



Exchange 2003 Standard 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 journaling process	2
Create a custom recipient (contact)	3
Create an SMTP connector	8
Activate journaling	17
Disable NDRs (non-delivery reports)	20
Add SMTP queue growth monitoring alert	23
Troubleshooting tips	27
Journaling best practices	29
Remove Exchange 2003 journaling setup	29
Removing SMTP growth alert	30
Deactivate journaling	34
Remove the journaling SMTP connector	36
Remove the journaling contact from active directory	38

Exchange 2003 Standard 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 standard journaling for Microsoft Exchange 2003. It explains:

- ◆ *What is journaling?*
- ◆ *Journaling prerequisites*
- ◆ *Set up journaling process*
- ◆ *Troubleshooting tips*
- ◆ *Journaling best practices*
- ◆ *Remove Exchange 2003 journaling setup*

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.

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 2000-2003 Standard server.

Exchange Server Prerequisites

1. Fully configured installation of Exchange 2003 Standard Server
2. Administrator access to the server

Set up journaling process

To configure Journaling on your Exchange 2003 Standard server, follow these steps:

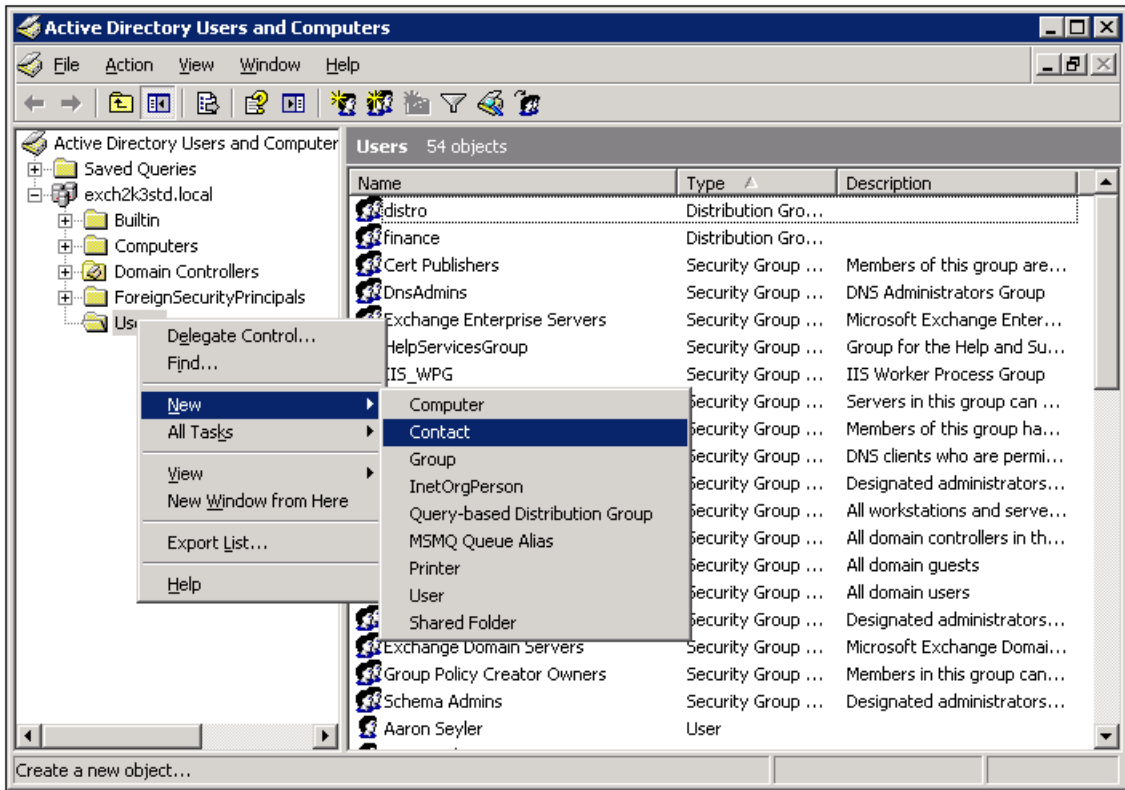
To setup message journaling for **all** email addresses, follow these steps:

1. *Create a custom recipient (contact)*
2. *Create an SMTP connector*
3. *Activate journaling*

4. *Disable NDRs (non-delivery reports)*
5. *Add SMTP queue growth monitoring alert*

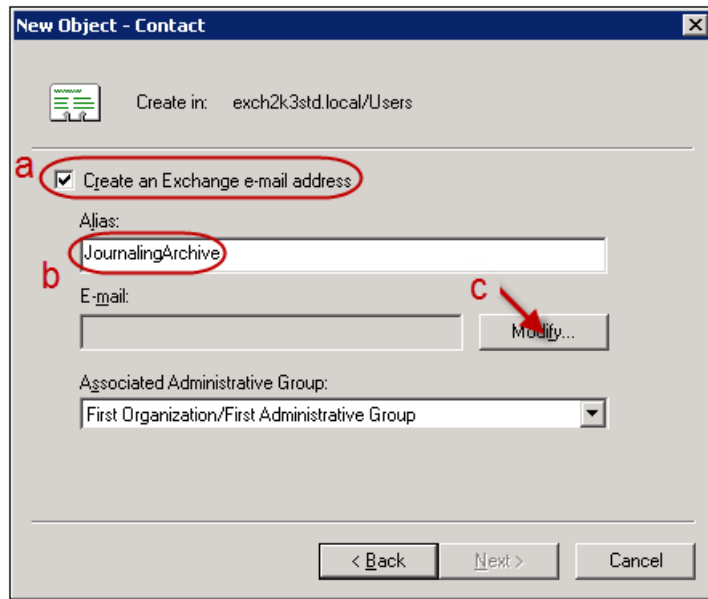
Create a custom recipient (contact)

1. Open the **Active Directory Users and Computers** window by selecting **Start > All Programs > Administrative Tools**.
2. Right click your mouse on **Users** and select **New**, then select **Contact**.

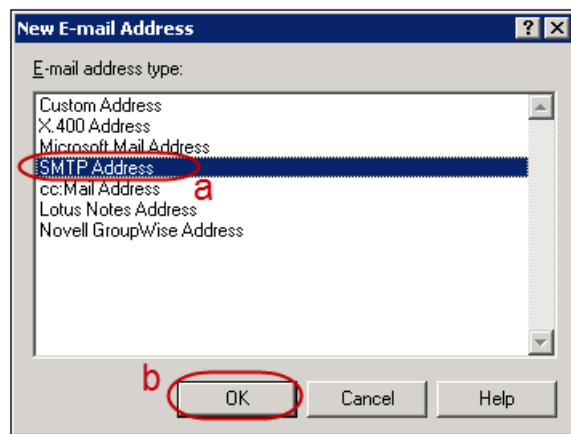


3. In the **New Object - Contact** window, type **"Journaling"** in the **First name** field, **"Archive"** in the **Last name** field (a). **"Journaling Archive"** should automatically populate in the **Full name** field. The **Display name** field is optional. Click **Next** (b).

4. Select the **Create an Exchange email address** checkbox (a). The **Alias** field should populate with the Full Name from the previous step (b). Click **Modify** (c).



5. Select **SMTP Address** in the **New E-mail Address** window (a) and then click **OK** (b).

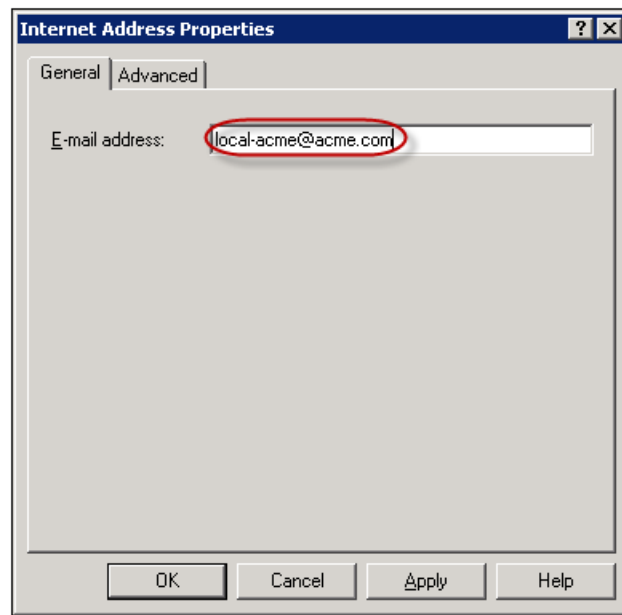


6. Type the **journaling address** provided to you in the **E-mail address** field on the **General** tab of the **Internet Address Properties** window.

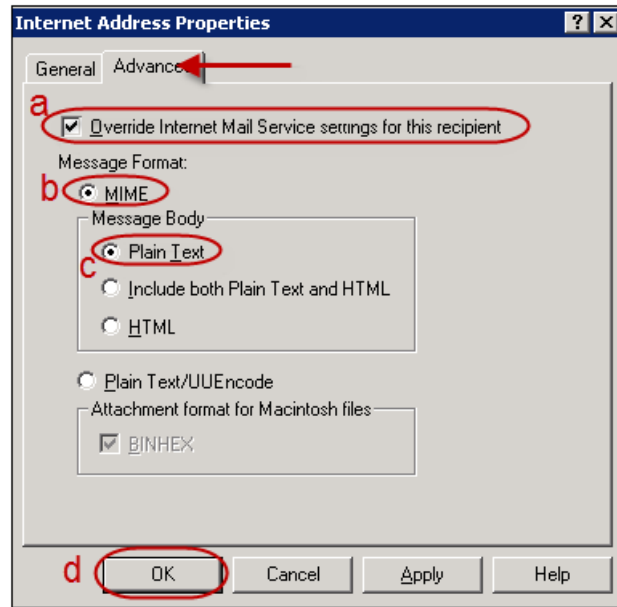


Note

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



7. In the **Internet Address Properties** window, click the **Advanced** tab and check the box for **Override Internet Mail settings for this recipient (a)**. Under Message Format: check the radio button for **MIME (b)**; under Message Body: check the radio button for **Plain Text (c)**, and then click **OK (d)**.



Note

Make sure you hide the journal recipient(s) from your Global Address List (GAL).

8. The **Internet Address Properties** window closes and the new email address you created appears in the **Email** field of the **New Object - Contact** popup window
(a). Click **Next (b)**.

The screenshot shows the 'New Object - Contact' dialog box. At the top, it says 'Create in: exch2k3std.local/Users'. There is a checked box for 'Create an Exchange e-mail address'. The 'Alias:' field contains 'JournalingArchive'. The 'E-mail:' field contains 'SMTP:local-acme@acme.com' and is circled in red with a red arrow pointing to it from the left, labeled 'a'. Below it is the 'Associated Administrative Group:' dropdown menu, which is set to 'First Organization/First Administrative Group'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is circled in red with a red arrow pointing to it from above, labeled 'b'.

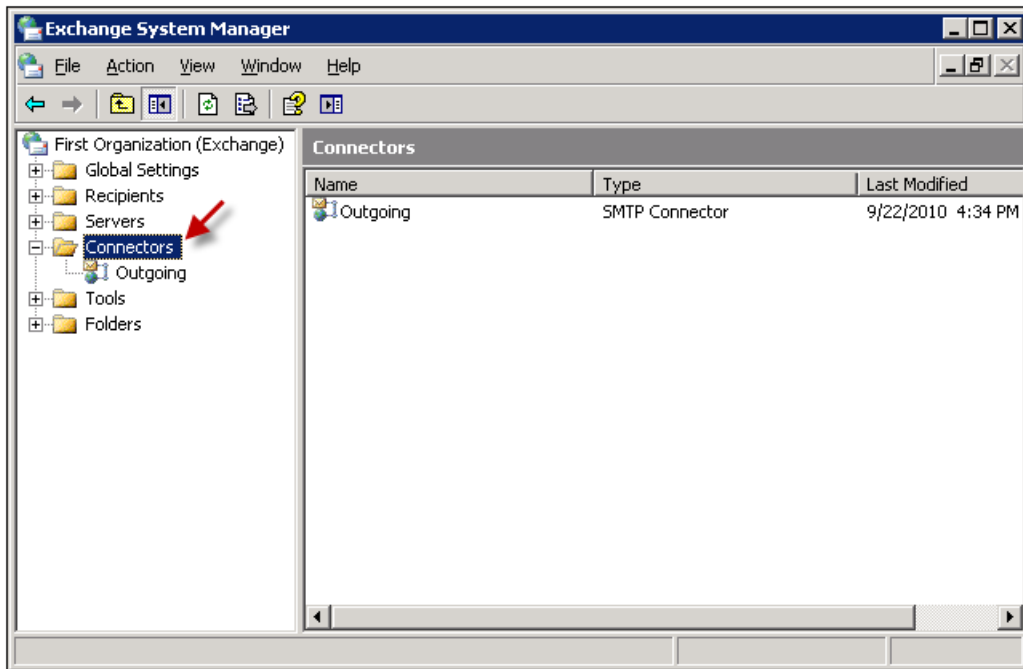
9. Click **Finish**.

