



GFI[®]

GFI WebMonitor[™]

ADMINISTRATOR GUIDE

Find out how to configure GFI WebMonitor in different environments, and learn how to set up advanced features.



The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or 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 warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

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

GFI and GFI WebMonitor are trademarks or registered trademarks of GFI Software or its affiliates in the US and other countries. Any other trademarks contained herein are the property of their respective owners.

GFI WebMonitor is copyright of GFI Software Ltd. - 1999-2017 GFI Software Ltd. All rights reserved.

Document Version: 11

Last updated (month/day/year): 12/05/2017

Contents

1 Introduction	7
1.1 How GFI WebMonitor Works	8
1.2 Why monitor and control Internet usage?	9
1.2.1 Downloading GFI WebMonitor	10
1.3 Licensing information	10
2 Getting Started with GFI WebMonitor	11
2.1 System requirements	11
2.1.1 Software requirements	11
2.1.2 Hardware Requirements	13
2.1.3 GFI WebMonitor Agent System Requirements	13
2.1.4 Backup software	14
2.1.5 Anti-virus software	14
2.1.6 Firewall settings	14
2.1.7 GFI WebMonitor services	15
2.1.8 Assigning log on as a service rights	15
2.2 Deployment scenarios	16
2.2.1 Deployment in an Internet Gateway environment	17
2.2.2 Gateway mode pre-requisites	18
2.2.3 Deployment in a Simple Proxy environment	19
2.2.4 Simple Proxy Mode Pre-requisites	20
2.2.5 Port blocking	20
2.2.6 Traffic forwarding	21
2.3 Installing GFI WebMonitor	22
2.3.1 Important notes to consider before installation	22
2.3.2 Running the installation wizard	23
2.4 Using the Post-installation Configuration Wizard	25
2.5 Launching GFI WebMonitor	26
2.6 Configure browser proxy settings on the clients' machine	27
2.7 Verify that GFI WebMonitor is working correctly	29
2.8 Deploying GFI WebMonitor in a Microsoft Forefront TMG environment.	30
2.8.1 Register as a Microsoft Forefront TMG plug-in	31
2.8.2 Install as a proxy in parallel to Microsoft Forefront TMG	32
2.8.3 Installing GFI WebMonitor as a plug-in GFI WebMonitor	33
2.8.4 Installing GFI WebMonitor in parallel with Microsoft Forefront TMG	35
2.9 Upgrading from previous versions	36
2.9.1 Upgrading from GFI WebMonitor 10	36
2.9.2 Upgrading from GFI WebMonitor 2015	37
2.9.3 Upgrading from GFI WebMonitor 2013	38
2.10 Uninstall information	40
3 Using GFI WebMonitor	41
3.1 Working with Policies	41
3.2 Configuring Blacklist	43
3.2.1 Adding Items to the Blacklist	44
3.3 Configuring the Whitelist	45
3.3.1 Adding items to the Whitelist	46
3.3.2 Removing items from the Whitelist	46
3.4 Adding a new policy	46

3.4.1 Policy action; Allow, Block, Warn or Monitor	48
3.4.2 Users, Groups, IPs	49
3.4.3 Websites	49
3.4.4 Applications	50
3.4.5 File Types	50
3.4.6 Exceptions	51
3.4.7 Bandwidth Limit	51
3.4.8 Time Limit	51
3.4.9 Breacher notifications	51
3.4.10 Administrator notifications	52
3.4.11 Log Alert	52
3.4.12 Hits alert	52
3.4.13 Schedule	52
3.4.14 Policy Expiry	52
3.4.15 Logging	52
3.4.16 How to use Default Policies	53
3.4.17 How to create a new blocking policy	53
3.4.18 How to create a streaming media policy	55
3.4.19 How to create a bandwidth threshold policy	55
3.4.20 How to create a time threshold policy	56
3.4.21 Using a soft blocking policy	56
3.5 Configuring Exceptions	57
3.6 Application control	57
3.7 Security scanning policies	58
3.8 Monitoring and filtering Internet browsing	59
3.9 Editing an existing Policy	59
3.10 Cloning a Policy	60
3.11 Enabling or disabling a configured policy	60
3.11.1 Deleting a policy	60
3.11.2 Web Categorization	60
3.12 Using the Dashboards	61
3.13 Overview of Internet Activity	62
3.13.1 Product Status	62
3.14 Monitoring Bandwidth	63
3.14.1 One-click Report Functionality	64
3.15 Monitoring Activity	65
3.15.1 One-click Report Functionality	66
3.16 Monitoring Security	67
3.16.1 One-click Report Functionality	68
3.17 Monitoring Real-Time Traffic	69
3.17.1 Terminating active connections	71
3.18 Using the Quotas Dashboard	71
3.19 Monitoring Agents	72
3.19.1 Using Web Category Lookup	73
3.19.2 Reputation Index	74
3.20 Using WebInsights	74
3.21 Productivity Insights	75
3.22 Security Insights	76
3.23 Bandwidth Insights	78
3.24 Working with Reports	79
3.24.1 Editing reports	80
3.24.2 Cloning reports	82

3.24.3 Removing reports	82
3.25 Notification Center	82

4 Configuring 84

4.1 Configuring Core Settings	84
4.1.1 Connection Settings	85
4.1.2 Network Interface Configuration	86
4.1.3 Configuring WPAD	87
4.1.4 Configure Internet browser for WPAD	88
4.1.5 Configuring Proxy Authentication Method	90
4.1.6 Authentication Test (in Real-Time)	91
4.1.7 Blocking Test by Username	91
4.1.8 Configuring Chained Proxy	92
4.1.9 Configuring Transparent Proxy	93
4.1.10 Enabling Transparent Proxy	94
4.1.11 Testing Transparent Proxy	96
4.1.12 HTTPS Proxy Scanning settings	97
4.1.13 Configuring HTTPS Proxy settings	98
4.1.14 Creating a new HTTPS Scanning certificate	100
4.1.15 Importing an HTTPS Scanning certificate	101
4.1.16 Exporting an HTTPS Scanning Certificate	101
4.1.17 Deploy the HTTPS Inspection certificate via GPO	102
4.1.18 Deploy the HTTPS Inspection certificate manually	103
4.1.19 Adding Items to the HTTPS Scanning Exclusion List	104
4.1.20 Configuring Databases	105
4.1.21 Admin Credentials for GFI WebMonitor Services	108
4.1.22 Updating Admin Credentials from services.msc	109
4.1.23 Configuring Email distribution settings for notifications	110
4.1.24 Configuring SMTP Settings for webmail accounts	111
4.2 Advanced Settings	112
4.3 Licensing and subscription details	113
4.3.1 Updating the license	114
4.3.2 Configuring a Licensing Exclusion List	114
4.4 UI Access Control	115
4.4.1 Configuring Windows Authentication	116
4.4.2 Add a new authorization rule	117
4.5 Configuring Activity Logging	118
4.6 Configuring Anonymization	119
4.7 Language settings	120
4.8 Configuring Security Engines	121
4.8.1 Configuring Kaspersky	123
4.9 Configuring WebGrade updates	124
4.10 Configuring system updates	125
4.11 Configuring search engine options	126
4.12 Configuring Caching settings	127
4.12.1 Adding Items to the Cache Exclusion list	128
4.13 Configuring the GFI WebMonitor Agent	129
4.13.1 Agent System Requirements	130
4.14 Downloading the GFI WebMonitor Agent	130
4.15 How the GFI WebMonitor Agent works	131
4.15.1 In internal mode:	131
4.15.2 In external mode:	132
4.16 Installing the WebMonitor Agent Manually	132

4.17 Installing the GFI WebMonitor Agent via GPO in Windows Server 2008	133
4.17.1 Step 1: Creating a distribution point	133
4.17.2 Step 2: Installing GFI WebMonitor Agent via GPO in Windows Server 2008	133
4.17.3 Step 3: Verify Agent installation parameters	134
4.18 Installing the GFI WebMonitor Agent via GPO - Windows Server 2008 R2 or later	135
4.18.1 Step 1: Prepare the software to install	135
4.18.2 Step 2: Configure the ADM file	136
4.18.3 Step 3: Configure the GFI WebMonitor server location	136
4.19 Configuring Remote Policies	137
4.20 Edit existing Remote Policies	137
4.21 Using the Settings Importer tool	138
4.21.1 Export settings to a chosen file/folder	139
4.21.2 Import settings from a file	139
4.21.3 Import settings from a folder	141
4.22 Configuring client's proxy settings	142
4.22.1 Configuring GFI WebMonitor machine as the Default Proxy using GPO	142
4.22.2 Disabling Internet connections page via GPO	143
5 Troubleshooting and support	145
5.1 Unable to browse	145
5.2 Policies are not applied	146
5.3 Old proxy settings detected	146
5.4 Blank Real-time dashboard	147
5.5 Page is not loading properly	147
5.6 Whitelist is not working	147
5.7 Certain HTTPS sites do not load	148
6 Glossary	149
7 Index	155

1 Introduction

GFI WebMonitor® is a comprehensive Internet usage monitoring solution. It 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 and other bandwidth consuming activities, 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 control over browsing and downloading habits. At the same time, it enables you to ensure legal liability and best practice initiatives without alienating network users.

For a 30 days trial plan see <http://go.gfi.com/?pageid=webmonhelp#cshid=thirtydaytrial>.

1.1 How GFI WebMonitor Works

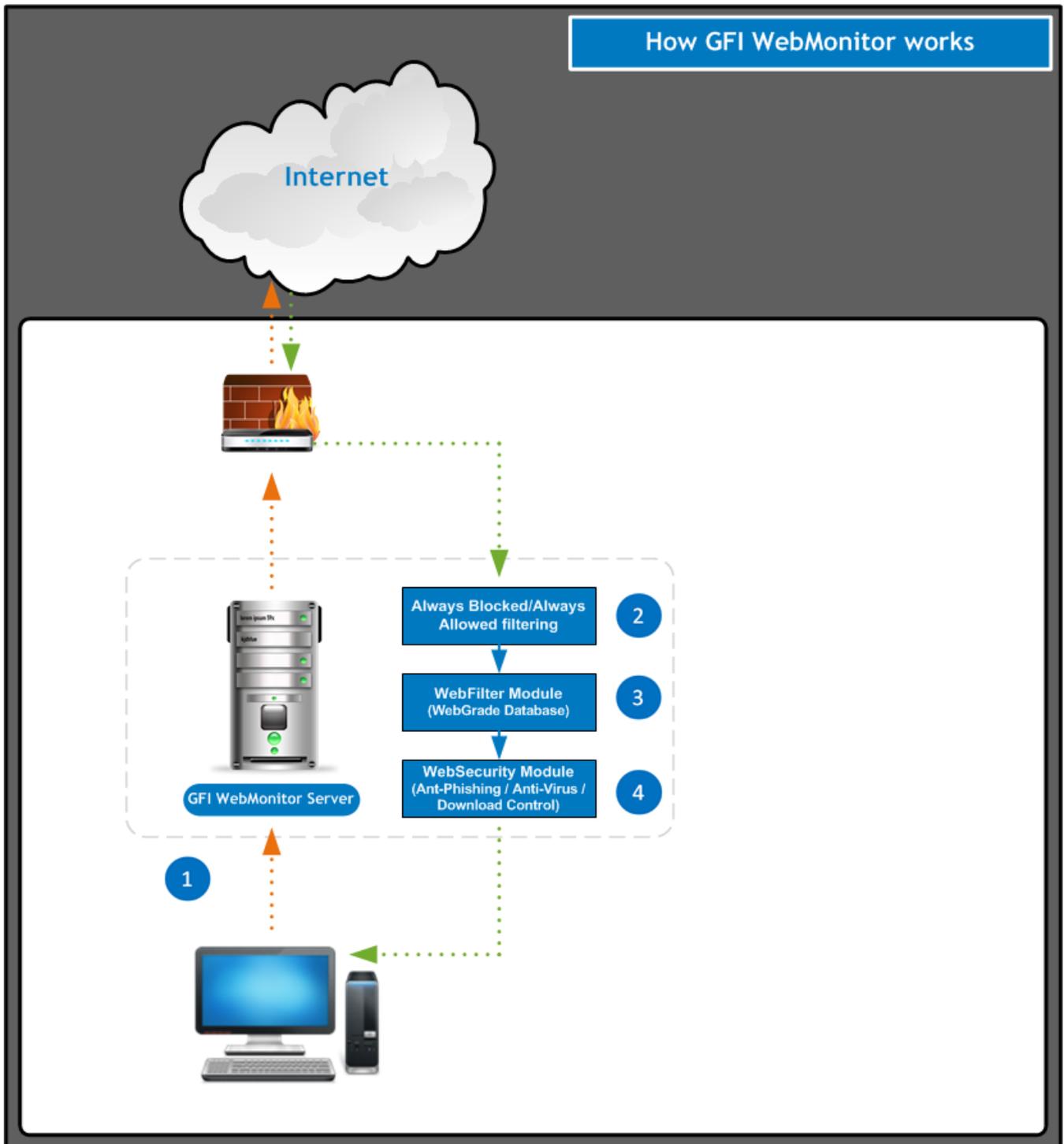


Figure 1: How GFI WebMonitor Works

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.

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.

1.2 Why monitor and control Internet usage?

Avoid legal liability by:

- » blocking access to problem sites such as gambling, pornography, and hacking
- » making sure pirated software or copyrighted media are not downloaded to company computers.

Ensure that employees are always safe from the most recent online security risks:

- » hidden malware
- » websites that exploit software vulnerabilities
- » phishing attacks that steal personal and company data
- » other online threats.

Improve productivity by:

- » monitoring Internet activity
- » identifying problem websites and applications (social networks, news, webmail),
- » filtering streaming media, categories or users
- » introducing more sensible control.

Make better use of your bandwidth by:

- » identifying any network bottlenecks (video sharing sites, online file storage and streaming media)
- » applying some limits to conserve resources as necessary.

1.2.1 Downloading GFI WebMonitor

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

1.3 Licensing information

GFI WebMonitor requires a license for every user (or IP address) that needs to be monitored. You can configure a list of users or IP addresses that do not need to be monitored or protected so that these users do not consume a license.

This can be done by configuring an **Exclusion list** through the Configuration Wizard or from **Settings > Licensing**. For more information, refer to [Configuring a Licensing Exclusion List](#) (page 114).

NOTES

- » Adding users or IPs to the default Whitelist policy excludes users from being monitored. However they still consume a license. For more information, refer to [Configuring the Whitelist](#) (page 45).
- » GFI WebMonitor for TMG and GFI WebMonitor Standalone Proxy use two different sets of license key that are not interchangeable between them. Contact your reseller if you need to shift between these two modes.

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

For further reading refer to:

[Licensing and subscription details](#)

2 Getting Started with GFI WebMonitor

Want to try out GFI WebMonitor? This topic provides a quick list of actions to help you set up a GFI WebMonitor account.

1 Sign up to GFI WebMonitor

Go to http://go.gfi.com/?pageid=webmon_trial and sign up for GFI WebMonitor. Follow the instructions to create your account and download your trial version. A 30-day evaluation key will be sent to you by email within a few minutes.

2 Prepare your GFI WebMonitor server

Before installing GFI WebMonitor on your test proxy server, ensure that the following guidelines are met:

- » [System requirements](#)
- » [Simple Proxy Mode requirements](#)
- » [Gateway Mode requirements](#)

3 Install GFI WebMonitor

Installing GFI WebMonitor is easy. You just need to follow the steps in the following topic: [Installing in a Simple Proxy environment](#). Run the installer as a user with administrative privileges on the target machine.

4 Post-installation setup

After performing the installation, use the Configuration Wizard to configure GFI WebMonitor for first use. For more information, refer to [Using the Post-installation Configuration Wizard](#) (page 25).

5 Redirect Internet traffic through the GFI WebMonitor server

GFI WebMonitor acts as a Proxy Server to provide a connection between your internal network and the Internet. This means that traffic from client machines needs to be redirected through the GFI WebMonitor server. GFI WebMonitor offers different options on how to route client traffic:

- » [Manual configuration of the users' browser settings](#)
- » [WPAD to automatically retrieve proxy settings](#)
- » [Transparent Proxy to monitor and control HTTP and HTTPS traffic transparently](#)

6 Test your GFI WebMonitor installation

Perform some tests to ensure GFI WebMonitor is working correctly. For more information, refer to [Verify that GFI WebMonitor is working correctly](#) (page 29).

7 Configure GFI WebMonitor for Trial

Configure monitoring and controlling policies that enable GFI WebMonitor to do the job it was designed to do. For more information, refer to [Working with Policies](#) (page 41).

For more detailed information on how to configure advanced settings refer to the [Administrator Guide](#).

8 Start the 30 day trial

The best way to approach your trial is in a number of phases that help you evaluate the benefits of GFI WebMonitor in 30 days. For a step by step guide on how to make the most out of your trial refer to the 30 Day Trial Guide. For more information refer to <http://manuals.gfi.com/en/webmon11/#cshid=1031>

2.1 System requirements

Before installing GFI WebMonitor, ensure the system meets or exceeds the below requirements. If these requirements are not met, you may encounter problems during installation or in functionality.

2.1.1 Software requirements

Supported operating systems

Install GFI WebMonitor on any of 64-bit versions of the operating systems listed below.

Operating system	Supported editions and notes
Windows Server® 2016	Supported editions: Standard, Datacenter & Essentials
Windows Server® 2012 R2	Supported editions: Standard, Datacenter & Essentials
Windows Server® 2012	Supported editions: Standard, Datacenter & Essentials
Windows Server® 2008 R2	Supported editions: Standard & Enterprise
Windows Server® 2008	Supported editions: Standard & Enterprise.
Windows® SBS 2011	Supported editions: Standard & Premium
Windows® SBS 2008	Supported edition: Standard
Windows® 10	Supported editions: Pro & Enterprise
Windows® 8 and 8.1	Supported editions: Pro & Enterprise
Windows® 7	Supported editions: Ultimate, Enterprise & Professional
Windows® Vista SP2 or later	Supported editions: Ultimate, Enterprise & Business Note: Transparent Proxy mode is not supported on this operating system.

NOTE

Next version of GFI WebMonitor will drop the support for some Operating Systems. For further information refer to <https://www.gfi.com/support/products/gfi-webmonitor/Changes-in-System-Requirements>

Supported backend database

GFI WebMonitor uses a backend database to store historical data that is used for reporting. GFI WebMonitor may have one of the backend databases listed below.

Database type	Notes
Firebird database	This version is included with the installation of GFI WebMonitor. It is meant for evaluation purpose only. Use SQL Server® when installing GFI WebMonitor in a production environment.
SQL Server® Express 2005 or later	This is a free version of the SQL Server®. It is advisable to adjust the activity logging limit for large installations. For more information, refer to Configuring Activity Logging (page 118).
SQL Server® 2005 or later	This is a licensed version of SQL Server®. If this is already available, you can use for GFI WebMonitor.

Supported Internet browsers

Any client browser that supports proxy settings can be used to browse the Internet. However, to display block / warn messages properly, one of the above browsers is required.

Server side
Microsoft Internet Explorer (v10 or later)
Microsoft Edge
Google Chrome (v36 or later)
Mozilla Firefox (v31 or later)

Client side

Microsoft Internet Explorer (v10 or later)

Microsoft Edge

Google Chrome (v36 or later)

Mozilla Firefox (v31 or later)

Safari

Other required components

Component	Environment
Microsoft® .NET Framework 4.5.2	Required by GFI WebMonitor. If not found, this is automatically installed by GFI WebMonitor during installation.
IIS Express	Required to run the interface. If not found, this is automatically installed by GFI WebMonitor during installation.
Routing and Remote Access Service (RRAS)	Required when using GFI WebMonitor in Gateway mode. For more information, refer to Deployment in an Internet Gateway environment (page 17).
Report Viewer	Required to run the reports properly. If not found, this is automatically installed by GFI WebMonitor during installation.
Visual C++ 2013 Redistributable	Required to run some internal engines. If not found, this is automatically installed by GFI WebMonitor during installation.

2.1.2 Hardware Requirements

Install GFI WebMonitor on a server with the following minimum specifications.

Component	Minimum hardware requirements
Processor	2.0 GHz (multi-core recommended)
Memory	8 GB RAM
Physical storage	24 GB of available disk space.

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.

Other Hardware

Component	Hardware requirements
Network card	» 2 network interface cards when installing in Gateway Mode » 1 network interface card required when installing in Simple Proxy Mode .
Router	A Router or gateway that supports traffic forwarding or port blocking when installing in Simple Proxy Mode .

2.1.3 GFI WebMonitor Agent System Requirements

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.

Agent Hardware

Component	Minimum hardware requirements
Memory	1 GB RAM
Physical storage	500 MB of available disk space

Agent Operating System

Operating system (32-bit or 64-bit)	Supported editions
Windows® 10	Pro & Enterprise
Windows® 8 and 8.1	Pro & Enterprise
Windows® 7	Ultimate, Enterprise & Professional
Windows® Vista SP2 or later	Ultimate, Enterprise & Business

2.1.4 Backup software

Backup software can cause GFI WebMonitor to malfunction if GFI WebMonitor is denied access to some of its files.

Backup GFI WebMonitor installation files only when GFI WebMonitor services are not running. From the Services applet, stop the following services before taking a backup:

- » GFI Proxy
- » GFI WebMonitor Core Service

2.1.5 Anti-virus software

Anti-virus software causes GFI WebMonitor to malfunction if GFI WebMonitor is denied access to some of its files. Add an anti-virus exclusion that prevents the anti-virus engine from scanning the GFI WebMonitor installation folder.

2.1.6 Firewall settings

Configure your firewall to allow connections from GFI WebMonitor server on the following ports:

Port	Protocol	Description
80	TCP	The default port to connect to client machines using HTTP. GFI WebMonitor downloads updates from the following locations: <ul style="list-style-type: none">» webmonupdate.gfi.com» gfi-downloader-137146314.us-east-1.elb.amazonaws.com» cdnupdate.gfi.com» update.gfi.com
443	TCP	The default port to connect to client machines using HTTPS.
8080	TCP	The default port used by the proxy.
8081	TCP	The default port used by the proxy when GFI WebMonitor is installed in parallel with Microsoft Forefront TMG.
8082	TCP	The default port used by the proxy when transparent proxy is enabled.
5996	TCP	The default port to communicate with the GFI WebMonitor Agent.

2.1.7 GFI WebMonitor services

The table below lists the GFI WebMonitor services that are created during installation. Note that these services run using an account with administrative privileges. For more information, refer to [Admin Credentials for GFI WebMonitor Services](#) (page 108).

Service name	Description	Account
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. NOTE This service is not created when installing GFI WebMonitor as a plug-in for Microsoft Forefront TMG.	Local System
GFI WebMonitor Core Service	The GFI WebMonitor Core Service is used 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	Member of Domain Admin group. Account needs access to AD.

NOTE

During product updates the GFI WebMonitor services need to be stopped and restarted. This action disrupts Internet connections going through GFI WebMonitor. Internet usage can resume once the services are restarted.

To view status of GFI WebMonitor services:

1. On the GFI WebMonitor server, click **Start > Run** and key in "services.msc"
2. From the list of services displayed locate the following services:
 - GFI Proxy
 - GFI WebMonitor Core Service

2.1.8 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® Vista/7/8

1. Go 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. Go 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 via GPO in Windows® Server 2008 or later

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

1. In the command prompt key in `mmc .exe` and press **Enter**.
2. In the **Console Root** window, go 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.

2.2 Deployment scenarios

The method of deployment depends on the network infrastructure and the network role of the machine where GFI WebMonitor is to be installed. GFI WebMonitor can be deployed in the following modes:

Mode	Description
Simple Proxy mode	Routes client HTTP traffic through GFI WebMonitor and non-HTTP traffic through a separate router. This setup requires an Internet facing router with port blocking and traffic forwarding capabilities.

Mode	Description
Gateway mode	Choose this mode if installing GFI WebMonitor on a server that is configured as an Internet gateway. All outbound and inbound client traffic (HTTP and non-HTTP) is routed through GFI WebMonitor. When GFI WebMonitor is deployed in this mode, you can enable Transparent Proxy, eliminating the need to set client browser settings to point to a specific proxy. For more information, refer to Configuring Transparent Proxy (page 93).
In parallel with Microsoft Forefront TMG	When installing GFI WebMonitor it can be configured to operate in parallel to Microsoft Forefront TMG. Use this setup to keep Microsoft Forefront TMG as a firewall and use the same machine to perform web filtering by GFI WebMonitor. This setup also provides an alternative when it is not possible to add another dedicated machine in the network just for GFI WebMonitor.
As Plug-in for Microsoft Forefront TMG	GFI WebMonitor 10 SR1 and later editions can be installed as a plug-in for Microsoft Forefront TMG. Use this setup when you want to keep the Microsoft Forefront TMG Server as the primary proxy server and use only the filtering capabilities of GFI WebMonitor. GFI WebMonitor features are not available when installing in this mode.

2.2.1 Deployment in an Internet Gateway environment

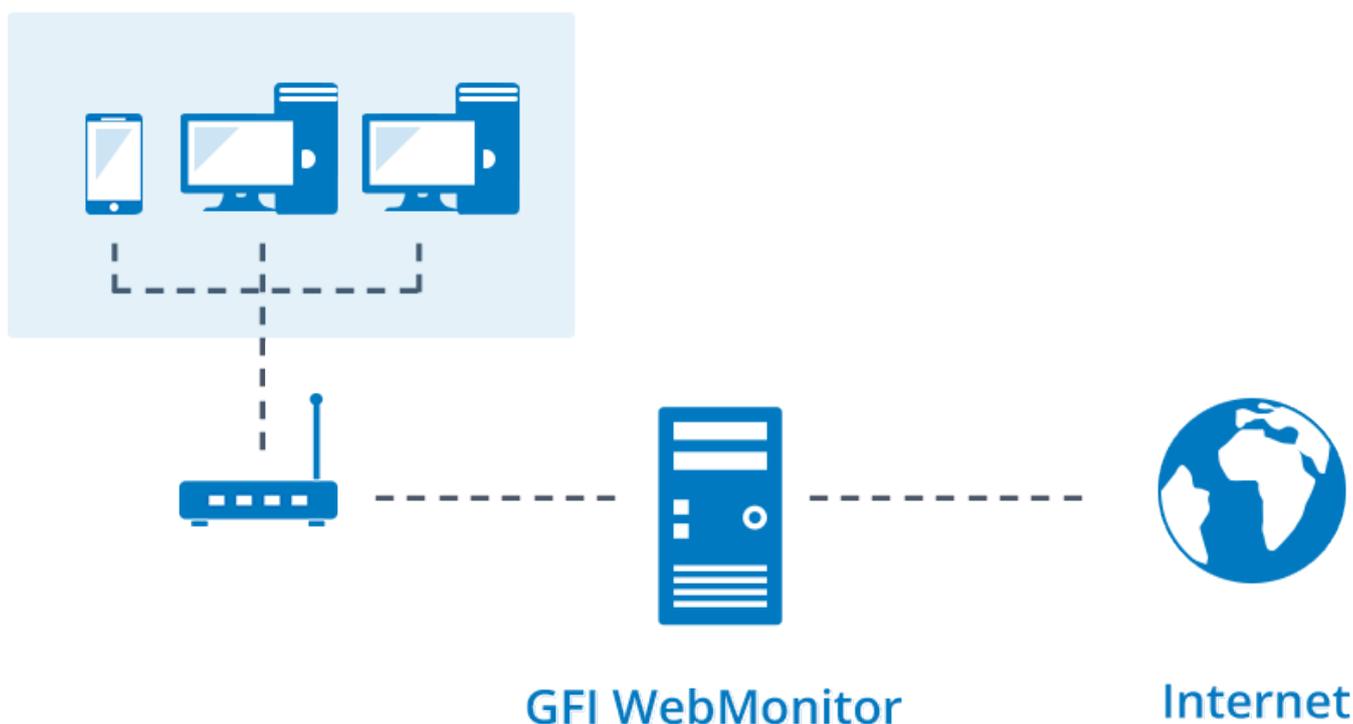
Install GFI WebMonitor in Gateway mode to use GFI WebMonitor as a trusted agent that can access the Internet on behalf of client computers. All outbound and inbound client traffic is routed through the GFI WebMonitor gateway.

NOTES

- » To configure GFI WebMonitor in Gateway mode, you need a server with two network cards. The option to configure GFI WebMonitor in Gateway mode is grayed out if only one network card is detected.
- » This feature is not available when GFI WebMonitor is installed as a plug-in for Microsoft Forefront TMG.

During the Configuration Wizard, you are asked to specify the Internal network interface card, and by default, WebMonitor will bind to it on port 8080.

Your Network



Screenshot 1: GFI WebMonitor installed on a gateway machine

In this scenario, GFI WebMonitor is installed on the gateway machine, and all network traffic passes through GFI WebMonitor. However only HTTP and HTTPS traffic are filtered.

The Gateway mode supports three types of proxy configuration:

Proxy configuration	Description
Transparent Proxy	When Transparent Proxy is enabled, GFI WebMonitor automatically enforces the client machine to use the proxy for Internet access and no further configuration on the clients are required. For more information, refer to Configuring Transparent Proxy (page 93).
WPAD	WPAD broadcasts the proxy settings to the browsers using a JavaScript file. When this option is enabled, the browser on the client machine must have their settings configured to automatically detect a proxy. For more information, refer to Configure Internet browser for WPAD (page 88).
Manual settings	The clients' browser can be set manually to use the proxy server. This option can be very convenient during evaluation and troubleshooting situations. For more information, refer to Configure browser proxy settings on the clients' machine (page 27).

2.2.2 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 2008 or later.

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

2.2.3 Deployment in a Simple Proxy environment

Install GFI WebMonitor in Simple Proxy mode if you want to route client HTTP traffic through GFI WebMonitor and non-HTTP traffic through a separate router. To select this mode, ensure that:

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

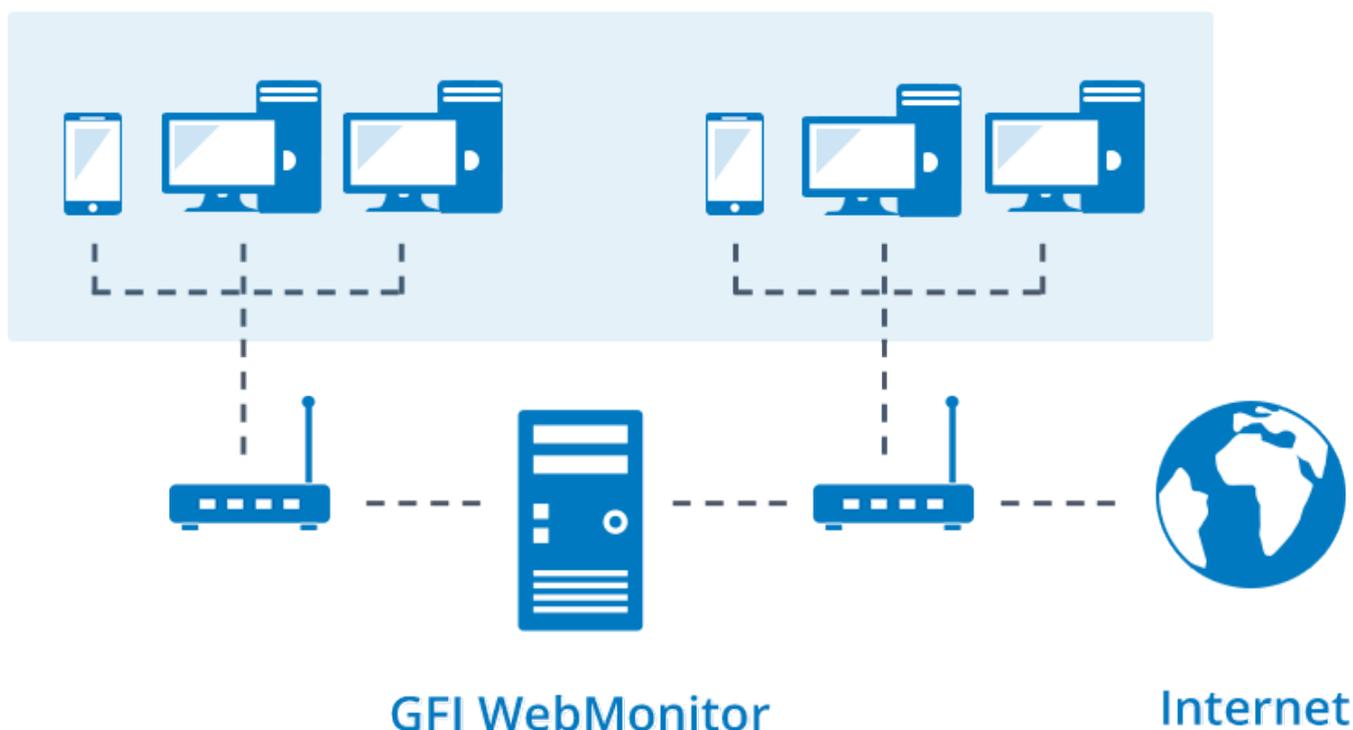
NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

IMPORTANT

The Transparent Proxy feature cannot be enabled when GFI WebMonitor is deployed in Simple Proxy mode. For more information, refer to [Configuring Transparent Proxy](#) (page 93).

Your Network



Screenshot 2: GFI WebMonitor installed in Simple Proxy mode

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.

The Simple Proxy mode supports two types of proxy configuration:

Proxy configuration	Description
WPAD	WPAD broadcasts the proxy settings to the browsers using a JavaScript file. When this option is enabled, the browser on the client machine must have their settings configure to automatically detect a proxy. For more information, refer to Configure Internet browser for WPAD (page 88).
Manual settings	The clients' browser can be set manually to use the proxy server. This option can be very convenient during evaluation and troubleshooting situations. For more information, refer to Configure browser proxy settings on the clients' machine (page 27).

2.2.4 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.

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

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

2.2.5 Port blocking

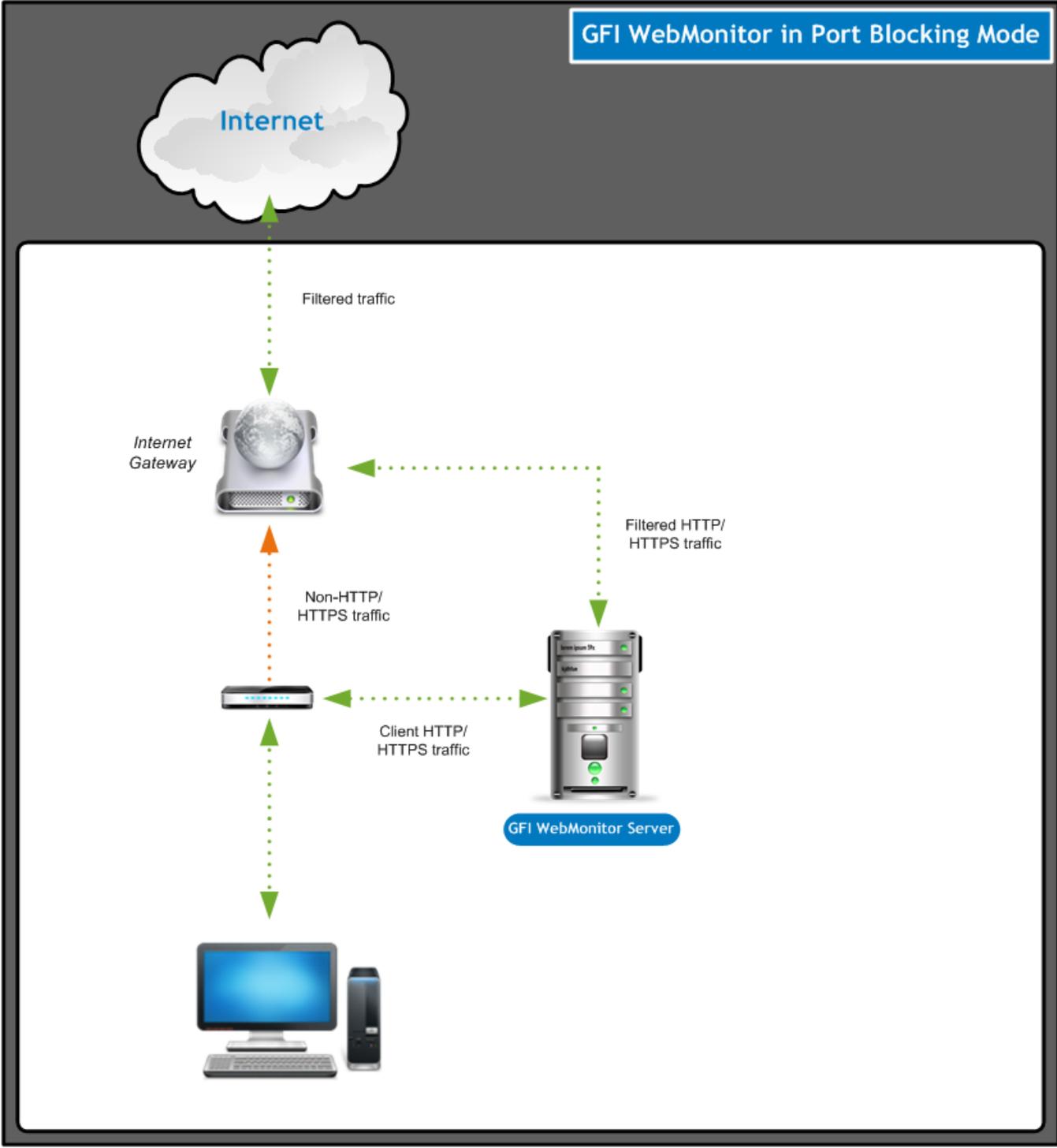
The router must be configured to allow both HTTP/HTTPS traffic generated from GFI WebMonitor machine and Non-HTTP/HTTPS traffic generated from client machines. In addition, it must also block HTTP/HTTPS traffic generated from client machines.

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

NOTE

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

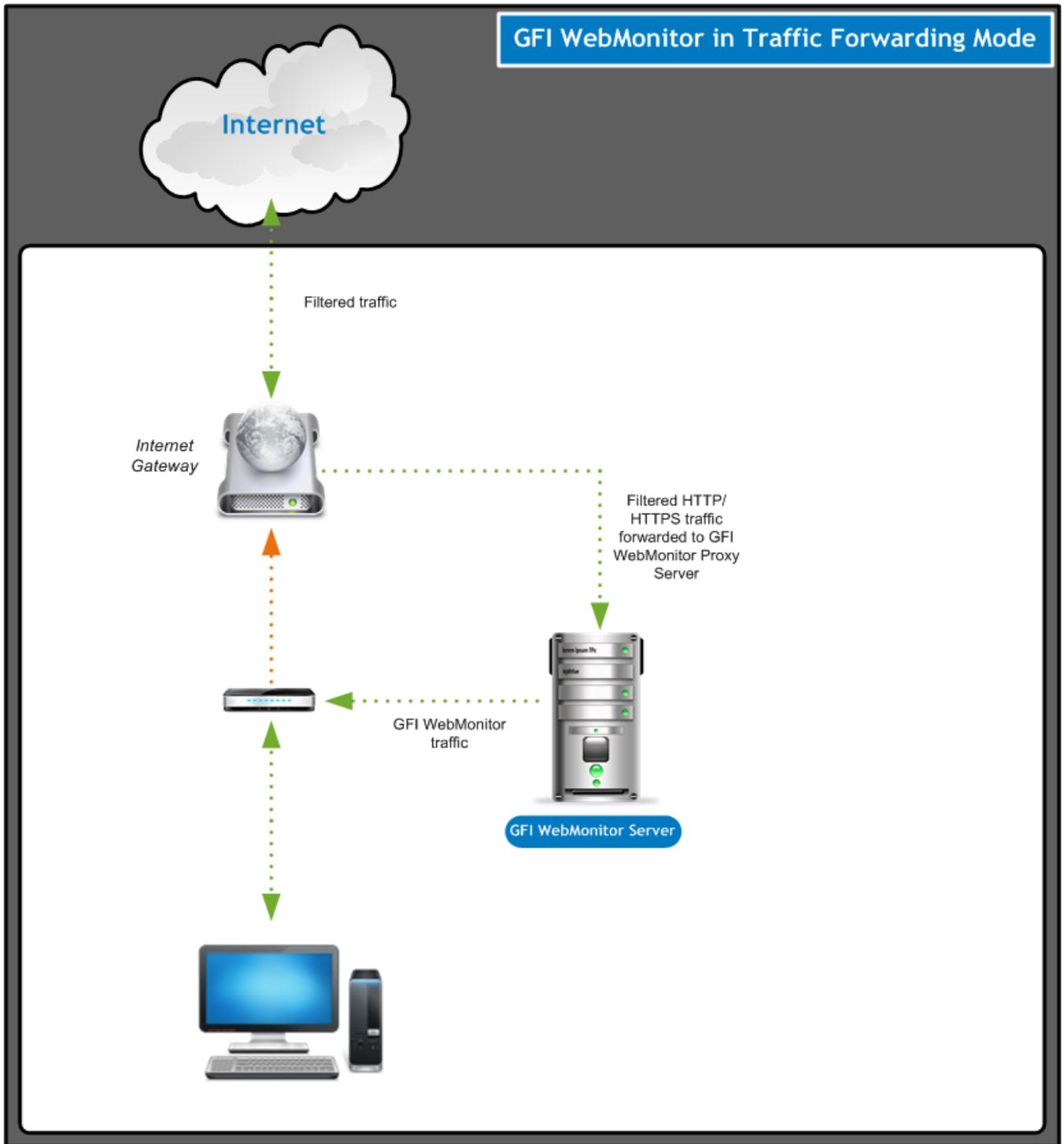


Screenshot 3: GFI WebMonitor installed on a proxy machine connected to a router supporting port blocking

2.2.6 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.

NOTE
This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.



Screenshot 4: 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](#).

2.3 Installing GFI WebMonitor

This section describes how to run the installation of GFI WebMonitor.

2.3.1 Important notes to consider before installation

Before running installation wizard, ensure that:

- » You are logged on using an account with administrative privileges.
- » The machine where GFI WebMonitor is going to be installed, meets the specified system requirements. For more information, refer to [System requirements](#) (page 11).
- » The listening port (default 8080) is not blocked by your firewall.
- » If you are currently using a previous version of GFI WebMonitor, you can upgrade your current installation while at the same time retaining all your existing configuration settings. For more information, refer to [Upgrading from previous versions](#) (page 36).
- » A license key is required. Register for a [GFI WebMonitor trial](#) to get an evaluation key or log in to the [GFI Customer Area](#) if you already have a key.
- » Disable third-party antivirus and backup software from scanning the installation folder of GFI WebMonitor.
- » Save any pending work and close all open applications on the machine.
- » On installation GFI WebMonitor performs a number of operations that require high CPU usage and downloads a large volume of updates. It is recommended to install GFI WebMonitor during off-peak hours and leave it overnight to perform these actions.

