



# Microsoft Exchange Intelligent Message Filter Deployment Guide

Product Version: Exchange Server 2003  
Reviewed by: Exchange Product Development  
Latest Content: [www.microsoft.com/exchange/library](http://www.microsoft.com/exchange/library)  
Author: Exchange Documentation Team





# Microsoft Exchange Intelligent Message Filter Deployment Guide

**Patricia Anderson**

**Published:** April 2004

**Applies to:** Exchange Server 2003

## **Copyright**

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2004 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows Server, Active Directory, and Outlook are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

## **Acknowledgments**

**Project Editor:** Cathy Anderson

**Contributing Editors:** Tony Ross, Lee Ross

**Technical Reviewers:** Simon Attwell

**Graphic Design:** Kristie Smith

**Production:** Sean Pohtilla

# Table of Contents

<b>Introduction .....</b>	<b>1</b>
How Is This Book Structured? .....	1
<b>Chapter 1</b>	
<b>Understanding Intelligent Message Filter .....</b>	<b>3</b>
Overview of Intelligent Message Filter .....	3
How Intelligent Message Filter Works.....	3
How Intelligent Message Filter Works with Exchange 2003 and Outlook Filtering Features .....	4
<b>Chapter 2</b>	
<b>Planning Your Intelligent Message Filter Deployment.....</b>	<b>7</b>
Securing Your Gateway SMTP Virtual Servers .....	7
Deploying in a Multiple Forest Scenario .....	8
Enabling Cross-Forest Authentication.....	8
Step 1: Creating a User Account in the Destination Forest with Send As Permissions .....	9
Step 2: Creating a Connector in the Connecting Forest .....	10
<b>Chapter 3</b>	
<b>Installing Intelligent Message Filter .....</b>	<b>13</b>
<b>Chapter 4</b>	
<b>Configuring and Enabling Intelligent Message Filter.....</b>	<b>15</b>
Determining the Appropriate Thresholds for Intelligent Message Filter .....	15
Configuring Intelligent Message Filter .....	16
Configuring Intelligent Message Filter at the Gateway .....	17
Configuring Intelligent Message Filter at the Mailbox Store.....	18
Enabling Intelligent Message Filter on SMTP Virtual Servers.....	18
<b>Chapter 5</b>	
<b>Monitoring and Troubleshooting Intelligent Message Filter .....</b>	<b>21</b>
Using Event Viewer.....	21
Using System Monitor and Performance Logs and Alerts .....	23

## **Chapter 6**

### **Customizing Intelligent Message Filter ..... 25**

Changing the Archive Location.....	25
Storing the SCL Rating with Archived Messages.....	25
Filtering Messages Sent through Authenticated Connections .....	26
Setting the Size of Spam Rules.....	26

## **Appendix A**

### **Additional Resources ..... 31**

Exchange Server 2003 Technical Papers.....	31
Other Resources.....	31
Microsoft Knowledge Base Articles.....	31

# Introduction

Microsoft® Exchange Intelligent Message Filter is a product developed by Microsoft to help companies reduce the amount of unsolicited commercial e-mail (UCE), also known as spam, received by users. This book explains how to deploy and configure Intelligent Message Filter in your Microsoft Exchange Server 2003 organization.

---

## How Is This Book Structured?

This book has six chapters and one appendix. For best results, review these chapters in order, as each chapter builds upon the concepts revealed in preceding chapters.

**Chapter 1, "Understanding Exchange Intelligent Message Filter"**

This chapter explains what Intelligent Message Filter is, its underlying technology, and how it detects and filters UCE at the gateway and on Exchange mailbox stores.

**Chapter 2, "Planning Your Intelligent Message Filter Deployment"**

This chapter contains deployment recommendations for Intelligent Message Filter.

**Chapter 3, "Installing Intelligent Message Filter"**

This chapter guides you through the process of installing Intelligent Message Filter.

**Chapter 4, "Configuring and Enabling Intelligent Message Filter"**

This chapter explains how you configure various options for Intelligent Message Filter and how you enable content filtering on your SMTP virtual servers.

**Chapter 5, "Monitoring and Troubleshooting Intelligent Message Filter"**

This chapter focuses on monitoring and troubleshooting tips for Intelligent Message Filter.

**Chapter 6, "Customizing Intelligent Message Filter"**

This chapter explains how you can customize various settings for Intelligent Message Filter.



# Understanding Intelligent Message Filter

This chapter provides a general overview of Microsoft® Exchange Intelligent Message Filter. This chapter also explains how Intelligent Message Filter works in an Exchange organization on Exchange gateway servers and on Exchange mailbox stores.

---

## Overview of Intelligent Message Filter

Intelligent Message Filter is based on patented machine learning technology from Microsoft Research. During its development, Intelligent Message Filter learned distinguishing characteristics of legitimate e-mail messages and unsolicited commercial e-mail (UCE) . This learning was based on e-mail messages submitted by Microsoft partners and classified as either legitimate messages or UCE.

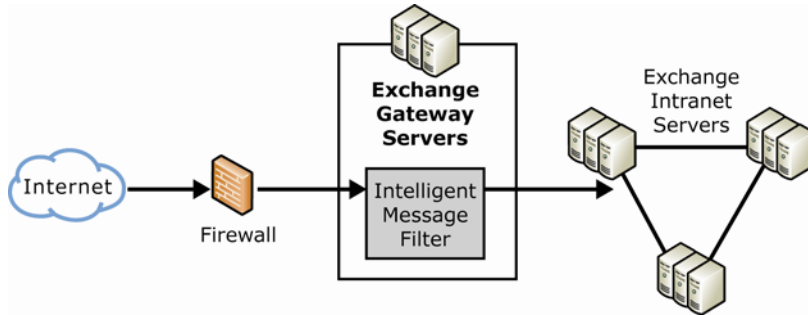
Based on the characteristics of millions of messages, Intelligent Message Filter recognizes indicators of both legitimate messages and UCE messages. Intelligent Message Filter can make an accurate assessment of the probability that an incoming e-mail message is either a legitimate message or UCE. Unlike many other filtering technologies, Intelligent Message Filter uses characteristics from a statistically sound sample of e-mail messages. In addition to UCE , the inclusion of legitimate messages in this sample reduces the likelihood of mistakes. Because Intelligent Message Filter recognizes characteristics of both legitimate and UCE messages, the accuracy of Intelligent Message Filter is increased.

---

## How Intelligent Message Filter Works

In a typical Exchange Server 2003 topology, e-mail servers that are connected to the Internet are deployed at the Internet perimeter and are isolated from the enterprise intranet. These e-mail servers (known as gateway servers), accept incoming Internet e-mail messages and forward these messages to the appropriate mailbox server. Generally, gateway servers do not contain user mailboxes. However, in smaller organizations, a gateway server may also contain user mailboxes. Intelligent Message Filter is installed on these gateway servers to filter incoming Internet e-mail messages. If you use a non-Microsoft e-mail system as your Internet gateway server, you should install Intelligent Message Filter on the Exchange bridgehead server that accepts incoming Internet e-mail messages from your gateway servers.

