

User Guide

Firewall Suite

August 1, 2003



© 2006 Marshal Limited, all rights reserved.

U.S. Government Restricted Rights: The software and the documentation are commercial computer software and documentation developed at private expense. Use, duplication, or disclosure by the U.S. Government is subject to the terms of the Marshal standard commercial license for the software, and where applicable, the restrictions set forth in the Rights in Technical Data and Computer Software clauses and any successor rules or regulations.

Marshal, MailMarshal, the Marshal logo, WebMarshal, Security Reporting Center and Firewall Suite are trademarks or registered trademarks of Marshal Limited or its subsidiaries in the United Kingdom and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Contents

Chapter 1	
Installation	1
System Requirements	2
Installing Firewall Suite	2
Installing from the Autorun	2
Installing from the Run Dialog Box	3
Software License Agreement	3
Registering your Software	4
Uninstalling Firewall Suite	4
License and Registration	5
Trial Mode	5
Purchasing Firewall Suite	6
Adding More Firewall Licenses	7
Chapter 2	
Getting Started	9
Creating Firewall Reports	9
Producing Firewall and Web Activity Reports	10
Configuring Your Firewall	10
Create a Profile	11
Generate a Report	12
Alerting and Monitoring	13
Starting Firewall Suite	13

The Main Console	14
Profile Description List	15
Tasks Area	17
Main Menu	18
Functions Area	22
Profile Type Tabs	22
Reports Using a Sample Profile	23
Using Shortcuts	24

Chapter 3
Firewall Profiles **27**

Profile Types	28
Viewing a Sample Profile	28
Choosing a Firewall Profile Type	30
Creating a Firewall Profile	31
Firewall Configuration Dialog Box	32
Title, Log File Format Dialog Box	34
About the WebTrends Syslog Service	37
Log File Retrieval Methods	38
List of Servers Dialog Box	40
Editing the Server List	42
Deleting a Server from the List	42
IPs Behind Firewall Dialog Box	43
Adding an IP Address	44
Removing an IP Address	44
Selecting or De-selecting an IP Address	44
Internet Resolution Dialog Box	45
Specifying Settings for DNS Lookup	46
Clearing the DNS Cache	48
Sharing the DNS Cache	49

URL Categorization	50
Choosing Settings for Categories	52
Category Types	52
Updating the URL Categorization Database	55
Incorrect Categorization of IP Addresses	55
System Performance and URL Categorization	56
Licensing the URL Categorization Database	56
Mapping URL Categories	57
Reporting with URL Categorization	59
Proxy Server Settings	59
Category Names	60
Interpreting Categorization Reports	61
Home Page Dialog Box	63
Filters Dialog Box	66
Creating a Filter	67
Editing a Filter	68
Deleting a Filter	68
Copying and Pasting a Filter	69
Bandwidth Cost Dialog Box	70
Specifying Bandwidth Cost	71
Database and Real-Time Dialog Box	72
FastTrends Database	72
Real-Time Analysis	73
Maintaining the FastTrends Database	73
Advanced FastTrends Dialog Box	76
Setting Up Syslog Dialog Box	77
Editing a Profile	78
Copying a Profile	79
Deleting a Profile	80
Specifying Log Files	81
Specifying a Single Log File	82
Specifying Multiple Log Files	82
Using Firewall Add-On Support for Clusters	88

Using Department Management	90
Defining a Department	91
Editing a Department	92
Running Firewall Activity Profiles from the Command Line	94
Basic Information	94
Command-Line Components	95
Command-Line Examples	98
Designing Firewall Profiles	99
Report Content	99

Chapter 4	
Alerting and Monitoring	103
Alerting and Monitoring Profiles	103
How Alerting and Monitoring Works	104
Sample Alerting and Monitoring Profiles	105
Alerting and Monitoring Profile Settings	106
Device or Object Being Monitored	106
Monitoring Schedule	107
Response Settings	107
Creating an Alerting and Monitoring Profile	109
Specify Profile Description and Type	110
Specify Profile Details	112
Specify Monitoring Schedule Settings	113
Specify Response Settings	114
Choosing Response Options	115
Adding a Response Schedule	118
Adding and Configuring Response Actions	123
Creating an Audio Alert	125
Creating an Email Alert	126
Creating an Execute Program Response Action	128
Creating a Multi-Response Action	129
Creating a Pager Alert	130

Creating a Reboot Response Action	138
Creating a Restart Service Response Action	140
Creating an SNMP Trap Alert	141
Customizing Text Messages	142
Formatting the Message	144
Defining Advanced Monitor Options	144
Configuring Alerting and Monitoring	
as a Windows Service	146
Setting up the Required Rights	146
Monitor Types	148

Chapter 5

Filtering for Focused Reports 157

Filter Basics	157
Filter Types	157
Filter Elements	158
Combining Multiple Filters	159
Working with Filters	160
Adding a Filter to a Profile	160
Modifying a Filter	162
Deleting a Filter	163
Filter Elements	164
Overview	164
Filter Element Descriptions	166
Actions	166
Authenticated Username	168
Browser	169
Category	169
Day and Time	171
Departments	172
Directory	173
External User Address	175

File	177
Firewall Actions	179
Firewall Name	180
Internal User Address	181
Multi-Homed Domain	182
Proxy Cache	184
Referrer	187
Return Codes	189
Rule	191
Sites	192
Firewall Status Code	193
Traffic Direction	194
Protocol Family	195
User Address	196
User (IP)	198

Chapter 6
Working with Reports **201**

Firewall Reports	201
Generating Firewall Activity Reports	202
Memorized Report Settings	203
Alerting and Monitoring Reports	213
Creating Alerting and Monitoring Reports	214
Memorized Alerting and Monitoring Report Settings	215
Customizing Reports	219
Report Range Definitions	230
Specifying a Distribution Method	235
Limiting Memory Used by Reports	237
Determining Memory Usage	237
Limiting Memory Usage	238

Chapter 7

Scheduling Reports	241
The Scheduler	241
Tabs	242
Functions Area	242
Scheduling and Running Events	243
Scheduling a New Event	243
Editing a Scheduled Event	249
Running a Scheduled Event on Demand	250
Stopping an Event from Processing	251
Specifying a Distribution Method	252
Date Macros	253
Managing Scheduled Events	255
Scheduled Events Tab Elements	256
Using the Scheduled Events Tab	259
Managing the Scheduled Events List	260
Schedule Log Tab Elements	261
Performance Analysis Log Tab Elements	264
Using the Options Tab	268
Simultaneous Processes	269
Schedule Log Files	270
Performance Analysis	270
Performance for On Demand Report	271
Miscellaneous	271
Commands	272
Using the Remote Scheduling Tab	272
Setting up the Remote Scheduling Server	273
Configuring Your User Account for Remote Scheduling	274
Accessing the Remote Scheduling Server	275
Schedule Log	276
Using the Performance Log	276
Scheduled Events	276
Running Reports	277
The Start or Stop WebTrends Service Dialog Box	277

Chapter 8	
Monitoring Activity	281
Monitoring Security Events	281
Finding the IP Addresses that Cause the Most Errors	283
Focusing on an IP Address	284
Monitoring Internet Searches	284
Monitoring Bandwidth Usage	285
Identifying High-Bandwidth Users	286
Chapter 9	
Options	287
Main Options	287
Main - General Dialog Box	289
Access to Internet Dialog Box	292
MS-Word and Excel Dialog Box	297
Search Engines Dialog Box	299
Report Ranges Dialog Box	303
Language Dialog Box	310
General Firewall Activity Options	314
General Firewall Activity - General Options	315
File Types Dialog Box	317
Domains Dialog Box	321
FTP Dialog Box	324
Protocols Dialog Box	325
DNS Dialog Box	329
Syslog Dialog Box	332
LEA Connections Dialog Box	334
Licensed Firewalls Dialog Box	339
Cisco PIX Interfaces Dialog Box	340

Alerting and Monitoring Options	341
Alerting & Monitoring - General Dialog Box	341
Response Schedules Dialog Box	343
Response Configurations Dialog Box	345
Response Actions Dialog Box	347
Language Dialog Box	349

Appendix A
Specifying Log Paths **351**

Formatting Log File Path Entries	351
Standard Examples	351
Compressed Logs	352
Wildcards	352
Date Macros	353
IP Addresses	354
Performance	355
Using Filters to Optimize Performance	355
Running Reports Without DNS Lookup	356
Activating FastTrends	356
Accessing the Log File	356
Selecting the Report Type	357
Zipping Archived Log Files	357

Appendix B
Silent Installation **359**

Disk Space	359
Licensing Issues	359
Silent Installation for Windows NT, Windows 2000, and Windows XP	360
Installing as Administrator	360

Glossary **363**

About This Book and the Library

The *User Guide* provides conceptual information about the NetIQ Firewall Suite product (Firewall Suite). This book defines terminology and various related concepts.

Intended Audience

This book provides information for individuals responsible for understanding Firewall Suite concepts.

Other Information in the Library

The library provides the following information resources:

Firewall Configuration Guide

Provides information about configuring your firewall to work with NetIQ firewall security applications

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	<ul style="list-style-type: none">• Window and menu items• Technical terms, when introduced
<i>Italics</i>	<ul style="list-style-type: none">• Book and CD-ROM titles• Variable names and values• Emphasized words
Fixed Font	<ul style="list-style-type: none">• File and folder names• Commands and code examples• Text you must type• Text (output) displayed in the command-line interface
Brackets, such as [value]	<ul style="list-style-type: none">• Optional parameters of a command
Braces, such as {value}	<ul style="list-style-type: none">• Required parameters of a command
Logical OR, such as value1 value 2	<ul style="list-style-type: none">• Exclusive parameters. Choose one parameter.

About Marshal

Marshal's Content Security products (MailMarshal for SMTP, MailMarshal for Exchange , WebMarshal, Security Reporting Center and Firewall Suite) deliver a complete email and Web security solution to a variety of Internet risks. They provide comprehensive protection by acting as a gateway between an organization and the Internet. It allows organizations to restrict, block, copy, archive, and automatically manage the sending and receiving of messages.

Marshal Products

Marshal's Content Security solution, which includes MailMarshal SMTP, MailMarshal for Exchange and WebMarshal, delivers a complete email and Web security solution to these risks by acting as a gateway between your organization and the Internet. The products sit behind your firewall but in front of your network systems to control outbound documents and their content. By providing anti-virus, anti-phishing and anti-spyware protection at the gateway, Marshal's Content Security solution offers you a strategic, flexible and scalable platform for policy-based filtering that protects your network, and as a result, your reputation.

Contacting Marshal

Please contact us with your questions and comments. We look forward to hearing from you. For support around the world, please contact your local partner. For a complete list of our partners, please see our Web site. If you cannot contact your partner, please contact our Technical Support team.

Telephone: +44 (0) 1256 848 080 (EMEA)
+1 404 759 2890 (Americas)
+ 64 9 984 5700 (Asia-Pacific)

Sales Email: info@marshal.com

Support: www.marshal.com/support

Web Site: www.marshal.com

Chapter 1

Installation

For security and performance reasons, we recommend that you install Firewall Suite on a workstation other than the one running the firewall or proxy server software. We also recommend that you do not install Firewall Suite on a Primary Domain Controller (PDC) or Backup Domain Controller (BDC).

This chapter covers topics related to installing your Firewall Reporting solution, including:

- System requirements
- Steps for installing and uninstalling the software
- Considerations when installing the Alerting and Monitoring module
- Product license and registration
- Addition of firewall licenses

System Requirements

The following is a list of *minimum* system requirements for the computer running Firewall Suite:

- Microsoft Windows NT 4.x, Windows 2000, or Windows XP
- 1.0 GB available disk space
- 512 MB RAM

More disk space and memory may be required to analyze large log files. Contact your Product Support representative for more information.

- Microsoft Office 97 or later (if you plan to use Microsoft Word or Excel reports)
- Internet Explorer 4.0 and higher or Netscape Navigator 4.5 and higher

Installing Firewall Suite

Note

Although you do not need to provide license information to install Firewall Suite, you must do so before you can run the application. See “License and Registration” on page 5 for details.

The installation uses a straightforward setup program. Choose the procedure that best suits your needs.

Installing from the Autorun

Use this procedure if your system is set up to run CD-ROMs automatically when you place them in the drive

To install Firewall Suite:

1. Insert the program CD into your CD-ROM drive to launch the setup program.
2. Follow the on-screen instructions to install the program.

Installing from the Run Dialog Box

Use this procedure to start the installation program manually.

To install Firewall Suite:

1. Insert the program CD into your CD-ROM drive, and then choose **Run** from the File or Start menu.
2. In the Run dialog box, type:
`d:\setup`
where *d*: is the letter of your CD-ROM drive.
3. Follow the on-screen instructions to install the program.

Software License Agreement

Before the program files are copied to your system, the Software License Agreement is presented.

- ***If you agree to the stated terms***, click **Accept**.
- ***If you do not agree***, click **Cancel** to exit the setup program without installing.

Registering your Software

If you installed Firewall Suite from a CD-ROM you purchased, you can register your product online. If you purchased the product online, your registration is recorded automatically. Registration allows you to access technical support and ensures that you receive information about new releases of the product and other benefits.

To register your product:

1. Install Firewall Suite and then start it from either the **Start > Programs** menu or your WebTrends Firewall Suite desktop shortcut icon. Instructions for installing the product accompany the installation wizard.
2. From the Help menu of the product Main Console, select **Registration**. The product will start your Web browser, then connect to the NetIQ customer service Web site.
3. Complete the registration information requested at the site.

Note

If you do not register when you install Firewall Suite, you can register later by opening the Help menu and selecting Registration.

Uninstalling Firewall Suite

You can uninstall the program from the Windows Control Panel.

License and Registration

When you download Firewall Suite from the Web site and run Setup for the first time, choose one of the following options in the first installation wizard panel:

- *Install a free time-limited trial.* During a limited trial, you may use the product free of charge to create profiles and run reports on your own log files for a period of 14 days. After that period expires, you must purchase the product to continue to create profiles or run reports. If you do not, the product runs in a limited demonstration mode, which restricts you to creating reports only for the sample profiles provided.
- You will need to register for a trial code in order to use Firewall Suite in its trial mode. See “Trial Mode” on page 5 for details.
- *Install purchased software.* Purchasing the product gives you a license to create profiles and run reports on your own log files without restrictions. You will need to supply purchase information online, via telephone or fax, or by mail. NetIQ will issue you a product serial number, which you can use to enable a full license for the product. See “Purchasing Firewall Suite” on page 6 for details.
- *Upgrade current product.* If you have a previous version of Firewall Suite installed on your system, use this option to install a current product version. Setup will detect any previous product licenses you have, or you may enter a product serial number during installation.

Trial Mode

If you selected the **Install a free time limited trial** option in the first wizard installation panel and then completed the remaining installation steps, Setup starts Firewall Suite and displays the Product Licensing dialog box.

To run the product in trial mode:

1. Click **Register for a Trial Serial Number**. Firewall Suite opens the NetIQ customer service Web site.
2. Complete the Registration form, then click **Submit**. Your trial code is shown in the browser window and is sent to the email address you specify in the registration form.
3. Copy your trial code.
4. Return to the Product Licensing dialog box and paste the code you copied into the text box provided.
5. Click **Submit**. Your trial mode registration is complete.

Purchasing Firewall Suite

If you selected the **Install purchased software** option in the first wizard installation panel, but did not enter a product serial number in the next panel, Setup will install Firewall Suite without a serial number. When you next start the product, the Product Licensing dialog box opens.

To purchase the product you downloaded:

1. Click **Purchase Information**. Firewall Suite starts your Web browser, then connects you to the NetIQ customer service Web site.
2. Complete the purchase information required at the site. When you have finished, you will receive a serial number for Firewall Suite.
3. Copy the serial number.
4. Return to the Product Licensing dialog box, then paste the serial number you copied into the text box provided.
5. Click **Submit**. You can now run the product under a full license, without restrictions.

Adding More Firewall Licenses

The standard software license lets you install Firewall Suite on one system and report on one firewall. If you want to report on more than one firewall, you must purchase Firewall Add-Ons. For example, if you purchased a three-firewall Add-On, you could install Firewall Suite on one system and report on a total of four firewalls. You can purchase Firewall Add-Ons by contacting NetIQ or your reseller.

Chapter 2

Getting Started

This chapter tells you what capabilities Firewall Suite offers your organization. You will learn the components of the user interface and how to create your first firewall activity report by using a sample profile to generate a report. In addition, you will set up monitors and alerts and run reports based on these settings.

Creating Firewall Reports

Firewall Suite enables you to accomplish two basic reporting tasks:

- Produce firewall and Web activity reports that detail security violations, protocol usage distribution, bandwidth usage, employee Web surfing habits, incoming and outgoing traffic, FTP transfers and more.
- Set up monitors and alerts and report on them. When a device goes down or stops responding, or when a critical security event is detected at your firewall, Firewall Suite can alert you to these events. Customize alerts to notify you when the number of times an event occurs over a specific time period has exceeded your defined threshold.

Many other capabilities fall within these two high-level capabilities, but these more detailed features will be discussed in later chapters.

Producing Firewall and Web Activity Reports

Creating a firewall report requires that you:

1. Configure your firewall to produce log files that may be accessed and used by Firewall Suite.
2. Create a profile to define the information you want to capture in your report.
3. Generate a report either on-demand or by scheduling a reporting event.

The following section discusses these three steps in detail.

Configuring Your Firewall

Most firewalls generate log files that contain data about the activity occurring around the firewall. Firewall Suite uses these log files to capture, analyze and report on firewall activity; however, you need to configure your firewall properly to enable Firewall Suite to access and get the most from your firewall log files. The *Firewall Configuration Guide* provides this information on a firewall-by-firewall basis.

The configuration guide includes information about:

- Which versions of your firewall are supported by Firewall Suite
- Where the logs are located and how to retrieve or access them
- How to optimize your firewall log format to display the information you want in reports

The printed guide is included with your purchase, but you may also download and view it in Adobe® Acrobat® Reader version 4.0 or greater by visiting www.netiq.com/support. Make sure the cover of the guide you download specifies Firewall Suite.

Understanding Firewall Log Files

Depending on which application protocols your firewall is configured to handle, your firewall log files may contain a variety of different information. For example, it could contain information about users, the protocols they used, what activity they generated, their system platforms, the search engine they used, keywords on which they searched, date and time information and more. To create a profile and generate a meaningful report on your firewall activity, you must determine which type and version of firewall you have, how the activity information is recorded in the log file, and how you can retrieve that log file.

For example, if Firewall Suite relies on FTP, HTTP, or Syslog/LEA service access to retrieve log files, there will be an issue with firewalls that do not allow these types of access. If this issue is recognized ahead of time, a workaround can be developed, such as making a copy of the log file on another server for use with Firewall Suite.

The WebTrends Syslog Service

Many of the firewall log file formats supported by Firewall Suite support the WebTrends Syslog Service, a service that gets firewall log files in a consistent format that is usable by Firewall Suite. For more information, see the *Firewall Configuration Guide*.

Create a Profile

A profile is a group of settings that defines the location of your firewall log file and the type of information you wish to capture from it and include in reports. Specifically, it contains the information needed to import, process and store log files for analysis.

The three types of firewall and Internet activity profiles are:

- *General Firewall Activity profiles.* Let you produce reports on firewall and VPN security-related activity, including bandwidth and protocol usage, firewall rules, and firewall errors and warnings.
- *Incoming Firewall Activity profiles.* Help you analyze the Web activity coming through the firewall from external sources. Information in reports includes top requested pages; least requested pages; top paths through the site; and visitors by domain, geography, organization, browser, and operating system.
- *Outgoing Firewall Activity profiles.* Let you analyze the Web activity originating from within your network. Reports include bandwidth usage by user or department, Web sites visited by IP address, search engine keywords used, and authenticated user

Note

Different firewalls support different types of firewall and Web activity reporting. For more information, see the *Firewall Configuration Guide*.

Generate a Report

Firewall Suite lets you tailor the appearance of your reports by letting you choose the graphs and tables to include and the colors, fonts, layouts and text to use. Tables and graphs are organized under expandable categories in HTML. See “Working with Reports” on page 201 for information on generating and customizing reports.

Reports output to multiple HTML files, which allows for smaller file sizes—exactly how much smaller depends on the tables and graphs included. These smaller-sized files simplify printing and speed download times over slow connections.

You may also use the Scheduler to automate the generation of reports that you run regularly. See “Scheduling Reports” on page 241 for details.

Alerting and Monitoring

Firewall Suite's Alerting and Monitoring capability lets you:

- Monitor Web-related devices and services
- Send alerts when something goes wrong with a Web-related device or service
- Automatically restore Web-related devices and services when something goes wrong
- Run reports on the status and health of Web-related devices and services

The Alerting and Monitoring profiles you create define the devices and services you want to monitor and the type of response you want to occur when the status of a monitored device or service changes.