2.3.2 Running the installation wizard

1. Logon using administrator credentials on the machine where you want to install GFI WebMonitor.
2. Right-click the GFI WebMonitor installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.
3. Launch the GFI WebMonitor installer.
4. Ensure you have no Windows programs running and click **Next**.
5. The installer checks if required components are installed, and automatically installs missing components.



Screenshot 5: Missing pre-requisites are installed by the install wizard.

6. Choose whether you want the installation wizard to search for a newer build of GFI WebMonitor on the GFI website and click **Next**.
7. Read the licensing agreement. To proceed with the installation select **I accept the terms in the license agreement** and click **Next**.
8. Key in the user name or IP address of users that need administrative access to the GFI WebMonitor web interface and click **Next**. Access can be managed later on from **Settings > Advanced Settings > UI Access Control**.



Screenshot 6: Configuration node of users and IPs with access to the configuration.

NOTE

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

9. Specify the Installation Folder where GFI WebMonitor will be installed. The default path is `C:\Program Files\GFI\WebMonitor\`. Click **Next**.

10. When installing GFI WebMonitor in the Microsoft Forefront TMG server, choose the type of Microsoft Forefront TMG installation mode. For more information, refer to [Deploying GFI WebMonitor in a Microsoft Forefront TMG environment](#). (page 30). Choose between these two options and click **Next**.

Option	Description
Register as Microsoft Forefront TMG plug-in	Use this option if you want to keep Microsoft Forefront TMG as proxy and use GFI WebMonitor only for web filtering. In this setup, you have GFI WebMonitor working as a plug-in of the Microsoft Forefront TMG Server. For more information, refer to Installing GFI WebMonitor as a plug-in GFI WebMonitor (page 33).
Install as a proxy in parallel to Microsoft Forefront TMG	Use this option to have GFI WebMonitor installed as the proxy running in parallel with Microsoft Forefront TMG. In this setup you have two independent software running in parallel. For more information, refer to Installing GFI WebMonitor in parallel with Microsoft Forefront TMG (page 35).

11. Click **Install** to start the installation, and wait for the installation to complete.
12. Click **Finish** to finalize setup.
13. After the installation, the GFI WebMonitor Configuration Wizard is launched automatically when opening the Interface for the first time. For more information, refer to [Using the Post-installation Configuration Wizard](#) (page 25).

2.4 Using the Post-installation Configuration Wizard

After performing the installation, use the Configuration Wizard to configure GFI WebMonitor for first use. In the welcome screen, click **Get started**. The wizard guides through the following steps:

Options	Description
Configure connection settings	<p>Choose your Network Mode depending on your current network setup. Establish a connection between your internal network and the Internet through the GFI WebMonitor server.</p> <p>NOTE This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.</p>
Enable Transparent Proxy	<p>Enable Transparent Proxy to monitor and control HTTP and HTTPS traffic transparently. When a user makes a request to a web server, the Transparent Proxy intercepts the request to deliver the requested content. When GFI WebMonitor is deployed in this mode, you do not need to set client browser settings to point to a specific proxy.</p> <p>NOTE Transparent Proxy can only work in Gateway Mode. It does not work not work in Simple Proxy mode or when GFI WebMonitor is installed as a plug-in for TMG.</p>
Enter your License key	<p>Key in a valid license to use GFI WebMonitor. This can either be a trial license or a regular license key obtained on renewal.</p>
Configure HTTPS Scanning	<p>Configure HTTPS scanning to monitor and block encrypted traffic.</p> <p>NOTE Ensure that by enabling HTTPS Scanning you are not violating any laws in your jurisdiction or any compliance regulations for your industry.</p> <p>NOTE This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.</p>
Set up the Database	<p>Configure the database to use with GFI WebMonitor where collected data is stored. Use the Firebird database only during the evaluation period. It is highly recommended to switch to a Microsoft SQL Server based database for live systems.</p>
Define Admin Credentials	<p>Key in the admin credentials required by the GFI WebMonitor services to control internal security engines, manage updates, send notifications and control data displayed in the User Interface. The GFI WebMonitor services are Windows services installed automatically during installation and require administrative privileges to operate.</p>
Setup Email notification settings	<p>Provide the email addresses required by GFI WebMonitor to send messages containing information related to tasks such as auto-updates and licensing issues.</p>
Configuring Internet Browsers to use a Proxy Server	<p>If you have not configured WPAD or Transparent Proxy, ensure that proxy settings of client machines are configured to use GFI WebMonitor as the default proxy. This ensures that Internet traffic is routed through GFI WebMonitor.</p> <p>NOTE This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.</p>

NOTE

The Configuration Wizard is launched automatically after installing GFI WebMonitor or manually from the **Settings** menu.

2.5 Launching GFI WebMonitor

On the same machine where GFI WebMonitor is installed:

There are two options for launching the GFI WebMonitor Management Console:

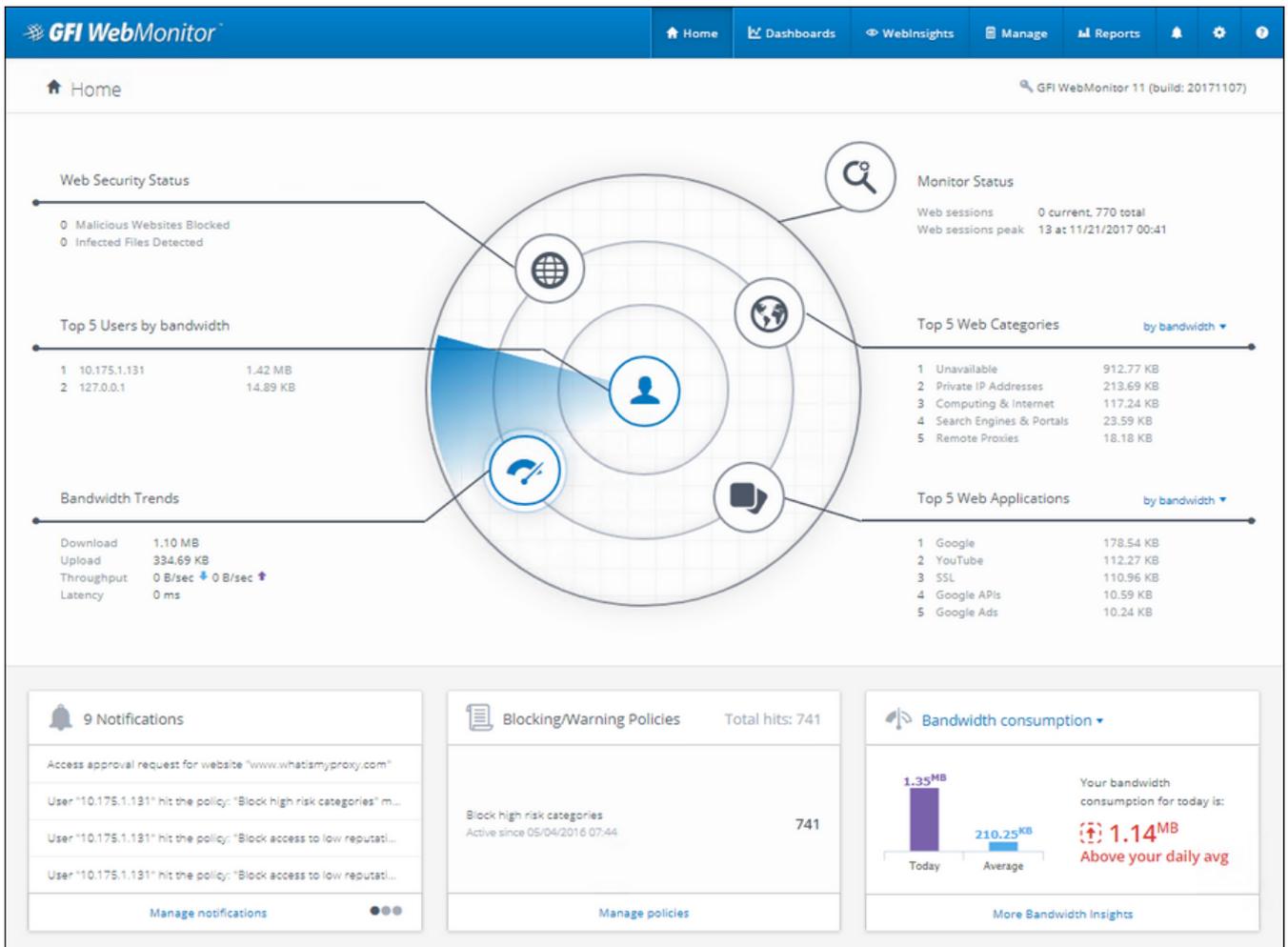
- » **Option 1:** click **Start > All Programs > GFI WebMonitor > GFI WebMonitor Management Console**
- » **Option 2:** Key in the URL <http://1.1.1.1> or <http://127.0.0.1:1007> in a web browser on the same machine.

NOTE

If using the GFI WebMonitor through the web browser interface on the same machine, Internet browser must be configured to use a proxy server. For <http://127.0.0.1:1007> disable **Bypass proxy server for local addresses** from Internet options. For more information, refer to [Configure browser proxy settings on the clients' machine](#) (page 27).

IMPORTANT

In <http://127.0.0.1:1007>, 1007 refers to the port on which the GFI WebMonitor Management Console listens by default. If this listening port is changed, the URL used to access the Management Console should reflect this, for example `http://127.0.0.1:<port>`. This is different from the port on which the GFI Proxy listens for incoming connections.



Screenshot 7: GFI WebMonitor Home page

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> or <http://127.0.0.1:1007> in a web browser from their machine. The Internet browser must be configured to use specific proxy settings to enable this access. For <http://127.0.0.1:1007> disable **Bypass proxy server for local addresses** from Internet options. For more information, refer to [Configure browser proxy settings on the clients' machine](#) (page 27).

NOTE

User access to the application can be granted either during installation or from **Settings > Advanced Settings > UI Access Control**.

2.6 Configure browser proxy settings on the clients' machine

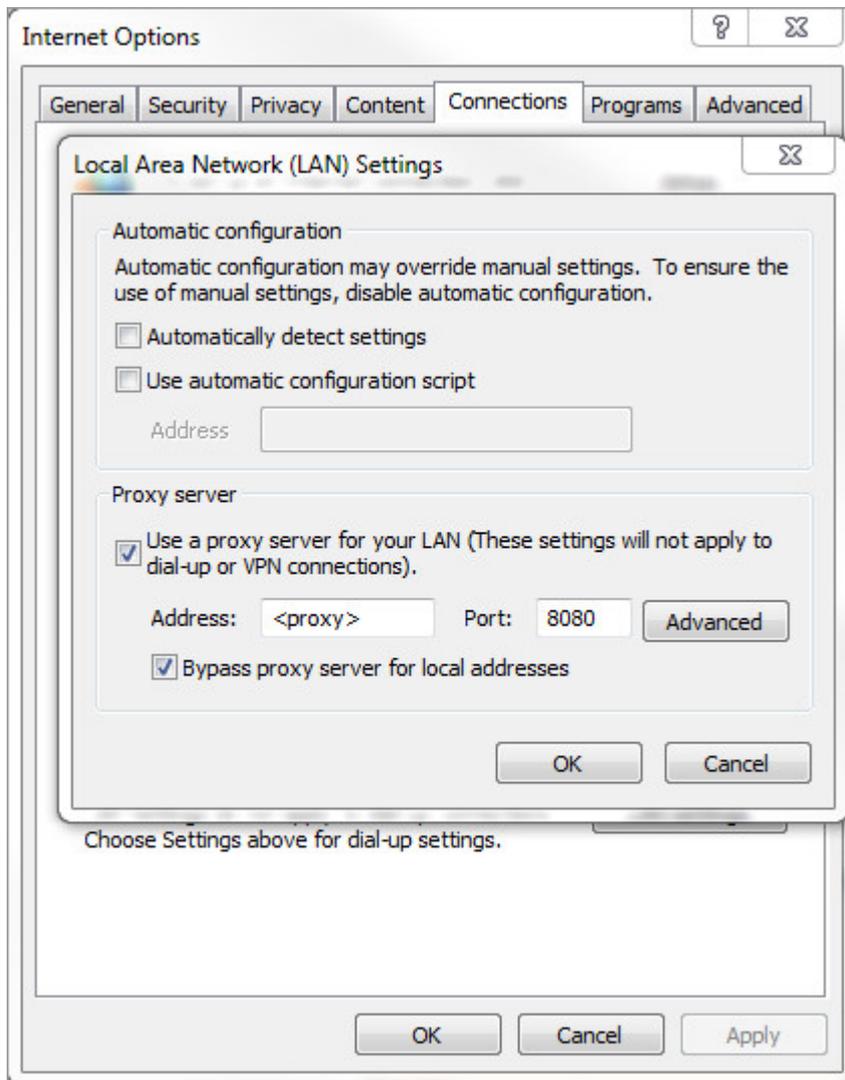
GFI WebMonitor acts as a Proxy Server to provide a connection between your internal network and the Internet. This means that traffic from client machines needs to be redirected through the GFI WebMonitor server.

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

This can be achieved by performing the following:

1. On the client machine, go to **Control Panel** and select **Internet Options**.
2. Click the **Connections** tab.
3. Click **LAN settings**.



Screenshot 8: Configure fixed proxy settings

4. Check **Use a proxy server for your LAN** checkbox.
5. In the **Address** field, key in the proxy server name or IP address of the GFI WebMonitor machine.
6. In the **Port** field, enter the port used (default = 8080).
7. Select the option **Bypass proxy server for local addresses**.

Once the evaluation period is over, a more permanent solution to configure the browser's settings can be used. The alternatives are:

- » [Using a GPO](#)
- » [Using WPAD](#)
- » [Using Transparent Proxy](#)

2.7 Verify that GFI WebMonitor is working correctly

To determine that GFI WebMonitor is working correctly, perform a simple test to check whether an Internet request is blocked. To do this:

1. Go to **Manage > Policies**.

NOTE

You will see that a Default Web Filtering Policy is already enabled. This policy applies to every user whose traffic is routed through GFI WebMonitor.

2. In the sidebar, select **Blacklist** from the list of configured policies.
3. Click **Edit**.
3. In the **Websites** element, type ***.example.com**.
4. Click the **Add** sign. The URL is added to the list of blocked sites.
5. Click **Save** to apply the changes.
6. Go back to your browser and open <http://www.example.com>. The GFI WebMonitor blocking page should now be displayed.



Access Denied

You have been blocked from downloading this file since it breaches a security policy.

Blocked Website	www.example.com
Breached Policy	Blacklist

Go Back

Powered by GFI WebMonitor®

Screenshot 9: Warning that the page you requested was blocked by GFI WebMonitor

If the warning above is displayed, then your GFI WebMonitor installation is working correctly.

You can now remove the URL from the Blacklist policy.

2.8 Deploying GFI WebMonitor in a Microsoft Forefront TMG environment.

When GFI WebMonitor is installed on a server that is also running Microsoft Forefront Threat Management Gateway (TMG) it can either be installed in parallel to Microsoft Forefront TMG or installed as Microsoft Forefront TMG plug-in.



Screenshot 10: Screen available only when the installation is running on a TMG Server.

During installation, choose the GFI WebMonitor deployment mode. Note that the installation mode cannot be changed after installation, so it is recommended to review the information in this topic to enable you to choose the ideal mode for your environment.

Note that Transparent proxy mode is not available when installing GFI WebMonitor on the Microsoft Forefront TMG server.

NOTE

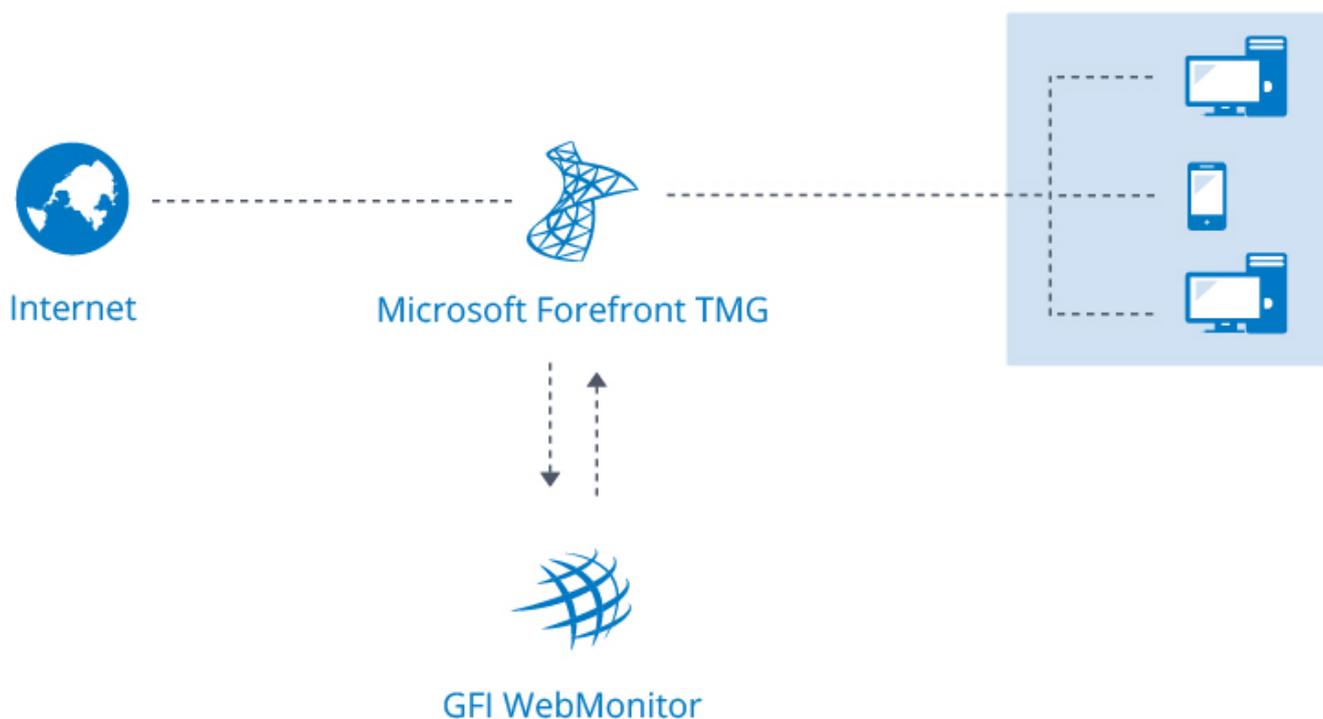
Review this information before installation, since this choice cannot be changed afterwards.

The two deployment options available are:

- » Register as a Microsoft Forefront TMG plug-in
- » Install as a proxy in parallel to Microsoft Forefront TMG

2.8.1 Register as a Microsoft Forefront TMG plug-in

Choose this option to keep Microsoft Forefront TMG as the firewall and proxy while using GFI WebMonitor for web filtering purposes only.



Screenshot 11: GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG

In this setup, GFI WebMonitor works as a plug-in of the Microsoft Forefront TMG Server.

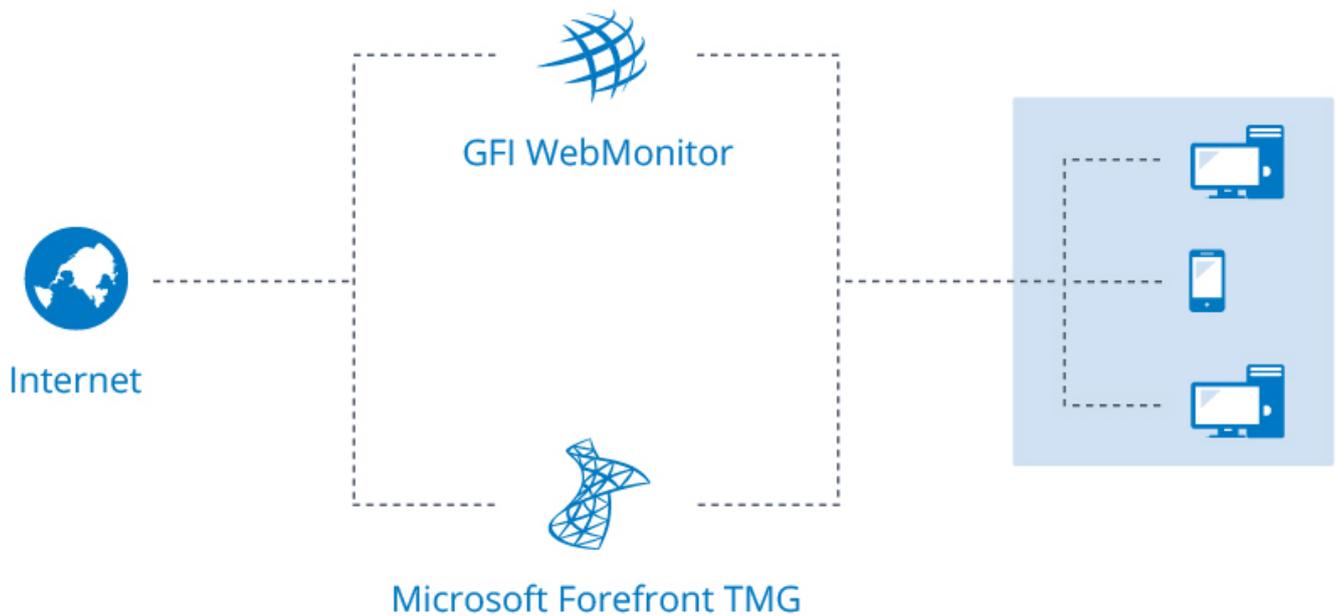
Important notes to consider:

- » This setup is easier to configure for clients that are upgrading from GFI WebMonitor 2013, because it keeps the same setup and no changes are required on the network.
- » This option is only available for servers that have Microsoft Forefront TMG installed. Microsoft Internet Security and Acceleration Server (ISA) is not supported.

For more information, refer to [Installing GFI WebMonitor as a plug-in GFI WebMonitor](#) (page 33).

2.8.2 Install as a proxy in parallel to Microsoft Forefront TMG

Choose this option to have GFI WebMonitor running as a standalone proxy.



Screenshot 12: GFI WebMonitor installed in parallel with Microsoft Forefront TMG

In this setup you have two independent software running in parallel.

Important notes to consider:

- » In this setup GFI WebMonitor is not dependent on Microsoft Forefront TMG and it works even if there are problems with TMG.
- » Network setup must be adjusted to point client machines to port 8081 to use the GFI WebMonitor proxy.
- » Contact your reseller. The license for GFI WebMonitor Proxy cannot be upgraded from the GFI WebMonitor TMG key.

In this mode GFI WebMonitor can also be chained to Microsoft Forefront TMG. For more information, refer to [Configuring Chained Proxy](#) (page 92).

For more information, refer to [Installing GFI WebMonitor in parallel with Microsoft Forefront TMG](#) (page 35).

2.8.3 Installing GFI WebMonitor as a plug-in GFI WebMonitor

GFI WebMonitor can be installed as a plug-in for Microsoft Forefront Threat Management Gateway (TMG).

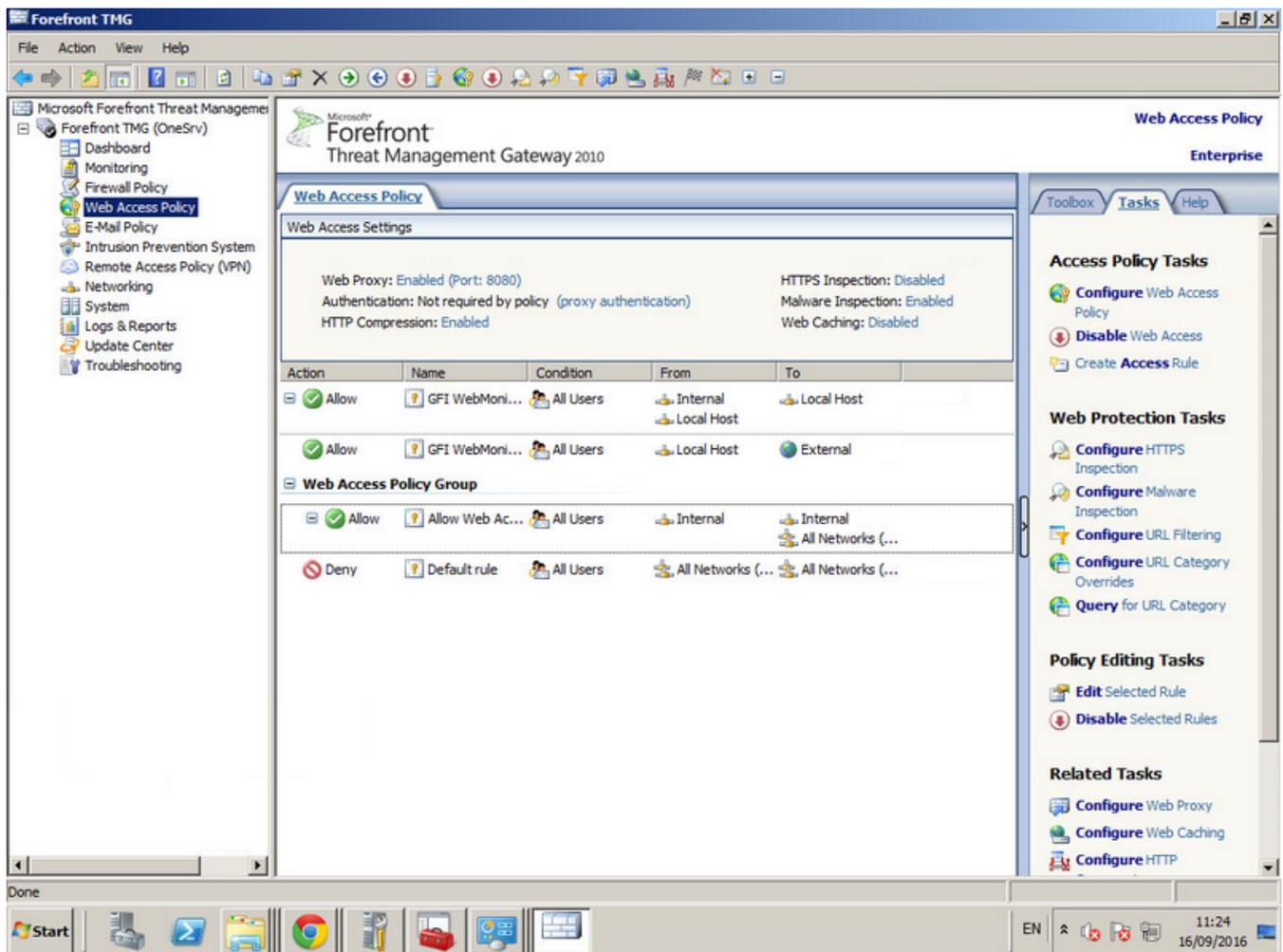
Microsoft Forefront TMG is a web gateway solution designed to protect users from web-based threats. GFI WebMonitor can complement this functionality. When installed in this environment, GFI WebMonitor enables the administrator to monitor users web traffic in real time.

GFI WebMonitor should be installed as a plug-in for Microsoft Forefront TMG when you want to keep Microsoft Forefront TMG as firewall and proxy while using the web filtering functions of GFI WebMonitor.

With this setup, when users request a webpage or a download over the Internet, the incoming and outgoing traffic generated by the request is received by the Microsoft Forefront TMG, which in turn refers to GFI WebMonitor to use the filtering mechanisms to analyze the request. Once the filtering is complete, the traffic is reverted to the Microsoft Forefront TMG for routing.

NOTE

GFI WebMonitor can only be installed or updated as plug-in for Microsoft Forefront TMG. The Microsoft Internet Security and Acceleration (ISA) Server is not supported.



Screenshot 13: Firewall rules created in TMG.

When GFI WebMonitor is installed as a plug-in for Microsoft Forefront TMG two new policies are created in the **Web Access Policy** and **Firewall Policy** nodes of TMG:

- » **GFI WebMonitor - Allow access to local host:** used to capture the Internet traffic to be filtered.
- » **GFI WebMonitor - Allow Internet access:** used to allow the updates for GFI WebMonitor.

NOTES

It is recommended to keep these two policies with the highest priority to ensure that no other TMG policies interfere with GFI WebMonitor activity.

If having problems when downloading updates, check your firewall settings to ensure that exceptions for the URLs used for updates are in place. For more information, refer to [Firewall settings](#) (page 14).

Upgrading from GFI WebMonitor 2013 for TMG

GFI WebMonitor 11 does not support an direct upgrade from GFI WebMonitor 2013. You need to upgrade to GFI WebMonitor version 10 first and then continue with the upgrade to GFI WebMonitor 11.

The complete upgrade process from GFI WebMonitor version 2013 to version 11 has the following steps.

1. Download and upgrade the 64-bit version of GFI Webmonitor 10.1 and follow the instructions in this article: <https://www.gfi.com/support/products/gfi-webmonitor/How-to-upgrade-to-GFI-WebMonitor-10>. Do not run the

post-install wizard, but continue to the next step.

2. Upgrade to GFI WebMonitor 11. For more information, refer to [Upgrading from GFI WebMonitor 10](#) (page 36).
3. Obtain the [license key](#) and continue with the post-install wizard. For more information, refer to [Using the Post-installation Configuration Wizard](#) (page 25).

2.8.4 Installing GFI WebMonitor in parallel with Microsoft Forefront TMG

GFI WebMonitor can be installed on the same machine where Microsoft Forefront TMG is running.

When installed in parallel with Microsoft Forefront TMG, GFI WebMonitor performs web filtering and proxy functions. Microsoft Forefront TMG serves as a firewall. This setup also provides an alternative when it is not possible to add another dedicated machine in the network just for GFI WebMonitor.

GFI WebMonitor for TMG and GFI WebMonitor Standalone Proxy use two different sets of license key that are not interchangeable between them. Contact your reseller if you need to shift between these two modes.

NOTE

GFI WebMonitor cannot be deployed in Transparent Proxy mode when installing on a Microsoft Forefront TMG server. For more information, refer to [Configuring Transparent Proxy](#) (page 93).

The installation process is similar to the regular GFI WebMonitor Proxy edition installation with an additional step that asks how to integrate GFI WebMonitor with Microsoft Forefront TMG. Choose **Install as a proxy in parallel to Microsoft Forefront TMG** to deploy using this method. For more information, refer to [Installing GFI WebMonitor](#) (page 22).

After installation or upgrade is complete, client machines need to be configured to use GFI WebMonitor as proxy instead of Microsoft Forefront TMG. In the proxy settings of the client's browser the IP must point to the IP of the server and use port 8081. This can be done either by [configuring every client browser manually](#) or [via GPO](#) or by [enabling WPAD](#).

Upgrading from GFI WebMonitor 2013 for TMG

GFI WebMonitor 11 does not support an direct upgrade from GFI WebMonitor 2013. You need to upgrade to GFI WebMonitor version 10 first and then continue with the upgrade to GFI WebMonitor 11.

The complete upgrade process from GFI WebMonitor version 2013 to version 11 has the following steps.

1. Download and upgrade the 64-bit version of GFI Webmonitor 10.1 and follow the instructions in this article: <https://www.gfi.com/support/products/gfi-webmonitor/How-to-upgrade-to-GFI-WebMonitor-10>. Do not run the post-install wizard, but continue to the next step.
2. Upgrade to GFI WebMonitor 11. For more information, refer to [Upgrading from GFI WebMonitor 10](#) (page 36).
3. Obtain the [license key](#) and continue with the post-install wizard. For more information, refer to [Using the Post-installation Configuration Wizard](#) (page 25).

A new GFI WebMonitor license key is required. Contact your reseller. The license for GFI WebMonitor Proxy cannot be upgrade from the GFI WebMonitor TMG key.

During upgrade, the previously defined GFI WebMonitor configuration is retained and converted to the new format.

After the upgrade process is complete, the [Configuration Wizard](#) guides the user in setting up the most important settings. The proxy related settings contain pre-configured values if no such setting is detected from previous installations. The [proxy listening port](#) is set to 8081 instead of the default port of 8080, in order to avoid conflict with Microsoft Forefront TMG's proxy.

Important notes:

- » Once the setup is complete and client machines point to GFI WebMonitor, Internet traffic generated by these machines is captured by the GFI proxy and only this traffic is monitored or controlled by GFI WebMonitor. The Microsoft Forefront TMG firewall can still capture traffic via its own proxy or in transparent mode; however this traffic will not be seen by GFI WebMonitor.
- » If GFI WebMonitor proxy is published on the network via WPAD, Microsoft Forefront TMG firewall's WPAD server needs to be de-activated in order to ensure all traffic is passing through the GFI WebMonitor proxy.
- » Previous GFI WebMonitor rules on the Microsoft Forefront TMG firewall configuration are no longer in effect and they can be disabled or deleted.
- » Microsoft Forefront TMG firewall remains operational and the GFI WebMonitor proxy works in parallel with the following Microsoft Forefront TMG operation modes:
 - **Single Network Adapter** - Microsoft Forefront TMG with one network adapter connected to the Internal network or to a Perimeter network.
 - **Edge Firewall** - Microsoft Forefront TMG located at the network edge, acting as an edge firewall and connected to two networks: the internal network and the external network (usually the Internet).
 - **3-Leg Perimeter** - Microsoft Forefront TMG deployed at the edge of the network, connected to the Internal network, the Perimeter network and the Internet.
 - **Back Firewall** - Microsoft Forefront TMG deployed at the edge of the network, connected to the Internal network and the Perimeter network.

2.9 Upgrading from previous versions

Choose your current GFI WebMonitor version for notes and instructions on how to upgrade to the latest version while retaining all settings:

- » [GFI WebMonitor 10](#)
- » [GFI WebMonitor 2015](#)
- » [GFI WebMonitor 2013](#)

NOTE

For versions older than 2013 SR1 we recommend to first upgrade to GFI WebMonitor 2013 SR1 and then to the current version.

To verify the version of GFI WebMonitor open the web interface and access the **Home** page.

2.9.1 Upgrading from GFI WebMonitor 10

This section describes how to upgrade a GFI WebMonitor 10 or higher installation to the latest version while retaining all settings.

Important notes when upgrading

- » GFI WebMonitor version 11 and later only supports installation in a 64-bit machine. An upgrade is not possible in a 32-bit machine and a new installation in a supported environment is required.
- » Upgrade is not reversible; you cannot downgrade to a previously installed version.

- » Export the GFI WebMonitor settings before upgrade. This backup may be useful to revert configuration if upgrade fails. For more information, refer to [Export settings to a chosen file/folder](#) (page 139).
- » Log in to the [GFI Customer Area](#) to get a new license key. Click the blue key icon on the right and select **Upgrade License Key**, or click **Renewal** to extend your maintenance agreement.
- » During upgrade, GFI WebMonitor services and its functionalities are stopped.
- » Check that the machine you are installing GFI WebMonitor on meets the latest version's [system and hardware requirements](#).
- » Log on as Administrator or use an account with administrative privileges.
- » Save any pending work and close all open applications on the machine.

Upgrade procedure

1. Download the latest build of GFI WebMonitor on the server where GFI WebMonitor is currently installed. Go to http://go.gfi.com/?pageid=WebMon_Download, click **Login** and key in your GFI Account credentials.
2. Right-click the newly downloaded installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.
3. Launch the newly downloaded installer and follow the on-screen instructions to install the latest version.
4. After the installation, the GFI WebMonitor Configuration Wizard is launched automatically in a web browser.
5. Test the functionality of GFI WebMonitor by monitoring some traffic. For more information, refer to [Verify that GFI WebMonitor is working correctly](#) (page 29).

2.9.2 Upgrading from GFI WebMonitor 2015

This section describes how to upgrade a GFI WebMonitor 2015 or higher installation to the latest version while retaining all settings.

Important notes when upgrading

- » GFI WebMonitor version 11 and later only supports installation in a 64-bit machine. An upgrade is not possible in a 32-bit machine and a new installation in a supported environment is required.
- » Upgrade is not reversible; you cannot downgrade to a previously installed version.
- » GFI WebMonitor 11 does not support an direct upgrade from GFI WebMonitor 2015. You need to upgrade to GFI WebMonitor version 10 first and then continue with the upgrade to GFI WebMonitor 11. Download and upgrade the 64-bit version of GFI Webmonitor 10.1 and follow the instructions in this article: <https://www.gfi.com/support/products/gfi-webmonitor/How-to-upgrade-to-GFI-WebMonitor-10>
- » Export the GFI WebMonitor settings before upgrade. This backup may be useful to revert configuration if upgrade fails. For more information, refer to [Export settings to a chosen file/folder](#) (page 139).
- » Log in to the [GFI Customer Area](#) to get a new license key. Click the blue key icon on the right and select **Upgrade License Key**, or click **Renewal** to extend your maintenance agreement.
- » During upgrade, GFI WebMonitor services and its functionalities are stopped.
- » Check that the machine you are installing GFI WebMonitor on meets the latest version's [system and hardware requirements](#).

- » Log on as Administrator or use an account with administrative privileges.
- » Save any pending work and close all open applications on the machine.

Upgrade procedure

1. Download the latest build of GFI WebMonitor on the server where GFI WebMonitor is currently installed. Go to http://go.gfi.com/?pageid=WebMon_Download, click **Login** and key in your GFI Account credentials.
2. Right-click the newly downloaded installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.
3. Launch the newly downloaded installer and follow the on-screen instructions to install the latest version.
4. After the installation, the GFI WebMonitor Configuration Wizard is launched automatically in a web browser.
5. Test the functionality of GFI WebMonitor by monitoring some traffic. For more information, refer to [Verify that GFI WebMonitor is working correctly](#) (page 29).

2.9.3 Upgrading from GFI WebMonitor 2013

This section describes how to upgrade a GFI WebMonitor 2013 installation to the latest version while retaining all settings.

Important notes when upgrading

- » GFI WebMonitor version 11 and later only supports installation in a 64-bit machine. An upgrade is not possible in a 32-bit machine and a new installation in a supported environment is required.
- » Upgrade is not reversible; you cannot downgrade to a previously installed version.
- » Ensure that you are running GFI WebMonitor 2013 SR1 (build 20130910) before upgrading to the latest version. Download the 2013 SR1 installer and follow the instructions in this article: <https://www.gfi.com/support/products/gfi-webmonitor/How-to-upgrade-to-GFI-WebMonitor-2013>
- » GFI WebMonitor 11 does not support an direct upgrade from GFI WebMonitor 2013. You need to upgrade to GFI WebMonitor version 10 first and then continue with the upgrade to GFI WebMonitor 11. Download and upgrade the 64-bit version of GFI Webmonitor 10.1 and follow the instructions in this article: <https://www.gfi.com/support/products/gfi-webmonitor/How-to-upgrade-to-GFI-WebMonitor-10>.
- » Customers using GFI WebMonitor 2013 for TMG also needs to upgrade to version GFI WebMonitor version 10 as described above. For more information, refer to [Deploying GFI WebMonitor in a Microsoft Forefront TMG environment](#). (page 30).
- » Make a backup of the GFI WebMonitor settings before upgrading. This backup may be useful in case the upgrade fails. Copy and save the following folders in the main directory of GFI WebMonitor, `Data` and `Interface/AppData`.
- » With a few exceptions, existing settings, policies, some alerts and reports are imported automatically during the upgrade process. For more information, refer to [List of exceptions when upgrading from GFI WebMonitor 2013](#) (page 39).
- » Log in to the [GFI Customer Area](#) to get a new license key. Click the blue key icon on the right and select **Upgrade License Key**, or click **Renewal** to extend your maintenance agreement.

- » During upgrade, GFI WebMonitor services and its functionalities are stopped.
- » Check that the machine you are installing GFI WebMonitor on meets the latest version's [system and hardware requirements](#).
- » Log on as Administrator or use an account with administrative privileges.
- » Save any pending work and close all open applications on the machine.

Upgrade procedure

1. Download the latest build of GFI WebMonitor on the server where GFI WebMonitor is currently installed. Go to http://go.gfi.com/?pageid=WebMon_Download, click **Login** and key in your GFI Account credentials.
2. Right-click the newly downloaded installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.
3. Launch the newly downloaded installer and follow the on-screen instructions to install the latest version.
4. After the installation, the GFI WebMonitor Configuration Wizard is launched automatically in a web browser.
5. Test the functionality of GFI WebMonitor by monitoring some traffic. For more information, refer to [Verify that GFI WebMonitor is working correctly](#) (page 29).

List of exceptions when upgrading from GFI WebMonitor 2013

When upgrading from GFI WebMonitor 2013 SR1 to the latest version, most existing settings, policies, some alerts and reports are imported automatically during the upgrade process. Due to the architectural changes in the latest version of GFI WebMonitor, there are some exceptions which either get imported differently or do not get imported.

