Exchange 2010 Journaling Guide

Websense® Email Security Solutions
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) 10
  Implement journal rules (select users only) ........ 11
  Disable NDRs (non-delivery reports) ............... 13
Troubleshooting tips ..................................... 16
Journaling best practices ............................... 18
Remove Exchange 2010 journaling setup .......... 19
  Remove address space domain ..................... 20
  Deactivate journaling ................................. 20
  Remove journal rule .................................... 22
  Remove the distribution group ..................... 23
  Remove SMTP send connector ...................... 23
  Remove the journaling contact .................... 26
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 2010. 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 2010 journaling setup*, page 19

### 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 2010 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 2010.

Exchange Server Prerequisites:

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

**Set up the journaling process**

To configure Journaling on your Exchange 2010 server, follow these steps:

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

**Create a journaling contact**

1. Select **Start > All Programs > Microsoft Exchange Server 2010 > Exchange Management Console.**
2. Click the + sign to the left of your Exchange server.
3. Click the + sign to the left of Recipient Configuration.
4. Click **Mail Contact** under Recipient Configuration.
5. In the Mail Contact page (a), click **New Mail Contact** in the Actions pane (b).
6. Select the **New Contact** option (a) and then click **Next** (b).
7. 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).
8. Type the journaling address provided to you (a) and then click OK (b).

![SMTP Address dialog box]

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

9. Click Next.
10. Click New.
11. Click Finish.

You have successfully created a journaling contact as shown below.

**Create an SMTP send connector**

2. Click the + sign to the left of your Exchange server.
3. Click the + sign to the left of Organization Configuration.
4. Click Hub Transport.
5. Click the Send Connectors tab.
6. In the Actions pane, click New Send Connector.
7. Type Journaling Connector for the Name field, for the Select the intended use for this Send connector drop-down list, select Custom (a). Click Next (b).

8. Click Add. The SMTP Address Space window opens.
9. In the Address field, type the Address Space (a). Leave the cost at 1 and then click OK (b).

10. Click Next.

11. Select the **Route mail through the following smart hosts** option and then click Add.

12. Select the **Fully qualified domain name (FQDN)** option, type the smart host provided to you and then click OK.

13. Click Next.
14. Select None for the Configure smart host authentication settings and then click Next.

**Note**
Exchange 2010 servers automatically send all outbound email via TLS encryption: no outbound security configuration is required by the Administrator.

15. Click Next.
16. Click New.
17. Click Finish.

You have successfully created a send connector as shown below.

---

**Activate journaling**

2. Click the + sign to the left of your Exchange server.
3. Click the + sign to the left of Organization Configuration.
4. Click Mailbox.
5. In the Database Management tab, right click your mailbox database and select Properties.

6. Click the Maintenance tab.
7. Select the **Journal Recipient** check box (a), and then click **Browse** (b).
8. Select **Journaling Contact** (a) and then click **OK** (b).

9. Click **OK**.

You have successfully activated message journaling.

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

1. Select **Start > All Programs > Microsoft Exchange Server 2010 > Exchange Management Console**.
2. Click the + sign to the left of your Exchange server.
3. Click the + sign to the left of Recipient Configuration.
4. Click **Distribution Group**.
5. In the Actions pane, click **New Distribution Group**.
6. Select the **New Group** option and then click **Next**.
7. In the New Distribution Group window, type Journaling Distro in the Name field and Alias field (a). Click Next (b).

![New Distribution Group window](image)

8. Click New.
9. Click Finish.

You have successfully created a distribution group.

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

**Implement journal rules (select users only)**

2. Click the + sign to the left of your Exchange server.
3. Click the + sign to the left of Organization Configuration.
4. Click Hub Transport.
5. Click the Journal Rules tab.
7. In the **Rule Name** field, type Journaling Rule (a) and then click **Browse** (b).

8. Select Journaling Contact from the list and then click **OK**.

9. Select the **Journal messages for recipient** check box and then click **Browse**.
10. Select Journaling Distro from the list (a) and click OK (b).

![Select Recipient - Entire Forest](image)

11. Click New.

12. Click Finish.

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

**Disable NDRs (non-delivery reports)**

2. Click the + sign to the left of your Exchange server.
3. Click the + sign to the left of Organization Configuration.
4. Click Hub Transport.
5. Click the Remote Domains tab.
7. In the **Name** field, type a name for the remote domain (a), in the **Domain name** field, type the domain name of the Address Space provided to you in the Domain name field (b). Click **New** (c).

8. Click **Finish**.

**Note**
If your **Address Space** is **Address.Space@AddressSpace.com**, then the **Address Space** domain is **AddressSpace.com**.
9. Right click Address Space Domain and then select **Properties**.

10. Click the **Message Format** tab.
11. Ensure the **Allow non-delivery reports** check box is deselected (a) and then click **OK** (b).

![Address Space Domain Properties](image)

12. 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 click **OK** (b).

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

d. A dialog displays with the following message: "Microsoft Exchange Transport service is being restarted." When the dialog closes, 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.

---

**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 ta
- Make sure you hide the journal recipient(s) from your Global Address List (GAL).
- Envelope Journaling using journaling rules
  - 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.
    - Open EMS
    - Set-transport agent: identity is "journaling agent," priority is "1".
• Restart services (services.msc) for MSExchangeTransport or via a Command window by typing net stop msexchangetransport & net start msexchangetransport.

• I want to journal all messages on my Exchange server, but do not want to enable journaling on each mailbox store.

• Create a new journaling rule, seen in the figure below.

  - On Send journal reports to e-mail address, click **Browse** to select a contact.
  - Select **Global – all messages**.
  - 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.

• Set-Mailbox &lt;Journal Mailbox Name&gt; -AcceptMessagesOnlyFrom "Microsoft Exchange" –RequireSenderAuthenticationEnabled:$true

## Remove Exchange 2010 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 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 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

2. Select the + sign to the left of your Exchange server.
3. Select the + sign to the left of Organization Configuration.
4. Select Hub Transport.
5. Click the Remote Domains tab.
6. Right click Address Space Domain and then select Remove.
7. Click Yes to confirm.

You have successfully removed the Address Space Domain.

Deactivate journaling

2. Select the + sign to the left of your Exchange server.
3. Select the + sign to the left of Organization Configuration.
4. Select Mailbox.
5. Within the **Database Management** tab, right-click your mailbox database and select **Properties** from the drop-down menu.
6. Select the **Maintenance** tab within the resulting Mailbox Database Properties window. Deselect the **Journal Recipient** check box (a) and then click **OK** (b).

You have successfully deactivated journaling

**Remove journal rule**

1. Open the Exchange Management Console window by selecting **Start -> All Programs -> Microsoft Exchange Server 2010 -> 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 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

2. Select the + sign to the left of Recipient Configuration.
4. Select the Distribution Group for the journaling setup you are deleting (a), from within the list, and 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 SMTP send connector

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. From the **Send Connectors** tab, 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, then this Send Connector must be deleted. Click **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 Send Connectors list (a), and 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

2. Select the + sign to the left of Recipient Configuration.
3. Select Mail Contact, within the Recipient Configuration node.
4. Your Mail Contacts display in a list. To find the Mail Contact associated with your journaling setup, follow these steps:
   a. Right-click a Mail Contact, from within the list, and then 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.

![Image of Journaling Contact Properties 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 Exchange 2010 journaling setup.