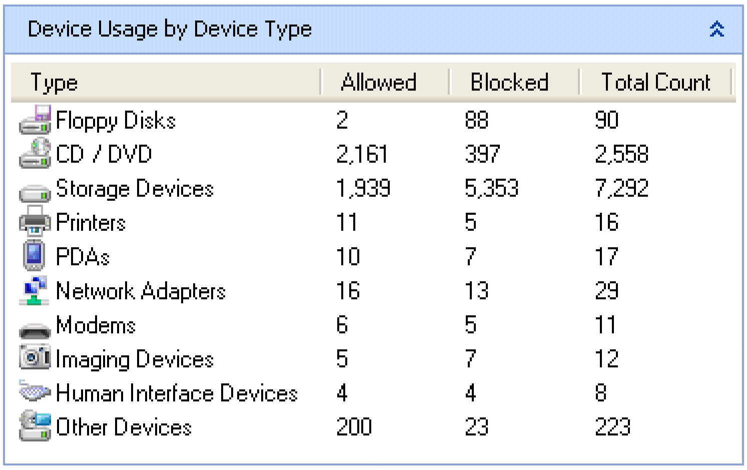
7.1.1 Protection Status



Screenshot 90: Protection Status area

This section graphically represents daily device usage on computers, differentiating between devices that have been blocked and devices that have been allowed by the agents. The information provided can be filtered for a specific computer or for all network computers.

7.1.2 Device Usage by Device Type

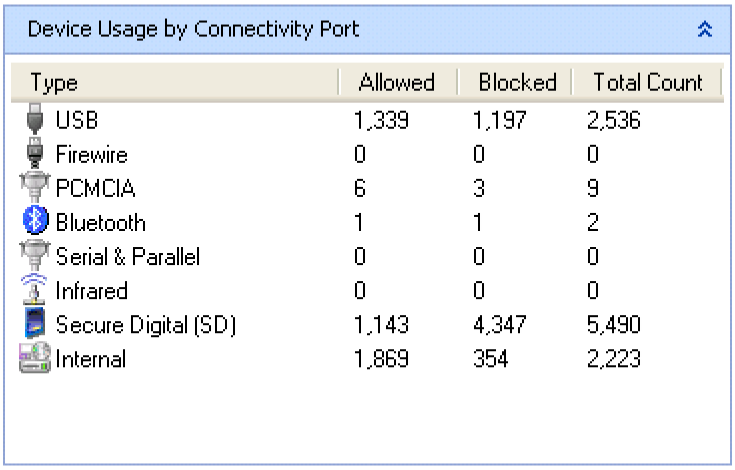


Type	Allowed	Blocked	Total Count
Floppy Disks	2	88	90
CD / DVD	2,161	397	2,558
Storage Devices	1,939	5,353	7,292
Printers	11	5	16
PDAs	10	7	17
Network Adapters	16	13	29
Modems	6	5	11
Imaging Devices	5	7	12
Human Interface Devices	4	4	8
Other Devices	200	23	223

Screenshot 91: Device Usage by Device Type area

This section enumerates device connection attempts by device type, that were either allowed or blocked. The information provided can be filtered for a specific computer or for all network computers.

7.1.3 Device Usage by Connectivity Port



Device Usage by Connectivity Port

Type	Allowed	Blocked	Total Count
USB	1,339	1,197	2,536
Firewire	0	0	0
PCMCIA	6	3	9
Bluetooth	1	1	2
Serial & Parallel	0	0	0
Infrared	0	0	0
Secure Digital (SD)	1,143	4,347	5,490
Internal	1,869	354	2,223

Screenshot 92: Device Usage by Connectivity Port area

This section enumerates device connection attempts by connectivity port, that were either allowed or blocked. The information provided can be filtered for a specific computer or for all network computers.

7.2 Activity

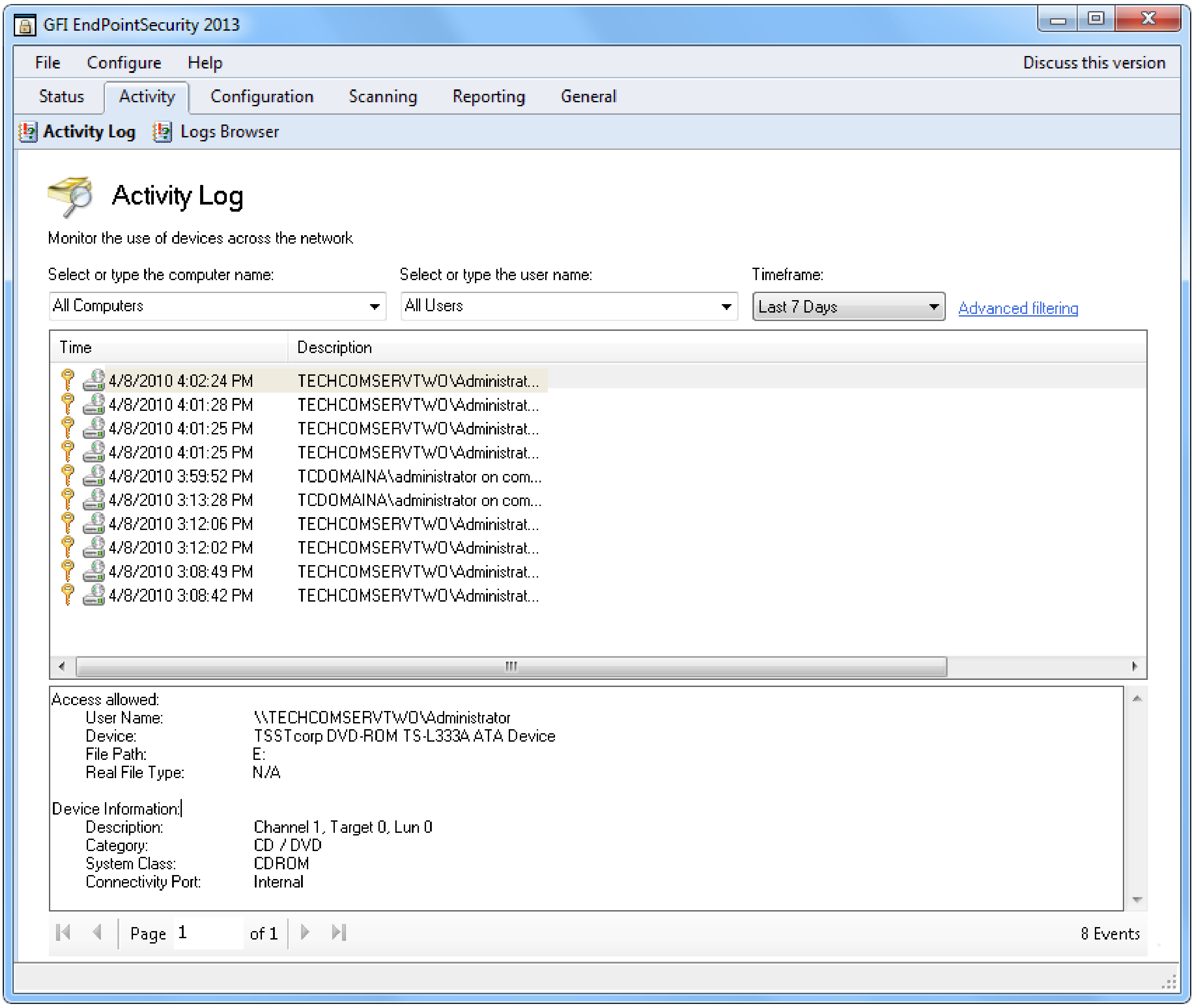
Use the Activity tab to monitor device usage across the network and logged events for a specific computer or for all network computers.

The Activity section contains information about:

- Activity Log
- Advanced Filtering
- Logs Browser
- Creating event queries

7.2.1 Activity Log

This sub-tab allows you to monitor the devices in use on the network. Select the computer and/or user from the relevant drop-down lists to filter the Activity Log list by computer and/or by user. In addition, this tab allows you to further filter down the list by the provided time filters.



Select or type the computer name: All Computers

Select or type the user name: All Users

Timeframe: Last 7 Days

Time	Description
4/8/2010 4:02:24 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 4:01:28 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 4:01:25 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 4:01:25 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 3:59:52 PM	TCDOMAINA\administrator on com...
4/8/2010 3:13:28 PM	TCDOMAINA\administrator on com...
4/8/2010 3:12:06 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 3:12:02 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 3:08:49 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 3:08:42 PM	TECHCOMSERVTWO\Administrat...

```
Access allowed:
      User Name:              \\TECHCOMSERVTWO\Administrator
      Device:                 TSSTcorp DVD-ROM TS-L333A ATA Device
      File Path:              E:
      Real File Type:         N/A

Device Information:
      Description:            Channel 1, Target 0, Lun 0
      Category:               CD / DVD
      System Class:           CDROM
      Connectivity Port:      Internal
```

Screenshot 93: Activity Log sub-tab

To access the Activity Log sub-tab, from GFI EndPointSecurity management console click **Activity** tab **>** **Activity Log**.

To view more details about a particular event, click on the event. Additional information is displayed in the events description pane at the bottom of the sub-tab.

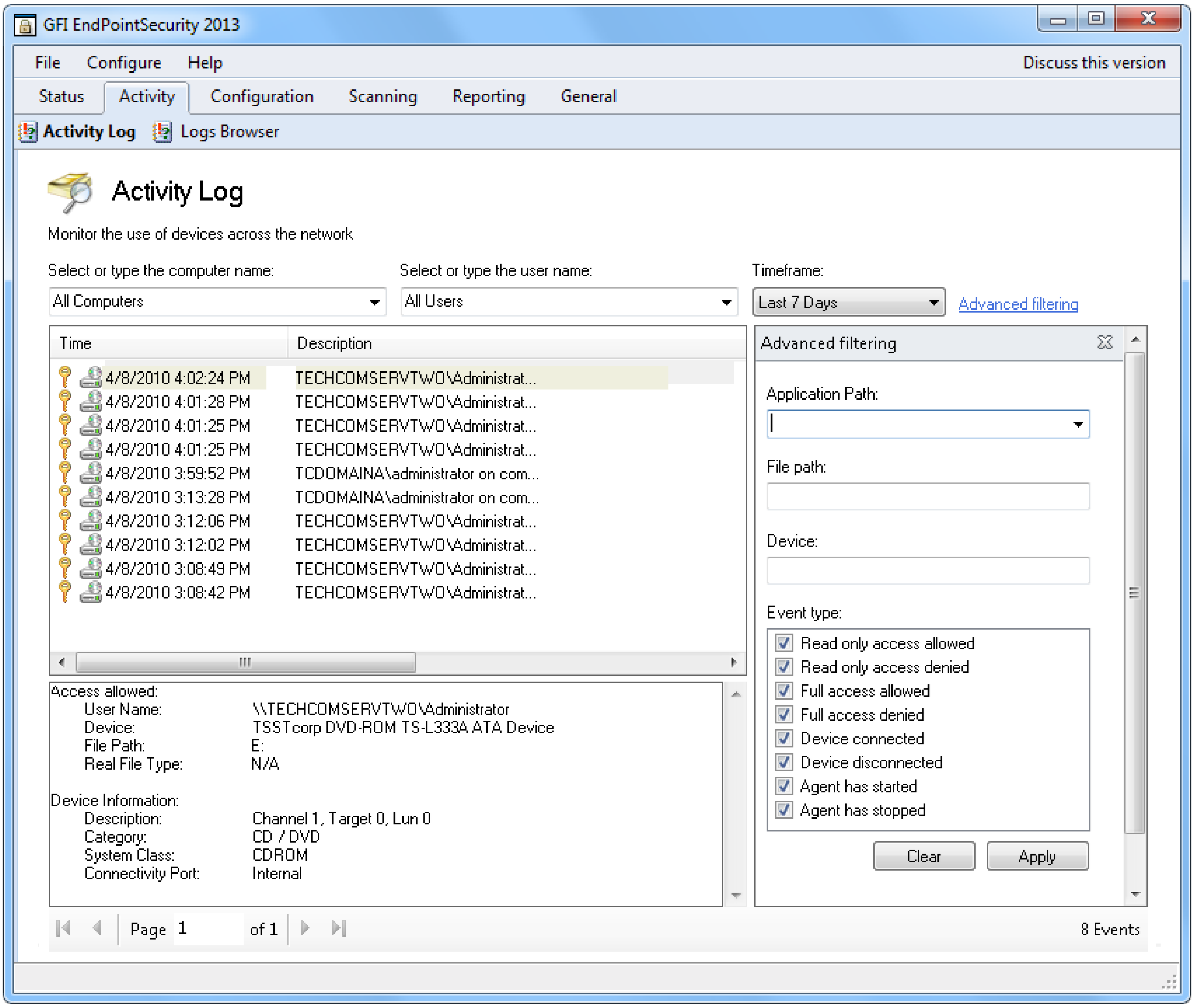
To customize the Activity Log sub-tab to suit your company's needs, right-click the header and select the columns that should be added to or removed from the view.

To change a column's position, select the column header, drag and drop it at the required position.

7.2.2 Advanced Filtering

This feature allows you to further filter down the device usage history logs using one or more criteria from the following set:

- Application Path
- File path
- Device
- Event type.



Activity Log

Monitor the use of devices across the network

Select or type the computer name: All Computers

Select or type the user name: All Users

Timeframe: Last 7 Days

Advanced filtering

Time	Description
4/8/2010 4:02:24 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 4:01:28 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 4:01:25 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 4:01:25 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 3:59:52 PM	TCDOMAINA\administrator on com...
4/8/2010 3:13:28 PM	TCDOMAINA\administrator on com...
4/8/2010 3:12:06 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 3:12:02 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 3:08:49 PM	TECHCOMSERVTWO\Administrat...
4/8/2010 3:08:42 PM	TECHCOMSERVTWO\Administrat...

```
Access allowed:
      User Name:           \\TECHCOMSERVTWO\Administrator
      Device:              TSSTcorp DVD-ROM TS-L333A ATA Device
      File Path:           E:
      Real File Type:      N/A

Device Information:
      Description:         Channel 1, Target 0, Lun 0
      Category:            CD / DVD
      System Class:        CDROM
      Connectivity Port:   Internal
```

Advanced filtering

Application Path:

File path:

Device:

Event type:

- ☑ Read only access allowed
- ☑ Read only access denied
- ☑ Full access allowed
- ☑ Full access denied
- ☑ Device connected
- ☑ Device disconnected
- ☑ Agent has started
- ☑ Agent has stopped

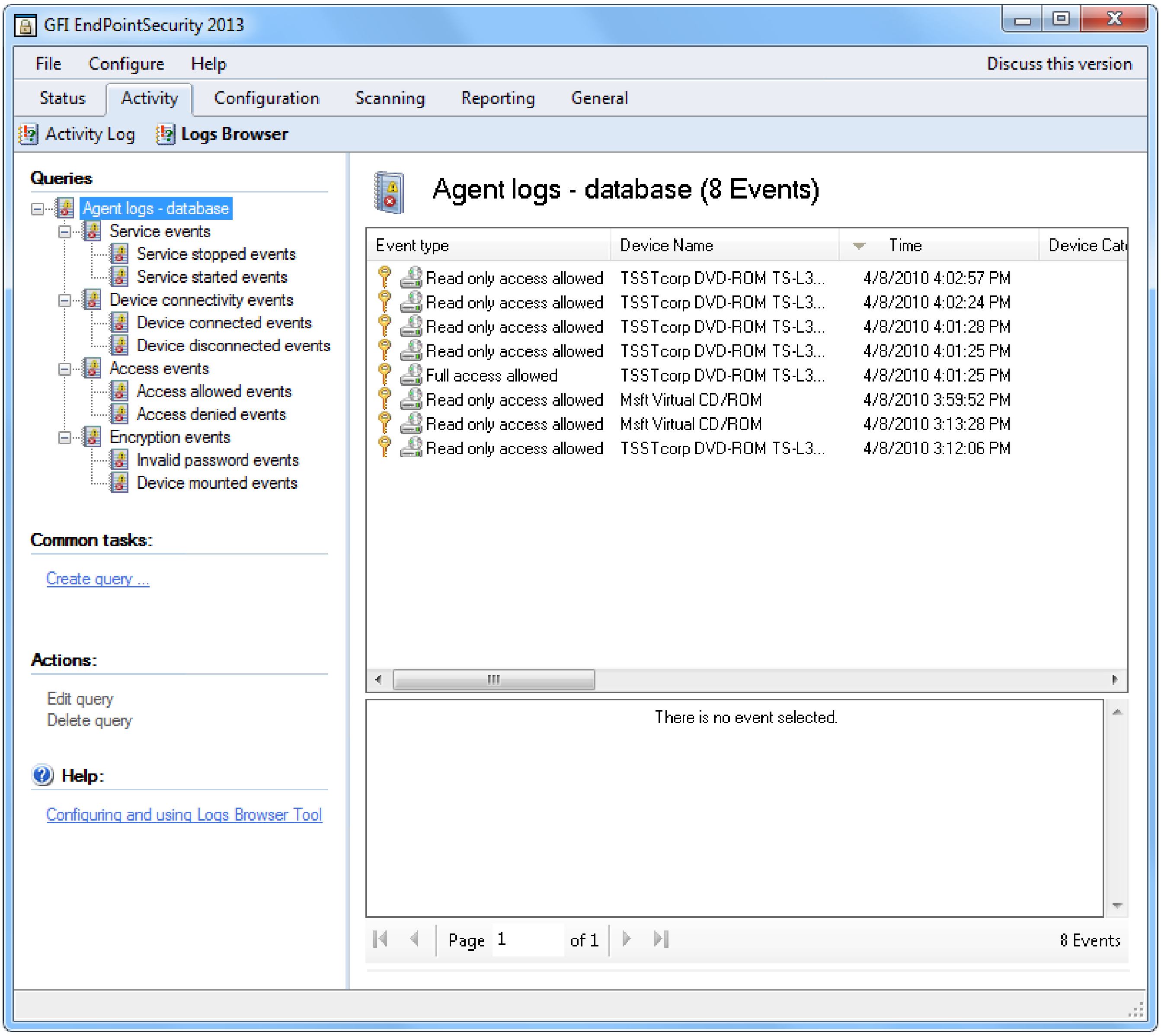
Screenshot 94: Activity Log sub-tab - Advanced filtering

To access advanced filtering options of Activity Log, click **Advanced filtering** in the **Activity Log** sub-tab.

