

GFI WebMonitor 2011 for ISA/TMG

GFI WebMonitorTM

Getting Started Guide



<http://www.gfi.com>
info@gfi.com

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or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors.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. GFI WebMonitor is copyright of GFI SOFTWARE Ltd. - 1999-2011 GFI Software Ltd. All rights reserved.

Last updated: 13 September 2011
Version number: WEBMON-ISATMG-GSG-EN-2.0.1

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 1 |
| 1.1 | Who is This Manual For? | 1 |
| 1.2 | About This Manual..... | 2 |
| 1.3 | Terms Used in This Manual..... | 3 |
| 1.4 | GFI WebMonitor Editions | 3 |
| 1.5 | GFI WebMonitor Licensing..... | 3 |
| 2 | About GFI WebMonitor | 5 |
| 2.1 | How Does GFI WebMonitor Work? | 5 |
| 2.2 | GFI WebMonitor in a Microsoft ISA Server / Forefront TMG Environment .. | 7 |
| 3 | Installing GFI WebMonitor | 9 |
| 3.1 | Introduction | 9 |
| 3.2 | System Requirements | 9 |
| 3.3 | Installation | 10 |
| 4 | Launching GFI WebMonitor | 27 |
| 4.1 | Introduction | 27 |
| 4.2 | Launching GFI WebMonitor..... | 27 |
| 4.3 | Navigating the Console | 27 |
| 5 | Miscellaneous | 29 |
| 5.1 | Introduction | 29 |
| 5.2 | Entering Your License Key After Installation | 29 |
| 5.3 | Disabling Internet Connections Settings on Client Machines | 30 |
| 5.4 | Assigning Log On As A Service Rights | 37 |
| 6 | Troubleshooting | 43 |
| 6.1 | Introduction | 43 |
| 6.2 | Knowledge Base | 43 |
| 6.3 | Web Forum | 43 |
| 6.4 | Request Technical Support..... | 43 |
| 6.5 | Build Notifications..... | 43 |
| 7 | Glossary | 45 |
| | Index | 49 |

1 Introduction

GFI WebMonitor is a comprehensive monitoring solution that enables you to monitor and filter network users' web traffic (browsing and file downloads) in real-time. It also enables you to block web connections in progress as well as to 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 and best practice initiatives without alienating your network users.

1.1 Who is This Manual For?

This manual is for users who want to use GFI WebMonitor as a plug-in for Microsoft ISA Server or Microsoft Forefront TMG.

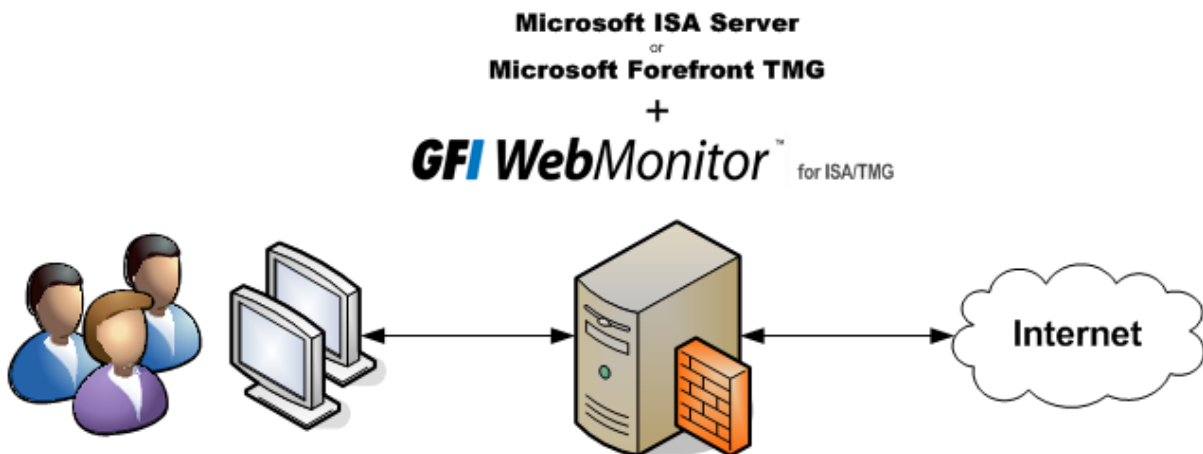


Figure 1- Environment: GFI WebMonitor as a plug-in for Microsoft ISA Server or Microsoft Forefront TMG

For environments where there is no Microsoft ISA Server or Microsoft Forefront TMG server, an independent version of GFI WebMonitor (GFI WebMonitor) is available. For more information, refer to: <http://www.gfi.com/internet-monitoring-software/webmonfeatures.htm>.

1.2 About This Manual

The aim of this manual is to help you install and run GFI WebMonitor on your network with minimum configuration 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.

This manual is structured as follows:

| CHAPTER | DESCRIPTION |
|-----------|--|
| Chapter 1 | Introduction Introduces this manual and provides information on GFI WebMonitor editions. |
| Chapter 2 | About GFI WebMonitor Provides a high-level overview of how GFI WebMonitor works and the different installation environments supported. |
| Chapter 3 | Installing GFI WebMonitor Provides information on how to install GFI WebMonitor on Microsoft ISA Server and Microsoft Forefront TMG. |
| Chapter 4 | Launching GFI WebMonitor Provides a high-level overview of the user console. |
| Chapter 5 | Miscellaneous Provides information on topics that do not strictly fall within other chapters. |
| Chapter 6 | Troubleshooting Provides all the necessary information on how to deal with any problems encountered while using GFI WebMonitor. Also provides extensive support information. |
| Chapter 7 | Glossary Defines technical terms used within GFI WebMonitor. |

1.2.1 Administration and Configuration Manual




Detailed administration and configuration guidelines are provided in the **Administration and Configuration Manual**, which is installed with the product or separately downloadable from the GFI website:

<http://www.gfi.com/products/gfi-webmonitor/manual>

The Administration and Configuration Manual complements this Getting Started Guide and provides more information on how to use and customize the features provided by GFI WebMonitor.

1.3 Terms Used in This Manual

The following terms are used in this manual:

| TERM | DESCRIPTION |
|---|--|
|  | 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. |
| <i><Italics text></i> | Parameters and values that you must replace with the applicable value, such as custom paths and filenames. |

For any technical terms and their definitions as used in this manual, refer to the [Glossary](#) chapter in this manual.

1.4 GFI WebMonitor Editions

GFI WebMonitor is available in three editions. Each edition caters for system administrators with different requirements:

- » **WebFilter Edition:** Filters web traffic and website use per user(s), group(s) and/or IP(s) and manages Internet access during specific periods, based on web categories defined within its built-in WebGrade database.
- » **WebSecurity Edition:** Provides a high degree of web security for downloaded web traffic. This is achieved through its built-in download control module and multiple anti-virus engines and anti-spyware scanning modules.
- » **Unified Protection Edition:** Provides all the features of the WebFilter Edition and the WebSecurity Edition in a single package.

1.5 GFI WebMonitor Licensing

For more information on licensing and evaluation, refer to the GFI website at:

<http://www.gfi.com/products/gfi-webmonitor/pricing/licensing>

For information on how GFI WebMonitor counts users, refer to KBBase article:

<http://kbase.gfi.com/showarticle.asp?id=KBID003528>.

2.1 How Does GFI WebMonitor Work?

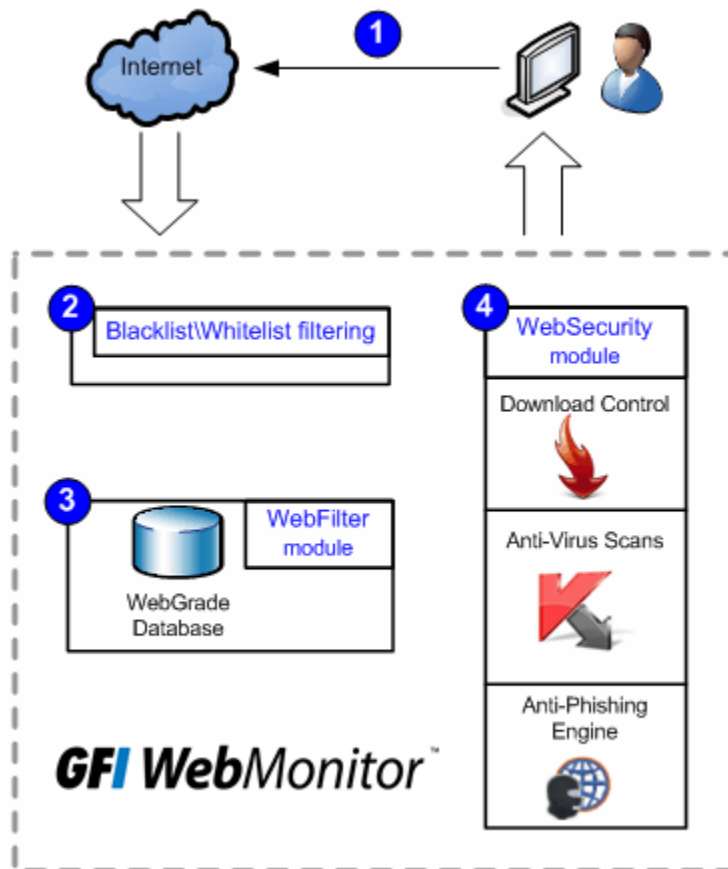


Figure 2 - How does GFI WebMonitor work?



Forwarding of incoming traffic generated by the user to GFI WebMonitor depends on the network environment; that is, where GFI WebMonitor is installed.

1 Request initiation: Users request a webpage or a download from the Internet. The incoming traffic generated by the user's request is forwarded to GFI WebMonitor.

2 Blacklist/Whitelist filtering: The internal GFI WebMonitor blacklist/whitelist filtering mechanism analyzes users' IDs and IP addresses and requested URLs. GFI WebMonitor takes the following actions regarding blacklist and whitelist web traffic:

- » Web traffic requested by blacklisted users whose IDs and/or IP addresses are blacklisted as well as requests for URLs which are blacklisted, is rejected immediately.
- » Web traffic requested by users whose IDs and/or IP addresses are whitelisted as well as requests for URLs which are whitelisted, is automatically granted access and forwarded to the user.
- » Web traffic requested by users whose IDs and/or IP addresses are neither blacklisted or whitelisted as well as requests for URLs which are neither blacklisted or whitelisted, is forwarded to the WebFilter module for processing.

3 WebFilter module: Analyzes uncategorized web traffic received from the blacklist/whitelist filtering mechanism against a list of categorized websites stored in the WebGrade database.

Web traffic is blocked, allowed or quarantined according to the configured policies. Quarantined web traffic can be manually approved or rejected by the administrators according to the user's needs and requirements, at a later stage. Approved quarantined URLs are moved in a temporary whitelist; a mechanism used to approve access to a site for a user or IP address for a temporary period.



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 whitelist/blacklist filtering mechanism to the WebSecurity module.

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

Infected material is allowed, blocked and quarantined or blocked and deleted according to the configured policies. Web traffic is also scanned for phishing material against a list of phishing sites stored in the updatable database of phishing sites. Thus, web traffic generated from a known phishing element is rejected. Finally, the approved web material is forwarded to the user.



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.



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

2.2 GFI WebMonitor in a Microsoft ISA Server / 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 a user's web traffic in real time.

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

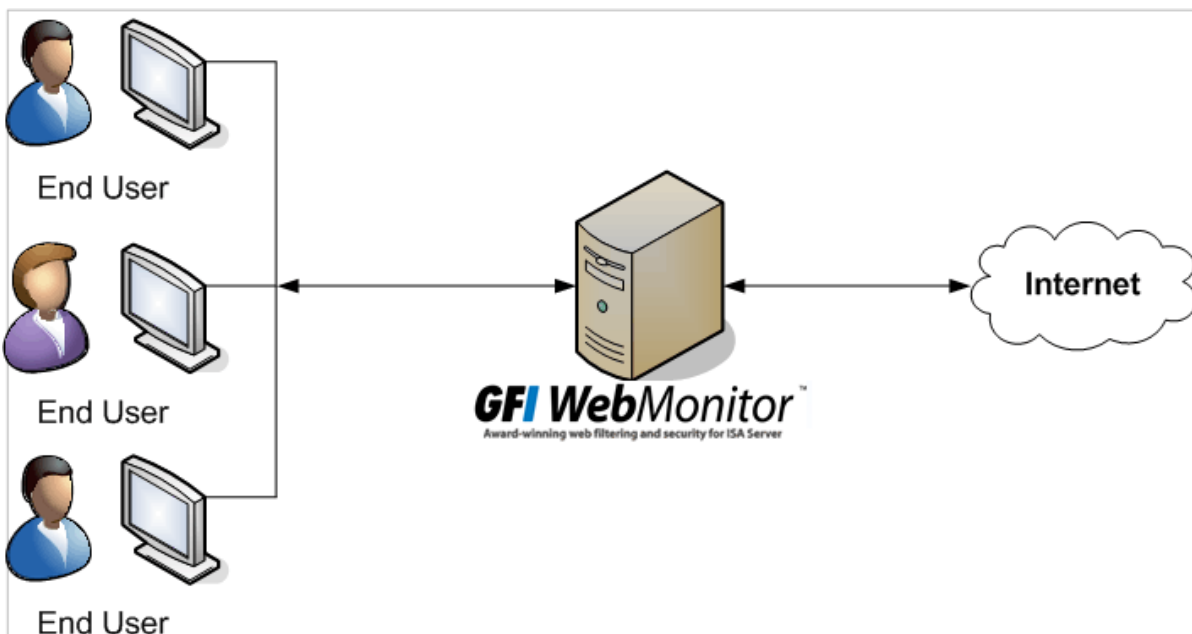


Figure 3 - GFI WebMonitor installed on Microsoft ISA Server / Forefront TMG

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

3 Installing GFI WebMonitor

3.1 Introduction

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

3.2 System Requirements

3.2.1 Software

| TYPE | SOFTWARE REQUIREMENTS |
|-----------------------------|--|
| Supported Operating Systems | <ul style="list-style-type: none">» Microsoft Windows Server 2003 (x86)» Microsoft Windows Server 2008 (x86 or x64)» Microsoft Windows Server 2008 R2 (x64) |
| Other required components | <ul style="list-style-type: none">» Microsoft ISA Server 2004 (SP3)» Microsoft ISA Server 2006» Microsoft Forefront TMG 2010 (Microsoft Windows Server 2008 R2)» Microsoft Internet Explorer 7 or later» Microsoft.NET Framework 2.0» TCP/IP port 1007» Microsoft SQL Server 2000 or later (for reporting purposes)» (Recommended) Microsoft Firewall Client for ISA Server» (Recommended) Microsoft Firewall Client for Microsoft Forefront TMG |

3.2.2 Hardware

Minimum hardware requirements depend on the GFI WebMonitor edition.

| EDITION | HARDWARE REQUIREMENTS |
|----------------------------|---|
| WebFilter Edition | <ul style="list-style-type: none">» Processor: 2.0 GHz» RAM: 1 GB (Recommended 4GB)» Hard disk: 2 GB of available disk space |
| WebSecurity Edition | <ul style="list-style-type: none">» Processor: 2.0 GHz» RAM: 1 GB (Recommended 4GB)» Hard disk: 10 GB of available disk space |
| Unified Protection Edition | <ul style="list-style-type: none">» Processor: 2.0 GHz» RAM: 2 GB (Recommended 4GB)» Hard disk: 12 GB of available disk space |



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 from 150-250GB.

