



## **Exchange 2007 Journaling Guide**

Websense® Email Security Solutions

## **Websense Advanced Email Encryption**

Copyright © 1996-2011 Websense, Inc. All rights reserved.

This document contains proprietary and confidential information of Websense, Inc. The contents of this document may not be disclosed to third parties, copied, or duplicated in any form, in whole or in part, without prior written permission of Websense, Inc.

Websense and the Websense Logo are registered trademarks of Websense, Inc. in the United States and/or other countries. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc. makes no warranties with respect to this documentation and disclaim any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

# Contents

What is journaling? . . . . .	1
Envelope versus standard . . . . .	2
Message size limit . . . . .	2
Journaling prerequisites . . . . .	2
Set up the journaling process . . . . .	2
Create a journaling contact . . . . .	3
Create an SMTP send connector . . . . .	4
Activate journaling . . . . .	7
Create a distribution group and add members (select users only) . . . . .	9
Implement journal rules (select users only) . . . . .	11
Disable NDRs (non-delivery reports) . . . . .	12
Troubleshooting tips . . . . .	15
Journaling best practices . . . . .	17
Remove Exchange 2007 journaling setup . . . . .	19
Remove address space domain . . . . .	19
Deactivate journaling . . . . .	20
Remove journal rule . . . . .	20
Remove the distribution group . . . . .	21
Remove the SMTP send connector . . . . .	22
Remove the journaling contact . . . . .	23



# 1

## Microsoft Exchange 2007 Journaling Guide

For regulatory and compliance reasons, many organizations are required to journal all communications in their organization, including email communication.

Microsoft Exchange Server provides a mechanism for journaling email messages. This mechanism can capture messages flowing through any MTA, including those in Websense email security solutions.

To use Exchange message journaling with Websense security products, you are required to have the Websense Email Archive add-on installed. Exchange message journaling works together with Websense Email Archive to record information about incoming and outgoing email messages.

This guide explains how to set up journaling for Microsoft Exchange 2007. It explains:

- ◆ [What is journaling?](#), page 1
- ◆ [Journaling prerequisites](#), page 2
- ◆ [Set up the journaling process](#), page 2
- ◆ [Troubleshooting tips](#), page 16
- ◆ [Journaling best practices](#), page 18
- ◆ [Remove Exchange 2007 journaling setup](#), page 20

### What is journaling?

---

Journaling is the ability to record all communications. Archiving, on the other hand, refers to reducing the strain of storing data by backing it up, removing it from its native environment, and storing it elsewhere. You can use Exchange journaling as a tool in your email retention or archival strategy.

Journaling is an operation on a customer's mail server that collects all email- inbound, outbound and internal- and can automatically and securely forward a copy to the archive.

Journaling does not capture existing messages stored in users' active mailboxes: it only captures new messages. As journaling captures new messages "in flight," users cannot alter nor delete email before it is archived.

Also, journaling does not capture miscellaneous items like contacts, calendar items or tasks. Consequently these items will not be saved in the archive.

## Envelope versus standard

In Exchange 2000 and 2003, the default method to capture messages sent to and from users ("Standard Journaling") does not capture all message header content like BCC recipients or distribution lists. As a result, later Exchange versions contain applications to capture this additional message information.

The new method to capture messages ("Envelope Journaling") forwards a single email to the Archive as an envelope with two parts: a report of message recipient information and the actual message (which becomes an attachment). Envelope Journaling associates all users with a message, including CC and BCC recipients and members of distribution groups. All envelope information is saved in the Archive.

By default, Exchange 2007 Journaling is Envelope format.

## Message size limit

Message size limit is currently 50MB for the Cloud Archive and 20MB for AdvisorMail. If you are dual-journaling to both Archives, your message size limit is 20MB.

Oversized messages sent via journaling cannot be saved in the Archive. If an email is oversized because of its attachments, neither the message nor the attachments will be archived.

## Journaling prerequisites

---

The following permissions and Microsoft Exchange components are required to configure Journaling for Exchange 2007.

Exchange Server Prerequisites:

1. Fully configured installation of Exchange
2. Administrator access to the server

## Set up the journaling process

---

There are 2 ways to configure Journaling on your Exchange 2007 server:

To set up message journaling for **all** email addresses, follow these steps:

1. [Create a journaling contact](#)
2. [Create an SMTP send connector](#)

3. *Activate journaling*
4. *Disable NDRs (non-delivery reports)*

To set up message journaling for **select** email addresses, follow these steps:

1. *Create a journaling contact*
2. *Create an SMTP send connector*
3. *Create a distribution group and add members (select users only)*
4. *Implement journal rules (select users only)*
5. *Disable NDRs (non-delivery reports)*

## Create a journaling contact

1. Open the Exchange Management Console window by selecting **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. Click the + sign to the left of Recipient Configuration.
3. Click **Mail Contact** under Recipient Configuration.
4. In the Actions pane, click **New Mail Contact**.
5. Select the **New Contact** option and then click **Next**.

6. In the New Mail Contact window, type Journaling in the **First Name** field, Contact in the **Last Name** field and Journaling Contact in the **Alias** field (a). Click **Edit** (b).

**New Mail Contact**

Introduction  
 **Contact Information**  
 New Mail Contact  
 Completion

**Contact Information**  
Enter the account information that is required to create a new mail contact or to mail-enable an existing mail contact.

Organizational unit:  
corp.contoso.com/Users

**a**

First name: Journaling Initials: Last name: Contact

Name: Journaling Contact

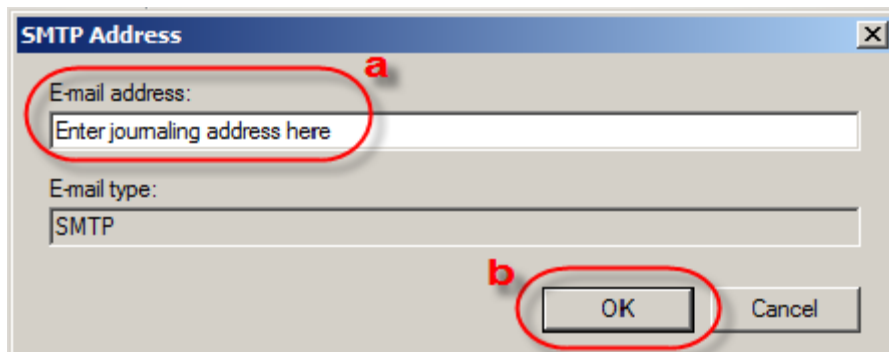
Alias: JournalingContact

External e-mail address:

**b**



7. Type the journaling address provided to you (a) and then click **OK** (b).

**Note**

The journaling address is unique to your organization. If you have not been provided with this address, please contact support.

