Norman Personal Firewall

Version 1.42

User’s Guide
Limited warranty

Norman guarantees that the enclosed diskette/CD-ROM and documentation do not have production flaws. If you report a flaw within 30 days of purchase, Norman will replace the defective diskette/CD-ROM and/or documentation at no charge. Proof of purchase must be enclosed with any claim.

This warranty is limited to replacement of the product. Norman is not liable for any other form of loss or damage arising from use of the software or documentation or from errors or deficiencies therein, including but not limited to loss of earnings.

With regard to defects or flaws in the diskette/CD-ROM or documentation, or this licensing agreement, this warranty supersedes any other warranties, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

In particular, and without the limitations imposed by the licensing agreement with regard to any special use or purpose, Norman will in no event be liable for loss of profits or other commercial damage including but not limited to incidental or consequential damages.

This warranty expires 30 days after purchase.

The information in this document as well as the functionality of the software is subject to change without notice. The software may be used in accordance with the terms of the license agreement. The purchaser may make one copy of the software for backup purposes. No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the explicit written permission of Norman.

The Norman logo is a registered trademark of Norman ASA.

Names of products mentioned in this documentation are either trademarks or registered trademarks of their respective owners. They are mentioned for identification purposes only.

NVC documentation and software are

Copyright © 1990-2004 Norman ASA.

All rights reserved.

Last revised on 22 September 2004.
Norman Offices
Norman Data Defense Systems AS
Blangstedgårdsvej 1, DK-Odense SØ, Denmark
Tel. +45 6311 0508 Fax: +45 6313 3901
E-mail: normandk@normandk.com Web: http://www.norman.no/dk

Norman Ibas OY
Läkkisepäntie 11, 00620 Helsinki, Finland.
Tel: +358 9 2727 210 Fax: +358 92727 2121
E-mail: norman@norman-ibas.fi Web: http://www.norman-ibas.fi

Norman Data Defense Systems GmbH
Kieler Str. 15, D-42697 Solingen, Germany.
Tel: +49 212 267 180 Fax: +49 212 267 1815
E-mail: norman@norman.de Web: http://www.norman.de

Norman/SHARK BV
Postbus 159, 2130 AD, Hoofddorp, The Netherlands.
Tel: +31 23 789 02 22 Fax: +31 23 561 3165
E-mail: support@norman.nl Web: http://www.norman.nl

Norman ASA
Mailing address: P.O. Box 43, N-1324, Lysaker, Norway.
Physical address: Strandveien 37, Lysaker, N-1324 Norway.
Tel: +47 67 10 97 00 Fax: +47 67 58 99 40
E-mail: norman@norman.no Web: http://www.norman.no/no

Norman Data Defense Systems AB
P.O. Box 5044, SE-194 05 Upplands Väsby, Sweden
Tel. +46 11 230 330 Fax: +46 8 87 52 52
E-mail: support.se@norman.no Web: http://www.norman.com/se

Norman Data Defense Systems AG
Postfach CH-4015, Basel, Switzerland.
Tel: +41 61 487 2500 Fax: +41 8 87 52 52
E-mail: norman@norman.ch Web: http://www.norman.ch

Norman Data Defense Systems (UK) Ltd
PO Box 5517, Milton Keynes MK5 6XJ, United Kingdom.
Tel: +44 08707 448044 Fax: +44 08717 176999
E-mail: norman@normanuk.com Web: http://www.normanuk.com

Norman Data Defense Systems Inc.
9302 Lee Highway, Suite 950A, Fairfax, VA 22031, USA
Tel: +1 703 267 6109, Fax: +1 703 934 6367
E-mail: norman@norman.com Web: http://www.norman.com

Training and Technical Support
For training or technical support, please contact your local dealer or Norman ASA.
Conventions

We use the following conventions throughout this manual:

When we give examples of what you should type in order to use a particular program, the examples look like this:

format a: /s /u [Enter]

We designate certain keys by surrounding the key name with “[“ and ”]”, as in:

[Ctrl]

When we describe a series of menu choices for you to choose, we will use the following:

Start|Run

This means that you should click on “Start” and from there click on the “Run” menu item.

Important notes appear in boxes like the one below:

**Note:** Right-click to start on-demand scanning.

We use bold face type to identify anything that you can click or select, for example, button names and dialog box names.

Click **OK** to view the **Scheduled task** dialog.

Individual words or phrases that we intend to stress are in *italic*:

This rule applies to *outgoing cookies* only...
System requirements

Norman Personal Firewall (NPF) can run on any machine that runs any national language version of Windows 95/98/Me and Windows NT/2000/XP installed.

For Windows 95, Internet Explorer 4.0 or higher is required.
For Windows NT, version 4 with SP4 or higher is required.
Windows NT/2000: You need administrator privileges to start/stop NPF.

Prerequisites

To take full advantage of all the functions in NPF, you should have some experience with your web browser, operating system, and applications that run on this platform.

Technical support

Norman provides technical support and consultancy services for Norman products and security issues in general. Technical support also comprises quality assurance of your anti-virus installation, including assistance in tailoring Norman’s software to match your exact needs.