The screenshot shows the 'New Object - Contact' dialog box in a later stage. It displays a preview of the object to be created: 'When you click Finish, the following object will be created:' followed by a text box containing 'Full name: Journaling Archive'. At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'. The 'Finish' button is circled in red with a red arrow pointing to it from above.

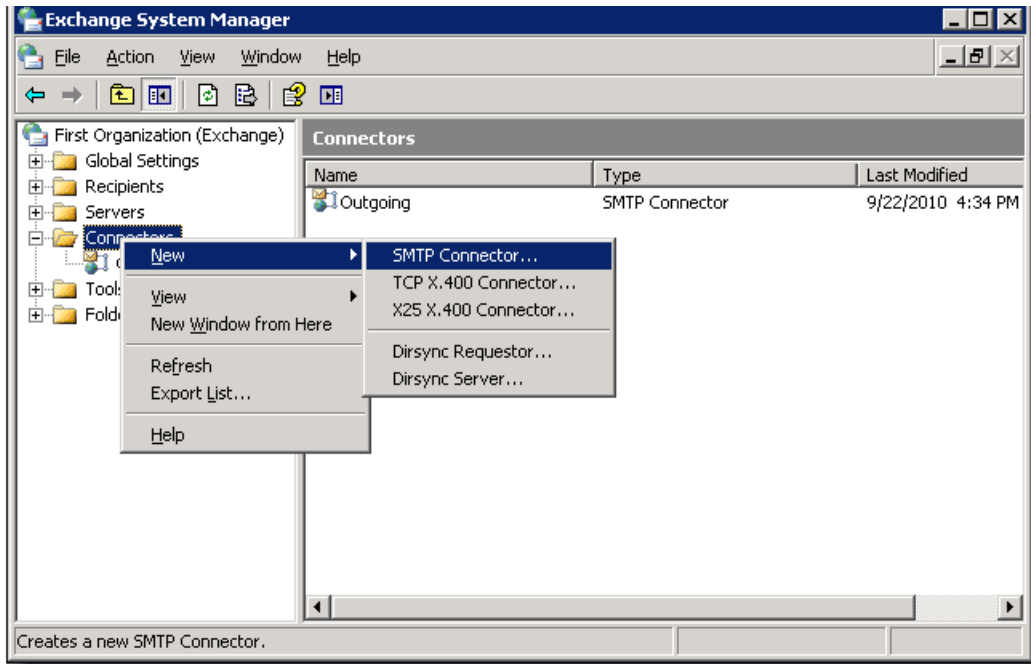
10. **You have successfully created a custom recipient.**

Create an SMTP connector

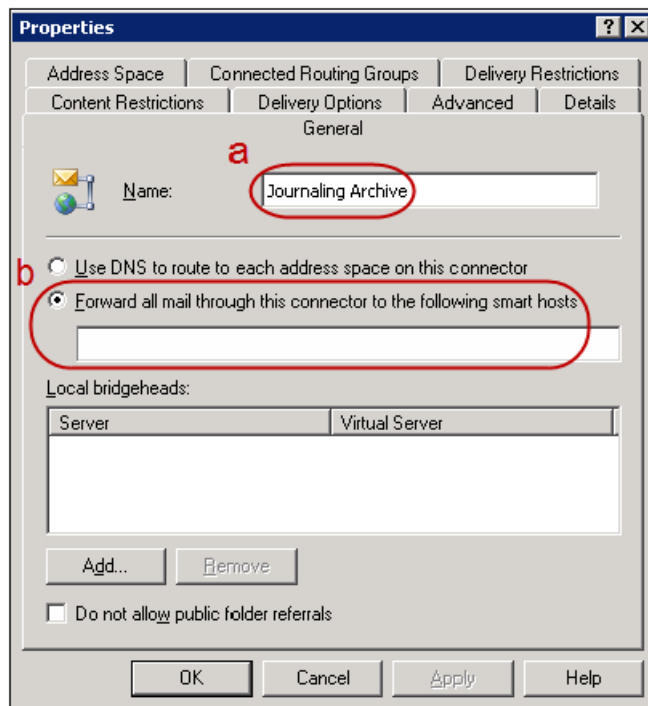
1. Open the **Exchange System Manager** window by selecting **Start -> Programs -> Microsoft Exchange -> System Manager**.
2. In the left-hand menu, right-click **Connectors**.



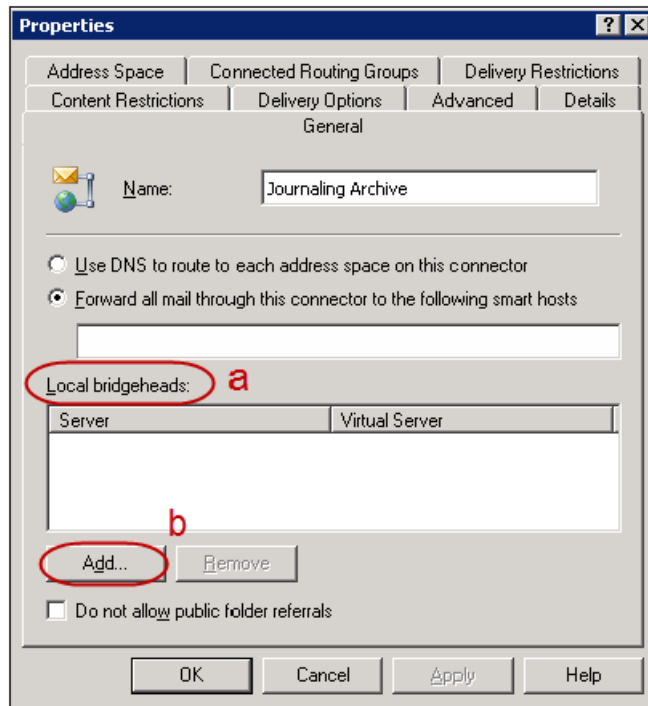
3. Select **New** and then select **SMTP Connector**.



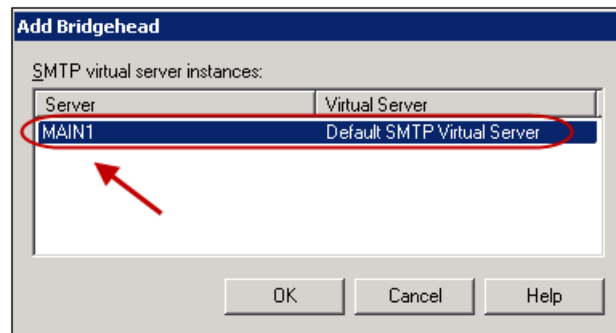
4. In the **Properties** window, type **Journaling Archive** in the Name field (a). Select **Forward all mail through this connector to the following smart hosts** and type the smart host your were provided into the resulting field (b).



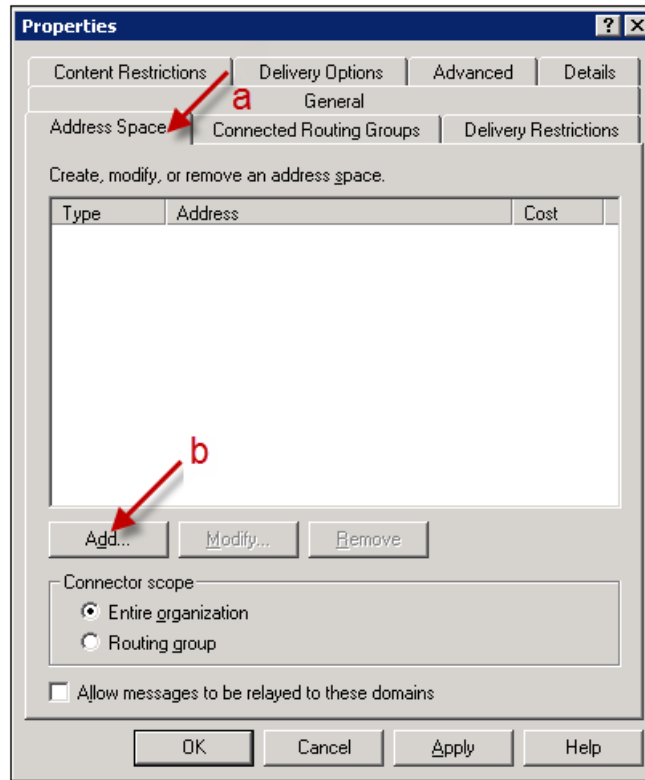
5. Within the Local Bridgeheads section (a), click **Add (b)**.



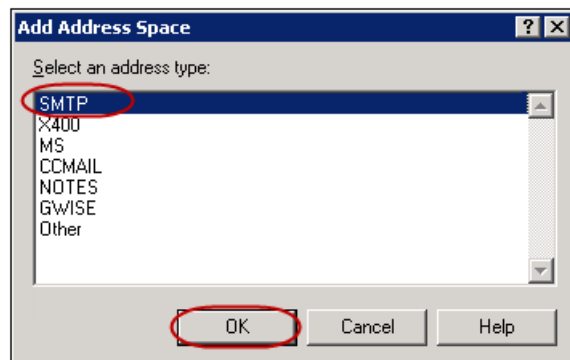
6. The **Add Bridgehead** dialog box displays. **Select the server** in which you would like to name the bridgehead, from within the list. Click **OK** to close the dialog box.



7. In the **Properties** window, click the **Address Space** tab (a). Click **Add** (b).



8. Select **SMTP** in the resulting **Add Address Space** dialog box. Click **OK**.

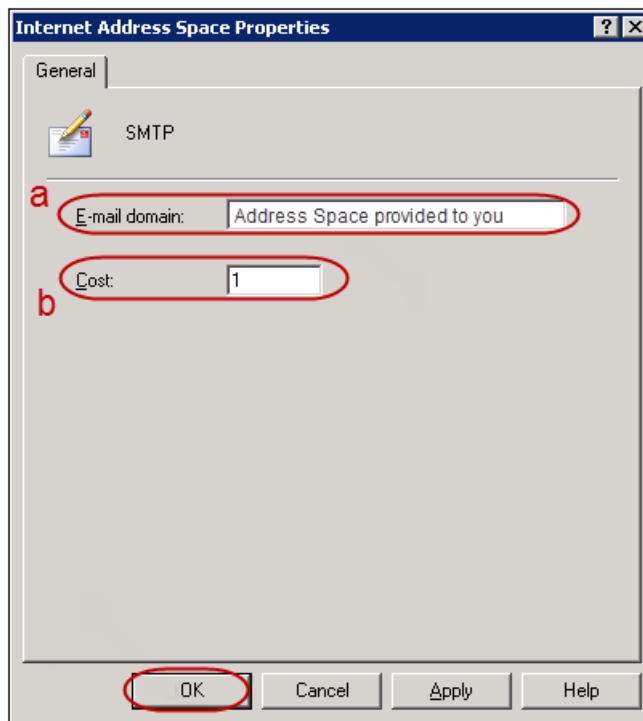


9. Type the **Address Space** provided to you in the Email Domain field **(a)**, in the **Internet Address Space Properties** dialog box. Type **1** in the Cost field **(b)**. Click **OK** to close the dialog box.