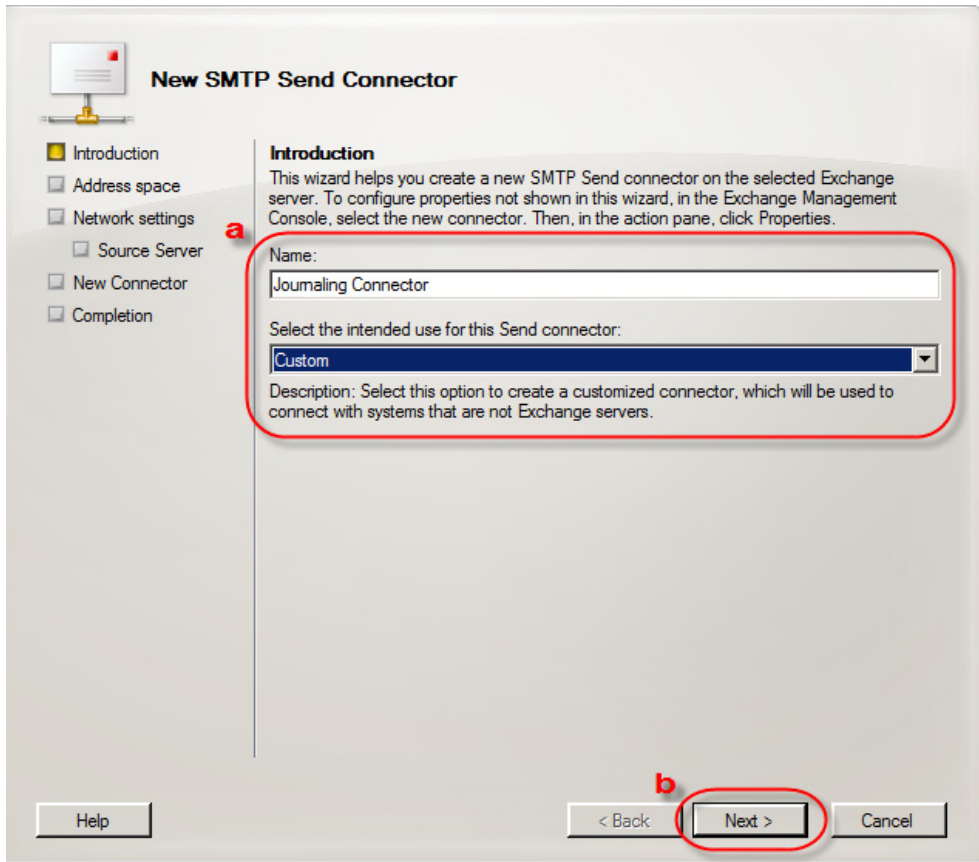
8. Click **Next**.
9. Click **New**.
10. Click **Finish**.

You have successfully created a journaling contact as shown below.

## Create an SMTP send connector

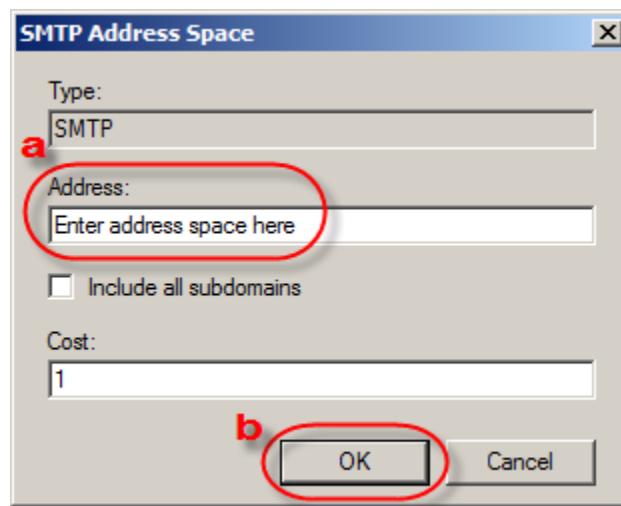
1. Open the Exchange Management Console window by selecting **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. Click the + sign to the left of Organization Configuration.
3. Click **Hub Transport**.
4. Click the **Send Connectors** tab.
5. In the Actions pane, click **New Send Connector**.

6. Type Journaling Connector for the **Name** and for the **Select the intended use for this Send connector** drop-down list, select **Custom** (a). Click **Next** (b).



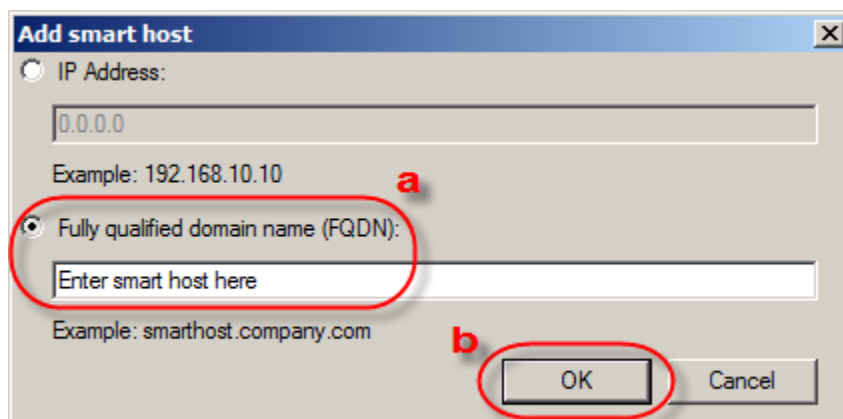
7. Click **Add**.

- In the SMTP Address Space window, type the Address Space provided to you in the **Address** field (a). Leave the cost at 1 and then click **OK** (b).



The screenshot shows the 'SMTP Address Space' dialog box. The 'Type' field is set to 'SMTP'. The 'Address' field is highlighted with a red circle and labeled 'a', containing the text 'Enter address space here'. The 'Cost' field is set to '1'. The 'OK' button is highlighted with a red circle and labeled 'b'.

- Click **Next**.
- Select the **Route mail through the following smart hosts** option and then click **Add**.
- Click the **Fully qualified domain name (FQDN)** option (a), type the Smart Host provided to you and click **OK** (b).



The screenshot shows the 'Add smart host' dialog box. The 'Fully qualified domain name (FQDN)' option is selected and highlighted with a red circle and labeled 'a'. The 'OK' button is highlighted with a red circle and labeled 'b'.

- Click **Next**.
- Select **None** for the **Configure smart host authentication settings** option, and then click **Next**.

