

## SmartGuide

Welkom bij GFI WebMonitor™. GFI WebMonitor (WebMonitor) verbetert de productiviteit van uw werknemers door u in realtime de volledige mogelijkheid te geven om de internetactiviteiten van gebruikers te bewaken en/of om ervoor te zorgen dat de bestanden die zij downloaden geen virussen of andere malware bevatten.

De GFI WebMonitor SmartGuide bevat een overzicht aan de hand waarvan u het product eenvoudig kunt implementeren. Neem de tijd om dit document te lezen voordat u het product installeert.

Voor gedetailleerdere en technische documentatie over GFI WebMonitor raadpleegt u de:

1. [Beheer- en configuratiehandleiding](#)
2. [GFI WebMonitor Veelgestelde vragen \(FAQ\)](#)
3. [GFI's Knowledge Base](#)
4. [GFI WebMonitor documentation](#)

Als u na het lezen van de SmartGuide nog vragen hebt over dit document, kunt u op de volgende manieren contact met ons opnemen: [CONTACTMOGELIJKHEDEN](#).

GFI WebMonitor heeft twee installatiemodi. Er is een standaardinstallatie (waarover meer in deze handleiding) en een speciale installatie voor de bijzondere behoeften van Microsoft ISA/TMG-server. Als u een ISA/TMG-server in uw netwerk gebruikt, downloadt u de [ISA/TMG-versie\\*](#). Het product is verkrijgbaar in drie (3) verschillende edities: WebFilter Edition, WebSecurity Edition en Unified Protection Edition.

*\*Opmerking: als u de ISA/TMG-versie downloadt, ontvangt u via e-mail de SmartGuide voor die versie.*

1. De **WebFilter Edition** bevat een dynamische database van meer dan 205.000.000 URLs. Deze websites zijn gerubriceerd op basis van de inhoud van de website: U hoeft alleen te bepalen of u de categorie of de website wilt ALLOW, BLOCK of QUARANTINE wilt plaatsen. Bijvoorbeeld, MySpace is gerubriceerd als een site voor sociaal netwerken. Er kan een beleid worden opgesteld om MySpace volledig te blokkeren, of er kan voor een minder strenge benadering worden gekozen door deze site bijvoorbeeld overdag te blokkeren en toe te staan tijdens lunchtijd of vóór en na de normale werktijden.
2. De **WebSecurity Edition**, waarin meerdere anti-virussystemen worden gebruikt, scant het webverkeer en beschermt u tegen virussen, malware/spyware en phishing websites. Kortom, elke download wordt gescand voor deze door gebruikers wordt geopend. Als een werknemer bijvoorbeeld naar een website gaat en een gratis videospel wil downloaden, geeft deze editie van GFI WebMonitor u de mogelijkheid om het bestand (of type bestand) toe te staan, te blokkeren of in quarantaine te plaatsen. Deze spellen kunnen malware en/of virussen bevatten en het is dan ook verstandig om ze in uw Internet Usage Policy\* op te nemen.
3. De **Unified Protection Edition is de meest uitgebreide oplossing** en is een combinatie van de WebFilter en WebSecurity Edition. Dit is de meest uitgebreide oplossing voor webmonitoring, met mogelijkheden om inhoud te filteren en om het systeem te beschermen tegen beveiligingsbedreigingen. De Unified Protection Edition wordt doorgaans gebruikt voor bedrijven die een totaal beleid voor webgebruik implementeren. Met deze editie kunt u de ideale oplossing voor internetmonitoring en toegangscontrole implementeren. U kunt de volgende zaken beheren:
  - a. grenzen instellen voor browsen en/of
  - b. het downloaden en installeren van software regelen.

Omdat u downloads en het browsegedrag in realtime kunt controleren, is het netwerk beschermd tegen malware. Dit is de meest uitgebreide en gebruikte oplossing.

