GFI WebMonitor

Manual

By GFI Software Ltd.

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

Version 3.0 – Last updated November 24, 2005

Contents

Introduction

What is GFI WebMonitor for ISA Server?

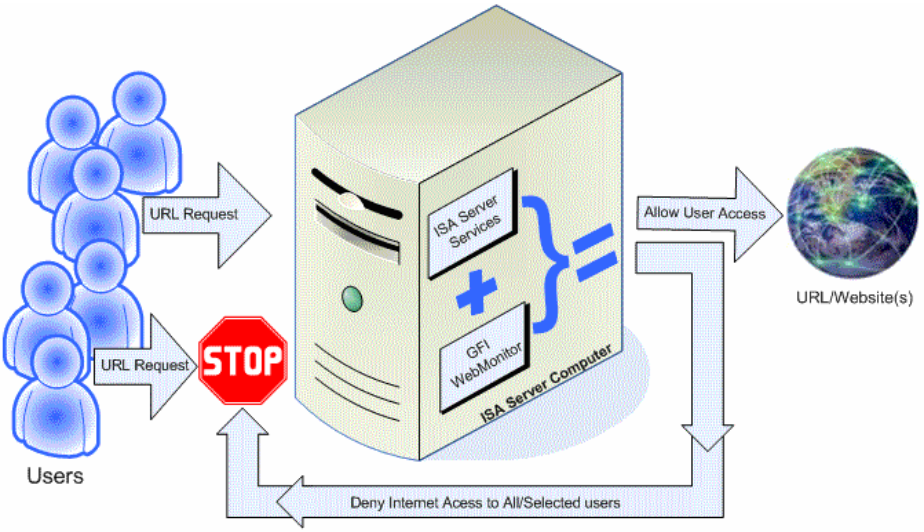


Figure 1 - GFI WebMonitor complements the protection already provided by the ISA Server

GFI WebMonitor is a lightweight monitoring tool, designed as a plug-in for Microsoft ISA Server. It allows you to monitor the sites users are browsing and the files they are downloading – in REAL-TIME. It also allows you to block web connections in progress as well as to scan traffic (i.e., downloaded objects) for viruses, Trojans and spyware.

GFI WebMonitor is the perfect solution to transparently exercise a degree of control over users' browsing habits and to ensure legal compliance – in a manner that will not alienate your network users.

Features

- Monitors web and FTP browsing in real-time.
- Allows administrators to block web access or downloads in progress.
- Active Connection view shows all current web connections.
- URL History view shows all visited websites.
- User History view shows all sites visited by each user.
- All views show the number of bytes transferred (sent/received).
- Native integration with ISA Server as a web filter.
- Web-based interface allows viewing from anywhere in the network.
- Supports Microsoft ISA Server 2000/2004 (both Standard and Enterprise Editions).
- Easy installation, minimal configuration required.

- Does not duplicate functionality already present in MS ISA Server.
- Site Rating - Proactive assisted real-time content filtering - GFI WebMonitor checks URLs for adult content through the Yahoo! SafeSearch™ categorization engine. Yahoo! SafeSearch™ is an online database which classifies and categorizes various sites on the Internet. GFI WebMonitor queries this database to detect sites with adult content. With GFI WebMonitor and Yahoo! SafeSearch™ database querying, your administrative overhead to keep your web filters up-to-date (with new adult sites opened) is obsolete.
- Web Traffic Scanning - Scanning downloaded content via HTTP and FTP for viruses using one or more virus scanning engines. GFI WebMonitor supports three virus scanning engines; BitDefender, Kaspersky and Norman.
- Real filetype signature check - GFI WebMonitor performs real filetype signature checks on all HTTP/FTP files being downloaded. Filetype signatures are a short series of bytes that define the true type and content of a file. GFI WebMonitor will detect and block dangerous/unauthorized files based on their filetype signature (i.e. blocking of documents or executables based on their file signature rather than on their declared file extension).
- Automatic anti-virus definition updates - GFI WebMonitor periodically checks and downloads new anti-virus definitions for its virus scanning engine(s). The frequency at which GFI WebMonitor checks for virus definition updates is customizable from GFI WebMonitor configuration interface.
- Email Notifications – On the occurrence of important events, GFI WebMonitor will send out administrative alerts via email notifications to a target recipient. Important events include:
  - Failed updating of the virus definition files used by the virus scanning engine(s).
  - Approaching of anti-virus license expiry.

Proactive content filtering and Access Control

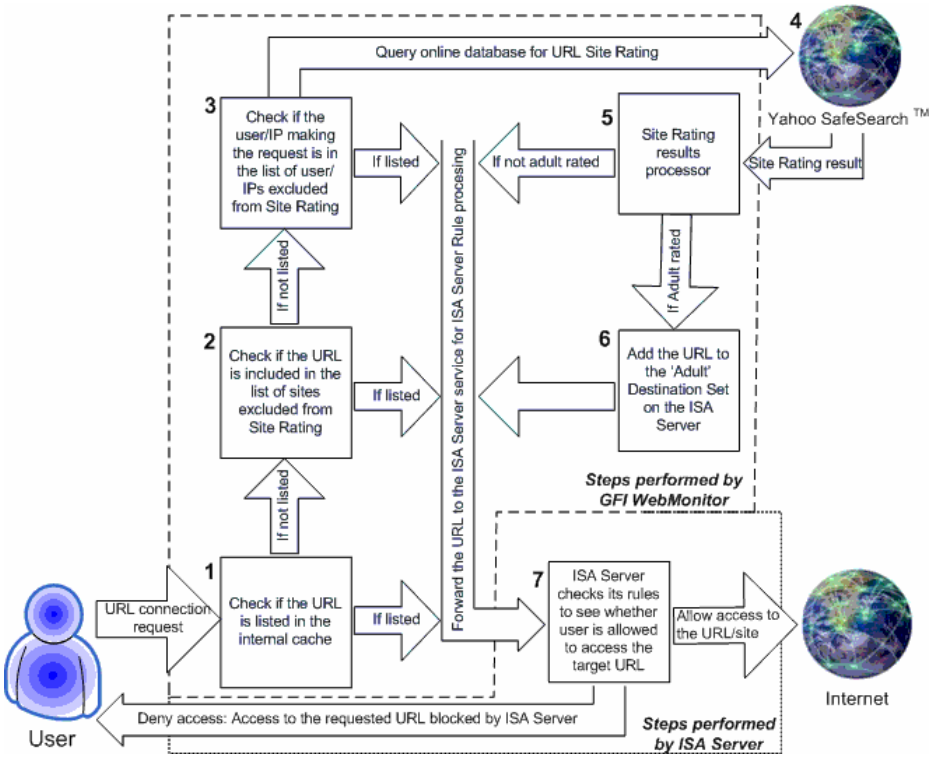


Figure 2 - Site Rating process flow

GFI WebMonitor can check for adult content in the URLs which users want to access. This is achieved by querying Yahoo! SafeSearch™ which is an online database that classifies and categorizes various sites on the Internet. When a user requests access to a site, GFI WebMonitor will query the Yahoo! SafeSearch™ database for the Content-Type held by that target URL. If the online web filter classifies the site as having adult content, GFI WebMonitor will add the target URL to the 'Adult' Destination Set on the ISA Server. If the ISA Server is configured to block access to the sites listed in the 'Adult' Destination/URL Set the user will be denied access to that site.

The benefits of a web-based content filter

It is estimated that three to five million websites are newly established or renamed each week. This means that administrators strive to maintain their local content filter databases updated. Missing one update might jeopardize the accuracy of a content filtering system.

GFI WebMonitor performs content filtering through a web-based filter and does not require a locally maintained filter database. All the required filter data is stored on the remote online database which is constantly maintained and updated by third-party content classification professionals. The benefits of using a web-based content filter include:

- Automatically updated and maintained URL block list.
- No local updates required - This reduces administrative loads by eliminating bothersome list updating procedures and research.
- Adult sites are notoriously known for being accompanied by unwanted spyware/Trojan installations. Through an automatically managed adult site list you reduce the chances of your users

opening holes in your network through the installation of unwanted software and ActiveX controls which frequently accompany visited adult sites.

- Less bandwidth is consumed on non-work related browsing.
- Less demand for local storage space - Less physical storage space is required locally to host a detailed and up-to-date content filter database which is continuously increasing in size. GFI WebMonitor will store only the blocked URLs which were requested by the company's internal users; as opposed to the Yahoo! SafeSearch™ filter database which includes the URLs of all sites that were accessed by a multitude of users around the world.

Web Traffic Scanning

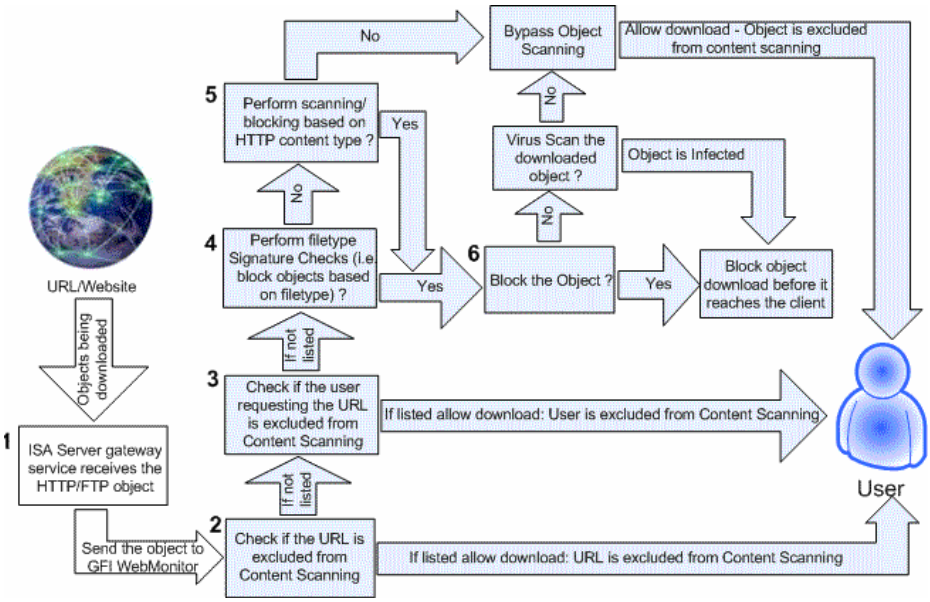


Figure 3 - Web Traffic Scanning

GFI WebMonitor can optionally perform Web Traffic Scanning. During Web Traffic Scanning, downloaded objects are checked for viruses, spyware and Trojans using the supported virus scanning engines. The paid version of GFI WebMonitor comes enabled with Norman and BitDefender free for the first year. Kaspersky can be added on for an additional charge. During Web Traffic Scanning, the virus scanner(s) inspect all HTTP and FTP (only FTP passing via HTTP proxy server) traffic going through the monitored ISA Server. Web Traffic Scanning blocks all infected files before reaching the client.

Dangerous files (filetypes) such as Trojan downloader programs often attempt to penetrate a system masked as innocuous files. During Web Traffic Scanning, GFI WebMonitor uses its built-in file signature scanner to analyze the signatures of HTTP/FTP files. Filetype signatures are bytes which define the true type and content of a file. GFI WebMonitor will immediately block dangerous filetypes before reaching the client.

For more information on filetype signatures visit: http://www.garykessler.net/library/file_sigs.html.

Installing GFI WebMonitor

GFI WebMonitor system requirements

- Microsoft Windows 2000 (SP 3) or 2003 Server.
- Microsoft ISA Server 2000 (not in firewall only mode) OR Microsoft ISA Server 2004 (Standard or Enterprise).
- Microsoft .NET Framework version 1.1.
- Microsoft Internet Explorer to access GFI WebMonitor.
- 20 MB free hard disk space.

Installing GFI WebMonitor

Before you install GFI WebMonitor for ISA Server, make sure:

- You are logged on as an administrator (or any account having administrative privileges) on the domain or computer(s) where GFI WebMonitor is being installed.
- You have Windows 2000/2003 Server and Microsoft ISA Server 2000/2004 installed and running.
- You have Microsoft .NET Framework version 1.1 installed on the computer(s) on which you will be running GFI WebMonitor. For more information on how to download, install or check if Microsoft .NET Framework 1.1 is running on your computer(s) visit http://msdn.microsoft.com/netframework/downloads/framework1_1/#section1.
- You do not have GFI DownloadSecurity installed on the same machine on which you will be running GFI WebMonitor.
- You close any other Windows application that is running on the computer where GFI WebMonitor is to be installed.

NOTE: GFI DownloadSecurity and GFI WebMonitor make use of common services and libraries (dlls, etc.). This may cause both software to conflict and perform incorrectly if installed and run simultaneously on the same computer. It is recommended that you uninstall GFI DownloadSecurity before installing GFI WebMonitor.

1. Logon to your ISA Server and launch GFI WebMonitor installation wizard by double clicking on **webmonitor3.exe**.

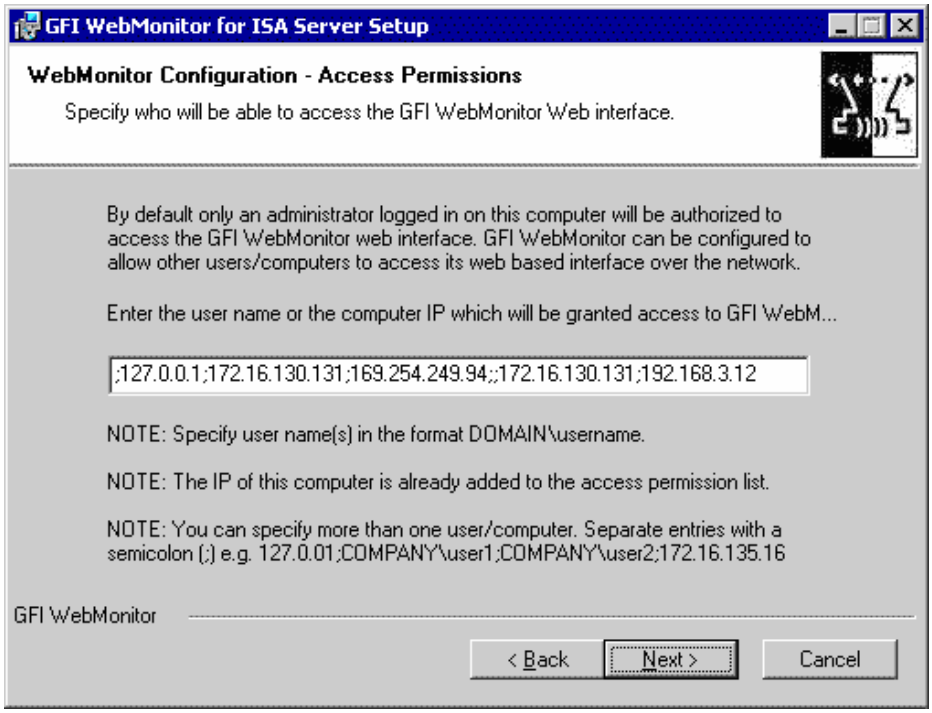
2. As soon as the welcome dialog appears click on **Next** to start the installation process.

3. Choose whether you want the installation wizard to check for a newer version of GFI WebMonitor on the GFI website. Click on **Next** to continue.

4. Read the license agreement. Select 'I Accept the Licensing agreement' and click on **Next** to continue.

5. Choose whether you want to make a clean install or import the settings of a previously installed build/version of GFI WebMonitor into the new installation. Click on next to continue.