14. Click **Next**.

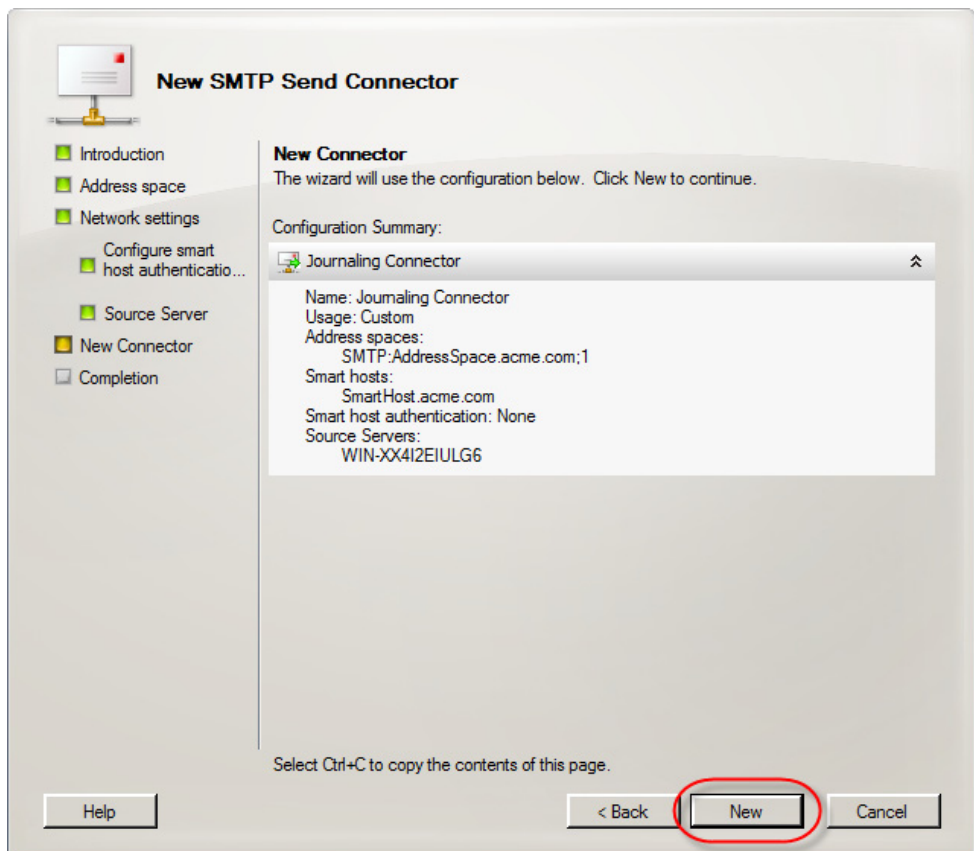


**Note**

Exchange 2007 servers automatically **send all outbound email via TLS encryption**: no outbound security configuration is required by the Administrator.

15. Click **New**.

16. Click **Finish**.

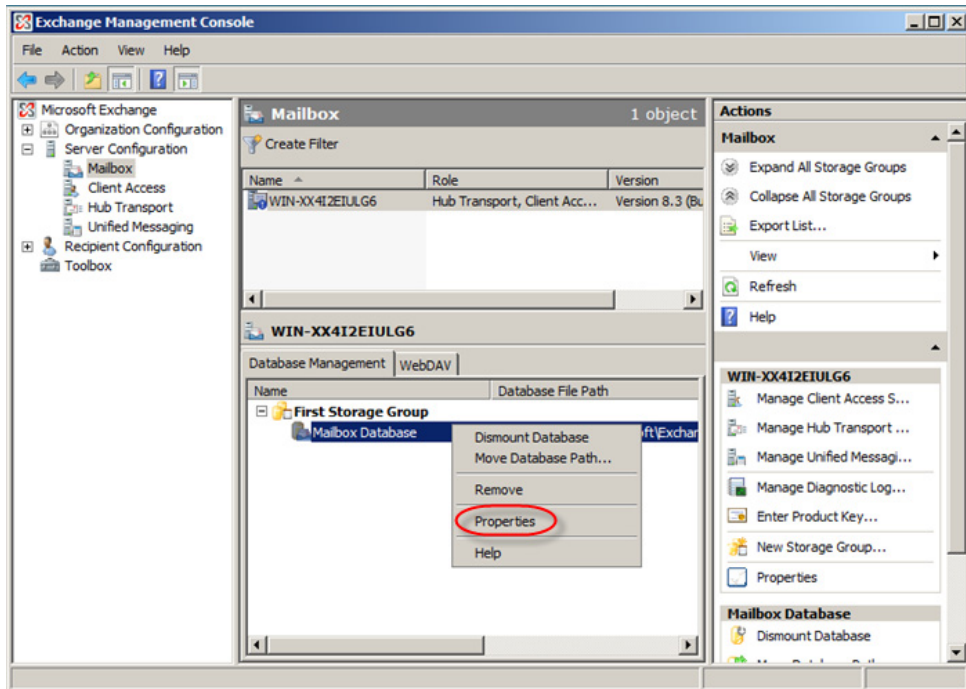


You have successfully created a send connector as shown below.

## Activate journaling

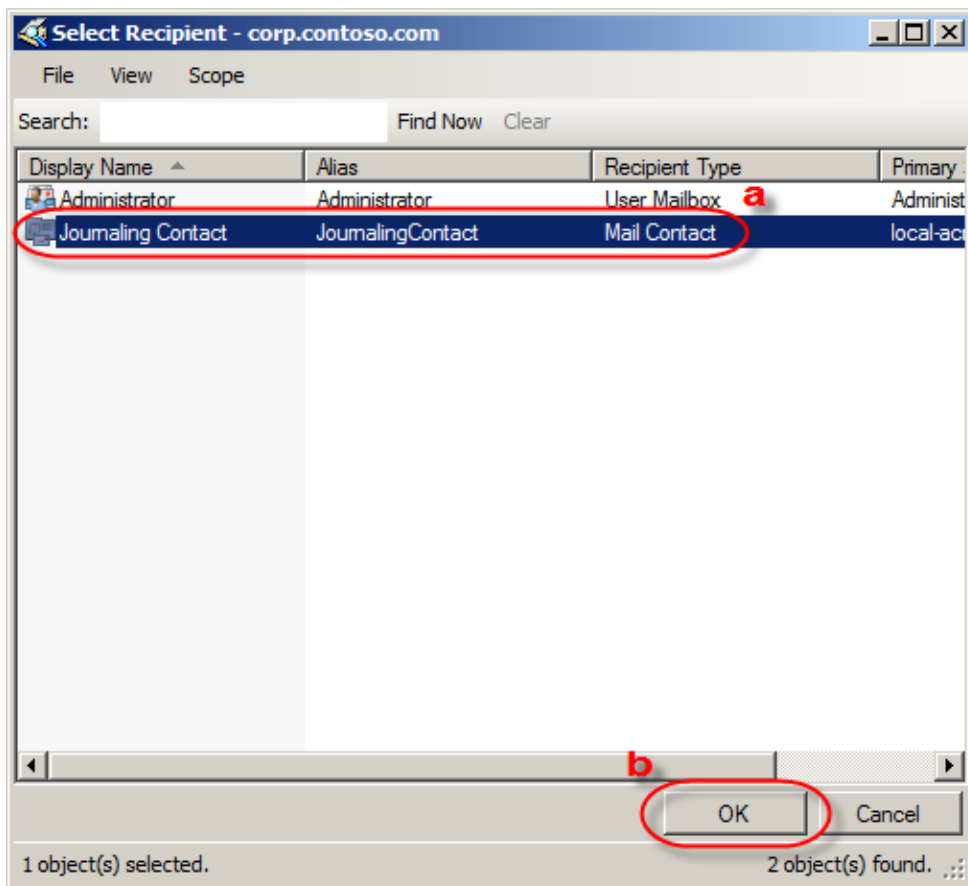
1. Open the Exchange Management Console window by selecting **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. Click the + sign to the left of Server Configuration.
3. Click **Mailbox**.

4. In the **Database Management** tab, right click your mailbox database and then select **Properties**.



5. In the Mailbox Database Properties window, select the **Journal Recipient** check box, and then click **Browse**.

6. Select **Journaling Contact** (a) and click **OK** (b).



7. Click **OK**.

You have successfully activated message journaling.

## Create a distribution group and add members (select users only)

1. Open the Exchange Management Console window by selecting **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. Click the + sign to the left of Recipient Configuration.
3. Click **Distribution Group**.
4. In the Actions pane, click **New Distribution Group**.
5. Ensure that the **New Group** option is selected and then click **Next**.

- In the New Distribution Group window, type Journaling Distro in the **Name** field and **Alias** field (a). Click **Next** (b).

**New Distribution Group**

Introduction  
Group Information  
New Distribution Group  
Completion

**Group Information**  
Enter account information for the distribution group.

Group type:  
 Distribution  
 Security

Organizational unit:  
corp.contoso.com/Users Browse...

