*GFI Product Manual*

# GFI WebMonitor™

*Evaluation Guide Part 2: Thirty Day Trial*



Document Version: 2.1.0

Last updated (month/day/year): 6/26/2013

# Contents

# 1 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 (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.

# 2 Trial Recommendations

Before you begin, consider the following recommendations for a successful GFI WebMonitor trial.

» **Testing users** – Users included in the trial of GFI WebMonitor determine the success of the trial. Consider avoiding high-profile users, at least until you get the setup right, and only test the software by including users where your testing will not have any negative impact. This way you can avoid unintended issues.

> **NOTE**
>
> The benefits offered by GFI WebMonitor are evident when testing is carried out on a large number of users rather than on a single user. However, **do not** test the software immediately on all the users in the company!

» **Groups** – To define policies, you can use Active Directory or Windows Workgroup Users, Groups or IPs. It is typically easier to define policies based on Groups. As a pre-installation exercise, we recommend that you set up Groups or IP ranges in a manner that can be used to apply policies to Groups/IP ranges.

For example, create the following groups:

- An **All Staff** Group
- Groups for each department (if you want to apply specific policies based on departments)
- Management Group
- Senior Management Group.

> **NOTE**
>
> The reason for creating different groups is that CEOs and senior management typically expect to have different policies than those applied to staff.

» **Trial phases** - we recommend you carry out your trial in phases. For more information, refer to Trial Phases (page 7).

» **Take it easy** – We're sure you're eager to start monitoring and filtering. However, immediate drastic changes create resentment and unease. Start by monitoring only, and apply blocks only where and when strictly necessary.

> **IMPORTANT**
>
> We're here to help – if you have any problems with setting up or configuring the software correctly, get in touch with Support.

# 3 What You Can Achieve With GFI WebMonitor

With GFI WebMonitor you can:

| | |
|---|---|
| Create **filtering policies** based on **website categories**. | Block or allow websites based on website content. |
| Create **time and bandwidth based limits**. | Allow users to browse leisure sites such as auctions, travel or social network for, for example, two hours a week, to download 100MB worth of YouTube™ videos per day. |
| Apply policies based on **Users, IPs, or AD groups**. | The **top-down approach** to evaluating policies ensures a flexible method of applying policies that allow access to different users as necessary. |
| Apply **time schedules** to a policy. | While some policies should always apply, others can be set to apply during specific hours, for example, to allow users access to gaming or social networking only during breaks or outside office hours. |
| **Block Streaming Media** and control abuses. | Internet radio hogging your bandwidth? News and sports video reports causing issues on your hosted applications? Using GFI WebMonitor you can silently block streaming media. |
| Perform **Real-time monitoring** of your Internet resources. | 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 security, bandwidth and activity give you visual indicators of the current situation. |
| Use **Interactive dashboards** that allow you to view the data the way you need. | Sort and drill-down to quickly arrive to the information you need. |
| Configure **Alerts** and get notified when important events occur. | For example, a user downloaded too much in a single hour, or a user hit too many malicious websites, or when a user tries to avoid the proxy and other events which need high priority action. |
| **Enforce SafeSearch** on Search engines. | Ensure users cannot bypass X-rated content blocking by using Image search on Search engines. |
| **Monitor searches** in Search engines for additional insight on what is happening within the organization. | You'll be able to see what users are searching for. |
| Ensure **Full web protection**. | GFI WebMonitor combines various technologies and engines to ensure nothing malicious gets through to your network through user web browsing. |
| Enforce Download control policies that **block downloads based on file types**. | For example, block exe files, or potentially copyrighted material such as MP3 and AVI files. |
| Scan downloads using **multiple antivirus engines** just in case anything gets past the block | With each AV engine having a different reaction time to different kinds of malware, the best protection is to have multiple antivirus scanning using multiple vendors to ensure that no malware slips through. |
| Use our **Web Reputation** engine to block the threat of potentially malicious websites. | The **ThreatTrack website blacklist** enables you to proactively block hundreds of thousands of websites with bad intent. |
| Configure the **Anti-phishing engine**. | GFI WebMonitor's inbuilt updatable anti-phishing engine ensures that any known phishing sites are blocked. |
| Create **IM Blocking** policies to disable the most common Instant Messaging application. | Define policies to block various IM clients including MSN Live Messenger, Yahoo! Messenger, GTalk and Gchat, Facebook chat and Online portals used to get around IM client blocks. |

# 4 Trial Phases

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. We recommend the following plan:

*Table 1: Trial Phases*

| PHASE | DESCRIPTION |
|---|---|
| **Phase 1: Day 0 to Day 8** Monitor the situation | Set up GFI WebMonitor without any blocking policies to monitor your current situation. GFI WebMonitor works behind the scenes to gather some essential reporting data that will be used later on in the trial. |
| **Phase 2: Day 9 to Day 15** Analyze | Have a look at the data gathered after one working week - what is the situation? Can you identify any problematic areas? Get a basic picture of what is happening in your company - you might be surprised! Analyze and distribute some reports to key stakeholders. |
| **Phase 3: Day 16 to Day 25** Start taking control | Now that you have a good idea of what is going on, introduce some limiting policies. |
| **Phase 4: Day 26+** Increase scope | Add more users selectively to get even more valid data. |

## 4.1 Phase 1: Day 0 to Day 8 - Monitor the Situation

The strength of GFI WebMonitor comes from applying policies based on the specific circumstances of your environment. Rather than applying policies blindly, it is best that you collect some data on your users' browsing habits - and then apply policies accordingly.

### 4.1.1 Installation and Configuration

Installation and configuration is outside the scope of this guide. Refer to the Quick Install Guide - a short reference guide designed to get you quickly off the ground with installation and some configurations or the Administrator Guide for more detailed information.

Additionally, our support center is always ready to help you out in any problems you may encounter while installing or using the product.

### 4.1.2 Testing users

Use Group Policy objects (GPOs) to set proxy settings in the default browsers across your network, or otherwise set up a number of testing users to get some relevant data on their browsing patterns. As stated before, ensure that you introduce users where web filtering/blocking does not create any issues. It is not recommended to include high-profile users (for example, CEO or senior management).

### 4.1.3 Default policies

We recommend you leave the initial setup as is. Upon installation, GFI WebMonitor includes the following default policies:

- Default web filtering policy - monitors all users but applies no blocking
- Default streaming media policy - allows all streaming media
- Default download control policy - allows downloads of all file types
- Default IM control policy - allows Instant Messaging traffic
- Default virus scanning policy - scans and blocks a number of risky file types (ZIP, EXE, RAR, Word, Excel, PPT/PPS, MSI, MP3, PDF, JAR, CAB, GZIP, WMF, ANI, Unknown).

