



**eSoft Gateway Antispyware  
Training Guide**  
version 1.0 October 1, 2006

# GATEWAY ANTISPYWARE SOFTPAK

## 1.1 Gateway Anti-spyware overview

eSoft's Gateway Anti-Spyware Softpak protects the local network from Spyware in three ways- first it blocks HTTP requests to known spyware hosting or data collection sites. Secondly, it recognizes and blocks known spyware content in HTTP, FTP and SMTP sessions. Last, it recognizes and blocks outbound activity from spyware that is active on the network to prevent reporting or any outbound communication of the spyware.

Once enabled, (on by default after installation) the Gateway Anti-Spyware Softpak will begin blocking HTTP requests to known spyware hosting locations immediately. Web users will begin to notice the existence of "pink screen" elements where advertising used to be in sites that have banner advertisements. The message reads: For your protection access to i.e.: ad.doubleclick.net has been blocked by eSoft gateway Antispyware as it has been associated with Spyware

### Example of "pink screen" elements

The screenshot displays a MarketWatch page with several red error messages overlaid on the content. The messages are: "For your protection access to ad.doubleclick.net has been blocked by eSoft Gateway Anti-Spyware as it has been associated with Spyware." The page includes a MarketWatch logo, a search bar, and a navigation menu with categories like NEWS & COMMENTARY, MARKETS, MUTUAL FUNDS & ETFS, PERSONAL FINANCE, TOOLS & RESEARCH, MY MARKETWATCH, and MY STORES. The main content area shows a stock chart for Wild Oats Markets Inc (OATS) with a price of 17.52 and a change of +0.37 (+2.16%). The chart shows a price increase from September to July. The error messages are scattered across the page, including one at the top left, one in the middle left, one in the middle right, and one at the bottom right.

## 1.2 Gateway Anti-spyware basic settings

There are few settings in GWAS- simply enable and choose the update interval- 30 minutes by default.

### 1.3 Gateway Anti-spyware advanced settings

---

Under the advanced tab, you can alter the following defaults:

Maximum file size to scan: 100 MB, block file if it exceeds the maximum size  
Scan FTP sessions  
Scan inbound SMTP (email) sessions  
Scan outbound SMTP (email) sessions

Altering these default settings is not recommended unless you have performance issues or problems with FTP or SMTP email sessions. Disabling these features will allow these protocols to pass without spyware scanning.

### 1.4 Gateway Anti-spyware threat levels

---

This feature allows you to set the level of spyware that will be blocked by the system. By default it is set at its most aggressive level, blocking all categories including consumer ware, which is considered the least problematic. If you choose to allow any category to pass you may make a change here.

Note: Changing the action for the threat level won't necessarily affect performance since all spyware signatures will still be scanned.

### 1.5 Gateway Anti-spyware custom destination rules

---

Sometimes it becomes necessary to whitelist a website to allow full functionality. This can be done by entering its URL or IP address as a custom destination.

### 1.6 Gateway Anti-spyware custom source rules

---

Custom source rules are whitelist rules for local computers. Whitelisting will prevent any outbound activity from a local computer to be construed as spyware activity. This is sometimes required for servers such as local DNS servers.

## 1.7 Tips & Traps

---

Gateway Anti-spyware begins working by default when it is installed. It will begin blocking access to some elements of web pages or entire sites based on their association with Spyware. It will have an immediate visual impact on the users browsing experience.

There may also be some perceptible delay in how fast web pages load. This should be expected, as sites are being checked vs. the database and content scanned for spyware.

If you experience a complete blockage of all sites, you could have situation where your local domain server is not being allowed to resolve addresses. You'll want to add this server as a trusted source.

False positives are also a possibility. If you have sites that you'd like to allow access to, you may add these to the trusted destination list.

Gateway Anti-spyware is very load intensive, scanning HTTP, FTP, SMTP. If a system is heavily burdened you have the option of disabling the FTP and or SMTP scanning. SMTP scanning happens as email is sent or received, so it's effect is "spikey" as email is passed through the system, disabling SMTP either inbound, outbound or both should help remove these low performance spikes, but will leave you vulnerable to spyware in SMTP email.

FTP scanning of larger files can create a "dragging" experience at the beginning of a download with the perception that the file transfer speed is very low at first, then recovering near the end of the file. If the file is very large, there can be some time-out issues.