A typical Exchange Server 2003 topology is shown in Figure 1.1.



**Figure 1.1 Exchange server topology with Intelligent Message Filter installed**

When an external user sends e-mail messages to an Exchange server with Intelligent Message Filter installed, Intelligent Message Filter evaluates the textual content of the messages and assigns the message a rating based on the probability that the message is UCE. This rating is stored as a message property called a spam confidence level (SCL) rating with the message itself. This rating is persisted with the message when the message is sent to other Exchange servers.

An administrator sets two thresholds that determine how Intelligent Message Filter handles e-mail messages with various SCL ratings: a gateway threshold with an associated action to take on messages above this threshold, and a mailbox store threshold. If a message has a rating higher than the gateway threshold, Intelligent Message Filter takes the action specified. If the message has a rating below the gateway threshold, the message is sent to the Exchange mailbox store of the recipient. At the Exchange mailbox store, if the message has a higher rating than the mailbox store threshold, the mailbox store delivers the message to the user's Junk E-mail folder rather than to the Inbox.

## How Intelligent Message Filter Works with Exchange 2003 and Outlook Filtering Features

Exchange 2003 provides a set of filtering features, which are also used to reduce UCE. These features are sender, recipient, and connection filtering. Each of these Exchange filters is checked during the SMTP session, when a connecting SMTP server attempts to send e-mail messages to an Exchange server. Intelligent Message Filter is applied after the SMTP session. Any e-mail messages filtered by recipient, sender, or connection filtering are handled individually and do not go through Intelligent Message Filter.

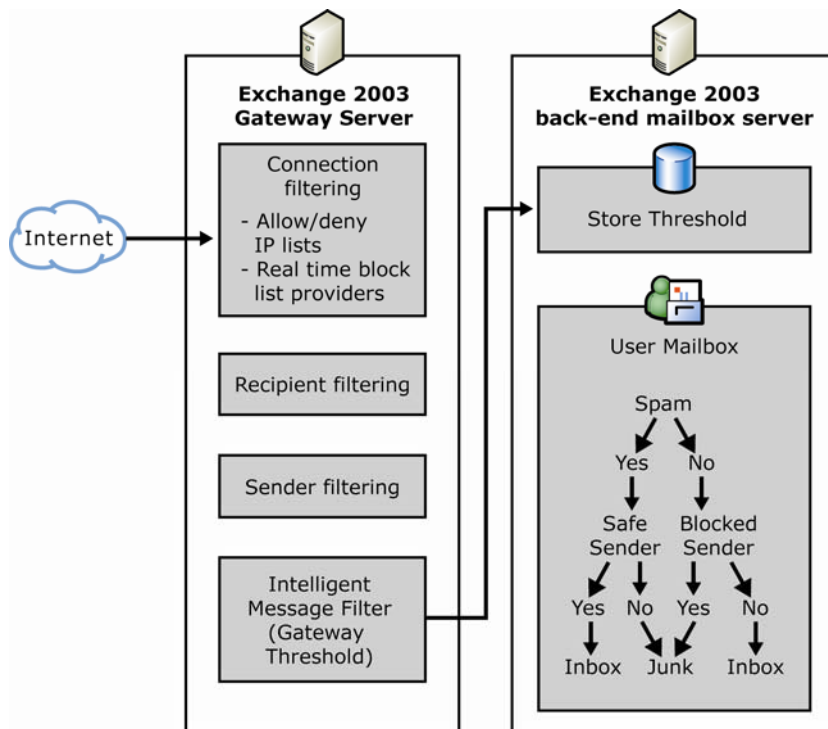
On the client side, Microsoft Office Outlook® 2003 and Microsoft Office Outlook Web Access for Exchange Server 2003 allow users to create a list of safe senders from whom they always want to accept e-mail messages and a list of blocked senders from whom they always want to reject e-mail messages. At the mailbox store, regardless of the SCL rating assigned to the message, Exchange delivers all messages from safe senders to the user's Inbox and all messages from blocked senders to the user's Junk E-mail folder. However, if the e-mail message has been blocked by the gateway threshold, it is not delivered to the user's Inbox because it is never delivered to the mailbox store.

If a user is running an earlier version of Outlook, the safe senders and blocked senders lists are not available. Any message marked as spam is delivered directly to the user's Inbox.

### Note

If your users run an earlier version of Outlook, but can use Outlook Web Access 2003, they can configure safe senders and blocked senders lists in Outlook Web Access.

Figure 1.2 illustrates how Intelligent Message Filter works with these Exchange and Outlook features.



**Figure 1.2 Message flow with Intelligent Message Filter and Exchange filtering**

As shown in Figure 1.2, filters are applied in the following order:

1. An SMTP server connects to Exchange and initiates an SMTP session.
2. During the SMTP session, Exchange applies connection filtering using the following criteria:
  - a. Connection filtering checks the global accept list. If an IP address is on the global accept list, no other connection, recipient, or sender filtering is applied, and the message is accepted.
  - b. Connection filtering checks the global deny list. If the IP address of the sending server is found on the global deny list, the message is automatically rejected and no other filters are applied.
  - c. Connection filtering checks the real-time block lists of any providers that you have configured. If the sending server's IP address is found on a block list, the message is rejected and no other filters are applied.
3. After connection filtering is applied, Exchange checks the sender address (the P1 information specified in the SMTP conversation by the MAIL FROM command) against the list of senders you configured in sender filtering. If a match is found, Exchange rejects the message and no other filters are applied.
4. Exchange checks the recipient against the recipient list that you have configured in recipient filtering. If the intended recipient matches an e-mail address that you filter, Exchange rejects the message and no other filters are applied.
5. After recipient filtering is applied, Exchange checks the resolved sender address (the P2 data) against the list of senders you configured in sender filtering. If the sender matches an address on the sender list, Exchange filters the message based on the options you configured and no other filters are applied.
6. If a message is not filtered by connection, recipient, or sender filtering, Intelligent Message Filter is applied, and one of two things happens at the gateway:
  - If Intelligent Message Filter assigns the message an SCL rating that is higher than your gateway threshold, Intelligent Message Filter takes the appropriate gateway action.
  - If Intelligent Message Filter assigns the message an SCL rating that is lower than or equal to your gateway threshold, the message is passed to the Exchange server with the user's mailbox store.