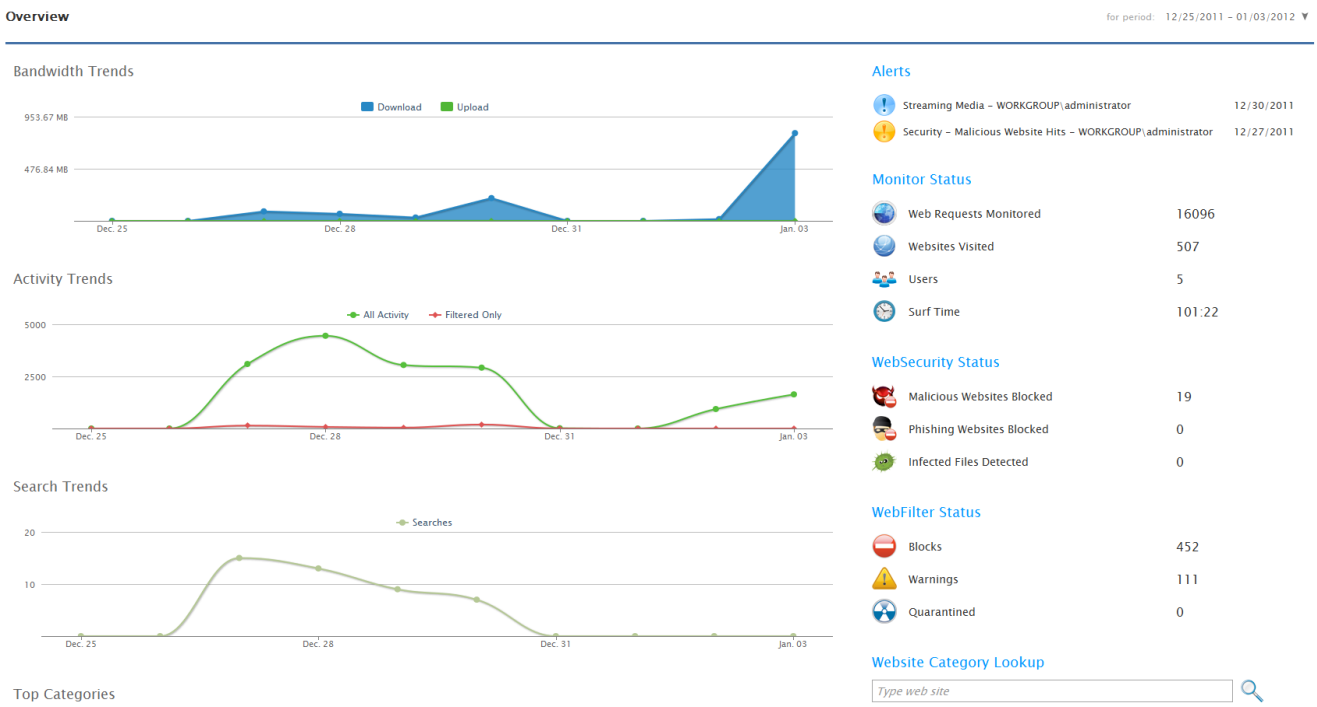
### 4.1.4 Dashboard

GFI WebMonitor has a dashboard that enables you to quickly get a glance of all the relevant information, such as:

- Surf Time
- Monitored Users
- Malware hits
- Infected files
- And other important information.

A number of charts give you a quick overview of the situation and help you identify any unusual spikes or suspicious behavior on your network. The data displayed in these charts includes graphical representations of:

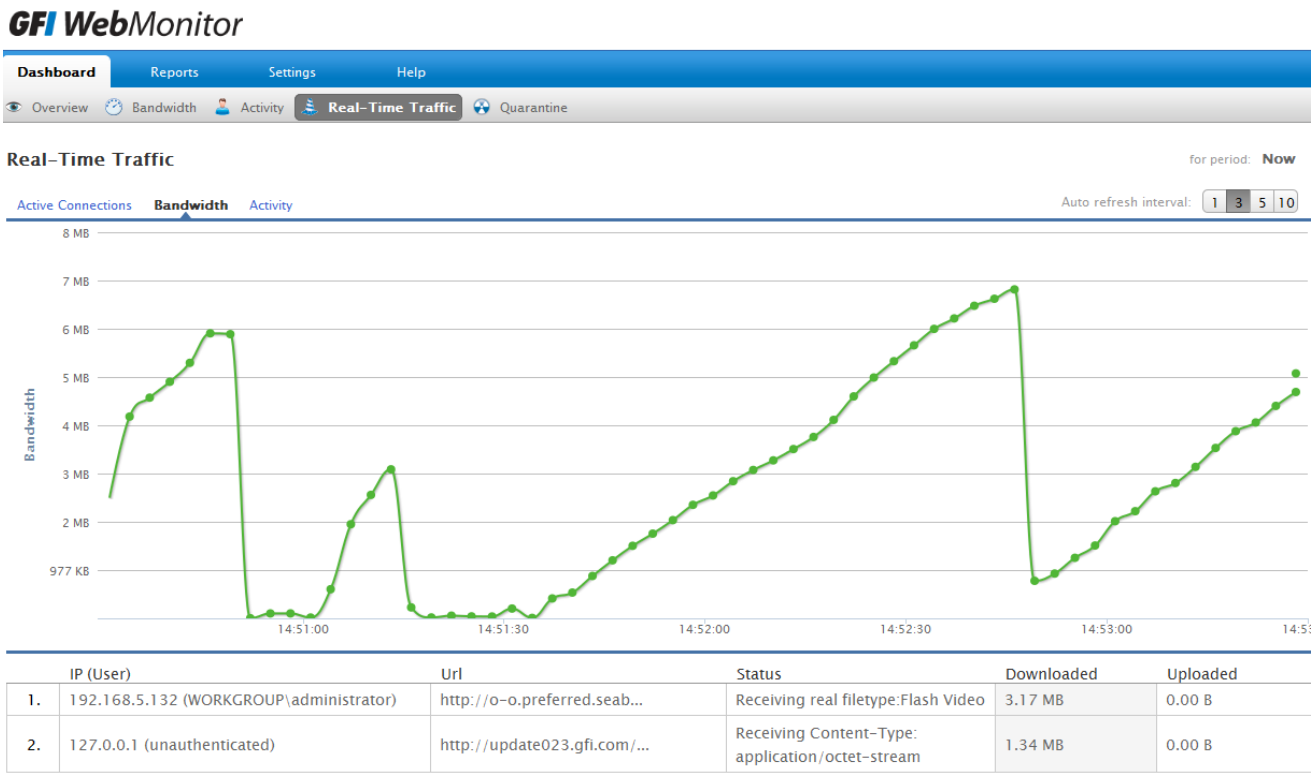
- Bandwidth usage
- Activity and Search Trends
- Top Categories
- Top Domains
- Top Users




*Screenshot 1: GFI WebMonitor dashboard*

### 4.1.5 Monitor for one working week

In the mean time you can look at the Interactive Bandwidth and Activity dashboards or the real-time traffic charts to know what is going on in real-time and analyze the current situation as necessary.