**a**

Name:  
Journaling Distro

Name (pre-Windows 2000):  
Journaling Distro

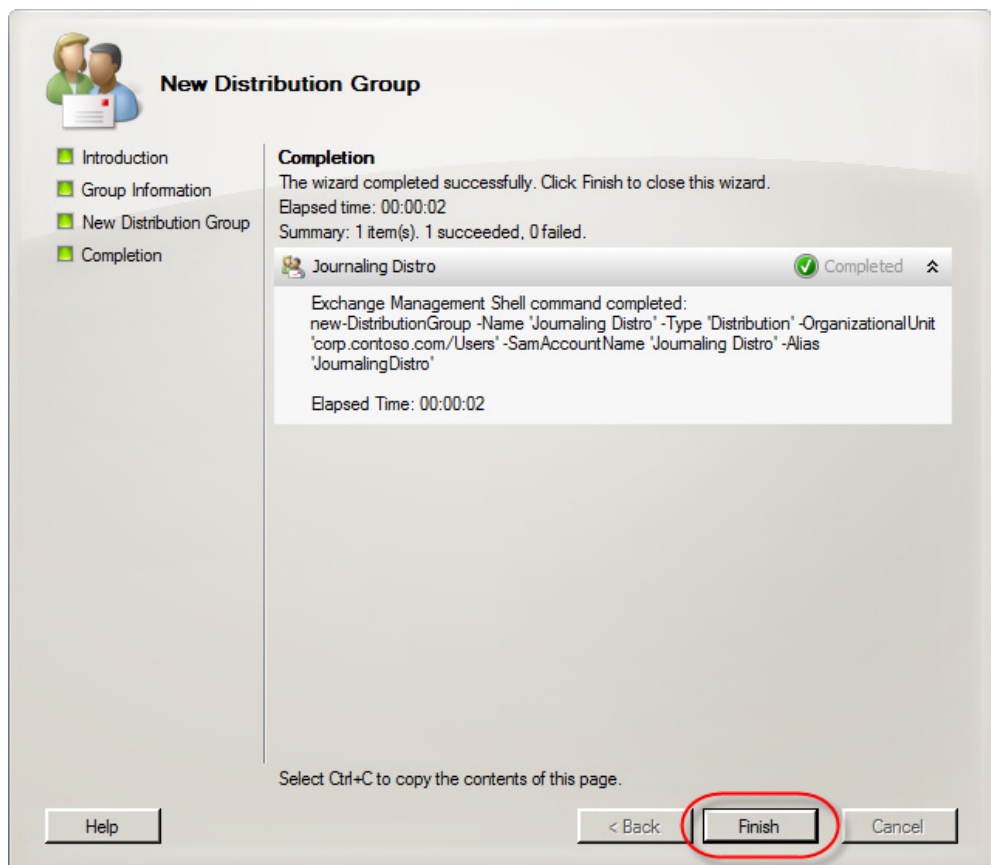
Alias:  
JournalingDistro

**b**

Help < Back Next > Cancel

- Click **New**.
- Click **Finish**.

You have successfully created a distribution group as shown below.



Add the users whose email messages you want journaled to the Journaling Distro distribution group.

## Implement journal rules (select users only)

1. Open the Exchange Management Console window by selecting **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. Click the + sign to the left of Organization Configuration.
3. Click **Hub Transport**.
4. In the Actions pane, click **New Journal Rule**.
5. In the New Journal Rule window, type Journaling Rule in the **Rule Name** field (a). Click **Browse** (b).
6. Select **Journaling Contact** from the list (a) and then click **OK** (b).
7. Select the **Journal messages for recipient** check box (a). Click **Browse** (b).
8. Select **Journaling Distro** from the list (a) and then click **OK** (b).
9. Click **New**.



10. Click **Finish**.

You have successfully implemented journal rules for select users in your organization.

## Disable NDRs (non-delivery reports)

1. Open the Exchange Management Console window by selecting **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. Click the + sign to the left of Organization Configuration.
3. Click **Hub Transport**.
4. Click the **Remote Domains** tab.
5. In the Actions pane, click **New Remote Domain**.

6. Enter a name for the remote domain in the **Name** field (a). Enter the domain name of the Address Space provided to you in the **Domain name** field (b). Click **New** (c).

**New Remote Domain**

New Remote Domain  
 Completion

**New Remote Domain**  
When you create a remote domain, you can control mail flow with more precision, apply message formatting and messaging policies, and specify acceptable character sets for messages that are sent to and received from the remote domain. After you create a remote domain, you can specify more advanced security, policy, and permission configurations for messages that you exchange with the remote domain.

a Name:  
Enter Remote Domain Description Here

b Domain name:  
Enter Address Space Domain Here

Include all subdomains

Help < Back **New** Cancel

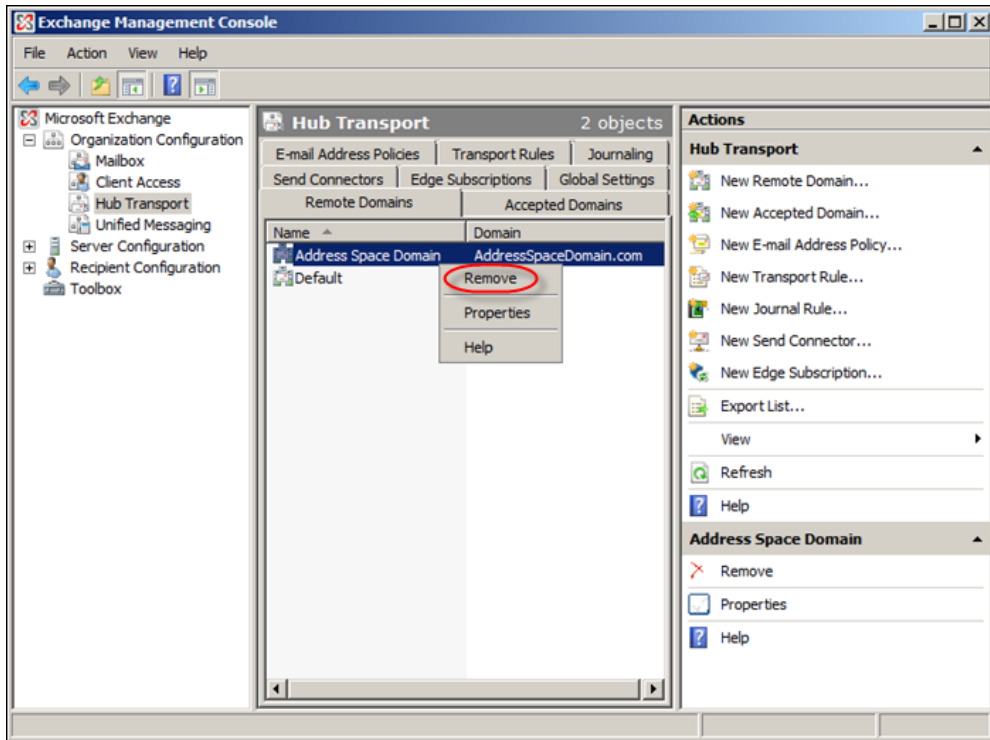


**Note**

If your address space is Address.Space@AddressSpace.com, then the Address Space domain is AddressSpace.com.

