Product Manual

GFI WebMonitor™

Administration and Configuration Manual

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

Last updated: 12 September 2011
Version number: WEBMON-GSG-EN-2.1.0

Contents

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 system administrators who want to use GFI WebMonitor in standalone proxy mode (for example, in environments where there is no Microsoft ISA Server or Microsoft Forefront TMG).

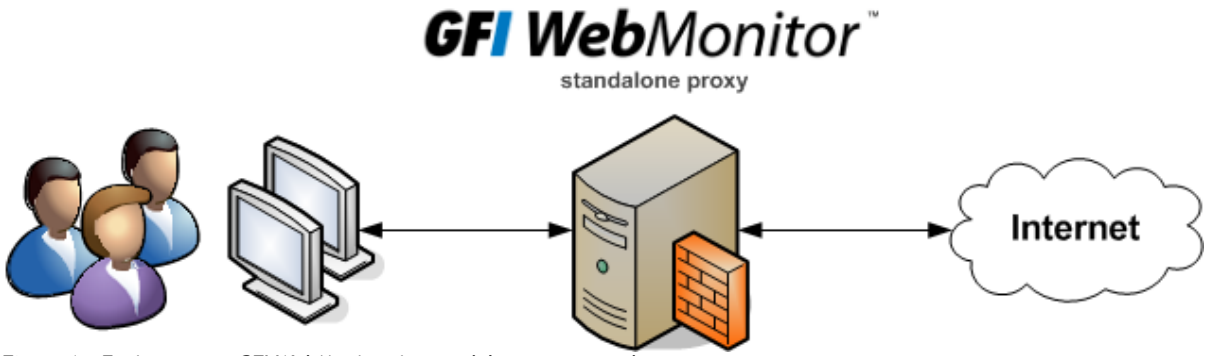


Figure 1 - *Environment: GFI WebMonitor in standalone proxy mode*

For environments with Microsoft ISA Server or Microsoft Forefront TMG, a dedicated version of GFI WebMonitor (GFI WebMonitor for ISA/TMG) is available. For more information, refer to: http://www.gfi.com/isa-server-monitoring-security.

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 in Gateway Mode** Provides information on how to install GFI WebMonitor in Gateway mode.
Chapter 4	**Installing in Simple Proxy Mode** Provides information on how to install GFI WebMonitor in Simple Proxy mode.

CHAPTER	DESCRIPTION
Chapter 5	**Launching GFI WebMonitor** Provides a high-level overview of the user console.
Chapter 6	**Miscellaneous** Provides information on topics that do not strictly fall within other chapters.
Chapter 7	**Troubleshooting** Provides all the necessary information on how to deal with any problems encountered while using GFI WebMonitor. Also provides extensive support information.
Chapter 8	**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** that is installed with the product or separately downloadable from the GFI website at http://www.gfi.com/products/gfi-webmonitor/manual.

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.
<Italic text>	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 the built-in download control module and multiple anti-virus and anti-spyware engines.
- **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 about licensing, refer to GFI Software Ltd. website at:

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

For more information on how GFI WebMonitor counts users for licensing purposes, refer to Knowledge Base article:

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

2 About GFI WebMonitor

2.1 How Does GFI WebMonitor Work?

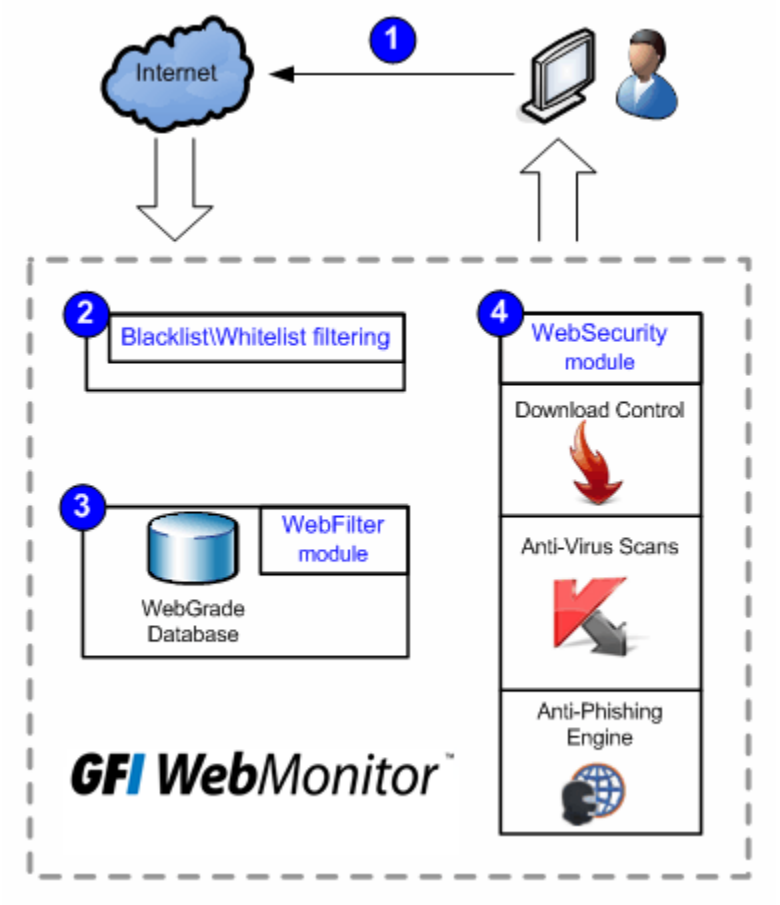


Figure 2 - How does GFI WebMonitor work?

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 the user ID, IP address and requested URLs, taking the following actions:

ACTION	DESCRIPTION
Blocks web traffic requests	» by blacklisted users and/or IP addresses, or » to access blacklisted URLs
Automatically allows web traffic requests	» by whitelisted users and/or IP addresses, or » to access whitelisted URLs
Forwards web traffic requests (to the WebFilter module)	» by users and/or IP addresses that are neither blacklisted nor whitelisted » to access URLs that are neither blacklisted nor whitelisted.

3 **WebFilter module:** Analyzes web traffic received from the blacklist/whitelist filtering mechanism against a list of categories stored in GFI WebMonitor's 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: http://kbase.gfi.com/showarticle.asp?id=KBID003165.

Web traffic is blocked, allowed or quarantined according to configured policies. Quarantined web traffic can be manually approved or rejected by the administrators according to the user's needs and requirements. 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 web traffic 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. Web traffic generated from a known phishing element is rejected while 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 How to Deploy GFI WebMonitor

2.2.1 Introduction

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

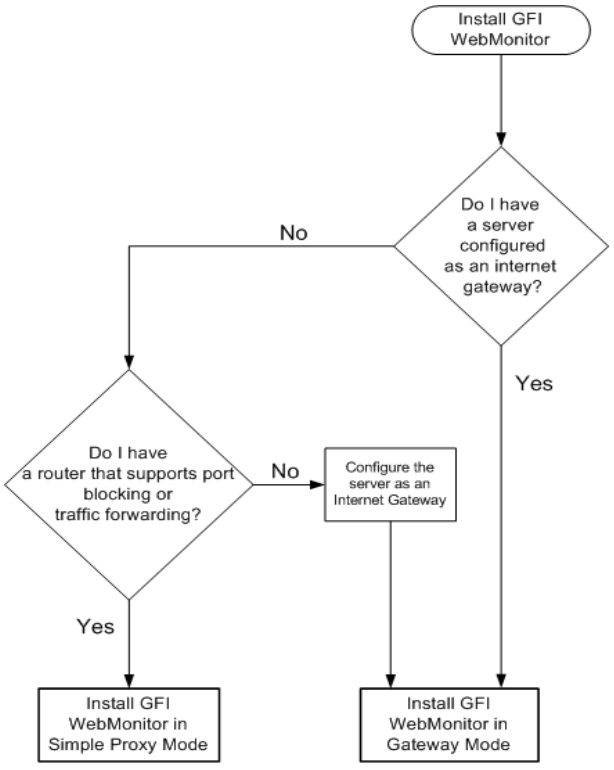


Figure 3 - Choosing your environment flow chart

2.2.2 Internet Gateway Environment

Install GFI WebMonitor in Gateway mode when an internet gateway is used by client machines to access the internet. GFI WebMonitor can be installed on the internet gateway machine to filter and process all outgoing/incoming HTTP/HTTPS traffic generated from/to user machines.

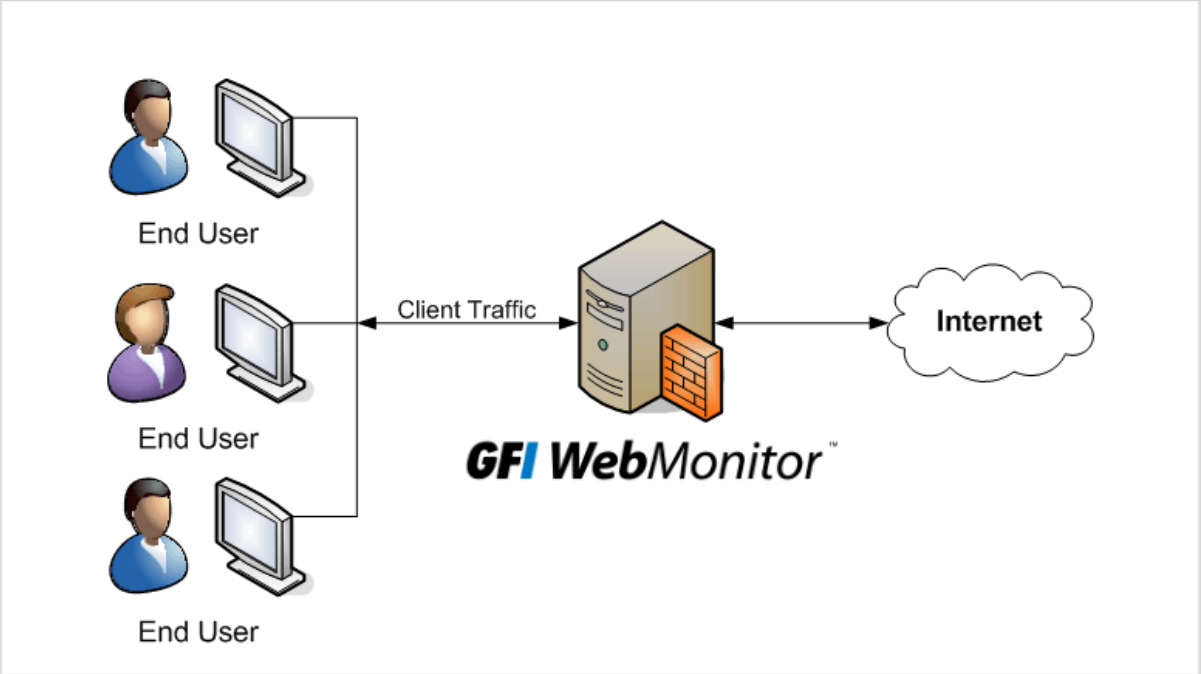


Figure 4 - GFI WebMonitor installed on a gateway machine

To install GFI WebMonitor on an Internet gateway, refer to the Installing in Gateway Mode chapter in this manual.

2.2.3 Simple Proxy Environment

Install GFI WebMonitor in Gateway mode when using a router/gateway for port blocking or traffic forwarding.

Port Blocking

The router/gateway must be configured to allow both HTTP/HTTPS traffic generated from GFI WebMonitor machine and Non-HTTP/HTTPS traffic generated from client machines. In addition, it must also block HTTP/HTTPS traffic generated from client machines.

Client machines must be configured to use the GFI WebMonitor machine as the default proxy server.

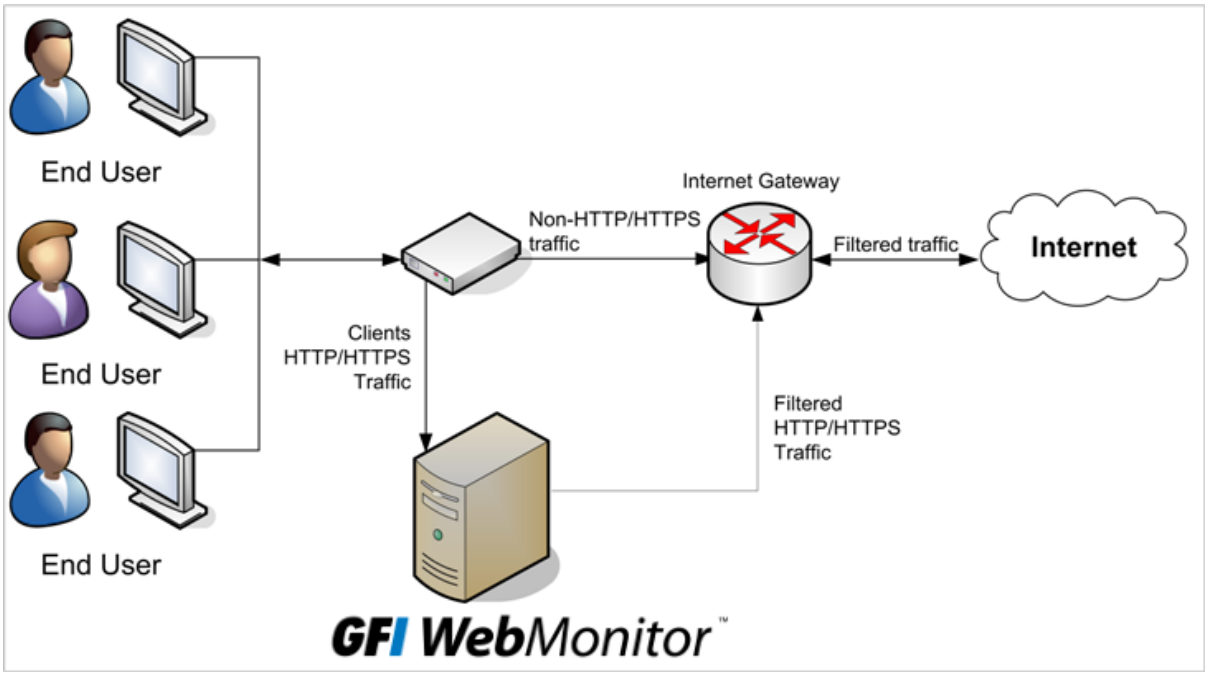


Figure 5 - GFI WebMonitor installed on a proxy machine connected to a router supporting port blocking

Traffic Forwarding

The router/gateway must be configured to allow outgoing web traffic generated by GFI WebMonitor only. In addition, it must forward client HTTP/HTTPS traffic to GFI WebMonitor.

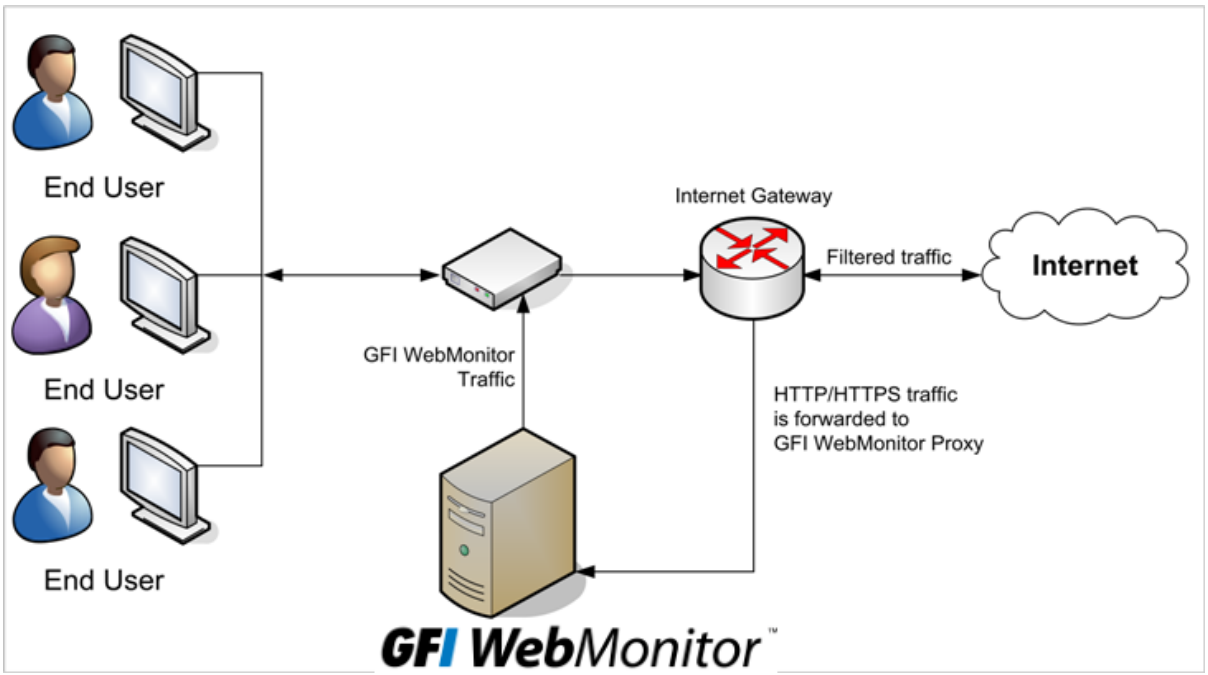


Figure 6 - GFI WebMonitor installed on a proxy machine connected to a router supporting traffic forwarding

To install GFI WebMonitor on a proxy server, refer to the Installing in Simple Proxy Mode chapter in this manual.

3 Installing in Gateway Mode

3.1 Introduction

This chapter provides you with information related to the installation of GFI WebMonitor on a machine configured as an Internet Gateway.

3.2 System Requirements

3.2.1 Software

TYPE	SOFTWARE REQUIREMENTS
Supported Operating Systems	» Microsoft Windows Server 2003 (x86) » Microsoft Windows Server 2008 (x86 or x64) » Microsoft Windows Server 2008 R2 (x64) » Microsoft Windows XP SP2 » Microsoft Windows Vista » Microsoft Windows 7
Other required components	» Microsoft Internet Explorer 7 or later » Microsoft.NET Framework 2.0 » Microsoft Message Queuing Service (MSMQ) » Routing and Remote Access configuration on Microsoft Windows Server 2003/2008 » Microsoft SQL Server 2000 or later (for reporting purposes)

3.2.2 Hardware

Minimum hardware requirements depend on the GFI WebMonitor edition.

EDITION	HARDWARE REQUIREMENTS
All Editions	» Two Network Interface Cards
WebFilter Edition	» Processor: 2.0 GHz » RAM: 1 GB (Recommended 4GB) » Hard disk: 2 GB of available disk space
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

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.

3.3 Installation

3.3.1 Pre-requisites

Before installing GFI WebMonitor on an Internet Gateway Server, ensure that:

1. Client machines are configured to use the server as the default internet gateway.

2. The server's network cards are connected:

» one to the internal network (LAN)

» one to the external network (WAN).

3. Start **Routing and Remote Access** service if installing GFI WebMonitor on Microsoft Windows Server 2003 or Microsoft Windows Server 2008. For more information, refer to the Configuring Routing and Remote Access section in this manual.

4. 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 http://kbase.gfi.com/showarticle.asp?id=KBID003879

3.3.2 Upgrades

In order to upgrade GFI WebMonitor, obtain the latest version from http://www.gfi.com/pages/webmon-selection-download.asp. The upgrade procedure is similar to the installation procedure. For more information, refer to the Installation Procedure section in this chapter.

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.

3.3.3 Installation Procedure

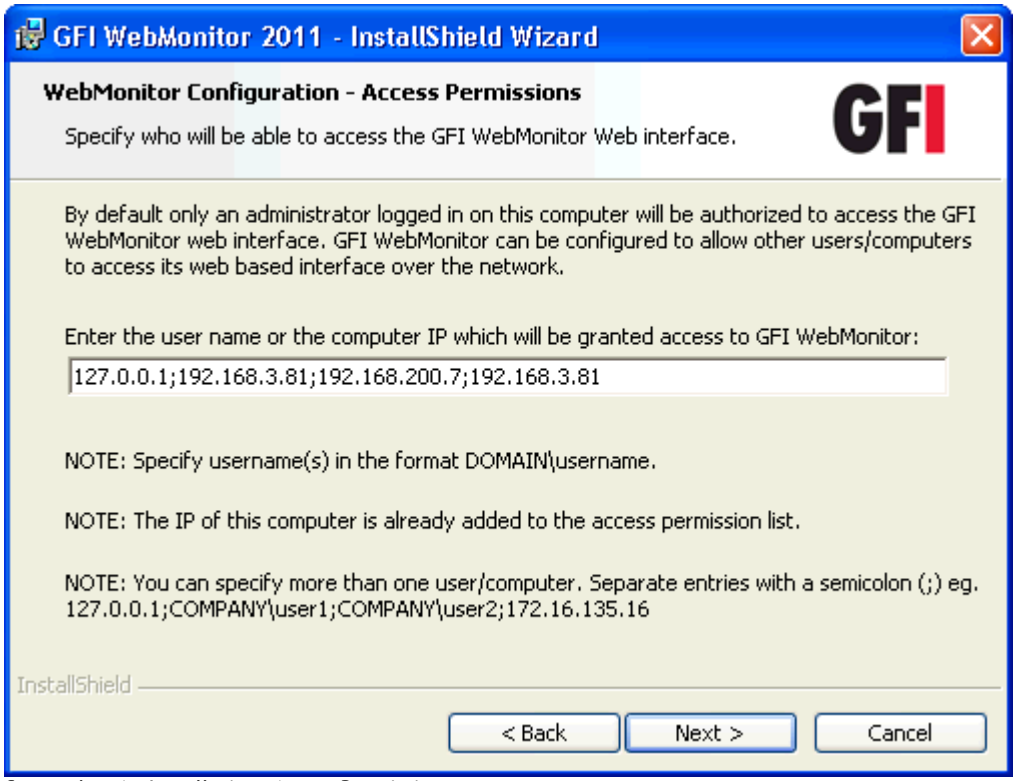
Run the installer as a user with administrative privileges on the target machine.

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**.

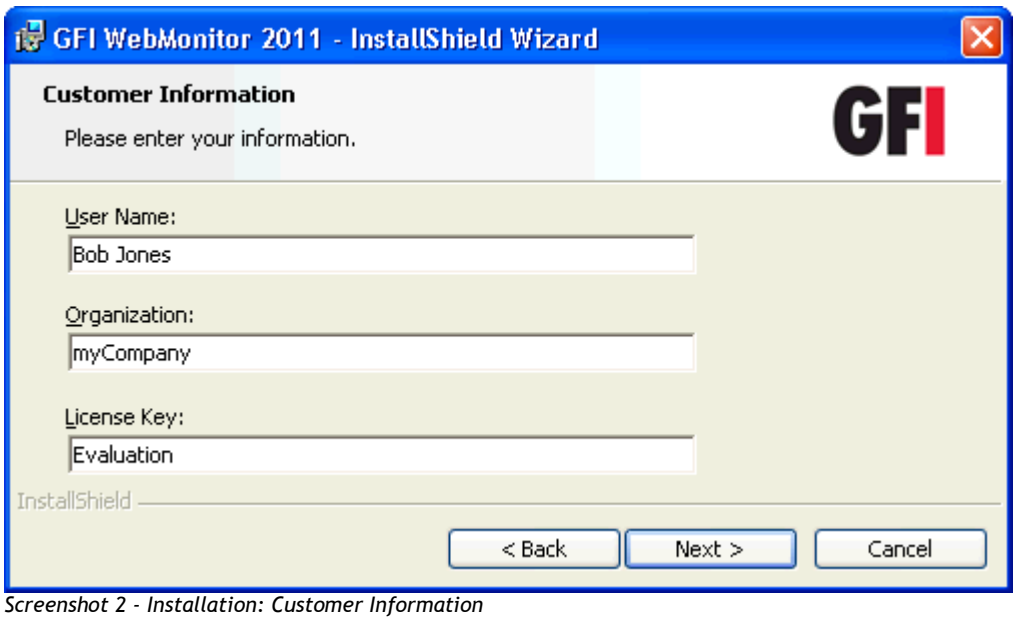
4. Read the licensing agreement. To proceed with the installation select **I accept the terms in the license agreement** and click **Next**.



Screenshot 1 - Installation: Access Permissions

5. Key in the user name or the IP address that 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

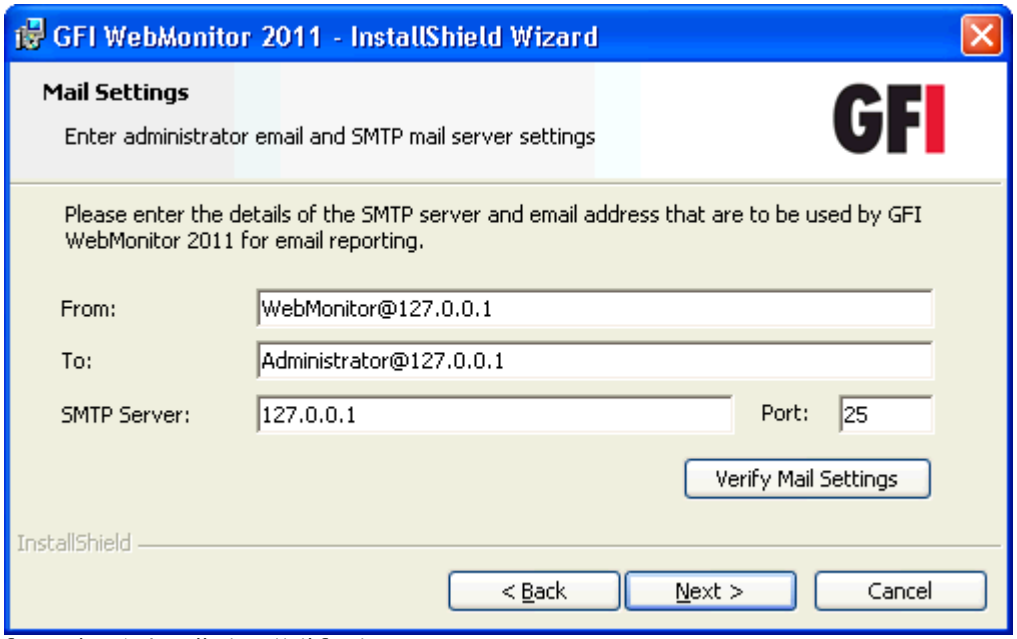
6. Key in the **User Name** and **Organization**. If you have a license key, update the **License Key** details and click **Next**.

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 this manual.

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 this manual.



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. If the Microsoft Message Queuing Service (MSMQ) is not installed, a message will prompt the user that the installation requirements have not been met. Click **Next** to install the service automatically.

11. Click **Install** to start the installation, and wait for the installation to complete.

12. Click **Finish** to finalize setup.

13. After the installation, **GFI WebMonitor Configuration Wizard** is launched automatically. This will help you configure the server in gateway mode.

14. In the welcome screen, click **Next**.

15. Select **Gateway mode** as your network environment and click **Next**.

16. In the **Current Gateway Configuration** screen, select the internal network card and click **Next**.

17. Click **Finish** to apply settings.

3.3.4 Launching GFI WebMonitor

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

- **Option 1:** click **Start ► Programs ► GFI WebMonitor ► GFI WebMonitor.** Further information can be found in the section entitled Launching GFI WebMonitor in this document.
- **Option 2:** Key in the URL http://monitor.isa in a web browser on the same machine.

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 Microsoft Internet Explorer section in this manual.

To launch GFI WebMonitor installation from machines of users and/or IP addresses that were allowed access to the application during installation:

- 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.

3.4 Post-installation Actions: Configure Proxy Settings

Configure the user machines to use GFI WebMonitor machine as the default proxy. This can be achieved by:

- **Option 1:** Configuring the client machines using the Group Policy object (GPO) feature within the Active Directory.
- **Option 2:** Configuring Internet browsers to use specific proxy settings on each client machine manually.

The client internet browser can be configured to detect the proxy settings automatically. This is possible if WPAD is enabled in GFI WebMonitor proxy settings. For more information, refer to the Enabling WPAD in Proxy Settings section in this manual.

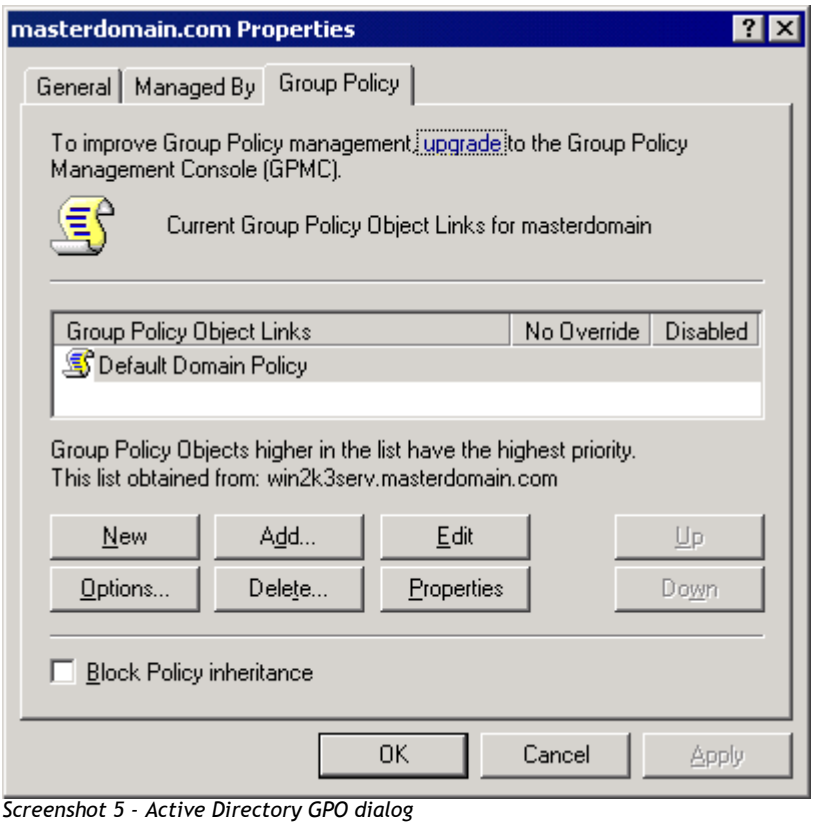
3.4.1 Configuring GFI WebMonitor Machine as the Default Proxy Using GPO in Microsoft Windows Server 2003

To configure the **Proxy Settings** on all client machines to use GFI WebMonitor as a proxy server through Microsoft Windows Server 2003 GPO:

1. Navigate to **Start ► Programs ► Administrative Tools ► Active Directory Users and Computers** on the Domain Controller.

2. Under the domain node, right-click the organizational unit where you wish to apply the group policy and click **Properties**.