NOTE: This dialog is shown only when installing on a computer where GFI WebMonitor was already installed.



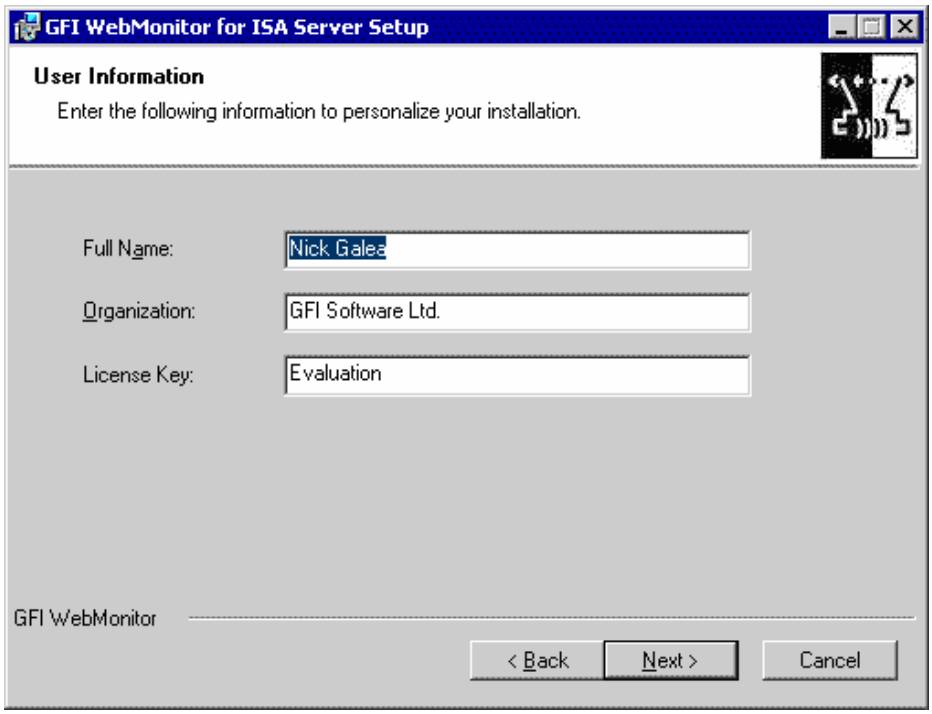
Screenshot 1 - Configuring access at installation

6. Specify the username(s) or IP address of the computer(s) that will be allowed to use and configure GFI WebMonitor. You can specify multiple IPs or usernames by separating them with ";" (e.g., 209.217.53.213**;**66.172.16.32**;**JasonM.)

NOTE 1: Only the IPs/Users specified in this dialog will have access (locally or remotely) to GFI WebMonitor interface.

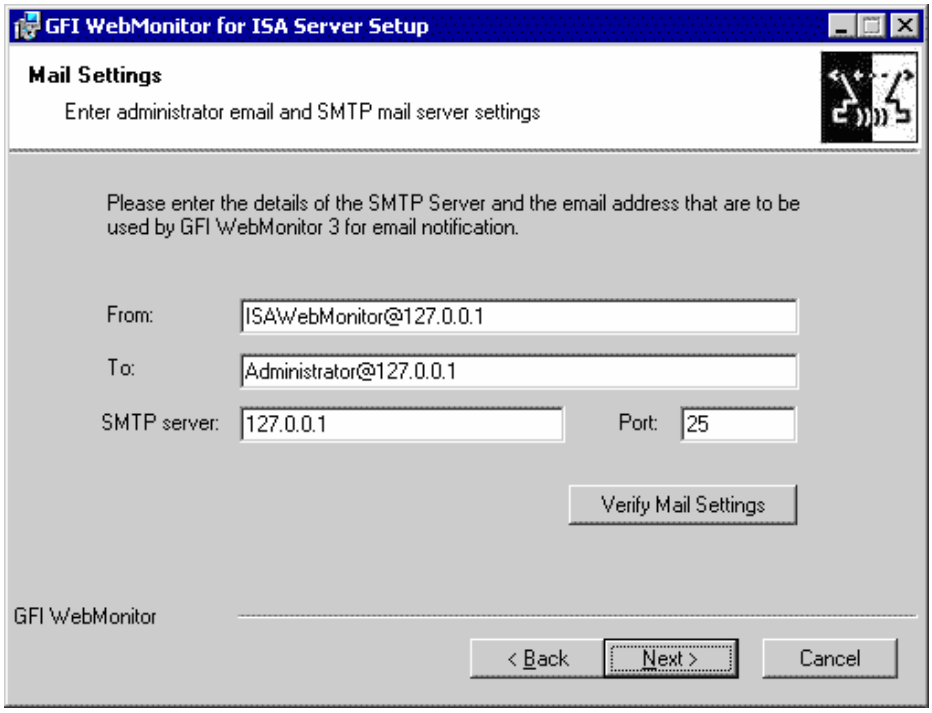
NOTE 2: After installation you can configure GFI WebMonitor to authorize other users to access GFI WebMonitor interface from the Configuration ▸ Access Permissions node. For more information on how to configure user access permissions, refer to the 'Accessing GFI WebMonitor' chapter.

NOTE 3: By default only the administrator on the ISA Server machine will have access to GFI WebMonitor configuration.



Screenshot 2 - Entering User Information

7. Specify the full username, the company name and the license key. If you are evaluating the product, leave the evaluation key as default (i.e., “Evaluation”). Click on **Next** to continue**.**



Screenshot 3 - Entering email notification details

8. Specify the SMTP/mail server details (Hostname/IP and Port) as well as the recipient where email notifications on important events will be sent. Click on **Next** to continue.

NOTE: After installation, you can change these settings from the Configuration ▸ General Options node.

9. Specify the installation path for GFI WebMonitor and click on **Next** to continue.

10. Click on **Next** to finalize the installation.

NOTE: If you will be using the Site Rating features of GFI WebMonitor you will need to create a user access policy on the ISA Server which blocks access to the URLs contained in the 'Adult' Destination/URL Set created on the ISA Server by the installation. Refer to the 'Access policy for adult sites on the ISA Server' section.

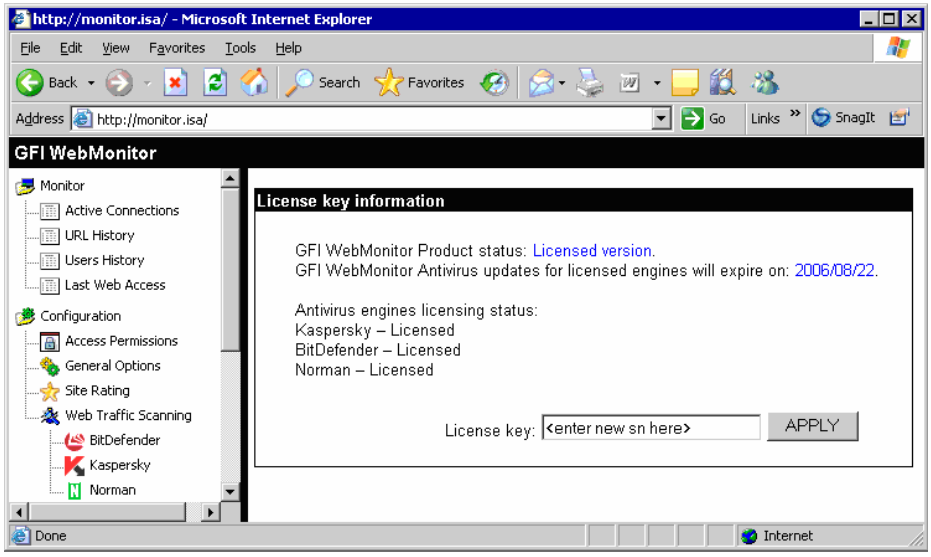
Access policy for adult sites on the ISA Server

To block users from accessing adult-rated sites you need to create an access policy rule on your ISA Server which blocks access to the URLs contained in the 'Adult' Destination/URL Set.

When the Site Rating feature is turned on, the Site Rating Processing Engine of GFI WebMonitor will add the URLs which contain adult material to the 'Adult' Destination/URL Set.

Follow the procedure described in the topic 'Creating ISA Server access policy rules' contained in the 'Common ISA Server Setup Tasks' chapter to create an access policy rule on your ISA Server which will block all users from accessing the sites listed in the 'Adult' Destination/URL Set managed by GFI WebMonitor.

Entering your license key after installation



Screenshot 4 - Viewing license information

By default, GFI WebMonitor has an unrestricted fully functional evaluation period of 10 days. If the data you provided in the download form is correct, you will receive by email a license key which enables you to evaluate GFI WebMonitor for 30 days.

If after the evaluation period you decide to purchase GFI WebMonitor, you do not have to re-install or reconfigure the product. Just enter your new License key in the General ▸ Licensing node. To find out how to buy GFI WebMonitor, click on the General ▸ How to purchase node.

NOTE 1: During evaluation you can use the General ▸ Licensing node to see how many evaluation days are remaining.

NOTE 2: You must license GFI WebMonitor for the number of computers that will connect to the ISA Server for Access Control and monitoring. If you will be installing on multiple ISA Servers you will need a license for each installation.

NOTE 3: Entering the license key should not be confused with the process of registering your company details on our website. This is important, since it allows us to give you support and notify you of important product news. Register on: http://www.gfi.com/pages/regfrm.htm

Advanced GFI WebMonitor deployments

The installation and usage of GFI WebMonitor always follows the same paths and procedures. Install GFI WebMonitor, open Internet Explorer and access the configuration and monitoring interface through the following URL: http://monitor.isa. The ISA Server which picks up the request will respond.

In the case of multiple routed ISA Server installations you need to manually edit a file so that the various GFI WebMonitor download windows will not interfere with each other. This is achieved by overwriting the default http://monitor.isa URL with a dedicated real/virtual IP which will clearly identify GFI WebMonitor making the request as well as identify which download window is to process the reply.

Deploying and using GFI WebMonitor on multiple ISA Servers or ISA Server arrays

1. Install GFI WebMonitor on each of the ISA Server computers that you want to monitor.

2. On each GFI WebMonitor deployment use Notepad (or an HTML editor) to open the **DownloadingPage.html** file located in GFI WebMonitor installation directory. Change the address contained in the following variables to a real/virtual IP address that is routable via the ISA Server on which you are making the change. E.g., http://130.168.0.1:

- "**ThisISAServerAddress**" variable which is set by default to **http://monitor.isa**.
- "**SecondISAServerAddress**" variable containing an IP address which is set by default to **http://1.1.1.1**. This variable must contain the same value that has been specified for the "**ThisISAServerAddress**" variable.

NOTE: Assign IP addresses to both of the above mentioned variables in order to avoid configuration problems.

3. After you have completed all the required changes, restart all ISA Servers where GFI WebMonitor is installed (i.e., the ISA Servers where the changes to the **DownloadingPage.html** have been made).

4. To open GFI WebMonitor interface page of a particular ISA Server, you must call it by the address specified in the relative "**ThisISAServerAddress**" or "**SecondISAServerAddress**" variables (e.g., http://130.168.0.1).

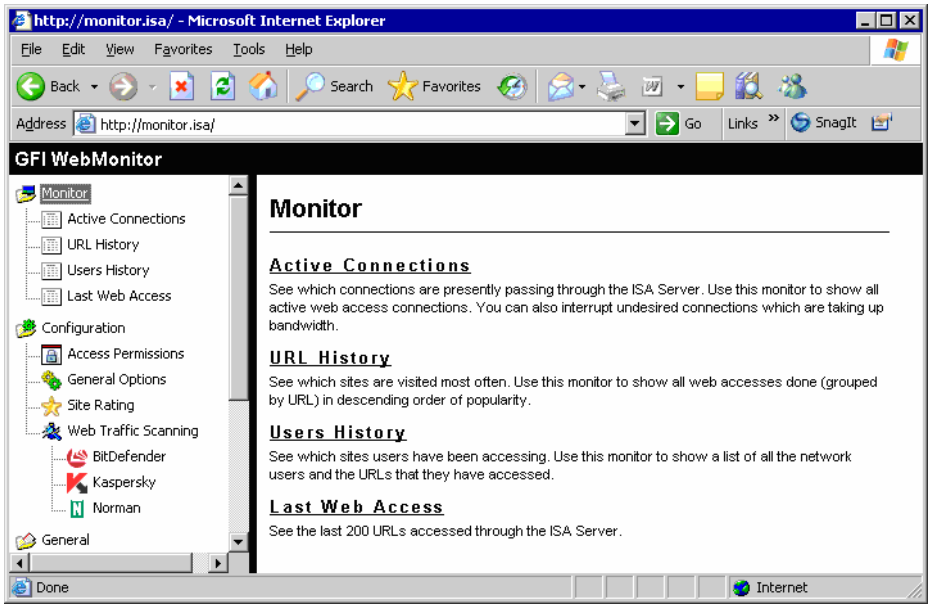
Accessing GFI WebMonitor

Introduction

Use GFI WebMonitor web-based interface for configuration and monitoring. The GFI WebMonitor interface can be launched in two ways:

- On the ISA Server on which GFI WebMonitor is installed by clicking on: Start ▸ Programs ▸ GFI WebMonitor ▸ GFI WebMonitor.
- Remotely over the network using Internet Explorer. Launch Internet Explorer by clicking on Start ▸ Run and typing in **`iexplore.exe`**. Then go to the following URL: **http://monitor.isa/**

NOTE: On a default installation only the administrator on the ISA Server machine will be allowed access to GFI WebMonitor.



Screenshot 5 - GFI WebMonitor configuration interface

Troubleshooting GFI WebMonitor access troubles

If you have trouble accessing GFI WebMonitor web interface chances are you are experiencing one of the following:

1. Your Internet Explorer settings are not using the ISA Server as its proxy server.

2. You are trying to access GFI WebMonitor from a computer which has not been given the necessary access permissions to GFI WebMonitor.

3. You are trying to access GFI WebMonitor using a user account which has not been given the necessary access permissions to GFI WebMonitor.

4. 'Access Denied - Authenticated user' message.

5. 'Access Denied - Non-Authenticated user' message.

Configuring Internet Explorer to use the ISA Server as its proxy

1. Click on Start ▸ Settings ▸ Control Panel ▸ Internet Settings.

2. Click on Tools ▸ Internet Options ▸ Connections ▸ LAN settings.

3. Specify the IP and proxy port of the ISA Server on which GFI WebMonitor was installed.

Giving the computer access permissions to access GFI WebMonitor

On a computer from which you can access GFI WebMonitor interface:

1. Launch GFI WebMonitor configuration interface.

2. Click on the Configuration ▸ Access Permissions node.

3. Specify the IP (e.g., 192.168.0.3) of the computer from which requests to access GFI WebMonitor will be allowed and click on the **Add** button.

4. Click on **Apply** to save the updated configuration settings.

Giving a user account access permissions to access GFI WebMonitor

On a computer from which you can access GFI WebMonitor interface:

1. Launch GFI WebMonitor configuration interface.

2. Click on the Configuration ▸ Access Permissions node.

3. Specify the username (in the format DOMAIN\user) of the user from which requests to access GFI WebMonitor will be allowed and click on the **Add** button.

4. Click on **Apply** to save the updated configuration settings.

Access Denied - Authenticated user

This message is shown when an authenticated user is denied access to the configuration. When this happens both the IP and the username are listed in the error message.