For more information, see “Alerting and Monitoring” on page 103.

Starting Firewall Suite

You can open the Main Console of Firewall Suite in any of these ways:

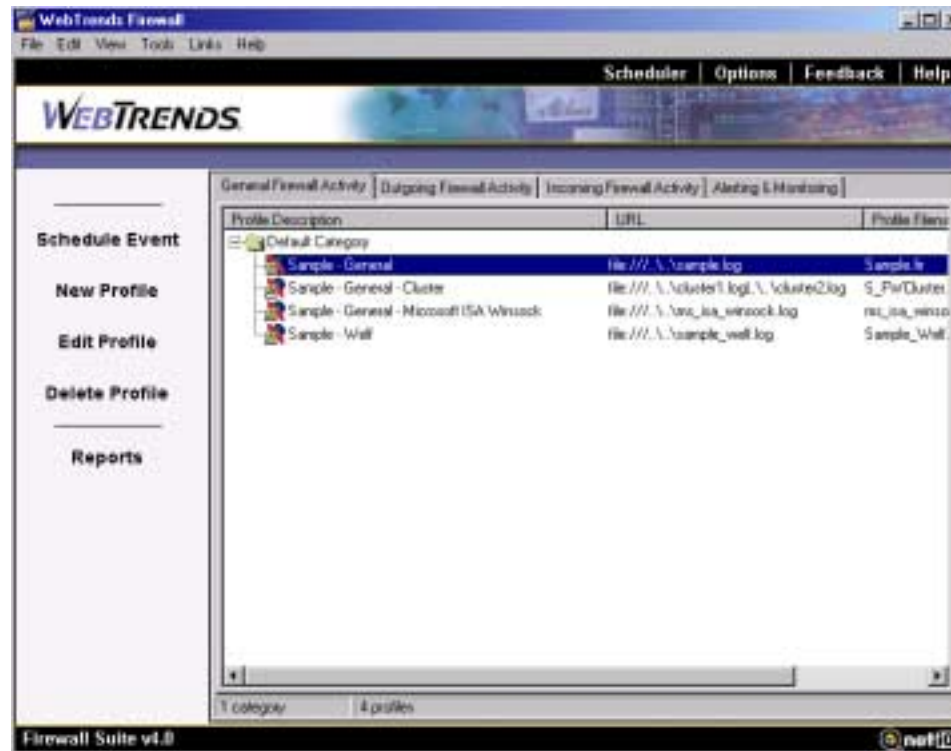
- Double-click the WebTrends Firewall Suite shortcut icon on your desktop
- Select **WebTrends Firewall Suite > WebTrends Firewall Suite** from the **Start > Programs** menu on your desktop
- Double-click wt_firewall.exe from the program group in the top level of Firewall Suite installation directory

The Main Console

The Main Console of Firewall Suite is the first window you see after starting the software. It contains five main areas:

- *Profile Description list.* Lists existing profiles, including sample profiles.
- *Tasks area.* Initiates common tasks such as profile creation and event scheduling.
- *Functions area.* Scheduler, Options, Feedback, and Help
- *Main menu.* File, Edit, etc.
- *Profile Type tabs.* General Firewall Activity, Outgoing Firewall Activity, etc.

The following figure shows the Main Console of Firewall Suite.



Profile Description List

Click one of the four Profile Type tabs: General Firewall Activity, Outgoing Firewall Activity, Incoming Firewall Activity or Alerting & Monitoring. For each tab, you see a list of the profiles available for running reports. This list includes sample profiles for each profile type, and if you already created profiles for an earlier version of Firewall Suite, these are automatically placed in the Default Category folder of the appropriate profile type.

The list contains folders, called categories, containing profiles. Each profile has an associated Profile Description column and other columns, depending on the selected profile type. Click any column heading to sort the list in alphabetically and numerically descending order (A, B, C... and 1, 2, 3...) according to the heading clicked.

For example, if you click the Incoming Firewall Activity tab, you will see the Profile Description called “Sample - Incoming” in the Default Category folder along with any other previously created Incoming Firewall Activity profiles. Beyond sorting the list of Profile Descriptions, there are other tasks you can perform on the Profile Description list.

Hiding or Showing Columns

When a profile description is so long that it can't display fully in the Profile Description column, you can hide the other columns to make room.

To hide or show columns:

1. Choose **Select Columns** from the View menu. The Select Columns dialog box displays.
2. Select a column check box to display the column, or clear the check box to hide the column. The Profile Description column cannot be hidden.
3. Click **OK**.

Organizing Profiles into Category Folders

You can organize your profiles using category folders. When you install Firewall Suite, the only category you have for each profile type is the Default Category. You can create, rename and delete these category folders as needed.

To create a new category:

1. Select **Category** from the File menu.
2. Type the new Category name and click **OK**.

To rename a category:

1. Select the category to rename.
2. Select **Rename** from the File menu.
3. Type the new Category name and click **OK**.

To delete a category:

1. Select the category to delete.
2. Select **Delete** from the Edit menu.
3. Type the new Category name and click **OK**.

Tasks Area

The tasks area, located along the left side of the Main Console, contains the features needed to manage, schedule an event for and generate reports on a selected profile.

- *Schedule Event*. Click this to open the Scheduler and the New Scheduled Event - Analysis wizard. The Scheduler displays profile reports that have been set up to run automatically. You can edit existing scheduled events in this window, or schedule automated events for additional profiles.
- *New Profile*. Click this to open the New Profile wizard and create a new profile in the selected profile type and category folder.
- *Edit Profile*. Click this to display a dialog box in which you can make changes to the selected profile.
- *Delete Profile*. Click this to delete the selected profile.
- *Reports*. Click this to open a list of available, pre-defined reports for the selected profile type. You can add, edit, rename or delete the available reports within this dialog box and you can choose what output format in which to create the report: HTML, Microsoft Word, Microsoft Excel, comma-delimited text, or text. You can also select a report and view a previously generated version of it or generate a report on-demand.

Main Menu

The Main menu contains the following items:

File Menu

- *Generate Report.* Accomplishes the same functionality as mentioned for Reports in the “Tasks Area” on page 17.
- *New Profile.* Accomplishes the same functionality as mentioned for New Profile in the “Tasks Area” on page 17.
- *New Category.* Lets you create a new category folder in the selected Profile Type and/or selected category folder by opening the Category Name dialog box.
- *New Report.* Opens up the New Report wizard, in which you define the report range, report format, location at which to save the report, report style and report content for a new report template. This template gets added to the list of available reports, and may be used with an appropriate profile.
- *Rename.* Lets you rename the selected category folder or profile.
- *Schedule Event for Profile.* Accomplishes the same functionality as mentioned for Schedule Event in the “Tasks Area” on page 17.
- *Open File/Saved Report.* Lets you open an existing report through a Windows Explorer-like interface.
- *Close.* Closes the program window, but the application continues to run, including any scheduled reports and real-time analysis.
- *Exit and Unload.* Shuts down the application and any automated processes, including the Scheduler and real-time analysis.

Notes

Many Main Menu tasks are also available through right-click functionality.

Edit Menu

- *Profile*. Accomplishes the same functionality as mentioned for Edit Profile in the “Tasks Area” on page 17.
- *Cut*. Allows you to cut a profile or category folder, which can later be pasted in another folder or directly under the root of the Profile Descriptions list.
- *Copy*. Allows you to copy a profile, which you can rename and edit as needed.
- *Paste*. Lets you paste a profile that was previously cut. This is useful if you want to move a profile from one folder to another within the Profiles Description list.
- *Delete*. Accomplishes the same functionality as mentioned for Delete Profile in the “Tasks Area” on page 17.

View Menu

- *Collapse All Categories*. Collapses category folders to show just the folders, not the profiles contained within them.
- *Expand All Categories*. Expands all category folders so that you can see the profiles in each.
- *Select Columns*. Lets you choose which columns to hide or show in the Profile Description list.
- *Align Columns*. Adjusts columns to show the maximum amount of information possible per column.
- *Auto Refresh Profile List*. Updates the profiles list with the most current information.
- *Print Profile List*. Prints the list of profiles as it appears on-screen (expanded or collapsed).

Tools Menu

- *Scheduler*. Opens the Event Scheduler main console.
- *Style Editor*. Opens the Style wizard, which lets you change the style of a selected available report style, or lets you create a new report style and add it to the list of available report styles. The Style Editor lets you change the colors, fonts, descriptive text, graph appearances and more for the reports you generate.
- *FastTrends Maintenance*. Lets you manage the contents of the FastTrends database associated with a given profile.
- *URL Categorization (Outgoing Firewall Activity profiles only)*. Opens the URL Categorization Databases dialog box, which lets you register or update the SurfControl databases available for use with Firewall Suite. Use these databases to track Web surfing activity of inappropriate Web content.
- *Status of LEA Connections*. Lets you check the status of connections between the WebTrends LEA Service and a Check Point Management Server.
- *Limit Memory Usage*. Lets you to limit the number of elements included in a specific section of a report to reduce memory consumption.
- *Department Management*. Lets you create, edit or delete departments by IP addresses. This feature allows you to later report on the activity for a specific department, or to break down activity by departments.
- *Options*. Opens the Options dialog box, which controls global options as well as options that affect only the Firewall Activity or the Alerting & Monitoring module.

Links Menu

- *GeoTrends Information.* Links you to a Web page from which you may download GeoTrends, an optional, free database that provides location information about Web visitors and companies for your reports.
- *Customer Feedback.* Opens a Web page in which you may enter your comments about NetIQ's WebTrends brand of products.
- *Contact Technical Support.* Links you to the technical support page, in which you may enter any technical questions you have about Firewall Suite.
- *Frequently Asked Questions.* Links to a page of the questions most commonly encountered by technical support.
- *Purchase Technical Support.* Opens a page on which you can learn about and compare our three technical support packages.
- *Purchase Additional Licenses.* Links to a page from which you can purchase additional licenses for Firewall Suite. You may also use the contact information to order from a WebTrends sales representative or reseller.

Help Menu

- *Contents.* Opens the Firewall Suite online Help.
- *Add Serial Numbers.* Opens the dialog box in which you may enter the serial number for a Maintenance Subscription or a Server Add-On License.
- *Check for Product Updates.* Runs a utility that lets you know if your Firewall Suite version is most current available version. You must have registered your product for this utility to provide accurate information.
- *View Release Notes.* Opens the latest copy of the product Release Notes.
- *View Product License.* Displays the license agreement you accepted when you installed Firewall Suite.
- *About.* Displays information such as Firewall Suite Version number, the number of Firewall Add-Ons and more.

Functions Area

The Functions area contains the following items:

- *Scheduler*. Opens the Event Scheduler.
- *Options*. Opens the Options dialog box
- *Feedback*. Links to the Customer Feedback page (see “Links Menu” on page 21).
- *Help*. Opens the Firewall Suite online Help.

Profile Type Tabs

The Profile Type tabs include:

- *General Firewall Activity*. Report on security related issues including email activity, FTP transfers, and Telnet connections. You can also track bandwidth usage and VPN activity. Identify large data transfers, failed connection attempts by IP, the source that triggered firewall rules and other suspicious activity.
- *Outgoing Firewall Activity*. Pinpoint where the employees in your organization are going on the Internet and how much time they’re spending there. You can report on all the IP addresses to perform an organizational analysis, or focus on just one IP address to report on an individual’s activity.
- *Incoming Firewall Activity*. If your Web server is behind your firewall, use Incoming Web Activity profiles to report on traffic coming into your Web site, including the volume of activity on your site, where users are coming from, and what pages interest them most.
- *Alerting & Monitoring*. Monitor any networked or Internet-connected device or service and receive alerts whenever a device goes down or automate actions to take when specific events occur.

Reports Using a Sample Profile

In this section, you will use a sample profile included with the installation to create a report. Use the sample Incoming Firewall Activity profile called “Sample – Incoming”.

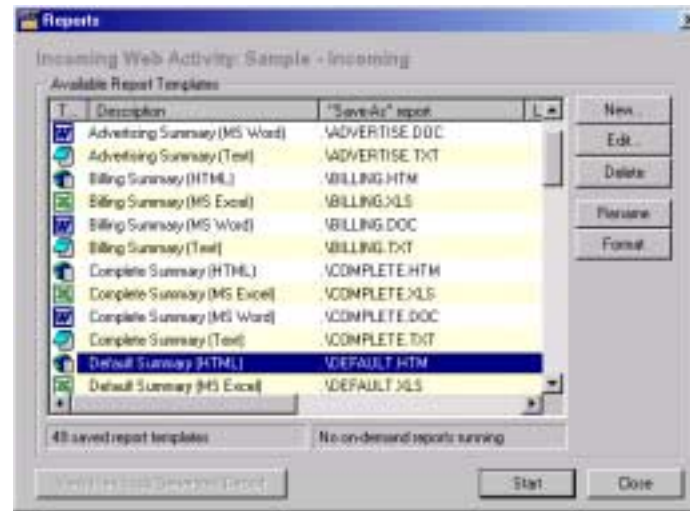
To create a report using the Sample – Incoming profile:

1. From the Main Console, click the **Incoming Firewall Activity** tab.
2. Select the profile called “Sample – Incoming”.
3. Review the profile’s settings by clicking **Edit > Profile** from the Main menu. The Edit Incoming Firewall Activity Profile dialog box opens.



4. Select any tab within the Edit Incoming Firewall Activity Profile dialog box to review the profile settings for the individual tabs. You can also modify profile settings within this dialog box. For more information about each setting in this dialog box, see “Firewall Profiles” on page 27.
5. Click **Cancel** to close the dialog box without making any changes.

6. Reselect the sample profile from the Profile Description list.
7. Generate a report for this profile by clicking **File > Generate Report** from the Main menu. The Reports dialog box opens.



For this example, just use the default settings for the report.

8. Click **Start** to generate the report. The report compiles and then opens.

Using Shortcuts

Firewall Suite includes a number navigational shortcuts.

Many Main Menu tasks are also available from the right-click menu. For example, to view a list of menu selections for a profile, select the profile in the Profile Description list and right-click. You can use right-click functionality to:

- Create a new category, profile, scheduled event or report.
- Edit a selected profile

- Generate a report
- Manage profiles.
- Collapse, expand, select, and align the columns in the Profile Description list.
- Print and refresh the profile list.
- Close or exit and unload the Firewall Suite application and its services.

In the Reports window, you can use right-click functionality to:

- Create, edit, rename, delete, start and format a report
- View a previously generated report
- Align and select columns
- Print a list of available reports

Chapter 3

Firewall Profiles

This chapter explains the various settings available for creating firewall and Web activity profiles. Firewall Suite produces a report on the data in your firewall or proxy server log files according to how these settings are configured. Profile settings specify:

- The hardware configuration of your firewall, which includes the firewall or proxy server and the computers behind your firewall.
- The location, format, and method for retrieving the log file data.
- The information from the log file you want to include in a report.
- The storage of log file analysis for future use.

Tables referenced in this chapter are included at the end of the chapter.

Alerting and Monitoring profiles use different settings. They are described in “Alerting and Monitoring” on page 103.

Notes

You may need to configure your firewall or proxy server before creating a firewall or Web activity profile. For more information, see the *Firewall Configuration Guide*.

Profile Types

The tabs in the Main Console correspond to the types of profiles you can create. These include:

- **General Firewall Activity.** Use these profiles to report on security-related issues, such as failed connection attempts by IP, firewall rules that were triggered, firewall warnings and errors and other suspicious activity. You can also track bandwidth usage, email activity, FTP transfers and Telnet connections.
- **Outgoing Firewall Activity.** Use these profiles to determine and generate reports on employee Internet surfing habits. In addition, these profiles let you report on all the IP addresses for an organization, or focus on just one IP address to report on an individual's activity.
- **Incoming Firewall Activity.** If your Web server is behind your firewall, use these profiles to report on traffic coming into your Web site from the outside, including the volume of activity on your site, where users are coming from and what pages interest them most.

Viewing a Sample Profile

Firewall profiles have numerous settings. Before creating a profile for the first time, it may be helpful to look at the settings for some of the sample firewall activity profiles included in your Firewall Suite installation.

- *Sample - General*, a General Firewall Activity profile for a firewall on a single computer.
- *Sample - General - Cluster*, a General Firewall Activity profile for a firewall configuration spread across multiple computers.
- *Sample - Outgoing*, an Outgoing Firewall Activity profile or a firewall on a single computer.
- *Sample - Incoming*, an Incoming Firewall Activity profile for a firewall on a single computer.

To view a sample profile:

1. On the Main Console, select any of the three firewall activity tabs, **General Firewall Activity**, **Outgoing Firewall Activity** or **Incoming Firewall Activity**.
2. Select the profile that you wish to view from the Profile Description list.
3. From the Edit menu, click **Profile**. The Edit Firewall Profile dialog box opens. Use this dialog box to review or make changes to the selected profile's settings by selecting the individual tabs associated with each profile.



Choosing a Firewall Profile Type

You need two pieces of information when deciding which of the three Firewall profile types to use to create the report you want.

- *The profile types supported by your firewall or proxy server.*

Note

Some firewalls and proxy servers do not support all the capabilities available with Firewall Suite. For more information about your firewall or proxy server, see the Firewall Configuration Guide.

For detailed information on designing Firewall Activity profiles, see “Designing Firewall Profiles” on page 99.

- *The log file information that you want to include in the report.* See “Report Content” on page 99 for more information about what content can be included in a report, how that information can be reported, and the profile type you should use to generate the report.

Creating a Firewall Profile

This procedure describes the sequence of panels in the New Profile wizard for creating a firewall profile. It describes the information required in each panel to set up a firewall profile. Refer to the online help in each panel for more information.

To create a new firewall profile using the New Profile wizard:

- 1.** Select a firewall profile type from the profile type tabs on the Main Console. Make your decision based on the type of firewall you have, and the type of information on which you wish to report.
- 2.** From the File menu or the Tasks area select **New Profile**. The New Profile wizard opens to the Firewall Configuration dialog box.

Firewall Configuration Dialog Box

The Firewall Configuration dialog box lets you specify whether your firewall is on one computer or distributed across multiple computers. A firewall or firewalls may be spread across multiple computers to distribute the work load for sites that experience high traffic volumes.

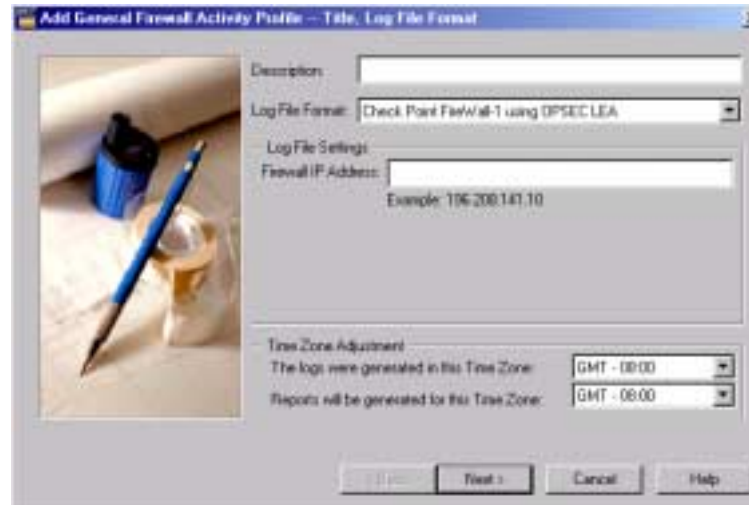


To specify your firewall configuration:

1. Choose one of the following two options depending on your circumstances:
 - *If your firewall resides on one computer*, select **My firewall is on one physical machine**.
 - *If your firewall resides on multiple computers*, select **My firewall is on multiple machines**.
2. Click **Next**. Depending on the selection you made in Step 1, the Title, Log File Format or the List of Servers dialog box opens. The next set of instructions will continue with creating a profile for a firewall on a single computer.
3. To continue creating a profile for a firewall on multiple computers, see “List of Servers Dialog Box” on page 40.

Title, Log File Format Dialog Box

If your firewall is on a single computer, use the Title, Log File Format dialog box to name the profile and specify the log file format and path. You also have the opportunity to use the built-in WebTrends Syslog Service, a Windows service that makes firewall log files accessible by converting them into a consistent log file format. For more information about the WebTrends Syslog Service, see “About the WebTrends Syslog Service” on page 37.