3.3 Installation

3.3.1 Upgrades

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



The upgrade process is similar to the installation instructions. For more information, refer to the [Installation Procedure](#) section in this chapter.

3.3.2 Installation Procedure

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

1. Double click the GFI WebMonitor executable file.
2. If the current version of Microsoft .NET Framework is not compatible with the required version, a warning dialog will be displayed. Click **OK**. This will stop the installation process. Install the required Microsoft .NET Framework version and start the installation of GFI WebMonitor again.
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. Select **I accept the terms in the license agreement** and click **Next**.



Screenshot 1 - Installation: Access Permissions

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



More than one user or machine can be specified. Separate entries with semicolons ‘;’

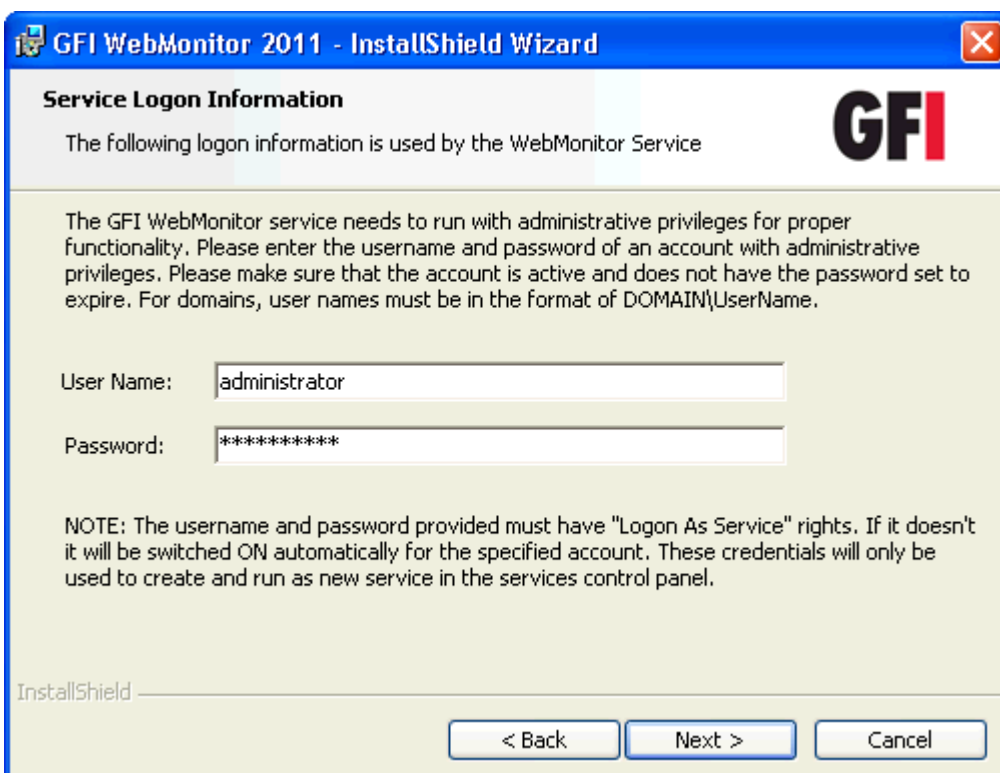


Screenshot 2 - Installation: Customer Information

6. Key in the **User Name** and **Organization**. If you have a license key, update the **License Key** details and click **Next**.



The license key can be keyed in after installation or expiration of the evaluation period of GFI WebMonitor. For more information, refer to the [Entering Your License Key After Installation](#) section in the Miscellaneous chapter.



Screenshot 3 - Installation: Service Logon Information

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



The user account must have **Log on as a service** rights; otherwise, rights are automatically assigned. For more information, refer to the [Assigning Log On As A Service Rights](#) section in the Miscellaneous chapter.

GFI WebMonitor 2011 - InstallShield Wizard

Mail Settings

Enter administrator email and SMTP mail server settings

GFI

Please enter the details of the SMTP server and email address that are to be used by GFI WebMonitor 2011 for email reporting.

From:

To:

SMTP Server: Port:

InstallShield

Screenshot 4 - Installation: Mail Settings

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

3.3.3 Post-installation Test

To test the installation from the machine where GFI WebMonitor was installed:

- » **Option 1:** Launch GFI WebMonitor web console by clicking **Start ► Programs ► GFI WebMonitor ► GFI WebMonitor**.
- » **Option 2:** Key in the URL <http://monitor.isa> in a web browser on the same machine.

To test 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.

3.3.4 Post-installation Actions

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
- » Configuring Internet browsers to use specific proxy settings on each client machine either automatically or manually.

Configuring FTP access in Microsoft ISA Server / Forefront TMG. This can be achieved by:

- » **Option 1:** Restricting or denying FTP access
- » **Option 2:** Disabling the FTP Access Filter

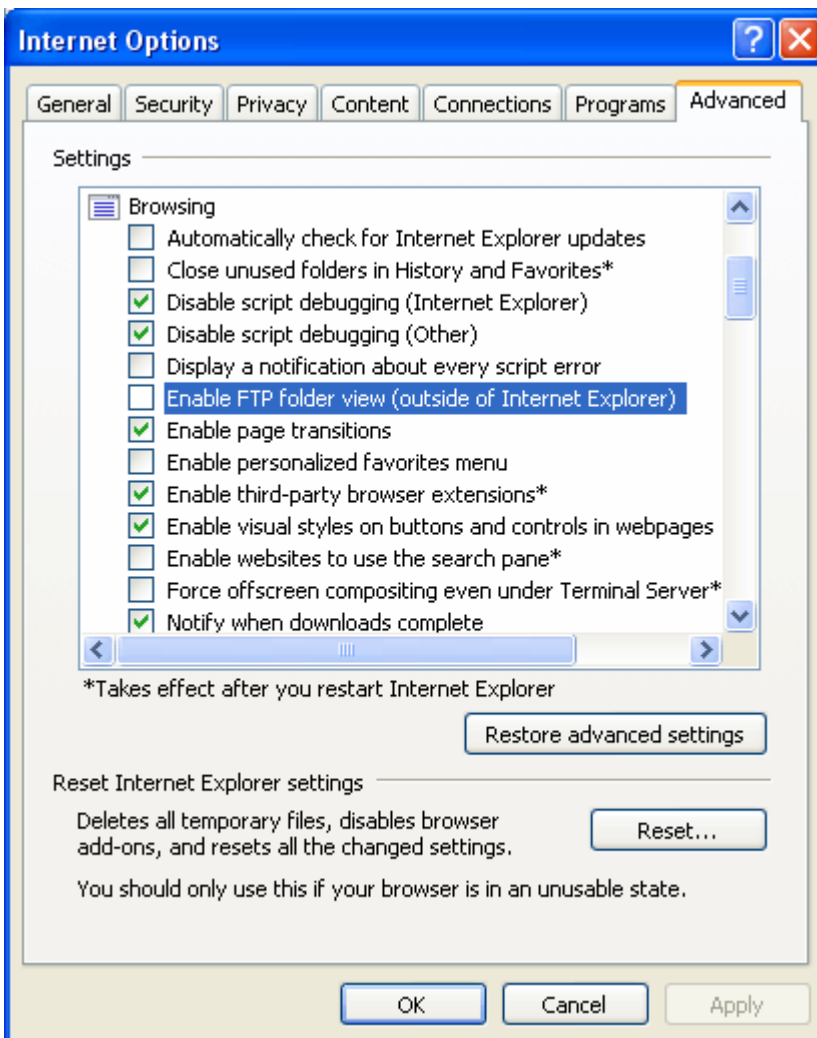
Routing FTP Downloads Through Proxy

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.

Step 1: Disabling Folder View in Microsoft Internet Explorer

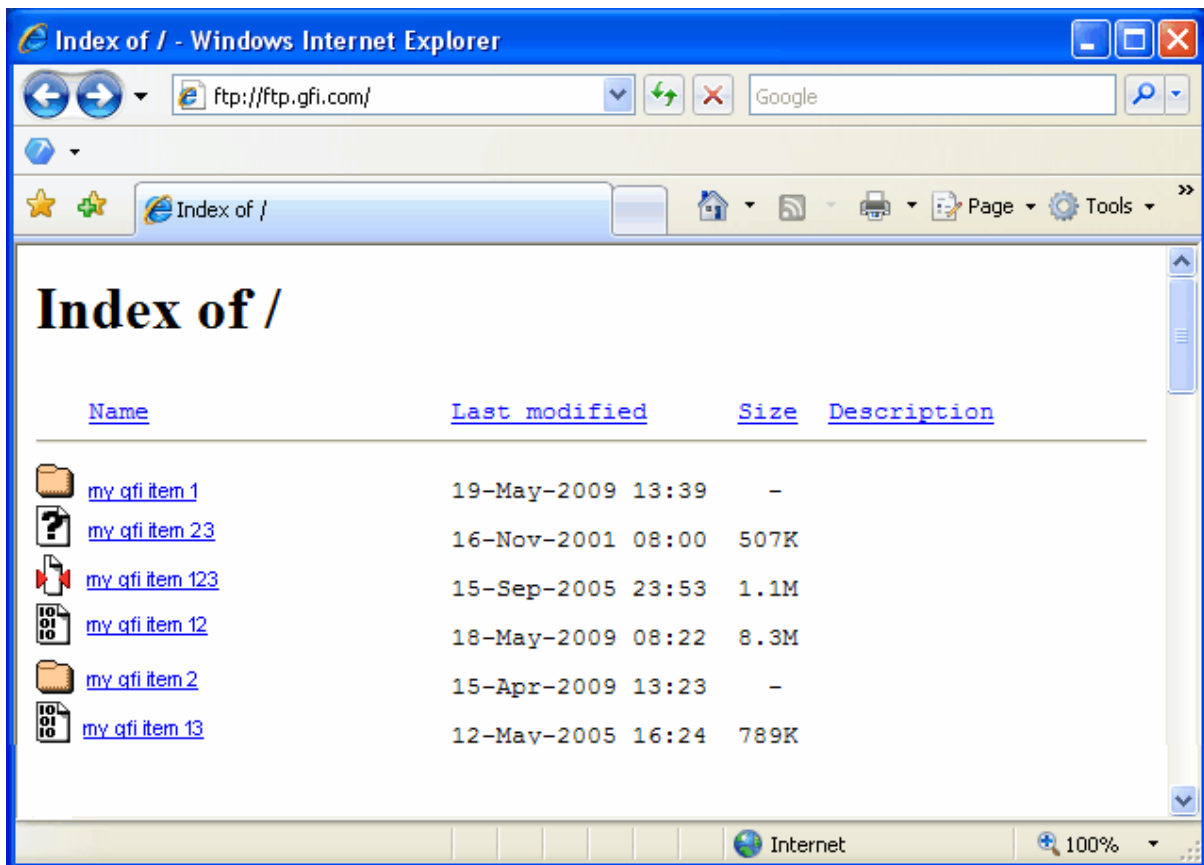
To disable folder view in Internet Explorer:

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



Screenshot 5 - Internet Options dialog box

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



Screenshot 6 - An FTP site viewed through Internet Explorer



When this checkbox is unchecked, browsing the contents of an FTP server looks like the preceding screenshot. Users will be able to browse and download from FTP servers using an HTTP based folder view. In addition, GFI WebMonitor will now be able to scan the FTP server contents and allow, quarantine or block the contents as applicable.