Screenshot 6 - Access Denied: Authenticated user

On a computer with access to GFI WebMonitor interface:

1. Launch GFI WebMonitor configuration interface.

2. Click on the Configuration ▸ Access Permissions node.

3. Specify the username (in the format DOMAIN\user) or IP (e.g., 192.168.0.3) of the computer from which requests to access GFI WebMonitor will be allowed and click on the **Add** button.

4. Click on **Apply** to save the updated configuration settings.

Access Denied - Non-Authenticated user

This message is shown when a non-authenticated user is denied access to the configuration. When this happens only the IP of the user trying to access GFI WebMonitor is listed in the error message.

Screenshot 7 - Access Denied: Non-Authenticated user

On a computer with access to GFI WebMonitor interface:

1. Launch GFI WebMonitor configuration interface.

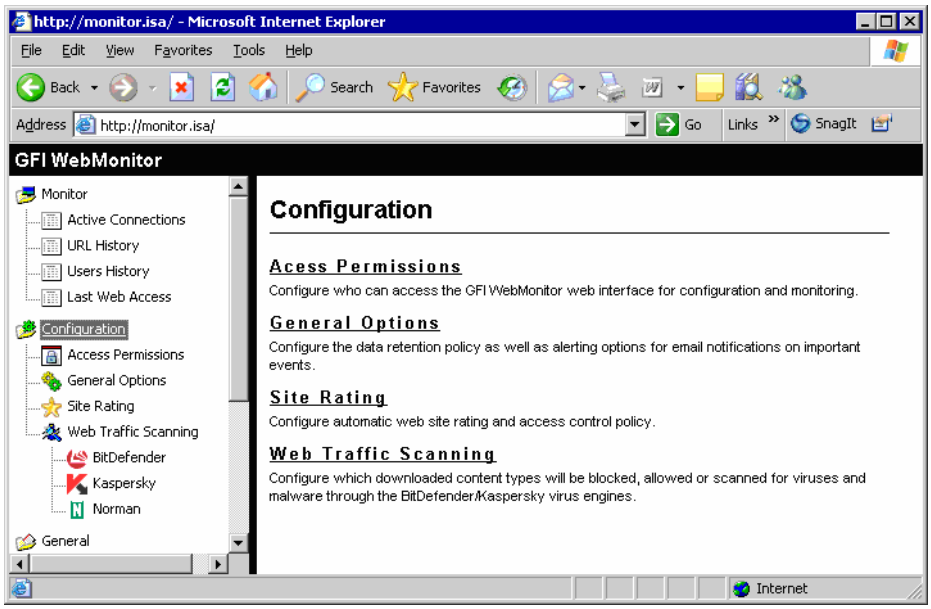
2. Click on the Configuration ▸ Access Permissions node.

3. Specify the IP (e.g., 192.168.0.3) of the computer from which requests to access GFI WebMonitor will be allowed and click on the **Add** button.

4. Click on **Apply** to save the updated configuration settings.

Configuring GFI WebMonitor

Introduction

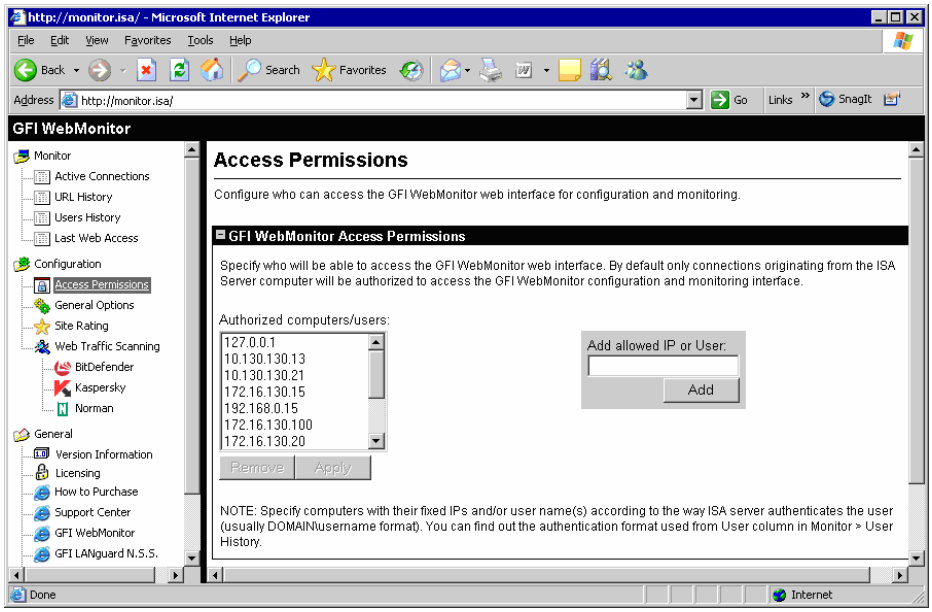


Screenshot 8 - The Configuration node

The GFI WebMonitor interface allows you to configure all of the functional parameters required for web traffic monitoring, processing and scanning. These parameters are setup through the four sub-nodes contained within the Configuration node which are:

- Access Permissions: Configure who can access GFI WebMonitor web interface for configuration and monitoring.
- General Options: Configure the data retention policy as well as alerting options for email notifications on important events.
- Site Rating: Configure automatic Site Rating and Access Control policy.
- Web Traffic Scanning: Configure content checking and anti-virus parameters to use for monitoring and scanning of downloaded files and Internet objects.

Access Permissions



Screenshot 9 - Security node: Access Permissions list

Access to GFI WebMonitor is based on the IP or windows authenticated username which are being used by the user attempting to gain access to the configuration. Only users/computers which are in the authorized users/IP list will be allowed access.

To add a user or IP to the access permissions list:

1. Click on the Configuration ▸ Access Permissions node.

2. Specify the username (in the format DOMAIN\user) or IP (e.g., 192.168.0.3) of the computer from which requests to access GFI WebMonitor will be allowed and click on the **Add** button.

3. Click on **Apply** to save the updated configuration settings.

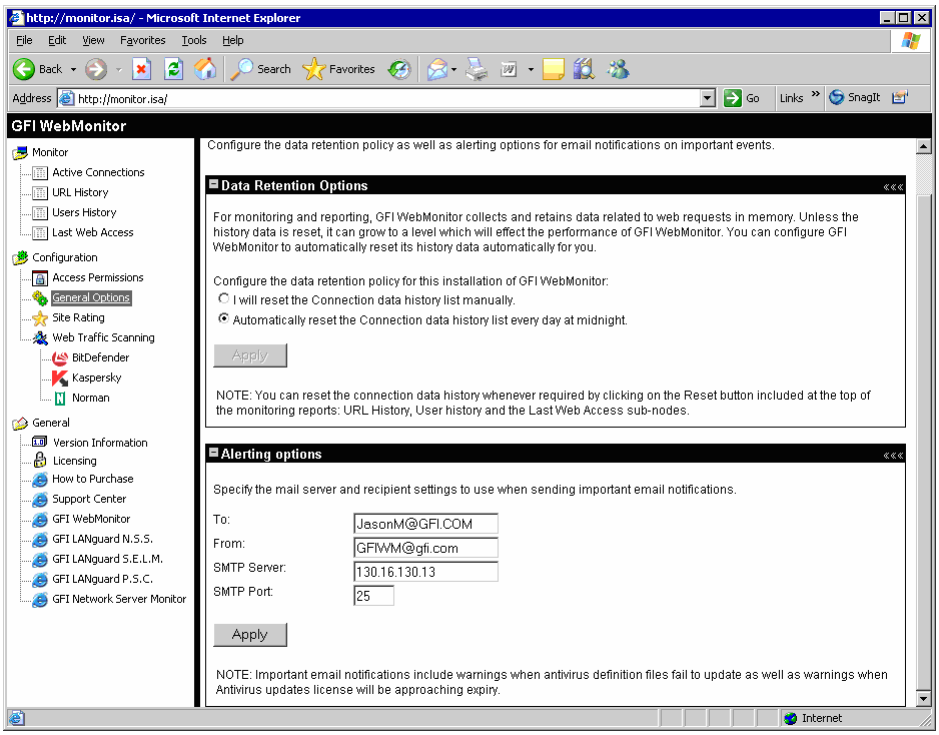
NOTE: When using IP Access Control, you must assign a fixed/static IP to every computer which is allowed access to GFI WebMonitor. This is required in order to avoid having to change your list of allowed IPs every time that a computer is rebooted or served a different IP by the DHCP Server.

General options

Use the General options node to configure:

- The retention period of the collected (Internet activity) data.
- The email alerting options.

Data Retention Options



Screenshot 10 - General options page

For monitoring and reporting, GFI WebMonitor collects and retains data related to web requests in memory. Unless the history data is reset, it can grow to a level which will affect the performance of GFI WebMonitor.

In GFI WebMonitor, you can reset the collected data in two ways:

- **Automatically:** GFI WebMonitor will automatically reset the collected data daily at midnight.
- **Manually:** You must reset the collected data by pressing a reset data button from GFI WebMonitor interface. You can reset the Internet activity data history whenever required by clicking on the **Reset** button included at the top of the monitoring reports accessible through the 'Monitor' node: (i.e., Monitor ▸ URL History, Monitor ▸ User History and the Monitor ▸ Last Web Access nodes).

To configure the data retention policy of GFI WebMonitor:

1. Click on the Configuration ▸ General Options node.
2. Go to the 'Data Retention Options' section.
3. Select one of the following options:

- **I will reset the Connection data history list manually** – Select this option to manually reset the history data cache.

NOTE: It is recommended that the collected data is cleared at least once a week.

- **Automatically reset the Connection data history list every day at midnight** – Select this option to let GFI WebMonitor automatically reset the history data cache daily at midnight.

4. Click on the **Apply** button to save the configuration settings.

NOTE: GFI WebMonitor can store up to a maximum of 3000 records in its website history cache. Exceeding the maximum limit will cause random deletion of information from the history cache. Whenever this happens, a "Data Overflow" message is displayed at the bottom of the URL History page.

Alerting Options

GFI WebMonitor will send an email notification on the occurrence of important events. Important email notifications include warnings when anti-virus definition files fail to update as well as warnings when the anti-virus license will be approaching expiry.

To configure the recipient and mail server settings to use for email notifications:

1. Click on the Configuration ▸ General Options node.

2. Go to the 'Alerting Options' section.

3. Specify the following parameters:

- **To:** – Specify the address to where email notifications will be sent.
- **From:** – Specify the email address from where the email notification will be sent.
- **SMTP Server:** - Specify the IP address of the SMTP Server which will forward the email notifications.
- **SMTP Port:** - Specify the port through which the email transmission will take place.

3. Click on the **Apply** button to save your configuration settings.

Extended Alerting Options

GFI WebMonitor can be configured to send the target recipient email notifications every time the virus definitions are successfully downloaded and updated.

To enable extended Alerting Options:

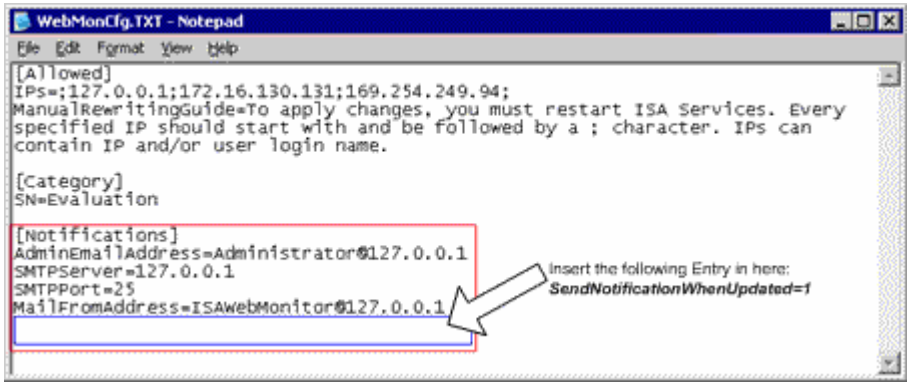
1. Exit GFI WebMonitor interface.

2. Open the file named 'WebMonCfg.TXT' in GFI WebMonitor installation directory.

3. Add the following entry in the [Notifications] area of the 'WebMonCfg.TXT' file: '**`SendNotificationWhenUpdated=1`**'.

4. Save and close the file.

5. Restart the ISA Server Web Proxy Server (W3PROXY) from the Service Control Manager (Start ▸ Settings ▸ Control Panel ▸ Administrative Tools ▸ Services).



Screenshot 11 - Editing the WebMonCfg.TXT file

NOTE: To revert back to the default notification settings (i.e., send notifications only on failed virus signature updates) repeat the same process but this time remove the entry '**`SendNotificationWhenUpdated=1`**'.

Site Rating

Introduction

Use GFI WebMonitor Site Rating feature together with the ISA Server web access blocking capabilities, to achieve automatic proactive blocking of sites which contain objectionable adult material such as pornographic images, candid scenes, offensive words and links to adult sites.

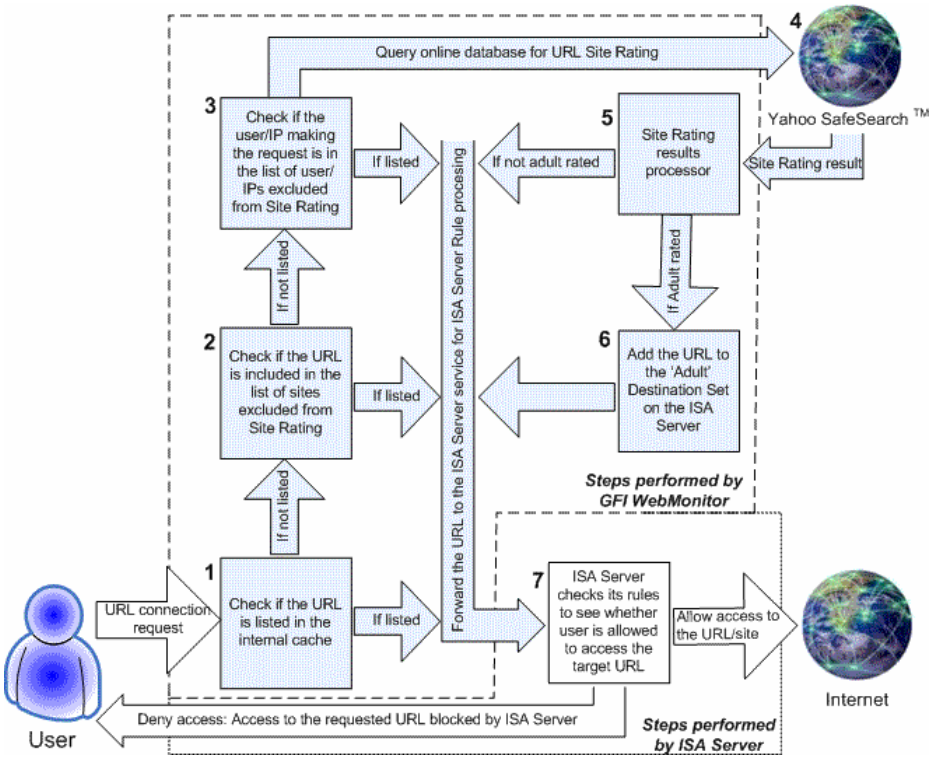


Figure 4 - Site Rating process flow

GFI WebMonitor can check for adult content in the URLs which users want to access. This is achieved by querying Yahoo! SafeSearch™ which is an online database that classifies and categorizes various sites on the Internet. When a user requests access to a site, GFI WebMonitor will query the Yahoo! SafeSearch™ database for the Content-Type held by that target URL. If the online web filter classifies the site as having adult content, GFI WebMonitor will add the target URL to the 'Adult' Destination Set on the ISA Server. If the ISA Server is configured to block access to the sites listed in the 'Adult' Destination/URL Set the user will be denied access to that site.