## WELKE GFI WEBMONITOR EDITION IS VOOR MIJ HET MEEST GESCHIKT?

Voordat u kiest welke editie van GFI WebMonitor u in licentie wilt nemen, is het belangrijk dat u de vereisten kent van het **Internet Usage Policy\*** van uw bedrijf. Een Internet Usage Policy zijn de bedrijfsbeleidsmaatregelen en -praktijken die u in het netwerk wilt afdwingen met een product als GFI WebMonitor. Fundamenteel kent een Internetgebruiksbeleid twee varianten. Ten eerste zijn er de beleidsmaatregelen die zijn bedoeld om de productiviteit van de werknemer te verbeteren door toegang tot **niet-productieve sites** (zoals spel- en goksites) uit te schakelen. Daarnaast zijn er de beleidsmaatregelen voor downloadcontrole. Dit type beleid is eerder gericht op het **verminderen van risico's en bedreigingen** die met betrekking tot virussen/malware en andere mogelijke problemen in de typen bestanden die werknemers zouden kunnen downloaden. (Bestandstypen als MP3-muziek kunnen een virus bevatten en kunnen nu worden gecontroleerd.)

Onze ervaring is dat GFI-klanten in het algemeen een GFI WebMonitor-licentie nemen om de volgende vier (4) redenen:

- De browsegewoonten van hun werknemers beheren (**WebFiltering Edition**),
- Realtime netwerkbescherming tegen schadelijke downloads (**WebSecurity Edition**),
- Voldoen aan juridische en/of nalevingsvereisten (**UnifiedProtection Edition**) of
- Een Internet Usage Policy\* in het bedrijf implementeren en afdwingen (**Unified Protection Edition**).

\*We begrijpen dat het ontwikkelen van een Internet Usage Policy misschien nieuw is voor uw organisatie, en daarom hebben we een voorbeeldbeleid opgenomen dat als richtlijn kan dienen bij het ontwikkelen van uw eigen interne beleid.

[Voorbeeld van een Internet Usage Policy](#)

We hebben een bedrijfsbehoefteendiagram opgenomen zodat u beter begrijpt welke editie van GFI WebMonitor het best aan uw behoeften voldoet:

### BEDRIJFSBEHOEFTE WAARAAN GFI WEBMONITOR TEGEMOETKOMT

Bedrijfsbehoefte	WebFilter	WebSecurity	Unified Protection
<b>Algemene functies</b>			
Ondersteunt Windows Workgroups	✓	✓	✓
Active Directory-integratie (gebruikers en groepen)	✓	✓	✓
Filteren van HTTP/FTP-protocol	✓	✓	✓
Filteren van HTTPS-protocol	✓*	✗	✓*
Zwart-wit-lijst van Gebruiker/IP/site	✓	✓	✓
<b>Beheer</b>			
Bewaren van browsegeschiedenis van gebruiker	✓	✓	✓
Quarantaine	✓	✓	✓
Goedkeuren en verwijderen van quarantaine	✓	✓	✓
<b>Realtime monitoring</b>			
Verbindingsmonitoring (actueel en in het verleden)	✓	✓	✓
Monitoring van gebruikers en sites	✓	✓	✓
Bandbreedtemonitoring	✓	✗	✓
<b>Webfiltering</b>			
Op gebruiker/groep gebaseerde URL-rubricering	✓	✗	✓
Webfilterbeleid voor gebruiker/group/IP	✓	✗	✓
Webfilterbeleid met tijds kader	✓	✗	✓

Inhoud en anti-virus			
Beleid voor downloadcontrole	✘	✓	✓
Controle op echtheid van bestandstype	✘	✓	✓
Controle van gecomprimeerde bestanden (zip)	✘	✓	✓
Meerdere anti-virussystemen	✘	✓	✓
Op gebruiker/groep/IP gebaseerde beleidsmaatregelen voor het scannen op virussen	✘	✓	✓
Bescherming tegen malware, spyware en greyware	✘	✓	✓
Heuristische scanning en macro's	✘	✓	✓
Anti-phishing	✘	✓	✓

\*Https-filtering gebeurt alleen op basis van inhoud. Downloads van https-verkeer worden in GFI WebMonitor niet gescand, gefilterd of geblokkeerd.

