



# **GFI WebMonitor**<sup>™</sup>

*Web security, monitoring and Internet access control*

## *Trial: Installation Guide*

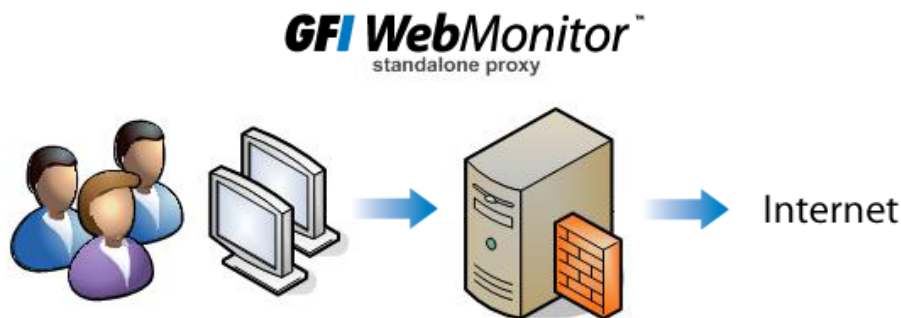
The following is a guide for installing and configuring GFI WebMonitor<sup>™</sup> for your trial period. In this document, we highlight the steps to successfully configure GFI WebMonitor.

## Introduction

Welcome to GFI WebMonitor - This solution gives you complete control, in real time, to monitor what users are browsing on the Internet and/or to ensure that any files they download or websites they visit are free of viruses and other malware. This installation document will help you install your trial version of GFI WebMonitor. This guide is not a full-blown manual – it is only meant to get you started with your trial so that you can test the software. You can download the full manual [here](#) as well as the [GFI WebMonitor – Getting Started Guide](#).

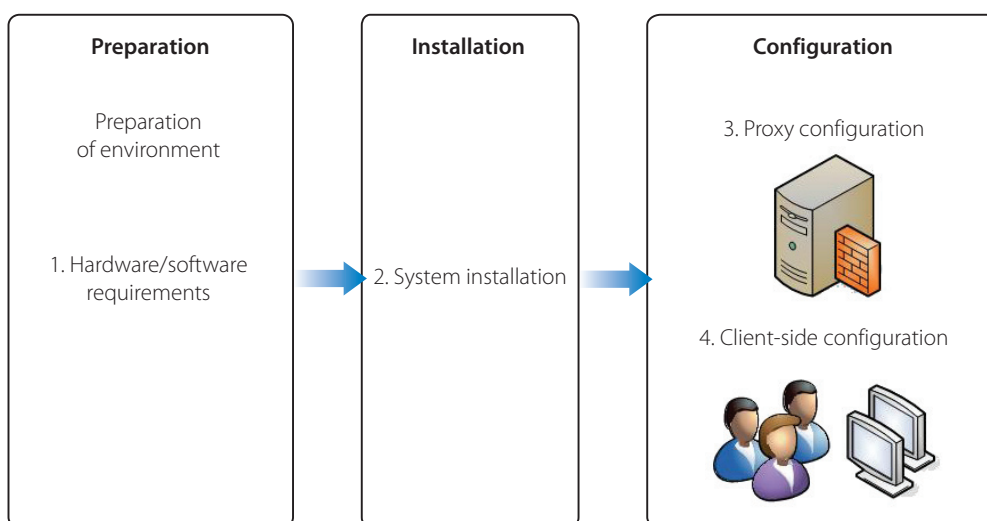
To keep your life simple during the trial, we recommend you trial the software as a standalone proxy on a test environment. This ensures no issues are created on your live environment – however, make sure that you can proxy user traffic through this test server – without any real user traffic, you are not going to appreciate the benefits of GFI WebMonitor.

Make sure that your proxy server test environment has unrestricted Internet access.



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

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



If at any time you require any help, please [contact our support team](#).

## System installation requirements

Below are minimum requirements to use and install GFI WebMonitor Unified Protection Edition which includes all functionality of GFI WebMonitor. We recommend the following hardware requirements.