NOTE 1: GFI WebMonitor will retain the classification of the last 3000 sites accessed. Every time a request to a target site is made, GFI WebMonitor will check if the requested URL is listed in its internal

cache. GFI WebMonitor will query the target online classification database only if the requested URL is not listed in its cache.

NOTE 2: GFI WebMonitor handles the adding of newly detected adult sites to the 'Adult' Destination/URL Set. ISA Server handles the blocking of the connections to the URLs listed in the 'Adult' Destination/URL Set.

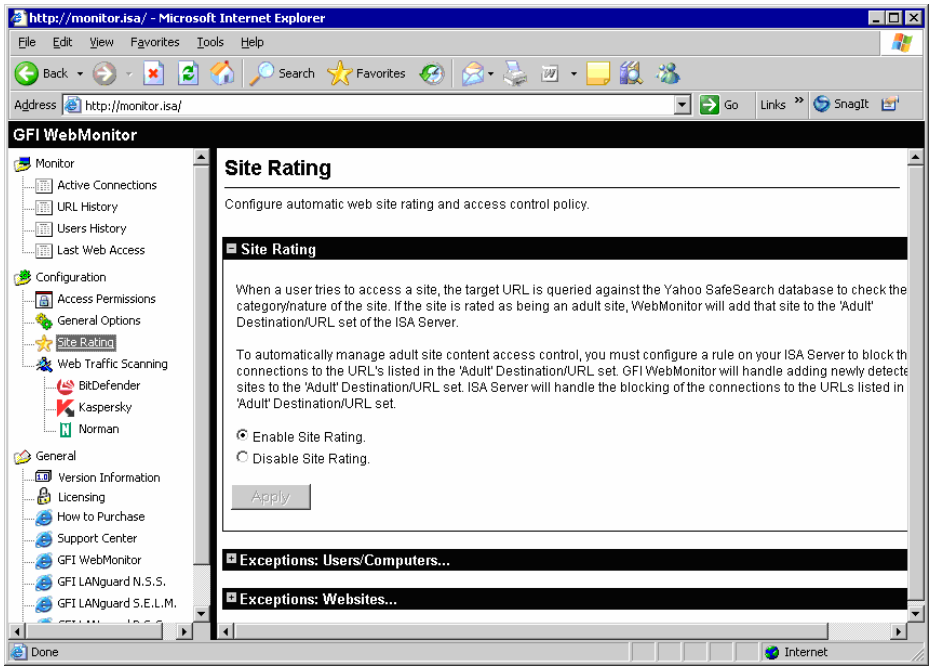
NOTE 3: The Destination/URL Set 'Adult' is created on the ISA Server during the installation of GFI WebMonitor. To restrict user access to adult-rated sites, you must manually configure a rule on your ISA Server which blocks the connections to the URLs listed in the 'Adult' Destination/URL Set.

NOTE 4: You can change the name and category of the Adult Destination Set from the **SiteJudge.js** script. This script is located in the installation folder of GFI WebMonitor.

For more information on Yahoo! SafeSearch™ visit

http://help.yahoo.com/help/us/ysearch/basics/basics-16.html

Enabling/Disabling Site Rating



Screenshot 12 – Site Rating: Adult & Site Rating section

To enable Site Rating:

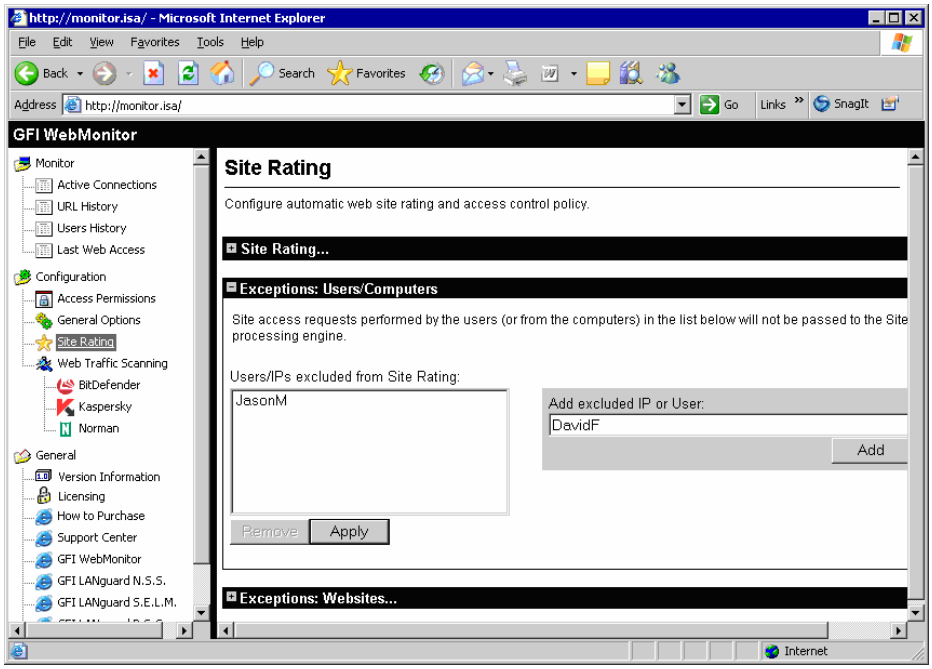
1. Click on the Configuration ▸ Site Rating node.
2. Go to the ‘Site Rating’ section.
3. Select the **Enable Site Rating** option.
4. Click on the **Apply** button to save your configuration settings.

To disable Site Rating:

1. Click on the Configuration ▸ Site Rating node.
2. Go to the ‘Site Rating’ section.
3. Select the **Disable Site Rating** option.

4. Click on the **Apply** button to save your configuration settings.

Excluding Users/IPs from Site Rating



Screenshot 13 - Site Rating node: Users/IPs excluded from Site Rating

You can configure GFI WebMonitor to block target URL requests made from specific users/Computer IPs to the Site Rating processing engine. This means that the URLs of sites visited by users listed in the user/IP exception list will not be checked and rated through the Yahoo! SafeSearch™ engine.

To configure User/IP exceptions:

1. Click on the Configuration ▸ Site Rating node.

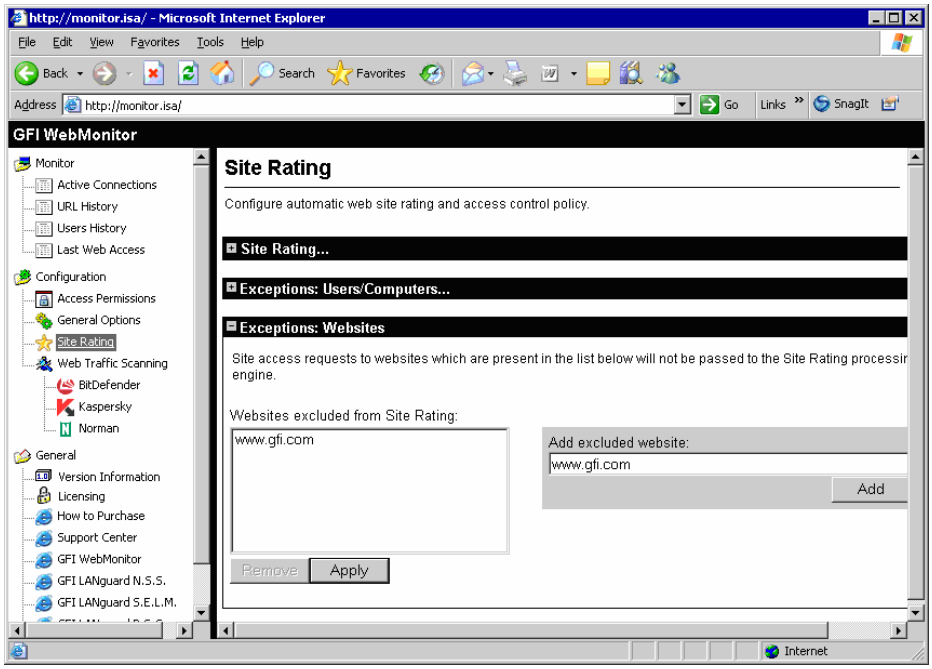
2. Go to the 'Exceptions: Users/Computers' section.

3. Specify the username or IP address of the computer that will be excluded from the Site Rating process and click on the **Add** button.

4. Click on the **Apply** button to save your configuration settings.

NOTE: If the target site is already a member of the 'Adult' Destination/URL Set, ISA Server will still block access to it. You will need to manually delete the target site from the 'Adult' Destination/URL Set to stop ISA Server from blocking access.

Excluding websites from Site Rating



Screenshot 14 - Site Rating node: Websites excluded from Site Rating

You can configure GFI WebMonitor to block requests made to specific sites for Site Rating processing. This means that the URLs of sites listed in the website Site Rating exception list will not be checked and rated through the Yahoo! SafeSearch™ engine.

To configure website exceptions:

1. Click on the Configuration ▸ Site Rating node.

2. Go to the 'Exceptions: Websites' section.

3. Specify the URL of the website that will be excluded from the Site Rating process and click on the **Add** button.

4. Click on the **Apply** button to save your configuration settings.

NOTE: If the target site is already a member of the 'Adult' Destination/URL Set, ISA Server will still block access to it. You will need to manually delete the target site from the 'Adult' Destination/URL Set to stop ISA Server from blocking access.

Viewing the contents of the 'Adult' Destination/URL Set on ISA Server

The 'Adult' Destination/URL Set is the ISA Server container in which GFI WebMonitor will add the adult-rated URLs classified by the Site Rating processing engine.

For instructions on how to access and maintain the 'Adult' Destination/URL Sets on your ISA Server, refer to the ‘Maintaining the ISA Server 'Adult' Destination/URL Sets’ section in the ‘Common ISA Server Setup Tasks’ chapter.

Web Traffic Scanning

Introduction

Web Traffic Scanning is the process which GFI WebMonitor performs on data objects which are downloaded through the ISA Server.

During Web Traffic Scanning, GFI WebMonitor performs the following functions on the downloaded data objects:

1. Extracts the HTTP Content-Type signature as advertised in the HTML code.

2. Detects the real filetype of the object by analyzing the first sets of bytes downloaded against a filetype signature database.

3. Uses the advertised HTTP Content-Type and detected real filetype data to block malicious or unwanted files.

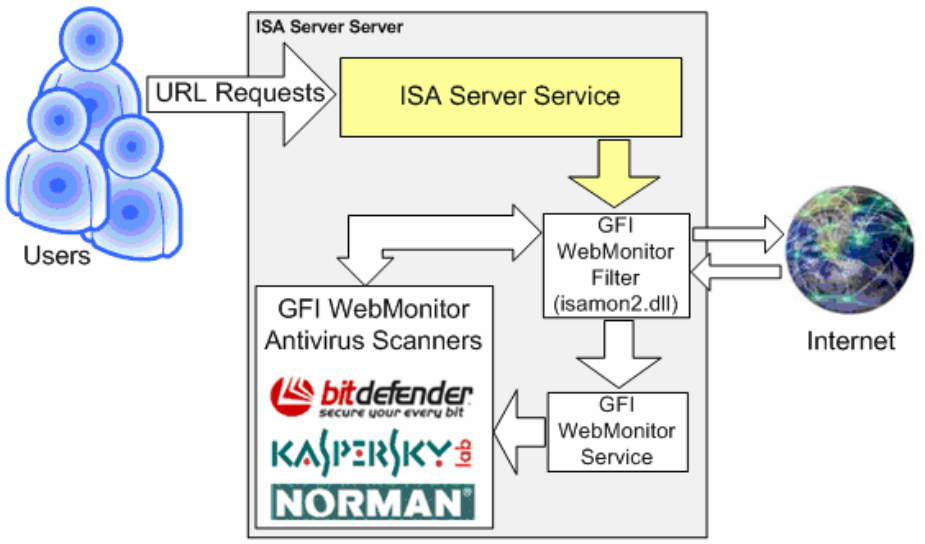


Figure 5 - GFI WebMonitor scan web traffic using the supported anti-virus scanning engines

4. Checks for viruses using the supported virus scanning engines.

5. Checks for spyware and adware using the supported virus scanning engines.

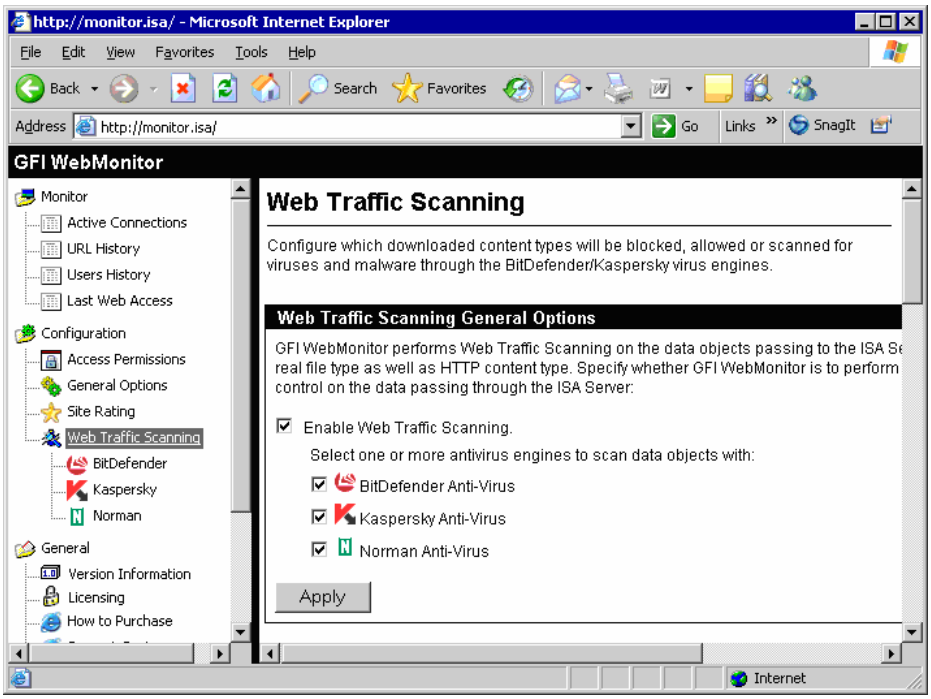
6. Checks for Trojans using the supported virus scanning engines.

To configure the Web Traffic Scanning options go to Configuration ▸ Web Traffic Scanning node. Options which can be configured include:

- Enable/Disable in its entirety the Web Traffic Scanning engine.
- Enable/Disable virus scanning engine(s) used to scan downloaded data objects for malware.
- Configuration of which data objects are to be allowed, blocked and scanned for malware through the selected anti-virus engine(s).

- Configuration of user exceptions: data objects downloaded by these users will not be passed through the Web Traffic Scanning processing engine.
- Configuration of website exceptions: data objects downloaded from these sites will not be allowed through the Web Traffic Scanning processing engine.

