# R-Guard Data Security Software

*User Manual*

# R-Guard Help

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

# Table of Contents

# 1 Introduction

Windows security services have various means of computer security control. These means are in the first place crucial for a computer working in a small network (a workgroup level). The system administrators can protect confidential information against unauthorized access by assigning various permissions (access rights) to system files and folders. Each user can have a specifically modified set of access rights to a file system object. Besides, a user can have exclusive access rights to a file or a folder if he or she created it.

**R-Guard** is a powerful tool for advanced access rights control and audit, which extends much beyond the scope of the standard **Windows** security system. **R-Guard** allows the user to control access rights to various file system objects (files and folders) not only for users, but for applications or system processes as well. **R-Guard** also provides tools for data encryption.  These features can prevent data theft, corruption, and deletion by various malicious programs such as viruses, trojan horses, spyware, etc.

**R-Guard** assigns access rights for:

- ***Users and Groups***. This can be done on the **Access Control** panel.
- ***Applications***. This can be done on the **Access Control** and the **Process Rules** panels.

**R-Guard** has six main panels:

- An **Access Control Panel** on which the user can define user and process access rights for files and folders;
- An **Encryption Panel** on which the user can encrypt files and folders and define users and groups of users to whom the encrypted files and folders will be accessible;
- A **Process Rules Panel** on which the user can view the whole set of existing mandatory rules for files and folders and remove rules;
- A **User Management Panel** on which the user can add new users and groups;
- An **Audit Panel** on which the user can view the list of all computer operations and processes with comments and date/time;
- A **File Monitor Panel** on which the user can view the list of current computer operations and processes.

Use the **View** button on the toolbar to switch between these panels or click the panel icons on the left pane of the window.
Use the **File** button to exit the program and to define the parameters of deleting old Audit files.

## 1.1 R-Guard Features

R-Guard has the following features:

**Total control over file/folder operations at the user application level**

- Two types of access control: user-specific and process-specific access rights
- Process-specific access rights (assigned to a folder) can be "recursive". Recursive access rights apply for the files and folders contained not only in a parent folder, but for objects in all subfolders, too
- An ability to completely isolate any file from any process
- Blocking file access (Read\Write\Rename\Delete) on any file system
- Block start of any executable file (.EXE .DLL .COM .BAT .HTML .XML .JS .CLASS, 32/16bit applications, Win32, Win16, Dos, DPMI)
- True file hiding ("True Hidden" is the possibility of hiding a file or a folder from the users. Moreover,

file access operations (reading, modifying, deletion and renaming) are also blocked)

- Wipe file on delete ("Wipe on deletion" is a total deletion of a file or a folder from the system that makes a file or a folder recovery with standard utilities impossible. Each file byte on a disk is physically overwritten and disk free space is increased.
- Transparent file encryption. For the users, working with an encrypted file is similar to that with any plain file of file system. Other users will not have access to this file. The user is not required to enter the password for files encryption and decryption because the key information is initialized when the Windows user is identified during logon.
- Protection against unauthorized file modification (CRC-128). If any local or network file has been modified during unauthorized access, **R-Guard** will block access to such file
- Extended attributes stored in a distributed database (UNIX-stile data security architecture). This feature allows the user to set extended attributes independently from a file system, or even on removable and network media
- Support for swap file encryption (Windows 95/98/ME only)
- Compatibility with all versions of Windows OS (starting Windows 95, excluding Windows 95 OSR2) and low system requirements
- Low volume space required on a hard drive (less than 4 Mb) mostly due to transparent file encryption
- A file monitor allows the user to view current file operations and tune applications access rights to files and folders
- Monitoring of local and network logons and blocking user logons according to **R-Guard** policy set by its administrator

**Flexible and detailed audit**

- Flexible and detailed audit of all operations for any file
- A compact binary audit format to save disk space
- Linking between users, processes, and file operations
- Powerful audit search by file masks, regular expressions, data, time
- Ability to tune audit and delete old audit notes

**Self-protection**

- A secure connection between **R-Guard** control panels and kernel
- Protection of **R-Guard** modules and audit files from unauthorized access
- Protection against **R-Guard** kernel debugging and unhooking

**User-friendly interface**

- A standard outlook-style interface
- Two additional tabs on the standard **Properties** window, which allow for assigning access rights to a file or a folder for users or processes
- Quick and easy creation of a user access rule to a file or a folder by using the Wizard

## 1.2 Contact Information and Technical Support

To obtain the latest version of **R-Guard**, go to:

Product Site: http://www.r-tt.com
Sales Department: sales@r-tt.com

The **R-Guard** Technical Support Team is available 24 hours a day, seven days a week, and has an average e-mail response time less than 4 hours.

Tech. Support: support@r-tt.com
Send your support request to: http://www.r-tt.com/Support_request.html

# 2 User R-Guard Interface

**R-Guard** is a standard Microsoft Windows application for providing the data security and for the access rights control, file or folder encryption and audit.
Upon installation, a shortcut to **R-Guard** with the "" icon appears in the **Start** menu .

- To start **R-Guard**, select ***Programs/R-Guard/R-Guard*** in the **Start** menu.
- To close the **R-Guard Main** window: select ***File/Exit*** in the **R-Guard** Main menu or click ***Close*** (☒) on the **R-Guard** window.

The **R-Guard**'s user interface consists of the following parts:

- R-Guard Main Window
- R-Guard Main Menu
- R-Guard Left Panel
- R-Guard Right Panel

## 2.1 R-Guard Main Window

The R-Guard Main window consists of:

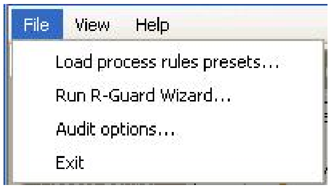
- The **R-Guard Main menu**, a bar with the names of the **R-Guard** command sets.
- The **R-Guard Left Panel** containing buttons for the main **R-Guard** functions.
  To select one of the functions:click a button or select a corresponding command of the **R-Guard** Main menu ***View\Access Control, Encryption, Process Rules, User Management, Audit, File Monitor.***
- The **R-Guard Right (informational) Panel** showing you **R-Guard** settings and allowing you to perform the main user`s actions. The buttons on the **R-Guard** Left Panel control the content of the **R-Guard** Right Panel.
- The **Status bar** displaying various information about the current **R-Guard** state (the current user and version, the kernel).

## 2.2 R-Guard Main Menu

The **R-Guard** Main Menu is a bar with the names of the **R-Guard** command sets.

The **File set** contains the following commands:

**File set**

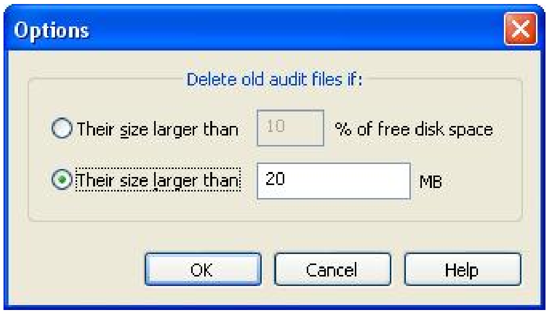


- ***Load process rules presets...***: loads the default access rules to the most used applications.
- ***Run R-Guard Wizard…***: starts the Wizard that creates access rules to files and folders.
- ***Audit options…***: opens the **Options** window allowing you to modify the Audit information storage mode (the Audit file operations). This information is displayed on the **R-Guard** Right Panel when

the **Audit** button is clicked.

In the **Options window** you can modify the following settings of the old Audit information deletion:

**Options window**



Delete old audit files if:

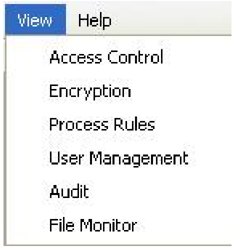
○ Their size larger than 10 % of free disk space

● Their size larger than 20 MB

- Select the ***Their size larger than % of disk free space*** option and enter the percent of the allowed free disk space in the text field. If the volume of the Audit information is larger than the assigned free disk space, the old Audit files will be gradually deleted at the appearance of new files.
- Select the ***Their size larger than MB*** option and enter the allowed number of MB. If the volume of the Audit information is larger than the allowed volume in MB, the old Audit files will be gradually deleted at the appearance of new files.
- Click **OK**.
- ***Exit***: stops the work of **R-Guard** and closes the application window.

The **View set** contains the following commands:

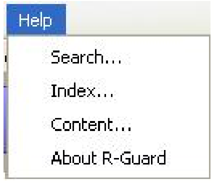
**View set**



- ***Access Control***, ***Encryption***, ***Process Rules***, ***User Management***, ***Audit***, ***File Monitor***, which correspond the buttons on the R-Guard Left Panel.

The **Help set** contains the following commands:

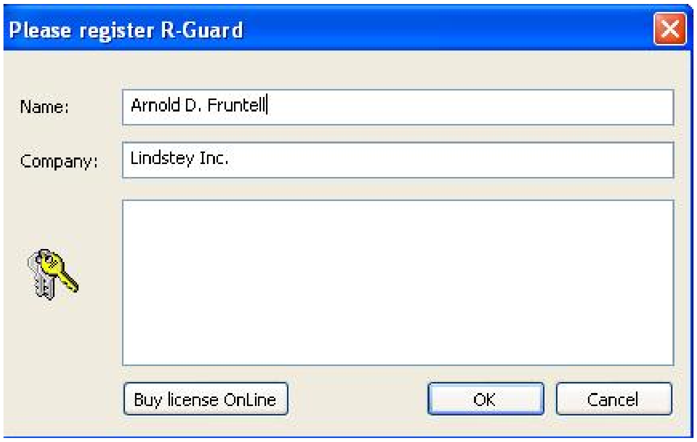
**Help set**



- The **R-Guard** Help commands (**Search**, **Index**, **Content**): opens this document.
- ***About R-Guard***: provides information about R-Guard, the version of the application (in the top right corner) and the registration status. If you are using a demo version, it shows how many days are left until the trial period is over. If you are a registered user, it shows the name of the user (***Registered to***), the company (***Company***) and the e-mail (***E-mail***). You should click ***Register*** button to register **R-Guard**. The Registration window will appear. You should enter the name of

**R-Guard** license owner in the field ***Name***, the name of the company in the field ***Company*** and the registration number in the low field. Then click ***OK***.

**Registration window**



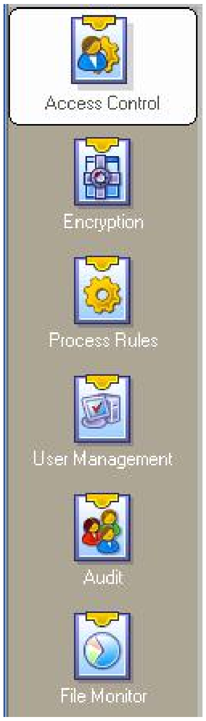
Name: Arnold D. Fruntell

Company: Lindstey Inc.

## 2.3 R-Guard Left Panel

The R-Guard Left Panel has the buttons for the main **R-Guard** functions. To activate a function, click the button or select the corresponding command of the **R-Guard** Main Menu: ***View\Access Control, Encryption, Process Rules, User Management, Audit, File Monitor.***

**R-Guard Left Panel**



Overall, the **R-Guard** Left Panel has 6 buttons:

- The **Access Control** button: displays on the **R-Guard** Right Panel the information about the main **R-Guard** functionality and allows you to control access of users and applications to files and folders. It is the main application mode.

- The **Encryption** button: displays on the **R-Guard** Right Panel the information, allowing you to encrypt files and folders. The Encryption function is also available on the **R-Guard** Access Control Panel.
- The **Process Rules** button: displays on the **R-Guard** Right Panel the information, allowing you to control the access of applications to files and folders;
- The **User Management** button: displays on the **R-Guard** Right Panel the information, allowing you to manage **R-Guard** users and their default access rights. Any user with the right to run **R-Guard** should have the Administrator status. In order to do this, he or she should belong to the **Administrators** group on this computer or at least have the Windows Administrator access rights (for Windows NT/2K/XP/2003);
- The **Audit** button: displays on the **R-Guard** Right Panel the information about the Operational System Audit and Audit filters;
- The **File Monitor** button: displays on the **R-Guard** Right Panel the information about the process monitoring.

## 2.4 R-Guard Right Panel

The **R-Guard** Right Panel displays the work and settings of **R-Guard**. The corresponding buttons on the R-Guard Left Panel allow you to navigate through the **R-Guard** Right Panel content.

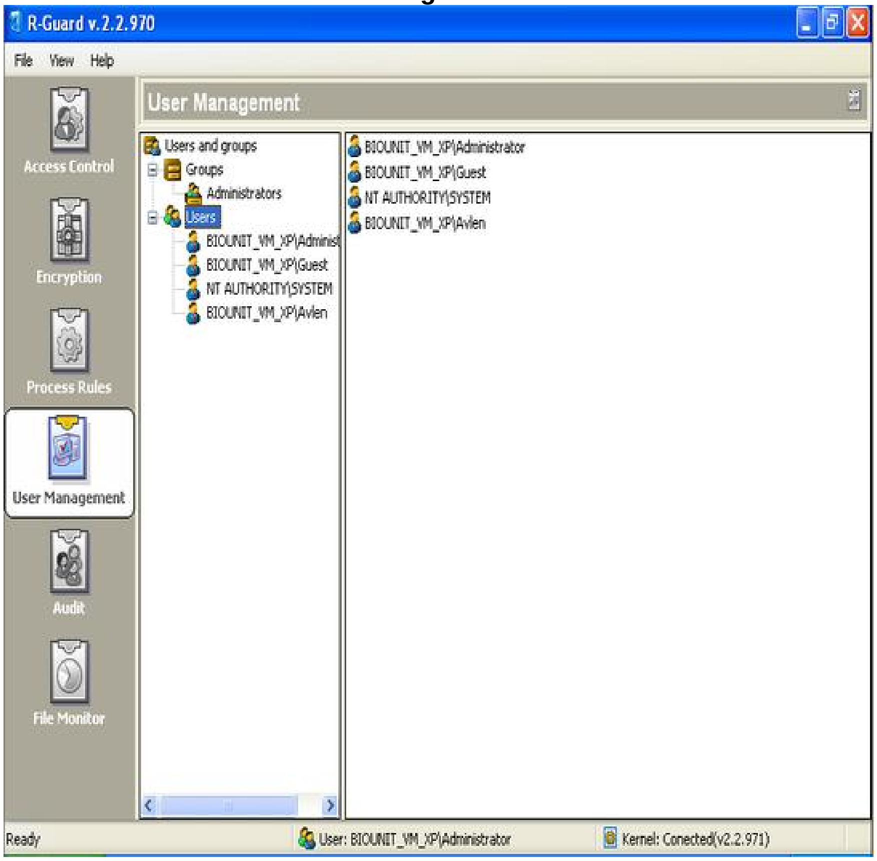
# 3 User Management Panel

You need to define users and user groups in **R-Guard** before assigning them access rights. This can be done on the **User Management** panel (click the **User Management** button on the left menu). Users not defined in **R-Guard** do not have remote access to this computer resources and they will have the Guest restrictions when working with **R-Guard**. You can also modify the default access rights of users to files or folders on this panel.

This panel contains:

- The left pane with the ***tree of users and groups***, for which access rights to objects are to be assigned;
- The ***right pane*** where you can view users of a group selected in the tree, or the group to which the selected user belongs.

**User Management Panel**



You can do the following operations on this panel:

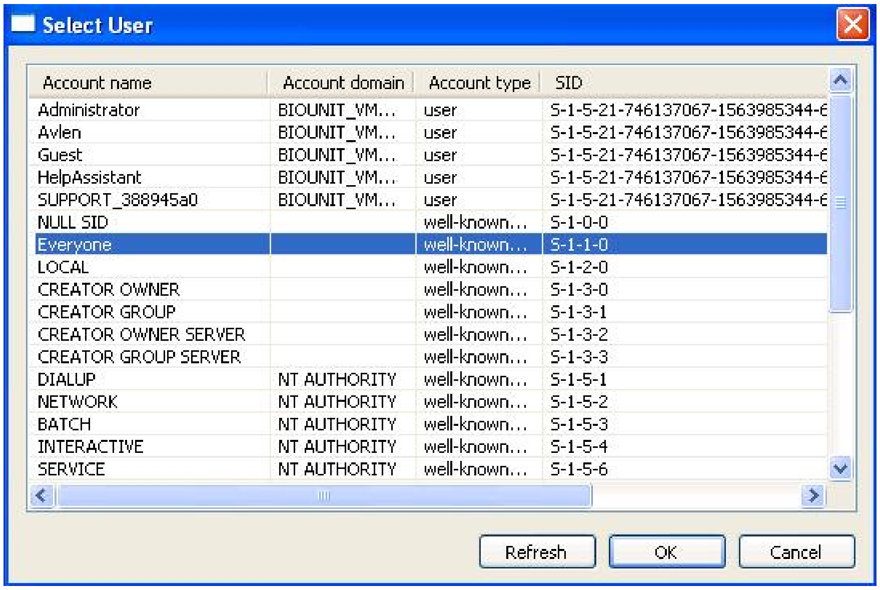
- Add a new user;
- Add a new group;
- Edit user properties;
- Edit group properties;
- Move users to groups;
- Remove user;
- Remove group.

## 3.1 Adding a New User

**Adding a new user for Windows 9x**.
**To add a new user, do the following:**

1. Right-click **Users** on the **Users and Groups** tree and select **Add new** from the menu. Users are added from the list of system users. Automatically the following users are added during the program installation: Guest, Administrator and System (NT Authority).
2. Select a user from the list of system users. This list contains the following information:

**List of system users**



| Account name | Account domain | Account type | SID |
|---|---|---|---|
| Administrator | BIOUNIT_VM... | user | S-1-5-21-746137067-1563985344-6 |
| Avlen | BIOUNIT_VM... | user | S-1-5-21-746137067-1563985344-6 |
| Guest | BIOUNIT_VM... | user | S-1-5-21-746137067-1563985344-6 |
| HelpAssistant | BIOUNIT_VM... | user | S-1-5-21-746137067-1563985344-6 |
| SUPPORT_388945a0 | BIOUNIT_VM... | user | S-1-5-21-746137067-1563985344-6 |
| NULL SID | | well-known... | S-1-0-0 |
| Everyone | | well-known... | S-1-1-0 |
| LOCAL | | well-known... | S-1-2-0 |
| CREATOR OWNER | | well-known... | S-1-3-0 |
| CREATOR GROUP | | well-known... | S-1-3-1 |
| CREATOR OWNER SERVER | | well-known... | S-1-3-2 |
| CREATOR GROUP SERVER | | well-known... | S-1-3-3 |
| DIALUP | NT AUTHORITY | well-known... | S-1-5-1 |
| NETWORK | NT AUTHORITY | well-known... | S-1-5-2 |
| BATCH | NT AUTHORITY | well-known... | S-1-5-3 |
| INTERACTIVE | NT AUTHORITY | well-known... | S-1-5-4 |
| SERVICE | NT AUTHORITY | well-known... | S-1-5-6 |

- **Account name** of the user. Any user on this computer should be included into the Administrators group (select **Start: Settings\Control Panel\User Accounts\Users** to view group membership).
- **Account domain** of the user. The computer should have access to the domain where the user is working. Otherwise the name of the local machine is contained in this field.
- **Account type** of the user (user, well-known group, etc.).
- **SID** is the identification number of the user member of the Windows domain. It consists of the ID number of this computer/domain and the ID number of this user in the domain.

