



Cryoserver

Exchange Envelope Journaling for Cryoserver

A detailed guide to configure Envelope Journaling for Cryoserver



Forensic & Compliance Systems Ltd
32 – 38 Lemon Street
London, E1 8EW
Tel: + 44 (0) 800 280 0525
info@cryoserver.com
www.cryoserver.com

Contents

Table of Figures.....	2
Exchange Envelope Journaling for Cryoserver	3
What is Envelope Journaling?.....	3
Supported Exchange versions.....	3
Supported Cryoserver versions	3
Overview of Envelope Journaling for Cryoserver	3
Exchange Set-up.....	4
Turn On Envelope Journaling flag	4
Turn On email forwarding.....	4
Routing journal mail to Cryoserver - connectors.....	6
The default connector.....	7
The Cryoserver Connector	8
Creating an Un-Archived Mail Store.....	9
Creating a Journal Mail Account.....	11
Set up Journal Mail Forwarding to Cryoserver	13
Configuring Cryoserver	16
Cryoserver Message Flow Monitoring.....	18
Testing the Email routing.....	18
Testing the Cryoserver Log-in	18
Enabling Journaling.....	19
Hide the Cryoserver Journal user from the address book.....	19
Clearing Down Journalled mail	20
Creating a Mailbox Management Policy.....	20
Scheduling the Mailbox Management Policy.....	23
Additional Exchange settings.....	25
Forwarding mail from Cryoserver to Exchange	25
Allowing Cryoserver service Alert emails to be relayed	26
Multiple Company per Exchange support	28
Exchange Configuration requirements	28
Cryoserver Configuration requirements.....	29
Summary	30
References	31

Document Version

4 th Sep 04	Mbeedell	Document basic Exchange Journaling
4 th May 05	Mbeedell	Extended to incorporate Envelope Journaling

Table of Figures

Figure 1 - a format that allows auto forwarding	5
Figure 2 - Set the body as plain text option.....	5
Figure 3 - Ensure that the Allow automatic forward is selected.....	6
Figure 4 - Connectors in Exchange	7
Figure 5 - The default connector uses DNS	7
Figure 6 - The default connector Address Space & Cost settings.....	8
Figure 7 - The Cryoserver connector – using an IP address.....	8
Figure 8 - Adding an SMTP Address Space entry for Cryoserver.....	9
Figure 9 - The final Address Space tab.....	9
Figure 10 - Create a new store that will not be Archived	10
Figure 11 - A Store that does not have Archive enabled	10
Figure 12 - Remove Limits and do not keep deleted items.....	11
Figure 13 - Create a new user to capture Journal email.....	11
Figure 14 - Cryoserver Journal is a good name to choose	12
Figure 15 - Ensure that the password never expires	12
Figure 16 - Select the non-archive mail store.....	13
Figure 17 - View the properties of the new user to see the FQDN.....	13
Figure 18 - The Exchange Delivery Forward to: option does not support Envelope Journaling	14
Figure 19 - Apply this rule to ALL email after it arrives	14
Figure 20 - Select "Yes" to this confirmation box.....	14
Figure 21 - Enter "cryouser@complianceinternet.co.uk" into the To-> box	15
Figure 22 - You must select a delete rule before proceeding this far	15
Figure 23 - The rule is now complete.....	16
Figure 24 - The completed rule.....	16
Figure 25 - Cryoserver Company - LDAP settings	17
Figure 26 - Set the LDAP type to Active Directory.....	17
Figure 27 - Select Envelope spool mode, and enable Message Flow Monitoring.....	17
Figure 28 - Select each mail store that requires Journaling.....	19
Figure 29 - Select the Cryoserver Journal user as the Archive recipient.....	19
Figure 30 - Preventing the Cryoserver Journal user from appearing in the Address book	20
Figure 31 - Adding a new Recipient Policy.....	20
Figure 32 - And select Mailbox Manager as the type of Recipient Policy	20
Figure 33 - Give the policy a name, and the mailbox(es) to which it applies	21
Figure 34 - The Mailbox Manager settings (policy) tab - select Delete Immediately	22
Figure 35 - Folder Retention settings.....	22
Figure 36 - Select a server, and open the properties dialog	23
Figure 37 - Under the Mailbox Management tab, select a custom schedule	24
Figure 38 - Use 15 Minute view, otherwise the policy is run 4 times each hour.....	24
Figure 39 - An example Mailbox Management report.....	25
Figure 40 - Allowing SMTP Connections for Cryoserver.....	26
Figure 41 – Connections; Setting the Cryoserver IP Address.....	26
Figure 42 - Setting up relay for a Cryoserver	27
Figure 43 - Cryoserver is running in host mode. Companies may be added in this mode.	29
Figure 44 - The company Tag must match the name used in the forwarding rule address.....	29
Figure 45 - For each company, a [Servers] button is available	29
Figure 46 - Enter the same server domain name for each company of a shared Exchange.....	29

Exchange Envelope Journaling for Cryoserver

This is a step by step guide to implementing Envelope Journaling on Exchange servers for Cryoserver.

What is Envelope Journaling?

There are three different types of journaling that you can enable in Exchange Server 2003.

- **Message-only journaling** Message-only journaling creates a copy of all messages and the corresponding P2 message header data to and from users on a mailbox database and sends the message copy to a specified mailbox. The P2 message header contains only the message recipient data that the sender declared to the recipients. If an external message is received from the Internet, Exchange journals the P1 message headers. The P1 message header is the address information that is used by message transfer agents (MTAs) to route mail. By default, when message-only journaling is enabled, Exchange does not account for blind carbon copy (Bcc) recipients, recipients from transport forwarding rules, or recipients from distribution group expansions.
- **Bcc journaling** Bcc journaling is message-only journaling with the added ability to capture the Bcc recipients. When Bcc journaling is enabled, Exchange captures all recipients (including Bcc recipients) that are known at the originating server. If this recipient list includes hidden distribution lists, query-based distribution lists, or distribution lists that are expanded on another server, the recipients for these lists will not be included in the journalized mail. This functionality is enabled by setting a registry key. For more information about setting this registry key, see Microsoft Knowledge Base article 810999, "XADM: Bcc Information Is Lost for Journalized Messages in Exchange 2000" (<http://go.microsoft.com/fwlink/?LinkId=3052&kbid=810999>).
- **Envelope journaling** Envelope journaling differs from message-only journaling and Bcc journaling because it permits you to archive transport envelope information (P1 message headers). This includes information about the recipients who actually received the message, including Bcc recipients and recipients from distribution groups. Envelope journaling delivers messages that are flagged to be archived by using an envelope message that contains a journal report together with the original message. The original message is delivered as an attachment. The body of the journal report contains the transport envelope data of the archived message.

Cryoserver works best with Envelope Journaling, because Cryoserver does not need to expand distribution lists – which may have altered since the original email was delivered by Exchange; and because Cryoserver receives the bcc recipient information.

Supported Exchange versions

For envelope Journaling to work you must be running either Exchange server 2003 with SP1 (service pack 1) on all servers, or Exchange server 2000 SP3 with roll-up fixes released after August 2004 (see <http://support.microsoft.com/?kbid=834634>)

Supported Cryoserver versions

You need to be running Cryoserver version 1.3.3e or greater to support Envelope Journaling.

Overview of Envelope Journaling for Cryoserver

For envelope journaling, you need to create a normal user with a mailbox. A copy of every *new* email in Exchange will then be copied to this mailbox, via the 'Archive' option in each mail-store's properties. An enterprise-wide flag in Active Directory tells Exchange that the email that is stored in the journal user mailbox will be adjusted to include the envelope information. An exchange server-side *rule* can then be added to forward all of the journalized emails to an external SMTP recipient (Cryoserver). However, mail will only be sent via this rule after a global Exchange SMTP 'format' is set to allow forwarding in this way. Once sent, the emails can be deleted – which means creating and scheduling a Mailbox Management policy.

Cryoserver simply needs to be configured to expect emails in the Envelope Journal format. Each email is inspected to see if it is actually in the correct format, so that PST file imports and other email sources will continue to be processed correctly.

Exchange Set-up

Turn On Envelope Journaling flag

This flag (known as the 'heuristic') is set in Active Directory, and can be manually created and updated. However, Microsoft have produced a simple DOS command-line utility, **exejcfg**, that sets; un-sets or displays the current flag.

The exejcfg tool is available in the Exchange Server 2003 SP1 download in the i386\RTW directory and can be used in Exchange 2000 or Exchange 2003 environments. You can also download the utility from Microsoft on

<http://www.microsoft.com/downloads/details.aspx?FamilyId=E7F73F10-7933-40F3-B07E-EBF38DF3400D&displaylang=en>

This article is titled: Exchange Server Email Journaling Advanced Configuration.

Once installed (unzipped), you can either read the word documentation describing the tool, or open a DOS window and run the executable. This will tell you the available command parameters. Two examples are shown below:

```
C:\Microsoft\Exchange\ExAllTools\Email Journaling Advanced Configuration\Exejc
fg.exe

Function : Enable/Disable/List the Email Journaling Advanced Configuration featu
re
Usage: exejcfg
        [-e -d -l]
        -e Enable   Email Journaling Advanced Configuration feature for the org
        -d Disable Email Journaling Advanced Configuration feature for the org
        -l List    Email Journaling Advanced Configuration feature for the org
        /? Prints this help message
Example: exejcfg -e
Note:     The domain must have LDAP service for the search.

C:\Microsoft\Exchange\ExAllTools\Email Journaling Advanced Configuration\Exejc
fg.exe -l
ExchangeOrgName : Forensic Compliance Ltd
Email Journaling Advanced Configuration feature is ENABLED
```

Turn On email forwarding

By default exchange will not allow any end user to simply forward emails to an SMTP email address – for example, where an employee wishes to forward a copy of their mail to a home address. This setting is found in Exchange Global Settings, Internet Message Formats.

There will be a default 'format', which you can edit – or you can add a new format specifically for the "complianceinternet.co.uk" domain. This is the Cryoserver archive domain.

Using Exchange System Manager, open the Global Settings and click on "Internet Message Formats". Right-Mouse click and select *New... Domain*.

Enter the following criteria...

[General Tab]

Format Name: Cryoserver
SMTP domain: complianceinternet.co.uk

[Message Format]

MIME message body in plain format (this makes it easier for Cryoserver to 'read' the envelope).

[Advanced]

Tick the *allow automatic forward* option. (This is ticked for *new* formats, but is un-ticked for the standard default format).
The other options can be ticked or un-ticked as required.

The following screen shots show these settings.