Note that the number of services available will vary between the different countries.
Contents

Conventions ........................................................................................................ iv
System requirements ............................................................................................ v
Technical support ................................................................................................ v

Introduction .............................................................................................................8

   IP addresses and DNS ....................................................................................9
   Services ..........................................................................................................9
   Cookies .........................................................................................................10
   Active content ...............................................................................................10
      Scripts ......................................................................................................11
      Applets ....................................................................................................11
      ActiveX ...................................................................................................11
   The bottom line .............................................................................................11

Installation .............................................................................................................12

   Uninstall .......................................................................................................13
   Uninstall with NIC .......................................................................................13

Getting familiar with NPF ...................................................................................14

   NPF Assistant ...............................................................................................15
   Connection alert ............................................................................................16
   Script alert ....................................................................................................16
   Aspects to consider when interacting with the pop-up dialogs ....................16
      NPF Assistant pop-up dialog example ....................................................18

NPF console ...........................................................................................................22

   Using NPF console .......................................................................................22
   Settings .........................................................................................................22
   Block referer .................................................................................................23
   Script, ActiveX, and Applet ..........................................................................23
Contents

Pop-up windows ................................................................. 23
Outgoing cookie .............................................................. 24
Clear session rules .......................................................... 24

NPF settings ........................................................................... 25
Status .................................................................................. 26
Security ............................................................................... 27
	Understanding how to configure your firewall ...................... 27
	Setting the security level for Active Content ....................... 29
	Customize security level .................................................. 30

How to manage rules .......................................................... 33
	Adding a rule .................................................................... 33
	Modifying a rule ............................................................ 35
Parental control .................................................................... 38
	User Manager ................................................................. 39
Advertisement blocking .................................................... 41
Web site filtering .................................................................. 42
Content filtering ............................................................... 43
Privacy ................................................................................ 44
	Block referrer ............................................................... 44
	Cookies .......................................................................... 44
Active Content ................................................................. 46
Log .................................................................................... 48
WEB .................................................................................... 49

Glossary .............................................................................. 51
	ActiveX control ........................................................... 51
	Applet ............................................................................ 51
	Cookie ........................................................................... 51
	Pop-up windows ......................................................... 51
	DNS/IP ......................................................................... 51
	JavaScript ..................................................................... 52
	Services ....................................................................... 52

Index ............................................................................... 41
Introduction

This document is aimed at inexperienced users, so if you are comfortable with concepts like services, IP addresses, cookies, and active content, you may skip this introduction and proceed to the installation instructions. The rest of you should keep on reading this brief introduction. Don’t worry, it’s not as hard as it seems.

So, what exactly is a firewall? It’s not an anti-virus program, nor does it spell-check your e-mail. Well, the short version is that it is a form of hacker protection. The more elaborate version follows.

Whenever you’re connected to the Internet, reading e-mail, surfing the web, you make connections to other computers all over the world. Normally this is okay. However, this also implies that other computers may connect to yours. And that’s mostly where the trouble starts.

Although advertisements present a rosy picture of the Internet, the truth is far from it. There are people out there who take great pleasure in destroying other people’s experience of the Internet. By hacking your computer, they may access your private documents, use your computer for their own acts of evil, or even render your computer completely useless by deleting important system files. We refer to this group of people as the terrorists of the Internet.

You’re not doomed yet though, because a hacker must be able to connect to your computer to do any real harm. This is when NPF steps in. Normally, your system does not tell you that a connection has been made to your computer. NPF allows you to monitor which connections are made and whether or not you will allow them. By doing so, you minimize the chance of your computer being exposed to the wrong kind of people.

The following section is a brief introduction to the terminology used when describing a firewall and its actions, and you should familiarize yourself with the basic terms. These terms are listed in the ‘Glossary’ on page 51 as well.
IP addresses and DNS

When you’re connected to a network, for example the Internet, your computer, as any other computer, is assigned a unique identification. This is called an IP address. It consists of 4 groups of numbers, ranging from 0 to 255, separated by a dot.  

Example: 10.0.0.255

Now, numbers are easy to handle for computers, but they are far from being intuitive. And haven’t you always typed addresses with letters, not numbers?

Enter the Domain Name Service, or DNS. This is a service that allows you to type easy-to-remember addresses, like www.norman.com. When you type in this address in your web browser, the information is sent to a DNS server, which has a list of all registered names and their corresponding IP addresses.

The DNS server then replies with the IP address to our web server. Now the computer finally understands where it’s heading, and you enter our web site. In effect, IP addresses and DNS are two sides of the same matter—IP addresses are just more difficult to read.

Services

A computer may offer several services to its users, such as web and e-mail. However, with only one IP address, how does it differentiate between the services it has to offer?

Think of the server as a block of flats. You know the address, but you also need to know which floor you’re going to. This problem is solved by the use of ports. When you instruct your web browser to go to www.norman.com, the browser, in addition to the address of the server, also sends a port number. In this case, the number sent is 80. This number is used to decide which service you are about to use, or metaphorically speaking, to which floor you’re heading.
Some common ports are:

<table>
<thead>
<tr>
<th>Application</th>
<th>Protocol(s)</th>
<th>Port(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browsing</td>
<td>HTTP</td>
<td>80</td>
</tr>
<tr>
<td>Receiving e-mail</td>
<td>POP3 and IMAP</td>
<td>110 and 143</td>
</tr>
<tr>
<td>Sending e-mail</td>
<td>SMTP</td>
<td>25</td>
</tr>
<tr>
<td>File transfer</td>
<td>FTP</td>
<td>20 and 21</td>
</tr>
</tbody>
</table>

The most commonly used ports are also listed with their respective names within NPF. A complete and updated list of port numbers can be found at the Internet Assigned Numbers Authority’s web site: www.iana.org.