3. Click **Refresh** to receive an updated list of system users.
4. Click **OK**.
5. Enter and confirm a password for the user for file encryption. Click **OK**.
6. Assign the default access rights for this user, including the user account name, status of the user (Supervisor, Administrator, User, Guest). In the **Event log** column specify the operations by this user that will be registered in the Audit.
7. Click **OK**.

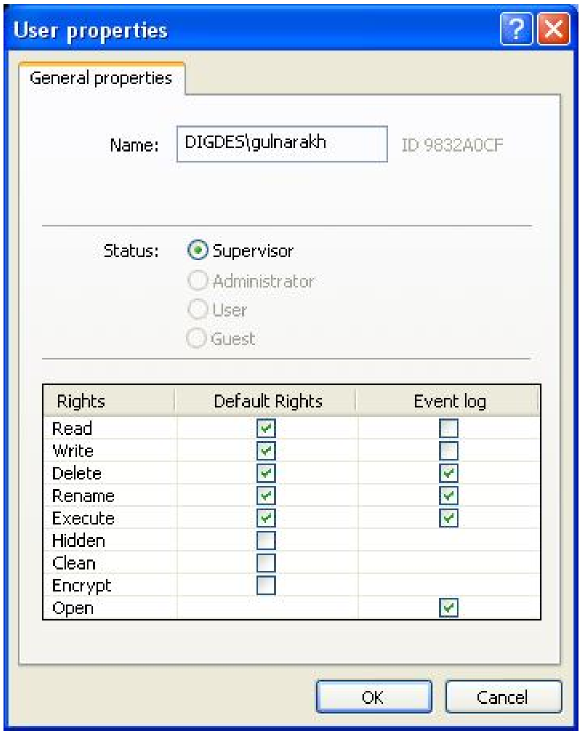
The selected used will be added to users on the **Users and Groups** tree.
Three default users are added automatically after installation into the **Users and Groups** tree: Administrator, Guest and System (NT Authority). Their statuses cannot be changed and they cannot be deleted from the system. The Administrator and System (NT Authority) users have the Supervisor status. These users always have individual access to files and folders, if a user/group of users has an individual access to a file or folder, these users with the Supervisor status will have the same access rights. If no user/group of users has individual access rights to a file or a folder, Supervisor will have access rights as Others have. Guest user has the Guest status.

**Adding a new user for Windows 9x**

**To add a new user, do the following**:

1. Right-click **Users** on the **Users and Groups** tree and select **Add new** from the menu. The **User properties** panel will appear.

**User properties**



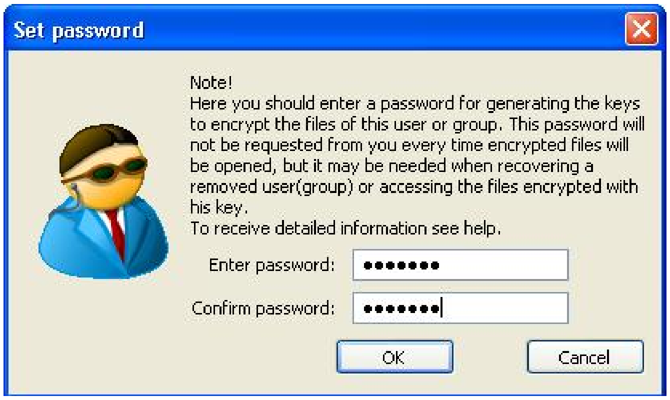
Name: DIGDES\gulnarakh ID 9832A0CF

Status:
● Supervisor
○ Administrator
○ User
○ Guest

| Rights | Default Rights | Event log |
|---|---|---|
| Read | ☑ | ☐ |
| Write | ☑ | ☐ |
| Delete | ☑ | ☑ |
| Rename | ☑ | ☑ |
| Execute | ☑ | ☑ |
| Hidden | ☐ | |
| Clean | ☐ | |
| Encrypt | ☐ | |
| Open | | ☑ |

2. Type the name of the new user in the **Name** text field. Click the **Change Password** button to activate the Set Password window and enter a password for the new user.

**Set Password**



Note!
Here you should enter a password for generating the keys to encrypt the files of this user or group. This password will not be requested from you every time encrypted files will be opened, but it may be needed when recovering a removed user(group) or accessing the files encrypted with his key.
To receive detailed information see help.

Enter password: •••••••

Confirm password: •••••••

3. Assign the status of the new user. You may choose between two user statuses: **Administrator** and **User**. The other two statuses (**Supervisor** and **Guest**) are created automatically by the system and ***cannot be removed*** from the system.
   1. Supervisor is a user with the most extended rights to control **R-Guard**. This user installed **R-Guard**. When he/she logs in, he/she has access to all files or folders and subjects in the system and also can start Wizard.
   2. Administrator is a user that can control access rights and create users. Only administrators can start the **R-Guard** console. They can also start Wizard and use shell extension.
   3. User is an authorized user that has a certain set of access rights. He/she can work with R-Guard but cannot start R-Guard console or Wizard, cannot use shell extension. The User can read, write, rename, delete, and execute files.
   4. Guest is any unauthorized user. He/she can read, write, and execute files, but cannot delete or

rename them.

4. Set the default access rights for the new user in the **Default AR** (Default Access Rights) column and default log events in the **Log events** column. They are set for the files without any specifically defined access rights.

***Default event log*** - for example, if an event log point "read" is assigned to a user, all read operations performed by this user will be recorded in the event log on the **Audit** panel. *The **Hidden**, **Clean** and **Encrypted** points do not exist in the log events list, as these are not actions, but states of files or folders.*
**Note:** Avoid assigning default **Read** and **Write** operations. Otherwise log files may become excessively large and contain abundant information.

**Note:** You should be very cautious while setting the advanced attributes for **Others** because too restrictive rules may cause system malfunctions when the other users try to log in.

6. In the **Set default group** option, set the default group which also has access rights to newly created objects.

7. Click **OK** to save the data for the newly created user.

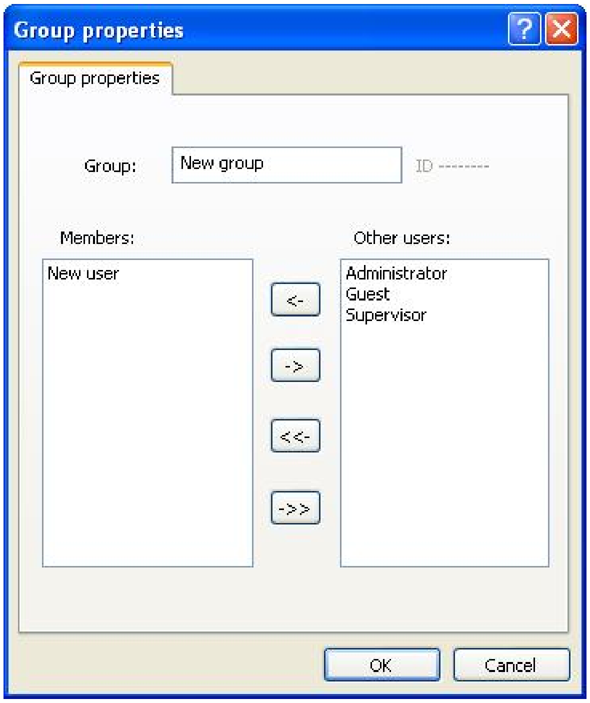
## 3.2 Adding New Group

**To add a new group, do the following:**

1. Right-click **Groups** on the **Users and Groups** tree and select **Add new** from the menu. Enter and confirm your password.

2. Click **OK**. **Group properties** panel will appear.

**Group properties**



Group properties

Group: New group

Members:

New user

Other users:

Administrator
Guest
Supervisor

3. Type the name of the new group in the **Group** text field.

4. Click the required user in the **Other users** field and click the left-arrow button to move users to the new group. They will appear in the **Members** field.

5. You can move all users to the new group by clicking the left double-arrow button.
6. To move users back to the **Other users** field, click the right-arrow buttons.
7. Click **OK** to save the data for the newly created group.

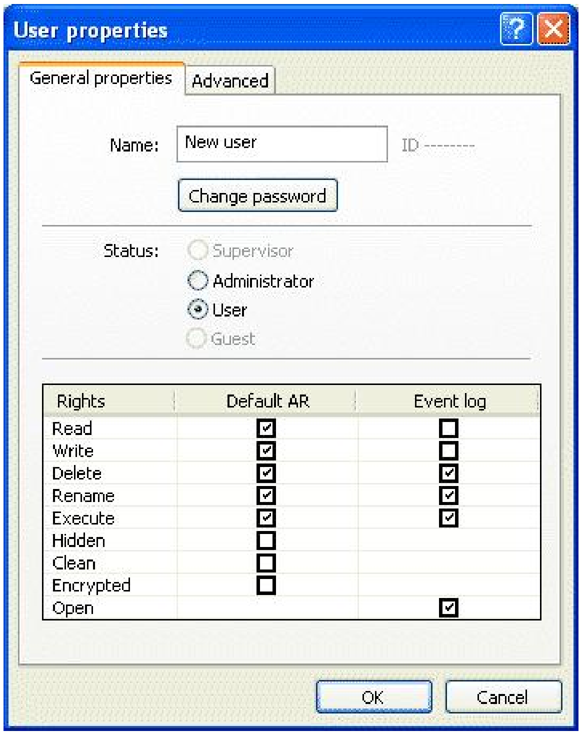
You can also add a user to group on the **Users and Groups** tree by drag-and-dropping him/her to the group. If a user is a member of one group and you need to add him/her to another group, drag-and-drop him/her to the group on the **Users and Groups** tree.

## 3.3 Editing User Properties

**To edit user properties do the following:**

1. Right-click **Users** on the **Users and Groups** tree and select **User properties** from the menu. The **User properties** panel will appear.

**User properties**



Name: New user ID --------

Status: ○ Supervisor ○ Administrator ● User ○ Guest

| Rights | Default AR | Event log |
|---|---|---|
| Read | ☑ | □ |
| Write | ☑ | □ |
| Delete | ☑ | ☑ |
| Rename | ☑ | ☑ |
| Execute | ☑ | ☑ |
| Hidden | □ | |
| Clean | □ | |
| Encrypted | □ | |
| Open | | ☑ |

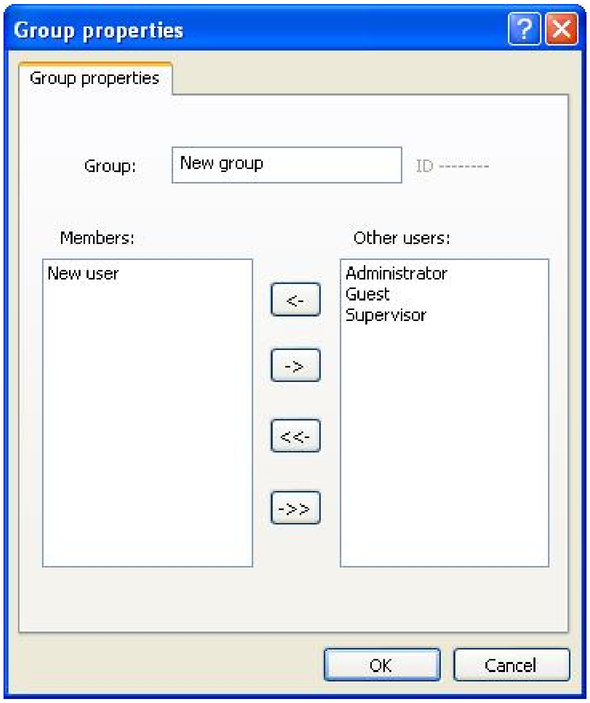
2. Make necessary changes in the user properties. You can change any user property except the name of the user (because it has a unique ID number given when the user has been created). You can see the user ID number next to the **Name** field.
3. Click **OK** to save changes.

## 3.4 Editing Group Properties

**To edit group properties do the following:**

1. Click **Group** on the **Users and Groups** tree and select **Group properties** from the menu. The **Group properties** panel will appear.

**Group properties**



Group: New group ID --------

Members:
New user

Other users:
Administrator
Guest
Supervisor

2. Make necessary changes in the group properties. You can change any properties except the name of the group (because it has a unique ID number given when the group has been created). You can see the group ID number next to the **Group** field.

3. Click **OK** to save changes.

## 3.5 Moving Users to Groups

**To move users to groups do the following:**

- Open the **Group properties** panel and move users to groups using the arrow buttons (go to the Editing Group properties help page for details).

**or**

- Select the required user and drag and drop the user to the required group.

## 3.6 Removing User or Group

To remove a user or a group do the following:

1. Right-click the required user or group in the **Users and Groups** tree and select **Remove** from the menu. A  confirmation message will appear.

2. Click **OK** to remove the user or group.

# 4 Access Control Panel

Click the **Access Control** button on the R-Guard Left Panel to view the information allowing you to control access of users and applications to files and folders. The **R-Guard** Right Panel displays the information about the main **R-Guard** functionality (it is the main application mode).

User and application access control to files and folders is necessary because:

- Files and folders may be used by several users with different access rights to the information. For example, employers should not be able to view or modify their manager's confidential information. Or children should be able to view only a certain set of files and folders and should not be able to delete or modify them.
- An application may not be working properly (there may be errors in its work), and it is reasonable to prohibit modification or deletion of valuable files by this application. Such files may all be located in a certain folder, thus it may be reasonable to prohibit modification or deletion of all files of this folder by this application.
- A "Trojan Horse" application may be installed on the user's computer without his or her knowledge. This application will try to transport secret information to the malefactor's computer. This problem can be solved by assigning access rights to the confidential files only for a limited set of applications. In this case, the access to the "Trojan Horse" application will be denied to the files, and there will be no loss of confidential information.

When the Access Control button is clicked, the **R-Guard** Right Panel is divided into three parts:

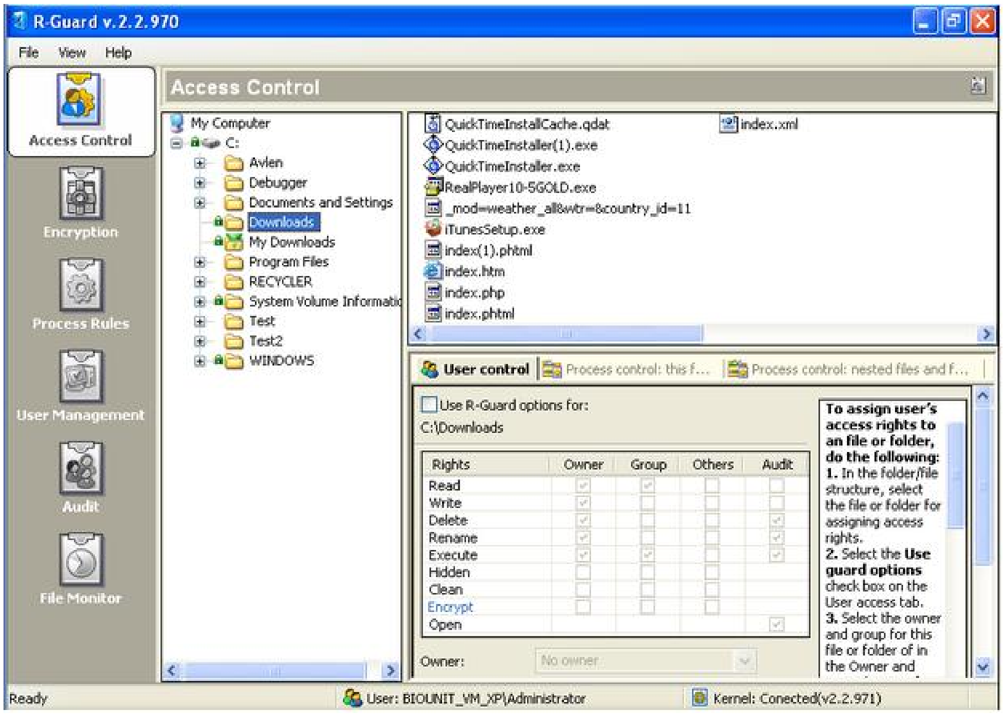
- The left pane displays the disk folders tree.
- The top right pane displays the content of a selected folder, in which there may be files or subfolders.

The contents of the bottom right pane depends on the type of the object selected on the top right pane (file or folder):
If a file is selected, the bottom right pane will contain two panels: User control and Process control: this file.
If a folder is selected, the bottom right pane will contain three panels: User control, Process control: this folder and Process control: nested files and folders.
If a global resource is selected (for example, **My Computer**), the bottom right pane will contain only one panel: Process control: nested files and folders.

You may set the access rights and process rules to folders/files on the **Access Control** panel. This panel contains:

- The left pane with the ***Folder/File structure*** of your computer;
- The right pane with two ***tabs***: ***User Control*** and ***Process control***.

**Access Control Panel**



□ Use R-Guard options for:
C:\Downloads

| Rights | Owner | Group | Others | Audit |
|---|---|---|---|---|
| Read | ☑ | ☑ | □ | □ |
| Write | ☑ | □ | □ | □ |
| Delete | ☑ | □ | □ | ☑ |
| Rename | ☑ | □ | □ | ☑ |
| Execute | ☑ | ☑ | □ | ☑ |
| Hidden | □ | □ | □ | |
| Clean | □ | □ | □ | |
| Encrypt | □ | □ | □ | |
| Open | | | | ☑ |

Owner: No owner

**To assign user's access rights to an file or folder, do the following:**
**1.** In the folder/file structure, select the file or folder for assigning access rights.
**2.** Select the **Use guard options** check box on the User access tab.
**3.** Select the owner and group for this file or folder of in the Owner and

User: BIOUNIT_VM_XP\Administrator
Kernel: Conected(v2.2.971)

You can do the following operations on this panel:

- Assign user access rights;
- Assign process rules.

## 4.1 Assigning User Access Rights

When the User Control panel is selected in the bottom right panel (both for a file and a folder), the information appears, allowing you to control the access of users and groups of users to this file or folder. The access rights control to a folder is the control of access to all files and subfolders of this folder.

Access rights to a file or a folder can be assigned individually for a user (owner), individually for a group of users, and for all other users. The main features of access rights control to files and folders of the system:

- If a user does not have individual access rights to a file or a folder or the user is not a member of a group (or there are no individual access rights for a group, to which the user belongs), that user has the access rights to a file or a folder as all other users;
- If a user does not have individual access rights to a file or a folder, but the user is a member of the group with the individual access rights to a file or a folder, this user has the same access rights as the group he belongs to.
- A user has individual access rights to a file or a folder if such rights have been specifically assigned to him or her.
- If a user has the Supervisor status he or she has the individual access rights to a file or a folder whether or not such rights have been specifically assigned to him or her (or he or she is a member of a group with individual access rights). This feature is not applied to transparent file encryption.
- If a user has no access rights specifically assigned by **R-Guard**, he or she has the default access rights assigned at creation of this user.
- When the **Use R-Guard options for** option is selected, the **Others** and **Audit** columns become

available in the **Rights** table. That means that the user has the access rights of other users right away.

- For network resources, access rights may be assigned only for their usage on this computer (for example, access rights can be assigned to files and folders of a network folder). **R-Guard** access rights, assigned to the files and folders of the local computer remotely, do not function.

**To assign user access rights to a file or a folder, do the following:**

1. In the folder/file structure, select the object (file or folder) for which access rights are to be assigned.
2. Select the **Use R-Guard options for** option on the **User control** tab. The full path to the file or folder, to which access rights are being assigned, is displayed under the **Use R-Guard options for** option.
3. Select the owner and group for this file or folder in the **Owner** and **Group** boxes. If you select **No owner** or **No group**, the **Owner** or **Group** columns in the **Rights** table will become unavailable.

