GFI Product Manual

GFI WebMonitor™

Evaluation Guide Part 1: Quick Install

Document Version: 2.1.0

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

Contents

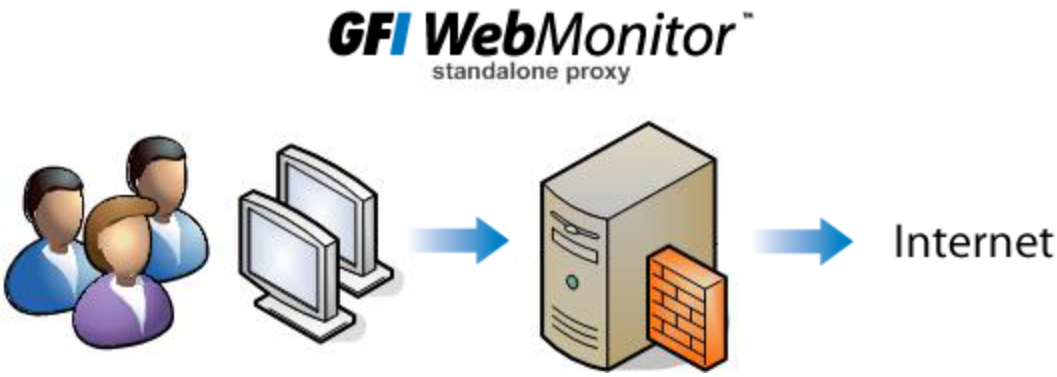
1 Introduction

Welcome to GFI WebMonitor- a solution designed to give you complete and real time control over user Internet browsing, ensuring that downloaded files or visited websites are free from viruses, malware or other security threats.

GFI WebMonitor gives you full visibility into user online activity, enabling you to discover how much bandwidth they are consuming and what websites they have been browsing and for how long.

This document helps you install your trial version of GFI WebMonitor. It is aimed to get you started with your trial so that you can test the software, but if you require more advanced information, you can download the full manual from our website.

To keep your life simple during the trial, we recommend you trial the software on a machine configured as a standalone proxy in a test environment. This ensures no issues are created on your live environment.



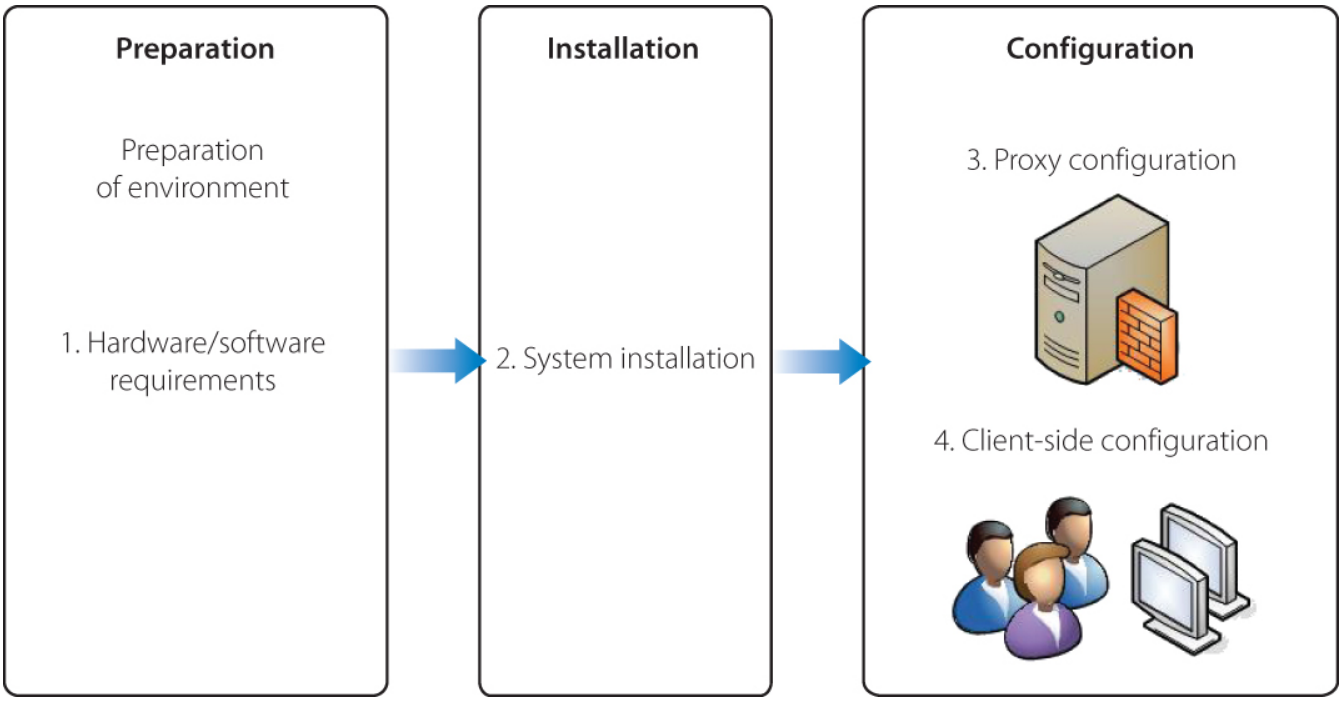
IMPORTANT

Before you begin, ensure that:

- **Your test environment has unrestricted Internet access**
- **You can route user traffic through your test server - without any real user traffic, you would not be able to appreciate the benefits of GFI WebMonitor.**

We will take you through the whole GFI WebMonitor trial setup including:

1. **System requirements**
2. **System installation**
3. **Proxy configuration**
4. **Client side configuration**



If at any time you require any help, please contact our support team.

