

## **Intelligent Message Filter v2 Operations Guide**

Microsoft Corporation

Published: February 7, 2007

This document provides information about working with version 2 of the Microsoft Exchange Server Intelligent Message Filter, which is installed automatically with Exchange Server 2003 Service Pack 2.

Comments? Send feedback to [exchdocs@microsoft.com](mailto:exchdocs@microsoft.com)

Reformatted for better reading by Rob Stoekenbroek, 24-feb-2007  
Included some additional information for clarity.  
[www.stoekenbroek.com/imfcompanion](http://www.stoekenbroek.com/imfcompanion)

# Contents

1	Introduction .....	1
1.1	Improvements in Message Hygiene.....	1
2	Understanding the Intelligent Message Filter .....	2
2.1	IMF and Outlook Filtering Features .....	3
3	Planning Your Exchange Server Intelligent Message Filter .....	6
3.1	Helping to Secure Your Gateway SMTP Virtual Servers.....	6
3.2	Deploying in a Multiple Forest Scenario .....	8
3.3	Enabling Cross-Forest Authentication .....	8
4	Configuring and Enabling IMF .....	13
4.1	Configuring Connection Filtering.....	13
4.2	How to Create an Intelligent Message Filter .....	14
4.3	How to Specify Sender ID Filtering Options .....	16
4.4	How to Specify IP Address Configuration Data for Sender ID Filtering.....	17
4.5	How to Specify IP Address Configuration Data for Connection Filtering.....	18
4.6	How to Create a Connection Filtering Rule .....	19
4.7	How to Enable Connection Filtering.....	21
4.8	How to Enable Intelligent Message Filtering.....	21
5	Updating the Exchange Server Intelligent Message Filter .....	22
5.1	Supported Scenarios .....	22
5.2	Schedule and Availability of Updates.....	22
5.3	How to Enable Updates .....	22
5.4	Version Numbers .....	23
5.5	The Update Process .....	23
5.6	How to Uninstall Updates.....	24
5.7	Service Packs .....	25
5.8	Custom Weight List Functionality.....	25
5.9	Unsupported Scenarios: Clustered Environment.....	25
5.10	Automatic Updates.....	26
6	Monitoring and Troubleshooting .....	27
6.1	How to Use Event Viewer .....	27
6.2	How to Use System Monitor and Performance Logs and Alerts .....	28
6.3	Uninstalling Version 1 of Intelligent Message Filter .....	29
7	Customizing Exchange Server Intelligent Message Filter .....	31
7.1	Changing the Archive Location .....	31
7.2	Storing the SCL Rating with Archived Messages .....	31
7.3	Filtering Messages Sent through Authenticated Connections.....	32
7.4	Setting the Size of Spam Rules .....	32
8	Appendix.....	33
8.1	Custom Weighting File .....	33
8.2	Known Issues.....	34
8.3	Hints and Tips .....	34
9	Copyright .....	35

# 1 Introduction

---

Microsoft® Exchange Server Intelligent Message Filter v2 helps companies reduce the amount of unsolicited commercial e-mail (UCE), also known as spam, received by users. This guide provides overall operational information to help optimize the performance of Exchange Server Intelligent Message Filter.



## Important:

The first version of Intelligent Message Filter was a stand-alone tool, and is no longer supported. Version 2 of the Intelligent Message Filter, to which this Operations Guide information applies, is installed automatically with Exchange Server 2003 Service Pack 2 (SP2). For download information about SP2, see <http://go.microsoft.com/fwlink/?linkid=54751>.

The Microsoft Exchange Server 2003 Service Pack 2 (SP2) Release Notes contain general information related to Exchange Server Intelligent Message Filter and Sender ID, an industry-standard framework. It also includes Known Issues at the time of release. It is recommended that you read through the release notes before you do any work with the Exchange Server Intelligent Message Filter. Obtain the release notes from <http://go.microsoft.com/fwlink/?linkid=52072>.

## 1.1 Improvements in Message Hygiene

The anti-spam improvements are driven by the release of the integrated Version 2 of the Intelligent Message Filter, and Sender ID, which is an industry-standard framework. Following are the highlights of the initiatives around anti-spam.

- **Intelligent message filtering** in the form of updated SmartScreen™ Technology (Microsoft research technology that is used to detect spam messages in Hotmail®, Exchange Server, and Office Outlook). This is achieved through Version 2 of the Microsoft Exchange Intelligent Message Filter that contains significant improvements in the anti-spam area for SP2.
- **Sender ID filtering** for addressing the problem of domain spoofing and phishing schemes by verifying the domain name from which the e-mail is sent. Sender ID has been integrated with the other anti-spam features that can be enabled on the General tab of the SMTP Virtual Server properties dialog box. This extends Exchange System Manager (ESM) and provides a single point for anti-spam features. Also, Sender ID can be implemented on the Exchange server that is located behind the perimeter, and work with any gateway server, for example, Sendmail.
- **Anti-phishing.** The spam confidence level (SCL) score will be changed, based on the current Exchange store and gateway thresholds as configured by the administrator. Anti-phishing is incorporated in the SmartScreen functionality.

## More Information

For general information about Exchange Server Intelligent Message Filter v2, see <http://go.microsoft.com/fwlink/?linkid=21607>.



**Note:** This document contains the original Microsoft documentation and includes additional material. Download the original [Microsoft Exchange Server Intelligent Message Filter v2 Operations Guide](http://go.microsoft.com/fwlink/?linkid=27922) (<http://go.microsoft.com/fwlink/?linkid=27922>) to print or read offline.

## 2 Understanding the Intelligent Message Filter

---

This topic provides an overview of Microsoft® Exchange Server Intelligent Message Filter. This topic also explains how Intelligent Message Filter works in an Exchange Server 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.

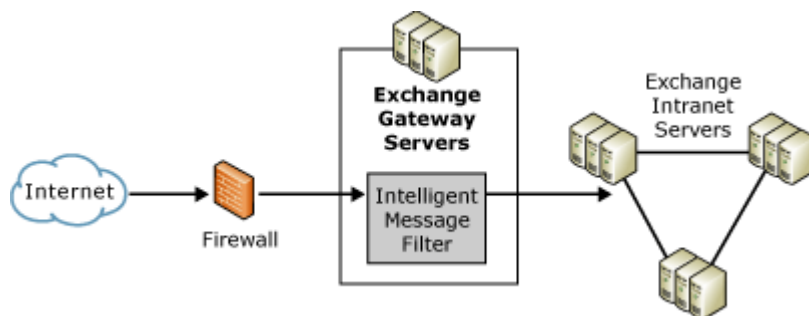
Based on the characteristics of millions of messages, Intelligent Message Filter recognizes indicators of both legitimate messages and UCE messages. Intelligent Message Filter can accurately assess the probability that an incoming e-mail message is either a legitimate message or UCE. Unlike many other 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 chance 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 enable 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 the following figure.

#### Exchange server topology with Intelligent Message Filter enabled



When an external user sends e-mail messages to an Exchange server that has Intelligent Message Filter enabled, 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 that have various SCL ratings: a gateway threshold with an associated action to take on messages greater

than this threshold, and a mailbox store threshold. If a message has a rating that is greater than or equal to the gateway threshold, Intelligent Message Filter takes the action specified. If the message has a rating lower than 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 rating greater than the mailbox store threshold, the mailbox store delivers the message to the user's Junk E-mail folder instead of to the Inbox.

