



NetOp

Desktop Firewall

Version 3.0

User's Manual

Moving expertise - not people®

Touchboards

205 Westwood Ave, Long Branch, NJ 07740

Phone: 866-94 BOARDS (26273) / (732)-222-1511

Fax: (732)-222-7088 | E-mail: sales@touchboards.com

Copyright © 2004 Danware Data A/S. All rights reserved

Document Revision: 2005074

Please send any comments to:

Danware Data A/S

Bregnerodvej 127

DK-3460 Birkerød

Denmark

Tel: +45 45 90 25 25

Fax: +45 45 90 25 26

E-mail: info@netop.com

Internet: <http://www.netop.com>

Warranty

Danware Data A/S warrants the quality of the physical material of the user package, that is manual and CD-ROM. If these items are defective, we will exchange them at no cost within 60 days of purchase from Danware Data.

Disclaimer

Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of any faults with the enclosed programs and/or documentation.

Licence

Danware Data A/S retains the copyright to the user manual. All patent, copyright and other proprietary rights in and to the programs will remain with Danware Data A/S or its licensors.

Your purchase gives you the right to copy and use the programs as described on your *Danware License Certificate* included in your package.

Please save your *Danware License Certificate* and your original CD-ROM. They serve as your legal right to use the software. You may also need them in order to receive future updates to the product.

Please be careful not to install or run the software on more PCs than your Danware License Certificates permits you to do.

The programs may be copied for backup purposes only, and only as long as the above mentioned rules are adhered to.

Trademarks

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this manual are trademarks of their respective manufacturers.



Contents

1 Introduction	7
1.1 Welcome	8
1.2 NetOp Desktop Firewall Features	8
1.2.1 Process Control	8
1.2.2 Communication Control	8
1.2.3 Information	10
1.2.4 Profiles	10
1.2.5 Protection	10
1.2.6 NetOp Policy Server Support	10
1.3 Documentation	10
1.3.1 Typographical Conventions	11
1.3.2 Standard Buttons	11
1.4 Updates	11
1.5 Common Controls	11
1.5.1 Window Controls	12
1.5.2 Menu Bar and Toolbar Controls	12
1.5.3 Table Controls	16
2 Installation	17
2.1 Summary	18
2.2 System Requirements	18
2.3 Before Install	18
2.4 Install	19
2.5 Setup Wizard	27
2.5.1 Installation Alternatives	30
2.5.2 Command Line Installation	31
2.1 Change or Remove	36
2.1.1 Change	37
2.1.2 Remove	41
3 NetOp Desktop Firewall	43
3.1 Summary	44
3.2 Startup Guide	44
3.2.1 Use and Configuration	44
3.2.2 Notification Area Button Menu	45
3.2.3 User Prompts and Messages	47
3.3 NetOp Desktop Firewall Window	49
3.3.1 Configuration Guide	49
3.3.1.1 Firewall Rules	50
3.3.1.2 Information	51
3.3.1.3 Profiles	52
3.3.1.4 Options	53
3.3.2 Title Bar	54
3.3.3 Menu Bar	54
3.3.3.1 File Menu	54
3.3.3.2 Edit Menu	54
3.3.3.3 View Menu	55
3.3.3.4 Tools Menu	56
3.3.3.5 Help Menu	56
3.3.4 Toolbars	57
3.3.4.1 Firewall Rules Toolbar	58
3.3.4.2 Information Toolbar	58
3.3.4.3 Options Toolbar	58
3.3.4.4 Play Toolbar	59

3.3.5 Work Pane	60
3.3.5.1 Firewall Rules	61
3.3.5.1.1 Programs	62
3.3.5.1.2 Ports	67
3.3.5.1.3 Protocols	71
3.3.5.1.4 Trusted Nets	74
3.3.5.1.5 Banned Nets	78
3.3.5.2 Information	81
3.3.5.2.1 Event Log	82
3.3.5.2.2 Packet Log	84
3.3.5.2.3 Traffic Matrix	88
3.3.5.2.4 Statistics	91
3.3.5.2.5 Program Manager	92
3.3.5.3 Profiles	94
3.3.5.3.1 Profile Rules	96
3.3.6 Status Bar	101
3.4 NetOp Desktop Firewall Tools	102
3.4.1 Options	102
3.4.1.1 General Tab	103
3.4.1.2 Password Tab	105
3.4.1.3 Policy Server Tab	107
3.4.1.4 Event Log Tab	109
3.4.1.5 Packet Log Tab	110
3.4.1.6 Colors Tab	113
3.4.1.7 Program Manager Tab	116
4 How NetOp Desktop Firewall Works	119
4.1 Summary	120
4.2 How a Firewall Works	120
4.3 How NetOp Desktop Firewall Works	120
4.3.1 Process Control	120
4.3.2 Hacker Resistance	121
4.3.3 Operational Benefits	121
4.3.4 Plug-and-Play with Highly Specific and Transparent Firewall Rules	121
4.3.5 NetOp Policy Server Support	121
5 Appendix	123
5.1 Trial Version	124

1 Introduction

1.1 Welcome

Welcome to *NetOp Desktop Firewall* from Danware.

We hope that this product will meet your requirements and fulfill your expectations.

If you encounter difficulties using this product, first consult with the User's Manual or the *Help* system that come with the product.

Additional technical information is available on our website www.netop.com, select *Support*.

Your local supplier of *NetOp Desktop Firewall* is available for advising you on how to obtain maximum benefit from the product.

As a last resort, you are invited to submit a support request by e-mail to us at support@security.netop.com. We will endeavour to get back to you as soon as possible with a solution to your problem.

NetOp Product Services

This chapter contains the sections:

- NetOp Desktop Firewall Features,
- Documentation,
- Updates
- Common Controls.

1.2 NetOp Desktop Firewall Features

NetOp Desktop Firewall is a single computer firewall with strong unique features.

It can operate both as a stand-alone computer firewall and as a local computer firewall in a distributed firewall system controlled centrally by *NetOp Policy Server*.

When *NetOp Desktop Firewall* is installed on a computer, it will always run while the computer is switched on. If you do not want *NetOp Desktop Firewall* to run on the computer, you must remove it.

To protect the computer, *NetOp Desktop Firewall* applies process control and communication control.

1.2.1 Process Control

Computer processes are executed by programs. Some programs belong to the computer operating system. Other programs belong to applications installed on the computer. *NetOp Desktop Firewall* monitors all programs running on the computer and controls programs by assigning a *Firewall Rule* to them.

NetOp Desktop Firewall monitors program activity on the computer in these *information* utilities listed below:

- *Event Log*
- *Packet Log*
- *Program Manager*

By default, *NetOp Desktop Firewall* will allow programs to run unless the *Firewall Rule* named *Kill Program* is assigned to them.

If the option *Run only authorized programs* is selected, *NetOp Desktop Firewall* will allow programs to run only if a *Firewall Rule* other than *Kill Program* is assigned to them.

1.2.2 Communication Control

NetOp Desktop Firewall controls communication, i.e. the passage of data packets across the computer communication interface, by *Firewall Rules* assigned to *Programs*, *Ports*, *Protocols*, *Trusted Nets* and *Banned Nets*.

Each data packet includes headers specifying the communication properties of the data packet. *NetOp Desktop Firewall* reads the headers of each data packet at the computer communication interface and if the communication properties do not meet specified *Firewall Rules*, it is denied passage.

Program Firewall Rules

These *Program* firewall rules are available:

- *Allow Communication*: Allows communication by this program file across the computer communication interface. *Port*, *Protocol*, *Trusted Net* and *Banned Net* firewall rules apply, see below.
- *Prompt on Communication*: Prompts the computer user upon attempted communication by this program file to assign a firewall rule to it.
- *Deny Communication*: Denies communication by this program file across the computer communication interface.
- *Kill Program*: Does not allow this program file to run on the computer.
- *Unrestricted Communication*: Allows communication by this program file across the computer communication interface without applying *Port* and *Protocol* firewall rules. *Banned Net* firewall rules apply, see below.
- *Trusted Net Only*: Allows communication by this program file only with computers on a *Trusted Net*, see below.

Port Firewall Rules

These *Port* firewall rules are available:

- *Inbound/Outbound Traffic*: Allows inbound and outbound communication through this port.
- *Outbound Traffic*: Allows outbound communication only through this port.
- *Inbound Traffic*: Allows inbound communication only through this port.
- *Blocked in Both Directions*: Allows no communication through this port.

Protocol Firewall Rules

These *Protocol* firewall rules are available:

- *Inbound/Outbound Traffic*: Allows inbound and outbound communication using this protocol.
- *Outbound Traffic*: Allows outbound communication only using this protocol.
- *Inbound Traffic*: Allows inbound communication only using this protocol.
- *Blocked in Both Directions*: Allows no communication using this protocol.

Trusted Net Firewall Rules

A *Trusted Net* is a range of remote computer addresses with which your computer shall be able to communicate without applying *Port* and *Protocol* firewall rules.

These *Trusted Net* firewall rules are available:

- *Inbound/Outbound Trust*: Applies no *Port* and *Protocol* firewall rules to inbound and outbound communication with computers on this *Trusted Net*.
- *Outbound Trust*: Applies no *Port* and *Protocol* firewall rules to outbound communication to computers on this *Trusted Net*.
- *Inbound Trust*: Applies no *Port* and *Protocol* firewall rules to inbound communication from computers on this *Trusted Net*.
- *Trust Inactive*: Disables trust in computers on this *Trusted Net*.

Banned Net Firewall Rules

A *Banned Net* is a range of remote computer addresses with which your computer shall not be able to communicate.

These *Banned Net* firewall rules are available:

- *Inbound/Outbound Ban*: Allows no inbound or outbound communication with computers on this *Banned Net*.
- *Outbound Ban*: Allows no outbound communication to computers on this *Banned Net*.
- *Inbound Ban*: Allows no inbound communication from computers on this *Banned Net*.

- *Ban Inactive*: Disables ban on computers on this *Banned Net*.

1.2.3 Information

A range of *Information* utilities enable the firewall user to view and analyze what is happening on the firewall:

- *Event Log* displays selected operational events in a table with event details.
- *Packet Log* displays programs opened, closed and killed and all data packets at the computer communication interface in a table with selected event details to enable an analysis of each event.
- *Traffic Matrix* displays data packet traffic at the computer communication interface in a circular graph to enable an analysis of connections and communicating computer addresses.
- *Statistics* displays in graphs and numbers current and historical sent, received and blocked data packets at the computer communication interface to monitor firewall activity.
- *Program Manager* displays programs running on the computer in a table with selected program details to enable program management.

1.2.4 Profiles

NetOp Desktop Firewall can specify *Profiles* to assign different sets of firewall rules to computers when used in different environments such as work, home or travel.

Profile Rules can be applied to automatically assign a profile matching detected current computer environment properties.

1.2.5 Protection

NetOp Desktop Firewall runs as a driver in the very heart of the computer. From this location it can control processes running on the computer and cannot be neutralized or removed by a remote hacking attempt. Removal of the *NetOp Desktop Firewall* driver requires authorized removal of the *NetOp Desktop Firewall* installation followed by computer restart.

The driver is controlled from the *NetOp Desktop Firewall* window that runs as an application on top of the operating system and communicates with the driver by hacker-proof encrypted communication. If this encrypted communication detects any abnormality, it immediately blocks all communication across the computer communication interface and alerts the user to fence off an ongoing remote hacking attempt.

Access to the *NetOp Desktop Firewall* window as well as the removal of *NetOp Desktop Firewall* can be password protected.

1.2.6 NetOp Policy Server Support

NetOp Desktop Firewall can be logged on to an organizational *NetOp Policy Server* to become supported or fully controlled by it.

NetOp Policy Server assigns a *Security Policy* to a logged on *NetOp Desktop Firewall* specifying *Program*, *Port*, *Protocol*, *Trusted Net* and *Banned Net* firewall rules. A *Security Policy* also specifies *Profiles*, *Profile Rules*, certain *Options* and the autonomy allowed to the firewall computer user.

When logged on, *NetOp Desktop Firewall* automatically refreshes its logon at regular short intervals to update its *Security Policy* by synchronization.

NetOp Policy Server centrally logs *NetOp Desktop Firewall* events to enable full control of an environment protected by *NetOp Desktop Firewalls*.

1.3 Documentation

NetOp Desktop Firewall comes with a printed Quick Guide that explains installation and how to start using *NetOp Desktop Firewall*. The Quick Guide is also available as a Portable Document Format (PDF) file on the product CD.

The User's Manual that is available as a PDF file on the product CD contains these chapters:

- 1 Introduction: Explains product features, documentation, updates and common controls.
- 2 Installation: Explains installation, setup, change and removal.
- 3 NetOp Desktop Firewall: Explains the functionality of *NetOp Desktop Firewall*.
- 4 How NetOp Desktop Firewall Works: Explains how *NetOp Desktop Firewall* works.

NetOp Desktop Firewall Help that contains the same information as the User's Manual is available from *NetOp Desktop Firewall* windows. In windows with a menu bar, select the *Help* menu *Contents* command. In windows with toolbars, click the *Help* toolbar *Contents* button. Generally, press F1 to open *NetOp Desktop Firewall Help* displaying the topic explaining the displayed window.

To open *NetOp Desktop Firewall Help* when no *NetOp Desktop Firewall* window is displayed, run (double-click) the *NDFEnUs.chm* file that resides in the directory where *NetOp Desktop Firewall* is installed.

NetOp Desktop Firewall Help contains these main sections:

- *Introduction*: Explains product features, documentation, updates and common controls.
- *Installation*: Explains installation, setup, change and removal.
- *NetOp Desktop Firewall*: Explains the functionality of *NetOp Desktop Firewall*.
- *How NetOp Desktop Firewall Works*: Explains how *NetOp Desktop Firewall* works.

The *NetOp Desktop Firewall Help* window left *Contents* tab contains a graphical table of contents. Find topics and window explanations from the *Index* tab. Find topics containing specified words from the *Search* tab.

1.3.1 Typographical Conventions

The documentation uses these typographical conventions:

Italics text represents screen text.

SMALL CAPS text represents a keyboard key. A + between keys signifies that keys must be pressed at the same time.

Lucida Console font text represents an entry from the keyboard.

In *Help* systems, [colored underlined](#) text represents a jump hotspot. Click a hotspot to jump to the topic explaining the underlined subject.

[Square brackets] enclosing text signify an optional entry.

<Angle brackets> enclosing text signify a content description.

1.3.2 Standard Buttons

While the documentation aims to explain all window elements, it will explain these standard buttons only if their functionality is different from their standard functionality:

OK: Click this button to close the window applying selections in the window.

Cancel: Click this button to close the window without applying selections in the window.

Help: Click this button or press F1 to open the *Help* system on the topic explaining the displayed window.

1.4 Updates

NetOp Desktop Firewall may be improved from time to time through the release of updated versions.

The *NetOp Desktop Firewall* window *Tools* menu contains a *Check for New Updates...* command. You should select this command regularly to connect to the *NetOp* website to check if a newer version of your installed product is available. If this is the case, download and install it to always have the newest version of the product installed on your computer.

The *NDFReadMe.txt* file accompanying an updated version will explain what has been updated from older versions of the product.

The Quick Guide, this User's Manual and *NetOp Desktop Firewall Help* may also be updated from time to time. This documentation cannot be expected to be fully updated at all times, so always check *NDFReadMe.txt* for the latest update information.

1.5 Common Controls

The user interface contains elements with common properties. The controls of some of these elements are explained in this section.

1.5.1 Window Controls

This section explains the window controls of windows with an icon at the left end of the title bar.

Click the title bar left icon, right-click anywhere in the title bar or press ALT+SPACE to display this standard window control menu:



Restore: This command is enabled and the matching button at the right end of the title bar is displayed if a window is maximized or minimized. Select this command or click the matching button to restore the window to its normal size.

Move: This command is enabled if the window can be moved. Select this command to display an arrow-pointed +. Use the keyboard arrow buttons to move the window frame. Press ENTER to execute moving the window to the frame position.

Note: Typically, move a window by dragging its title bar.

Size: This command is enabled if the window can be resized. Select this command to display an arrow-pointed +. Use the keyboard arrow buttons to display a double arrow at a window edge and move the window edge to resize the window. Press ENTER to execute resizing the window.

Note: Typically, resize a window by dragging its edges or corners.

Minimize: This command and the matching button at the right end of the title bar are enabled if a window can be minimized. Select this command or click the matching button to minimize the window. Click a task bar minimized window button or double-click a task bar tray minimized window icon to restore the window.

Maximize: This command and the matching button at the right end of the title bar are enabled if a window can be maximized. Select this command or click the matching button to maximize the window.

Close: Select this command, click the matching button at the right end of the title bar, press ALT+F4 or double-click the title bar icon to close the window without applying selections in the window. If the open window represents a loaded program, the program will be unloaded.

1.5.2 Menu Bar and Toolbar Controls

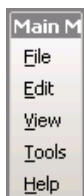
NetOp Desktop Firewall windows use Windows 2003 menu bar and toolbar controls. They are explained in this section.

A window menu is placed in a menu bar, by default below the window title bar:



The menu bar extends across the width of the window and has a handle at its left end marked by gray dots.

Drag the menu bar handle to place the menu bar along one of the borders of the window below the title bar and above any status bar or inside or outside the window as a *Main Menu* box:



Window toolbars are by default placed in one row across the width of the window below the menu bar:



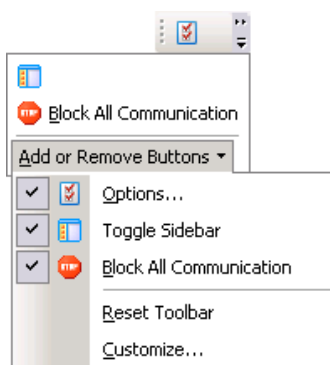
Each toolbar has a left gray dots handle and a right gray area with a down pointer button.

Drag the toolbar handle to place the toolbar along one of the borders of the window below the title bar and above any status bar, including placing toolbars in multiple rows, or inside or outside the window as a toolbox:



If the window is not wide enough to accommodate all buttons of all toolbars, some toolbars will be truncated as indicated by two *More Buttons* right pointers in the right gray area.

Click the toolbar or toolbox down pointer button to display this:



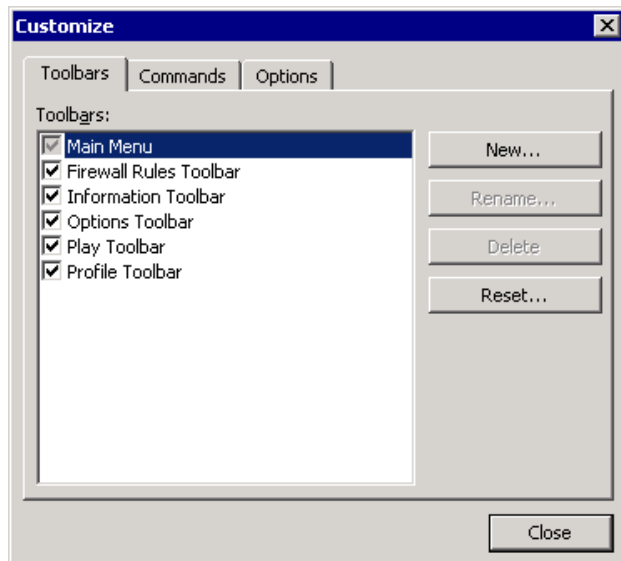
The down pointer button of a truncated *NetOp Desktop Firewall* window toolbar was clicked to display the buttons that could not be accommodated in the toolbar and an *Add or Remove Buttons* field with a down pointer button. This down pointer button was clicked to display the toolbar control menu.

The upper section of the toolbar control menu contains checkboxed commands for all buttons belonging to the toolbar. Select a command to remove/restore the checkbox. When a checkbox is removed, the button will not be displayed in the toolbar/toolbox.

The lower section of the toolbar control menu contains these commands:

Reset Toolbar: Select this command to display a confirmation window to confirm restoring all checkboxes in the upper section to display all tool bar buttons.

Customize...: Select this command to display this window:

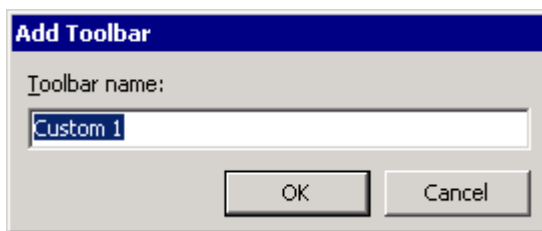


This window that customizes the toolbars of the window has the tabs *Toolbars*, *Commands* and *Options*.

Toolbars Tab

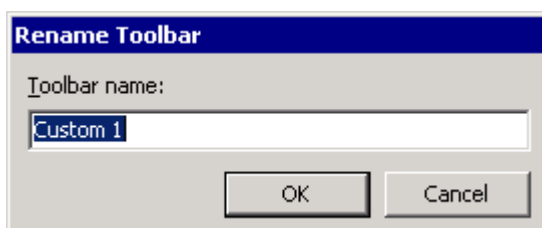
Toolbars: []: The pane contains checkboxed names of tool bars. Check/uncheck boxes (default: *Main Menu* and default tool bars checked) to display/hide tool bar sections. *Main Menu* representing the menu bar cannot be unchecked.

New...: Select this command to display this window:



Toolbar Name: []: Specify in the field a name and click *OK* to create a new user defined tool bar.

Rename...: Select a user defined tool bar in the pane and select this command to display this window:

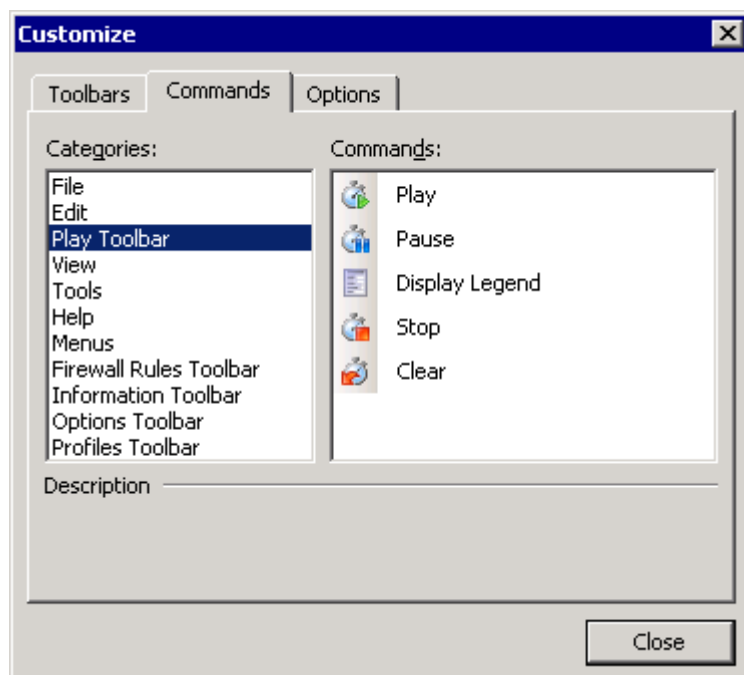


Toolbar Name: Specify in the field the new tool bar name and click *OK* to apply the new name.

Delete: Select a user defined tool bar in the pane and select this command to display a confirmation window to confirm deleting the tool bar.

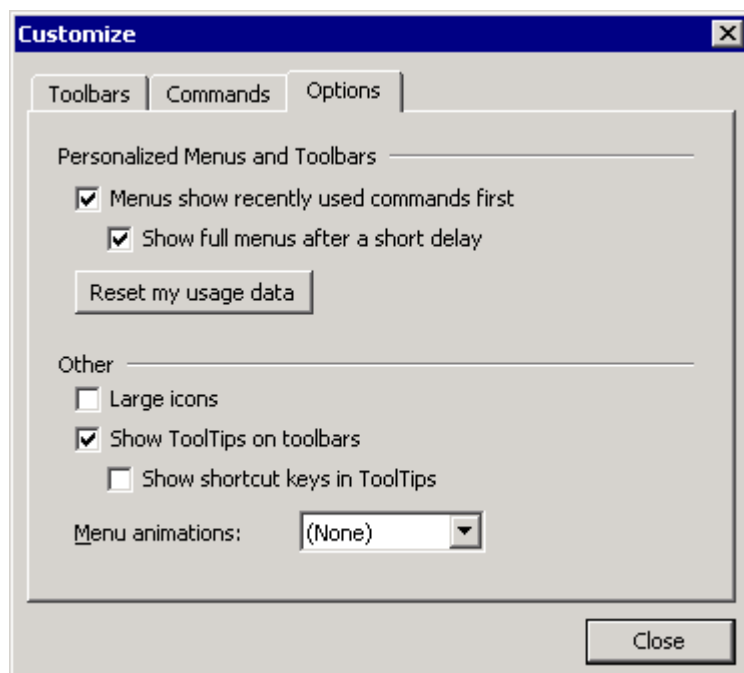
Reset...: Select a tool bar in the pane and select this command to display a confirmation window to confirm restoring all buttons in the tool bar.

Commands Tab



This tab contains a left *Categories* pane and a right *Commands* pane. Select a category in the *Categories* pane to display its commands in the *Commands* pane.

Options Tab



Personalized Menus and Toolbars

[] Menu show recently used commands first: Check this box (default: checked) to display initially only recently used commands in menus.

[] Show full menus after a short delay: Check this box (default: checked) to display the full menu content after displaying only recently used commands for a while.

Common Controls

Reset my usage data: Click this button to delete usage data determining which menu commands are displayed initially.

Other

[] Large icons: Check this box (default: unchecked) to display 32x32 pixel tool bar icons instead of 16x16 pixel tool bar icons.

[] Show ToolTips on toolbars: Check this box (default: checked) to display an explanatory text after leaving the mouse pointer on a tool bar button for a while.

[] Show shortcut keys in ToolTips: Check this box (default: unchecked) to display shortcut key sequences after ToolTip text.

Menu animations: *[]:* The drop-down box field displays the selected menu animation determining how a menu displays when selected (default: *(None)*). The drop-down list contains a range of options. Select an option in the list to display it in the field.

1.5.3 Table Controls

Typically, these controls are available with tables in window panes:

Resize the pane by resizing the window by dragging its borders. Change the width of a column by dragging the right border of its heading. Sort records (ascending/descending) by any column by clicking the column heading. If table contents extend beyond the pane, it has scroll bars.

Click a record to select and highlight it. Click a record and while pressing **SHIFT** click another record to select and highlight both records and records in between. Click a record and while pressing **CTRL** click other records to select and highlight clicked records.

2 Installation

2.1 Summary

This chapter explains how to install *NetOp Desktop Firewall* on computers running on the operating systems Windows 2000 or XP.

It contains the sections:

- System Requirements, see section 2.2, "System Requirements"
- Before Install, see section 2.3, "Before Install"
- Install, see section 2.4, "Install"
- Setup Wizard, see section 2.5, "Setup Wizard"
- Change or Remove, see section 2.1, "Change or Remove"

2.2 System Requirements

These system requirements apply when installing this version of *NetOp Desktop Firewall* on a computer:

Computer	Intel Pentium processor 233 MHz or higher or 100% compatible.
Memory	Operating System requirement plus additional 16 MB RAM (32 MB recommended).
Video	Any 100% VGA compatible graphics adapter supported by Windows
Disk space	10 MB free disk space.
Platform	Windows XP Professional Windows XP Home Edition Windows 2000 Professional
Communications	At least one network adapter or modem TCP/IP: Winsock 2 or compatible Internet access

Note: *NetOp Desktop Firewall does not support any server platforms.*

2.3 Before Install

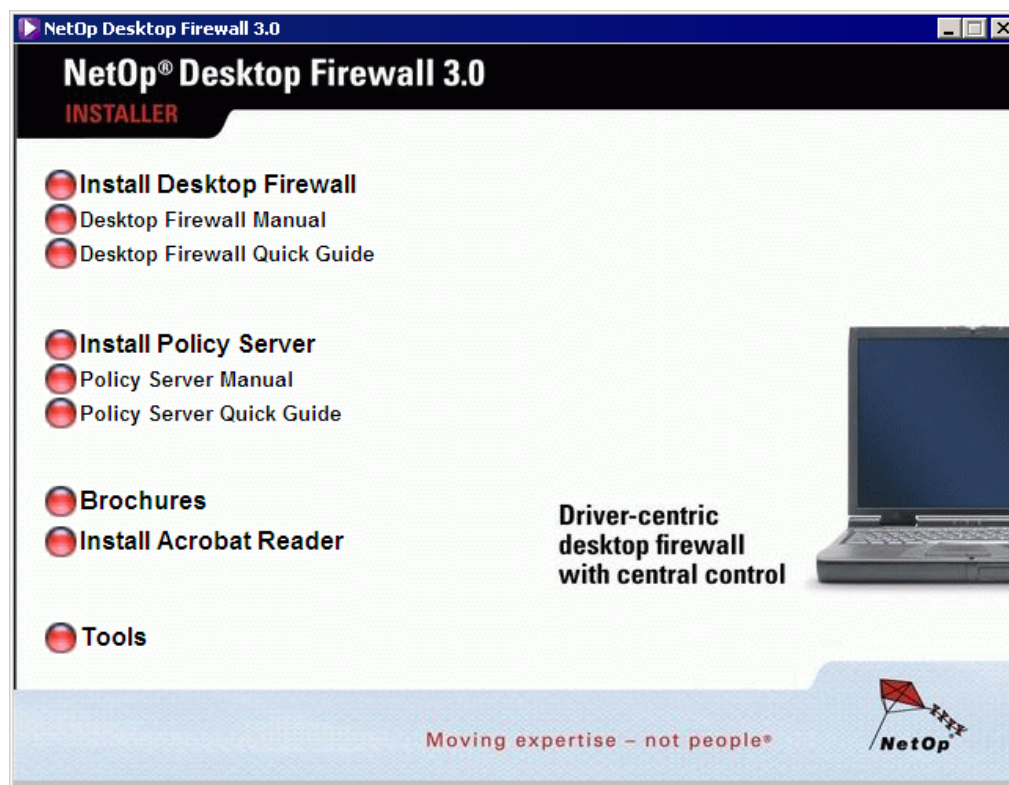
Before installing, read the *NDFReadMe.txt* file that resides in the root directory of the CD. This file contains important general information and may contain update information that was not available when this documentation was last edited.

- 1 Uninstall other firewalls.
- 2 Scan your computer with an updated anti virus product.
- 3 Save all data and shut down all running Windows applications.

Note: *To install a licensed version of NetOp Desktop Firewall, the computer must be connected to the Internet. If connected to the Internet by a dial-up connection, the dial-up connection must be running.*

2.4 Install

Insert the CD into the CD drive of your computer to display this window:



Note: If the NetOp Desktop Firewall screen does not display automatically, navigate to the root directory of the NetOp Desktop Firewall CD and double-click Setup.exe.

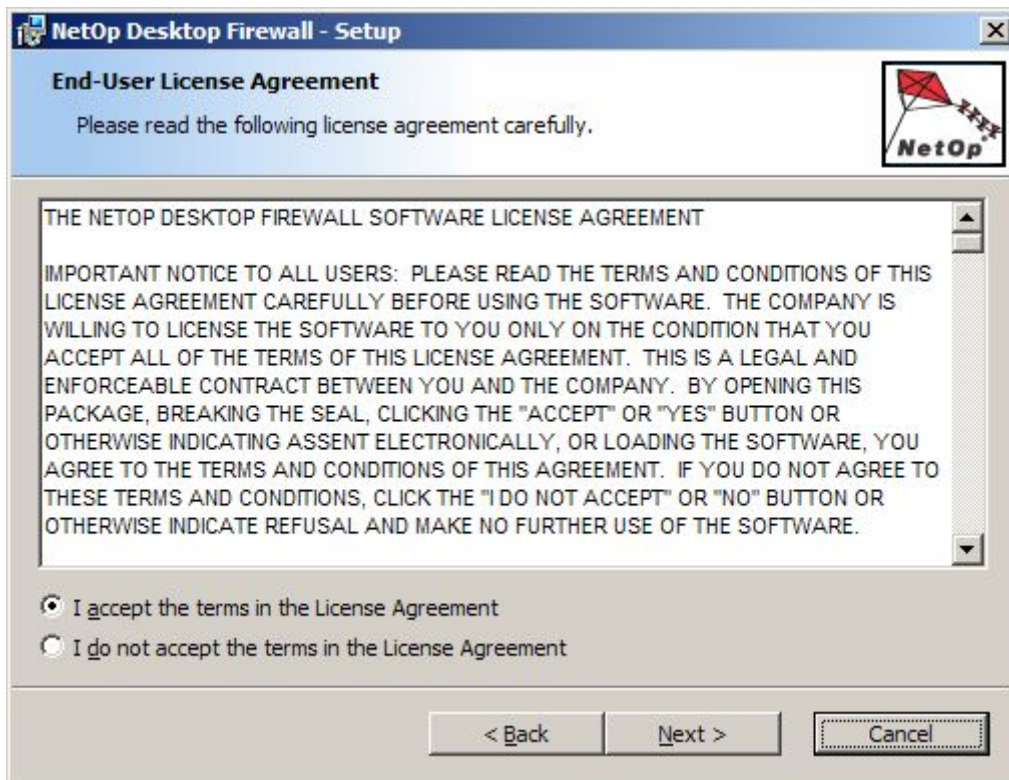
This window contains menu buttons for the options available from the CD:

- *Install Desktop Firewall:* Click this button to start installing *NetOp Desktop Firewall*.
- *Desktop Firewall Manual:* Click this button to display the *NetOp Desktop Firewall User's Manual* as a Portable Document Format (PDF) document.
- *Desktop Firewall Quick Guide:* Click this button to display the *NetOp Desktop Firewall Quick Guide* as a PDF document.
- *Install Policy Server:* Click this button to start installing *NetOp Policy Server*.
- *Policy Server Manual:* Click this button to display the *NetOp Policy Server User's Manual* as a PDF document.
- *Policy Server Quick Guide:* Click this button to display the *NetOp Policy Server Quick Guide* as a PDF document.
- *Brochures:* Click this button to display a window with NetOp product brochures options.
- *Install Acrobat Reader:* Click this button to install Adobe Acrobat Reader that must be installed on your computer to display PDF documents.
- *Tools:* Click this button to find the Transform-file. Use this file if you want to distribute *NetOp Desktop Firewall* over the network to a number of units (computers and workstations). Clicking this button opens a new page from where the *Installer Transform* application can be started. For more information, see section 2.5.1, "Installation Alternatives".

Click *Install Desktop Firewall* to display this window:



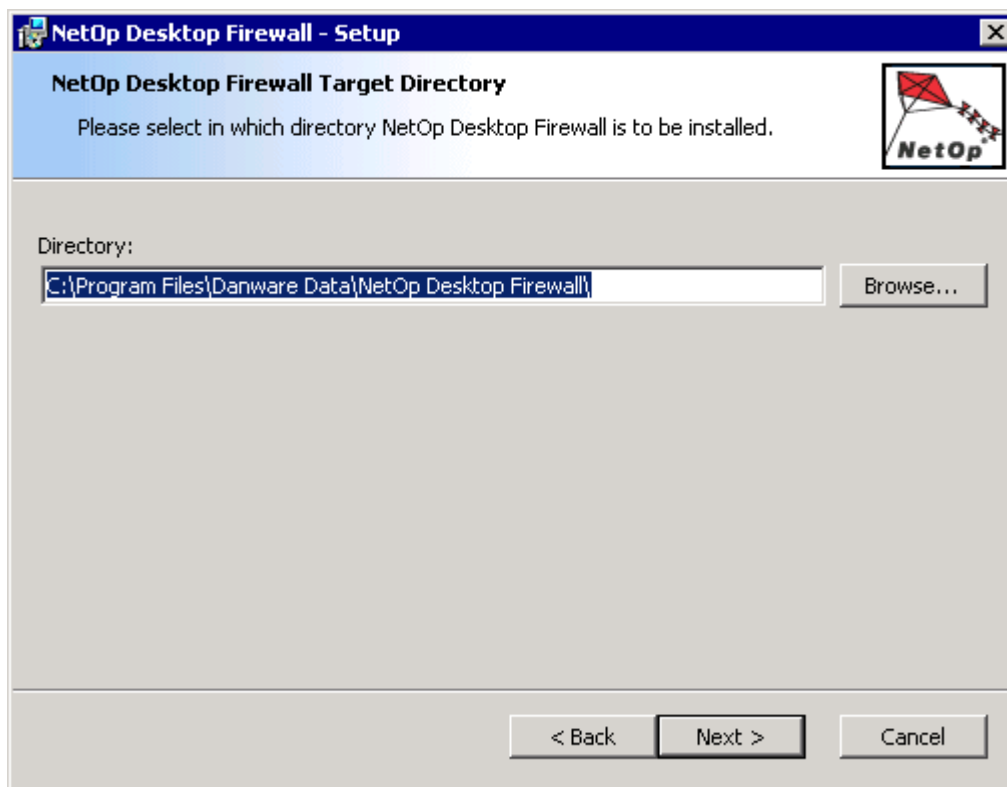
Click *Next >* to display this window:



Select one of the options:

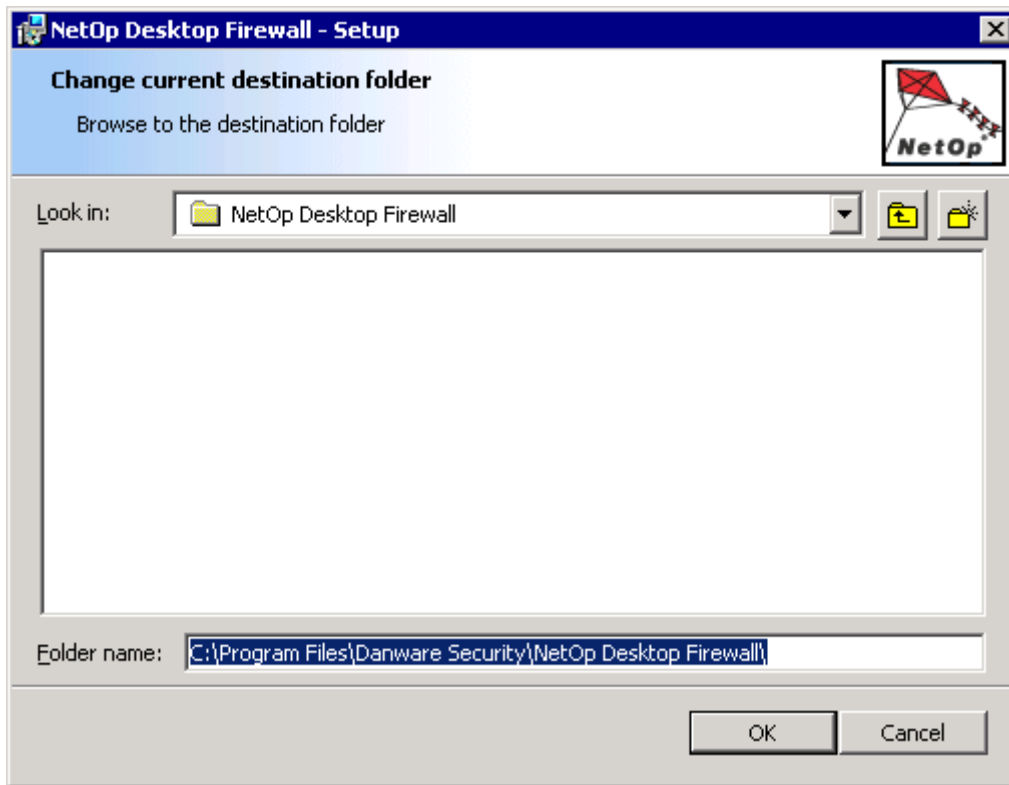
() I accept the terms in the License Agreement: Click this button to enable the *Next >* button.