2 Installation

Installing GFI WebMonitor is a two-step process:

1. Run the GFI WebMonitor installer to install GFI WebMonitor and missing pre-requisites.

2. Follow the GFI WebMonitor post-install wizard to configure GFI WebMonitor and its operating environment.

2.1 System Requirements

2.1.1 Software

TYPE	SOFTWARE REQUIREMENTS (x86 and x64)
Supported Operating Systems	» Windows® Server 2003 SP 2 » Windows® Server 2008 » Windows® Server 2008 R2 » Windows® XP SP3 » Windows® Vista SP2 » Windows® 7 » Windows® 8
Gateway and Simple Proxy Environments - Other required components	» Internet Explorer® 8 or later » Microsoft.NET® Framework 4.0 » Microsoft® Message Queuing Service (MSMQ) » IIS® Express » SQL Server® Express 2005 or later » SQL Server® 2005 or later (for reporting purposes)
Gateway Environment - Other required components	» Routing and Remote Access configuration on Windows® Server 2003/2008
GFI WebMonitor Agent	» Windows® Vista SP2 or later

2.1.2 Hardware

Minimum hardware requirements depend on the GFI WebMonitor edition.

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

IMPORTANT

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

NOTE

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

2.2 System Prerequisites

Before installing GFI WebMonitor on your test proxy server, ensure that:

» The machine you are using has unrestricted Internet access

» The listening port (default = 8080) is not blocked by your firewall. Follow the link to find more information on how to enable firewall ports on Microsoft Windows Firewall.

» You have administrative privileges on the test machine.

NOTE

GFI WebMonitor starts a number of filtering and monitoring engines soon after the installation. This is quite a heavy operation, which can affect performance and cause high CPU usage whilst GFI WebMonitor is started.

It is advisable that if this server is being used for other services, installation is done during an off-peak period. GFI WebMonitor also performs a large volume of updates after installation, we thus suggest you install GFI WebMonitor and leave it overnight to download its updates.

2.3 Installing GFI WebMonitor in Simple Proxy Mode

Installing GFI WebMonitor is easy. The steps below guide you through the process.

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

1. Double click the GFI WebMonitor executable file.

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

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

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

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

NOTE

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

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

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

NOTE

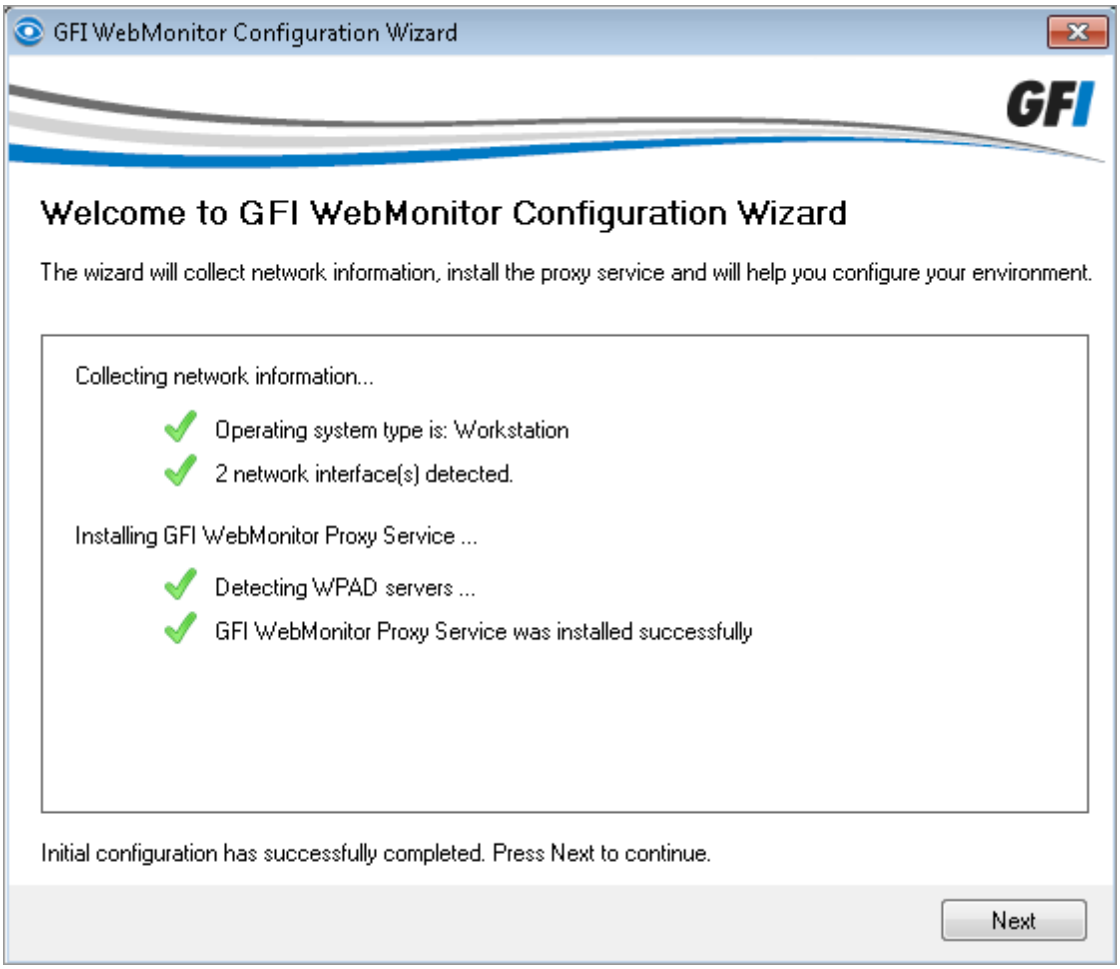
You can choose to leave SMTP settings empty and set them later, but you will not be able to receive notifications until you set them.

