How to Configure Microsoft Exchange Server 5.5 Service Pack 1 for Message Journaling

Table of Contents

Purpose of this Document

The goal of this document is to increase your understanding and proficiency in configuring Message Journaling for your Microsoft® Exchange Server 5.5 Service Pack 1 (SP1) computer.

The target audience for this document has a working knowledge of Exchange Server 5.5.

Table Of Contents

Overview

Message Journaling enables you to save copies of all messages sent or received by users of your Exchange Server computer, site, or organization. You may need to save copies of all messages to comply with laws or regulations that apply to your business. You can choose to send the collected messages to a mailbox, a public folder, or a custom recipient. You then need to permanently store or otherwise process the message copies.

When the Exchange Server computer is correctly configured, Message Journaling saves copies of the following types of messages:

- Messages sent or received by an Exchange Server user.
- Messages relayed through Microsoft Internet Mail Service.
- Read receipts for messages.

- Messages sent to public folders.
- Delivery reports for messages sent using Internet Mail Service.

Message Journaling does *not* save copies of the following types of messages:

- Messages posted to public folders.
- Delivery reports and nondelivery reports (NDRs). Exceptions are delivery reports for messages sent through the Internet Mail Service, which are saved.
- Directory replication messages.
- Public folder replication messages.
- Link monitor messages.
- X.400 probe messages.
- Message copies sent to the Message Journal.

If Message Journaling is configured at the server level, a message is copied when it is first sent from or received by the server. If Message Journaling is configured at the site level, a message is copied when it is first sent or received within the site. If Message Journaling is configured at the organization level, the message is copied when it is first sent or received within the organization.

Enabling Message Journaling

To enable Message Journaling throughout an Exchange Server site or organization, each server must be running Exchange Server 5.5 Service Pack 1 or later, and each server must be configured for Message Journaling.

You can configure Message Journaling at the server level, site level, or organization level. If you configure Message Journaling at the site level, a message that is sent between two sites in the organization is saved twice — once at the sending site and once at the receiving site.

To enable and configure Message Journaling using Microsoft Windows NT Server registry settings, complete the following steps on each server.

Step One: Specify Where Messages Are Saved

To specify where messages are saved, a registry key needs to be added with the distinguished name of the mailbox, public folder, or custom recipient.

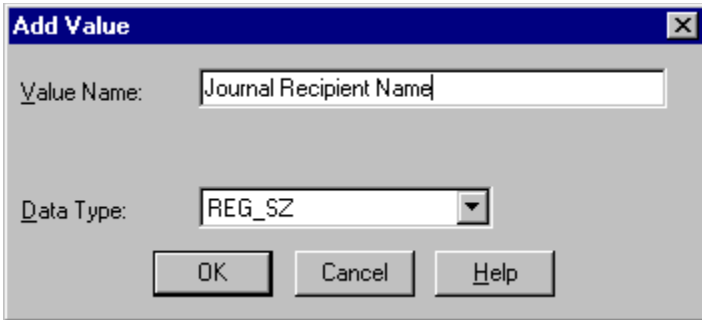To view the distinguished name of a Message Journal recipient or public folder:

1. Run the Exchange Server Administrator program in raw mode by typing **c:\ exchsrvr\bin\admin /r** at a command prompt.
2. Click the recipient mailbox, public folder, or custom recipient object in its respective container.