Enable/Disable Web Traffic Scanning



Screenshot 15 – Virus Scanning Engines node: Engine options

To enable Web Traffic Scanning:

1. Click on the Configuration ▸ Web Traffic Scanning node.
2. Go to the 'Web Traffic Scanning General Options' section.
3. Select the 'Enable Web Traffic Scanning' option.
4. Select one or more anti-virus engine(s) to scan data objects for malware. The anti-virus engines supported include:

- Kaspersky
- BitDefender
- Norman.

5. Click on the **Apply** button to save your configuration settings.

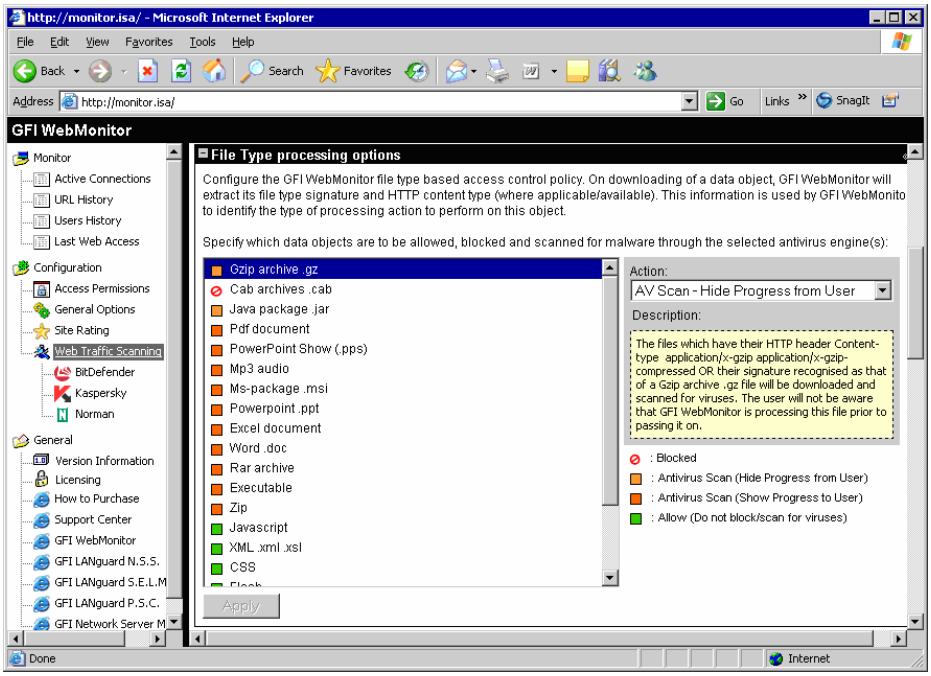
NOTE 1: During evaluation, all supported anti-virus engines can be configured and used. On evaluation expiration you will need to purchase a license key which will enable one or more of the anti-virus scanning engines to continue using the Web Traffic Scanning feature of GFI WebMonitor.

NOTE 2: All paid versions of GFI WebMonitor are shipped with a one year anti-virus update license.

Configuring supported filetypes to be scanned/blocked

Web Traffic Scanning works on the data objects which are being downloaded. When content is downloaded, GFI WebMonitor will both extract the advertised Content-Type (when applicable/available) as well as determine the real filetype of the downloaded object. Using this information, GFI WebMonitor will check the Web Traffic Scanning processing engine configuration to see how to process the object.

GFI WebMonitor ships with the capability to detect a number of filetypes. For every filetype, you can configure what type of action GFI WebMonitor is to take when processing a downloaded object which matches the indicated filetype.



Screenshot 16 - Configuring filetypes to scan / block

To configure the Web Traffic Scanning action for the listed filetypes:

1. Click on the Configuration ▸ Web Traffic Scanning node.

2. Go to the 'File Type processing options' section.

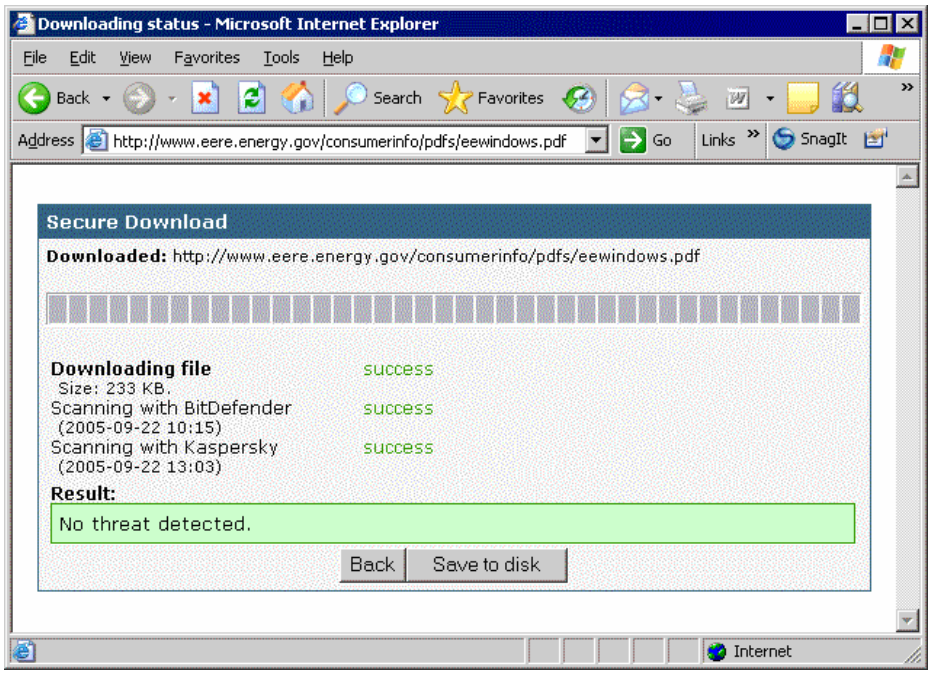
3. From the list of filetypes supported, click on the filetype to configure. From the action combo box, specify the way which GFI WebMonitor is to act on downloaded objects with the indicated filetype. For every object type the following actions are supported:

Block – block all objects that match the indicated filetype.

Allow (Do not block/scan for viruses) – do not block or scan downloaded objects that match the indicated filetype.

AV Scan (Hide Progress from User) - files which match the indicated Content-Type will be downloaded and scanned for viruses. The user will not be aware that GFI WebMonitor is processing this file prior to passing it on.

AV Scan (Show Progress to User) - files which match the indicated Content-Type will be downloaded and scanned for viruses. The user will be informed that GFI WebMonitor is processing this file prior to passing it on.



Screenshot 17 – AV Scan (Show Progress to User) real-time download feedback in status window

4. Click on the **Apply** button to save your configuration settings.

NOTE 1: When using the action option 'Scan (Show Progress to User)' GFI WebMonitor will show in real-time on the client web browser, the status of the download in progress on a web page equivalent of the download status. When the download completes, client users can save the downloaded object to disk by using the '**Save to disk'** button on the download web page. This process requires the manual intervention of the user in order to save the downloaded object.

NOTE 2: The action option 'Scan (Show Progress to User)' can interfere with auto update sites like windows update. Be sure to add the site which is being contacted for auto updates to the Exclusion list (described further on in this chapter).

Configuring new filetypes to be scanned/blocked

GFI WebMonitor ships with the capability to detect a set of data object types. To configure Web Traffic Scanning action support for objects whose HTTP Content-Types are advertised in the HTTP code:

To configure the Web Traffic Scanning action for the listed filetypes:

1. Click on the Configuration ▸ Web Traffic Scanning node.

2. Go to the 'Extended File Type processing options' section.

3. Specify the HTTP Content-Type of the object to process.

4. Specify the action to take when GFI WebMonitor meets data objects of same filetype.

NOTE: Actions configurable for the extended filetypes are the same as the actions configurable for the default supported filetypes, i.e.:

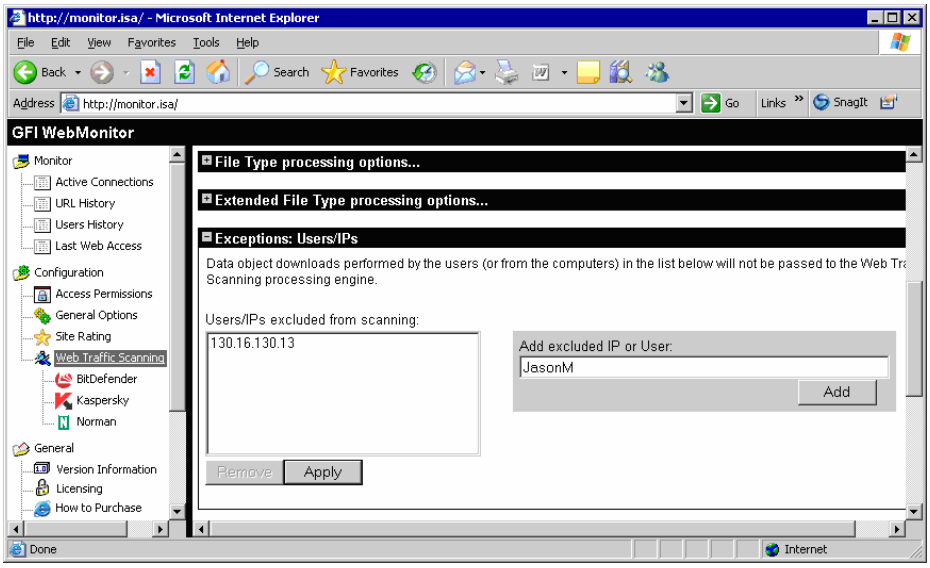
Block,

Allow (Do not block/scan for viruses)

- AV Scan (Hide Progress from User)
- AV Scan (Show Progress to User)

5. Click on the **Apply** button to save your configuration settings.

Excluding Users/IPs from Web Traffic Scanning



Screenshot 18 – Enumerating Users/IPs excluded from Web Traffic Scanning

You can configure GFI WebMonitor to block objects downloaded by specific users/Computer IPs to the Web Traffic Scanning processing engine. This means that the data objects downloaded by users listed in the user/IP exception list will not be run against the Web Traffic Scanning action parameters.

To configure User/IP exceptions:

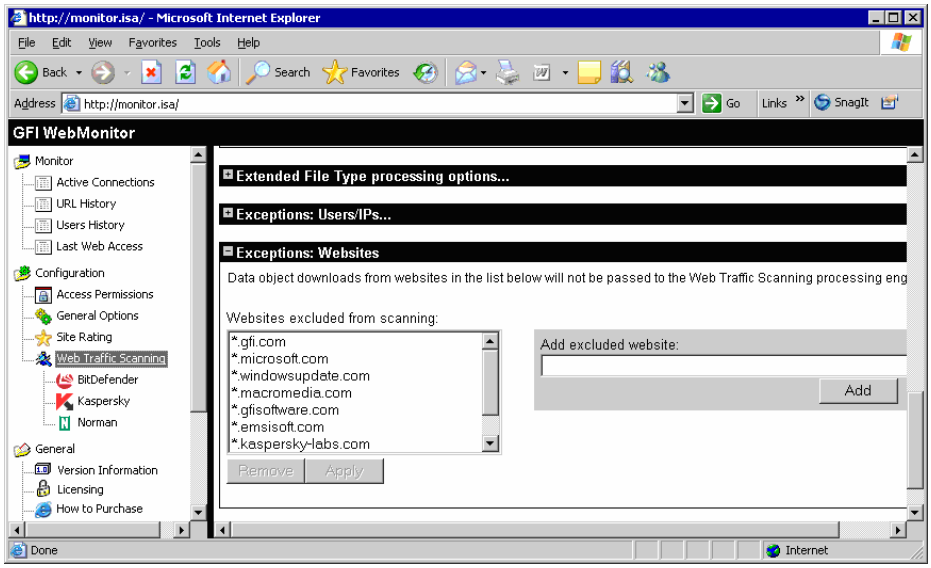
1. Click on the Configuration ▸ Web Traffic Scanning node.

2. Go to the 'Exceptions: Users/Computers' section.

3. Specify the username or IP address of the computer that will be excluded from the Web Traffic Scanning process and click on the **Add** button.

4. Click on the **Apply** button to save your configuration settings.

Excluding websites from Web Traffic processing



Screenshot 19 - Site Rating node: Websites excluded from Site Rating

You can configure GFI WebMonitor to block data objects downloaded from specific sites to the Web Traffic Scanning processing engine. This means that the data objects downloaded by users from the listed websites will not be run against the Web Traffic Scanning action parameters.

To configure website exceptions:

1. Click on the Configuration ▸ Web Scanning Traffic node.

2. Go to the 'Exceptions: Websites' section.

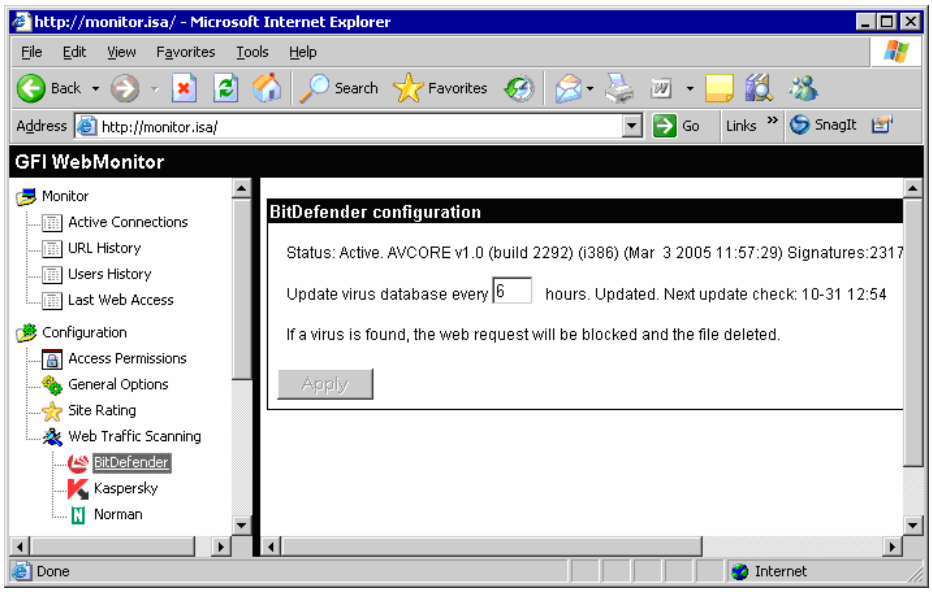
3. Specify the URL of the website that will be excluded from the Web Traffic Scanning process and click on the **Add** button.

4. Click on the **Apply** button to save your configuration settings.

Updating Anti-virus Definition Files

New malware in the form of viruses, worms, spyware, Trojans and adware are released hourly. To stop new malware from spreading and penetrating into your network you need to ensure that the anti-virus definition files are up-to-date with the latest definition files released by the respective vendors.

GFI WebMonitor periodically checks and downloads new anti-virus definition files made available for the supported virus scanning engine(s).



Screenshot 20 - Configuring the virus update frequency

Keeping the virus scanning engine(s) up-to-date

To view the properties of supported virus scanning engines as well as configure the update frequency policy of the respective signature files:

1. Select the scanning engine to be configured (e.g. BitDefender) from the list provided under the Configuration ▸ Web Traffic Scanning node.

2. In the configuration section displayed in the right pane, specify the required signature file update frequency in hours.