*Screenshot 2: Active (real-time) connections*

## 4.2 Phase 2: Day 9 to Day 15 – Analyze!

Now that you have a week's worth of browsing data it is time to check out what is going on in the organization. Find out how people are using the Internet to identify any problematic users or websites, and start deciding on how to tackle any issues.

### 4.2.1 Access monitoring reports

Start by analyzing the activity of the first 7 days of the trial.

1. Go to **Dashboard > Bandwidth**.

2. In the **for period** calendar, select the days when GFI WebMonitor was monitoring traffic.

3. You will now see a chart of what has happened in terms of downloaded and uploaded traffic. Switch to **Download Only** or **Upload Only**for a more specific analysis. Using the tabs underneath the chart, you can see which **Categories** consumed the most bandwidth, and if you switch to the **Websites** or **Users** tab, you will see the websites or users that consumed the most bandwidth. The information nuggets also give you the projected download and upload for the whole month based on current data.

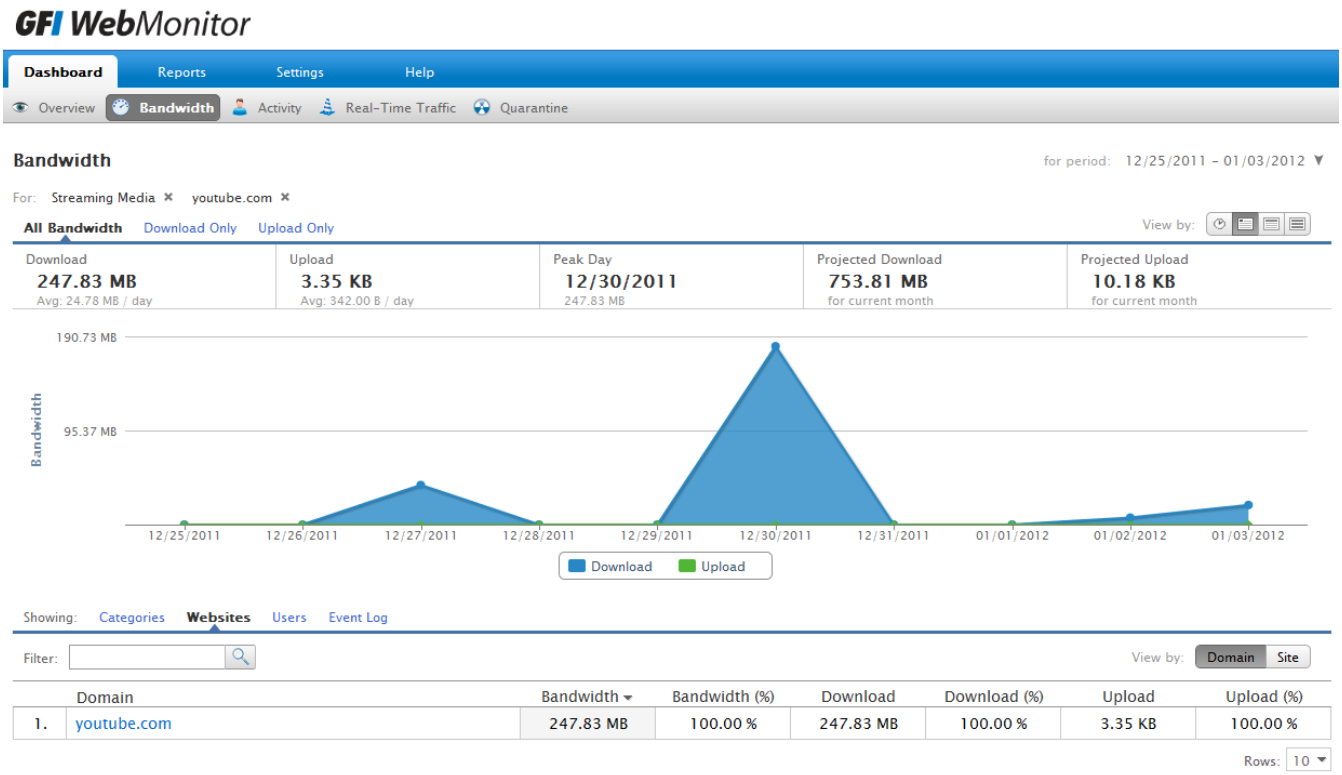
4. To analyze further, simply click on the **Category**, **Website** or **User** that interests you, and the data will be filtered by the item you have chosen. You can progressively drill down until you arrive to the data you require. You can also **sort by any column**, and search using the tab. Remove the current filter by clicking the on the applied filter.

> **NOTE**
>
> Although Bandwidth information may be of particular interest to IT Administrators, you can also make a mark by showing the same type of **reports based on Activity and Surf Time** to relevant management persons.

5. When browsing the Activity reports, keep an eye out for specific categories such as: “Abused Drugs”, “Gambling”, “Hacking”, “Job Search” and other questionable content. If you see any objectionable activity, it is recommended you go to the relevant person and advise them of the situation.

6. If there is little activity to see, then you need to **add more users** to build up data. No data is displayed in the **Activity > Filtered Only** reports if you have not put any blocks in place.

> **NOTE**
>
> Show the reporting capabilities of GFI WebMonitor on your computer, or via the web interface to interested managers. The drill-down feature gives you so much flexibility in quickly finding out what is happening on your company Internet connection.




*Screenshot 3: Drill-down reports*

### 4.2.2 Start talks with stakeholders

By now, you have some idea of common issues in your organization. You should now start thinking about introducing some control. Start discussions with stakeholders following the reports you have shown them. Until discussions are concluded, keep monitoring, and add more users if necessary.