## 2.1 IMF and Outlook Filtering Features

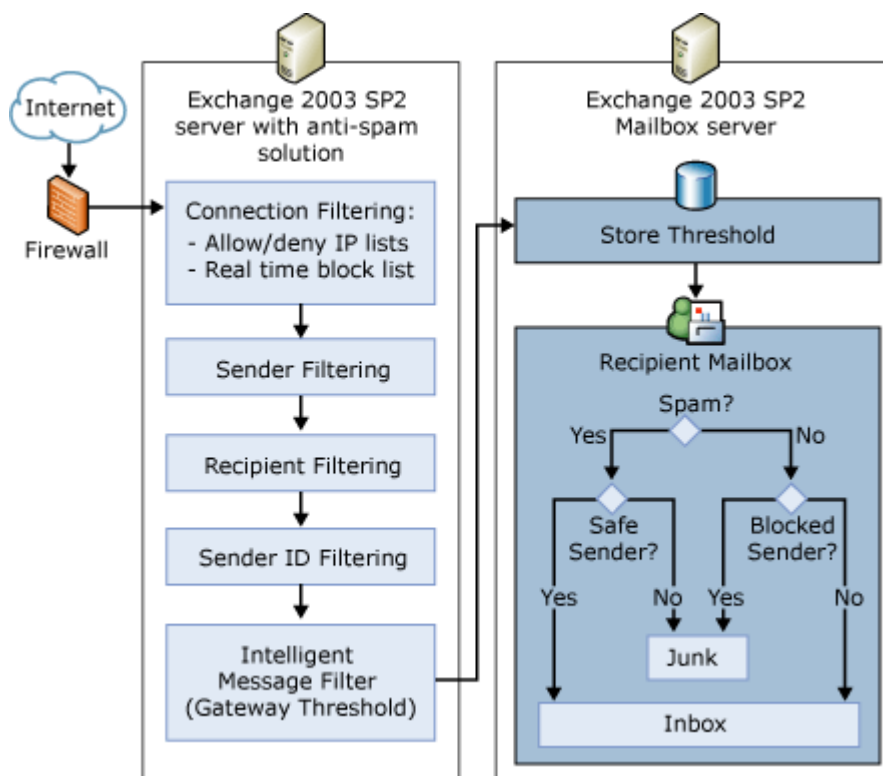
Exchange 2003 provides a set of filtering features, which are also used to reduce UCE. These features are sender, recipient, and connection filtering. Each of these Exchange filters is checked during the SMTP session, when a connecting SMTP server tries to send e-mail messages to an Exchange server. Intelligent Message Filter is applied after the SMTP session. 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 let users 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 than 2003, the Safe Senders and Blocked Senders lists cannot be modified from that e-mail client. However, these lists can be modified using Outlook Web Access 2003. If Outlook Web Access 2003 is used in this manner to enable junk e-mail filtering, messages where the sender is on the Blocked Senders list or messages that are marked as UCE will be delivered to the user's Junk E-mail folder. Messages marked as UCE whose sender is on the Safe Senders list will be delivered to the user's Inbox. If Outlook Web Access 2003 has not been used to enable junk e-mail filtering, every message, including those marked as UCE, is delivered directly to the user's Inbox.

The following figure shows how Intelligent Message Filter works with these Exchange and Outlook features.

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



As shown in the figure, 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 RFC2821 MAIL FROM command) against the list of senders that 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 this action (if enabled), Exchange checks and filters recipients who are not in the directory (Directory Lookups).
6. After recipient filtering is applied, Exchange checks the resolved sender address (the P2 data from RFC2822 headers) against the Blank Sender. If a match is found, Exchange filters the message based on the options that you configured and no other filters are applied.
7. Sender ID filter is applied (if enabled) before Intelligent Message Filter.
8. If a message is not filtered by connection, recipient, or sender filtering, Intelligent Message Filter is applied, and one of two actions occurs at the gateway:
  - If Intelligent Message Filter assigns the message an SCL rating that is greater than or equal to 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 to your gateway threshold, the message is passed to the Exchange server that has the user's mailbox store.
9. 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 occurs:
  - 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 occurs:
    - 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 unavailable 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 greater 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 occurs:
    - 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 unavailable or defined, the message is delivered to the recipient's Junk E-mail folder.



**Important:**

If users are using versions of Outlook earlier than Outlook 2003, the mailbox store thresholds have no effect and messages that are filtered in step 9 are instead delivered to the users' Inboxes.

However, if clients can access e-mail using Outlook Web Access 2003, the store thresholds are applied as described in step 9.

## 3 Planning Your Exchange Server Intelligent Message Filter

---

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 the 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 the 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 that is accepting Internet e-mail messages on the Exchange bridgehead servers.

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

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

### 3.1 Helping to Secure Your Gateway SMTP Virtual Servers

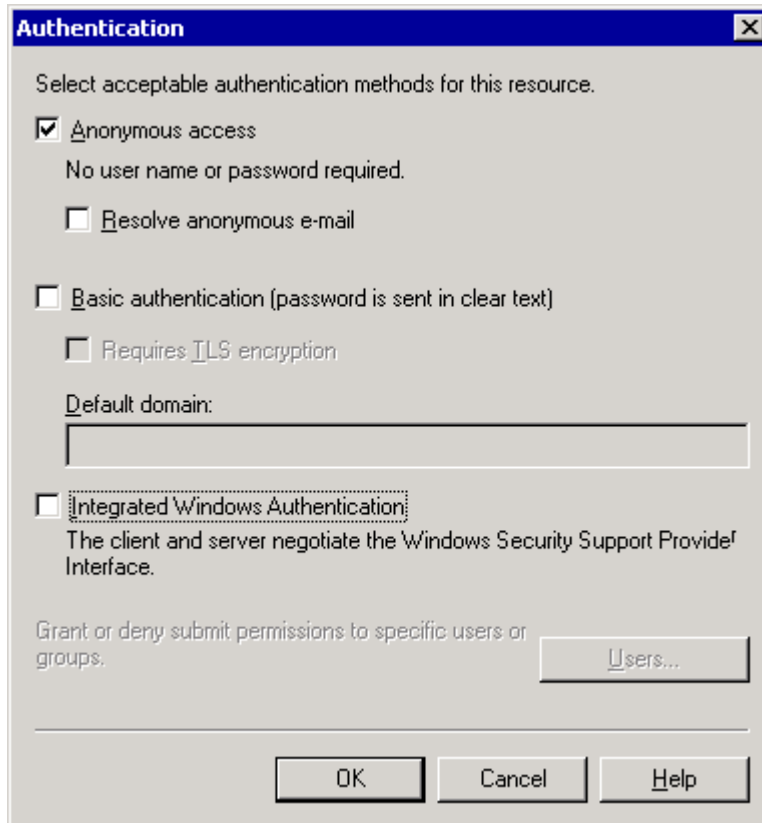
Dictionary attacks are brute force attacks that use common words as possible passwords to discover valid passwords for well-known accounts, such as the administrator account. Malicious users attempt dictionary attacks to gain access to computers.

To help 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 the 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.

**Authentication dialog box**



If you cannot disable authenticated access on your SMTP virtual server for business reasons, such as a partner company authenticating, follow these steps to increase security on your gateway server:

- Enforce a strong password policy for all user accounts, specifically 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" at <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.

## 3.2 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 Server 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. Moreover, 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.