**Note:** The **Owner** of the file or folder does not necessarily belong to the **Group**.

4. You can change the default access rights and assign new ones according to your requirements.

***Access rights*** **-** permissions of a user to do certain actions with a file, folder,etc. There are the following access rights in **R-Guard**:

- **Read**: a permission to view files or folders. If the **Audit** option is selected, the **Read** operation will be registered as a separate Event Log record;
- **Write**: a permission to edit files or folders. If the **Audit** option is selected, the **Write** operation will be registered as a separate Event Log record;
- **Delete**: a permission to delete files or folders from the system. If the **Audit** option is selected, the **Delete** operation will be registered as a separate Event Log record. **Note**: after deletion the access rights to the file or folder are saved and will be applied for the restored file or folder or for a created file or folder with the same name;
- **Rename**: a permission to give other names to files or folders. If the **Audit** option is selected, the **Rename** operation will be registered as a separate Event Log record. Note: after renaming the access rights to the file or folder are saved;
- **Execute**: a permission to execute, perform commands and files. If the **Audit** option is selected, the **Execute** operation will be registered as a separate Event Log record;
- **Open**: a permission to open files or folders (not assigned for the **Owner**, **Group**, and **Other** users as it is part of other operations: read, rename, etc; used for Audit only if it is important to register this operation as a separate Event Log record).

There are also three rights that are ***states*** of files or folders assigned for the user rather than rights to perform actions with files or folders:

- **Hidden**: invisible files or folders;
- **Clean**: the files or folders will be wiped if the user deletes them;
- **Encrypt**: all users or groups have their own private keys, which they use to encrypt files or folders. Transparent encryption may be assigned for a user, for a group of users, or for other users (all **R-Guard** users will have access to a file or folder). When the **Encrypted** state is assigned, files or folders are encrypted with the user/group key transparently and invisibly for other users. Therefore the Read, Write, and Execute options will be unavailable for other users.

The access rights can be assigned for the following users:

**Owner**: is selected in the **Owner** option (see 3);
**Group**: is selected in the **Group** option (see 3);
**Others**: are the other users not belonging to the selected owner or group;
**Audit**: all actions with the files or folders will be listed on the **Audit** panel regardless of the default audit settings for the user.

5. You can assign additional properties for the file or folder using the following options on the **User**

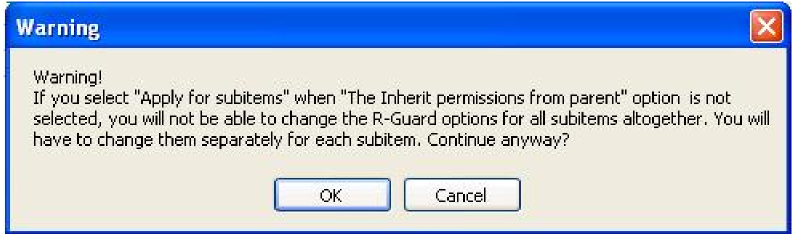
**Access** tab:

**Inherit permissions from parent**: when this option is selected, the file or folder access rights are copied from the parent folder. Effective only if the file or folder parent folder has the **Apply for subitems** option selected and its **R-Guard** options have been changed.
**CRC**: when this option is selected, the system records the original attributes of the file or folder and notifies the user whether or not the file or folder has been modified. You will see the **Status: OK** message if the file or folder properties have not been changed. Otherwise access to the file or folder will be blocked.
**Apply for sub items** (available for folders only): when this option is selected, all access rights assigned for a folder, automatically are applied to all its subfolders and their content which have the **Inherit permissions from parent** option selected. **R-Guard** treats the files or folders with the clear **R-Guard options** option as if they have the **Inherit permissions from parent** option selected.
The **Apply for subitems** check box peculiarities:

After you clicked the **Apply** button this check box (**Apply for subitems**) becomes disabled. It is enabled only when there are any modifications in the user/group of users/other users access rights. If the **Apply for subitems** check box is selected, the modified access rights will be assigned to the files and folders of this folder. If the **Apply for subitems** check box is cleared, the modified access rights will not be assigned for the files ond folders of this folder.

If access control is disabled (the **Use R-Guard options for** check box is cleared), the **Apply for subitems** check box will be enabled. If this check box is left after the **Use R-Guard options for** check box has been cleared, access control will be also cancelled for the files and folders of this folder. If this check box is cleared after the **Use R-Guard options for** check box has been cleared, access control will be disabled for this folder only, and not for the files and folders of this folder.

If the **Apply for subitems** check box is selected for a folder, and the **Inherit permissions from parent** check box is cleared, for all files and folders there will not have the same access rights, and a warning message appears.



Warning!
If you select "Apply for subitems" when "The Inherit permissions from parent" option is not selected, you will not be able to change the R-Guard options for all subitems altogether. You will have to change them separately for each subitem. Continue anyway?

6. Click **Apply** to save the changes. (If you want to assign process rules for the file or folder, go to the Process Rules tab). The file or folder will have a blue lock sign (🔒), showing that certain access rights have been assigned for it.

To cancel all access rights for this user, clear the **Use R-Guard options** option and click **Apply.**

## 4.2 Assigning Process Rules

**You can assign various process rules to an object, including:**

- Folders;
- Files.

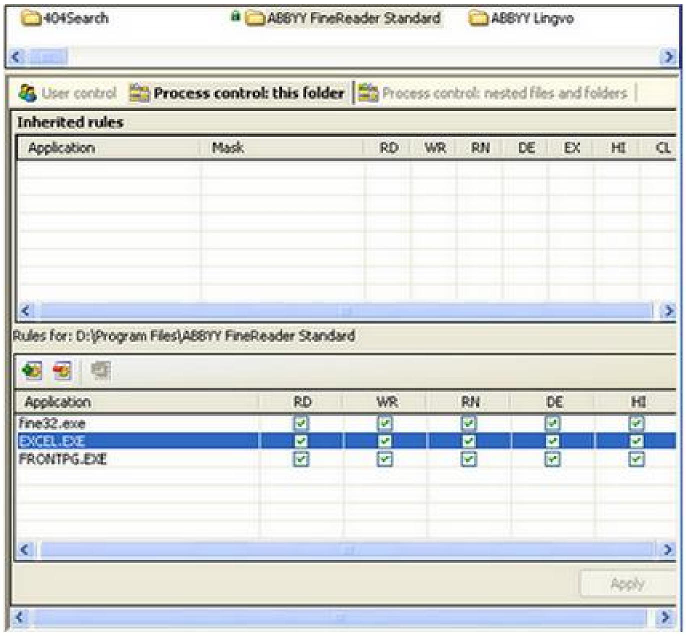
### 4.2.1 Assigning Proces Rules for Folders

**To assign process rules to a folder, do the following:**

1. Go to the **Process control tabs**.
2. Select the required folder in the file structure of your computer for which you are going to assign

process rules.

**Folder Process Rules**



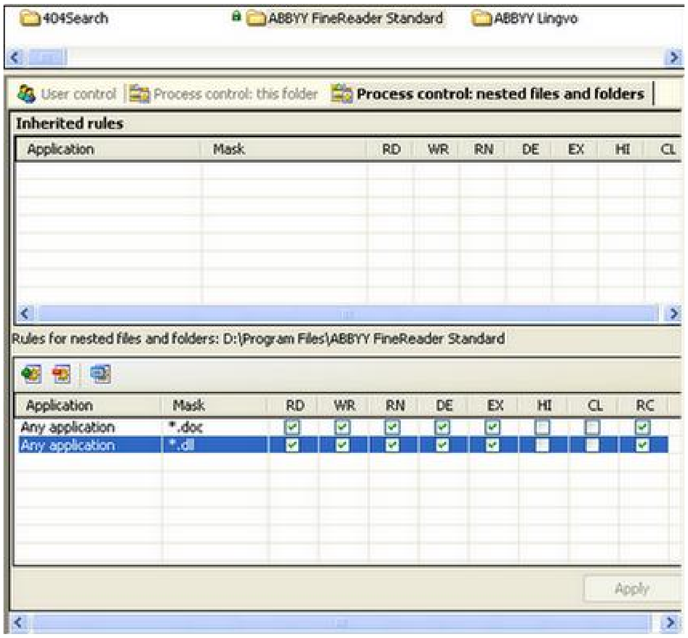
404Search
ABBYY FineReader Standard
ABBYY Lingvo
User control
Process control: this folder
Process control: nested files and folders
Inherited rules

| Application | Mask | RD | WR | RN | DE | EX | HI | CL |
|---|---|---|---|---|---|---|---|---|

Rules for: D:\Program Files\ABBYY FineReader Standard

| Application | RD | WR | RN | DE | HI |
|---|---|---|---|---|---|
| Fine32.exe | ☑ | ☑ | ☑ | ☑ | ☑ |
| EXCEL.EXE | ☑ | ☑ | ☑ | ☑ | ☑ |
| FRONTPG.EXE | ☑ | ☑ | ☑ | ☑ | ☑ |

**Process Rules for Nested Files and Folders**



404Search
ABBYY FineReader Standard
ABBYY Lingvo
User control
Process control: this folder
Process control: nested files and folders
Inherited rules

| Application | Mask | RD | WR | RN | DE | EX | HI | CL |
|---|---|---|---|---|---|---|---|---|

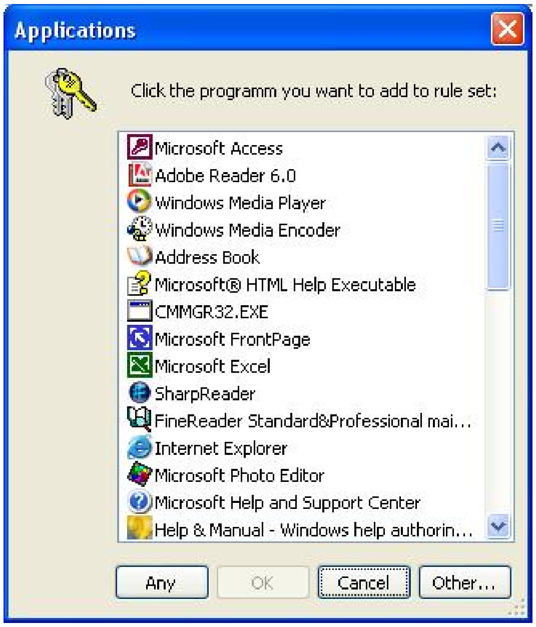
Rules for nested files and folders: D:\Program Files\ABBYY FineReader Standard

| Application | Mask | RD | WR | RN | DE | EX | HI | CL | RC |
|---|---|---|---|---|---|---|---|---|---|
| Any application | *.doc | ☑ | ☑ | ☑ | ☑ | ☑ | □ | □ | ☑ |
| Any application | *.dll | ☑ | ☑ | ☑ | ☑ | ☑ | □ | □ | ☑ |

**To assign process rules for folders**:

1. Go to the **Process control: this folder** tab. In the lower part of the tab press **Add rule** (). Define the new rule properties.

**New rule properties**



Click the programm you want to add to rule set:

2. Select the application for the process rule and click **OK**. Or click **Any** if the rule is assigned for all applications installed on your computer. Or click **Other** and choose the executable file of the application installed on your computer.
3. Select the required rules in the rule set. You cannot assign the **Clean** or **Execute** access rights because they are disabled for a folder.
4. Click **Apply** to save the changes you have made. The file or folder will have a green lock sign, showing that certain process rules have been assigned for it. If the folder has both user and process control assigned for it, the lock sign will be black.

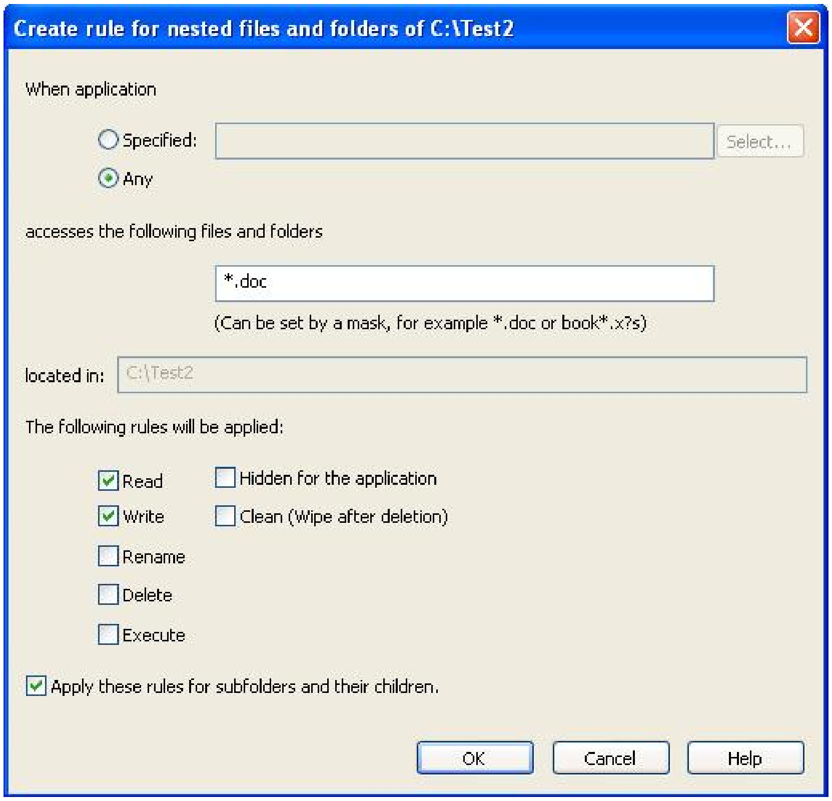
   You can delete any access rule by clicking the **Remove** button () or by selecting the **Remove rule** command from the context menu or by pressing the **<Delete>** button on the keyboard.
   You can also assign access rules for a folder by drag-and-dropping a folder to the **Rules for:...** section of this tab.
   You can modify the assigned access rule by selecting or deselecting the options in the **Rules for** field. Then click **Apply** to save the changes you have made.

The content of the inherited rule for files of this folder are displayed in the top right **Inherited rules** section of the tab. You cannot delete or modify this rule.

**To assign process rules for folders using masks**:

1. Go to the **Process control: nested files and folders** tab. In the lower part of the tab press **Add rule** (). Define the new rule properties. Assign process rules for the following subjects:

**New rule properties**



Create rule for nested files and folders of C:\Test2

When application

○ Specified:

● Any

accesses the following files and folders

*.doc

(Can be set by a mask, for example *.doc or book*.x?s)

located in: C:\Test2

The following rules will be applied:

☑ Read

☑ Write

☐ Rename

☐ Delete

☐ Execute

☐ Hidden for the application

☐ Clean (Wipe after deletion)

☑ Apply these rules for subfolders and their children.

**Any application:** click **Any** if you are defining rules to this file or folder for all applications installed on your computer.

**A specific application**: click **Specified** to add a certain application. Click the **Select** button and select a subject (application), for which you want to add a new rule, from the file structure of your computer. Note: be sure that you select the application you wanted to. Otherwise click **Other** and select the executable file of application installed on your computer. For instance, there are two applications `notepad.exe` in installed Windows XP, one in the `Windows` folder and another in the `System32` folder.

2. In the **accesses the following files and folders** field enter the path or a mask for the file or folder. For example, `*.doc`. The created access rule will be a personal rule for the files of this folder. If this rule affects the subfolders of this folder, the files of the subfolders will have this rule as an inherited rule. If a file of this folder is specified, a message will be displayed saying that the access rule will be created individually for this file. If the file does not exist, this rule will be created for it when it is created.

   In the field **located in** the full path to a folder is specified.

3. Select the required rules in the **the following rules will be applicable** section.

4. Click **Apply these rules for subfolders and their children** if you want this process rule to be inherited by subfolders and their files. They will have this rule as an inherited rule, and it will be impossible to modify it.

5. Click **OK**. Click **Help** to receive help on how to add a new rule. ***Note*** that a file or a folder deleted into **Recycle Bin** is renamed rather than actually deleted permanently. Therefore, the operation of deleting into the **Recycle Bin** will be registered as a renaming operation.
6. Click **Apply** to save the changes you have made. The file or folder will have a lock sign (🔒) showing that certain process rules have been assigned for it. If the folder has both user and process control assigned for it, the lock sign will be black.

You can delete any access rule by clicking the **Remove** button () or by selecting the **Remove rule** command from the context menu or by pressing the **<Delete>** button on the keyboard. Then click **Apply** to save it.

You can view or modify the details of the rule by clicking the **Details** () button or by selecting the **Details** command from the context menu. Then click **Apply** to save it.
The contents of the inherited rule for files of this folder are displayed in the upper part of the tab (**Inherited rules** section). You cannot delete or modify this rule.

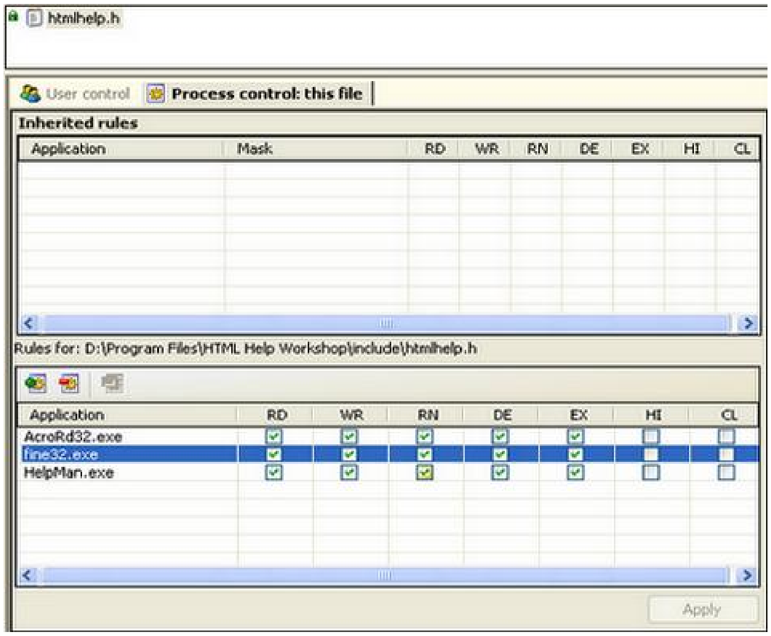
You can also assign access rules for a folder by drag-and-dropping a folder to the **Rules for nested files and folders** section of this tab.
You can view the following information for any rule in **Rules for nested files and folders** and **Inherited rules** sections:
1) in column **Application**: the application whose access to file or folder is controlled by the rule (only executable file of the application, to view the full path to this application, see hint);
2) in column **Mask**: a mask of files which are controlled by the rule;
A file mask can be assigned by special symbols: wildcard parameters:
"*" is a set of any number of any symbols (including no symbols at all).
For example, t*y is the name of two or more symbols, starting with "t" and ending with "y"; a* is the name of one or more symbols, starting with "a".
"?" is any single symbol (must be at least one symbol).
For example, "??" is the name of any two symbols; "?h" is the name of two symbols, the first of which can be any symbol, the second one must be "h"; "*?" is the name of any number of symbols (at least one); "n*?" is the name of any number of symbols (at least two symbols), the first one of which is n.
3) in columns **RD, WR, RN, DE, EX, HI**: access rules (rights) to file or folder;
4) in column **RC**: if the rule is inherited by folder's subfolders and their files (only for inherited rules).

### 4.2.2 Assigning Proces Rules for Files

**To assign process rules to an object, do the following:**

1. Go to the **Process control** tab.
2. Select the required file in the file structure of your computer, for which you are going to assign process rules.