To specify the profile log file settings for a firewall on a single computer:

- 1.** In the **Description** text box, enter the name you wish to call your profile.
- 2.** In the **Logs were generated in this Time Zone** dropdown list, select the time zone, in comparison to Greenwich Mean time (GMT), in which the log files are generated. For example, if your firewall is located in the Pacific Time Zone, select **GMT -08:00** because this zone is eight hours behind Greenwich Mean Time.
- 3.** In the **Reports will be generated for this Time Zone** dropdown list, select the time zone for which reports for this profile will be generated. For example, while you may work in the Pacific Time Zone, the reports you generate may be destined for your Paris offices. Because Paris is one hour ahead of GMT, select **GMT +01:00**.
- 4.** In the **Log File Format** area, which lists the firewalls supported by the selected Profile Type tab, select the firewall type and the format of your firewall's log files.

Note

The options and fields available in the lower half of the dialog box vary depending on the format you select.

- 5.** *If you selected a Check Point firewall with OPSEC LEA*, skip to “Check Point LEA Instructions” on page 36.
- 6.** *If you are using any other firewall or log file format*, continue with the following steps.

7. If you want to use logs that are accessible by the Firewall Suite computer:

- a.** Select **The log files are already in a location accessible by this machine.**
 - b.** Select the firewall log file retrieval method from the dropdown list in the Log File Path area. For firewalls on a single computer, Firewall Suite supports `file:\\`, `ftp:\\` or `http:\\`. For more information on selecting the appropriate retrieval method, see “Log File Retrieval Methods” on page 38.
 - c.** Enter or browse to the location of your log file in the text box to the right of the log retrieval method. For more information on using Firewall Suite’s browse features, see “Specifying a Single Log File” on page 82 and “Specifying Multiple Log Files” on page 82.
- 8.** *If you want to use the WebTrends Syslog Service to collect your firewall log files, use the following steps:*
- a.** Enter the IP address of your firewall in the **Firewall IP Address** text box.
 - b.** Enter or browse to the location in which the WebTrends Syslog Service should save the collected log files in the **Save Log Files To** text box.

Check Point LEA Instructions

If you selected Check Point LEA, you must choose a Check Point OPSEC LEA connection to collect the data. Check Point LEA Connections are configured using the LEA Connection options under General Firewall Activity Options. Before you can configure a LEA connection, you must configure your Check Point firewall to work with OPSEC LEA. For more information, see the *Firewall Configuration Guide*.

If you are using a Check Point firewall with OPSEC LEA:

1. Make sure you selected the correct Check Point firewall type from the Log File Format list.
2. **If no connections have been configured**, click **Create or Manage Connections** to open the Manage Connections dialog box, and follow the instructions for creating a new OPSEC LEA connection on page “LEA Connections Dialog Box” on page 334.
3. **If one or more connections have been configured**, select a connection from the list.

About the WebTrends Syslog Service

Your firewall must be configured to use the WebTrends Syslog Service. Refer to the *Firewall Configuration Guide* for information about configuring your firewall.

Note

Because the WebTrends Syslog Service runs as a Windows service, you must run Firewall Suite on a Windows NT, Windows 2000, or Windows XP system and you must have administrator rights to configure Firewall Suite as a Windows service.

To make firewall log files accessible in a consistent log file format, the Syslog daemon of the WebTrends Syslog Service collects firewall log data from the firewall. The daemon then writes a log file in a usable format to an IP address on the computer running Firewall Suite. The log files created by the WebTrends Syslog Service are stored locally on the computer running Firewall Suite, and log files created by the firewall remain there.

The WebTrends Syslog Service standardizes the prefix of the firewall log records. In the following example, the part of the firewall record that is formatted by WebTrends Syslog Service appears in bold:

```
WTsyslog [2001-11-01 00:31:41 ip=192.168.9.1 pri=6] 304001
192.168.10.20 accessed URL 192.9.24.116:template/sunstyle.css
```

By default, the WebTrends Syslog Service is bound to the IP address on the computer running Firewall Suite where it writes log data. If the computer running Firewall Suite has more than one IP address, WebTrends Syslog Service binds to all IP addresses by default. We recommend that you do not bind the WebTrends Syslog Service to a single IP address unless absolutely necessary.

You can select the frequency with which log files are rotated in the Syslog dialog box of the General Firewall Activity section of the Options window. Log files are rotated when the current log file is archived and a new log is started.

Because the WebTrends Syslog Service collects data in real time, up-to-date logs are available for reporting. If the WebTrends Syslog Service is not running, however, any log data generated is lost.

When you create a profile that uses the WebTrends Syslog Service, the server is configured to start whenever the computer running Firewall Suite is started. The WebTrends Syslog Service will continue to run as long as the computer is running.

Log File Retrieval Methods

Firewall Suite supports the following retrieval methods:

- **file:///** (file retrieval). Select this option if you have a drive mapped to your firewall server. You can identify single, multiple, and compressed log files in one of three ways:
 - Type the complete log file path in the **Log File URL Path** text box.
To specify multiple log files, use wildcards or use a vertical bar (|) between log file path names. For more information, see “Specifying Log Paths” on page 351.
 - Click **Normal Browse** to browse to the location of a single file.

- Click **Extended Browse** to open the Selected Logfiles dialog box and specify multiple log files. See “Specifying a Single Log File” on page 82 and “Specifying Multiple Log Files” on page 82 for instructions and examples.
- **ftp://** (FTP retrieval). Select this option to retrieve your log file using FTP.
 - a. Type the path and file name in the **Log File URL Path** text box, or click **Browse** to navigate to the log file location. When you specify an FTP URL, you must type the full path from the root of the FTP server.
 - b. Type your user name and password for the FTP site.
- **http://** (HTTP retrieval). Select this option to retrieve your Web server log file over the Internet using HTTP.
 - a. Type the path and file name in the **Log File URL Path** text box.
 - b. If you are accessing a secure Web site, type the user name and password information. This is usually not required to access a Web server.

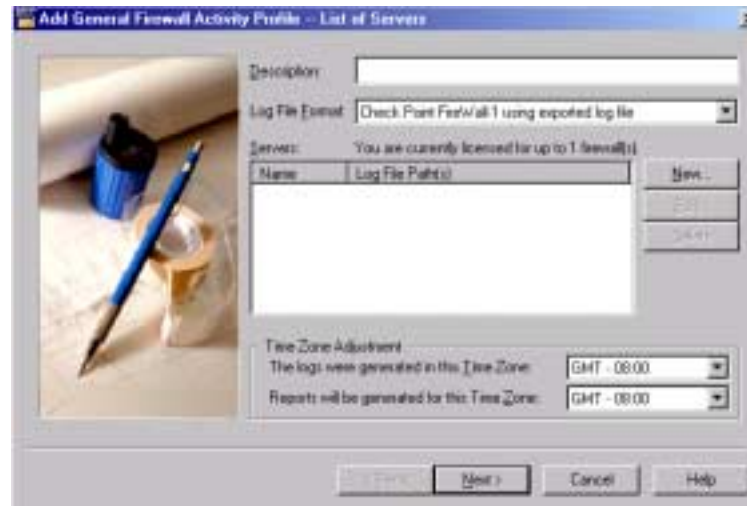
See “Specifying a Single Log File” on page 82 and “Specifying Multiple Log Files” on page 82 for detailed instructions on using the browse features associated with each log retrieval method.

Note

ftp and http retrieval are only available for firewalls that use single servers. Clustered servers are assumed to have log files aggregated and stored in a single file location.

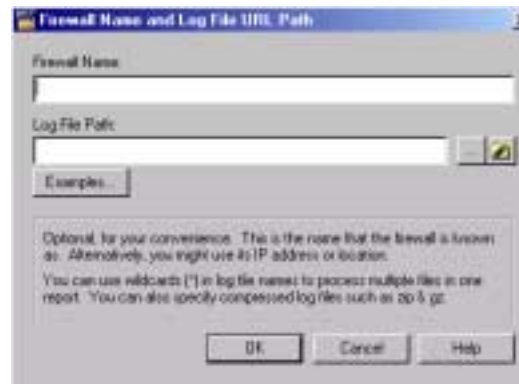
List of Servers Dialog Box

The settings in the List of Servers dialog box parallel the Title, Log File Format dialog box for firewalls on single servers, only they pertain to firewall configurations that have firewalls and log files on multiple servers. This may occur when network traffic is heavy, and firewalls need to spread the workload to multiple computers.



To specify the profile log file settings for a firewall on multiple computers:

1. In the **Description** text box, type the name you wish to call your profile.
2. In the **Logs originate in Time Zone GMT** dropdown list, select the time zone, in comparison to Greenwich Mean time (GMT), in which the log files are generated. For example, if your firewall is located in the Pacific Time Zone, this setting is eight hours behind Greenwich Mean Time, so you would select **GMT -08:00**.
3. In the **Report in GMT** dropdown list, select the time zone for which reports for this profile will be generated. For example, while you may work in the Pacific Time Zone, the reports you generate may be destined for your Paris offices, which is one hour ahead of GMT. Therefore, select **GMT +01:00**.
4. In the **Log File Format** area, which lists the firewalls supported by the selected Profile Type tab, select the firewall and log file type of your firewall configuration.
5. Click **New**, to add a server and the path to a log file or files for that server. The Firewall Name and Log File Path dialog box opens.



6. In the **Firewall Name** text box, type the name for your firewall.

7. In the **Log File Path** text box, either type or browse to the location of the log file(s) for that firewall.

Note

Use wildcards (*) in log file names to process multiple log files in one report. You can also specify compressed log files such as zip or gzip.

8. Click **OK** to return to the List of Servers dialog box. The new server and path is added to the Servers list.
9. Click **Next**. The IPs Behind Firewalls dialog box opens.

Editing the Server List

To edit a server in the list:

1. In the **Server** list, select the server you wish to edit.
2. Click **Edit**. The Firewall Name and Log File URL Path dialog box opens.
3. Edit the server settings as needed and click **OK**.

Deleting a Server from the List

To delete a server from the list:

1. In the **Server** list, select the server you wish to delete.
2. Click **Delete**. A confirmation message displays.
3. Click **Yes** to confirm the deletion. The selected server is deleted from the list.

IPs Behind Firewall Dialog Box

The IPs Behind Firewall dialog box allows you to specify the IP addresses or domains of computers located behind your firewall. The information in this dialog box tells Firewall Suite which computers are behind your firewall so it can distinguish between activity that originates inside the firewall (in other words, from within your organization) and activity that originates outside.



Adding an IP Address

To add an IP address to the list:

1. Enter an IP address or domain name in the text box above the **Add** button.

Note

You can use wildcards (*) to specify a group of IP addresses or domain names. For example, type 192.168.* to indicate that all addresses that begin with 192.168. are behind the firewall. Type the domain name *.webtrends.com to add all computers on the webtrends.com domain to the list. Adding *.webtrends.com includes all computers on internal.webtrends.com and pdx.webtrends.com.

2. Click **Add**. The contents of the text box are added to the list.
3. Click **Next**. The DNS Lookup dialog box opens.

Removing an IP Address

To remove an IP address or domain name from the list:

1. Select an IP address or domain name in the list.
2. Click **Remove**. The selected item is deleted from the list.

Selecting or De-selecting an IP Address

To select or de-select all IP addresses or domain names from the list:

- Click **Select All** to select all items in the list
- Click **Un-select All** to deselect any selected items in the list.

Internet Resolution Dialog Box

DNS lookup is the process of translating numeric IP addresses into domain names. Most users consider domain names more useful for analysis and reports than IP addresses; however, IP resolution can be a slow process, and for this reason, you may choose to not use this capability.

In general, DNS lookups are performed more efficiently by the firewall or proxy server as the log is created, rather than during log file analysis by Firewall Suite. If your firewall or proxy server does not perform DNS lookups or your administrator has disabled that capability, Firewall Suite can do it for you.

The Internet Resolution dialog box allows you to choose whether or not to perform DNS lookup for the current profile. Resolving IP addresses into domain names takes a large amount of processing power the first time, but once resolution has occurred, the results are stored in a profile-specific DNS cache that is readily and quickly accessed for future analyses with the profile.

Note

If multiple profiles refer to the same IP address, they may all share the same DNS cache rather than perform the same DNS resolution for each profile.



Specifying Settings for DNS Lookup

Depending on the Resolution mode and/or cache settings you choose, you may be required to fill in or choose additional settings.

To specify settings for DNS lookup:

1. In the **Domain Name/IP Resolution Mode** dropdown list, select one of the following options:
 - **Quick mode.** Uses the format from the log file. In this mode, Firewall Suite does not perform DNS lookups, but maintains the address in its original state in the log file. This is the fastest method for creating reports. If you select this mode, **Cache Control** is grayed out in the dialog box.
 - **Resolve mode.** Does a lookup for all numeric IP addresses. Select this option if your firewall or proxy does not perform DNS lookups and you need geographic or other domain-related information.
 - **Auto mode.** This is the best method to use if you don't know whether you log file contains IP addresses or domain names, but you want domain names in your analyses. In Auto mode, Firewall Suite examines the first record in the log. If the first record contains an IP address, it attempts to translate all IP addresses. If the first record contains a domain name, it turns on Quick mode.

2. In the **Cache Control** area, select how and where you want the results of the IP address resolution to be stored. Cache Control settings allow you to load the DNS cache in the Firewall Suite default location and/or store it in a custom location of your choice. Choose one of the following two options:

- **Load DNS cache in memory.** Places the DNS cache in a profile-specific default location. The DNS cache is made up of two files, dnscache.din and dnscache.dtx. The default storage location uses the profile's file name when creating the storage path for these two files. For example, with the profile:

```
install_dir\wtm_FirewallOther\datfiles\0000dc.fir
```

the DNS cache files are:

```
install_dir\wtm_FirewallOther\datfiles\0000dc.dns\dnscache.din
```

```
install_dir\wtm_FirewallOther\datfiles\0000dc.dns\dnscache.dtx
```

- **Store DNS Cache in custom location.** Places the DNS cache files in a location of your choice. Type or browse to the location.

3. Click **Next**. If this profile is for:

- General Firewall Activity, the Filters dialog box opens.
- Outgoing Firewall Activity, the Categories dialog box opens.
- Incoming Firewall Activity, the Home Page dialog box opens.

Clearing the DNS Cache

You can clear the DNS cache for the current profile to dispose of unresolved or out-dated entries. The cache repopulates when the next DNS lookup is performed.

To clear the DNS cache:

Click the **Flush DNS Cache** button.

Sharing the DNS Cache

You can share a DNS cache among multiple profiles by choosing the **Storing the DNS cache in custom location** option, and pointing each profile to that custom location.

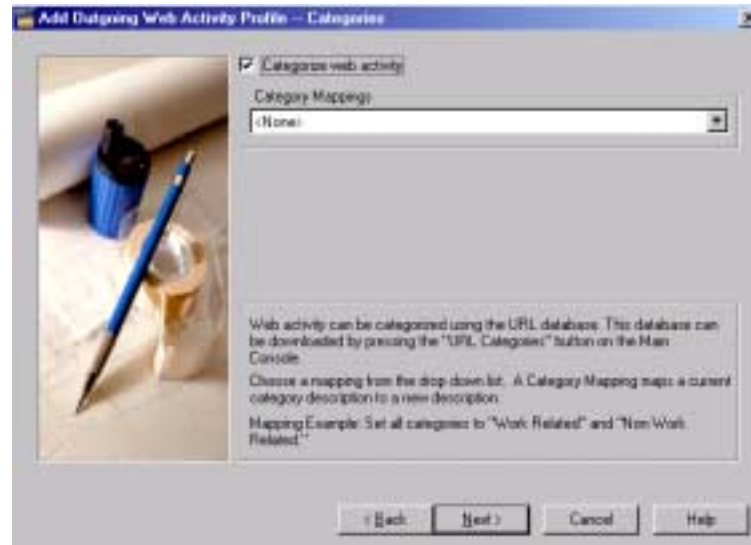
URL Categorization

With Outgoing Firewall Activity profiles, Firewall Suite provides access to databases from SurfControl. These databases list Internet URLs that may expose the organization to legal liability, detract from employee productivity, or waste bandwidth. Firewall Suite uses a modifiable `.ini` file to map these Internet URLs to categories such as Hate Speech or General News. The software can then track and report on the categories of Internet content that individuals in your organization access to ensure that employees do not visit inappropriate Web sites.

The Firewall Suite software includes the SurfControl categorization engine that licenses and accesses the categorization databases. Once you have downloaded the databases and activated URL Categorization, you can create profiles with filters to track the scope and nature of Internet usage in your organization.

Because Web sites change and new Web sites are continually being added, you can update the database periodically to obtain access to the most current list of sites.

Use the Categories dialog box to enable categorization and assign either the default category mapping, or a custom mapping you have created.



Choosing Settings for Categories

To choose settings for Categories:

1. In the Categories dialog box, click **Categorize web activity** to enable URL categorization.
2. In the **Category Mappings** dropdown list, select the type of category mapping you wish to use.
3. Click **Next**. The Filters dialog box opens.

Note

You can create your own categories by assigning the existing categories new names and associating them with one of the two major category types, Core or General. See “Mapping URL Categories” on page 57 for information about creating your own category names.

Category Types

The Firewall Suite installation includes a Core Categories database. Core Categories include Web sites that contain objectionable content that may result in liability issues. You can purchase a separate license to download a General categories database that contains content believed to reduce employee productivity.

Core Categories

The Core categories database includes URLs of Web sites with the following types of content:

- Adult/Sexually Explicit
- Criminal Skills
- Drugs, Alcohol & Tobacco
- Gambling
- Hacking
- Hate Speech
- Violence
- Weapons

General Categories

Firewall Suite's General Categories database contains the following additional categories of URLs that, while not objectionable, reduce employee productivity:

- Advertisements
- Arts & Entertainment
- Chat
- Computing & Internet
- Education
- Finance & Investment
- Food & Drink
- Games
- Glamour & Intimate Apparel
- Government & Politics
- Health & Medicine
- Hobbies & Recreation
- Hosting Sites
- Job Search & Career Development
- Kids Sites
- Lifestyle & Culture
- Motor Vehicles
- News
- Personals & Dating
- Photo Searches
- Real Estate
- Reference
- Religion
- Remote Proxies
- Search Engines
- Shopping
- Sports
- Streaming Media
- Travel
- Usenet News
- Web-based Email
- Sex Education

Updating the URL Categorization Database

Because the database is frequently updated to provide more relevant reports, use the URL Categorization Database dialog box to check the status of your database and update it when necessary. A good rule of thumb is to update the database monthly.

Note

If you are accessing the Internet through a proxy server, you must provide your proxy connection settings before you can update the database. See “Proxy Server Settings” on page 59.

To determine whether your database needs updating:

1. Select **URL Categorization** from the Tools menu. The URL Categorization dialog box opens.
2. Review the information in the **Database Information** area at the bottom of the dialog box. The Status tells you whether or not the database is up to date.

To update your database:

1. Select **URL Categorization** from the Tools menu. The URL Categorization dialog box opens.
2. Click **Update Database**. The Update URL Database dialog box opens.
3. Click **Get Update**.

Incorrect Categorization of IP Addresses

When a single IP address hosts multiple sites, visits to any site hosted by that address can be mis-categorized. For example, the same IP address may host both a sexually explicit site and a news site. If a person visited the news site, reports may incorrectly categorize the visit as one to a sexually explicit site. You can avoid this problem of mis-categorization by not categorizing IP addresses.

To disable categorization of IP addresses:

1. Select **URL Categorization** from the Tools menu. The URL Categorization Databases dialog box opens.
2. Select the **Do not categorize IPs** check box.

System Performance and URL Categorization

URL categorization will categorize all file types unless you specify otherwise. In most cases, you only need to categorize document file types, which you specified in the File Types dialog box. These typically include files with .htm, .html, .asp, .txt, and similar extensions. Access the File Types dialog box by clicking **Tools > Options> General Firewall Activity > File Types**.

By only categorizing document file types, you significantly improve system performance because Firewall Suite does not have to categorize every file.

To improve system performance for URL categorization:

1. Select **URL Categorization** from the Tools menu. The URL Categorization dialog box opens.
2. Select the **Only categorize documents** check box.

Licensing the URL Categorization Database

When you install Firewall Suite, you install a sample database. A full Firewall Suite license lets you update the database as many times as you like.

Mapping URL Categories

You can create new mappings for your standard URL categories to create URL categories that help your reports answer the questions you need to answer. For example, to see whether employee Web surfing activity is for work-related or non-work-related purposes, you can use the pre-defined Work Mappings setting, which assigns the pre-defined categories to either the Work-Related or Non-Work-Related mapping. Individual categories such as Sexually Explicit or Hate are not shown, but visits to these categories are shown under the mapped categories.

Each category is made up of two elements:

- *Category Type*. Core or General. Reports are broken down by Core or General categories. For example, among the many URL categorization reports possible, you can generate a Most Popular Core Categories graph and table, a Users Visiting Most Popular Core Categories table and a General Categories Visited by Most Active Users table.
- *Category Name*. For example, Sexually Explicit, Hate Speech, Entertainment, General News. These names can be changed into names that are more meaningful for the user's or organization's reports.