The table below lists the exceptions and other important changes:

Feature	Description
Policies	<p>The upgrade process imports existing policies to the latest version of GFI WebMonitor. However, the list of policies will be different.</p> <ul style="list-style-type: none"> » Web Filtering policies – for a WebFiltering policy 2013 that has both block and warn actions set, after the upgrade there will be two corresponding policies: <ul style="list-style-type: none"> • WebFiltering policy 2013 - block - this will contain the blocked categories, the sites from Always Blocked section and the Reputation Index. • WebFiltering policy 2013 - warn - this will have Warn action and the corresponding categories. • Both policies will have the settings that were configured in the previous version: Notification, Logging enabled and Schedule. The policy with Block action has the higher priority. » Web Browsing policies – existing web browsing policies are imported with the same settings. » Web Security policies – for an existing Web security policy that has both block and warn actions set, after the upgrade there will be two new corresponding policies. Additionally, if in the existing policy there are file types with download window enabled and others that do not, after the upgrade these will be separated into two policies, one with AV Scanning and Download Window enabled and one with only AV Scanning. » Streaming Media and Instant Messaging – Existing Streaming Media and Instant Messaging policies will be imported into a new policy with Block action and corresponding applications added. » ThreatTrack and AntiPhishing – If at least one of these features was enabled in the previous version, a new policy with Block action and URL Scanning enabled is added after the upgrade. Since ThreatTrack and AntiPhishing are no longer separated, both features will be enabled in the latest version. <p>NOTE GFI WebMonitor 2013 had an advanced setting that allowed the user to set a condition on multiple categories with AND operator between them. This is not imported.</p>

Feature	Description
Activity Logging	The Activity Logging settings in the latest version of GFI WebMonitor are different than version 2013 and previous versions. This feature is now integrated in the new policy builder, using the Logging element. Therefore, if your current installation contains Activity Logging policies, note that no corresponding policy is added after the upgrade.
Alerts	In previous versions, Monitor, Bandwidth and Security Alerts could be set up from a separate location to apply to all policies. In the latest GFI WebMonitor version, these are now configured per policy using the Log Alert element. The upgrade process can import some existing alerts with a few exceptions as detailed below: <ul style="list-style-type: none"> » Existing Monitoring Alerts that were set for Sites Accessed will be imported into new policies with Monitor action. However, alerts for Warning Bypassed and Sites Blocked are not imported. » Existing Security Alerts are not imported. » Bandwidth Alerts that were set for All Users cannot be imported. All other bandwidth alerts are imported into new policies with a Monitor action.
Reports	The following reports cannot be imported into the latest GFI WebMonitor version: <ul style="list-style-type: none"> » Bandwidth - Download Only » Bandwidth - Upload Only » Activity - Filtered Only by Type » Bandwidth Usage Trends - Downloads » Bandwidth Usage Trends - Uploads » Bandwidth - Non productive traffic

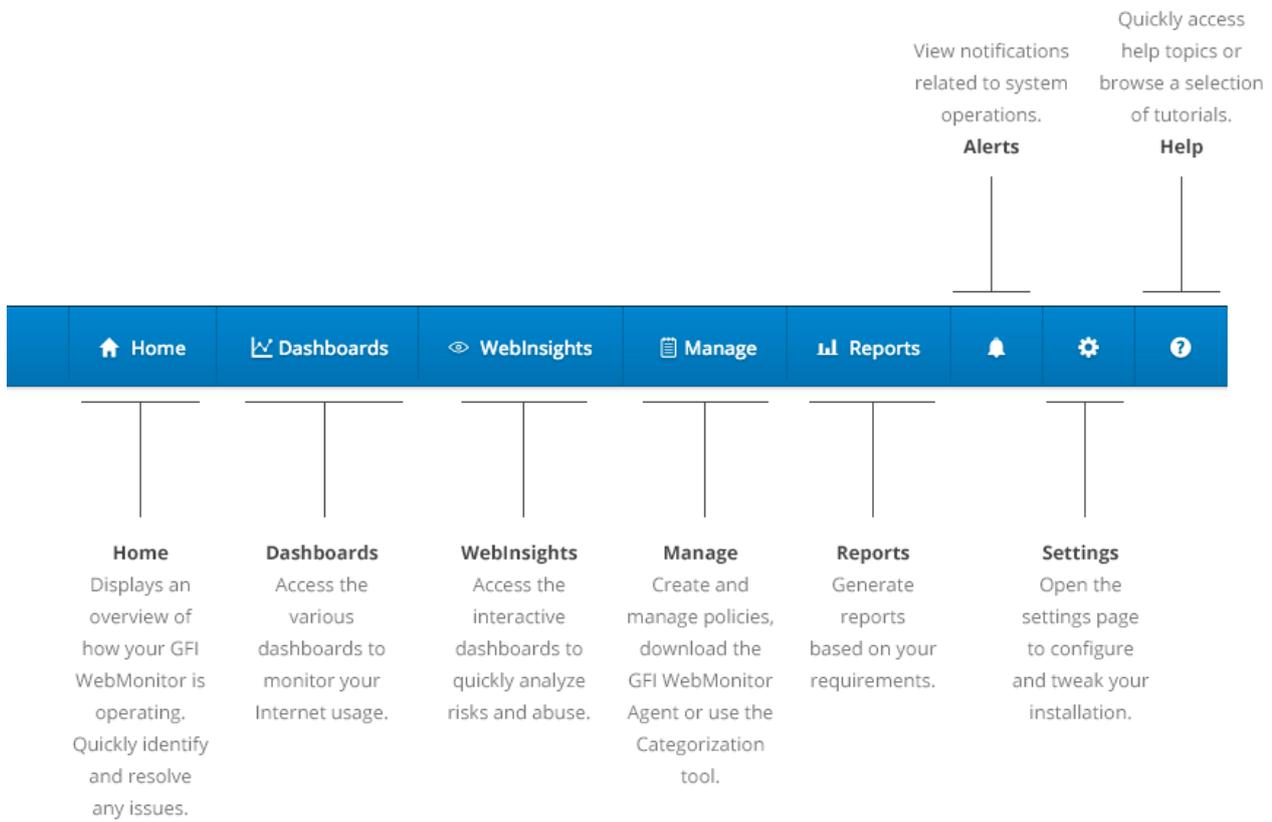
2.10 Uninstall information

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 Using GFI WebMonitor

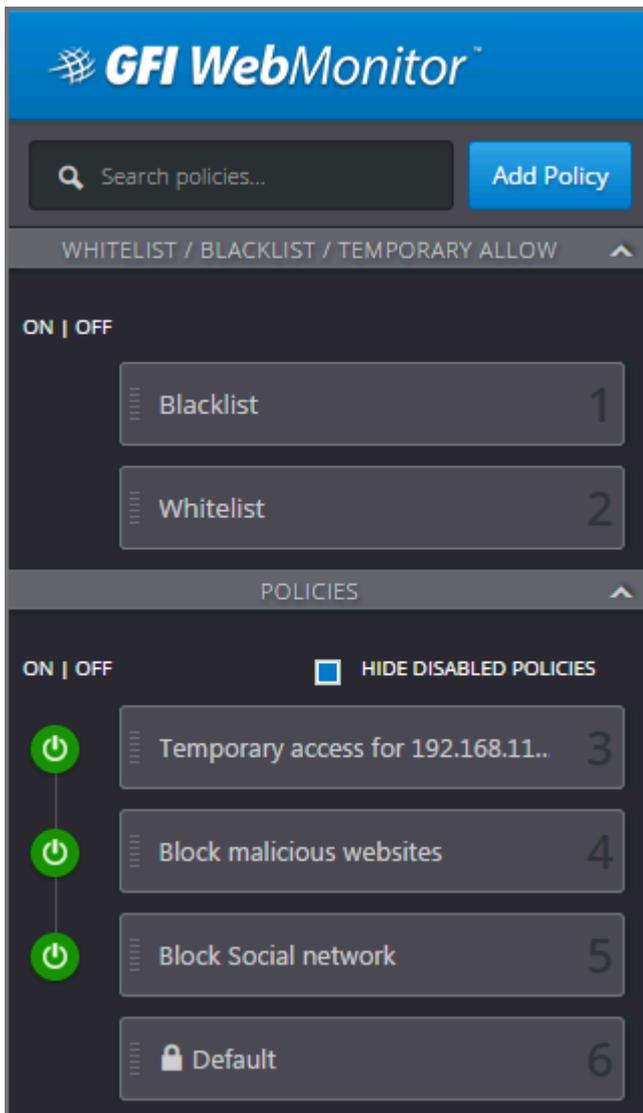
After the initial configuration is complete, the home page is displayed. Use the main navigation bar to access all the product features.



Screenshot 14: The product toolbar

3.1 Working with Policies

Policies enable you to exercise control over Internet activity that can effect security, productivity, performance and legal issues.



Screenshot 15: Policies are executed in a sequential order from top to bottom.

You can create as many new policies as required, either by configuring each new policy from scratch or by cloning existing policies. Configured policies are displayed as a list in the left sidebar. Click the switch next to configured policies to activate or deactivate as required.

IMPORTANT

GFI WebMonitor policies work in a sequential order. The policies at the top take precedence over the ones beneath. It is possible to change the order of the configured policies by dragging a policy to the desired place in the list, however this may have repercussions on your setup.

A default policy is automatically created when GFI WebMonitor is installed. This is the fallback policy – if no policies are matched for a given situation, the default policy will apply.

This policy is configured to **Allow** all Internet traffic to **Everyone**. You can change the policy type to **Block**, but you cannot delete or disable this default policy. New policies are added on top of the default policy to provide monitoring and filtering options as required.

2 additional policies are also enabled by default when GFI WebMonitor is installed:

Policy	Description
Blacklist	The Blacklist is a list of sites, users and IP addresses that are always blocked by GFI WebMonitor.
Whitelist	The Whitelist is a list of sites, users and IP addresses that are automatically excluded from all filtering policies configured in GFI WebMonitor.

The default policies:

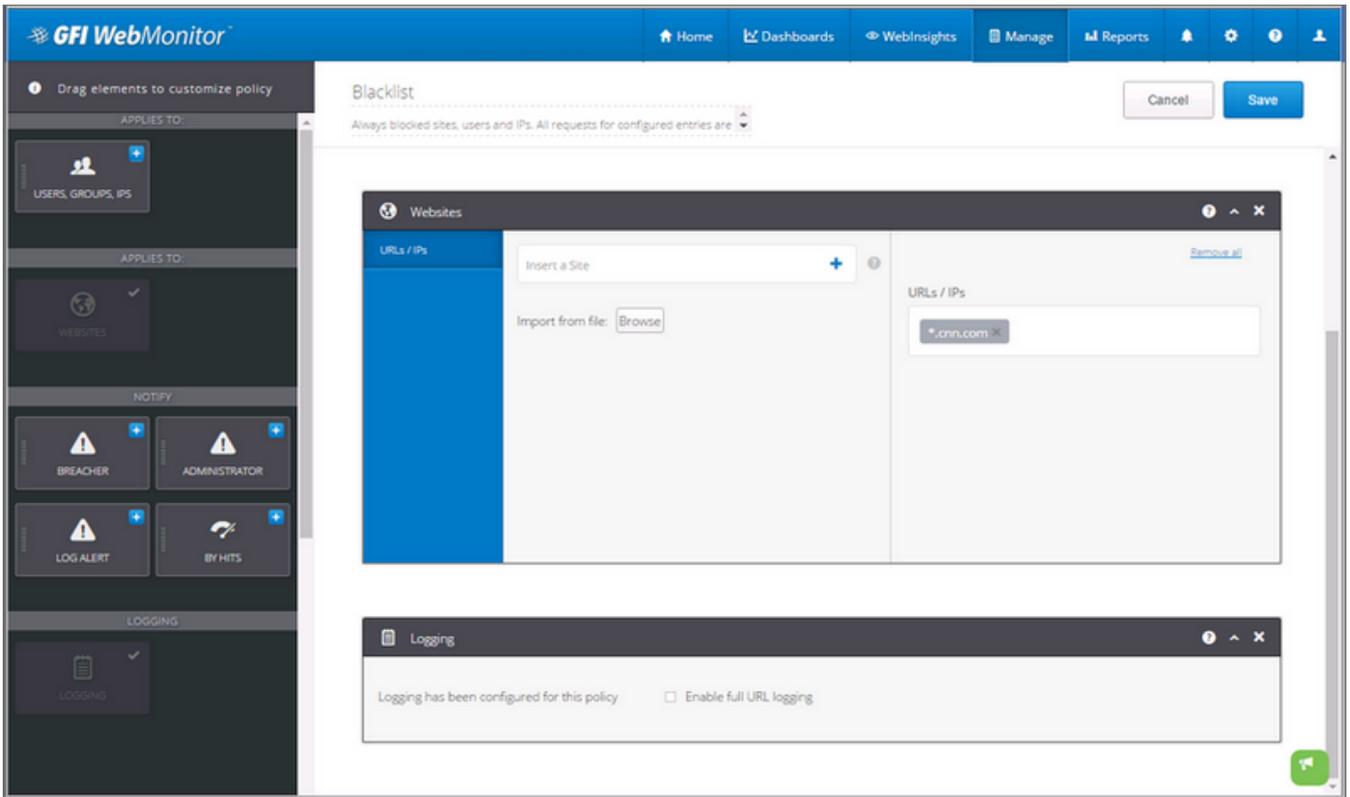
- » Apply to everyone
- » Can be edited - customization of default policy is limited
- » Cannot be disabled or deleted

For each configured policy, GFI WebMonitor provides a summary of the configured values. These values include:

Option	Description
Policy Type	There are 2 types of policies, Default Policy or Custom Policy .
Policy Action	Displays the action the policy will take when the configured criteria are met. The action can be Allow, Block, Warn or Monitor.
Status	Shows if the selected policy is Active or Inactive .
Active Since	If the policy status is Active , the summary displays the date since the policy has been active.
Applies To	Displays the number of users, groups or IPs the selected policy applies to.
Allow, Warn, Monitor or Block	This area shows how many websites, applications or file types are affected by the configured policy action.
Thresholds	Displays configured limits based on bandwidth, hits or time.
Notify	Shows any configured notifications. Can be User, Administrator or both.
Scheduled on	Displays the period during which the selected policy is active.
Exceptions	Displays configured exceptions that are not affected by the policy.

3.2 Configuring Blacklist

The **Blacklist** list is a list of sites, users and IP addresses that should always be blocked.



Screenshot 16: Blacklist contains sites that are always blocked

The **Blacklist** takes priority over all other policies. The **Blacklist** cannot be switched off, however when GFI WebMonitor is first installed, the **Blacklist** policy is inactive. This is because by default, the **Blacklist** does not contain any pre-configured websites.

IMPORTANT

In GFI WebMonitor, the **Blacklist** takes priority over the **Whitelist**. Therefore, if a site is listed both in the **Whitelist** and in the **Blacklist**, access to the site is blocked.

We recommend adding potentially unsafe sites to the **Blacklist** so that these are always blocked. These sites should include websites known for their malicious content or illegal material such as malware sites, bot nets and fraudulent websites.

NOTE

The **Blacklist** functions using an OR method. Any item added to the list will be blocked.

3.2.1 Adding Items to the Blacklist

By default, the GFI WebMonitor Blacklist does not contain any pre-configured websites. We recommend adding potentially unsafe sites to the Blacklist so that these are always blocked. These sites should include websites known for their malicious content or illegal material such as malware sites, bot nets and fraudulent websites.

NOTE

The **Blacklist** functions using an OR method. Any item added to the list will be blocked.

To add an item to the Blacklist:

1. Go to **Manage > Policies > Blacklist**.
2. Click **Edit**.
3. Drag the Websites element into the policy builder.
4. Insert the URL or IP of the website you want to block and click the add symbol.
5. Drag any other elements from the left sidebar that you want to include.

NOTE

Customization of system policies is limited to ensure that the intended policy function is not altered. In these policies, customization is limited to: Users, Groups or IPs, Websites filtering, notifications and logging.

6. Click **Save**.

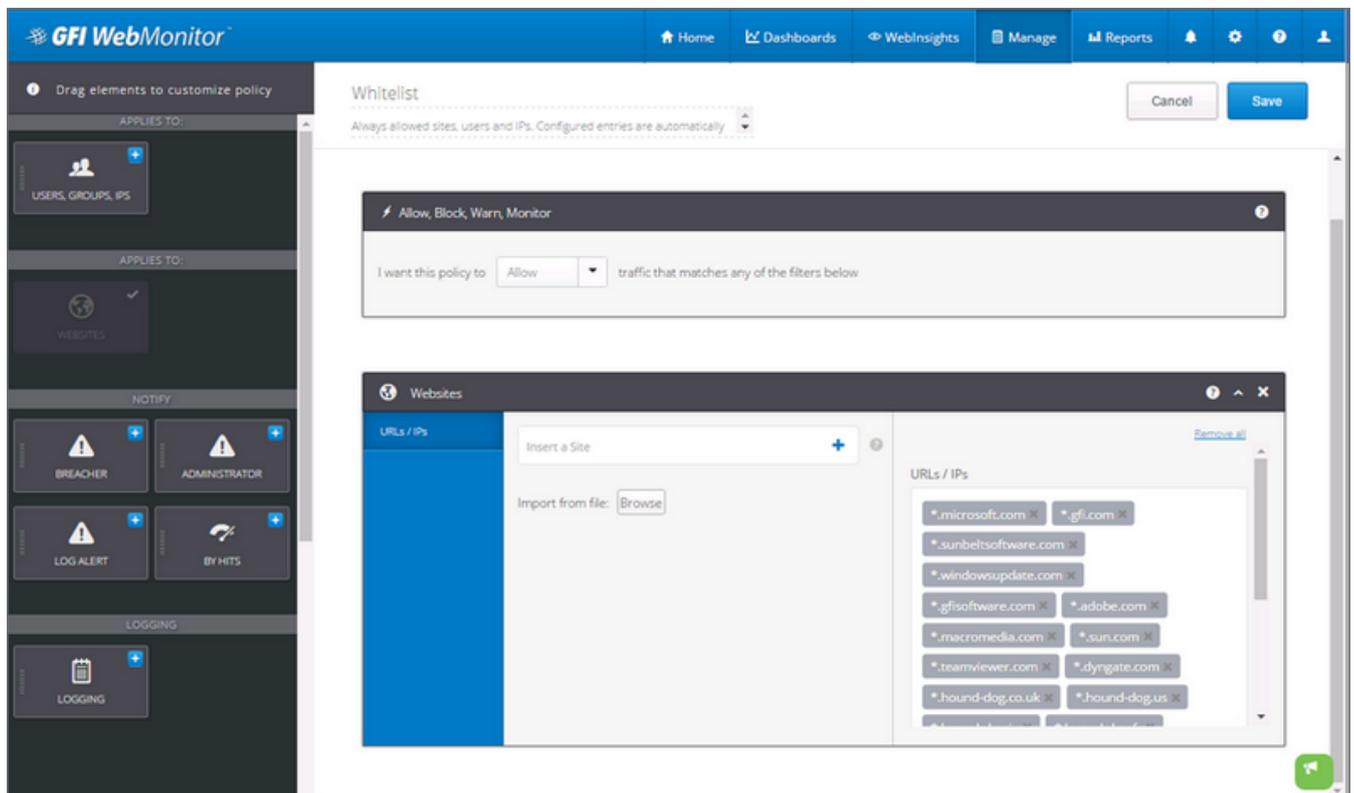
Removing items from the Blacklist

To delete an item from the Blacklist:

1. Go to **Manage > Policies > Blacklist**.
2. Click **Edit**.
3. Locate the relevant element and click the icon next to the item to delete.
4. Click **Save**.

3.3 Configuring the Whitelist

The **Whitelist** is a list of sites, users and IP addresses that are automatically excluded from all filtering policies configured in GFI WebMonitor.



Screenshot 17: Whitelist contains a list of sites that are always allowed

When GFI WebMonitor is installed, the **Whitelist** is automatically populated with a list of sites that are needed by GFI WebMonitor for system updates. Removing these sites from the **Whitelist** is not recommended.

NOTES

If the items in the **Whitelist** are also added to the **Blacklist**, priority is granted to the **Blacklist** and access is blocked. If having problems when downloading updates, check your firewall settings to ensure that exceptions for the URLs used for updates are in place. For more information, refer to [Firewall settings](#) (page 14).

Using the whitelist, you can configure a list of users or IP addresses that do not need to be monitored or protected. These users still consume a product license. For more information, refer to [Licensing information](#) (page 10).

3.3.1 Adding items to the Whitelist

By default, GFI WebMonitor includes a number of pre-configured sites in the **Whitelist**. Additional items may be included in the Whitelist to ensure they are always allowed access.

NOTE

The Whitelist functions using an OR method. Any item added to the list will be allowed.

To add an item to the **Whitelist**:

1. Go to **Manage > Policies > Whitelist**.
2. Click **Edit**.
3. In the Websites element, insert the URL or IP of the website you want to allow and click the add symbol.
4. Use the left menu to drag any elements you want to include.

NOTE

Customization of system policies is limited to ensure that the intended policy function is not altered. In these policies, customization is limited to: Users, Groups or IPs, Websites filtering, notifications and logging.

5. Click **Save**.

3.3.2 Removing items from the Whitelist

To delete an item from the Whitelist:

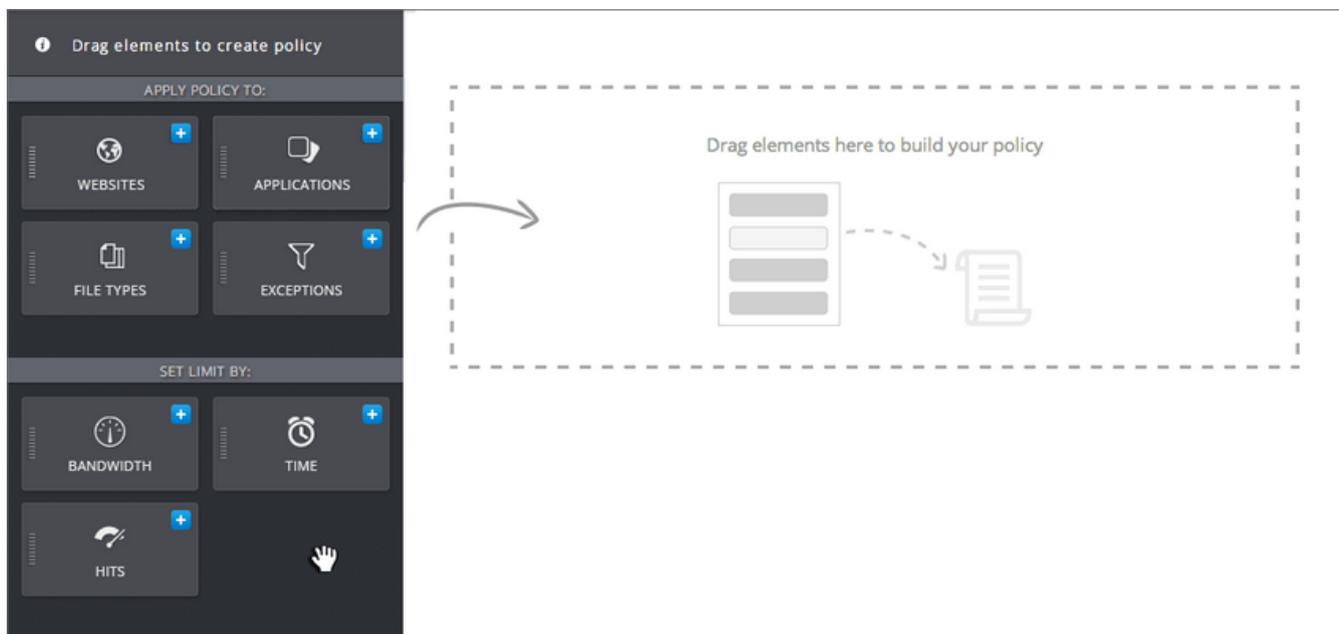
1. Go to **Manage > Policies > Whitelist**.
2. Click **Edit**.
3. Locate the relevant element and click the icon next to the item to delete.
4. Click **Save**.

3.4 Adding a new policy

GFI WebMonitor uses different elements that can be configured individually to create a policy.

NOTE

Policies use an AND method, where for the policy to function all the conditions of the configured elements in the policy must be satisfied.



Screenshot 18: Drag elements to create policy

To add a new policy:

1. Go to **Manage > Policies**.
2. Click **Add Policy**.
3. In **Add policy name** field key in a title for that policy.
4. Add a policy description.
5. Some policy elements are already available in the main policy window. Drag additional elements from the list of elements on the left. Available elements are:

Element	Description
Policy Action: Allow, Block, Warn or Monitor	Select the action taken by GFI WebMonitor when filtering internet traffic. Available options are: Allow , Block , Warn or Monitor .
Users, Groups, IPs	Specify Users , Groups or IPs for whom the new policy applies.
Websites	Specify for which websites the policy applies. Select between All Websites or specific website categories.
Applications	Specify for which applications the policy applies. Select between All Applications, application categories or specific applications.
File Types	Specify for which file types the policy applies. Select between All file types, file type categories or specific file types.
Exceptions	Define users, groups, IP addresses, websites or applications that are to be excluded from the policy.
Bandwidth limit	Select the type of bandwidth limit applied to users.

Element	Description
Time limit	Define time limits during which users specified in the policy are allowed/denied to perform particular actions.
Schedule	Select the time-window during which the policy is active.
Schedule Expiry	Specify a deactivation date after which the policy will become inactive.
Breacher	Configure notifications sent to the users who infringe a policy. Provide the body text of the notification email in the available space.
Administrator	Configure notifications sent to System Administrators when a user infringes policy. Provide the body text of the notification email in the available space.
Log Alert	Automatically send alert notifications when the criteria in the configured policy are met.
Hits limit	Specify a limit type and the number of hits per period after which GFI WebMonitor will perform the action specified in the Policy Type element.
Logging	Enable advanced logging options that keep track of full URLs visited by users. This option is useful for investigative purposes.

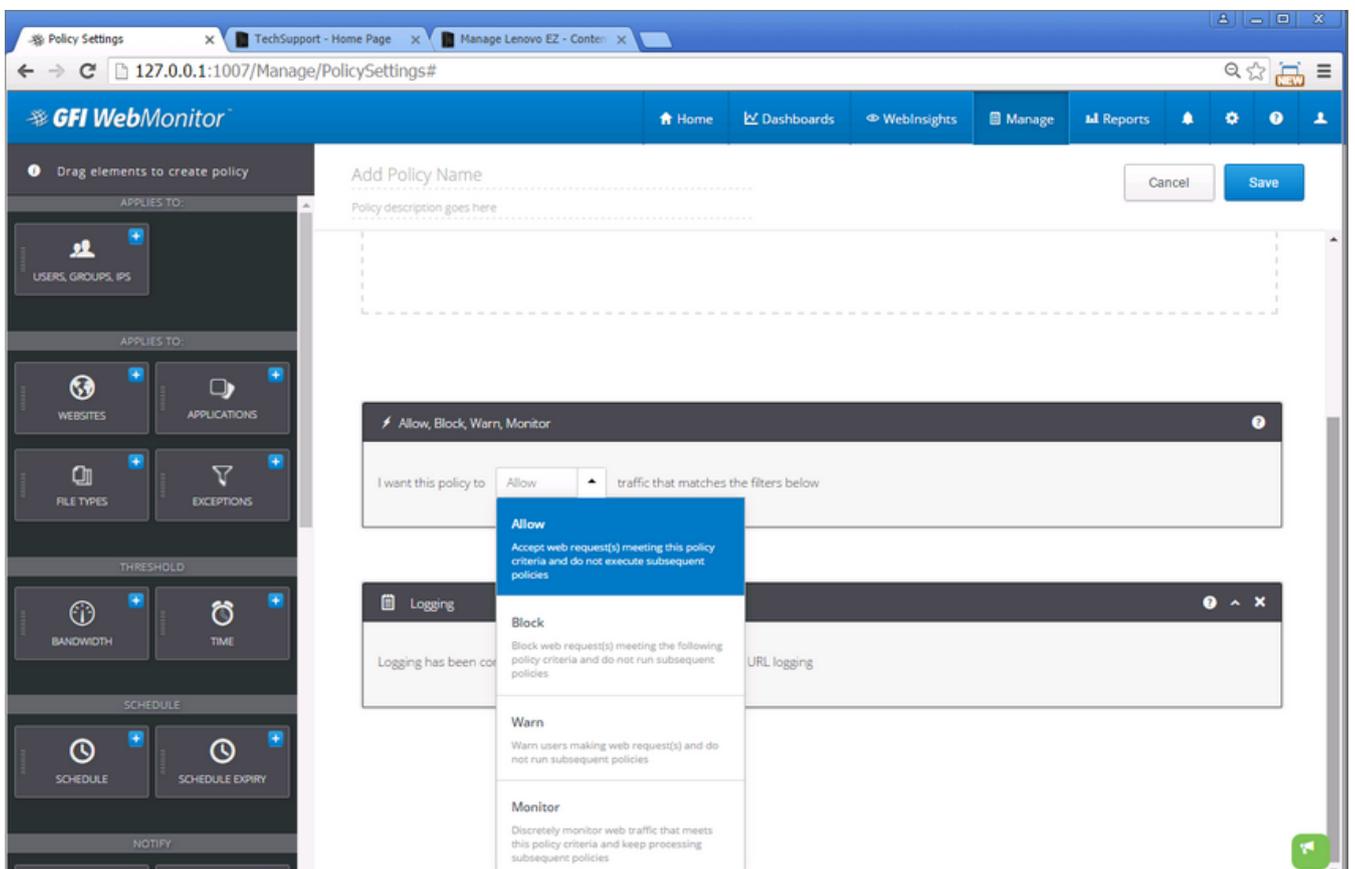
NOTE

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.

6. Click **Save**.

3.4.1 Policy action; Allow, Block, Warn or Monitor

GFI WebMonitor uses different elements that can be configured individually to create a policy.



Screenshot 19: A policy can be set to allow, block, warn or monitor.

Select what action the policy should take when the configured policy parameters are met. The options are:

Option	Description
Allow	GFI WebMonitor allows the user to access the requested content. Subsequent policies are not applied.
Block	The content requested by the user is blocked. Subsequent policies are not applied. The user attempting to access a blocked website is notified that his request has been blocked. This notification contains a Request Access button that works in conjunction with the Log Alert element to alert the system administrator that a user is requesting temporary access to a blocked site. For more information, refer to Notification Center (page 82).
Warn	The user receives a notification that the requested content breaches a configured policy, but enables user to access the content. Subsequent policies are not applied.
Monitor	GFI WebMonitor allows access to requested content and moves to the next applicable policy.
Enable users temporary access request	When enabled, a button called ' Request Access ' is displayed in the blocking page, enabling users to request temporary access to certain pages.

3.4.2 Users, Groups, IPs

Specify Active Directory Users or Groups for whom the new policy applies. Select the following options:

Option	Description
Users	Key in user names in the available field and click the add icon.
Groups	Key in an Active Directory group name in the available field and click the add icon.
IPs	Key in an IP address in the available field and click the add icon.

3.4.3 Websites

Use the Websites element to specify for which websites the policy applies.

1. Drag the Websites element into the policy to edit.
2. Select from the following options:

Option	Description
Categories	Key in the website categories in the available field and click the add icon. To select multiple categories at the same time, click the menu icon next to the add sign, select the required categories and click Add To Policy .
URLs / IPs	Key in website URL or IP address in the available field and click the add icon. Multiple URLs or IP addresses can be included in the policy using the Import from file feature. Prepare a text (.txt) file with the URLs and IPs to import. Click Browse and select the file. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE</p> <p>When keying in a URL for a website you can use the wildcard character [*], for example:</p> <p>Type *.com to allow or block all '.com' top-level domains</p> <p>Type *.website.com to allow or block all sub-domains of 'website.com'</p> </div>
URL Scanning	When this feature is enabled, all accessed URLs are scanned by ThreatTrack and AntiPhishing engines. URLs identified as malicious, vulnerable, phishing or pointing to dangerous domains will be allowed/blocked/warned/monitored depending on the configured action with that policy.

Option	Description
Filter by Reputation	<p>Move the slider to enable filtering by reputation. Filter by Reputation works with a range from 1 to 4, that matches the index reputation of a page from 100 to 0:</p> <ul style="list-style-type: none"> » Green "1" button signifies Low Risk reputation. Saves range "81-100" into policies for reputation index » Yellow "2" button signifies Unknown reputation. Saves range "61-80" into policies for reputation index. » Orange "3" button signifies Medium Risk reputation. Saves range "21-60" into policies for reputation index. » Red "4" button signifies High Risk reputation. Saves range "0-20" into policies for reputation index.

3.4.4 Applications

Use the Applications element to specify for which applications the policy applies.

1. Drag the Applications element into the policy to edit.
2. Select from the following options:

Option	Description
Application Category	Key in the application category in the available field and click the add icon. To select multiple categories at the same time, click the menu icon next to the add sign, select the required categories and click Add To Policy .
Applications	Key in a specific application name in the available field and click the add icon. To select multiple applications at the same time, click the menu icon next to the add sign. Browse the list of application, use available filters or the search tool to locate required applications. Select the applications and click Add To Policy .

3.4.5 File Types

Specify for which file types the policy applies.

NOTES

For better file type detection, enter the exact content-type header like `text/html; charset=utf-8`, rather than generic content type like `mp3`.

You can use third-party tools like Wireshark or Fiddler to obtain the exact content-type header.

1. Drag the File Types element into the policy to edit.
2. Select from the following options:

Option	Description
File Type Categories	Key in the File Type category in the available field and click the add icon. To select multiple categories at the same time, click the menu icon next to the add sign, select the required categories and click Add To Policy .
File Types	Key in a specific file type in the available field and click the add icon. To select multiple file types at the same time, click the menu icon next to the add sign, select the required applications and click Add To Policy .
Custom File Types	Click Manage File Types to add new File Types not available by default. Specify the file type (Content-type header found from Fiddler or Whireshark) in the Content Type field, key in additional information in the Description field and click Add . To add the newly created Custom File Type to the policy, start typing in the Insert a Custom File Type field, select the File Type and click the Add icon.
AV Scanning	When enabled, GFI WebMonitor scans the downloaded file using the internal Anti-Virus engines. Click Configure Engines to select which AV engines to use.
Download Progress Window	Enable to show download progress information when users download file types configured in the policy.

3.4.6 Exceptions

Define users, groups, websites or applications that are to be excluded from the policy.

1. Drag the Exceptions element into the policy to edit.
2. Select from the following options:

Option	Description
Users	Key in user names in the available field and click the add icon.
User IP Addresses	Key in the IP address or a range of IP addresses of user machines to exclude from the policy.
Groups	Key in an Active Directory group name in the available field and click the add icon.
URLs / IPs	Key in an IP address in the available field and click the add icon.
Applications	Key in a specific application name in the available field and click the add icon. To select multiple applications at the same time, click the menu icon next to the add sign, select the required applications and click Add To Policy .

3.4.7 Bandwidth Limit

Select the type of bandwidth limit applied to users. Select from the following options:

Option	Description
Total Bandwidth	Select to set a limit according to specific value for combined download and upload bandwidth.
Download	Select to set a limit according to specific value for download bandwidth.
Upload	Select to set a limit according to specific value for upload bandwidth.
Size	Input a value in the available field and select KB, MB or GB from the drop down menu.
Period	Specify if the limit is set per hour, day, week or month.

3.4.8 Time Limit

Define time limits during which users specified in the policy are allowed/denied to perform particular actions.

Option	Description
Limit by	Key in a value to set a limit.
Time	Select if the limit value is in minutes or hours from the drop down menu.
Period	Specify if the limit is set per hour, day, week or month.

3.4.9 Breacher notifications

Use the **Breacher** element to enable notifications to send when a user infringes policy. Provide the body text of the notification email in the available space.

For example, you can trigger a notification in a policy that blocks Pornography. The message would say: 'Pornography is strictly prohibited.'

3.4.10 Administrator notifications

Use the **Administrators** element to send notifications when a user infringes a policy. Add the administrator's email address and provide the body text of the notification email. Some examples include:

- » Notifications when a specific threshold is exceeded. Thresholds can be related to number of sites accessed, blocked or the number of times a user bypassed warnings.
- » Notifications sent to administrators when a bandwidth limit is exceeded. Limits can be set on the total bandwidth (download + upload traffic) consumed during a designated period, on download traffic only or on upload traffic only.
- » Notifications when specific security issues arise. These include detection of cyber-attacks, virus detection, phishing campaigns and potential threats from malware.

3.4.11 Log Alert

Add the Log Alert element to any policy to automatically send alert notifications when the criteria in the configured policy are met. Sent alerts are visible from the [Notification Center](#).

3.4.12 Hits alert

Specify the number of hits per period after which GFI WebMonitor sends a notification specified in the Breacher and/or Administrator elements.

Option	Description
The number of hits before a notification is triggered	Input a value in the available field.
Period	Specify if the limit is set per hour, day, week or month.

3.4.13 Schedule

Use the **Schedule** element to specify the time period during which the new policy is enforced.

1. In the **Applies from** and **to** fields, specify the time during which the policy will be active.
2. Select the days of the week.
3. Click **Add**.

3.4.14 Policy Expiry

Specify a deactivation date after which the policy will become inactive.

1. Click in the **Automatically deactivate policy on** field and select a date from the calendar.
2. Click in the **at** field to key in the time.

3.4.15 Logging

Click **Enable full URL Logging** to 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.

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. For more information, refer to [Configuring Activity Logging](#) (page 118).

3.4.16 How to use Default Policies

A default policy is automatically created when GFI WebMonitor is installed. This is the fallback policy – if no policies are matched for a given situation, the default policy will apply.

This policy is configured to **Allow** all Internet traffic to **Everyone**. You can change the policy type to **Block**, but you cannot delete or disable this default policy. New policies are added on top of the default policy to provide monitoring and filtering options as required.

2 additional policies are also enabled by default when GFI WebMonitor is installed:

Policy	Description
Blacklist	The Blacklist is a list of sites, users and IP addresses that are always blocked by GFI WebMonitor.
Whitelist	The Whitelist is a list of sites, users and IP addresses that are automatically excluded from all filtering policies configured in GFI WebMonitor.

The default policies:

- » Apply to everyone
- » Can be edited - customization of default policy is limited
- » Cannot be disabled or deleted

We recommend you use the blacklist policy to block only highly problematic websites, typically considered as high risk (for example, sites in the following categories: Adult / Porn, Gambling in general, Malware, Spyware, Piracy & Copyright Theft, Phishing Sites, Botnets, Remote Proxies, SPAM and Infected Sites).

3.4.17 How to create a new blocking policy

In addition to the pre-configured and default policies which are automatically installed, you can add more policies to refine your setup. The following steps guide you through the steps required to create a new policy that blocks social networks and other leisure browsing to most users during office hours, but allows it for top management, marketing and specific users.

<p>Allow</p> <p>Accept web request(s) meeting this policy criteria and do not execute subsequent policies</p>
<p>Block</p> <p>Block web request(s) meeting the following policy criteria and do not run subsequent policies</p>
<p>Warn</p> <p>Warn users making web request(s) and do not run subsequent policies</p>
<p>Monitor</p> <p>Discretely monitor web traffic that meets this policy criteria and keep processing subsequent policies</p>

Screenshot 20: Using the block action to create policies that stop undesirable traffic

To create a new policy:

1. Go to **Manage > Policies**.
2. Click **Add Policy**.
3. In the **Policy Name** field, enter **Block social networks and leisure browsing**.
4. In **Policy Description**, enter a description.
5. In the **Block, Warn, Allow, Monitor** element, select **Block**
6. From the left sidebar, add the **Websites** element to block categories such as Auctions, Dating, Entertainment / Venues / Activities, Fashion and Beauty, Games, Travel & Tourism, Web based chat, Music, Recreation and Hobbies, Shopping / Retail, Social Network in general and any other categories which could cause productivity issues in your company. Remember also to block any Security and Legal Liability categories.
7. This policy blocks all users. To exclude specific users add the **Users, Groups, IPs** element to the policy. Use the **Exceptions** element to configure any exclusions.
8. Add the **Schedule** element and define the policy to be active Monday to Friday, during working hours (for example 08:00 to 12:00, and 13:00 to 17:00). This means the policy will not apply during lunch break hours and after office hours.
9. Click **Save**.

3.4.18 How to create a streaming media policy

Bandwidth hogging can be a major concern in any organization. GFI WebMonitor can help you reduce the headaches associated with bandwidth intensive operations through appropriate blocking policies.

Streaming audio and video are bandwidth intensive. Coupled with the fact that this is not a temporary download, but can go on for extended periods of time, streaming media can quickly create bandwidth issues. Internet radio can easily be forgotten and you only require a few users to create a serious bottleneck. Websites in the News and Sports categories are also bandwidth intensive due to video streaming – and highly newsworthy events or sports events can create serious bandwidth issues.

For this purpose, we suggest you create a streaming media policy as described below:

1. Go to **Manage > Policies**.
2. Locate one of the existing blocking policies. Hold and drag to the middle of the UI and drop it over **Drag policies here to clone**.
3. In the **Policy Name** field, replace the existing name with **Block streaming media**.
4. In **Policy Description**, enter a description.
5. In the **Block, Warn, Allow, Monitor** element, select **Block**
6. From the left sidebar, add the **Websites** element and block categories such as: Music, Entertainment/Venues/Activities, News, Peer to Peer / Torrents, YouTube and Streaming Media.
7. Add the **Applications** element and block the Streaming Media category.

NOTE

The policy we are creating blocks all users. If you wish to exclude specific users add the **Users, Groups, IPs** element to the policy.

8. Click **Save**.

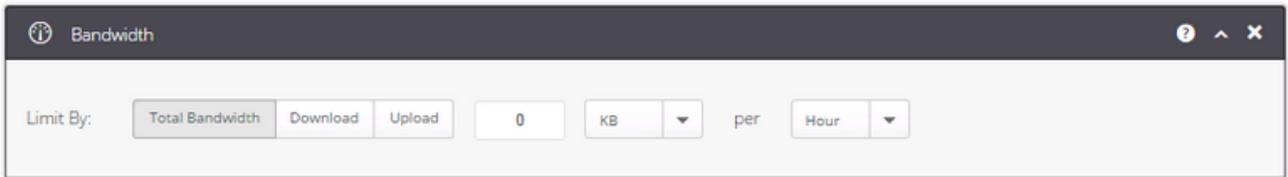
3.4.19 How to create a bandwidth threshold policy

GFI WebMonitor enables you to create bandwidth thresholds on a per user level. For example, you can create a policy that allows users to download from specific sites not more than 100 MB.

Note that you can add users to an Active Directory group, and add the group in the **Users/Group/IP Element**. The limits will still be applied to each individual user in the group.

To limit bandwidth intensive sites to a specific download value:

1. Go to **Manage > Policies**.
2. Click **Add Policy**.
3. In the **Policy Name** field, enter **Block by bandwidth limit**.
4. In **Policy Description**, enter a description.
5. In the **Block, Warn, Allow, Monitor** element, select **Block**
6. From the left sidebar, add the **Users, Groups, IPs** element to add specific users known to be “Bandwidth Hogs”.
7. Add the **Websites** element and select the following categories: **Peer to Peer / Torrents, Storage Services** and **Streaming Media**. These filters will apply to YouTube and similar sites.



Screenshot 21: Adding a Bandwidth control to limit data consumption within a certain period.

8. Add also the **Bandwidth** element and configure it to limit by downloads of 100 MB per day.
9. Click **Save**.

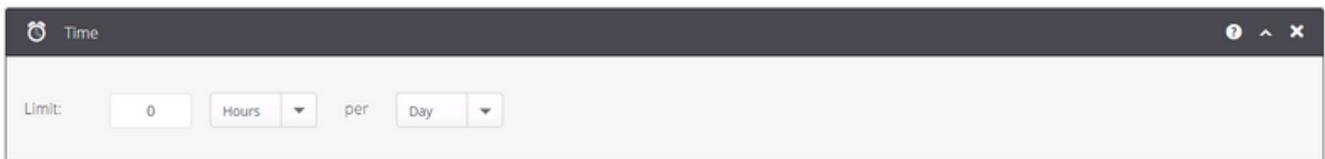
3.4.20 How to create a time threshold policy

GFI WebMonitor enables you to create policies that allow a user/group to browse certain websites for a maximum amount of time per day only. For example, you can create a policy that allows users to browse specific sites for only 30 minutes a day.

