



# Best Practices

## SurfControl E-mail Filter for SMTP

*v5.2*

---



- 
- 
- **Notice**

## NOTICE

© 2006 SurfControl. All rights reserved. SurfControl, SurfControl E-mail Filter, Enterprise Threat Shield, SurfControl Web Filter, SurfControl RiskFilter, SurfControl Mobile Filter, SurfControl Report Central, Single Management Console, Virtual Control Agent, Anti-Spam Agent, Anti-Virus Agent, Virtual Learning Agent, Virtual Image Agent, and the LexiMatch logos are registered trademarks and trademarks of SurfControl plc. All other trademarks are properties of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner.

SurfControl E-mail Filter for SMTP manages the risks and emerging threats that are inherent to e-mail access in the workplace -- risks such as spam, viruses, phishing, and spyware -- while protecting your network from leakage of confidential or sensitive information. Scalable to any size, SurfControl E-mail Filter manages employees' e-mail usage and significantly reduces security threats, legal liability, productivity loss, and network abuse.

## HOW TO USE THIS GUIDE

**This guide provides SurfControl's specific recommendations for getting your system up and running, and can help optimize performance in most environments.** Use this guide to walk through the initial configuration after you install or upgrade.

This document contains several references to the SurfControl Knowledge Base. Each article is hot-linked to the Knowledge Base as [KBarticlenuumber](#) (for example, [KB1053](#)). Click the link to view the correlating article.

For deployment and load balancing recommendations, refer to the technical white paper, [Deploying SurfControl E-mail Filter for SMTP](#).

For the purposes of this guide, SurfControl E-mail Filter for SMTP is abbreviated to "E-mail Filter."

## SERVER CONFIGURATION

You configure most of your server settings during installation. The recommendations provided in this Guide refer to accessing or changing these settings after the install. For detailed instructions about the installation itself, refer to the [SurfControl E-mail Filter Installation Guide](#)

You can access your system settings by clicking the **Server Configuration** button in the Monitor. Server Configuration options include Pre-Screening settings, user and queue settings for message administration, and routing options.

## RECEIVE SERVICE SETTINGS

The Receive Service is where you configure your SMTP and connection properties, and where you establish which pre-screening features you want to use.

## Configuration

The SMTP Properties settings effect how E-mail Filter receives e-mail; the Connections settings effect how much e-mail gets processed at any one time. For best results, leave the SMTP Properties and Connections settings at their defaults. Figure 1 displays the default Connections settings.



Figure 1 Recommended Connection Settings

## Pre-Screening

In addition to the SMTP and connection settings, the Receive service is also where you configure your e-mail connection management options, as shown in Figure 2. By pre-screening e-mail, you can eliminate certain threats and other unwanted content before the e-mail passes through your enabled rules. E-mail Filter's pre-screening features help to increase efficiency and performance.

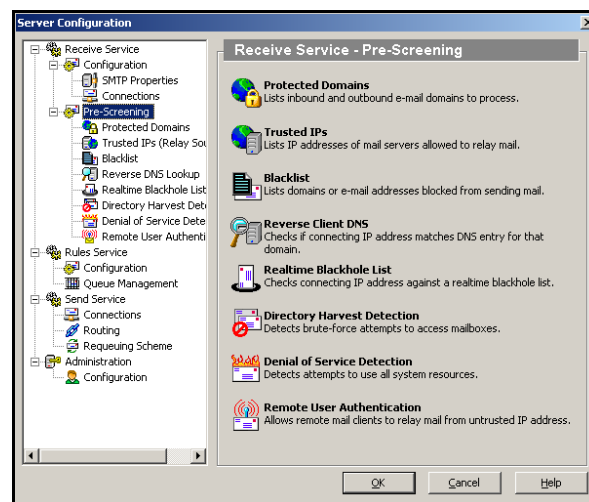


Figure 2 Receive Service Pre-Screening Options

**E-mail Connection Management Settings.** The following settings help prevent spam, viruses, directory harvest attacks, and other threats from entering your network. SurfControl recommends that you enable the following pre-screening options as directed below.