7. If a user is using Outlook 2003 or Outlook Web Access with Exchange 2003, the user's mailbox store compares the message's SCL rating with the store threshold you configured, and one of two things happens:
  - If the message rating is lower than or equal to the store threshold, the mailbox store checks the user's blocked senders list configured in Outlook or Outlook Web Access, and one of two things happens:
    - If the sender of the message is not on a blocked senders list configured in Outlook or Outlook Web Access, or if a blocked senders list is not available or defined, the message is delivered to the recipient's Inbox.
    - If the sender appears on the blocked senders list configured in Outlook or Outlook Web Access, the message is delivered to the user's Junk E-mail folder.
  - If the message rating is higher than the store threshold, the mailbox store checks the user's safe senders list configured in Outlook or Outlook Web Access, and one of two things happens:
    - If the sender appears on the safe senders list, the message is delivered to the recipients Inbox.
    - If the sender does not appear on the safe senders list or if a safe senders list is not available or defined, the message is delivered to the recipient's Junk E-mail folder.

**Important**

If your users are using versions of Outlook earlier than Outlook 2003, the mailbox store thresholds have no effect and messages filtered in Step 7 are instead delivered to the users' Inboxes. However, if your clients can access e-mail using Outlook Web Access 2003, the store thresholds are applied as described in Step 7.

# Planning Your Intelligent Message Filter Deployment

Microsoft® Exchange Intelligent Message Filter is designed to identify messages that are likely to be unsolicited commercial e-mail (UCE). When administrators use Intelligent Message Filter, they can filter these messages by deleting, archiving, or rejecting them at the gateway, or moving them to a user's Junk E-mail folder on a mailbox store.

To filter UCE effectively, you must deploy Intelligent Message Filter on your Exchange gateway servers that accept incoming Internet e-mail messages. Additionally, Intelligent Message Filter must be enabled on each SMTP virtual server that accepts Internet e-mail messages on your Exchange gateway servers.

If you use non-Microsoft e-mail servers at the gateway to accept Internet e-mail messages, you must deploy Intelligent Message Filter on the Exchange bridgehead servers that accept incoming Internet e-mail messages from the non-Microsoft gateway servers. Additionally, you must enable Intelligent Message Filter on each SMTP virtual server accepting Internet e-mail messages on your Exchange bridgehead servers.

Intelligent Message Filter is not supported on either of the following:

- Exchange 2000 Server or earlier servers
- Exchange Server 2003 clusters

---

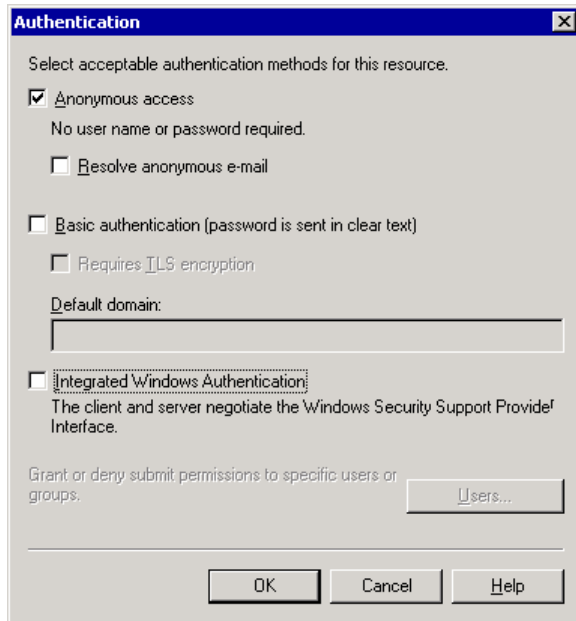
## Securing Your Gateway SMTP Virtual Servers

Dictionary attacks are brute force attacks that use common words as possible passwords to discover valid passwords for well-known accounts, such as the administrator account. Malicious users attempt dictionary attacks to gain access to computers.

To protect your SMTP gateway servers from possible dictionary attacks, you can disable all forms of authentication on your inbound SMTP virtual servers that accept Internet mail. Because no authentication is permitted, malicious users cannot use dictionary attacks to discover passwords and authenticate to your computer to relay mail or perform other unauthorized actions.

### To disable authentication on your SMTP virtual server

1. In Exchange System Manager, expand **Servers**, expand *<your inbound Exchange server>*, expand **Protocols**, and then expand **SMTP**.
2. Right-click your inbound SMTP virtual server, and then click **Properties**.
3. Click the **Access** tab, and then click **Authentication**.
4. In **Authentication**, clear the **Basic authentication** and **Integrated Windows Authentication** check boxes (Figure 2.1).



**Figure 2.1 Authentication dialog box**

If you cannot disable authenticated access on your SMTP virtual server for business reasons, such as a partner company authenticating, perform the following tasks to increase security on your gateway server:

- Enforce a strong password policy for all user accounts, particularly the administrator account.
- Disable the guest account. For more information about disabling this account, see Microsoft Knowledge Base article 320053, "HOW TO: Rename the Administrator and Guest Account in Windows 2000" (<http://go.microsoft.com/fwlink/?LinkId=3052&kbid=320053>). Although this article applies to Microsoft Windows® 2000 Server, similar principles apply for Microsoft Windows Server™ 2003.

---

## Deploying in a Multiple Forest Scenario

In a multiple forest topology where an Internet bridgehead server in one forest accepts e-mail messages for users in another forest, you must enable cross-forest authentication for the spam confidence level (SCL) rating to be sent between forests.

Enabling cross-forest authentication also allows users in each forest to resolve to their display names in the global address list (GAL). To prevent spoofing (forging identities), Exchange 2003 requires authentication before a sender's name is resolved to its display name in the GAL. Therefore, in an organization that spans two forests, a user who sends e-mail messages from one forest to another forest is not authenticated. Furthermore, the user's name is not resolved to a display name in the GAL, even if the user exists as a contact in the destination forest, unless authentication is enabled.

---

## Enabling Cross-Forest Authentication

To enable cross-forest SMTP authentication, you must create connectors in each forest that use an authenticated account from the other forest. After you create these connectors, when e-mail messages are sent between the two forests, the extended properties of the messages are also sent, which allows the SCL rating to be passed to the appropriate mailbox store in the destination forest.

Consider a two-forest environment for A. Datum Corporation and Fabrikam, Inc. With the Adatum forest and Fabrikam forest, users in each forest exist in contacts in the other forest. The following sections discuss how to perform the following steps to set up cross-forest authentication:

1. Create an account in the Fabrikam forest that has Send As permissions. (For all users in the Adatum forest, a contact also exists in the Fabrikam forest. Therefore, this account allows Adatum users to send authenticated e-mail messages.) Configure these permissions on all Exchange servers that will accept incoming e-mail messages from Adatum.
2. On an Exchange server in the Adatum forest, create a connector that requires authentication using this account to send outbound e-mail messages.

Similarly, to set up cross-forest authentication from the Fabrikam forest to the Adatum forest, repeat these steps, creating the account in Adatum and the connector in Fabrikam.