## 3.3 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 are in contacts in the other forest. The following sections describe how to follow these 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 is also 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.

## Creating a User Account in the Destination Forest

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. This allows 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:

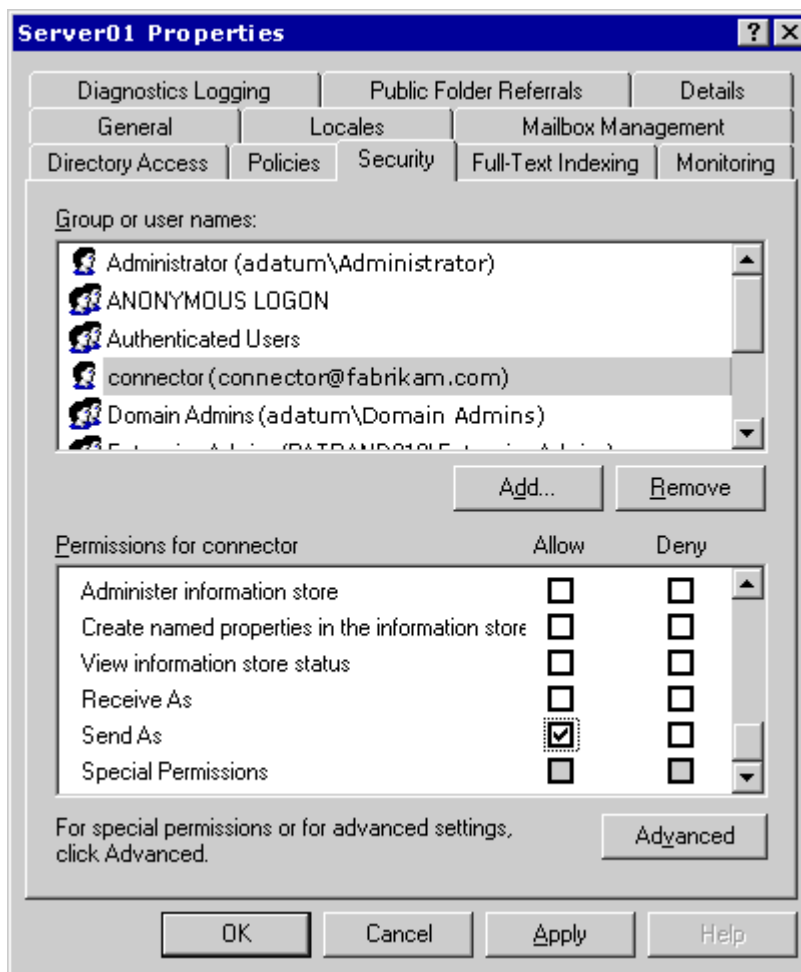
#### **Note:**

Be careful when you create 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.

- Start Exchange System Manager.
- In the console tree, expand **Servers**, right-click an Exchange server that will accept incoming connections from the connecting forest, and then click **Properties**.
- In <Server Name>**Properties**, on the **Security** tab, click **Add**.
- In **Select Users, Computers, or Groups**, add the account you just created, and then click **OK**.
- On the **Security** tab, under **Group or user names**, select the account.
- Under **Permissions**, next to **Send As**, select the **Allow** check box.

#### Allowing the Send As permission



## Creating a Connector in the Connecting Forest

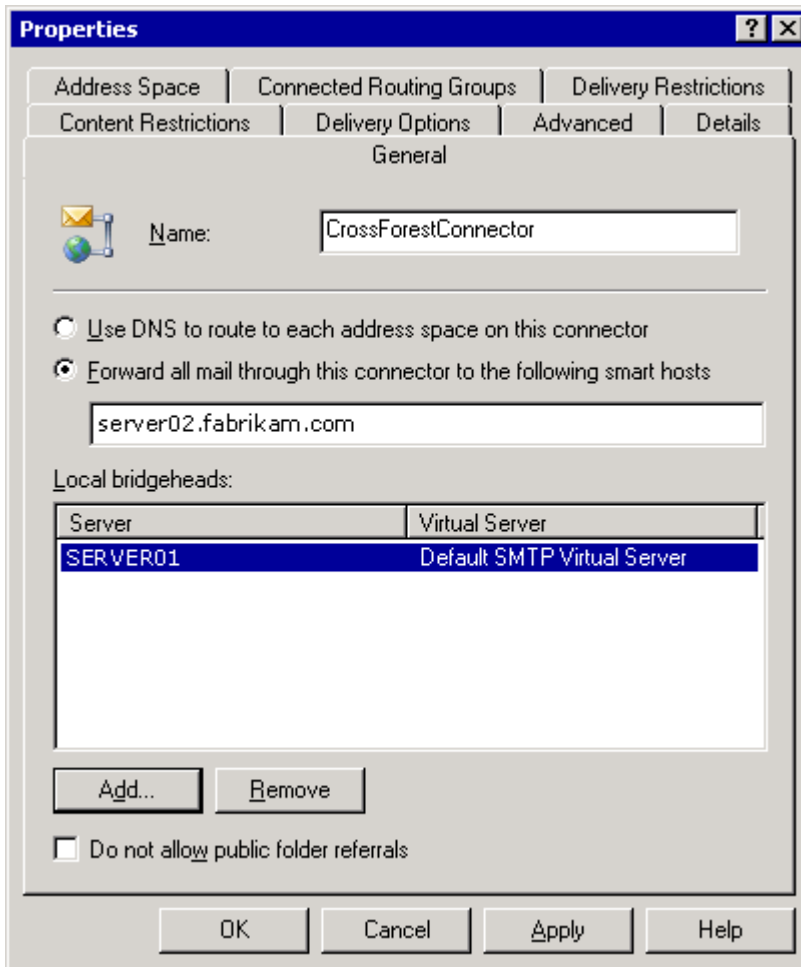
After you create the account with the correct permissions in the destination forest, create a connector in the connecting forest and require authentication using the account you just created. In the following procedure, assume that you are creating a connector on an Exchange server in the Adatum forest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

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

1. Start Exchange System Manager.

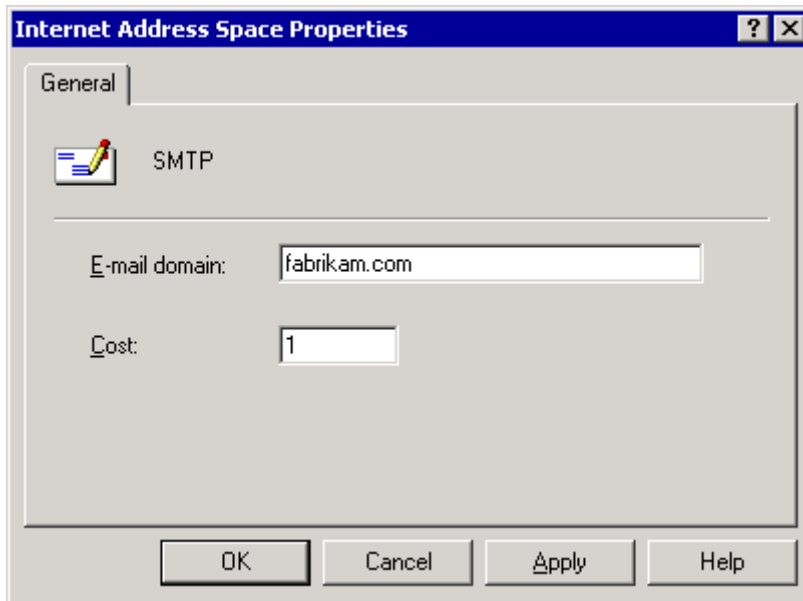
2. In the console tree, right-click **Connectors**, point to **New**, and then click **SMTP Connector**.
3. On the **General** tab, in the **Name** box, type a name for the connector.
4. Click **Forward all mail through this connector to the following smart hosts**, and then type the fully qualified 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.

