
WatchGuard® SpamScreen Guide

Thank you for purchasing WatchGuard SpamScreen 1.2. This document describes how 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

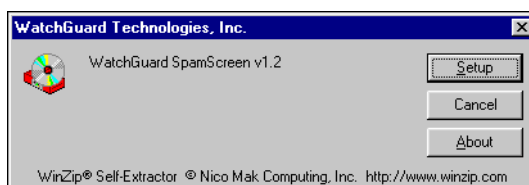
Your purchase of the WatchGuard SpamScreen includes these instructions as well as a license key. You must register your license key and then download the software itself from the WatchGuard LiveSecurity Service Web site.

Registering SpamScreen

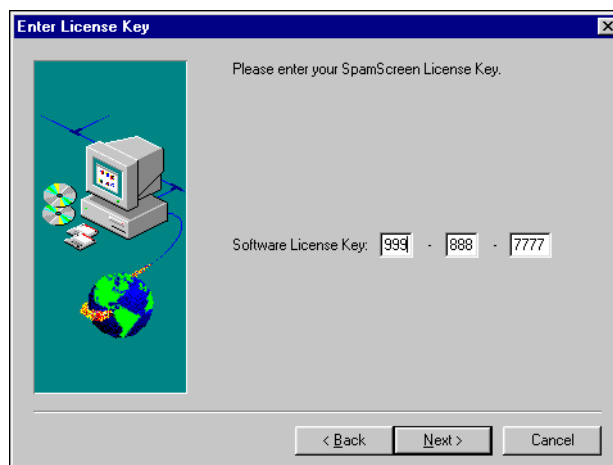
1. Open your Web browser to the LiveSecurity Service Web site at:

<https://www.watchguard.com/support/>

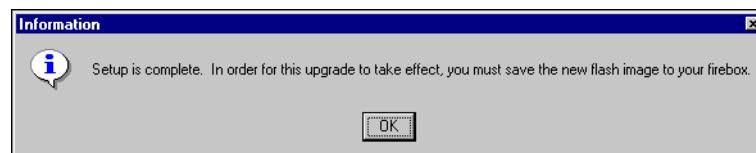
2. Log in.
3. Click **Register SpamScreen**.



3. Click **Setup**.
The installation wizard starts.
4. Click **Yes** to accept the end-user license agreement.



5. Enter your SpamScreen license key. Click **Next**.
The installation wizard enables SpamScreen in the Policy Manager Setup menu.



6. Click **OK**.

Configuring SpamScreen Message Handling

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

- **Deny** – Deletes the message.
- **Allow** – 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.



SpamScreen requires the SMTP proxy service. If it is not already configured, use the Policy Manager to add the SMTP proxy service. For more information, see the *LiveSecurity System User Guide*.

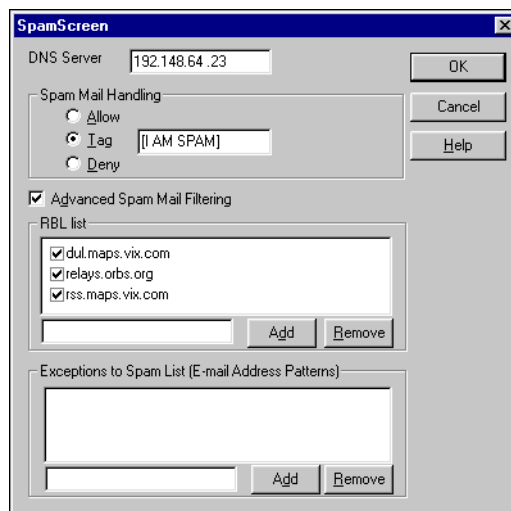
SpamScreen offers two levels of checks: normal and Advanced. Normal SpamScreen checks headers for known spam sources. It also runs a known characteristics check and screens for bulk mailer tags. (For more information, see “How SpamScreen Identifies Spam” on page 6.)