**Note:** These features require that you deploy E-mail Filter upstream from an anti-virus or other receiving mail server. In order to use the following features:

- The E-mail Filter server must receive e-mail directly from the Internet.
- Your firewall must be configured to allow e-mail directly to the E-mail Filter server.

- **Blacklist.** A blacklist is an administrator-defined anti-spam tool that blocks e-mail from specified sources. Use this area to enter or import domains or e-mail addresses of sources from whom you do not want to receive e-mail. This is an effective way to block unwanted messages as soon as they enter E-mail Filter.

You can also provide exclusions to your blacklist. For example, if the domain xyz.com is on your blacklist, but you still want to receive e-mail from user1@xyz.com, you can enter user1@xyz.com on the Exclusions list and still receive e-mail from that user.

- **Reverse DNS Lookup.** The Reverse DNS Lookup feature can help detect spoofed e-mail by confirming that the sender's PTR record matches the IP address included in the header.

SurfControl recommends that you enable this option and leave the default action of **Log Only**. This allows you to take advantage of the Reverse DNS Lookup feature, but does not deny e-mail from sources that may have mis-configured DNS settings or have no PTR record. The **Log Only** option generates a log if there is a mismatch between the IP address and the domain name, but does not reject e-mail; this option lets you keep track of e-mail sent from illegitimate addresses.

- **Realtime Blackhole List (RBL).** This feature allows E-mail Filter to handshake with third-party “real-time blackhole lists,” (RBLs) which are externally hosted lists of known spammers.

The Anti-Spam Agent and most other spam layers of E-mail Filter perform spam blocking in the Rules service. If you use an RBL service and would like to eliminate a significant portion of spam before it enters the Rules service, SurfControl recommends that you enable RBL lookups and set the action to **Deny Connection**.

When RBL lookups are enabled and set to Deny Connection, E-mail Filter checks the sending host's IP address against the RBL, verifying that the IP address is not on the spam list. If the IP address is on the list, E-mail Filter drops the connection. If not, E-mail Filter continues to process the e-mail.

If you have enabled this option, you can enter domains, e-mail addresses, or IP addresses in the Exclusions list. This list contains senders for whom you do not want to perform the RBL lookup.

- 
- 
- **Server Configuration**

**Note:** If you enter the IP address of the RBL server on either the RBL list or the RBL Exclusions list, you must also enable **Reverse DNS Lookup**.

For more information on RBLs and the RBL Exclusions list, refer to [KB1053](#).

- **Directory Harvest Detection.** This feature protects your network from directory harvest and phishing attacks, and stops a significant amount of e-mail-based threats from entering your network. By integrating with your LDAP server, the Directory Harvest Detection feature ensures that incoming e-mail is addressed to users who are currently in your Active Directory structure.

SurfControl recommends that you enable this feature and leave the default action of **Deny connections from IP for: 24 hours**. With this option enabled, if E-mail Filter detects a directory harvest attack (defined by the number of invalid connections or addresses per hour), E-mail Filter blocks all e-mail from that source for the next 24 hours.

For details on using this feature in an environment with multiple LDAP servers, refer to [KB1536](#).

- **Denial of Service Detection.** This feature detects attempts to use all your system resources. SurfControl recommends that you enable this feature, and increase the setting of **5 maximum incomplete sessions from each IP per hour** to **50**.

At these default settings, E-mail Filter detects a denial of service attack if there are five incomplete sessions from one IP address per hour. If E-mail Filter detects a denial of service attack, E-mail Filter blocks all connections from that IP address for the next 24 hours.

## RULES SERVICE SETTINGS

The Rules service is what performs the bulk of message processing. The Rules service performs automatic actions on the e-mail (such as extracting all archive files, decompressing embedded objects, and parsing out HTML) and then passes the e-mail through your set of enabled rules.