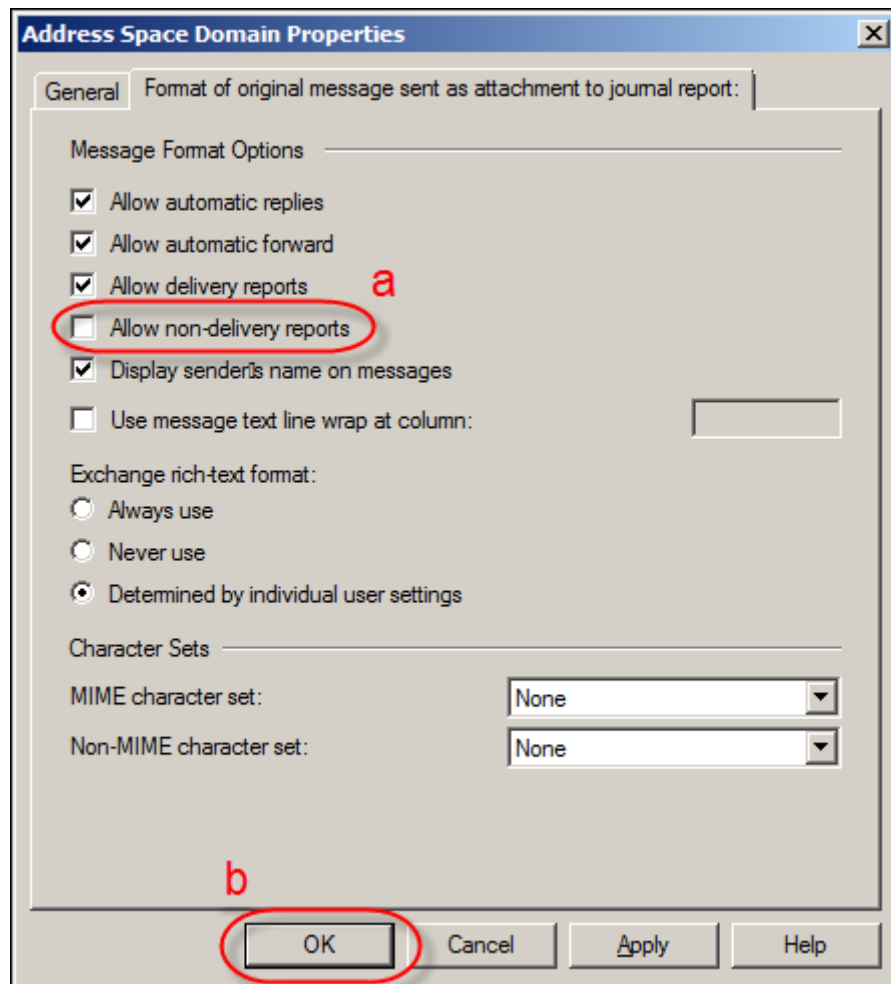
7. Click **Finish**.

8. In the **Remote Domains** tab, right click the Address Space Domain and select **Properties**.



9. Click the **Format of original message sent as attachment to journal report** tab.

10. Deselect the **Allow non-delivery reports** check box (a) and then click **OK** (b).



You have successfully disabled NDRs.



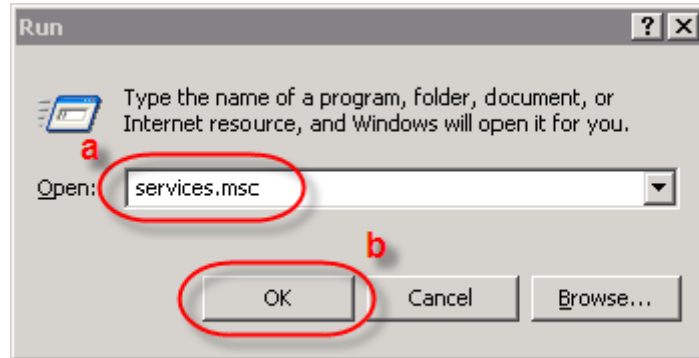
#### Note

Your Journaling set up is now complete. If you encounter any problems with the journaling process, or if journaling stops, please refer to the [Troubleshooting tips](#) below. If journaling stops for an extended period of time, we cannot recover lost email.

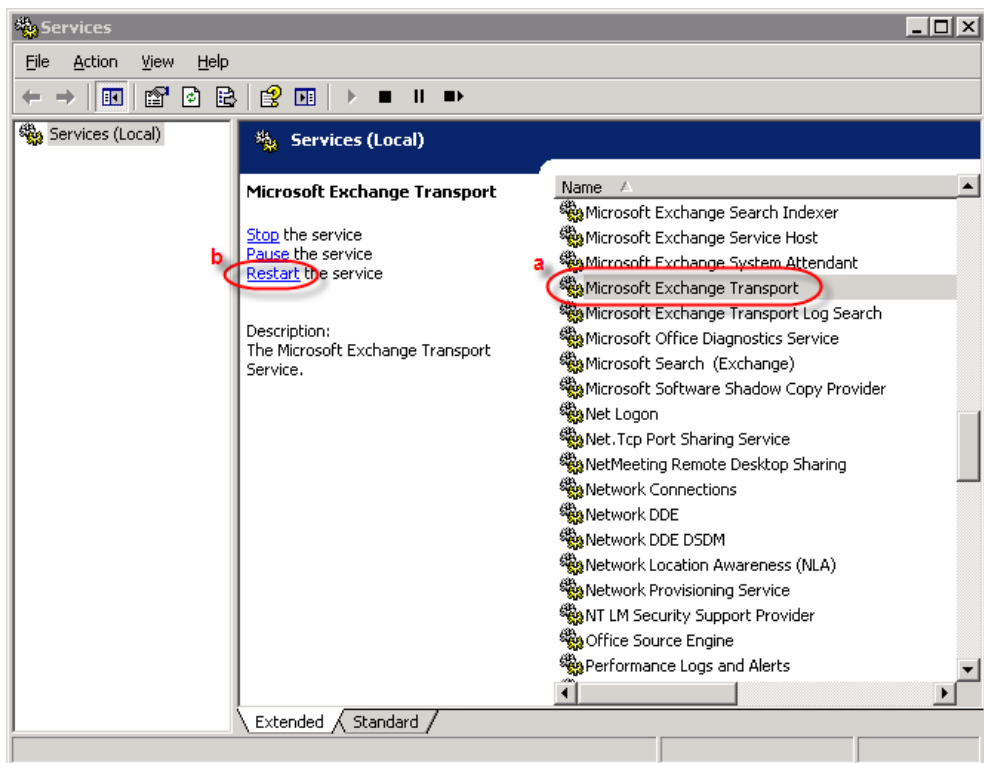
## Troubleshooting tips

- ◆ Make sure the Journaling Contact SMTP Email Address (journal address provided to you) is spelled correctly

- ◆ Restart the Microsoft Exchange Transport Service.
  - a. Click **Start** and then click **Run**.
  - b. Type **services.msc** in the text box (a) and then click **OK** (b).