## 4.3 Phase 3: Day 16 to Day 25 – Start Taking Control

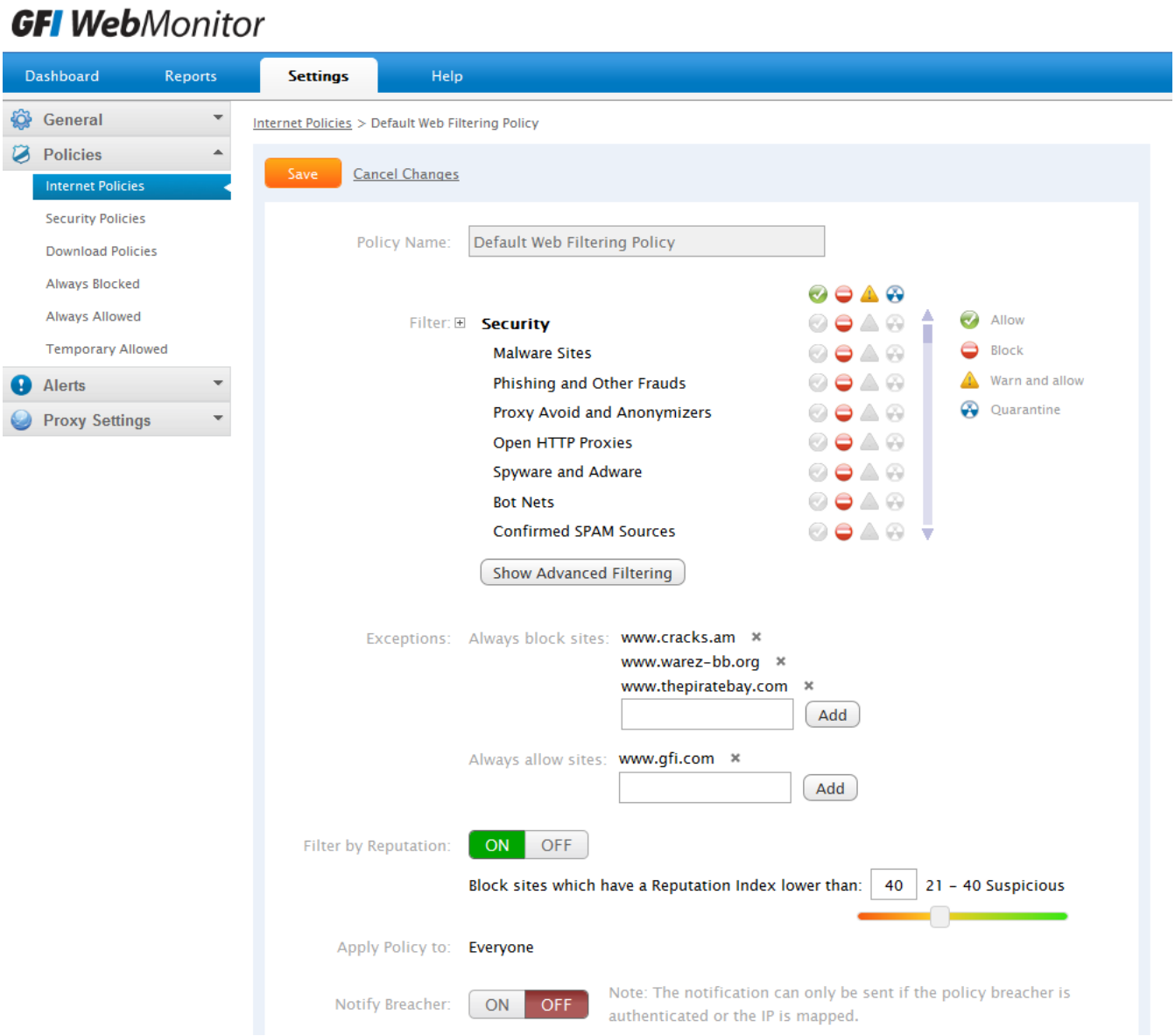
Now that you have seen what is going on, it is time to start taking control and introduce some blocking or limiting policies. Here we explain what to do and consider a few common scenarios for applying policies.

1. Make an official announcement to all your staff that Internet use is now being monitored and see how many of your problem users moderate their surfing habits over the next ten days.

2. Block access to sites that should never be accessed on company computers. Categories to note would be anything in the Security category group, for example **Adult and Pornography** or **Gambling**, and others in the Legal Liability category, as well as others that may be relevant to your work environment. The How to create a web filtering policy section below shows you how to do this.

**NOTE**

If you are serious about web security, you should also enforce blocking by web reputation. The **Web Reputation Index** is a score based on the safety of a website and enables you to block websites identified as “Unknown”, “Suspicious” or “Medium Risk”. Web reputation scores are valid across any category, since any type of website may contain malicious content. With Web Reputation you ensure that sites are blocked BEFORE they become a threat.




*Screenshot 4: Setting up a security focused default policy*

3. If you are concerned with leisure browsing, limit access to **Shopping**, **Games**, **Social Network** and other categories you identify as potential time wasters. Access to such sites can be limited to a certain amount per week (for example, 3 hours per week) using the **Web Browsing Quota Policies**. For more information, refer to How to Create a Web Filtering Policy (page 13).

4. If you identified users who are "bandwidth hogs", apply some bandwidth limits. For more information, refer to How to Create a Web Browsing Threshold Policy (page 18).

5. After applying some controlling policies, create management reports and send these out to the relevant persons within the company:

» Run the **Bandwidth Usage Trends** report to discover which domains, categories and users are hogging Bandwidth

» Run **Activity Usage Trends** report to discover the top domains being accessed, and the categories that are most popular with users.

» To find who and what could be creating security problems, run the **Top Users blocked by Security Polices** report.

» For HR issues, run one of the pre-defined HR reports such as **Drug Related Access** report or **Job Search Websites** report and send these to HR and managers. Show managers these reports through the web interface (http://1.1.1.1) or schedule them for automatic distribution by email.

> **NOTE**
>
> You can create targeted department reports by including specific users.

> **NOTE**
>
> You can export reports in CSV format and send them to the appropriate managers by email, or show them these reports directly through the web interface (log using http://1.1.1.1 on the machine where GFI WebMonitor is installed). Remember that for http://1.1.1.1 to work the following conditions must be met:
>
> » Access to the UI has been granted
>
> » Internet browser has been configured to use GFI WebMonitor as the Proxy server.