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

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

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

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

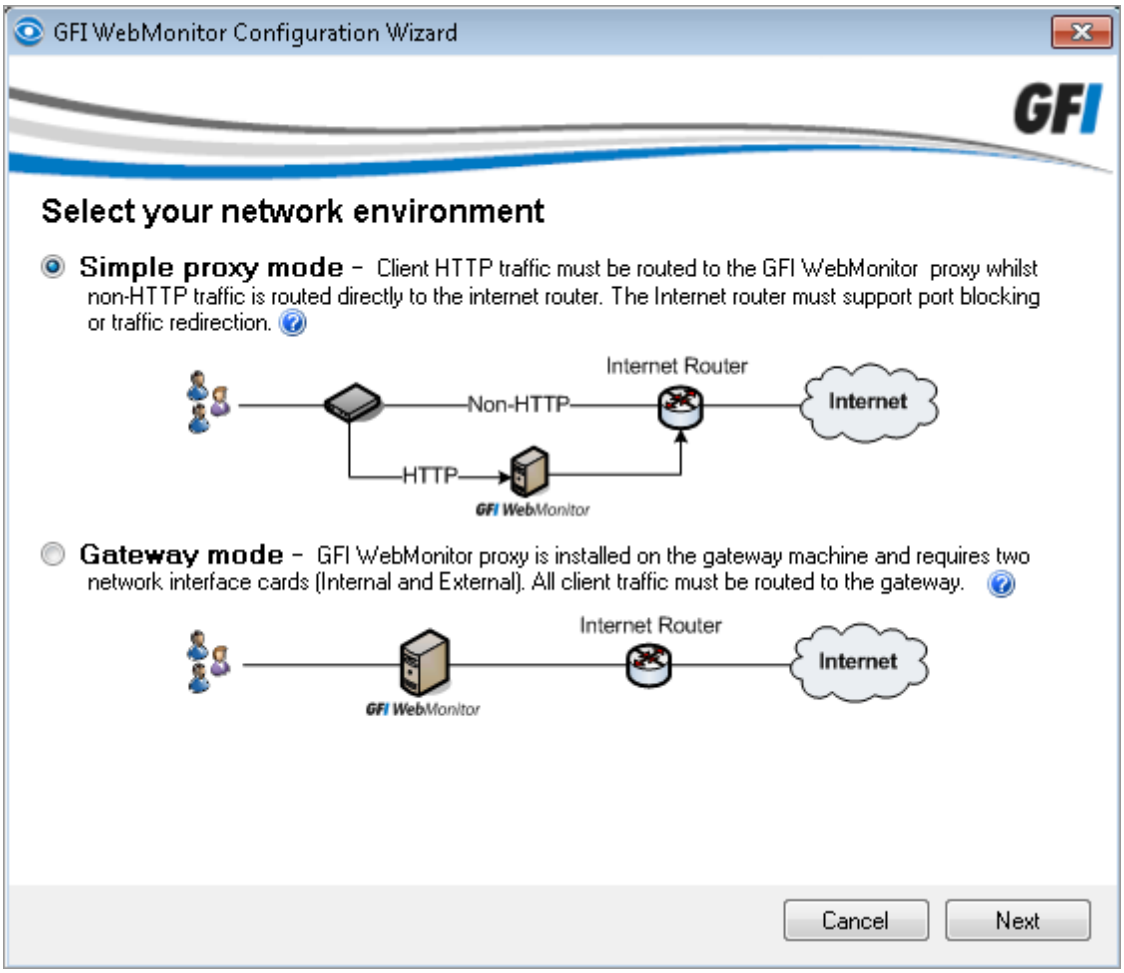


Screenshot 1: GFI WebMonitor Configuration Wizard welcome screen

NOTE

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

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



Screenshot 2: GFI WebMonitor Configuration Wizard - Simple proxy mode

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

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

> **NOTE**
>
> Expect a temporary decline in performance and high CPU usage while all GFI WebMonitor engines are started and updated. This might take a few minutes and the computer might feel sluggish until this operation is completed. Please allow the CPU usage to come back to normal before continuing, to ensure a smooth usage experience.
>
> Also ensure that all GFI WebMonitor services have started successfully in the Services panel (**Administrative Tools > Services >** Scroll to GFI). If any services have not started, start them manually before you proceed to the next phase.

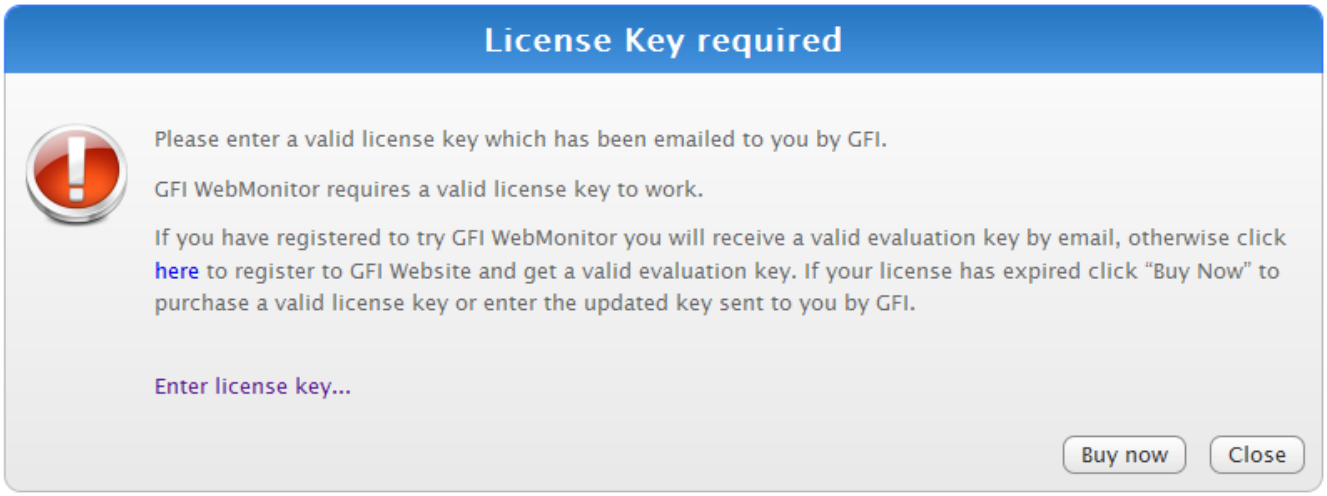
2.4 Post-installation Tasks

2.4.1 Test Your Installation

To verify installation completed successfully, open the GFI WebMonitor interface from the machine where GFI WebMonitor was installed:

1. Click **Start > Programs > GFI WebMonitor > GFI WebMonitor - Management Console**.

You should now see the following message:



You simply need to enter the evaluation license key you received by email. If you did not receive it, register to receive your evaluation key. Click **here** to access the licensing page.