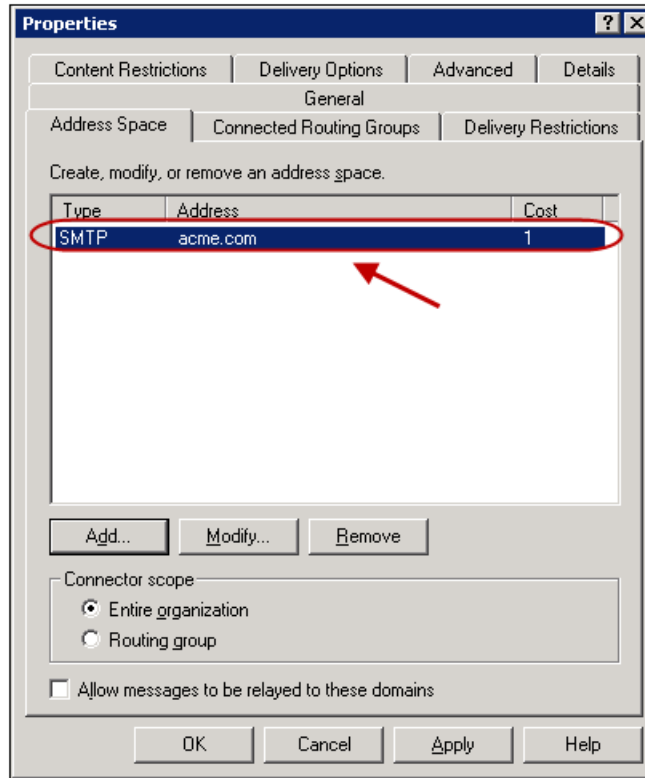


Note

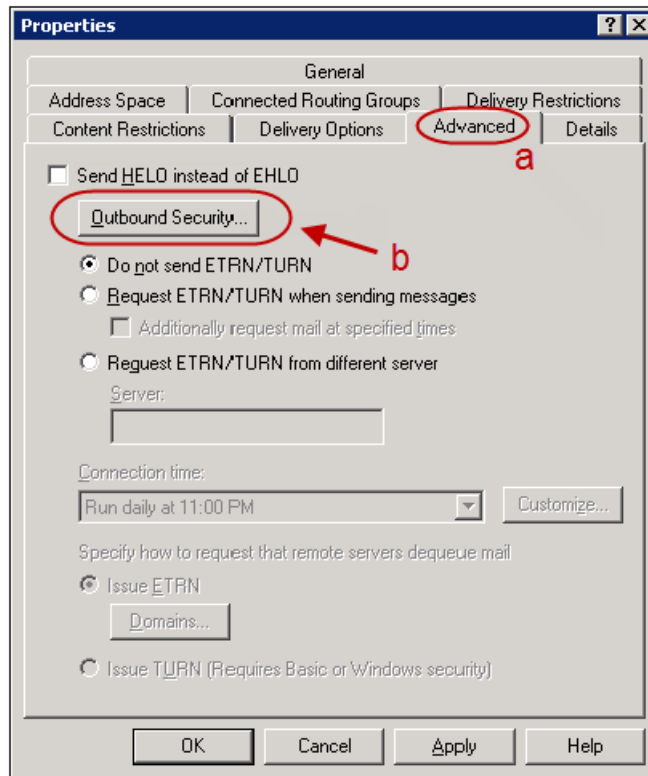
The address space is unique to your organization. If you have not been provided with this address, please contact support.



10. Your new **Address Space** displays in the **Properties** window. **Only this item should be selected** in the Address Space field.



11. In the **Properties** window, click the **Advanced** tab (a). Click **Outbound Security** (b).



12. Select the **TLS encryption** checkbox, in the resulting **Outbound Security** dialog box. Click **OK** to close the dialog box.



Note

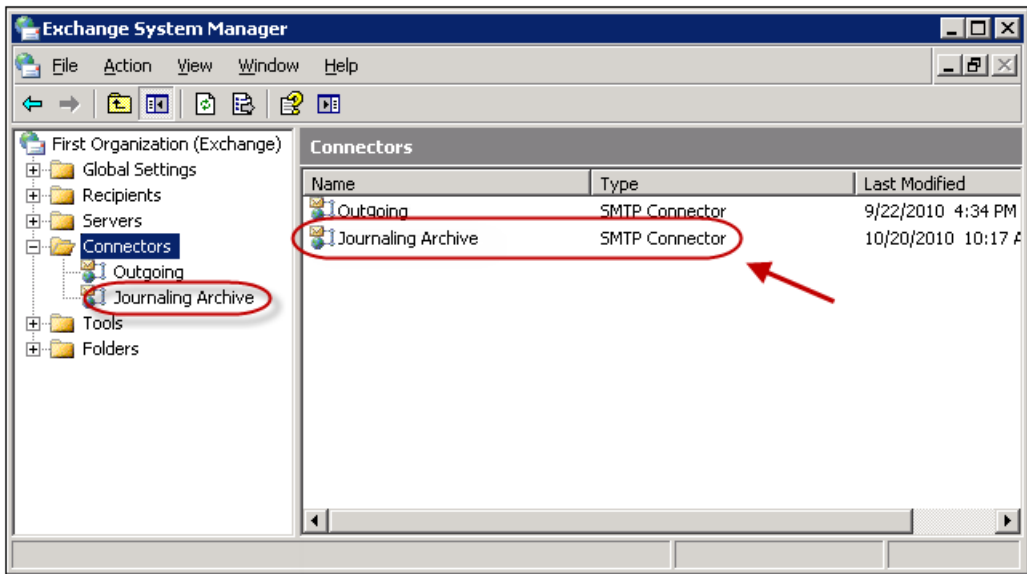
Confirm that your Network supports outbound TLS connections to SMTP services. If you have a CISCO firewall, you may need to change its ESMTP configuration to allow TLS encryption: refer to the Troubleshooting Tips below for details.

Any inbound email messages to your Exchange server **from** the Archive (for example, "Restoring" a message back to your active mailbox) is automatically sent via opportunistic TLS.



13. Click **OK** to close the **Properties** window.

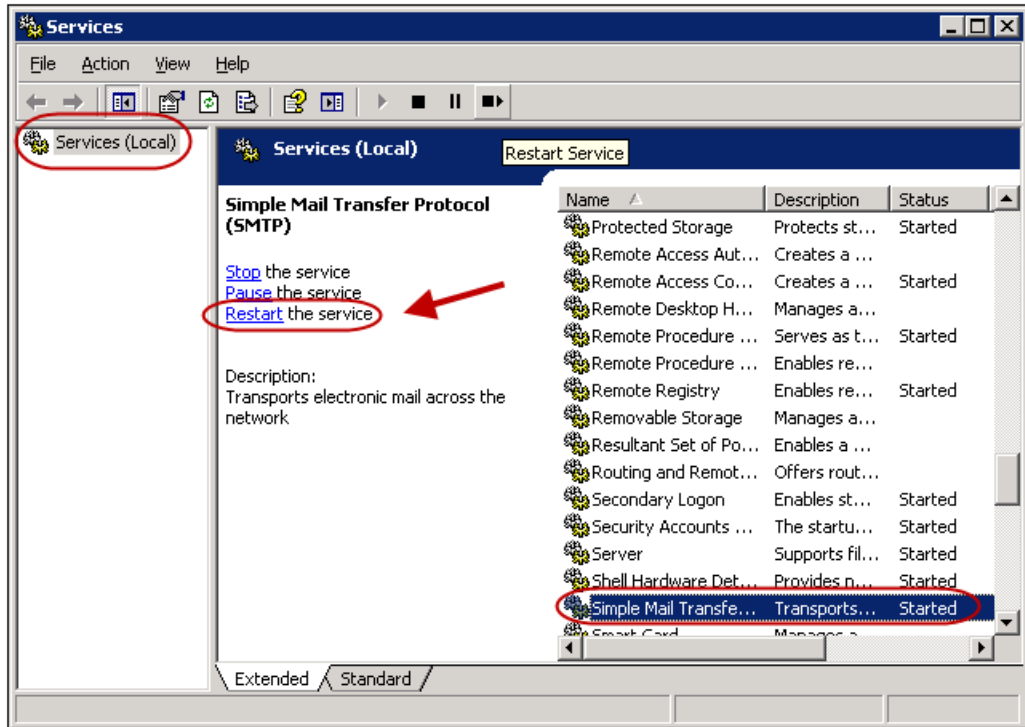
14. You have successfully created a new **Connector**: name **Journaling Archive** and type **SMTP Connector**.



Note

You must restart your SMTP Services to ensure your new Connector takes effect.

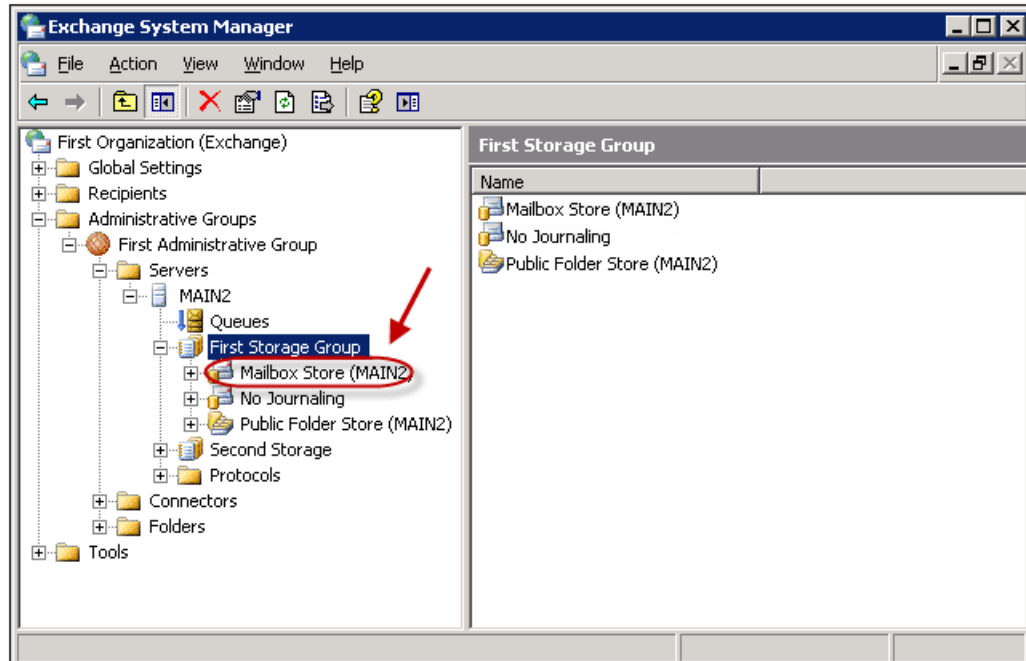
15. To restart the SMTP Service: go to **Start**, then **Run**, and type in **services.msc**. The **Services** dialog box displays, which lists all services running on your server. Select **Simple Mail Transfer Protocol (SMTP)** from within the list and click **Restart** in the left-hand navigation menu. Your new Connector setup is complete.