Social Networking is a good candidate for creating blocking or limiting policies based on browsing time, since sites in this category often create serious productivity loss. Policies can be created that limit the amount of time spent on these websites.

To create a policy for Social Networking:

1. Go to **Manage > Policies**.
2. Click **Add Policy**.
3. In the **Policy Name** field, enter **Block social networks by time limit**.
4. In **Policy Description**, enter a description.
5. In the **Block, Warn, Allow, Monitor** element, select **Block**.
6. From the left sidebar, add the **Users, Groups, IPs** element to add specific users known to be “Social Network” addicts.
7. Add the **Websites** element and add the **Social Network in General** category.



Screenshot 22: Set a time limit within a period in which a category is allowed

8. Add also the **Time** element and configure the limit to 30 minutes per day.

NOTE

You can add users to a group, and add the group in the **Apply Policy To** field. The limits will still be applied to each individual user in the group.

9. Click **Save**.

3.4.21 Using a soft blocking policy

We all know that although web filtering is required, being too restrictive may cause resentment. It may also lead to people actually being stopped from doing productive work when some certain legitimate sites are blocked.

With soft-blocking you can advise a user that it is against the organization's policy to visit the site, and leave it up to the user to decide whether they really need to access this site or not. This allows you to empower your users rather than stifle them.

NOTE

To apply "soft-blocking" policies, use the **Block, Warn, Allow or Monitor** element in configured policies. Instead of "Block" use the "Warn" option.

3.5 Configuring Exceptions

To configure exceptions in GFI WebMonitor you can either use the **Blacklist** and **Whitelist** policies or use the **Exceptions** element in the policy builder, which can be added to any custom policy.

The **Blacklist** is a list of sites, users and IP addresses banned from performing any web activity. The **Blacklist** list takes priority over all policies.

The **Whitelist** is a list of sites, users and IP addresses automatically excluded from all filtering policies configured in GFI WebMonitor, allowing them to bypass filtering and scanning policies.

IMPORTANT

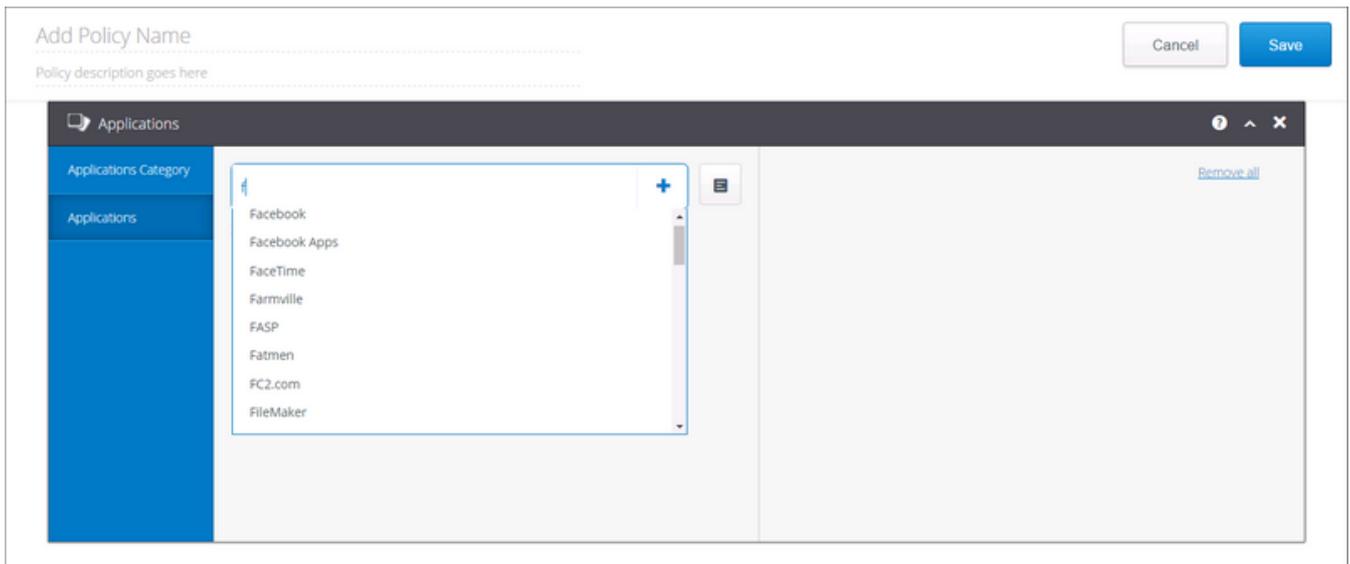
In GFI WebMonitor, the **Blacklist** takes priority over the **Whitelist** list. Therefore, if a site is listed in the **Blacklist** and that same site is listed in the **Whitelist**, access to the site is blocked.

The **Exceptions** element can be added to any custom policy to add exceptions per policy for:

- » Specific users
- » Groups of users
- » Websites and IP addresses
- » Specific applications

3.6 Application control

Using the **Applications** element within the policy builder, you can exert control over applications used within your organization.



Screenshot 23: GFI WebMonitor allows a granular control over the applications running on your network.

This includes instant messaging apps, social networking, games, streaming apps and many more.

If a policy is breached, GFI WebMonitor uses the configured policy to determine what action to take.

When GFI WebMonitor is installed, a number of pre-configured policies are automatically configured for your convenience. These policies are switched off by default but can be enabled as required:

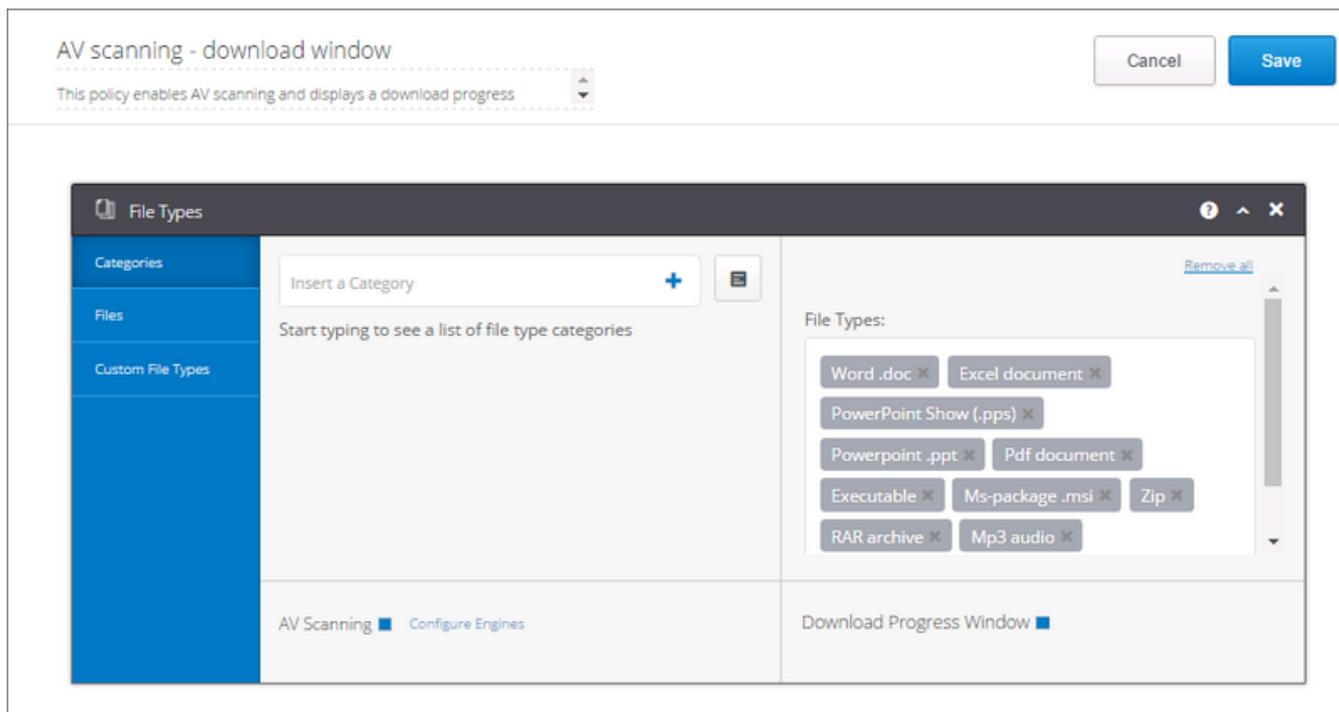
- » Block streaming media applications
- » Block P2P
- » Block free VPN and Tunneling applications
- » Block application access to Proxy and Anonymity networks

During trial these policies are typically sufficient, but if you wish to create a new policy or edit one of the existing policies, you can do this from: **Manage > Policies**.

For more information, refer to [Adding a new policy](#) (page 46).

3.7 Security scanning policies

The **Security Scanning Policy with Download Window** policy that ships by default with GFI WebMonitor is pre-configured to block files that may contain malicious content. This policy is set to apply to every user on the domain and to scan all file types using the inbuilt BitDefender and Kaspersky engines. This policy can be modified as required.



Screenshot 24: AV Scanning policy is configured to scan downloads for security threats.

The **Download Progress Window** option in this policy ensures that a progress window is shown whenever a users tries to download a file. If you don't want your users to see a download progress bar, uncheck this option.

To view or edit this policy go to **Manage > Policies**. You can customize the policy as necessary; however, the initial setup should suffice for the trial period.

3.8 Monitoring and filtering Internet browsing

Using the Websites elements, GFI WebMonitor gives you the facility to create policies aimed at monitoring and filtering user browsing. , GFI WebMonitor determines what action to take, according to what you configured in that policy. This may be one of the following actions:

- » **Allow, Block, Warn or Monitor** Internet browsing
- » **Scan** URLs for viruses and malicious content
- » **Filter by reputation** using inbuilt controls that apply filters based on a website's reputation
- » **Notify** specific users when certain URLs are requested
- » **Limit** - limit browsing based on surf time or bandwidth limits

GFI WebMonitor ships with a number of pre-configured policies that are typically sufficient for the purposes of the trial. However, if you wish to create a new policy or edit one of the existing policies, you can do this from: **Manage > Policies**.

3.9 Editing an existing Policy

To edit an existing policy:

1. Go to **Manage > Policies**.
2. From the policy sidebar, select an existing policy.
3. Click **Edit** to enter in edit mode.

4. Change the required settings.
5. Click **Save**.

3.10 Cloning a Policy

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

To clone a policy:

1. Go to **Manage > Policies**
2. From the policy sidebar, select an existing policy.
3. Hold and drag the selected policy to the main window.
4. The cloned policy is added to the policy sidebar.
5. Select the cloned policy and click **Edit** to configure.
6. Click **Save**.

NOTE

Default policies cannot be cloned.

3.11 Enabling or disabling a configured policy

To enable or disable a policy:

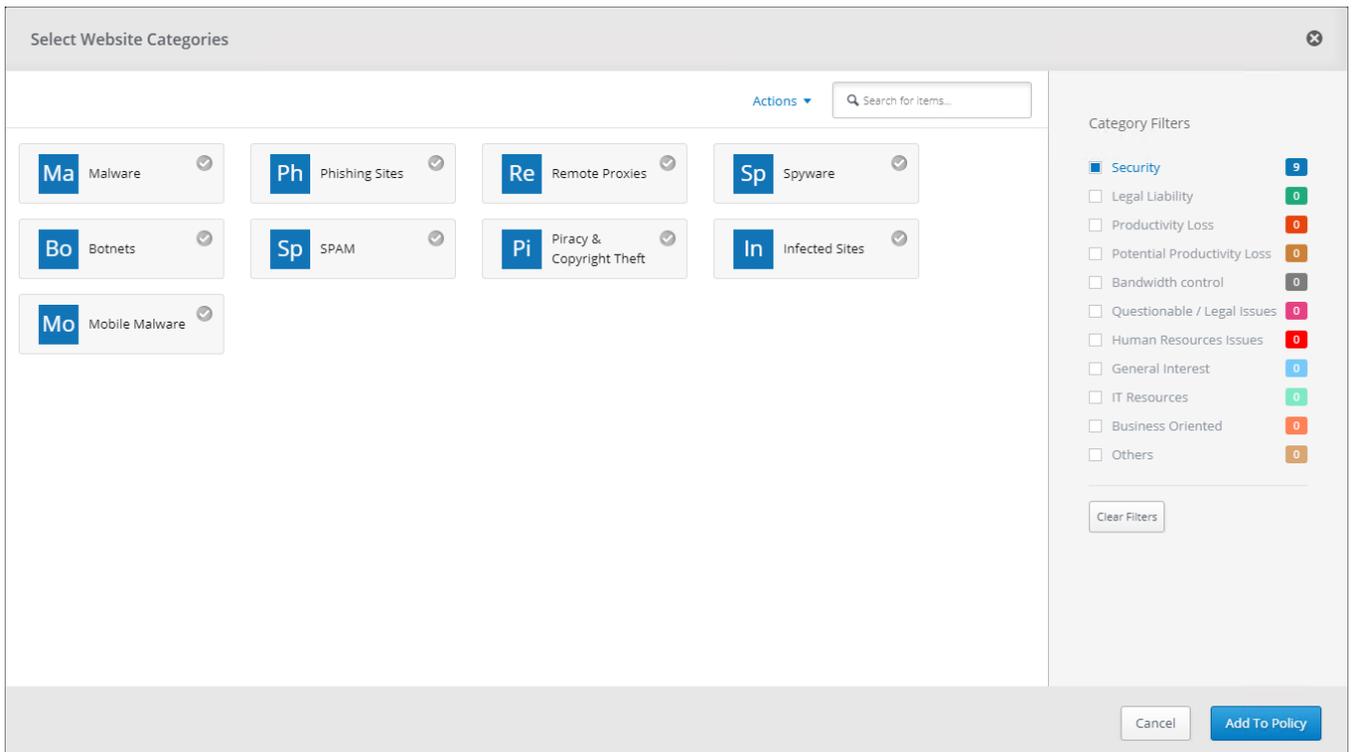
1. Go to **Manage > Policies**.
2. Click the switch next to the desired policy to enable or disable.

3.11.1 Deleting a policy

To delete a policy click on the policy you want to delete, hold and drag into the recycle bin icon.

3.11.2 Web Categorization

GFI WebMonitor provides the functionality to categorize URLs into one or more categories.



Screenshot 25: Categories available under the Security filter

The categories can be used to create or edit policies to block or allow sites based on the category they are classified. For more information, refer to [Working with Policies](#) (page 41).

The [WebGrade customer feedback](#) form can be used to submit feedback on URLs categorized within the WebGrade Database.

The submissions for corrections in the categorization of websites are considered daily. After a decision has been made to add a website, changes will be implemented in the database.

Note that the process may vary depending on several factors since each submission needs to be individually reviewed. It may take a few days for the change to reflect in the software. As an alternative while we process your request, please consider whitelisting or blacklisting the URL in question.

A list of the available categories can be found in this knowledge base article:

<https://www.gfi.com/support/products/gfi-webmonitor/GFI-WebMonitor-WebGrade-Database-category-information>

3.12 Using the Dashboards

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

Option	Description
Overview (Home)	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.

Option	Description
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.
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 [Configuring Anonymization](#) (page 119).

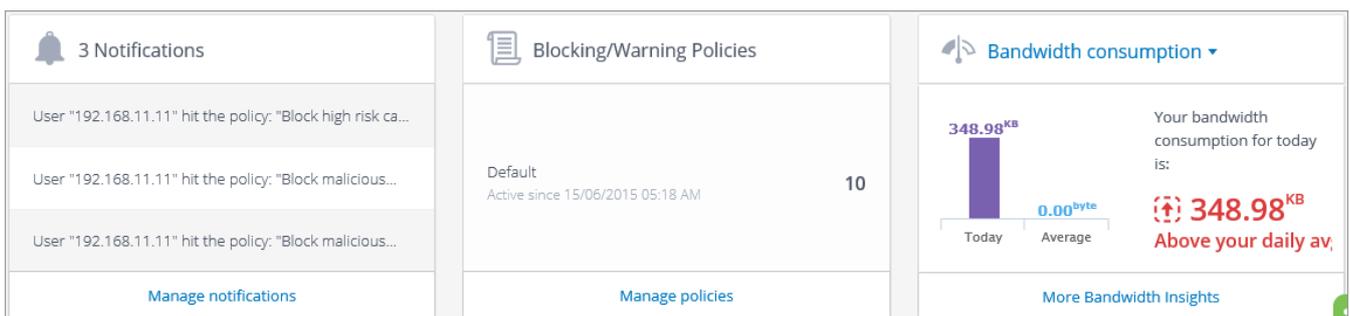
3.13 Overview of Internet Activity

On **launching** GFI WebMonitor, the home page is displayed by default. You can return to the home page anytime by clicking **Home** in the main navigation bar.

The page contains information about Internet usage trends, such as:

- » The bandwidth trends for the current day
- » Web Security issues identified by GFI WebMonitor
- » Top Web Categories displayed either by bandwidth consumed or by number of users
- » Top Web Applications displayed either by bandwidth consumed or by number of users
- » Top users consuming the most bandwidth.
- » Information related to current web sessions

3.13.1 Product Status



Screenshot 26: Product status widgets

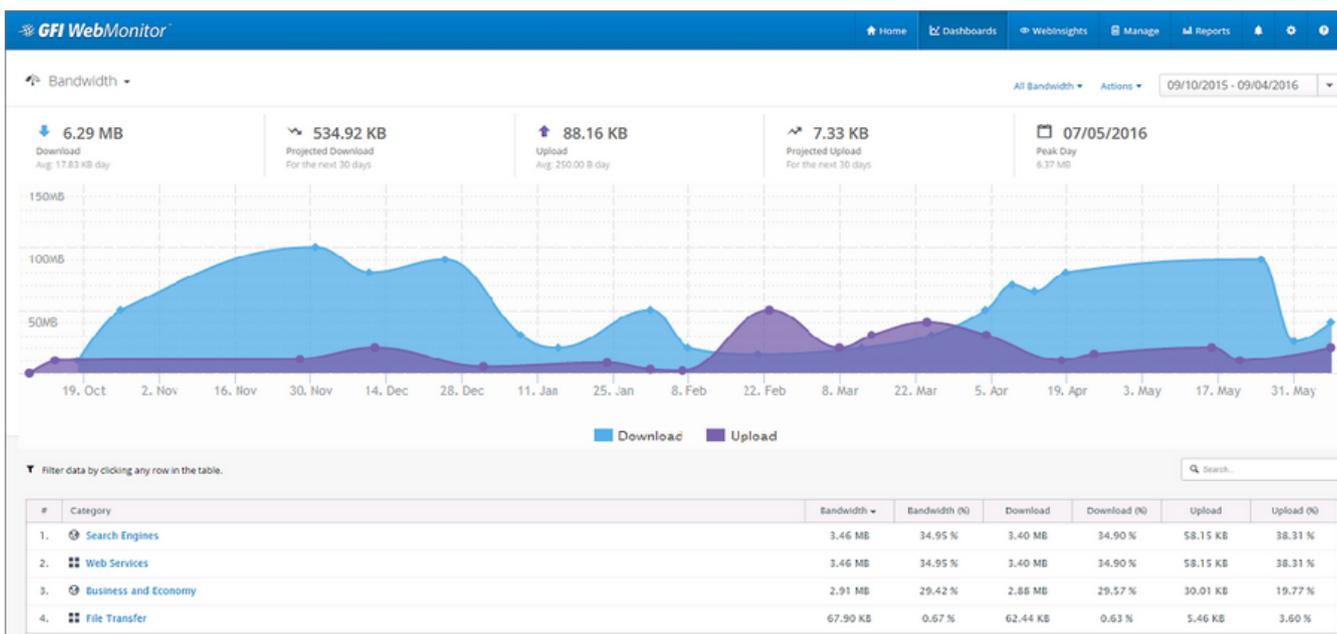
Use the **Status widgets** at the bottom of the page to verify details related to:

Status	Description
Notifications	A list of critical items is displayed in the home page for the attention of the System Administrator. Links are provided to the item that requires attention. Click Manage notifications to view the Notification Center.
Active Policies	Check how many policies are active and use the Manage policies shortcut to manage configured policies or create new policies. For more information, refer to Working with Policies (page 41).

Status	Description
Bandwidth consumption	Displays the average bandwidth consumption for the current day. Click More Bandwidth Insights to be redirected to the Bandwidth Insights page. For more information, refer to Bandwidth Insights (page 78).
Licensing	Click on the drop down list next to Bandwidth Consumption and select Licensing to display the number of active users being monitored. Click Update license to view the current license or enter a new key. For more information on how GFI WebMonitor counts users for licensing purposes, refer to Knowledge Base article: http://go.gfi.com/?pageid=WebMon_Licensing .

3.14 Monitoring Bandwidth

The Bandwidth dashboard provides information related to traffic and user activity that affects bandwidth consumption.



Screenshot 27: Bandwidth dashboard gives an overview of Internet activity.

To access the dashboard, click **Dashboards > Bandwidth**.

A summary at the top provides the following information:

- » Download
- » Projected Download
- » Upload
- » Projected Upload
- » Peak Day

Filter Dashboard data according to the following:

Option	Description
All Bandwidth	Shows download and upload traffic.
Websites	Displays bandwidth consumed by websites only.
Applications	Displays bandwidth consumed by applications only.
Download	Displays only downloaded traffic.

Option	Description
Upload	Displays only uploaded traffic.
Period	Use the controls to switch between Hour, Day, Week or Month.
View by:	Use the filter in the top right corner of the page to view data for a specific date range.

The lower side 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 bandwidth consumption for each category.
Websites/Applications	A list of websites and applications with information related to bandwidth consumption.
Users	A list of users and bandwidth consumption information for a specified period.
Event Log	A log of all the web requests for a single day, displaying: <ul style="list-style-type: none"> » Website/Application Name » Time - date and time of request » User - User name » IP - IP address » Machine Name - the name of the machine from which the request originated.

3.14.1 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 **Actions** and select **Export Report**.
2. GFI WebMonitor displays the exported report in a separate window in your browser.
3. Click **Save** 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 **Actions** and select **Schedule Report**.
2. GFI WebMonitor redirects you automatically to the **Reports** area.
3. Edit the report as required.
4. Save the report.

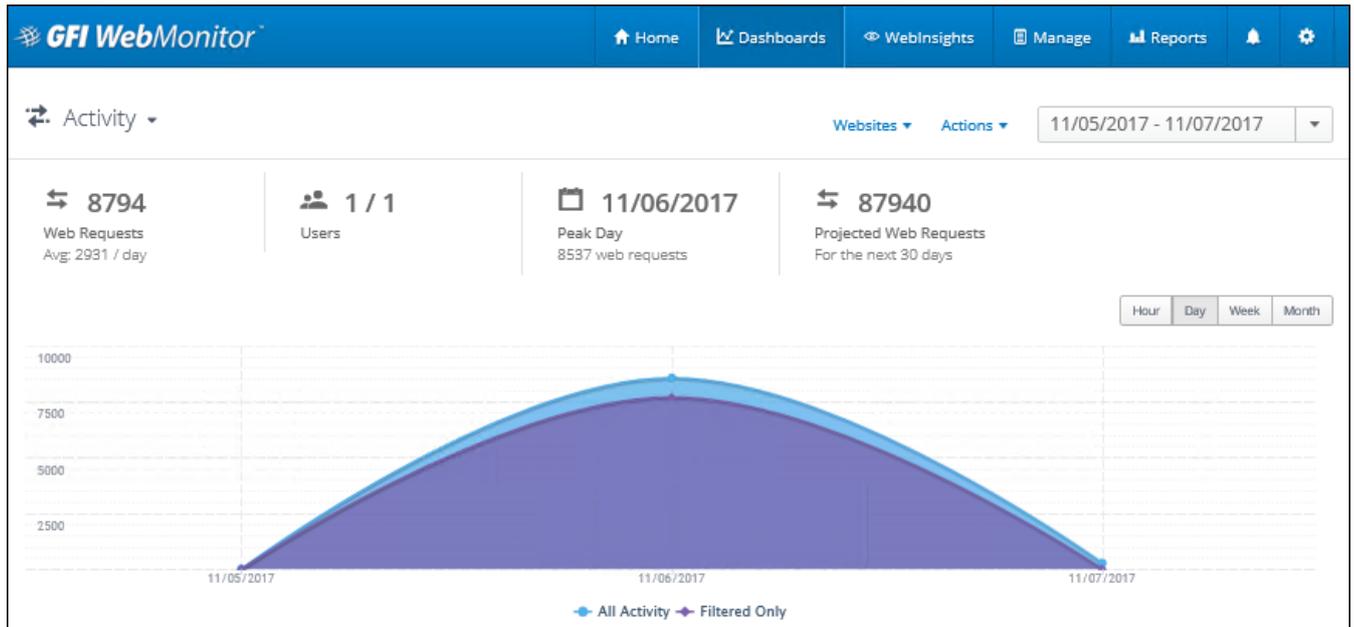
For more information, refer to [Working with Reports](#) (page 79).

IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information, refer to [Configuring Anonymization](#) (page 119).

3.15 Monitoring Activity

The **Activity** dashboard provides information related to web requests and user activity for a specified period. To access the dashboard, click **Dashboards > Activity**.



Screenshot 28: Activity Dashboard

A report summary at the top provides the following information:

- » Users
- » Peak Day
- » Requests
- » Projected Requests

Filter dashboard data according to the following:

Option	Description
All Activity	Shows all web requests (filtered and unfiltered) made through GFI WebMonitor in the specified period.
Websites	Displays only traffic related to websites.
Applications	Displays only traffic related to application usage.
Searches	Shows the activity related to searches performed by users.
Period	Use the controls to switch between Hour, Day, Week or Month.
View by:	Use the filter in the top right corner of the page to view data for a specific date range.

Categories Websites/Applications Users Event Log							
<input type="text" value="Search..."/>							
#	Websites/Application Name	Time	Machine Name	User	IP	Policy Action	Block
1.	YouTube	11/07/2017 00:07	WIN-IGUVT54F14D.ec2.internal	10.175.1.131	10.175.1.131	Allowed	
2.	beacons.gvt2.com	11/07/2017 00:07	WIN-IGUVT54F14D.ec2.internal	10.175.1.131	10.175.1.131	Allowed	
3.	YouTube	11/07/2017 00:07	WIN-IGUVT54F14D.ec2.internal	10.175.1.131	10.175.1.131	Allowed	
4.	169.254.169.254	11/07/2017 00:06	WIN-IGUVT54F14D.ec2.internal	10.175.1.131	10.175.1.131	Allowed	

Screenshot 29: Event Log tab

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 Requests for each category.
Websites/Applications	A list of websites and applications with information related to Requests .
Users	A list of users and the total Surf Time and number of Web Requests for a specified period. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE</p> <p>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> </div>
Event Log	<p>When Logging is enabled in Policies, GFI WebMonitor provides a log of all the web requests that fall within a specified period, displaying:</p> <ul style="list-style-type: none"> » Website/Application Name » Time - date and time of request » Machine Name - the name of the machine from which the request originated. » User - User name » IP - IP address » Policy Action - The action that was taken by GFI WebMonitor. » Block - For traffic that is allowed by GFI WebMonitor, click the block icon to block the user activity. A blocking policy is automatically created by GFI WebMonitor and the user is redirected automatically to the Policy area. Click Save to enable the blocking policy or Cancel to discard. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE</p> <p>The Event Log does not show any data when Logging is not enabled. For more information, refer to Logging (page 52).</p> </div>

3.15.1 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 **Actions** and select **Export Report**.
2. GFI WebMonitor displays the exported report in a separate window in your browser.
3. Click **Save** 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 **Actions** 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 [Working with Reports](#) (page 79).

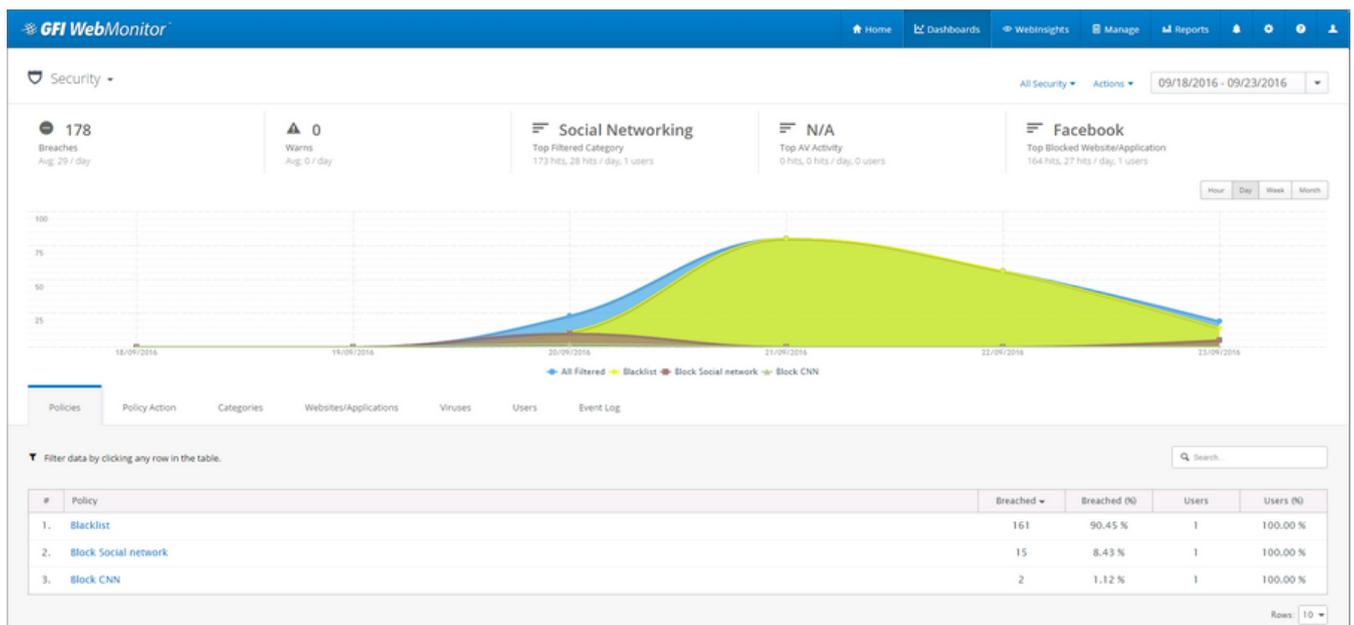
IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information, refer to [Configuring Anonymization](#) (page 119).

3.16 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.



Screenshot 30: Security Dashboard gives an overview of security issues on the network

To access this dashboard, click **Dashboard > Security**.

A report summary at the top provides the following information:

- » Breaches
- » Warns
- » Top Filtered Category
- » Top AV Activity
- » Top Blocked Website/Application

Filter available data to provide information related to:

Option	Description
All Security	Shows all activity made through GFI WebMonitor in the specified period.
Websites	Displays only security issues related to websites.
Applications	Displays only security issues related to application usage.
Period	Use the controls to switch between Hour, Day, Week or Month.
View by:	Use the filter in the top right corner of the page to view data for a specific date range.

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
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.
Policy Action	The type of action taken by GFI WebMonitor. Can be Blocked or Warned.
Categories	Select to view a list of categories with total number of Breaches for each category.
Websites/Applications	A list of websites or Applications with respective total number of Breaches . Data can be viewed by Domain or by Site using the provided controls.
Viruses	A list of detected viruses, with the total number of Breaches .
Users	A list of users and the total Breaches for a specified period, broken down under the following headings: Infected and Malicious .
Event Log	Provides a log of all the web requests that fall within the specified period, displaying: <ul style="list-style-type: none">» Websites / Application Name - URL of request» Time - date and time of request» Machine Name - the name of the machine from which the request originated.» User - User name» IP - IP address» Policy Action - The type of action taken by GFI WebMonitor. Can be Blocked or Warned.

3.16.1 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 **Actions** and select **Export Report**.
2. GFI WebMonitor displays the exported report in a separate window in your browser.
3. Click **Save** 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 **Actions** 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 [Working with Reports](#) (page 79).

IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information, refer to [Configuring Anonymization](#) (page 119).

3.17 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.

The Real-Time Traffic dashboard allows administrators to terminate connections that are having a bad impact in the network speed or bandwidth available.

IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information, refer to [Configuring Anonymization](#) (page 119).

Real-Time Traffic ▾		Active Connections ▾		Terminate	↻
<input type="checkbox"/>	IP(User)	Url	Status	Download ▾	Uploaded
<input type="checkbox"/>	10.175.1.131 (Unauthenticated)	https://api.wistia.com:443	Receiving from server	12.18 KB	1.33 KB
<input type="checkbox"/>	10.175.1.131 (Unauthenticated)	https://secure-gl.imnworl...	Receiving from server	4.83 KB	586.00 B
<input type="checkbox"/>	10.175.1.131 (Unauthenticated)	https://secure-gg.imnworl...	Receiving from server	4.83 KB	586.00 B
<input type="checkbox"/>	10.175.1.131 (Unauthenticated)	https://s.innovid.com:443	Receiving from server	4.03 KB	1.77 KB
<input type="checkbox"/>	10.175.1.131 (Unauthenticated)	https://secure-gg.imnworl...	Receiving from server	4.83 KB	586.00 B
<input type="checkbox"/>	10.175.1.131 (Unauthenticated)	https://s.innovid.com:443	Receiving from server	4.03 KB	1.77 KB

Screenshot 31: Active connections in Real-Time dashboard

To access the Real-Time Traffic dashboard:

1. Go to **Dashboards > Real-Time Traffic**.
2. Click one of the following tabs:

Option	Description
Active Connections	<p>Provides information related to current active connections. Active connections can be terminated to free up bandwidth. For more information, refer to Terminating active connections (page 71). Additional filtering is available by:</p> <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	<p>A graph displays the current bandwidth consumption in KB/sec. Additional information includes:</p> <ul style="list-style-type: none"> » IP (User) » Url » Status » Downloaded » Uploaded
Activity	<p>Displays the number of current web requests</p> <ul style="list-style-type: none"> » IP (User) » Url » Status » Downloaded » Uploaded

Click **Terminate** if you want to close any active connection. This option may be useful when large downloads are affecting the network speed.

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.

3.17.1 Terminating active connections

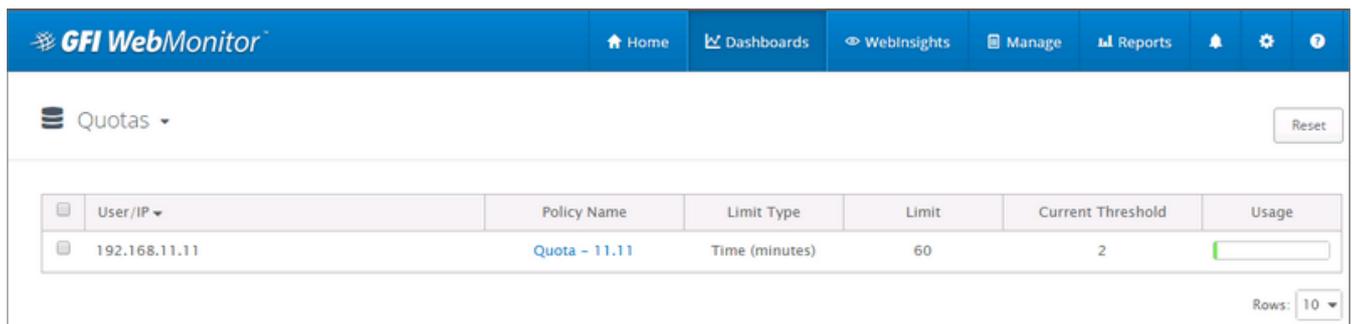
GFI WebMonitor enables you to terminate any active connections for bandwidth optimization. This action can be performed from the Real-Time Dashboard.

To terminate a connection:

1. Go to **Dashboards > Real-Time Traffic**.
2. Select **Active Connections** view.
3. Click the refresh button to display a list of currently active connections.
4. Select the connections you want to terminate and click **Terminate**.
5. Click **Confirm**.

3.18 Using the Quotas Dashboard

The **Quotas** dashboard lists active Policies based on web browsing quotas 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.



Screenshot 32: 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 Configuring Anonymization (page 119).
Policy Name	The name of the active policy. Click the policy name to access the settings page and edit the policy.
Limit Type	Limit by Bandwidth or by Time.
Limit	Displays the amount of Bandwidth or Time allocated in the respective Policy.
Current Threshold	Shows the current threshold for the configured policy. Click to sort by the current threshold.
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» Policy 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 **Dashboards > 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**.

3.19 Monitoring Agents

The Agents dashboard provides information related to the status of configured GFI WebMonitor Agents. The GFI WebMonitor Agent can be deployed on portable computers 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).

The information provided by the Agents Dashboard 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
Host Name	Machine name where the GFI WebMonitor Agent is installed.
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 Ver- sion	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 at the bottom of the dashboard lists Agent versions. This information is useful to identify outdated Agents.

Removing Agents from the Dashboard

Agents can be removed from the dashboard when, for example, they are no longer active. This action does not remove any information generated by the selected Agent/s or uninstall the WebMonitor Agent/s from the client machine.

To remove an Agent from the list:

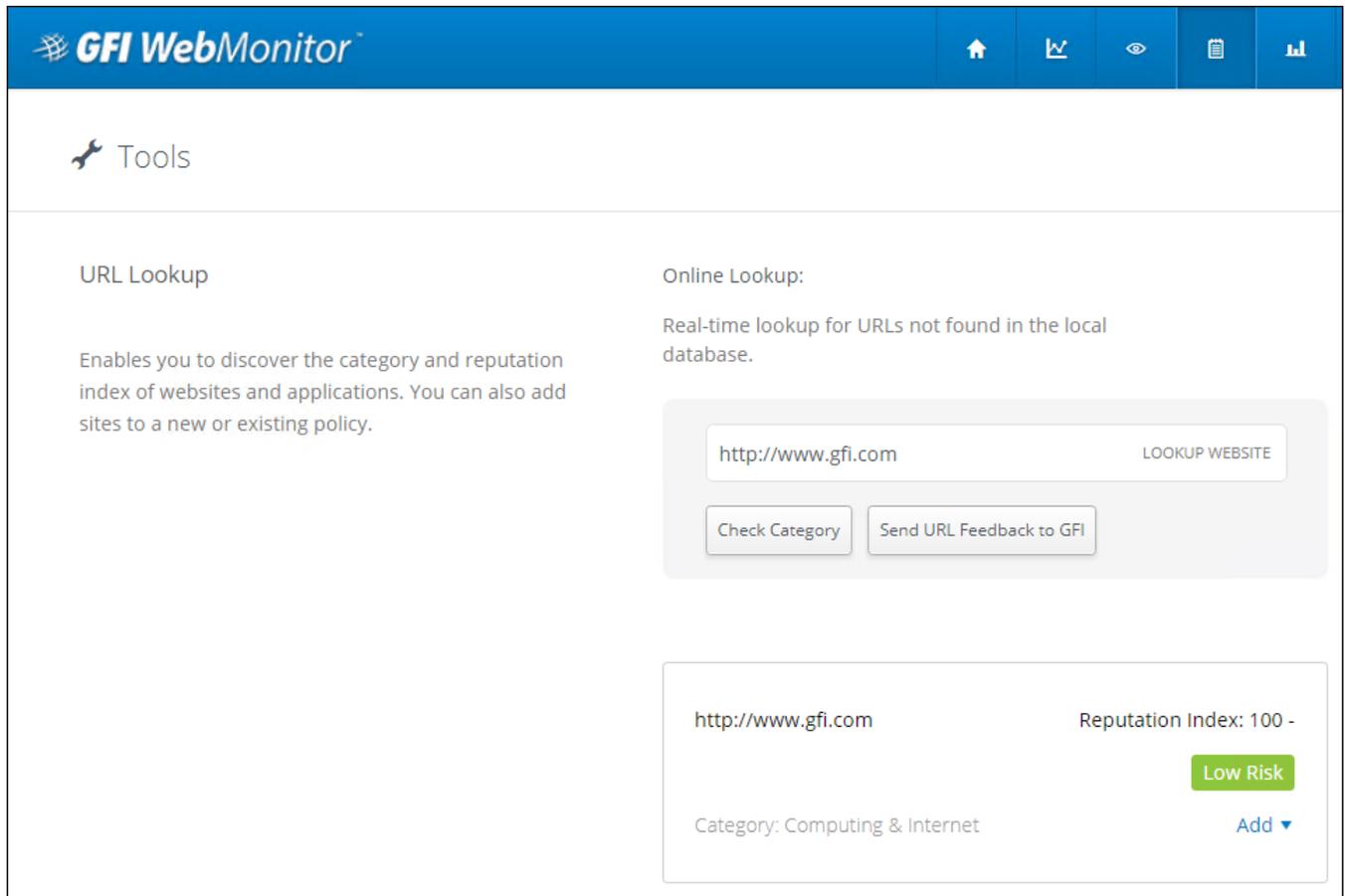
1. Go to **Dashboards > Agents**
2. Select the checkbox next to the Agent you want to remove.
3. Click **Delete**.

3.19.1 Using Web Category Lookup

When GFI WebMonitor is installed, a database populated 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 URLs not found in the local database.

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



Screenshot 33: URL Lookup tool

To look up a URL:

1. Go to **Manage > Tools**.
2. Enter a URL in the **Lookup website** field.
3. Click **Check Category**.
4. The **Category** and the **Reputation Index** are displayed. If you think the website is wrongly categorized, click **Send URL Feedback to GFI** to report the problem.
5. Click **Add** in the results box and perform one of the following actions:

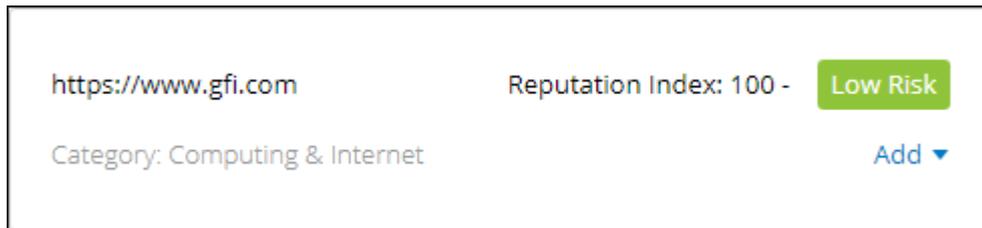
Action	Description
Add to existing policy	Click to open the policy wizard and add the selected URL to an existing policy.
Create new policy	Click to open the policy wizard and add the selected URL to a new policy.
Create new remote policy	Click to open the policy wizard and add the selected URL to a new remote policy.