**File Process Rules**



htmlhelp.h

Inherited rules

| Application | Mask | RD | WR | RN | DE | EX | HI | CL |
|---|---|---|---|---|---|---|---|---|

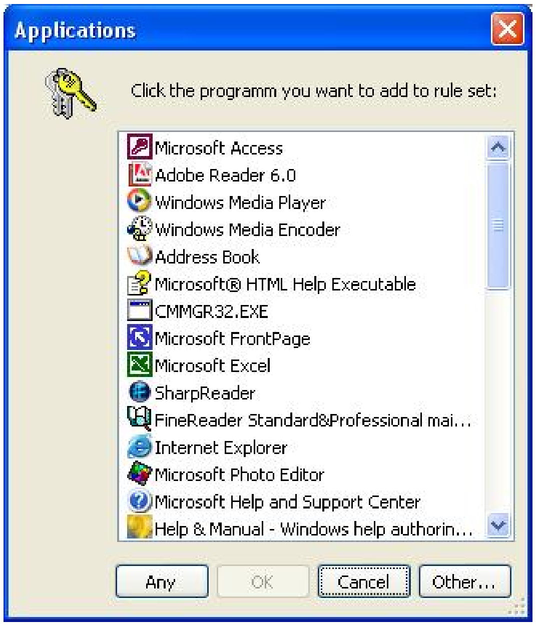
Rules for: D:\Program Files\HTML Help Workshop\include\htmlhelp.h

| Application | RD | WR | RN | DE | EX | HI | CL |
|---|---|---|---|---|---|---|---|
| AcroRd32.exe | ☑ | ☑ | ☑ | ☑ | ☑ | □ | □ |
| fine32.exe | ☑ | ☑ | ☑ | ☑ | ☑ | □ | □ |
| HelpMan.exe | ☑ | ☑ | ☑ | ☑ | ☑ | □ | □ |

**To assign process rules for files**:

1. Click **Add rule** () in the lower part of the tab. Define the new rule properties.

**New rule properties**



Applications

Click the programm you want to add to rule set:

- Microsoft Access
- Adobe Reader 6.0
- Windows Media Player
- Windows Media Encoder
- Address Book
- Microsoft® HTML Help Executable
- CMMGR32.EXE
- Microsoft FrontPage
- Microsoft Excel
- SharpReader
- FineReader Standard&Professional mai...
- Internet Explorer
- Microsoft Photo Editor
- Microsoft Help and Support Center
- Help & Manual - Windows help authorin...

2. Select the application for the process rule and click **OK**. Or click **Any** if the rule is assigned for all applications installed on your computer. Or click **Other** and select the executable file of the application installed on your computer.

3. Select the required rules in the rule set.

4. Click **Apply** to save the changes you have made. The file will have a green lock sign (🔒) showing that certain process rules have been assigned for it. If the file has both user and process control,

the lock will be black. You can later modify the assigned access rights.

You can delete any access rule by clicking the **Remove** button () or by selecting the **Remove rule** command from the context menu or by pressing the **<Delete>** button on the keyboard.

You can also create an access rule for a file by drag-and-dropping the icon or the shortcut of the file into the **Rules for:...** section of this tab.
You can modify the assigned access rule by selecting or deselecting the options in the **Rules for** field. Then click **Apply** to save the changes you have made.

The contents of the inherited rule for files in the same folder are shown in the top right **Inherited rules** section of the tab. You cannot delete or modify this rule.

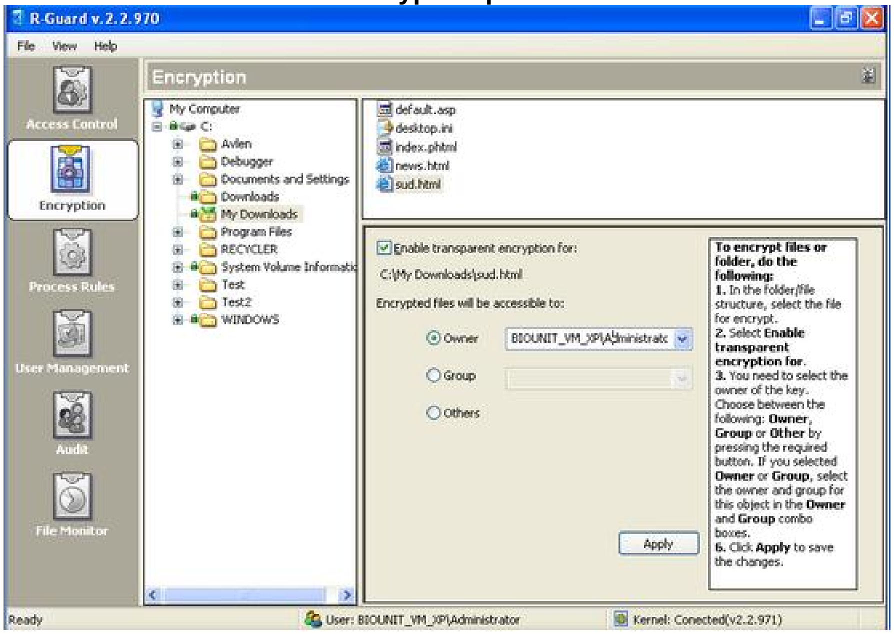
# 5 Encryption Panel

Click the **Encryption** button on the left menu to encrypt files and specify users that will be able to access these files on the **Encryption** panel. The encryption function is also available on the **Access Control** right panel.

This panel contains:

- The left pane with the ***Folder/File structure*** of your computer;
- The right pane with two tabs: the upper one with the **contents (files or sub folders) of the selected folder** and the lower one with the **information about transparent encryption of the selected file or folder**.

**Encryption panel**



☑ Enable transparent encryption for:

C:\My Downloads\sud.html

Encrypted files will be accessible to:

● Owner BIOUNIT_VM_XP\Administratc

○ Group

○ Others

**To encrypt files or folder, do the following:**
**1.** In the folder/file structure, select the file for encrypt.
**2.** Select **Enable transparent encryption for**.
**3.** You need to select the owner of the key. Choose between the following: **Owner**, **Group** or **Other** by pressing the required button. If you selected **Owner** or **Group**, select the owner and group for this object in the **Owner** and **Group** combo boxes.
**6.** Click **Apply** to save the changes.

User: BIOUNIT_VM_XP\Administrator

Kernel: Conected(v2.2.971)

**R-Guard** encrypts files transparently. So the user can work with the file that he or she has encrypted just like with a unencrypted file. Other users, when trying to access the encrypted file, cannot reach it and receive a warning message about an access error.

**R-Guard** transparent encryption is a vital necessity because:

- your computer may be stolen. Without encryption all confidential information is vulnerable to unauthorised access.

- your computer may be left operating unattended. Without encryption any user can access confidential information on this computer. A domain user can also access network information from this computer.
- if the non-transparent encryption is used, user has to decrypt the file before using and then to encrypt it again. This is a very time-consuming and tiresome process. The user may also forget to encrypt the file, which makes this information unprotected.
- if non-transparent encryption is used, information may be accessed from temporary files and files created by various applications during documents editing.
- if the non-transparent encryption is used, it is necessary to remember a password to encrypt or decrypt a file. If the password is lost, information cannot be recovered (as most products for information encryption do not provide ways of lost password recovery). This is an additional reason why the user may avoid encrypting information.

You can do the following operations on this panel:

- Encrypt files and select owner.

## 5.1 Selecting an Owner and Group for Encrypted Files

**To encrypt a file or folder, do the following:**

1. Select the object (a file or folder) to encrypt in the folder/file structure.
2. Select the **Enable transparent encryption for** option. The path to the file or folder to encrypt is displayed under this option.
3. The **R-Guard** transparent encryption can be set individually for a user, for a group of users, or for other users. If a file or folder is encrypted for a user, no one except this user can access this file or folder for reading or writing, as it is encrypted with the user`s private key. If a file or a folder is encrypted for a group of users, no one except the members of this group can access this file or folder for reading or writing, as it is encrypted with the group`s private key. If a file or a folder is encrypted for other users, all **R-Guard** users can access this file or folder, as it is encrypted with the common key generated at installation. Select the **Owner**, **Group**, or **Other** option. Select the user or group of users that will have access to the encrypted file.
4. Click **Apply**. A sign of blue lock appears near the file after encryption.

**To disable transparent encryption of a file or folder, do the following:**

1. Clear the **Enable transparent encryption for** option.
2. Click **Apply**.

Or clear the **Encrypt** option for a user/group of users/other users on the User Control tab.

The sign of blue lock near the file remains there even after the encryption has been disabled. This is necessary because the encryption function is also available on the **Access Control** panel, and after setting the transparent encryption some access rights for this file may be changed.

The lower right part of the **Encryption** panel contains a brief description of the actions for encryption of a file or a folder.

# 6 Process Rules Panel

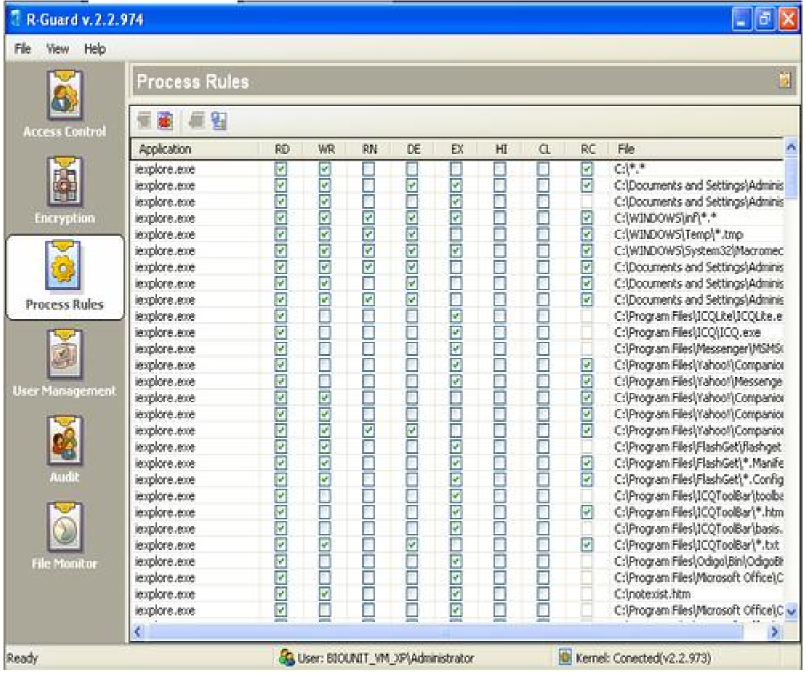
Click the **Process Rules** button on the left menu to specify process rules for subjects and objects on this panel. This panel contains:

- A ***Toolbar*** with buttons;

| **Buttons** | **Click it to:** |
|---|---|
| | Save the process rule set. |
| | Remove the selected rule. |
| | Remove all rules. |

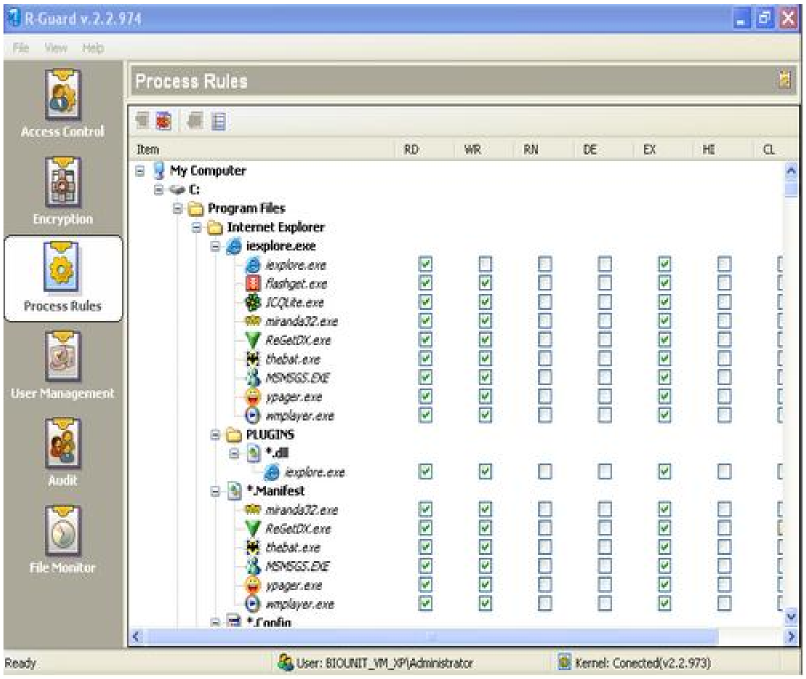
- A ***table*** or a ***tree*** with all process rules assigned to various applications on the **Process Rules** tab of the **Access Control** panel. To switch between the two ways of presenting the process rules, use the or buttons.

**Process Rules panel**



| Application | RD | WR | RN | DE | EX | HI | CL | RC | File |
|---|---|---|---|---|---|---|---|---|---|
| iexplore.exe | ☑ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | C:\*.* |
| iexplore.exe | ☑ | ☑ | ☐ | ☑ | ☑ | ☐ | ☐ | ☑ | C:\Documents and Settings\Adminis |
| iexplore.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ | | C:\Documents and Settings\Adminis |
| iexplore.exe | ☑ | ☑ | ☑ | ☑ | ☑ | ☐ | ☐ | ☑ | C:\WINDOWS\inf\*.* |
| iexplore.exe | ☑ | ☑ | ☑ | ☑ | ☐ | ☐ | ☐ | ☑ | C:\WINDOWS\Temp\*.tmp |
| iexplore.exe | ☑ | ☑ | ☑ | ☑ | ☑ | ☐ | ☐ | ☑ | C:\WINDOWS\System32\Macromec |
| iexplore.exe | ☑ | ☑ | ☑ | ☑ | ☐ | ☐ | ☐ | ☑ | C:\Documents and Settings\Adminis |
| iexplore.exe | ☑ | ☑ | ☐ | ☑ | ☐ | ☐ | ☐ | ☑ | C:\Documents and Settings\Adminis |
| iexplore.exe | ☑ | ☑ | ☑ | ☑ | ☐ | ☐ | ☐ | ☑ | C:\Documents and Settings\Adminis |
| iexplore.exe | ☑ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | | C:\Program Files\ICQLite\ICQLite.e |
| iexplore.exe | ☑ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | | C:\Program Files\ICQ\ICQ.exe |
| iexplore.exe | ☑ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | | C:\Program Files\Messenger\MSMS( |
| iexplore.exe | ☑ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☑ | C:\Program Files\Yahoo!\Companio |
| iexplore.exe | ☑ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☑ | C:\Program Files\Yahoo!\Messenge |
| iexplore.exe | ☑ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | C:\Program Files\Yahoo!\Companio |
| iexplore.exe | ☑ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | C:\Program Files\Yahoo!\Companio |
| iexplore.exe | ☑ | ☑ | ☑ | ☑ | ☐ | ☐ | ☐ | ☑ | C:\Program Files\Yahoo!\Companio |
| iexplore.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ | | C:\Program Files\FlashGet\flashget |
| iexplore.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ | ☑ | C:\Program Files\FlashGet\*.Manife |
| iexplore.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ | ☑ | C:\Program Files\FlashGet\*.Config |
| iexplore.exe | ☑ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | | C:\Program Files\ICQToolBar\toolba |
| iexplore.exe | ☑ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☑ | C:\Program Files\ICQToolBar\*.htm |
| iexplore.exe | ☑ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | | C:\Program Files\ICQToolBar\basis. |
| iexplore.exe | ☑ | ☑ | ☐ | ☑ | ☐ | ☐ | ☐ | ☑ | C:\Program Files\ICQToolBar\*.txt |
| iexplore.exe | ☑ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | | C:\Program Files\Odigo\Bin\OdigoB |
| iexplore.exe | ☑ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | | C:\Program Files\Microsoft Office\C |
| iexplore.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ | | C:\notexist.htm |
| iexplore.exe | ☑ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | | C:\Program Files\Microsoft Office\C |

Ready User: BIOUNIT_VM_XP\Administrator Kernel: Conected(v2.2.973)



| Item | RD | WR | RN | DE | EX | HI | CL |
|---|---|---|---|---|---|---|---|
| My Computer | | | | | | | |
| C: | | | | | | | |
| Program Files | | | | | | | |
| Internet Explorer | | | | | | | |
| iexplore.exe | | | | | | | |
| iexplore.exe | ☑ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ |
| flashget.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| ICQLite.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| miranda32.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| ReGetDX.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| thebat.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| MSMSGS.EXE | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| ypager.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| wmplayer.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| PLUGINS | | | | | | | |
| *.dll | | | | | | | |
| iexplore.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| *.Manifest | | | | | | | |
| miranda32.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| ReGetDX.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| thebat.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| MSMSGS.EXE | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| ypager.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| wmplayer.exe | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| *.Config | | | | | | | |

Ready User: BIOUNIT_VM_XP\Administrator Kernel: Conected(v2.2.973)

For the convenience of **R-Guard** users it contains default process rules created for the most used applications to files and folders. These process rules allow the user to prevent questionable operations (for example, writing onto system folders). These process rules are loaded automatically at the first start of **R-Guard** and click the **Process Rules** button on the left menu. You can load them yourself by selecting **Load process rules presets** in the **R-Guard File menu**.
You can do the following operations on this panel:

- View existing rules;
- Edit existing rules;
- Save the rule set;
- Remove a rule;
- Change the order of rules;
- Remove all rules.

## 6.1 Viewing Existing Rules

You can view the existing process rules on the **Rules** list. The table (or tree) contains the following columns:

- **Application**: contains the application for which the rules (the access rights to the files or folders) are assigned.
- **Rules**: contains the set of rules assigned to a subject. For rules controlling access of applications to a folder the columns **EX** and **CL** are not used and appear disabled.
- **RC**: contains information about whether this rule is applied to the subfolders of the selected folder. This column is disabled for rules controlling access of applications to one folder or one file.
- **File**: contains a full path to the file or folder to which rules are assigned for this application. It can be a path to a certain file, a folder or several files defined by a mask.

## 6.2 Editing Existing Rules

**To edit the existing rules, do the following:**

1. Select a required rule in the **Rules** table.
2. Make the necessary changes in the rule set.
3. Click the **Save** button.

## 6.3 Saving Rule Set

**To save the rule set, do the following:**

Click the **Save** button.

## 6.4 Removing Rule

**To remove a rule from the rule set, do the following:**

1. Select a required rule in the **Rules** table.
2. Click the **Remove** button. A confirmation message will appear. Click **Yes** to continue. (OR: Right-

click the required rule and select **Remove rule** from the menu, or press the **<Delete>** button on the keyboard).
You cannot create a new rule in the **Process Rules** section.

## 6.5 Changing the order of rules

You can change the order of process rules on the tree by drag-and-dropping them. Select the file (or the mask of files) and drag it up and drop. Note: you can change the order of process rules only for files (or masks of files) located in one folder.