1. Click **Enter license key...**

2. Enter the license key and click **Save Settings**.

Your trial period starts now!

> **NOTE**
>
> You should wait until GFI WebMonitor downloads the latest version of the WebGrade database, and other updates, such as latest antivirus engine signatures. Ideally you should leave GFI WebMonitor running overnight or until all downloads have completed.

At this point you should already start seeing some traffic generated by the updates in the **Dashboard > Real-Time Activity > Active Connections** or **Bandwidth**.

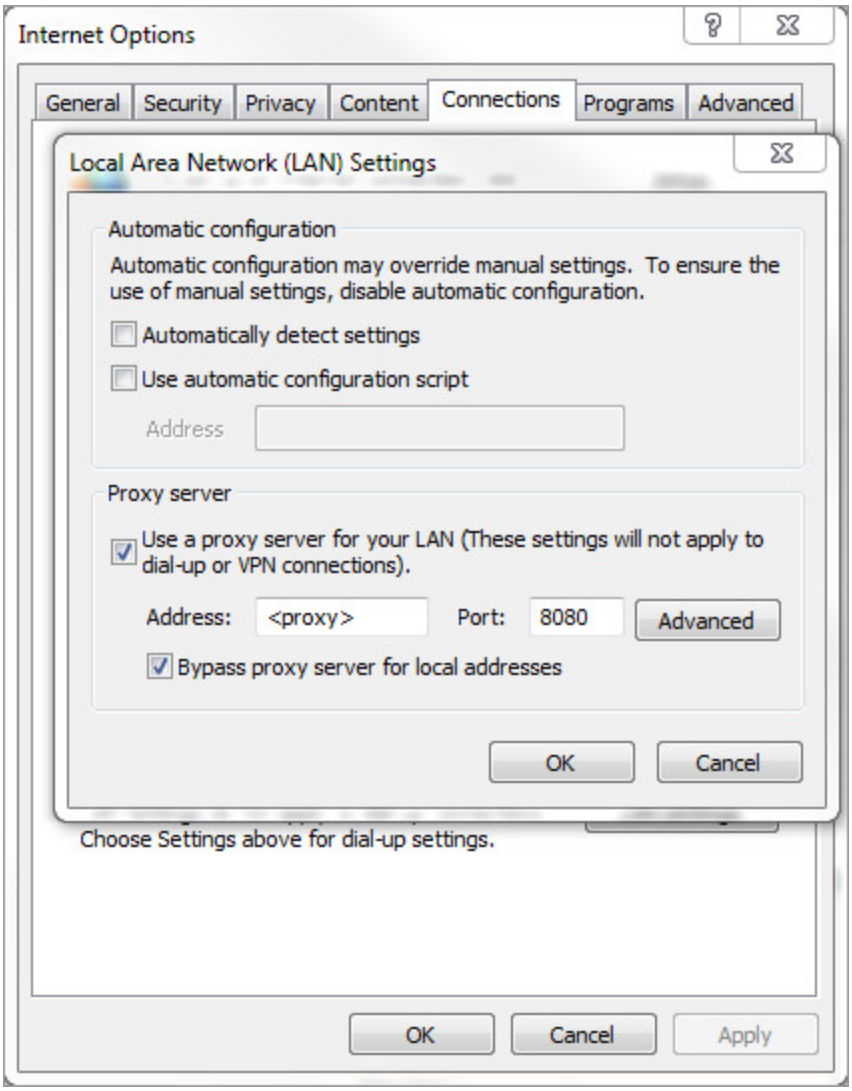
Go through the following sections to set up proxy settings in Internet Explorer to route web traffic through the test environment so that you can try some configurations.

2.4.2 Configure Browser Proxy Settings on GFI WebMonitor Machine

Configure Internet Explorer to use GFI WebMonitor machine as the default proxy. This can be achieved by performing the following:

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

2. Click **LAN settings**.



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

4. In the **Address** field, key in the proxy server name or IP address of the GFI WebMonitor machine.

5. In the **Port** field enter the port used (default = 8080).

NOTE

GFI WebMonitor can be deployed to allow Internet browsers on client machines to automatically detect proxy server configuration settings. This can be achieved by using Web Proxy Auto Discovery (WPAD). Refer to Appendix I for more information on how to do this.

2.4.3 Configure Client Web Browsers

It is now time to set up a few testing users. On every client machine, set up browser proxy settings so that Internet traffic is redirected through the GFI WebMonitor proxy. Once again, simply go to the Browser settings of the client machines and set the IP of GFI WebMonitor.

NOTE

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.

Internet Explorer

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

Mozilla Firefox

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

Google Chrome

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

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

> **NOTE**
>
> After evaluating GFI WebMonitor, you can set the proxy settings of every user to pass through GFI WebMonitor using Active Directory GPO or by enabling Web Proxy Auto Discovery (WPAD). For more information, refer to Appendix I - Enabling GFI WebMonitor without Fixed Proxy Settings (page 27).

