GFI Product Manual

GFI WebMonitor™

Administrator Guide for ISA/TMG

Document Version: 1.2.2

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

Contents

List of Figures

List of Tables

1 Introduction

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

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

1.1 About This Guide

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

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

1.1.1 Terms Used in This Manual

The following terms are used in this manual:

1.1.2 Terms and Conventions Used in This Guide

Table 1: Terms and conventions 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.
Italics text	Parameters and values that you must replace with the applicable value, such as custom paths and filenames.
`Code`	Indicates text values to key in, such as commands and addresses.

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

1.2 About GFI WebMonitor

GFI WebMonitor is available in three editions:

Table 2: GFI WebMonitor Editions

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

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

1.3 How Does GFI WebMonitor Work?

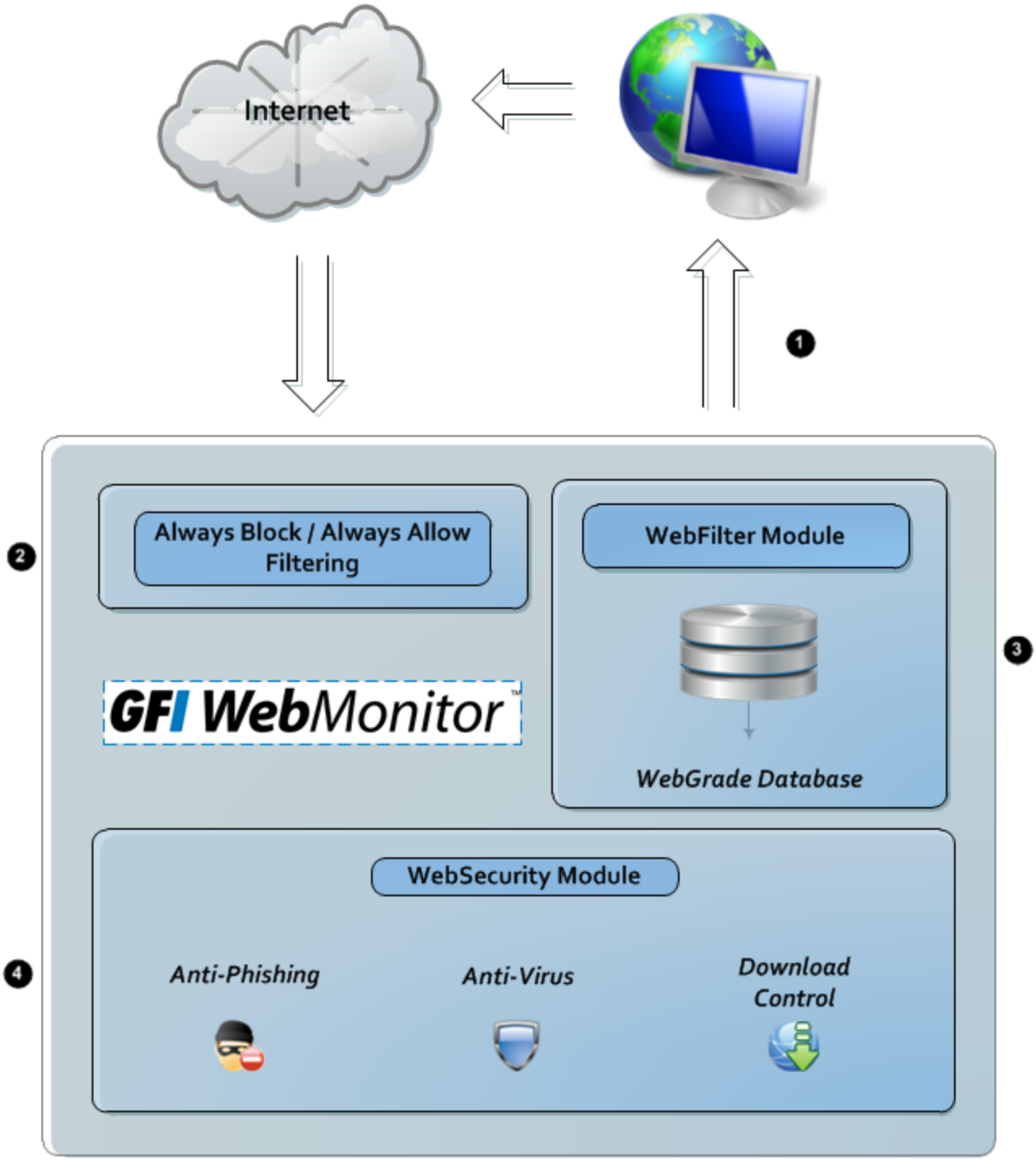


Figure 1: How Does GFI WebMonitor Work?

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

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

Table 3: Always Blocked/Always Allowed filtering actions

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

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

For more information about these categories, refer to Knowledge Base article: http://go.gfi.com/?pageid=WebMon_WebGrade.

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

NOTE

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

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

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

NOTE

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

IMPORTANT

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

1.3.1 Downloading GFI WebMonitor

GFI WebMonitor can be downloaded from: http://go.gfi.com/?pageid=WebMon_Download.

1.3.2 Licensing Information

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

IMPORTANT

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

For more information about licensing, refer to GFI Software Ltd. website at: http://go.gfi.com/?pageid=WebMon_LicensingInformation

1.3.3 Upgrading

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

NOTE

The upgrade procedure is similar to the installation procedure.

NOTE

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

1.4 GFI WebMonitor Services

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

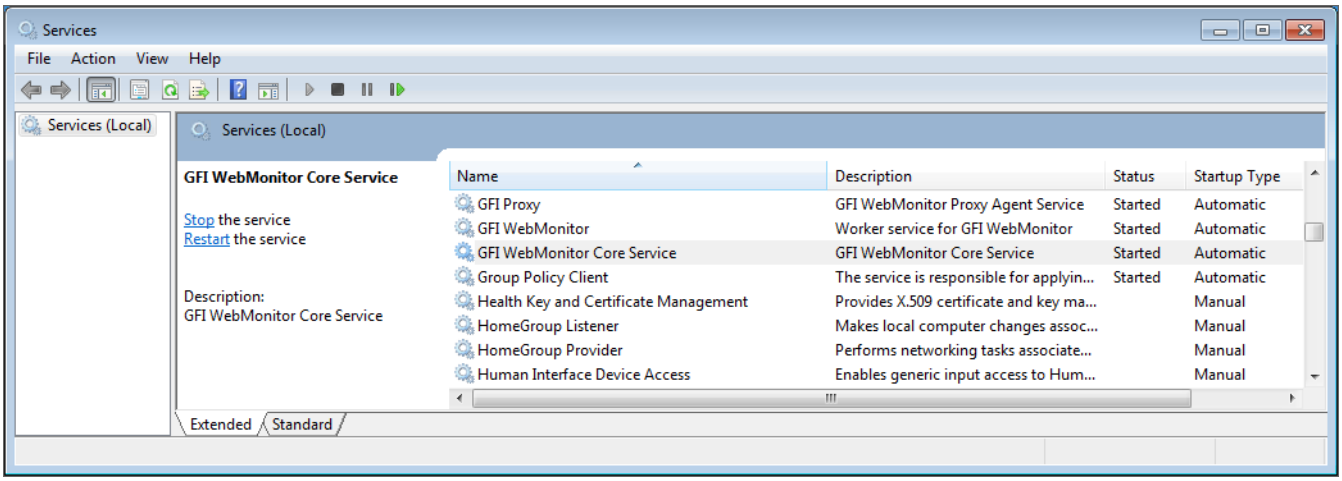
Table 4: GFI WebMonitor Windows® Services

SERVICE NAME	DESCRIPTION	LOCATION AND NAME	USER CREDENTIALS
GFI Proxy	The GFI Proxy service is only created in the Standalone Proxy Version of GFI WebMonitor. It is used as an agent service for the Proxy server, ISAPI module and Web Filtering.	<drive>:\Program Files\GFI\WebMonitor\GFiProxy.exe	Local System

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

To view status of GFI WebMonitor services:

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



Screenshot 1: GFI WebMonitor Services

2. From the list of services displayed locate the following services:

- GFI Proxy
- GFI WebMonitor
- GFI WebMonitor Core Service

2 Installing GFI WebMonitor

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

2.1 System Requirements

2.1.1 Software

Table 5: Software requirements

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

2.1.2 Hardware

Minimum hardware requirements depend on the GFI WebMonitor edition.

Table 6: Hardware requirements

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

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

IMPORTANT

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

NOTE

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

2.1.3 Microsoft® ISA / Forefront TMG Mode Pre-requisites

IMPORTANT

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

2.2 Deployment Scenarios

GFI WebMonitor can be deployed in three modes:

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

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

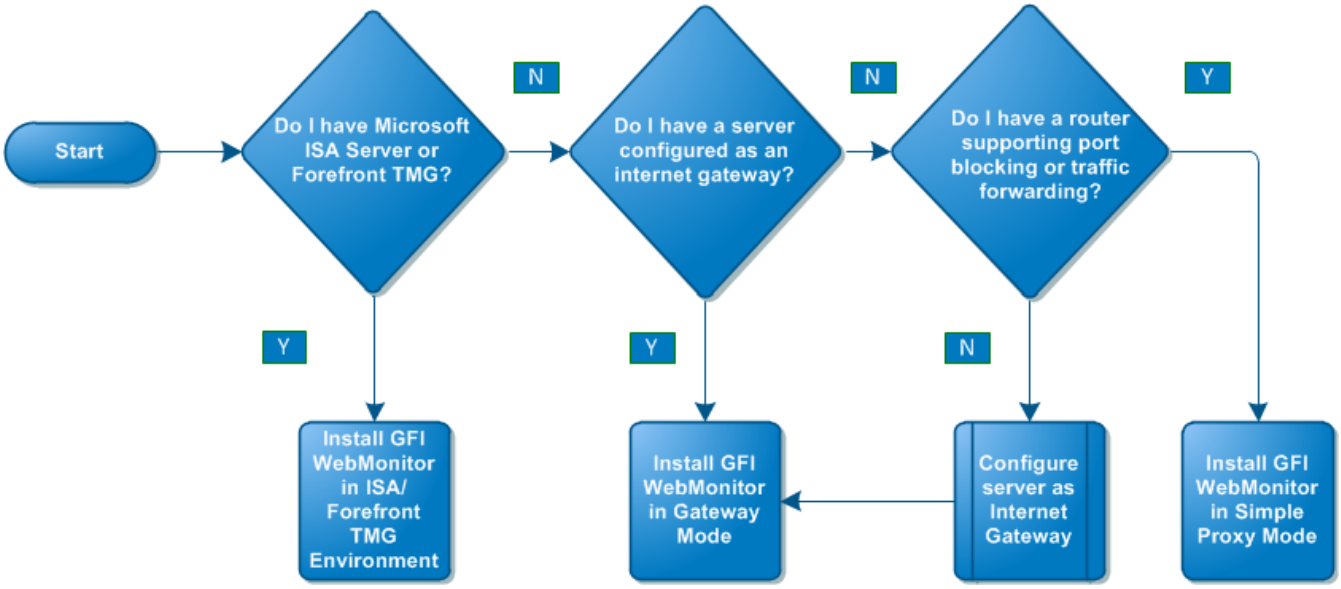
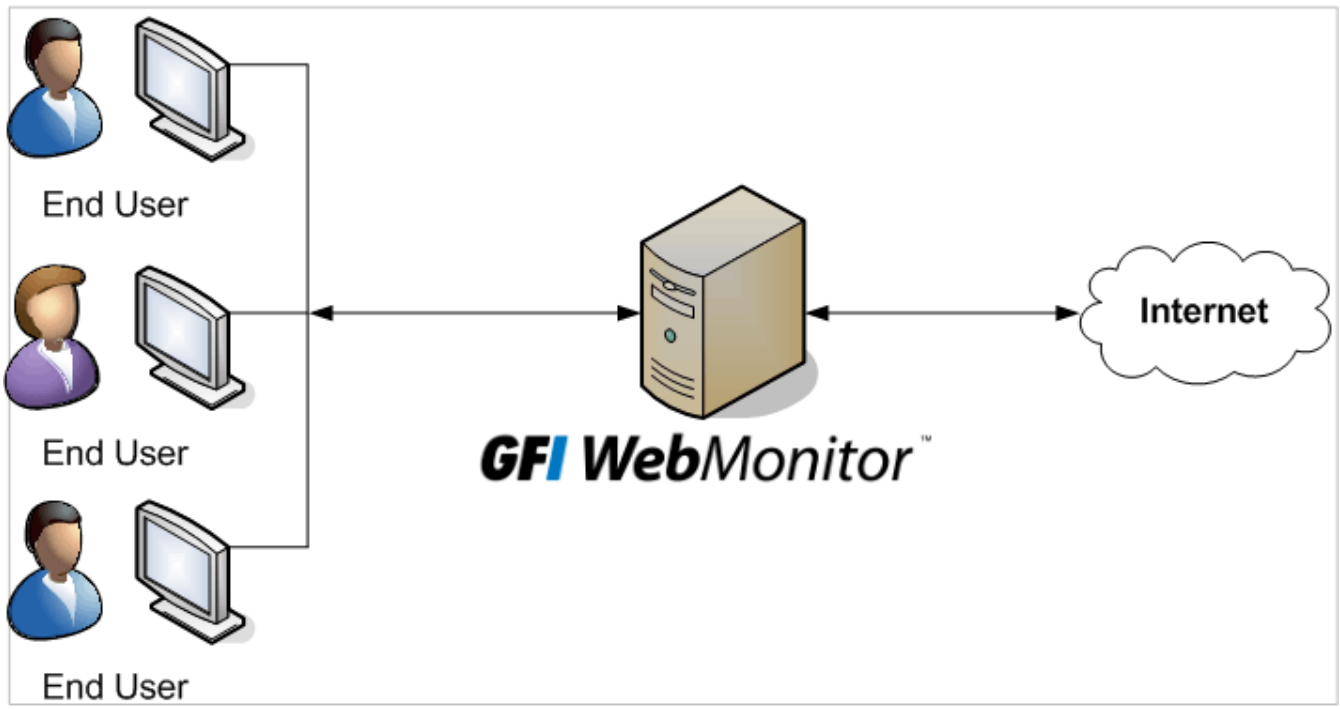


Figure 2: Choosing your environment

2.2.1 Deployment in a Microsoft ISA Server or Forefront TMG Environment

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



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

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

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

2.3 Installing GFI WebMonitor for IsaTmg

2.3.1 Introduction

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

2.3.2 Installation Procedure

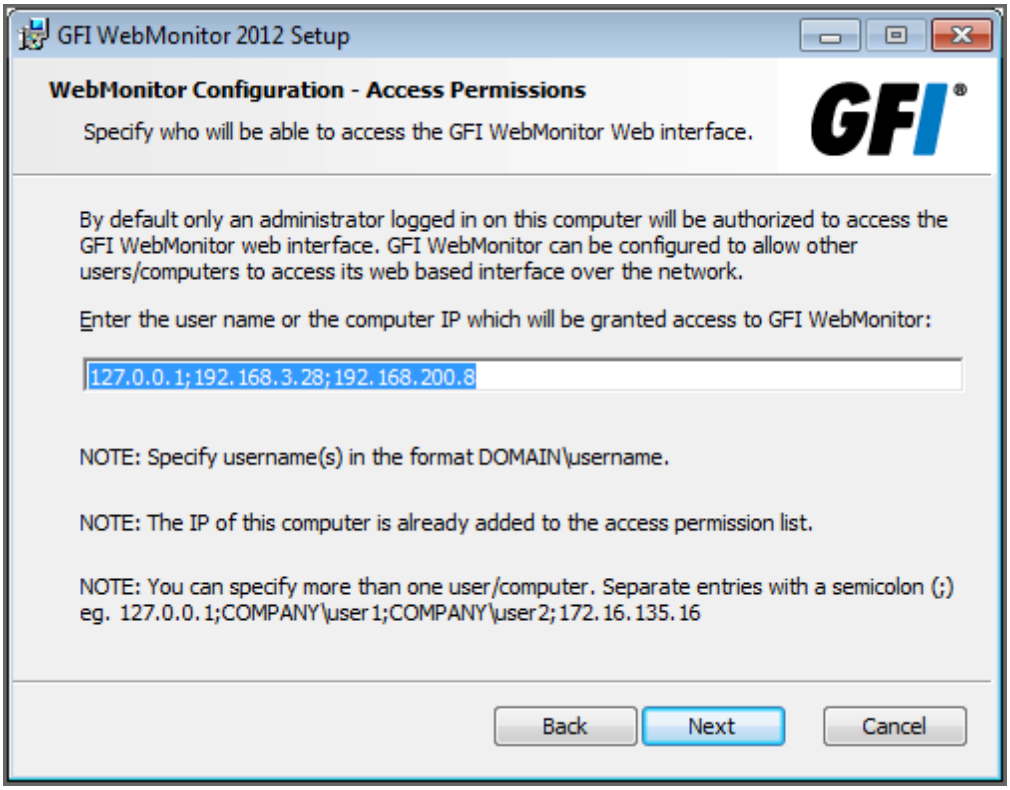
Run the installer as a user with administrative privileges on the target machine.

1. Double click the GFI WebMonitor executable file.

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

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

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



Screenshot 3: Installation: Access Permissions

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

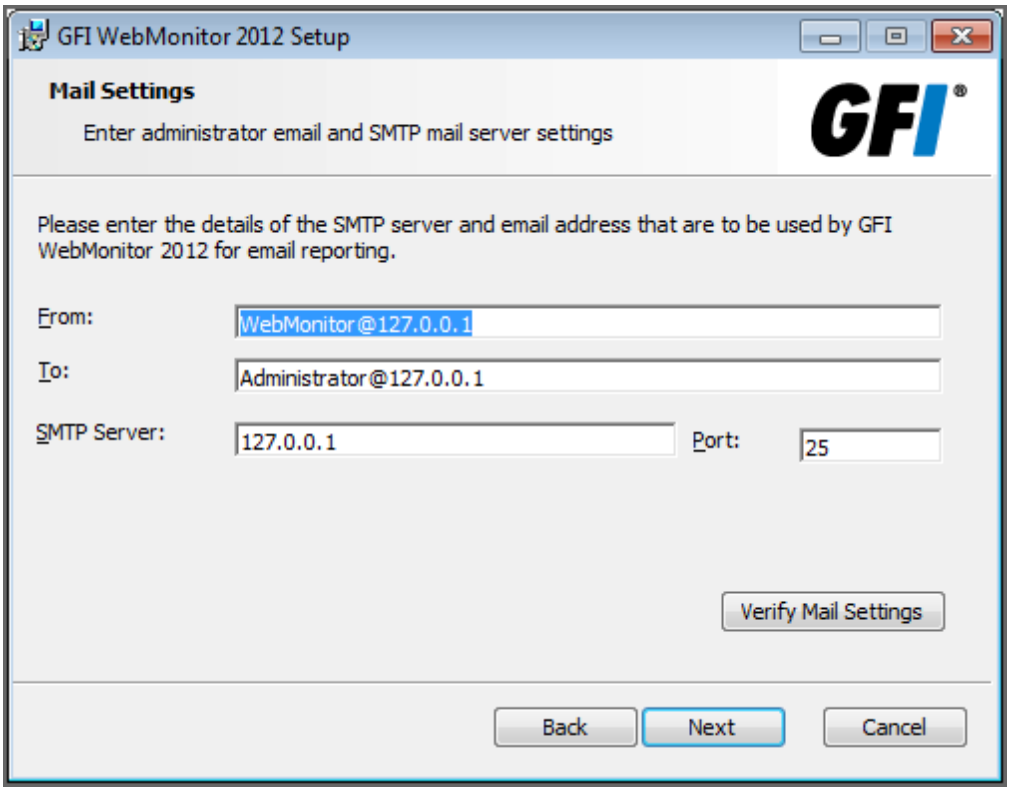
> **NOTE**
>
> More than one user or machine can be specified. Separate entries with semicolons ';'

Screenshot 4: Installation: Service Logon Information

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

NOTE

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



Screenshot 5: Installation: Mail Settings

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

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

8. Click **Next** to install in default location or click **Change** to change installation path.

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

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

3 Post Installation Actions

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

3.1 Launching GFI WebMonitor

On the same machine where GFI WebMonitor is installed:

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

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

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

From a remote machine:

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

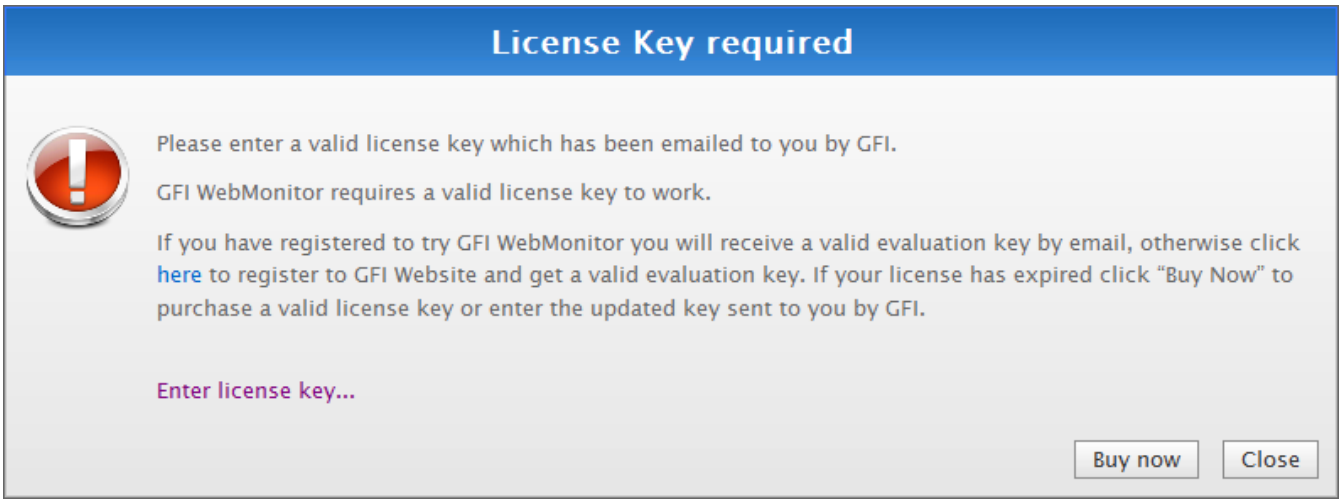
> **NOTE**
>
> User access to the application can be granted either during installation or from the Remote Access Control node.

3.2 Enter a Valid License Key

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

NOTE

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



Screenshot 6: License key required

To enter your license key:

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

NOTE

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

NOTE

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

See Also:

Licensing Information

3.3 Configure Proxy Settings

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

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

3.4 Configuring FTP

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

» Disabling folder view in Microsoft Internet Explorer on each client machine

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

» Configuring FTP access in Microsoft ISA Server / Forefront TMG.

- FTP access can be configured by:
  - **Option 1:** Restricting or denying FTP access
  - **Option 2:** Disabling the FTP Access Filter

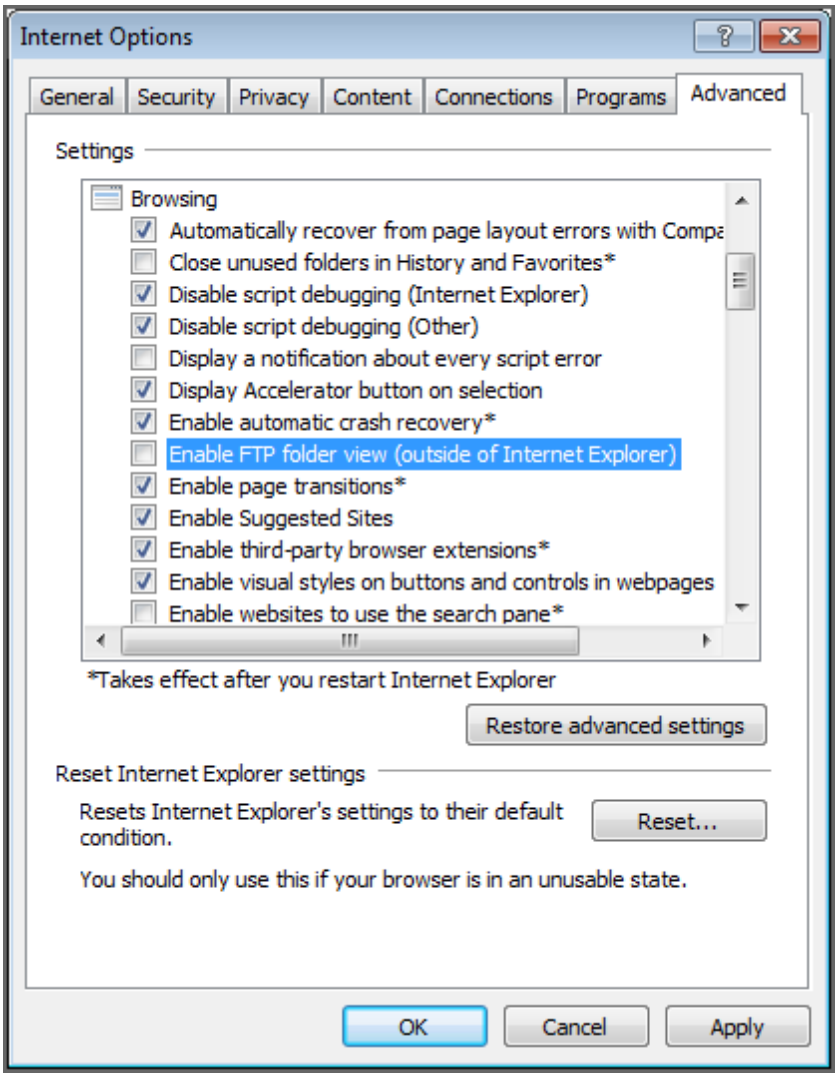
> **NOTE**
>
> To ensure that all users browse and download from FTP servers through proxy, the administrator should disable folder view and configure the proxy settings on the users' machines.

3.4.1 Step 1: Disabling Folder View in Microsoft Internet Explorer

To disable folder view in Microsoft Internet Explorer:

1. Launch **Microsoft Internet Explorer** on the client machine.

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



Screenshot 7: Internet Options dialog box

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

NOTE

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

3.4.2 Step 2: Configuring Browsers to Use a Proxy Server

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

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

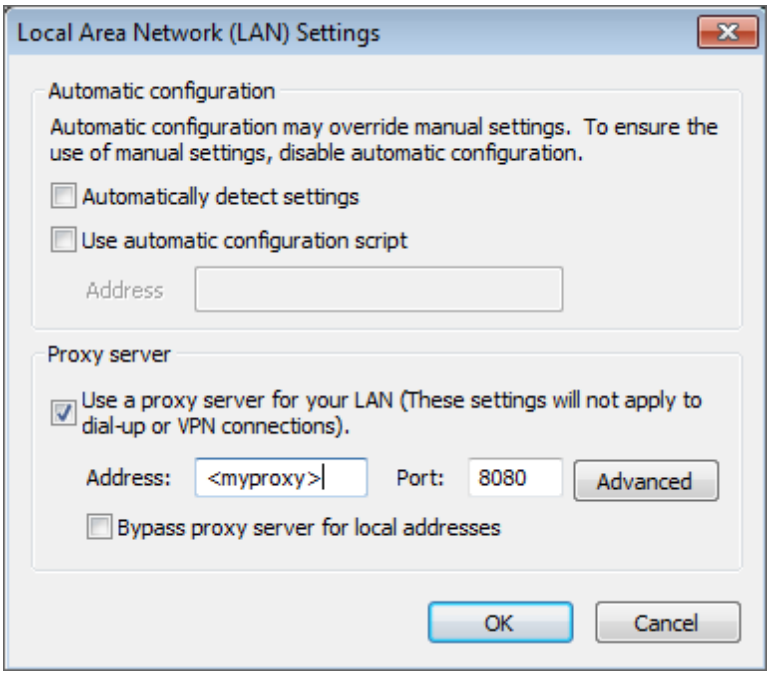
3.4.3 Option 2: Configuring Proxy settings manually

To configure proxy settings manually:

1. Launch **Microsoft Internet Explorer**

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

3. Click **LAN settings**.



Screenshot 8: LAN Settings dialog

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

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

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

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

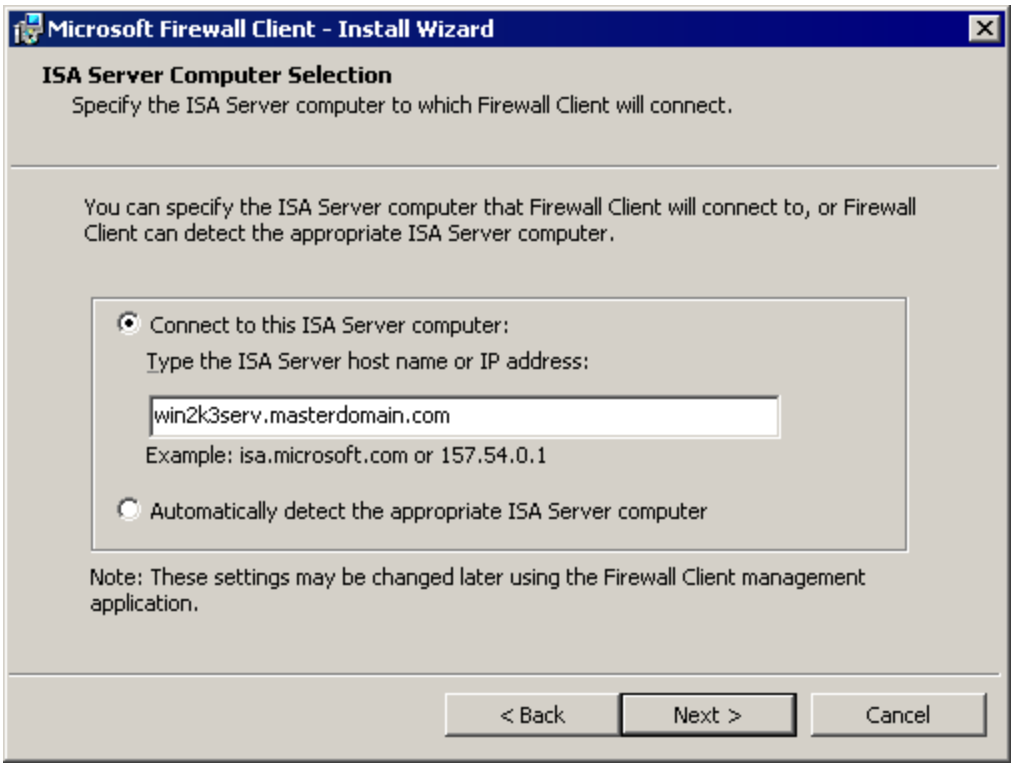
3.4.4 Option 1: Configuring Proxy settings automatically in Microsoft® ISA Server and Microsoft® Forefront TMG

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

To install Microsoft® Firewall Client for ISA Server:

1. Download **Microsoft Firewall Client for ISA Server** from the Microsoft® web site.

2. Double click the **Microsoft Firewall Client for ISA Server** executable file.



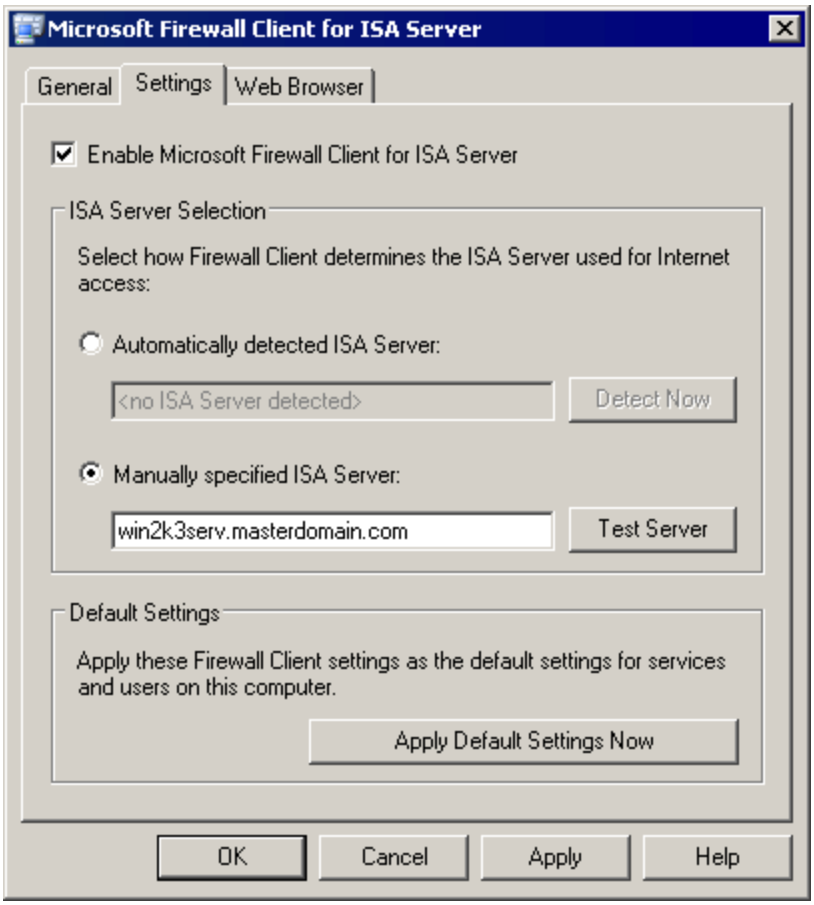
Screenshot 9: Microsoft Firewall Client for ISA Server: Installation wizard dialog

3. Select **Connect to this ISA Server computer**.

4. Key in the full machine name or IP address and continue to finalize the setup.

5. After installation, restart the client machine.

6. Right click in the Windows® notification area and choose **Configure**.



Screenshot 10: Microsoft® Firewall Client for ISA Server: Settings tab

NOTE

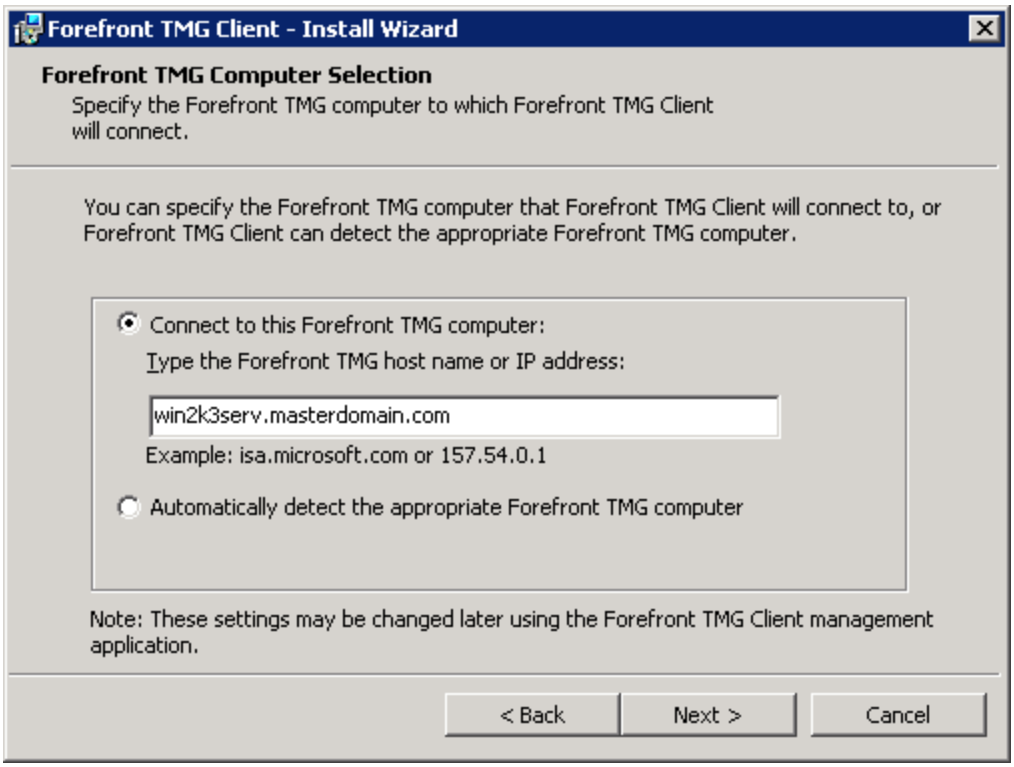
Click **Settings** Tab to modify the server configurations.

