GFI Product Manual

# **GFI Web**Monitor<sup>™</sup>

Administrator Guide for ISA/TMG





The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

All product and company names herein may be trademarks of their respective owners. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

GFI WebMonitor is copyright of GFI SOFTWARE Ltd. - 1999-2012 GFI Software Ltd. All rights reserved.

Document Version: 1.2.2

Last updated (month/day/year): 8/27/2012

## Contents

1 Introduction	10
1.1 About This Guide	10
1.1.1 Terms Used in This Manual	10
1.1.2 Terms and Conventions Used in This Guide	10
1.2 About GFI WebMonitor	10
1.3 How Does GFI WebMonitor Work?	11
1.3.1 Downloading GFI WebMonitor	13
1.3.2 Licensing Information	13
1.3.3 Upgrading	13
1.4 GFI WebMonitor Services	13
2 Installing GFI WebMonitor	16
2.1 System Requirements	16
2.1.1 Software	16
2.1.2 Hardware	16
2.1.3 Microsoft® ISA / Forefront TMG Mode Pre-requisites	17
2.2 Deployment Scenarios	17
2.2.1 Deployment in a Microsoft ISA Server or Forefront TMG Environment	18
2.3 Installing GFI WebMonitor for IsaTmg	19
2.3.1 Introduction	19
2.3.2 Installation Procedure	19
3 Post Installation Actions	22
3.1 Launching GEL WebMonitor	22
3.2 Enter a Valid License Key	23
3.3 Configure Proxy Settings	23
3.4 Configuring FTP	0
3.4.1 Step 1: Disabling Folder View in Microsoft Internet Explorer	
3.4.2 Step 2: Configuring Browsers to Use a Proxy Server	25
3.4.3 Option 2: Configuring Proxy settings manually	25
3.4.4 Option 1: Configuring Proxy settings automatically in Microsoft® ISA Server and	
Microsoft® Forefront TMG	26
3.4.5 Step 3: Configuring FTP access	29
3.4.6 Option 1: Restricting or denying FTP access in Microsoft ISA Server or Microsoft	
Forefront TMG	32
3.5 Using the Settings Importer Tool	37
3.5.1 Exporting / Importing Configuration Settings	37
4 Achieving Results	40
4.1 Achieving Results with GFI WebMonitor - Protecting Your Network	40
4.2 Achieving Results with GFI WebMonitor - Maximize Bandwidth Availability	41
4.3 Achieving Results with GFI WebMonitor - Increase Productivity	42
5 Using the Dashboard	44
5.1 Overview of Internet Activity	44

	46
5.1.2 Pending Task List	46
5.1.3 Web Monitoring Status	47
5.1.4 Product Status	
5.2 Monitoring Bandwidth	
5.2.1 One-click Report Functionality	
5.3 Monitoring Activity	
5.3.1 One-click Report Functionality	
5.4 Monitoring Security	54
5.4.1 One-click Report Functionality	
5.5 Monitoring Real-Time Traffic	
5.6 Using Quarantine	
6 Reporting	60
( A Channel Descente	
6.1 Starred Reports	
6.2 Activity Reports	
6.2.1 Editing Activity Reports	
6.3 Bandwidth Reports	
6.3.1 Editing Bandwidth Reports	
6.4 Security Reports	
6.4.1 Editing Security Reports	67
6.4.2 Cloning Reports	68
7 Configuring GFI WebMonitor	
7.1 General Settings	
/.1.1 Updating License Manually	70
<ul><li>7.1.1 Updating License Manually</li><li>7.1.2 Remote Access Control</li></ul>	70 71
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> </ul>	70 71 74
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> </ul>	
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> </ul>	
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> </ul>	
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> </ul>	70 71 74 75 77 77 78 79
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> </ul>	
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> <li>7.2.2 Configuring Internet Policies</li> </ul>	70 71 74 75 77 78 79 80 80
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> <li>7.2.2 Configuring Internet Policies</li> <li>7.2.3 Configuring Always Blocked List</li> </ul>	
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> <li>7.2.2 Configuring Internet Policies</li> <li>7.2.3 Configuring Always Blocked List</li> <li>7.2.4 Deleting Items From the Always Blocked list</li> </ul>	70 71 74 75 77 78 79 80 80 80 80 80 89 90
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> <li>7.2.2 Configuring Internet Policies</li> <li>7.2.3 Configuring Always Blocked List</li> <li>7.2.4 Deleting Items From the Always Blocked list</li> <li>7.2.5 Configuring Always Allowed List</li> </ul>	70 71 74 75 75 77 78 79 80 80 80 80 80 80 89 90
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> <li>7.2.2 Configuring Internet Policies</li> <li>7.2.3 Configuring Always Blocked List</li> <li>7.2.4 Deleting Items From the Always Blocked list</li> <li>7.2.5 Configuring Always Allowed List</li> <li>7.2.6 Configuring Temporary Allowed List</li> </ul>	70 71 74 75 77 78 79 80 80 80 80 80 80 80 80 80 80 80 80 80
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> <li>7.2.2 Configuring Internet Policies</li> <li>7.2.3 Configuring Always Blocked List</li> <li>7.2.4 Deleting Items From the Always Blocked list</li> <li>7.2.5 Configuring Always Allowed List</li> <li>7.2.6 Configuring Temporary Allowed List</li> <li>7.2.7 WebSecurity Edition Policies</li> </ul>	70 71 74 75 75 77 78 79 80 80 80 80 80 80 80 80 80 80 80 80 80
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> <li>7.2.2 Configuring Internet Policies</li> <li>7.2.3 Configuring Always Blocked List</li> <li>7.2.4 Deleting Items From the Always Blocked list</li> <li>7.2.5 Configuring Temporary Allowed List</li> <li>7.2.7 WebSecurity Edition Policies</li> <li>7.2.8 Configuring Security Policies</li> </ul>	70 71 74 75 77 78 79 80 80 80 80 80 80 90 91 91 93 94 94
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> <li>7.2.2 Configuring Internet Policies</li> <li>7.2.3 Configuring Always Blocked List</li> <li>7.2.4 Deleting Items From the Always Blocked list</li> <li>7.2.5 Configuring Temporary Allowed List</li> <li>7.2.7 WebSecurity Edition Policies</li> <li>7.2.8 Configuring Security Policies</li> <li>7.2.9 Adding a New Security Policy</li> </ul>	70 71 74 75 75 77 78 78 79 80 80 80 80 80 80 80 80 80 80 80 80 80
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> <li>7.2.2 Configuring Internet Policies</li> <li>7.2.3 Configuring Always Blocked List</li> <li>7.2.4 Deleting Items From the Always Blocked list</li> <li>7.2.5 Configuring Temporary Allowed List</li> <li>7.2.7 WebSecurity Edition Policies</li> <li>7.2.8 Configuring Security Policies</li> <li>7.2.9 Adding a New Security Policy</li> <li>7.2.10 Configuring Security Engines</li> </ul>	70 71 74 75 77 78 79 80 80 80 80 80 80 80 80 80 80 80 80 80
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> <li>7.2.2 Configuring Internet Policies</li> <li>7.2.3 Configuring Always Blocked List</li> <li>7.2.4 Deleting Items From the Always Blocked list</li> <li>7.2.5 Configuring Temporary Allowed List</li> <li>7.2.7 WebSecurity Edition Policies</li> <li>7.2.8 Configuring Security Policies</li> <li>7.2.9 Adding a New Security Policy</li> <li>7.2.10 Configuring Security Engines</li> <li>7.2.11 Configuring Kaspersky</li> </ul>	70 71 74 75 75 77 78 79 80 80 80 80 80 80 80 80 80 80 80 80 80
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> <li>7.2.2 Configuring Internet Policies</li> <li>7.2.3 Configuring Always Blocked List</li> <li>7.2.4 Deleting Items From the Always Blocked list</li> <li>7.2.5 Configuring Temporary Allowed List</li> <li>7.2.6 Configuring Security Policies</li> <li>7.2.8 Configuring Security Policies</li> <li>7.2.9 Adding a New Security Policy</li> <li>7.2.10 Configuring Kaspersky</li> <li>7.2.12 Configuring Anti Phishing Notifications</li> </ul>	70 71 74 75 77 78 79 80 80 80 80 80 80 89 90 91 91 93 93 94 94 97 100 101
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> <li>7.2.2 Configuring Internet Policies</li> <li>7.2.3 Configuring Always Blocked List</li> <li>7.2.4 Deleting Items From the Always Blocked list</li> <li>7.2.5 Configuring Temporary Allowed List</li> <li>7.2.6 Configuring Security Policies</li> <li>7.2.8 Configuring Security Policies</li> <li>7.2.9 Adding a New Security Policies</li> <li>7.2.10 Configuring Kaspersky</li> <li>7.2.12 Configuring Anti Phishing Notifications</li> <li>7.2.13 Configuring ThreatTrack</li> </ul>	70 71 74 75 75 77 78 79 80 80 80 80 80 80 80 80 80 80 80 80 80
<ul> <li>7.1.1 Updating License Manually</li> <li>7.1.2 Remote Access Control</li> <li>7.1.3 Configuring Auto-Update</li> <li>7.1.4 Configuring Databases</li> <li>7.1.5 Configuring Notifications</li> <li>7.1.6 Configuring Web Categorization</li> <li>7.2 Configuring Policies</li> <li>7.2.1 WebFilter Edition Policies</li> <li>7.2.2 Configuring Internet Policies</li> <li>7.2.3 Configuring Always Blocked List</li> <li>7.2.4 Deleting Items From the Always Blocked list</li> <li>7.2.5 Configuring Temporary Allowed List</li> <li>7.2.7 WebSecurity Edition Policies</li> <li>7.2.8 Configuring Security Policies</li> <li>7.2.9 Adding a New Security Policies</li> <li>7.2.10 Configuring Security Engines</li> <li>7.2.11 Configuring Mati Phishing Notifications</li> <li>7.2.13 Configuring ThreatTrack</li> <li>7.2.14 Configuring Download Policies</li> </ul>	70 71 74 75 75 77 78 78 79 80 80 80 80 80 80 90 91 91 93 93 94 94 97 100 101 101 101 102 103

7.3.1 Configuring Monitoring Alerts	106
7.3.2 Configuring Bandwidth Alerts	108
7.3.3 Configuring Security Alerts	109
8 Troubleshooting and support	112
8.1 Introduction	112
8.2 GFI SkyNet	112
8.3 Web Forum	112
8.4 Request Technical Support	112
8.5 Documentation	112
8.6 Common Issues	113
9 Glossary	115
10 Appendix 1	121
10.1 Assigning Log On As A Service Rights	121
10.2 Configuring Routing and Remote Access	126
10.3 Disabling Internet Connection Settings On Client Machines	127
10.3.1 Disabling Internet Connections Page Using GPO in Windows® Server 2003	127
10.3.2 Disabling Internet Connections Page Using GPO in Windows® Server 2008	130
10.4 Uninstall Information	133
11 Index	134

## List of Figures

Screenshot 1: GFI WebMonitor Services	15
Screenshot 2: GFI WebMonitor installed on Microsoft ISA Server / Forefront TMG	
Screenshot 3: Installation: Access Permissions	
Screenshot 4: Installation: Service Logon Information	
Screenshot 5: Installation: Mail Settings	21
Screenshot 6: License key required	23
Screenshot 7: Internet Options dialog box	
Screenshot 8: LAN Settings dialog	26
Screenshot 9: Microsoft Firewall Client for ISA Server: Installation wizard dialog	
Screenshot 10: Microsoft® Firewall Client for ISA Server: Settings tab	
Screenshot 11: Microsoft® Firewall Client for Forefront TMG: Installation wizard dialog	
Screenshot 12: Microsoft ISA Server 2004: Configured Application filters	30
Screenshot 13: Microsoft ISA Server 2006: Configured Application filters	31
Screenshot 14: Microsoft Forefront TMG: Configured Application filters	32
Screenshot 15: Microsoft ISA Server: Configured Firewall policies	33
Screenshot 16: Microsoft ISA Server: Protocols dialog	
Screenshot 17: Microsoft ISA Server: Add Users dialog	
Screenshot 18: Microsoft Forefront TMG: Protocols dialog	35
Screenshot 19: Microsoft Forefront TMG: Access Rule Sources dialog	
Screenshot 20: Microsoft ISA Server: Add Users dialog	
Screenshot 21: Settings Importer Tool Controls	
Screenshot 22: Dashboard Overview	45
Screenshot 23: Using the calendar to set period	
Screenshot 24: Website Category Lookup feature	46
Screenshot 25: Pending tasks list	47
Screenshot 26: Dashboard Overview statistical information	
Screenshot 27: Dashboard Overview product status	48
Screenshot 28: Monitoring bandwidth	50
Screenshot 29: Activity Dashboard	52
Screenshot 30: Security Dashboard	55
Screenshot 31: Real-Time Traffic Dashboard, Bandwidth monitoring	57
Screenshot 32: Quarantine dashboard	
Screenshot 33: Default activity report list	61
Screenshot 34: Editing a report	62
Screenshot 35: Scheduling an activity report	63
Screenshot 36: Default bandwidth reports list	64
Screenshot 37: Editing a report	64
Screenshot 38: Scheduling an activity report	65

Screenshot 39: Default Security reports list	66
Screenshot 40: Editing a report	67
Screenshot 41: Scheduling an activity report	68
Screenshot 42: Configuring Access Control	72
Screenshot 43: Adding a new Authorization Rule	73
Screenshot 44: Configuring Auto-update	74
Screenshot 45: Configured database	75
Screenshot 46: Configuring Databases	76
Screenshot 47: Configuring administrative notifications	78
Screenshot 48: Configuring Web Categorization	79
Screenshot 49: Creating a new Web Filtering policy	81
Screenshot 50: Enabling reputation filtering	82
Screenshot 51: Creating a new Web Browsing Quota Policy	83
Screenshot 52: Creating a new IM Policy	85
Screenshot 53: Configuring Streaming Media policy 1	87
Screenshot 54: Safe Search and Search Terms Monitoring	88
Screenshot 55: Configuring Always Blocked list	90
Screenshot 56: Adding items to Always Allowed list	92
Screenshot 57: Configuring Temporary Allowed list	93
Screenshot 58: Configuring Default Virus Scanning Policy	95
Screenshot 59: Creating a new Security Policy	98
Screenshot 60: Configuring Security Engines	100
Screenshot 61: Configuring Kaspersky security engine	101
Screenshot 62: Configuring ThreatTrack notifications	102
Screenshot 63: New download policy	104
Screenshot 64: Configuring Monitoring alerts	107
Screenshot 65: Configuring Bandwidth alerts	108
Screenshot 66: Configuring Security alerts	110
Screenshot 67: Microsoft Windows Server: Local Security Policy window	. 122
Screenshot 68: Active Directory GPO dialog	123
Screenshot 69: GPO Editor window	124
Screenshot 70: Add/Remove Snap-ins window	125
Screenshot 71: Console Root domain window	. 125
Screenshot 72: Group Policy Management Editor window	126
Screenshot 73: Microsoft Windows Server 2003: Routing and Remote Access Server Setup Wizard dialog .	127
Screenshot 74: Active Directory GPO dialog	128
Screenshot 75: GPO Editor window	129
Screenshot 76: Disable the Connection page Properties dialog	130
Screenshot 77: Add/Remove Snap-ins window	131
Screenshot 78: Console Root domain window	131

Screenshot 79: Group Policy Management Editor window	132
Screenshot 80: Disable the Connection page Properties dialog	132

## List of Tables

Table 1: Terms and conventions used in this manual	10
Table 2: GFI WebMonitor Editions	10
Table 3: Always Blocked/Always Allowed filtering actions	12
Table 4: GFI WebMonitor Windows® Services	13
Table 5: Software requirements	16
Table 6: Hardware requirements	16
Table 7: Monitoring tools	44
Table 8: Product status overview	
Table 9: Bandwidth dashboard options	
Table 10: Bandwidth monitoring filtering options	
Table 11: Export report options	51
Table 12: Activity dashboard options	51
Table 13: Activity monitoring filtering options	
Table 14: Export report options	53
Table 15: Security dashboard options	54
Table 16: Security monitoring filtering options	
Table 17: Export report options	
Table 18: Real-Time Traffic dashboard options	57
Table 19: Quarantine options	58
Table 20: Activity report schedule options	
Table 21: Activity report distribution options	63
Table 22: Activity report schedule options	
Table 23: Activity report distribution options	
Table 24: Activity report schedule options	
Table 25: Activity report distribution options	
Table 26: General Settings	70
Table 27: Back-end databases	75
Table 28: SQL Server® Authentication method	77
Table 29: Configuring administrative notifications	78
Table 30: Reputation index classification	82
Table 31: Scanning options	
Table 32: Scanning options	
Table 33: Kaspersky engine options	101
Table 34: Filtering options	104
Table 35: Bandwidth alert trigger options	109
Table 36: Bandwidth alerts filtering options	109
Table 37: Security alerts trigger options	110
Table 38: Common troubleshooting issues	

## 1 Introduction

GFI WebMonitor<sup>®</sup> is a comprehensive Internet usage monitoring solution that enables you to monitor and filter Web browsing and file downloads in real-time. It also enables you to optimize bandwidth by limiting access to streaming media, while enhancing network security with built-in tools that scan traffic for viruses, trojans, spyware and phishing material.

It is the ideal solution to transparently and seamlessly exercise a substantial degree of control over your network users' browsing and downloading habits. At the same time, it enables you to ensure legal liability and best practice initiatives without alienating network users.

## 1.1 About This Guide

The aim of this guide is to help System Administrators install, configure and run GFI WebMonitor with minimum effort. It describes:

- » The various network environments that GFI WebMonitor can support
- » How to install GFI WebMonitor to monitor your environment
- » How to get GFI WebMonitor running on default settings
- » How to configure GFI WebMonitor to achieve results.

## 1.1.1 Terms Used in This Manual

The following terms are used in this manual:

## 1.1.2 Terms and Conventions Used in This Guide

TERM	DESCRIPTION
0	Additional information and references essential for the operation of GFI WebMonitor.
	Important notifications and cautions regarding potential issues that are commonly encountered.
>	Step by step navigational instructions to access a specific function.
Bold text	Items to select such as nodes, menu options or command buttons.
Italics text	Parameters and values that you must replace with the applicable value, such as custom paths and fil- enames.
Code	Indicates text values to key in, such as commands and addresses.

For any technical terms and their definitions, refer to the Glossary section in this manual.

## 1.2 About GFI WebMonitor

GFI WebMonitor is available in three editions:

EDITION	DESCRIPTION	
WebFilter Edition	Increases productivity with Web Filtering and Web Browsing policies. Helps to optimize bandwidth use with Streaming Media policies and website categorization features. Additionally, Web Reputation Index and ThreatTrack help lower incidence of attacks and infringements.	
WebSecurity Edition	Provides a high degree of web security using combined tools that help mitigate phish- ing, malware, trojans and virus attacks. This is achieved through the built-in down- load control module and multiple anti-virus and anti-spyware engines.	

Table 2: GFI WebMonitor Editions

EDITION	DESCRIPTION
Unified Protection Edition	Provides all the features of the WebFilter Edition and the WebSecurity Edition in a single package.

## 1.3 How Does GFI WebMonitor Work?



**1. Request initiation:** User requests a webpage or a download from the Internet. Incoming traffic generated by this request is forwarded to GFI WebMonitor.

**2. Always Blocked/Always Allowed filtering:** The internal GFI WebMonitor Always Blocked/Always Allowed filtering mechanism analyzes user ID, IP address and requested URL, taking the following actions:

 Table 3: Always Blocked/Always Allowed filtering actions

ACTION	DESCRIPTION
Blocks web traffic requests	» by adding users and/or IP addresses to the Always Blocked list, or
	* to access URLs in the Always Blocked list
Automatically allows web traffic	» by allowed users and/or IP addresses, or
requests	» to access allowed URLs
Forwards web traffic requests (to the WebFiltering module)	by users and/or IP addresses that are neither in the Always Blocked list nor in the Always Allowed list
	to access URLs that are neither in the Always Blocked list nor in the Always Allowed list.

**3. WebFilter module**: Analyzes web traffic received from the Always Blocked/Always Allowed filtering mechanism against a list of categories stored in WebGrade database. These categories are used to classify and then filter web pages requested by users.

For more information about these categories, refer to Knowledge Base article: <a href="http://go.gfi.com/?pageid=WebMon\_WebGrade">http://go.gfi.com/?pageid=WebMon\_WebGrade</a>.

GFI WebMonitor can Block, Warn and Allow or Quarantine web traffic according to configured policies. Quarantined web traffic can be manually approved or rejected by the administrators. Approved quarantined URLs are moved in **Temporary Allowed** area; a mechanism used to approve access to a site for a user or IP address for a temporary period.

## NOTE

The WebFilter module is only available in the **WebFilter Edition** and the **Unified Protection Edition** of GFI WebMonitor. In the **WebSecurity Edition**, web traffic is sent directly from the **Always Allowed/Always Blocked** filtering mechanism to the WebSecurity module.

**4. WebSecurity module**: Analyzes web traffic through the download control module and scans incoming web traffic for viruses, spyware and other malware.

GFI WebMonitor can Block, Warn and Allow or Quarantine suspicious material according to configured policies. Web traffic is also scanned for phishing material against a list of phishing sites stored in the updatable database of phishing sites. Web traffic generated from a known phishing element is rejected while approved web material is forwarded to the user.

## 🚹 NOTE

The WebSecurity module is only available in the WebSecurity Edition and Unified Protection Edition of GFI WebMonitor. In the WebFilter Edition, WebSecurity processing is not performed, and web traffic is forwarded on to the user.

## IMPORTANT

Forwarding of approved web material by GFI WebMonitor to the user depends on the network environment; that is, where GFI WebMonitor is installed.

## 1.3.1 Downloading GFI WebMonitor

GFI WebMonitor can be downloaded from: <u>http://go.gfi.com/?pageid=WebMon\_Download</u>.

## 1.3.2 Licensing Information

GFI WebMonitor counts either users or IP addresses for licensing purposes. You can configure a list of users or IP addresses who do not need to be monitored or protected so that these users do not consume a license. For more information, refer to <u>Configuring Always Allowed List</u> (page 91).

## IMPORTANT

Unlicensed users are automatically allowed unrestricted and unfiltered access to the Internet. The traffic generated by these clients will not be monitored. For more information on how GFI WebMonitor counts users for licensing purposes, refer to Knowledge Base article: http://go.gfi.com/?pageid=WebMon\_Licensing.

For more information about licensing, refer to GFI Software Ltd. website at: <a href="http://go.gfi.com/?pageid=WebMon\_LicensingInformation">http://go.gfi.com/?pageid=WebMon\_LicensingInformation</a>

## 1.3.3 Upgrading

In order to upgrade GFI WebMonitor, obtain the latest version from <a href="http://www.gfi.com/pages/webmon-selection-download.asp">http://www.gfi.com/pages/webmon-selection-download.asp</a>.



The upgrade procedure is similar to the installation procedure.

## 🚹 NOTE

If installing a new version of GFI WebMonitor on a different infrastructure, it is recommended to uninstall the previous version before installing the new one.

## **1.4 GFI WebMonitor Services**

The table below lists Windows® services used by GFI WebMonitor.