Step 2: Configuring Browsers to Use a Proxy Server

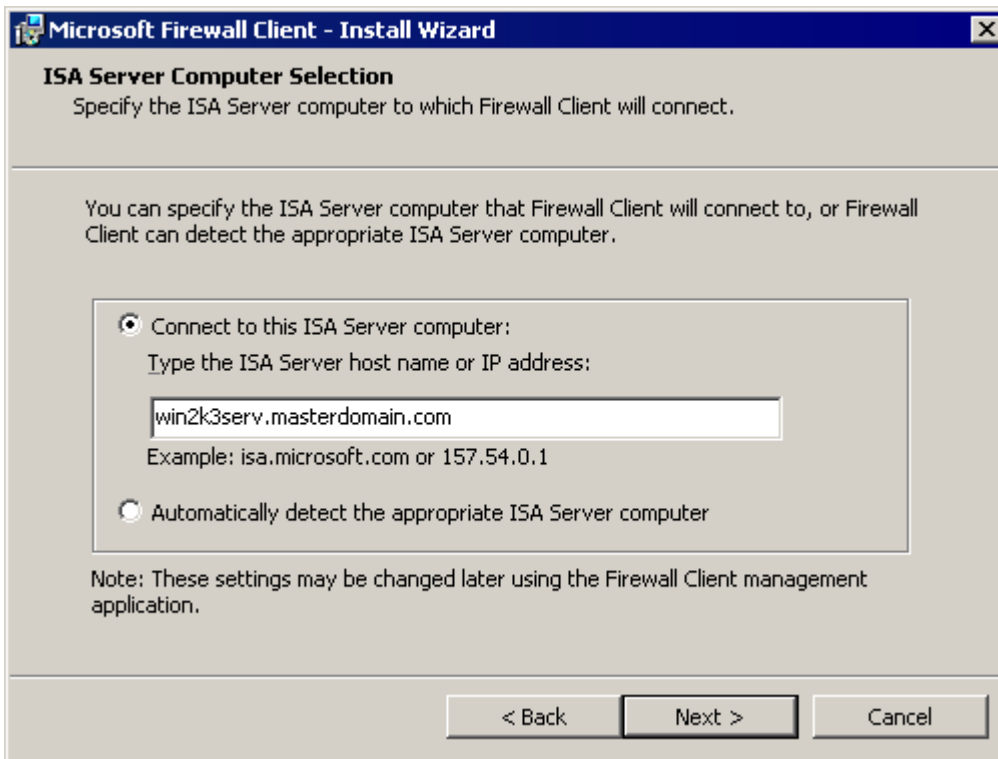
Internet browsers can be configured either automatically or manually to use a proxy server.

Option 1: Configuring Proxy settings automatically in Microsoft ISA Server and Microsoft Forefront TMG


Microsoft Firewall Client for ISA Server or Microsoft Firewall Client for Forefront TMG automatically configures proxy settings.

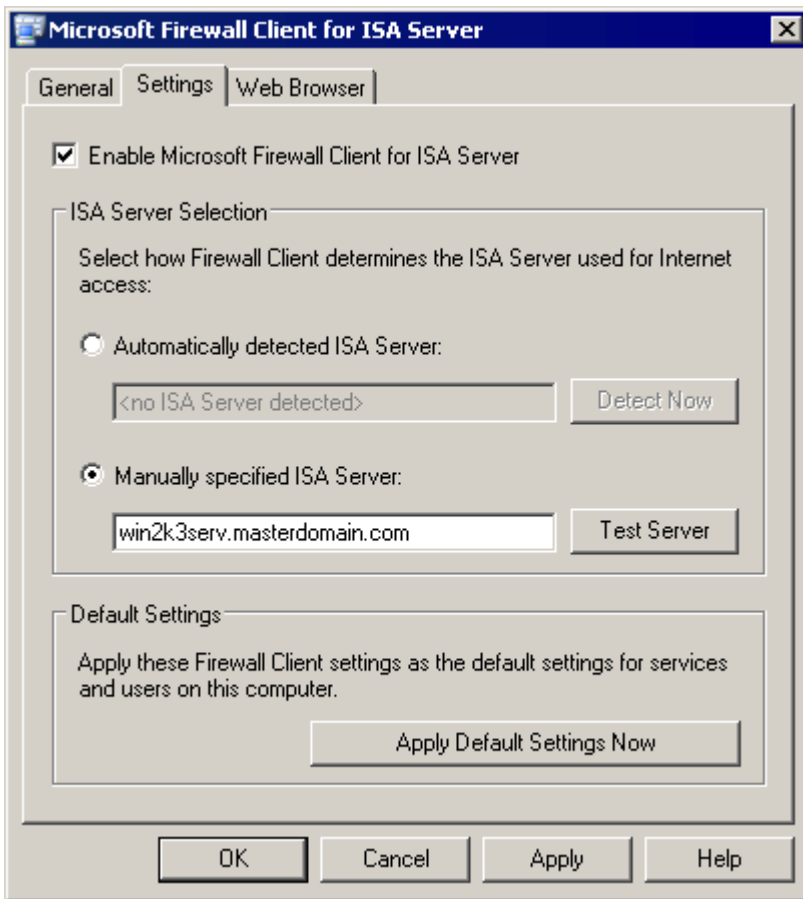
To install the Microsoft Firewall Client for ISA Server:

1. Download **Microsoft Firewall Client for ISA Server** from Microsoft's web site.
2. Double click the **Microsoft Firewall Client for ISA Server** executable file.



Screenshot 7 - 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 the icon  in the windows notification area and choose **Configure**.



Screenshot 8 - Microsoft Firewall Client for ISA Server: Settings tab



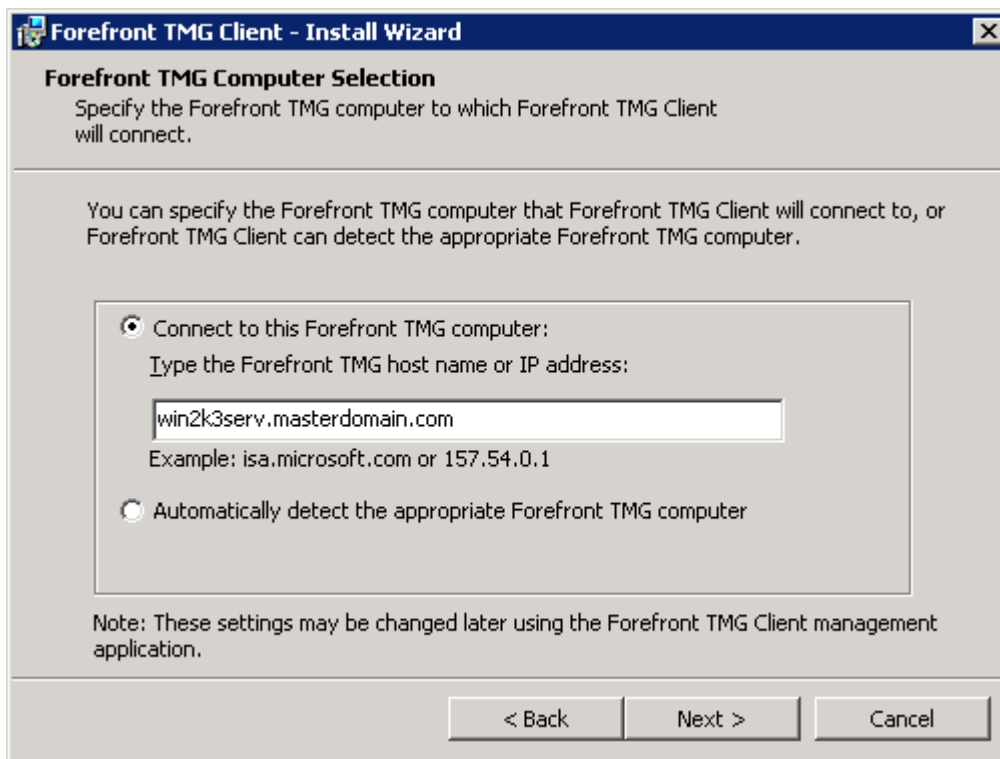
Click **Settings** Tab to modify the server configurations.

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** button.
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**.



Screenshot 9 - Microsoft 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**.

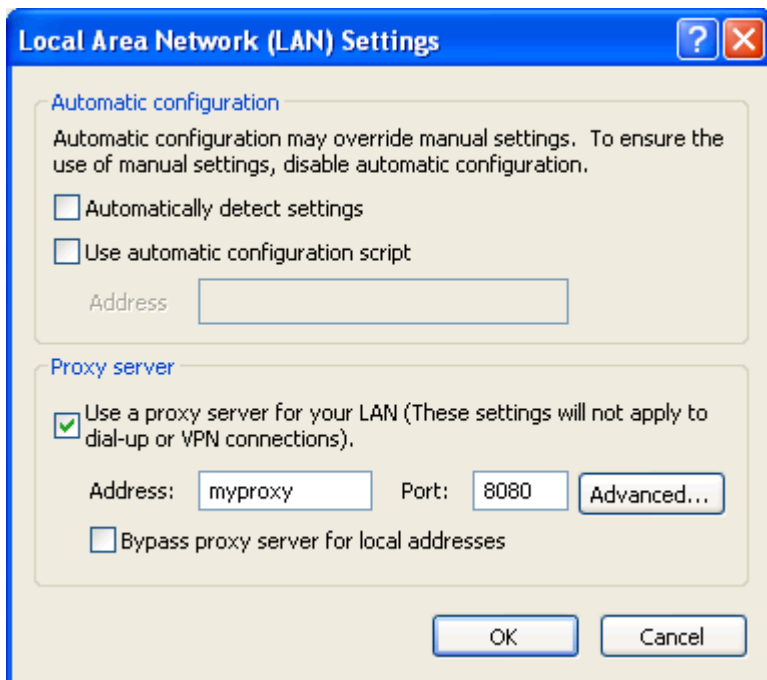
To configure the web browser automatically:

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** button.
4. Click **OK**.

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** button.



Screenshot 10 - 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.

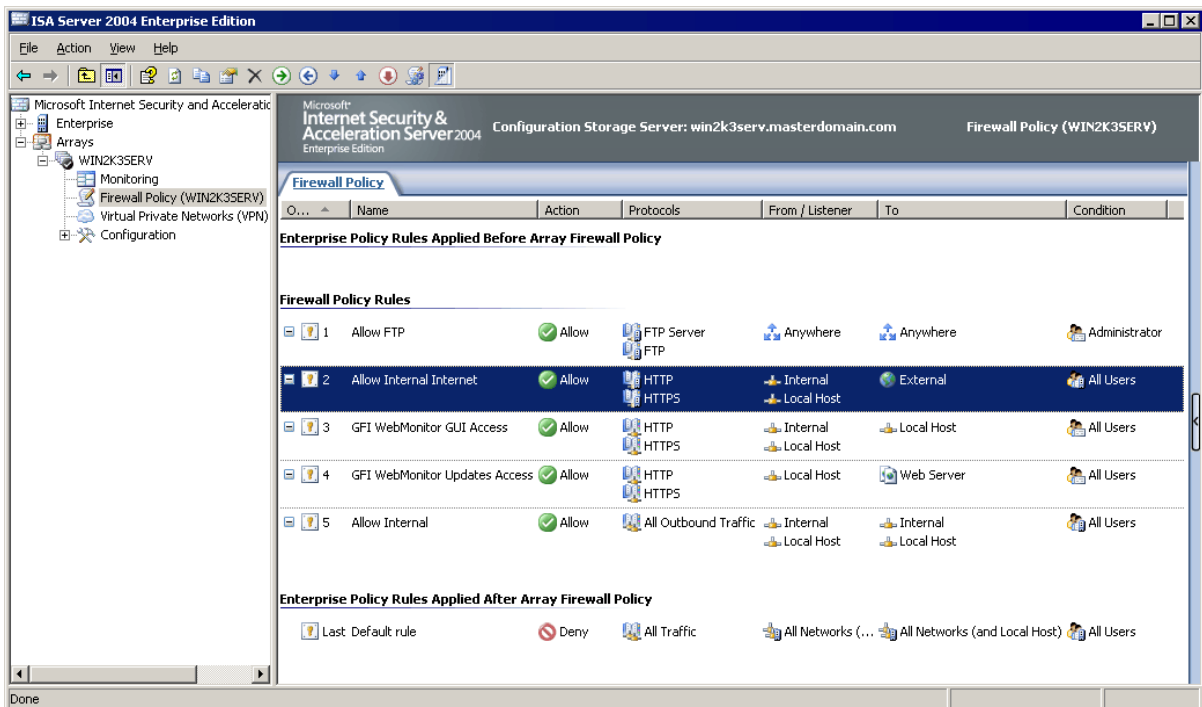
Configuring FTP access

By default, Microsoft ISA Server / Forefront TMG deny 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.

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.