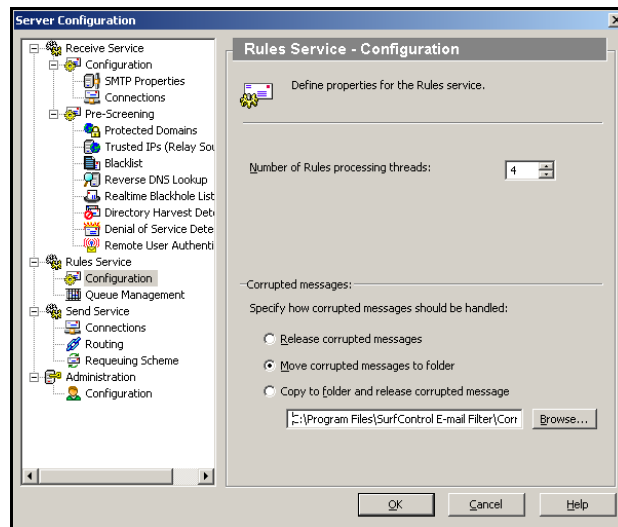
The Rules service area of the Server Configuration interface is where you configure how the Rules service interacts with e-mail; actual rule policy is established in the Rules Administrator. (See page 7 for recommended enabled rules.)

### Configuration

The Configuration area of the Rules service is where you define the settings for how the Rules service processes e-mail.

The Rules Processing Thread setting specifies the number of messages that the Rules service can process at any one time. For example, using the default setting of 4 means that the Rules service can check four e-mails at the same time. SurfControl recommends that you leave the default at **4**.

If an e-mail is corrupted, the Rules service may not be able to process it normally. For optimal handling of corrupted messages, SurfControl recommends that you select **Move corrupted messages to folder** and create a folder for corrupted messages, as shown in Figure 3. This quarantines corrupted messages for later review and prevents them from being delivered.



**Figure 3** Recommended Rules Service Configuration

## Queue Management

By default, E-mail Filter quarantines e-mail into Isolate queues when an e-mail triggers your enabled rules. The Queue Management area of the Server Configuration interface gives you many options for managing these and custom queues, for managing queue administrator accounts, and for managing the contents of the queues as they grow.

E-mail Filter's Automated Queue Management feature helps to optimally and automatically manage your queues. This feature regularly releases, deletes, or moves isolated e-mails on a time schedule, and greatly reduces administrative overhead. Although you can configure some of your Isolate queues for automated queue management during the installation, **SurfControl strongly recommends that you configure all Isolate queues for Automated Queue Management.**

A queue should not contain over 10,000 e-mails at any one time. SurfControl recommends that you configure each queue for Automated Queue Management, so the queues never exceed the recommended size.

As you schedule each queue for Automated Queue Management, make sure to also enable **Administrator alerts** for that queue, and specify the alert to occur when the queue reaches **10,000 messages**.

For details on how to configure Automated Queue Management, refer to [KB1304](#).

## SEND SERVICE SETTINGS

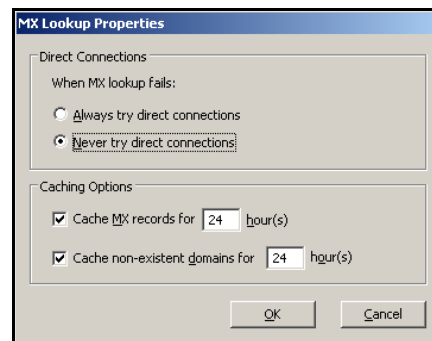
The Send service is what relays e-mail to the next server for delivery; the Send service area of the Server Configuration dialog box is where you can configure the appropriate routing if you did not configure it during the installation.

For details on configuring Send service routing, refer to page 68 of the [SurfControl E-mail Filter Administrators' Guide](#).

When you are configuring these settings, you can choose between a static route that you define, or a route based on MX records obtained when E-mail Filter performs an MX Lookup. If you are using MX lookups, perform the configuration described below.

### MX Lookups

If you are using MX lookups, SurfControl recommends that you configure E-mail Filter to **never try direct connections** for undefined routes when a connection fails, as shown in Figure 4. This ensures optimal performance.