Table 4: GFI WebMonitor Windows $^{ extsf{B}}$  Services

SERVICE NAME	DESCRIPTION	LOCATION AND NAME	USER CRE- DEN- TIALS
GFI Proxy	The GFI Proxy service is only created in the Standalone Proxy Version of GFI WebMonitor. It is used as an agent service for the Proxy server, ISAPI module and Web Filtering.	<drive>:\Program Files\GFI\W- ebMonitor\GFiProxy.exe</drive>	Local Sys- tem

SERVICE NAME	DESCRIPTION	LOCATION AND NAME	USER CRE- DEN- TIALS
GFI Web- Monitor	<ul> <li>The GFI WebMonitor service is used in both the ISA/TMG version and the Standalone Proxy version as a worker service. Its functionality includes:</li> <li>Scanning downloads via AV scanning engines.</li> <li>Managing content updates for the various GFI WebMonitor modules.</li> <li>Sending notification emails to administrator and users.</li> <li>Provide services used to host admin UI.</li> <li>Loading WebGrade database to memory</li> </ul>	<drive>:\Program Files\GFI\W- ebMonitor\WMonSrv.exe</drive>	Admin- istrator
GFI Web- Monitor Core Service	<ul> <li>The GFI WebMonitor Core Service is composed by the following different components:</li> <li>WebMon.Common - Common data structures and algorithms</li> <li>WebMon.Core - Starts/Stops the IIS express process, Hosts the WCF services (AlertingService, AutoUpdateSettingsService, CategoryService, DataImporterService, DataLayerService, EngineStatusService, GeneralSettingsService, LicensingService, NetworkService, PolicySettingsService, ProxySettingsService, QuarantineService, ReporterService, ReportSettingsService, WebBrowsingService)</li> <li>WebMon.ConfigManager - Handles the configurations files (config.db &amp; xml settings)</li> <li>WebMon.Dal - Data persistence (FB &amp; SQL Server) &amp; data maintenance</li> <li>WebMon.DataAnonymizer - All data before going to the UI si filtered through this module</li> <li>WebMon.FilterComm - Used for communication with the WebMonitor filter (e.g. reload of the settings, real time traffic,)</li> <li>WebMon.MessageCollector - Reads the data from MSMQ sends it to the Alerter and SearchTerms modules for processing. Uses a new MSMQ queue to stock up to X requests or 1 min until they are send to the database, MSMQ is transactional and if the db is temporary offline no data will be lost</li> <li>WebMon.Net - Network related functionality (i.e. enumeration of sql servers or users from domains)</li> <li>WebMon.Scheduler - Schedules general purposes tasks like database maintenance, or scheduled reports</li> <li>WebMon.SearchTerms - Processes the data received from the filter and triggers the alerts, also responsible for sending email notifications generated by the core service</li> </ul>	<pre><drive>:\Program Files\GFI\WebMonitor</drive></pre>	Local Sys- tem

To view status of GFI WebMonitor services:

1. Click Start > Run and key in "services.msc"

Services						×
File Action View	Help					
	à 🔒 🛛 📷 🕨 🔲 II 🕪					
Services (Local)	Services (Local)					
	GELWebMonitor Core Service	Name	Description	Status	Startup Type	
		GFI Proxy	GFI WebMonitor Proxy Agent Service	Started	Automatic	
	Stop the service	GFI WebMonitor	Worker service for GFI WebMonitor	Started	Automatic	
Restart the service		😘 GFI WebMonitor Core Service	GFI WebMonitor Core Service	Started	Automatic	
		🔍 Group Policy Client	The service is responsible for applyin	Started	Automatic	
	Description:	🔍 Health Key and Certificate Management	Provides X.509 certificate and key ma		Manual	
	GFI WebMonitor Core Service	🔍 HomeGroup Listener	Makes local computer changes assoc		Manual	
		🎑 HomeGroup Provider	Performs networking tasks associate		Manual	
		🎑 Human Interface Device Access	Enables generic input access to Hum		Manual	-
		•	III			۶
	Extended Standard					

Screenshot 1: GFI WebMonitor Services

- 2. From the list of services displayed locate the following services:
- » GFI Proxy
- » GFI WebMonitor
- » GFI WebMonitor Core Service

## 2 Installing GFI WebMonitor

The following sections provide information for the successful deployment of GFI WebMonitor.

2.1 System Requirements	16
2.1.1 Software	16
2.1.2 Hardware	16
2.1.3 Microsoft® ISA / Forefront TMG Mode Pre-requisites	17
2.2 Deployment Scenarios	17
2.2.1 Deployment in a Microsoft ISA Server or Forefront TMG Environment	18
2.3 Installing GFI WebMonitor for IsaTmg	19
2.3.1 Introduction	19
2.3.2 Installation Procedure	19

## 2.1 System Requirements

## 2.1.1 Software

Table 5: Software requirements

ТҮРЕ	SOFTWARE REQUIREMENTS
Supported Operating Systems	» Windows <sup>®</sup> Server 2003 SP2
	» Windows <sup>®</sup> Server 2008
	» Windows <sup>®</sup> Server 2008 R2
Other required components	» Microsoft <sup>®</sup> ISA Server 2004 (SP3)
	» Microsoft <sup>®</sup> ISA Server 2006
	» Microsoft <sup>®</sup> Forefront TMG 2010 (Windows <sup>®</sup> Server 2008 R2)
	» Internet Explorer <sup>®</sup> 8 or later
	» Microsoft.NET <sup>®</sup> Framework 4.0
	» TCP/IP port 1007
	SQL Server <sup>®</sup> Express 2005 or later
	» SQL Server <sup>®</sup> 2005 or later (for reporting purposes)
	» (Recommended) Microsoft <sup>®</sup> Firewall Client for ISA Server
	» (Recommended) Microsoft <sup>®</sup> Firewall Client for Microsoft <sup>®</sup> Forefront TMG Microsoft IIS <sup>®</sup> Express

#### 2.1.2 Hardware

Minimum hardware requirements depend on the GFI WebMonitor edition.

#### Table 6: Hardware requirements

EDITION	HARDWARE REQUIREMENTS		
WebFilter Edition	» Processor: 2.0 GHz		
	» RAM: 1 GB (Recommended 4GB)		
	» Hard disk: 2 GB of available disk space		

EDITION	HARDWARE REQUIREMENTS
WebSecurity Edition	» Processor: 2.0 GHz
	» RAM: 1 GB (Recommended 4GB)
	» Hard disk: 10 GB of available disk space
Unified Protection Edition	» Processor: 2.0 GHz
	» RAM: 2 GB (Recommended 4GB)
	» Hard disk: 12 GB of available disk space

## IMPORTANT

GFI WebMonitor requires 2 network interface cards when installing in Gateway Mode or in a Microsoft<sup>®</sup> ISA/TMG environment. When installing in Simple Proxy mode only 1 network interface card is required.

## 🚹 NOTE

Allocation of hard disk space depends on your environment. The size specified in the requirements is the minimum required to install and use GFI WebMonitor. The recommended size is between 150 and 250GB.

## 2.1.3 Microsoft<sup>®</sup> ISA / Forefront TMG Mode Pre-requisites

## IMPORTANT

Ensure that the listening port (default 8080) is not blocked by your firewall. For more information on how to enable firewall ports on Microsoft Windows Firewall, refer to <a href="http://go.gfi.com/?pageid=WebMon\_WIndowsFirewall">http://go.gfi.com/?pageid=WebMon\_WIndowsFirewall</a>

## 2.2 Deployment Scenarios

GFI WebMonitor can be deployed in three modes:

- » In an Internet Gateway Environment
- » In a Simple Proxy Environment
- » In a Microsoft ISA Server or Forefront TMG environment

Deployment depends on the network infrastructure and the network role of the machine where GFI WebMonitor is to be installed. The following diagram helps you choose the correct GFI WebMonitor installation mode to suit your environment.





## 2.2.1 Deployment in a Microsoft ISA Server or Forefront TMG Environment

GFI WebMonitor can complement the functionality provided by Microsoft ISA Server or Microsoft Forefront TMG. When installed in this environment, GFI WebMonitor enables the administrator to monitor users web traffic in real time.



Screenshot 2: GFI WebMonitor installed on Microsoft ISA Server / Forefront TMG

Users request a webpage or a download over the Internet. The incoming traffic generated by the request is received by Microsoft Server, which in turn refers to GFI WebMonitor to use the filtering mechanisms to analyze the request.

To install GFI WebMonitor as a plug-in to Microsoft ISA Server / Forefront TMG, refer to the Installing GFI WebMonitor chapter in this manual.

## 2.3 Installing GFI WebMonitor for IsaTmg

## 2.3.1 Introduction

This chapter provides you with information related to the installation of GFI WebMonitor on Microsoft ISA Server / Forefront TMG.

## 2.3.2 Installation Procedure

Run the installer as a user with administrative privileges on the target machine.

1. Double click the GFI WebMonitor executable file.

2. The installer checks if required components are installed, and automatically installs missing components.

3. Choose whether you want the installation wizard to search for a newer build of GFI WebMonitor on the GFI website and click **Next**.

4. Read the licensing agreement. To proceed with the installation select I accept the terms in the license agreement and click Next.



Screenshot 3: Installation: Access Permissions

5. Key in the user name or the IP address that will be used to access the web interface of GFI WebMonitor and click Next.



🛃 GFI WebMonitor 201	2 Setup	- • •				
Service Logon Inform The following logon	nation nformation is used by the WebMonitor Service	<b>GF</b>				
The GFI WebMonitor service needs to run with administrative privileges for proper functionality. Please enter the username and password of an account with administrative privileges. Please make sure that the account is active and does not have the password set to expire. For domains, user names must be in the format of DOMAIN\UserName.						
<u>U</u> ser Name:	John Smith					
Password:	•••••					
NOTE: The usernam doesn't it will be swi only be used to crea	e and password provided must have "Logon As Ser tched ON automatically for the specified account. T ate and run as new service in the services control p	rvice" rights. If it These credentials will vanel.				
	Back Next	Cancel				

Screenshot 4: Installation: Service Logon Information

6. Key in the logon credentials of an account with administrative privileges and click Next.

## i NOTE The user account must have Log on as a service rights; otherwise, rights are automatically assigned. For more information, refer to <u>Assigning Log On As A Service</u> <u>Rights</u> (page 121).

😸 GFI WebMonito	r 2012 Setup		- • •
Mail Settings Enter administ	rator email and SMTP mail server settings		<b>GF</b> /°
Please enter the de WebMonitor 2012 f	tails of the SMTP server and email address tha or email reporting.	t are to be ι	used by GFI
Erom:	WebMonitor@127.0.0.1		
<u>T</u> o:	Administrator@127.0.0.1		
SMTP Server:	127.0.0.1	Port:	25
		Verif	fy Mail Settings
	Back	Next	Cancel

Screenshot 5: Installation: Mail Settings

7. Provide the SMTP mail server details and email address to which administrator notifications will be sent.

Optionally click Verify Mail Settings to send a test email. Click Next.

- 8. Click **Next** to install in default location or click **Change** to change installation path.
- 9. Click Install to start the installation, and wait for the installation to complete.

10. Click **Finish** to finalize setup.

## **3 Post Installation Actions**

After installation is complete, you need to perform a number of actions to ensure that GFI WebMonitor is deployed successfully.

3.1 Launching GFI WebMonitor	22
3.2 Enter a Valid License Key	23
3.3 Configure Proxy Settings	23
3.4 Configuring FTP	24
3.4.1 Step 1: Disabling Folder View in Microsoft Internet Explorer	24
3.4.2 Step 2: Configuring Browsers to Use a Proxy Server	25
3.4.3 Option 2: Configuring Proxy settings manually	25
3.4.4 Option 1: Configuring Proxy settings automatically in Microsoft® ISA Server and Microsoft®	
Forefront TMG	26
3.4.5 Step 3: Configuring FTP access	29
3.4.6 Option 1: Restricting or denying FTP access in Microsoft ISA Server or Microsoft Forefront TA	NG 32
3.5 Using the Settings Importer Tool	37
3.5.1 Exporting / Importing Configuration Settings	37

## 3.1 Launching GFI WebMonitor

On the same machine where GFI WebMonitor is installed:

There are 2 options for launching the GFI WebMonitor web console:

- » Option 1: click Start > All Programs > GFI WebMonitor > GFI WebMonitor Management Console
- » **Option 2:** Key in the URL http://monitor.isa in a web browser on the same machine.

## 🚹 NOTE

If using the GFI WebMonitor through the web browser interface on the same machine, Internet Explorer must be configured to use a proxy server. For more information refer to <u>Configure Microsoft Internet Explorer to Use a Proxy Server</u>.

## From a remote machine:

To launch GFI WebMonitor installation from machines of users and/or IP addresses that were allowed access to the application, key in the URL http://monitor.isa in a web browser from their machine. The Internet browser must be configured to use specific proxy settings to enable this access. For more information, refer to Configure Proxy Settings (page 23).

## 📄 NOTE

User access to the application can be granted either during <u>installation</u> or from the <u>Remote Access Control</u> node.

## 3.2 Enter a Valid License Key

After GFI WebMonitor is installed, a valid license key is required to start monitoring traffic and creating policies.

## 🚹 NOTE

If you are evaluating GFI WebMonitor, a 30 day unlimited evaluation key will be sent by email after registering.

	License Key required
	Please enter a valid license key which has been emailed to you by GFI.
	GFI WebMonitor requires a valid license key to work.
0	If you have registered to try GFI WebMonitor you will receive a valid evaluation key by email, otherwise click here to register to GFI Website and get a valid evaluation key. If your license has expired click "Buy Now" to purchase a valid license key or enter the updated key sent to you by GFI.
	Enter license key
	Litter neerbe key
	Buy now Close

Screenshot 6: License key required

To enter your license key:

- 1. Click Enter license key...
- 2. Enter your license key in the available field.
- 3. Click Apply.

## 🚹 NOTE

GFI WebMonitor enables you to update the license key manually after evaluating the product. For more information, refer to <u>Updating License Manually</u> (page 70).

🚺 NOTE

To activate license key, an Internet connection must be available.

#### See Also:

Licensing Information

## 3.3 Configure Proxy Settings

Client Internet Browsers need to be configured to use GFI WebMonitor as the default proxy server. If this setting is not deployed, the client machines will by-pass GFI WebMonitor and the Internet traffic they generate will remain undetected.

Proxy settings can be configured manually, by carrying out the configuration on every machine on your network that is going to access the Internet, or through GPO (Group Policy Object), that lets you configure settings for a group of active directory users.

## 3.4 Configuring FTP

Configure the user machines to route all FTP downloads through the Microsoft ISA Server / Forefront TMG proxy service. This can be achieved by:

- » Disabling folder view in Microsoft Internet Explorer on each client machine
- » <u>Configuring Internet browsers to use specific proxy settings on each client machine either auto-</u> <u>matically or manually</u>.
- » Configuring FTP access in Microsoft ISA Server / Forefront TMG.
  - FTP access can be configured by:
    - Option 1: Restricting or denying FTP access
    - Option 2: Disabling the FTP Access Filter

## 🚹 ΝΟΤΕ

To ensure that all users browse and download from FTP servers through proxy, the administrator should disable folder view and configure the proxy settings on the users' machines.

## 3.4.1 Step 1: Disabling Folder View in Microsoft Internet Explorer

To disable folder view in Microsoft Internet Explorer:

- 1. Launch Microsoft Internet Explorer on the client machine.
- 2. From **Tools** menu, choose **Internet Options** and select the **Advanced** tab.

Internet Options					?
General Securit	Privacy	Content	Connections	Programs	Advanced
Settings  Settings  Settings  Settings  Observer from page layout errors with Compa Close unused folders in History and Favorites*  Disable script debugging (Internet Explorer)  Disable script debugging (Other)  Display a notification about every script error  Display Accelerator button on selection					
<ul> <li>✓ Ena</li> </ul>	<ul> <li>Enable automatic crash recovery*</li> <li>Enable FTP folder view (outside of Internet Explorer)</li> <li>Enable page transitions*</li> <li>Enable Suggested Sites</li> <li>Enable third-party browser extensions*</li> <li>Enable visual styles on buttons and controls in webpages</li> <li>Enable websites to use the search pane*</li> </ul>				
*Takes effec	t after you	restart Int	ernet Explorer		
Reset Internet Explorer settings Resets Internet Explorer's settings to their default Reset You should only use this if your browser is in an unusable state.					
OK Cancel Apply					

Screenshot 7: Internet Options dialog box

3. Uncheck Enable FTP folder view checkbox from the Browsing node.

## NOTE

If unchecked, users will browse and download from FTP servers using an HTTP based folder view. In addition, GFI WebMonitor will now scan the FTP server contents and allow, guarantine or block the contents as applicable.

#### 3.4.2 Step 2: Configuring Browsers to Use a Proxy Server

Internet browsers can be configured either automatically or manually to use a proxy server in Microsoft ISA Server and Microsoft Forefront TMG. The following sections help you configure proxy settings:

- » Option 1: Configuring Proxy settings automatically
- » Option 2: Configuring Proxy settings manually

#### 3.4.3 Option 2: Configuring Proxy settings manually

To configure proxy settings manually:

1. Launch Microsoft Internet Explorer

- 2. From the **Tools** menu, choose **Internet Options** and select the **Connections** tab.
- 3. Click LAN settings.

Local Area Network (LAN) Settings						
Automatic configuration						
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.						
Automatically detect settings						
Use automatic configuration script						
Address						
Proxy server						
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).						
Address: <myproxy> Port: 8080 Advanced</myproxy>						
Bypass proxy server for local addresses						
OK Cancel						

Screenshot 8: LAN Settings dialog

4. Check Use a proxy server for your LAN checkbox.

5. Key in the proxy server name or IP address and the port used (Default 8080) in the Address and Port text boxes.

- 6. Click OK to close LAN Settings dialog.
- 7. Click OK to close Internet Options dialog.

## 3.4.4 Option 1: Configuring Proxy settings automatically in ${\rm Microsoft}^{\circledast}$ ISA Server and ${\rm Microsoft}^{\circledast}$ Forefront TMG

Microsoft<sup>®</sup> Firewall Client for ISA Server or Microsoft<sup>®</sup> Firewall Client for Microsoft<sup>®</sup> Forefront TMG automatically configures proxy settings.

To install Microsoft<sup>®</sup> Firewall Client for ISA Server:

- 1. Download **Microsoft Firewall Client for ISA Server** from the Microsoft<sup>®</sup> web site.
- 2. Double click the Microsoft Firewall Client for ISA Server executable file.

🙀 Microsoft Firewall Client - Install Wizard	×
ISA Server Computer Selection Specify the ISA Server computer to which Firewall Client will connect.	
You can specify the ISA Server computer that Firewall Client will connect to, or Firewall Client can detect the appropriate ISA Server computer.	
<ul> <li>Connect to this ISA Server computer:</li> <li>Type the ISA Server host name or IP address:</li> </ul>	
win2k3serv.masterdomain.com	
Example: isa.microsoft.com or 157.54.0.1	
C Automatically detect the appropriate ISA Server computer	
Note: These settings may be changed later using the Firewall Client management application.	
< Back Next > Cancel	

Screenshot 9: Microsoft Firewall Client for ISA Server: Installation wizard dialog

- 3. Select Connect to this ISA Server computer.
- 4. Key in the full machine name or IP address and continue to finalize the setup.
- 5. After installation, restart the client machine.
- 6. Right click 🐷 in the Windows<sup>®</sup> notification area and choose **Configure**.

🚰 Microsoft Firewall Client for ISA Server	X				
General Settings Web Browser					
Enable Microsoft Firewall Client for ISA Server					
☐ ISA Server Selection	٦ I				
Select how Firewall Client determines the ISA Server used for Internet access:					
C Automatically detected ISA Server:					
<pre><no detected="" isa="" server=""></no></pre> Detect Now					
<ul> <li>Manually specified ISA Server:</li> </ul>					
win2k3serv.masterdomain.com Test Server					
Default Settings Apply these Firewall Client settings as the default settings for services and users on this computer.					
Apply Default Settings Now					
OK Cancel Apply Help					

Screenshot 10: Microsoft<sup>®</sup> Firewall Client for ISA Server: Settings tab

## 📄 NOTE

Click Settings Tab to modify the server configurations.

To configure the web browser automatically:

- 1. Select Web Browser tab in the Microsoft Firewall Client for ISA Server dialog.
- 2. Check Enable Web browser automatic configuration checkbox.
- 3. Click **Configure Now**.
- 4. Click OK.

## To install the Microsoft Firewall Client for Microsoft Forefront TMG:

- 1. Locate the Microsoft Firewall Client for Forefront TMG from your server installation files.
- 2. Double click the Microsoft Firewall Client for Forefront TMG installation program and click Next.
- 3. Select I accept the terms in the license agreement and click Next.
- 4. Select the installation path were to install Microsoft Client and click Next.

📅 Forefront TMG Client - Install Wizard 🛛 🗙
Forefront TMG Computer Selection Specify the Forefront TMG computer to which Forefront TMG Client will connect.
You can specify the Forefront TMG computer that Forefront TMG Client will connect to, or Forefront TMG Client can detect the appropriate Forefront TMG computer.
Connect to this Forefront TMG computer:
Type the Forefront TMG host name or IP address:
win2k3serv.masterdomain.com
Example: isa.microsoft.com or 157.54.0.1
C Automatically detect the appropriate Forefront TMG computer
Note: These settings may be changed later using the Forefront TMG Client management application.
< Back Next > Cancel

 ${\it Screenshot 11: Microsoft} {\it \$} {\it Firewall Client for Forefront TMG: Installation wizard dialog}$ 

#### 5. Select Connect to this Forefront TMG computer.

- 6. Key in the full machine name or IP address and click Next.
- 7. Click Install and click Finish.

To configure the web browser automatically:

- 1. Select Web Browser tab in the Microsoft Firewall Client for Forefront TMG dialog.
- 2. Check Enable Web browser automatic configuration checkbox.
- 3. Click Configure Now.
- 4. Click OK.

## 3.4.5 Step 3: Configuring FTP access

By default, Microsoft ISA Server / Forefront TMG denies all traffic between all clients and external locations. After installation, GFI WebMonitor automatically adds 2 rules:

- » one to allow access between clients and GFI WebMonitor update server,
- » and another to allow the administrator to access GFI WebMonitor's user interface.

To ensure that no (or only specific) users are allowed to use the FTP protocol the administrator should create relevant rules in the Microsoft ISA Server / Forefront TMG. The following options are available:

Option 1: <u>Restricting or denying FTP access in Microsoft ISA Server or Microsoft Forefront TMG</u> Option 2: <u>Disabling the FTP Access Filter</u>

## Option 2: Disabling the FTP Access Filter

When the FTP Access Filter is disabled, users are not allowed to access an FTP server over the network.

## Disabling the FTP Access Filter in Microsoft ISA Server 2004

To disable the FTP Access Filter:

1. On the ISA Server machine, navigate to **Start > Programs > Microsoft ISA Server > ISA Server Management**.

📾 Microsoft Internet Security and Acceleration Server 2004					
Action View $\Rightarrow$ $\Rightarrow$ $\boxed{1}$ $\boxed{2}$ $\boxed{2}$					
Tree Microsoft Internet Secur 2KWMON Monitoring Firewall Policy	Microsoft Internet Security & Acceleration Server 2004 Standard Edition (1) Click here to learn about the learn of the	Customer Experience Improvement Program	<u>n.</u>	Add-ins	
Virtual Private N	Application Filters Web Filters	/			
- A Networks	Name	Description	Vendor Version		
	∘⊡ DNS Filter	Filters DNS traffic	Microsoft 4.0		
General	• FTP Access Filter	Properties TTP protocols (client and server)	Microsoft 4.0		
	• 🖬 H.323 Filter	protocol	Microsoft 4.0		
	MMS Filter	Enables Microsoft Media Streaming protocol	Microsoft 4.0		
	🛯 PNM Filter	Enables RealNetworks Streaming Media protocol	Microsoft 4.0		
	Intrusion Detection Filter	Checks for POP buffer overflow attacks	Microsoft 4.0		
	🛯 PPTP Filter	Enables PPTP tunneling through ISA Server	Microsoft 4.0		
	🖾 RPC Filter	Enables publishing of RPC servers	Microsoft 4.0		
	🖙 RTSP Filter	Enables Real Time Streaming Protocol	Microsoft 4.0		
	🖙 SMTP Filter	Filters SMTP traffic	Microsoft 4.0		
	👦 SOCKS V4 Filter	Enables SOCKS 4 communication	Microsoft 4.0		
	🖙 Web Proxy Filter	Enables HTTP proxy and cache	Microsoft 4.0		
- F					
Disable	,				

Screenshot 12: Microsoft ISA Server 2004: Configured Application filters

2. From the left panel expand <machine name> > Configuration > Add-ins.

- 3. Right-click FTP Access Filter and select Disable.
- 4. Save settings before exiting.