() I do not accept the terms in the License Agreement: Click this button to leave the setup wizard.
Click *Next >* to display this window:



Directory: The default destination directory path is displayed in the field (default: *C:\Program Files\Danware Security\NetOp Desktop Firewall*).

Browse: Click this button to display this window:



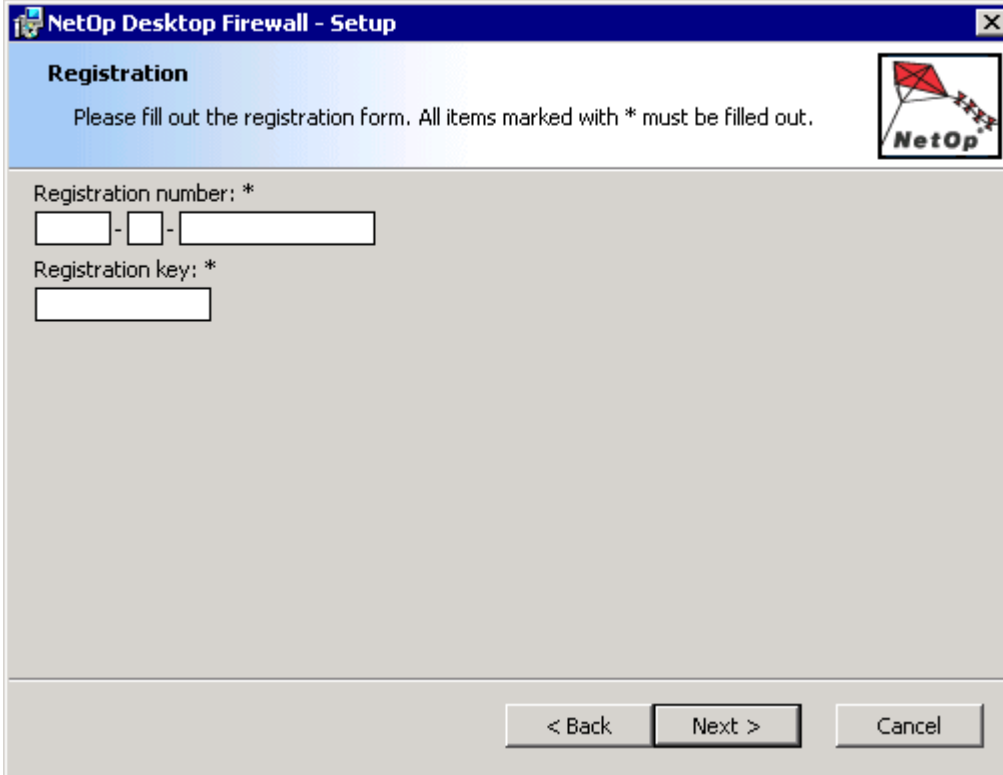
Look in: This drop-down box field displays the selected destination directory. The drop-down box field contains directories on the computer. Select a directory in the list to display it in the field to display the directories under it in the pane below.

Folder name: Select a directory in the pane to display its path in this field.

Click OK to close this window and specify the *Folder name:* path in the *Target Directory* window *Directory:* field.

Note: *The Install Directory must be on the same directory as Windows.*

Click *Next >* to display this window unless a trial version of the product is being installed:



The image shows a Windows-style dialog box titled "NetOp Desktop Firewall - Setup". The window has a blue header bar with the title and a close button. Below the header, the word "Registration" is displayed in bold. A message reads: "Please fill out the registration form. All items marked with * must be filled out." In the top right corner of the main area, there is a logo for NetOp, which features a red kite and the text "NetOp".

The registration form contains two fields:

- "Registration number: *" with three input boxes separated by hyphens.
- "Registration key: *" with a single input box.

At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

The user license must be registered with the manufacturer to enable full firewall functionality.

Registration number: Specify in the fields your registration number.

Registration key: Specify in the field your registration key.

Click *Next >* to display this window:

Registration Wizard

NetOp Desktop Firewall Service 3.0
Please fill out Registration Form, all items marked with * must be filled out

Full name: *
Peter Hansen

Company name:
YourCompany

Address:
[Empty]

Address 2:
[Empty]

City: [Empty] State/Region: [Empty] Country: *
Denmark

E-mail address: *
ph@yourcompany.dk

Verify E-mail address: *
ph@yourcompany.dk

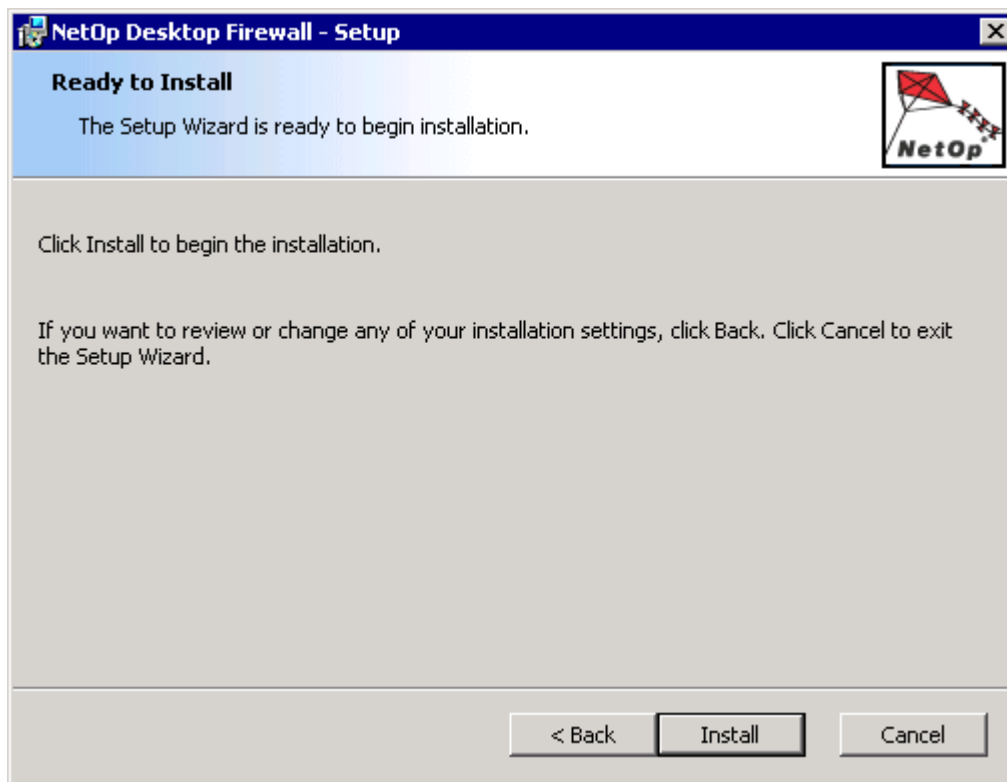
< Back Next > Cancel

The fields marked with an asterisk must be filled in.

Click *Next >* to submit the registration.

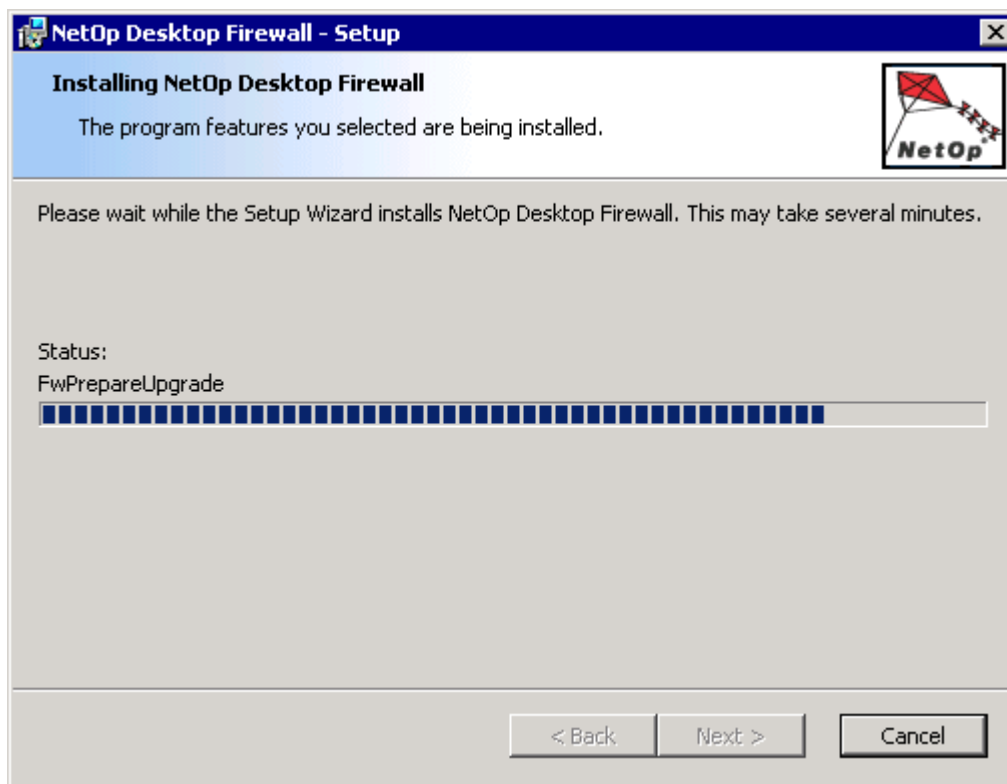
Note: Registered information will be displayed in the About NetOp Desktop Firewall window, see section 3.2.2, "Notification Area Button Menu".

When registered, this window will be displayed:



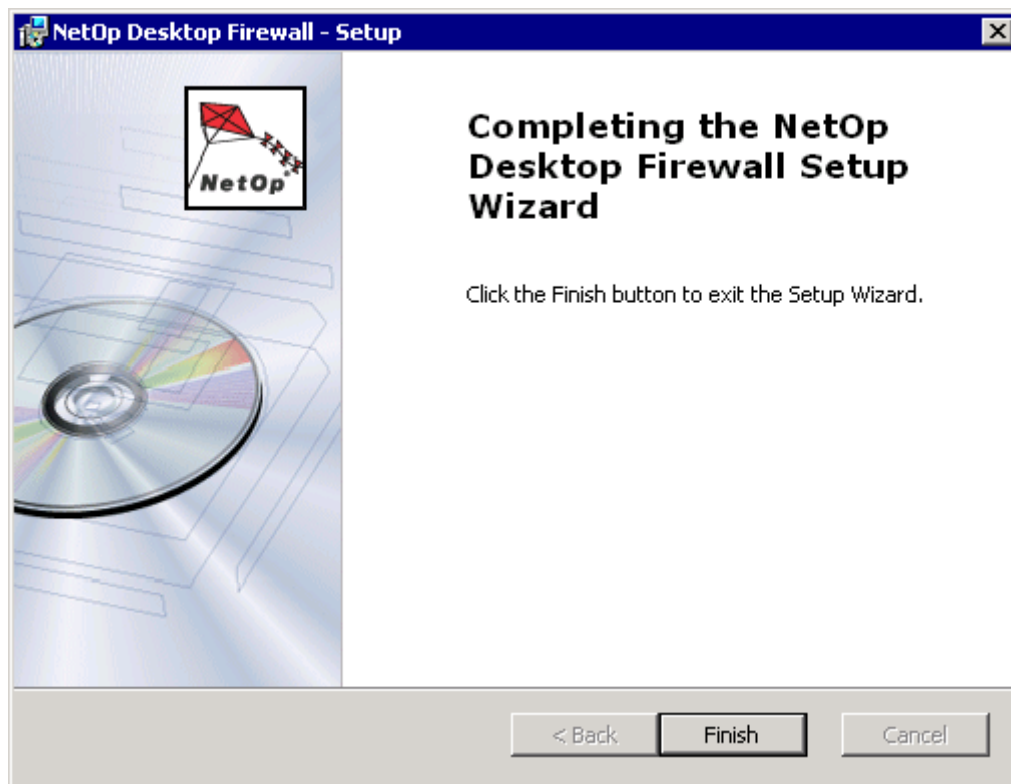
Click *< Back* to return to the previous window to change specifications.

Click *Install* to start installation and display this window:

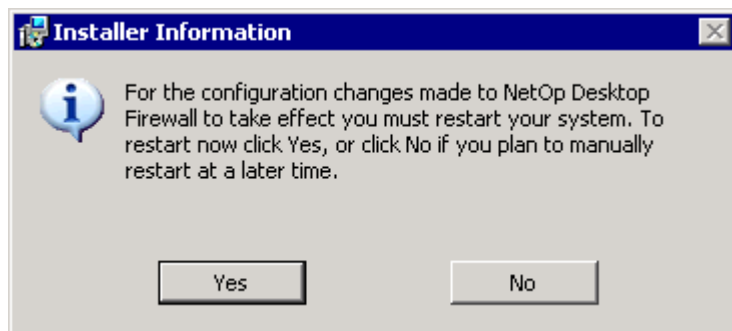


During installation, progress will be displayed in the colored blocks progress bar.

When the firewall has been installed, this window will be displayed:



Click *Finish* to leave the installation program and display this window:



Yes: Click this button to close the window and restart the computer.

No: Click this button to close the window without restarting the computer.

Note: *Until the computer is restarted, NetOp Desktop Firewall will not be operational and not affect communication across the computer communication interface.*

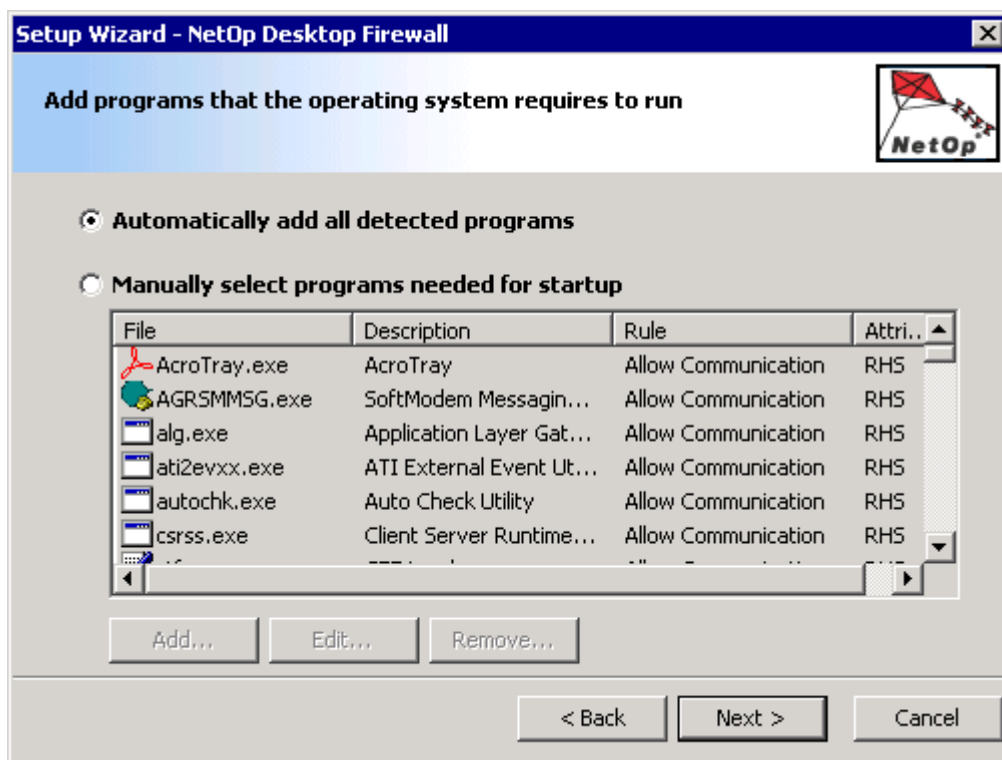
2.5 Setup Wizard

When the computer has been restarted after initial installation or when *Run Setup Wizard...* is selected in the *Tools* menu, this window will be displayed:



Note: We recommend running this setup wizard on your usual local area network after initial installation to automatically configure NetOp Desktop Firewall for a smooth computer startup.

Click *Next >* to display this window:



Setup Wizard

After initial installation and computer restart, *NetOp Desktop Firewall* records all programs that started running after computer restart and lists them in the table of this window.

The setup wizard suggests to assign to them the firewall rule *Allow Communication* as shown in the *Rule* column and the attributes *Read-only*, *Hidden* and *System* as shown in the *Attributes* column to secure a smooth computer startup in the current environment.

Firewall rules and attributes are explained in *Programs*, see section 3.3.5.1.1, "Programs"

If running the setup wizard later from the *Tools* menu, this table contains the *Program* firewall rules and attributes specified in the *Programs* display pane.

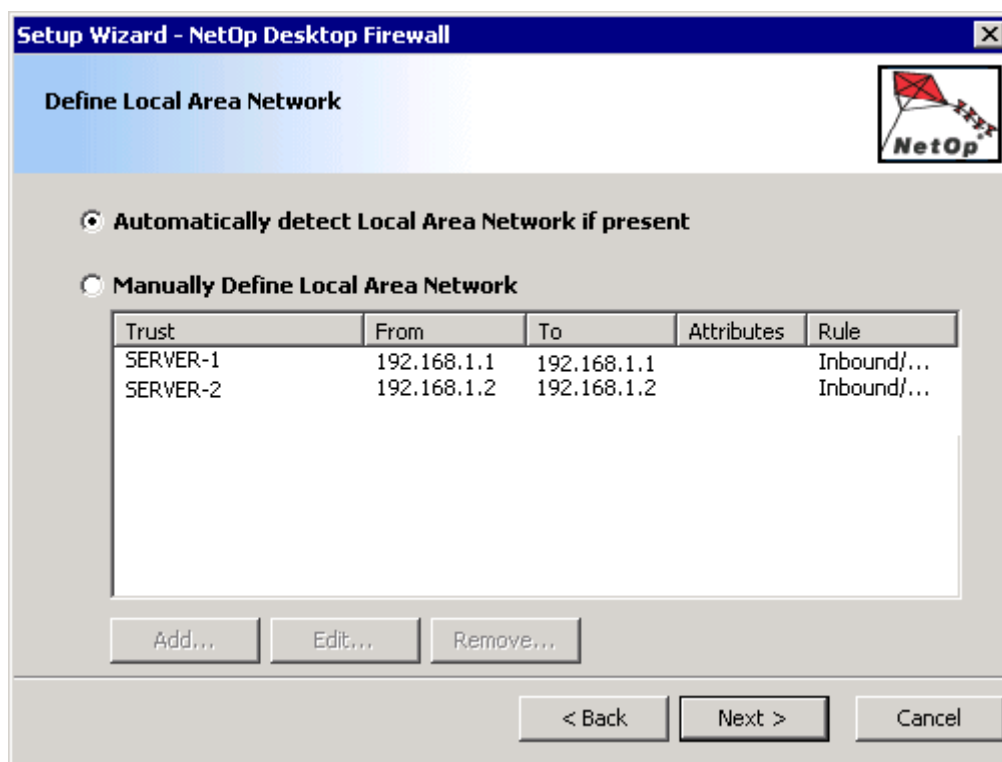
Select one of the options:

() Automatically add all detected programs: Select this option (default selection) to accept the table contents.

() Manually select programs needed for startup: Select this option to enable editing the table contents.

Note: *We generally recommend the default selection.*

Click *Next >* to display this window:



After initial installation and computer restart, *NetOp Desktop Firewall* detects the names and addresses of local area network computers connected to during computer restart and lists them in the table of this window.

The setup wizard suggests to assign to them the firewall rule *Inbound/Outbound Trust* as shown in the *Rule* column and no attributes as shown in the *Attributes* column to secure a smooth computer startup in the current environment.

Firewall rules and attributes are explained in *Trusted Nets*, see section 3.3.5.1.4, "Trusted Nets"

If running the setup wizard later from the *Tools* menu, this table contains the *Trusted Net* firewall rules and attributes specified in the *Trusted Nets* display pane.

Select one of the options:

() Automatically detect Local Area Network if present: Select this option (default selection) to accept the table contents.

() *Manually Define Local Area Network*: Select this option to enable editing the table contents.

Note: *We generally recommend the default selection.*

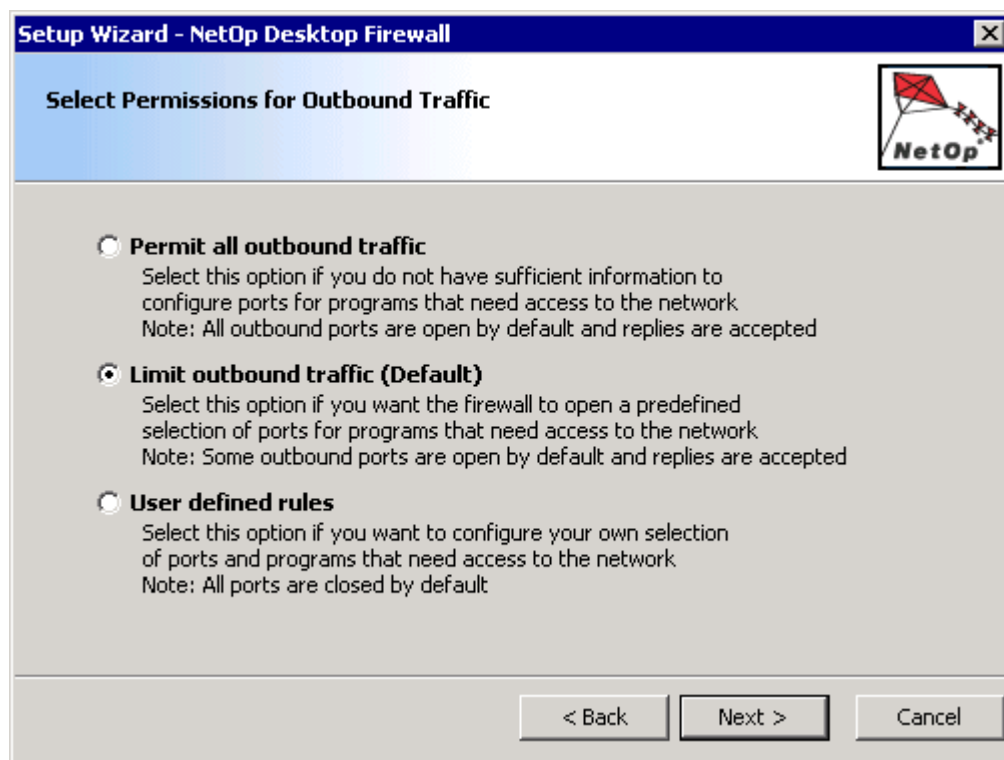
If restarting the computer after initial installation without being connected to your usual local area network, no local area network computers will be detected and no trust with them will be suggested.

There will be long delays starting the pc up if LAN trusts are required but not specified. Lack of LAN trusts will cause the firewall to block inbound network communication.

To avoid long delays, manually define local area network computers in the table.

Alternatively, before starting up the computer connected to the local area network specify all available IP addresses (0.0.0.0 to 255.255.255.255) as a *Trusted Net*. This will make the setup wizard run upon startup an replace the all available IP addresses trust by trusts with local area network computers connected to during computer startup.

Click *Next >* to display this window:



By default, the *Port* firewall rule *Outbound Traffic* is assigned to a predefined selection of commonly used ports. This window offers the alternatives of assigning one of the firewall rules *Outbound Traffic* or *Blocked in Both Directions* to all available port numbers (0-65535).

Firewall rules and attributes are explained in *Ports*, see section 3.3.5.1.2, "Ports"

Select one of the options:

() *Permit all outbound traffic*: Select this option to assign the firewall rule *Outbound Traffic* to all available port numbers.

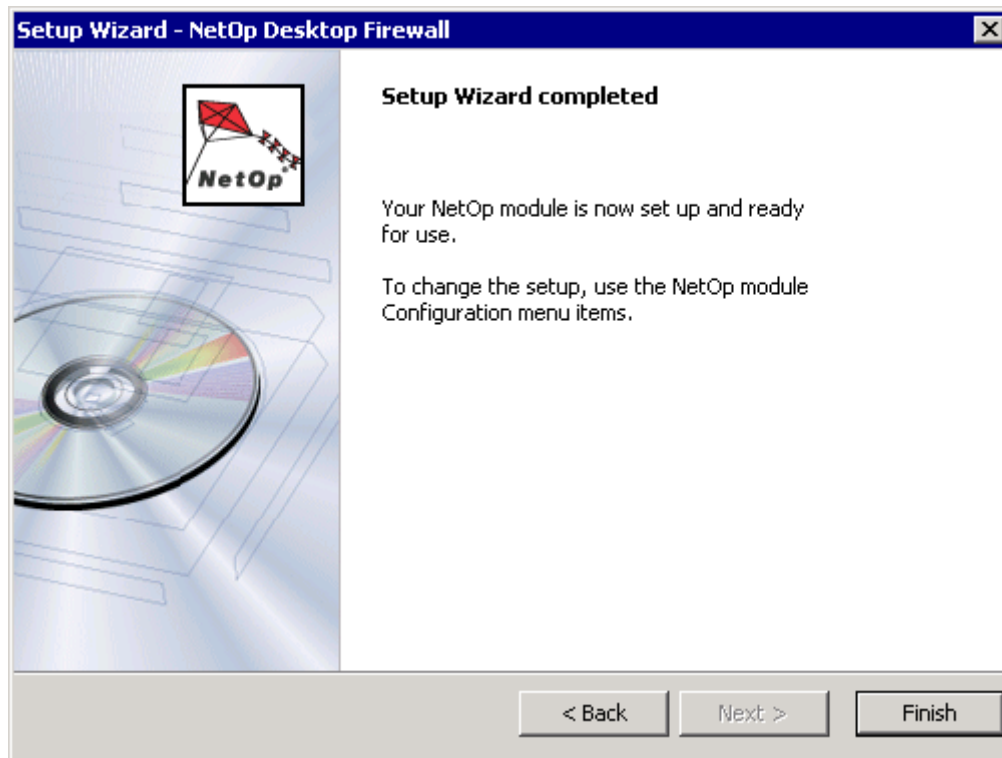
This selection matches checking the *Options* window *General* tab *Outbound Traffic Permissions* section *Permit traffic on all outbound ports* box, see section 3.5.1.1, "General Tab".

() *Limit outbound traffic (Default)*: Select this option (default selection) to apply the firewall rules assigned in the *Ports* display pane (default: *Outbound Traffic* for all specified ports).

() *User defined rules*: Select this option to assign the firewall rule *Blocked in Both Directions* to all available port numbers to open individual ports manually afterwards.

Note: *We generally recommend the default selection.*

Click *Next >* to display this window:



Click *< Back* to return to the previous wizard window to change your selections.

Click *Finish* to leave the setup wizard applying its selections.

2.5.1 Installation Alternatives

Installation alternatives enable installing *NetOp Desktop Firewall* with little or no user intervention, quietly (not displaying any windows during installation), on remote computers, in a configured state and by deployment.

The installation of *NetOp Desktop Firewall* uses Windows Installer.

The Windows Installer program *msiexec.exe* installs and removes program features specified in an installation package file with the extension *msi* according to the command syntax:

```
msiexec <Option> <Required parameter> [<Optional parameter>]
```

The command can contain multiple options and parameters.

Available options are displayed in a window when on a computer with *msiexec.exe* version 3+ (standard in newer Windows) in its `\Windows\System32\` directory running the command:

```
msiexec
```

These options are relevant for *NetOp Desktop Firewall* installation alternatives:

Option	Effect
/i	Installs the installation package <code><Product>.msi</code> in a specified directory. <code><Path>\<Product>.msi</code> is a required parameter.
/a	Unpacks the installation package <code><Product>.msi</code> in a specified directory without installing it. <code><Path>\<Product>.msi</code> is a required parameter.
/qn	Executes in quiet mode (no windows displayed) with no user interaction.
/l*v	Logs all information with verbose output in the log file <code><Log name>.log</code> . <code><Path>\<Log name>.log</code> is a required parameter.

`TRANSFORMS=<Transformation file>` is a standard optional parameter that applies transformations specified in a required format transformation file with the extension *mst*.

Other optional parameters can be used.

Note: *Command line operations are case sensitive.*

2.5.2 Command Line Installation

The next pages contain examples of command line installation and an example of deployment:

- Normal installation,
- Quiet installation,
- Installing in a configured state,
- Deployment.

Normal installation

Run this command for a normal installation from the *NetOp Desktop Firewall* installation package *setup.msi*:

```
msiexec /i <Path>\setup.msi
```

Note: *If a parameter contains spaces, it must be enclosed by double quotation marks.*

This is actually the command that is run from the *Install Desktop Firewall* button in the CD menu.

The license number and key can be specified in two added optional parameters:

```
DW_REG_NUMBER=DWS-X-XXXXXXXXX DW_REG_KEY=XXXXXXXXX
```

If these parameters are used, the window for specifying these numbers will not be displayed, and if the product has already been registered, the window for specifying personal data will not be displayed either.

Create a License Registration File

Registering during the installation creates a license registration file named *ndf.lic*, it is saved in the directory where *NetOp Desktop Firewall* is installed.

To create a *ndf.lic* file without installing, run this command:

```
msiexec /a <Path>\setup.msi
```

To specify the license number, key and personal data from a *ndf.lic* file, use this optional parameter:

```
DW_LICENSE_FILE=<Path>\ndf.lic
```

instead of the two specified above.

Quiet Installation

To install *NetOp Desktop Firewall* on multiple computers, a quiet installation with no user intervention is preferable. Run this installation command:

```
msiexec /i <Path>\setup.msi /qn DW_LICENSE_FILE=<Path>\ndf.lic
```

/qn executes the installation in quiet mode with no user intervention, *DW_LICENSE_FILE=<Path>\ndf.lic* applies the license registration file.

This can be done in two ways:

Run this command from each computer pointing to a network directory containing the *setup.msi* and *ndf.lic* files.

Place this command in a logon script distributed to selected computers to run it when users log on.

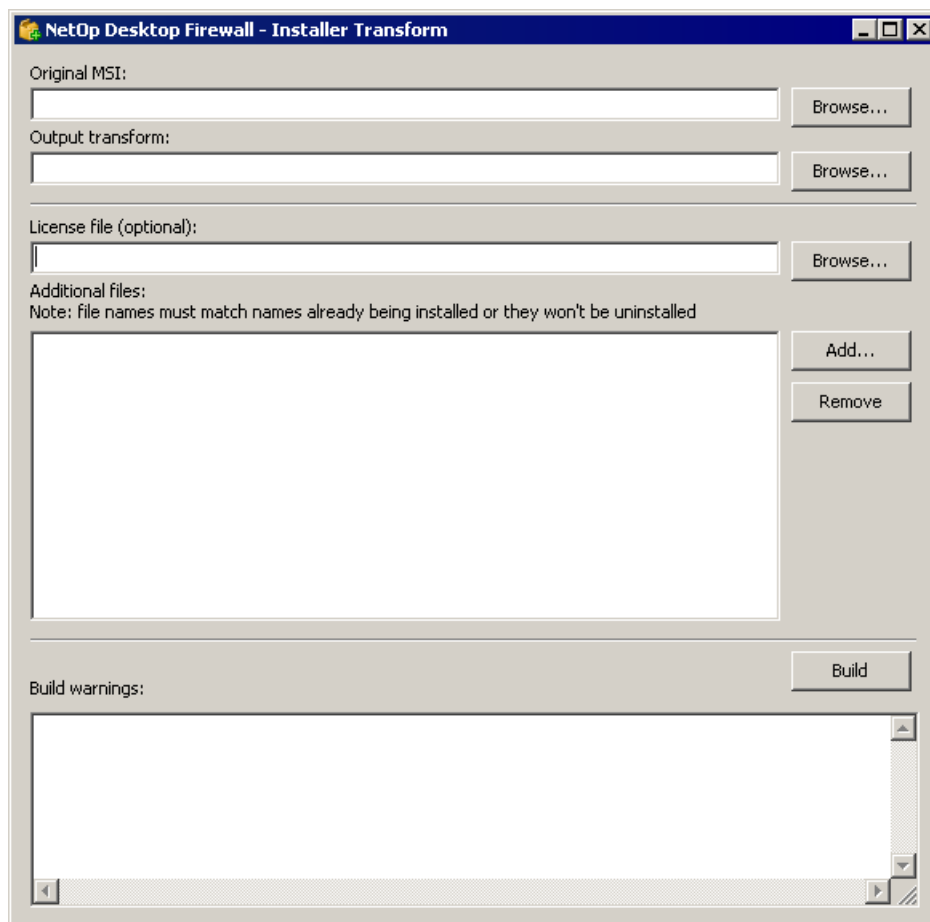
Note: *This command causes the computer to reboot without warning.*

Install NetOp Desktop Firewall in a Configured State

To make life easier for users, not least if user *NetOp Desktop Firewalls* are to be controlled from a *NetOp Policy Server*, we recommend to install them in a configured state.

To do this, first install one *NetOp Desktop Firewall* and configure it exactly as you want user firewalls to be configured.

Then, create a transformation file from the configuration of this firewall. In the CD menu, select *Tools* and, on the new page, select *Installer Transform*, or run the *ndfmst.exe* file that resides on the CD in the *\NDF\TOOLS* directory to display this window:



This window creates a *mst* transformation file from what you specify in the window.

Original MSI: *[[Browse...]]*: Preferably, you should place your installation files in the same network directory. Copy *setup.msi* from the *\install\UK* directory on the CD to your preferred network directory. Click *Browse...* to get the *setup.msi* file from your preferred network directory.

Output transform: *[[Browse...]]*: In this field enter a file name with the extension *mst*. Click *Browse...* to get the *mst*-file from your preferred network directory.

License file (optional): *[[Browse...]]*: This file by default specifies *ndf.lic* pointing to the directory where *NetOp Desktop Firewall* is installed by default. Create a license registration file, see above, and copy it to your preferred network directory. Click *Browse...* to get the *ndf.lic* file from your preferred network directory.

Verify that the entry in the field points to the *ndf.lic* file in your preferred network directory.

Additional files: *[[Add...]]**[[Remove]]*: Click *Add...* to display a Windows *Open* window. Navigate to the directory where your configured *NetOp Desktop Firewall* was installed and select and open all files with the extension *dat* to add their paths and names in the pane to apply all of the configuration of your configured *NetOp Desktop Firewall* to your *mst* file.

Note: *The contents of dat files are explained in the NDFReadMe.txt file.*

Build: Click this button to build the *mst* file. While building, look for any alarming warnings in the *Build warnings* pane.

If the build fails, review specifications and rebuild. When satisfied, close the window.

Now, make a trial installation using your *mst* file in this command:


```
msiexec /i <Path>\setup.msi TRANSFORMS=<Path>\<Preferred name>.mst  
/qn DW_LICENSE_FILE=<Path>\ndf.lic
```

Verify that the newly installed *NetOp Desktop Firewall* is configured as desired. If OK, proceed with other installations.

Logging

If the installation fails, a log file can be useful to identify when what failed. To create a log file from your installation, add this option and required parameter to your installation command:

```
/! *v <Path>\<Log name>.log
```

This will create a log file named <Log name>.log in the specified path. Open it in any text editor, e.g. Notepad.

If you want to know more about Windows Installer requirements and options, visit the www.microsoft.com website and search for “Windows Installer”.

Deployment

An example of deploying the *NetOp Desktop Firewall* to a group of users makes use of the Windows Active Directory functionality.

To do this, first install one *NetOp Desktop Firewall* and configure it exactly as you want user firewalls to be configured.

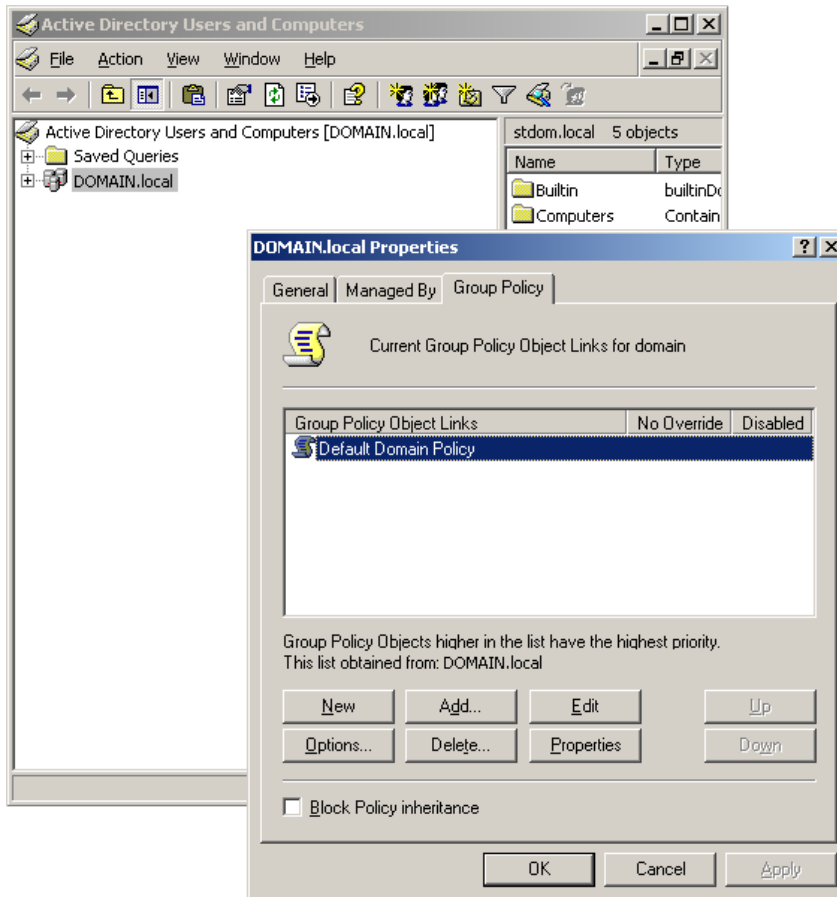
Then, create a transformation file from the configuration of this firewall. Please, refer to the previous section (page 32) for handling details.

Note: *You have to have domain administrator rights to deploy via the Active Directory.*

With the transform file ready, follow these steps:

1. Click the ‘Start’ button on the Windows taskbar, select ‘Settings’ and select Control Panel

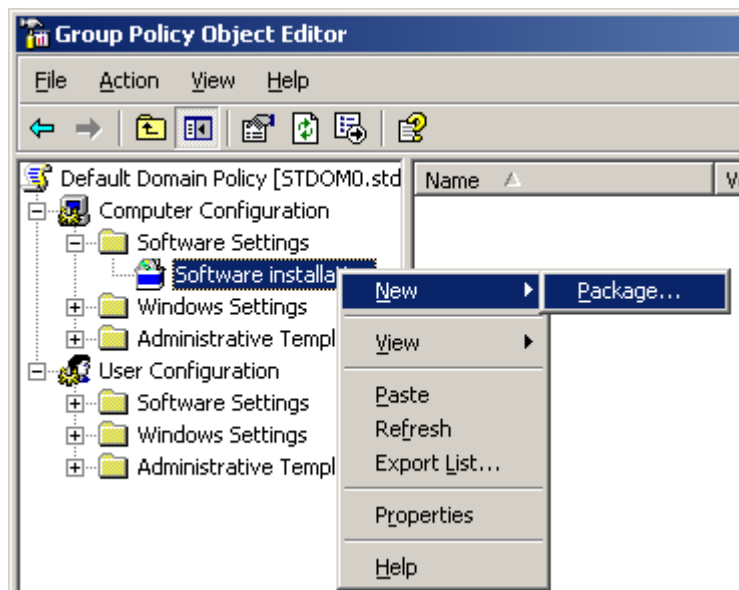
2. Select *Administrative Tools* and left-click *Active Directory Users and Computers* to open the



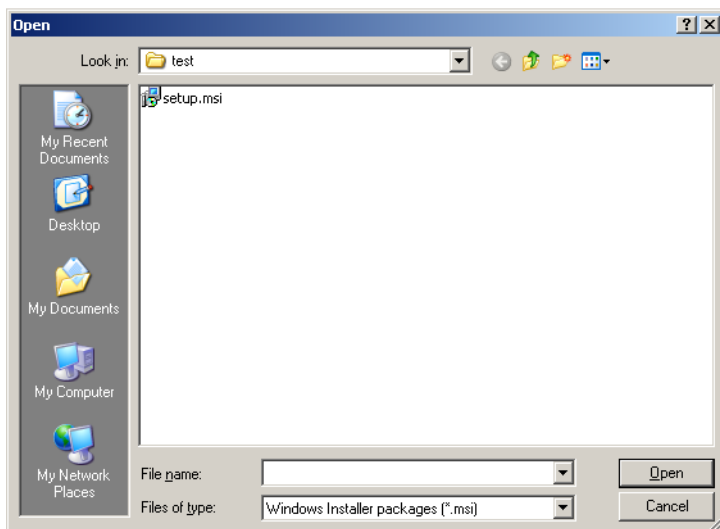
Active Directory Users and Computers file explorer. Select the domain to which you want to deploy the *NetOp Desktop Firewall* to.