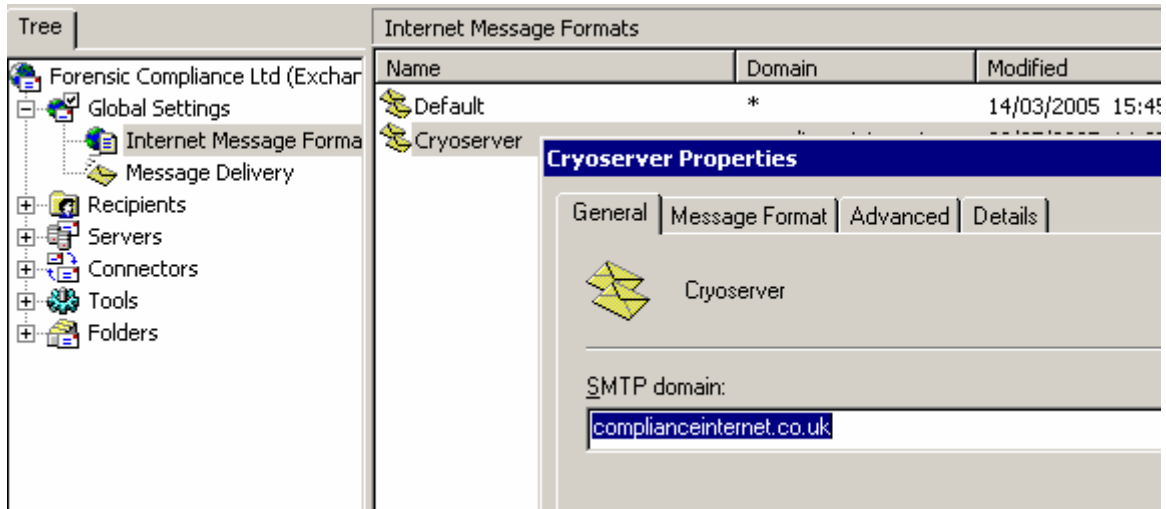


Figure 1 - a format that allows auto forwarding

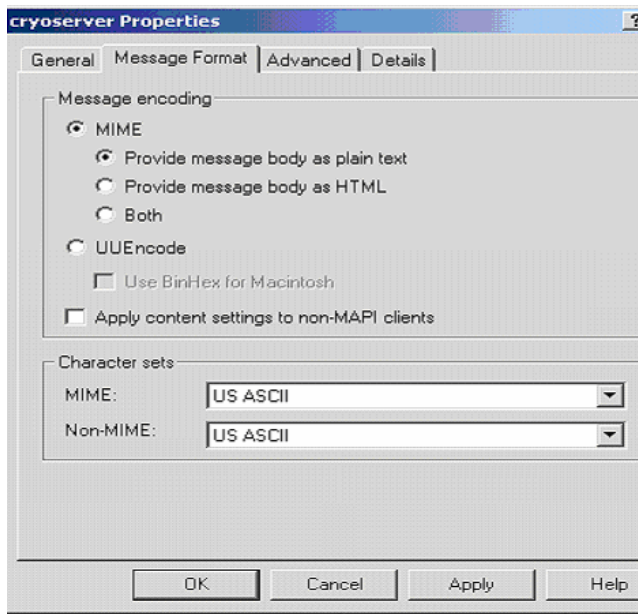


Figure 2 - Set the body as plain text option

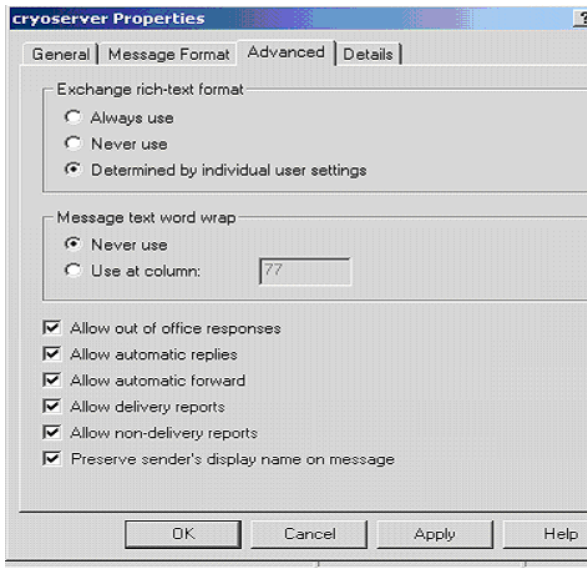


Figure 3 - Ensure that the Allow automatic forward is selected

Routing journal mail to Cryoserver - connectors

Archiving in Exchange 2000 is a feature of an exchange **store**. Every email sent via that store will be bcc'd to the archive recipient. In order for the email to be sent directly from Exchange to Cryoserver, without going through the public web, a connector must be added to instruct Exchange to route these mails separately. The following notes describe how to set this up.

A typical exchange will have a single Internet (SMTP) route or connector. This will route all email [that contain mail with one or more SMTP format email addresses] to the outside world. The aim is to add a new connector that tells exchange to route all cryoserver journal mail to a specific IP address.

Cryoserver is an SMTP end-point or 'smart host' – it will receive SMTP format email destined for *cryouser@complianceinternet.co.uk*. The new connector will only handle mail destined for the *complianceinternet.co.uk* domain, all other domains will be unaffected.

The way that Exchange decides which connector to use for each email is to compare the **address space** (domain list) for each connector. Where two connectors could validly handle an email address, then the one with the *lowest cost* will be selected. If the connectors have the *same* cost, then the connectors are selected randomly or by some load-balancing model.

Therefore, we need to create a connector for Cryoserver which has a *lower* cost than any other that could be a valid match (i.e. the default connector).

Where an organisation has several servers and several Internet connections, then the costing may need to be set in several places.

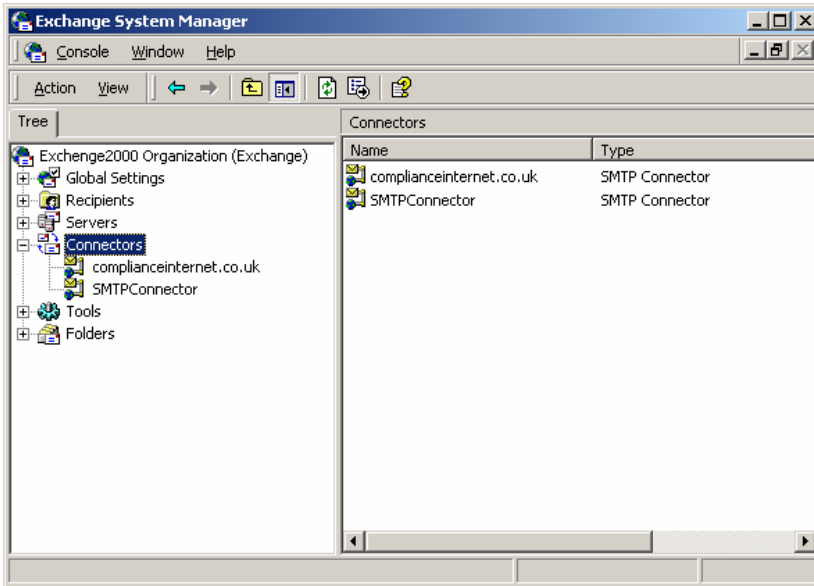


Figure 4 - Connectors in Exchange

The default connector

Exchange does not need a default connector for SMTP mail to work – just installing the SMTP service will suffice. However, it may be clearer to understand if a default connector is used.

The key requirements for the Default connector is that it routes mail using DNS, and that it handles mail for the * address space (i.e. for all domains).

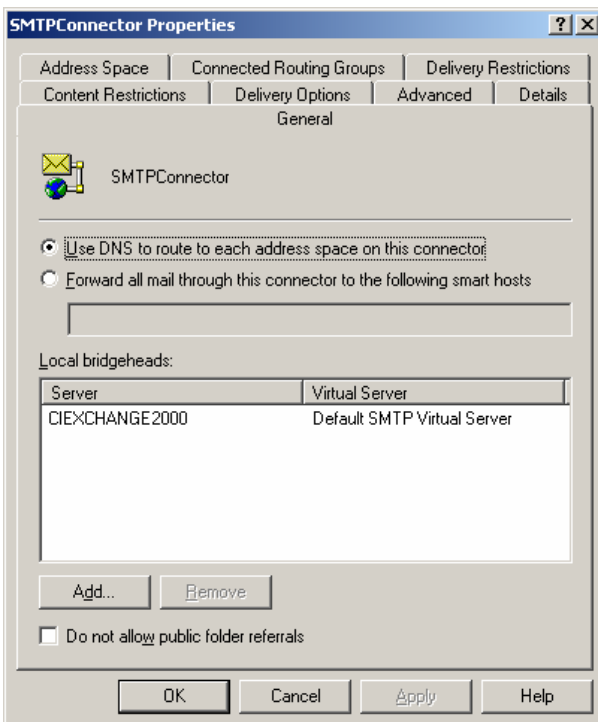


Figure 5 - The default connector uses DNS

The default connector has an address space of *, and (by default) a cost of 1. You *must* adjust the cost to "2" or higher. The actual value does not seem to matter, it just allows you to add connectors that can be selected in preference to this one.

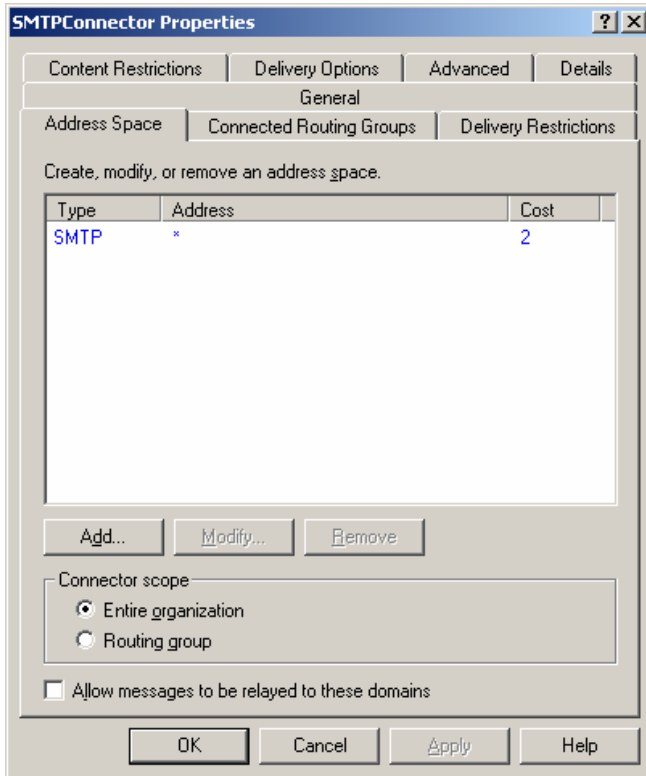


Figure 6 - The default connector Address Space & Cost settings

The Cryoserver Connector

Create another connector that will route mail directly to the Cryoserver. Check the *forward all mail through this connector to the following smart hosts* option. To enter an IP address it MUST be enclosed in square brackets, e.g. [10.10.10.12]. Use a host name if a suitable host record has been added to the local DNS.