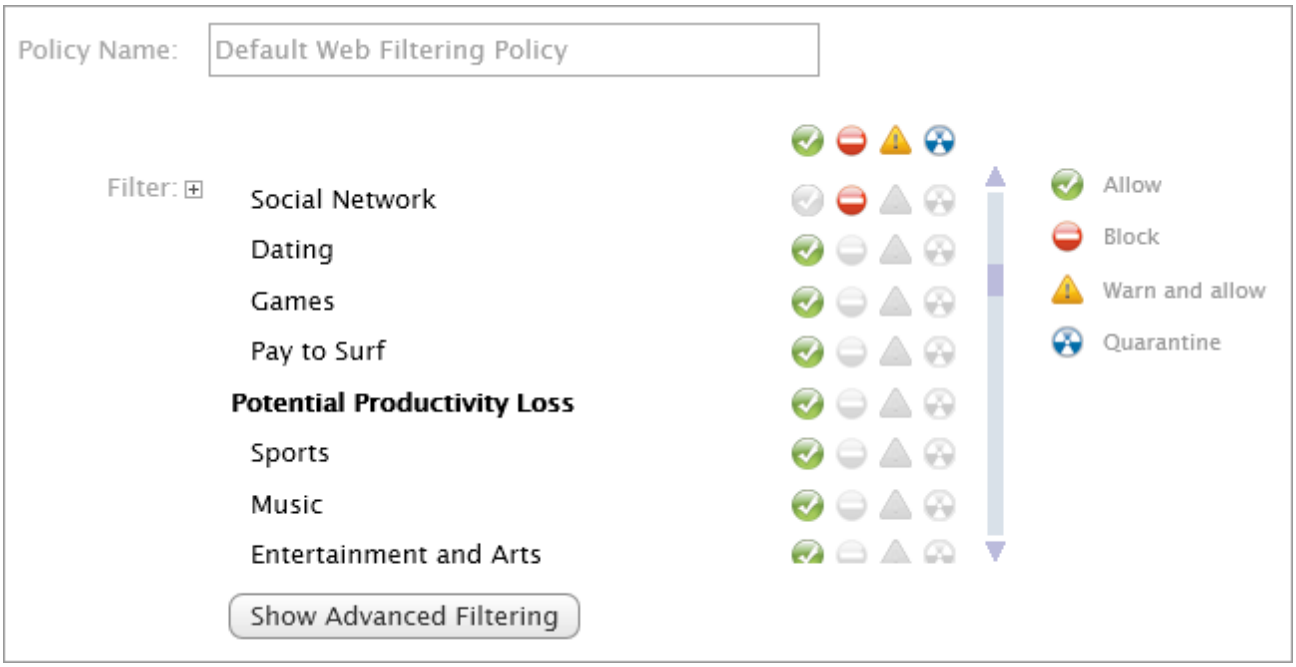
2.5 Verify that GFI WebMonitor is Working Correctly

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 **Settings > Policies > Internet Policies**.

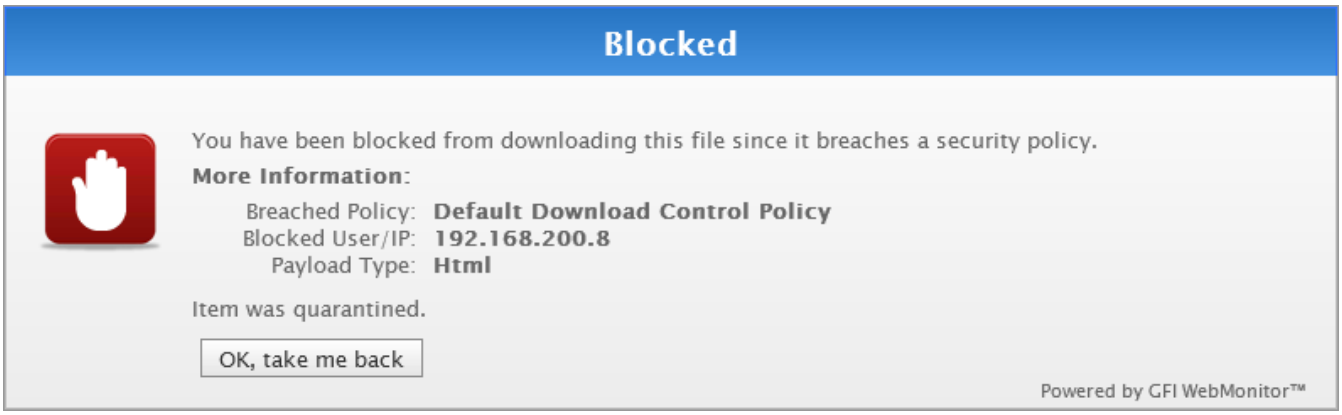
> **NOTE**
>
> You will see that a Default Web Filtering Policy is already enabled. This policy applies to every user whose traffic is routed through GFI WebMonitor.

2. Click on **Default Web Filtering Policy**.
3. In the **Filter** area, scroll down through the categories until you find **Productivity Loss**.



Screenshot 3: Blocking Social Network in the Default Web Filtering Policy

4. Next to Social Networks, click  to block social networking websites (for our blocking test).
5. Click **Save** to apply the changes.
6. Go back to your browser and open http://www.facebook.com. The GFI WebMonitor blocking page should now be displayed.



Screenshot 4: 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 disable the Social Networks block by redoing the previous steps but clicking **Allow** instead of **Block** and then, **Save**.

IMPORTANT

At this point GFI WebMonitor has been installed in 'bare essentials' mode. We recommend you follow the rest of this guide to ensure all essential configurations are in place.

3 Configuring GFI WebMonitor for Trial

This section guides you through the configuration of monitoring and controlling polices that enable GFI WebMonitor to do the job it was designed to do. For more detailed information on how to configure advanced settings refer to the Administrator Guide available from our website.

3.1 Default Policies

When GFI WebMonitor is installed, a number of pre-configured policies are automatically created to ensure an initial working setup. These are called **Default** policies and apply to every user whose traffic is routed through GFI WebMonitor. If you intend to apply the same policy to everyone, you can edit the default policies according to your organization's requirements, otherwise you can create new policies and apply them to specific Active Directory users, groups or IPs as necessary.

IMPORTANT

Policies in the same node are applied in a top-down approach. Every new policy is displayed on top of the older ones in a numbered sequence.

3.2 Authentication

If you would like to set policies using Windows or Active Directory users and groups you need to enable authentication.

During installation, the GFI WebMonitor Proxy Authentication is set to **No Authentication**. This means that:

» Only IP addresses of machines whose Internet traffic is being routed through GFI WebMonitor will be reported.

» Policies need to be applied by IP address. If you have joined your test server to your Active Directory domain and would like to see usernames and be able to set policies by Active Directory users and groups, you will need to set GFI WebMonitor to use authentication.

