



GFI Product Manual

GFI WebMonitor™

Administrator Guide



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or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors.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

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

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

GFI WebMonitor is copyright of GFI SOFTWARE Ltd. - 1999-2013 GFI Software Ltd All rights reserved.

Document Version: 2.1.0

Last updated (month/day/year): 11/11/2013

Contents

1 Introduction	5
1.1 About this guide	5
1.2 About GFI WebMonitor	5
1.3 How Does GFI WebMonitor Work?	6
1.4 GFI WebMonitor services	8
2 Installing GFI WebMonitor	10
2.1 System requirements	10
2.2 Deployment scenarios	12
2.3 Installing GFI WebMonitor in Gateway Mode	19
2.4 Configuring Routing and Remote Access	21
2.5 Installing GFI WebMonitor in Simple Proxy Mode	22
2.6 Disabling Internet Connection Settings On Client Machines	26
2.7 Uninstall Information	27
3 Post Installation actions	28
3.1 Launching GFI WebMonitor	28
3.2 Enter a valid license key	28
3.3 Configure Proxy settings	29
3.4 Using the Settings Importer Tool	32
4 Achieving results	35
4.1 Achieving results with GFI WebMonitor - Protecting your network	35
4.2 Achieving results with GFI WebMonitor - Maximize bandwidth availability	36
4.3 Achieving results with GFI WebMonitor - Increase productivity	37
5 Using the Dashboard	39
5.1 Overview of Internet Activity	39
5.2 Monitoring Bandwidth	44
5.3 Monitoring Activity	46
5.4 Monitoring Security	48
5.5 Monitoring Real-Time Traffic	50
5.6 Using Quarantine	51
5.7 Using the Quotas Dashboard	52
5.8 Monitoring Agents	53
6 Reporting	55
6.1 Starred reports	55
6.2 Activity reports	55
6.3 Bandwidth reports	57
6.4 Security reports	59
7 Configuring GFI WebMonitor	62
7.1 General settings	63
7.2 Configuring Web Activity Logging	68

7.3 Configuring Policies	74
7.4 Configuring the GFI WebMonitor Agent	98
7.5 Downloading the GFI WebMonitor Agent	98
7.6 Installing the WebMonitor Agent Manually	100
7.7 Installing the GFI WebMonitor Agent via GPO in Windows Server 2008	101
7.8 Configuring Alerts	105
7.9 Proxy Settings	110
7.10 Network Access Policy Configuration	113
8 Troubleshooting and support	124
8.1 Introduction	124
8.2 GFI SkyNet	124
8.3 Web Forum	124
8.4 Request Technical Support	124
8.5 Documentation	124
8.6 Common issues	124
9 Glossary	127
10 Index	133

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:

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

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

1.2 About GFI WebMonitor

GFI WebMonitor is available in three editions:

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

1.3 How Does GFI WebMonitor Work?

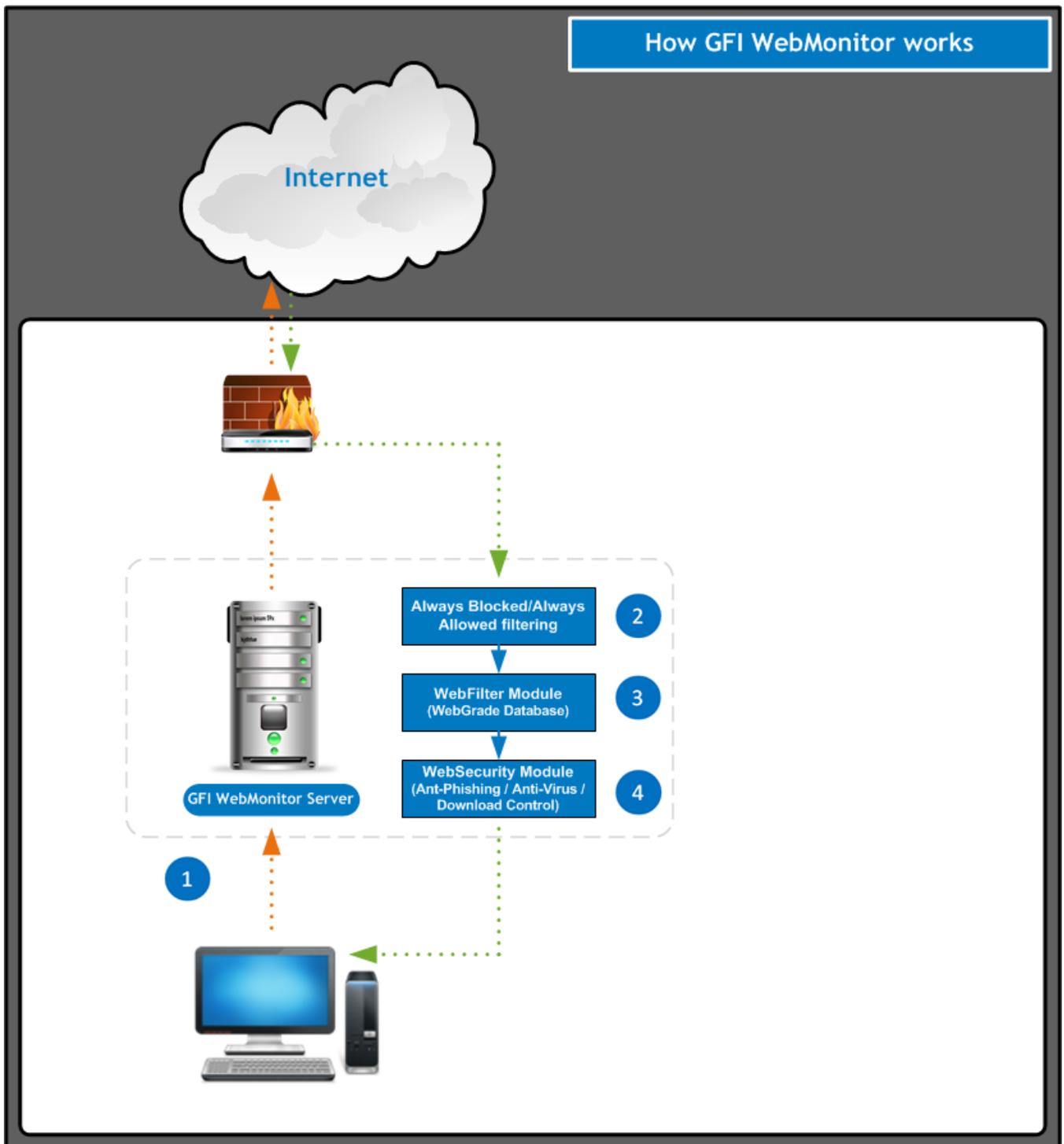


Figure 1: How Does GFI WebMonitor Work?

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:

ACTION	DESCRIPTION
Blocks web traffic requests	<ul style="list-style-type: none"> » 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	<ul style="list-style-type: none"> » by allowed users and/or IP addresses, or » to access allowed URLs
Forwards web traffic requests (to the WebFiltering module)	<ul style="list-style-type: none"> » 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.

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 85).



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

The upgrade procedure is similar to the installation procedure. For more information, refer to [Installing GFI WebMonitor](#) (page 10). Before upgrading, ensure you have the latest version of GFI WebMonitor. This can be downloaded from http://go.gfi.com/?pageid=WebMon_Download.



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.

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
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: <ul style="list-style-type: none"> » 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

SERVICE NAME	DESCRIPTION	LOCATION AND NAME	USER CREDENTIALS
GFI WebMonitor Core Service	<p>The GFI WebMonitor Core Service is composed by the following different components:</p> <ul style="list-style-type: none"> » 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 is 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`”
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.

- » [System requirements for Simple Proxy / Gateway mode](#)
- » [Gateway mode pre-requisites](#)
- » [Simple Proxy mode pre-requisites](#)
- » [Deployment scenarios](#)
- » [Installing GFI WebMonitor in Gateway mode](#)
- » [Installing GFI WebMonitor in Simple Proxy mode](#)

2.1 System requirements

2.1.1 Software

TYPE	SOFTWARE REQUIREMENTS (x86 and x64)
Supported Operating Systems	<ul style="list-style-type: none">» Windows® Server 2003 SP 2» Windows® Server 2008» Windows® Server 2008 R2» Windows Small Business Server 2003 R2» Windows Small Business Server 2008» Windows Small Business Server 2011» Windows® XP SP3» Windows® Vista SP2» Windows® 7» Windows® 8
Gateway and Simple Proxy Environments - Other required components	<ul style="list-style-type: none">» Internet Explorer® 8 or later» Microsoft.NET® Framework 4.0» Microsoft® Message Queuing Service (MSMQ)» IIS® Express» SQL Server® Express 2005 or later» SQL Server® 2005 or later (for reporting purposes)
Gateway Environment - Other required components	<ul style="list-style-type: none">» Routing and Remote Access configuration on Windows® Server 2003/2008
GFI WebMonitor Agent	<ul style="list-style-type: none">» Windows® Vista SP2 or later



NOTE

The installation wizard checks that Microsoft .NET® 4.0, MSMQ, Report Viewer, Windows® Image Component, .net Hotfix, Microsoft® Visual C++ Redistributable and IIS® Express are installed. If not installed the wizard will guide you through the installation automatically.

2.1.2 Hardware

Minimum hardware requirements depend on the GFI WebMonitor edition.

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



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 Listening ports

PRODUCT	PORT
GFI WebMonitor Gateway, Simply Proxy and ISA/TMG Mode	Listening Port (Default 8080)
GFI WebMonitor Agent	Listening Port (Default 5995) - this port will accept transfer of data from the agent to the server

2.1.4 Gateway mode pre-requisites

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

1. Client machines are configured to use the server as the default Internet gateway.
2. The server's network cards are connected:
 - » one to the internal network (LAN)
 - » one to the external network (WAN)
3. Start Routing and Remote Access service if installing GFI WebMonitor on Windows® Server 2003 or Windows® Server 2008. For more information, refer to [Configuring Routing and Remote Access](#) (page 21).



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

2.1.5 Simple Proxy Mode Pre-requisites

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

- » Block all outgoing HTTP/HTTPS traffic generated from the client machines
- » Allow outgoing HTTP/HTTPS traffic generated by GFI WebMonitor only
- » Allow Non-HTTP/HTTPS traffic generated from client machines.

In this environment, traffic forwarding can be used to forward HTTP/HTTPS traffic from the client machines to GFI WebMonitor machine.



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.

Choosing your environment			
	Internet facing Router supporting port blocking / traffic forwarding	Server configured as an Internet gateway	Microsoft ISA Server / Forefront TMG
GFI WebMonitor Simple Proxy Mode	✓		
GFI WebMonitor Gateway Mode		✓	
GFI WebMonitor ISA / TMG Mode			✓

Figure 2: Choosing your environment

2.2.1 Deployment in an Internet Gateway environment

Install GFI WebMonitor in gateway mode when you have:

- » A server configured with 2 network cards
- » Users are using this server as an Internet gateway to access the Internet
- » GFI WebMonitor is installed on this server
- » All inbound and outbound traffic passes through this server.

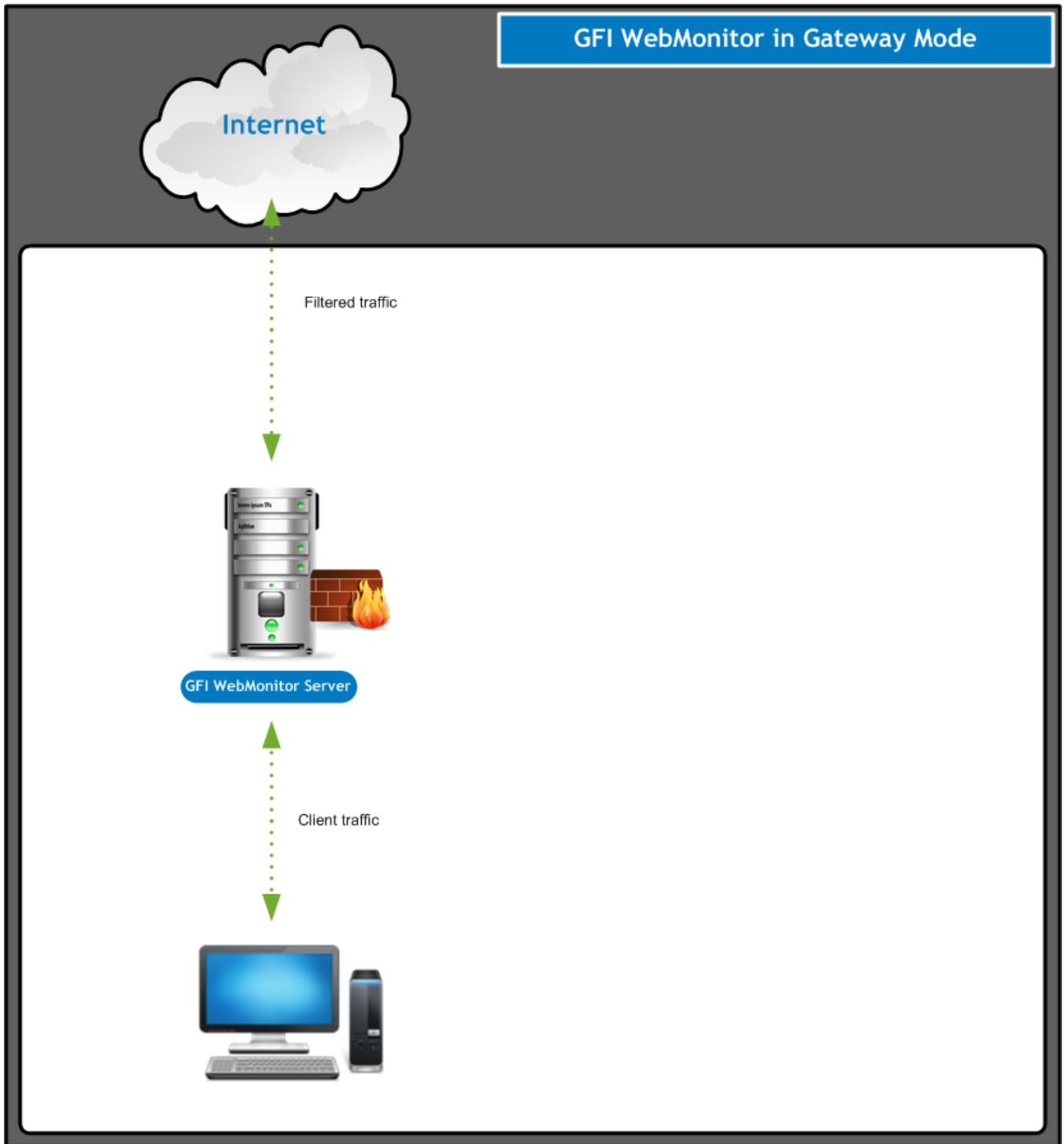


Figure 3: GFI WebMonitor installed on a gateway machine

To install GFI WebMonitor on an Internet gateway, refer to [Installing in Gateway Mode](#).

2.2.2 Deployment in a Simple Proxy environment

Install GFI WebMonitor in Simple Proxy mode when:

- » Users are using a router to connect to the Internet
- » GFI WebMonitor is installed within the local LAN.

The router must be configured to block all traffic except traffic generated by GFI WebMonitor. This can be achieved by using one of the following methods:

OPTION	DESCRIPTION
Port Blocking	Blocking client requests and allowing GFI WebMonitor traffic.
Traffic Forwarding	Forwarding all traffic from the client to GFI WebMonitor machine.

Port blocking

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



NOTE

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

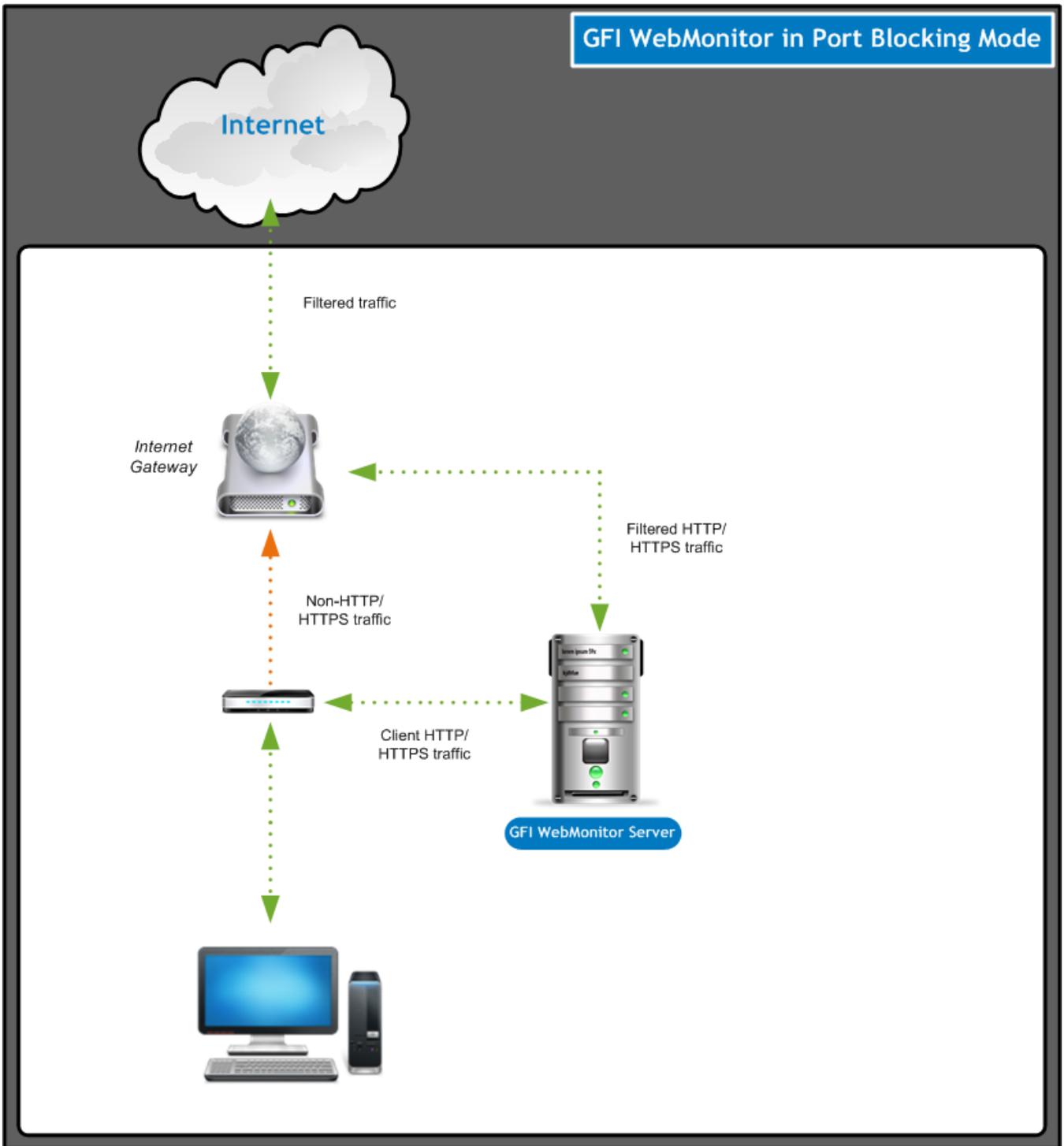


Figure 4: GFI WebMonitor installed on a proxy machine connected to a router supporting port blocking

2.2.3 Traffic forwarding

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

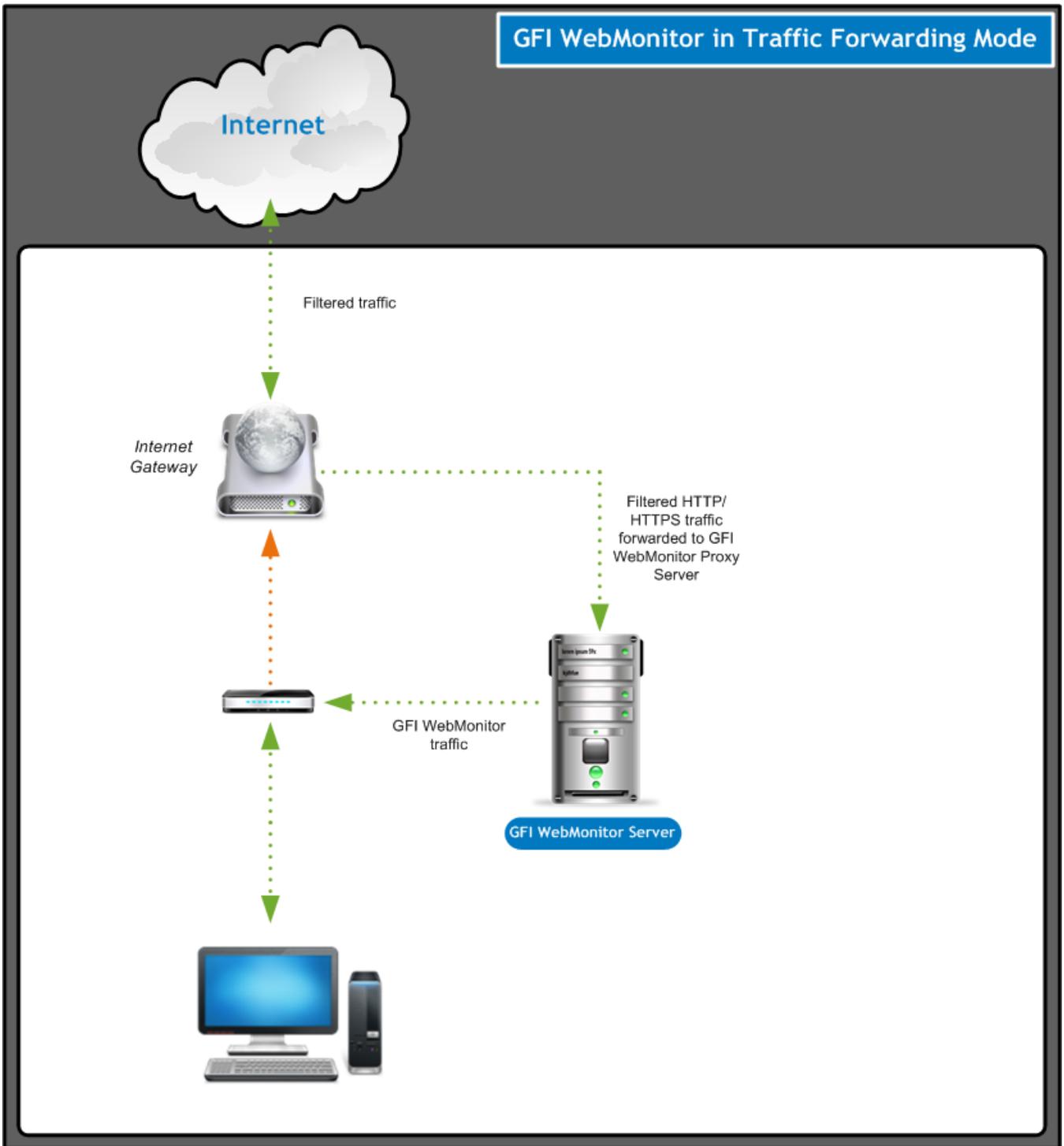


Figure 5: GFI WebMonitor installed on a proxy machine connected to a router supporting traffic forwarding

To install GFI WebMonitor on a proxy server, refer to [Installing in Simple Proxy Mode](#).