### Minimum hardware requirements

Processor	RAM	Hard Disk
2.0 GHz	2+ GB	4+ GB of available disk space

### Recommended hardware requirements

Processor	RAM	Hard Disk
2.0+ GHz	4+ GB	10+ GB of available disk space

### Minimum software requirements

Supported Operating Systems	Other Required / Recommended Components
Microsoft Windows Server 2003	Microsoft Internet Explorer 7 or later
Microsoft Windows Server 2008	Microsoft.NET framework 2.0
Microsoft Windows 7	Microsoft SQL Server 2000 or later (for Report Pack)
Microsoft Windows Vista	
Microsoft Windows XP SP2	

## System installation

### Pre-requisites

Before installing GFI WebMonitor on your test proxy server, make sure the machine you are using has unrestricted Internet access.

Ensure that the listening port (default 8080) is not blocked by your firewall. You can find more information on [how to enable firewall ports on Microsoft Windows Firewall](#).

NB: GFI WebMonitor starts a number of filtering and monitoring engines soon after the installation. This is quite a heavy operation, and expect a performance hit and high CPU usage whilst GFI WebMonitor is started.

It is advisable that if this server is being used for other services, that the installation is done during an off-peak period.

### Installation procedure

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

1. Double click the GFI WebMonitor executable file.
2. Choose whether you want the installation wizard to search for a newer build of GFI WebMonitor on the GFI website (it is recommended that you should always install the latest build).
3. Read the licensing agreement and proceed with the installation.
4. GFI WebMonitor is used through the browser via a web interface. The screen below grants access to the user interface to the named IPs or usernames.

Key in the username or the IP address that will be used to access the web interface of GFI WebMonitor. Typically these would be the IT administrators. Essentially since you are trialling WebMonitor you should put in only the IPs of the machine where GFI WebMonitor is being installed.

**NB:** You don't need to enter IPs of users who will be proxied through GFI WebMonitor, only those of IPs who will be configuring GFI WebMonitor.



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



6. (Optional) Provide the SMTP mail server details and email address to which administrator notifications will be sent. Select **Verify Mail Settings** to send a test email. Click **Next**. You can choose to leave these empty and set them later but you won't be able to receive notification until you set them.
7. If the Microsoft Message Queuing Service (MSMQ) is not installed, a message will prompt the user that the installation requirements have not been met. Click **Next** to install the service automatically.
8. Click **Install** to start the installation and wait for the installation to complete.

## Proxy configuration

### Post installation wizard

1. After the installation, **GFI WebMonitor Configuration Wizard** is launched automatically. This will help you configure the server in simple proxy mode.
2. Select **Simple proxy mode** as your network environment and click **Next**.
3. Click **Finish** to apply proxy settings.

NB: Expect a temporary performance hit and high CPU usage whilst all GFI WebMonitor engines are started and updated - this might take a few minutes and the computer might feel sluggish whilst this operation completes. 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 (Administrative Tools > Services > Scroll to GFI) have started successfully in the Services panel. If any services have not started, start them manually before you proceed to the next phase.

### Initial Configuration

#### Post-installation test

To see the GFI WebMonitor interface from the machine where GFI WebMonitor was installed:

Click **Start > Programs > GFI WebMonitor > GFI WebMonitor**.

Do not be alarmed! You will now see:



You simply need to enter the evaluation license key which you received by email. If you did not receive it, please [register](#) and get your evaluation key.

Click on the "[click here](#)", which will take you to the licensing page. Enter the license key and click **Save Settings**. Your trial period starts now!