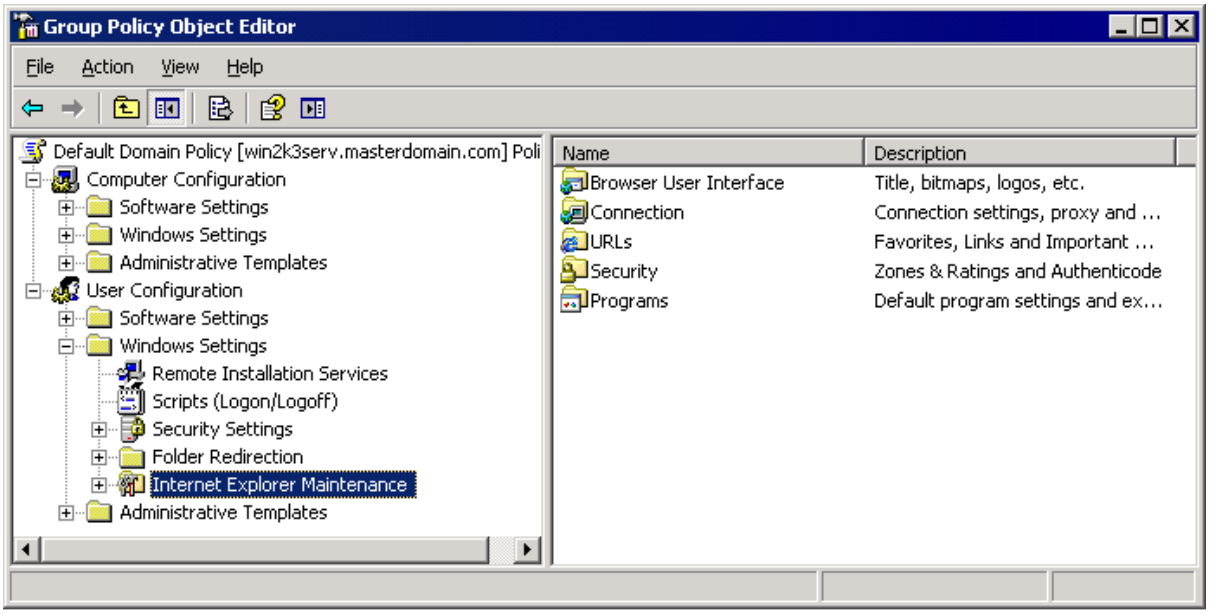
To apply the group policy to all the computers on the domain, right-click on the domain node directly and click **Properties**.



Screenshot 5 - Active Directory GPO dialog

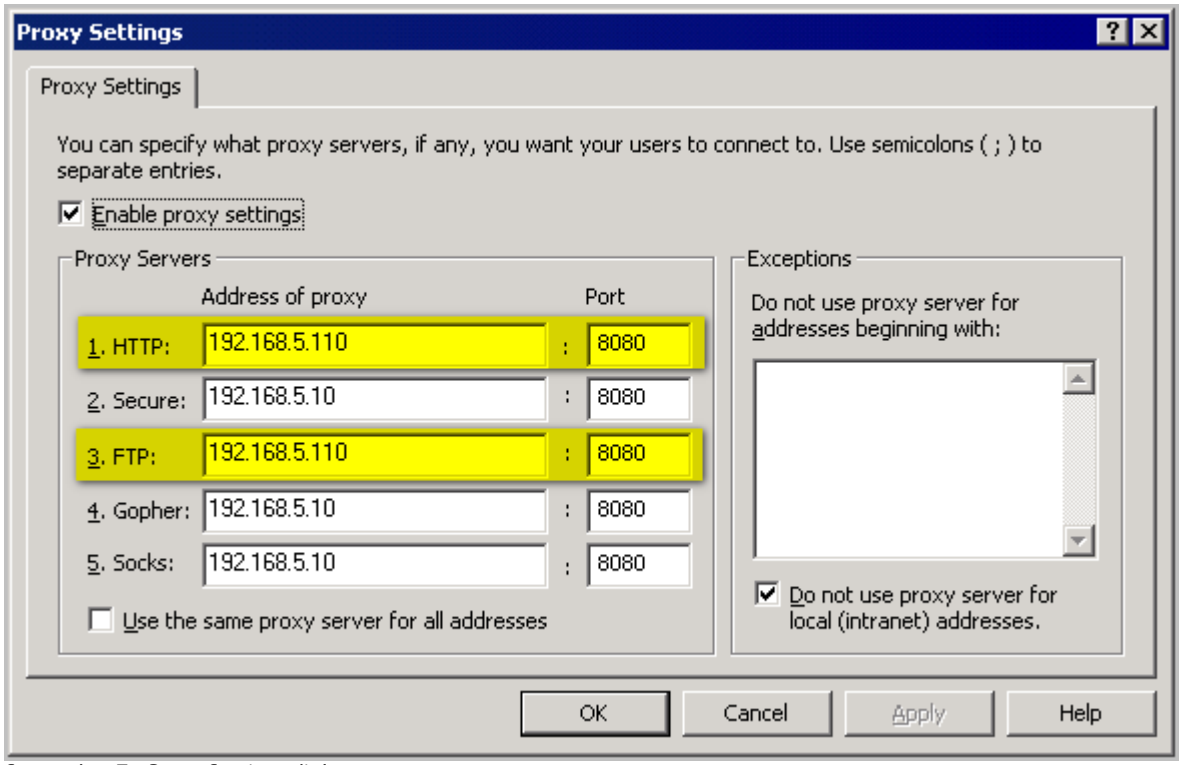
3. Select **Group Policy** tab in the **Domain Properties** dialog.

4. Select **Default Domain Policy** from the list and click **Edit**.



Screenshot 6 - GPO Editor window

5. Expand **User Configuration** ► **Windows Settings** ► **Internet Explorer Maintenance** ► **Connection** and double-click **Proxy Settings** to open the **Proxy Settings** dialog.



Screenshot 7 - Proxy Settings dialog

6. Check **Enable proxy settings** checkbox.

7. Uncheck **Use the same proxy server for all addresses** checkbox.

8. Key in the proxy server IP address and the port used (Default 8080) in the **HTTP** and **FTP** text boxes.

9. Click **OK** to apply changes.

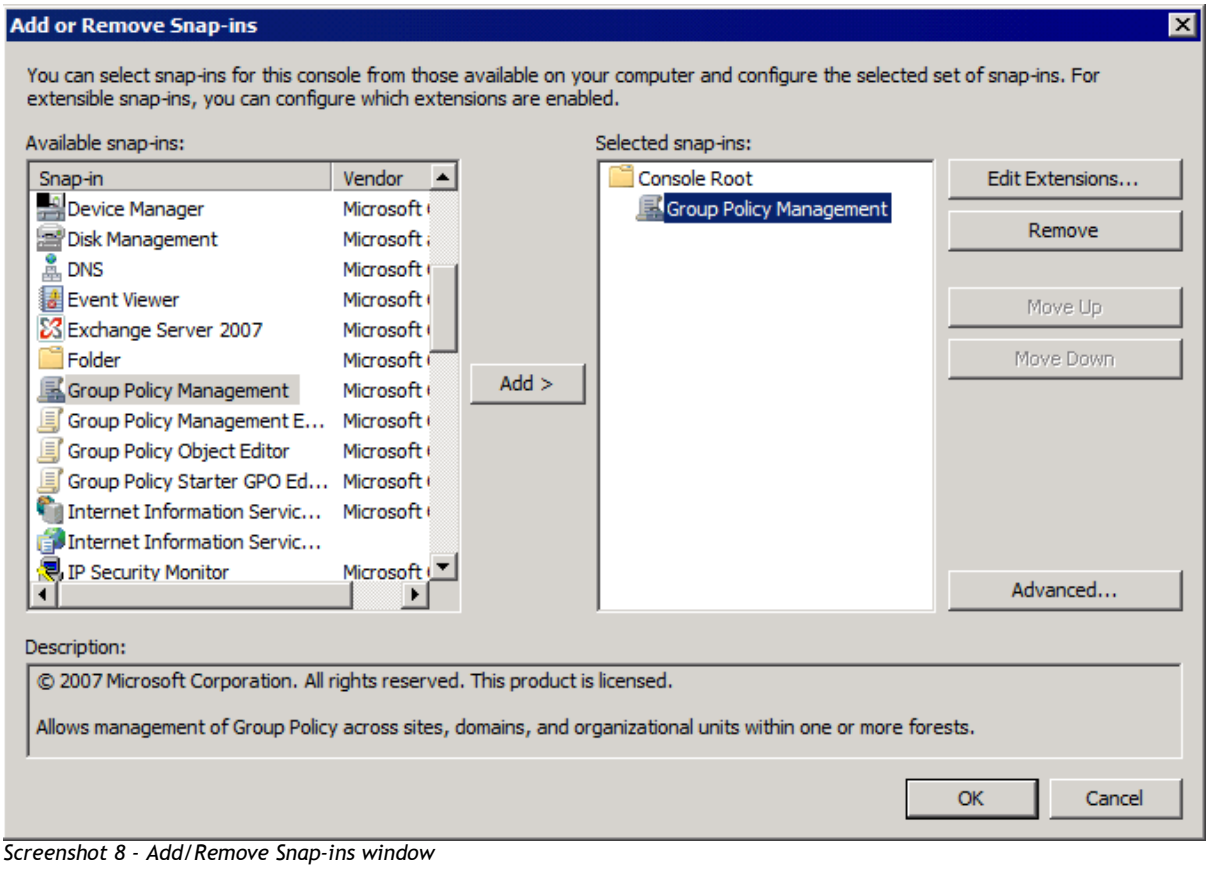
10. Close all open windows.

3.4.2 Configuring GFI WebMonitor Machine as the Default Proxy Using GPO in Microsoft Windows Server 2008

To configure the **Proxy Settings** on all client machines to use GFI WebMonitor as a proxy server through Microsoft Windows Server 2008 GPO:

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

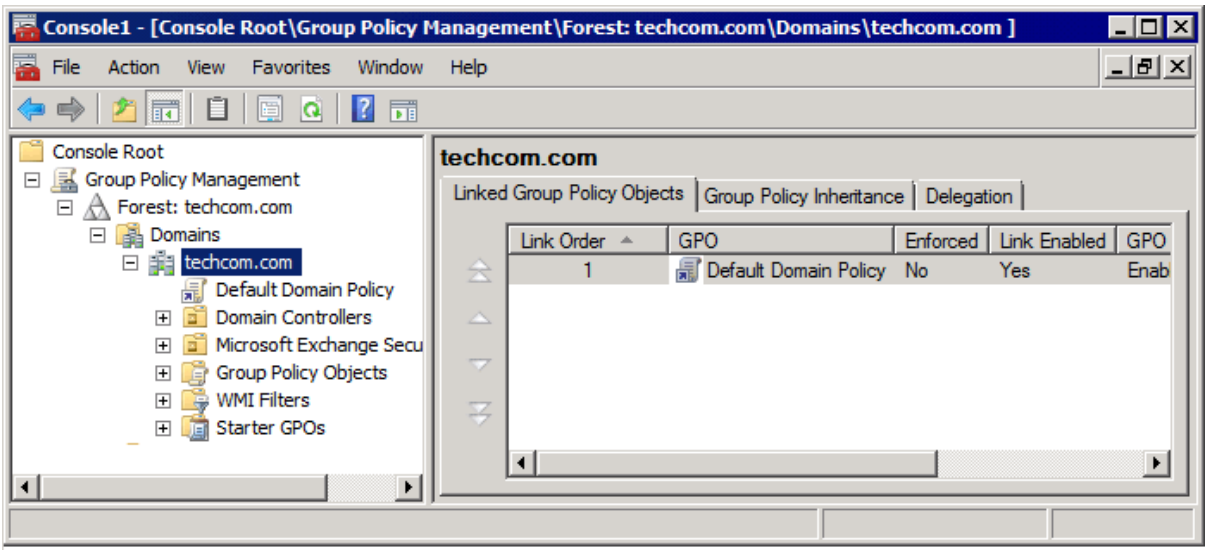
2. In the **Console Root** window, navigate to **File ► Add/Remove Snap-in…** to open the **Add or Remove Snap-ins** window.



Screenshot 8 - Add/Remove Snap-ins window

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

4. Click **OK**.

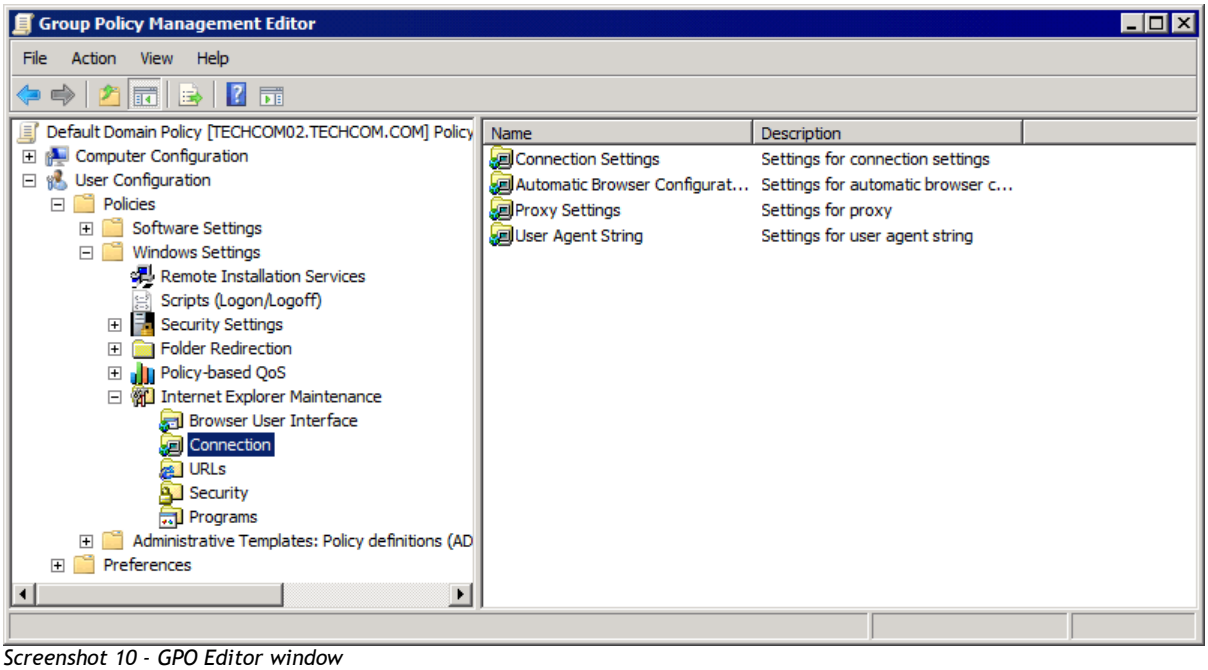


Screenshot 9 - Console Root domain window

5. Expand **Group Policy Management ► Forest ► Domains** and **<domain>,** then select the organizational unit where you wish to apply the group policy.

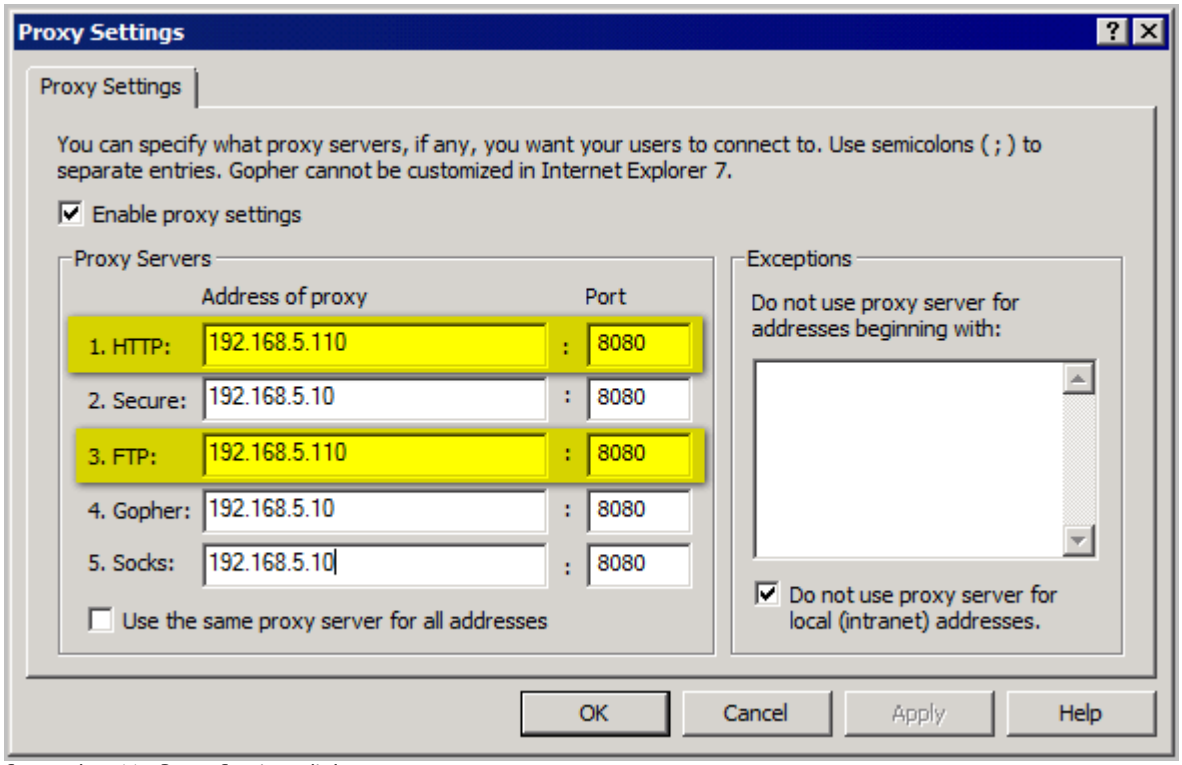
To apply the group policy to all the computers on the domain, select the domain node directly.

6. Right-click **Default Domain Policy** and click **Edit** to open the **Group Policy Management Editor**.



Screenshot 10 - GPO Editor window

7. Expand **User Configuration ► Policies ► Windows Settings ► Internet Explorer Maintenance ► Connection** and double-click **Proxy Settings** to open the **Proxy Settings** dialog.



Screenshot 11 - Proxy Settings dialog

8. Check **Enable proxy settings** checkbox.

9. Uncheck **Use the same proxy server for all addresses** checkbox.

10. Key in the proxy server IP address and the port used (Default 8080) in the **HTTP** and **FTP** text boxes.

11. Click **OK** to apply changes

12. Close **Proxy Settings** dialog.

13. Close **Group Policy Management Editor** dialog and save the management console.

When using Active Directory, the administrator can disable the Internet connection settings tab from the client machines. For more information, refer to the Disabling Internet Connections Settings on Client Machines section in this manual.

3.4.3 Configuring Internet Browsers to Use a Proxy Server

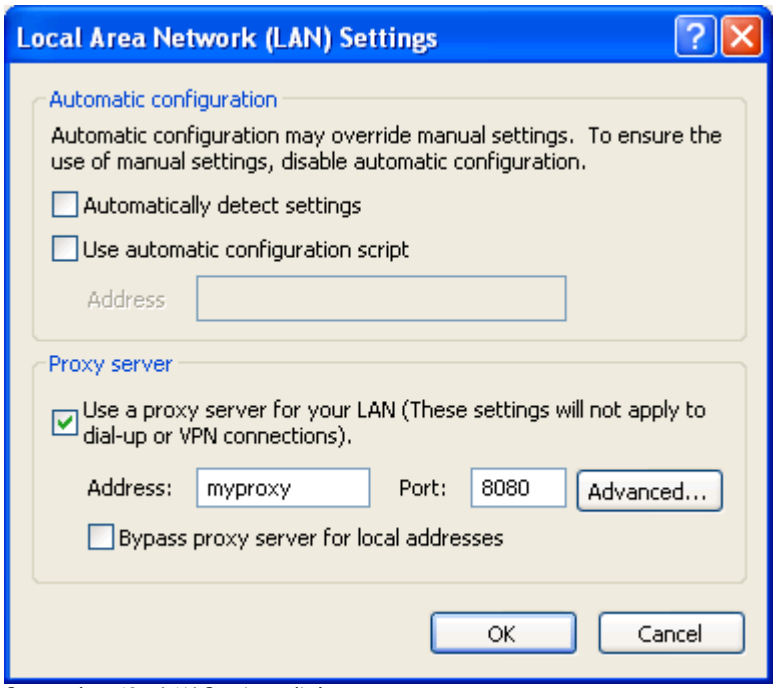
You can also configure each individual user machine manually to set the GFI WebMonitor machine as the default proxy. This section shows how to configure proxy settings in the most commonly used internet browsers.

Microsoft Internet Explorer

1. Launch **Microsoft Internet Explorer**.

2. From the **Tools** menu, choose **Internet Options** and select the **Connections** tab.

3. Click **LAN settings** button.



Screenshot 12 - LAN Settings dialog

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

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

If WPAD is enabled in GFI WebMonitor proxy settings check the **Automatically detect settings** checkbox in the **Automatic configuration** area. For more information, refer to the Enabling WPAD in Proxy Settings section in this manual.

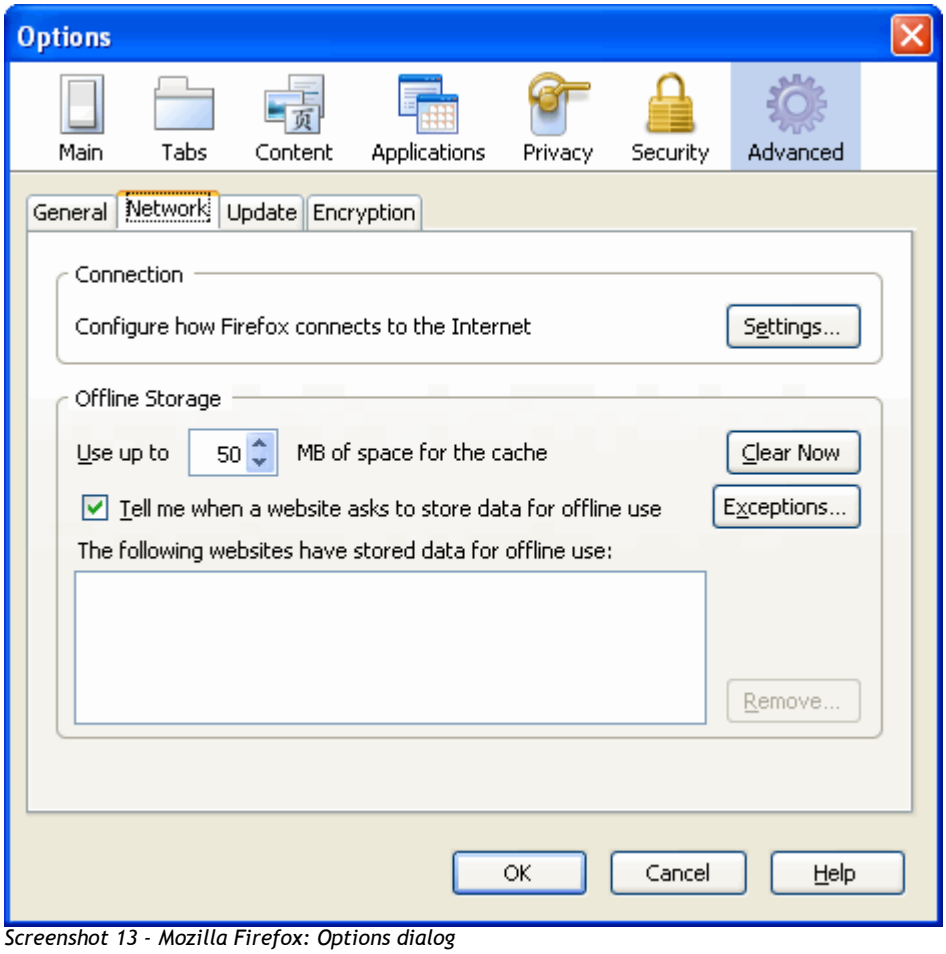
6. Click **OK** to close **LAN Settings** dialog.

7. Click **OK** to close **Internet Options** dialog.

Mozilla Firefox

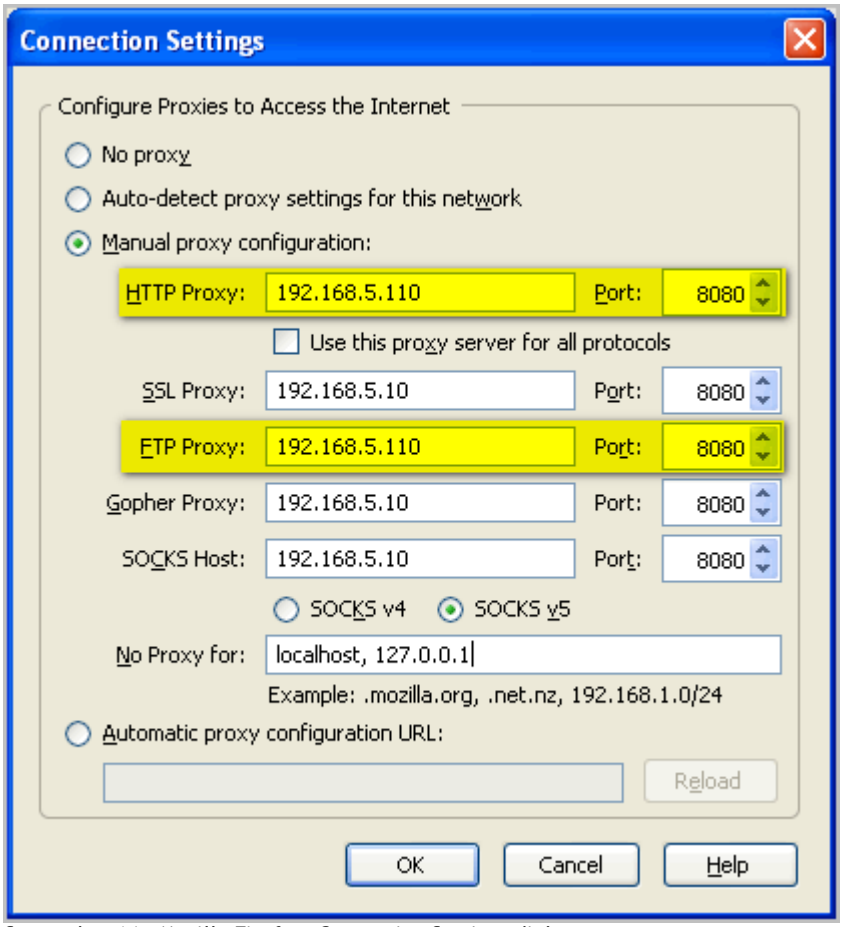
1. Launch **Mozilla Firefox**.

2. Click **Tools** ► **Options** ► **Advanced** tab ► **Network** tab.



Screenshot 13 - Mozilla Firefox: Options dialog

3. Click **Settings button** to open the **Connection Settings** dialog.



Screenshot 14 - Mozilla Firefox: Connection Settings dialog

4. Select **Manual proxy configuration**.

5. Uncheck **Use this proxy server for all protocols** checkbox.

6. Key in the proxy server IP address and the port used (Default 8080) in the **HTTP Proxy**, **FTP Proxy** and related **Port** text boxes.

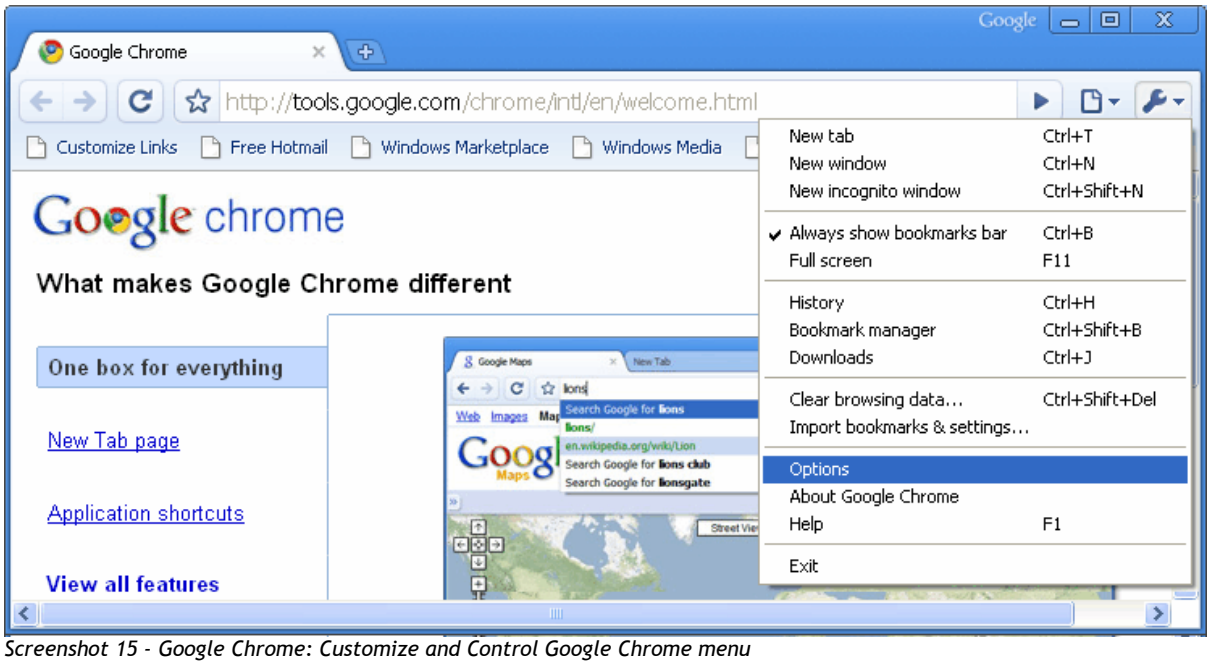
If WPAD is enabled in GFI WebMonitor proxy settings, select **Auto-detect proxy settings for this network**. For more information, refer to the Enabling WPAD in Proxy Settings section in this manual.