---

## Step 1: Creating a User Account in the Destination Forest with Send As Permissions

Before you set up your connector in the connecting forest, you must create an account in the destination forest (the forest to which you are connecting) that has Send As permissions. Configure these permissions on all servers in the destination forest that will accept inbound connections from the connecting forest. The following procedures show you how to set up an account in the Fabrikam forest and a connector in the Adatum forest, thereby allowing users in the Adatum forest to send e-mail messages to the Fabrikam forest with resolved e-mail addresses.

### To create the account used for cross-forest authentication

1. In the destination forest (in this case, the Fabrikam forest), create a user account in Active Directory Users and Computers. This account must be an active account, but it does not require the following permissions: log on locally or log on through terminal server.
2. On each Exchange server that will accept incoming connections from the connecting forest, configure Send As permissions for this account:

#### Note

Be careful when creating the password policy. If you set the password to expire, ensure that you have a policy in place that changes the password before its expiration date. If the password for this account expires, cross-forest authentication will fail.

- a. Start Exchange System Manager: Click **Start**, point to **All Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
- b. In the console tree, expand **Servers**, right-click an Exchange server that will accept incoming connections from the connecting forest, and then click **Properties**.
- c. In <Server Name> **Properties**, on the **Security** tab, click **Add**.
- d. In **Select Users, Computers, or Groups**, add the account you just created, and then click **OK**.
- e. On the **Security** tab, under **Group or user names**, select the account.
- f. Under **Permissions**, next to **Send As**, select the **Allow** check box (Figure 2.2).

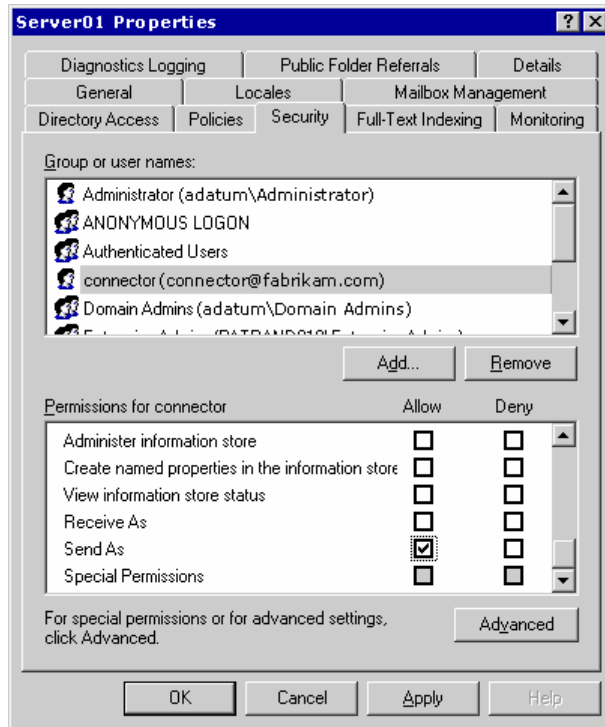


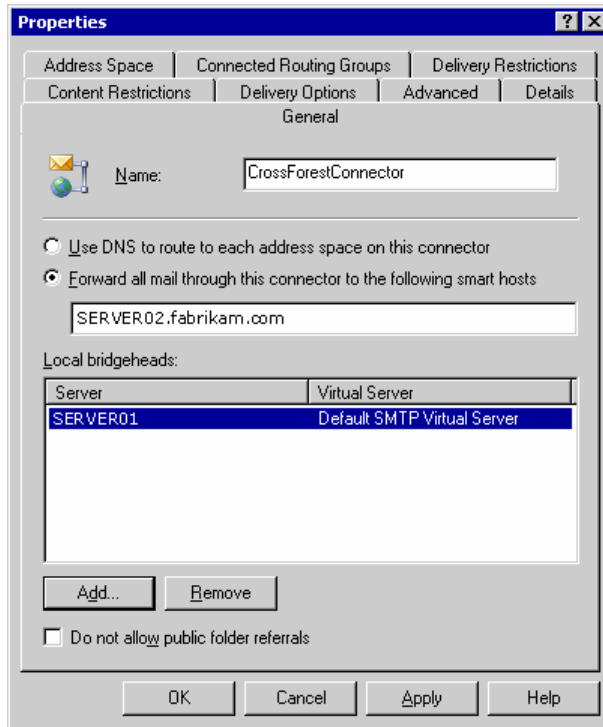
Figure 2.2 Allowing the Send As permission

## Step 2: Creating a Connector in the Connecting Forest

After you create the account with the proper permissions in the destination forest, create a connector in the connecting forest and require authentication using the account you just created. In the following procedure, assume that you are creating a connector on an Exchange server in the Adatum forest that connects to the Fabrikam forest.

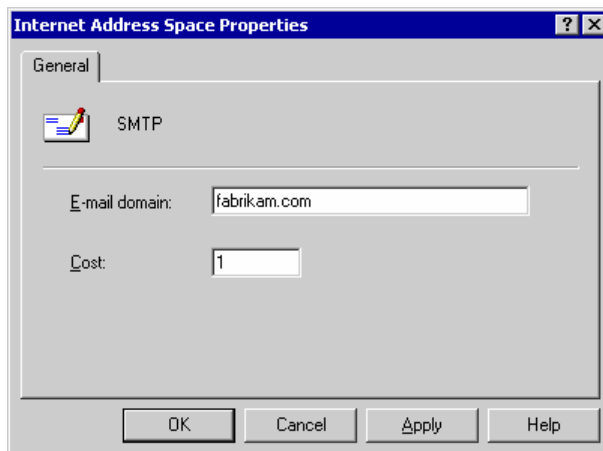
### To configure a connector and require authentication for cross-forest authentication

1. Start Exchange System Manager: Click **Start**, point to **All Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. In the console tree, right-click **Connectors**, point to **New**, and then click **SMTP Connector**.
3. On the **General** tab, in the **Name** box, type a name for the connector.
4. Click **Forward all mail through this connector to the following smart hosts**, and then type the fully qualified domain name or IP address of the receiving bridgehead server.
5. Click **Add** to select a local bridgehead server and SMTP virtual server to host the connector (Figure 2.3).



**Figure 2.3 The General tab in an SMTP virtual server's Properties dialog box**

6. On the **Address Space** tab, click **Add**, select **SMTP**, and then click **OK**.
7. In **Internet Address Space Properties**, type the domain of the forest to which you want to connect, and then click **OK**. In this example, because the connector is sending from the Adatum forest to the Fabrikam forest, the address space matches the domain for the forest, fabrikam.com (Figure 2.4).



**Figure 2.4 The Internet Address Space Properties dialog box**

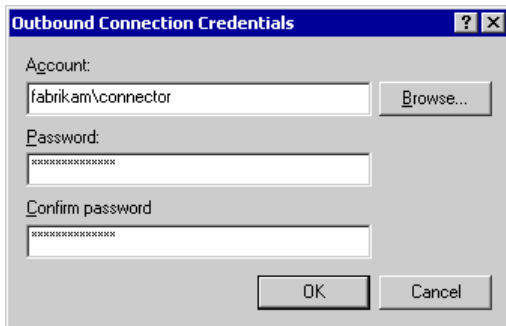
Exchange will now route all e-mail messages destined to fabrikam.com (the Fabrikam forest) through this connector.