Screenshot 11 - Microsoft ISA Server: Configured Firewall policies

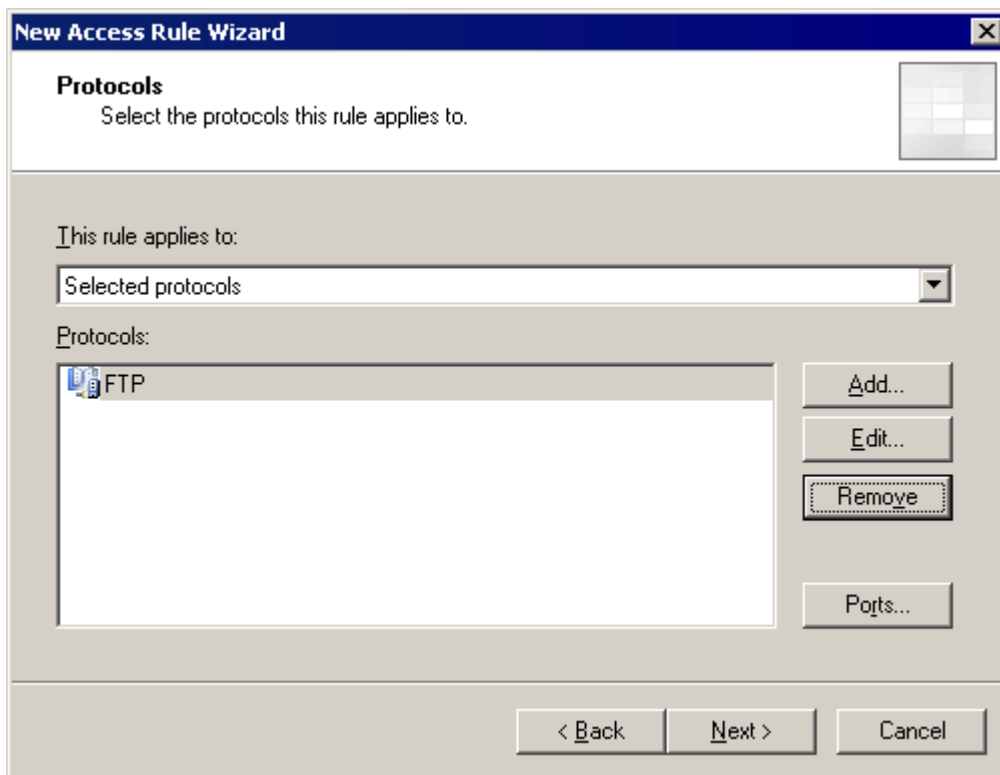
The preceding screenshot shows both rules.

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:

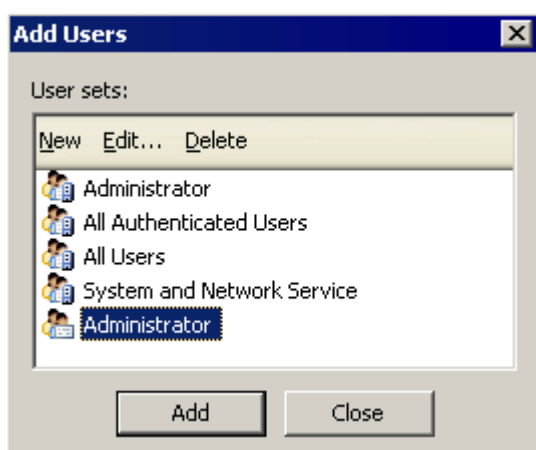
On Microsoft ISA Server

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**.



Screenshot 12 - 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 click **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**.

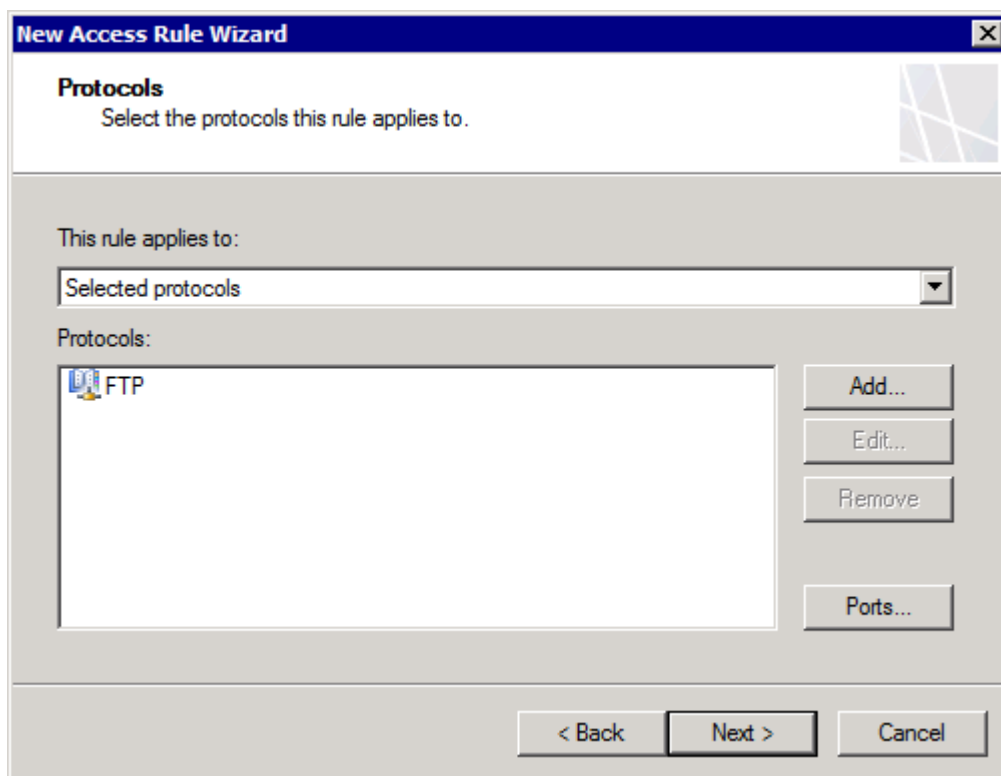


Screenshot 13 - Microsoft ISA Server: Add Users dialog

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.

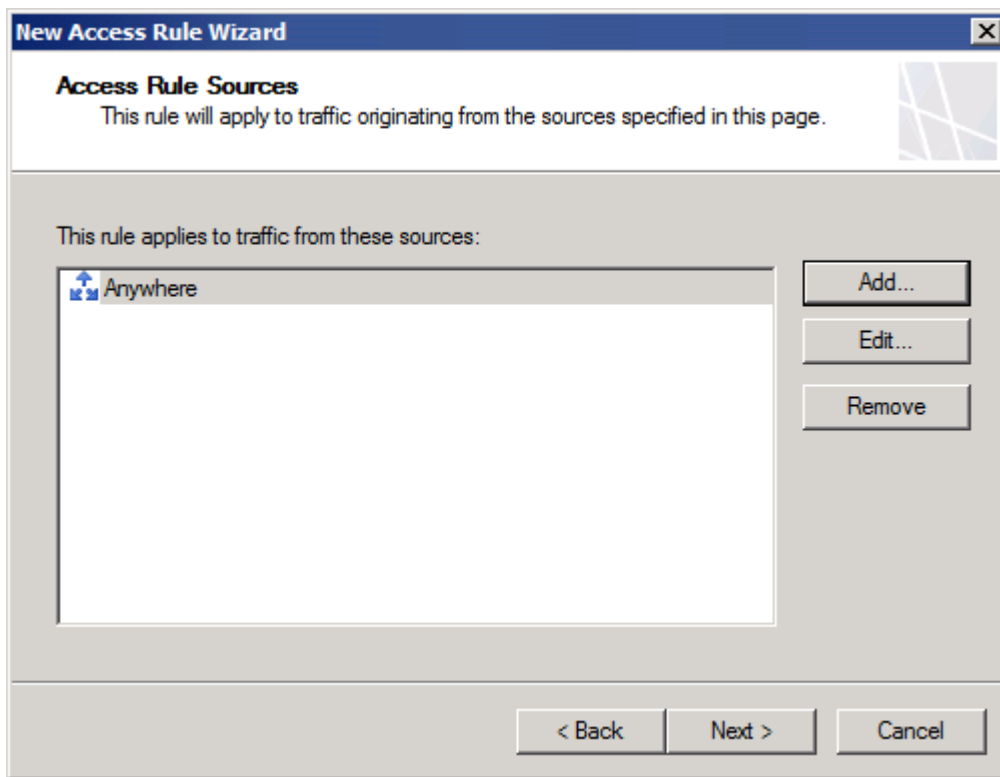
On Microsoft Forefront TMG

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**.



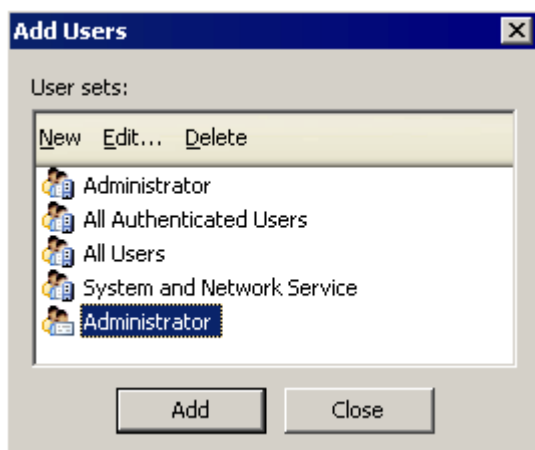
Screenshot 14 - Microsoft Forefront TMG: Protocols dialog

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**.



Screenshot 15 - 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**.



Screenshot 16 - 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.

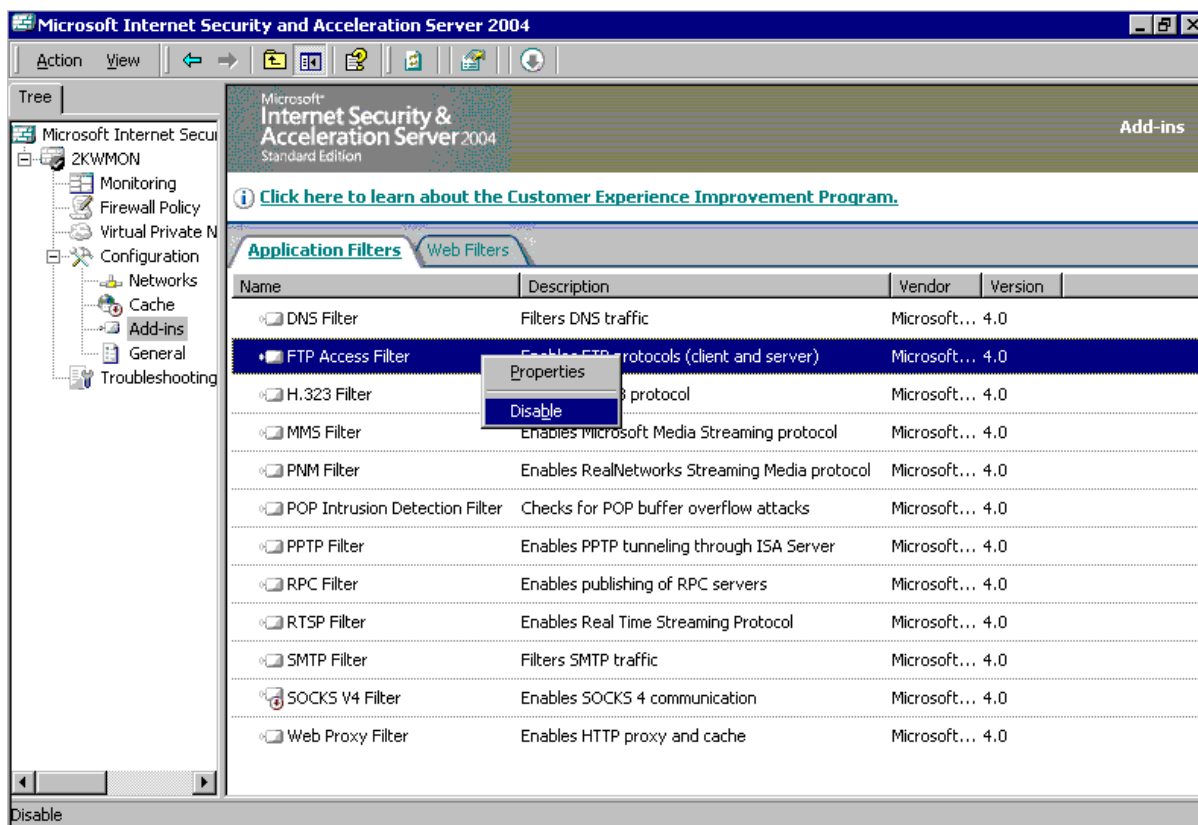
Option 2: Disabling the FTP Access Filter

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**.



Screenshot 17 - Microsoft ISA Server 2004: Configured Application filters

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

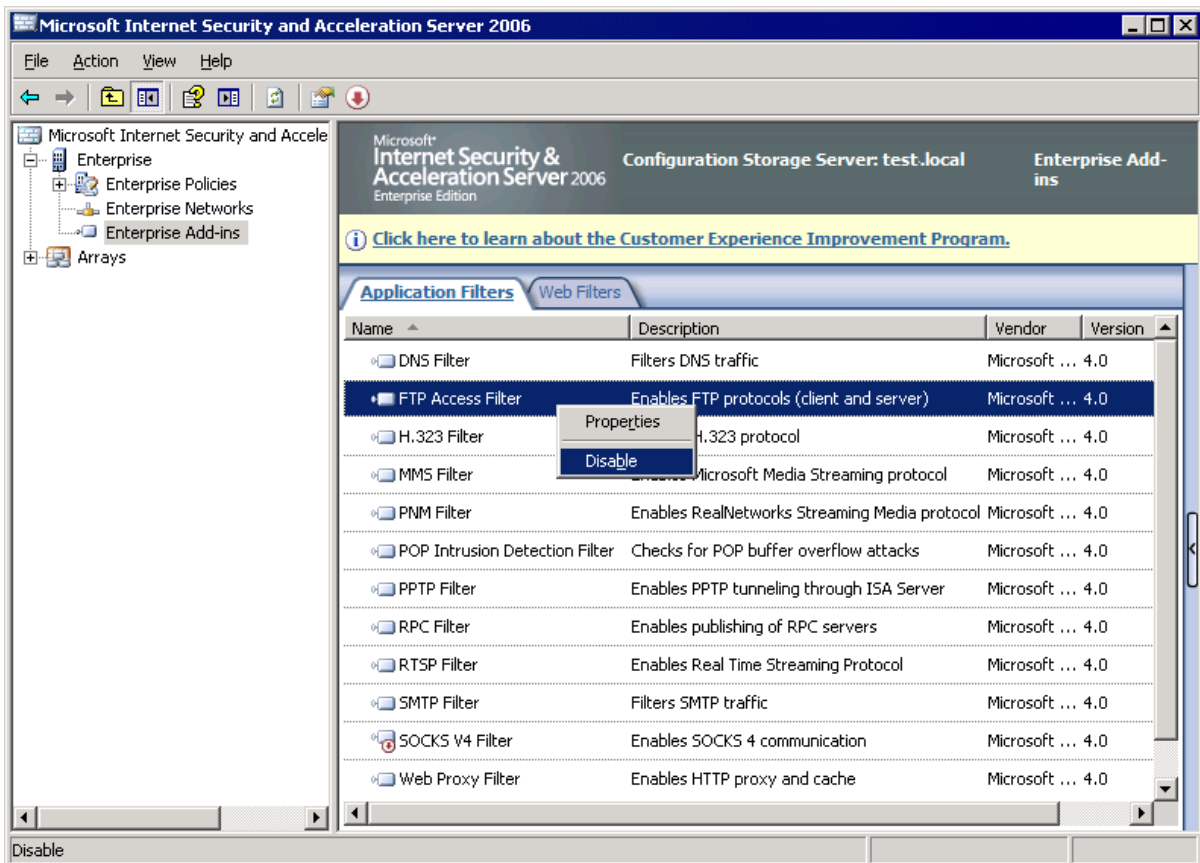
3. Right-click **FTP Access Filter** and select **Disable**.