To configure the web browser automatically:

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

To install the Microsoft Firewall Client for Microsoft Forefront TMG:

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



Screenshot 11: Microsoft® Firewall Client for Forefront TMG: Installation wizard dialog

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

6. Key in the full machine name or IP address and click **Next**.

7. Click **Install** and click **Finish**.

To configure the web browser automatically:

1. Select **Web Browser** tab in the **Microsoft Firewall Client for Forefront TMG** dialog.

2. Check **Enable Web browser automatic configuration** checkbox.

3. Click **Configure Now**.

4. Click **OK**.

3.4.5 Step 3: Configuring FTP access

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

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

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

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

Option 2: Disabling the FTP Access Filter

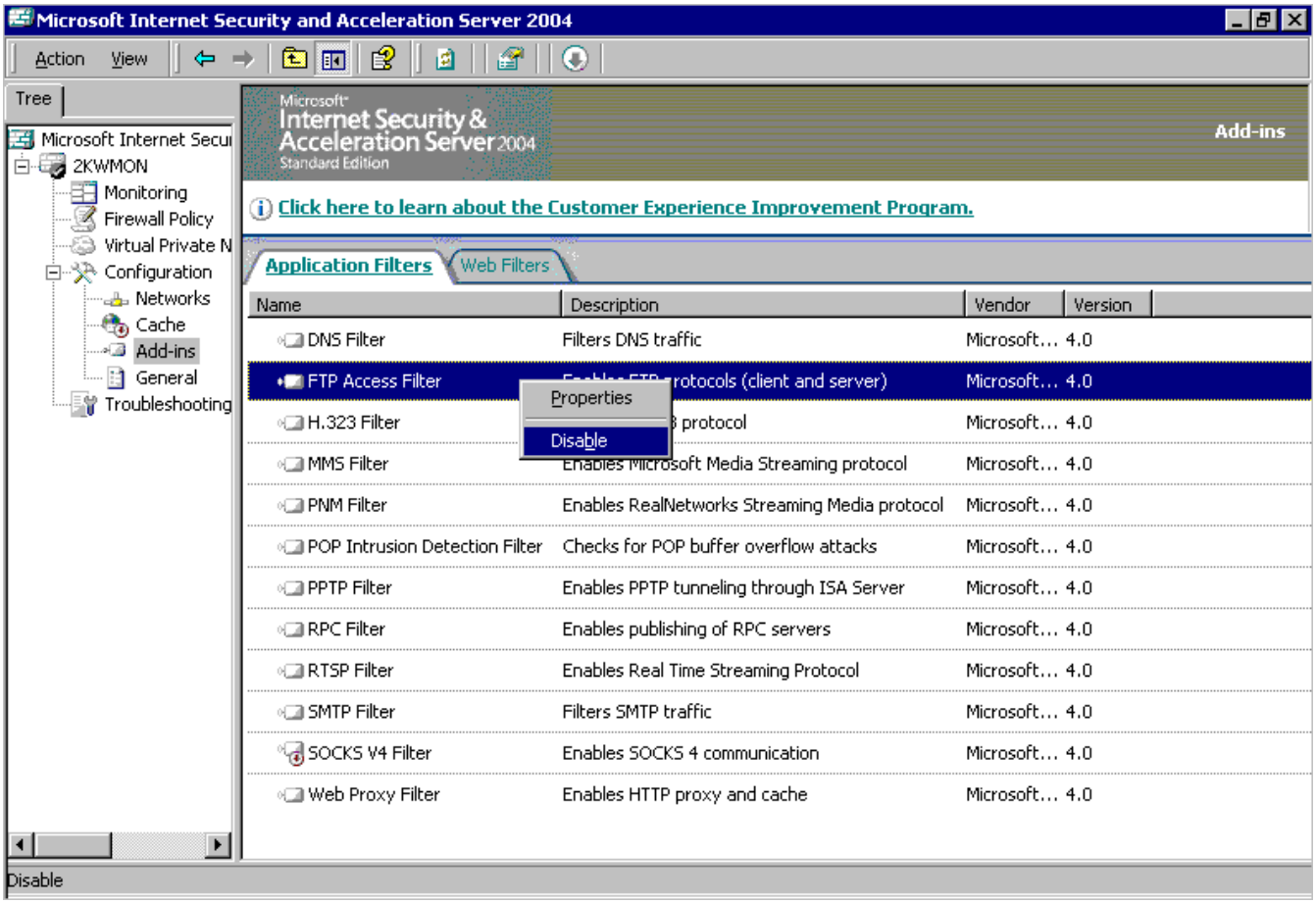
Option 2: Disabling the FTP Access Filter

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

Disabling the FTP Access Filter in Microsoft ISA Server 2004

To disable the FTP Access Filter:

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



Screenshot 12: Microsoft ISA Server 2004: Configured Application filters

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

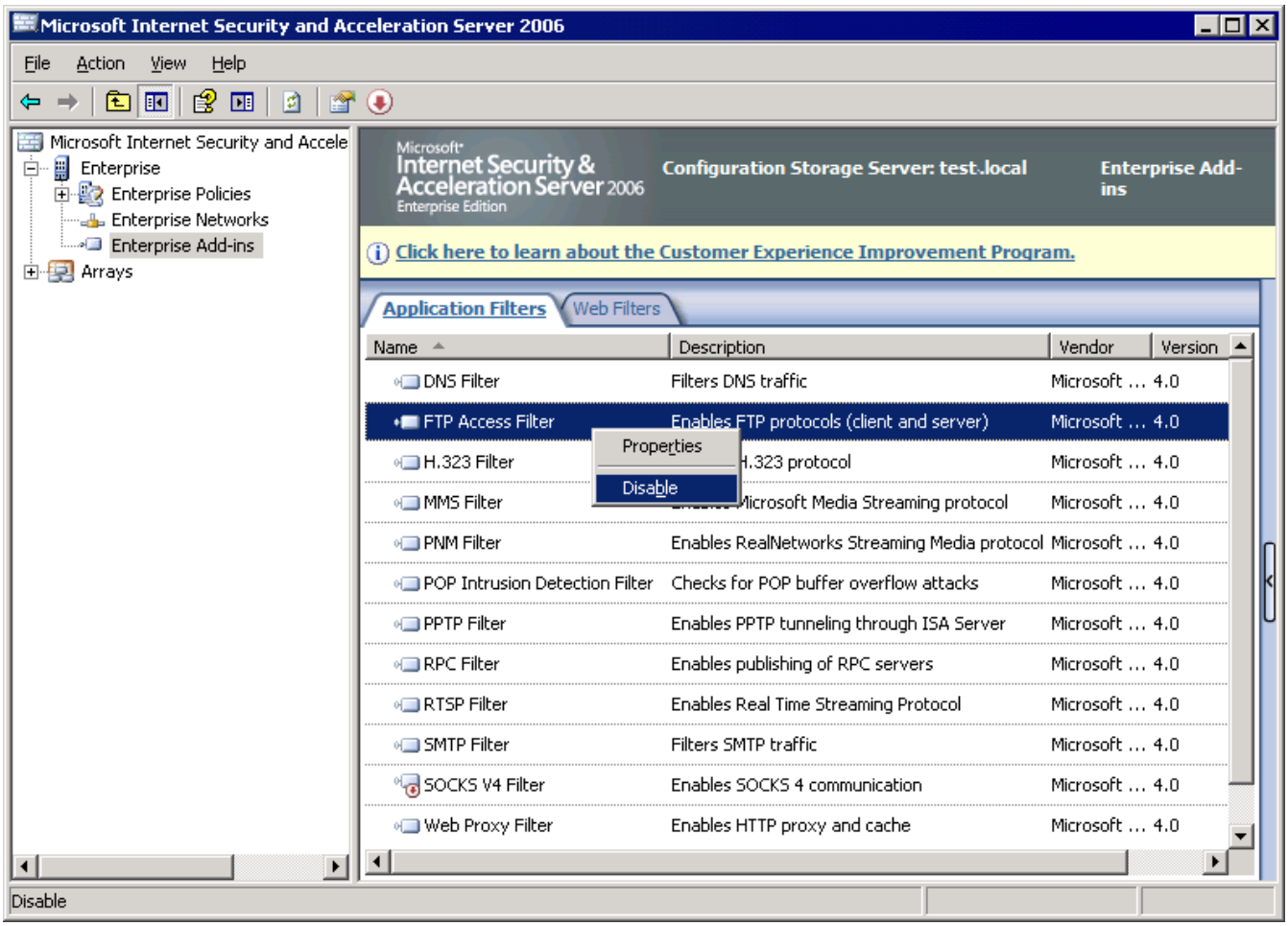
3. Right-click **FTP Access Filter** and select **Disable**.

4. Save settings before exiting.

Disabling the FTP Access Filter in Microsoft ISA Server 2006

To disable the FTP Access Filter:

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



Screenshot 13: Microsoft ISA Server 2006: Configured Application filters

2. From the left panel, expand **Enterprise > Enterprise Add-ins**.

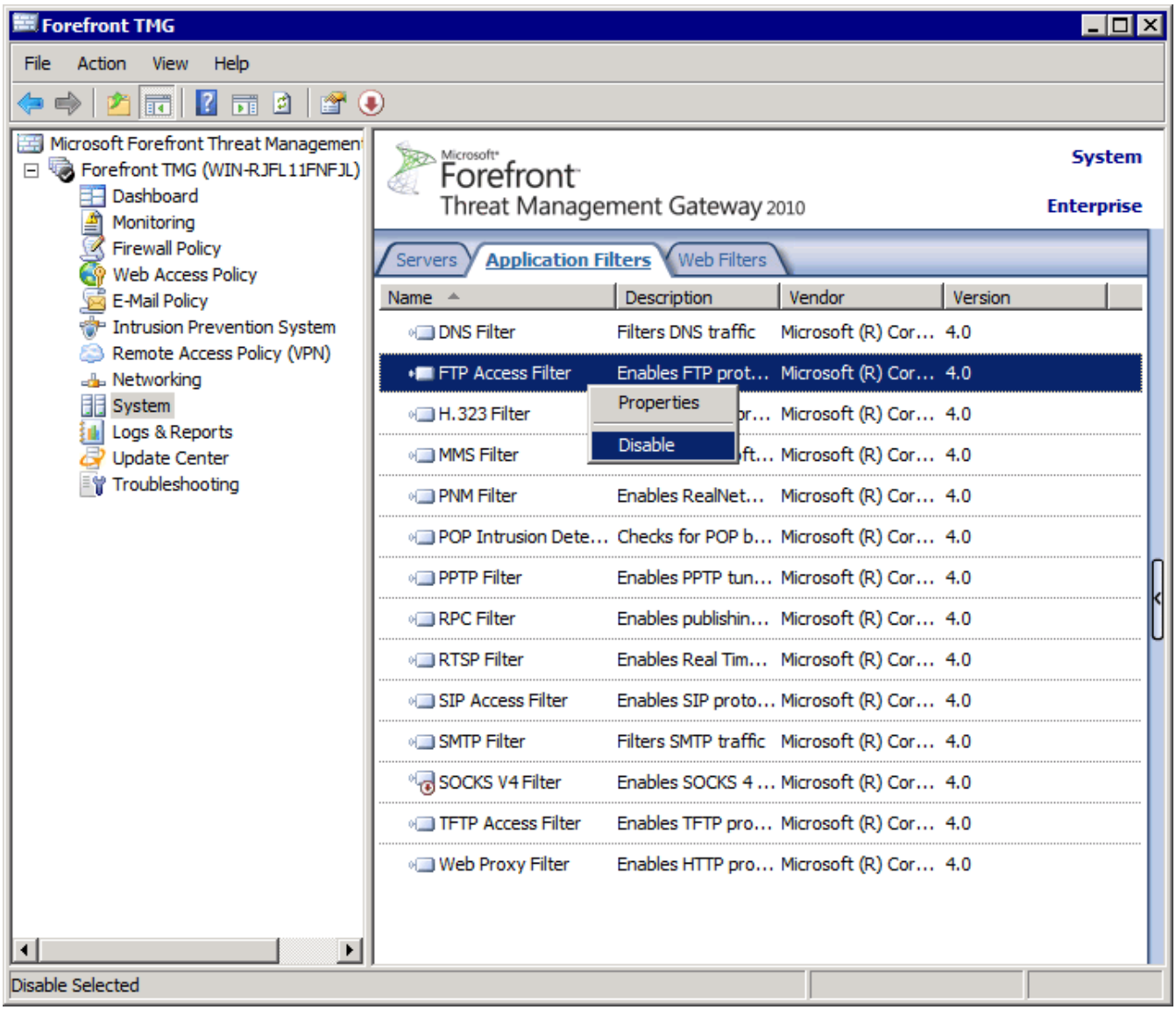
3. Right-click **FTP Access Filter** and select **Disable**.

4. Save settings before exiting.

Disable FTP Access Filter in Microsoft Forefront TMG

To disable the FTP Access Filter:

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



Screenshot 14: Microsoft Forefront TMG: Configured Application filters

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

3. From the right panel, click **Application Filters** tab.

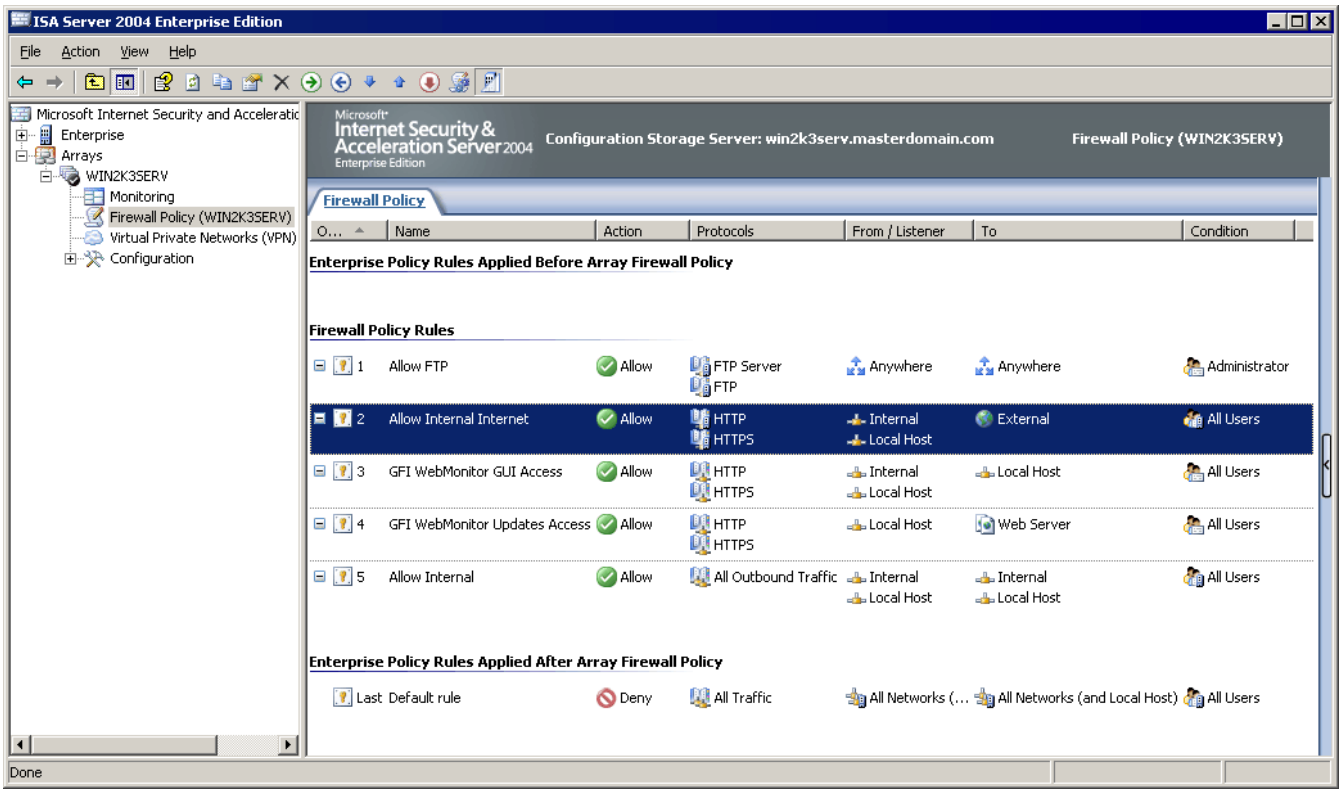
4. Right click **FTP Access Filter** and select **Disable**.

5. Click **Apply**.

6. Save settings.

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

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



Screenshot 15: Microsoft ISA Server: Configured Firewall policies

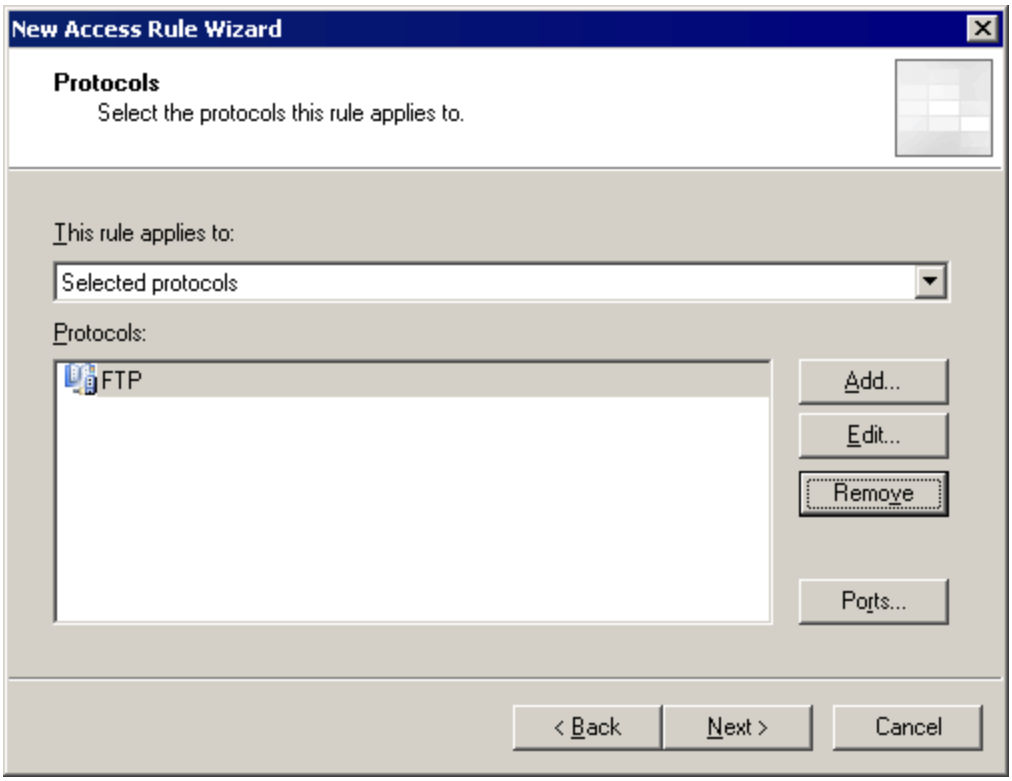
The preceding screenshot shows both rules.

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

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

On Microsoft ISA Server

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



Screenshot 16: Microsoft ISA Server: Protocols dialog

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

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

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

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

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

11. In the **Access Rule Sources** dialog click **Next**.

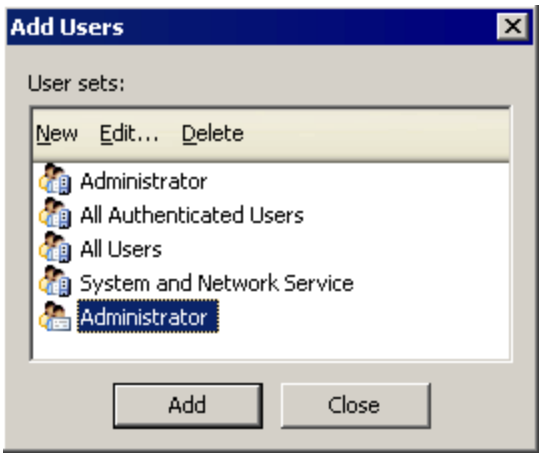
12. In the **Access Rule Destinations** dialog, click **Add**.

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

14. In the **Access Rule Destinations** dialog click **Next**.

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

16. Click **Add**.



Screenshot 17: Microsoft ISA Server: Add Users dialog

17. In the **Add Users** dialog, select **Administrator**, click **Add** and click **Close**.

18. Click **Next** and **Finish**.

19. Make sure to save settings before exiting.

On Microsoft Forefront TMG

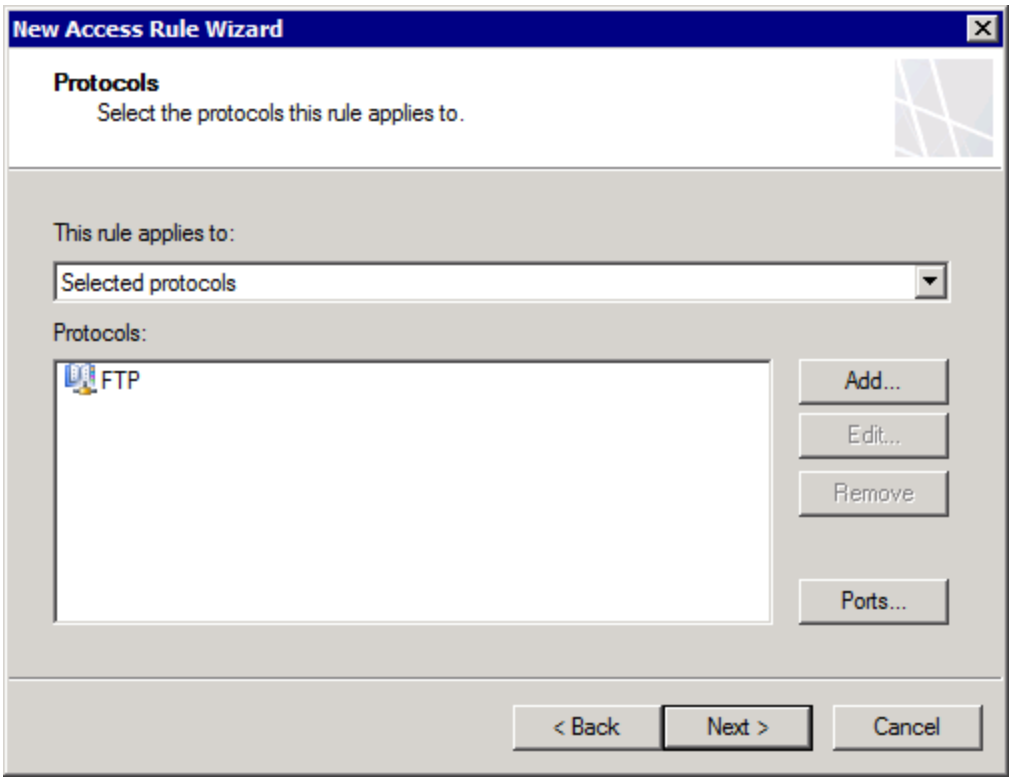
1. On the Microsoft Forefront TMG machine, navigate to **Start > Programs > Microsoft Forefront TMG > Forefront TMG Management**.

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

3. Right-click **Firewall Policy** and select **New > Access Rule**.

4. Key in a name for this rule; for example 'Allow FTP' and click **Next**.

5. Select **Allow** and click **Next**.

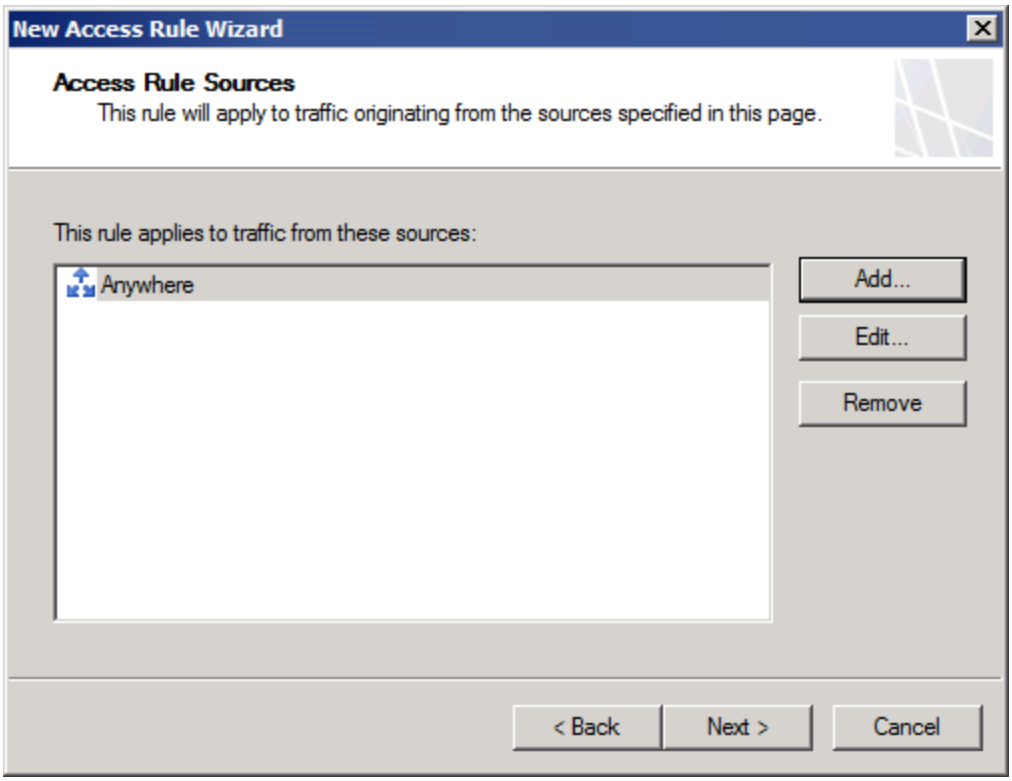


Screenshot 18: Microsoft Forefront TMG: Protocols dialog

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

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

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



Screenshot 19: Microsoft Forefront TMG: Access Rule Sources dialog

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

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

11. In the **Access Rule Sources** dialog click **Next**.

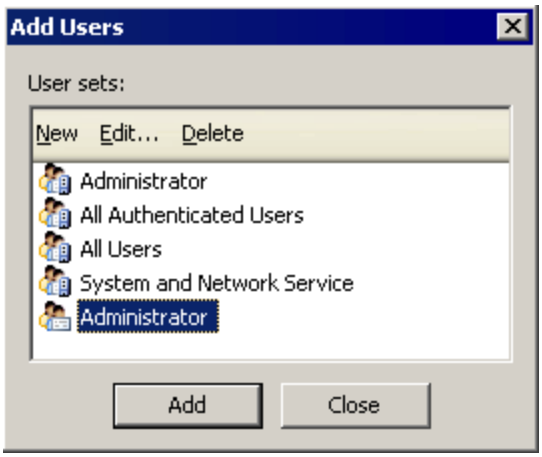
12. In the **Access Rule Destinations** dialog, click **Add**.

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

14. In the **Access Rule Destinations** dialog click **Next**.

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

16. Click **Add**.



Screenshot 20: Microsoft ISA Server: Add Users dialog

17. In the **Add Users** dialog, select **Administrator**, click **Add** and click **Close**.

18. Click **Next** and **Finish**.

19. Save settings before exiting.

3.5 Using the Settings Importer Tool

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

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

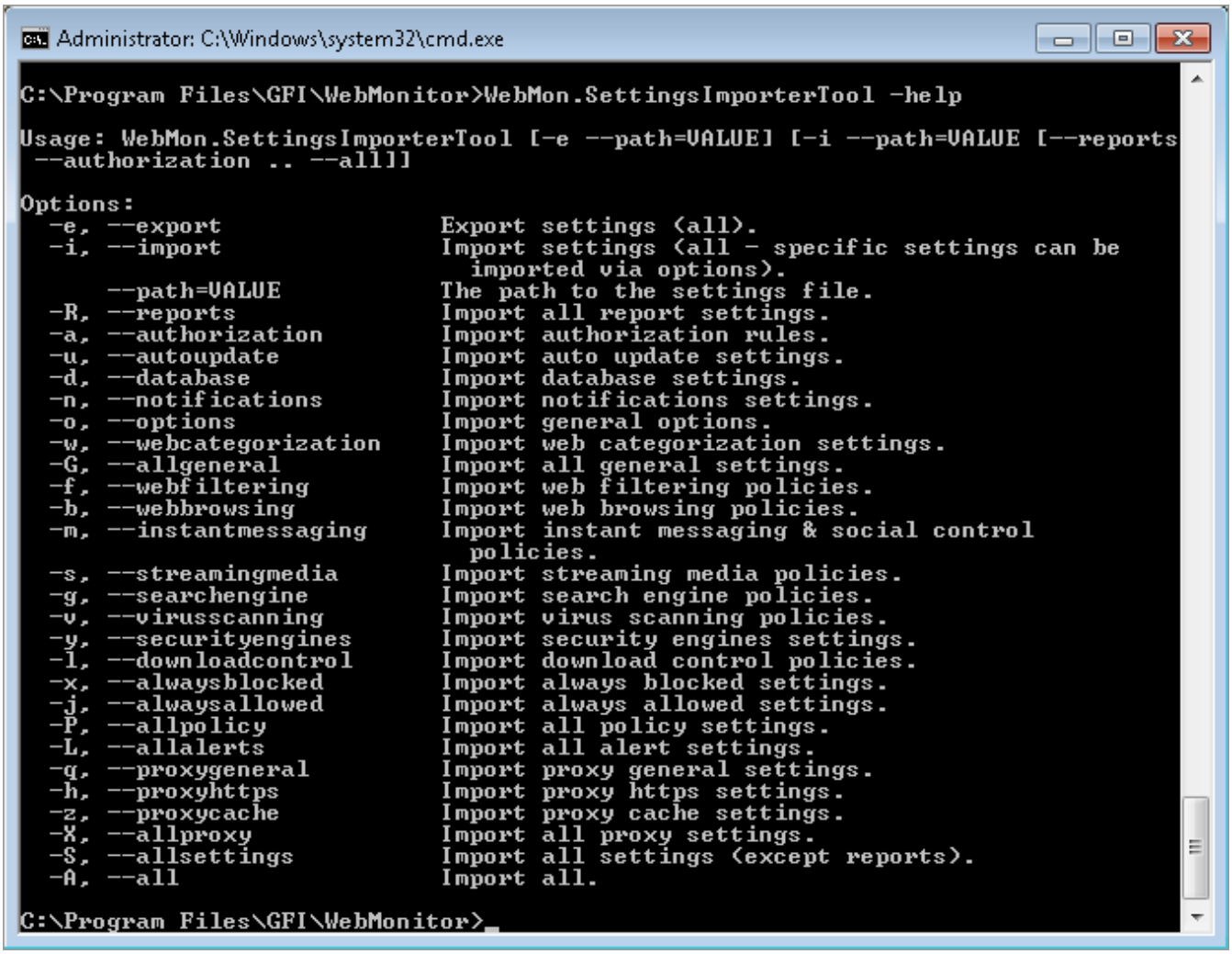
3.5.1 Exporting / Importing Configuration Settings

To use the Settings Importer Tool:

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

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

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



Screenshot 21: Settings Importer Tool Controls

NOTE

The controls apply only when importing configuration settings.