8. On the **Advanced** tab, click **Outbound Security**.
9. Click **Integrated Windows Authentication** (Figure 2.5).



**Figure 2.5 The Integrated Windows Authentication button in the Outbound Security dialog box**

10. Click **Modify**.
11. In **Outbound Connection Credentials**, in the **Account**, **Password**, and **Confirm password** boxes, specify an account and password in the destination forest (in this case, Fabrikam) that has Send As permissions and is an authenticated Fabrikam account (Figure 2.6). Use the following format for the account name: *domain\username*, where:
  - *domain* is a domain in the destination forest.
  - *username* represents an account in the destination forest with Send As permissions on all Exchange servers in the destination forest that will accept e-mail messages from this connector.



**Figure 2.6 The Outbound Connection Credentials dialog box**

12. Click **OK**.

# Installing Intelligent Message Filter

Use the wizard to install Microsoft® Exchange Intelligent Message Filter and specify which components you want to install. You can install the Intelligent Message Filter functionality or just the management tools (the user interface that allows you to administer Intelligent Message Filter). If you want to install the functionality on one computer and use another computer to administer and configure Intelligent Message Filter, you can do so.

To install Intelligent Message Filter, use an account that has local administrative rights and a member of a group that has had Exchange Administrators role applied.

**Note**

You can install the management tools on a workstation if you want to remotely administer Intelligent Message Filter on a server. However, the computer must have the Exchange management tools (Exchange System Manager) installed.

**To install Intelligent Message Filter**

1. Start the Intelligent Message Filter Wizard.
2. On the **Welcome** page, click **Next**.
3. On the **End User License** page, read the license agreement. If you agree to the terms, click **I accept**, and then click **Next**.
4. On the **Components** page, select the components that you want to install:
  - **Management Tools for Intelligent Message Filter** includes the user interface for administering Intelligent Message Filter. When you install the management tools, the wizard adds the following user interfaces to Exchange System Management:
    - An **Intelligent Message Filtering** tab in Message Delivery Properties under Global Settings.
    - An **Intelligent Message Filtering** node under the SMTP protocol on the Exchange server where you install Intelligent Message Filter.
  - **Functionality for Intelligent Message Filter** includes the actual Intelligent Message Filter that filters UCE on the server itself. You may choose to install the functionality on a gateway server and administer this functionality using the management tools on another workstation.
5. Click **Next** and continue through the wizard.



# Configuring and Enabling Intelligent Message Filter

After you install Microsoft® Exchange Intelligent Message Filter, you must configure the settings that you want to use in your organization. You must also enable Intelligent Message Filter on each SMTP virtual server that you want to filter unsolicited commercial e-mail (UCE).

---

## Determining the Appropriate Thresholds for Intelligent Message Filter

Chapter 5 discusses the available performance counters that you can use to monitor Intelligent Message Filter and view the distribution of messages with specific SCL ratings. The higher the SCL rating assigned to a message, the more likely the message is spam. To determine the distribution of messages with respective SCL ratings, monitor the **Total Messages Assigned an SCL Rating of X** counters.

### To determine the appropriate thresholds to set at your gateway and mailbox stores

1. In **Global Settings** in **Message Delivery Properties**, under **Gateway Blocking Configuration**, select **No action** in the **When blocking UCE** list.

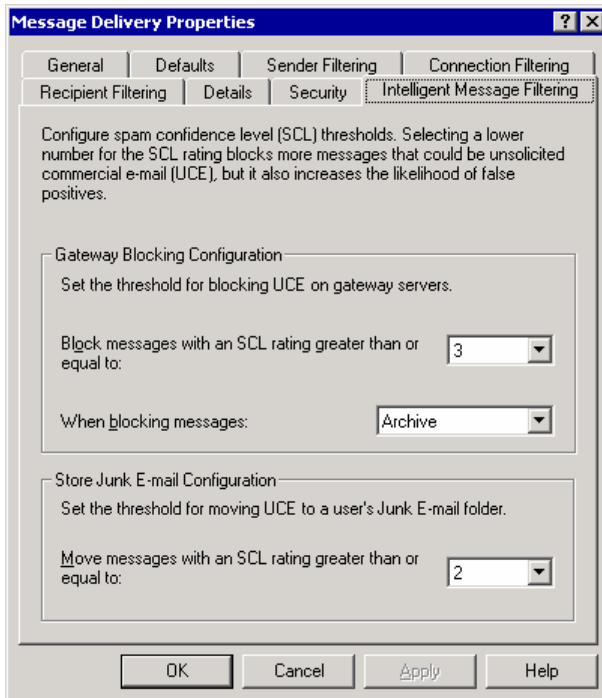
**Note**

When you select **No action**, Intelligent Message Filter still scans each incoming message and assigns it the appropriate SCL rating.

2. Monitor the **Total Messages Assigned an SCL Rating of X** performance counters, and examine the distribution of messages. Look for the highest SCL rating with the largest number of messages.
3. Set the gateway threshold to this SCL rating.
  - In **Message Delivery Properties**, on the **Intelligent Message Filtering** tab, under **Store Junk E-mail Configuration**, set the mailbox store threshold to an SCL rating of mid-range value between 0 and the gateway threshold.
4. Change the gateway action to **Archive**.
  - In **Message Delivery Properties**, on the **Intelligent Message Filtering** tab, under **Gateway Blocking Configuration**, select **Archive** in the **When blocking UCE** list.
5. Monitor and review the blocked content in the archive directory.
6. Adjust the gateway threshold as appropriate based on the monitoring you perform in Step 5.
  - In **Message Delivery Properties**, on the **Intelligent Message Filtering** tab, under **Gateway Blocking Configuration**, select **Reject** or **Delete** in the **When blocking UCE** list.

# Configuring Intelligent Message Filter

When you install Management Tools for Intelligent Message Filter, the installation package creates a new tab, **Intelligent Message Filtering**, under **Global Settings** in **Message Delivery Properties**. Use the **Intelligent Message Filtering** tab to specify how you want Intelligent Message Filter to handle e-mail messages that it marks as UCE (Figure 4.1).



**Figure 4.1** The Intelligent Message Filtering tab in the Message Delivery Properties dialog box

You configure Intelligent Message Filter using two basic settings:

- In **Gateway Blocking Configuration**, you establish a threshold based on a message's spam confidence level (SCL) rating, above which the gateway server takes action on the message. You also define the type of action you want the gateway to take.
- In **Store Junk E-mail Configuration**, you define the threshold based on a message's SCL rating that Exchange mailbox stores use to determine whether to deliver messages to a user's Junk E-mail folder or to a user's Inbox.