3.19.2 Reputation Index

Reputation Index boosts protection against current and future malicious content on the web for Internet browsers. Using Reputation Index, websites are assessed for immediate and potential threats, malicious content and risky characteristics. A score numerical between 0 and 100 rates the threat.

Similar to the way Content Categorization places websites into different categories and classifies them based on their content, Reputation Index scores are used to determine the risk factor of each website.

Once the score for a website has been determined, an administrator can take action and block or allow access to those websites.



Screenshot 34: Reputation Index showing in the URL Lookup tool

To use reputation index:

1. Go to **Manage > Tools**.
2. Enter a URL in the **Lookup website** field.
3. Click **Check Category**.
4. The **Category** and the **Reputation Index** are displayed.

The Reputation Index are divided into four risk levels:

Level	Description
High Risk	Site known for malicious activities. GFI WebMonitor considers this as having reputation index value 0.
Medium Risk	Possible risk such as tracking, adware, etc. GFI WebMonitor considers this as having reputation index value 21.
Unknown	The site has never been seen. GFI WebMonitor considers this as having reputation index value 61.
Low Risk	Index value of 100. Site with relatively long history online and good popularity.

When creating a new policy, the Reputation Index can be used as criteria to filter websites. For more information, refer to [Websites](#) (page 49).

3.20 Using WebInsights

WebInsights is an interactive facility within GFI WebMonitor that uses real-time and historical records to deliver information related to Internet usage and trends. Using an internal behavior analysis engine, GFI WebMonitor establishes a baseline based on your historical Internet usage data.

The WebInsights dashboards compare real-time data to this baseline, enabling you to gain a quick insight on Web resource use, or misuse, while also identifying threats to your network.

IMPORTANT

The WebInsights dashboards are available in GFI WebMonitor 2015 SR2 edition and later.

The available dashboards are:

Dashboard	Description
Bandwidth Insights	The Bandwidth Insights dashboard provides information related to traffic and user activity that affects bandwidth consumption.
Security Insights	The Security Insights 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.
Productivity Insights	The Productivity Insights dashboard provides information related to web requests and user activity for a specified period. The information helps you identify unproductive users at a glance.

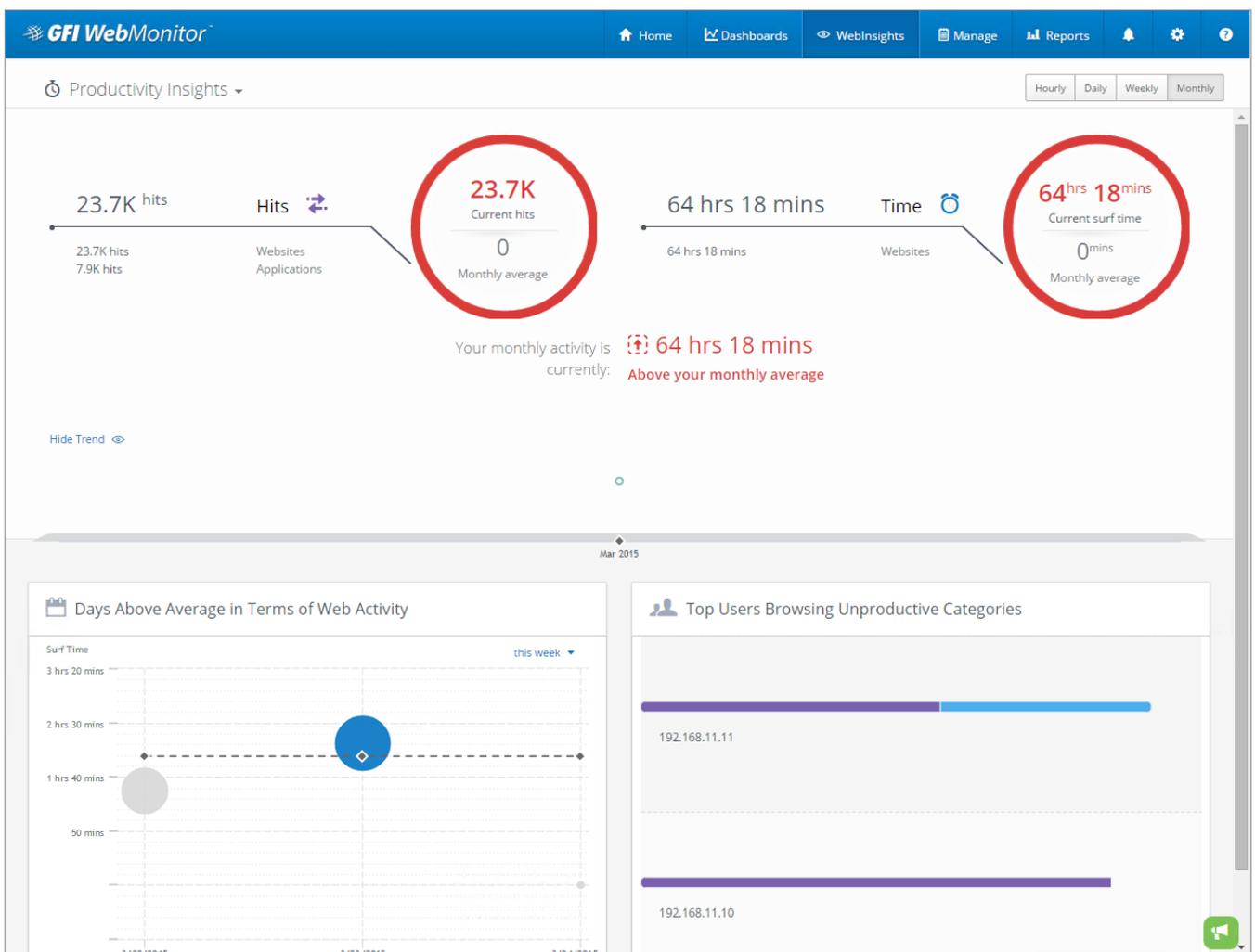
NOTE

When GFI WebMonitor is installed for the first time, the WebInsights dashboards do not display any data. Please wait for a minimum of 1 hour until GFI WebMonitor gathers enough information to start populating the dashboards.

3.21 Productivity Insights

The Productivity Insights dashboard provides information related to web requests and user activity for a specified period. The information helps you quantify your losses in terms of productivity and identify potential unproductive users, enabling you to take adequate action.

To access the dashboard, click **WebInsights > Productivity**.



Screenshot 35: Productivity Insights dashboard

NOTE

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

A summary at the top provides the following information:

- » Number of hits on websites and applications in the Productivity Loss category.
- » Time spent on websites and applications in the Productivity Loss category.
- » An estimate of productivity loss compared to the average for the same period.
- » Trend - this graph shows the peaks and lows of productivity loss compared to the average for the same period. Move the cursor over the graph to display the projected loss on the selected period.

The lower portion of the WebInsights Productivity dashboard is composed of two widgets:

- » The **Days Above Average in Terms of Web Activity** widget compares current productivity loss with the previous period averages. The period changes according to the filtering option selected.
- » The **Top Users Browsing Unproductive Categories** widget displays a list of users that browse sites that belong to unproductive categories.

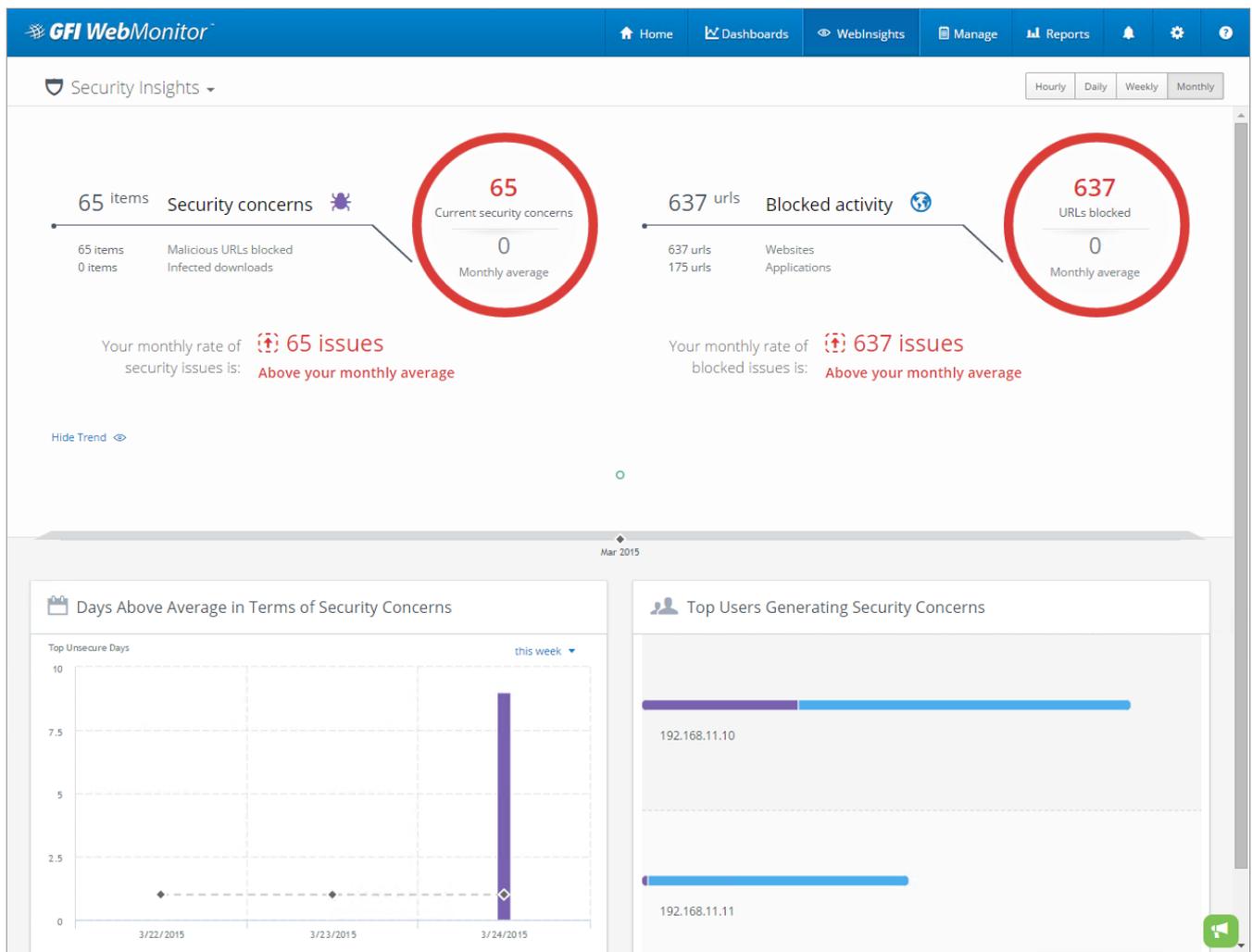
IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information, refer to [Configuring Anonymization](#) (page 119).

3.22 Security Insights

The Security Insights dashboard provides information related to malicious activity and infected files for a specified period. The information provided enables you to identify security risks and threats to your network environment at a glance.

To access the dashboard, click **WebInsights > Security**.



Screenshot 36: Security Insights dashboard

NOTE

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

A summary at the top provides the following information:

- » Security concerns broken down between blocked malicious URLs and infected downloads.
- » Blocked requests broken down between websites and applications.
- » Trend - this graph shows the peaks and lows of actual security issues compared to the average consumption for the same period. Move the cursor over the graph to display the amount of issues for the selected period.

The lower portion of the WebInsights Security dashboard is composed of two widgets:

- » The **Days Above Average in Terms of Security Concerns** widget shows on which days of the week your network experienced security concerns that were above average. Toggle the view between results for **this week** or for the **previous week**
- » The **Top Users Generating Security Concerns** widget displays a list of users that are accessing content that is creating security concerns to your organization.

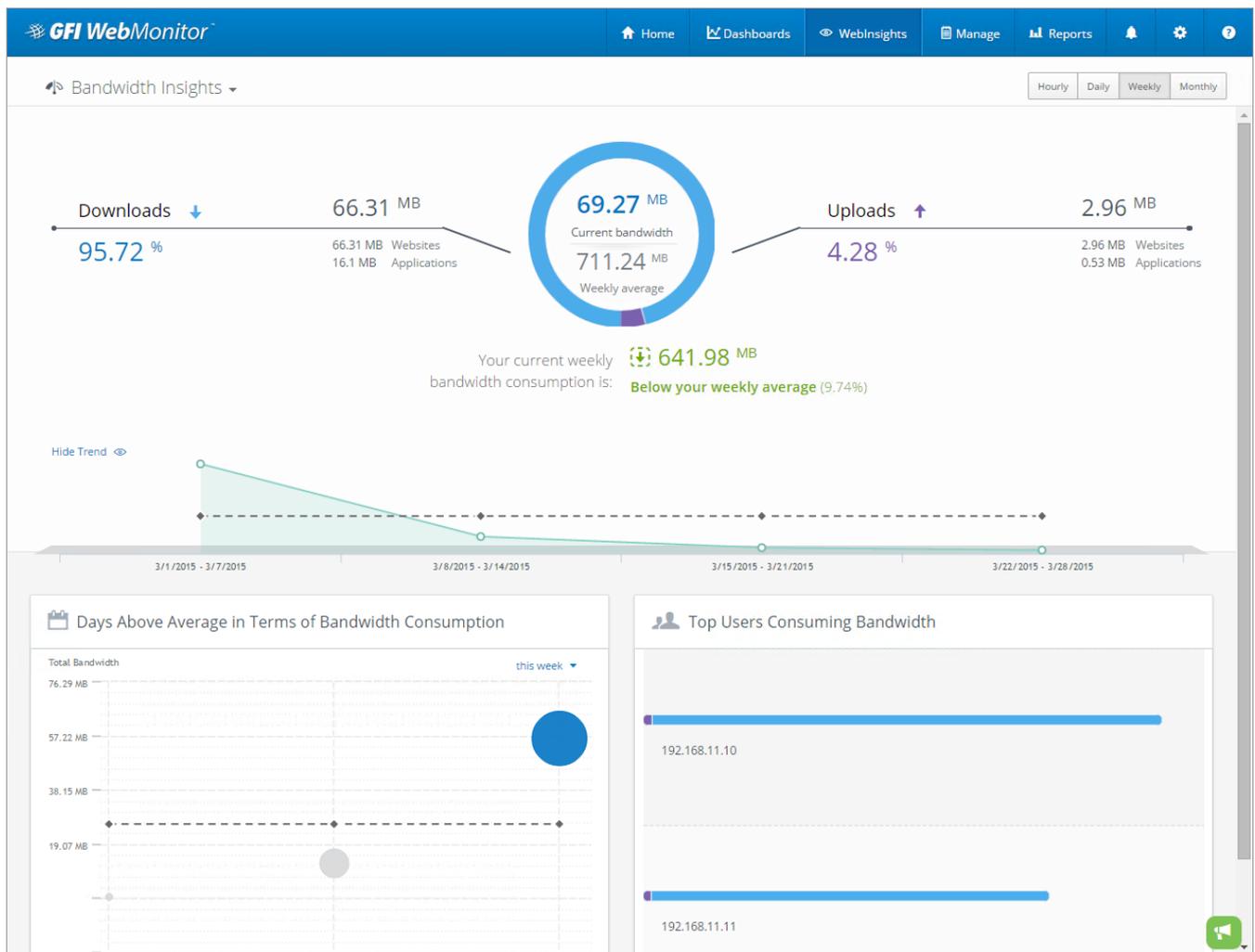
IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information, refer to [Configuring Anonymization](#) (page 119).

3.23 Bandwidth Insights

The Bandwidth Insights dashboard provides quick information related to traffic and user activity that affects bandwidth consumption. The dashboard is useful to understand how allocated bandwidth is being used on your network and to identify critical issues at a glance.

To access the dashboard, click **WebInsights > Bandwidth**.



Screenshot 37: Bandwidth Insights dashboard

NOTE

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

A summary at the top provides the following information:

- » Bandwidth consumed by user downloads. This information is broken down between downloads originating from websites and that originating from applications.

- » Bandwidth consumed by user uploads. This information is broken down between uploads to websites and to applications.
- » Total bandwidth consumption for the selected period. The total downloads plus total uploads. The amount is compared to the average for the same period.
- » Trend - this graph shows the peaks and lows of actual bandwidth consumption compared to the average consumption for the same period. Move the cursor over the graph to display the amount of download and upload bandwidth consumed on the selected period.

The lower portion of the WebInsights Bandwidth dashboard is composed of two widgets:

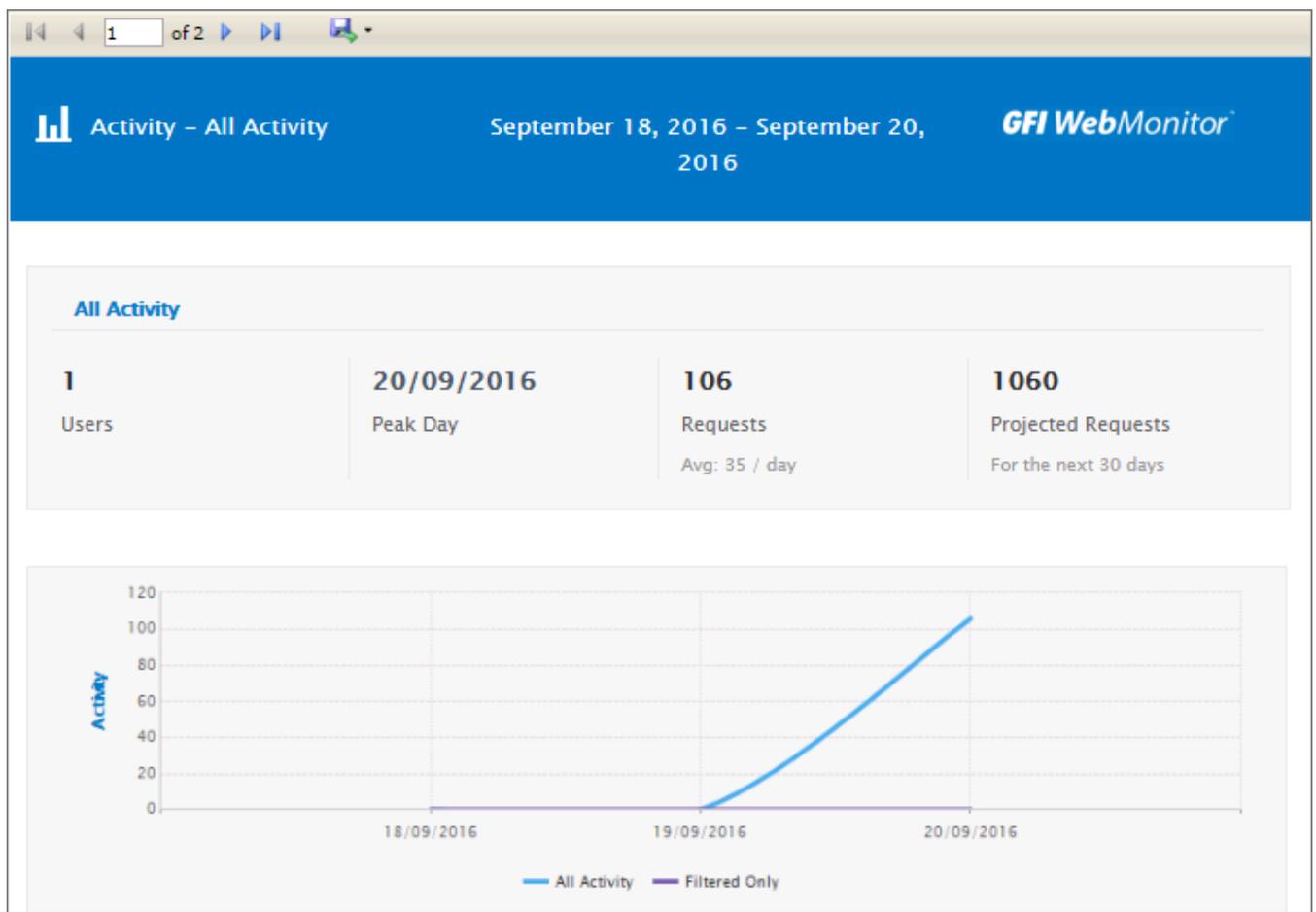
- » The **Days Above Average in Terms of Bandwidth Consumption** widget compares current bandwidth usage with the previous period averages. The period changes according to the filtering option selected.
- » The **Top Users Consuming Bandwidth** widget displays the users that consumed the most bandwidth.

IMPORTANT

If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information, refer to [Configuring Anonymization](#) (page 119).

3.24 Working with Reports

GFI WebMonitor enables administrators to access and generate reports that provide insight on Internet usage and trends.



Screenshot 38: A sample report

Use the reporting feature to create:

- » Department based reporting that can be scheduled and sent to the relevant department heads
- » Targeted and relevant reports based on inclusions and exclusions of users, categories and websites.
- » Need based reporting based on Browsing Activity / Bandwidth / Security and other needs
- » Scheduled reports distributed in various formats.

The following is a list of available report categories:

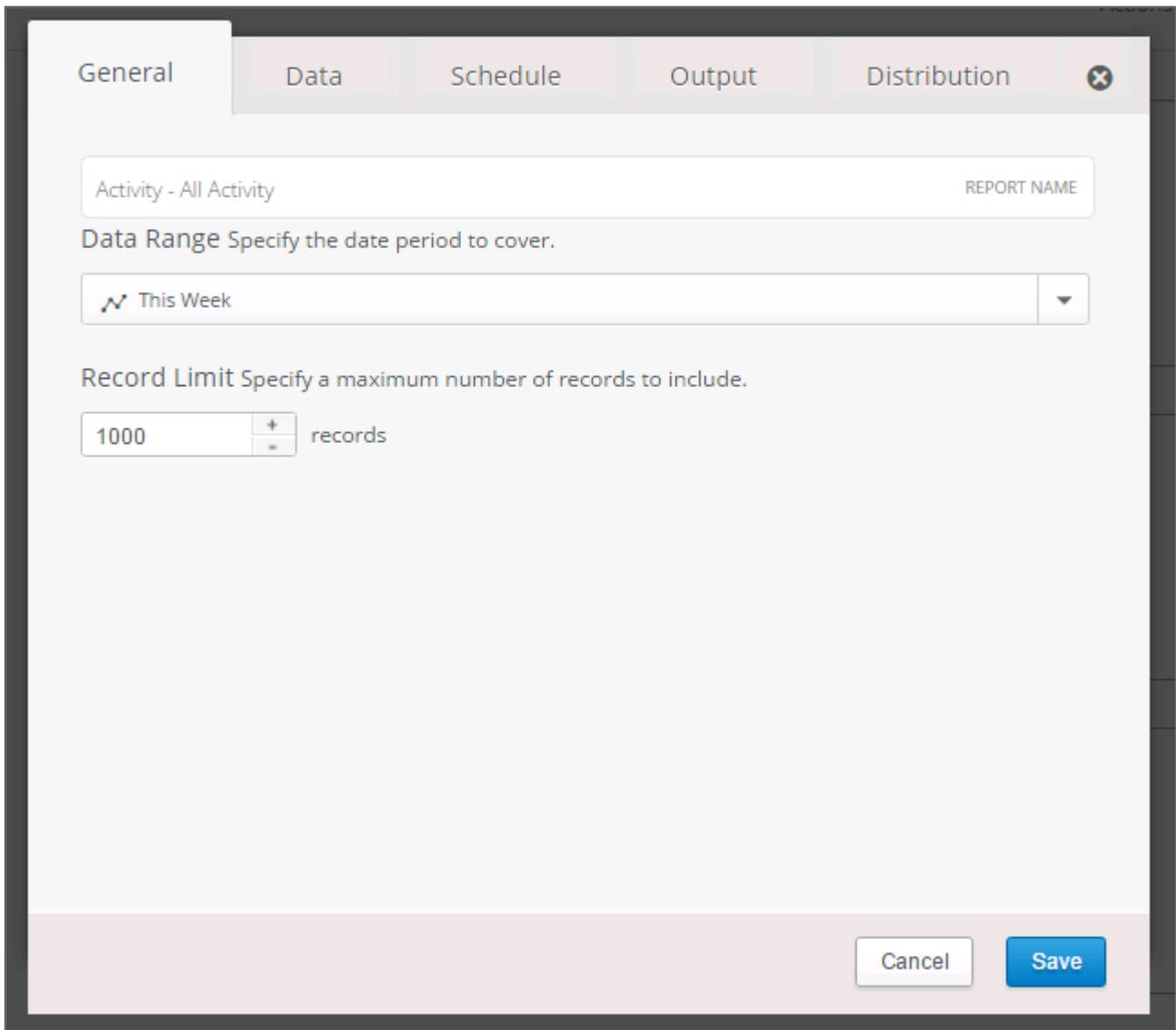
Report category	Description
All	All the reports from Activity, Bandwidth and Security are displayed in this area.
Bandwidth	Monitor bandwidth activity on your network. Use these reports to identify non-productive traffic, download trends and usage patterns.
Activity	Use activity reports to gain insight into what sites users are visiting, what applications they are using and what content is downloaded to your network.
Security	Spot any security problems to prevent attacks to your network. The security reports give you full visibility into results of virus detections, hits to malicious websites and other security issues.
Starred	A list of frequently used reports. Select a report you want to mark as favorite. Click the star in top left corner of the report tile.
Scheduled	Any reports scheduled to run at a future date are automatically added to this list.
Generated	Click Generated tab in the sidebar to display a list of previously generated reports.

To use one of the reports:

1. Go to **Reports** and select a report category from the left sidebar.
2. Click one of the report names to edit or click **Generate** to run the report.

3.24.1 Editing reports

All existing reports can be edited to change configured settings.



Screenshot 39: Edit reports to customize parameters.

To edit a report:

1. Go to **Reports**.
2. From the left sidebar select a report category.
3. Click the report tile to edit and click the Edit icon  within the tile.

Option	Description
General	<ol style="list-style-type: none"> 1. [Optional] Change the name of the report. 2. Provide a date range covered by the report. 3. Set the maximum number of records shown in the report (Default 1000).
Data	<p>Select the filters that will be applied to the report. For each filter specify the elements to include or exclude:</p> <ul style="list-style-type: none"> » Click Users/IPs to add users or IP addresses to include or exclude in the report. » Click Users Groups tab and add the users or groups to include or exclude in the report. » Click Websites tab and add the domains to include or exclude in the report. » Click Web Categories tab to add any of the pre-defined categories to include or exclude in the report » Click Applications tab to add the applications to include or exclude in the report » Click Policies tab to add the policies to include or exclude in the report

Option	Description
Schedule	<p>1. Click the Scheduled switch to enable report scheduling.</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin: 5px 0;"> <p>NOTE If the schedule is disabled, report is not automatically generated.</p> </div> <p>2. In the Runs area, select if report is going to be generated: Once, Daily, Weekly, Monthly</p> <p>3. In the Run every field, define the interval in days when the report is generated.</p> <p>4. In the Time to run field, specify at which time of day to execute the report.</p> <p>5. Use the Repeat until option to select if you want the occurrence to end after a specified period. Select Date and define the date, otherwise set the setting to Never (Default).</p>
Output	Select the report output format and specify a location to save the report.
Distribution	[Optional] Add a recipient email address to send the document by email.

4. Click **Save**.

5. To run the report, click **Generate**.

3.24.2 Cloning reports

All existing reports can be cloned to create new custom reports.

To clone a report:

1. Go to **Reports** and select one or more reports you want to clone.
2. Click **Actions > Clone**.
3. Change the name of the report and edit the report as required.

3.24.3 Removing reports

Cloned reports can be removed from the list of reports.

NOTE

GFI WebMonitor ships with a set of default reports that can be modified but cannot be deleted.

To remove:

o clone a report:

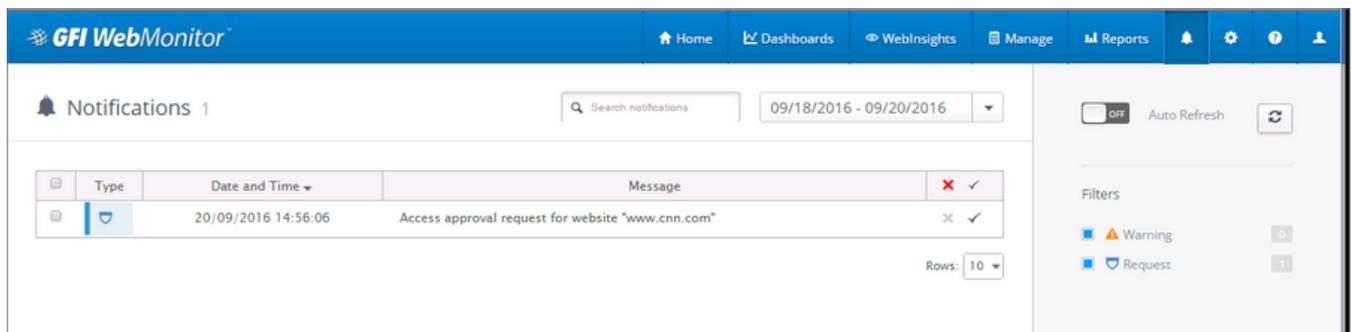
1. Go to **Reports** and select one or more reports.
2. Click **Actions > Remove**.
3. Click **OK** to confirm deletion.

3.25 Notification Center

Using the **Log Alert** element from within policies, GFI WebMonitor lets you configure alerts based on specific usage patterns, such as warnings bypassed or sites that have been blocked. Some examples include:

- » Monitoring alerts when a specific threshold is exceeded. Thresholds can be related to number of sites accessed, blocked or the number of times a user bypassed warnings.

- » Alerts when bandwidth limit is exceeded. Limits can be set on the total bandwidth (download + upload traffic) consumed during a designated period, on download traffic only or on upload traffic only.
- » Access requests from users asking approval to visit blocked sites.
- » Alerts related to security issues. These include detection of cyber-attacks, virus detection, phishing campaigns and potential threats from malware.



Screenshot 40: Viewing received notifications in the notification center

You can view a list of alerts in the Notifications Center. Click the notifications icon  in the toolbar and use the following filters to sort and view data:

Option	Description
Type	Indicates the type of the alert.
Date & Time	The date and time of the alert.
Message	A description of why the alert was triggered.
Auto-refresh	Disabled by default. Enable to periodically refresh the list of alerts.
Search	Key in search criteria and click the magnifying glass to search for specific alerts.
Warning filter	Click to display only warning alerts.
Request filter	Click to view only requests for temporary access to websites. These requests are generated from policies that block website access. To approve access, select the request you want to approve and click <input checked="" type="checkbox"/> to grant temporary access to the blocked website. If access is approved, a new temporary policy is created with top priority on the policies page. When approving, the IT Admin can define when the temporary access will expire. This creates a time window when the user can access the website. If no selection is made the default value of 24 hours is applied. The temporary policy is automatically deleted once it expires, unless the policy is edited.

To delete alerts, select the alerts you want to remove and click .

4 Configuring

The following topics contain information on how to configure your GFI WebMonitor deployment to your needs and requirements:

4.1 Configuring Core Settings

The Core Settings ensure that your GFI WebMonitor installation is properly configured to start monitoring Internet traffic on your network. After installation is complete, the Configuration Wizard helps you configure the following settings to start achieving results immediately:

Options	Description
Configure connection settings	<p>Choose your Network Mode depending on your current network setup. Establish a connection between your internal network and the Internet through the GFI WebMonitor server.</p> <p>NOTE This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.</p>
Enable Transparent Proxy	<p>Enable Transparent Proxy to monitor and control HTTP and HTTPS traffic transparently. When a user makes a request to a web server, the Transparent Proxy intercepts the request to deliver the requested content. When GFI WebMonitor is deployed in this mode, you do not need to set client browser settings to point to a specific proxy.</p> <p>NOTE Transparent Proxy can only work in Gateway Mode. It does not work not work in Simple Proxy mode or when GFI WebMonitor is installed as a plug-in for TMG.</p>
Enter your License key	<p>Key in a valid license to use GFI WebMonitor. This can either be a trial license or a regular license key obtained on renewal.</p>
Configure HTTPS Scanning	<p>Configure HTTPS scanning to monitor and block encrypted traffic.</p> <p>NOTE Ensure that by enabling HTTPS Scanning you are not violating any laws in your jurisdiction or any compliance regulations for your industry.</p> <p>NOTE This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.</p>
Set up the Database	<p>Configure the database to use with GFI WebMonitor where collected data is stored. Use the Firebird database only during the evaluation period. It is highly recommended to switch to a Microsoft SQL Server based database for live systems.</p>
Define Admin Credentials	<p>Key in the admin credentials required by the GFI WebMonitor services to control internal security engines, manage updates, send notifications and control data displayed in the User Interface. The GFI WebMonitor services are Windows services installed automatically during installation and require administrative privileges to operate.</p>
Setup Email notification settings	<p>Provide the email addresses required by GFI WebMonitor to send messages containing information related to tasks such as auto-updates and licensing issues.</p>
Configuring Internet Browsers to use a Proxy Server	<p>If you have not configured WPAD or Transparent Proxy, ensure that proxy settings of client machines are configured to use GFI WebMonitor as the default proxy. This ensures that Internet traffic is routed through GFI WebMonitor.</p> <p>NOTE This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.</p>

NOTE

The Configuration Wizard is launched automatically after installing GFI WebMonitor or manually from the **Settings** menu.

4.1.1 Connection Settings

Select how GFI WebMonitor is configured within your network and configure the connection between your internal network and the Internet through the GFI WebMonitor server.

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

To configure connection settings:

1. Go to **Settings > Core Settings > Connection Settings**.
2. In the **Network Mode** area, select one of the following options:

Mode	Description
Simple Proxy mode	Routes client HTTP traffic through GFI WebMonitor and non-HTTP traffic through a separate router. This setup requires an Internet facing router with port blocking and traffic forwarding capabilities.
Gateway mode	Choose this mode if installing GFI WebMonitor on a server that is configured as an Internet gateway. All outbound and inbound client traffic (HTTP and non-HTTP) is routed through GFI WebMonitor. When GFI WebMonitor is deployed in this mode, you can enable Transparent Proxy, eliminating the need to set client browser settings to point to a specific proxy. For more information, refer to Configuring Transparent Proxy (page 93).
In parallel with Microsoft Forefront TMG	When installing GFI WebMonitor it can be configured to operate in parallel to Microsoft Forefront TMG. Use this setup to keep Microsoft Forefront TMG as a firewall and use the same machine to perform web filtering by GFI WebMonitor. This setup also provides an alternative when it is not possible to add another dedicated machine in the network just for GFI WebMonitor.
As Plug-in for Microsoft Forefront TMG	GFI WebMonitor 10 SR1 and later editions can be installed as a plug-in for Microsoft Forefront TMG. Use this setup when you want to keep the Microsoft Forefront TMG Server as the primary proxy server and use only the filtering capabilities of GFI WebMonitor. GFI WebMonitor features are not available when installing in this mode.

If you selected **Simple Proxy mode**, configure the following settings:

Option	Description
Listen on all network interfaces	Configure GFI WebMonitor to listen for incoming HTTP and HTTPS requests on all available network interface cards.
Proxy Server	In the Proxy Server field, enter the IP address of the computer where GFI WebMonitor is installed.
Port	In the Port field, enter the port number used by GFI WebMonitor to listen to traffic (Default is 8080).
Use WPAD	[Optional] Enable Use WPAD if you want to use Web Proxy Auto-Discovery to enable client computers to automatically detect the GFI WebMonitor server.
Repeat WPAD detection	Click to enable GFI WebMonitor to search for available WPAD servers on your network.

Option	Description
Proxy Authentication	Configure the authentication method used when client machines are validated when accessing the Internet.
Chained Proxy	Connecting several proxy servers together to obtain greater anonymity. These servers act together as one proxy server to process web requests.

If you selected **Gateway mode**, configure the following settings:

Option	Description
Internal Network card	Select a network card from the available drop-down list. GFI WebMonitor listens for incoming HTTP and HTTPS requests on the selected network card.
IP Address	If the chosen network adapter has multiple IP addresses, select the IP address you want to use from the list.
Use WPAD	[Optional] Enable Use WPAD if you want to use Web Proxy Auto-Discovery to enable client computers to automatically detect the GFI WebMonitor server.
Repeat WPAD detection	Click to enable GFI WebMonitor to search for available WPAD servers on your network.
Proxy Authentication	Configure the authentication method used when client machines are validated when accessing the Internet.
Chained Proxy	Connecting several proxy servers together to obtain greater anonymity. These servers act together as one proxy server to process web requests.

3. Click **Next**.

4.1.2 Network Interface Configuration

GFI WebMonitor must be configured to listen for incoming HTTP and HTTPS requests originating from client computers on the internal network. You can configure GFI WebMonitor to listen on a specific network card or to listen on all network cards installed on the server.

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

Screenshot 41: Network settings

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

1. Go to **Settings > Core Settings > Connection Settings**.

2. Select from the following options:

Option	Description
Proxy Server	Key in the IP Address of the internal facing network card that will listen to traffic from client computers.
Port	Specify the port number on which the internal facing network card will listen to requests.
Listen on all network interfaces	If you want GFI WebMonitor to listen for incoming requests on all available network cards, click Show Advanced Options . Click the switch to enable.

3. Click **Save**.

4.1.3 Configuring WPAD

The Web Proxy Auto Discovery (WPAD) is an Internet protocol supported by major Internet browsers. It enables web browsers to automatically retrieve proxy settings from a WPAD data file stored on a machine on your network.

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

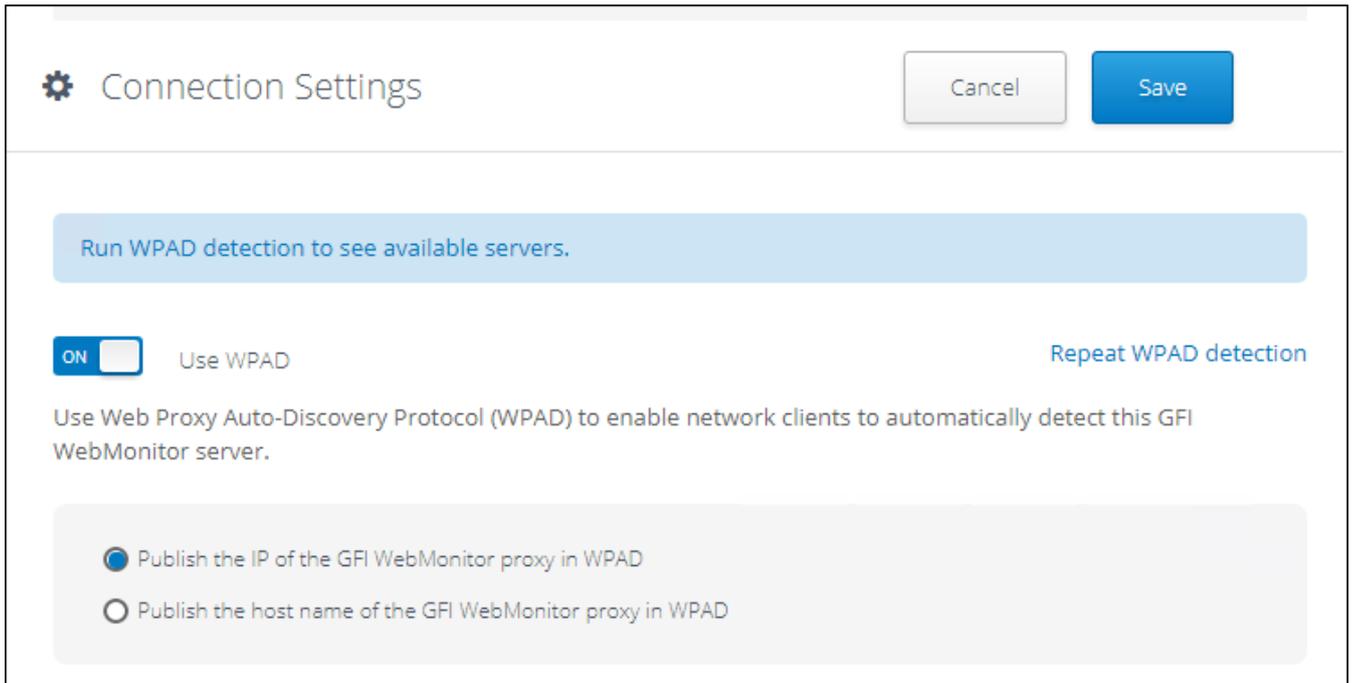
WPAD is a convenient way for administrators to configure client machines to use the GFI WebMonitor machine as a proxy server without having to supply settings manually or via Active Directory Group Policies. When this feature is enabled and the Internet browser connection settings are configured to 'Automatically Detect Settings', each client machine will automatically determine the IP address of the GFI WebMonitor server and use it as a proxy without further configuration.

WPAD is particularly 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.

NOTE

For client Internet browsers to use WPAD, these must be configured to automatically detect proxy settings. For more information, refer to [Configure Internet browser for WPAD](#) (page 88).

When GFI WebMonitor is installed the first time, it tries to detect available WPAD servers. Discovered WPAD servers are listed in an information window.



Screenshot 42: WPAD settings

To enable WPAD:

1. Go to **Core Settings > Connection Settings**.
2. Locate **Use WPAD** switch. Click **ON** to enable.

NOTE

If GFI WebMonitor does not discover any WPAD Servers on your network, this option is disabled. Click **Repeat WPAD detection** to check for available servers.

3. A warning is displayed informing you that by enabling WPAD, server information is updated that might create network conflicts. These conflicts may arise when you have multiple GFI WebMonitor installations within the same network. Click **Proceed** to continue.

4. Select one of the following options:

Option	Description
Publish the IP of the GFI WebMonitor proxy in WPAD	Select to include the GFI WebMonitor IP address in the WPAD.dat file. Recommended when the proxy machine has a fixed IP address.
Publish the host name of the GFI WebMonitor proxy in WPAD	Select to include the GFI WebMonitor host name in the WPAD.dat file. Recommended when the proxy machine has a dynamic IP address.