Het bepalen van de juiste editie voor uw bedrijf kan worden vereenvoudigd door een vraag te beantwoorden over de doelstellingen van uw bedrijf ten aanzien van een Internet Usage Policy.

💡 Wilt u voornamelijk: de *productiviteit* van de werknemer verhogen **OF** de *risico's en bedreigingen* voor het netwerk verminderen **OF** beide?

Als u alleen gericht bent op Productiviteit, is de **WebFiltering Edition** het meest geschikt.

Als u het meest gericht bent op het Verminderen van bedreigingen, is de **WebSecurity Edition** het meest geschikt.

Als u voor Beide hebt gekozen, is de **Unified Protection Edition** het meest geschikt.

Als u niet precies weet welke editie het meest geschikt is voor uw bedrijf, neemt u contact op met uw **GFI-accountbeheerder**.

## AANDACHTSPUNTEN BIJ DE IMPLEMENTATIE VAN GFI WEBMONITOR

Er zijn vijf (5) belangrijke zaken waarmee u rekening moet houden bij de implementatie van GFI WebMonitor. Het is belangrijk dat u deze zaken goed begrijpt. Als u na het lezen van de volgende paragrafen nog vragen hebt of deze verder wilt bespreken, kunt u **contact met ons opnemen**.

1. **GFI WebMonitor-licenties: Het aantal licenties bepalen**
2. **Systeeminstallatievereisten**
3. **Clientbrowsers verifiëren en configureren**
4. **Het Internet Usage Policy in GFI WebMonitor afdwingen**
5. **Rapporteren met GFI WebMonitor**

### 1. GFI WEBMONITOR-LICENTIES: HET AANTAL LICENTIES BEPALEN

**ZORGVULDIG LEZEN, AUB!** Het is belangrijk dat u begrijpt hoe een licentie wordt geteld: **Als het aantal in gebruik hoger is dan het aantal in licentie** (betaalde licenties), dan worden **de extra gebruikers/IPs** boven de licentielimiet **NIET beschermd door GFI WebMonitor**.

Een GFI WebMonitor-eenheid is een zetel. Een zetel is gedefinieerd als een IP-adres of gebruiker, afhankelijk van de vraag of de verbinding die door GFI WebMonitor wordt verwerkt is "**geverifieerd**" of "**niet geverifieerd**":

- Een **zetel is gedefinieerd als een gebruiker** als er een geverifieerde verbinding is. Een "geverifieerde verbinding" is een verbinding waarbij GFI WebMonitor de gebruikersnaam registreert van de gebruiker die de verbinding tot stand brengt.
- Een **zetel is gedefinieerd als een IP-adres** als een verbinding niet geverifieerd is. Een "niet-geverifieerde verbinding" is een verbinding waarbij GFI WebMonitor het IP-adres registreert van de computer die de verbinding tot stand brengt.

Er zijn situaties waarin geverifieerde en niet-geverifieerde verbindingen binnen hetzelfde netwerk tot stand gebracht worden. In dergelijke gevallen wordt het aantal licenties als volgt bepaald.

VERBINDING	AANTAL LICENTIES
Geverifieerde en niet-geverifieerde verbinding vanuit dezelfde computer	1
Geverifieerde gebruiker brengt twee (2) verbindingen tot stand vanaf verschillende computers (dus verschillende IPs)	1
Verbindingen vanuit IP-adressen op witte lijst	0
Twee (2) geverifieerde gebruikers die vanaf dezelfde computer verbinding maken	2

⚠ Gebruikers kunnen echter ook op de witte lijst staan. Als echter een serviceaccount die gebruikmaakt van verificatie, verbinding maakt met internet, dan wordt deze als een extra gebruiker met licentie beschouwd. Daarom wordt u geadviseerd om IPs in plaats van gebruikers op de witte lijst te plaatsen zodat verkeer vanaf die computer op de witte lijst staat.