#### Disabling the FTP Access Filter in Microsoft ISA Server 2006

To disable the FTP Access Filter:

1. On the ISA Server machine, navigate to **Start > Programs > Microsoft ISA Server > ISA Server Management**.

Microsoft Internet Security and Ac	celeration Server 2006		
<u>File Action View H</u> elp			
← → 🗈 🖬 😫 🖬 🖄 😭	٩		
Microsoft Internet Security and Accele  Contempose  Enterprise Policies  Contempose Networks  Contempose Add-ins  Arrays	Microsoft Internet Security & Acceleration Server 2006 Enterprise Edition (1) <u>Click here to learn about the</u>	Configuration Storage Server: test.local Customer Experience Improvement Progr	Enterprise Add- ins <u>am.</u>
	Application Filters Web Filters		
	Name 🔺	Description	Vendor Version 🔺
	In the second se	Filters DNS traffic	Microsoft 4.0
	• FTP Access Filter	Enables FTP protocols (client and server)	Microsoft 4.0
	H.323 Filter	erties	Microsoft 4.0
	MMS Filter	ole Microsoft Media Streaming protocol	Microsoft 4.0
	🔲 PNM Filter	Enables RealNetworks Streaming Media protocol	Microsoft 4.0
	Intrusion Detection Filter	Checks for POP buffer overflow attacks	Microsoft 4.0
	I PPTP Filter	Enables PPTP tunneling through ISA Server	Microsoft 4.0
	🔲 RPC Filter	Enables publishing of RPC servers	Microsoft 4.0
	🔲 RTSP Filter	Enables Real Time Streaming Protocol	Microsoft 4.0
	In SMTP Filter	Filters SMTP traffic	Microsoft 4.0
	North Socks V4 Filter	Enables SOCKS 4 communication	Microsoft 4.0
	🔲 Web Proxy Filter	Enables HTTP proxy and cache	Microsoft 4.0
ł			
Disable			

Screenshot 13: Microsoft ISA Server 2006: Configured Application filters

- 2. From the left panel, expand Enterprise > Enterprise Add-ins.
- 3. Right-click FTP Access Filter and select Disable.
- 4. Save settings before exiting.

## Disable FTP Access Filter in Microsoft Forefront TMG

To disable the FTP Access Filter:

1. On Microsoft Forefront TMG machine, navigate to Start > Programs > Microsoft Forefront TMG > Forefront TMG Management.

📰 Forefront TMG					_ 🗆 🗵
File Action View Help					
🗢 🔿 🙍 🖬 🚺 🖬 🍳	D				
Microsoft Forefront Threat Management Forefront TMG (WIN-RJFL11FNFJL)	Forefront				System
A Monitoring	Threat Manage	Threat Management Gateway 2010			
	Servers Application F	ilters Web Filters			
E-Mail Policy	Name 🔺	Description	Vendor	Version	
Intrusion Prevention System	প🗐 DNS Filter	Filters DNS traffic	Microsoft (R) Cor	4.0	
	•     FTP Access Filter	Enables FTP prot	Microsoft (R) Cor	4.0	
System	الم H. 323 Filter	Properties pr	Microsoft (R) Cor	4.0	
🥏 Update Center	🔲 MMS Filter	Disable ft	Microsoft (R) Cor	4.0	
Troubleshooting	গ্ৰ PNM Filter	Enables RealNet	Microsoft (R) Cor	4.0	
	M POP Intrusion Dete.	. Checks for POP b	Microsoft (R) Cor	4.0	
	M PPTP Filter	Enables PPTP tun	Microsoft (R) Cor	4.0	1
	₀ RPC Filter	Enables publishin	Microsoft (R) Cor	4.0	×
	₀ RTSP Filter	Enables Real Tim	Microsoft (R) Cor	4.0	
	In SIP Access Filter	Enables SIP proto	Microsoft (R) Cor	4.0	
	গ্ৰা SMTP Filter	Filters SMTP traffic	Microsoft (R) Cor	4.0	
	Reference Socks V4 Filter	Enables SOCKS 4	Microsoft (R) Cor	4.0	
	M TFTP Access Filter	Enables TFTP pro	Microsoft (R) Cor	4.0	
	্র Web Proxy Filter	Enables HTTP pro	Microsoft (R) Cor	4.0	
Disable Selected					

Screenshot 14: Microsoft Forefront TMG: Configured Application filters

2. From the left panel, expand Forefront TMG <machine name> > System

- 3. From the right panel, click Application Filters tab.
- 4. Right click FTP Access Filter and select Disable.
- 5. Click Apply.
- 6. Save settings.

3.4.6 Option 1: Restricting or denying FTP access in Microsoft ISA Server or Microsoft Forefront TMG

To restrict FTP to specific users only, it is advisable to create two rules: one to allow usage of common protocols to all users except FTP, and another to allow FTP to particular users only, example the administrator.

ISA Server 2004 Enterprise Edition							
Eile Action View Help							
← → 🗈 🖬 😫 🗈 😁 🗙	ج 📀 🗧	* 🖲 援 🗾					
Microsoft Internet Security and Acceleratic Microsoft Internet Security and Acceleratic Finternet Security & Acceleration Server2004 Microsoft Internet Security & Acceleration Server2004 Enterprise Edition Firewall Policy (WIN2K3SERV Firewall Policy							y (WIN2K35ER¥)
Firewall Policy (WIN2K35ERV)      Virtual Private Networks (VPN)	0 🔺	Name	Action	Protocols	From / Listener	То	Condition
由- 決 Configuration	Enterprise Firewall P	e Policy Rules Applied Before / olicy Rules	Array Firewa	ll Policy			
	🖃 🂽 1	Allow FTP	🥑 Allow	FTP Server	📩 Anywhere	📩 Anywhere	http://www.administrator
	🗖 🚺 2	Allow Internal Internet	🥝 Allow	Un HTTP Un HTTPS	-1- Internal -1- Local Host	🔇 External	h All Users
	🖃 📝 З	GFI WebMonitor GUI Access	🕜 Allow	M HTTP M HTTPS	👍 Internal 👍 Local Host	👍 Local Host	All Users 🔇
	🖃 📝 4	GFI WebMonitor Updates Access	: 🥝 Allow	MHTTP MHTTPS	👍 Local Host	💽 Web Server	📇 All Users
	🖃 💽 5	Allow Internal	🥝 Allow	🟭 All Outbound Traffic	👍 Internal 👍 Local Host	👍 Internal 👍 Local Host	衡 All Users
	Enterpris	e Policy Rules Applied After A	rray Firewall	Policy			
	💽 Las	t Default rule	🚫 Deny	腿 All Traffic	👍 All Networks (	. <sub>物</sub> All Networks (and Local Ho	st) 衡 All Users
Done	]						

Screenshot 15: Microsoft ISA Server: Configured Firewall policies

The preceding screenshot shows both rules.

Firewall Policy Rule 2 allows common protocol traffic from all users to pass from the internal network to the Internet. Note that the Protocols list does not include the FTP protocol.

Firewall Policy Rule 1 allows FTP protocol usage only by the Administrator. To set this rule to allow the administrator to access an FTP server:

## On Microsoft ISA Server

1. On the Microsoft ISA Server machine, navigate to Start > Programs > Microsoft ISA Server > ISA Server Management.

- 2. From the left panel, expand **Arrays > <machine name> > Firewall Policy**.
- 3. Right-click Firewall Policy and select New >Access Rule.
- 4. Key in a name for this rule; for example 'Allow FTP' and click Next.
- 5. Select Allow and click Next.

New Access Rule Wizard	×
<b>Protocols</b> Select the protocols this rule applies to.	
I his rule applies to:	
Selected protocols	•
Protocols:	
FTP	Add Edit [Remove] Po <u>r</u> ts
	< <u>B</u> ack <u>N</u> ext > Cancel

Screenshot 16: Microsoft ISA Server: Protocols dialog

6. In the **Protocols** dialog, click **Add**.

7. In the Add Protocols dialog, expand All Protocols, select FTP, click Add and Close.

8. In the **Protocols** dialog click **Next**.

9. In the Access Rule Sources dialog, click Add.

10. In the Add Network Entities dialog, expand Computer Sets, select Anywhere, click Add and click Close.

11. In the Access Rule Sources dialog click Next.

12. In the Access Rule Destinations dialog, click Add.

13. In the Add Network Entities dialog, expand Computer Sets, select Anywhere, click Add and click Close.

14. In the Access Rule Destinations dialog click Next.

15. In the User Sets dialog, select All Users and click Remove.

16. Click Add.

Add Users 🛛 🗙
User sets:
New Edit Delete
Administrator         All Authenticated Users         All Users         System and Network Service         Administrator
Add Close

Screenshot 17: Microsoft ISA Server: Add Users dialog

- 17. In the Add Users dialog, select Administrator, click Add and click Close.
- 18. Click Next and Finish.
- 19. Make sure to save settings before exiting.

## On Microsoft Forefront TMG

1. On the Microsoft Forefront TMG machine, navigate to Start > Programs > Microsoft Forefront TMG

- > Forefront TMG Management.
- 2. From the left panel expand Forefront TMG <machine name>.
- 3. Right-click Firewall Policy and select New > Access Rule.
- 4. Key in a name for this rule; for example 'Allow FTP' and click Next.
- 5. Select Allow and click Next.

New Access Rule Wizard			×
<b>Protocols</b> Select the protocols this rule applies to.		A	
This rule applies to:			
Selected protocols		•	
Protocols:			
Щ, FTP		Add Edit Remove	
		Ports	
	< Back	Next > Cancel	

Screenshot 18: Microsoft Forefront TMG: Protocols dialog

6. In the **Protocols** dialog, click Add.

- 7. In the Add Protocols dialog, expand All Protocols, select FTP, click Add and click Close.
- 8. In the **Protocols** dialog click **Next**.

New Access Rule Wizard		×
Access Rule Sources This rule will apply to traffic originating from t	the sources specified in this p	age.
This rule applies to traffic from these sources:		
Anywhere		Add
		Edit
		Remove
	< Back Next >	Cancel

Screenshot 19: Microsoft Forefront TMG: Access Rule Sources dialog

9. In the Access Rule Sources dialog, click Add.

10. In the Add Network Entities dialog, expand Computer Sets, select Anywhere, click Add and click Close.

11. In the Access Rule Sources dialog click Next.

12. In the Access Rule Destinations dialog, click Add.

13. In the Add Network Entities dialog, expand Computer Sets, select Anywhere, click Add and click Close.

- 14. In the Access Rule Destinations dialog click Next.
- 15. In the User Sets dialog, select All Users and click Remove.
- 16. Click Add.
| Add Users  | × |
|--|---|
| User sets:   |   |
| <u>N</u> ew <u>E</u> dit <u>D</u> elete  |   |
| Image: Administrator         Image: All Authenticated Users         Image: All Users         Image: All Users         Image: System and Network Service         Image: Administrator |   |
| Add Close  |   |

Screenshot 20: Microsoft ISA Server: Add Users dialog

- 17. In the Add Users dialog, select Administrator, click Add and click Close.
- 18. Click **Next** and **Finish**.
- 19. Save settings before exiting.

### 3.5 Using the Settings Importer Tool

The Settings Importer Tool is a command line tool that enables you to export settings from a configured GFI WebMonitor installation and import the same settings into a new installation. The tool is particularly useful when you have more than one GFI WebMonitor instance deployed in your organization. Using simple command line scripting, you can export and import GFI WebMonitor configurations to synchronize the multiple instances.

The configuration settings are exported into a single file that can then be imported as required. This functionality ensures that any changes are replicated to all instances without having to synchronize manually.

#### 3.5.1 Exporting / Importing Configuration Settings

To use the Settings Importer Tool:

1. On the machine where GFI WebMonitor is installed, go to **Start > Run** and type **cmd**. This action calls the Microsoft Windows command line interface.

2. To list all the controls that can be used to operate the Settings Importer Tool, type:

- WebMon.SettingsImporterTool --help for Windows 32-bit
- WebMon.SettingsImporterTool --help For Windows 64-bit

Administrator: C:\Windows\system32	.cmd.exe	x
C:\Program Files\GFI\WebMoni	tor>WebMon.SettingsImporterTool -help	^
Usage: WebMon.SettingsImport authorizationall]]	erTool [-epath=VALUE] [-ipath=VALUE [report	S
Ontions:		
-eexport	Frankt settings (all).	
-i,import	Import settings (all - specific settings can be imported via options).	
nath=UALIE	The math to the settings file.	
-Rreports	Import all report settings.	
-aauthorization	Import authorization rules.	
-u,autoupdate	Import auto update settings.	
-d,database	Import database settings.	
-n,notifications	Import notifications settings.	
-o,options	Import general options.	
-w,webcategorization	Import web categorization settings.	
-G,allgeneral	Import all general settings.	
-f,webfiltering	Import web filtering policies.	
-b,webbrowsing	Import web browsing policies.	
-m,instantmessaging	lmport instant messaging & social control policies.	
-s,streamingmedia	Import streaming media policies.	
-g,searchengine	Import search engine policies.	
-v,virusscanning	Import virus scanning policies.	
-y,securityengines	Import security engines settings.	
-1,downloadcontrol	Import download control policies.	
-x,alwaysblocked	Import always blocked settings.	
-j,alwaysallowed	Import always allowed settings.	
-P,allpolicy	Import all policy settings.	
-L,allalerts	Import all alert settings.	
-q,proxygeneral	Import proxy general settings.	
-n,proxynttps	Import proxy https settings.	
-2,proxycache	Import proxy cache settings.	
-S $$ all proxy	Import all proxy settings.	=
-0 $$ $$ $$ $$ $$ $$ $$	Import all settings (except reports).	
	Import all.	
C:\Program Files\GFI\WebMoni	tor>	-

Screenshot 21: Settings Importer Tool Controls

# 🚺 ΝΟΤΕ

The controls apply only when importing configuration settings.

3. The following are some examples on how to perform export and import functions:

#### Example 1 - Exporting all settings:

To export the current settings, type:

WebMon.SettingsImporterTool -e

Settings are exported to a single file and when the process is complete, the following message is displayed: Exported WebMonitor settings to C:Program Files\GFI\WebMonitor\<filename>.gz

#### Example 2 - Importing settings:

#### To import exported settings, type:

WebMon.SettingsImporterTool -i /path=<filename>.gz

#### When import is complete, the following message is displayed:

Successfully imported <All> WebMonitor settings from <filename>

## 🚹 NOTE

Additional examples are included in 2 text files in the GFI WebMonitor installation folder; ExportSettingsExample.bat and ImportSettingsExamples.bat.

## 4 Achieving Results

Refer to the following sections to configure GFI WebMonitor and start achieving results:

- » Protect Your Network
- » Increase Productivity
- » Maximize Available Bandwidth

### 4.1 Achieving Results with GFI WebMonitor - Protecting Your Network

See the information below for information on how to proactively protect your network before it is compromised.

### WebFilter Edition



- 1. Block website categories in the Security group (such as Malware Sites, Phishing and Other Frauds, Spyware and Adware, Bot Nets and Confirmed SPAM Sources).
- » Configure Web Filtering Polices



- 2. Block access to sites with low reputation (having a Reputation Index of 40 or less).
- » Configure Web Filtering Polices
- Configure Always Blocked list
- Configuring Web Categorization



- 3. Block social engineering, phishing and online scams
- » Configuring Internet Policies

### WebSecurity Edition

1. Block Known Malicious Websites and Phishing.

- » Configure ThreatTrack
- Configuring Anti-Phishing in Security Policies
- Configure Auto-update of all security engines
- Configure Auto-update of all security engines
- 2. Control and scan your downloads using multiple anti-virus engines.
- Configure Downloads Policies
- Configuring Security Policies

GFI also recommends to create an awareness policy with safe use guidelines for your employees. For more information refer to: http://www.gfi.com/whitepapers/acceptable\_use\_policy.pdf.

### 4.2 Achieving Results with GFI WebMonitor - Maximize Bandwidth Availability

Analyze your bandwidth activity and make informed decisions based on those results.

- Deploy GFI WebMonitoron your network without any filtering policies. Use the inbuilt monitoring and reporting tools to observe Internet usage and identify patterns that impact bandwidth optimization. For example, identify excessive bandwidth usage or access to certain unwanted sites. Create adequate policies based on the results obtained from these reports.
- » Generate Activity reports
- » Generate Bandwidth reports
- » Configure Internet Policies



- 2. Monitor and manage Internet connections in real-time to optimize bandwidth.
- Use the Bandwidth Dashboard
- Use the Activity Dashboard
- » Terminate active connections from the Real-Time Traffic Dashboard



- 3. Manage website categories in the Bandwidth control group (such as Streaming Media, P2P, Online Personal Storage).
- Configure Web Filtering Polices



- 4. Block access to unwanted streaming applications such as YouTube and similar video sharing web sites.
- Configure Streaming Media Policies



- 5. Block access to unwanted Instant Messaging applications (such as MSN, Google Talk, Yahoo Messenger, Facebook Chat and Online Portals.
  - Configure Instant Messaging Policies



- 6. Set bandwidth thresholds to limit access to specific web site categories, based on time or bandwidth limits.
- Configure Web Browsing Quota Policies



GFI also recommends to create an awareness policy with safe use guidelines for your employees. For more information refer to: http://www.gfi.com/whitepapers/acceptable\_use\_policy.pdf.

### 4.3 Achieving Results with GFI WebMonitor - Increase Productivity

Configure options and measures and set up policies that filter web traffic with the aim of increasing your workforce productivity.



- 1. Deploy GFI WebMonitoron your network without any filtering policies. Use the inbuilt monitoring and reporting tools to observe Internet use and identify patterns that impact your organization's productivity. Create adequate policies based on the results obtained from these reports.
- Use the Bandwidth Dashboard
- Use the Activity Dashboard
- » Generate Activity reports
- » Generate Bandwidth reports
- » Configure Internet Policies
- 2. Block website categories in the Productivity Loss and Potential Productivity Loss groups (such as Social Network, Dating, Games and Pay to Surf).
- » Configure Web Filtering Polices



- 3. Block access to streaming applications.
- Configure Streaming Media Policies



- 4. Block access to Instant Messaging applications (such as MSN, Google Talk, Yahoo Messenger, Facebook Chat and Online Portals.
- » Configure Instant Messaging Policies

- 5. Limit access to specific web site categories based on time or bandwidth limits.
  - » Configure Web Browsing Quota Policies

 GFI also recommends to create an awareness policy with safe use guidelines for your employees. For more information refer to: <u>http://www.gfi.com/whitepapers/acceptable\_use\_policy.pdf.</u>

## 5 Using the Dashboard

The GFI WebMonitor Dashboard provides quick insight to activity on your network. Use the following monitoring tools to identify potential problems:

Table 7: Monitor	ring tools
OPTION	DESCRIPTION
<u>Overview</u>	Provides a quick glance of current activity on the network, enabling you to identify network usage trends and tasks that need to be carried out by the administrator.
<u>Bandwidth</u>	Shows activity related to bandwidth consumption. Use the provided filters to spot downloads or uploads that are affecting your network performance.
Activity	Gives you insight on different types of activity during specific times of the day.
Security	Displays activity related to security issues such as detection of infected files, malicious and phishing sites, as well as information related to the most common viruses attacking your network.
Real-Time Traffic	Shows network traffic in real-time.
Quarantine	Provides controls to authorize traffic that requires approval.

## NOTE

If Anonymization is enabled, personal data (such as User Names and IPs) is masked. For more information on how to enable Anonymization refer to <u>General Options</u>.

### 5.1 Overview of Internet Activity

On launching GFI WebMonitor, the overview page is displayed by default.



Screenshot 22: Dashboard Overview

The page contains a graphical representation of Internet usage trends, such as:

- » The bandwidth consumption for the current day
- » Activity filtered by any configured policy
- » Information related to searches performed by users
- » Top categories and domains that are being accessed by users
- » Top users and policies.

### 🚹 NOTE

By default, the data provided in the **Overview** page is for the current week. This filter can be changed from the **for period** field in the top right corner of the screen.

<u> S M T</u>	WTF	C C			November 2011 December 2011 January 2012						
		دد	м	Т	W	Т	F S				
<b>5</b> 27 28 29	30 1 2	3 1	2	3	4	5	6 7				
2 4 5 6	7 8 9	10 8	9	10	11	12 1	13 1				
9 11 12 13	14 15 16	17 15	16	17	18						
26 18 19 20	21 22 23	<b>24</b> 22									
25 26 27	28 29 30	31 29									
1	5 27 28 29 12 4 5 6 19 11 12 13 26 18 19 20 3 25 26 27	5       27       28       29       30       1       2         12       4       5       6       7       8       9         19       11       12       13       14       15       16         26       18       19       20       21       22       23         3       25       26       27       28       29       30	5       27       28       29       30       1       2       3       1         12       4       5       6       7       8       9       10       8         19       11       12       13       14       15       16       17       15         26       18       19       20       21       22       23       24       22         3       25       26       27       28       29       30       31       29	5       27       28       29       30       1       2       3       1       2         12       4       5       6       7       8       9       10       8       9         19       11       12       13       14       15       16       17       15       16         26       18       19       20       21       22       23       24       22       23         3       25       26       27       28       29       30       31       29       30	5       27       28       29       30       1       2       3       1       2       3         12       4       5       6       7       8       9       10       8       9       10         19       11       12       13       14       15       16       17       15       16       17         26       18       19       20       21       22       23       24       22       23       24         3       25       26       27       28       29       30       31       29       30       31	5       27       28       29       30       1       2       3       1       2       3       4         12       4       5       6       7       8       9       10       8       9       10       11       1         19       11       12       13       14       15       16       17       15       16       17       18         26       18       19       20       21       22       23       24       22       23       24       25       3         3       25       26       27       28       29       30       31       29       30       31       1	5       27       28       29       30       1       2       3       1       2       3       4       5         12       4       5       6       7       8       9       10       8       9       10       11       12       1         19       11       12       13       14       15       16       17       15       16       17       18       19       2         26       18       19       20       21       22       23       24       22       24       25       26       27       28       29       30       31       29       30       31       1       2				

Screenshot 23: Using the calendar to set period

#### 5.1.1 WebGrade Categorization

The **Website Category Lookup** area enables you to check the categorization of a URL and its Reputation Index.

Website Category Lookup	
Type web site	$\mathbb{Q}$
Screenshot 24: Website Category Lookup feature To check a website:	
2. Click icon	

For more information, refer to Configuring Web Categorization (page 78).

### 5.1.2 Pending Task List

A list of important tasks is displayed in the Dashboard for the attention of the System Administrator.

After performing a task, click Dismiss to remove it from the list.



Screenshot 25: Pending tasks list

## IMPORTANT When a task is dismissed, it does not appear again on the dashboard.

### 5.1.3 Web Monitoring Status

The **Overview** page displays statistics related to Internet use, such as the total number of Websites visited by all users, the number of infected files detected by GFI WebMonitor and the number of websites blocked by a configured policy.

### 🚹 NOTE

If Alerts are configured, a notification appears in the **Overview** window, above **Monitor Status** area. For more information, refer to <u>Configuring Alerts</u> (page 106).



Screenshot 26: Dashboard Overview statistical information

### 5.1.4 Product Status





Use the Product Status area to verify details related to:

Table 8: Product status overview

STATUS	DESCRIPTION
Product Version	Displays the current installed version of GFI WebMonitor and the build number.
Licensed Module	Check which modules are licensed and active. For more information, refer to <u>Licensing Information</u> (page 13).
Licensed Users	Shows the number of users being monitored. For more information on how GFI WebMonitor counts users for licensing purposes, refer to Knowledge Base article: <a href="http://go.gfi.com/?pageid=WebMon_Licensing">http://go.gfi.com/?pageid=WebMon_Licensing</a> .
Subscription	Displays the date when the GFI WebMonitor license is due for renewal.

## 5.2 Monitoring Bandwidth

The Bandwidth dashboard provides information related to traffic and user activity that affects bandwidth consumption. Filter data according to the following:

Table 9: Bandwidth dashboard options

OPTION	DESCRIPTION
All Bandwidth	Shows download and upload traffic.
Download Only	Displays only downloaded traffic.
Upload Only	Displays only uploaded traffic.