Note

For a complete list of Category Names, see “Core Categories” on page 53 and “General Categories” on page 54.

Category mappings are defined in the `urlcatmap.ini` file, which is located in the `install_dir\wtm\Firewall\weboutdirectory`. If this file is empty, no mappings are available in the Category Mappings list.

An Example of Mapped Categories

Firewall Suite includes one preconfigured alternate mapping called *Work Mappings*, which can be selected from the Category Mappings dropdown list. View this mapping by navigating to and opening the `urlcatmap.ini` file from the above location. Firewall Suite includes one pre-defined category mapping, Work Mappings. By default, this mapping maps all SurfControl categories to the category type "General" and the category "Non Work Related." You can modify this mapping in the `urlcatmap.ini` file to change the way it maps categories.

Remapping Syntax

Add new mappings to the `URLcatmap.ini` file. Each mapping must be a separate block of code from any other mapping code. You can add it at the top of the `.ini` text file or at the very end of any text in the `.ini` file. The order of the mappings in the `.ini` file determines their order in the Category Mappings dialog box.

Each new mapping must have a new mapping name. For example, the Work Mappings settings are initiated by the mapping heading:

```
[work Mappings]
```

Category type and name changes can be assigned as follows:

```
Category Type, Category Name = New Category Name, Reassigned Category Type
```

or

```
Category Type, Category Name = New Category Name
```

The order of Category Type and Name are reversed on the right side of the equals sign in syntax example 1. In example 2, the Category Type will not be reassigned, only the Category Name will be changed--an example of this is shown in the

```
General, Chat = Non Work Related
```

mapping on the second line of the sample mapping excerpt from the `URLcatmap.ini` file.

Reporting with URL Categorization

The reports that you generate can include tables and graphs showing the most active authenticated users, non-authenticated users, and host names or IP addresses connecting to the proxy server. Of the categorized sites most visited, you can list the number of users that visit a site; the names of the categories of visited sites; the number of hits on each site; the number of user sessions; the amount of time visitors spent at a site; and the amount of data (in KB) that was downloaded.

You can generate a report for all activity related to categorized sites, or you can create filters to limit reports to specific categories or category mappings. For instruction on including or excluding categories of outgoing activity, see “Filters Dialog Box” on page 66, “Working with Filters” on page 160, and “Category” on page 169.

Proxy Server Settings

If you connect to the Internet via a proxy server, you will need to provide your proxy connection settings in order to update the database.

To provide your proxy connection settings:

1. On the Main Console, select **Tools > Options** from the Configure menu or click **Options** in the Functions area.
2. Click **Main Options**.
3. Select the **Access to Internet** option.
4. Select the **Connect through a Proxy Server** check box and type the address of the proxy server and the port.
5. Choose one of the following options:
 - ***If your access requires authentication***, select the **HTTP access requires a User Name/Password** and type the user name and password for your proxy server.

- *If your access does not require authentication*, clear the check box.

6. Click **OK**.

Category Names

The Category Mappings choice selected in the URL Categorization Databases dialog box determines which Category Names are available for the selected profile. You can see which Category Names are available from the Include Filter and Exclude Filter dialog boxes.

For instruction on including or excluding categories of outgoing activity, see “Filters Dialog Box” on page 66, “Working with Filters” on page 160 and “Category” on page 169.

To view the category names available for a selected profile:

1. While editing an existing profile or creating a new one, open the Filters dialog box.
2. Either edit an existing filter or create a new one
3. Select **Include/Exclude activity based upon**.
4. Choose one of the following:
 - *If you are editing an existing filter*, select the **Category** check box and select the **Category** tab.

– ***If you are creating a new filter***, click **Next**. The Category dialog box opens.

5. Click **Examples** to see a list of available Category Names available for using with category filters.



Interpreting Categorization Reports

The categorization feature is powerful, and the reports, when interpreted properly, can point to Web abuse and possibly head off potential litigious issues. However, there are some aspects to Internet technology that require caution when interpreting categorization reports.

Some Internet providers and Web hosting services host several Web sites on a single server. These Web sites are referred to as virtual Web sites. For such sites there are at least two host names: the host name of the virtual Web site itself and the host name of the server. The host name used for URL Categorization depends on how your firewall or proxy server records this information. If both are recorded, the virtual host name is categorized and the server host name is understood to belong to that category. This may mean that a server computer can trigger a “core category” ranking because it hosts a virtual Web site that is registered as objectionable. Thus, a visit to an innocuous site on that server will also trigger the “core category” ranking.

Ads or other embedded objects on a page may be served up by a totally different site from the page itself. The page may be registered as an objectionable site when it is the site serving up the ad that is objectionable. This is complicated when ads come from sites on virtual servers.

Note

The table “Core Categories Visited by Active Users” can be misinterpreted. It does not list the top offenders of the Core Categories, but rather lists a breakdown of the Core sites visited by the Most Active Users.

With page title retrieval turned on, the analyzing host may register as hitting the objectionable sites found by the analysis.

To maximize the usefulness of the information in reports, look carefully at the KB transferred, at the number of hits, and of course, visit pages to judge the content for yourself.

Before any action is taken to warn an employee about potential misuse, it is highly recommended that the URLs in question be double-checked for their content and appropriateness.

Home Page Dialog Box

With Incoming Firewall Activity profiles, you can use the Home Page dialog box to obtain accurate data about hits to your home page(s). Home pages are the pages a Web server defaults to when the user requests a URL without a specific file name. For example, if a user requests:

```
http://www.webtrends.com/
```

and `index.htm` is the home page for the uppermost level of the site, the Web server delivers:

```
http://www.webtrends.com/index.htm
```

Similarly, if the user requests:

```
http://www.webtrends.com/reports/incoming
```

and `default.htm` is the home page for that directory, the Web server delivers:

```
http://www.webtrends.com/reports/incoming/default.htm
```

Both `index.htm` and `default.htm` are home pages for the site (though for different directories), so if you wish to accurately count the number of hits to home pages, specify any file names used as home pages for the entire site. The specified paths and file names are shown in Firewall Suite reports.

You may also wish to specify multiple home page file names when a home page file name changes, but you still want to perform analysis on log files created before and after the name change. For example, if the home page for `www.webtrends.com`, `default.htm`, was changed to `index.htm`, but you wanted to report on hits to both the new and old home page file names.



To specify the home page:

1. In the **Home Page File Names** text box of the Home Page dialog box, type the home page file names that the Web server defaults to when a visitor requests a URL without a specific file name. The most common filenames are provided by default.
 - Separate multiple file names with spaces.
 - You can type up to 255 characters.
2. Specify your Web site URL using the entire path from the root of your site. Do not include your default home page file name.
 - ***If you access your Web site from a mapped drive or by using a Universal Naming Convention (UNC) name to identify a shared file***, select **file:///** from the dropdown list and type the URL path or browse to it. For example, type `c:\inetpub\wwwroot\`.
 - ***If you access your Web site by FTP***, select **ftp://** and type or browse to the location of the site. For example, type `ftp.isp.com/~user`. If required, provide a user name and password.
 - ***If yours is an HTTP site***, select **http://** and type your Web site URL, for example `www.domain.com/`. If authentication is required, click **HTTP access requires User Name and Password** and provide user name and password. This is not usually required.
3. Click **Next**. The Filters dialog box opens.

Filters Dialog Box

Filters focus the contents of a report by including only the data you want to analyze. You can use filters that include data based on defined criteria, and you can use filters to exclude data based on defined criteria. Because filters are such a powerful tool, they are discussed in their own chapter. See “Filtering for Focused Reports” on page 157 for detailed information about filters, and how to add, delete, edit, copy and combine them.

You can create a profile without using any filters. By default, this means that all log file data is included in the log file analysis.

Use the Filters dialog box to create, edit, copy and delete filters.



Creating a Filter

To create a filter:

1. In the Filters dialog box, click **New** to create a new filter using the New Filter wizard.



2. Select one of the following options:
 - **Include** to include Web site activity that meets the selected criteria in your analysis and reports.
 - **Exclude** to exclude the Web site activity that meets the selected criteria in your analysis and reports.
 - **Copy of another filter** to copy an existing filter from a list of existing filters for the selected profile type and edit it as needed.
3. Click **Next**.
4. **If you selected** *Copy of another filter*, select the filter you wish to copy and click **Next**.
5. **If you selected** *Include or Exclude*, type a name for the filter in the text box and click **Next**.

- 6.** Click **Include/Exclude activity based upon**.
- 7.** Select any filter elements you wish to include or exclude from your log file analysis and reports.
- 8.** Click **Next**. The dialog box for the first filter element you selected opens.
- 9.** Fill in the settings for the filter element dialog box.
- 10.** Click **Next** and continue to fill in the settings for the remaining selected filter elements. For more information, review “Filter Basics” on page 157.
- 11.** Click **Next**. The Database and Real-Time dialog box opens.

Editing a Filter

To edit a filter:

- 1.** In the Filters dialog box, select the filter you wish to edit from the filters list.
- 2.** Click **Edit** and edit the filter as needed. See “Filter Elements” on page 164 for a list of filter elements. See “Filter Element Descriptions” on page 166 for a full description of each filter element.
- 3.** Click **OK**.

Deleting a Filter

To delete a filter:

- 1.** In the Filters dialog box, select the filter you wish to delete from the filters list.
- 2.** Click **Delete**. A confirmation message displays.
- 3.** Click **Yes** to confirm the deletion. The filter is now deleted.

Copying and Pasting a Filter

To copy and paste a filter:

1. In the Filters dialog box, select the filter you wish to copy from the filters list.
2. Click **Copy**.
3. Click **Paste**. A copy of the filter is placed in the list with the name “Copy of filter name”.
4. Select and edit the copied filter as needed.

Bandwidth Cost Dialog Box

Use the Bandwidth Cost dialog box to specify the cost of service for each kilobyte of data transferred for General Firewall Activity profiles. The information collected in the Bandwidth Usage report chapter includes the number of events, the percent of total events, the kilobytes transferred, and the cost of bandwidth used by top user addresses, outgoing protocols, and incoming protocols.

Firewall Suite calculates and reports the cost of bandwidth usage for all types of incoming and outgoing Internet activity. Bandwidth cost is calculated by multiplying the Cost of Bandwidth per Kilobyte you supplied by the number of kilobytes transferred. All firewall events that log a value for kilobytes transferred are included. Typically, firewalls log this value for events associated with a protocol.

To report on bandwidth cost accounting, you must include the graphs and tables for Top Users by Bandwidth Utilization, Outgoing Protocol Usage and Incoming Protocol Usage.



Specifying Bandwidth Cost

To specify the bandwidth cost:

1. In the **Currency** dropdown list of the Bandwidth Cost dialog box, select the currency to use when calculating bandwidth cost.
2. In the **Cost of Bandwidth per Kilobyte** text box, enter the cost per kilobyte transferred.

Database and Real-Time Dialog Box

The Database and Real-Time dialog box allows you to activate the FastTrends™ database and use real-time analysis when analyzing that data. Both features are useful for speeding up analysis and reporting, especially if your firewall generates large amounts of data.



FastTrends Database

Using the FastTrends database allows Firewall Suite to store analysis results in a cache. Because the cached data is more accessible, Firewall Suite can perform more efficient future analysis and report generation on the current profile. For example, if you activate the FastTrends database option and generate a report on Monday, Firewall Suite stores the data in the FastTrends database. If you run a report on the same profile for Monday *and* Tuesday, only the data for Tuesday needs to be analyzed.

Real-Time Analysis

Firewall Suite's real-time analysis feature can keep your log file analysis as current as possible. Real-time analysis enables Firewall Suite to monitor log files at regular intervals and check for any new activity. If new activity is found, then FastTrends analyzes the new data in the background, and stores the analysis results in the FastTrends database.

Real-time analysis is useful if your firewall generates unusually large amounts of data and initial analysis of an entire log file would take a significant amount of time. By collecting and analyzing log file information at regular intervals, when an analysis and reporting event kicks off, only the new log file records will need to undergo analysis before a report can be generated.

To specify settings for the FastTrends database and real-time analysis:

1. To store the results of log file analysis in a database to use for future reports, select the Use FastTrends Database checkbox. . The default location of the FastTrends database is
InstallDir\wtm_FirewallOther\datfiles\profile_name.dat.

Use the Advanced FastTrends tab (enabled when you activate FastTrends) to specify a location for the database different from the default location

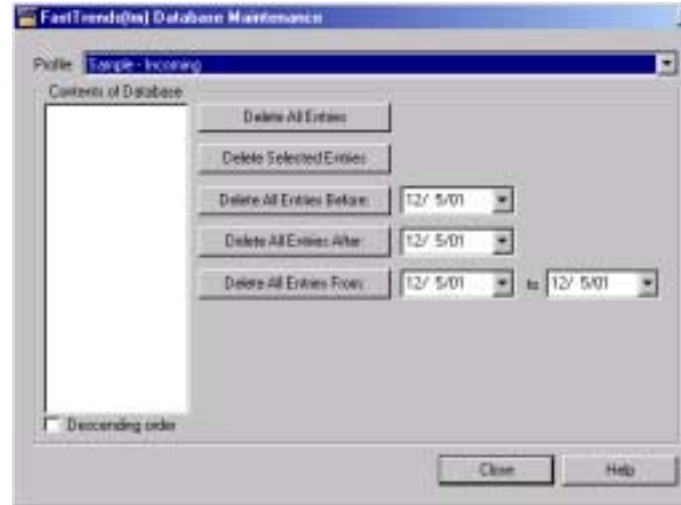
2. Select or clear the **Analyze log files in real-time** check box to determine whether log files are analyzed in real time. For more information on real-time analysis, see "Advanced FastTrends Dialog Box" on page 76.

Maintaining the FastTrends Database

You may need to manage the amount of data in your FastTrends database to free up available space.

To maintain the FastTrends database:

1. On the Main Console, select the profile type tab containing the profile for which you want to perform FastTrends database maintenance.
2. On the Main Console, select **Tools > FastTrends Maintenance**. The FastTrends Database Maintenance dialog box opens.



3. From the **Profile** dropdown list, select the profile for which you want to perform FastTrends database maintenance. The **Contents of Database** list shows all the FastTrends database entries by date.

The **Contents of Database** list may be sorted in ascending or descending order. Select the **Descending order** check box to sort in descending order. Clear the check box to sort in ascending order.

4. Delete entries from the list using one of the following buttons:
 - Click **Delete All Entries** to delete all entries in the list.
 - Click **Delete Selected Entries** to delete a selected entry from the list.
 - Click **Delete All Entries Before** to delete all entries before a specified date.
 - Click **Delete All Entries After** to delete all entries after a specified date.
 - Click **Delete all Entries From** to delete all entries between two user-specified dates
5. Click **Close**.

Notes

If you make changes to a profile, for example by using a different log file, changing DNS Lookup settings, or modifying the filters, clear the database and rerun the analysis to store the correct data in the database.

If you turn off FastTrends, clear the database to free up disk space.

Advanced FastTrends Dialog Box

This dialog box is shown only if you activated FastTrends database in the Database and Real-Time dialog box. The Advanced FastTrends dialog box lets you specify a database location other than the default location.

Storing FastTrends data in a location other than the default can save space on your local computer; however, it can slow down processing.



To specify an alternate data storage location:

1. Clear the **Store FastTrends databases in default location** check box.
2. Type the path and directory for the new location in the **Alternate Location** text box, or use the browse button to navigate to the new location.
3. Click **Finish**.

Setting Up Syslog Dialog Box

The Setting Up Syslog dialog box is the last dialog box you will see when setting up a profile that uses the WebTrends Syslog Service.

If you have not already configured your firewall to send its log files to the WebTrends Syslog Service, you will need to do so. The *Firewall Configuration Guide* contains specific information for your firewall.



To finish setting up your profile:

1. Write down the IP Address or addresses you find at the bottom of the Setting Up Syslog dialog box. These are the addresses on the computer running Firewall Suite to which the WebTrends Syslog Service is bound.
2. Click **Finish**.

Editing a Profile

You can edit an existing profile in the Edit profile window.

To edit an existing profile:

1. On the Main Console, select the profile that you want to change in the Profile Description list.
2. Select **Edit > Profile** from the Main menu, or **Edit Profile** on the Tasks area. The Edit Firewall Activity Profile window opens.



3. View the current settings for the profile by selecting the tabs at the top of the window to open the associated dialog box. The tabs correspond to the dialog boxes used in the New Profile wizard. See “Creating a Firewall Profile” on page 31 for more information on the settings for each tab. Make any needed changes to the settings.
4. Click **Cancel** to close the window without saving any changes, or click **OK** to save your changes and close the window.

Copying a Profile

You can create a new profile based on existing profile settings. This may be useful if many of the settings in the existing profile are needed in the new profile.

To copy a profile:

- 1.** On the Main Console, select the profile you want to copy and modify from the Profile Description list.
- 2.** Select **Edit > Copy Profile** from the Main menu. The Edit Firewall Activity Profile window opens.
- 3.** Select the **Title, Log File Format** or **List of Servers** tab, and then type a name for your new profile in the Description text.
- 4.** Select other tabs as needed, making any necessary changes. Use the scroll arrows in the upper-right corner of the window to access all of the tabs
- 5.** Click **OK** to save the new profile and its settings.

Deleting a Profile

If you have profiles that are no longer needed, you can delete them.

To delete a profile:

- 1.** On the Main Console, select the profile that you want to delete from the Profile Description list.
- 2.** Click **Edit > Delete** from the Main menu or **Delete Profile** from the Tasks area. A confirmation message displays.
- 3.** Click **Yes** to confirm the deletion. The profile is deleted.


Specifying Log Files

When creating or editing a profile, you can specify single or multiple log files using the browse buttons in the Log File Path section of the Title, Log File Format dialog box. This section discusses how to browse for log files and how to specify multiple logs using date macros or wildcards. For most firewalls, you will see the dialog box shown below.



Specifying a Single Log File

To specify a single log file:

1. In the Title, Log File Format dialog box, click the browse button .
2. Navigate to the directory with the log file.
3. Select the file, and click **Open**.

Note

You can specify compressed logs, such as .zip or .gz files.

4. Click **Next**.

Specifying Multiple Log Files



Firewall Suite provides you with a number of ways to select multiple log files:

- Using a browser
- Using wildcards to select log files with similar names
- Using date macros to select log files that have dates as names

Multiple log files are specified using the Selected Log Files dialog box.




To add files using the browser:

1. Choose one of the following two options:
 - **Firewall on single machine.** Click the extended browse button  on the Title, Log File Format dialog box. The Selected Logfiles dialog box opens.
 - **Firewall on multiple machines:**
 - a. Click New in the List of Servers dialog box to open the Firewall Name and Log File URL Path dialog box.
 - b. Click the extended browse button . The Selected Logfiles dialog box opens.
2. Click **New**.
3. Navigate to the directory that contains the log file. Select the log file.
4. Click **OK** to add the file to the File Specification and Log File List.

5. Repeat to add additional files.
6. Click **OK** to return to the Title, Log File Format dialog box.


To add files using wildcards:

1. On the Title, Log File Format dialog box, click the extended browse button . The Selected Logfiles dialog box opens.
2. Click **Wildcard**. The Wildcard dialog box opens.



3. Select the directory that contains the log files.
4. In the **Wildcard Specification** text box, type the log file path names or file names using * or ?. See "Specifying Log Paths" on page 351 for examples.
5. Click **OK** to add the files to the File Specification and Log File List.
6. Click **OK** again to return to the Title, Log File Format dialog box.

To add files using date macros:

1. On the Title, Log File Format dialog box, click . The Selected Logfiles dialog box opens.
2. Click **Date Macro**. The Create or Edit Date Macro dialog box opens.



3. In the **Location** text box, type the path to the log file or browse to the directory.
4. In the **Style** text box, use the dropdown list to specify the way in which the date is arranged in the file name.

5. In the various **Log File Name** text boxes, specify the following:

- **Prefix:** Type any text that precedes the date.
- **Year:** If the file name contains the year, select a year format from the dropdown list.
- **Month:** If the file name contains a month, select a month format from the dropdown list.

The three-character text abbreviations for the month are case sensitive. Select the case desired.
- **Day:** If the file name contains a day, select a day format from the dropdown list.
- **Suffix:** Type the log file extension.

6. Make any necessary adjustments to the system date:

- Select **Use the current system date** to make no changes to the system date.
- Select **Subtract this many days from the system date** to subtract days, then type the number of days to be subtracted into the text box.
- Select **Add this many days to the system date** to add days, then type the number of days to be added into the text box.