## 2. SYSTEEMINSTALLATIEVEREISTEN

De installatievereisten voor GFI WebMonitor zijn afhankelijk van de editie.

GELICENTIEERDE EDITIE: De installatievereisten voor elke editie – WebFilter, WebSecurity en UnifiedProtection – verschillen in kleine mate:

Editie	Minimale hardwarevereisten		
	Processor	RAM	Vaste schijf
WebFilter	2,0 GHz	1 GB*	2 GB beschikbare schijfruimte
WebSecurity	2,0 GHz	1 GB*	10 GB beschikbare schijfruimte
Unified Protection	2,0 GHz	2 GB*	12 GB beschikbare schijfruimte

\*4 GB RAM wordt aanbevolen voor optimale prestaties.

Installatiemodus	Ondersteund besturingssysteem	Overige vereiste/ aanbevolen onderdelen
<b>GFI WebMonitor 2009 (Zelfstandige proxyversie)</b>	<ul style="list-style-type: none"> <li>• Microsoft Windows Server 2008</li> <li>• Microsoft Windows Server 2003</li> <li>• Microsoft Windows 7</li> <li>• Microsoft Windows Vista</li> <li>• Microsoft Windows XP SP2</li> </ul>	<ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 6 of hoger</li> <li>• Microsoft.NET framework 2.0</li> <li>• Routing en externe toegang configureren op Microsoft Windows Server 2003/2008</li> <li>• Microsoft SQL Server 2000 of hoger (voor rapportagedoeleinden)</li> <li>• Twee netwerkinterfacekaarten (bij installatie in de internet-gatewaymodus)</li> </ul>

⚠ Afhankelijk van het aantal zetels dat het product filtert, moeten meerdere installaties van GFI WebMonitor worden overwogen. U wordt geadviseerd om voor elke 500 zetels (gebruikers of IPs) een installatie van GFI WebMonitor te gebruiken om verkeer te filteren.

## 3. CLIENTBROWSERS VERIFIËREN EN CONFIGUREREN

Er zijn gevallen waarin een bedrijf geverifieerde verbindingen wil afdwingen. (Een bedrijf zou verifieerde verbindingen kunnen afdwingen zodat beheerders er gemakkelijker voor kunnen zorgen dat de verbindingen van alle gebruikers worden gefilterd via GFI WebMonitor.) Deze paragraaf behandelt de verschillende methoden waarmee verificatie kan worden afgedwongen en de configuratie van de webbrowsers van de client (eindgebruiker).

### (a) Verificatie afdwingen

Als uw organisatie ervoor kiest om geverifieerde verbindingen af te dwingen, dan kan GFI WebMonitor met behulp van een van de volgende twee methoden worden geconfigureerd om verificatie af te dwingen:

- Geïntegreerde verificatie (aanbevolen), of
- basisverificatie.

Meer informatie vindt u [HIER](#).

## **(b) De webbrowsers van de client (eindgebruiker) configureren**

Voor GFI WebMonitor moet u de browser van de gebruiker zo configureren dat deze de computer van GFI WebMonitor als de proxyserver voor aanvragen voor webverkeer gebruikt. Op die manier kan het product ervoor zorgen dat alle gebruikers worden gefilterd. Daartoe gaat u als volgt te werk:

1. Configureer de browser van de gebruiker handmatig zodat deze naar de computer wijst waarop GFI WebMonitor is geïnstalleerd als de proxyserver, of
2. Gebruik Groepsbeleid om de browsers automatisch te configureren\*
3. Gebruik automatische detectie in de gebruikersinterface van GFI WebMonitor en browsers.