4. Make sure to 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**.



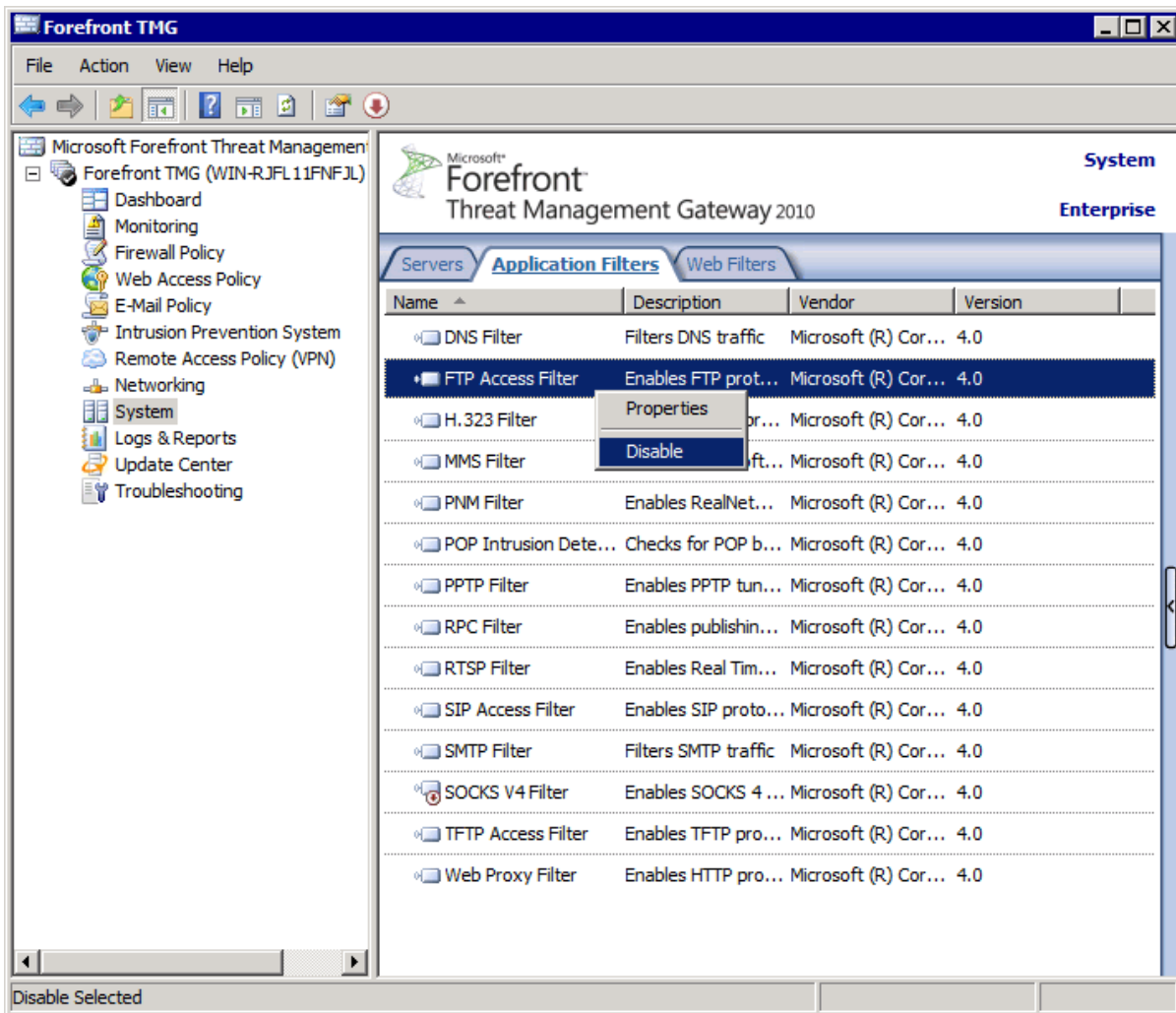
Screenshot 18 - Microsoft ISA Server 2006: Configured Application filters

2. From the left panel expand **Enterprise ► Enterprise Add-ins**.
3. Right-click **FTP Access Filter** and select **Disable**.
4. Make sure to 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**.



Screenshot 19 - 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. Make sure to save settings before exiting.

4 Launching GFI WebMonitor

4.1 Introduction

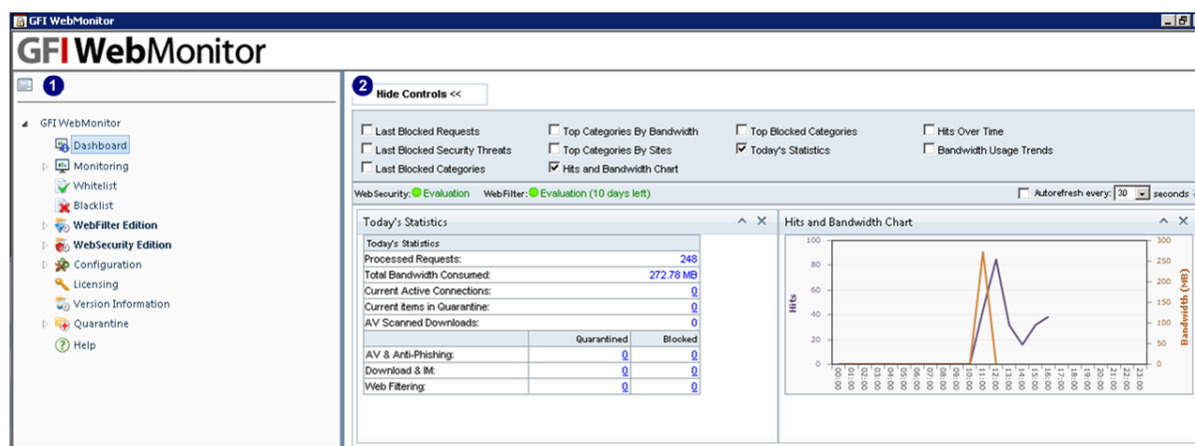
This chapter provides you with information related to the launching of GFI WebMonitor and an overview of the application's console.

4.2 Launching GFI WebMonitor

To launch GFI WebMonitor, navigate to **Start ► Programs ► GFI WebMonitor ► GFI WebMonitor**.

4.3 Navigating the Console

GFI WebMonitor's console provides you with all the administrative functionality to monitor and manage network internet traffic.



Screenshot 20 - GFI WebMonitor console view

1 Navigation Bar - The navigation bar is located on the left-hand side of the console, and contains a number of nodes used to view and configure settings. The available nodes are:

- » **Dashboard** - Provides a graphical overview of statistical information.
- » **Monitoring** - Provides several monitoring reports.
- » **Whitelist/Blacklist** - Permanent and/or temporary whitelisting and blacklisting functions.
- » **WebFilter Edition** - Provides access management for specific website categories for users, groups and IP addresses during specified periods.
- » **WebSecurity Edition** - Provides access management and control restrictions to web applications for users, groups and IP addresses.
- » **Configuration** - Provides configuration settings and administrative features for GFI WebMonitor.
- » **Licensing and Version Information** - Provides access to the licensing setup and version information.
- » **Quarantine** - Provides configuration and management of quarantined items that were blocked by GFI WebMonitor.

» **Help** - Provides help on all aspects of GFI WebMonitor's functionality.

2 Viewing Pane - The viewing pane is located on the right-hand side of the console, and allows the administrator to view and configure settings according to the node selected from the Navigation Bar.

5 *Miscellaneous*

5.1 Introduction

The miscellaneous chapter gathers all the other information that falls outside the initial configuration of GFI WebMonitor.

5.2 Entering Your License Key After Installation

After installing GFI WebMonitor, you can enter your license key without re-installing or re-configuring the application.

To enter your license key:

1. Navigate to the **Licensing** node.
2. In the **License Key** text box, key in the license key provided by GFI Software for one of the three GFI WebMonitor editions.
3. Click **Save Settings** to finalize entering your license key.



Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

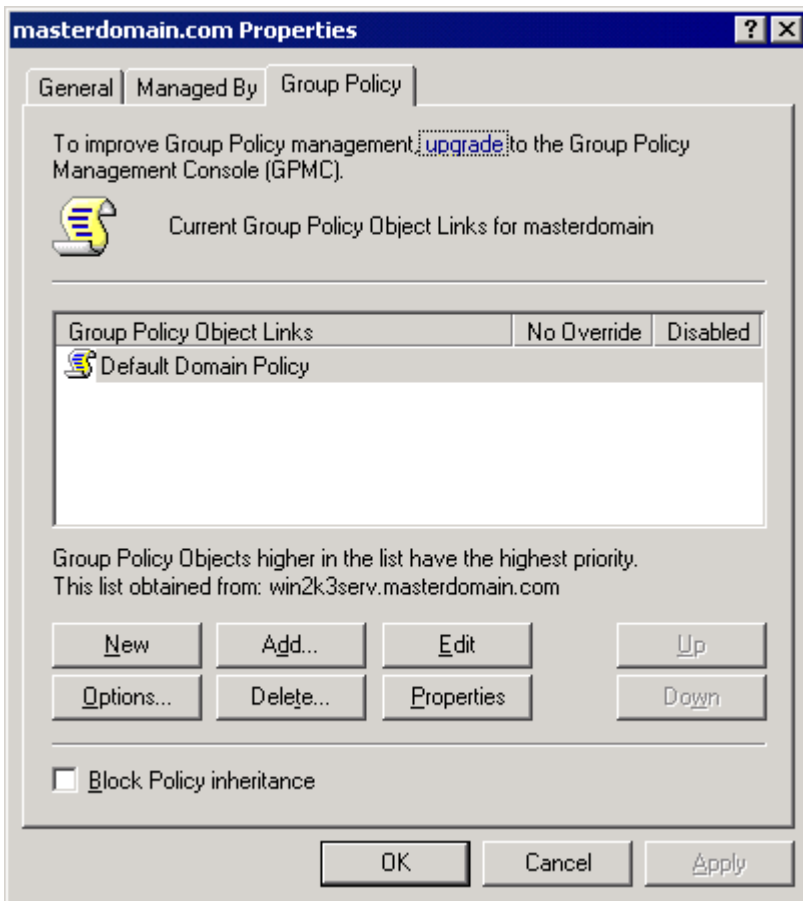
5.3 Disabling Internet Connections Settings on Client Machines