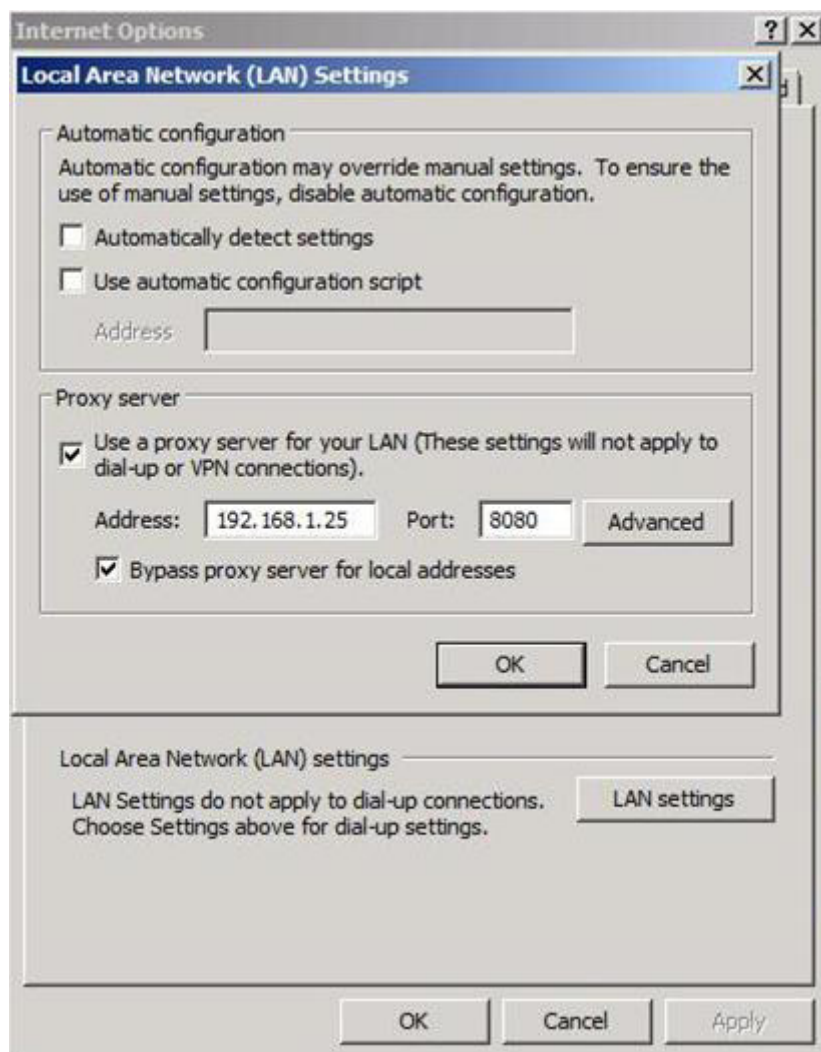
At this point you should wait until GFI WebMonitor downloads the latest version of the WebGrade database, and other updates such as latest antivirus engine signatures. You should already start seeing some traffic for the updates in the **Monitoring > Active Connections** or **Monitoring > Past connections**.

Set up the proxy settings on Internet Explorer to route web traffic through the test environment so that you can try some configurations of GFI WebMonitor as per below.

### *Post-installation actions: Configure proxy settings*

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** button.



3. Check **Use a proxy server for your LAN** checkbox.
4. Key in the proxy server name or IP address of the GFI WebMonitor machine and the port used (default 8080) in the **Address** and **Port** text boxes.

## Blocking test

One of your first actions to determine that GFI WebMonitor is working correctly would be to check whether it is blocking pages.

Click **GFI WebMonitor > WebFilter Edition > Web Filtering Policies**

You can see that a Default Web Filtering Policy has been created which **Applies to everyone**. Click on Default Web Filtering Policy, click on the Web Filtering tab, scroll down the categories and click the **X (Block)** icon on Search Engines to block search engines (temporarily until we test). Click on Save Settings to apply the changes.

Go back to your browser and browse to <http://www.google.com>. The GFI WebMonitor blocking page should now be displayed. If it does, then your GFI WebMonitor installation is working correctly!



You should now disable the Search Engines block by redoing the previous steps but clicking on Allow instead of Block and Save Settings.

At this point your 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.

## Default Policies

GFI WebMonitor creates a **Default** policy which **Applies to everyone** in each policy node. This ensures a working initial setup. You can either choose to change this policy if you are going to apply the same policy to everyone. Otherwise you can create more policies which are applied to users/groups/IPs as necessary. Policies in the same node are applied in a top-down approach – with the first rule hit being applied.