Informatie over de bovengenoemde configuratieopties vindt u [HIER](#).

\*als u een beleid wilt toepassen op gebruikers/groepen, MOET u GFI WebMonitor zo instellen dat deze geverifieerde verbindingen VERPLICHT STELT. Als u GFI WebMonitor niet zo instelt dat deze geverifieerde verbindingen verplicht stelt, wordt het gemaakte gebruikers- of groepsbeleid niet toegepast. Meer details over hoe u geverifieerde verbindingen configureert, vindt u [HIER](#).

## **4. HET INTERNET USAGE POLICY IN GFI WEBMONITOR AFDWINGEN**

Nadat u een Internet Usage Policy voor uw bedrijf hebt opgesteld, moet u deze beleidsmaatregelen gaan afdwingen met GFI WebMonitor. GFI WebMonitor gebruikt twee soorten beleidsmaatregelen, webfiltermaatregelen, die in de WebFiltering-editie van het product voorkomen, en downloadcontrolemaatregelen, die in de WebSecurity Edition van het product voorkomen. Hier volgen enkele voorbeelden van de twee soorten beleidsmaatregelen.

### **WebFiltering-maatregelen**

Een maatregel voor het filteren van webinhoud is gebaseerd op de inhoud van een site. Dit type beleid wordt vaak beschreven als een beleid dat het productiviteitsverlies vermindert waartoe onbeperkte toegang tot internet kan leiden. GFI WebMonitor WebFiltering Edition heeft als doel dit type beleid af te dwingen. Een eenvoudig voorbeeld van hoe het product een beleid afdwingt, is wanneer GFI WebMonitor wordt ingesteld om toegang te blokkeren tot websites die zijn gerubriceerd als 'Streaming media'. Hiermee wordt de toegang geblokkeerd tot websites met streaming media, zoals YouTube, die een hoog bandbreedtegebruik in het netwerk met zich meebrengen, waardoor het bedoelde netwerkgebruik wordt vertraagd. Bedrijven hoeven daardoor mogelijk geen dure bandbreedte-upgrades door hun ISP te laten uitvoeren.

### **Beleid voor downloadcontrole**

Terwijl een webfilterbeleid is gericht op de inhoud van de webpagina's, zijn maatregelen voor downloadcontrole gericht op de risico's en bedreigingen voor uw bedrijf. Het is een feit dat internet een essentieel onderdeel is voor het functioneren van uw bedrijf. Het beleid voor downloadcontrole is daarom gericht op vijandige zaken, zoals virussen, malware en phishing websites, die een probleemloos internetgebruik (zoals het netwerk en gegevens) in uw bedrijf kunnen voorkomen. Een eenvoudig voorbeeld is het controleren van bestandstypen (zoals films) die dikwijls heel groot zijn, zodat deze niet naar het netwerk kunnen worden gedownload en teveel opslagruimte in beslag nemen. Hiermee kunt u de aanschaf van dure upgrades van opslagruimte verminderen en voorkomen dat back-ups worden gemaakt van ongeschikte gegevens.

U kunt GFI WebMonitor op basis van de behoeften van uw bedrijf implementeren: Webfilter- en downloadcontrolemaatregelen kunnen 'all inclusive' worden toegepast op alle IPs, alle gebruikers, alle groepen, enzovoort, of afgestemd op specifieke IPs, gebruikers of groepen. Beleidsmaatregelen kunnen ook tijdens specifieke uren of continu gelden. Beleidsmaatregelen worden in de drie (3) edities van GFI WebMonitor opgesteld. Wanneer u een beleid hebt opgesteld, kunt u zelf bepalen welke acties moeten worden ondernomen.

Het product biedt drie (3) acties die u in een beleid kunt uitvoeren. U kunt ALLOW, QUARANTINE of BLOCK.