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

5.3.1 Disabling Internet Connections Page Using GPO in Microsoft Windows Server 2003

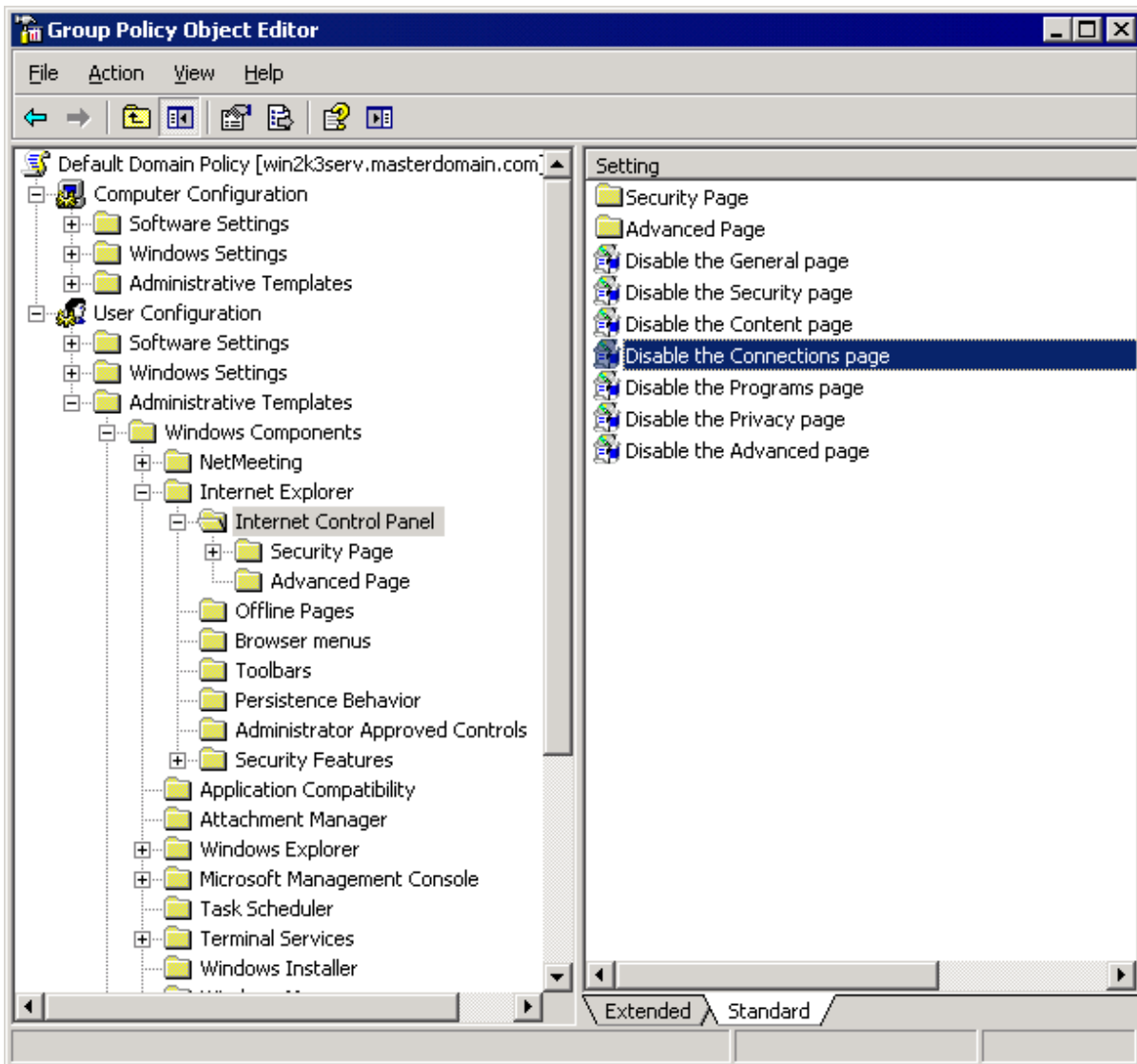
To disable Connections settings on client machines through Microsoft Windows Server 2003 GPO:

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**.



Screenshot 21 - Active Directory GPO dialog

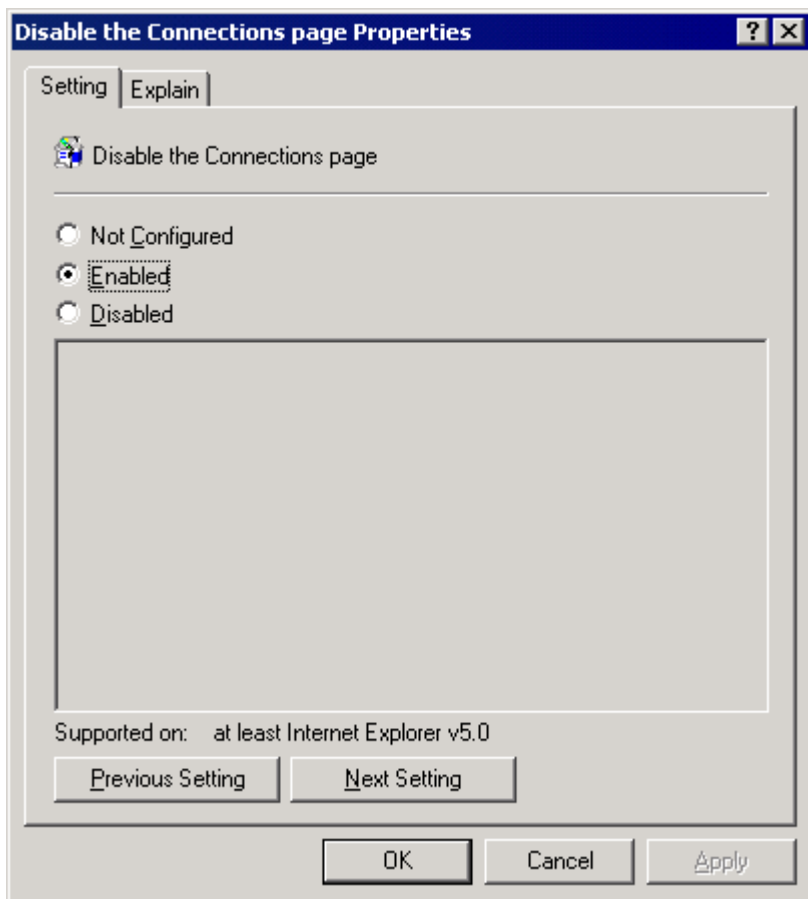
3. Select **Group Policy** tab in the **Domain Properties** dialog.
4. Select **Default Domain Policy** from the list and click **Edit**.



Screenshot 22 - 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**.



Screenshot 23 - Disable the Connection page Properties dialog

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



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

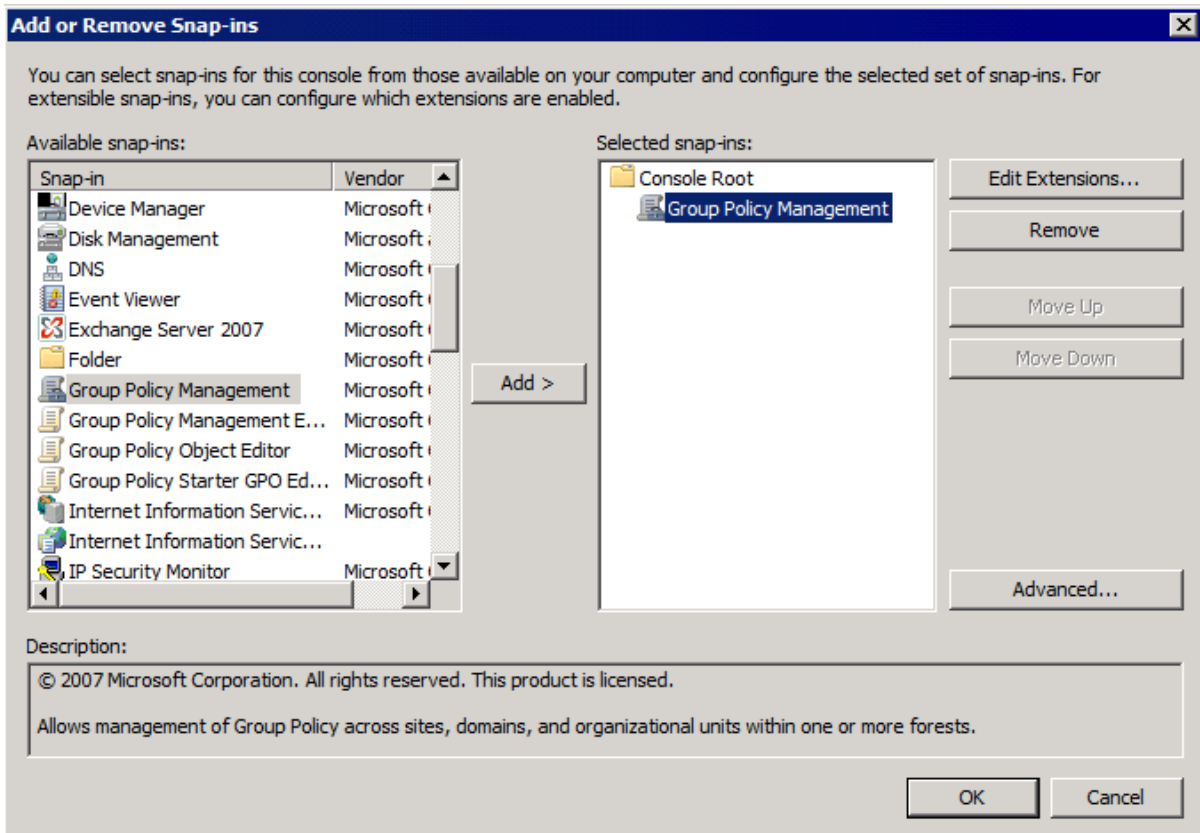
8. Click **Apply** and **OK**.

9. Close all open windows.

5.3.2 Disabling Internet Connections Page Using GPO in Microsoft Windows Server 2008

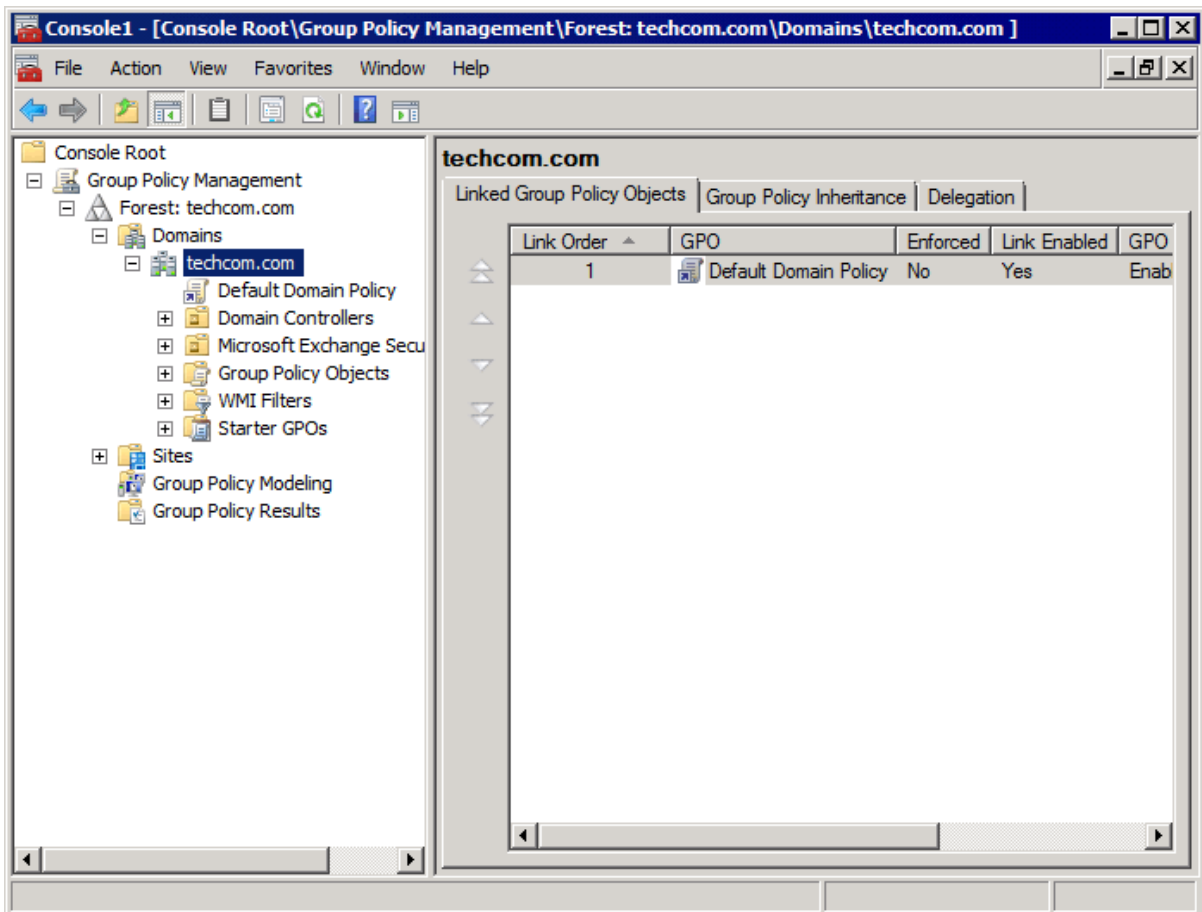
To disable **Connections** settings on clients' machines through Microsoft Windows Server 2008 GPO:

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.