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

Example 1 - Exporting all settings:

To export the current settings, type:

```
WebMon.SettingsImporterTool -e
```

Settings are exported to a single file and when the process is complete, the following message is displayed:

```
Exported WebMonitor settings to C:Program Files\GFI\WebMonitor\<filename>.gz
```

Example 2 - Importing settings:

To import exported settings, type:

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

When import is complete, the following message is displayed:

```
Successfully imported <All> WebMonitor settings from <filename>
```

NOTE

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

4 Achieving Results

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

- Protect Your Network
- Increase Productivity
- Maximize Available Bandwidth

4.1 Achieving Results with GFI WebMonitor - Protecting Your Network

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

WebFilter Edition

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

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

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

WebSecurity Edition

1. **Block Known Malicious Websites and Phishing.**
   - Configure ThreatTrack
   - Configuring Anti-Phishing in Security Policies
   - Configure Auto-update of all security engines
   - Configure Auto-update of all security engines

2. **Control and scan your downloads using multiple anti-virus engines.**
   - Configure Downloads Policies
   - Configuring Security Policies

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

4.2 Achieving Results with GFI WebMonitor - Maximize Bandwidth Availability

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

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

» Generate Activity reports

» Generate Bandwidth reports

» Configure Internet Policies

2. **Monitor and manage Internet connections in real-time to optimize bandwidth.**

» Use the Bandwidth Dashboard

» Use the Activity Dashboard

» Terminate active connections from the Real-Time Traffic Dashboard

3. **Manage website categories in the Bandwidth control group (such as Streaming Media, P2P, Online Personal Storage).**

» Configure Web Filtering Polices

4. **Block access to unwanted streaming applications such as YouTube and similar video sharing web sites.**

» Configure Streaming Media Policies

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

» Configure Instant Messaging Policies

6. **Set bandwidth thresholds to limit access to specific web site categories, based on time or bandwidth limits.**

» Configure Web Browsing Quota Policies

7. **Use proxy caching to accelerate service requests and optimize bandwidth. This functionality retrieves content saved from a previous client request.**

» Configure Cache Settings

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

4.3 Achieving Results with GFI WebMonitor - Increase Productivity

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

1. **Deploy GFI WebMonitoron your network without any filtering policies. Use the inbuilt monitoring and reporting tools to observe Internet use and identify patterns that impact your organization's productivity. Create adequate policies based on the results obtained from these reports.**

» Use the Bandwidth Dashboard

» Use the Activity Dashboard

» Generate Activity reports

» Generate Bandwidth reports

» Configure Internet Policies

2. **Block website categories in the Productivity Loss and Potential Productivity Loss groups (such as Social Network, Dating, Games and Pay to Surf).**

» Configure Web Filtering Polices

3. **Block access to streaming applications.**

» Configure Streaming Media Policies

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

» Configure Instant Messaging Policies

5. **Limit access to specific web site categories based on time or bandwidth limits.**

» Configure Web Browsing Quota Policies

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

5 Using the Dashboard

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

Table 7: Monitoring tools

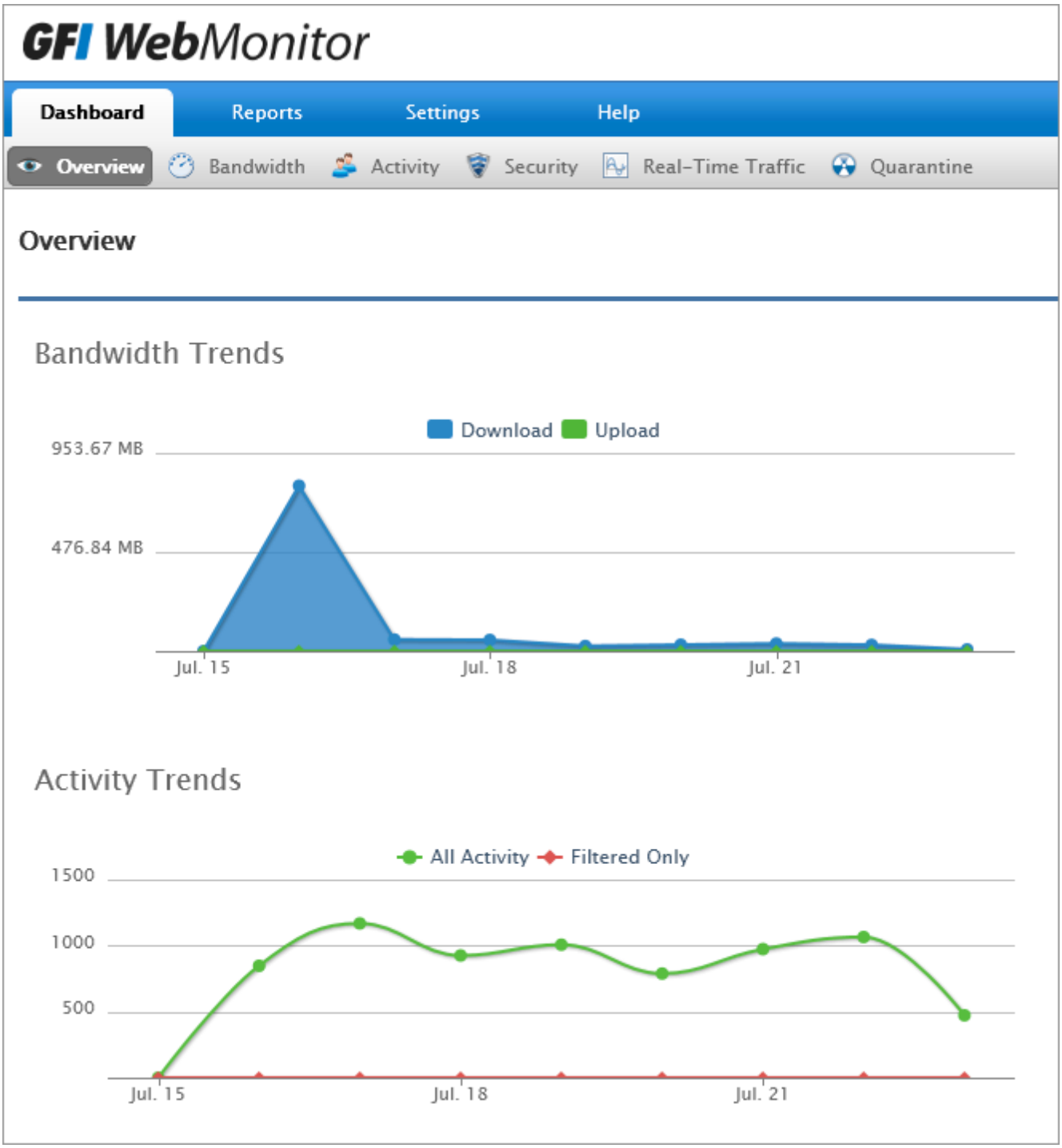
OPTION	DESCRIPTION
Overview	Provides a quick glance of current activity on the network, enabling you to identify network usage trends and tasks that need to be carried out by the administrator.
Bandwidth	Shows activity related to bandwidth consumption. Use the provided filters to spot downloads or uploads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

NOTE

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

5.1 Overview of Internet Activity

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



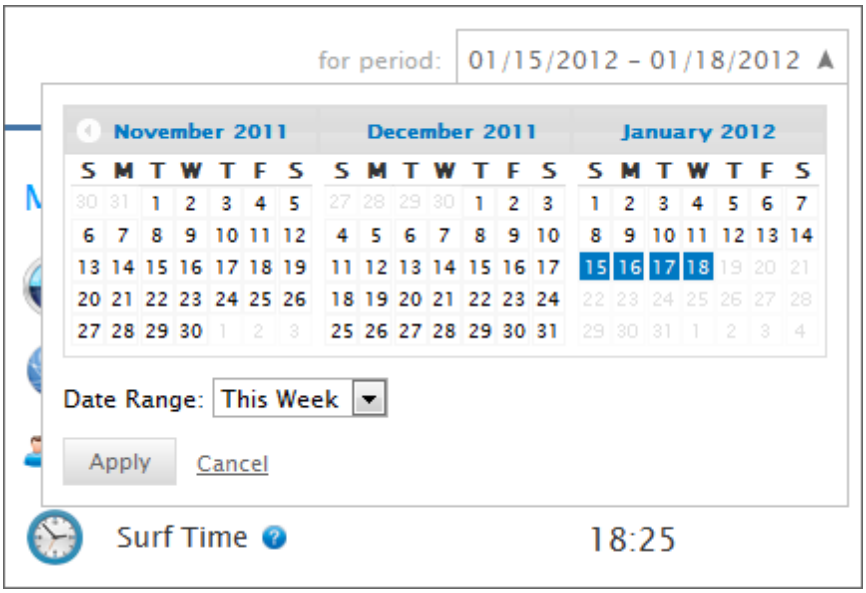
Screenshot 22: Dashboard Overview

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

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

NOTE

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



Screenshot 23: Using the calendar to set period

5.1.1 WebGrade Categorization

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

Screenshot 24: Website Category Lookup feature

To check a website:

1. Type URL in the space provided.

2. Click  icon.

NOTE

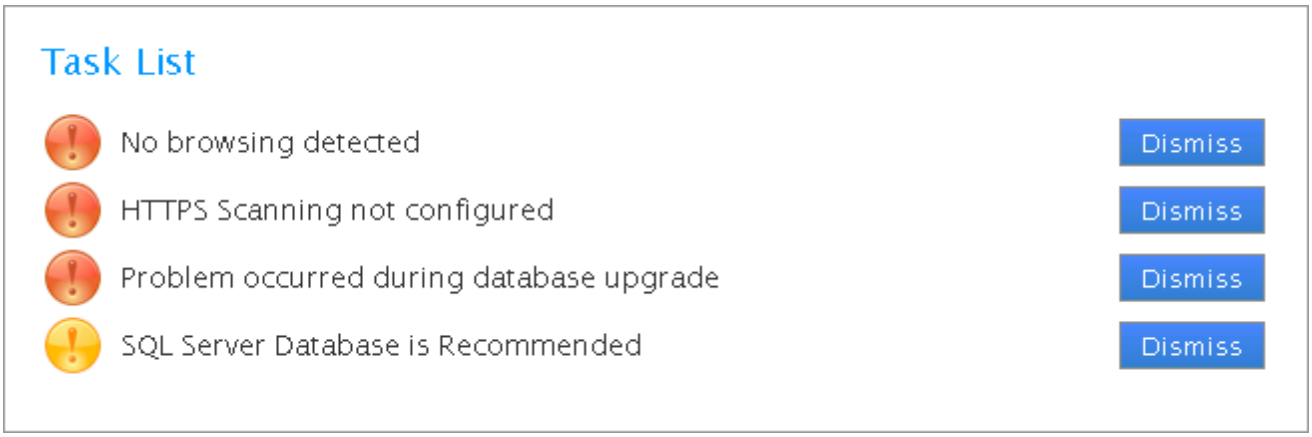
For more information, refer to Configuring Web Categorization (page 78).

5.1.2 Pending Task List

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

After performing a task, click 

to remove it from the list.



Screenshot 25: Pending tasks list

IMPORTANT

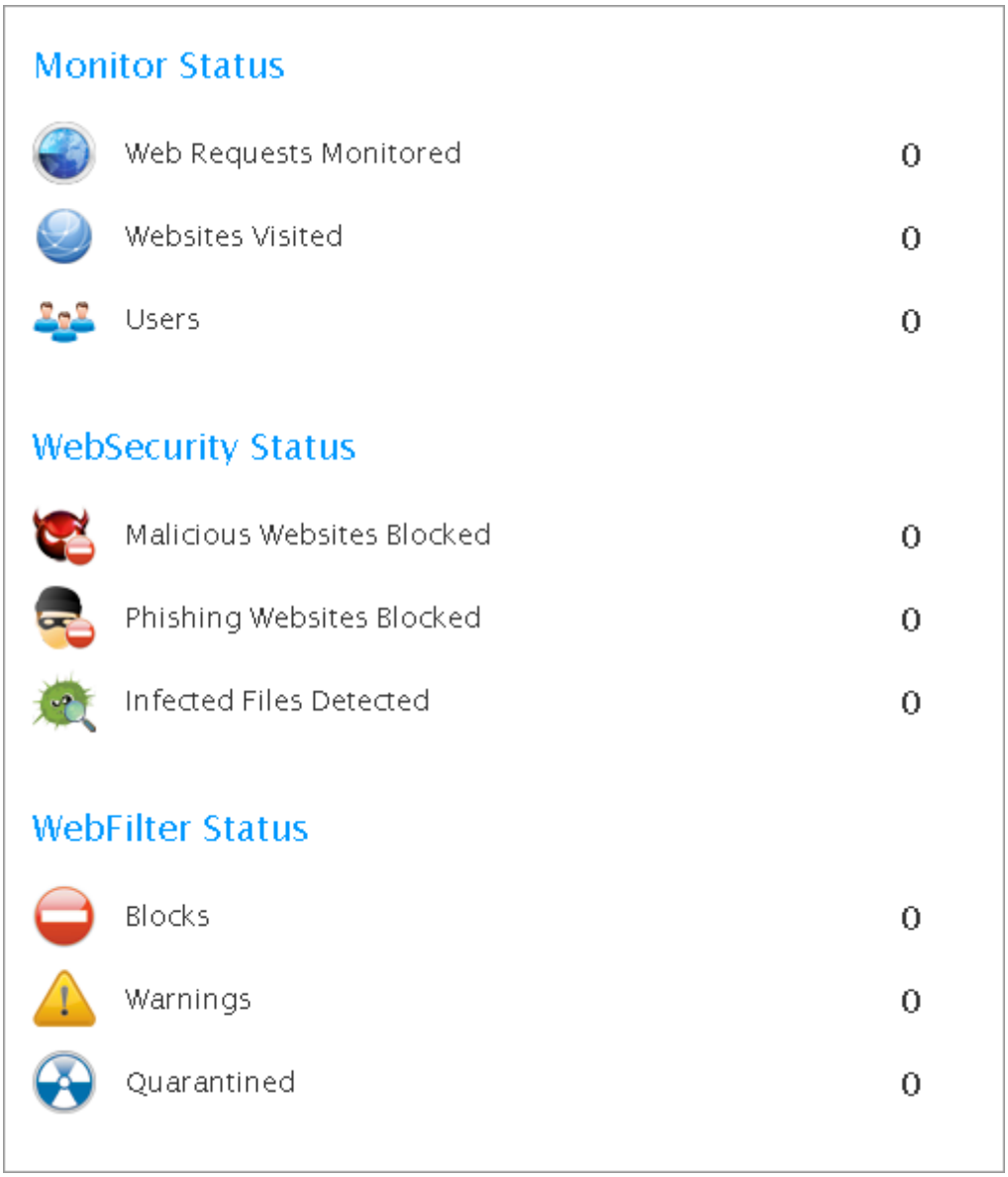
When a task is dismissed, it does not appear again on the dashboard.

5.1.3 Web Monitoring Status

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

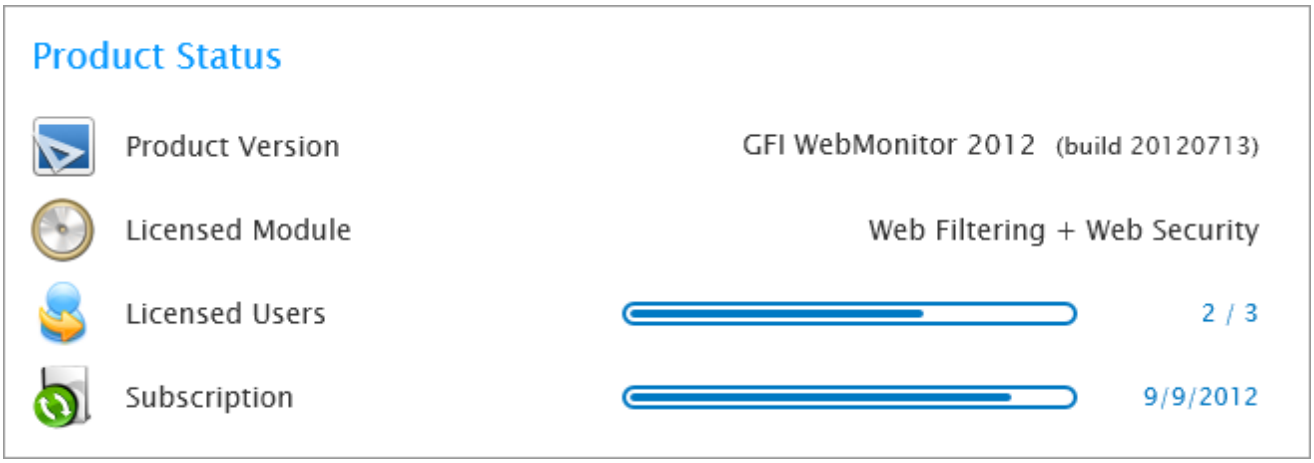
NOTE

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



Screenshot 26: Dashboard Overview statistical information

5.1.4 Product Status



Screenshot 27: Dashboard Overview product status

Use the Product Status area to verify details related to:

Table 8: Product status overview

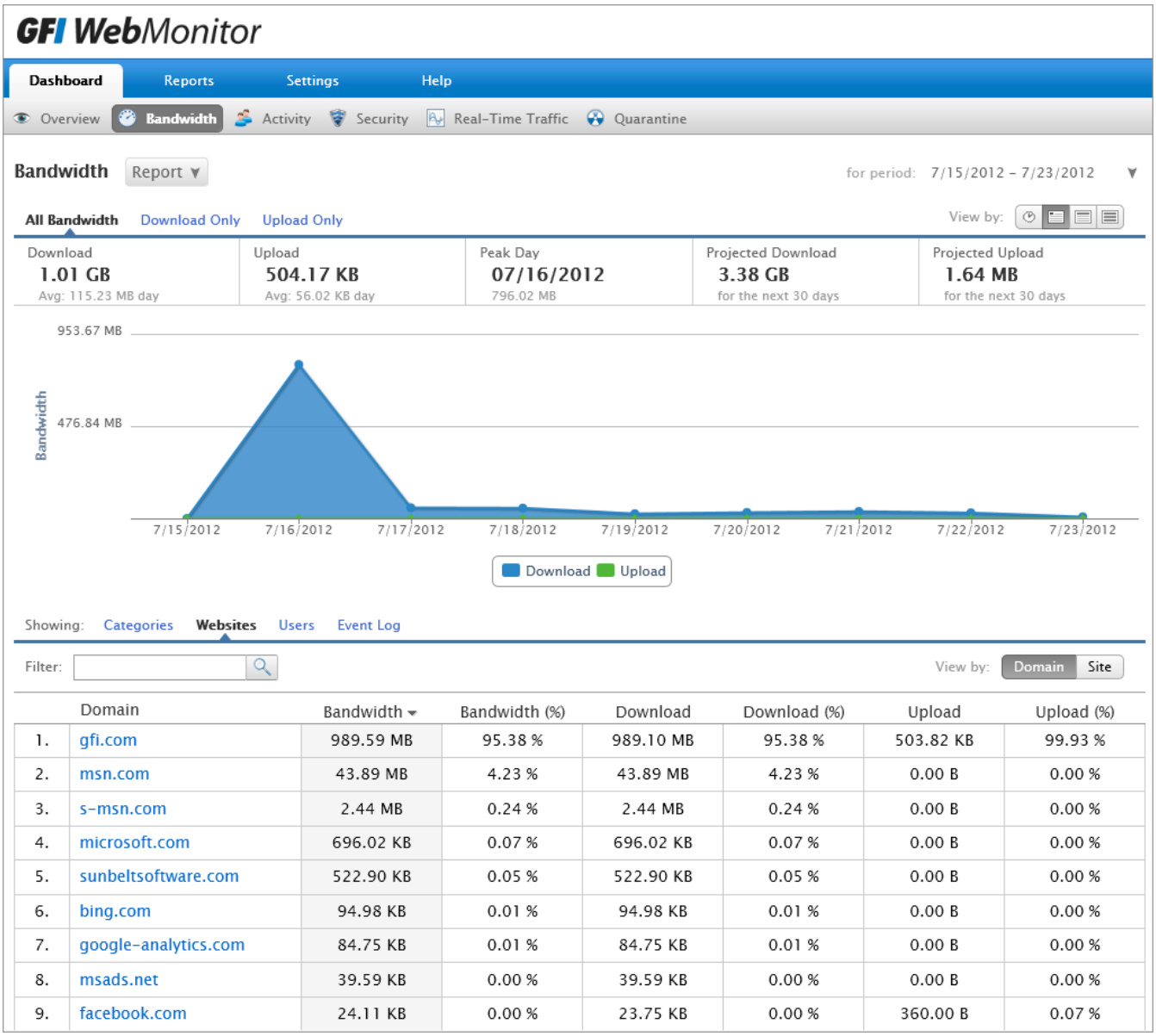
STATUS	DESCRIPTION
Product Version	Displays the current installed version of GFI WebMonitor and the build number.
Licensed Module	Check which modules are licensed and active. For more information, refer to Licensing Information (page 13).
Licensed Users	Shows the number of users being monitored. For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

5.2 Monitoring Bandwidth

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

Table 9: Bandwidth dashboard options

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



	Domain	Bandwidth	Bandwidth (%)	Download	Download (%)	Upload	Upload (%)
1.	gfi.com	989.59 MB	95.38 %	989.10 MB	95.38 %	503.82 KB	99.93 %
2.	msn.com	43.89 MB	4.23 %	43.89 MB	4.23 %	0.00 B	0.00 %
3.	s-msn.com	2.44 MB	0.24 %	2.44 MB	0.24 %	0.00 B	0.00 %
4.	microsoft.com	696.02 KB	0.07 %	696.02 KB	0.07 %	0.00 B	0.00 %
5.	sunbeltsoftware.com	522.90 KB	0.05 %	522.90 KB	0.05 %	0.00 B	0.00 %
6.	bing.com	94.98 KB	0.01 %	94.98 KB	0.01 %	0.00 B	0.00 %
7.	google-analytics.com	84.75 KB	0.01 %	84.75 KB	0.01 %	0.00 B	0.00 %
8.	msads.net	39.59 KB	0.00 %	39.59 KB	0.00 %	0.00 B	0.00 %
9.	facebook.com	24.11 KB	0.00 %	23.75 KB	0.00 %	360.00 B	0.07 %

Screenshot 28: Monitoring bandwidth

NOTE

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

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

Data is broken down as follows:

Table 10: Bandwidth monitoring filtering options

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

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

5.2.1 One-click Report Functionality

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

Export Report

To export the report:

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

Table 11: Export report options

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

Schedule Report

To schedule the report:

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

For more information, refer to Reporting (page 60).

4. Save the report.

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

5.3 Monitoring Activity

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

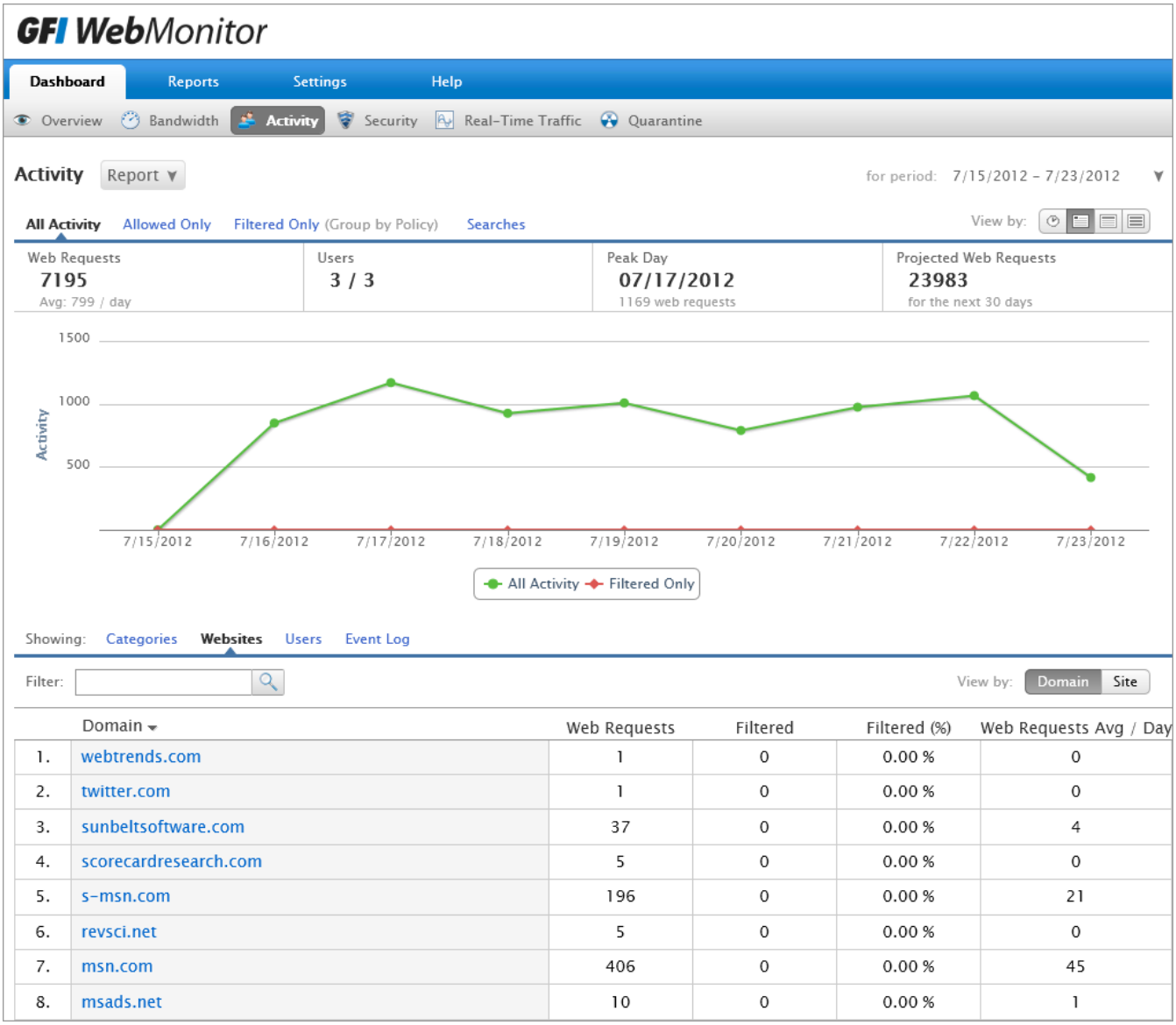
Table 12: Activity dashboard options

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

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

NOTE

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



Screenshot 29: Activity Dashboard

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

Data is broken down as follows:

Table 13: Activity monitoring filtering options

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

5.3.1 One-click Report Functionality

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

Export Report

To export the report:

1. From the top of the Dashboard, click 

and select **Export Report**.
2. GFI WebMonitor displays the exported report in a separate window in your browser.
3. Click  and select one of the following options:

Table 14: Export report options

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

Schedule Report

To schedule the report:

1. From the top of the Dashboard, click 

and select **Schedule Report**.
2. GFI WebMonitor redirects you automatically to the Reports area.

For more information, refer to Reporting (page 60).

4. Save the report.

IMPORTANT

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

5.4 Monitoring Security

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

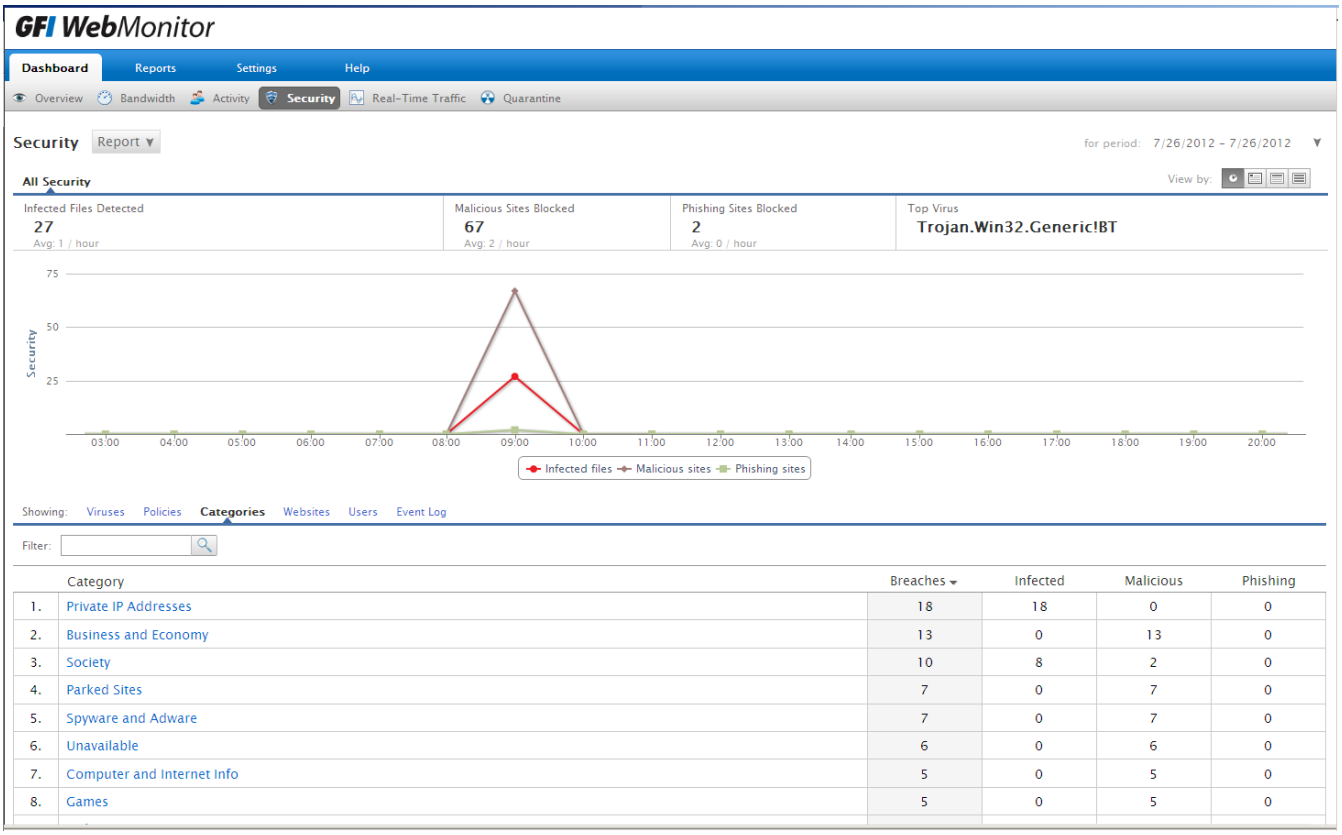
Data is filtered to provide information related to:

Table 15: Security dashboard options

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

NOTE

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



Screenshot 30: Security Dashboard

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

Table 16: Security monitoring filtering options

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

5.4.1 One-click Report Functionality

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

Export Report

To export the report:

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

Table 17: Export report options

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

Schedule Report

To schedule the report:

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

For more information, refer to Reporting (page 60).

4. Save the report.

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

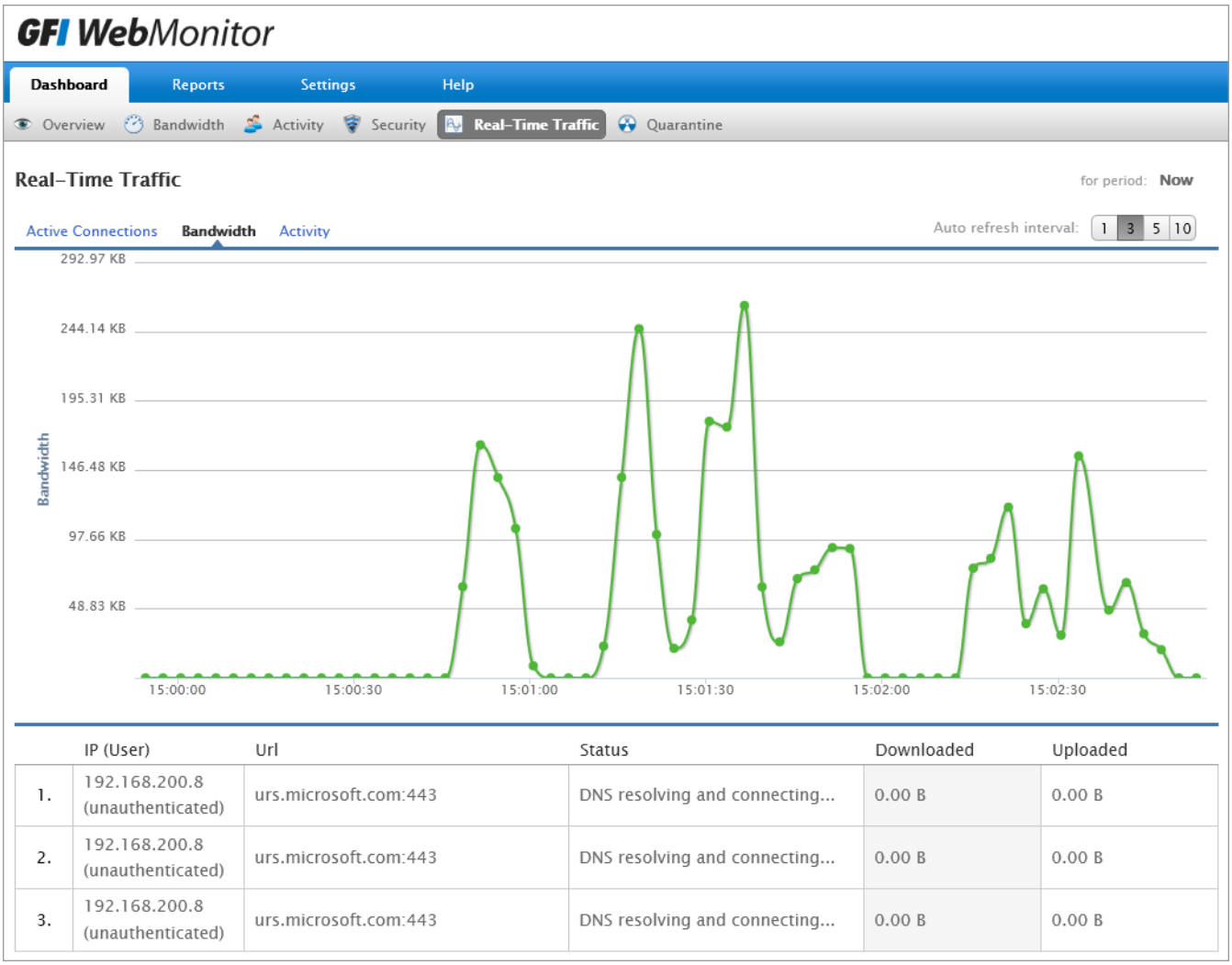
5.5 Monitoring Real-Time Traffic

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

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

To access the Real-Time Traffic dashboard:

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



Screenshot 31: Real-Time Traffic Dashboard, Bandwidth monitoring

2. Click one of the following tabs:

Table 18: Real-Time Traffic dashboard options

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

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

NOTE

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

5.6 Using Quarantine

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

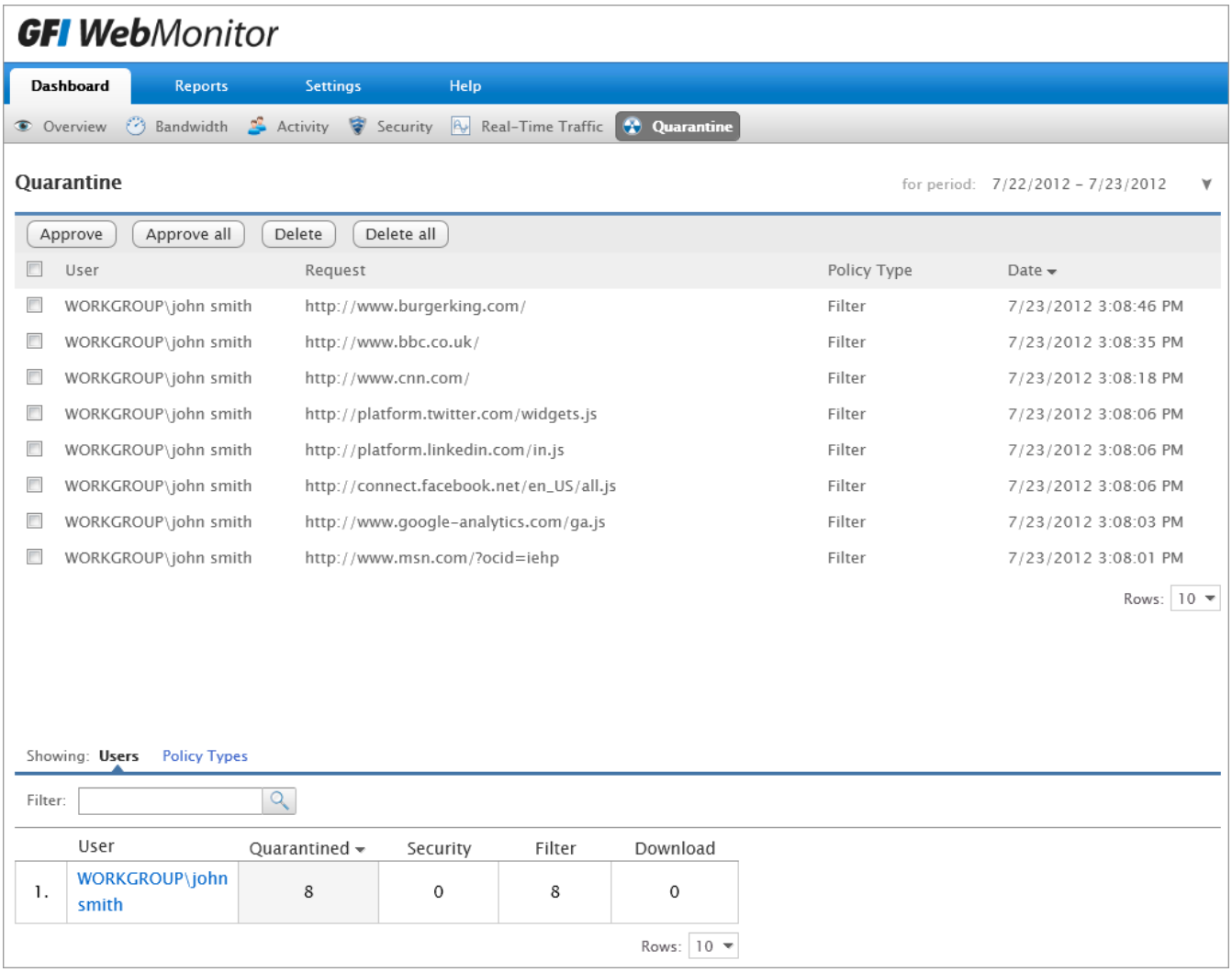
Table 19: Quarantine options

OPTION	DESCRIPTION
Approve	Approve a single item in the list.
Approve All	Approve all items in the list.
Delete	Delete a single item in the list.
Delete All	Delete all items in the list.