**Figure 4** Recommended MX Lookups Properties

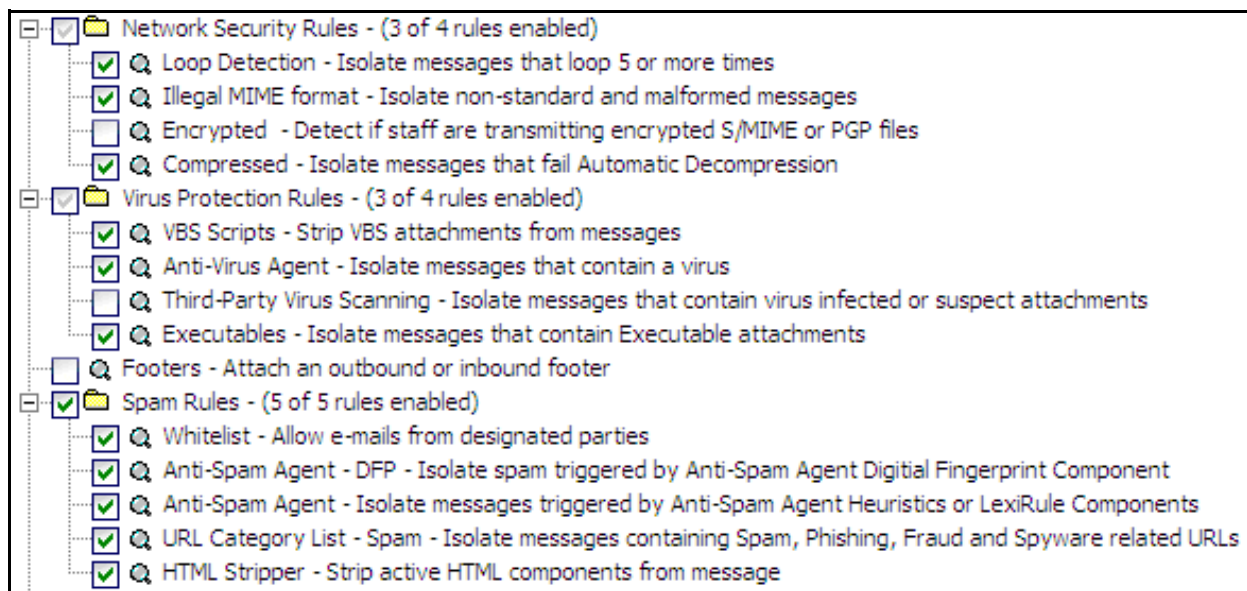
To perform this configuration:

- 1 Under Routing, select **Use MX records**.
- 2 Click **Configure....**
- 3 Under Direct Connections, select **Never try direct connects**.

## RULE CONFIGURATION

SurfControl E-mail Filter's default rules provide out-of-the-box protection from spam, viruses, and leakage of confidential information. E-mail Filter's innate granularity allows you to customize the pre-built rules, or simply enable them at their default settings. You can auto-enable the Network Security, Spam, and Virus rules during the installation. If you are performing a fresh installation, SurfControl recommends that you enable the pre-configured rules during the install.

Regardless of whether you enabled rules during the installation or have performed an upgrade, SurfControl recommends that you make sure the following rules are enabled, as shown in Figure 5.



**Figure 5** Recommended Enabled Rules

If this is a fresh installation, you may want to disable some of the default rules, as shown above. For optimal filtering with the least amount of false positives, SurfControl recommends that you enable the following default Network Security, Virus Protection, and Spam rules.

### RECOMMENDED NETWORK SECURITY RULES

SurfControl recommends that you enable the following Network Security rules.

#### Loop Detection

This rule detects looping messages between two or more e-mail servers, and isolates looping messages into the Network Security queue.

- 
- 
- **Rule Configuration**

## Illegal MIME Format

The Illegal MIME Format rule detects messages and attachments that do not pass SurfControl E-mail Filter's rigorous DeMIME-ing process, and isolates non-standard or malformed messages into the Network Security queue.

## Compressed

The Rules service automatically decompresses archived files. The Compressed rule isolates any e-mail that fails this automatic decompression into the File Formats folder.

## RECOMMENDED VIRUS PROTECTION RULES

SurfControl recommends that you enable the following Virus Protection rules:

### VBS Scripts

This rule protects your network from malicious content by stripping VBS attachments from messages.