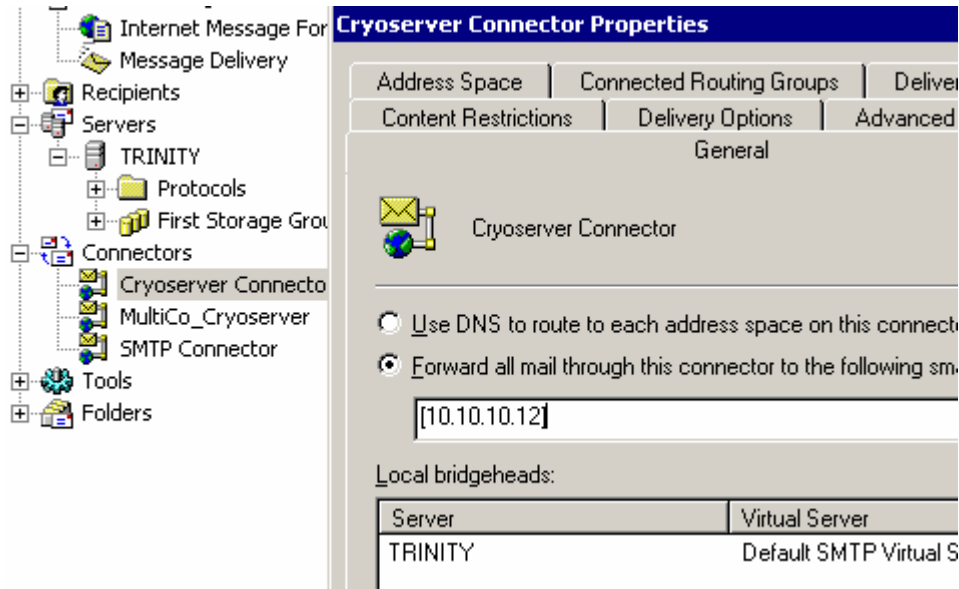


Figure 7 - The Cryoserver connector – using an IP address

Select the Address Space tab, and *add* an entry for type SMTP, with the domain **complianceinternet.co.uk** with a cost of 1 (or a lower value than the default connector).

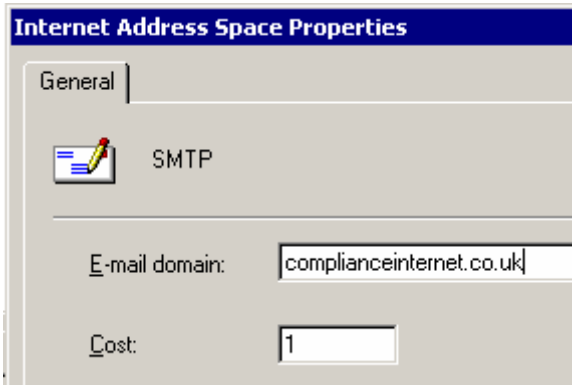


Figure 8 - Adding an SMTP Address Space entry for Cryoserver

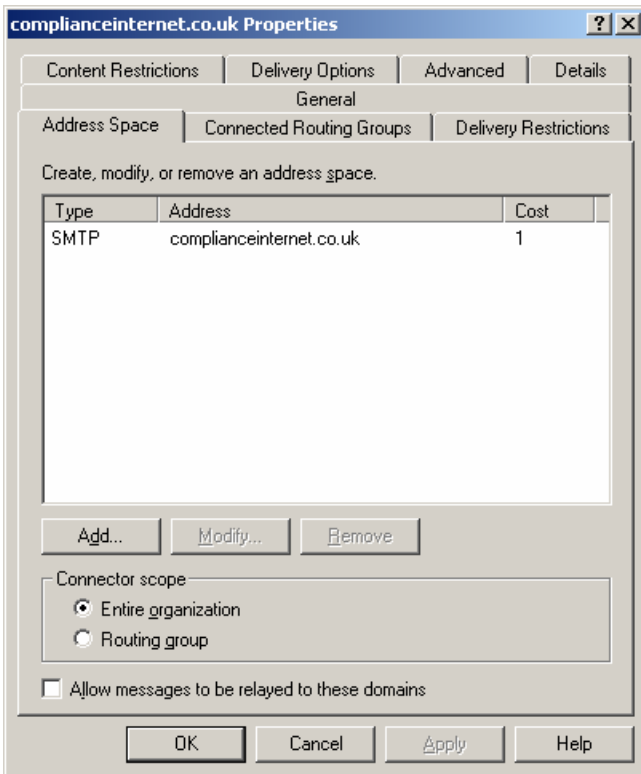


Figure 9 - The final Address Space tab

You can now test this connector by sending a message directly to *cryouser@complianceinternet.co.uk* using Outlook.

PLEASE NOTE: if there is a connectivity issue with Cryoserver, then emails could be routed via the default connector. Cryoserver will not receive them because complianceinternet.co.uk does not really exist.

Creating an Un-Archived Mail Store

Because every email will be forwarded to Cryoserver using an Exchange server-side *rule*, Exchange will attempt to Archive the forwarded messages as well. To prevent this circular journaling from occurring, the Mail Store that contains the Journal user mailbox must not have the "Archive" property turned on.

If you already have a mail store that contains mailboxes that will NOT need to be journaled (say, for holding storing mail from automated email services), then use this. Otherwise, a new store will need to be created.

In an Exchange, you may have 4 Storage Groups, and within each group up to 5 Stores. This makes a total of 20 stores. A simple Exchange set-up will use just two – a default store for all user mailboxes, and a public folder store.

Add a store to any group that has sufficient space, place the database files in the appropriate place. Ensure that the *Archive all messages sent or received by mailboxes on this store* is left blank.

Please remove any limits on this Store, and ensure that the *Keep deleted items for (days)* is set to 0.

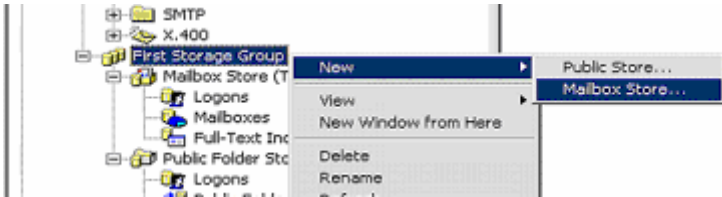


Figure 10 - Create a new store that will not be Archived

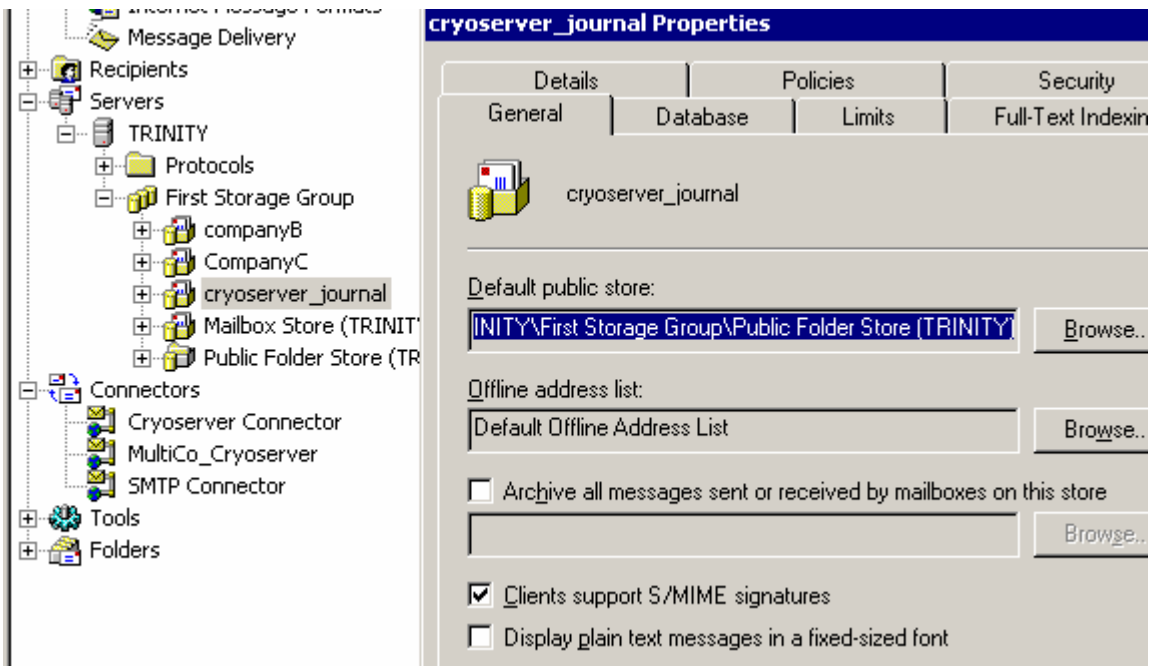


Figure 11 - A Store that does not have Archive enabled

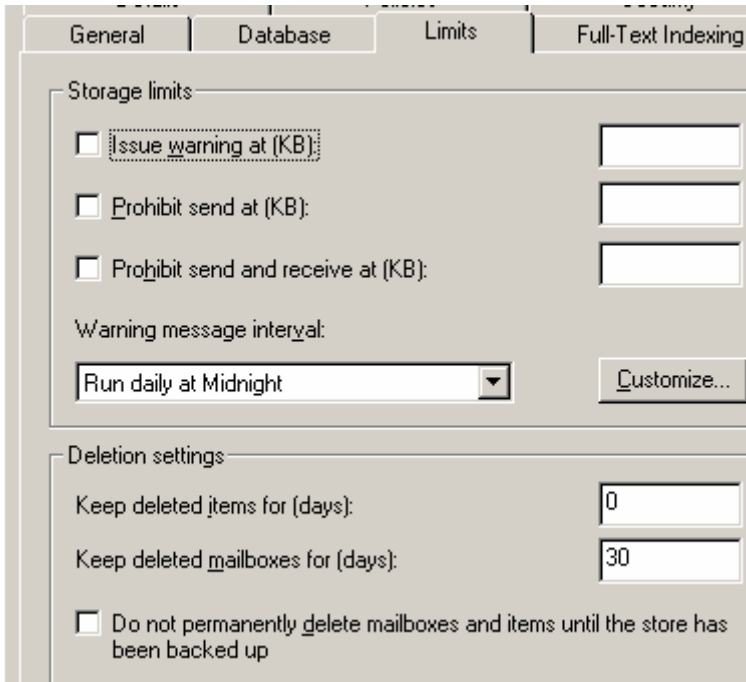


Figure 12 - Remove Limits and do not keep deleted items

Creating a Journal Mail Account

Each mail store that will Journal mail to Cryoserver will actually send mail to a normal user mailbox.

Use the Active Directory Users and Computers facility to add a new user with mailbox. The user can have any name, but *Cryoserver Journal* would probably be easiest to understand later. Please note down the *Full Name*, the *User Logon Name* and *password*, as these will be used later when configuring Cryoserver's LDAP.

Ensure that this user's mailbox is created in the Un-Archived store.