## Authentication

If you would like to set policies using Windows or Active Directory users and groups you will need to enable authentication. If you've joined your test server to your Active Directory domain, you will be able to use the users of that domain. If not, you can still use the local users and groups in the Server Manager. Otherwise you can use the IPs of the machines which will be accessing the Internet.

During the installation, the GFI WebMonitor Proxy Authentication is set to No Authentication. This means that only the IPs of the machines being proxied through WebMonitor will be reported, and the policies need to be applied by IP. If you would like to see usernames and be able to set policies by users and groups, you will need to set the GFI WebMonitor to use authentication.

GFI WebMonitor standard can be configured to authenticate using one of two methods:

- » Basic authentication
- » Integrated authentication

**Basic authentication** – Select this checkbox if the user will be required to enter logon credentials when a new Internet session is launched.

**Integrated authentication (recommended)** – Users will not be prompted to provide logon information; instead GFI WebMonitor proxy will authenticate users by using the client machine's credentials.

Click **GFI WebMonitor > Configuration > Proxy Settings > Authentication Method > Uncheck No authentication** and select the authentication method you require. Click **Save Settings** and **OK** to restart the proxy service to enforce the new authentication.

### Authentication test

Try browsing to <http://www.google.com> and the page should be allowed if you have disabled the search engines block. If you click on **Monitoring > Past Connections** you should see the requests to <http://www.google.com> listed as the user you are logged on with to the test machine.

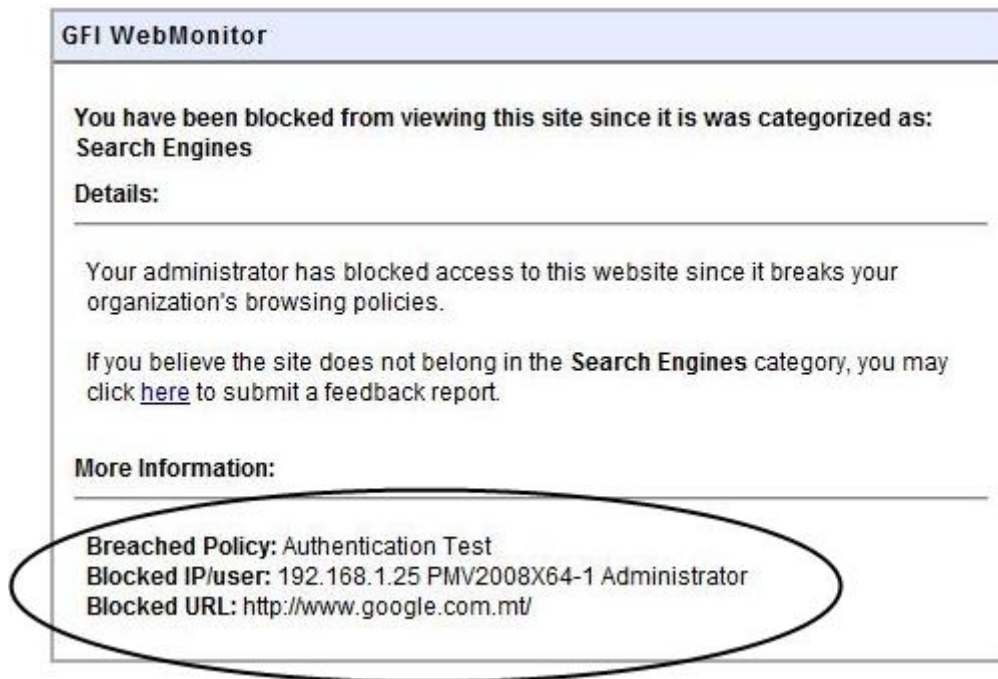
### Test the policies by username

To test that policies are now working by username we can try the same blocking test using the logged on user.