7. Click **OK** to close **Connection Settings** dialog.

8. Click **OK** to close **Options** dialog.

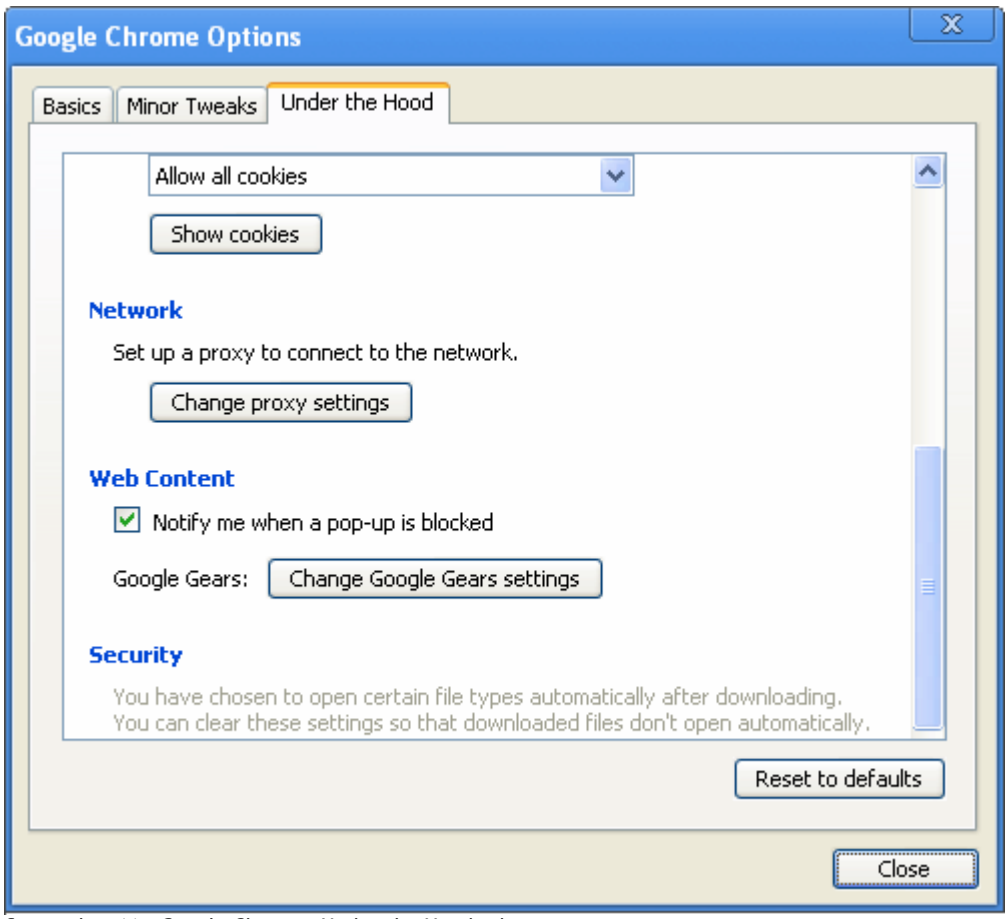
Google Chrome

1. Launch **Google Chrome**.



Screenshot 15 - Google Chrome: Customize and Control Google Chrome menu

2. Click **Customize and Control Google Chrome ► Options**.



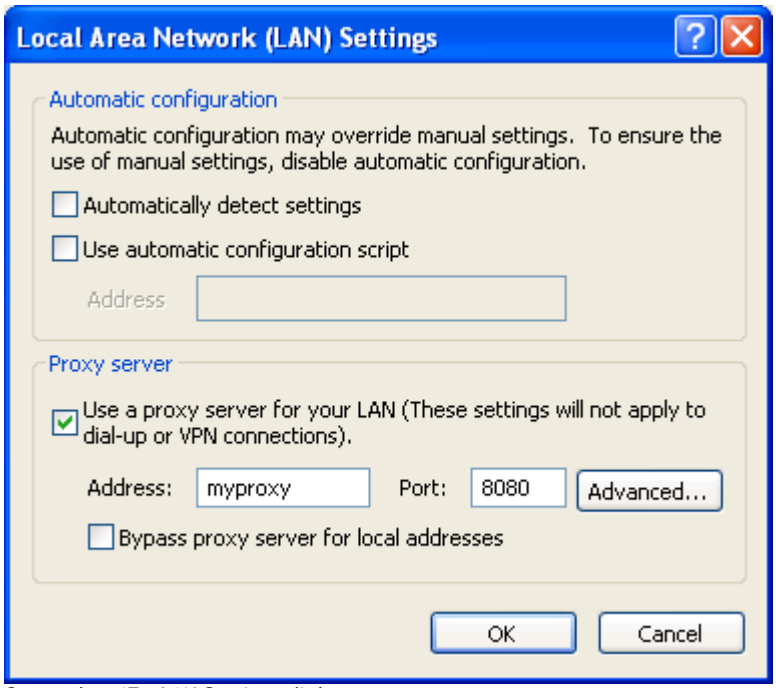
Screenshot 16 - Google Chrome: Under the Hood tab

3. In the **Google Chrome Options** dialog, click **Under the Hood** tab.

4. Click **Change proxy settings** button to open **Internet Properties** dialog.

5. Select the **Connections** tab.

6. Click **LAN settings** button.



Screenshot 17 - LAN Settings dialog

7. Check **Use a proxy server for your LAN** checkbox.

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

If WPAD is enabled in GFI WebMonitor proxy settings check the **Automatically detect settings** checkbox in the **Automatic configuration** area. For more information, refer to the Enabling WPAD in Proxy Settings section in this manual.

9. Click **OK** to close **LAN Settings** dialog.

10. Click **OK** to close **Internet Options** dialog.

4 Installing in Simple Proxy Mode

4.1 Introduction

This chapter provides you with information related to the installation of GFI WebMonitor on a machine configured as a Proxy server.

4.2 System Requirements

4.2.1 Software

GFI WebMonitor in Simple Proxy mode can be installed on:

TYPE	SOFTWARE REQUIREMENTS
Supported Operating Systems	» Microsoft Windows Server 2003 (x86) » Microsoft Windows Server 2008 (x86 or x64) » Microsoft Windows Server 2008 R2 (x64) » Microsoft Windows XP SP2 » Microsoft Windows Vista » Microsoft Windows 7
Other required components	» Microsoft Internet Explorer 7 or later » Microsoft.NET Framework 2.0 » Microsoft Message Queuing Service (MSMQ) » Microsoft SQL Server 2000 or later (for reporting purposes)

4.2.2 Hardware

Minimum hardware requirements depend on the GFI WebMonitor edition.

EDITION	HARDWARE REQUIREMENTS
All Editions	» Router/gateway that supports traffic forwarding or port blocking
WebFilter Edition	» Processor: 2.0 GHz » RAM: 1 GB (Recommended 4GB) » Hard disk: 2 GB of available disk space
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

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.

4.3 Installation

4.3.1 Pre-requisites

Before installing GFI WebMonitor on a Proxy server, the router/gateway must be configured to:

» Block all outgoing HTTP/HTTPS traffic generated from the client machines

» Allow outgoing HTTP/HTTPS traffic generated by GFI WebMonitor only

» Allow Non-HTTP/HTTPS traffic generated from client machines.

In this environment, traffic forwarding can be used to forward HTTP/HTTPS traffic from the client machines to GFI WebMonitor machine. For more information, refer to the Configuring Commonly Used Routers section in this manual.

4. 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 http://kbase.gfi.com/showarticle.asp?id=KBID003879

4.3.2 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.

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

4.3.3 Installation Procedure

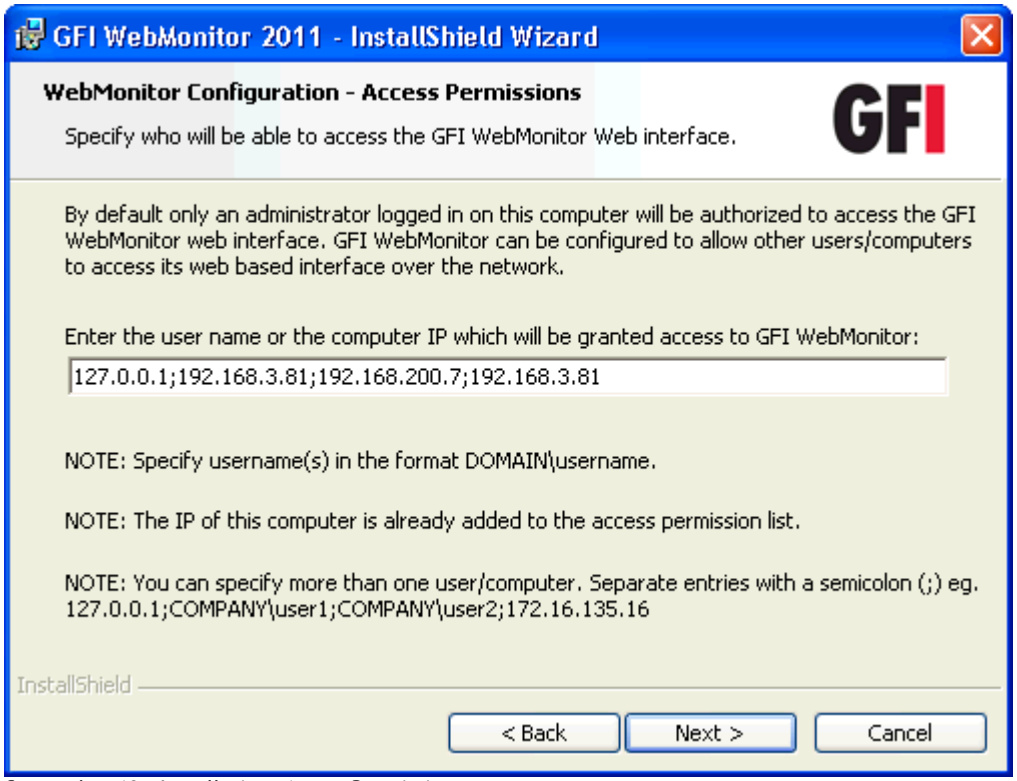
Run the installer as a user with administrative privileges on the target machine.

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**.

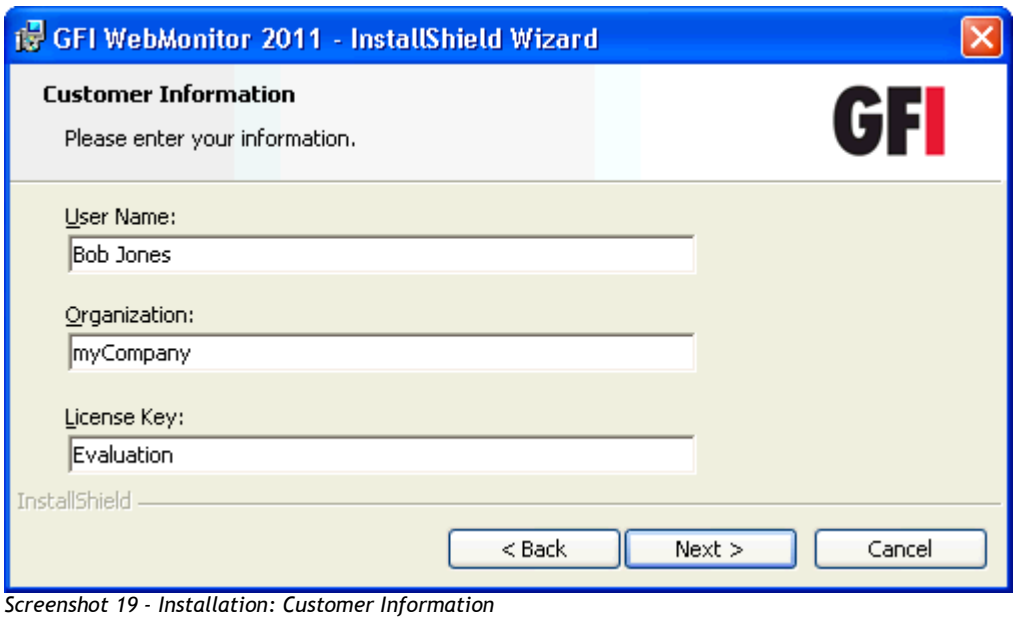
4. Read the licensing agreement. To proceed with the installation select **I accept the terms in the license agreement** and click **Next**.



Screenshot 18 - 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**.

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



Screenshot 19 - Installation: Customer Information

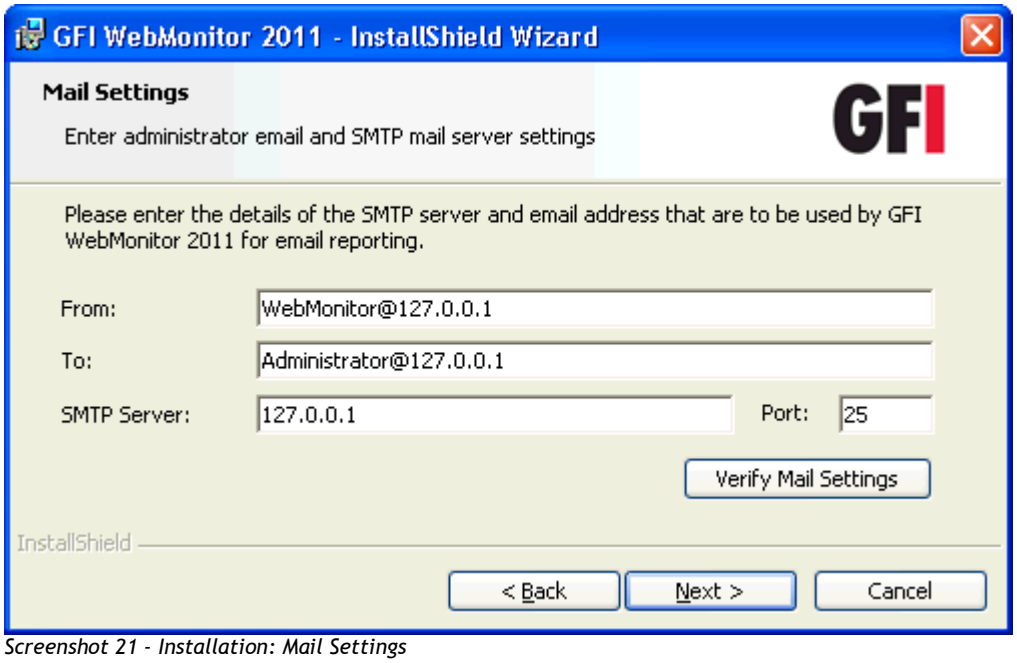
6. Key in the **User Name** and **Organization**. If you have a license key, update the **License Key** details and click **Next**.

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 this manual.

Screenshot 20 - 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. For more information, refer to the Assigning Log On As A Service Rights section in this manual.



Screenshot 21 - Installation: Mail Settings

8. Provide the SMTP mail server details and email address to which administrator notifications will be sent. Select **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. If the Microsoft Message Queuing Service (MSMQ) is not installed, a message will prompt the user that the installation requirements have not been met. Click **Next** to install the service automatically.

11. Click **Install** to start the installation and wait for the installation to complete.

12. Click **Finish**.

13. After the installation, **GFI WebMonitor Configuration Wizard** is launched automatically. This will help you configure the server in simple proxy mode.

14. In the welcome screen, click **Next**.

15. Select **Simple proxy mode** as your network environment and click **Next**.

To view help on how to configure most commonly used routers, select the **Click here** link. For more information, refer to the Configuring Commonly Used Routers section in this manual.

16. Click **Finish** to apply proxy settings.

4.3.4 Post-installation Test

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

» **Option 1**: Click **Start** ► **Programs** ► **GFI WebMonitor** ► **GFI WebMonitor**. Further information can be found in the section entitled Launching GFI WebMonitor in this document.

» **Option 2**: Key in the URL http://monitor.isa in a web browser on the same machine.

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 Microsoft Internet Explorer section in this manual.

To test GFI WebMonitor installation from machines of users and/or IP addresses that were allowed access to the application during installation:

» 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.

4.4 Post-installation Actions: Configure Proxy Settings

Configure the user machines to use GFI WebMonitor machine as the default proxy. This can be achieved by:

» **Option 1:** Configuring the client machines using the Group Policy object (GPO) feature within the Active Directory.

» **Option 2**: Configuring Internet browsers to use specific proxy settings on each client machine manually.

If WPAD is enabled, the client internet browser can be configured to detect the proxy settings automatically. For more information, refer to the Enabling WPAD in Proxy Settings section in this manual.

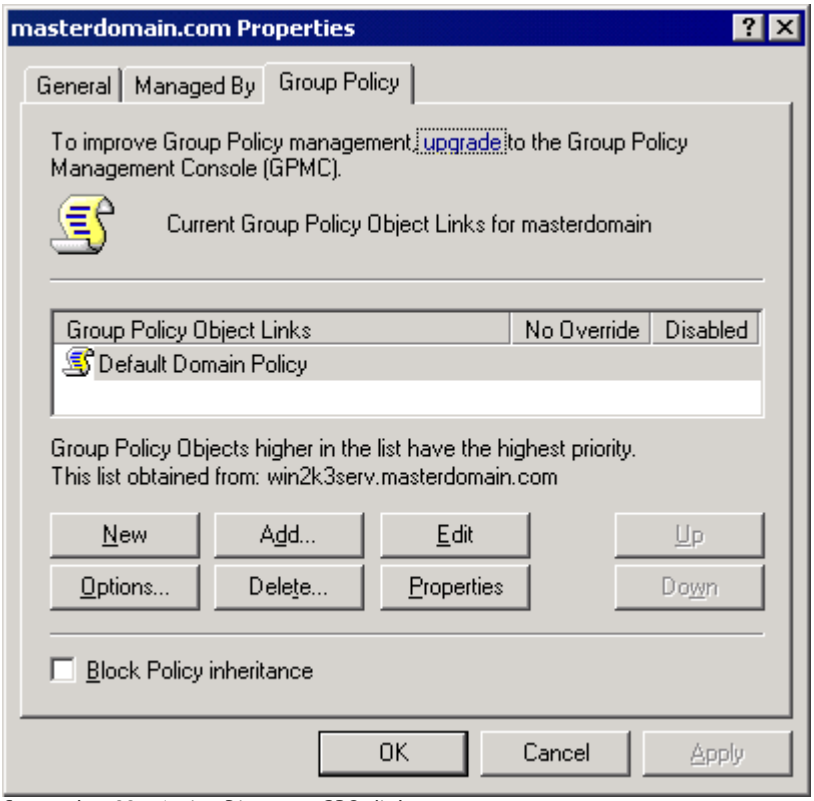
4.4.1 Configuring GFI WebMonitor Machine as the Default Proxy Using GPO in Microsoft Windows Server 2003

To configure the **Proxy Settings** on all client machines to use GFI WebMonitor as a proxy server through Microsoft Windows Server 2003 GPO:

1. Navigate to **Start** ► **Programs** ► **Administrative Tools** ► **Active Directory Users and Computers** on the Domain Controller.

2. Under the domain node, right-click the organizational unit where you wish to apply the group policy and click **Properties**.

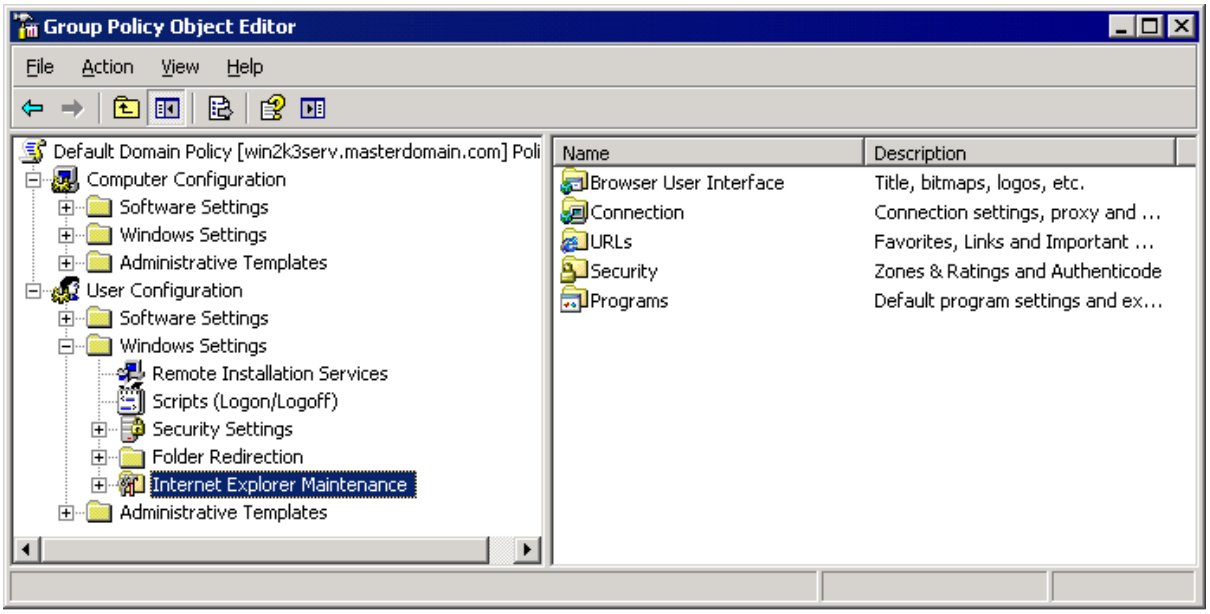
to apply the group policy to all the computers on the domain, right-click on the domain node directly and click **Properties**.



Screenshot 22 - Active Directory GPO dialog

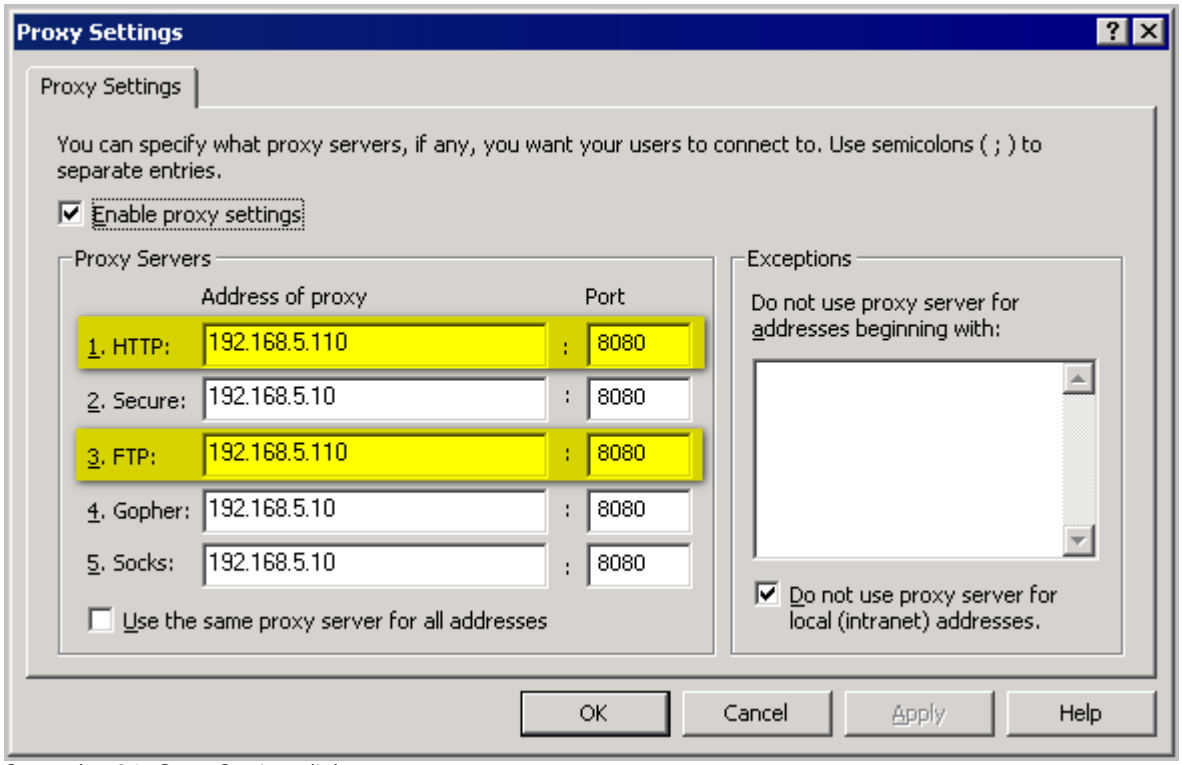
3. Select **Group Policy** tab in the **Domain Properties** dialog.

4. Select **Default Domain Policy** from the list and click **Edit**.



Screenshot 23 - GPO Editor window

5. Expand **User Configuration ► Windows Settings ► Internet Explorer Maintenance ► Connection** and double-click **Proxy Settings** to open the **Proxy Settings** dialog.



Screenshot 24 - Proxy Settings dialog

6. Check **Enable proxy settings** checkbox.

7. Uncheck **Use the same proxy server for all addresses** checkbox.

8. Key in the proxy server IP address and the port used (Default 8080) in the **HTTP** and **FTP** text boxes.

9. Click **OK** to apply changes.

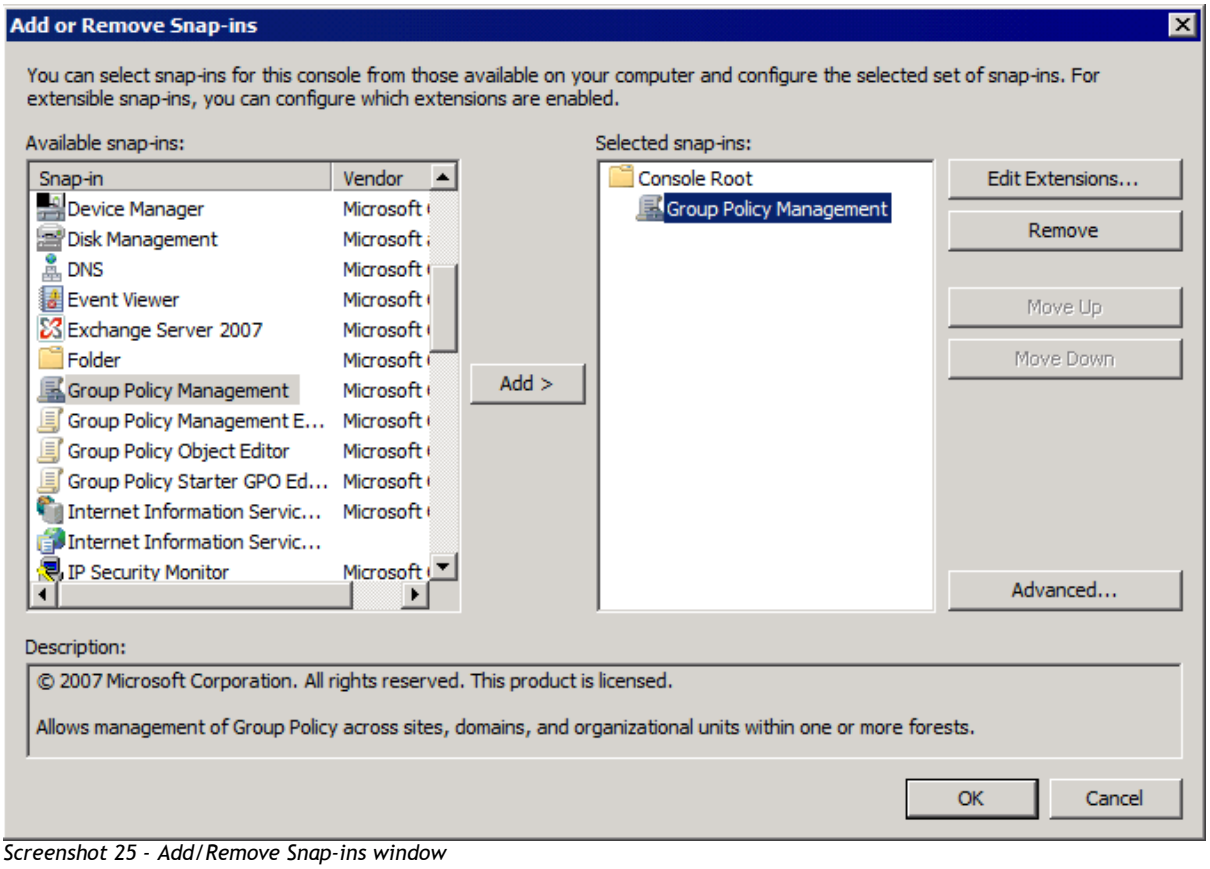
10. Close all open windows.

4.4.2 Configuring GFI WebMonitor Machine as the Default Proxy Using GPO in Microsoft Windows Server 2008

To configure the **Proxy Settings** on all client machines to use GFI WebMonitor as a proxy server through Microsoft Windows Server 2008 GPO:

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

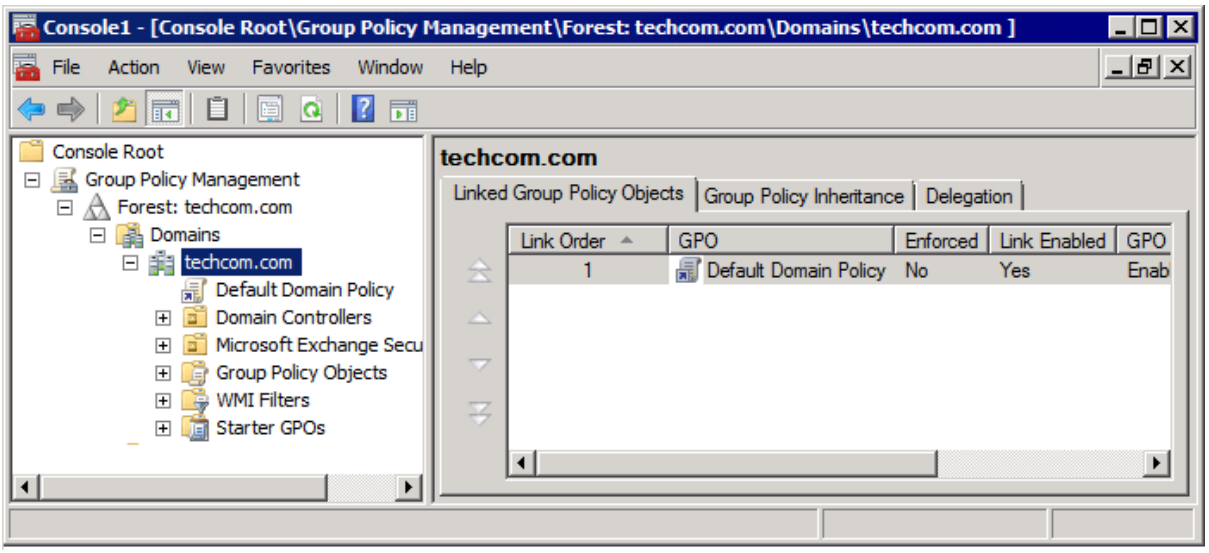
2. In the **Console Root** window, navigate to **File ► Add/Remove Snap-in…** to open the **Add or Remove Snap-ins** window.



Screenshot 25 - Add/Remove Snap-ins window

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

4. Click **OK**.

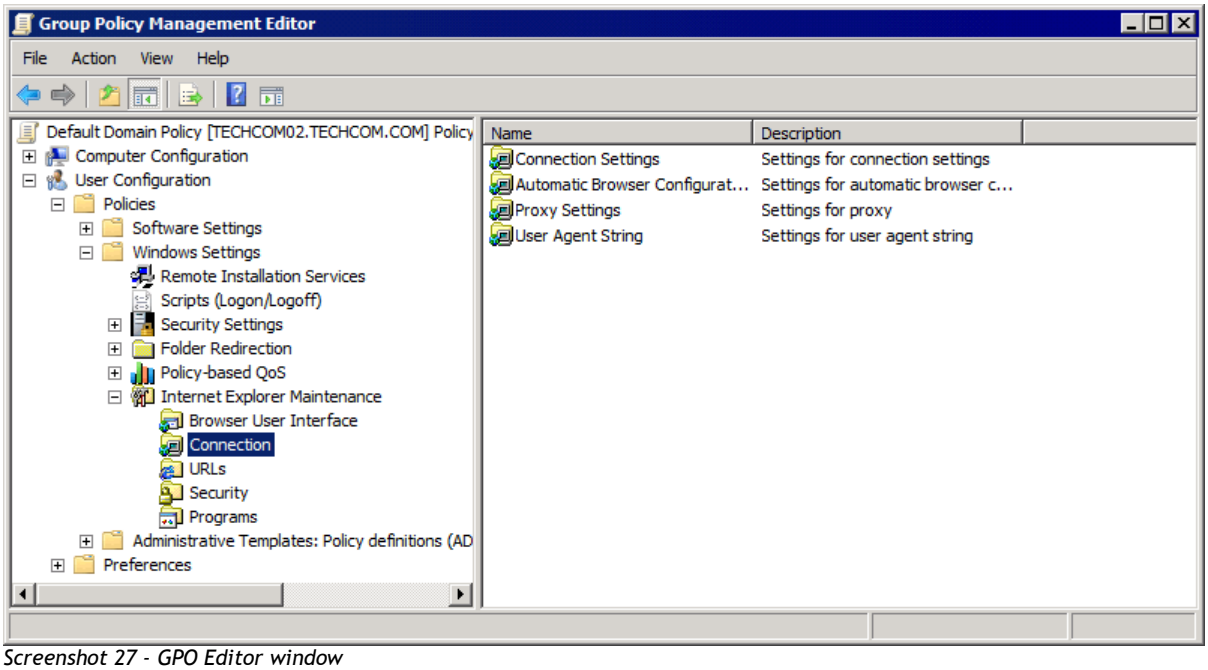


Screenshot 26 - Console Root domain window

5. Expand **Group Policy Management ► Forest ► Domains** and **<domain>**, then select the organizational unit where you wish to apply the group policy.