7.2.3 Logs Browser

The Logs Browser sub-tab allows you to access and browse events currently stored in the database backend.

GFI EndPointSecurity also includes a query builder to simplify searching for specific events. With the events query builder you can create custom filters that filter events data and display only the information that you need to browse - without deleting records from your database backend.



Agent logs - database (8 Events)

Event type	Device Name	Time	Device Cat
Read only access allowed	TSSTcorp DVD-ROM TS-L3...	4/8/2010 4:02:57 PM	
Read only access allowed	TSSTcorp DVD-ROM TS-L3...	4/8/2010 4:02:24 PM	
Read only access allowed	TSSTcorp DVD-ROM TS-L3...	4/8/2010 4:01:28 PM	
Read only access allowed	TSSTcorp DVD-ROM TS-L3...	4/8/2010 4:01:25 PM	
Full access allowed	TSSTcorp DVD-ROM TS-L3...	4/8/2010 4:01:25 PM	
Read only access allowed	Msft Virtual CD/ROM	4/8/2010 3:59:52 PM	
Read only access allowed	Msft Virtual CD/ROM	4/8/2010 3:13:28 PM	
Read only access allowed	TSSTcorp DVD-ROM TS-L3...	4/8/2010 3:12:06 PM	

There is no event selected.

Screenshot 95: Logs Browser sub-tab

To access the Logs Browser sub-tab, from GFI EndPointSecurity management console click **Activity** tab > **Logs Browser**.

To view more details about a particular event, click on the event. Additional information is displayed in the events description pane at the bottom of the sub-tab.

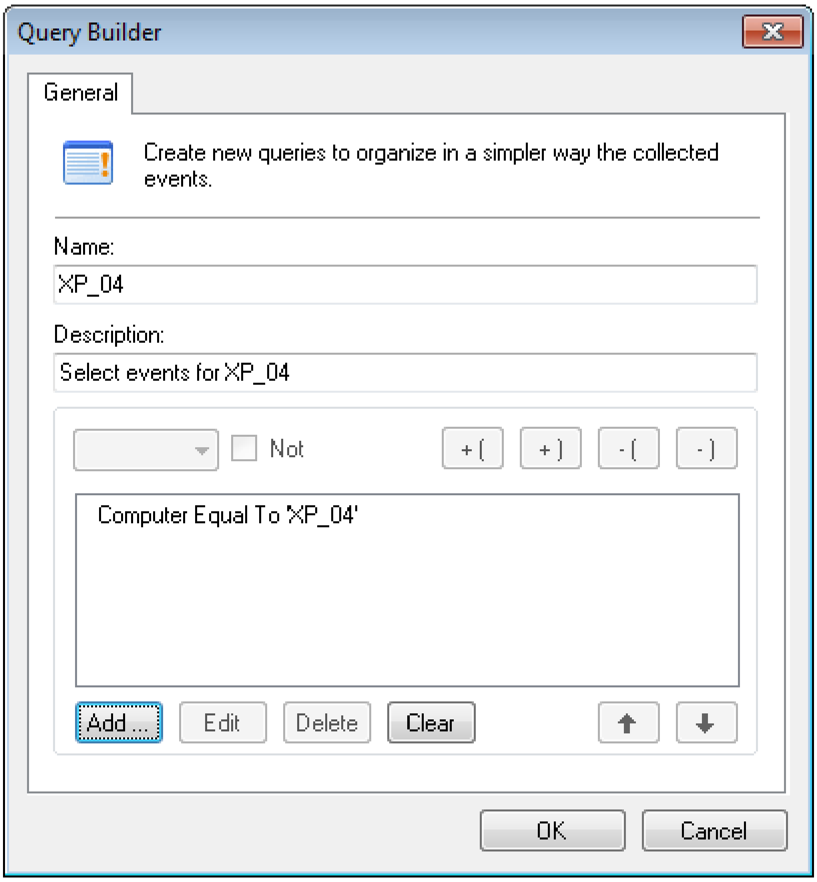
7.2.4 Creating event queries

To create custom event queries:

1. From GFI EndPointSecurity management console, click **Activity** tab.

2. Click **Logs Browser** sub-tab.

3. In the left pane, right-click **Agent logs - database** node and select **Create query…**.



Query Builder

General

Create new queries to organize in a simpler way the collected events.

Name: XP_04

Description: Select events for XP_04

Computer Equal To 'XP_04'

Screenshot 96: Query Builder options

4. In the **Query Builder** dialog, specify a name and a description for the new query.

5. Click **Add…**, configure the required query condition(s) and click **OK** Repeat until all required query conditions have been specified.

6. Click **OK** to finalize your settings. The custom query is added as a sub-node within **Agent logs - database** node.

> **Note**
>
> You can also filter the results of existing event queries by creating more specific sub-queries. To do this right-click on a query and select **Create query…**.

8 Status Monitoring

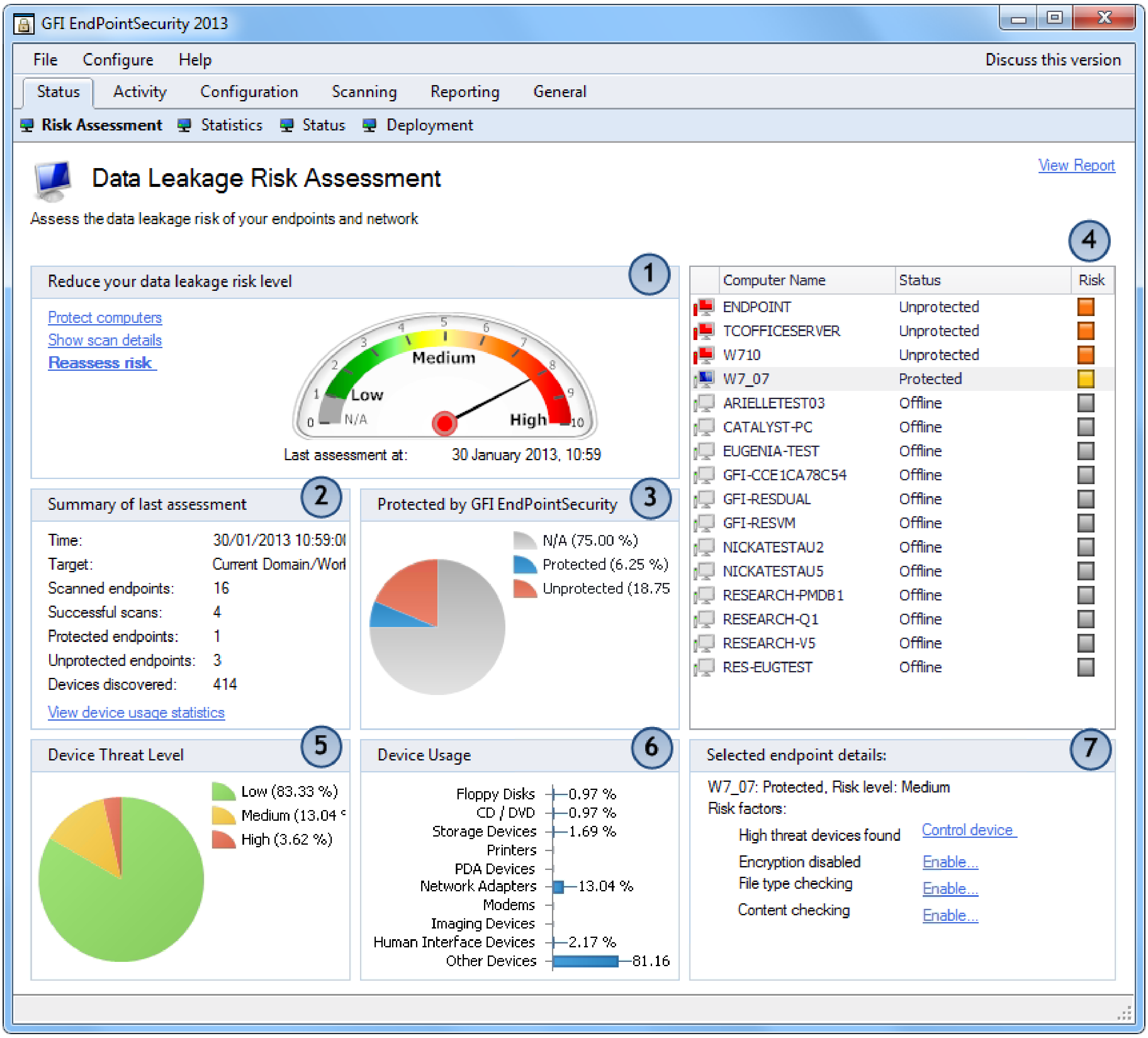
This chapter provides with information related to monitoring the status of GFI EndPointSecurity as well as the status of GFI EndPointSecurity Agents. The status views provide you with graphs and statistical information related to device usage.

Topics in this chapter

8.1 Risk Assessment view

Use the Risk Assessment sub-tab to view the status of:

- Risk assessment level on the network computers with GFI EndPointSecurity agents installed on them.
- GFI EndPointSecurity agents deployed on network computers.
- Device usage such as the number and percentage of devices blocked and the number of devices allowed.
- Device threat level of devices on the network.



Data Leakage Risk Assessment

Assess the data leakage risk of your endpoints and network

Reduce your data leakage risk level

Protect computers
Show scan details
Reassess risk

Last assessment at: 30 January 2013, 10:59

Summary of last assessment

Time:	30/01/2013 10:59:0(
Target:	Current Domain/Worl
Scanned endpoints:	16
Successful scans:	4
Protected endpoints:	1
Unprotected endpoints:	3
Devices discovered:	414

View device usage statistics

Protected by GFI EndPointSecurity

Device Threat Level

Device Usage

Computer Name	Status	Risk
ENDPOINT	Unprotected	🟧
TCOFFICESERVER	Unprotected	🟧
W710	Unprotected	🟧
W7_07	Protected	🟨
ARIELLETEST03	Offline	▢
CATALYST-PC	Offline	▢
EUGENIA-TEST	Offline	▢
GFI-CCE1CA78C54	Offline	▢
GFI-RESDUAL	Offline	▢
GFI-RESVM	Offline	▢
NICKATESTAU2	Offline	▢
NICKATESTAU5	Offline	▢
RESEARCH-PMDB1	Offline	▢
RESEARCH-Q1	Offline	▢
RESEARCH-V5	Offline	▢
RES-EUGTEST	Offline	▢

Selected endpoint details:

W7_07: Protected, Risk level: Medium
Risk factors:

High threat devices found	Control device
Encryption disabled	Enable...
File type checking	Enable...
Content checking	Enable...

Screenshot 97: Risk Assessment sub-tab

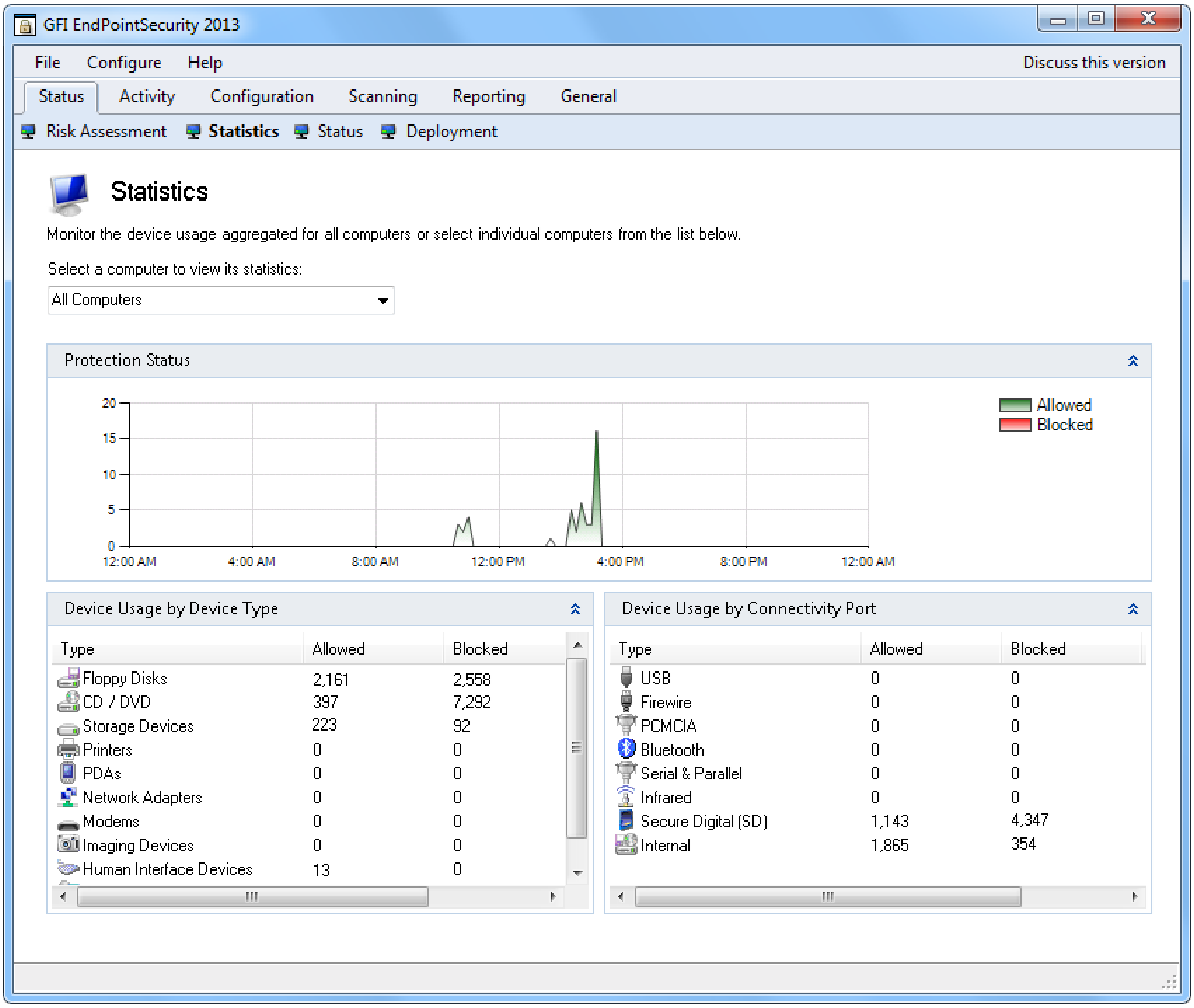
To access the Risk Assessment sub-tab, from GFI EndPointSecurity management console click **Status** tab > **Risk Assessment**.

Feature	Description
1	This section shows: » The gauge showing risk assessment results of the network computers. » The option to re-scan the network to obtain the latest risk assessment results. » The Time of the last risk assessment.

Feature	Description
2	This section lists the cumulative values of the number of: » Scanned endpoints » Successful scans » Protected endpoints » Unprotected endpoints » Devices discovered This section also represents: » The network where agents are installed » The time and date of the last risk assessment.
3	This section graphically represents the number of agents that are currently: » Awaiting installation on network computers » Protected by GFI EndPointSecurity » Not protected by GFI EndPointSecurity
4	This section represents all agents deployed on network computers, differentiating between those currently online and those that are offline. For more information, refer to Status view (page 107).
5	This section graphically represents the device threat percentage levels as logged by the agents of network computers that have GFI EndPointSecurity installed on them.
6	This section graphically represents the percentages of user accesses per device category of the total cumulative amount of user accesses to devices, as logged by the agents. User accesses to devices refer to both allowed and blocked device accesses.
7	This section lists: » The user account under which the GFI EndPointSecurity service is running. » The risk factor level. » The current encryption status on the endpoint. » The file type checking feature status. » The content checking feature status.

8.2 Statistics view

Use the Statistics sub-tab to view the daily device activity trends and statistics for a specific computer or for all network computers.



Statistics

Monitor the device usage aggregated for all computers or select individual computers from the list below.

Select a computer to view its statistics: All Computers

Protection Status

Device Usage by Device Type

Type	Allowed	Blocked
Floppy Disks	2,161	2,558
CD / DVD	397	7,292
Storage Devices	223	92
Printers	0	0
PDAs	0	0
Network Adapters	0	0
Modems	0	0
Imaging Devices	0	0
Human Interface Devices	13	0

Device Usage by Connectivity Port

Type	Allowed	Blocked
USB	0	0
Firewire	0	0
PCMCIA	0	0
Bluetooth	0	0
Serial & Parallel	0	0
Infrared	0	0
Secure Digital (SD)	1,143	4,347
Internal	1,865	354

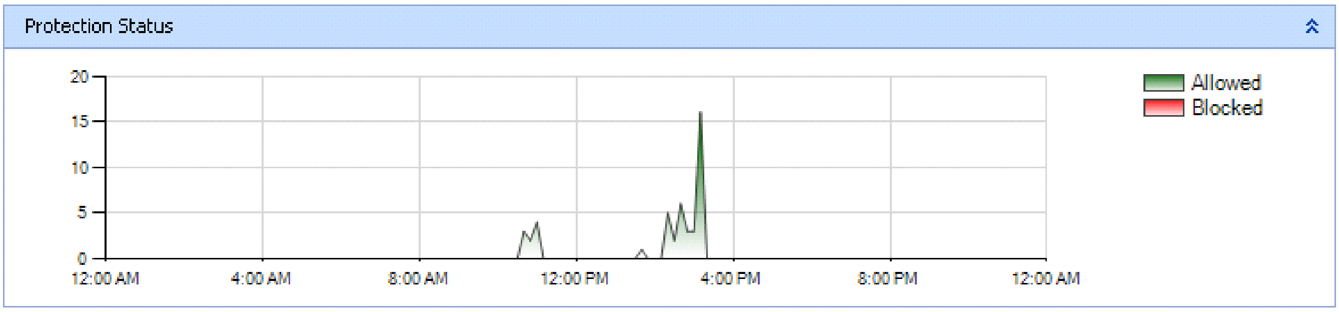
Screenshot 98: Statistics sub-tab

To access the Statistics sub-tab, from GFI EndPointSecurity management console click **Status** tab > **Statistics**.