•••	<b>GFI Web</b> Monitor						
Dashl	board Reports	Settings He	lp				
💿 Ove	rview 🥙 Bandwidth 🗳 Ac	tivity 🦃 Security 🖪	Real-Time Traffic	🚱 Quarantine			
Bandwidth         Report ▼           for period:         7/15/2012 - 7/23/2012							
All Ba	All Bandwidth Download Only Upload Only View by: 📀 🗐 🗐						
Down 1.0 Avg:	Ioad         Upl           I CB         5           115.23 MB day         Av	0 <b>4.17 KB</b> g: 56.02 KB day	Peak Day 07/16/20 796.02 MB	012	Projected Download 3.38 GB for the next 30 days	Projected U 1.64 M for the ne	Upload <b>IB</b> ext 30 days
476.84 MB 7/15/2012 7/16/2012 7/17/2012 7/18/2012 7/19/2012 7/20/2012 7/21/2012 7/22/2012 7/23/2012 Download Upload							
Showi	ng: Categories Websites	Users Event Log	Downloa	ad 📕 Upload			.,
Showin Filter:	ng: Categories Websites	Users Event Log	Downloa	ad 📕 Upload		View by:	Domain Site
Showin Filter:	ng: Categories Websites	Users Event Log Bandwidth <del>-</del>	Downloa	d Upload	Download (%)	View by: Upload	Domain Site Upload (%)
Showin Filter:	ng: Categories Websites	Users Event Log Bandwidth <del>•</del> 989.59 MB	Bandwidth (%) 95.38 %	Download 989.10 MB	Download (%) 95.38 %	View by: Upload 503.82 KB	Domain Site Upload (%) 99.93 %
Showin Filter:	ng: Categories Websites	Users Event Log Bandwidth - 989.59 MB 43.89 MB	Downloa     Downloa     Bandwidth (%)     95.38 %     4.23 %	Download 989.10 MB 43.89 MB	Download (%) 95.38 % 4.23 %	View by: Upload 503.82 KB 0.00 B	Domain         Site           Upload (%)         99.93 %           0.00 %         0
Showi Filter: 1. 2. 3.	ng: Categories Websites	Users Event Log Bandwidth → 989.59 MB 43.89 MB 2.44 MB	Downloa Bandwidth (%) 95.38 % 4.23 % 0.24 %	Download 989.10 MB 43.89 MB 2.44 MB	Download (%) 95.38 % 4.23 % 0.24 %	View by: Upload 503.82 KB 0.00 B 0.00 B	Domain         Site           Upload (%)         99.93 %           0.00 %         0.00 %
Showin Filter: 1. 2. 3. 4.	ng: Categories Websites	Users         Event Log           Bandwidth •         989.59 MB           43.89 MB         2.44 MB           696.02 KB         696.02 KB	Downloa Bandwidth (%) 95.38 % 4.23 % 0.24 % 0.07 %	Download 989.10 MB 43.89 MB 2.44 MB 696.02 KB	Download (%) 95.38 % 4.23 % 0.24 % 0.07 %	View by: Upload 503.82 KB 0.00 B 0.00 B 0.00 B	Domain         Site           Upload (%)         99.93 %           0.00 %         0.00 %           0.00 %         0.00 %
Showin Filter:	ng: Categories Websites	Users Event Log Bandwidth → 989.59 MB 43.89 MB 2.44 MB 696.02 KB 522.90 KB	Downloa Bandwidth (%) 95.38 % 4.23 % 0.24 % 0.07 % 0.05 %	Download 989.10 MB 43.89 MB 2.44 MB 696.02 KB 522.90 KB	Download (%)           95.38 %           4.23 %           0.24 %           0.07 %           0.05 %	View by: Upload 503.82 KB 0.00 B 0.00 B 0.00 B 0.00 B	Domain         Site           Upload (%)         99.93 %           0.00 %         0.00 %           0.00 %         0.00 %
Showin Filter: 1. 2. 3. 4. 5. 6.	ng: Categories Websites	Users         Event Log           Bandwidth •         989.59 MB           43.89 MB         2.44 MB           696.02 KB         522.90 KB           94.98 KB         94.98 KB	Download	Download 989.10 MB 43.89 MB 2.44 MB 696.02 KB 522.90 KB 94.98 KB	Download (%) 95.38 % 4.23 % 0.24 % 0.07 % 0.05 % 0.01 %	View by: Upload 503.82 KB 0.00 B 0.00 B 0.00 B 0.00 B 0.00 B	Domain         Site           Upload (%)         99.93 %           0.00 %         0.00 %           0.00 %         0.00 %           0.00 %         0.00 %
Showin Filter: 1. 2. 3. 4. 5. 6. 7.	ng: Categories Websites	Users Event Log Bandwidth → 989.59 MB 43.89 MB 2.44 MB 2.44 MB 696.02 KB 522.90 KB 522.90 KB 94.98 KB 84.75 KB	Download	Download 989.10 MB 43.89 MB 2.44 MB 696.02 KB 522.90 KB 94.98 KB 84.75 KB	Download (%)           95.38 %           4.23 %           0.24 %           0.07 %           0.05 %           0.01 %	View by: Upload 503.82 KB 0.00 B 0.00 B 0.00 B 0.00 B 0.00 B	Domain         Site           Upload (%)         99.93 %           0.00 %         0.00 %           0.00 %         0.00 %           0.00 %         0.00 %           0.00 %         0.00 %
Showin Filter: 1. 2. 3. 4. 5. 6. 7. 8.	ng: Categories Websites	Users         Event Log           Bandwidth •         989.59 MB           989.59 MB         43.89 MB           2.44 MB         2.44 MB           696.02 KB         522.90 KB           94.98 KB         94.98 KB           84.75 KB         39.59 KB	Download	Download 989.10 MB 43.89 MB 2.44 MB 696.02 KB 522.90 KB 94.98 KB 84.75 KB 39.59 KB	Download (%) 95.38 % 4.23 % 0.24 % 0.07 % 0.05 % 0.01 % 0.01 % 0.01 % 0.00 %	View by: Upload 503.82 KB 0.00 B 0.00 B 0.00 B 0.00 B 0.00 B 0.00 B	Domain         Site           Upload (%)         99.93 %           0.00 %         0.00 %           0.00 %         0.00 %           0.00 %         0.00 %           0.00 %         0.00 %           0.00 %         0.00 %

Screenshot 28: Monitoring bandwidth

### 🚺 ΝΟΤΕ

Use the **View by:** filter in the top right corner of the page to view data for a specific date range.

The lower portion of the Bandwidth page provides a breakdown of the data monitored in the specified period.

### Data is broken down as follows:

Table	10:	Bandwidth	monitoring	filtering	options
-------	-----	-----------	------------	-----------	---------

FILTER	DESCRIPTION
Categories	Select to view a list of categories and size of download for each category.
Websites	A list of websites with respective download size. Data can be viewed by Domain or by Site using the pro- vided controls.
Users	A list of users and the total size of downloads for a specified period.

FILTER	DESCRIPTION
Even Log	Provides a log of all the web requests that fall within the specified period, displaying: Web Request - URL of request
	» Time - date and time of request
	» Download - size of download
	» User - User name
	» IP - IP address

### 5.2.1 One-click Report Functionality

After you customize the dashboard, the view can be exported as a report or scheduled to be sent automatically as required.

### Export Report

To export the report:

- 1. From the top of the Dashboard, click Report A and select Export Report.
- 2. GFI WebMonitor displays the exported report in a separate window in your browser.

3. Click and select one of the following options:

Table	11:	Export	report	options

OPTION	DESCRIPTION
Excel	The report is exported in Microsoft Excel format (.xls)
PDF	The report is exported in PDF format.
Word	The report is exported in Microsoft Word format (.doc)

#### Schedule Report

To schedule the report:

- 1. From the top of the Dashboard, click Report A and select Schedule Report.
- 2. GFI WebMonitor redirects you automatically to the Reports area.

For more information, refer to <u>Reporting</u> (page 60).

4. Save the report.

### IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information refer to <u>General Options</u>.

### 5.3 Monitoring Activity

The Activity dashboard provides information related to web requests and user activity for a specified period. Filter data according to the following:

Table 12: Activity dashboard options

OPTION	DESCRIPTION
All Activity	Shows all web requests (filtered and unfiltered) made through GFI WebMonitor in the specified period.

OPTION	DESCRIPTION
Allowed Only	Displays only traffic that has been allowed by GFI WebMonitor.
Filtered Only	Displays only traffic that has been blocked by configured policies.
Searches	Shows the activity related to searches performed by users.

🚹 NOTE

Use the **View by:** filter in the top right corner of the page to view data for a specific date range.

#### **GFI Web**Monitor Dashboard Reports Help Activity 💱 Security 💫 Real-Time Traffic 🚱 Quarantine 👁 Overview 🧭 Bandwidth Activity Report v for period: 7/15/2012 - 7/23/2012 View by: 🕑 🖿 🔳 Allowed Only Filtered Only (Group by Policy) All Activity Searches Web Requests Users Peak Day Projected Web Requests 7195 3/3 07/17/2012 23983 for the next 30 days Avg: 799 / day 1169 web requests 1500 1000 Activity 500 7/15/2012 7/16/2012 7/17/2012 7/18/2012 7/19/2012 7/20/2012 7/21/2012 7/22/2012 7/23/2012 - All Activity + Filtered Only Showing: Categories Websites Users Event Log View by: Domain Site 9 Filter: Domain 👻 Filtered Web Requests Filtered (%) Web Requests Avg / Day 1. webtrends.com 1 0 0.00 % 0 2. twitter.com 1 0 0.00 % 0 37 0 0.00 % 4 sunbeltsoftware.com 3. 4. scorecardresearch.com 5 0 0.00 % 0 5. s-msn.com 196 0 0.00 % 21 revsci.net 5 0 0.00 % 0 6. 7. msn.com 406 0 0.00 % 45 8. msads.net 10 0 0.00 % 1

Screenshot 29: Activity Dashboard

The lower portion of the **Activity** page provides a breakdown of the data monitored in the specified period.

Data is broken down as follows:

Table 13: Activity monitoring filtering options

FILTER	DESCRIPTION
Categories	Select to view a list of categories with total number of Web Requests for each category.
Websites	A list of websites with respective total number of <b>Web Requests</b> . Data can be viewed by Domain or by Site using the provided controls.
Users	A list of users and the total <b>Surf Time</b> and number of <b>Web Requests</b> for a specified period. <b>NOTE</b> <b>Surf Time</b> is an approximate time calculated by timing access to web sites. Every time a user accesses a website, 1 surf time minute will be added for that user. During this minute, the user can access other web sites without adding to the surf time. When the 1 minute has passed, another minute will be added if the user is still browsing.
Event Log	<ul> <li>Provides a log of all the web requests that fall within the specified period, displaying:</li> <li>Web Request - URL of request</li> <li>Time - date and time of request</li> <li>Download - size of download</li> <li>User - User name</li> <li>IP - IP address</li> </ul>

### 5.3.1 One-click Report Functionality

After you customize the dashboard, the view can be exported as a report or scheduled to be sent automatically as required.

#### **Export Report**

To export the report:

- 1. From the top of the Dashboard, click Report A and select Export Report.
- 2. GFI WebMonitor displays the exported report in a separate window in your browser.

3. Click and select one of the following options:

OPTION	DESCRIPTION
Excel	The report is exported in Microsoft Excel format (.xls)
PDF	The report is exported in PDF format.
Word	The report is exported in Microsoft Word format (.doc)

#### Schedule Report

To schedule the report:

- 1. From the top of the Dashboard, click Report A and select Schedule Report.
- 2. GFI WebMonitor redirects you automatically to the Reports area.

For more information, refer to <u>Reporting</u> (page 60).

4. Save the report.

### IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information refer to <u>General Options</u>.

### 5.4 Monitoring Security

The Security dashboard provides information related to web requests and user activity for a specified period. The information provided enables you to identify security risks and threats to your network environment at a glance.

Data is filtered to provide information related to:	Data	is	filtered	to	provide	information	related to:
---	------	----	----------	----	---------	-------------	-------------

, ,	
OPTION	DESCRIPTION
Infected Files Detected	Shows all files that have been detected as being infected by a virus by GFI WebMonitor for the selected period.
Malicious Sites Blocked	Displays all the websites that have been detected as being malicious within the selected period.
Phishing Sites Blocked	Displays all the sites that GFI WebMonitor has identified as known phishing websites within the selected time period.
Top Virus	Shows the name of the top virus detected by GFI WebMonitor for the selected period.

Table 15: Security dashboard options

### 🚹 NOTE

Use the **View by:** filter in the top right corner of the page to view data for a specific date range.

<b>GFI Web</b> Monitor					
Dashboard Reports Settings	Help				
👁 Overview 🧭 Bandwidth 🗳 Activity 闵 Securit	🗸 🔃 Real-Time Traffic 😽 Quarantine				
Security Report V	-		fo	r period: 7/26/201	2 - 7/26/2012 ¥
All Security				View by	
Infected Files Detected <b>27</b> Avg: 1 / hour	Malicious Sites Blocked 67 Avg: 2 / hour	Phishing Sites Blocked Top Virus 2 Avg: 0 / hour Trojan.	Win32.Generic	!BT	
75 50 25					
03.00 04.00 05.00 06.00 Showing: Viruses Policies <b>Categories</b> Websites	07 <sup>5</sup> 00 08 <sup>5</sup> 00 09 <sup>5</sup> 00 10 <sup>5</sup> 00 11 <sup>5</sup> 00 11 <sup>5</sup> 00 ← Infected files ← Malic Users Event Log	0 12 <sup>7</sup> 00 13 <sup>7</sup> 00 14 <sup>7</sup> 00 15 <sup>7</sup> 00 cious sites -⊪- Phishing sites	16/00 17/00	18:00 19:00	20/00
Filter:					
Category		Breaches 👻	Infected	Malicious	Phishing
1. Private IP Addresses		18	18	0	0
2. Business and Economy		13	0	13	0
3. Society		10	8	2	0
4. Parked Sites		7	0	7	0
5. Spyware and Adware		7	0	7	0
6. Unavailable		6	0	6	0
7. Computer and Internet Info		5	0	5	0
8. Games		5	0	5	0

Screenshot 30: Security Dashboard

The lower portion of the **Security** page provides a breakdown of the data monitored in the specified period. Click the available tabs to view information filtered by the following categories:

Table 16: Security	monitoring filtering options

FILTER	DESCRIPTION
Viruses	A list of detected viruses, with the total number of Breaches.
Policies	Affected policies are listed in this tab, together with the total number of <b>Breaches</b> and the name of the users who made the request.
Categories	Select to view a list of categories with total number of Breaches for each category.
Websites	A list of websites with respective total number of <b>Breaches</b> . Data can be viewed by Domain or by Site using the provided controls.
Users	A list of users and the total <b>Breaches</b> for a specified period, broken down under three headings: Infected, Malicious or Phishing. NOTE Surf Time is an approximate time calculated by timing access to web sites. Every time a user accesses a website, 1 surf time minute will be added for that user. During this minute, the user can access other web sites without adding to the surf time. When the 1 minute has passed, another minute will be added if the user is still browsing.
Event Log	<ul> <li>Provides a log of all the web requests that fall within the specified period, displaying:</li> <li>Web Request - URL of request</li> <li>Time - date and time of request</li> <li>User - User name</li> <li>IP - IP address</li> <li>Reputation Index - the WebGrade index given to the accessed site</li> <li>Engine - the name of the engine that detected the threat</li> </ul>

### 5.4.1 One-click Report Functionality

After you customize the dashboard, the view can be exported as a report or scheduled to be sent automatically as required.

### Export Report

To export the report:

- 1. From the top of the Dashboard, click Report A and select Export Report.
- 2. GFI WebMonitor displays the exported report in a separate window in your browser.
- 3. Click and select one of the following options:

Table 17: Export report options

OPTION	DESCRIPTION
Excel	The report is exported in Microsoft Excel format (.xls)
PDF	The report is exported in PDF format.
Word	The report is exported in Microsoft Word format (.doc)

#### **Schedule Report**

To schedule the report:

- 1. From the top of the Dashboard, click Report A and select Schedule Report.
- 2. GFI WebMonitor redirects you automatically to the Reports area.

For more information, refer to <u>Reporting</u> (page 60).

4. Save the report.

### IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information refer to <u>General Options</u>.

### 5.5 Monitoring Real-Time Traffic

The Real-Time Traffic dashboard enables you to monitor Internet usage in real-time. Monitor current active connections and terminate them if necessary (for example, streaming media or large unauthorized downloads), and view most recent connections. Real-time graphs of bandwidth and activity give you visual indicators of the current situation.

#### IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information refer to <u>General Options</u>.

To access the Real-Time Traffic dashboard:

```
1. Go to Dashboard > Real-Time Traffic.
```

<b>GF</b>	<b>GFI Web</b> Monitor									
Dashb	ooard Reports	Settings	Help							
Over	view 🥝 Bandwidth	🗳 Activity 😵 Security	🚱 Real-Time Tr	raffic 😯 Quarantine						
Real-T	Real-Time Traffic for period: Now									
Active	Connections Bandwi	dth Activity			Auto refresh i	nterval: 1 3 5 10				
29	92.97 KB									
24	44.14 KB			$\wedge$						
19	95.31 KB									
14 Bandwidth 4	16.48 KB 97.66 KB 18.83 KB 15:00:00	15:00:30	15:01:00	15:01:30	15:02:00	15:02:30				
	IP (User)	Url		Status	Downloaded	Uploaded				
1.	192.168.200.8 (unauthenticated)	urs.microsoft.com:443	3	DNS resolving and connecting	0.00 B	0.00 B				
2. 192.168.200.8 (unauthenticated) urs.microsoft.com:443		3	DNS resolving and connecting	0.00 B	0.00 B					
3.	192.168.200.8 (unauthenticated)	urs.microsoft.com:443	3	DNS resolving and connecting	0.00 B	0.00 B				

Screenshot 31: Real-Time Traffic Dashboard, Bandwidth monitoring

#### 2. Click one of the following tabs:

#### Table 18: Real-Time Traffic dashboard options

OPTION	DESCRIPTION
Active Con- nections	Provides information related to current active connections. Active connections can be terminated to free up bandwidth. Additional filtering is available by:
	Categories - Select to view a list of categories with total Web Requests and Bandwidth con- sumption for each category.
	Websites - A list of websites with respective total Web Requestsand Bandwidth consumption per site. Data can be viewed by Domain or by Site using the provided controls.
	» Users - A list of users with total Web Requests and Bandwidth consumption per user.
Bandwidth	A graph displays the current bandwidth consumption in MB. Additional information includes: » IP (User)
	» Url
	» Status
	» Downloaded
	» Uploaded

OPTION	DESCRIPTION
Activity	Displays the number of current web requests
	» IP (User)
	» Url
	» Status
	» Downloaded
	» Uploaded

### **NOTE**

For **Bandwidth** and **Activity** real-time traffic graph, set the **Auto refresh interval** at the top right corner of the page. Default is set to 3.

### 5.6 Using Quarantine

The Quarantine area holds filtered content until the administrator reviews the item and decides what action to take. Perform one of the following actions:

Table 19: Quarantine options				
OPTION	DESCRIPTION			
Approve	Approve a single item in the list.			
Approve All	Approve all items in the list.			
Delete	Delete a single item in the list.			
Delete All	Delete all items in the list.			

The Quarantine list is populated following actions taken by pre-configured policies. The policy which blocked the quarantined item will be listed under **Policy Type**, together with the user, details of the request, date and time.

To approve or delete an item from the Quarantine list:

### 1. Go to Dashboard > Quarantine

GF	<b>GFI Web</b> Monitor							
Das	hboard Reports	Settings	Help					
• 0	verview 🧭 Bandwidth	🝰 Activity 🛭 💱	Security 🙌 Re	al-Time Traffic	😵 Quarantine			
Quarantine for period: 7/22/2012 - 7/23/2012							riod: 7/22/2012 - 7/23/2012 ¥	
A	oprove Approve all	Delete D	elete all					
	User	Request				Policy Type	Date 🔻	
	WORKGROUP\john smi	th http://ww	w.burgerking.c	om/		Filter	7/23/2012 3:08:46 PM	
	WORKGROUP\john smi	th http://ww	w.bbc.co.uk/			Filter	7/23/2012 3:08:35 PM	
	WORKGROUP\john smi	th http://ww	w.cnn.com/			Filter	7/23/2012 3:08:18 PM	
	WORKGROUP\john smi	th http://pla	tform.twitter.co	m/widgets.js		Filter	7/23/2012 3:08:06 PM	
	WORKGROUP\john smi	th http://pla	tform.linkedin.o	.com/in.js		Filter	7/23/2012 3:08:06 PM	
	WORKGROUP\john smi	th http://co	nnect.facebook.	net/en_US/all.j	S	Filter	7/23/2012 3:08:06 PM	
	WORKGROUP\john smi	th http://ww	w.google-analy	rtics.com/ga.js		Filter	7/23/2012 3:08:03 PM	
	WORKGROUP\john smi	th http://ww	w.msn.com/?oo	id=iehp		Filter	7/23/2012 3:08:01 PM	
							Rows: 10 🔻	
Shov	wing: Users Policy Type	s						
Filte	r:	9						
	User	Quarantined 👻	Security	Filter	Download			
1.	WORKGROUP\john smith	8	0	8	0			
					Rows: 10 💌			

Screenshot 32: Quarantine dashboard

- 2. Locate the item to approve or delete, and select the checkbox next to it.
- 3. Click **Approve** or **Delete**.
- 4. From the Approve Access Requests window, click Confirm.

## 6 Reporting

GFI WebMonitor makes use of an in-built reporting engine that enables you to create reports without having to leave the GUI.

You can create reports based on inclusions and exclusions of users, categories and websites thus making sure that reports are targeted and relevant.

Use the reporting engine to create:

- » Department based reporting that can be scheduled and sent to the relevant department heads
- Reports which exclude certain data such as salesforce.com, and other websites or data which is irrelevant
- » Reports which only include certain categories of websites. For example, generate productivity loss reports where only Productivity Loss related categories are added to the report
- » Need based reporting based on Browsing Activity / Bandwidth / Security and other needs
- » Scheduled reports distributed in various formats.

The following sections will help you configure and run the following:

- » Activity Reports
- » Bandwidth Reports
- » Security Reports

### 6.1 Starred Reports

Click **Reports** to access **Starred Reports** and create a list of frequently used reports.

GI	<b>GFI Web</b> Monitor									
Da	Dashboard Reports Settings Help									
🪖 s	tarred 🧭 Bandwidth 🍰 Activity 💱 Security									
<b>"</b>	Starred Reports									
	Report		Scheduled	Report Period	Last Run					
*	Activity – All Activity	🕑 Run	No	This Week	N/A					
*	Activity – Searches	🕟 Run	No	This Week	N/A					
*	Activity Usage Trends	🕑 Run	No	This Week	N/A					
*	Bandwidth – All Bandwidth	🕑 Run	No	This Week	N/A					
*	Bandwidth Usage Trends	🕑 Run	No	This Week	N/A					
*	Productivity - Social Networking Users	🕑 Run	No	This Week	N/A	Î				
*	Search Activity	🕑 Run	No	This Week	N/A					
*	Security – All Security	🕑 Run	No	This Week	N/A					
*	Security – Users Blocked by Security Policies	🕑 Run	No	This Week	N/A	Û				
*	Security - Who is downloading executables?	🕑 Run	No	This Week	N/A	Î				
*	Top Activity Users	🕑 Run	No	This Week	N/A					
*	Top Blocked Users	🕑 Run	No	This Week	N/A					
*	User Activity Log	🖲 Run	No	This Week	N/A					

To add a report to the Starred Reports list:

- 1. Go to **Reports > Bandwidth** or **Activity** tab.
- 2. Click 🖈 next to report name.

3. Starred reports will be marked with  $\star$ .

## 6.2 Activity Reports

GFI WebMonitor offers a set of reports that help you monitor user activity on your network. You can modify existing reports or add new ones customized to your requirements.