2.2.4 Assigning log on as a service rights

The GFI WebMonitor service needs to run with administrative privileges. The username and password provided for the GFI WebMonitor service must have **Logon as a service rights**.

Log on as a service rights allow a user 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**.
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**.
3. Select **Group Policy** tab in the **Domain Properties** dialog.
4. Select **Default Domain Policy** from the list and click **Edit**
5. Expand **Computer Configuration > Windows Settings > Security Settings > Local Policies** and click **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.
3. Select **Group Policy Management** from the **Available snap-ins list**, and click **Add**.
4. Click **OK**.
5. Expand **Group Policy Management > Forest > Domains and <domain>**.
6. Right-click **Default Domain Policy** and click **Edit** to open the **Group Policy Management Editor**.
7. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies** and click **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.

2.3 Installing GFI WebMonitor in Gateway Mode

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



NOTE

Enter only users who need access to configure GFI WebMonitor. Do not enter IPs of normal users who will be proxied through GFI WebMonitor. More than one user or machine can be specified by separating entries with semicolons ‘;’

6. In the **Service Logon Information** window, key in the logon credentials of an account with administrative privileges and click **Next**.

i NOTE

The user account must have **Log on as a service** rights; otherwise, rights are automatically assigned. For more information, refer to [Assigning log on as a service rights](#) (page 17).

7. [Optional] Provide SMTP mail server details and an email address to which administrator notifications will be sent. Click **Verify Mail Settings** to send a test email. Click **Next**.

i NOTE

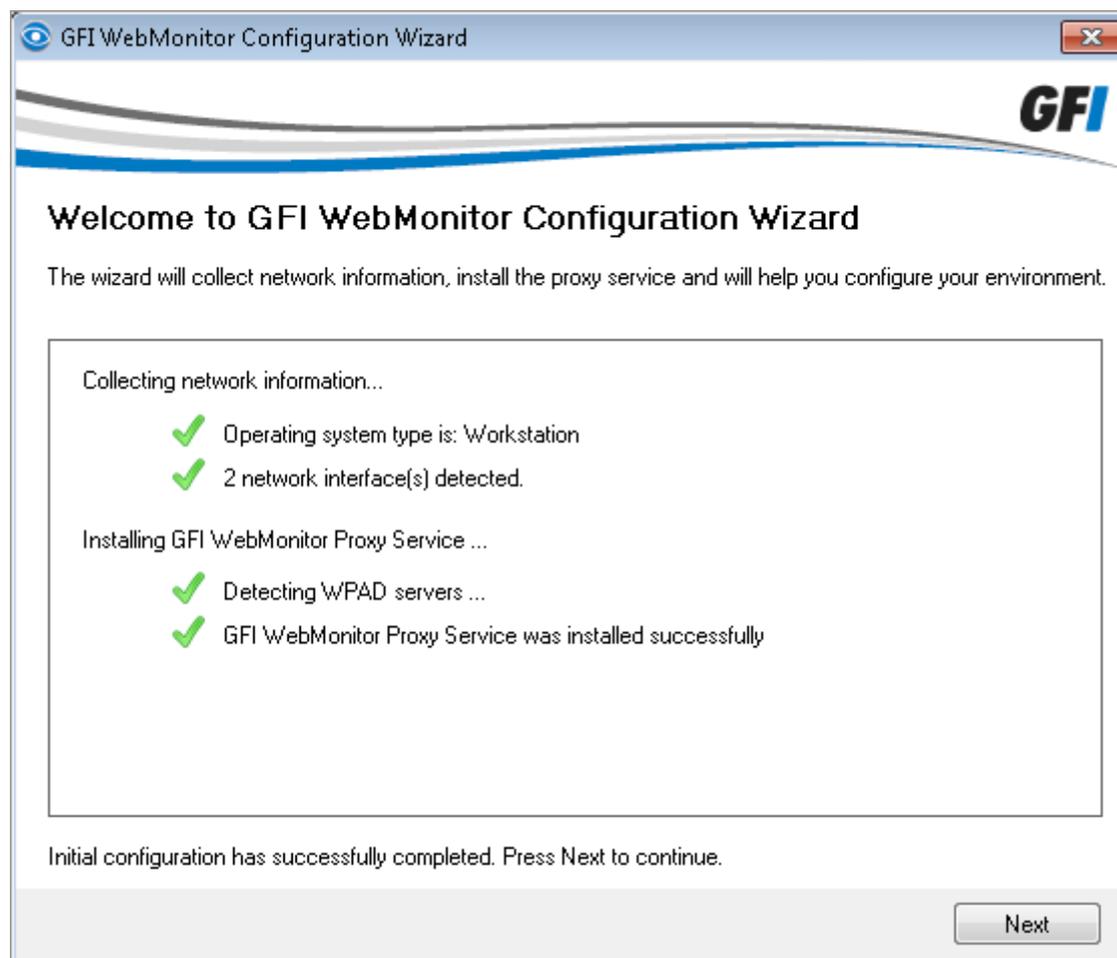
You can choose to leave SMTP settings empty and set them later, but you will not be able to receive notifications until you set them.

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.

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

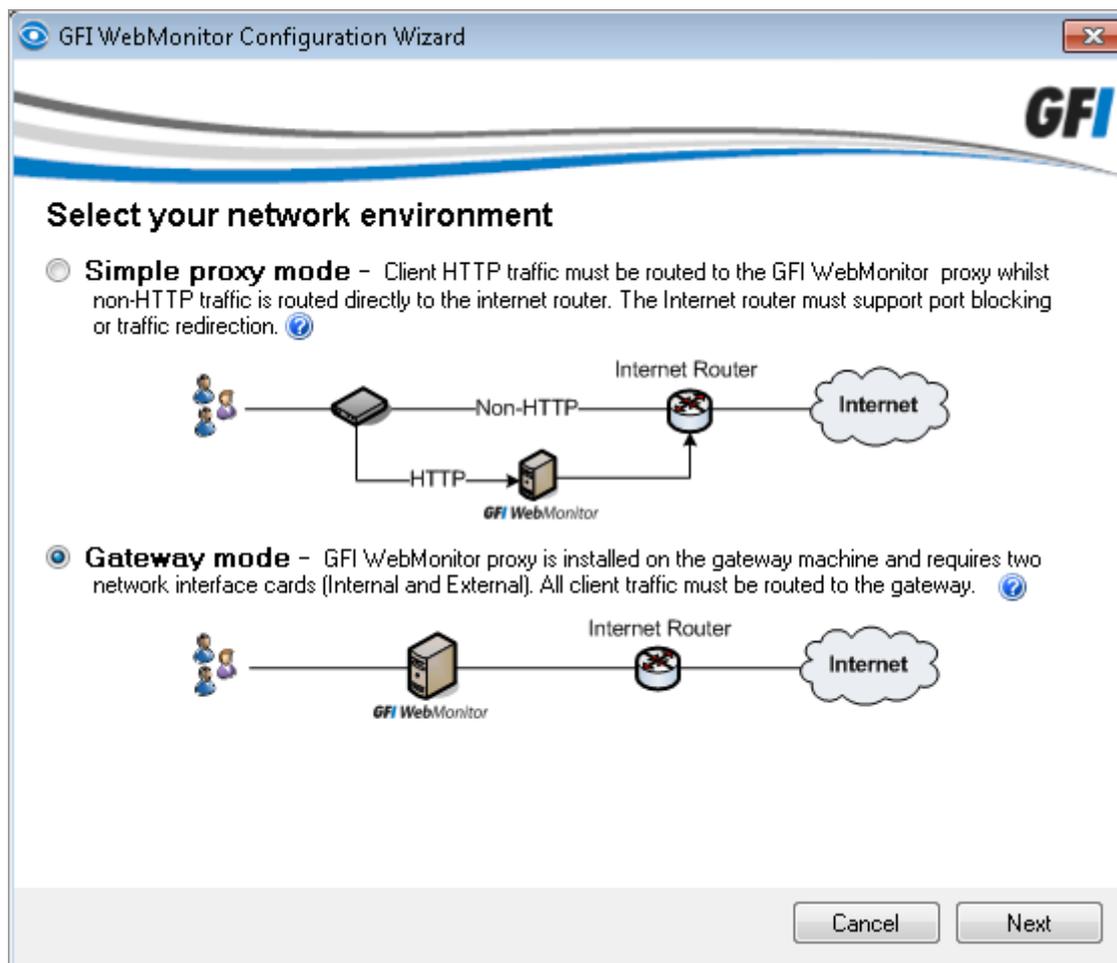


Screenshot 1: GFI WebMonitor Configuration Wizard welcome screen

i NOTE

The GFI WebMonitor Configuration Wizard can be launched manually from C:\Program Files\GFI\WebMonitor and selecting GatewayWiz.exe.

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



Screenshot 2: GFI WebMonitor Configuration Wizard - Gateway mode

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

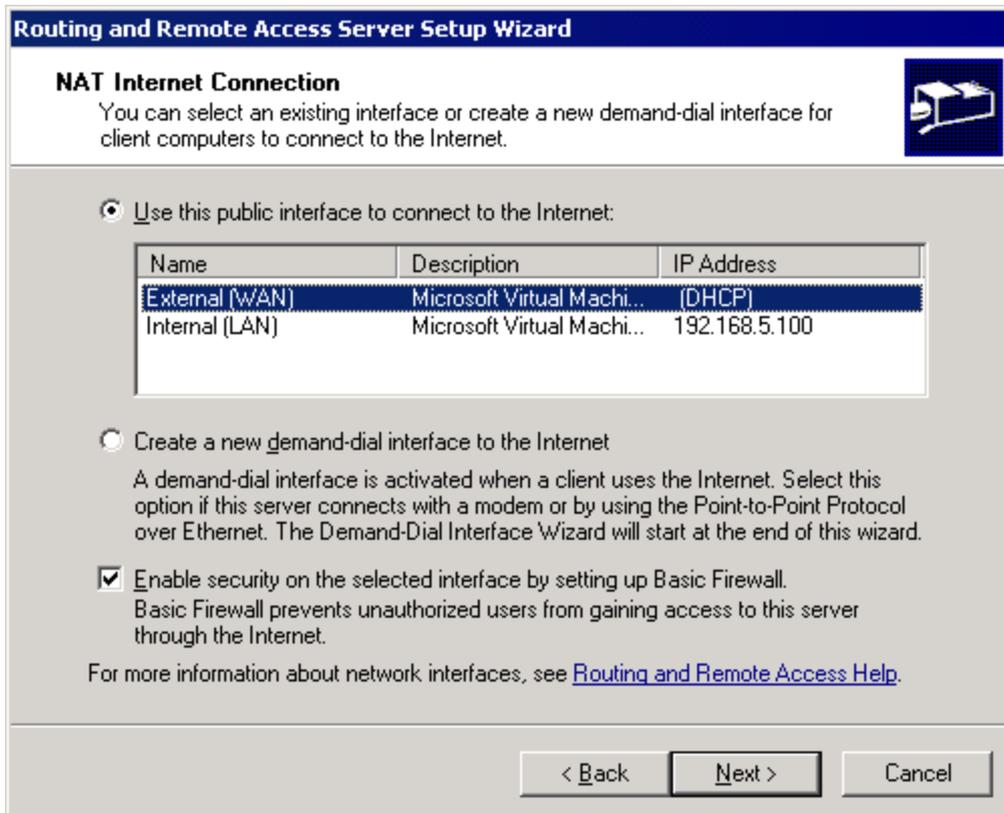
14. In the **Current Gateway Configuration** screen, select the internal network card and click **Next**.

15. Click **Finish** to apply settings.

2.4 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 3: 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.**

2.5 Installing GFI WebMonitor in Simple Proxy Mode

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

 **NOTE**

Enter only users who need access to configure GFI WebMonitor. Do not enter IPs of normal users who will be proxied through GFI WebMonitor. More than one user or machine can be specified by separating entries with semicolons ‘;’

6. In the Service Logon Information window, 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 17).

7. [Optional] Provide SMTP mail server details and an email address to which administrator notifications will be sent. Click **Verify Mail Settings** to send a test email. Click **Next**.

 **NOTE**

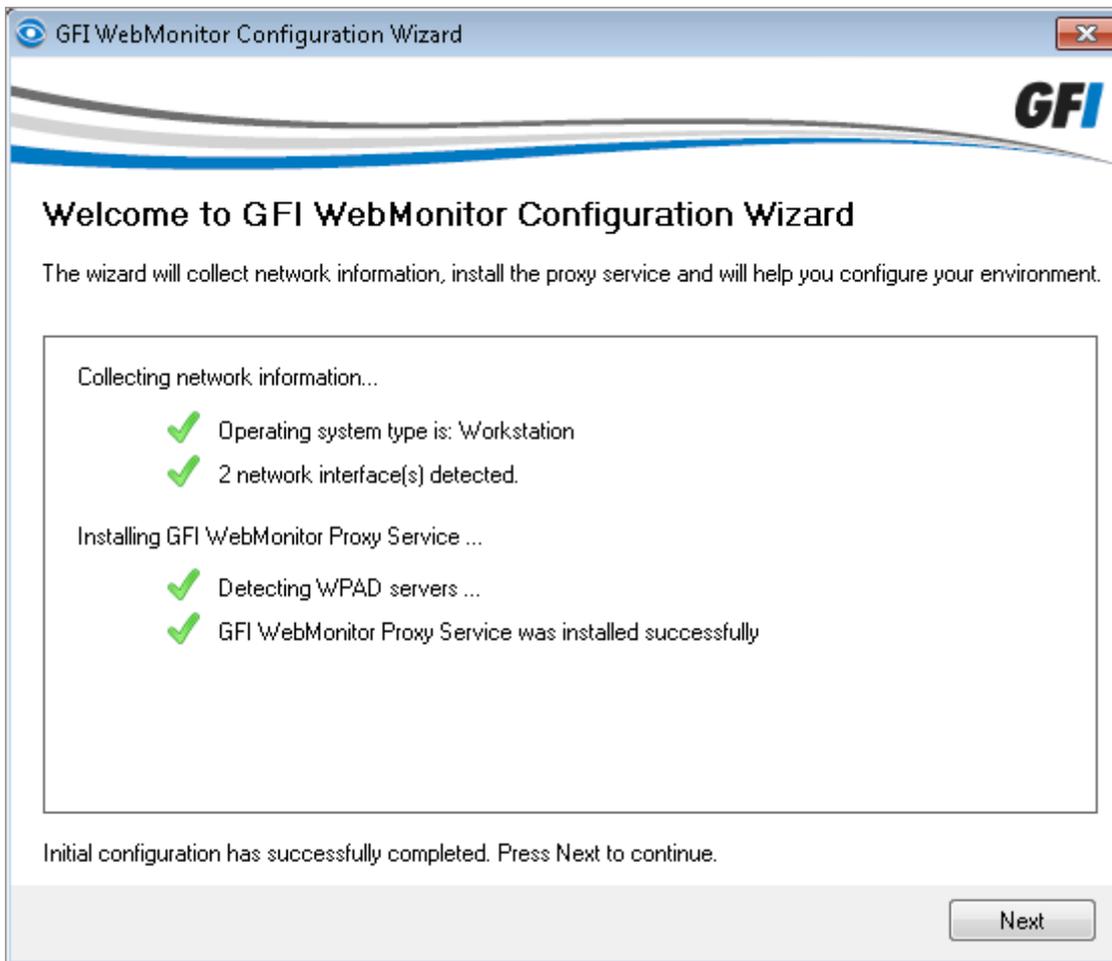
You can choose to leave SMTP settings empty and set them later, but you will not be able to receive notifications until you set them.

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.

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



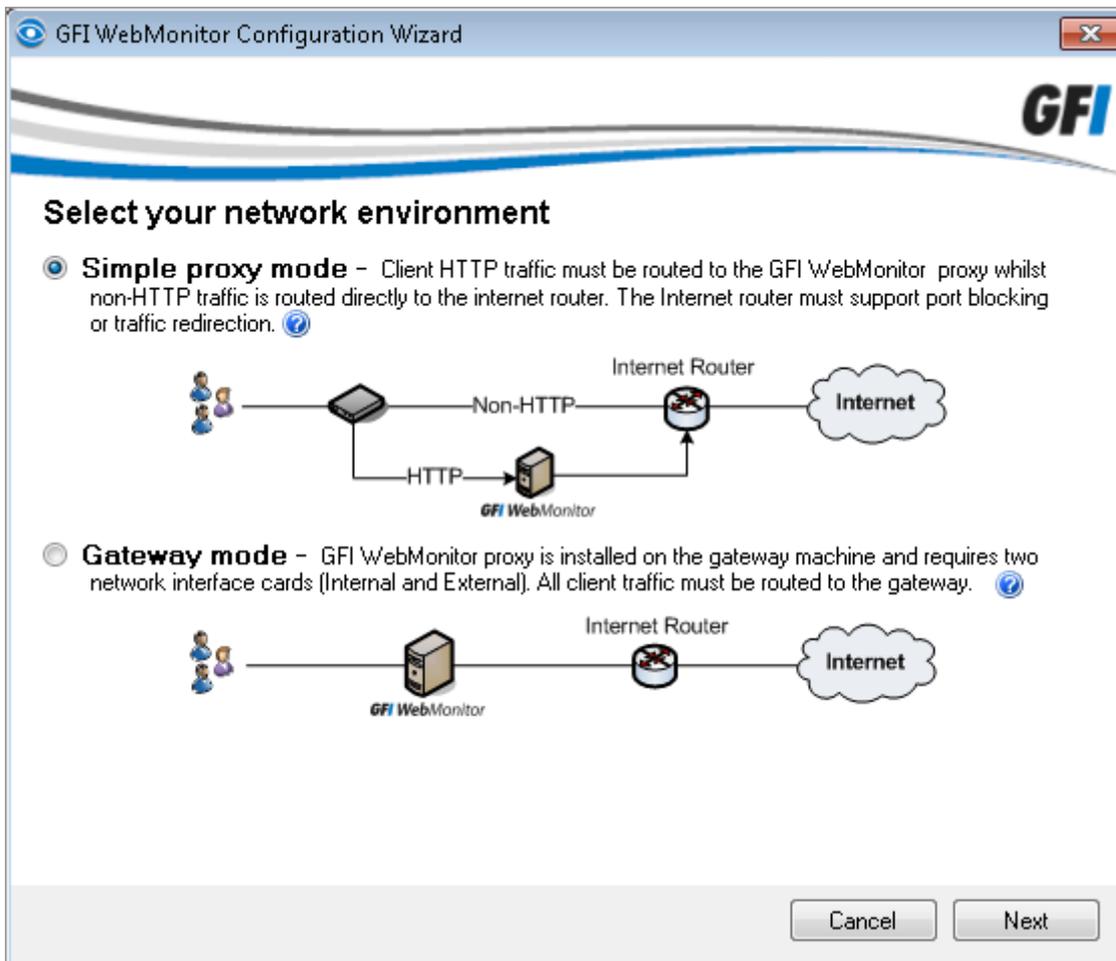
Screenshot 4: GFI WebMonitor Configuration Wizard welcome screen



NOTE

The GFI WebMonitor Configuration Wizard can be launched manually from `C:\Program Files\GFI\WebMonitor` and selecting `GatewayWiz.exe`.

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



Screenshot 5: GFI WebMonitor Configuration Wizard - Simple proxy mode

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

i NOTE

To view help on how to configure most commonly used routers, select the [Click here](#) link. For more information, refer to [Simple Proxy Mode Pre-requisites](#) (page 12).

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

2.5.1 Configuring commonly used routers

When installing GFI WebMonitor in Simple Proxy mode, ensure that your router is configured to support port blocking or traffic forwarding. For most routers this is done by creating firewall access/filtering rules to allow HTTP traffic originating from GFI WebMonitor Proxy machine and block all outgoing HTTP traffic.