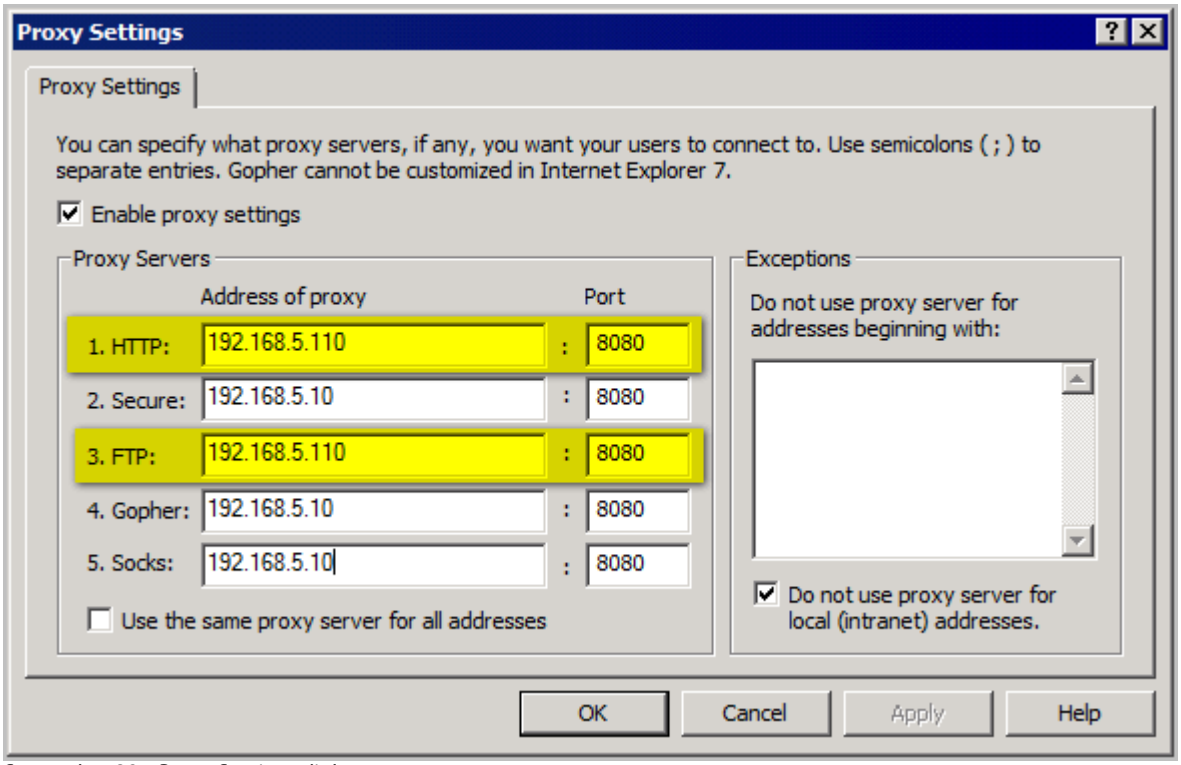
To apply the group policy to all the computers on the domain, select the domain node directly.

6. Right-click **Default Domain Policy** and click **Edit** to open the **Group Policy Management Editor**.



Screenshot 27 - GPO Editor window

7. Expand **User Configuration ► Policies ► Windows Settings ► Internet Explorer Maintenance ► Connection** and double-click **Proxy Settings** to open the **Proxy Settings** dialog.



Screenshot 28 - Proxy Settings dialog

8. Check **Enable proxy settings** checkbox.

9. Uncheck **Use the same proxy server for all addresses** checkbox.

10. Key in the proxy server IP address and the port used (Default 8080) in the **HTTP** and **FTP** text boxes.

11. Click **OK** to apply changes

12. Close **Proxy Settings** dialog.

13. Close **Group Policy Management Editor** dialog and save the management console created.

When using Active Directory, the administrator can disable the Internet connection settings tab from the client machines. For more information, refer to the Disabling Internet Connections Settings on Client Machines section in this manual.

4.4.3 Configuring Internet Browsers to Use a Proxy Server

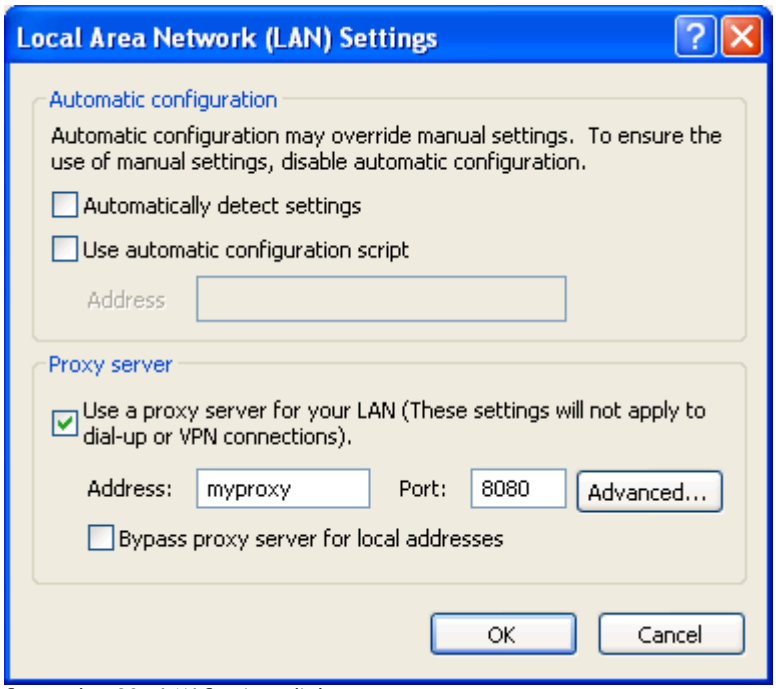
You can also configure each individual user machine manually to set the GFI WebMonitor machine as the default proxy. This section shows how to configure the most commonly used Internet browsers to use a proxy server.

Microsoft Internet Explorer

1. Launch **Microsoft Internet Explorer**.

2. From the **Tools** menu, choose **Internet Options** and select the **Connections** tab.

3. Click **LAN settings** button.



Screenshot 29 - LAN Settings dialog

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

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

If WPAD is enabled in GFI WebMonitor proxy settings check the **Automatically detect settings** checkbox in the **Automatic configuration** area. For more information, refer to the Enabling WPAD in Proxy Settings section in this manual.

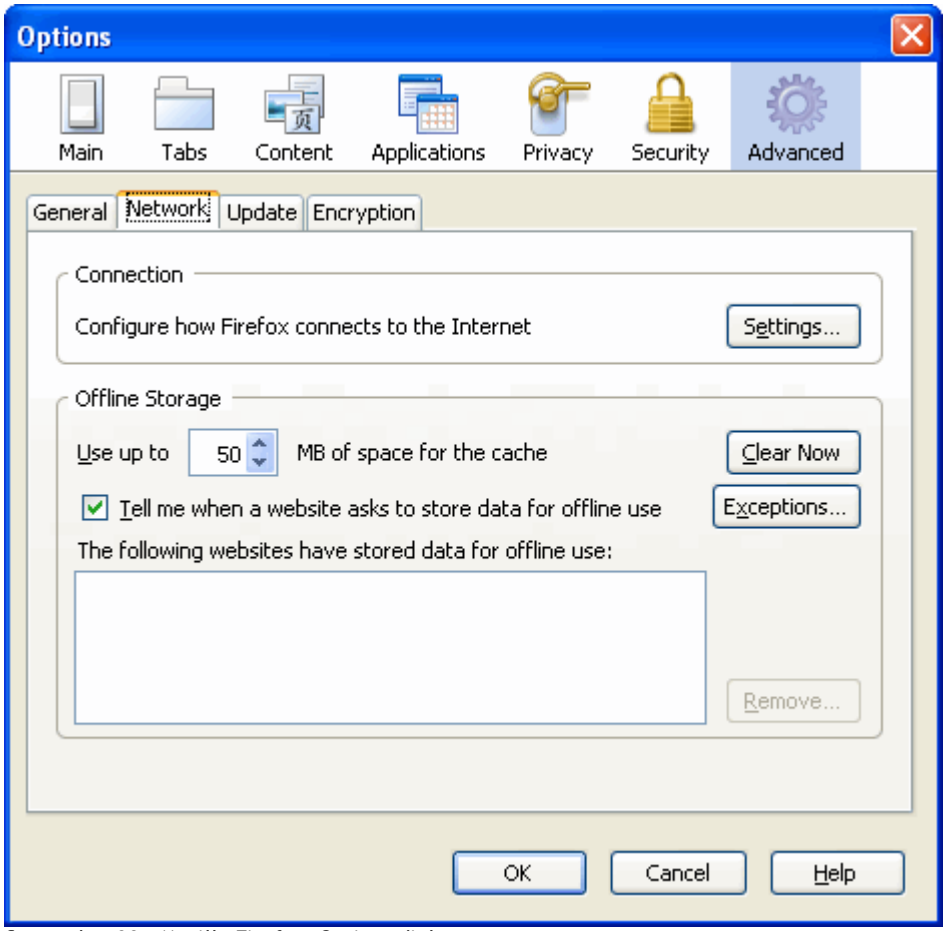
6. Click **OK** to close **LAN Settings** dialog.

7. Click **OK** to close **Internet Options** dialog.

Mozilla Firefox

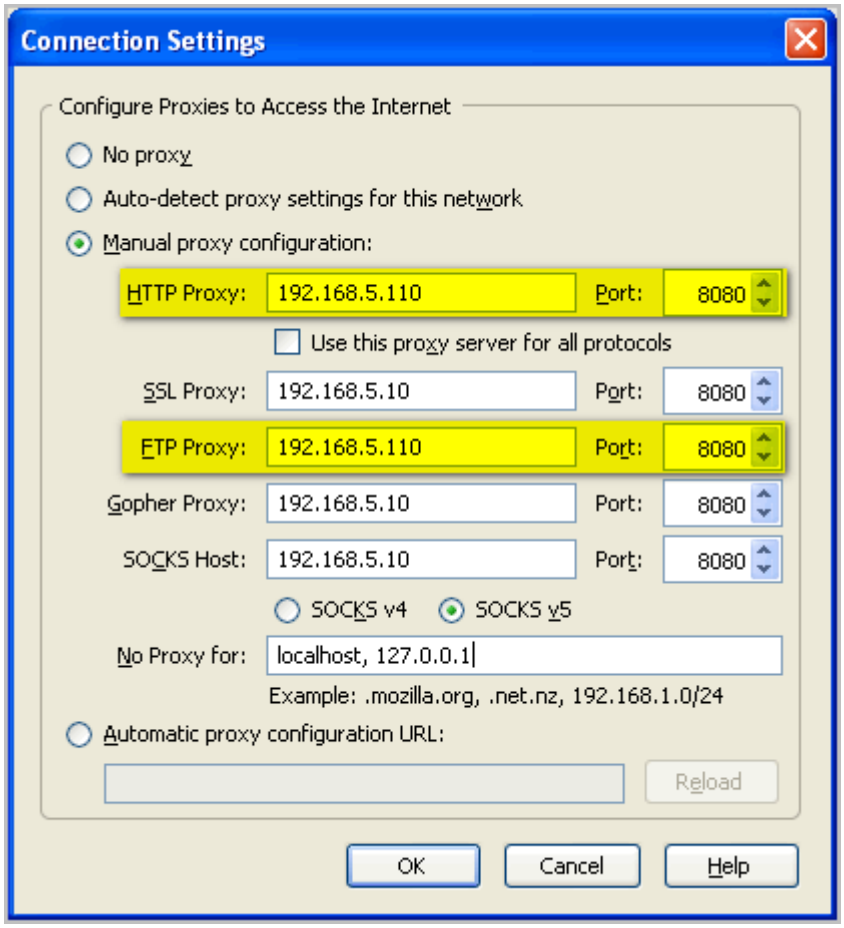
1. Launch **Mozilla Firefox**.

2. Click **Tools** ► **Options** ► **Advanced** tab ► **Network** tab.



Screenshot 30 - Mozilla Firefox: Options dialog

3. Click **Settings button** to open the **Connection Settings** dialog.

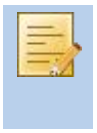


Screenshot 31 - Mozilla Firefox: Connection Settings dialog

4. Select **Manual proxy configuration**.

5. Uncheck **Use this proxy server for all protocols** checkbox.

6. Key in the proxy server IP address and the port used (Default 8080) in the **HTTP Proxy**, **FTP Proxy** and related **Port** text boxes.



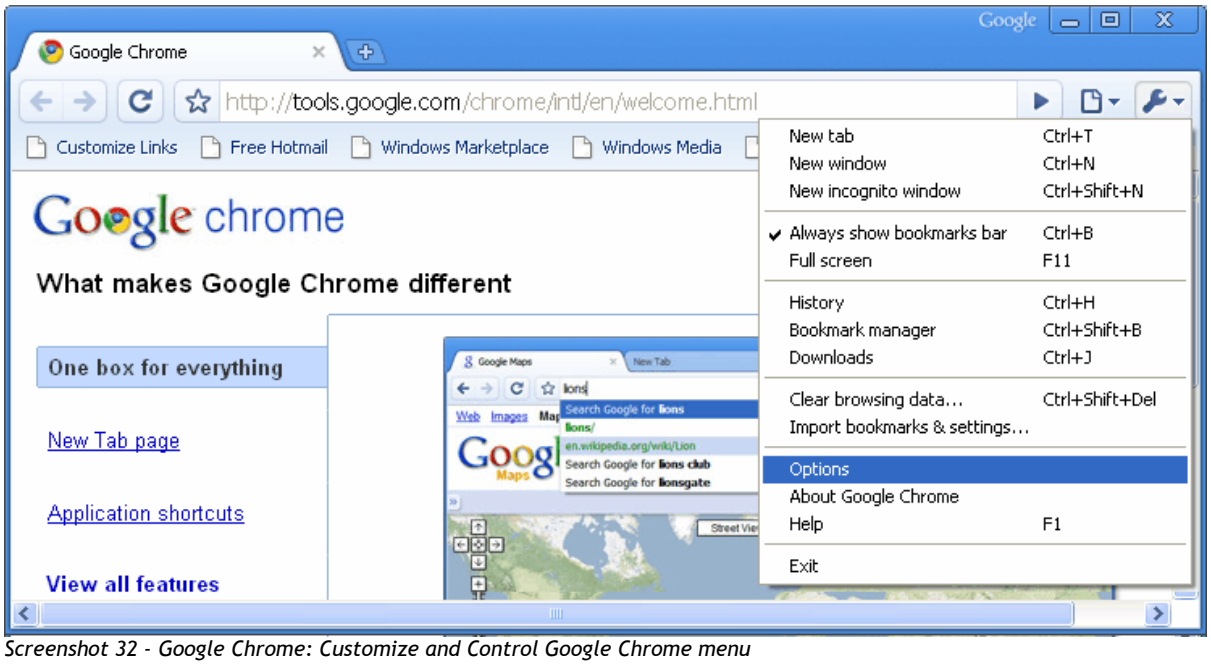
If WPAD is enabled in GFI WebMonitor proxy settings, select **Auto-detect proxy settings for this network**. For more information, refer to the Enabling WPAD in Proxy Settings section in this manual.

7. Click **OK** to close **Connection Settings** dialog.

8. Click **OK** to close **Options** dialog.

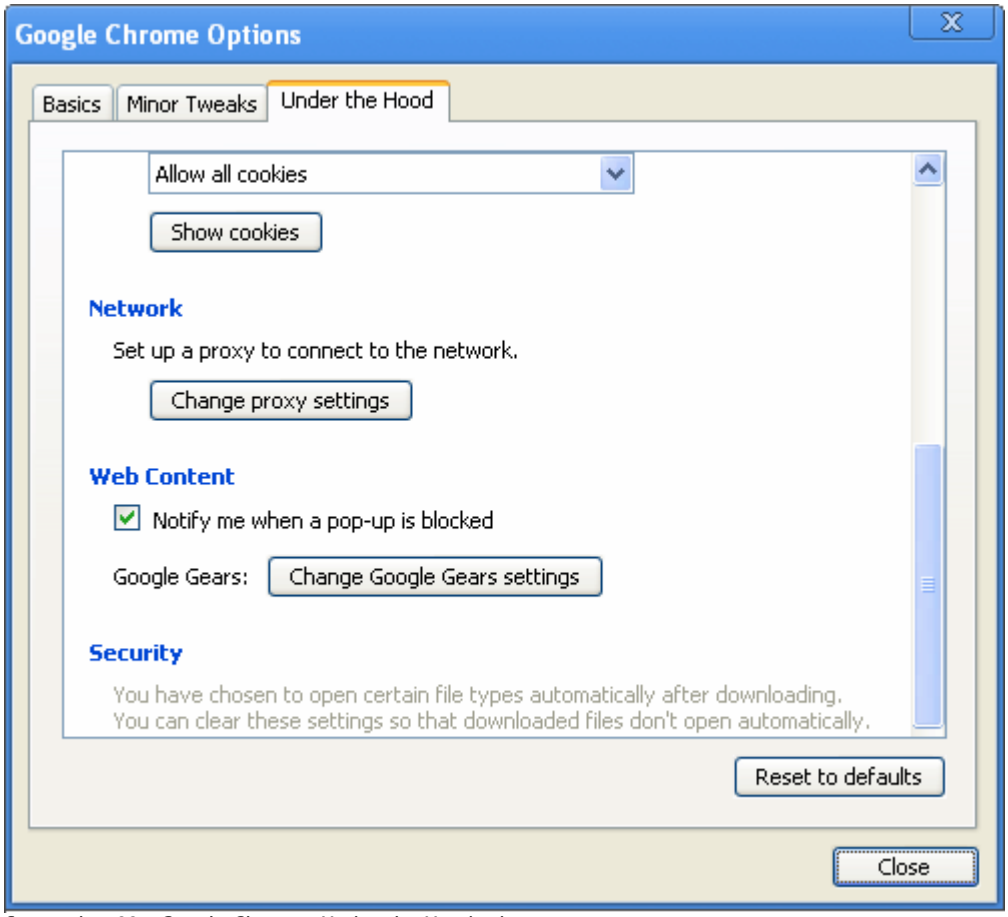
Google Chrome

1. Launch **Google Chrome**.



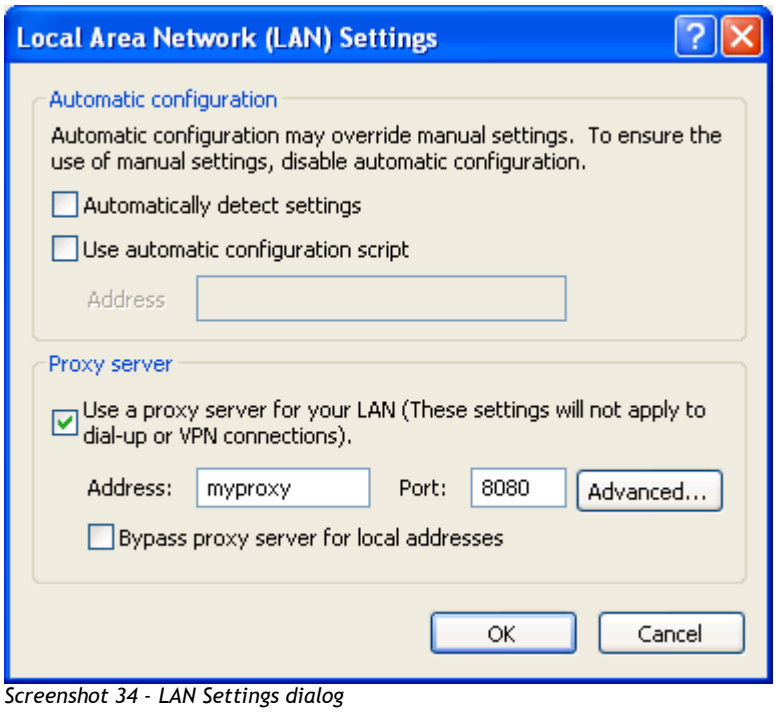
Screenshot 32 - Google Chrome: Customize and Control Google Chrome menu

2. Click **Customize and Control Google Chrome ► Options**.



Screenshot 33 - Google Chrome: Under the Hood tab

3. In the **Google Chrome Options** dialog, click **Under the Hood** tab.
4. Click **Change proxy settings** button to open **Internet Properties** dialog.
5. Select the **Connections** tab.
6. Click **LAN settings** button.



Screenshot 34 - LAN Settings dialog

7. Check **Use a proxy server for your LAN** checkbox.

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

If WPAD is enabled in GFI WebMonitor proxy settings check the **Automatically detect settings** checkbox in the **Automatic configuration** area. For more information, refer to the Enabling WPAD in Proxy Settings section in this manual.

9. Click **OK** to close **LAN Settings** dialog.

10. Click **OK** to close **Internet Options** dialog.

5 Launching GFI WebMonitor

5.1 Introduction

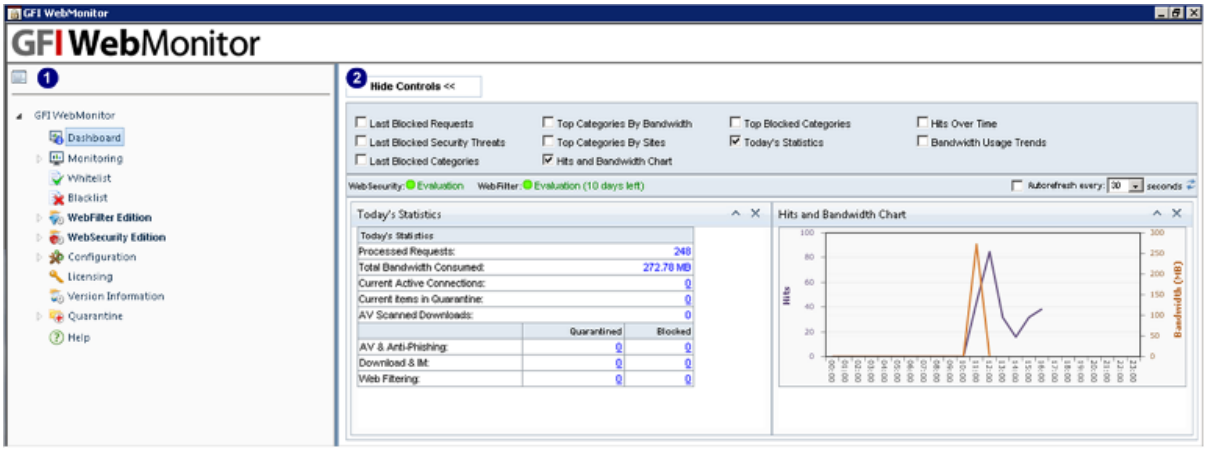
This chapter provides you with information related to the launching of GFI WebMonitor and an overview of the application's console.

5.2 Launching GFI WebMonitor

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

5.3 Navigating the Console

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



Screenshot 35 - GFI WebMonitor console view

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 -** A graphical overview of GFI WebMonitor activity.
- **Monitoring -** Enables generation of several 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.

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

6 Miscellaneous

6.1 Introduction

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

6.2 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 Ltd..

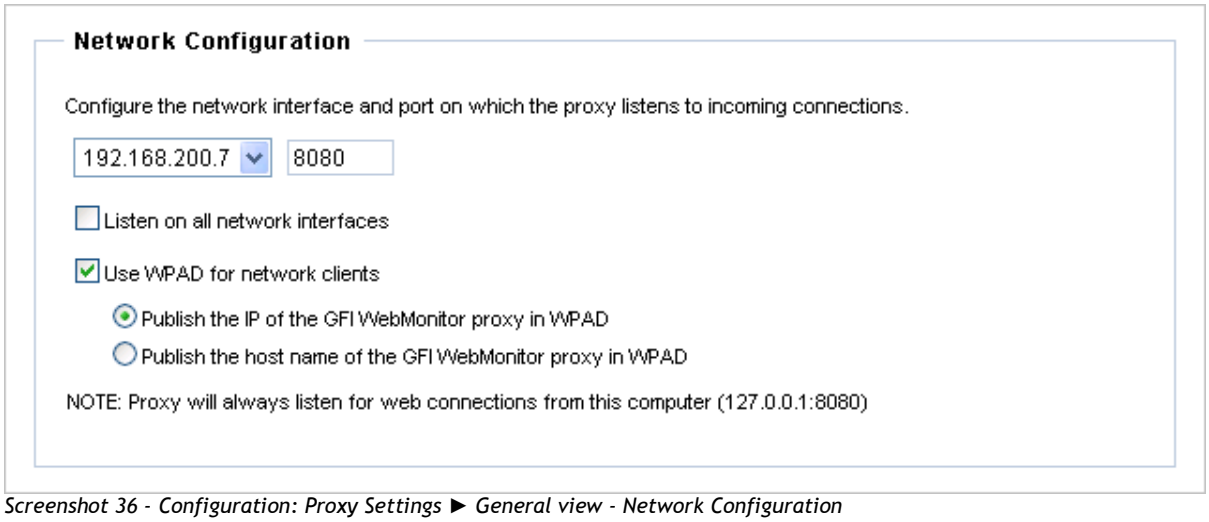
3. Click **Save Settings**.

6.3 Enabling WPAD in Proxy Settings

To allow client browsers to detect proxy settings automatically, Web Proxy AutoDiscovery (WPAD) can be enabled within GFI WebMonitor.

To enable WPAD:

1. Navigate to **Configuration ► Proxy Settings ► General**.



Screenshot 36 - Configuration: Proxy Settings ► General view - Network Configuration

2. From the **Network Configuration** area, select the **Use WPAD for network clients** to allow client machines to detect the server as the default proxy.

3. Select:

OPTION	DESCRIPTION
Publish the IP of the GFI WebMonitor proxy in WPAD	Includes the GFI WebMonitor IP address in the WPAD.dat file
Publish the host name of the GFI WebMonitor proxy in WPAD	Includes the GFI WebMonitor host name in the WPAD.dat file

4. Click **Save Settings** to finalize enabling WPAD.

6.4 Refreshing Cached Microsoft Internet Explorer Settings

Microsoft Internet Explorer may cache previously configured Internet settings. To ensure that the updated Internet settings are automatically detected by a client browser:

1. Launch **Microsoft Internet Explorer** on the client machine.
2. From the **Tools** menu, choose **Internet Options** and select the **Connections** tab.
3. Click **LAN settings** button.
4. Uncheck **Automatically detect settings** checkbox.
5. Click **OK** to close **LAN Settings** dialog.
6. Click **OK** to close **Internet Options** dialog.
7. Restart Internet Explorer.
8. Repeat steps 2 to 3.
9. Check **Automatically detect settings** checkbox.
10. Click **OK** to close **LAN Settings** dialog.
11. Click **OK** to close **Internet Options** dialog.
12. Restart Internet Explorer to refresh the cached Internet Explorer settings.

For more information visit:

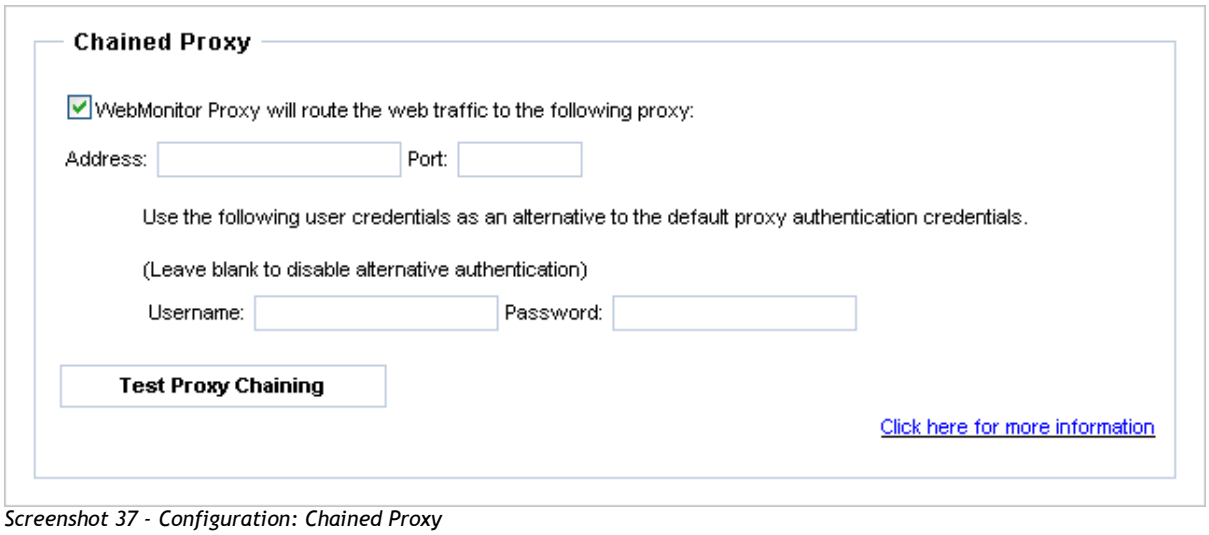
http://technet.microsoft.com/en-us/library/cc302643.aspx

6.5 Configuring Chained Proxy

Client machines can be configured to forward web traffic to the GFI WebMonitor server. In addition, the GFI WebMonitor server forwards the filtered traffic to a proxy server.

To configure GFI WebMonitor to forward web traffic to another proxy machine:

1. Navigate to **Configuration ► Proxy Settings ► General**.

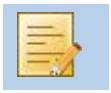


Screenshot 37 - Configuration: Chained Proxy

2. From the **Chained Proxy** area, select the **WebMonitor Proxy will route the web traffic to the following proxy:** checkbox.

3. Key in the proxy server IP address in the **Address** text box and key in the chained proxy's port (default 8080) in the **Port** text box.

4. If proxy authentication requires alternate credentials, key in the required credentials in the **Username** and **Password** fields.



If no credentials are keyed in, the default user credentials are used.

5. (Optional) Click the **Test Proxy Chaining** button to test the connection between the GFI WebMonitor machine and the proxy server.

6. Click **Save Settings**.

6.6 Configuring Routing and Remote Access

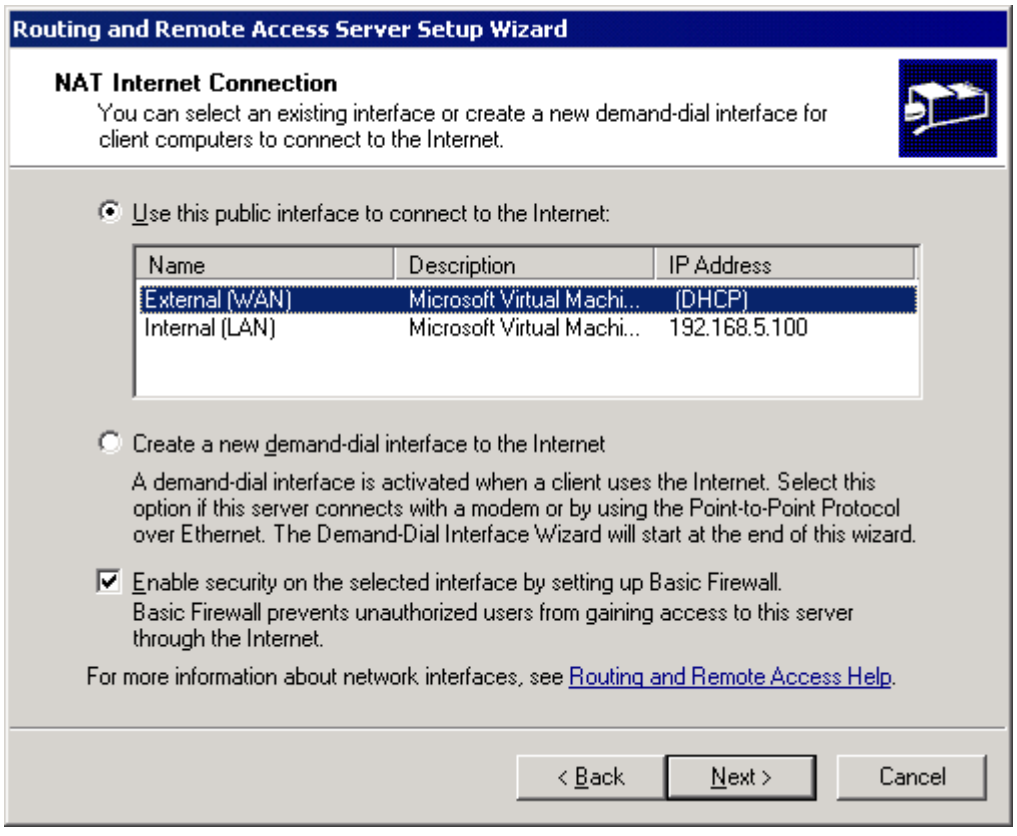
When installing GFI WebMonitor in Gateway mode on a Microsoft Windows Server 2003 or Microsoft Windows Server 2008, the Routing and Remote Access must be configured to use Network Address Translation (NAT). This can be done by:

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

2. Right-click the **<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**.



Screenshot 38 - 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**.