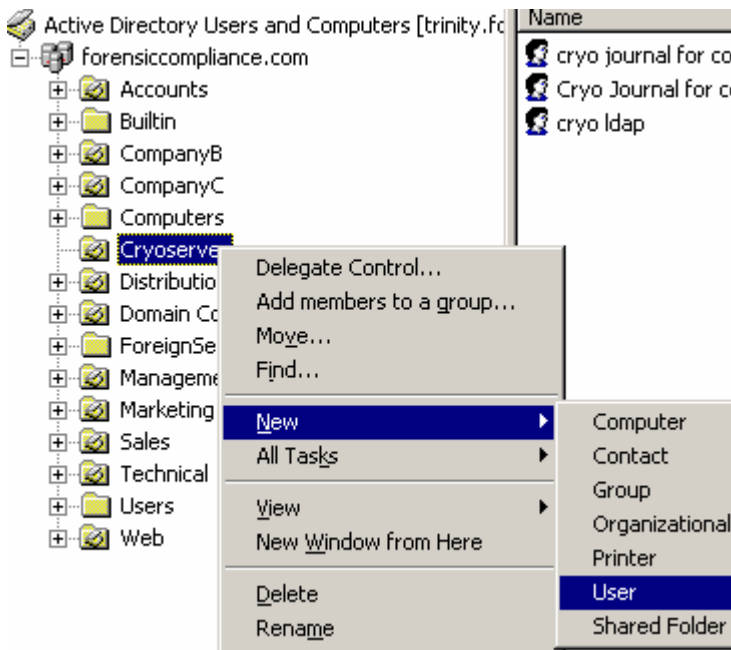


Figure 13 - Create a new user to capture Journal email

New Object - User

Create in: forensiccompliance.com/Cryoserver

First name: Cryoserver Initials:

Last name: Journal

Full name: Cryoserver Journal

User logon name: CryoserverJournal @forensiccompliance.com

User logon name (pre-Windows 2000): FCOMPLIANCE\CryoserverJournal

Figure 14 - Cryoserver Journal is a good name to choose

New Object - User

Create in: forensiccompliance.com/Cryoserver

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

Figure 15 - Ensure that the password never expires

Create in: forensiccompliance.com/Cryoserver

Create an Exchange mailbox

Alias:
CryoserverJournal

Server:
Forensic Compliance Ltd/First Administrative Group/TRINITY

Mailbox Store:
First Storage Group/cryoserver_journal
First Storage Group/companyB
First Storage Group/CompanyC
First Storage Group/cryoserver_journal
First Storage Group/Mailbox Store (TRINITY)

Figure 16 - Select the non-archive mail store

With Users and Computers in View / *Advanced Features* mode, you can see the Fully Qualified Domain Name (FQDN) of this user on the user's property's Object tab. Unfortunately, LDAP requires this information in a different format – as required when configuring Cryoserver later.

Cryoserver Journal Properties

Environment | Sessions | Remote control | Terminal Service

Exchange General | E-mail Addresses

Exchange Features | Exchange Advance

General | Address | Account | Profile | Telephones | Org

Published Certificates | Member Of | Dial-in | Object

Update sequence numbers (USNs) are used to track changes to objects stored in Active Directory.

Fully qualified domain name of object:
forensiccompliance.com/Cryoserver/Cryoserver Journal

Object class: User

Created: 04/05/2005 10:02:33

Figure 17 - View the properties of the new user to see the FQDN

Set up Journal Mail Forwarding to Cryoserver

When journaling is turned on later, emails will be sent to the Journal user mailbox. To get these emails into Cryoserver, they must be forwarded by a server-side rule. The easiest way to create this rule is to use Outlook. [In Exchange 2003, Outlook Web Access may also provide a way to create this rule]. Exchange itself runs all server-side rules, and after it has been set up you will no longer need to access the mailbox using Outlook or OWA.

Please note: the Enveloping of each journaled email occurs just at delivery time to this Journal User mailbox. If you use *Users and Computers* to set the 'Forward to:' option in the *Delivery Options* for the journal recipient mailbox, cryoserver will receive the original emails **without** the envelope wrapper.

The rule requires two actions

1. To forward the email to "cryouser@complianceinternet.co.uk"
2. To move the email to the *deleted items* folder

While you may want to permanently delete each email with the rule, unfortunately you cannot do this with server-side rules. Permanent delete only works when outlook is running.

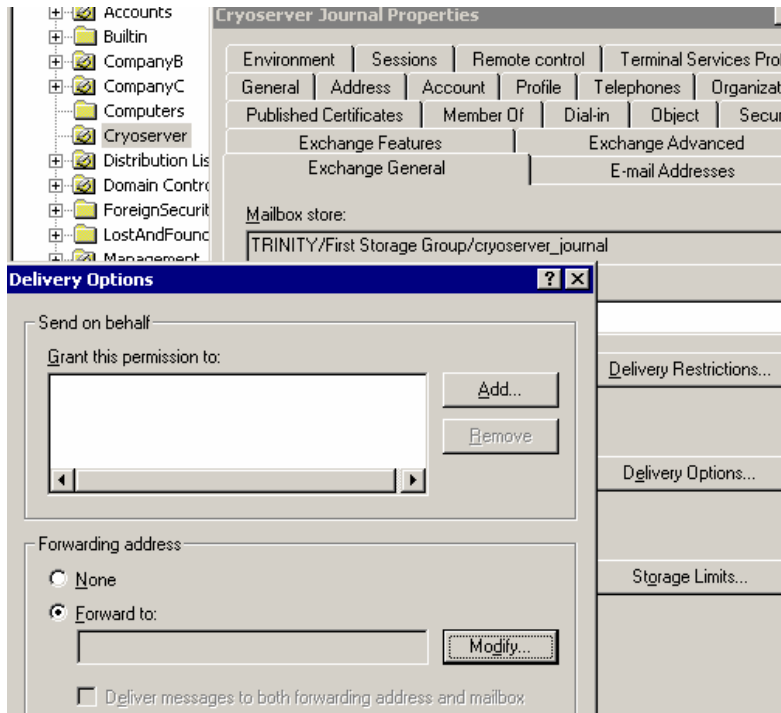


Figure 18 - The Exchange Delivery Forward to: option does not support Envelope Journaling

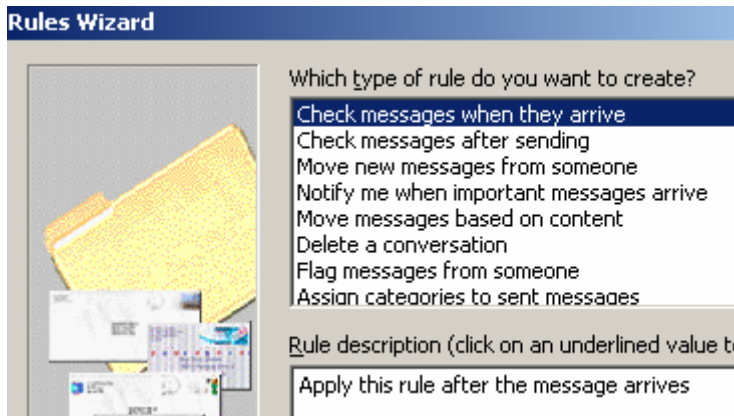


Figure 19 - Apply this rule to ALL email after it arrives

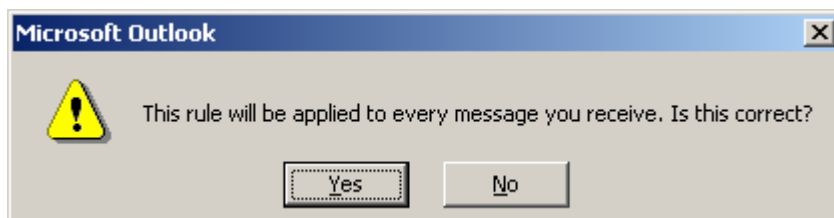


Figure 20 - Select "Yes" to this confirmation box

Next you need to select the user to whom the emails will be forwarded. Select the *forward it to people or distribution list* option and then click on the *people or distribution list* link in the rule box below.

While you can select any existing user in the address book, you actually need to type directly into the large text box on the right (labelled "Specify whom to forward messages to"), and enter *cryouser@complianceinternet.co.uk*.

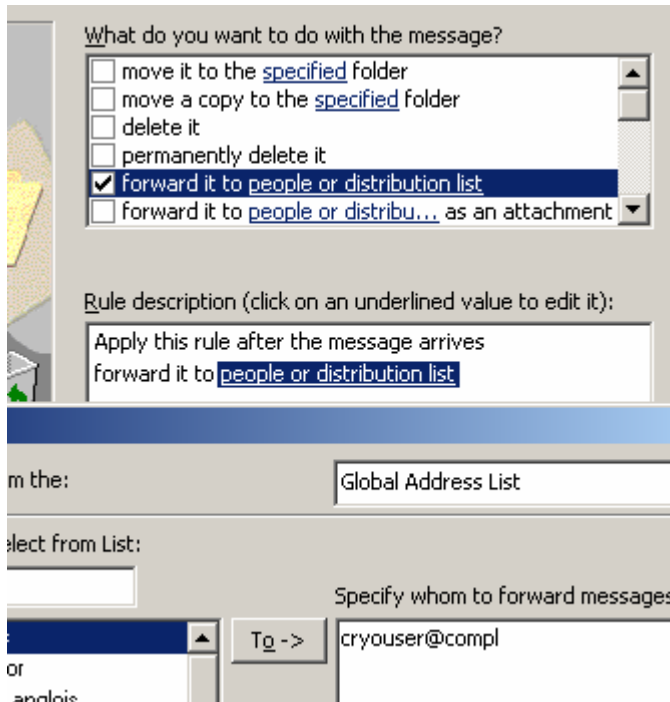


Figure 21 - Enter "cryouser@complianceinternet.co.uk" into the To-> box

You do not need to enter any exception cases to this rule, but you *do* need to add a deletion part to the rule. So if you get this far, press < **B**ack to go back to the actions list.

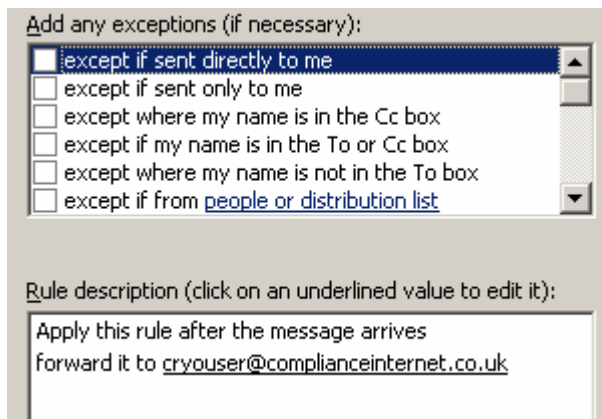


Figure 22 - You must select a delete rule before proceeding this far

What do you want to do with the message?

forward it to [people or distribution list](#)

move it to the [specified](#) folder

move a copy to the [specified](#) folder

delete it

permanently delete it

forward it to [people or distribu...](#) as an attachment

Rule description (click on an underlined value to edit it):

Apply this rule after the message arrives
 forward it to [cryouser@complianceinternet.co.uk](#)
 and delete it

Figure 23 - The rule is now complete

Once the forward and delete (**not** the *permanently delete it* option, but *move it to the <deleted items> folder* is a correct alternative) rules are selected you can press **Finish** or **Next** twice and then provide a suitable name for the rule.

Rules Wizard

Apply rules in the following order:

cryouser@complianceinternet.co.uk

New...
 Copy
 Modify...
 Rename...
 Delete

Move Up Move Down

Rule description (click on an underlined value to edit it):

Apply this rule after the message arrives
 forward it to [cryouser@complianceinternet.co.uk](#)
 and delete it

OK Cancel Run Now... Options...