Refer to the following articles for information on how to configure the most commonly used routers:

- » [Cisco ADSL Router Cisco 878 \(MPC8272\)](#)
- » [DrayTek VIGOR 2820N ADSL2](#)
- » [Linksys WRT54GL Wireless Router](#)
- » [Netgear Wireless Router DG834GT](#)

- » [SonicWall NSA 2400](#)
- » [SonicWall TZ 180](#)
- » [Thomson Wireless Broadband Router TG585 v7](#)

2.6 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 the Internet connections page using GPO in Microsoft Windows Server 2003](#)
- » [Disabling the Internet connections page using GPO in Microsoft Windows Server 2008](#)

2.6.1 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**.
3. Select **Group Policy** tab in the **Domain Properties** dialog.
4. Select **Default Domain Policy** from the list and click **Edit**.
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**.
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.

2.6.2 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.
3. Select **Group Policy Management** from the **Available snap-ins** list, and click **Add**.
4. Click **OK**.
5. Expand **Group Policy Management > Forest > Domains** and **<domain>**.
6. Right-click **Default Domain Policy** and click **Edit** to open the **Group Policy Management Editor**.
7. Expand **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**.

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.

2.7 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 uninstall GFI WebMonitor?** appears, click **Yes**.
4. On completion, click **Finish**.

3 Post Installation actions

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

- » [Launching GFI WebMonitor](#)
- » [Entering a license key](#)
- » [Configuring Proxy settings](#)
- » [Configuring Internet Browsers to use a Proxy Server](#)
- » [Using the Settings Importer Tool](#)

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://1.1.1.1> 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](#) (page 31).

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://1.1.1.1> 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 29).

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, you are notified that 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. To manually update the license key after evaluating the product, refer to [Licensing information](#).

To enter your license key:

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



NOTE

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

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.

3.3.1 Configuring GFI WebMonitor machine as the Default Proxy using GPO in Windows® Server 2003

To configure all client machines to use GFI WebMonitor as a proxy server through Windows® Server 2003 GPO:

1. On the Domain Controller, go to **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
2. Under the domain node, right-click the organizational unit where you wish to apply the group policy and click **Properties**.



NOTE

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

3. In the **Domain Properties** dialog, select **Group Policy** tab.
4. Select **Default Domain Policy** from the list and click **Edit**.
5. Expand **User Configuration > Windows Settings > Internet Explorer Maintenance > Connection** and double-click **Proxy Settings** to open the **Proxy Settings** dialog.
6. Check **Enable proxy settings** checkbox.
7. Uncheck **Use the same proxy server for all addresses** checkbox.
8. In the **HTTP** and **FTP** text boxes key in the proxy server IP address and the port used (Default 8080).
9. Click **OK** to apply changes.
10. Close all open windows.

3.3.2 Configuring GFI WebMonitor machine as the Default Proxy using GPO in Windows® Server 2008

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

1. In command prompt, key in `mmc.exe` and press **Enter**.
2. In the **Console Root** window, navigate to **File > Add/Remove Snap-in...** to open the **Add or Remove Snap-ins** window.
3. Select **Group Policy Management** from the **Available snap-ins** list, and click **Add**.
4. Click **OK**.
5. Expand **Group Policy Management > Forest > Domains and <domain>**, then select the organizational unit where you wish to apply the group policy.



NOTE

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

6. Right-click **Default Domain Policy** and click **Edit** to open the **Group Policy Management Editor**.
7. Expand **User Configuration > Policies > Windows Settings > Internet Explorer Maintenance > Connection** and double-click **Proxy Settings** to open the **Proxy Settings** dialog.
8. Check **Enable proxy settings** checkbox.
9. Uncheck **Use the same proxy server for all addresses** checkbox.
10. In the **HTTP** and **FTP** text boxes key in the proxy server IP address and the port used (Default 8080).
11. Click **OK** to apply changes
12. Close **Proxy Settings** dialog.
13. Close **Group Policy Management Editor** dialog and save the management console.



IMPORTANT

When using Active Directory, the administrator can disable the Internet connection settings tab from the client machines. For more information, refer to [Disabling Internet Connection Settings On Client Machines](#) (page 26).

3.3.3 Configuring Internet Browsers to use a Proxy Server

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

- » [Microsoft Internet Explorer](#)
- » [Mozilla Firefox](#)
- » [Google Chrome](#)

3.3.4 Configure Microsoft Internet Explorer to use a Proxy Server

You can manually configure each individual user machine to set the GFI WebMonitor machine as the default proxy. To configure proxy settings in Microsoft Internet Explorer:

1. Launch **Microsoft Internet Explorer**.
2. From the **Tools** menu, choose **Internet Options** and select the **Connections** tab.
3. Click **LAN settings** button.
4. Check **Use a proxy server for your LAN** checkbox.
5. In the **Address** and **Port** text boxes, key in the proxy server name or IP address of the GFI WebMonitor machine and the port used (Default 8080) .
6. Click **OK** to close **LAN Settings** dialog.
7. Click **OK** to close **Internet Options** dialog.



NOTE

If WPAD is enabled in GFI WebMonitor, select **Auto-detect proxy settings for this network**. For more information, refer to [Configuring WPAD](#) (page 111).

3.3.5 Configuring Firefox to use a Proxy Server

You can manually configure each individual user machine to set the GFI WebMonitor machine as the default proxy. To configure proxy settings in Mozilla Firefox:

1. Launch **Mozilla Firefox**.
2. Click **Firefox > Options > Options > Advanced tab > Network** tab.
3. Click **Settings** button to open the **Connection Settings** dialog.
4. Select **Manual proxy configuration**.
5. Uncheck **Use this proxy server for all protocols** checkbox.
6. In the **HTTP Proxy**, **FTP Proxy** and related **Port** text boxes, key in the proxy server IP address and the port used (Default 8080).
7. Click **OK** to close **Connection Settings** dialog.
8. Click **OK** to close **Options** dialog.



NOTE

If WPAD is enabled in GFI WebMonitor, select **Auto-detect proxy settings for this network**. For more information, refer to [Configuring WPAD](#) (page 111).

3.3.6 Configure Google Chrome to Use a Proxy Server

You can manually configure each individual user machine to set the GFI WebMonitor machine as the default proxy. To configure proxy settings in Google Chrome:

1. Launch **Google Chrome**.
2. Click  and select **Options**.

3. In **Options** dialog, click **Under the Hood** tab.
4. Click **Change proxy settings** button to open **Internet Properties** dialog.
5. Select **Connections** tab.
6. Click **LAN settings** button.
7. Check **Use a proxy server for your LAN** checkbox.
8. In the **Address** and **Port** text boxes, key in the proxy server name or IP address and the port used (Default 8080).
9. Click **OK** to close **LAN Settings** dialog.
10. Click **OK** to close **Internet Options** dialog.



NOTE

If WPAD is enabled in GFI WebMonitor, select **Auto-detect proxy settings for this network**. For more information, refer to [Configuring WPAD](#) (page 111).

3.4 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.

3.4.1 Exporting / Importing Configuration Settings

To use the Settings Importer Tool:

1. On the machine where GFI WebMonitor is installed, go to **Start > Run** and type `cmd`. This action calls the Microsoft Windows command line interface.
2. To list all the controls that can be used to operate the Settings Importer Tool, type:
 - `WebMon.SettingsImporterTool --help - for Windows 32-bit`
 - `WebMon.SettingsImporterTool --help - For Windows 64-bit`

```

Administrator: C:\Windows\system32\cmd.exe
C:\Program Files\GFI\WebMonitor>WebMon.SettingsImporterTool -help
Usage: WebMon.SettingsImporterTool [-e --path=VALUE] [-i --path=VALUE [--reports
--authorization .. --all]]
Options:
-e, --export           Export settings (all).
-i, --import           Import settings (all - specific settings can be
                       imported via options).
                       --path=VALUE       The path to the settings file.
-R, --reports          Import all report settings.
-a, --authorization   Import authorization rules.
-u, --autoupdate       Import auto update settings.
-d, --database         Import database settings.
-n, --notifications   Import notifications settings.
-o, --options          Import general options.
-w, --webcategorization Import web categorization settings.
-G, --allgeneral       Import all general settings.
-f, --webfiltering     Import web filtering policies.
-b, --webbrowsing      Import web browsing policies.
-m, --instantmessaging Import instant messaging & social control
                       policies.
-s, --streamingmedia   Import streaming media policies.
-g, --searchengine     Import search engine policies.
-v, --virusscanning    Import virus scanning policies.
-y, --securityengines  Import security engines settings.
-l, --downloadcontrol  Import download control policies.
-x, --alwaysblocked    Import always blocked settings.
-j, --alwaysallowed    Import always allowed settings.
-P, --allpolicy        Import all policy settings.
-L, --allalerts        Import all alert settings.
-q, --proxygeneral     Import proxy general settings.
-h, --proxyhttps       Import proxy https settings.
-z, --proxycache       Import proxy cache settings.
-X, --allproxy         Import all proxy settings.
-S, --allsettings      Import all settings (except reports).
-A, --all              Import all.
C:\Program Files\GFI\WebMonitor>

```

Screenshot 6: 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](#)
-



4. Protect from Malware in HTTPS traffic

- » [Configure HTTPS Proxy Scanning Settings](#)
-

WebSecurity Edition



1. Block Known Malicious Websites and Phishing.

- » [Configure ThreatTrack](#)
 - » [Configure Auto-update of all security engines](#)
 - » [Configuring Anti-Phishing in Security Policies](#)
 - » [Configure Auto-update of all security engines](#)
-



2. Control and scan your downloads using multiple anti-virus engines.

- » [Configure Downloads Policies](#)
- » [Configuring Security Policies](#)



3. Protect from Malware in HTTPS traffic

- » [Configure HTTPS Proxy Scanning Settings](#)



GFI Software Ltd also recommends creating an awareness policy with safe use guidelines for your employees. For more information refer to: [Acceptable Use Policy Whitepaper](#)

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 WebMonitor on 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 Policies](#)



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 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 Software Ltd also recommends creating an awareness policy with safe use guidelines for your employees. For more information refer to: [Acceptable Use Policy Whitepaper](#)

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 WebMonitor on 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 Policies](#)



3. Block access to streaming applications.

» [Configure Streaming Media Policies](#)



4. Block access to Instant Messaging applications (such as 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 Software Ltd also recommends creating an awareness policy with safe use guidelines for your employees. For more information refer to: [Acceptable Use Policy Whitepaper](#)

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:

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.
Quotas	The Quotas dashboard lists active Web Browsing Quota Policies and their respective status.
Agents	The Agents dashboard provides information related to the status of configured Agents.

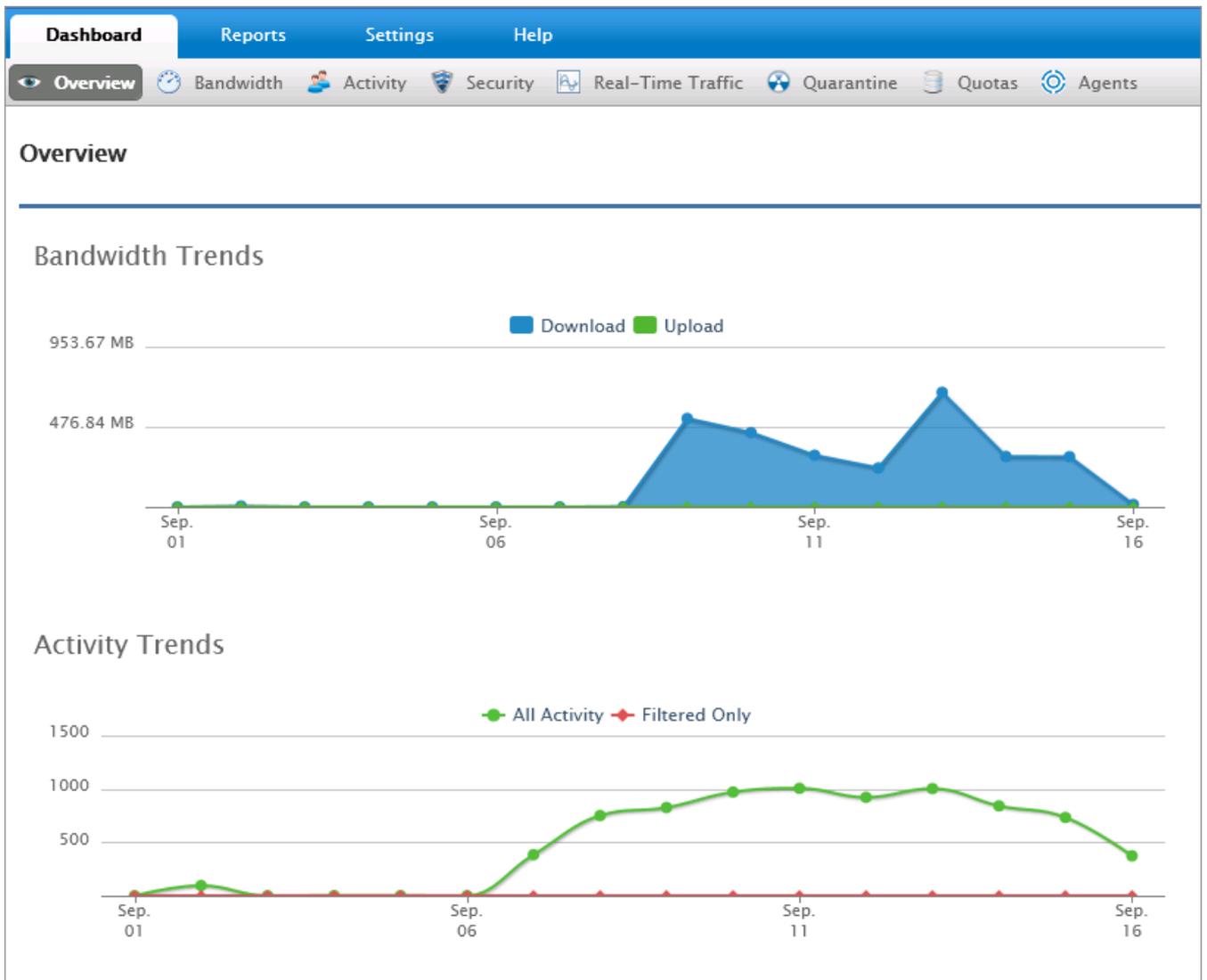


NOTE

If Anonymization is enabled, personal data (such as User Names and IPs) is masked. For more information, refer to [General Options](#) (page 71).

5.1 Overview of Internet Activity

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



Screenshot 7: Dashboard Overview

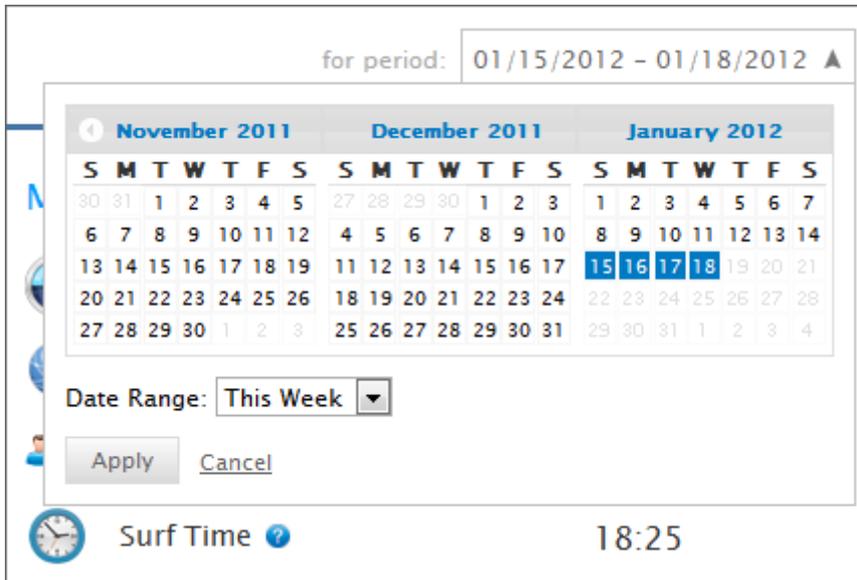
The page contains a graphical representation of Internet usage trends, such as:

- » 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 8: 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 9: 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 73).

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.

Task List

 No browsing detected	Dismiss
 HTTPS Scanning not configured	Dismiss
 Problem occurred during database upgrade	Dismiss
 SQL Server Database is Recommended	Dismiss

Screenshot 10: 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 105).

Monitor Status

	Web Requests Monitored	0
	Websites Visited	0
	Users	0

WebSecurity Status

	Malicious Websites Blocked	0
	Phishing Websites Blocked	0
	Infected Files Detected	0

WebFilter Status

	Blocks	0
	Warnings	0
	Quarantined	0

Screenshot 11: Dashboard Overview statistical information

5.1.4 Product Status

Product Status

	Product Version	GFI WebMonitor 2012 (build 20120713)
	Licensed Module	Web Filtering + Web Security
	Licensed Users	 2 / 3
	Subscription	 9/9/2012

Screenshot 12: Dashboard Overview product status

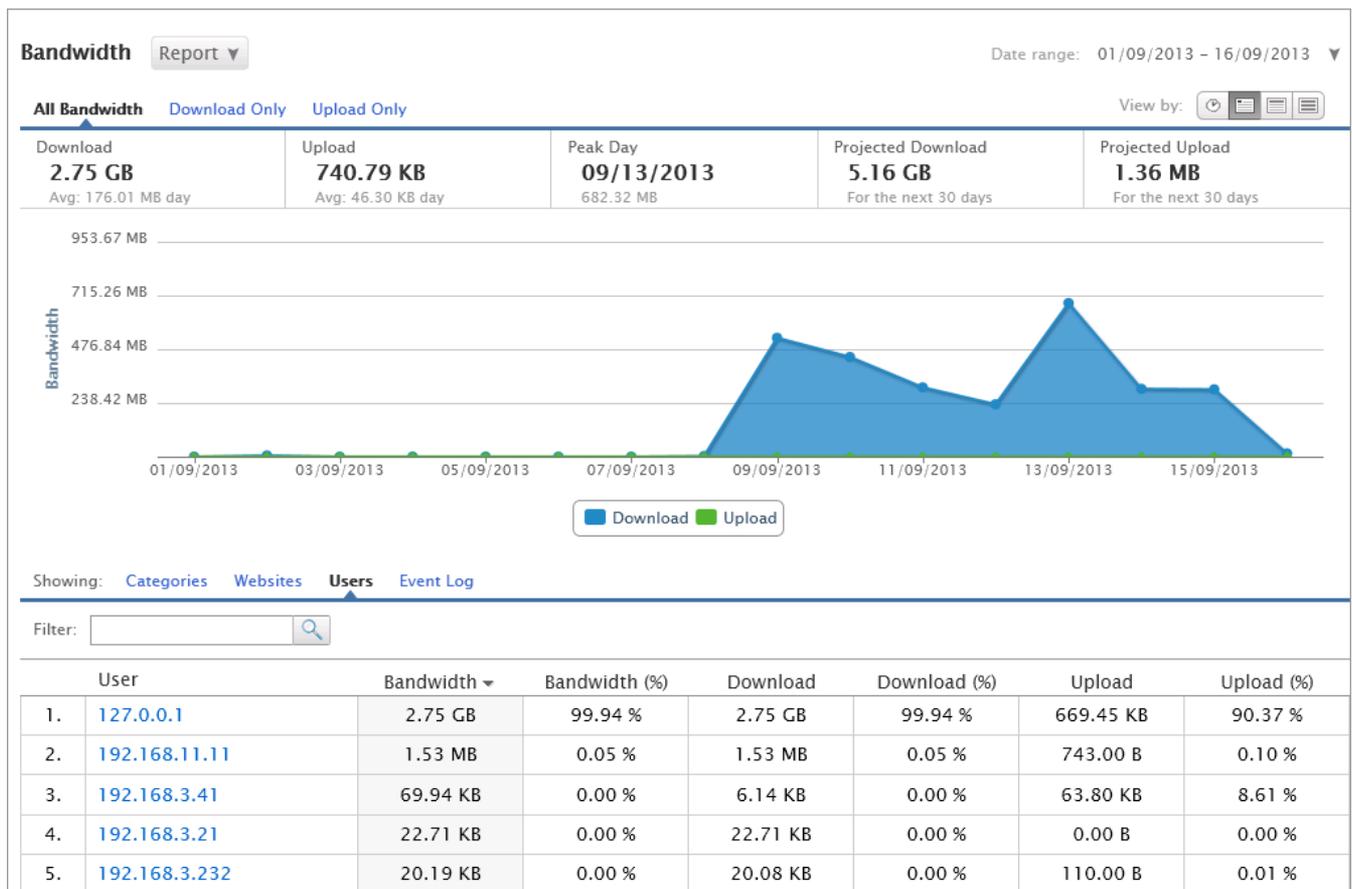
Use the Product Status area to verify details related to:

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 7).
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. Click **Dashboard > Bandwidth** and filter data according to the following:

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



Screenshot 13: 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:

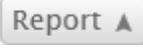
FILTER	DESCRIPTION
Categories	Select to view a list of categories and size of download for each category.
Websites	A list of websites with respective download size. Data can be viewed by Domain or by Site using the provided controls.
Users	A list of users and the total size of downloads for a specified period.
Even Log	Provides a log of all the web requests that fall within the specified period, displaying: <ul style="list-style-type: none"> » 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  and select **Export Report**.
2. GFI WebMonitor displays the exported report in a separate window in your browser.
3. Click  and select one of the following options:

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

Schedule Report

To schedule the report:

1. From the top of the Dashboard, click  and select **Schedule Report**.
2. GFI WebMonitor redirects you automatically to the **Reports** area.
3. Edit the report as required.
4. Save the report.