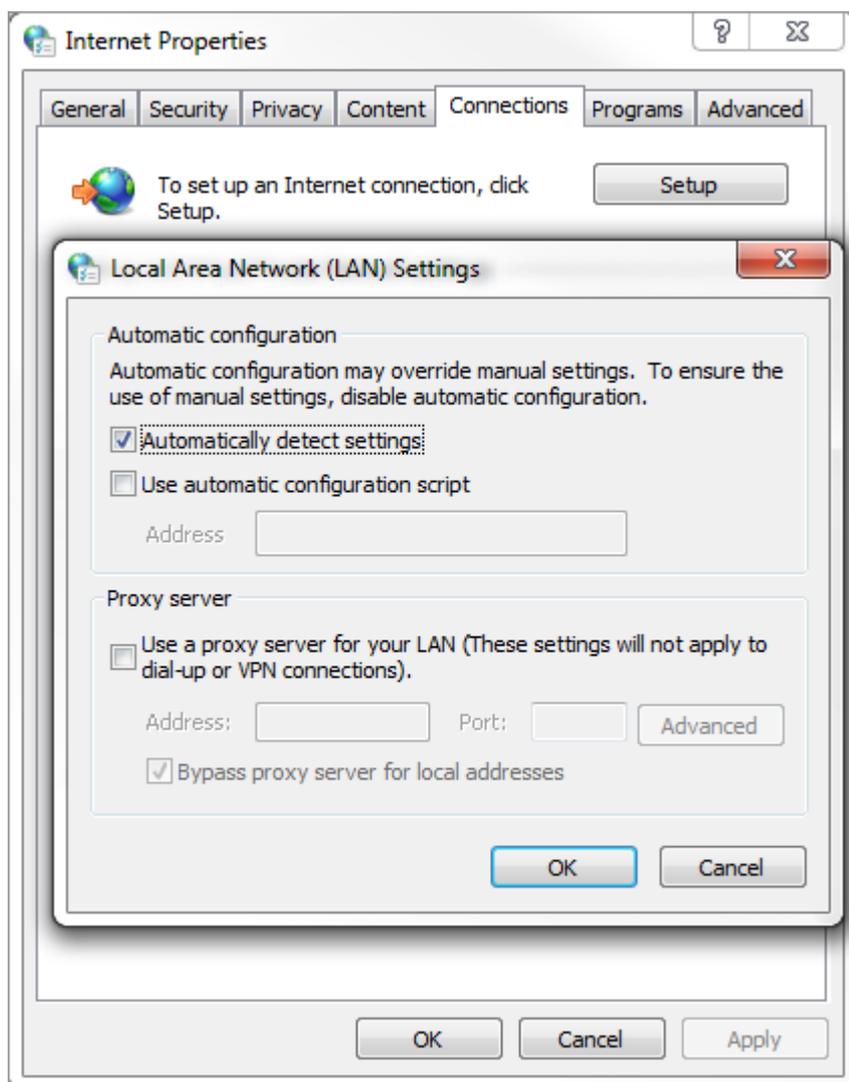
5. Click **Save**.

4.1.4 Configure Internet browser for WPAD

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

1. On the client machine, go to **Control Panel** and select **Internet Options**.
2. Click the **Connections** tab.

3. Click **LAN settings**.
4. Check **Automatically detect settings** checkbox.



Screenshot 43: Configuring Automatically detect settings

5. Close **LAN Settings** dialog.
6. Click **OK** to close **Internet Options** dialog.
7. Restart Internet browser to refresh settings.

These settings can be enforced via GPO. For more information, refer to [Configuring GFI WebMonitor machine as the Default Proxy using GPO](#) (page 142).

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

NOTE

WPAD is supported by all major Internet browsers.

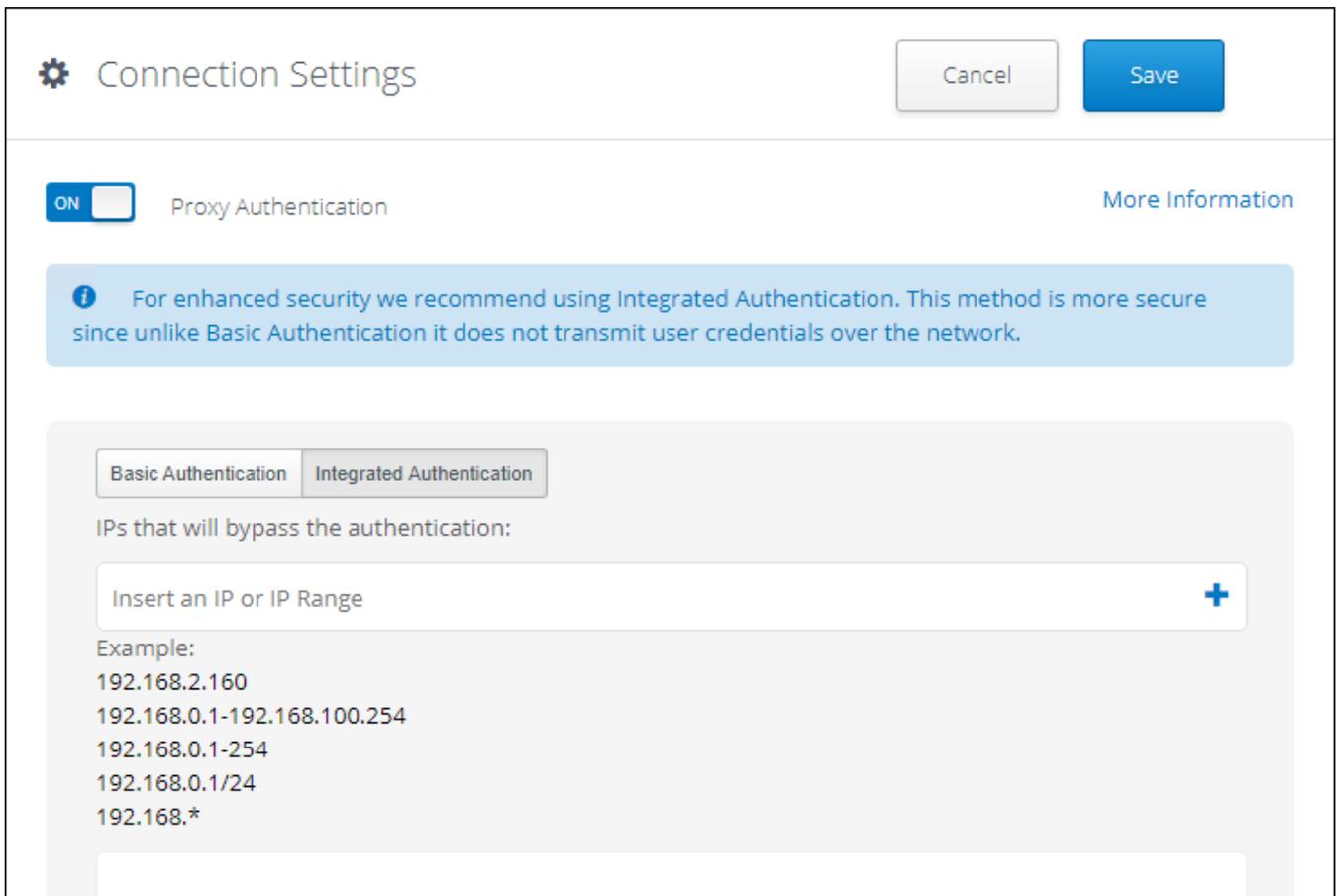
4.1.5 Configuring Proxy Authentication Method

Proxy Authentication 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 policies for users or groups. By default, Proxy Authentication is disabled. When Proxy Authentication is disabled, you are only allowed to configure new policies using IP addresses.

For enhanced security we recommend using Integrated Authentication. This method is more secure since unlike Basic Authentication it does not transmit user credentials over the network.

NOTE

The Configuration Wizard is launched automatically after installing GFI WebMonitor or manually from the **Settings** menu.



The screenshot shows the 'Connection Settings' dialog box. At the top, there is a gear icon, the title 'Connection Settings', and 'Cancel' and 'Save' buttons. Below the title, there is a toggle switch for 'Proxy Authentication' which is currently turned 'ON'. To the right of the toggle is a 'More Information' link. A blue information box contains the text: 'For enhanced security we recommend using Integrated Authentication. This method is more secure since unlike Basic Authentication it does not transmit user credentials over the network.' Below this, there are two tabs: 'Basic Authentication' and 'Integrated Authentication'. Under the 'Integrated Authentication' tab, the text reads 'IPs that will bypass the authentication:' followed by a text input field with the placeholder 'Insert an IP or IP Range' and a plus sign button. Below the input field, there is an 'Example:' section listing several IP addresses and ranges: 192.168.2.160, 192.168.0.1-192.168.100.254, 192.168.0.1-254, 192.168.0.1/24, and 192.168.*.

Screenshot 44: Proxy authentication settings

To configure user authentication method:

1. Go to **Core Settings > Connection Settings**.
2. Click the **Proxy Authentication** switch to enable.
3. In the **Proxy Authentication** area, select one of the following options:

Option 1: Leave Proxy Authentication off if the user is not required to provide login credentials when new Internet sessions are launched.

Option 2: 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. When using Basic authentication, the browser prompts the user for a user name and password. This information is transmitted across HTTP as plain text and considered insecure.
Integrated authentication	(Recommended) This option enables GFI WebMonitor proxy to authenticate users by using the client machine access control service. User is not prompted to provide login credentials when new Internet sessions are launched. We recommend using Integrated authentication in a Windows domain environment since this method of authentication does not transmit user passwords across the network.

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.

4. [Optional] In the **IP's that will bypass the authentication** field, key in IP addresses to exclude from proxy authentication. IP addresses specified in this field will not be prompted to provide login credentials when new Internet sessions are launched.

5. Click **Save**.

4.1.6 Authentication Test (in Real-Time)

Try browsing to <http://www.youtube.com> and open a video of considerable length (more than 10 minutes should be enough). If you have chosen **Basic Authentication** you are prompted for a username and password. Enter the credentials you used to log onto the machine you are using, then you should be able to proceed.

If you go to **Dashboards > Real-Time Traffic** you should see the connection to <http://www.youtube.com> listed. Other details include the IP of the test machine and your user name, status of traffic and size of download.

Real-Time Bandwidth Chart

If you now switch from **Active Connections** to **Bandwidth** you will see a real time graph of bandwidth being used at that point in time. The more connections you open, the higher the graph will climb.

4.1.7 Blocking Test by Username

With GFI WebMonitor configured to use **Basic Authentication**, repeat the blocking test previously carried out, but this time use the logged on user credentials. The outcome of this test will confirm that policies are being applied by username.

1. Go to **Manage > Policies** and create a new Policy.
2. In **Policy Name** field, enter **Authentication Test**.
3. In **Policy Description**, enter a description.
3. Change the **Allow, Block, Warn, Monitor** element to **Block**
4. From the left sidebar, add the **Websites** element.
5. Locate and insert the **Computer and Internet Info** category to block social networking websites (for blocking test purposes).
6. Insert the **Users, Groups, IPs** and insert the username currently logged on the machine.
7. Click **Save** to apply the changes.

8. Go back to your browser and open `www.example.com`. The GFI WebMonitor blocking page should now be displayed. Note that this time the label **Breached Policy** has changed to **'Authentication Test'**.

If the warning is displayed, then GFI WebMonitor is working correctly!

If the block did not work, make sure you have entered all details correctly, and that you have saved changes to the policy. Try closing and re-opening the browser, and check the **Real-Time Traffic** dashboard in the GFI WebMonitor interface to ensure that traffic is being routed through the proxy correctly. If you see the request with the IP, this means that you have not forced authentication correctly and you should use IPs for your policies. If you see a different username, you need to enter this username in the policy.

If you don't manage to get this part working you should [contact our support team](#) so that we can help you to troubleshoot your installation.

4.1.8 Configuring Chained Proxy

Proxy Chaining is a method of connecting several proxy servers together to obtain greater anonymity or safer connection. 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 another proxy server.

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

The screenshot shows the 'Chained Proxy' configuration interface. At the top, there is a toggle switch labeled 'ON' and 'Chained Proxy'. Below this is a descriptive text: 'Connect several proxy servers together and route traffic to them. Chained proxy servers act as a single proxy server to provide better anonymity.' The configuration area contains several input fields: 'PROXY SERVER' with the value '192.168.10.10', 'PORT' with the value '8080', 'Current Credentials' with the value 'Administrator', and 'Alternative Credentials' which is masked with dots. A 'Test Proxy Chaining' button is located at the bottom left of the configuration area.

Screenshot 45: Chained proxy configuration settings

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

1. Go to **Settings > Core Settings > Connection Settings**.
2. Click the **Chained Proxy** switch to turn on and enable GFI WebMonitor to route traffic to another proxy server.
3. In the Proxy Server field, key in the IP address
4. In the Port field, key in the port number (default 8080).

5. [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.

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

4.1.9 Configuring Transparent Proxy

When configured as a Transparent Proxy, GFI WebMonitor acts as an intermediary between client machines and web servers to monitor and control HTTP and HTTPS traffic transparently. When a user makes a request to a web server, the Transparent Proxy intercepts the request to deliver the requested content. When GFI WebMonitor is deployed in this mode, you do not need to set client browser settings to point to a specific proxy.

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

NOTE

Transparent Proxy can filter only HTTP (TCP port 80) and HTTPS (TCP port 443) traffic.

Environment considerations when GFI WebMonitor is configured as a Transparent Proxy

Type	Description
Supported Operating Systems	Transparent Proxy can be enabled on servers running the following operating systems: <ul style="list-style-type: none">» Windows® Server 2016» Windows® Server 2012 (Including R2)» Windows® Server 2008 R2» Windows® 10» Windows® 8.1» Windows® 7 <p>NOTE Ensure the operating system is up-to-date with all Windows updates installed.</p>
Ports	By default, Transparent Proxy uses port 8082. Ensure that the listening port does not conflict with other applications. When the port is changed the proxy is restarted and ongoing connections are terminated. Applications do not need to be configured to connect to the Transparent Proxy port. The port is needed for internal operations by GFI WebMonitor.
Gateway Mode	Ensure that GFI WebMonitor is running in Gateway mode. Transparent Proxy cannot work in Simple Proxy mode. For more information, refer to Deployment in an Internet Gateway environment (page 17).
Microsoft TMG fire-wall and Transparent Proxy	Transparent proxy is not compatible with Microsoft Forefront TMG.
Proxy Chaining	Transparent proxy cannot be enabled if Proxy Chaining is already used, because of possible conflicts. For more information, refer to Configuring Chained Proxy (page 92).

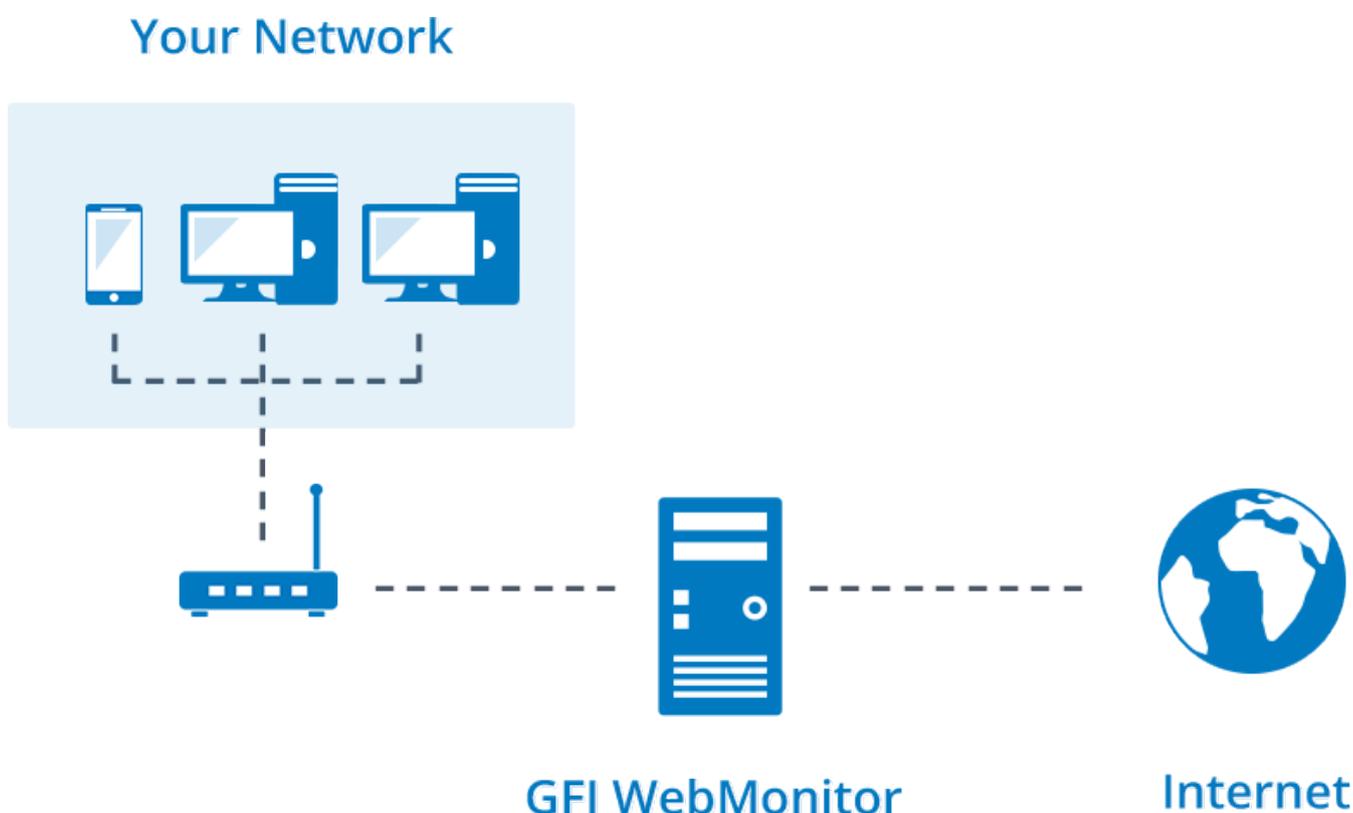
Type	Description
Network address translation (NAT)	Ensure Network address translation (NAT) is disabled on the GFI WebMonitor server for Transparent Proxy to work. Network address translation (NAT) modifies network address information in HTTP and HTTPS traffic.

NOTE

Certain restrictions may apply on Transparent Proxy usage depending on the network topology. Configuration changes might be needed on the network to enable transparent mode.

How it works

Transparent Proxy can work in parallel with the regular proxy. HTTP and HTTPS traffic originating from client machines that are not set to explicitly point to GFI WebMonitor (manually or through WPAD) is captured by the Transparent Proxy once this functionality is enabled.



Screenshot 46: How Transparent Proxy works

When a user makes a request, the GFI WebMonitor Transparent Proxy intercepts the request even if the client machine has no configured proxy. If the requested content is allowed by GFI WebMonitor, the Transparent Proxy delivers it to the destination.

Enabling Transparent Proxy

4.1.10 Enabling Transparent Proxy

When configured as a Transparent Proxy, GFI WebMonitor acts as an intermediary between client machines and web servers to monitor and control HTTP and HTTPS traffic transparently. For more information, refer to [Configuring Transparent Proxy](#) (page 93).

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

Transparent Proxy Settings

Enable Transparent Proxy

The diagram illustrates the network architecture for transparent proxy. It shows a group of devices (labeled 'Your Network') connected to a wireless router. This router is connected to a server labeled 'GFI WebMonitor' which has 'WPAD' and 'FIREBIRD' components. The WebMonitor is connected to a 'Router' (represented by a four-way arrow icon), which is then connected to the 'Internet' (represented by a globe icon).

GFI WebMonitor can process traffic transparently when in Gateway mode. Please ensure that your internet router can properly route incoming packets to the WebMonitor machine.

8082 PORT

Use general proxy authentication settings

Screenshot 47: Transparent Proxy Settings

To enable Transparent Proxy:

1. Go to **Core Settings > Transparent settings**.
2. Click the **Enable Transparent Proxy** switch to enable.
3. Configure the following options:

Option	Description
Port	Specify the port number on which the internal facing network card will listen to requests. The default port is 8082. IMPORTANT Ensure the listening port does not conflict with other applications. When the port is changed, the proxy is restarted and ongoing connections are terminated.
Save and Test Transparent Proxy	Use the Save and Test Transparent Proxy button to check if the Transparent Proxy is operational. NOTE The test checks if the Transparent Proxy driver and modules are working well and if traffic generated from the GFI WebMonitor server machine is filtered properly. It cannot guarantee that traffic coming from the internal network gets processed properly.
Use general proxy authentication settings	By default, Transparent Proxy inherits the authentication settings from the regular proxy set from Connection Settings > Proxy Authentication . For more information, refer to Configuring Proxy Authentication Method (page 90). To override the regular authentication settings, uncheck this option and then set new authentication settings in the Proxy Authentication area.
Proxy Authentication	<ul style="list-style-type: none"> » Basic authentication - Select if a user is required to provide login credentials when new Internet sessions are launched. When using Basic authentication, the browser prompts the user for a user name and password. This information is transmitted across HTTP as plain text and considered insecure. » Integrated authentication - (Recommended) This option enables GFI WebMonitor proxy to authenticate users by using the client machine access control service. User is not prompted to provide login credentials when new Internet sessions are launched. We recommend using Integrated authentication in a Windows domain environment since this method of authentication does not transmit user passwords across the network. 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.
IPs that will bypass the authentication	Key in the IP addresses of machines to be excluded from authentication. Traffic from excluded IPs will not be authenticated by GFI WebMonitor. The dashboards will display only IP addresses and not user names.

4. Click **Save**.

4.1.11 Testing Transparent Proxy

The GFI WebMonitor user interface provides a test button in the Transparent Proxy settings screen. Use this feature to check if the Transparent Proxy is operational. This test checks only if the Transparent Proxy driver and modules are working well and traffic generated from the GFI WebMonitor server machine is filtered properly. It cannot guarantee that traffic coming from the internal network gets processed properly.

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

To test if traffic generated from the internal network is properly filtered by the Transparent Proxy, perform the following steps:

1. Ensure the client browser is not configured to use any proxy. Also uncheck options of automatic proxy detections within browser to avoid regular proxy usage through WPAD. For more information, refer to [Configuring WPAD](#) (page

87).

2. From the client browser try to access the following URL: `whatismyproxy.com`. GFI WebMonitor policies might block the URL and in that case the GFI WebMonitor blocking page will appear. Otherwise, the opening web site should detect that the browser is passing through the GFI Proxy. Both behaviors prove that traffic flows through GFI WebMonitor (via transparent mode).

3. Additionally, if you have set up logging within the GFI WebMonitor policies, you can also check the Dashboards and locate requests made by the client machine. If requests were captured and logged by the product, Transparent Proxy is configured correctly. For more information, refer to [Logging](#) (page 52).

4.1.12 HTTPS Proxy Scanning settings

HTTPS Scanning gives GFI WebMonitor visibility into secure Internet sessions (URLs starting with `https://`). This feature enables you to apply policies to this type of traffic and to scan the content for threats that may be present in these sites and on downloaded files.

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

With HTTPS Proxy Scanning enabled, GFI WebMonitor can monitor and block traffic within an encrypted stream. This includes blocking and Anti-Virus scanning of downloads within that stream. HTTPS inspection decrypts the data in the connection coming from the client, then processes the traffic, and encrypts the traffic going to the target web server.



Screenshot 48: HTTPS traffic flow

The actual data that is passed between source and destination is not shown because GFI WebMonitor cannot read the encrypted contents. Only the destination web server is shown. Therefore, an administrator cannot see details of the data sent, such as account information, usernames and passwords.

NOTE

Ensure that by enabling HTTPS Scanning you are not violating any laws in your jurisdiction or any compliance regulations for your industry.

When HTTPS inspection is enabled, two secure connections are started 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

When HTTPS Scanning is not enabled, GFI WebMonitor allows users to browse HTTPS websites without decrypting and inspecting their contents.

GFI WebMonitor needs a valid certificate for these two secure connections to be established. The Internet browser must verify that the certificate is signed by a trusted Certification Authority (CA). This means that 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](#)
- » [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](#).

4.1.13 Configuring HTTPS Proxy settings

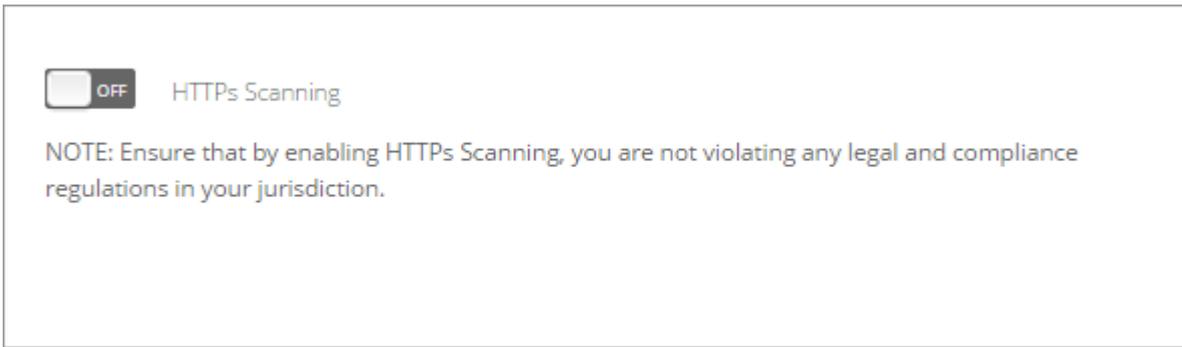
Enable HTTPS Scanning to monitor and block traffic within encrypted streams (URLs starting with https://). This prevents threats from malicious content that may be present in HTTPS sites or downloads. GFI WebMonitor does not read or display any encrypted contents.

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

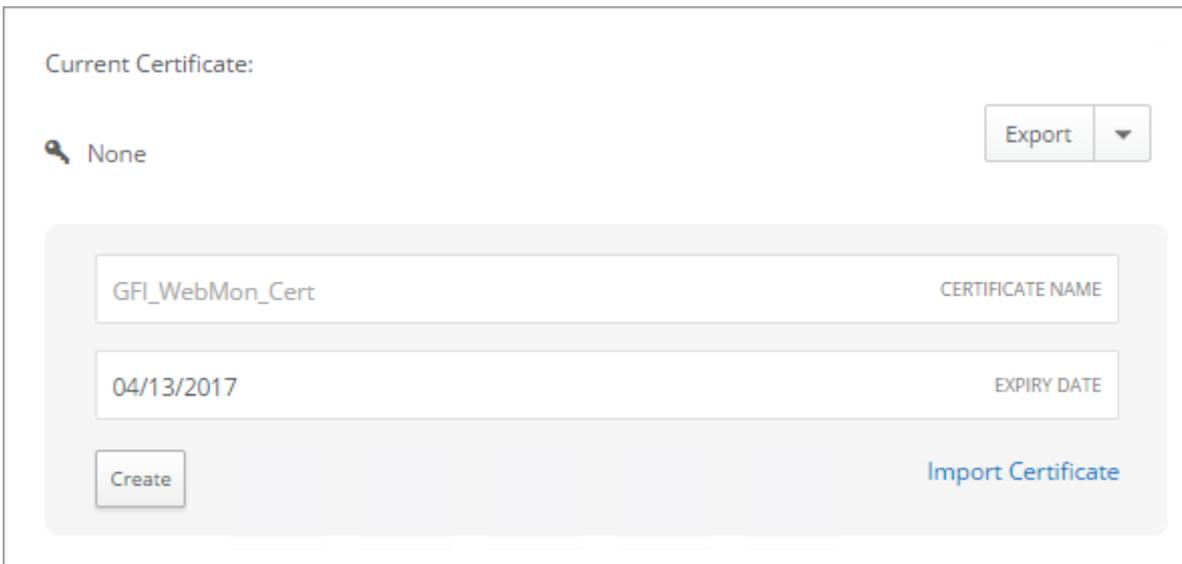
To configure HTTPS Scanning settings:

1. Go to **Settings > Core Settings > HTTPS Scanning**.



Screenshot 49: Enable HTTPS Scanning

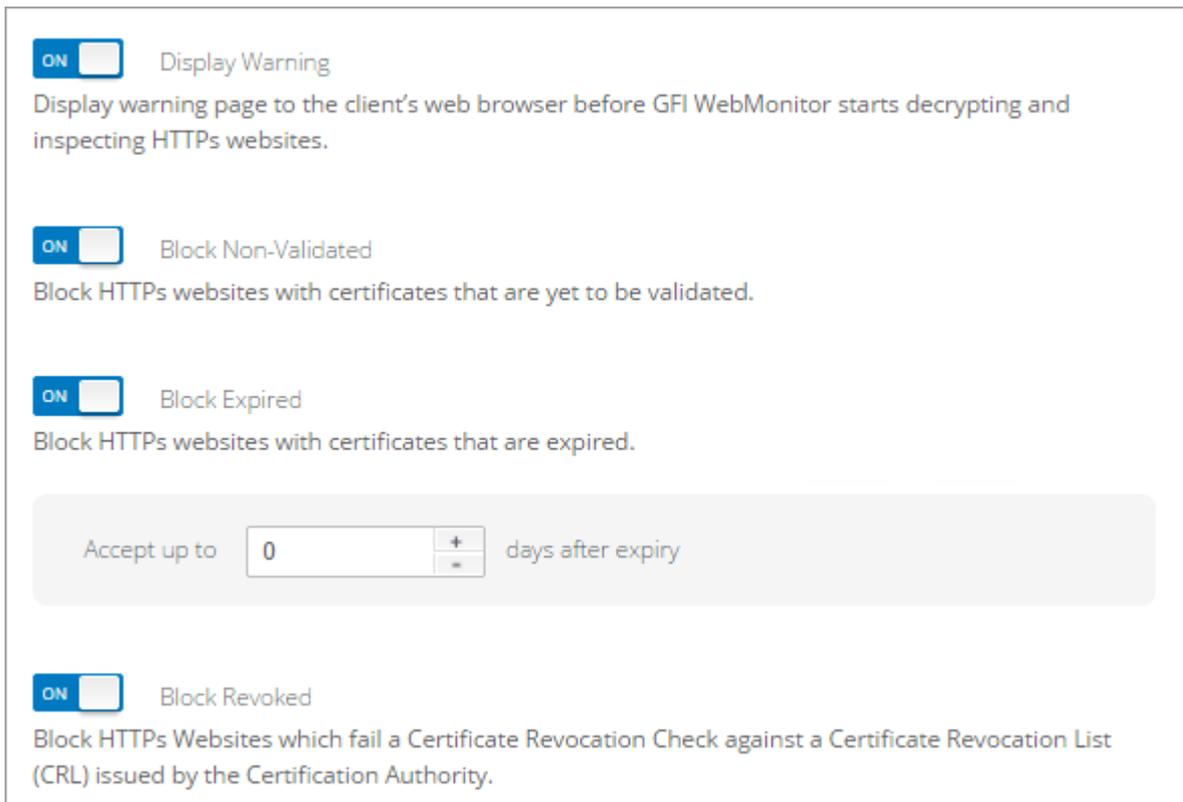
2. Click the **HTTPS Scanning** switch to turn on.



Screenshot 50: Information related to active certificate

3. In the **Current Certificate** area, view relevant information of the currently used certificate. GFI WebMonitor needs a valid certificate to inspect HTTPS traffic. If no certificate is currently enabled, consult the following sections that show you how to work with certificates:

- » [Creating a new HTTPS Scanning certificate](#)
- » [Import an existing HTTPS Scanning certificate](#)
- » [Export an HTTPS Scanning certificate](#)



Screenshot 51: Configure advanced HTTPS options

4. Click the **Display Warning** switch to display a warning page to users before GFI WebMonitor starts decrypting and inspecting HTTPS traffic.
5. Click the **Block Non-Validated** switch to start blocking HTTPS websites with certificates that are not yet validated.
6. Click the **Block Expired** switch to block pages that contain expired certificates.
7. Use the **Accept up to 'x' days after expiry** field to accept websites whose certificate has expired by a number of days.
8. Click the **Block Revoked** switch to block websites with revoked certificates.

NOTE

Ensure that by enabling HTTPS Scanning you are not violating any laws in your jurisdiction or any compliance regulations for your industry.

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](#).

4.1.14 Creating a new HTTPS Scanning certificate

After decrypting HTTPS websites, GFI WebMonitor can re-encrypt these websites for secure transmission to the client browser. To perform these actions, GFI WebMonitor requires a valid certificate signed by a trusted Certification Authority (CA). You can [import an existing certificate](#) or create a new certificate in GFI WebMonitor by performing the following steps:

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 > Core Settings > HTTPS Scanning**.

Current Certificate:

GFI_Certificate_WebMonitor (Expires : 26/09/2018 01:00:00) Export

New_Certificate CERTIFICATE NAME

09/26/2018 EXPIRY DATE

Create Import Certificate

Screenshot 52: Settings for a new certificate

2. In the Current Certificate area, click **Create Certificate**.
3. In the **Certificate Name** field, type a name for the certificate.
4. Set the expiration date and click **Create**.

4.1.15 Importing an HTTPS Scanning certificate

To import an existing HTTPS Scanning certificate:

1. Go to **Settings > Core Settings > HTTPS Scanning**.
2. In the Current Certificate area, click **Import Certificate**.
3. Click **Browse** and locate the certificate you want to import.
4. Click **Import**.
5. If the certificate you are importing is password protected, key in the required password.

4.1.16 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.

To export an existing certificate:

1. Go to **Settings > Core Settings > HTTPS Scanning**.



Screenshot 53: Export certificate options

2. In the Current Certificate area, click **Export as .cer** or **Export as .pfx** as required.

By default the exported certificates are saved on the download folder.

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 client computers, refer to: http://go.gfi.com/?pageid=WebMon_HTTPSInspectionCertificate

4.1.17 Deploy the HTTPS Inspection certificate via GPO

For your client machines to access HTTPS sites, a trusted HTTPS Inspection certificate needs to be deployed on client computers.

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

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 Domain 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 which 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 > Policies > 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.

4.1.18 Deploy the HTTPS Inspection certificate manually

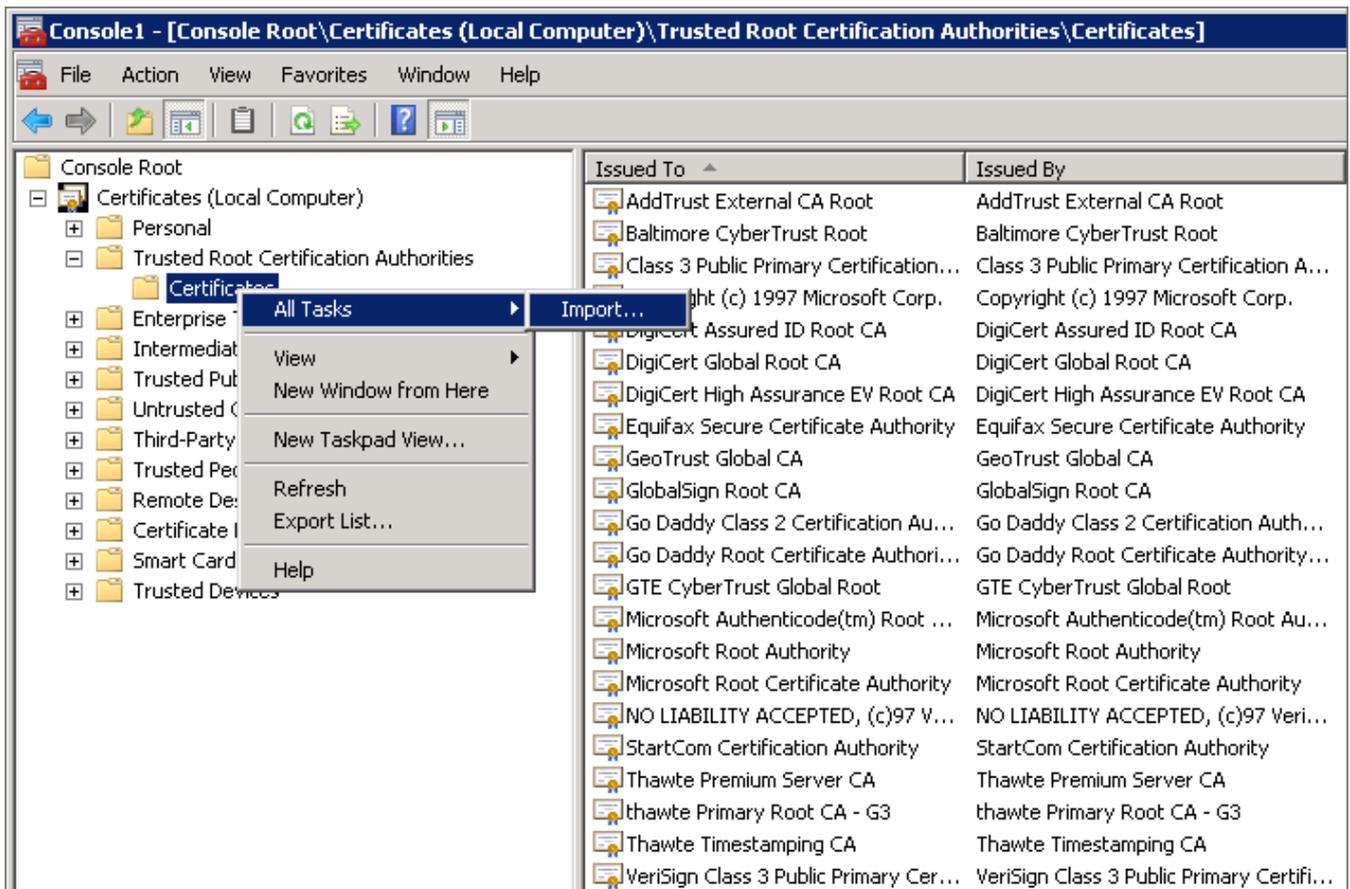
For your client machines to access HTTPS sites, a trusted HTTPS Inspection certificate needs to be deployed on client computers.

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.

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**.



Screenshot 54: Certificate management console

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 (such as 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**

4.1.19 Adding Items to the HTTPS Scanning Exclusion List

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.

IMPORTANT

Backup ProxyConfig.xml before making any changes.

Excluding Domains

1. Open ..\WebMonitor\Data\ProxyConfig.xml
2. Remove <DomainsExcludedFromHTTPSInspection /> tag
3. Add the sites exclude between a DomainsExcludedFromHTTPSInspection tag. For example:

```
<DomainsExcludedFromHTTPSInspection>  
<string>www.domain.com</string>  
<string>*.domain.com</string>  
</DomainsExcludedFromHTTPSInspection >
```
4. Save file.

Excluding Users

1. Open ..\WebMonitor\Data\ProxyConfig.xml
2. Remove the <UsersExcludedFromHTTPSInspection /> tag
3. Add the users to be excluded between a UsersExcludedFromHTTPSInspection tag, for example:

```
<UsersExcludedFromHTTPSInspection>  
<string>mydomain\user1</string>  
<string>mydomain\user2</string>  
</UsersExcludedFromHTTPSInspection>
```
4. Save file.

Excluding Client IPs

1. Open ..\WebMonitor\Data\ProxyConfig.xml
2. Remove the <UserIPsExcludedFromHTTPSInspection /> tag
3. Add the client IP addresses to be excluded between a UsersExcludedFromHTTPSInspection tag, for example:

```
<UserIPsExcludedFromHTTPSInspection>  
<string>10.0.0.11</string>  
<string>10.0.0.23</string>  
</UserIPsExcludedFromHTTPSInspection>
```
4. Save file.

NOTE

Changes are applied as soon as the file is saved.

4.1.20 Configuring Databases

GFI WebMonitor supports two types of databases that can be configured to store collected monitoring data. This data is used to populate the dashboards and for reporting purposes by GFI WebMonitor. The supported databases are:

Database	Description
Firebird Database	Firebird is the default database, embedded automatically with the installation. We highly recommend using this database for evaluation purposes only.
Microsoft SQL Database	GFI WebMonitor supports both Microsoft SQL Express and Microsoft SQL Server databases.

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

NOTE

The Configuration Wizard is launched automatically after installing GFI WebMonitor or manually from the **Settings** menu.

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

- » [Configuring the embedded Firebird Database](#)
- » [Configuring Microsoft SQL Database](#)
- » [Create a new Microsoft SQL Database](#)

Configuring the Embedded Database

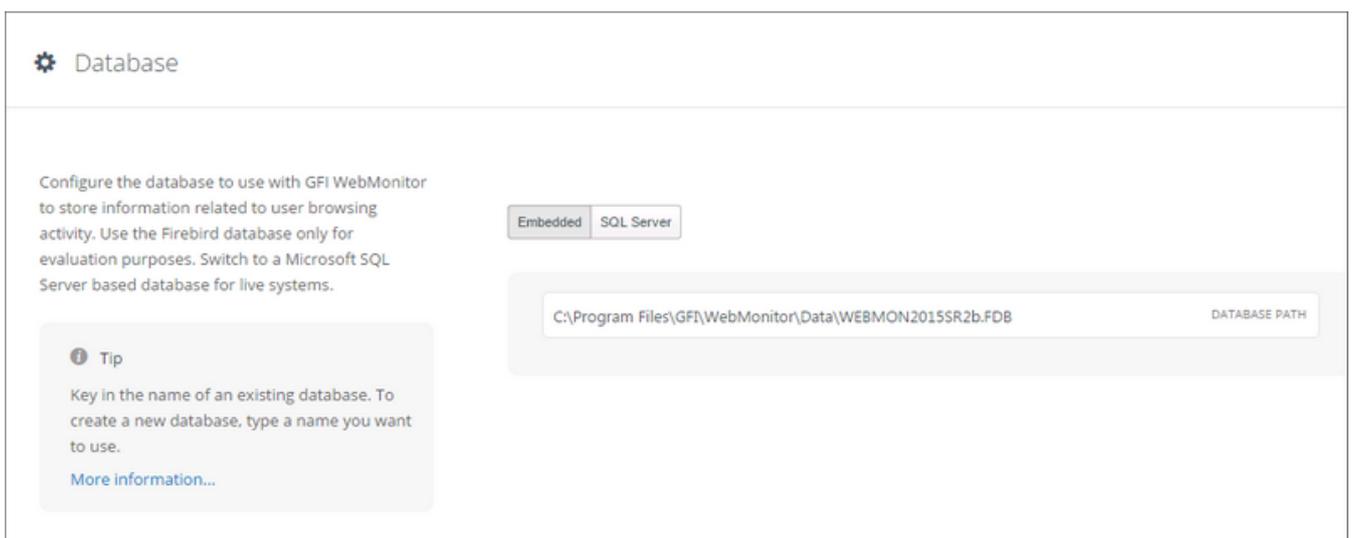
During installation, GFI WebMonitor automatically installs a Firebird database that is used by the application as the default database. The default path is: `C:\Program Files\GFI\WebMonitor\Data\WEBMON.FDB`.