You configure Intelligent Message Filter by setting thresholds for the spam confidence level (SCL) ratings assigned to incoming messages on both the gateway and the Exchange mailbox stores. Intelligent Message Filter evaluates each incoming message and assigns it an SCL rating based on the likelihood that the message is UCE. To set the thresholds above which Intelligent Message Filter takes action on the messages at the gateway and at the mailbox store, use the **Block messages with an SCL rating greater than or equal to** list in **Gateway Block Configuration** and the **Move messages with an SCL rating greater than or equal to** list in **Store Junk E-mail Configuration**. Each setting on the scale corresponds to an SCL rating that Intelligent Message Filter assigns to incoming messages based on the probability that the message is UCE.

## Configuring Intelligent Message Filter at the Gateway

At the gateway, you configure the following settings:

- The threshold (or SCL rating) above which Intelligent Message Filter acts on a message at the gateway.
- The specific action that Intelligent Message Filter takes on a message with an SCL rating above the specified threshold.

---

### Setting the Gateway Threshold

On the **Intelligent Message Filtering** tab, under **Gateway Blocking Configuration**, in **Block messages with an SCL rating greater than or equal to**, select a number to set the threshold for the action taken at the gateway on messages. Use the following criteria and your specific organizational requirements to set your gateway threshold:

- Selecting a lower number for the SCL rating blocks more messages that could be UCE, but it also increases the likelihood of false positives, which are legitimate messages that Intelligent Message Filter marks as UCE. Some organizations find it acceptable to block a percentage of legitimate e-mail messages to significantly reduce the amount of UCE delivered to their users. If this is the case in your organization, select a lower number for the SCL rating threshold.
- Selecting a higher number for the SCL rating blocks fewer messages that could be UCE, but it reduces the likelihood of false positives. Many organizations would rather handle more UCE than risk legitimate e-mail messages being blocked. If this is the case in your organization, select a higher number for the SCL rating threshold.

---

### Specifying the Action Taken at the Gateway

After you set the gateway threshold, you must specify the action that Intelligent Message Filter takes when it assigns a message an SCL rating above the threshold you specify.

On the **Intelligent Message Filtering** tab, from the list in **When blocking messages**, select the action that you want Intelligent Message Filter to take when it assigns a message an SCL rating above the specified threshold. Choose from the following actions:

- **Archive** to archive all messages marked as UCE with a rating above the specified threshold. Archived messages are saved to the archive directory. This directory is in the root directory of the Queue directory specified on the **Messages** tab of the SMTP virtual server properties. By default, the archive directory is `Exchsrvr\Mailroot\vs1 n\UCEArchive`, where *n* is the SMTP virtual server instance number. By default, the `\Exchsrvr` directory is created in the `<drive letter>:\Program Files` parent directory. You can review messages in the archive directory by opening them in Notepad or using Microsoft Outlook Express. If you discover a legitimate e-mail message that has been archived, you can resubmit the message by placing it in the `Exchsrvr\Mailroot\vs1 n\pickup` directory. The SMTP service will then deliver the e-mail message to the appropriate mailbox.
- **Delete** to delete all messages marked as UCE with a rating above the specified threshold. The message is accepted by Exchange and is then deleted. Neither the sender nor the intended recipient are notified that the message has been deleted.
- **No Action** to take no action on messages marked as UCE with a rating above the specified threshold. This UCE rating is saved with the other message properties and these properties are sent with the message to other Exchange servers. Exchange mailbox servers use the UCE rating and the settings specified in **Store Junk E-mail Configuration** to determine whether to deliver a message to a user's Inbox or the Junk E-mail folder.
- **Reject** to reject the message at the gateway. Exchange rejects the message during the SMTP session, and the connecting SMTP server is then responsible for delivering the non-delivery report to the sender.

## Configuring Intelligent Message Filter at the Mailbox Store

On the **Intelligent Message Filtering** tab, under **Store Junk E-mail Configuration**, use the **Move messages with an SCL rating greater than or equal to** list to specify the threshold above which incoming messages are moved to a user's Junk E-mail folder, unless the sender appears on a user's safe senders list. These settings work similar to the settings in **Gateway Blocking Configuration**. Select a threshold above which an Exchange mailbox store moves messages to a user's Junk E-mail folder based on the following criteria:

- Selecting a lower number for the SCL rating reduces the amount of UCE delivered to a user's Inbox, but it also increases the likelihood of false positives being moved to a user's Junk E-mail folder. Thus, legitimate e-mail messages can inadvertently be moved to the user's Junk E-mail folder when you select a setting to move more UCE.
- Selecting a higher number for the SCL rating increases the amount of UCE delivered to a user's Inbox, but it also decreases the likelihood of false positives being delivered to a user's Junk E-mail folder.

---

## Enabling Intelligent Message Filter on SMTP Virtual Servers

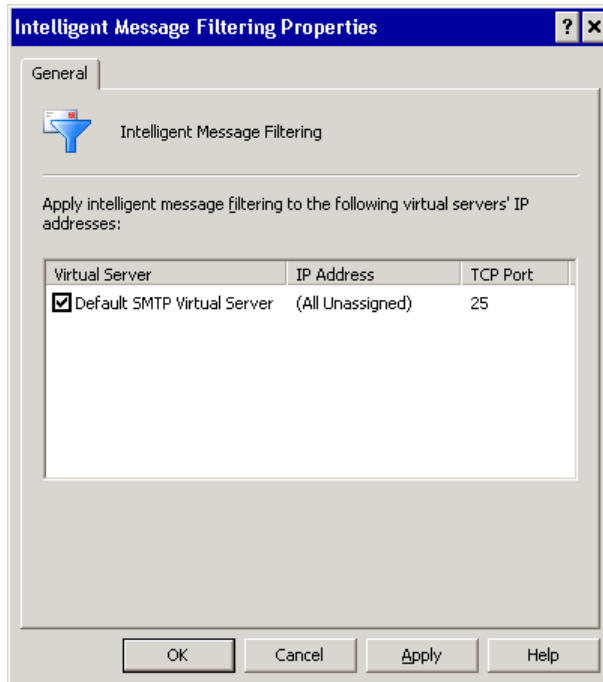
After you configure the appropriate settings on the **Intelligent Message Filtering** tab in **Message Deliver Properties**, you must enable Intelligent Message Filter on each SMTP virtual server that accepts incoming Internet e-mail messages. You enable Intelligent Message Filter using the **Intelligent Message Filtering** node under SMTP. The **General** tab of Intelligent Message Filtering Properties displays the SMTP virtual servers on any Exchange server where Intelligent Message Filter is applied.

### Note

The **Intelligent Message Filtering** node is only available on Exchange servers where Intelligent Message Filter is applied. If you access Exchange System Manager using an Exchange server without Intelligent Message Filter installed, this dialog box is not available. You must install the management tools for Intelligent Message Filter if you want to manage a gateway server remotely.