The **Statistics** section contains information about:

- Protection Status
- Device Usage by Device Type
- Device Usage by Connectivity Port

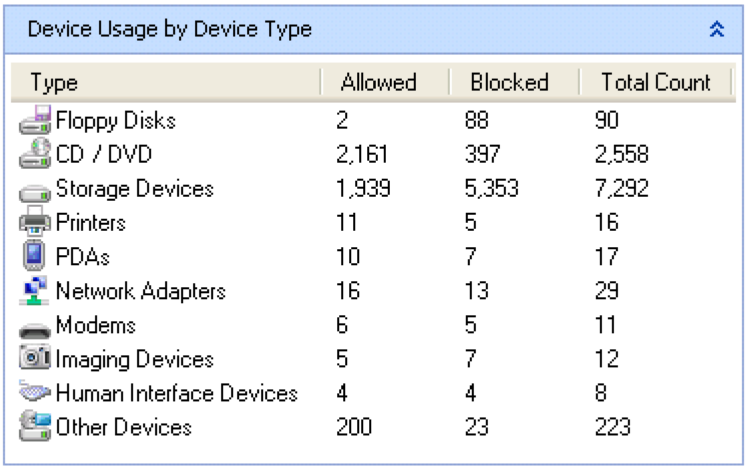
8.2.1 Protection Status



Screenshot 99: Protection Status area

This section graphically represents daily device usage on computers, differentiating between devices that have been blocked and devices that have been allowed by the agents. The information provided can be filtered for a specific computer or for all network computers.

8.2.2 Device Usage by Device Type



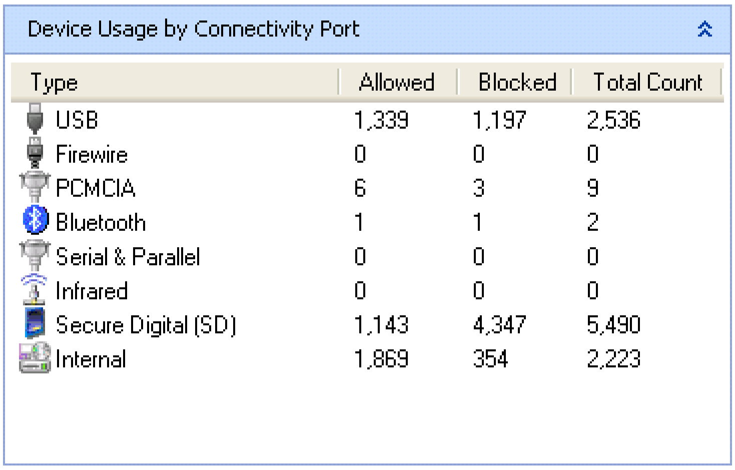
Device Usage by Device Type

Type	Allowed	Blocked	Total Count
Floppy Disks	2	88	90
CD / DVD	2,161	397	2,558
Storage Devices	1,939	5,353	7,292
Printers	11	5	16
PDAs	10	7	17
Network Adapters	16	13	29
Modems	6	5	11
Imaging Devices	5	7	12
Human Interface Devices	4	4	8
Other Devices	200	23	223

Screenshot 100: Device Usage by Device Type area

This section enumerates device connection attempts by device type, that were either allowed or blocked. The information provided can be filtered for a specific computer or for all network computers.

8.2.3 Device Usage by Connectivity Port



Device Usage by Connectivity Port

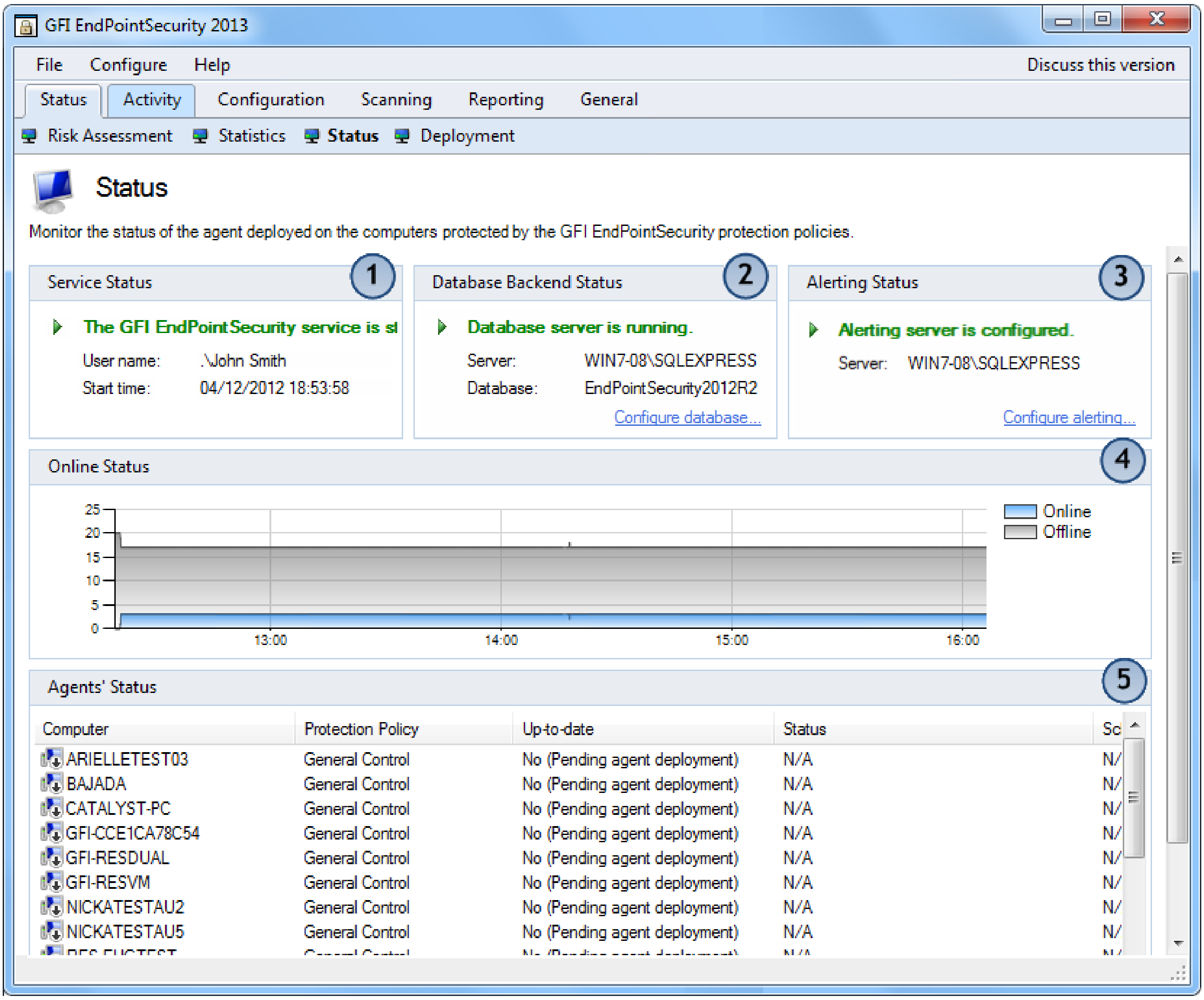
Type	Allowed	Blocked	Total Count
USB	1,339	1,197	2,536
Firewire	0	0	0
PCMCIA	6	3	9
Bluetooth	1	1	2
Serial & Parallel	0	0	0
Infrared	0	0	0
Secure Digital (SD)	1,143	4,347	5,490
Internal	1,869	354	2,223

Screenshot 101: Device Usage by Connectivity Port area

This section enumerates device connection attempts by connectivity port, that were either allowed or blocked. The information provided can be filtered for a specific computer or for all network computers.

8.3 Status view

Use the Status sub-tab to determine the status of all deployment operations performed on your network targets. For each target computer, information displayed shows:


GFI EndPointSecurity 2013
File Configure Help
Discuss this version
Status Activity Configuration Scanning Reporting General
Risk Assessment Statistics Status Deployment
1
2
3
4
5
25
20
15
10
5
0
13:00
14:00
15:00
16:00
Online
Offline

Status

Monitor the status of the agent deployed on the computers protected by the GFI EndPointSecurity protection policies.

Service Status

The GFI EndPointSecurity service is st

User name: .\John Smith

Start time: 04/12/2012 18:53:58

Database Backend Status

Database server is running.

Server: WIN7-08\SQLEXPRESS

Database: EndPointSecurity2012R2

Configure database...

Alerting Status

Alerting server is configured.

Server: WIN7-08\SQLEXPRESS

Configure alerting...

Online Status

Agents' Status

Computer	Protection Policy	Up-to-date	Status	Sc
ARIELLETEST03	General Control	No (Pending agent deployment)	N/A	N/
BAJADA	General Control	No (Pending agent deployment)	N/A	N/
CATALYST-PC	General Control	No (Pending agent deployment)	N/A	N/
GFI-CCE1CA78C54	General Control	No (Pending agent deployment)	N/A	N/
GFI-RESDUAL	General Control	No (Pending agent deployment)	N/A	N/
GFI-RESVM	General Control	No (Pending agent deployment)	N/A	N/
NICKATESTAU2	General Control	No (Pending agent deployment)	N/A	N/
NICKATESTAU5	General Control	No (Pending agent deployment)	N/A	N/

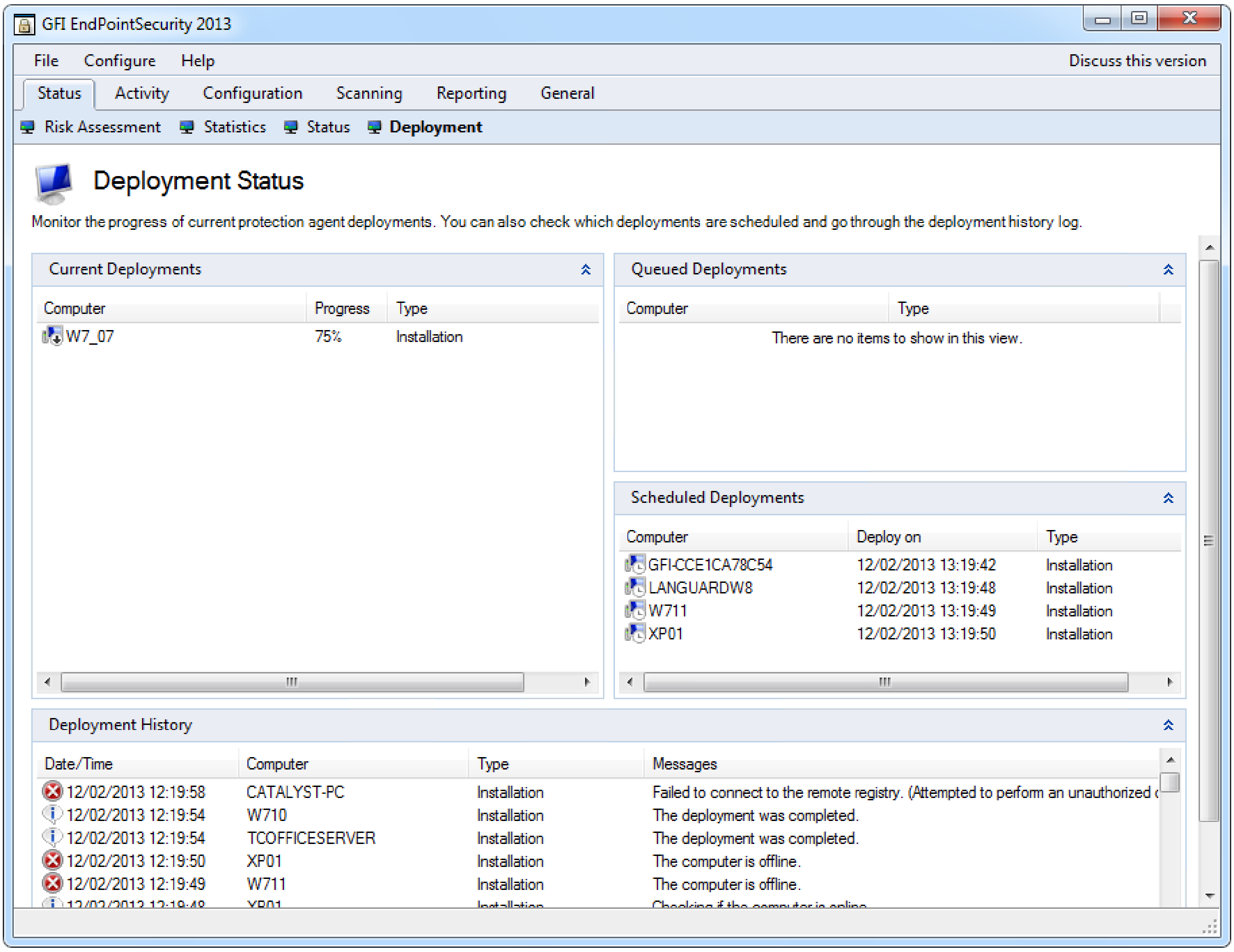
Screenshot 102: Status sub-tab

Feature	Description
1	This section lists: » The operational status of GFI EndPointSecurity management console service. » The user account under which the GFI EndPointSecurity service is running. » The time when the service was last started.
2	This section lists: » The operational status of the database server currently used by GFI EndPointSecurity . » The name or IP address of the database server currently used by GFI EndPointSecurity. » The name of the database where GFI EndPointSecurity is archiving events. To modify any of the current database settings, click **Configure database…**. This launches the **Database Backend** dialog. For more information, refer to Managing the Database Backend (page 131).
3	This section lists: » The operational status of the alerting server currently used by GFI EndPointSecurity. » The name or IP address of the alerting server currently used by GFI EndPointSecurity. To modify any of the current alerts related settings, click **Configure alerting …**. This launches the **Alerting Options** dialog. For more information, refer to Configuring alerts (page 85).

Feature	Description
4	This section graphically represents all agents deployed on network computers, differentiating between those currently online and offline.
5	This selection lists: » Target computer name and applicable protection policy. » The status of the GFI EndPointSecurity Agent, whether currently deployed and up-to-date, or awaiting deployment. » The status of the target computer, whether currently online, or offline. To deploy pending agents: 1. Select one or more computers from **Agents' Status**. 2. Right-click the selected computers and select **Deploy selected agent(s)** or **Schedule deployment for selected agent(s)…**. 3. Click **OK**. **Note** If a target computer is offline, deployment is differed by an hour. GFI EndPointSecurity tries to deploy that policy every hour, until the target computer is back online. **Note** Each agent sends its online status to GFI EndPointSecurity at regular intervals. If this data is not received by the main application, the agent is considered to be offline.

8.4 Deployment status view

8.4.1 About Deployment status view



Deployment Status

Monitor the progress of current protection agent deployments. You can also check which deployments are scheduled and go through the deployment history log.

Current Deployments

Computer	Progress	Type
W7_07	75%	Installation

Queued Deployments

Computer	Type

There are no items to show in this view.

Scheduled Deployments

Computer	Deploy on	Type
GFI-CCE1CA78C54	12/02/2013 13:19:42	Installation
LANGUARDW8	12/02/2013 13:19:48	Installation
W711	12/02/2013 13:19:49	Installation
XP01	12/02/2013 13:19:50	Installation

Deployment History

Date/Time	Computer	Type	Messages
12/02/2013 12:19:58	CATALYST-PC	Installation	Failed to connect to the remote registry. (Attempted to perform an unauthorized
12/02/2013 12:19:54	W710	Installation	The deployment was completed.
12/02/2013 12:19:54	TCOFFICESERVER	Installation	The deployment was completed.
12/02/2013 12:19:50	XP01	Installation	The computer is offline.
12/02/2013 12:19:49	W711	Installation	The computer is offline.
12/02/2013 12:19:48	XP01	Installation	Checking if the computer is online

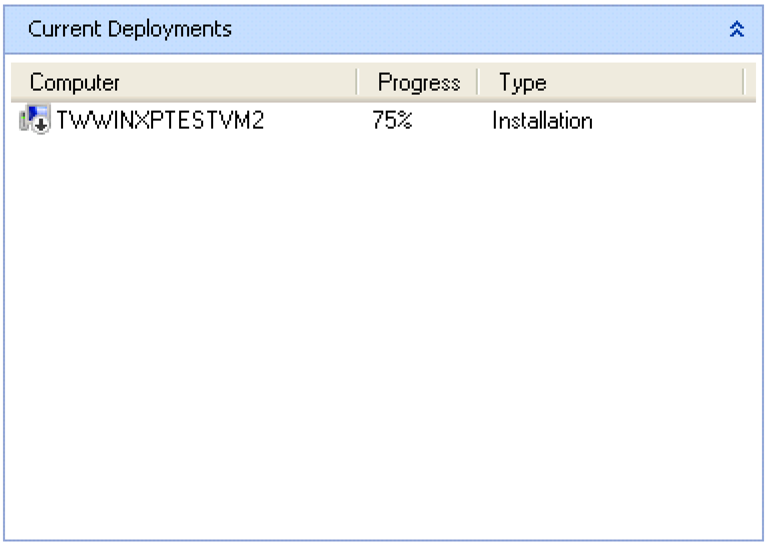
Screenshot 103: Deployment sub-tab

Use the Deployment sub-tab to view:

- Current deployment activity
- Queued deployments
- Scheduled deployments
- Deployment history.

To access the Deployment sub-tab, from GFI EndPointSecurity management console, click **Status** tab > **Deployment**.