Figure 24 - The completed rule

While you can run the rule on any test mail in the Journal User mailbox via the **Run Now...** option, it does not appear to be very reliable. Only about 50% of the mails will get forwarded – yet all will be deleted (moved to the deleted items folder). The ones that are successfully forwarded will have a copy in the *Sent Items* folder.

However, the rule appears to be 100% reliable for all *new* mail entering the mailbox. In this case, *no* copy of the forwarded mail is saved into the *Sent Items* folder. This is exactly what we want.

Configuring Cryoserver

Cryoserver will need to be configured to so that user Logins will work, and to expect emails in the Envelope Journal format by default.

To do this, log in to Cryoserver using the Super User url and a super user login account. Select or add a company into which these mails are to be stored, and press the **[Edit]** button.

On the company edit page, enter the LDAP settings corresponding to the company's master active directory domain controller, and the Cryoserver Journal user account details. The Fully Qualified Domain Name (FQDN) for the Cryoserver Journal user account is split into two parts:

1. The directory user, which is in the format of
 cn=<user display name>, ou=<organisational unit>, ou=<parent org unit>
 where the organisational unit list is as long as required;
 or, if the Cryoserver Journal user is added to the built-in 'users' group,
 cn=<user display name>, **cn=users**
2. The LDAP base DN. This contains a set of **dc=** parts that typically correspond to the companies email domain name. It is shown below as dc=forensiccompliance, dc=com.

Please note the other setting shown below.

LDAP server	10.10.10.16
LDAP port	389
LDAP directory user	cn=cryoserver journal,ou=cryoserver
LDAP directory password	*****
Confirm password	*****
LDAP user DN	#
LDAP base DN	dc=forensiccompliance,dc=com
LDAP search DNs	dc=forensiccompliance,dc=com

Figure 25 - Cryoserver Company - LDAP settings

LDAP type

Exchange 5.5
 Active Directory
 Domino 6
 Custom

Figure 26 - Set the LDAP type to Active Directory

By setting the LDAP type to Active Directory, Cryoserver will use preset values for all of the other LDAP settings. Therefore you will not need to enter the *LDAP primary field name*, and so on. These settings are only needed if the LDAP type is set to *custom*.

Spool mode

RFC822
 RFC3462
 Envelope

Average message interval minutes (0, if Message Flow Monitoring)

Feedback email

Figure 27 - Select Envelope spool mode, and enable Message Flow Monitoring

Select the Envelope spool mode, to tell Cryoserver to accept emails in this format. If this is not done, then Cryoserver will store the whole email including the Envelope wrapper part – and all emails will appear to be sent to cryouser rather than the original recipient list.

The Average message interval (Message Flow Monitoring) options are discussed below.

Cryoserver Message Flow Monitoring

Message flow monitoring is available in Cryoserver version 1.3.4 onwards. It is recommended to use the Cryoserver Journal mail account for any Flow Monitoring emails that may be sent. This will ensure that any flow monitoring emails are deleted from Exchange.

A Message flow monitoring email is *only* sent when *no* emails are spooled for processing within the configured **Average message interval**. In this case, an email is sent to the Feedback email account. If this email is *not* received back into Cryoserver within the message interval time, then an alert email is raised.

Possible causes of the Message flow stopping are:

1. Exchange failure leads to the server being re-built and data restored. The Mail-store Archive facility may not be re-configured properly.
2. The Mail-store Archive option may be cleared
3. The server-side rule may fail
4. The routing connector for complianceinternet.co.uk may have been deleted, or be given the same cost as a general SMTP connector (one with * domain rule).

Testing the Email routing

Before Exchange journaling is turned on, you can test to see if mail that is sent to the Cryoserver Journal user mailbox do actually get received by Cryoserver.

Firstly, stop the Cryoserver. We only want to see that the email is received onto the Cryoserver server, and placed into the Cryoserver spool queue sub-directory. A cryoserver engineer is needed to perform this step – otherwise the Cryoserver can be left running and a normal search can be performed to identify the test emails.

Now send a test email to the Cryoserver Journal user. This email should arrive in the Cryoserver Journal mailbox (*without* any envelope – this is only added via the Store Archive feature). The mail is then forwarded to *cryouser@complianceinternet.co.uk* and deleted. The forwarded mail should get delivered directly to the Cryoserver, because the connector matches the *complianceinternet.co.uk* domain part, and routes it to a specific ip address or internal DNS domain name. The mail should be received by the Cryoserver SMTP service, and dropped into the Cryoserver spool directory.

If this works, then a Cryoserver engineer will be able to confirm that the mail has been delivered to Cryoserver correctly.

If the mail does not appear in the Cryoserver spool directory, check

- If Cryoserver is running (the mail would get processed and removed from the spool queue)
- Postfix logs (*/var/log/maillog* or */var/log/mail*)
- Exchange Message Tracking (turn it on, if it is not enabled and repeat the test)
- Cryoserver Journal mailbox, using Outlook or OWA (Outlook Web Access)

The test email can be deleted – or Cryoserver can be enabled and the mail processed in the normal way.

Testing the Cryoserver Log-in

Now that LDAP has been configured, you can test it by performing a normal user log-in.

Ensure that Cryoserver is running, and enter the cryoserver URL into a browser window. Ask an end-user to enter their normal network login details. If the Search screen does not appear, then the Super User company configuration settings may not be quite correct.

Use the LDAP Browser application (installed by default on Cryoservers, in the */root/utills* directory) to validate the LDAP login details for the Cryoserver Journal user.

Please note: the Cryoserver Journal user should have rights to see (read only) the whole of the Active Directory – or at least the parts holding the companies users. Without this, Cryoserver logins cannot work.

Enabling Journaling

Now all of the pre-requisites to Journaling have been performed, you can now turn on the Archive feature on every mail store that requires it.

Locate each Mailbox Store¹ in the Servers branch².

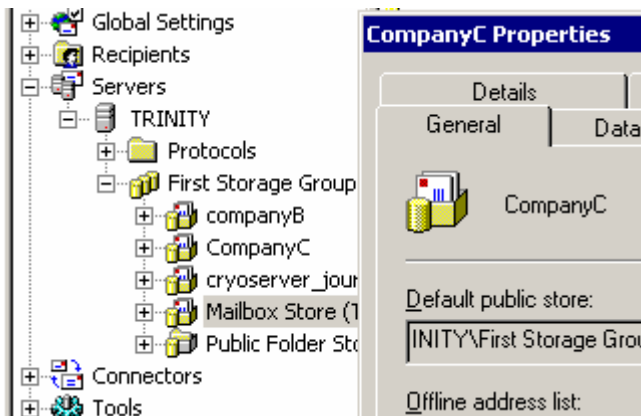


Figure 28 - Select each mail store that requires Journaling

To open the properties sheet - Double-Click a store name or select properties from the Right click menu. Check the “Archive all message” box and set the recipient to the “Cryoserver Journal” user that was previously created.

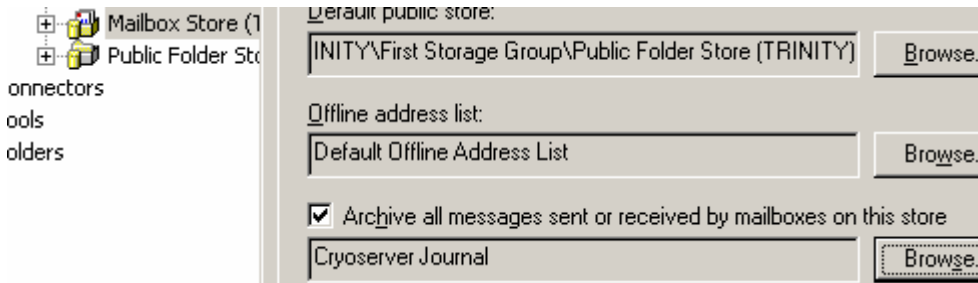


Figure 29 - Select the Cryoserver Journal user as the Archive recipient

Hide the Cryoserver Journal user from the address book

Now that the Cryoserver Journal user has been set up and enabled, it should no longer be needed for selection purposes (such as for selecting the “Archive all messages...” recipient). To prevent peculiar issues where, for example, users send mail directly to the Journal user, the Journal user can be hidden from appearing in the address book.

Using the Active Directory Users and Computers facility, select Advanced Features from the View menu. Select the Cryoserver Journal user and open the Properties dialog box. Under the *Exchange Advanced* tab, check the “Hide from Exchange address lists”.

¹ Public folder stores do not have an Archive facility.

² Note: If you have enabled the *Display Administrative Groups* property for the Exchange Organization, then you will find the Servers listed within the appropriate Administrative group.

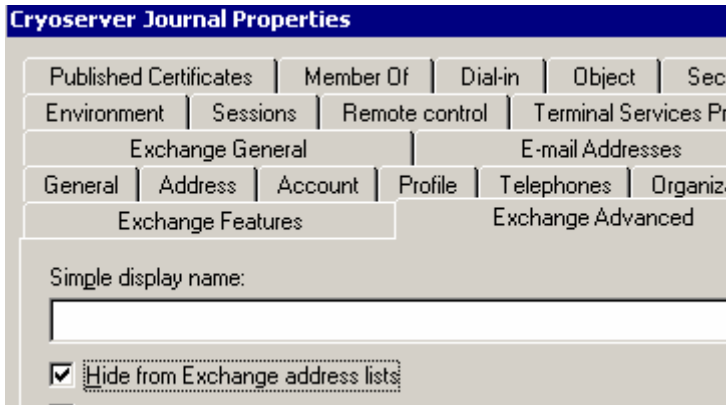


Figure 30 - Preventing the Cryoserver Journal user from appearing in the Address book

Clearing Down Journalled mail

Mail that is archived to the Cryoserver Journal mailbox is not deleted, even by the server-side rule. The rule simply moves mail to the deleted items folder.

To permanently delete the mail items:

1. a Mailbox Management policy is needed.
2. the Mailbox Management policy needs to be scheduled to run regularly.
3. the Mail store's *keep deleted items* property must be set to 0.

Creating a Mailbox Management Policy

To create a new Mailbox Management policy, you create start via the Recipients Policies. Create a new *Recipient Policy...* and set it as a Mailbox Management type.