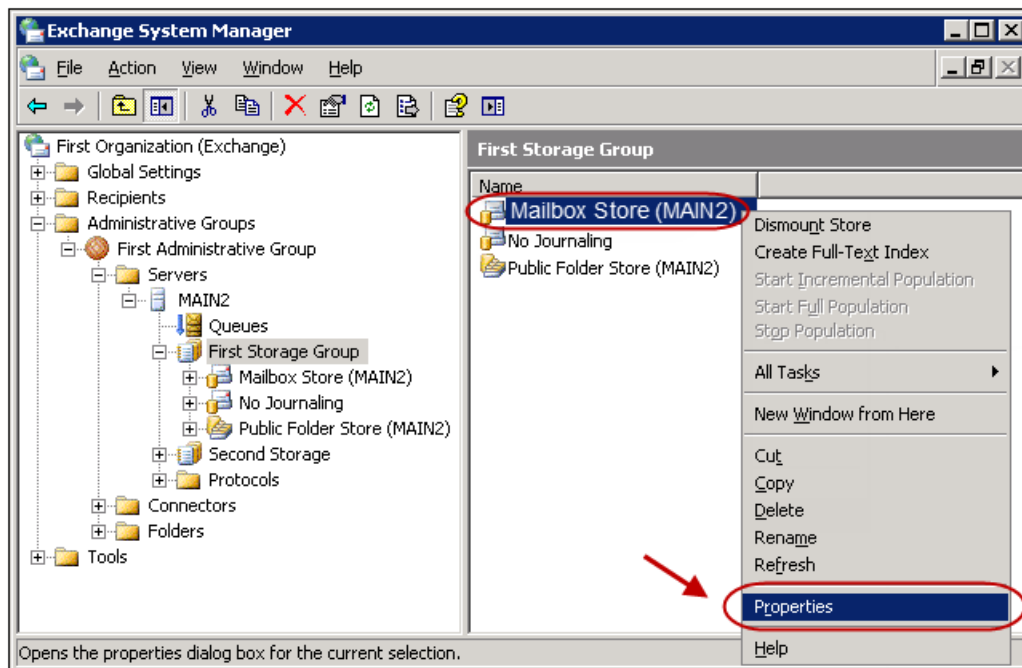
Activate journaling

1. Open the **Exchange System Manager** window by selecting **Start -> Programs -> Microsoft Exchange -> System Manager**.

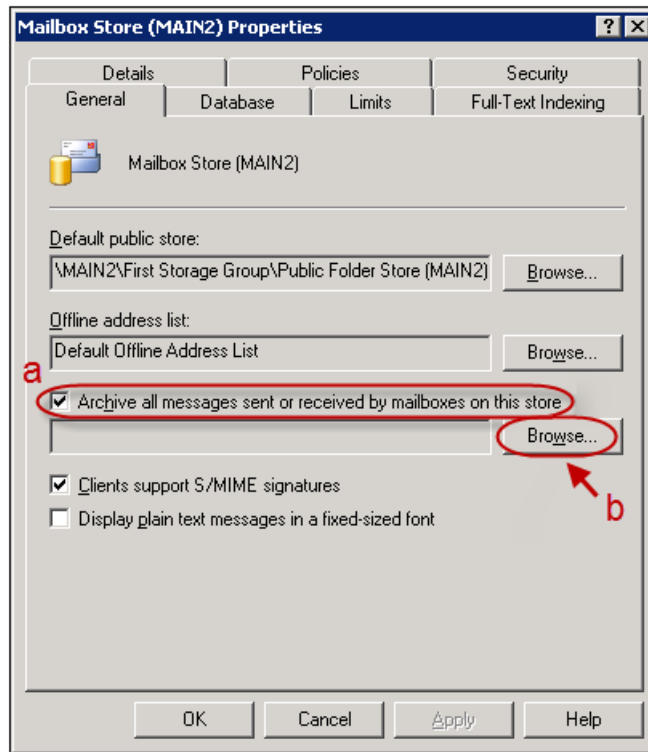
- In the left navigation menu, select **Servers**, select ***your server name** and then select the **Storage Group** that contains the mailboxes to which you wish to apply journaling. In this example, it is Mailbox Store (MAIN 2).



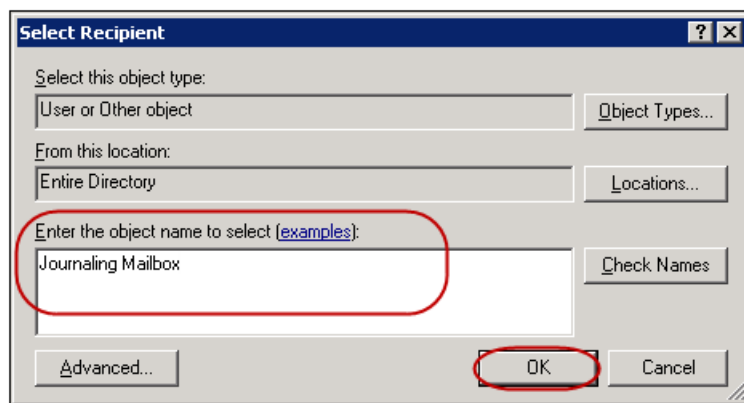
- In the right-hand content frame, **right-click the Mailbox Store** you wish to apply journaling, from within the list. Select **Properties** in the drop-down menu.



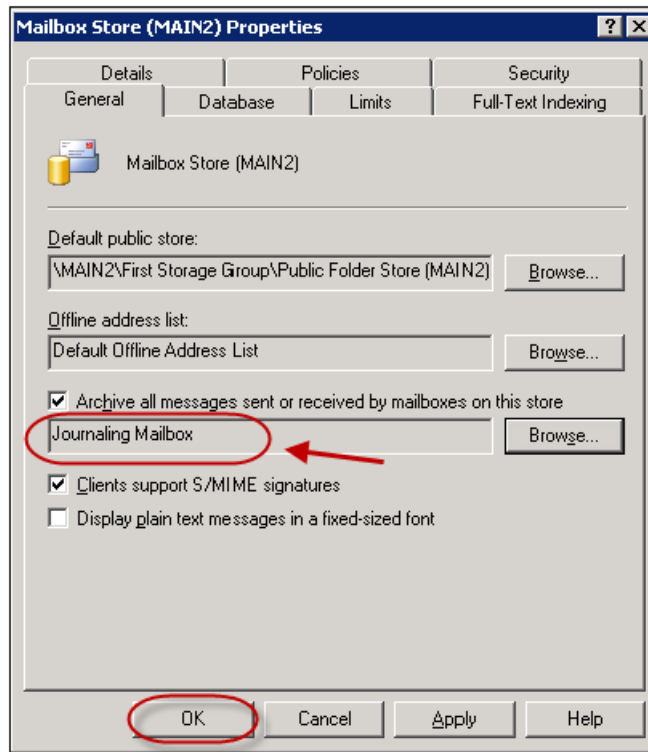
4. In the **Mailbox Store Properties** window, select the **Archive all messages sent or received by mailboxes on this store** checkbox (a). Click **Browse** (b)



5. Type the **Journaling Mailbox** you created in Step Four into the available field, in the resulting Select Recipient dialog box. Click **OK**.



- The **Journaling Mailbox** will appear within the **Mailbox Store Properties** window. Click **OK** to close the window.



Note

All messages passing through this Mailbox Store will now be copied into the Journaling Mailbox. To confirm this process, you can connect to the Journal Mailbox via Outlook or Outlook Web Access.

Disable NDRs (non-delivery reports)

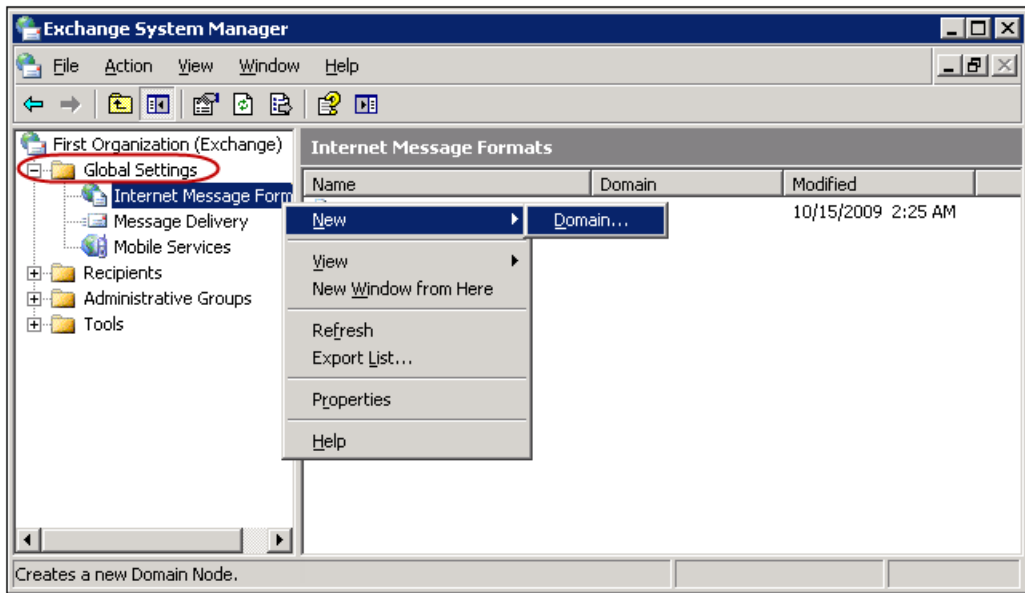
You must disable NDRs for the domain to which you are journaling; this is the same domain entered in the address space when creating the SMTP connector.

If there are any issues delivering your journaled email messages, this step prevents NDRs from being sent back to the original sender(s) (giving the false impression that their email was not delivered). This step is also necessary for email messages to journal with the message header information in plain text and to allow automatic forwarding of journaled email.

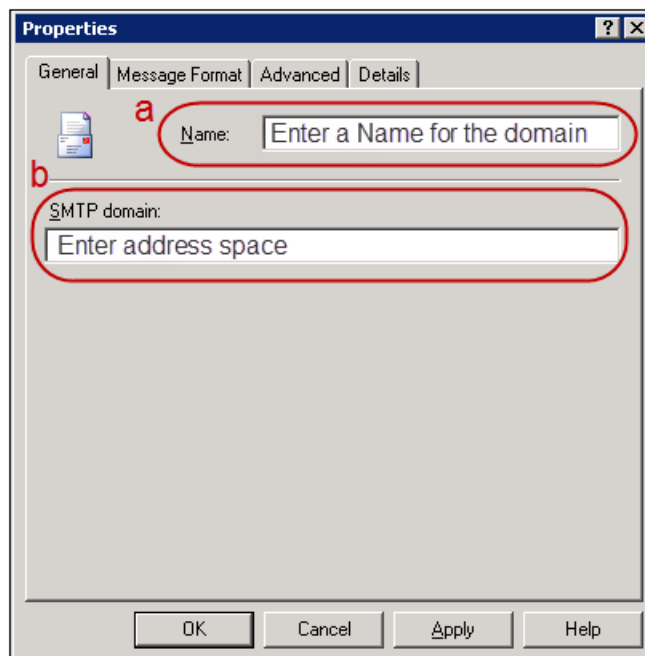
To create a custom rule to disable NDRs, follow these steps:

- Open the **Exchange System Manager** window by selecting **Start -> Programs -> Microsoft Exchange -> System Manager**.

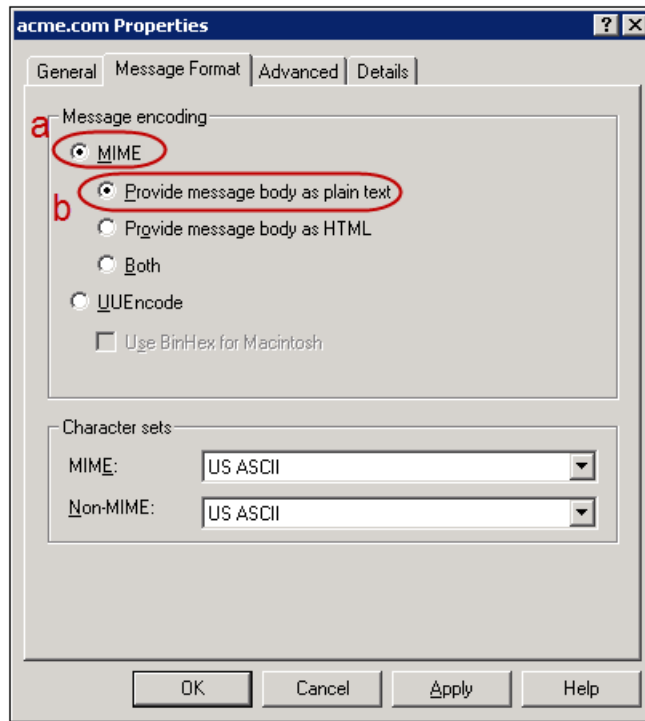
- Expand the **Global Settings** folder in the left navigation menu, right-click **Internet Message Formats**, then select **New** and then select **Domain**.