8.4.2 Current Deployments



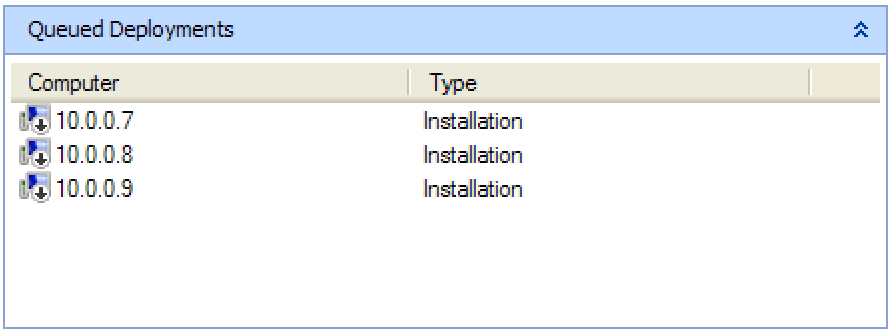
Current Deployments

Computer	Progress	Type
TWWINXPTESTVM2	75%	Installation

Screenshot 104: Current Deployments area

This section displays a list of deployments currently taking place. The information provided includes the computer name, deployment progress and deployment type. The deployment is an installation, un-installation or update.

8.4.3 Queued Deployments



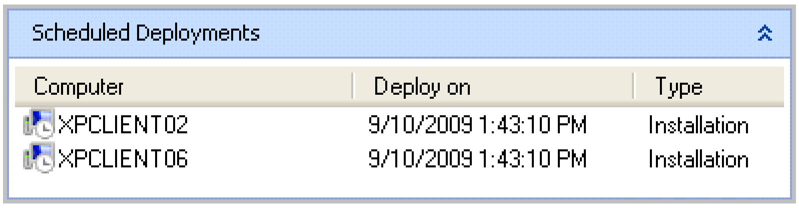
Queued Deployments

Computer	Type
10.0.0.7	Installation
10.0.0.8	Installation
10.0.0.9	Installation

Screenshot 105: Queued Deployments area

This section displays a list of pending deployments. The information provided includes the computer name and deployment type.

8.4.4 Scheduled Deployments



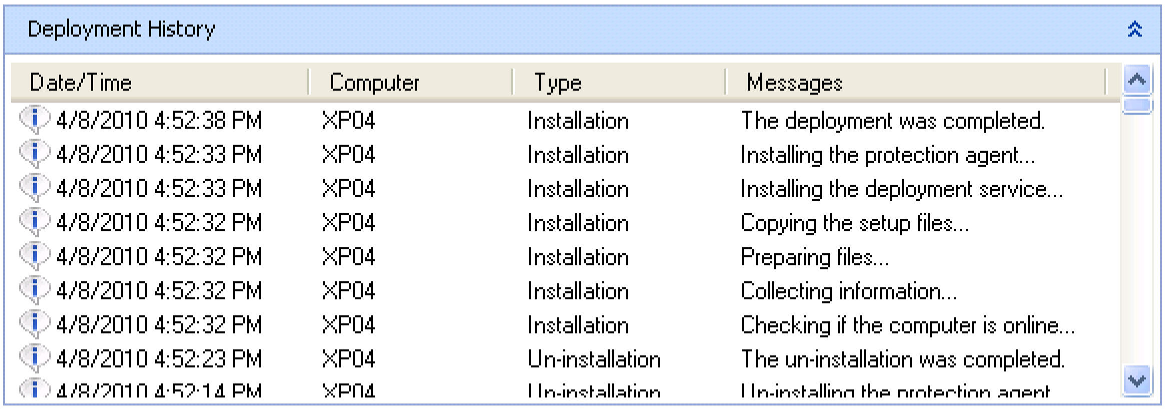
Scheduled Deployments

Computer	Deploy on	Type
XPCLIENT02	9/10/2009 1:43:10 PM	Installation
XPCLIENT06	9/10/2009 1:43:10 PM	Installation

Screenshot 106: Scheduled Deployments area

This section displays a list of scheduled deployments. The information provided includes the computer name, scheduled time and deployment type.

8.4.5 Deployment History



Date/Time	Computer	Type	Messages
4/8/2010 4:52:38 PM	XP04	Installation	The deployment was completed.
4/8/2010 4:52:33 PM	XP04	Installation	Installing the protection agent...
4/8/2010 4:52:33 PM	XP04	Installation	Installing the deployment service...
4/8/2010 4:52:32 PM	XP04	Installation	Copying the setup files...
4/8/2010 4:52:32 PM	XP04	Installation	Preparing files...
4/8/2010 4:52:32 PM	XP04	Installation	Collecting information...
4/8/2010 4:52:32 PM	XP04	Installation	Checking if the computer is online...
4/8/2010 4:52:23 PM	XP04	Un-installation	The un-installation was completed.
4/8/2010 4:52:14 PM	XP04	Un-installation	Un-installing the protection agent

Screenshot 107: Deployment History area

This section displays an audit trail for all stages of all agent or protection policy deployments carried out by GFI EndPointSecurity. The information provided includes the timestamp of each log entry, the computer name, deployment type and errors and information messages generated during the deployment process. For more information, refer to Troubleshooting and Support (page 139).

To remove displayed log entries, right-click in the **Deployment History** area and select **Clear all messages**.

9 Reporting

The GFI EndPointSecurity Report Pack is a fully-fledged reporting add-on to GFI EndPointSecurity. This reporting package can be scheduled to automatically generate graphical IT-level and management reports based on data collected by GFI EndPointSecurity, giving you the ability to report on devices connected to the network, device usage trends by machine or by user, files copied to and from devices (including actual names of files copied) and much more.

Topics in this chapter

9.1 GFI EndPointSecurity Report Pack

To generate reports, you need to download and install the GFI EndPointSecurity Report Pack add-on. To download the add-on visit: http://go.gfi.com/?pageid=esec_reportpack.

For more information about GFI EndPointSecurity Report Pack:

1. Click **Reporting** tab.

2. From the left pane, select either **GFI EndPointSecurity Report Pack** or **GFI ReportCenter**.

> **Note**
>
> An Internet connection is required.

9.2 Generating Digest reports

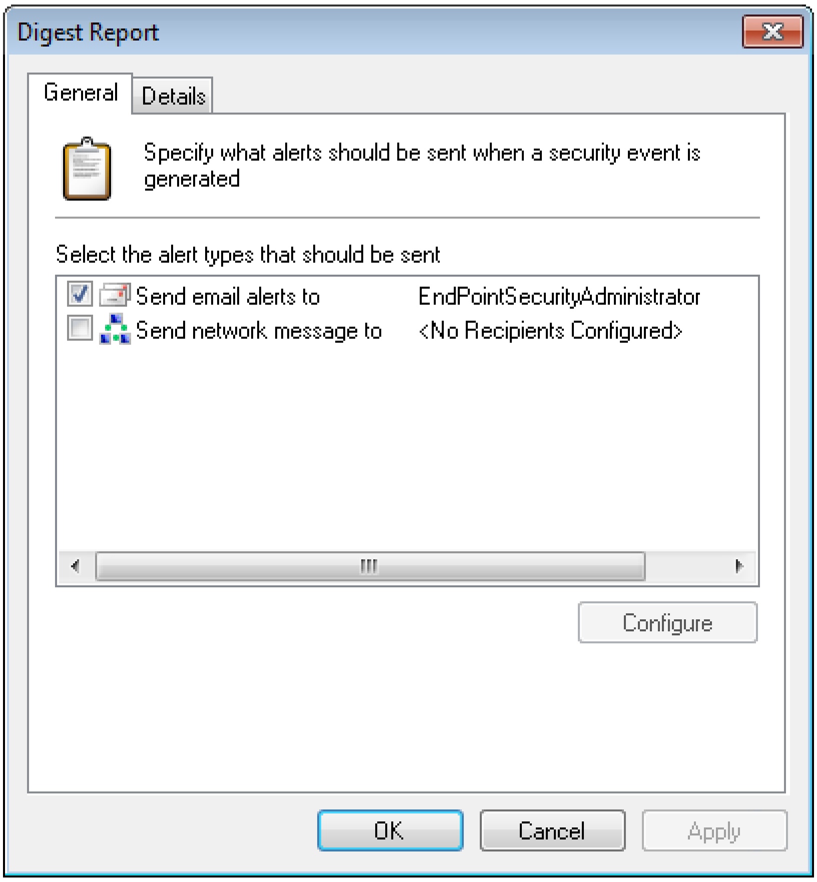
GFI EndPointSecurity enables you to generate Digest reports to the configured recipients. Digest reports contain a summary of periodical activity statistics as detected by GFI EndPointSecurity.

Alert recipients are not Active Directory (AD) users and/or user groups, but are profile accounts created by GFI EndPointSecurity to hold the contact details of users intended to alerts. It is best to create alert recipients prior to configuring alerts. For more information, refer to Configuring alerts recipients (page 128).

To configure Digest reports:

1. Click **Configuration** tab **>** **Options** sub-tab.

2. From **Configure**, click **Alerting Options** and from the right pane, click **Configure the digest report**.



Specify what alerts should be sent when a security event is generated

Select the alert types that should be sent

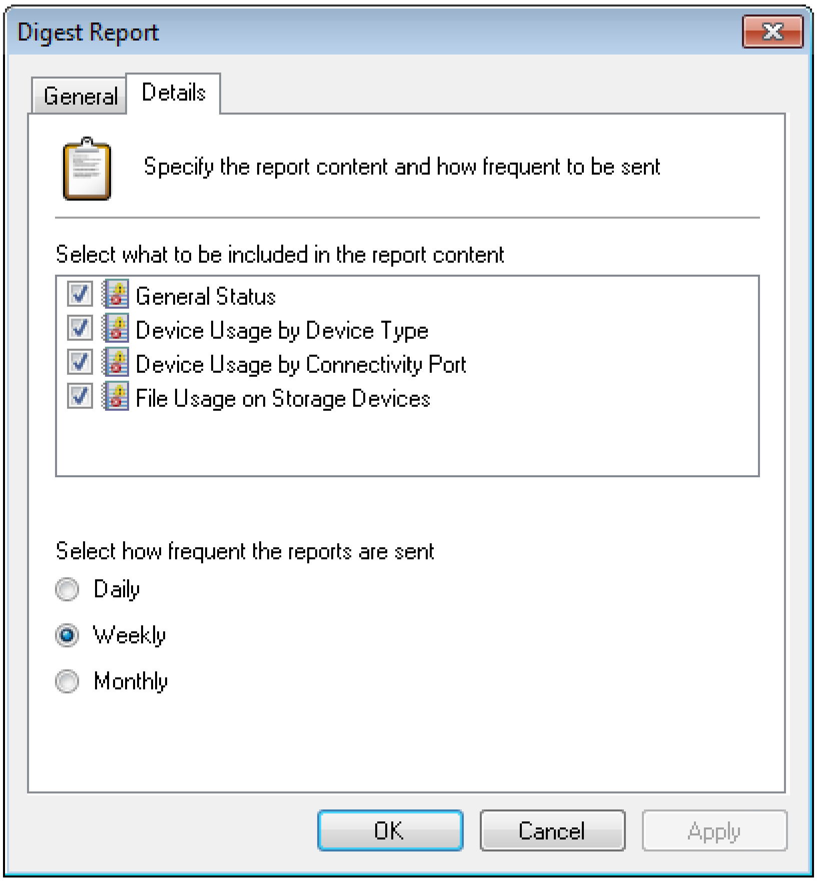
☑ Send email alerts to EndPointSecurityAdministrator

□ Send network message to <No Recipients Configured>

Screenshot 108: Digest Report options - General tab

3. From the **Genera**l tab of the **Digest Report** dialog, select/unselect the preferred alerting method.

4. For each alert type selected, click **Configure** to specify the user(s)/group(s) to whom the alert is sent.



Specify the report content and how frequent to be sent

Select what to be included in the report content

- ☑ General Status
- ☑ Device Usage by Device Type
- ☑ Device Usage by Connectivity Port
- ☑ File Usage on Storage Devices

Select how frequent the reports are sent

- ○ Daily
- ● Weekly
- ○ Monthly

Screenshot 109: Digest Report options - Details tab

5. Click **Details** tab to select/unselect report content items to include in the digest report.

6. Select the sending frequency of the report, from **Daily**, **Weekly** or **Monthly**.

7. Click **Apply** and **OK**

10 Configuring GFI EndPointSecurity

GFI EndPointSecurity enables you to configure the computers you intend to install updates and display user messages on.

Topics in this chapter

10.1 Configuring Agent options

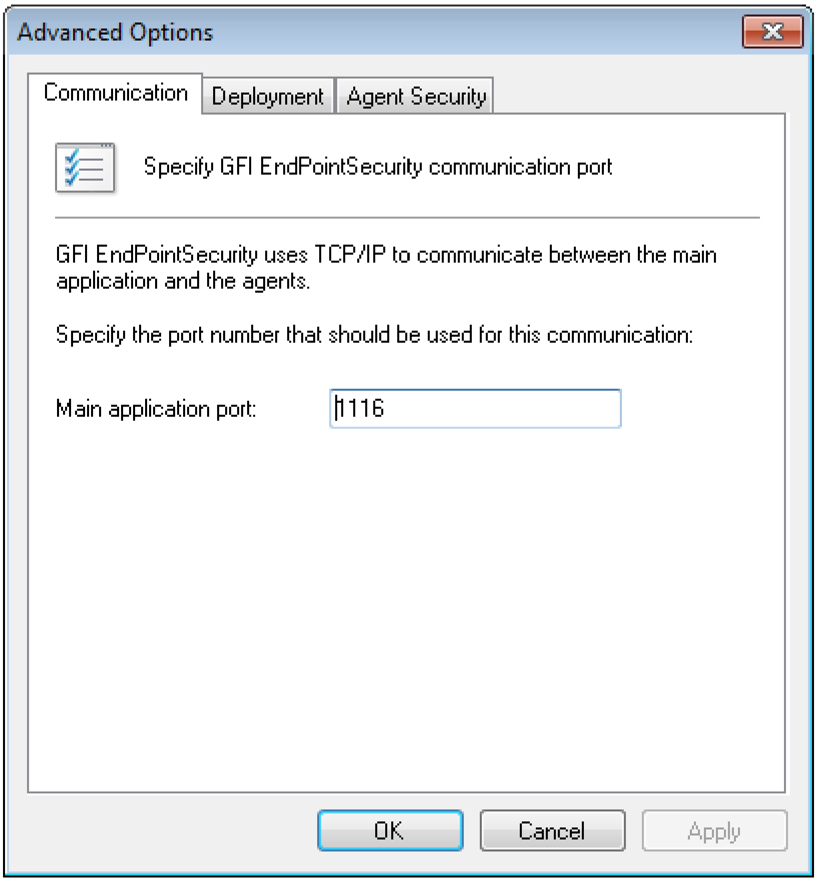
This topic provides information on how to configure GFI EndPointSecurity Agent advanced options:

- Main communication TCP/IP port
- Deployment options
- Agents control password.

To configure advance options:

1. Click **Configuration** tab **>** **Options** sub-tab.

2. From **Configure**, right-click **Advanced Options** node and select **Modify advanced options...**.



Specify GFI EndPointSecurity communication port

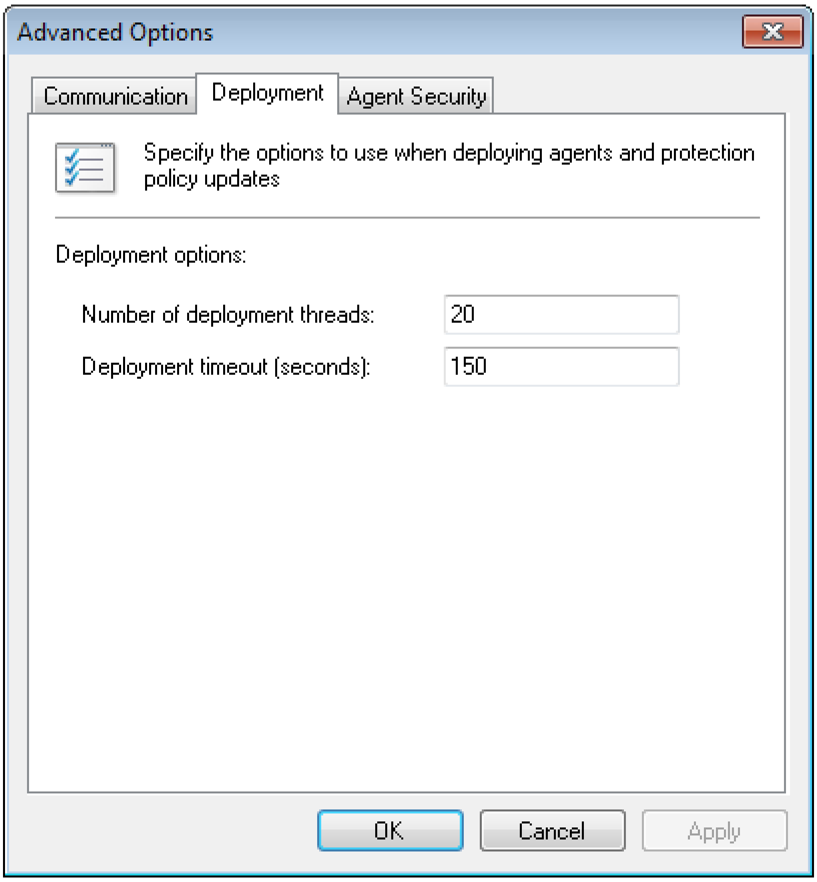
GFI EndPointSecurity uses TCP/IP to communicate between the main application and the agents.

Specify the port number that should be used for this communication:

Main application port: 1116

Screenshot 110: Advanced Options - Communication tab

3. From the **Communication** tab, key in the required TCP/IP port number to be used for communication between GFI EndPointSecurity and GFI EndPointSecurity Agents. By default, port **1116** is specified.