Note: *It is only possible to select one domain at a time.*

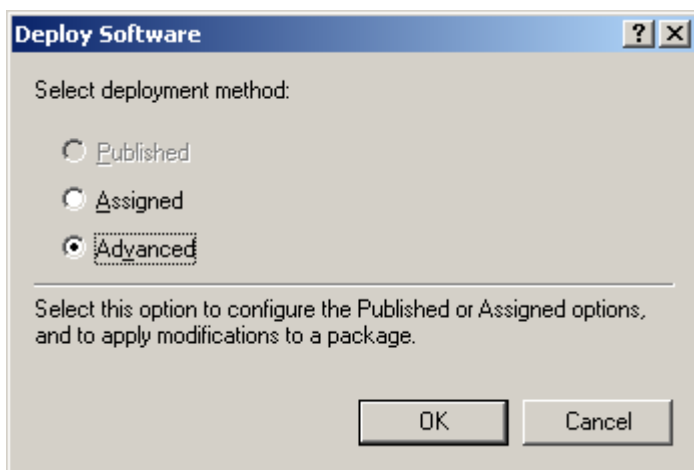
3. Right-click the domain and select *Properties*
4. Select the *Group Policy* tap and click *Edit*



5. Open the folder *Software Settings* and right-click *Software Installation*, select *New, Package*

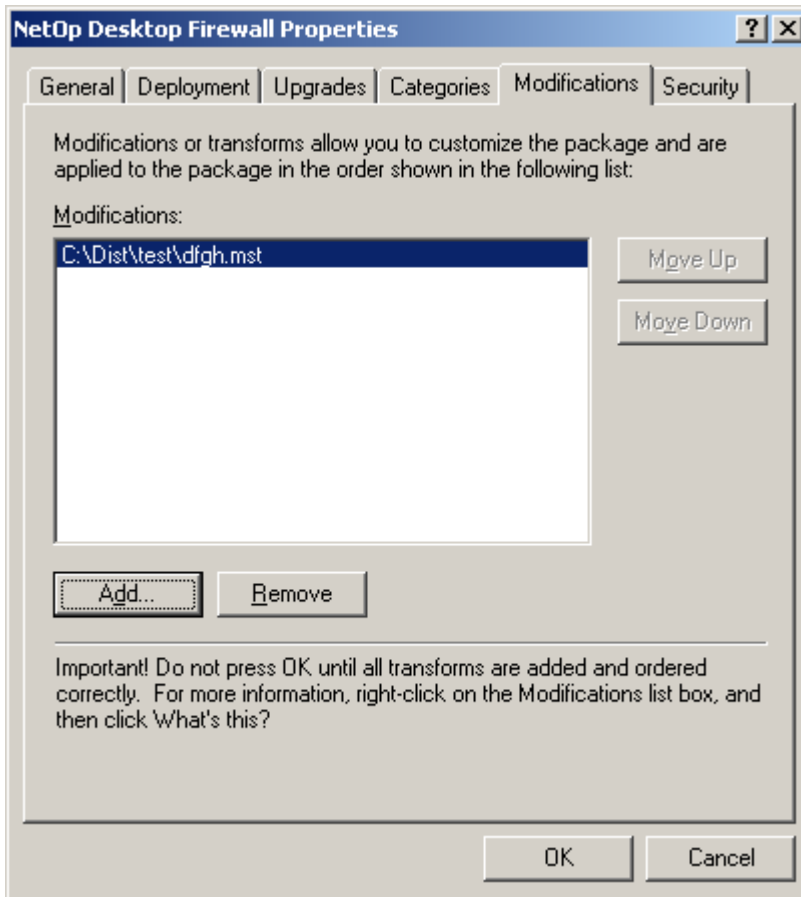


6. Locate the installation file (setup.msi) and click *Open*
7. Select *Advanced* and click *OK*



8. In the *NetOp Desktop Firewall Properties* window, select the *Modifications* pane.

9. Click *Add* to open a file explorer and locate the *.mst file



10. Click *OK* and the deployment takes place.

This completes the Active Directories Deployment.

2.1 Change or Remove

To change or remove your *NetOp Desktop Firewall* installation, select *Start > (Settings >) Control Panel* to display the *Control Panel* window. Select *Add or Remove Programs* and in the *Add or Remove Programs* window select *NetOp Desktop Firewall* to expand.

Select *Change* to change your installation, see section 2.1.1, "Change".

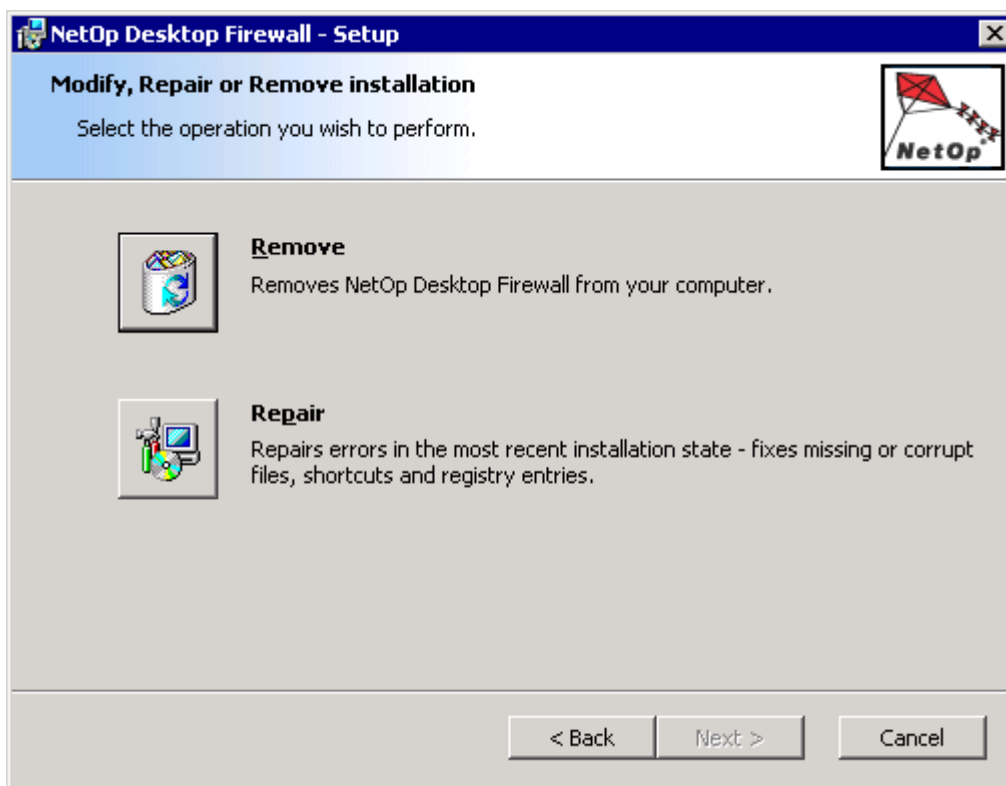
Select *Remove* to remove your installation, see section 2.1.2, "Remove".

2.1.1 Change

In the *Add or Remove Programs* window expanded *NetOp Desktop Firewall* command, click *Change* to display this window:



Click *Next >* to display this window:



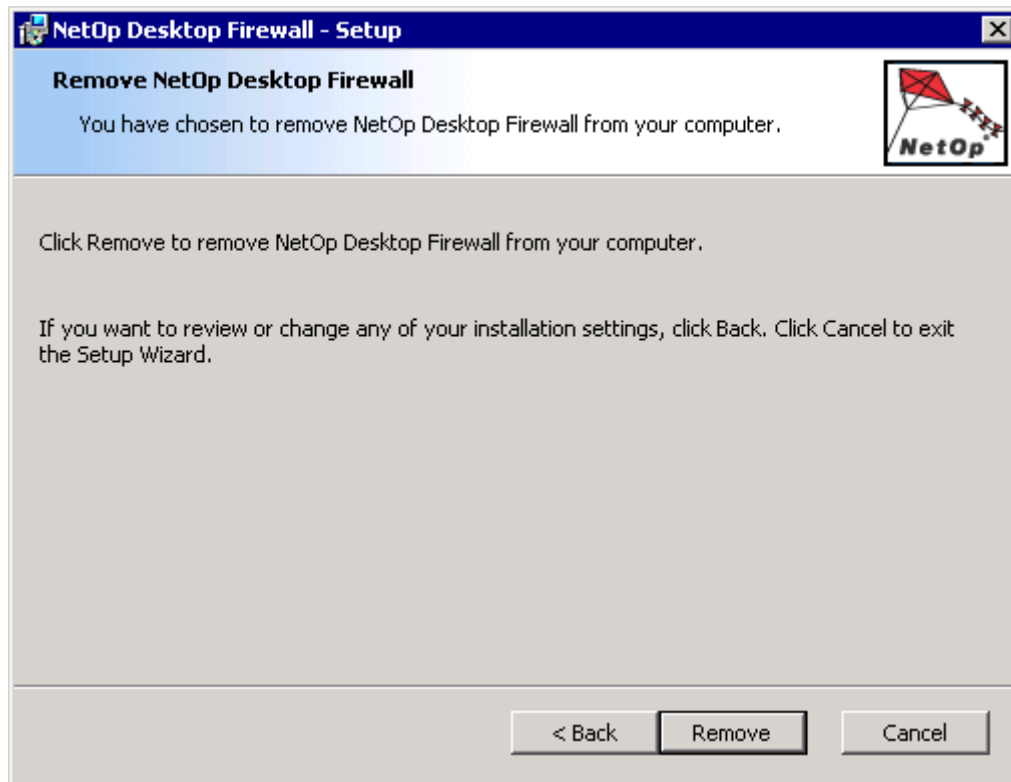
Change or Remove

The *Remove* option is explained in the “Change > Remove” subsection below.

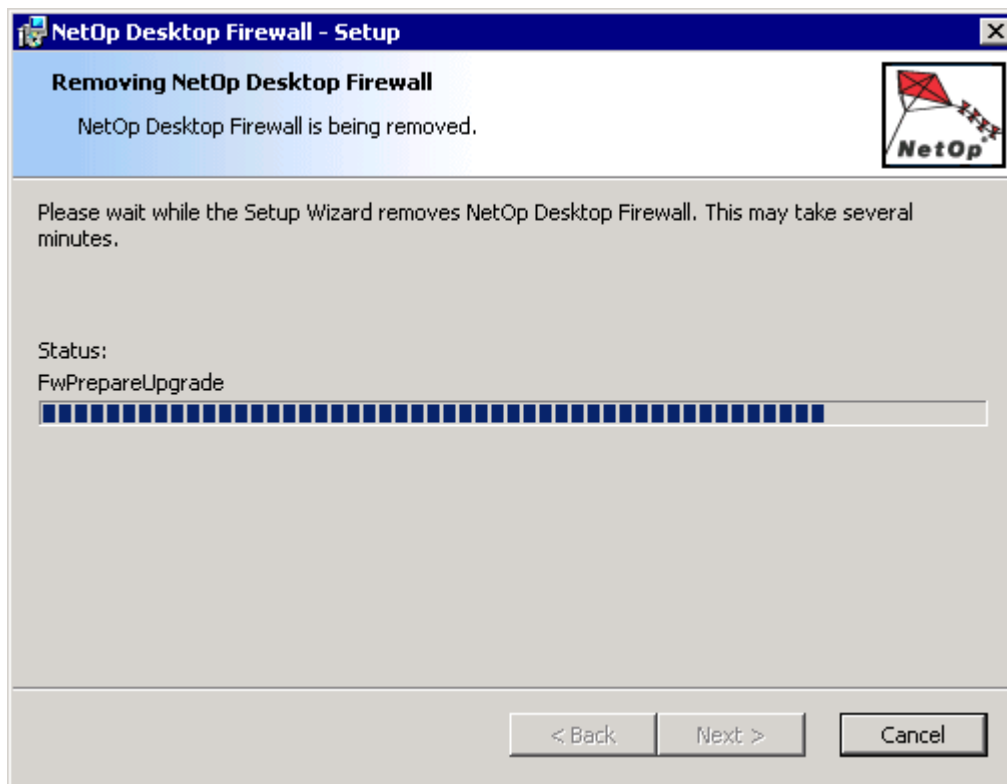
The *Repair* option is explained in the “Change > Repair” subsection below.

Change > Remove

In the *Modify, Repair or Remove Installation* window, click *Remove* and *Next >* to display this window:



This window will be displayed while the *NetOp Desktop Firewall* installation is being removed:



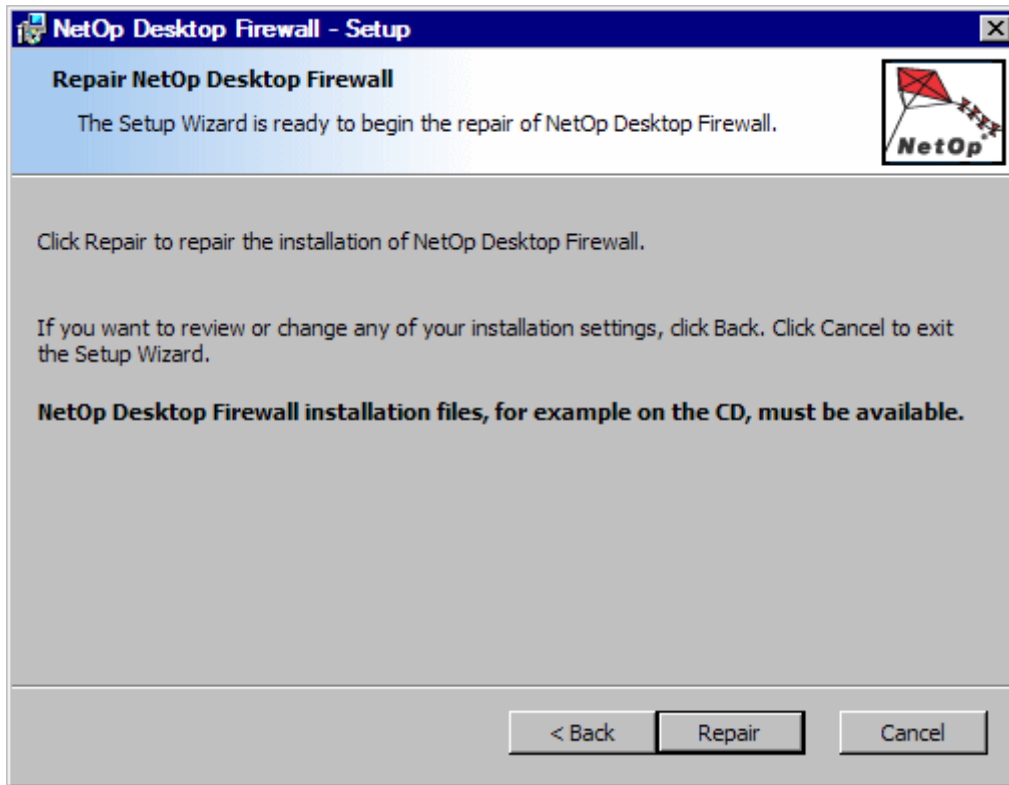
When the *NetOp Desktop Firewall* installation has been removed, the *Completing the NetOp Desktop Firewall Setup Wizard* window, see section 2.4, "Install", will be displayed.

The computer must be restarted to completely remove *NetOp Desktop Firewall*.

Change or Remove

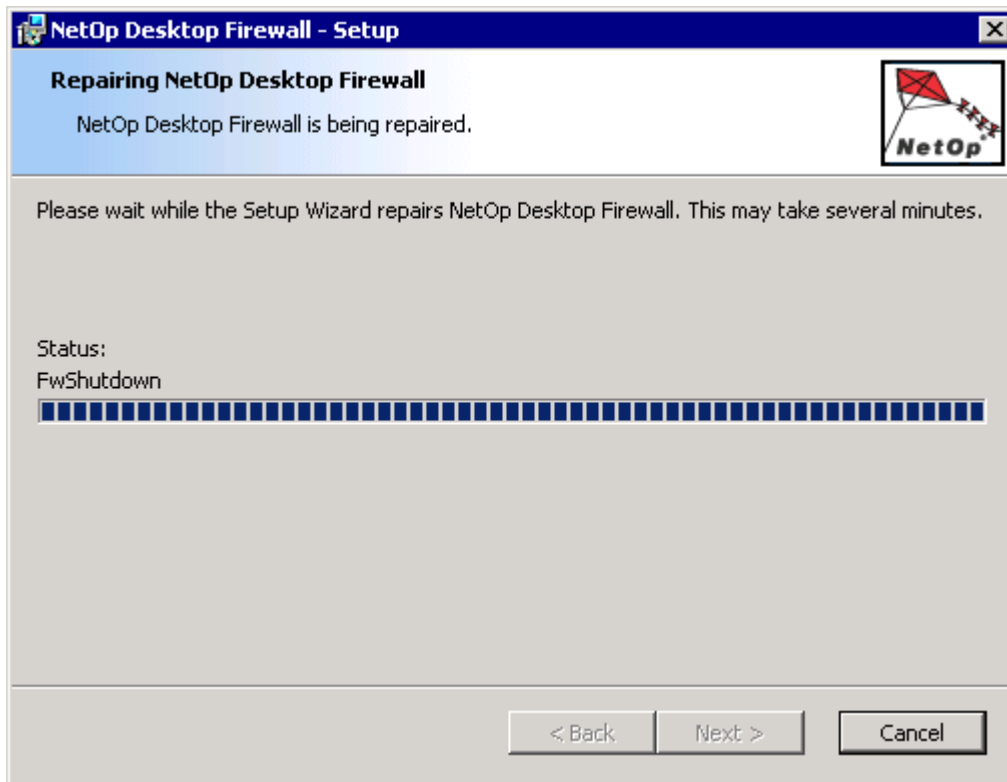
Change > Repair

In the *Modify, Repair or Remove Installation* window, click *Repair* and *Next >* to display this window:



Note: *Repair* reinstalls NetOp Desktop Firewall without changing its configuration. NetOp Desktop Firewall installation files, e.g. on the CD, must be available.

Click *Repair* to display this window while the *NetOp Desktop Firewall* installation is being repaired:

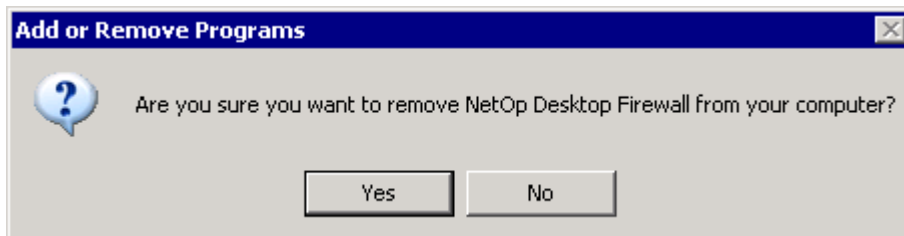


When the *NetOp Desktop Firewall* installation has been repaired, the *Completing the NetOp Desktop Firewall Setup Wizard* window, see section 2.4, "Install", will be displayed.

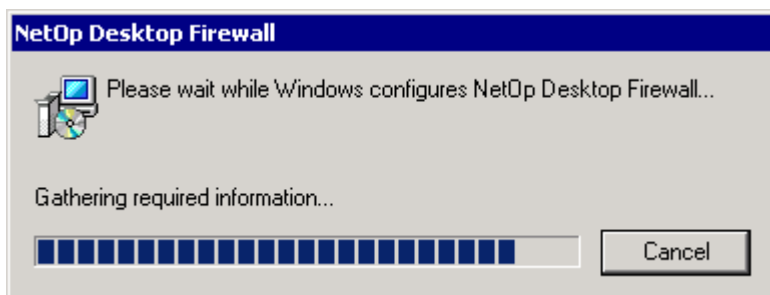
The computer must be restarted to complete the repair.

2.1.2 Remove

In the *Add or Remove Programs* window expanded *NetOp Desktop Firewall* command, click *Remove* to display this window:



Click *Yes* to display this window:



When the *NetOp Desktop Firewall* installation has been removed, the computer must be restarted to complete the removal.

3 NetOp Desktop Firewall

3.1 Summary

This chapter explains the functionality of *NetOp Desktop Firewall*.

It contains the sections:

- Startup Guide, see section 3.2, "Startup Guide"
- NetOp Desktop Firewall Window, see section 3.3, "NetOp Desktop Firewall Window"
- NetOp Desktop Firewall Tools, see section 3.4, "NetOp Desktop Firewall Tools".

3.2 Startup Guide

When *NetOp Desktop Firewall* is installed on a computer, by default this button will appear in the notification area in the lower right corner of the screen:



By default, as a stand-alone application, the background of the bars in the icon is black. The button tooltip displays *NetOp Desktop Firewall 3.0 Firewall OK*.



If *NetOp Desktop Firewall* is logged on to a *NetOp Policy Server*, see section 3.4.1.3, "Policy Server Tab", the background of the bars in the icon is yellow. The button tooltip displays *NetOp Desktop Firewall 3.0 Policy Server*.



If all communication across the computer communication interface is blocked, see section 3.2.2, "Notification Area Button Menu", the button icon displays a *Stop* sign. The button tooltip displays *NetOp Desktop Firewall 3.0 Block All*.



If *NetOp Desktop Firewall* is password protected, the button icon displays a padlock, see section 3.4.1.2, "Password Tab". The button tooltip displays *NetOp Desktop Firewall 3.0 Password Protected*.

No *NetOp Desktop Firewall* button will be displayed in the notification area if the *NetOp Desktop Firewall* window *Tools* menu *Options* command/window *General* tab *Appearance* section the *Show icon in notification area* box is unchecked, see section 3.4.1.1, "General Tab". However, user prompts and user messages will still be displayed.

Note: *If the trial period of an installed trial version of NetOp Desktop Firewall is about to expire, a reminder window will be displayed, see section 5.1, "Trial Version"*

3.2.1 Use and Configuration

When *NetOp Desktop Firewall* has been installed and automatically configured in its usual computer environment by the setup wizard using default selections, the computer will be well protected, see section 2.5, "Setup Wizard"

The typical computer user will be safe by refraining from any further configuration of the firewall and practically forget about it.

Occasionally, the firewall may display a user prompt that the user must respond to or a user message, see section 3.2.3, "User Prompts and Messages".

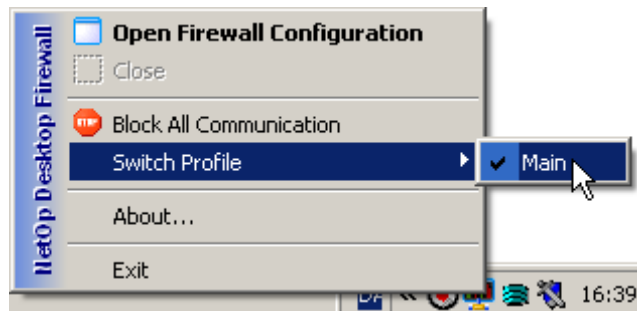
Applications using special communication may require an adjustment of default firewall rules to work satisfactorily. Typically, communication troubleshooting starts by viewing the *Packet Log* that will reveal if application communication is being blocked by the firewall, see section 3.3.5.2.2, "Packet Log".

In daily use, the user does not need to be concerned about firewall configuration. This applies even stronger to a firewall that is logged on to a *NetOp Policy Server* in a distributed firewall system, see section 3.4.1.3, "Policy Server Tab".

However, *NetOp Desktop Firewall* has a wide range of configuration options and powerful information utilities, all of which can be accessed from the *NetOp Desktop Firewall* window, see section 3.3, "NetOp Desktop Firewall Window".

3.2.2 Notification Area Button Menu

Right-click the notification area *NetOp Desktop Firewall* button to display this menu, see section 3.2, "Startup Guide":



This menu contains these commands:

Note: Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".

Open Firewall Configuration: Select this command or double-click the notification area button to display the *NetOp Desktop Firewall* window, see section 3.3, "NetOp Desktop Firewall Window".

Close: Select this command or the matching *NetOp Desktop Firewall* window title bar window control menu command or click the title bar window control *Close* button to close the *NetOp Desktop Firewall* window.

Block All/Allow Communication: Select this command (default: *Block All Communication*) or the matching *NetOp Desktop Firewall* window *Tools* menu command or click the matching *Options* toolbar button to block all/allow communication across the computer communication interface. When all communication is blocked, the notification area *NetOp Desktop Firewall* button displays a *Stop* sign, see section 3.2, "Startup Guide".

Switch Profile: This command expands into the main profile (by default named *Main*) and available sub-profiles, see section 3.3.5.3, "Profiles".

The selected profile is checkmarked. Select an unchecked profile to make it active. If profile rules prohibiting switching between profiles have been applied, it is impossible to select other profiles than the rule allows.

Note: If selecting a profile fails, it will typically be because its profile rule prohibits switching into it if its profile rule is not met, see section 3.3.5.3.1, "Profile Rules".

About...: Select this command to display this window:



This window displays the version of the installed product and license information. If you request technical support, the version number may be asked for.

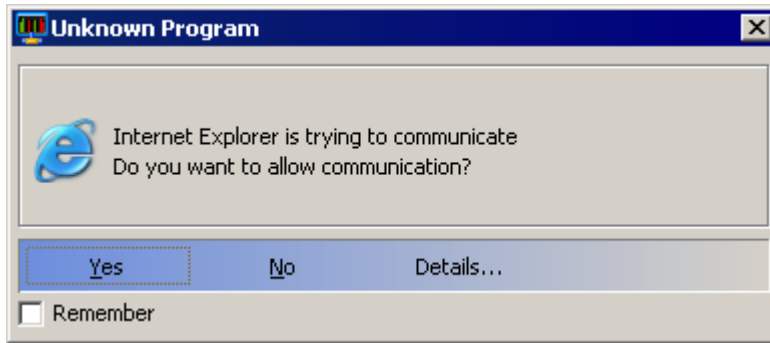
Exit: Select this command to unload the *NetOp Desktop Firewall* user interface and remove all elements of it including the notification area button from the screen. This also causes that no user messages or prompts will be displayed.

Note: *While the user interface is unloaded, NetOp Desktop Firewall continues to run on the computer. User prompts and messages will not be displayed, see section 3.2.3, "User Prompts and Messages". When the user interface is reloaded, any user prompts and messages accumulated while unloaded will be displayed.*

To load the user interface, select *Start > All > Programs > NetOp Desktop Firewall > NetOp Desktop Firewall* or run (double-click) the file *NDFConf.exe* that resides in the directory where *NetOp Desktop Firewall* is installed.

3.2.3 User Prompts and Messages

If a program that has been assigned the firewall rule *Prompt for Communication* or no firewall rule attempts communication, the user will be prompted by this window:



Note: *Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".*

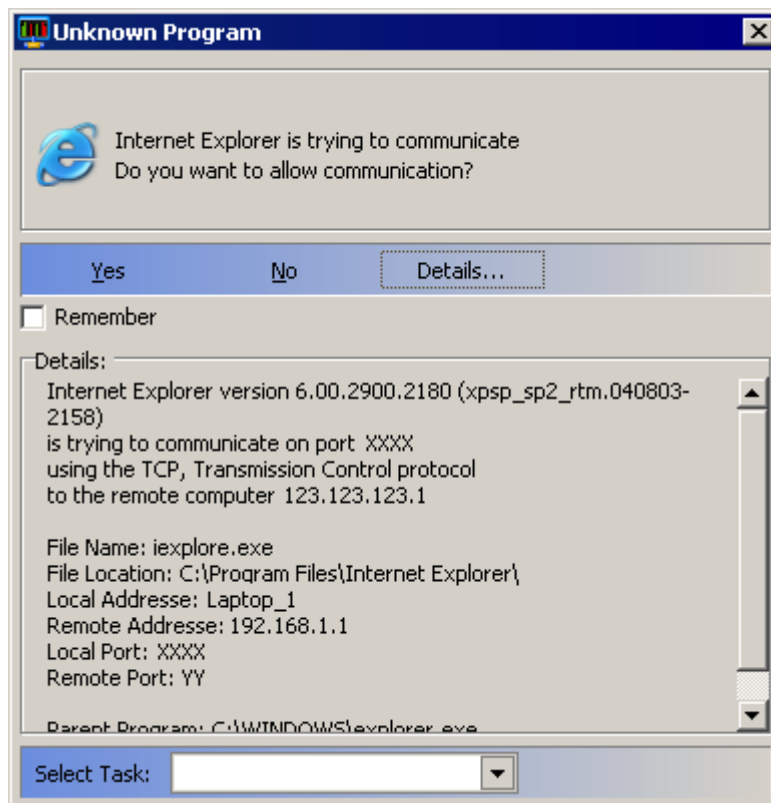
Yes: Click this button, press ENTER or click the title bar *Close* button to close the window allowing communication.

No: Click this button to close the window denying communication.

Note: *If you are in doubt whether it is safe to allow communication or not, consult with your system or network administrator.*

Note: *If the same window is displayed repeatedly after allowing communication, it is because the program attempting communication times out during user interaction in this window. Check the Remember box below to assign the firewall rule Allow Communication to the program file, see section 3.3.5.1.1, "Programs". Then, the program file will no longer prompt for communication.*

Details...: Click this button to display/hide this lower extension of the window:



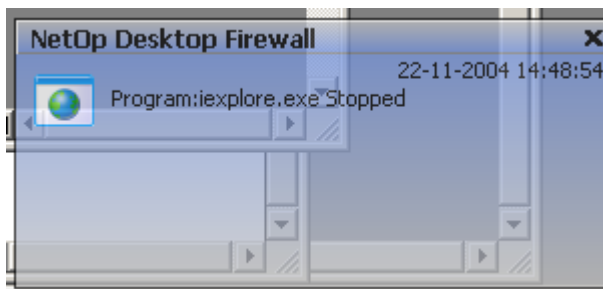
Details: To assist you in identifying the program file and the purpose of its communication, this section displays details on the attempted communication.

Select Task: : The field of this drop-down box displays the default program firewall rule selection *Allow Communication*. The drop-down box list contains the names of available program firewall rules, and *Open Containing Folder...* Select *Open Containing Folder...* to display the directory containing the file attempting communication. Select a firewall rule to apply it to the file attempting communication and close the window.

Remember: Leave this box unchecked (default: unchecked) to apply your selection for this occasion only. Check the box to assign the applied firewall rule to the program file record in the *Programs* display pane, see section 3.3.1.1, "Firewall Rules".

Several *NetOp Desktop Firewall* functionalities can display a user message upon a specified event. Click *OK* in the message window to acknowledge the message and close the window.

Applying a message to a program will cause the firewall to display a message whenever the program is started and stopped. The message looks like this:



The message is semi-transparent and by default displays the program and the action.

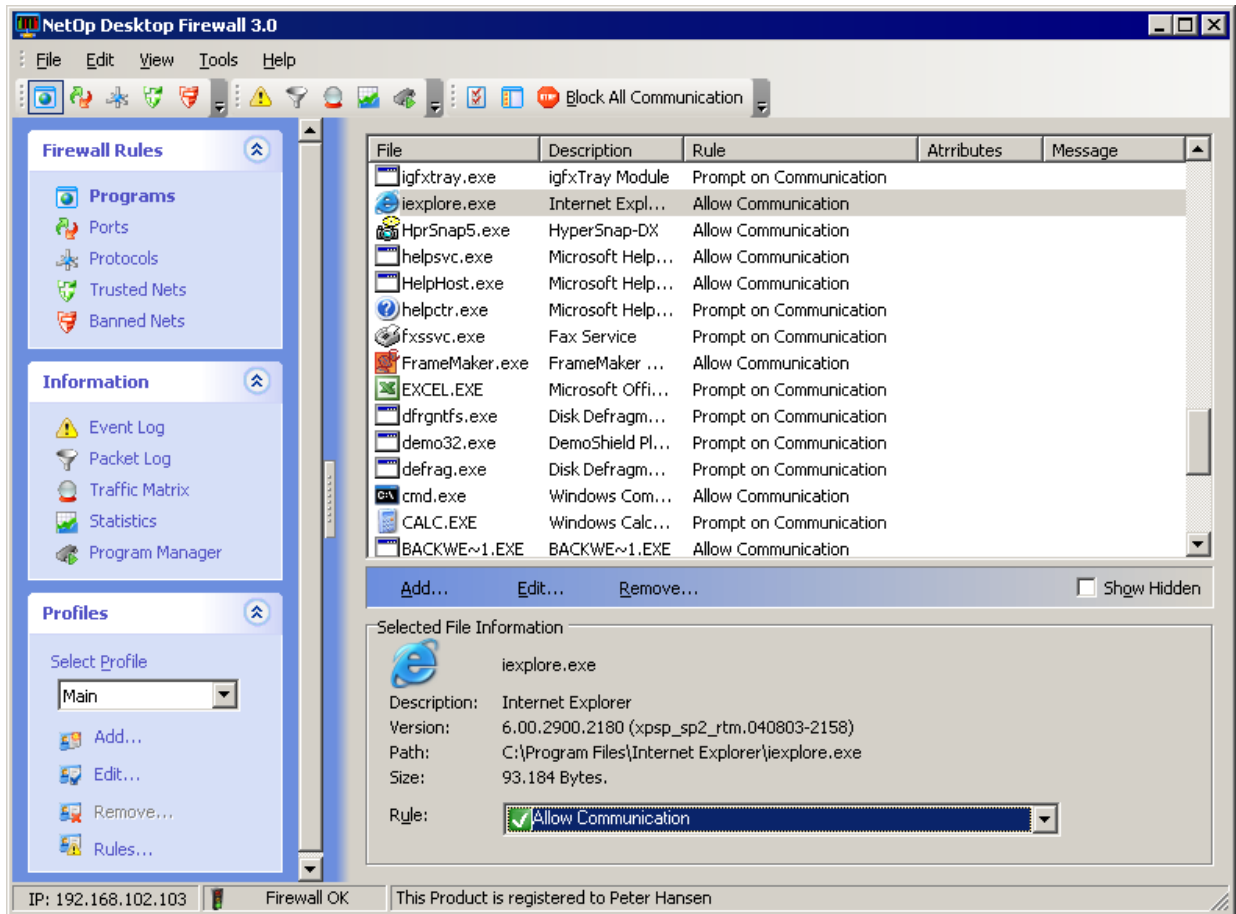
In the properties pane of *Programs*, *Ports*, *Protocols*, *Trusted* and *Banned Nets* it is possible to enter a user-defined message.

Note: *No user prompts and messages will be displayed if the Display No User Prompts and Messages box is checked on the Options window General tab, see section 3.4.1.1, "General Tab". Program communication requests will be denied.*

Note: *If the user interface is unloaded no user prompts and messages will be displayed. When the user interface is reloaded, any user prompts and messages accumulated while unloaded will be displayed, see section 3.2.2, "Notification Area Button Menu".*

3.3 NetOp Desktop Firewall Window

To display this window, double-click the notification area *NetOp Desktop Firewall* button, right-click it to display its menu, and select *Open Firewall Configuration...* select *Start > Programs > NetOp Desktop Firewall > NetOp Desktop Firewall* or run (double-click) the file *NDFConf.exe* in the directory where *NetOp Desktop Firewall* was installed:



Note: *Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".*

This is the *NetOp Desktop Firewall* main user interface that provides access to all available functionalities except *Exit*.

