

WatchGuard SpamScreen

Control Junk E-Mail

Thank you for purchasing WatchGuard SpamScreen 1.0. This document steps through the process to register, download, install and configure SpamScreen to immediately reduce the time and effort of controlling junk e-mail on your network.

Registering and Installing SpamScreen

Your purchase of the WatchGuard SpamScreen includes these instructions as well as a license key. You must register your license key and then download the software itself from the WatchGuard LiveSecurity Archive.

Registering SpamScreen

1. Open your Web browser to the LiveSecurity archive at:
<http://www.watchguard.com/archive/>
2. Log in to the LiveSecurity Archive.
3. Click Register SpamScreen Now.
The SpamScreen Registration page appears.

How to Buy | Products | **Support** | Press Room | About Us | Search

SUPPORT
End Users

SpamScreen Registration

Enter your SpamScreen License Key below.

LiveSecurity Subscription Key : **123-456-7890**

SpamScreen License Key :

Note: Future announcements about your SpamScreen Software may be broadcast to you using your registered LiveSecurity Subscription key:
123-456-7890

4. Enter your SpamScreen license key including the hyphens.
The most common reason for registration to fail is incorrectly typing the numbers and hyphens of the License Key.
5. Click Register.
The SpamScreen license key is associated with your LiveSecurity license to ensure that you receive regular updates to the SpamScreen utility. The download page opens.

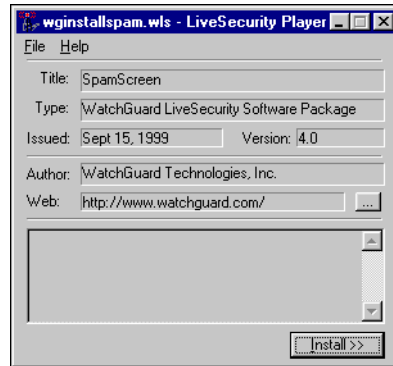
6. Click Download Now.

A prompt appears to open or save the SpamScreen installation file. The file name is `wGInstallSpam.wls`.

7. Save the file to your Windows desktop.

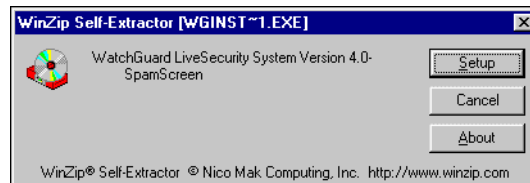
Installing SpamScreen

1. On your Windows desktop, double-click `wGInstallSpam.wls`.
WatchGuard Player appears.



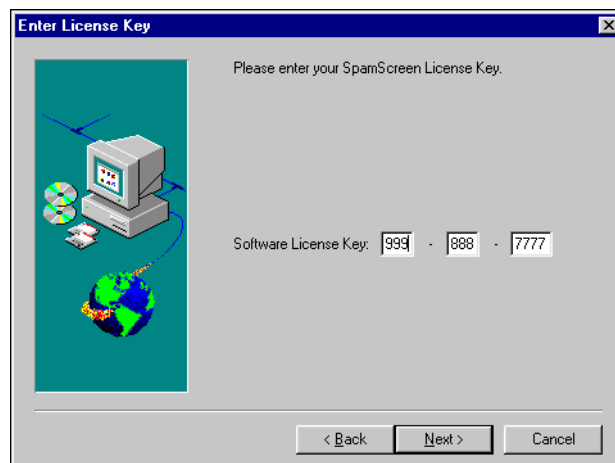
2. Click Install.

The SpamScreen extractor appears.



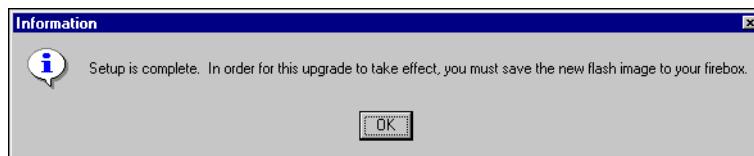
3. Click Setup.

The installation wizard starts.



4. Enter your SpamScreen license key. Click Next.

The installation wizard enables SpamScreen in the Policy Manager Setup menu.



5. Click OK.

Configuring SpamScreen Message Handling

SpamScreen can handle a spam message in one of three ways:

- Deny - Deletes the message.
- Allow - Completely disables SpamScreen and allows messages to pass to the recipient unchanged.
- Tag - Passes the message to the recipient with a tag phrase in the Subject line.



NOTE

SpamScreen requires the SMTP proxy service. If you have not already done so, use the Policy Manager to add the SMTP proxy service. For more information, see the WatchGuard LiveSecurity System User Guide.