Specify the options to use when deploying agents and protection policy updates

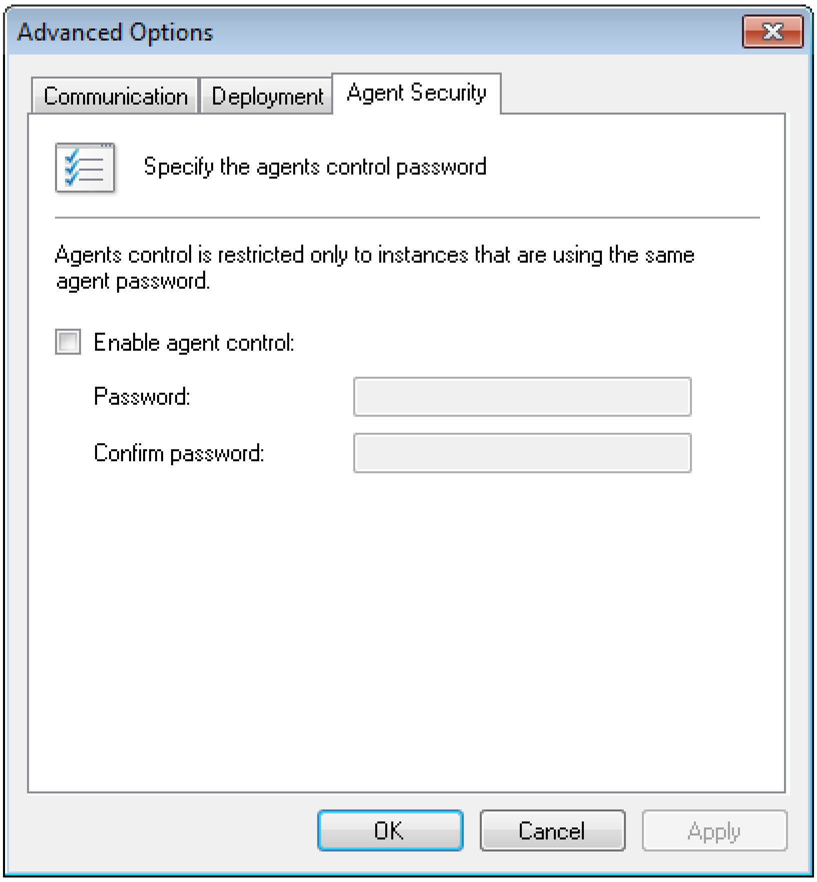
Deployment options:

Number of deployment threads: 20

Deployment timeout (seconds): 150

Screenshot 111: Advanced Options - Deployment tab

4. Click **Deployment** tab and key in the required **Number of deployment threads** and **Deployment timeout (seconds)** values.



Specify the agents control password

Agents control is restricted only to instances that are using the same agent password.

□ Enable agent control:

Password:

Confirm password:

Screenshot 112: Advanced Options - Agent Security tab

5. Click **Agent Security** tab and select/unselect **Enable agent control**. Use this option to assign particular logon credentials to all GFI EndPointSecurity Agents deployed on your network.

6. Click **Apply** and **OK**.

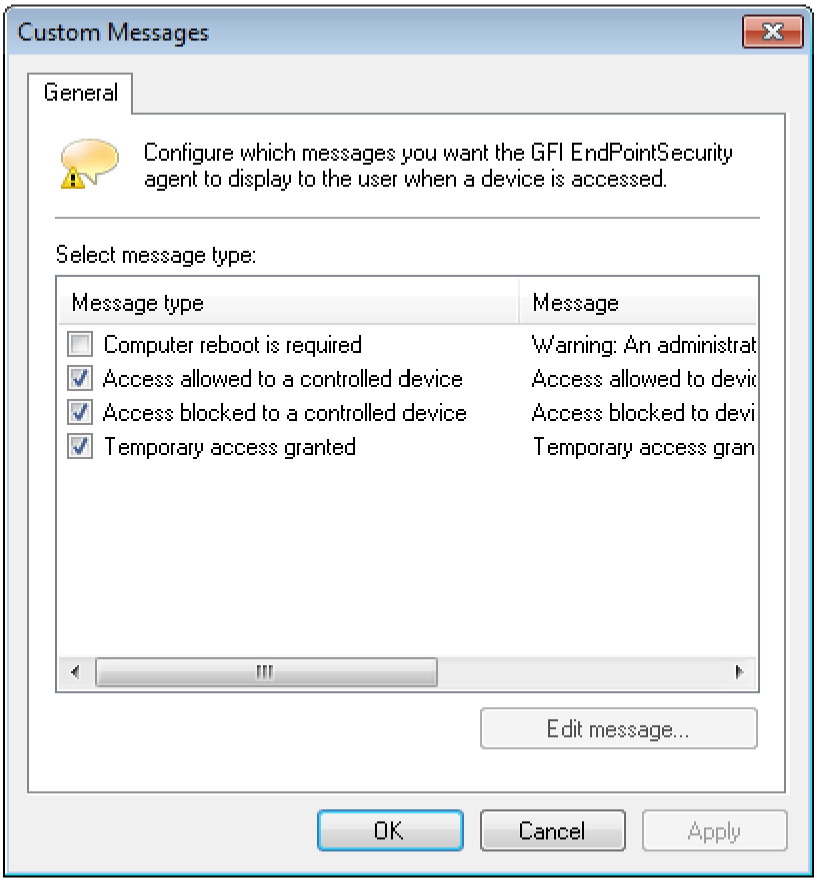
10.2 Configuring user messages

GFI EndPointSecurity enables you to customize messages displayed by GFI EndPointSecurity Agents on target computers when devices are accessed.

To customize user messages:

1. Click **Configuration** tab **>** **Options** sub-tab.

2. From **Configure**, right-click **Custom Messages** and select **Customize user messages**.



Configure which messages you want the GFI EndPointSecurity agent to display to the user when a device is accessed.

Select message type:

Message type	Message
□ Computer reboot is required	Warning: An administrat
☑ Access allowed to a controlled device	Access allowed to devic
☑ Access blocked to a controlled device	Access blocked to devi
☑ Temporary access granted	Temporary access gran

Screenshot 113: Custom Messages dialog options

3. Select/unselect the message types you want to customize.

4. For each message type selected, click **Edit message…**, modify the text as required, and click **Save**. Repeat this step for each message you want to modify.

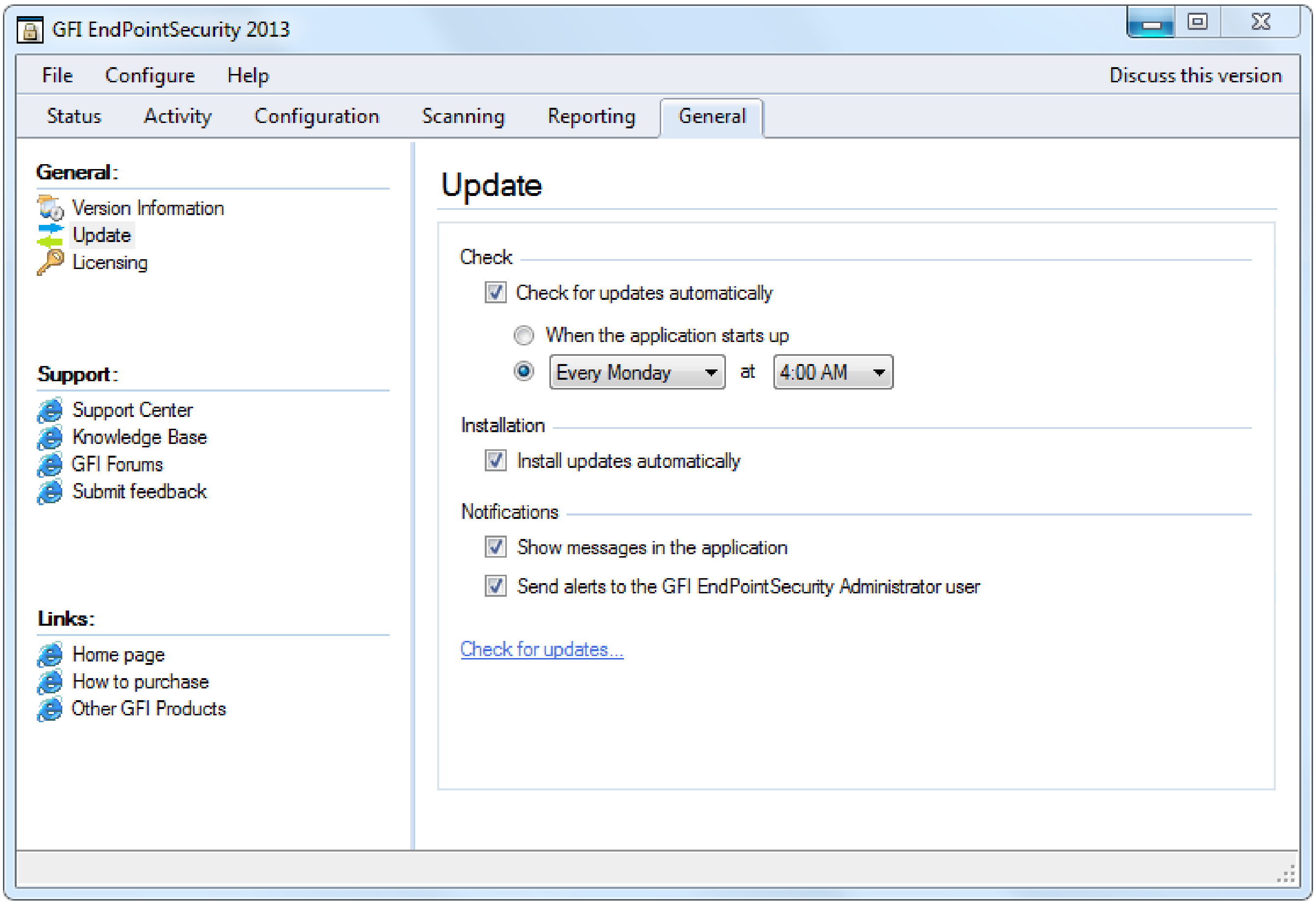
5. Click **Apply** and **OK**.

10.3 Configuring product updates

GFI EndPointSecurity can be configured to download and install updates automatically on a schedule or on startup. To configure updates:

1. Click **General** tab.

2. From the left pane, click **Updates**.



Update

Check

☑ Check for updates automatically

○ When the application starts up

● Every Monday at 4:00 AM

Installation

☑ Install updates automatically

Notifications

☑ Show messages in the application

☑ Send alerts to the GFI EndPointSecurity Administrator user

Check for updates...

Screenshot 114: General tab - Updates

3. From the right pane, configure the options described below:

Option	Description
Check for updates automatically	Connect to the GFI update servers and download product updates automatically. Select When the application starts up, or specify a day and time when to check and download updates.
Install updates automatically	If an update is found, GFI EndPointSecurity will download and install the update automatically.
Show messages in the application	If an update is found and installed, a message is displayed in GFI EndPointSecurity application.
Send alerts to the GFI EndPointSecurity Administrator user	Once an update is downloaded and installed, an email message is sent to the GFI EndPointSecurity Administrator. For more information, refer to Configuring the alerts administrator account (page 124).
Check for updates	Click the link to instantly run the GFI EndPointSecurity updates engine, download and install any missing updates.

11 Alerting Options

This topic provides you with information about configuring the GFI EndPointSecurity alerting options and alerts recipients. Alerting is a crucial part of GFI EndPointSecurity's operation which help you take remedial actions as soon as a threat is detected.

11.1 Configuring alerting options

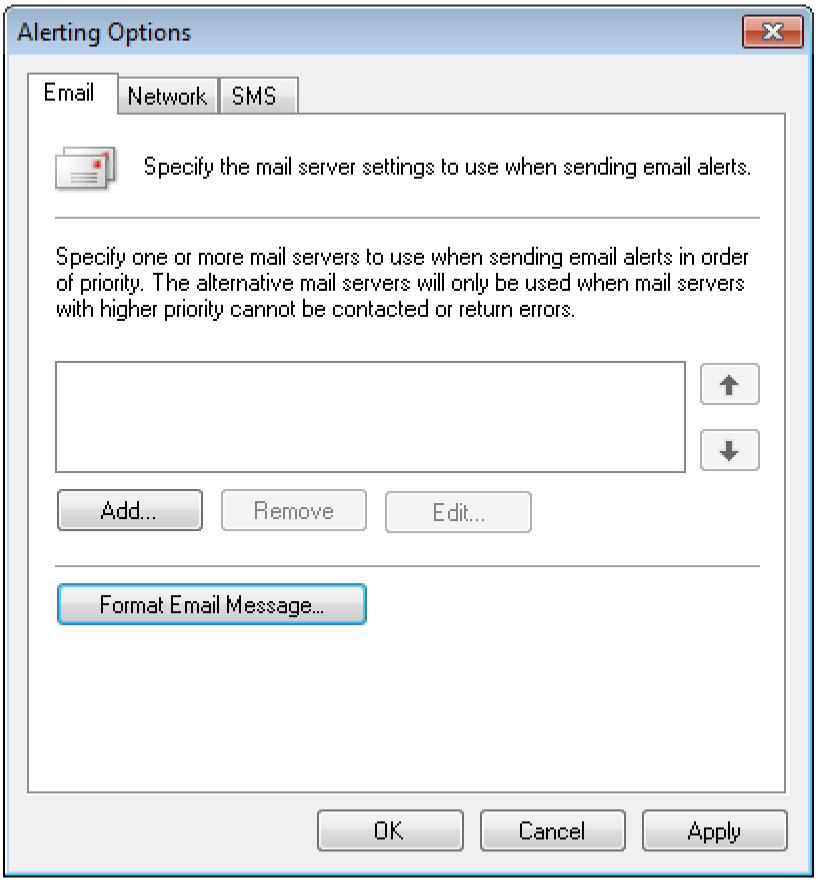
GFI EndPointSecurity allows you configure the following alerting options:

- The mail server settings, sender details and email message that are used when email alerts
- The network message to use when sending network alerts
- The SMS gateway and SMS message that is used when sending SMS alerts.

To configure alerting options:

1. Click **Configuration** tab **>** **Options** sub-tab.

2. From **Configure**, right-click **Alerting Options** node and select **Edit alerting options...**.



Alerting Options

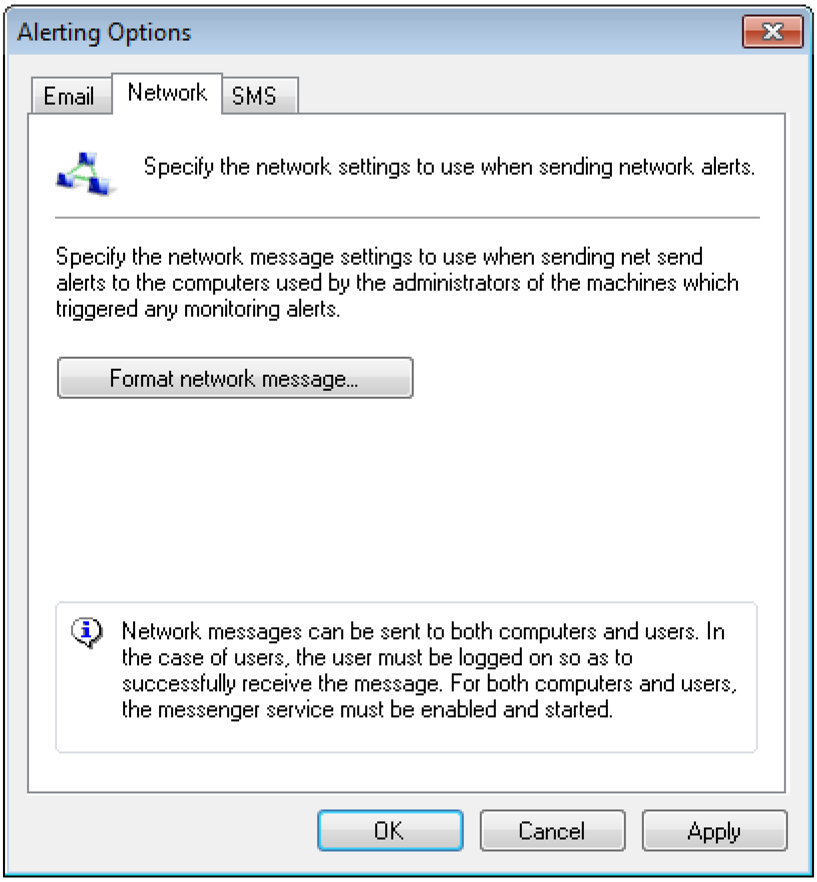
Specify the mail server settings to use when sending email alerts.

Specify one or more mail servers to use when sending email alerts in order of priority. The alternative mail servers will only be used when mail servers with higher priority cannot be contacted or return errors.

Screenshot 115: Alerting Options - Email tab

3. From **Email** tab , click **Add...**, to specify your mail server settings. Click **OK** to close the **Mailserver properties** dialog.

4. To edit the email message, click **Format Email Message…**, modify the **Subject** and **Message** fields as required, and click **Save**.



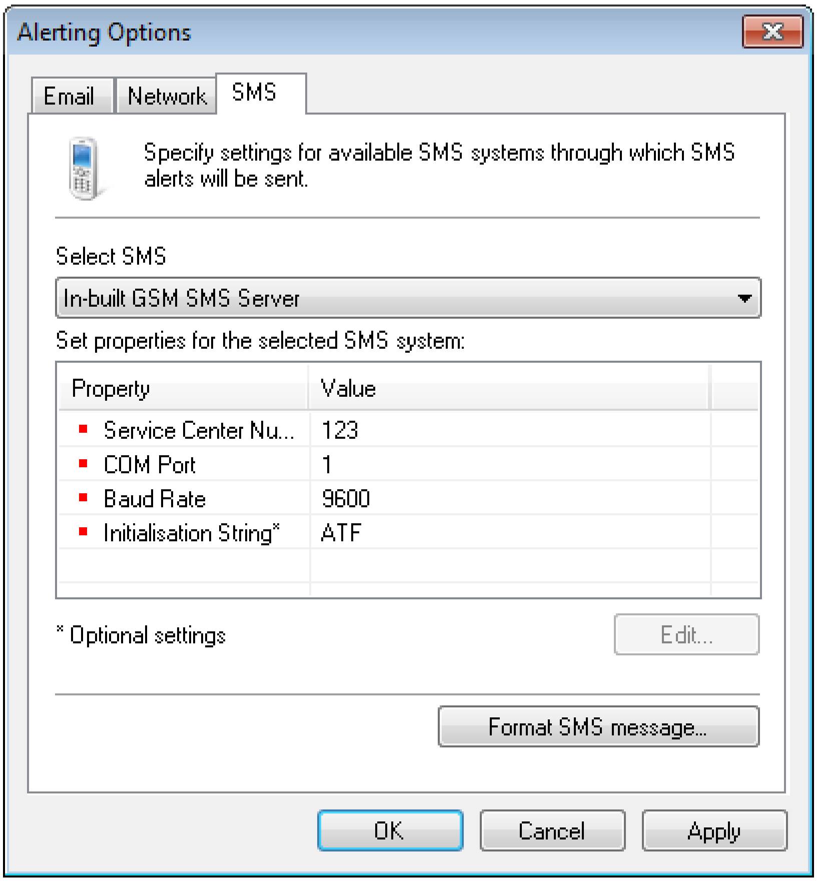
Specify the network settings to use when sending network alerts.