- » Click **GFI WebMonitor > WebFilterEdition > WebFiltering Policies > Add Policy**
- » Name the new policy – Authentication Test
- » Go to the **Web Filtering** tab, scroll to **Search Engines** and click on the **X** to block.
- » Go to the **Applies To** tab, add the user you are currently logged in as (username which showed up in the past connections) as the user in the form of **DOMAIN\User** or **MACHINENAME\Username**. Make sure you enter the exact correct details and click **Add** and **Save Settings**.



Try browsing again to <http://www.google.com> and the page should be blocked. In the details you should see that the actual breached policy has changed to "Authentication Test".

A screenshot of a GFI WebMonitor error message. The title bar reads "GFI WebMonitor". The main text says: "You have been blocked from viewing this site since it is was categorized as: Search Engines". Below this, under "Details:", it states: "Your administrator has blocked access to this website since it breaks your organization's browsing policies." and "If you believe the site does not belong in the Search Engines category, you may click [here](#) to submit a feedback report." Under "More Information:", the following details are listed: "Breached Policy: Authentication Test", "Blocked IP/user: 192.168.1.25 PMV2008X64-1 Administrator", and "Blocked URL: http://www.google.com.mt/". The "More Information" section is circled in black in the original image.

**GFI WebMonitor**

**You have been blocked from viewing this site since it is was categorized as:  
Search Engines**

**Details:**

---

Your administrator has blocked access to this website since it breaks your organization's browsing policies.

If you believe the site does not belong in the **Search Engines** category, you may click [here](#) to submit a feedback report.

**More Information:**

---

**Breached Policy:** Authentication Test  
**Blocked IP/user:** 192.168.1.25 PMV2008X64-1 Administrator  
**Blocked URL:** <http://www.google.com.mt/>

If your block did not work, make sure you have entered all details correctly, especially the username, and that you have saved the policy. Try closing and re-opening the browser, and check the **Monitoring > Past connections** 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.

### *Drill-down interactive reporting*

You can now take a brief look at the UI reporting (though please do note that there is very little data and thus these are not very helpful – for now; the reports will be more useful once a number of days have passed with your trial). Go to **Monitoring > Access Monitoring** and **Monitoring > Blocked Monitoring**. Click on **Monitoring > Blocked Monitoring > By Users** and View Data for Today. You should see your username/IP listed with a number of informational columns. Each column is sortable if you click on it – while if you click on the row you can see the sites/categories/domains accessed.

You can now delete the Authentication Test policy.

### *Download control policies*

If you want to restrict downloads of certain file types, go to **GFI WebMonitor > WebSecurity Edition > Download Control Policies > Default Download Control Policy**. Here you can apply blocking policies for certain file types as necessary either for everyone on the default policy or by user/group/IP.

### *Virus scanning policies*

You can choose the scanning actions to perform by file type too. Go to **GFI WebMonitor > WebSecurity Edition > Virus Scanning Policies > Default Virus Scanning Policy**. In the virus scanning policy, you can choose which file types to scan with which antivirus engine.

You can customize the Default Virus Scanning Policy as necessary; however, the initial setup should suffice.

## *IM control policies*

By default, all IM is allowed. For your trial this is typically sufficient though you can go to **GFI WebMonitor > WebSecurity Edition > IM Control Policies** to create specific policies.

## *Web browsing policies*

Web browsing policies allow you to define policies based on quotas for surf time or by bandwidth. No policies are created here by default, so you can choose to create your own. Go to **GFI WebMonitor > WebFilter Edition > Web Browsing Policies** to add policies to limit user browsing.

## *Whitelist/blacklist*

The whitelist and blacklist can be used to configure exceptions. With the whitelist, sites and users which have been whitelisted bypass all filtering and scanning policies. Blacklisted sites and users are banned from performing any web activity.

## *Dashboard*

You can use the widget-based dashboard to add important information such as:

- » Daily statistics
- » Hits over time
- » Top categories by sites or by bandwidth.
- » Top blocked categories

## *Monitoring: Active connections*

These are the actual real-time connections which are going through the proxy at this specific moment.

## *Monitoring: Past connections*

These are the last few thousands connections which have gone through the GFI WebMonitor proxy.