6. Take some time to evaluate additional reports that can help you increase productivity and identify security issues within your environment:

» **Top Bandwidth Hogs** – sort by Downloaded

» **Top Productivity Logs** – sort by Surf Time

» **Security issues** – find categories related to security, such as “Hacking”, “Malware Sites”, “Proxy Avoidance and Anonymizers”.

7. Once you have put in a few controls and limits, let GFI WebMonitor do its work again for a few days.

### 4.3.1 How to Create a Web Filtering Policy

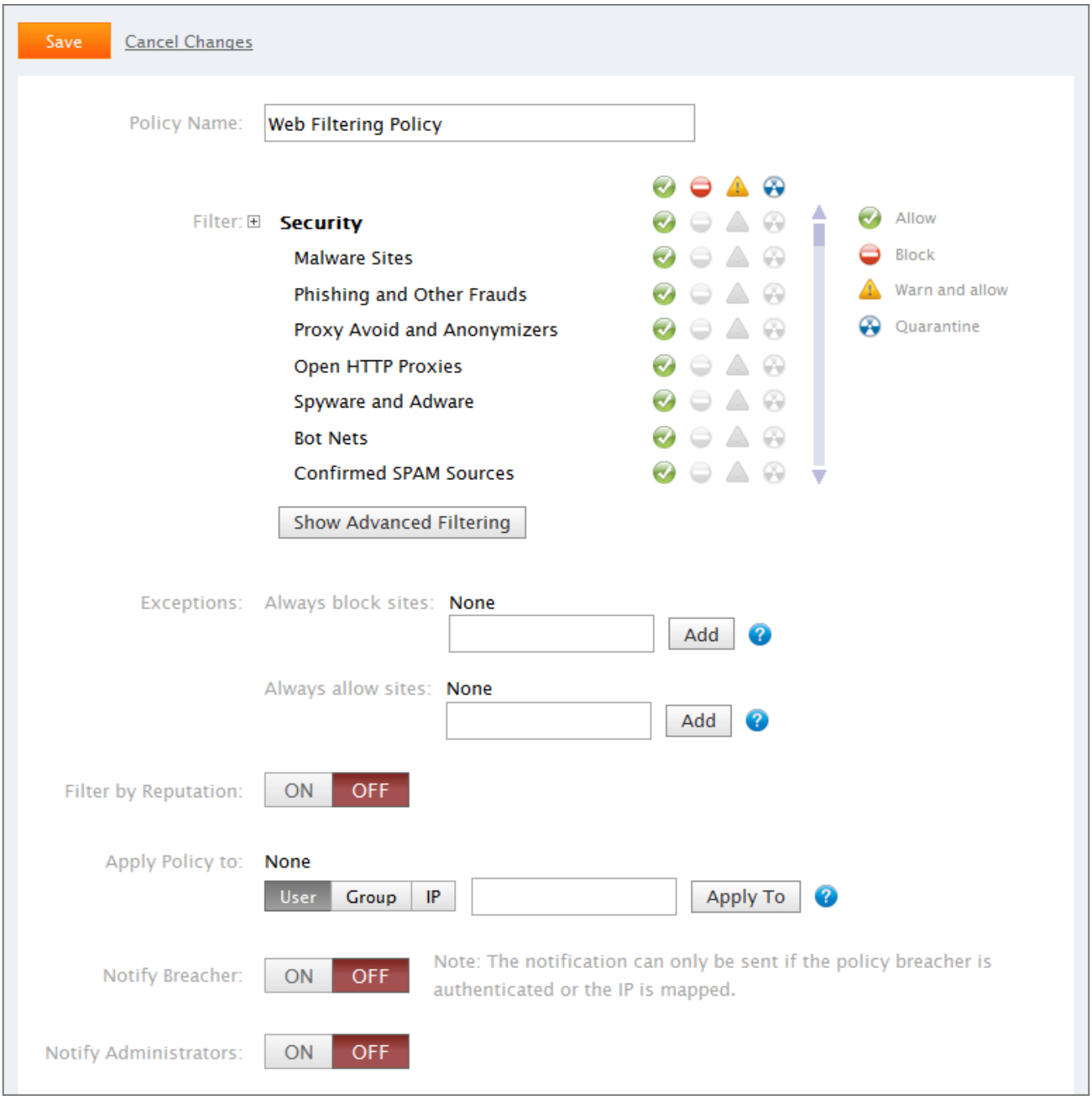
Set up filtering policies from **Settings > Policies > Internet Policies > Web Filtering Policies**.

#### Default filtering policy

GFI WebMonitor ships with a **Default Web Filtering Policy** that applies to **all users**. This is the fallback policy – if no policies are matched for a given situation, the default policy will apply. By default, this policy allows access to all categories of websites for everybody, without any filtering.

We recommend you use this policy to block only highly problematic categories typically considered as high risk, such as **Security** and **Legal Liability Groups** (for example, Adult and Pornography, Gambling, Malware sites, Phishing and Other Frauds, Proxy Avoidance and Anonymizers, SPAM URLs and Unconfirmed SPAM Sources).

> **NOTE**
>
> You cannot disable this policy, and you cannot change the users it is applied to. We recommend you set up additional higher priority policies where necessary.




*Screenshot 5: Creating a web filtering policy*

### 4.3.2 Creating a Leisure browsing policy

Once you have established the **Default Web Filtering Policy**, add more policies to refine your setup. The following steps guide you through the steps required to create a new Web Browsing Policy that blocks social networks (Facebook) and other leisure browsing to most users during office hours, but allow it for Top Management, Marketing and specific users.

To create a new Leisure Browsing Policy in the Web Filtering Policies:

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

2. Click **Add Policy**.

3. In the **Policy Name** field, enter **Leisure Browsing Policy**.

4. Use the provided filters to block categories such as: Auctions, Dating, Entertainment and Arts, Fashion and Beauty, Games, Hunting and Fishing, Internet Communications, Music, Recreation and Hobbies, Shopping, Social Network and any other categories which could cause productivity issues in your company. Remember also to block any Security and Legal Liability categories.

5. In the **Apply Policy To** field, add a Group that includes all users on your domain.

> **NOTE**
>
> The policy we are creating blocks all users. In the next section we define another policy that excludes specific users and caters for marketing and exceptions to the policy.

6. In the Policy Schedule, 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.

7. Click **Save**.

### 4.3.3 Soft blocking policies

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 in the web filtering polices, instead of "Block" ( ), click "Warn" ( ).