SpamScreen checks the IP address of the server against several public RBL (realtime blackhole list) servers. These are special-purpose DNS servers that store IP addresses of known spammers and other hosts that may be vulnerable to spam attacks (eg, mail relays).

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 may result in SpamScreen identifying mailing list messages as spam.

From the Policy Manager in the Advanced view:

1. Select **Setup**⇒ **SpamScreen**.



2. Enter the DNS Server IP address.
3. Select **Spam Mail Handling**.
4. Select RBL servers if desired.
For more information, see “RealTime BlackHole List” on page 7.
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, identified by its prepended message tag, into a folder for later perusal. You define the message tag. Example tags 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 how to filter mail based on Subject line.

Creating Exceptions to the Spam List

Allowing Blocked Addressees

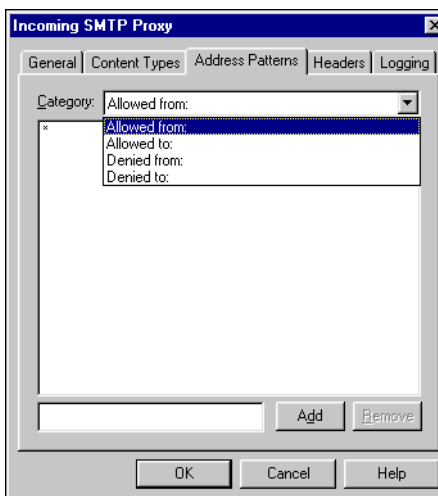
Occasionally a message will be mistakenly determined to be spam. If you know the sender's address, you can configure exceptions so that address will not be checked by SpamScreen, and subsequently tagged as spam. From the Policy Manager in the Advanced View:

1. Click **Setup**⇒ **SpamScreen**.
The SpamScreen dialog box appears.
2. Under **Exceptions**, enter 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 Exceptions to Spam 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 spammer that has not been detected by SpamScreen, 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 a SpamScreen software update, you can always download the most recent version from the LiveSecurity Service.

1. Open your Web browser to the LiveSecurity Service Web site at:

<https://www.watchguard.com/support/>

2. Log in.
3. Scroll down to the SpamScreen software; click **Download Now**.

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 determines whether or not the message is spam. If it concludes the message is spam, the SMTP proxy automatically either refuses the messages or places a tag in the subject line before delivering it to the recipient.

SpamScreen uses several methods to identify 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.

SpamScreen comes pre-configured with the following RBL servers:

rbl.maps.vix.com

The MAPS Realtime Blackhole List server contains IP addresses of known spammers. MAPS adds addresses to their list only when some effort has been made to contact the suspected spammers and verify that they are indeed intentionally spamming (that is, that their systems are not being used unknowingly by a third party). As such, the MAPS RBL server may not be comprehensive, but is generally more accurate than other RBL servers.

You can obtain more information on the MAPS RBL list from

<http://maps.vix.com/rbl/>.

dul.maps.vix.com

The MAPS Dial-up User List server contains network IP addresses owned by Internet service providers (ISPs) who provide dial-up access. The rationale behind the DUL list is that dial-up users should be sending e-mail through their ISP's mail server, not directly out to the servers where the recipients' accounts reside. Dial-up users who do send directly have a higher chance of being spammers using bulk-e-mailer applications.

You can obtain more information on the MAPS DUL RBL list from [http://](http://maps.vix.com/dul/)

maps.vix.com/dul/.

rss.maps.vix.com

The MAPS Relay Spam Stopper server contains IP addresses of e-mail (SMTP) servers known to allow third-party relaying. If a server accepts a message from one server and agrees to relay it to another server, it is called an open relay. Open relay is frequently used for spamming. Many legitimate e-mail servers may be on this list, however. Enable the RSS server only if you wish to be very strict in blocking spam. To avoid blocking legitimate e-mail, we suggest that Spam Mail Handling be set to Tag instead of Deny.