### Cookies

Cookies are information capsules, used to identify you—not the computer. When you log on to a web site, using for instance username and password, you receive a cookie that will identify you as an individual user, rather than just the computer. The cookie is stored on your computer for later use.

Later on, when the web site needs to show you customized or personalized information, it retrieves the cookie, ensuring that you are indeed the person for which the information is intended.

Today cookies are used on most popular sites, and some of the information gathered using cookies could be used for marketing purposes. As a rule of thumb, you should only allow cookies from sites which you are familiar with, such as your online bank or search engines.

### Active content

Active content like scripts, applets and ActiveX components differ from the standard web documents in that they are actually small programs. They are intended to enhance your browsing experience. However, these programs may also contain malicious code.
**Scripts**

Scripts are most commonly used to enable dynamic content, for example changing a picture when you point at it, or to add other experiences to a web page with simple animations. They pose a security threat as they can alter system settings and potentially invade your privacy.

**Applets**

Applets are small programs devised to be launched inside a host application. Java is a good example of this kind of active content. Applets have limited access to the operating system, making them more secure than other types of active content. However, examples of these applets using security holes in the host application have been reported.

**ActiveX**

ActiveX is a set of rules for information sharing between applications. These rules are comparable to applets, but ActiveX components pose a potential threat as they have access to the operating system.

**The bottom line**

So now you know why you want a firewall, and you have acquired the basic concepts about networking. So how does this affect you?

The firewall is never more secure than the user. It may help you on the way, but at the end of the day it you who make the decisions. Therefore, you should disallow any connection that you are not comfortable with.
Installation

The following chapter will guide you in installing Norman Personal Firewall (NPF).

1. Insert the CD-ROM into its drive.

   **Note:** If you download the program from the web, double-click the downloaded file and proceed to step 4.

2. Autorun launches the installation program (or click on Start|Run from the menu).

3. In the dialog box, type the path of the SETUP.EXE and click on **OK**.

4. Setup will now prepare the wizard for the installation program.

5. Click on **Next** when the welcome screen appears.

6. Click on **Next** again when you come to the License Agreement page.

7. Type in the drive and directory where you want to install NPF. By default, the path is `C:\Program Files\Norman\NPF`. Click on **Next** when you’re done.

8. If you wish to install NPF into another directory, click on the **Browse** button. A new dialog box will appear and then select the DRIVE followed by the directory. Click on **Next**.

9. Setup will now install the program on your hard disk. When the transfer is complete, the installation program prompts you to restart the computer.

When the machine is restarted, the Freshie’s Assistant is launched to help you set the basic rules for the NPF.

   **Note:** If you are upgrading from a previous version of NPF and want to import the rules, click **Yes**. Then your previous rules are imported and the assistant is skipped altogether. If you answer **No**, proceed with the assistant’s wizard.

Click **Auto Setup** or **Manual Setup** to start the Assistant or **Cancel** to skip the entire process. All the rules set by the
Assistant can later be modified or deleted using the NPF Settings (see page 25). This may come in handy if you later find that you have configured the firewall more strictly than you intended, or if you want to set up or edit rules manually.

If your web browser is Internet Explorer and your e-mail client is Outlook or Outlook Express, you should click Auto Setup. The assistant will then complete the basic firewall configuration automatically. The default password for the firewall administrator will be set to “1234”.

If you run other browsers or e-mail clients, or want to customize the basic firewall rules during installation, you should select Manual Setup.

Uninstall

1. To uninstall NPF, open the Start menu.
2. From the menu, select Settings and Control Panel.
3. Select Add/Remove Program.
4. From this dialog, select Norman Personal Firewall and click on the Add/Remove button.
5. NPF will be removed from your PC.

Uninstall with NIC

If you have Norman Internet Control (NIC) installed, then follow these steps:

1. Open NVC’s Configuration Editor, select Installation settings, then the tabbed dialog Install.
2. Clear the option Personal Firewall from the list by removing the check mark.
3. Click Save.
4. Restart your computer.
Getting familiar with NPF

After the installation, NPF needs to be instructed which applications, services and addresses that should be granted connections to and from the Internet/network. Whenever an application or service on your computer wants to access the Internet/network, the NPF Assistant pops up and ask you for permission. These pop-ups don’t necessarily mean that something is wrong. They are only dialogs with the purpose of guiding you safely through the Internet jungle. It is up to you to provide the information that NPF needs to do its job properly. Once you have approved an application, service, or address, you don’t have to do it again the next time a known feature try to access the Internet, for example. It is therefore normal that the frequency of pop-up dialogs will be higher shortly after installation than after NPF has been actively used for a while. The following sections will give some general recommendations on how to respond to/interact with the NPF Assistant’s pop-up dialogs.