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

To approve or delete an item from the Quarantine list:

1. Go to **Dashboard > Quarantine**



Screenshot 32: Quarantine dashboard

2. Locate the item to approve or delete, and select the checkbox next to it.

3. Click **Approve** or **Delete**.

4. From the **Approve Access Requests** window, click **Confirm**.

6 Reporting

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

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

Use the reporting engine to create:

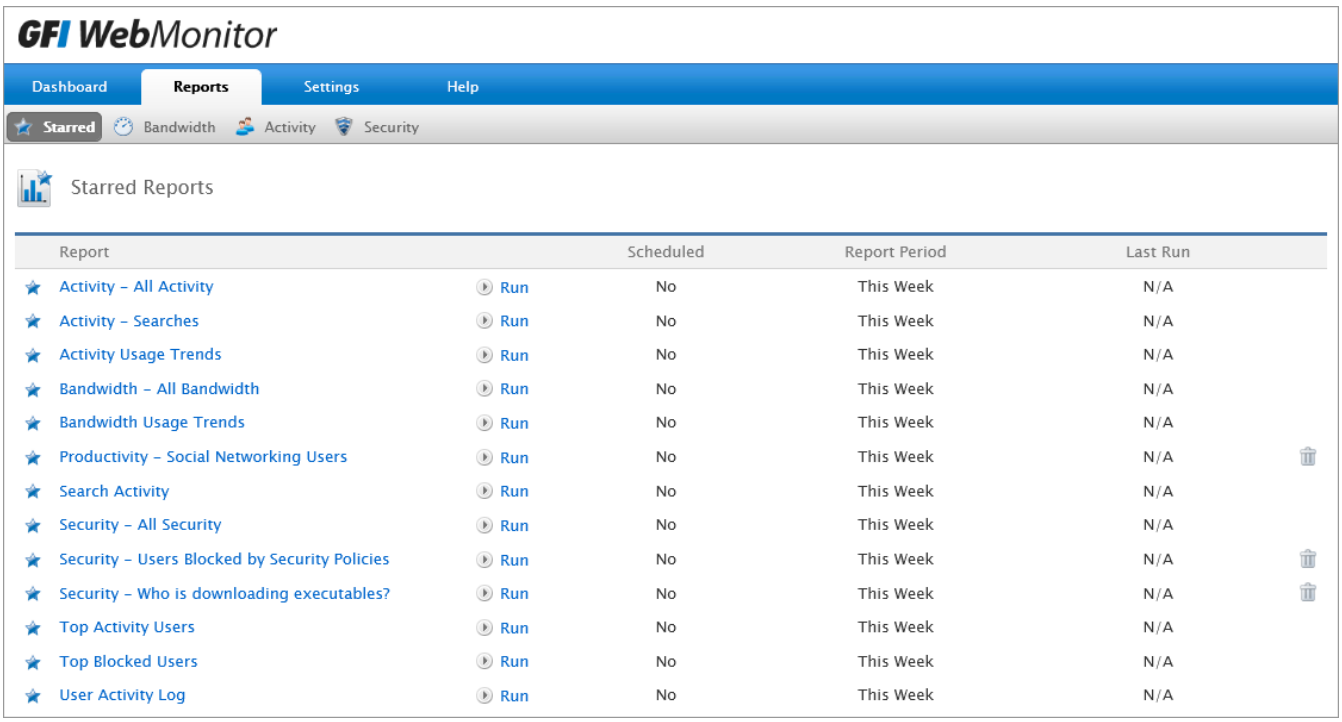
- Department based reporting that can be scheduled and sent to the relevant department heads
- Reports which exclude certain data such as `salesforce.com`, and other websites or data which is irrelevant
- Reports which only include certain categories of websites. For example, generate productivity loss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

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

- Activity Reports
- Bandwidth Reports
- Security Reports

6.1 Starred Reports

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



To add a report to the Starred Reports list:

1. Go to **Reports** > **Bandwidth** or **Activity** tab.

2. Click ☆ next to report name.

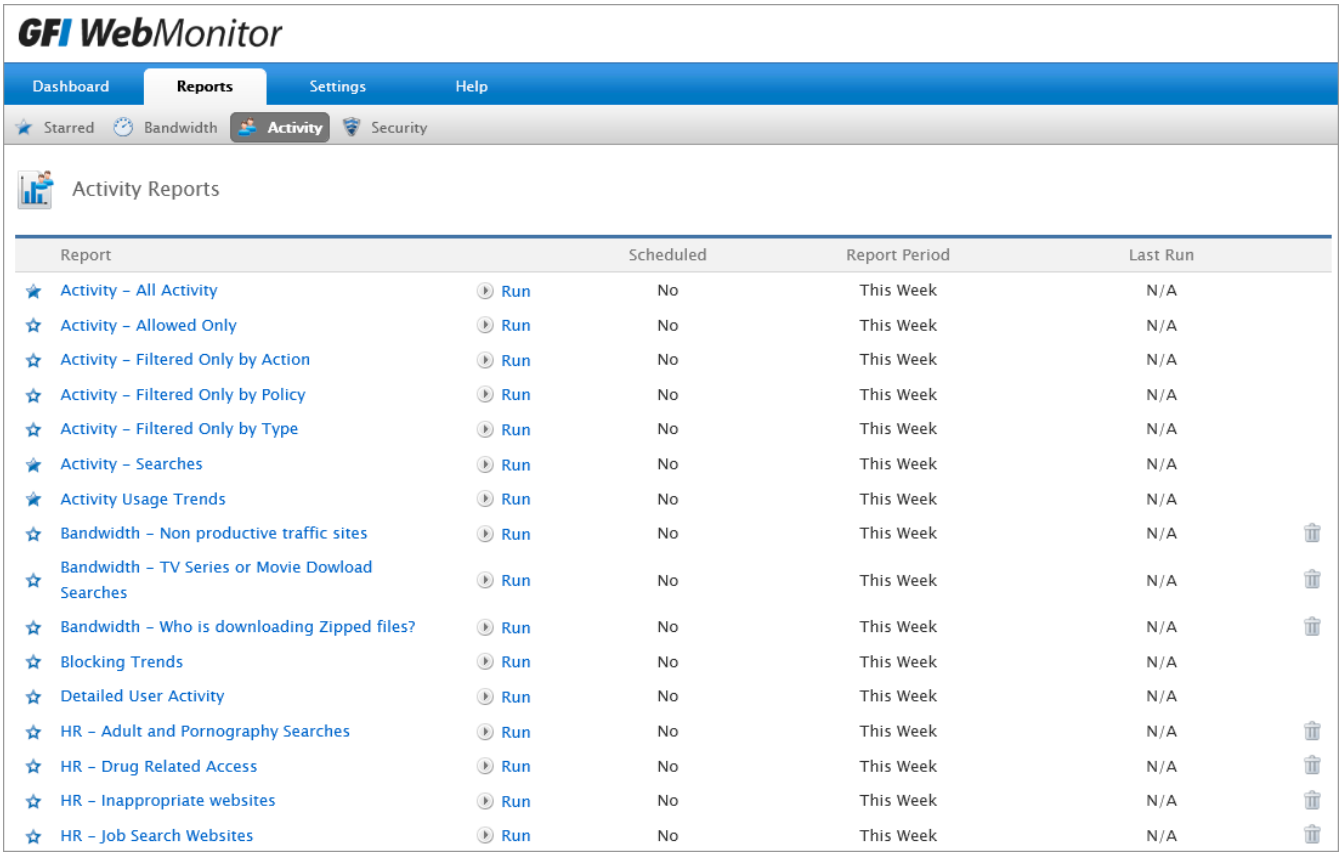
3. Starred reports will be marked with ★.

6.2 Activity Reports

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

To use one of the above reports:

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



Screenshot 33: Default activity report list

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

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

See also:

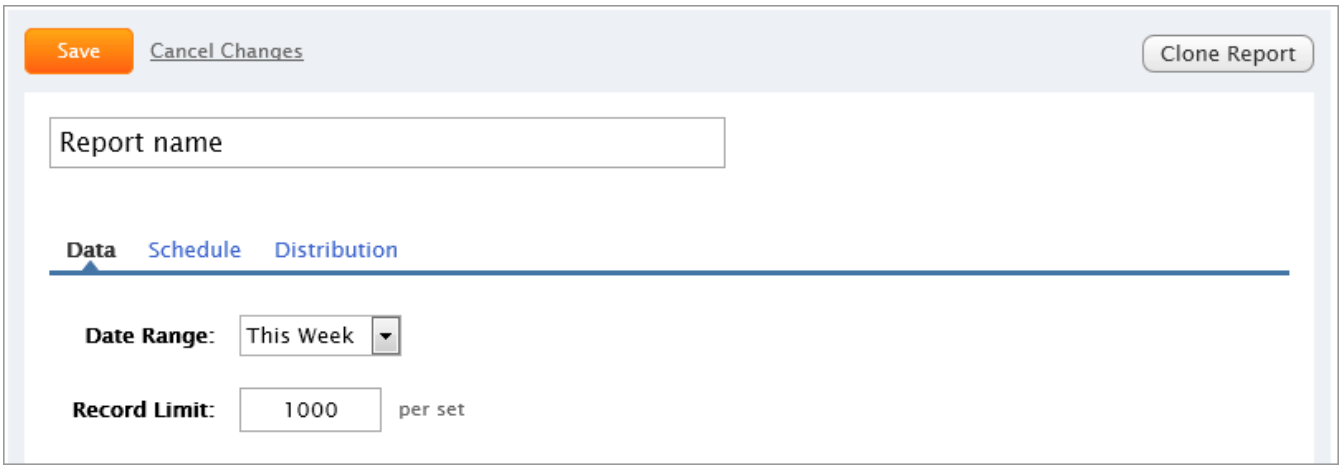
Cloning a report

Editing Activity Report

6.2.1 Editing Activity Reports

To edit an activity report:

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



Screenshot 34: Editing a report

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

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

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

6. In the **Include** area:

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

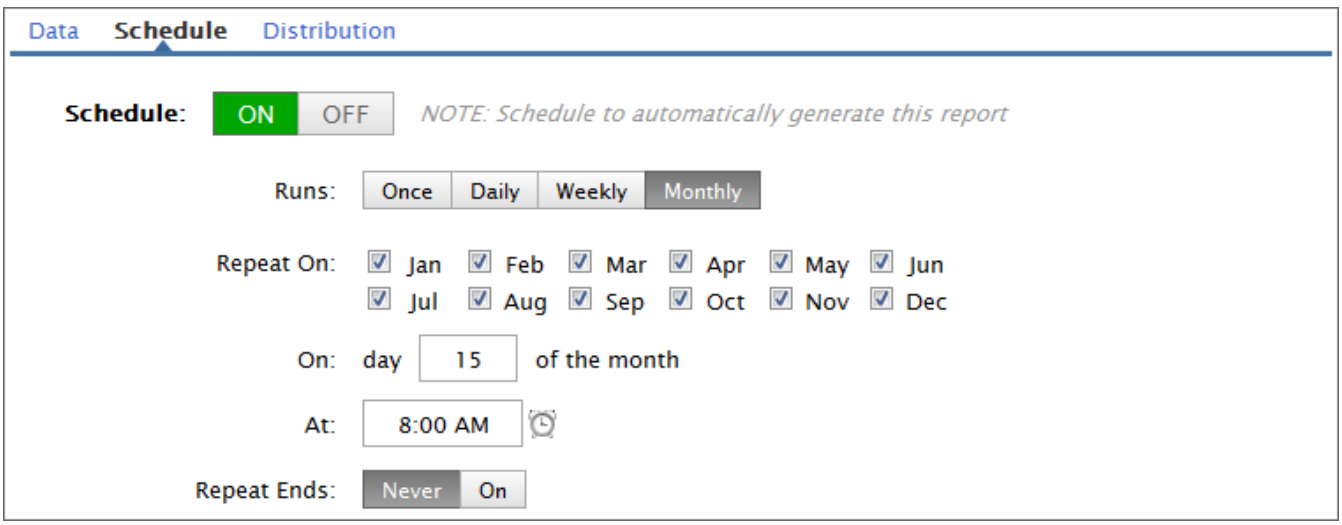
   b. Click **Categories** tab to add the categories to include or exclude in the report

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

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

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

> **NOTE**
>
> If the schedule is disabled, report is not automatically generated.



Screenshot 35: Scheduling an activity report

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

Table 20: Activity report schedule options

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

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

Table 21: Activity report distribution options

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

10. Click **Save**.

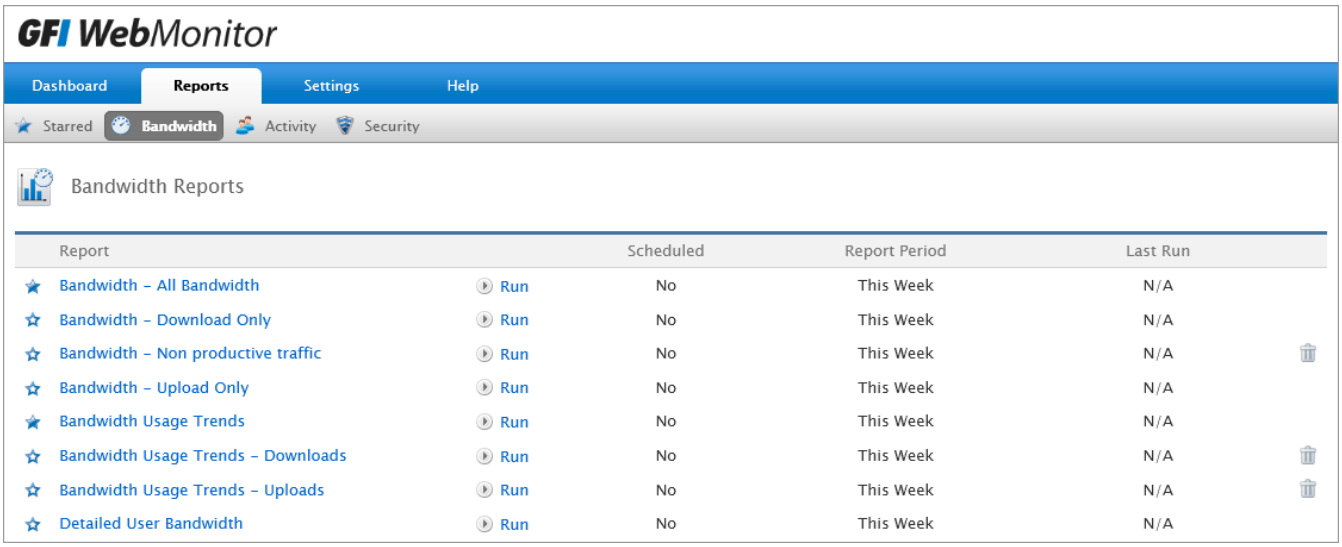
11. To generate the report, click **Run**.

6.3 Bandwidth Reports

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

To use one of the above reports:

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



Screenshot 36: Default bandwidth reports list

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

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

See also:

Cloning a report

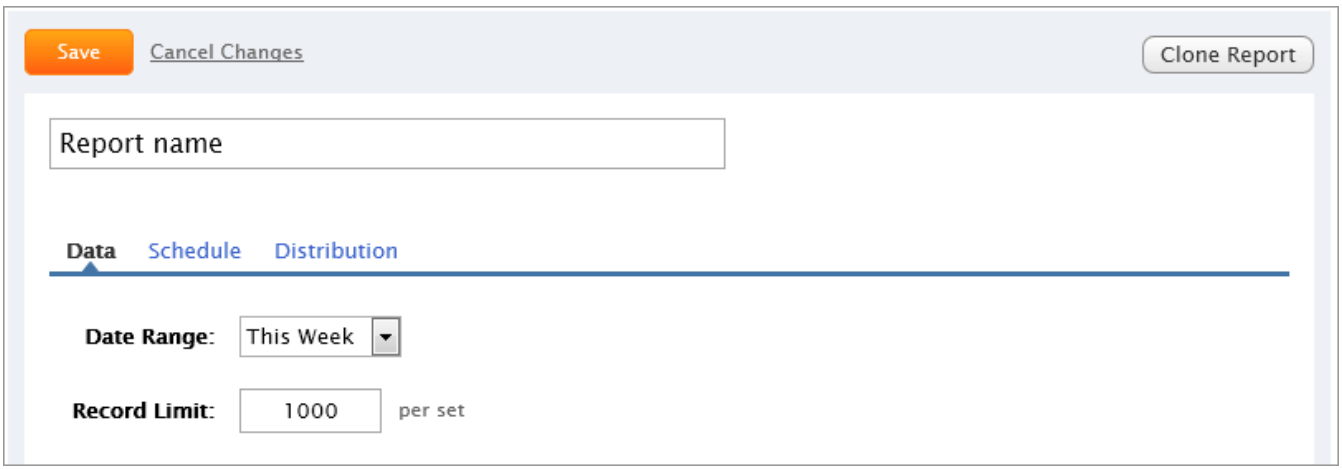
Editing Bandwidth Report

6.3.1 Editing Bandwidth Reports

To edit an bandwidth report:

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

2. Click report name to edit.



Screenshot 37: Editing a report

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

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

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

6. In the **Include** area:

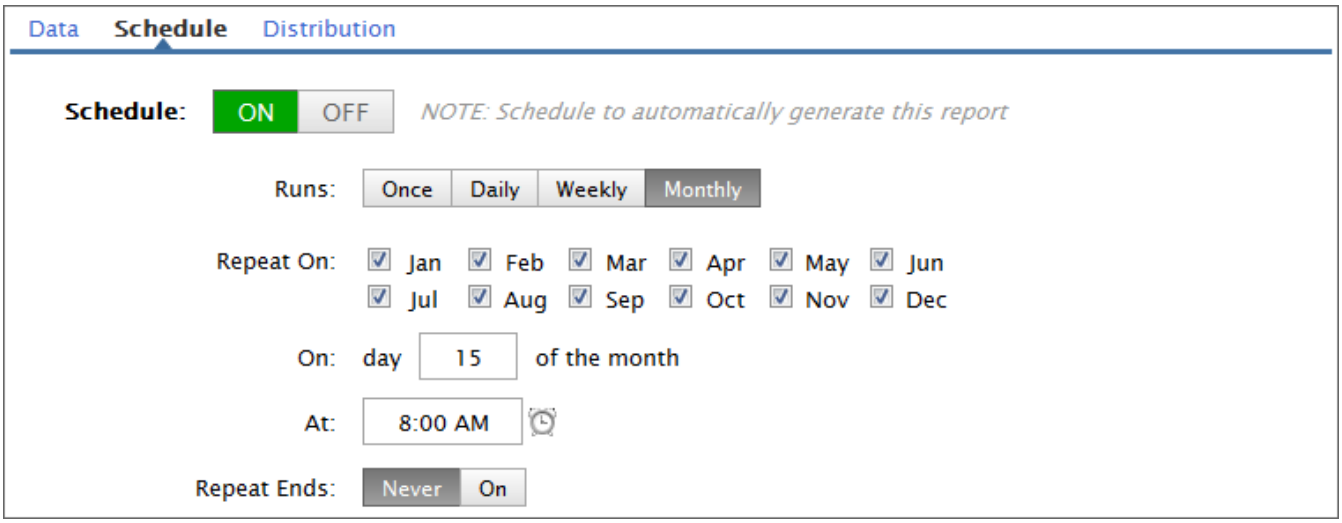
   a. Click **Users / Groups** tab and add the users or groups to include or exclude in the report.

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

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

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

> **NOTE**
>
> If the schedule is disabled, report is not automatically generated.



Screenshot 38: Scheduling an activity report

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

Table 22: Activity report schedule options

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

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

Table 23: Activity report distribution options

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

10. Click **Save**.

11. To generate the report, click **Run**.

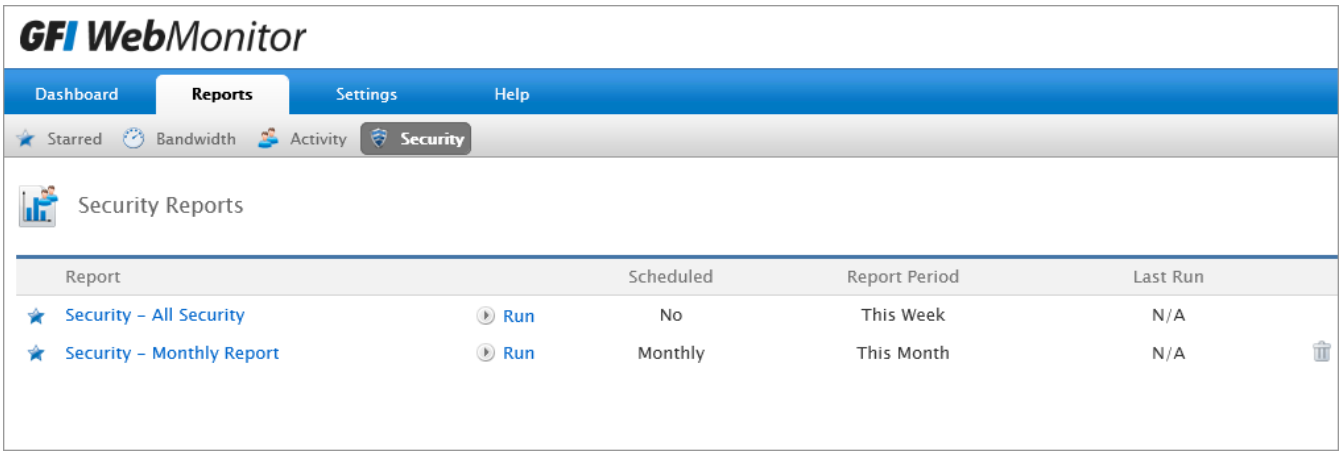
6.4 Security Reports

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

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

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

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



Screenshot 39: Default Security reports list

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

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

See also:

Cloning a report

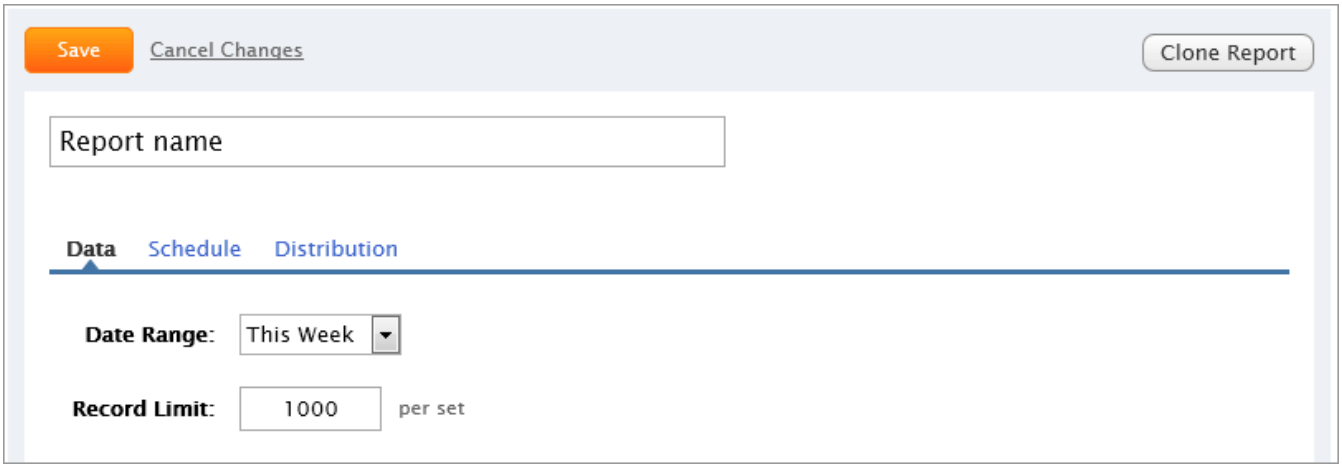
Editing Security Report

6.4.1 Editing Security Reports

To edit a Security report:

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

2. Click report name to edit.



Screenshot 40: Editing a report

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

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

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

6. In the **Include** area:

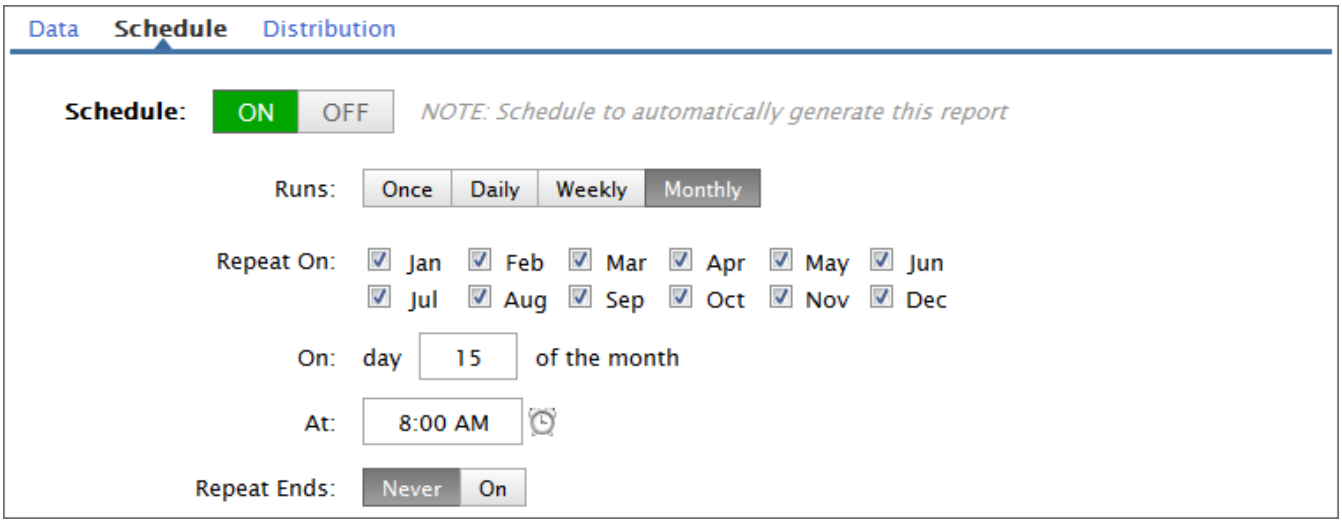
   a. Click **Users / Groups** tab and add the users or groups to include or exclude in the report.

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

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

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

> **NOTE**
>
> If the schedule is disabled, report is not automatically generated.



Screenshot 41: Scheduling an activity report

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

Table 24: Activity report schedule options

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

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

Table 25: Activity report distribution options

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

10. Click **Save**.

11. To generate the report, click **Run**.

6.4.2 Cloning Reports

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

To clone a report:

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

7 Configuring GFI WebMonitor

This chapter assists in the configuration of the following:

General settings

1. Licensing

2. Remote Access Control

3. Data Retention, Notification language and Anonymization

4. Auto-update of internal scanning engines

5. Web Categorization

6. Database settings

Policies

1. Security policies

2. Internet policies

3. Download control policies

4. Always Blocked list, Always Allowed list and Temporary Allowed configuration

Alerts

1. Monitoring, Bandwidth and Security alerts

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

7.1 General Settings

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

Table 26: General Settings

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

7.1.1 Updating License Manually

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

To update product license key:

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

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

See Also:

Licensing Information.

Post-Installation Actions.

7.1.2 Remote Access Control

The **Remote Access Control** node enables you to:

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

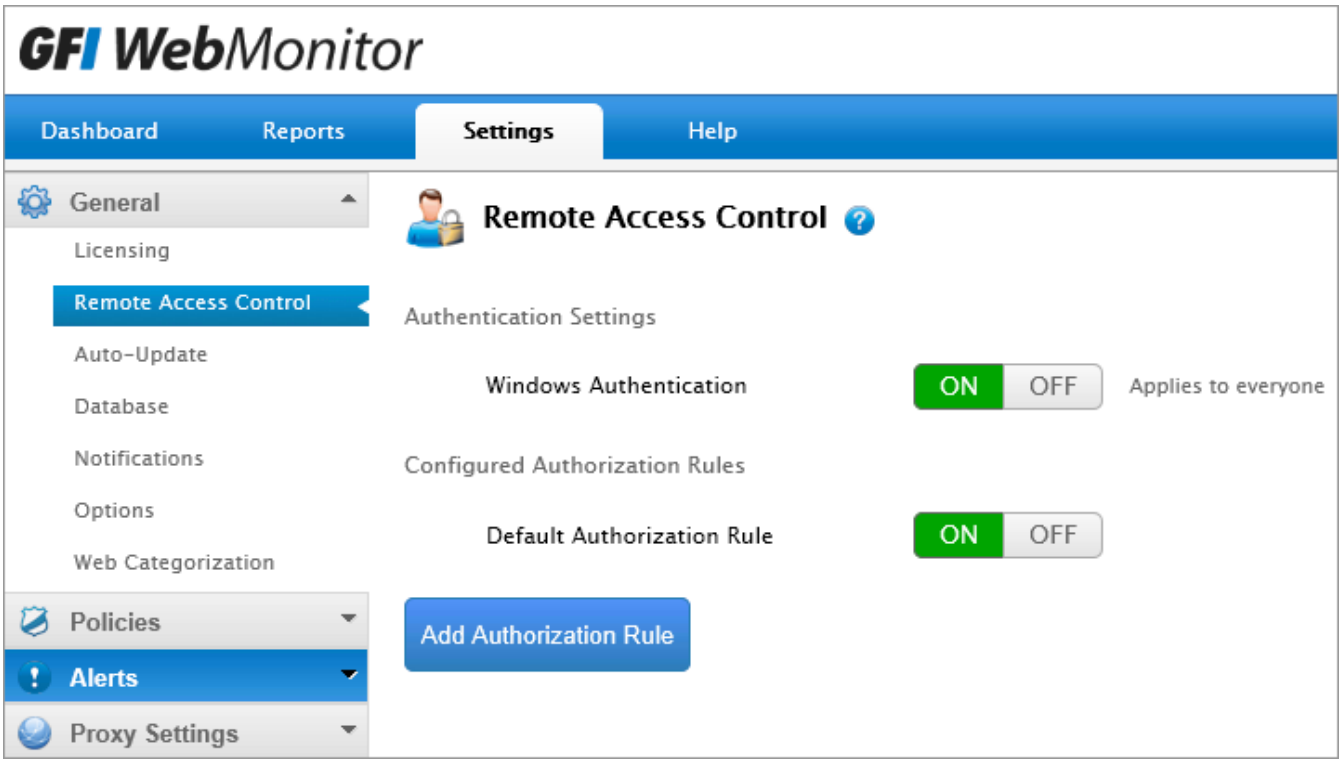
Configuring Windows Authentication

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

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

To turn **Windows Authentication** on or off:

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



Screenshot 42: Configuring Access Control

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

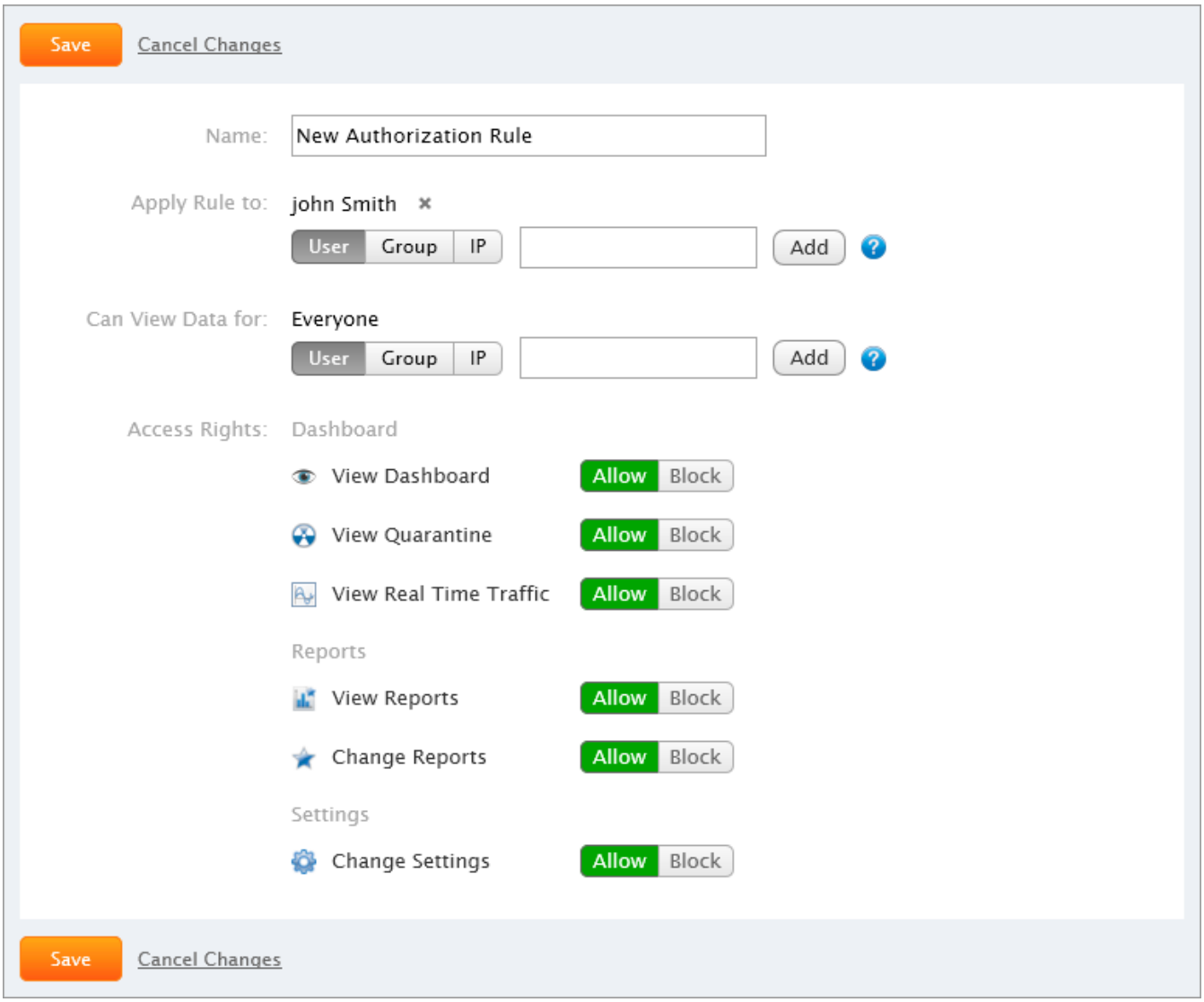
Add a New Authorization Rule

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

To add a new Authorization Rule:

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

2. Click **Add Authorization Rule**.



Screenshot 43: Adding a new Authorization Rule

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

IMPORTANT

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

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

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

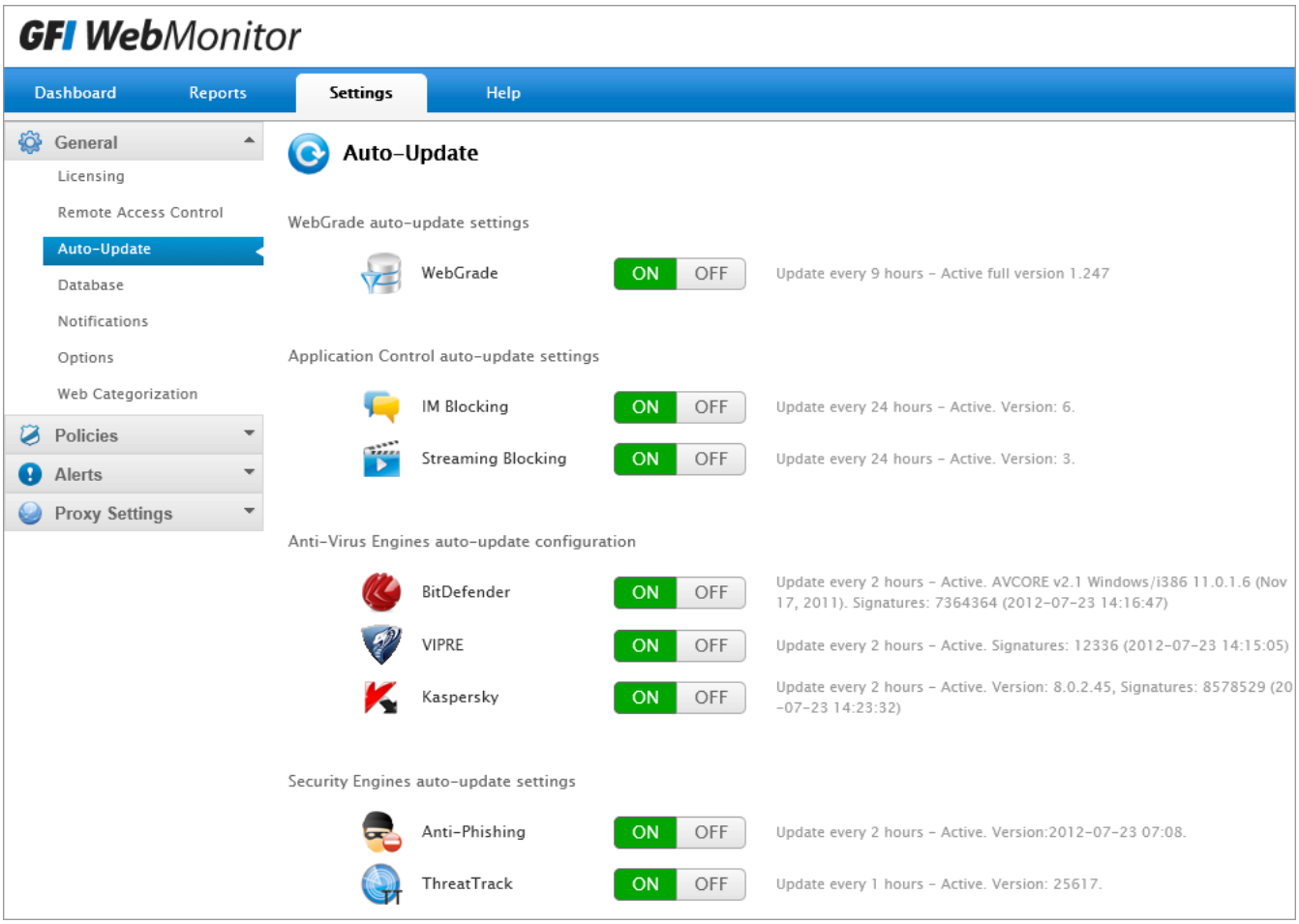
OPTION	DESCRIPTION
View Dashboard	When enabled, user can view Bandwidth, Activity and Security Dashboard. Access to Quarantine and Real Time Traffic dashboards can be granted or denied using additional controls.