### To enable Intelligent Message Filter

1. In Exchange System Manager, expand **Servers**, expand <Server name>, expand **Protocols**, expand **SMTP**, right-click **Intelligent Message Filtering**, and then click **Properties**.
2. On the **General** tab, under **Apply intelligent message filtering to the following virtual servers' IP addresses**, click the check box next to each SMTP virtual server on which you want to enable Intelligent Message Filter (Figure 4.2).



**Figure 4.2 The Intelligent Message Filtering Properties dialog box**

**Important**

To filter UCE, you must enable Intelligent Message Filter on all SMTP virtual servers that accept incoming Internet e-mail messages. However, you do not need to enable Intelligent Message Filter on SMTP virtual servers on Exchange mailbox stores.



# Monitoring and Troubleshooting Intelligent Message Filter

You can monitor and troubleshoot issues with Microsoft® Exchange Intelligent Message Filter using Event Viewer and System Monitor.

## Using Event Viewer

In Event Viewer, both the Application Log and the System Log contain errors, warnings, and informational events related to the operation of Exchange, the SMTP service, and other applications. To help you identify the cause of Intelligent Message Filter problems, carefully review the data contained in the Application Log and System Log. Intelligent Message Filter writes events to Event Viewer using the source MExchangeTransport and the category SMTP Protocol.

### To view errors, warnings, and informational events in the Application Log

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Event Viewer**.
2. In the console tree, click **Application Log**.
3. To sort the log alphabetically and quickly locate an entry for an Exchange service, in the details pane, click **Source**.
4. To filter the log to list entries for events logged for Intelligent Message Filter, from the **View** menu, click **Filter**.
5. In **Application Log Properties**, use the Event source list to select **MExchangeTransport**.
6. In the **Category** list, select **SMTP Protocol**.

Table 5.1 explains the events that Intelligent Message Filter logs. Unless otherwise noted, all events are logged at the default logging level.

**Table 5.1 Events logged by Intelligent Message Filter**

Event	Explanation
<p><b>Event ID: 7512</b></p> <p>Severity=Informational</p> <p>Text:</p> <p>The message with ID &lt;message id&gt;, P1 From &lt;sender name&gt;, Subject &lt;subject&gt; from remote host &lt;host name&gt; was Rejected/Deleted by the Intelligent Message Filter.</p>	<p>Intelligent Message Filter writes this event when it rejects or deletes a message at the gateway.</p> <p>This event is recorded only when the logging level is set to <b>medium</b> or <b>maximum</b> for the SMTP Protocol category of the MExchangeTransport service. To set the logging level, use the <b>Diagnostic Logging</b> tab of the Exchange server properties.</p>

Event	Explanation
<p><b>Event ID: 7513</b></p> <p>Severity=Informational</p> <p>Text:</p> <p>Microsoft Exchange Intelligent Message Filter was refreshed for code version &lt;version number&gt;, data version &lt;version number&gt;. Microsoft Exchange Intelligent Message Filter is now enabled. A refresh occurs when the SMTP service is restarted or Microsoft Exchange Intelligent Message Filter is updated.</p>	<p>Intelligent Message Filter writes this event when Intelligent Message Filter is installed for the first time or when Intelligent Message Filter is updated. This event log is also written when the SMTP service is restarted.</p>
<p><b>Event ID: 7514</b></p> <p>Severity=Error</p> <p>Text:</p> <p>An error occurred while loading Microsoft Exchange Intelligent Message Filter.</p> <p>The error code is &lt;error code&gt;.</p>	<p>Intelligent Message Filter writes this event when an error occurs while installing or updating Intelligent Message Filter.</p> <p>Uninstall the new version of Intelligent Message Filter and attempt to reinstall.</p>
<p><b>Event ID: 7515</b></p> <p>Severity=Error</p> <p>Text:</p> <p>An error occurred while Microsoft Intelligent Message Filter attempted to filter a message with ID &lt;message ID&gt;, P1 From &lt;sender&gt;, Subject &lt;subject&gt;. This message will not be filtered.</p> <p>The error code is &lt;error code&gt;.</p>	<p>Intelligent Message Filter writes this event when it is unable to filter a message. Possible causes are corrupted or malformed messages.</p>

# Using System Monitor and Performance Logs and Alerts

Intelligent Message Filter has several performance counters that you can use to monitor its performance and operation.

## To monitor Intelligent Message Filter using System Monitor

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Performance**.
2. Right-click **System Monitor**, and then click **Add Counters**.
3. In **Add Counters**, under **Performance Object**, select **MSExchange Intelligent Message Filter**.

Table 5.2 explains the list of performance counters available for Intelligent Message Filter.

**Table 5.2 Performance counters for Intelligent Message Filter**

Counter	Description
Total Messages Scanned for UCE	The total number of messages scanned by Intelligent Message Filter. If this number is 0 or very low, Intelligent Message Filter may not be functioning properly.
Messages Scanned for UCE/sec	The number of messages scanned per second by Intelligent Message Filter. This counter indicates how quickly Intelligent Message Filter is operating.
Total UCE Messages Deleted	The total number of messages deleted at the gateway. This counter indicates that Intelligent Message Filter has identified these messages as UCE and deleted them, based on the action specified by an administrator. If you configure Intelligent Message Filter to take another action on messages identified as UCE at the gateway, this counter displays 0.
UCE Messages Deleted/sec	The number of messages deleted per second by Intelligent Message Filter. This counter indicates how quickly Intelligent Message Filter deletes messages identified as UCE. If you did not configure Intelligent Message Filter to delete messages identified as UCE, this counter displays 0.
Total UCE Messages Rejected	The total number of messages rejected at the gateway. This counter indicates that Intelligent Message Filter has identified these messages as UCE and rejected them, based on the action specified by an administrator. If you configure Intelligent Message Filter to take another action on messages identified as UCE at the gateway, this counter displays 0.
UCE Messages Rejected/sec	The number of messages rejected per second by Intelligent Message Filter. This counter indicates how quickly Intelligent Message Filter rejects messages identified as UCE. If you did not configure Intelligent Message Filter to reject messages identified as UCE, this counter displays 0.

<b>Counter</b>	<b>Description</b>
Total UCE Messages Archived	The total number of messages archived at the gateway. This counter indicates that Intelligent Message Filter has identified these messages as UCE and archived them, based on the action specified by an administrator. If you configured Intelligent Message Filter to take another action on messages identified as UCE at the gateway, this counter displays 0.
UCE Messages Archived/sec	The number of messages archived per second by Intelligent Message Filter. This counter indicates how quickly Intelligent Message Filter archives messages identified as UCE. If you did not configure Intelligent Message Filter to archive messages identified as UCE, this counter displays 0.
% UCE out of Total Messages Scanned	The percentage of the total number of messages scanned by Intelligent Message Filter that were identified as UCE.
% UCE of Messages Scanned in the previous 30 minutes	The percentage of the number of messages scanned by Intelligent Message Filter in the previous 30 minutes that were identified as UCE.
Total Messages Assigned an SCL Rating of <i>X</i>	The total number of messages scanned by Intelligent Message Filter that were assigned a spam confidence level (SCL) rating of <i>x</i> , where <i>x</i> is a spam rating of 0 to 9.