Specify the network message settings to use when sending net send alerts to the computers used by the administrators of the machines which triggered any monitoring alerts.

Network messages can be sent to both computers and users. In the case of users, the user must be logged on so as to successfully receive the message. For both computers and users, the messenger service must be enabled and started.

Screenshot 116: Alerting Options - Network tab

5. Click **Network** tab **> Format network message…**, to edit the network message. Click **Save**.



Specify settings for available SMS systems through which SMS alerts will be sent.

Select SMS

In-built GSM SMS Server

Set properties for the selected SMS system:

Property	Value
Service Center Nu...	123
COM Port	1
Baud Rate	9600
Initialisation String*	ATF

* Optional settings

Edit...

Format SMS message...

Screenshot 117: Alerting Options - SMS tab

6. Click **SMS** tab and from the **Select SMS** drop-down menu, select the SMS gateway you want to use. Supported SMS systems include:

- In-built GSM SMS Server
- GFI FaxMaker SMS gateway
- Clickatell Email to SMS service gateway
- Generic SMS provides gateway.

7. From the **Set properties for the selected SMS system** area, highlight the property you want to configure and click **Edit**. Repeat this step for each SMS system property you want to modify.

8. Click **Format SMS message…**, to modify the Subject and Message as required. Click **Save**.

9. Click **OK**

11.2 Configuring the alerts administrator account

GFI EndPointSecurity enables you to configure profile accounts to hold contact details of users intended to receive e-mail alerts, network messages and SMS messages. Upon installation, GFI EndPointSecurity automatically creates an alerts administrator account. Alert administrators are not Active Directory (AD) users and/or user groups.

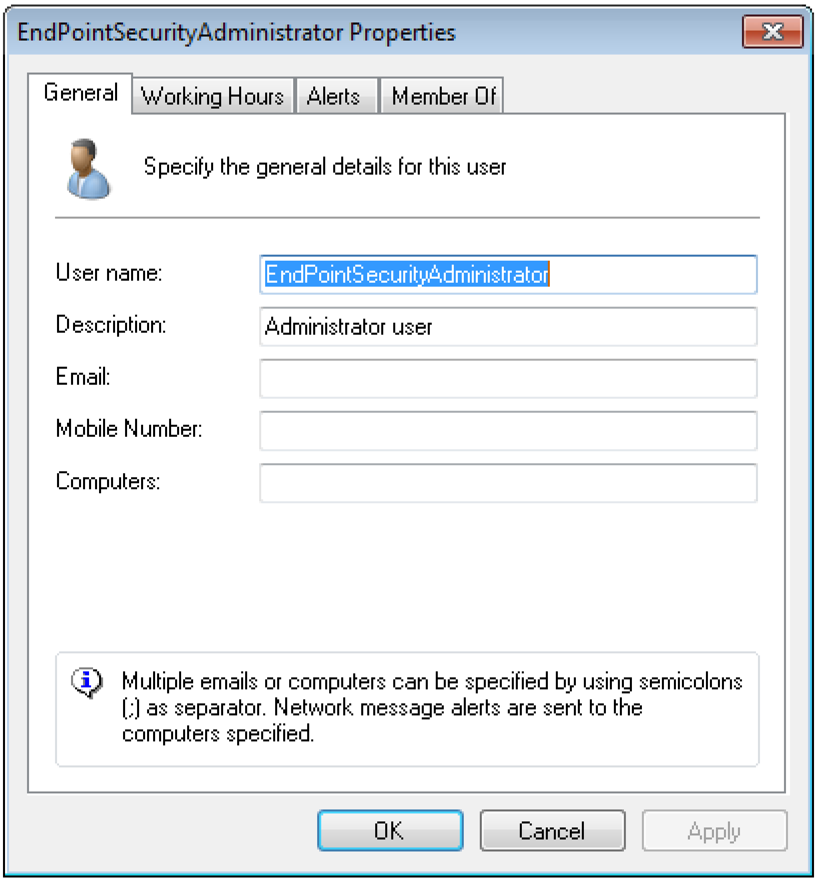
By default GFI EndPointSecurity automatically creates the EndPointSecurityAdministrator account (for alerts purposes) upon installation and sets it as a member of the EndPointSecurityAdministrators notification group.

To configure the GFI EndPointSecurityAdministrator account:

1. Click **Configuration** tab > **Options** sub-tab.

2. From **Configure**, click **Alerting Options > Users** sub-node.

3. From the right pane, right-click **EndPointSecurityAdministrator** and select **Properties**.



Specify the general details for this user

User name: EndPointSecurityAdministrator

Description: Administrator user

Email:

Mobile Number:

Computers:

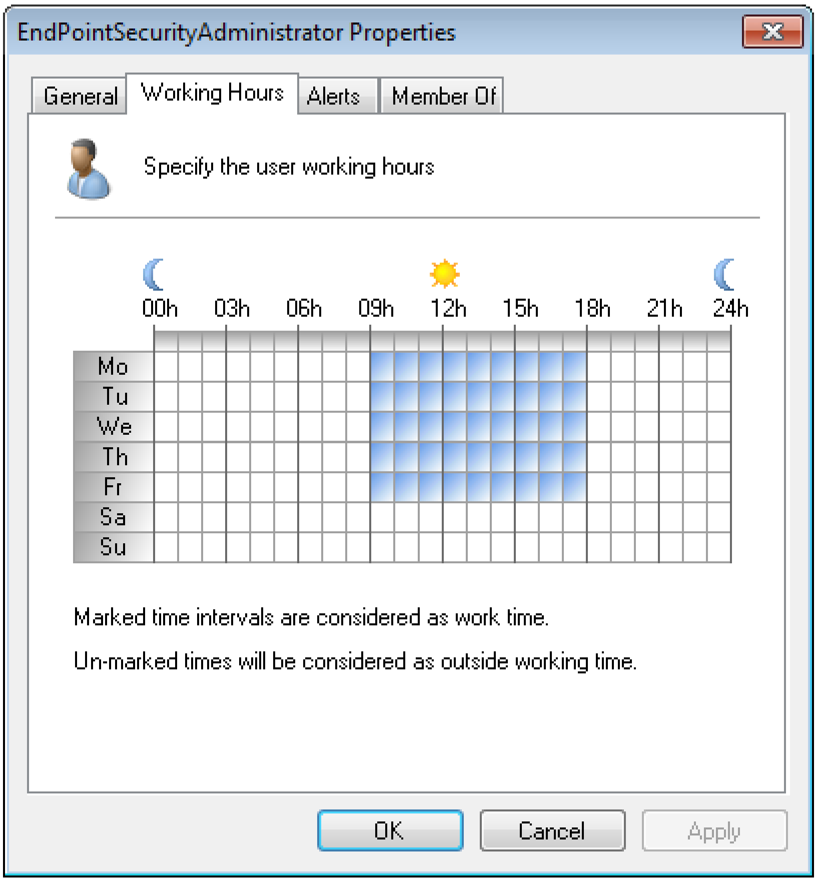
Multiple emails or computers can be specified by using semicolons (;) as separator. Network message alerts are sent to the computers specified.

Screenshot 118: EndPointSecurityAdministrator Properties options - General tab

4. From the General tab, key in the following details:

- Account user name
- Account Description
- Email address
- Mobile number
- Computers (network messages are sent to the specified computers)

> **Note**
>
> More than one email address and more than one computer name/IP address can be specified. Separate entries with semicolons ';'.



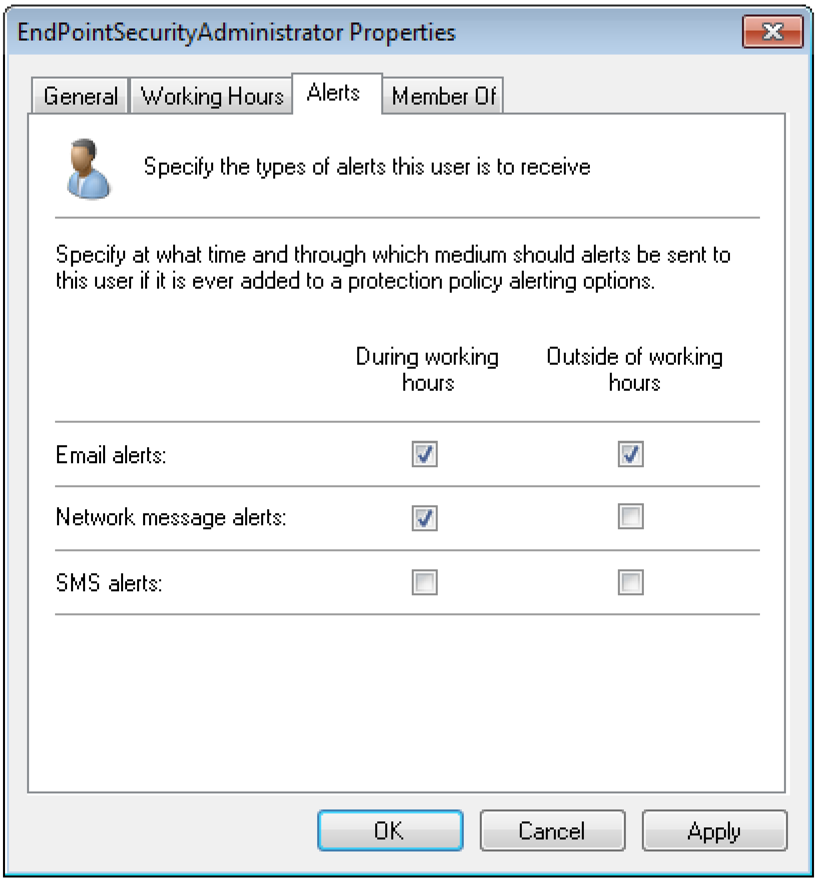
Specify the user working hours

Marked time intervals are considered as work time.

Un-marked times will be considered as outside working time.

Screenshot 119: EndPointSecurityAdministrator Properties options - Working Hours tab

5. Click **Working Hours** tab and mark the typical working hours of the user. Marked time intervals are considered as working hours.



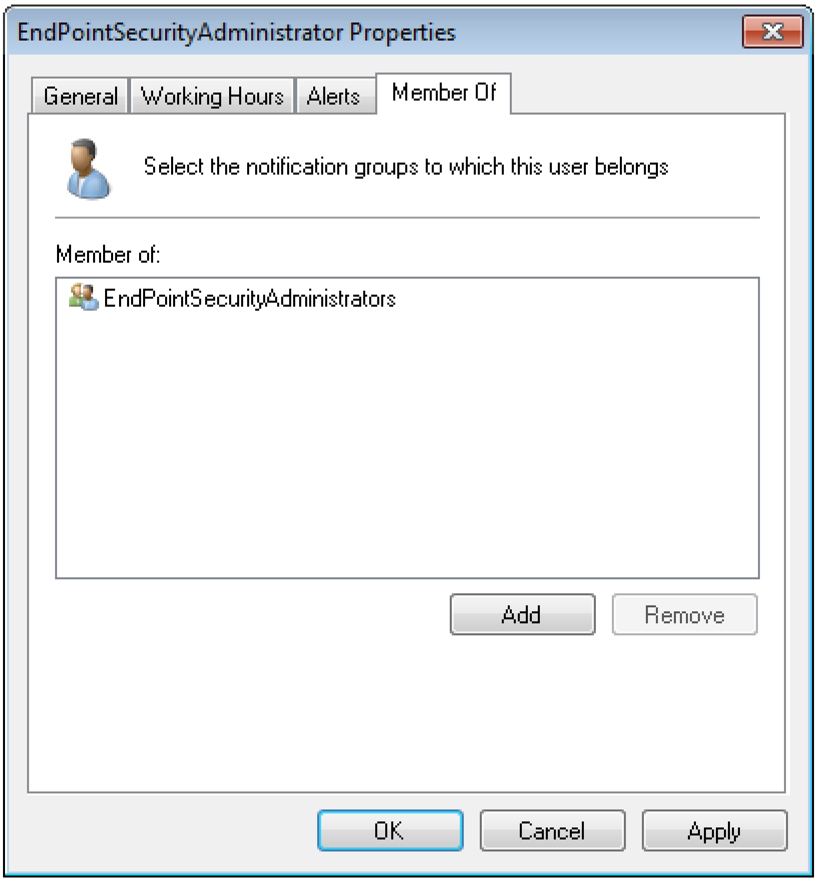
Specify the types of alerts this user is to receive

Specify at what time and through which medium should alerts be sent to this user if it is ever added to a protection policy alerting options.

	During working hours	Outside of working hours
Email alerts:	☑	☑
Network message alerts:	☑	□
SMS alerts:	□	□

Screenshot 120: EndPointSecurityAdministrator Properties options - Alerts tab

6. Click **Alerts** tab and select the alerts to be sent and at what time alerts are sent.


EndPointSecurityAdministrator Properties
General
Working Hours
Alerts
Member Of
Select the notification groups to which this user belongs
Member of:
EndPointSecurityAdministrators
Add
Remove
OK
Cancel
Apply

Screenshot 121: EndPointSecurityAdministrator Properties options - Member Of tab

7. Click **Member Of** tab and click **Add** to add the user to notification group(s).

8. Click **Apply** and **OK**

11.3 Configuring alerts recipients

GFI EndPointSecurity enables you to configure other profile accounts (apart from the default GFI EndPointSecurity Administrator account) to hold the contact details of users intended to receive e-mail alerts, network messages and SMS messages.

Alert recipients are not Active Directory (AD) users and/or user groups, but are profile accounts created by GFI EndPointSecurity to hold the contact details of users intended to alerts.

- Creating alert recipients
- Editing alert recipients properties
- Deleting alert recipients

11.3.1 Creating alert recipients

To create a new alert recipient:

1. Click **Configuration** tab **> Options** sub-tab.

2. From **Configure**, click **Alerting Options > Users** sub-node.

3. From the left pane, click the **Create user…**.

4. For more information about configuring the settings to create a new recipient, refer to Configuring the alerts administrator account.

11.3.2 Editing alert recipient properties

To edit alert recipient's properties:

1. Click **Configuration** tab **>** **Options** sub-tab.

2. From **Configure**, click **Alerting Options > Users** sub-node.

3. From the right pane, right-click the user you want to edit and select **Properties**.

4. For more information about configuring the settings to edit a recipient, refer to Configuring the alerts administrator account.

11.3.3 Deleting alert recipients

To delete an alert recipient:

1. Click **Configuration** tab **>** **Options** sub-tab.

2. From **Configure**, click **Alerting Options > Users** sub-node.

3. From the right pane, right-click the user you want to edit and select **Delete**.

4. Click **Yes** to confirm deletion.

11.4 Configuring groups of alert recipients

GFI EndPointSecurity enables you to organize your alert recipients into groups in order to facilitate the management of alert recipients.

- Creating groups of alert recipients
- Editing group of alert recipients properties
- Deleting groups of alert recipients

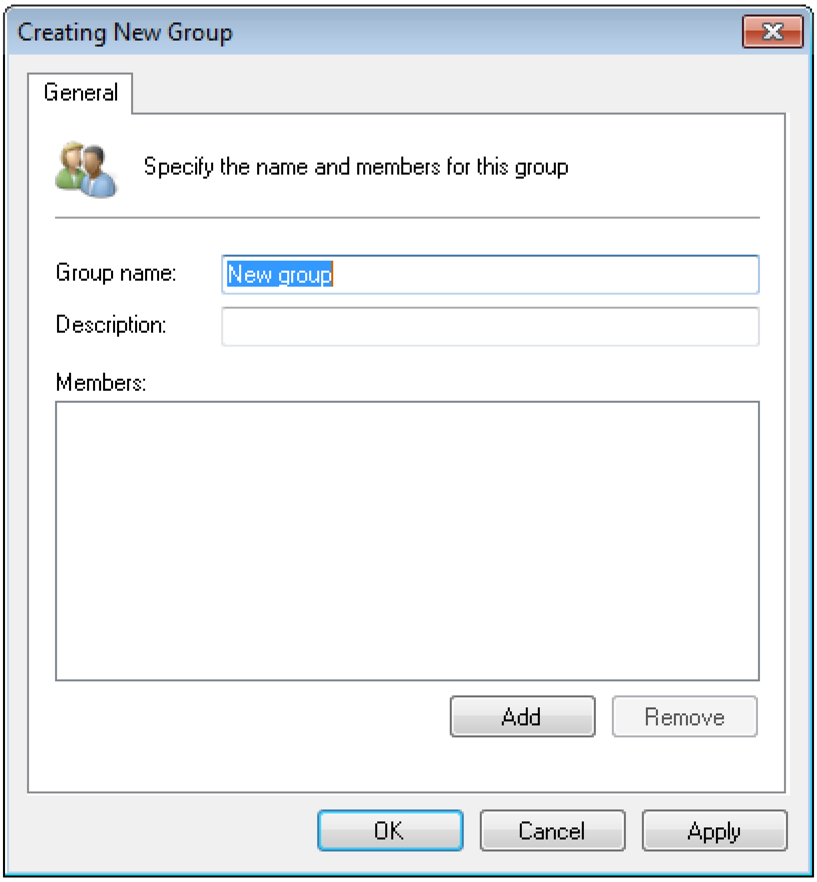
11.4.1 Creating groups of alert recipients

To create a new group of alert recipients:

1. Click **Configuration** tab **>** **Options** sub-tab.

2. Click **Alerting Options > Groups** sub-node.

3. From the left pane, click **Create group…**.



Group name: New group

Screenshot 122: Creating New Group options

4. From the **Creating New Group** dialog key in the group name and an optional description.

5. Click **Add** to select the user(s) that belong to this notification group, and click **OK**

11.4.2 Editing group of alert recipients properties

To edit group of alert recipient's properties:

1. Click **Configuration** tab **>** **Options** sub-tab.

2. Click **Alerting Options** > **Groups** sub-node.

3. From the right pane, right-click the group you want to edit and select **Properties**.

4. For more information on how to edit the settings of groups, refer to Creating groups of alert recipients.

11.4.3 Deleting groups of alert recipients

To delete a group of alert recipients:

1. Click **Configuration** tab **>** **Options** sub-tab.

2. Click **Alerting Options** > **Groups** sub-node.

3. From the right pane, right-click the group you want to delete and select **Delete**.

4. Click **Yes** to confirm deletion of the group.

12 Managing the Database Backend

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.