NOTE:

NPF provides two types of assistants, namely:

- the Freshie Assistant, and
- the Norman Personal Firewall Assistant (NPF Assistant)

The Freshie version is—as the name suggests—aimed at inexperienced users and is only invoked during installation and upgrades. The NPF Assistant pops up when for example incoming or outgoing traffic takes place where the PC tries to establish connection that are not defined in rules or are suspicious in other ways. Thus the NPF Assistant can detect traffic generated by trojans, for example.
The two main types of NPF Assistant pop-up dialogs are:

**Connection Alert**

Despite the “Alert” name of the dialogs, it doesn’t necessarily mean that you should deny the connection or script in question.
From the NPF Console, you may also configure NPF to pop up for other scripts and cookies, or configure it to automatically permit/deny all the technologies above. By default NPF will only prompt you for outgoing and incoming connections, as well as active content like ActiveX and Applets.

**Connection alert**

Connection Alert dialogs will always indicate whether a connection is outgoing (to the Internet/network) or incoming (from the Internet/network). All Internet applications on your computer should generally be permitted to connect to the Internet, but very few applications services require that you permit incoming connections.

**Script alert**

Pop-ups concerning scripts, applets and ActiveX indicates that the web site you are visiting contains elements using one of these active content technologies. Normally such elements are used to enhance your browsing experience with moving images, interactive menus etc. and they are not harmful at all. However, they also have wide access to core operating system functions, and should therefore be treated with care if they come from sites or addresses that you are not familiar with.

**Aspects to consider when interacting with the pop-up dialogs**

- Do you know which application that tries to establish the connection? Is it for example a module in an Internet application, an e-mail client, a web browser, a peer-to-peer application or an Instant Messaging system?

- Do you recognize the actual service (web, ftp, e-mail services like outgoing (SMTP) or incoming (POP3) e-mail)?

If the answer to any of these questions is YES, the appropriate action is to permit the connection.

If the answer to any of the situations above is NO, you should consider denying the connection, at least for the current session.
If you are uncertain what the dialog means, we recommend that you deny the connection for the current session and investigate the different parameters closer.

- Is it an outgoing or an incoming connection, or a script alert?
- Does the program that tries to connect to the Internet belong to an application that is updated automatically over the Internet?
- Have you recently scanned your hard drive(s) with updated antivirus software to make sure that the program asking for permission is not a Trojan/Backdoor?
- Is there any available information about this service/port in security forums or on web sites of known firewall vendors?

**Cookies** compromise privacy and should be refused unless you know that they are required for a web site’s functionality. Such sites include:

- Online banks.
- Web-based e-mail readers, such as Hotmail.
- Search engines, such as Google, Altavista and AllTheWeb.
- Any other site which requires that you to log on with a user name and password.

You should also block active content from sites that you do not trust.

As you will see from the pop-up dialogs, there is an option to make NPF remember the rules you create. The amount of pop-ups and questions will therefore decrease when you have responded to the most commonly used Internet applications web sites.

You can always go back and modify firewall rules if you find that the current rules are too rigid, for example. The NPF Console section will tell you more about this.
**NPF Assistant pop-up dialog example**

This example will show how you grant MSN Messenger the appropriate rights to perform its tasks by establishing a rule for this particular application.

When starting the MSN Messenger application for the first time after installing NPF, you will get a pop-up dialog like this:

![Connection Alert](image)

As you can see this is a Connection Alert where NPF wants to know if you want to permit outgoing connections to the Internet from `msnmsgr`, a vital part of MSN Messenger. MSN Messenger users should definitely allow this connection.

The next parts of the dialog will tell more about the service/port and address in question.
This wizard will help you create a firewall rule that permits outgoing TCP network communication.

You will be asked about the following rule properties:

Application: msnmsgr
Remote service: 1863
Remote address: 207.46.104.20

To begin creating the firewall rule, click on Next.
Current rule definition: Allow "msnmsgr" to perform outgoing TCP communication.

Choose whether this rule permits network communication using only the "1863" service or any service. A network service defines what type of communication can take place with another computer (for example, web browsing [http] or email [pop, smtp, imap]).

The rule applies to:

- Any service
- 1863
MSN Messenger offers a lot of features and may need access to several services and addresses, so consider permitting access for “Any service” and “Any address” for this application.

**Special note regarding incoming connections**

In the rule editor it is possible to permit an incoming connection only for a specified application. If you permit incoming connections to a service/port, you are in fact permitting incoming connections for *any* application on that port from the address in question, since the firewall do not know which application will handle this request.

You should therefore treat such a rule with extreme caution. Allow only specific addresses and ports connection to your computer. Avoid vagueness by admitting “any” address or service/port.
Using NPF console

When you have installed Norman Personal Firewall (NPF), a new icon appears in the system tray. This is called the NPF Console:

When you right click this icon, a menu with various shortcuts appears:

Settings

Click Settings to start the NPF configuration utility.
Block referer

When you click on a link in a web browser, the browser sends information to the new location about your current location. Enable this setting if you don’t want web servers to log your origin. Note that some sites require that you issue the referer.

Script, ActiveX, and Applet

Active content like scripts, applets and ActiveX components differ from the standard web documents in that they are actually small programs, intended to enhance your experience of a web site. However, these programs may also contain malicious code. The options Permit and Restrict set definitive rules for files of these types, whereas Assist launches the NPF Assistant for each instance.

Pop-up windows

Pop-up windows are scripts that can be launched without the user’s consent. NPF allows you to specify which pop-up
windows to allow, and which to deny. The default option for Scripts is Permit. If you want to filter these pop-ups you should select Assist or Deny.