7. The resulting macro is displayed in the **Review Results** text box. Click **OK** to close the dialog box.

Note

You can also use macros in the Log File URL path as well as the Save As paths of the Scheduler and the Create Report dialog boxes.

8. Click **OK** to return to the Title, Log File Format dialog box.

To remove log files from the File Specifications and Log File List:

1. On the Title, Log File Format dialog box, click . The Selected Logfiles dialog box opens.
2. Select the log files in the list.
3. Click **Delete**. A confirmation message displays.
4. Click **Yes** to confirm. The log file is removed from the list.

Using Date Macros

If your firewall maintains a separate log file for each day named by the date, and you would like to define a log profile which incorporates only the previous day's firewall activity, type a line like the following in the **Log File Path** text box in the Title, Log File Format dialog box, or use the Create or Edit Date Macro dialog box.

```
C:\WEBSRVR\LOGFILES\%DATE-1%%mm%%dd%%yy%.log
```

If your firewall maintains a separate log file for each day named by the date, and you would like to specify the previous three days' worth of log files, type a line like the following in the **Log File Path** text box in the Title, Log File Format dialog box, or use the Create or Edit Date Macro dialog box.

```
C:\WEBSRVR\LOGFILES\%DATE-3%%mm%%dd%%yy%.log|%DATE-2%%mm%%dd%%yy%.log|%DATE-1%%mm%%dd%%yy%.log
```

Using Firewall Add-On Support for Clusters

The Firewall Add-On analyzes the multiple log files created by firewalls, VPNs, or proxy servers hosted on multiple servers or server clusters. Using WebTrends ClusterTrends technology, it automatically consolidates the data to provide an accurate analysis of firewall activity. While Firewall Suite offers accurate, sophisticated reporting for log files for a single firewall, the Firewall Add-On support for clusters provides additional reporting capability for firewalls hosted by multiple servers. Firewall Add-On addresses the problem of overlapping log files.

A firewall cluster is a group of firewalls, VPNs, or proxy servers cooperating to provide high bandwidth and reliable access. The simplest and most common form of a firewall cluster includes multiple servers and a load balancing device or redirector. Each server has identical firewall content and usually runs mirroring software to maintain the duplicate content across all the firewalls in the cluster.

Activity through the firewall is distributed among all the firewalls, VPNs, or proxy servers in the cluster by a redirector device. The redirector achieves a balanced load for each server in the cluster.

Firewall clusters provide the following benefits:

- *High bandwidth capabilities.* Because of the load balancing hardware or software that distributes the requests, you can achieve greater bandwidth than with a single server configuration.
- *Reliability.* Because an identical firewall is on each server, if one server is down because of software or hardware problems, the other servers can continue to handle activity.
- *Maintenance.* You can upload changes to one firewall server while others are still available for access. Once uploaded, changes are copied to other servers in the cluster.

However, the individual log files from the firewalls in the cluster yield inaccurate data because they are logging only part of the activity.

To remedy this issue, the Firewall Add-On time-stamps firewall activity, and records it in sequence, even though the activity may be directed to and logged on different firewalls in the cluster. Using the time stamp, the Firewall Add-On collects all of the data from each server, reorders it, and analyzes it to produce accurate and complete results for the firewall. You must purchase a Firewall Add-On to implement this technology.

Using Department Management

You may wish to configure your profile using the Department Management feature. This feature provides a more detailed break-down of your organization's domain name into groups of users using their IP address or domain names. You can configure Firewall Suite to report on domain activity by department including the following:

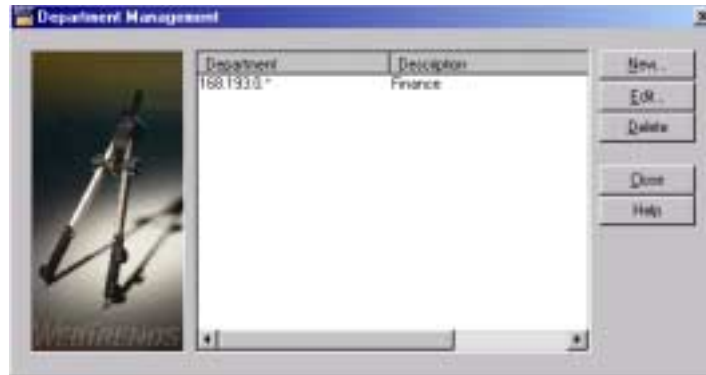
- Which pages users access, and how much time they spend on them.
- Which departments access your intranet and when that access occurs.
- Where your users and departments are located.
- Which operating systems are used most widely within the your organization.
- Which browsers are used.
- Which days and times are the most active and inactive.
- Which forms users submit.
- Which scripts run and when they run.

Once you have set up departments, this information is automatically included in General and Outgoing Firewall Activity reports. You can also use the Departments filter element to report on just the ones you are interested in. See "Departments" on page 172.

Defining a Department

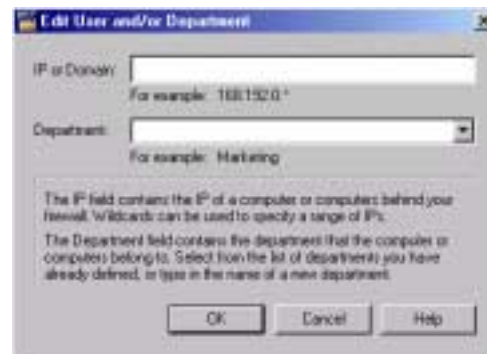
To set up departments to be included in reports or used in filters:

1. On the Main Console, select **Tools > Department Management**. The Department Management dialog box appears.



A list of departments that have been defined appears in the list window.

2. Click **New**. The Edit User and/or Department dialog box opens.



3. In the **IP or Domain** text box, type an IP address, IP address range, or domain name.

– You can type a subnet using CIDR format. For example:

206.13.01.48/26

where /26 indicates the number of bits used to identify the network.

– You can use wildcards to specify a range of addresses. For example, type:

255.255.255.*

to specify an entire Class C subnet, or type:

255.255.*

to specify a Class B subnet, or type

255.*

to specify a Class A subnet.

You *cannot* list IP addresses or domain names separated by spaces or commas.

4. Do one of the following:

– Select a previously-defined department from the **Department** dropdown list.

– In the **Department** text box, type a new department name as you want it to appear in reports.

5. Click **OK**.

Editing a Department

You can make changes to the departments and the IP addresses or domains associated with the departments within the Department Management dialog box.

To edit a department:

1. On the Main Console, click **Tools > Departments**. The Department Management dialog box opens.
2. In the Department Management dialog box, select the department definition that you want to change, and click **Edit**. The Edit User and/or Department dialog box opens.
3. In the **IP or Domain** text box, type an IP address, IP address range, or domain name.
4. Do one of the following:
 - Select a previously-defined department from the **Department** dropdown list.
 - In the **Department** text box, type a new department name as you want it to appear in reports.
5. Click **OK** to save your changes, or click **Cancel** to return to the Department Management dialog box without saving your changes.

Running Firewall Activity Profiles from the Command Line

You can run any profile from the command line. To prevent collisions, the Scheduler handles command-line processing. When you run a profile, it is placed in the Scheduler queue until it can be processed.

Basic Information

Command-Line Help

Get help for any command by typing:

unknown

Files

Each profile type is referred to as a *cartridge*. The command syntax for running a profile specifies three files:

- The cartridge application extension
- The profile configuration
- The memorized report.

Following each command-line component section is a table that lists the files and their locations.

Syntax

The syntax for running a profile is:

```
"runevent cartridge profile memorized report distribution"
```

Note

The distribution option is not required.

Command-Line Components

The following sections provide descriptions of each component. You can use the name of the component, its file name, or its complete path and file name.

Cartridge

Use the following command to specify the cartridge:

```
/c="cartridge filename"
```

where *cartridge filename* is the cartridge application extension file name.

Cartridge	File name	Location
General	wtm_FirewallOther.dll	\WebTrends Firewall Suite
Incoming	wtm_FirewallWebIn.dll	\WebTrends Firewall Suite
Outgoing	wtm_FirewallWebOut.dll	\WebTrends Firewall Suite

Profile

Use /p or /pf to identify the profile. For example:

```
/p=profile description
```

or

```
/pf=profile file name
```

where *profile description* is the value of the Description parameter in the profile configuration file (or the profile description from the Main Console) and *profile file name* is the name of the profile configuration file.

Note

When you use the user interface to create profiles, the corresponding configuration files are named numerically beginning with 00000001.fir. You can rename them.

The following table shows profile configuration file extensions.

Cartridge	File name	Location
General	*.fir	\WebTrends Firewall Suite\wtm_Firewall\Other\datfiles
Incoming	*.fwi	\WebTrends Firewall Suite\wtm_Firewall\WebIn\Datfiles
Outgoing	*.fwo	\WebTrends Firewall Suite\wtm_Firewall\WebOut\Datfiles

Memorized Report

If you are running a report, use /m or /mf to specify the memorized report. For example, type

/m=memorized report description

or

/mf=memorized report file name

where *memorized report description* is the value of the Description parameter in the memorized report configuration file (or the memorized report name in the Create Report window of the user interface) and *memorized report file name* is the file name of the memorized report configuration file.

The following table shows memorized report file extensions.

Cartridge	File Name	Location
General	.mss	\WebTrends Firewall Suite\wtm_Firewall\other\datfiles
Incoming	.mss	\WebTrends Firewall Suite\wtm_Firewall\WebIn\Datfiles
Outgoing	.mss	\WebTrends Firewall Suite\wtm_Firewall\WebOut\Datfiles

Distribution Method

If you are running a report, use `/s` to specify how the report is saved or distributed. You can save a report to a file, transfer it using FTP, or send it as an email attachment.

Note

Using `/s` overrides the distribution method in the memorized report.

In this example:

```
/s="path and report name"
```

path and report name is the complete path of the location where you want to save the report and the file name for the report.

In this example:

```
/s="ftp://ftp site/path and report name  
/username=username /password=password"
```

ftp site is the domain name of the FTP site; *path and report name* is the path from the root directory of the site and the file name for the report; *username* and *password* are the login name and password required to access the FTP site.

In this example:

```
/s="mailto:user@domain.com/c:\directory\report.html"
```

user@domain.com is the recipient of the report, and *c:\directory\report.html* is the directory and file name for saving the report. Note that there is no space between the recipient and the /save-to directory path.

Command-Line Examples

In these examples, the options and their values are displayed on separate lines. Each command is on a single line, with a single space preceding each option.

This example uses the profile and the memorized report descriptions for the General Firewall Activity cartridge. The report is saved to a local directory.

```
"runevent /c="wtm_FirewallOther.dll"  
/p="General Firewall Activity"  
/m="Default Summary (HTML)"  
/s="c:\reports\report.htm"
```

This example uses file names for the General Firewall Activity cartridge to identify the cartridge, profile, and memorized report. This report is sent via email:

```
"runevent /c="wtm_FirewallOther.dll"  
/pf="sample.fir"  
/mf="DEFAULT_htm.mss"  
/s="mailto:administrator@webtrends.com/c:\reports\report.html"
```

Designing Firewall Profiles

This section contains information that will help you design a Firewall or Web Activity Profile.

Report Content

The following table shows which type of profile you should use to get the report content you need.

To Report On	Using These Criteria	Use This Profile Type
Bandwidth	Users, by protocol	General Firewall Activity
	Users, by day of week	Incoming Firewall Activity
	Users, through proxy server	Incoming Firewall Activity
Categories	Categories of Web sites accessed by organization user	Outgoing Firewall Activity
Directories	Most accessed	Incoming Firewall Activity
Email	Top senders by direction, largest messages by direction	General Firewall Activity
Files	Files downloaded by an external user by type	Incoming Firewall Activity
	Files downloaded most by an internal user	Outgoing Firewall Activity
FTP	Upload activity, download activity, largest uploads/downloads	General Firewall Activity

To Report On	Using These Criteria	Use This Profile Type
Geographic Information	By country, by North America, by city for external users	Incoming Firewall Activity
	Countries accessed by internal users	Outgoing Firewall Activity
Incoming Activity Summary	Activity by day, by hour	Incoming Firewall Activity
Incoming Activity Details	Activity by day, by hour	Incoming Firewall Activity
Organizations	Visited by internal users	Outgoing Firewall Activity
	Visited by external users	Incoming Firewall Activity
Outgoing Web Activity Summary	Activity by hour, by day	Outgoing Firewall Activity
Outgoing Web Activity Details	Activity by hour, by day	Outgoing Firewall Activity
Pages	Most/least requested pages, top entry pages, top exit pages, single access pages, paths through sites	Incoming Firewall Activity
Rules	By internal address, by external address, by protocol	General Firewall Activity
Telnet	Top telnet users by direction, largest telnet sessions	General Firewall Activity
Traffic	By direction, by time of day, by day of week	General Firewall Activity

To Report On	Using These Criteria	Use This Profile Type
Users	By region, organization, paths through site	Incoming Firewall Activity
	email senders, telnet sessions, FTP activity, users triggering firewall rules	General Firewall Activity
VPNs	IP addresses, events	General Firewall Activity

Chapter 4

Alerting and Monitoring

This chapter explains how to create and use profiles for the Alerting and Monitoring module. Firewall and Web Activity profiles are covered in “Firewall Profiles” on page 27.

The Alerting and Monitoring module keeps tabs on a number of different types of networked objects such as Web sites, files, event logs, services, ODBC database servers, and devices identified with an (IP) address—networked objects in your organization that must be running and available. If an event or a change of state occurs with a monitored object, the module can notify you, start recovery actions, or do both.

The module can also generate reports that help you track how reliable each monitored device or object is and determine how the software responded when any device failed. You can tailor your reports to see which objects tend to fail, when they do so, and for how long. You can also automate status reports that find the data you need and make it available when you need it most.

Alerting and Monitoring Profiles

Much like the firewall activity modules, you must first create a profile to take advantage of the features available with the Alerting and Monitoring module. Once you’ve created a profile, you can generate reports of response activity for that profile. See “Working with Reports” on page 201.

Use alerting and monitoring profiles to:

- Monitor Web-related devices and services for changes in state. For a complete list of devices you can monitor, see “Monitor Types” on page 148.
- Send and receive alerts when the state of a device changes or a particular event triggers an alert.
- Set up recovery actions to automatically restore devices and services that have stopped operating.
- Run alerting reports that contain information about the status of monitored devices and services.
- Create automated status reports.

How Alerting and Monitoring Works

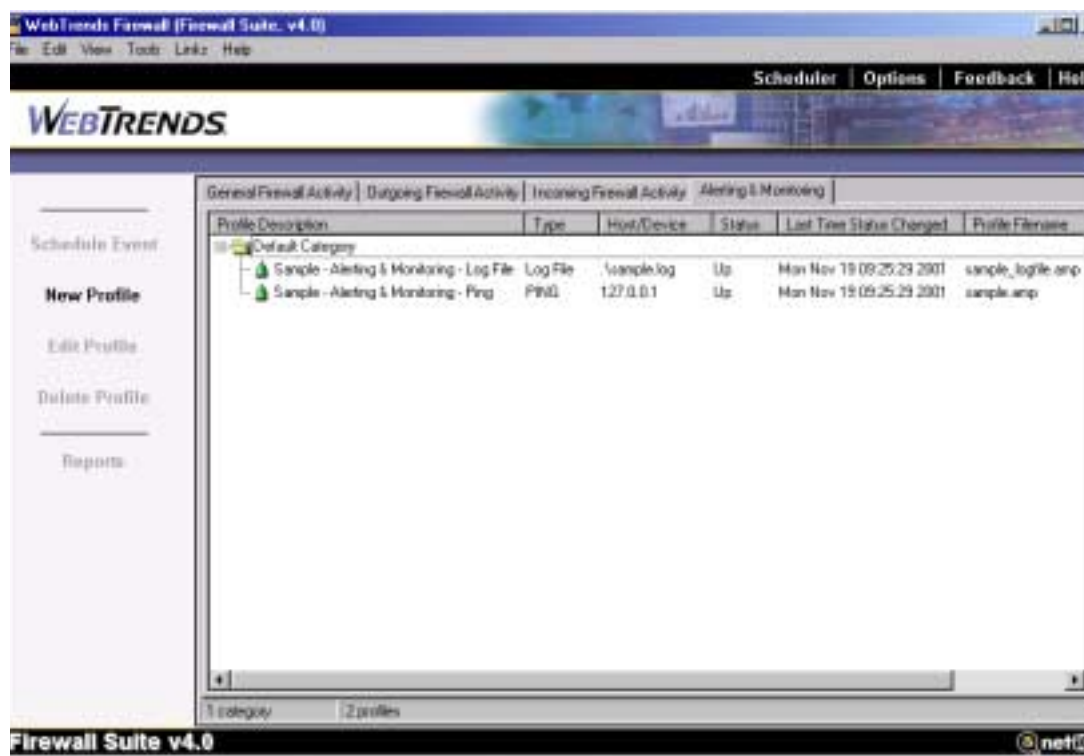
A *state* is a condition that can be repeatedly tested. For example, a network device that is operating is considered to be in an *up* state, while a device that is not operating is in a *down* state. The Alerting and Monitoring module functions by polling a target object—that is, using a Ping utility to repeatedly query the object about its state at user-specified intervals.

In contrast, an *event* is a unique occurrence. For example, an NT Event error that is entered in your Web server log a single time is an event. In addition to monitoring an object’s state, the module can watch for certain events that might occur.

When an object’s status varies from a certain preset state, or when a trigger event occurs, the Alerting and Monitoring module uses a pre-programmed method to alert you and takes a course of pre-determined recovery actions to respond to the event or return the object to its initial state.

Sample Alerting and Monitoring Profiles

It may be helpful to view a sample profile as you review the next section, “Alerting and Monitoring Profile Settings” on page 106. Two sample alerting and monitoring profiles are provided in the profile description list of the Main Console under the **Alerting & Monitoring** tab. In one sample, the profile specifies a network device to be monitored using the Ping utility, the response configuration specifies a single-phase response, and the response action profile specifies an audio alert.



To view the sample Alerting and Monitoring profile:

1. Select the **Alerting & Monitoring** tab on the Main Console.
2. Select the profile called "Sample - Alerting & Monitoring - Ping".
3. Click **Edit > Profile** from the Main menu. The sample profile opens.
4. Select the various tabs in the Edit Alerting & Monitoring Profile dialog box to view the settings specified for the profile.

Alerting and Monitoring Profile Settings

When creating an alerting and monitoring profile, you must define which device or object to monitor, when to monitor the device, what event or change in state for that device should trigger a response, and what action or actions should occur when the response is triggered. These elements are discussed in the following sections.

Configuring some of these elements requires drilling down several dialog boxes deep. To familiarize you with these dialog boxes and their settings, instructions for creating an alerting and monitoring profile follow this section.

Device or Object Being Monitored

When first creating an alerting and monitoring profile, you must specify which device to monitor and point to the device so that the Alerting and Monitoring module can access it. For a complete list of devices you can monitor, see "Monitor Types" on page 148.

Monitoring Schedule

The monitoring schedule specifies when the alerting and monitoring profile should actively monitor the specified device or object by polling it with the Ping utility. The monitoring schedule also includes the frequency with which to poll the device, and the amount of time to wait after a failure occurs before initiating a response.

Response Settings

The combination of settings and dialog boxes in which you specify:

- The device state change or event that triggers a response. Use the Response Settings dialog box to make these selections.
- The schedule for applying the response. Use the Edit Response Schedule dialog box to specify these settings.
- The set of actions that constitute the response, the order in which to apply those actions, and how many times to apply each action. Use the Select Response Configuration, Response Configuration Settings, and the Response Profile Phase Settings dialog boxes as needed to specify these settings.
- The specific configurations for each action that constitutes the response. Use the Select Response Actions dialog boxes and the individual configuration dialog boxes for each possible action to specify the appropriate settings.

Response Schedule

The response schedule specifies how and when to apply response configurations in reaction to an event or change of state in a monitored device. You can create new response schedules, or you can edit, copy, or link to existing response schedules.

Once you have created and saved a response schedule, you can use it for other monitoring and alerting profiles.

Response Configuration

A response configuration specifies the response or responses you want to occur for a given time period when a state changes or an event occurs. This includes any response actions and those actions' settings, and if applicable, the settings that specify when to escalate from one phase to the next.

Once you have created and saved a response configuration, it can be used in multiple response schedules.

A response can be either of two types: single phase or multi phase.

Single-phase applies any assigned actions simultaneously. For example, when a server goes down, a pager alert could be sent to the server administrator, while simultaneously, the module could attempt to reboot the server.

Note

A response phase can consist of a single action or multiple actions.