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

6. Click **Save**.

7.1.3 Configuring Auto-Update

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



Screenshot 44: Configuring Auto-update

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

1. Go to **Settings > General > Auto-Update**.

2. Click **ON** or **OFF** to enable or disable the components as required.

NOTE

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

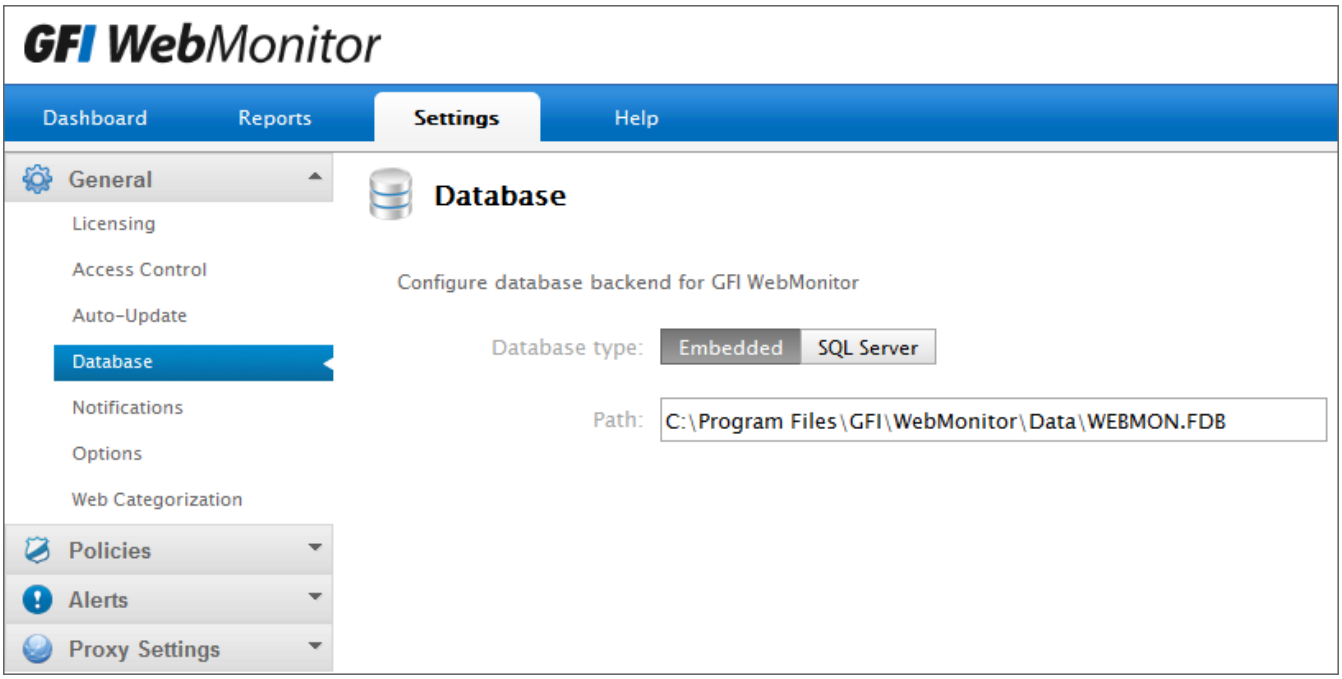
7.1.4 Configuring Databases

GFI WebMonitor supports two types of databases:

Table 27: Back-end databases

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

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



Screenshot 45: Configured database

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

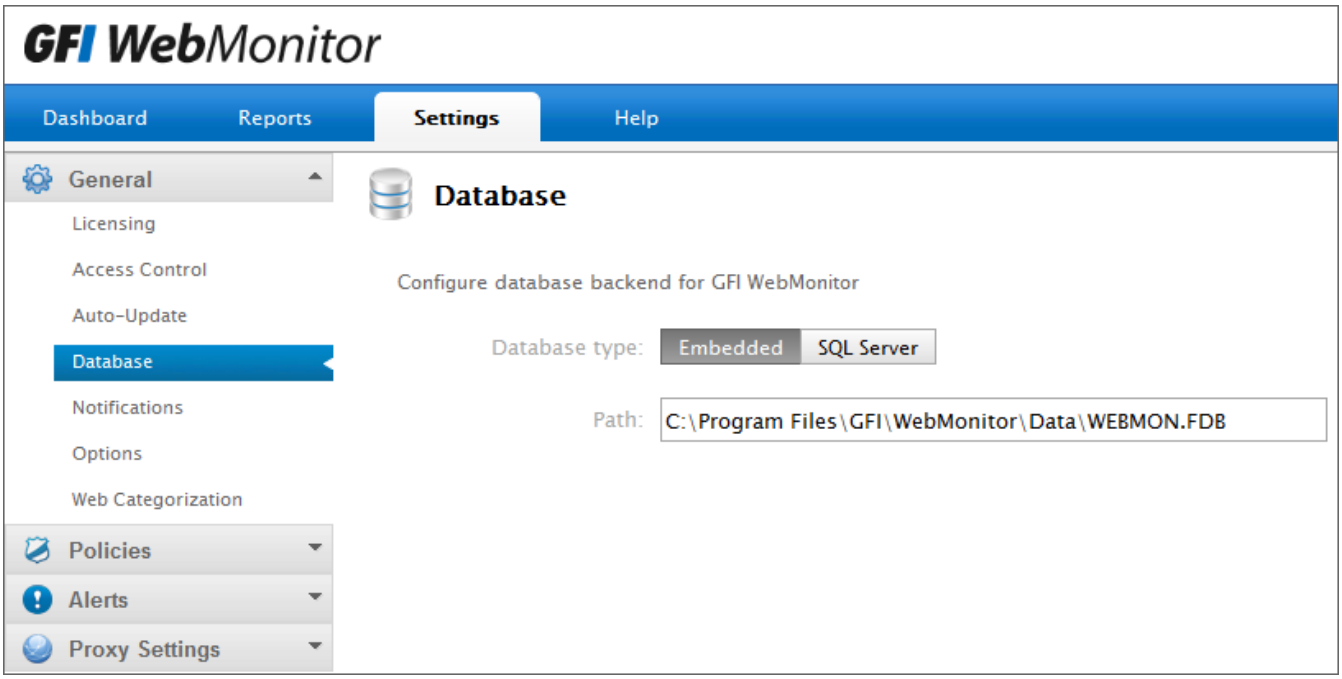
- Configuring Firebird Database
- Configuring Microsoft SQL Database

Configuring Firebird Database

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

To change the default location of the Firebird database:

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



Screenshot 46: Configuring Databases

4. From **Database Type**, select **Embedded**.

5. In the **Path** field, change the path to the point to the new location.

6. Click **Save**.

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

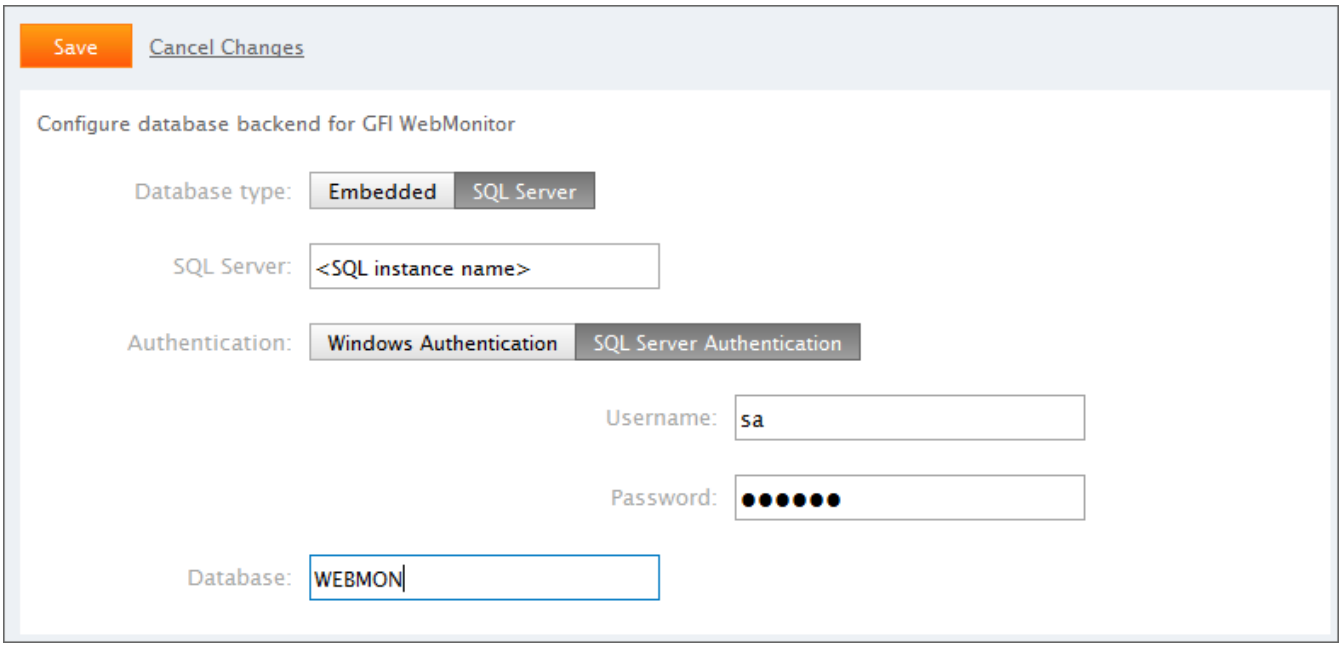
Configuring Microsoft® SQL Database

GFI WebMonitor supports both Microsoft® SQL Server Express and Microsoft® SQL Server databases.

To point GFI WebMonitor to use a previously created Microsoft® SQL Server database:

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

2. From **Database Type**, select **SQL Server**.



3. In the **SQL Server** field, type the SQL Server® instance name.

4. In the **Authentication** area, select one of the following:

Table 28: SQL Server® Authentication method

OPTION	DESCRIPTION
Windows Authentication	Select this option to use Windows® credentials when connecting to your SQL Server®.
SQL Server Authentication	If your SQL Server® has been installed in SQL Server Authentication Mode, select this option and provide **Username** and **Password**.

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

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

6. Click **Save**.

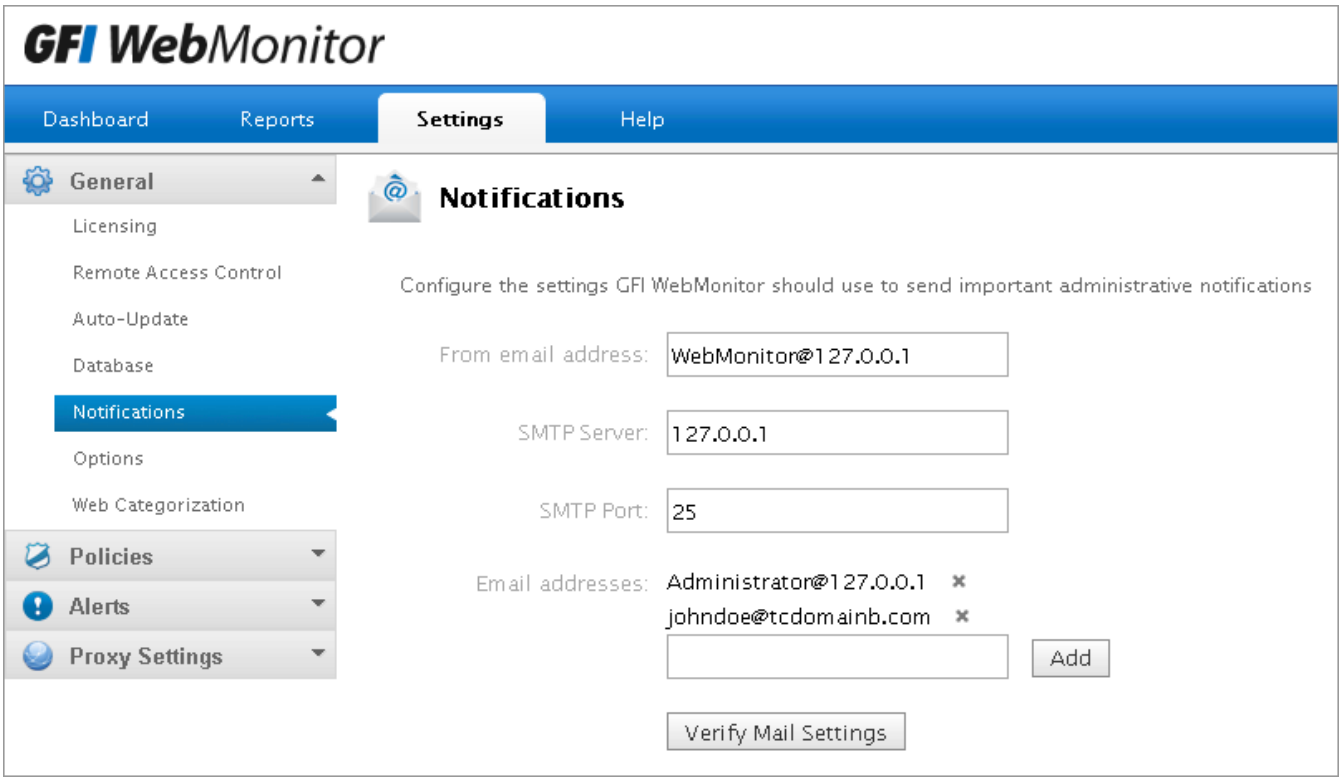
> **NOTE**
>
> You can create a new database from within GFI WebMonitor. To create a new database, enter a new database name and click **Save**.

7.1.5 Configuring Notifications

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

To change the administrative notifications setup configured during installation:

1. Go to **Settings > General > Notifications**.



Screenshot 47: Configuring administrative notifications

2. Change any of the following options:

Table 29: Configuring administrative notifications

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

3. Click **Save**.

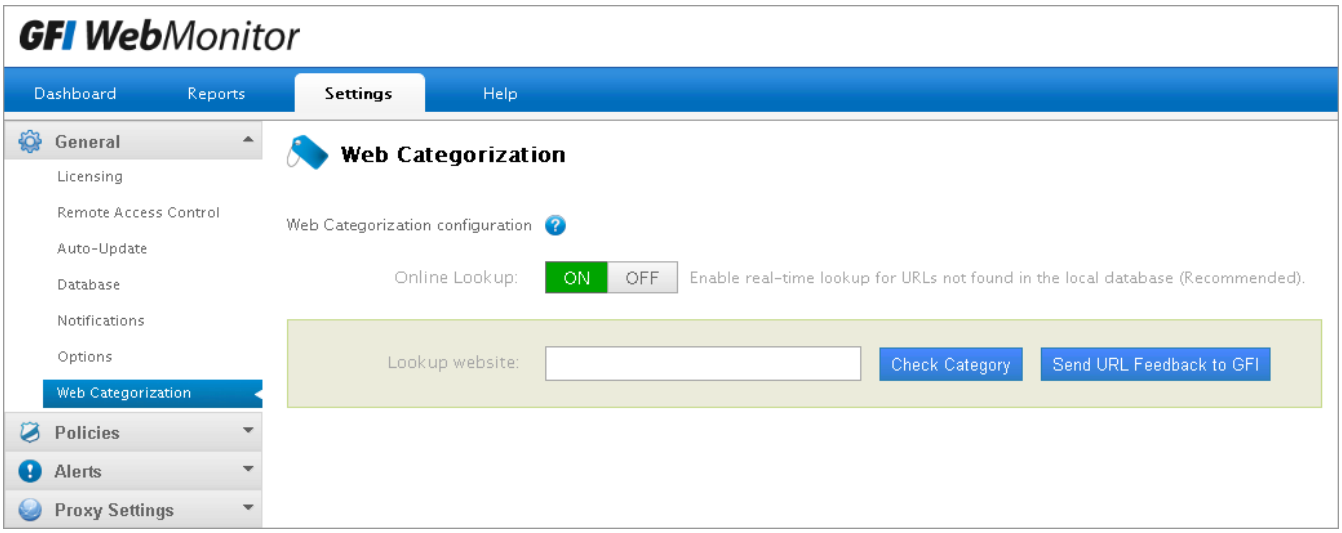
7.1.6 Configuring Web Categorization

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

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

NOTE

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



Screenshot 48: Configuring Web Categorization

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

To look up a URL:

1. Enter a URL in the **Lookup website** field.

2. Click **Check Category**.

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

7.2 Configuring Policies

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

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

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

1. Configuring Internet Policies

2. Configuring Always Blocked list

3. Configuring Always Allowed list

4. Configuring Temporary Allowed list

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

1. Configuring Security Policies

2. Configuring Download Policies

7.2.1 WebFilter Edition Policies

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

The following sections help you:

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

Enabling or Disabling a Configured Policy

To enable or disable a policy:

1. Go to **Settings > Policies > Internet Policies**.

2. Click **ON** to enable or **OFF** to disable the desired policy.

Deleting a Policy

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

7.2.2 Configuring Internet Policies

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

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

Web Filtering Policy

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

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

NOTE

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

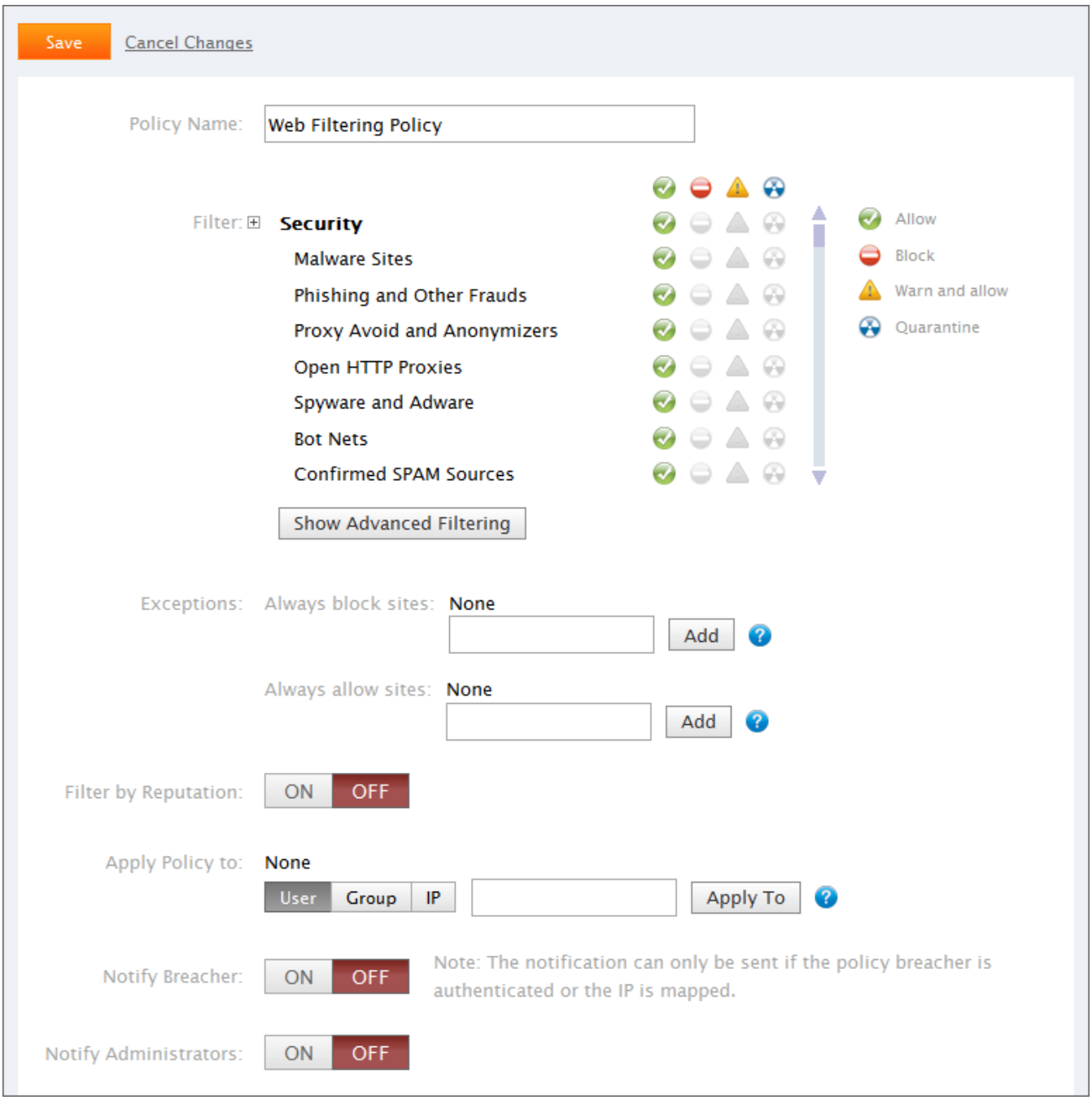
IMPORTANT

All added policies take priority over the default policy.

To add a Web Filtering Policy:

1. Go to **Settings > Policies > Internet Policies**.

2. In the **Web Filtering Policies** area, click **Add Policy**.



Screenshot 49: Creating a new Web Filtering policy

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

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

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

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

Screenshot 50: Enabling reputation filtering

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

Table 30: Reputation index classification

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

NOTE

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

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

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

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

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

12. Click **Save**.

See also:

Cloning a Policy

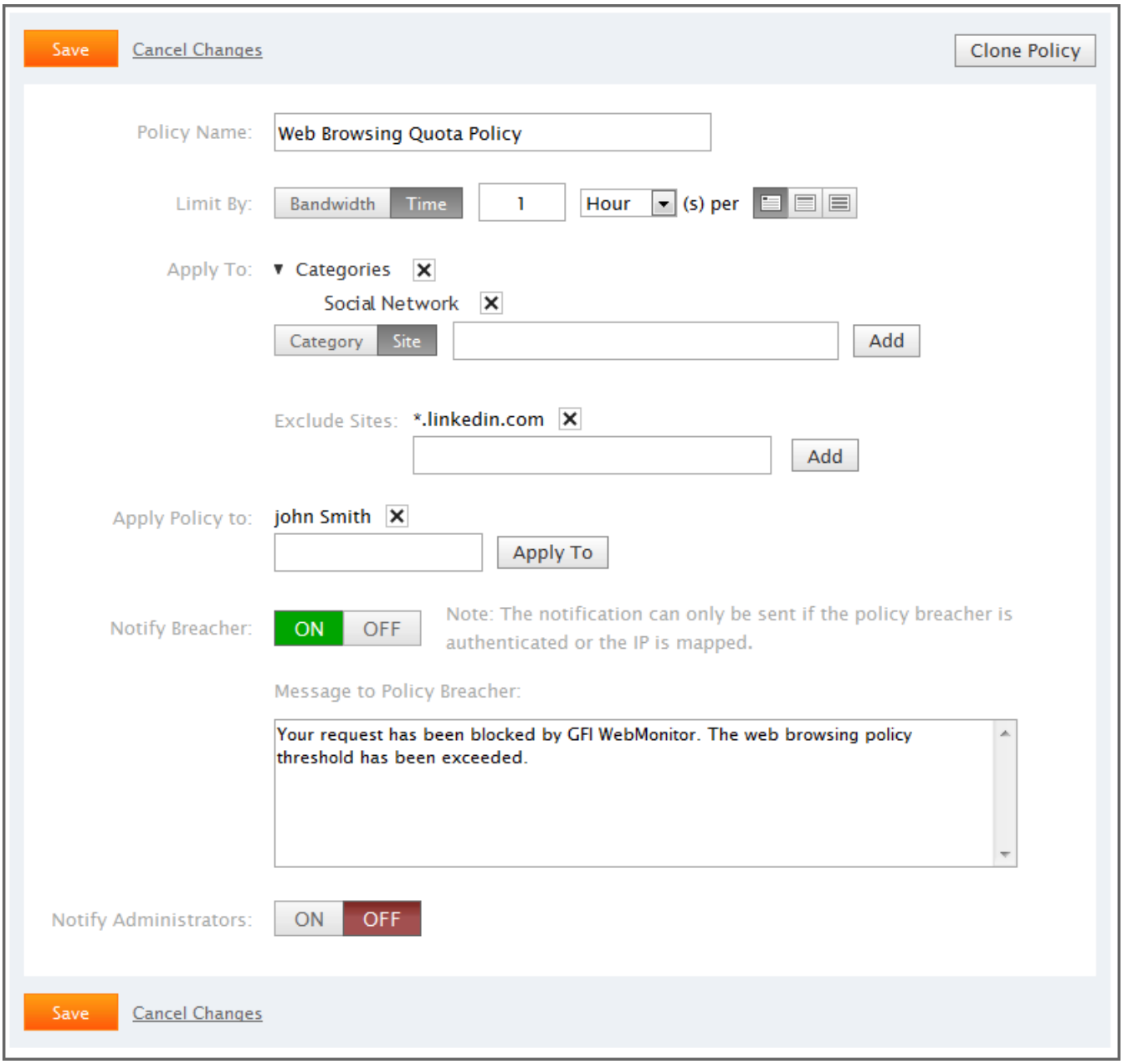
Web Browsing Quota Policy

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

To create a new Web Browsing Quota Policy:

1. Go to **Settings > Policies > Internet Policies**.

2. In the **Web Browsing Quota Policy** area, click **Add Policy**.



Screenshot 51: Creating a new Web Browsing Quota Policy

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

4. In the **Limit By** area specify:

   a. If the threshold will be based on **Bandwidth** or **Time**

   b. The duration in hours or minutes

   c. If the duration is per day, week or month

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

   a. Select which categories or sites are effected by policy.

   b. Add sites which are to be excluded from policy.

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

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

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

9. Click **Save**.

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

See also:

Cloning a Policy

Instant Messaging and Social Control Policy

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

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

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

Social Controls, grant or deny access to the following:

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

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

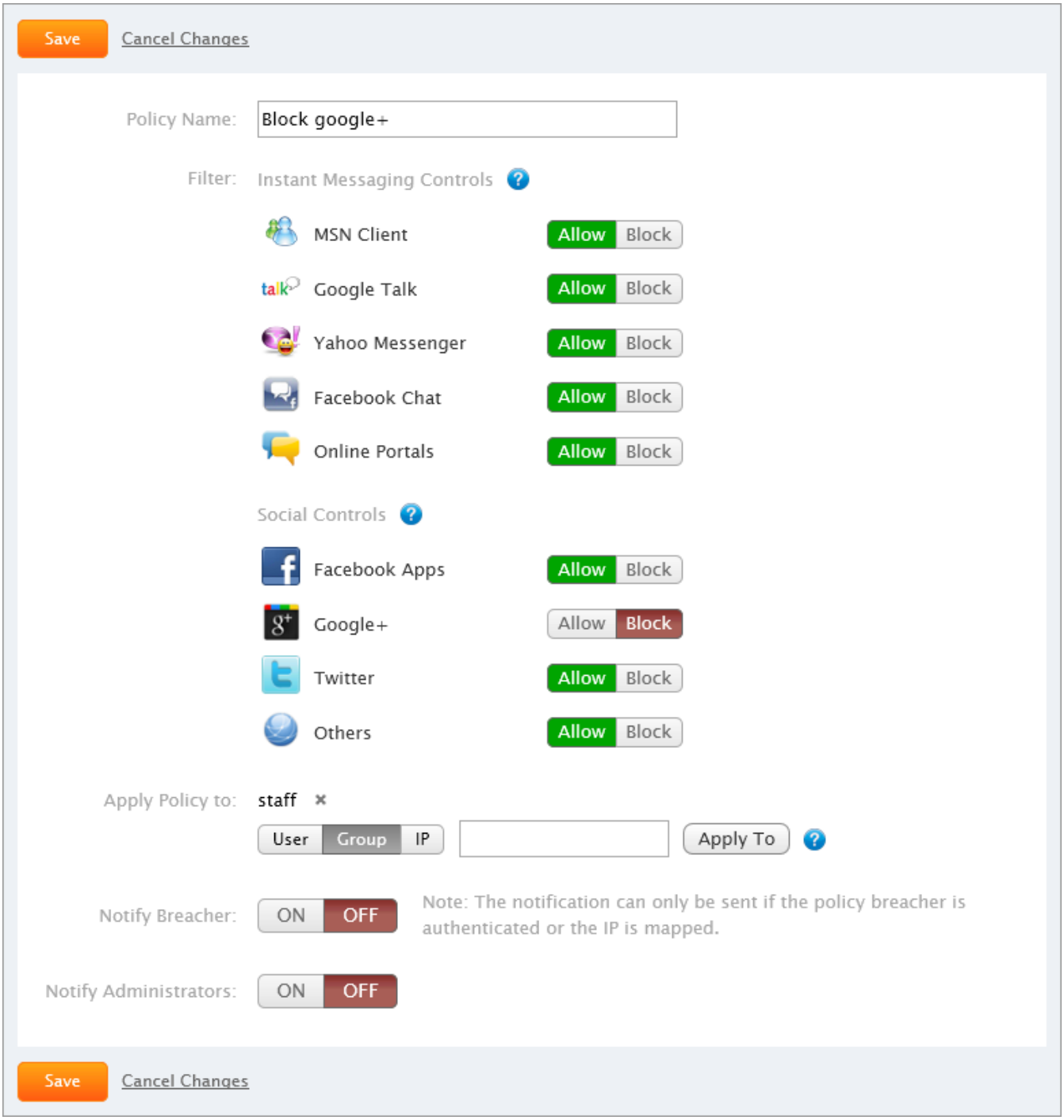
> **NOTE**
>
> Certain fields in the default policy cannot be edited. These include **Policy Name** and **Apply Policy To**.

IMPORTANT

All added policies take priority over the default policy.

To create a new IM Policy:

1. Go to **Settings > Policies > Internet Policies**.
2. In the **Instant Messaging / Social Control Policies** area, click **Add Policy**.