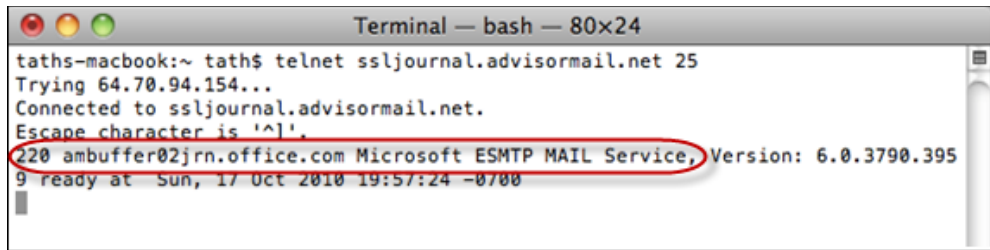
- c. Locate and click the **Microsoft Exchange Transport** service (a) and then click **Restart** (b).



A pop-up window will display with the message "Microsoft Exchange Transport service is being restarted." When the pop-up window automatically disappears, you have successfully restarted the service.

- ◆ Your firewall may be blocking outbound email messages.

- a. Many firewalls can block email messages sent using TLS encryption, even if they are set to allow all outbound email messages.
  - b. If you have a Cisco firewall, chances are very high that the ESMTP packet inspection is enabled and blocking the TLS-encrypted email messages. For more information, visit Cisco support by clicking on the link below or copying and pasting it into your web browser. <http://www.cisco.com/en/US/docs/security/asa/asa72/release/notes/asarn723.html#wp219670>.
- ◆ Verify there are no enabled Send Connectors utilizing the domain name of the contact being journaled to. Get-SendConnector | Where {\$\_.AddressSpaces – match “domain.com”} If you get a match on one, then there is a send connector handling that domains email.
  - ◆ Check if you are having a connection issue.
    - a. Issue telnet to smarthost (i.e. telnet ssljournal.advisormail.net 25) this should return a 220 banner, seen in the figure below.



```
Terminal — bash — 80x24
taths-macbook:~ tath$ telnet ssljournal.advisormail.net 25
Trying 64.70.94.154...
Connected to ssljournal.advisormail.net.
Escape character is '^['.
220 ambuffer02jrn.office.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.395
9 ready at Sun, 17 Oct 2010 19:57:24 -0700
```

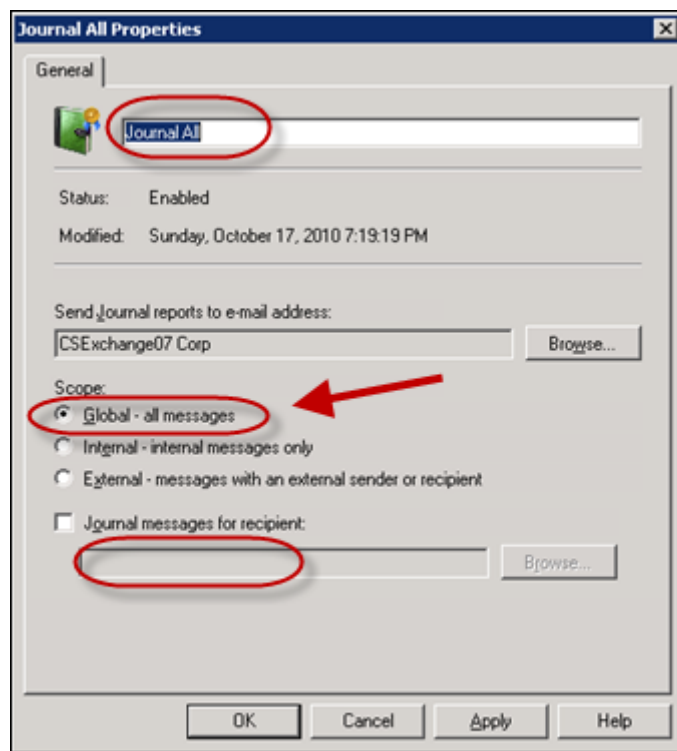
- ◆ If email messages are journaling, but some or all messages seem to archive incorrectly, check the following:
  - a. Add domain.com (shown on address space of send connector) to the remote domain tab under **Organization Configuration > Hub Transport**.
  - b. Click on the **Format of original message sent as attachment to journal report** tab.
  - c. On **Exchange rich-text format** select the **Never use** option.

## Journaling best practices

---

- ◆ Contact Archiving Support if you make any changes to your host provider or upgrade your Exchange Server. You will be provided new setup instructions to update your journaling configuration.
- ◆ Monitor your Exchange Server for issues.
- ◆ When adding or deleting a user mailbox on your Exchange Server, make sure you also update that user in the Archive Administration tab.

- ◆ Make sure you hide the journal recipient(s) from your Global Address List (GAL).
- ◆ Envelope journaling using journaling rules
  - a. When journaling rules are implemented under the Hub transport, exchange transport agent is executed first and can conflict with messages being archive (if there's transport rules to drop messages). You need to set the journaling agent as first priority using the steps below. Once this is set even messages that are meant to drop will be archived.
  - b. Open EMS.
  - c. Set-transport agent: identity is "journaling agent," priority is "1".
  - d. Restart services (services.msc) for MExchangeTransport or via a Command window by typing net stop msxchangetransport & net start msxchangetransport.
- ◆ I want to journal all messages on my Exchange server, but do not want to enable journaling on each mailbox store.
  - a. Create a new journaling rule, seen in the figure below.



- b. On Send journal reports to e-mail address, click **Browse** to select a contact.
- c. Select **Global – all messages**.
- d. Ensure the **Journal messages for recipient** option is deselected. Selecting this will journal all messages for all users for the entire Organization.

- ◆ Verify the journaling mailbox is set to allow mail only from Microsoft Exchange and Authenticated Senders Only.
  - a. Set-Mailbox <Journal Mailbox Name> -AcceptMessagesOnlyFrom "Microsoft Exchange" -RequireSenderAuthenticationEnabled:\$true

## Remove Exchange 2007 journaling setup

---

There are 2 ways to remove Exchange 2007 journaling setup:

Remove Exchange 2007 journaling setup for **all** users, follow these steps:

1. *Remove address space domain*
2. *Deactivate journaling*
3. *Remove the SMTP send connector*
4. *Remove the journaling contact*

Remove Exchange 2007 journaling setup for **select** users, follow these steps:

1. *Remove address space domain*
2. *Remove journal rule*
3. *Remove the distribution group*
4. *Remove the SMTP send connector*
5. *Remove the journaling contact*



### Note

Only complete the above steps if you wish to stop sending email to the Archive. Once you remove the journaling setup, email cannot be saved in the Archive.

---

## Remove address space domain

1. Open the Exchange Management Console window by selecting **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. Select the + sign to the left of Organization Configuration.
3. Select **Hub Transport**.
4. Select the **Remote Domains** tab.
5. Right click **Address Space Domain** and then select **Remove**.
6. Click **Yes** to confirm.

You have successfully removed the Address Space Domain.