For more information refer to [Reporting](#).



IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information, refer to [General Options](#) (page 71).

5.3 Monitoring Activity

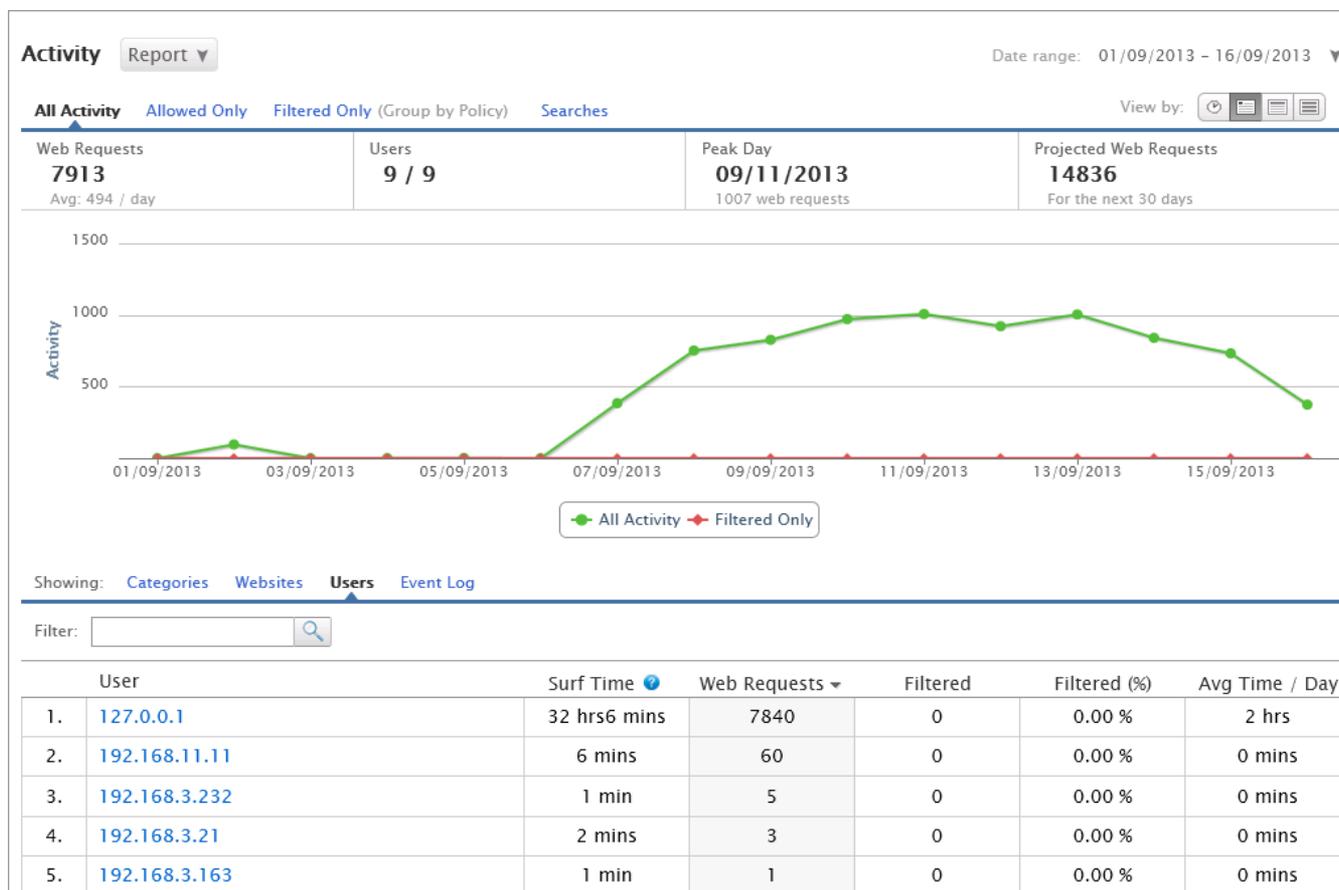
The Activity dashboard provides information related to web requests and user activity for a specified period. Click **Dashboard > Activity** and filter data according to the following:

OPTION	DESCRIPTION
All Activity	Shows all web requests (filtered and unfiltered) made through GFI WebMonitor in the specified period.
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 14: 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:

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	<p>A list of users and the total Surf Time and number of Web Requests for a specified period.</p> <p>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.</p>
Event Log	<p>Provides a log of all the web requests that fall within the specified period, displaying:</p> <ul style="list-style-type: none"> » 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:

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.
3. Edit the report as required.
4. Save the report.

For more information refer to [Reporting](#).



IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information, refer to [General Options](#) (page 71).

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.

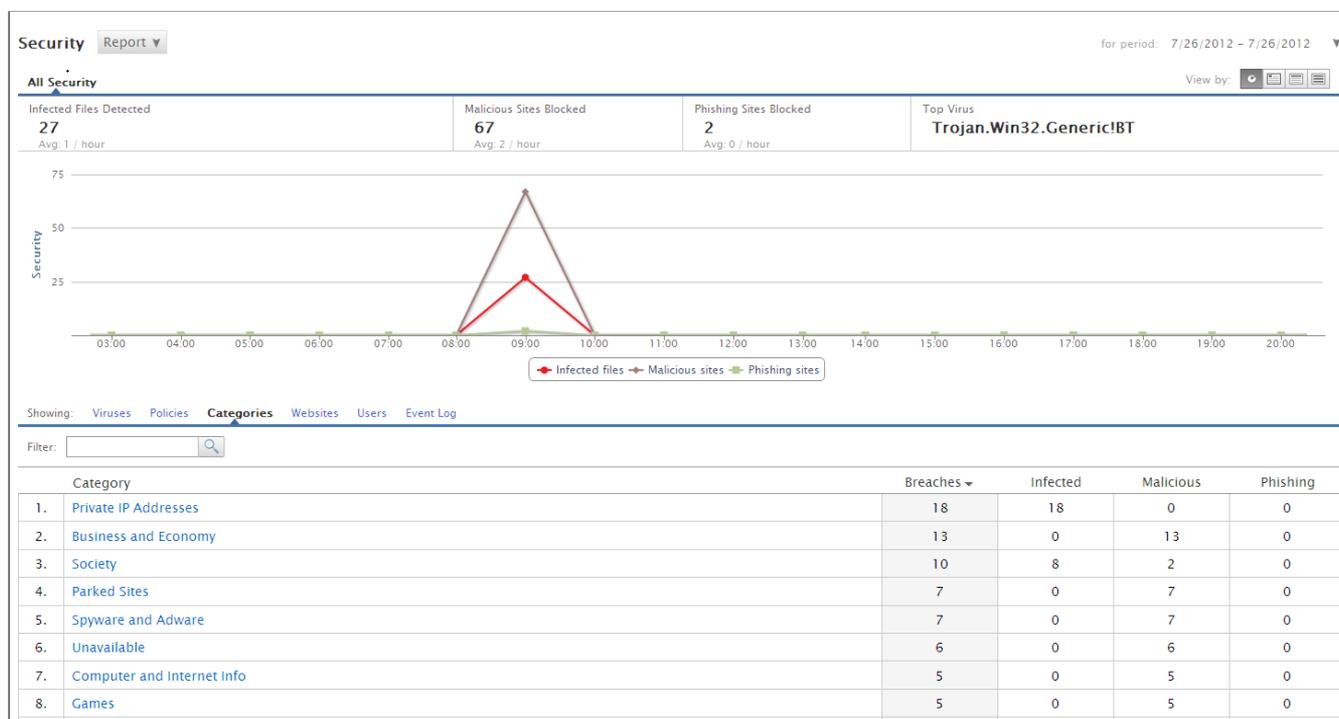
Click **Dashboard > Security** and filter available data to provide information related to:

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



NOTE

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



Screenshot 15: 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:

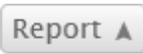
FILTER	DESCRIPTION
Viruses	A list of detected viruses, with the total number of Breaches .
Policies	Affected policies are listed in this tab, together with the total number of Breaches and the name of the users who made the request.
Categories	Select to view a list of categories with total number of 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	<p>A list of users and the total Breaches for a specified period, broken down under three headings: Infected, Malicious or Phishing.</p> <p> 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.</p>
Event Log	<p>Provides a log of all the web requests that fall within the specified period, displaying:</p> <ul style="list-style-type: none"> » 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  and select **Export Report**.
2. GFI WebMonitor displays the exported report in a separate window in your browser.
3. Click  and select one of the following options:

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

Schedule Report

To schedule the report:

1. From the top of the Dashboard, click  and select **Schedule Report**.
2. GFI WebMonitor redirects you automatically to the **Reports** area.
3. Edit the report as required.
4. Save the report.

For more information refer to [Reporting](#).

! IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information, refer to [General Options](#) (page 71).

5.5 Monitoring Real-Time Traffic

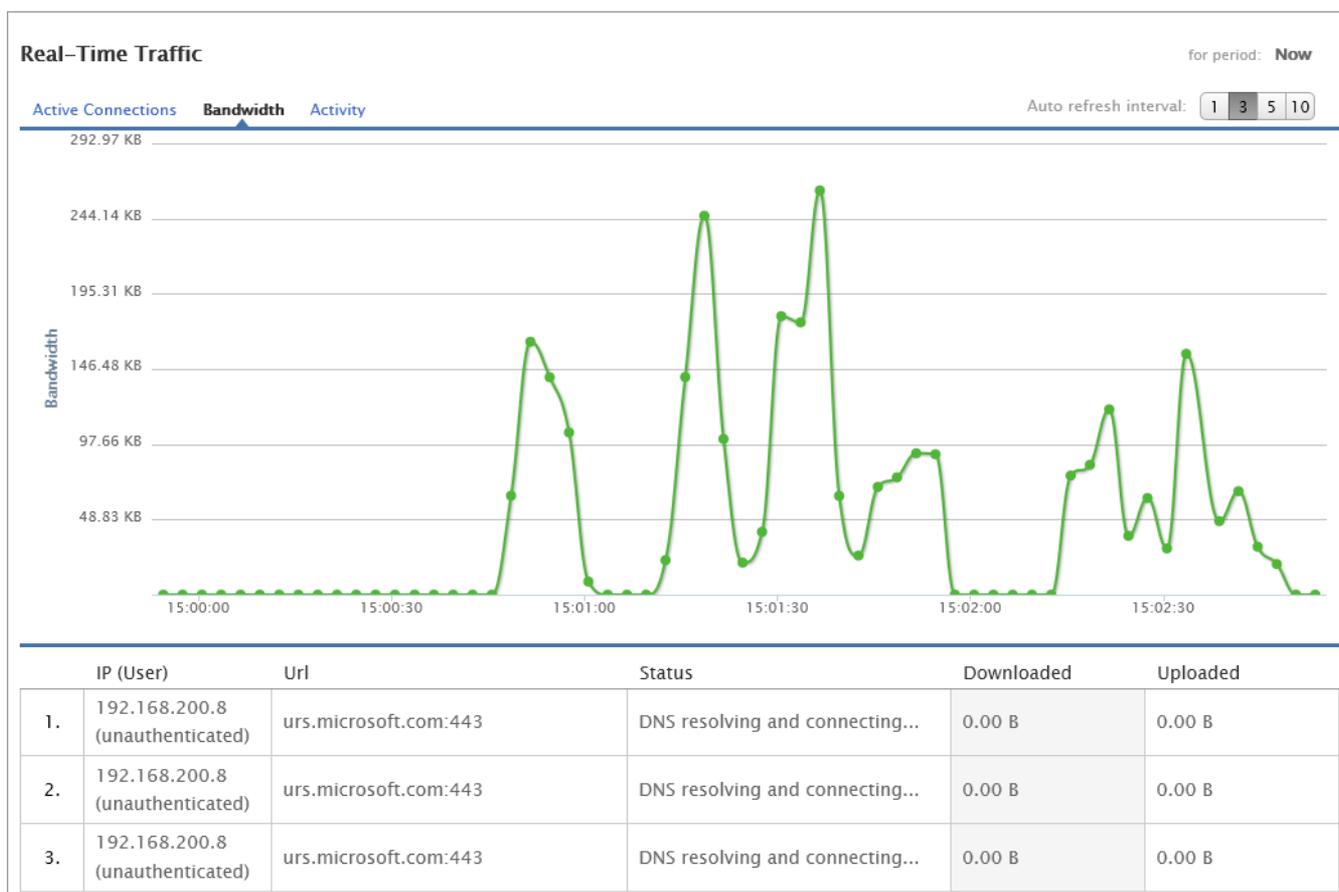
The Real-Time Traffic dashboard enables you to monitor Internet usage in real-time. Monitor current active connections and terminate them if necessary (for example, streaming media or large unauthorized downloads), and view most recent connections. Real-time graphs of bandwidth and activity give you 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](#) (page 71).

To access the Real-Time Traffic dashboard:

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



Screenshot 16: Real-Time Traffic Dashboard, Bandwidth monitoring

2. Click one of the following tabs:

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: <ul style="list-style-type: none"> » 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: <ul style="list-style-type: none"> » IP (User) » Url » Status » Downloaded » Uploaded
Activity	Displays the number of current web requests <ul style="list-style-type: none"> » 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:

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**.
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**.

5.7 Using the Quotas Dashboard

The Quotas dashboard lists active [Web Browsing Quota Policies](#) and their respective status. If a quota is exceeded, the administrator can review the listed items and decide on what action to take. If the policy is not reset, browsing is blocked and a message displayed in the user's browser stating the reason why the browsing was blocked and the name of the policy.

Quotas

Reset Reset All

<input type="checkbox"/>	User/IP	Policy Name	Limit Type	Limit	Usage
<input type="checkbox"/>	192.168.11.10	Limit Autoamtic Updates from Security Sites	Bandwidth (MB)	10	0 <input type="text"/>
<input type="checkbox"/>	192.168.11.10	Limit Social Media	Time (minutes)	10	3
<input type="checkbox"/>	192.168.11.10	Limit Streaming Media by bandwidth	Bandwidth (MB)	10	9.74
<input type="checkbox"/>	192.168.11.10	Web Browsing Quota Policy	Time (minutes)	10	0 <input type="text"/>
<input type="checkbox"/>	192.168.11.10	Limit YouTube by Time	Time (minutes)	5	3
<input type="checkbox"/>	192.168.11.10	Allow 1hr Online Shopping	Time (minutes)	60	4
<input type="checkbox"/>	192.168.11.10	Limit Entertainment Sites	Time (minutes)	1	0 <input type="text"/>

Rows: 10

Showing: **Users** **Limit Type**

Limit Type	Policies
1. Time	5
2. Bandwidth	2

Rows: 10

Screenshot 17: Quotas dashboard

The Quotas Dashboard provides the following information:

OPTION	DESCRIPTION
User/IP	Displays the user name or IP address being blocked. If Anonymization is enabled, the data shown is generic, for example, User 0, User 1. For more information, refer to General Options (page 71).
Policy Name	The name of the active policy. Click policy name to access settings page and edit the policy.
Limit Type	Limit type can be by Bandwidth (in KB or MB) or by Time (minutes or hours).
Limit	Displays the amount of Bandwidth or Time allocated in the respective Web Browsing Quota Policy.

OPTION	DESCRIPTION
Usage	Lists the amount remaining for each Web Browsing Quota Policy and a bar that fills up according to usage. Statistics are displayed when the mouse is hovered over the bar and contains the following: <ul style="list-style-type: none"> » Limited per » Limited Categories » Excluded sites » Enabled » Priority

An additional filter lets you view data by the following criteria:

OPTION	DESCRIPTION
Users (Default)	Lists Users or IP Addresses with a filter to search for entries of a particular user.
Limit Type	Click to filter data by the Limit Types. Drill down further by clicking on the types.

To reset an item from the Quotas list:

1. Go to **Dashboard > Quotas**.
2. Locate the item to reset, and select the check box next to it. You can also select multiple items.
3. To reset an exceeded policy perform one of the following actions:

OPTION	DESCRIPTION
Reset	Click to reset selected items in the list.
Reset All	Click to reset all items in the list.

4. From the **Reset Web Browsing Quota For User** window, click **Confirm**.



NOTE

You can also reset a quota from the [Web Browsing Quota Policy](#) page by clicking the refresh button next to the configured policy name.

5.8 Monitoring Agents

The Agents dashboard provides information related to the status of configured Agents. The information provided enables you to quickly identify when remote users last synchronized with your GFI WebMonitor server .

Data is filtered to provide information related to:

OPTION	DESCRIPTION
IP	Displays the detected GFI WebMonitor Agent by IP address.
Last Request	Lists the date and time of the last communication between the GFI WebMonitor Agent and the GFI WebMonitor server.
Agent Version	Displays the version number of the detected GFI WebMonitor Agent. An icon shows if the Agent is up to date or not.

An additional filter lets you view data by IP Addresses with a filter to search for entries of a particular user.



IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information, refer to [General Options](#) (page 71).

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.

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.
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.

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.
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.

Data **Schedule** **Distribution**

Schedule: **ON** **OFF** *NOTE: Schedule to automatically generate this report*

Runs: **Once** **Daily** **Weekly** **Monthly**

Repeat On: **Jan** **Feb** **Mar** **Apr** **May** **Jun**
 Jul **Aug** **Sep** **Oct** **Nov** **Dec**

On: day of the month

At:

Repeat Ends: **Never** **On**

Screenshot 18: Scheduling an activity report

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

OPTION	DESCRIPTION
Once	In the Run On field, specify a date and time to generate the report one time.
Daily	In the 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:

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.
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.

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.
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.

Data **Schedule** **Distribution**

Schedule: ON OFF *NOTE: Schedule to automatically generate this report*

Runs: Once Daily Weekly Monthly

Repeat On: Jan Feb Mar Apr May Jun
 Jul Aug Sep Oct Nov Dec

On: day of the month

At:

Repeat Ends: Never On

Screenshot 19: Scheduling an activity report

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

OPTION	DESCRIPTION
Once	In the Run On field, specify a date and time to generate the report one time.
Daily	In the 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:

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.
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.

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.
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.

Data **Schedule** Distribution

Schedule: ON OFF *NOTE: Schedule to automatically generate this report*

Runs:

Repeat On: Jan Feb Mar Apr May Jun
 Jul Aug Sep Oct Nov Dec

On: day of the month

At:

Repeat Ends:

Screenshot 20: Scheduling an activity report

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

OPTION	DESCRIPTION
Once	In the Run On field, specify a date and time to generate the report one time.
Daily	In the 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:

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

The following topics contain information on how to configure GFI WebMonitor:

General settings

- [1. Licensing](#)
- [2. UI Access Control](#)
- [3. Auto-update of internal scanning engines](#)
- [4. Database settings](#)
- [5. Configuring Web Activity Logging](#)
- [6. Downloaded files retention, Notification language, Temporary allowed period and Anonymization of personal data](#)
- [7. Web Categorization](#)

Policies

- [1. Internet policies](#)
- [2. Security policies](#)
- [3. Download control policies](#)
- [4. Always Blocked list, Always Allowed list and Temporary Allowed configuration](#)

Configuring Remote Devices

- [1. Downloading the GFI WebMonitor Agent](#)
- [2. How the WebMonitor Agent works](#)
- [3. Installing the WebMonitor Agent Manually](#)
- [4. Installing the GFI WebMonitor Agent via GPO](#)
- [5. Configuring Remote Filtering Policies](#)

Alerts

- [1. Configuring Monitoring Alerts](#)
- [2. Configuring Bandwidth Alerts](#)
- [3. Configuring Security Alerts](#)

Proxy Settings

- [1. General proxy settings](#)
- [2. HTTPS Proxy scanning settings](#)
- [3. Caching](#)

i 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 32).

7.1 General settings

The following topics help you configure settings related to how GFI WebMonitor work:

OPTION	DESCRIPTION
Licensing	View current licensing configuration or update with a new license key.
UI 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 Licensing information

The Licensing screen provides the following information:

OPTION	DESCRIPTION
Product Version	Shows the currently installed version of GFI WebMonitor and the build number.
License Key	Displays the active license key and provides the option to update it.
License Status	Defines which edition of GFI WebMonitor is currently installed. For more information, refer to About GFI WebMonitor (page 5).
Subscription	Shows the date of expiry of the current license.
Licensed Seats	Displays the number of licensed users and how many are currently active on the network.

7.1.2 Updating the license

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**.

i NOTE

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

7.1.3 UI Access Control

The **UI 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](#) (page 64)..
- » 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 64).

Configuring Windows Authentication

When **Windows Authentication** is enabled, you can For more information, refer to [Configuring Windows Authentication](#) (page 64).