**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.

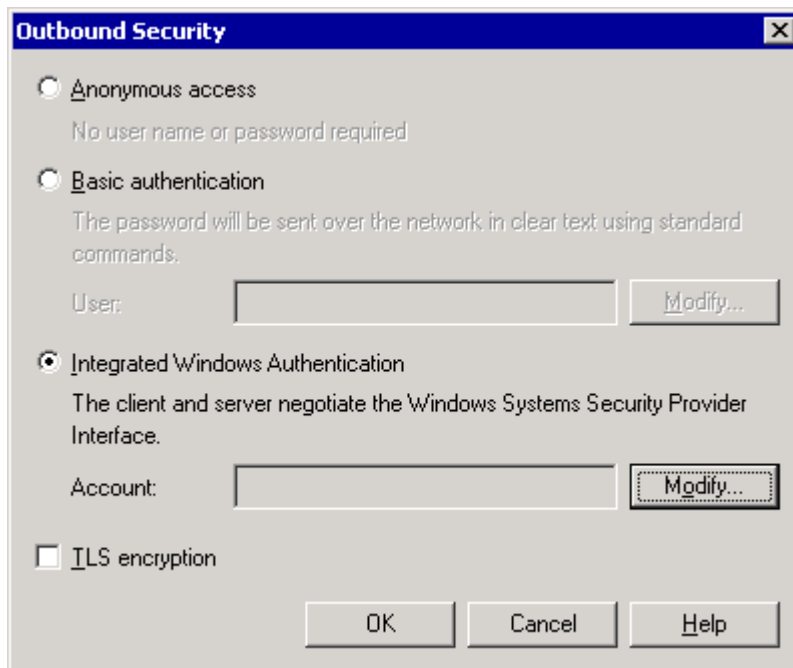
**The Internet Address Space Properties dialog box**



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**.

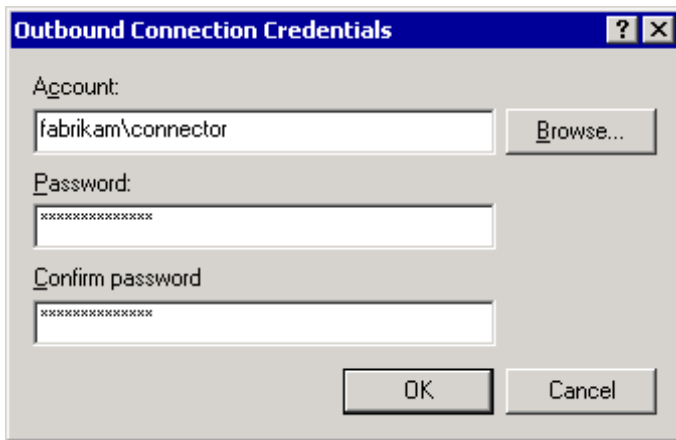
#### The Integrated Windows Authentication button in the Outbound Security dialog box



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. 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.

#### The Outbound Connection Credentials dialog box



12. Click **OK**; you're done now!

## 4 Configuring and Enabling IMF

---

After you install Microsoft® Exchange Server 2003 Service Pack 2, which includes the Exchange Server Intelligent Message Filter, you must configure the settings that you want to use in your organization. You also need to enable Intelligent Message Filter on each Simple Mail Transfer Protocol (SMTP) virtual server for which you want to filter unsolicited commercial e-mail (UCE).

Intelligent message filtering lets you block UCE on your gateway SMTP virtual servers. Gateway SMTP virtual servers are SMTP virtual servers that accept incoming Internet e-mail. Intelligent message filtering is defined globally, but enabled at the SMTP virtual server on a per-IP address basis.

This topic includes three key procedural topics, as follows, that help configure and enable Exchange Server Intelligent Message Filter.

- [How to Create an Intelligent Message Filter](#)
- [How to Specify Sender ID Filtering Options](#)
- [How to Enable Intelligent Message Filtering](#)

Additionally, there are several topics there provide procedural information about Sender ID and connection filtering.

The Exchange Server 2003 Service Pack 2 Online Help, which is the main repository for much of the procedural information about Exchange Server 2003, contains other procedures that relate to configuration and enabling. Use the Search to find specific topics that you are interested in.

The online Help is downloadable at <http://go.microsoft.com/fwlink/?linkid=63470>.

### 4.1 Configuring Connection Filtering

Exchange 2003 supports connection filtering based on block lists. Connection filtering takes advantage of externally-based services that list known sources of unsolicited e-mail sources, dial-up user account lists, and servers open for relay based on IP addresses on block lists that they maintain. Connection filtering complements third-party content filter products. This feature lets you to check an incoming IP address against a provider's block list for the categories you want to filter. If a match is found on the provider's list, SMTP issues a "550 5.x.x" error in response to the RCPT TO: command.

You can also implement connection filtering without using a block list provider because you can create global accept and deny lists of SMTP addresses from which you want to globally accept or deny all e-mail messages.

Connection filtering is defined globally but enabled at the SMTP virtual server on a per-IP address basis. Different groups of users can log on with any number of IP address/TCP port combinations. You can decide which combinations, and therefore which users or groups, will have their messages filtered.

To configure connection filtering, you must first create and configure a connection filtering rule and then apply it at the SMTP virtual server level. The following topics explain how to perform each of these tasks:

- [How to Create a Connection Filtering Rule](#)
- [How to Specify IP Address Configuration Data for Connection Filtering](#)
- [How to Enable Connection Filtering](#)

## 4.2 How to Create an Intelligent Message Filter

The following procedure outlines how to create an intelligent message filter. You need to do this before you enable intelligent message filtering on a virtual server.

### ▶ To create an intelligent message filter

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Double-click **Global Settings**.
3. Right-click **Message Delivery**, and then click **Properties**.
4. Click the **Intelligent Message Filtering** tab.
5. 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.
6. Under **Gateway Blocking Configuration**, 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. The following options are available for selection:
  - Select **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 putting it in the Exchsrvr\Mailroot\vs1 n\pickup directory. The SMTP service will then deliver the e-mail message to the appropriate mailbox.
  - Select **Delete** to delete all messages marked as UCE with a rating greater than the specified threshold. The message is accepted by Exchange Server and is then deleted. Neither the sender nor the intended recipient is notified that the message has been deleted.
  - Select **No Action** to take no action on messages marked as UCE with a rating greater than 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.

- Select **Reject** to reject the message at the gateway. Exchange Server rejects the message during the SMTP session, and the connecting SMTP server is then responsible for delivering the non-delivery report to the sender.
7. Under **Store Junk E-mail Configuration**, in **Move messages with an SCL rating greater than or equal 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 Server 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 probability of false positives being moved to a user's Junk E-mail folder. Therefore, legitimate e-mail messages can unintentionally 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.

## 4.3 How to Specify Sender ID Filtering Options

Sender ID filtering allows you to specify how the server should handle messages that failed Sender ID verification. Sender ID filtering is an industry standard that you can use to provide more protection against UCE and phishing schemes.