## Deactivate journaling

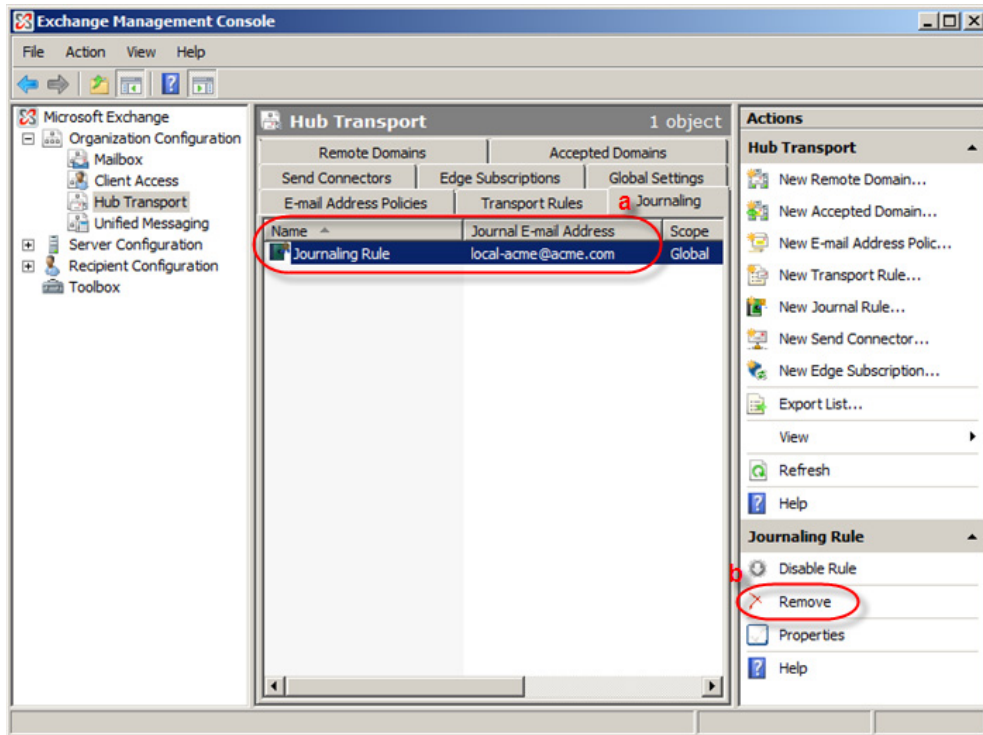
1. Open the Exchange Management Console window by selecting **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. Select the + sign to the left of Server Configuration.
3. Select **Mailbox**.
4. Within the Database Management section, right-click your mailbox database and select **Properties**.
5. Within the **General** tab, deselect the **Journal Recipient** check box and then click **OK**.

You have successfully deactivated journaling.

## Remove journal rule

1. Open the Exchange Management Console window by selecting **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. Select the + sign to the left of Organization Configuration.
3. Select **Hub Transport**.
4. Select the **Journaling** tab.

5. Select the Journal Rule whose Journal Email Address, from within the list, that matches the journaling address used during the journaling setup (a) and then select **Remove** in the right-hand Actions pane (b).



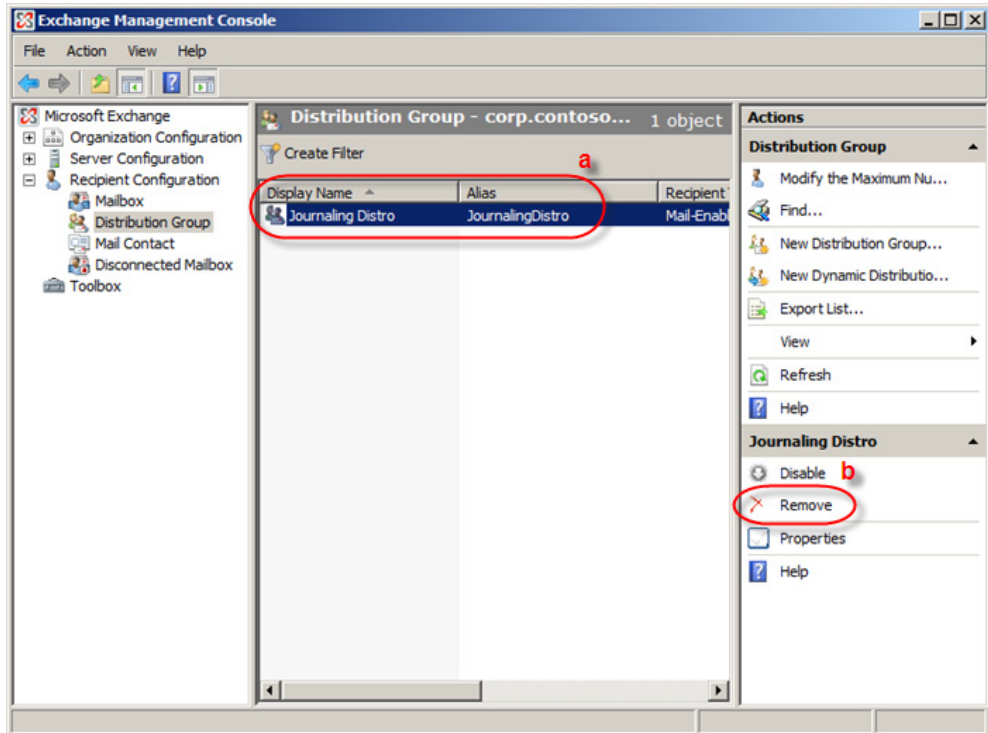
6. Click **Yes** in the resulting confirmation dialog box.

You have successfully deleted the Journal Rule.

## Remove the distribution group

1. Open the Exchange Management Console window by selecting **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. Select the + sign to the left of Recipient Configuration.
3. Select **Distribution Group**.

4. Select the distribution group for the journaling setup you are deleting (a), from within the list, and then click **Remove** in the Actions pane (b).



5. Select **Yes** in the resulting confirmation dialog box.

You have successfully deleted the Journaling Distribution Group.

## Remove the SMTP send connector

1. Open the Exchange Management Console window by selecting **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. Select the + sign to the left of Organization Configuration.
3. Select **Hub Transport**.
4. Select the **Send Connectors** tab.
5. Your Send Connectors display in a list. To find the Send Connector associated with your journaling setup, follow these steps:
  - a. Right-click a **Send Connector**, from within the list, and then select **Properties**.

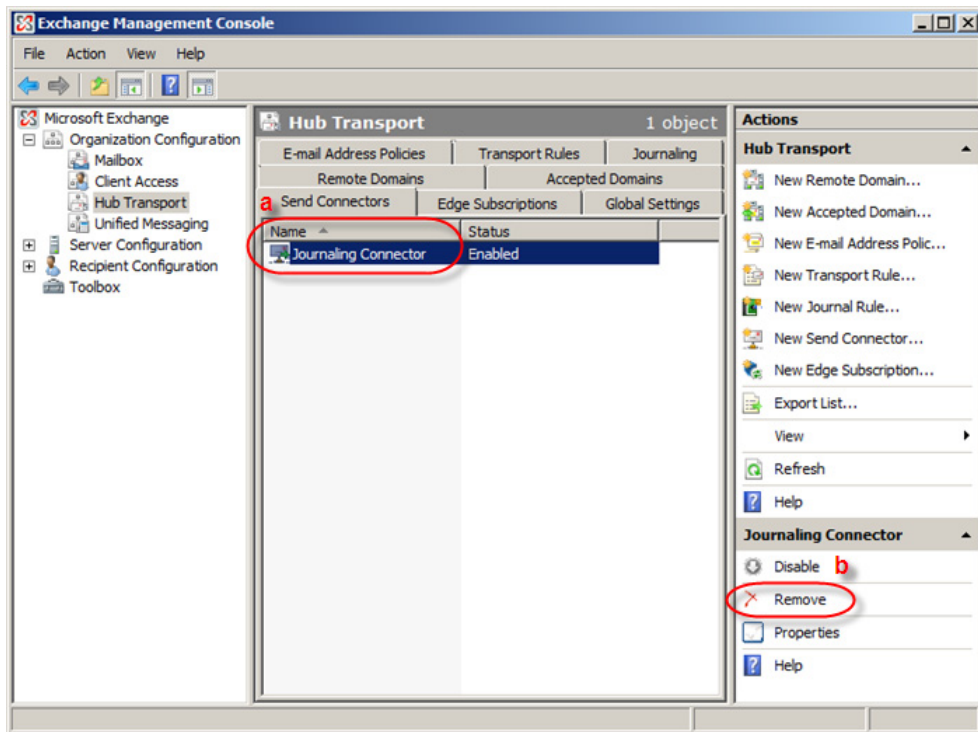
- b. Select the **Address Space** tab, within the Journaling Connector Properties dialog box. If the address listed (a) matches the Address Space used during the journaling setup, this Send Connector must be deleted. Select **Cancel** (b) to close the dialog box.