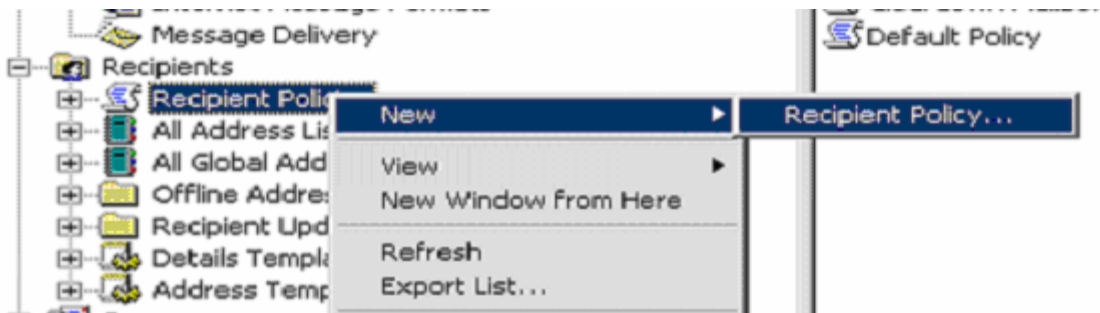


Figure 31 - Adding a new Recipient Policy

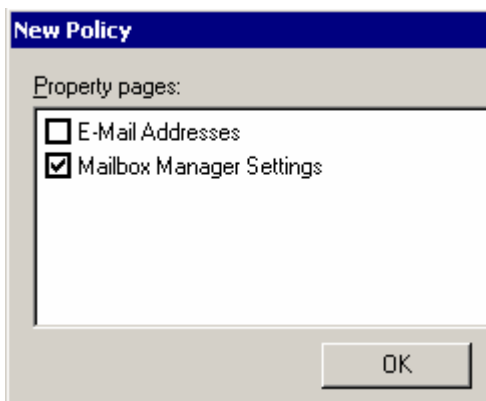


Figure 32 - And select Mailbox Manager as the type of Recipient Policy

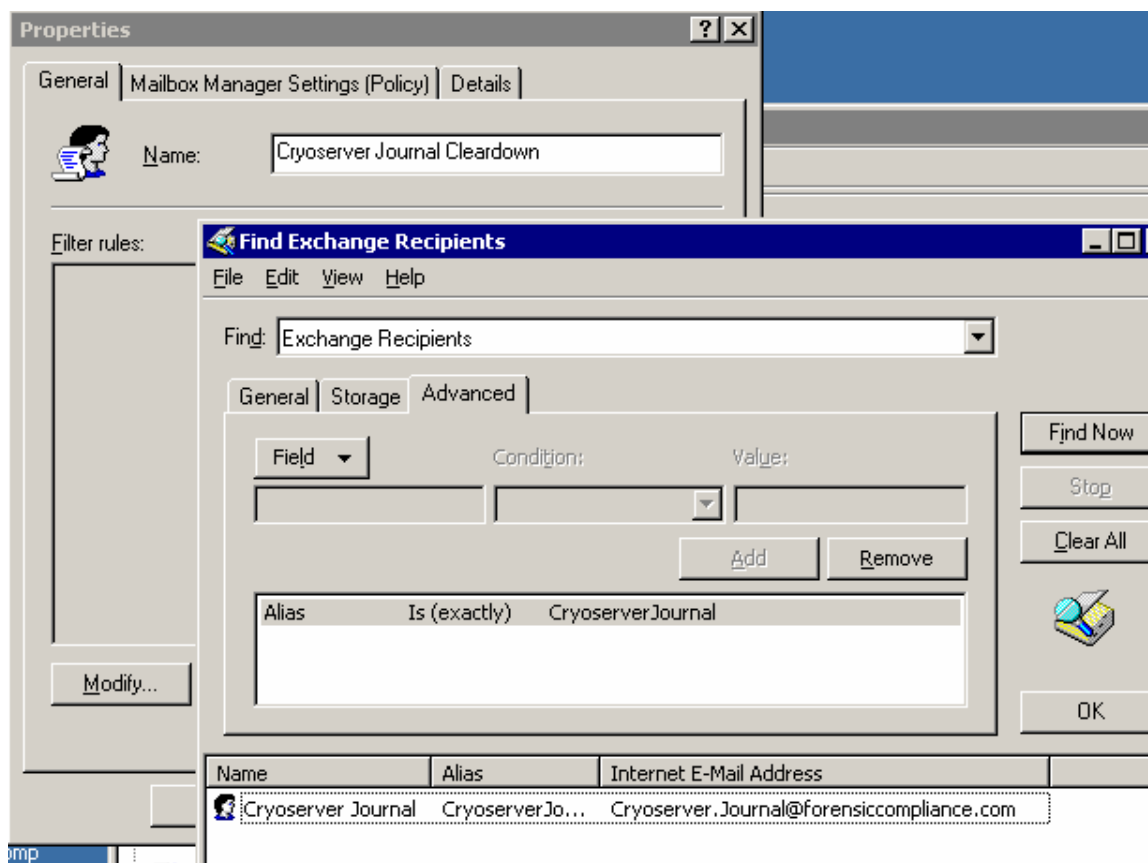


Figure 33 - Give the policy a name, and the mailbox(es) to which it applies

A management policy applies to one or more mailboxes (it does not work with public folders). You need to create a filter rule that selects only the mailboxes that you require. To set up this filter rule, you need to use the *Find Exchange Recipients* dialog box – and this can be most un-intuitive. Unfortunately, it is as bad in both Exchange versions.

The most important thing is that when you press the *Find Now* button in the Find screen, that the list below contains **ONLY** the recipients that the policy should apply to. **WARNING:** If the Find Now list includes additional entries, and you just **highlight** the Cryoserver Journal entry and press OK, then the rule will actually apply to the **whole** list, *not* the highlighted one.

Try to keep this rule as specific and as simple as possible – as shown above.

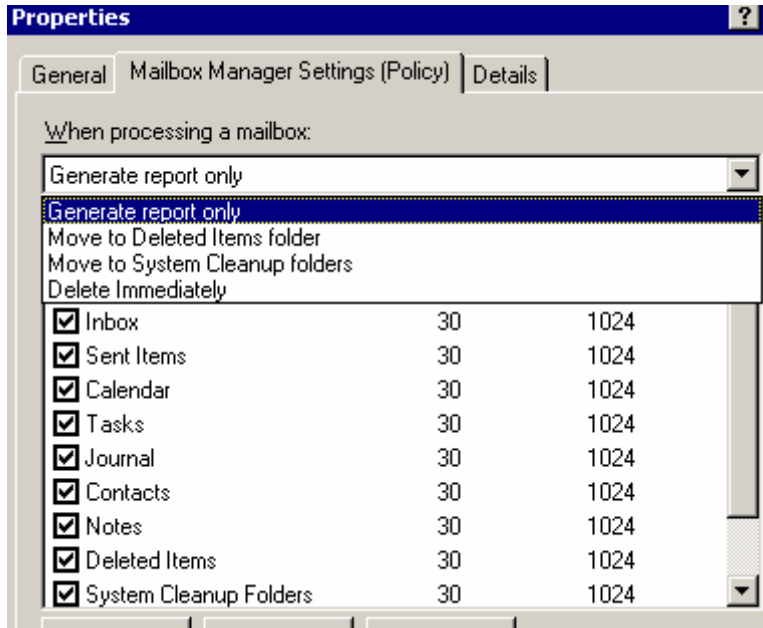


Figure 34 - The Mailbox Manager settings (policy) tab - select Delete Immediately

Select the *Delete Immediately* option under “When processing a mailbox:”.

For each folder listed in the policy, either un-check the tick box (you should not run this rule on the Inbox, for example); or click the folder name to pop-up the Settings dialog box.

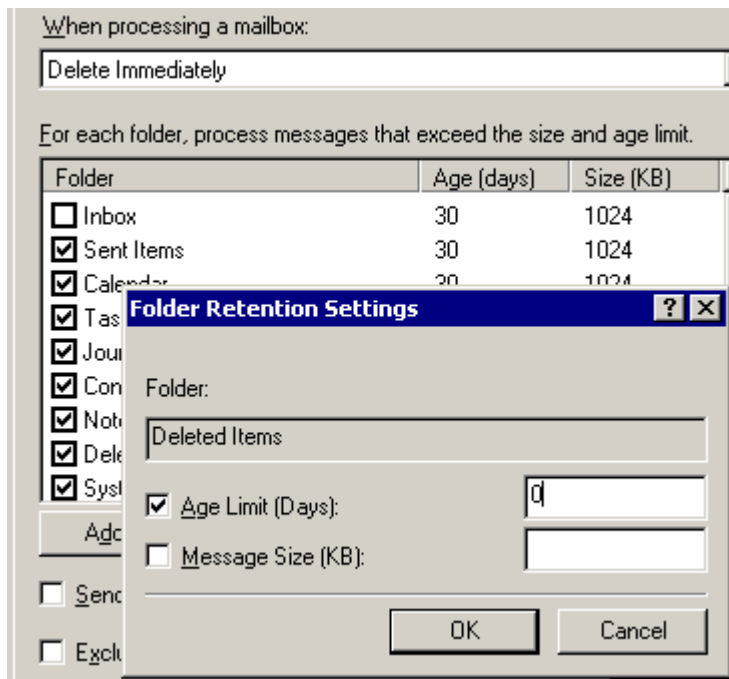


Figure 35 - Folder Retention settings

Set the retention period to 0 or to any reasonable value, and *uncheck* the Message Size option. If the Message Size is included, then mail is only deleted if it is older than the limit AND larger than the size value.

While the Inbox and Deleted Items are the only active folders in the Cryoserver Journal user mailbox, you can set values for any other folder as desired.

Scheduling the Mailbox Management Policy

Schedule this policy to be run on a daily, or regular basis, via the Server properties. Only the server that holds the Cryoserver Journal mailbox needs to schedule the policy.

It is advised that the management processes is scheduled to run before any other daily Exchange or Windows tasks e.g. defragmentation and backup.

Exchange will run *ALL* recipient policies that include a Mailbox Management policy at the scheduled time(s). It is *not* possible to run a specific policy on a specific mail store, or to have multiple or separate schedules for different policies.

Mailbox Management policies can be run manually, by selecting the “Start Mailbox Management Process” menu option for an Exchange Server. Otherwise, open the properties dialog box. Select the Mailbox Management tab, select a Custom Schedule (use ¼ hour time view, or else the Management process will run 4 times for each selected hour).

If you want to see how many emails were removed, select a Reporting option, and select a recipient for the report.