Sender ID filtering is defined globally, but enabled at the SMTP virtual server on a per-IP address basis.

You can enable Sender ID filtering behind the perimeter of the network. To do this, you specify the IP addresses of the servers in your internal network that you want excluded from Sender ID filtering. For information about how to enable Sender ID filtering behind the perimeter, see [How to Specify IP Address Configuration Data for Sender ID Filtering](#).

### To specify Sender ID filtering options

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Double-click **Global Settings**.
3. Right-click **Message Delivery**, and then click **Properties**.
4. Click the **Sender ID Filtering** tab.
5. Under If ID validation fails, take the following action, specify the action you want Exchange Server to take when Send ID verification fails.



#### **Important:**

After you configure these options, you must enable Send ID filtering on your SMTP servers.

## 4.4 How to Specify IP Address Configuration Data for Sender ID Filtering

You can enable Sender ID filtering behind the perimeter of your network by specifying the IP addresses of the servers in your internal network that you want to be excluded from Sender ID filtering.



### Note:

Before you can use Sender ID filtering, you must specify Sender ID filtering options and enable Sender ID filtering on an SMTP virtual server.

### ▶ To specify IP address configuration data for Sender ID filtering

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Move to **Message Delivery** starting from **Global Settings**.
3. Right-click **Message Delivery**, and then click **Properties**.
4. On the **General** tab, click **Add**.
5. Under **Perimeter IP List and Internal IP Range Configuration**, click **Add**.
6. In Sender ID and Connection Filtering Configuration Settings, the IP addresses that you configured to be excluded from Sender ID filtering and connection filtering are displayed. If the Sender ID filtering or connection filtering deployment servers find an IP address in this list in an e-mail message, Exchange Server skips the IP address without running Sender ID filtering or connection filtering validation on it. You can add up to 196 IP addresses to the list. To add an IP address to the list, click **Add**.
7. In IP Address (Mask), specify the IP addresses that you want to exclude from IP address validation. You must include all servers in your organization that process incoming SMTP mail. You must also include all servers that route mail to the Sender ID and connection filtering deployment servers. If any of the servers that process SMTP mail are located on the perimeter, you should include all perimeter IP addresses of these servers. You can specify individual IP addresses or groups of IP addresses.
  - Click **Single IP address** to specify an individual IP address to be excluded from Sender ID filtering and connection filtering. In **IP address**, type the IP address of the computer that you want to exclude from Sender ID filtering.
  - Click **Group of IP addresses** to specify an entire subnet to exclude from Sender ID filtering and connection filtering. In **Subnet address**, specify the subnet address of the subnet you want to exclude. In **Subnet mask**, type the subnet mask for the subnet you want to exclude.
8. Restart the Simple Mail Transfer Protocol (SMTP) service.

## 4.5 How to Specify IP Address Configuration Data for Connection Filtering

You can enable connection filtering behind the perimeter of your network by specifying the IP addresses of the servers in your internal network that you want to be excluded from connection filtering.

 **Note:**

Before you can use connection filtering, you must create a connection filter and enable connection filtering on an SMTP virtual server. For information about how to configure connection filtering, see [Configuring and Enabling Exchange Server Intelligent Message Filter](#).

 **To specify IP address configuration data for Sender ID filtering**

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Move to **Message Delivery** starting from **Global Settings**.
3. Right-click **Message Delivery**, and then click **Properties**.
4. On the **General** tab, click **Add**.
5. Under **Perimeter IP List and Internal IP Range Configuration**, click **Add**.
6. In **Sender ID and Connection Filtering Configuration Settings**, the IP addresses that you configured to be excluded from Sender ID filtering and connection filtering are displayed. If the Sender ID filtering or connection filtering deployment servers find an IP address in this list in an e-mail message, Exchange Server skips the IP address without running Sender ID filtering or connection filtering validation on it. You can add up to 196 IP addresses to the list. To add an IP address to the list, click **Add**.
7. In **IP Address (Mask)**, specify the IP addresses that you want to exclude from IP address validation. You must include all servers in your organization that process incoming SMTP mail. You must also include all servers that route mail to the Sender ID and connection filtering deployment servers. If any of the servers that process SMTP mail are located on the perimeter, you should include all perimeter IP addresses of these servers. You can specify individual IP addresses or groups of IP addresses.
  - Click **Single IP address** to specify an individual IP address to be excluded from Sender ID filtering and connection filtering. In **IP address**, type the IP address of the computer that you want to exclude from Sender ID filtering.
  - Click **Group of IP addresses** to specify an entire subnet to exclude from Sender ID filtering and connection filtering. In **Subnet address**, specify the subnet address of the subnet you want to exclude. In **Subnet mask**, type the subnet mask for the subnet you want to exclude.
8. Restart the Simple Mail Transfer Protocol (SMTP) service.

## 4.6 How to Create a Connection Filtering Rule

This topic includes a procedure for creating a connection filtering rule, and one for configuring a return status code on a new or existing connection filtering rule.

### ▶ To create a connection filtering rule

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Double-click **Global Settings**.
3. Right-click **Message Delivery**, and then click **Properties**.
4. Click the **Connection Filtering** tab, and then click **Add**.
5. In the **Display Name** box, type a name for the connection filter.
6. In the **DNS Suffix of Provider** box, type the DNS suffix that your provider appends to the IP address.
7. In the **Custom Error Message to Return (default error message will be used if left blank)** box, if you want, type a custom error to return to the sender. Leave this field blank to return the default message. The default message is:

**<Connecting IP Address> has been blocked by <name of connection filter rule>**

You can use the following variables to generate a custom message:

- %0 - connecting IP address
- %1 - name of the connection filter rule
- %2- the block list provider

To include a percentage sign (%) in your error message, you must enter %% for the percentage sign to display.

8. Click **Return Status Code** to configure the return status codes that you want this rule to filter.

### ▶ To configure a return status code on a new or existing connection filtering rule

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Double-click **Global Settings**.
3. Right-click **Message Delivery**, and then click **Properties**.
4. Click the **Connection Filtering** tab, and then do one of the following:
  - To configure a return status code on a new rule, click **Add** for a new rule.
  - To configure a return status code on an existing rule, select the rule, and then click **Edit**.
5. In **Connection Filtering Rule**, click **Return Status Code**.
6. Select one of the following options:
  - Click **Match Filter Rule to Any Return Code (this connection filter rule is matched to any return status code received from the provider service)** to match all return codes with the rule. If an IP address is found on any list, the block list provider service sends a return code, and the filter rule blocks the IP address. This is the default setting.
  - Click **Match Filter Rule to the Following Mask (this connection filter rule is matched to**

**return status codes received from the provider service by using a mask to interpret them)** to enter a mask to interpret the return status codes from the block list provider service. Check with your block list provider service to determine the conventions used in the block list provider's masks.

 **Note:**

Remember that a mask checks only against a single value. If you set a mask value that is returned when an IP address appears on two lists, the mask will match only the IP settings that satisfy both settings. To check for either of these two settings, enter the status code for these settings.

- Click **Match Filter Rule to Any of the Following Responses (this connection filter rule is matched to return status codes received from the provider service by using the specific values of the return status codes below)** if you want the filter rule to match one of multiple return status codes. For each return status code you want the rule to match, click **Add**, type the return status code, and then click **OK**.