### Outgoing cookie

When you accept a cookie from a web site it may be stored for later use. If you feel that your privacy may be compromised by this, you can use NPF to control the retrieval of cookies. Note that some sites require that you accept cookies.

The options Permit and Restrict set definitive rules for files of these types, whereas Assist will launch the NPF Assistant for each instance.

### Clear session rules

This option removes all rules established during the current session, unless you have instructed NPF to remember these rules. A session is the time span from when a user accesses an application until the user quits the same application.

*Note:* If the web site you are visiting is stored among the browser’s temporary files, Clear Session Rules has no effect.
NPF settings

All NPF’s settings can be configured from this central configuration utility, ranging from editing the rule set, to setting the time of day an Internet connection is allowed.
Status

This panel displays the current status of your firewall, and allows you to switch the entire firewall on and off.

The Firewall Engine is the component that monitors all connections made between your computer and the network. If you stop the engine, NPF will no longer monitor any connections on your PC. As a consequence, the PC is unprotected and exposed to external strikes.

The NPF Assistant is the component that prompts you when unknown connections are made. If you disable the assistant only, your PC is protected, but any connection without a set rule will be refused.

**Note:** If the NPF Assistant is turned off, the rules for Parental Control and Active Content are disabled at the same time. Existing rules are reactivated as soon the assistant is started again.
Security

This panel allows you to edit rules about connections:

![Security Panel](image)

**Understanding how to configure your firewall**

If you have your own *private* network, you may want to share resources between your computers. The *Local Intranet* setting allows you to do so in a private network, while keeping other computers and networks out.

However, if your ISP assigns your computer a *public* IP address, then others in the same ISP network segment may access your computer. Then the *Intranet Resources* security setting will provide better protection for your computer.

Please consult your ISP to find out how IP addresses are assigned.
**Local Intranet (Full intranet access)**

Select this option to allow all connections to your computer from PCs in the local network. You grant access to all services on your computer, including, but not limited to, file and printer sharing.

**Intranet Resources ((Allow resource sharing)**

Select this option if you only want access to your files and printers from the local network.

**Intranet Resources ((Deny resource sharing)**

Denies all Intranet access, even though you have established shares.

**Deny all**

This setting terminates all connections to and from your computer. It should only be used if you suspect that there has been established an unauthorized connection through one of your allowed applications, for example Internet Explorer.

This setting will not be overruled by set rules.

**Ask first**

This setting will always ask you for any connection that is not specified by any rule.
Setting the security level for Active Content

Use the slider in this screen to set the desired security level. You may select one of the three predefined security levels, or click **Reset** to retrieve predefined settings.

The settings that apply to the selected security level are listed to the right of the slider, and you will see the description of the different levels change as you move the slider up or down:

> Please refer to ‘Active Content’ on page 46 for more information on how to handle Active Content.
Customize security level

**Note:** This dialog is primarily for experienced users. These settings allow you to customize your general security level.

### Monitoring

- **Log all website access**

  Checking this option will log all web sites visited by the user. Can be combined with Parental Control settings to keep track of web surfing.

---

**Monitoring**

- **Log all website access**

  Checking this option will log all web sites visited by the user. Can be combined with Parental Control settings to keep track of web surfing.
Log Intrusions
This setting will log all attempts to intrude your computer.

Log Port Scans
This option will log all attempts to scan any ports on your computer.

ICMP

Block Incoming ICMP
This option allows you to block all incoming ICMP requests, like the commonly used “ping” command.

Block Outgoing ICMP
This option allows you to block all outgoing ICMP requests, like the famous “ping” command.

Trusted IPs
This setting allows you to add trusted IP addresses to your firewall. A trusted IP address or range can connect to your computer regardless of all set rules.

You can use wildcards to specify an IP range like this:

192.168.0.*

In this example you trust the whole 192.168.0.0 subnet and all the computers in this network.

Trust by MAC address
This setting allows you to trust computers by their network card address, rather than the IP address. You can add the MAC address manually or detect the MAC address in your network by clicking Detect, and then adding them to the Trusted MAC Address list.
Note: MAC addresses are normally unique to every network card, but it is possible to “fake” the MAC address on many network cards. Because it is relatively easy to change the MAC address, we recommend that this option is used with great caution.
How to manage rules

Click Rules to add, modify or delete a highlighted rule. A new screen appears, listing details about the selected rule.

Adding a rule

**Note:** Normally there is no need to add rules manually, as they can be set automatically by the NPF assistant. However, if you feel comfortable with the concepts of a firewall, this option may represent a more convenient way to customize your firewall.

1. Click Add. In the dialog that appears, select the action you want NPF to take when the rule is matched. Then select whether the connection is made by a remote computer (Incoming), by you (Outgoing), or if it has been established by Both.

2. Now you should select the protocol used by the application(s). TCP is the standard for file transfers, as it has built-in error handling. UDP is faster than TCP, but doesn’t provide error handling. It’s normally used for streaming data, such as video feeds and on-line games, where loss of data is of less importance.

3. Under the Application tab you can specify whether this rule applies to any program or a specific application. If you selected Application shown above, click Browse to locate the application.

4. Then select the Service tab. You must enter which ports are used by the application(s), either by entering the port number(s), or by selecting one of the pre-defined services from the list.