6.7 Configuring Commonly Used Routers

When installing GFI WebMonitor in Simple Proxy mode, the router must support port blocking or traffic forwarding. This sub-section contains information on how to configure some of the most commonly used routers.

6.7.1 SonicWall TZ 180

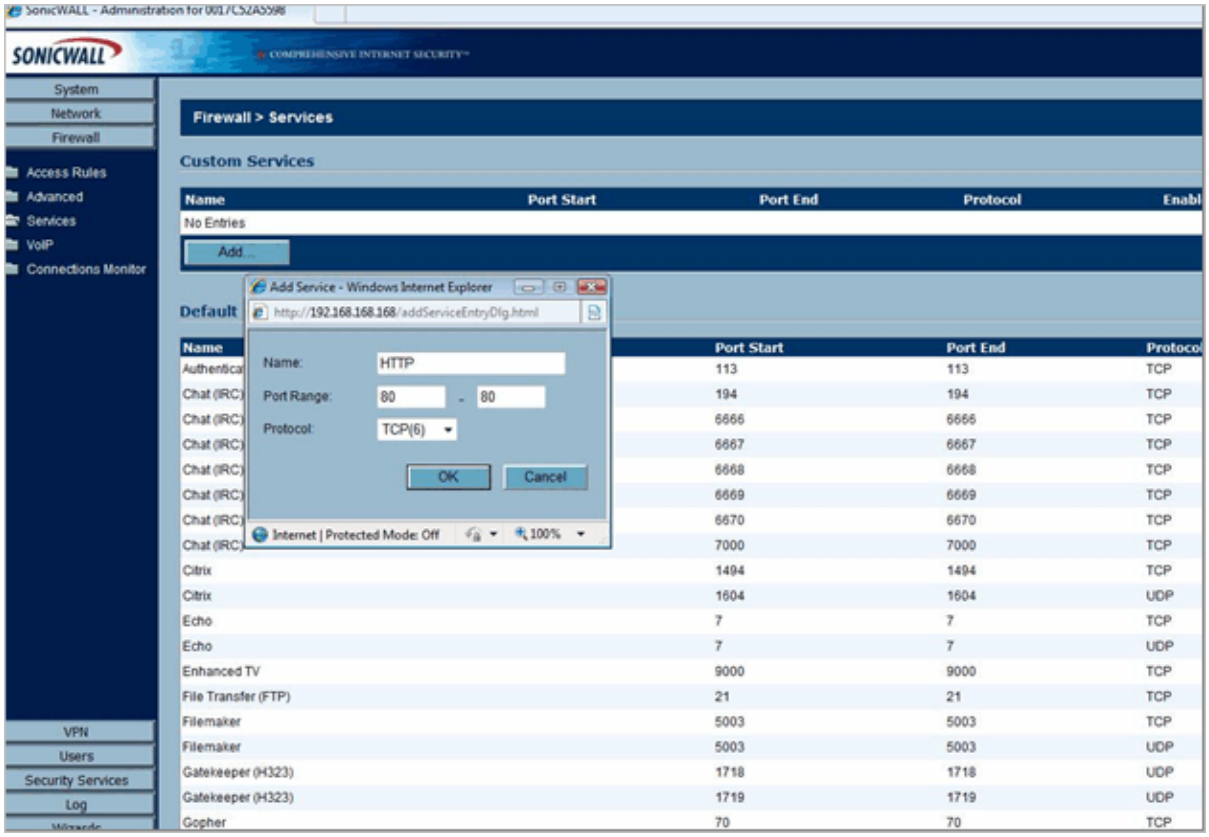
On **SonicWall TZ 180**, ports are blocked by creating firewall access rules.

Step 1: Creating a New Firewall Service for Port 80

To create a new firewall service for port 80:

1. Open the web configuration page from an internet browser.

2. Provide any credentials required.



Screenshot 39 - SonicWall: Services view and Add Service dialog

3. From the router's configuration web interface, click **Firewall ► Services**

4. Click **Add** to open the **Add Service** console.

5. Key in a name in the **Name** text box, for example "**HTTP**".

6. In **Port Range**, key in **80-80**.

7. From the **Protocol** drop-down list, select **TCP**.

8. Click **OK**.

Step 2: Blocking the New Service

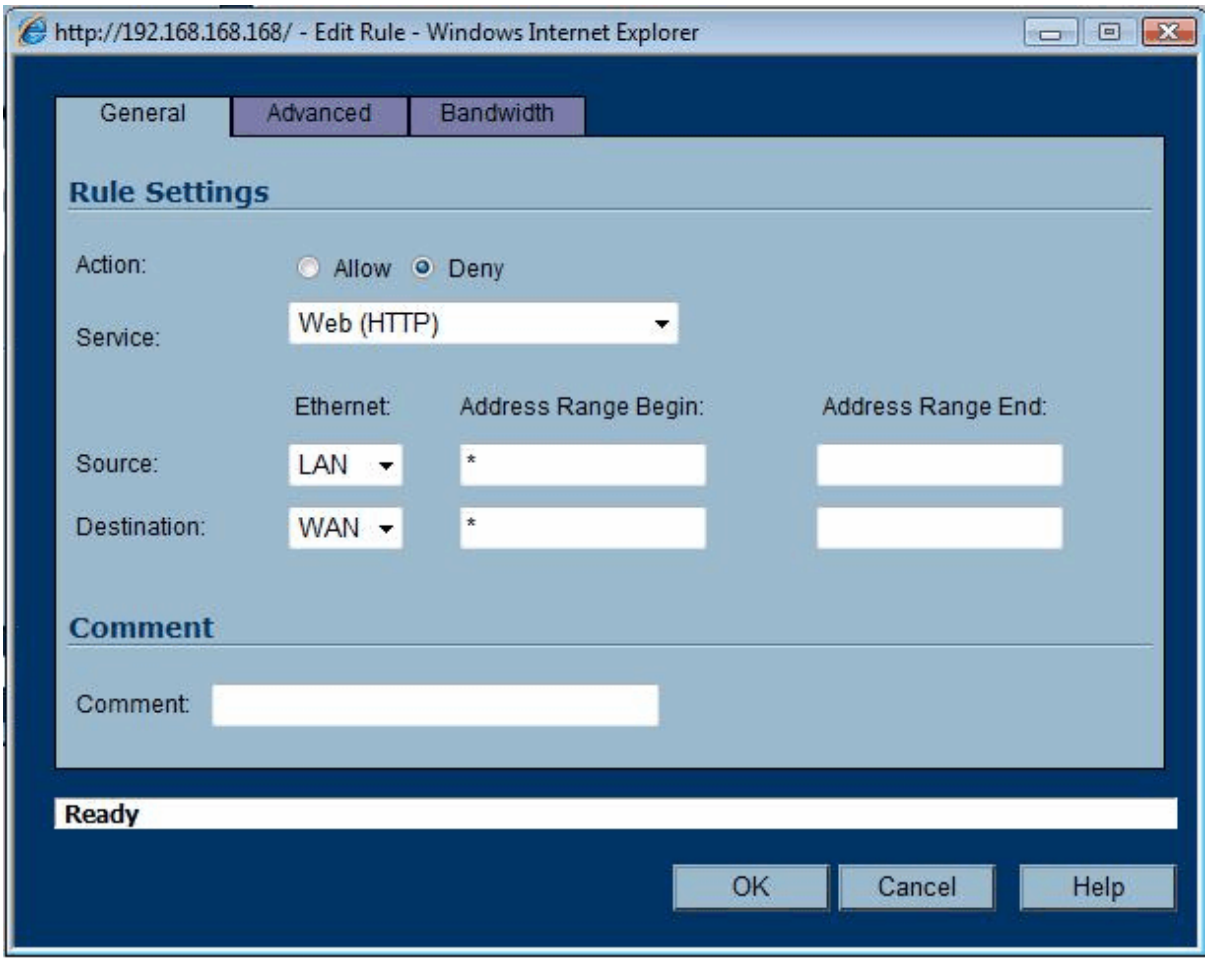
To create a firewall access rule to block the newly created service:

1. Open the web configuration page from an internet browser.

2. Provide any credentials required.

3. From the router's configuration web interface, click **Firewall ► Access Rules**.

4. Click **Add** button to open the **Add Rule** console.



Screenshot 40 - SonicWall: Edit Rule dialog

5. Select the **General** tab.

6. From the **Action** radio buttons, select **Deny**.

7. From the **Service** drop-down list, select **Web (HTTP)**.

8. In the **Source** row, select **LAN** from the **Ethernet** drop-down list, and key in "*" in **Address Range Begin** text box.

By selecting the wildcard "*", all inbound network traffic and all IP ranges on port 80 are blocked.

9. In the **Destination** row, select **WAN** from the **Ethernet** drop-down list and key in "*" in **Address Range Begin** text box.

10. (Optional) Select the **Advanced** tab to configure a time-based schedule.

11. Click **OK** button.

Step 3: Creating a Firewall Access Rule to Allow HTTP Traffic From GFI WebMonitor Proxy

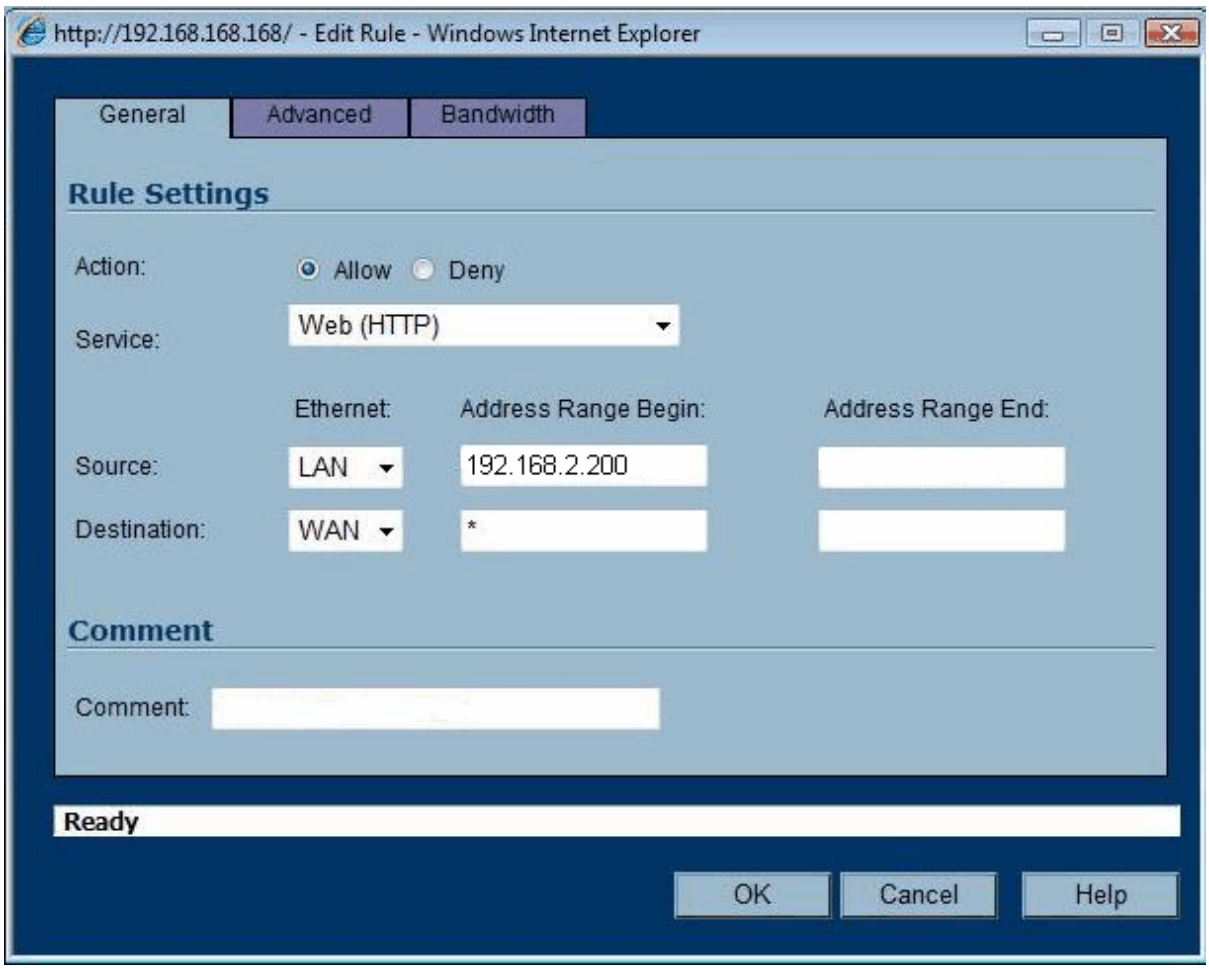
To create a firewall access rule to allow Web (HTTP) traffic originating from GFI WebMonitor Proxy machine:

1. Open the web configuration page from an internet browser.

2. Provide any credentials required.

3. From the router's configuration web interface, click **Firewall ► Access Rules**.

4. Click **Add** button to open the **Add Rule** console.



Screenshot 41 - SonicWall: Edit Rule dialog

5. Select the **General** tab.

6. From the **Action** radio buttons, select **Allow**.

7. From the **Service** drop-down list, select **Web (HTTP)**.

8. In the **Source** row, select **LAN** from the **Ethernet** drop-down list, and key in the IP address of the GFI WebMonitor proxy machine in **Address Range Begin** text box.

9. In the **Destination** row, select **WAN** from the **Ethernet** drop-down list and key in **"*"** in **Address Range Begin** text box.

10. (Optional) Select the **Advanced** tab to configure a time-based schedule.

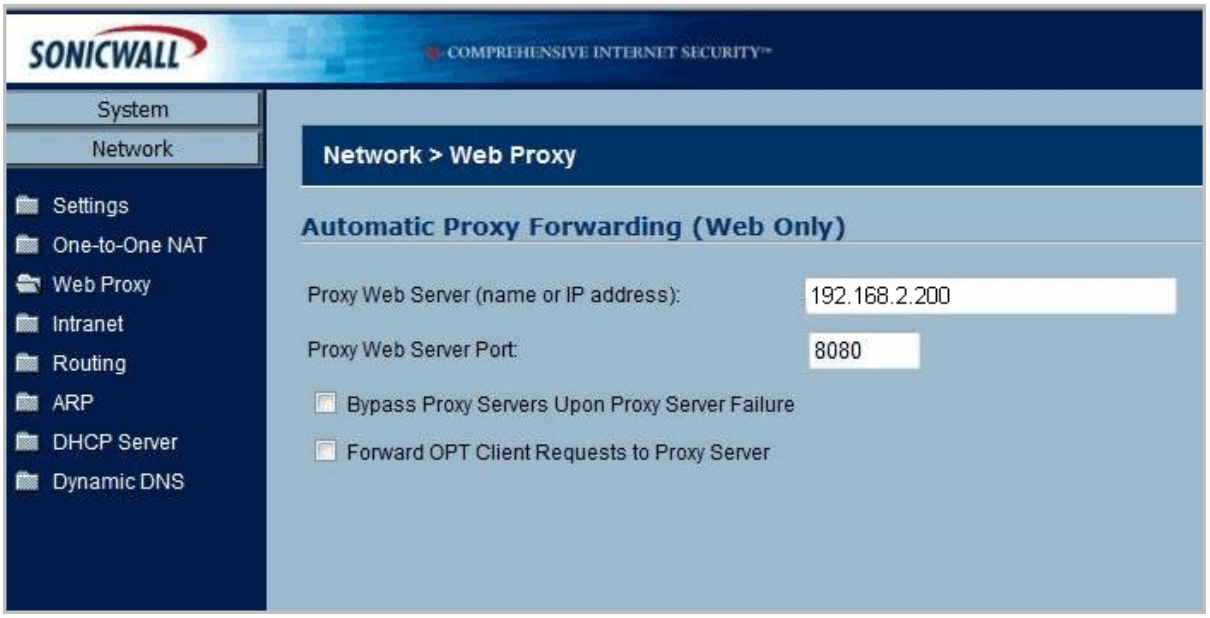
11. Click **OK** button.

Step 4: Traffic Forwarding to GFI WebMonitor Proxy

To forward network traffic through the GFI WebMonitor Proxy:

1. Open the web configuration page from an internet browser.

2. Provide any credentials required.



Screenshot 42 - SonicWall: Automatic Proxy Forwarding view

3. From the router's configuration web interface, click **Network ► Web Proxy**.

4. In the **Proxy Web Server (name or IP address)** text box, key in the IP address of the GFI WebMonitor proxy machine

5. In the **Proxy Web Server Port** text box, key in the port used (Default 8080).

6. Click **Apply** button.

6.7.2 SonicWall NSA 2400

On **SonicWall NSA 2400** two steps are required to:

» Define the external and internal network cards

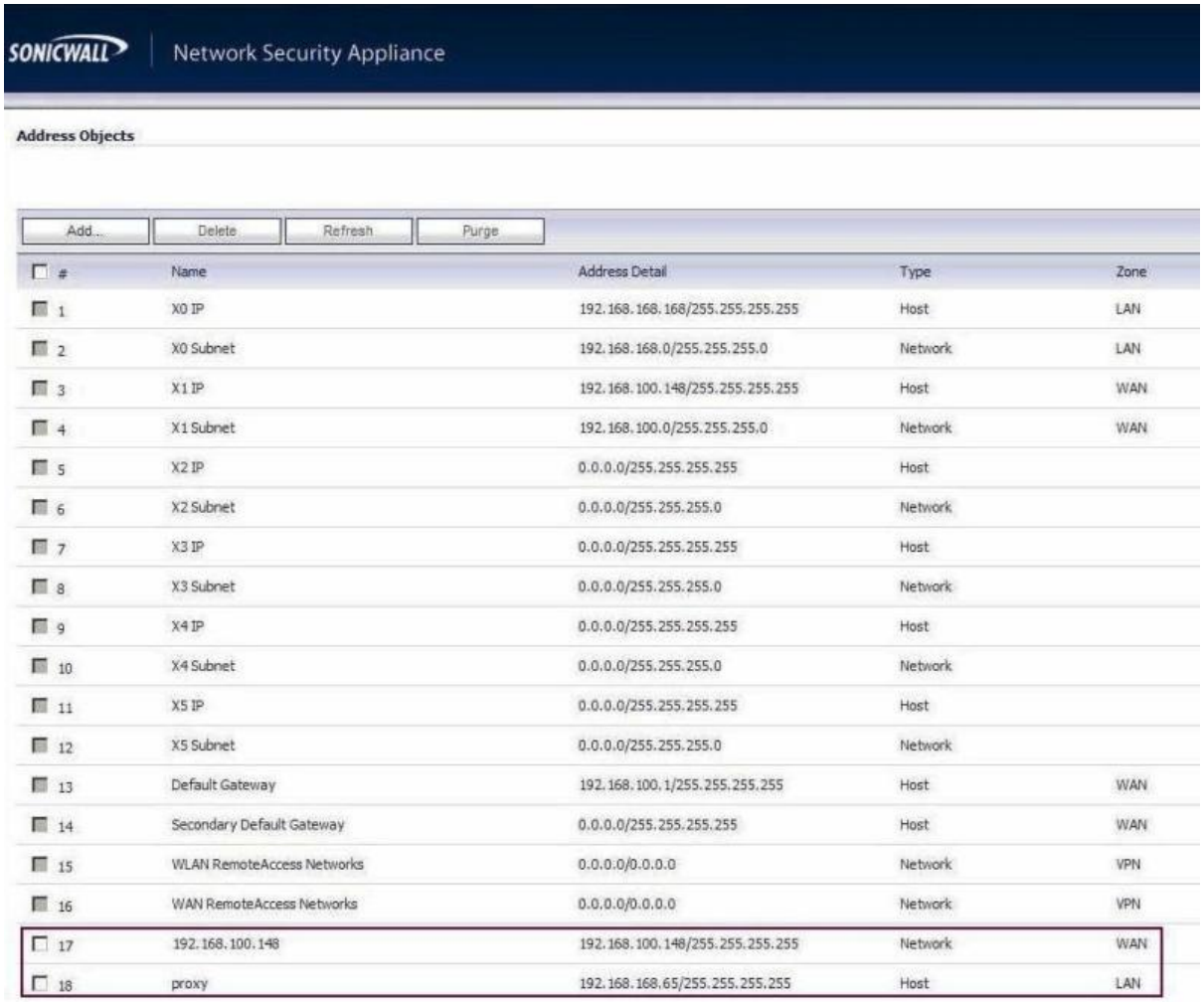
» Create traffic controlling firewall rules

Step 1: Defining Network Addresses

To define the external and internal network cards:

1. Open the web configuration page from an internet browser.

2. Provide any credentials required.



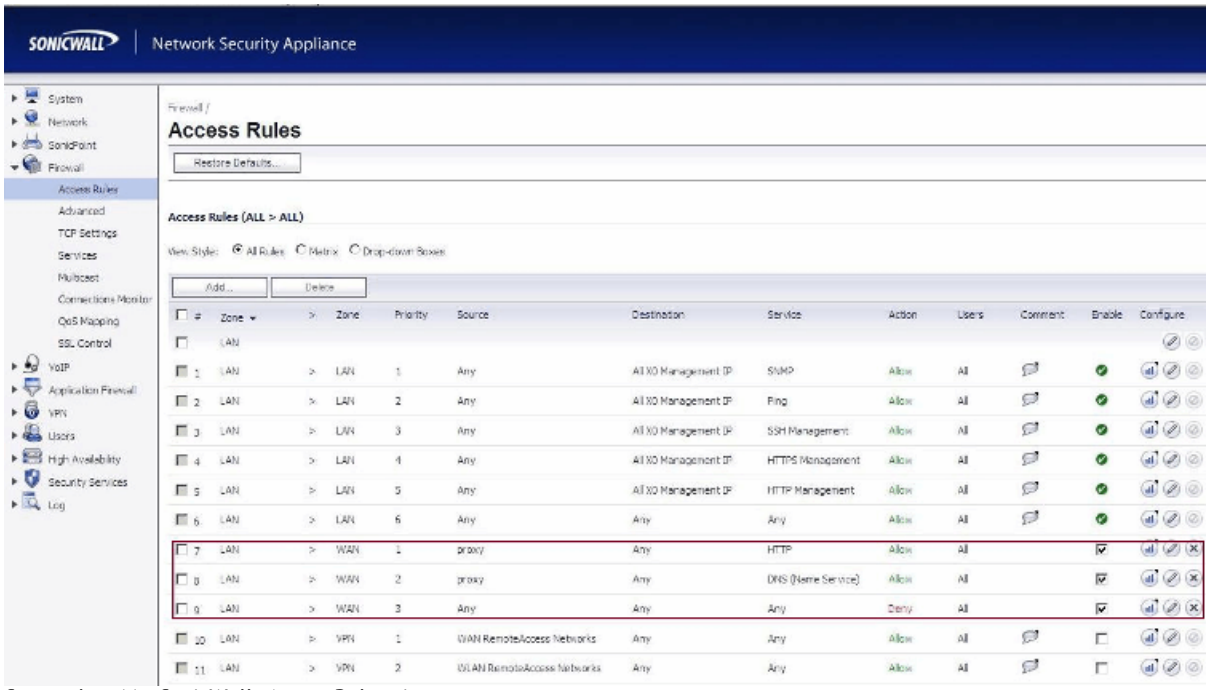
Screenshot 43 - *SonicWall*: Address Objects view

3. From the router's configuration web interface, click **Network ► Address Objects**
4. Click **Add** button to add a WAN connection
5. In the **Address Detail** column, key in the IP address of the external network card.
6. In the **Type** column, select **Network**.
7. In the **Zone** column, select **WAN**.
8. Click **Add** button to add a LAN connection
9. In the **Address Detail** column, key in the IP address of the internal network card.
10. In the **Type** column, select **Host**.
11. In the **Zone** column, select **LAN**.

Step 2: Creating Firewall Rules

To create traffic controlling firewall rules:

1. Open the web configuration page from an internet browser.
2. Provide any credentials required.



Screenshot 44 - SonicWall: Access Rules view

3. From the router's configuration web interface, click **Firewall ► Access Rules**.

4. Click **Add** button to add a new rule.

5. Repeat step 4 to create three rules with the following information:

ZONE	PRIORITY	SOURCE	DESTINATION	SERVICE	ACTION
LAN>WAN	1	Proxy	Any	HTTP	Allow
LAN>WAN	2	Proxy	Any	DNS	Allow
LAN>WAN	3	Any	Any	Any	Deny

6.7.3 Cisco ADSL Router Cisco 878 (MPC8272)

The **Cisco** command console enables the administrator to manage the router. Port 80 is blocked by executing an **Access-list** command.

The format of an access-list console command is:

```
access-list [Number] [Action] [Source] [Destination] [Port]
```

To deny access to port 80, key in the following command in the Cisco command console:

```
Access-list 100 deny any any eq 80
```

6.7.4 Netgear Wireless Router DG834GT

On **Netgear Wireless Router DG834GT**, ports are blocked by creating firewall access rules. This section describes how to:

» Create a firewall access rule to allow Web (HTTP) traffic originating from GFI WebMonitor Proxy machine

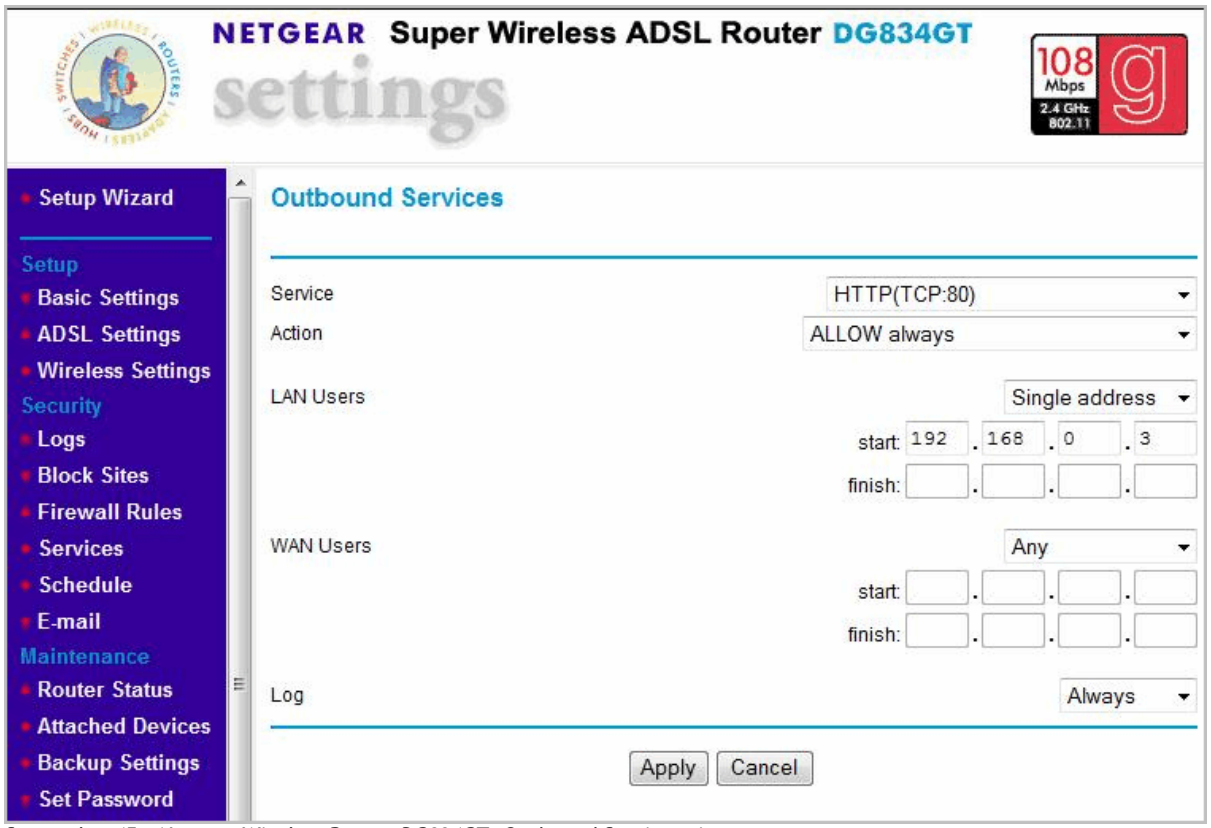
» Create a firewall access rule to block all outgoing HTTP traffic

Step 1: Creating a Firewall Access Rule to Allow HTTP Traffic From GFI WebMonitor Proxy

To create a firewall access rule to allow Web (HTTP) traffic originating from GFI WebMonitor Proxy machine:

1. Open the web configuration page from an internet browser.

2. Provide any credentials required.



Screenshot 45 - Netgear Wireless Router DG834GT: Outbound Services view

3. From the router's configuration web interface, click **Firewall Rules ► Outbound Services**.

4. From the **Service** drop-down list, select **HTTP (TCP80)**.

5. From the **Action** drop-down list, select **ALLOW always**.

6. From the **LAN Users** drop-down list, select **Single address.**

7. In the **Start** text box, key in the IP address of the GFI WebMonitor proxy machine

8. From the **WAN Users** drop-down list, select **Any**.

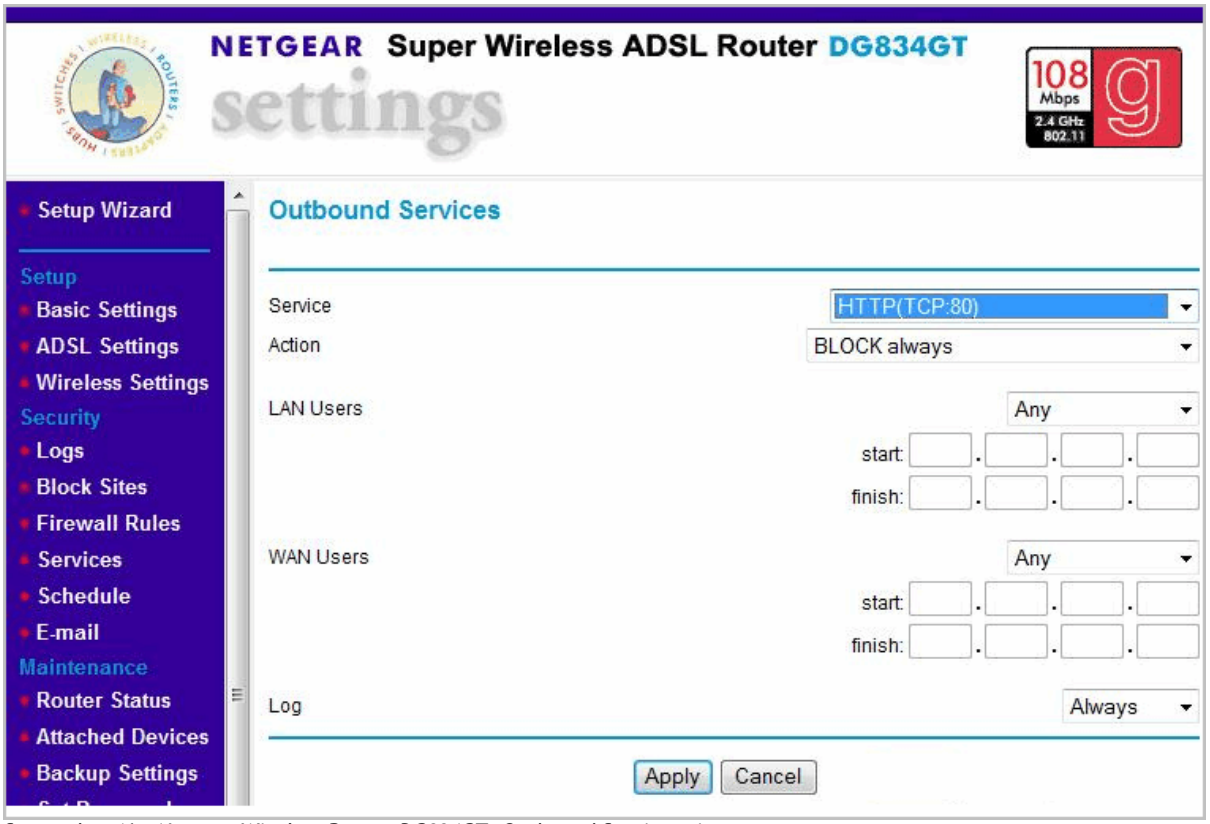
9. Click **Apply** to save settings.