3. On the **File** menu, click **Raw Properties**.

4. In the **Objects attributes** box, click **Obj-Dist-Name**. The distinguished name of the object is displayed in the **Edit value** box. It is recommended that you copy this value to ensure there are no typographical errors when you create the registry key. To copy this value, select the value, and then press CTRL+C.
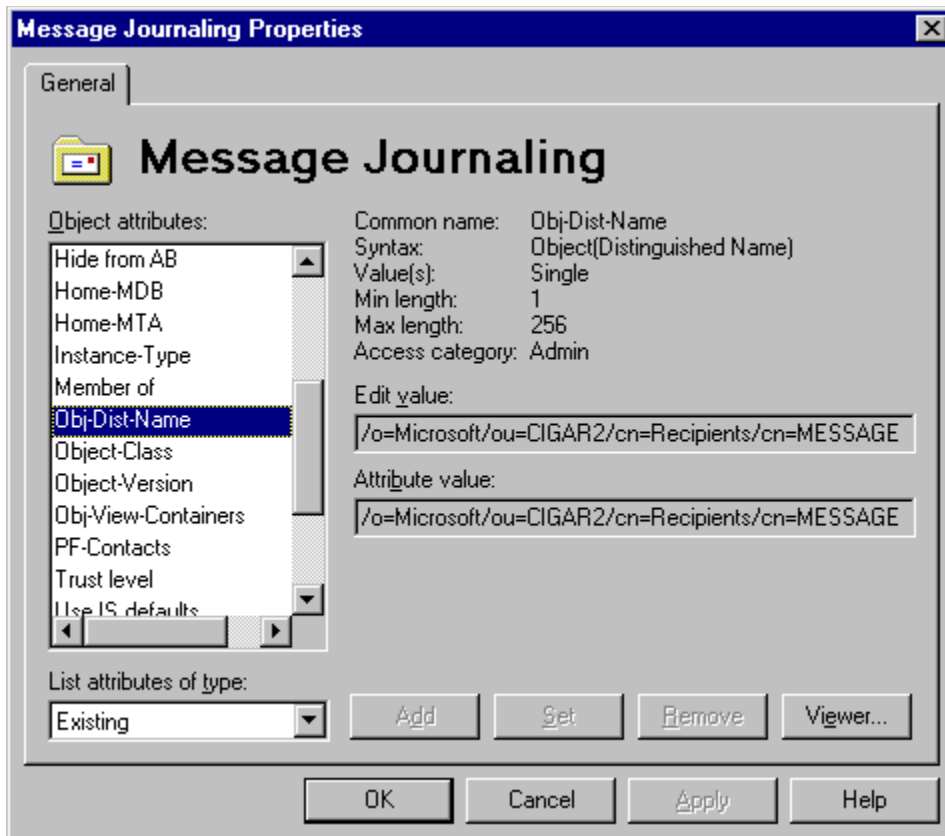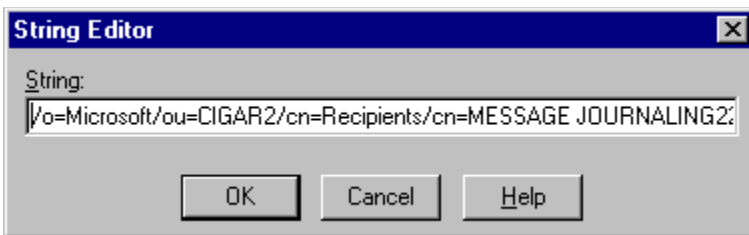
After the distinguished name information is copied, the appropriate registry key must be created:

1. Open the following registry key:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ MSExchangeMTA\Parameters

2. Add a new string value named **Journal Recipient Name**.

3. Set the string value of **Journal Recipient Name** to the distinguished name of the mailbox, public folder, or custom recipient.

Step Two: Specifying Message Journaling at the Server, Site, or Organization Level

You can specify whether Message Journaling is to be performed at the server, site, or organization level. By default, Message Journaling is performed at the organization level.

1. Open the following registry key:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ MSExchangeMTA\Parameters

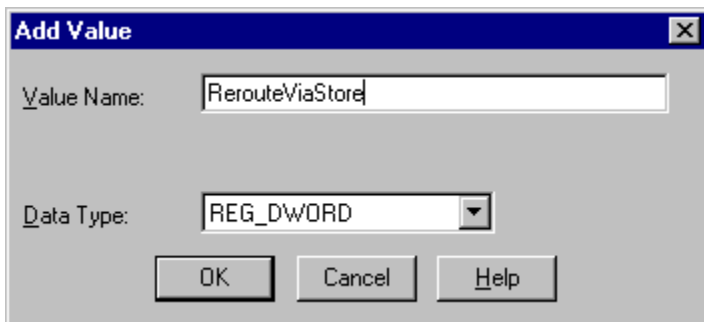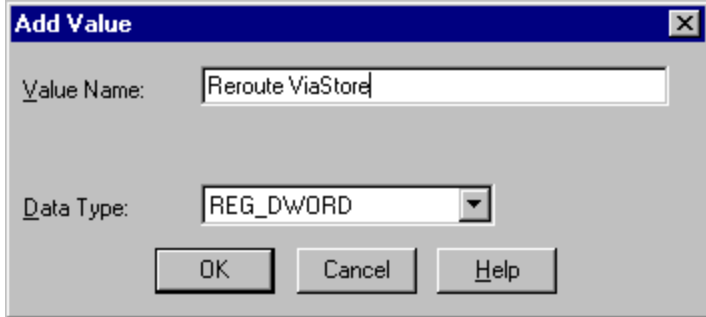2. Add a new DWORD value named **Per-Site Journal Required**.
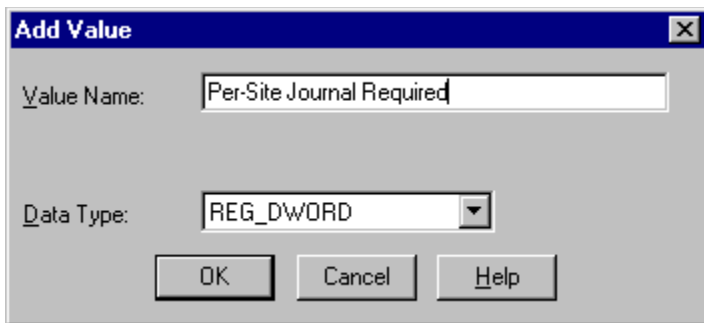
3. For Message Journaling at the server level, set the value of **Per-Site Journal Required** to 2. For Message Journaling at the site level, set the value of **Per-Site Journal Required** to 1. For Message Journaling at the organization level, set the value of **Per-Site Journal Required** to 0.