Note: *Remember that Exit terminates the session leaving the computer unprotected whereas Close only closes the window, the firewall continues protecting the computer. For more information, see section 3.2.2, "Notification Area Button Menu".*

3.3.1 Configuration Guide

This configuration guide briefly explains:

Firewall Rules, see section 3.3.1.1, "Firewall Rules"

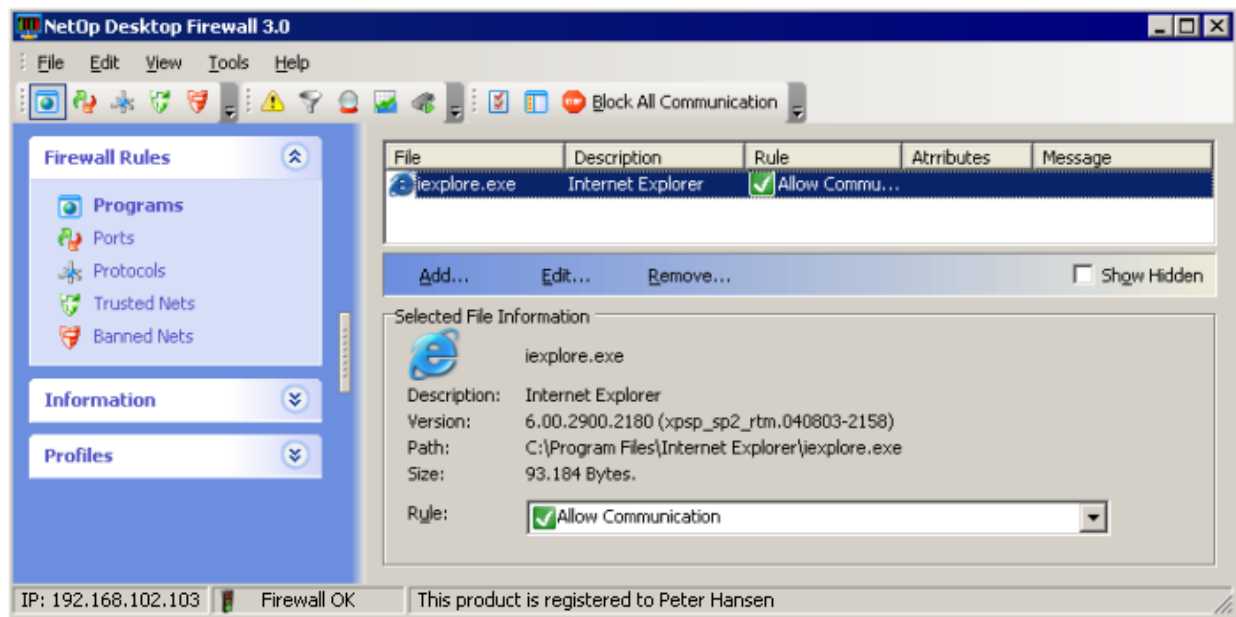
Information utilities, see section 3.3.1.2, "Information"

Profiles, see section 3.3.1.3, "Profiles"

Options, see section 3.3.1.4, "Options"

3.3.1.1 Firewall Rules

In the work panel left selection pane *Firewall Rules* section, select a command to bold it and show its display pane to the right:



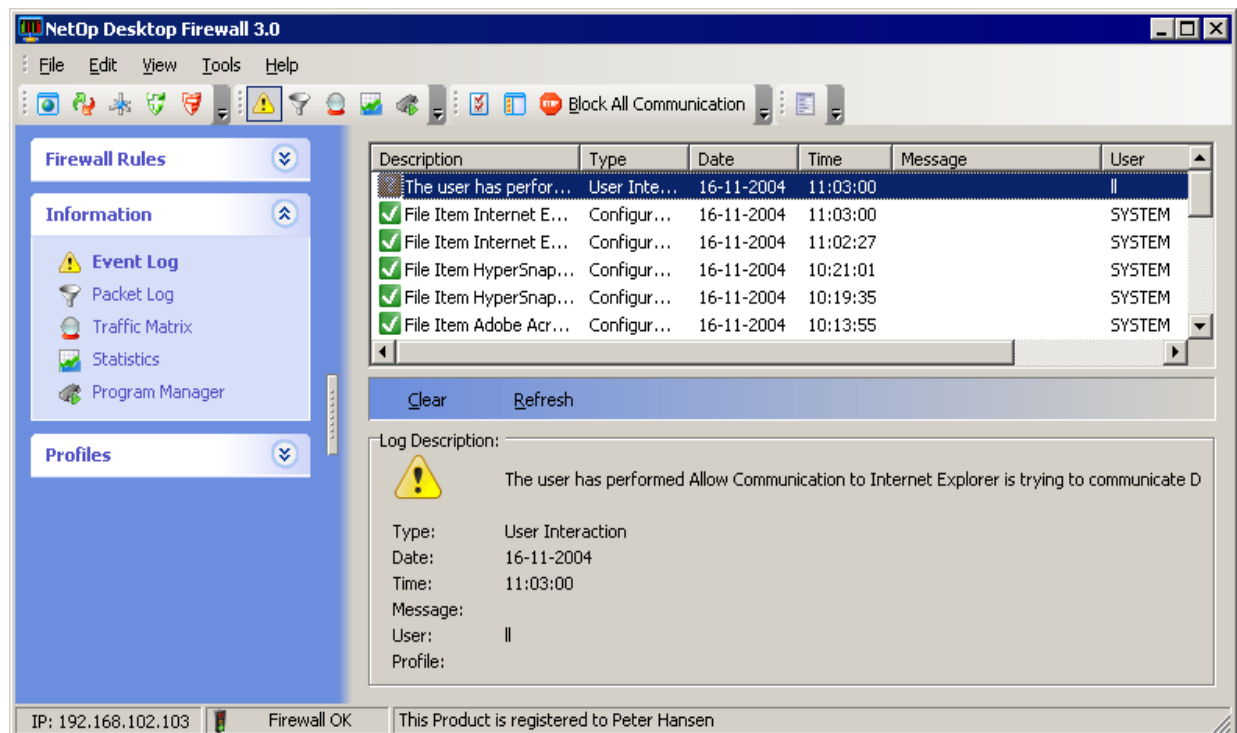
The upper display pane table contains records of elements that have been assigned a firewall rule. The lower section displays information on the record selected in the table above and a drop-down box in which the assigned firewall rule can be changed.

Firewall Rules display panes contain these elements:

- *Programs*: Contains program file records, see section 3.3.5.1.1, "Programs".
- *Ports*: Contains TCP/IP port records, see section 3.3.5.1.2, "Ports".
- *Protocols*: Contains TCP/IP protocol records, see section 3.3.5.1.3, "Protocols".
- *Trusted Nets*: Contains records of trusted remote computer address ranges, see section 3.3.5.1.4, "Trusted Nets".
- *Banned Nets*: Contains records of banned remote computer address ranges, see section 3.3.5.1.5, "Banned Nets".

3.3.1.2 Information

In the work panel selection pane *Information* section, select a command to bold it and show its display pane to the right:



Information utilities enable the user to view and analyze what is happening on the firewall and take relevant actions.

Information utilities include:

- *Event Log*: Displays selected operational events in a table displaying event details, see section 3.3.5.2.1, "Event Log".
- *Packet Log*: Displays *Program Opened*, *Program Closed* and *Program Killed* events and all data packets at the computer communication interface in a table displaying selected event details to enable an analysis of each event, see section 3.3.5.2.2, "Packet Log".
- *Traffic Matrix*: Displays data packet traffic at the computer communication interface in a circular graph to enable an analysis of connections and communicating computer addresses, see section 3.3.5.2.3, "Traffic Matrix".
- *Statistics*: Displays in graphs and numbers current and historical sent, received and blocked data packets at the computer communication interface to monitor firewall activity, see section 3.3.5.2.4, "Statistics".
- *Program Manager*: Displays programs running on the computer in a table displaying selected program details to enable program management, see section 3.3.5.2.5, "Program Manager".

Information utilities can be configured in the *Options* window, see section 3.3.1.4, "Options".

3.3.1.3 Profiles



This work panel selection pane section selects a profile, manages profiles and specifies profile rules, see section 3.3.5.3, "Profiles".

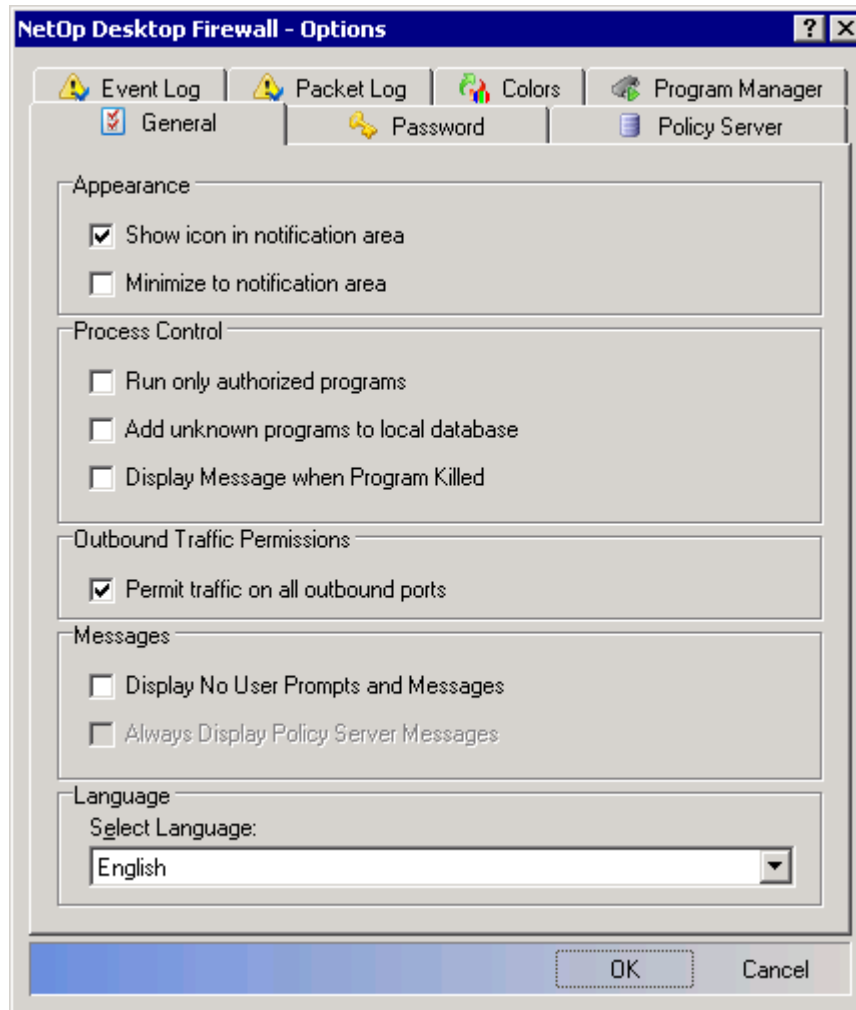
NetOp Desktop Firewall initially has one main profile named *Main*. This profile may be renamed but not removed.

To create customized sets of firewall rules for a computer used in different environments, add sub-profiles of the main profile named e.g. *Work*, *Home* and *Travel* from the *Add...* command. Rename profiles from the *Edit...* command. Remove sub-profiles from the *Remove...* command.

Select *Rules...* to display the *Profile Rules* window to specify rules determining which profiles are applicable in the computer environment.

3.3.1.4 Options

Select the *Tools* menu *Options...* command to display this window:

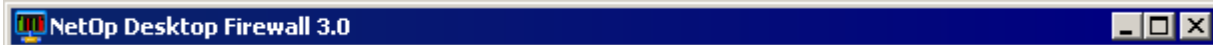


This window specifies *NetOp Desktop Firewall* options.

It has these tabs:

- *General*: This tab specifies general options, see section 3.4.1.1, "General Tab".
- *Password*: This tab specifies password protection, see section 3.4.1.2, "Password Tab".
- *Policy Server*: This tab specifies and logs on to a *NetOp Policy Server*, see section 3.4.1.3, "Policy Server Tab".
- *Event Log*: This tab specifies operational events displayed in the *Event Log*, see section 3.4.1.4, "Event Log Tab".
- *Packet Log*: This tab specifies the columns displayed in *Packet Log*, see section 3.4.1.5, "Packet Log Tab".
- *Colors*: This tab specifies *Packet Log* and *Traffic Matrix* color schemes, see section 3.4.1.6, "Colors Tab".
- *Program Manager*: This tab specifies the columns displayed in *Program Manager*, see section 3.4.1.7, "Program Manager Tab".

3.3.2 Title Bar



Title bar window controls are explained in section 1.5.1, "Window Controls".

3.3.3 Menu Bar



Menu bar and toolbar controls are explained in section 1.5.2, "Menu Bar and Toolbar Controls".

The menu bar contains these menus:

File: See section 3.3.3.1, "File Menu".

Edit: See section 3.3.3.2, "Edit Menu".

View: See section 3.3.3.3, "View Menu".

Tools: See section 3.3.3.4, "Tools Menu".

Help: See section 3.3.3.5, "Help Menu".

3.3.3.1 File Menu

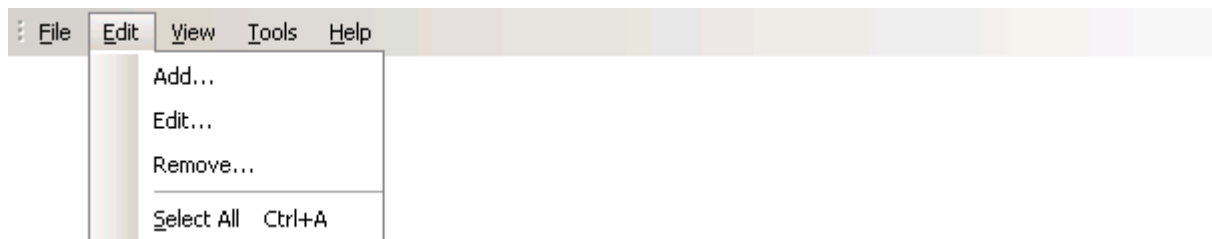


This menu contains these commands:

Save As: Select this command to display a Windows *Save...* window to save *Event Log* or *Packet Log* table contents as a text file. Use the *Save As* command to export your data to other applications.

Close: Select this command, the notification area button menu *Close* command or the title bar window control menu *Close* command or click the title bar *Close* button to close the *NetOp Desktop Firewall* window.

3.3.3.2 Edit Menu



Note: This menu is hidden if inapplicable to the current display pane selection.

This menu contains these commands:

Add...: Select this command or the matching *Firewall Rules* display pane right-click popup menu command or click the matching display pane button to open a display pane matching *Add...* window to add a record, see the matching subsection of section 3.3.1.1, "Firewall Rules".

Edit...: Select a *Firewall Rules* display pane record and select this command or the matching display pane right-click popup menu *Properties...* command or click the matching display pane button to open a display pane matching *...Properties* window to view and edit the properties of the selected record, see the matching subsection of section 3.3.5.1, "Firewall Rules".

Remove... Del: Select one or multiple *Firewall Rules* display pane records and select this command or the matching display pane right-click popup menu command, press *DELETE* or click the matching display pane button to display a confirmation window to confirm removing selected records.

Select All Ctrl+A: Select this command or press *CTRL+A* to select all records in the display pane.

Note: Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".

3.3.3.3 View Menu



This menu contains these commands:

Programs: Select this command or the work panel selection pane *Firewall Rules* section *Programs* command or click the *Firewall Rules* toolbar *Programs* button to display the *Programs* display pane, see section 3.3.5.1.1, "Programs".

Ports: Select this command or the work panel selection pane *Firewall Rules* section *Ports* command or click the *Firewall Rules* toolbar *Ports* button to display the *Ports* display pane, see section 3.3.5.1.2, "Ports".

Protocols: Select this command or the work panel selection pane *Firewall Rules* section *Protocols* command or click the *Firewall Rules* toolbar *Protocols* button to display the *Protocols* display pane, see section 3.3.5.1.3, "Protocols".

Trusted Nets: Select this command or the work panel selection pane *Firewall Rules* section *Trusted Nets* command or click the *Firewall Rules* toolbar *Trusted Nets* button to display the *Trusted Nets* display pane, see section 3.3.5.1.4, "Trusted Nets".

Banned Nets: Select this command or the work panel selection pane *Firewall Rules* section *Banned Net* command or click the *Firewall Rules* toolbar *Banned Nets* button to display the *Banned Nets* display pane, see section 3.3.5.1.5, "Banned Nets".

Event Log: Select this command or the work panel selection pane *Information* section *Event Log* command or click the *Information* toolbar *Event Log* button to display the *Event Log* display pane, see section 3.3.5.2.1, "Event Log".

Packet Log: Select this command or the work panel selection pane *Information* section *Packet Log* command or click the *Information* toolbar *Packet Log* button to display the *Packet Log* display pane, see section 3.3.5.2.2, "Packet Log".

Traffic Matrix: Select this command or the work panel selection pane *Information* section *Traffic Matrix* command or click the *Information* toolbar *Traffic Matrix* button to display the *Traffic Matrix* display pane, see section 3.3.5.2.3, "Traffic Matrix".

Statistics: Select this command or the work panel selection pane *Information* section *Statistics* command or click the *Information* toolbar *Statistics* button to display the *Statistics* display pane, see section 3.3.5.2.4, "Statistics".

Program Manager: Select this command or the work panel selection pane *Information* section *Program Manager* command, or click the *Information* toolbar *Program Manager* button to display the *Program Manager* display pane, see section 3.3.5.2.5, "Program Manager".

Note: *The icon of the displayed display pane (default: Programs) is framed.*

Toolbar: Select this command to hide/display toolbars. When toolbars are displayed, the command is checkmarked (default: checkmarked).

Status Bar: Select this command to hide/display the status bar. When the status bar is displayed, the command is checkmarked (default: checkmarked).

3.3.3.4 Tools Menu



This menu contains these commands:

Options...: Select this command or click the *Options* toolbar *Options* button to display the *Options* window, see section 3.4.1, "Options".

Check for New Updates: Select this command to connect to the *NetOp Desktop Firewall* update server to check for updates to your installed version of *NetOp Desktop Firewall*. If an update with a higher version number than the version number of your installed *NetOp Desktop Firewall* is available, download and install it.

Note: *A NetOp Policy Server can act as an update server for the NetOp Desktop Firewall.*

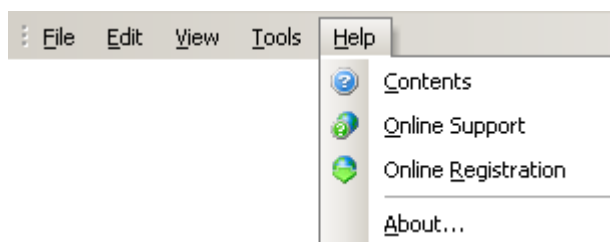
Run Setup Wizard: Select this command to run the *Setup Wizard*, see section 2.5, "Setup Wizard".

Block All/Allow Communication: Select this command or the matching notification area *NetOp Desktop Firewall* button menu command or click the *Options* toolbar *Block/Allow communication* button to block/allow communication across the computer communication interface, see section 3.3.4.3, "Options Toolbar".

When communication is disabled, the notification area *NetOp Desktop Firewall* button displays a *Stop* sign, see section 3.2, "Startup Guide".

Note: *Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".*

3.3.3.5 Help Menu



This menu contains these commands:

Contents: Select this command or press F1 to open the *NetOp Desktop Firewall Help* system on the *NetOp Desktop Firewall Window* topic. The right part of the window displays a graphical table of contents.

Online Support: Select this command to open the Danware online support page with your Internet browser.

Online Registration: Select this command to display the *Registration Wizard*, see section 5.1, "Trial Version", to register your installed product with the manufacturer across the Internet.

About...: Select this command to display the *About* window, see section 3.2.2, "Notification Area Button Menu".

3.3.4 Toolbars



Toolbars are displayed unless hidden from the *View* menu *Toolbars* command, see section 3.3.3.3, "View Menu".

These toolbars are available:

Firewall Rules: See section 3.3.4.1, "Firewall Rules Toolbar".

Information: See section 3.3.4.2, "Information Toolbar".

Options: See section 3.3.4.3, "Options Toolbar".

Play: See section 3.3.4.4, "Play Toolbar".

3.3.4.1 Firewall Rules Toolbar



Menu bar and toolbar controls are explained in section 1.5.2, "Menu Bar and Toolbar Controls".

This toolbar contains these buttons:



Programs: Click this button or select the *View* menu *Programs* command or work panel selection pane *Firewall Rules* section *Programs* command to display the work panel *Programs* display pane, see section 3.3.5.1.1, "Programs".



Ports: Click this button or select the *View* menu *Ports* command or work panel selection pane *Firewall Rules* section *Ports* command to display the work panel *Ports* display pane, see section 3.3.5.1.2, "Ports".



Protocols: Click this button or select the *View* menu *Protocols* command or work panel selection pane *Firewall Rules* section *Protocols* command to display the work panel *Protocols* display pane, see section 3.3.5.1.3, "Protocols".



Trusted Nets: Click this button or select the *View* menu *Trusted Nets* command or work panel selection pane *Firewall Rules* section *Trusted Nets* command to display the work panel *Trusted Nets* display pane, see section 3.3.5.1.4, "Trusted Nets".



Banned Nets: Click this button or select the *View* menu *Banned Nets* command or work panel selection pane *Firewall Rules* section *Banned Nets* command to display the work panel *Banned Nets* display pane, see section 3.3.5.1.5, "Banned Nets".

Note: *The button of the displayed display pane (default: Programs) is framed.*

3.3.4.2 Information Toolbar



Menu bar and toolbar controls are explained in section 1.5.2, "Menu Bar and Toolbar Controls".

This toolbar contains these buttons:



Event Log: Click this button or select the *View* menu *Event Log* command or work panel selection pane *Information* section *Event Log* command to display the work panel *Event Log* display pane, see section 3.3.5.2.1, "Event Log".



Packet Log: Click this button or select the *View* menu *Packet Log* command or work panel selection pane *Information* section *Packet Log* command to display the work panel *Packet Log* display pane, see section 3.3.5.2.2, "Packet Log".



Traffic Matrix: Click this button or select the *View* menu *Traffic Matrix* command or work panel selection pane *Information* section *Traffic Matrix* command to display the work panel *Traffic Matrix* display pane, see section 3.3.5.2.3, "Traffic Matrix".



Statistics: Click this button or select the *View* menu *Statistics* command or work panel selection pane *Information* section *Statistics* command to display the work panel *Statistics* display pane, see section 3.3.5.2.4, "Statistics".



Program Manager: Click this button or select the *View* menu *Program Manager* command or work panel selection pane *Information* section *Program Manager* command to display the work panel *Program Manager* display pane, see section 3.3.5.2.5, "Program Manager".

Note: *The button of the displayed display pane (default: Programs) is framed.*

3.3.4.3 Options Toolbar



Menu bar and toolbar controls are explained in see section 1.5.2, "Menu Bar and Toolbar Controls".

This toolbar contains these buttons:



Options: Click this button or select the *Tools* menu *Options...* command to display the *Options* window, see section 3.4.1, "Options".



Show/Hide Sidebar: Click this button or the work panel pane separator button to hide/display the work panel selection pane. When the selection pane is hidden the button is framed. See section 3.3.5, "Work Pane".



Block All/Allow Communication: Click this button or select the matching notification area button menu command or *Tools* menu command to block all/allow communication across the computer communication interface.

Note: *Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".*

3.3.4.4 Play Toolbar



Menu bar and toolbar controls are explained in section 1.5.2, "Menu Bar and Toolbar Controls".

This toolbar contains these buttons:



Play: Click this button or select the matching display pane right-click popup menu command to start playing after *Pause* or *Stop*. While playing, the button is framed (default: playing).



Pause: Click this button or select the matching display pane right-click popup menu command to pause playing. When selecting *Play* after *Pause*, new data will be added to existing data. While paused, the button is framed.



Stop: Click this button or select the matching display pane right-click popup menu command to stop playing. When selecting *Play* after *Stop*, existing data will be cleared and new data will be added. While stopped, the button is framed.



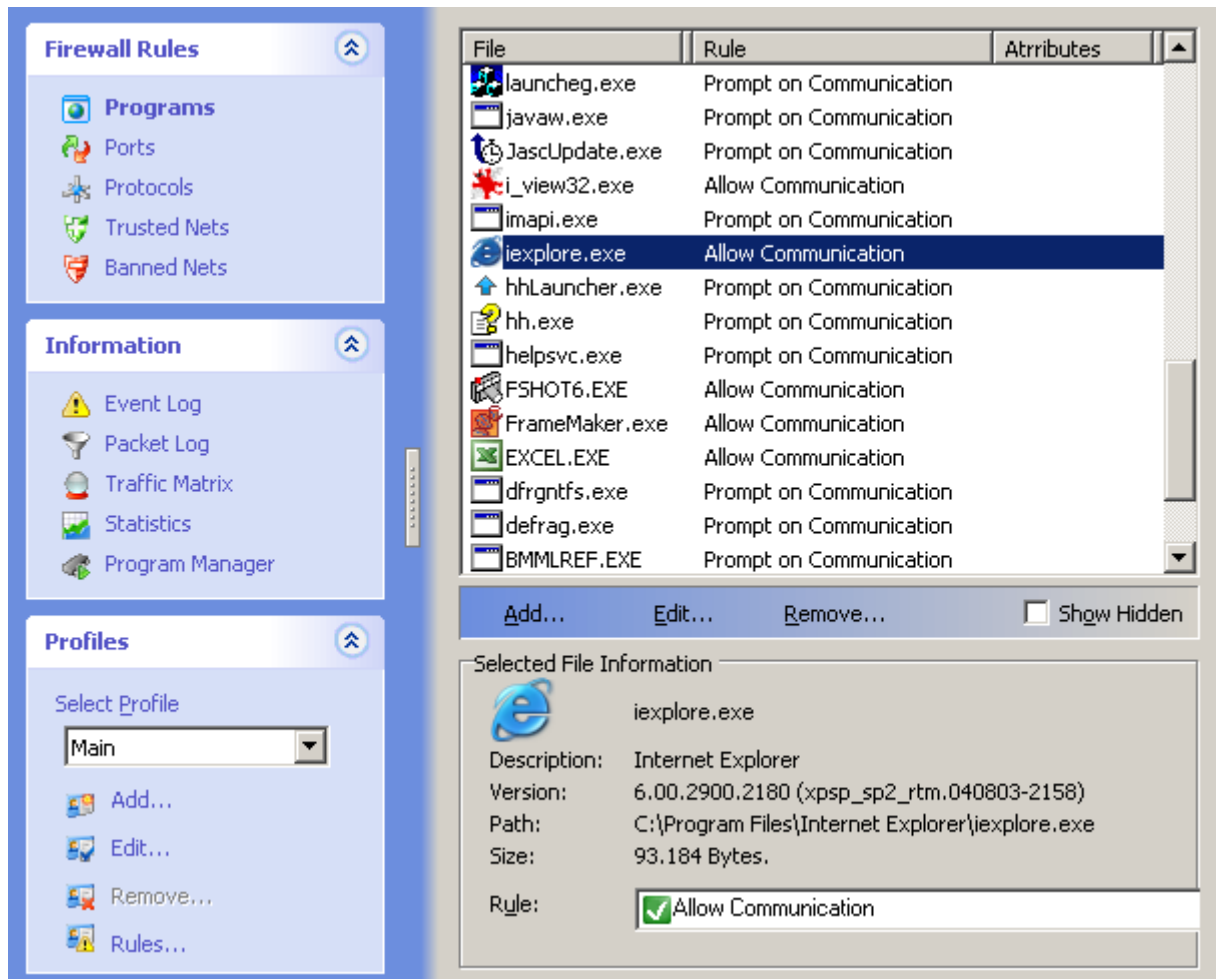
Clear: Click this button or select the matching display pane right-click popup menu command to clear data without changing the current *Play*, *Pause* or *Stop* status.



Legend: Click this button or select the matching *Packet Log* display pane right-click popup menu command to display/hide the *Legend* and *Record Colors* pane. While displayed, the button is framed (default: hidden).

Note: *This toolbar is displayed only when the Packet Log, Traffic Matrix or Statistics display pane is displayed.*

3.3.5 Work Pane

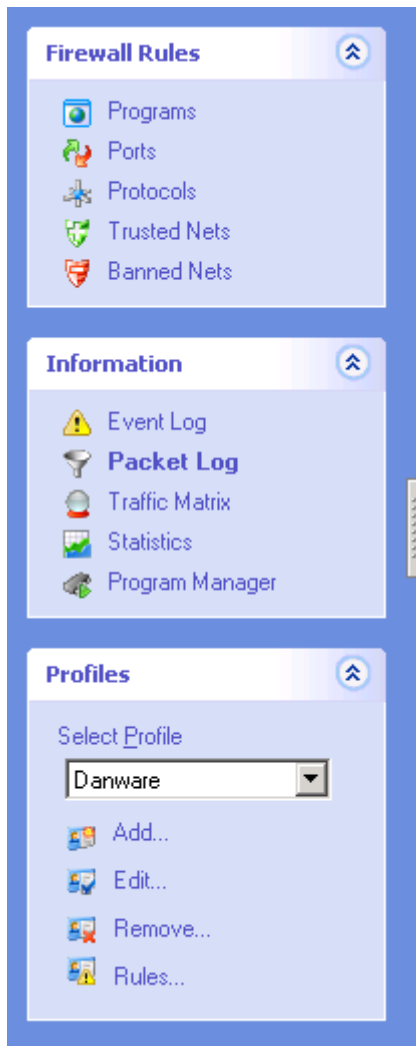


The work panel by default displays a left selection pane and a right display pane.,

Drag the pane separator to change pane widths.

Click the button in the pane separator or the *Options* toolbar *Show/Hide Sidebar* button to hide/display the selection pane, see section 3.3.4.3, "Options Toolbar".

The selection pane contains these sections:



Firewall Rules: Select a command in this section to bold it and display the matching display pane to the right. *Firewall Rules* display panes are explained in section 3.3.5.1, "Firewall Rules".

Information: Select a command in this section to bold it and display the matching display pane to the right. *Information* display panes are explained in section 3.3.1.2, "Information".

Profiles: This section selects a profile to apply it and display its contents in the *Firewall Rules* display panes, adds, edits and removes profiles and displays the *Profile Rules* window to specify profile rules, see section 3.3.5.3, "Profiles".

To collapse a section, click the up pointer button. To expand a section, click the down pointer button.

3.3.5.1 Firewall Rules



This work panel selection pane section contains these commands:

Programs: Select this command or the *View* menu *Programs* command or click the *Firewall Rules* toolbar *Programs* button to display the *Programs* display pane, see section 3.3.5.1.1, "Programs".

Ports: Select this command or the *View* menu *Ports* command or click the *Firewall Rules* toolbar *Ports* button to display the *Ports* display pane, see section 3.3.5.1.2, "Ports".

NetOp Desktop Firewall Window

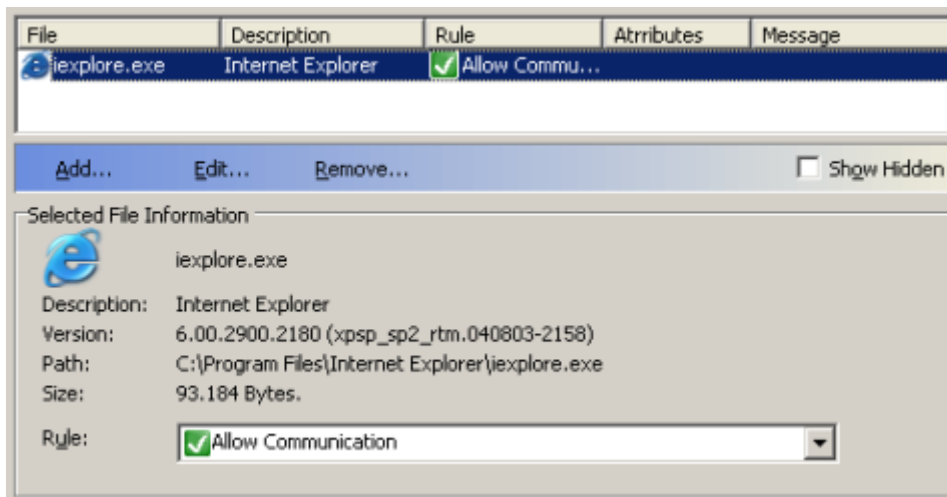
Protocols: Select this command or the *View* menu *Protocols* command or click the *Firewall Rules* toolbar *Protocols* button to display the *Protocols* display pane, see section 3.3.5.1.3, "Protocols".

Trusted Nets: Select this command or the *View* menu *Trusted Nets* command or click the *Firewall Rules* toolbar *Trusted Nets* button to display the *Trusted Nets* display pane, see section 3.3.5.1.4, "Trusted Nets".

Banned Nets: Select this command or the *View* menu *Banned Nets* command or click the *Firewall Rules* toolbar *Banned Nets* button to display the *Banned Nets* display pane, see section 3.3.5.1.5, "Banned Nets".

3.3.5.1.1 Programs

Select the *NetOp Desktop Firewall* window *View* menu or work panel selection pane *Firewall Rules* section *Programs* command or click the *Firewall Rules* toolbar *Programs* button to display this display pane:















This display pane specifies *Program* firewall rules.

The upper pane contains records of program files that have been assigned a firewall rule in a table with these column contents:

File: File icon and name.

Description: File description.

Rule: Rule icon and firewall rule assigned to this record. These *Program* firewall rules are available:

-  *Allow Communication:* Allows communication by this program file across the computer communication interface. *Port, Protocol, Trusted Net* and *Banned Net* firewall rules apply.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
Note: *Windows operating system communication across the computer communication interface typically uses the file ntoskrnl.exe. If a more restrictive firewall rule than Allow Communication is assigned to ntoskrnl.exe, computer malfunction may occur.*
-  *Prompt on Communication:* Prompts the computer user upon attempted communication by this program file to assign a firewall rule to it, see section 3.2.3, "User Prompts and Messages".
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
Note: *By default, this firewall rule applies to a file for which no record exists in the Programs display pane.*
-  *Deny Communication:* Denies communication by this program file across the computer communication interface.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
-  *Kill Program:* Does not allow this program file to run on the computer.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
Caution: *Do not assign this firewall rule to Windows operating system files, as this may cause computer malfunction. Windows operating system files typically reside in the system directory <Boot drive letter>:\WINDOWS\ (XP) or <Boot drive letter>:\WINNT\ (2000).*
-  *Unrestricted Communication:* Allows communication by this program file across the computer communication interface without applying *Port* and *Protocol* firewall rules. *Banned Net* firewall rules apply.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
Caution: *Assign this firewall rule applying low protection only temporarily for communication troubleshooting.*
-  *Trusted Net Only:* Allows communication by this program file across the computer communication interface only with computers on a *Trusted Net*.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
Note: *Port and Protocol firewall rules do not apply to communication with computers on a Trusted Net.*

Note: *Communication means sending or receiving data packets.*

Attributes: First letters of attributes assigned to this record, see below.

Message: Message assigned to this record, see below.

Table controls are explained in section 1.5.3, "Table Controls".

Note: *Check the box Show Hidden to display records with the attribute Hidden.*

NetOp Desktop Firewall Window

Select a record in the pane to display this information in the lower *Selected File Information* section:

<Selected record file icon> and file name.

Description: Selected record file description.

Version: Selected record file version.

Path: Selected record file path.

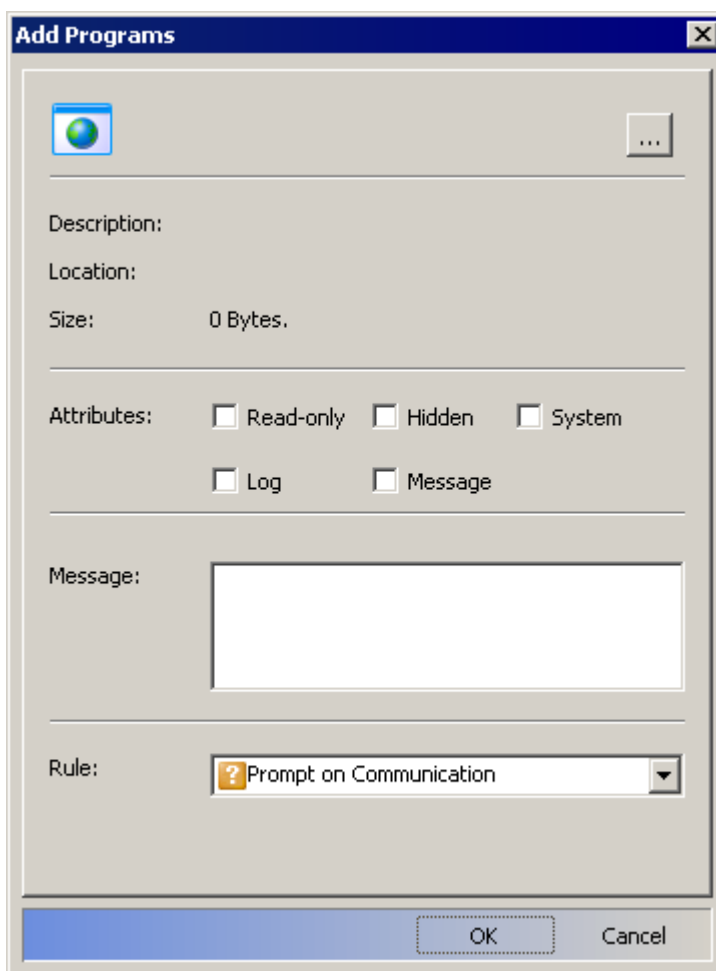
Size: Selected record file size.

Rule: The field of this drop-down box displays the icon and name of the firewall rule assigned to the selected record. The drop-down box list contains available firewall rules, see above. Select a firewall rule in the list to display it in the field to assign it to the selected record.

The buttons and checkbox below the pane have this functionality:

Note: Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".

Add...: Click this button or select the matching *Edit* menu or display pane right-click popup menu command to display this window:



This window adds program file records to the display pane table.

<NetOp Desktop Firewall icon> [...]: Click the ellipsis button [...] to display a Windows *Open* window. Select one or multiple program files (executable files, typically with the extension *exe*) and click *Open* to display the icon of the last selected file instead of the *NetOp Desktop Firewall* icon and all selected file names.

Description: Displays *Single File* if one file is selected or *Multiple Files* if multiple files are selected.

Location: Displays the directory path of selected files.

Size: Displays *0 Bytes*.

Attributes: Check boxes (default: all unchecked) to assign attributes to the added records of selected program files:

Read-only: Check this box to display a warning if attempting to edit or remove added records.

Hidden: Check this box to hide added records unless the *Show Hidden* box is checked.

System: Check this box to disable editing sub-profile properties of added records.

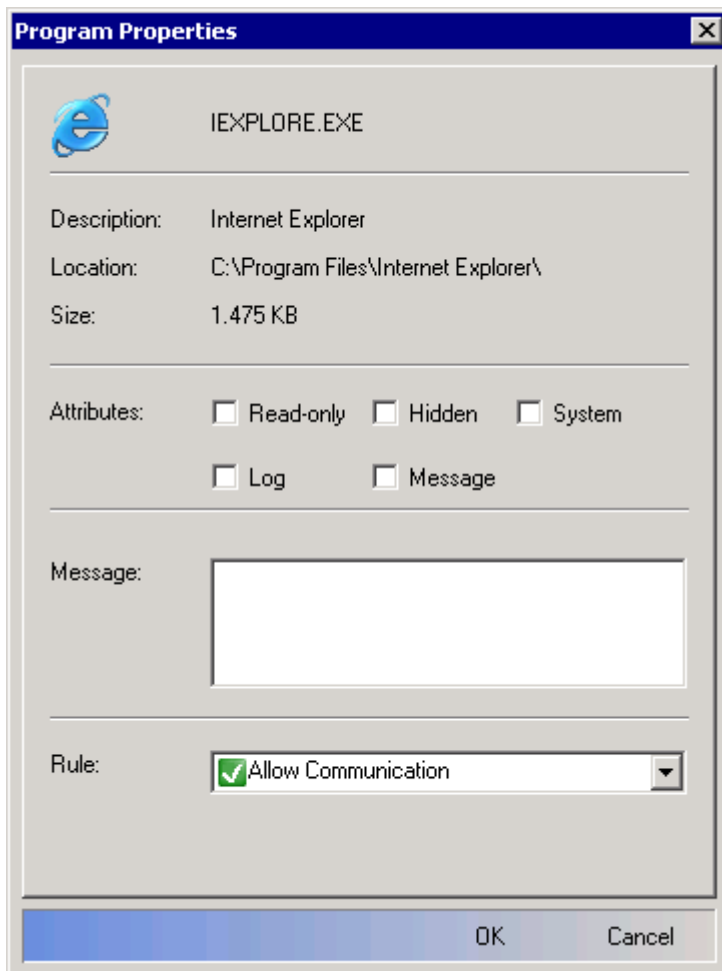
Log: Check this box to log events of added records in the *Event Log*, see section 3.3.5.2.1, "Event Log".

Message: Check this box to display a user message with events of added records, see section 3.2.3, "User Prompts and Messages".

Message: : Optionally, specify a message text for added records in the pane (default: record file description).

Rule: : This drop-down box matches the *Programs* display pane *Rule* drop-down box, see above.

Edit...: Select a record and click this button or select the matching *Edit* menu command or the display pane right-click popup menu *Properties...* command to display this window:



NetOp Desktop Firewall Window

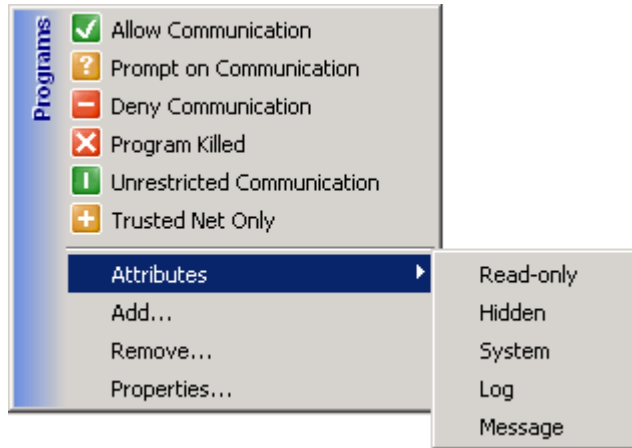
This window contains the same elements as the *Add Programs* window explained above. *Attributes*, *Message* and *Rule* properties can be edited.