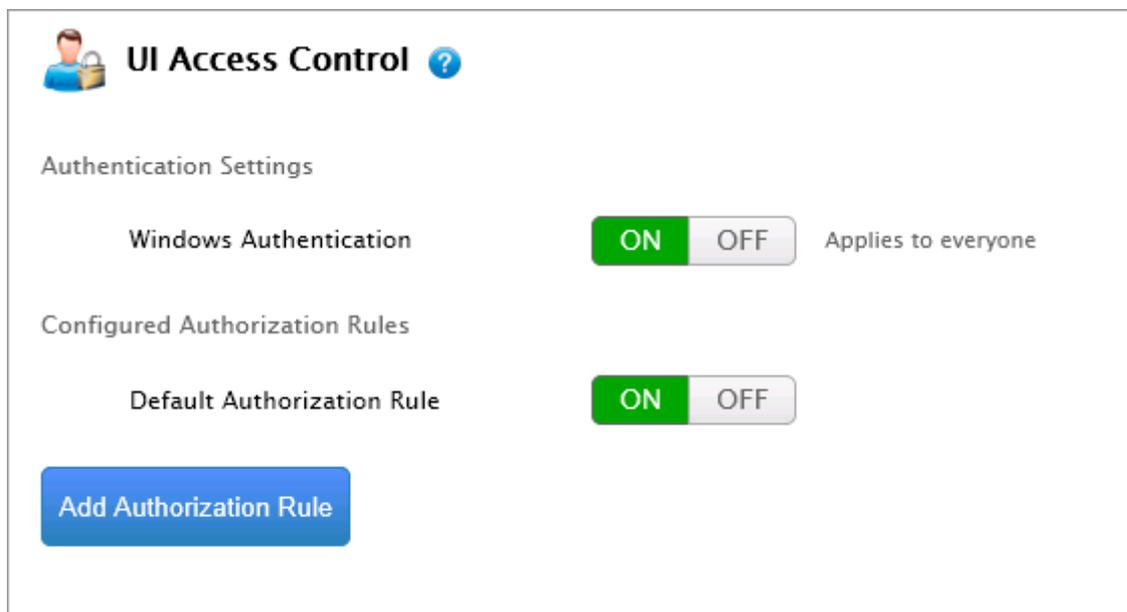


IMPORTANT

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 > UI Access Control**.



Screenshot 21: 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 > UI Access Control**.
2. Click **Add 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 64).

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.
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**.

7.1.4 Configuring Auto-Update

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

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.

3. [Optional] Click on any of the Monitoring Engines in the Auto-Update page and configure the following options:

OPTION	DESCRIPTION
Check for updates, and if available install them, every:	Specify the frequency (in hours) to check for available updates.
Update Now	Click to update the monitoring engine manually.
Send an email notification to the administrator on successfully updating the engine	Enable to send email notifications to the administrator when an engine is successfully updated. <div style="border: 1px solid #ccc; padding: 5px;"> <p>NOTE If an engine update fails, an email notification is always sent to the administrator.</p> </div>

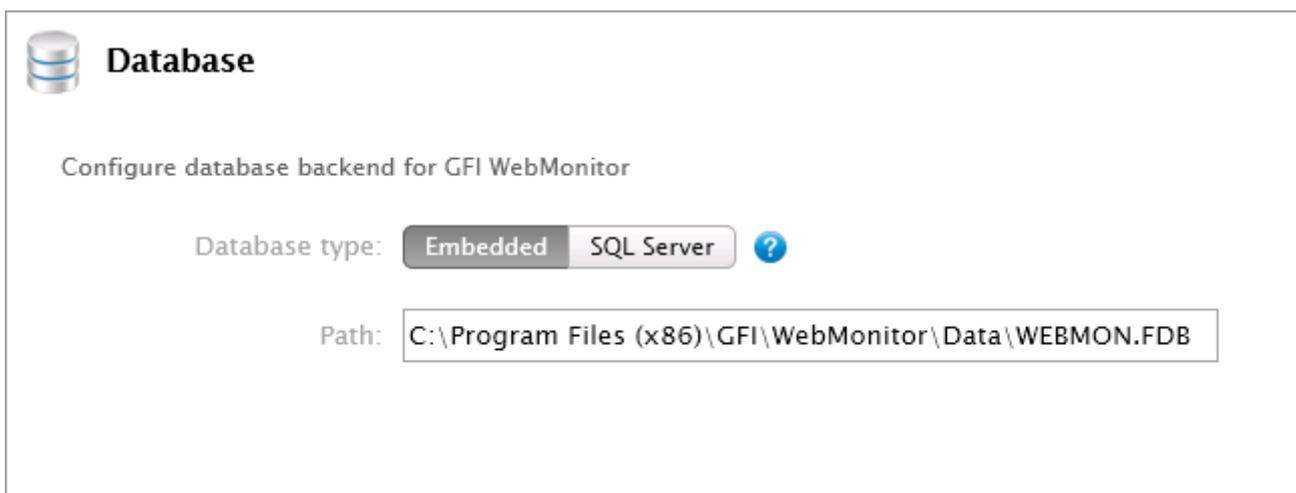
4. Click **Save**.

7.1.5 Configuring Databases

GFI WebMonitor supports two types of 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 22: Configured 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**.

Database

Configure database backend for GFI WebMonitor

Database type: Embedded SQL Server ?

Path: C:\Program Files (x86)\GFI\WebMonitor\Data\WEBMON.FDB

Screenshot 23: Configuring Databases

4. From **Database Type**, select **Embedded**.
5. In the **Path** field, change the path to 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**.

[Cancel Changes](#)

Configure database backend for GFI WebMonitor

Database type: Embedded SQL Server

SQL Server:

Authentication: Windows Authentication SQL Server Authentication

Username:

Password:

Database:

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

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

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**.

7.2 Configuring Web Activity Logging

By default, all Internet traffic (excluding GFI WebMonitor updates), is routed through GFI WebMonitor for all licensed users. This data is required to populate dashboards and reports.

 **IMPORTANT**

If logging is disabled, traffic is still filtered but data will no longer be available for reporting.

GFI WebMonitor enables you to customize logging options to exclude specific users, web site categories and domains from activity logging. This feature is useful when, for example, you want to exclude traffic to your own company's domain from appearing in reports.

Additionally, you can also enable advanced logging options that keep track of full URLs visited by users. This option is useful for investigative purposes. When enabled, Dashboards and reports display the full address of visited sites. Full URL logging can be enabled for users (or IP), for specific categories or on a domain basis.

 **NOTE**

Full URL logging generates a large amount of data in the database. We recommend using this feature only for specific users (or domains) and only for a limited period of time. Additionally, use the Data Retention options to store activity logs for a shorter period of time to save database space.

To configure logging options:

1. Go to **Settings > General > Activity Logging**.
2. By default the **Logging status** is set to **Enabled**. Click **Disabled** to turn off activity logging completely.

 **IMPORTANT**

If logging is disabled, traffic is still filtered but data will no longer be available for reporting.

3. For optimization purposes, configure Data Retention using the following options:

OPTION	DESCRIPTION
Retain activity data for	<p>Specify the length of time that all type of data collected by GFI WebMonitor is retained. Data is deleted after the specified period expires. To configure for how long to retain data, key in the number of days in this field. The default value is set to 365 days.</p> <p> NOTE Activity data affect database size. Store activity data for a shorter period of time to save space. Data older than the specified number of days will no longer be available in Dashboard. Reports defined for earlier periods will be empty.</p>

OPTION	DESCRIPTION
Retain Event Log data for	<p>Define for how long event log data is kept in the database. After the specified period expires, only Event Log data is deleted - other data collected by GFI WebMonitor is not affected by this option. We recommend setting a shorter retention period when Full URL logging is enabled.</p> <p>NOTE When Event Log data is deleted, information in the Event Log column in Bandwidth, Activity and Security dashboards will no longer be available. Some detailed reports are also affected.</p>

3. In the **Exclude logging for** area, configure options for:

OPTION	DESCRIPTION
Users	Specify users to exclude from logging, either by their Active Directory/Windows user name or by IP.
Categories	Enter specific Categories to exclude from Activity Logging. Start typing in the Category field and select from the provided list.
Domains	Specify domains to exclude using the format domain.com or subdomain.domain.com .

4. [Optional] In the **Enable full URL logging for** area, configure the following options:

OPTION	DESCRIPTION
Users	Specify users either by their Active Directory/Windows user name or by IP.
Categories	Enter specific Categories from the GFI WebMonitor categories database.
Domains	Specify domains using the format domain.com or subdomain.domain.com .

5. Click **Save**.

7.2.1 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 24: Configuring administrative notifications

2. Change any of the following options:

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.
Authentication	If you are using a hosted email provider, enable Authentication and provide a Username and Password to connect to your hosted mail server and send notifications. If SSL is required, click ON in the Enable SSL area.
Email addresses	Enter recipient email addresses.
Verify Mail Settings	Click to send a test email and verify the mail server settings are configured correctly.

3. Click **Save**.

7.2.2 General Options

Use the Options tab to configure:

- » Data retention periods
- » Length of time to keep downloaded files in cache
- » Language used when displaying blocking notifications or warnings
- » Length of time to keep websites in Temporary Allowed list
- » Anonymization of personal data.

Options

[Save](#) [Cancel Changes](#)

General WebMonitor configuration options

Downloaded files cached for: hours

Language:

Temporary allowed period: hours

Anonymize: ON OFF [?](#)

Responsible Person 1

Password: Confirm:

Responsible Person 2

Password: Confirm:

[Save](#) [Cancel Changes](#)

Screenshot 25: Configuring general options

Downloaded files cached for

When Caching is enabled, GFI WebMonitor stores retrieved data in a local database so that future requests for that same data are served faster. Use this option to set the length of time to keep this data. For more information, refer to [Configuring Caching settings](#) (page 121).

Language

When GFI WebMonitor blocks user activity, a warning message is sent to the user, stating which policy was breached. The language of these warning messages can be configured from a pre-defined list.

To change the language of warning messages, select a language from the drop down list and click **Save**.

Temporary allowed period

Use this option to control for how long GFI WebMonitor will keep websites in the **Temporary Allowed** list of sites.

Anonymization

Anonymization enables masking private user data in accordance with European privacy and data protection laws. If enabled, GFI WebMonitor:

» Cloaks personal data (User name and IP) so that it can no longer be viewed from the **Dashboard** or **Monitoring Reports**

» Enables a validation process requiring two passwords from two different users

» Masks any features in the User Interface that provide access to private user information.

To enable Anonymization:

1. Go to **Settings > Options**.
2. In the Anonymize area, click **ON**.
3. Enter the passwords for **Responsible Person 1** and **Responsible Person 2**
4. Click **Save** .



NOTE

To disable Anonymization, click **OFF** and enter the required passwords.

7.2.3 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: [How Web Reputation increases your online protection](#).



NOTE

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

Web Categorization

Web Categorization configuration ?

Online Lookup: **ON** OFF Enable real-time lookup for URLs not found in the local database (Recommended).

Lookup website: **Check Category** **Send URL Feedback to GFI**

Screenshot 26: 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 Internet Activity Dashboard. For more information, refer to [Overview of Internet Activity](#) (page 39).

7.3 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](#)

7.3.1 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.

7.3.2 Configuring Internet Policies

The following topics guide you through the configuration of Internet 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**.

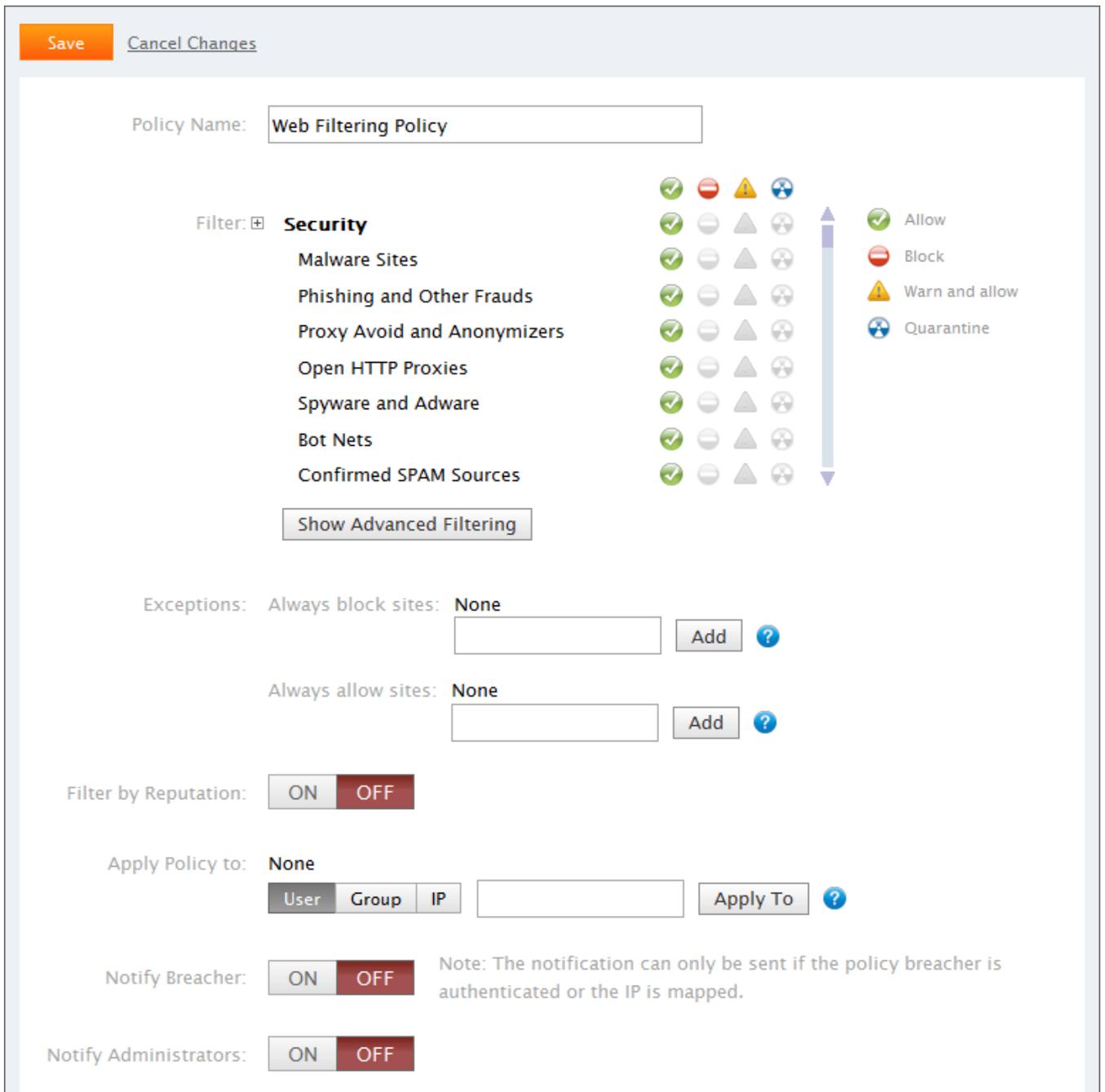


IMPORTANT

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 27: 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 28: 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:

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 73).

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

OPTION	DESCRIPTION
Basic authentication	Select if user is required to provide login credentials when new Internet sessions are launched
Integrated authentication	This option enables GFI WebMonitor proxy to authenticate users by using the client machines' access control service. User is not prompted to provide login credentials when new Internet sessions are launched. (Recommended)

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**.

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**.

The screenshot shows a web-based configuration interface for creating a new Web Browsing Quota Policy. At the top, there are buttons for 'Save' (highlighted in orange), 'Cancel Changes', and 'Clone Policy'. The main form area contains the following sections:

- Policy Name:** A text input field containing 'Web Browsing Quota Policy'.
- Limit By:** Two radio buttons, 'Bandwidth' and 'Time', with 'Time' selected. Next to it is a text input field with the value '1', followed by a dropdown menu set to 'Hour' and the text '(s) per'. To the right are three document icons.
- Apply To:** A dropdown menu set to 'Categories' with a close button (X). Below it, 'Social Network' is selected with a close button (X). There are two radio buttons, 'Category' and 'Site', with 'Site' selected. To the right is a text input field and an 'Add' button.
- Exclude Sites:** A text input field containing '*.linkedin.com' with a close button (X). To the right is an 'Add' button.
- Apply Policy to:** A text input field containing 'john Smith' with a close button (X). To the right is an 'Apply To' button.
- Notify Breacher:** Two radio buttons, 'ON' (highlighted in green) and 'OFF'. To the right is a note: 'Note: The notification can only be sent if the policy breacher is authenticated or the IP is mapped.'
- Message to Policy Breacher:** A text area containing the message: 'Your request has been blocked by GFI WebMonitor. The web browsing policy threshold has been exceeded.'
- Notify Administrators:** Two radio buttons, 'ON' and 'OFF', with 'OFF' highlighted in red.

At the bottom of the form, there are buttons for 'Save' (highlighted in orange), 'Cancel Changes', and 'Clone Policy'.

Screenshot 29: Creating a new Web Browsing Quota Policy

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

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

- If the threshold will be based on **Bandwidth** or **Time**
- The duration in hours or minutes
- If the duration is per day, week or month

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

- Select which categories or sites are affected by policy.
- 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**.

OPTION	DESCRIPTION
Basic authentication	Select if user is required to provide login credentials when new Internet sessions are launched
Integrated authentication	This option enables GFI WebMonitor proxy to authenticate users by using the client machines' access control service. User is not prompted to provide login credentials when new Internet sessions are launched. (Recommended)

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 or use the [Quotas Dashboard](#).

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:

- » 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**.

The screenshot shows the 'Create a new IM Policy' configuration window. At the top, there are 'Save' and 'Cancel Changes' buttons. The 'Policy Name' field contains 'Default IM / Social Control Policy'. The 'Filter' is set to 'Instant Messaging Controls'. Under 'Instant Messaging Controls', there are four items: Google Talk, Yahoo Messenger, Facebook Chat, and Online Portals, each with 'Allow' and 'Block' buttons. Under 'Social Controls', there are five items: Facebook Apps, Google+, Twitter, and Others, each with 'Allow' and 'Block' buttons. The 'Apply Policy to' is set to 'Everyone'. The 'Notify Breacher' and 'Notify Administrators' options are both set to 'OFF'. A note states: 'Note: The notification can only be sent if the policy breacher is authenticated or the IP is mapped.' At the bottom, there are 'Save' and 'Cancel Changes' buttons.

Screenshot 30: 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**.

OPTION	DESCRIPTION
Basic authentication	Select if user is required to provide login credentials when new Internet sessions are launched
Integrated authentication	This option enables GFI WebMonitor proxy to authenticate users by using the client machines' access control service. User is not prompted to provide login credentials when new Internet sessions are launched. (Recommended)



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**.

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**.

[Cancel Changes](#)

Policy Name:

Filter: Streaming Media Categories

 Streaming Media

 Image and Video Search

Streaming Applications

 iTunes

 QuickTime

 Winamp

 Windows Media Player

Generic Site Streams

 Generic Site Streams

Exceptions: Always block sites: **None**



Always allow sites: **None**



Apply Policy to: **None**



Screenshot 31: Configuring Streaming Media policy 1

- In the **Policy Name** field, type a policy name.
- In the **Filter** area, select the **Streaming Media Categories**, **Streaming Applications** and **Generic Site Streams** to **Allow** or **Block**.
- 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.
- In the **Apply Policy To** field, specify **Users**, **Groups** or **IPs** for whom the new policy applies, then click **Add**.

OPTION	DESCRIPTION
Basic authentication	Select if user is required to provide login credentials when new Internet sessions are launched
Integrated authentication	This option enables GFI WebMonitor proxy to authenticate users by using the client machines' access control service. User is not prompted to provide login credentials when new Internet sessions are launched. (Recommended)



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**.

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 32: 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**.

7.3.3 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**.
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'

7.3.4 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**.

7.3.5 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 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

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:

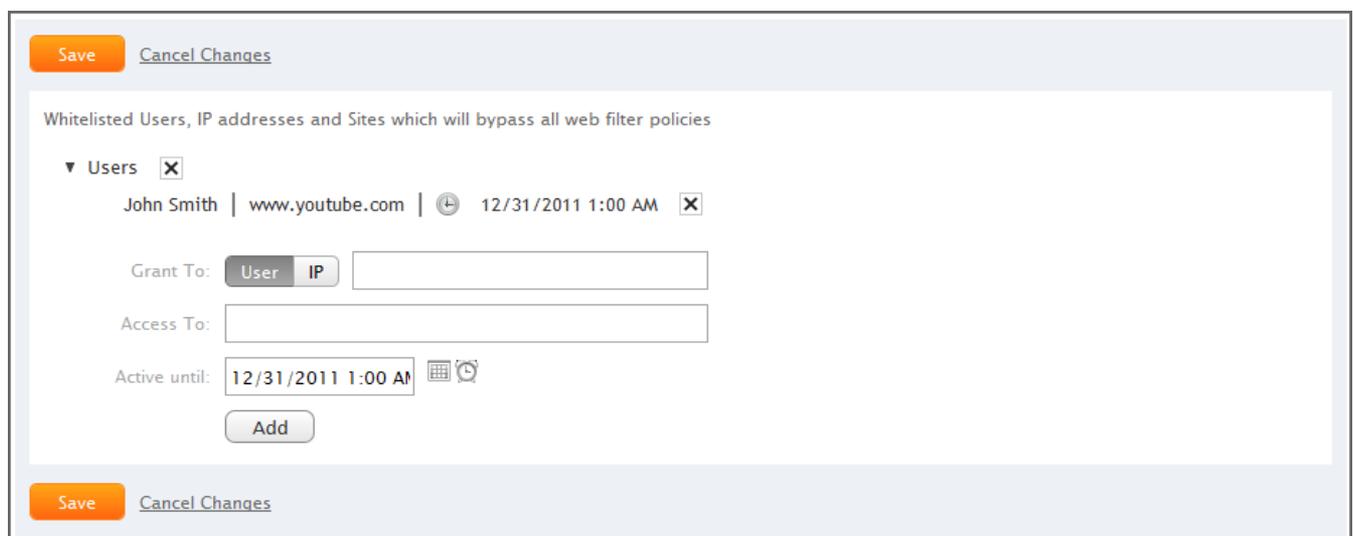
1. Go to **Settings > Policies > Always Allowed**.
2. Click the **Delete** icon next to the item to delete.
3. Click **Save**.