### 4.3.4 How to Create a Leisure Browsing Exclusion Policy

1. In the Web Filtering Policies page, click the **Leisure Browsing Policy** you have just created and click **Clone Policy**.

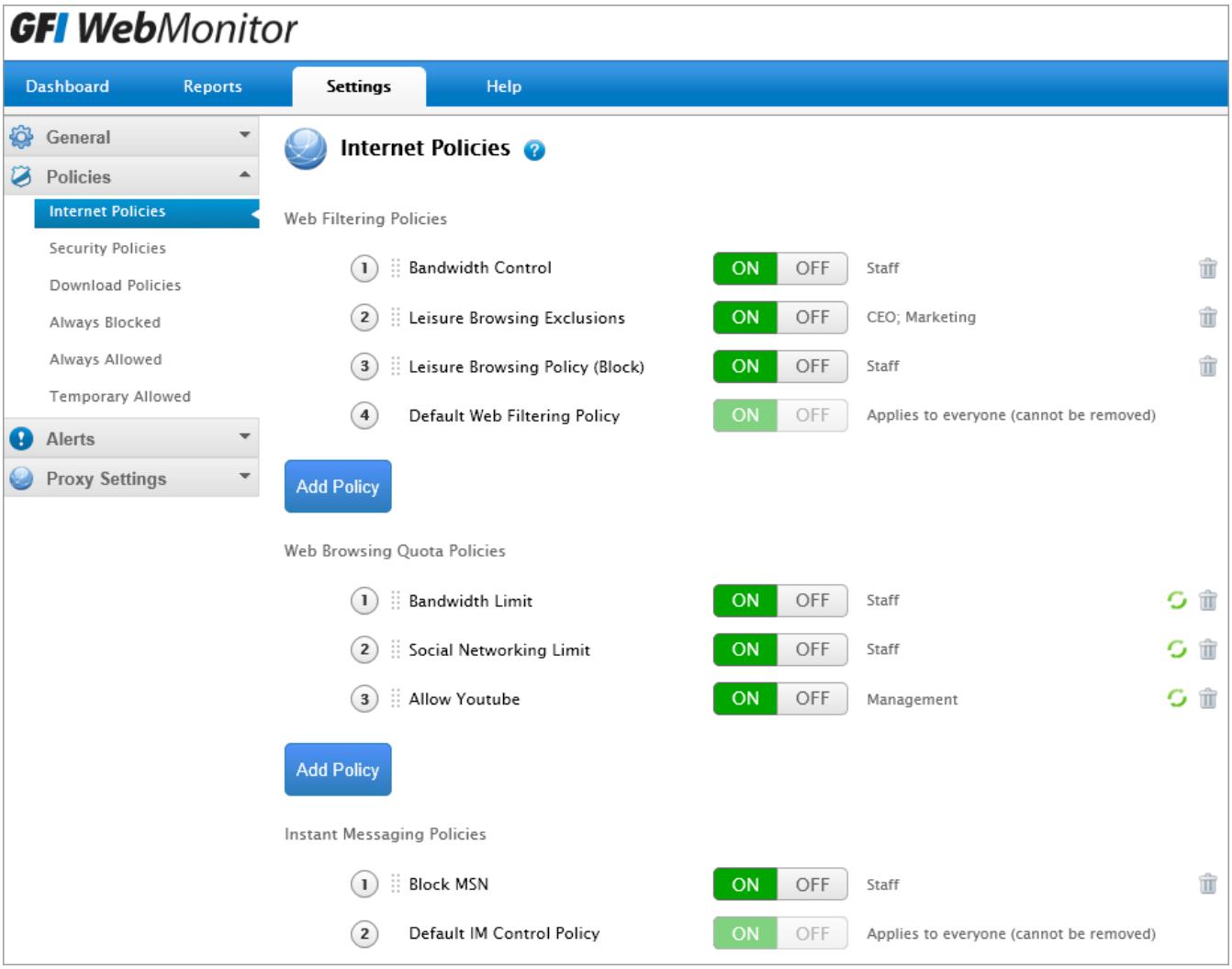
2. Change the name of the new policy to **Leisure Browsing Exclusions**.

3. In the **Filter** area, click to **Allow** the Social Network categories and any other categories you want to allow. Remember also to block certain default policies such as categories under the security group and those under Legal Liability.

4. In the **Apply Policy To** add "Top Management" group, "Marketing" group and specific users as separate records.

**NOTE**

Once you have saved this policy you will see that it is placed **above** the Leisure Browsing Policy. This ensures that when Marketing users browse for www.facebook.com they hit the Exclusions policy first (and are allowed). Users who are not defined in the Exclusions policy will trickle to the Leisure policy which would block them during work hours.




*Screenshot 6: Top down evaluation of rules will allow Social Websites to certain users since they will hit this rule first*

### 4.3.5 How to Create Bandwidth Controlling Policies

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. For this purpose, we suggest you create a Bandwidth Usage Policy and a Streaming Media Policy as described below.

### 4.3.6 Bandwidth Usage Policy

If you are concerned with bandwidth problems, we suggest you create a bandwidth usage policy to block categories which are potentially bandwidth-intensive.

Create a new Bandwidth Usage Policy based on another blocking policy (using the cloning functionality). In this policy, besides the current blocked categories, block also the following:

- Image and Video Search
- P2P
- Streaming Media

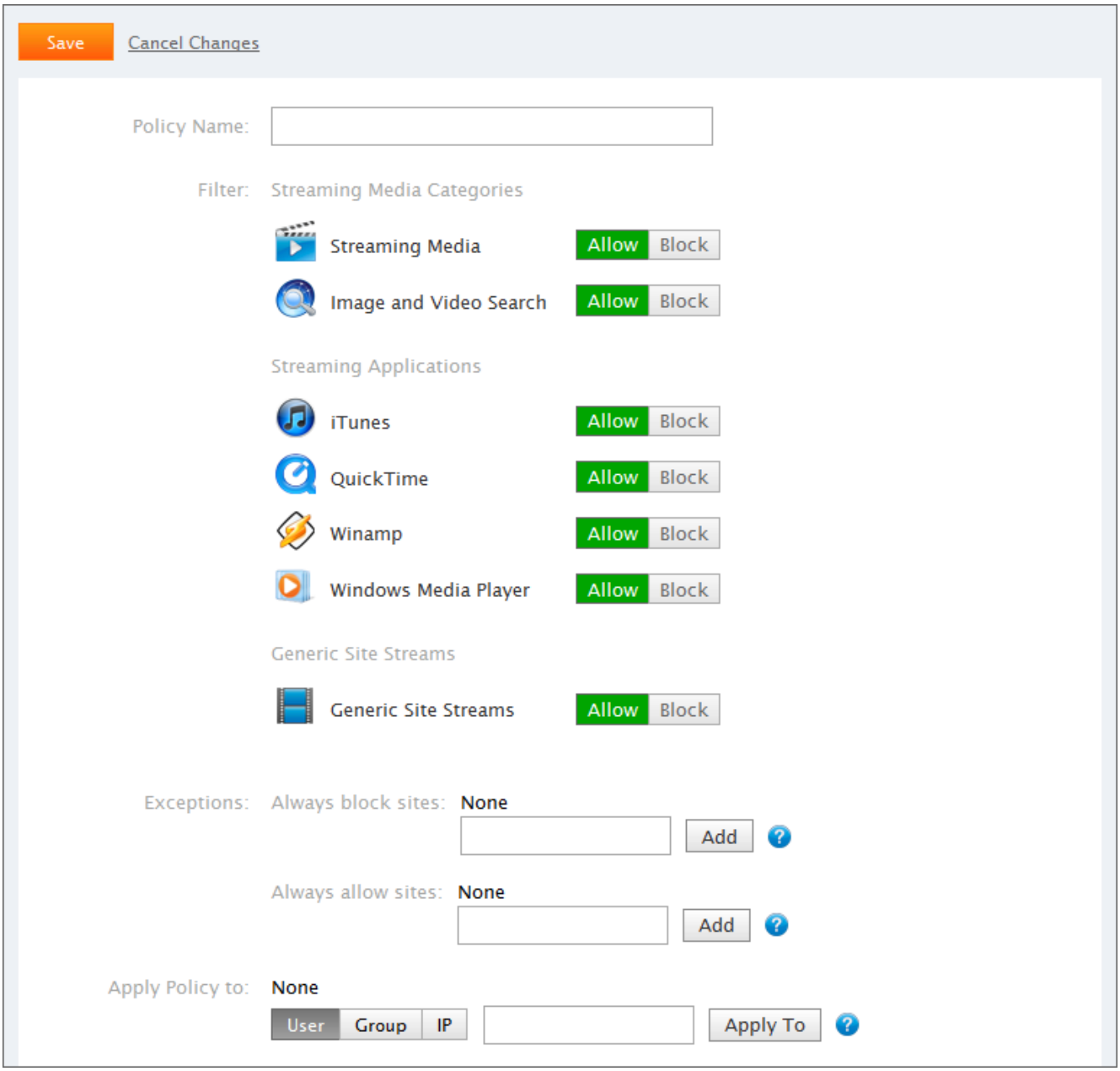
### 4.3.7 Streaming Media Policy

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.

The streaming media policy allows you to control this problem by creating policies that can be applied to specific users and based on different types of streaming media. The table below describes possible options:

*Table 2: Streaming media policy options*

| OPTION | DESCRIPTION |
|---|---|
| **Streaming Media Categories** | Block websites categorized as **Streaming Media** and **Image and Video Search** since these are by their very nature bandwidth intensive. |
| **Streaming Applications** | Block also streaming media coming over a number of applications such as **iTunes**, **QuickTime**, **Winamp** and **Windows Media Player** - this policy blocks the streams rather than the application itself. |
| **Generic Sites Streams** | The generic site streams block enables you to drop streams from websites without blocking the website itself. This enables you to block video and audio embedded within websites such as News and Sports websites. |




*Screenshot 7: Block website categories and applications considered bandwidth intensive*

### 4.3.8 How to Create a Web Browsing Threshold Policy

GFI WebMonitor enables you to create time and consumed bandwidth thresholds on a per user level. For example, you can create a policy that allows users to browse specific sites for only 10 minutes a day or download from specific sites not more than 100 MB.

### 4.3.9 Social network threshold policy

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 **Settings > Policies > Internet Policies > Web Browsing Quota Policies**.

2. Click **Add Policy** to create a new policy.

3. In the **Policy Name** field, enter **Social Networking Limit**.

4. In the **Limit By** area, select to limit by **Time** and put 10 minutes per day.

5. In the **Apply To**, add the category **Social Network**.

6. In the **Apply Policy To** field, add specific users known to be "Social Network" addicts.

> **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.

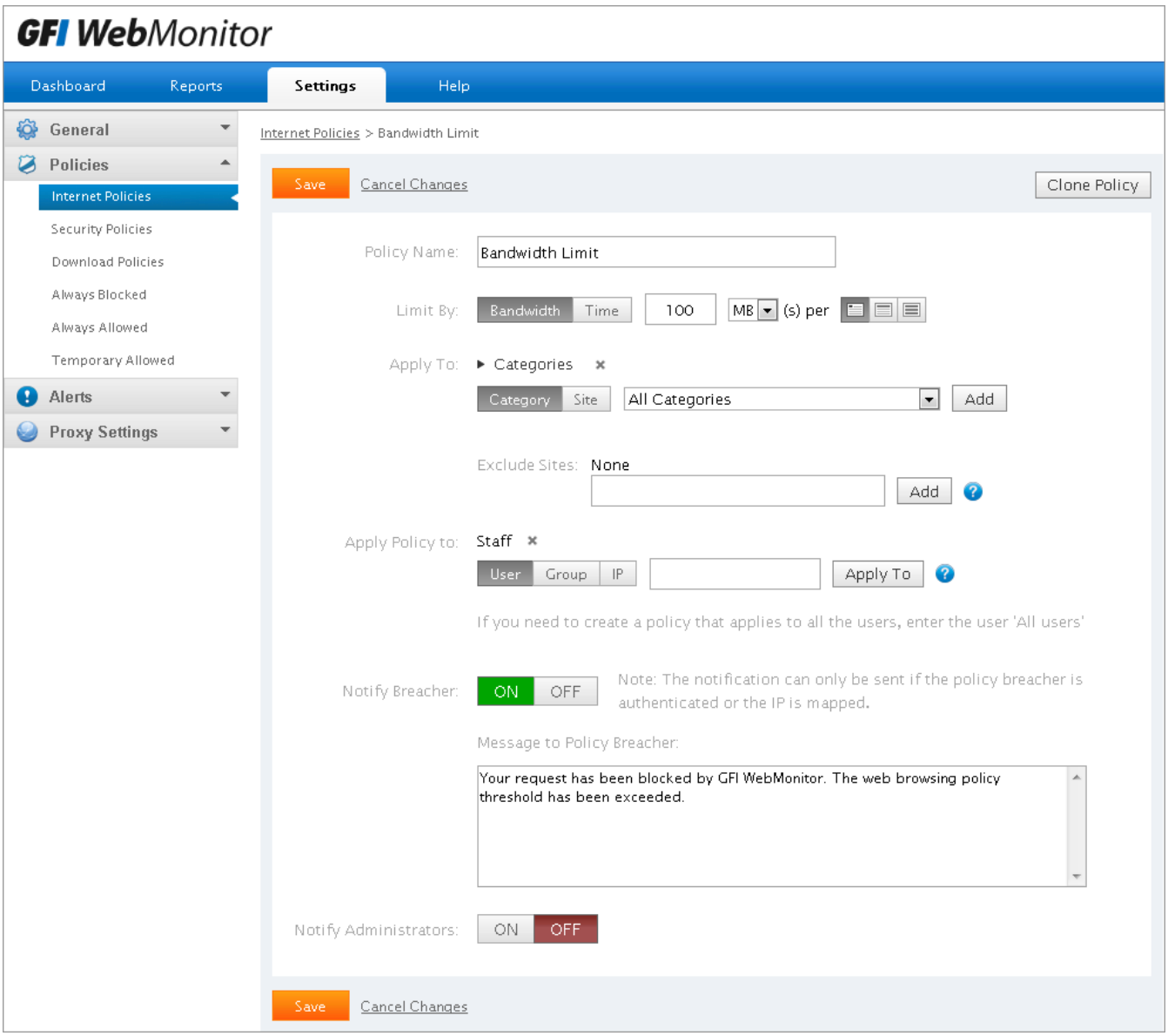
7. Click **Save**.