GFI WebMonitorcan be configured to authenticate users using one of two methods:

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

The next section describes how to enable Authentication in GFI WebMonitor.

3.2.1 Configuring Proxy Authentication Method

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

To configure user authentication method:

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

2. From the **Proxy Authentication** area, leave Proxy Authentication off if the user is not required to provide login credentials when new Internet sessions are launched.

3. If proxy authentication is required, select one of the following options:

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

NOTE

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

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

NOTE

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

5. Click **Save**.

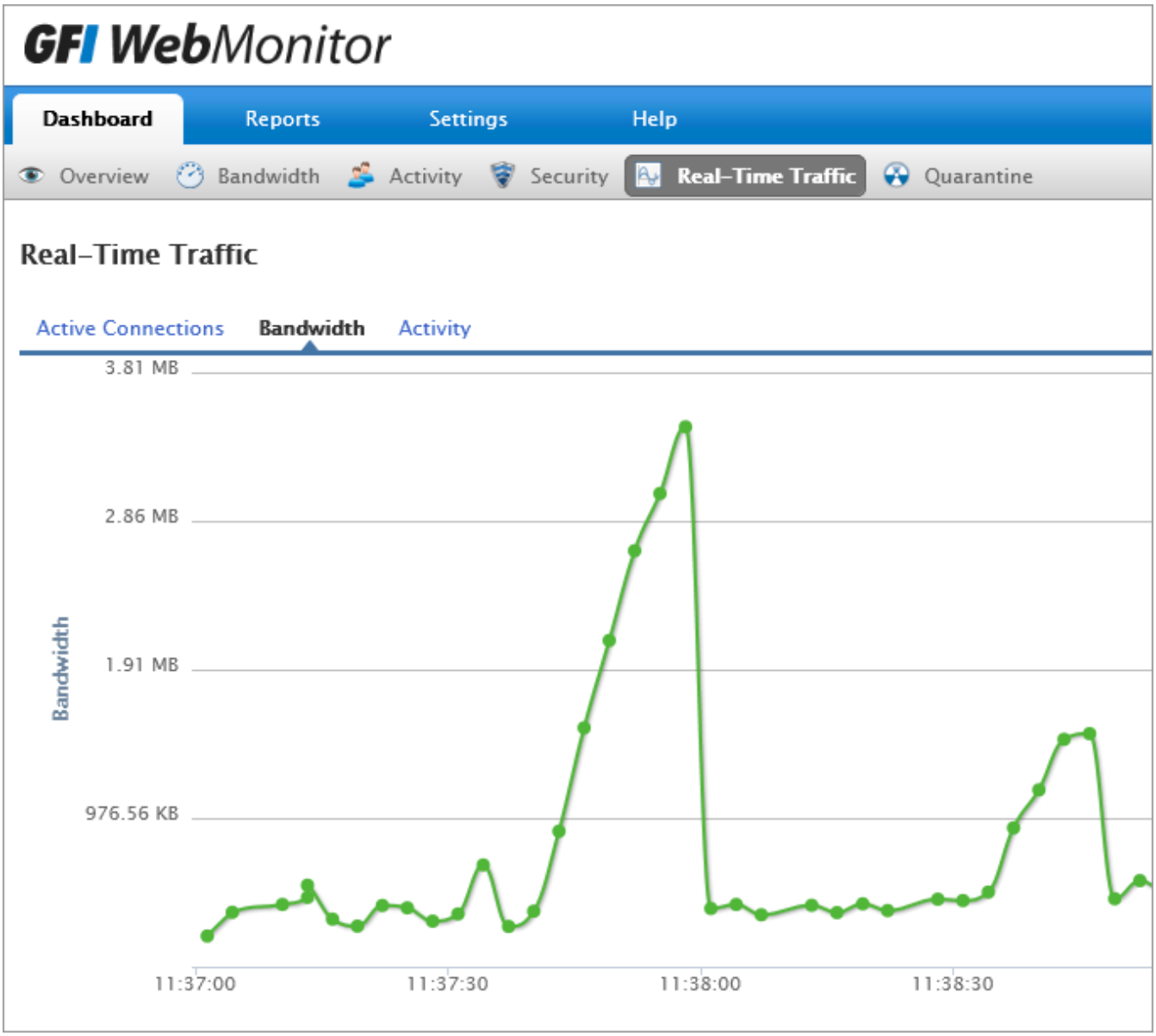
3.2.2 Authentication Test (in Real-Time)

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 **Dashboard > 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.



Screenshot 5: Real-Time Traffic Bandwidth graph

3.2.3 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 **Settings > Policies > Internet Policies**.

2. In **Policy Name** field, enter **Authentication Test**.

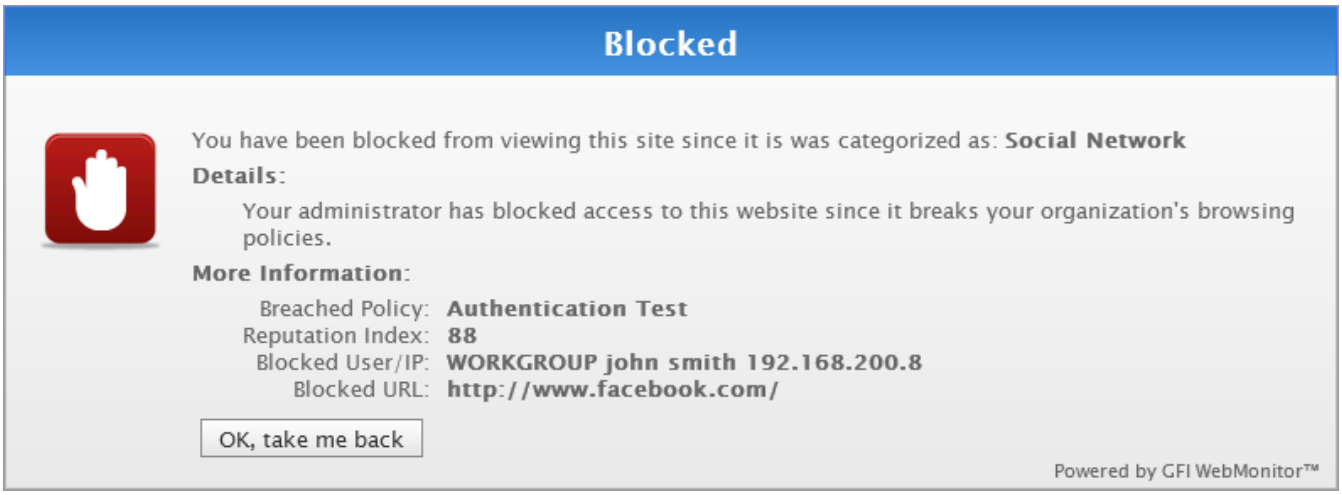
3. In the **Filter** area, scroll down through the categories until you find **Productivity Loss**.