3. Click on the **Apply** button to save your configuration settings.

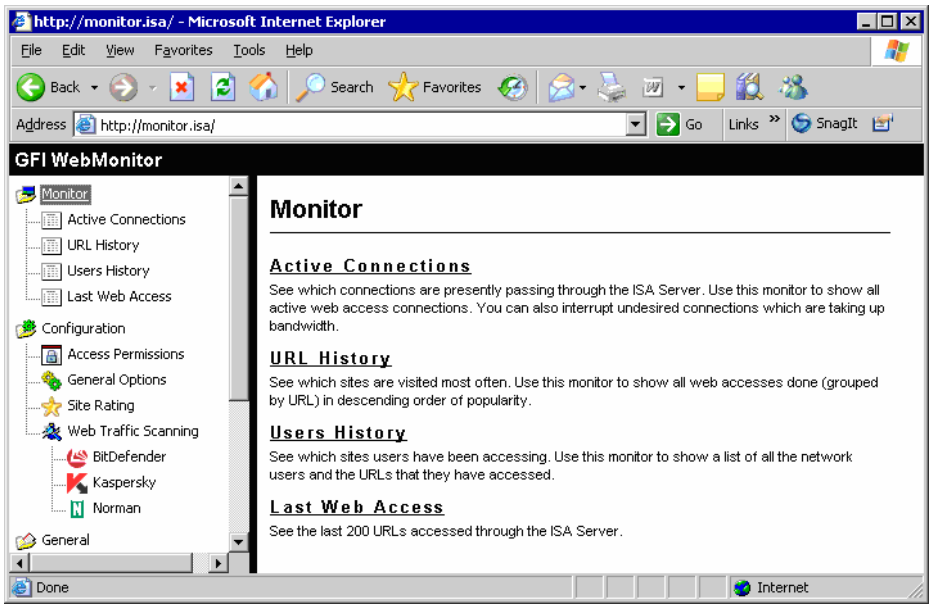
NOTE 1: It is recommended to check for anti-virus definition files at least once every 24 hours.

NOTE 2: Web Traffic Scanning for viruses will remain active even during the definition file updating process.

NOTE 3: GFI WebMonitor will check for anti-virus definition updates every time a change is made to the update frequency policy.

Monitoring Internet activity

Introduction



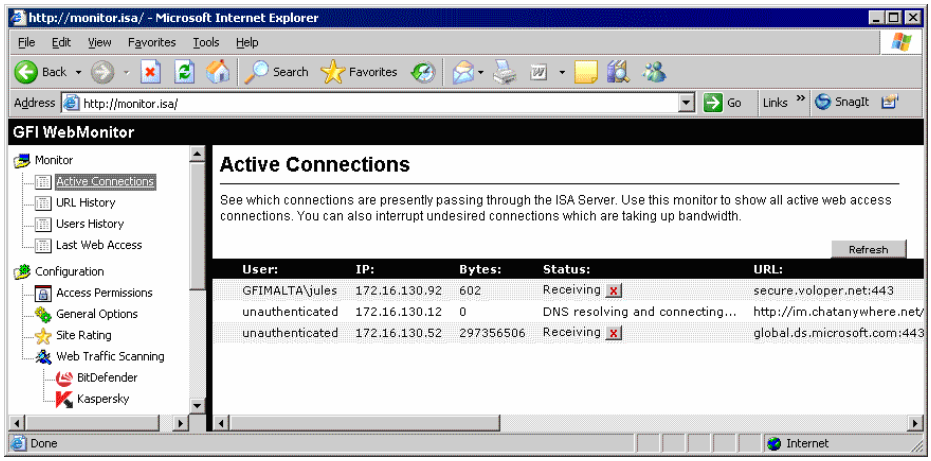
Screenshot 21 – The Monitor node

Use the GFI Monitor nodes and sub-nodes to access different views of the web requests (both active and past) which passed through the ISA Server.

To get a view of the data which is constantly collected by GFI WebMonitor (reflecting the data going through the ISA Server) click on any of sub-nodes listed under the 'Monitor' node. These include:

- Active connections sub-node
- URL History sub-node
- Users History sub-node
- Last Web Access sub-node

Active connections



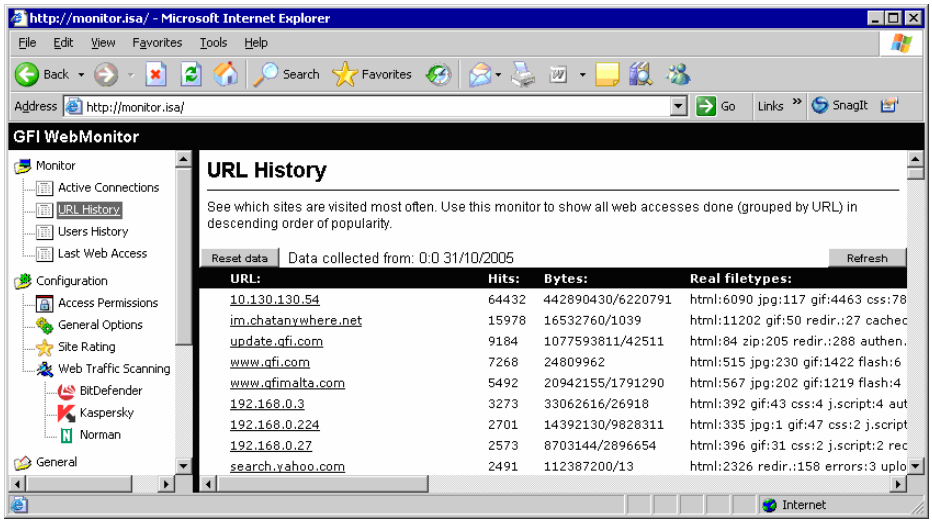
Screenshot 22 - Active Internet connections

The 'Active connections' view shows all of the currently active TCP connections which are passing through your ISA Server. The information shown includes the username, Source IP, bytes Received/Sent, Status as well as details on the URL being accessed.

You can also use this view to cancel and disconnect an active Internet connection (e.g., You can interrupt a big file download which will take up too much bandwidth). To interrupt a connection, click on the button included in the 'Status' column (of the connection to be interrupted).

NOTE: The information displayed is not automatically refreshed. Click on the **Refresh** button in the upper right of the view to update the information being shown.

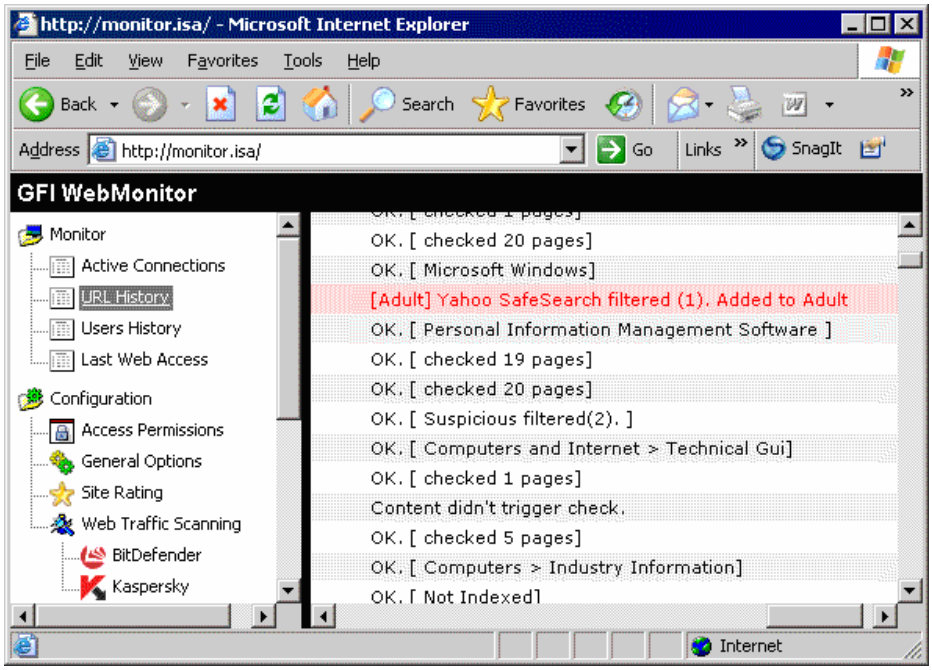
URL History



Screenshot 23 - URL History view

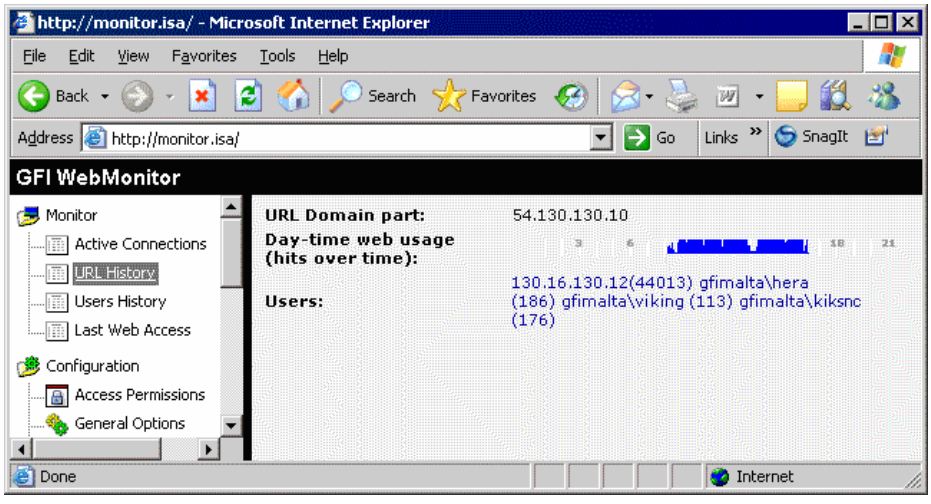
The 'URL History' view shows the URLs/sites that were most frequently accessed (through ISA Server) by network users. The information shown is sorted in descending order of popularity (most popular URL is listed on top) and includes:

- The URLs which were accessed.
- The number of times that this URL was accessed (i.e., number of hits).
- The number of bytes that were Received/Sent from each URL.
- The real filetypes accessed from each URL.
- The URL Category.
- The users/IPs that have accessed the URL.
- The Site Check results



Screenshot 24 - Site check results

You can also click on any of the URLs listed to gain access to more information about how it was accessed including a full list of users who have accessed that site as well as a graphical representation of the URL's hits over time.



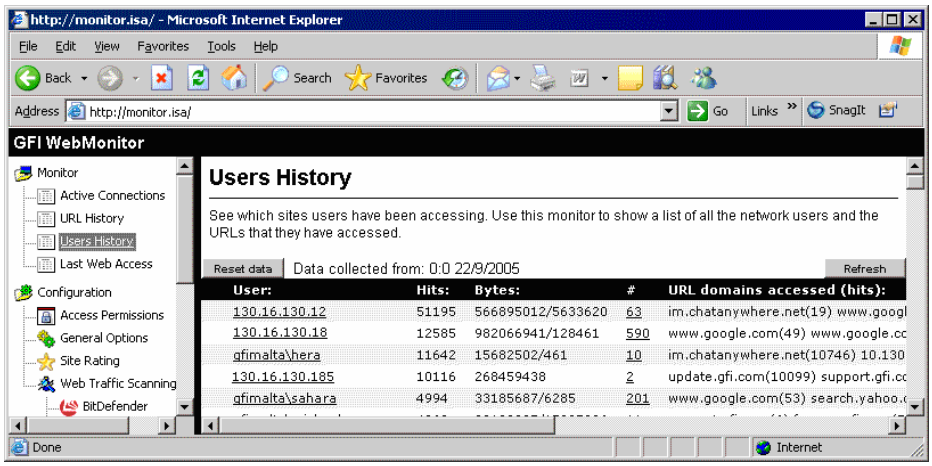
Screenshot 25 – URL detailed information view

This graphical representation helps you to identify the time slice(s) during which this site is most frequently accessed (daily/based on 24 hrs).

To reset the data collected by GFI WebMonitor click on the **Reset Data** button at the top of the URL History view. Deleted data cannot be recovered/undone!

NOTE: The information displayed is not automatically refreshed. Click on the **Refresh** button in the upper right of the view to update the information being shown.

Users History

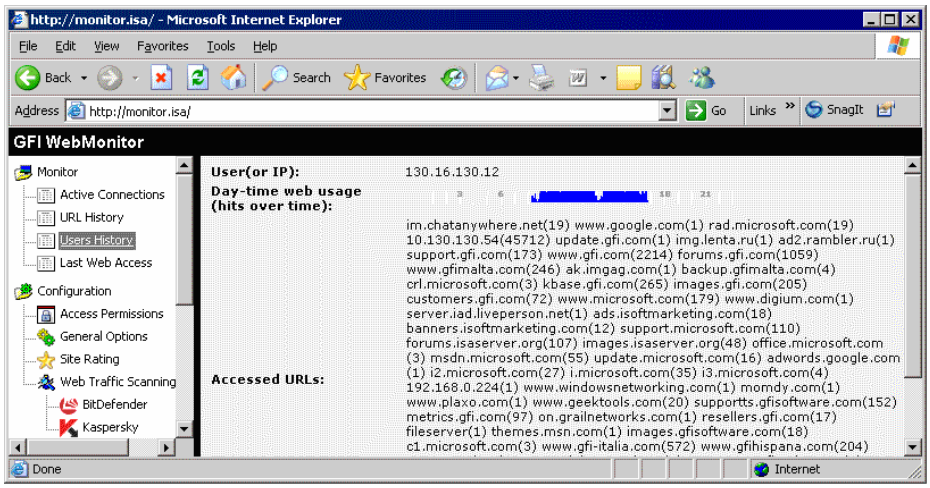


Screenshot 26 - Users History view

The 'Users History' view shows the Internet activity (which passed through the ISA Server) of all your network users. The information shown in this sub-node is sorted in descending order of user hits (most active user is listed on top) and includes:

- The username/IP.
- The total number of sites (hits) visited/accessed by each user.
- The total number of bytes that were received/sent by each user.
- The URLs accessed by each user.

Use the 'Users History' view to gain access to even more detailed information on the user's Internet activity.



Screenshot 27 - User History detailed information view

This detailed information includes:

- The complete list of all URLs accessed by the selected user (or from the selected computer).
- A graphical representation of the user's web-browsing time distribution.

From this graphical representation you can extract the following information:

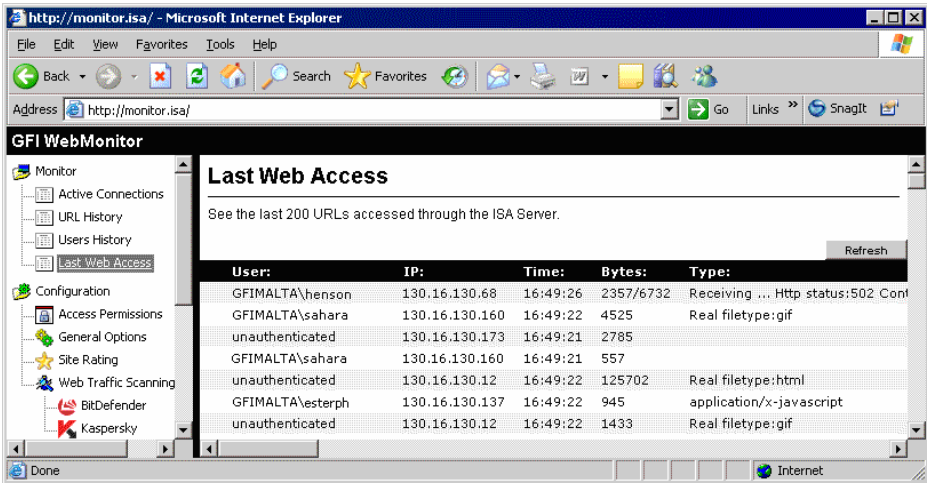
- The time slice(s) during which each user makes most use of the provided Internet connection.
- The number of hours that each user is spending on Internet browsing.
- The period during which your web traffic is at its peak.