Step 2: Creating a Firewall Access Rule to Block All Outgoing HTTP Traffic

To create a firewall access rule to block all Web (HTTP) traffic:

1. Open the web configuration page from an internet browser.

2. Provide any credentials required.



Screenshot 46 - Netgear Wireless Router DG834GT: Outbound Services view

3. From the router's configuration web interface, click **Firewall Rules ► Outbound Services**.
4. From the **Service** drop-down list, select **HTTP (TCP80)**.
5. From the **Action** drop-down list, select **BLOCK always**.
6. From the **LAN Users** drop-down list, select **Any.**
7. From the **WAN Users** drop-down list, select **Any**.
8. Click **Apply** to save settings.

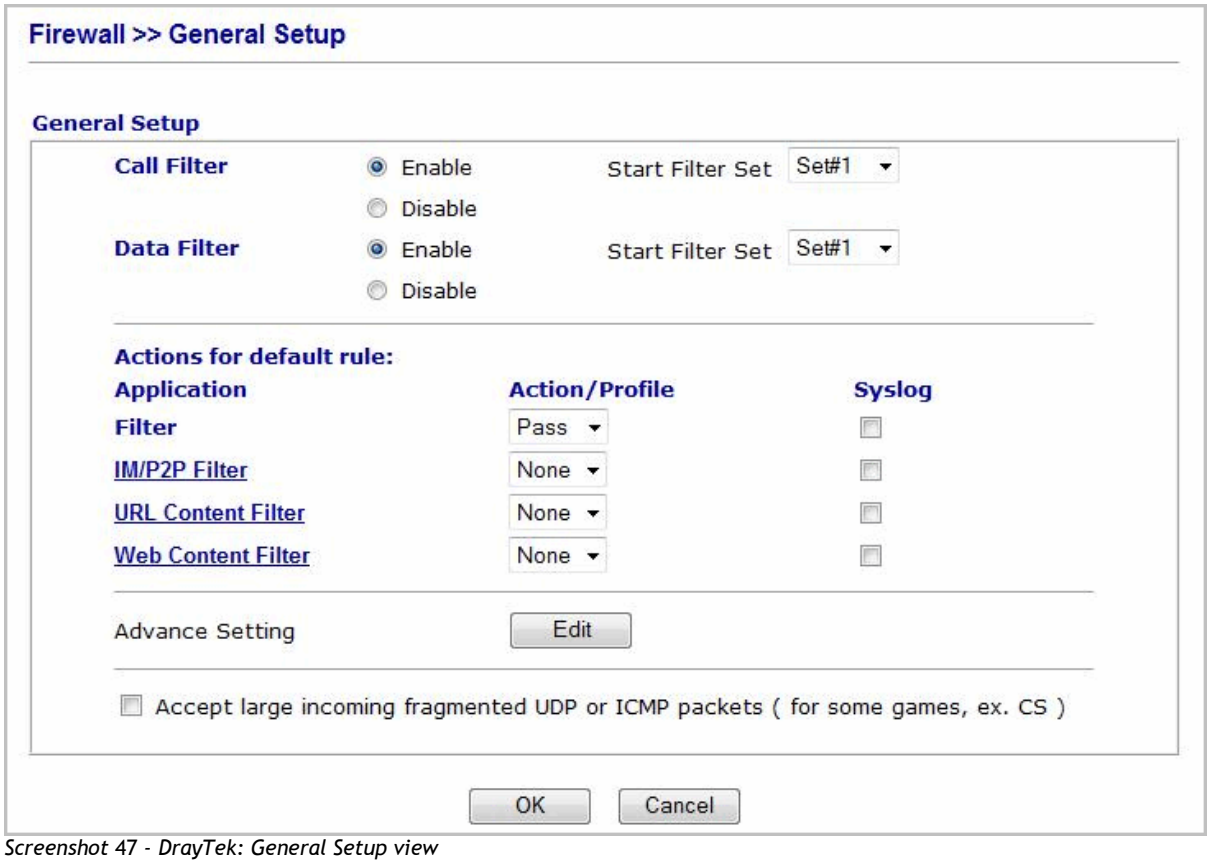
6.7.5 DrayTek VIGOR 2820N ADSL2

On **DrayTek VIGOR 2820 series**, port 80 is blocked on all machines except the proxy by creating two firewall filter rules. To do this create the following two rules:

- First rule blocks IP addresses smaller than the GFI WebMonitor proxy machine IP address (excluding the proxy machine's IP address)
- Second rule blocks IP addresses greater than the GFI WebMonitor proxy machine IP address (excluding the proxy machine's IP address)

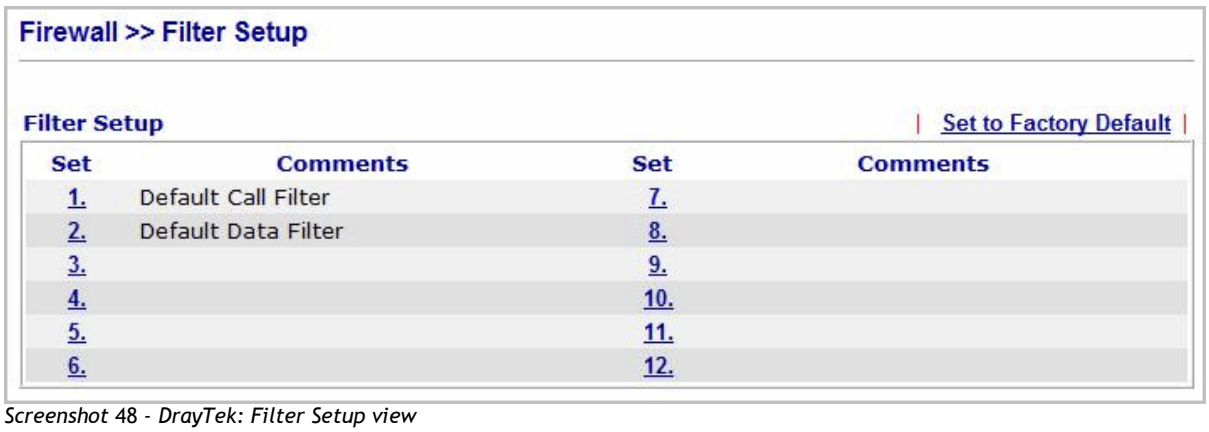
By default the router, contains a pre-defined rule for NetBios DNS lookups. To view or configure the firewall rules:

1. Open the web configuration page from an internet browser.
2. Provide any credentials required.



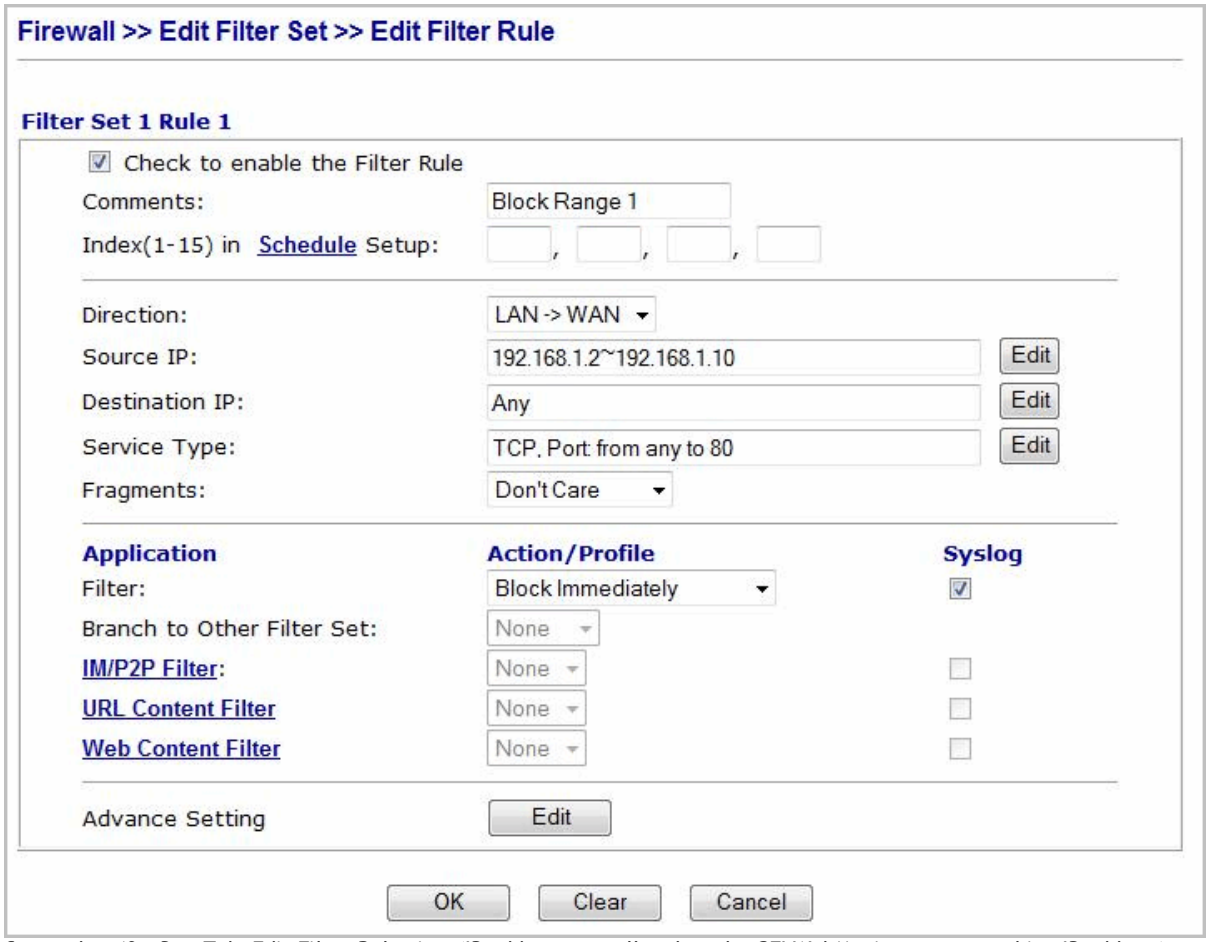
Screenshot 47 - DrayTek: General Setup view

4. From the **Start Filter Set** drop-down lists of both **Call Filter** and **Data Filter**, select **Set#1**.
5. Click **OK** to save the changes
6. Select **Firewall ► Filter Setup** menu. This page contains the collection of rules.



Screenshot 48 - DrayTek: Filter Setup view

7. Select rule number **1** from the **Set** list to open the **Edit Filter Set** page.



Screenshot 49 - DrayTek: Edit Filter Rule view (IP addresses smaller than the GFI WebMonitor proxy machine IP address)

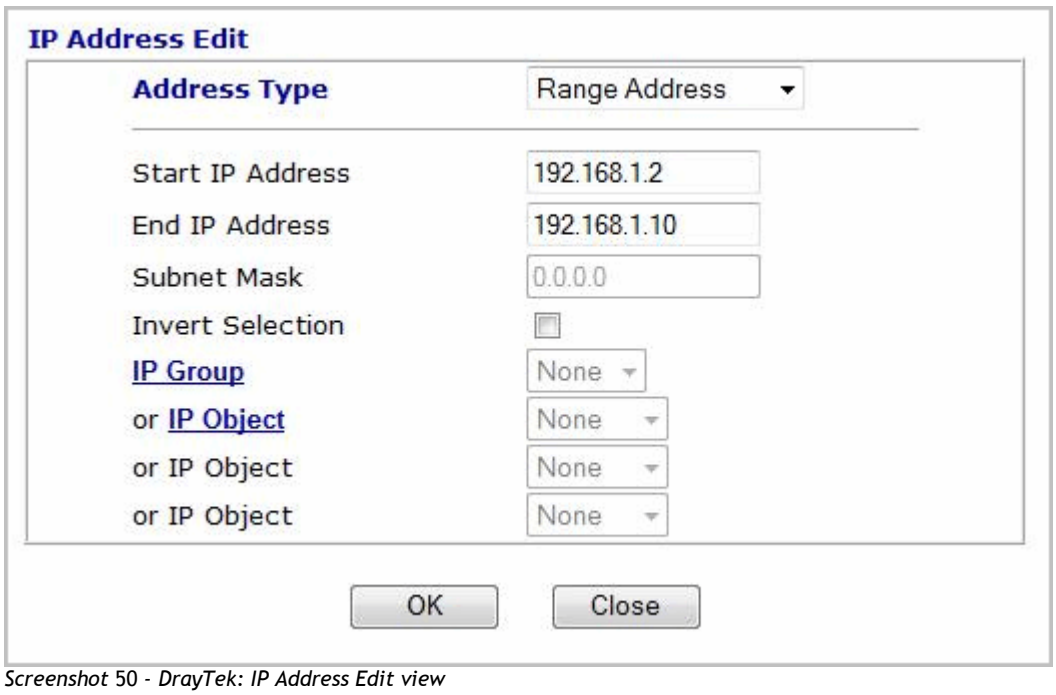
8. Double click the first rule (Block NetBios) to open the filter page.

9. In the filter page, click "**1**" to open the Filter Rule configuration

10. Key in a name, example "Block Range 1" in the **Comments** text box.

11. From the **Direction** drop-down list, select **LAN->WAN.**

12. Click **Edit** button of the **Source IP** field. This opens the **IP Address Edit** page.



Screenshot 50 - DrayTek: IP Address Edit view

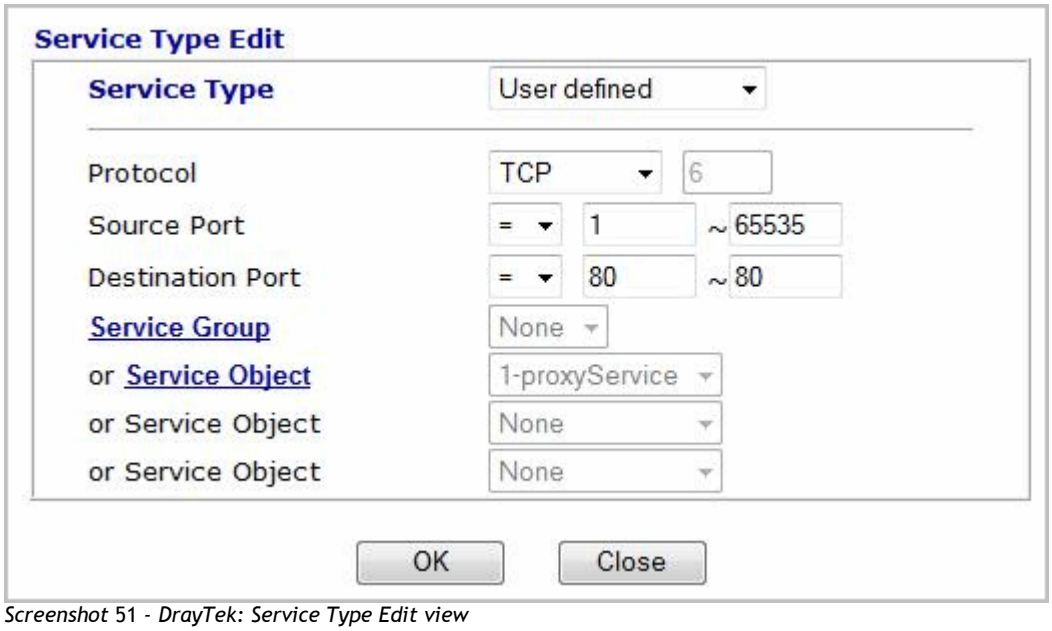
13. From the **Address Type** drop-down list, select **Range Address**.

14. In the **Start IP Address** text box, key in the smallest IP address of the range of IP addresses smaller than the GFI WebMonitor proxy machine IP address.

15. In the **End IP Address** text box, key in the largest IP address of the range of IP addresses smaller than the GFI WebMonitor proxy machine IP address (excluding the proxy machine's IP address).

16. Click **OK** to apply settings.

17. In the **Edit Filter Rule** page, click **Edit** button of the **Service Type** field.



Screenshot 51 - DrayTek: Service Type Edit view

18. From the **Service Type** drop-down list, select **User defined**.

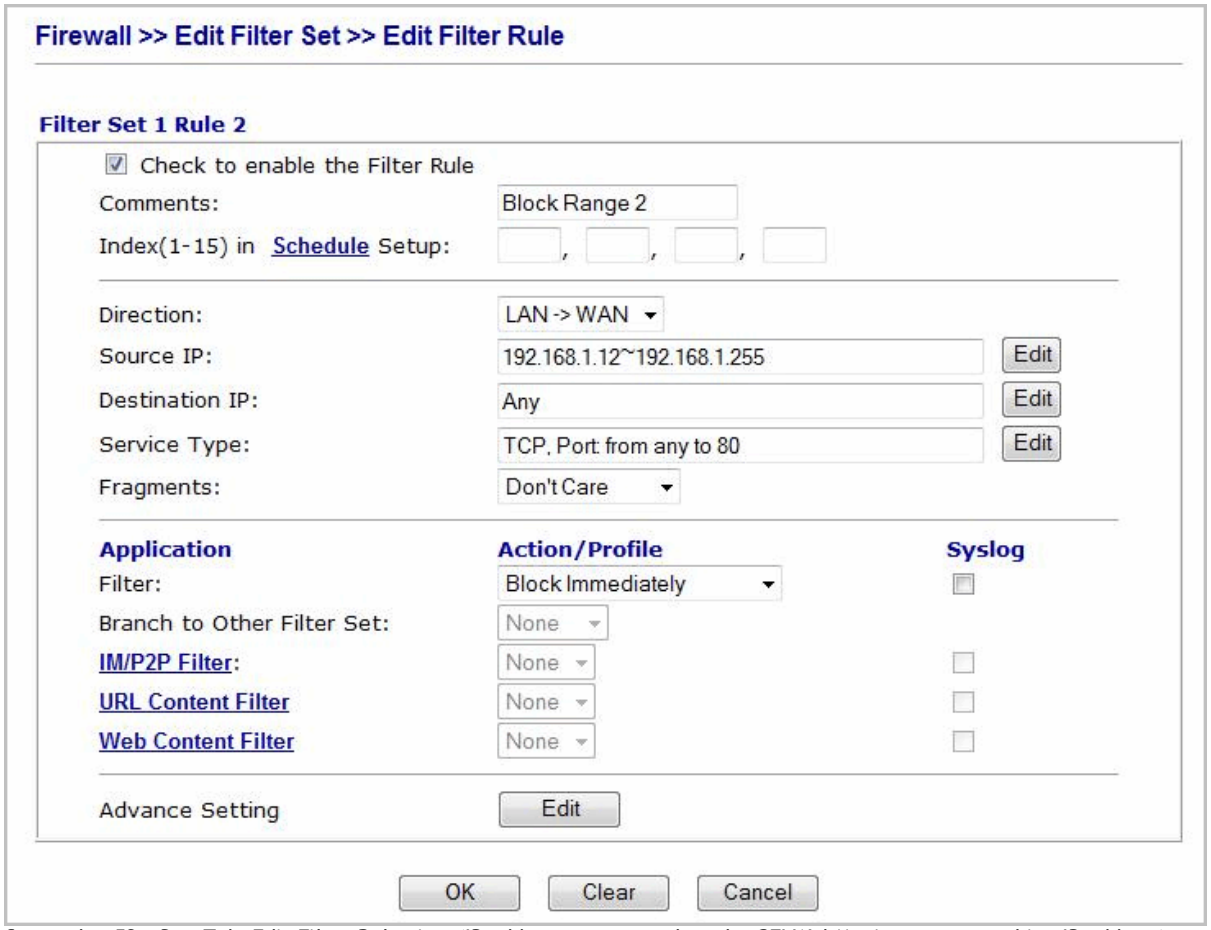
19. From the **Protocol** drop-down list, select **TCP**.

20. In the **Source Port** text boxes, key in "1" and "65535" respectively.

21. In the **Destination Port** text boxes, key in "80" and "80" respectively.

22. Click **OK** to apply settings.

23. Repeat steps 1 to 22 to block IP addresses greater than the GFI WebMonitor proxy machine IP address (excluding the proxy machine's IP address).



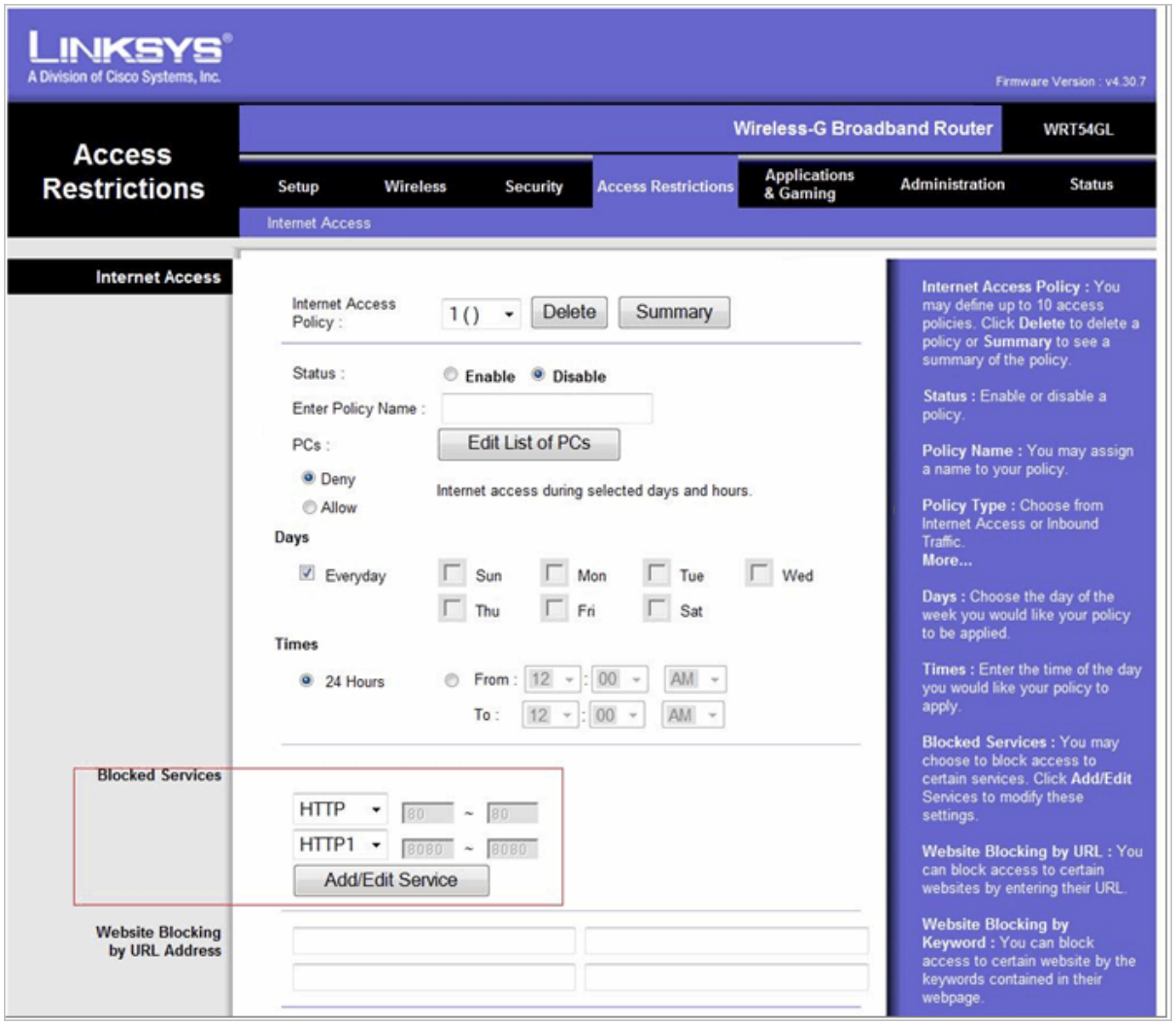
Screenshot 52 - DrayTek: Edit Filter Rule view (IP addresses greater than the GFI WebMonitor proxy machine IP address)

6.7.6 Linksys WRT54GL Wireless Router

On **Linksys WRT54GL Wireless Router**, ports are not blocked directly; they are blocked by creating internet access restrictions. To create a restriction to block HTTP on port 80:

1. Open the web configuration page from an internet browser.

2. Provide any credentials required.



Screenshot 53 - Linksys WRT54GL Wireless Router: Internet Access view

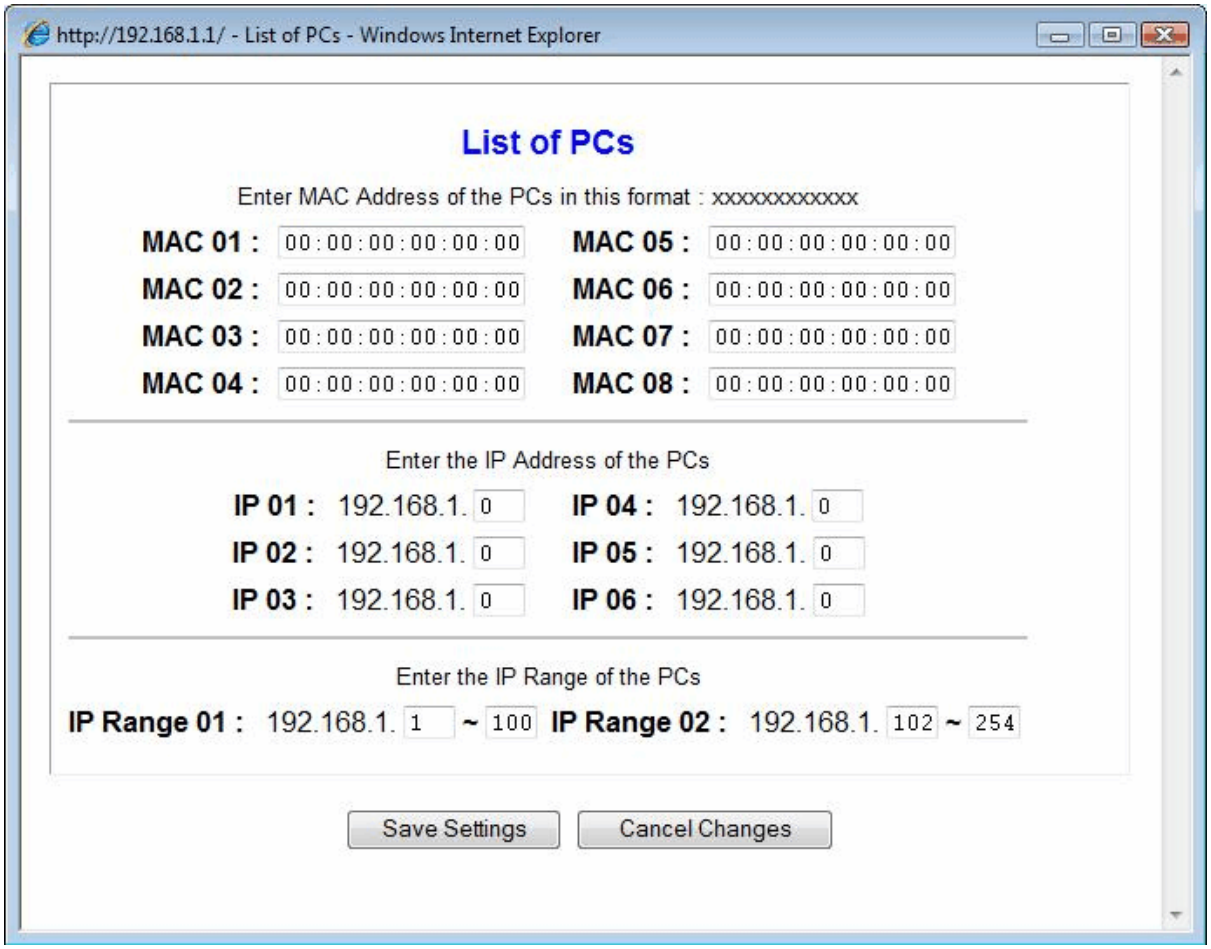
3. From the router's configuration web interface, click **Access Restrictions** tab ► **Internet Access**.

4. From the **Internet Access Policy** drop-down list, select a number.

5. From the **Status** radio buttons, select **Disable**. (Select **Enable** to start blocking immediately).

6. In the **Enter Policy Name** text box, key in a name.

7. Click **Edit List of PCs** button.



Screenshot 54 - Linksys WRT54GL Wireless Router: List of PCs dialog

8. In **IP Range 01** text boxes, key in the IP addresses of the range of IP addresses smaller than the GFI WebMonitor proxy machine IP address (excluding the proxy machine's IP address).

9. In **IP Range 02** text boxes, key in the IP addresses of the range of IP addresses greater than the GFI WebMonitor proxy machine IP address (excluding the proxy machine's IP address).

10. Click **Save Settings** button.

11. From the **PCs** radio buttons, select **Deny**.

12. From the **Blocked Services** first drop-down list, select **HTTP** and key in "80" and "80" respectively.

13. (Optional) Click **Add/Edit Service** to create or modify a service.