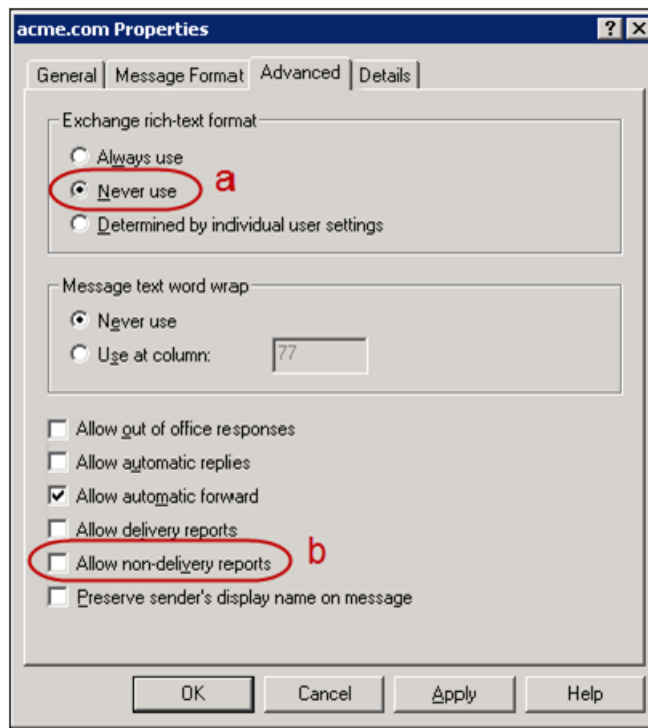
- In the **General tab** of the Properties window, enter a **Name** for your domain (**a**) and enter the **Domain (address space)** used to create the SMTP Connector in Step 6 (**b**).



4. In the **Message Format** tab of the Properties window, select the **MIME** radio button **(a)** and select **Provide message body as plain text** radio button **(b)**.



5. In the **Advanced tab** of the Properties window, select the **Never use** radio button within the Exchange rich-text format section **(a)**. Deselect the **Allow non-delivery reports** checkbox **(b)**.



6. Click **OK** to close the Properties window. You have successfully disabled non-delivery reports.

Add SMTP queue growth monitoring alert

This setting allows an Exchange Administrator to easily monitor their journaling queue. When the queue becomes too large or if the queue stops journaling email-- after a set time determined by each company-- the Administrator will be notified via email.

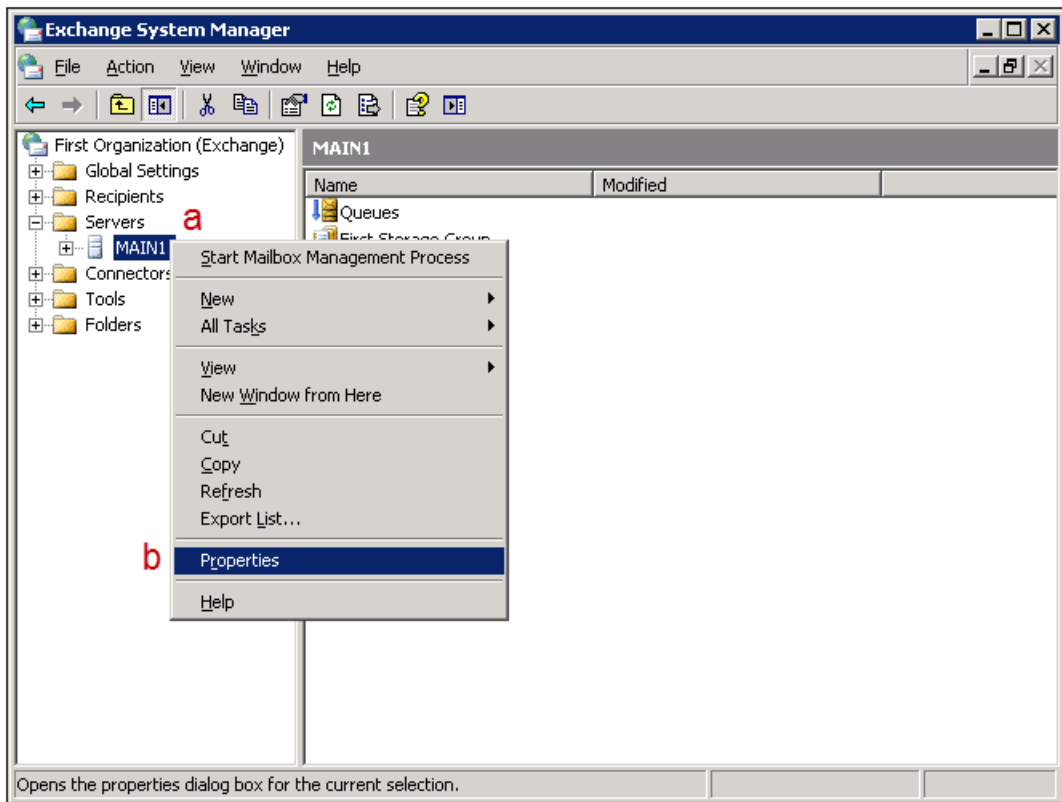


Note

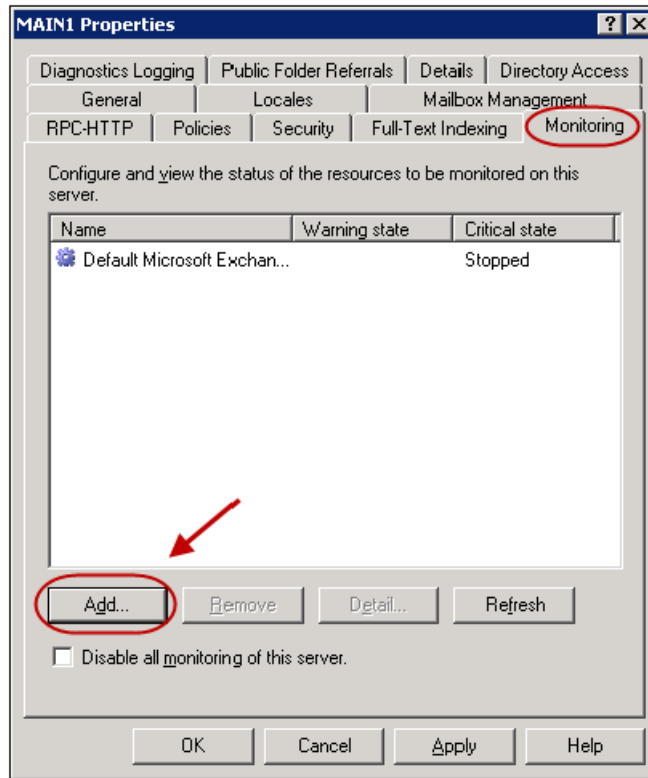
Some message queuing on the server is normal. If unusual queuing patterns occur or large amounts of email queue up, journaling may not be working.

1. Open the **Exchange System Manager** window by selecting **Start -> Programs -> Microsoft Exchange -> System Manager**.

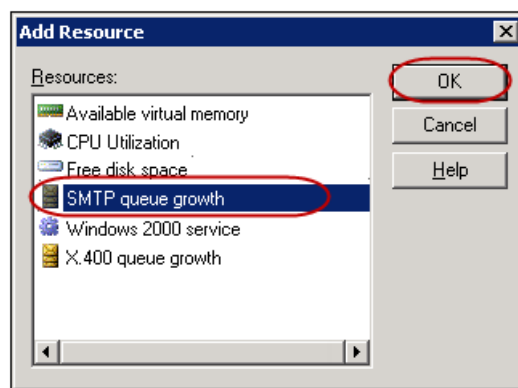
- Expand the **Servers** item in the left navigation pane. **Right-click the server** you wish to monitor **(a)** and select **Properties** from the drop-down menu **(b)**.



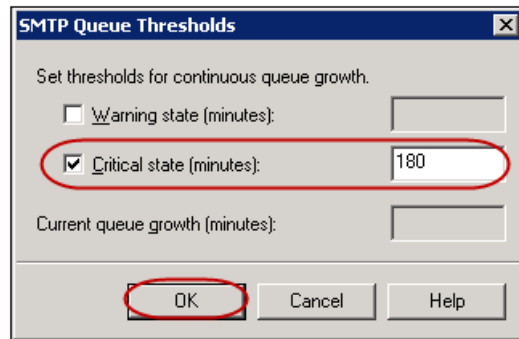
3. Within the **Monitoring** tab, click **Add**.



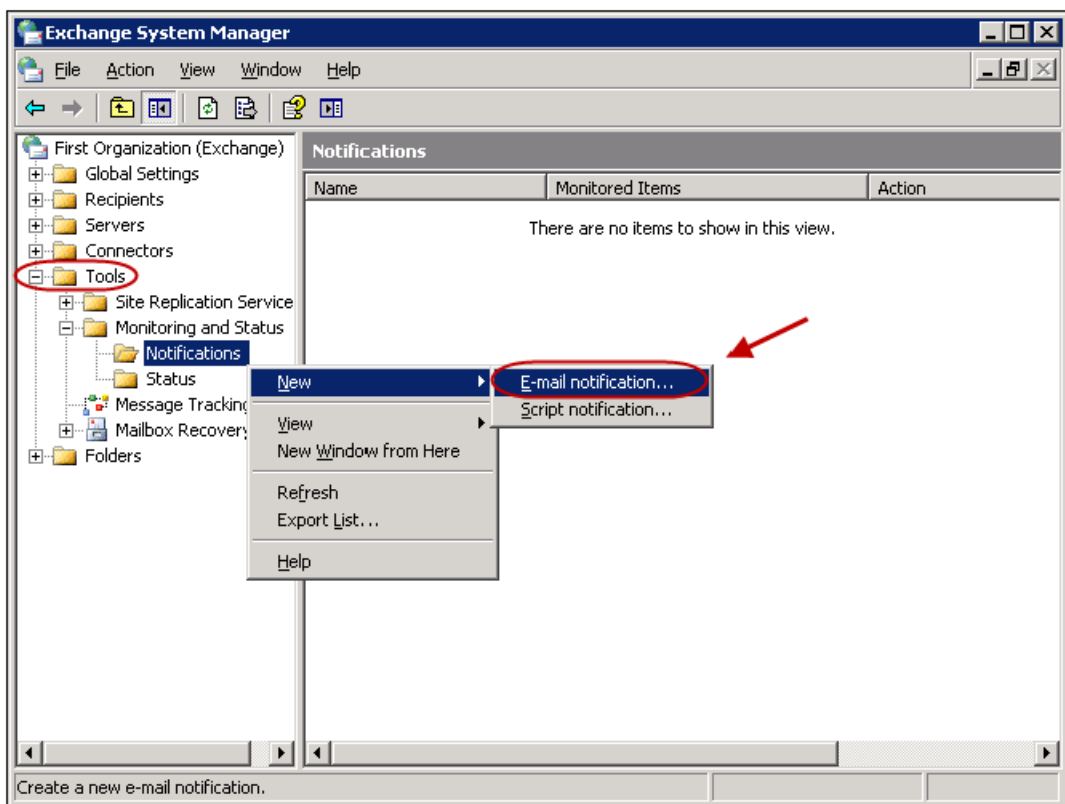
4. In the Add Resource dialog box, select **SMTP queue growth** from within the list and click **OK**.



5. In the SMTP Queue Thresholds dialog box, select the **Critical state (minutes)** checkbox and enter **the amount of time** you will allow the queue to build up before being alerted. We recommend **180 minutes**. Click **OK**.