This section provides you with information related to managing and maintaining the database where data gathered by GFI EndPointSecurity is stored. After installing GFI EndPointSecurity you can choose to:

» Download and install an instance of Microsoft SQL Server Express Edition and to automatically create a database for GFI EndPointSecurity. This can be done through the **Quick Start wizard**.

» Connect to an available Microsoft SQL Server instance and connect to an existing database or else create a new one. This can be done through the **Quick Start wizard**, the **General Status** or the **Options** sub-tabs.

Topics in this chapter

12.1 Maintaining the database backend

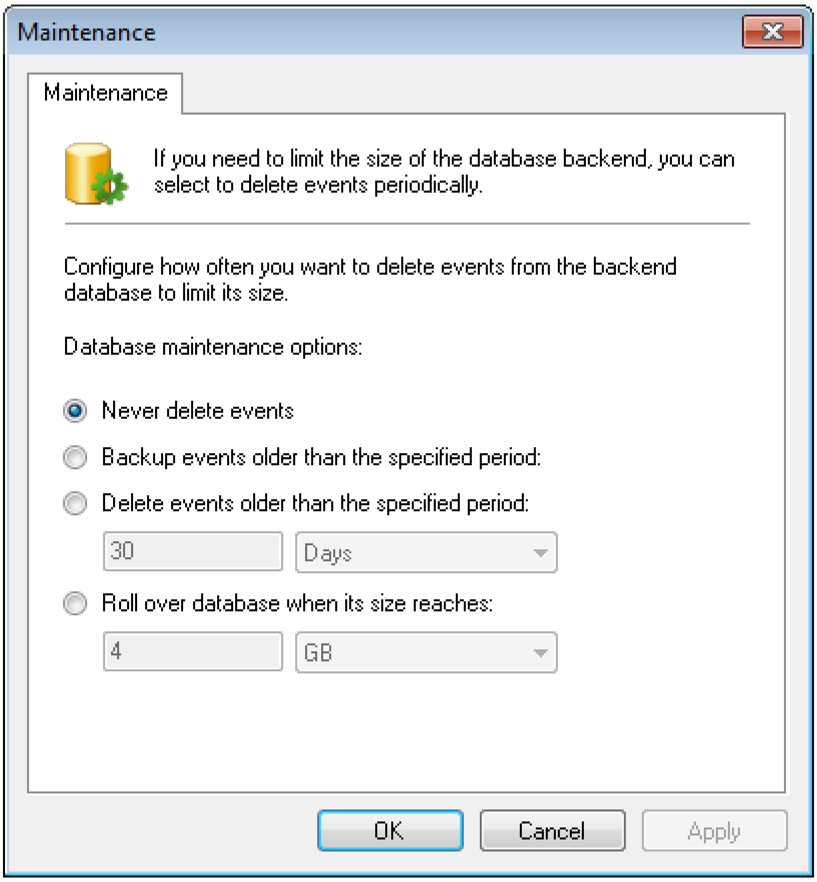
Periodical database maintenance is essential in order to prevent your database backend from growing too much. GFI EndPointSecurity provides you with the facility to configure parameters that automatically maintain your database backend.

To configure database backend maintenance:

1. Click **Configuration** tab **>** **Options** sub-tab.

2. From **Configure**, select **Database Backend**.

3. From the right pane, click **Database maintenance**.



If you need to limit the size of the database backend, you can select to delete events periodically.

Configure how often you want to delete events from the backend database to limit its size.

Database maintenance options:

● Never delete events

○ Backup events older than the specified period:

○ Delete events older than the specified period:

30 Days

○ Roll over database when its size reaches:

4 GB

Screenshot 123: Maintenance options

4. From the **Maintenance** dialog, configure how often events are deleted from the database backend. Select from the options described below:

Option	Description
Never delete events	Keep all events in your database backend, without deleting old ones. **Note** Ensure that manual deletion of old records is done to prevent GFI EndPointSecurity performance loss.
Backup events older than the specified period	Select this option and specify how old events have to be before they are backed up in a separate database.
Delete events older than the specified period	Select this option and specify how old events have to be before they are deleted.
Roll over database when its size reaches	Specify the maximum size a database can grow before GFI EndPointSecurity automatically switches to a new database.

5. Click **Apply** and **OK**

> **Note**
>
> Since Microsoft SQL Express 2005 has a database size limitation of 4 GB and Microsoft SQL Express 2008 R2 has a database limitation of 10 GB, it is recommended to use Roll over database option. For more information on Microsoft SQL Server Edition, engine specifications, refer to http://go.gfi.com/?pageid=ESEC_SqlSpecs

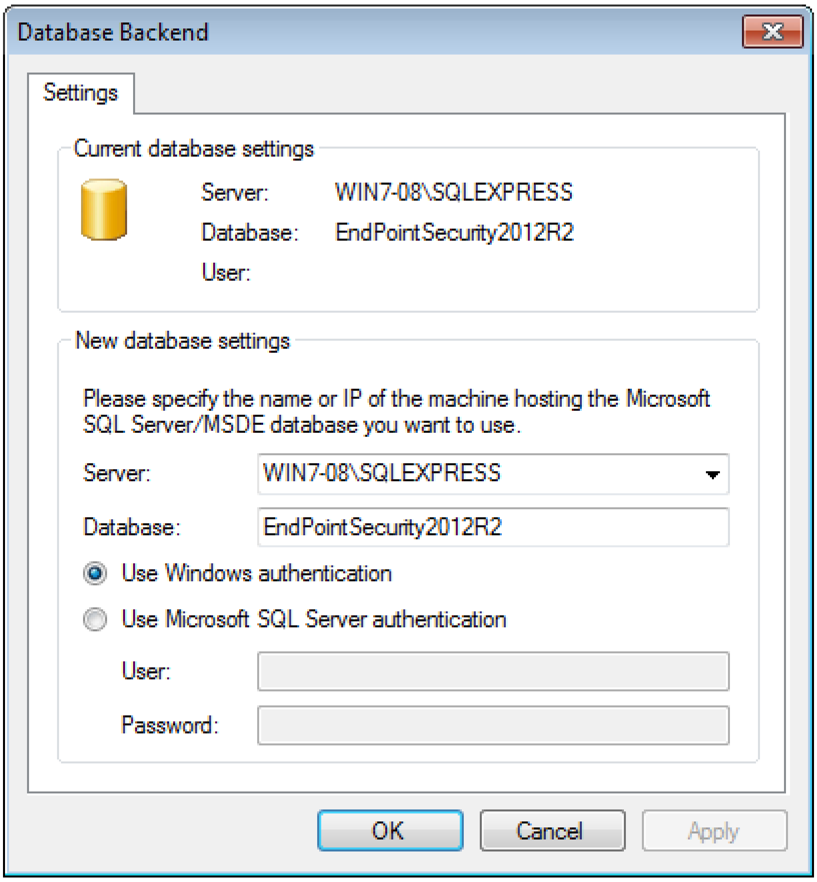
12.2 Using an existing SQL Server instance

To connect to an existing SQL Server instance:

1. Click **Configuration** tab **>** **Options** sub-tab.

2. From **Configure**, select **Database Backend**.

3. From the right pane, click **Change database backend**.



Database Backend

Settings

Current database settings

Server: WIN7-08\SQLEXPRESS

Database: EndPointSecurity2012R2

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: WIN7-08\SQLEXPRESS

Database: EndPointSecurity2012R2

● Use Windows authentication

○ Use Microsoft SQL Server authentication

User:

Password:

Screenshot 124: Change Database Backend

4. From the **Server** drop-down menu, select the SQL Server you want to use.

5. Specify the name of the database in the **Database** text box.

6. Select the authentication mode and specify the logon credentials, if necessary.

7. Click **Apply** and **OK**

13 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.

14 Uninstalling GFI EndPointSecurity

GFI EndPointSecurity enables you to easily uninstall both the GFI EndPointSecurity agents and the GFI EndPointSecurity application.

This chapter covers the following topics:

- Uninstalling GFI EndpointSecurity agents
- Uninstalling GFI EndpointSecurity application

> **Warning**
> GFI EndPointSecurity agents are not uninstalled automatically during the un-installation of the GFI EndPointSecurity application. It is best that first you uninstall the GFI EndPointSecurity agents and next the GFI EndPointSecurity application.

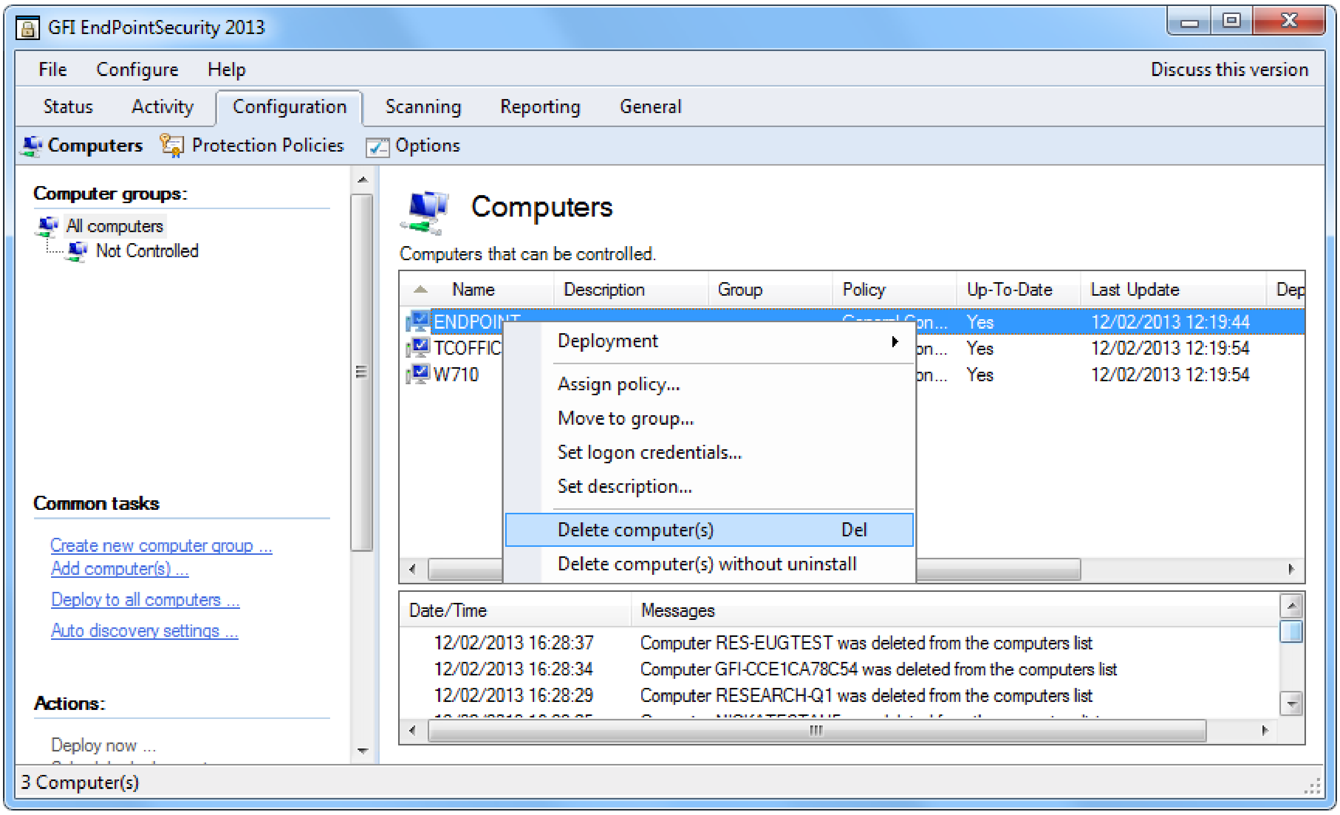
14.1 Uninstalling GFI EndPointSecurity agents

> **Warning**
> GFI EndPointSecurity agents are not uninstalled automatically during the un-installation of the GFI EndPointSecurity application. It is best that first you uninstall the GFI EndPointSecurity agents and next the GFI EndPointSecurity application.

To uninstall a GFI EndPointSecurity agent:

1. From the GFI EndPointSecurity management console, click **Configuration** tab.

2. Click **Computers** sub-tab.



Computers

Computers that can be controlled.

Name	Description	Group	Policy	Up-To-Date	Last Update	Dep
ENDPOINT			General Con...	Yes	12/02/2013 12:19:44	
TCOFFIC			...on...	Yes	12/02/2013 12:19:54	
W710			...on...	Yes	12/02/2013 12:19:54	

Date/Time	Messages
12/02/2013 16:28:37	Computer RES-EUGTEST was deleted from the computers list
12/02/2013 16:28:34	Computer GFI-CCE1CA78C54 was deleted from the computers list
12/02/2013 16:28:29	Computer RESEARCH-Q1 was deleted from the computers list

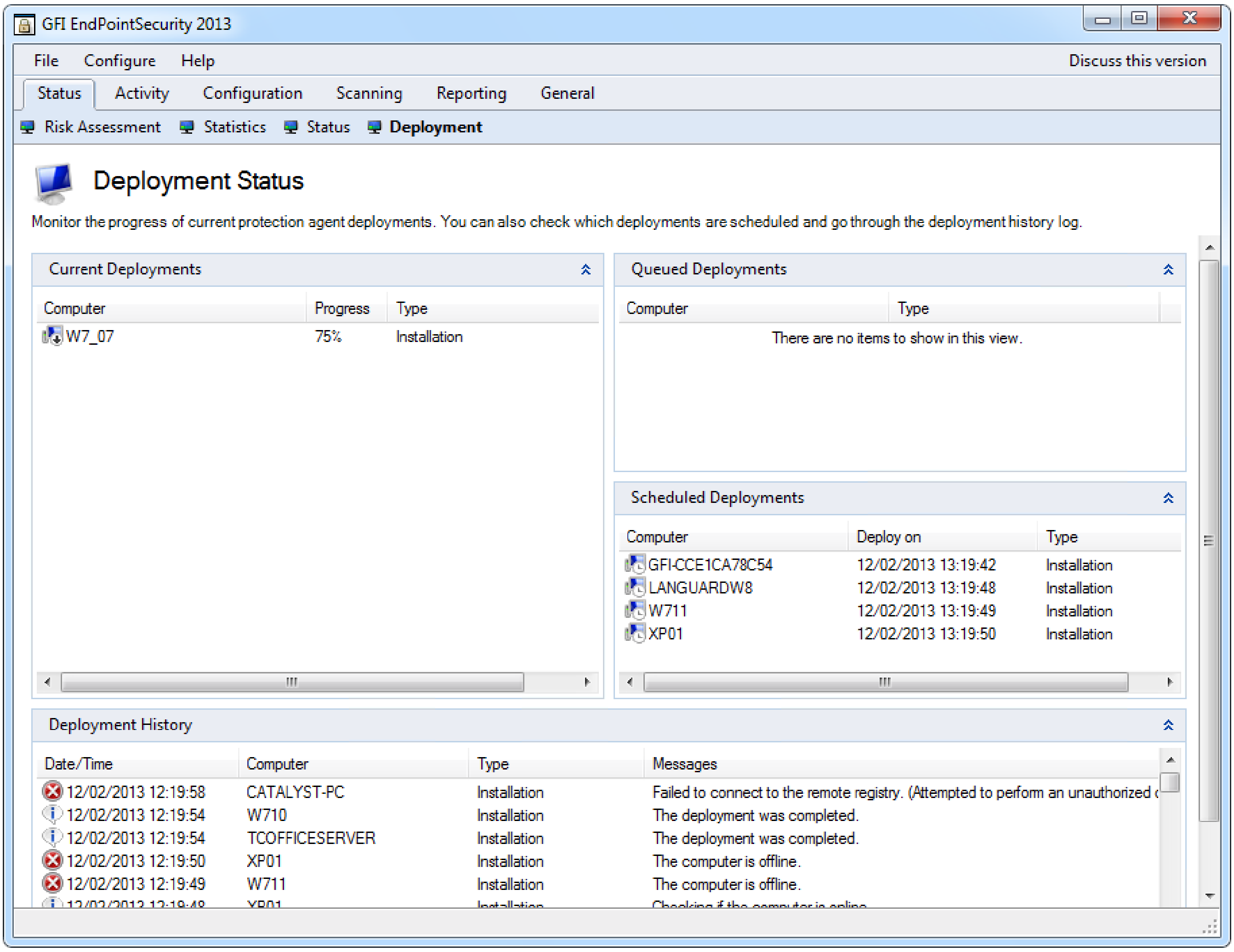
Screenshot 125: Computers sub-tab - delete computer(s)

3. From the right pane, right-click target computer that you would like to uninstall and select:

Deleting Computer(s)	
Deleting computer(s) - **with** uninstallation	GFI EndPointSecurity will deploy protection policy updates and uninstalls Agent.
Deleting computer(s) - **without** uninstallation	GFI EndPointSecurity will deploy protection policy updates and removes the relevant computer entry from the Computers list. However it leaves the agent installed on the target computer. This is useful in the event that the target computer was removed from the network and GFI EndPointSecurity application is unable to connect to it to uninstall the agent.

4. Click **Yes** to confirm the deletion of the selected computer from the list.

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



Deployment Status

Monitor the progress of current protection agent deployments. You can also check which deployments are scheduled and go through the deployment history log.