5. Finally, specify the IP addresses from which you will permit or deny connections. Select the Addresses tab. This menu defaults to Any address, marked by an asterisk (*), but you can import several addresses or specify an IP range, for example the range in your private network.
Click **OK** to finalize your settings. The rule takes effect immediately.

**Note:** Never add an incoming rule that consists of any local port and any remote port. This effectively removes the incoming protection of NPF even if you specified a particular application. The reason for this is that when an incoming connection/packet arrives, it’s not possible to see if this packet is actually issued from a particular application on the Internet/network.
Modifying a rule

The best way to explain how to modify an existing rule is by providing an example:

After running NPF for a while you are no longer able to connect to the Internet with the Adobe Acrobat reader application to view PDF files. To check if a too rigid firewall rule is causing the problem, follow this steps.

1. Click the NPF icon in the System tray or select Norman Personal Firewall from Windows’ Start menu.

2. Select **Settings** and enter the section where you want to modify a rule (“Security” or “Active content”). As the problem seems connection-related you are probably dealing with a Security rule.

3. Select **Rules**.
4. You will now see all security rules that you have configured since NPF was installed.
The overview may seem a little overwhelming, but it is really not that difficult. To sort the columns, click the column header with the criteria that you want to sort by. In this example, only four firewall rules are defined. After a closer look on the rules, you discover that there is a rule where “Action” is set to Deny for AcroRd32.exe in the “Application” column. Highlight this rule and click Modify.

5. You can now change “Action” for this particular rule. Select Permit: Allow the connection from the drop-down menu and click OK.
Adobe Acrobat Reader should now be able to connect to the Internet again

**Parental control**

The Parental Control feature allows you to filter web contents, block advertisements, to restrict access to specified web sites only, and even schedule a surfing time.
To enable Parental Control you must first create a new user to apply restrictions to.

The default user **admin** cannot be restricted.

The default user **admin** has the password “1234”, unless you have created a password yourself.

To add new users, click **Settings**. Click **Add** in the new window that appears.

Enter the desired name in the **Name** field. The default password is “password”.

Click **OK**. To add more options to the user that you have just created, select the user and click on **Modify**.

In the “Filtering” display, make the desired selections.

You must set the *newly created user as the default user* for the Parental Control settings to take effect. At next restart this user will be the default user for Norman Personal Firewall.

To change any settings you must provide the “admin” password when prompted by the Norman Personal Firewall Settings.
Use Advertisement Blocking - enables all the pre-defined rules for advertisement blocking. Blocked advertisements appear on the web pages as rectangular blank regions.

Use Web Site Filtering - enables all the pre-defined rules for web site filtering.

Use Content Filtering - enables all the pre-defined rules for content filtering.

Allow only sites in Personal List - enables the pre-defined sites only. To define the sites, click on the Edit Personal List button. This option will disable all other filtering settings.

- A new window appears. Click on Add to display the next window. Enter the HTML string (URL) and click on OK.
- To edit / change an entry, select the entry and click on Modify. Make the necessary changes and click on OK.
- To delete an entry, select the entry and click on the Delete button.

Note: Be cautious when using the Personal List feature. Web sites can often link to content from other sites, and may during certain circumstances look crippled if these sites are not in the Personal List.

Example:

http://www.disney.com will try to link to several other sites, including disney.go.com. The entry www.disney.com in the Personal List does not display the web site correctly. But entering only disney will make the site appear better, even
though several other sites are being linked to it that are not allowed.

In the **Schedule** dialog, click on the **Schedule** button. A new window appears.

In the **User schedule** dialog, click on the **Add** button. Another window appears. Select the desired days and enter the duration of time. Note that the format is 24 hours. Click on **OK**.

![Duration Dialog](image)

Enter the quota for Internet browsing here. Enter the number of days and hours the user can browse the Internet in the period. For example, if you select 7 days and 10 hours, this means that this user can browse the Internet for 10 hours in 7 days.

Finally, if you are satisfied with the specified options, click on **OK** to save your entries.

**Advertisement blocking**

In the ‘Advertisement Blocking’ dialog, click on the **Setting** button. A new window appears.

To add to the expressions, click on the **Add** button. Another window appears where you can enter the expressions in the HTML strings before clicking **OK**. A typical expression would be `/adclient`.

To see the pre-defined list of expressions, click the **Default list** button.
To edit/change an entry, select the entry and click on the Modify button. Make the necessary changes and click on OK.

To delete an entry, select the entry and then click on Delete.

To change the default list, click on the Default button and repeat the steps above.

**Web site filtering**

When you click on the Setting button in the Web Site Filtering dialog, a new window appears with a list of pre-defined regular expressions.

To add to the expressions, click on the Add button. Another window appears where you can enter the expressions into the HTML strings before you click OK.

To edit/change an entry, select the entry and click on the Modify button. Make the necessary changes and click on OK.

To delete an entry, select the entry and then click on the Delete button.

To change the default list, click on the Default button and repeat the steps above.

Do not use the http:// prefix when adding expressions.
Example:

You want to block *msn*. If you add *http://www.msn.com*, *msn* will not be blocked. Simply enter *www.msn.com*.