- ALLOW wordt gebruikt in gevallen waarin een beleid is gemaakt om ervoor te zorgen dat specifiek verkeer altijd toegankelijk is;
- QUARANTINE wordt gebruikt wanneer verkeer *mogelijk* schadelijk is. De quarantaine wordt gebruikt om de website tijdelijk vast te houden zodat de IT-beheerder kan bepalen of de website is toegestaan of moet worden geblokkeerd.
- BLOCK wordt gebruikt als is bepaald dat verkeer altijd moet worden geweigerd of geblokkeerd.

Aangezien het instellen van een beleid erg belangrijk is in GFI WebMonitor, vindt u hier meer informatie over hoe u dat doet:

### Webfilterbeleid (WebFilter Edition) Beleid voor downloadcontrole (WebSecurity Edition)

## 5. RAPPORTEREN MET GFI WEBMONITOR

GFI WebMonitor is een krachtig hulpmiddel voor het beschermen van uw bedrijf door het internetgebruik te beveiligen. Het beschikt over een zeer uitgebreide rapportagefunctie die is gericht op zowel het dagelijks beheer van een netwerk als op de gedetailleerde rapportage die wordt gebruikt om productiviteit te meten en het algehele internetgebruik van uw bedrijf te beheren. Alle edities van GFI WebMonitor bieden realtime en historische rapportagemogelijkheden.

Let wel: de ReportPack is een afzonderlijke installatie waarvoor het GFI Report Center is vereist. Het GFI Report Center vindt u [HIER](#) en het ReportPack vindt u [HIER](#).

GFI WebMonitor biedt een realtime dashboard waar u onmiddellijk belangrijke informatie over het huidige internetgebruik kunt zien. Hiertoe behoren het aantal aangevraagde URLs, de totale bandbreedte in gebruik, de bandbreedte per uur, het aantal huidige actieve verbindingen, het aantal gescande downloads, het aantal items in quarantaine, het huidige aantal verbindingen dat door beleidsmaatregelen is geblokkeerd en de bandbreedtetendens over een bepaalde tijd.

Beheerders hebben ook een dashboard voor monitoring waarmee ze de huidige verbindingen kunnen zien die in het netwerk tot stand worden gebracht en waarmee ze deze in realtime kunnen annuleren.

Hoewel het GFI WebMonitor-dashboard over realtime rapportagemogelijkheden beschikt, heeft GFI een gebruiksvriendelijke rapportagefaciliteit gemaakt voor de meeste informatie die WebMonitor verzamelt, de [GFI WebMonitor ReportPack](#). Met de GFI WebMonitor ReportPack kunt u de uitvoering van rapporten plannen en deze op regelmatige basis per e-mail laten versturen.

Met de GFI WebMonitor ReportPack kunnen managers en IT-beheerders doeltreffend gebruik maken van resources.

Met GFI WebMonitor ReportPack kunt u de volgende typen rapporten maken:

- **Bandwidth Reports:** De bandbreedtecategorie bevat rapporten aan de hand waarvan beheerders het gebruik van bandbreedte kunnen observeren. ([Voorbeeldrapport](#))
- **Hits Reports:** De categorie Treffers bevat rapporten waaruit statistische gegevens worden gehaald over website-treffers. ([Voorbeeldrapport](#))
- **Threat Reports:** De categorie Bedreigingen bevat rapporten waaruit statistische gegevens worden gehaald over geblokkeerde websites. ([Voorbeeldrapport](#))
- **Web Usage Trend Reports:** De categorie Webgebruikstrends bevat rapporten aan de hand waarvan de webgebruikstrends van gebruikers worden bepaald. ([Voorbeeldrapport](#))

Volledige documentatie over GFI WebMonitor ReportPack vindt u op de volgende website:  
<http://www.gfi.com/webmon/webmon2009rpmanual.pdf>

© 2010. GFI Software. Alle rechten voorbehouden. Alle product- en bedrijfsnamen in dit document zijn handelsmerken van hun respectieve eigenaren.