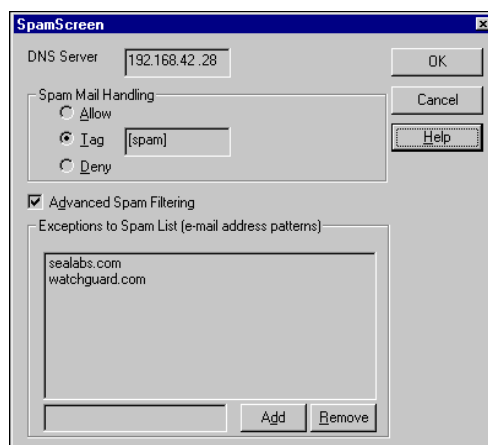
SpamScreen also operates with two levels of checks. Normal SpamScreen checks headers for known spam sources. It also runs a common criteria check and screens for bulk mailer tags. For more information, see “How SpamScreen Identifies Spam” on page 5.

With Advanced Spam Filtering enabled, SpamScreen expands the headers evaluated. This option considerably reduces “false negatives”— SpamScreen failing to identify a spam message as spam. The disadvantage is that it makes SpamScreen considerably more sensitive and may increase the number of “false positives”— SpamScreen identifying a normal message as spam. Advanced Spam Filtering also results in SpamScreen identifying most mailing list messages as spam.

From the Policy Manager in the Advanced view:

1. Select Setup ⇒ SpamScreen.

The SpamScreen dialog box appears.



-
2. Enter the DNS Server IP address.
SpamScreen must be directed to a DNS server on the trusted network.
 3. Select a Message Handling option.
 4. If desired, enable Advanced Spam Filtering.
 5. Click OK.

Tagging Spam

The Tag spam mail handling option prepends a word or phrase in the Subject line of each message identified as spam. This option lets recipients filter and redirect spam into a folder for later perusal. You define the message tag. Examples include: [UCE] or [SPAM]. From the Policy Manager:

1. Select Setup ⇒ SpamScreen.
2. Select the Tag spam mail handling option.
3. Enter a tag word or phrase.
4. Click OK.

Consult the documentation for your e-mail application to learn methods of filtering mail on the Subject line.

Creating Exceptions to the Spam List

Allowing Blocked Addressees

Occasionally an address appears on the RealTime BlackHole List from whom you would like to receive mail. Use SpamScreen to configure exceptions to the RBL. From the Policy Manager in the Advanced View:

1. Click Setup ⇒ SpamScreen.
The SpamScreen dialog box appears.
2. Type the domain name or e-mail address in the text box to the left of the Add button.
3. Click Add.

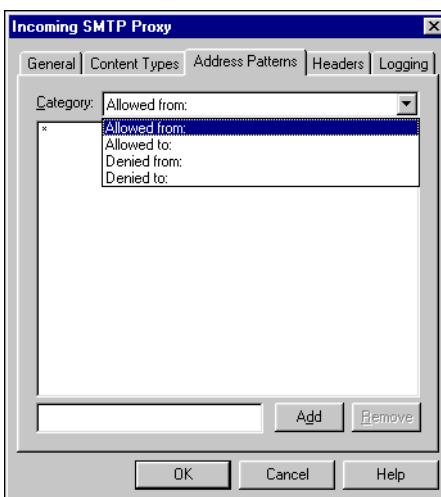
The host name or e-mail address appears in the Exception list. SpamScreen will no longer check any messages originating from that address.

Blocking Addresses Not on the Spam List

If you are the target of a spammer not on the WatchGuard spam list, you can block incoming messages from a host name or IP address using the Incoming SMTP Proxy dialog box.

1. In the Services Arena double-click the SMTP Proxy icon.
The service Properties dialog box opens.
2. Click the Properties tab.
3. Click Incoming.

The Incoming SMTP Proxy dialog box appears displaying the General tab.



4. Click the Address Patterns tab.
5. Use the Category drop list to select Denied From.
6. Type the address pattern in the text box to the left of the Add button.
7. Click Add.

The address pattern appears in the pattern list. Repeat for the address pattern of each spammer not blocked automatically by SpamScreen.

8. Click OK.

Keeping SpamScreen Current

Our team at WatchGuard monitors anti-spam newsgroups, mailing lists, and Web sites in order to keep our product current with the latest tactics in the battle against spam.

Receiving an Update Via LiveSecurity

As a LiveSecurity subscriber, you will automatically receive periodic updates to the SpamScreen utility. Like other broadcasts, these software updates will automatically appear in the LiveSecurity Inbox. Follow the directions to install the software update.

Downloading SpamScreen Updates from the LiveSecurity Archive

If you do not receive or delete a SpamScreen software update, you can always download the most recent version from the LiveSecurity Archive. Point your browser to:

<http://www.watchguard.com/archive>

How SpamScreen Identifies Spam

SpamScreen considerably enhances your ability to deal with spam at the point where it attempts to enter your system: the SMTP proxy service of your firewall.