7.3.6 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 policies 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**.



Whitelisted Users, IP addresses and Sites which will bypass all web filter policies

▼ Users X

John Smith | www.youtube.com | 12/31/2011 1:00 AM X

Grant To: User IP

Access To:

Active until: 12/31/2011 1:00 AM

Add

Save Cancel Changes

Screenshot 33: 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**.

7.3.7 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.

7.3.8 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 scan all file types using the inbuilt BitDefender, VIPRE and Kaspersky engines. 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**.

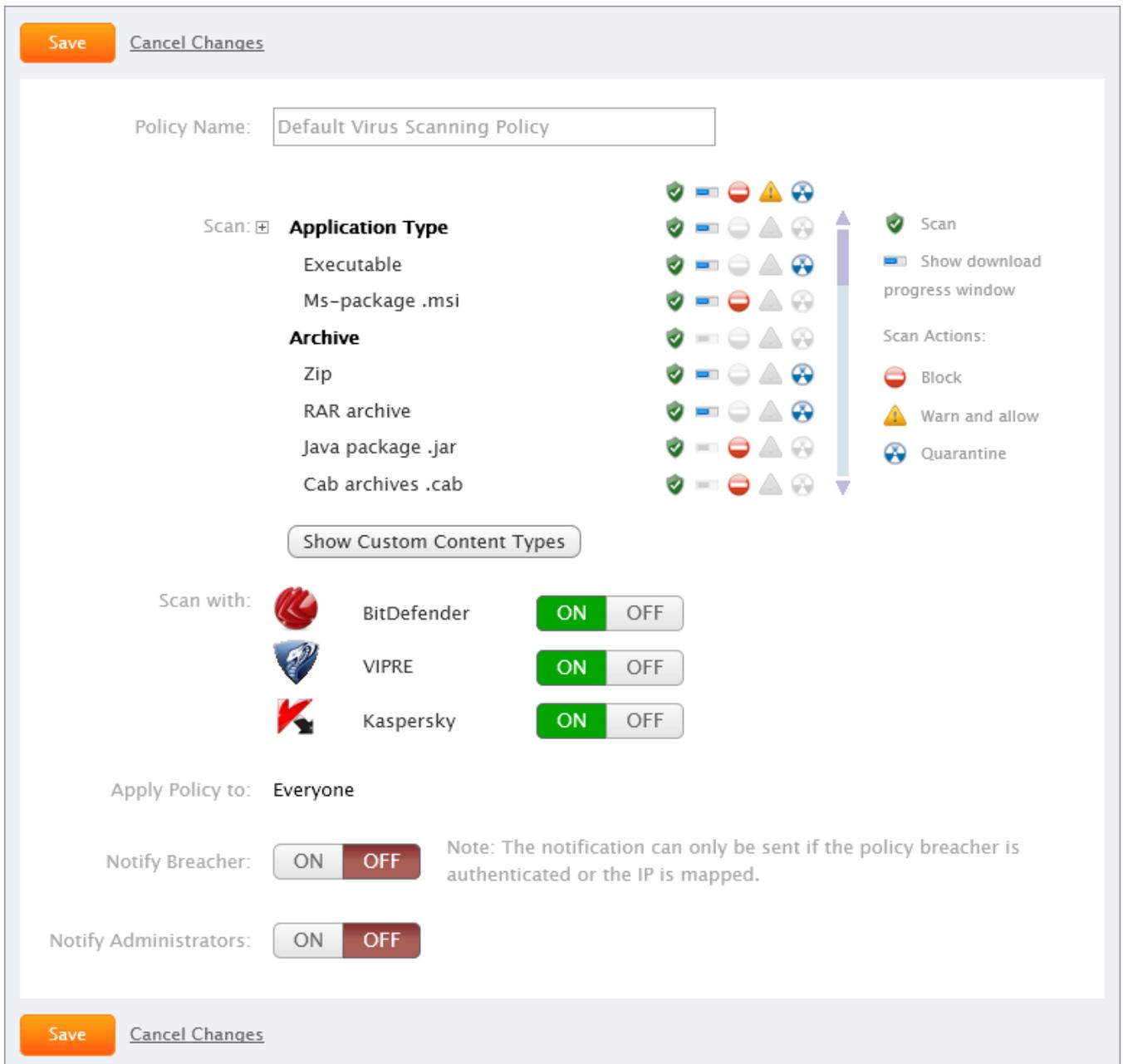


IMPORTANT

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 34: 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**:

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.
	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 51).

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**.

OPTION	DESCRIPTION
Basic authentication	Select if user is required to provide login credentials when new Internet sessions are launched
Integrated authentication	This option enables GFI WebMonitor proxy to authenticate users by using the client machines' access control service. User is not prompted to provide login credentials when new Internet sessions are launched. (Recommended)

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.

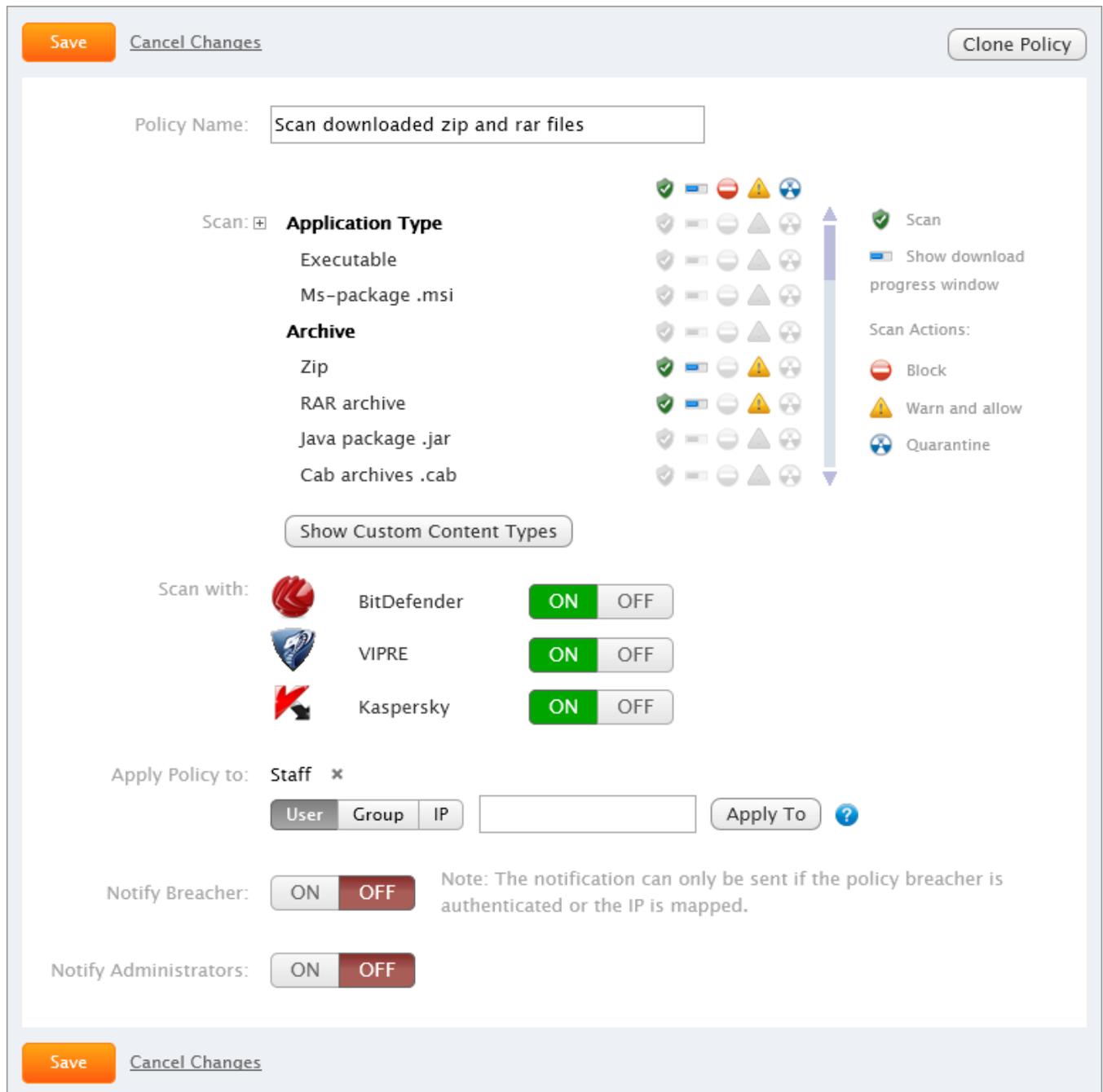
9. [Optional] In the **Notify Administrators** area, click **ON** to enable notifications. Specify an email address in the available box and click **Add**. You can also edit the notification message in the **Message to Policy Breacher** window.

10. Click **Save**.

7.3.9 Adding a New Security Policy

To add a new Security Policy:

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



Screenshot 35: Creating a new Security Policy

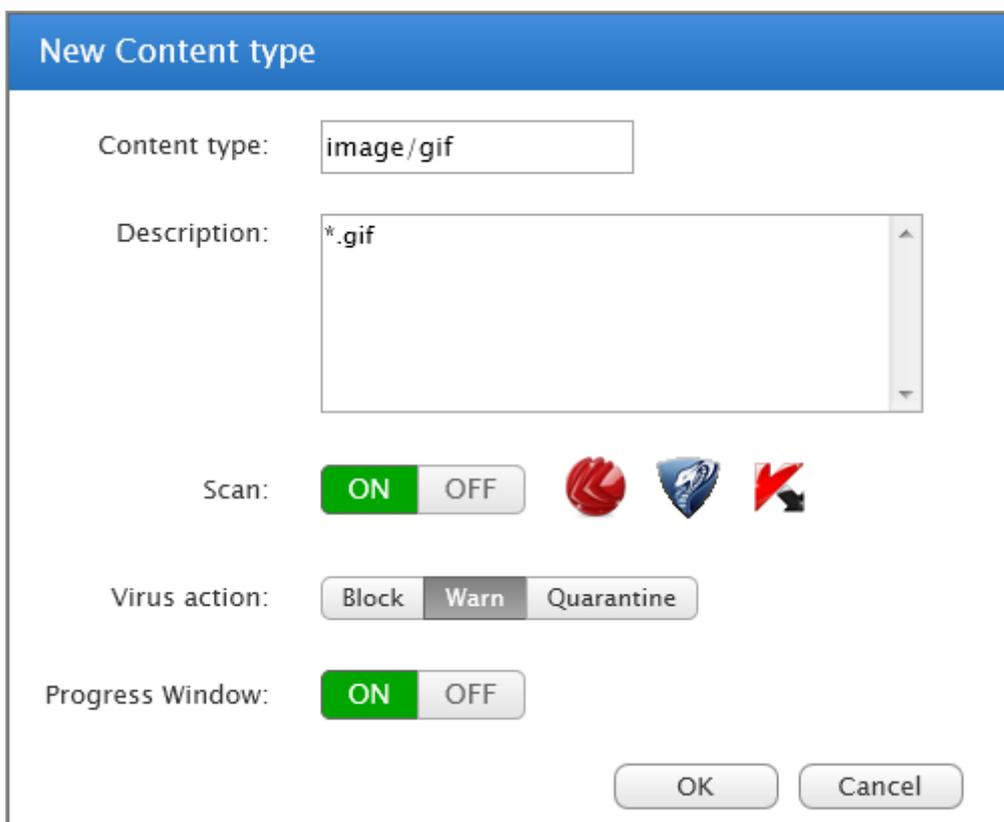
3. In the **Policy Name** field enter a name for the new policy. This field is not available when editing the **Default Virus Scanning Policy**.

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

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.
	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 51).

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

a. Click **Add Content Type**.



New Content type

Content type:

Description:

Scan: ON OFF   

Virus action:

Progress Window: ON OFF

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**.

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

OPTION	DESCRIPTION
Basic authentication	Select if user is required to provide login credentials when new Internet sessions are launched
Integrated authentication	This option enables GFI WebMonitor proxy to authenticate users by using the client machines' access control service. User is not prompted to provide login credentials when new Internet sessions are launched. (Recommended)

- [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.
- [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.
- Click **Save**.

7.3.10 Configuring Security Engines

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

To turn off a security engine:

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

The screenshot displays the GFI WebMonitor interface for configuring security policies. The 'Settings' tab is active, and the 'Security Policies' section is expanded. Under 'Configured Virus Scanning Policies', there are two entries: 'Blocking Policy' (ON) and 'Default Virus Scanning Policy' (ON). Below this is the 'Security Engines' section, which lists five engines: BitDefender, VIPRE, Kaspersky, Anti-Phishing, and ThreatTrack. Each engine has an 'ON' button next to it, indicating it is currently enabled.

Screenshot 36: Configuring Security Engines

- 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](#)

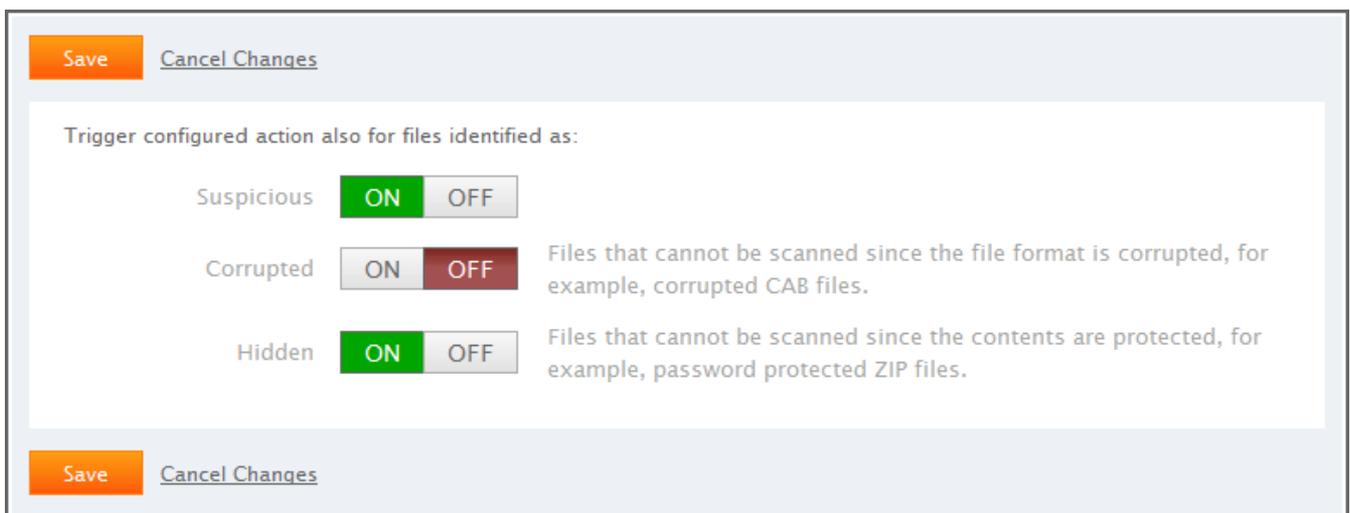
7.3.11 Configuring Kaspersky

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:

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 37: 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**.

7.3.12 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**.

7.3.13 Configuring ThreatTrack

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

To configure ThreatTrack:

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

Security Policies > Threat Track Details

Save Cancel Changes

Notify Breacher: ON OFF Note: The notification can only be sent if the policy breacher is authenticated or the IP is mapped.

Message to Policy Breacher:

GFI WebMonitor protected you from accessing a known ThreatTrack site.

Notify Administrators: ON OFF

johnsmith@domain.com ✕

Input field: Add Specify email address of who needs to be notified

Message to Administrators:

GFI WebMonitor blocked access to a known ThreatTrack site.

Save Cancel Changes

Screenshot 38: 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**.

7.3.14 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.

Adding a new Download Policy

To add a Download Policy:

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

[Cancel Changes](#)

Policy Name:

Filter: **Application Type**

- Executable
- Ms-package .msi

Archive

- Zip
- RAR archive
- Java package .jar
- Cab archives .cab

Apply Policy to:

Notify Breacher: ON OFF
 Note: The notification can only be sent if the policy breacher is authenticated or the IP is mapped.

Message to Policy Breacher:

Your download has been blocked. The content breaches a GFI WebMonitor download control policy.

Notify Administrators: ON OFF

Screenshot 39: 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:

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 51).



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**.

OPTION	DESCRIPTION
Basic authentication	Select if user is required to provide login credentials when new Internet sessions are launched
Integrated authentication	This option enables GFI WebMonitor proxy to authenticate users by using the client machines' access control service. User is not prompted to provide login credentials when new Internet sessions are launched. (Recommended)



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**.

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**.

Cloning a Policy

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

To clone a policy:

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

4. Click **Clone Policy**.



NOTE

Default policies cannot be cloned.

7.4 Configuring the GFI WebMonitor Agent

The GFI WebMonitor Agent is a small footprint version of GFI WebMonitor. It can be deployed on portable computers (as a service) to apply web filtering policies when the machine is disconnected from the corporate network (for example when the user is at home or traveling on business).

While the device is connected to the corporate network, the GFI WebMonitor Agent downloads Remote Filtering Policies locally. These are specific policies that can be set up to be applied when roaming. With this functionality, the IT Administrator can apply policies based on whether users are at the office or away. For example, Streaming Media can be allowed outside the internal network but Adult material is always denied.

Web activity logging is still performed when the user is outside the network, providing full reporting capabilities. The GFI WebMonitor Agent uploads the collected data to the server once the machine is connected to the corporate network.



NOTE

Anti-virus protection is not deployed with the GFI WebMonitor Agent. For a complete web security solution, we recommend an additional local antivirus agent besides the web filtering agent.

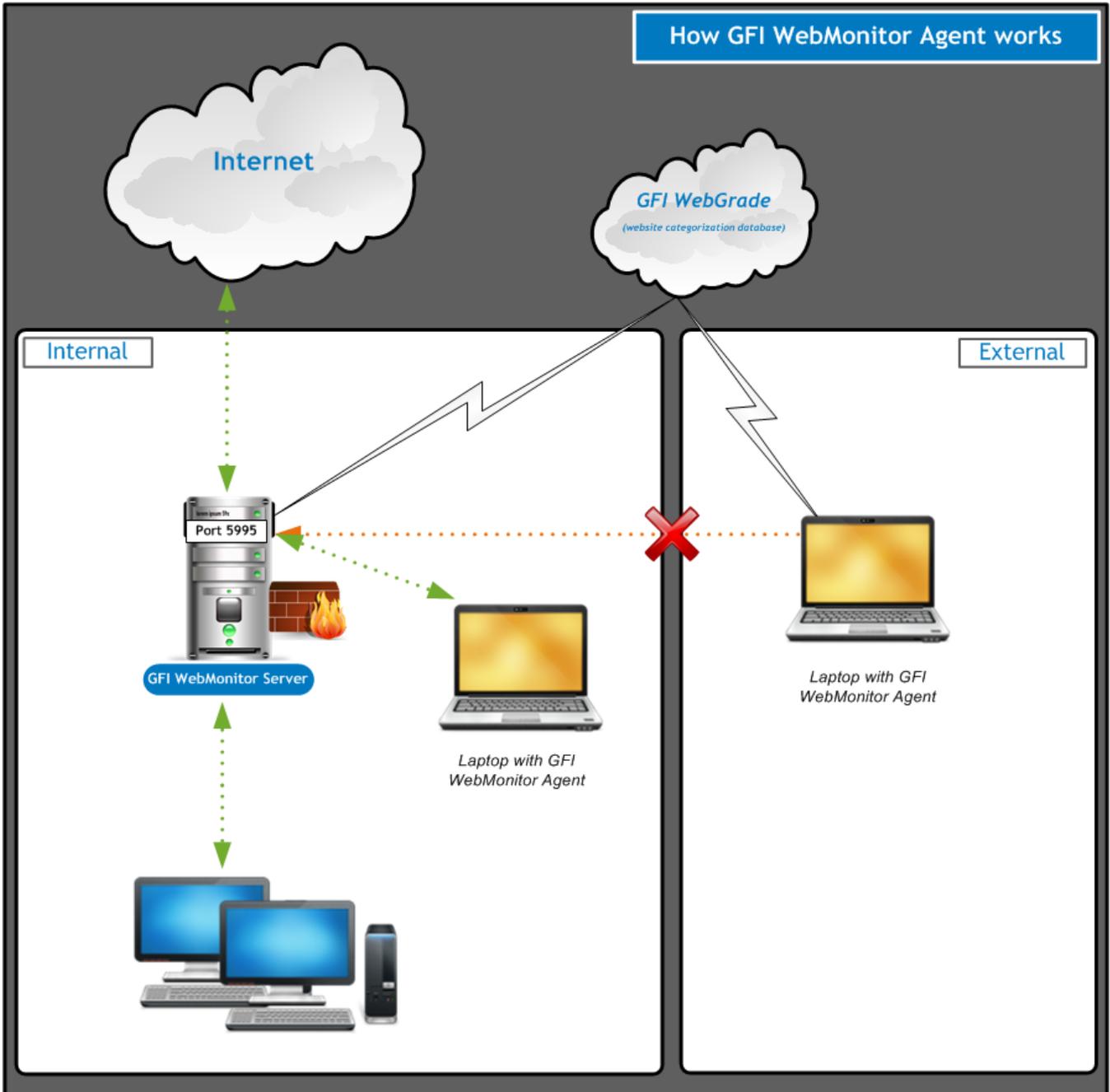
When roaming, Web filtering is done by the agent (on the local computer) and therefore there is no additional complexity of making any changes to your corporate network's infrastructure to enable remote filtering capabilities. For categorization and lookup purposes, the GFI WebMonitor Agent performs online lookups against the GFI WebGrade categorization service.