To use one of the above reports:

1. Go to **Reports** and select **Activity** tab.

G	<b>GFI Web</b> Monitor									
Da	ishboard	Reports	Settings	Help						
÷ 🖈	starred 🥝	Bandwidth  🐣	Activity 🧋 Securit	У						
ı.	Activity Reports									
	Report				Scheduled	Report Period	Last Run			
*	Activity –	All Activity		🕑 Run	No	This Week	N/A			
☆	Activity –	Allowed Only		🕑 Run	No	This Week	N/A			
☆	Activity – I	Filtered Only by A	ction	🕑 Run	No	This Week	N/A			
☆	Activity – I	Filtered Only by Po	olicy	🕟 Run	No	This Week	N/A			
☆	Activity – I	Filtered Only by T	ype	🕟 Run	No	This Week	N/A			
*	Activity – S	Searches		🕑 Run	No	This Week	N/A			
*	Activity Us	age Trends		🕑 Run	No	This Week	N/A			
☆	Bandwidth	- Non productive	e traffic sites	🕑 Run	No	This Week	N/A	Û		
\$	Bandwidth Searches	- TV Series or Mo	ovie Dowload	🕑 Run	No	This Week	N/A	Û		
☆	Bandwidth	- Who is downloa	ading Zipped files?	🕑 Run	No	This Week	N/A	Û		
☆	Blocking T	rends		🕑 Run	No	This Week	N/A			
☆	Detailed U	ser Activity		🕑 Run	No	This Week	N/A			
☆	HR – Adult	t and Pornography	y Searches	🕑 Run	No	This Week	N/A	Û		
☆	HR – Drug	Related Access		🕑 Run	No	This Week	N/A	Û		
☆	HR – Inapp	propriate websites	5	🕑 Run	No	This Week	N/A	Û		
☆	HR – Job S	earch Websites		🕑 Run	No	This Week	N/A	Û		

Screenshot 33: Default activity report list

### 2. Click one of the report names to edit or click Run to generate the report.



Every report can be exported to Excel, PDF or Word, and can also be sent to a printer.

#### See also:

**Cloning a report** 

**Editing Activity Report** 

#### 6.2.1 Editing Activity Reports

To edit an activity report:

- 1. Go to **Reports** and select **Activity** tab.
- 2. Click report name to edit.

Save <u>Cancel Changes</u>	Clone Report
Report name	
Data Schedule Distribution	
Date Range: This Week 💌	
Record Limit: 1000 per set	

Screenshot 34: Editing a report

- 3. [Optional] Change the name of the report.
- 4. In the Data tab, select a Date Range from the drop down list.

5. In the **Record Limit** field, set the maximum number of records shown in the report. Default is set to 1000 per set.

6. In the **Include** area:

a. Click **Users / Groups** tab and add the users or groups to include or exclude in the report.

b. Click Categories tab to add the categories to include or exclude in the report

c. Click Websites tab and add the domains to include or exclude in the report.

d. Click **Policies** tab to add the policies to include or exclude in the report. You can add policies by name, by the action these policies perform (Limited or Warned) or by policy type (Download, Filter or Security).

7. Go to the Schedule tab and click ON to enable report scheduling.



Data Schedule Distribu	ition						
Schedule: ON OFF NOTE: Schedule to automatically generate this report							
Runs:	Once Daily Weekly Monthly						
Repeat On:	☑ Jan ☑ Feb ☑ Mar ☑ Apr ☑ May ☑ Jun ☑ Jul ☑ Aug ☑ Sep ☑ Oct ☑ Nov ☑ Dec						
On:	day 15 of the month						
At:	8:00 AM						
Repeat Ends:	Never On						

### 8. From the **Runs** area, select if report is going to be generated:

OPTION	DESCRIPTION
Once	In the Run On field, specify a date and time to generate the report one time.
Daily	In the <b>Run Every</b> field, specify the interval in days after which to generate the report. In the <b>At</b> field, specify at which time of day to execute the report. If you want the occurrence to end after a specified period, select <b>On</b> in the <b>Repeat Ends</b> area and define the date, otherwise set the setting to <b>Never</b> (Default).
Weekly	In the <b>Run Every</b> field, specify the interval in weeks and use the <b>Repeat On</b> checkboxes to select the week days on which to generate the report. In the <b>At</b> field, specify at which time of day to execute the report. If you want the occurrence to end after a specified period, select <b>On</b> in the <b>Repeat Ends</b> area and define the date, otherwise set the setting to <b>Never</b> (Default).
Monthly	Use the <b>Repeat On</b> checkboxes to select the months in which the report will be generated. In the <b>On</b> field, specify the day of the month and use the <b>At</b> field to specify at which time of day to execute the report. If you want the occurrence to end after a specified period, select <b>On</b> in the <b>Repeat Ends</b> area and define the date, otherwise set the setting to <b>Never</b> (Default).

Table 20: Activity report schedule options

#### 9. Go to Distribution tab and select one of the following options:

#### Table 21: Activity report distribution options

OPTION	DESCRIPTION
Distribute PDF	Enable to save a PDF document in the path specified in the <b>Folder Destination</b> field. [Optional] In the <b>Email Recipients</b> field, add a recipient email address to send the document by email.
Distribute XLS	Enable to save a document in .XLS format in the path specified in the <b>Folder Destination</b> field. [Optional] In the <b>Email Recipients</b> field, add a recipient email address to send the document by email.
Distribute DOC	Enable to save a document in .DOC format in the path specified in the <b>Folder Destination</b> field. [Optional] In the <b>Email Recipients</b> field, add a recipient email address to send the document by email.

#### 10. Click Save.

11. To generate the report, click Run.

### 6.3 Bandwidth Reports

GFI WebMonitor offers a set of reports that help you monitor bandwidth activity on your network. Use these reports to identify non-productive traffic, download trends and usage patterns, so that adequate action can be taken if need be. You can modify existing reports or add new ones customized to your requirements.

To use one of the above reports:

1. Go to **Reports** and select **Bandwidth** tab.

G	<b>GFI Web</b> Monitor								
Da	ishboard Repor	ts Settings	Help						
* 2	itarred 🤭 Bandwidth	🗳 Activity 🛭 💱 Secu	rity						
<u>الل</u>	Bandwidth Reports								
	Report			Scheduled	Report Period	Last Run			
*	Bandwidth – All Band	width	🕑 Run	No	This Week	N/A			
\$	Bandwidth - Downloa	ad Only	🕑 Run	No	This Week	N/A			
☆	Bandwidth – Non pro	ductive traffic	🕑 Run	No	This Week	N/A	ŵ		
\$	Bandwidth - Upload	Only	🕑 Run	No	This Week	N/A			
*	Bandwidth Usage Tre	nds	🕑 Run	No	This Week	N/A			
☆	Bandwidth Usage Tre	nds – Downloads	🕑 Run	No	This Week	N/A	Û		
\$	Bandwidth Usage Tre	nds – Uploads	🕑 Run	No	This Week	N/A	ŵ		
☆	Detailed User Bandwi	dth	🕑 Run	No	This Week	N/A			

Screenshot 36: Default bandwidth reports list

2. Click one of the report names to edit or click **Run** to generate the report.

#### 

Every report can be exported to Excel, PDF or Word, and can also be sent to a printer.

### See also:

#### Cloning a report

Editing Bandwidth Report

#### 6.3.1 Editing Bandwidth Reports

To edit an bandwidth report:

- 1. Go to Reports and select Bandwidth tab.
- 2. Click report name to edit.

Save <u>Cancel Changes</u>	Clone Report
Report name	
Data Schedule Distribution	
Date Range: This Week 💌	
Record Limit: 1000 per set	

Screenshot 37: Editing a report

- 3. [Optional] Change the name of the report.
- 4. In the Data tab, select a Date Range from the drop down list.

5. In the **Record Limit** field, set the maximum number of records shown in the report. Default is set to 1000 per set.

6. In the Include area:

a. Click **Users / Groups** tab and add the users or groups to include or exclude in the report.

- b. Click **Categories** tab to add the categories to include or exclude in the report
- c. Click Websites tab and add the domains to include or exclude in the report.
- 7. Go to the Schedule tab and click ON to enable report scheduling.



Data <b>Schedule</b> Distribu	ition			
Schedule: ON OFF NOTE: Schedule to automatically generate this report				
Runs:	Once Daily Weekly Monthly			
Repeat On:	🗹 Jan 🗹 Feb 🔍 Mar 🗹 Apr 🗹 May 🔍 Jun 🕼 Jul 🔍 Aug 🔍 Sep 🕼 Oct 🔍 Nov 🔍 Dec			
On:	day 15 of the month			
At:	8:00 AM			
Repeat Ends:	Never On			

Screenshot 38: Scheduling an activity report

#### 8. From the **Runs** area, select if report is going to be generated:

OPTION	DESCRIPTION
Once	In the <b>Run On</b> field, specify a date and time to generate the report one time.
Daily	In the <b>Run Every</b> field, specify the interval in days after which to generate the report. In the <b>At</b> field, specify at which time of day to execute the report. If you want the occurrence to end after a specified period, select <b>On</b> in the <b>Repeat Ends</b> area and define the date, otherwise set the setting to <b>Never</b> (Default).
Weekly	In the <b>Run Every</b> field, specify the interval in weeks and use the <b>Repeat On</b> checkboxes to select the week days on which to generate the report. In the <b>At</b> field, specify at which time of day to execute the report. If you want the occurrence to end after a specified period, select <b>On</b> in the <b>Repeat Ends</b> area and define the date, otherwise set the setting to <b>Never</b> (Default).
Monthly	Use the <b>Repeat On</b> checkboxes to select the months in which the report will be generated. In the <b>On</b> field, specify the day of the month and use the <b>At</b> field to specify at which time of day to execute the report. If you want the occurrence to end after a specified period, select <b>On</b> in the <b>Repeat Ends</b> area and define the date, otherwise set the setting to <b>Never</b> (Default).

Table 22: Activity report schedule options

9. Go to Distribution tab and select one of the following options:

Table 23: Activity report distribution options

OPTION	DESCRIPTION
Distribute PDF	Enable to save a PDF document in the path specified in the <b>Folder Destination</b> field. [Optional] In the <b>Email Recipients</b> field, add a recipient email address to send the document by email.
Distribute XLS	Enable to save a document in .XLS format in the path specified in the <b>Folder Destination</b> field. [Optional] In the <b>Email Recipients</b> field, add a recipient email address to send the document by email.
Distribute DOC	Enable to save a document in .DOC format in the path specified in the <b>Folder Destination</b> field. [Optional] In the <b>Email Recipients</b> field, add a recipient email address to send the document by email.

10. Click Save.

11. To generate the report, click Run.

### 6.4 Security Reports

GFI WebMonitor offers a set of reports that help you monitor suspicious activity on your network. Use the Security Reports to identify:

- » The amount of infected files detected by GFI WebMonitor
- » Details of any Phishing sites blocked
- » A list of viruses that threatened your organization's network.

You can modify existing reports or add new ones customized to your requirements:

1. Go to **Reports** and select **Security** tab.

<b>GFI Web</b> Monitor							
Dashboard	Reports	Settings Help					
🚖 Starred 🧭	Bandwidth 🗳	Activity 😽 Security					
💼 Securit	Security Reports						
Report			Scheduled	Report Period	Last Run		
🖌 Security –	All Security	🕑 Run	No	This Week	N/A		
😭 Security –	Monthly Report	🖲 Run	Monthly	This Month	N/A	Û	

Screenshot 39: Default Security reports list

2. Click one of the report names to edit or click Run to generate the report.



See also: <u>Cloning a report</u> <u>Editing Security Report</u>

### 6.4.1 Editing Security Reports

To edit a Security report:

- 1. Go to **Reports** and select **Activity** tab.
- 2. Click report name to edit.

Save <u>Cancel Changes</u>	Clone Report
Report name	
Data Schedule Distribution Date Range: This Week	
Record Limit: 1000 per set	

Screenshot 40: Editing a report

3. [Optional] Change the name of the report.

4. In the Data tab, select a Date Range from the drop down list.

5. In the **Record Limit** field, set the maximum number of records shown in the report. Default is set to 1000 per set.

6. In the **Include** area:

a. Click **Users / Groups** tab and add the users or groups to include or exclude in the report.

- b. Click **Categories** tab to add the categories to include or exclude in the report
- c. Click Websites tab and add the domains to include or exclude in the report.
- 7. Go to the Schedule tab and click ON to enable report scheduling.



If the schedule is disabled, report is not automatically generated.

Data Schedule Distribu	ution				
Schedule: ON OFF NOTE: Schedule to automatically generate this report					
Runs:	Once Daily Weekly Monthly				
Repeat On:	☑ Jan ☑ Feb ☑ Mar ☑ Apr ☑ May ☑ Jun ☑ Jul ☑ Aug ☑ Sep ☑ Oct ☑ Nov ☑ Dec				
On:	day 15 of the month				
At:	8:00 AM				
Repeat Ends:	Never On				

Screenshot 41: Scheduling an activity report

#### 8. From the **Runs** area, select if report is going to be generated:

OPTION	DESCRIPTION				
Once	In the Run On field, specify a date and time to generate the report one time.				
Daily	In the <b>Run Every</b> field, specify the interval in days after which to generate the report. In the <b>At</b> field, specify at which time of day to execute the report. If you want the occurrence to end after a specified period, select <b>On</b> in the <b>Repeat Ends</b> area and define the date, otherwise set the setting to <b>Never</b> (Default).				
Weekly	In the <b>Run Every</b> field, specify the interval in weeks and use the <b>Repeat On</b> checkboxes to select the week days on which to generate the report. In the <b>At</b> field, specify at which time of day to execute the report. If you want the occurrence to end after a specified period, select <b>On</b> in the <b>Repeat Ends</b> area and define the date, otherwise set the setting to <b>Never</b> (Default).				
Monthly	Use the <b>Repeat On</b> checkboxes to select the months in which the report will be generated. In the <b>On</b> field, specify the day of the month and use the <b>At</b> field to specify at which time of day to execute the report. If you want the occurrence to end after a specified period, select <b>On</b> in the <b>Repeat Ends</b> area and define the date, otherwise set the setting to <b>Never</b> (Default).				

#### Table 24: Activity report schedule options

#### 9. Go to Distribution tab and select one of the following options:

OPTION	DESCRIPTION
Distribute PDF	Enable to save a PDF document in the path specified in the <b>Folder Destination</b> field. [Optional] In the <b>Email Recipients</b> field, add a recipient email address to send the document by email.
Distribute XLS	Enable to save a document in .XLS format in the path specified in the <b>Folder Destination</b> field. [Optional] In the <b>Email Recipients</b> field, add a recipient email address to send the document by email.
Distribute DOC	Enable to save a document in .DOC format in the path specified in the Folder Destination field. [Optional] In the Email Recipients field, add a recipient email address to send the document by email.

### Table 25: Activity report distribution options

### 10. Click Save.

11. To generate the report, click Run.

### 6.4.2 Cloning Reports

All the default reports can be cloned to create new custom reports.

To clone a report:

- 1. Go to **Reports** and select **Bandwidth** or **Activity** tab.
- 2. Click Edit Report next to the report you want to clone.
- 3. Change the name of the report and click **Clone Report**.

## 7 Configuring GFI WebMonitor

This chapter assists in the configuration of the following:

### General settings

- 1. Licensing
- 2. Remote Access Control
- 3. Data Retention, Notification language and Anonymization
- 4. Auto-update of internal scanning engines
- 5. Web Categorization
- 6. Database settings

### Policies

- 1. Security policies
- 2. Internet policies
- 3. Download control policies
- 4. Always Blocked list, Always Allowed list and Temporary Allowed configuration

### Alerts

1. Monitoring, Bandwidth and Security alerts

### 🚹 ΝΟΤΕ

When you have more than one GFI WebMonitor instance deployed in your organization, use the Settings Importer Tool to quickly export settings from a configured GFI WebMonitor installation and import the same settings into a new installation. Using simple command line scripting, you can export and import GFI WebMonitor configurations to synchronize the multiple instances. For more information, refer to Using the Settings Importer Tool (page 37).

### 7.1 General Settings

The following sections help you configure settings related to how GFI WebMonitor works.

OPTION	DESCRIPTION
Licensing	View current licensing configuration or update with a new license key.
Remote Access Control	Configure windows authentication and create authorization rules to grant or deny user access to the application.
Auto-update	Turn on or off auto-update settings for the core components of GFI WebMonitor
Database	Specify the backend database type for GFI WebMonitor
Notifications	Define settings for notifications related to administrative tasks.
Options	Configure data retention period, downloaded file cache size, notification language, expiry period for temporary allowed browsing and anonymization.
Web categorization	Enable Web Categorization online lookup for web sites not found within the local database.

#### Table 26: General Settings

### 7.1.1 Updating License Manually

To start using GFI WebMonitor, a valid license key must be activated.

To update product license key:

- 1. Go to Settings > General > Licensing
- 2. Click Update License and enter license key.
- 3. Click Apply.

## 📄 note

To activate license key, an Internet connection must be available.

### See Also:

Licensing Information.

Post-Installation Actions.

### 7.1.2 Remote Access Control

The Remote Access Control node enables you to:

- Turn Windows Authentication on or off for users defined in the configured Authorization Rules. When Windows Authentication is enabled, you can grant access to the GFI WebMonitor UI using Active Directory Users and Groups. For more information refer to <u>Configuring Windows Authen-</u><u>tication</u>.
- Add new Authorization Rules to grant limited access to users to different sections of GFI Web-Monitor. Users, groups or IPs listed in the configured Authorization Rules will have access to limited views on the data so that, for example, Departmental Managers can access the Dashboards and Reports of members of their teams. For more information, refer to Add a New Authorization <u>Rule</u> (page 72).

### **Configuring Windows Authentication**

When **Windows Authentication** is enabled, you can For more information, refer to <u>Configuring</u> <u>Windows Authentication</u> (page 71).

### IMPORTANT

Users or groups specified in the **Authorization Rules** are allowed access **only** if their username is authenticated.

To turn Windows Authentication on or off:

1. Go to Settings > General > Remote Access Control.

<b>GFI</b> WebMonitor							
D	ashboard	Reports	Settings	Help			
ŵ	General Licensing		🚑 Remote	Access Control	?		
	Remote Access Auto-Update	Control	Authentication Set Windows A	tings authentication	ON	OFF	Applies to everyone
	Notifications Options		Configured Author Default Au	rization Rules thorization Rule	ON	OFF	
8	Web Categorizat	tion •	Add Authorizatio	n Rule			
	Proxy Settings						

Screenshot 42: Configuring Access Control

2. Next to Windows Authentication, click ON or OFF.

### Add a New Authorization Rule

Configured **Authorization Rules** grant or deny access to users to different sections of GFI WebMonitor. Users, groups or IPs listed in the configured Authorization Rules will have access to limited views on the data so that, for example, Departmental Managers can access the Dashboards and Reports of members of their teams.

To add a new Authorization Rule:

- 1. Go to Settings > General > Remote Access Control.
- 2. Click Add Authorization Rule.
| Save <u>Cancel Changes</u> | i de la constante de |
|----------------------------|--|
| Name:                      | New Authorization Rule   |
| Apply Rule to:             | john Smith ×<br>User Group IP Add ?  |
| Can View Data for:         | Everyone User Group IP Add ?   |
| Access Rights:             | Dashboard     View Dashboard     Allow Block   |
|                            | S View Quarantine Allow Block  |
|                            | View Real Time Traffic Allow Block   |
|                            | Reports       Image: View Reports     Allow     Block  |
|                            | Change Reports Allow Block   |
|                            | Settings   |
|                            |  |
| Save <u>Cancel Changes</u> |  |

Screenshot 43: Adding a new Authorization Rule

3. In the **Apply Rule to** field, specify the **User**, **Group** or **IP Address**, to whom the rule will apply. Repeat for all required users, groups and/or IPs.

# IMPORTANT

Users or groups specified in the Authorization Rules are allowed access only if Windows Authentication is enabled and their username is authenticated. When Windows Authentication is disabled, use IP addresses instead. For more information, refer to <u>Configuring Windows Authentication</u> (page 71).

4. In the **Can View Data for** field, specify the **User**, **Group** or **IP Address**, to whom the user specified in the previous step has access to. For example, John Smith, the Marketing Manager, has access to all users in the Marketing group. Repeat for all required users, groups and/or IPs.

5. In the Access Rights area, Allow or Block the following:

OPTION	DESCRIPTION
View Dash- board	When enabled, user can view Bandwidth, Activity and Security Dashboard. Access to Quarantine and Real Time Traffic dashboards can be granted or denied using additional controls.

OPTION	DESCRIPTION
View Quar- antine	This option is only available when <b>View Dashboard</b> is enabled. Click <b>Allow</b> to grant access to Quarantine area.
View Real Time Traffic	When enabled, user can monitor Real-time traffic and terminate active connections.
View Reports	Click Allow to enable access to Reports node. User will be able to generate all configured reports.
Change Reports	When enabled, user can modify, delete and create new reports. Only available if <b>View Reports</b> is enabled.
Change Set- tings	When enabled, user is allowed access to Settings area and can modify GFI WebMonitor settings.

6. Click Save.

### 7.1.3 Configuring Auto-Update

The **Auto-Update** page provides a centralized area where to configure auto-update settings for the core components of GFI WebMonitor.



Screenshot 44: Configuring Auto-update

To enable or disable auto-update for the available components:

- 1. Go to Settings > General > Auto-Update.
- 2. Click **ON** or **OFF** to enable or disable the components as required.

🚹 NOTE

It is recommended that all auto-updates are enabled for maximum protection.

#### 7.1.4 Configuring Databases

GFI WebMonitor supports two types of databases:

Table 27: Back-end databases	
DATABASE	DESCRIPTION
Firebird Database	Firebird is the default database, configured automatically with the installation.
Microsoft SQL Database	GFI WebMonitor supports both Microsoft SQL Express and Microsoft SQL server databases.

The currently configured database can be viewed from Settings > General > Database.

<b>GFI Web</b> Monitor							
Dashl	board I	Reports	Settings	Help			
Ge Lic Ac Au Da No Op	eneral eensing cess Control tto-Update tabase utifications ptions	•	Configure data	ASE         :abase backend for GFI WebMonitor         tabase type:       Embedded       SQL Server         Path:       C:\Program Files\GFI\WebMonitor\Data\WEBMON.FDB			
<ul> <li>Po</li> <li>Ale</li> <li>Pro</li> </ul>	licies erts oxy Settings	* * *					

Screenshot 45: Configured database

To change the current database configuration refer to the following sections:

- » Configuring Firebird Database
- » Configuring Microsoft SQL Database

#### **Configuring Firebird Database**

During installation, GFI WebMonitor automatically installs a Firebird database that is used by the application as the default database. The default path is: C:\Program Files\GFI\WebMonitor\Data\WEBMON.FDB.

To change the default location of the Firebird database:

- 1. Go to C:\Program Files\GFI\WebMonitor\Data and copy the WEBMON.FDB file.
- 2. Save the copied file to the new location.
- 3. In GFI WebMonitor, go to **Settings > General > Database**.

G	GFI WebMonitor						
D	ashboard	Reports	Settings	Help	p		
ŵ	General Licensing		😑 Databas	ie i			
	Access Control Auto-Update Database		Configure datal Data	base backend base type:	Embedded SQL Server		
	Notifications Options Web Categorizatio	n		Path:	C:\Program Files\GFI\WebMonitor\Data\WEBMON.FDB		
٨	Policies	*					
0	Alerts	*					
0	Proxy Settings	*					

Screenshot 46: Configuring Databases

- 4. From Database Type, select Embedded.
- 5. In the **Path** field, change the path to the point to the new location.
- 6. Click Save.



To create a new Firebird Database, enter a new database name in the following format: <*database name*>.fdb

# Configuring Microsoft<sup>®</sup> SQL Database

GFI WebMonitor supports both Microsoft<sup>®</sup> SQL Server Express and Microsoft<sup>®</sup> SQL Server databases.

To point GFI WebMonitor to use a previously created Microsoft<sup>®</sup> SQL Server database:

1. In GFI WebMonitor, go to **Settings > General > Database**.

2. From Database Type, select SQL Server.

Save <u>Cancel Changes</u>	
Configure database backen	d for GFI WebMonitor
Database type:	Embedded SQL Server
SQL Server:	<sql instance="" name=""></sql>
Authentication:	Windows Authentication SQL Server Authentication
	Username: sa
	Password:
Database:	WEBMON

- 3. In the SQL Server field, type the SQL Server<sup>®</sup> instance name.
- 4. In the Authentication area, select one of the following:

#### Table 28: SQL Server<sup>®</sup> Authentication method

OPTION	DESCRIPTION
Windows Authen- tication	Select this option to use Windows $^{\ensuremath{\mathbb{B}}}$ credentials when connecting to your SQL Server $^{\ensuremath{\mathbb{R}}}$ .
SQL Server Authen- tication	If your SQL Server <sup>®</sup> has been installed in SQL Server Authentication Mode, select this option and provide <b>Username</b> and <b>Password</b> .