Through this information you can quickly identify users which abuse of their Internet privilege. This helps you plan adequate Internet restriction policies and improve your bandwidth management. To view detailed information on the user's Internet activity, click on the respective username/IP.

To reset the data collected by GFI WebMonitor click on the **Reset Data** button at the top of the Users History view. Deleted data cannot be recovered/undone!

NOTE: The information displayed is not automatically refreshed. Click on the **Refresh** button in the upper right of the view to update the information being shown.

Last Web Access



Screenshot 28 - Last Web Access view

The 'Last Web Access' view shows the last 200 URLs accessed through your ISA Server. The information shown in this sub-node is sorted (in descending order) according to the time that the URL was accessed (most recent listed on top) and includes:

- The name of the authenticated user that accessed the URL.
- The IP address of the computer from where the URL was accessed.

- The time when the URL was accessed.
- The total number of bytes that were received/sent by each user when accessing that site.
- The file/Content-Type(s) of objects downloaded from the accessed URL.
- The complete (ungrouped) URLs list that were accessed by the user.

To reset the data collected by GFI WebMonitor click on the **Reset Data** button at the top of the Last Web Access view. Deleted data cannot be recovered/undone!

NOTE: The information displayed is not automatically refreshed. Click on the **Refresh** button in the upper right of the view to update the information being shown.

Common ISA Server Setup Tasks

Introduction

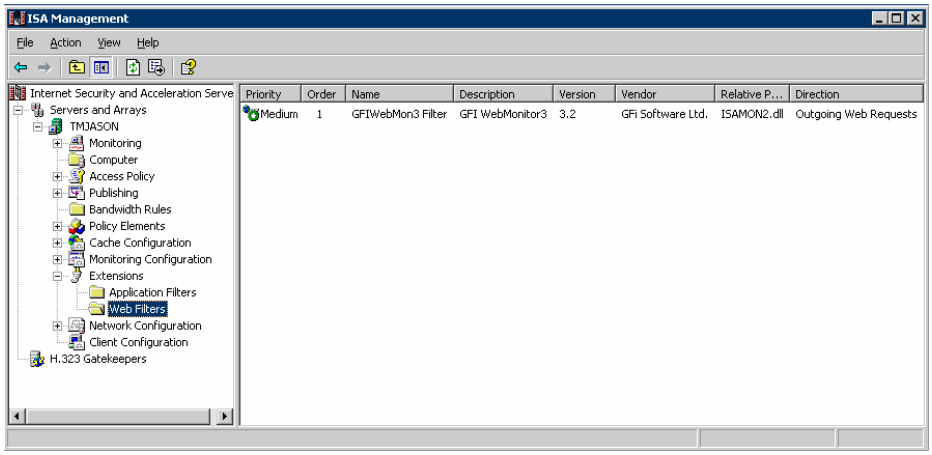
Use the guides in this section to perform common administrative tasks which may be required on the ISA Server(s) in your network for optimal integration with GFI WebMonitor.

Locating GFI WebMonitor Web Filter

The GFI WebMonitor Web Filter (ISAMON2.dll) is an ISAPI Web Filter which installs and plugs into both ISA Server 2000 and ISA Server 2004.

Locating GFI WebMonitor Web Filter on ISA Server 2000

1. Launch the ISA Server Management console.
2. Expand the Extensions node.
3. Click on the Web Filters node.

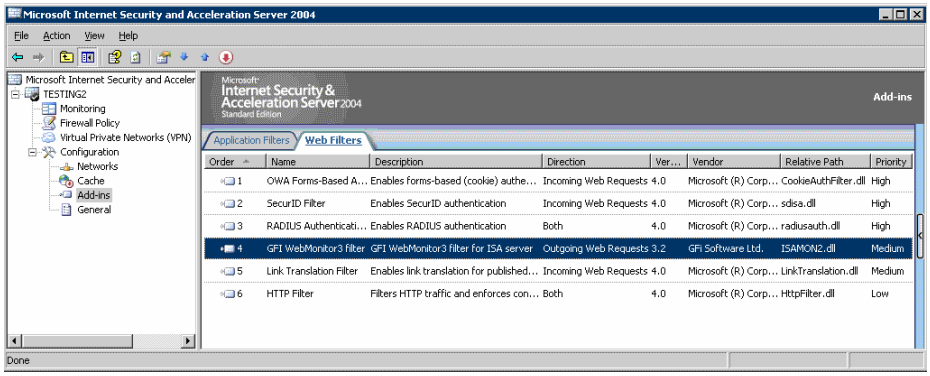


Screenshot 29 - The GFI WebMonitor web filter listed under Extensions in ISA Server 2000

A list of plug-in web filters will be displayed in the right pane.

Locating GFI WebMonitor Web Filter on ISA Server 2004

1. Launch the ISA Server Management console.
2. Expand the Configuration node.
3. Click on the Add-ins node.
4. In the right pane click on the 'Web filters' tab.



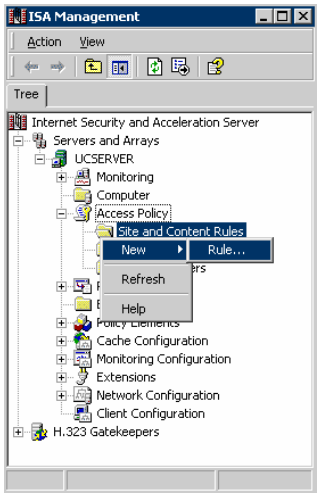
Screenshot 30 - The GFI WebMonitor web filter listed under Add-ins in ISA Server 2004

A list of plug-in web filters will be displayed in the Web filters page in the right pane.

Creating ISA Server access policy rules

Creating an Access Rule policy on ISA Server 2000

1. Launch ISA Server 2000 Management console.



Screenshot 31 - ISA Server 2000: Access Policy node

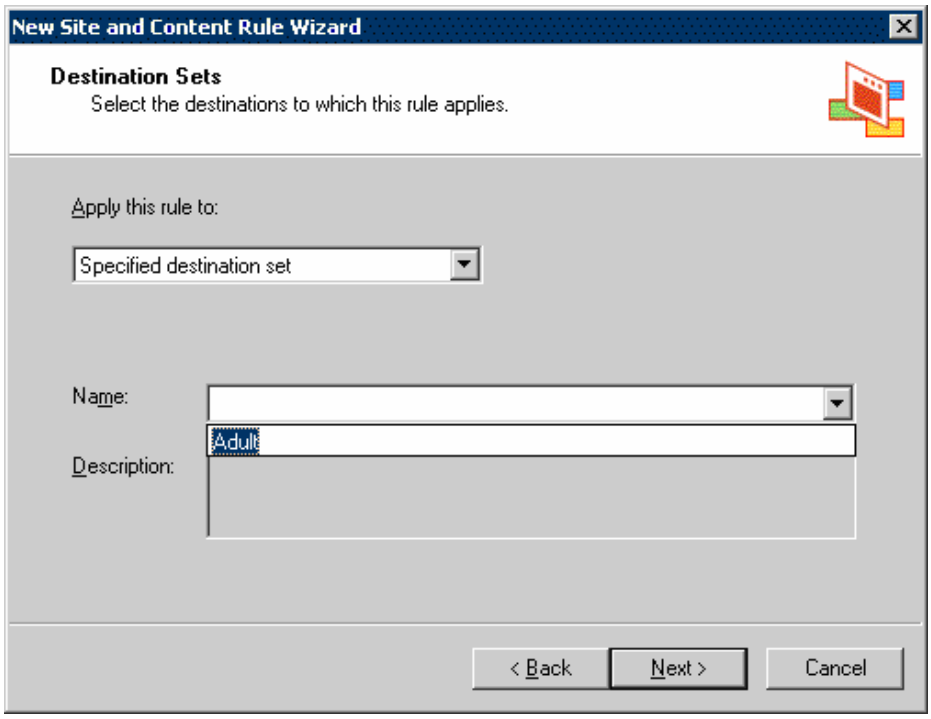
2. Expand the Access Policy node.

3. Right click on the Site and Content Rules ▸ New… ▸ Rule…This will bring up the New Site and Content Rule Wizard.

4. Give the rule the name " Block Adult Sites – Based on URLs in Adult Destination Set". Click on **Next** to continue.

5. In the Rule Action page, set the permission to 'Deny' and click on **Next** to continue.

6. In the Rule configuration page, select the option "Deny access based on destination". Click on **Next** to continue.



Screenshot 32 - Specify the Destination Set to which this rule applies

7. In the Destination Sets page, set the option to "Specified destination set" and select the 'Adult' Destination Set from the list provided. Click on **Next** to continue.

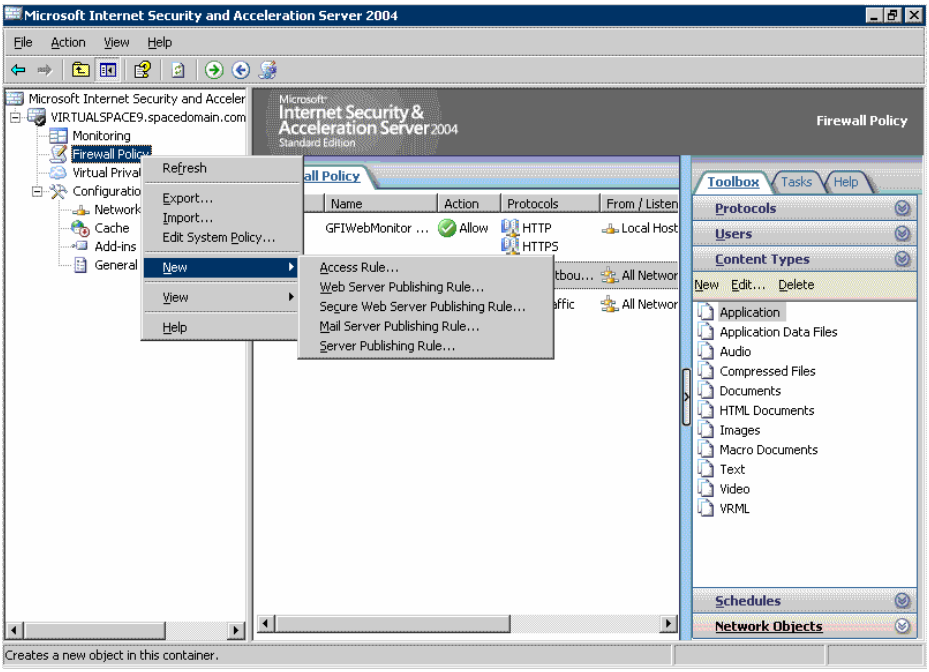
Screenshot 33 - Site and Content Rule Wizard: Final dialog showing the configured rule details

8. Click on **Finish**. The new Access Rule policy is now set up on your ISA Server 2000 to block all users from accessing the sites listed in the 'Adult' Destination Set.

NOTE: The adult Destination/URL Set was created on the ISA Server during GFI WebMonitor installation.

Creating an Access Rule policy on ISA Server 2004

1. Launch ISA Server 2004 Management console

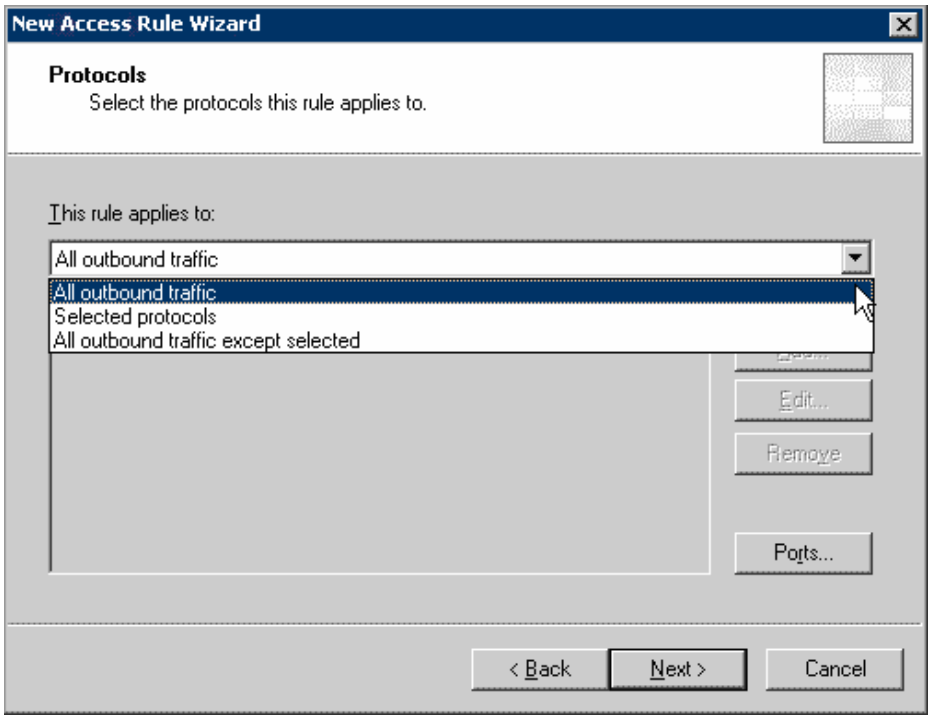


Screenshot 34 - ISA Server 2004: Firewall Policy Node

2. Right click on the 'Firewall Policy' node and select New ▸ Access Rule…This will bring up the New Access Rule Wizard.

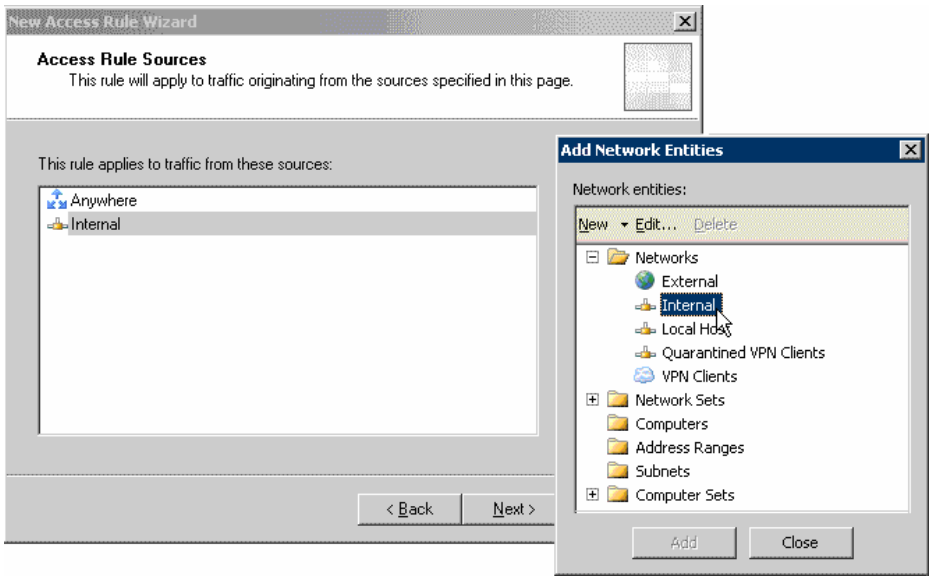
3. Give the rule the name "Block Adult Sites – Based on URLs in Adult Destination Set". Click on **Next** to continue.