Step Three: Routing Internet Mail Service Messages Through the Private Information Store

To be copied correctly, all Internet Mail Service messages must be routed through the private information store.

1. Open the following registry key:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ MSExchangeIMC\Parameters

2. Add a new DWORD value named **RerouteViaStore**.

Add Value ☒

Value Name: | Reroute ViaStore

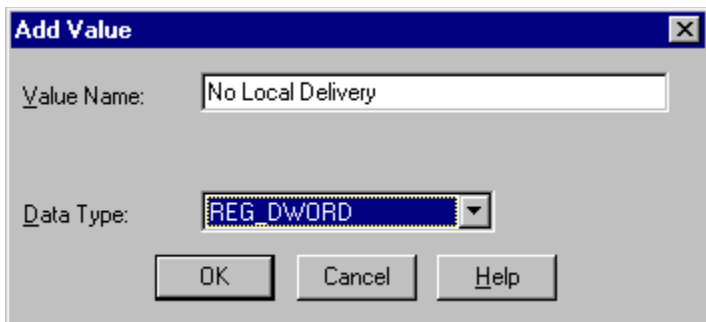Data Type: | REG_DWORD ▼

[OK] [Cancel] [Help]

3. Set the value of **RerouteViaStore** to 1.

Step Four: Routing Local Messages Through the MTA

To be copied correctly, local messages must be routed through the message transfer agent (MTA) instead of being delivered directly by the private information store.

1. Open the following registry key:
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \MSExchangeIS\ParametersSystem

2. Add a new DWORD value named **No Local Delivery**.

Add Value ☒

Value Name: | No Local Delivery

Data Type: | REG_DWORD ▼

[OK] [Cancel] [Help]

3. Set the value of **No Local Delivery** to 1.

Security

It is important to limit who can change the registry entries that control Message Journaling. By default, all users with Windows NT Server Administrator permissions can change these registry entries.

There are two primary security issues in Message Journaling:

- Unauthorized disabling of Message Journaling when it should be used.
- Unauthorized use of Message Journaling to intercept messages.

The mailbox, public folder, or custom recipient that receives the message copies must be secure. This recipient should be hidden from the directory. If the recipient is a public folder, on the **Permissions** tab for the public folder, set the Roles for the default user to Contributor, and then clear all permissions except Create Items.

Copies of encrypted messages are saved in a manner similar to that of other messages, but they are not decrypted.

Table Of Contents

Performance

Message Journaling adds processing overhead to the Exchange Server computer and increases network traffic. Use Windows NT Performance Monitor after you enable Message Journaling to ensure that your system can handle the additional load. If the system cannot handle the load, you may need to upgrade your hardware or balance system resources.

Note: The performance enhancements in the MTA in Service Pack 1 should help balance the processing overhead of Message Journaling. The mailbox, public folder, or custom recipient that receives the message copies must always be available, or Message Journaling does not work. Depending on the message volume, you might need to set up the mailbox or public folder on a dedicated Exchange Server computer within the site.

Table Of Contents

Additional Considerations

- If you need to archive message-tracking data with the message copies, click **Enable message tracking** on the **General** property page of the **MTA Site Configuration** object. Then copy the daily log files from the Exchsrvr\ Tracking.log folder to your archive location.