Multi-phase applies to an assigned action or actions in phases. With the previous example, when the server goes down, the computer could first try rebooting. This would be the first phase. Then, if the computer does not come back up (change state) for a specified amount of time or number of attempts at rebooting, a second phase could be initiated, in which the server administrator is sent an email message and is also paged.

With a multi-phase response, you can set each phase to:

- Wait a specified number of seconds before repeating the response action.
- Repeat a phase a specified number of times before escalating to the next phase of response action.
- Repeat a phase until the profile state changes, which causes the response profile to reset itself.

Response Actions

A single action, such as a pager alert, a system reboot, or an audio alert that can be configured to occur in a specified manner when an event or a change of state for a device or object triggers a response. Once the settings for a response action have been configured, they can be used within either a single or multi phase response.

Possible response actions include:

- Sending an audio or email alert
- Broadcasting an alert to a pager
- Passing an SNMP trap
- Running a program
- Running a group of responses
- Rebooting a device
- Restarting a Windows service

A response action can initiate a single action or, in the case of running a group of responses, can initiate multiple successive actions. You can use the same response action with different response configurations.

Creating an Alerting and Monitoring Profile

This procedure describes the sequence of panels in the New Profile wizard for creating an alerting and monitoring profile. It describes the information required in each panel to set up the profile. Refer to the online help in each panel for more information.

Note

You can create an unlimited number of alerting and monitoring profiles.

To create a new alerting and monitoring profile:

1. Select the **Alerting & Monitoring** profile type tab on the Main Console.
2. From the File menu or the Tasks area select **New Profile**. The New Profile wizard opens to the Specify Profile Description and Type dialog box.

Specify Profile Description and Type

In this dialog box, you specify a name for the alerting and monitoring profile, select a device to monitor, and specify any dependencies the profile you are creating has on other profiles. See “Defining Advanced Monitor Options” on page 144 for more information on dependencies.

Note

You can create an unlimited number of alerting and monitoring profiles.



To specify the profile name and device to monitor:

1. Type a name for the profile in the **Description** text box. The description identifies the profile in the Profile Description list in the Main Console and is used as a sub-heading for reports.
2. Select the device you want to monitor with this profile from the **Device to Monitor** dropdown list.

Note

The list is sorted by device type: IP Device, NT System Monitors, SNMP Monitors, LAN Computer Monitors, Disk and File Monitors. For a list of monitors with descriptions, see “Monitor Types” on page 148.

3. *If you wish to set dependencies on other profiles:*
 - a. Click **Advanced Monitor Settings** to set dependencies on other profiles monitoring other objects. The Advanced Monitor Settings dialog box opens. See “Defining Advanced Monitor Options” on page 144.
 - b. In the Monitor Profiles list, select the check boxes of any profiles that the current profile depends on.

Notes

The current profile is enabled only when the devices for the profiles you select here are active. If one of these profiles goes down, the current profile is disabled.

If you are editing an existing profile, click **Flush Log File** in this dialog box to delete the profile’s log data. Use this option only after you have created the reports you need.

- c. Click **OK** to return to the Specify Profile Description and Type dialog box.
4. Click **Next**. The Specify Profile Details dialog box opens.

Specify Profile Details

Use this dialog box to enter the location of the device to be monitored and settings relevant to the selected device. The fields that appear in this dialog box vary according to the device selected.

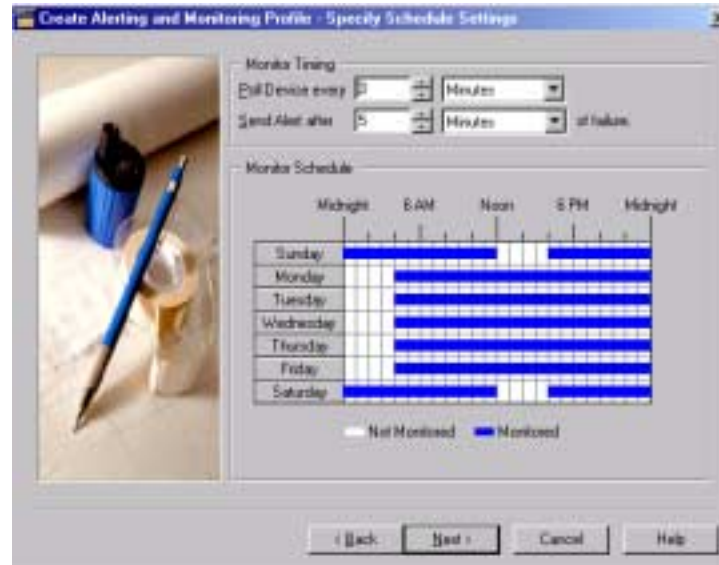


To specify profile details:

1. Fill in the fields in this dialog box, clicking the **Help** button in the dialog box to get device-specific information.
2. Click **Next**. The Specify Schedule Settings dialog box opens.

Specify Monitoring Schedule Settings

Use this dialog box to enter the frequency with which you want to poll the monitored device and specify how long to wait after a device fails before sending an alert. Then set up a weekly monitoring schedule using the monitor schedule. For more information, see “Monitoring Schedule” on page 107.



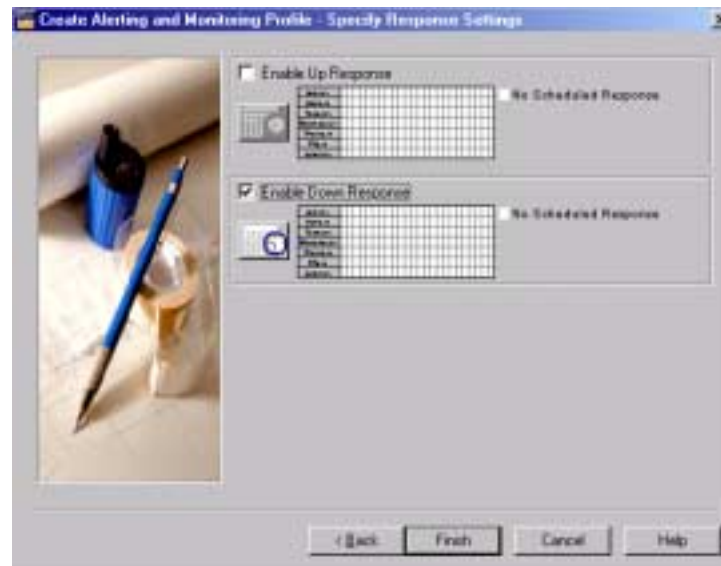
To specify the monitor schedule settings:

1. Enter the frequency with which you want the Ping utility to poll the monitored device by typing or scrolling to a number to set the **Poll Devices every** values in the Monitor Timing area and in the dropdown box. Select either Seconds or Minutes as the time unit.
2. Enter the amount of time after a device has failed to initiate a response by typing or scrolling to a number in the **Send Alert after... of failure** values in the Monitoring area and in the dropdown box. Select either Seconds or Minutes as the time unit.

3. Set the Monitor Schedule by clicking on or off individual grid squares or by clicking and dragging vertically or horizontally to select or un-select days and hours. The areas in blue indicate the times that this profile will actively monitor the device.
4. Click **Next**. The Specify Response Settings dialog box opens.

Specify Response Settings

What you see in this dialog box depends on which device you have chosen to monitor. Some devices allow you to monitor for an “up” state or a “down” state—that is, whether the device is functional or accessible to the Alerting and Monitoring module. Other devices allow you to monitor an additional state particular to the device. You can choose to create a response schedule for any or all of the states available with that device. You can also create and reuse response schedules with different monitoring profiles.



Choosing Response Options

To create a response schedule for the device you want to monitor, select the state or states to which you want the module to respond. You can specify more than one state by creating multiple schedules. For example, if you want to be notified when a server is down and when it comes back up, create response schedules for both states.

- **Enable Up Response.** Select this option if you want to receive notification and/or trigger a response when the monitored object or device is “up,” as indicated by its ability to respond to the module’s polling request. You would choose this option if the normal state for the object is down or inaccessible, or if the object you want to monitor does not yet exist and you want notification when it becomes available, active, or accessible.


For example, if you want to be alerted when your Web server has created and saved a new log file for processing, configure the alerting and monitoring module to poll the directory where the log file is created. Ordinarily, that file will not exist until the server creates it, so its state will be “down.” Once the server creates the file, however, its state will change to “up,” and the module can notify you.

- **Enable Down Response.** Select this option if you want to receive notification and/or trigger a response when the monitored object or device goes “down,” which means that it no longer responds to the module’s polling request. Choose this option if the monitored object or device is normally active, available, or accessible and you want notification when that state changes.

For example, if you want to monitor the state of your Web server to ensure its availability, you would have the module poll it periodically to check its state. If the server fails to respond to the polling request, after a specified time period of non-responsiveness, the module could notify you that the server is down and initiate the response action you have programmed into your response profile for that condition.

- **Enable [other] Response.** Select this option if you want to receive notification and/or trigger a response when the monitored object or device changes its state from an expected state. What happens to change the state from the expected state to a different state depends on the nature of the object or device property you want to monitor.

To specify response settings in the response schedule:

1. In the Specify Response Settings dialog box, select one or more response states to configure, for example Enable Up Response, or Enable Down Response.
2. Click the  button located below the check box for a selected response state to open the Edit Response Schedule dialog box.



3. In this dialog box, specify which actions the module should take when the monitored device changes state. Using this dialog box you can:

- *Create a new response schedule* by clicking **Add New** and defining new response configurations and their response actions. If you choose to save the response schedule, you can use it later with another monitoring profile. For more information, see “To create a response schedule:” on page 119.
- *Edit an existing response that is already associated with the profile* by selecting a response schedule in the list of response schedules and clicking **Edit New**.
- *Dissociate an existing response schedule from the current profile* by selecting a response schedule in the list of response schedules and clicking **Remove Response**.
- *Load an existing response schedule* by clicking **Load**, then altering and saving it to suit the current monitoring profile. A loaded schedule is a standalone copy of the original response schedule. If you make changes to the loaded (copied) schedule, changes to it only affect the monitoring profile to which it is attached. When you modify the response schedule, you are asked to give it a new name. The schedule is identified by this name when loading or linking to it from other monitoring profiles.
- *Link to an existing response schedule* by clicking **Link** to apply its settings to the current monitoring profile. Because the monitoring profile is only linked by reference to the response schedule, changes made to the schedule affect *every* monitoring profile linked to it. Typically, you link to a schedule if several monitoring profiles need to have the same response schedule applied and you do not want to re-enter the settings for each profile.

Conversely, you can unlink from an existing profile by clicking **Unlink** to dissociate the current monitoring profile from a linked response schedule.

- *Save a response schedule* by clicking **Save** to save the response schedule settings. Once saved, you can use a loaded or new response schedule with other profiles. If you made changes to a linked profile, saving these changes affects all other profiles to which the response schedule is linked.
4. If necessary, add another response schedule for the current response state, or add a response schedule for another state.

Note

You can add more than one response schedule for a given response state.

5. Click **Finish** to complete your Alerting and Monitoring profile. It now appears in your Profile Description list in the Main Console.

Adding a Response Schedule

You can create a response schedule:


- While creating a new Monitoring and Alerting profile in the Specify Response Settings dialog box.
- While editing an existing Alerting and Monitoring profile using the **Response Settings** tab.

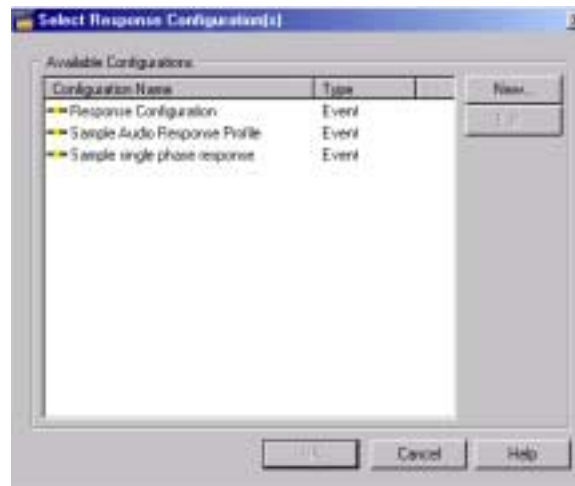
When a response schedule is complete, its name appears in the Available Schedules list in the Select a Response Schedule dialog box. You can use this response schedule with the current or other profiles by selecting it from this list.

If the response schedule appears in the Edit Response Schedule dialog box's list, then it is active for the current Alerting and Monitoring profile.

The following procedure follows the steps for creating a response schedule while editing an existing Alerting and Monitoring profile. This procedure could be followed just as well when creating a new profile.

To create a response schedule:

1. Select an Alerting and Monitoring profile from the Profile Description list in the Main Console.
2. Click **Edit** on the toolbar and select the **Response Settings** tab.
3. Click the  button located below the check box for a selected response state to open the Edit Response Schedule dialog box.
4. Click **Add Response**. The Select Response Configuration(s) dialog box opens.



5. *To use an existing response configuration*, select an existing response configuration from the list at the bottom of the dialog box and click **OK** to exit.
6. *To edit an existing response configuration*, select an existing response configuration and click **Edit**. Skip to Step 8.
7. *To create a new response configuration*, click **New**.

8. Type a name for the Response Profile. This name will appear in the list of Response profiles. You can select it for other Alerting and Monitoring profiles.
9. Select one of the following response types:
 - **This is a single phase Event Response Profile.** Select this option to create a response configuration that triggers all of its component response actions once, simultaneously, before resetting.
 - **This is a multi phase Escalating State Response Profile.** Select this option if the condition that originally triggered the response persists for a set time, and you wish to escalate to a new phase that has new or different response actions.
10. Choose one of the following options:
 - **New Phase** (only available if you selected multi phase). Choose this to add a new phase of response actions that will be applied according to the settings. See “Adding or Editing a New Phase” on page 120 to continue this procedure.
 - **Edit Phase.** Select an existing phase from the Response Details list, and click **Edit Phase** to open the Response Profile Phase Settings dialog box.
11. Click **OK**.

Adding or Editing a New Phase

With a single phase response configuration, you can edit the existing phase (there will always be a default phase called "Single Phase" with no actions configured for it). With a multi phase response configuration, you can add new phases or edit existing phases. This procedure assumes the Response Configuration Settings dialog box is already open.

To add or edit a new phase:

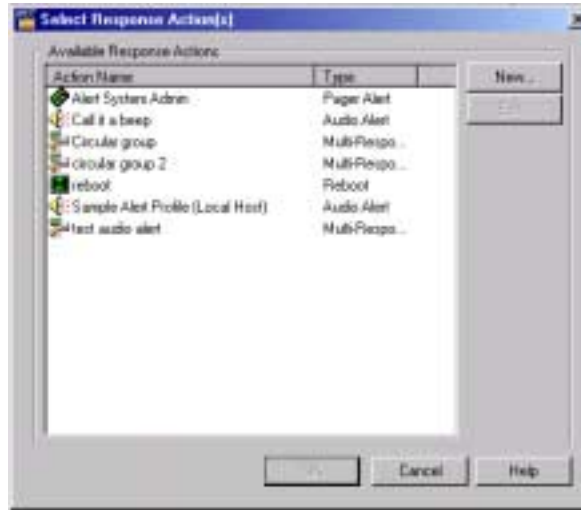
1. Click **New Phase** or select an existing phase and click **Edit Phase**. The Response Profile Phase Settings dialog box opens.



2. Enter a descriptive name in the **Display Text (Optional)** text box, or edit the existing name. This name will appear in the Response Details list.

3. Select from among the following options:

- Add a new action. Click **Add Action** to open the Select Response Action(s) dialog box, in which you may add and configure an action using the steps that follow.



- Click **New** to configure a new action and make it available in the Available Response Actions List. See “Adding and Configuring Response Actions” on page 123 for detailed instructions on configuring the various types of available response actions.
- Select an action from the Available Response Actions List and click **Edit** to change the settings for the selected response action. Make changes to the selected response action as needed. See “Adding and Configuring Response Actions” on page 123 for detailed instructions on configuring the various types of available response actions.

- Remove an action. Select an action in the Phase Action List, then click **Remove Action** to remove the action from the list.
- Reorder the action list. Select an action in the Phase Action List, then click **Move Up** or **Move Down** to specify the order in which you want the actions to be applied. Although the actions occur almost simultaneously, they are applied in the order in which they appear in the Phase Action List.

4. *If the **Wait N sec. before repeating this phase or escalating response field is available** (for multi phase responses only), type a number of seconds to wait before repeating this phase or escalating to the next phase.*

5. *If the **Response Phase Repeat settings are available** (for multi phase responses only), do one of the following:*

- If you want a specific number of repetitions, select **Repeat this Response Phase N times before escalating** and type a number of times to repeat.
- If you want the phase repeated until the profile state changes, select **Repeat this Response Phase until the profile state changes.**

6. Click **OK**.

Adding and Configuring Response Actions

You can add and configure a response action from the Select Response Action(s) dialog box. You can access this dialog box while editing a profile, or while creating a new profile using the New Profile wizard. You can get to this dialog box by following the instructions up through Step **3** for “Adding or Editing a New Phase” on page 120.

To add and configure a response action profile:

1. In the Select Response Actions dialog box, click **New**. The Select Response Action dialog box opens with all possible response actions available.



2. Select a response action and the configuration dialog box for that action opens.
 - **Audio Alert:** See “Creating an Audio Alert” on page 125.
 - **E-mail Alert:** See “Creating an Email Alert” on page 126.
 - **Execute Program:** See “Creating an Execute Program Response Action” on page 128.
 - **Multi-Response:** See “Creating a Multi-Response Action” on page 129.
 - **Pager Alert:** See “Creating a Pager Alert” on page 130.
 - **Reboot:** See “Creating a Reboot Response Action” on page 138.
 - **Restart Service:** See “Creating a Restart Service Response Action” on page 140.
 - **SNMP Trap Alert:** See “Creating an SNMP Trap Alert” on page 141.
3. Complete the settings for the response action, and click **OK**. You return to the Select Response Action(s) dialog box with the newly configured response action appearing in the list of Available Response Actions.
4. Click **OK**. You return to the Response Profile Phase Settings dialog box.

Creating an Audio Alert

An Audio Alert plays a system sound, such as a beep, when the Alerting and Monitoring module detects a change in state of the monitored object or device.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create an audio alert:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **Audio Alert**. The Audio Alert Profile dialog box opens.



3. Type a name for the audio configuration in the **Profile Name** text box.

It may be useful to name this profile something like Audio Alert. Whenever you need an audio alert, you can select it by name to use with other response phases for this or other Response profiles.

4. Select the sound to use:
 - **System Beep** plays a predefined beep.
 - **Wave File** plays a .wav file. Click **Browse** to specify the exact location of the file.

5. Specify the duration by choosing one of the following options:
 - **Sound for** sets the number of seconds that the sound will play. Select the number of seconds to play the sound.
 - **Repeat** specifies the number of times to repeat the sound.
6. Click **Test** to make sure your alert works.
7. Click **OK**.

Creating an Email Alert

An E-mail Alert sends an email message to the address you specify when the Alerting and Monitoring module detects a change in state of the monitored object or device.

Note

You must configure your email server settings in the General Options dialog box for email alerts to work.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create an email alert:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **E-Mail Alert** from the Select Response Action dialog box. The E-Mail Alert Profile dialog box opens.



3. Type a description for this alert in the **Profile Name** text box.
4. Type the email address to which you wish to send the alert in the **Send To** text box.
5. Type the text that you want to appear on the subject line of the message in the **Subject** text box.
6. Click **Customize Message** to change the message sent for the alert. See “Customizing Text Messages” on page 142 for details.
7. Click **Test** to make sure your alert works.
8. Click **OK**.

Creating an Execute Program Response Action

The Execute Program response launches a specified program when the Alerting and Monitoring module detects a change in state of the monitored object or device.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create a response action:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **Execute Program** from the Select Response Action dialog box. The Configure Execute/Launch Program dialog box opens.



3. Type a name in the **Profile Name** text box.
4. Type the path to the executable file or command line in the **Path/Command Line** text box. If desired, click **Browse** to navigate to an executable file.
5. Click **OK**.

Creating a Multi-Response Action

A multi-response action carries out a series of response actions when the Alerting and Monitoring module detects a change in state for the monitored object or device. Response actions can include one or more of the existing response action types such as audio alert or pager alert. A response action can also consist of another multi-response action.

See “Adding and Configuring Response Actions” on page 123 for more information about accessing the Select Response Action(s) dialog box.

To configure a multi-response action:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **Multi-Response** from the Select Response Action dialog box. The Response Profile Phase Settings dialog box for a multi-response action opens.
3. In the **Response Group Profile Name** text box, type a name for this group of response actions.
4. Click **Add Action** to open the multi-response version of the Select Response Action(s) dialog box, which lists the available configured actions you can select and add to your multi-response action.