Remove...: Select one or multiple records and click this button or select the matching *Edit* menu or display pane right-click popup menu command to display a confirmation window to confirm removing selected records.

Caution: Do not remove the record of the file *ntoskrnl.exe*, as this may cause computer malfunction.

Show Hidden: Check this box (default: unchecked) to display records with the attribute *Hidden*.

Right-click a record or select multiple records and right-click to display this menu:



The commands of this menu edit record properties.

The upper section contains *Rule* commands, see above. Select a command to assign this *Rule* to selected records.

Attributes: This command expands into attribute commands, see above. Commands are checkmarked if attributes are assigned. Select a command to checkmark/uncheckmark it.

Add...: Select this command or the matching *Edit* menu command or click the matching display pane button to display the *Add Programs* window to add records, see above.

Remove...: Select this command or the matching *Edit* menu command or click the matching display pane button to display a confirmation window to confirm removing selected records.

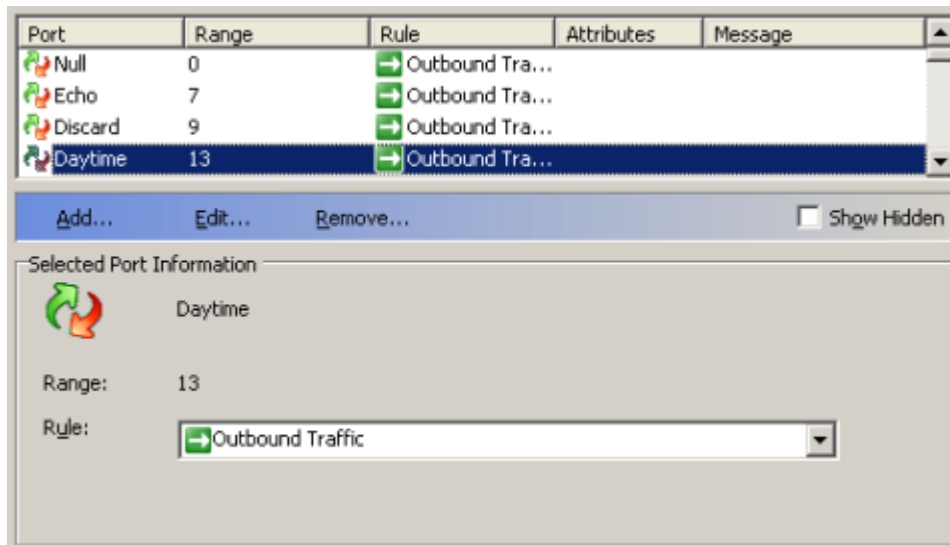
Caution: Do not remove the record of the file *ntoskrnl.exe*, as this may cause computer malfunction.

Properties...: Select this command or the *Edit* menu *Edit...* command or click the display pane *Edit...* button to display the *Program Properties* window to edit the properties of the selected record, see above.

Note: Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".

3.3.5.1.2 Ports

Select the *NetOp Desktop Firewall* window *View* menu or work panel selection pane *Firewall Rules* section *Ports* command or click the *Firewall Rules* toolbar *Ports* button to display this display pane:











This display pane specifies *Port* firewall rules.

The upper pane contains records of TCP/IP ports to which a firewall rule has been assigned (initially a selection of commonly used ports) in a table with these column contents:

Port: Port icon and name.

Range: Port number or number range.

Rule: Icon and name of the firewall rule assigned to this record (initially *Outbound Traffic* for all displayed records). These *Port* firewall rules are available:

-  *Inbound/Outbound Traffic*: Allows inbound and outbound communication through this port.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
-  *Outbound Traffic*: Allows outbound communication only through this port.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
-  *Inbound Traffic*: Allows inbound communication only through this port.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
-  *Blocked in Both Directions*: Allows no communication through this port.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.

Note: Communication means sending or receiving data packets.

Attributes: First letters of attributes assigned to this record, see below.

Message: Message assigned to this record, see below.

Table controls are explained in section 1.5.3, "Table Controls".

Note: Check the box Show Hidden to display records with the attribute Hidden.

NetOp Desktop Firewall Window

Select a record in the pane to display this information in the lower *Selected Port Information* section:

<Port icon> and selected record port name.

Range: Selected record port number or number range.

Rule: The field of this drop-down box displays the icon and name of the firewall rule assigned to the selected record. The drop-down box list contains available firewall rules, see above. Select a firewall rule in the list to display it in the field to assign it to the selected record.

The buttons and checkbox below the pane have this functionality:

Note: Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".

Add...: Click this button or select the matching *Edit* menu or display pane right-click popup menu command to display this window:

The screenshot shows the 'Add Port' dialog box. It features a title bar with the text 'Add Port' and a close button. The main area contains several input fields and controls: a port name field with a refresh icon, a 'Port Range' section with 'From' and 'To' fields (both set to 0), an 'Attributes' section with checkboxes for 'Read-only', 'Hidden', 'System', 'Log', and 'Message', a 'Message' text area, and a 'Rule' dropdown menu currently showing 'Outbound Traffic'. At the bottom are 'OK' and 'Cancel' buttons.

This window adds a port record to the display pane.

<Port icon> []: Specify in the field the added record port name.

Port Range:

From: []: Specify in the field the lowest port number in the range.

To: []: Specify in the field the highest port number in the range.

Attributes: Check boxes (default: all unchecked) to assign attributes to the added record:

[] *Read-only:* Check this box to display a warning if attempting to edit or remove the added record.

[] Hidden: Check this box to hide the added record unless the *Show Hidden* box is checked.

[] System: Check this box to disable editing sub-profile properties of the added record.

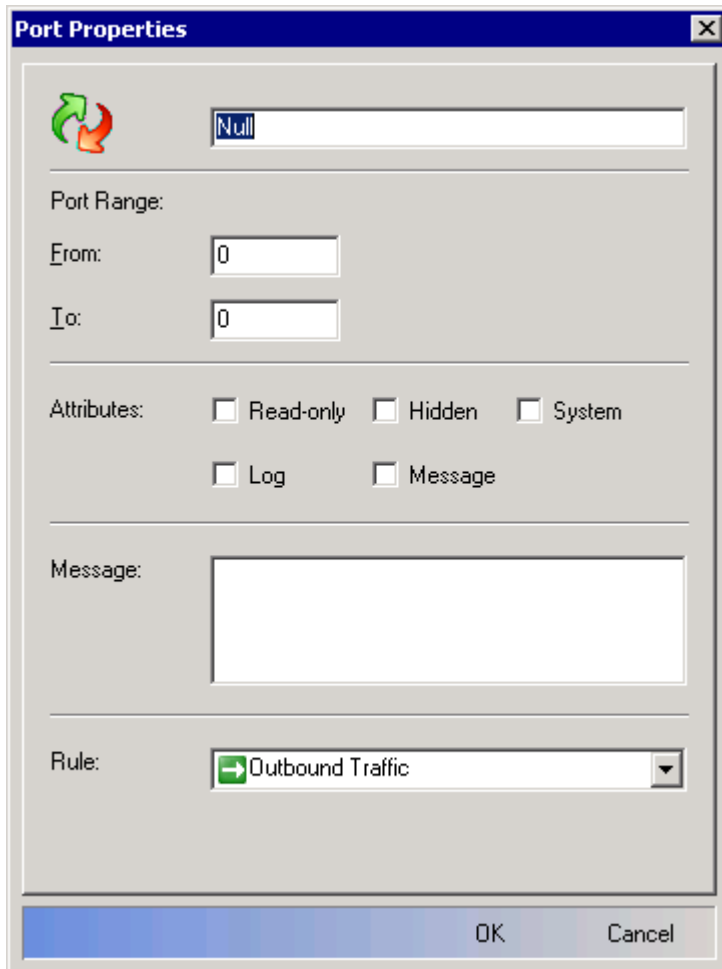
[] Log: Check this box to log events of the added record in the *Event Log*, see section 3.3.5.2.1, "Event Log".

[] Message: Check this box to display a user message with events of the added record, see section 3.2.3, "User Prompts and Messages".

Message: []: Optionally, specify a record message text in the pane (default: program and port name).

Rule: []: This drop-down box matches the display pane *Rule* drop-down box, see above.

Edit...: Select a record and click this button or select the matching *Edit* menu command or the display pane right-click popup menu *Properties...* command to display this window:

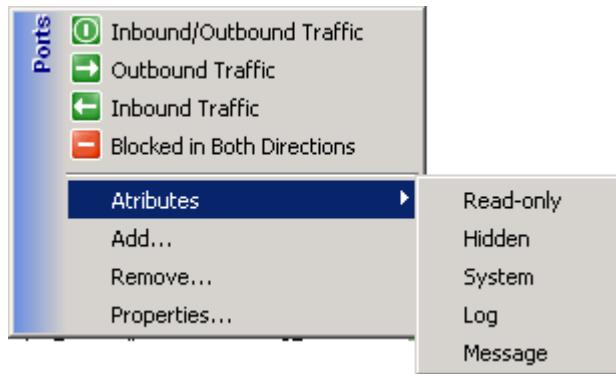


This window contains the same elements as the *Add Port* window explained above. All elements can be edited.

Remove...: Select one or multiple records and click this button or select the matching *Edit* menu or display pane right-click popup menu command to display a confirmation window to confirm removing selected records.

[] Show Hidden: Check this box (default: unchecked) to display records with the attribute *Hidden*.

Right-click a record or select multiple records and right-click to display this menu:



The commands of this menu edit record properties.

Note: Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".

The upper section contains *Rule* commands, see above. Select a command to apply this *Rule* to selected records.

Attributes: This command expands into attribute commands, see above. Commands are checkmarked if attributes are assigned. Select a command to checkmark/uncheckmark it.

Add...: Select this command or the matching *Edit* menu command or click the matching display pane button to display the *Add Port* window to add a record, see above.

Remove...: Select this command or the matching *Edit* menu command or click the matching display pane button to display a confirmation window to confirm removing selected records.

Properties...: Select this command or the *Edit* menu *Edit...* command or click the display pane *Edit...* button to display the *Port Properties* window to edit the properties of the selected record, see above.

Port Notes

Computers communicate through TCP/IP ports numbered in the range 0 - 65535.

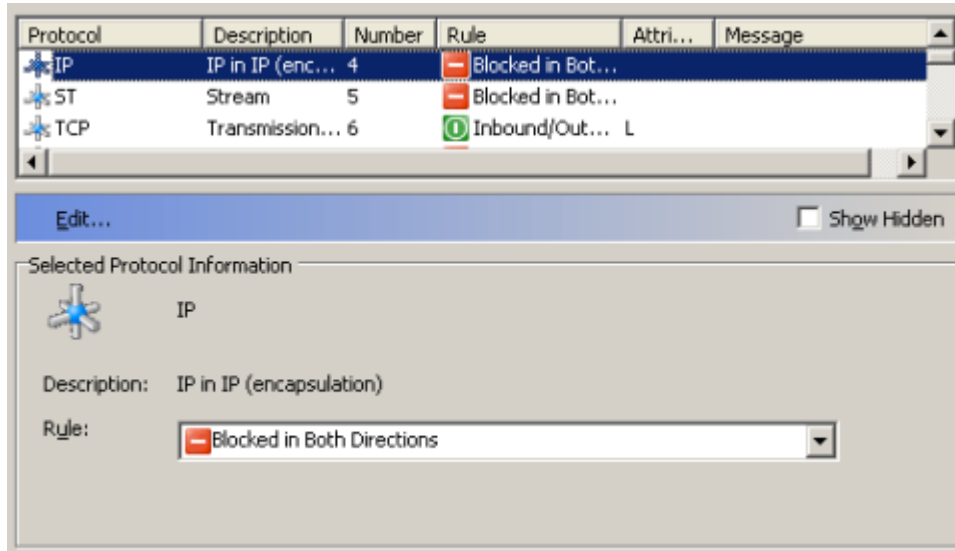
Some port numbers are officially assigned to specific applications. The port numbers and ranges specified initially in the *Ports* display pane are port numbers assigned to generally used applications.

Assigning the firewall rule *Outbound Traffic* to a port is quite safe, as it allows outbound and return communication through the port but not communication initiated from outside the computer.

If the communication of an application fails and you suspect that the failure is caused by a port or protocol problem, you can test it by temporarily assigning the *Unrestricted Communication* firewall rule to the application program file. If communication succeeds in the test, identify the port and protocol used by the application to assign the required firewall rules to them.

3.3.5.1.3 Protocols

Select the *NetOp Desktop Firewall* window *View* menu or work panel selection pane *Firewall Rules* section *Protocols* command or click the *Firewall Rules* toolbar *Protocols* button to display this display pane:



This display pane specifies *Protocol* firewall rules.









The upper pane contains records of the TCP/IP protocol suite protocols in a table with these column contents:

Protocol: Protocol icon and name.

Description: Protocol description.

Number: Protocol number.

Rule: Icon and name of the firewall rule assigned to this record (initially *Outbound Traffic* for *ICMP* and *IGMP*, *Inbound/Outbound Traffic* for *TCP* and *UDP*, *Blocked in Both Directions* for all others, by default hidden). These protocol firewall rules are available:

-  *Inbound/Outbound Traffic*: Allows inbound and outbound communication using this protocol.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
-  *Outbound Traffic*: Allows outbound communication only using this protocol.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
-  *Inbound Traffic*: Allows inbound communication only using this protocol.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
-  *Blocked in Both Directions*: Allows no communication using this protocol.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.

Note: *Communication means sending or receiving data packets.*

Attributes: First letters of attributes assigned to this record, see below.

Message: Message assigned to this record, see below.

NetOp Desktop Firewall Window

Table controls are explained in section 1.5.3, "Table Controls".

Note: Check the box Show Hidden to display records with the attribute Hidden.

Select a record in the pane to display this information in the lower *Selected Protocol Information* section:

<Protocol icon> and selected protocol name.

Description: Selected protocol description.

Rule: The field of this drop-down box field displays the icon and name of the firewall rule assigned to the selected record. The drop-down box list contains available firewall rules, see above. Select a firewall rule in the list to display it in the field to assign it to the selected record.

The button and checkbox below the pane have this functionality:

Note: Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".

Edit...: Select a record and click this button or select the matching *Edit* menu command or the display pane right-click popup menu *Properties...* command to display this window:

The screenshot shows a dialog box titled "Protocol Properties". At the top left is a star icon. To its right is a text field containing "HOPOPT". Below this is a "Description:" label followed by a text field containing "IPv6 Hop-by-Hop Option". Underneath is a "Number:" label followed by a text field containing "0". An "Attributes:" section contains five checkboxes: "Read-only", "Hidden", "System", "Log", and "Message", all of which are unchecked. Below the attributes is a "Message:" label followed by a large empty text area. At the bottom, a "Rule:" label is followed by a dropdown menu showing a red minus icon and the text "Blocked in Both Directions". The dialog ends with "OK" and "Cancel" buttons.

This window edits a display pane protocol record.

Protocol Name: Displays the protocol name that cannot be edited.

Protocol Description: Displays the protocol description that cannot be edited.

Protocol Number: Displays the protocol number that cannot be edited.

Attributes: Check boxes (default: all unchecked) to assign attributes to the selected record:

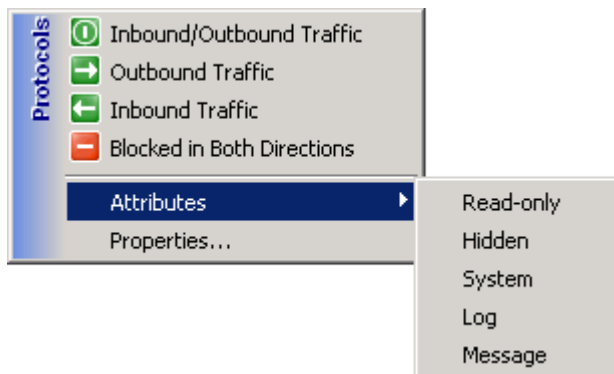
- Read-only*: Check this box to display a warning if attempting to edit the selected record.
- Hidden*: Check this box to hide the selected record unless the *Show Hidden* box is checked.
- System*: Check this box to disable editing sub-profile properties of the selected record.
- Log*: Check this box to log events of the selected record in the *Event Log*, see section 3.3.5.2.1, "Event Log".
- Message*: Check this box to display a user message with events of the selected record, see section 3.2.3, "User Prompts and Messages".

Message: : Optionally, specify a record message text in the pane (default: protocol name).

Rule: : This drop-down box matches the *Protocols* display pane *Rule* drop-down box explained above.

Show Hidden: Check this box (default: unchecked) to display records with the attribute *Hidden*.

Right-click a record or select multiple records and right-click to display this menu:



The commands of this menu edit record properties.

Note: *Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".*

The upper section contains firewall rule commands, see above. Select a command to apply this firewall rule to selected records.

Attributes: This command expands into attribute commands, see above. Commands are checkmarked if attributes are assigned. Select a command to checkmark/uncheckmark it.

Properties...: Select this command or the *Edit* menu *Edit...* command or click the display pane *Edit...* button to display the *Protocol Properties* window to edit the properties of the selected record, see above.

Protocol Notes

ICMP (Internet Control Message Protocol) is used by e.g. the PING utility detecting if an IP connection is available.

IGMP (Internet Group Management Protocol) provides a way for an Internet computer to report its multicast group membership to adjacent routers. Multicasting allows one computer on the Internet to send content to multiple other computers.









TCP (Transmission Control Protocol) is a commonly used data transmission protocol. Data packets can be lost, duplicated or lose data in transit. TCP detects lost and duplicated packets as well as lost packet data and triggers retransmission until complete data has been received.

UDP (User Datagram Protocol) is a commonly used communication protocol. UDP does not detect lost or duplicate packets or lost packet data.

If the communication of an application fails and you suspect that the failure is caused by a port or protocol problem, you can test it by temporarily assigning the *Unrestricted Communication* firewall rule to the application program file. If communication succeeds in the test, identify the port and protocol used by the application to assign the required firewall rules to them.

3.3.5.1.4 Trusted Nets

Select the *NetOp Desktop Firewall* window *View* menu or work panel selection pane *Firewall Rules* section *Trusted Nets* command or click the *Firewall Rules* toolbar *Trusted* button to display this display pane:

Trust	From	To	Rule	Attributes	Message
 Server1	192.168.1.1	192.168.1.1	 Inbou...		
 Server2	192.168.1.2	192.168.1.2	 Inbou...		
 Workstation1	192.168.1.3	192.168.1.3	 Inbou...		
 Workstation2	192.168.1.4	192.168.1.4	 Inbou...		

Show Hidden

This display pane specifies *Trusted Net* firewall rules.

A *Trusted Net* is a range of remote computer addresses with which the computer shall be able to communicate without applying *Port* and *Protocol* firewall rules, e.g. the range of addresses used by the computers in your organization.









The upper pane contains records of *Trusted Nets* in a table with these column contents:

Trust: *Trusted Net* icon and name.

From: Lowest address in *Trusted Net*.

To: Highest address in *Trusted Net*.

Rule: Icon and name of the firewall rule assigned to this record. These trusted net firewall rules are available:

-  *Inbound/Outbound Trust*: Applies no *Port* and *Protocol* firewall rules to inbound and outbound communication with computers on this *Trusted Net*.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
-  *Outbound Trust*: Applies no *Port* and *Protocol* firewall rules to outbound communication to computers on this *Trusted Net*.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
-  *Inbound Trust*: Applies no *Port* and *Protocol* firewall rules to inbound communication from computers on this *Trusted Net*.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
-  *Trust Inactive*: Disables trust in computers on this *Trusted Net*.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.

Attributes: First letters of attributes assigned to this record, see below.

Message: Message assigned to this record, see below.

Table controls are explained in section 1.5.2, "Menu Bar and Toolbar Controls".

Note: Check the box *Show Hidden* to display records with the attribute *Hidden*.

Select a record in the pane to display this information in the lower *Selected Trust Information* section:

<Trusted net icon> and selected record *Trusted Net* name.

From: Lowest address in selected record *Trusted Net*.

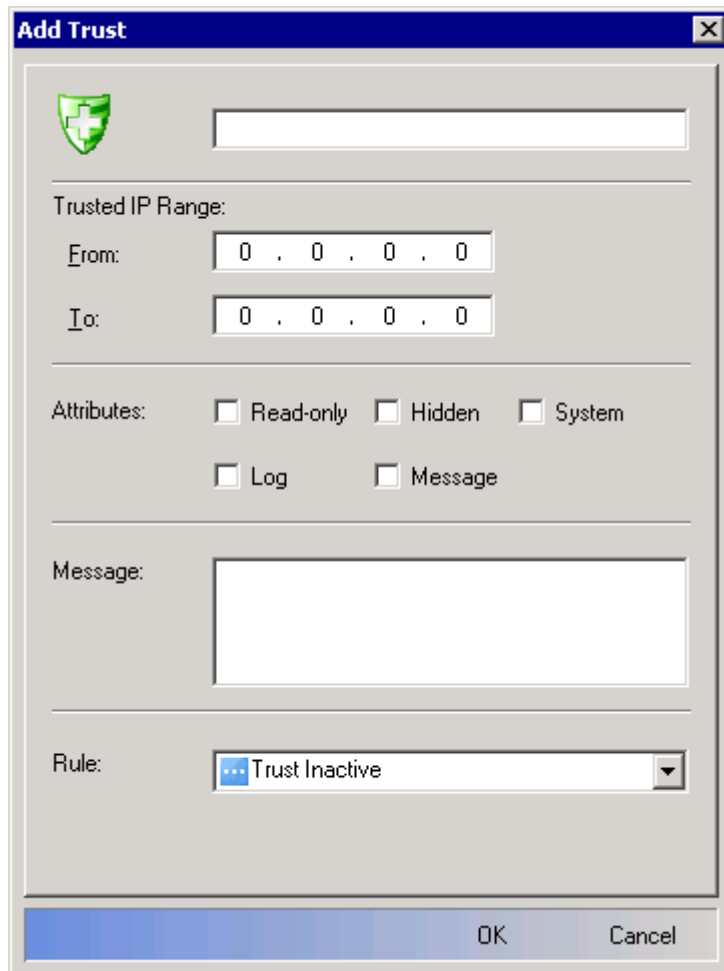
To: Highest address in selected record *Trusted Net*.

Rule: The field of this drop-down box displays the icon and name of the firewall rule assigned to the selected record. The drop-down box list contains available firewall rules, see above. Select a firewall rule in the list to display it in the field to assign it to the selected record.

The buttons and checkbox below the pane have this functionality:

Note: Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".

Add...: Click this button or select the matching *Edit* menu or display pane right-click popup menu command to display this window:



This window adds a *Trusted Net* record in the display pane.

<Trusted net icon>: *[]*: Specify in the field the *Trusted Net* name.

Trusted Net Range:

From: *[]*: Specify in the field the lowest address in the *Trusted Net*.

To: *[]*: Specify in the field the highest address in the *Trusted Net*.

Attributes: Check boxes (default: all unchecked) to assign attributes to the added record:

[] Read-only: Check this box to display a warning if attempting to edit or remove the added record.

[] Hidden: Check this box to hide the added record unless the *Show Hidden* box is checked.

[] System: Check this box to disable editing sub-profile properties of the added record.

NetOp Desktop Firewall Window

[] Log: Check this box to log events of the added record in the *Event Log*, see section 3.3.5.2.1, "Event Log".

[] Message: Check this box to display a user message with events of the added record, see section 3.2.3, "User Prompts and Messages".

Message: []: Optionally, specify a record message text in the pane (default: *Trusted Net* name).

Rule: []: This drop-down box matches the display pane *Rule* drop-down box, see above.

Edit...: Select a record and click this button or select the matching *Edit* menu command or the display pane right-click popup menu *Properties...* command to display this window:

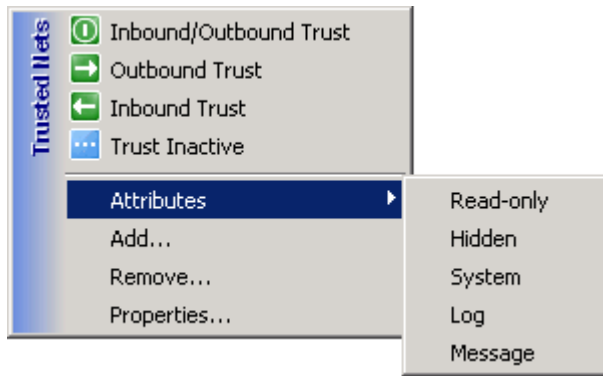
The screenshot shows the 'Trusted Net Properties' dialog box. The title bar is blue with the text 'Trusted Net Properties' and a close button. The main area is light gray. At the top left is a green shield icon with a white cross. To its right is a text field containing 'Danware'. Below this is the 'Trusted IP Range' section with 'From:' and 'To:' fields containing '192 . 168 . 1 . 1' and '192 . 168 . 1 . 255' respectively. The 'Attributes' section has checkboxes for 'Read-only', 'Hidden', 'System', 'Log', and 'Message', all of which are unchecked. A 'Message:' text area is empty. The 'Rule:' dropdown menu is set to 'Trust Inactive'. At the bottom are 'OK' and 'Cancel' buttons.

This window contains the same elements as the *Add Trust* window explained above. All elements can be edited.

Remove...: Select one or multiple records and click this button or select the matching *Edit* menu or display pane right-click popup menu command to display a confirmation window to confirm removing selected records.

[] Show Hidden: Check this box (default: unchecked) to display records with the attribute *Hidden*.

Right-click a record or select multiple records and right-click to display this menu:



The commands of this menu edit record properties.

Note: Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".

The upper section contains *Rule* commands, see above. Select a command to apply this *Rule* to selected records.

Attributes: This command expands into attribute commands, see above. Commands are checkmarked if attributes are assigned. Select a command to checkmark/uncheckmark it.

Add...: Select this command or the matching *Edit* menu command or click the matching display pane button to display the *Add Trust* window to add a record, see above.

Remove...: Select this command or the matching *Edit* menu command or click the matching display pane button to display a confirmation window to confirm removing selected records.

Properties...: Select this command or the *Edit* menu *Edit...* command or click the display pane *Edit...* button to display the *Trusted Net Properties* window to edit the properties of the selected record, see above.

Trusted Net Notes

With this version of *NetOp Desktop Firewall*, address means IP address.

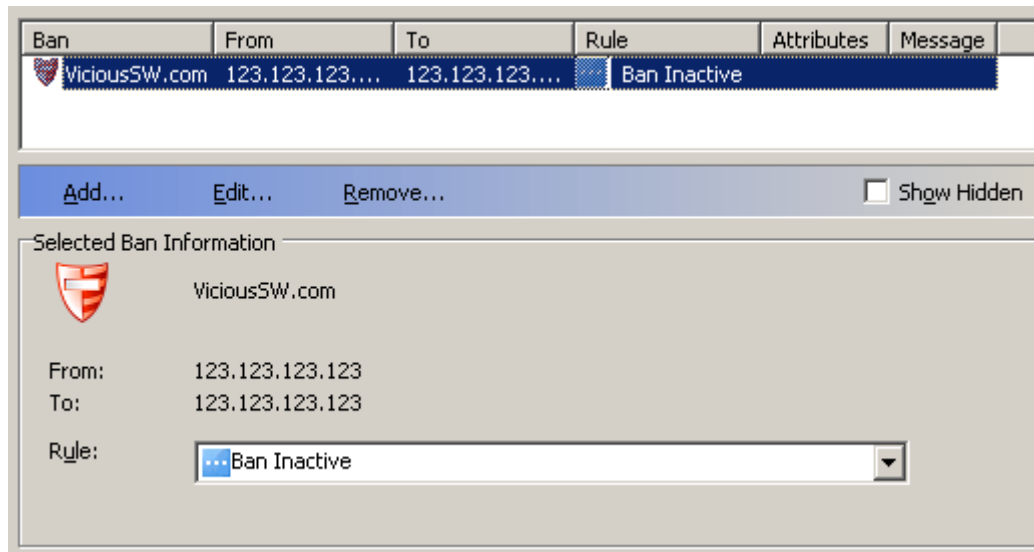
Typically, you would specify the IP address range used by the computers on your workplace local area network (LAN) as a *Trusted Net*.

Note: If you experience difficulties or long delays in logging on to your LAN after installing NetOp Desktop Firewall, it will typically be because you have not specified a trusted net including the IP addresses of LAN servers involved in your network logon.

Lack of trusted IP addresses to other computers, printers etc. may cause difficulties in connecting to them. To learn more, see section 2.5, "Setup Wizard".

3.3.5.1.5 Banned Nets

Select the *NetOp Desktop Firewall* window *View* menu or work panel selection pane *Firewall Rules* section *Banned Nets* command or click the *Information* toolbar *Banned Nets* button to display this display pane:



This display pane specifies *Banned Net* firewall rules.

A *Banned Net* is a range of remote computer addresses with which your computer shall not be able to communicate.









The upper pane contains records of *Banned Nets* (initially none) in a table with these column contents:

Ban: *Banned Net* icon and name.

From: Lowest address in *Banned Net*.

To: Highest address in *Banned Net*.

Rule: Icon and name of the firewall rule assigned to this record. These *Banned Net* firewall rules are available:

-  *Inbound/Outbound Ban*: Allows no inbound or outbound communication with computers on this *Banned Net*.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
-  *Outbound Ban*: Allows no outbound communication to computers on this *Banned Net*.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
-  *Inbound Ban*: Allows no inbound communication from computers on this *Banned Net*.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.
-  *Ban Inactive*: Disables ban on computers on this *Banned Net*.
-  This action is not allowed if the icon is covered by a padlock. This is controlled by *NetOp Policy Server*.

Attributes: First letters of attributes assigned to this record, see below.

Message: Message assigned to this record, see below.

Table controls are explained in section 1.5.3, "Table Controls".

Note: Check the box Show Hidden to display records with the attribute Hidden.

Select a record in the pane to display this information in the lower *Selected Ban Information* section:

<Banned net icon>: Selected record *Banned Net* name.

From: Lowest address in selected record *Banned Net*.

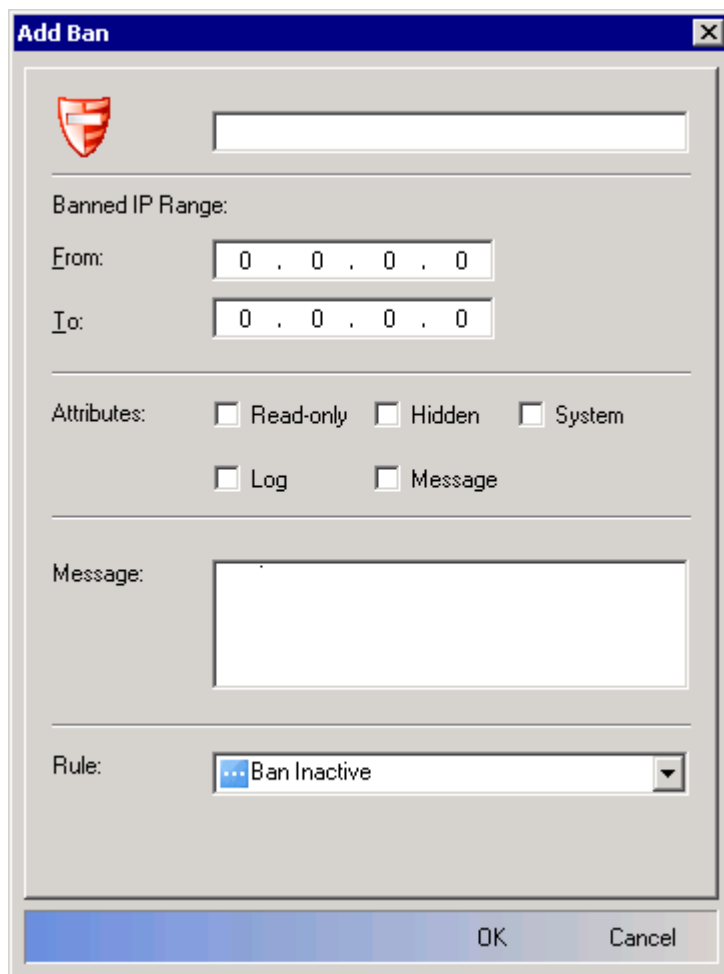
To: Highest address in selected record *Banned Net*.

Rule: The field of this drop-down box displays the icon and name of the firewall rule assigned to the selected record. The drop-down box list contains available firewall rules, see above. Select a firewall rule in the list to display it in the field to assign it to the selected record.

The buttons and checkbox below the pane have this functionality:

Note: Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".

Add...: Click this button or select the matching *Edit* menu or display pane right-click popup menu command to display this window:



This window adds a *Banned Net* record in the display pane.

<Banned net icon> []: Specify in the field the *Banned Net* name.

Banned Net Range:

From: []: Specify or edit in the field the lowest address in the range.

NetOp Desktop Firewall Window

To: []: Specify or edit in the field the highest address in the range.

Attributes: Check boxes (default: all unchecked) to assign attributes to the added record:

[] *Read-only:* Check this box to display a warning if attempting to edit or remove the added record.

[] *Hidden:* Check this box to hide the added record unless the *Show Hidden* box is checked.

[] *System:* Check this box to disable editing sub-profile properties of the added record.

[] *Log:* Check this box to log events of the added record in the *Event Log*, see section 3.3.5.2.1, "Event Log".

[] *Message:* Check this box to display a user message with events of the added record, see section 3.2.3, "User Prompts and Messages".

Message: []: Optionally, specify a record message text in the pane (default: *Banned Net* name).

Rule: []: This drop-down box matches the display pane *Rule* drop-down box, see above.

Edit...: Select a record and click this button or select the matching *Edit* menu command or the display pane right-click popup menu *Properties...* command to display this window:

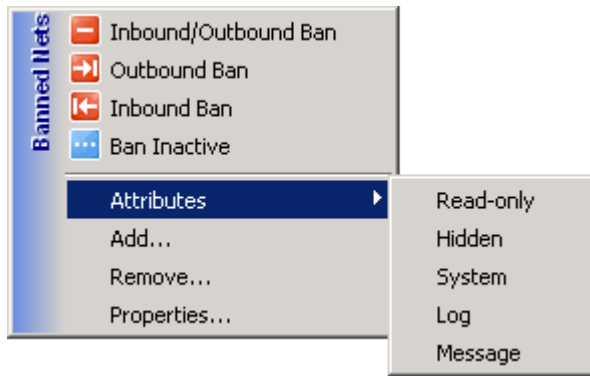
The screenshot shows the 'Add Ban' dialog box. It features a title bar with the text 'Add Ban' and a close button. The main area contains a shield icon on the left and a text input field containing 'VicioiusSW.com'. Below this is a section labeled 'Banned IP Range:' with two input fields: 'From:' and 'To:', both containing the text '123 , 123 , 123 , 123'. Underneath is an 'Attributes:' section with five checkboxes: 'Read-only', 'Hidden', 'System', 'Log', and 'Message', all of which are unchecked. A 'Message:' text area is located below the attributes, and it is currently empty. At the bottom of the dialog, there is a 'Rule:' dropdown menu with 'Ban Inactive' selected. The dialog concludes with 'OK' and 'Cancel' buttons.

This window contains the same elements as the *Add Ban* window explained above. All elements can be edited.

Remove...: Select one or multiple records and click this button or select the matching *Edit* menu or display pane right-click popup menu command to display a confirmation window to confirm removing selected records.

[] *Show Hidden:* Check this box (default: unchecked) to display records with the attribute *Hidden*.

Right-click a record or select multiple records and right-click to display this menu:



The commands of this menu edit record properties.

Note: Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".

The upper section contains *Rule* commands, see above. Select a command to apply this *Rule* to selected records.

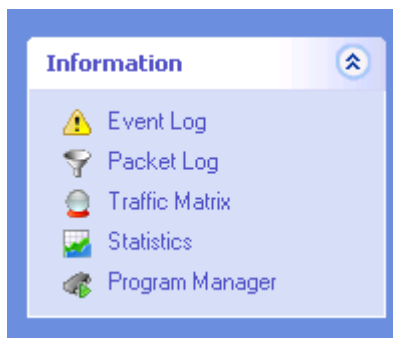
Attributes: This command expands into attribute commands, see above. Commands are checkmarked if attributes are assigned. Select a command to checkmark/uncheckmark it.

Add...: Select this command or the matching *Edit* menu command or click the matching display pane button to display the *Add Ban* window to add a record, see above.

Remove...: Select this command or the matching *Edit* menu command or click the matching display pane button to display a confirmation window to confirm removing selected records.

Properties...: Select this command or the *Edit* menu *Edit...* command or click the display pane *Edit...* button to display the *Banned Net Properties* window to edit the properties of the selected record, see above.

3.3.5.2 Information



This section contains these commands:

Event Log: Select this command or the *View* menu *Event Log* command or click the *Information* toolbar *Event Log* button to display the *Event Log* display pane, see section 3.3.5.2.1, "Event Log".

Packet Log: Select this command or the *View* menu *Packet Log* command or click the *Information* toolbar *Packet Log* button to display the *Packet Log* display pane, see section 3.3.5.2.2, "Packet Log".

Traffic Matrix: Select this command or the *View* menu *Traffic Matrix* command or click the *Information* toolbar *Traffic Matrix* button to display the *Traffic Matrix* display pane, see section 3.3.5.2.3, "Traffic Matrix".

Statistics: Select this command or the *View* menu *Statistics* command or click the *Information* toolbar *Statistics* button to display the *Statistics* display pane, see section 3.3.5.2.4, "Statistics".

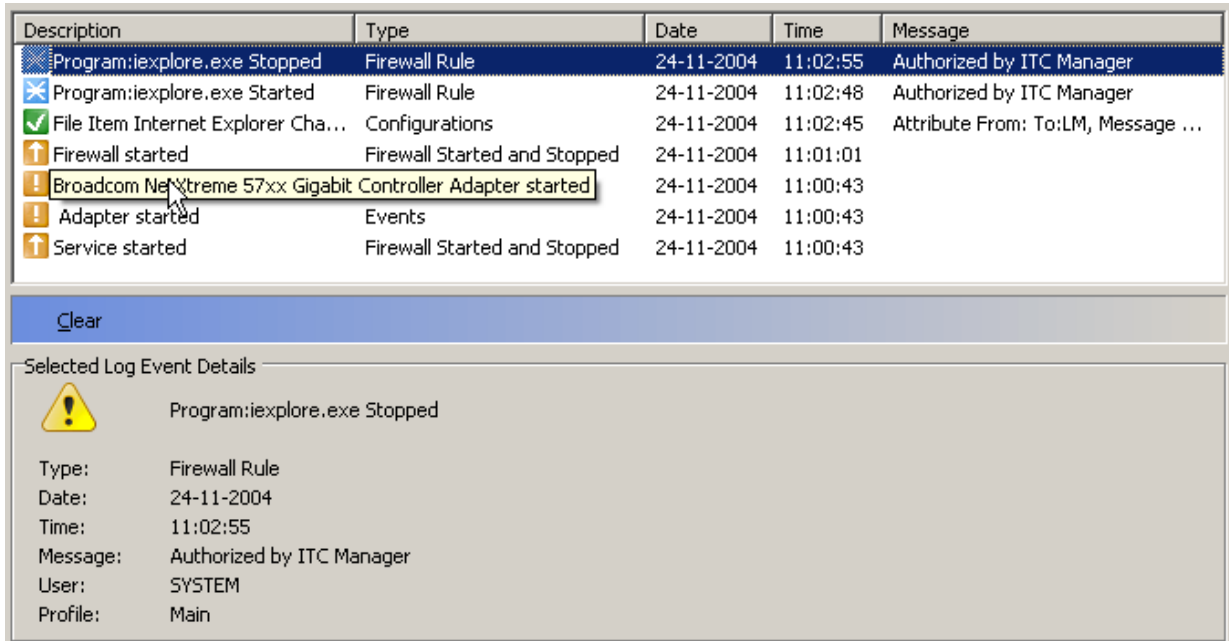
NetOp Desktop Firewall Window








Program Manager: Select this command or the *View* menu *Program Manager* command or click the *Information* toolbar *Program Manager* button to display the *Program Manager* display pane, see section 3.3.5.2.5, "Program Manager".