5. In the **Database** field, type the name of the database created in SQL Server<sup>®</sup>.

#### IMPORTANT

Ensure that the database name entered is unique, otherwise you will overwrite the existing database.

#### 6. Click Save.

### 🚹 NOTE

You can create a new database from within GFI WebMonitor. To create a new database, enter a new database name and click **Save**.

#### 7.1.5 Configuring Notifications

When Notifications are configured, GFI WebMonitor sends email messages containing information related to tasks such as auto-updates and licensing issues to specified email addresses.

To change the administrative notifications setup configured during installation:

1. Go to Settings > General > Notifications.

<b>GF</b>	<b>GFI Web</b> Monitor					
Dashb	poard Repor	ts Settings He	lp			
🚱 Ge	neral	Notifications				
Rer	ensing mote Access Control	Configure the settings GFI	WebMonitor should use to send important administrative notifications			
Dat	tabase	From email address	WebMonitor@127.0.0.1			
Not Op	tifications tions	SMTP Server	127.0.0.1			
We	b Categorization	SMTP Port	25			
<ul><li>Pol</li><li>Ale</li><li>Pro</li></ul>	licies erts	<ul> <li>Email addresses</li> </ul>	Administrator@127.0.0.1 × johndoe@tcdomainb.com ×			
J PR	ovà serrinda		Verify Mail Settings			

Screenshot 47: Configuring administrative notifications

#### 2. Change any of the following options:

Table 29: Configuring administrative notifications

OPTION	DESCRIPTION
From email address	Specify the email address from which notifications will be sent.
SMTP Server	Enter the name or IP of the SMTP server.
SMTP Port	Key in a port number.
Email addresses	Enter recipient email addresses.

#### 3. Click Save.

#### 7.1.6 Configuring Web Categorization

When GFI WebMonitor is installed, a database with a limited amount of categorized web sites is installed. GFI WebMonitor updates this local database on activation.

Web categorization is a feature that connects to the Internet to look up URL's not found in the local database. For more information on website categorization refer to the following whitepaper: <a href="http://www.gfi.com/whitepapers/web-reputation-wp.pdf">http://www.gfi.com/whitepapers/web-reputation-wp.pdf</a>.

### NOTE

This feature is enabled by default. To disable Web Categorization, click **OFF** next to **Online Lookup**.

GFI WebMonitor								
Dashboard Re	ports	Settings	Help					
😂 General		📏 Web Cate	gorization					
Remote Access Contr Auto-Update	rol	Web Categorization c	onfiguration 🥐					
Database		Online	Lookup: ON	OFF	Enable real-t	ime lookup for	URLs not found i	in the local database (Recommen
Options		Lookup	website:				Check Category	Send URL Feedback to GFI
Web Categorization	-							
Alerts	*							
🥪 Proxy Settings	*							

Screenshot 48: Configuring Web Categorization

The Web Categorization page also provides a lookup area where you can check a category for a specific URL.

To look up a URL:

F)

- 1. Enter a URL in the Lookup website field.
- 2. Click Check Category.

NOTE

This feature is also available on the Dashboard. For more information, refer to <u>Overview of Internet Activity</u> (page 44).

# 7.2 Configuring Policies

Policies within GFI WebMonitor help you boost employee productivity while putting your mind at rest about security breaches. These can be very costly to your business.

GFI WebMonitor lets you define web filtering and web security policies to help enforce an effective Internet Usage Policy:

WebFilter Edition Policies - offering time, bandwidth and category based policies

1. Configuring Internet Policies

2. Configuring Always Blocked list

3. Configuring Always Allowed list

4. Configuring Temporary Allowed list

**WebSecurity Edition Policies** - to protect against viruses, spyware, phishing scams and other malware

- 1. Configuring Security Policies
- 2. Configuring Download Policies

#### 7.2.1 WebFilter Edition Policies

WebFilter edition includes policies related to time and bandwidth based browsing control, website categorization and URL filtering for increased productivity and security.

#### The following sections help you:

- » Configure Internet Policies
- » Configure Always Blocked list
- » Configure Always Allowed list
- » Configure Temporary Allowed list

#### Enabling or Disabling a Configured Policy

To enable or disable a policy:

- 1. Go to Settings > Policies > Internet Policies.
- 2. Click **ON** to enable or **OFF** to disable the desired policy.

#### Deleting a Policy

To delete a policy click the **Delete** icon next to the policy to delete.

#### 7.2.2 Configuring Internet Policies

The following chapters guide you through the configuration of the following policies:

POLICY	DESCRIPTION
Web Filtering Policy	Exercise control over web browsing habits that can effect security, productivity, performance and legal issues.
Web Browsing Quota Policy	Control how your users browse specific categories or sites based on bandwidth or time thresholds.
Instant Messaging and Social Con- trol Policy	Provide control over the use of instant messaging clients.
Streaming Media Policy	Define policies that block various types of streaming media across all websites.
Search Engine Policy	Provides monitoring and control over user searching habits.

#### Web Filtering Policy

Web filtering policies enable you to exercise control over web browsing habits that can effect security, productivity, performance and legal issues.

A Default Web Filtering Policy is enabled when GFI WebMonitor is installed. It is pre-configured to apply to everyone and to allow web browsing of all categories. The default policy can be edited, but cannot be disabled or deleted.

# 🚺 ΝΟΤΕ

Certain fields in the default policy cannot be edited. These include **Policy Name** and **Apply Policy To**.

#### IMPORTANT

All added policies take priority over the default policy.

To add a Web Filtering Policy:

- 1. Go to Settings > Policies > Internet Policies.
- 2. In the Web Filtering Policies area, click Add Policy.

Save <u>Cancel Changes</u>	
Policy Name: Web Filtering Policy	
Filter:	Image: Second system   Image: Second system
Bot Nets Confirmed SPAM Sources	
Show Advanced Filtering Exceptions: Always block sites: None	Add 📀
Always allow sites: None	Add 🕜
Filter by Reputation: ON OFF	
Apply Policy to: None User Group IP	Арріу То 📀
Notify Breacher: ON OFF Note: The notificati authenticated or the	on can only be sent if the policy breacher is e IP is mapped.
Notify Administrators: ON OFF	

Screenshot 49: Creating a new Web Filtering policy

3. In the **Policy Name** field, type a policy name.

4. In the Filter area, select the categories to Allow, Block, Warn and Allow or Quarantine.

5. [Optional] Click **Show Advanced Filtering** to add conditions that override actions specified in the **Filter** area.

6. In the **Exceptions** area, use the **Always block sites** and **Always allow sites**fields to key in specific URL's of websites to include or exclude from policy.



7. [Optional] In the Filter by Reputation area, click **ON** to enable filtering by reputation. The following table defines how reputation is classified within the categorization database:

Table 30: Reputation index classification

INDEX	DEFINITION
(1 - 20)	High Risk
(21 - 40)	Suspicious
(41 - 60)	Moderate Risk
(61 - 80)	Low Risk
(81 - 100)	Trustworthy

# 🚹 NOTE

Setting up a Reputation Index of 40 or below blocks websites categorized as "Unknown". When GFI WebMonitor is deployed, a local web categorization database is installed with a limited amount of entries. URL's not found in the local database will be automatically categorized as "Unknown". Ensure that Online Lookup is enabled so that GFI WebMonitor can access a store of over 280 million websites. For more information, refer to <u>Configuring Web Categorization</u> (page 78).

8. In the **Apply Policy To** field, specify **Users, Groups** or **IPs**for whom the new policy applies, and click**Add**.

9. [Optional] In the **Notify Breacher** area, click **ON**to enable notifications to send when a user infringes policy. Provide the body text of the notification email in the available space.

10. [Optional] Use the **Notify Administrators** area to send notifications when the downloaded content infringes this policy. Add the administrator's email address and provide the body text of the notification email.

11. In the **Schedule**area specify the time period during which the new policy is enforced.

12. Click Save.

See also:

#### **Cloning a Policy**

#### Web Browsing Quota Policy

Create a Web Browsing Quota Policy to control how your users browse specific categories or sites based on bandwidth or time thresholds.

To create a new Web Browsing Quota Policy:

- 1. Go to Settings > Policies > Internet Policies.
- 2. In the Web Browsing Quota Policy area, click Add Policy.

Save <u>Cancel Changes</u>	Clone Policy
Policy Name:	Web Browsing Quota Policy
Limit By:	Bandwidth Time 1 Hour (s) per 🗐 🗐
Apply To:	▼ Categories X Social Network X Category Site Add
	Exclude Sites: *.linkedin.com 🗶
Apply Policy to:	john Smith 🕱 Apply To
Notify Breacher:	ON OFF Note: The notification can only be sent if the policy breacher is authenticated or the IP is mapped.
	Message to Policy Breacher:
	Your request has been blocked by GFI WebMonitor. The web browsing policy threshold has been exceeded.
Notify Administrators:	ON OFF
Save <u>Cancel Changes</u>	

Screenshot 51: Creating a new Web Browsing Quota Policy

- 3. In the **Policy Name** field, type a policy name.
- 4. In the Limit By area specify:
  - a. If the threshold will be based on Bandwidth or Time
  - b. The duration in hours or minutes
  - c. If the duration is per day, week or month

#### 5. In the **Apply To** area:

- a. Select which categories or sites are effected by policy.
- b. Add sites which are to be excluded from policy.

6. In the **Apply Policy To** field, specify **Users, Groups** or **IPs** for whom the new policy applies, then click **Add**.

7. [Optional] In the **Notify Breacher** area, click **ON** to enable notifications to send when a user infringes this policy. Provide the body text of the notification email in the available space.

8. [Optional] Use the **Notify Administrators** area to send notifications when the downloaded content infringes this policy. Add the administrator's email address and provide the body text of the notification email.

9. Click Save.

# 📄 ΝΟΤΕ

To reset the Web Browsing Quota Policy, click the refresh icon from the Internet Policies page.

#### See also:

#### Cloning a Policy

#### Instant Messaging and Social Control Policy

Instant Messaging (or IM) and Social Control policies provide control over the use of instant messaging clients and social networking services. If a policy is breached, GFI WebMonitor uses the configured policy to determine what action to take.

The Instant Messaging Policy feature can allow or block access to the following clients:

- » MSN<sup>®</sup> Messenger and Microsoft Windows Live<sup>®</sup> Messenger
- » Gmail Chat/GTalk and
- » Yahoo! Messenger
- » Facebook Chat
- » Online instant messaging portals.

Social Controls, grant or deny access to the following:

- » facebook
- » google+
- » Twitter
- » Other social networking sites

A Default IM and Social Control policy is enabled when GFI WebMonitor is installed. It is pre-configured to allow access to all instant messaging clients and social networking services to all users on your network. The default policy can be edited, but cannot be disabled or deleted. Any changes made to the default policy apply to all users.

### 🚹 NOTE

Certain fields in the default policy cannot be edited. These include **Policy Name** and **Apply Policy To**.

#### IMPORTANT

All added policies take priority over the default policy.

- To create a new IM Policy:
- 1. Go to Settings > Policies > Internet Policies.
- 2. In the Instant Messaging / Social Control Policies area, click Add Policy.

Save <u>Cancel Change</u>	5	
Policy Name:	Block google+	
Filter:	Instant Messaging Controls 💡	
	🍓 MSN Client	Allow Block
	talk Google Talk	Allow Block
	🚭 Yahoo Messenger	Allow Block
	Racebook Chat	Allow Block
	🦰 Online Portals	Allow Block
	Social Controls 💡	
	Facebook Apps	Allow Block
	8 <sup>+</sup> Google+	Allow Block
	E Twitter	Allow Block
	Others	Allow Block
Apply Policy to:	staff ×	
	User Group IP	Apply To ?
Notify Breacher:	ON OFF Note: The not authenticated	tification can only be sent if the policy breacher is I or the IP is mapped.
Notify Administrators:	ON OFF	
Save <u>Cancel Change</u>	5	



- 3. In the **Policy Name** field, type a policy name.
- 4. In the Filter area:

- Under Instant Messaging Controls, specify which instant messaging client to block or allow.
- Under Social Controls, specify which social networking service to block or allow.

5. In the **Apply Policy To** field, specify **Users, Groups** or **IPs** for whom the new policy applies, then click **Add**.

# 🚺 ΝΟΤΕ

It is recommended that only one IM Control Policy is applied to a user, a group and/or IP address. In cases where more than one IM Control Policy is applied to the same user, group or IP, the top most policy takes priority over subsequent policies.

6. [Optional] In the **Notify Breacher** area, click **ON** to enable notifications to send when a user infringes this policy. Provide the body text of the notification email in the available space.

7. [Optional] Use the **Notify Administrators** area to send notifications when the downloaded content infringes this policy. Add the administrator's email address and provide the body text of the notification email.

8. Click Save.

See also:

**Cloning a Policy** 

#### **Streaming Media Policy**

Streaming Media Policies enable you to define policies that block various types of streaming media across all websites. This conserves and optimizes bandwidth resources.

A Default Streaming Media Policy is enabled when GFI WebMonitor is installed. It is pre-configured to allow streaming media access to everyone. The default policy can be edited, but cannot be disabled or deleted.

### 📄 NOTE

Certain fields in the default policy cannot be edited. These include **Policy Name** and **Apply Policy To**.

### IMPORTANT

All added policies take priority over the default policy.

To add a Streaming Media Policy:

- 1. Go to Settings > Policies > Internet Policies.
- 2. In the Streaming Media Policies area, click Add Policy.

Save (	Cancel Changes		
	Policy Name:		
	Filter:	Streaming Media Categories	
		Streaming Media Allow Block	
		Image and Video Search Allow Block	
		Streaming Applications	
		iTunes Allow Block	
		QuickTime Allow Block	
		Winamp Allow Block	
		Vindows Media Player Allow Block	
		Generic Site Streams	
		Generic Site Streams Allow Block	
	Exceptions:	Always block sites: None Add ?	
		Always allow sites: None Add ?	
Apj	ply Policy to:	None User Group IP Apply To ?	

Screenshot 53: Configuring Streaming Media policy 1

3. In the **Policy Name** field, type a policy name.

4. In the Filter area, select the Streaming Media Categories, Streaming Applications and Generic Site Streams to Allow or Block.

5. Use the **Always block sites** and **Always allow sites** fields to key in specific URL's of websites you would like included or excluded from the policy.

6. In the **Apply Policy To** field, specify **Users, Groups** or **IPs** for whom the new policy applies, then click **Add**.

🚹 NOTE

- » When keying in a **User**, specify the username in the format domain\user.
- When keying in a Client IP, you can use IP ranges (for example, "10.0.0.10-12" includes these IP addresses: "10.0.0.10", "10.0.0.11" and "10.0.0.12").

7. [Optional] In the **Notify Breacher** area, click **ON** to enable notifications to send when a user infringes this policy. Provide the body text of the notification email in the available space.

8. [Optional] Use the **Notify Administrators** area to send notifications when the downloaded content infringes this policy. Add the administrator's email address and provide the body text of the notification email.

9. In the Filter On area specify the time period during which the new policy will be enforced.

10. Click Save.

See also:

**Cloning a Policy** 

### Search Engine Policies

GFI WebMonitor has two search engine policies that are disabled by default when the product is installed.

### Safe Search

**Safe Search** is a feature supported by a number of search engines. If enabled, GFI WebMonitor enforces filtering of explicit email and images from user searches.

Safe Search is compatible with the following search engines:

- » Google
- » Yahoo
- » Lycos
- » Bing.

📄 NOTE

The Safe Search feature is available in the GFI WebMonitor WebFilter Edition.

Search Engine Policies	
Safe Search	ON OFF Applies to everyone
Search Terms Monitoring	ON OFF Applies to everyone

Screenshot 54: Safe Search and Search Terms Monitoring

#### To enable Safe Search

1. Go to Settings > Internet Polices > Safe Search.

#### 2. Click ON.

#### Search Terms Monitoring

**Search Terms Monitoring** is a feature that monitors and logs terms used during searches. If enabled, you will be able to monitor what your users are searching for in various search engines to get a better insight on what users are using the web for.

To enable Search Terms Monitoring

- 1. Go to Settings > Internet Polices > Search Terms Monitoring.
- 2. Click ON.

To exclude users or IP addresses from monitoring:

- 1. Go to Settings > Internet Polices > Search Terms Monitoring.
- 2. Click Search Terms Monitoring.
- 3. Key in the User name or IP Address in the field provided and click **Exclude**.

#### 7.2.3 Configuring Always Blocked List

The Always Blocked list is a list of sites, users and IP addresses that should always be blocked. The Always Blocked list takes priority over all WebFilter and WebSecurity policies.

## 🚺 ΝΟΤΕ

If the items in the Always Blocked list are also added to the Always Allowed list, priority is granted to the Always Allowed list and access is granted.

#### Adding Items to the Always Blocked list

To add an item to the Always Blocked list:

1. Go to Settings > Policies > Always Blocked.

<b>GFI</b> WebMonitor				
Dashboard Re	ports Se	ttings	Help	
<ul><li>General</li><li>Policies</li></ul>		Always Bloc	ked	
Internet Policies Security Policies	The U	sers, IP addresse	s and Sites which will always b	e blocked
Download Policies Always Blocked Always Allowed		sites <b>x</b> *.domain.com www.domain.c https://www.	× om × lomain.com ×	
Temporary Allowed         Image: Allowed         Ima	• • •	Jsers X P Addresses X User Site I	•	Add

Screenshot 55: Configuring Always Blocked list

- 2. Select User, Site or IP and key in the value in the space provided.
- 3. Click Add.
- 4. Click Save.

#### NOTE

- » When keying in a **User**, specify the username in the format domain\user.
- When keying in a Client IP, you can use IP ranges (for example, "10.0.0.10-12" includes these IP addresses: "10.0.0.10", "10.0.0.11" and "10.0.0.12").

### 🚹 NOTE

When keying in a URL for a website you can use the wildcard character [\*], for example:

Type \*.com to allow or block all '.com' top-level domains

Type \*.website.com to allow or block all sub-domains of 'website.com'

### 7.2.4 Deleting Items From the Always Blocked list

To delete an item from the Always Blocked list:

- 1. Go to Settings > Policies > Always Blocked.
- 2. Click the **Delete** icon next to the item to delete.
- 3. Click Save.

#### 7.2.5 Configuring Always Allowed List

The Always Allowed list is a list of sites, users and IP addresses that are automatically excluded from all filtering policies configured in GFI WebMonitor. Besides the Always Allowed list, there is also a **Temporary Allowed** list that is used to temporarily approve access to a site for a user or IP address.

### IMPORTANT

In GFI WebMonitor, the **Temporary Allowed** list takes priority over the **Always Allowed** list. Furthermore, both **Always Allowed** lists take priority over the **Always Blocked** list. Therefore, if a site is listed in the **Always Allowed** or **Temporary Allowed** lists and that same site is listed in the **Always Blocked** list, access to the site is allowed.

#### Pre-configured Items

By default, GFI WebMonitor includes a number of pre-configured sites in the Always Allowed list. These include GFI Software Ltd websites to allow automatic updates to GFI WebMonitor and Microsoft<sup>®</sup> websites to allow automatic updates to Windows<sup>®</sup>. Removing any of these sites may stop important updates from being automatically effected.

😡 Always Allowed
The Users, IP addresses and Sites which will bypass all web filter policies
▼ Sites ×
*.microsoft.com ×
*.sunbeltsoftware.com ×
*.windowsupdate.com ×
*.adobe.com ×
*.macromedia.com ×
*.sun.com ×
*.teamviewer.com ×
*.dyngate.com ×
*.hound-dog.co.uk ×
*.hound-dog.us ×
*.hound-dog.ie ×
*.hound-dog.fr ×
*.hound-dog.com.au ×
*.systemmonitor.co.uk ×
*.systemmonitor.us 🗙
*.systemmonitor.eu.com ×
*.system-monitor.com ×
*.mav.system-monitor.com 🛛 🕷
Grant To: User Site IP Add ?

Screenshot 56: Adding items to Always Allowed list

To add an item to the Always Allowed list:

- 1. Go to Settings > Policies > Always Allowed.
- 2. In the Grant To field, select User, Site or IP and key in the value in the space provided.
- 3. Click Add.
- 4. Click Save.



# 🚹 NOTE

When keying in a URL for a website you can use the wildcard character [\*], for example:

Type \*.com to allow or block all '.com' top-level domains

Type \*.website.com to allow or block all sub-domains of 'website.com'

### Deleting Items From the Always Allowed List

To delete an item from the Always Allowed list:

- 1. Go to Settings > Policies > Always Allowed.
- 2. Click the **Delete** icon next to the item to delete.
- 3. Click Save.
- 7.2.6 Configuring Temporary Allowed List

The **Temporary Allowed List** is a list of URL's, users or IP addresses that are allowed to bypass all web filtering polices for a specified amount of time. The list is populated either automatically with items approved from quarantine or manually by adding specific entries.

To manually configure temporary access to sites, users or IP addresses:

#### 1. Go to Settings > Policies > Temporary Allowed List.

Save <u>Cancel Changes</u>
Whitelisted Users, IP addresses and Sites which will bypass all web filter policies
V Users X
John Smith   www.youtube.com   🕒 12/31/2011 1:00 AM 🗙
Grant To: User IP
Access To:
Active until: 12/31/2011 1:00 AI III
Add
Save Cancel Changes

Screenshot 57: Configuring Temporary Allowed list

2. In the **Grant To** field, select **User** or **IP** and key in the user or **IP** address to grant access to in the space provided.

- 3. In the Access To field, type the URL of the website to grant access to.
- 4. In the Active until area, select the date and time during which the policy will be active.
- 5. Click Save.

### Deleting Items From the Temporary Allowed list

To delete an item from the Temporary Allowed list:

- 1. Go to Settings > Policies > Temporary Allowed.
- 2. Click the **Delete** icon next to the item to delete.

#### 3. Click Save.

#### 7.2.7 WebSecurity Edition Policies

WebSecurity edition includes download control, virus scanning through multiple anti-virus engines and anti-phishing as well as control for most IM clients.

The following sections help you:

- » Configure Security Policies
- » Configure Download Policies
- » Configure Security Engines

### Enabling or Disabling a Configured Policy

To enable or disable a policy:

- 1. Go to Settings > Policies > Security Policies.
- 2. Click **ON** to enable or **OFF** to disable the desired policy.

#### **Deleting a Policy**

To delete a policy click the **Delete** icon next to the policy to delete.

#### 7.2.8 Configuring Security Policies

A default security policy is enabled when GFI WebMonitor is installed. It is pre-configured to apply to every user on the domain and to allow web browsing of all categories. This policy is called **Default Virus Scanning Policy**, and can be edited, but not disabled or deleted.

#### NOTE

Certain fields in the default policy cannot be edited. These include **Policy Name** and **Apply Policy To**.

### IMPORTANT

All added policies take priority over the default policy.

To edit the Default Virus Scanning Policy:

- 1. Go to Settings > Policies > Security Policies.
- 2. Under Configured Virus Scanning Policy, click Default Virus Scanning Policy.



Screenshot 58: Configuring Default Virus Scanning Policy

3. In the **Policy Name** field enter a name for the new policy. This field is not available when editing the **Default Virus Scanning Policy**.

4. In the Scan area, select the action to perform for the required Content Types:

Fable 31: Scanning options		
OPTION	DESCRIPTION	
1	<b>Scan</b> - select to enable scanning of web traffic related to a content type. If disabled, web requests are allowed without being scanned by the configured anti virus engines.	
	Show download progress window - When enabled, a progress window is displayed during downloads.	
0	Block - select to block the content type completely.	
<u> </u>	Warn and allow - when selected, users receive a warning that their web request or download is against com- pany policy, but their action is still allowed.	

OPTION	DESCRIPTION
<b>e</b>	<b>Quarantine</b> - the requested web page or download is sent to a quarantine area within GFI WebMonitor, from where the Systems Administrator can then approve or decline the request. For more information, refer to Using Quarantine (page 58).

- 5. [Optional] To define custom content types, click Show Custom Content Types, then:
  - a. Click Add Content Type.

New Content typ	e
Content type:	image/gif
Description:	*.gif
Scan:	ON OFF 🔇 💞 📉
Virus action:	Block Warn Quarantine
Progress Window:	ON OFF
	OK Cancel

b. In the **Content Type** field, enter the string for the file type to add.