IMPORTANT

It is highly recommended to use this database for evaluation purposes only.

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 > Core Settings > Database**.



Screenshot 55: Firebird database settings

- From **Database Type**, select **Embedded**.
- In the **Database Path** field, change the path to point to the new location.

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:

- In GFI WebMonitor, go to **Settings > Core Settings > Database**.

Screenshot 56: SQL database settings

- From **Database Type**, select **SQL Server**.
- In the **SQL Server** field, type the SQL Server instance name.
- 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 .

- In the **Database Name** 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.

NOTE

You can create a new database from within GFI WebMonitor. For more information, refer to [Creating a new Microsoft SQL Database](#) (page 108).

Creating a new Microsoft SQL Database

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

NOTE

There is no need to create a blank database in SQL first. Just add a unique name on the **Database Name** field and GFI WebMonitor creates a new database on the background.

To create a new database:

1. In GFI WebMonitor, go to **Settings > Core Settings > Database**.
2. From **Database Type**, select **SQL Server**.
3. In the **SQL Server** field, type the SQL Server instance name.
4. In the **Authentication** area, select one of the following:

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 Name** field, type the name of the database you want to create in SQL Server®.

4.1.21 Admin Credentials for GFI WebMonitor Services

When GFI WebMonitor is installed, the following Windows services are created:

- » GFI Proxy
- » GFI WebMonitor Core Service

An account with Administrative privileges is required by these Windows services to control internal security engines, manage updates, notifications and User Interface. These credentials are configured after installation using the Configuration Wizard.

IMPORTANT

We do not recommend updating the password as this change impacts GFI WebMonitor operations.

To manage the admin credentials from within the Configuration Wizard:

1. Go to **Settings > Configuration Wizard**.
2. Follow the wizard until you are presented with the Admin Credentials screen.
3. Use the provided fields to enter the server's Admin credentials. For example:

- Admin Username: [domain name]\Administrator
- Admin Password: [key in password]

4. Click **Validate** to have the entered credentials validated by GFI WebMonitor.

5. Click **Next** and wait for GFI WebMonitor to restart the services.

NOTE

The Configuration Wizard is launched automatically after installing GFI WebMonitor or manually from the **Settings** menu.

4.1.22 Updating Admin Credentials from services.msc

When GFI WebMonitor is installed, the following Windows services are created:

- » GFI Proxy
- » GFI WebMonitor Core Service

An account with Administrative privileges is required by the GFI WebMonitor Core Service to control internal security engines, manage updates, notifications and User Interface. These credentials are configured after installation using the Configuration Wizard. For more information, refer to [Using the Post-installation Configuration Wizard](#) (page 25).

NOTE

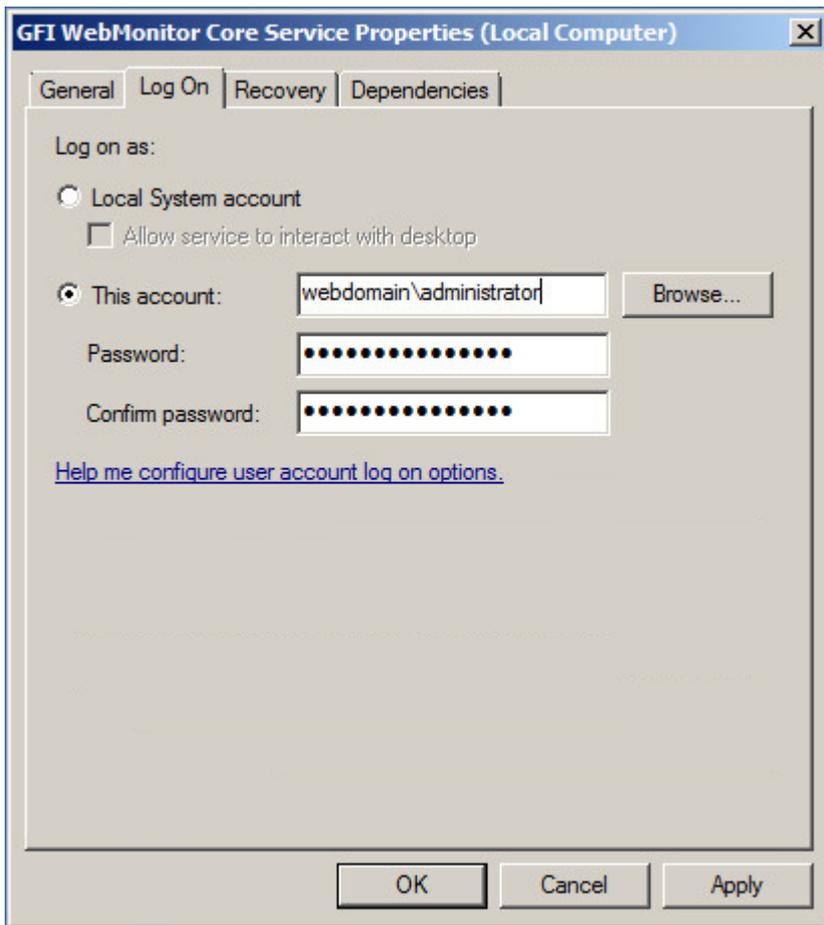
The GFI Proxy service should use the Local System Account.

If you need to update the Admin Credentials after your GFI WebMonitor installation has been set up:

IMPORTANT

We do not recommend updating the password as this change impacts GFI WebMonitor operations.

1. On the GFI WebMonitor server, go to **Start > Run** and key in `services.msc`
2. Locate the GFI WebMonitor Core Service, right-click and select **Properties**.
3. Go to the **Log On** tab and select **This account**.



Screenshot 57: Log On properties of the GFI WebMonitor Core service,

4. Update the account name and the password.

NOTE

The account must have local administrator rights, including **Log on as service** rights.

5. Restart the GFI WebMonitor Core Service.

4.1.23 Configuring Email distribution settings for notifications

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

These settings can be defined when running the Post-Install wizard after installing GFI WebMonitor or at any time from the **Settings** menu.

To manage distribution settings:

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

SMTP Server Details

Google mail (Gmail) ▼

WebMonitor@mydomain.com FROM EMAIL ADDRESS

smtp.gmail.com SMTP SERVER 587 SMTP PORT

ON Authentication

user@gmail.com USER NAME PASSWORD

Enable SSL

Screenshot 58: SMTP settings of e-mail address to receive notifications

2. Change any of the following options:

Option	Description
From Email	Specify the email address from which notifications are sent.
SMTP Server	Enter the name or IP of the SMTP server. For more information, refer to Configuring SMTP Settings for webmail accounts (page 111).
SMTP Port	Key in the port number of the SMTP server (Default 25).
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.
Enable Secure Sockets Layer (SSL)	If SSL is required to provide secure transmission between sender and recipients, check Enable Secure Sockets Layer (SSL) checkbox.
Email Recipients	Enter recipient email address and click the plus sign to add. You can key in as many recipients as required.
Verify Mail Settings	Click to send a test email and verify the mail server settings are configured correctly.

4.1.24 Configuring SMTP Settings for webmail accounts

You can set up webmail accounts as the delivery mechanism for notifications in GFI WebMonitor. The following is a list of popular webmail providers with SMTP settings:

Provider	SMTP server details
Gmail	Email address from which notifications are sent. Example, example@gmail.com SMTP Server: smtp.gmail.com SMTP Port: 587 Authentication: Yes User Name: Your email address Password: Gmail password Enable SSL: Yes
Yahoo!	Email address from which notifications are sent. Example, example@yahoo.com SMTP Server: smtp.mail.yahoo.com SMTP Port: 587 Authentication: Yes User Name: Your email address Password: Yahoo! ID password Enable SSL: Yes
Outlook	Email address from which notifications are sent. Example, example@outlook.com SMTP Server: smtp-mail.outlook.com SMTP Port: 587 Authentication: Yes User Name: Your email address Password: outlook.com password Enable SSL: Yes

4.2 Advanced Settings

After GFI WebMonitor is up and running, tweak your installation by configuring the following advanced options:

Option	Description
Licensing and subscription details	View information about the currently installed license. Renew or change your license.
Licensing Exclusion List	Set up a list of users that are always allowed access to the Internet without being monitored. Excluded users do not consume a license.
UI Access Control	Turn Windows Authentication on or off for users defined in the configured Authorization Rules. Add new Authorization Rules to grant limited access to users to different sections of GFI WebMonitor.
Configuring Activity Logging	Configure data retention settings to enable the recording of data related to user activity. Collected data is used by GFI WebMonitor for dashboards and reports. You can also enable/disable Anonymization; a feature that masks user names in compliance with some countries' data protection laws.
Configuring Anonymization	Anonymization enables masking private user data in accordance with European privacy and data protection laws.
Language settings	Change the language of warning messages sent to the user when GFI WebMonitor blocks user activity.
Configuring Security Engines	Configure various security technologies such as anti-virus and anti-phishing engines to protect your network.
WebGrade updates	Configure WebGrade updates to ensure that categorization and websites and applications monitored by GFI WebMonitor is always up to date.
System updates	Configure the frequency of GFI WebMonitor product updates.

Option	Description
Configuring search engine options	GFI WebMonitor can monitor user search queries to help identify potential risks, while also providing valuable insight into the mindset of your users.
Enable Caching	Caching transparently stores data so that future requests for that data are served faster. Caching helps bandwidth optimization. <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p>NOTE This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.</p> </div>
Configuring Proxy settings on client Internet browsers	When WPAD is not enabled, 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. <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p>NOTE This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.</p> </div>

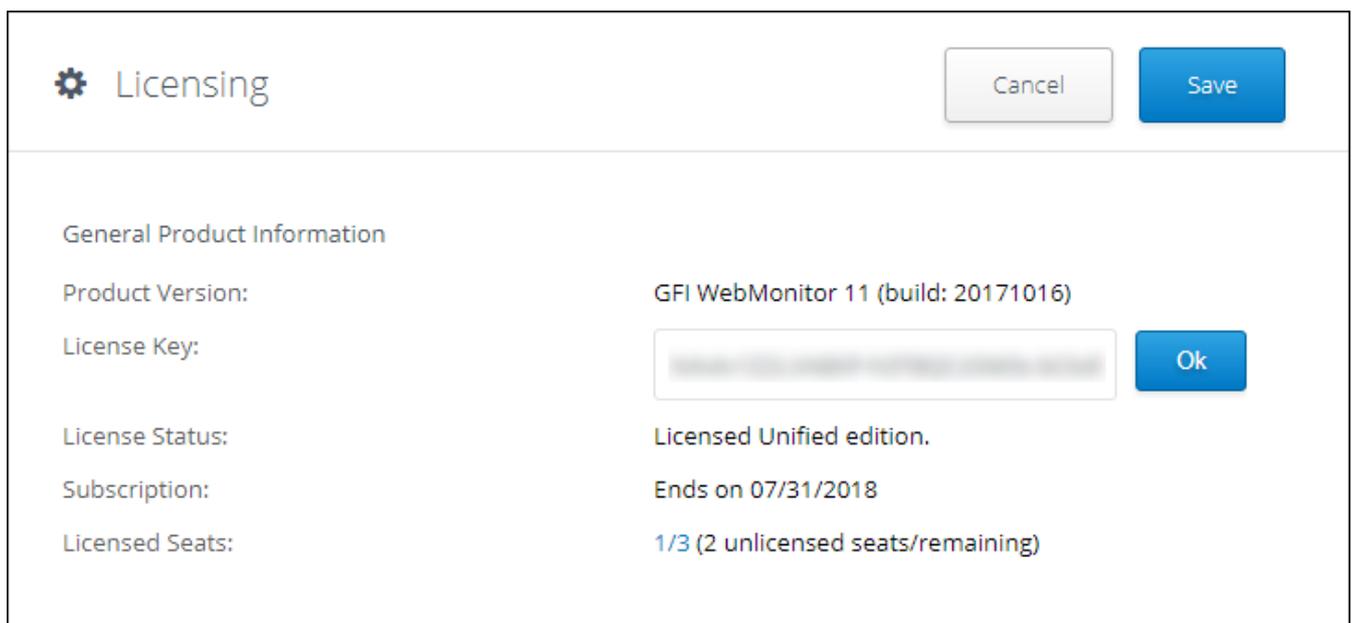
4.3 Licensing and subscription details

A valid license key is required by GFI WebMonitor. When the product is installed for the first time, the configuration wizard guides you to this area to enter the key you received when downloading the product. For more information, refer to [Licensing information](#) (page 10).

NOTE

The Configuration Wizard is launched automatically after installing GFI WebMonitor or manually from the **Settings** menu.

In GFI WebMonitor, users can be excluded from being counted against the license. For more information, refer to [Configuring a Licensing Exclusion List](#) (page 114).



Screenshot 59: Licensing details

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	For a new GFI WebMonitor installation, key in your license key in this field and click Update License . For an existing GFI WebMonitor deployment, this field displays the current license key. NOTE For users who wish to try out the product, an evaluation license key can be acquired from the GFI Software Ltd website. Click register to fill in the registration form and receive your evaluation key by email.
License Status	Defines the status of the current license, for example, whether the license key is active, expired, invalid or a trial license.
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.

4.3.1 Updating the license

NOTE

License activation requires an Internet connection.

To update the current product license key:

1. Go to **Settings > Advanced Settings > Licensing**
2. Type the new license key in the **License key** text box.
3. Click **Ok** and click **Save**.

4.3.2 Configuring a Licensing Exclusion List

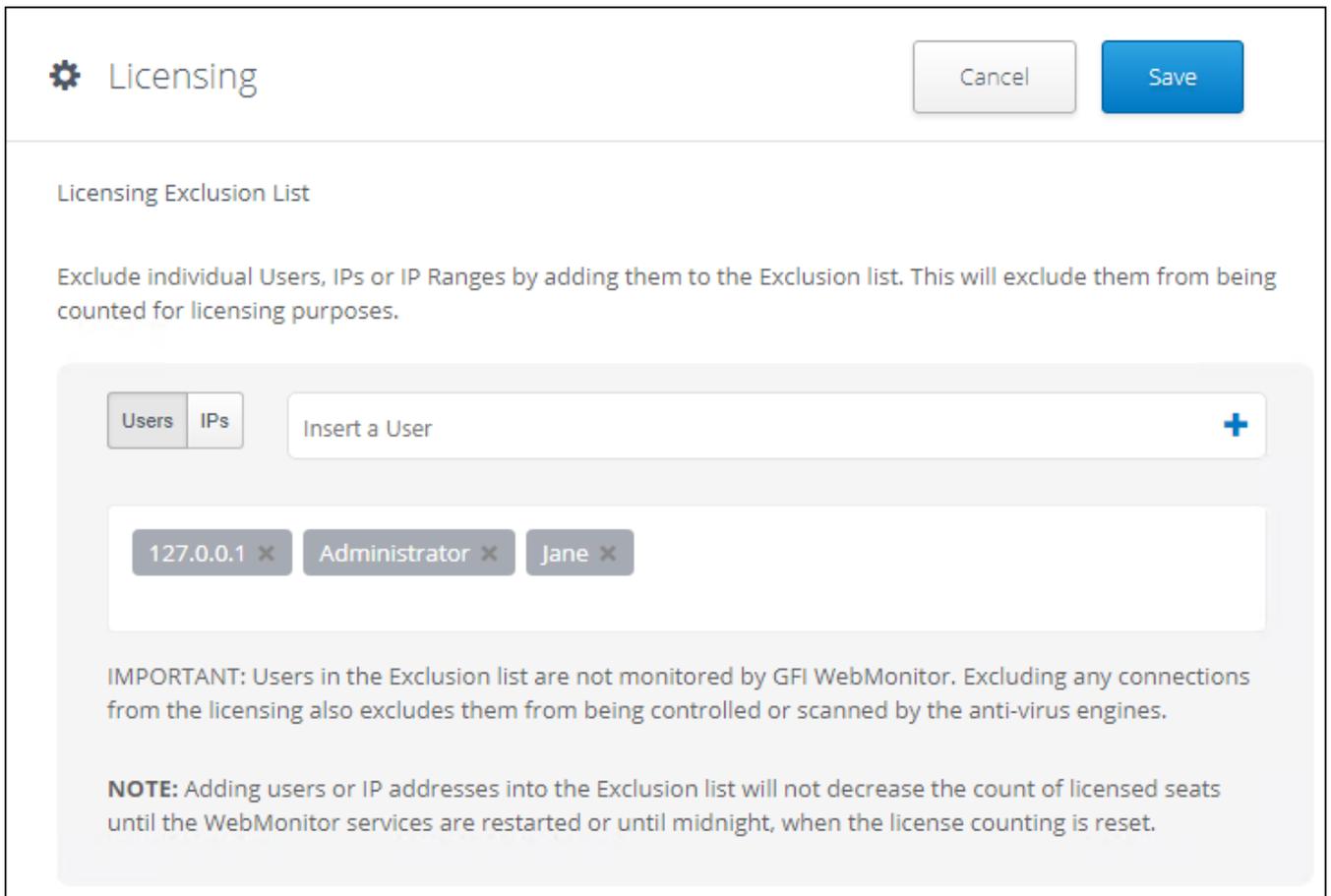
The Licensing Exclusion List is a feature that enables users specified in the list to be excluded from licensing. The users in the list are still allowed full access to the Internet, but they are not be counted for licensing purposes.

IMPORTANT

Users in the Licensing Exclusion List are not monitored by GFI WebMonitor. Connections from the users in the list are excluded from being controlled or scanned by the antivirus engines.

NOTE

The Licensing Exclusion List feature is not available when the Configuration Wizard runs for the first time. It becomes available after the initial setup has been completed.



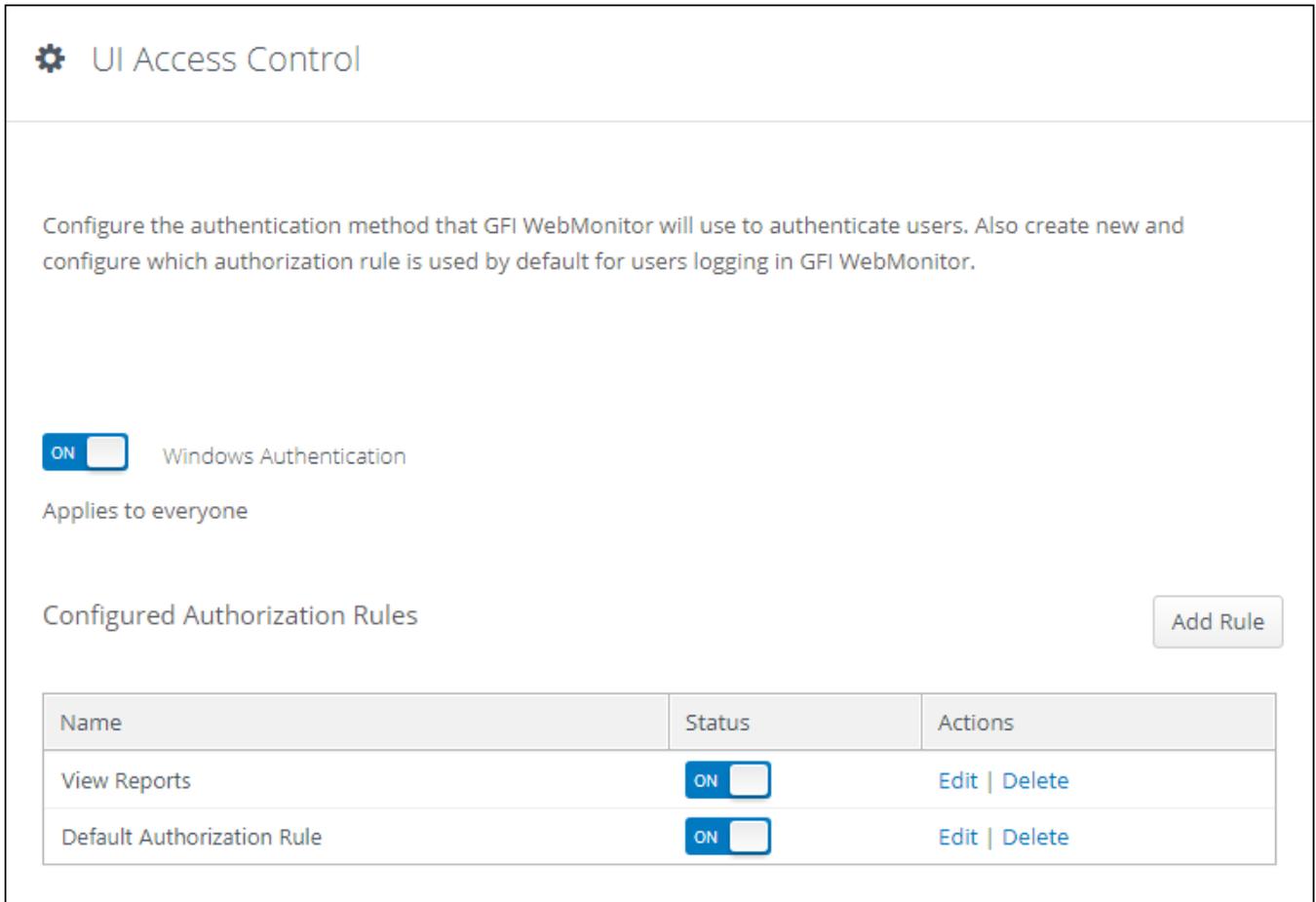
Screenshot 60: Licensing exception list

To add users or IPs to the list:

1. Go to **Settings > Advanced Settings > Licensing**.
2. In the Licensing Exclusion List area select Users and enter a user name in the available field, or select IPs and key in the IP address.
3. Click the **Add** sign.
4. Click **Save**.

4.4 UI Access Control

The **UI Access Control** grants or denies access to users for different sections of GFI WebMonitor. Users, groups or IPs listed in the configured Authorization Rules 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.



Screenshot 61: UI Access Control options

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

Options	Description
Use Windows Authentication to configure how GFI WebMonitor authenticates users.	When Windows Authentication is enabled, users are required to enter their credentials in their browsers when accessing GFI WebMonitor UI. GFI WebMonitor Authentication uses Active Directory Users and Groups.
Add new Authorization Rules to grant users access 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.

4.4.1 Configuring Windows Authentication

When **Windows Authentication** is enabled, GFI WebMonitor uses Active Directory or Windows Users and Groups to grant users access to the UI. Users are asked to enter their credentials when navigating within the GFI WebMonitor UI.

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 > Advanced Settings > UI Access Control**.
2. Click the **Windows Authentication** switch on or off.

3. Configure **Authorization Rules** to allow access to the GFI WebMonitor UI.

4.4.2 Add a new authorization rule

Configured Authorization Rules grant or deny access to users for different sections of GFI WebMonitor. Users, groups or IPs listed in the configured Authorization Rules 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.

The screenshot shows a configuration window titled 'Access Right' with two tabs: 'UI Control' and 'Access Right'. The 'UI Control' tab is active. It contains a text input field with the value 'View Reports' and a 'NAME' label. Below this is the 'Apply Rule to:' section with three radio buttons: 'Users', 'User Groups', and 'IPs'. The 'User Groups' radio button is selected, and the input field contains 'Insert a User Group' with a '+' icon and a '?' icon. Below this is a list of selected user groups, showing 'Power Users' with an 'x' icon. The 'Can View Data for:' section has three radio buttons: 'Users', 'User Groups', and 'IPs'. The 'Users' radio button is selected, and the input field contains 'Insert a User' with a '+' icon and a '?' icon. Below this is a list of selected users, showing 'bob' with an 'x' icon. At the bottom right are 'Cancel' and 'Save' buttons.

Screenshot 62: Authorization rule options

To add a new authorization rule:

1. Go to **Settings > Advanced Settings > UI Access Control**.
2. Click **Add Rule**.
3. Click **UI Control** tab.
4. In the **Name** field, enter a name for the new rule.
5. In the **Apply Rule to** area, specify the **User**, **User Groups** or **IP Address**, to which the rule will apply. Repeat for all required users, groups and/or IPs.

IMPORTANT

Users or groups specified in the **Configured 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 116).

6. In the **Can View Data for** area, specify the **User, Group** or **IP Address**, to which 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.

7. Click **Access Rights** tab. **Allow** or **Block** the following:

Option	Description
View Dashboard	When enabled, user can view all GFI WebMonitor Dashboards.
View Reports	When enabled, user can access the Reports tab and generate reports.
Change Settings	When enabled, user is allowed to modify GFI WebMonitor settings.

8. Click **Save**.

9. New rules are displayed in the Configured Authorization Rules area. Use the Actions menu to perform additional action:

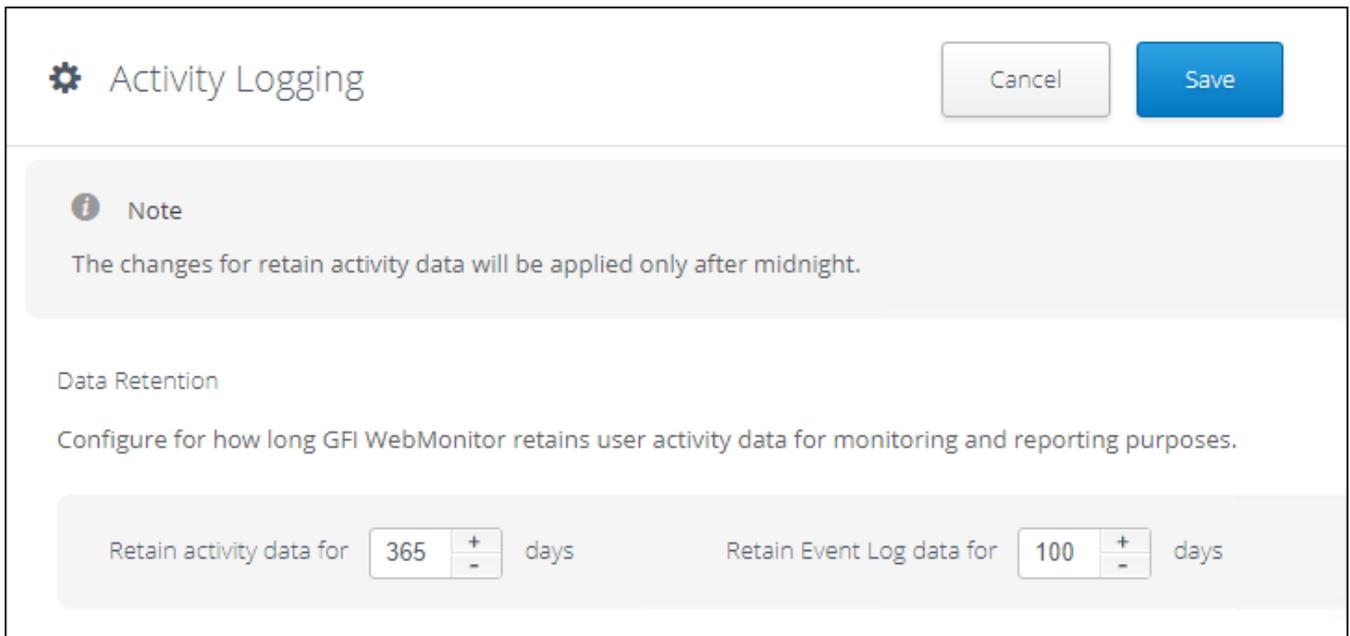
Option	Description
Edit	Click to enter editing mode. Change settings as required.
Delete	Click to delete the configured rule.
View	View a summary of the configured rule.

4.5 Configuring Activity Logging

All Internet traffic (excluding GFI WebMonitor updates) routed through GFI WebMonitor is logged for all licensed users by default. This data is required to populate dashboards and reports. GFI WebMonitor enables you to customize how long data is kept in the database.

NOTE

The changes for retain activity data are applied after midnight.



Screenshot 63: Activity logging options

To configure logging options:

1. Go to **Settings > Advanced Settings > Activity Logging**.
2. 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 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 affects 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>
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. Click **Save**.

4.6 Configuring Anonymization

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

- » Cloaks personal data so that user names and IPs 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.

Screenshot 64: Anonymization options

To enable Anonymization:

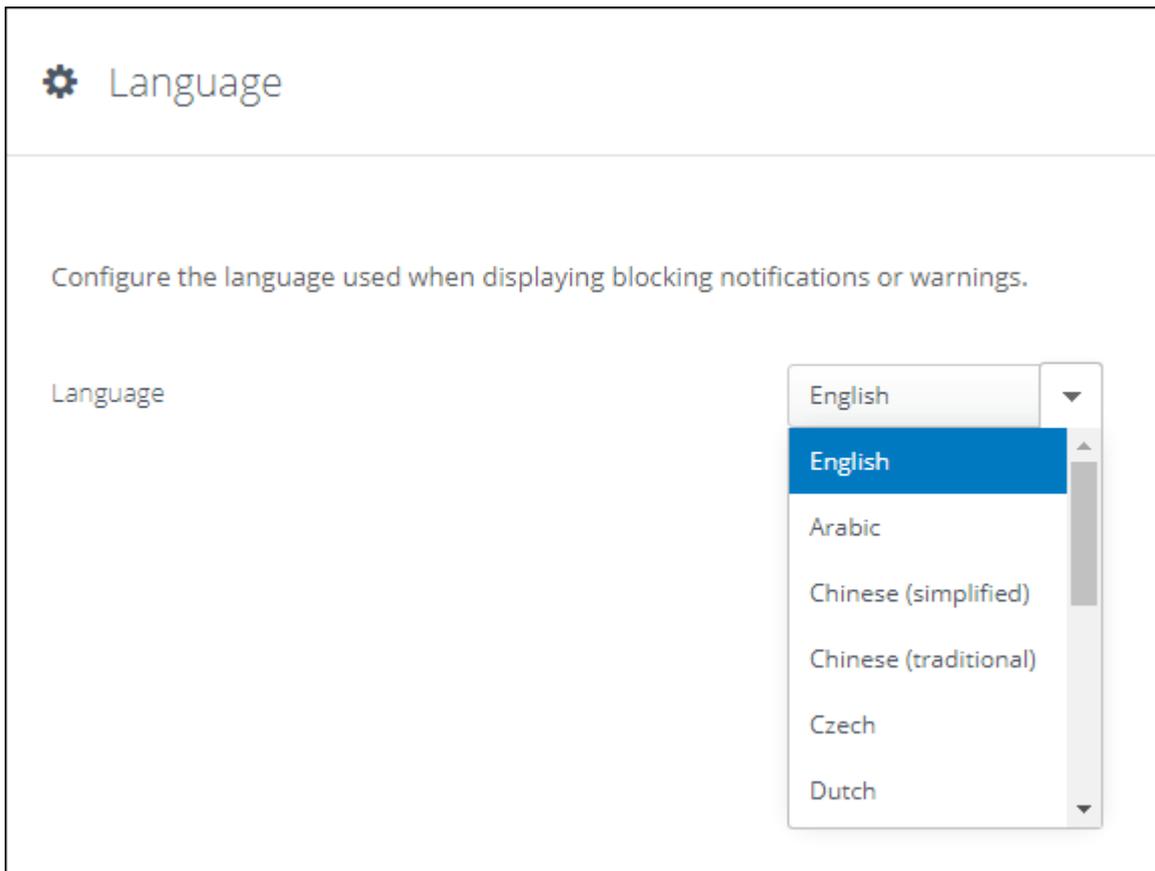
1. Go to **Settings > Advanced Settings > Activity Logging**.
2. Click the **Anonymize** switch to turn anonymization on.
3. Enter the passwords for **Responsible Person 1** and **Responsible Person 2**
4. Click **Save**.

NOTE

To disable Anonymization, click the **Anonymize** switch to the off position and enter the required passwords.

4.7 Language settings

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.



Screenshot 65: Language settings options

To change the language of warning messages:

1. Go to **Settings > Advanced Settings > Language**
2. select a language from the drop down list.

The new settings are saved automatically.

4.8 Configuring Security Engines

GFI WebMonitor uses various security technologies such as malware protection, anti-virus and anti-phishing engines to protect your network by scanning HTTP traffic. By default, all the security engines in GFI WebMonitor are enabled.

Security Engines

BitDefender (Version: 28757)
11/02/2017 13:37 Download finished

Check and update every 2 hours Update Now

Kaspersky (Version: 9688) Settings
11/02/2017 13:35 Download finished

Check and update every 2 hours Update Now

AntiPhishing (Version: 960902)
11/02/2017 13:27 Download finished

Check and update every 2 hours Update Now

ThreatTrack (Version: N/A)
Waiting for the first update ... Download failed

Check and update every 1 hours Update Now

Screenshot 66: Security engine settings

To configure a security engine:

1. Go to **Settings > Advanced Settings > Security & Updates > Security Engines**.
2. In the **Security Engines** area, slide the switch next to the engine to enable or disable it.
3. For each individual engine, configure the following:

Option	Description
Check and update every x hours	Configure the update frequency for individual engines by specifying the value in hours.
Update Now	Click to manually update individual engines.

4. [Optional] Configure the following options for all enabled security engines:

Option	Description
Send me an email when updates are successful	If an engine update fails, an email notification is sent to the domain administrator. For more information, refer to Admin Credentials for GFI WebMonitor Services (page 108).

NOTE

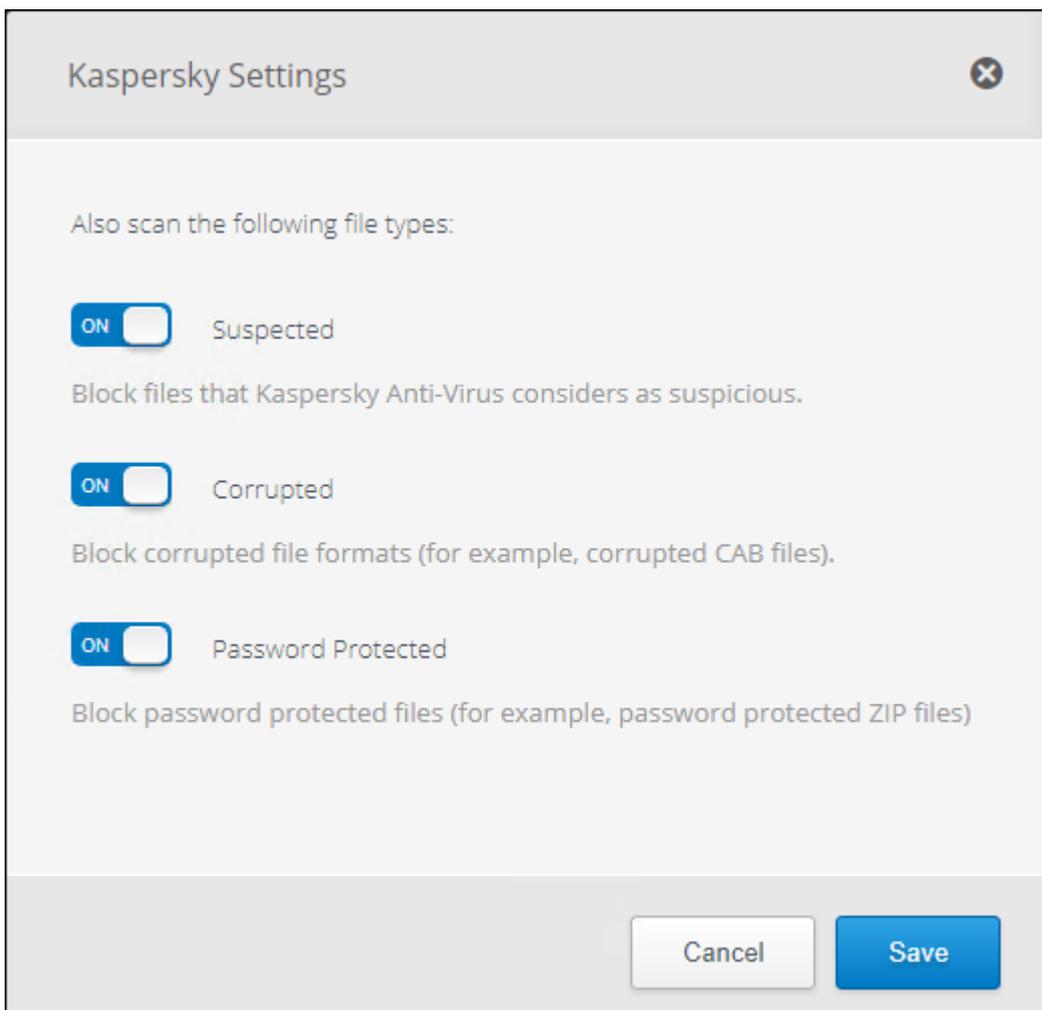
If you have problems when downloading updates, check your firewall settings to ensure exceptions for the URLs used for updates are in place. For more information, refer to [Firewall settings](#) (page 14).

Additional options are available for the Kaspersky engine. To perform additional configuration refer to the following section: [Configuring Kaspersky](#).

4.8.1 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.



Screenshot 67: Kaspersky extra configuration settings

To configure Kaspersky:

1. Go to **Settings > Advanced Settings > Security & Updates > Security Engines**.
2. Next to **Kaspersky**, click **Settings**.
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 **Password Protected**, click **ON** to enable scanning of protected files.
6. Click **Save**.

4.9 Configuring WebGrade updates

The WebGrade engine ensures that categorization for websites and applications monitored by GFI WebMonitor is always up to date. These updates are enabled by default when GFI WebMonitor is installed.

 WebGrade

Configure WebGrade updates frequency.

Send me an email when updates are successful

NOTE: The GFI WebMonitor administrator is notified immediately if an engine update fails.

ON WebGrade (Version: 337)

11/07/2017 04:10 Download finished

WebGrade categorization

Enable real-time lookup for URLs not found in the local database

WebGrade (local) database update

Check and update every hours

Screenshot 68: Webgrade Update settings

To change update settings:

1. Go to **Advanced Settings > Security & Updates > WebGrade**.

2. Configure the following options:

Option	Description
Send me an email when updates are successful	If an engine update fails, an email notification is sent to the domain administrator. For more information, refer to Admin Credentials for GFI WebMonitor Services (page 108).
Enable real-time lookup for URLs not found in the local database	This setting is enabled by default to allow GFI WebMonitor to search online for URL categories not found in the local WebGrade database.
Check and update every x hours	Configure the update frequency for individual engines by specifying the value in hours. Default is nine hours.
Update Now	Click to send an update request.

4.10 Configuring system updates

System updates enable you to keep your GFI WebMonitor installation up to date. When enabled, GFI WebMonitor checks for new updates at specified intervals, then downloads and installs them.

NOTE

During product updates the GFI WebMonitor services need to be stopped and restarted. This action disrupts Internet connections going through GFI WebMonitor. Internet usage can resume once the services are restarted.

GFI WebMonitor Updates

Configure the frequency of GFI WebMonitor product updates.

Send me an email when updates are successful

NOTE: The GFI WebMonitor administrator is notified immediately if an engine update fails.

Product Updates

11/07/2017 06:01 Download finished

During the product update, GFI WebMonitor services need to be stopped. This will cause all internet connections going through GFI WebMonitor to be terminated. Normal internet usage will be resumed once the services are started again.

Check and update weekly on **Saturday** at **00:00** **Update Now**

Screenshot 69: GFI WebMonitor Updates settings

To configure system updates:

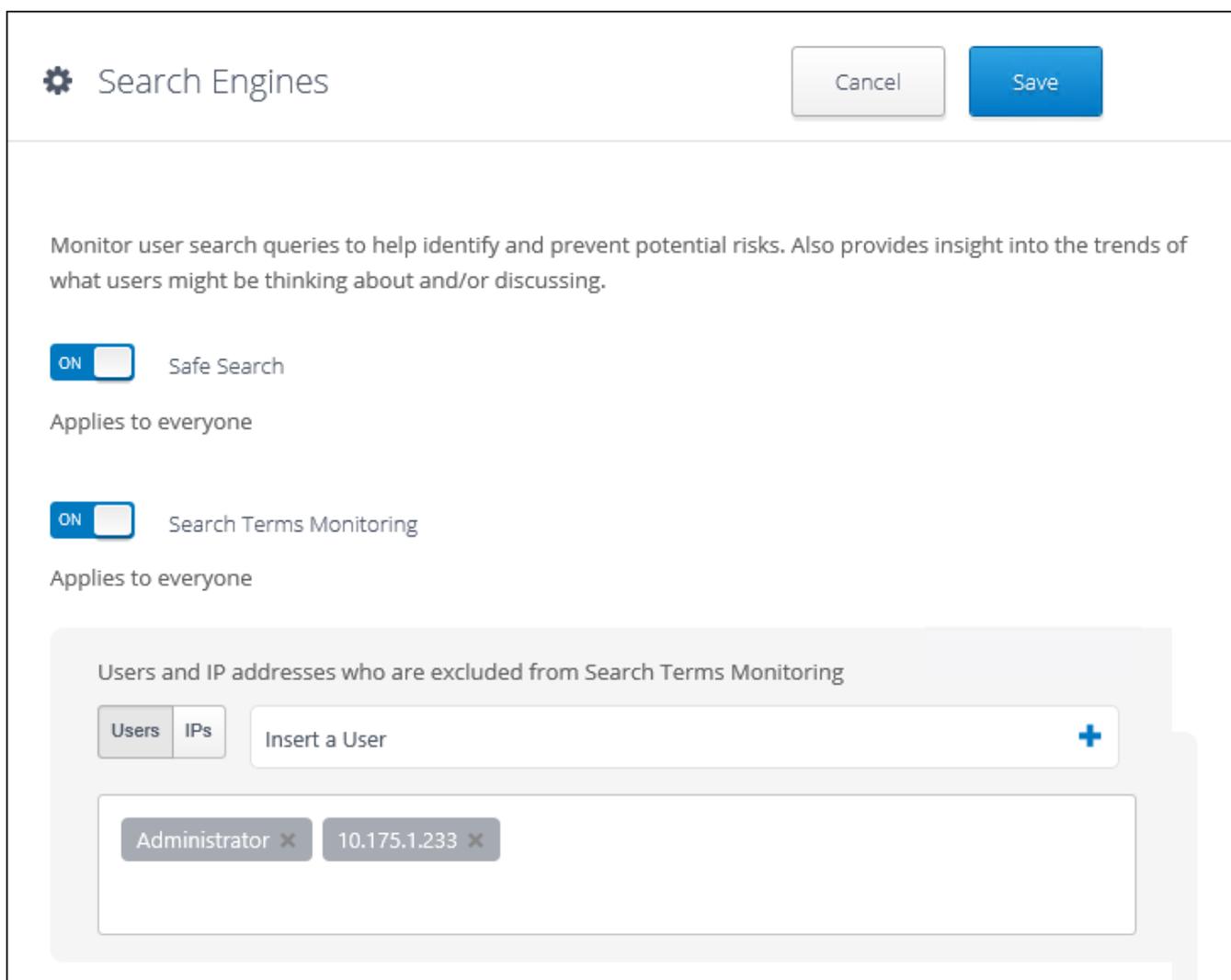
1. Go to **Settings > Advanced Settings > Security & Updates > GFI WebMonitor Updates**.