14. Click **Save Settings**.

6.7.7 Thomson Wireless Broadband Router TG585 v7

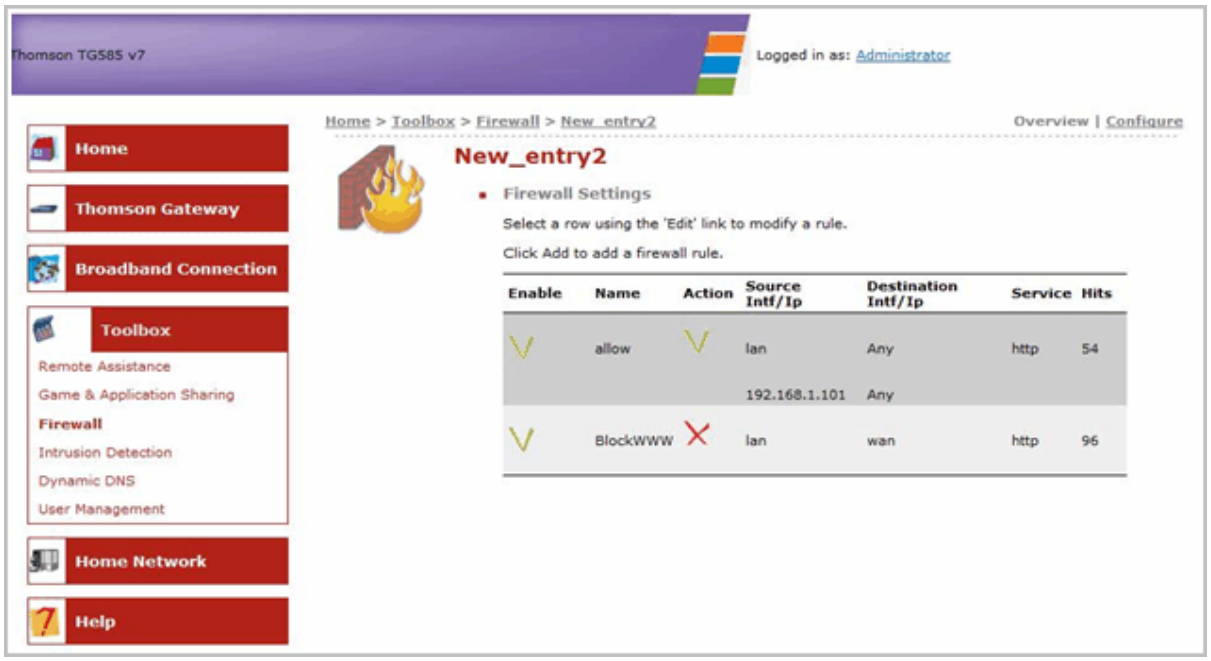
On **Thompson Wireless Broadband Router TG585 v7**, ports are blocked by creating firewall access rules. This section describes how to:

- Create a firewall access rule to allow Web (HTTP) traffic originating from GFI WebMonitor Proxy machine
- Create a firewall access rule to block all outgoing HTTP traffic

Step 1: Creating a Firewall Access Rule to Allow HTTP Traffic From GFI WebMonitor Proxy

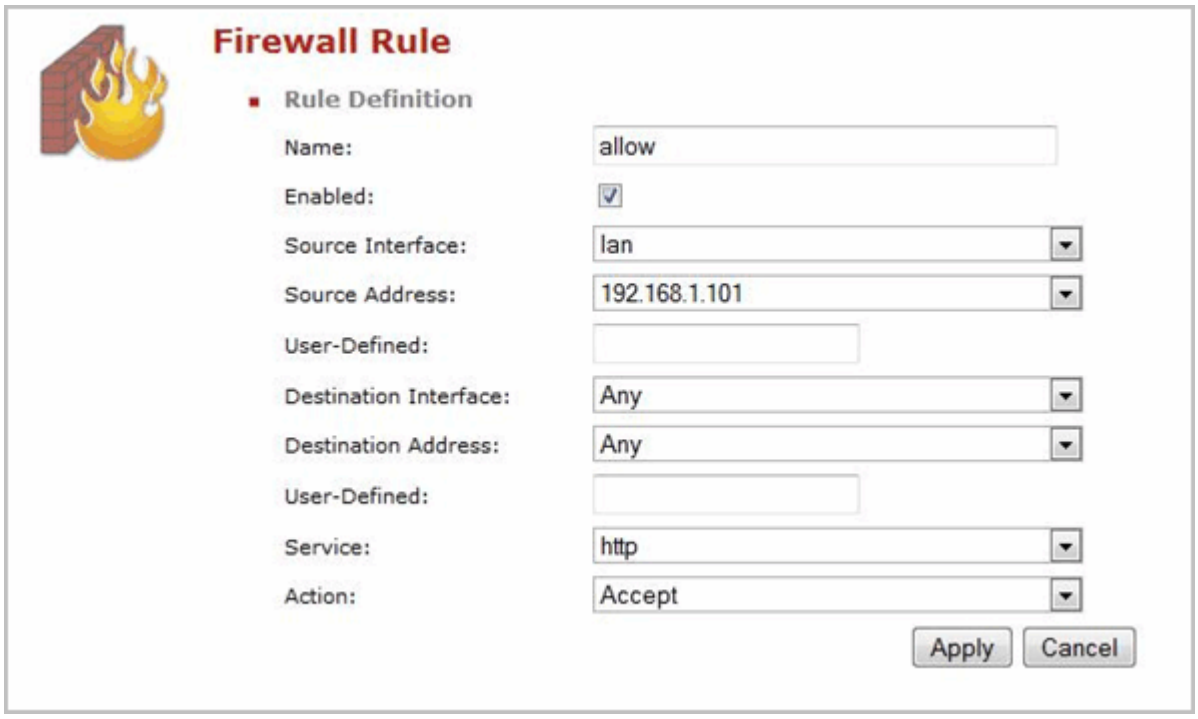
To create a firewall access rule to allow Web (HTTP) traffic originating from GFI WebMonitor Proxy machine:

1. Open the web configuration page from an internet browser.
2. Provide any credentials required.



Screenshot 55 - Thompson Wireless Broadband Router TG585 v7: Firewall Settings view

3. From the router's configuration web interface, click **Toolbox ► Firewall**.
4. From the **Firewall Settings,** select **Configure**.
5. Click **Add** button to add a new firewall rule.



Screenshot 56 - Thompson Wireless Broadband Router TG585 v7: Firewall Rule view

6. Key in a name in the **Name** text box, for example "**allow**".
7. Check **Enabled** checkbox**.**
8. From the **Source Interface** drop-down list, select **lan**.
9. To specify the IP address of the GFI WebMonitor proxy machine:

» Option 1: From the **Source Address** drop-down list, select the IP address of the GFI WebMonitor proxy machine.

» Option 2: In the **User-Defined** text box, key in the IP address of the GFI WebMonitor proxy machine

10. From the **Destination Interface** drop-down list, select **Any**.

11. From the **Destination Address** drop-down list, select **Any**.

12. From the **Service** drop-down list, select **HTTP**.

13. From the **Action** drop-down list, select **Accept**.

14. Click **Apply** to save settings.

Step 2: Creating a Firewall Access Rule to Block All Outgoing HTTP Traffic

To create a firewall access rule to block all Web (HTTP) traffic:

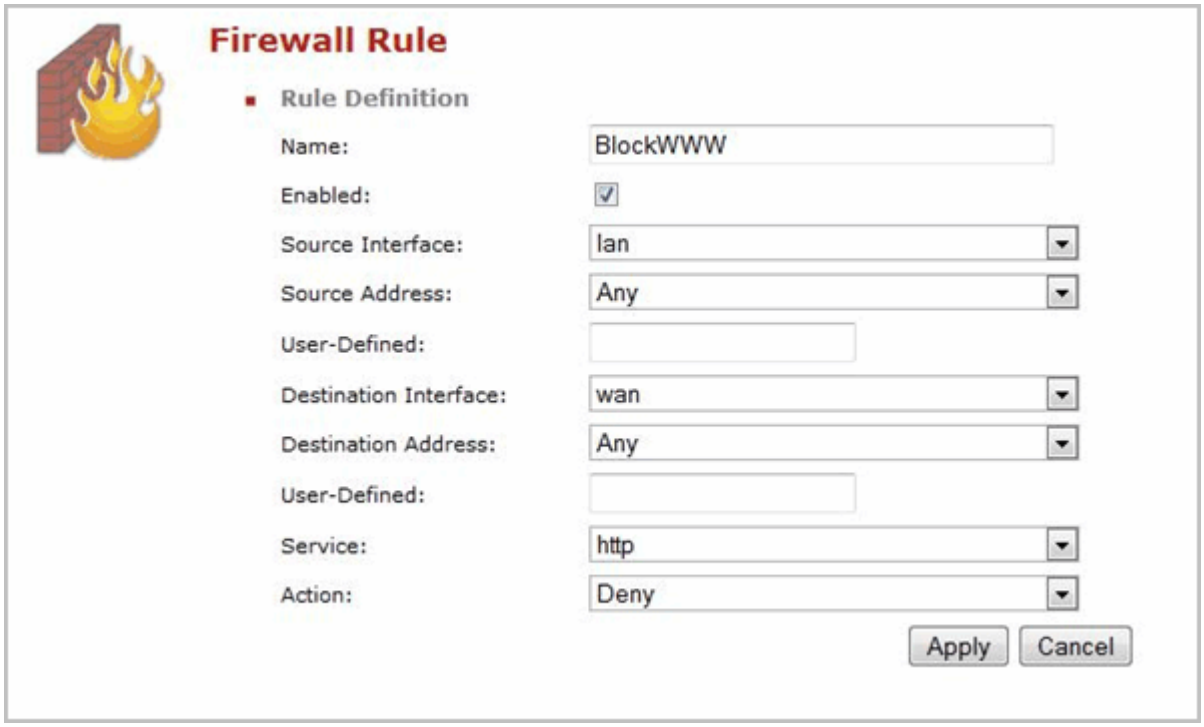
1. Open the web configuration page from an internet browser.

2. Provide any credentials required.

3. From the router's configuration web interface, click **Toolbox ► Firewall**.

4. From the **Firewall Settings,** select **Configure**.

5. Click **Add** button to add a new firewall rule.



Screenshot 57 - Thompson Wireless Broadband Router TG585 v7: Firewall Rule view

6. Key in a name in the **Name** text box, for example **"BlockWWW"**.

7. Check **Enabled** checkbox.

8. From the **Source Interface** drop-down list, select **lan**.

9. From the **Source Address** drop-down list, select **Any**.

10. From the **Destination Interface** drop-down list, select **wan**.

11. From the **Destination Address** drop-down list, select **Any**.

12. From the **Service** drop-down list, select **HTTP**.

13. From the **Action** drop-down list, select **Deny**.

14. Click **Apply** to save settings.

6.8 Disabling Internet Connections Settings on Client Machines

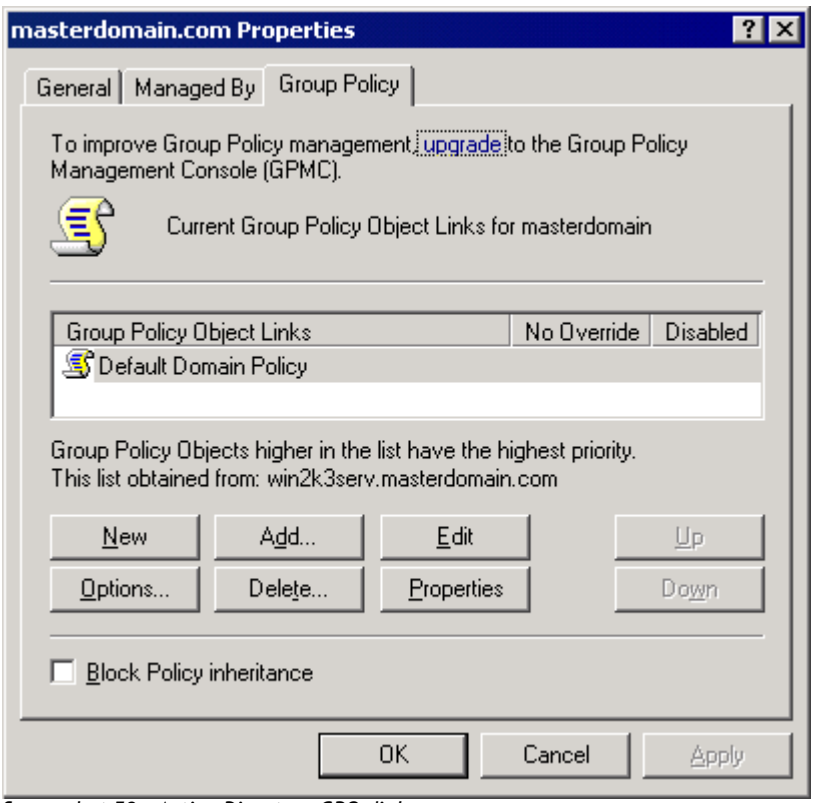
To prevent users from modifying Internet settings and thus bypassing GFI WebMonitor, the Internet **Connections** settings tab can be disabled on client machines.

6.8.1 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.

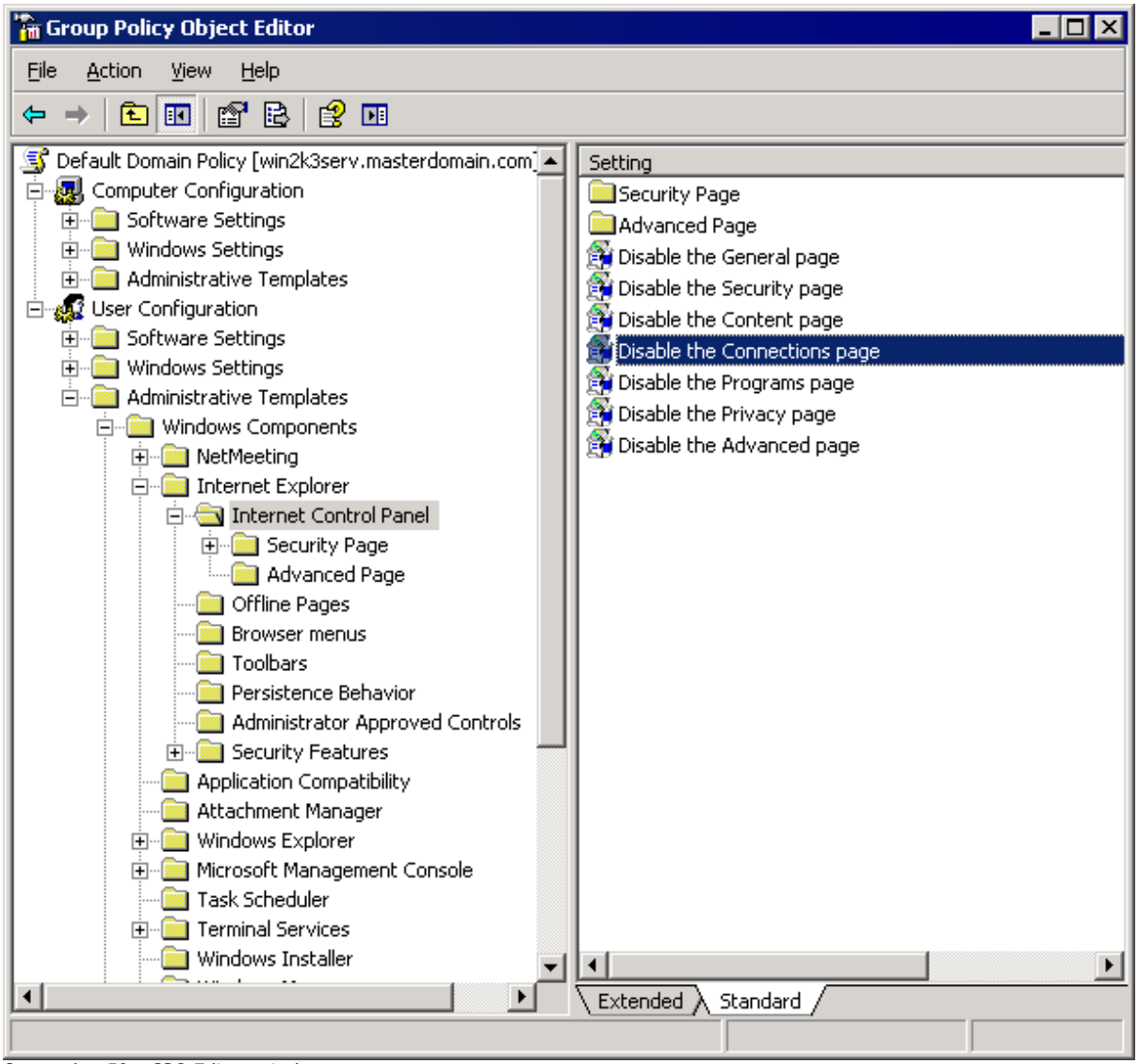
2. Right-click the domain node and click **Properties**.



Screenshot 58 - Active Directory GPO dialog

3. Select **Group Policy** tab in the **Domain Properties** dialog.

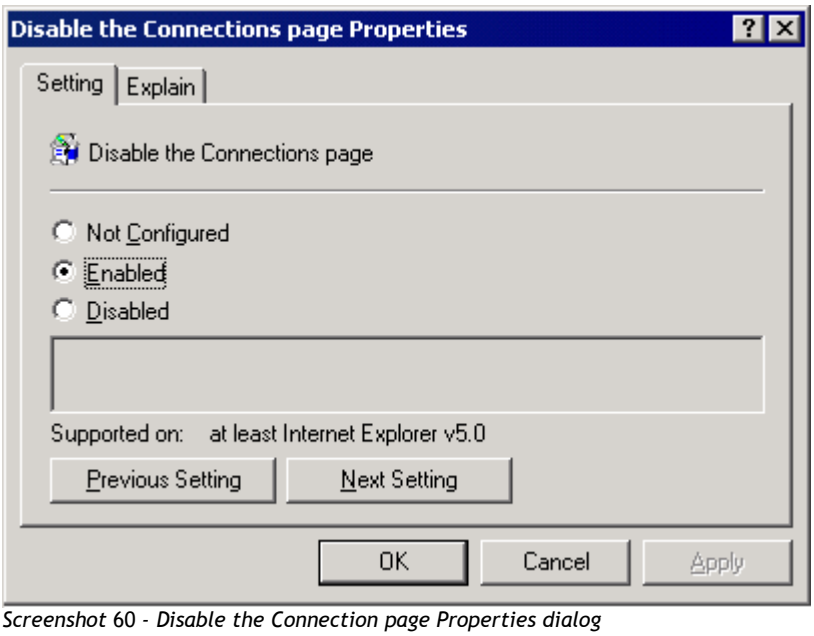
4. Select **Default Domain Policy** from the list and click **Edit**.



Screenshot 59 - 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 60 - 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**.

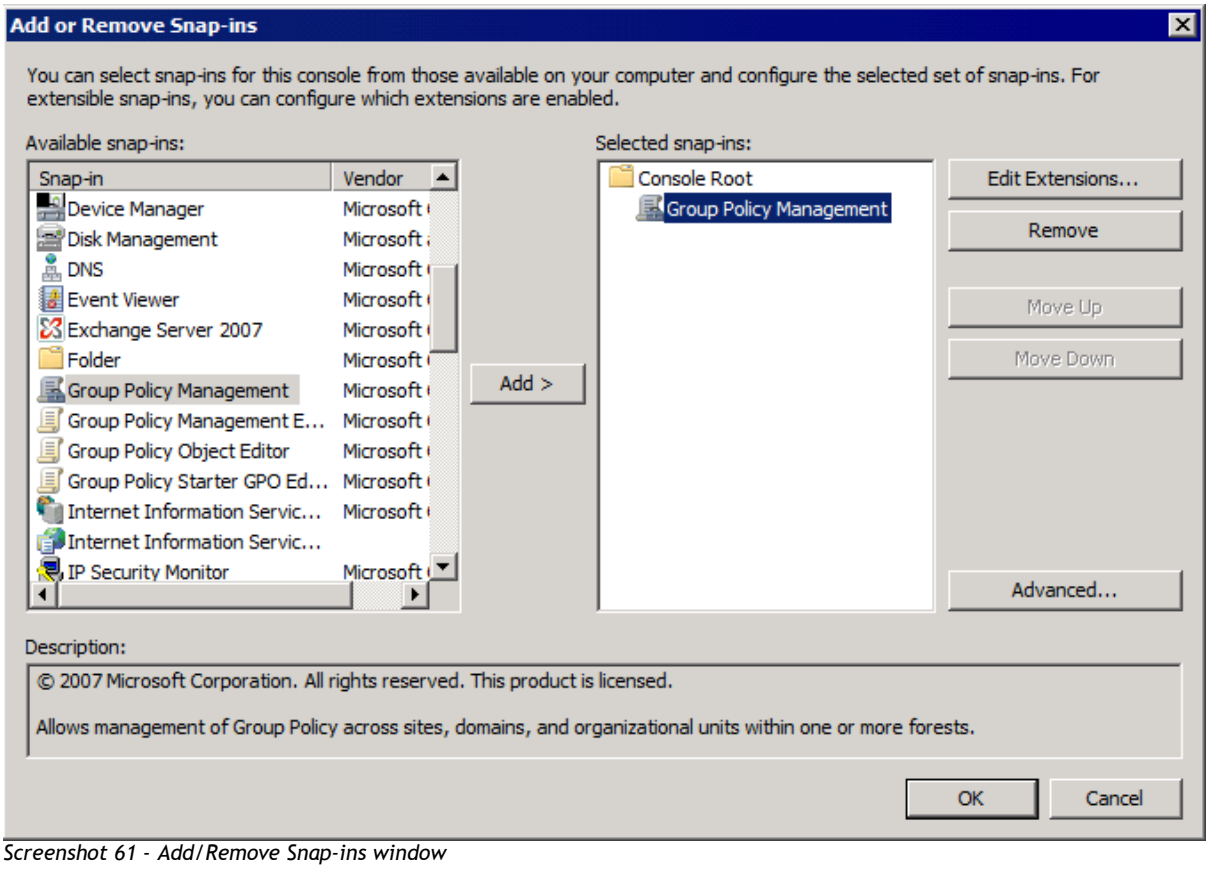
9. Close all open windows.

6.8.2 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**.

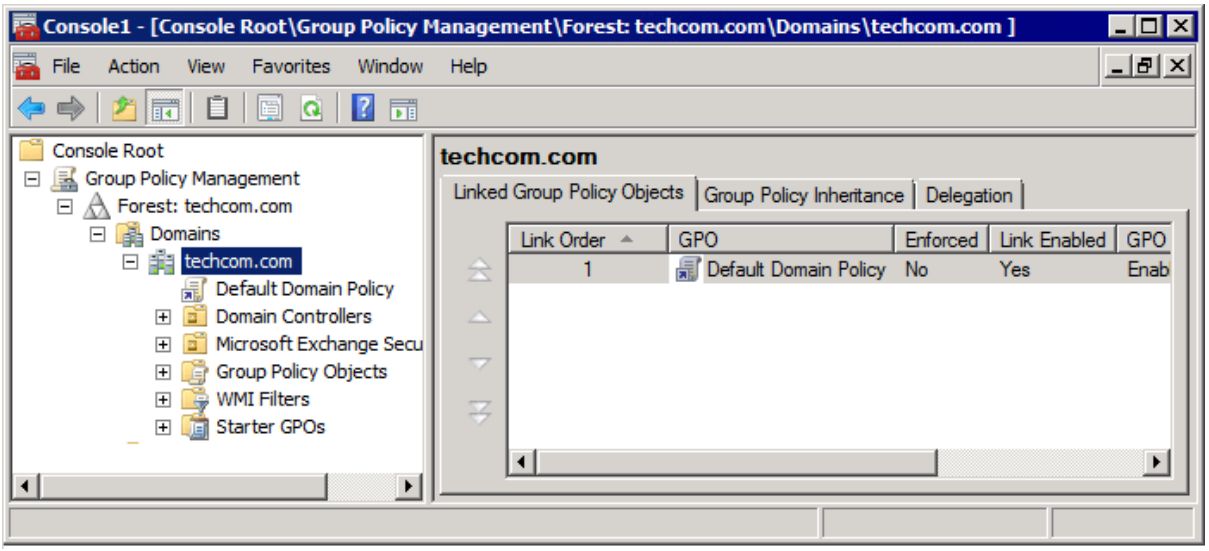
2. In the **Console Root** window, navigate to **File ► Add/Remove Snap-in…** to open the **Add or Remove Snap-ins** window.



Screenshot 61 - Add/Remove Snap-ins window

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

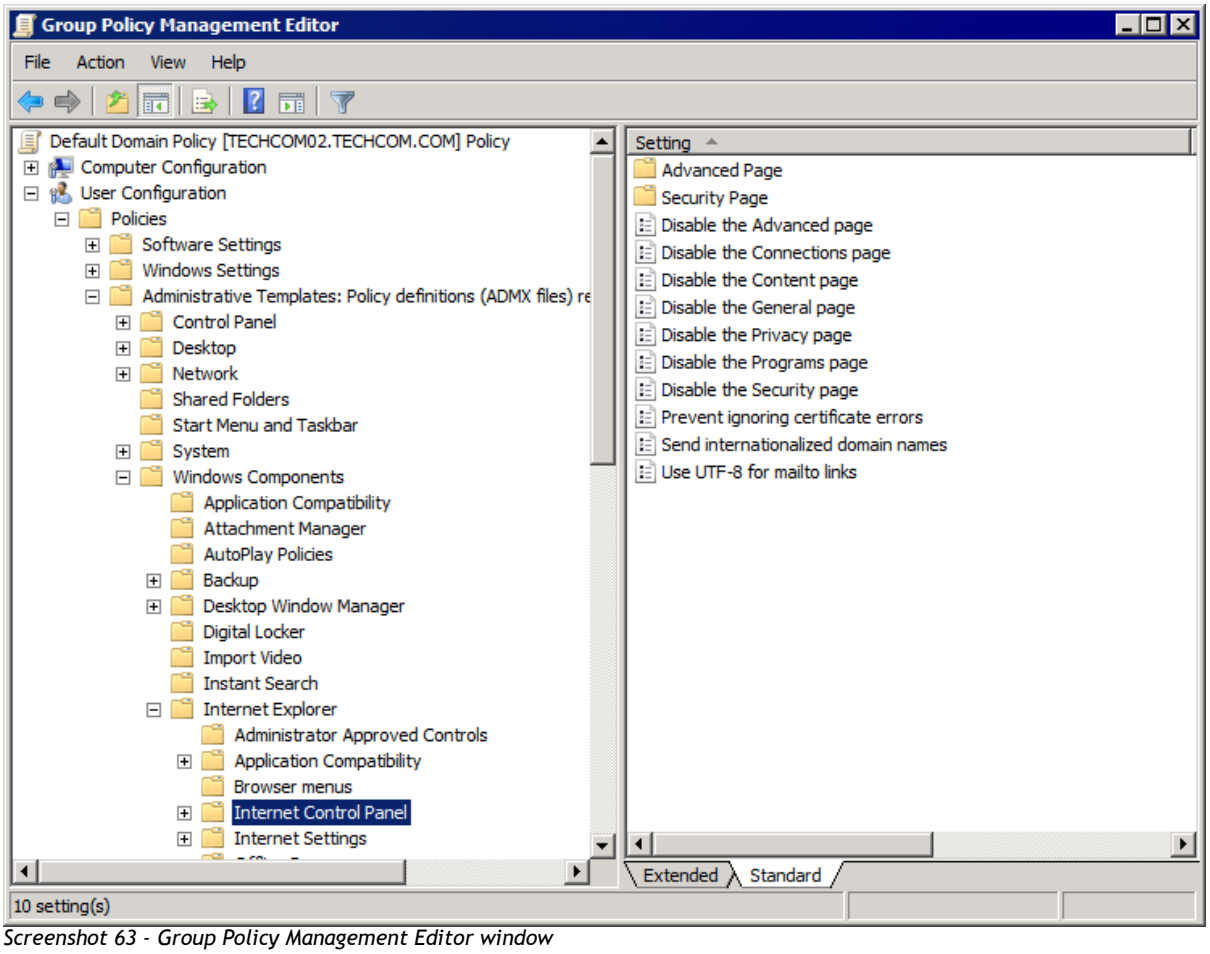
4. Click **OK**.



Screenshot 62 - Console Root domain window

5. Expand **Group Policy Management ► Forest ► Domains** and **<domain>**.

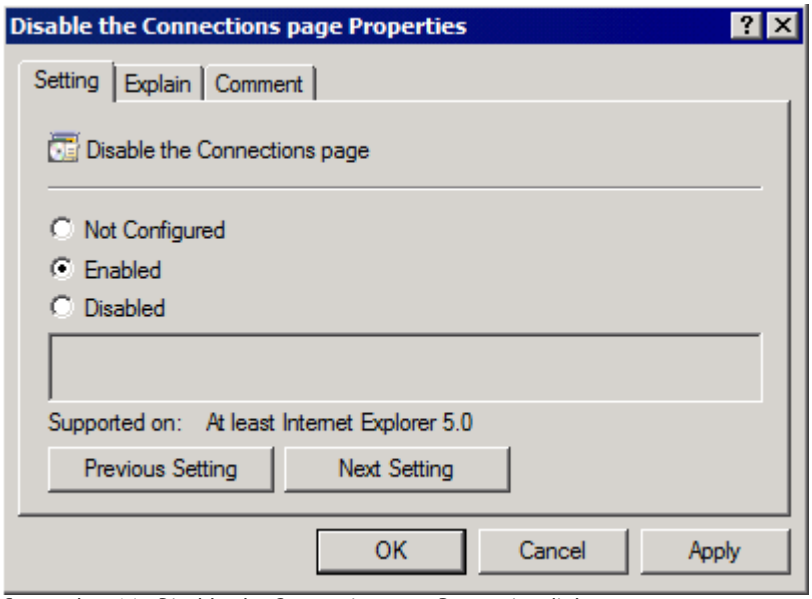
6. Right-click **Default Domain Policy** and click **Edit** to open the **Group Policy Management Editor**.



Screenshot 63 - 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 64 - 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.

6.9 Assigning Log On As A Service Rights

6.9.1 Assigning Log On As A Service Rights on Microsoft Windows XP, Microsoft Windows Vista and Microsoft Windows 7 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**.

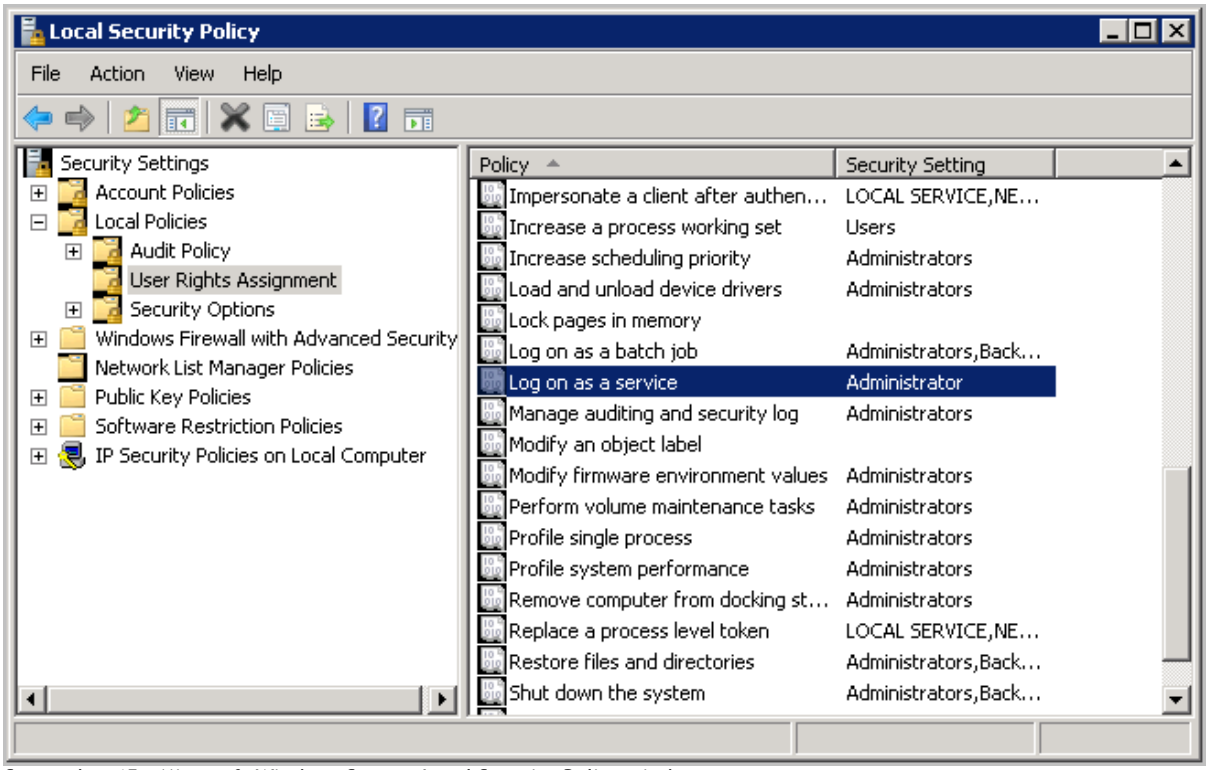
8. Close **Local Security Settings** dialog.