# Customizing Intelligent Message Filter

You can customize the following configuration settings in Microsoft® Exchange Intelligent Message Filter:

- Change the location of the archive directory.
- Store the spam confidence level (SCL) rating when archiving messages. By default, Intelligent Message Filter does not save the SCL rating on messages it archives.
- Filter messages sent by authenticated users. By default, authenticated users bypass Intelligent Message Filter.

To customize any of these settings, you must create a registry key value under the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange\ContentFilter
```

**Warning**

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

Additionally, you can create a registry key to configure the maximum size of safe senders lists and blocked senders lists. For more information, see the section "Setting the Size of Spam Rules" later in this chapter.

---

## Changing the Archive Location

The archive location is the directory where Intelligent Message Filter saves filtered messages when you choose to archive messages marked as UCE that have a rating above the specified gateway threshold configured on the **Connection Filtering** tab in **Message Delivery Properties**. By default, messages are archived in `\Exchsrvr\mailroot\vs1 n\UCEArchive` where *n* is the SMTP virtual server instance number. By default the `\Exchsrvr` directory is created in the `<drive letter>:\Program Files` parent directory.

### To change the location of the archive directory

1. In Registry Editor (regedit), in the details pane, right-click **ContentFilter**, click **New**, and then click **String value**.
2. Type **ArchiveDir** for the registry key value.
3. Right-click **ArchiveDir**, and then click **Modify**.
4. In **Edit String**, under **Value Data**, enter the full directory path where you want to archive messages filtered by Intelligent Message Filter. For example, type `C:\Archive`.

## Storing the SCL Rating with Archived Messages

By default, when Intelligent Message Filter archives a message, it does not archive the SCL rating assigned to the message. If you want to archive the SCL rating along with the message, you can create a registry key DWORD value, `ArchiveSCL`, and assign it a value of 1.

**To archive the SCL rating with archived messages**

1. In Registry Editor (regedit), right-click **ContentFilter**, click **New**, and then click **DWORD value**.
2. Type **ArchiveSCL** for the registry key value.
3. Right-click **ArchiveSCL**, and then click **Modify**.
4. In **Edit DWORD**, under **Value Data**, type **1**.

When this registry key value is set to 1, Intelligent Message Filter saves the SCL rating with the archived messages. The SCL rating is persisted in the message as an extended message header (X-SCL).

When this registry key is set to 0, or if the registry key value does not exist, Intelligent Message Filter archives the message, but does not save its associated SCL rating.

---

## Filtering Messages Sent through Authenticated Connections

By default, Intelligent Message Filter only filters messages and assigns SCL ratings to messages sent through anonymous connections. Messages sent by authenticated users bypass Intelligent Message Filter. If you want Intelligent Message Filter to assign SCL ratings to messages sent by authenticated connections, you can create a registry key DWORD value, **CheckAuthSessions**, and assign it a value of 1.

**To filter messages sent through authenticated connections**

1. In Registry Editor (regedit), right-click **ContentFilter**, click **New**, and then click **DWORD value**.
2. Type **CheckAuthSessions** for the registry key value.
3. Right-click **CheckAuthSessions**, and then click **Modify**.
4. In **Edit DWORD**, under **Value Data**, type **1**.

When this registry key value is set to 1, Intelligent Message Filter will filter messages sent by both authenticated and anonymous users.

By default, Intelligent Message Filter only filters messages sent by anonymous users. When the **CheckAuthSessions** registry key value is set to 0, or if the registry key value does not exist, the default behavior applies.

---

## Setting the Size of Spam Rules

The spam rule on a user's Inbox includes the user's safe senders list, blocked senders list, and Outlook metadata of about 300 bytes. By default, the size limit for a user's rule is 510 KB. This default size typically allows for about 2,000 entries in the safe senders and blocked senders lists.

Because the safe senders and blocked senders lists are synchronized between Outlook clients and the mailbox store, large lists can affect performance. You may choose to reduce the size limit. Conversely, you may choose to increase the size limit to allow users more flexibility in configuring the safe senders and blocked senders lists.

You can set a custom size limit for these rules by adding a new registry key value to the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSEExchangeIS\
ParametersSystem\
```

**Note**

You must enter the new size limit in bytes when using this registry key.

**To customize the size limit of a user's spam rule**

1. In Registry Editor (regedit), in the details pane, right-click **System**, click **New**, and then click **DWORD value**.
2. Type **Max Extended Rule Size** for the registry key value.
3. In **Edit DWORD**, under **Value Data**, enter the maximum size in bytes you want to allow for a user's spam rule.



# Appendix





# Additional Resources

For information and the latest updates to Microsoft® Exchange Intelligent Message Filter, see <http://go.microsoft.com/fwlink/?LinkId=21607>.

For information about Microsoft Exchange Server, see <http://go.microsoft.com/fwlink/?LinkId=21573>. Additionally, the following technical papers, resource kits, and Microsoft Knowledge Base articles provide valuable information regarding disaster recovery concepts and processes.

**Note**

To download a self-extracting executable of all Exchange Product Team technical articles and online books, see <http://go.microsoft.com/fwlink/?LinkId=10687>

---

## Exchange Server 2003 Technical Papers

- What's New in Exchange Server 2003  
(<http://go.microsoft.com/fwlink/?LinkId=21765>)
- 

## Other Resources

- Configuring SMTP in Exchange 2000 Server  
(<http://go.microsoft.com/fwlink/?LinkId=24866>)
  - Microsoft Exchange Server 2003 Software Development Kit  
(<http://go.microsoft.com/fwlink/?LinkId=24705>)
- 

## Microsoft Knowledge Base Articles

The following Microsoft Knowledge Base article is available on the Web at <http://go.microsoft.com/fwlink/?LinkId=14898>:

- 320053, "HOW TO: Rename the Administrator and Guest Account in Windows 2000"  
(<http://go.microsoft.com/fwlink/?LinkId=3052&kbid=320053>)



**Does this book help you?** Give us your feedback. On a scale of 1 (poor) to 5 (excellent), how do you rate this book?

E-mail feedback to [exchdocs@microsoft.com](mailto:exchdocs@microsoft.com).

For the latest information about Exchange, see the following Web pages:

- Exchange Server 2003 Technical Library  
<http://go.microsoft.com/fwlink/?LinkId=21277>
- Exchange Tools and Updates  
<http://go.microsoft.com/fwlink/?LinkId=25097>
- Self-extracting executable containing all Exchange Product Team technical articles and books  
<http://go.microsoft.com/fwlink/?LinkId=10687>