Screenshot 52: Creating a new IM Policy

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

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

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

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

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

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

8. Click **Save**.

See also:

Cloning a Policy

Streaming Media Policy

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

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

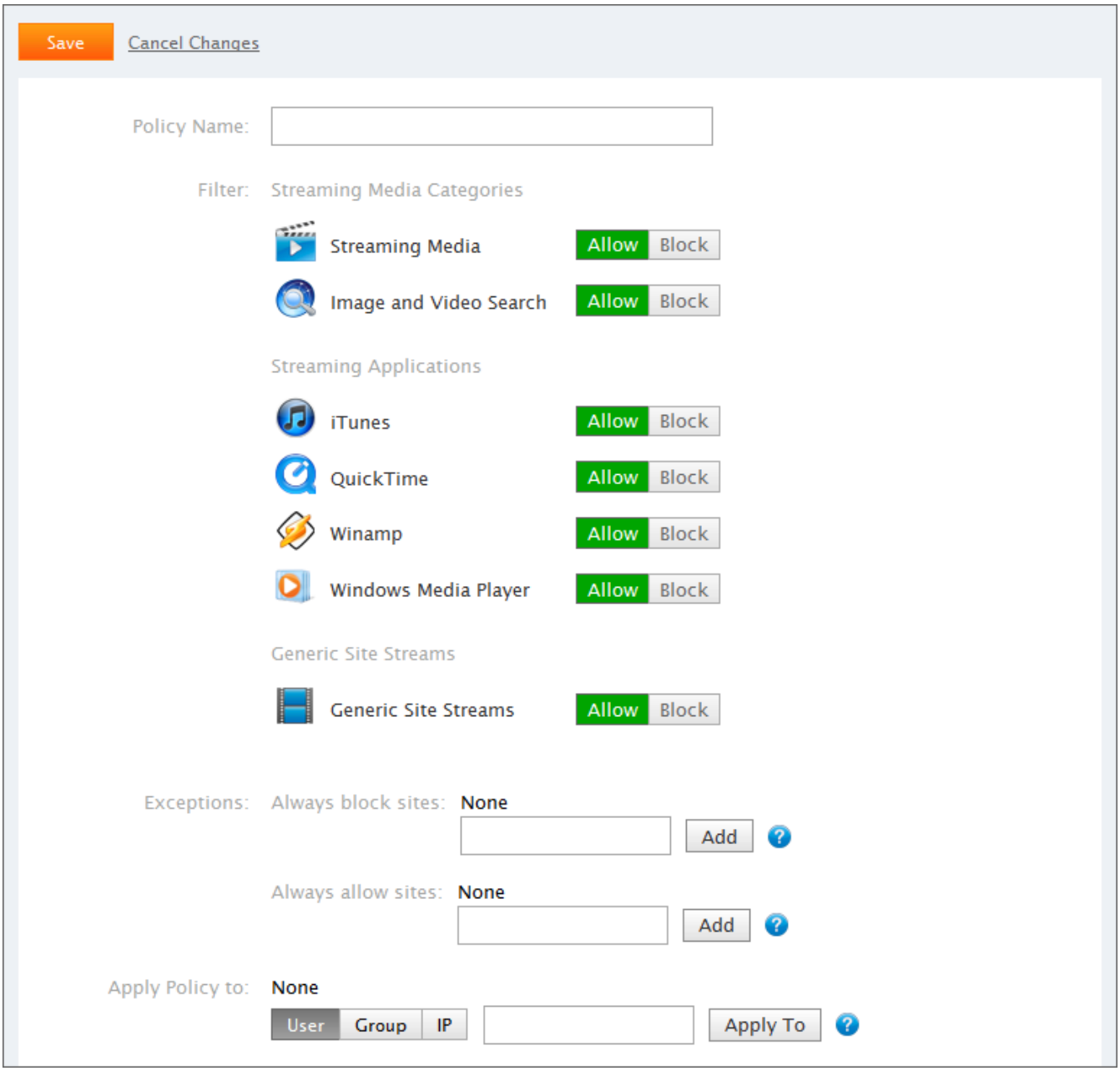
> **NOTE**
>
> Certain fields in the default policy cannot be edited. These include **Policy Name** and **Apply Policy To**.

> **IMPORTANT**
>
> **All added policies take priority over the default policy.**

To add a Streaming Media Policy:

1. Go to **Settings > Policies > Internet Policies**.

2. In the **Streaming Media Policies** area, click **Add Policy**.



Screenshot 53: Configuring Streaming Media policy 1

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

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

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

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

NOTE

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

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

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

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

10. Click **Save**.

See also:

Cloning a Policy

Search Engine Policies

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

Safe Search

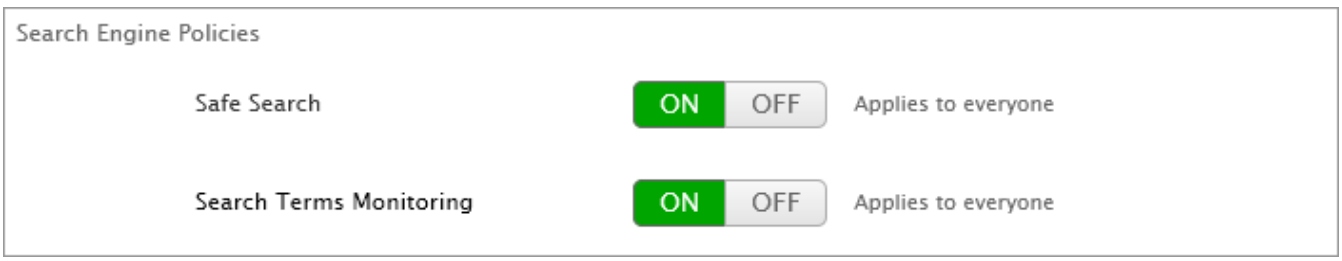
Safe Search is a feature supported by a number of search engines. If enabled, GFI WebMonitor enforces filtering of explicit email and images from user searches.

Safe Search is compatible with the following search engines:

- Google
- Yahoo
- Lycos
- Bing.

NOTE

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



Screenshot 54: Safe Search and Search Terms Monitoring

To enable Safe Search

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

2. Click **ON**.

Search Terms Monitoring

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

To enable Search Terms Monitoring

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

To exclude users or IP addresses from monitoring:

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

7.2.3 Configuring Always Blocked List

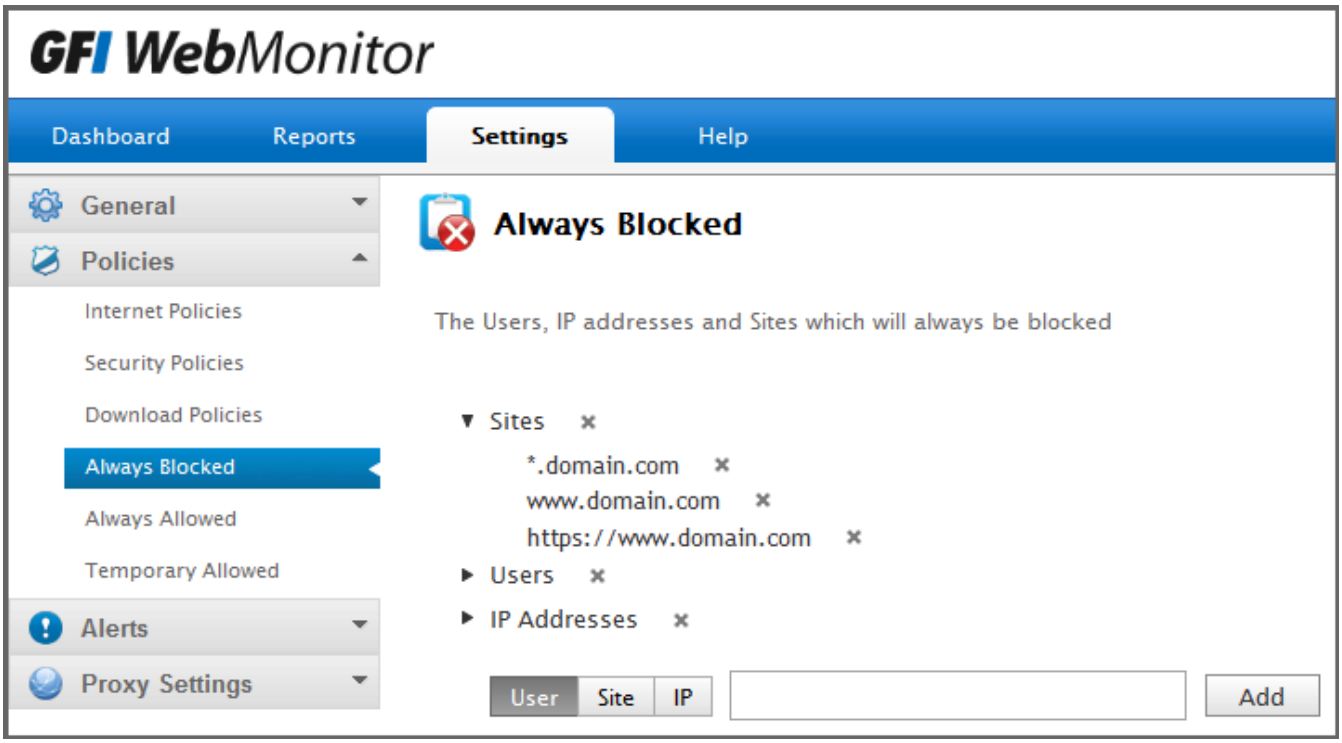
The **Always Blocked** list is a list of sites, users and IP addresses that should always be blocked. The **Always Blocked** list takes priority over all WebFilter and WebSecurity policies.

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

Adding Items to the Always Blocked list

To add an item to the Always Blocked list:

1. Go to **Settings > Policies > Always Blocked**.



Screenshot 55: Configuring Always Blocked list

2. Select **User**, **Site** or **IP** and key in the value in the space provided.

3. Click **Add**.

4. Click **Save**.

NOTE

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

NOTE

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

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

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

7.2.4 Deleting Items From the Always Blocked list

To delete an item from the Always Blocked list:

1. Go to **Settings > Policies > Always Blocked**.

2. Click the **Delete** icon next to the item to delete.

3. Click **Save**.

7.2.5 Configuring Always Allowed List

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

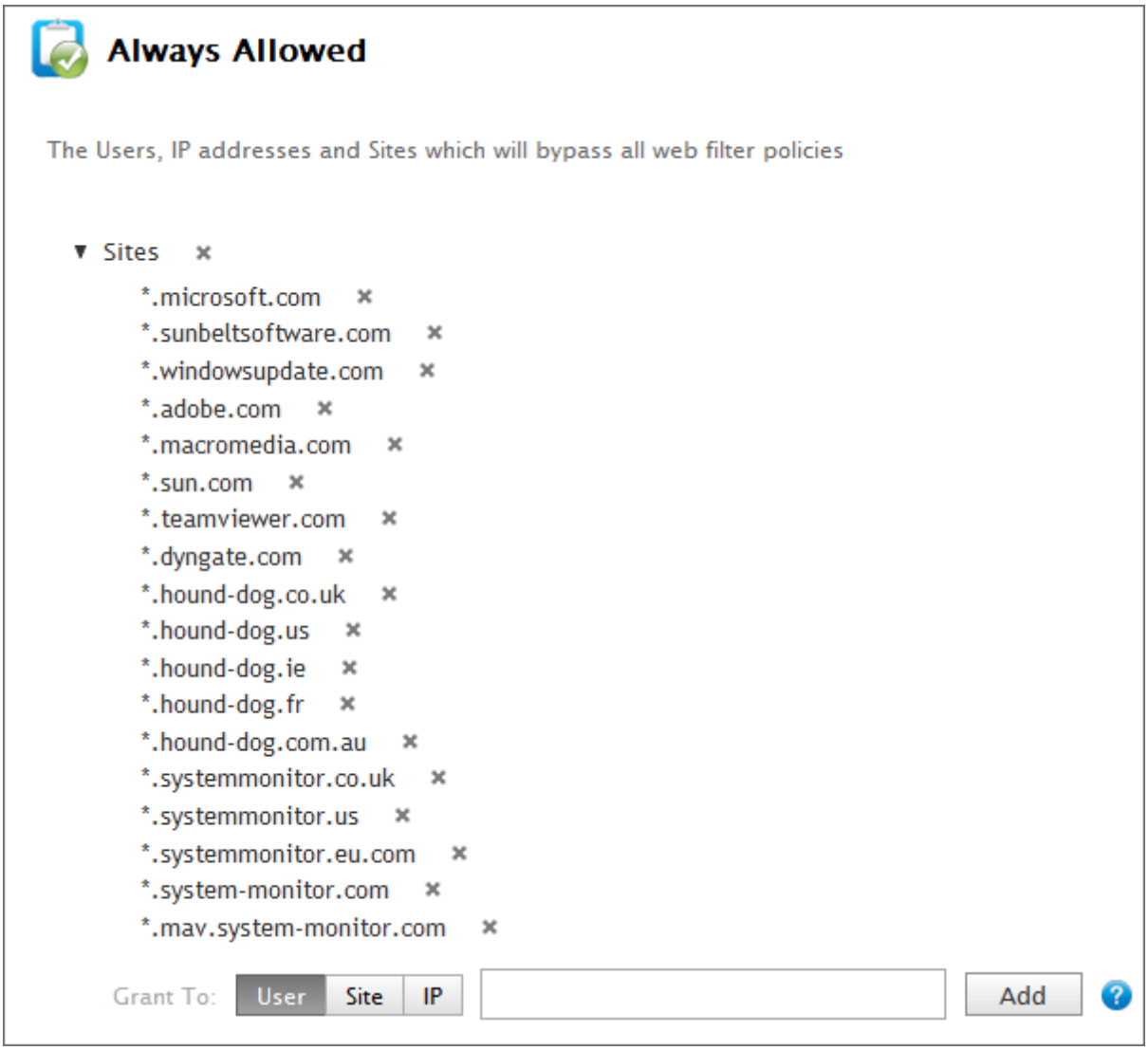
IMPORTANT

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

Pre-configured Items

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

Adding Items to the Always Allowed List



Screenshot 56: Adding items to Always Allowed list

To add an item to the **Always Allowed** list:

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

NOTE

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

NOTE

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

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

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

Deleting Items From the Always Allowed List

To delete an item from the Always Allowed list:

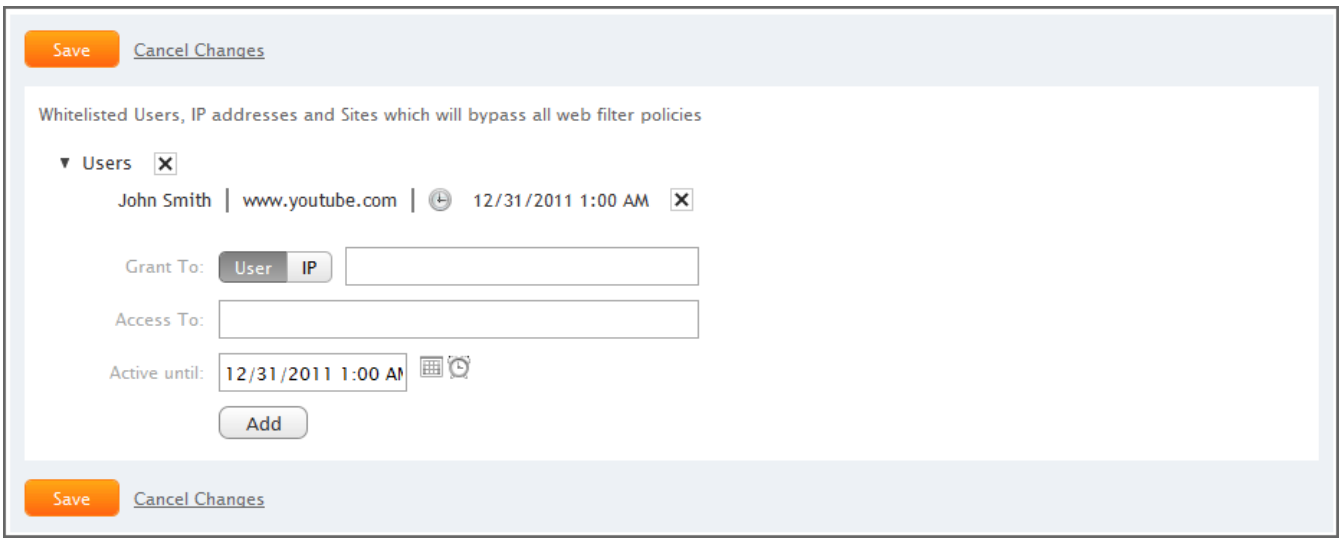
1. Go to **Settings > Policies > Always Allowed**.
2. Click the **Delete** icon next to the item to delete.
3. Click **Save**.

7.2.6 Configuring Temporary Allowed List

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

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

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



Screenshot 57: Configuring Temporary Allowed list

2. In the **Grant To** field, select **User** or **IP** and key in the user or IP address to grant access to in the space provided.
3. In the **Access To** field, type the URL of the website to grant access to.
4. In the **Active until** area, select the date and time during which the policy will be active.
5. Click **Save**.

Deleting Items From the Temporary Allowed list

To delete an item from the Temporary Allowed list:

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

3. Click **Save**.

7.2.7 WebSecurity Edition Policies

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

The following sections help you:

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

Enabling or Disabling a Configured Policy

To enable or disable a policy:

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

Deleting a Policy

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

7.2.8 Configuring Security Policies

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

NOTE

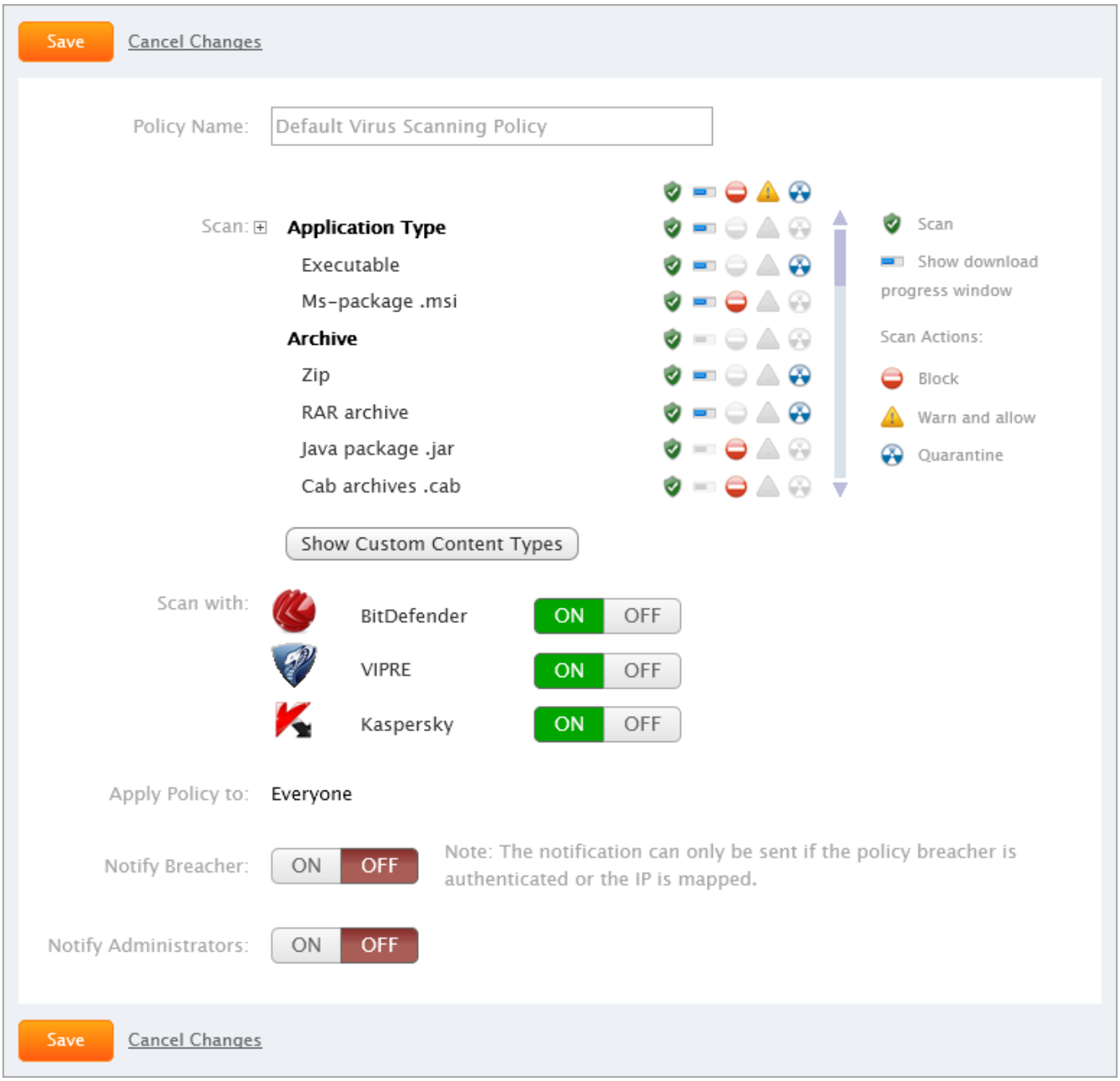
Certain fields in the default policy cannot be edited. These include **Policy Name** and **Apply Policy To**.

IMPORTANT

All added policies take priority over the default policy.

To edit the Default Virus Scanning Policy:

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



Screenshot 58: Configuring Default Virus Scanning Policy

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

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

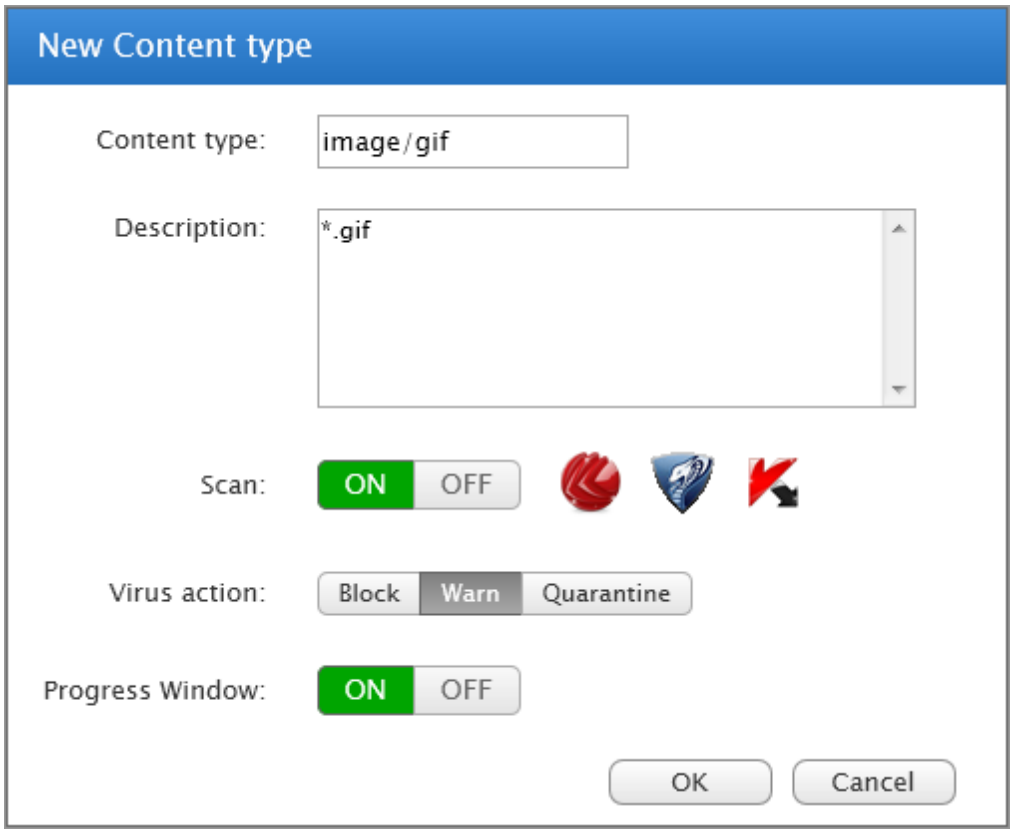
Table 31: Scanning options

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

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

5. [Optional] To define custom content types, click **Show Custom Content Types**, then:

a. Click **Add Content Type**.



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

> **NOTE**
>
> This must be a MIME type, for example, if you want to add a content type for *.gif, type: `image/gif`.

c. In the Description field, enter a description.

d. Define the actions to take when the content type is downloaded.

e. Click **OK**.

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

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

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

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

10. Click **Save**.

IMPORTANT

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

IMPORTANT

Click **Save** before you navigate away from page.

See also:

Cloning a Policy

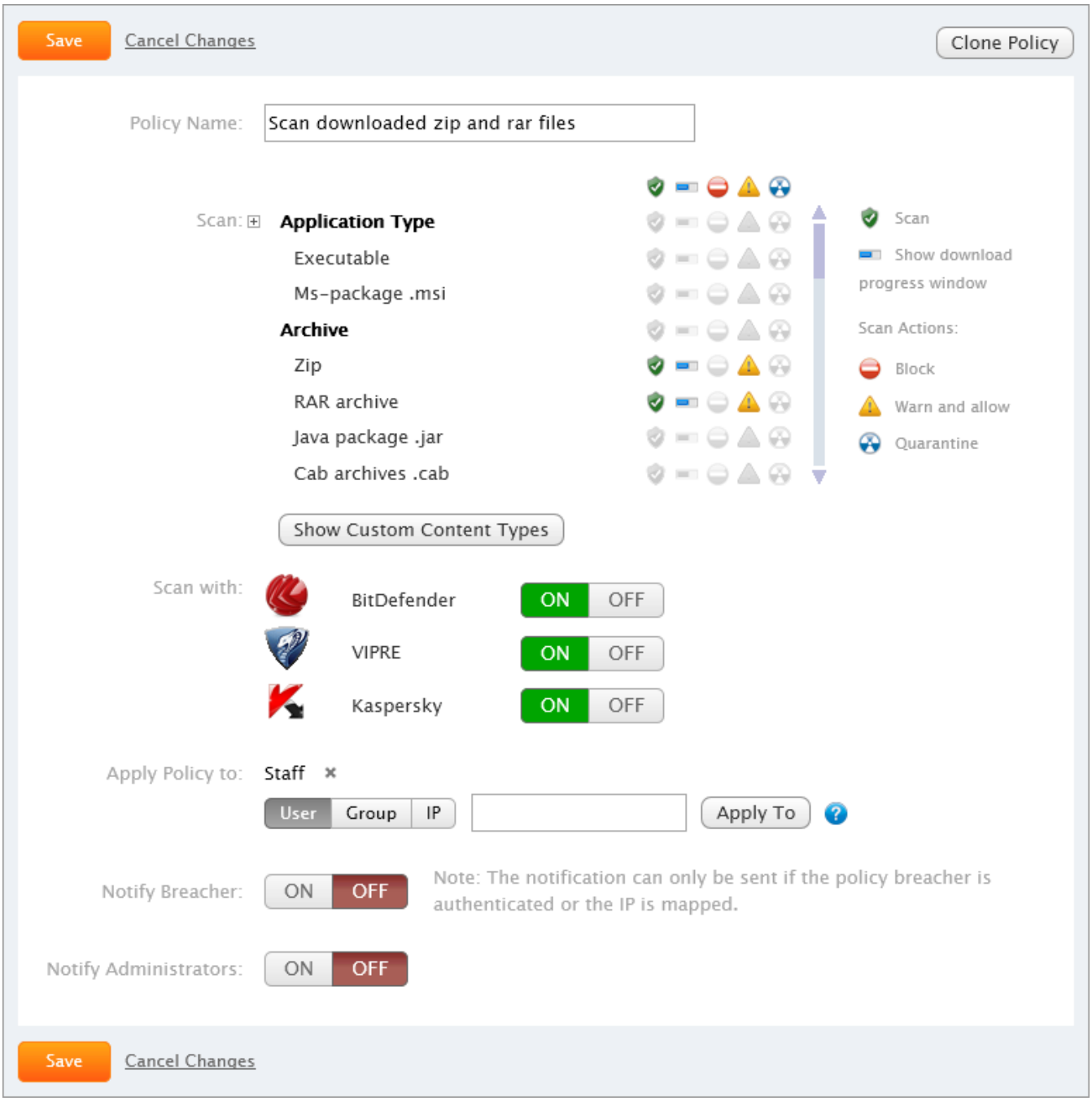
Adding a New Security Policy

7.2.9 Adding a New Security Policy

To add a new Security Policy:

1. Go to **Settings > Policies > Security Policies**.

2. Click **Add Policy**.



Screenshot 59: Creating a new Security Policy

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

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

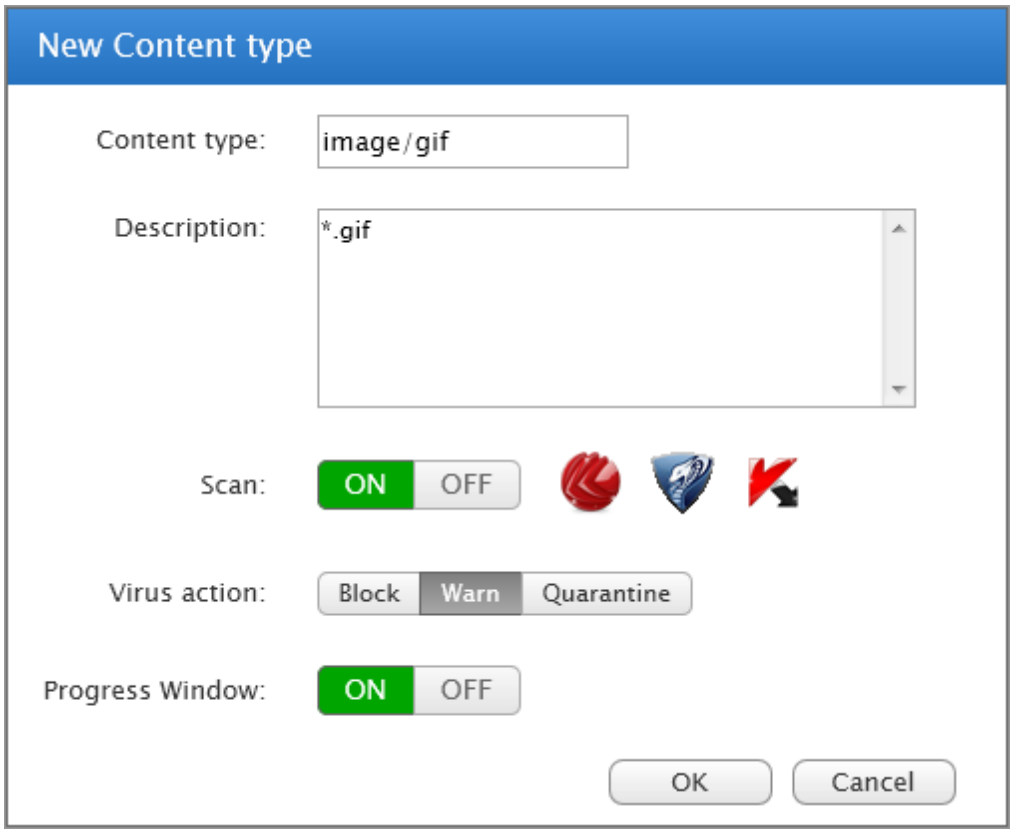
Table 32: Scanning options

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

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

5. [Optional] To define custom content types, click **Show Custom Content Types**, then:

a. Click **Add Content Type**.



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

> **NOTE**
>
> This must be a MIME type, for example, if you want to add a content type for *.gif, type: `image/gif`.

c. In the Description field, enter a description.

d. Define the actions to take when the content type is downloaded.

e. Click **OK**.

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

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

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

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

10. Click **Save**.

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

> **IMPORTANT**
>
> Click **Save** before you navigate away from page.

See also:

Cloning a Policy

7.2.10 Configuring Security Engines

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

To turn off a security engine:

1. Go to **Settings > Security Policies**.

Screenshot 60: Configuring Security Engines

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

To perform additional configuration refer to the following sections:

- Configuring Kaspersky
- Configuring Anti Phishing
- Configuring ThreatTrack

7.2.11 Configuring Kaspersky

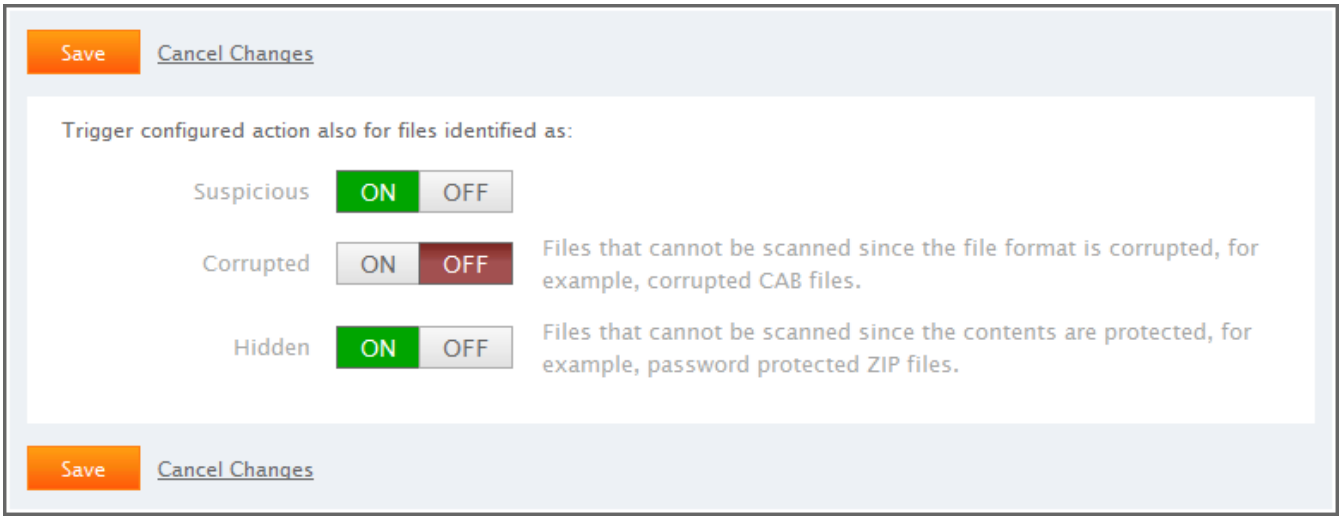
The **Kaspersky** anti-virus scanning engine enables you to state whether the actions specified in the **Virus Scanning Policies** should also be used when files are identified as:

Table 33: Kaspersky engine options

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

To configure Kaspersky:

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



Screenshot 61: Configuring Kaspersky security engine

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

7.2.12 Configuring Anti Phishing Notifications

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

To configure notifications:

1. Go to **Settings > Policies > Security Policies**.
2. Click **Anti-Phishing**.
3. Next to **Notify Breacher**, click **ON** to enable notifications to be sent to the person attempting to access a known phishing site.