## 6.6 Removing all rules

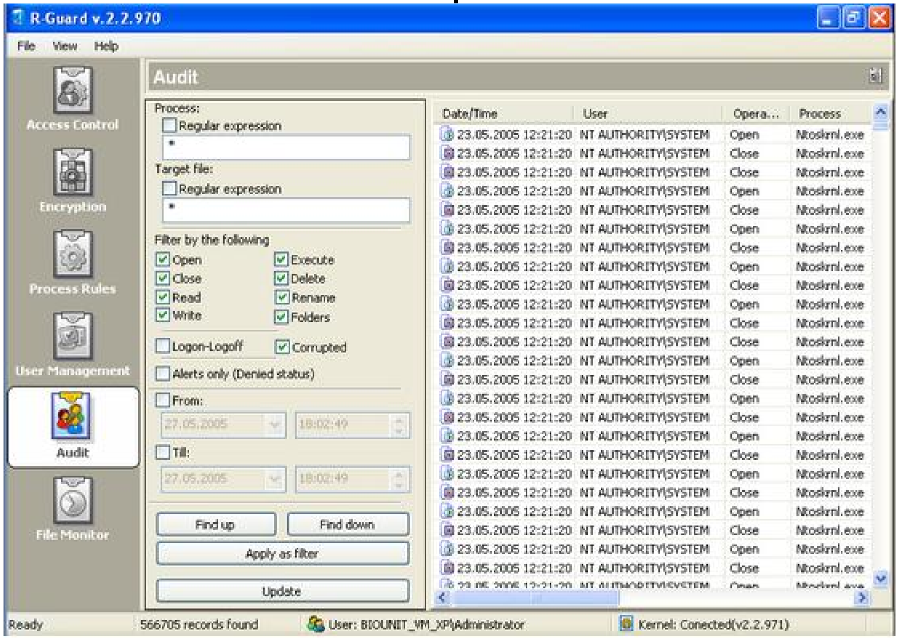
Click the **Remove all rules button**. All rules will be removed.

# 7 Audit Panel

Press **Audit** on the left menu to view the Audit panel. You may view all audit events and audit filter settings on this panel. Audit of the operational system (OS) is a process allowing the user to register all security events in the OS. For example, logon to the system or attempting to create a file or folder, accessing or deleting it, etc. If there are no **R-Guard** access rules assigned for a file or folder, the information about operations with this file or folder will be registered in the Audit according to the default Audit settings (More detail about the access rights). If there are **R-Guard** access rules set for a file or folder, the information about operations with this file or folder will be registered in the Audit according to the Audit settings (More detail about the access rights).
This panel contains:

- The ***Filter options*** pane for configuring filter options;
- An **Operations/Processes** table with operations, processes, comments, users, status, and date/time of performing these operations .

**Audit panel**



Process:
□ Regular expression
*

Target file:
□ Regular expression
*

Filter by the following
☑ Open ☑ Execute
☑ Close ☑ Delete
☑ Read ☑ Rename
☑ Write ☑ Folders
□ Logon-Logoff ☑ Corrupted
□ Alerts only (Denied status)
□ From: 27.05.2005 18:02:49
□ Till: 27.05.2005 18:02:49

| Date/Time | User | Opera... | Process |
|---|---|---|---|
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Open | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Close | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Close | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Open | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Close | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Open | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Close | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Open | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Close | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Open | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Close | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Close | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Open | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Close | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Open | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Close | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Open | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Close | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Open | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Close | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Open | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Close | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Open | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Close | Ntoskrnl.exe |
| 23.05.2005 12:21:20 | NT AUTHORITY\SYSTEM | Open | Ntoskrnl.exe |

Ready 566705 records found User: BIOUNIT_VM_XP\Administrator Kernel: Conected(v2.2.971)

You can do the following operations on this panel:

- View the audit notes;
- Filter the audit notes;

- Search the audit notes up and down the list.

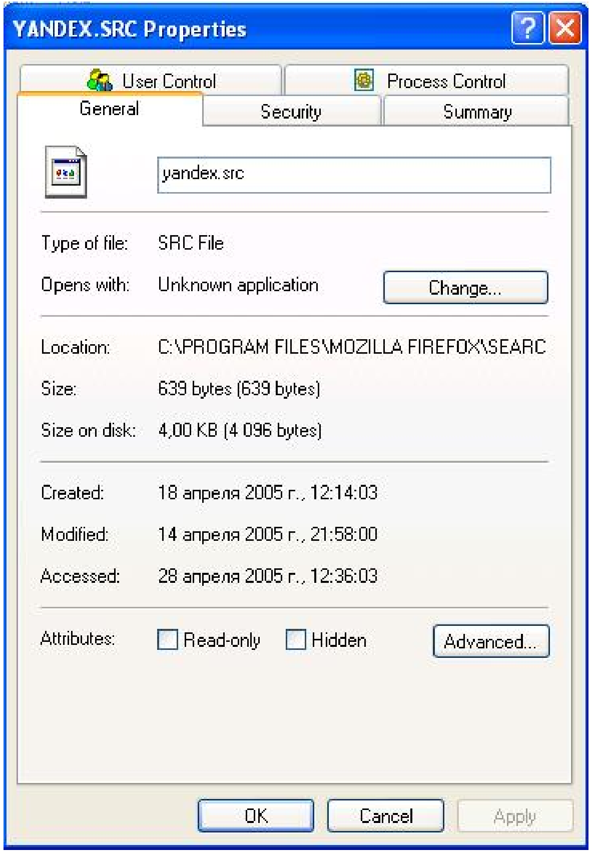
## 7.1 Viewing Audit Notes

You can view the Audit notes on the **Operations/Processes** table. This table contains the following columns, displaying various information for each operation:

- **Date/Time** contains the date and time of performing an operation or a process.
- **User** contains the account name of the user that performed the operation.
- **Operation** contains the name of the operation (Read, Write, etc.).
- **Process** contains the name of the process (the executable file of the operation).
- **Status** contains a note about the result (the status) of the operation. Audit allows you to monitor both successful and unsuccessful attempts of performing some kind of operation. So while viewing the Audit notes, it is possible to find out who attempted to perform a prohibited action. There are three possible results (statuses) of a performed operation: **OK** (The operation is successful), **Error** (The operation failed due to a specified problem. The numeric code of the error is shown here with a short description.) and **Deny** (The access to the operation is denied by **R-Guard**).
- **Comments** contains some details of the operation (the name of the file on which the operation is performed, its size, etc.).

Each Audit note has the following context menu commands:

- ***Show file properties*** opens a properties window of the file or folder affected by the operation.



YANDEX.SRC Properties

yandex.src

Type of file: SRC File

Opens with: Unknown application

Location: C:\PROGRAM FILES\MOZILLA FIREFOX\SEARC

Size: 639 bytes (639 bytes)

Size on disk: 4,00 KB (4 096 bytes)

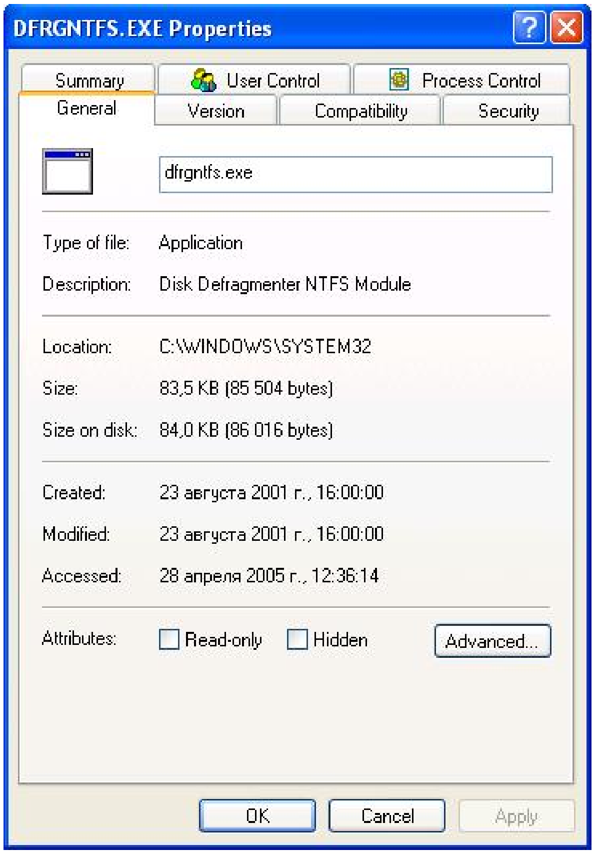
Created: 18 апреля 2005 г., 12:14:03

Modified: 14 апреля 2005 г., 21:58:00

Accessed: 28 апреля 2005 г., 12:36:03

Attributes: □ Read-only □ Hidden

- ***Show process properties*** opens a properties window of the executable operation file - process.



dfrgntfs.exe

Type of file: Application

Description: Disk Defragmenter NTFS Module

Location: C:\WINDOWS\SYSTEM32

Size: 83,5 KB (85 504 bytes)

Size on disk: 84,0 KB (86 016 bytes)

Created: 23 августа 2001 г., 16:00:00

Modified: 23 августа 2001 г., 16:00:00

Accessed: 28 апреля 2005 г., 12:36:14

Attributes: □ Read-only □ Hidden

- ***Create process rule*** opens the window of assigning access rules to a file or folder.

## 7.2 Using Filter

**To filter the list of operations, do the following:**

1. Define the filter parameters for processes and object files on the **Filter options** pane. You can filter the Audit notes by:

- The name of the executable operation file - process. You can select this filter option by using the:
  - wildcard parameters. Clear the **Regular expression** option and type a mask in the field provided (for example, "*.doc").

    A file mask can be assigned by special symbols: wildcard parameters:

    "*" is a set of any number of any symbols (including no symbols at all).

    For example, t*y is the name of two or more symbols, starting with "t" and ending with "y"; a* is the name of one or more symbols, starting with "a".

    "?" is any single symbol (must be at least one symbol).

    For example, "??" is the name of any two symbols; "?h" is the name of two symbols, the first of which can be any symbol, the second one must be "h"; "*?" is the name of any number of symbols (at least one); "n*?" is the name of any number of symbols (at least two symbols), the first one of which is n.
  - Or you can use a regular expression. Select the **Regular expression** option and type the regular expression in the field.

- The name of the file or folder affected by the performed operation - target file. You can select this filter option by using the:
  - wildcard parameters. Clear the **Regular expression** option and type a mask in the field (for example, "*.doc").

- Or you can use a regular expression. Select the **Regular expression** option and type the regular expression in the field provided.

2. In the **Filter by the following** field, select operations (access rights) by which you want to filter Audit. Specify whether you want to view operations with folders (including the operations of checking their existence) by selecting the **Folders** option. Specify if you want to view **Logon-Logoff**, **Corrupted** (for example, in case of abnormal exiting of **R-Guard**) and only with denied status (the access was denied by **R-Guard**) operations.

***Note*** that a file or a folder deleted into **Recycle Bin** is renamed rather than actually deleted permanently. Therefore, the operation of deleting into the **Recycle Bin** will be registered in Audit as a renaming operation.

3. Specify the period of time for which you want to view operations in Audit: select the **From** and **Till** option and specify the periods of time.
4. Click **Apply as filter**. The filter will be applied to all operations until the last Audit update. To apply the filter to operations until the current moment click **Update** to refresh the audit data first and then click **Apply as filter**.

## 7.3 Find Up and Find Down Options

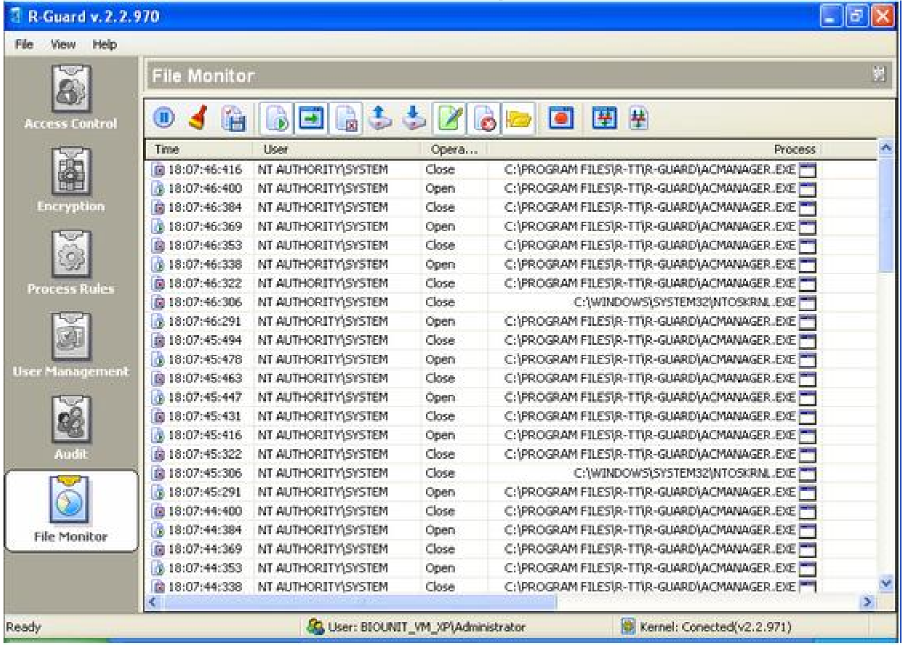
The **Find up** and **Find down** options are useful for selecting Audit notes following or preceding a selected one:

1. Select a required note.
2. Click **Find up** to select a note above the selected one. Or:
3. Click **Find down** to select a note below the selected one.

# 8 File Monitor Panel

Click **File Monitor** on the left menu to view the **File Monitor** panel. You may view audit notes of *current* events on this panel. The maximum number of notes is 1000. This panel contains the **Operations/Processes** table with operations, processes, target, and status of performing these operations. You can filter the notes by the name of operations and by the mask of process/target file.

**File Monitor panel**



| Time | User | Opera... | Process |
|---|---|---|---|
| 18:07:46:416 | NT AUTHORITY\SYSTEM | Close | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:46:400 | NT AUTHORITY\SYSTEM | Open | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:46:384 | NT AUTHORITY\SYSTEM | Close | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:46:369 | NT AUTHORITY\SYSTEM | Open | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:46:353 | NT AUTHORITY\SYSTEM | Close | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:46:338 | NT AUTHORITY\SYSTEM | Open | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:46:322 | NT AUTHORITY\SYSTEM | Close | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:46:306 | NT AUTHORITY\SYSTEM | Close | C:\WINDOWS\SYSTEM32\NTOSKRNL.EXE |
| 18:07:46:291 | NT AUTHORITY\SYSTEM | Open | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:45:494 | NT AUTHORITY\SYSTEM | Close | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:45:478 | NT AUTHORITY\SYSTEM | Open | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:45:463 | NT AUTHORITY\SYSTEM | Close | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:45:447 | NT AUTHORITY\SYSTEM | Open | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:45:431 | NT AUTHORITY\SYSTEM | Close | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:45:416 | NT AUTHORITY\SYSTEM | Open | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:45:322 | NT AUTHORITY\SYSTEM | Close | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:45:306 | NT AUTHORITY\SYSTEM | Close | C:\WINDOWS\SYSTEM32\NTOSKRNL.EXE |
| 18:07:45:291 | NT AUTHORITY\SYSTEM | Open | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:44:400 | NT AUTHORITY\SYSTEM | Close | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:44:384 | NT AUTHORITY\SYSTEM | Open | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:44:369 | NT AUTHORITY\SYSTEM | Close | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:44:353 | NT AUTHORITY\SYSTEM | Open | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |
| 18:07:44:338 | NT AUTHORITY\SYSTEM | Close | C:\PROGRAM FILES\R-TT\R-GUARD\ACMANAGER.EXE |

Ready User: BIOUNIT_VM_XP\Administrator Kernel: Conected(v2.2.971)

You can do the following operations on this panel:

- View the file monitor notes;
- Save the file monitor notes;
- Filter file monitor notes;
- Pause and clear the File Monitor notes.

## 8.1 Viewing File Monitor notes

You can view the **File Monitor** notes on the **Operations/Processes** table. This table contains the following columns:

- **Time**: contains the date and time of performing an operation or a process.
- **User**: contains the account name of the user that performed the operation.
- **Operation**: contains the name of the operation (Read, Write, etc.) which took place at a certain moment of time.
- **Process**: contains the name of the process.
- **Target**: contains the name of the file affected in the operation.
- **Status**: contains a note about the result (the status) of the operation. Audit allows you to monitor both successful and unsuccessful attempts of performing some kind of operation. So while viewing the Audit notes, it is possible to find out who attempted to perform a prohibited action. Three results (statuses) of a performed operation are possible: **OK** (The operation was successful), **Error** (The operation failed due to a specified problem. The error numeric code is shown here with a short description.), and **Deny** (The access to the operation is denied by **R-Guard**).
- **Other**: contains some additional details of the operation (the name of the file affected by the operation, its size, etc.).

## 8.2 Saving File Monitor Notes

**To save the notes of the File Monitor, do the following:**

1. Click the **Save to file** button () on the **File Monitor** toolbar.
2. Select a folder in the system to keep the file and enter the name and type to save the **File Monitor** notes.

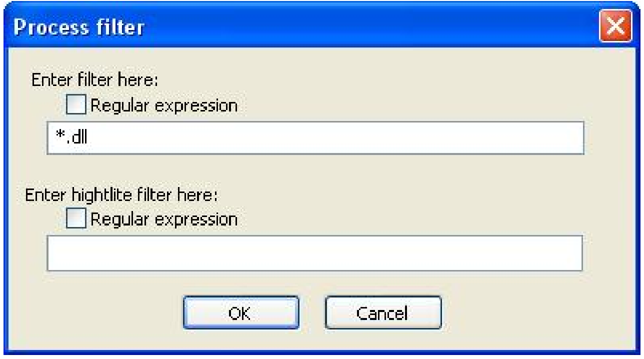
## 8.3 Filtering File Monitor notes

**To filter the list of operations, do the following:**

1. Click the buttons on the **File Monitor** toolbar that correspond to the operations by which you want to filter the notes. ***Note*** that a file or a folder deleted into **Recycle Bin** is renamed rather than actually deleted permanently. Therefore, the operation of deleting into the **Recycle Bin** will be registered in **File Monitor** as a renaming operation.

| Button | Action |
|---|---|
| | Open |
| | Execute |
| | Close |
| | Read |
| | Write |
| | Rename |
| | Delete |
| | Folder actions |

2. To filter the **File Monitor** by the processes, click the **Process Filter** button () on the toolbar. Enter a wildcard parameter in the new window. Clear the **Regular expression** option and type a mask in the **Filter** field (for example, "*.dll"). Or use a regular expression by selecting the **Regular expression** option and entering a regular expression. You can use the **Highlight** filter if you want **R-Guard** to highlight the found notes in the red colour (you can use masks and regular expressions, too).



Process filter

Enter filter here:

□ Regular expression

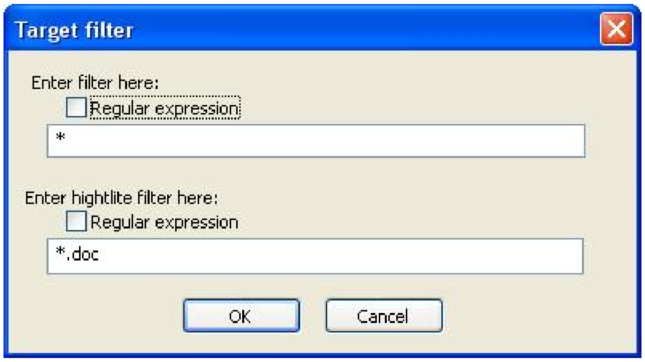
*.dll

Enter hightlite filter here:

□ Regular expression

3. To filter the File Monitor by the files affected by the operation, click the **Target Filter** button () on

the toolbar. Enter a wildcard parameter in the new window. Clear the **Regular expression** option and type a mask in the **Filter** field (for example, "*.doc"). Or use a regular expression by selecting the **Regular expression** option and entering a regular expression. You can use the **Highlight** filter if you want **R-Guard** to highlight the found notes in the red colour (you can use masks and regular expressions too).