Current Deployments

Computer	Progress	Type
W7_07	75%	Installation

Queued Deployments

Computer	Type

There are no items to show in this view.

Scheduled Deployments

Computer	Deploy on	Type
GFI-CCE1CA78C54	12/02/2013 13:19:42	Installation
LANGUARDW8	12/02/2013 13:19:48	Installation
W711	12/02/2013 13:19:49	Installation
XP01	12/02/2013 13:19:50	Installation

Deployment History

Date/Time	Computer	Type	Messages
☒ 12/02/2013 12:19:58	CATALYST-PC	Installation	Failed to connect to the remote registry. (Attempted to perform an unauthorized c
ⓘ 12/02/2013 12:19:54	W710	Installation	The deployment was completed.
ⓘ 12/02/2013 12:19:54	TCOFFICESERVER	Installation	The deployment was completed.
☒ 12/02/2013 12:19:50	XP01	Installation	The computer is offline.
☒ 12/02/2013 12:19:49	W711	Installation	The computer is offline.
ⓘ 12/02/2013 12:19:48	XP01	Installation	Checking if the computer is online.

Screenshot 126: Deployment sub-tab

6. From the **Deployment History** area, confirm the successful completion of the un-installation from the target computer.

14.2 Uninstalling GFI EndPointSecurity application

To uninstall the GFI EndPointSecurity application:

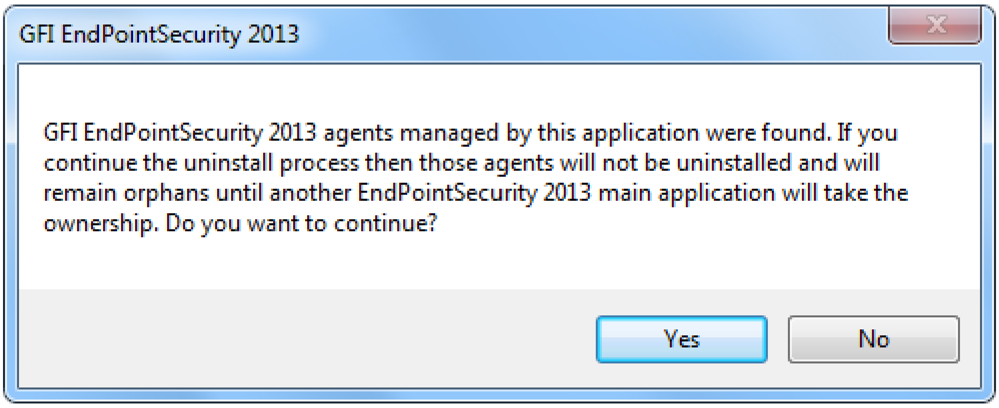
> **Note**
>
> Run the uninstaller as a user with administrative privileges on the computer.

1. From the **Microsoft Windows Control Panel**, select **Add/Remove Programs** or **Programs and Features** option.

2. Select GFI EndPointSecurity.

3. Click **Change** to start the un-installation of GFI EndPointSecurity application.

4. Click **Next** at the Welcome screen to continue un-installation.


GFI EndPointSecurity 2013

GFI EndPointSecurity 2013 agents managed by this application were found. If you continue the uninstall process then those agents will not be uninstalled and will remain orphans until another EndPointSecurity 2013 main application will take the ownership. Do you want to continue?

Screenshot 127: Uninstallation information message

> **Note**
>
> If any agents are still installed, an information dialog is displayed asking you whether you would like to continue (the agents will remain installed and orphans) or stop the un-installation process. For more information about uninstalling agents, refer to the Uninstalling GFI EndPointSecurity agents section in this chapter.

5. Select **Uninstall without deleting configuration files** or **Complete uninstall** option and click **Next** to continue.

6. Upon completion, click **Finish** to finalize un-installation.

15 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.

15.1 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.

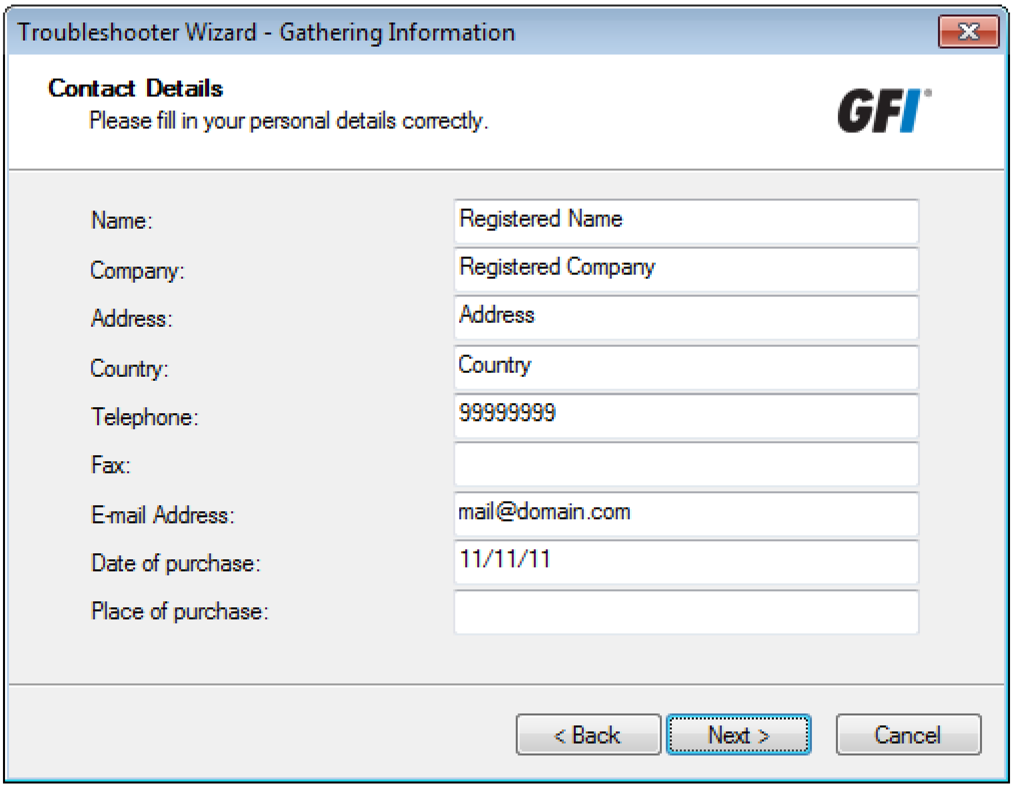
Issue	Possible Cause	Possible Solution
Failed to install the deployment service. (error)	GFI EndPointSecurity agent was not able to be installed or uninstalled by the service running on the target computer.	For more details about the cause of the error and a possible solution, refer to the system error message within the parenthesis.
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**.

15.2 Using GFI EndPointSecurity Troubleshooter

To use the troubleshooting tool provided by GFI EndPointSecurity:

1. Click **Start > Programs > GFI EndPointSecurity2013 > GFI EndPointSecurity2013 Troubleshooter**.

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

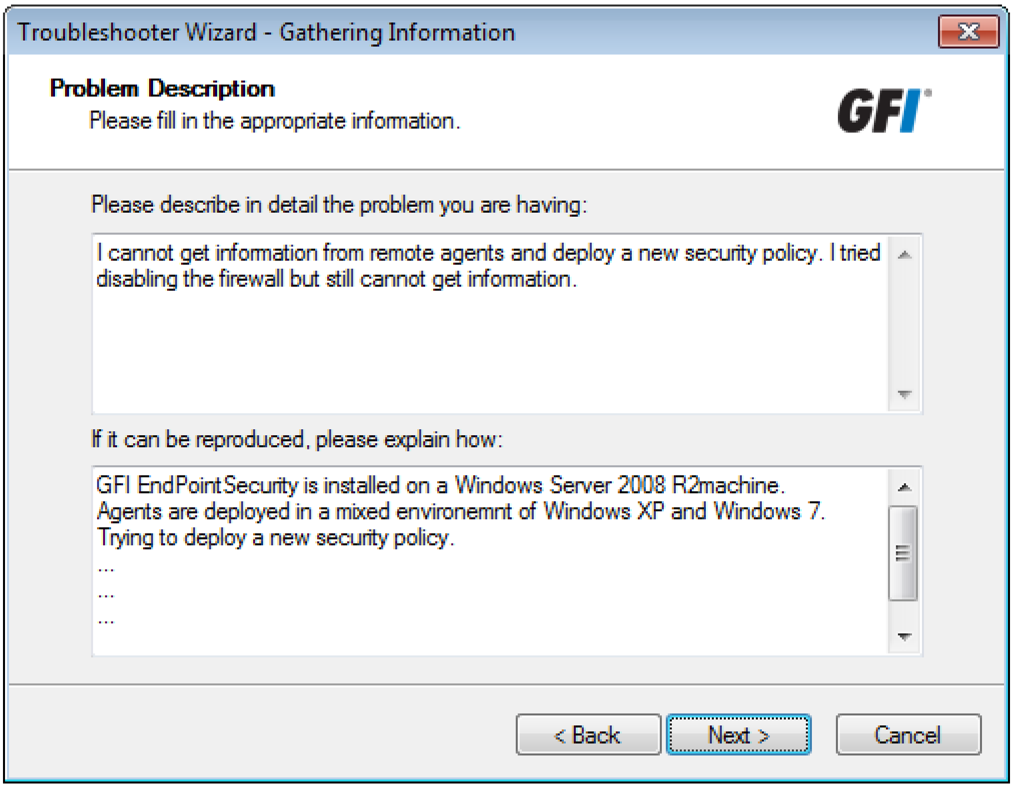


Troubleshooter Wizard - Gathering Information
Contact Details
Please fill in your personal details correctly.
GFI
< Back
Next >
Cancel

Name:	Registered Name
Company:	Registered Company
Address:	Address
Country:	Country
Telephone:	99999999
Fax:	
E-mail Address:	mail@domain.com
Date of purchase:	11/11/11
Place of purchase:	

Screenshot 128: Specifying contact and purchase details

3. Key in your contact details so that our support team would be able to contact you for further analysis information. Click **Next**.



Problem Description

Please fill in the appropriate information.

Please describe in detail the problem you are having:

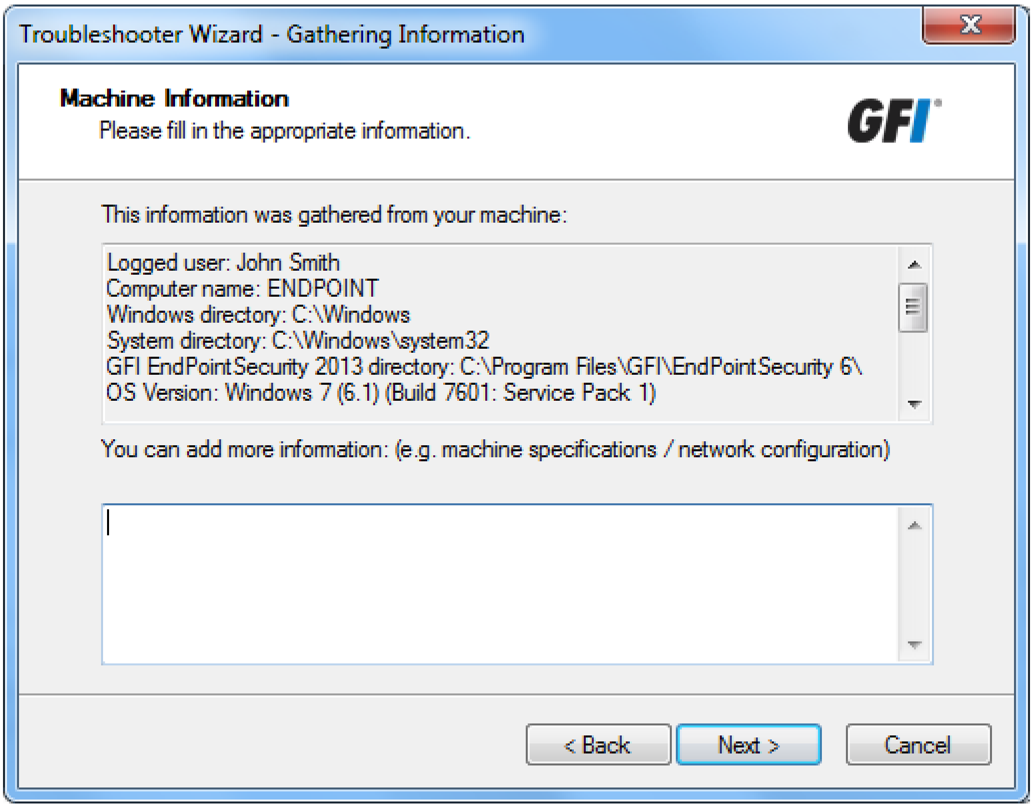
I cannot get information from remote agents and deploy a new security policy. I tried disabling the firewall but still cannot get information.

If it can be reproduced, please explain how:

GFI EndPointSecurity is installed on a Windows Server 2008 R2machine.
Agents are deployed in a mixed environemnt of Windows XP and Windows 7.
Trying to deploy a new security policy.
...
...
...

Screenshot 129: Specifying issue details and other relevant information to recreate the problem

4. Specify the error you are getting and other information that would help our support team recreate this issue. Click **Next**.



Machine Information

Please fill in the appropriate information.

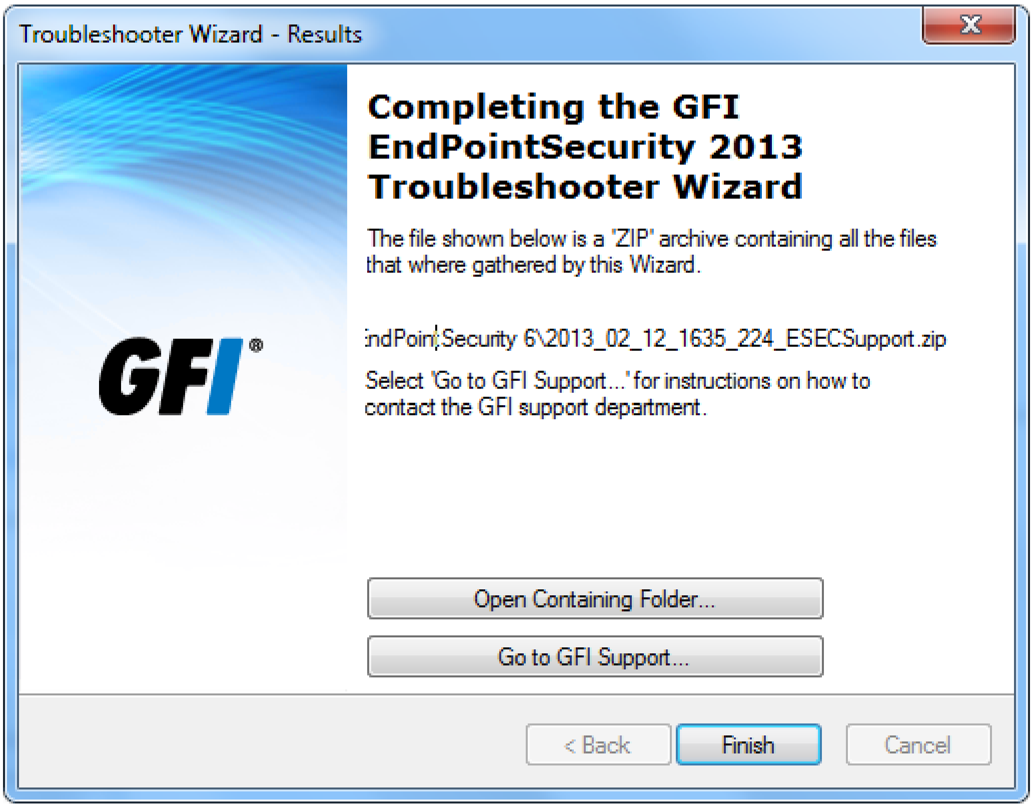
This information was gathered from your machine:

Logged user: John Smith
Computer name: ENDPOINT
Windows directory: C:\Windows
System directory: C:\Windows\system32
GFI EndPointSecurity 2013 directory: C:\Program Files\GFI\EndPointSecurity 6\
OS Version: Windows 7 (6.1) (Build 7601: Service Pack 1)

You can add more information: (e.g. machine specifications / network configuration)

Screenshot 130: Gathering machine information

5. The troubleshooter scans your system to get hardware information. You can manually add more information in the space provided or click **Next**.



Troubleshooter Wizard - Results

Completing the GFI EndPointSecurity 2013 Troubleshooter Wizard

The file shown below is a 'ZIP' archive containing all the files that where gathered by this Wizard.

:ndPoint Security 6\2013_02_12_1635_224_ESECSupport.zip

Select 'Go to GFI Support...' for instructions on how to contact the GFI support department.

Screenshot 131: Finalizing the Troubleshooter wizard

6. At this stage, the troubleshooter creates a package with the information gathered from the previous steps. Next, send this package to our support team so they can analyze and troubleshoot your problem. Click the buttons described below for sending options:

- **Open Containing Folder** - Opens the folder containing the troubleshooter package so that you can send the package manually via email
- **Go to GFI Support** - Opens the support page of GFI website.

7. Click **Finish**.

15.3 Resources

15.3.1 GFI knowledge base

GFI maintains a comprehensive knowledge base repository, which includes answers to the most common problems. GFI knowledge base always has the most up-to-date listing of technical support questions and patches. In case that the information in this guide does not solve your problems, next refer to GFI knowledge base by visiting: http://www.gfi.com/support.

15.3.2 Web Forum

User to user technical support is available via the GFI web forum. Access the web forum by visiting: http://forums.gfi.com/.

15.3.3 Request technical support

If none of the resources listed above enable you to solve your issues, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online**: Fill out the support request form and follow the instructions on this page closely to submit your support request on: http://support.gfi.com/supportrequestform.asp
- **Phone**: To obtain the correct technical support phone number for your region visit: http://www.gfi.com/company/contact.htm

> **NOTE**
> Before contacting Technical Support, have your Customer ID available. Your Customer ID is the online account number that is assigned to you when first registering your license keys in the GFI Customer Area at: http://customers.gfi.com.

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

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.

16 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.

17 Index