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

5. Click **Save**.

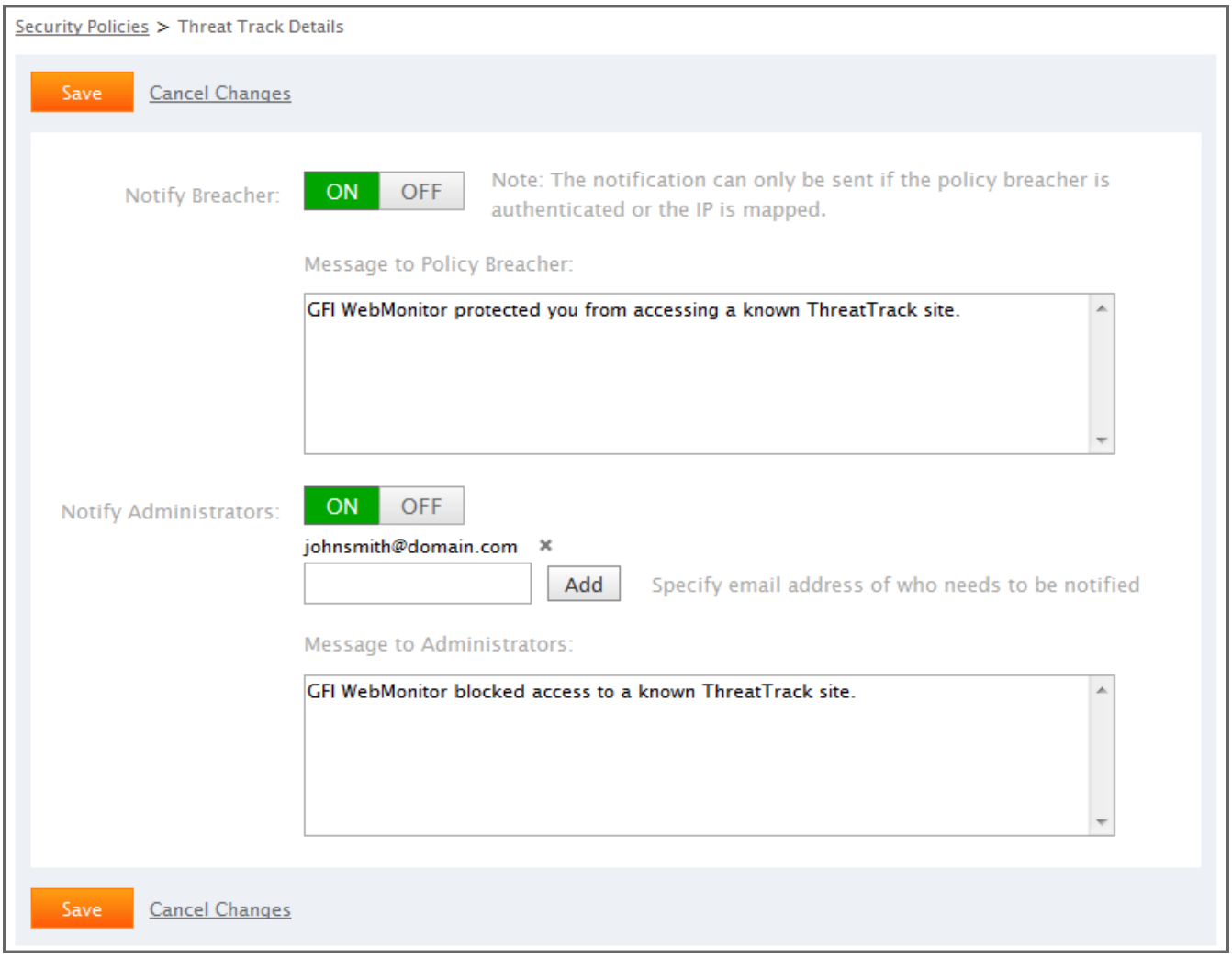
7.2.13 Configuring ThreatTrack

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

To configure ThreatTrack:

1. Go to **Settings > Policies > Security Policies**.

2. Click **ThreatTrack**.



Screenshot 62: Configuring ThreatTrack notifications

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

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

5. Click **Save**.

7.2.14 Configuring Download Policies

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

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

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

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

> **IMPORTANT**
>
> **All added policies take priority over the default policy.**

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

Enabling or Disabling a Download Policy

To enable or disable a Download Policy:

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

Deleting a Download Control Policy

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

See also:

Cloning a Policy

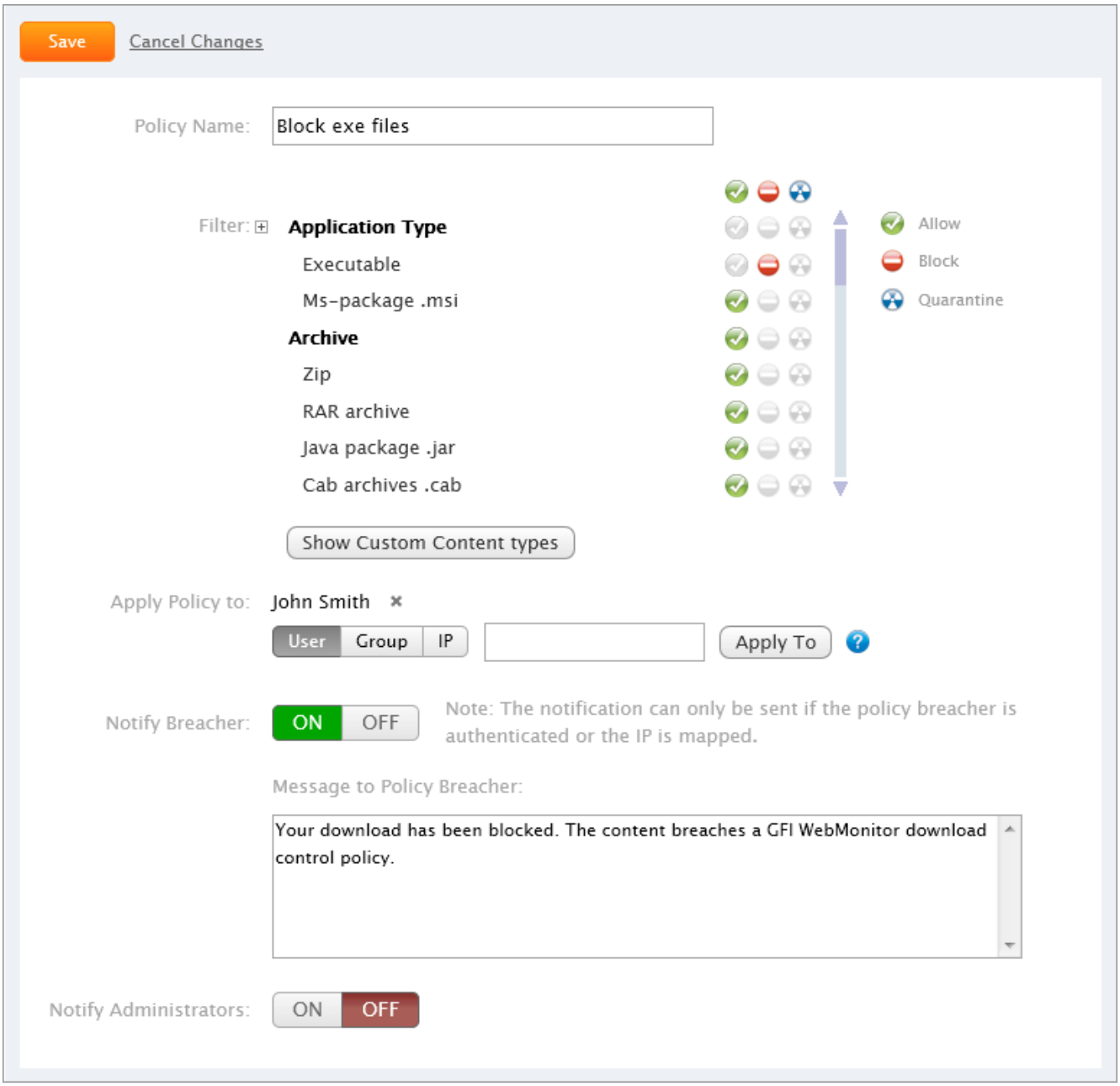
Adding a New Download Policy

Editing an Existing Download Policy

Adding a New Download Policy

To add a Download Policy:

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



Screenshot 63: New download policy

2. Click **Add Policy**.

3. In the **Policy Name** field, key in a Policy Name.

4. From the **Filter** area, select action to be taken for file types. Available options are:

Table 34: Filtering options

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

NOTE

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

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

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

NOTE

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

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

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

9. Click **Save**.

See also:

Cloning a Policy

Configuring Download Policies

Editing an Existing Download Policy

Editing an Existing Download Policy

To edit a Download Control Policy:

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

2. Click the policy name to edit.

3. Change the required settings.

4. Click **Save**.

See also:

Cloning a Policy

Configuring Download Policies

Adding a New Download Policy

Cloning a Policy

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

To clone a policy:

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

> **NOTE**
>
> Default policies cannot be cloned.

7.3 Configuring Alerts

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

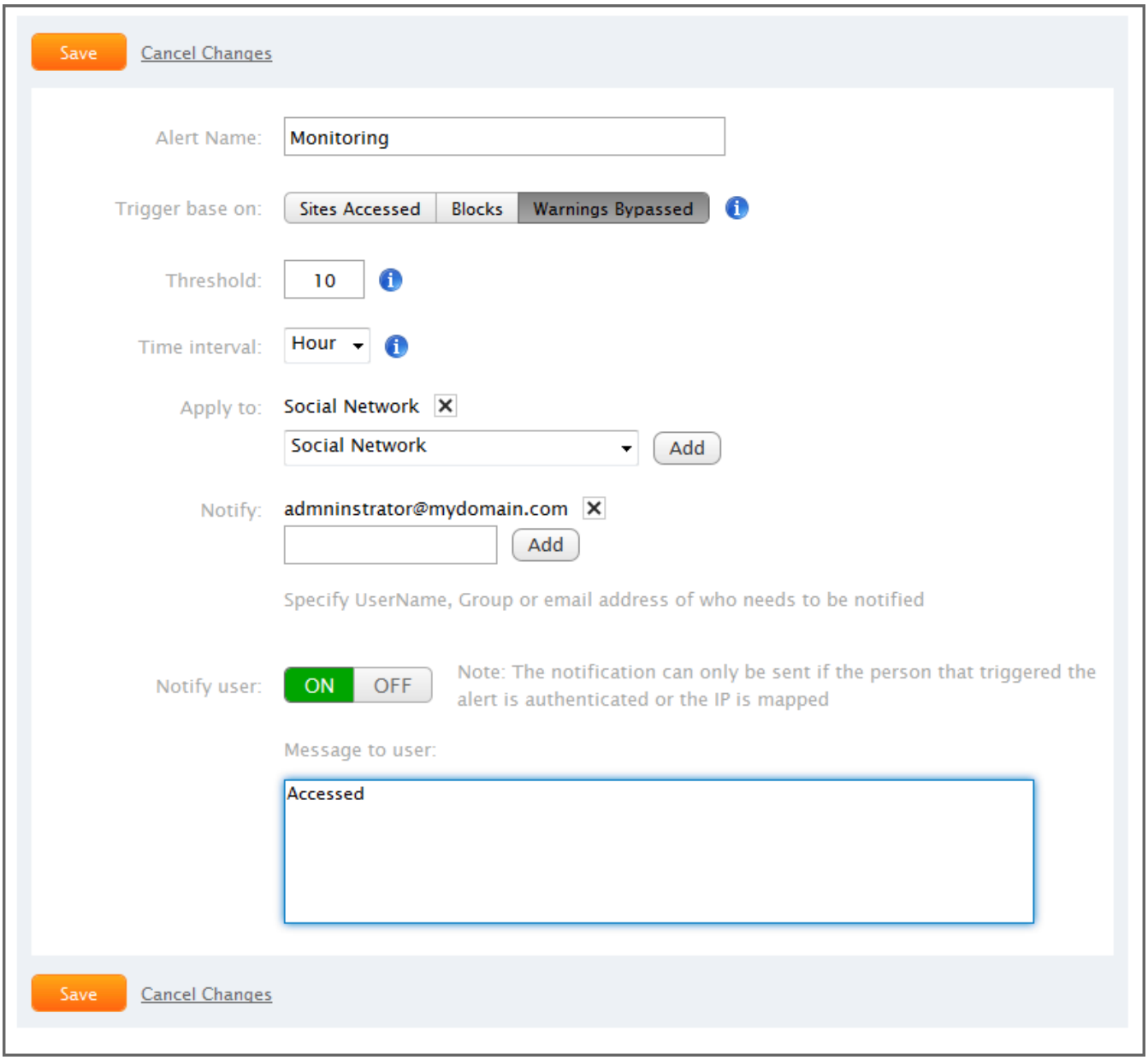
- Configuring Monitoring Alerts
- Configuring Bandwidth Alerts
- Configuring Security Alerts

7.3.1 Configuring Monitoring Alerts

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

To configure monitoring alerts:

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



Screenshot 64: Configuring Monitoring alerts

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

4. In the **Trigger base on** area, select a one of the following options:

- **Sites Accessed** - the alert will be triggered if the total number of specified sites is exceeded
- **Blocks** - selected users will be notified when the specified number of Blocks is exceeded
- **Warnings Bypassed** - selected users will be notified when the specified number of bypassed warnings is exceeded

5. In the **Threshold** area, specify a number that will trigger the alert if exceeded.

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

- Hour
- Day
- Week

7. In the **Apply to** field, select a category from the available list and click **Add**.

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

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

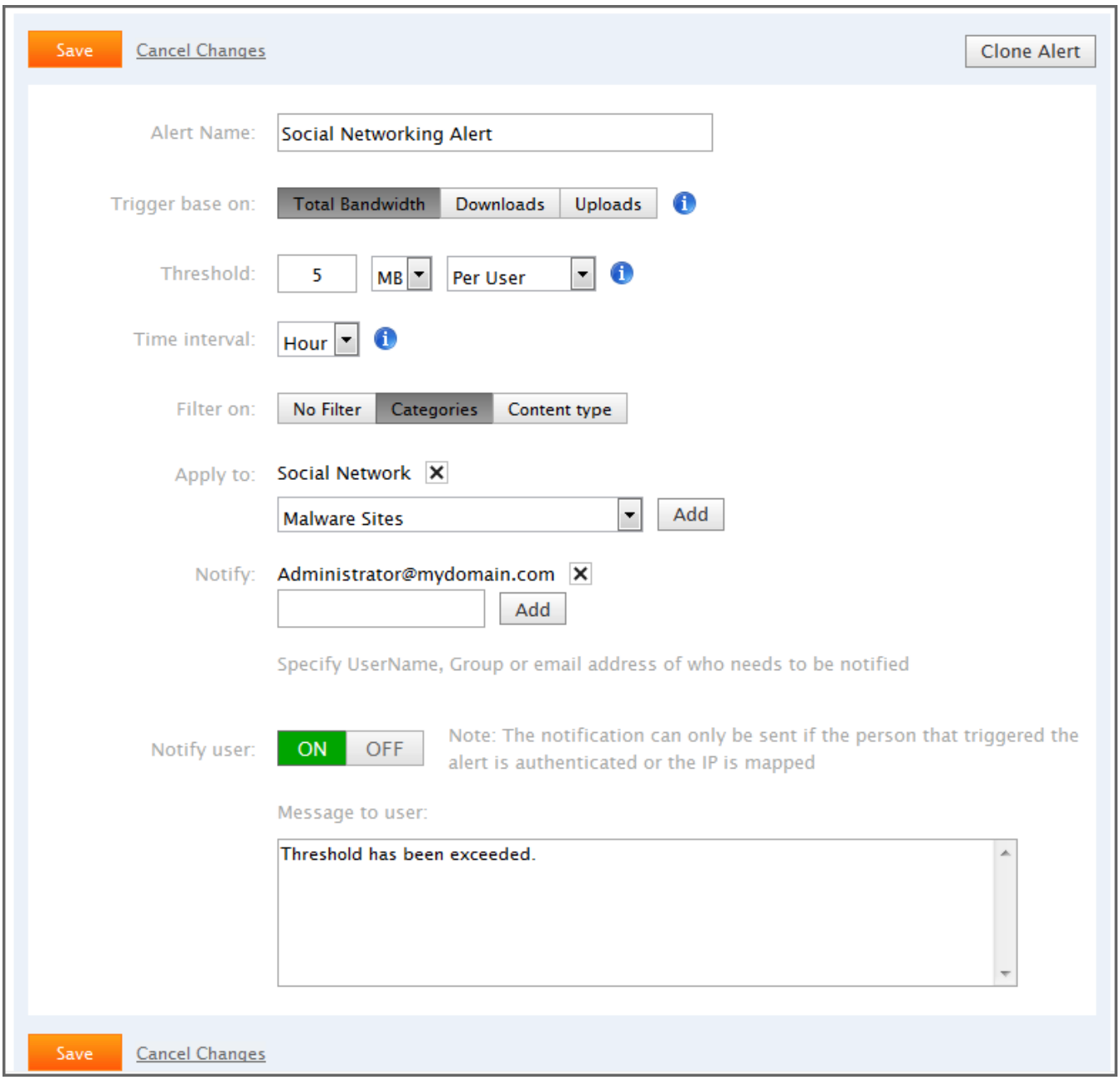
10. Click **Save**.

7.3.2 Configuring Bandwidth Alerts

To configure bandwidth alerts:

1. Go to **Settings > Alerts > Bandwidth Alerts**.

2. Click **Add Alert**.



Screenshot 65: Configuring Bandwidth alerts

3. In the **Alert Name** field, key in a name.

4. In the **Trigger base on** area, select a one of the following options:

Table 35: Bandwidth alert trigger options

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

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

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

- Hour
- Day
- Week

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

Table 36: Bandwidth alerts filtering options

FILTER	DESCRIPTION
No Filter	Select this option to make the alert available on all type of traffic.
Categories	Select desired categories from a predefined list and click **Add**.
Content type	Select desired content types from a predefined list and click **Add**.

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

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

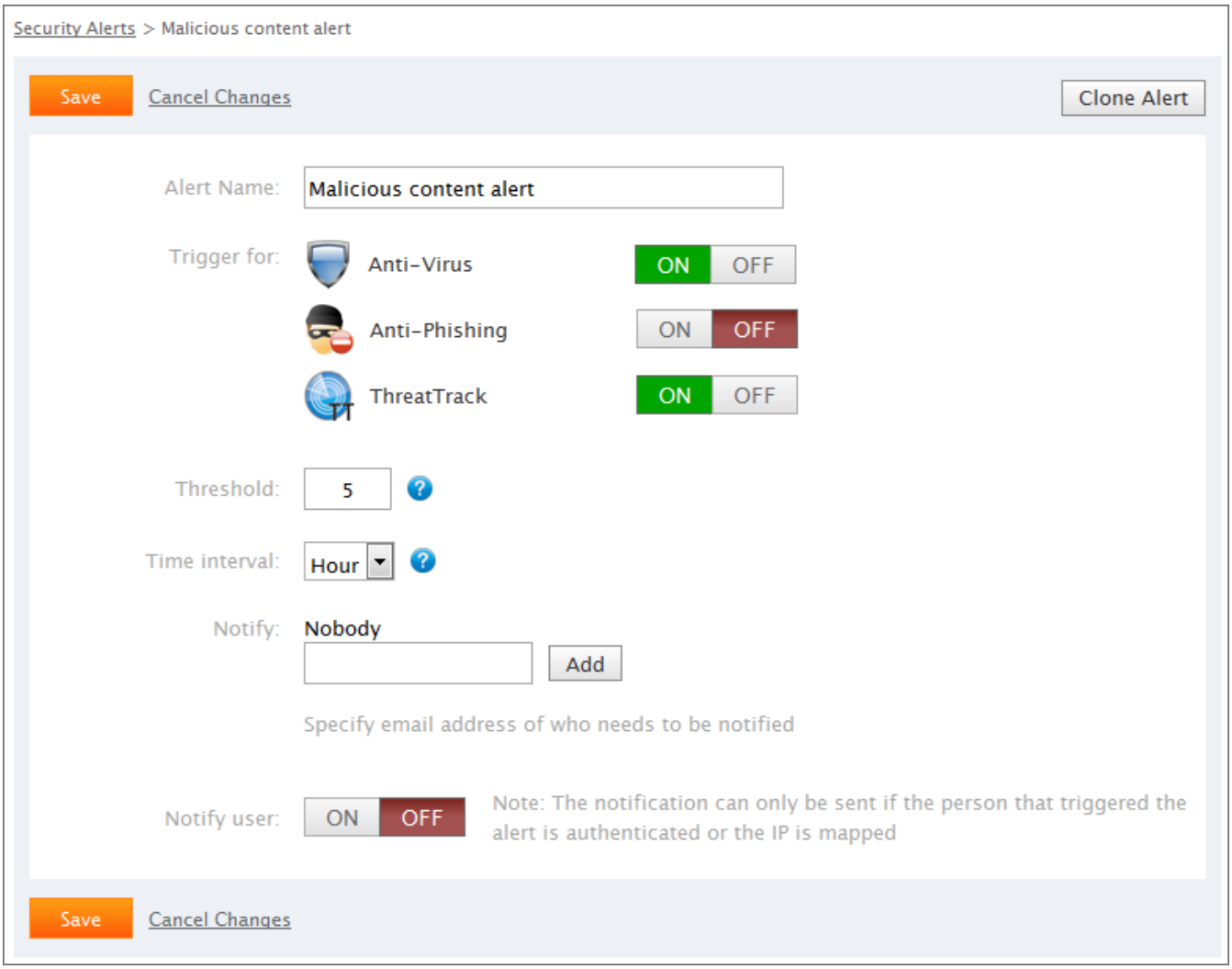
10. Click **Save**.

7.3.3 Configuring Security Alerts

To configure security alerts:

1. Go to **Settings > Alerts > Security Alerts**.

2. Click **Add Alert**.



Screenshot 66: Configuring Security alerts

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

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

Table 37: Security alerts trigger options

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

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

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

- Hour
- Day
- Week

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

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

9. Click **Save**.

8 Troubleshooting and support

8.1 Introduction

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

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

8.2 GFI SkyNet

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

8.3 Web Forum

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

8.4 Request Technical Support

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

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

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

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

8.5 Documentation

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

8.6 Common Issues

Table 38: Common troubleshooting issues

ISSUE ENCOUNTERED	SOLUTION
WebFilter module fails to register correctly on all members of the array when GFI WebMonitor is installed on Microsoft® TMG (where Microsoft® TMG is in array of other Microsoft® TMG Severs)	The GFI WebMonitor DLL does not get registered and needs to be registered manually. Run the command `regsrv32 webmonplg.dll` from the folder that contains the **webmonplg.dll**. This is typically located in the Microsoft® ISA or Microsoft® TMG folder on each server where GFI WebMonitor is installed.
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. Next, Internet browsers on client machines have to be configured to use the GFI WebMonitor proxy machine as the default proxy. For more information, refer to Post Installation Actions (page 22). In the event that the users are still not able to browse and/or download from the Internet, add an exception rule in the firewall on the GFI WebMonitor proxy machine to allow incoming TCP traffic on port 8080. For more information on how to enable firewall ports on Windows® Firewall, refer to http://go.gfi.com/?pageid=WebMon_WIndowsFirewall
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://go.gfi.com/?pageid=WebMon_AutomaticDetection
Users are still required to authenticate themselves manually when browsing, even when Integrated authentication is used.	Integrated authentication will fail when GFI WebMonitor is installed on a Windows® 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**.

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 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 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 (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://go.gfi.com/?pageid=WebMon_FirefoxIssues

9 Glossary

A

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

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

AD
See Active Directory

Administrator
The person responsible for installing and configuring GFI WebMonitor.

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

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

Anti-virus
Software that detects viruses on a computer.

B

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

C

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

CER
See CER file format

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

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

Chained Proxy

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

Console

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

CRL

See Certificate Revocation List

D

Dashboard

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

E

Expired Certificate

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

F

File Transfer Protocol

A protocol used to transfer files between computers.

FTP

See File Transfer Protocol.

G

Google Chrome

A web browser developed and distributed by Google.

GPO

See Group Policy Objects.

Group Policy Objects

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

H

Hidden Downloads

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

HTTP

See Hypertext Transfer Protocol.

HTTPS

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

HyperText Transfer Protocol

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

HyperText Transfer Protocol over Secure Socket Layer (SSL)

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

I

Internet Browser

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

Internet Gateway

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

L

LAN

See Local Area Network.

LDAP

See Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol

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

Local Area Network

An internal network that connects machines in a small area.

M

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

N

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.

P

Personal Information Exchange file format

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

PFX

See Personal Information Exchange file format.

Phishing

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

Port Blocking

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

Proxy Server

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

Q

Quarantine

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

R

Revoked Certificate

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

S

Spyware

Unwanted software that publishes private information to an external source.

T

Traffic Forwarding

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

U

Uniform Resource Locator

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

URL

See Uniform Resource Locator.

User Agent

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

V

Virus

Unwanted software that infects a computer.

W

WAN

See Wide Area Network.

Web Proxy AutoDiscovery protocol

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

Web traffic

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

WebFilter Edition

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

WebGrade Database

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

WebSecurity Edition

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

Wide Area Network

An external network that connects machines in large areas.

WPAD

See Web Proxy AutoDiscovery protocol.

10 Appendix 1

This section contains the following topics:

10.1 Assigning Log On As A Service Rights

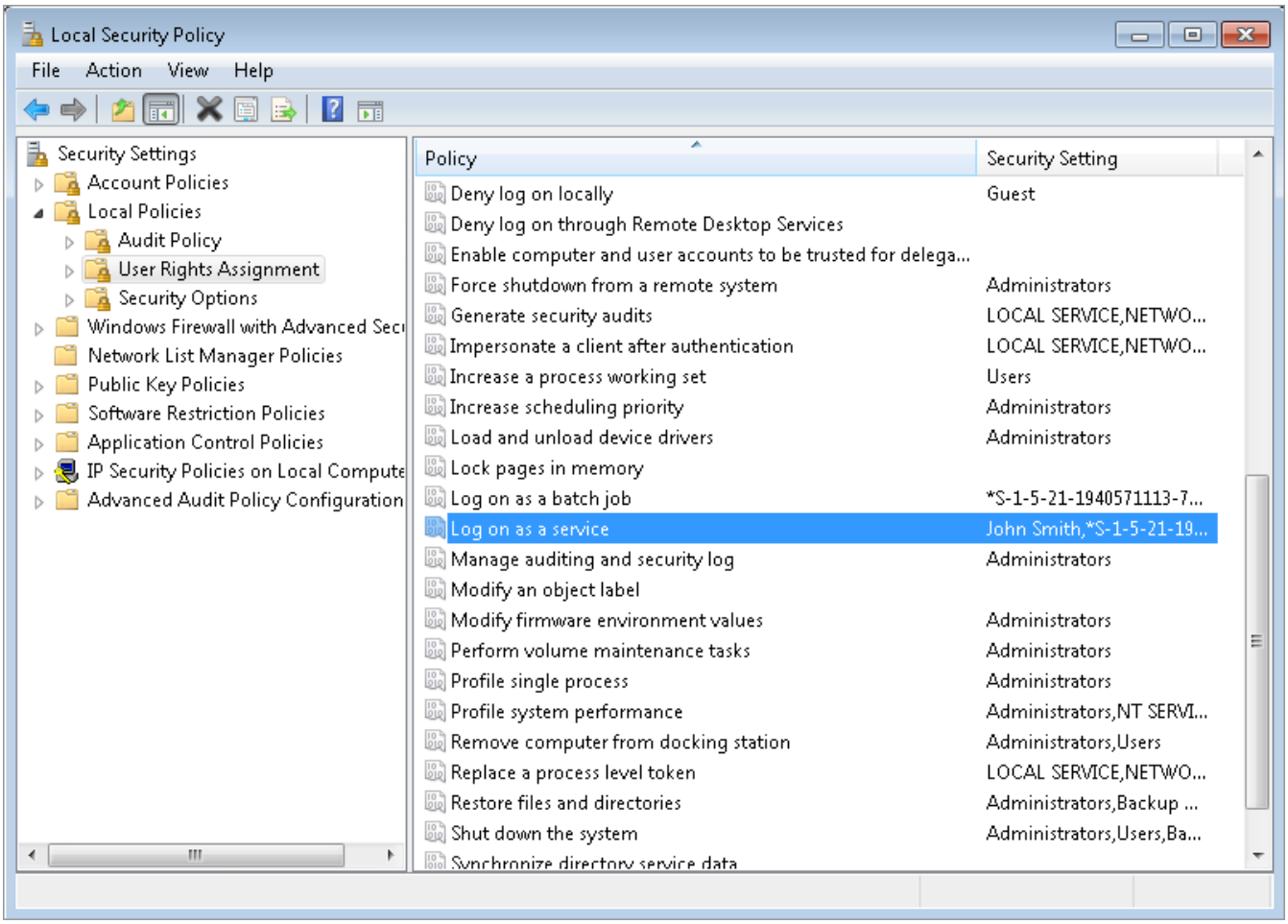
Logon rights control who is authorized to log on to a computer and how they can log on. **Log on as a service** rights allow a security principal to log on as a service. Services can be configured to run under the Local System, Local Service, or Network Service accounts, which have a built-in right to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

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

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

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

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



Screenshot 67: Microsoft Windows Server: Local Security Policy window

2. Expand **Security Settings > Local Policies > User Rights Assignment**.

3. Right-click **Log on as a service** from the right panel and click **Properties**.

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

5. Click **Add User or Group** button.

6. Key in the account name and click **OK**.

7. Click **Apply** and **OK**.

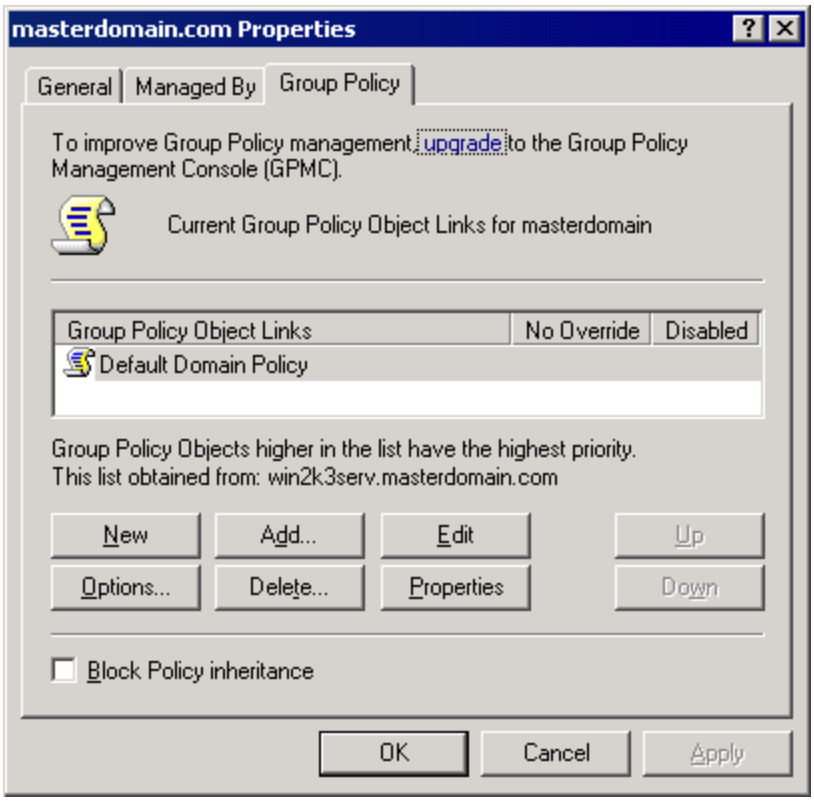
8. Close all open windows.

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

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

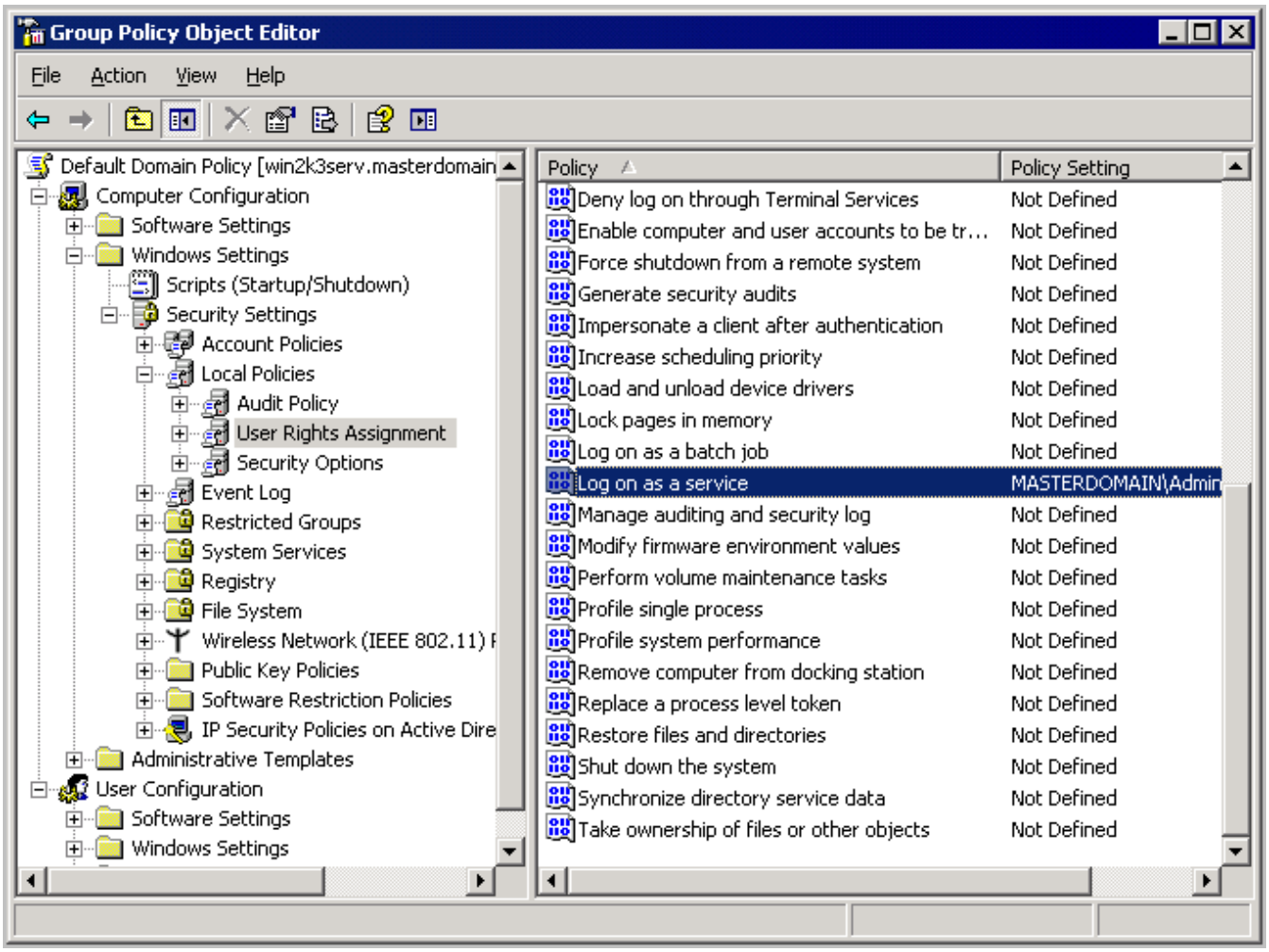
1. Navigate to **Start > Programs > Administrative Tools > Active Directory Users and Computers** on the DNS server.