2. Configure the following:

Option	Description
Product Updates	Setting is enabled by default to keep GFI WebMonitor up to date with the latest updates. If disabled, GFI WebMonitor will still be active but the latest system updates are not downloaded.
Check and update weekly on <week day> at <time>	Configure the update frequency by specifying the day of the week and the time of day when GFI WebMonitor checks for updates.
Update Now	Click to manually check for system updates.
Send me an email when updates are successful	If an engine update fails, an email notification is sent automatically to the domain administrator. When this option is checked an email is also sent when the update completes successfully.

4.11 Configuring search engine options

GFI WebMonitor can monitor user search queries to help identify potential risks, while also providing valuable insight into the mindset of your users.



Screenshot 70: Search Engines options

The following search engine features are disabled by default when the product is installed:

Option	Description
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: <ul style="list-style-type: none"> » Google » Yahoo » Bing
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. Monitoring user searches helps identify potential high-risk issues as well as providing general mood indicators for your organization.

To exclude Users and IP addresses from Search Terms Monitoring:

1. Go to **Settings > Advanced Settings > Search Engines**.
2. Enable **Search Terms Monitoring**.
3. Insert the user name or IP address to exclude in the available field.
4. Click the **Add** icon.
5. Click **Save**.

Administrators can monitor search activity going to **Dashboards > Activity > Searches**.

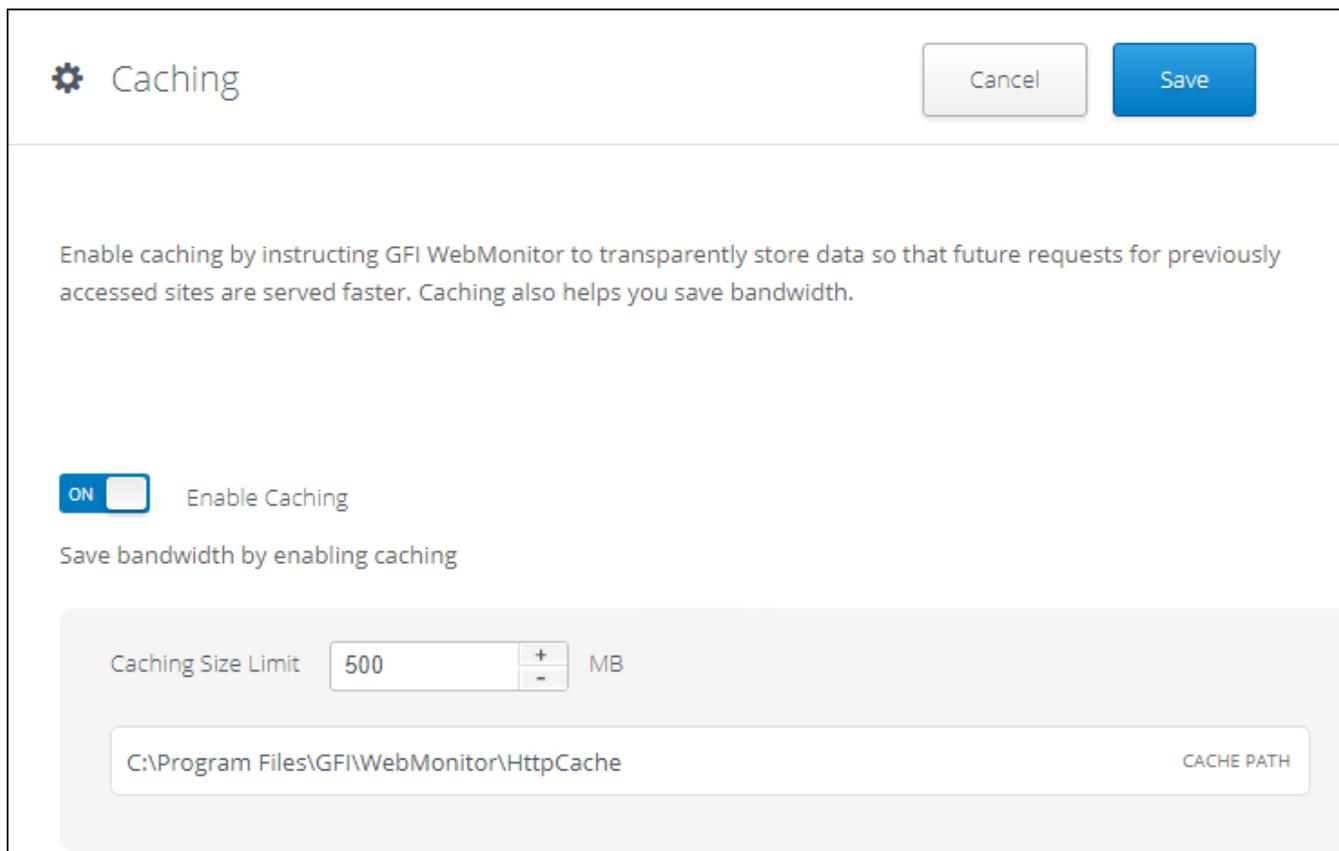
4.12 Configuring Caching settings

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 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](#) (page 128).

NOTE

This feature is not available for GFI WebMonitor installed as a plug-in for Microsoft Forefront TMG.



Screenshot 71: Caching settings

Caching is disabled by default.

To enable and configure cache settings:

1. Go to **Settings > Advanced Settings > Proxy Settings**.
2. Click **Caching**.
3. Click the **Enable Caching** switch to turn on.
4. In the **Caching Size Limit** field, specify the amount of data to keep in cache in MB.
5. In the **Cache Path** field, specify a location where to store temporary cached files. If no path is specified the settings cannot be saved.

NOTE

Ensure the path exists and the account under which GFI WebMonitor is running has sufficient privileges.

6. Click **Save**.

4.12.1 Adding Items to the Cache Exclusion list

When caching is enabled, content downloaded via HTTP is stored for future requests to the same resource, reducing bandwidth consumption.

IMPORTANT

Backup `ProxyConfig.xml` before making any changes.

To exclude sites from having their content cached, add them to the Cache exclusion list as follows:

1. Open `..\WebMonitor\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

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.

Disabling the FTP Access Filter

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

NOTE

This option is only available when GFI WebMonitor is installed as a TMG plug-in. For more information, refer to [Installing GFI WebMonitor as a plug-in GFI WebMonitor](#) (page 33).

Disable FTP Access Filter in Microsoft Forefront TMG

To disable the FTP Access Filter:

1. On Microsoft Forefront TMG machine, Go to **Start > Programs > Microsoft Forefront TMG > Forefront TMG Management**.
2. From the left panel, expand **Forefront TMG <machine name> > System**
3. From the right panel, click **Application Filters** tab.
4. Right click **FTP Access Filter** and select **Disable**.
5. Click **Apply**.
6. Save settings.

4.13 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.

The GFI WebMonitor Agent agent is delivered with small light database for categorization and lookup purposes. When a website is not found on the local database, the agent performs online lookups against the GFI WebGrade categorization service.

4.13.1 Agent System Requirements

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.

Agent Hardware

Component	Minimum hardware requirements
Memory	1 GB RAM
Physical storage	500 MB of available disk space

Agent Operating System

Operating system (32-bit or 64-bit)	Supported editions
Windows® 10	Pro & Enterprise
Windows® 8 and 8.1	Pro & Enterprise
Windows® 7	Ultimate, Enterprise & Professional
Windows® Vista SP2 or later	Ultimate, Enterprise & Business

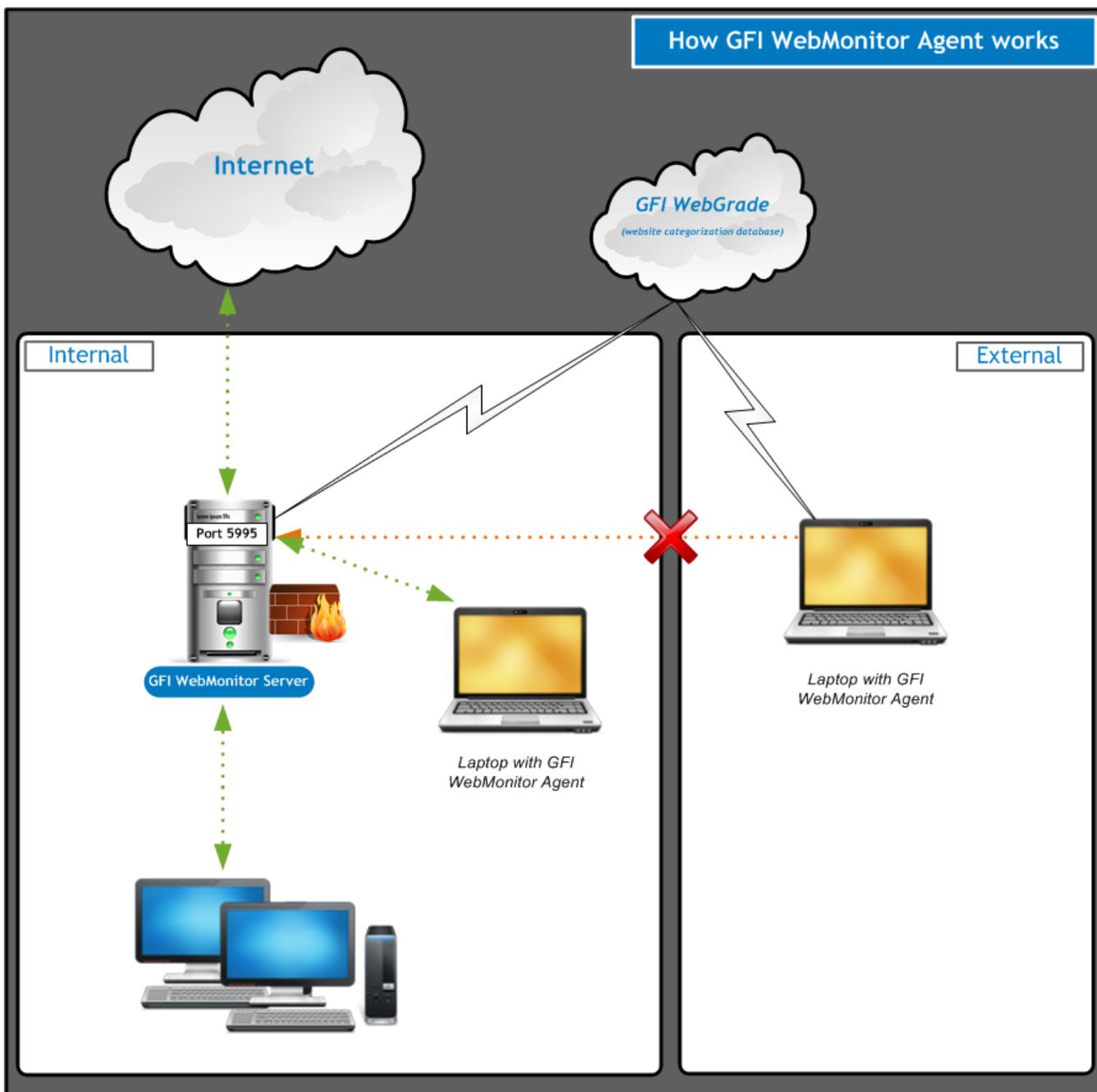
4.14 Downloading the GFI WebMonitor Agent

To download the GFI WebMonitor Agent:

1. In GFI WebMonitor, go to **Manage > Agents**.
2. Select one of the following download options:

Option	Description
Download (32-bit)	Select to install the agent on a 32-bit operating system. This downloads the following file: GFIWebMonitorAgent_x86.msi
Download (64-bit)	Select to install the agent on a 64-bit operating system. This downloads the following file: GFIWebMonitorAgent_x64.msi

4.15 How the GFI WebMonitor Agent works



Screenshot 72: GFI WebMonitor Agent functionality inside and outside the network

4.15.1 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 5996 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.

4.15.2 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.

4.16 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 115).

3. Click **Manage > Agents**.
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 5996.

IMPORTANT

Ensure port 5996 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. Click **Finish**.

4.17 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

4.17.1 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 130).
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.

4.17.2 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://<host-name>/<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 the 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](#)

4.17.3 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](#)

4.18 Installing the GFI WebMonitor Agent via GPO - Windows Server 2008 R2 or later

Group Policy software installation is a method that enables you to install applications automatically across your entire network. This topic describes how to install the GFI WebMonitor Agent via GPO on the following server operating systems:

- » Windows Server 2008 R2
- » Windows Server 2012 (including R2)
- » Windows Server 2016

To install the GFI WebMonitor Agent via GPO, run the following steps:

4.18.1 Step 1: Prepare the software to install	135
4.18.2 Step 2: Configure the ADM file	136
4.18.3 Step 3: Configure the GFI WebMonitor server location	136

4.18.1 Step 1: Prepare the software to install

1. Open the following location on the GFI WebMonitor server: <Program Files\GFI\WebMonitor\Agent\> and copy one of the following installation packages:

- » GFIWebMonitorAgent_x86 (Installer for Microsoft Windows 32-bit computers only)
- » GFIWebMonitorAgent_x64 (Installer for Microsoft Windows 64-bit computers only)

NOTE

Make sure that when deploying the 32-bit version of the GFI WebMonitor Agent, the domain policy used contains only computers running Microsoft Windows 32-bit version.

Similarly, ensure that when deploying GFI WebMonitor Agent 64-bit edition, the domain policy used contains only computers running Microsoft Windows 64-bit version.

2. Save the file to a shared folder on your network, accessible by all domains.
3. Locate the downloaded file. Take note of the folder path for later use.
4. Click **Start > Administrative Tools > Group Policy Management**.
5. Expand **Forest > Domains > domain name**. Right-click the domain name and select **Create a GPO in this domain, and Link it here...**
6. Enter a name for the new Group Policy Object (GPO). For example: GFI WebMonitor Agent. Click **OK**
7. Right-click the newly created Linked GPO and click **Edit**.
8. In the **Group Policy Management Editor** window, expand **User Configuration > Policies > Software settings > Software Installation**. Right click **Software Installation > New > Package** to configure the GPO to install on log in.
9. Enter the network path of the shared folder that contains the GFI WebMonitor Agent package. Click **OK**

NOTE

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

1. In the **Deploy Software** pop-up, select **Assigned** and click **OK**
2. The new package is now added under **Software Installation**.

4.18.2 Step 2: Configure the ADM file

1. Use an Administrative Template file (ADM) to set up and manage the required registry settings for the GFI WebMonitor Agent to communicate with GFI WebMonitor server.
2. To add an ADM template:
3. Click **Start > Administrative Tools > Group Policy Management**.
4. Expand **Forest > Domains > domain name**. Right-click GFI WebMonitor Agent and select **Edit**
5. In the **Group Policy Management Editor** window, expand **User Configuration > Policies > Software settings > Software Installation**.
6. Double-click the package to open the properties window.
7. In the **Deployment** tab, select **Install this application at logon**.
8. Click **Apply** and **OK** to close the window.
9. In the **Group Policy Management** window expand **Forest > Domains > domain name > GFI WebMonitor Agent**
10. In the **Security Filtering Pane**, click **Add**.
11. In **Select User, Computer or Group** add **Domain Users** and click **OK**
12. In **Group Policy Management**, expand **Forest > Domains > Group Policy Objects**. Right click GFI WebMonitor Agent and click **Edit**.
13. In the **Group Policy Management Editor**, expand GFI WebMonitor Agent > **User Configuration > Policies > Administrative Templates**.
14. Right-click **Administrative Templates** and select **Add/Remove Templates**.
15. Click **Add**. Open the GFI WebMonitor installation folder (default path: <Program Files\GFI\WebMonitor\Agent>).
16. Locate `GFIWebMonitorAgentSettingsTemplate.adm` and click **Open** to add the template. Click **Close**.

4.18.3 Step 3: Configure the GFI WebMonitor server location

1. In the **Group Policy Management Editor**, expand GFI WebMonitor Agent > **Computer Configuration > Policies > Administrative Templates > Classic Administrative Templates (ADM) > Software > GFI > GFI WebMonitor Agent Policies**.
2. In the right-hand pane, double click **Specify the settings used by the GFI WebMonitor Agent to connect to GFI WebMonitor Server**.
3. Select the **Enabled** radio-button.
4. In the **Server URL** field, type the GFI WebMonitor URL. Click **Apply** and **OK** to close the window.

5. The set up should now be complete. GFI WebMonitor Agent will be installed the **Next** time each client machine is started.

4.19 Configuring Remote Policies

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

A default policy is automatically created when GFI WebMonitor is installed. This policy is configured to **Allow** all Internet traffic to **Everyone**. You can change the policy type to **Block**, but you cannot delete or disable this default policy. New policies are added on top of the default policy to provide monitoring and filtering options as required.

To add a new policy:

1. Go to **Manage > Remote Policies**
2. Click **Add Policy**.
3. In the **Add Policy Name** field, type a policy name.
4. Drag policy elements from the left sidebar to the main policy screen. Available elements include:

Element	Description
Policy Type	Select the action taken by GFI WebMonitor when filtering internet traffic. Available options are: Allow , Block or Warn .
Users or Groups	Specify Users or Groups for whom the new policy applies.
Websites	Specify for which websites the policy applies. You can define specific website categories or input the URLs or IPs of websites to include in the policy.
Exceptions	Define users, groups or websites that are to be excluded from the policy.
Schedule	Select the time-window during which the policy is active.
Logging	The logging feature is enabled by default and cannot be disabled for Remote Policies. This feature is used to keep track of URLs visited by users.

5. Click **Save**.

4.20 Edit existing Remote Policies

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

To edit an existing policy:

1. Go to **Manage > Remote Policies**
2. Click **Edit**.
3. Make the required changes. For more information, refer to [Configuring Remote Policies](#) (page 137).
4. Click **Save**.

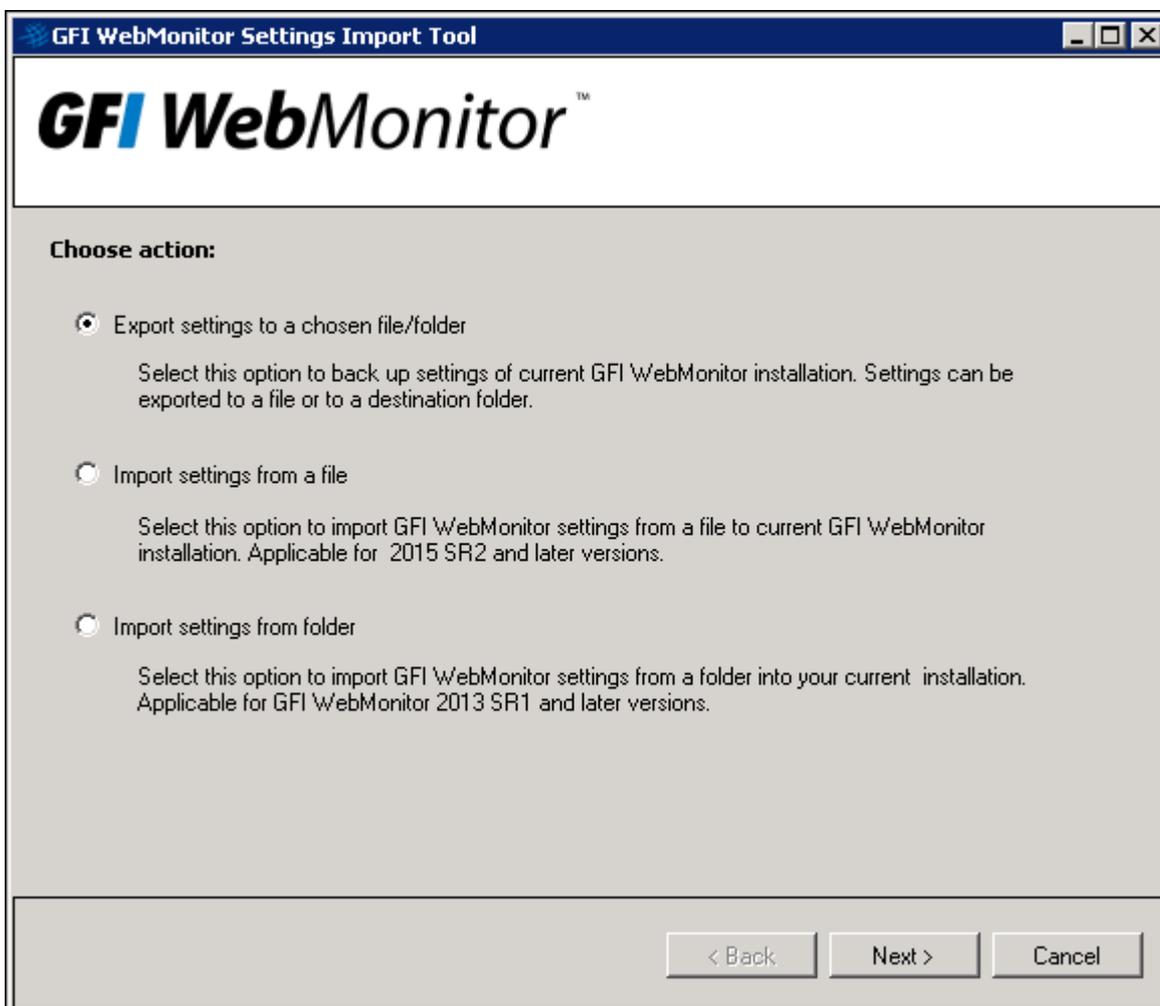
4.21 Using the Settings Importer tool

The Settings Importer Tool helps you import GFI WebMonitor settings from one server to another. The tool can be used to migrate GFI WebMonitor previous versions. For example, you can use this tool to import settings configured on a machine with GFI WebMonitor 2015 to a new machine on which you have the latest GFI WebMonitor installed.

NOTE

The Settings Importer Tool is available in GFI WebMonitor 2015 SR2 and later.

There are two versions of the Settings Importer Tool. The command line version of the tool is located in the GFI WebMonitor installation folder. The default path is `C:\Program Files\GFI\WebMonitor\Interface\Bin\WebMon.SettingsImporterTool.exe`. For more information on how to use this tool refer to the following article: http://go.gfi.com/?pageid=webmon_settingsimporttool.



Screenshot 73: Settings Importer Tool main interface.

1. From `C:\Program Files\GFI\WebMonitor\Interface\Bin\` locate and double click `WebMon.SettingsImporterTool.exe`.
2. Select from the following options:

Option	Description
Export settings to a chosen file/folder	Select this option to back up settings of current GFI WebMonitor installation. Settings can be exported to a file or to a destination folder.
Import settings from a file	Select this option to import GFI WebMonitor settings from a file to current GFI WebMonitor installation. Applicable for GFI WebMonitor 2015 SR2 and later versions.
Import settings from a folder	Select this option to import GFI WebMonitor settings from a folder into your current GFI WebMonitor installation. Applicable for GFI WebMonitor 2013 SR1 and later versions.

4.21.1 Export settings to a chosen file/folder

The Settings Importer Tool helps to export and import GFI WebMonitor settings.

To export settings to a file or folder:

1. From `C:\Program Files\GFI\WebMonitor\Interface\Bin\` locate and double click `WebMon.SettingsImporterTool.exe`.
2. In the GFI WebMonitor Settings Import Tool, select **Export settings to a chosen file/folder** and click **Next**.
3. Select one of the following options:

Option	Description
Use the settings from the current GFI WebMonitor installation	When selecting this option, the wizard automatically selects the default settings folder for export.
Select custom settings folder	Select this option to use an external settings folder. Click Choose source to browse and locate the desired folder.

4. Click **Next**.
5. Click **Choose destination folder** and provide the path where the settings file will be saved.
6. Select one of the following Export options:

Option	Description
Use pre-defined file-name	Select this option to use the filename created automatically by the wizard.
Use custom file name	Select this option to provide a custom name for the exported file.
Export to folder	Select this option to export settings to a folder. The wizard creates a folder called Data and a PAC File called <code>proxypac.pac</code> .

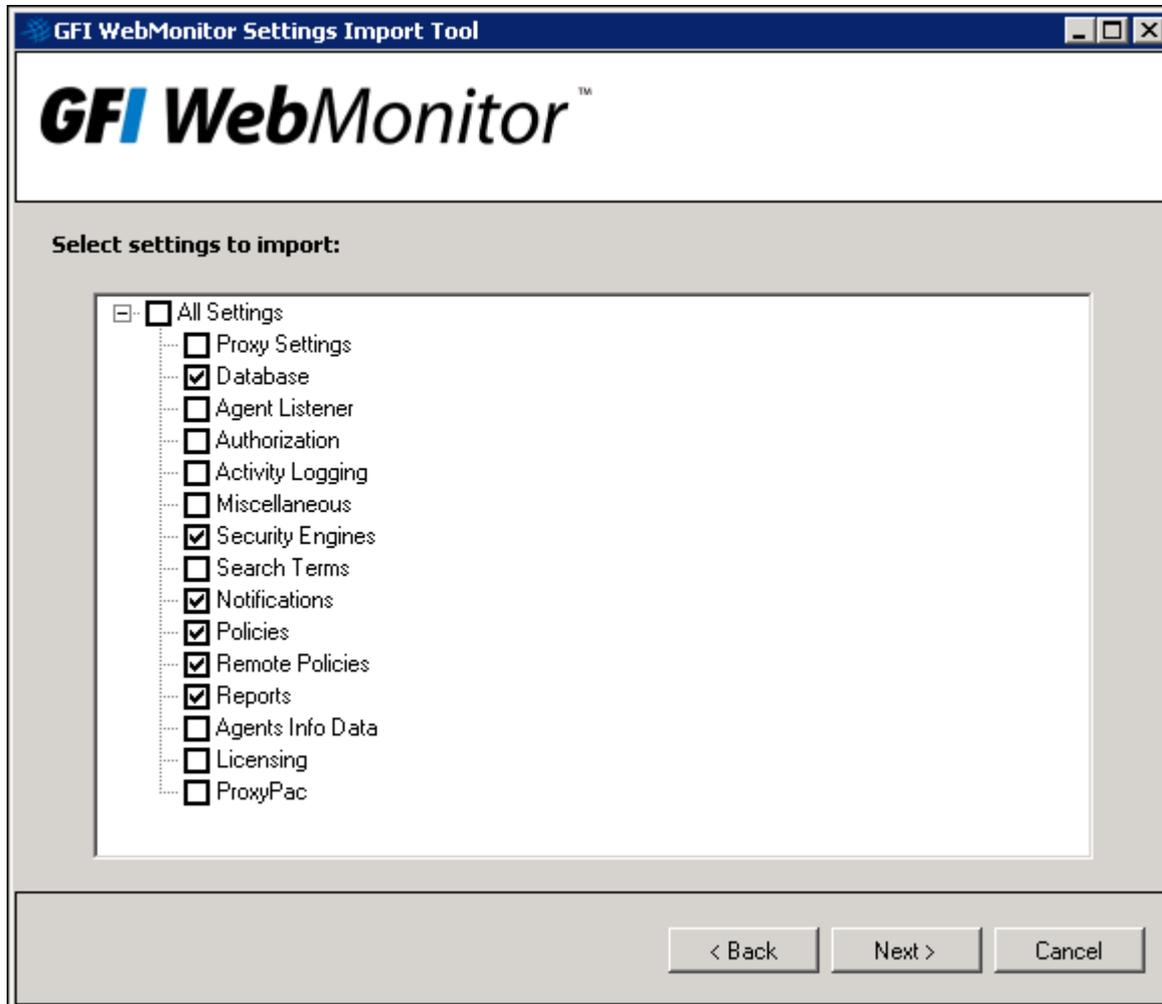
7. Click **Next**.
8. Review the Summary and use the link to open the export location.
9. Click **Close**.

4.21.2 Import settings from a file

The Settings Importer Tool helps to export and import GFI WebMonitor settings.

To import settings from a file for GFI WebMonitor 2015 SR2 and later versions:

1. From `C:\Program Files\GFI\WebMonitor\Interface\Bin\` locate and double click `WebMon.SettingsImporterTool.exe`.
2. In the GFI WebMonitor Settings Import Tool, select **Import settings from a file** and click **Next**.
3. Click **Choose source** and select the file that contains the settings to import and Click **Next**.



Screenshot 74: Options available when importing settings

4. Select the settings to import or check the **All Settings** checkbox to select them all. Click **Next**.
5. Click **Choose destination folder** to change the default location where to save the settings. The default path is set to `C:\Program Files\GFI\WebMonitor`. Click **Next**.
6. View the summary and click **Finish** to start the import.
7. When the import is complete, select one of the following options:

Option	Description
Click here to browse import location	Click to open the location where the settings have been saved.
Click here to restart WebMonitor services	If you have chosen to use the default destination folder in Step 5, GFI WebMonitor services need to be restarted after the import is ready. Click this link to let the wizard restart the services.

8. Click **Close**.

4.21.3 Import settings from a folder

The Settings Importer Tool helps to export and import GFI WebMonitor settings.

To import settings from a folder for GFI WebMonitor 2013 SR1 and later versions:

1. From `C:\Program Files\GFI\WebMonitor\Interface\Bin\` locate and double click `WebMon.SettingsImporterTool.exe`.
2. In the GFI WebMonitor Settings Import Tool, select **Import settings from folder** and click **Next**.
3. Click **Choose source** and select the folder that contains the settings to import.
4. Click **Next**.
5. Select the settings to import or check the **All Settings** checkbox to select them all. Click **Next**.
6. Click **Choose destination folder** to change the default location where to save the settings. The default path is set to `C:\Program Files\GFI\WebMonitor`. Click **Next**.
7. View the summary and click **Finish** to start the import.



Screenshot 75: Options available once the import is complete

8. When the import is complete, select one of the following options:

Option	Description
Click here to browse import location	Click to open the location where the settings have been saved.
Click here to restart WebMonitor services	If you have chosen to use the default destination folder in Step 5, GFI WebMonitor services need to be restarted after the import is ready. Click this link to let the wizard restart the services.

9. Click **Close**.

4.22 Configuring client's proxy settings

GFI WebMonitor acts as a Proxy Server to provide a connection between your internal network and the Internet. This means that traffic from client machines needs to be redirected through the GFI WebMonitor server. GFI WebMonitor offers different options on how to route client traffic.

Option	Description
Using fixed Proxy Settings	<p>Set up browser proxy settings on every client machine so that Internet traffic is redirected through the GFI WebMonitor proxy. Simply go to the Browser settings of the client machines and set the IP of GFI WebMonitor. To facilitate the administration of this feature GPOs can be used to:</p> <ul style="list-style-type: none"> » Assign the proxy settings » Disable proxy options
Using WPAD	<p>When deploying in Simple Proxy Mode, you can use WPAD to avoid configuring fixed proxy settings on client machines. WPAD allows client computers to automatically detect proxy server configuration settings. When this feature is enabled and the Internet browser connection settings are configured to 'Automatically Detect Settings', each client machine will automatically determine the IP address of the GFI WebMonitor server and use it as a proxy without further configuration.</p> <p>NOTE If WPAD is enabled, all browsers configured to 'Automatically Detect Settings' start automatically pointing to the GFI WebMonitor proxy. This is something you might want to avoid during the trial period.</p>
Using Transparent Proxy	<p>If you are deploying GFI WebMonitor in Gateway mode, you can use Transparent Proxy - a feature used to monitor and control HTTP and HTTPS traffic transparently. When a user makes a request to a web server, the Transparent Proxy intercepts the request to deliver the requested content. When GFI WebMonitor is deployed in this mode, you do not need to set client browser settings to point to a proxy.</p> <p>NOTE Transparent Proxy cannot be enabled in Simple Proxy Mode. If using Gateway Mode, we still suggest using fixed proxy settings for the trial since with Transparent Proxy, GFI WebMonitor is able to capture all traffic on the network.</p>

4.22.1 Configuring GFI WebMonitor machine as the Default Proxy using GPO

Group Policy can be used to enforce proxy settings across the domain, making it easier the administration of such task. GPO can be use in combination with WPAD, enforcing that clients' computers have the option to automatically detect the proxy settings. Alternatively, the proxy can be set directly on the GPO pointing to the correct IP and port used by the proxy.

To configure the **Proxy Settings** via GPO:

1. In command prompt, run `mmc .exe`.
2. In the **Console Root** window, go 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**.

- Click **OK**
- 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.

- Right-click **Default Domain Policy** and click **Edit** to open the **Group Policy Management Editor**.
- Expand **User Configuration > Preferences > Windows Settings > Internet Settings** and right-click **New**. Select the Internet Explorer version. Note that Internet Explorer 10 also applies to Internet Explorer 11.
- In the Internet Explorer properties navigate to **Connections > LAN Settings**.
- Enter the proxy details according to the way you want to publish the proxy. The Option are:

Option	Step
Publish the proxy using WPAD	Check the option Automatically detect setting .
Publish the proxy directly	Check Use a proxy server for your LAN checkbox. In the Address box key in the proxy server IP address. In the Port key in the port used (Default 8080).

- Click **OK** twice to apply changes
- 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 connections page via GPO](#) (page 143).

4.22.2 Disabling Internet connections page via GPO

The Internet **Connections** settings tab can be disabled on client machines to prevent users from modifying Internet settings to bypass GFI WebMonitor.

IMPORTANT

When deploying GFI WebMonitor in Transparent Proxy mode, you do not need to disable Internet connection settings on client computers if a gateway machine is configured as the only possible exit point to the internet. Traffic is filtered by the Transparent Proxy. For more information, refer to [Configuring Transparent Proxy](#) (page 93).

To disable **Connections** settings on clients machines through Windows[®] Server GPO:

- In the command prompt run `mmc .exe`.
- In the **Console Root** window, go to **File > Add/Remove Snap-in...** to open the **Add or Remove Snap-ins** window.
- Select **Group Policy Management** from the **Available snap-ins** list, and click **Add**.
- Click **OK**
- 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.

5 Troubleshooting and support

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

GFI knowledge base

GFI maintains a comprehensive knowledge base repository, which includes answers to the most common problems. GFI knowledge base 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 [knowledge base](#).

Web Forum

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

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.

Fill out the [Technical support form](#) and follow the instructions on this page to submit your support request.

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.

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.

5.1 Unable to browse

Issue encountered

Users are not able to browse or download files from the Internet after installing GFI WebMonitor in Gateway or in Simple Proxy mode.

Cause

Requests for web pages are blocked in the network.

Solution

Add an exception rule in the firewall on the GFI WebMonitor proxy machine to allow incoming TCP traffic on port 8080, port 80 and port 443. For more information on how to enable firewall ports on Windows® Firewall, refer to http://go.gfi.com/?pageid=WebMon_WindowsFirewall

5.2 Policies are not applied

Issue encountered

Policies are configured correctly, but they are not being applied to the clients.

Cause

Client browsers are not configured to use a proxy server. This can be tested by accessing http://go.gfi.com/?pageid=proxy_test. The test shows if GFI WebMonitor is used as proxy or not.

Possible solutions

After the installation, GFI WebMonitor proxy machine has to be configured to listen for incoming user requests.

Option 1:

Enable WPAD to enable client computers to automatically detect GFI WebMonitor as the default proxy. Then configure Internet browsers to automatically detect proxy settings. For more information, refer to [Configure Internet browser for WPAD](#) (page 88).

Option 2:

Configure client Internet browsers to use the GFI WebMonitor proxy machine as the default proxy by providing a fixed IP Address and Port number.

5.3 Old proxy settings detected

Issue encountered

Latest changes done to policies or to proxy settings are not taking effect.

Cause

Client browsers are still retrieving old proxy Internet settings.

Solution

Refreshing settings on each client browser is a manual process. Follow these steps:

1. In Internet Explorer, clear the **Automatically detect settings** check box, and save the changes.
2. Restart Internet Explorer, select the **Automatically detect settings** check box
3. Restart Internet Explorer again.

This forces a refresh of the Wpad.dat file

If the problem persists check further possible solutions http://go.gfi.com/?pageid=WebMon_AutomaticDetection.

5.4 Blank Real-time dashboard

Issue encountered

Real-Time Traffic Dashboard displays no traffic. The page is blank. Clients are using the proxy and policies are being applied correctly.

Causes

When GFI Proxy service is restarted while Real-Time Traffic page is open, no traffic is shown in the Real-Time Traffic Dashboard.

Solution

Restart both the GFI Proxy service and the GFI WebMonitor Core Service, then refresh the browser.

5.5 Page is not loading properly

Issue encountered

Some content, such as images, URLs and scripts are not displayed when visiting a website.

Cause

Many sites make use of Content Delivery Networks (CDNs) to dynamically display information. A CDN system keeps the copies of files at different servers across a global network. These networks are made up of several dedicated servers which work as distributed hosts of the content especially for static files such as images, videos, Java scripts, CSS files etc.

Possible solutions

Option 1:

To discover the sources, look in the lower left-hand corner of your browser for a caution sign. Double-click it to open a list of rendering errors on the page. In the list of errors, look for URLs that are linked to the errors.

After identifying the location of these images, and if the website is trusted, add them in the GFI WebMonitor Whitelist from **Manage > Policies > Whitelist**.

Option 2:

Make sure that the CDNs category is not blocked by one of the policies. From the GFI WebMonitor console, go to **Manage > Policies**. Check the settings of the policies and remove CDNs category if blocked by any policy.

5.6 Whitelist is not working

Issue encountered

URLs or domains added to the whitelist are still blocked by GFI WebMonitor.

Causes

The whitelist entry is not matching the page accessed, or there are invalid entries in the whitelist.

Possible Solutions

Option 1

Check the entries in the whitelist and see if they match the URL used. For example, `www.example.com` will not block access to `http://example.com`. Add new items as necessary.

Option2

Revise the whitelist entries and search for invalid entries like `*example.com` or `example.com*`

These entries will trigger an error if entered in the interface, but may get in the configuration files during an upgrade.

5.7 Certain HTTPS sites do not load

Issue encountered

Sites using HTTPS are not loading at all. The site loads correctly if the option **HTTPS scanning** is disabled.

Causes

The security level of certain sites is not compatible with HTTPS scanning.

Solution

Edit the **ProxyConfig.xml** file and add the domain to the list of excluded domains from HTTPS scanning. For more information, refer to [Adding Items to the HTTPS Scanning Exclusion List](#) (page 104).

6 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

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

Blacklist

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

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

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

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

File Transfer Protocol.

G**Google Chrome**

A web browser developed and distributed by Google.

GPO

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

Hypertext Transfer Protocol.

HTTPS

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

Local Area Network.

LDAP

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

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 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

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

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

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

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

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

Wide Area Network.

Web Proxy AutoDiscovery protocol

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

Web traffic

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

WebFilter Edition

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

WebGrade Database

A database in GFI WebMonitor, used to categorize sites.

WebSecurity Edition

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

Whitelist

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

Wide Area Network

An external network that connects machines in large areas.

WPAD

Web Proxy AutoDiscovery protocol.

7 Index

A

Advanced Settings 11, 24, 27, 110, 112, 114-117, 119-122, 124-128

Always Allowed 9-10, 43-46, 53, 57, 147

Always Blocked 8, 39, 43-44, 53

Anonymization 62, 65, 67, 69, 71, 76, 78-79, 112, 119

Anti-virus 14, 112, 121, 123, 130, 132

B

Bandwidth 7, 9, 40, 43, 47, 51-52, 55, 59, 61, 63, 70-71, 75, 78, 80, 83, 91, 113, 119, 127-128

C

Cache 127-128

Chained Proxy 86, 92

Configuration 10-11, 16-17, 20, 24-25, 37-39, 41, 84, 86-87, 90, 92, 94, 103, 106, 108-109, 113-114, 123, 133, 135, 142-144, 148

Console 16, 26, 103-104, 133, 142-143, 147

Credentials 23, 25, 37-39, 84, 90-91, 93, 96, 107-109, 116

D

Dashboard 67, 71-72, 75-76, 78, 92, 119, 147

F

FTP 129

H

HTTP 11, 14, 16, 18-21, 25, 84-86, 91, 93-94, 121, 128, 142

HTTPS Scanning 25, 84, 97-98, 100-101, 104

I

Installation 11, 15, 24-25, 27, 30-31, 35-38, 40, 84, 92, 106, 108-109, 112, 114, 125, 133-135, 138-139, 145-146

Integrated authentication 91, 96

Internet Gateway 17-18, 85

Internet Policies

 Search Engine Policies 127

K

Knowledge Base 9, 61, 63, 145

L

License key 10, 23, 25, 35, 37-38, 84, 114, 134

Log on as a service rights 15

M

Malware 9, 44, 52-53, 83, 121

Microsoft Forefront TMG 14-15, 17, 19-21, 24-25, 27, 30, 33, 35, 84-87, 89, 92-93, 95-98, 102-103, 113, 127, 129

O

Online lookups 130, 132

P

Phishing 7, 9, 52-53, 62, 83, 112, 121

Port Blocking 13, 16, 20-21, 85

Proxy Server 11, 15, 17-18, 20, 22, 25-27, 84-85, 87, 92, 113, 142-143, 146

R

Remote Access Control 24, 27, 91, 96, 112, 115-117

 Windows Authentication 107-108, 112, 116, 118

Reporting 12, 80, 105, 130

S

Security Policies

 Security Engines 112, 121, 124

Simple Proxy 11, 13, 16, 19-20, 22, 25, 84-85, 93, 142, 145

Snap-ins 16, 142-143

Spyware 7, 53

T

Technical Support 145

Temporary Allowed 9

Traffic Forwarding 13, 16, 20, 22, 85

Troubleshooting 18, 20, 145

W

Web Categorization 60, 73

Web Forum 145

Web traffic 9, 21, 33, 92

WebGrade Database 9, 15, 61, 125

Wildcards 129

WPAD 11, 18, 20, 25, 28, 35, 84-85, 87-88, 94, 96, 113, 132, 142, 146