3.3.5.2.1 Event Log

This display pane always displays logged firewall events as specified on *Firewall Rule* events of firewall rule records. Logging of operational events, which is optional, is set up in the *Options* window *Event Log* tab whose *Log* attribute is enabled, see e.g. section 3.3.5.1.1, "Programs".


Select the *NetOp Desktop Firewall* window *View* menu or work panel selection pane *Information* section *Event Log* command or click the *Information* toolbar *Event Log* button to display this display pane:



Description	Type	Date	Time	Message
 Program:iexplore.exe Stopped	Firewall Rule	24-11-2004	11:02:55	Authorized by ITC Manager
 Program:iexplore.exe Started	Firewall Rule	24-11-2004	11:02:48	Authorized by ITC Manager
 File Item Internet Explorer Cha...	Configurations	24-11-2004	11:02:45	Attribute From: To:LM, Message ...
 Firewall started	Firewall Started and Stopped	24-11-2004	11:01:01	
 Broadcom NetXtreme 57xx Gigabit Controller Adapter started	Events	24-11-2004	11:00:43	
 Adapter started	Events	24-11-2004	11:00:43	
 Service started	Firewall Started and Stopped	24-11-2004	11:00:43	

Clear

Selected Log Event Details

 Program:iexplore.exe Stopped

Type: Firewall Rule
Date: 24-11-2004
Time: 11:02:55
Message: Authorized by ITC Manager
User: SYSTEM
Profile: Main

The upper pane contains event log records in a table with the column contents:

Description: Event type icon and description of event.

Note: The names of event type icons are displayed in the Legend pane, see below.

Type: Event type name.

Date: Event date.

Time: Event time of day.

Message: Event message, if any.

Note: A Firewall Rule event of a firewall rule record whose Message attribute is enabled will display a message.

User: Windows logon name of the computer user causing the event or *SYSTEM* if the event is caused by the firewall or the operating system.

Profile: Profile assigned at the time of the event.

Table controls are explained in section 1.5.3, "Table Controls".

Select a record in the pane to display this information in the lower *Log Description* section:

<Event Log icon> and event description.

Type: Event type name.

Date: Event date.

Time: Event time of day.

Message: Event message, if any.

User: Windows logon name of the computer user causing the event or *SYSTEM* if the event is caused by the firewall or the operating system.

Profile: Profile assigned at the time of the event.

Clear: Click this button or select the right-click popup menu *Clear* command to clear the *Event Log* contents.

Note: Event Log entries older than a specified period are removed automatically, see section 3.4.1.4, "Event Log Tab".

Refresh: Click this button or select the right-click popup menu *Refresh* command to refresh the *Event Log* display.

Note: To protect the user interface from becoming overloaded, the firewall driver sends its recorded events to the user interface only at intervals. To retrieve the most recent firewall driver events to display them, refresh.

Right-click in the pane to display this menu:



This menu contains these commands:

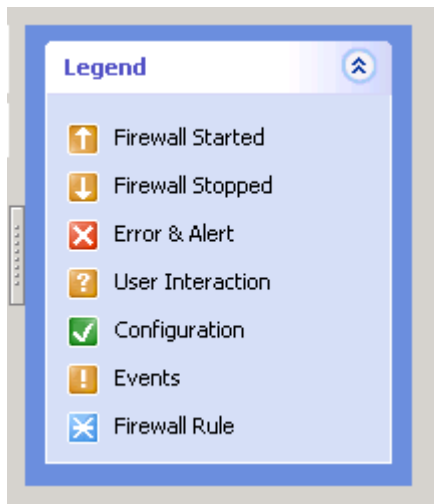
Clear: Select this command or click the *Clear* button to clear the *Event Log* contents.

Note: Event Log entries older than a specified period are removed automatically, see section 3.4.1.4, "Event Log Tab".

Refresh: Select this command or click the *Clear* button to refresh the *Event Log* display.

Note: To protect the user interface from becoming overloaded, the firewall driver sends its recorded events to the user interface only at intervals. To retrieve the most recent firewall driver events to display them, refresh.

Legend: Select this command or click the *Information* toolbar *Legend* button to open/close this pane in the right side of the display pane:



By default, the pane is closed. When the pane is opened, the *Legend* button is framed. Click the button in the pane separator to hide/display the pane.

This pane contains a *Legend* section. Click the up button to collapse and down button to expand the section.

This section displays available event type icons and their matching event type names.

3.3.5.2.2 Packet Log

This display pane displays firewall detected *Program Opened*, *Program Closed*, *Program Killed* and computer communication interface data packet events.

Select the *NetOp desktop Firewall* window *View* menu or work panel selection pane *Information* section *Packet Log* command or click the *information* toolbar *Packet Log* button to display this display pane:

Process Name	Action	Protocol description	Remote IP Address	Local Port	Remote Port	Parent Process Nam
→ iexplore.exe	Process allowed	TCP, Transmission Control	129.142.90.62	2461	80	explorer.exe
← iexplore.exe	Process allowed	TCP, Transmission Control	129.142.90.62	2461	80	explorer.exe
→ iexplore.exe	Process allowed	TCP, Transmission Control	129.142.90.62	2461	80	explorer.exe
→ iexplore.exe	Process allowed	TCP, Transmission Control	129.142.90.62	2461	80	explorer.exe
← iexplore.exe	Process allowed	TCP, Transmission Control	129.142.90.62	2462	80	explorer.exe
← iexplore.exe	Process allowed	TCP, Transmission Control	129.142.90.62	2461	80	explorer.exe
→ iexplore.exe	Process allowed	TCP, Transmission Control	129.142.90.62	2461	80	explorer.exe

0	00 0F 1F 8E 26 67 00 04 80 2B B9 00 08 00 45 00 05 DC	...&g...+¹...E..Û.ë@
18	90 EB 40 00 78 06 69 54 81 8E 5A 3E C0 A8 66 67 00 50	.x.iT..Z>Ä'fg.P..6SIF
36	09 9D 36 53 CF 46 37 A0 E2 94 50 10 FD 8A DD F0 00 00	7 ä.P.ý.ÿ8.. "<a href
54	22 3E 3C 61 20 68 72 65 66 3D 22 2F 5F 41 62 6F 75 74	="/_About+Danware/_Ma
72	2B 44 61 6E 77 61 72 65 2F 5F 4D 61 6E 61 67 65 6D 65	nagement/_Contact+CEO
90	6E 74 2F 5F 43 6F 6E 74 61 63 74 2B 43 45 4F 22 3E 43	">Contact CEO - Your
108	6F 6E 74 61 63 74 20 43 45 4F 20 2D 20 59 6F 75 72 20	link to the top<b
126	6C 69 6E 6B 20 74 6F 20 74 68 65 20 74 6F 70 3C 2F 61	r></td>.</tr>
144	3E 3C 62 72 3E 3C 2F 73 70 61 6E 3E 3C 2F 74 64 3E 0A	</table>.</div>.</td>
162	3C 2F 74 72 3E 0A 3C 2F 74 61 62 6C 65 3E 0A 3C 2F 64	.<td valign="bottom">
180	69 76 3E 0A 3C 2F 74 64 3E 0A 3C 74 64 20 76 61 6C 69	.<table border="0" ce

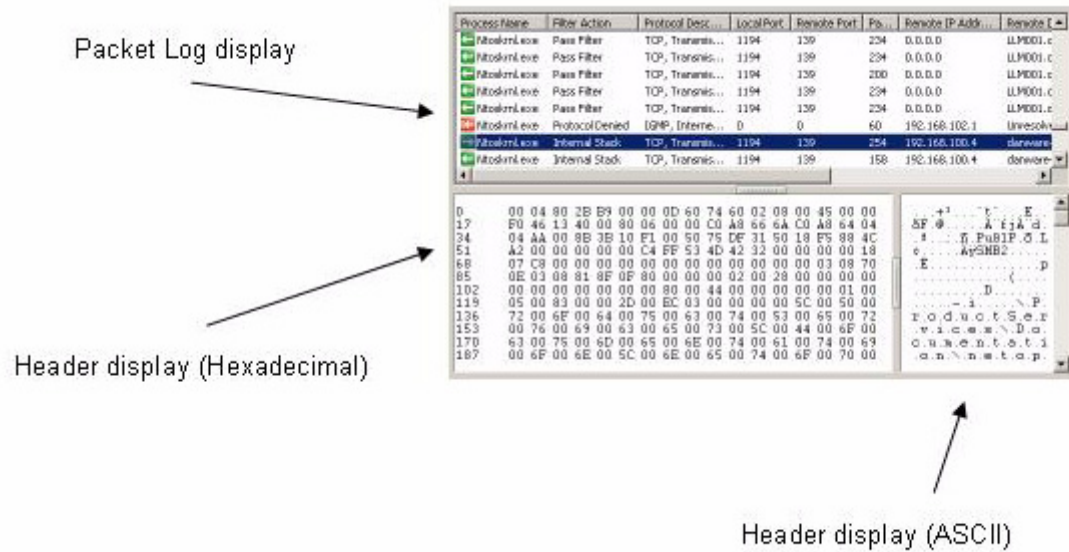
Use the *Packet Log* to trouble-shoot programs that are not functioning as expected. By looking at the *Action* column you can see what action the firewall takes, for example *Process allowed*.

The display pane contains an upper records pane, a lower left hexadecimal pane and a lower right ASCII pane, see the subsection “Records, Hexadecimal and ASCII Panes” below.

A pane containing *Legend* and *Record Colors* sections can be added in the right side of the display pane, see the subsection “Legend and Record Colors Pane” below. Hide/display this pane by clicking the button in the pane separator.

By default, *Packet Log*, *Traffic Matrix* and *Statistics* play displaying what is currently happening on the firewall. Play controls are explained in the “Play Controls” subsection below.

Records, Hexadecimal and ASCII Panes



The *Packet Log* display pane records pane contains table records of firewall detected events in chronological descending order (last packets first).

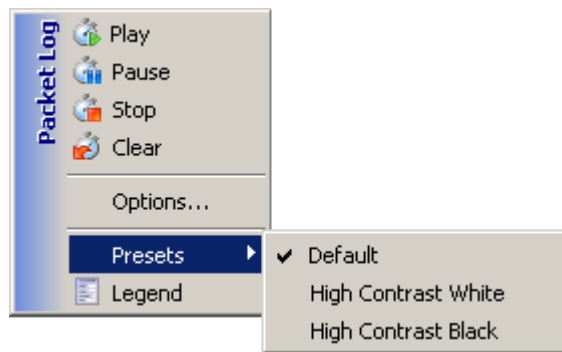
Table columns are specified on the *Options* window *Packet Log* tab, see section 3.4.1.5, "Packet Log Tab".

Table controls are explained in section 1.5.3, "Table Controls".

Select a record to display the data packet header and first 100 bytes of data in matching lines in hexadecimal representation in the lower left hexadecimal pane and in ASCII character representation in the lower right ASCII pane.

Drag pane separators to mutually resize panes. Hide/display the lower right ASCII pane by clicking the button in the vertical pane separator. Hide/display both lower panes by clicking the button in the horizontal pane separator.

Right-click a records pane table cell to display this popup menu:



This menu contains the commands:

The top section contains play control commands that are explained in the "Play Controls" subsection below.

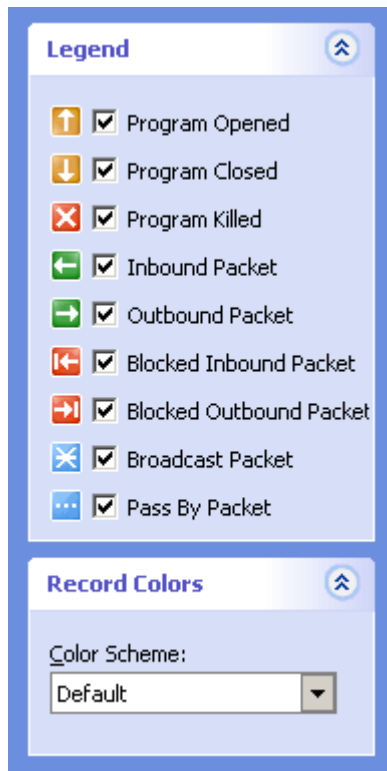
Options...: Select this command to display the *Options* window displaying the *Packet Log* tab to specify *Packet Log* columns, see section 3.4.1.5, "Packet Log Tab".

Presets: This command expands into available color schemes, see section 3.4.1.6, "Colors Tab". The applied color scheme (default: *Default*) is checkmarked. Select an uncheckmarked color scheme or select a color scheme in the *Legend and Record Colors* pane *Color Scheme* drop-down box to apply it, see the "Legend and Record Colors Pane" subsection below.

Drag across contents in the hexadecimal or ASCII panes and right-click to display a *Copy* popup command. Select this command or press CTRL+C to copy selected contents to the clipboard.

Legend and Record Colors Pane

Click the *Play* toolbar *Legend* button, see section 3.3.4.4, "Play Toolbar", to add/remove (default: removed) this pane in the right side of the *Packet Log* display pane:



Click the button in the pane separator to hide/display this pane.

This pane contains the sections *Legend* and *Record Colors*. Click the up button to collapse and down button to expand a section.

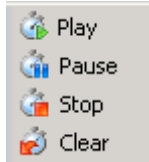
Legend: This section provides both packet filtering options and a legend to the icons displayed in the left records pane column. By default all will be listed in the display pane (all icons are checked). If the user only wants information about blocked packets, only these checkmarks should remain.

Note: *The filter only influences what gets listed in the display pane.*

Record Colors: This section contains a *Color Scheme* drop-down box. A color scheme specified on the *Options* window *Colors* tab specifies different foreground (characters) and background colors for records of different types of events to facilitate distinguishing them from each other, see section 3.4.1.6, "Colors Tab".

Color Scheme: []: The field of this drop-down box displays the name of the selected color scheme (default: *Default*). The drop-down box list contains the names of available color schemes. Select a color scheme name in the list to display it in the field or select in the records pane right-click popup menu expanded *Presets* command a color scheme command to apply it, see the "Records, Hexadecimal and ASCII Panes" section above.

Play Controls



The playing of *Packet Log*, *Traffic Matrix* and *Statistics* is controlled from these play controls:

Play: Select the display pane (*Packet Log*: records pane) right-click popup menu *Play* command or click the *Play* toolbar *Play* button to start playing after *Pause* or *Stop*. While playing, the toolbar button is framed (default: playing).

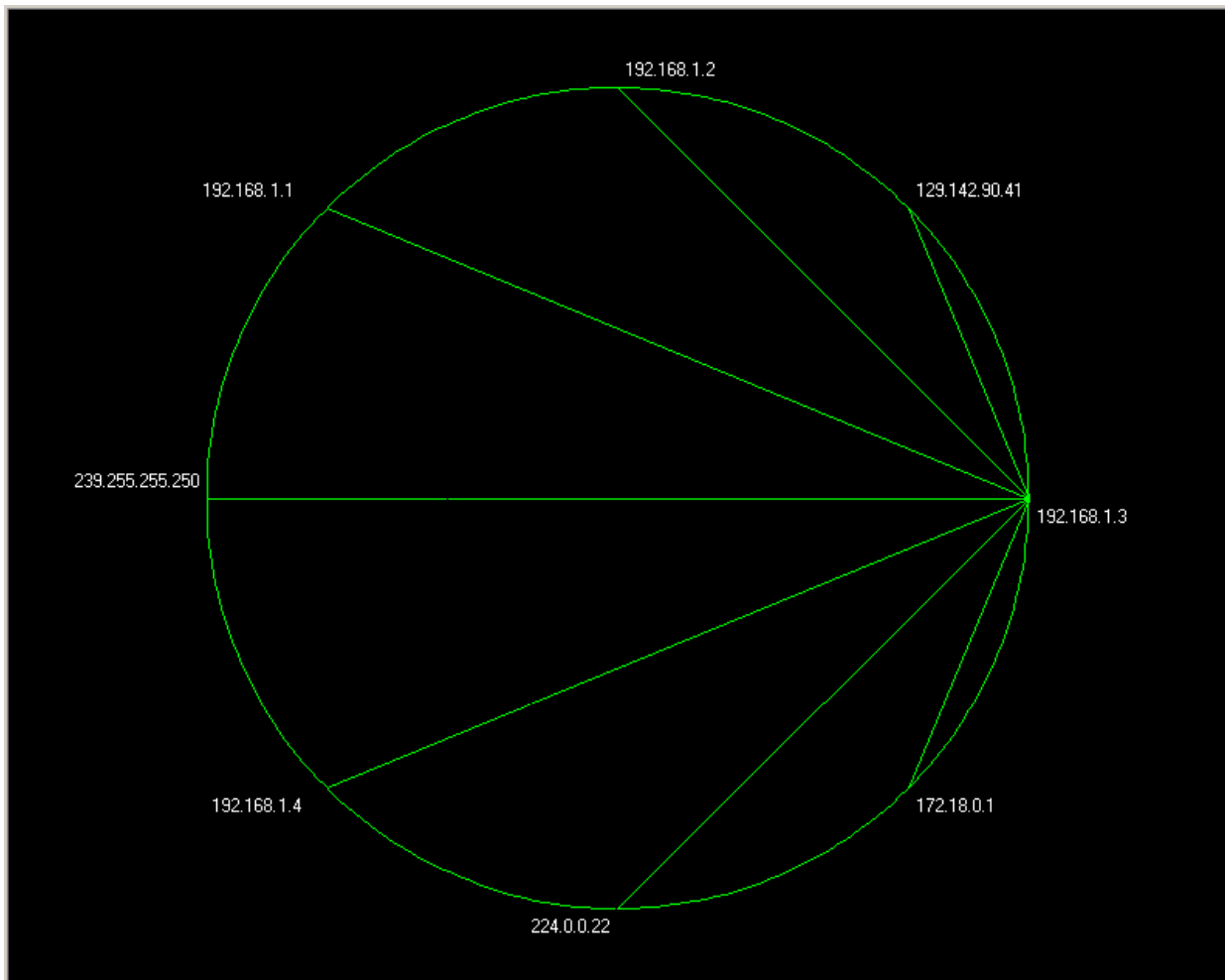
Pause: Select the display pane (*Packet Log*: records pane) right-click popup menu *Pause* command or click the *Play* toolbar *Pause* button to pause playing. When selecting *Play* after *Pause*, new data will be added to existing data. While paused, the toolbar button is framed.

Stop: Select the display pane (*Packet Log*: records pane) right-click popup menu *Stop* command or click the *Play* toolbar *Stop* button to stop playing. When selecting *Play* after *Stop*, existing data will be cleared and new data will be added. While stopped, the toolbar button is framed.

Clear: Select the display pane (*Packet Log*: records pane) right-click popup menu *Clear* command or click the *Play* toolbar *Clear* button to clear the records pane contents without changing the current *Play*, *Pause* or *Stop* status.

3.3.5.2.3 Traffic Matrix

Select the *NetOp Firewall* window *View* menu or work panel selection pane *Information* section *Traffic Matrix* command or click the *Information* toolbar *Traffic Matrix* button to display this display pane:

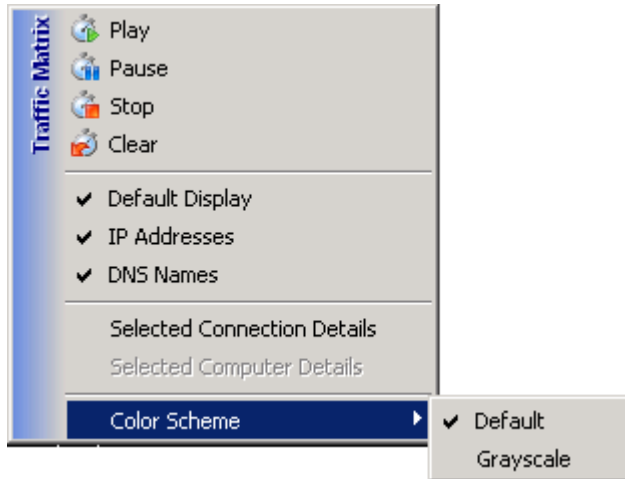


This display pane graphically displays firewall detected data packet traffic at the computer communication interface. Traffic is displayed as *Connection* lines between circle *Computer* points labeled by their IP address and Domain Name Service (DNS) name, if the IP address was resolved into a DNS name.

Connection lines can gradually change their color from an initial color to a final color through a number of color shades to visualize traffic development.

By default, *Packet Log*, *Traffic Matrix* and *Statistics* play displaying what is currently happening on the firewall. Play controls are explained in the “Play Controls” subsection below.

Right-click to display this popup menu:



This menu contains these commands:

The top section contains play control commands that are explained in the “Play Controls” section, see page 87.

Default Display: Select this command to uncheckmark/checkmark it (default: checkmarked). When checkmarked, the circle is centered in the display pane and its size is adapted to the display pane size. When uncheckmarked, the circle can be resized and moved:

Press the keyboard up arrow or PAGEUP to increase the circle diameter in small or large steps.

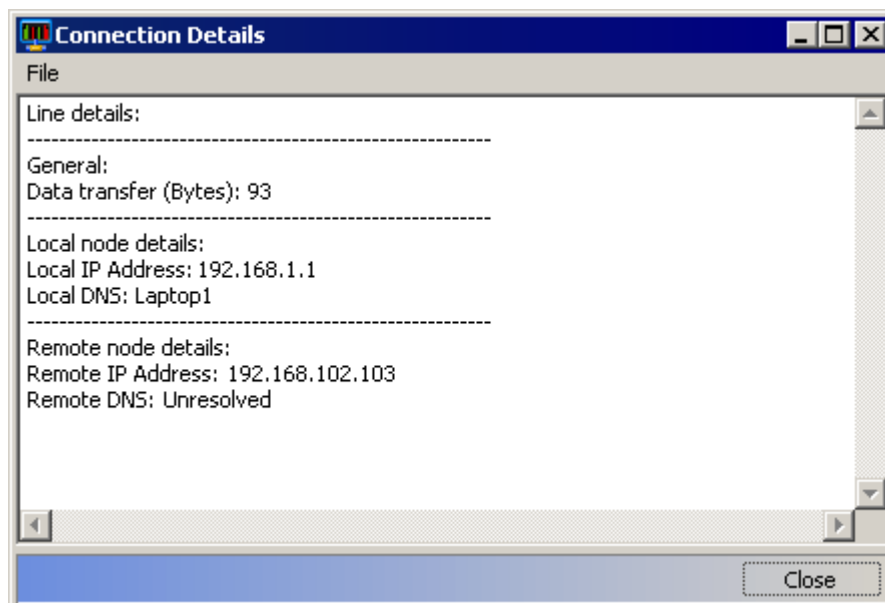
Press the keyboard down arrow or PAGEDOWN to decrease the circle diameter in small or large steps.

Press SHIFT and drag to move the circle.

IP Addresses: Select this command to uncheckmark/checkmark it (default: checkmarked). When checkmarked, circle *Computer* points are labeled by their IP address.

DNS Names: Select this command to uncheckmark/checkmark it (default: checkmarked). When checkmarked, circle *Computer* points are labeled by their DNS name.

Selected Connection Details: Select a *Connection* line across the circle to highlight it and select this command to display this window:



NetOp Desktop Firewall Window

This window displays details of the selected *Connection*.

Window controls are explained in section 1.5.1, "Window Controls".

Select *File* to display this menu:

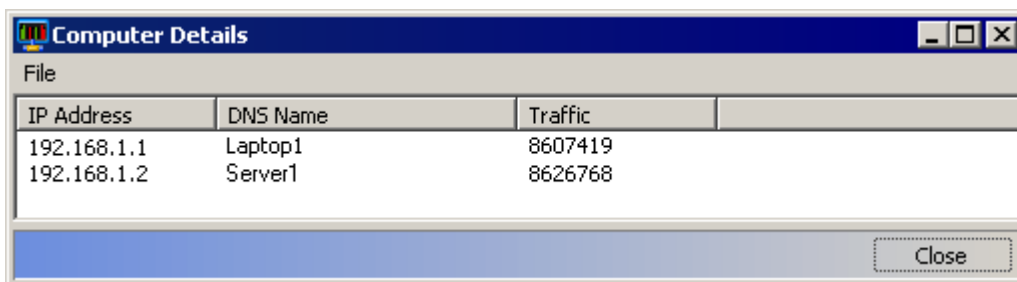


This menu contains these commands:

Save As...: Select this command to display a Windows *Save As* window displaying *Files of type: Text files (*.Txt)*. Specify a file name and click *Save* to save the pane contents as a text file.

Exit: Select this command or the matching window control menu command or click the *Close* window control button to close the window.

Selected Computer Details: Select a *Computer* label outside the circle to highlight it and select this command to display this window:



This window displays details of the selected *Computer*.

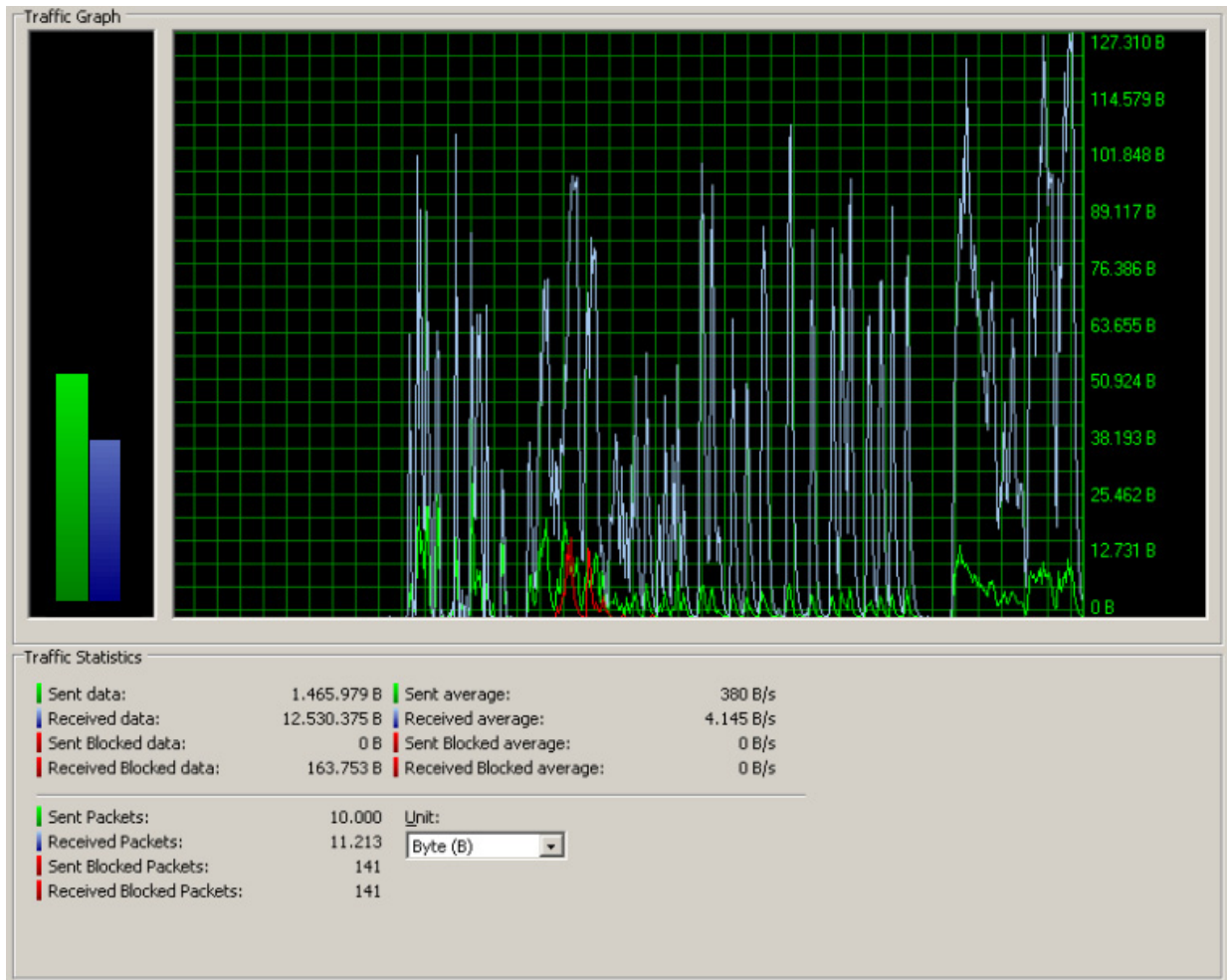
Window controls are explained in section 1.5.1, "Window Controls".

File menu contents are the same as in the *Connection Details* window explained above.

Color Scheme: This command expands into available *Color Schemes*. The applied *Color Scheme* (default: *Default*) is checkmarked. Select an uncheckmarked *Color Scheme* to apply it. See section 3.4.1.6, "Colors Tab".

3.3.5.2.4 Statistics

Select the *NetOp Desktop Firewall* window *View* menu or work panel selection pane *Information* section *Statistics* command or click the *Information* toolbar *Statistics* button to display this display pane:



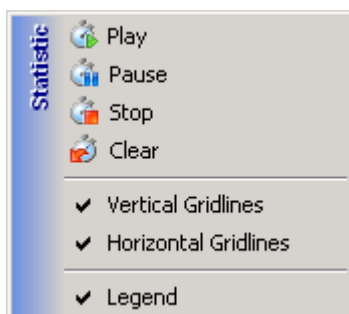
This display pane displays statistics on sent, received and blocked data packets.

By default, *Packet Log*, *Traffic Matrix* and *Statistics* play displaying what is currently happening on the firewall. Play controls are explained in the “Play Controls” subsection on page 87 .

Traffic Graph

The left meter graph displays the current volume of sent (green), received (blue) and blocked (red) data. The right line graph displays the same values historically.

Right-click in the line graph area to display this popup menu:



This menu contains these commands:

NetOp Desktop Firewall Window

The top section contains play control commands that are explained in the “Play Controls” on page 87.

Vertical Gridlines: Select this command to uncheckmark/checkmark it (default: checkmarked). When checkmarked, vertical gridlines are displayed in the line graph.

Horizontal Gridlines: Select this command to uncheckmark/checkmark it (default: checkmarked). When checkmarked, horizontal gridlines are displayed in the line graph.

Legend: Select this command to uncheckmark/checkmark it (default: checkmarked). When checkmarked, a scale is displayed at the right border of the line graph. The legend has the same unit as selected in the *Unit* drop-down box.

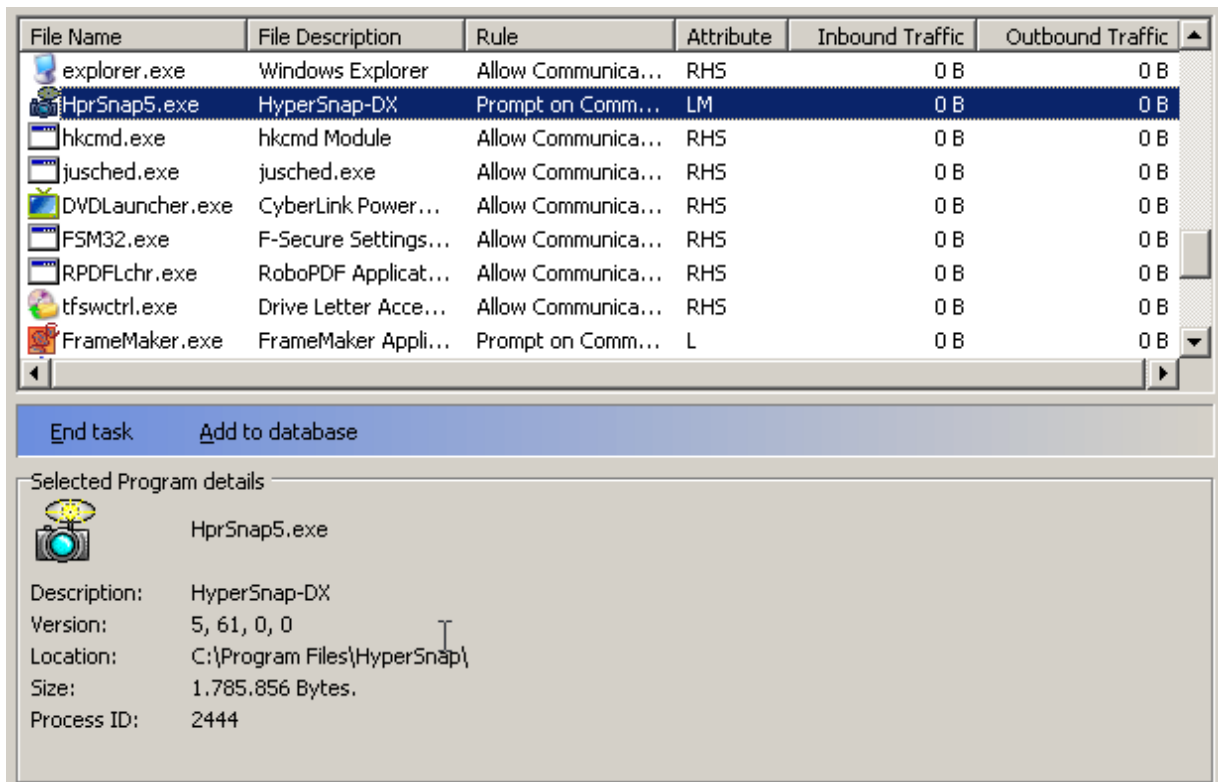
Traffic Statistics

The upper part of the section displays total and average data amounts over the recording period.

The lower part of the section displays total packets over the recording period and a *Unit* drop-down box for selecting the desired data amount unit in Bytes (B) or Bits (bit) with prefixes K (Kilo), M (Mega) or G (Giga).

3.3.5.2.5 Program Manager


Select the *NetOp Desktop Firewall* window *View* menu or work panel selection pane *Information* section *Program Manager* command or click the *Information* toolbar *Program Manager* button to display this display pane:



File Name	File Description	Rule	Attribute	Inbound Traffic	Outbound Traffic
explorer.exe	Windows Explorer	Allow Communica...	RHS	0 B	0 B
HprSnap5.exe	HyperSnap-DX	Prompt on Comm...	LM	0 B	0 B
hkcmd.exe	hkcmd Module	Allow Communica...	RHS	0 B	0 B
jusched.exe	jusched.exe	Allow Communica...	RHS	0 B	0 B
DVDLauncher.exe	CyberLink Power...	Allow Communica...	RHS	0 B	0 B
FSM32.exe	F-Secure Settings...	Allow Communica...	RHS	0 B	0 B
RPDFLchr.exe	RoboPDF Applicat...	Allow Communica...	RHS	0 B	0 B
tfswctrl.exe	Drive Letter Acce...	Allow Communica...	RHS	0 B	0 B
FrameMaker.exe	FrameMaker Appli...	Prompt on Comm...	L	0 B	0 B

End task Add to database

Selected Program details

 HprSnap5.exe

Description: HyperSnap-DX
Version: 5, 61, 0, 0
Location: C:\Program Files\HyperSnap\
Size: 1.785.856 Bytes.
Process ID: 2444

This display pane displays programs running on the computer.

The upper pane displays program file records with details in columns according to the specification on the *Options* window *Program Manager* tab, see section 3.4.1.7, "Program Manager Tab".

Table controls are explained in section 1.5.3, "Table Controls".

Select a record in the pane to display this information in the lower *Selected Program details* section:

<File icon> and file name

Description: File description, if available.

Version: File version, if available.

Location: File path.

Size: File size.

Process ID: Process identification number (PID).

The buttons below the pane have this functionality:

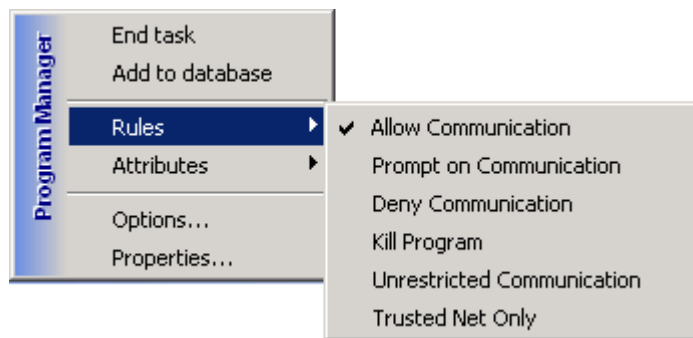
End Task: Select a record and click this button to close the record program. Take into consideration that ending any selected program will stop it from running immediately - including SYSTEM processes.

Caution: *Do not close a Windows program, as this can cause computer malfunction. Windows program files typically reside in the system directory, <Boot drive letter>:\Windows\ (XP) or <Boot drive letter>:\WINNT\ (2000).*

Add to database: Select a record and click this button to add a record of the file in the *Programs* display pane, see section 3.3.5.1.1, "Programs".

Note: *A record added to the Programs display pane will be assigned the firewall rule Prompt on Communication if the Run only authorized programs box is unchecked and Kill Program if the Run only authorized programs box is checked, see section 3.4.1.1, "General Tab".*

Right-click a record or select multiple records and right-click to display this popup menu:



This menu contains these commands:

Note: *Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".*

End task: Select this command to close the selected record program. Take into consideration that ending any selected program will stop it from running immediately - including SYSTEM processes.

Add to database: Select this command to add records of selected record files in the *Programs* display pane, see section 3.3.5.1.1, "Programs". This command will have no effect on files for which a record already exists in the *Programs* display pane.

Rules: This command expands into commands of program firewall rules. The command of the firewall rule assigned to the selected record file *Programs* display pane record is checkmarked. It is not possible to change the attributes in this view.

Attributes: This command expands into commands of available attributes. Commands of attributes assigned to the selected record file *Programs* display pane record are checkmarked. It is not possible to change the attributes in this view.

Options...: Select this command to display the *Options* window *Program Manager* tab to specify *Program Manager* display pane columns, see section 3.4.1.7, "Program Manager Tab".

Properties...: Select this command to display the Windows <File name> *Properties* window to view and edit the Windows properties of the selected record file.

3.3.5.3 Profiles



This work panel selection pane section selects, adds, edits and removes profiles and specifies profile rules.

Note: Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".

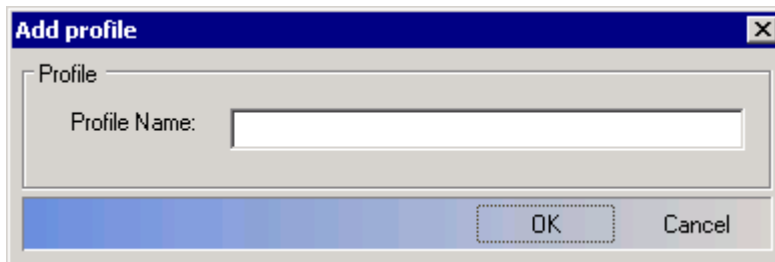
Initially, *NetOp Desktop Firewall* has one main profile named *Main*. Sub-profiles of this profile can be created to apply different sets of firewall rules in different computer environments.