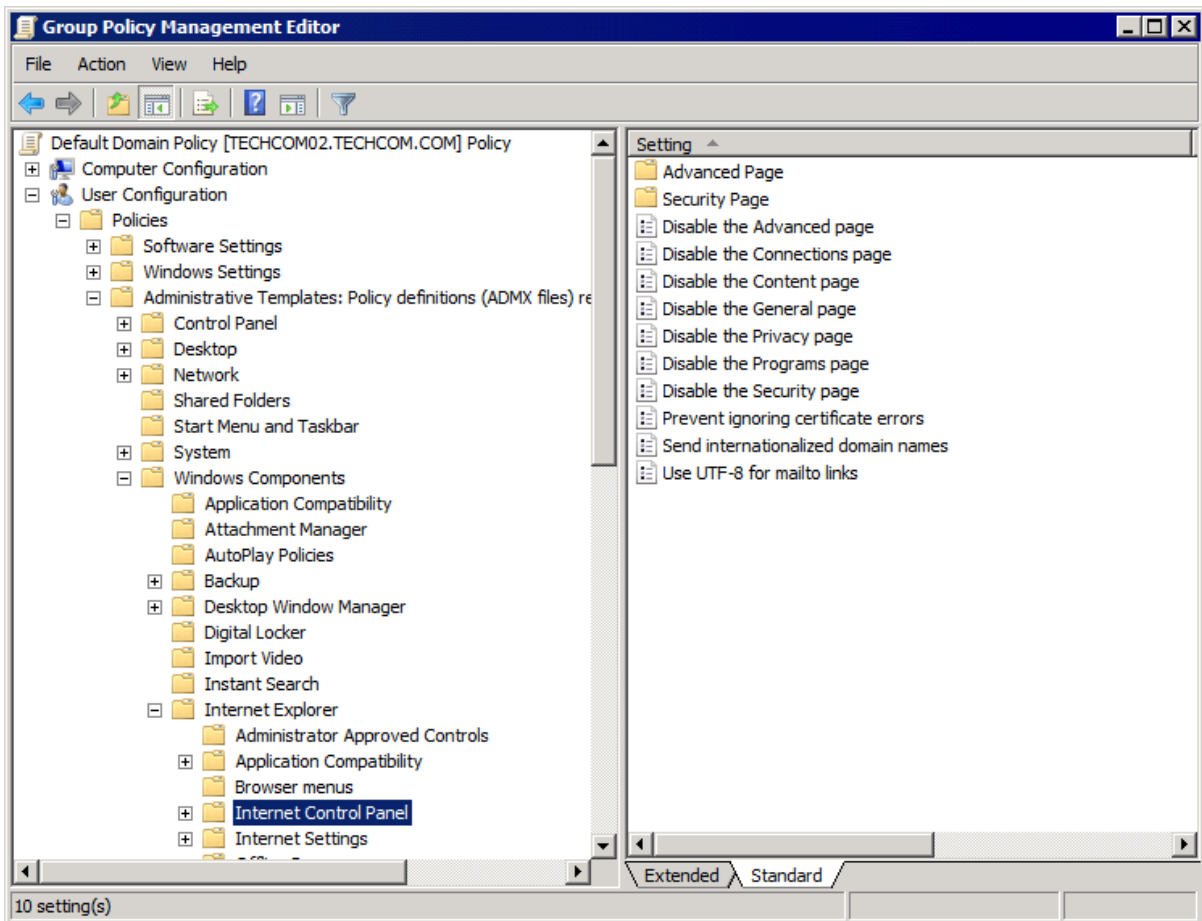
Screenshot 24 - Add/Remove Snap-ins window

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



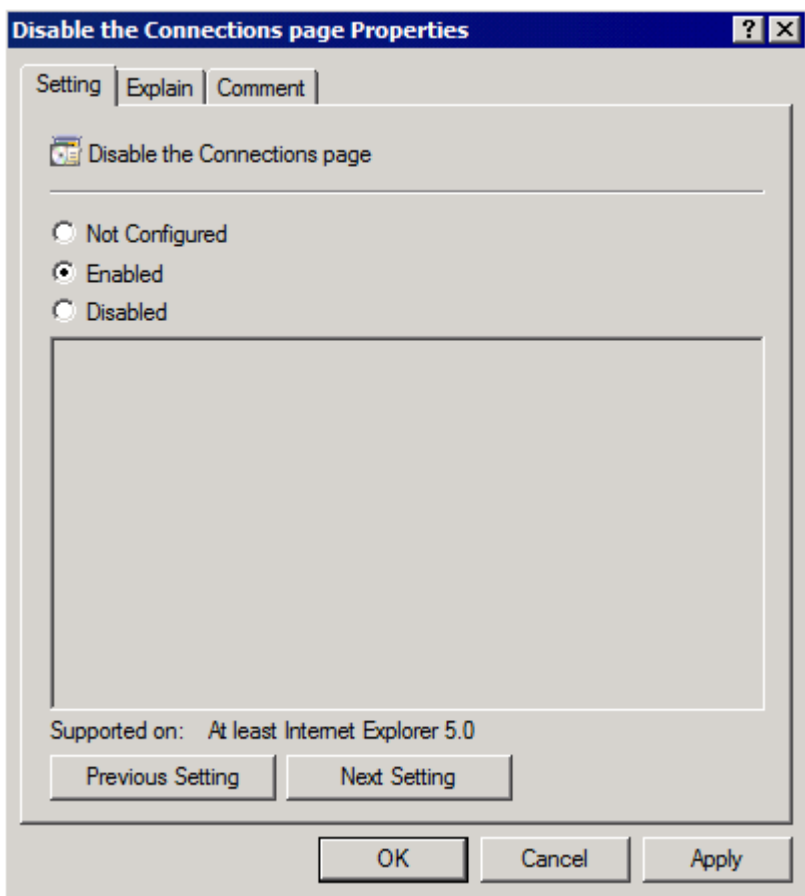
Screenshot 25 - Console Root domain window

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 26 - 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**.



Screenshot 27 - Disable the Connection page Properties dialog

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



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.

5.4 Assigning Log On As A Service Rights

5.4.1 Assigning Log On As A Service Rights on Microsoft Windows XP and Microsoft Windows Vista Manually

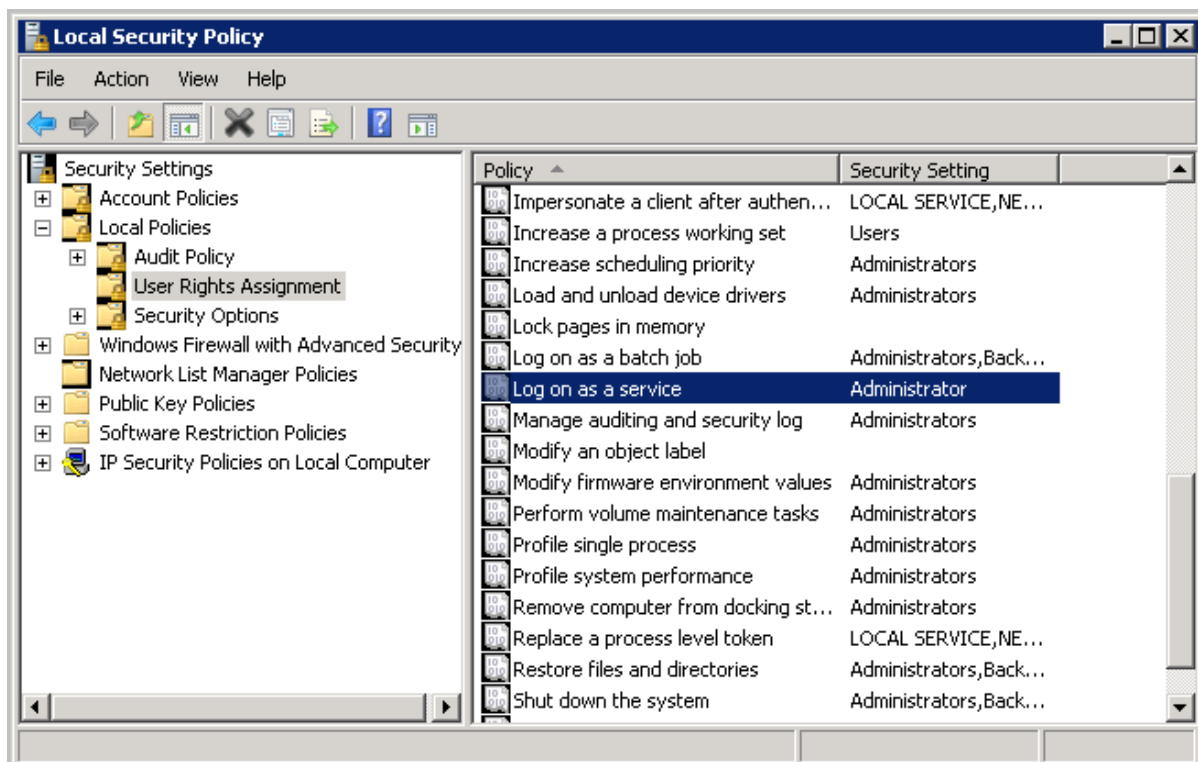
To assign **Log on as a service** rights to a user account on Microsoft Windows XP (SP2) or Microsoft Windows Vista machine manually:

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** button.
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.

5.4.2 Assigning Log On As A Service Rights on a Server Machine Manually

To assign **Log on as service** rights to a user account on Microsoft Windows Server 2003 or Microsoft Windows Server 2008 machines manually:

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



Screenshot 28 - Microsoft Windows Server: Local Security Policy window

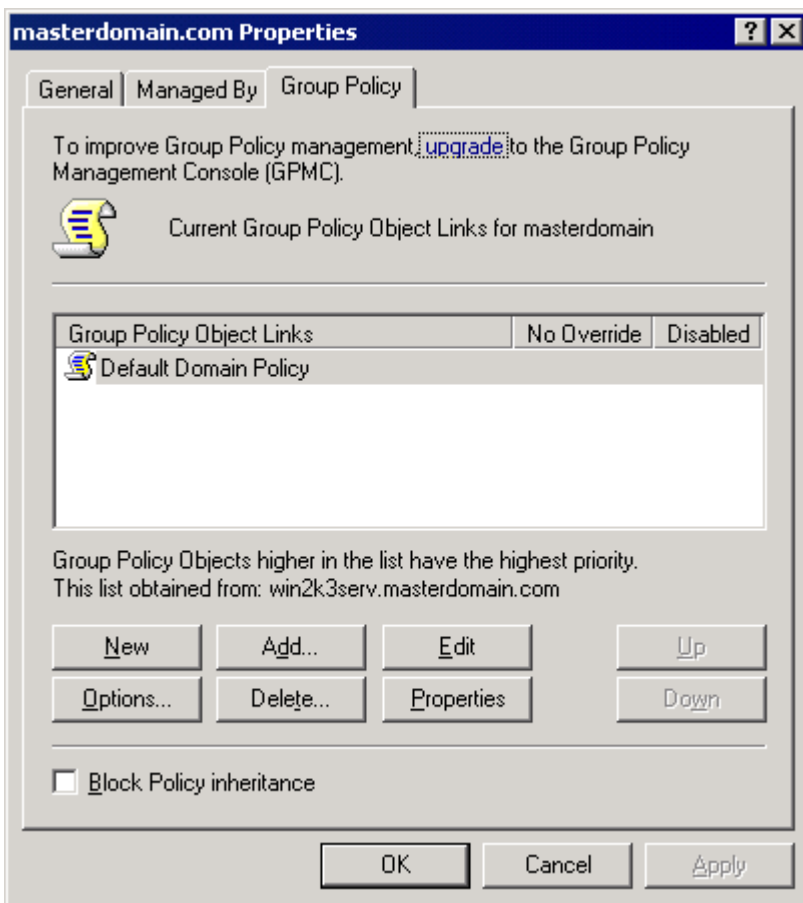
2. Expand **Security Settings ► Local Policies ► User Rights Assignment**.
3. Right-click **Log on as a service** from the right panel and click **Properties**.

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.

5.4.3 Assigning Log On As A Service Rights Using GPO in Microsoft Windows Server 2003

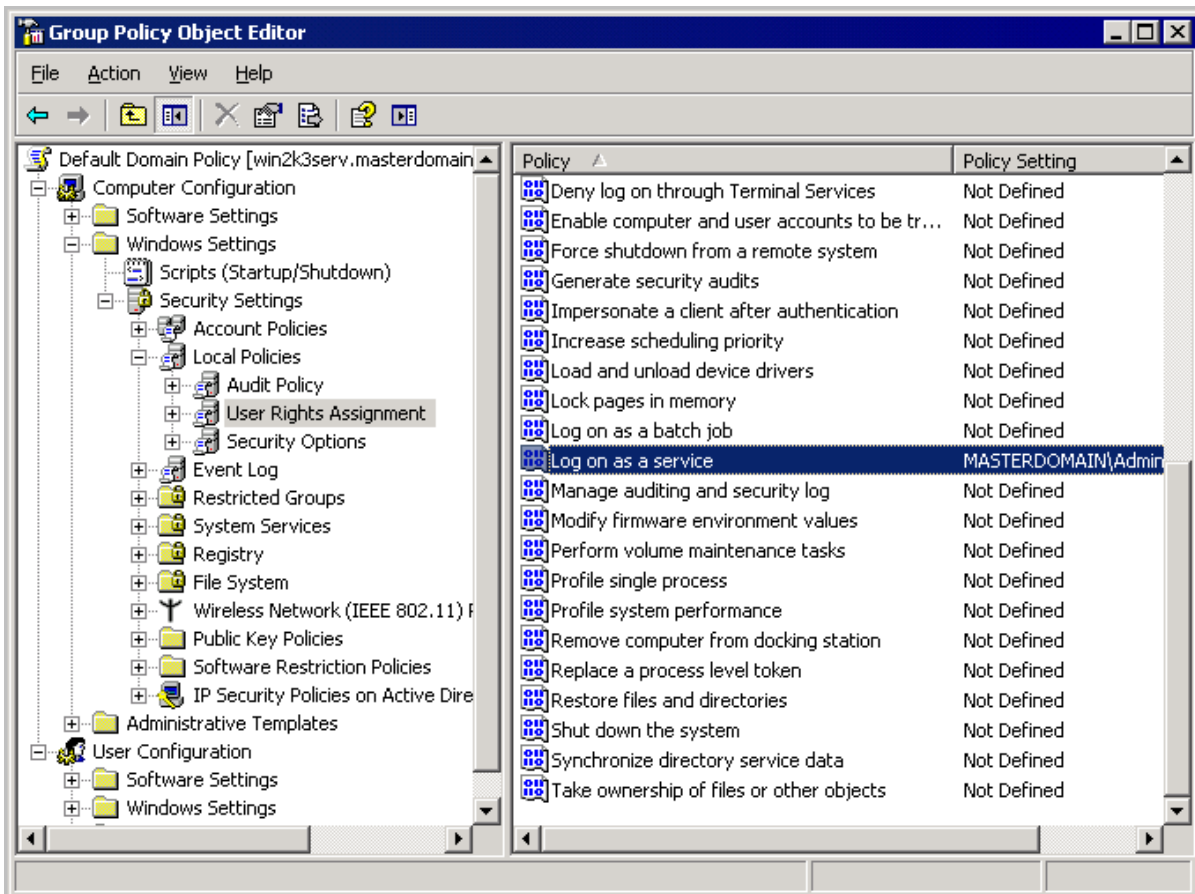
To assign **Log on as service** rights on clients' machines through Microsoft Windows Server 2003 GPO:

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**.