- c. In the Description field, enter a description.
- d. Define the actions to take when the content type is downloaded.
- e. Click **OK**.

6. Select the virus scanning engines to use by switching the available engines **On** or **Off** as required.

7. In the **Apply Policy To** field, specify **Users, Groups** or **IPs** for whom the new policy applies, and click **Apply To**. This field is not available when editing the **Default Virus Scanning Policy**.

8. [Optional] In the **Notify Breacher** area, click **ON** to enable notifications. You can also edit the notification message in the **Message to Policy Breacher** window.

9. [Optional] In the **Notify Administrators** area, click **ON** to enable notifications. Specify an email address in the available box and click **Add**. You can also edit the notification message in the **Message to Policy Breacher** window.

10. Click Save.

### IMPORTANT

You can add as many policies as required, however the top most policy has precedence over the ones below it.

### IMPORTANT

Click Save before you navigate away from page.

See also:

**Cloning a Policy** 

Adding a New Security Policy

7.2.9 Adding a New Security Policy

To add a new Security Policy:

- 1. Go to Settings > Policies > Security Policies.
- 2. Click Add Policy.



Screenshot 59: Creating a new Security Policy

3. In the **Policy Name** field enter a name for the new policy. This field is not available when editing the **Default Virus Scanning Policy**.

4. In the Scan area, select the action to perform for the required Content Types:

Table 32: Scanning options

OPTION	DESCRIPTION
1	Scan - select to enable scanning of web traffic related to a content type. If disabled, web requests are allowed without being scanned by the configured anti virus engines.
	Show download progress window - When enabled, a progress window is displayed during downloads.
<b>e</b>	Block - select to block the content type completely.

OPTION	DESCRIPTION
<u> </u>	Warn and allow - when selected, users receive a warning that their web request or download is against company policy, but their action is still allowed.
↔	<b>Quarantine</b> - the requested web page or download is sent to a quarantine area within GFI WebMonitor, from where the Systems Administrator can then approve or decline the request. For more information, refer to Using Quarantine (page 58).

- 5. [Optional] To define custom content types, click Show Custom Content Types, then:
  - a. Click Add Content Type.

New Content type			
Content type:	image/gif		
Description:	*.gif		
Scan:	ON OFF 🍪 💞 K		
Virus action:	Block Warn Quarantine		
Progress Window:	ON OFF		
	OK Cancel		

b. In the **Content Type** field, enter the string for the file type to add.



- c. In the Description field, enter a description.
- d. Define the actions to take when the content type is downloaded.
- e. Click OK.

6. Select the virus scanning engines to use by switching the available engines On or Off as required.

7. In the **Apply Policy To** field, specify **Users, Groups** or **IPs** for whom the new policy applies, and click **Apply To**. This field is not available when editing the **Default Virus Scanning Policy**.

8. [Optional] In the **Notify Breacher** area, click **ON** to enable notifications. You can also edit the notification message in the **Message to Policy Breacher** window.

9. [Optional] In the **Notify Administrators** area, click **ON** to enable notifications. Specify an email address in the available box and click **Add**. You can also edit the notification message in the **Message to Policy Breacher** window.

10. Click Save.

### IMPORTANT

You can add as many policies as required, however the top most policy has precedence over the ones below it.

### IMPORTANT

Click Save before you navigate away from page.

#### See also:

#### **Cloning a Policy**

#### 7.2.10 Configuring Security Engines

By default, all the Security Engines in GFI WebMonitor are enabled.

To turn off a security engine:

1. Go to Settings > Security Policies.

G	<b>GFI Web</b> Monitor					
Di	ashboard	Reports	Settings	Help		
ŵ	General	*	Security F	Policies 🕜		
٨	Policies		~			
	Internet Policies		Configured Virus Sc	anning Policies		
	Security Policies	<u>مر</u>	1    Bloc	king Policy	ON OFF	John Smith
	Always Blocked		2 Defa	ault Virus Scanning Policy	ON OFF	Applies to everyone (cannot be removed)
	Always Allowed					
	Temporary Allow	ved	Add Policy			
9	Alerts	*	Security Engines			
<b>e</b>	Proxy Settings	*	(L)	BitDefender	ON OFF	Applies to everyone
			P	VIPRE	ON OFF	Applies to everyone
			K	Kaspersky	ON OFF	Applies to everyone
			=	Anti-Phishing	ON OFF	Applies to everyone
			G	ThreatTrack	ON OFF	Applies to everyone

Screenshot 60: Configuring Security Engines

2. In the Security Engines area, click OFF next to the engine you want to disable.

To perform additional configuration refer to the following sections:

- » Configuring Kaspersky
- » Configuring Anti Phishing
- » Configuring ThreatTrack

#### 7.2.11 Configuring Kaspersky

The **Kaspersky** anti-virus scanning engine enables you to state whether the actions specified in the **Virus Scanning Policies** should also be used when files are identified as:

Table 33: Kaspersky engine options			
OPTION	DESCRIPTION		
Suspicious	Files identified as suspicious.		
Corrupted	Files that cannot be scanned since the file format is corrupted, for example, corrupted CAB files.		
Hidden	Files that cannot be scanned since the contents are protected, for example, password protected ZIP files.		

To configure Kaspersky:

- 1. Go to Settings > Policies > Security Policies.
- 2. Click Kaspersky.

Save <u>Cancel Changes</u>		
Trigger configured action a	also for files identifie	d as:
Suspicious	ON OFF	
Corrupted	ON OFF	Files that cannot be scanned since the file format is corrupted, for example, corrupted CAB files.
Hidden	ON OFF	Files that cannot be scanned since the contents are protected, for example, password protected ZIP files.
Save <u>Cancel Changes</u>		

Screenshot 61: Configuring Kaspersky security engine

- 3. Next to **Suspicious**, click **ON** to enable scanning of files considered to be suspicious.
- 4. Next to Corrupted, click ON to enable scanning of corrupted files.
- 5. Next to Hidden, click ON to enable scanning of protected files.
- 6. Click Save.

#### 7.2.12 Configuring Anti Phishing Notifications

You can set up notifications that inform users whenever GFI WebMonitor protects them from known phishing sites.

To configure notifications:

- 1. Go to Settings > Policies > Security Policies.
- 2. Click Anti-Phishing.

3. Next to **Notify Breacher**, click **ON** to enable notifications to be sent to the person attempting to access a known phishing site.

4. Next to **Notify Administrators**, click **ON** to enable notifications, then specify the email addresses of the persons who need to be notified.

5. Click Save.

### 7.2.13 Configuring ThreatTrack

The ThreatTrack protection feature ensures that the latest malware and phishing threats are blocked even when originating from compromised legitimate sites. If enabled, GFI WebMonitor automatically blocks sites confirmed to be distributing malicious content or used for phishing purposes.

To configure ThreatTrack:

- 1. Go to Settings > Policies > Security Policies.
- 2. Click ThreatTrack.

Security Policies > Threat Track Details		
Save <u>Cancel Changes</u>		
Notify Breacher: ON OFF Note: The notification can only be sent if the policy breacher is authenticated or the IP is mapped.		
Message to Policy Breacher:		
Notify Administrators:     ON   OFF   johnsmith@domain.com     Add   Specify email address of who needs to be notified   Message to Administrators:   GFI WebMonitor blocked access to a known ThreatTrack site.		
Save <u>Cancel Changes</u>		

Screenshot 62: Configuring ThreatTrack notifications

3. Next to **Notify Breacher**, click **ON** to enable notifications to be sent to the person attempting to access a known ThreatTrack site.

4. Next to **Notify Administrators**, click **ON** to enable notifications, then specify the email addresses of the persons who need to be notified.

5. Click Save.

#### 7.2.14 Configuring Download Policies

**Download Policies** enable you to manage file downloads based on file types. If a user tries to download a file that triggers a Download Policy, GFI WebMonitor determines what action to take, according to what you configured in that policy. This may be one of the following actions:

- » Allow file download
- » Quarantine downloaded file
- » Block file from being downloaded

A Default Download Policy is enabled when GFI WebMonitor is installed. It is pre-configured to apply to everyone and to allow downloads of all file types. The default download policy can be edited, but cannot be disabled or deleted.

# 🚺 ΝΟΤΕ

Certain fields in the default policy cannot be edited. These include **Policy Name** and **Apply Policy To**.

## IMPORTANT

All added policies take priority over the default policy.

## 🚹 NOTE

It is recommended that only one Download Policy is applied to a user, a group or IP address. In cases where more than one Download Policy is applied to the same user, group or IP, the top most policy takes priority over subsequent policies.

### Enabling or Disabling a Download Policy

To enable or disable a Download Policy:

- 1. Go to Settings > Policies > Download Policies.
- 2. Click ON to enable or OFF to disable the policy.

#### Deleting a Download Control Policy

To delete a Download Control Policy click the **Delete** icon next to the policy to delete.

See also:

<u>Cloning a Policy</u> <u>Adding a New Download Policy</u> Editing an Existing Download Policy

#### Adding a New Download Policy

To add a Download Policy:

1. Go to Settings > Policies > Download Policies.

Save <u>Cancel Changes</u>		
Policy Name: Block exe files		
	Ø 🖨 😵	
Filter:      Application Type	Ø 🗢 😔 🛔	🕢 🕢 Allow
Executable	Ø 🖨 😣	😑 Block
Ms-package .msi	🧭 🖨 😔	🚱 Quarantine
Archive	🧭 🖨 😔	
Zip	🤣 🖨 😔	
RAR archive	🧭 🖨 😔	
Java package .jar	S	
Cab archives .cab	🥝 🖨 🗧 🔻	,
Show Custom Content types		
Apply Policy to: John Smith × User Group IP	Apply To	0
Notify Breacher: ON OFF Note: The notification of authenticated or the IP	can only be sent if the is mapped.	e policy breacher is
Message to Policy Breacher:		
Your download has been blocked. The conten control policy.	nt breaches a GFI WebM	lonitor download
Notify Administrators: ON OFF		



- 2. Click Add Policy.
- 3. In the **Policy Name** field, key in a Policy Name.
- 4. From the **Filter** area, select action to be taken for file types. Available options are:

OPTION	DESCRIPTION
<b></b>	Allow - select to allow downloads for content type.
0	Block - select to block the content type completely.
<b>↔</b>	<b>Quarantine</b> - the requested download is sent to a quarantine area within GFI WebMonitor, from where the Systems Administrator can then approve or decline the request. For more information, refer to <u>Using Quarantine</u> (page 58).

## 🚹 NOTE

These settings can also be configured by clicking on a file type and selecting the desired **Action**. A description about each file type is also provided.

5. [Optional] To add custom file types not present in the pre-defined list, click **Show Custom Content Types**, then click **Add Content-type**to add new file types.

6. In the **Apply Policy To** field, specify **Users, Groups** or **IPs**for whom the new policy applies, and click**Add**.

# 🚺 ΝΟΤΕ

- » When keying in a **User**, specify the username in the format domain\user.
- When keying in a Client IP, you can use IP ranges (for example, "10.0.0.10-12" includes these IP addresses: "10.0.0.10", "10.0.0.11" and "10.0.0.12").

7. [Optional] In the **Notify Breacher** area, click **ON** to enable notifications to send when a user infringes this policy. Provide the body text of the notification email in the available space.

8. [Optional] To send a notification to administrators when the downloaded content infringes this policy, click **ON** in the **Notify Administrators** area. Add the administrator's email address and provide the body text of the notification email in the available space.

9. Click Save.

See also:

<u>Cloning a Policy</u> Configuring Download Policies

Editing an Existing Download Policy

### Editing an Existing Download Policy

To edit a Download Control Policy:

#### 1. Go to Settings > Policies > Download Policies.

- 2. Click the policy name to edit.
- 3. Change the required settings.
- 4. Click Save.

See also:

**Cloning a Policy** 

Configuring Download Policies

Adding a New Download Policy

### Cloning a Policy

Existing WebFiltering and WebSecurity policies can be cloned to quickly create new polices which can then be edited as required.

To clone a policy:

- 1. Go to Settings > Policies
- 2. Select Security Polices, Internet Policies or Download Policies.
- 3. Click the policy name you want to edit.
- 4. Click Clone Policy.

# 🚺 NOTE

Default policies cannot be cloned.

# 7.3 Configuring Alerts

GFI WebMonitor lets you configure alerts based on specific usage patterns, such as warnings bypassed or sites that have been blocked by configured policies. The following sections will help you configure the following:

- » Configuring Monitoring Alerts
- » Configuring Bandwidth Alerts
- » Configuring Security Alerts

#### 7.3.1 Configuring Monitoring Alerts

Monitoring Alerts can be set up to send notifications when specific policies are triggered off. For example, if you have configured an Internet browsing policy that allows browsing Social Networks for X hours, you may want to notify the user or management when this threshold is exceeded.

To configure monitoring alerts:

- 1. Go to Settings > Alerts > Monitoring Alerts.
- 2. Click Add Alert.

Save <u>Cancel Changes</u>	
Alert Name:	Monitoring
Trigger base on:	Sites Accessed Blocks Warnings Bypassed (1
Threshold:	10 1
Time interval:	Hour 👻 🚺
Apply to:	Social Network
Notify:	admninstrator@mydomain.com
Notify user:	Specify UserName, Group or email address of who needs to be notified           ON         OFF           Note: The notification can only be sent if the person that triggered the alert is authenticated or the IP is mapped
	Message to user:
Save <u>Cancel Changes</u>	

Screenshot 64: Configuring Monitoring alerts

- 3. In the Alert Name filed, key in a name.
- 4. In the **Trigger base on** area, select a one of the following options:
- » Sites Accessed the alert will be triggered if the total number of specified sites is exceeded
- » Blocks selected users will be notified when the specified number of Blocks is exceeded
- Warnings Bypassed selected users will be notified when the specified number of bypassed warnings is exceeded
- 5. In the **Threshold** area, specify a number that will trigger the alert if exceeded.

6. Specify the frequency that GFI WebMonitor checks against the specified threshold. Time intervals can be set to:

- » Hour
- » Day
- » Week

- 7. In the Apply to field, select a category from the available list and click Add.
- 8. In the Notify field, specify users or groups who need to be notified, then click Add.
- 9. In the Notify user field, Click ON and type the alert message in the Message to user field.

10. Click Save.

### 7.3.2 Configuring Bandwidth Alerts

To configure bandwidth alerts:

- 1. Go to Settings > Alerts > Bandwidth Alerts.
- 2. Click Add Alert.

Save <u>Cancel Changes</u>	Clone Alert
Alert Name:	Social Networking Alert
Trigger base on:	Total Bandwidth Downloads Uploads (
Threshold:	5 MB Per User I
Time interval:	Hour 💌 🚺
Filter on:	No Filter Categories Content type
Apply to:	Social Network 🗙
	Malware Sites  Add
Notify:	Administrator@mydomain.com
	Specify UserName, Group or email address of who needs to be notified
Notify user:	ON OFF Note: The notification can only be sent if the person that triggered the alert is authenticated or the IP is mapped
	Message to user:
	Threshold has been exceeded.
Save <u>Cancel Changes</u>	

Screenshot 65: Configuring Bandwidth alerts

- 3. In the Alert Name field, key in a name.
- 4. In the **Trigger base on** area, select a one of the following options:
Table 35: Bandwidth alert trigger options

TRIGGER	DESCRIPTION
Total Bandwidth	Alert will be triggered if the total specified bandwidth is exceeded.
Downloads	Selected users will be notified when the specified download limit is exceeded.
Uploads	Selected users will be notified when the specified upload limit is exceeded.

5. In the **Threshold** area, specify the size of data in MB or GB that triggers the alert. Specify if this amount is applicable per user or for all users on domain.

6. Specify the frequency that GFI WebMonitor checks against the specified threshold. Time intervals can be set to:

- » Hour
- » Day
- » Week

7. In the **Filter on** options, select the type of filtering to use. These can be:

Table 36: Bandwidth alerts filtering options		
DESCRIPTION		
Select this option to make the alert available on all type of traffic.		
Select desired categories from a predefined list and click Add.		
Select desired content types from a predefined list and click Add.		

8. In the Notify field, specify the users or groups to notify and click Add.

9. In the Notify user field, click ON and type the alert message in the Message to user field.

10. Click Save.

#### 7.3.3 Configuring Security Alerts

To configure security alerts:

- 1. Go to Settings > Alerts > Security Alerts.
- 2. Click Add Alert.

Security Alerts > Malicious conte	ent alert
Save <u>Cancel Changes</u>	Clone Alert
Alert Name:	Malicious content alert
Trigger for:	Anti-Virus ON OFF
	Anti-Phishing ON OFF
	ThreatTrack ON OFF
Threshold:	5 🕜
Time interval:	Hour 💌 😮
Notify:	Nobody Add
	Specify email address of who needs to be notified
Notify user:	ON OFF Note: The notification can only be sent if the person that triggered the alert is authenticated or the IP is mapped
Save <u>Cancel Changes</u>	i

Screenshot 66: Configuring Security alerts

#### 3. In the Alert Name filed, key in a name.

## 4. In the **Trigger for** area, select any of the following options:

Table	37:	Security	alerts	trigger	options
Tuble	57.	Jecunty	alcris	crigger	options

TRIGGER	DESCRIPTION
Anti-Virus	Alert will be triggered when the number of blocks made by the Anti-virus engine exceeds the threshold specified in the next step.
Anti-Phishing	Alert will be triggered when the number of blocks made by the Anti-phishing engine exceeds the threshold specified in the next step.
ThreatTrack	Alert will be triggered when the number of blocks made by the ThreatTrack engine exceeds the threshold specified in the next step.

5. In the **Threshold** area, specify the total hits that will trigger the alert when exceeded. This setting will apply for the selected security engines.

6. Specify the frequency that GFI WebMonitor checks against the specified threshold. Time intervals can be set to:

- » Hour
- » Day
- » Week

7. In the Notify field, specify users or groups who need to be notified, then click Add.

8. In the Notify user field, Click ON and type the alert message in the Message to user field.

9. Click Save.

# 8 Troubleshooting and support

# 8.1 Introduction

This chapter explains how to resolve any issues encountered during installation of GFI WebMonitor. The main sources of information available to solve these issues are:

- » This manual most issues can be solved through the information in this section.
- » GFI Knowledge Base articles
- » Web forum
- » Contacting GFI Technical Support

# 8.2 GFI SkyNet

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

# 8.3 Web Forum

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

# 8.4 Request Technical Support

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

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

# 🚹 NOTE

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

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

# 8.5 Documentation

If this manual does not satisfy your expectations, or if you think that this documentation can be improved in any way, let us know via email on: <u>documentation@gfi.com</u>.

# 8.6 Common Issues

Table 38: Common troubleshooting issues

ISSUE ENCOUNTERED	SOLUTION
WebFilter module fails to register cor- rectly on all members of the array when GFI WebMonitor is installed on Microsoft <sup>®</sup> TMG (where Microsoft <sup>®</sup> TMG is in array of other Microsoft <sup>®</sup> TMG Severs)	The GFI WebMonitor DLL does not get registered and needs to be registered manually. Run the command regsrv32 webmonplg.dll from the folder that contains the <b>webmonplg.dll</b> . This is typically located in the Microsoft <sup>®</sup> ISA or Microsoft <sup>®</sup> TMG folder on each server where GFI WebMonitor is installed.
Users are not able to browse and/or download from the Internet after install- ing GFI WebMonitor in Gateway or in Sim- ple Proxy mode.	After the installation, GFI WebMonitor proxy machine has to be configured to listen for incoming user requests. Next, Internet browsers on client machines have to be configured to use the GFI WebMonitor proxy machine as the default proxy. For more information, refer to Post Installation Actions (page 22). In the event that the users are still not able to browse and/or download from the Internet, add an exception rule in the firewall on the GFI WebMonitor proxy machine to allow incoming TCP traffic on port 8080. For more information on how to enable firewall ports on Windows <sup>®</sup> Firewall, refer to <u>http://go.gfi.com/?pageid=WebMon_WIndowsFirewall</u>
Client browsers are still retrieving old proxy Internet settings although the browsers are configured to automatically detect settings.	Internet explorer may not refresh cached Internet settings so client browsers will retrieve old Internet settings. Refreshing settings is a manual process on each client browser. For more information, refer to the <b>Refresh cached Internet Explorer</b> <b>settings</b> section within the <b>Miscellaneous</b> chapter in GFI WebMonitor <b>Getting Started Guide</b> . Or visit: <u>http://go.gfi.com/?pageid=WebMon_AutomaticDetection</u>
Users are still required to authenticate themselves manually when browsing, even when Integrated authentication is used.	Integrated authentication will fail when GFI WebMonitor is installed on a Windows <sup>®</sup> XP Pro machine that has never been joined to a Domain Controller and where the Network access setting is set to <b>Guest only - local users authenticate as Guest</b> .

ISSUE ENCOUNTERED	SOLUTION
Users using Mozilla Firefox browsers are repeatedly asked to key in credentials after installing GFI WebMonitor in Gate- way or in Simple Proxy mode.	<ul> <li>The server and the client machine will use NTLMv2 for authentication when:</li> <li>GFI WebMonitor is installed on Windows<sup>®</sup> Server 2008 and LAN Manager authentication security policy is defined as Send NTLMv2 response only</li> </ul>
	and
	The client machine LAN Manager is not defined (this is the default set- ting in Windows <sup>®</sup> 7) NTLMv2 is not supported in Mozilla Firefox and the user's browser will repeatedly ask for credentials.
	To solve this issue do one of the following :
	1. Navigate to Configuration > Proxy Settings.
	2. In the Network Configuration area select the Use WPAD for network clients checkbox.
	3. Select Publish the host name of the GFI WebMonitor proxy in WPAD.
	Or change authentication mechanism on either of the following:
	On GFI WebMonitor server (Windows <sup>®</sup> Server 2008):
	1. Navigate to Start > Administrative Tools > Local Security Policy.
	2. Expand Local Policies > Security Options.
	3. Right-click <b>Network Security: LAN Manager authentication level</b> from the right panel and click Properties.
	4. Select Local Security Setting tab in the Network Security: LAN Manager authentication level Properties dialog.
	5. Select <b>Send LM &amp; NTLM - use NTLMv2 session security if negotiated</b> from the Network security drop-down list.
	6. Click Apply and OK.
	7. Close Local Security Policy dialog.
	8. Close all open windows.
	Client machines (Microsoft Windows 7) using Active Directory GPO:
	1. Navigate to Start > Control Panel > System and Security > Administrative Tools > Local Security Policy.
	2. Expand Local Policies > Security Options.
	3. Right-click Network Security: LAN Manager authentication level from the right panel and click Properties.
	4. Select Local Security Setting tab in the Network Security: LAN Manager authentication level Properties dialog.
	5. Select Send LM & NTLM - use NTLMv2 session security if negotiated from the Network security drop-down list.
	6. Click Apply and OK.
	7. Close Local Security Policy dialog.
	8. Close all open windows.
	For more information visit: http://go.gfi.com/?pageid=WebMon_FirefoxIssues

# 9 Glossary

# Α

#### **Access Control**

"A feature that allows or denies users access to resources, for example, Internet access."

#### Active Directory

"A technology that provides a variety of network services, including LDAP-like directory services."

## AD

See Active Directory

#### Administrator

The person responsible for installing and configuring GFI WebMonitor.

## **Always Allowed List**

A list that contains information about what should be allowed by GFI WebMonitor.

#### **Always Blocked List**

A list that contains information about what should be blocked by GFI WebMonitor.

## Anti-virus

Software that detects viruses on a computer.

# В

#### Bandwidth

The maximum amount of data transferred over a medium. Typically measured in bits per second.

# С

# Cache

A location where GFI WebMonitor temporarily keeps downloaded files. This will speed up subsequent requests for the same file as GFI WebMonitor would serve the file directly from the cache instead of downloading it again.

## CER

See CER file format

#### CER file format

A certificate file format that contains the certificate data but not the private key.

# Certificate Revocation List

A list issued by a Certification Authority listing HTTPS websites certificates that were revoked.

#### **Chained Proxy**

When client machines connect to more than one proxy server before accessing the requested destination.

#### Console

An interface that provides administration tools that enable the monitoring and management of Internet traffic.

#### CRL

See Certificate Revocation List

# D

## Dashboard

Enables the user to obtain graphical and statistical information related to GFI WebMonitor operations.