Select Profile: []: The field of this drop-down box displays the name of the selected profile (default: *Main*). The drop-down box list contains the names of available profiles. Select a profile name in the list to display it in the field to display its firewall rules in the *Firewall Rules* display panes and apply them.

Note: A profile can also be selected in the notification area button menu, see section 3.2.2, "Notification Area Button Menu".

If selecting a profile fails, it will typically be because its profile rule prohibits switching into it if its profile rule is not met, see section 3.3.5.3.1, "Profile Rules".

Add...: Select this command to display this window:

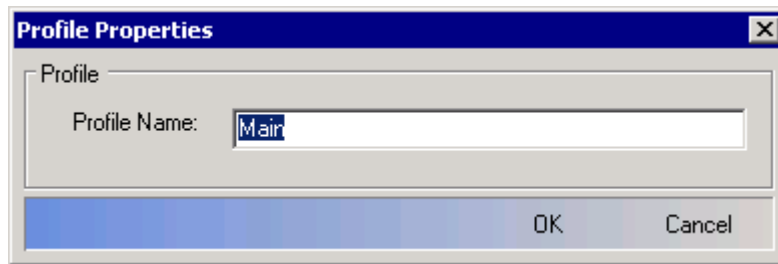


This window adds a profile.

Profile Name: []: Specify in the field the profile name.

Click *OK* to add this profile to the *Select Profile* drop-down box list and make it the selected profile.

Edit...: Select this command to display this window:



This window edits the name of the selected profile.

Profile Name: []: Edit the profile name in the field as desired.

Remove...: Select this command to display a confirmation window to confirm removing the selected profile.

Note: The main profile cannot be removed.

Rules...: Select this command to display the *Profile Rules* window, see section 3.3.5.3.1, "Profile Rules", to specify profile rules.

Note: Profile rules can automatically select a profile that matches the computer environment and disable selecting a profile if its rule is not met by the computer environment.

Profile Records

The main profile and its sub-profiles contain the same records in the *Programs*, *Ports*, *Protocols*, *Trusted Nets* and *Banned Nets* display panes.

Each record can have different *Rule*, *Attributes* and *Message* in different profiles to satisfy different firewall rule demands in different computer environments.

The records of a newly added profile have the same *Rule*, *Attributes* and *Message* as the matching main profile records.

To specify the record *Rule*, *Attributes* and *Message* of a profile, select the profile and edit records in the *Programs*, *Ports*, *Protocols*, *Trusted Nets* and *Banned Nets* display panes as desired.

Note: sub-profile records with the attribute System cannot be edited.

The *Rule*, *Attributes* and *Message* of records in sub-profiles will appear gray if they are the same as in the main profile and black if they are different.

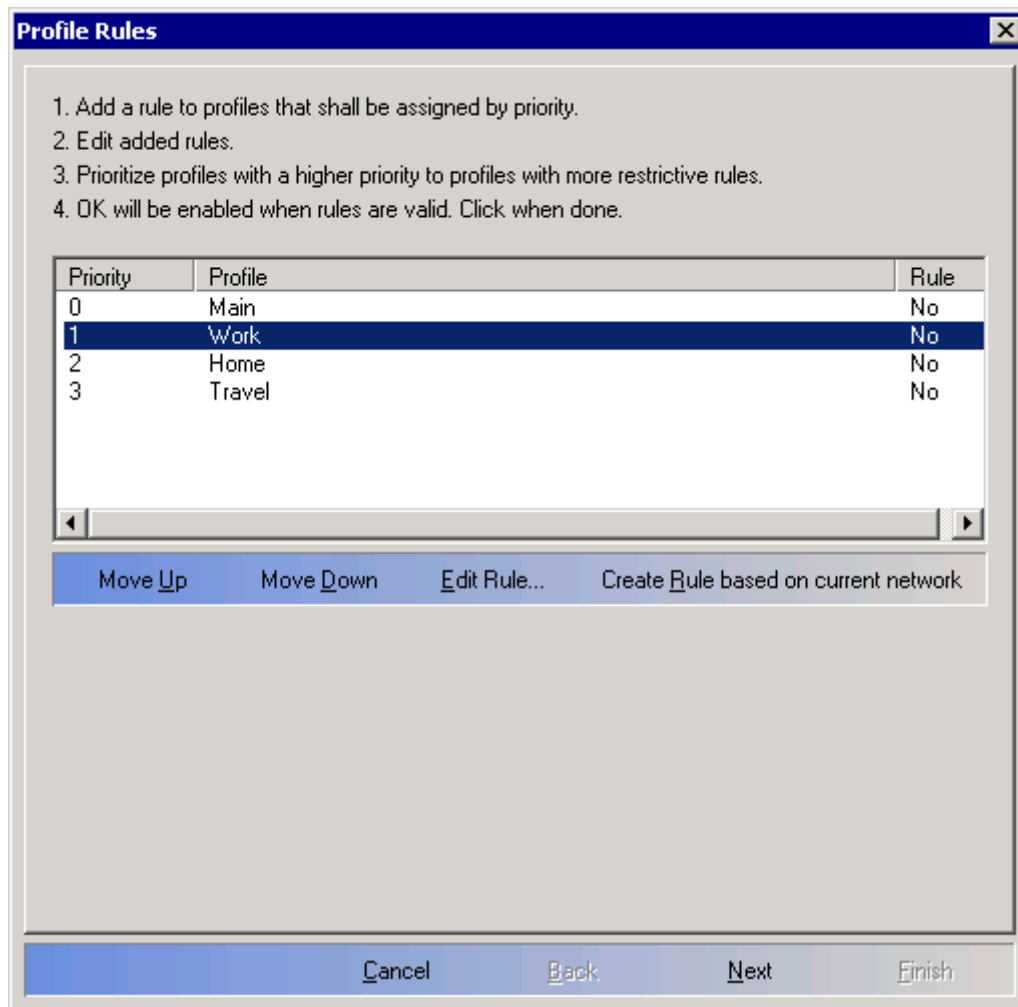
Record's Color Code

If a computer is part of a *NetOp Policy Server* controlled domain, the user only is allowed to change the firewall rule if the text preceding the record-icon is blue. Records whose firewall rule must not be changed have black text.

If the text is grey, the record has a inherited firewall rule. The heritage records occur if the computer has more than one profile. If the computer has two profiles, *Main* and *Home*, firewall rules are inherited from the *Main* profile to the *Home* profile. Some of the *Main* firewall rules do not necessarily apply to the home network. This means that the user can apply a firewall rule that fits their needs.

3.3.5.3.1 Profile Rules

Select the work panel selection pane *Profiles* section *Rules...* command to display this window:



This window specifies profile rules.

Its pane displays prioritized records of profiles in a table with these column contents:

Priority: Profile priority number. 0 indicates the highest priority profile whose rule will be tested first against detected computer environment properties. If a profile rule is not met, the rule of the next lower priority profile will be tested. The first found profile whose rule is met will be assigned to the firewall. If the test reaches the end of the prioritized list without rules being met, the last profile in the list will be assigned even if its rule is not met.

Profile: Profile name.

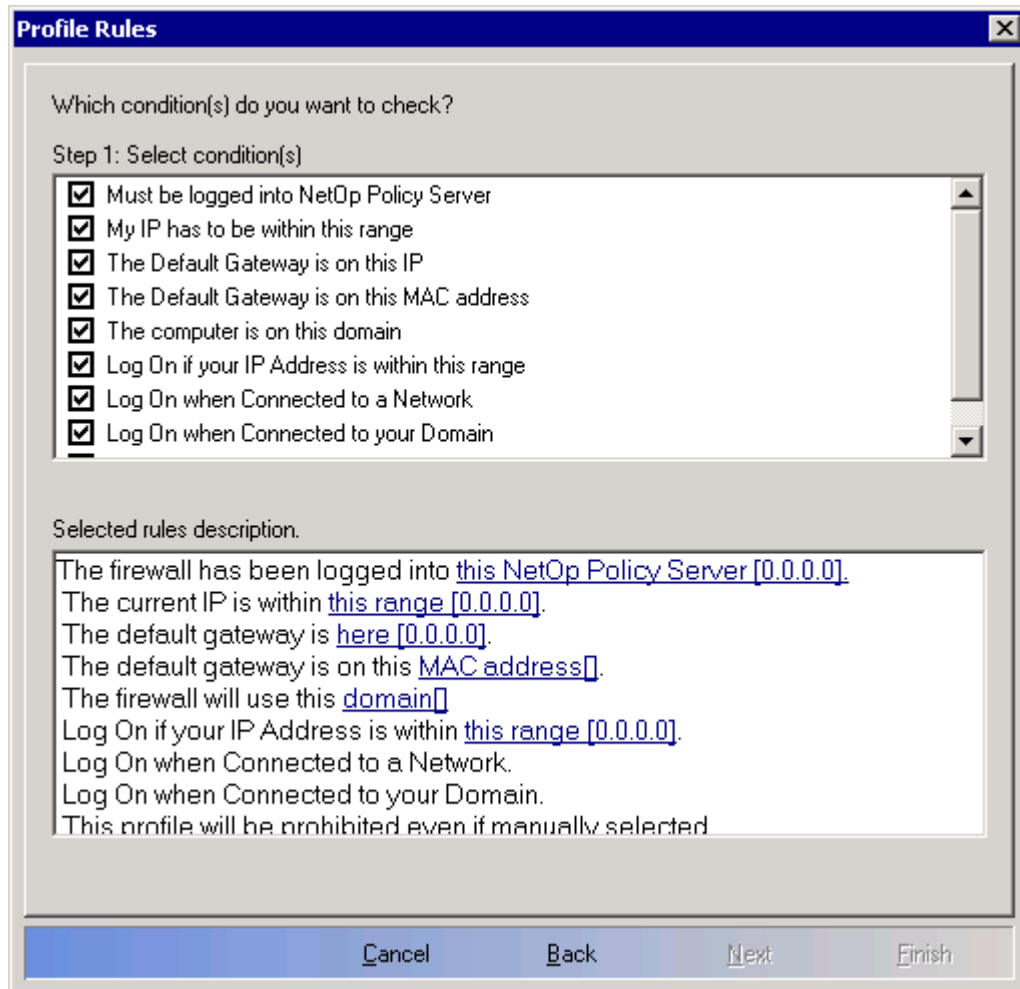
Note: To illustrate this, three sub-profiles named **Work, Home and Travel** have been added to the **Main** profile in the window shown above.

Rule: Displays *No* (default) if no rule is specified or *Yes* if a rule is specified for this profile.

Table controls are explained in section 1.5.3, "Table Controls".

Move Up/Move Down: Select a profile record in the pane and click one of these buttons to move it up or down to change its priority.

Edit Rule...: Select a profile record and click this button or the *Next >* button below to display this rule editing page:



This page specifies a profile rule in an upper *Conditions* pane and a lower *Values* pane.

If a profile record with no rule (displaying *No* in the *Rule* column) was selected on the front page of the window, the boxes in the *Conditions* pane are unchecked and the *Values* pane is blank. Check boxes in the *Conditions* pane to display matching value statements in the *Values* pane.

Note: To illustrate this, the image above displays this page after selecting a profile record with no rule and checking all boxes in the *Conditions* pane to display all available value statements in the *Values* pane.

The upper *Conditions* pane contains these checked conditions:

Must be logged into NetOp Policy Server: Check this box to assign the selected profile only if the firewall is logged on to a *NetOp Policy Server* with the IP address specified in the matching value statement in the *Values* pane.

My IP has to be within this range: Check this box to assign the selected profile only if the IP address of the firewall computer is within the IP address range specified in the matching value statement in the *Values* pane.

The Default Gateway is on this IP: Check this box to assign the selected profile only if the IP address of the default gateway on the firewall computer network is the IP address specified in the matching value statement in the *Values* pane.

NetOp Desktop Firewall Window

[] The Default Gateway is on this MAC address: Check this box to assign the selected profile only if the MAC address of the default gateway on the firewall computer network is the MAC address specified in the matching value statement in the *Values* pane.

[] The computer is on this domain: Check this box to assign the selected profile only if the domain of the firewall computer is the domain specified in the matching value statement in the *Values* pane.

[] Log On if your IP Address is within this range: Check this box to log on *NetOp Desktop Firewall* to the *NetOp Policy Server* address specified in the first value statement if the IP address of the firewall computer is within the IP address range specified in the matching value statement in the *Values* pane.

[] Log On when connected to a Network: Check this box to log on to the *NetOp Policy Server* address specified in the first value statement if the firewall computer is connected to a network (i.e. any network connected to the Internet).

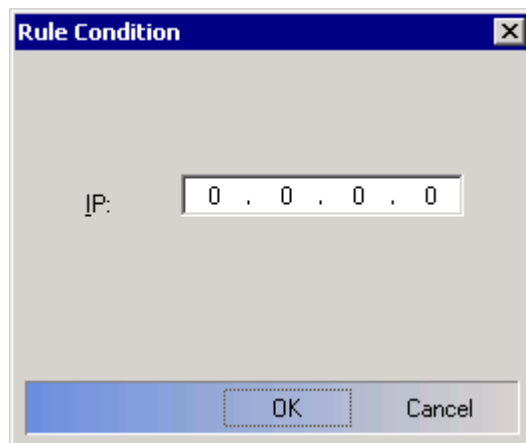
[] Log On when connected to your Domain: Check this box to log on to the *NetOp Policy Server* address specified in the first value statement if the firewall computer is connected to the local area network that recognizes it as a domain computer.

[] Prohibit switching into this profile when rules are not met: Check this box to disable selecting this profile if its rule is not met by the computer environment properties.

Note: This condition is not applicable to the lowest priority profile rule.

The lower *Values* pane will contain statements matching checked conditions in the *Conditions* pane specifying a value within square brackets (default: no value) if applicable.

Select [this NetOp Policy Server \[0.0.0.0\]](#) to display this window:



Specify the required *NetOp Policy Server* IP address in the field and click *OK* to insert it between the value statement square brackets.

Select [this range \[0.0.0.0\]](#) to display this window:

Specify in the *From* field the lowest IP address and in the *To* field the highest IP address in the required firewall computer IP address range and click *OK* to insert the range between the value statement square brackets.

Select [here \[0.0.0.0\]](#) to display this window:

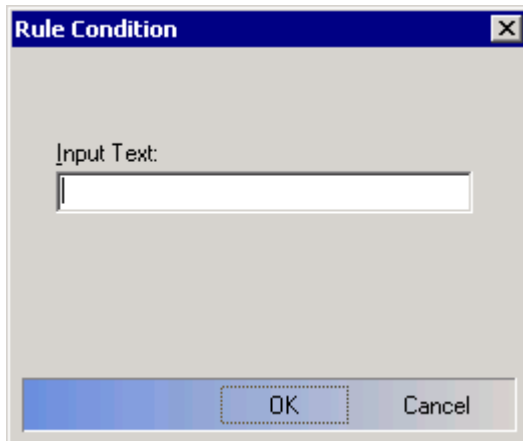
Specify the required default gateway IP address in the field and click *OK* to insert it between the value statement square brackets.

Select [MAC address \[\]](#) to display this window:

NetOp Desktop Firewall Window

Specify the required default gateway MAC address in the field and click *OK* to insert it between the value statement square brackets.

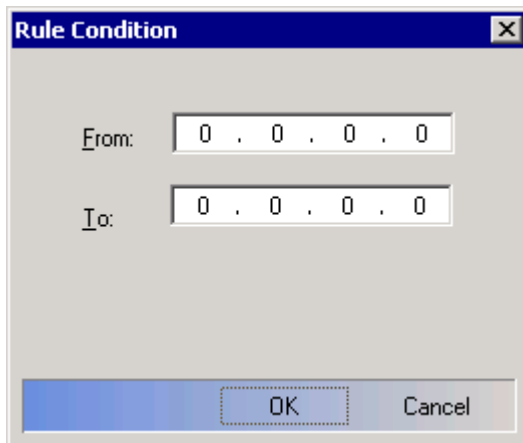
Select [domain \[\]](#) to display this window:



The screenshot shows a dialog box titled "Rule Condition" with a close button (X) in the top right corner. Inside the dialog, there is a label "Input Text:" followed by a single-line text input field. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Specify the required domain name in the field and click *OK* to insert it between the value statement square brackets.

Select the "Log On" [this range \[0.0.0.0\]](#) to display this window:



The screenshot shows a dialog box titled "Rule Condition" with a close button (X) in the top right corner. Inside the dialog, there are two labels: "From:" and "To:". Each label is followed by a four-part IP address input field, with each part containing the digit "0" and separated by a period. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Specify in the *From* field the lowest IP address and in the *To* field the highest IP address in the "Log On" required firewall computer IP address range and click *OK* to insert the range between the value statement square brackets.

When valid values have been specified in all value statements in the lower *Values* pane, the *Finish* button will become enabled.

Click < *Back* to return to the front page of the window to apply rules to other profiles.

Create/Remove Rule based on current network: Select a record in the pane and click this button to automatically specify a rule identifying the network currently connected to or remove a specified rule. An automatically specified rule should be reviewed, as it may need editing to become valid.

Finally, make the profile assignment-test work as intended by placing the profile records in a priority order.

Note: *Add a rule to profiles that shall be assigned by priority. Edit the added rules. Prioritize profiles with a higher priority to profiles with more restrictive rules. Otherwise, a less restrictive rule profile will be used before the more restrictive rule profile.*

When profile rules and priority have been specified, click *Finish* to close the window and apply the profile rules.

3.3.6 Status Bar



The status bar contains these fields:

[*IP*: <IP Address>]: This field displays the computer's IP address.

[Traffic light <Status message>]: These traffic light colors and messages can be displayed:

<Green> *Firewall OK*: Firewall and *NetOp Policy Server* support, if applied, are OK.

<Yellow>: *NetOp Policy Server Error*: NetOp Policy Server support is not working correctly.

<Red> *Firewall Error*: The firewall is not working correctly.

Note: *In case of an error, hold the mouse pointer over the field to display a tooltip explaining what the error is about.*

[*This Product is registered to*: <Name>]: This field displays the registered licensee name. If a trial version is installed, *This product is a Demo* will be displayed.

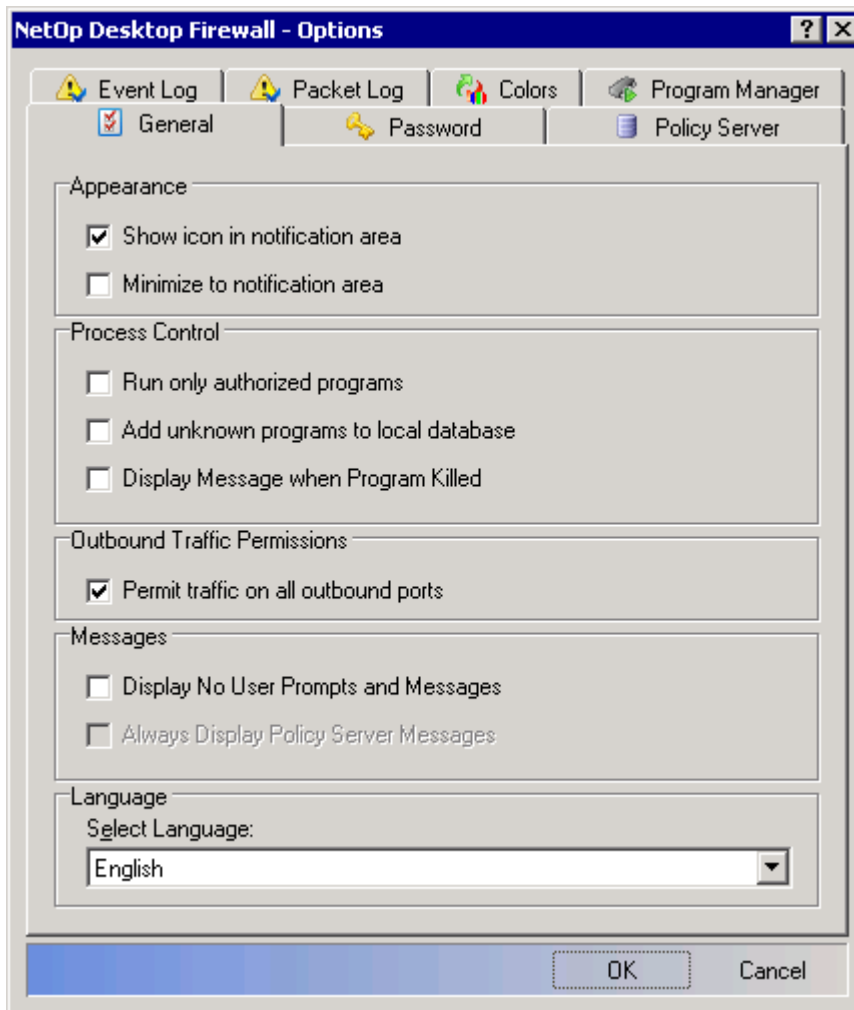
3.4 NetOp Desktop Firewall Tools

This section contains the subsection:

Options, see section 3.4.1, "Options".

3.4.1 Options

Select the *Tools* menu *Options* command to display this window:



This window has these tabs:

General, see section 3.4.1.1, "General Tab".

Password, see section 3.4.1.2, "Password Tab".

Policy Server, see section 3.4.1.3, "Policy Server Tab".

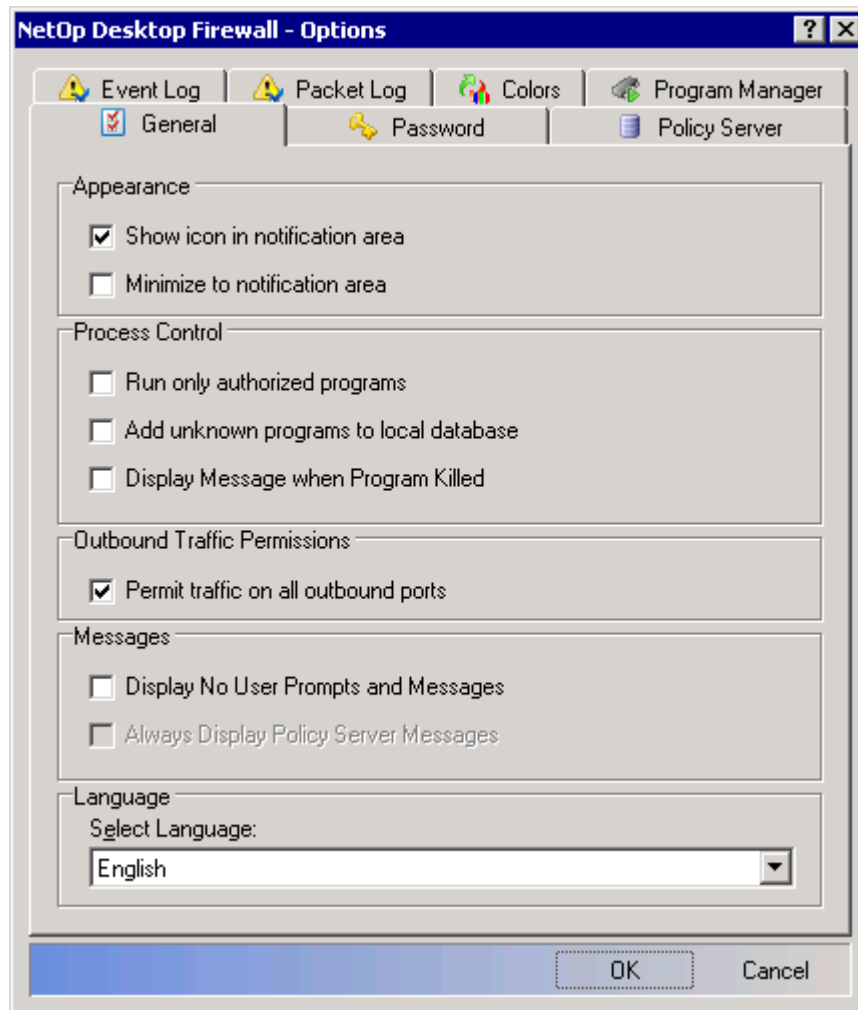
Event Log, see section 3.4.1.4, "Event Log Tab".

Packet Log, see section 3.4.1.5, "Packet Log Tab".

Colors, see section 3.4.1.6, "Colors Tab".

Program Manager, see section 3.4.1.7, "Program Manager Tab".

3.4.1.1 General Tab



This tab specifies general options.

Note: *Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".*

Appearance

[] *Show icon in notification area:* Leave this box checked (default: checked) to display the *NetOp Desktop Firewall* button in the notification area in the lower right corner of the screen. Uncheck this box to hide this button. If you want the button to be visible, open the *NetOp Desktop Firewall* window from the *Start* menu or run the *ndfconf.exe* file, see section 3.3, "NetOp Desktop Firewall Window".

[] *Minimize to notification area:* This option is available if the *Show icon in notification area* box above is checked.

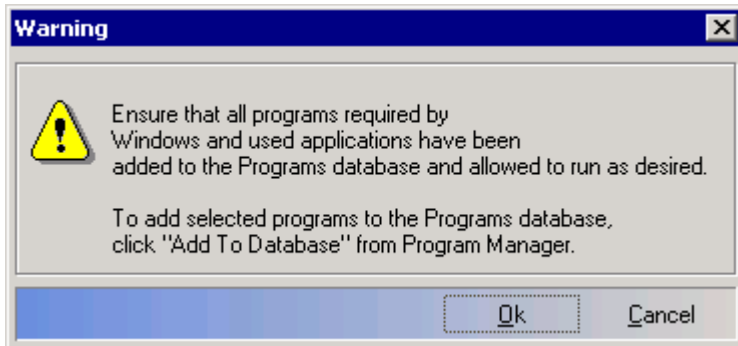
If this box is unchecked (default: unchecked), there will be a *NetOp Desktop Firewall* button in the taskbar at the bottom of the screen when the *NetOp Desktop Firewall* window is open. Click this button to display the window if covered by another window or to restore it if minimized.

If this box is checked, there will be no *NetOp Desktop Firewall* button in the taskbar if the window is minimized. Double-click the notification area *NetOp Desktop Firewall* button or select the notification area button menu *Open Firewall Configuration* command to restore the minimized window.

Process Control

[] *Run only authorized programs:* Check this box (default: unchecked) to allow only program files that have been assigned a firewall rule other than *Kill Program* in the *Programs* display pane to run, see section 3.3.5.1.1, "Programs".

Note: Checking this box provides tight process control. On the one hand, unwanted programs such as computer virus introduced programs will not be allowed to run. On the other hand, wanted programs to which no firewall rule has been assigned will not be allowed to run either. Therefore, this warning will be displayed:



OK: Click this button to acknowledge the warning and leave the checkmark on the *General* Tab.

Cancel: Click this button to acknowledge the warning and remove the checkmark on the *General* Tab.

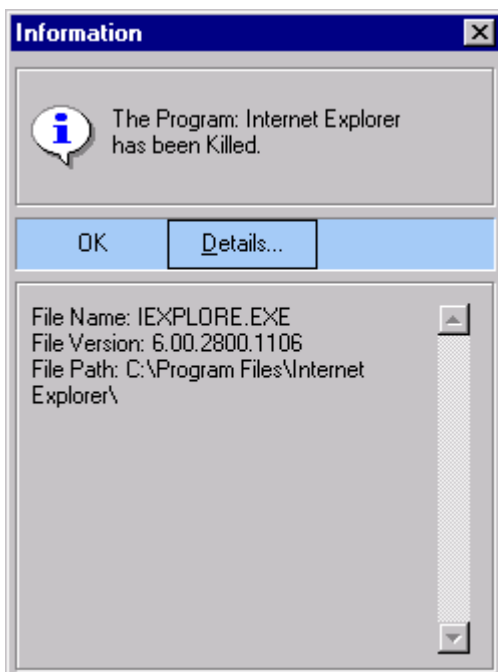
[] Add unknown programs to local database: Check this box (default: checked) to add records of program files not in the *Programs* display pane that attempt to communicate to the pane, see section 3.3.5.1.1, "Programs".

Note: When this box is checked:

If the box Run only authorized programs above is unchecked, program file records will be added with the firewall rule Prompt for Communication.

If the box Run only authorized programs above is checked, program file records will be added with the firewall rule Kill Program.

[] Display Message when Program Killed: Check this box (default: checked) to display this message when a program is killed by the *NetOp Desktop Firewall*:



Initially, only the upper part of the window is displayed. Click the *Details...* button to expand the window to display its lower part.

Outbound Traffic Permissions

Permit traffic on all outbound ports: Check this box to override any firewall rules assigned in the *Ports* display pane to apply the firewall rule *Outbound Traffic* to all ports in the entire port number range 0 - 65535, see section 3.3.5.1.2, "Ports".

Messages

Display No User Prompts and Messages: Check this box (default: unchecked) to display no user prompts and messages.

Always Display Policy Server Messages: Check this box (default: unchecked) to display messages from *NetOp Policy Server* even if the *Display No User Prompts and Messages* box above is checked.

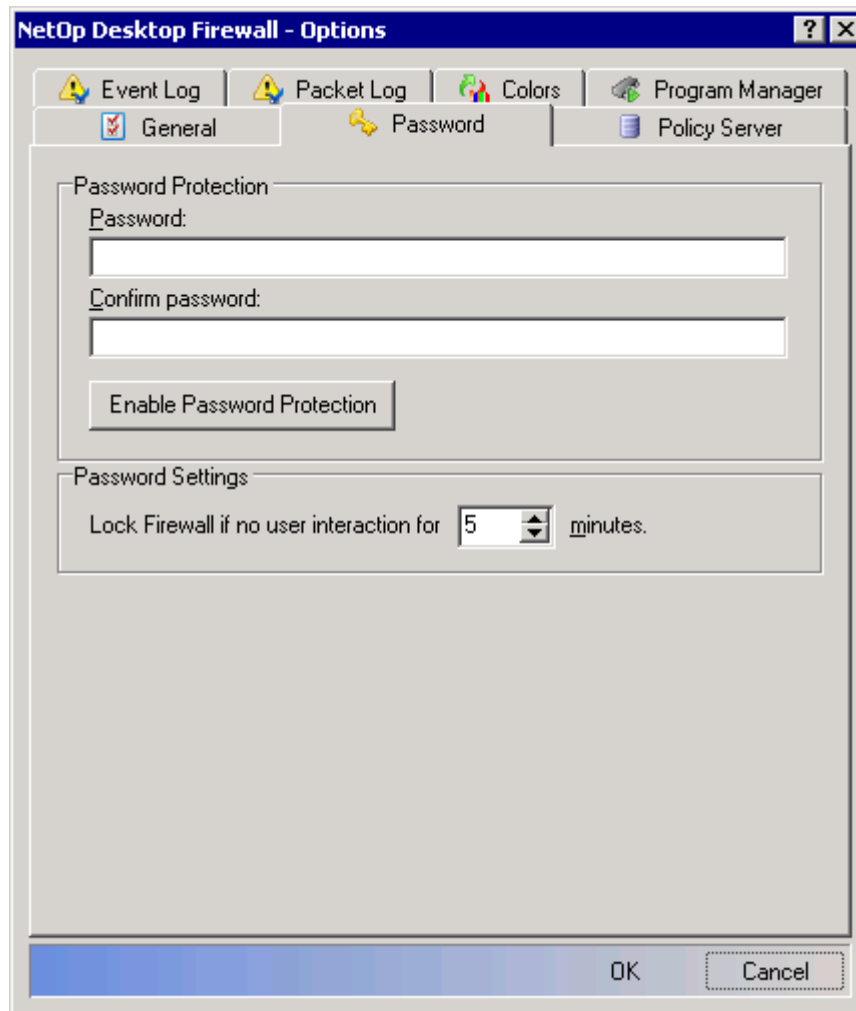
Language

Select Language: : The field of this drop-down box displays the name of the user interface language. The drop-down box list contains names of available user interface languages. Select a language name in the list to display it in the field to apply this user interface language.

Note: *Currently, only English is available.*

Note: *Click OK to apply your selections and close the window.*

3.4.1.2 Password Tab



This tab specifies password protection.

Note: *Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server, see section 3.4.1.3, "Policy Server Tab".*

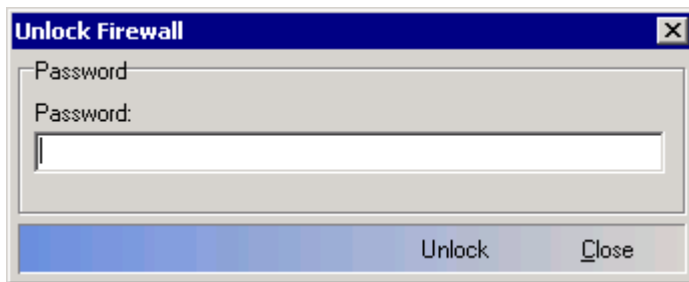
Password Protection

Password: []: Specify the password in this field. Keyboard entries appear as asterisks (*).

Confirm Password: []: Re-specify the password in this field for confirmation.

Enable/Disable Password Protection: After specifying the same password in the *Password* and *Confirm Password* fields, click this button displaying *Enable Password Protection* to enable password protection to make the button display *Disable Password Protection* and disable the fields above. After clicking *OK*, a padlock will be displayed on the notification area button icon indicating that password protection is enabled, see section 3.2, "Startup Guide".

Click this button displaying *Disable Password Protection* to display this window:



Password: []: Specify the password in the field and click *Unlock* or press ENTER to make the button display *Enable Password Protection* and empty and enable the fields above. After clicking *OK* in the window, the padlock on the notification area button icon will be removed indicating that no password protection is applied.

When password protection is applied, the *Unlock Firewall* window will be displayed when attempting to access the *NetOp Desktop Firewall* window and when attempting to change or remove the *NetOp Desktop Firewall* installation.

Warning: If you password protect NetOp Desktop Firewall and forget your password, you cannot open the NetOp Desktop Firewall window and you cannot change or remove your NetOp Desktop Firewall installation.

If the specified password is unavailable, the access to NetOp Desktop Firewall cannot be restored, and NetOp Desktop Firewall cannot be removed by a user.

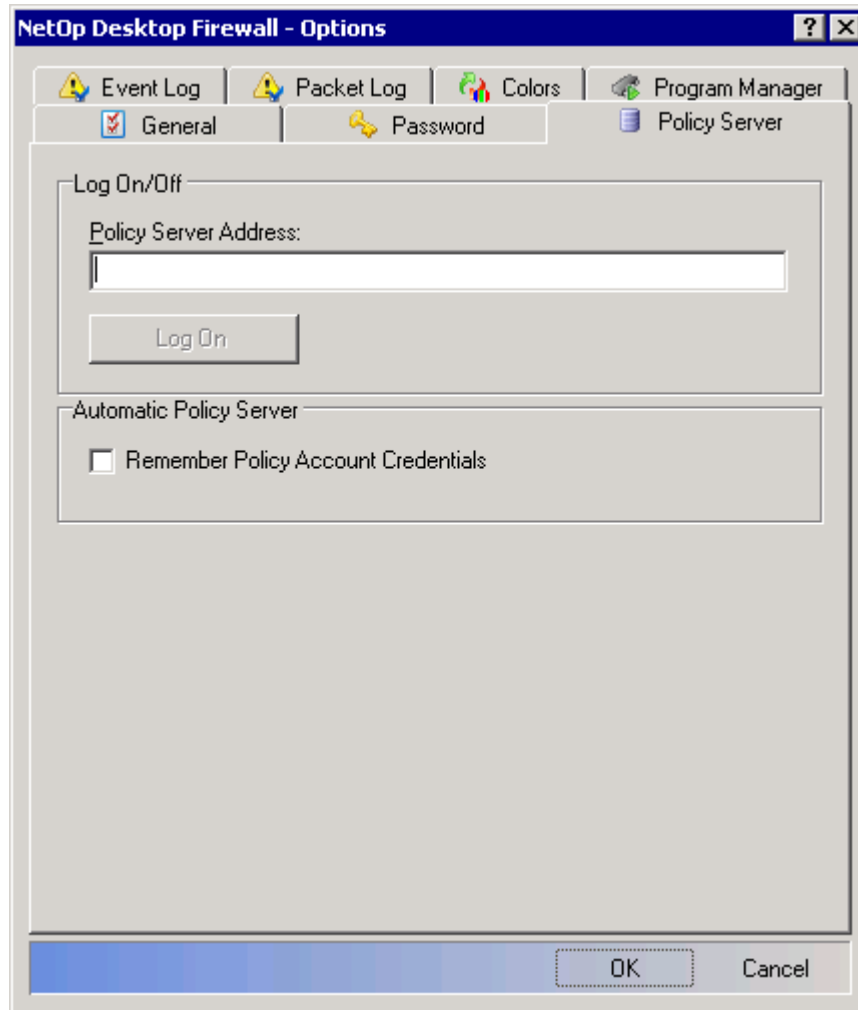
In this case, NetOp Desktop Firewall must be removed by assistance from Danware. We reserve the right to charge a fee for this assistance.

Password Settings

Lock Firewall if no user interaction for [] minutes.: When password protection is applied, an unlocked *NetOp Desktop Firewall* window will lock automatically after the number of minutes specified in the spinbox. Adjust the number in the spinbox (default: 5, range 1-60) or specify a valid number to change it.

Note: Click OK to apply your selections and close the window.

3.4.1.3 Policy Server Tab



This tab specifies *NetOp Policy Server* logon.

Note: *If NetOp Desktop Firewall shall operate without NetOp Policy Server support, leave this tab empty.*

Note: *Commands, buttons and options are enabled if applicable to the current selection unless disabled by the Security Policy assigned by a logged on to NetOp Policy Server. On the interface the icons of Ports, Protocols, Events etc. change when the firewall is controlled by NetOp Policy Server. A padlock is shown on in the icon to visualize the change .*

Log On/Off

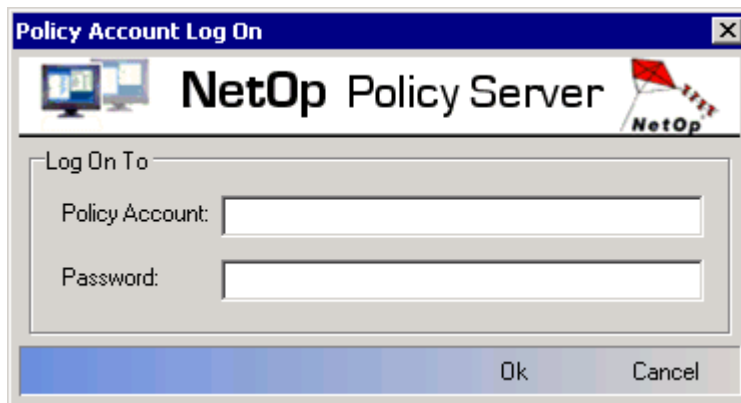
Policy Server Address: []: Specify in this field the *NetOp Policy Server* computer name, IP address or DNS name as prescribed by *NetOp Policy Server* administrators.

Log On/Log Off: To log on to *NetOp Policy Server*, click this button displaying *Log On*. If the logon is successful, the button will display *Log Off*.

Note: *A profile rule may log on automatically, see section 3.3.5.3.1, "Profile Rules".*

NetOp Policy Server will initially attempt to identify the *NetOp Desktop Firewall* computer by its computer name in Windows *Active Directory*. This will succeed if the *NetOp Desktop Firewall* computer is connected to the network of *NetOp Policy Server* and a *Security Policy* is assigned to the *Active Directory Group* to which the *NetOp Desktop Firewall* computer belongs. In this case, *NetOp Desktop Firewall* will be assigned this *Security Policy*.