### 4.3.10 Bandwidth Usage Threshold Policy

You can also choose to limit Bandwidth intensive sites to a specific download value, for example, to 100 MB/day.

1. Go to **Settings > Policies > Internet Policies > Web Browsing Quota Policies**.

2. Click **Add Policy** to create a new policy.



*Screenshot 8: Creating a web browsing threshold policy*

3. In the **Policy Name** field, enter **Bandwidth Limit**.

4. In the **Limit By** area, select to limit by **Bandwidth** and put 100 MB per Day.

5. In the **Apply To** area, add the category **Image and Video Search** for YouTube and similar sites, and **Streaming Media**.

6. In the **Apply Policy To** field, add specific users known to be "Bandwidth Hogs".

## 4.4 Phase 4: Day 26+ - Analyze the Changes

Now that you have been using GFI WebMonitor and monitoring your organization's Internet usage for quite a few days, you have a good sample of data to analyze better.

Start by running a few reports again. Compare today's reports with the original set of reports and see what has changed. Have a look at the **Activity > Filtered Only Dashboard** to see who is hitting each policy you have in place. Identify users who tried to browse blocked websites or those who exceeded their threshold.

Export this information and send it to the stakeholders.

You should see that leisure surfing has gone down and all traffic to the sites you blocked will have stopped. You have also placed limits on the time people can spend on social media sites, so time spent there should have gone down significantly.

> **NOTE**
>
> Increase database performance by using SQL Server or SQL Server Express 2008 R2 as the logging database.

### 4.4.1 Internet Usage Policy

One of the most important actions you should take to ensure that Internet is used safely and adequately, is to develop a comprehensive **Internet Usage Policy**. This gives employees rules and guidelines about the appropriate use of company equipment, network and Internet access. Having such a policy in place helps protect both the business and the employee; the employee will be aware that browsing certain sites or downloading files is prohibited and that the policy must be adhered to, failing which there could be serious repercussions. For the business, this policy helps lower security risks related to employee negligence.

The most important part of this strategy is to ensure that your staff are aware of the policy and the reasons it is being put into place.

Staff who are aware of the threats posed by uncontrolled surfing will take more care and become proactive in maintaining this key layer of security.

# 5 GFI WebMonitor: Make a Positive Impact

Effective control of what users are doing across your Internet connection can have a huge positive impact on productivity and network security.

It is very easy and plausible for a user to spend an hour a day on leisure browsing. Consider the following scenario:

- Facebook including chat – five minutes, three times a day = 15 minutes
- Webmail including chat – 5 minutes; twice a day = 10 minutes
- News, local and International = 10 minutes
- Sports or entertainment = 10 minutes
- YouTube – two videos of 4 minutes = 8 minutes
- Twitter = 5 minutes.

Take your hourly pay as an average, multiply that by the number of employees in your company and multiply it by five (one hour per day per week). That is the cost saving this week if employees have just surfed for one hour a day! (See also the ROI section below!)

That excludes any time spent cleaning up infected PCs and the mess malware leaves behind them. It also excludes the potential cost of lawsuits which web browsing of objectionable or illicit material can expose you to, or any data leaks through socially engineered phishing attacks.

As staff get used to the new software, their surfing activities will revert to old ways unless you keep your web monitoring in place. With continued web monitoring, you can spend some time refining the policies you have in place until you find the right balance for your organization. And you can rest assured that infected downloads do not slip through.

## 5.1 Web monitoring ROI: It's easy to justify buying GFI WebMonitor

Take a look at our ROI Guide and use it to present a case to your management.

Misuse of Internet access continues to eat away at productivity at the work place. GFI WebMonitor can reclaim more than $185,000 worth of lost time a year for a 50-person company in which $15-an-hour employees spend just one hour a day in personal web surfing.

Companies report that Internet usage drops by up to 25% when software to monitor employee browsing habits is in place. Even a small company can lose tens of thousands of dollars in work time over the course of a year from cyberslacking.

The presence of pornography in the workplace is grounds for potentially expensive sexual harassment lawsuits. These can cost an average of $250,000 – excluding the cost of any negative PR which you might get.

At $18 per user, a 50-user company would spend only around $900 for web monitoring and filtering, and $1550 for comprehensive filtering monitoring and security.

# 6 Resources You May Need or Find Useful:

Installation Guide

Knowledge Base

Support

# 7 About GFI

GFI Software Ltd provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMBs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at http://www.gfi.com.

### USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104 Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

### UK AND REPUBLIC OF IRELAND

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

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

### EUROPE, MIDDLE EAST AND AFRICA

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

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

### AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com


GFI®