Enter filter here:
□ Regular expression
*

Enter hightlite filter here:
□ Regular expression
*.doc

4. To filter the File Monitor by the **Deny** status operation (the access to the operation is denied by **R-Guard**), click the **Deny Status** button ( ) on the toolbar.

## 8.4 Pausing and Clearing File Monitor

**To pause or clear the File Monitor, do the following:**

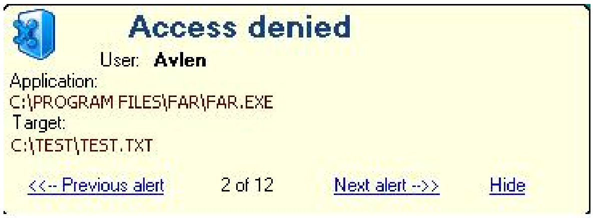
Click the **Pause** button ( ) on the **File Monitor** toolbar to stop the file monitoring. To resume the **File Monitor** activity, click this button again.

Click the **Clear** button ( ) on the File Monitor toolbar to clear all notes from **File Monitor**.

# 9 Alert Monitor

After **R-Guard** installation, a special application, Alert Monitor, starts every time the OS is running. It enables you to visually monitor all moments when **R-Guard** blocks access to objects in the following format: **User name/Process name/File or Folder name**. It also displays all local and network logons/logoffs and current/total alerts. **Previous alert** and **Next alert** buttons allow to display accordingly previous and next alerts. If **Hide** button is selected, this window won't be displayed untill next alert. Maximum size of alerts in this window is 200 entries.

**Alert Monitor**



Access denied
User: Avlen
Application:
C:\PROGRAM FILES\FAR\FAR.EXE
Target:
C:\TEST\TEST.TXT
2 of 12

File Monitor can also work in the **Alert Monitor** mode, but it shows only denial of access. At each event, **File Monitor** produces a special sound. To make File Monitor work in the Alert Monitor mode, it is necessary to run the `monitor.exe` file located in the **R-Guard** installation folder. This file should have the following parameters:

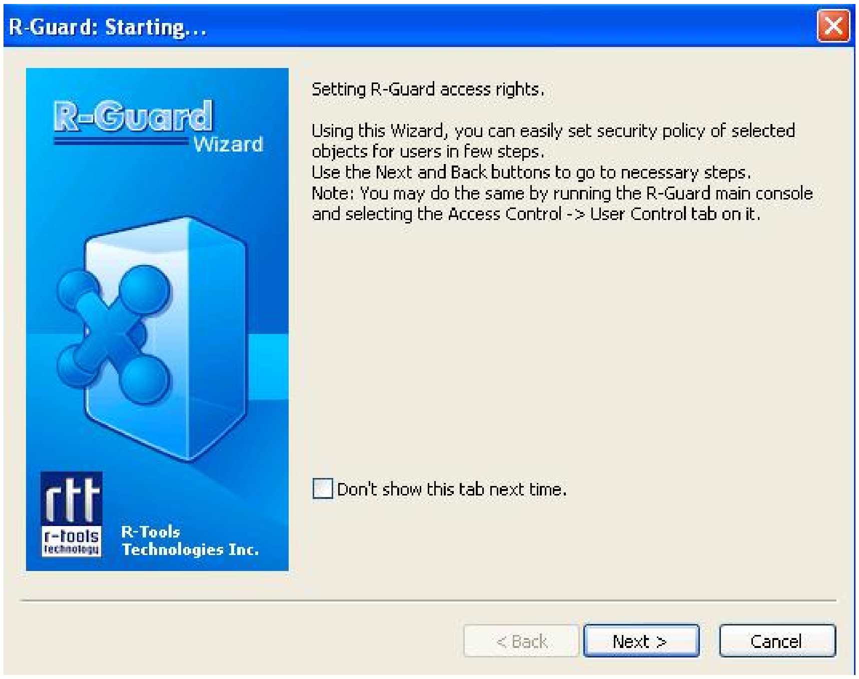
`monitor.exe` options

- `monitor.exe-a` shows that File Monitor is working in the **Alert Monitor** mode;

- `monitor.exe -aoerwcndf` displays access denials of the Open, Execute, Read, Write, Close, Rename, Delete, Folder operations;
- `monitor.exe /?` displays brief help about `monitor.exe` parameters.

# 10 R-Guard Wizard

When **R-Guard** is installed, a new command **R-Guard Wizard** appears in the context menu of any file or folder (also the application icon appears in the Windows Quick Launch area, on the desktop, in the **Start** button menu). This command (or icon) starts R-Guard Wizard that creates users` access rules to files or folders. You can also use ***File\Run R-Guard Wizard...*** in the **R-Guard Main** menu to initialize R-Guard Wizard.

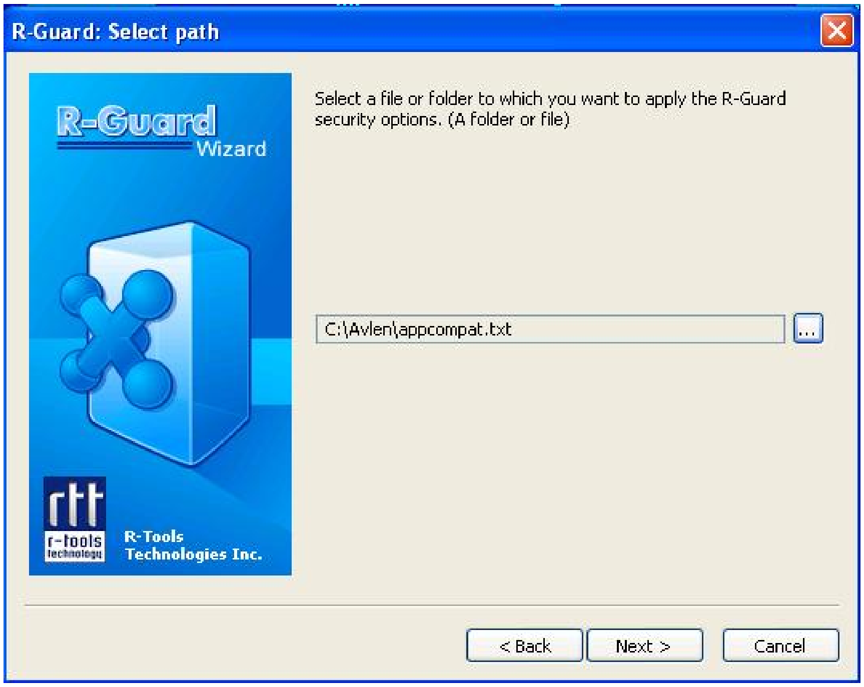


Setting R-Guard access rights.

Using this Wizard, you can easily set security policy of selected objects for users in few steps.
Use the Next and Back buttons to go to necessary steps.
Note: You may do the same by running the R-Guard main console and selecting the Access Control -> User Control tab on it.

□ Don't show this tab next time.

1. Click **Next** to specify the file or a folder to which access rights are being assigned. Click **Next**.

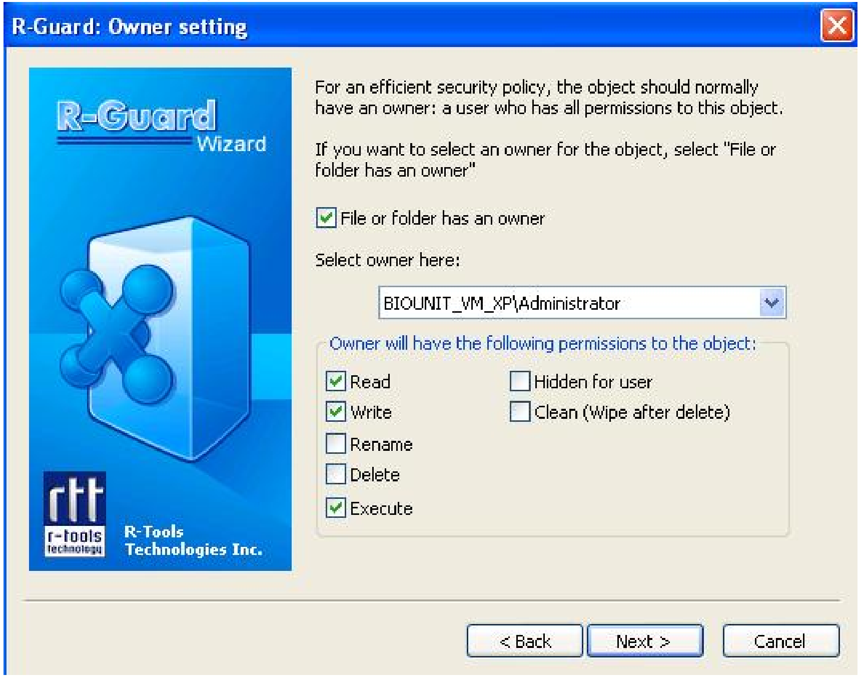


R-Guard: Select path

Select a file or folder to which you want to apply the R-Guard security options. (A folder or file)

C:\Avlen\appcompat.txt

2. Select the owner for the file or folder and assign him or her access rights to it. To do this, select the **Object has an owner** option and select a user from the **Select owner here** drop-down list. Select the necessary access rights (Read, Write, etc.) in the **Owner will have the following permissions to the object** section. More detail about the access rights. Click **Next**.



R-Guard: Owner setting

For an efficient security policy, the object should normally have an owner: a user who has all permissions to this object.

If you want to select an owner for the object, select "File or folder has an owner"

☑ File or folder has an owner

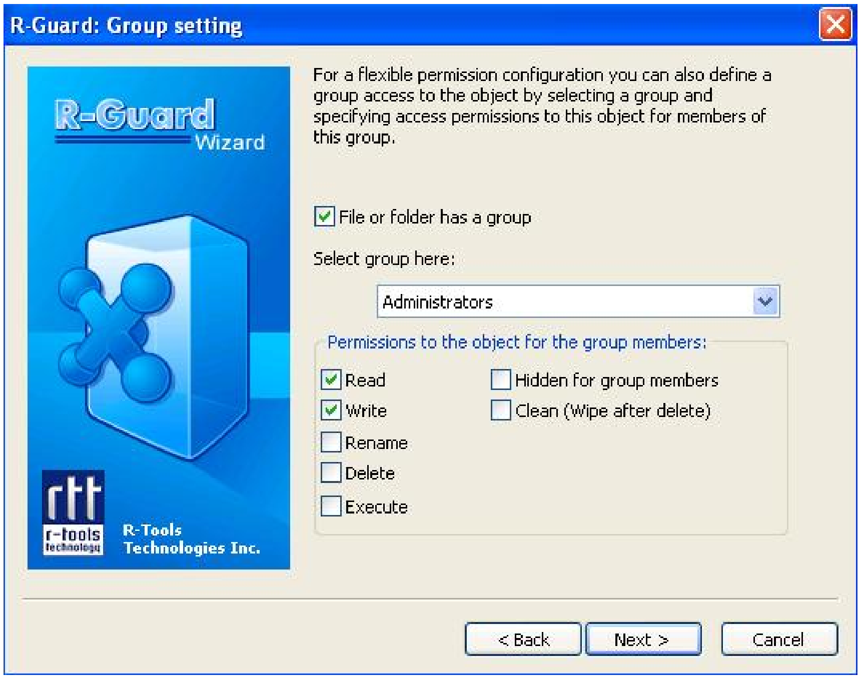
Select owner here:

BIOUNIT_VM_XP\Administrator

Owner will have the following permissions to the object:

☑ Read
☑ Write
☐ Rename
☐ Delete
☑ Execute
☐ Hidden for user
☐ Clean (Wipe after delete)

3. Select a group of users and assign access rights for this group. To do this, select the **Object has a group** option and select a group of users from the **Select group here** drop-down list. Select the necessary access rights (Read, Write, etc.) in the **The group members will have the following permissions to this object** section. More detail about the access rights. Click **Next**.



R-Guard: Group setting

For a flexible permission configuration you can also define a group access to the object by selecting a group and specifying access permissions to this object for members of this group.

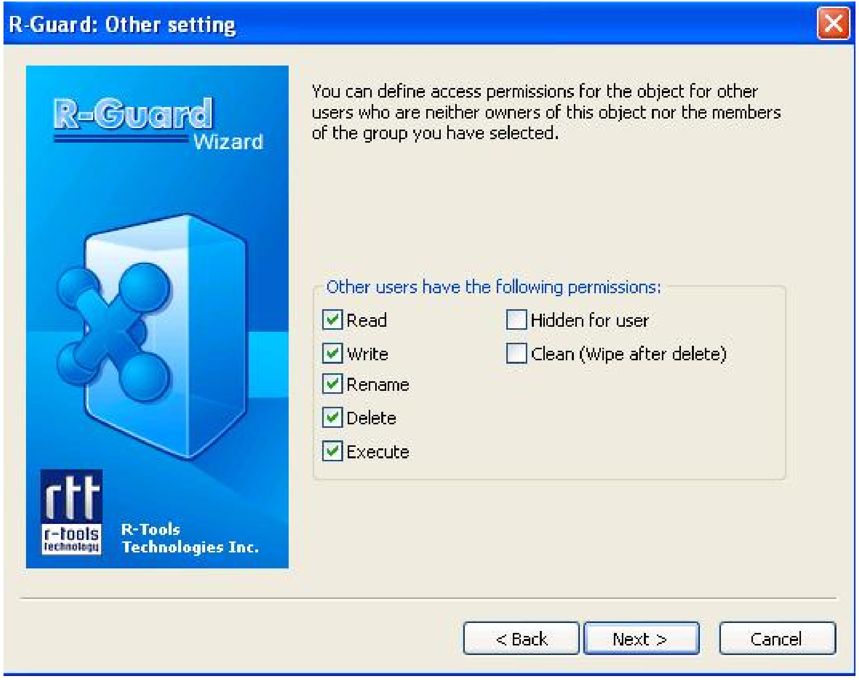
☑ File or folder has a group

Select group here: Administrators

Permissions to the object for the group members:

☑ Read ☐ Hidden for group members
☑ Write ☐ Clean (Wipe after delete)
☐ Rename
☐ Delete
☐ Execute

4. Assign access rights to the file or folder for other users. To do this, select the necessary access rights (Read, Write, etc.) in the **Other users have the following rights** section. More detail about the access rights. Click **Next**.



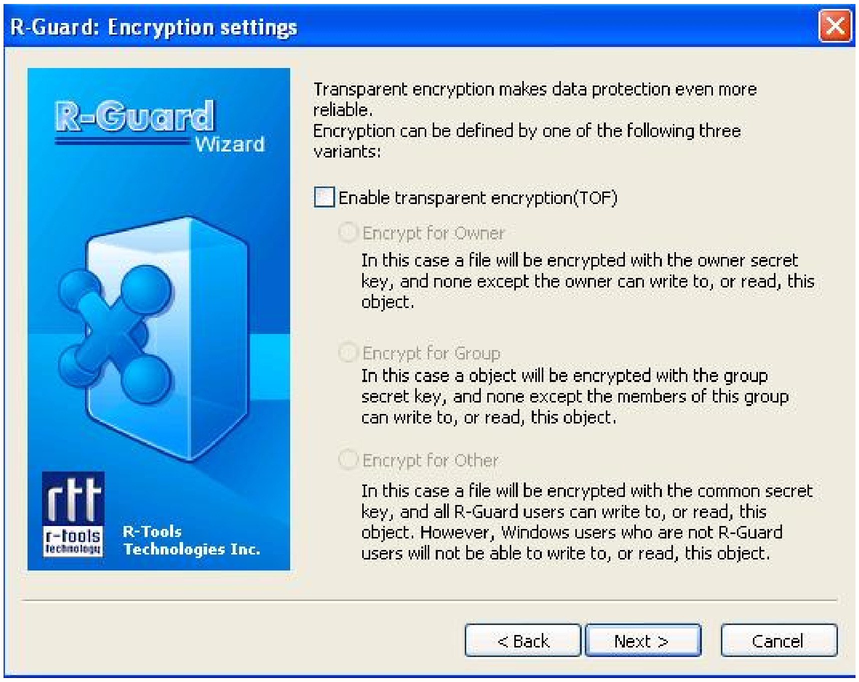
R-Guard: Other setting

You can define access permissions for the object for other users who are neither owners of this object nor the members of the group you have selected.

Other users have the following permissions:

☑ Read ☐ Hidden for user
☑ Write ☐ Clean (Wipe after delete)
☑ Rename
☑ Delete
☑ Execute

5. Set the transparent encryption option for a file or a folder. The **R-Guard** transparent encryption of a file or a folder can be set individually for a user, for a group of users, or for all other users. To do this, select the **Enable transparent encryption (TOF)** option and the corresponding option: **Encrypt for owner**, **Encrypt for group**, or **Encrypt for other**. Click **Next**.



R-Guard: Encryption settings

Transparent encryption makes data protection even more reliable.
Encryption can be defined by one of the following three variants:

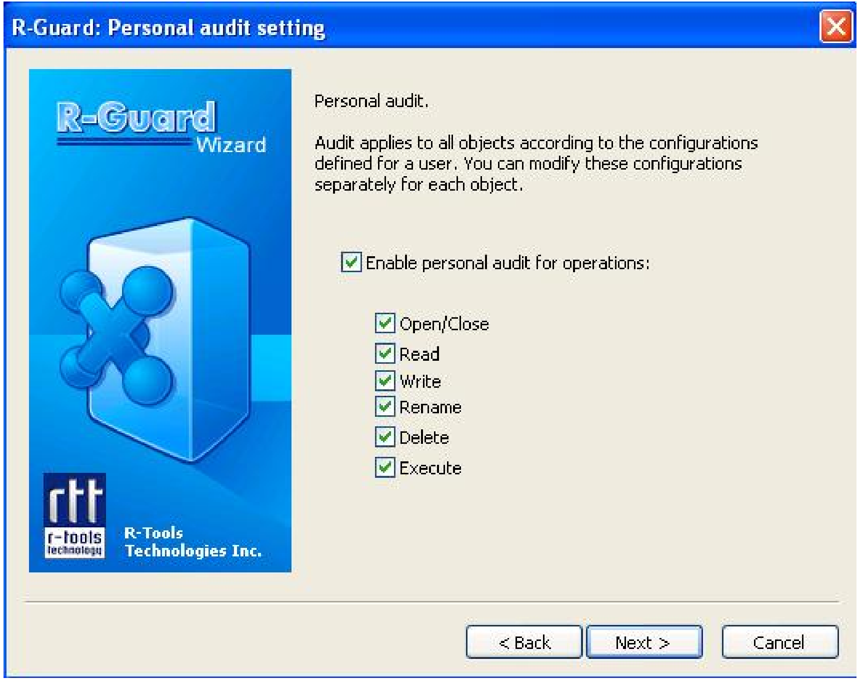
□ Enable transparent encryption(TOF)

○ Encrypt for Owner
In this case a file will be encrypted with the owner secret key, and none except the owner can write to, or read, this object.

○ Encrypt for Group
In this case a object will be encrypted with the group secret key, and none except the members of this group can write to, or read, this object.

○ Encrypt for Other
In this case a file will be encrypted with the common secret key, and all R-Guard users can write to, or read, this object. However, Windows users who are not R-Guard users will not be able to write to, or read, this object.

6. Specify the operations with the file or folder which will be logged in **R-Guard Audit**. To do this, select the **Enable personal audit for operations** option and select the necessary operation (Read, Write, etc.). More detail about the access rights. Click **Next**.