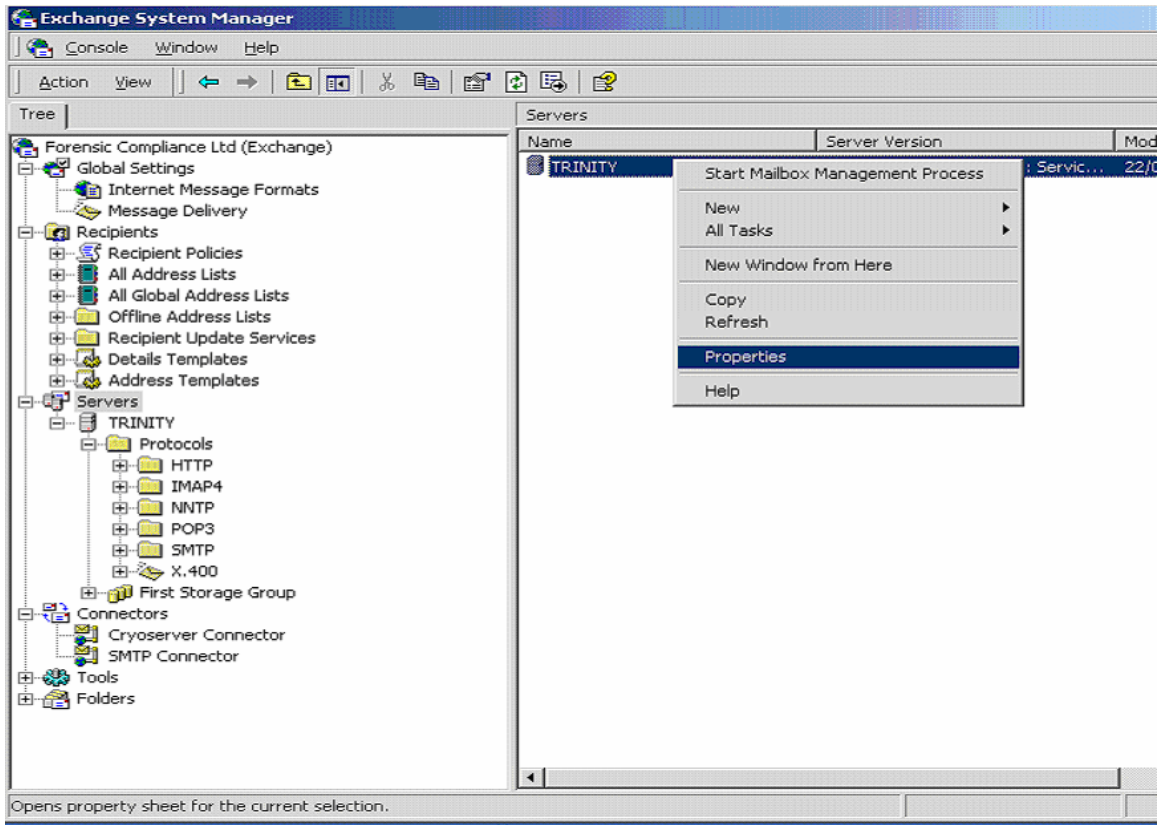


Figure 36 - Select a server, and open the properties dialog

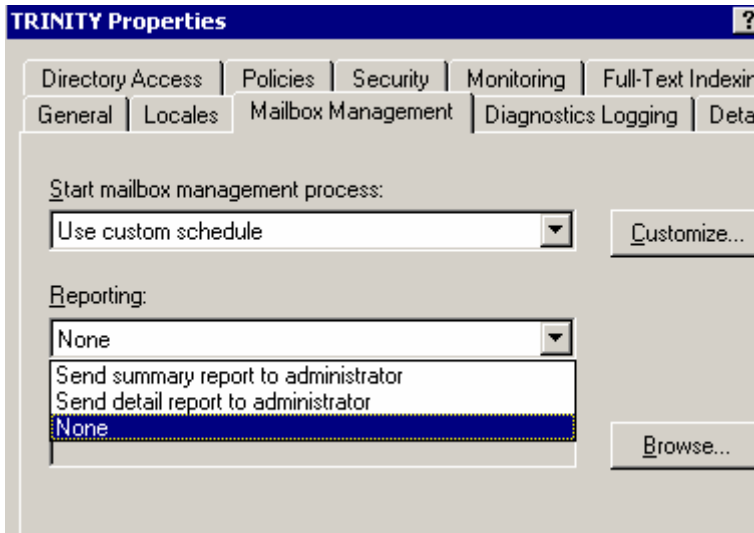


Figure 37 - Under the Mailbox Management tab, select a custom schedule

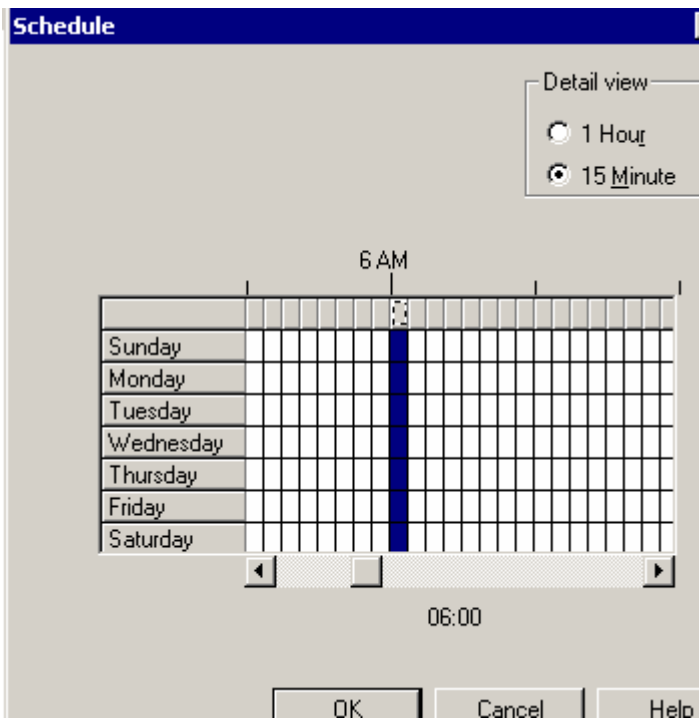


Figure 38 - Use 15 Minute view, otherwise the policy is run 4 times each hour

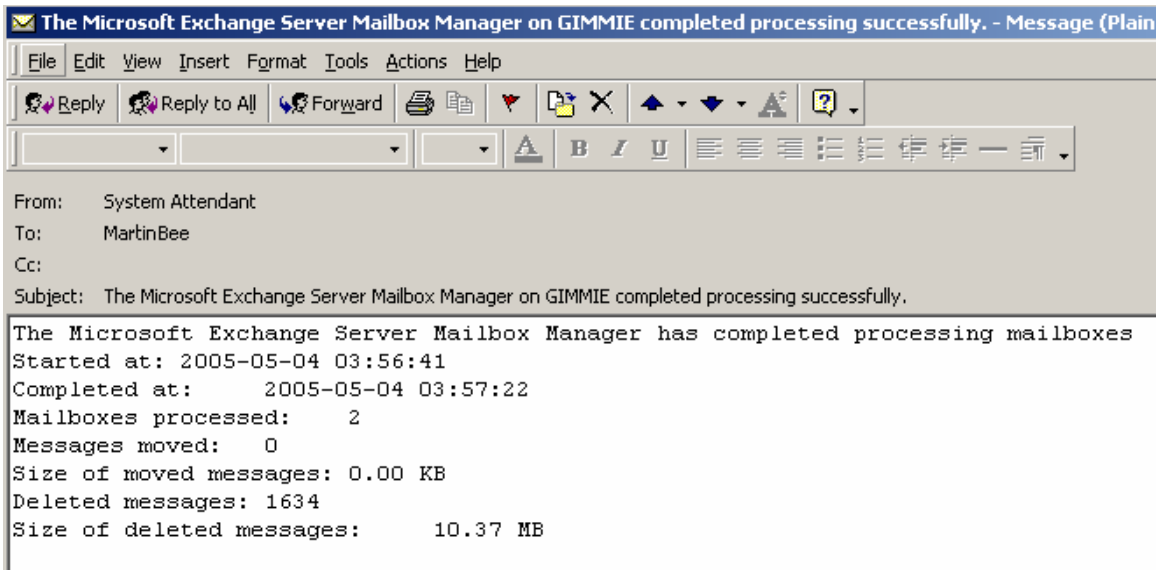


Figure 39 - An example Mailbox Management report

If "Send detail report to administrator" is selected, then the report includes an attachment detailing the mailboxes and folders that were processed.

Additional Exchange settings

Forwarding mail from Cryoserver to Exchange

The exchange server may be configured to accept SMTP from fixed IP addresses – for example, if you have an external Spam and Virus detection service (e.g. MessageLabs). In this case, Cryoserver would not be allowed to send emails back to the Exchange system until the Cryoserver IP addresses have been allowed.

This could also be enforced via the company firewall.

To see if Exchange has SMTP connection restrictions, use the Exchange System Manager and open up the *Protocols* section under the appropriate *Server*. Now display the properties for the SMTP virtual server. Select the second tab (*Access*) as shown below:

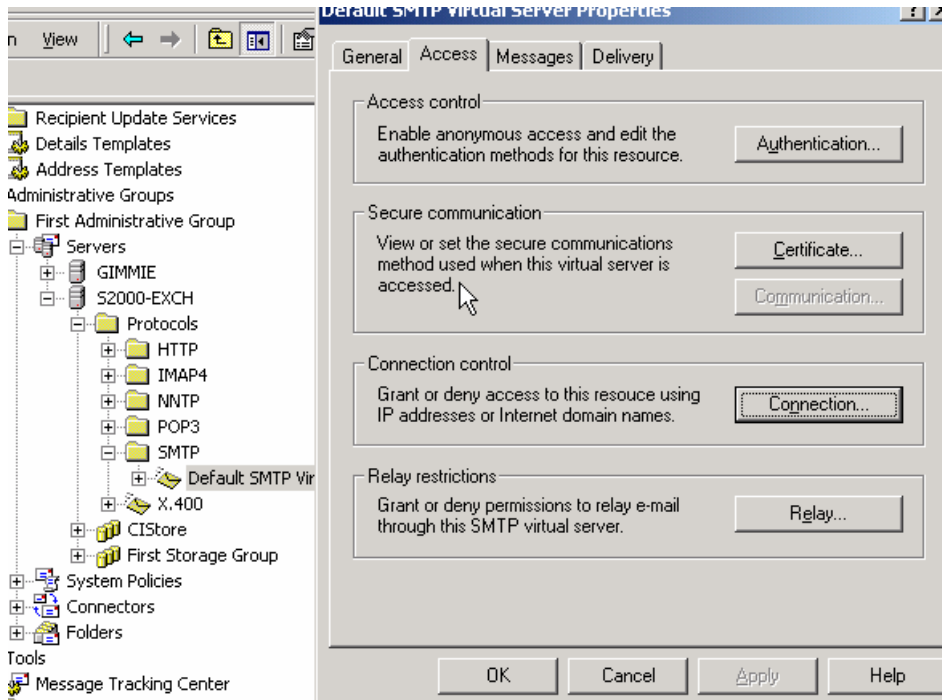


Figure 40 - Allowing SMTP Connections for Cryoserver

Now click the *Connection* button. This allows you to specify single IP addresses, or ranges of addresses, from which SMTP mail may be received. Either allow all connections – and restrict access using the Firewall configuration, or add in the IP addresses of the Cryoserver mail store and also the Cryoserver Web site.

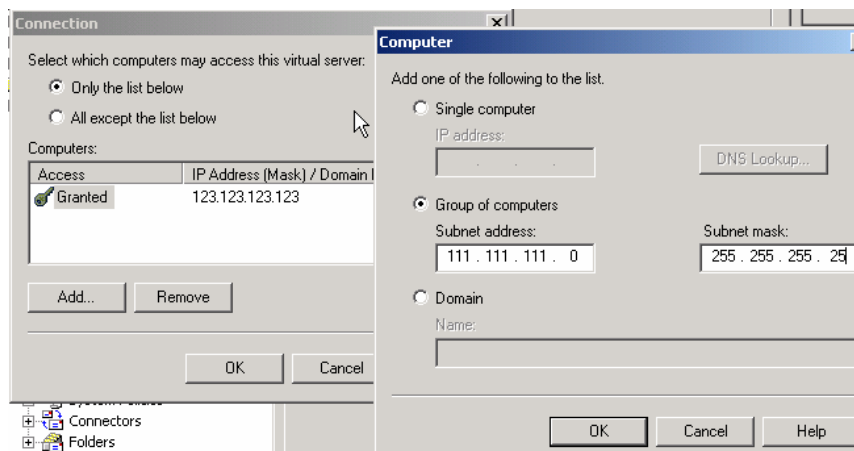


Figure 41 – Connections; Setting the Cryoserver IP Address

Allowing Cryoserver service Alert emails to be relayed

Cryoserver will send alerts when it detects a variety of problems. While these emails may be routed to email addresses within the clients organisation, by default they are sent to Cryoserver engineers. Cryoserver Alert configuration can only be set by a Cryoserver engineer, and any changes require the Cryoserver to be re-started.