## *Client-side configuration*

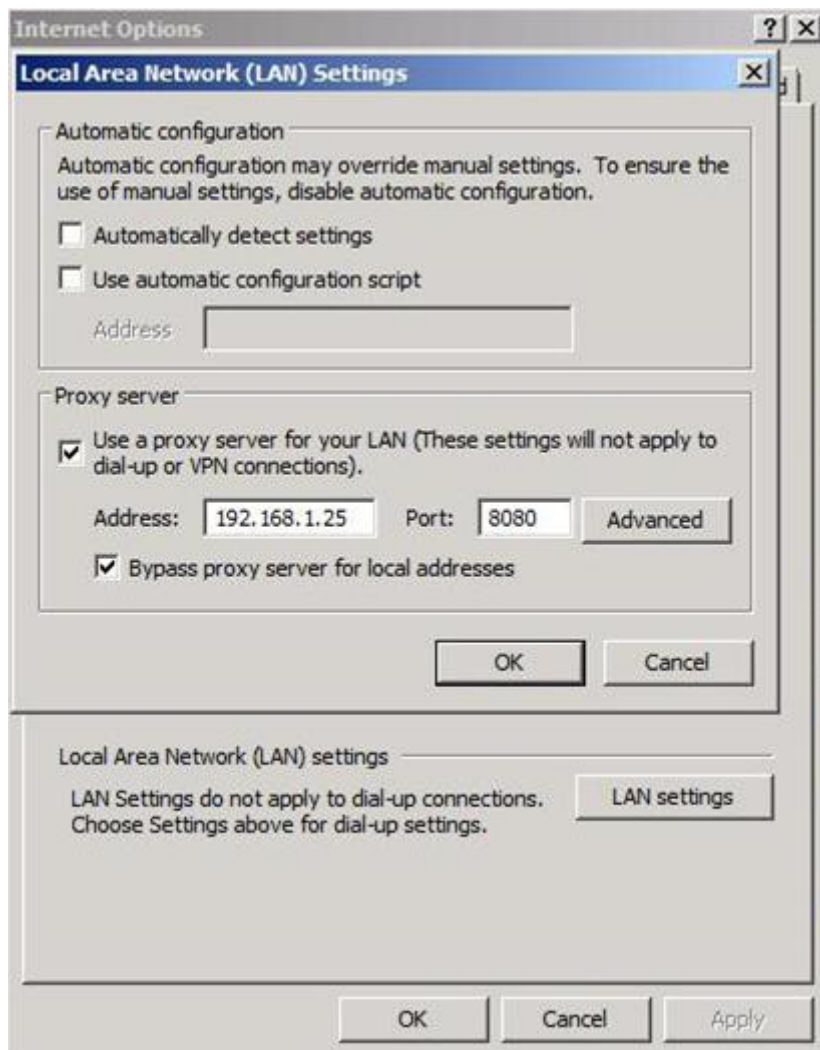
### **Configuring client web browsers**

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

Make sure you only add a few test users initially.

## *Internet Explorer*

1. From the **Tools** menu, choose **Internet Options** and select the **Connections** tab.
2. Click **LAN settings** button.
3. Check **Use a proxy server for your LAN** checkbox.
4. Key in the proxy server name or IP address of the GFI WebMonitor machine and the port used (Default 8080) in the **Address** and **Port** text boxes.



## Firefox

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

## Chrome

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

You can eventually set the proxy settings of every user to pass through GFI WebMonitor through an Active Directory GPO.

## *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*

Now that you've successfully setup GFI WebMonitor, we suggest you take a look at the [GFI WebMonitor Evaluation Guide](#). Here we will take you through some recommendations for evaluation GFI WebMonitor in order to get the most value out of your GFI WebMonitor trial.

## *About GFI*

GFI Software provides web and mail security, archiving, backup 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](mailto:ussales@gfi.com)

**UK AND REPUBLIC OF IRELAND**

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

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

[sales@gfi.co.uk](mailto: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](mailto: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](mailto:sales@gfiap.com)

**Disclaimer**

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

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

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