### ONE of the Virus Scanning Rules

If you are not using an upstream virus scanner, SurfControl recommends that you enable either of the following rules:

- **Anti-Virus Agent.** The Anti-Virus Agent helps protect your system by deleting viruses and cleaning infected files when they occur. It uses a McAfee Anti-Virus engine to detect files that could damage your system.

The Anti-Virus Agent is an additional subscription to the Anti-Spam Agent. If you are running an evaluation copy of SurfControl E-mail Filter, you can use the Anti-Virus Agent without an activation key for the 30-day evaluation period. For more information on the benefits of the Anti-Virus Agent, and the different virus scanning options it provides, refer to the [SurfControl E-mail Filter Administrators' Guide](#).

### OR

- **Third-Party Virus Scanning.** The Third-Party Virus Scanning object uses third-party, gateway virus software to detect viruses in e-mail messages and attachments, and can use multiple anti-virus scanners within this rule.

The Third-Party Virus Scanning rule supports the following gateway anti-virus solutions:

- McAfee/Network Associates NetShield.
- Norman Defense Systems.
- Sophos SAVI.
- Symantec (SAVSE).
- Trend InterScan VirusWall.
- IKARUS.

If you are using the Third-Party Virus Scanning rule, you must exclude the following directories from any automatic file level or directory-level scanning performed by your anti-virus software. (Scanning these directories with anti-virus software can interfere with E-mail Filter's performance.)

- C:\Program Files\SurfControl E-mail Filter\**In**.
- C:\Program Files\SurfControl E-mail Filter\**Out**.
- C:\Program Files\SurfControl E-mail Filter\**Work**.
- C:\Program Files\SurfControl E-mail Filter\**Temp**.

## Executables

Since so many viruses are transmitted as executable files, enabling this rule provides another important layer of protection, and is effective even if the executables have been re-named or disguised.

- 
- 
- **Rule Configuration**

## RECOMMENDED SPAM RULES

SurfControl recommends that you enable the following Spam Protection rules:

### Whitelist

The Whitelist rule allows e-mail from administrator-defined parties, bypassing the subsequent enabled rules. SurfControl recommends that you add senders to the whitelist when you know you want to receive e-mail from those sources.

### Anti-Spam Agent -- DFP

This topmost layer of the Anti-Spam Agent stops spam with perfect accuracy. Using Digital Fingerprinting (DFP) technology, this rule references the Anti-Spam Agent DFP database, which is a SurfControl-maintained database of digital spam fingerprints. If an e-mail comes into your network and matches one of the fingerprints in the DFP database, SurfControl isolates it into the **Anti-Spam Agent -- DFP** folder.

Because of the reliability of the Digital Fingerprinting database, SurfControl recommends that you configure the **Anti-Spam Agent -- DFP** queue for automated queue management, and configure this queue to automatically purge each isolated e-mail after a three-day delay.

### Anti-Spam Agent for Heuristics and LexiRules

This rule contains two components designed to proactively stop spam threats that are too new to be in the DFP database. The Heuristics layer analyzes the entire e-mail, performing a series of tests that determine how closely an e-mail resembles spam. The LexiRules layer contains rules designed to target specific spam outbreaks.

### URL Category List (Internet Threat Database)

This rule leverages SurfControl's Internet Threat Database (also embedded in SurfControl Web Filter) to block e-mail that contains URLs or IP addresses relating to spyware, adult, and gambling-related sites.

### HTML Stripper

This rule strips active HTML components from e-mail. Active content, commonly used in spyware, is code that can execute on a client PC (such as JavaScript / VBScript, Java Applets or ActiveX objects). Active content can also include malicious actions executed by the mail client when the user is viewing the message.

### End User Spam Management

SurfControl End User Spam Management (EUSM) allows end users to delete or release their own spam. Specifically designed for spam that is isolated by an anti-spam layer other than Digital Fingerprints, EUSM can be an important part of message administration, as it distributes the overhead of reviewing spam among all users in your network.

If you use EUSM, SurfControl recommends that you do not apply EUSM to the Anti-Spam Agent - DFP rule.

For more information on installing and configuring EUSM, refer to the [EUSM Installation and Administrator's Guide](#).