- Do not disable the Per-Domain-Bilateral-Info field if you are using Message Journaling. The Per-Domain-Bilateral-Info field is disabled when the following registry key is set to 1:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
  \MSExchangeMTA\Parameters\Do not generate Bilateral Info
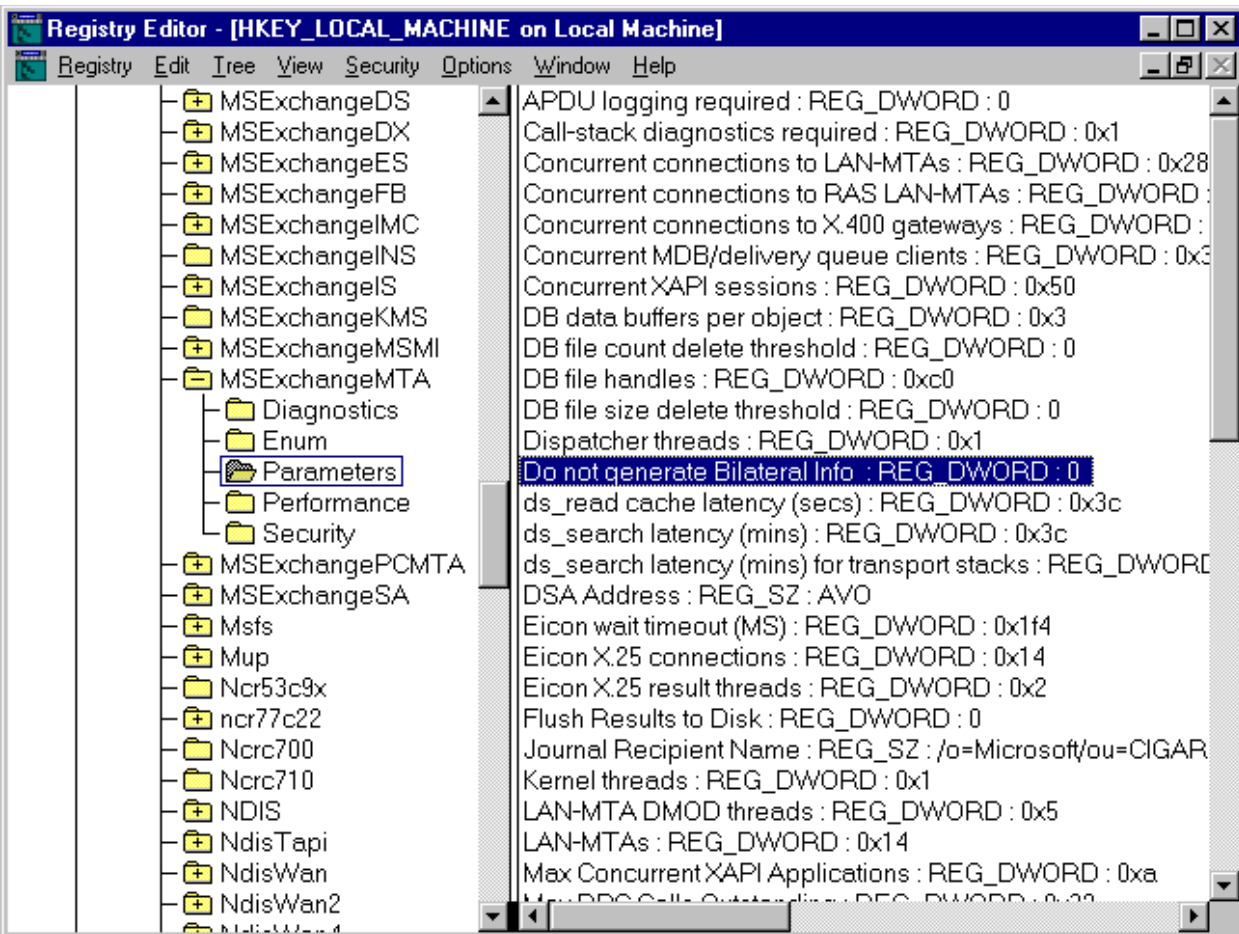
- For more information, see Microsoft Knowledge Base article Q157358, "XCON: Per-Domain-Bilateral-Info and Third Party Systems." You can find this and other Microsoft Knowledge Base articles on the Microsoft support Web site at: http://www.microsoft.com/support.

- Message Journaling can only capture messages that pass through the Exchange Server MTA. If a user connects to an external e-mail server using a client that submits e-mail using SMTP (POP3 and IMAP4 clients) without passing through

Exchange Server, the messages are be captured. Likewise, messages sent using other e-mail systems (such as Microsoft Mail) that do not pass through an Exchange Server computer cannot be captured, even if the other e-mail system has a connector to an Exchange Server computer.

Table Of Contents