7. Click **OK**.

## 4.7 How to Enable Connection Filtering

When you enable connection filtering on an SMTP virtual server, e-mail messages received from any IP address matched by a connection filtering rule or e-mail messages from an IP address specified on the global deny list are not accepted.

Connection filtering is defined globally, but enabled at the SMTP virtual server on a per-IP address basis. Different groups of users can log on with any number of IP address/TCP port combinations. You can decide which combinations, and therefore which users or groups will have connection filtering enabled for their messages.

### **Note:**

Before you can enable connection filtering on a virtual server, you must create a connection filter. The topic, [How to Create an Intelligent Message Filter](#), provides guidelines for doing this.

### **To enable connection filtering on a virtual server**

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Move to the SMTP virtual server, starting with Server.
3. Right-click the SMTP virtual server, and then click **Properties**.
4. On the **General** tab, click **Advanced**.
5. In **Advanced**, select the IP address to which you want to apply the connection filtering, and then click **Edit**.
6. In **Identification**, select the **Apply Connection Filter** check box, and then click **OK**. In **Advanced**, under the **Filter Enabled** column, **Yes** appears.
7. To disable filtering, clear the **Apply Connection Filter** check box.

## 4.8 How to Enable Intelligent Message Filtering

Before you can enable intelligent message filtering on a virtual server, you must create an intelligent message filter. For information about how to create an intelligent message filter, see [How to Create an Intelligent Message Filter](#).

### **To enable intelligent message filtering on a virtual server**

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Move to the SMTP virtual server, starting with **Servers**.
3. Right-click the SMTP virtual server, and then click **Properties**.
4. On the **General** tab, click **Advanced**.
5. In **Identification**, select the **Apply Intelligent Message Filtering** check box, and then click **OK**. In **Advanced**, under the **Filter Enabled** column, **Yes** appears.
6. To disable filtering, clear the **Apply Intelligent Message Filtering** check box.

## 5 Updating the Exchange Server Intelligent Message Filter

---

This topic describes the update process for the Microsoft® Exchange Server Intelligent Message Filter feature that is included with Exchange Server 2003 Service Pack 2 (SP2). By default, the Intelligent Message Filter feature is installed with Exchange Server 2003 SP2. You must manually enable the Intelligent Message Filter feature to obtain the benefits of this new message filtering technology. After you enable the Intelligent Message Filter feature, the .dat file and the .dll file must be updated regularly to keep the filter current and effective.

For more information about the update process and issues that can occur, see the Exchange Server Team blog article, "Demystifying Exchange Server 2003 SP2 IMF Updates" at <http://go.microsoft.com/fwlink/?linkid=67401>.



### Note:

The content of each blog and its URL are subject to change without notice.

### 5.1 Supported Scenarios

Intelligent Message Filter updates are supported in the following configurations:

- On a server that is running Exchange Server 2003 SP2 or a later version of Exchange Server 2003, with Intelligent Message Filter enabled
- On a server that is running both Microsoft Small Business Server and Exchange Server 2003 SP2 or a later version of Exchange Server 2003, with Intelligent Message Filter enabled

### 5.2 Schedule and Availability of Updates

Intelligent Message Filter updates are available every first and third Wednesday through Microsoft Update and Automatic Updates technologies. Organizations can also use Windows Server Update Services (WSUS) and System Management Services to deliver the updates in a corporate environment.

When the Exchange Server team cannot release the update on a Wednesday, they will release the update on the following day. If the update is unavailable on a Thursday, the update for that week will be skipped. Then, the update will be released on the next scheduled Wednesday.

The Intelligent Message Filter is language-independent. Intelligent Message Filter updates are offered for all language versions of Exchange Server 2003.

### 5.3 How to Enable Updates

After you enable the Intelligent Message Filter in Exchange System Manager, to enable Intelligent Message Filter updates, you must create the **ContentFilterState** registry entry. To do this, follow these steps.



### Caution:

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.

#### ▶ To create the ContentFilterState registry entry

1. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
2. Expand the following registry sub key:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange`

3. In the left pane, click **Exchange**. Then, right-click in the right pane, point to **New**, and then click **DWORD Value**.
4. Type **ContentFilterState**, and then press **Enter** to name the new registry entry.
5. Right-click **ContentFilterState**, and then click **Modify**.
6. In the **Data value** box, type **1**, and then click **OK**.
7. Quit Registry Editor.
8. In the Services snap-in, restart the **Simple Mail Transfer Protocol (SMTP)** service.

## 5.4 Version Numbers

An Intelligent Message Filter update package includes both a .dll file and a .dat file for the filter. The version information for the Intelligent Message Filter update files MExchange.UceContentFilter.dll and MExchange.UceContentFilter.dat reflects the Exchange Server build versioning in the following format:

MajorProductVersion.MinorProductVersion.MajorNumber.MinorNumber.

The version numbers are consistent with the Exchange Server build number, such as 6.5.XXXX.X. This makes it easier to identify the version number of the Intelligent Message Filter update that you have installed on the computer.

The update package version of an Intelligent Message Filter update is based on the date of the package build. Additionally, the update package version of an Intelligent Message Filter update is identified in the package name. For example, an update package that is dated December 14, 2005 has the following title:

Update for Intelligent Message Filter on Exchange Server 2003: 2005.12.14 (KB907747)

The executable package for this update has the following file name:

IMF-KB907747-2005.12.14-x86.exe

## 5.5 The Update Process

By default, when the Intelligent Message Filter is installed together with Exchange Server 2003 SP2, a new folder that is named **MSCFV2** is created. The Intelligent Message Filter engine and the .dat file are stored in the following location:

- *Drive\_Letter:\Program Files\Exchsvr\Bin\MSCFV2*

Subsequent updates are stored in subfolders under the MSCFV2 folder. The subfolders are named according to the version number of the updates. For example, after you install several updates, the folder structure may appear as follows:

- *Drive\_Letter:\Program Files\Exchsvr\Bin\MSCFV2*
- *Drive\_Letter:\Program Files\Exchsvr\Bin\MSCFV2\6.5.7612.0*
- *Drive\_Letter:\Program Files\Exchsvr\Bin\MSCFV2\6.5.7615.0*
- *Drive\_Letter:\Program Files\Exchsvr\Bin\MSCFV2\6.5.7620.0*

The registry entry that is described in the "How to Enable Updates" section reflects the state of the Intelligent Message Filter. This registry entry also serves as a reference point for the Intelligent Message Filter update package installer and for the Microsoft Update detection logic. This registry entry enables the update package installer to know whether the Intelligent Message Filter update functionality has been enabled on the server. If the registry entry does not exist, Intelligent Message Filter update packages are not offered. If the registry entry exists, Intelligent Message Filter update packages are offered.