4. Next to Social Networks, click  to block social networking websites (for blocking test purposes).

5. Scroll to the **Apply Policy To**, and add the user you are currently logged in as (username which showed up in the past connections) . As soon as you start typing the username should show up, and you can select this user and click the **Apply To** button.

6. Click **Save** to apply the changes.

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



Screenshot 6: Warning that the page you requested was blocked by GFI WebMonitor

If the warning above is displayed, then GFI WebMonitoris working correctly!

If the block did not work, make sure you have entered all details correctly, especially the username, and that you have saved changes to the policy. Try closing and re-opening the browser, and check the **Replace Monitoring > Past Connections with Real-Time Traffic** 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.

3.3 Download Control Policies

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

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

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

To view configured download policies or create a new one, go to **GFI WebMonitor > Settings > Policies > Download Policies**.

3.4 Virus Scanning Policies

A default security policy is enabled when GFI WebMonitor is installed. It is pre-configured to apply to every user on the domain and to scan all file types using the inbuilt BitDefender, VIPRE and Kaspersky engines. This policy is called **Default Virus Scanning Policy**, and can be edited, but not disabled or deleted.

To view or edit the **Default Virus Scanning Policy** go to **Settings > Policies > Security Policies**. You can customize the **Default Virus Scanning Policy** as necessary; however, the initial setup should suffice for the trial period.

3.5 IM and Social Control Policies

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

A Default IM and Social Control policy is enabled when GFI WebMonitor is installed. It is pre-configured to allow access to all instant messaging clients and social networking services to all users on your network. For your trial this is typically sufficient, but if you wish to create a new policy or edit the default policy, you can do this from: **Settings > Internet Policies > Instant Messaging Policies**.

NOTE

The default policy can be edited, but cannot be disabled or deleted. Any changes made to the default policy apply to all users.

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

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

Social Controls, grant or deny access to the following:

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

3.6 Web Browsing Policies

Web Browsing policies is where you can define policies aimed at limiting user browsing. These are based on quotas for surf time or by bandwidth. No policies are created here by default, so you can choose to create your own.

Create a new Web Browsing Quota Policy from **Settings > Internet Policies > Web Browsing Quota Policies**.

3.7 Configuring Exceptions

The **Always Allowed** and **Always Blocked** policies can be used to configure exceptions.

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

Temporary Allowed list, there is also a **Temporary Allowed** list that is used to temporarily approve access to a site for a user or IP address.

IMPORTANT

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

Pre-configured Items

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

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

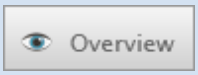
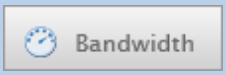
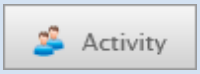
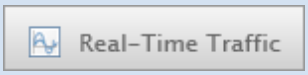
NOTE

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

4 Using GFI WebMonitor

4.1 Using the Dashboards

GFI WebMonitor contains 6 dashboards that provide essential information such as:

DASHBOARD	DESCRIPTION
	Get a quick overview of bandwidth and activity trends, as well as reminders for tasks that need to be addressed to make your network safer. Identify **Top Categories**, **Domains** and **Users** on your network at a glance and be aware of several statuses related to web browsing and security issues identified by GFI WebMonitor.
	Access information related to traffic and user activity that affects bandwidth consumption. The information is presented in a graph that shows upload and download bandwidth viewed by hour, day, week or month to monitor any spikes. The legend is filtered by category, website and users, sorted by the different columns, with search functionality for specific items in the filter. This allows you to easily arrive to relevant information and analyze data as required.
	View web requests and user activity for a specified period. The Activity graph displays **All Activity** in green and **Filtered** traffic in red for easy identification. The summary at the top identifies the total web requests for the selected period, the number of monitored users, the day within that period when traffic was most intensive and also gives the projected web requests for the next 30 days.
	Identify security risks and threats to your network environment. Focusing on the various facets of Internet security, the dashboard offers quick information related to detection of Infected Files, Malicious and Phishing sites that have been blocked and the top viruses that GFI WebMonitor has identified.
	Monitor current active connections and terminate them if necessary (for example, streaming media or large unauthorized downloads), and view most recent connections. Filter real-time connections by Category, Website or User to see what is going on. For example, you could filter Streaming Media when too much bandwidth is being consumed and terminate at will. Real-time graphs of bandwidth and activity give you visual indicators of the current situation while it happens. In this way, you can keep your eye on the situation from the perspective which most affects you.
	This area holds content filtered by active policies until you review each item and decide whether to allow or discard the request.

4.2 Interactive Reporting

You can now take a brief look at the reporting feature of GFI WebMonitor. Reports can either be triggered directly from within the **Bandwidth**, **Activity** and **Security Dashboards** or accessed from the **Reports** tab of the UI.

For the purpose of this trial, let us have a look at the report functionality from within the Activity Dashboard.

> **NOTE**
>
> At this point of your trial, there is very little data available for reporting. The reports will be more useful once a number of days have passed with your trial.

Go to **Dashboard > Activity**. The Dashboard consists of a graph displaying a representation of activity on your network. Use the various controls to extract the information you require. For example, click **Filtered Only** to view user browsing grouped by policy. The graph changes according to your selection. From the bottom section, drill down further by clicking on specific categories, websites or users.