Be careful and precise when you add expressions to the web site filtering list. Below you will find some examples of expressions and how NPF will use them:

**IC**

If you add only “ic”, the firewall will block all addresses containing “ic”:

- *http://www.ic.org*
- *http://www.icq.com*
- *http://www.microsoft.com*

**WWW.IC**


**IC.ORG**


**ICQ.COM**

If you add “icq.com”, the firewall will block *http://www.icq.com* but not *http://www.icq.dk*.

**Content filtering**

In **Content Filtering**, click on the **Settings** button. A new window appears with a list of pre-defined regular expressions.

To add to the expressions, click on **Add**. Another window appears where you can enter the expressions into the “HTML String” before clicking **OK**.
To edit/change an entry, select the entry and click on the Modify button. Enter your changes and click on OK.

To delete an entry, select the entry and then click Delete.

To change the default list, click on the Default button and repeat the steps above.

Privacy

From this panel you can configure elements concerning information that can be traced from your web browsing. Such traceable information includes cookies and so-called referring.

Block referrer

When you click on a link in a web browser, the browser sends information to the new location about your current location. Enable this setting if you don’t want web servers to log your origin.

Cookies

You can also set up customized rules for cookies. Cookies are used as a tool to identify you to certain web sites, thereby distinguishing you from other users. Cookies pose no threat by themselves, but they may violate your privacy on the web.

For incoming, as well as outgoing cookies, you can choose between Permit, Deny and Assist. In addition, the option I trust this domain for scripts, cookies, active-x, pop-ups and applets has the effect that the current domain will be trusted and all other active contents and cookies will be permitted for the said domain.

You can specify more rules for cookies by clicking the Advanced button. This will present you with a list of existing rules.
Click **Add** to add a new rule for cookies. Then select the direction of the cookie: outgoing, incoming or both. Select the action you want NPF to take for this rule, either permit or block the cookie. If you want assistant help, select **Assist (Prompt me)**.

If you know the name, select **The name shown above** and type in the name of the cookie. If not, select **Any name**.

Finally, select any domain or path. If you want to restrict this rule to one domain only, select **The domain or path shown above** and type in the domain or path name. Click **OK** when you’re done.

To change an entry, highlight it and click **Modify**. Highlight and click **Delete** to remove a rule.
Active Content

**Note:** See also ‘Setting the security level for Active Content’ on page 29 for information on how to select level, and how the different security levels affect how the different elements are handled.

This panel displays the settings for active content. Active content like scripts, applets and ActiveX components differ from the standard web documents in that they are actually small programs, intended to enhance your experience of a web site. However, these programs may also contain malicious code.

When the Active Content assistant appears, you can either Permit or Deny the content in question. In addition, the option I trust this domain for scripts, cookies, active-x, pop-ups and applets has the effect that the current domain will be trusted. All other active contents and cookies are permitted for the said domain.

**Note:** To learn more about ActiveX, scripts and applets, please refer to the Glossary on page 51.
You can permit, deny or restrict active content on a generic basis, or set up individual rules for active content. To set these rules click on **Advanced**.

Click **Add** to add a new rule for active content. Then select the type of active content and what action you want NPF to take. If you need assistant help, select **Assist** *(prompt me)*.
Select the type of active content you would like to add a rule for, and if you would like to permit or deny this.

Select **The domain shown above** and specify the domain to which this rule applies, or select **Any domain**. Click **OK** when you’re done.

To change an entry, highlight it and click **Modify**. Highlight and click **Delete** to remove a rule.

**Log**

NPF can also keep a log of net-based activity for later review. To view a log file, select the log file and click on **View**. To remove a log file, select the log file and click **Delete**.
You can also set the log limit by size by clicking **Advanced**. The advanced menu also displays the location of the log files.

NPF generates four different log types:

1. **Application Intrusions**
   This refers to connections issued by applications that are denied by NPF. The log contains the full path of the application and the activity that was denied.

2. **Packet Intrusions**
   Incoming packets that are denied by NPF are listed here. The log contains parameters of the packet and the source/destination that is intended for.

3. **Port Scans**
   When a number of packets arrives at your system looking for important ports that your system might or might not have opened, this pattern will be logged as a port scan. This indicates that someone is scanning your system for services or vulnerabilities, and gathers information prior to a possible attempt to hack.
   NPF will log the source of the scan.

4. **Web Sites**
   NPF logs the URL of web sites that users of your system have visited. The log contains the URL of various resources accessed during the visits.

### WEB

The Web panel allows you to customize additional ports for web monitoring. Ports listed in this panel means that they will be monitored against cookies, scripts, Active-Xs, Java Applets, JavaScripts as well as web site’s logging.

The normal port for web browsing is port 80. Some web sites use other ports for different reasons. Use this feature if you are browsing web sites that specifically use other ports than port 80 to be sure these will be monitored for Active content.

**Port to monitor**

Enter additional port here and click **Add** to insert the port to the list. You can remove any of the ports by selecting on it and click **Delete**.
You can add extra port numbers for web access (HTTP). Type in the port number and click on the **Add** button.

To remove a port, select a port and click on the **Delete** button.
Glossary

**ActiveX control**
A set of rules for information sharing between applications. Browsers can download and execute ActiveX controls automatically.

These rules are comparable to *applets*, but ActiveX controls pose a potential threat because they have access to the operating system.

**Applet**
Applets are programs devised to be launched from inside another application. However, applets cannot be executed directly from an operating system, like applications. A browser can interpret applets from a web server. Applets are small (in file size), compatible, and secure, and consequently perfect for small Internet applications that can be accessed from a browser.