With SpamScreen enabled, the WatchGuard SMTP proxy evaluates each message and makes a determination on whether or not the message is spam. If it concludes the message is spam, the SMTP proxy automatically either deletes the messages or places a tag in the subject line before delivering it to the recipient.

SpamScreen uses a three phase approach to identifying spam.

RealTime BlackHole List

SpamScreen first checks the message against the RealTime BlackHole List (RBL). The RBL is a name server that has DNS records for sites considered to be spammers, spam relays, or spam-friendly service providers. If the message originates from an address on the RBL, SpamScreen marks the message as spam.

Common Criteria Check

Typically, spam messages share one or more characteristics found in the message header. The indicators are frequently a by-product of the spammer's desire to hide their address and avoid a deluge of bounced mail and irritated replies. Examples of common criteria include:

- From or Reply-To with noreply@
- From, To, or CC with friend[0-9a-zA-Z]@
- From, To, or CC with moneymakers@
- To or CC with blank before the @ sign
- To or CC with "(Recipient list suppressed)"
- To or CC with to.all.our.friends@
- Reply-To with "remove" in the string

SpamScreen checks the message against a long list of common criteria. If any one of these conditions are true, SpamScreen marks the message as spam.

Commercial Bulk Mailer Tags

Most commercial bulk e-mailer applications leave some "fingerprint" on the message header. For example, many include an "X-" header identifying the name of the application. SpamScreen checks the message against a list of known bulk mailer tags. If a tag is found, SpamScreen marks the message as spam.

SpamScreen Message Header

After processing a message through all three checks, SpamScreen allows it to pass through the firewall. SpamScreen adds an "X-SpamScreen" header to every message. If the message is spam, SpamScreen includes a description of why the message was marked as spam.

```
X-SpamScreen: Protected by WatchGuard SpamScreen (tm)  
Copyright (C) 1999 WGTI
```

Monitoring SpamScreen Activity

Viewing Message Header Notifications

Spam is often readily identifiable by the contents of the message headers. SpamScreen uses these headers to mark spam. In addition, SpamScreen adds an "X-" header to every e-mail message it processes. Most mail systems require special instructions to display full message headers. The following are instructions for the most commonly used mail systems. Consult your mail system documentation if application is not listed here.

Microsoft Outlook 97 and Microsoft Outlook Express

1. Open the message.
2. Select File ⇒ Properties.
3. Click the Details tab.

Microsoft Outlook 98

1. Open the message.
2. Select View ⇒ Options.
The Internet headers field displays the entire message header.

Netscape Messenger

1. Open the message.
2. Select View ⇒ Headers ⇒ All.

Pine

1. Enable full header command mode. From the Main Menu, type S to enter Setup menu. Type C to enter the configuration screen.
2. Use the space or down arrow key to scroll down until you locate:

[] enable-full-header-cmd
3. Type X to enable full header command. Type E to exit configuration. Type Y to confirm changes.
4. Open the message.
5. Type H to display full headers.

Interpreting Log Messages

When SpamScreen identifies a message as spam it generates a message in the logdb file. Typically, these log entries explain why SpamScreen identified the message as spam. Some examples of log messages include:

Examples of Log Entries Generated by SpamScreen

Message	Interpretation
Found spam from 192.168.200.2	192.168.200.2 is trying to send e-mail and is in the RBL list.
RBL list returned 00000003 for 192.168.200.2, funky	When SpamScreen looked up 192.168.200.2 it got an odd result. Usually indicates a DNS server that is down or otherwise crippled.
lookup for 192.168.200.2 failed, (for some reason)	The RBL lookup failed for 192.168.200.2, but SpamScreen could provide more information than the previous case
Probable spammer domain in From:	We saw a domain name that looked like a domain from our spam database in a header. Similar messages could appear for From, X-From, Reply-To, Return-Path, Sender, X-Sender, and Errors-To.
Comments field has 'Authenticated sender is <>'	Certain bulk-mailers generate this string. Unfortunately, so does the free Pegasus mail program.
noreply@ in From: or Reply-To:	Frequently a condition of spam messages.
friend@ in recipient field	Frequently a condition of spam messages.
moneymakers@ in recipient field	Frequently a condition of spam messages.
null before @ in recipient field	Frequently a condition of spam messages.
Suppressed or undisclosed recipients	Frequently a condition of spam messages.
'remove' in Reply-To	Frequently a condition of spam messages.
Message generated by a bulk e-mailer	SpamScreen identified a bulk e-mailer tag.

Troubleshooting

I installed SpamScreen but the command doesn't appear in the Setup menu?

The SpamScreen command only appears in the Policy Manager Advanced view. To toggle from the Basic to the Advanced view, select View ⇒ Advanced.