If Windows *Active Directory* logon fails, *NetOp Policy Server* will attempt to log on the *NetOp Desktop Firewall* computer by a *Policy Account* specified on *NetOp Policy Server*. This window will be displayed:



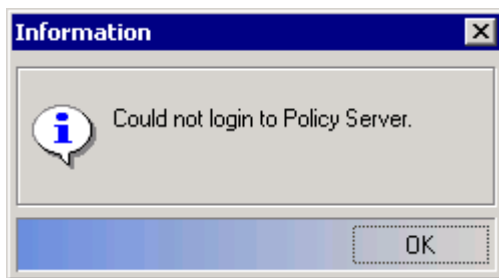
Policy Account: Specify in this field the *Policy Account* name as prescribed by *NetOp Policy Server* administrators.

Password: Specify in this field the *Policy Account* password as prescribed by *NetOp Policy Server* administrators.

If *Policy Account* logon is successful, *NetOp Desktop Firewall* will be assigned the *Security Policy* assigned to the logged on to *Policy Account*.

If *Policy Account* logon fails, *NetOp Policy Server* will log on the *NetOp Desktop Firewall* computer by *Anonymous Account*, if enabled on *NetOp Policy Server*. If enabled, *NetOp Desktop Firewall* will be assigned the *Security Policy* assigned to *Anonymous Account*.

If logon fails, the button will continue to display *Log On* and this window will be displayed:



Note: When logged on to *NetOp Policy Server*, the assigned *Security Policy* determines the autonomy allowed to the *NetOp Desktop Firewall* computer user. To the extent that control is taken over by *NetOp Policy Server*, commands, buttons and options in the user interface will be disabled to the *NetOp Desktop Firewall* computer user.

To log off from *NetOp Policy Server*, click this button displaying *Log Off* to make the button display *Log On*.

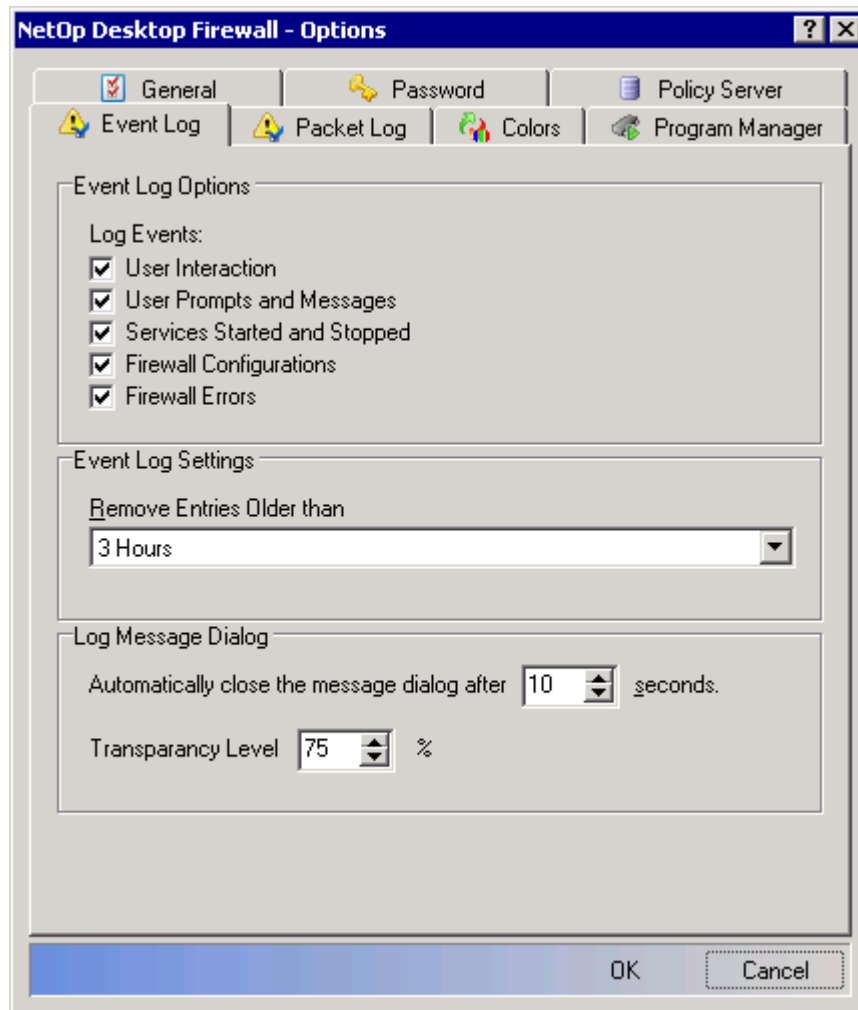
Note: *NetOp Policy Server log-off* may be protected by a *NetOp Policy Server* specified password.

Automatic Policy Server

Remember Policy Account Credentials: Check this box (default: unchecked) to store *Policy Account* logon credentials to automatically specify them when requested next time without displaying the *Policy Account Log On* window explained above.

Note: Click *OK* to apply your selections and close the window.

3.4.1.4 Event Log Tab



This tab specifies which records will be displayed in the *Event Log* display pane table.

Event Log Options

Log Events:

User Interaction: Check this box (default: unchecked) to display records of user interaction events.

User Prompts and Messages: Check this box (default: checked) to display records of user prompt and message events.

Services Started and Stopped: Check this box (default: checked) to display records of started and stopped service events.

Firewall Configurations: Check this box (default: checked) to display records of firewall configuration events.

Firewall Errors: Check this box (default: checked) to display records of firewall error events.

Note: *In addition to the events selected above, records of events of firewall rule records with the attribute Log always will be displayed.*

Event Log Settings

Remove Entries Older than: : The field of this drop-down box displays the current selection (default: *1 Week*). The drop-down box list contains periods from *1 Hour* to *1 Year* and *Indefinitely*. Select a period in the list to display it in the field to automatically remove *Event Log* entries older than the specified period.

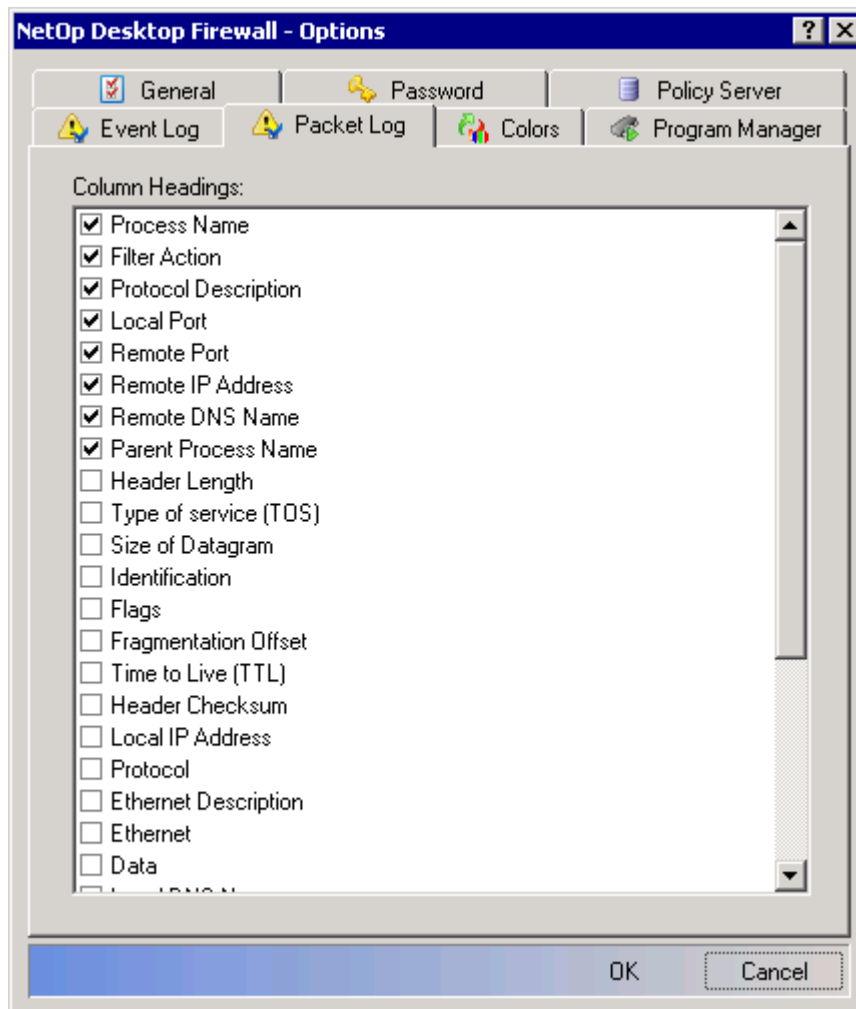
Log Message Dialog

Automatically close the message dialog after [] seconds: An *Event Log* message window will close automatically after the number of seconds specified in the spinbox. Adjust the number in the spinbox (default: 10, range 0-240) or specify a valid number to change it.

Transparency Level: [] %: An *Event Log* message window can be made more or less transparent. Adjust the number in the spinbox (default: 75, range 0 (transparent)-100 (opaque)) or specify a valid number to change it.

Note: Click **OK** to apply your selections and close the window.

3.4.1.5 Packet Log Tab



This tab specifies which columns will be displayed in the *Packet Log* display pane records pane table.

Column Headings: This pane contains the names of all available column headings in a checkboxed list.

Available column headings include:

- Firewall information (*Filter Action* icon and description),
- Process information (*Process Name*, *Process ID*, *Process Path*, *Parent Process Name*, *Parent Process ID* and *Parent Process Path*) and
- Data packet information (*Ethernet* number, *Ethernet Description*, *Timestamp* and IP header details and data, see below).

To display columns with the headings of checked names, check boxes. Click **OK** to move checked names to the top of the list before unchecked names. The *Packet Log* display pane table will display columns from left to right according to the list top to bottom order of checked names.

Drag and drop checked names to achieve the desired table column order.

By default, the *Packet Log* display pane table will contain these columns in this order:

<Action icon> and *Process Name*

Action

Protocol Description

Local Port

Remote Port

Remote DNS

Parent Process Name

Note: The Action icon will always be displayed in the first column. A valid selection must check at least one name. If no name is checked, the default selection will be applied.

Note: To apply your selections, click OK to close the window.

IP Header Details

All data packets sent between different computers include an IP header that serves as an address label including information on the data packet and instructions on how it must be handled. The IP header contains these details:

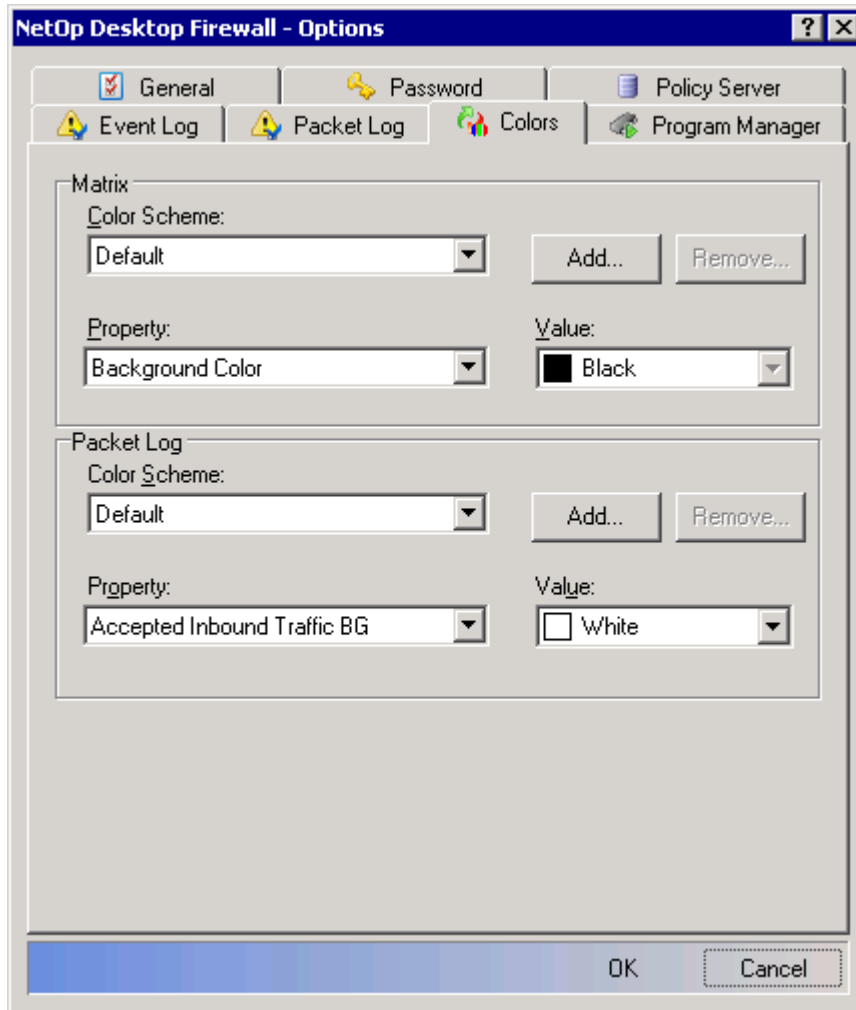
<i>Action</i>	The way <i>NetOp Desktop Firewall</i> acts on a given event.
<i>Data</i>	The binary dump of the packet or process in question.
<i>Ethernet</i>	Indicates the protocol family of the data in this packet.
<i>Ethernet Description</i>	The description of the Ethernet type.
<i>IP Checksum</i>	The IP header checksum. A simple checksum of the bytes in the IP Header.
<i>IP Flags</i>	None, some or all of the following flags may be set in the IP Header: More fragments: Indicates that this packet has been split into multiple packets and that this is not the last packet. Do not fragment: Indicates that this packet is not supposed to be split into multiple packets during transmission.
<i>IP Header Length</i>	The IP header size in bytes.
<i>IP Identification</i>	Distinguishes this packet from other packets sent from the same IP Address. If a packet is split (fragmented) during transmission, all the packets will still have the same IP identification.
<i>IP Offset</i>	If this packet has been split into multiple packets this indicates the number of bytes that were in the previous fragments. This is '0' if the packet has not been split or this is the first fragment of a split packet.
<i>IP Version</i>	This indicates if this packet is in the IP version 4 or IP version 6 format.
<i>Length of datagram</i>	The length of the data following the IP header in bytes.
<i>Local DNS</i>	The DNS name corresponding to the IP Address of this computer as it appears in this packet.
<i>Local IP Address</i>	The IP Address of this computer as it appears in this packet.
<i>Local MAC</i>	The MAC Address of this computer as it appears to this packet.
<i>Local Port</i>	The port number on this computer as it appears to this packet, see section 3.3.5.1.2, "Ports".
<i>Parent Process ID</i>	Distinguishes this running program (process) from all other programs running on this computer at the same time, including other programs with the same name.
<i>Parent Process Name</i>	The name of the file containing the program that started this program.
<i>Parent Process Path</i>	The directory containing the file containing the program that started this program.
<i>Process ID</i>	Distinguishes this running program (process) from all other programs running on this computer at the same time, including other programs with the same name.
<i>Process Name</i>	The name of the file this program was started from.
<i>Process Path</i>	The process runs from this location on the computer.

<i>Protocol</i>	Identifies how the remainder of the packet is formatted. IANA (www.iana.com) assigns this number that ranges from 0 to 255.
<i>Protocol description</i>	The name of the protocol that defines the rest of the packet
<i>Remote DNS</i>	This DNS name corresponding to the IP Address of the other computer as it appears in this packet.
<i>Remote IP Address</i>	The IP Address of the other computer as it appears in this packet.
<i>Remote MAC</i>	The MAC Address of the other computer as it appears in this packet.
<i>Remote Port</i>	The port number on the other computer as it appears in this packet.
<i>TCP Acknowledgement</i>	Confirms that the TCP packet with the value as TCP sequence plus data length has been received in the opposite direction.
<i>TCP Checksum</i>	A simple checksum of all the bytes after the TCP Header.
<i>TCP Flags</i>	None, some or all of the following flags may be set in the TCP Header: FIN: Indicates that this is the end of the transmission. SYN: Indicates that this is the beginning of the transmission. RST: Indicates that the other end does not know of this transmission or is actively refusing it. PSH: Indicates that the data in this packet and all previous packets should be processed now and not queued. ACK: Indicates that the TCP acknowledgement-field in this packet should not be ignored. URP: Indicates that this packet or a later packet contains urgent data. ECE: Indicates that the Internet is clogged in the opposite direction and requests that data is sent at a lower transmission rate. If both ECE and SYN are sent this just indicates that the sender is able to use the ECE and CWR flags. CWR: Indicates that this packet with ECE set has been received and that the transmission rate has been lowered. If all of ECE, SYN and CWR are set in the first packet of a transmission it indicates that the sender is able to use ECE and CWR flags.
<i>TCP Offset</i>	Offset from start of TCP header to data (size of TCP Header).
<i>TCP Sequence</i>	Number of bytes since the first packet of the connection in question plus a random start number generated when the connection was started.
<i>TCP Urgent</i>	This many bytes from the start of the data in this packet is urgent.
<i>TCP Windows</i>	How many bytes may be sent in the opposite direction without waiting for an acknowledgement from the sender.
<i>Timestamp</i>	The date and time of an event.
<i>TOS (Type of service)</i>	Contains various flags indicating the priority of this packet and how routers should handle various transmission problems. The exact format of this field is different depending on which version of the IP Standard was used as the operating system was created.
<i>TTL (Time to Live)</i>	The time to live number that specifies the maximum number of network connection elements (routers, etc.) the data packet can pass. When the data packet passes a network connection element, the <i>TTL</i> number is decreased by 1. When the count reaches 0, the data packet is discarded.
<i>UDP Checksum</i>	A simple checksum of all the bytes after the IP Header (UDP Header + data).
<i>UDP Length</i>	The UDP Header size in bytes.

Note: Some protocols (such as HOPOPT and ICMP) do not use any port. They are assigned a port named NULL with number 0 (zero). This port can be configured to allow or disallow traffic that is not using any port.

With certain Internet communication, NetOp Desktop Firewall can assign a dynamic (different for each occasion) Local Port number to allow for return communication.

3.4.1.6 Colors Tab

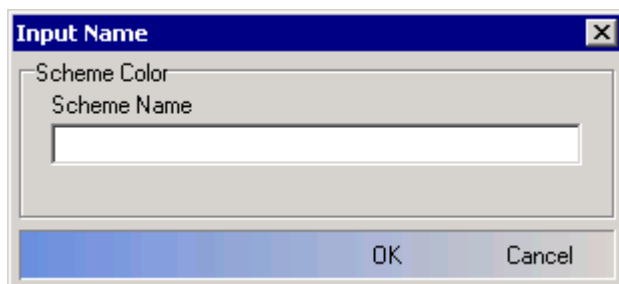


This tab specifies *Color Schemes* for *Traffic Matrix* and *Packet Log*.

The sections *Matrix* and *Packet Log* have similar contents as explained below.

Color Scheme: []: The field of this drop-down box displays the name of the selected color scheme (initially *Default*). The drop-down box list contains the names of available color schemes, initially *Default* and *Grayscale* for *Matrix* and *Default*, *High Contrast White* and *High Contrast Black* for *Packet Log*. Select a color scheme name in the list to display it in the field.

Add...: Click this button to display this window:



Color Scheme Name: []: Specify in the field a name for the added *Color Scheme*.

Click *OK* to add the color scheme name in the *Color Scheme* drop-down box list and display it in the field.

Note: An added color scheme initially has the property values of the color scheme named Default. Property values can be edited from the Property and Value drop-down boxes.

Remove...: Click this button to display a confirmation window to confirm removing the color scheme whose name is displayed in the *Color Scheme* drop-down box field.

Note: Initial color schemes cannot be removed.

Property: []: The field of this drop-down box displays a property of the color scheme selected in the *Color Scheme* drop-down box. The drop-down box list contains the names of available properties, see below. Select a property name in the list to display it in the field.

Value: []: The field of this drop-down box displays the value of the property selected in the *Property* drop-down box. The drop-down box list contains available values, see below. Select a value in the list to display it in the field.

Note: Initial color schemes cannot be edited.

Matrix Properties

<i>Background Color</i>	Display background color.
<i>Circle Color</i>	Circle color.
<i>Start Color</i>	Connection line initial color.
<i>End Color</i>	Connection line final color.
<i>Selected Color</i>	Selected connection line color.
<i>Text Color</i>	Computer address color.
<i>Selected Text Color</i>	Selected computer address color.
<i>Dispersion</i>	Number of connection line color shades between Start Color and End Color
<i>Rate</i>	Milliseconds displaying each connection line color shade between Start Color and End Color

Matrix Values

<i>Colors</i>	64 named colors.
<i>Dispersion</i>	2-255.
<i>Rate</i>	30-1000.

Packet Log Properties

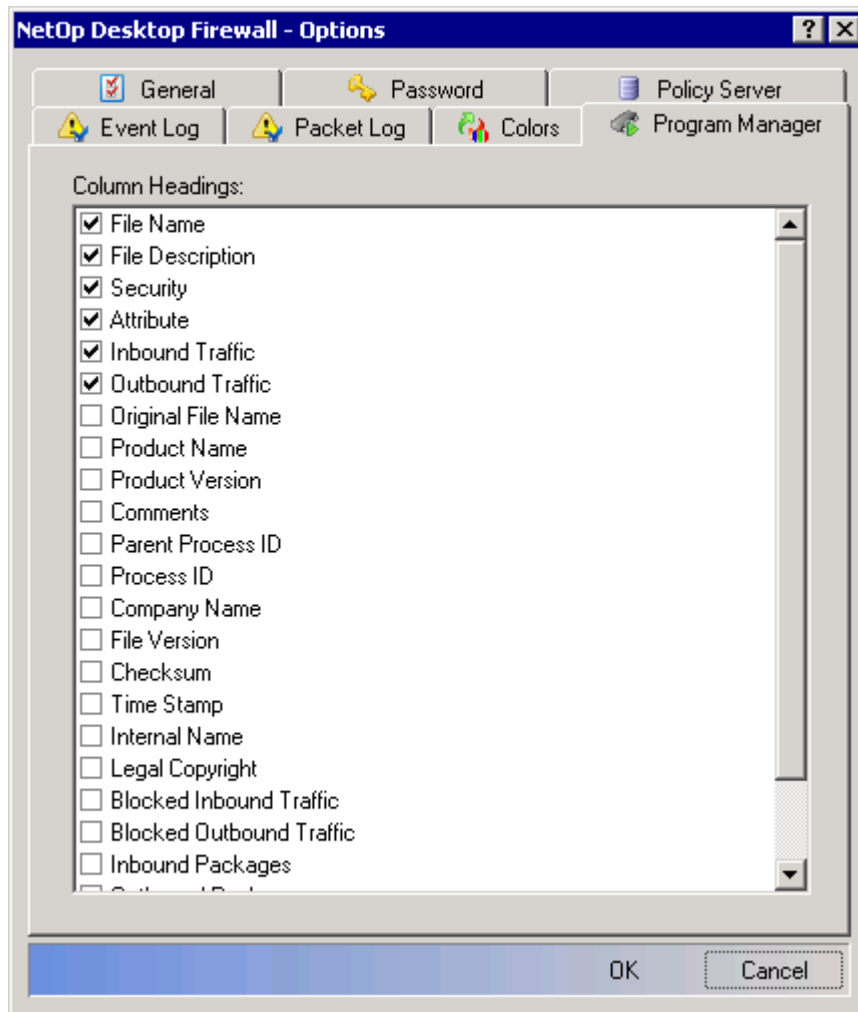
<i>Accepted Inbound Traffic BG</i>	Inbound packet records background color.
<i>Accepted Inbound Traffic FG</i>	Inbound packet records character color.
<i>Accepted Outbound Traffic BG</i>	Outbound packet records background color.
<i>Accepted Outbound Traffic FG</i>	Outbound packet records character color.
<i>Background BG</i>	Unfilled area background color.
<i>Background FG</i>	Unfilled area foreground color.
<i>Blocked Inbound Traffic BG</i>	Blocked Inbound packet records background color.
<i>Blocked Inbound Traffic FG</i>	Blocked Inbound packet records character color.
<i>Blocked Outbound Traffic BG</i>	Blocked Outbound packet records background color.
<i>Blocked Outbound Traffic FG</i>	Blocked Outbound packet records character color.
<i>Broadcast BG</i>	Broadcast packet records background color.
<i>Broadcast FG</i>	Broadcast packet records character color.
<i>Pass By BG</i>	Pass By packet records background color.
<i>Pass By FG</i>	Pass By packet records character color.
<i>Program closing down BG</i>	Program closed records background color.
<i>Program closing down FG</i>	Program closed records character color.
<i>Program killed BG</i>	Program killed records background color.
<i>Program killed FG</i>	Program killed records character color.
<i>Program starting up BG</i>	Program opened records background color.
<i>Program starting up FG</i>	Program opened records character color.
<i>Selected BG</i>	Selected records background color.
<i>Selected FG</i>	Selected records character color.

Packet Log Values

<i>Colors</i>	64 named colors.
---------------	------------------

Note: To apply your selections, click **OK** to close the window.

3.4.1.7 Program Manager Tab



This tab specifies which columns will be displayed in the *Program Manager* display pane table.

Column Headings: This pane contains the names of all available column headings in a checkboxed list, see below.

Check/uncheck boxes to display columns with the headings of checked names. Click *OK* to move checked names to the top of the list before unchecked names. The *Program Manager* display pane table will display columns from left to right according to the list top to bottom order of checked names.

Drag and drop checked names to achieve the desired table column order..

By default, the *Program Manager* display pane table will contain these columns in this order:

<File icon> and *File Name*

File Description

Inbound Traffic

Outbound Traffic

Security

Note: *The file icon will always be displayed in the first column. A valid selection must check at least one name. If no name is checked, the default selection will be applied.*

Column Headings: Cell Content

<i>File Name</i>	Name of the record file.
<i>Original File Name</i>	Name of the record file when originally created.
<i>Internal Name</i>	Internal name of the record file, if any.
<i>File Description</i>	Description of the record file, if any.
<i>File Version</i>	Version of the record file.
<i>Process Path</i>	The process runs from this location on the computer.
<i>Comments</i>	Comments from the program.
<i>Checksum</i>	Checksum of the record file identifying it.
<i>Company Name</i>	Name of the company that supplied the record file.
<i>Legal Copyright</i>	Legal copyright information for the record file.
<i>Product Name</i>	Name of the product that the record file belongs to.
<i>Product Version</i>	Version of the product that the record file belongs to.
<i>Process ID</i>	Process identification (PID) of the record file, if unidentified 0 (zero).
<i>Parent Process ID</i>	Process identification (PID) of the file that can open the record file, if any.
<i>Time Stamp</i>	Time when the record file was opened.
<i>Rule</i>	Firewall rule assigned by NetOp Desktop Firewall to the record file.
<i>Attribute</i>	Attributes assigned by NetOp Desktop Firewall to the record file.
<i>Inbound Traffic</i>	Number of bytes in inbound packets of the record file.
<i>Outbound Traffic</i>	Number of bytes in outbound packets of the record file.
<i>Blocked Inbound Traffic</i>	Number of bytes in blocked inbound packets of the record file.
<i>Blocked Outbound Traffic</i>	Number of bytes in blocked outbound packets of the record file.
<i>Inbound Packages</i>	Number of inbound packets of the record file.
<i>Outbound Packages</i>	Number of outbound packets of the record file.
<i>Blocked Inbound Packages</i>	Number of blocked inbound packets of the record file.
<i>Blocked Outbound Packages</i>	Number of blocked outbound packets of the record file.

Note: Any .exe, .dll or executable binary file (except 16 bit files) contains a field named VS_VERSIONINFO that has these fields: File Description, Company Name, File Version, Internal Name, Original Name, Product Name, Product Version and Comment. It is optional whether the field are filled.

4 How NetOp Desktop Firewall Works

4.1 Summary

This chapter explains how *NetOp Desktop Firewall* works.

It contains the main sections:

- How a Firewall Works on page 120
- How NetOp Desktop Firewall Works, on page 120

4.2 How a Firewall Works

A firewall is typically a program that analyzes data packets attempting to pass a computer communication interface and based on this analysis allows or denies data packet passage.

Typically, firewalls protect networks against undesired Internet communication. Internet communication uses the protocols of the TCP/IP protocol suite. TCP/IP data packets contain in their IP header information on the data packet type, size, handling requirements, protocol, sender port and address and receiver port and address, see section 3.4.1.5, "Packet Log Tab".

Firewall administrators specify IP header element firewall rules to make the firewall allow or deny passage to data packets according to these rules. These rules typically apply to program, port, protocol and address properties.

4.3 How NetOp Desktop Firewall Works

NetOp Desktop Firewall not only controls communication across the computer communication interface but monitors and controls processes running on the computer. It has many additional benefits.

4.3.1 Process Control

Concurrently with installing *NetOp Desktop Firewall* a *Danware Security* filter driver is being installed with the file name *DWSNdis.sys*. It is a miniport type of device driver.

Miniport device drivers were introduced with version 5.0 of the Windows Network Driver Interface Specification (NDIS) that is available only with Windows 98, 2000 and later Windows versions. Miniport device drivers typically facilitate the plug-and-play features of installed hardware.

The *Danware Security* filter driver that runs in the core of the Windows operating system enables control of processes running on the computer. It is controlled from and reports events to the *NetOp Desktop Firewall* application that runs on top of the Windows operating system.

NetOp Desktop Firewall can assign one of these firewall rules to program files running processes on the computer, see section 3.3.5.1.1, "Programs":

Allow Communication

Prompt for Communication

Deny Communication

Kill Program

Unrestricted Communication

Trusted Net Only

If *Kill Program* is assigned to a program, the *Danware Security* filter driver will not allow the program to run on the computer.

If one of the other program firewall rules is assigned to a program, the *Danware Security* filter driver will apply it if the program attempts communication across the computer communication interface.

If no firewall rule is assigned to a program, by default the *Danware Security* filter driver will allow it to run inside the computer, but if it attempts communication, the computer user will be prompted to decide if it can communicate or not.

For maximum protection, *NetOp Desktop Firewall* can be configured to *Run only authorized programs*, see section 3.4.1.1, "General Tab". In this case, the *Danware Security* filter driver will allow a program to run only if a firewall rule other than *Kill Program* is assigned to it.

Note: *If applying Run only authorized programs, a firewall rule other than Kill Program must be assigned to all programs that are necessary for the computer to run. Otherwise, computer or application malfunction will occur.*

4.3.2 Hacker Resistance

NetOp Desktop Firewall has strong hacker resistance.

Typically, in a hacker attack from outside a firewall, the first thing the hacker will attempt to do is to disable firewall protection. This is virtually impossible with *NetOp Desktop Firewall*.

NetOp Desktop Firewall can be disabled only by removal of its installation followed by a complete restart (reboot) of the computer. Only then the *Danware Security* filter driver is unloaded. Removal as well as access to the *NetOp Desktop Firewall* window can be password protected, section 3.4.1.2, "Password Tab".

Knowing how *NetOp Desktop Firewall* works, a hacker might attempt to modify the instructions given by *NetOp Desktop Firewall* to the *Danware Security* filter driver. This will not be successful either.

The communication between *NetOp Desktop Firewall* and the *Danware Security* filter driver as well as the tables specifying firewall rules are encrypted by acknowledged hacker-proof algorithms. Encryption ensures confidentiality, authentication and integrity.

If the encryption detects any abnormality, as would happen in case of a hacker attack on communication or firewall rule tables, the *Danware Security* filter driver assigns the firewall rule *Prompt on Communication* to all programs running on the computer. This disables communication across the computer communication interface preventing the outside hacker from communicating with the computer. Communication can be restored only by a user from the physical computer interface (keyboard and mouse).

4.3.3 Operational Benefits

NetOp Desktop Firewall complies with all Windows standards assuring no conflict with the computer operating system.

NetOp Desktop Firewall takes up considerably less disk space than other firewalls with a comparable functionality.

Communication slowdown is often a problem with a firewall analyzing every data packet at the computer communication interface to determine whether it can be allowed passage or not. The unique construction of *NetOp Desktop Firewall* keeps communication slowdown at a minimum, typically low single-digit percentages compared to the usual double-digit percentages experienced with most other firewalls.

Note: *NetOp Desktop Firewall does not replace an anti-virus system but greatly enhances the power to fight virus attacks on a computer.*

4.3.4 Plug-and-Play with Highly Specific and Transparent Firewall Rules

While *NetOp Desktop Firewall* immediately after installation is fully operational with a high level of protection to the typical computer user, it also provides very specific firewall rules that are fully transparent to the user.

NetOp Desktop Firewall enables specifying a wide selection of *Program* firewall rules including *Kill Program* and bidirectional *Port*, *Protocol*, *Trusted Net* and *Banned Net* firewall rules. Although most users do not need this high specificity, it provides the opportunity to tailor firewall rules exactly to the actual requirements.

Firewall rules are displayed schematically in the *NetOp Desktop Firewall* window to enable the user to identify transparently which firewall rules apply.

4.3.5 NetOp Policy Server Support

NetOp Desktop Firewall is designed to run as a stand-alone computer firewall, but it is also designed to be logged on to a *NetOp Policy Server* to operate as an element in an organizational distributed firewall system, see section 3.4.1.3, "Policy Server Tab".

The responsibility for specifying firewall rules in a stand-alone *NetOp Desktop Firewall* computer, disallowing unknown programs attempting to run, lies solely with the computer user.

How NetOp Desktop Firewall Works

In a distributed firewall system, this responsibility can be partly or fully left to the administrators of an organizational *NetOp Policy Server* to relieve individual computer users from this task and apply organization-wide firewall Policies.

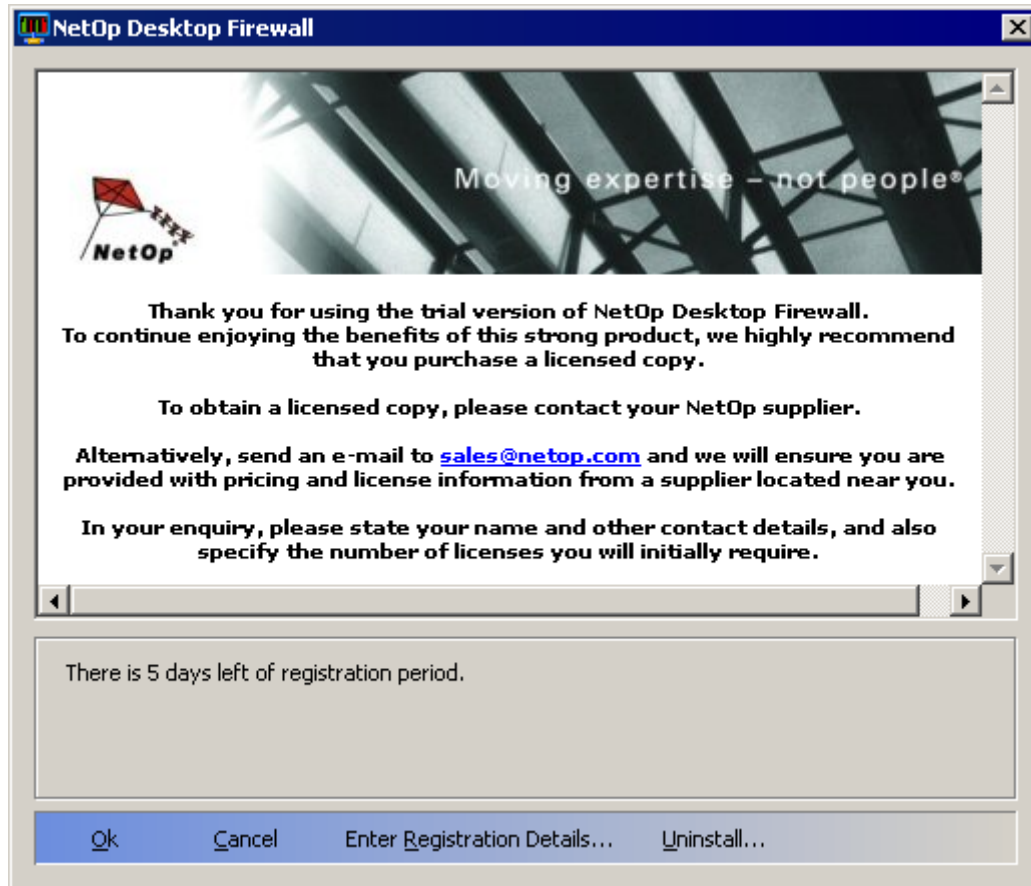
A *NetOp Policy Server* distributed firewall system is fully and continuously scalable from one stand-alone *NetOp Desktop Firewall* to a multi-site distributed firewall system with several *NetOp Policy Servers* and several thousands *NetOp Desktop Firewalls*.

5 Appendix

5.1 Trial Version

The free trial version of *NetOp Desktop Firewall* comes as fully operationable product with a limited duration.

If the trial period of an installed trial version of *NetOp Desktop Firewall* is about to expire, this window will be displayed when opening the *NetOp Desktop Firewall* window:



This window displays the number of days left of the trial period.

OK: Click this button to continue.

Cancel: Click this button or the *Close* button to abort.

Enter Registration Details...: Click this button to go to the *Installation*, see section 2.4, "Install".

Uninstall...: Click this button to display the window for changing or uninstalling an installation, see section 2.1.1, "Change".

A
Appearance 103
Automatic Policy Server 108
B
Banned Nets 78
Before Install 18
C
Change 37
Change > Remove 38
Change > Repair 40
Change or Remove 36
Colors Tab 113
Command Line Installation 31
Configuration Guide 49
Create a License Registration File 31
E
Edit Menu 54
Event Log 82
Event Log Options 109
Event Log Settings 109
Event Log Tab 109
export data 54
F
File Menu 54
Firewall Rules (Overview) 50
Firewall Rules (Selection Pane Section) 61
Firewall Rules Toolbar 58
G
General Tab 103
H
Hacker Resistance 121
Help Menu 56
How a Firewall Works 120
How NetOp Desktop Firewall Works 120
I
Information (Overview) 51
Information (Selection Pane Section) 81
Information Toolbar 58
Install 19
Install NetOp Desktop Firewall in a Configured State 31
Installation 17
IP Header Details 111
L
Language 105
Legend and Record Colors Pane 86
Log Message Dialog 110
Logging 33

M
Matrix Properties 114
Matrix Values 114
Menu Bar 54
Messages 105
N
NetOp Desktop Firewall 43
NetOp Desktop Firewall Tools 102
NetOp Desktop Firewall Window 49
NetOp Policy Server Support 121
Normal installation 31
Notification Area Button Menu 45
O
Operational Benefits 121
Options 53, 102
Options Toolbar 58
Outbound Traffic Permissions 105
P
Packet Log 84
Packet Log Properties 115
Packet Log Tab 110
Packet Log Values 115
Password Protection 106
Password Settings 106
Password Tab 105
Play Controls 87
Play Toolbar 59
Plug-and-Play with Highly Specific and Transparent Firewall Rules 121
Port Notes 70
Ports 67
Process Control 103, 120
Profile Records 95
Profile Rules 96
Profiles 52, 94
Program Manager 92
Program Manager Tab 116
Programs 62
Protocol Notes 73
Protocols 71
Q
Quiet Installation 31
R
Records, Hexadecimal and ASCII Panes 85
S
Setup Wizard 27
Startup Guide 44
Statistics 91
Status Bar 101

Summary 18
Summary (how NetOp Desktop Firewall Works) 120
System Requirements 18
T
Title Bar 54
Toolbars 57
Tools Menu 56
Traffic Graph 91
Traffic Matrix 88
Traffic Statistics 92
Trusted Net Notes 77
Trusted Nets 74
U
Use and Configuration 44
V
View Menu 55
W
Work Pane 60