## SCHEDULED UPDATES AND EVENTS

During the installation, E-mail Filter schedules regular updates for the Anti-Spam Agent, the URL Category List, and the Anti-Virus Agent (if you have purchased or are evaluating the Anti-Virus Agent).

SurfControl recommends that you increase the default scheduled updates, as shown in Table 1.

**Table 1**

Event	Frequency
Anti-Virus Agent Update	Hourly
Anti-Spam Agent Update	Every two hours
URL Category List Update	Once daily
Queue Synchronization	Once daily

### Anti-Virus Agent Updates

SurfControl updates the Anti-Virus Agent with McAfee's virus definitions every 15 minutes.

If you are using the Anti-Virus Agent, SurfControl recommends that you obtain updates to the Anti-Virus Agent hourly.

### Anti-Spam Agent Updates

Anti-Spam Agent updates include the latest digital spam fingerprints, Heuristics, and LexiRules. SurfControl updates these databases continuously, and recommends that you configure Anti-Spam Agent updates to occur every two hours. This frequency ensures that you receive any emergency updates SurfControl releases in response to spam outbreaks.

### URL Category List Updates

SurfControl updates the URL Category List (Internet Threat Database) continuously. By default, updates to the URL Category List occur daily, and SurfControl recommends that you keep this configuration.

### Queue Synchronization

Synchronize Queues Daily is a default event that synchronizes the contents of Isolate queues with the listing in the log database. This improves the performance of the Message Administrator and maintains the integrity between your database and message files.

By default, queue synchronization occurs daily; in most cases, this is the best configuration.

## DATABASE MAINTENANCE AND CONNECTIVITY

In order to maintain SurfControl E-mail Filter at its optimum level of performance (and to prevent your system from crashing or hanging), SurfControl recommends that you implement the database maintenance schedule listed below.

**Note:** MSDE has a 2 GB size limit. If you are using an MSDE database, be sure that your database maintenance plan keeps your database at under 2 GB.

Use the guidelines listed in Table 2 for performing database maintenance.

**Table 2** Recommended Database Maintenance Plan

Action	Method	Frequency
Archive STEMLog database	SurfControl Scheduler	Monthly
Archive STEMConfig database	Windows Scheduled Tasks  Use SEFDBBackup.bat to configure this event (located by default in C:\Program Files\SurfControl E-mail Filter\Database).	Weekly
Purge STEMLog database (to occur after the archive)	SurfControl Scheduler	Weekly
Shrink STEMLog database (to occur after the purge)	SurfControl Scheduler	Weekly

### PURGE RECOMMENDATIONS

In order to retain data for a reasonable period of time, SurfControl recommends that when you schedule your purge, you select **Purge data older than 30 days** within the Scheduler -- a setting that allows you to keep a month's worth of data even though you are purging the database weekly.

Also, when performing a purge, make sure that you have enough disk space for the purge to be successful. (The available disk space on your server should be twice the size of the database.)

### DATABASE SIZING

The size of your database correlates to the number of e-mails your organization receives per day, and to the length of time you plan to retain the logged data (used for message administration and reporting purposes). To size your database appropriately, SurfControl estimates that each e-mail generates approximately 1 KB of log data stored in the database. (This calculation is also helpful when determining whether MSDE is sufficient in your environment.)

For more information on database sizing and deployment scenarios, refer to the [SurfControl E-mail Filter Deployment Guide](#).

## CONNECTING TO THE DATABASE

By default, SurfControl E-mail Filter uses SQL authentication. If you have changed your authentication method to Windows authentication, you must change the Scheduler and Administration services to run as accounts with database administrative privileges.

To perform this configuration:

- 1 From the **Start** menu, select **Settings, Control Panel**.
- 2 Open **Administrative Tools, Services**.
- 3 Double-click **SurfControl E-mail Filter Scheduler**.
- 4 In the **Log On** tab, select **This account** and click **Browse**.
- 5 Select an account that has database administrative privileges.
- 6 Make sure you have entered the correct password, and click **OK**.
- 7 Double-click **SurfControl E-mail Filter Administrator Server**.
- 8 In the **Log On** tab, select **This account** and click **Browse**.
- 9 Select an account that has database administrative privileges.
- 10 Make sure you have entered the correct password, and click **OK**.