**Cookie**
Information/message sent to a web browser from a web server. The browser saves the message to the text file `cookie.txt`. Then the message is returned to the server whenever the browser addresses a page on the server.

The principal objective for cookies is to recognize Internet users and perhaps present tailor-made web pages for them.

**Pop-up windows**
Any window that pop up without your consent while you are surfing are simply called pop-up windows. There are many ways to generate a pop-up window, where the easiest technique is to use JavaScript-related commands.

**DNS/IP**
DNS is short for Domain Name System (or Service). This is an Internet service that converts domain names into IP addresses.
Domain names are alphabetic and consequently easier to remember than the number-based IP addresses. But the Internet is really based on IP addresses. So whenever you specify a domain name, a DNS service must convert the name into the related IP address. For example, the domain name www.norman.com might translate to 10.0.0.255.

Note that the DNS system is actually its own network. If a DNS server cannot figure out a particular domain name, it addresses another and so on until the correct IP address is returned.

**JavaScript**

A scripting language used by web masters to design interactive sites. JavaScript can interact with HTML source code, and allows web masters to create more exciting and dynamic sites.

**Services**

A computer may offer several services to its users, including web and e-mail. The computer is allocated with one IP address only, and uses ports to tell one service from another. When a web browser is instructed to look up www.norman.com, the browser - in addition to the server address - sends a port number. In our example the number that is sent is 80. This number is the common port number for web browsing, like 25 is the port number for sending e-mail. For a complete list of port numbers, please refer to the Internet Assigned Numbers Authority’s web site: www.iana.org.
Index

---A---
Active content 8, 26, 47, 49
ActiveX 46
applets 46
monitor port 49
rules 48
scripts 46
scripts, applets, ActiveX 10
trust domains 46
Active-X 49
ActiveX 10, 11, 23
Add ports (HTTP) 50
admin
default password 39
admin password 39
administrator privileges v
AllTheWeb 17
Altavista 17
Any address 21
Any service 21
applet 10
applets 11, 23
Application intrusions 49
Auto setup 12

---B---
block addresses 43
Block Incoming ICMP 31
Block Outgoing ICMP 31
block referer 23

---C---
Connection alert (NPF Assistant) 15
Content Filtering 43
HTML strings 43
content filtering 40
Conventions iv
cookies 8, 10, 49
customized rules 44
Create rule
Any address 21
Any service 21
Customize security level
Block Incoming ICMP 31
Block Outgoing ICMP 31
Log all website access 30
Log Intrusions 31
Log Port Scans 31
Monitoring 30
Trust by MAC address 31
Trusted IPs 31

---D---
DNS 9, 51
DNS server 9
DNS service 52
Domain Name Service 9
Domain Name System (DNS) 51
domain names 52
dynamic content 11

---E---
expressions
content filtering 43

---F---
filter web contents 38
Filtering
Advertisement Blocking 40
Allow only sites in Personal List 40
Content Filtering 40
Web Site Filtering 40
Filtering display 39
Firewall Engine 26
Freshie Assistant 12, 14

---G---
Google 17
hacking attempt 49
Hotmail 17
HTML strings 42
Content filtering 43

ICMP 31
incoming connection/packet 34
installation path 12
Intranet Resources 27
IP address 8, 9, 51

Java 11
Java Applets 49
JavaScript and HTML source code 52
JavaScripts 49

Log all website access 30
Log Intrusions 31
Log Port Scans 31
Log types
Application Intrusions 49
Packet Intrusions 49
Port Scans 49
Web Sites 49

MAC address 31
Manual setup 12
Monitor ports 49
Monitoring 30
MSN Messenger 18

NIC 13
Norman Internet Control (NIC) 13
Norman Personal Firewall Assistant 14
NPF Assistant 23, 26

Connection alert 15
Script Alert 15
NPF assistant
Managing rules 33
NPF Console 16, 22

outgoing cookie 24

Packet intrusions 49
Parental Control 26, 30
create new user 39
ping 31
pop-up window 23
Pop-up windows and browsing 51
port number 52
common ports 10
Port scans 49
Privacy
block cookies 45
Block referrer 44
Cookies 44
public IP address 27

Requirements, system v

Schedule 41
schedule surfing time 38
Script alert (NPF Assistant) 15
scripts 10, 11, 23, 49
Security
Ask first 28
Deny all 28
Full Intranet Access 28
Intranet Resources (Allow sharing) 28
Intranet Resources (Deny sharing) 28
Intranet rules 28
Local Intranet 28
services 8, 9, 52
SETUP.EXE 12
slider for Active Content 29
System requirements v
system tray 22

---T---
TCP 33
Technical support v
The Internet Assigned Numbers Authority 52
Trust by MAC address 31
trust domain for scripts, cookies, active-x, pop-ups and applets 44
trust domains 46
trusted IP address 31
Trusted IPs 31

---U---
UDP 33
Use Advertisement Blocking 40
Use Content Filtering 40
Use Web Site Filtering 40
User Manager
  Personal List 40
User schedule 41

---W---
Web panel 49
  Monitor ports 49
Web site filtering
  Block addresses 43
  Example 43
  HTML strings 42
web site filtering 40
Web sites (logging) 49