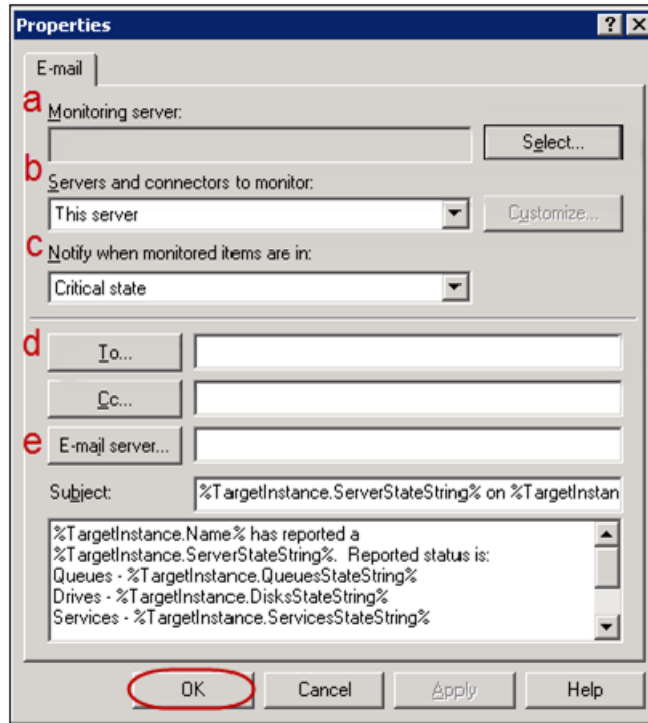


6. In the **Exchange System Manager**, go to **Tools -> Monitoring and Status -> Right-click Notifications -> New** and select **Email notification**.



7. Enter the following details into the **Properties** window:
 - a. Enter **Name of your Server** into the Monitoring server field **(a)**.
 - b. Select **This server** from the Server and Connectors to monitor drop-down menu **(b)**.

- c. Select **Critical state** from the "Notify when monitored items are in" drop-down menu **(c)**.
- d. In the **To field**, enter the email address(es) you want the notifications sent to **(d)**.
- e. In the **Email server field**, enter the name of your **sending server (e)**.
- f. Click **OK** to close the **Properties** window.



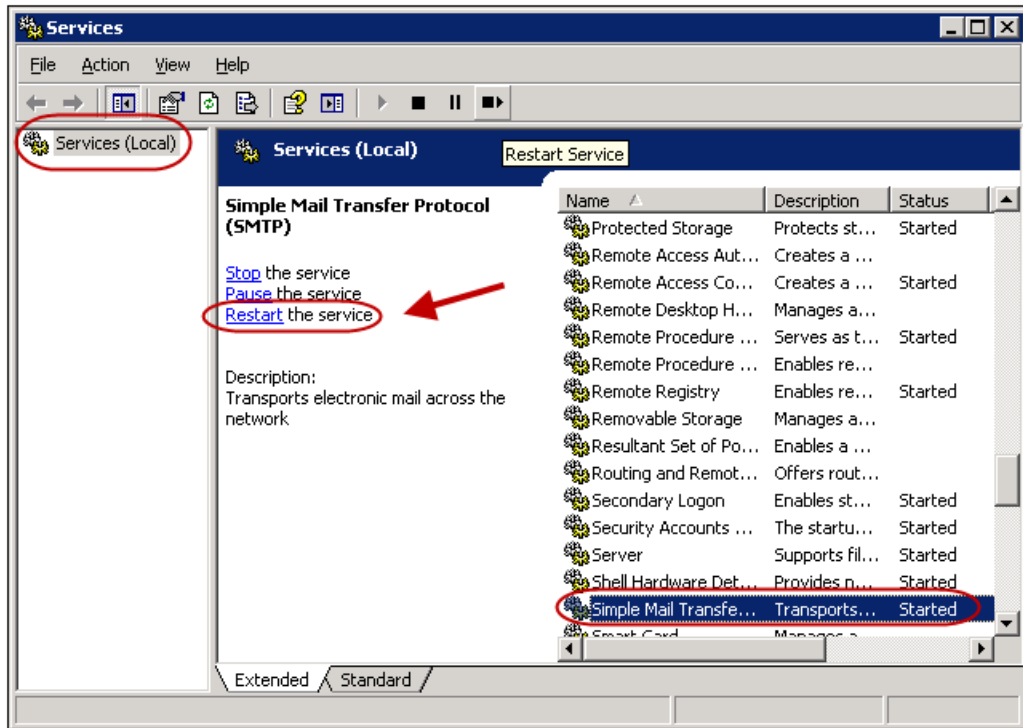
Note

Your Journaling setup 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

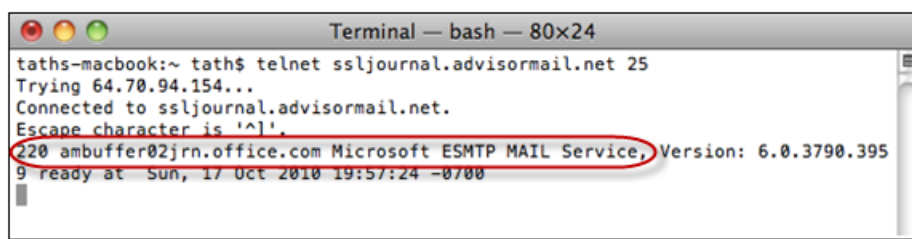
1. Make sure the **Journaling Contact SMTP Email Address** is spelled correctly.
2. Restart the SMTP Services

- a. To restart the SMTP Service: go to **Start**, then **Run**, and type in **services.msc**. The **Services** dialog box displays, which lists all services running on your server. Select **Simple Mail Transfer Protocol (SMTP)** from within the list and click **Restart** in the left-hand navigation menu.