R-Guard: Personal audit setting

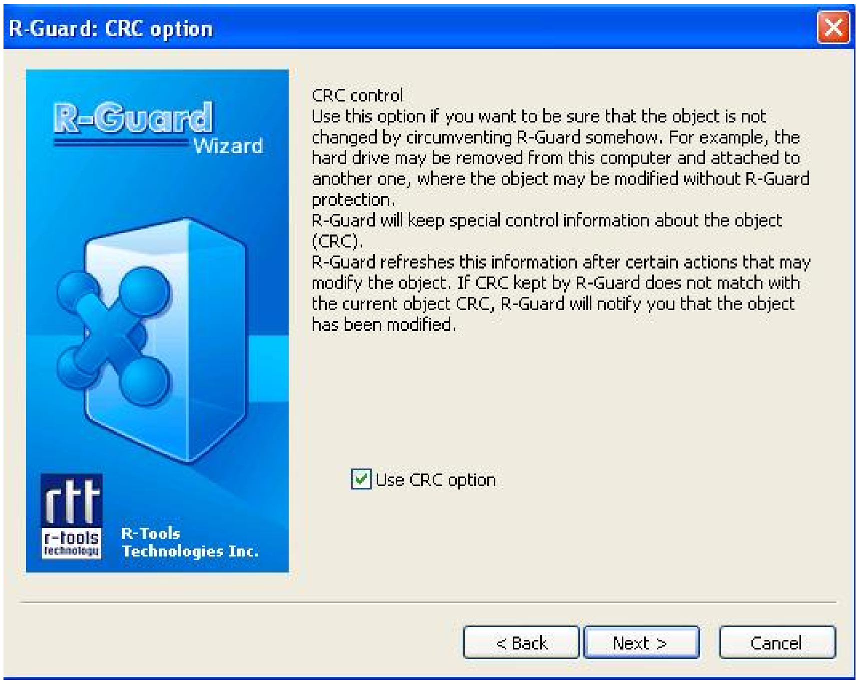
Personal audit.

Audit applies to all objects according to the configurations defined for a user. You can modify these configurations separately for each object.

☑ Enable personal audit for operations:

☑ Open/Close
☑ Read
☑ Write
☑ Rename
☑ Delete
☑ Execute

7. Set the CRC control option for a file or a folder. Select the **Use CRC option** for this. Click **Next**.

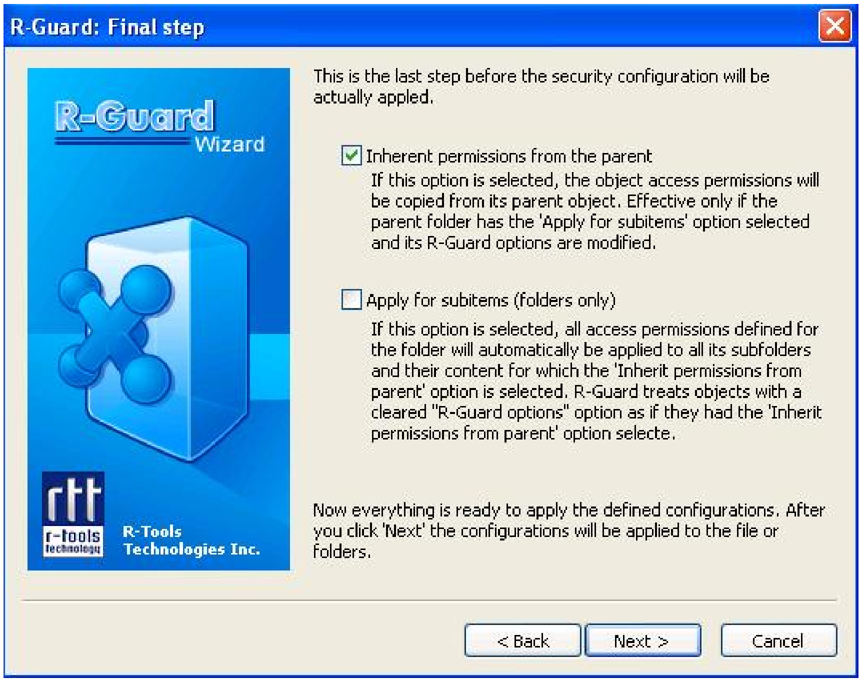


R-Guard: CRC option

CRC control
Use this option if you want to be sure that the object is not changed by circumventing R-Guard somehow. For example, the hard drive may be removed from this computer and attached to another one, where the object may be modified without R-Guard protection.
R-Guard will keep special control information about the object (CRC).
R-Guard refreshes this information after certain actions that may modify the object. If CRC kept by R-Guard does not match with the current object CRC, R-Guard will notify you that the object has been modified.

☑ Use CRC option

8. Specify whether the access rights to this file or folder are the same as the ones of the parental folder. Select the **Inherit permissions from parent** option for this. Also, for folders only, you can specify whether the access rights of the subfolders and files in this folder are the same as its access rights. More detail about the access rights. Select the **Apply for subitems (folders only)** option for this. Click **Next**.



R-Guard: Final step

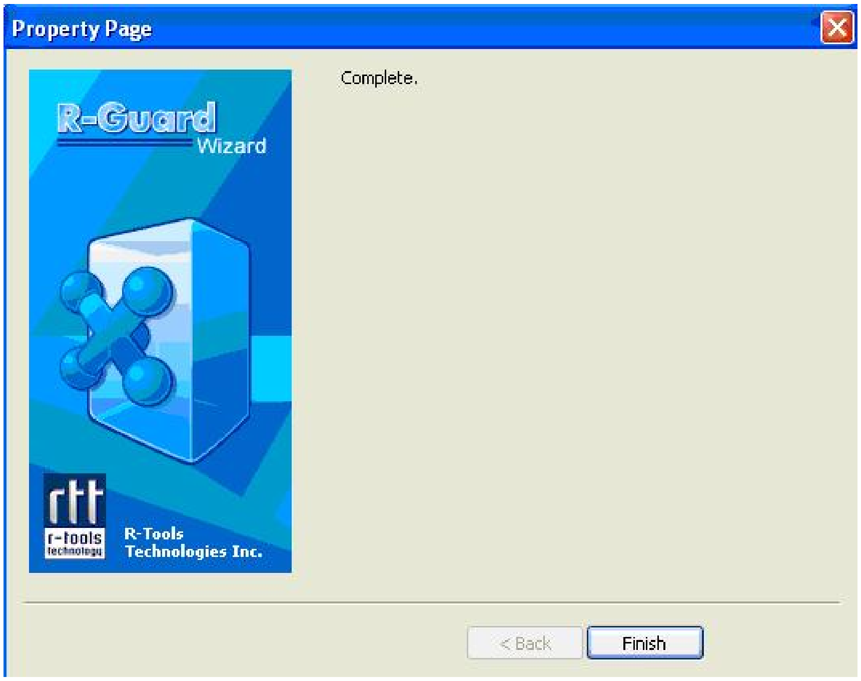
This is the last step before the security configuration will be actually appled.

☑ Inherent permissions from the parent
If this option is selected, the object access permissions will be copied from its parent object. Effective only if the parent folder has the 'Apply for subitems' option selected and its R-Guard options are modified.

□ Apply for subitems (folders only)
If this option is selected, all access permissions defined for the folder will automatically be applied to all its subfolders and their content for which the 'Inherit permissions from parent' option is selected. R-Guard treats objects with a cleared "R-Guard options" option as if they had the 'Inherit permissions from parent' option selecte.

Now everything is ready to apply the defined configurations. After you click 'Next' the configurations will be applied to the file or folders.

9. View the final page of the Wizard. Click **Finish** to close Wizard.



Complete.

# 11 R-Guard Shell Extension

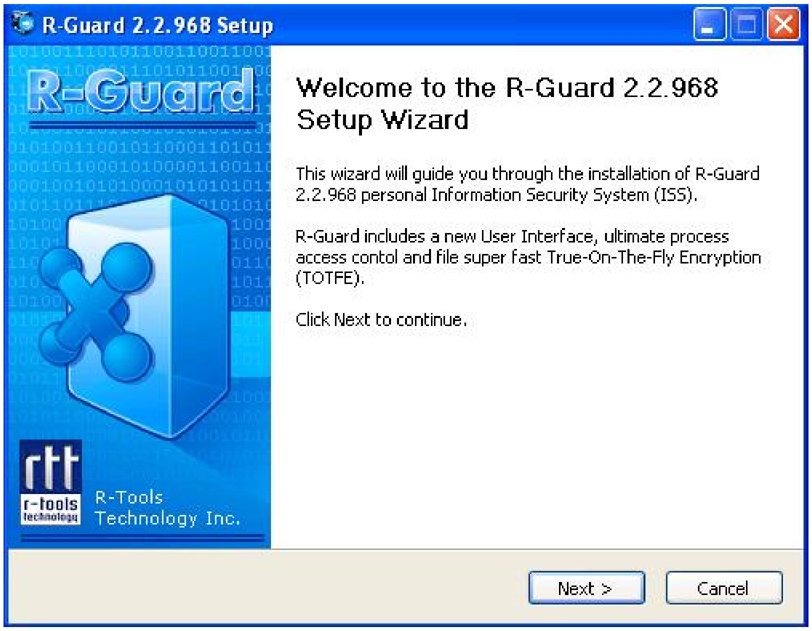
When **R-Guard** is installed, the Properties window of any file or folder will have two additional tabs:

- **User Control**: allows you to assign access rights to files or folders right from the Properties window of a file or a folder without the need of opening the **R-Guard** main window. This tab is identical to the User Control panel.
- **Process Control**: allows you to assign access rights to processes right from the properties window of a process without the need of opening the **R-Guard** main window. This tab is identical to the Process control panels.

# 12 Installing R-Guard

The **R-Guard** installation is similar to the installation of the most Windows-based applications. It is recommended to close all programs before beginning of the R-Guard installation because you will have to restart your computer after **R-Guard** installation.

1. Run the `R-GuardInstaller.exe` file. A window will appear warning that the **R-Guard** installing process has started.


R-Guard 2.2.968 Setup

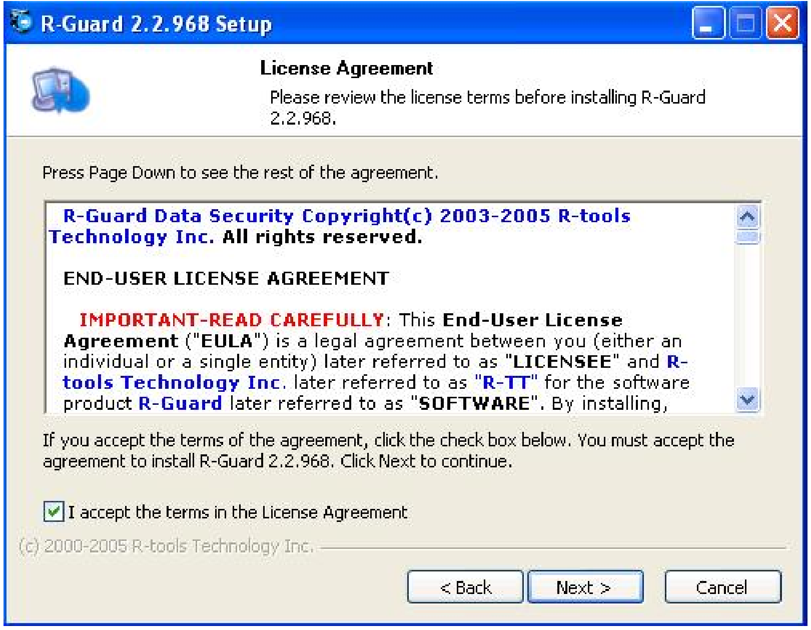
Welcome to the R-Guard 2.2.968 Setup Wizard

This wizard will guide you through the installation of R-Guard 2.2.968 personal Information Security System (ISS).

R-Guard includes a new User Interface, ultimate process access contol and file super fast True-On-The-Fly Encryption (TOTFE).

Click Next to continue.

2. Click the **Next** button to enter the **License Agreement** window. To continue **R-Guard** installation, you have to accept this agreement by selecting the ***I accept the terms in the License Agreement*** option.


R-Guard 2.2.968 Setup

**License Agreement**

Please review the license terms before installing R-Guard 2.2.968.

Press Page Down to see the rest of the agreement.

**R-Guard Data Security Copyright(c) 2003-2005 R-tools Technology Inc. All rights reserved.**

**END-USER LICENSE AGREEMENT**

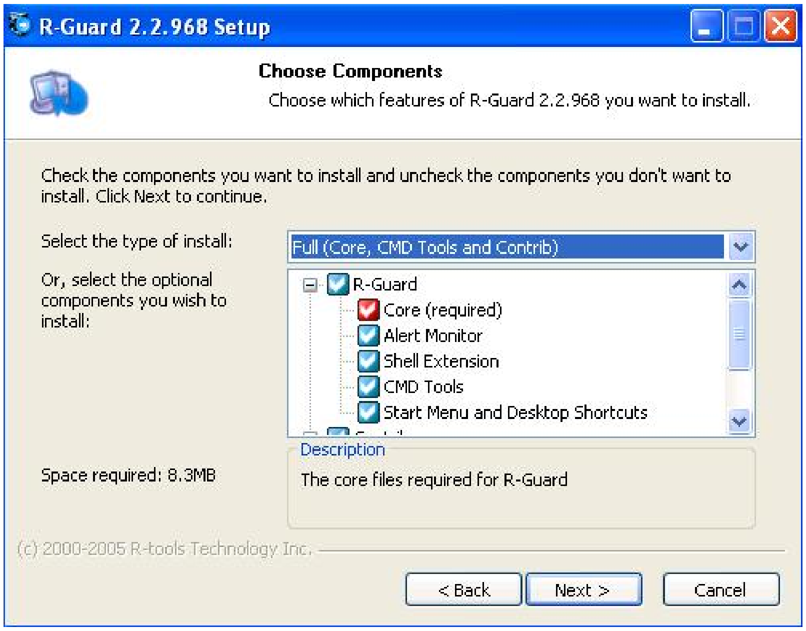
IMPORTANT-READ CAREFULLY: This **End-User License Agreement** ("**EULA**") is a legal agreement between you (either an individual or a single entity) later referred to as "**LICENSEE**" and **R-tools Technology Inc**. later referred to as "**R-TT**" for the software product **R-Guard** later referred to as "**SOFTWARE**". By installing,

If you accept the terms of the agreement, click the check box below. You must accept the agreement to install R-Guard 2.2.968. Click Next to continue.

☑ I accept the terms in the License Agreement

(c) 2000-2005 R-tools Technology Inc.

3. Click the **Next** button to enter the window where you can choose **R-Guard** components to install. Select each component you want to install. It is recommended to install all **R-Guard** components. When you drag the mouse over the component, you will see the description of this component in the **Description** field. If **R-Guard** has already been installed and the same (or newer) version is being installed, a window will appear allowing you to select **Add/Reinstall components** if you want to install a new **R-Guard** version and **Uninstall R-Guard** if you want to uninstall **R-Guard** before installing a new version.



**Choose Components**

Choose which features of R-Guard 2.2.968 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Full (Core, CMD Tools and Contrib)

Or, select the optional components you wish to install:

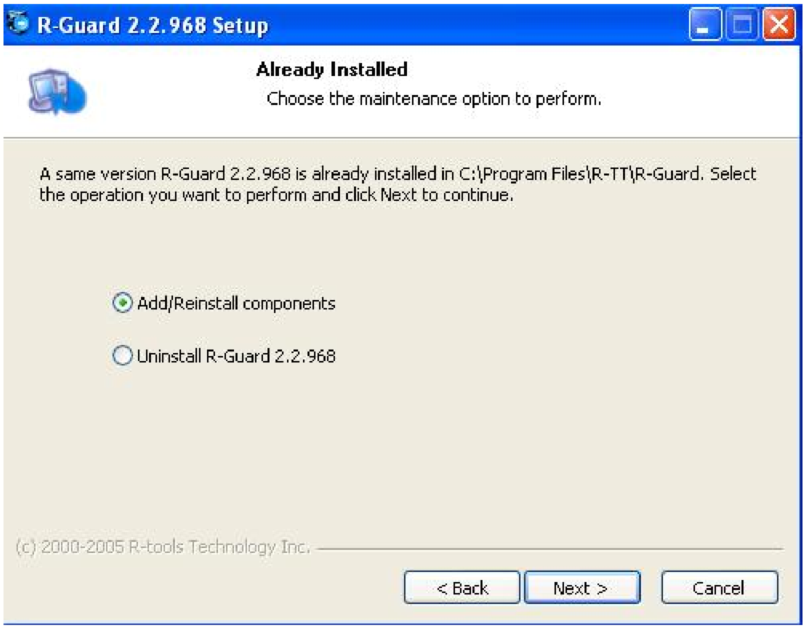
- ☑ R-Guard
  - ☑ Core (required)
  - ☑ Alert Monitor
  - ☑ Shell Extension
  - ☑ CMD Tools
  - ☑ Start Menu and Desktop Shortcuts

Space required: 8.3MB

Description

The core files required for R-Guard

(c) 2000-2005 R-tools Technology Inc.
< Back
Next >
Cancel



**Already Installed**

Choose the maintenance option to perform.

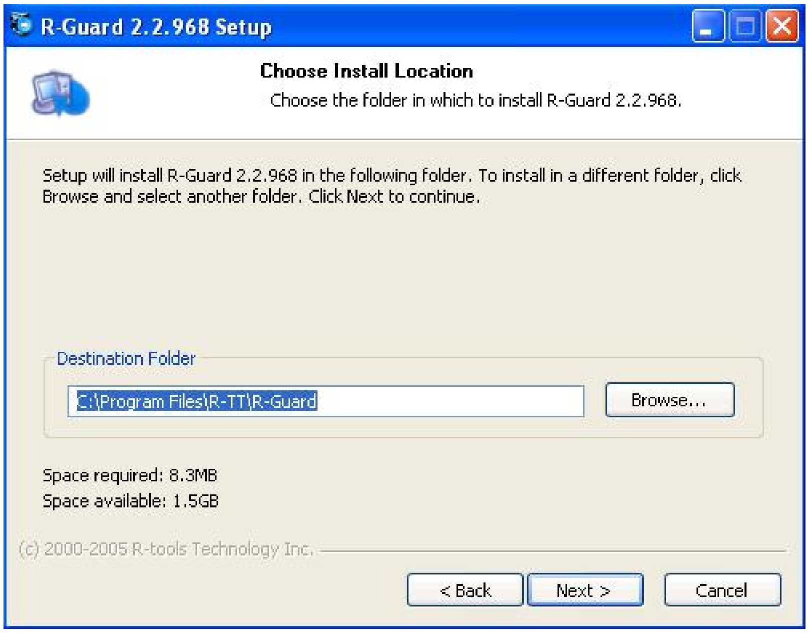
A same version R-Guard 2.2.968 is already installed in C:\Program Files\R-TT\R-Guard. Select the operation you want to perform and click Next to continue.

● Add/Reinstall components

○ Uninstall R-Guard 2.2.968

(c) 2000-2005 R-tools Technology Inc.
< Back
Next >
Cancel

4. Click the **Next** button to enter the window where you can select the **R-Guard** installation folder.



R-Guard 2.2.968 Setup

**Choose Install Location**

Choose the folder in which to install R-Guard 2.2.968.