**Note**

If the address listed does not match the Address Space used during the journaling setup, repeat the above steps.

6. Select the Send Connector that needs to be deleted, from within the list (a), and then select **Remove** in the right-hand Actions pane (b).



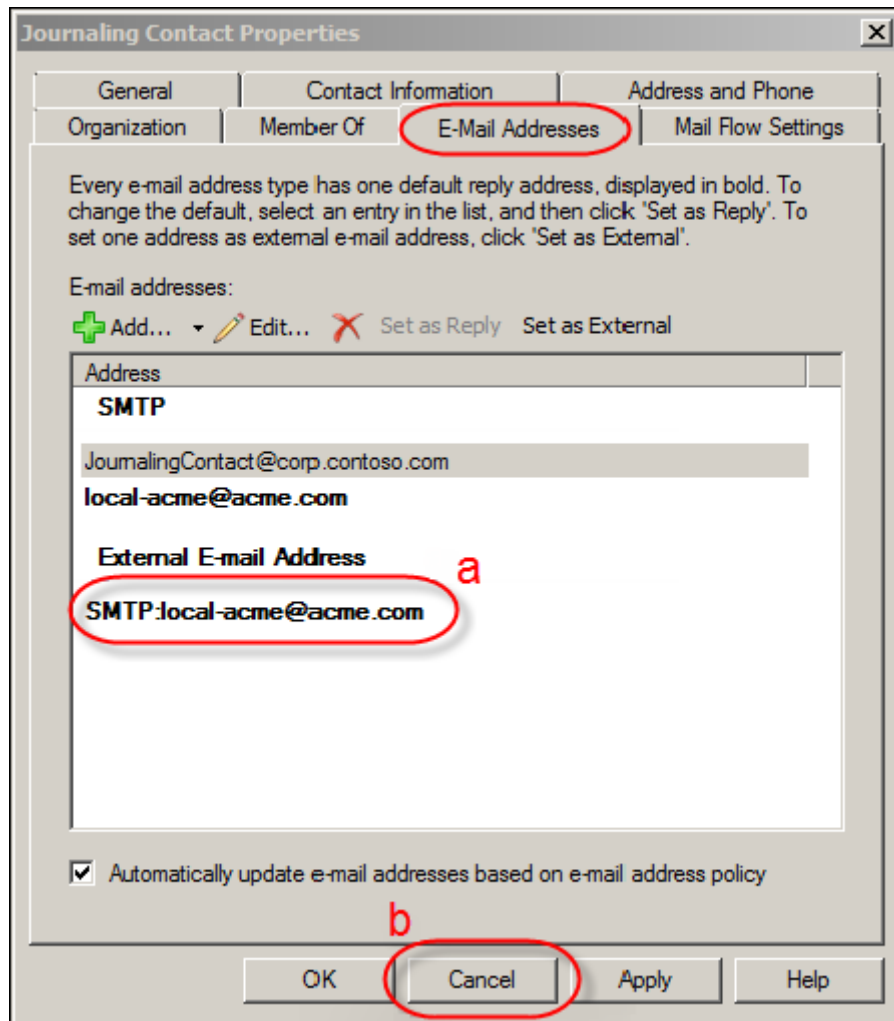
7. Select **Yes** on the resulting warning dialog box.

You have successfully deleted the SMTP Send Connector.

## Remove the journaling contact

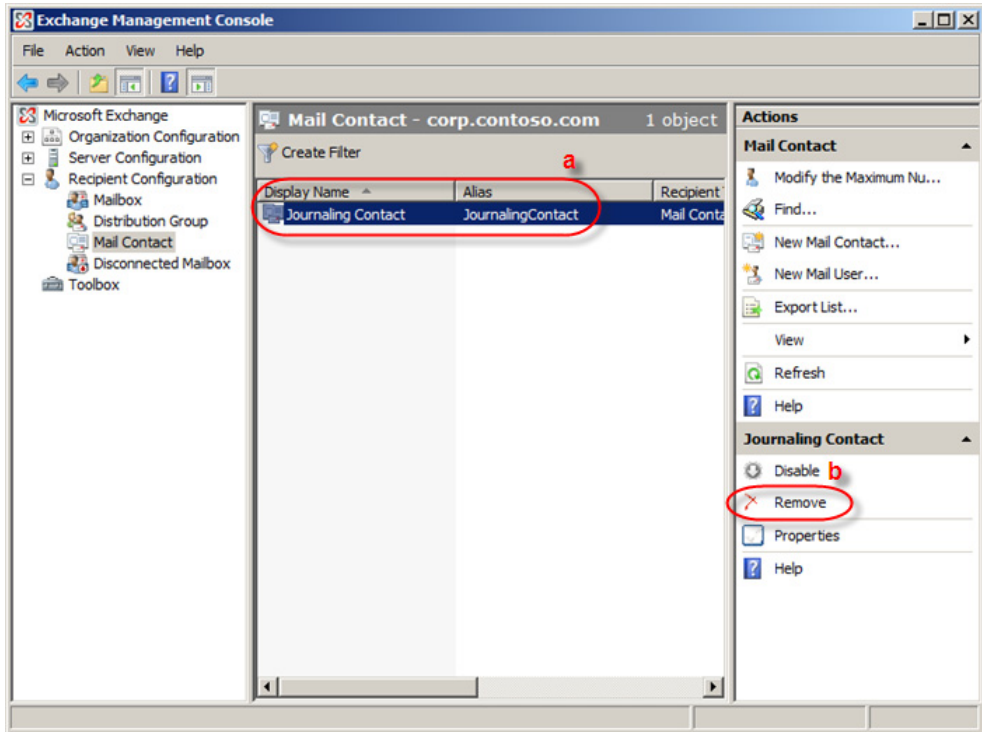
1. Open the Exchange Management Console window by selecting **Start > All Programs > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. Select the + sign to the left of Recipient Configuration.
3. Select **Mail Contact**, within the Recipient Configuration node. Your Mail Contacts display in a list.

4. To find the Mail Contact associated with your journaling setup, follow these steps:
  - a. Right-click a Mail Contact, from within the list, and select **Properties**.
  - b. Select the Email Addresses tab. If the external email address (a) matches the Journaling Address used during the journaling setup, this Mail Contact must be deleted. Select Cancel (b) to close the dialog box.

**Note**

If the external address listed does not match the **Journal Address** used during the journaling setup, repeat the above steps.

5. Select the Mail Contact that needs to be deleted, from within the list (a), and then select **Remove** in the right-hand Actions pane (b).



6. Select **Yes** on the resulting warning dialog box.  
You have successfully removed the journaling contact.