Screenshot 29 - 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**



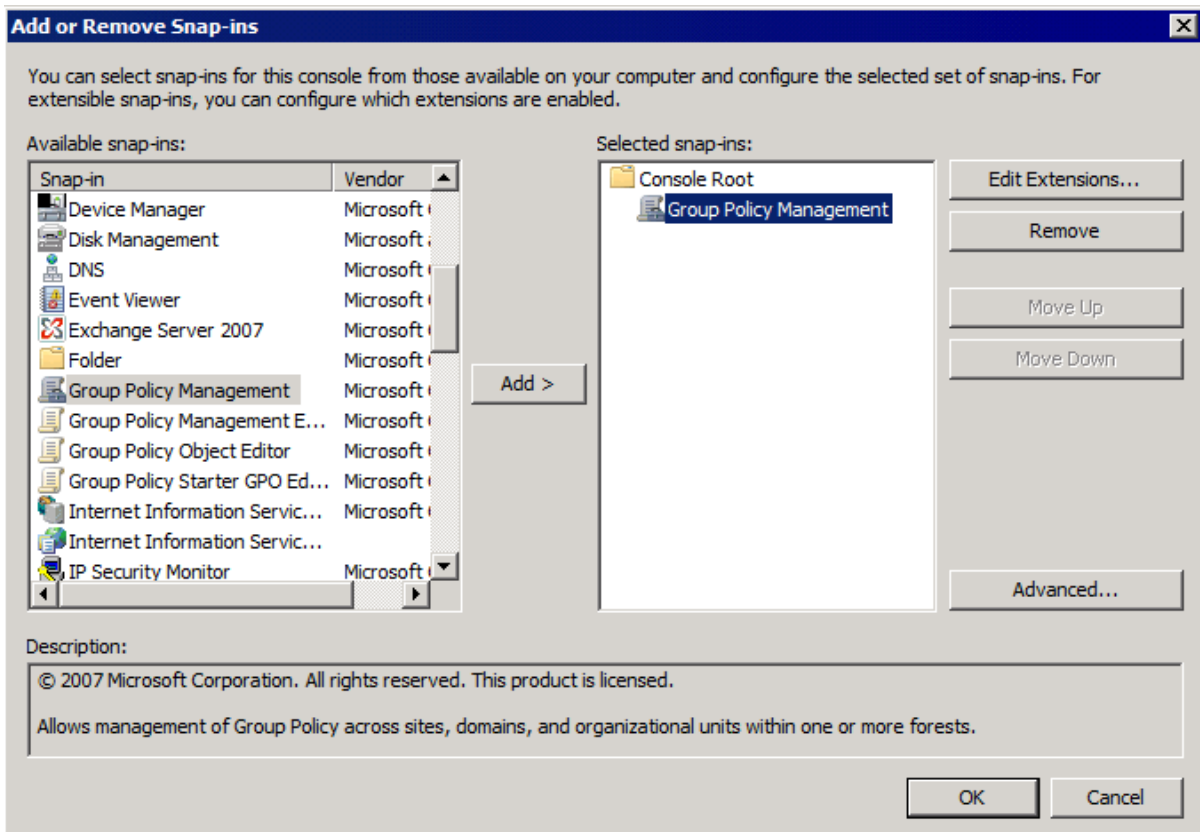
Screenshot 30 - GPO Editor window

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.

5.4.4 Assigning Log On As A Service Rights Using GPO in Microsoft Windows Server 2008

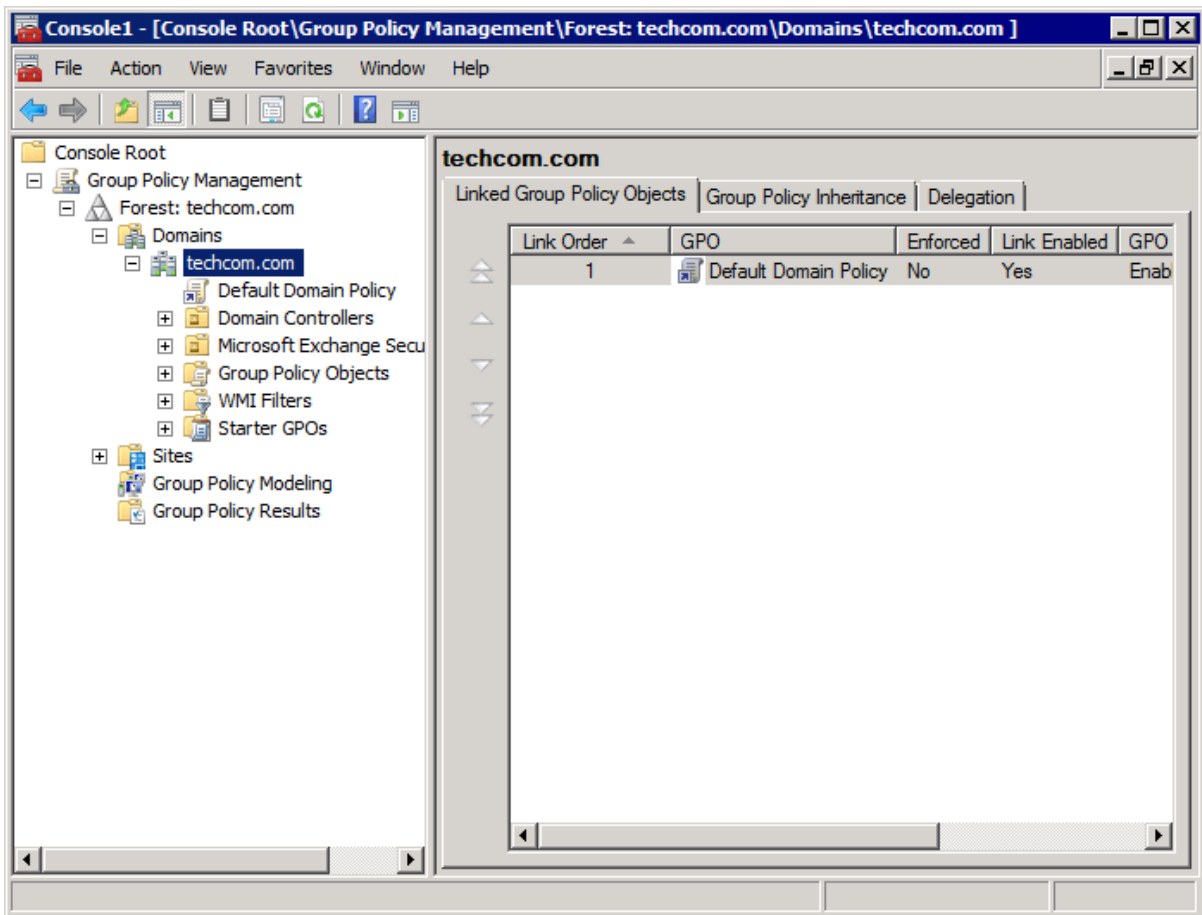
To assign Log on as service rights on clients' machines through Microsoft Windows Server 2008 GPO:

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.



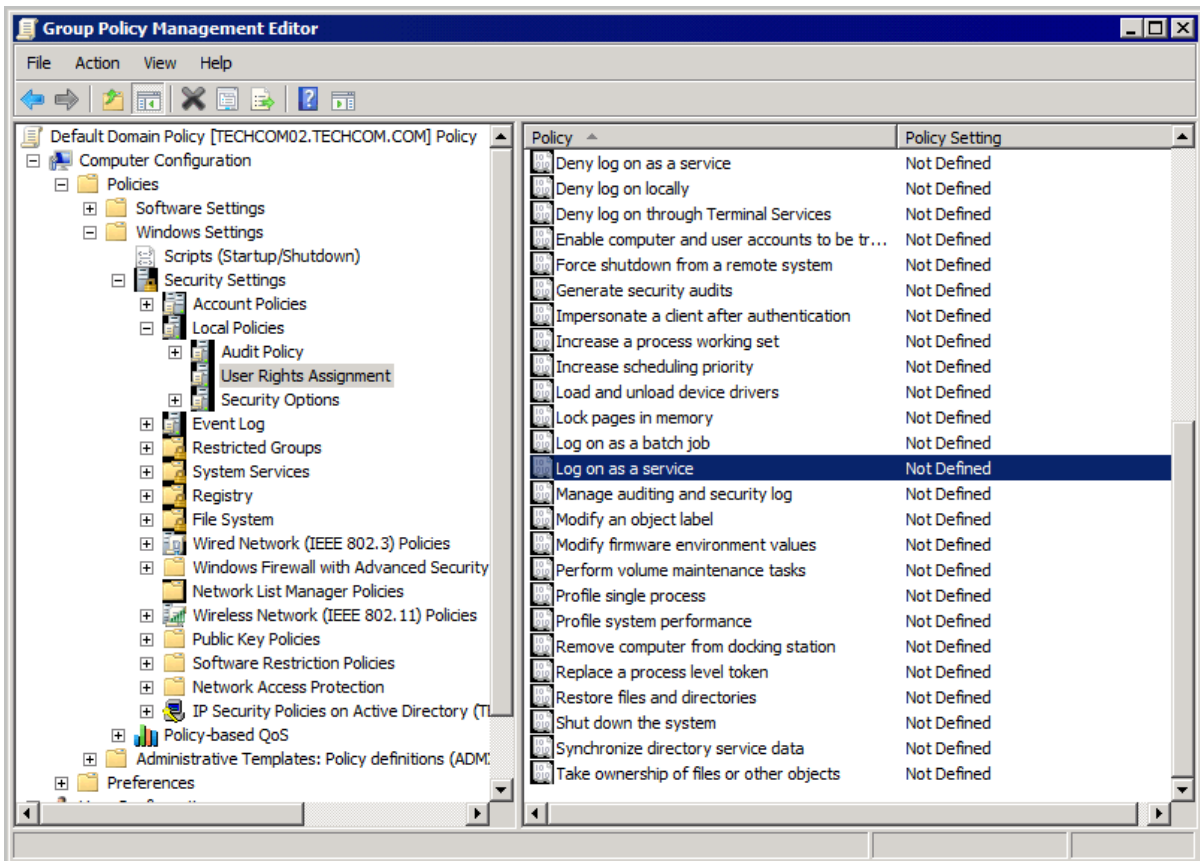
Screenshot 31 - Add/Remove Snap-ins window

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



Screenshot 32 - 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 33 - 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.

6 Troubleshooting

6.1 Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- » The manual - most issues can be solved by reading this manual
- » GFI Knowledge Base articles
- » Web forum
- » Contacting GFI Technical Support

6.2 Knowledge Base

GFI maintains a comprehensive Knowledge Base repository, which includes answers to the most common problems. In case that the information in this manual does not solve your installation problems, next refer to the Knowledge Base. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. Access the Knowledge Base by visiting: <http://kbase.gfi.com/>.

6.3 Web Forum

User to user technical support is available via the web forum. The forum can be found at: <http://forums.gfi.com/>.

6.4 Request Technical Support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

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



Before you contact our Technical Support team, have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at <https://customers.gfi.com/login.aspx>.

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

6.5 Build Notifications

We recommend that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit: <http://www.gfi.com/pages/productmailing.htm>

7 Glossary

| TERM | DEFINITION |
|---|--|
| 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. |
| Anti-virus | Software that detects viruses on a computer. |
| Bandwidth | The maximum amount of data transferred over a medium. Typically measured in bits per second. |
| Blacklist | A list that contains information about what should be blocked by GFI WebMonitor. |
| 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 |
| Dashboard | Enables the user to obtain graphical and statistical information related to GFI WebMonitor operations. |
| Expired Certificate | An expired certificate has an end date that is earlier than the date when the certificate is validated by GFI WebMonitor. |
| File Transfer Protocol | A protocol used to transfer files between computers. |
| FTP | See File Transfer Protocol. |
| 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. |
| 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:. |
| 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. |

| TERM | DEFINITION |
|---|--|
| 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. |
| 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 |
| 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. |
| 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. |
| Quarantine | A temporary storage for unknown data that awaits approval from an administrator. |
| 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). |
| Spyware | Unwanted software that publishes private information to an external source. |
| Traffic Forwarding | The act of forwarding internal/external network traffic to a specific server through a router. |
| 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. |

| TERM | DEFINITION |
|---|--|
| User Agent | A client application that connects to the Internet and performs automatic actions. |
| Virus | Unwanted software that infects a computer. |
| 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. |
| Whitelist | A list that contains information about what should be allowed by GFI WebMonitor. |
| Wide Area Network | An external network that connects machines in large areas. |
| WPAD | See Web Proxy AutoDiscovery protocol. |

Index

A

Access Control 47
Active Directory GPO 30

B

Build Notifications 45

C

Chained Proxy 47

F

FTP 12, 13, 14, 18, 19, 23, 24, 25

H

Hidden downloads 47
HTTP 14

I

Internet Gateway 47

L

LDAP 47
License key 11, 29, 45
Log on as a service rights 37, 39

M

Malware 6
Microsoft Forefront TMG 1, 21, 24
MSN 48

P

Phishing 1, 6
Port Blocking 48
Proxy Server 14, 18, 47

S

Snap-ins 33, 41

Spyware 1, 6

T

Technical Support 45
Traffic Forwarding 48

U

Unified Protection Edition 3, 6
User Agent 49

W

Web Forum 45
Web traffic 1, 3, 5, 6, 49
WebGrade Database 3, 49
WPAD 49

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

Email: ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

Email: sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

Email: 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

Email: sales@gfiap.com



Disclaimer

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners. 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.