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



Screenshot 68: Active Directory GPO dialog

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



Screenshot 69: GPO Editor window

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

6. Right-click **Log on as a service** from the right panel and click **Properties**.

7. Select the **Security Policy Setting** tab.

8. Check **Define these policy settings** checkbox

9. Click **Add User or Group** button.

10. Key in the account name and click **OK**.

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

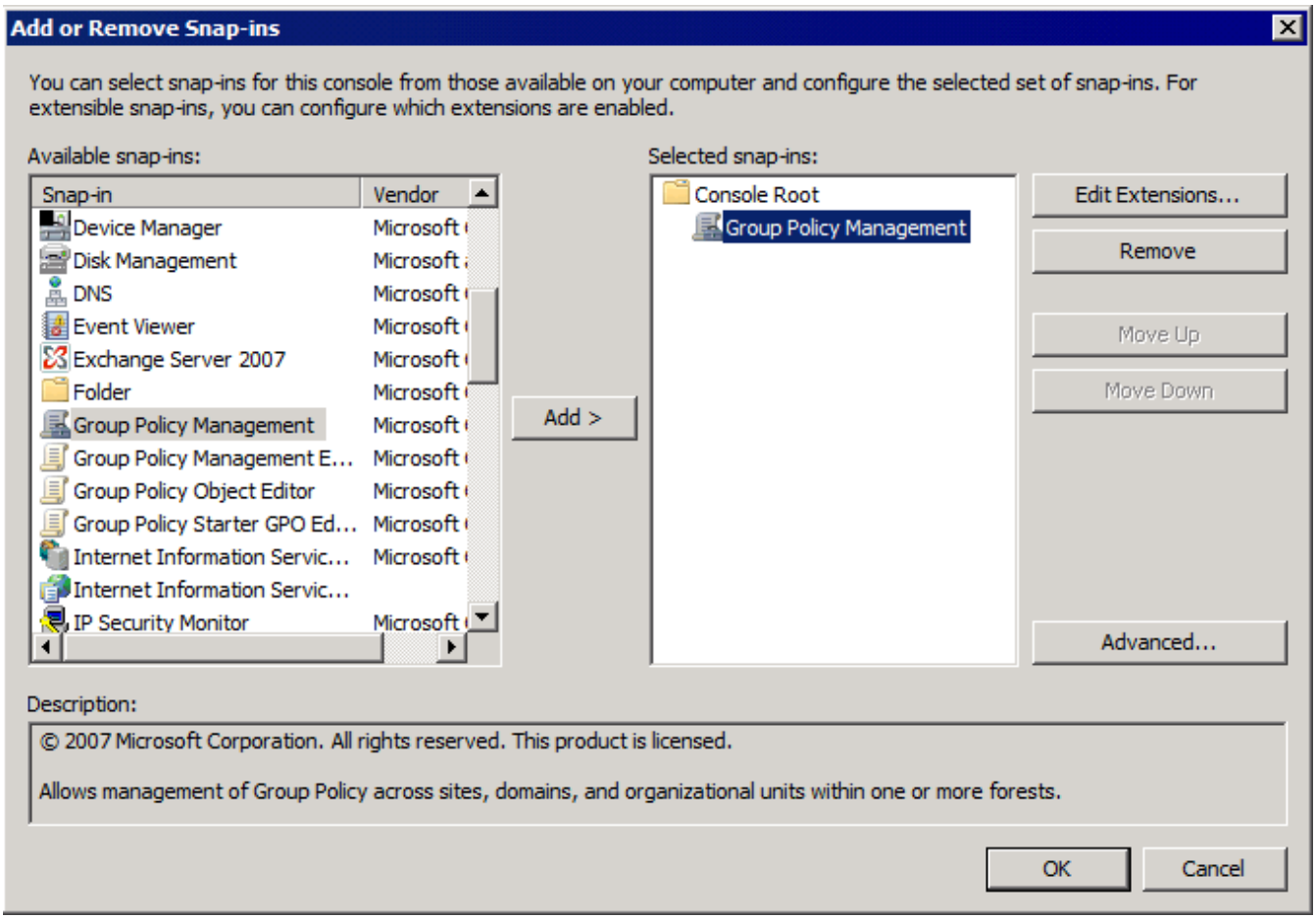
12. Close all open windows.

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

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

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

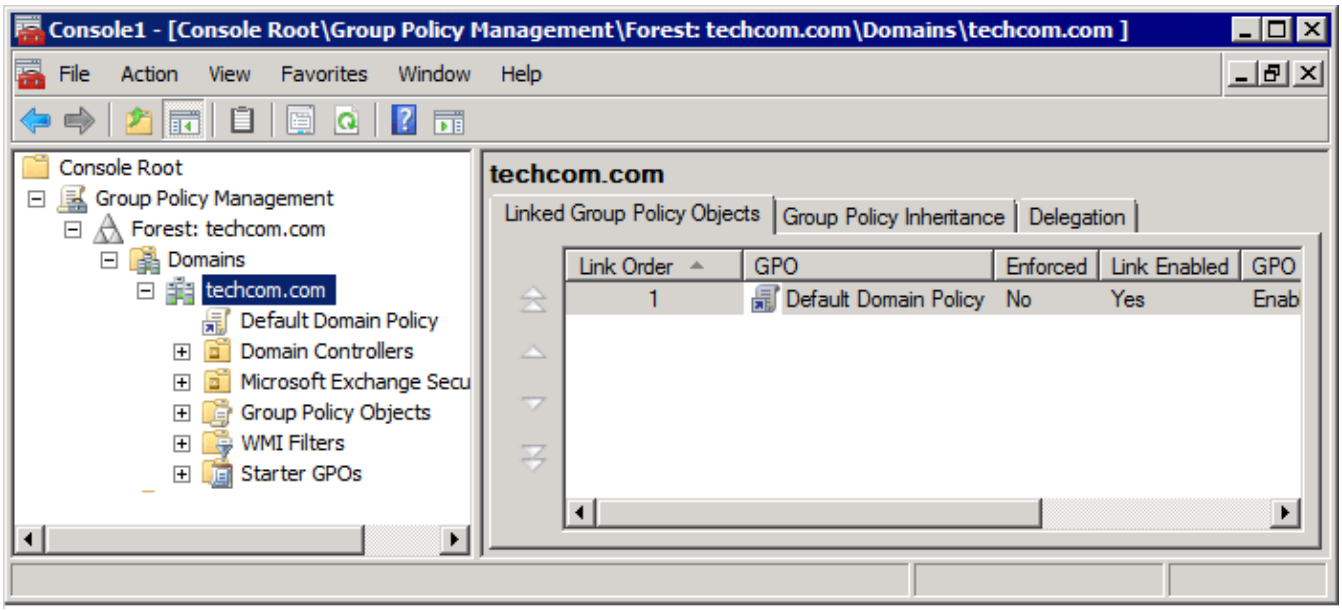
2. In the **Console Root** window, navigate to **File > Add/Remove Snap-in…** to open the **Add or Remove Snap-ins** window.



Screenshot 70: Add/Remove Snap-ins window

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

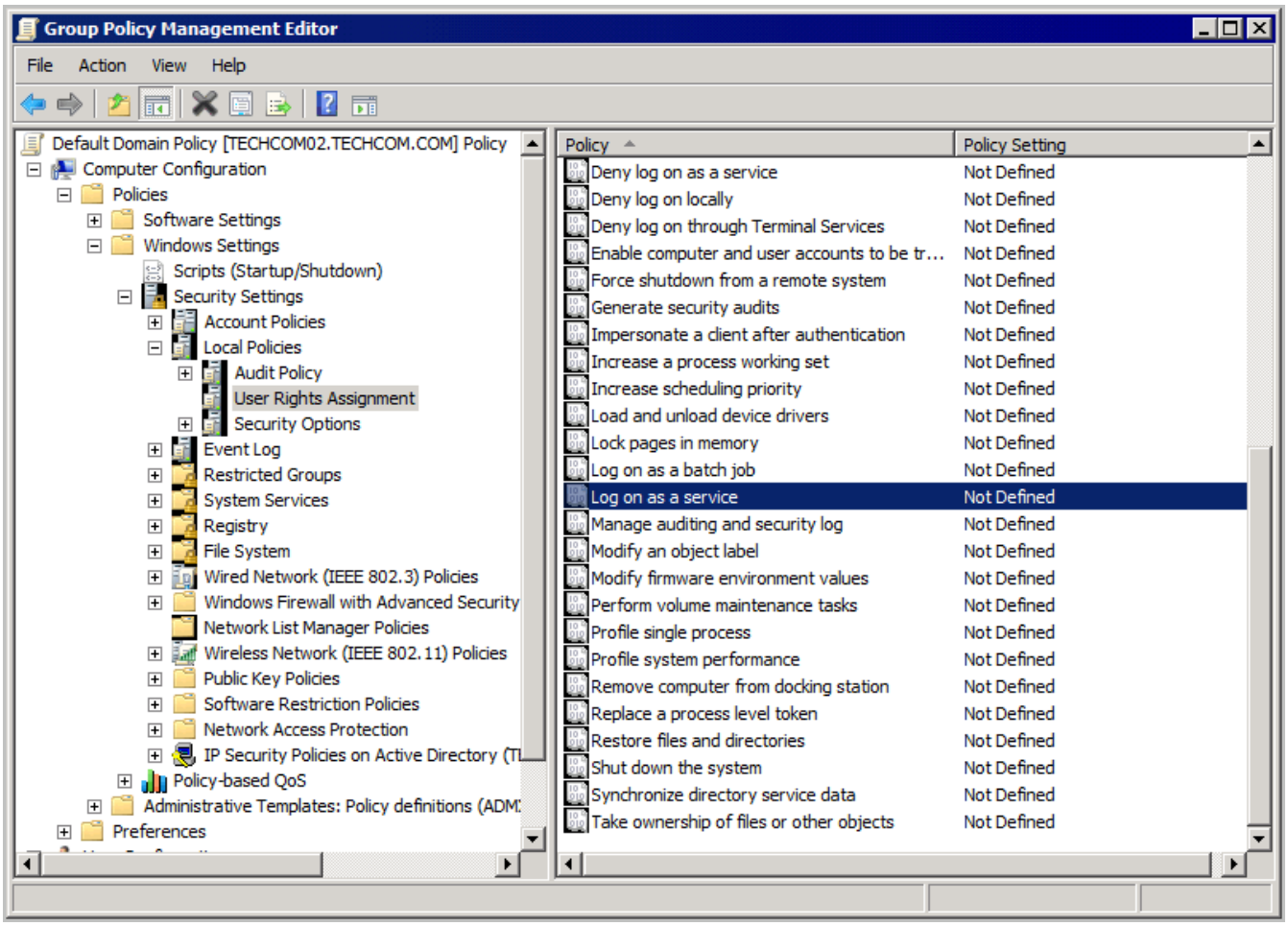
4. Click **OK**.



Screenshot 71: Console Root domain window

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

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



Screenshot 72: Group Policy Management Editor window

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

8. Right-click **Log on as a service** from the right panel and click **Properties**.

9. Select the **Security Policy Setting** tab.

10. Check **Define these policy settings** checkbox

11. Click **Add User or Group** button.

12. Key in the account name and click **OK**.

13. Click **Apply** and **OK**.

14. Close all open windows.

10.2 Configuring Routing and Remote Access

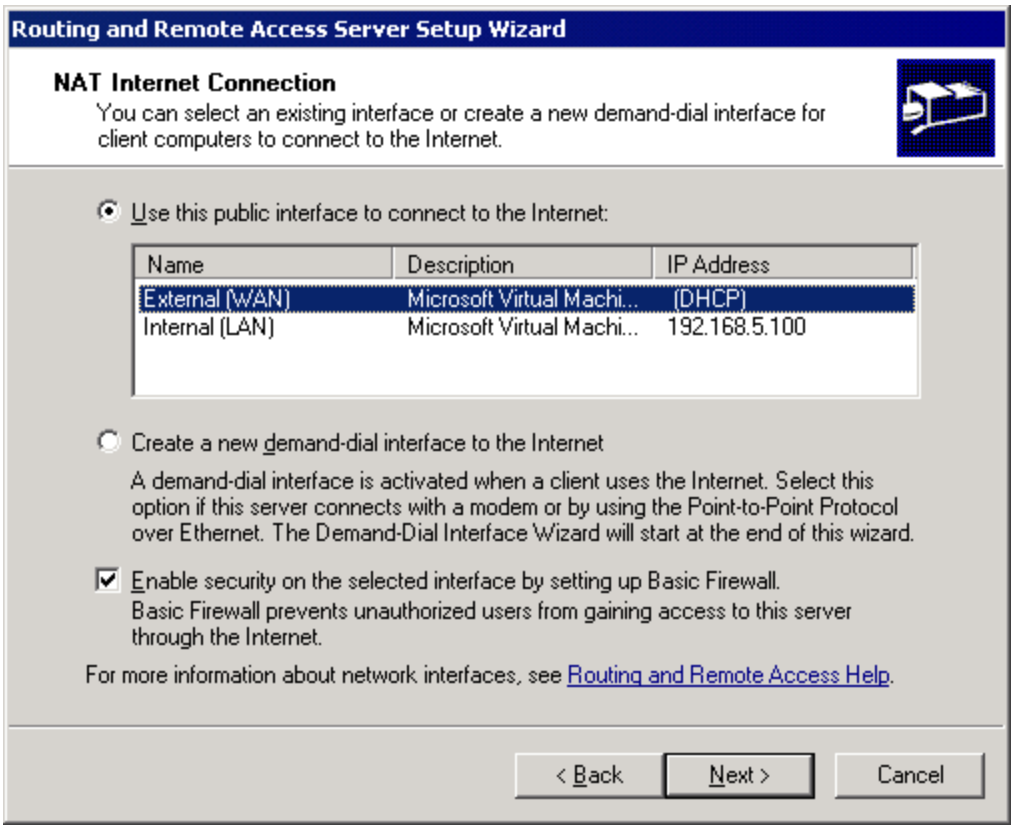
When installing GFI WebMonitor in Gateway mode on a Windows® Server 2003 or Windows® Server 2008, the Routing and Remote Access must be configured to use Network Address Translation (NAT). This can be done by:

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

2. Right-click **<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 73: Microsoft Windows Server 2003: Routing and Remote Access Server Setup Wizard dialog

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

6. Select the network card connected to the external network and click **Next**.

7. Click **Finish**.

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

1. From command prompt, key in `services.msc`

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

10.3 Disabling Internet Connection Settings On Client Machines

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

Disabling Internet Connections Page Using GPO in Microsoft Windows Server 2003

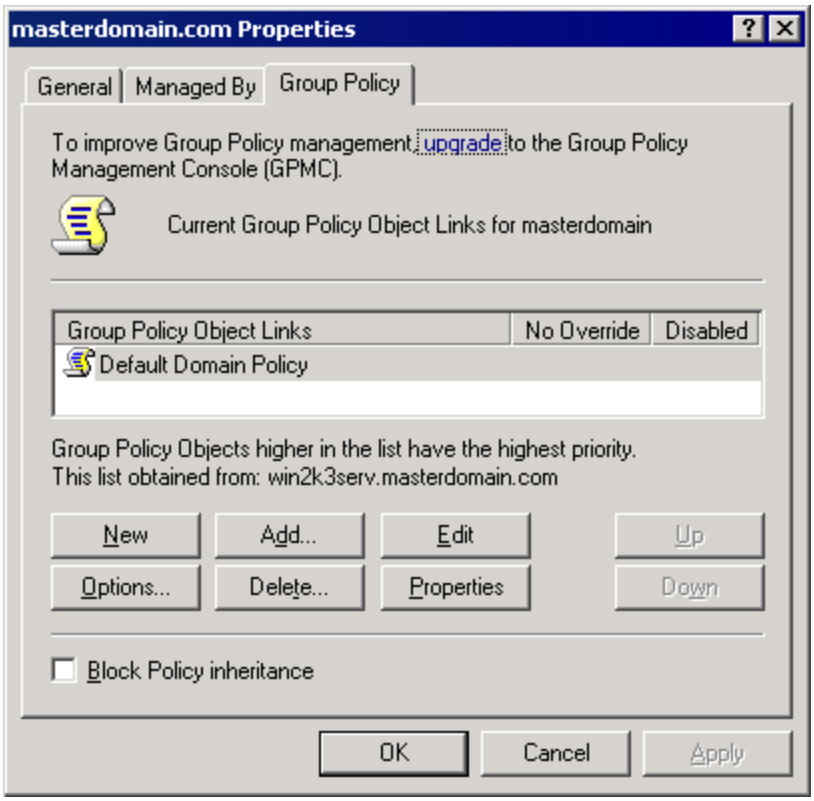
Disabling Internet Connections Page Using GPO in Microsoft Windows Server 2008

10.3.1 Disabling Internet Connections Page Using GPO in Windows® Server 2003

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

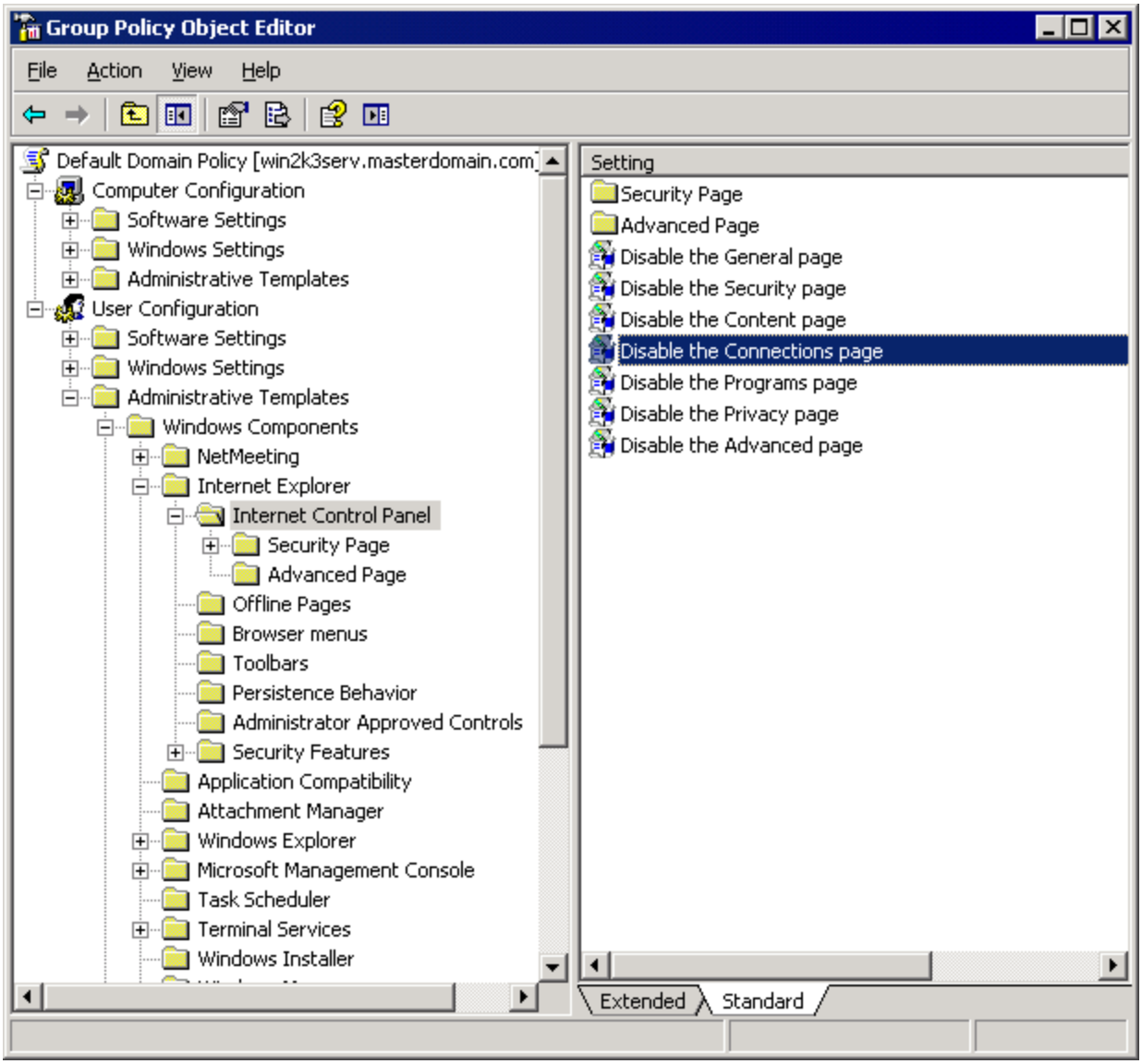
1. Navigate to **Start > Programs > Administrative Tools > Active Directory Users and Computers** on the DNS server.

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



Screenshot 74: Active Directory GPO dialog

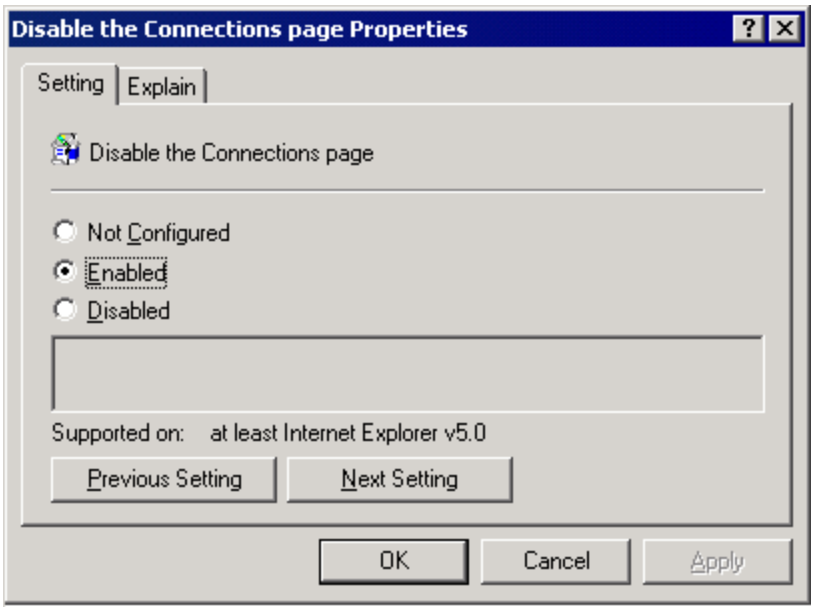
3. Select **Group Policy** tab in the **Domain Properties** dialog.
4. Select **Default Domain Policy** from the list and click **Edit**.



Screenshot 75: GPO Editor window

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

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



Screenshot 76: Disable the Connection page Properties dialog

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

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

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

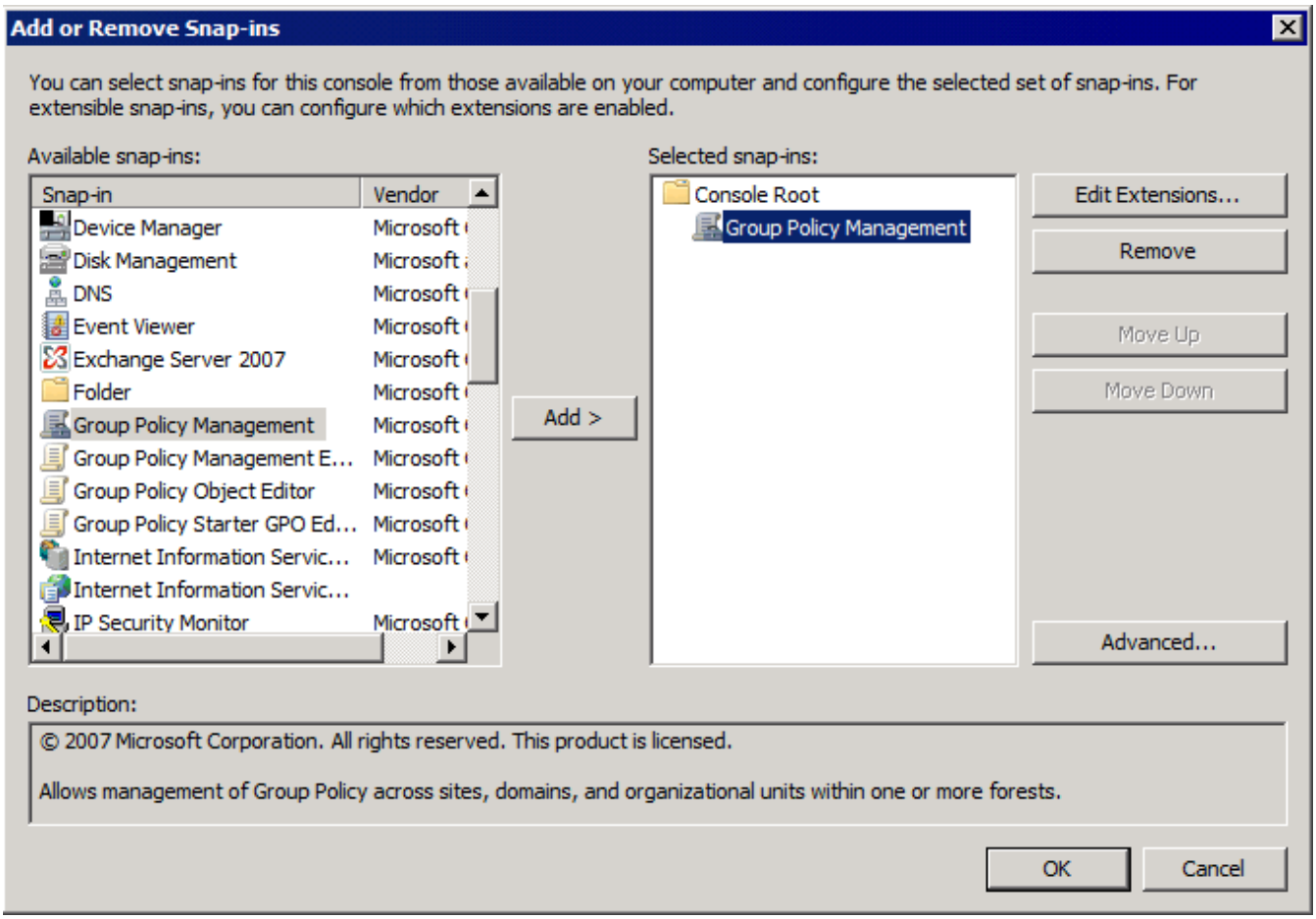
9. Close all open windows.

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

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

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

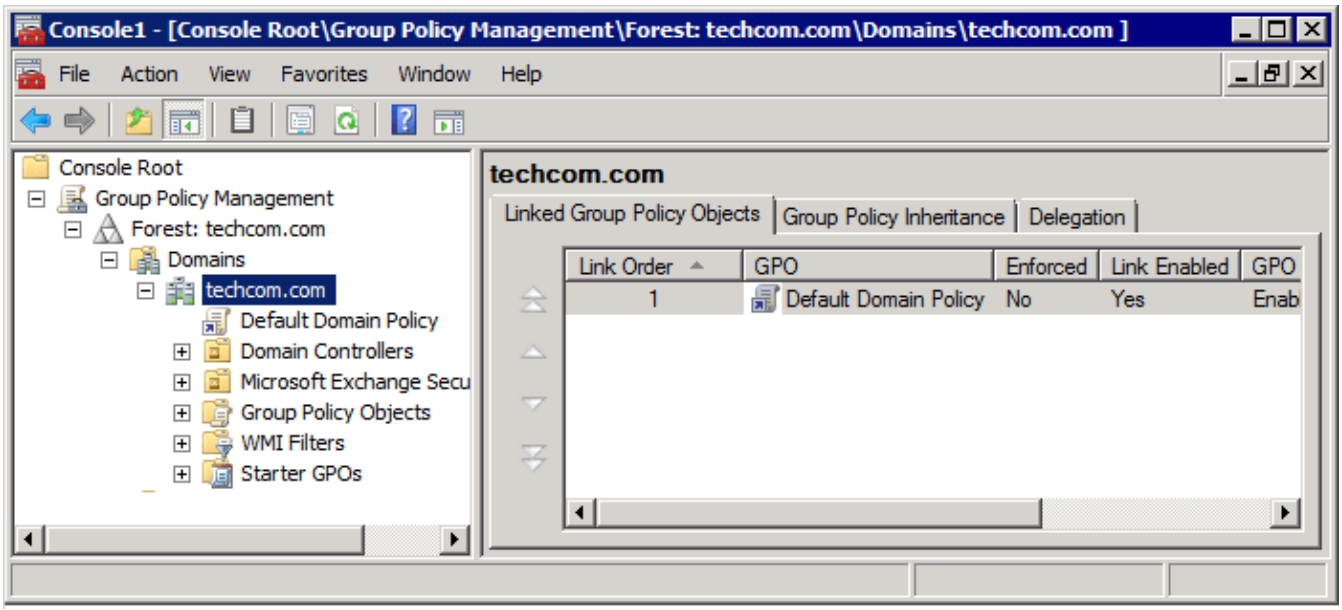
2. In the **Console Root** window, navigate to **File > Add/Remove Snap-in…** to open the **Add or Remove Snap-ins** window.



Screenshot 77: Add/Remove Snap-ins window

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

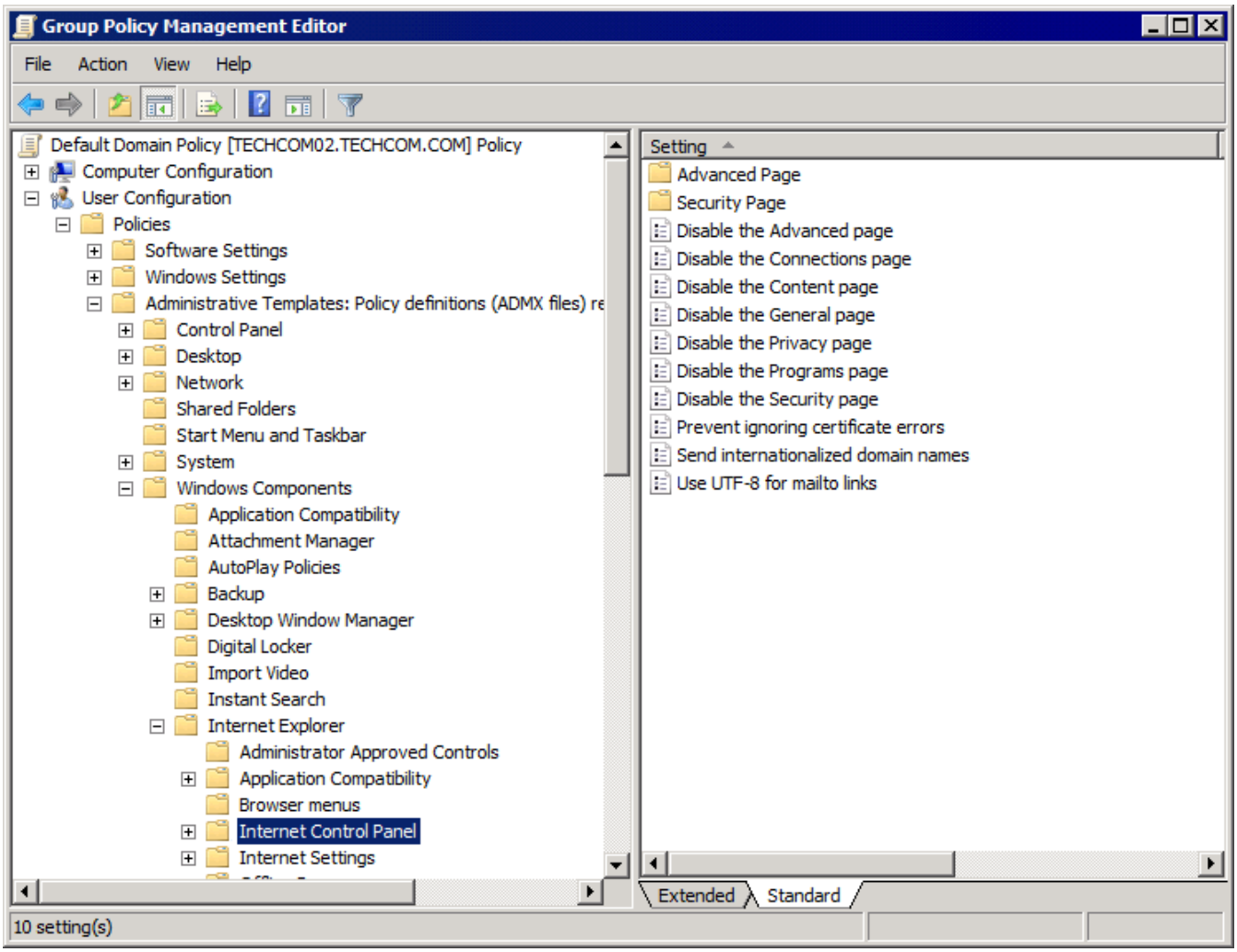
4. Click **OK**.



Screenshot 78: Console Root domain window

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

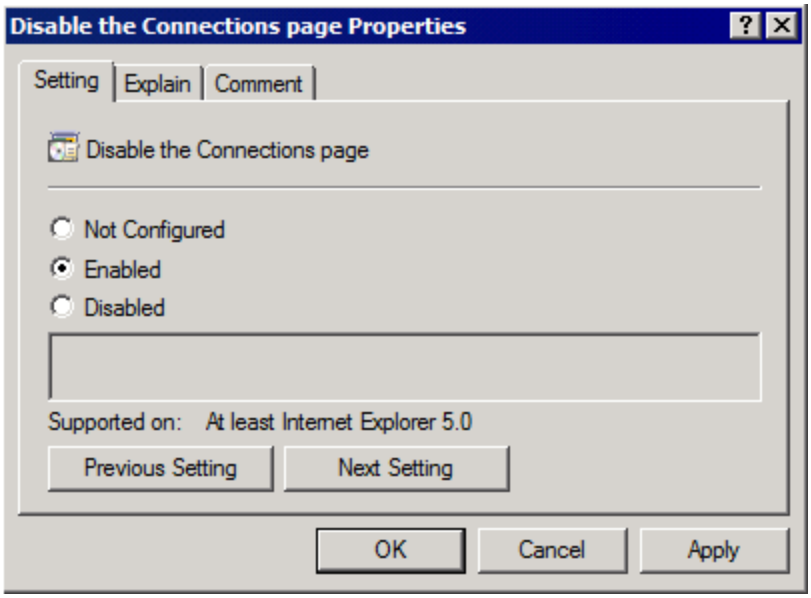
6. Right-click **Default Domain Policy** and click **Edit** to open the **Group Policy Management Editor**.



Screenshot 79: Group Policy Management Editor window

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

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



Screenshot 80: Disable the Connection page Properties dialog

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

NOTE

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

10. Click **Apply** and **OK**.

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

10.4 Uninstall Information

To uninstall GFI WebMonitor:

1. Click **Start > Control Panel > Programs > Programs and Features**.

2. Select GFI WebMonitor from the list, and click **Uninstall**.

3. When **Are you sure you want to ununstall GFI WebMonitor 2012?** appears, click Yes.

4. On completion, click **Finish**.

11 Index

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

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

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

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.com

EUROPE, MIDDLE EAST AND AFRICA

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

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

GFI®