3. 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>
4. Verify there are no enabled Send Connectors utilizing the domain name of the contact being journaled to.
5. 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 ESMTPL MAIL Service, Version: 6.0.3790.3959 ready at Sun, 17 Oct 2010 19:57:24 -0700
```

6. When adding/removing SMTP connector(s). Make sure to restart SMTP service, explained above and MS Exchange Routing Engine.

Journaling best practices

1. 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.
2. Setup SMTP Queue Growth Monitoring alerts, completed above, and monitor your Exchange Server for issues.
3. When adding or deleting a user mailbox on your Exchange Server, make sure you also update that user in the Archive Administration tab.

Remove Exchange 2003 journaling setup

To remove the journaling setup from your Exchange 2003 Standard server, follow these steps:

1. [Removing SMTP growth alert](#)
2. [Deactivate journaling](#)
3. [Remove the journaling SMTP connector](#)
4. [Remove the journaling contact from active directory](#)

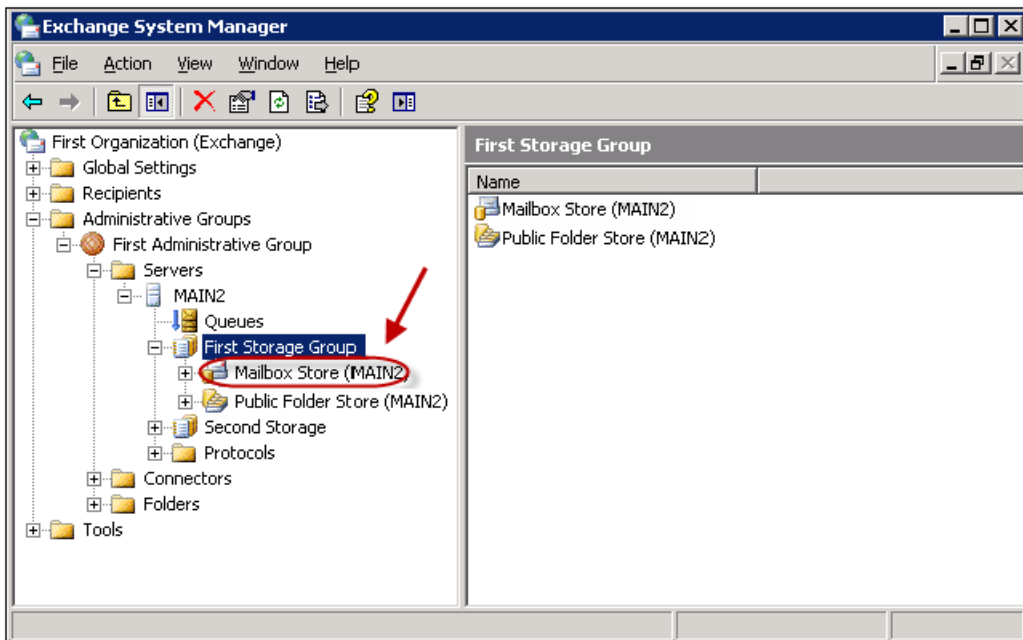


Note

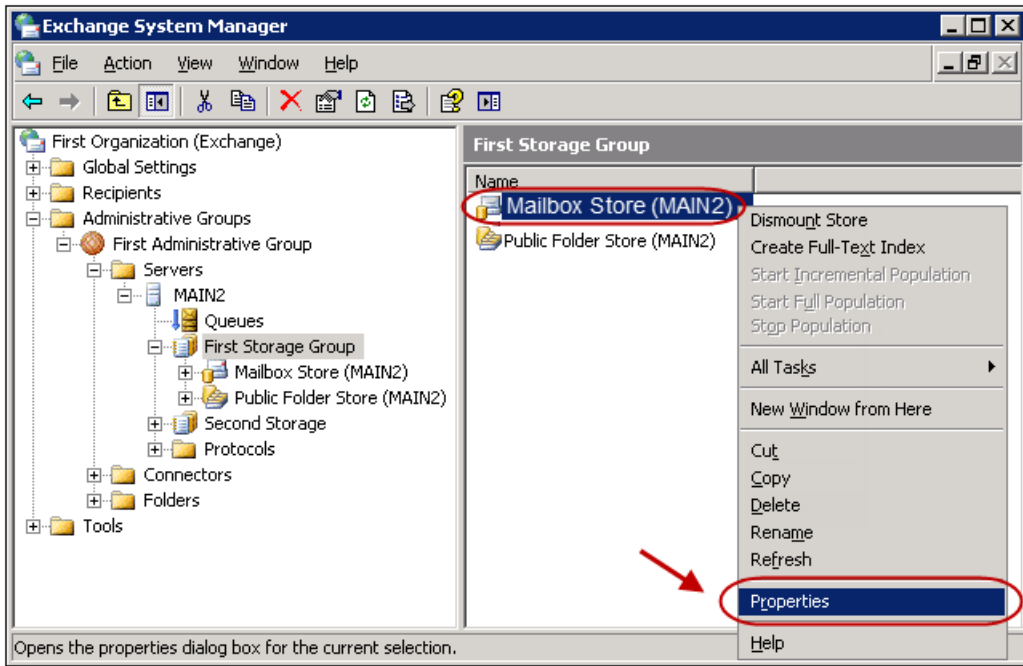
Only complete the following steps if you wish to stop sending email to the Archive. Once you remove the journaling setup, email cannot be saved in the archive.

Removing SMTP growth alert

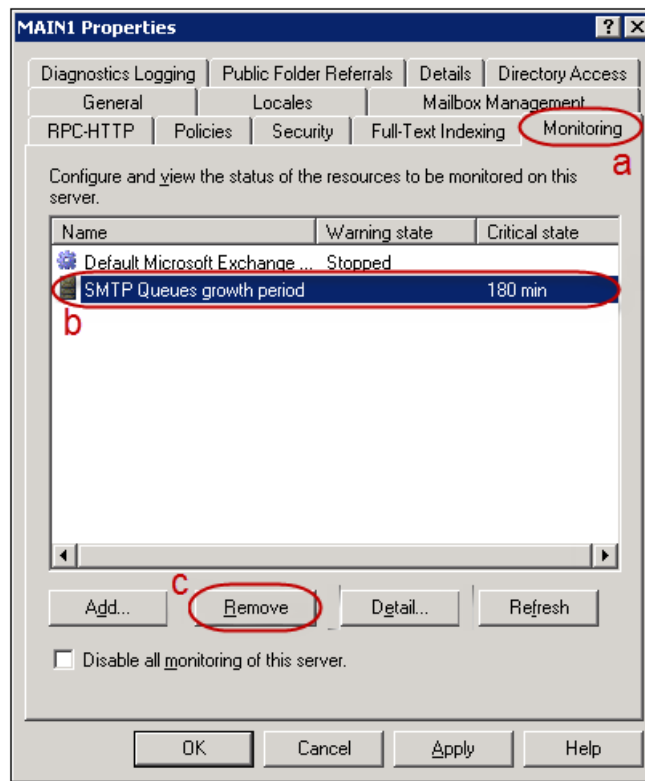
1. Open the **Exchange System Manager** window by selecting **Start -> All Programs -> Microsoft Exchange -> System Manager**.
2. In the left-hand navigation menu, select **Servers**, select your **server name** and then select the **Storage Group** that contains the mailboxes to which you applied journaling. In this example, it is Mailbox Store (MAIN2).



3. In the right-hand content frame, **right-click the Mailbox Store** to which you applied journaling, from within the list. Select **Properties** in the drop-down menu.



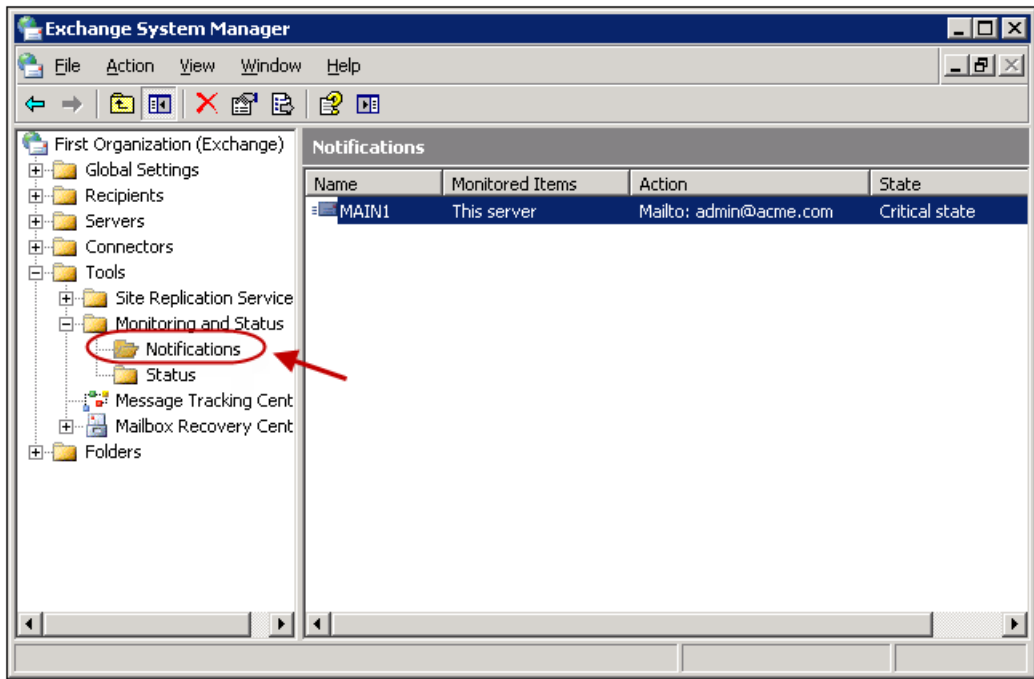
4. Within the **Properties** window, select the **Monitoring tab (a)**. Select the **SMTP Queues growth period** item, with a critical state of 180 minutes, from within the list **(b)**. Click **Remove (c)**.



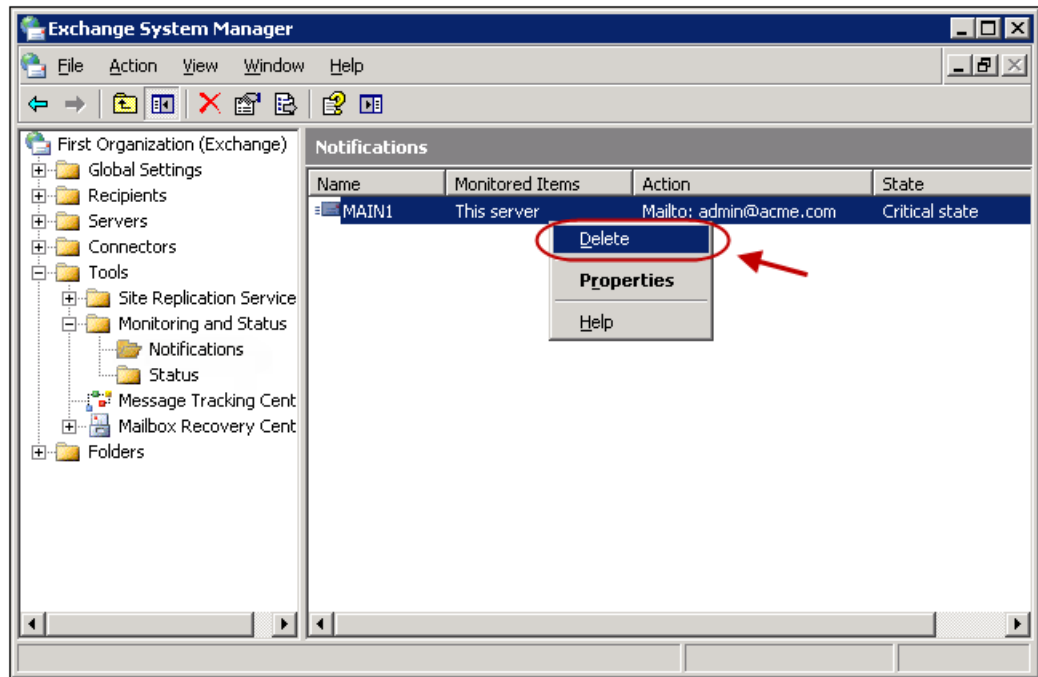
Note

If this queue monitoring item is being used for multiple queue alerts, those other alerts will also stop working after this item is deleted.

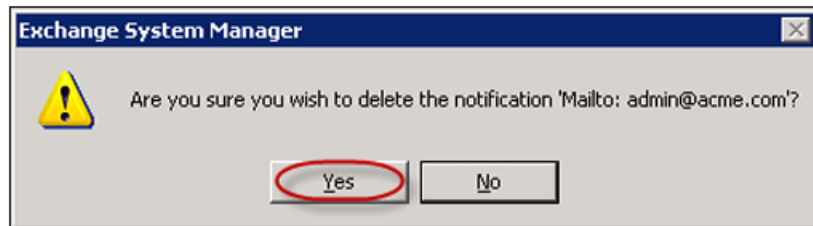
5. In the **Exchange System Manager**, go to **Tools -> Monitoring and Status -> Notifications**.



6. **Right-click any notification items** used for journaling monitoring from within the list. Select **Delete** from the drop-down menu. In this example, the Main 1 server item.



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

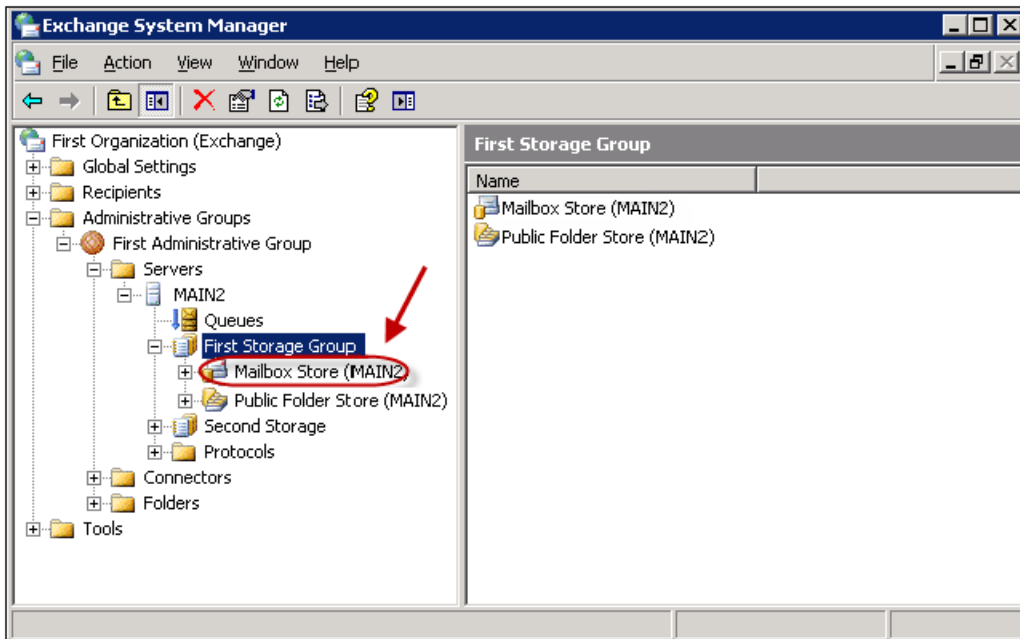