The existing active version of the .dat file that is currently installed on the computer is recorded under the following registry sub key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Exchange Server 2003\SP3
```

For example, after you install the IMF-KB907747-2005.12.14-x86.exe update, the registry entry is similar to the following:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Exchange Server 2003\SP3\KB907747
```

This registry entry is verified every time that an update is offered for installation. If an update is successfully installed, the registry entry is updated. The update package installer knows which update is currently being installed. The update package installer compares that value to the current registry entry value. If the value is earlier than the update that is currently being offered, the update package installer performs the following actions, in this order:

1. Verifies that Exchange Server 2003 SP2 or a later version is installed on the server.
2. Records the existing active version number from the following registry entry:  

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Updates\Exchange Server 2003\SP3.
```
3. Creates a subfolder that is named the same as the build number. This subfolder is created in the MSCFV2 folder. The path of the folder is similar to the following: Drive\_Letter:\Program Files\ExchSrvr\Bin\ MSCFV2\BuildNumber.
4. Copies the Intelligent Message Filter .dll file and the Intelligent Message Filter .dat file to the newly created subfolder.
5. Registers the Intelligent Message Filter .dll file.
6. Updates the registry key based on the update version number.
7. Deletes all updates that exist on the system except for the current update that has been installed by the update package installer and the last two updates. Therefore, after the first three updates, the next update removes the oldest update. This always leaves the latest three updates on the computer. Updates are installed in a sequential order. For example, if updates U1, U2, U4 are installed, the next update that can be installed is U5 or a later update. When U5 is installed, U1 is removed.
8. During the update process, the update package installer restarts the IIS Admin Service for the package to take effect.

## 5.6 How to Uninstall Updates

The latest Intelligent Message Filter updates can be uninstalled by using **Add or Remove Programs** in Control Panel. If you uninstall the latest Intelligent Message Filter update, the files from the corresponding subfolder in the MSCFV2 folder are removed. Additionally, the registry entry under the following sub key is removed:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Exchange Server 2003\SP3\KB907747
```

If the Intelligent Message Filter update packages have been uninstalled by using **Add or Remove Programs**, the base version is re-registered. Therefore, the Intelligent Message Filter is functional based on the original .dat file that was shipped in Exchange Server 2003 SP2.

## How to Manually Install an Update or Roll Back to an Earlier Version

You can also manually install the Intelligent Message Filter update by browsing the Microsoft Update site, scanning for updates, and then selecting the Intelligent Message Filter update.

When it is required, you can quickly roll back the Intelligent Message Filter version by re-registering the .dll file from any one of the three folders that contain the last three updates. To do this, follow these steps.

#### **Notes:**

- For this example, assume that the following conditions are true. The three folders are as follows and you want to register Intelligent Message Filter version 6.5.7615.0.
- Drive\_Letter:\Program Files\Exchsvr\Bin\MSCFV2\6.5.7612.0
- Drive\_Letter:\Program Files\Exchsvr\Bin\MSCFV2\6.5.7615.0
- Drive\_Letter:\Program Files\Exchsvr\Bin\MSCFV2\6.5.7620.0

#### **To manually install an update or roll back to an earlier version**

1. Click **Start**, click **Run**, type the following command, and then click **OK**: **regsvr32 "Drive\_Letter:\Program Files\Exchsvr\Bin\MSCFV2\6.5.7615.0\MSEExchange.UceContentFilter.dll"**
2. Click **OK** to accept the registration confirmation message.
3. Click **Start**, click **Run**, type **iisreset**, and then click **OK**.

## **5.7 Service Packs**

When new service packs for Exchange Server 2003 are released, you might not be able to immediately upgrade to the new service pack. For example, suppose that Exchange Server 2003 Service Pack (SP3) is released. You continue to install the Intelligent Message Filter updates on schedule. Later, if you install the new service pack (Exchange Server 2003 SP3), the Intelligent Message Filter update is replaced by the version of the Intelligent Message Filter that is available in Exchange Server 2003 SP3. In this scenario, you must manually install the latest Intelligent Message Filter update.

When you regularly update the Intelligent Message Filter, at some point in time, you may reinstall a service pack. In this scenario, the Intelligent Message Filter update is replaced by an earlier version of the Intelligent Message Filter update that was available with the service pack. You must manually install the latest Intelligent Message Filter update.

## **5.8 Custom Weight List Functionality**

If you enable the Custom Weight List functionality on the server that is running Exchange Server 2003 SP2, you must manually copy the Custom Weight List file MSEExchange.UceContentFilter.xml to the newly created MSCFV2 folder.

After the Intelligent Message Filter updates, you have to manually copy the following Custom Weight List file to the subfolder of the MSCFV2 folder that was created during the update: MSEExchange.UceContentFilter.xml.

The subfolder of the MSCFV2 folder contains the updated filter.

For more information about the Custom Weight List, including a sample XML file, see the Microsoft Exchange Server 2003 Service Pack 2 Release Notes at <http://go.microsoft.com/fwlink/?linkid=52072>. Or refer to Appendix 1 of this document.

## **5.9 Unsupported Scenarios: Clustered Environment**

The Intelligent Message Filter is not supported in a clustered environment. Therefore, Intelligent Message Filter updates are not offered to Exchange Server 2003 servers in a clustered environment.

#### **Note:**

Intelligent Message Filter updates are supported in Network Load Balancing clusters.

## 5.10 Automatic Updates

When you select the **Automatic** option in Automatic Updates, Intelligent Message Filter updates, together with other updates, are downloaded and installed on the computer without user intervention. However, you should not enable Automatic Updates to automate installation of Intelligent Message Filter updates. When you use Automatic Updates, the following options are available:

1. Automatic download and installation of an update
2. Automatic download of an update
3. Notification of an update

These options are per computer and cannot be applied to an individual update. Because an automatic download and installation of the Intelligent Message Filter update will cause a restart of the IIS Admin Service, make sure that this setting is set for option 2 on servers that are running the Intelligent Message Filter. This will prevent any unplanned downtime. Also, it is recommended that you apply Intelligent Message Filter updates when there is a reduced load on the server to minimize disruption of services.

## 6 Monitoring and Troubleshooting

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

### 6.1 How to Use Event Viewer

In Event Viewer, both the Application log and the System log contain errors, warnings, and informational events that relate to the operation of Exchange Server, the Simple Mail Transfer Protocol (SMTP) service, and other applications. To help you determine the cause of Intelligent Message Filter problems, carefully review the data 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, on 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**.

The following table explains the events that are logged by Intelligent Message Filter. Unless otherwise noted, all events are logged at the default logging level.

Event	Explanation
<b>Event ID: 7512</b> Severity=Informational Text: The message with ID <message id>, P1 From <sender name>, Subject <subject> from remote host <host name> was Rejected/Deleted by the Intelligent Message Filter.	Intelligent Message Filter writes this event when it rejects or deletes a message at the gateway.  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.

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 enabled 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 when enabling or updating Intelligent Message Filter.</p> <p>Uninstall the new version of Intelligent Message Filter (newly installed Intelligent Message Filter Update package) and try 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 tried 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 cannot filter a message. Possible causes are corrupted or malformed messages.</p>

## 6.2 How to Use System Monitor and Performance Logs and Alerts

Intelligent Message Filter has several performance counters that you can use to monitor 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**.

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 might not be functioning correctly.

Counter	Description
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 Acted Upon	The total number of messages that Intelligent Message Filter has identified as UCE and acted on based on the action specified by an administrator.
UCE Messages Acted Upon/sec	The number of messages acted on per second by Intelligent Message Filter. This counter indicates how quickly Intelligent Message Filter takes action on items that are identified as UCE.
% 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 X	The total number of messages scanned by Intelligent Message Filter that were assigned a spam confidence level (SCL) rating of x, where x is a spam rating of 0 to 9.


## 6.3 Uninstalling Version 1 of Intelligent Message Filter

You must uninstall Intelligent Message Filter v1, which was an add-in, before you can install Exchange Server 2003 Service Pack 2 (SP2) which includes Intelligent Message Filter v2. Typically, you use the **Add or Remove Programs** option from Control Panel to perform an uninstall. (Click **Start**, click **Control Panel**, and then click **Add or Remove Programs**.) However, in some cases, Intelligent Message Filter v1 does not appear in the list of programs, or the SP2 installation is blocked after you do find and uninstall v1. Possible reasons for this are as follows.