## Ε

## **Expired Certificate**

An expired certificate has an end date that is earlier than the date when the certificate is validated by GFI WebMonitor.

## F

# File Transfer Protocol

A protocol used to transfer files between computers.

# FTP

See File Transfer Protocol.

# G

#### Google Chrome

A web browser developed and distributed by Google.

#### GPO

See Group Policy Objects.

#### **Group Policy Objects**

An Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.

### Η

# Hidden Downloads

"Unwanted downloads from hidden applications (for example, trojans) or forgotten downloads initiated by users."

# HTTP

See Hypertext Transfer Protocol.

## HTTPS

See Hypertext Transfer Protocol over Secure Socket Layer (SSL).

## HyperText Transfer Protocol

A protocol used to transfer hypertext data between servers and Internet browsers.

#### HyperText Transfer Protocol over Secure Socket Layer (SSL)

A protocol used to securely transfer encrypted hypertext data between servers and Internet browsers. The URL of a secure connection (SSL connection) starts with https: instead of http:.

I

#### **Internet Browser**

An application installed on a client machine that is used to access the Internet.

#### Internet Gateway

"A computer that has both an internal and an external network card. Internet sharing is enabled, and client machines on the internal network use this computer to access the Internet."

### L

#### LAN

See Local Area Network.

#### LDAP

See Lightweight Directory Access Protocol.

#### Lightweight Directory Access Protocol

A set of open protocols for accessing directory information such as email addresses and public keys.

#### Local Area Network

An internal network that connects machines in a small area.

#### Μ

# Malware

Short for malicious software.Unwanted software designed to infect a computer such as a virus or a trojan.

#### Microsoft Forefront Threat Management Gateway

A Microsoft product that provides firewall and web proxy services. It also enables administrators to manage Internet access through policies. It is the successor of the Microsoft ISA Server and is part of the Microsoft Forefront line of business security software.

#### Microsoft Forefront TMG

See Microsoft Forefront Threat Management Gateway

#### Microsoft Internet Explorer

A web browser developed and distributed by Microsoft Corporation.

#### Microsoft Internet Security and Acceleration Server

A Microsoft product that provides firewall and web proxy services. It also enables administrators to manage Internet access through policies.

#### **Microsoft ISA Server**

See Microsoft Internet Security and Acceleration Server.

#### **Microsoft SQL Server**

A Microsoft database management system used by GFI WebMonitor to store and retrieve data.

#### **Microsoft Windows Live Messenger**

An instant messaging application developed by Microsoft used by users to communicate on the Internet.

#### Mozilla Firefox

Mozilla Firefox is an open source Internet browser.

### MSN

See Microsoft Windows Live Messenger

#### Ν

#### Non-validated Certificate

An non-validated certificate has a start date that falls after the date when the certificate is validated by GFI WebMonitor.

#### NT LAN Manager

A Microsoft network authentication protocol.

#### NTLM

See NT LAN Manager.

#### Ρ

#### Personal Information Exchange file format

A certificate file format that contains the certificate data and its public and private keys.

## PFX

See Personal Information Exchange file format.

#### Phishing

The act of collecting personal data such as credit card and bank account numbers by sending fake emails which then direct users to sites asking for such information.

#### **Port Blocking**

The act of blocking or allowing traffic over specific ports through a router.

## **Proxy Server**

A server or software application that receives requests from client machines and responds according to filtering policies configured in GFI WebMonitor.

# Q

# Quarantine

A temporary storage for unknown data that awaits approval from an administrator.

# R

# **Revoked Certificate**

"A revoked certificate is a valid certificate that has been withdrawn before its expiry date (for example, superseded by a newer certificate or lost/exposed private key)."

# S

# Spyware

Unwanted software that publishes private information to an external source.

# Т

# Traffic Forwarding

The act of forwarding internal/external network traffic to a specific server through a router.

# U

# **Uniform Resource Locator**

The address of a web page on the world wide web. It contains information about the location and the protocol.

URL

See Uniform Resource Locator.

#### **User Agent**

A client application that connects to the Internet and performs automatic actions.

۷

# Virus

Unwanted software that infects a computer.

#### W

## WAN

See Wide Area Network.

# Web Proxy AutoDiscovery protocol

An Internet protocol used by browsers to automatically retrieve proxy settings from a WPAD data file.

# Web traffic

The data sent and received by clients over the network to websites.

## WebFilter Edition

A configurable database that allows site access according to specified site categories per user/group/IP address and time.

# WebGrade Database

"A database in GFI WebMonitor, used to categorize sites."

## WebSecurity Edition

WebSecurity contains multiple anti-virus engines to scan web traffic accessed and downloaded by the clients.

#### Wide Area Network

An external network that connects machines in large areas.

#### WPAD

See Web Proxy AutoDiscovery protocol.

# 10 Appendix 1

This section contains the following topics:

- » Assigning Log On As A Service Rights
- » Configuring Routing and Remote Access
- » Disabling Internet Connection Settings On Client Machines

# 10.1 Assigning Log On As A Service Rights

Logon rights control who is authorized to log on to a computer and how they can log on. Log on as a service rights allow a security principal to log on as a service. Services can be configured to run under the Local System, Local Service, or Network Service accounts, which have a built-in right to log on as a service. Any service that runs under a separate user account must be assigned the right.

Manually assigning Log On As A Service Rights on Windows<sup>®</sup> XP/Vista/7

- 1. Navigate to Start > Control Panel > Administrative Tools > Local Security Policy.
- 2. Expand Security Settings > Local Policies > User Rights Assignment.
- 3. Right-click Log on as a service from the right panel and click Properties.
- 4. Select the Local Security Setting tab.
- 5. Click Add User or Group.
- 6. Key in the account name and click **OK**.
- 7. Click Apply and OK.
- 8. Close Local Security Settings dialog.
- 9. Close all open windows.

Manually assigning Log On As A Service Rights on a Server Machine

1. Navigate to **Start > Programs > Administrative Tools > Local Security Policy**.

🚡 Local Security Policy			
File Action View Help			
🗢 赵 💼 🗙 🗎 🖬			
<ul> <li>Security Settings</li> <li>Account Policies</li> <li>Local Policies</li> <li>Audit Policy</li> <li>Audit Policy</li> <li>User Rights Assignment</li> <li>Security Options</li> <li>Windows Firewall with Advanced Security Network List Manager Policies</li> <li>Public Key Policies</li> <li>Software Restriction Policies</li> <li>Software Restriction Policies</li> <li>IP Security Policies on Local Compute</li> </ul>	Policy  Deny log on locally  Deny log on through Remote Desktop Services  Enable computer and user accounts to be trusted for delega  Force shutdown from a remote system  Generate security audits  Impersonate a client after authentication  Increase a process working set  Increase scheduling priority  Load and unload device drivers  Lock pages in memory  Lock pages in memory	Security Setting Guest Administrators LOCAL SERVICE,NETWO LOCAL SERVICE,NETWO Users Administrators Administrators	
Advanced Audit Policy Configuration	<ul> <li>Log on as a service</li> <li>Manage auditing and security log</li> <li>Modify an object label</li> <li>Modify firmware environment values</li> <li>Perform volume maintenance tasks</li> <li>Profile single process</li> <li>Profile system performance</li> <li>Remove computer from docking station</li> <li>Replace a process level token</li> <li>Restore files and directories</li> <li>Shut down the system</li> </ul>	Administrators Administrators Administrators Administrators Administrators Administrators,NT SERVI Administrators,Users LOCAL SERVICE,NETWO Administrators,Users,Ba	E

Screenshot 67: Microsoft Windows Server: Local Security Policy window

- 2. Expand Security Settings > Local Policies > User Rights Assignment.
- 3. Right-click Log on as a service from the right panel and click Properties.
- 4. Select the Local Security Setting tab.
- 5. Click Add User or Group button.
- 6. Key in the account name and click OK.
- 7. Click Apply and OK.
- 8. Close all open windows.

Assigning Log On As A Service Rights Using GPO in Windows<sup>®</sup> Server 2003

To assign Log on as service rights on clients' machines through Windows<sup>®</sup> Server 2003 GPO:

1. Navigate to **Start > Programs > Administrative Tools > Active Directory Users and Computers** on the DNS server.

2. Right-click the domain node and click **Properties**.

masterdomain.com Properties
General Managed By Group Policy
To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).
Current Group Policy Object Links for masterdomain
Group Policy Object Links No Override Disabled
, Group Policy Objects higher in the list have the highest priority. This list obtained from: win2k3serv.masterdomain.com
New     Add     Edit     Up       Options     Delete     Properties     Down
□ <u>B</u> lock Policy inheritance
OK Cancel Apply

Screenshot 68: Active Directory GPO dialog

- 3. Select Group Policy tab in the Domain Properties dialog.
- 4. Select **Default Domain Policy** from the list and click **Edit**

🚡 Group Policy Object Editor			
<u>File Action View H</u> elp			
🛐 Default Domain Policy [win2k3serv.masterdomain	Policy 🛆	Policy Setting	
📄 礘 Computer Configuration	BDeny log on through Terminal Services	Not Defined	
E Software Settings	Enable computer and user accounts to be tr	Not Defined	
🗄 🖳 Windows Settings	BForce shutdown from a remote system	Not Defined	
Scripts (Startup/Shutdown)	📖 Generate security audits	Not Defined	
Security Settings	Impersonate a client after authentication	Not Defined	
	Increase scheduling priority	Not Defined	
	Builtoad and unload device drivers	Not Defined	
	BLock pages in memory	Not Defined	
	🕮 Log on as a batch job	Not Defined	
The Provide State of	📆 Log on as a service	MASTERDOMAIN\Admin	
	🔀 Manage auditing and security log	Not Defined	
🕀 🧰 System Services	Bill Modify firmware environment values	Not Defined	
🕀 🧰 Registry	Berform volume maintenance tasks	Not Defined	
🕀 🚾 File System	B Profile single process	Not Defined	
∰      ₩ Wireless Network (IEEE 802.11) F	B Profile system performance	Not Defined	
😥 💼 Public Key Policies	BRemove computer from docking station	Not Defined	
🗄 📄 Software Restriction Policies	🔀 Replace a process level token	Not Defined	
🗄 🛃 IP Security Policies on Active Dire	Bestore files and directories	Not Defined	
	避 Shut down the system	Not Defined	
E Structure Configuration	B Synchronize directory service data	Not Defined	
E Software Settings	🔀 Take ownership of files or other objects	Not Defined	

Screenshot 69: GPO Editor window

5. Expand Computer Configuration > Windows Settings > Security Settings > Local Policies and click User Rights Assignment.

- 6. Right-click Log on as a service from the right panel and click Properties.
- 7. Select the Security Policy Setting tab.
- 8. Check **Define these policy settings** checkbox
- 9. Click Add User or Group button.
- 10. Key in the account name and click **OK**.
- 11. Click **Apply** and **OK**.
- 12. Close all open windows.

Assigning Log On As A Service Rights Using GPO in Windows<sup>®</sup> Server 2008

To assign Log on as service rights on clients' machines through Windows<sup>®</sup> Server 2008 GPO:

1. In the command prompt key in mmc.exe and press Enter.

2. In the **Console Root** window, navigate to **File > Add/Remove Snap-in**... to open the **Add or Remove Snap-ins** window.

iabio shaphins. Iabin	Vendor 🔺	[	Console Root	Edit Extensions
Device Manager Disk Management DNS Event Viewer Exchange Server 2007 Folder Group Policy Management Group Policy Management E Group Policy Object Editor Group Policy Starter GPO Ed Internet Information Servic	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	∖dd >	E Group Policy Management	Remove Move Up Move Down
IP Security Monitor	Microsoft 💌			Advanced

Screenshot 70: Add/Remove Snap-ins window

- 3. Select Group Policy Management from the Available snap-ins list, and click Add.
- 4. Click OK.

🚟 Console1 - [Console Root\Group Policy	Management\Forest: techcom.com\Domains\techcom.com ]
🚟 File Action View Favorites Window	Help
🗢 🔿 🙎 🖬 📋 📮 🧟 📝 🖬	
Console Root	techcom.com
🖃 🔜 Group Policy Management	Linked Group Policy Objects Group Policy Inheritance Delegation
E A Forest: techcom.com	
Domains	Link Order A GPO Enforced Link Enabled GPO
E techcom.com	🚖 1 🛒 Default Domain Policy No Yes Enab
📷 Detault Domain Policy	
E Microsoft Exchange Secu	
File osore Exchange occu     File osore Exchange occu     File Group Policy Objects	$\overline{}$
🕀 📑 WMI Filters	
🛨 🛅 Starter GPOs	

Screenshot 71: Console Root domain window

- 5. Expand Group Policy Management > Forest > Domains and <domain>.
- 6. Right-click Default Domain Policy and click Edit to open the Group Policy Management Editor.



Screenshot 72: Group Policy Management Editor window

7. Expand Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies and click User Rights Assignment.

- 8. Right-click Log on as a service from the right panel and click Properties.
- 9. Select the Security Policy Setting tab.
- 10. Check Define these policy settings checkbox
- 11. Click Add User or Group button.
- 12. Key in the account name and click **OK**.
- 13. Click Apply and OK.
- 14. Close all open windows.

# 10.2 Configuring Routing and Remote Access

When installing GFI WebMonitor in Gateway mode on a Windows<sup>®</sup> Server 2003 or Windows<sup>®</sup> Server 2008, the Routing and Remote Access must be configured to use Network Address Translation (NAT). This can be done by:

1. Navigate to Start > Programs > Administrative Tools > Routing and Remote Access.

- 2. Right-click <machine name> and select Configure and Enable Routing and Remote Access.
- 3. Click Next in the Routing and Remote Access Server Setup Wizard dialog.
- 4. Select Network address translation (NAT) and click Next.

outing and Remote Access S	erver Setup Wizard	
NAT Internet Connection You can select an existing client computers to connec	interface or create a new dema ct to the Internet.	nd-dial interface for
Use this public interface	e to connect to the Internet:	
Name	Description	IP Address
External (WAN)	Microsoft Virtual Machi	(DHCP)
Internal (LAN)	Microsoft Virtual Machi	192.168.5.100
C Create a new <u>d</u> emand-	dial interface to the Internet	
A demand-dial interface option if this server con over Ethernet. The Der	is activated when a client uses nects with a modem or by using nand-Dial Interface Wizard will (	s the Internet. Select this the Point-to-Point Protocol start at the end of this wizard.
Enable security on the Basic Firewall prevents through the Internet.	selected interface by setting up unauthorized users from gaining	Basic Firewall. glaccess to this server
For more information about r	network interfaces, see <u>Routing</u>	and Remote Access Help.
	< <u>B</u> ack	Next > Cancel

Screenshot 73: Microsoft Windows Server 2003: Routing and Remote Access Server Setup Wizard dialog

#### 5. Select Use this public interface to connect to the Internet.

- 6. Select the network card connected to the external network and click Next.
- 7. Click Finish.

To confirm that the Routing and Remote Access service is started:

1. From command prompt, key in services.msc

2. Check that the status of the Routing and Remote Access service is Started.

# 10.3 Disabling Internet Connection Settings On Client Machines

To prevent users from modifying Internet settings and thus bypassing GFI WebMonitor, the Internet **Connections** settings tab can be disabled on client machines.

Disabling Internet Connections Page Using GPO in Microsoft Windows Server 2003

Disabling Internet Connections Page Using GPO in Microsoft Windows Server 2008

# 10.3.1 Disabling Internet Connections Page Using GPO in Windows<sup>®</sup> Server 2003

To disable Connections settings on client machines through Windows<sup>®</sup> Server 2003 GPO:

1. Navigate to **Start > Programs > Administrative Tools > Active Directory Users and Computers** on the DNS server.

2. Right-click the domain node and click **Properties**.

masterdomain.com Properties	X			
General Managed By Group Policy				
To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).				
Current Group Policy Object Links for masterdomain				
Group Policy Object Links No Override Disabled	[			
Group Policy Objects higher in the list have the highest priority. This list obtained from: win2k3serv.masterdomain.com				
New     Add     Edit     Up       Options     Delete     Properties     Down				
□	_			
OK Cancel Apply				

Screenshot 74: Active Directory GPO dialog

- 3. Select Group Policy tab in the Domain Properties dialog.
- 4. Select **Default Domain Policy** from the list and click **Edit**.



Screenshot 75: GPO Editor window

5. Expand User Configuration > Administrative Templates > Windows Components > Internet Explorer and click Internet Control Panel.

6. Right-click **Disable the Connections page** from the right panel and click **Properties**.

Disable the Connections page Properties	? ×
Setting Explain	
😭 Disable the Connections page	
O Not <u>C</u> onfigured	
Enabled	
C Disabled	
Supported on: at least Internet Explorer v5.0	
Previous Setting <u>N</u> ext Setting	
OK Cancel Ap	ply

Screenshot 76: Disable the Connection page Properties dialog

7. In the **Setting** tab, select **Enabled**.

# 🚺 ΝΟΤΕ

This policy prevents users from viewing and modifying connection and proxy settings from their client machines.

- 8. Click **Apply** and **OK**.
- 9. Close all open windows.

#### 10.3.2 Disabling Internet Connections Page Using GPO in Windows® Server 2008

To disable **Connections** settings on clients' machines through Windows<sup>®</sup> Server 2008 GPO:

1. In the command prompt key in mmc.exe and press Enter.

2. In the **Console Root** window, navigate to **File > Add/Remove Snap-in**... to open the **Add or Remove Snap-ins** window.

ap-in	Vendor 🔺	[	Console Root	Edit Extensions
Device Manager Disk Management DNS Event Viewer Exchange Server 2007 Folder Group Policy Management Group Policy Management E Group Policy Object Editor Group Policy Starter GPO Ed Internet Information Servic	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	∖dd >	E Group Policy Management	Remove Move Up Move Down
IP Security Monitor	Microsoft 💌			Advanced

Screenshot 77: Add/Remove Snap-ins window

- 3. Select Group Policy Management from the Available snap-ins list, and click Add.
- 4. Click OK.

🚟 Console1 - [Console Root\Group Policy	Management\Forest: techcom.com\Domains\techcom.com ]
🚟 File Action View Favorites Window	Help
🗢 🔿 🙎 🖬 📋 📮 🧟 👔 🖬	
Console Root	techcom.com
<ul> <li>Koroup Policy Management</li> <li>A Forest: techcom.com</li> </ul>	Linked Group Policy Objects Group Policy Inheritance Delegation
🖃 🙀 Domains	Link Order 🔺 GPO Enforced Link Enabled GPO
E 📰 techcom.com	🔶 1 🛒 Default Domain Policy No Yes Enab
Detault Domain Policy	
🕀 📑 Group Policy Objects	
🕀 📑 WMI Filters 🕀 🚺 Starter GPOs	$\Xi$
	,

Screenshot 78: Console Root domain window

- 5. Expand Group Policy Management > Forest > Domains and <domain>.
- 6. Right-click Default Domain Policy and click Edit to open the Group Policy Management Editor.

🗐 Group Policy Management Editor	
File Action View Help	
(= =) ( <u>2</u> 📷 🔒 🛛 🖬 🝸	
<ul> <li>Default Domain Policy [TECHCOM02.TECHCOM.COM] Policy</li> <li>Computer Configuration</li> <li>Ver Configuration</li> <li>Policies</li> <li>Software Settings</li> <li>Administrative Templates: Policy definitions (ADMX files) re</li> <li>Control Panel</li> <li>Control Panel</li> <li>Desktop</li> <li>Network</li> <li>Shared Folders</li> <li>Start Menu and Taskbar</li> <li>System</li> <li>Windows Components</li> <li>Application Compatibility</li> <li>Attachment Manager</li> <li>AutoPlay Policies</li> <li>Backup</li> <li>Desktop Window Manager</li> <li>Digital Locker</li> <li>Import Video</li> <li>Instant Search</li> <li>Mathinistrator Approved Controls</li> <li>Application Compatibility</li> </ul>	Setting Advanced Page Security Page Disable the Advanced page Disable the Connections page Disable the Content page Disable the General page Disable the Privacy page Disable the Programs page Disable the Security page Prevent ignoring certificate errors Send internationalized domain names Use UTF-8 for mailto links
Internet Control Panel      Internet Settings	Extended & Standard
10 setting(s)	

Screenshot 79: Group Policy Management Editor window

7. Expand User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer and click Internet Control Panel.

8. Right-click **Disable the Connection** page from the right panel and click **Properties**.

Disable the Connections page Properties	? ×
Setting Explain Comment	
Disable the Connections page	
Not Configured	
C Enabled	
C Disabled	
Supported on: At least Internet Explorer 5.0	
Previous Setting Next Setting	
OK Cancel App	y

Screenshot 80: Disable the Connection page Properties dialog

# 9. In the Setting tab, select Enabled.

# 🚹 ΝΟΤΕ

This policy prevents users from viewing and modifying connection and proxy settings from their client machines.

- 10. Click **Apply** and **OK**.
- 11. Close Group Policy Management Editor dialog and save the management console created.

# 10.4 Uninstall Information

To uninstall GFI WebMonitor:

- 1. Click Start > Control Panel > Programs > Programs and Features.
- 2. Select GFI WebMonitor from the list, and click Uninstall.
- 3. When Are you sure you want to ununstall GFI WebMonitor 2012? appears, click Yes.
- 4. On completion, click Finish.

# 11 Index

# A

Active Directory GPO 114, 123, 128 Always Allowed 12, 79-80, 92 Always Blocked 11, 40, 70, 79-80, 89, 91 Anonymization 44, 51, 54, 56, 70 Anti-virus 40, 94, 101, 110

#### В

Bandwidth 10, 40-42, 44-45, 49, 57, 60, 63-64, 69-70, 73, 79-80, 82, 106, 108

## С

Cache 42, 70 Configuration 24, 30, 70, 75, 80, 100, 114, 124, 129, 132 Configuring GFI WebMonitor 70 Console 22, 124, 130 Credentials 20, 77, 114

## D

Dashboard 41-42, 44-45, 49, 51, 54, 56, 58, 79 Download Control Policy 103, 105 Download Policies 79, 94, 103, 105-106

#### F

FTP 24-25, 29, 32

## G

General Options 44, 51, 54, 56

#### Н

HTTP 25

#### I

IM Control Policy 86 Installation 13, 17, 19, 22, 27, 37, 70-71, 75, 77, 112 Integrated authentication 113 Internet Gateway 17 Internet Policies 40-42, 79-82, 85-86, 106 Instant Messaging and Social Control Policies 80, 84 Search Engine Policies 88 Streaming Media Policies 41-42, 86 Web Browsing Quota Policies 41, 43 Web Filtering Policies 81

# K

Knowledge Base 12-13, 49, 112 L License key 23, 70 Log on as a service rights 121

# Μ

Malware 40, 102 Microsoft Forefront TMG 18, 28-29, 31, 35 Microsoft ISA Server 17-18, 24-25, 29-30, 33 MSN 41-42, 84

#### Ρ

Phishing 10, 40, 44, 54, 66, 101-102, 110 Proxy Server 13, 22-23, 25-26

## R

Remote Access Control 22, 70-72 Authorization Rule 72 Windows Authentication 71, 73, 77 Reporting 16, 41-42, 60

## S

Security Policies 40, 79, 94, 97, 100-102 Security Engines 94, 100 Virus Scanning Policy 94, 98 Simple Proxy 17, 113 Snap-ins 124, 130 Spyware 12, 79

# Т

Technical Support 112 Temporary Allowed 12, 79-80, 91, 93 Troubleshooting 112

# U

Unified Protection Edition 11, 17 Uninstall Information 133

#### W

Web Categorization 40, 46, 70, 78 Web Forum 112 Web traffic 12, 18, 42, 95, 98 WebFilter Edition 10, 16, 40, 79-80, 88 WebGrade Database 12, 14 WebSecurity Edition 10, 17, 40, 79, 94 WPAD 114

## USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104 Cary, NC 27513, USA Telephone: +1 (888) 243-4329 Fax: +1 (919) 379-3402 <u>ussales@gfi.com</u>

## UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK Telephone: +44 (0) 870 770 5370 Fax: +44 (0) 870 770 5377 sales@gfi.com

# EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta Telephone: +356 2205 2000 Fax: +356 2138 2419 sales@gfi.com

# AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia Telephone: +61 8 8273 3000 Fax: +61 8 8273 3099 sales@gfiap.com