5. Select an existing action in the list and click **Select**. You return to the Response Profile Phase Settings dialog box, and the selected item appears in the Response Action List.



6. Add more actions as needed by repeating Steps 2 and 3.
7. Click **OK**. You return to the Select Response Action(s) dialog box, and the new multi-response alert is added to the Available Response Actions list.

Creating a Pager Alert

A pager alert sends a page when the Alerting and Monitoring module detects a change in state of the monitored object or device.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create a pager alert:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **Pager Alert** from the Select Response Action dialog box. The Pager Alert Profile dialog box opens.



3. In the **Profile Name** field, type a description for this alert.
4. In the Pager Type section, specify the type of pager:
 - Select Alpha-Numeric Pager if the pager accepts messages with either letters or numbers. Specify the ID number needed to send the page in the **ID** field.
 - Click **Advanced** if you need to further define the pager settings. See “Defining Alpha-Numeric Pager Settings” on page 132 for details.
 - Select Numeric Pager if the pager accepts only messages with numbers. If your paging service requires a PIN, type it in the **PIN** text box.
 - Click **Advanced** if you need to further define the pager settings. See “Defining Numeric Pager Settings” on page 134 for details.

5. Specify how your pager can be accessed:

- Select **Web** if your paging service supports Web paging, then select your paging service from the list.
- If your service doesn't appear in the list, select the Custom list item, and click **Advanced** to set up your paging service options. "Defining Custom Web Paging Settings" on page 134 for details.
- Select **Modem** to access your pager through a modem connection, then type the complete telephone number in the **Phone Number** text box. Click **Advanced** to display the Modem Settings dialog box if you need to modify the default modem settings. See "Changing the Modem Settings" on page 136.

6. Click **Test** to make sure your alert works.

7. Click **OK**.

Defining Alpha-Numeric Pager Settings

Use the Advanced Alpha-Numeric Pager Settings dialog box to define a message length or password for alpha-numeric paging.

To define settings:

1. In the Pager Alert Profile dialog box, select **Alpha-Numeric Pager** in the Pager Type area.
2. Click **Advanced** in the Pager Type area. The Advanced Alpha-Numeric Pager Settings dialog box opens.



3. Use the **Length** list box to define the length of the message your pager will accept.

Most alpha numeric pager will accept messages with up to 180 characters. Some have a higher restriction on the number of characters for each message. If this is the case for your pager, use this setting to specify the maximum length of the message sent by Firewall Suite your pager will accept. Select or type the maximum number of characters that may be sent to this alpha-numeric pager.

4. If your service requires a password, type the pager's password in the **Password** text box.
5. Click **Customize Message** to tailor the message that is sent for the alert. See "Customizing Text Messages" on page 142 for details.
6. Click **Time Range** to open the Edit Schedule dialog box in which you can specify when you want the alert enabled.

Defining Numeric Pager Settings

You can modify the pager message sent when the device goes down, and the message sent if the device has recovered.

To define settings:

1. In the Pager Alert Profile dialog box, select **Numeric Pager** in the Pager Type area.
2. Click **Advanced** in the Pager Type area. The Advanced Numeric Pager Settings dialog box opens



3. In the **Down** text box, type the message to be sent when the device is down. The default message is 0000.
4. In the **Reactivated** text box, type the message to be sent when the device is reactivated. The default alert is 9999.
5. Click **Time Range** to open the Edit Schedule dialog box in which you can specify when you want the alert enabled.

Defining Custom Web Paging Settings

Use these settings if your paging service supports Web paging, but your service doesn't appear in the **Service Name** dropdown list.

To define custom Web paging settings:

1. In the Pager Alert Profile dialog box, select **Web** in the Connect to Paging Service via area,
2. In the **Service Name** dropdown list, select **Custom**.
3. Click **Advanced** in the Connect to Paging Service via area. The Advanced Web Pager Settings dialog box appears.



4. In the **HTTP Get Request** text box, copy the URL from the paging service Web page that provides a paging form. The URL should specify the Get request, and look something like this:

`http://www.paging-service.net?arg:Date=%date%&To=%id%&Message=%msg%`

In this example, you would type values for *date*, *id*, and *msg*. The arguments and the data you use vary according to paging service. See “Custom Web Paging Variables” on page 136 for details on using variables to include user defined values.

5. Click **Time Range** to open the Edit Schedule dialog box in which you can specify when you want the alert enabled.
6. Click **OK** to save your changes and close the dialog box.

Custom Web Paging Variables

If your paging service doesn't appear in the Web paging service list in the Pager Alert dialog box, you can set it up using a custom Web paging alert. You can use any of the variables listed below in your custom Web paging settings.

The following table shows the supported variables.

This variable:	Does this:
<code>%arg: title= default value%</code>	Adds a field to the Advanced Web Pager Alert dialog box displaying the default value you specify.
<code>%id%</code>	Includes the paging ID specified in the Pager Alert dialog box.
<code>%msg%</code>	Includes the pager alert message. For numeric pagers, this is the alert specified in the Advanced Numeric Pager settings dialog box.
<code>%num%</code>	Includes the phone number used in the Pager dialog box.
<code>??post data</code>	Indicates that the preceding URL is an HTTP post. For example: <code>http://www.pagingservice.net??arg:Date=%date%&To=%id%&Message=%msg%</code>

Changing the Modem Settings

If you need to modify the modem default settings for your pager alert, you can do so in the Modem Settings dialog box.

To change modem settings:

1. In the Pager Alert Profile dialog box, select **Modem** in the Connect to Paging Service via area.
2. Enter the complete phone number (area code + number) in the **Phone Number** text box.

3. Click **Advanced** in the Connect to Paging Service via area. The Modem Settings dialog box opens.



4. Make any needed changes to the following settings:

- **Port.** Select the port used by the modem.
- **Baud Rate.** Select the rate of data transmittal (bps).
- **Data.** Select the number of bits in a data word.

The default is 7, which is usually right for pager services. The pager service provider can give you a description of the service's settings. It looks something like [Data][Parity][Stop]. For example, 8N1, 7E2, 7E1.

- **Stop Bits.** Select the number of stop bits terminating each data word (either 1 or 2). This option defaults to the most common setting.
- **Parity.** Select the type of data checking that you want to use (odd, even or none).

- **Init String.** Type any necessary modem initialization string.
- **Dial String.** Type the command that tells the modem to start dialing.
- **Dial Prefix.** Type any prefix that must be entered before dialing the phone number. For example, type 9 if you are required to enter 9 before dialing the phone number.
- **Dial Suffix.** If you must enter a suffix such as a dialing code or an extension number, type the number here.

Note

You can select the number of seconds that Firewall Suite should wait before entering the suffix. Use commas to specify the number of seconds to wait. One comma is equal to 2 seconds of delay.

- **Timeout connection after x seconds.** Select the number of seconds to wait before ending an attempted transmission.
 - **Wait.** Select the number of seconds for each waiting period. If your connection doesn't require a waiting period, leave the text box empty.
5. Click **Time Range** to open the Edit Schedule dialog box in which you can specify when you want the alert enabled.
 6. Click **OK** to save your settings.

Creating a Reboot Response Action

A reboot response action reboots the system when the Alerting and Monitoring module detects a change in state of the monitored object or device.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create a reboot response action:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **Reboot** from the Select Response Action dialog box. The Configure Reboot Computer dialog box opens.



3. Type a name in the **Profile Name** text box.
4. Choose **Select System** to open the Select System dialog box.
5. Navigate to and select the system to reboot. This selection populates the **System Name** text box.
6. If required, type the **User Name** and **Password** for the system.
7. Click **OK** to return to the Configure Reboot Computer dialog box.
8. Select the **Display Warning before Rebooting Computer** check box to set the response.
9. Type the message to display into the text box, and select the number of minutes to display the message.
10. Click **OK**.

Creating a Restart Service Response Action

A restart service response action restarts a Microsoft Windows service when the Alerting and Monitoring module detects a change in state of the monitored object or device.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create a restart service response action:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **Restart Service** from the Select Response Action dialog box. The Configure Restart NT Service Recovery dialog box opens.



3. Type a name in the **Profile Name** text box.
4. Choose **Select System** to open the Select System dialog box.
5. Navigate to and select the system to reboot. This selection populates the **System Name** text box.
6. If required, type the **User Name** and **Password** for the system.
7. Click **OK** to return to the Configure Restart NT Service Recovery dialog box.
8. Select a service from the **Select NT Service** dropdown list.
9. Click **OK**.

Creating an SNMP Trap Alert

If you have an SNMP Management console and the WebTrends SNMP Agent is activated, you can have an SNMP trap sent if the device you are monitoring fails.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create an alert:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **SNMP Trap Alert** from the Select Response Action dialog box. The SNMP Alert Profile dialog box opens.



3. Type a name for the SNMP Alert profile in the **Specify a name for this SNMP Alert Profile** text box.
4. Click **Test** to make sure your alert works. See “Configuring Options” on page 291 for details on enabling the WebTrends SNMP Agent.

5. To create a custom alert message, click **Customize Message**. See “Customizing Text Messages” on page 142 for more information about this feature.
6. Click **OK**.

Customizing Text Messages

Many of the alerting dialog boxes have a Customize Alert Message feature which enables you to change the message used for the alert.

To change the message:

1. Click **Customize Message** in the dialog box you’re working in (such as the E-mail Alert Profile dialog box). A Customize Alert Message dialog box appears.



2. Type the new message. You can include any of the variables described in the table below in your message.
3. Click **OK**.

The following table shows the variables you can use to customize your messages.

Variable	Result
%%PROFILE_DESC%%	Includes the text from the profile's Description field.
%%HOST_NAME%%	If a host name or IP address has been defined, it is included.
%%PORT%%	If a port number for the device has been defined, as it is for the HTTP monitor, the port is included.
%%MONITOR_DEVICE%%	Includes the device specified in the profile.
%%MONITOR_TYPE%%	Includes the monitor type specified in the Device to Monitor list.
%%MONITOR_STATE%%	Includes the state of the device, such as down.
%%MONITOR_STATE_TIME%%	Includes the length of time that the monitor has been in the current state.
%%MONITOR_EVENT%%	Includes the last event that was logged for the profile.
%%MONITOR_EVENT_TIME%%	Includes the time that the last event occurred.
%%MONITOR_EVENT_MESSAGE%%	Includes additional information about the event.
%%RECOVERY_STAGE%%	Includes the number of the most recent recovery attempt (first, second, or third).
%%RECOVERY_ATTEMPT%%	Includes the number of the most recent retry for the current recovery attempt.

Formatting the Message

Use \" to put quotation marks around a word or phrase. This example:

```
\">%MONITOR_EVENT_MESSAGE%\ "
```

puts quotation marks around the results of the event message variable in the message sent.

Use \r\n to insert a paragraph return.

Defining Advanced Monitor Options

Define the dependencies of the current profile on others, disable the current profile, and flush the logs for the current profile.

To define advanced options:

1. On the Main Console, select a profile and click **Edit**.
2. Select the **General** tab.

3. Click **Advanced**. The Advanced Monitor Settings dialog box opens, with a list of all available Monitoring profiles.



4. Select the check boxes of any profiles on which the current profile depends. The current profile is enabled only when the devices for the profiles you select here are active. If one of these profiles goes down, the current profile is disabled.
5. If desired, select the **Disable Profile** check box to disable the current profile.
6. If you no longer need existing log data for reports, click **Flush Log File** to delete the for the current profile. Use this option only after you have created the reports that you need.
7. Click **OK**.

Configuring Alerting and Monitoring as a Windows Service

If you are running Firewall Suite on a Windows NT, Windows 2000, or Windows XP system, Alerting and Monitoring installs as a service. You must configure your Windows NT, Windows 2000, or Windows XP system to give Firewall Suite the rights it needs.

Monitoring systems over multiple domains is possible as long as the proper trust relationships exist.

Setting up the Required Rights

To run Alerting and Monitoring as a service, the account you use must have the following privileges:

- Act as part of the operating system
- Log on as a service
- Log on locally

To monitor systems remotely, the account you use must also have:

- Administrative rights on the system doing the monitoring
- Administrative rights on each of the systems that are being monitored

To set up administrative rights:

1. Select **Start > Programs > Administrative Tools > User Manager**.
2. Select the **Policies, User Rights** command.
3. In the User Rights Policy dialog box, select the **Show Advanced User Rights** check box.
4. Select **Act as Part of the Operating System** from the Right list.

5. Click **Add** and select the account that Firewall Suite uses to run as a service.
6. Click **OK**.
7. Select **Log on Locally** from the Right list.
8. Click **Add** and select the account that Firewall Suite uses to run as a service.
9. Click **OK**.
10. Select **Log on as a Service** from the Right list.
11. Click **Add** and select the account that Firewall Suite uses to run as a service.
12. Click **OK**.
13. Click **OK** to close the User Rights dialog box.

Running the Service

To run Alerting and Monitoring as a service:

1. Close Firewall Suite.
2. Select **Start > Settings > Control Panel**.
3. Select **WebTrends Alerting and Monitoring for Firewall Suite**.
4. Click **Start Up**.
5. Select **This Account**.
6. Type a user name and password that meets the above criteria.
7. Stop and restart the service. Firewall Suite can be restarted.

Monitor Types

The following table lists the monitor types used by Firewall Suite, along with each monitor's default port and the monitoring method used.

Type	Purpose	Default port	Method
All device monitors, excluding DNS	Test connection	Various	All device monitors, excluding DNS, do a simple port connect test unless Advanced Protocol Monitoring is available and enabled.
IP device monitors			
BOOTP	Monitors a BOOTP server. BOOTP gives diskless client computers the information they need to start-up (or boot).	TCP 67	
DNS	Monitors a Domain Name System (DNS). DNS translates numeric IP addresses into domain names.	UDP 53	Alerting and Monitoring sends a DNS request to the DNS server at the specified address.
Echo	Monitors an Echo server. Echo is a basic server that sends the client the same message it received. This is useful for troubleshooting network communication problems where data is being corrupted.	7	If you use the Advanced Protocol Validation, Alerting and Monitoring will send a specific string to the port ("WebTrends Echo Test") and ensure that it receives the proper response.

Type	Purpose	Default port	Method
Finger	Monitors a finger daemon. A finger daemon provides information about users such as the last login time, terminal location and other information.	79	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a properly formatted finger response.
FTP	Monitors an FTP server, which provides users/visitors remote access to files.	21	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a successful banner.
Gopher	Monitors a Gopher server, which provides access to WAIS services similar to HTTP.	70	
HTTP	Monitors a Web server, which handles HTTP requests from browsers.	80	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a properly formatted HTTP response.
HTTPS	Monitors a secure Web server, which handles HTTP requests from browsers.	443	
IMAP3	Monitors an IMAP3 mail server, which enables user to manage remote mailboxes. This is a simple port connect test.	220	
IMAP4	Monitors an IMAP4 server, which uses SMTP to provide remote mailbox management.	143	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a successful banner.

Type	Purpose	Default port	Method
IRC	Monitors an Internet Relay Chat (IRC) server, which provides a system for “chatting” on the Internet.	6667	
Kerberos	Monitors a Kerberos server. Kerberos handles requests for those using the Kerberos data authentication system. Typically, it is used to verify the identity of a user to a host when using Telnet or FTP.	88	
NFS	Monitors an NFS server. NFS allows users to access shared files on remote computers as if they were stored locally.	2049	
NNTP	Monitors a Network News Transfer Protocol (NNTP) server that enables users to post or read messages on a newsgroup.	119	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a successful banner.
PING	Sends an ICMP PING request to the specified device and waits for a response.	ICMP	
POP2	POP2 is a client-side email protocol. A POP2 server stores incoming email for client retrieval.	109	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a successful banner.

Type	Purpose	Default port	Method
POP3	POP3 is a client-side email protocol. A POP3 server stores incoming email for client retrieval.	110	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a successful banner.
RLOGIN	Monitors an RLOGIN server, which handles requests for users accessing a remote computer. RLOGIN enables users to access local services.	221	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a properly formatted Rlogin response.
RPC	Monitors an (RPC) Remote Procedure Call used by programs and hidden to users.	530	
RSH	Monitors an Rshell server, which allows users to access to a Unix computer remotely.	222	
RWHOIS	Monitors a RWHOIS server, which can tell users about a second-level domain name and allows for recursive queries. An experimental form of WHOIS.	4321	
SMTP	Monitors an SMTP server. SMTP servers are used to transfer Internet email.	25	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a successful banner.
SPOP3	A secure version of the POP3 mail protocol.	995	

Type	Purpose	Default port	Method
Telnet	Monitors a TELNET host, which allows users to log on and use the host services.	23	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a login prompt and responds to telnet escape codes.
Time	Monitors a Time server, which is used to return the current date and time.	13	
UUCP	Monitors a server used to automatically copy files from one Unix computer to another.	540	
WHO	Monitors a WHO server which provides information about a domain.	513	
WHOIS	Monitors a WHOIS server, which can tell users about a second-level domain name, such as the owner of the domain.	43	
Windows NT system monitors			
NT Service	Monitors a Windows NT service. If you are monitoring remote computers, the Windows API uses the SMB and/or RPC requests to operate.	None/SMB	If the service has the status RUNNING, its Alerting and Monitoring status is UP. Otherwise, the Alerting and Monitoring status is DOWN.

Type	Purpose	Default port	Method
NT EventLog	Watches for new entries matching user specified criteria in the NT Event log. You select the system, event source, and type. If you are monitoring remote computers, the Windows API uses the SMB and/or RPC requests to operate.	None/SMB	
NT Performance Data	Monitors the Windows NT performance data. If you are monitoring remote computers, the Windows API uses the SMB and/or RPC requests to operate.	None/SMB	
SNMP monitors			
SNMP Get	Monitors the value of a SNMP get request variable.	161	The get request is sent in by the SNMP manager to the SNMP agent.
SNMP Trap	Monitors an SNMP trap, which is sent from the SNMP agent to the SNMP manager.	162	The trap is used to monitor the agent and when the predefined value is reached, the trap is sent.
LAN computer monitors			
Windows System	Monitors presence and/or accessibility of a Windows Networking computer on your local network.	SMB	Uses windows networking to determine whether a computer is present / accessible.

Type	Purpose	Default port	Method
Netware Server	Monitors presence and/or accessibility of a Netware server on your local network.	SMB	<p>Uses windows networking to determine whether a computer is present / accessible.</p> <p>A valid Netware driver must be installed.</p>
Disk and file monitors			
File	Monitors a file to which you have access. When the file size or date stamp changes (or does not change), a response is sent. If you are monitoring remote computers, the Windows API uses the SMB and/or RPC requests to operate.	None/SMB	

Type	Purpose	Default port	Method
Log File	<p>Monitors a user specified log file for new entries matching user specified criteria. Generates an event when a new matching entry is found. This profile type can optionally register a down state when the specified log file is inaccessible. Many programs record relevant activity in a file called a log file. The application must allow other programs access to its log file between writes. Monitoring will not be possible if an application keep its log file(s) locked between writes.</p>	None/SMB	

Type	Purpose	Default port	Method
ODBC	Monitors a remote ODBC database sources. SQL Server and other ODBC data sources can be configured for a wide variety of protocol options. Port activity depends on the local configuration.	Depends on ODBC data source	
Disk Space	Monitors a drive on a computer. A response is sent if the minimum disk space specified can not be verified on the specified drive. If you are monitoring remote computers, the Windows API uses the SMB and/or RPC requests to operate.	None/SMB	
URL	Monitors a specified Web page or ftp file for availability/content.	TCP 80/ TCP 21	

Chapter 5

Filtering for Focused Reports

This chapter explains how to use filters to make your reports include only the data you need, while excluding the data you don't need. Filters are only available for General Firewall Activity, Incoming Firewall Activity, and Outgoing Firewall Activity profiles.

Filter Basics

When you configure a filter, you can specify one of two *filter types* and one or more *filter elements*.

Filter Types

There are two possible filter types: *Include* and *Exclude*. Include filters ensure that only activity in the log file that matches the criteria you have defined will be processed. Exclude filters ensure that all log file activity *except* the activity matching the criteria you specify will be processed.

For example, if you have a multi-home log file (one that crosses multiple domains) and you want to store activity for only one of its domains, you might create an include filter to include data for only one domain. If your multi-home log contains activity for three of your domains, and you want to store activity for two of them only, you might create an Exclude filter to exclude the domain you want to leave out.

Filter Elements

A filter element defines one of the criteria used for filtering.

For example, suppose the firewall log includes events for more than one firewall. If you wanted to filter the log file data to view only events related to one firewall, you could create an Include filter specifying that firewall. To do so, you would create an **Include** filter and select the **Firewall Name** filter element, specifying the name of the firewall you want to include.

You can find a complete list of available filter elements in “Filter Elements” on page 164. For a full description of each filter element, see “Filter Element Descriptions” on page 166.