For alert emails to be sent directly to Cryoserver engineers (cryoalerts@cryoserver.com), the client's Exchange must be configured to relay these emails. Without relay, the emails will be rejected. In this case, a distribution group can be set up allowing alerts to be sent to both the Client and Cryoserver Engineers in one go.

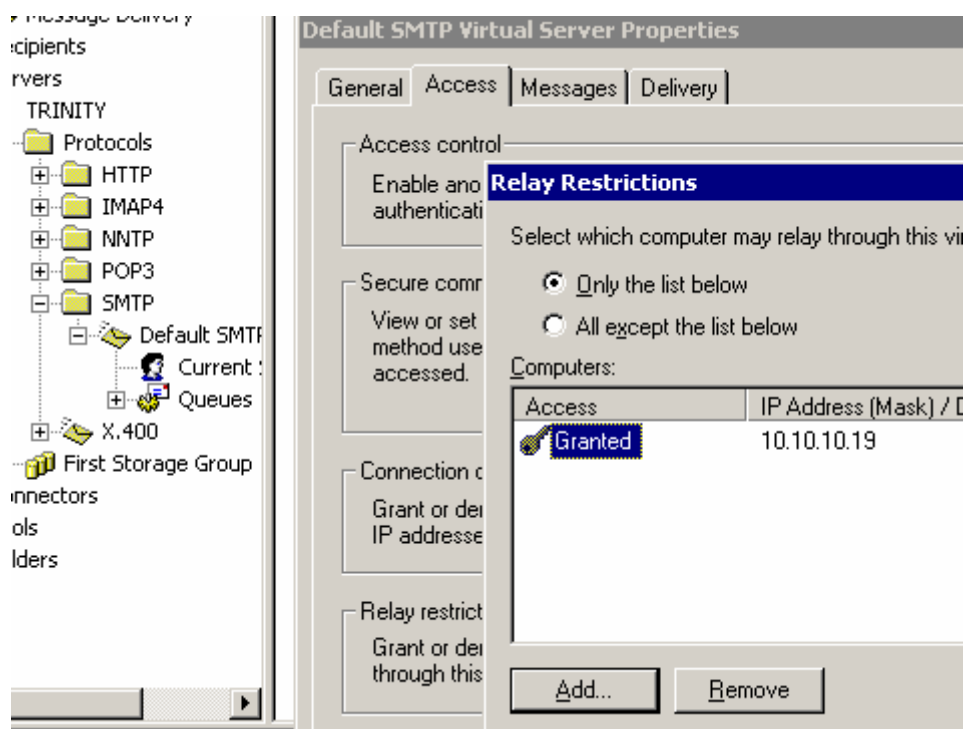


Figure 42 - Setting up relay for a Cryoserver

Multiple Company per Exchange support

Starting with Cryoserver version 1.3.4c, emails from a single Exchange Server but that represent mail from separate companies is now supported. This section documents the requirements for such a configuration.

Normally, Cryoserver will determine (if required) which company the email belongs to by examining the *Received: from <servername>* email header. Where two or more company's emails are hosted on a single Exchange, Cryoserver is unable to determine which company just by reading the *Received: from* header. This method of Company detection is known as 'host mode'.

As an alternative, each email address in the email can be examined and the domain parts of those email addresses used to match against each company registered in Cryoserver. Where domains in email addresses match more than one Cryoserver company, then the email is duplicated and stored separately for each company. This has major drawbacks: First, this is likely to introduce unexpected mail duplication; Secondly, a bcc'd email may not match any company, so it will be errored; Thirdly, this is a very slow and error prone method. This method of Company detection is known as 'domain mode'.

Cryoserver has now extended the 'host mode' facility to detect not only the *Received: from* header, but also to detect the Cryoserver Recipient email address. By assigning a different recipient for each company, cryoserver is able to select the correct company for each email.

Now mail should be sent to *cryouser@companyname.complianceinternet.co.uk*. For example:

cryouser@companya.complianceinternet.co.uk
cryouser@companyb.complianceinternet.co.uk

The company name used here *must match* the Cryoserver **Tag name**, as configured by the Super User administration Edit Company facility.

This process will work even if Envelope Journaling is not used – yet the benefits of Envelope Journaling should mean that this is the only realistic method to use.

Exchange Configuration requirements

The basic requirements are that

1. A company's mailboxes must be stored in separate mail store(s) from other companies.
2. A separate Cryoserver Journal user is needed to capture mail for each company. All of these user accounts should be held in a single non-archived mail store.
3. The mail store 'Archive all mail to...' option must select the corresponding Cryoserver Journal user.
4. The connector that routes mail to the Cryoserver server must include address space domains for either a wild-card entry (*.complianceinternet.co.uk), or separate entries for each company.
5. The server-side rule that forwards emails to Cryoserver must send to the appropriate *cryouser@company.complianceinternet.co.uk* email address.
6. The Mailbox Management process should select all Cryoserver Journal user mailboxes.

It should be noted that if a *single* Archive recipient is selected for multiple mail stores, then a *single* copy of each email is journaled – even where an email is sent to mailboxes in different mail stores.

However, if *separate* Archive recipients are created, one for each mail store (and hence one for each company), then *separate* copies of emails are journaled for each store. Therefore, if an email is sent to recipients in multiple mail stores, there will be separate journal copies of that mail for each mail store.

Cryoserver Configuration requirements

The Cryoserver needs to be running in 'host mode'. A Cryoserver engineer is required to set this mode setting. In the Super User system, the Companies tab will show "Tag Mode: host".

Cryoserver will automatically detect when more than one Cryoserver Company has been configured with the same server name.

When you add each company, ensure that the company Tag name exactly matches the name used in the extended cryouser@**companyname**.complianceinternet.co.uk address. This address is used in the server-side forward-to rule, where Envelope Journaling is used. For non-envelope journaling, a [Active Directory Users and Computers] contact entry will need to be created for each company, and the contact selected in the Archive all mail to... option in each mail store.



Figure 43 - Cryoserver is running in host mode. Companies may be added in this mode.



Figure 44 - The company Tag must match the name used in the forwarding rule address

In this case, the Cryoserver address is "cryouser@dreamkitchens.complianceinternet.co.uk". PLEASE NOTE: You *MUST NOT* change the tag name after emails have been stored for that company. A Cryoserver engineer may change the tag name, because they can adjust the data store values accordingly.



Figure 45 - For each company, a [Servers] button is available

For each company, you *must* enter the same server name. The server name appears in the "Received: from " header of each email that is spooled on the Cryoserver server.

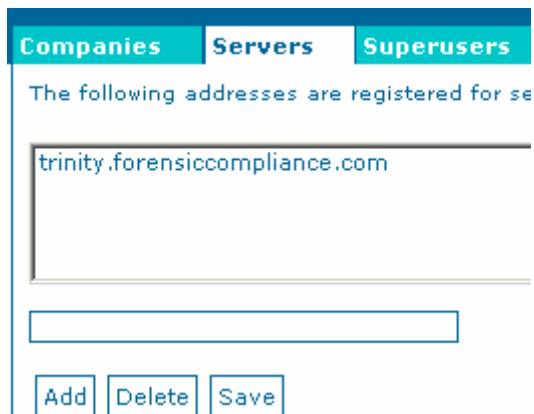


Figure 46 - Enter the same server domain name for each company of a shared Exchange

Summary

Tasks to be performed on the exchange server:

1. Set up a connector for *complianceinternet.co.uk*
2. Send a test message to the *cryouser@complianceinternet.co.uk*
[Stop cryoserver first, then check to see if this message is placed into the Cryoserver spool directory]
3. Create a Mail Store that will NOT have journaling enabled.
4. Create a Journaling recipient user & mailbox (e.g. CryoserverJournalUser). Place the user's mailbox into the non-journaled mail store. This prevents a circular journaling issue.
5. In Global Settings, add an Internet Message Format that allows *Automatic Forward* in plain text format for the complianceinternet domain. [This allows the Mailbox Forwarding rule to work]
6. Using Outlook against the Journal user Mailbox, add a rule that:
 - Forwards ALL mail to *cryouser@complianceinternet.co.uk*
 - Moves the mail to Deleted Items
7. In Recipients/Recipient Policies, add a Mailbox Policy to delete items from the Journal mailbox's Deleted Items. Set this for 1 day, and NO size limit.
8. Schedule the Mailbox Policy to run on a regular (daily) basis.
[Use 15 minute time view, else it runs 4 times each hour]

On the cryoserver:

- If Cryoserver is in 'host' tag.mode, then
 - Extract the server name from the *received: from* email header of the test email (3. above)
 - Add this server name in the Super User Server button for the associated company.
- Use the LDAP Browser utility to confirm the LDAP login and base DN of the Journal User.
 - You need the IP Address/Domain name of the Domain Controller
 - The Base DN is usually in the format: *dc=companyname,dc=co,dc=uk*
 - The user DN is either: *cn=auser, ou=org unit* or *cn=auser, cn=users*
- Enter the Client and LDAP user details in the Super User Company Edit web interface.
 - Just tick the Active Directory option, and leave the LDAP primary/secondary field names blank
- Confirm the above as working by
 - viewing the Super User area of cryoserver - Monitoring tab.
 - logging in as an end user

Completion tasks:

9. Switch on Archiving to the Cryoserver Journal user for the required Private Message Store(s):
Note the Date & Time for this:
and then hide the Cryoserver Journal and LDAP User from Exchange address lists
10. Send an email (to any recipient)
11. Check web access – remember it uses *https:*
optionally: arrange for DNS to include a simple host name for the IP address
12. Log in to Cryoserver as a user,
search for some emails (i.e. the email sent in step 9) [*allow up to 5 minutes for this*],
verify that *forward to inbox* works
13. Set up Data Guardians, via the Super User admin area.
14. Set up privileged accounts, via the Admin user.
15. Test the privileged access Search
Confirm that you receive an Audit alert
16. Make sure Exchange is configured to accept SMTP connections from Cryoserver IP address(es)
[this allows forward to inbox, and audit emails to work]

References

This is Microsoft's comprehensive online documentation regarding Envelope Journaling.

<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/journaling.mspx>

Some additional notes can be found here:

<http://support.microsoft.com/default.aspx?scid=kb:en-us:843105>

This includes the link for the Envelope Journaling Switch utility (to turn the "Heuristics" setting On or Off).