4.2.1 One-click Report Functionality

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

Export Report

To export the report:

1. From the top of the Dashboard, click 

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

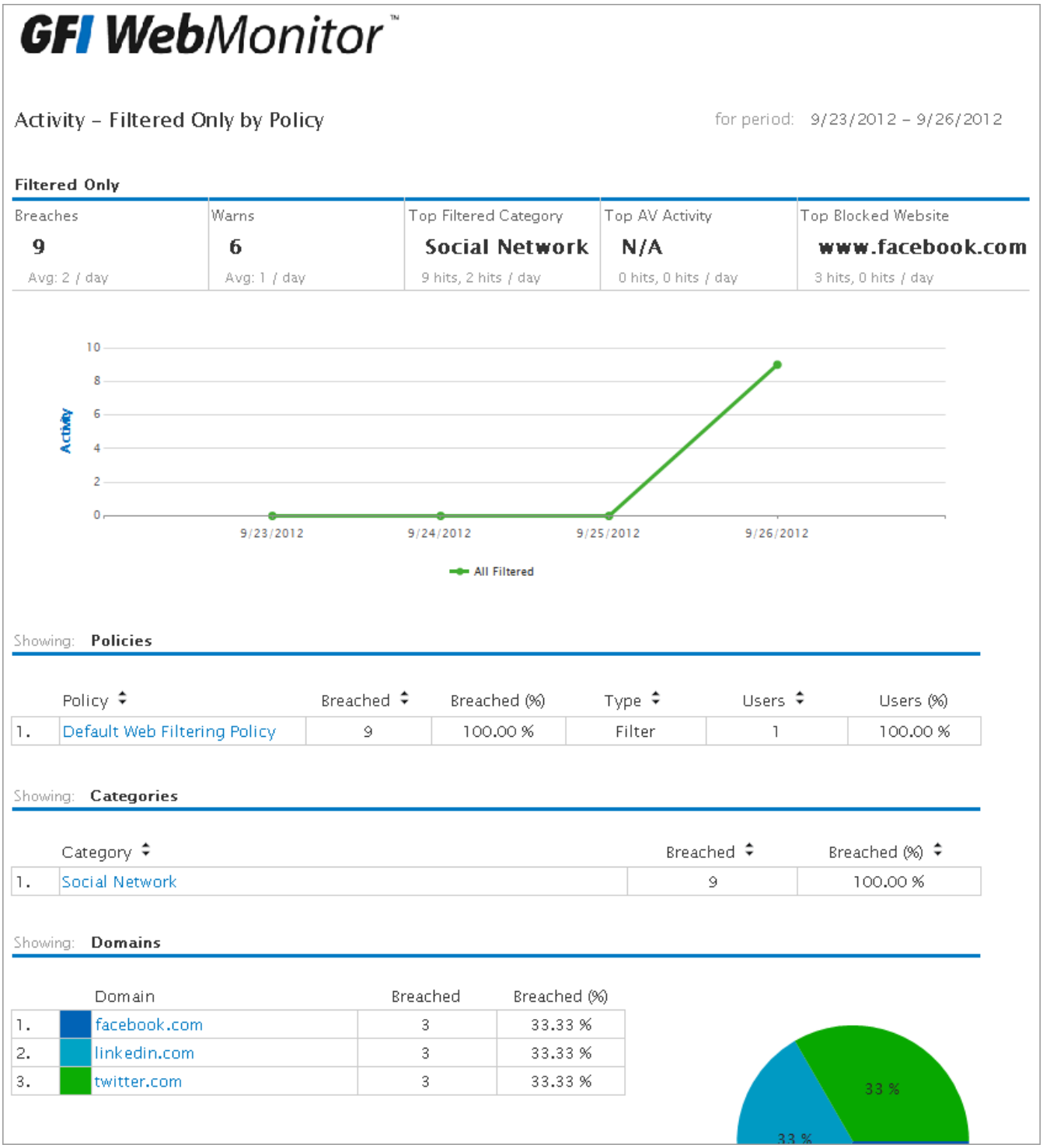
OPTION	DESCRIPTION
Excel	The report is exported in Microsoft Excel format (.xls)
PDF	The report is exported in PDF format.
Word	The report is exported in Microsoft Word format (.doc)

Schedule Report

To schedule the report:

1. From the top of the Dashboard, click 

and select **Schedule Report**.
2. GFI WebMonitor redirects you automatically to the **Reports** area.
3. Edit the report as required.
4. Save the report.



Screenshot 7: Exported Activity Report showing filtered browsing

The exported report can be viewed in your browser. The top part of the report consists of a graph showing a graphical representation of trends, while the bottom part can be used to drill-down on specific categories, domains, websites or users.

5 Support

Remember that support is available during your GFI WebMonitor trial. If you have any problems during the above steps, you can get in touch with our support center.

Evaluation Guide Part 2: Thirty Day Trial

Now that you've successfully setup GFI WebMonitor, we suggest you take a look at the Evaluation Guide Part 2: Thirty Day Trial. Here we will take you through some recommendations for evaluating GFI WebMonitor in order to get the most value out of your GFI WebMonitor trial.

6 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.

7 Appendix I - Enabling GFI WebMonitor without Fixed Proxy Settings

To avoid problems caused by fixed proxy settings on roaming computers (such as laptops), set up WPAD within GFI WebMonitor. WPAD allows client computers to automatically detect proxy server configuration settings.

7.1 About WPAD

WPAD, or Web Proxy Auto-Discovery Protocol, 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. This works with Microsoft Internet Explorer, Google™ Chrome, and Mozilla FireFox browsers.

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.

7.1.1 Configuring WPAD

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

To enable WPAD:

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

Screenshot 8: Configuring WPAD

2. In the **Use WPAD** field, click **ON** to enable.

3. Select one of the following options:

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

4. Click **Save**.

7.1.2 Configure Microsoft Internet Explorer for WPAD

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

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

> **NOTE**
>
> WPAD is supported by all major Internet browsers.

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®