Formatting Filter Element Criteria

Use a space to separate several entries.

Use quotation marks to enclose filter element criteria entries that contain spaces or commas. For example, the URL:

```
welcome to oregon.htm
```

looks like this as a filter element:

```
“welcome to oregon.htm”
```

Use wildcards to filter groups of items. For example, *.gif filters all files with a .gif extension, while image*.gif filters image1.gif, image2.gif, and so on.

Multi-Element Filters

You can also combine several filter elements in one filter. If Firewall Suite finds a match that meets all criteria, it returns the result to you and writes the result to the report.

For example, you can filter the data in the log files defined in the current profile for all activity related to the internal IP addresses you have defined, and at the same time, filter for the occurrence of a particular firewall rule.

In this case you would first select the Include filter type and the **Internal Address** filter element. You would then place an asterisk (*) in **the Internal Address** text box to indicate *all* internal addresses. See “Formatting Filter Element Criteria” on page 158. Next, you would select the **Rule** filter element. If Firewall Suite finds a match that meets both criteria, it returns the result to you and writes the result to the report.

When you select more than one filter element, Firewall Suite reads the elements as Boolean AND statements. For example, if Log File Activity matches Filter Element1 AND matches Filter Element2 AND... then include or exclude the result in the report.

Combining Multiple Filters

Firewall Suite lets you combine multiple filters in a profile. Multiple filters of the same type are processed with Boolean OR logic. This means that if the criteria of any one of the filters is met, the record is included in the report.

You can also combine include and exclude filters within a profile. The result of this combination is dependent on the sequence in which the filters are processed. Include filters are always processed first.

For example, you might want to look at all outgoing activity from your organization, except for that of users in the Finance department.

In this case, you would create an include filter that specifies to include all outbound activity using the **Traffic Direction** tab. You would then create a separate exclude filter that specifies to exclude the Finance department using the **Departments** tab. This assumes that you earlier defined the IP addresses associated with the Finance department of your organization. If Firewall Suite finds a match that meets both criteria, it returns the result to you and writes the result to the report.

The include filter selects all outgoing activity, and then the exclude filter filters out the Finance department users.

Tip

To create reports on a single log file using different sets of filters, you must use a separate profile for each set of filters. Use the Copy option on the File menu to copy a selected profile and modify it to specify the desired filter(s).

Working with Filters

This section provides step-by-step instructions for adding filters to profiles, modifying the settings for filters, and deleting filters.

Note

When you create a profile, the Include All filter is used by default. This filter processes and stores all log file data. To use your own filters, you must delete the Include All filter because it overrides all other filters.

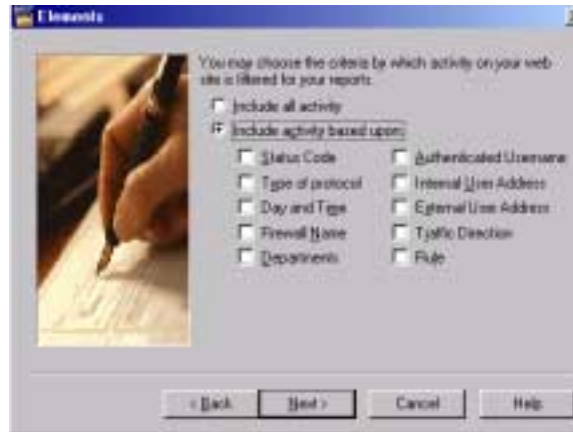
Adding a Filter to a Profile

To create a more focused report, you can add one or more filters to any profile.

To define a filter for a profile:

1. Select the profile that you want to filter in the Profile Description list of the Main Console.
2. Click **Edit**.
3. Select the **Filters** tab in the Edit Profile dialog box.
4. Select the Include Everything filter, and click **Delete**.
5. The Include All filter is selected by default. It overrides all other filters. For a new filter to take effect, you must delete the Include All filter.
6. Click **Yes** to confirm the deletion.

7. Click **New** to open the Type dialog box.
8. Choose whether to add an Include or Exclude filter.
9. Click **Next**. The Title dialog box opens.
10. In the **Name** text box, type a unique name to identify the filter in the **Filters** tab.
11. Click **Next**. The Elements dialog box opens.



12. Select the **Include (Exclude) activity based upon** option.
13. Select the check box for each filter element you want to include in this filter. The specific filter elements available vary according to whether you are using a general, incoming, or outgoing profile.
14. Click **Next** to display the individual dialog boxes in which you may configure the filter elements you selected. Enter the criteria for the activity you want to filter in this profile. See “Filter Element Descriptions” on page 166 for details about each filter element.

15. After you have defined the filter criteria in the Filter Elements dialog boxes, the Summary dialog box opens. Click **Back** if you need to back up and make adjustments.
16. Click **Finish** to return to the Edit Profile window.

Modifying a Filter

You can change the filter criteria if you want to change the results.

To modify a filter:

1. In the Profile Description list of the Main Console, select the profile that has the filter that you want to modify.
2. Click **Edit**. The Edit Filter dialog box opens.



3. Select the **Filters** tab, then select the filter that you want to modify.

4. Click **Edit**. The Filter Properties dialog box opens with the **General** tab selected. Select and clear the check boxes to add or remove filter elements. A tab will appear for each filter element that you select.
5. Select the filter elements tabs to make changes to the criteria of specific elements.
6. When you have made your changes, click **OK**.

Note

If you are using FastTrends technology, clear the existing database and update it after editing a filter.

Deleting a Filter

Firewall Suite looks for data that matches all the criteria you have defined through your filters. You can remove a filter from a profile if you no longer want to use it.

To delete a filter:

1. In the Profile Description list of the Main Console, select the profile that has the filter that you want to delete.
2. Click **Edit**.
3. Select the **Filters** tab in the Edit Profile window.
4. Select the name of the filter that you want to delete in the list of existing filters.
5. Click **Delete**.
6. When you are prompted to confirm your action, click **Yes** to delete the selected filter or **No** to continue without deleting the selected filter.

Filter Elements

Overview

The table lists each filter element, along with a short description of the filter criteria and the profile types with which the filter can be used.

Filter element	Specifies:	Profile types supported
Actions	Firewall actions based on categorization. Only for firewalls using WELF format.	Actions
Authenticated Username	Authenticated users. This filter is useful if your Web site requires visitors to log on with a user names and password.	Authenticated Username
Browser	Spider or robot.	Browser
Category	Web site content.	Category
Day and Time	Hour of the day for each day of the week.	General Incoming Outgoing
Department	Departments in your organization, broken down by domain name.	General Outgoing
Directory	A particular directory on your Web site.	Incoming
External User Address	Specific domains or IP addresses coming from outside the firewall.	General
File	A particular file name or type on your Web site, for example .gif.	Incoming Outgoing
Firewall Actions	Check Point VPN-1/Firewall-1 actions. Actions can include responses to logon attempts or data transfers.	General (Check Point VPN-1/ Firewall-1 only)

Filter element	Specifies:	Profile types supported
Firewall Name	Activity for a specific firewall. This is useful if your firewall log file includes events for more than one firewall.	General
Internal User Address	Hits from specific domains or IP addresses behind the firewall.	General
Multi Homed Domain	Domains.	Incoming
Proxy Cache	Codes associated with the request.	Outgoing
Referrer	Entire user session coming from the specified referrers. Using this, you can establish the effectiveness of your Internet advertising.	Incoming
Return Code	Browser return codes. The log file records the results received from browsers, which are called return codes.	Incoming
Rule	Specific firewall rule. A rule identifies what activities and protocols are allowed through the firewall. They are usually identified by a number and vary from firewall to firewall.	General
Sites	A specific Web site or group of sites to include or exclude in your report (for example *.edu).	Outgoing
Status Codes	Status codes. These are numeric responses to attempts made to logon to the network to perform an activity or access a service.	General
Traffic Direction	Where the activity was initiated. This can be either <i>inbound</i> or <i>outbound</i> .	General

Filter element	Specifies:	Profile types supported
Type of Traffic	Protocols associated with traffic.	General
User Address or Country	Domains, IP addresses, or countries from the results of this profile.	Incoming
Users by IP	Activity of specific computers according to their IP address.	Outgoing

Filter Element Descriptions

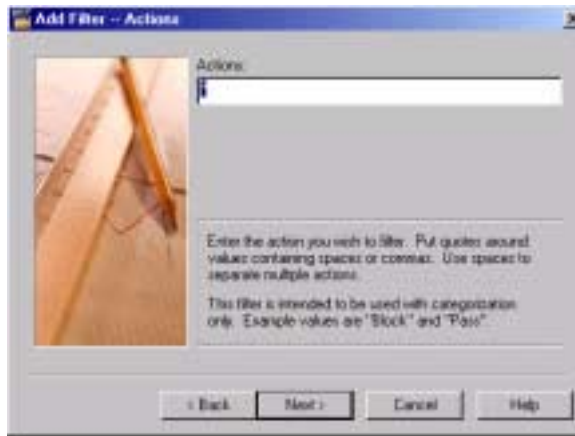
Actions

The actions filter relates to URL categorization and is only available for firewalls using WELF format. Based on how a site is categorized, a firewall may block that site or allow access to it. The firewall logs the action of attempting to visit a blocked site as well as the action of visiting an approved (or passed) site.

The Actions filter element includes data on those firewall actions in the report, or excludes that data from the report.

Note

The Actions filter element is available only for firewalls using WELF format.



To add an Actions filter element:

1. The default includes both possible values (*) and reports all visits. If you do not want to accept the default, type one of the following:
 - **Block** reports the attempts to visit blocked sites.
 - **Pass** reports visits to all other sites, including non-categorized sites.
2. Click **Next**.

Authenticated Username

If you have a secure site that requires visitors to log on with a user name and password, you can use the Authenticated Username filter element to include or exclude authenticated users from the report. Use quotations mark around any authenticated user name that includes a space. For example, type `janesmith` to filter the authenticated user `janesmith`, but type `"Jane Smith"` to filter the authenticated user `Jane Smith`.



To include or exclude all authenticated user names:

1. Select **Include** or **Exclude Only Authenticated Users**.
2. Click **Next**.

To include (exclude) specific authenticated user names:

1. In the **Authenticated Username** text box, type the names you want to filter. Put quotation marks around names that contain spaces. Separate individual entries with spaces. Select the **Case Sensitive** check box if you want to look for exact case matches. Most servers do not require case-sensitive matches.
2. Click **Next**.

Browser

Use the Browser filter element to either include or exclude a browser, spider or robot from the report. You can filter for any browser if you know how it appears in the agent field of the log file.

To define a Browser filter element:

1. In the **Browsers** text box, type the name of the browser you want to filter as it appears in the log file, or use the dropdown list to select common browsers, spiders, and robots. Use a space to separate multiple browsers. Use quotation marks to surround browser names that contain spaces. For example, type "Microsoft Internet Explorer/4." to include or exclude any activity that matches Internet Explorer v4.x.

Wildcards are not supported for Browser filters. Firewall Suite assumes that wildcards at either end of each browser entry when comparing it to the agent field in the log file.

Note

Filtering for Netscape Navigator may not return accurate results because many browsers identify themselves as Netscape Navigator.

2. Click **Next**.

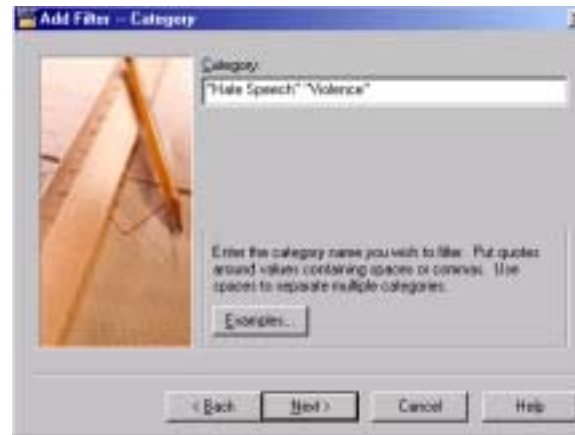
Category

Use the Category filter element to include or exclude information in your reports about sites visited by users from inside your organization. You can monitor Internet usage by category for bandwidth, productivity, and liability concerns.

The Category filter element lets you generate a report for all activity related to categorized sites, or limit the reports to specified categories.

Note

The categories available for filtering depend on the category databases that you download. Click **Examples** in the Add Filter—Category dialog box for a list.



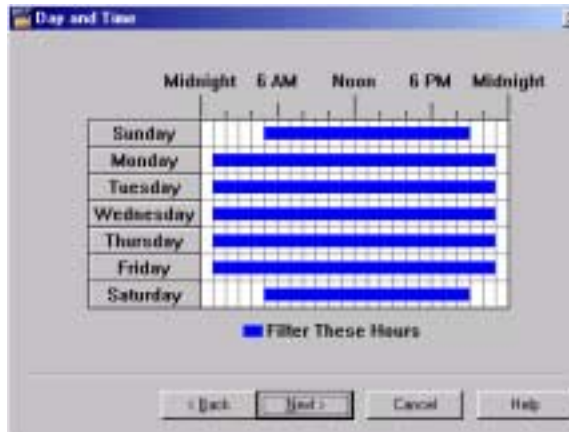
To define a Category filter element:

- 1.** In the **Category** text box, type the names of the categories that you want to include or exclude in your reports. The default is to filter all categories
 - Separate categories with spaces.
 - Put quotation marks around categories that contain spaces or commas.
- 2.** Click **Next**.

See “URL Categorization” on page 50 for more information about categories and category databases.

Day and Time

The Day and Time filter element includes or excludes activity according to the day of the week and the time of day.

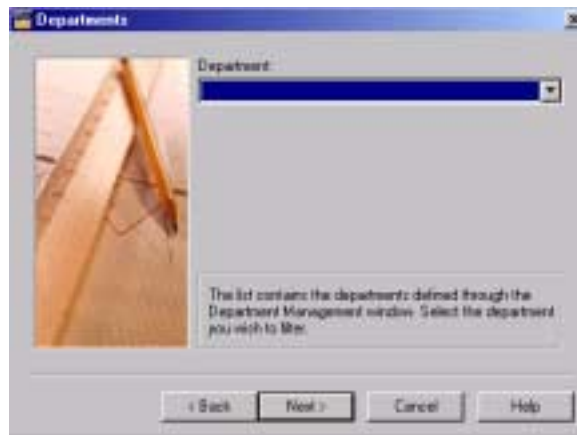


To define a Day and Time filter element:

1. Click on boxes, or drag rows or columns to select them. A blue box indicates an hour is selected. The figure shows Monday through Friday, 8:00 a.m. to 5:00 p.m. selected.
2. Click **Next**.

Departments

The Departments filter element includes or excludes departments from your analysis and reporting. For example, you can find out which department is using the Internet the most.



To define a Departments filter element:

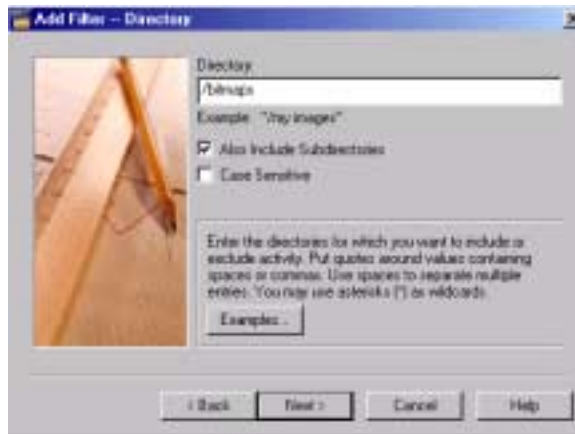
1. Use the **Department** dropdown list to select the department that you want to include or exclude.

Any departments already defined using the Department Management dialog box appear in the dropdown list. See “Using Department Management” on page 90 for information about setting up departments.

2. Click **Next**.

Directory

Use the Directory dialog box to include or exclude the activity of a specific directory.



To define a Directory filter element:

1. In the **Directory** text box, type the path for the directory to be filtered. Use wildcards to specify multiple directories. Separate directories with a space. Put quotation marks around directory names that contain spaces. For more information, see the table of Directory filter examples.

By default, an include directory filter element includes all directories starting at the root directory, indicated by a slash (/) in the **Directory** text box. There is no default for an exclude directory filter.

2. If you do not want to include or exclude all subdirectories, clear the **Also Include/Exclude Subdirectories** check box. Otherwise, Firewall Suite will activate the subdirectories by default.
3. Select the **Case Sensitive** check box to look for exact case matches. Most servers do not require case-sensitive matches.
4. Click **Next**.

The following table shows examples of Directory filter definitions.

Example	Result
/images	Specifies the directory /images is to be included or excluded. If Include Subdirectories is selected, all subdirectories of /images will also be included or excluded.
"/image files"	Specifies the long directory /image files.
"/image files" / intranet /graphics	Specifies the directories /image files, /intranet, and /graphics.
/*graphics	Specifies any first-level directory whose name ends in graphics, such as /bitmap graphics, but not /intranet/bitmap graphics.
/*/graphics	Specifies all second-level directories named /graphics, such as /home/graphics and /intranet/graphics, but not /home/sales/graphics. Includes directories such as /home/graphics/logos only if Include Subdirectories is selected.
/graphics /*/ graphics /*/*/ graphics	Specifies all first-, second-, and third-level directories named graphics, such as /graphics, /home/graphics, and /home/sales/graphics. Includes subdirectories such as /home/graphics/logos and /home/sales/graphics/logos/specials only if Include Subdirectories is selected.
/*graphics*/	Specifies all first-level directories with names containing graphics, such as /graphics, /graphics files, and /bitmap graphics.

External User Address

Use the External User Address filter element to include or exclude activity from specific domains or IP addresses *outside* the firewall. For example, you can create a filter that includes activity from a questionable IP address if you think someone is trying to break into your firewall.



To define an External User Address filter element:

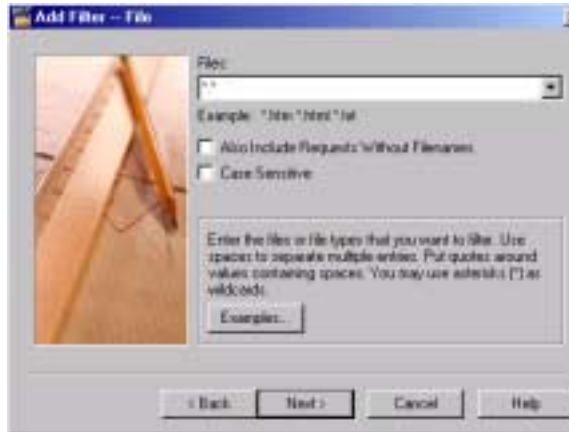
1. In the **External User Address** box, type the user addresses that you want to specify, or use the dropdown list to select a predefined user address. The default setting is All User Addresses (*).
2. Click **Next**.

The following table shows examples of how to specify user addresses.

Example	Result
204.245.240.0-63	Specifies all numeric IP addresses from 204.245.240.0 through 204.245.240.63
204.245.240.0-204.245.240.64	Specifies all numeric IP addresses from 204.245.240.0 through 204.245.240.64
204.245.240.64/26	CIDR notation. Specifies all addresses of the classless subnet: 204.245.240.64 - 204.245.240.127.
111.92.76.0/26	Specifies all subnet addresses from 111.92.76.0 through 111.92.76.63.
*.webTrends.com	Only those addresses with a subdomain that appears to the left of this domain, for example www.WebTrends.com and ftp.WebTrends.com. Excludes addresses without a subdomain.
*webTrends.com	Any address that includes the specified domain, with or without a subdomain, for example www.WebTrends.com, ftp.WebTrends.com, or WebTrends.com. Tip: You can specify IP addresses as well as domain names in filter text boxes if you are uncertain whether DNS lookups are being performed.
*.edu *.com *.net	All addresses that have the domain types edu, com, or net.
*.de	All addresses from Germany.
www.*	Only those addresses that have www as a subdomain.

File

Use the File filter element to include or exclude specific files.



To define a File filter element:

1. In the **Files** text box, type the file name or extension, or select a file type from the dropdown list. Use wildcard characters to specify file names or extensions, such as all HTML files (*.htm) or all GIF files (*.gif). You can specify several file types at once by inserting a space between each file type.

The default for an Include files filter element is to include all files, indicated by *.* in the **Files** text box. There is no default for an exclude filter.

2. Select the **Also Include Requests Without Filenames** check box to include activity in which no filenames are specified. For example, if a visitor to your site accesses `http://www.mydomain.com`, the Web server may log this hit without a file name, but return the file `http://www.mydomain.com.default.htm`.

Note

If you used the default setting for your filter, selecting the **Also Include Requests Without Filenames** check box has no effect.