7.5 Downloading the GFI WebMonitor Agent

To download the GFI WebMonitor Agent:

1. In GFI WebMonitor, go to **Settings** page.
2. Click **Remote Devices**, then click **Downloads**.
3. Select one of the following download options:
 - » To install the agent on a 32-bit operating system click **Download (32-bit)**. This downloads the following file: GFIWebMonitorAgent_x86.msi
 - » To install the agent on a 64-bit operating system click **Download (64-bit)**. This downloads the following file: GFIWebMonitorAgent_x64.msi

7.5.1 How the GFI WebMonitor Agent works



Screenshot 40: GFI WebMonitor Agent functionality inside and outside the network

In internal mode:

When a laptop or other roaming machine (installed with the GFI WebMonitor Agent) is connected to the corporate network, Remote Filtering Policies are downloaded from the GFI WebMonitor server to the laptop. These policies are applied when the laptop is taken outside the network.

Web activity logging collected by the laptop while outside the network is uploaded to the GFI WebMonitor server. The GFI WebMonitor Agent disables itself after it completes the update processes.



IMPORTANT

Ensure port 5995 is not exposed outside the internal network



NOTE

Ensure that WPAD/Proxy settings are configured when the machine is on the Internal network, otherwise it will not connect to the GFI WebMonitor server.

In external mode:

When the laptop is taken outside the network, the GFI WebMonitor Agent activates automatically to filter and log Internet activity according to configured policies. For categorization and lookup purposes, GFI WebMonitor Agent performs online lookups against the GFI WebGrade categorization service.



NOTE

Anti-virus protection is not deployed with the GFI WebMonitor Agent. For a complete web security solution, we recommend an additional local antivirus agent besides the web filtering agent.

7.6 Installing the WebMonitor Agent Manually

To manually install GFI WebMonitor Agent:

1. Log on the client machine with Administrative rights.
2. Open GFI WebMonitor through a Web browser.



NOTE

To access GFI WebMonitor from a remote location, first grant remote access to the GFI WebMonitor server. For more information, refer to [UI Access Control](#) (page 64).

3. Click **Settings > Remote Devices > Downloads**.
4. Download the GFI WebMonitor Agent to a local folder.
5. Double click the downloaded file and follow the wizard to install.
6. Read the **End-User License Agreement** and click **I accept the terms in the License Agreement** to continue, then click **Next**.
7. In the **Server Information** window, provide the following settings:

OPTION	DESCRIPTION
Server Address	Enter the IP address of the GFI WebMonitor server to get the filtering settings and to send browsing reports.
Server Port	Enter the Port number used by the GFI WebMonitor Agent to communicate with the GFI WebMonitor server. Default is 5995.



IMPORTANT

Ensure port 5995 is not exposed outside the internal network

8. Click **Next**.
9. Select an installation folder where the GFI WebMonitor Agent will be installed, then click **Next**.
10. Click **Install**.
11. Enter credentials for an account with Administrative privileges when prompted.
12. Click **Finish**.

7.7 Installing the GFI WebMonitor Agent via GPO in Windows Server 2008

You can deploy the GFI WebMonitor Agent as an MSI package using Group Policy Objects (GPO). This method assigns the agent on a per-user or a per-machine basis. If assigned per-user basis, it is installed when the user logs on. If assigned per-machine basis then the agent is installed for all users when the machine starts.

How the GFI WebMonitor Agent works

7.7.1 Step 1: Creating a distribution point

The first step in deploying the GFI WebMonitor Agent MSI through GPO is to create a distribution point on the publishing server, with a shared folder to contain the MSI package:

1. Download the GFI WebMonitor Agent. For more information, refer to [Downloading the GFI WebMonitor Agent](#) (page 98).
2. Log on to the server as a user with Administrative rights.
3. Create a shared network folder.
4. Set permissions on this folder in order to allow access to the distribution package.
5. Copy the downloaded GFI WebMonitor Agent MSI in the shared folder.

7.7.2 Step 2: Installing GFI WebMonitor Agent via GPO in Windows Server 2008

To distribute the GFI WebMonitor Agent MSI package through GPO as a Group Policy Object:

1. Go to command prompt, key in: `mmc.exe` and click **Enter** to launch the Microsoft Management Console.
2. Click **File > Add/Remove Snap-in...** and click **Add...**
3. Select **Group Policy Management Editor** snap-in and click **Add**.
4. Click **Browse...** and select the domain policy to edit.
5. Select the domain policy and click **OK**.
6. Click **Finish** to close 'Select Group Policy Object' dialog. Click **Close** to close 'Add standalone Snap-in' dialog and click **OK** to close 'Add/Remove Snap-in' dialog; to return to the Microsoft Management Console.
7. Go to **Console Root > <domain policy> > User Configuration > Policies**, right-click **Administrative Templates**, and select **Add/Remove Templates....**
8. Click **Add...**, browse for the file `GFIWebMonitorAgentSettings.adm` located in: `<Program Files>\GFI\WebMonitor\Agent` and click **Open**.

 **NOTE**

The license key value is not added to the registry when the .adm file is used. This value is taken from the server after the agent starts and communicates with the GFI WebMonitor server for the first time.

9. Click **Close** to return to the Microsoft Management Console.
10. Expand **Console Root > <domain policy> > User Configuration > Policies > Administrative Templates > Classic Administrative Templates (ADM) > GFI Applications**.
11. From the right pane, double click **GFI WebMonitor Server Location** policy and select **Enabled**. In the Server URL text box enter the URL where user machines can access GFI WebMonitor in the form `http://<hostname>/<GFI WebMonitor virtual folder name>`

 **NOTE**

When specifying the name of a machine in the domain, enter the machine name only, without the domain name. The IP address can also be used.

12. Click **OK** when all settings are configured.
13. Select **Console Root > <domain policy> > Computer Configuration > Policies > Software Settings**.
14. Right click **Software installation** and select **New > Package...**
15. In the **Open** dialog, locate the share where msi file is saved.

 **NOTE**

When selecting the location of the msi file ensure that this is done through 'My network locations' so that the share name in GFI WebMonitor includes the full network share location rather than the local path.

16. Choose the deployment option - select **Assigned** and **OK**.
17. GFI WebMonitor Agent will be installed the **Next** time each client machine is started.

How the Agent works

7.7.3 Step 3: Verify Agent installation parameters

To verify the parameters have been set up:

1. On the server where GFI WebMonitor is installed, go to **Start > Run** and type **regedit** to open the **Registry Editor**.
2. Expand **HKEY_LOCAL_MACHINE > SOFTWARE > GFI > WebMonitorAgent** for 32 bit systems and **HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > GFI > WebMonitorAgent** for 64 bit systems
3. Check the following keys: **LicenseKey**, **ServerAddress**, **ServerPort**.



NOTE

The license key value is not added to the registry when the .adm file is used. This value is taken from the server after the agent starts and communicates with the GFI WebMonitor server for the first time.

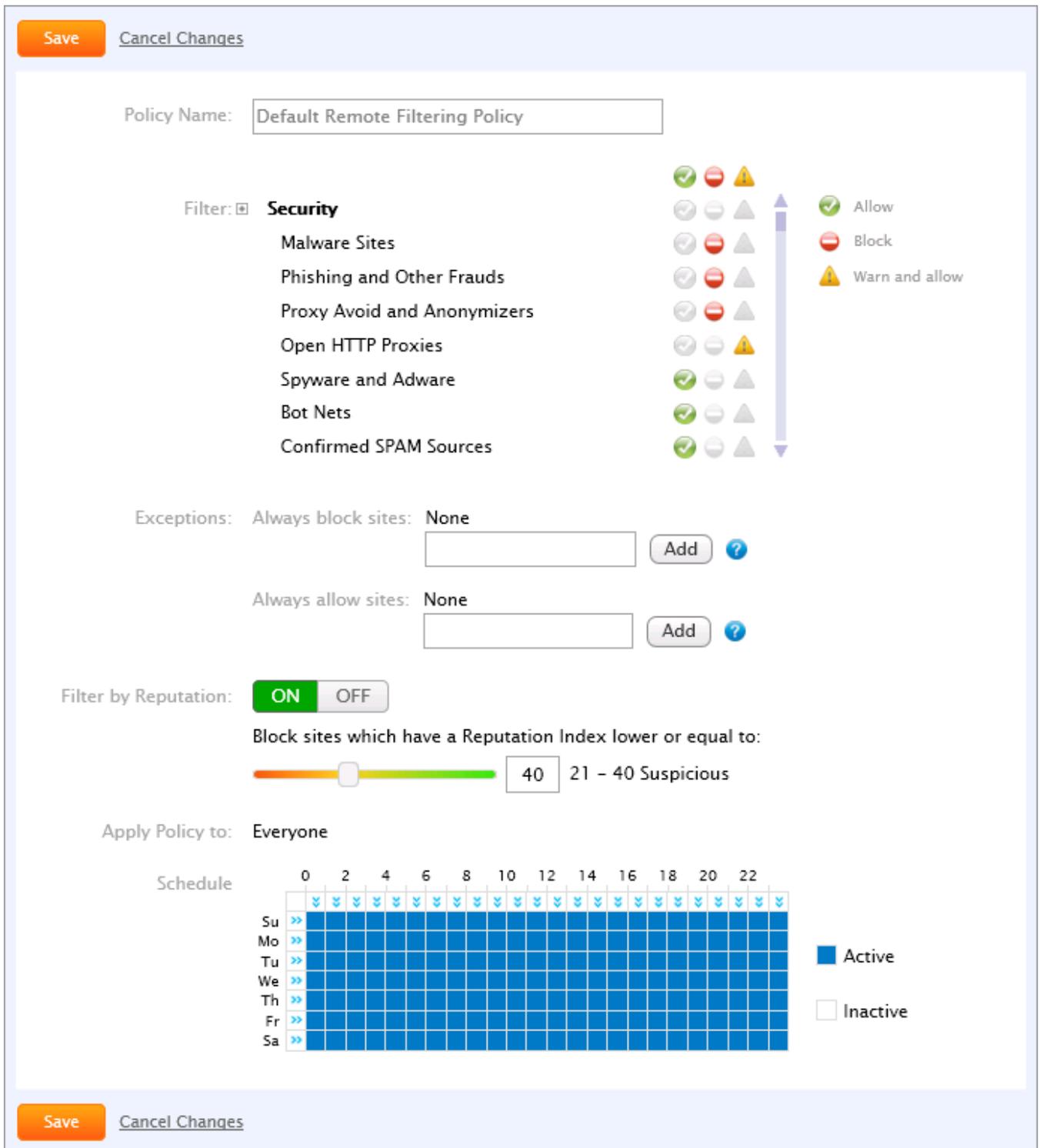
How the Agent works

7.7.4 Configuring Remote Filtering Policies

Remote Filtering Policies control Web activity on remote devices, offering the same level of web filtering protection to users who take their devices with them outside the office. New or updated Remote Filtering Policies are downloaded from the GFI WebMonitor server when the device is connected to the corporate network.

To add a Remote Filtering Policy:

1. Go to **Settings > Remote Devices**
2. In the **Remote Filtering Policies** area, click **Add Policy**.



Screenshot 41: Creating a new Remote Filtering policy

3. In the **Policy Name** field, type a policy name.
4. In the **Filter** area, select the categories to **Allow**, **Block** or **Warn and Allow**.
5. 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 42: Enabling reputation filtering

6. [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:

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

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

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

9. Click **Save**.

7.8 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](#)

7.8.1 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**.

The screenshot shows a configuration window for monitoring alerts. At the top, there are two buttons: 'Save' (orange) and 'Cancel Changes' (blue). The main area contains the following fields and options:

- Alert Name:** A text input field containing 'Monitoring'.
- Trigger base on:** Three radio buttons: 'Sites Accessed', 'Blocks', and 'Warnings Bypassed' (which is selected). There is an information icon (i) to the right.
- Threshold:** A text input field containing '10' and an information icon (i).
- Time interval:** A dropdown menu set to 'Hour' and an information icon (i).
- Apply to:** A dropdown menu set to 'Social Network' with an 'X' icon, and an 'Add' button.
- Notify:** A text input field containing 'administrator@mydomain.com' with an 'X' icon, and an 'Add' button.
- Specify UserName, Group or email address of who needs to be notified:** A note below the 'Notify' field.
- Notify user:** Two radio buttons: 'ON' (selected) and 'OFF'. To the right is a note: 'Note: The notification can only be sent if the person that triggered the alert is authenticated or the IP is mapped'.
- Message to user:** A text area containing the text 'Accessed'.

At the bottom of the window, there are two buttons: 'Save' (orange) and 'Cancel Changes' (blue).

Screenshot 43: Configuring Monitoring 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:
 - » **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**.

7.8.2 Configuring Bandwidth Alerts

To configure bandwidth alerts:

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

The screenshot shows a configuration window for a bandwidth alert. At the top, there are buttons for 'Save' (orange), 'Cancel Changes' (blue), and 'Clone Alert' (grey). The main form area contains the following fields and options:

- Alert Name:** A text input field containing 'Social Networking Alert'.
- Trigger base on:** Three tabs: 'Total Bandwidth' (selected), 'Downloads', and 'Uploads'. An information icon is to the right.
- Threshold:** A text input field with '5', a unit dropdown menu with 'MB' selected, and a frequency dropdown menu with 'Per User' selected. An information icon is to the right.
- Time interval:** A dropdown menu with 'Hour' selected. An information icon is to the right.
- Filter on:** Three tabs: 'No Filter', 'Categories' (selected), and 'Content type'.
- Apply to:** A dropdown menu with 'Social Network' selected and a close button (X). Below it is another dropdown menu with 'Malware Sites' selected and an 'Add' button.
- Notify:** A text input field with 'Administrator@mydomain.com' and a close button (X). Below it is another empty text input field and an 'Add' button.
- Specify UserName, Group or email address of who needs to be notified** (grey text instruction).
- Notify user:** Two radio buttons: 'ON' (selected, green) and 'OFF' (grey). To the right is a note: 'Note: The notification can only be sent if the person that triggered the alert is authenticated or the IP is mapped'.
- Message to user:** A text area containing the text 'Threshold has been exceeded.'

At the bottom of the form, there are buttons for 'Save' (orange), 'Cancel Changes' (blue), and 'Clone Alert' (grey).

Screenshot 44: 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:

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:

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**.

7.8.3 Configuring Security Alerts

To configure security alerts:

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

Security Alerts > Malicious content alert

Save Cancel Changes Clone Alert

Alert Name: Malicious content alert

Trigger for:

- Anti-Virus ON OFF
- Anti-Phishing ON OFF
- ThreatTrack ON OFF

Threshold: 5 ?

Time interval: Hour ?

Notify: Nobody

Add

Specify email address of who needs to be notified

Notify user: ON OFF Note: The notification can only be sent if the person that triggered the alert is authenticated or the IP is mapped

Save Cancel Changes

Screenshot 45: Configuring Security alerts

- In the **Alert Name** field, key in a name.
- In the **Trigger for** area, select any of the following 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.

- In the **Threshold** area, specify the total hits that will trigger the alert when exceeded. This setting will apply for the selected security engines.
- Specify the frequency that GFI WebMonitor checks against the specified threshold. Time intervals can be set to:
 - » Hour
 - » Day
 - » Week
- 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**.

7.9 Proxy Settings

When GFI WebMonitor is installed in Gateway or Simple Proxy mode, it acts as a proxy server that filters client requests seeking resources from other servers.

When a client requests some service, such as a file, connection, web page, or other resource from a different server, GFI WebMonitorevaluates the request according to the configured filtering rules. If the request is allowed, GFI WebMonitor provides the resource by connecting to the relevant server and requesting the service on behalf of the client.

Additionally, if caching is enabled, GFI WebMonitor saves responses from the remote server, and returns subsequent requests for the same content directly without contacting the specified server.

The following sections will help you configure advanced proxy settings to enhance performance or fine-tune GFI WebMonitor according to your organizational requirements:

- » [General Proxy Settings](#)
- » [HTTPS Proxy Scanning Settings](#)
- » [Caching Settings](#)

7.9.1 Configuring General Proxy Settings

The **General Settings** tab enables you to configure generic proxy related settings.

General Proxy Settings

General Proxy Settings ?

Proxy Server: 192.168.11.11 Port: 8080
Note: WebMonitor will always listen to web connections from this computer.

Listen on All: ON OFF Listen on network interfaces

Use WPAD: ON OFF Use Web Proxy Auto-Discovery Protocol (WPAD) for network clients to automatically detect this GFI WebMonitor server.

Publish the IP of the GFI WebMonitor proxy in WPAD
 Publish the host name of the GFI WebMonitor proxy in WPAD

Proxy Authentication: ON OFF ?

Chained Proxy: ON OFF Route traffic from GFI WebMonitor to another proxy

Screenshot 46: Configuring general proxy settings

The settings include:

OPTIONS	DESCRIPTION
Network Configuration	Listening for incoming user requests on a specific network card.
Configuring WPAD	Configuring Web Proxy Auto-Discovery Protocol (WPAD) to enable client computers to automatically detect GFI WebMonitor.
Configuring Authentication Method	Configuring the proxy authentication method.
Configuring Chained Proxy	Enabling Chained Proxy to forward web traffic received by the GFI WebMonitor machine to another proxy.

7.9.2 Network Configuration

GFI WebMonitor must be configured to listen for incoming HTTP and HTTPS requests on a specific network card.



NOTE

The settings related to the network interface card can be configured through the GFI WebMonitor Configuration Wizard. This wizard is launched automatically after installing GFI WebMonitor in standalone proxy mode.

To configure GFI WebMonitor to listen for incoming HTTP and HTTPS requests:

1. Go to **Settings > Proxy Settings > General**.
2. From the **Proxy Server** area, specify the IP address of a specific network card listening to incoming requests.
3. [Optional] Enable **Listen to All** for GFI WebMonitor to listen for incoming requests on multiple network interface cards.
4. Click **Save**.

7.9.3 Configuring WPAD

The Web Proxy Auto Discovery (WPAD) Internet protocol enables client machines to automatically retrieve proxy settings from a WPAD data file, stored on the same GFI WebMonitor machine. It is useful when you want to configure roaming devices such as laptops and tablets to use GFI WebMonitor as the proxy server when they are in the office.

To enable WPAD:

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



Screenshot 47: Configuring WPAD

2. In the **Use WPAD** field, click **ON** to enable.
3. Select one of the following options:

OPTION	DESCRIPTION
Publish the IP of the GFI WebMonitor proxy in WPAD	Select to include theGFI WebMonitor IP address in the WPAD.dat file.
Publish the host name of the GFI WebMonitor proxy in WPAD	Select to include theGFI WebMonitor host name in the WPAD.dat file.

4. Click **Save**.

7.9.4 Configure Microsoft Internet Explorer for WPAD

After enabling WPAD in GFI WebMonitor, ensure that the updated Internet settings are automatically detected by a client browser:

1. Launch **Microsoft Internet Explorer** on the client machine or device.
2. From the **Tools** menu, select **Internet Options**, then go to **Connections**.
3. Click **LAN settings**.
4. Check **Automatically detect settings** checkbox.
5. Close **LAN Settings** dialog.
6. Click **OK** to close **Internet Options** dialog.
7. Restart Internet Explorer to refresh settings.



NOTE

WPAD is supported by all major Internet browsers.

7.9.5 Configuring Proxy Authentication Method

The **Proxy Authentication** area enables you to configure the authentication method used by the proxy. This determines how client machines are validated when accessing the Internet. **Proxy Authentication** must be enabled to be able to create new polices for users or groups. By default, Proxy Authentication is disabled.

To configure user authentication method:

1. Go to **Settings > Proxy Settings > General**.
2. From the **Proxy Authentication** area, leave Proxy Authentication off if the user is not required to provide login credentials when new Internet sessions are launched.
3. If proxy authentication is required, select one of the following options:

OPTION	DESCRIPTION
Basic authentication	Select if user is required to provide login credentials when new Internet sessions are launched.
Integrated authentication	(Recommended) This option enables GFI WebMonitor proxy to authenticate users by using the client machines' access control service. User is not prompted to provide login credentials when new Internet sessions are launched. NOTE Integrated authentication is disabled if the GFI WebMonitor machine authenticates local users as Guest. The Guest only network access model grants all users the same level of access to system resources and so GFI WebMonitor proxy will not be able to differentiate between the different users using a client machine.



NOTE

On Windows® XP Pro machines that have never been joined to a Domain Controller, **Local Security Setting** policy is enabled by default.

4. [Optional] In the **IP's that will bypass the authentication** field, key in IP addresses to exclude from proxy authentication.



NOTE

IP addresses specified in this field will not be prompted to provide login credentials when new Internet sessions are launched.

5. Click **Save**.

7.9.6 Configuring Chained Proxy

Proxy Chaining is a method of connecting several proxy servers together to obtain greater anonymity. These servers act together as one proxy server to process web requests.

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

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

1. Go to **Settings > Proxy Settings > General**.
2. From the **Chained Proxy** area, click **ON** to enable GFI WebMonitor to route traffic to another proxy server.
3. Key in the proxy server IP address in the **Address** text box and key in the chained proxy's port (default 8080) in the **Port** text box.
4. [Optional] If proxy authentication requires alternate credentials, click **Alternative Credentials** and key in the required credentials in the **Username** and **Password** fields.