4. In the Rule Action page set the permission to 'Deny' and click on **Next** to continue.



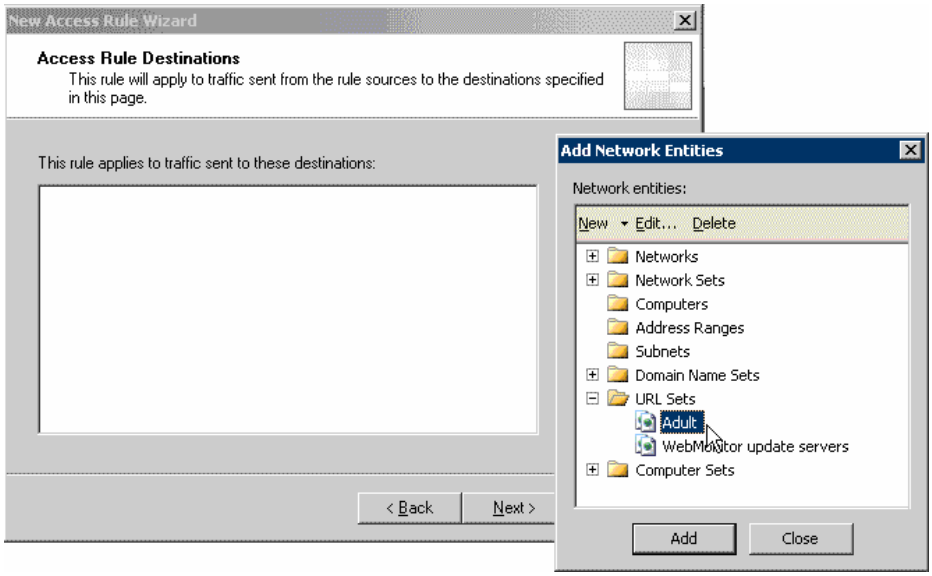
Screenshot 35 - Select the protocols to which this rule applies

5. In the Protocols configuration page, select the option "All outbound traffic". Click on **Next** to continue.



Screenshot 36 - Select the traffic sources to which this rule applies

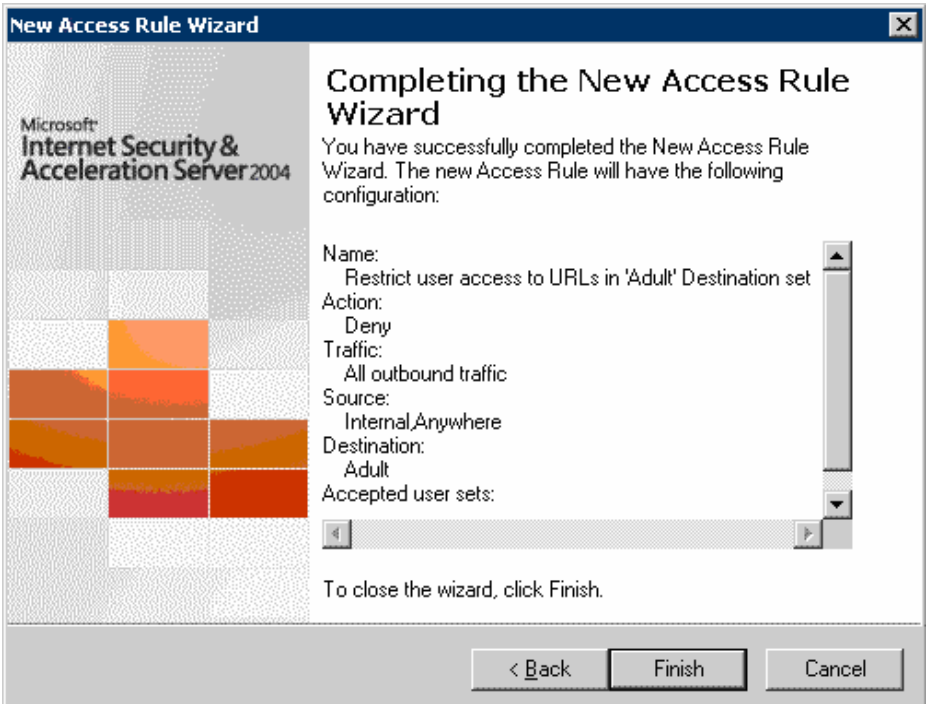
6. In the Access Rule Sources configuration page, click on **Add**. Expand the Networks node and select 'Internal'. Click on **Add** followed by **Close**. Click on **Next** to continue.



Screenshot 37 - Specify the Destination Set to which this rule applies

7. In the Access Rule Destinations page, click on **Add**. Expand the URL Sets node and select the 'Adult' Destination Set. Click on **Add** followed by **Close**. Click on **Next** to continue.

8. In the User Sets page, click on **Next** to continue (the required parameter is already set by default to 'All Users').



Screenshot 38 - Site and Content Rule Wizard: Final dialog showing the configured rule details

9. Click on **Finish**. The new Access Rule policy is now set up on your ISA Server 2004 to block all users from accessing the sites listed in the 'Adult' Destination Set.

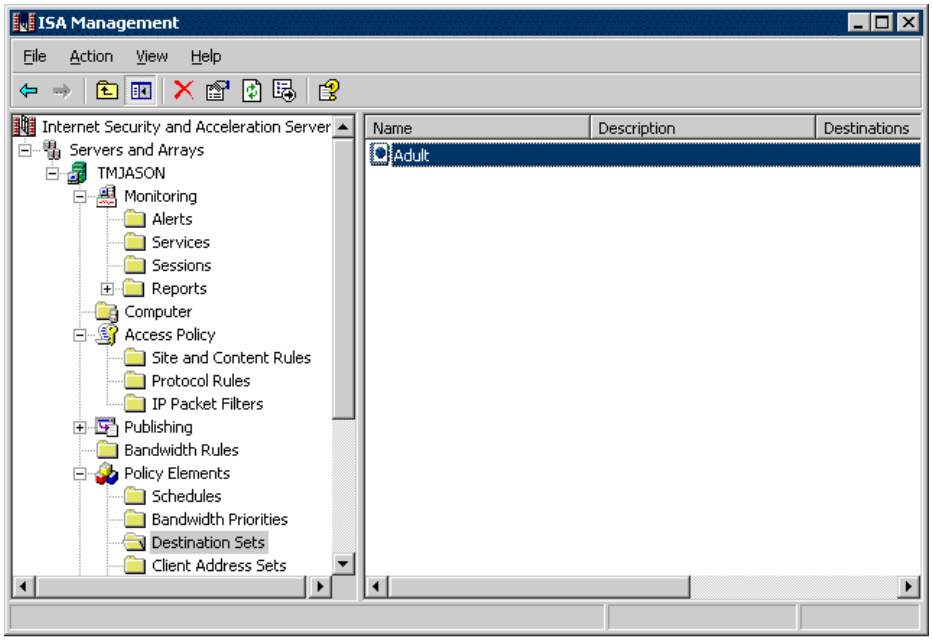
NOTE: The adult Destination/URL Set was created on the ISA Server by GFI WebMonitor installation.

Maintaining the ISA Server 'Adult' Destination/URL Sets

Accessing the 'Adult' Destination Set on ISA Server 2000

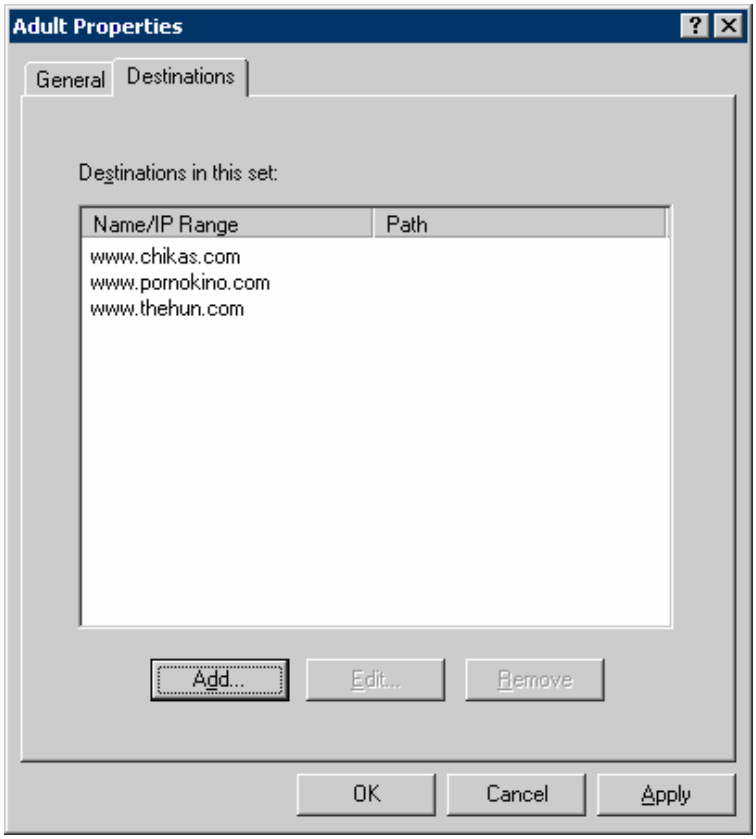
To view the list of sites which are presently contained in the 'Adult' Destination Set of ISA Server 2000:

1. Launch the ISA Server Management console.



Screenshot 39 - List of existing Destination Sets

2. Click on the Policy Elements ▸ Destination Sets node. A list of existing Destination Sets will be displayed in the right pane.



Screenshot 40 – Properties dialog: Viewing the URLs contained in the Adults Destination Set

3. Right click on the entry 'Adult' and select Properties.

4. Go to the 'Destinations' tab to see the list of URLs which were added by GFI WebMonitor in the 'Adult' Destination Set.

NOTE: You can maintain the list through the **Add**, **Edit** and **Remove** buttons respectively.

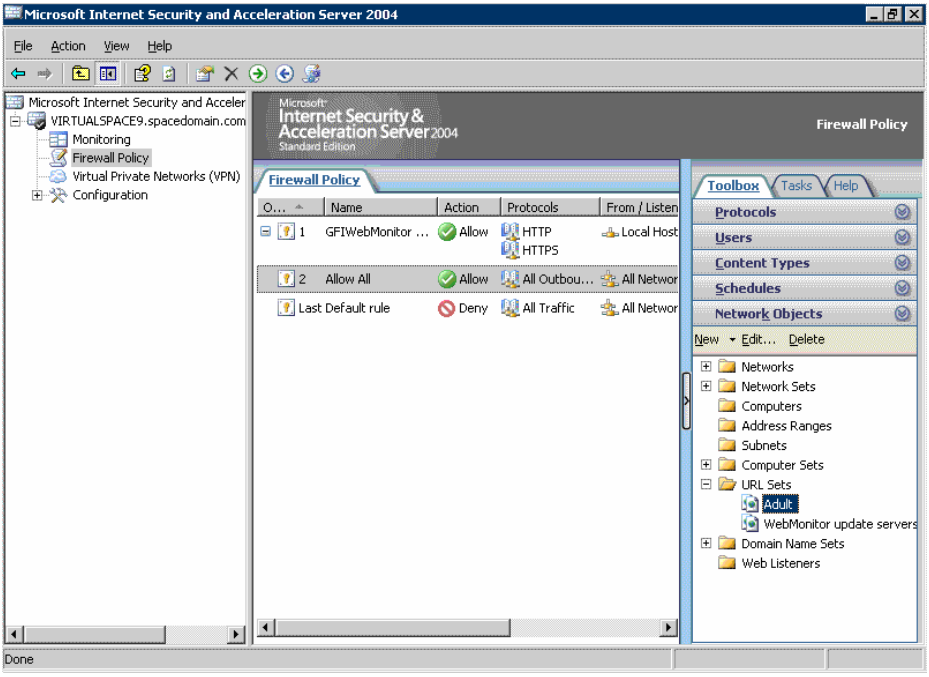
Accessing the 'Adult' Destination Set on ISA Server 2004

To view the list of sites which are presently contained in the 'Adult' URL set of ISA Server 2004:

1. Launch the ISA Server Management console.

2. In the left pane, select the Firewall Policy node.

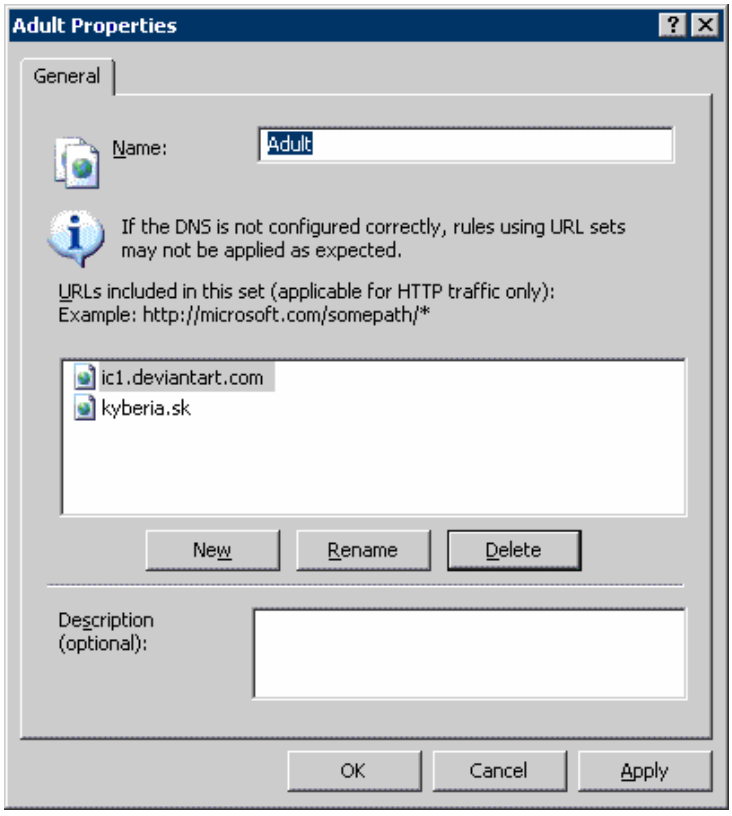
3. In the task pane, click on the 'Toolbox' tab.



Screenshot 41 - List of existing Destination Sets

4. Go to the Network Objects section, and expand the tree node 'URL Sets'.

5. Right click on the entry 'Adult' and select Properties.



Screenshot 42 – Properties dialog: Viewing the URLs contained in the Adults DestinationSset

The ‘General’ tab of the 'Adult' URL set properties lists the URLs which were added by GFI WebMonitor.

NOTE: You can maintain the list through the **Add**, **Edit** and **Remove**

Troubleshooting

Introduction

The troubleshooting chapter explains how to go about resolving any issues you might have. We also recommend visiting the GFI support site.

Knowledge Base

GFI maintains a knowledgebase, which includes answers to most common problems. If you have a problem, please consult the knowledgebase first. The knowledgebase always has the most up-to-date listing of support questions and patches.

The knowledgebase can be found on http://kbase.gfi.com

Web Forum

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

Build notifications

We strongly suggest 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, go to: http://support.gfi.com

Index

V

W