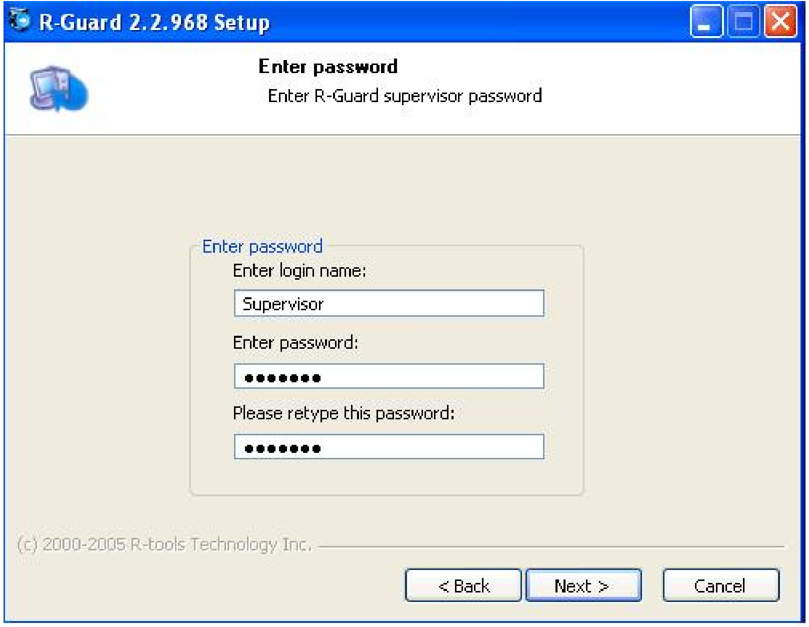
Setup will install R-Guard 2.2.968 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: C:\Program Files\R-TT\R-Guard

Space required: 8.3MB
Space available: 1.5GB

(c) 2000-2005 R-tools Technology Inc.

5. Click the **Next** button to enter the window where you should enter the user login and password which will be used for disabling the **R-Guard** attributes. You should enter the user login and password in the fields **Enter login name** and **Enter password for R-Guard turning off** and confirm the password in the field **Please retype this password**. In order to disable the **R-Guard** attributes, you should press the left **<Ctrl>** button on the keyboard during Windows startup. Then enter the user login and password.



R-Guard 2.2.968 Setup

**Enter password**

Enter R-Guard supervisor password

Enter password

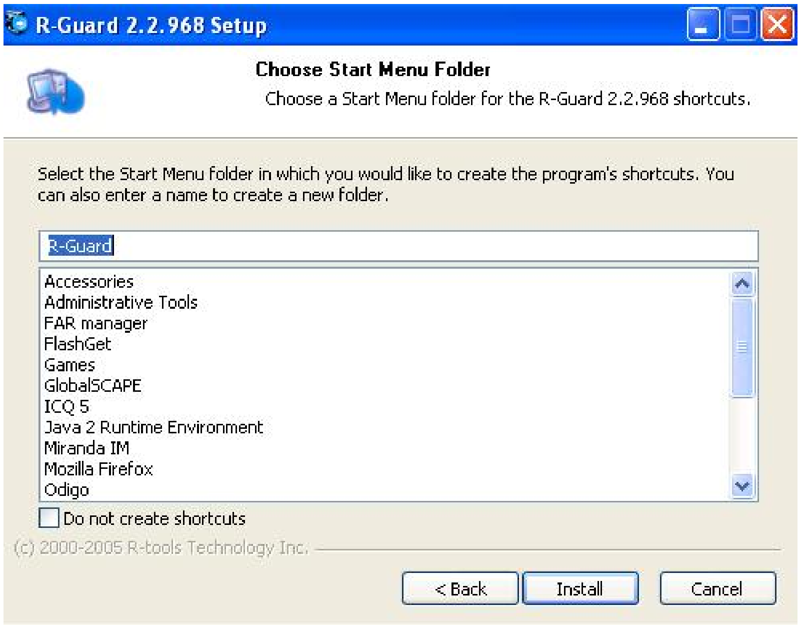
Enter login name: Supervisor

Enter password: •••••••

Please retype this password: •••••••

(c) 2000-2005 R-tools Technology Inc.

6. Click the **Next** button to enter the window where you can choose the folder in the **Start** menu for the **R-Guard** shortcut.



R-Guard 2.2.968 Setup

**Choose Start Menu Folder**

Choose a Start Menu folder for the R-Guard 2.2.968 shortcuts.

Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

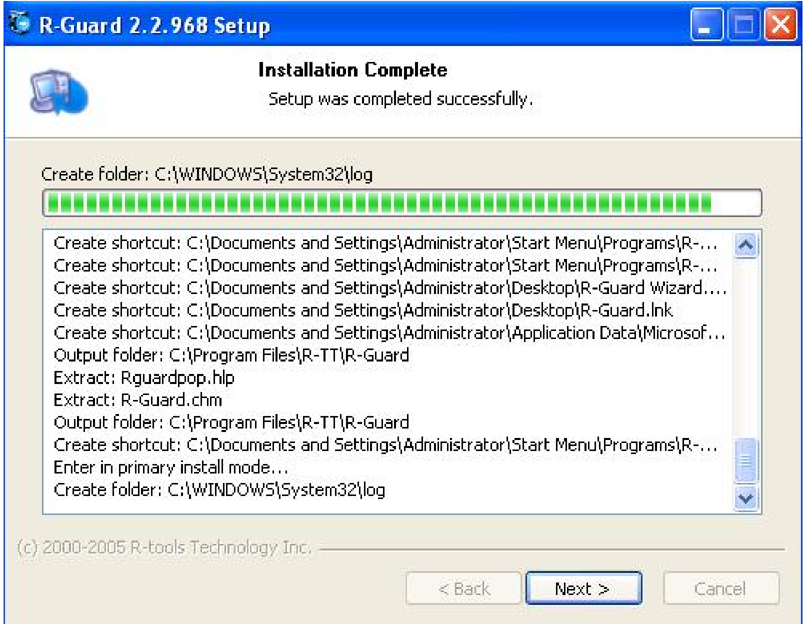
R-Guard

```
Accessories
Administrative Tools
FAR manager
FlashGet
Games
GlobalSCAPE
ICQ 5
Java 2 Runtime Environment
Miranda IM
Mozilla Firefox
Odigo
```

□ Do not create shortcuts

(c) 2000-2005 R-tools Technology Inc.

7. Press the **Install** button to start the **R-Guard** installation process.



R-Guard 2.2.968 Setup

**Installation Complete**

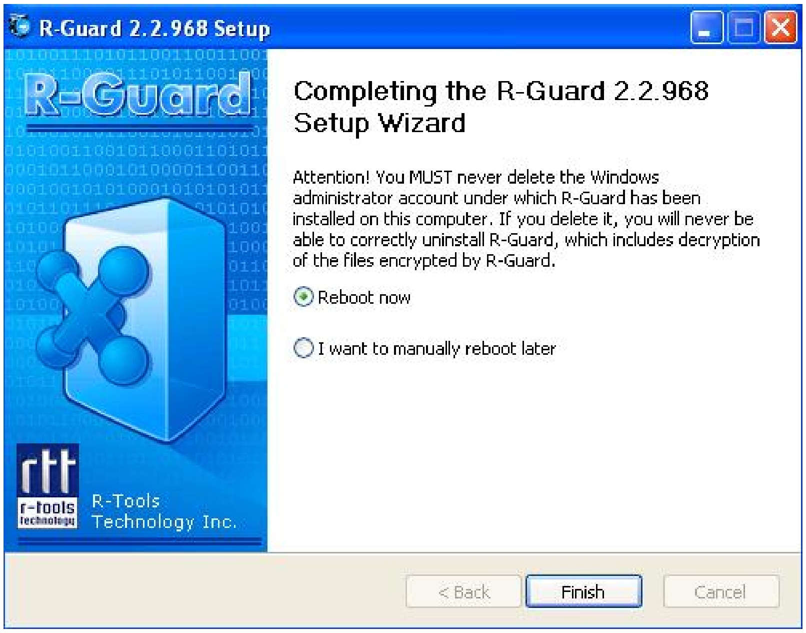
Setup was completed successfully.

Create folder: C:\WINDOWS\System32\log

```
Create shortcut: C:\Documents and Settings\Administrator\Start Menu\Programs\R-...
Create shortcut: C:\Documents and Settings\Administrator\Start Menu\Programs\R-...
Create shortcut: C:\Documents and Settings\Administrator\Desktop\R-Guard Wizard....
Create shortcut: C:\Documents and Settings\Administrator\Desktop\R-Guard.lnk
Create shortcut: C:\Documents and Settings\Administrator\Application Data\Microsof...
Output folder: C:\Program Files\R-TT\R-Guard
Extract: Rguardpop.hlp
Extract: R-Guard.chm
Output folder: C:\Program Files\R-TT\R-Guard
Create shortcut: C:\Documents and Settings\Administrator\Start Menu\Programs\R-...
Enter in primary install mode...
Create folder: C:\WINDOWS\System32\log
```

(c) 2000-2005 R-tools Technology Inc.

8. Click **Next** to finish the installation. A window will appear asking you to reboot your computer. Select **Reboot now** and click **Finish**.



Completing the R-Guard 2.2.968 Setup Wizard

Attention! You MUST never delete the Windows administrator account under which R-Guard has been installed on this computer. If you delete it, you will never be able to correctly uninstall R-Guard, which includes decryption of the files encrypted by R-Guard.

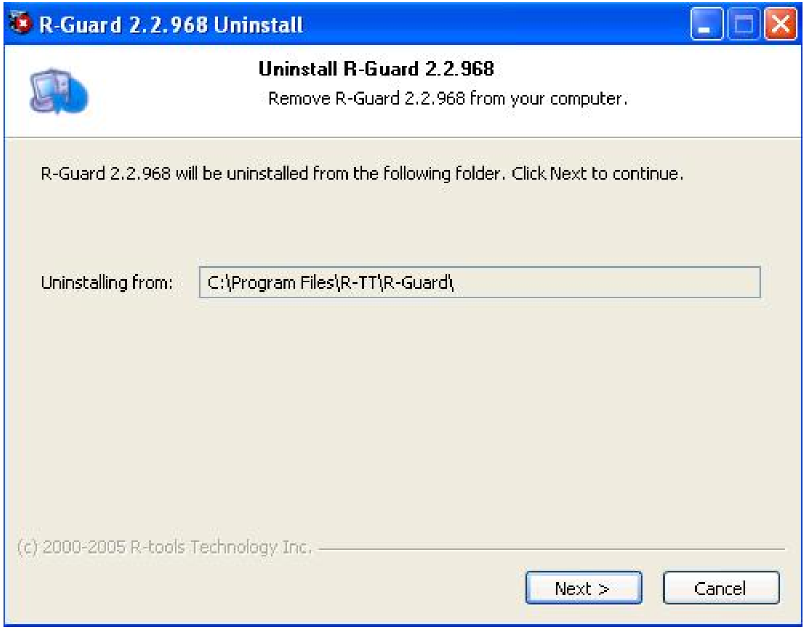
● Reboot now

○ I want to manually reboot later

# 13 Uninstalling R-Guard

In order to uninstall **R-Guard** from a computer you should run a special deinstallation program:

1. Run the uninst-R-Guard.exe file. You can do this by selecting ***Programs\R-Guard\R-Guard Uninstall*** in the **Start** button menu or by selecting ***Settings\Control Panel\Add or Remove Programs\R-Guard Uninstall\Currently installed programs\R-Guard*** in the **Start** button menu and selecting **Change/Remove**. After starting the uninst-R-Guard.exe file a window will appear warning that the **R-Guard** uninstalling process has started.



Uninstall R-Guard 2.2.968

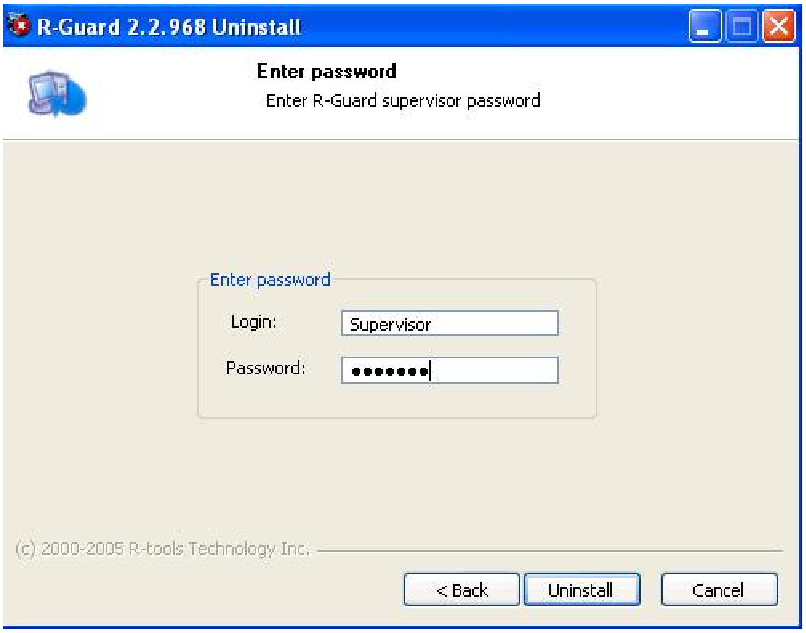
Remove R-Guard 2.2.968 from your computer.

R-Guard 2.2.968 will be uninstalled from the following folder. Click Next to continue.

Uninstalling from: C:\Program Files\R-TT\R-Guard\

(c) 2000-2005 R-tools Technology Inc.

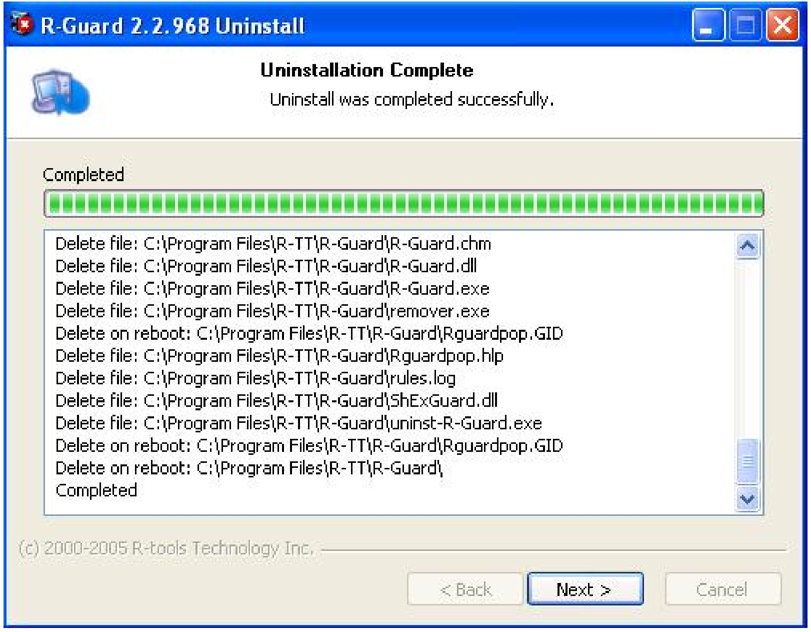
2. Click the **Next** button to enter the user login and password which were used for disabling the **R-Guard** attributes.


R-Guard 2.2.968 Uninstall
Enter password
Enter R-Guard supervisor password
Enter password
(c) 2000-2005 R-tools Technology Inc.
< Back
Uninstall
Cancel

Login: Supervisor

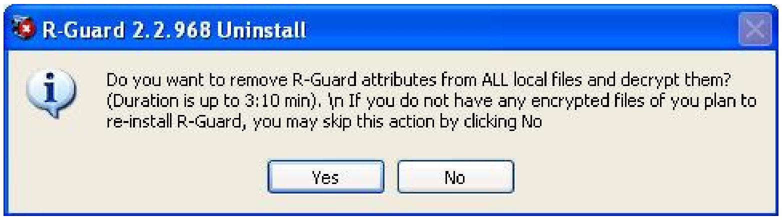
Password: •••••••

3. Click the **Uninstall** button to start the **R-Guard** uninstallation process.


R-Guard 2.2.968 Uninstall
Uninstallation Complete
Uninstall was completed successfully.
Completed
(c) 2000-2005 R-tools Technology Inc.
< Back
Next >
Cancel

```
Delete file: C:\Program Files\R-TT\R-Guard\R-Guard.chm
Delete file: C:\Program Files\R-TT\R-Guard\R-Guard.dll
Delete file: C:\Program Files\R-TT\R-Guard\R-Guard.exe
Delete file: C:\Program Files\R-TT\R-Guard\remover.exe
Delete on reboot: C:\Program Files\R-TT\R-Guard\Rguardpop.GID
Delete file: C:\Program Files\R-TT\R-Guard\Rguardpop.hlp
Delete file: C:\Program Files\R-TT\R-Guard\rules.log
Delete file: C:\Program Files\R-TT\R-Guard\ShExGuard.dll
Delete file: C:\Program Files\R-TT\R-Guard\uninst-R-Guard.exe
Delete on reboot: C:\Program Files\R-TT\R-Guard\Rguardpop.GID
Delete on reboot: C:\Program Files\R-TT\R-Guard\
Completed
```

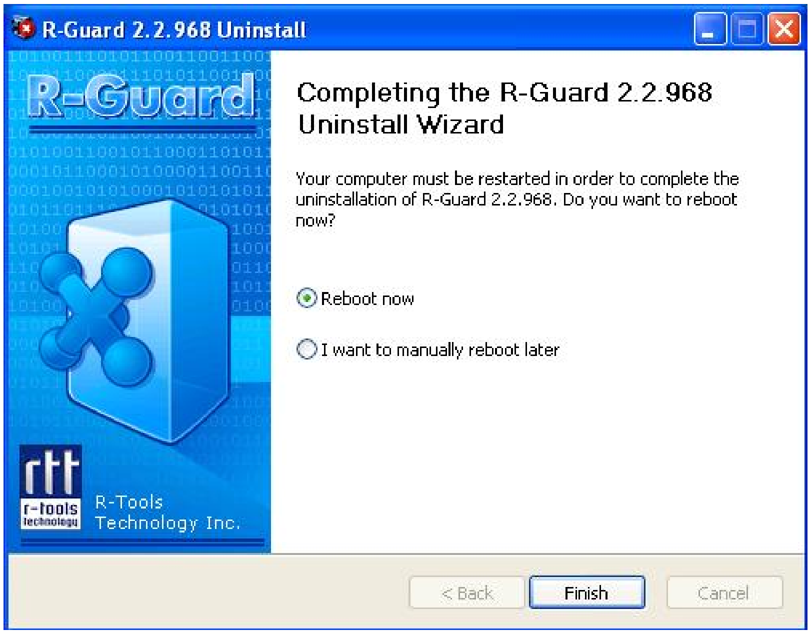
4. While uninstalling **R-Guard** from the system, a window requesting confirmation of the **R-Guard** access rights deletion appears. Click **Yes** to delete all user- (or application-) assigned access rights, Click **No** to retain them.



R-Guard 2.2.968 Uninstall

Do you want to remove R-Guard attributes from ALL local files and decrypt them? (Duration is up to 3:10 min). \n If you do not have any encrypted files of you plan to re-install R-Guard, you may skip this action by clicking No

5. Click **Next** to finish the procedure of uninstallation. A window will appear asking you to reboot your computer. Select **Reboot now** and click **Finish**.



R-Guard 2.2.968 Uninstall

Completing the R-Guard 2.2.968 Uninstall Wizard

Your computer must be restarted in order to complete the uninstallation of R-Guard 2.2.968. Do you want to reboot now?

● Reboot now

○ I want to manually reboot later

# Index