9. Close all open windows.

6.9.2 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 65 - 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**.

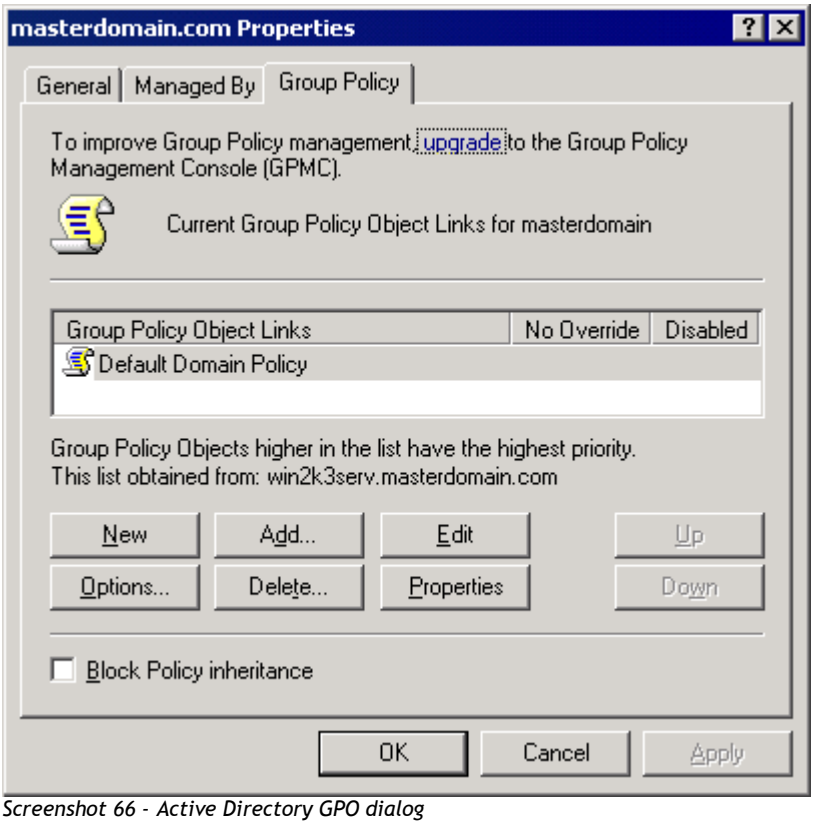
8. Close all open windows.

6.9.3 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.

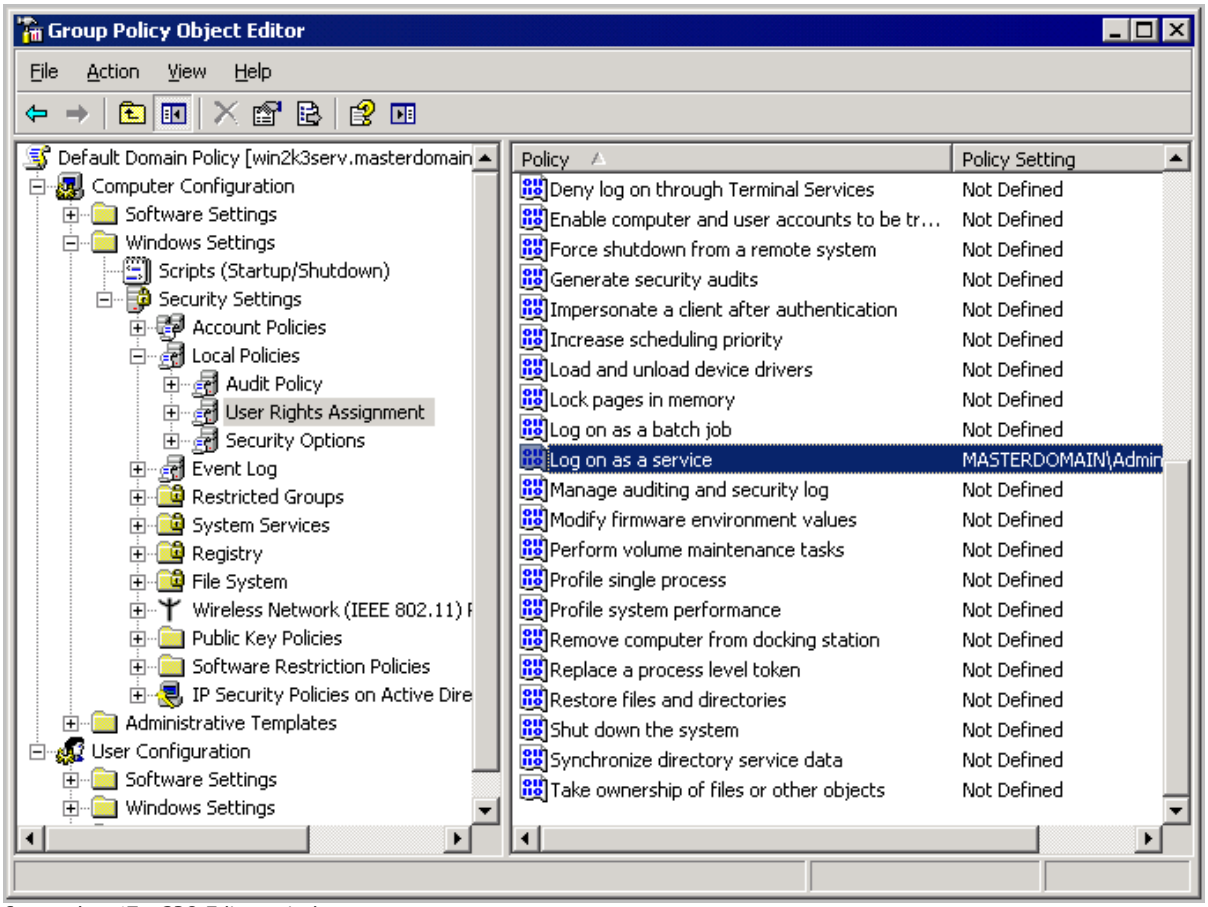
2. Right-click the domain node and click **Properties**.



Screenshot 66 - 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 67 - 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**.

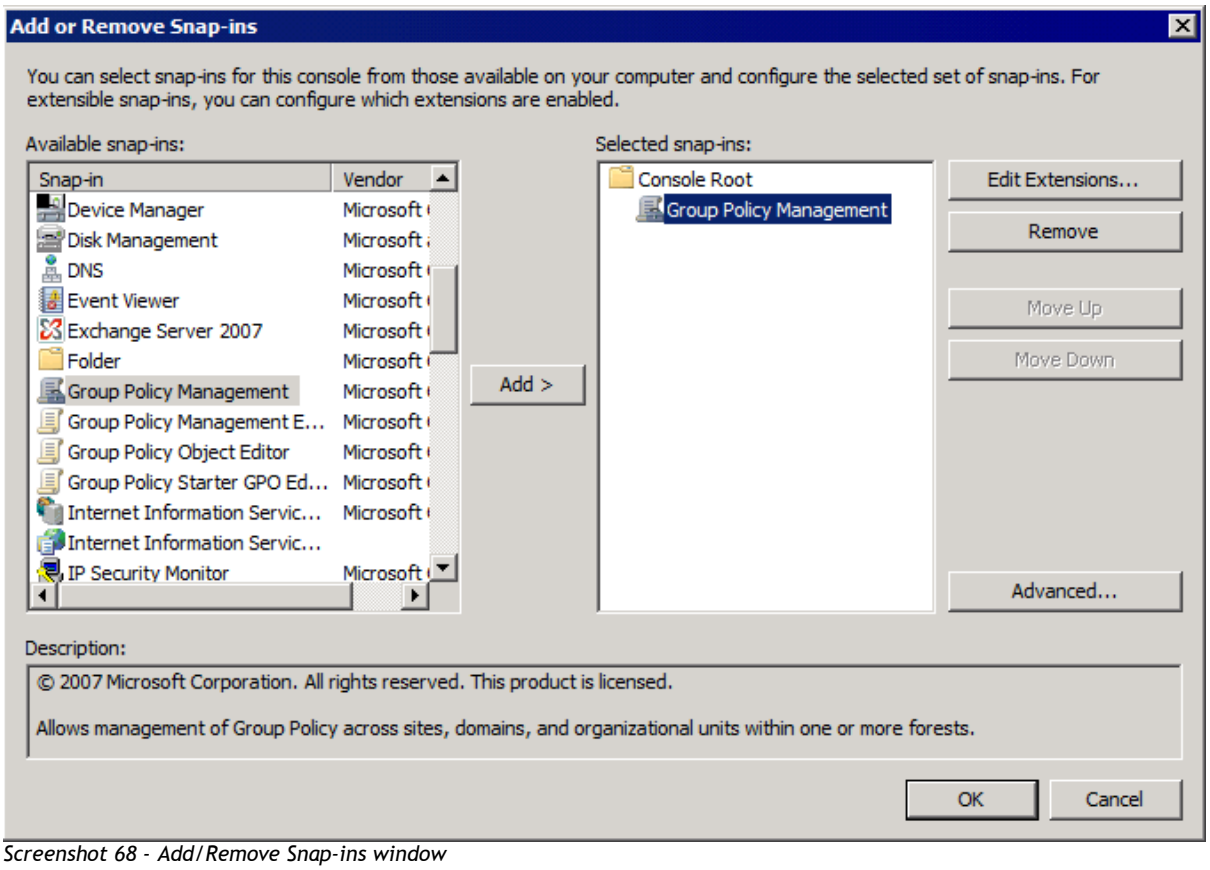
12. Close all open windows.

6.9.4 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**.

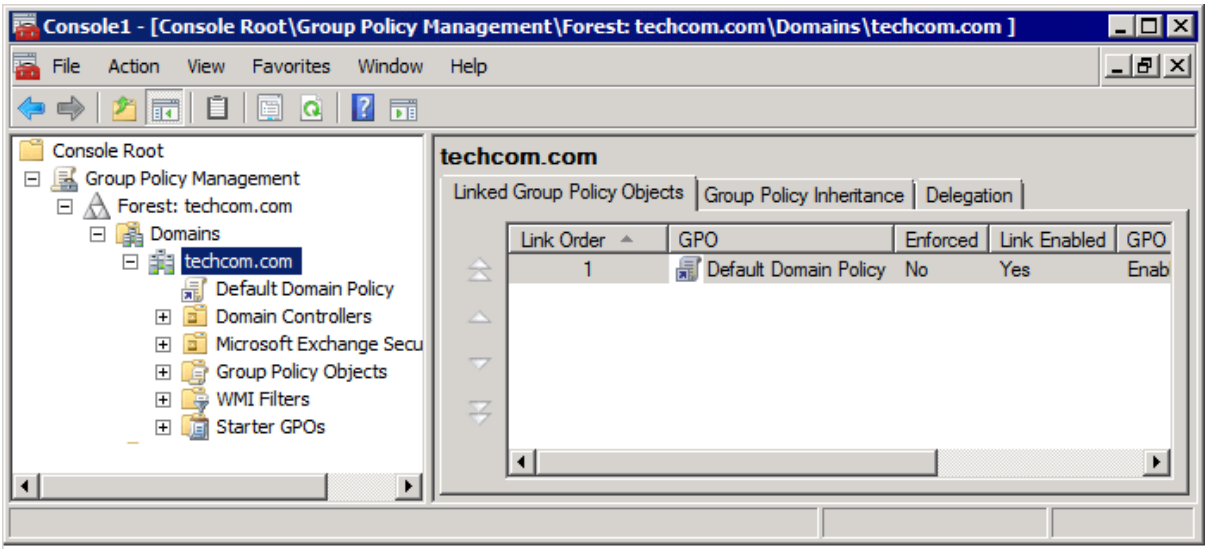
2. In the **Console Root** window, navigate to **File** ► **Add/Remove Snap-in…** to open the **Add or Remove Snap-ins** window.



Screenshot 68 - Add/Remove Snap-ins window

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

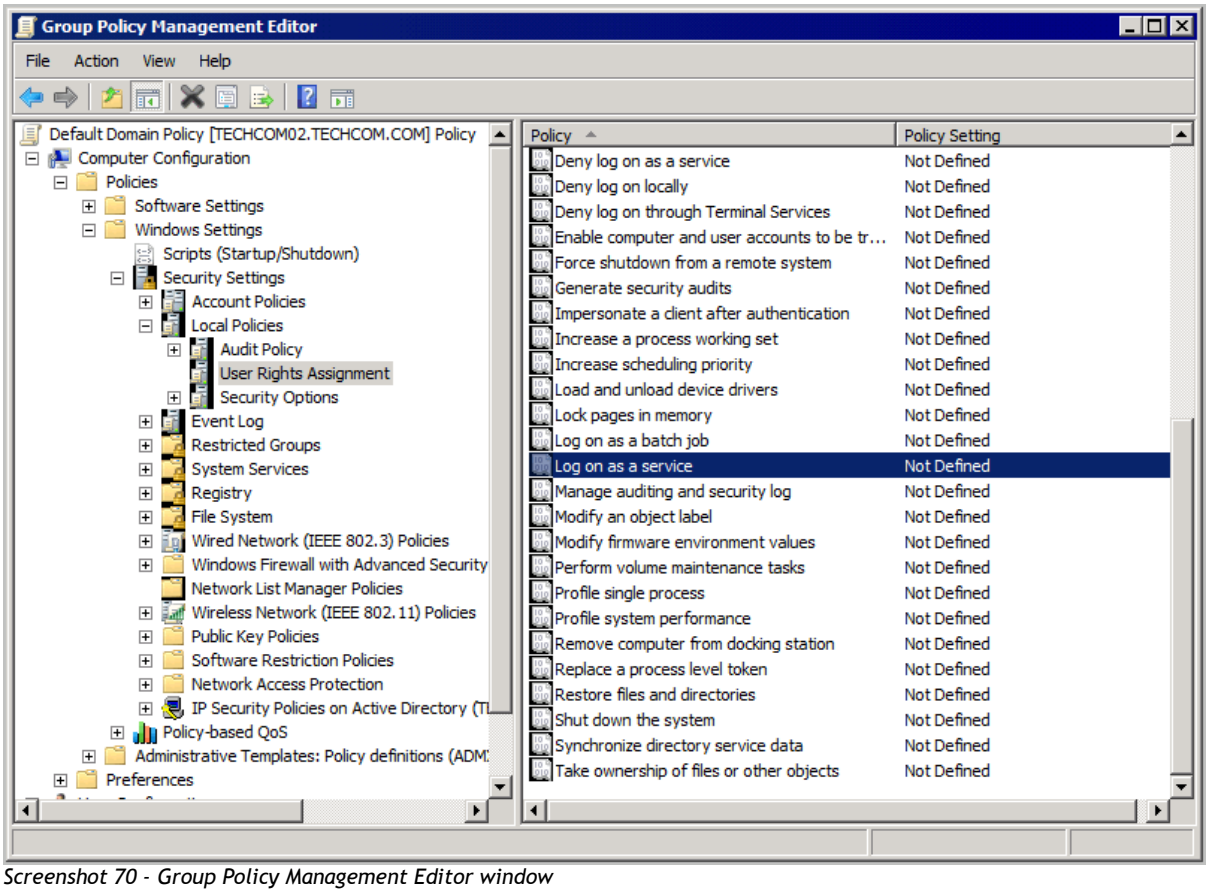
4. Click **OK**.



Screenshot 69 - 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 70 - 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.

6.10 Configuring Network Access Policy

In the **Configuration ► Proxy Settings** area, the **Integrated authentication** option is disabled on GFI WebMonitor machines where the Network access setting is set to **Guest only - local users authenticate as Guest**. On a Microsoft Windows XP Pro machine that has never been joined to a Domain Controller, this setting is set by default.

The Network access setting can be configured on each GFI WebMonitor machine:

» Manually or,

» Using Active Directory GPO.

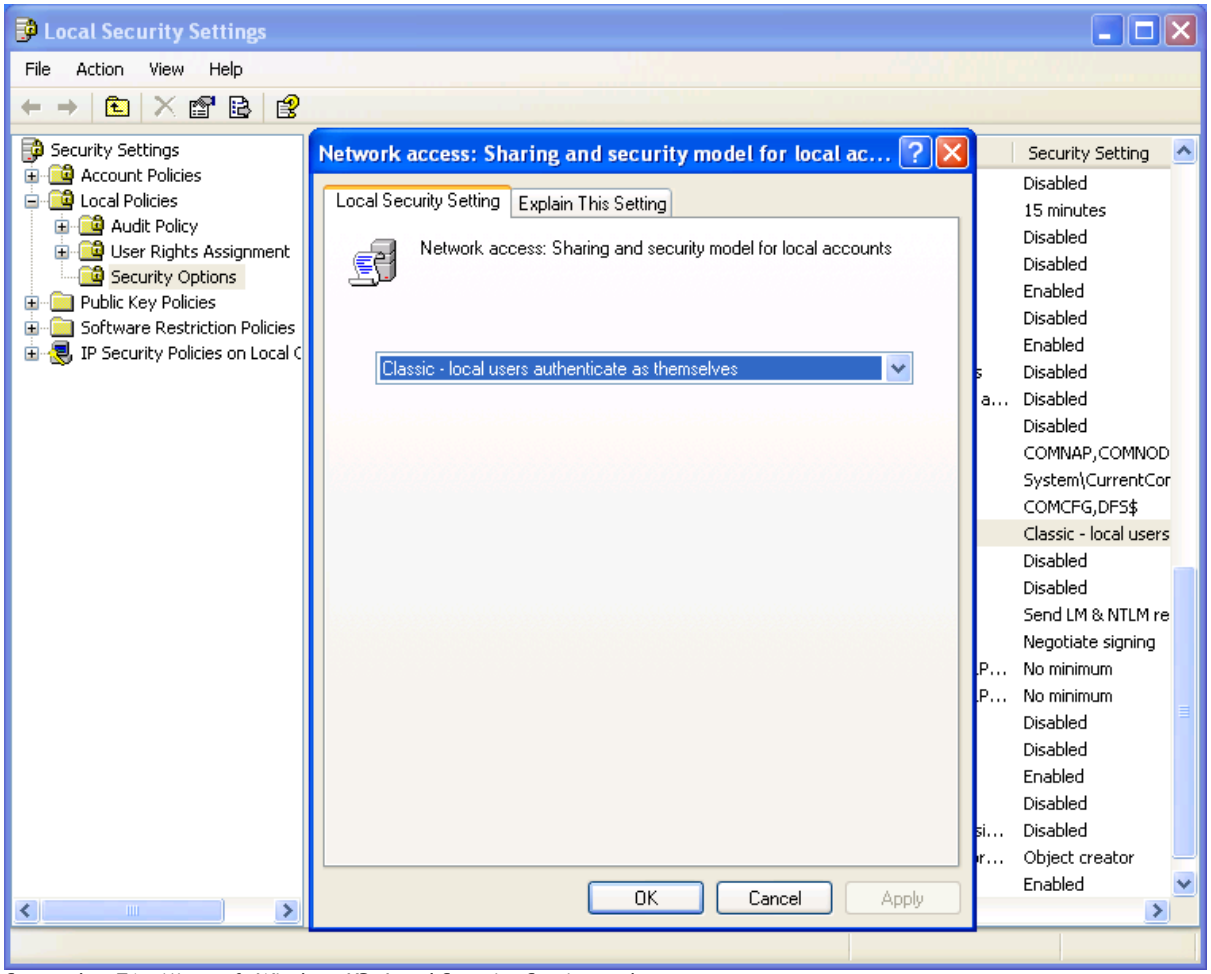
Configuring Network Access Manually

To configure **Network access** setting on a GFI WebMonitor machine manually:

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

2. Expand **Security Settings ► Local Policies ► Security Options**.

3. Right-click **Network access: Sharing and security model for local accounts** from the right panel and click **Properties**.



Screenshot 71 - Microsoft Windows XP: Local Security Settings tab

4. Select the **Local Security Setting** tab.

5. Select **Classic - local users authenticate as themselves** from the Network access drop-down list.

6. Click **Apply** and **OK**.

7. Close **Local Security Settings** dialog.

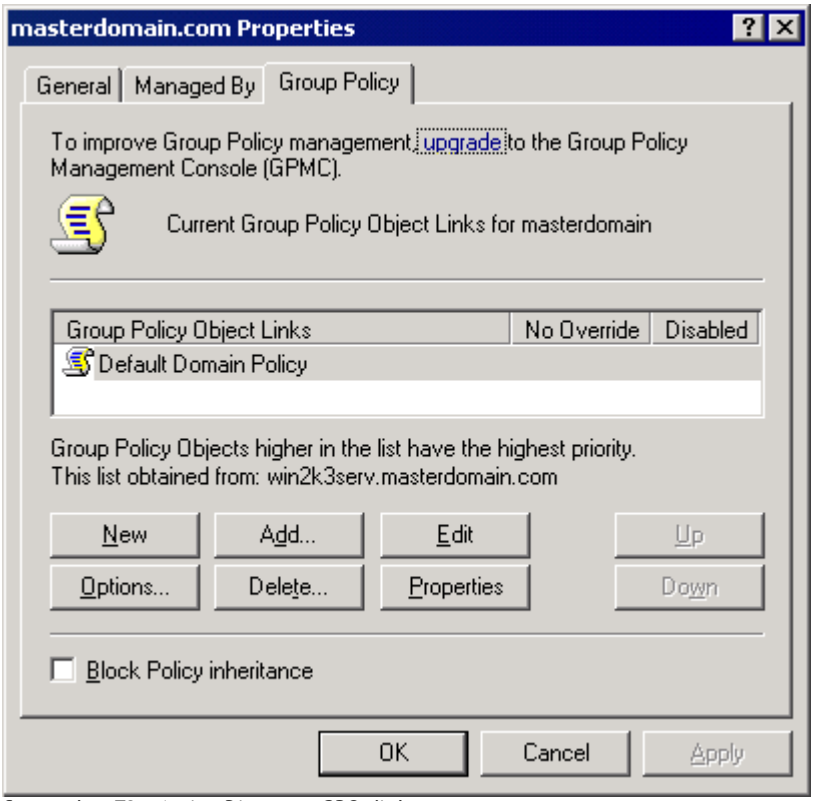
8. Close all open windows.

Configuring Network Access Using GPO in Microsoft Windows Server 2003

To configure **Network access** setting on GFI WebMonitor 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 72 - 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**.

5. Expand **Computer Configuration ► Windows Settings ► Security Settings ► Local Policies** and click **Security Options**.

6. Right-click **Network access: Sharing and security model for local accounts** from the right panel and click **Properties**.

7. In the **Security Policy Setting** tab, check **Define this policy setting** checkbox.

8. Select **Classic - local users authenticate as themselves** from the Network access drop-down list.

9. Click **Apply** and **OK**.

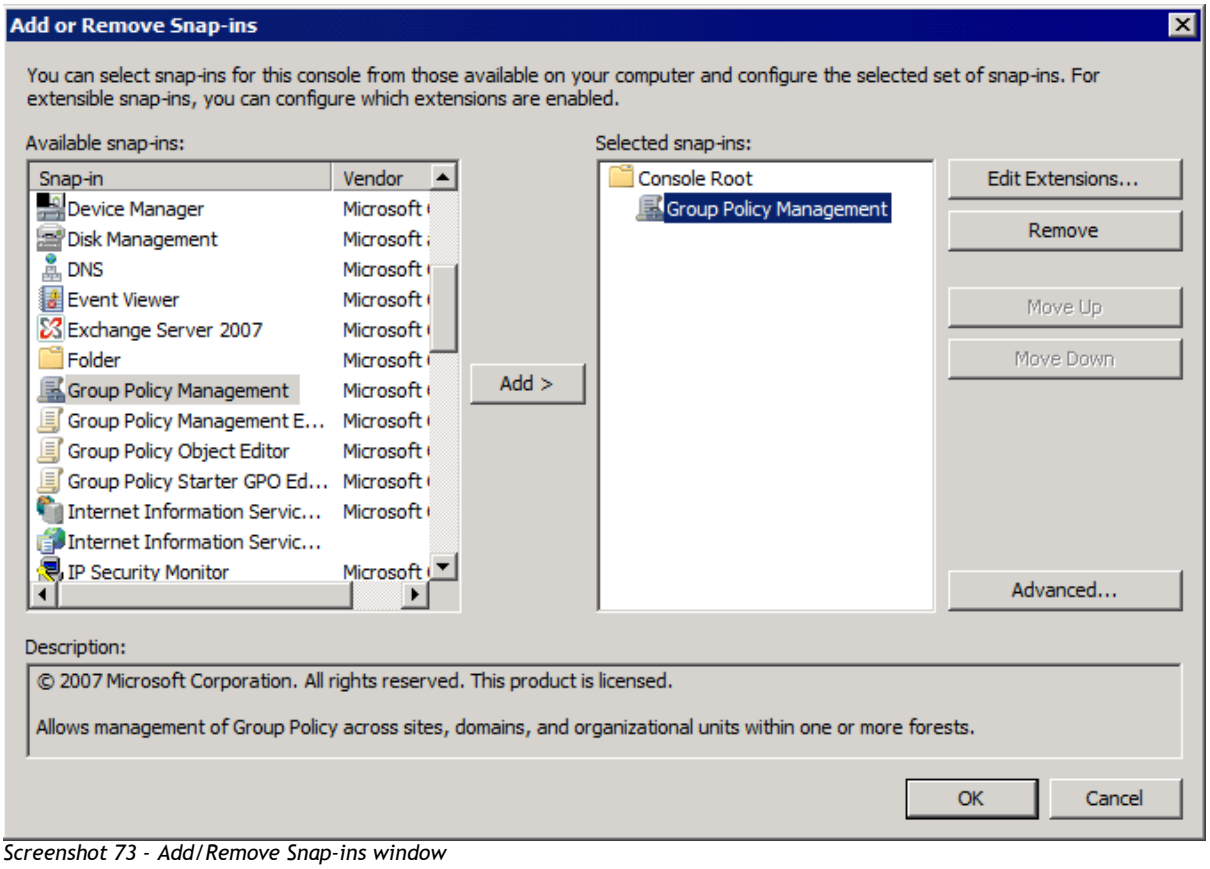
10. Close all open windows.

Configuring Network Access Using GPO in Microsoft Windows Server 2008

To configure **Network access** setting on GFI WebMonitor machines through Microsoft Windows Server 2008 GPO:

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

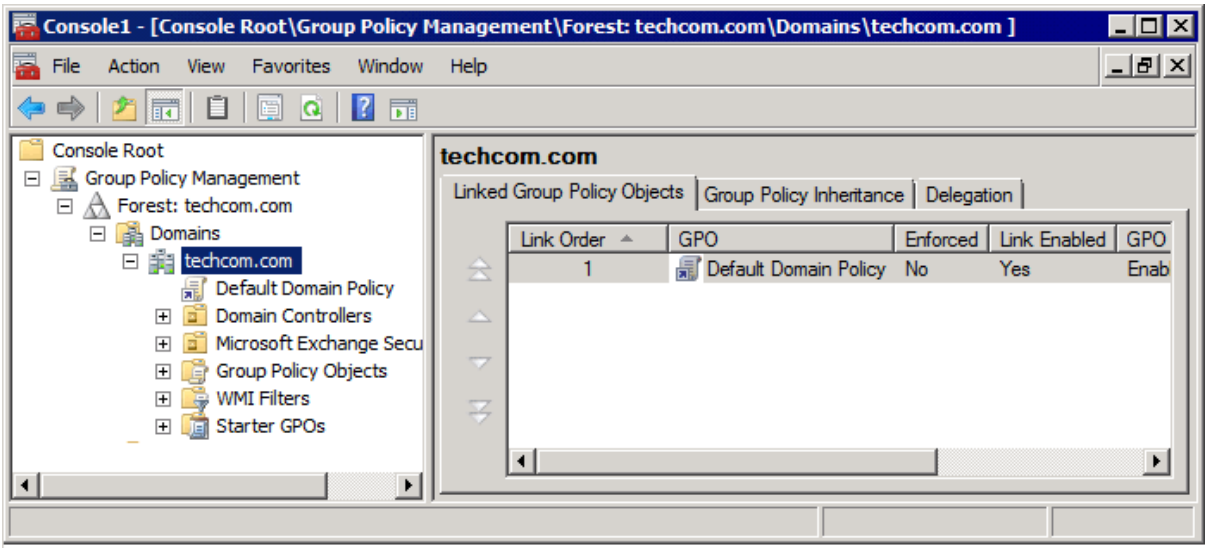
2. In the **Console Root** window, navigate to **File ► Add/Remove Snap-in…** to open the **Add or Remove Snap-ins** window.



Screenshot 73 - Add/Remove Snap-ins window

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

4. Click **OK**.



Screenshot 74 - 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**.

7. Expand **Computer Configuration** ► **Policies** ► **Windows Settings** ► **Security Settings** ► **Local Policies** and click **Security Options**.

8. Right-click **Network access: Sharing and security model for local accounts** from the right panel and click **Properties**.

9. In the **Security Policy Setting** tab, check **Define this policy setting** checkbox.

10. Select **Classic - local users authenticate as themselves** from the Network access drop-down list.

11. Click **Apply** and **OK**.

12. Close **Group Policy Management Editor** dialog and save the management console created.

This information is also available in KBase article:

http://kbase.gfi.com/showarticle.asp?id=KBID003666

7 Troubleshooting

7.1 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

7.2 Common Issues

ISSUE ENCOUNTERED	SOLUTION
Users are not able to browse and/or download from the Internet after installing GFI WebMonitor in Gateway or in Simple Proxy mode.	After the installation, GFI WebMonitor proxy machine has to be configured to listen for incoming user requests. For more information, refer to the Administration and Configuration manual. 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 the Post-installation Actions section in the **Installing in Gateway mode** chapter or refer to the Post-installation Actions section in the **Installing in Simple Proxy mode** chapter as applicable. 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 Microsoft Windows Firewall, refer to http://kbase.gfi.com/showarticle.asp?id=KBID003879
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 **Refresh cached Internet Explorer settings** section within the **Miscellaneous** chapter in GFI WebMonitor **Getting Started Guide**. Or visit: http://technet.microsoft.com/en-us/library/cc302643.aspx
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 Microsoft Windows XP Pro machine that has never been joined to a Domain Controller and where the Network access setting is set to **Guest only - local users authenticate as Guest**. For more information, refer to the Configuring Network Access Policy section in the Miscellaneous chapter.

ISSUE ENCOUNTERED	SOLUTION
Users using Mozilla Firefox browsers are repeatedly asked to key in credentials after installing GFI WebMonitor in Gateway or in Simple Proxy mode.	The server and the client machine will use NTLMv2 for authentication when: » GFI WebMonitor is installed on Microsoft Windows Server 2008 and LAN Manager authentication security policy is defined as **Send NTLMv2 response only** and » The client machine LAN Manager is not defined (this is the default setting in Microsoft Windows 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 (Microsoft Windows Server 2008)**: 1. Navigate to **Start ► 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. **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://kbase.gfi.com/showarticle.asp?id=KBID001782

7.3 Knowledge Base

GFI maintains a comprehensive Knowledge Base repository that 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/.

7.4 Web Forum

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

7.5 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.

7.6 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.

8 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 that 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

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