8. **You have successfully deleted the SMTP Growth Alert.** All email notifications retaining to it will stop and the item's configured settings are permanently deleted.

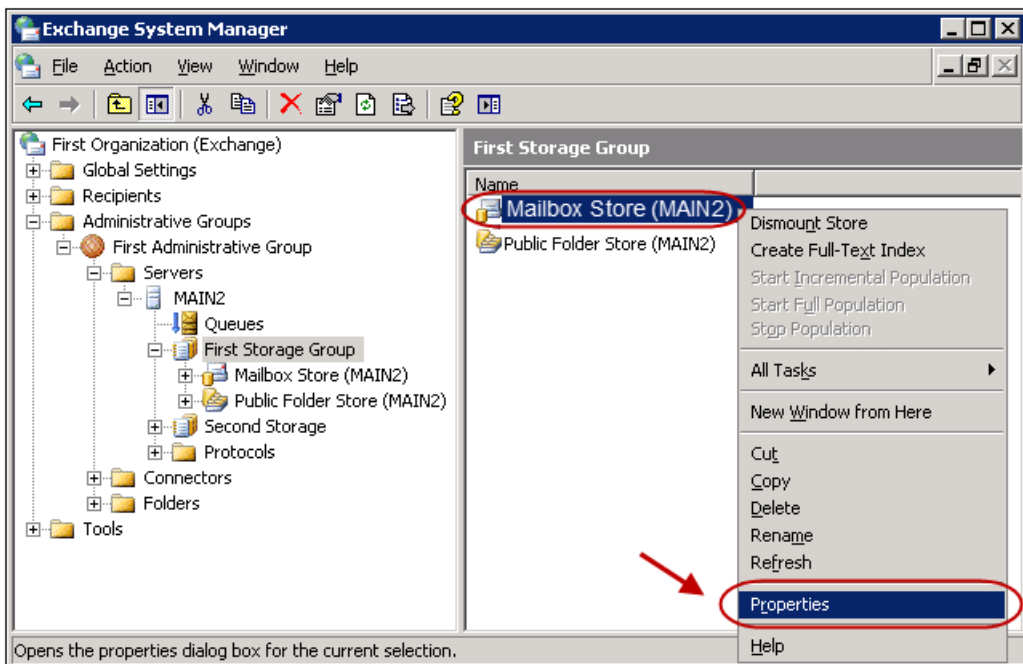
Deactivate journaling

1. Open the **Exchange System Manager** window by selecting **Start -> All Programs -> Microsoft Exchange -> System Manager**.

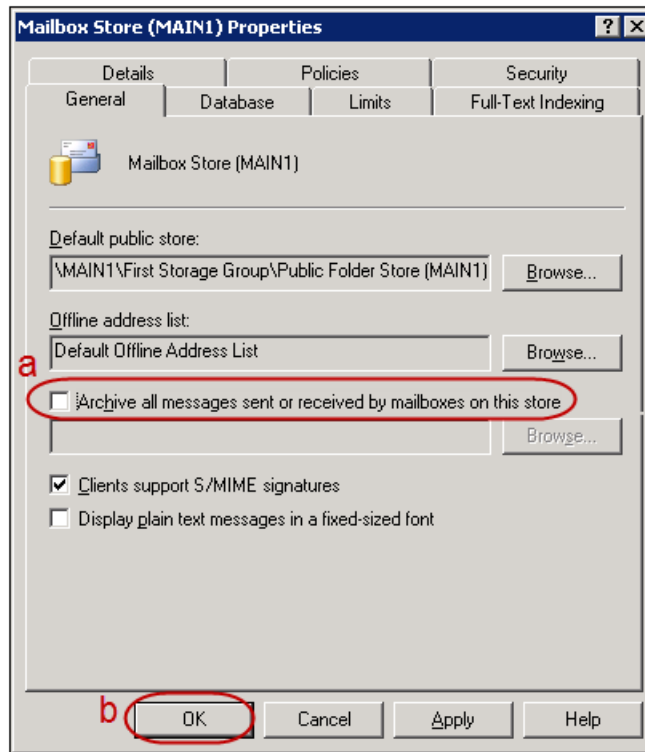
- In the left-hand navigation menu, select **Servers**, select your **server name** and then select the **Storage Group** to which you applied journaling. In this example, it is Mailbox Store (MAIN 2).



- In the right-hand content frame, **right-click the Mailbox Store** to which you applied journaling, from within the list. Select **Properties** in the drop-down menu.



4. Within the **General** tab, deselect the **Archive all messages sent or received by mailboxes on this store** checkbox (a). Click **OK** to close the window (b).

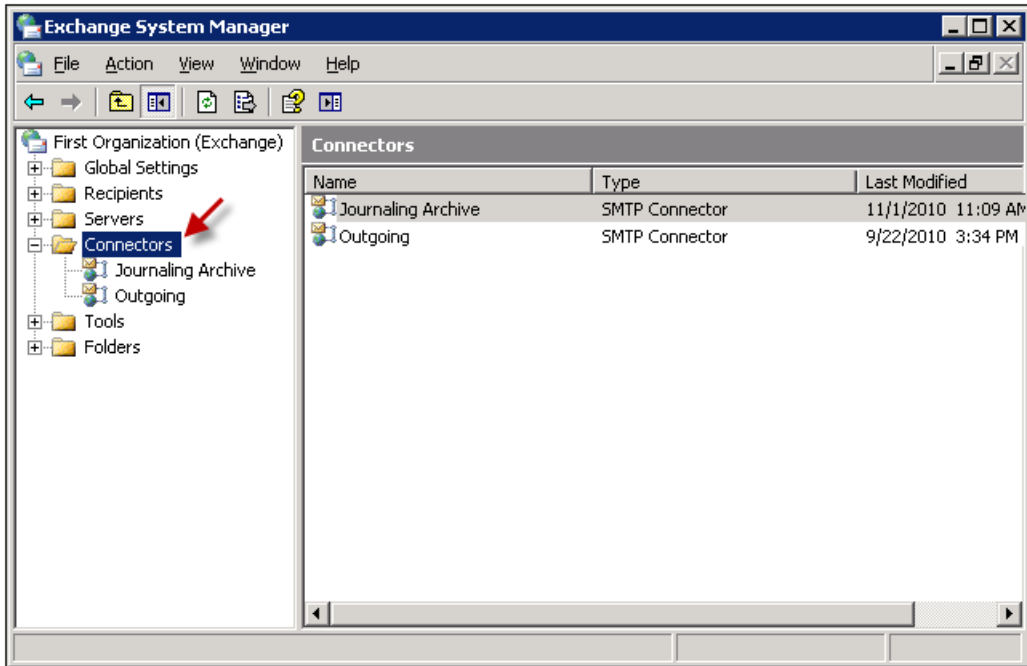


5. You have successfully deactivated journaling.

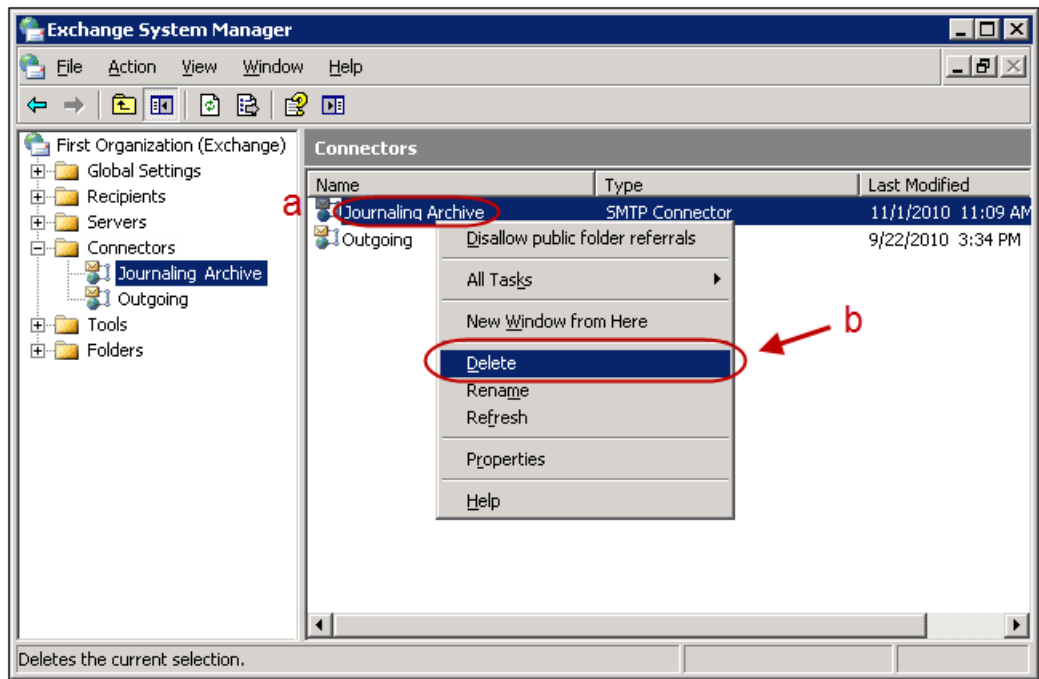
Remove the journaling SMTP connector

1. Open the **Exchange System Manager** window by selecting **Start -> All Programs -> Microsoft Exchange -> System Manager**.

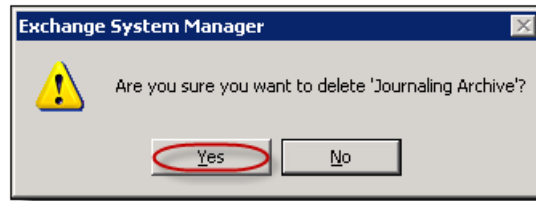
2. In the left-hand menu, right-click **Connectors**.



3. **Right-click** the connector called **Journaling Archive** (a) and select **Delete** from the drop-down menu (b).



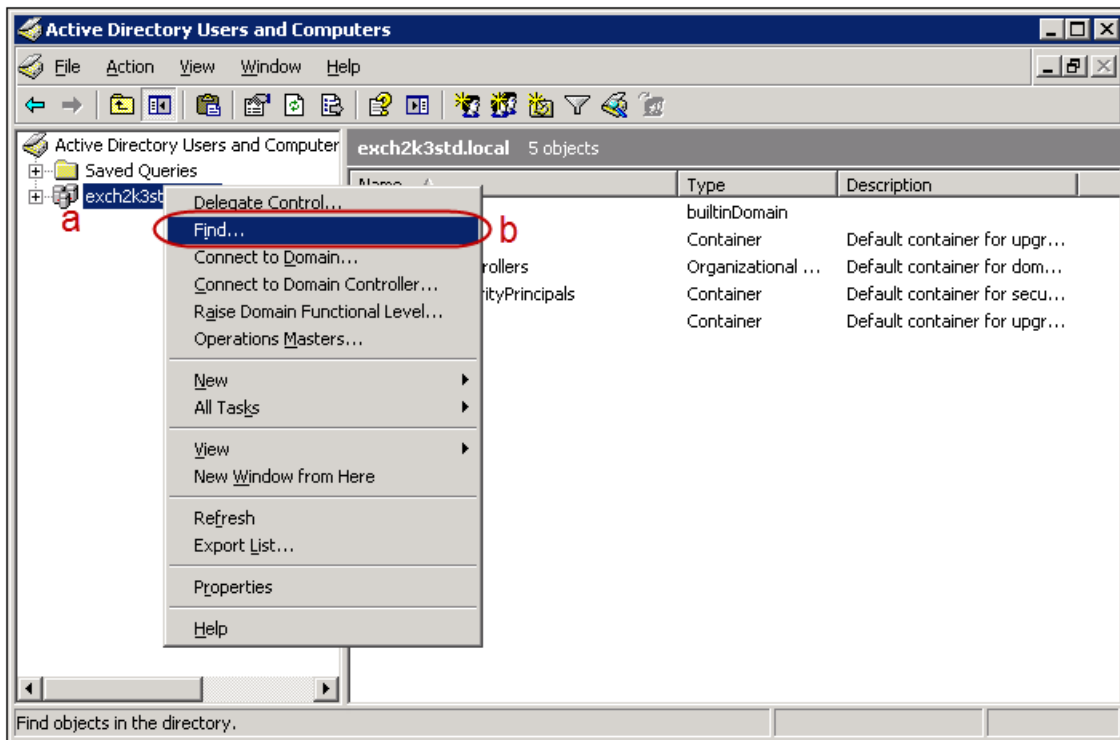
- Click **Yes** on the resulting warning dialog box.



- You have successfully removed the Journaling SMTP Connector.

Remove the journaling contact from active directory

- Open the **Active Directory Users and Computers** application by selecting **Start -> All Programs -> Microsoft Exchange -> Active Directory Computers and Users**.
- Right-click** the domain where the journaling contact is located, within the left navigation pane (a). Select **Find** from the drop-down menu (b).



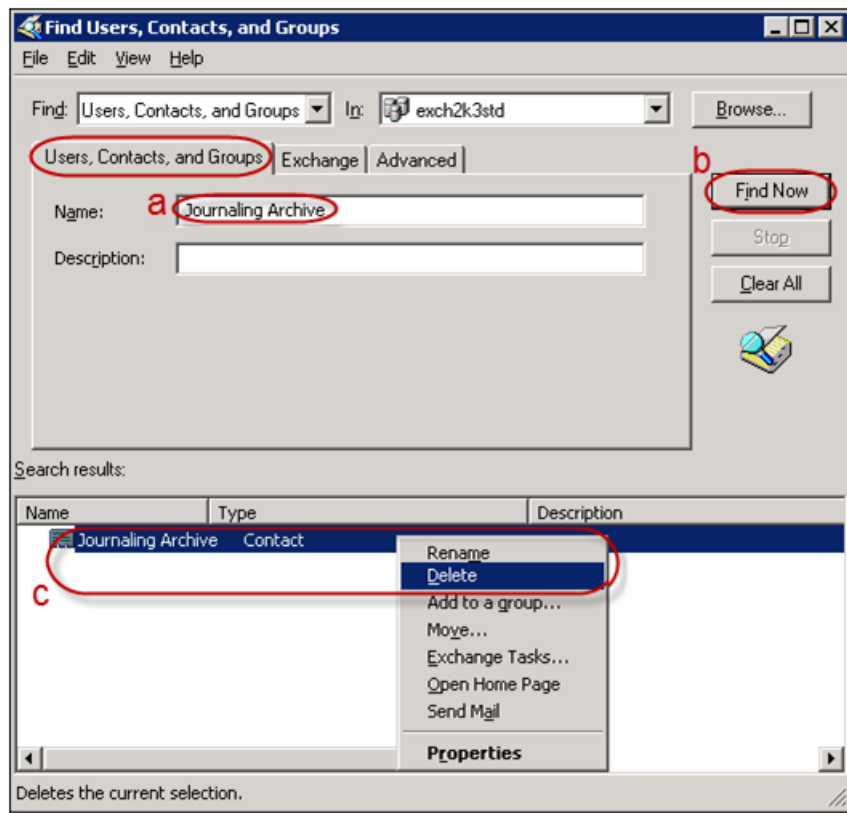
- The **Find Users, Contacts and Groups** window displays.
- Within the **Users, Contacts and Groups** tab, enter the following information:
 - Enter **Journaling Archive** into the Name field (a): this is the name assigned to the Journaling Contact in Step One of the Journaling setup above.

- b. Click **Find Now (b)**.
- c. The contact **Journaling Archive** displays in the **Search Results** area. Right-click the contact and select **Delete** from the drop-down menu.



Note

If you cannot find the contact **Journaling Archive**, try searching under another name or browsing the default OU's it may have been created in.



5. **You have successfully removed the Journaling Contact.**



Note

The removal of your Journaling Setup is now complete.