NOTE

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

5. [Optional] Click **Test Proxy Chaining** to test the connection between GFI WebMonitor machine and proxy server.

6. Click **Save**.

7.10 Network Access Policy Configuration

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

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

» Manually

- For more information, refer to [Manually Configuring Network Access](#) (page 114).

» Using Active Directory GPO

- For more information, refer to [Configuring Network Access via GPO in Windows® Server 2003](#) (page 114).
- For more information, refer to [Configuring Network Access via GPO in Windows® Server 2008](#) (page 114).

This information is also available in KBase article: http://go.gfi.com/?pageid=WebMon_IntegratedAuthentication

7.10.1 Manually Configuring Network Access

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

1. Navigate to **Start > Control Panel > Administrative Tools > Local Security Policy**.
2. Expand **Security Settings > Local Policies > Security Options**.
3. Right-click **Network access: Sharing and security model for local accounts** from the right panel and click **Properties**.
4. Select the **Local Security Setting** tab.
5. Select **Classic - local users authenticate as themselves** from the **Network access** drop-down list.
6. Click **Apply** and **OK**.
7. Close **Local Security Settings** dialog.
8. Close all open windows.

7.10.2 Configuring Network Access via GPO in Windows® Server 2003

To configure Network access setting on GFI WebMonitor 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**.
3. Select **Group Policy** tab in the **Domain Properties** dialog.
4. Select **Default Domain Policy** from the list and click **Edit**.
5. Expand **Computer Configuration > Windows Settings > Security Settings > Local Policies** and click **Security Options**.
6. Right-click **Network access: Sharing and security model for local accounts** from the right panel and click **Properties**.
7. In the **Security Policy Setting** tab, check **Define this policy setting** checkbox.
8. Select **Classic - local users authenticate as themselves** from the **Network access** drop-down list.
9. Click **Apply** and **OK**.
10. Close all open windows.

7.10.3 Configuring Network Access via GPO in Windows® Server 2008

To configure Network access setting on GFI WebMonitor 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.
3. Select **Group Policy Management** from the **Available snap-ins** list, and click **Add**.
4. Click **OK**.
5. Expand **Group Policy Management > Forest > Domains** and **<domain>**.
6. Right-click **Default Domain Policy** and click **Edit** to open the **Group Policy Management Editor**.
7. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies** and click **Security Options**.
8. Right-click **Network access: Sharing and security model for local accounts** from the right panel and click **Properties**.
9. In the **Security Policy Setting** tab, check **Define this policy setting** checkbox.
10. Select **Classic - local users authenticate as themselves** from the **Network access** drop-down list.
11. Click **Apply** and **OK**.
12. Close **Group Policy Management Editor** dialog and save the management console created.

7.10.4 HTTPS Proxy Scanning settings

HTTPS Scanning gives you visibility into secure surfing sessions that can threaten your network's security. Malicious content may be included in sites visited or files downloaded over HTTPS. The HTTPS filtering mechanism within GFI WebMonitor enables you to scan this traffic. There are two ways to configure HTTPS Proxy Scanning Settings, via the integrated **HTTPS Scanning Wizard** or manually.



IMPORTANT

Ensure that by enabling HTTPS Scanning, you are not violating any legal and compliance regulations.

When HTTPS inspection is enabled, two secure connections are initiated for each HTTPS session; one between the web server and the GFI WebMonitor Proxy and one between the GFI WebMonitor Proxy and the client browser.



NOTE

If HTTPS Scanning is disabled, GFI WebMonitor enables users to browse HTTPS websites without decrypting and inspecting their contents.

In both cases, for the connection to be established, the client must verify that the certificate is signed by a trusted Certification Authority (CA). This means that in order for your client machines to be able to access HTTPS sites, they need to trust the certificate used by GFI WebMonitor to sign certificates. CA certificates trusted by Windows machines are stored in the *'Trusted Root Certification Authorities'* certificate store. Export the certificate from your GFI WebMonitor and deploy it on client machines manually or through Group Policy in an Active Directory domain environment.

The following topics will guide you through the steps required to:

- » [Configure HTTPS Proxy Settings Manually](#)
- » [Configure HTTPS Proxy Scanning Settings Using Wizard](#)
- » [Create a new HTTPS Scanning certificate](#)
- » [Import an existing HTTPS Scanning certificate](#)
- » [Export an HTTPS Scanning certificate](#)
- » [Deploy an HTTPS Inspection Certificate Manually](#)
- » [Deploy an HTTPS Inspection Certificate Using GPO](#)



NOTE

It is recommended that any HTTPS website that would be inappropriate for GFI WebMonitor to decrypt and inspect is added to the HTTPS scanning exclusion list. For more information refer to [Adding Items to the HTTPS Scanning Exclusion List](#).

Configuring HTTPS Proxy settings manually

To configure HTTPS Scanning settings manually:

1. Go to **Settings > Proxy Settings > HTTPS**.

Proxy Scanning

HTTPS Proxy Scanning Settings ? Launch Wizard

HTTPS Scanning: ON OFF NOTE: Ensure that by enabling HTTPS Scanning, you are not violating any legal and compliance regulations in your jurisdiction.

Display Warning: ON OFF Display warning page to the client's web browser before GFI WebMonitor starts decrypting and inspecting HTTPS websites.

Block Non-Validated: ON OFF Block HTTPS websites with certificates that are yet to be validated.

Block Expired: ON OFF Block HTTPS websites with certificates that are expired.
 Accept up to days after expiry

Block Revoked: ON OFF Block HTTPS Websites which fail a Certificate Revocation Check against a Certificate Revocation List (CRL) issued by the Certification Authority.

Current Certificate: GFIWebMon (5/17/2014 5:00:00 PM) Export as .cer Export as .pfx
Create Certificate Import Certificate

Name:

Expiration Date:
Create

Screenshot 48: HTTPS Proxy Scanning Settings

2. In the **HTTPS Scanning** field, click **ON**.



IMPORTANT

Ensure that by enabling HTTPS Scanning, you are not violating any legal and compliance regulations.

3. In the **Display Warning** field click **ON** to display a warning page to users before GFI WebMonitor starts decrypting and inspecting HTTPS traffic .
4. In the **Block Non-Validated** area, click **ON** to start blocking HTTPS websites with certificates not yet validated.
5. In the **Block Expired** area, click **ON** to block pages that contain expired certificates. Use the **Accept up to 'x' days after expiry** field to accept websites whose certificate has expired by a number of days.
6. To block websites with revoked certificates, click **ON** next to **Block Revoked**.
7. Click **Save**.
8. In the **Current Certificate** area, view relevant information of the currently used certificate. If no certificate is currently enabled, consult the following sections that show you how to work with certificates.



NOTE

It is recommended that any HTTPS website that would be inappropriate for GFI WebMonitor to decrypt and inspect is added to the HTTPS scanning exclusion list. For more information refer to [Adding Items to the HTTPS Scanning Exclusion List](#).

Configuring HTTPS Proxy Scanning settings using wizard

The **HTTPS Scanning Wizard** is a guide to aid configuration of the following HTTPS Scanning settings:

- » HTTPS Scanning Warning page
- » Create or import certificate
- » Certificate checks
- » Export certificate

To configure HTTPS Scanning settings using the configuration wizard:

1. Go to **Settings > Proxy Settings > HTTPS**.
2. Click **Launch Wizard**.
3. Navigate through the wizard and configure the settings as required.
4. Click **Finish** to complete the HTTPS Scanning Wizard

Creating an HTTPS Scanning certificate

After decrypting HTTPS websites, GFI WebMonitor can re-encrypt these websites for secure transmission to the client browser. This is done by creating a new certificate in GFI WebMonitor or by

importing an existing certificate.



NOTE

When the certificate expires, browsing of HTTPS websites is not allowed. Renew, export and deploy the certificate again to client computers.

To create a new certificate:

1. Go to **Settings > Proxy Settings > HTTPS**
2. Click **Create Certificate**.
3. In the **Name** field, type a name for the certificate.
4. Set the expiration date and click **Create**.
5. Click **Save** to confirm your changes.

Importing an HTTPS Scanning certificate

To import an existing HTTPS Scanning certificate:

1. Go to **Settings > Proxy Settings > HTTPS**
2. Click **Import Certificate**.
3. Click **Select...** and locate the existing certificate.
4. Click **Import**.
5. Click **Save**.

Exporting an HTTPS Scanning Certificate

A created or imported certificate can be exported from GFI WebMonitor in the following file formats:

FILE FORMAT	DESCRIPTION
Personal Information Exchange file format (.pfx)	Contains the certificate data and its public and private keys. Required by GFI WebMonitor proxy to re-encrypt inspected HTTPS traffic. Ideal for backing up the certificate and its keys.
Certificate file format (.cer)	Contains the certificate data but not its private key. Ideal for deploying the certificate as a trusted certificate to the client computer.



NOTE

Keep the private key of the certificate safe to avoid unauthorized generation of trusted certificates.

 **NOTE**

It is recommended that when the certificate is not issued by a trusted Certificate Authority, it is exported from GFI WebMonitor and deployed to the client computers as a trusted certificate. For more information on how to deploy a certificate to clients' computers, refer to: http://go.gfi.com/?pageid=WebMon_HTTPSInspectionCertificate

To export an existing certificate:

1. Go to **Settings > Proxy Settings > HTTPS**
2. Click **Export as .cer** or **Export as .pfx** as required.
3. Specify the destination path of the certificate.
4. Click **Save**.

Deploy the HTTPS Inspection certificate via GPO

In order for your client machines to be able to access HTTPS sites, a trusted HTTPS Inspection certificate needs to be deployed on client computers. Use the **Export Certificate** functionality to save the certificate to disk, then deploy your certificate to multiple computers using Active Directory Domain Services and a Group Policy object (GPO). A GPO can contain multiple configuration options, and is applied to all computers that are within the scope of the GPO.

 **NOTE**

To complete this procedure you need Administrator rights.

To deploy a certificate by using GPO:

1. Open **Group Policy Management Console**.
2. Find an existing or create a new GPO to contain the certificate settings. Ensure that the GPO is associated with the domain, site, or organizational unit whose users you want affected by the policy.
3. Right-click the GPO, and then select **Edit**. Group Policy Management Editor opens, and displays the current contents of the policy object.
4. In the navigation pane, open **Computer Configuration > Windows Settings > Security Settings > Public Key Policies > Trusted Publishers**.
5. Click the Action menu, and then click **Import**.
6. Follow the instructions in the **Certificate Import Wizard** to find and import the certificate.
7. If the certificate is self-signed, and cannot be traced back to a certificate that is in the Trusted Root Certification Authorities certificate store, then you must also copy the certificate to that store. In the navigation pane, click **Trusted Root Certification Authorities**, and then repeat steps 5 and 6 to install a copy of the certificate to that store.

Deploy the HTTPS Inspection certificate manually

In order for your client machines to be able to access HTTPS sites, a trusted HTTPS Inspection certificate needs to be deployed on client computers. Use the **Export Certificate** functionality to save the certificate to disk, then deploy your certificate manually as follows:

1. Copy the exported certificate to the client machine.
2. On the client machine, go to **Start > Run > mmc.exe**
3. In the MMC window, select **File > Add/Remove Snap-in**
4. Click **Add**, select **Certificates** and click **Add**.
5. Select **Computer Account** and click **Next**.
6. Select **Local computer** and click **Finish**.
7. In the MMC, browse to **Certificates (Local Computer) > Trusted Root Certification Authorities**.
8. Right click on the node and select **All Tasks > Import**.
9. Locate the certificate copied in step 1 and import the certificate.
10. Leave the password field blank and proceed to the end of the wizard.

To verify that the certificate was successfully imported, open an Internet browser on the client machine and browse to any HTTPS site. Verify that no warnings are shown.



NOTE

Some applications or browsers (e.g. Mozilla Firefox), might have their own custom certificate store. For such applications the certificate will need to be imported to the certificate store separately. To import the certificate in Firefox, perform the following steps.

1. Go to **Tools > Options > Advanced > Encryption > View Certificates**.
2. Click **Import** and select the certificate.
3. Click **OK**.

7.10.5 Adding Items to the HTTPS Scanning Exclusion List



IMPORTANT

This information applies only to GFI WebMonitor Standalone Proxy Version.

When HTTPS inspection is enabled, by default this applies to all HTTPS sessions passing via the GFI WebMonitor Proxy. Administrators may however wish to exclude some domains, users, or client IPs from having their sessions inspected. This is achieved by adding them to the HTTPS scanning exclusion list.

Excluding Domains

1. Open `..\WebMonitor\Interface\App_Data\ProxyConfig.xml`
2. Remove `<DomainsExceptedFromHTTPSInspection />` tag
3. Add the sites exclude between a `DomainsExceptedFromHTTPSInspection` tag. For example:


```
<DomainsExceptedFromHTTPSInspection>
<string>www.domain.com</string>
<string>*.domain.com</string>
</DomainsExceptedFromHTTPSInspection >
```

4. Save file.

Excluding Users

1. Open `..\WebMonitor\Interface\App_Data\ProxyConfig.xml`

2. Remove the `<UsersExceptedFromHTTPSInspection />` tag

3. Add the users to be excluded between a `UsersExceptedFromHTTPSInspection` tag, for example:

```
<UsersExceptedFromHTTPSInspection>
<string>mydomain\user1</string>
<string>mydomain\user2</string>
</UsersExceptedFromHTTPSInspection>
```

4. Save file.

Excluding Client IPs

1. Open `..\WebMonitor\Interface\App_Data\ProxyConfig.xml`

2. Remove the `<UserIPsExceptedFromHTTPSInspection />` tag

3. Add the client IP addresses to be excluded between a `UsersExceptedFromHTTPSInspection` tag, for example:

```
<UserIPsExceptedFromHTTPSInspection>
<string>10.0.0.11</string>
<string>10.0.0.23</string>
</UserIPsExceptedFromHTTPSInspection>
```

4. Save file.



NOTE

Backup `ProxyConfig.xml` before making any changes.



NOTE

Changes are applied as soon as the file is saved.

7.10.6 Configuring Caching settings

If enabled, GFI WebMonitor caching transparently stores data so that future requests for that data are served faster. Caching helps bandwidth optimization. It is recommended that any website that is not required to be kept in GFI WebMonitor's cache, is added to the Cache exclusion list. For more information refer to: [Adding Items to the Cache Exclusion List](#).

 **NOTE**

GFI WebMonitor lets you specify the length of time to keep data from user requests in its local database. For more information, refer to [Configuring Web Activity Logging](#) (page 68).

To configure cache settings:

1. Go to **Settings > Proxy Settings > Caching**.
2. In the **Enable Caching** field, click **ON**.
3. In the **Caching Size Limit** field, specify the amount of data to keep in cache in KB.
4. [Optional] In the **Cache Path** field, specify a location where to store temporary cached files. If no path is specified cache is stored in the GFI WebMonitor installation folder.

 **NOTE**

Ensure that the path exists and that the account under which GFI WebMonitor is running has sufficient privileges. GFI WebMonitor will save to a default path if the path is either invalid or unspecified.

5. Click **Save**.

7.10.7 Adding Items to the Cache Exclusion list

 **IMPORTANT**

This information applies only to GFI WebMonitor Standalone Proxy Version.

When caching is enabled, content downloaded via HTTP is stored for future requests to the same resource, reducing bandwidth consumption. To exclude sites from having their content cached, add them to the Cache exclusion list as follows:

1. Open `..\WebMonitor\Interface\App_Data\ProxyConfig.xml`
2. Add the sites to exclude between the `CacheWhiteList` tag. For example:

```
<CacheWhiteList>
<string>1.1.1.1</string>
<string>1.1.1.1</string>
<string>your_excluded_domain.com</string>
</CacheWhitelist>
```

3. Save file.

 **NOTE**

Backup `ProxyConfig.xml` before making any changes.

**NOTE**

Changes are applied as soon as the file is saved.

**NOTE**

The following wildcards are supported:

- » * substitutes any number of characters in the string.
- » ? substitutes a single character in the string.
- » # substitutes a single digit in the string.

8 Troubleshooting and support

8.1 Introduction

This section 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. If the information in this guide does not solve your problems, refer to [SkyNet](#).

8.3 Web Forum

User to user technical support is available via the GFI [Web Forum](#).

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 [Technical support form](#) and follow the instructions on this page to submit your support request.
- » **Phone:** To obtain the correct technical support phone number for your region visit [our website](#).



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](#).

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

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 Servers)	The GFI WebMonitor DLL does not get registered and needs to be registered manually. Run the command <code>regsvr32 webmonplg.dll</code> 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.

ISSUE ENCOUNTERED	SOLUTION
<p>Users are not able to browse and/or download from the Internet after installing GFI WebMonitor in Gateway or in Simple Proxy mode.</p>	<p>After the installation, GFI WebMonitor proxy machine has to be configured to listen for incoming user requests.</p> <p>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 28).</p> <p>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</p>
<p>Client browsers are still retrieving old proxy Internet settings although the browsers are configured to automatically detect settings.</p>	<p>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.</p> <p>For more information visit: http://go.gfi.com/?pageid=WebMon_AutomaticDetection</p>
<p>Users are still required to authenticate themselves manually when browsing, even when Integrated authentication is used.</p>	<p>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.</p>

ISSUE ENCOUNTERED	SOLUTION
<p>Users using Mozilla Firefox browsers are repeatedly asked to key in credentials after installing GFI WebMonitor in Gateway or in Simple Proxy mode.</p>	<p>The server and the client machine will use NTLMv2 for authentication when:</p> <ul style="list-style-type: none"> » 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. <p>To solve this issue do one of the following :</p> <ol style="list-style-type: none"> 1. Navigate to Settings > Proxy Settings. 2. In the General Proxy Settings area, locate Use WPAD and click ON to enable. 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): <ol style="list-style-type: none"> 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. <p>Client machines (Microsoft Windows 7) using Active Directory GPO:</p> <ol style="list-style-type: none"> 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. <p>For more information visit: http://go.gfi.com/?pageid=WebMon_FirefoxIssues</p>

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 Index

A

Active Directory GPO 114, 126
Always Allowed 7, 74, 85
Always Blocked 6, 35, 62, 74, 84-85
Anonymization 39, 46, 48, 50, 52, 54, 62, 71
Anti-virus 35, 86, 93, 98, 100, 109

B

Bandwidth 5, 35-37, 39-40, 44, 50, 52, 55, 57, 60, 62, 65, 70, 74-75, 77, 105, 107, 121

C

Cache 37, 63, 71, 121-122
Chained Proxy 111, 113
Cisco ADSL Router Cisco 25
Configuration 10, 18, 20, 23, 26, 29-31, 63, 74, 92, 101, 111, 113-115, 117, 119
Console 19, 26, 28, 30, 101, 115, 119
Credentials 19, 23, 68, 77, 79, 81-82, 89, 92, 97, 101, 112-113, 126

D

Dashboard 36-37, 39-40, 44, 46, 48, 50-53, 73-74, 79
Download Control Policy 95, 97
Download Policies 74, 87, 94-95, 97
DrayTek VIGOR 25

F

FTP 29-30

G

General Options 71

H

HTTP 12, 15, 25, 29-31, 111, 122
HTTPS Scanning 115-118, 120

I

IM Control Policy 81
Installation 8, 10, 12, 19, 22, 28, 32, 63, 66, 70, 101-102, 122, 124
Integrated authentication 77, 79, 81-82, 89, 92, 97, 112-113, 125
Internet Gateway 11-13

Internet Policies 35-37, 74-75, 77, 80-81, 97
Instant Messaging and Social Control Policies 75, 79
Search Engine Policies 83
Streaming Media Policies 36-37, 81
Web Browsing Quota Policies 37-38
Web Filtering Policies 75

K

Knowledge Base 7-8, 44, 124

L

License key 28, 63, 102-103
Linksys 25
Log on as a service rights 17

M

Malware 35, 94
Microsoft ISA Server 12

N

Netgear Wireless Router 25

O

Online lookups 98, 100

P

Phishing 5, 35, 39, 48, 59, 93-94, 109
Port Blocking 15
Proxy Server 8, 12, 15, 28-31, 111

R

Remote Access Control 28, 62-65, 77, 79, 81-82, 89, 92, 97, 112
Authorization Rule 64-65
Windows Authentication 64-65, 68
Reporting 10, 36-37, 45, 47, 49, 55, 69, 98

S

Security Policies 35, 74, 87, 90, 92-94
Security Engines 87, 92
Virus Scanning Policy 87, 90
Simple Proxy 10, 12, 14, 22, 25, 110, 125
Snap-ins 19, 26, 30, 115
SonicWall 26

Spyware 7, 74

T

Technical Support 124

Temporary Allowed 7, 71, 74, 85-86

Thomson 26

Traffic Forwarding 12, 15

Troubleshooting 124

U

Unified Protection Edition 5, 11

Uninstall Information 27

W

Web Categorization 35, 41, 62-63, 73

Web Forum 124

Web traffic 7, 16, 37, 88, 91, 111, 113

WebFilter Edition 5, 11, 35, 74, 83

WebGrade Database 7-8

WebSecurity Edition 5, 11, 35, 74, 86

Wildcards 123

WPAD 31-32, 100, 111, 126

USA, CANADA AND CENTRAL AND SOUTH AMERICA

4309 Emperor Blvd, Suite 400, Durham, NC 27703, 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.co.uk

EUROPE, MIDDLE EAST AND AFRICA

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

Telephone: +356 2205 2000

Fax: +356 2138 2419

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