You can obtain more information on the MAPS RSS RBL list from

<http://maps.vix.com/rss/>.

relays.orbs.org

The ORBS server is similar to the MAPS' RSS server – it also contains IP addresses of SMTP servers that allow third-party relaying. However, the ORBS server is updated automatically, by scanning the Internet for open SMTP relays. Because of this, use of the ORBS server may result in a higher proportion of legitimate e-mail being tagged by SpamScreen. Enable the ORBS server only if you wish to be very strict in blocking spam. To avoid blocking legitimate e-mail, we suggest that Spam Mail Handling be set to Tag instead of Deny.

You can obtain more information on the ORBS RBL server from

<http://www.orbs.org/>.

You can enable use of one or more of these RBL servers by clicking the checkbox to the left of the particular name. You can also use the Add and Remove buttons to configure other RBL servers.

Addresses you enter in the RBL list must reference a special-purpose DNS server that is specifically designated as an RBL server. A normal DNS server will not function correctly.

You may find additional RBL servers at the following Web sites:

- <http://www.mail-abuse.org>
- <http://www.orgs.org>
- <http://www.abuse.net>

Known Characteristics Check

Typically, spam messages share one or more characteristics found in the message header. The indicators are frequently a by-product of the spammers' desire to hide their address and avoid a deluge of bounced mail and irritated replies. Examples of known characteristics 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 an extensive list of known characteristics. 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 patterns. If a pattern is found, SpamScreen marks the message as spam.

Valid Sender Address

To escape complaints, many spammers send e-mail messages from domains that do not exist and are therefore impossible to reply to. To detect this, SpamScreen attempts to validate addresses in the From and Reply-To headers. It does this by querying the configured DNS name server for a Mail Exchanger (MX) record for any domains in those headers. If an MX record does not exist, 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)
v4.10.B481 Copyright (C) 1996-2000 WGTI WGTI

Found spam from 127.0.0.1 (faux-MS bulk emailer;
no MX record for sender [noname.com])

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-SpamScreen” 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 your 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-command`
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.

DNS Errors

Errors and diagnostic logs relating to DNS queries are of the format:

query #*N* to *Server* for *Domain*: ...

where:

N is the query number assigned by SpamScreen.

Server is the DNS server configured to handle SpamScreen.

Domain is either the domain of the RBL server or the MX server.

Common errors include:

DNS Error Message	Meaning
can't connect to DNS socket error in sending query error in receiving response	An error occurred while attempting to send a request or receive a response from the DNS name server. Make sure the Firebox is configured with the address of a working name server.
no server to query	No DNS name server was configured. Make sure the Firebox is configured with the address of a working name server.
nameserver responded with error	The name server received an unexpected error while processing the request.
timed out — resending	The DNS request timed out, and was resent. This may happen if the Firebox is misconfigured, the DNS server is not working, or downstream DNS servers were unable to look up a domain name quickly enough.
too many tries	Several DNS requests were made, and none completed. This may happen if there are misconfigured downstream DNS servers.

Info Logs

These are log messages that SpamScreen generates when spam is detected or overridden.

Message	Meaning
Found spam from <i>server-IP (reason)</i> from <i>user@domain</i> Where <i>server-ip</i> is the IP address of the sending SMTP server, <i>reason</i> explains why SpamScreen marked the message as spam and <i>user@domain</i> is the sender of the message.	The message was determined to be spam, based on the SpamScreen rules.
<i>user@domain</i> overrides spam list Where <i>user@domain</i> is the sender of the message	The sender address was found on the exceptions list, and spam checks were skipped.

Troubleshooting

I installed SpamScreen but the command doesn't appear in the Setup menu
The SpamScreen command appears only in the Policy Manager Advanced view. To toggle from the Basic to the Advanced view, select **View⇒ Advanced**.

Copyright and Patent Information

Copyright© 1998 - 2000 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, Firebox, LiveSecurity, and SpamScreen are either a trademark or registered trademark of WatchGuard Technologies, Inc. in the United States and other countries. This product is covered by one or more pending patent applications.

DocVer S-1.2-SpamScreen-1