When Intelligent Message Filter v1 does not appear in the **Add or Remove Programs** list, a likely reason is that you are trying to uninstall it from a different account than what was used to originally install it. If, for example, Intelligent Message Filter v1 was installed with Administrator permissions, but you are trying to use an Administrator-equivalent account to install Exchange Server 2003 SP2, the SP2 installer will fail and Intelligent Message Filter will not be listed in **Add or Remove Programs**. In this case, log on with the account that was used to install Intelligent Message Filter v1, and then uninstall.

If the Intelligent Message Filter v1 is listed in **Add or Remove Programs** but the SP2 installation is still being blocked, try to first uninstall Intelligent Message Filter, install it again, restart, and uninstall. Usually, this should clean up the Intelligent Message Filter enough for SP2 to install cleanly.

If you still cannot uninstall v1, manually remove the Intelligent Message Filter from the server following these steps.

 **Caution:** Incorrectly editing the registry can cause serious problems that may require that you reinstall the operating system. Problems that results from editing the registry incorrectly may be unable to be resolved. Before editing the registry, back up any valuable data.

 **To manually remove Intelligent Message Filter v1**

1. Stop all Exchange services (Information Store, System Attendant, SMTP, and Exchange-aware antivirus services).
2. Rename the MSCFV1 folder in `X:\Program Files\Exchsrvr\bin`, where `X` is the drive letter where Exchange Server is installed.
3. Rename the ContentFilter.dll file in `X:\Program Files\Exchsrvr\bin\`, where `X` is the drive letter where Exchange Server is installed.
4. Open **regedit** and export the key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange`
5. Delete the **ContentFilterVersion** sub key from the registry.
6. Restart the server. You should now be able to install Exchange Server 2003 SP2 without errors.

## 7 Customizing Exchange Server Intelligent Message Filter


---

You can customize the following configuration settings in Microsoft® Exchange Server 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 that it archives.
- Filter messages sent by authenticated users. By default, authenticated users bypass Intelligent Message Filter.

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

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

 **Caution:** Incorrectly editing the registry can cause serious problems that may require that you reinstall the 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 topic.

### 7.1 Changing the Archive Location

The archive location is the directory where Intelligent Message Filter saves filtered messages when you decide to archive messages marked as UCE that have a rating greater than the specified gateway threshold configured on the **Connection Filtering** tab in **Message Delivery Properties**. By default, messages are archived in \Exchsrvr\mailroot\vsini\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**.

### 7.2 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 together 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.

## 7.3 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, 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 filters 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.

## 7.4 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 approximately 300 bytes. By default, the size limit for a user's rule is 510 KB. This default size typically allows for approximately 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 want to reduce the size limit. Conversely, you may want 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 you use 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.

## 8 Appendix

### 8.1 Custom Weighting File

The custom weighting feature in Intelligent Message Filter for SP2 lets administrators customize the behavior of Intelligent Message Filter, based on phrases that are in the body of an e-mail message, the subject line, or both.

There is no user interface associated with the custom weighting feature. Custom weighting is made available in the form of an XML configuration file that is read by Intelligent Message Filter upon initialization, and then reloaded any time the file changes. If the XML configuration file is not present when Intelligent Message Filter is started, you must restart the SMTP service. The custom weighting file, `MSExchange.UceContentFilter.xml`, should be located in the same directory as the `MSExchange.UceContentFilter.dll` and `.dat` files.

#### Sample XML File

The following sample XML file and the table of values demonstrate how this feature can be used, and how the behavior of Intelligent Message Filter can be customized.

```
<?xml version="1.0" encoding="UTF-16"?>
<CustomWeightEntries xmlns="http://schemas.microsoft.com/2005/CustomWeight">
  <CustomWeightEntry Type="BODY" Change="1" Text="foo1"/>
  <CustomWeightEntry Type="BODY" Change="-1" Text="foo2"/>
  <CustomWeightEntry Type="BODY" Change="5" Text="Special offer"/>
  <CustomWeightEntry Type="BODY" Change="-9" Text="Verlängertes Angebot"/>
  <CustomWeightEntry Type="SUBJECT" Change="MIN" Text="特別提供"/>
  <CustomWeightEntry Type="BOTH" Change="MAX" Text="Offre spéciale"/>
</CustomWeightEntries>
```

The following table describes the custom weight values.

Value	Description
Type=BODY	Searches for a match in the displayed body of a message.
Type=SUBJECT	Searches for a match in the displayed subject of a message.
Type=BOTH	Searches for a match in both the subject and body of a message.
Change	Defines what the effect of a match will be on the spam confidence level (SCL) score of a matched message. Change can be any integer value. If the phrase is matched, the change will be added to the original SCL value. SCL values will be normalized to a 0 to 9 range (if they exceed that range because of custom weights).  Change can also use the MIN or MAX keywords. Any time a phrase with the MIN keyword is matched, the message is given an SCL of 0 regardless of any other weights. Any time a phrase with the MAX keyword is matched, the message is given an SCL of 9 regardless of any other weights. Any time there is both MIN and MAX matches for one message, the message is given an SCL of 0.
Text	Custom weighting can accept any Unicode phrase up to 1,000 characters.

## Troubleshooting Custom Weighting

When the schema of the custom weighting file is broken or malformed, it will cause the filter of Intelligent Message Filter to fail loading.

If the custom weighting file does not exist, Intelligent Message Filter will continue to load and/or behave normally, without the use of the custom weighting feature.

After first creating a custom weighting file, the SMTP service must be restarted to pick up the file. When the filter has been loaded with a valid custom weighting file, any changes that you made to the file are immediately picked up.

### 8.2 Known Issues

- Microsoft Exchange Intelligent Message Filter Exchange Server 2003 SP2 does not create the registry key named ContentFilter under  
`HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange`  
during an upgrade from Exchange Server 2003 or Exchange Server 2003 SP1, where Intelligent Message Filter version 1 was not previously installed. Therefore, to obtain an extended functionality (for example, change the Archive directory), you must manually create the  
`HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange\ContentFilter`  
key and restart the SMTP service.
- After the restart of SMTP, all the values created under this key are automatically picked up and no additional restarts of services are required. If you are upgrading the computer where Intelligent Message Filter version 1 was previously installed, no action is required because the registry key is preserved during the upgrade.
- There is an error in the user interface in the Global Settings for Intelligent Message Filtering. Under Store Junk E-mail Configuration, the selection that reads Move messages with an SCL rating greater than or equal to, should only indicate "greater than."

### 8.3 Hints and Tips

By default when Exchange IMF archives a message, it does not archive the SCL rating assigned to the message. To direct Exchange to do so, create a registry key DWORD value, ArchiveSCL, and assign it a value of 1.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange\ContentFilter]
"ArchiveSCL"=dword:00000001
```

## 9 Copyright

---

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

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.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2007 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows Server, Windows Vista, Active Directory, ActiveSync, ActiveX, Entourage, Excel, FrontPage, Hotmail, JScript, Microsoft Press, MSDN, MSN, Outlook, SharePoint, Visual Basic, Visual C++, Visual Studio, Win32, Windows Mobile, Windows NT, and Windows Server System are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.